Coherent Ring

Thierry Coquand

September 2010

This lecture

We present a notion typical of constructive mathematics: the notion of *coherent* ring

It can be seen as a constructive approximation of the notion of Noetherian ring. It was introduced explicitely in Bourbaki.

It illustrates the connection between *constructive reasoning* and *algorithms*. All the proofs I will present can be thought of/rewritten as programs.

Coherence is not a first-order notion, but there are various first-order conditions that imply coherence

Prüfer domain is a first-order approximation of Dedekind domain

Coherent ring: motivation

Over a field, we know how to solve a linear system

$$AX = 0 \qquad\qquad AX = B$$

Gauss elimination

Over a ring, one approximation of this is to be able to generate all solutions, i.e. to find L such that

$$AX = 0 \leftrightarrow \exists Y.X = LY$$

The columns of L generate all the solutions

Coherent ring: motivation

If the ring R is Noetherian, it can be shown that any submodule of R^n is finitely generated

In particular, the submodule $\{X \in R^n \mid AX = 0\}$ is finitely generated

Classically, $AX = B$ has at least one solution X_0, and then $AX = B$ iff $A(X - X_0) = 0$, or no solution

In particular over $k[X_1, \dots, X_n]$, one can generate the solutions of any linear system

But since we use Noetherianity, and classical logic, we do not get any algorithm

Coherent ring: definition

A ring R is *coherent* iff for any A we can find L such that

$$AX = 0 \leftrightarrow \exists Y. X = LY$$

Theorem: *The ring* $k[X_1, \ldots, X_n]$ *is coherent*

e.g. using Gröbner basis

Coherent and Noetherian

Any Noetherian ring is coherent

If B infinite Boolean algebra, then B is coherent and not Noetherian

More generally, if R is vN regular (forall a there exists b such that $a^2b = a$) then R is coherent as well as $R[X_1, \ldots, X_n]$

Strongly discrete ring

A ring is *strongly discrete* iff we can decide membership to any finitely generated ideal, i.e. we can decide if a system

$$a_1x_1 + \cdots + a_nx_n = b$$

has a solution or not

Theorem: *The ring $k[X_1, \ldots, X_n]$ is strongly discrete*

using Gröbner basis

Strongly discrete and coherent ring

Theorem: *If the ring R is coherent and strongly discrete we can decide if a system $AX = B$ has a solution*

What is good for?

Symbolic representation of differential equations

Method of separation of symbols (Argobast, Boole)

An equation like $\partial_x f + \partial_y g + \partial_z h = 0$ is seen symbolicaly as an equation on $\mathbb{Q}[\partial_x, \partial_y, \partial_z]$ seeing $\partial_x, \partial_y, \partial_z$ as *indeterminates*

One is then lead to the system $XU + YV + ZW = 0$ on $\mathbb{Q}[X, Y, Z]$

The solutions are generated by $(-Y, X, 0),\ (0, -Z, Y),\ (Z, 0, -X)$

Cf. divergence, gradient and curl in physics

What is good for?

One important application of algorithms on coherent rings is in the (algebraic) analysis of systems of differential equations

To each system is associated a matrix A over a polynomial ring

For instance, the problem of whether the system is parametrizable can be analyzed algebraically

What is good for?

The system $\partial_x f + \partial_y g + \partial_z h = 0$ is parametrizable

The system $f' = -g,\ g' = f$ is not parametrizable

A. Quadrat, System HOMALG (Aachen) is a computer system for solving these kind of questions

The notion of coherent and strongly discrete ring is essential

Equivalent Definitions

Proposition 1: *If we can generate solutions of one line system* $AX = 0$ *then we can generate solutions of any system* $AX = 0$

Proposition 2: *If the intersection of two finitely generated ideals is finitely generated over a domain* R *then* R *is coherent. Conversely if* R *is a coherent ring then the intersection of two finitely generated ideals is finitely generated.*

Proposition 3: *In general, a ring* R *is coherent iff the intersection of two finitely generated ideals is finitely generated and for any element* a *the ideal* $\mathsf{Ann}(a) = \{x \in R \mid ax = 0\}$ *is finitely generated*

Principal Ideal Domain?

