Constructive Algebra

Thierry Coquand

September 2010
This course

An introduction to constructive algebra, as developed by F. Richman, H. Lombardi, P. Schuster, I. Yengui, ... but also Kronecker, H. Edwards

The first lecture will consist of some historical and logical remarks, and a presentation of some examples that will be analyzed in following lectures
This course

Lecture 2: coherent rings
Lecture 3: prime ideals and Zariski spectrum
Lecture 4: algebraically closed fields
Lecture 5: constructive homological algebra
The word *algebra* comes from the title of a book *Hibab al-jabr wal-muqubala* (around 825)

The word *algorithm* comes from the name of the author of this book *Al-Khwarizmi*

Until 1800 most works in algebra are presenting clever computations

Example: elimination theory (Bezout, Poisson), Lagrange
Some history

The situation changes with Gauss, Abel, Galois

Concept of *irreducible* polynomial: Gauss (cyclotomic polynomial), fundamental notion for Abel and Galois

Construction of the splitting field of a polynomial (very interesting from the constructive/logical point of view. The importance of this problem has been stressed by H. Edwards)

Rational functions of given quantities (which will become *domain of rationality* for Kronecker, and later our notion of field, introduced by Dedekind)
Some history

The proofs still have a direct algorithmic interpretation, though Galois insists on the *ideal* character of these computations.

"If now, you give me an equation that you have in any way you like and you want to know whether it is or not solvable by radicals, I have nothing to do but to indicate to you the way to reply to the question, but without to obliging either myself or anyone else to do so. In other word, the calculations are impracticable."
The connection between reasoning and algorithms became then less and less clear.

Typical example: different versions that Dedekind will give to his theory of ideals


Other typical example: all ideals of $K[X_1, \ldots, X_n]$ are of finite type (Hilbert’s basis theorem)

Noetherian: all ideals are of finite type
Dedekind domains

There are now described as: Noetherian integrally closed domain where any nonzero prime ideal is maximal

But a lot of important and computational properties of Dedekind domains are best captured without the Noetherian hypothesis (Prüfer domain)

For instance the fact that the intersection of two finitely generated ideals is finitely generated in a Dedekind domain corresponds to a nice algorithm (fundamental for Dedekind) which is hidden if we use the notion of Noetherian ring
We have lost the direct connection between reasoning and computing.

It may be that, from a proof of an existence statement in mathematics, it is *not possible* to extract from it a computation of the witness the existence of which is claimed by this statement.

Where does this non-effectiveness come from?

Two aspects: the objects/sets we manipulate and the logic we use to reason about these objects.
Constructive objects

Example: symbols, natural numbers, integers, rational numbers, formulae, matrices, rational polynomials

They can be coded as natural numbers, but it is convenient to work with the general notion of constructive objects

*Constructive objects derive their importance from the fact that they are the only objects which we can communicate to each other in complete detail*

Martin-Löf, *Notes on constructive mathematics*

*Abstract objects*: function, well-founded tree, real number, set
Constructive objects

This notion of constructive object is essential, but is usually not made explicit.

For instance, is \( \mathbb{Z} \) Noetherian, in the sense that for any ideal \( I \subseteq \mathbb{Z} \) we can find a finite set \( G \) of generators?

The input \( I \) is abstract, the output \( G \) is a concrete object.

No way to compute \( G \) from \( I \) if for instance \( I \) is \( \{0\} \cup \{n \in \mathbb{Z} \mid P\} \) where \( P \) is some undecided proposition.
What is a set in constructive mathematics?

A set is defined when we describe how to construct its members and describe what it means for two members of $S$ to be equal.

Example of sets: $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ and $k[X]$, $k[[X]]$, $k((X))$

A set is discrete iff one can decide the equality; $\mathbb{N}$, $\mathbb{Q}$ are discrete sets but $k[[X]]$ and $k((X))$ are not.

A set of concrete objects is discrete (the converse is not valid).
Rings and fields

The usual view of a ring $R$ is that it is a set with two functions on it.

In set theory, a function is a *functional relation*.

