Concrete proofs with abstract objects

in modern algebra

Henri Lombardi
Université de Franche-Comté, Besançon, France

Oberwolfach, April 11, 2008

Mathematical Logic: Proof Theory, Constructive mathematics

Contents

• The computer algebra system D5, and Galois variation
• Local global principles, Zariski spectrum, other global objects
• Elimination of minimal primes
• Elimination of maximal primes

Printable version of these slides:
Slides:

The computer algebra system D5

Classical Theorem. Any field \( K \) is contained in an algebraically closed field.

Recursive counter example. It is possible to construct a computable field \( K \supseteq \mathbb{Q} \) 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 \( K[X] \) there exists a field \( L \supseteq K \) where \( f \) has at least one root.

The computer algebra system D5. 2

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.
In classical mathematics, two algebraic closures of a field $K$ 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.

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

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

The field $L$ is represented by the universal splitting algebra $A$ of the polynomial, with “Galois group” $S_n$. Possibly the computations inside $L$ 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 $S_n$ by a convenient subgroup.

I.e., we improve step by step our knowledge of $L$ 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 $x_3$).

The isomorphism theorem becomes:

If two computations lead to two Galois quotients $L_1$ and $L_2$ of $A$, then there exists a third one, $L_3$ such that $L_1 \simeq L_3^r$ and $L_2 \simeq L_3^s$.

The two distinct informations about $L$ can be glued together!

Very simple: our dynamical computations are safe!  

**Proof of this fact?** The universal splitting algebra $A$ exists, with “Galois group” $S_n$! (which is based on Euclidean division).

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

Constructively we only know successive approximations of $L$ and $G$.

When dealing with all the roots of a given polynomial, the global concrete object (equality being constructed through the computations) is a better approach than the “naive” D5 (no duplicated computations).
Although we compute in a reliable way inside $L$, our decomposition field $L$ 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 motto in abstract algebra:

\begin{center}
\begin{minipage}{0.45\textwidth}
\textit{in order to get a concrete result when dealing with a commutative ring see what happens after localization at an arbitrary prime.}
\end{minipage}
\end{center}

“Localizing at an arbitrary prime” has the following concrete content:

\begin{center}
\begin{minipage}{0.45\textwidth}
\textit{consider the same (rigid) structure, but add the axioms of local rings, you get a (non-rigid) dynamical structure, and you see what happens.}
\end{minipage}
\end{center}

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 $\text{Spec } A$”, 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 $A$ with the basic opens

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

However, even if the ring $A$ 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 $A$ is a map $D : A \to L$ in a distributive lattice $L$ satisfying the conditions

\[
D(0) = 0 \quad D(1) = 1 \quad D(ab) = D(a) \land D(b) \quad D(a + b) \leq D(a) \lor D(b)
\]

The Zariski spectrum can then be defined as the free support on $A$

**Zariski spectrum. 3**

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

**Theorem:** $D(a) \leq D(b_1) \lor \cdots \lor D(b_n)$ 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. $D(a)$: finite piece of information about a prime ideal.

L. Español. *Constructive Krull dimension of lattices.*

L. Español. *Dimension of Boolean valued lattices and rings.*


T. Coquand, H. Lombardi, M.-F. Roy.
*An elementary characterisation of Krull dimension*

---

The pointfree version of Zar $A$ 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 assumptions concerning the Krull dimension.

---

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*

---


---

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

$$\operatorname{Rad}(A) \overset{\text{def}}{=} \bigcap_{m \in \operatorname{Max}(A)} m = \{ x \in A \mid 1 + x A \subseteq A^x \} = \{ x \mid \langle x, z \rangle = \langle 1 \rangle \Rightarrow \langle z \rangle = \langle 1 \rangle \}$$

In addition

$$\bigcap_{m \in \operatorname{Max}(A)} (A \setminus m) = A^x.$$
Minimal prime ideals are the prime ideals \( p \) such that \( A_p \) is zero dimensional. In general, these ideal objects are not reachable from a constructive point of view, but their intersection is!

\[
\bigcap_{p \in \text{Min}(A)} p = \sqrt{(0)} = D_A(0) = \{ x \in A \mid \exists n \ x^n = 0 \}
\]

In addition

\[
\bigcap_{p \in \text{Min}(A)} (A \setminus p) = \{ a \in A \mid \forall y \in A \ (0 = D_A(ay) \Rightarrow 0 = D_A(y)) \}.
\]

Other global objects related to prime ideals

A prime ideal \( \mathfrak{p} \subseteq A \) can be used in classical algebra in three different ways.

1. Constructing the quotient \( A/\mathfrak{p} \), which is a \textit{domain}.
2. Constructing the localisation \( A_\mathfrak{p} \), which is a \textit{local ring}.
3. Constructing the \textit{field} \( K_A(\mathfrak{p}) = \text{Quot}(A/\mathfrak{p}) \simeq (A_\mathfrak{p})/\mathfrak{p}A_\mathfrak{p} \).

