Three lectures on Constructive Algebra

Niš Meeting

Constructive Mathematics:
Foundations and Practice

University of Niš, Faculty of Mechanical Engineering, Serbia.

June 24-28, 2013

H. Lombardi, Besançon

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

Poincaré on Cantorism

With most of us these prejudices have been dissipated, but it has come to pass that we have encountered certain paradoxes, certain apparent contradictions that would have delighted Zeno the Eleatic and the school of Megara. And then each must seek the remedy.

For my part, I think, and I am not the only one, that the important thing is never to introduce entities not completely definable in a finite number of words.

Whatever be the cure adopted, we may promise ourselves the joy of the doctor called in to follow a beautiful pathologic case.

Poincaré in *The future of mathematics; 1908*

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.

1. Structure of finitely generated abelian groups

Printable version of these slides:

http://hlombardi.free.fr/publis/Nis-LectDoc1.pdf

Basic references for constructive algebra

[MRR] *A Course in Constructive Algebra*
Mines R., Richman F., Ruitenburg W. (1985) Springer

[ACMC] *Algèbre Commutative, Méthodes Constructives*
Lombardi H., Quitté C. (2011) Calvage&Mounet.
http://hlombardi.free.fr/publis//LivresBrochures.html

Summary

- Structure of finitely generated abelian groups (classical mathematics)
- Smith diagonalization and consequences.
- Finitely presented abelian groups.
- Solutions of linear systems over a commutative ring. Coherence.
- Nœtherianity versus coherence.
- Principal Ideal Domains

Structure theorem for finitely generated abelian groups

We analyse the constructive content of a famous structure theorem.

Theorem 1. *A finitely generated abelian group is the direct sum*

- *of a free group* $\mathbb{Z}^k$ *(possibly* $k = 0$*)*
- *and of a torsion group* $\mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_r\mathbb{Z}$ *with all* $a_i > 1$ *and* a_i *divides* a_{i+1} *for* $1 \leqslant i < r$ *(possibly* $r = 0$*).*

We shall see that this theorem has no constructive proof, and we shall examine its constructive versions.

In fact we are interested by a more precise theorem.

Structure theorem for finitely generated abelian groups

Theorem 2. (Existence of a good basis, 1, classical mathematics). *Let G be a subgroup of $(\mathbb{Z}^n, +)$.*

1. *There exist a $\mathbb{Z}$-basis $(e_1, \ldots, e_n)$ of $\mathbb{Z}^n$, an integer r $(0 \leqslant r \leqslant n)$, and integers $a_1, \ldots, a_r \geqslant 1$ such that:*
   - *a_i divides a_{i+1} for $1 \leqslant i < r$*
   - *$(a_1 e_1, \ldots, a_r e_r)$ is a $\mathbb{Z}$-basis of G.*
2. *The subgroup $\tilde{G} = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_r$ of $\mathbb{Z}^n$ depends uniquely on G: it is equal to $\{\, x \,|\, \exists k > 0,\, kx \in G \,\}$.*
3. *$\mathbb{Z}^n/G \simeq \mathbb{Z}^{n-r} \oplus \tilde{G}/G$ with $\tilde{G}/G \simeq \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_r\mathbb{Z}$.*
4. *The list $[a_1, \ldots, a_r]$ is uniquely determined, $|\tilde{G} : G| = a_1 \cdots a_r$.*

Smith diagonalization of matrices over $\mathbb{Z}$

Theorem 3. (Smith reduction over $\mathbb{Z}$)
Let A be a matrix $\in \mathbb{Z}^{n\times m}$. It admits a Smith reduction*: we can construct $C \in \mathbb{GL}_m(\mathbb{Z})$ and $L \in \mathbb{GL}_n(\mathbb{Z})$ such that*

$$L\,A\,C = \boxed{L}\,\boxed{A}\,\boxed{C} = D = \begin{array}{|c|c|}\hline D_1 & 0 \\ \hline 0 & 0 \\ \hline \end{array}$$

with $D_1 = \mathrm{Diag}(a_1, \ldots, a_k)$, $0 \leqslant k \leqslant \min(m, n)$, $a_i > 0$ for $1 \leqslant i \leqslant k$, and a_i divides a_{i+1} for $1 \leqslant i \leqslant k-1$. Moreover, the a_i's are uniquely determined by A. The product $a_1 \cdots a_k$ is equal to the gcd of all $k \times k$ minors of A.

Consequences of Smith diagonalization

We are able to solve linear systems $AX = B$ over $\mathbb{Z}$, and to give equations and congruences characterizing good B's.

The good basis theorem applies constructively for subgroups $M \subseteq \mathbb{Z}^n$ which are finitely generated.

