Plan

Lecture 1: Kripke-Joyal, some examples

Lecture 2: Another example, Zariski topos

Lecture 3: Zariski topos, light condensed sets; towards higher topos

Zariski spectrum

A *support* of a ring A is a pair L, d where L distributive lattice and $d : A \to L$ such that

$$d(0) = 0 \quad d(1) = 1 \qquad d(ab) = d(a) \wedge d(b) \qquad d(a+b) \leqslant d(a) \vee d(b)$$

Define the Zariski lattice $Z(A), D$ to be the *universal* support

We write $D(b_1, \dots, b_n)$ for $D(b_1) \vee \cdots \vee D(b_n)$ they represent exactly the *compact open* of the Zariski spectrum (as a topological space)

Zariski spectrum

Solution of a given universal problem

$$\begin{tikzcd}
A \arrow[r, "D"] \arrow[dr, "d"'] & Z(A) \arrow[d, dotted] \\
 & L
\end{tikzcd}$$

It can be realized as the lattice of radical of finitely generated ideals

$D(a) = \sqrt{(a)}$

Zariski spectrum

$D(a) \leqslant D(b_1, \ldots, b_n)$ iff a power of a belongs to $(b_1, \ldots, b_n)$

$D(a) = 0$ iff a is nilpotent

Think of $D(a)$ as $a \notin \alpha$ where α is a *prime ideal*

The terminology *ideal* comes from Kummer: analogy with chemistry, thinking of a *prime ideal factor* as a *ideal simple element* (he even had in mind a concrete ideal simple element, fluorine, that was later isolated!)

This example of prime ideal factor was then used by Hilbert in his program

Zariski spectrum

$A \to A_\alpha$ universal solution for forcing all $a \notin \alpha$ invertible

A_α is a *local* ring: $\forall_x U(x) \vee U(1-x)$ holds in this ring

$A \to A[1/a]$ universal solution for forcing a to be invertible

If $D(b) \leqslant D(a)$ there is a canonical map $A[1/a] \to A[1/b]$

If $D(b) \leqslant D(a)$ then $D(b)$ gives more information about α than $D(a)$

$D(b)$ is a smaller open set than $D(a)$

Zariski spectrum

We have the *local-global* principles if $1 = (b_1, \dots, b_n)$

Lemma: *A linear system in* A *has a solution iff it has a solution in each* $A[1/b_i]$

Lemma: *If* u_i *in* $A[1/b_i]$ *and* $u_i = u_j$ *in* $A[1/b_i b_j]$ *then there is a unique* u *in* A *such that* $u = u_i$ *in each* $A[1/b_i]$

(I don't write explicitely the canonical maps $A[1/b_i] \rightarrow A[1/b_i b_j]$)

The proofs are elementary (the second is non trivial, and not so easy to formalize in Lean or Agda)

Forcing over Zariski spectrum

Let k be an *arbitrary* commutative ring

Define $R(D(a)) = k[1/a]$

If $D(b) \leqslant D(a)$ we have a transition map $k[1/a] \to k[1/b]$

Theorem: R *defines a* sheaf *over the Zariski spectrum* $Z(k)$

This is an application of the second local-global principle

Interpretation: $D(a)$ finite piece of information about α and $k[1/a]$ finite approximation of k_α

Forcing over Zariski spectrum

$D(a) \Vdash u = v$ if $u = v$ in $A[1/a]$

$D(a) \Vdash \psi_0 \rightarrow \psi_1$ if $D(b) \leqslant D(a)$ and $D(b) \Vdash \psi_0$ implies $D(b) \Vdash \psi_1$

$D(a) \Vdash \psi_0 \wedge \psi_1$ if $D(a) \Vdash \psi_0$ and $D(a) \Vdash \psi_1$

$D(a) \Vdash \psi_0 \vee \psi_1$ if we can find $D(a) = D(b_1, \dots, b_n)$ and $D(b_i) \Vdash \psi_0$ or $D(b_i) \Vdash \psi_1$

This is an instance of *Beth semantics*

Forcing over Zariski spectrum

$D(a) \Vdash \forall_x \psi$ if $D(b) \leqslant D(a)$ and v in $k[1/b]$ implies $D(b) \Vdash \psi(v/x)$

