General Methods in Constructive Algebra for deciphering noneffective proofs

Besançon, 23-27 sept. 2013
Conference on Algebraic and explicit methods in Number Theory

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

More details in spanish http://hlombardi.free.fr/publis/Gaceta.pdf
More details in french http://hlombardi.free.fr/publis/Plaidoyer.pdf
To see the slides: http://hlombardi.free.fr/publis/BesanconSlides.pdf

Hilbert's programme

Hilbert's programme 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 programme in its original finitist form was ruined by the incompleteness theorems of Gödel.

Henri Poincaré's programme

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). Reprint in *Dernières pensées*, Flammarion.

Bishop's Constructive Analysis

Poincaré's programme "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 programme.
Bishop's book (1967) **Foundations of Constructive Analysis** is a kind of realization of the Poincaré's programme.
But also a realization of Hilbert's programme, when one replaces finitist requirements by less stringent requirements, constructive ones.

Richman's work on Constructive Algebra

Mines R., Richman F., Ruitenburg W.
A Course in Constructive Algebra.
Universitext. Springer-Verlag, (1988)
This wonderful 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 $s_1, \ldots, s_n$ 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 understand 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 clear 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 large parts of commutative algebra.

Finite free resolutions

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

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

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 searchs 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.

Finite free resolutions, 2

A very good book on this 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).

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.

page 11

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

page 12

An acceptable definition for Krull dimension

We note $\mathrm{D}_{\mathbf{A}}(I) = \sqrt[\mathbf{A}]{I}$ the radical of an ideal I in $\mathbf{A}$.
Ideals $\mathrm{D}_{\mathbf{A}}(I)$ for finitely generated ideals I are the elements of the **Zariski lattice of the ring A**.
$\mathrm{D}_{\mathbf{A}}(I) \vee \mathrm{D}_{\mathbf{A}}(J) = \mathrm{D}_{\mathbf{A}}(I+J)$, $\mathrm{D}_{\mathbf{A}}(I) \wedge \mathrm{D}_{\mathbf{A}}(J) = \mathrm{D}_{\mathbf{A}}(IJ)$.
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 (Joyal 1974).

page 13

An acceptable definition for Krull dimension

A simple way to define $\mathsf{Kdim}\,\mathbf{A} \leqslant d$ is by induction on $d \geqslant -1$.
We note $I_x = \langle x \rangle + (\mathrm{D}_{\mathbf{A}}(0) : x)$: the ideal generated by x and the y's s.t. xy is nilpotent. We call it the **Krull boundary ideal of** x.

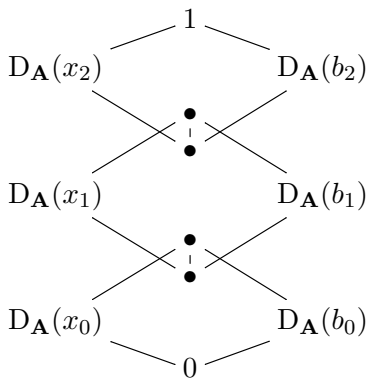
- $\mathsf{Kdim}\,\mathbf{A} \leqslant -1$ if and only if $\mathbf{A}$ is trivial ($\mathbf{A} = \{0\}$).
- For $d \geqslant 0$, $\mathsf{Kdim}\,\mathbf{A} \leqslant d$ if and only if for all $x \in \mathbf{A}$, $\mathsf{Kdim}(\mathbf{A}/I_x) \leqslant d-1$.

This definition does not use ideal objects as prime ideals: only concrete ones: lists of elements of the ring.

page 14

An acceptable definition for Krull dimension

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



For all (x_0, x_1, x_2) in $\mathbf{A}$ there exist (b_0, b_1, b_2) s.t. inclusions drawn in the picture are true.

An acceptable definition for Krull dimension

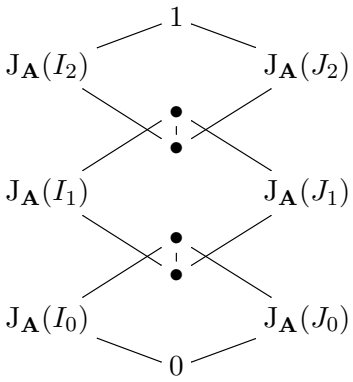
Heitmann has given non-Noetherian versions of theorems of Kronecker, Bass, Forster-Swan and Serre, with Krull dimension.
Since a constructive acceptable definition has been found for Krull dimension, these theorems can be obtained in a fully constructive form.
Heitmann R. **Generating non-Noetherian modules efficiently.**
Michigan Math. 31 (1984), 167–180.
Coquand T., Lombardi H., Quitté C.
Generating non-Noetherian modules constructively. Manuscripta mathematica, 115 (2004), 513–520.

