Curves and coherent Prüfer rings

Thierry Coquand (*) Henri Lombardi (†), Claude Quitté (‡)

January 21, 2009

Introduction

Usual definitions of Dedekind domain are not well suited for an algorithmic treatment. Indeed, the notion of Noetherian rings is subtle from a constructive point of view, and to be able to get prime ideals involve strong hypotheses. For instance, if $\mathbf{k}$ is a field, even given explicitely, there is in general no method to factorize polynomials in $\mathbf{k}[X]$.

The work [2] analyses the notion of Dedekind domain from a constructive point of view. A first good constructive approximation of the notion of Dedekind domain is the notion of *coherent Prüfer ring*[1]. We recall the required definitions. Classically, a ring $\mathbf{R}$ is *arithmetical* iff any localisation $\mathbf{R}_{\mathfrak{p}}$ at any prime $\mathfrak{p}$ of $\mathbf{R}$ is a valuation ring, i.e. such that the divisibility relation is linear. A ring $\mathbf{R}$ is arithmetical iff its lattice of ideal is distributive iff for any pair of elements x, y we can find u, v, w such that $xv = yu$ and $x(1-u) = yw$. Yet another equivalent definition, which can be seen as a formal version of the classical definition is that for any pair of elements x, y we can find a covering $D(w_1), \ldots, D(w_n)$ of the Zariski spectrum of $\mathbf{R}$ such that x divides y or y divides x in each localisation $\mathbf{R}_{w_i}$. We say that a ring is a *Prüfer ring* iff all its ideal are flat iff it is arithmetical and reduced (if $x^2 = 0$ then $x = 0$). One can then show that a Prüfer ring is *coherent* (i.e. any finitely generated ideal is finitely presented) iff it is a pp-ring (i.e. the annihilator of any element is generated by an idempotent)[2]. In particular any domain which is arithmetical is a coherent Prüfer ring. However to assume the ring to be integral is too strong constructively since we cannot decide irreducibility in general.

The goal of this paper is to show, in constructive mathematics, that if $\mathbf{k}$ is a discrete field and f an arbitrary polynomial in $\mathbf{k}[x, y]$ then the localisation $\mathbf{R}_{f'_y}$ is *always* a coherent Prüfer ring[3], where $\mathbf{R}$ denotes the ring $\mathbf{k}[x, y]$ quotiented by f. (Computationally, this means in particular that we have to solve the following problem: given g, h two elements of $\mathbf{k}[x, y]$ to find $u_0 = g, v_0 = h, u_1, v_1, \ldots, u_n, v_n$ in $\mathbf{k}[x, y]$ such that $v_i g = u_i h$ modulo f for $i = 0, \ldots, n$ and $D(f'_y)$ is covered by $D(u_0), D(v_0), \ldots, D(u_n), D(v_n)$ in the Zariski spectrum of $\mathbf{R}$.) An important corollary is that $\mathbf{R}$ is a coherent Prüfer ring whenever $1 = \langle f, f'_x, f'_y \rangle$.

We first give a simple argument in the case where $\mathbf{k}$ is algebraically closed and f is irreducible. As a preliminary to the general case, we present after a generalisation of the notion of Hasse-

* Chalmers, University of Göteborg, Sweden, email: coquand@chalmers.se

† Equipe de Mathématiques, CNRS UMR 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25 030 BESANCON cedex, FRANCE, email: henri.lombardi@univ-fcomte.fr

‡ Laboratoire de Mathématiques, SP2MI, Boulevard 3, Teleport 2, BP 179, 86960 FUTUROSCOPE Cedex, FRANCE, email: quitte@mathlabo.univ-poitiers.fr

[1] This notion is particularly interesting logically since it is first-order.

[2] Coherent Prüfer rings are also called *semihereditary rings.* Since a pp-ring is reduced, a ring is a coherent Prüfer ring iff it is arithmetical and a pp-ring.

[3] Using the work [1], it would be possible to show also that this ring is of Krull dimension $\leqslant 1$.

Schmidt derivatives, which has an interest on its own. We then explain what happens in general, and conclude with a `magma` program which follows this argument and some examples.

1 The case where k is algebraically closed and f irreducible

If f is irreducible then $\mathbf{R}$ is a domain. In this case we show that $\mathbf{R}_{f'_y}$ is a Prüfer domain by showing that any localisation $\mathbf{R}_{\mathfrak{p}}$ is a valuation ring, where $\mathfrak{p}$ is a prime ideal not containing f'_y.

