Constructive semantics for nonconstructive principles

Oberseminar Mathematische Logik. Munich

16th June 2010

H. Lombardi, Besançon

henri.lombardi@univ-fcomte.fr, http://hlombardi.free.fr

if you want to print these slides:

http://hlombardi.free.fr/publis/Munich2010Doc.pdf

Introduction

Deciphering a computational content for idealistic objects and non-constructive principles in classical mathematics can be understood as the search for constructive semantics hidden in abstract recipes.

We will try to compare by examples such possible constructive semantics.

Example 1: prime ideals in (classical) commutative algebra

Let $\mathbf{A}$ be a commutative ring, $\mathfrak{a}$ an ideal, S a MCS (multiplicatively closed subset) and assume that $\mathfrak{a} \cap S = \emptyset$.

Krull Theorem. *There exists a field* $\mathbf{K}$ *and a ring homorphism* $\varphi : \mathbf{A} \to \mathbf{K}$ *such that* $\varphi(\mathfrak{a}) = 0$ *and* $\varphi(S) \subseteq \mathbf{K}^\times$

The kernel $\mathfrak{p}$ of φ is called a prime ideal of $\mathbf{A}$.

The quotient ring $\mathbf{A}/\mathfrak{p}$ is an integral domain $\mathbf{B}$ and one can take $\mathbf{K} = \mathrm{Frac}(\mathbf{B})$.

The set $S_\mathfrak{p} = \mathbf{A} \setminus \mathfrak{p}$ is a MCS and the localised ring $\mathbf{C} = S_\mathfrak{p}^{-1}\mathbf{A}$ is a local ring. One can take for $\mathbf{K}$ the residue field of $\mathbf{C}$ (which is isomorphic to $\mathrm{Frac}(\mathbf{B})$).

Example 1: prime ideals in (classical) commutative algebra (2)

Krull Theorem, refinement.
The intersection of all possible $\mathfrak{p}$ *in Krull Theorem is equal to*

$$Sat(\mathfrak{a}, S) = \{\, x \in \mathbf{A} \mid \exists s \in S \text{ and } n \in \mathbb{N} \text{ such that } sx^n \in \mathfrak{a} \,\}$$

We have also a concrete description for the intersection of all $S_{\mathfrak{p}}$*'s*

Using Krull Theorem in classical mathematics.

1. In order to prove that $\mathfrak{a} \cap S$ is inhabited, show that the conclusion of Krull Theorem is absurd.

2. In order to prove that some x is in $Sat(\mathfrak{a}, S)$ show that for every ring homomorphism φ from $\mathbf{A}$ to any field $\mathbf{K}$, one has $\varphi(x) = 0$

3. . . . (local global principles)

Example 1: prime ideals in (classical) commutative algebra (3)

Constructive semantics via first order logic

Consider the first order theory built from the hypotheses of Krull theorem.

I.e., the theory $T_{fields}(\mathbf{A}, \mathfrak{a}, S)$ of fields, adding as constants all elements $a \in \mathbf{A}$, and as axioms

- the positive diagram of $\mathbf{A}$
- $a = 0$ for $a \in \mathfrak{a}$
- s is invertible for $s \in S$

Using Krull Theorem and classical mathematics when analysing first order logic you know that the following concrete result is true:

if $T_{fields}(\mathbf{A}, \mathfrak{a}, S)$ is inconsistent, then $\mathfrak{a} \cap S$ is inhabited

Example 1: prime ideals in (classical) commutative algebra (4)

Constructive semantics via first order logic (2)

Examining in a detailed way the classical proofs (they use TEM, Choice and Gödel's completeness theorem, which have no constructive interpretation, but also some concrete computations) involved in this result, you see that the concrete result can be obtained in a direct way by considering the computations appearing in the classical proof.

So Krull Theorem appears as an "abus de pouvoir" allowing classical mathematicians to deduce abstract existence theorems via only one nonconstructive principle: Gödel's completeness theorem (much weaker than TEM)

Example 1: prime ideals in (classical) commutative algebra (5)

Constructive semantics via first order logic (3)

Krull refinement Theorem has the following constructive content: form a proof of $x = 0$ for an $x \in \mathbf{A}$ in the formal theory $T_{fields}(\mathbf{A}, \mathfrak{a}, S)$, on can find an $s \in S$ and an $n \in \mathbb{N}$ such that $sx^n \in \mathfrak{a}$.

Here again the abstract Krull refinement Theorem is nothing but a translation of the concrete result through an "abus de pouvoir" using Gödel's completeness theorem.

