Concrete proofs with abstract objects in modern algebra

Henri Lombardi
Université de Franche-Comté, Besançon, France
Henri.Lombardi@univ-fcomte.fr, http://hlombardi.free.fr

Oberwolfach, April 11, 2008

Mathematical Logic: Proof Theory, Constructive mathematics

Contents

Printable version of these slides:

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

Slides:

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

The computer algebra system D5

Classical Theorem. Any field $\mathbf{K}$ is contained in an algebraically closed field.

Recursive counter example. It is possible to construct a computable field $\mathbf{K} \supseteq \mathbb{Q}$ in which there is no (recursive) algorithm for factoring polynomials $X^2 - p$ (p a prime).

First classical step. Given any polynomial f of degree $d \geq 1$ in $\mathbf{K}[X]$ there exists a field $\mathbf{L} \supseteq \mathbf{K}$ where f has at least one root.

The computer algebra system D5. 2

A possible solution: D5.
Computing dynamically in a reliable way inside the algebraic closure,
even if *this object does not exist as a constructive static object*.

The too abstract object "algebraic closure" is replaced by a dynamical object, a concrete one.

Excluded middle (or uncertainty) is replaced by: try the two cases.

The computer algebra system D5. 3

Constructive rereading of | the algebraic closure exists | ?

Very simple: | our dynamical computations are safe | !

Proof of this fact? The same as in classical mathematics: make the Euclidean division!

Zorn's lemma? only an abstract (mysterious) trick saying that a coherent first order theory has a model. The important fact is we have a constructive proof that the theory is coherent.

The computer algebra system D5. 4

In classical mathematics, two algebraic closures of a field $\mathbf{K}$ are isomorphic.

This isomorphism cannot be constructed in the dynamical constructive setting.

Nevertheless, there is a constructive version related to dynamical decomposition fields of a given polynomial: finite approximations of the isomorphism are available.

Galois variation

Classical Galois approach. Given any polynomial f of degree $d \geq 1$ in $\mathbf{K}[X]$ there exists a field $\mathbf{L} \supseteq \mathbf{K}$ with $f(X) = \prod_{i=1}^{d}(X - x_i)$ inside $\mathbf{L}[X]$. This field carries some ambiguities, related to the Galois group of the equation.

A possible solution: computing in a reliable way inside the field $\mathbf{L}$ generated by the roots of f, even if, at any step of the computation we don't know the dimension of the $\mathbf{K}$-vector space $\mathbf{L}$.

Galois variation. 2

The field $\mathbf{L}$ is represented by the universal splitting algebra $\mathbf{A}$ of the polynomial, with "Galois group" $\mathfrak{S}_n$.

Possibly the computations inside $\mathbf{L}$ show us that we have to pass to a quotient algebra, (a Galois quotient of the previous algebra) i.e., to improve the equality relation and to replace $\mathfrak{S}_n$ by a convenient subgroup.

I.e., we improve step by step our knowlege of $\mathbf{L}$ without contradicting previous informations about it.

At each improvement, we have to make an arbitrary choice (e.g., if the computation shows that the sum of 3 $x'_i s$ is zero, we have to say something as: OK, we take x_1, x_2 and x_3).

Galois variation. 3

The isomorphism theorem becomes:

> If two computations lead to two Galois quotients $\mathbf{L}_1$ and $\mathbf{L}_2$ of $\mathbf{A}$,
> then there exists a third one, $\mathbf{L}_3$
> such that $\mathbf{L}_1 \simeq \mathbf{L}_3^{r_1}$ and $\mathbf{L}_2 \simeq \mathbf{L}_3^{r_2}$.

The two distinct informations about $\mathbf{L}$ can be glued together!

Galois variation. 4

Constructive rereading of | the decomposition field of f exists | ?

Very simple: | our dynamical computations are safe | !

Proof of this fact? The universal splitting algebra $\mathbf{A}$ exists, with "Galois group" $\mathfrak{S}_n$! (which is based on Euclidean division).

In classical mathematics: TEM allows to get directly a minimal idempotent of $\mathbf{A}$, so $\mathbf{A}/\langle 1-e\rangle$ is a decomposition field. The Galois group is $G = \mathrm{Stab}(e)$.

Constructively we only know successive approximations of $\mathbf{L}$ and G.