Dimension of the maximal spectrum?

Theorems of Bass, Forster-Swan and Serre have formulations with the dimension of the maximal spectrum (the j-spectrum) for Noetherian rings. Heitmann remarks that the maximal spectrum is a spectral space (i.e., a dual of a distributive lattice) only for Noetherian rings. He proposed a new spectral space, **the J-spectrum**, and succeeded to prove Bass theorem for the J-dimension. The J-spectrum is the dual of a simple distributive lattice (not appearing in his paper). The elements of *the Heitmann lattice* are the ideals $\mathrm{J}_{\mathbf{A}}(I)$ for finitely generated ideals of $\mathbf{A}$.
Jacobson radical of I: $x \in \mathrm{J}_{\mathbf{A}}(I) \iff \forall y,\ 1+xy$ is invertible modulo I

Dimension of the maximal spectrum?

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



For all (I_0, I_1, I_2) there exist (J_0, J_1, J_2) s.t. inclusions drawn in the picture are true.

Dimension of the maximal spectrum?

In fact, examining the inductive proof of Heitmann, we found another dimension, better for doing induction.
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* $J_x = \langle x \rangle + (\mathrm{J}_{\mathbf{A}}(0) : x)$.

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

Quillen-Suslin and Lequain-Simis

A finitely generated projective module over $\mathbf{A}[X_1, \ldots, X_n]$, where $\mathbf{A}$ is a field *(Suslin)* or a PID *(Quillen)*, is free.
A finitely generated projective module over $\mathbf{A}[X_1, \ldots, X_n]$, where $\mathbf{A}$ is a Bezout domain of Krull dimension $\leqslant 1$, is free. A projective module over $\mathbf{A}[X_1, \ldots, X_n]$, where $\mathbf{A}$ is a Prüfer domain of Krull dimension $\leqslant 1$, is extended from $\mathbf{A}$ *(Maroscia, Brewer&Costa)*.
A finitely generated projective module over $\mathbf{A}[X]$, where $\mathbf{A}$ is a valuation domain of finite Krull dimension, is free *(Bass)*.
A finitely generated projective module over $\mathbf{A}[X_1, \ldots, X_n]$, where $\mathbf{A}$ is a Bezout domain, is free. A projective module over $\mathbf{A}[X_1, \ldots, X_n]$, where $\mathbf{A}$ is an arithmetical ring, is extended from $\mathbf{A}$ *(Lequain&Simis)*.

When does this work?

Coquand T., Lombardi H. **A logical approach to abstract algebra.** (survey) Math. Struct. in Comput. Science **16** (2006), 885–900.
$\forall\exists$*-theorems in Peano*: YES, Dragalin-Friedman translation
$\forall\exists\forall$*-theorems in Peano*: NO: a priori there is a divergence between the constructive meaning and the classical one. $\Rightarrow$ no miracle with Falting's theorem.
Geometric theories: formal theories with $\forall\exists$-axioms, generalized to infinite disjunctions replacing the existential quantifier (e.g., theories using minimal primes or maximal primes)
Experimental evidence that this works for Abstract Algebra in more general situations (e.g., flatness, coherence and many usefull notions are not formalizable in the "geometric" form).

Towards New Foundations of Mathematics

http://homotopytypetheory.org/book/
Homotopy type theory is a new branch of mathematics that combines aspects of several different fields in a surprising way. It is based on a recently discovered connection between homotopy theory and type theory. It touches on topics as seemingly distant as the homotopy groups of spheres, the algorithms for type checking, and the definition of weak ∞-groupoids. Homotopy type theory offers a new univalent foundation of mathematics, in which a central role is played by Voevodsky's univalence axiom and higher inductive types. The present book is intended as a first systematic exposition of the basics of univalent foundations, and a collection of examples of this new style of reasoning — but without requiring the reader to know or learn any formal logic, or to use any computer proof assistant. We believe that univalent foundations will eventually become a viable alternative to set theory as the implicit foundation for the unformalized mathematics done by most mathematicians.

Some Books (see http://en.bookfi.org/)

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).

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

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

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).

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

Thank you