Constructive algebra

Thierry Coquand

May 2018

Constructive Algebra

Constructive algebra is algebra done in the context of intuitionistic logic

Constructive Algebra

H. Lombardi, C. Quitté *Commutative Algebra: Constructive Methods*, 2016

I. Yengui *Constructive Commutative Algebra*, 2017

R. Mines, F. Richman, W. Ruitenburg *A course in constructive algebra*, 1988

Constructive Algebra

(1) Connection with logic and Hilbert's program

Use of non effective methods, “ideal” methods to prove “concrete” statements

Hilbert's program seems to work on actual examples in algebra

Statements in *algebra* often have a simple logical form

Constructive Algebra

(2) Topos theory and sheaf models

Leray-Cartan (ca.1950), Beth (1956), Kripke (1958), Grothendieck (ca.1960)

Logic of topos $=$ intuitionistic logic

Interesting algorithms, connected to sheaf models, e.g. Gröbner basis computation for $\mathbb{Z}[X_1, \dots, X_n]$ (I. Yengui) connected to the notion of "dynamical" computations (D. Duval)

Constructive Algebra

In a parallel universe, mathematicians have not found out that they can use excluded middle as a proof method in algebra

They put the emphasis on simple (definable in a first-order way) structures

-l-groups (F. Riesz, Lorenzen, Prüfer, Stone)

-Prüfer domains (more fundamental than Dedekind domain: finitely generated ideals are invertible)

Fundamental notions, such as the Zariski *spectrum* of a ring, are defined using notions of universal algebra

Ideal methods, Ex. 1

The intersection of all *prime* ideals is the set of nilpotent elements

Hence if $x^2 = 0$ and $y^3 = 0$ we should be able to find n such that $(x+y)^n = 0$

$\mathbb{Z}[X,Y]/\langle X^2, Y^3\rangle$ we have n such that $(X+Y)^n \in \langle X^2, Y^3\rangle$

Ideal methods, Ex. 2

The intersection of all *maximal* ideals

$J(x)$ defined as $\forall y \; inv(1-xy)$

This is defined in a first-order way

We should be able to prove $J(x) \wedge J(y) \rightarrow J(x+y)$ in the theory of rings

Completeness Theorem!

Furthermore, the proof can be done in intuitionistic logic (coherent fragment)!

Use of prime ideals

This example will motivate the point-free presentation of *Zariski spectrum* and the *structure sheaf* of a ring

Let R be a ring. We say that a polynomial $a_0 + \cdots + a_n X^n$ is *primitive* iff $\langle a_0, \ldots, a_n \rangle = 1$

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

Use of prime ideals

Lemma: *A polynomial is primitive iff it is not zero modulo any prime ideal*

Lemma: *If R is an integral domain then $R[X]$ is an integral domain*

Integral domain: the product of two non zero element is non zero

Product of primitive polynomials

$$P = a_0 + a_1 X \qquad Q = b_0 + b_1 X \qquad R = c_0 + c_1 X + x_2 X^2$$

$$c_0 = a_0 b_0 \qquad c_1 = a_0 b_1 + a_1 b_0 \qquad c_2 = a_1 b_1$$

By completeness theorem, in the theory of rings (equational theory) we can show the implication

$$a_0 x_0 + a_1 x_1 = 1 \quad \wedge \quad b_0 y_0 + b_1 y_1 = 1 \ \rightarrow$$

$$\exists z_0 \ z_1 \ z_2 . \ a_0 b_0 z_0 + (a_0 b_1 + a_1 b_0) z_1 + a_1 b_1 z_2 = 1$$

Hence we should be able to find explicitly z_0, z_1, z_2 (as polynomials in the input parameters)

Prime ideals

Recall the definition of the Zariski spectrum of a ring R!