Galois variation. 5

One has Spec $\mathbf{A} = \mathrm{Spec}(\mathbb{B}(\mathbf{A}))$ where $\mathbb{B}(\mathbf{A})$ is the Boolean algebra of idempotent elements $(e^2 = e)$ in $\mathbf{A}$
$(e \wedge e' = ee'$, $e \vee e' = e + e' - ee'$, $\neg e = 1 - e)$.

We have a bound on the number $\#\mathbb{B}(\mathbf{A})$.

The obstacle comes from the fact that we don't know precisely the "finite" Boolean algebra $\mathbb{B}(\mathbf{A})$.

The concrete computations inside $\mathbf{L}$ lead to removing ambiguities, i.e., better knowing the equality relation and the Galois group.

Galois variation. 6

When dealing with all the roots of a given polynomial, the global concrete object

universal splitting algebra as a representation for $\mathbf{L}$

(equality being constructed through the computations) is a better approach than the "naive" D5 (no duplicated computations).

Galois variation. 7

Although we compute in a reliable way inside $\mathbf{L}$, our decomposition field $\mathbf{L}$ cannot be defined as a "set" in the Bishop style.

Bishop's sets are static (rigid) objects: we have to say at the beginning what is the meaning of the equality.

In the dynamical context, equality is constructed step after step, in an interactive way. It depends on the computations we need to perform.

Dynamic evaluation is nothing but lazy evaluation.

Local-global principles

Classical moto in abstract algebra:

> *in order to get a concrete result when dealing with a commutative ring*
> *see what happens after localization at an arbitrary prime.*

"Localizing at an arbitrary prime" has the following **concrete content**:

> *consider the same (rigid) structure, but add the axioms of local rings,*
> *you get a (non-rigid) dynamical structure, and you see what happens.*

Local-global principles. 2

In the classical abstract proof you think that you are looking at all primes.

But the corresponding "set" (the Zariski spectrum of the ring) is really too big and too mysterious.

In fact, you are only writing a proof, which is a finite object, using only a finite amount of information about the "generic prime" you consider.

Constructive rereading: replace "all primes" by "a generic prime", and "compacity of Spec $\mathbf{A}$", that is "sums are finite in algebra", by "proofs are finite in our books".

Zariski spectrum

Fundamental object in abstract algebra, usually defined as the set of prime ideals of a ring $\mathbf{A}$ with the basic opens

$$D(a) = \{\mathfrak{P} \mid a \notin \mathfrak{P}\}.$$

However, even if the ring $\mathbf{A}$ is given concretely (i.e., we are able to make basic computations in it) it may be difficult to show effectively the existence of prime.

Often, what matters is not *one* particular prime ideal, but the collection of *all* prime ideals.

Zariski spectrum. 2

Zariski spectrum is best seen as a *point-free* space

A. Joyal (1972) definition of the Zariski spectrum

A *support* on $\mathbf{A}$ is a map $D : \mathbf{A} \longrightarrow L$ in a *distributive lattice* L satisfying the conditions

$$D(0) = 0 \qquad D(1) = 1 \qquad D(ab) = D(a) \wedge D(b) \qquad D(a + b) \leq D(a) \vee D(b)$$

The Zariski spectrum can then be defined as **the free support** on $\mathbf{A}$

Zariski spectrum. 3

This definition is purely algebraic (no need of Zorn's Lemma)

Theorem: $D(a) \leq D(b_1) \vee \cdots \vee D(b_n)$ *holds iff* a *is in the radical ideal generated by* $b_1, \ldots, b_n$.

This is also known as the *formal* version of the Nullstellensatz.

The proof is direct: one shows that the lattice of finitely generated radical ideals is the free support.

$D(u)$: finite piece of information about a prime ideal.

Zariski spectrum. 4

A. Joyal. *Le théorème de Chevalley-Tarski.*
Cahiers de Topologie et Géometrie Differentielle, (1975).

L. Español. *Constructive Krull dimension of lattices.*
Rev. Acad. Cienc. Zaragoza (2) 37 (1982), 5–9.

L. Español. *Dimension of Boolean valued lattices and rings.*
J. Pure Appl. Algebra 42 (1986), no. 3, 223–236.

T. Coquand, H. Lombardi. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings*, 477–499, Commutative ring theory and applications, Lecture notes in pure and applied mathematics vol 231. M. Dekker (2002)

T. Coquand, H. Lombardi, M.-F. Roy.
An elementary characterisation of Krull dimension
From Sets and Types to Analysis and Topology (L. Crosilla, P. Schuster, eds.). Oxford University Press. (2005) 239–244.

