Constructive semantics for classical formal proofs

Logic Colloquium 2011

Barcelona, July 2011
H. Lombardi, Besançon
Henri.Lombardi@univ-fcomte.fr, http://hlombardi.free.fr
http ://hlombardi.free.fr/publis/LC2011Slides.pdf
To print these slides in an economic way :
http ://hlombardi.free.fr/publis/LC2011Doc.pdf

Joint work

This talk is based on joint works with T. Coquand, M.E. Alonso, M. Coste, G. Díaz-Toca, C. Quitté, M.-F. Roy and I. Yengui
Survey papers with a logical flavour
Coquand T., L. H. **A logical approach to abstract algebra.** (survey) Math. Struct. in Comput. Science **16** (2006), 885–900.
Coste M., L. H., Roy M.-F. **Dynamical method in algebra : Effective Nullstellensätze**. A.P.A.L., **111**, (2001) 203–256.
L. H. **Algèbre dynamique, espaces topologiques sans points et programme de Hilbert.** A.P.A.L., **137** (2006), 256–290.
A book to appear (an english version in preparation)
L. H. and Quitté C. **Algèbre Commutative, méthodes constructives.**

Summary

Hilbert's programme

Classical mathematics are expected to work within set theory à la ZFC.
Nevertheless, the intuition behind ZFC is not at all correctly translated in a theory admitting countable models. And the presence of oddities as Banach-Tarski's Theorem is counterintuitive.
There is a lack of clear semantics for this (very abstract) theory. Moreover the Hilbert's programme, which was settled in order to secure Cantor set theory, has failed in its original form, asking finitary proofs of consistance.

Hilbert's programme

This is in strong constrast with the facts that many concrete results obtained by suspicious arguments inside ZFC become completely secured after further work (see references thereafter) and that no contradiction has appeared in this theory after a century of practical use.

Bishop E. *Foundations of Constructive Analysis.* McGraw Hill, 1967
Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext, Springer-Verlag, (1988).
Martin-Löf P. *The Hilbert-Brouwer controversy resolved ?*
One hundred years of intuitionism (1907-2007), (Cerisy), (Mark Van Atten & al., editors) Publications des Archives Henri Poincaré, Birkhaüser Basel, 2008, pp. 243–256.

Hilbert's programme

Mathematicians and logicians who do not think that ZFC has a clear content aim to solve the mystery of its fairly good concrete behaviour.
A possible issue is to develop a systematic way of finding constructive semantics, not for all classical objects, but at least for classical proofs giving "concrete" results.
Since we are not confident with the semantics of ZFC, and since we think that there is no miracle in mathematics, we have to explain why a large class of classical results are TRUE.
Here, we deal with a precise semantics of TRUE : something for which we have a constructive proof.

Hilbert's programme. An historical success

Gödel's incompleteness theorem kills Hilbert's programme in its original, finitistic, form. But this does not kill Hilbert's programme in its constructive form.
Theorem (Dragalin-Friedman)
In Peano*, a statement of the form*

$$\forall m,\ \exists n,\ f(m,n)=0$$

where f is primitive recursive, if provable with classical logic, is also provable with intuitionnistic logic.
Certainly this is far from proving consistency of ZFC, but this is a great success.

Hilbert's programme. Logical limitations

Since THERE EXISTS and OR do not have the same meaning in classical and constructive logic, some unavoidable limits appear in our "constructive Hilbert's programme".
First example. We can find a primitive recursive function $f : \mathbb{N}^3 \to \mathbb{N}$ such that the statement

$$\forall m,\ \exists n,\ \forall p,\quad f(m,n,p)=0$$

is provable with classical logic, and unprovable with intuitionnistic logic.
The logical structure of this statement is too high : $\forall\,\exists\,\forall\ \ldots\ldots$
Classical and constructive semantics conflict here with the meaning of TRUE for such a statement.

Hilbert's programme. Logical limitations

Second example. (Basic example in algebra)
If $\mathbf{K}$ *is a field, every polynomial* $f(X) \in \mathbf{K}[X]$ *of degree* ≥ 1 *has an irreducible factor.*
The logical structure of this statement is

$$\forall f,\ \exists g\ , \forall h\ \ldots\ldots\ldots$$

This is too much!

