Constructive algebra

Thierry Coquand

May 2018

Constructive Algebra

Constructive algebra is algebra done in the context of intuitionistic logic

Support of a ring

Distributive lattice L with a map $D : R \to L$

$D(1) = 1$

$D(0) = 0$

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

$D(ab) = D(a) \wedge D(b)$

We write $D(a_1, \dots, a_n)$ for $D(a_1) \vee \cdots \vee D(a_n)$

Universal support

Support $Z(R)$ (Zariski lattice) with $D_Z : R \to Z(R)$

Satisfies the universal property

$$\begin{tikzcd} R \arrow[r, "D_Z"] \arrow[dr] & Z(R) \arrow[d, dotted, "\exists!"'] \\ & L \end{tikzcd}$$

Universal support

By abstract reasoning, we know the universal support exists

Unique up to isomorphism

Can we have $1 = 0$ in $D_Z(R)$?

This is a *consistency* problem

We build effectively the universal support

Universal support

$I, J, K, \ldots$ finite subset of R

$\langle J \rangle$ is the ideal generated by the elements of J

Define $a \vdash J$ by: some power of a belongs to $\langle J \rangle$

$I \leqslant J$ by: $a \vdash J$ for all a in I

Universal support

Lemma: *If* $a \vdash b_1, \dots, b_m, K$ *and* $b_1 \vdash K, \ \dots, \ b_m \vdash K$ *then* $a \vdash K$

This is cut-elimination

It follows from this that $\leqslant$ is transitive

Universal support

Lemma: *If* $a \vdash J$ *then* $ac \vdash Jc$

Lemma: *If* $a \vdash J$ *and* $a \vdash K$ *then then* $a \vdash JK$

$I \simeq J$ by: $I \leqslant J$ and $J \leqslant I$

$I \wedge J = IJ$ and $I \vee J = I, J$ define a lattice structure $Z(R)$

The canonical map $D_Z : R \to Z(R)$ is a support

This is *the* universal support

Universal support

If $a^2 = 0$ and $b^3 = 0$ then $D_Z(a) = D_Z(b) = 0$

We have $a + b \vdash a, b$ and $a \vdash$ and $b \vdash$

By cuts, $a + b \vdash$

$a + b = a + b$ then $(a + b)^2 = b(2a + b)$ and $(a + b)^6 = b^3(2a + b)^3 = 0$

We get $(a + b)^n = 0$ with $n = 6$!

Structure sheaf of a ring

$Z(R)$ can be seen as a *point-free* description of the Zariski spectrum of R

The elements $D_Z(a)$ form a basis of the topology

$a \vdash b_1, \ldots, b_m$ describes the covering relation for this topology

$F_R(a) = R[1/a]$ defines a (generalized) Beth model structure

To simplify the discussion we assume that R is an integral domain: the equality in R is decidable and R is a subring of a (discrete) field K

$R[1/a] \subseteq K$ if $a \neq 0$

$a \vdash b$ is the same as $R[1/b] \subseteq R[1/a]$ for $a \neq 0, \; b \neq 0$

Structure sheaf of a ring

We define $a \Vdash \varphi$ where φ is a formula in the language of rings with parameters in $R[1/a]$

$a \Vdash t = u$ if $t = u$ in $R[1/a]$

$a \Vdash \varphi \rightarrow \psi$ if $b \vdash a$ and $b \Vdash \varphi$ implies $b \Vdash \psi$

$a \Vdash \varphi \wedge \psi$ if $a \Vdash \varphi$ and $a \Vdash \psi$

$a \Vdash \forall x\ \varphi$ if $b \vdash a$ and u in $R[1/b]$ imply $b \Vdash \varphi(x/u)$

Structure sheaf of a ring

$a \Vdash \varphi \vee \psi$ if we have $D_Z(a) = D_Z(a_1, \ldots, a_n)$ in $Z(R)$ and $a_i \Vdash \varphi$ or $a_i \Vdash \psi$