If $\mathbf{k}$ is algebraically closed, a non zero prime ideal $\mathfrak{p}$ of $\mathbf{R}$ is on the form $\mathfrak{p} = \langle x-a, y-b\rangle$ where a, b are in $\mathbf{k}$ such that $f(a,b) = 0$. If f'_y is not in $\mathfrak{p}$ this means that we have furthermore $f'_y(a,b) \neq 0$. We simply follow the usual proof that $\mathbf{R}_{\mathfrak{p}}$ is a discrete valuation ring with $x-a$ as uniformising parameter.

For analysing this, we write in $\mathbf{k}[x,y]$

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

with u and v in $\mathbf{k}[x,y]$. One can take v in $\mathbf{k}[y]$, in which case $(y-b)v = -f(a,y) + f(a,b)$. We have then $v(a,b) = -f'_y(a,b) \neq 0$ and, in $\mathbf{R}$

$$0 = (x-a)u - (y-b)v$$

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

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

and hence in $\mathbf{R}$

$$vg = vg(a,b) + (x-a)r_1$$

with $r_1 = pv - qu$. Doing the same operation with r_1 instead of g we get similarly

$$v^2g = v^2g(a,b) + (x-a)vg_1 + (x-a)^2r_2$$

with $g_1 = r_1(a,b)$. In general, we have an equality

$$v^ng = v^ng(a,b) + (x-a)v^{n-1}g_1 + \ldots + (x-a)^{n-1}vg_{n-1} + (x-a)^nr_n$$

and we have $g_n = r_n(a,b)$ and it is natural to write $g_0 = g(a,b)$.

If $g \neq 0$ in $\mathbf{R}$ then the resultant $d = Res_y(f,g)$ in $\mathbf{k}[x]$ is non zero. We can write $d = \sigma f + \theta g$ in $\mathbf{k}[x,y]$ and so $d = \theta g$ in $\mathbf{R}$. If $g_0 = \ldots = g_{n-1} = 0$ we have in $\mathbf{R}$

$$(*) \qquad v^nd = (x-a)^nr_n\theta$$

Since $f'_y(a,b) \neq 0$ we have that $x-a$ and f are relatively prime in $\mathbf{k}[x,y]$ and so $x-a$ is regular in $\mathbf{R}$. (Otherwise $x-a$ divides f and so divides f'_y and $f'_y(a,b) = 0$.) If we write $d = u_0 + (x-a)u_1 + \ldots$, with $u_0, u_1 \ldots$ in $\mathbf{k}$, using the fact that $x-a$ is regular in $\mathbf{R}$, the equality $(*)$ implies that $u_i = 0$ for $i < n$ and hence $(x-a)^n$ divides d in $\mathbf{k}[x]$. It follows that there exists n such that $g_0 = \ldots = g_{n-1} = 0$ and $g_n \neq 0$. (We can have $n = 0$ in which case $g_0 \neq 0$.) The integer n is the (discrete) valuation of g at $\mathfrak{p}$.

If g and h are two elements of $\mathbf{k}[x,y]$ that are non zero mod. $\langle f\rangle$ we have that g divides h in $\mathbf{R}_{\mathfrak{p}}$ iff the valuation of g is $\leqslant$ the valuation of h.

2 A generalisation of Hasse-Schmidt derivatives

From now on, all our arguments are constructive, following [3, 4]. Let $\mathbf{B}$ a commutative ring, and a, b two elements of $\mathbf{B}$. We write $\delta_0 : \mathbf{B}[x, y] \to \mathbf{B}$ the evaluation $\delta_0(t) = t(a, b)$. We may write t_0 instead of $\delta_0(t)$. 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 are going to define a family of maps $\delta_n : \mathbf{B}[x, y] \to \mathbf{B}$ so that, intuitively, the formal power serie $\sum_{i=0}^{\infty} \delta_i(g)t^i$ represents the development of the function g w.r.t. the parameter $t = (x - a)/v = (y - b)/u$. These functions will satisfy

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

and can be seen as a generalisation of the notion 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 $\Delta(g) = pv - qu$. This is well defined modulo $f - f_0$. Indeed if we have also $g - \delta_0(g) = (x - a)p' - (y - b)q'$ then we can write $p' = p + (y - b)w,\ q' = q + (x - a)w$ with w in $\mathbf{B}[x, y]$ and then

$$p'v - q'u = pv - qu - w((x - a)u - (y - b)v) = (pv - qu) - w(f - f_0)$$

Also if we have $h = g + w(f - f_0)$ and $g - g_0 = (x - a)p - (y - b)q$ then

$$h - h_0 = (x - a)(p + wu) - (y - b)(q + wv)$$

and $(p + wu)v - (q + wv)u$ is equal to $pv - qu$.