Zariski spectrum and Krull dimension

The pointfree version of Zar $\mathbf{A}$ has been shown to be a very efficient tool in deciphering abstract proofs that use prime ideals.

In particular it has lead to a constructive characterisation of Krull dimension of a ring. This (new) constructive definition of Krull dimension is manageable for usual rings appearing in mathematics.

This has opened the possibility of finding constructive proofs for theorems stating concrete results under some asumptions concerning the Krull dimension.

Zariski spectrum and Krull dimension. 2

O. Forster
Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring
Math.Z. 84 1964, 80-87

J.-P. Serre
Modules projectifs et espaces fibrés à fibre vectorielle
Séminaire P. Dubreil, Année 1957/1958

R.G. Swan
The Number of Generators of a Module
Math.Z. 102 (1967), 318-322

R. Heitmann
Generating non-Noetherian modules efficiently
Michigan Math. J. 31 (1984), 167-180

Zariski spectrum and Krull dimension. 3

T. Coquand. *Sur un théorème de Kronecker concernant les variétés algébriques.* C.R.Acad.Sci., Paris, Ser I, 338 (2004), Pages 291-294

T. Coquand, H. Lombardi, C. Quitté. *Generating non-Noetherian modules constructively.* Manuscripta Mathematica, 115 (2004), Pages 513-520

T. Coquand, H. Lombardi, C. Quitté. *Dimension de Heitmann des treillis distributifs et des anneaux commutatifs.* Publications mathématiques de Besançon (2006), 51 pages.

Simple global objects related to maximal prime ideals

Maximal ideals are the prime ideals $\mathfrak{m}$ such that $\mathbf{A}/\mathfrak{m}$ is zero dimensional. In general, these ideal objects are not reachable from a constructive point of view, but their intersection is!

$$\mathrm{Rad}(\mathbf{A}) \stackrel{\mathrm{def}}{=} \bigcap_{\mathfrak{m}\in \mathsf{Max}(\mathbf{A})} \mathfrak{m} = \Big\{\, x \in \mathbf{A} \,|\, 1 + x\mathbf{A} \subseteq \mathbf{A}^{\times} \,\Big\} = \{\, x \mid \langle x, z\rangle = \langle 1\rangle \Rightarrow \langle z\rangle = \langle 1\rangle \,\}$$

In addition

$$\bigcap_{\mathfrak{m}\in \mathsf{Max}(\mathbf{A})} (\mathbf{A} \setminus \mathfrak{m}) = \mathbf{A}^{\times}.$$

Simple global objects related to minimal prime ideals

Minimal prime ideals are the prime ideals $\mathfrak{p}$ such that $\mathbf{A}_{\mathfrak{p}}$ is zero dimensional. In general, these ideal objects are not reachable from a constructive point of view, but their intersection is!

$$\bigcap_{\mathfrak{p}\in \mathrm{Min}(\mathbf{A})} \mathfrak{p} = \sqrt{\langle 0\rangle} = \mathrm{D}_{\mathbf{A}}(0) = \{\, x \in \mathbf{A} \mid \exists n\ x^n = 0 \,\}$$

In addition

$$\bigcap_{\mathfrak{p}\in \mathrm{Min}(\mathbf{A})} (\mathbf{A} \setminus \mathfrak{p}) = \{\, a \in \mathbf{A} \mid \forall y \in \mathbf{A} \quad (0 = \mathrm{D}_{\mathbf{A}}(ay) \ \Rightarrow\ 0 = \mathrm{D}_{\mathbf{A}}(y)) \,\}\,.$$

Other global objects related to prime ideals

A prime ideal $\mathfrak{P} \subseteq \mathbf{A}$ can be used in classical algebra in three different ways.

1. Constructing the quotient $\mathbf{A}/\mathfrak{P}$, which is a **domain**.
2. Constructing the localisation $\mathbf{A}_{\mathfrak{P}}$, which is a **local ring**.
3. Constructing the **field** $\mathrm{K}_{\mathbf{A}}(\mathfrak{P}) = \mathrm{Quot}(\mathbf{A}/\mathfrak{P}) \simeq (\mathbf{A}_{\mathfrak{P}})/\mathfrak{P}\mathbf{A}_{\mathfrak{P}}$.