It may have no computational meaning.

$$\forall x. \exists! y. R(x, y)$$
“Explicitely given” ring and field

“Its elements are uniquely represented by distinguishable symbols with which addition, substraction, multiplication and division can be performed in a finite number of operations” (van der Waerden)

Explicitely given implies discrete

Example: if the field $k$ is explicitely given, then so is the field $k(X)$
Excluded-Middle, a simple example

**Proposition:** If $K$ is a field and $P$ is a non constant polynomial in $K[X]$ there exists $Q$ in $K[X]$ such that $Q$ is irreducible and $Q$ divides $P$

The classical proof claims the existence of such a polynomial $Q$ but it cannot gives an algorithm for finding $Q$
Constructive algebra

**Proposition:** There is no irreducibility test for $k[X]$ even if $k$ is discrete

Let $P$ be an arbitrary proposition and $k$ be the field

$$\mathbb{Q} \cup \{ z \in \mathbb{Q}[i] \mid P \}$$

Intuitively $k$ is in between $\mathbb{Q}$ and $\mathbb{Q}[i]$ but we cannot decide where. The field $k$ is *discrete*.

$X^2 + 1$ is reducible over $k[X]$ iff $P$ holds. So we cannot hope to decide the reducibility of $X^2 + 1$
For some special discrete field $k$ there is such a test

Kronecker gives a test in the case $k = \mathbb{Q}(X_1, \ldots, X_n)$ or for algebraic extensions of such field. See H. Edwards’ *Essays in Constructive Mathematics* or van der Waerden *Modern Algebra*

In Kronecker’s approach/Edwards’ book, such an irreducibility test plays a fundamental role

We present a different approach in this course
Excluded-Middle

What this example illustrates is that it is the law of Excluded-Middle

$$(\forall x. \neg \psi(x)) \lor \exists x. \psi(x)$$

which is the cause of the non effectiveness of mathematical arguments and the lack of direct connection between reasoning and computation

This has been noticed explicitly first by Brouwer (and probably Hilbert was already aware of this point)

Not at all obvious when Brouwer made this remark since at the time people thought about the Axiom of Choice as the source of non effectivity in mathematics
Constructive mathematics is best characterised as mathematics developed using intuitionistic logic (logic without excluded middle).

Notice that this characterization does not mention the notion of computable function, Turing machine, ...
This gives a purely *logical* characterisation of constructive algebra.

Mathematics is more than logic, we need some sort of set theory.

Two research directions:

- Type theory, non set-theoretic foundation, direct connection with programming, a new very general formulation of the axiom of extensionality (Voevodsky).

- Constructive set theory, constructive reformulation of forcing, large cardinals, ...
Axiom of Choice

The axiom of choice can be stated as the fact that any surjective map has a section.

This is not valid constructively:

\[ \{ -1, 0, 1 \}^\mathbb{N} \to [-1, 1] \]

\[ (b_n) \mapsto \sum b_n / 2^n \]

This is a surjective map, but it has no continuous section.
Axiom of Choice and Excluded Middle

**Theorem:** \( AC \rightarrow EM \)

where \( AC \) is the Axiom of Choice and \( EM \) is the law of Excluded-Middle
Axiom of Choice and Excluded Middle

Let $X$ be a set and $\sim$ be an equivalence relation on $X$

We write $Y = X/\sim$ and $\varphi : X \to Y$, $a \mapsto [a]$ the canonical surjection

**Lemma:** If $\varphi$ has a section $\psi$ and $X$ is discrete then $\sim$ is decidable (and $Y$ is discrete as well)

Indeed

$$a_1 \sim a_2 \iff [a_1] =_Y [a_2] \iff \psi([a_1]) =_X \psi([a_2])$$
Axiom of Choice and Excluded Middle

In particular, $N_2 = \{0, 1\}$ is a discrete set.

Let $P$ be an arbitrary proposition, and define $a \sim_P b$ by $P \lor a = b$.

$\sim_P$ is an equivalence relation.