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

Other global objects related to prime ideals. 2

The rings

\[
\prod_{\mathfrak{p} \in \text{Spec} A} A/\mathfrak{p}, \quad \prod_{\mathfrak{p} \in \text{Spec} A} A_\mathfrak{p}, \quad \prod_{\mathfrak{p} \in \text{Spec} A} K_A(\mathfrak{p}).
\]

The modules

\[
\bigoplus_{\mathfrak{p} \in \text{Spec} A} A/\mathfrak{p}, \quad \bigoplus_{\mathfrak{p} \in \text{Spec} A} A_\mathfrak{p}, \quad \bigoplus_{\mathfrak{p} \in \text{Spec} A} K_A(\mathfrak{p}).
\]

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

\[
\prod_{\mathfrak{p} \in \text{Spec} A} A/\mathfrak{p}
\]

can be viewed as a completion of \( A_{pp} \): the \textit{pp-ring} generated by \( A \).

\[
\prod_{\mathfrak{p} \in \text{Spec} A} K_A(\mathfrak{p})
\]

can be viewed as a completion of \( A_{vNr} \): the von Neuman regular ring generated by \( A \).

\[
\prod_{\mathfrak{p} \in \text{Spec} A} A_\mathfrak{p}
\]

can be viewed as a completion of \( A_{dec} \): the decomposable ring generated by \( A \).

Other global objects related to prime ideals. 4

\textit{pp-ring}. Convenient generalisation of a domain in equational algebra, the annihilator of any element \( a \) is generated by an idempotent \( e_a \).

\textit{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 \( a(1-ab) = 0 \).

\textit{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 \( a(1-ab) \in \text{Rad}A \).
Bourbaki uses the module $\bigoplus_{m \in \text{Max } A} A_m$ 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 $\text{Spec } A$ instead of $\text{Max } A$).

A first deciphering of this abstract principle can be obtained by using the dynamical rereading philosophy: replace this module by the module $\bigoplus_{i=1}^n A_{S_i}$, or by the ring $\prod_{i=1}^n A_{S_i}$ 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 $A_{\text{dec}}$ 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.


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 $\prod_{P} K_A(P)$, 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 $K_A(P)$”, or you use $A_{\text{vNr}}$.

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

$$x \in \mathfrak{P} \lor x \notin \mathfrak{P}$$

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

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 $\mathfrak{P}$.

When you add the axioms

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

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 $A$, the minimal models are the localisations of $A$ 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.

Let us try to do the something 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.

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

- the ring $A$ localised at a minimal prime ideal, but
- the field $K_A(\mathcal{P})$ for any prime ideal $\mathcal{P}$.

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!).

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

$$x \in \mathcal{F} \lor \bigvee_{y \in \mathcal{F}} xy \text{ nilpotent}$$


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 $C = A/(A : B)$ where $A \subseteq B$ in order to prove that $A = B$. Finding a contradiction when assuming the existence of a minimal prime shows that $C$ is trivial, so $1 \in (A : B)$ and $A = B$.

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

The first one is the dynamical rereading of the classical “proof by contradiction” showing that the reduced $C$ 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 choosing always the branch “$x$ invertible” (i.e. $x \in \mathcal{F}$).

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

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

$$\prod_{\mathcal{P} \in \text{Min } A} A_{\mathcal{P}} \simeq \prod_{\mathcal{P} \in \text{Min } A} K_A(\mathcal{P}) \simeq \text{Quot} \left( \prod_{\mathcal{P} \in \text{Min } A} A_{\mathcal{P}} \right)$$

The constructive substitute of $\prod_{\mathcal{P} \in \text{Min } A} A_{\mathcal{P}}$ is the ring $A_{\text{min}}$ obtained by inductive iteration of the following construction (where $a \in A$)

$$(A, a) \mapsto A/\text{Ann}(a) \times A/\text{Ann}(\text{Ann}(a))$$

The constructive substitute of $\prod_{\mathcal{P} \in \text{Min } A} A_{\mathcal{P}}$ is $\text{Quot}(A_{\text{min}})$ and can be obtained by inductive iteration of the following construction (where $a \in A$)

$$(A, a) \mapsto A/\text{Ann}(a) \times A[1/a]$$
Elimination of maximal primes

I. Yengui

Making the use of maximal ideals constructive.


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.

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

\[ x \in \mathfrak{M} \lor \bigvee_{y \in R} 1 - xy \in \mathfrak{M} \]

Idea: when rereading dynamically the proof follow systematically the branch \( x_i \in \mathfrak{M} \) any time you find a disjunction \( x \in \mathfrak{M} \lor x \not\in \mathfrak{M} \) in the proof.

Once you get \( 1 = 0 \) in the quotient, this means \( 1 \in (x_1, \ldots, x_k) \), 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 \( 1 - ax_k \in \langle x_1, \ldots, x_{k-1} \rangle \).

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

\[ \prod_{P \in \text{Max}_A} K_A(P) \simeq \prod_{P \in \text{Max}_A} A/P \]

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

THE END