Hilbert's programme. Logical limitations

We can easily construct a counterexample to the above statement in a mathematical world with only Turing-computable objects.
E.g., a recursive countable field for which it is impossible fo find g from f as a result of a recursive computation, even when restricted to $\mathsf{deg}(f) = 2$.
Even if we don't want to work in such a restricted mathematical world, the counterexample shows that there is no hope to get a constructive proof of the statement.
From a constructive point of view, the statement is not exactly true, but its proof using TEM is interesting.
The proof says us how to use constructively the statement when it appears in a classical proof as an intermediate "idealistic" result which is used in order to prove a more concrete one.

Hilbert's programme. Logical limitations

A partial solution

This leads to a new, interesting, relevant semantics for "the splitting field of a polynomial".
The classical "static" splitting field (whose "construction" uses TEM) is replaced by a dynamic object, implementable on a computer.
This dynamic object offers a constructive semantics for the splitting field of a polynomial, and for the algebraic closure of a field.
D5 : Della Dora J., Dicrescenzo C., Duval D.
About a new method for computing in algebraic number fields. In Caviness B.F. (Ed.) EUROCAL '85. L.N.C.S. 204, 289–290.
Díaz-Toca G., L. H.
Dynamic Galois Theory. J. Symb. Comp. **45**, (2010) 1316–1329.

Hilbert's programme. A partial solution

We use a general, rather informal, recipe, in order to extract a computational content of classical proofs when they lead to concrete results.
The general idea is : use only formalizations with low logical complexity (e.g., only axioms in the form $\forall\ \exists\ \ldots$).
Replace logic, TEM and Choice by dynamical computations, i.e., lazzy and branching computations, as in D5.
In practice, this works for pieces of abstract algebra that can be formalized in "geometric theories".

Geometric first order theories
Dynamical computations

Example 1. Discrete fields

$(\mathbf{A}, \bullet = 0, +, -, \times, 0, 1)$

Commutative rings

Computational machinery of commutative rings, plus three very simple axioms :

$$\vdash\ 0 = 0, \qquad x = 0\ \vdash\ xy = 0, \qquad x = 0,\ y = 0\ \vdash\ x + y = 0.$$

A : generators and relations for a commutative ring

NB : $a = b$ is an abreviation for $a - b = 0$, and usual axioms for equality and ring-structure are consequence of the computational machinery inside $\mathbb{Z}[x, y, z]$.

Axiom of discrete fields (a geometric axiom)

- $\vdash\ x = 0\ \vee\ \exists y\ xy = 1$

Geometric first order theories, dynamical computations, example 1

Using the geometric axiom as a dynamical computation

An example : prove the dynamical rule : • $x^2 = 0\ \vdash\ x = 0$.

Open two branches.

In the first one, $x = 0$.

In the second one, add a parameter y and the equation $1 - xy = 0$,

deduce $x^2 y = 0$ (commutative ring),

deduce $x(1 - xy) = 0$ (commutative ring).

deduce $x(1 - xy) + x^2 y = 0$ (commutative ring).

the computational machinery tells us LHS equals x,

i.e., it reduces $x - LHS$ to 0

You have got $x = 0$ at the two leaves.

Geometric first order theories, dynamical computations

Cut elimination

A first order theory is said to be geometric when all axioms are "geometric first order axioms" :

- $A(\underline{x})\ \vdash\ \exists \underline{y}\, B(\underline{x}, \underline{y})\ \vee\ \exists \underline{z}\, C(\underline{x}, \underline{z})\ \vee\ \ldots$

where A, B, C are conjunctions of predicates over terms.

These axioms can be viewed as deduction rules and used, without logic, as computational rules inside "proof trees" : what we call a dynamical computation (or dynamical proof)

Theorem *For a first order geometric theory, in order to prove facts or geometric rules, TFAE*

1. First order theory with classical logic

2. First order theory with constructive logic

3. Dynamical computations

Geometric first order theories, cut elimination

Orevkov V. P. *On Glivenko sequent classes.* In Logical and logico-mathematical calculi [11], pages 131–154 (Russian), 147–173 (English). Trudy Matematicheskogo Instituta imeni V.A. Steklova, (1968). English translation, The calculi of symbolic logic. I, Proceedings of the Steklov Institute of Mathematics, vol. 98 (1971).
Nadathur G. *Correspondence between classical, intuitionistic and uniform provability.* Theoretical Computer Science, **232** 273–298, (2000).
Coste M., L. H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* A.P.A.L., **111**, (2001) 203–256.
Avigad J. *Forcing in Proof Theory.* The Bulletin of Symbolic Logic, **10** (2004), pp. 305–333
Schwichtenberg H., Senjak, C. *Minimal from classical proofs.* To appear : CALCO-Tools 2011.