Space of all prime ideals, with basic open $D(a)$ for a in R

We can look at the distributive lattice of compact open

If $D(a) = 0$ then a is nilpotent

This lattice satisfies the relations

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

Support of a ring

Let $D : R \to L$ be a *support*, L distributive lattice, if we have

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

A. Joyal had the idea of redefining the Zariski spectrum as the *universal* support

This is abstract algebra, and an effective (and simple) definition

Support of a ring

If R is a local ring and $1 \neq 0$ then $D(a) = inv(a)$ is a support

If $inv(a+b)$ then $inv(a)$ or $inv(b)$

For instance $\mathbb{R}$ is a local ring (not a discrete field), $inv(a)$ is the same as $a\#0$

$D(ab) = D(a) \wedge D(b)$ means $ab\#0$ iff $a\#0$ *and* $b\#0$

In particular $a^2\#0$ iff $a\#0$

Other example: $R = k[[X]]$ and $D(a_0 + a_1X + \dots)$ is $\exists n \; a_n \neq 0$

Support of a ring

We write $D(a_1,\dots,a_n) = D(a_1) \vee \cdots \vee D(a_n)$ so that the last relation can be written $D(a+b) \leqslant D(a,b)$

We have $D(a^2) = D(a^3) = \cdots = D(a)$ and $D(a) = 0$ if a is nilpotent

All elements of the lattice are of the form $D(a_1,\dots,a_n)$

In general we don't have $D(a,b) = D(a+b)$ only $D(a+b) \leqslant D(a,b)$

We have $D(a,b) = D(a{+}b)$ if $D(ab) = 0$ and in general $D(a,b) = D(a{+}b, ab)$

Also $D(a,b,c) = D(a+b+c, ab+bc+ca, abc)$

Support

If $D : R \to L$ we can define the (abstract) content of a polynomial as $c(a_0 + \cdots + a_n X^n) = D(a_0, \ldots, a_n)$

Theorem: (Gauss-Joyal) $c(PQ) = c(P) \wedge c(Q)$

We think of $D : R \to L$ as a L-valued predicate (sheaf model)

In this sense R becomes an integral domain

Boolean algebra

If L is a distributive lattice we build the free Boolean algebra over L

How to add freely a complement of a

$L_a = L/\langle a\rangle \times L[1/a]$

$L \to L_a$ embedding and isomorphism iff a has a complement in L

We have $(L_a)_b = (L_b)_a = L_{a,b}$

Inductive limit of all $L_{a_1,\dots,a_n}$ is free Boolean algebra over L

Constructible topology

So if we have a support $D : R \to L$ we can compose with $L \to B$

B free Boolean algebra over L

We get a Boolean valued model and if we interpret $D(a)$ as $a \neq 0$ we can reason exactly like classically for an integral domain

We get Gauss-Joyal's result $c(PQ) = c(P) \wedge c(Q)$!

Logical interpretation

"Lattice-valued" model: the predicate $a \longmapsto D(a)$ is a predicate on the ring R with values in the Zariski lattice

This predicate defines a prime filter on the ring

This is a generic prime filter. This prime filter exists, but in a forcing extension/sheaf model over the Zariski spectrum

Zariski lattice

All this can be derived from the relations, but we did not use that the lattice is *generated* by these relations

We have to show that if $D(a_1,\dots,a_n) = 1$ holds then $a_0,\dots,a_n$ is unimodular

Zariski lattice

Theorem: *We have* $D(a) \leqslant D(b_1, \ldots, b_m)$ *iff* a *is in the radical of the ideal generated by* $b_1, \ldots, b_m$. *In particular* $D(a_1, \ldots, a_n) = 1$ *iff* $a_1, \ldots, a_n$ *is unimodular*

If I is an ideal the *radical* $\sqrt{I}$ of I is the set of elements a that have a power in I i.e. $\{a \in R \mid (\exists N)\ a^N \in I\}$

The *formal Nullstellensatz* states precisely that this lattice will coincide with the lattice of compact open subsets of the Zariski spectrum

Zariski lattice

For proving the Theorem, we give a *realization* of the Zariski lattice, by interpreting $D(a_1, \dots, a_n)$ as the radical of the ideal $\langle a_1, \dots, a_n \rangle$

Clearly if $a^N = b_1 v_1 + \cdots + b_m v_m$ then we have $D(a) \leqslant D(b_1, \dots, b_m)$

The theorem can be seen as a kind of normal form for proofs: any proof of $D(a) \leqslant D(b_1, \dots, b_m)$ is given by an algebraic equality $a^N = b_1 v_1 + \cdots + b_m v_m$