Hence we have defined a $\mathbf{B}$-linear map $\Delta : \mathbf{B}[x, y]/\langle f - f_0\rangle \to \mathbf{B}[x, y]/\langle f - f_0\rangle,\ g \longmapsto pv - qu$ (for $g - g_0 = (x - a)p - (y - b)q$). We define $\delta_n : \mathbf{B}[x, y]/\langle f - f_0\rangle \to \mathbf{B}$ by

$$\delta_n = \delta_0 \circ \Delta^n$$

We show next that $\Delta(gh) = g\Delta(h) + \delta_0(h)\Delta(g)$ in $\mathbf{B}[x, y]/\langle f - f_0\rangle$. For this, we write

$$g - g_0 = (x - a)p - (y - b)q, \qquad h - h_0 = (x - a)p' - (y - b)q'$$

and

$$gh - g_0h_0 = (h - h_0)g + (g - g_0)h_0 = (x - a)(gp' + h_0p) - (y - b)(gq' + h_0q)$$

so that

$$(gp' + h_0p)v - (gq' + h_0q)u = g(p'v - q'u) + h_0(pv - qu) = g\Delta(h) + \delta_0(h)\Delta(g)$$

By symmetry we have as well $\Delta(gh) = h\Delta(g) + \delta_0(g)\Delta(h)$.

We can iterate the previous equality

$$\Delta^2(gh) = g\Delta^2(h) + \delta_1(h)\Delta(g) + \delta_0(h)\Delta^2(g)$$

and more generally

$$\Delta^n(gh) = g\Delta^n(h) + \sum_{i=1}^{n} \delta_{n-i}(h)\Delta^i(g)$$

If we apply δ_0 we get

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

Lemma 2.1 *We have $h\Delta^n(g) = g\Delta^n(h)$ in $\mathbf{B}/\langle f - f_0\rangle$ modulo $\delta_0(g), \dots, \delta_{n-1}(g), \delta_0(h), \dots, \delta_{n-1}(h)$.*

Proof. The equality $\Delta^n(gh) = g\Delta^n(h) + \sum_{i=1}^n \delta_{n-i}(h)\Delta^i(g)$ gives

$$h\Delta^n(g) - g\Delta^n(h) = \sum_{i=1}^n \delta_{n-i}(g)\Delta^i(h) - \sum_{i=1}^n \delta_{n-i}(h)\Delta^i(g)$$

hence the result. □

As said above, we can consider the map $\mathbf{B}[x, y]/\langle f - f_0\rangle \to \mathbf{B}[[t]],\ g \mapsto \sum_{i=0}^\infty \delta_i(g)t^i$ and the equality $\delta_n(gh) = \sum_{i+j=n} \delta_i(g)\delta_j(h)$ shows that this is a map of $\mathbf{B}$-algebras. One can ask when this map is injective.

Lemma 2.2 *If we have d in $\langle f, g\rangle \cap \mathbf{B}[x]$ which is* primitive*, so that we can write $d = \sum_{i=0}^n u_i x^i$ with $1 = \langle u_0, \dots, u_n\rangle$ in $\mathbf{B}$ then $D(\delta_0(f'_y))$ is covered by $D(\delta_0(f), \delta_0(g), \dots, \delta_n(g))$ in the Zariski spectrum of $\mathbf{B}$.*

Proof. We can write $d = \sum_{i=0}^n c_i(x - a)^i$ and we have $1 = \langle u_0, \dots, u_n\rangle = \langle c_0, \dots, c_n\rangle$. We have also in $\mathbf{B}[x, y]$ an equality of the form $d = Af + Bg$. This shows that $c_0 = \delta_0(d)$ is in $\langle \delta_0(f), \delta_0(g)\rangle$.

Using $\delta_n(gh) = \sum_{i+j=n} \delta_i(g)\delta_j(h)$ one shows by induction that $\delta_k((x - a)^j) = 0$ if $j > k$ and $\delta_k((x - a)^k) = \delta_0(v)^k = (-\delta_0(f'_y))^k$. We have also $\delta_k(f) = 0$ if $k > 0$.

We let $\mathbf{C}$ be the ring $\mathbf{B}$ quotiented by $\delta_0(f), \delta_0(g), \dots, \delta_n(g)$ and localised in $\delta_0(f'_y)$. The Lemma states that the ring $\mathbf{C}$ is trivial. We know already that $c_0 = 0$ in $\mathbf{C}$. If we apply δ_1 to $\sum_{i=0}^n c_i(x - a)^i = Af + Bg$ we get $c_1 = 0$ in $\mathbf{C}$. Similarly we show $c_2 = \ldots = c_n = 0$ in $\mathbf{C}$ and hence $1 = 0$ in $\mathbf{C}$, as expected. □

Notice that this reasoning shows actually that $D(\delta_0(f'_y)) \leqslant D(\delta_0(f), \delta_0(g), \dots, \delta_m(g))$ as soon as $1 = \langle u_0, \dots, u_m\rangle$.