$D(a) \Vdash \exists_x \psi$ if we can find $D(a) = D(b_1, \ldots, b_n)$ and v_i in $k[1/b_i]$ with $D(b_i) \Vdash \psi(v_i/x)$

Note that we don't ask the v_i to be compatible

$D(a) \Vdash \perp$ iff a is nilpotent

Descent

$\exists_x P(x) = 0$

In general if we have only solutions *locally* $P(x_i) = 0$ in $A[1/b_i]$ with $1 = (b_1, \ldots, b_n)$ and these solutions are not compatible, we cannot patch them together (we can if P is linear)

This is a *descent* problem

One insight of Grothendieck was to realize the similarity with Galois descent: if we have a solution in a field extension we can "descend" this solution iff it is invariant by automorphisms (patching condition)

Forcing over Zariski spectrum

The symbol $\Vdash$ was introduced by Dana Scott, who noticed, for intuitionistic derivability

Theorem: *if* $\psi_1, \dots, \psi_n \vdash \psi$ *then* $D(a) \Vdash \psi_1, \dots, D(a) \Vdash \psi_n$ *imply* $D(a) \Vdash \psi$

$D(a)$ represents a finite piece of information about an ideal object

This intuition was fundamental in Cohen's approach to forcing: one forces the existence of a non constructible subset S of $\mathbb{N}$ by using finite pieces of information $X \subseteq S$, $Y \cap S = \emptyset$ about this subset, with X and Y disjoint finite subsets of $\mathbb{N}$

Example

I claim that, if k is *reduced* (i.e. 0 is the only nilpotent element) then we have $k \Vdash \forall_x \neg U(x) \rightarrow x = 0$

Indeed $D(b) \Vdash \neg U(x)$ iff x nilpotent in $k[1/b]$ but $k[1/b]$ is reduced so $x = 0$ in $k[1/b]$

We interpret this as: the “generic” ring R satisfies $\neg U(x) \rightarrow x = 0$

“Almost” but not quite a discrete field, which is the *classically equivalent* condition $U(x) \vee x = 0$

Use of sheaf models/topos theory

So far, we have seen two uses: to show underivability and to force existence of ideal objects

Another use, suggested early on in the 70s, is to look at an intuitionistic statement and at its interpretation in a sheaf model/topos

Use of sheaf models/topos theory

We *may* get in this way an interesting statement, with an intuitionistic proof

This uses the fact that intuitionistic logic is *sound* in topos (and this was a surprising fact, since intuitionism was very far from the mind of algebraic geometers who studied sheaf models!)

In his 2017 PhD thesis, Ingo Blechschmidt has a nice example of this technique

Use of sheaf models/topos theory

The statement may look a little artificial

Let us consider a ring R satisfying $\neg U(x) \rightarrow x = 0$

Proposition: *If M is a finitely generated R-module then M is not not free*

The proof proceeds by induction on the number n of generators on M

If $n = 0$ then M is free

If the proposition holds for $m < n$ and we have generators $a_1, \dots, a_n$ we show that this family is free if M is not free!

Use of sheaf models/topos theory

Assume M not free

Indeed if we have $\Sigma_i a_i b_i = 0$ then we cannot have $U(b_1)$, otherwise a_1 can be expressed in term of $a_2, \dots, a_n$ and M is generated by $n-1$ elements and hence is not not free by induction hypothesis, contradiction!

So we have $\neg U(b_1)$ but then, by assumption on R, we have $b_1 = 0$

Similarly, we show $b_2 = \cdots = b_n = 0$

Hence $a_1, \dots, a_n$ is free and M is free; contradiction!

