Algebraically Closed Fields

Thierry Coquand

May 2018

Constructive Algebra

Constructive algebra is algebra done in the context of intuitionistic logic

Algebraic closure

In the previous lecture, we have seen how to "force" the existence of prime ideals, even in a weak framework where we don't have choice axiom

A prime filter always exists in the Zariski topos

Instead of "forcing" the existence of a point of a space (a mathematical object), we are going to "force" the existence of a model (a mathematical structure)

Forcing/Beth models/Kripke models

1956 Beth models

1958 Kripke models

1962 Cohen forcing

1964 sheaf models, site models, topos

1966 Boolean valued models

Algebraic closure

The first step to build a closure of a field k is to show that we can build a splitting field of any polynomial P in $k[X]$. We have to build an extension of k where P decomposes in linear factor.

However in the theory of discrete fields we cannot prove

$$\exists x \ (x^2 + 1 = 0) \vee \forall x \ (x^2 + 1 \neq 0)$$

Irreducibe polynomial

Indeed, this is not valid in the following Kripke model over $0 \leqslant 1$

At level 0 we take $k = \mathbb{Q}$

At level 1 we take $k = \mathbb{Q}[i]$

Essentially the same argument can be found in

van der Waerden (1930) *Eine Bemerkung über die Unzerlegbarkeit von Polynomen*

(before recursive functions theory was developped!)

Algebraically closed fields

Language of ring. Theory of ring, equational

Field axioms $1 \neq 0$ and

$x = 0 \vee \exists y.\ 1 = xy$

Algebraically closed $\exists x.\ x^n + a_1 x^{n-1} + \cdots + a_n = 0$

For an extension of k we add the diagram of k

$a \neq b$ stands for $\neg(a = b)$ and $\neg\varphi$ stands for $\varphi \rightarrow \bot$

Algebraically closed fields

Let k be a field of characteristic 0

We show effectively the consistency of this theory by defining a forcing relation

$R \Vdash \varphi$

where R is a finitely presented k-algebra

Thus R is of the form $k[X_1, \ldots, X_n]/\langle P_1, \ldots, P_m \rangle$

This forcing relation will be sound: $\vdash \varphi$ implies $R \Vdash \varphi$

We shall have $R \Vdash 1 = 0$ iff $1 = 0$ in R

Algebraically closed fields

R represents a state of knowledge about the (ideal) model: we have a finite number of indeterminates $X_1, \ldots, X_n$ and a finite number of conditions $P_1 = \cdots = P_m = 0$

Refinement of the model

If we are at the node $R = k[x]/\langle x^2-3x+2\rangle$ and we want to force $a = 0 \vee \mathsf{inv}(a)$ for $a = x - 3$

We can directly see that a is invertible in R 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 $-x/2$

Refinement of the model

Similarly for $a = x - 1$ we find

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

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

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

Refinement of the model

Finally in characteristic 0 (or over a perfect field) we can assume that we restrict the addition of roots to separable polynomials, by GCD computations

In this way, the nodes are all given by a finite number of indeterminates $x_1, \ldots, x_n$ and polynomial constraints

$$p_1(x_1) = 0, \ p_2(x_1, x_2) = 0, \ \ldots, \ p_n(x_1, \ldots, x_n) = 0$$

and the algebra $R = k[x_1, \ldots, x_n]/\langle p_1, \ldots, p_n \rangle$ is vN regular

Site model

All the nodes R will be *reduced* (no nilpotent elements) and 0-dimensional: $Z(R)$ is a *Boolean* algebra

Site model

Elementary covering

If $1 = e_1 + \cdots + e_n$ with $e_i^2 = e_i$ and $e_i e_j = 0$ for $i \neq j$ then $R \to R[1/e_i] = R/\langle 1 - e_i \rangle$ is a covering

algebraically closed fields: we add $R \to R[X]/\langle p \rangle$ where p is a monic non constant separable polynomial

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

Site model

The presheaf $R \longmapsto R$ is a *sheaf*

In the case of the covering $R \to R[x]/\langle p \rangle$ we have to show that if $u(x) = u(y)$ in $R[x,y]/\langle p(x), p(y) \rangle$ then $u(x) = u(y)$ is a constant in R

This sheaf is a discrete field, which is the generic algebraic closure of k

Site model

One defines a forcing relation $R \Vdash \varphi$ by induction on φ

$R \Vdash \varphi(a_1, \ldots, a_n) \rightarrow \psi(a_1, \ldots, a_n)$ iff $S \Vdash \varphi(f(a_1), \ldots, f(a_n))$ implies $S \Vdash \psi(f(a_1), \ldots, f(a_n))$ for any map $f : R \rightarrow S$

$R \Vdash \forall x.\varphi(a_1, \ldots, a_n, x)$ iff for any map $R \rightarrow S$ and any element b in S we have $S \Vdash \varphi(f(a_1), \ldots, f(a_n), b)$

$R \Vdash \varphi_0 \wedge \varphi_1$ iff we have $R \Vdash \varphi_0$ and $R \Vdash \varphi_1$

Site model

$R \Vdash \exists x.\varphi(a_1, \ldots, a_n, x)$ iff we have a covering $f_i : R \to R_i$ and elements b_i in R_i such that $R_i \Vdash \varphi(f_i(a_1), \ldots, f_i(a_n), b_i)$