The structure theorem for finitely generated groups has a constructive proof when the group is finitely presented.

Consequences of Smith diagonalization

The kernel of any matrix is free (with an explicit basis) and it admits a free summand.

Duality: we are able to find a finite generator system for the solutions of a system of linear equations and congruences.

A subgroup $M \subseteq \mathbb{Z}^n$ which is a finite intersection of finitely generated subgroups is itself finitely generated.

Solutions of linear systems, coherence, strong discreteness

The problem of computing kernels of matrices, and generators for intersections of finitely many finitely generated submodules of a free module is a basic one. This leads to the notion of **coherent rings**.

Definition 4.

1. *A ring* $\mathbf{A}$ *is* **coherent** *if every linear form* $\mathbf{A}^n \to \mathbf{A}$ *has a finitely generated kernel.*
2. *An* $\mathbf{A}$*-module* M *is* **coherent** *if every linear map* $\mathbf{A}^n \to M$ *has a finitely generated kernel.*
3. *A ring* $\mathbf{A}$ *is* **strongly discrete** *if for every linear form* $\alpha : \mathbf{A}^n \to \mathbf{A}$ *and every* $x \in \mathbf{A}$*, either* $x \in \mathrm{Im}\alpha$ *or* $x \notin \mathrm{Im}\alpha$*.*
4. *An* $\mathbf{A}$*-module* M *is* **strongly discrete** *if for every linear map* $\alpha : \mathbf{A}^n \to M$ *and every* $x \in M$*, either* $x \in \mathrm{Im}\alpha$ *or* $x \notin \mathrm{Im}\alpha$*.*

Characterizations of coherence

Coherence is what is needed to **control homogeneous linear systems**.

Theorem 5. *A ring $\mathbf{A}$ is coherent if and only if the kernel of any linear map $\varphi : \mathbf{A}^n \to \mathbf{A}^m$ is finitely generated.*
An $\mathbf{A}$-module M is coherent if and only if the kernel of any linear map $\varphi : \mathbf{A}^n \to M^m$ is finitely generated.

If you add strong discreteness you control all linear systems: you are able to decide if a given right hand side B in linear system $AX = B$ has a solution.

Characterizations of coherence

Theorem 6. *A ring $\mathbf{A}$ is coherent if and only if*

1. *The intersection of two finitely generated ideals is always a finitely generated ideal.*
2. *The annihilator of any element $x \in \mathbf{A}$, i.e., $\{\, y \in \mathbf{A} \mid yx = 0 \,\}$ is a finitely generated ideal.*

Theorem 7. *An $\mathbf{A}$-module is coherent if and only if*

1. *The intersection of two finitely generated submodules is always a finitely generated submodule.*
2. *The annihilator of any element $x \in M$, i.e., $\{\, y \in \mathbf{A} \mid yx = 0 \,\}$ is a finitely generated ideal.*

Coherence.
From rings to finitely presented modules

Theorem 8.

1. *If* $\mathbf{A}$ *is a coherent ring, then so is any finitely presented* $\mathbf{A}$*-module.*

2. *If* $\mathbf{A}$ *is a strongly discrete coherent ring, then so is any finitely presented* $\mathbf{A}$*-module.*

Nœtherianity

The good basis theorem of classical mathematics can be seen as:

- Each finitely generated subgroup of $\mathbb{Z}^n$ admits a good basis (clearly constructive from Smith's diagonalization).
- Each subgroup of $\mathbb{Z}^n$ is finitely generated: Nœtherian property, problematic from a constructive point of view.

Nœtherianity

In order to analise constructively the Nœtherian property let us consider the five following variants for an $\mathbf{A}$-module M.

N1: Each submodule of M is finitely generated.

N2: Each nondecreasing chain of submodules

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

is eventually constant.

N3: Each nondecreasing chain of **finitely generated** submodules is eventually constant.

N4: In each nondecreasing chain of finitely generated submodules there are two equal consecutive terms.

N5: A strictly increasing chain of finitely generated submodules is impossible.

Nœtherianity

Each implication **N1** $\Rightarrow$ **N2** $\Rightarrow$ **N3** $\Rightarrow$ **N4** $\Rightarrow$ **N5** does have an algorithmic content.

But the reverse implications are problematic.

A solution? Choose good definitions and don't try to prove unprovable theorems!

A good definition of Noetherianity is **N4**: we say that the ring is **RS-Noetherian**

Coherence and Nœtherianity

In classical mathematics Noetherianity implies coherence. But strong "counterexamples" show that this implication has **no computational content**.

From a computational point of view, coherence is much more usefull than Noetherianity.