3 The general case

We consider the case where $\mathbf{k}$ is a discrete field and f is an arbitrary polynomial in $\mathbf{k}[x, y]$. An important result we use is that polynomial rings over fields are gcd domain [4] (which can be seen as a constructive version of the fact that such rings are classically unique factorisation domain). As before we write $\mathbf{R}$ for the ring $\mathbf{k}[x, y]$ quotiented by f. We let $\mathbf{A}$ be the localisation $\mathbf{R}_{f'_y}$. Given two elements g and h of $\mathbf{k}[x, y]$ we show how to build a finite covering of the Zariski spectrum of $\mathbf{A}$ by elements $D(w)$ such that g divides h or h divides g in each localisation $\mathbf{A}_w$.

We shall need the following general result about Gröbner basis.

Lemma 3.1 *Let $\mathbf{k}[\underline{a}, \underline{x}] = \mathbf{k}[a_1, \dots, a_m, x_1, \dots, x_n]$ with a monomial ordering $\preceq$ and I an ideal of $\mathbf{k}[\underline{a}]$ of initial monomial ideal $\mathrm{init}_\preceq(I) \subseteq \mathbf{k}[\underline{a}]$. If $J = I\mathbf{k}[\underline{a}, \underline{x}]$ we have $\mathrm{init}_\preceq(J) = \mathrm{init}_\preceq(I)\mathbf{k}[\underline{a}, \underline{x}] = \mathrm{init}_\preceq(I)\mathbf{k}[\underline{x}]$ and for $f \in \mathbf{k}[\underline{x}]$ and $r \in \mathbf{k}[\underline{a}, \underline{x}]$ we have an equality of normal form w.r.t. J*

$$N(rf) = N(r)f$$

We explain first why the localisation $\mathbf{A}$ is a pp-ring.

Lemma 3.2 *Each divisor h of f in $\mathbf{k}[x, y]$ determines an idempotent e_h in $\mathbf{A}$ such that $\langle h\rangle = \langle e_h\rangle$ in $\mathbf{A}$.*

Proof. We have $f = hq$ and hence $f'_y = h'_y q + hq'_y$. In $\mathbf{R}$ we have $hq = 0$ and $f'_y h = q'_y h^2$. In $\mathbf{A}$ we have $h = {f'_y}^{-1} q'_y h^2$ and $e_h = {f'_y}^{-1} q'_y h$ is an idempotent such that $\langle h\rangle = \langle e_h\rangle$. □

Proposition 3.3 $\mathbf{A}$ *is a pp-ring.*

Proof. If g is an element in $\mathbf{k}[x,y]$ then $\mathrm{Ann}(g) = \langle h\rangle$ in $\mathbf{R}$ with $h = f/\mathrm{gcd}(f,g)$. Indeed since h and $g/\mathrm{gcd}(f,g)$ are relatively prime in $\mathbf{k}[x,y]$

$$f|wg \;\Leftrightarrow\; h|w\frac{g}{\mathrm{gcd}(f,g)} \;\Leftrightarrow\; h|w$$

It follows that, in $\mathbf{A}$, we have $\mathrm{Ann}(g) = \langle e_h\rangle$. □

Let g be an element of $\mathbf{k}[x,y]$. We can write $g = k_1 \dots k_n g_n$ where each k_i divides f and g_n, f are relatively prime in $\mathbf{k}[x,y]$. For each k_i we can find an idempotent e_i of $\mathbf{A}$ such that $\langle k_i\rangle = \langle e_i\rangle$ in $\mathbf{A}$ by Lemma 3.2. Notice also that $D(e_i)$, $D(1-e_i)$ is a partition of the Zariski spectrum of $\mathbf{A}$ and that k_i is invertible in $\mathbf{A}_{e_i}$ and zero in $\mathbf{A}_{1-e_i}$. It follows that, in the problem of finding a covering of the Zariski spectrum of $\mathbf{A}$ 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 polynomial g and f are relatively prime in $\mathbf{k}[x,y]$.