So M is not not free

Use of sheaf models/topos theory

What we obtain is the elegant generalization of Grothendieck's generic freeness Lemma (without Noetherianity hypotheses)

Theorem: *If* M *is finitely generated module over* k *and* $M[1/a]$ *free over* $R[1/a]$ *implies* $a = 0$ *then* $k = 0$

Use of sheaf models/topos theory

Classically this is equivalent to

Theorem: (classical) *If* $k \neq 0$ *and* M *is finitely generated module over* k *there exists* $a \neq 0$ *in* k *such that* $M[1/a]$ *is free over* $R[1/a]$

Compare with EGA IV 2, Lemma 6.9.2, where k is supposed to be integral domain *and* Noetherian

Martin Brandenburg has a nice application of this result to a characterisation of functors on finitely generated S-module, for R-algebra S, that commute with base changes

Big Zariski topos

Use a *site* instead of a topological space

Base category: finitely presented k-algebra $A = k[x_1, \dots, x_n]/(p_1, \dots, p_m)$

$A \Vdash u = v$ if $u = v$ in A

$A \Vdash \psi_0 \rightarrow \psi_1$ if $f : A \rightarrow B$ and $B \Vdash \psi_0 f$ implies $B \Vdash \psi_1 f$

$A \Vdash \psi_0 \wedge \psi_1$ if $A \Vdash \psi_0$ and $A \Vdash \psi_1$

$A \Vdash \psi_0 \vee \psi_1$ if we can find $1 = (b_1, \dots, b_n)$ and $A[1/b_i] \Vdash \psi_0$ or $A[1/b_i] \Vdash \psi_1$

(We don't write explicitely the canonical maps $A \rightarrow A[1/b_i]$)

Big Zariski topos

$A \Vdash \forall_x \psi$ if $f : A \rightarrow B$ and v in B implies $B \Vdash \psi f(v/x)$

$A \Vdash \exists_x \psi$ if we can find $1 = (b_1, \dots, b_n)$ and v_i in $A[1/b_i]$ with $A[1/b_i] \Vdash \psi(v_i/x)$

Note that we don't ask the v_i to be compatible

$A \Vdash \perp$ iff $1 = 0$ in A

Use of sheaf models/topos theory

The generic ring R is the presheaf represented by $k[X]$

Theorem: R *is a sheaf for the Zariski topology*

We have now a *site* with covering $A \to A[1/b_1], \dots, A \to A[1/b_n]$ for $1 = (b_1, \dots, b_n)$

Theorem: R *is a local ring*

We have $A \Vdash U(a) \vee U(1-a)$ for any a in A since $A \to A[1/a], A \to A[1/1-a]$ covering

Use of sheaf models/topos theory

In the Zariski topos, the generic ring R satisfies

$\neg(x = 0) \rightarrow U(x)$

Indeed if we have $A \Vdash \neg(x = 0)$ then $A/(x) \Vdash \perp$ since $A/(x) \Vdash x = 0$ and so $1 = 0$ in $A/(x)$ and x is a unit!

Model of spaces

In the 70s there was a very active development of topos theory

Topos Theoretic Methods in Geometry

Collection of articles edited by A. Kock, 1979

Summary in *Synthetic Reasoning and Variable Sets* Gonzalo E. Reyes

Model of spaces

"In three lectures at the University of Chicago in 1967, published in A. Kock (Ed. 1979), F. W. Lawvere proposed to use the theory of variable sets (= topos theory), developed by the Grothendieck school of Algebraic Geometry, as a foundation for synthetic reasoning. This program was part of a vast research program whose aim was to provide a direct, intrinsic axiomatization of Continuum Mechanics as developed by Walter Noll and others."

Model of spaces

From the point of view of variable sets, to give a continuum R is to give a category E of ”abstract” spaces and ”abstract” maps, *containing R as an object*, together with a subcategory Z of ”concrete” spaces (and ”concrete” maps) subject to some relations best described as follows: we view an object F of E as a ”variable set” whose elements are maps C→E (where C ranges over objects of Z). Given a ”concrete” map C'→C and an element of E at stage C (i.e., a map with domain C) we obtain, by composition in E, a new element of E at stage C'. In other words, E is identified with a (contravariant) set-valued functor on Z. In a similar vein, we view a morphism F→G as a map of ”variable sets”, which sends elements of F at stage C into elements of G at the same stage (via composition in E). This association being natural, is thus identified with a natural transformation between the functors F and G

Model of spaces

These identifications amount to giving a functor from E into the category of (contravariant) set-valued functors and natural transformations on Z, which we shall assume to be full and faithful, thus identifying the ”abstract” maps of spaces with the corresponding natural transformation

Model of spaces

Two examples:

-Zariski topos: we work with finitely presented k-algebra, where k is an *arbitrary ring*

-Model of Choice Sequences: another presentation of the model studied by Chuangje Xu and Martin Escardo *A Constructive Model of Uniform Continuity*

Big Zariski topos

k arbitrary ring

Site of finitely presented k-algebra $A, B, \ldots$

The covering are $A \to A[1/u_1], \ldots, A \to A[1/u_n]$ if $(u_1, \ldots, u_n) = 1$ in A

We have the generic ring R where $R(A)$ is the set underlying A

R is represented by $k[X]$ so we are in the situation described by G. Reyes

Big Zariski topos

Theorem: R *is a local ring*

Indeed A is always covered by $A[1/u]$ and $A[1/1-u]$ for any u in A

So we have $A \Vdash \forall_x U(x) \vee U(1-x)$ for any A

Big Zariski topos

Furthermore, there is a *completness theorem* for the first-order theory of local k-algebra

Theorem: *A coherent formula is provable in this theory iff it holds in the Zariski topos*

Big Zariski topos

A. Kock 1974 discovered that R satisfies (non coherent!) formulae that are not intuitionistically provable

Proposition: *R satisfies $\neg(x=0)\rightarrow U(x)$ and more generally*

$\neg(x_1=\cdots=x_n=0)\rightarrow U(x_1)\vee\cdots\vee U(x_n)$

Big Zariski topos

Ingo Blechschmidt PhD thesis 2017 presents the following generalisation

Let A be any finitely presented R-algebra (internally!), define $Sp(A)$ to be $Hom(A,R)$

Theorem: (Duality Principle) *The canonical map*

$A \rightarrow R^{Sp(A)}$

is an isomorphism

Big Zariski topos

$Sp(R/(r))$ is the proposition $r = 0$

$Sp(R[1/r])$ is the proposition $U(r)$

$Sp(R[X])$ is R

Any map $Sp(A) \to Sp(B)$ corresponds to a morphism $Hom(B, A)$ of R-algebra

In particular any map $R \to R$ is a polynomial, since $Hom(R[X], R[X])$ is $R[X]$ as a set

Model of choice sequences

We work with the site of Boolean algebra with covering $B[1/e_i]$ for $e_1, \dots, e_n$ partition of unity (Boolean version of the "gros" Zariski topos)

Internally consider the Boolean algebra B of propositional logic (free Boolean algebra on countably many generators) then we have $Sp(B) = Hom(B, 2) = 2^{\mathbb{N}}$

Theorem: (Duality Principle) *The canonical map*

$$B \to 2^{Sp(B)}$$

is an isomorphism

Model of choice sequences

We get a model of Brouwer's *fan theorem*: any function $2^{\mathbb{N}} \to 2$ is uniformly continuous

Note that this is not valid if we consider only recursive points of Cantor space

This is similar to Kreisel and Troelstra model of choice sequences

Sheaf models

Sheaves form a model of *simple type theory* but the language of simple type theory is not enough to describe mathematical structures

Martin-Löf's original motivation 1971 for extending simple type theory with a universe

The simple theory of finite types, although proof theoretically quite strong, has some unnatural limitations (for example, it permits only finite iterations of the power operation) and, above all, it is not adequate for a formalization of mathematics that talk about arbitrary sets and not just sets of natural numbers, sets of sets of natural numbers, and so on.

Sheaf models

Ingo Blechschmidt in his PhD thesis uses Mike Shulman so-called “stack” semantics to be able to quantify over arbitrary sets, but this is not enough to form collection of structures

Presheaf models of type theory

For *presheaves* there is no problem

Martin Hofmann *Syntax and Semantics of Type Theory*

See also *What is a model of type theory*, Th. C.