$a \Vdash \exists x\ \varphi$ if we have $D_Z(a) = D_Z(a_1, \ldots, a_n)$ in $Z(R)$ and u_i in $R[1/a_i]$ with $a_i \Vdash \varphi(x/u_i)$

$a \Vdash \perp$ iff $a = 0$ "exploding" node

Note that $a \Vdash 1 = 0$ if $a = 0$

Structure sheaf of a ring

A *local* ring is a ring such that

$inv(x + y) \rightarrow inv(x) \vee inv(y)$

or, equivalently, for all x

$inv(x) \vee inv(1 - x)$

Classically: a ring with a unique maximal ideal

Lemma: *We have* $\Vdash \forall x \ (inv(x) \vee inv(1 - x))$

So the structure sheaf is a local ring!

Structure sheaf of a ring

Classically we have prime ideals $\alpha, \beta, \ldots$ in $Sp(R)$

For each α we define $R_\alpha = \varinjlim_{\alpha \in D_Z(a)} R[1/a]$

We have a "continuous" family of local rings R_α varying with α

Structure sheaf of a ring, Exercise

We always have (don't forget that R is supposed to be integral domain)

$\Vdash (\neg inv(x)) \rightarrow x = 0$

Classically $(\neg inv(x)) \rightarrow x = 0$ is equivalent to $inv(x) \vee x = 0$

Prüfer domain

Define $x|y$ by $\exists u \ (y = ux)$

A *valuation* domain is an integral domain such that $\forall x\ y\ (x|y\ \vee\ y|x)$

The algorithm on a valuation domain would work with an oracle taking x and y and producing either $x|y$ or $y|x$

A *Prüfer* domain is an integral domain such that

$\Vdash \forall x\ y\ (x|y\ \vee\ y|x)$

So a Prüfer domain is an integral domain such that its structure sheaf is a valuation domain

Prüfer domain

Note: should $\vee$ and $\exists$ be undertood as in univalent mathematics?

The issue does not appear for $x = 0 \vee \exists y \ (xy = 1)$

y is uniquely determined if it exists

Prüfer domain

Let us unfold the definition

We have $1 = \langle u_1, \ldots, u_n, v_1, \ldots, v_m \rangle$

We have $yb_i = xu_i^N$ and $xa_j = yv_j^N$ for some N

We can find r_i, s_j such that $\Sigma r_i u_i^N + \Sigma s_j v_j^N = 1$

Then $y(\Sigma r_i b_i) = xu$ and $x(\Sigma s_j a_j) = yv$

$u = \Sigma r_i u_i^N$ and $v = \Sigma s_j v_j^N$

We get $yb = xu$ and $xa = yv$ with $u + v = 1$

Prüfer domain

A *Prüfer* domain is an integral domain such that

$$\forall\ x\ y\ \exists\ a\ b\ u\ v\ (yb = xu\ \wedge\ xa = yv\ \wedge\ u + v = 1)$$

This is a *first-order* definition

A *Dedekind* domain is exactly a *Noetherian* Prüfer domain

However, some important algorithmic properties of Dedekind domain can be seen at the level of Prüfer domain

Prüfer domain

One of the most important algorithmic property of Dedekind domain is

If a belongs to $\langle J\rangle$ then there exists K such that $\langle a\rangle = \langle JK\rangle$

More generally if $\langle I\rangle \subseteq \langle J\rangle$ then there exists K such that $\langle I\rangle = \langle JK\rangle$

Prüfer domain

This holds for valuation domain

For a valuation domain, given $b_1, \ldots, b_m$ there exists i such that $\langle b_i \rangle = \langle b_1, \ldots, b_m \rangle$

This is a local-global property

Hence it holds for a Prüfer domain!

