Dynamical Method
in Constructive Algebra

Murcia, 7th june, 2013

Recent Trends in Rings and Algebras

H. Lombardi, Besançon

Henri.Lombardi@univ-fcomte.fr, http://hlombardi.free.fr

Proyecto MTM2011-22435

To print the slides:

http://hlombardi.free.fr/publis/MurciaDynamic2013Doc.pdf

Hilbert's program

Hilbert's program was an attempt to save Cantorian mathematics through the use of formalism.

From this point of view, too abstract objects (with no clear semantics) are replaced by their formal descriptions. Their hypothetical existence is replaced by the non-contradiction of their formal theory.

However, Hilbert's program in its original finitist form was ruined by the incompleteness theorems of Godel.

Henri Poincaré's program

As for me, I would propose that we be guided by the following rules:

1. Never consider any objects but those capable of being defined in a finite number of words;

2. Never lose sight of the fact that every proposition concerning infinity must be the translation, the precise statement of propositions concerning the finite;

3. Avoid nonpredicative classifications and definitions.

Henri Poincaré, in *La logique de l'infini* (Revue de Métaphysique et de Morale 1909). See also *Dernières pensées*, Flammarion.

Bishop’s Constructive Analysis

Poincaré’s program “Never lose sight of the fact that every proposition concerning infinity must be the translation, the precise statement of propositions concerning the finite” is even more ambitious than Hilbert’s program.

Bishop’s book (1967) **Foundations of Constructive Analysis** is a kind of realization of the Poincaré’s program.

But also a realization of Hilbert’s program, when one replaces finitist requirements by less stringent requirements, constructive ones.

Richman's Constructive Algebra

Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988)

This book does the same job for constructive algebra as Bishop's book did for constructive analysis.

Baby example, idempotent matrices

The theory of idempotent matrices is "samething" as the theory of finitely generated projective modules.

The first theorem about finitely generated projective modules in "Commutative Algebra" (Bourbaki), says that given an $\mathbf{A}$-module P which is finitely generated projective, there exist elements s_1, ..., s_n in $\mathbf{A}$ such that $\langle s_1, \ldots, s_n \rangle = \langle 1 \rangle$ and on each $\mathbf{A}[1/s_i]$, the module P becomes finite rank free.

How to find these s_i's from the idempotent matrix seems impossible to see when you read the proof (or the exercices) of Bourbaki.

New methods

Dynamical Constructive Algebra

The Computer Algebra **software D5** was invented in order to deal with the algebraic closure of an explicit field, even when the algebraic closure is impossible to construct.

This leads to the general idea to replace **too abstract objects (without actual existence)** of Cantorian mathematics by **finite approximations**: uncomplete specifications of these objects.

Abstract proofs about these abstract objects are to be reread as constructive proofs about their finite approximations.

The surprise is: **THIS WORKS!**, at least for constructivizing commutative algebra.

Finite free resolutions

The theory of finite free resolutions studies exact sequences of matrices:

$$\boxed{L_\bullet : \quad 0 \to L_m \xrightarrow{A_m} L_{m-1} \xrightarrow{A_{m-1}} \cdots\cdots \xrightarrow{A_2} L_1 \xrightarrow{A_1} L_0 \ .} \ (**)$$

where $L_k = \mathbf{A}^{p_k}$, $A_k \in \mathbb{M}_{p_{k-1},p_k}(\mathbf{A})$ and $\mathrm{Im}(A_k) = \mathrm{Ker}(A_{k-1})$ for $k = m, \ldots, 1$.

One searches to identify properties of matrices A_k and the structure of the $\mathbf{A}$-module

$$M = \mathrm{Coker}(A_1) = L_0/\mathrm{Im}(A_1)$$

for which the sequence $(**)$ is a finite free resolution.

Constructive finite free resolutions, 2

A very good book on the topic is Northcott [Finite Free Resolutions].

Nothcott insists many times on the concrete content of theorems.

But he has to rely on abstract proofs using maximal primes or minimal primes, loosing the algorithmic content of the results.

E.g., an ideal admitting a finite free resolution has a strong gcd, but the proof does not give the way of computing this gcd in the general situation (i.e. when computability hypotheses on the ring are only: we can compute $+$ and $\times$ in the ring).

Constructive finite free resolutions, 3

In the paper
Coquand T. & Quitté C. **Constructive finite free resolutions**. Manuscripta Math., 137, (2012), 331–345.
all the content of Northcott's book is made constructive, using simple technical tools.
In particular localizations at minimal primes are replaced by localizations at finitely many coregular elements.

More details on
http://hlombardi.free.fr/publis/ACMC-FFR.

Finding acceptable definitions

A typical example is the definition of Krull dimension. This notion appears in important theorems:

Kronecker theorem of the number of elements generating radically an arbitratry finitely generated ideal

Bass stable range theorem

Serre's Splitting off

Forster-Swan theorem

An acceptable definition for Krull dimension

We note $\mathsf{D}_{\mathbf{A}}(I) = \sqrt[\mathbf{A}]{I}$ the radical of an ideal I in $\mathbf{A}$.