Geometric first order theories, dynamical computations, example 1

Theorem 1 TFAE :
1. **A** proves $1 = 0$ (i.e., the ring is trivial) as a commutative ring
2. 1 belongs to the ideal generated by the relations given in **A**
3. **A** proves $1 = 0$ as a discrete field (first order theory)
3°. **A** proves $1 = 0$ as a discrete field by dynamical computations
4. $\mathbf{A} \cup \{z; f(z) = 0\}$ (f monic of degree ≥ 1) proves $1 = 0$ as a discrete field (first order theory)
4°. $\mathbf{A} \cup \{z; f(z) = 0\}$ (f monic of degree ≥ 1) proves $1 = 0$ as a discrete field by dynamical computations
5. **A** proves $1 = 0$ as an algebraically closed discrete field (first order theory)
5°. **A** proves $1 = 0$ as an algebraically closed discrete field by dynamical computations

Geometric first order theories, dynamical computations, example 1

Theorem 2 TFAE :
1. **A** proves $a = 0$ as a commutative reduced ring
2. **A** proves $a = 0$ as a discrete field (first order theory)
2°. **A** proves $a = 0$ as a discrete field by dynamical computations
3. for some $N \geq 0$, a^N is in the ideal generated by the relations given in **A**
4. **A** proves $a = 0$ as an algebraically closed discrete field (first order theory)
4°. **A** proves $a = 0$ as an algebraically closed discrete field by dynamical computations

Geometric first order theories, dynamical computations, example 1

Corollary 1 **Hilbert's Nullstellensatz**
If $g, f_1, \ldots, f_r \in \mathbf{K}[X_1, \ldots, X_n]$, where $\mathbf{K} \subseteq \mathbf{L}$ algebraically closed, there is a test for "g vanishes at the zeroes of $f_1, \ldots, f_r$ in $\mathbf{L}^n$ ".
This test is done by a dynamical computation which either gives $g^N \in \langle f_1, \ldots, f_r \rangle$ for an $N \geq 0$, or computes a point $x \in \mathbf{L}^n$ such that $g(x) \in \mathbf{L}^\times$ and $f_1(x) = \cdots = f_r(x) = 0$.
Corollary 2 **Formal Hilbert's Nullstellensatz**
If $g, f_1, \ldots, f_r \in \mathbb{Z}[X_1, \ldots, X_n]$, we have a test for $g = 0$ being a consequence of $f_1 =$

$\cdots = f_r = 0$ *in all reduced rings.*
This test is done by a dynamical computation which either gives $g^N \in \langle f_1, \ldots, f_r \rangle$ *for an* $N \geq 0$*, or computes a finite field* $\mathbf{F}$ *and a point* $x \in \mathbf{F}^n$ *such that* $g(x) \in \mathbf{F}^\times$ *and* $f_1(x) = \cdots = f_r(x) = 0$*.*

Geometric first order theories, dynamical computations

Example 2. Local rings

Axiom of local rings
In words : $x + y$ *invertible implies* x *invertible or* y *invertible.*

- $(x+y)z = 1 \vdash \exists u\, xu = 1 \vee \exists v\, yv = 1$

Axioms of residually discrete local rings
In words : *every element is invertible or in the Jacobson radical.*
We need to introduce two more predicates, $\mathsf{Iv}(x)$ for "x invertible", and $\mathsf{Zr}(x)$ for "x is in the Jacobson radical" (is zero residually).

- $x = 0 \vdash \mathsf{Zr}(x)$
- $\mathsf{Zr}(x) \vdash \mathsf{Zr}(xy)$
- $\mathsf{Zr}(x), \mathsf{Zr}(y) \vdash \mathsf{Zr}(x+y)$
- $\mathsf{Zr}(x), \mathsf{Iv}(y) \vdash \mathsf{Iv}(x+y)$
- $\vdash \mathsf{Iv}(1)$
- $\mathsf{Iv}(xy) \vdash \mathsf{Iv}(x)$
- $\mathsf{Iv}(x) \vdash \exists u\, ux = 1$
- $\vdash \mathsf{Iv}(x) \vee \mathsf{Zr}(x)$