This leads to some (huge) global objects in classical mathematics . . .

Other global objects related to prime ideals. 2

The rings

$$\prod_{\mathfrak{P}\in \mathrm{Spec}\,\mathbf{A}} \mathbf{A}/\mathfrak{P}\,, \qquad \prod_{\mathfrak{P}\in \mathrm{Spec}\,\mathbf{A}} \mathbf{A}_{\mathfrak{P}}, \qquad \prod_{\mathfrak{P}\in \mathrm{Spec}\,\mathbf{A}} \mathrm{K}_{\mathbf{A}}(\mathfrak{P}).$$

The modules

$$\bigoplus_{\mathfrak{P}\in \mathrm{Spec}\,\mathbf{A}} \mathbf{A}/\mathfrak{P}\,, \qquad \bigoplus_{\mathfrak{P}\in \mathrm{Spec}\,\mathbf{A}} \mathbf{A}_{\mathfrak{P}}, \qquad \bigoplus_{\mathfrak{P}\in \mathrm{Spec}\,\mathbf{A}} \mathrm{K}_{\mathbf{A}}(\mathfrak{P}).$$

All these objects are out of the scope of concrete constructions (except for some particular rings). But it is possible to construct global objects which are constructive substitutes to the above ones, in a purely algebraic way, defining them as solutions of "universal problems".

Other global objects related to prime ideals. 3

$$\prod_{\mathfrak{P}\in \operatorname{Spec}\mathbf{A}} \mathbf{A}/\mathfrak{P}$$

can be viewed as a completion of $\mathbf{A}_{\mathrm{pp}}$: the pp-ring generated by $\mathbf{A}$.

$$\prod_{\mathfrak{P}\in \operatorname{Spec}\mathbf{A}} \mathrm{K}_{\mathbf{A}}(\mathfrak{P})$$

can be viewed as a completion of $\mathbf{A}_{\mathrm{vNr}}$: the von Neuman regular ring generated by $\mathbf{A}$.

$$\prod_{\mathfrak{P}\in \operatorname{Spec}\mathbf{A}} \mathbf{A}_{\mathfrak{P}}$$

can be viewed as a completion of $\mathbf{A}_{\mathrm{dec}}$: the decomposable ring generated by $\mathbf{A}$.

Other global objects related to prime ideals. 4

pp-**ring**. Convenient generalisation of a domain in equational algebra, the annihilator of any element a is generated by an idempotent e_a.

von Neuman regular ring. Convenient generalisation of a field in equational algebra, any element a has a quasi-inverse b: $b(1-ab)=0$ and $a(1-ab)=0$.

decomposable ring. Convenient generalisation of a local ring in equational algebra, any element a is decomposable, i.e., it has a weak quasi-inverse b: $b(1-ab)=0$ and $a(1-ab)\in \mathrm{Rad}\mathbf{A}$.

Other global objects related to prime ideals. 5

Bourbaki uses the module $\boxed{\bigoplus_{\mathfrak{m}\in \mathrm{Max}\,\mathbf{A}} \mathbf{A}_{\mathfrak{m}}}$ in order to explain an abstract local global principle. They say: this module is faithfully flat.
(NB: when localising, maximal ideals are not better than ordinary prime ideals, so they could have used Spec $\mathbf{A}$ instead of Max $\mathbf{A}$).

A first deciphering of this abstract principle can be obtained by using the dynamical rereading philosophy: replace this module by the module $\bigoplus_{i=1}^{n} \mathbf{A}_{S_i}$, or by the ring $\prod_{i=1}^{n} \mathbf{A}_{S_i}$ where the S_i's $(i = 1, \ldots, n)$ are comaximal monoids that are "constructed" by the classical proof when it uses a localisation at an arbitrary maximal ideal.

Another possible deciphering should be to use $\mathbf{A}_{\mathrm{dec}}$ and to say: this ring extension is faithfully flat, and the classical proof using a localisation at an arbitrary prime ideal works as well for any decomposable ring.

Other global objects related to prime ideals. 6

Th. Coquand *On seminormality*, Journal of Algebra. **305** (2006), 585-602.

In the proof of Traverso-Swan theorem about seminormal rings, the main step is to prove the result for domains, using their quotient field.

For an arbitrary reduced ring, we have to go back to the case of a domain.

