# Curves and coherent Prüfer rings
# A simple computation

**Mega 09. Barcelona, June 15-19 2009**

T. Coquand, Göteborg. H. Lombardi, Besançon.
C. Quitté, Poitiers.

coquand@chalmers.se, http://www.math.chalmers.se/~coquand/
Henri.Lombardi@univ-fcomte.fr, http://hlombardi.free.fr
quitte@mathlabo.univ-poitiers.fr

A printable version of these slides :
http://hlombardi.free.fr/publis/Mega09Doc.pdf
An article on the subject
http://hlombardi.free.fr/publis/prufer-courbes.pdf

## Our problem

The coordinate ring of a smooth plane curve is a Dedekind domain. We study the computational meaning of this theorem.

## Outline

1. Dedekind domains
2. Smooth algebraic plane curve
3. A classical proof
4. Towards a constructive rewriting of the classical proof
5. A generalisation of Hasse-Schmidt derivatives
6. Algorithmic solution of the problem

# 1. Dedekind domains (constructively)

Usual definitions of Dedekind domain are not well suited for an algorithmic treatment.

For instance, if **k** is a field, even given explicitely, there is in general no method to factorise polynomials in $\mathbf{k}[X]$.

So the definition as "a domain where finitely generated nonzero ideals are decomposable in product of maximal ideals" is not satisfactory.

# Dedekind domains

Dedekind considered that the main divisibility property was the following one :

For all $x_1, \ldots, x_n \in \mathbf{A}$ there exist $\gamma_1, \ldots, \gamma_n \in$ Frac$(\mathbf{A})$ such that $\sum_i \gamma_i x_i = 1$ and all $\gamma_i x_j$ are in $\mathbf{A}$.

See : Avigad J. *Methodology and metaphysics in the development of Dedekind's theory of ideals*. In : José Ferreirós and Jeremy Gray, editors, The Architecture of Modern Mathematics, Oxford University Press, (2006), 159–186.

This is a concrete formulation of **arithmeticity** for a domain. A ring is called **arithmetical** when f.g. ideals are **locally principal**, i.e., for any f.g. ideal $\mathfrak{a} = \langle x_1, \ldots, x_n \rangle$ there exist comaximal elements $e_1, \ldots, e_n$ s.t. in each $\mathbf{A}[1/e_i]$, $\mathfrak{a} = \langle x_i \rangle$. In the Dedekind formulation $e_i = \gamma_i x_i$.

## Dedekind domains

Also a ring is arithmetical iff its lattice of ideals is distributive.

An arithmetical domain is called a **Prüfer domain**.

In particular a Prüfer domain is a **coherent** ring :
i.e. every f.g. ideal is finitely presented.
Or also : the kernel of a matrix is always finitely generated.
This is a very important property for computations.

From a constructive point of view, we define a Dedekind domain as a **strongly discrete Noetherian Prüfer domain**.

## Dedekind domains

We define a **Prüfer ring** as an arithmetical reduced ring.

A ring is a **pp-ring** if for all $x$ there is an idempotent $e$ s.t. Ann$(x) =$ Ann$(e)$. So in $\mathbf{A}/\langle e\rangle$, $x$ is regular, and in $\mathbf{A}/\langle 1 - e\rangle$, $x = 0$.

A ring is **coherent and Prüfer** iff it is **an arithmetical pp-ring**.

We think that **coherent Prüfer rings** are the best generalisation of Prüfer domains in presence of zerodivisors.

In rings with no factorisation algorithms, zerodivisors are unavoidable when passing to quotients.

## Dedekind domains

For a general constructive exposition of arithmetical, Prüfer and Dedekind rings see :

Lionel Ducos, Henri Lombardi, Claude Quitté, and Maimouna Salou. *Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind.* J. Algebra, **281**, (2004) 604–650.

H. Lombardi, C. Quitté. *Algèbre Commutative, Méthodes Constructives.* (chapters 3, 8 and 12) To appear.
Available at http://hlombardi.free.fr/publis/LivresBrochures.html.