Example 1: prime ideals in (classical) commutative algebra (6)

Constructive semantics via dynamical algebraic structures

It is convenient, in order to be understood more widely, to reconsider the previous constructive semantics in a language more directly accessible to all mathematicians.

This is rather easy any time you can see the first order theory you consider as a geometric theory.

Then it is known that all proofs of sufficiently elementary results can be managed without logic in a purely computational way.

Dynamical semantics

It is often possible to understand "too abstract objects in classical mathematics" (too abstract means that TEM and Choice are too much used) as "nonstatic constructive objects, dynamical ones"

Let us see on the blackboard how this works when deciphering classical local-global principles.

Zariski spectrum and dynamical semantics

The 3 natural topology of $\mathrm{Spec}(\mathbf{A})$ correspond to 3 dynamical semantics (and three first order theories)

Considering the ring as a dynamical local ring.

Considering the ring as a dynamical integral ring.

Considering the ring as a dynamical field.

Example 2: the splitting field of a separable polynomial

Let $\mathbf{K}$ be a field and $f \in \mathbf{K}[T]$ a *separable polynomial* of degree n (this means that $\exists u, v \in \mathbf{K}[T]$, $uf + v\frac{\partial f}{\partial T} = 1$).

Theorem.

1. There exists a splitting field for f, i.e., an over field $\mathbf{L} \supseteq \mathbf{K}$ and $x_1, \ldots, x_n \in \mathbf{L}$ such that $x_i - x_j \in \mathbf{L}^\times$ if $i \neq j$ and
   (a) in $\mathbf{L}[T]$ we have $f(T) = \prod_{i=1}^{n}(T - x_i)$
   (b) $\mathbf{L} = \mathbf{K}[x_1, \ldots, x_n]$, i.e., any element of $\mathbf{L}$ can be written as $Q(x_1, \ldots, x_n)$ for some $Q \in \mathbf{K}[X_1, \ldots, X_n]$. Moreover $\mathbf{L}$ is a finite dimensional $\mathbf{K}$-vector space (the notation for the dimension is $[\mathbf{L} : \mathbf{K}]$)

2. If $\mathbf{L}'$ is another splitting field for f over $\mathbf{K}$, there exists an isomorphism $\varphi : \mathbf{L} \to \mathbf{L}'$ as $\mathbf{K}$-algebras.

Example 2: the splitting field of a separable polynomial (2)

The proof in classical mathematics.

- Let g_1 be an irreducible factor of f, consider

$$\mathbf{K}_1 = \mathbf{K}[x_1] = \mathbf{K}[X_1]/\langle g_1(X_1)\rangle$$

We have $[\mathbf{K}_1 : \mathbf{K}] = \mathsf{deg}(g_1)$.

- Let $f_1(T) = f(T)/(T - x_1) \in \mathbf{K}_1[T]$. Let g_2 be an irreducible factor of f_1, consider

$$\mathbf{K}_2 = \mathbf{K}_1[x_2] = \mathbf{K}[X_1, X_2]/\langle g_1(X_1), h_2(X_1, X_2)\rangle$$

where $h_2(x_1, X_2) = g_2(X_2)$. We have $[\mathbf{K}_2 : \mathbf{K}] = \mathsf{deg}(g_1)\,\mathsf{deg}(g_2)$.

- And so on ...

Example 2: the splitting field of a separable polynomial (3)

Semantics à la Richman.

There is a possible description of classical mathematics as

"constructive mathematics when allowing TEM (and often Choice)" (see Fred Richman).

Analysing the use of TEM in the above classical proof leads to the constructive notion of "separably factorial discrete fields".

Discrete fields: fields with a zero test. They satisfy the axiom "every element is zero or invertible".

Separably factorial fields: fields where separable polynomials do have a factorisation in product of irreducible factors.

Example 2: the splitting field of a separable polynomial (4)

Semantics à la Richman (2).

With these extra hypotheses, the classical theory becomes constructive, but we need a fine constructive theorem:

Theorem. If $\mathbf{K}$ is a separably factorial discrete field, then so is any extension $\mathbf{K}[X]/\langle g(X)\rangle$ where g is separable and irreducible.

Note that this theorem is trivially true in classical mathematics since all fields are discrete and separably factorial when using TEM.

So we have found and shown hidden TEM hypotheses and an hidden fine theorem corresponding to the classical proof.

Example 2: the splitting field of a separable polynomial (5)

Semantics via Model Theory.