This notion is not so well behaved constructively: *any* ideal is principal, quantification on all subsets

It is replaced by a first-order approximation, of *Bezout* domain: any finitely generated ideal is principal

This can be expressed by a first-order (positive) condition

$$\forall p\ q.\exists g\ u\ v\ a\ b.\ \ p = gu \wedge q = gv \wedge g = ap + bq$$

Theorem: *The ring $k[X]$ is a Bezout domain*

Principal Ideal Domain?

Theorem: *Any Bezout domain is coherent*

Theorem: *A Bezout domain is strongly discrete iff we can decide divisibility*

Euclidean domain

We have a norm $N : (R - \{0\}) \to \mathbb{N}$ such that if $a \neq 0$

$$\forall b. \exists q\ r.\ a = bq + r \wedge (r = 0 \vee N(r) < N(a))$$

Example: $\mathbb{Z}$ and $k[X]$

Theorem: *Any Euclidean domain is a Bezout domain*

Hence any Euclidean domain is coherent

GCD domain

$k[X,Y]$ is not a Bezout domain: $\langle X,Y\rangle$ cannot be generated by one element

R is a *GCD domain* iff any two elements have a gcd

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

Hence $k[X_1,\dots,X_n]$ is a GCD domain

Classically this is an Unique Factorization Domain; GCD domain is a first-order approximation of UFD

Coherent domain

It is *not true* in general that if R is coherent then so is $R[X]$

If R is coherent and $A : R^m \rightarrow R^n$ we can find $A_1 : R^{m_1} \rightarrow R^m$ such that

$$AX = 0 \leftrightarrow \exists Y. X = A_1 Y$$

We build in this way a sequence

$$\ldots \longrightarrow R^{m_3} \xrightarrow{A_3} R^{m_2} \xrightarrow{A_2} R^{m_1} \xrightarrow{A_1} R^m \xrightarrow{A} R^n$$

Free Resolution

In particular if we have a finitely generated ideal I we have a map

$$R^m \xrightarrow{A} I \longrightarrow 0$$

and we can build a sequence

$$\ldots \longrightarrow R^{m_3} \xrightarrow{A_3} R^{m_2} \xrightarrow{A_2} R^{m_1} \xrightarrow{A_1} R^m \xrightarrow{A} I \longrightarrow 0$$

This is called a *free resolution* of the ideal

This measures the "complexity" of the ideal: relations between generators, then relations between relations, and so on.

Free Resolution

If we have $m_k = 0$ for $k > N$ we say that I has a *finite free resolution*

$$0 \longrightarrow R^{m_N} \xrightarrow{A_N} \dots \xrightarrow{A_2} R^{m_1} \xrightarrow{A_1} R^m \xrightarrow{A} I \longrightarrow 0$$

Theorem: *If* $\langle a_1, \dots, a_l \rangle$ *has a finite free resolution then* $a_1, \dots, a_l$ *have a gcd*

For fixed sizes this is a first-order statement!

Not so easy even for $0 \longrightarrow R^2 \longrightarrow R^3 \longrightarrow I \longrightarrow 0$

Finitely presented modules

Over a field, *finitely generated* vector spaces

If $u : F \rightarrow G$ and F, G are finitely generated then so are Ker u and CoKer u

Over coherent rings, we consider *finitely presented* modules

If $u : F \rightarrow G$ and F, G are finitely presented then so are Ker u and CoKer u

Finitely presented modules

Concretely a finitely presented module is given by a matrix

$$R^n \xrightarrow{A} R^m \longrightarrow M \longrightarrow 0$$

The module M is isomorphic to $R^m/\mathrm{Im}\ A$

We have m generators and n relations

Example: $R = \mathbb{Q}[X]$ and $A = \begin{pmatrix} X & -1 \\ 1 & X \end{pmatrix}$

Finitely presented modules

Theorem: *The category of finitely presented modules over a coherent ring is an abelian category*

Finitely presented modules

If R is a ring like $\mathbb{Q}[\partial_1, \partial_2, \partial_3]$ a matrix represents a system of differential equations

The properties of this system are reflected in the properties of the finitely presented module associated to this matrix

For instance, to have an algorithm for Quillen-Suslin Theorem is interesting in this context