Lemma 3.4 *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 $u_0 = g, v_0 = h, u_1, v_1, \dots, u_n, v_n$ in $\mathbf{k}[x,y]$ such that $v_i g = u_i h$ for $i = 0, \dots, n$ and $D(f'_y)$ is covered by $D(u_0), D(v_0), \dots, D(u_n), D(v_n)$ in the Zariski spectrum of $\mathbf{R}$.*

Proof. 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 use the notations and results of the previous section. Given g and h in $\mathbf{k}[x,y]$ we write $g_i = \delta_i(g)$, $h_i = \delta_i(h)$ in $\mathbf{B}$ and $r_i = \Delta^i(g)$, $s_i = \Delta^i(h)$ in $\mathbf{B}[x,y]$[4]. Let us write I_n for the sequence $f_0, g_0, h_0, \dots, g_{n-1}, h_{n-1}$ of elements in $\mathbf{B}$. By Lemma 2.1, we have $hr_n = gs_n$ modulo $\langle f, I_n\rangle$. This means that we have an equality of the form $r_n h - s_n g = ft$ mod. $\langle I_n\rangle$ for some t in $\mathbf{k}[a,b,x,y]$. Let us write $N(p)$ the normal form of an element p in $\mathbf{k}[a,b,x,y]$ w.r.t. a Gröbner basis of the ideal generated by I_n and let p_n be $N(r_n)$ and q_n be $N(s_n)$. We have by Lemma 3.1 since f, g, h are in $\mathbf{k}[x,y]$

$$N(r_n h - s_n g) = p_n h - q_n g = N(ft) = fN(t)$$

and hence in $\mathbf{k}[a,b,x,y]$

$$p_n h = q_n g \quad \text{mod. } \langle f\rangle$$

In particular, if we write $u_n = p_n(x,y,x,y)$ and $v_n = q_n(x,y,x,y)$ in $\mathbf{k}[x,y]$ (notice that $u_0 = p_0 = g$ and $v_0 = q_0 = h$)

$$u_n h = v_n g \quad \text{mod. } \langle f\rangle$$

Also, by construction, we have $p_n = r_n$ and $q_n = s_n$ modulo $\langle I_n\rangle$. Hence, modulo $\langle I_n\rangle$

$$u_n(a,b) = \delta_0(r_n) = g_n$$

$$v_n(a,b) = \delta_0(s_n) = h_n$$

It follows that, in the Zariski spectrum of $\mathbf{R}$

$$D(g_0(x,y), h_0(x,y), \dots, g_n(x,y), h_n(x,y)) = D(u_0, v_0, \dots, u_n, v_n)$$

and we have finished since, by Lemma 2.2, there exists n such that $D(f'_y)$ is covered by $D(g_0(x,y), \dots, g_n(x,y))$. □

[4] More precisely, we take for r_i and s_i a represent in $\mathbf{B}[x,y]$ of $\Delta^i(g), \Delta^i(h)$, that are only defined modulo $f - f_0$.

Theorem 3.5 *The ring $\mathbf{A} = \mathbf{R}_{f'_y}$ is a coherent Prüfer ring.*

Corollary 3.6 *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.*

Proof. The ring $\mathbf{R}$ is arithmetical, reduced and coherent since each ring $\mathbf{R}_{f'_x}$ and $\mathbf{R}_{f'_y}$ is arithmetical, reduced and coherent. □

4 Examples

In all examples and in the program `magma`, we use the graded reverse lexicographical order on $\mathbf{k}[a,b,x,y]$.

4.1 Example 1

We consider $f = x^2 + y^2 - 1$ and $g = 2x^2 - 1$ and $h = x - y$. We write

$$f - f(a,b) = (x-a)(x+a) + (y-b)(y+b)$$

so that $u = x + a$ and $v = -(y+b)$. We have then

$$g = g_0 + 2(x-a)(x+a), \qquad h = h_0 + (x-a) - (y-b)$$

so that

$$r_1 = -2(y+b)(x+a), \qquad s_1 = -(x+y+a+b)$$

We compute the normal form of $s_1 g$ and $r_1 h$ mod. $\langle f_0, g_0, h_0 \rangle$.

$$p_1 = -2xy - 2b(x+y) - 1, \qquad q_1 = -(x+y+2b)$$

and so

$$u_1 = -2y^2 - 4xy - 1, \qquad v_1 = -(x+3y)$$

We can check the identity $gv_1 = hu_1$ mod. f.

4.2 Example 2

We take $f = y^2 + x^4 - 1$ and $g = x$ and $h = 1 - y$. We write

$$f - f(a,b) = (x-a)(x^3 + x^2a + xa^2 + a^3) + (y-b)(y+b)$$

so that $u = x^3 + x^2a + xa^2 + a^3$ and $v = -(y+b)$. We have then

$$g = g_0 + x - a \qquad h = h_0 - (y-b)$$

so that

$$r_1 = -(y+b) \qquad s_1 = -(x^3 + x^2a + xa^2 + a^3)$$

We compute the normal form of $s_1 g$ and $r_1 h$ mod. $\langle f_0, g_0, h_0 \rangle$.

$$p_1 = -(y+1) \qquad q_1 = -x^3$$

and so $u_1 = -(y+1)$ and $v_1 = -x^3$.