If the axiom of choice holds, then $\sim_P$ is decidable and so we have $P \lor \neg P$. 
Because of this, if we want a connection between reasoning and computation we cannot use Zorn’s Lemma

So it seems that we have to develop algebra without using

- Prime ideals, maximal ideals, minimal prime ideals
- Noetherianity
- Excluded-Middle

How is it possible to develop algebra without these tools? Several effective/concrete properties are proved using these non effective notions
Let $R$ be a ring. We say that $a_0, \ldots, a_n$ is unimodular iff $\langle a_0, \ldots, a_n \rangle = 1$

We say that $\Sigma a_i X^i$ is primitive iff $a_0, \ldots, a_n$ is unimodular

**Theorem:** The product of two primitive polynomials is primitive

**Lemma:** A sequence $a_0, \ldots, a_n$ is unimodular iff it is not zero modulo any prime ideal

**Lemma:** If $R$ is an integral domain then so is $R[X]$
Use of prime ideals

The statement proved is something “concrete”: if we have two relations

\[ \sum a_i u_i = 1 \quad \sum b_j v_j = 1 \]

and we define \( c_k = \sum_{i+j=k} a_i b_j \) then we can find \((w_k)\) such that

\[ \sum c_k w_k = 1 \]

Because the use of Zorn’s Lemma and Excluded Middle, it is not so clear how we can compute \((w_k)\).
Classically one defines \( J \subseteq R \) as the intersection of all maximal ideals of \( R \).

One can prove \( x \in J \iff \forall z. \text{inv}(1 - xz) \) where \( \text{inv}(u) \equiv \exists y. uy = 1 \), using Zorn’s Lemma.

It follows that we have

\[
\forall z. \text{inv}(1 - uz) \land \forall z. \text{inv}(1 - vz) \rightarrow \forall z. \text{inv}(1 - (u + v)z)
\]
Algebraic closure

First step for building the algebraic closure: existence of a splitting field

Let $P$ be a polynomial in $k[X]$, how to build an extension $L$ of $k$ in which $P$ can be decomposed in linear factors

The usual argument relies on taking an irreducible factor of $P$!

So it is difficult to build a splitting field for $X^2 + 1$, without deciding whether $X^2 + 1$ has a root in $k$ or not
We say that $a$ in $R$ is regular iff $ax = 0 \rightarrow x = 0$

An ideal $I$ is regular iff $xI = 0 \rightarrow x = 0$

**Theorem:** A regular finitely generated ideal contains a regular element if the ring $R$ is Noetherian

Kaplansky (commutative rings) states that this is “a result that is among the most useful in the theory of commutative rings”

The result may not hold if $R$ is not Noetherian
Serre's problem (Quillen-Suslin's Theorem)

**Theorem**: An idempotent matrix over a polynomial ring is similar to a canonical projection matrix of the form $I_{r,n} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$

Given such a matrix $M$ satisfying $M^2 = I_n$ we can find an invertible matrix $P$ such that $PMP^{-1} = I_{r,n}$

The proof by Suslin uses a maximal ideal. Does this proof indicate a way to compute the matrix $P$ given $M$?
Non constructive reasoning

Non effective reasoning is used often to prove existence of concrete objects satisfying a decidable property

Is the use of non effective reasoning essential in some cases?

Can we always “extract” from a non effective reasoning its “computational content” and provide a constructive explanation of this reasoning?
Non constructive reasoning

Hilbert’s program: if we can show some concrete statements by non effective reasoning, then there is a concrete/simple direct argument

Gödel has shown that this is not valid for arithmetic

For algebra?
Help from logic: Logical complexity

1 equational logic: theory of rings

2 (first-order) logic: theory of fields

3 higher-order logic: to be Noetherian
Logical complexity

Noetherian: all ideals are finitely generated

This involves a quantification over all *subsets* of the ring

First-order: we quantify only over the elements of the ring
Logical complexity

There is *no* completeness theorem for higher-order logic (Gödel)

For first-order logic, as shown by Skolem and Gödel there is a completeness theorem (however the proof is not constructive)

Most notions in algebra can be captured by first-order logic
Completeness Theorem for first-order logic plays an important heuristic role in our presentation of constructive algebra.

*If a result expressed in first-order logic is semantically valid then it can be proved in first-order logic.*

This is a remarkable result, which can be seen as a partial realisation of Hilbert’s Program.

We can replace *semantics* by *syntax*.
Summary

The source of non-effectivity in mathematical arguments is the law of Excluded-Middle.

Intuitionistic logic is logic without using the law of excluded-middle. Any argument in intuitionistic logic has a direct computational interpretation.

Completeness holds for first-order logic (and holds constructively for coherent logic). There is no completeness for higher-order logic. Several notions in algebra are naturally expressed in first-order logic.

How can one develop algebra without prime ideals, maximal ideals, Noetherianity?