We note $I_x = \langle x \rangle + (\mathsf{D}_{\mathbf{A}}(0) : x)$: the ideal generated by x and the y's s.t. xy is nilpotent.

Ideals $\mathsf{D}_{\mathbf{A}}(I)$ for finitely generated ideals I are the elements of the **Zariski lattice of the ring** $\mathbf{A}$.
This is a concrete distributive lattice and its dual space is the famous abstract topological space **Zariski spectrum of the ring** $\mathsf{Spec}(\mathbf{A})$.

Krull dimension of a distributive lattice has a nice simple constructive definition.

An acceptable definition for Krull dimension

A simple way to define $\mathsf{Kdim}\,\mathbf{A} \leqslant d$ is by induction on $d \geqslant -1$.

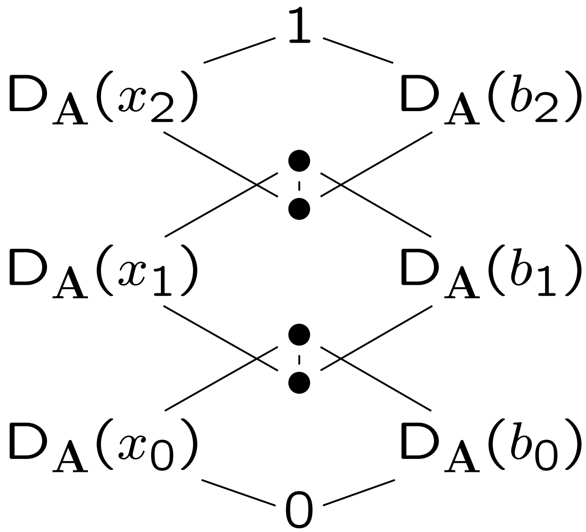
$\mathsf{Kdim}\,\mathbf{A} \leqslant -1$ if and only if $\mathbf{A}$ is trivial ($\mathbf{A} = \{0\}$).

For $d \geqslant 0$, $\mathsf{Kdim}\,\mathbf{A} \leqslant d$ if and only if for all $x \in \mathbf{A}$, $\mathsf{Kdim}(\mathbf{A}/I_x) \leqslant d - 1$.

An acceptable definition for Krull dimension

E.g. for dimension $\leqslant 2$, the definition corresponds to the following picture in $\mathsf{Zar}\,\mathbf{A}$.

Note: $\mathsf{D}_{\mathbf{A}}(xy) = \mathsf{D}_{\mathbf{A}}(x) \wedge \mathsf{D}_{\mathbf{A}}(y)$ and $\mathsf{D}_{\mathbf{A}}(x, y) = \mathsf{D}_{\mathbf{A}}(x) \vee \mathsf{D}_{\mathbf{A}}(y)$.



For all (x_0, x_1, x_2) there exist (b_0, b_1, b_2) s.t. inclusions drawn in the picture are true.

Dimension of the maximal spectrum?

Definition. *We define the* **Heitmann dimension** $\mathsf{Hdim}(\mathbf{A})$ *by induction.*

- $\mathsf{Hdim}(\mathbf{A}) = -1$ *if and only if* $\mathbf{A}$ *is trivial*
- *For* $\ell \geqslant 0$, $\mathsf{Hdim}(\mathbf{A}) \leqslant \ell$ *if and only if for all* $x \in \mathbf{A}$, $\mathsf{Hdim}(\mathbf{A}/J_x) \leqslant \ell - 1$ *where* $J_x = \langle x \rangle + (\mathrm{J}_{\mathbf{A}}(0) : x)$ *where* $\mathrm{J}_{\mathbf{A}}(0)$ *is the Jacobson radical of* $\mathbf{A}$.

This gives the dimension of the maximal spectrum in the Nœtherian case, and a good generalization in the general case.
This definition allows us to generalize Serre's splitting off and Forster-Swan theorem in the non-Nœtherian case, with a fully constructive proof.

Coquand T., Lombardi H., Quitté C. *Generating non-Nœtherian modules constructively*. Manuscripta mathematica, **115** (2004), 513–520.

Some References

Bishop E. *Foundations of Constructive Analysis*, (1967).

Weyl H. *The Continuum. A critical examination of the foundations of Analysis.* English translation by S. Polard & T. Bole. Thomas Jefferson Press, University Press of America (1987).

Feferman S. *In the Light of Logic*. Oxford University Press, (1998).

Bridges D., Richman F. *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press, (1987).

Coquand T., Lombardi H. *A logical approach to abstract algebra.* (survey) Math. Struct. in Comput. Science **16** (2006), 885–900.

Heitmann R. *Generating non-Nœtherian modules efficiently.* Michigan Math. **31** 2 (1984), 167–180.

Lombardi H., Quitté C. *Algèbre Commutative, Méthodes Constructives.* Calvage & Mounet, (2011).