4.3 Example 3

We take $f = y^3x + x^3 + y$ and $g = y^2x + x^2 + y$ and $h = xy$. This is best done using the following program in magma. The program finds the following identities mod. f

$$(x^3y - x^2y^2 + y^3 + 2x^2 - y^2 - 2x)h = (x^3 - y)g$$

$$(y^5 + x^2y^2 - y^4 - x^2y - x + 1)h = -(y^3 + x^2)g$$

References

[1] Thierry Coquand, Lionel Ducos, Henri Lombardi, and Claude Quitté. Constructive Krull Dimension I: Integral Extensions. To appear in Journal of Algebra and its Applications.

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

[3] H. Lombardi, C. Quitté. *Algèbre Commutative, Modules projectifs de type fini.* forthcoming. Preliminary version available at the home page of H. Lombardi.

[4] Mines, Ray and Richman, Fred and Ruitenburg, Wim. *A Course in Constructive Algebra.* Universitext. New York: Springer, 1988.

Implementation in magma

```
delta0 := function(q)              // q in R[a,b,x,y, ...], retourne q(a,b,a,b, ...)
  A := Parent(q) ;
  return hom <A -> A | [a,b, a,b] cat [A.i : i in [5..Rank(A)]] >(q)
         where a is A.1 where b is A.2 ;
end function ;

ab2xy := function(q)              // q in R[a,b,x,y, ...], retourne q(x,y,x,y, ....)
  A := Parent(q) ;
  return hom <A -> A | [x,y] cat [A.i : i in [3..Rank(A)]]>(q)
         where x is A.3 where y is A.4 ;
end function ;

Composantes := function(f)        // f in R[a,b,x,y, ....]
  // f(x,y) - f(a,b) = (x-a)*p - (y-b)*q
  // p = p(a,b,x,y),   q = q(a,b,y)
  A := Parent(f) ;   a := A.1 ; b := A.2 ; x := A.3 ;  y := A.4 ;
  fay := Evaluate(f, x, a) ;   // f(a,b,a,y)
  f0 := delta0(f) ;
  // faire x = a pour determiner q qui ne depend pas de x
  q := -ExactQuotient(fay - f0, y-b) ;
  p := ExactQuotient(f - f0 + (y-b)*q, x-a) ;
  assert f - f0 eq (x-a)*p - (y-b)*q ;
  return p, q ;
end function ;

Delta := function(f, g)       // f, g in R[a,b,x,y, ....]
  A := Parent(f) ;
  u, v := Composantes(f) ;     p, q := Composantes(g) ;
  r := p*v - q*u ;
  assert v*g eq v*delta0(g) + (x-a)*r + q*(f-delta0(f)) where a is A.1 where x is A.3 ;
  return r, q ;
end function ;

Developpement := function(f, g, N)  // f, g in R[a,b,x,y, ...]
  A := Parent(f) ;   a := A.1 ; x := A.3 ;
  _, v := Composantes(f) ;    Df := f - delta0(f) ;
  G := [A |] ;    r := g ;   q := 0 ;
  for n := 1 to N do
     // G of length n-1
     assert v^(n-1) * g eq
          &+[A| G[i]*(x-a)^(i-1) * v^(n-i) : i in [1..n-1]] + r*(x-a)^(n-1) + q*Df ;
     Append(~G, delta0(r)) ;  // G[n] = r(a,b, a,b)
     old_r := r ;
     r, q2 := Delta(f, r) ;
     assert v*old_r eq v*G[n] + (x-a)*r + q2*Df ;
     q := q2*(x-a)^(n-1) + v*q ;
  end for ;
  Append(~G, r) ;
  assert #G eq N+1 ;
  assert v^N * g eq &+[A| G[i+1]*(x-a)^i * v^(N-i) : i in [0..N]] + q*Df ;
  return G, q ;
end function ;

Developpements := function(f, g, h, n)
  // Retourne
  // G = [g_0, g_1, ..., g_n], H = [h_0, h_1, ..., u_n]