Finitely presented modules

If M is finitely presented over a coherent *and* strongly discrete ring R we can decide whether $M = 0$ or not

Indeed, we can decide whether $R^n \xrightarrow{A} R^m$ is surjective or not

Torsion module

If M is a module over a domain R we define

$$t(M) = \{m \in M \mid \exists r \neq 0 \; rm = 0\}$$

Theorem: *If R is a coherent domain and M is finitely presented then so is $t(M)$.*

Corollary: *If R is a coherent and strongly discrete domain and M is finitely presented then we can decide whether $t(M) = 0$ or not*

Torsion module

For instance if we take $R = \mathbb{Q}[X]$ and $A = \begin{pmatrix} X & -1 \\ 1 & X \end{pmatrix}$

Then we have $(X^2 + 1)m = 0$ for all m in M and so we have $t(M) = M$

Torsion module

Algorithm for computing a presentation of $t(M)$

$$R^n \xrightarrow{A} R^m \longrightarrow M \longrightarrow 0$$

We compute B such that $\text{Im } B = \text{Ker } A^{\mathrm{T}}$ which is possible since R is coherent

We then have $\text{Im } A \subseteq \text{Ker } B^{\mathrm{T}}$ and $t(M)$ is isomorphic to the quotient $\text{Ker } B^{\mathrm{T}}/\text{Im } A$

Indeed, over $K = \text{Frac}(R)$ we have $\text{Im } A = \text{Ker } B^{\mathrm{T}}$ by usual linear algebra over a field

Torsion module

What is the meaning in term of differential equations?

Let $\mathcal{F}$ be a module of "functions"

-If $\mathcal{F}$ is *injective* and the module presented by A has no torsion (we have $\text{Im } A = \text{Ker } B^{\mathrm{T}}$) then the system defined by A is parametrizable (by B^{T})

-If $\mathcal{F}$ is a cogenerator, i.e. $Hom(M, \mathcal{F}) = 0$ implies $M = 0$, and the system defined by A is parametrizable, then the module presented by A has no torsion

Example: $C^{\infty}(\mathbb{R}^3)$ is an injective cogenerator over $\mathbb{R}[\partial_x, \partial_y, \partial_z]$

Prüfer domain

In commutative algebra, an important notion is the one of *Dedekind domain*

Noetherian integrally closed such that any non zero prime ideal is maximal

This definition is quite far from what Dedekind considered important about his notion, and not easy to interpret computationally

J. Avigad *Methodology and metaphysics in the development of Dedekind's theory of ideals*

Prüfer domain

For Dedekind what was important was the possibility of finding an inverse to any finitely generated ideal

This is algorithmic: for any $a_1, \dots, a_n$ we can find $b_1, \dots, b_m$ such that the product ideal

$$\langle a_1, \dots, a_n \rangle \langle b_1, \dots, b_m \rangle = \langle a_1 b_1, \dots, a_n b_m \rangle$$

is a principal ideal

Theorem: *Prüfer domain are coherent*

Prüfer domain

Algorithm to compute $I \cap J$

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

Let K be an inverse of $I + J$: we have $K(I + J) = \langle c \rangle$

Then $c(I \cap J) = KIJ$ and c divides all elements in KI so we find generators for $I \cap J$

Prüfer domain

Examples: $\mathbb{Z}[\sqrt{-5}]$ (algebraic numbers)

$\mathbb{Q}[x, y]$ with $y^2 = 1 - x^4$ (algebraic curves)

Prüfer domain

Dedekind domain are exactly *Noetherian* Prüfer domain so that the previous result does not appear in the usual presentation of Dedekind domain

There is a simple first-order characterisation of Prüfer domain

$$\forall a\ b. \exists u\ v\ w.\ \ au = bv \wedge aw = b(1-u)$$

Intuitively, we write that any localization at any prime is a valuation domain (divisibility is a total order) in a finite way

An equivalent condition is: the lattice of ideal is distributive

Prüfer domain

Theorem: *If R is a Prüfer domain then $R[X_1, \dots, X_n]$ is coherent*

This is proved in classical mathematics using complex methods (Gruson-Raynaud)

I. Yengui has recently found an algorithm for showing that $R[X]$ is coherent if R is a Prüfer domain