Zariski lattice

The key fact is that the cut rule

$D(a) \wedge D(b) \leqslant D(b_1, \dots, b_m)$

$D(a) \leqslant D(b_1, \dots, b_m, b)$

imply $D(a) \leqslant D(b_1, \dots, b_m)$

is satisfied

If ab is nilpotent and a nilpotent mod. $\langle b \rangle$ then a nilpotent

Application 1: Primitive polynomials

In particular, if both $P = \Sigma a_i X^i$ and $Q = \Sigma b_j X^j$ are primitive we have

$$D(a_0, \dots, a_n) = D(b_0, \dots, b_m) = 1$$

and so, by Gauss-Joyal if $\Sigma c_k X^k = PQ$ then

$$D(c_0, \dots, c_l) = 1$$

We get an elementary proof that the product two primitive polynomials is primitive, which corresponds to the non effective argument

Application 2: nilpotent elements

For a to be nilpotent can be rewritten $D(a) = 0$

We have $D(a+b) \leqslant D(a) \vee D(b)$

If $D(a) \leqslant 0$ and $D(b) \leqslant 0$ by two cuts we get

$D(a+b) \leqslant 0$

in the lattice of radical ideals

Use of prime ideals

It can be shown that, even if the ring is given effectively, it is not possible in general to define effectively a prime ideal on this ring

Lawvere (ICM 1970) conjectured the existence of a prime filter for any non trivial ring in an arbitrary topos. Joyal built topos where a ring does not have any prime filter

This indicates that we cannot follow naively the previous proof in an effective context or in an arbitrary topos

Use of prime ideals

In the previous argument, we use a prime filter in a generic way

We use a method similar the one of forcing in set theory, to "force" the existence of a generic prime ideal

Though we cannot describe the points of this space effectively in general, we can describe the topology of the space effectively

We give a direct effective description of this lattice

Logical interpretation

There is always a generic prime filter of this formal space, in a sheaf model (introduction), and we can then eliminate the use of this prime filter

This is a possible interpretation of Hilbert's method of introduction and elimination of ideal elements

Point-free spaces/locales

We can see the universal support $D : R \to L$ as a *point-free* description of the Zariski spectrum of R

We describe only the distributive lattice of compact open

We don't see this as an "actual" set of points

Point-free spaces/locales

Basis of the topology: open $D(a)$ closed by intersection $D(ab) = D(a) \wedge D(b)$

We have a canonical *sheaf* on this space

$F_R(D(a)) = R[1/a]$

We can check the sheaf condition

Clear if R is a domain

In this sheaf model, F_R is a *local* ring

F_R is the *structure sheaf* of the ring R

Point-free spaces/locales

A *valuation* domain is a domain such that $a|b$ or $b|a$

In a valuation domain, divisibility is linear

A *Prüfer* domain is a domain such that F_R is a valuation domain

Given a and b "locally" we have $a|b$ or $b|a$

Structure sheaf on $\mathbb{Z}$

For instance $\mathbb{Z}$ as a sheaf becomes a valuation domain

Over $\mathbb{Z}[X_1,\dots,X_n]$ we have a membership problem

$P \in \langle Q_1,\dots,Q_m\rangle$?

If this holds over $\mathbb{Z}[1/2]$ and $\mathbb{Z}[1/3]$ then it holds over $\mathbb{Z}$

Use Bezout identity between 2^n and 3^m to glue solutions: “local-global” principle

Finding the right structures

What I learnt was: if R is a *unique factorisation domain* then so is $R[X]$

So if k is a field, $k[X_1, \dots, X_n]$ should be a unique factorisation domain

But if k is a discrete field, $k[X]$ is *not* effectively a factorial domain

What I should have learnt instead is: if R is a *gcd domain* then so is $R[X]$

Furthermore, underlying the theory of gcd domain, we have the fundamental notion of l-group

l-group and ordered cancellative monoid

Let G be an ordered group (we have $x + z \leqslant y + z$ if $x \leqslant y$)

Definition G *is a* l*-group if any two elements have an inf*

Can be presented in an equational way we equations $z+(x\wedge y) = (z+x)\wedge(z+y)$

Then any two elements have a sup (fundamental relation)

$$x \vee y + x \wedge y = x + y$$

Thus any l-group is a lattice

l-group and ordered cancellative monoid

If R is a gcd domain that $R^{\times}$ is an ordered cancellative monoid and $K^{\times}$ has a canonical l-group structure $K =$ fraction field of R