Existence of the splitting field

Uniqueness of the splitting field

Example 2: the splitting field of a separable polynomial (6)

An intriguing example

What about the splitting field of $T^2 - a$, $a \neq 0$ (in characteristic $\neq 2$)

The splitting field as dynamical algebraic structure

You start with a discrete field. It is possible to compute in a secure way inside the splitting field of f if you accept that it is not a usual static object, but a dynamical one.

At the beginning your field is represented by the splitting algebra of f.

Moreover you have a candidate for the Galois group, that is S_n.

Any time you find an element contradicting the axiom of fields, you are able to immediately, improve your knowledge of the splitting field, in considering a good quotient of your previous "splitting field".

This works for all theorems of the so called Galois theory of f

Example 3: Classical Galois Theory

1. (Galois group) Let us denote $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ the group of $\mathbf{K}$-automorphisms of $\mathbf{L}$ (such an automorphism ψ is characterised by the permutation σ it induces over $x_1, \ldots, x_n$, so $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ can be viewed as a subgroup of S_n). Then $|\mathrm{Gal}(\mathbf{L}/\mathbf{K})| = [\mathbf{L} : \mathbf{K}]$

Galois correspondance

For a subgroup H of $G = \mathrm{Gal}(\mathbf{L}/\mathbf{K})$ let us denote $\mathrm{Fix}_{\mathbf{L}}(H)$, or $\mathbf{L}^H$ the sub-$\mathbf{K}$-algebra of $\mathbf{L}$ defined as

$$\mathbf{L}^H = \{\, y \in \mathbf{L} \,|\, \forall \psi \in H,\, \psi(y) = y \,\}$$

For a field $\mathbf{M}$ with $\mathbf{K} \subseteq \mathbf{M} \subseteq \mathbf{L}$ tel us denote $\mathrm{Stp}_G(\mathbf{M})$ the subgroup H of G defined as

$$H = \{\, \psi \in G \,|\, \forall y \in \mathbf{M},\, \psi(y) = y \,\}.$$

2. $\mathrm{Fix}_{\mathbf{L}}$ and Stp_G are decreasing one to one correspondances between

   $$\{\text{subgroups of } G\} \text{ and } \{\text{fields } \mathbf{M} \text{ s.t. } \mathbf{K} \subseteq \mathbf{M} \subseteq \mathbf{L}\}$$

   with $\mathrm{Stp} \circ \mathrm{Fix} = \mathrm{Id}_{\text{subgroups}}$ and $\mathrm{Fix} \circ \mathrm{Stp} = \mathrm{Id}_{\text{subfields}}$

Galois correspondance, continued

3. If $\mathbf{L}^H = \mathbf{M}$, then $\mathbf{L}$ is a splitting field for f over $\mathbf{M}$.
   Moreover $\mathrm{Gal}(\mathbf{L}/\mathbf{M}) = H$.

4. For $\psi \in G$, $\psi(\mathbf{L}^H) = \mathbf{L}^{\psi H \psi^{-1}}$.

5. $\mathbf{L}^H = \mathbf{M}$ is a splitting field for some polynomial $g \in \mathbf{K}[T]$ if and only if H is a normal subgroup of G.
   In this case $\mathrm{Gal}(\mathbf{M}/\mathbf{K}) \simeq G/H$.

6. In characteristic 0 the equation $f(x) = 0$ is solvable by extractions of m-th roots if and only if G is solvable.

Bases over $\mathbf{K}$

7. (resolvent) For $z \in \mathbf{L}$,

   – let $z_1, \ldots, z_r$ be the orbit $G.z$,

   – $H = \mathsf{Stab}_G(z) = \mathsf{Stp}_G(\mathbf{K}[z])$ (so $r \cdot |H| = |G|$)

   – and $R_z(T) = \prod_{i=1}^{r}(T - z_i)$.

   Then $R_z(T)$ is the minimal polynomial of z over $\mathbf{K}$.

   As a particular case $\mathsf{Stab}_G(z) = \{\mathrm{Id}\}$ if and only if $\mathbf{L} = \mathbf{K}[z]$ (primitive elements).

8. (normal basis) There exists a basis of $\mathbf{L}$ as $\mathbf{K}$-vector space made of $\psi(y)'s$ for some y in $\mathbf{L}$ and all $\psi \in \mathsf{Gal}(\mathbf{L}/\mathbf{K})$.

Dynamical semantics beyond first order logic

Maximal ideals.

Minimal prime ideals.

Thank you