# 2. Smooth algebraic plane curve

Let **k** be a discrete field and $f(x, y)$ an absolutely irreducible polynomial. Let $\mathbf{R} = \mathbf{k}[x, y]/\langle f \rangle$ the coordinate ring of the curve $f(x, y) = 0$.

We assume that the curve is smooth. I.e., there is no singularity.
By the Nullstellensatz this means that $1 \in \langle f, f_x, f_y \rangle$.

**Theorem 1. R** *is a Dedekind domain.*

We are interested in the computational content of this theorem.

More precisely we want to construct an algorithm showing that **R** is a Prüfer domain.

## Smooth algebraic plane curve

We are to give the following slightly more general result.

**Theorem 2.** *Let* $\mathbf{k}$ *be a discrete field,* $f(x,y) \in \mathbf{k}[x,y]$ *an arbitrary polynomial and* $\mathbf{R} = \mathbf{k}[x,y]/\langle f \rangle$*. Assume that* $1 \in \langle f, f_x, f_y \rangle$*. Then* $\mathbf{R}$ *is a coherent Prüfer ring.*

In classical mathematics it follows that $\mathbf{R}$ is a finite product of Dedekind domains.

Theorem 2 is an immediate consequence of the following general theorem.

**Theorem 3.** *Let* $\mathbf{k}$ *be a discrete field,* $f(x,y) \in \mathbf{k}[x,y]$ *an arbitrary polynomial and* $\mathbf{R} = \mathbf{k}[x,y]/\langle f \rangle$*. Then* $\mathbf{R}_{f_y}$ *is a coherent Prüfer ring.*

# 3. A classical proof

In the case where $\mathbf{k}$ is algebraically closed, $f$ irreducible and $f_y \neq 0$. Let $\mathbf{A} = \mathbf{R}_{f_y} = (\mathbf{k}[x,y]/\langle f \rangle)_{f_y}$

Clearly $\mathbf{A}$ is a Noetherian domain. So it is Dedekind iff it is Prüfer.

One proves that $\mathbf{A}$ is a Prüfer domain by showing that any localisation $\mathbf{R}_{\mathfrak{p}}$ is a valuation ring, where $\mathfrak{p}$ is an arbitrary maximal ideal not containing $f_y$.

## A classical proof

Since **k** is algebraically closed, a maximal ideal $\mathfrak{p}$ of **R** is on the form $\mathfrak{p} = \langle x - a, y - b\rangle$ where $a, b$ are in **k** such that $f(a, b) = 0$.

The fact that $f_y$ is not in $\mathfrak{p}$ means that we have $f_y(a, b) \neq 0$. So $f_y$ is invertible in $\mathbf{R}_{\mathfrak{p}}$.

We simply follow the usual proof that $\mathbf{R}_{\mathfrak{p}}$ is a discrete valuation ring with $x - a$ as uniformising parameter :
we show that any nonzero element in **R** can be written $w \cdot (x - a)^m$ with $w$ invertible in $\mathbf{R}_{\mathfrak{p}}$ and $m \in \mathbb{N}$ ($n$ is the “valuation” of $g$ at $\mathfrak{p}$).

# A classical proof

We write in $\mathbf{k}[x,y]$

$$f - f(a,b) = (x-a)u - (y-b)v$$

with $u$ and $v$ in $\mathbf{k}[x,y]$. We have then $v(a,b) = -f_y(a,b) \neq 0$. So, in $\mathbf{R}_{\mathfrak{p}}$

$$(y-b) = (x-a)uv^{-1}$$

Similarly, for an arbitrary element $g$ in $\mathbf{k}[x,y]$ nonzero in $\mathbf{R}$ we can write

$$g = g(a,b) + (x-a)p - (y-b)q$$

with $p, q \in \mathbf{k}[x,y]$ and hence in $\mathbf{R}_{\mathfrak{p}}$

$$g = g(a,b) + t\, r_1$$

with $r_1 = pv - qu$ and the parameter $t = (x-a)v^{-1} \in \mathfrak{p}\mathbf{R}_{\mathfrak{p}}$.