Prüfer domain

Theorem: *If* $MI \subseteq MJ$ *and* $M \neq 0$ *then* $I \subseteq J$

This holds for a valuation domain and is a local-global property

Application

We have $IJ \subseteq I + J$ hence there exists M such that

$M(I + J) = IJ$

Proposition: *If* $M(I + J) = IJ$ *we have* $M = I \cap J$

We have $M(I + J) \subseteq I(I + J)$ hence $M \subseteq I$

We have $M(I + J) \subseteq J(I + J)$ hence $M \subseteq J$

If $M' \subseteq I$ and $M' \subseteq J$ then $M'(I + J) \subseteq IJ$ hence $M' \subseteq M$

Application

Hence if I and J are finitely generated ideals then so is $I \cap J$

This property of Prüfer and hence Dedekind domain is hidden with usual definitions of Dedekind domain

But it was considered as a *crucial* property of Dedekind domain by Dedekind!

Application

In a Prüfer domain we have

$I \cap (J + K) = (I \cap J) + (I \cap K)$

This follows from cancellation property

It also can be seen as a local-global property

And this is equivalent to being Prüfer

Exercise about l-group!

Coherent domain

An integral domain is *coherent* iff $I \cap J$ is finitely generated when I and J are finitely generated

Given a finitely generated ideal I we can then compute a *resolution* of I

$$\cdots \to R^{m_1} \to R^{m_0} \to I \to 0$$

Coherent domain

Classically any Noetherian domain is coherent

Exercise: If R is an integral domain and $Z(R)$ is a Boolean algebra (R is 0-dimensional) then any polynomial ring $R[X_1, \ldots, X_n]$ is coherent (but it does not need to be Noetherian)

Dedekind domain

Compare with the “usual” definition

A *Dedekind* domain is a domain where any proper ideal is a product of prime ideals

From this definition it is difficult to extract an algorithm which computes generators for $I \cap J$, i.e. to prove effectively that a Dedekind domain is coherent

Dedekind has had several versions of his theory of ideals

See the papers of J. Avigad and H. Edwards on development of ideal theory

Integral closure

Let $R \subseteq K$ be a domain and s an element in a field extension L of K

Let S be the integral closure of R in L

Theorem: *If t is a root of a primitive polynomial in $R[X]$ then we can find $s_1, \dots, s_m$ in L all integral over R and $r_1, \dots, r_m$ in R such that $\Sigma r_i s_i = 1$ for all i we have t or $1/t$ in $S[1/s_i]$*

Lemma: *If $a_n t^n + \cdots + a_0 = 0$ with $a_n, \dots, a_0$ in R then all elements $b_n = a_n, b_{n-1} = a_n t + a_{n-1}, \dots,\ b_1 = b_2 t + a_1,\ b_0 = b_1 t + a_0$ are in S*

Integral closure

Corollary *If R is a Bezout domain then S is a Prüfer domain*

Bezout domain: given a, b in R we can find g, u, v, x, y such that $a = gu,\ b = gv$ and $ux + vy = 1$

Examples: $\mathbb{Z}$ and $k[X]$ is X is a field

Examples: $\mathbb{Z}[\sqrt{-5}]$ and $k[x, y]$ with $y^2 = 1 - x^4$ are Prüfer domain

For instance we can compute I such that $\langle x \rangle = \langle x, y \rangle I$

Gruson-Raynaud

If V is a valuation domain (or a Prüfer domain) one can show

The intersection of two finitely generated ideals of $V[X_1, \ldots, X_n]$ *is finitely generated*

This is a result of a paper of Gruson-Raynaud *Critères de platitude et de projectivité*, 1971

There is a direct algorithm (I. Yengui, C. Quitté, H. Lombardi, 2014)

Is it possible to extract an algorithm from Gruson-Raynaud's proof?

Riemann-Roch

Conjecture: *If* k *is a perfect field and* $y^n + a_1(x)y^{n-1} + \cdots + a_n(x) = 0$ *a* separable *polynomial in* $k[x, y]$ *then the integral closure of* $k[x]$ *in* $k(x, y)$ *is a free* $k[x]$*-module*

This would allow a general effective treatment of Riemann-Roch Theorem