  // U = [u_0, u_1, ..., u_n], V = [v_0, v_1, ..., v_n]
  // with g_i, h_i, u_i, v_i in k[x,y, ....]
  // P = [p_0, p_1, ..., p_n], Q = [q_0, q_1, ..., q_n]
  // with p_i, q_i in k[a,b,x,y, ...]
  A := Parent(f) ;  a := A.1 ; x := A.3 ;
  f0 := delta0(f) ;  // f0 := f(a,b)
  _, w := Composantes(f) ;
  // G, H, U, V, P, Q : polynomes in A
  G := [A| ] ; H := [A| ] ; U := [A| ] ; V := [A| ] ; P := [A| ] ; Q := [A| ] ;
  // r contains r_0, r_1, ... Idem s contains s_0, s_1, ...
  r := g ;  s := h ;
  qg := 0 ;  qh := 0 ;

  for k := 0 to n do
    // G = [g_0, ..., g_{k-1}],  H = [h_0, ..., h_{k-1}],
    // U = [u_0, ..., u_{k-1}],  V = [v_0, ..., v_{k-1}]
    // P = [p_0, ..., p_{k-1}],  Q = [q_0, ..., q_{k-1}]
    // r = r_k,  s = s_k
    G0 := [delta0(gi) : gi in G] ;  H0 := [delta0(hi) : hi in H] ;

    assert w^k * g eq
      &+[A| G0[i+1]*(x-a)^i*w^(k-i) : i in [0..k-1]] + r*(x-a)^k + qg*(f-f0) ;
    assert w^k * h eq
      &+[A| H0[i+1]*(x-a)^i*w^(k-i) : i in [0..k-1]] + s*(x-a)^k + qh*(f-f0) ;
    // Calcul de u_k et v_k
    I := ideal < A | f0, G0, H0 > ;
    p := NormalForm(r,I) ;  q := NormalForm(s,I) ;
    Append(~P, p) ;  Append(~Q, q) ;
    u := ab2xy(p) ;  v := ab2xy(q) ;
    assert IsDivisibleBy(v*g - u*h, f) ;
    // Calcul de g_k et h_k
    Append(~U, u) ;         Append(~V, v) ;
    Append(~G, ab2xy(r)) ;  Append(~H, ab2xy(s)) ;
    assert [U[k+1]-G[k+1], V[k+1]-H[k+1]] subset ideal <A | f,G[1..k],H[1..k]> ;
    assert ideal <A | f, G, H> eq ideal <A | f, U, V> ;
    // Computation of r_{k+1} et s_{k+1}
    r, qr := Delta(f, r) ;  s, qs := Delta(f, s) ;
    qg := qr*(x-a)^k + w*qg ;  qh := qs*(x-a)^k + w*qh ;
    // G = [g_0, ..., g_k],  H = [h_0, ..., h_k],
    // U = [u_0, ..., u_k],  V = [v_0, ..., v_k]
    // P = [p_0, ..., p_k],  Q = [q_0, ..., q_k]
    // r = r_{k+1},  s = s_{k+1}
  end for ;

  G0 := [delta0(gi) : gi in G] ;  H0 := [delta0(hi) : hi in H] ;
  assert w^(n+1) * g eq
    &+[A| G0[i+1]*(x-a)^i * w^(n+1-i) : i in [0..n]] + r*(x-a)^(n+1) + qg*(f-f0) ;
  assert w^(n+1) * h eq
    &+[A| H0[i+1]*(x-a)^i * w^(n+1-i) : i in [0..n]] + s*(x-a)^(n+1) + qh*(f-f0) ;

  return G, H, U, V, P, Q ;
end function ;
// the first example

load "PlaneCurveTools.magma" ;
k := RationalField() ;   kabxy<a,b,x,y> := PolynomialRing(k, 4) ;
f := x^2 + y^2 - 1 ;
Composantes(f) ;
g := 2*x^2 - 1 ;  h := x - y ;
g0, r1 := Explode(Developpement(f, g, 1)) ;
g0, r1 ;
h0, s1 := Explode(Developpement(f, h, 1)) ;
h0, s1 ;

G, H, U, V, P, Q := Developpements(f, g, h, 1) ;
1 in ideal < kabxy | f, G> ;
1 in ideal < kabxy | f, H> ;
1 in ideal < kabxy | f, U> ;
1 in ideal < kabxy | f, V> ;
> f := x^2 + y^2 - 1 ;
> Composantes(f) ;
a + x
-b - y
> g := 2*x^2 - 1 ;  h := x - y ;
> g0, r1 := Explode(Developpement(f, g, 1)) ;
> g0, r1 ;
2*a^2 - 1
-2*a*b - 2*a*y - 2*b*x - 2*x*y