We define $x \perp y$ if $x \wedge y = 0$

Lemma: (Euclide's Lemma) *If* $x \perp z$ *and* $x \leqslant y + z$ *then* $x \leqslant y$

Corollary: (Ex.) *If* $0 \leqslant 2x$ *then* $0 \leqslant x$

Thus in a gcd domain if $x^2|y^2$ then $x|y$

Proposition: (Ex.) *The lattice structure of a* l*-group is* distributive

l-group and ordered cancellative monoid

In any l-group we can define $a^+ = a \vee 0$ and $a^- = (-a) \vee 0$

We have $a = a^+ - a^-$

Lemma: $a^+ \perp a^-$

Lemma: *If* $x = a - b$ *and* $a \perp b$ *then* $a = x^+$ *and* $b = x^-$

Corollary: *For any* $n \geqslant 0$ *we have* $nx^+ = (nx)^+$ *and* $nx^- = (nx)^-$

Gcd domain

Theorem: *If R is a gcd domain then so is $R[X]$*

Key Lemma: if P in $R[X]$ define $c(P)$ $=$ gcd of the coefficients of P

Lemma: $c(PQ) = 1$ *if* $c(P) = c(Q) = 1$ *and in general* $c(PQ) = c(P)c(Q)$

For an elegant proof see Mines, Richman, Ruitenburg

We are going to see another proof of this result

In particular this gives an algorithm for computing gcd in $k[X_1, \dots, X_n]$

Alternative algorithm using homological algebra (last lecture)

Gcd domain

The notion of gcd domain is first-order

The notion of unique factorisation domain is logically much more complex

Application 2: GCD domain

Theorem: *If R is a GCD domain then so is $R[X]$*

The Noetherian version of this theorem is that $R[X]$ is UFD if R is UFD

The main Lemma is that if the GCD of the coefficients of $\Sigma a_i X^i$ is 1 and the GCD of the coefficients of $\Sigma b_j X^j$ is 1 then so is the GCD of the coefficients of the product $\Sigma c_k X^K$

This follows from Gauss-Joyal since we have N such that if u divides all c_k then it divides all $a_i^N b_j^N$

Lemma: *In a GCD domain if an element is relatively prime to two elements then it is relatively prime to their product*

Chevalley Theorem and quantifier elimination

The map $B(R) \rightarrow B(R[X])$ has an *adjoint* which defines an existential quantifier

The projection of $V(aX - 1)$ is $D(a)$ (read $V(r)$ as $r = 0$ and $D(r)$ as $r \neq 0$)

The projection of $V(aX + b)$ is $D(a) \vee V(b)$

This corresponds to both Tarski's quantifier elimination and Chevalley's projection theorem (the projection of a constructible set is constructible)

Chevalley Theorem and quantifier elimination

Chevalley Theorem holds for any finitely presentated extensions: the following map has an adjoint

$B(R) \to B(R[X_1, \dots, X_n]/\langle p_1, \dots, p_m \rangle)$

By composition it is enough to show it for $R \to R[X]$ and $R \to R/\langle p \rangle$

Thus Chevalley Theorem can be seen as a refinement of Tarski quantifier elimination

$B(\mathbb{Z}[X_1, \dots, X_n])$ is $S_n(T)$ where T is the theory of algebraically closed fields

Kronecker Theorem

Any element of the Zariski lattice is of the form

$$D(a_1,\dots,a_n) = D(a_1) \vee \cdots \vee D(a_n)$$

We have seen that $D(a,b) = D(a+b)$ if $D(ab) = 0$

In general we cannot write $D(a_1,\dots,a_n)$ as $D(a)$ for *one* element a

We can ask: what is the least number m such that *any* element of $\mathsf{Zar}(R)$ can be written on the form $D(a_1,\dots,a_m)$. An answer is given by the following version of *Kronecker's Theorem*: this holds if $\mathsf{Kdim}\ R < m$

References

P. Johnstone *Stone spaces*, Cambridge University Press

B. Banaschewski and J. J. C. Vermeulen. Polynomials and radical ideals. *Journal of pure and applied algebra*, (113):219–227, 1996.