A simple argument in classical mathematics should be: embed the ring in the product $\prod_{\mathfrak{P}} \mathrm{K}_{\mathbf{A}}(\mathfrak{P})$, which will replace the missing fraction field (the total quotient ring doesn't work because it is not zero dimensional).

There are two ways of deciphering this classical trick. Either you reread dynamically "the product of all $\mathrm{K}_{\mathbf{A}}(\mathfrak{P})$", or you use $\mathbf{A}_{\mathrm{vNr}}$.

Elimination of primes.

Reasoning with a generic prime ideal in order to prove some concrete thing is something like: *in order to prove that a ring is trivial, show that it doesn't contain any prime ideal, or equivalently:*

"after localisation at a prime ideal the ring becomes trivial",

When rereading the classical proof you construct a finite tree by using the disjunctions

$$x \in \mathfrak{P} \quad \vee \quad x \notin \mathfrak{P}$$

At the leaves of the tree you get comaximal monoids S_i with $1 = 0$ in each localisation $\mathbf{A}_{S_i}$. This implies that $\mathbf{A}$ is trivial.

Elimination of primes. 2

Let us rewrite the same thing using logic.

First order theory: theory of
a commutative ring
$+$ an ideal I such that $I = \sqrt{I}$,
$+$ a multiplicative monoid U such that $U + I = U$.

Call $V(x)$ and $J(x)$ the predicates for $x \in U$ and $x \in I$.

(I, U) partial information about a prime ideal $\mathfrak{P}$.

Elimination of primes. 3

When you add the axioms

$$V(x) \vdash \exists y\, xy = 1 \quad \text{and} \quad \vdash V(x) \vee J(x)$$

you force the ring to be local.

Moreover if $1 = 0$ after adding these axioms, then $1 = 0$ before adding the axioms.

Adding the positive diagram of a ring $\mathbf{A}$, the minimal models are the localisations of $\mathbf{A}$ at any prime ideal.

If you are able to translate in this theory the classical proof that the ring becomes trivial after localisation at any prime, you get a constructive proof that the ring is trivial.

Elimination of minimal primes

Let us try to do the samething with minimal primes.

Reasoning with a generic minimal prime in order to prove some concrete thing is something like:
in order to prove that a ring is trivial, show that it doesn't contain any minimal prime ideal, or equivalently:

"after localisation at a minimal prime ideal the ring becomes trivial",

This cannot be captured by an argument using only first order logic:

Indeed, localising at a minimal prime gives a zero dimensional local ring. And a zero dimensional local ring is, up to nilpotent elements, a field.

Elimination of minimal primes. 2

So adding the positive diagram of a reduced ring $\mathbf{A}$, the minimal models are not:

the ring $\mathbf{A}$ *localised at a minimal prime ideal*, but

the field $\mathrm{K}_{\mathbf{A}}(\mathfrak{P})$ *for any prime ideal* $\mathfrak{P}$.

In order to capture the notion of minimal prime ideal you have to use an infinite disjunction (a disjunction over all elements of the ring: this is **not** captured by an existential quantifier!). svp un petit dessin

If $\mathfrak{F}$ is the corresponding maximal filter (complement of the minimal prime) here is the infinite disjunction

$$x \in \mathfrak{F} \quad \vee \quad \bigvee_{y \in \mathfrak{F}} xy \ nilpotent$$

Elimination of minimal primes. 3

T. Coquand. *Zariski Main Theorem.* Preprint (2007)

In this paper, T. Coquand gives a constructive proof of the celebrated Zariski Main Theorem in the generalised version due to Grothendieck.

The constructive proof is based on a classical abstract proof by Peskine.

A crucial non constructive step in the classical proof uses the localisation at a generic minimal prime in the ring $\mathbf{C} = \mathbf{A}/(\mathbf{A} : \mathbf{B})$ where $\mathbf{A} \subseteq \mathbf{B}$ in order to prove that $\mathbf{A} = \mathbf{B}$. Finding a contradiction when assuming the existence of a minimal prime shows that $\mathbf{C}$ is trivial, so $1 \in (\mathbf{A} : \mathbf{B})$ and $\mathbf{A} = \mathbf{B}$.

For rereading this proof in a constructive way there are two possibilities.

Elimination of minimal primes. 4

The first one is the dynamical rereading of the classical "proof by contradiction" showing that the reduced $\mathbf{C}$ is trivial since it doesn't have a minimal prime, i.e. it doesn't have a localisation which is a field.