Presheaf models of type theory

In this setting, we represent forcing as follows

We have a family of proposition p_i

Let $E(p)$ be $\{0 \mid p\}$

A type X is a *sheaf* iff each diagonal map $X \to X^{E(p_i)}$ is a bijection

Intuitively X believes that p_i is true

It is direct that such types are closed by dependent products and sums

Sheaf models

In the lecture I will go quickly over the next example of Newton-Puiseux series

This is from the joint work with Bassel Mannaa
A Sheaf Model of the Algebraic Closure

and his PhD thesis *Sheaf Semantics in Constructive Algebra and Type Theory*

Sheaf models

What I will present now is inspired from two papers

“La logique des topos” A. Boileau and A. Joyal, JSL 1980

“Les théorèmes de Chevalley-Tarski et remarques sur l’algèbre constructive” A. Joyal, CTGD,58, 1

But the arguments may be different from the ones of A. Joyal

Roughly speaking: Joyal proves also quantifier elimination, while I prove only consistency

Sheaf models

Any map $R \to S$ gives a map $B(R) \to B(S)$

Theorem: *The map* $B(\iota) : B(R) \to B(R[X])$ *has a left adjoint*

This is Chevalley's theorem: the projection of a constructible set is constructible

This corresponds to quantifier elimination $\exists : B(R[X]) \to B(R)$ We have $\exists(\psi(X)) \leqslant \varphi$ iff $\psi(X) \leqslant B(\iota)(\varphi)$

The argument is not developped in Joyal's papers, but there are now notes from Luis Español González, which describes the argument: e.g. reduces the general case of the Theorem to the case where R is a field

Algebraic closure

Instead of “forcing” the existence of a point of a space, a mathematical *object* (like a prime ideal), we are going to “force” the existence of mathematical *structure*

We work on a sheaf model over a *site* and not over a topological space

“Gros” topos vs “petit” topos

Algebraic closure

We want to build the algebraic closure of a given perfect field k

Problem: we cannot decide irreducibility of polynomials

How can we add a root of $X^2 + 1$ for instance?

$A = k[X]/\langle X^2 + 1\rangle$ may not be a field

However it is reduced 0-dimensional, and $Z(A) = B(A)$ is a Boolean algebra

If α prime (=maximal) ideal of A then A/α is a field extension of k

Abel versus Galois

Splitting field of $P = X^3 - a_1X^2 + a_2X - a_3$

Analysis of Galois' work in "Essays in constructive mathematics", H. Edwards

We consider $A = k[X_1, X_2, X_3]/I$ where I is the ideal

$\langle X_1 + X_2 + X_3 - a_1,\ X_1X_2 + X_2X_3 + X_3X_1 - a_2,\ X_1X_2X_3 - a_3\rangle$

For any k one can show (effectively) that I is *proper*

We know A is non trivial and anly α prime ideal of A determines a splitting field A/α of P

Algebraic closure

We take the site of all étale finitely presented k-algebras

Such an algebra can be presented as a triangular algebra $k[a_1,\dots,a_n]$

a_{i+1} root of $p(X,a_1,\dots,a_i)=0$ with p separable in $k[a_1,\dots,a_i][X]$

Covering: A is covered by $A[1/e_1],\dots,A[1/e_n]$ where $e_1,\dots,e_n$ idempotents pairwise incompatible with $1=e_1+\dots+e_n$

A is covered by $A[X]/\langle p\rangle$ where p is separable

An arbitrary covering is obtained by iterating elementary coverings (in all these cases, we obtain only finite coverings)

We "force" $x=0\vee U(x)$ and $\exists x\ p(x)=0$

Algebraically closed fields

Any such algebra A represents a state of knowledge about the (ideal) algebraic closure: we have a finite number of indeterminates $X_1, \dots, X_n$ and a finite number of conditions $P_1 = \cdots = P_m = 0$

Algebraic closure

Over this site, we have a presheaf $K(A)$ set underlying A

In this sheaf model, K is the algebraic closure of k!

We build an algebraic closure, not in the category of sets, but in a sheaf model

Refinement of the model

If we are at the node $A = k[x]/\langle x^2 - 3x + 2\rangle$ and we want to force $a = 0 \vee U(a)$ for $a = x - 3$ with k of characteristic 0

We can directly see that a is invertible in A by computing the GCD of $x^2 - 3x + 2$ and $x - 3$

$$x^2 - 3x + 2 = x(x - 3) + 2$$

so that the inverse of a is $-x/2$

Note that we do the computation both for $x = 1$ and $x = 2$ in parallel!