Geometric first order theories, dynamical computations, example 2

Local-global principle

Theorem Let $S : AX = B$ be a linear system on $\mathbf{A}$.
TFAE :

1. $\mathbf{A}$ proves that S has a solution as a commutative ring
2. $\mathbf{A}$ proves that S has a solution as a local ring (first order theory)

2°. $\mathbf{A}$ proves that S has a solution as a local ring by dynamical computations

3°. $\mathbf{A}$ proves that S has a solution as a residually discrete local ring by dynamical computations

In classical mathematics, local rings are always residually discrete and point 2. means (using Choice) : S has a solution after localization at all prime ideals
In constructive mathematics, the fact that point 3°. implies point 1. is the basic tool for deciphering classical proofs that use localization at all prime ideals.

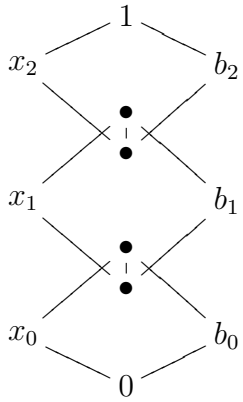
Geometric first order theories, dynamical computations

Example 3. Spectral spaces

Spectral spaces are very important in abstract algebra. As shown by Stone in 1930, the category of spectral spaces is (in classical mathematics) equivalent to the opposite category of distributive lattices.
To a spectral space corresponds the distributive lattice made of compact open subspaces. This dual lattice gives a constructive semantics for the spectral space. Indeed, a distributive lattice is a simple algebraic structure $(L, \vee, \wedge, 0, 1)$. But the existence of "points" of the dual spectral space $\mathsf{Spec}(L)$ (i.e., morphisms $L \to \{0, 1\}$) need choice and TEM.

Geometric first order theories, dynamical computations, example 3

The notion of Krull dimension of a spectral space is often important in concrete applications, so it is useful to understand what is its meaning for the constructive object L. This was done by Joyal in 1974, and is now given in a very simple formulation.
For example, $\mathsf{Kdim}(L) \leq 2$ means that for each $x_0, x_1, x_2 \in L$ we can find b_0, b_1, b_2 with the following inequalities



Geometric first order theories, dynamical computations, example 3

This is much simpler than the usual definition of Krull dimension which needs quantification over elements of $\mathsf{Spec}(L)$, which is second order.
Nevertheless, in order to use this very simple definition in commutative algebra, we have to deal with various spectra which are dual to various distributive lattices attached to a ring, and this needs "geometric logic", which is more powerful than "geometric first order theories".

Geometric theories. Barr's Theorem

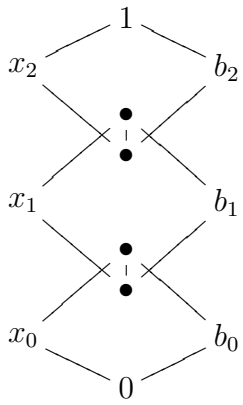
First order geometric theories are not enough powerful for explaining the success story of abstract algebra in classical mathematics.
Many basic notions do not fit in the pattern.
For example, to be a reduced ring is first order, but to be nilpotent (for an element of a ring) is not first order. This needs an existential quantification over $\mathbb{N}$. But $\mathbb{N}$ is very complicated, as Gödel told us.
So it is convenient to replace $\quad \exists N \in \mathbb{N},\ a^N = 0 \quad$ by a "more concrete" infinite disjunction

$$1 = 0 \ \vee \ a = 0 \ \vee \ a^2 = 0 \ \vee \ a^3 = 0 \ \vee \ \ldots$$

Geometric theories

Another example is the notion of Krull dimension of a ring. We need to deal with a concrete definition of Krull dimension for a commutative ring $\mathbf{A}$. The distributive lattice $\mathsf{Zar}(\mathbf{A})$, dual of the spectral space $\mathsf{Spec}(\mathbf{A})$ (the Zariski spectrum) is the lattice of ideals

of the form $\sqrt{\langle a_1, \ldots, a_r \rangle}$ (for all finite sequences in $\mathbf{A}$). So $\mathsf{Kdim}\,\mathbf{A} \leq 2$ means that for each $x_0, x_1, x_2 \in \mathsf{Zar}(\mathbf{A})$ we can find $b_0, b_1, b_2 \in \mathsf{Zar}(\mathbf{A})$ with the following inequalities



Geometric theories

So $\mathsf{Kdim}(\mathbf{A}) \leq r$ is a geometric notion. In order to work with it, we found an equivalent more manageable version.