In the infinite branching tree corresponding to the consideration of this generic minimal prime, we follow the computation in the proof by chosing always the branch "x invertible" (i.e. $x \in \mathfrak{F}$).

When the classical computation finds a "contradiction", i.e. $1 = 0$ in the ring $\mathbf{C}[1/(c_1 \dots c_k)]$ we are very happy: it is a positive information saying that $c_k = 0$ in $\mathbf{C}[1/(c_1 \dots c_{k-1})]$. We go back one step . . .

Elimination of minimal primes. 5

The second possible deciphering of the "localisation at an arbitrary minimal prime" uses a constructive substitute to the classical "mysterious" ring

$$\prod_{\mathfrak{P}\in \mathrm{Min}\,\mathbf{A}} \mathbf{A}_{\mathfrak{P}} \;\simeq\; \prod_{\mathfrak{P}\in \mathrm{Min}\,\mathbf{A}} \mathrm{K}_{\mathbf{A}}(\mathfrak{P}) \;\simeq\; \mathrm{Quot}\left(\prod_{\mathfrak{P}\in \mathrm{Min}\,\mathbf{A}} \mathbf{A}/\mathfrak{P}\right)$$

Elimination of minimal primes. 6

The constructive substitute of $\prod_{\mathfrak{P}\in \mathrm{Min}\,\mathbf{A}} \mathbf{A}/\mathfrak{P}$ is the ring $\mathbf{A}_{\min}$ obtained by inductive iteration of the following construction (where $a \in \mathbf{A}$)

$$(\mathbf{A}, a) \longmapsto \mathbf{A}/\mathrm{Ann}(a) \times \mathbf{A}/\mathrm{Ann}(\mathrm{Ann}(a))$$

The constructive substitute of $\prod_{\mathfrak{P}\in \mathrm{Min}\,\mathbf{A}} \mathbf{A}_{\mathfrak{P}}$ is $\mathrm{Quot}(\mathbf{A}_{\min})$ and can be obtained by inductive iteration of the following construction (where $a \in \mathbf{A}$)

$$(\mathbf{A}, a) \longmapsto \mathbf{A}/\mathrm{Ann}(a) \times \mathbf{A}[1/a]$$

Elimination of maximal primes

I. Yengui
Making the use of maximal ideals constructive.
Theoretical Computer Science, **392**, (2008) 174–178.

As for minimal primes, from a logical point of view, eliminating a (generic) maximal prime from an abstract reasoning seems *much more difficult* than eliminating a (generic) prime.

Reasoning with a generic maximal prime in order to prove some concrete thing is something like:
in order to prove that a ring is trivial, show that it doesn't contain any maximal ideal.

This cannot be captured by an argument using only first order logic.

Elimination of maximal primes. 2

In order to capture the notion of maximal ideal you have to use an infinite disjunction (a disjunction over all elements of the ring).

$$x \in \mathfrak{M} \quad \vee \quad \bigvee_{y \in R} 1 - xy \in \mathfrak{M}$$

svp un petit dessin

Idea: when rereading dynamically the proof follow systematically the branch $x_i \in \mathfrak{M}$ any time you find a disjunction $x \in \mathfrak{M} \ \vee \ x \notin \mathfrak{M}$ in the proof.

Once you get $1 = 0$ in the quotient, this means $1 \in \langle x_1, \ldots, x_k \rangle$, so this leaf has the good answer and moreover, at the node $\langle x_1, \ldots, x_{k-1} \rangle \subseteq \mathfrak{M}$ you know a concrete $a \in R$ such that $1 - ax_k \in \langle x_1, \ldots, x_{k-1} \rangle$.

Elimination of maximal primes. 3

So you can follow the proof.

If the proof given for a generic maximal ideal is sufficiently "uniform" you know a bound for the depth of the (infinite branching) tree. So your "branching dynamical evaluation" is finite: you get an algorithm.

Challenge:

1) Find the constructive substitute for the mysterious classical ring

$$\prod_{\mathfrak{P}\in \mathrm{Max}\,\mathbf{A}} \mathrm{K}_{\mathbf{A}}(\mathfrak{P}) \;\simeq\; \prod_{\mathfrak{P}\in \mathrm{Max}\,\mathbf{A}} \mathbf{A}/\mathfrak{P}$$

2) Use this global object instead of the dynamical search.

THE END