## A classical proof

Doing the same operation with $r_1$ instead of $g$ we get similarly in $\mathbf{R}_{\mathfrak{p}}$

$$g = g(x,y) = g(a,b) + t\,r_1(a,b) + t^2\,r_2(x,y)$$

It is natural to write $r_0 = g$. We let $g_0 = g(a,b)$, $g_1 = r_1(a,b) \in \mathbf{k}$.
In general, we have an equality in $\mathbf{R}_{\mathfrak{p}}$

$$g = g_0 + t\,g_1 + \cdots + t^{n-1}\,g_{n-1} + t^n\,r_n$$

with $g_k = r_k(a,b) \in \mathbf{k}$.

A constructive argument using the nonzero resultant $d(x) = \mathrm{Res}_y(f,g)$ shows that some $g_m$ is nonzero.
The first $m$ such that $g_m \neq 0$ is the valuation of $g$ at $\mathfrak{p}$.

# 4. Towards a constructive rewriting of the classical proof

The preceeding classical proof uses strong abstract arguments : nonzero primes of **R** are written $\langle x-a, y-b\rangle$ with $(a,b)$ on the curve, and a domain is Prüfer iff all localisations at maximal ideals are valuation rings.

Besides these strong arguments (the second one is nonconstructive), the computations in the proof are very simple. The computation does depend on $(a,b)$ (the valuation of $g$ at $\langle x-a, y-b\rangle$ depends on $(a,b)$), but intuitively it is always the same computation.

So there must be simple analog computations not using the fact that **k** is algebraically closed and showing that $\mathbf{R}_{f_y}$ is arithmetical without using nonconstructive steps.

## Towards a constructive rewriting of the classical proof

First we show a uniform rewriting of the computation giving the valuation at $\mathfrak{p} = \langle x - a, y - b \rangle$ (a generalisation of Hasse-Schmidt derivatives).

Second the idea underlying the constructive deciphering of the classical proof is to replace "all points of the curve with coordinates in an algebraic closure of **k**" by *the* generic zero of $f$, which is $(a, b)$ in $\mathbf{k}[a, b]/\langle f(a, b) \rangle$.

# 5. A generalisation of Hasse-Schmidt derivatives

The preceeding computations are in fact uniform if we modify the context, in a straightforward generalisation.

Let **B** be a commutative ring, and $a, b$ two elements of **B**. We write $\delta_0 : \mathbf{B}[x,y] \to \mathbf{B}$ the evaluation $\delta_0(h) = h(a,b)$. In a shorter way : $h_0 = h(a,b)$.

If $f$ is a polynomial in $\mathbf{B}[x,y]$ we can write in $\mathbf{B}[x,y]$

$$f - f_0 = (x-a)u - (y-b)v$$

We let $\boxed{\mathbf{R} = \mathbf{B}[x,y]/\langle f - f_0\rangle}$ and $\boxed{\mathbf{A} = \mathbf{R}_{f_y}}$ (**B** is simply an arbitrary ring and **A** replaces $\mathbf{R}_{\mathfrak{p}}$).
We have $\delta_0(v) = -\delta_0(f_y)$, so $\delta_0(v)$ is invertible in **A**.

## A generalisation of Hasse-Schmidt derivatives

For an element $g$ of $\mathbf{B}[x,y]$ we can write

$$g - \delta_0(g) = (x-a)p - (y-b)q$$

and hence define $\Delta(g) = pv - qu$.
In **A**, with $\boxed{t = (x-a)v^{-1}}$ we get

$$g = g_0 + t\,\Delta(g)$$

It is easy to see that $\Delta$ is a well defined **B**-linear map **R** → **R**. Doing for $\Delta(g)$ the samething we get

$$g = g_0 + t\,g_1 + t^2\,\Delta(\Delta(g))$$

with $g_1 = \Delta(g)(a,b) = (\delta_0 \circ \Delta)(g)$.