Definition 1 If $a \in \mathbf{A}$ we call $\mathcal{K}(a) = a\mathbf{A} + (\sqrt{0} : a)$ the *Krull boundary ideal of* a : i.e. $\mathcal{K}(a) = \{\, ax + y \mid ya \text{ is nilpotent} \,\}$.

Definition 2

We give the following *inductive definition* for $\mathsf{Kdim}\,\mathbf{A} \leq n$:

- $\mathsf{Kdim}\,\mathbf{A} \leq -1$ means that the ring is trivial $(1 = 0)$,
- for $n \geq 0$, $\mathsf{Kdim}\,\mathbf{A} \leq n$ means that for each $a \in \mathbf{A}$, $\mathsf{Kdim}(\mathbf{A}/\mathcal{K}(a)) \leq n - 1$.

Geometric theories

Another typical example (see [Wraith]) of notion expressed geometrically is the notion of *flat* module M over a ring $\mathbf{A}$.

It says that if we have a relation $PX = 0$ where P is a row vector with elements in $\mathbf{A}$ and X a column vector with elements in M then we can find a rectangular matrix Q and a vector Y such that $QY = X$ and $PQ = 0$.

In words : *linear dependance relations in* M *can always be explained in* $\mathbf{A}$.

Since we don't say anything about the size of Q and Y, this statement involves implicitely an infinite disjunction over matrices of arbitrary size. Thus the notion of flat module is not first-order but geometric.

G. Wraith *Intuitionistic algebra : some recent developments in topos theory.* Proceedings of the International Congress of Mathematicians (Helsinki, 1978), pp. 331–337, Acad. Sci. Fennica, Helsinki, 1980.

Geometric theories. Barr's Theorem

As stressed by G. Wraith the importance of geometric formulae comes from *Barr's theorem* :

Theorem *If a geometric sentence is deducible from a geometric theory in classical logic, with the axiom of choice, then it is also deducible from it intuitionistically.*

Furthermore in this case there is always a proof with a branching tree form, a *dynamical* proof. In general, this tree may be infinitely branching.

But Barr's theorem cannot have a constructive proof. So, it is an experimental work : "interesting geometric theorems" in commutative algebra can "always" be proven by well controlled branching trees.
Barr M. *Toposes without points.* J.P.A.A, **5**, 265–280, (1974).

page 30

Geometric theories

Example 1. Serre splitting off and Forster

Theorem 1 (Forster theorem, 1964)
If $\mathbf{A}$ *is a Nœtherian ring,* $\mathsf{Kdim}\ \mathbf{A} \leq r$ *and* M *is a finitely presented module locally generated by* r *elements, then it can be generated by* $n + r$ *elements.*
Theorem 2 (Heitmann, 1984 : nonNœtherian Forster theorem and Serre splitting off for Krull dimension, concrete version)
If $\mathsf{Kdim}\ \mathbf{A} < n$ *and if* F *is a rectangular matrix over* $\mathbf{A}$ *such that* $\Delta_n(F) = 1$*, then there exists a linear combination of the columns of* F *which is unimodular.*

page 31

Geometric theories. Example 1

Serre splitting off and Forster theorem work also (in classical mathematics) for Nœtherian rings with the dimension of the maximal spectrum.
In general, the maximal spectrum is not a spectral space.
So, Heitmann suggested a nonNœtherian generalization.
He considered *a new spectral space* (equal to the maximal spectrum in the Nœtherian case) with a complicated definition.
It turns out that the corresponding distributive lattice $\mathsf{Heit}(\mathbf{A})$ is the set of ideals of the form

$$\mathcal{H}(a_1, \ldots, a_r) = \{\, x \mid \forall y,\, \exists u,\, 1 - (1 + xy)u \in \langle a_1, \ldots, a_r \rangle \,\}$$

This makes the definition of $\mathsf{Kdim}(\mathsf{Heit}(\mathbf{A})) \leq n$ no more geometric.

page 32

Geometric theories. Example 1

Remark : you can obtain the definition of $\mathsf{Kdim}(\mathsf{Heit}(\mathbf{A})) \leq n$ in a geometric form if you introduce predicates (with suitable axioms) for $x \in \mathcal{H}(a_1, \ldots, a_r)$.
Heitmann did not succeed to prove Serre splitting off and Forster theorem for $\mathsf{Kdim}(\mathsf{Heit}(\mathbf{A}))$.

page 33

Geometric theories. Example 1.