$R \Vdash \varphi_0(a_1, \ldots, a_n) \vee \varphi_1(a_1, \ldots, a_n)$ iff we have a covering $f_i : R \to R_i$ and $R_i \Vdash \varphi_0(f_i(a_1), \ldots, f_i(a_n))$ or $R_i \Vdash \varphi_1(f_i(a_1), \ldots, f_i(a_n))$ for all i

Site model

$R \Vdash t(a_1, \ldots, a_n) = u(a_1, \ldots, a_n)$ iff we have a covering $f_i : R \to R_i$ and $t(f_i(a_1), \ldots, f_i(a_n)) = u(f_i(a_1), \ldots, f_i(a_n))$ in each R_i

$R \Vdash \perp$ iff we have a covering $f_i : R \to R_i$ and $1 = 0$ in each R_i

Site model

In this way, we "force"

$R \Vdash a = 0 \vee \mathsf{inv}(a)$ theory of fields, where $\mathsf{inv}(a)$ is $\exists x.ax = 1$

$R \Vdash \exists x.x^n + a_1 x^{n-1} + \cdots + a_n = 0$ theory of algebraically closed fields

Soundness Theorem

Theorem: *If we have $\varphi_1, \ldots, \varphi_n \vdash \varphi$ in intuitionistic natural deduction and if $R \Vdash \varphi_1, \ldots, R \Vdash \varphi_n$ then we have $R \Vdash \varphi$*

This is proved by induction on the proof of $\varphi_1, \ldots, \varphi_n \vdash \varphi$

Similar to the proof of soundness for Kripke/Beth models

Hence if we have $\vdash 1 = 0$ we have $R \Vdash 1 = 0$ for all finitely presented k-algebra R

Soundness Theorem

Lemma: *If $R \to S$ and we have a covering $f_i : R \to R_i$ then we can find a corresponding covering $g_i : S \to S_i$ with commuting maps $h_i : R_i \to S_i$*

Lemma: *If $R \Vdash \varphi(a_1, \ldots, a_n)$ and $f : R \to S$ then $S \Vdash \varphi(f(a_1), \ldots, f(a_n))$*

Site model

We can see this forcing relation as defining one model, similar to Beth/Kripke model

This model (the "generic" model, similar to the initial model for equational theories) can be described in a weak metatheory (no axiom of choice)

This gives an *effective consistency* proof for the theory of algebraically closed fields

Indeed $R \Vdash 1 = 0$ iff $1 = 0$ in R

This builds a *generic* model, where the truth-values are non standard

Completeness Theorem

We say that a formula φ is positive iff it does not contain $\forall$, $\rightarrow$

$$\varphi \ ::= \ \perp \mid t = u \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists x.\varphi$$

For a positive formula, a proof of $R \Vdash \varphi$ has a simple tree structure building a covering of R

We can see this as a cut-free proof of φ

Completeness Theorem

Two approaches for completeness

(1) Henkin-Lindenbaum

(2) Löwenheim-Skolem-Herbrand-Gödel, gives completeness of *cut-free* proofs

Completeness Theorem

For positive formulae, to be true in a site model means to have a cut-free proof (well-founded tree)

Indeed, a proof theory with exactly this notion of proof tree is described in the paper

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

The semantics is sound w.r.t. intuitionistic derivation, and the proof of soundness is similar to a proof of admissibility of the cut rule

Refinement of the model

The two covering relations are

-$R \to R_0 = R/\langle e \rangle$ and $R \to R_1 = R/\langle 1 - e \rangle$, so that $R = R_0 \times R_1$

-$R \to R[X]/\langle p \rangle$ where p is separable

Refinement of the model

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

$$a = 0 \vee \mathsf{inv}(a)$$

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

$$R_0 = k[x, y]/\langle x^2 - 2, y - x \rangle \qquad R_1 = k[x, y]/\langle x^2 - 2, y + x \rangle$$

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 computation

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 in this way what is known as *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

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* $\eta_1, \ldots, \eta_n$ *in* $K[[X]]$ *such that* $P(T^m, Y) = \Pi(Y - \eta_i)$

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

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

Site model

This is reminiscent of the description of Kronecker's work by H. Edwards

The necessity of using an algebraically closed ground field introduced -and has perpetuated for 110 years- a fundamentally transcendental *construction at the foundation of the theory of* algebraic curves. *Kronecker's approach, which calls for adjoining new constants algebraically as they are needed, is much more consonant with the nature of the subject*

H. Edwards *Mathematical Ideas, Ideals, and Ideology*, Math. Intelligencer 14 (1992), no. 2, 6–19.

Cf. T. Mora *Solving Polynomial Equation Systems I, The Kronecker-Duval Philosophy*

Other theories

Theory of *local* rings

$$\mathsf{inv}(x) \vee \mathsf{inv}(1 - x)$$

where $\mathsf{inv}(u)$ means $\exists y.\ 1 = yu$

The elementary covering are now $R \to R[x^{-1}]$ and $R \to R[(1 - x)^{-1}]$

Lemma: *We have $R \Vdash inv(x)$ iff x is invertible in R*

Lemma: *We have $R \Vdash J(x)$ iff x is nilpotent in R*

Corollary: *We don't have $\vdash inv(x) \vee J(x)$ in the (intuitionistic) theory of local rings*