Refinement of the model

Similarly for $a = x - 1$ we find

$$x^2 - 3x + 2 = (x-1)(x-2)$$

so that one branch is $A \to k[x]/\langle x-1\rangle$ where $a = x - 1$ is 0 and the other branch is $A \to k[x]/\langle x-2\rangle$ where $a = x - 1$ is invertible (and is equal to 1)

$$A[a^{-1}] = \quad k[x]/\langle x-2\rangle \qquad\qquad A/\langle a\rangle = \quad k[x]/\langle x-1\rangle$$

Refinement of the model

For instance if $A = k[x,y]/\langle x^2-2, y^2-2\rangle$ and we want to force

$$a = 0 \vee U(a)$$

for $a = y - x$ we get the covering

$$A_0 = k[x,y]/\langle x^2-2, y-x\rangle \qquad A_1 = k[x,y]/\langle x^2-2, y+x\rangle$$

Refinement of the model

This gives a *computational model* of the algebraic closure of a field, for which we don't use a factorisation algorithm for polynomials over k, only GCD computations

This might be interesting even if we have a factorization algorithm for polynomials over k

One can think of each such finitely presented k-algebra as a *finite approximation* of the (ideal) algebraic closure of k

Dynamical evaluation

We get something close to the technique of *dynamical evaluation* in computer algebra (D. Duval; one application: computation of branches of an algebraic curves)

The notion of site model gives a theoretical model of dynamical evaluation

The same technique can be used for several other first-order theories

M. Coste, H. Lombardi and M.F. Roy, *Dynamical method in algebra*, Ann. Pure Appl. Logic 111 (2001), 203-256

We think this is close to what Herbrand had in mind when he mentions that he could show the consistency of the theory of real closed fields without having to prove quantifier eliminations

Dynamical evaluation

We can for instance look at Abhyankar's proof of Newton-Puiseux Theorem in *Algebraic geometry for Scientists and Engineers*

Theorem: *If $P(x,Y)=0$ is a* separable *polynomial in Y in $k[x,Y]$ of degree n then there exists $m \geqslant 1$ and $\eta_1,\dots,\eta_n$ in $K[[x]]$ such that $P(T^m,Y)=\Pi(Y-\eta_i)$*

In this statement K is the separable closure of k

This makes sense in the sheaf model we have described

We get an algorithm which given P computes a *finite* extension of k where such a decomposition can be found

Dynamical evaluation

$P(x,Y) = Y^6 + 3x^2Y^4 + (3x^4 - 4x^2)Y^2 + x^6$ and $k = \mathbb{Q}$

$k[a,b,c,d,e]$ where $m = 2$ and

$$\begin{aligned}
a^4 - 2 &= 0\\
b - a/5 &= 0\\
c^2 - 1/4 &= 0\\
d^3 + 2/3a^2d + 20/27a^3 &= 0\\
e^2 + 3/4d^2 + 2/3a^2 &= 0
\end{aligned}$$

Dynamical evaluation

$P(x,Y) = Y^6 + 3x^2Y^4 + (3x^4 - 4x^2)Y^2 + x^6$ and $k = \mathbb{Q}$

$$P(x,Y) = (Y - ax^{1/2} + 3/16a^3x^{3/2} + \dots)(Y - cx^2 + \dots)$$
$$(Y + cx^2 + \dots)(Y + (-e + d/2 + a/3)x^{1/2} + \dots)(Y + (e + d/2 + 1/3)x^{1/2} + \dots)$$

$$\begin{aligned}
a^4 - 2 &= 0\\
b - a/5 &= 0\\
c^2 - 1/4 &= 0\\
d^3 + 2/3a^2d + 20/27a^3 &= 0\\
e^2 + 3/4d^2 + 2/3a^2 &= 0
\end{aligned}$$

Dynamical evaluation

Note that $K[[x]]$ is $K^{\mathbb{N}}$ and hence, we know *a priori* that a finite extension of k will be enough to compute *all* coefficients of the rational power serie

This is not obvious a priori if we follow usual methods, e.g. the one presented in Edwards *Essays in constructive mathematics*: it may be that we have to introduce infinitely new algebraic numbers

Exercise

Show that in this model, there is no function $r : K \to K$ such that

$$\forall_{a:K} r(a)^2 = a$$