Nevertheless, his approach suggests to use a new notion of dimension, which mimics the inductive definition of Krull dimension, replacing in the definition $\sqrt{0}$ by the Jacobson radical. This new dimension (we call it Heitmann dimension) is $\leq \mathsf{Kdim}(\mathsf{Heit}(\mathbf{A}))$.
And Serre splitting off and Forster theorem do work for Heitmann dimension.
This gives a new result (even better than the one conjectured by Heitmann) in commutative algebra. This was made possible because the proof for Krull dimension was more clear and more simple in the constructive setting than in the classical one.

Geometric theories

Example 2. Dedekind domains

Theorem (using classical matheatics)
Let **A** be a Nœtherian domain, integrally closed in its fraction field, and with Krull dimension ≤ 1. Then ideals of **A** are locally free.
Extracting the constructive content of the proof gives the following
Theorem Let **A** be a coherent domain, integrally closed in its fraction field, and with Krull dimension ≤ 1.
Then **A** is an arithmetical ring : finitely generated ideals are locally principal : for all a, b you can find s, u, v such that $sa = ub$ and $(1 - s)b = va$.

Geometric theories

Example 3. Using maximal ideals

Another typical example of notion expressed geometrically is the notion of maximal ideal.
If you try to express the notion as a first order one, what you get is in fact the notion or prime ideal.
This is related to the fact that in model theory, existential statements are allowed to be verified by elements outside the initial structure (think to algebraic closure).
A predicate $M(x)$ with the meaning of "x belongs to a (generic) maximal prime of the ring **A**" has to verify an infinite disjunction

$$M(x) \ \vee \bigvee_{y \in \mathbf{A}} M(xy - 1)$$

Geometric theories. Example 3

Assume you deal with a classical proof that says : in order to prove that the ring you have constructed is trivial, take the quotient by an arbitrary maximal prime and find a contradiction.
You introduce a predicate $M(x)$ for the generic maximal prime and you follow the classical proof. Each time you have to chose a branch for an element x_i, you try the branch $M(x_i)$.
At a moment, the classical proof shows "a contradiction". This means that $\langle x_1, \ldots, x_n \rangle$ contains 1. This shows that x_n is invertible modulo $\langle x_1, \ldots, x_{n-1} \rangle$, so the infinite disjunction under x_n is satisfied in one branch with an element y you have computed.

Geometric theories. Example 3

And you can follow the proof.
Yengui have done this job for a crucial Suslin Lemma in the Suslin proof for Quillen-Suslin theorem.
Yengui I. *Making the use of maximal ideals constructive.*
Theoretical Computer Science, **392**, (2008) 174–178.

Geometric theories

Examples using minimal prime ideals

Theorem **Traverso-Swan**
For a reduced ring $\mathbf{A}$, TFAE
1. $\mathbf{A}$ is seminormal : if $x^2 = y^3$ there exists z, $z^2 = y$ and $z^3 = x$.
2. any rank 1 projective module over $\mathbf{A}[X]$ is extended from $\mathbf{A}$
3. any rank 1 projective module over $\mathbf{A}[X, Y]$ is extended from $\mathbf{A}$

Theorem **Zariski Main Theorem**
Let $\mathbf{A}$ be a ring with an ideal $\mathfrak{J}$ and $\mathbf{B}$ be a finitely generated algebra $\mathbf{A}[x_1, \ldots, x_n]$ such that $\mathbf{B}/\mathfrak{J}\mathbf{B}$ is a finite generated $\mathbf{A}/\mathfrak{J}$-module, then there exists $s \in 1 + \mathfrak{J}\mathbf{B}$ such that $s, sx_1, \ldots, sx_n$ are integral over $\mathbf{A}$.

Beyond

So Hilbert's programme works in practice for many important theorems in abstract commutative algebra.
Mainly when we are able to use geometric theories.
But ...
What about Nœtherianity ?
(definitively outside the scope of geometric theories)
What about coherent rings ?
This notion captures a good part of the constructive content of Nœtherianity, but this is not a geometric notion.
What about real numbers ?
We need a constructive theory of O-minimal structures.

Thank you