## A generalisation of Hasse-Schmidt derivatives

We let $\delta_n = \delta_0 \circ \Delta^n$, $r_n = \Delta^n(g)$ and $g_n = \delta_n(g) = r_n(a,b)$. We get the following general “Taylor expansion” for $g$ in **A** near $(a,b)$

$$g = g_0 + t\,g_1 + \cdots + t^{n-1}\,g_{n-1} + t^n\,r_n \qquad g_i \in \mathbf{B},\ t \in \mathbf{A},\ g, r_n \in \mathbf{R}.$$

Considering two elements $g, h$ of **R** one shows

$$\Delta^n(gh) = g\Delta^n(h) + \textstyle\sum_{i=1}^{n} \delta_{n-i}(h)\Delta^i(g) \qquad (n > 0).$$

If we apply $\delta_0$ we get

$$\delta_n(gh) = \textstyle\sum_{i+j=n} \delta_i(g)\delta_j(h)$$

## A generalisation of Hasse-Schmidt derivatives

We can consider the map

$$\mathbf{R} \to \mathbf{B}[[t]], \;\; g \mapsto \sum_{i=0}^{\infty} \delta_i(g)t^i$$

and the equality $\delta_n(gh) = \sum_{i+j=n} \delta_i(g)\delta_j(h)$ shows that this is a map of **B**-algebras.

## A generalisation of Hasse-Schmidt derivatives

**Lemma 4.** *We have for any $n \geq 1$*

$$h\Delta^n(g) = g\Delta^n(h) \text{ in } \mathbf{B}[x,y]/\langle f - f_0\rangle$$
$$\text{modulo } \delta_0(g), \ldots, \delta_{n-1}(g), \delta_0(h), \ldots, \delta_{n-1}(h).$$

**Lemma 5.** *If we have $d$ in $\langle f, g\rangle \cap \mathbf{B}[x]$ which is* primitive, *i.e. $d = \sum_{i=0}^{n} u_i x^i$ with $1 \in \langle u_0, \ldots, u_n\rangle$ in $\mathbf{B}$ then $D(\delta_0(f_y))$ is covered by $D(\delta_0(f), \delta_0(g), \ldots, \delta_n(g))$ in the Zariski spectrum of $\mathbf{B}$.*
*Equivalently the Zariski spectrum of $\mathbf{B}_{f_y(a,b)}$ is covered by*

$$D(\delta_0(f), \delta_0(g), \ldots, \delta_n(g)),$$

*i.e., $\langle 1\rangle = \langle f_0, g_0, \ldots, g_n\rangle$ in $\mathbf{B}_{f_y(a,b)}$.*

# 6. Algorithmic solution of the problem

We consider the case where **k** is a discrete field and $f$ is an arbitrary polynomial in **k**$[x, y]$.

As before we write **R** for the ring **k**$[x, y]$ quotiented by $f$. We let **A** be the localisation $\mathbf{R}_{f_y}$.

**Lemma 6.** *Each divisor $p$ of $f$ in* **k**$[x, y]$ *determines an idempotent $e_p$ in* **A** *such that $\langle p \rangle = \langle e_p \rangle$ in* **A**.
*Moreover if $f = pq$ we have $e_q = 1 - e_p$ and $\mathbf{A}_{e_p} \simeq (\mathbf{k}[x, y]/\langle q \rangle)_{pq_y}$, which is a localisation of $(\mathbf{k}[x, y]/\langle q \rangle)_{q_y}$.*

## Algorithmic solution of the problem

**Example.** Let $\boxed{f = y^2(y+x+1)(y+2x+1) = pq}$ with

$$p = y(y+x+1) \text{ and } q = y(y+2x+1) = yr$$

Let $\boxed{g = (y+x+1)(y+2x+1)}$. We obtain

$$\mathbf{A} = (\mathbf{k}[x,y]/\langle f\rangle)_{f_y} \simeq (\mathbf{k}[x,y]/\langle g\rangle)_{g_y}$$