Nevertheless Noetherianity is interesting for obtaining proofs of termination for certain algorithms

Nœther Basis Theorem

Here Noetherian means RS-Noetherian.

Proposition 9. *If $\mathbf{A}$ is a Noetherian coherent ring, then so is any finitely presented $\mathbf{A}$-module.*

Theorem 10. (Hilbert, Nœther, Richman, Seidenberg)

1. *If $\mathbf{A}$ is a Noetherian coherent ring, then so is $\mathbf{A}[X]$.*
2. *If $\mathbf{A}$ is a strongly discrete Noetherian coherent ring, then so is $\mathbf{A}[X]$.*

Corollary 11.

1. *If $\mathbf{A}$ is a Noetherian coherent ring, then so is any finitely presented $\mathbf{A}$-algebra.*
2. *If $\mathbf{A}$ is a strongly discrete Noetherian coherent ring, then so is any finitely presented $\mathbf{A}$-algebra.*

Principal ideal domains

- $\mathbf{A}$ is a discrete domain: every element is regular or equal to 0. Equivalently, $\forall x \in \mathbf{A} \quad \mathrm{Ann}_{\mathbf{A}}(x) = \{0\}$ or $\langle 1 \rangle$.

- $\mathbf{A}$ is Bezout: each finitely generated ideal is principal. Equivalently (for a discrete domain) $\forall a, b,\ \exists u, v, s, t, g$ such that

$$\begin{bmatrix} u & v \\ s & t \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} g \\ 0 \end{bmatrix}, \quad \begin{vmatrix} u & v \\ s & t \end{vmatrix} = 1$$

- $\mathbf{A}$ is RS-Nœtherian: each ascending chain of finitely generated ideals has two consecutive terms equal.

Remark: We don't need an explicit divisibility relation, but without this condition the last item is a bit disturbing, and the algoritms are more complicated.

Structure theorem: finitely generated modules over a PID

Theorem 12. (Existence of a good basis). *Let* $\mathbf{A}$ *be a nontrivial PID and* M *a finitely generated submodule of* $\mathbf{A}^n$.

1. *There exist an* $\mathbf{A}$*-basis* $(e_1, \ldots, e_n)$ *of* $\mathbf{A}^n$, *an integer* r $(0 \leqslant r \leqslant n)$, *and regular elements* $a_1, \ldots, a_r \in \mathbf{A}$ *such that:*
   - a_i *divides* a_{i+1} $(1 \leqslant i < r)$
   - $(a_1 e_1, \ldots, a_r e_r)$ *is an* $\mathbf{A}$*-basis of* M.
2. *The submodule* $\widetilde{M} = \mathbf{A}e_1 \oplus \cdots \oplus \mathbf{A}e_r$ *of* $\mathbf{A}^n$ *depends uniquely of* M*: it is equal to* $\{\, x \,|\, \exists a \in \mathbf{A}, a \text{ regular}, ax \in M \,\}$.
3. $\mathbf{A}^n/M \simeq \mathbf{A}^{n-r} \oplus \widetilde{M}/M$, $\widetilde{M}/M \simeq \mathbf{A}/a_1\mathbf{A} \oplus \cdots \oplus \mathbf{A}/a_r\mathbf{A}$.
4. *The list* $[a_1\mathbf{A}, \ldots, a_r\mathbf{A}]$ *is uniquely determined.*

NB: M and $\widetilde{M}$ are free.

Smith diagonalization of matrices

Theorem 13. (Smith reduction over a PID $\mathbf{A}$)
Let A be a matrix $\in \mathbf{A}^{n\times m}$. It admits a Smith reduction*: we can construct $C \in \mathbb{GL}_m(\mathbf{A})$ and $L \in \mathbb{GL}_n(\mathbf{A})$ such that*

$$L\,A\,C = \boxed{L}\,\boxed{A}\,\boxed{C} = D = \begin{array}{|c|c|}\hline D_1 & 0 \\ \hline 0 & 0 \\ \hline \end{array}$$

with $D_1 = \mathrm{Diag}(a_1, \ldots, a_k)$, $0 \leqslant k \leqslant \min(m, n)$, $a_i \neq 0$ for $1 \leqslant i \leqslant k$, and a_i divides a_{i+1} for $1 \leqslant i \leqslant k-1$. Moreover, the $\langle a_i \rangle$'s are uniquely determined by A.

In fact Smith diagonalization works for Bezout domains of Krull dimension $\leqslant 1$ and PID do have dimension $\leqslant 1$.

Smith diagonalization of matrices

In fact Smith diagonalization works for Bezout domains of Krull dimension $\leqslant 1$ and PID do have dimension $\leqslant 1$.