> h0, s1 := Explode(Developpement(f, h, 1)) ;
> h0, s1 ;
a - b
-a - b - x - y
>
> G, H, U, V, P, Q := Developpements(f, g, h, 1) ;
> 1 in ideal < kabxy | f, G> ;
true
> 1 in ideal < kabxy | f, H> ;
true
> 1 in ideal < kabxy | f, U> ;
false
> 1 in ideal < kabxy | f, V> ;
true
> G ;
[
    2*x^2 - 1,
    -8*x*y
]
> H ;
[
    x - y,
    -2*x - 2*y
]
> U ;
[
    2*x^2 - 1,
    -4*x*y - 2*y^2 - 1
]
> V ;
[
    x - y,
    -x - 3*y
]
> P ;
[
    2*x^2 - 1,
    -2*b*x - 2*b*y - 2*x*y - 1
]
> Q ;
[
    x - y,
    -2*b - x - y
]

// Example 2
load "PlaneCurveTools.magma" ;
k := RationalField() ;   kabxy<a,b,x,y> := PolynomialRing(k, 4) ;
f := y^2 + x^4 - 1 ;
Composantes(f) ;
g := x ;  h := 1-y ;
```

```
g0, r1 := Explode(Developpement(f, g, 1)) ;
g0, r1 ;
h0, s1 := Explode(Developpement(f, h, 1)) ;
h0, s1 ;
G, H, U, V, P, Q := Developpements(f, g, h, 1) ;
1 in ideal < kabxy | f, G> ;
1 in ideal < kabxy | f, H> ;
1 in ideal < kabxy | f, U> ;
1 in ideal < kabxy | f, V> ;
1 in ideal < kabxy | f, U, V> ;
> f := y^2 + x^4 - 1 ;
> Composantes(f) ;
a^3 + a^2*x + a*x^2 + x^3
-b - y
> g := x ;  h := 1-y ;
> g0, r1 := Explode(Developpement(f, g, 1)) ;
> g0, r1 ;
a
-b - y
> h0, s1 := Explode(Developpement(f, h, 1)) ;
> h0, s1 ;
-b + 1
-a^3 - a^2*x - a*x^2 - x^3
>
> G, H, U, V, P, Q := Developpements(f, g, h, 1) ;
> 1 in ideal < kabxy | f, G> ;
true
> 1 in ideal < kabxy | f, H> ;
false
> 1 in ideal < kabxy | f, U> ;
false
> 1 in ideal < kabxy | f, V> ;
false
> 1 in ideal < kabxy | f, U, V> ;
true
> G ;
[
    x,
    -2*y
]
> H ;
[
    -y + 1,
    -4*x^3
]
> U ;
[
    x,
    -y - 1
]
> V ;
[
    -y + 1,
    -x^3
]
> P ;
[
    x,
    -y - 1
]
> Q ;
[
    -y + 1,
    -x^3
]
// Example 3
// Here, Z is the base ring
load "PlaneCurveTools.magma" ;
Z := IntegerRing() ;   Zabxy<a,b,x,y> := PolynomialRing(Z, 4) ;
f := y^3*x + x^3 + y ;
g := y^2*x + x^2 + y ; h := x*y ;
G, H, U, V := Developpements(f, g, h, 2) ;
1 in ideal < Zabxy | f, G> ;
3 in ideal < Zabxy | f, G> ;
1 in ideal < Zabxy | f, H> ;
3 in ideal < Zabxy | f, U> ;
1 in ideal < Zabxy | f, V> ;
1 in ideal < Zabxy | f, U, V> ;
> f := y^3*x + x^3 + y ;
> g := y^2*x + x^2 + y ; h := x*y ;
> G, H, U, V := Developpements(f, g, h, 2) ;
> 1 in ideal < Zabxy | f, G> ;
false
> 3 in ideal < Zabxy | f, G> ;
true
> 1 in ideal < Zabxy | f, H> ;
false
> 3 in ideal < Zabxy | f, U> ;
false
> 1 in ideal < Zabxy | f, V> ;
false
> 1 in ideal < Zabxy | f, U, V> ;
true
> G ;
```

```
[
    x^2 + x*y^2 + y,
    6*x^3*y - 6*x^2*y^2 + 3*x^2 - x*y^4 - 2*x + y^3 - y^2,
    9*x^5 - 18*x^4*y - 21*x^3*y^3 + 3*x^2*y^4 - 12*x^2*y - 2*x*y^6 + 6*x*y^2 -
        3*x + 3*y^5 - 2*y^4 + 1
]
> H ;
[
    x*y,
    3*x^3 - 2*x*y^3 - y,
    -18*x^3*y^2 - 6*x^2 - 3*x*y^5 - y^3
]
> U ;
[
    x^2 + x*y^2 + y,
    x^3*y - x^2*y^2 + 2*x^2 - 2*x + y^3 - y^2,
    x^2*y^2 - x^2*y - x + y^5 - y^4 + 1
]
> V ;
[
    x*y,
    x^3 - y,
    -x^2 - y^3
]
```