In $(\mathbf{k}[x,y]/\langle q\rangle)_{q_y}$, $p$ is not regular and

$$(\mathbf{k}[x,y]/\langle q\rangle)_{pq_y} \simeq (\mathbf{k}[x,y]/\langle r\rangle)_{pr_y} = (\mathbf{k}[x,y]/\langle r\rangle)_{p} \simeq (\mathbf{k}[x])_{x(2x+1)}$$

## Algorithmic solution of the problem

Two consequences of Lemma 6 :

**Proposition 7.** **A** *is a pp-ring.*

**Fact**. in the problem of finding a covering of the Zariski spectrum of **A** by elements $D(w)$ such that on each localisation $\mathbf{A}_w$ we have that $g$ divides $h$ or $h$ divides $g$, we can as well suppose that the polynomials $g$ and $f$ are relatively prime in $\mathbf{k}[x, y]$.

## Algorithmic solution of the problem

**Lemma 8.** *(crucial lemma) Let $g, h$ be two elements of* $\mathbf{k}[x,y]$ *such that $g$ and $f$ are relatively prime in* $\mathbf{k}[x,y]$*. We can find $u_0 = g, v_0 = h, u_1, v_1, \ldots, u_m, v_m$ in* $\mathbf{k}[x,y]$ *such that $v_i g = u_i h$ for $i = 0, \ldots, n$ and $D(f_y)$ is covered by $D(u_0), D(v_0), \ldots, D(u_m), D(v_m)$ in the Zariski spectrum of* $\mathbf{R}$*.*

We consider now $a, b$ as *new indeterminates* and consider the ring $\mathbf{B} = \mathbf{k}[a,b]$ and fix a monomial ordering on $\mathbf{B}[x,y] = \mathbf{k}[a,b,x,y]$.

We write

$$g_i = \delta_i(g),\ h_i = \delta_i(h) \quad \text{in} \quad \mathbf{B}, \qquad r_i = \Delta^i(g),\ s_i = \Delta^i(h) \quad \text{in} \quad \mathbf{B}[x,y]$$

## Algorithmic solution of the problem

Since $f$ and $g$ are relatively prime in $\mathbf{k}[x,y]$ the intersection $\langle f,g\rangle \cap \mathbf{k}[x]$ is nonzero.

So we can apply Lemma 5 and there exists $m$ such that $D(f_y(a,b))$ is covered by $D(f_0, g_0, \ldots, g_m)$ in $\mathbf{B} = \mathbf{k}[a,b]$.

Replacing $a$ and $b$ by $x$ and $y$, we see that $D(f_y)$ is covered by $D(g_0(x,y), \ldots, g_m(x,y))$ in $\mathbf{R} = \mathbf{k}[x,y]/\langle f\rangle$

# Algorithmic solution of the problem

Let $n \geq 1$. Let us write $N(p)$ the normal form of an element $p$ in $\mathbf{k}[a,b,x,y] = \mathbf{B}[x,y]$ w.r.t. a Gröbner basis of the ideal $I_n$ generated by

$$f_0, g_0, h_0, \ldots, g_{n-1}, h_{n-1}$$

Note that this ideal is defined on **B**.

Let $p_n = N(r_n) = p_n(a,b,x,y)$ and $q_n = N(s_n) = q_n(a,b,x,y)$ $(n \geq 1)$.

We let $u_0 = g$, $v_0 = h$ and for $n \in [1,m]$,

$$u_n = p_n(x,y,x,y) \text{ and } v_n = q_n(x,y,x,y)$$

We are done !

## Algorithmic solution of the problem

**Theorem 9.** *The ring $\mathbf{A} = \mathbf{R}_{f_y}$ is a coherent Prüfer ring.*

**Corollary 10.** *If $f$ is a polynomial in $\mathbf{k}[x, y]$ such that $1 = \langle f, f_x, f_y \rangle$ then $\mathbf{k}[x, y]/\langle f \rangle$ is a coherent Prüfer ring.*

We provide an implementation in `Magma` of the algorithm which is obtained by following the constructive proof.

**Thank you**

**Thanks to the organizers**