Some known results on polynomial factorization over towers of field extensions

Guénaël Renault, Éric Schost

July 21, 2009

1 Jacobians and conductors: the irreducible case

We consider the polynomial ring $\mathbb{S}[t_1, \dots, t_n]$, with either:

- $\mathbb{S} = \mathbb{Z}$
- or $\mathbb{S} = \mathbb{F}_q$, with q a prime power, and in this case $n > 0$.

We let $\mathbb{K}$ be the fraction field of $\mathbb{S}$ and introduce the field of fractions $\mathbb{K}(t_1, \dots, t_n)$; we are interested in a field extension $\mathbb{L}$ of $\mathbb{K}(t_1, \dots, t_n)$ of the form

$$\mathbb{L} = \mathbb{K}(t_1, \dots, t_n)[x_1, \dots, x_k]/\langle f_1, \dots, f_k \rangle,$$

where for $i = 1, \dots, k$, f_i is in $\mathbb{K}(t_1, \dots, t_n)[x_1, \dots, x_i]$ and monic in x_i (thus, the ideal $\langle f_1, \dots, f_k \rangle$ is maximal). Hereafter, we write $\mathbf{t} = t_1, \dots, t_n$, $\mathbf{x} = x_1, \dots, x_k$ and $d_i = \deg(f_i, x_i)$; for $i = 1, \dots, k$, we let h_i be in $\mathbb{S}[\mathbf{t}]$ such that $f_i^\star = h_i f_i$ is in $\mathbb{S}[\mathbf{t}, \mathbf{x}]$ and we set $h = h_1 \cdots h_k$.

We are interested in the possible denominators arising when factoring univariate polynomials modulo $\langle f_1, \dots, f_k \rangle$. Precisely, we say that $\delta \in \mathbb{S}[\mathbf{t}] - \{0\}$ is a *common denominator* for $(f_1, \dots, f_k)$ if the following property holds. Let A, B, C in $\mathbb{K}(\mathbf{t})[\mathbf{x}, Y]$ and α in $\mathbb{S}[\mathbf{t}]$ be such that:

1. A, B, C are reduced with respect to $(f_1, \dots, f_k)$, in the sense that $\deg(A, x_i) < d_i$, $\deg(B, x_i) < d_i$ and $\deg(C, x_i) < d_i$ hold for all i;
2. $A = BC$ in $\mathbb{L}[Y]$;
3. αA is in the subring $\mathbb{S}[\mathbf{t}, \mathbf{x}, Y]$ of $\mathbb{K}(\mathbf{t})[\mathbf{x}, Y]$;
4. A, B, C are monic in Y.

Then, $\alpha \delta h^b B$ and $\alpha \delta h^c C$ are in $\mathbb{S}[\mathbf{t}, \mathbf{x}, Y]$, for some non-negative integers b, c (remark that our criterion is rather loose, as we impose no control on b and c, but sufficient for the application we have in mind).

Proposition 1. *Let* $\Delta \in \mathbb{K}(\mathbf{t})[\mathbf{x}]$ *be a* $k \times k$*-minor of the Jacobian matrix of* $(f_1, \ldots, f_k)$ *with respect to* $(t_1, \ldots, t_n, x_1, \ldots, x_k)$*, and let*

$$\delta = \mathrm{res}(\cdots \mathrm{res}(\Delta, f_k, x_k), \cdots, f_1, x_1).$$

Then, if $\delta \neq 0$*, there exists an integer* $d \geq 0$ *such that* $h^d \delta$ *is a common denominator of* $(f_1, \ldots, f_k)$*.*

Suppose for simplicity that f_i is in $\mathbb{S}[\mathbf{t}, \mathbf{x}]$ for all i, so $h = 1$. For $i \geq 1$, let Δ_i be the partial derivative of f_i with respect to x_i, and let $\Delta = \Delta_1 \cdots \Delta_k$ and let as before δ be the iterated resultant

$$\delta = \mathrm{res}(\cdots \mathrm{res}(\Delta, f_k, x_k), \cdots, f_1, x_1) \in \mathbb{S}[\mathbf{t}].$$

If $\mathbb{K} \to \mathbb{L}$ is separable, it is known [1] that δ is non-zero and that it is a common denominator for $(f_1, \ldots, f_k)$. If $\mathbb{K} \to \mathbb{L}$ is not separable, though, $\delta = 0$. In this case, the proposition states that instead of considering Δ, some other $k \times k$ minor of the Jacobian matrix of $(f_1, \ldots, f_k)$ with respect to the whole set of variables $\mathbf{t}$ and $\mathbf{x}$ may do (actually, such a non-zero δ always exists). This result is not new; however, since it seems not widely known, it seems useful to restate it here.

Consider for example the simplest such case, with $n = k = 1$ (so we write $t_1 = t$, $x_1 = x$ and $f_1 = f$), $\mathbb{K} = \mathbb{S} = \mathbb{F}_p$ and $f(t, x) = x^p - \varphi(t)$, with $\varphi \in \mathbb{F}_p[t]$ not a pth power. In this case, $\delta = \partial f / \partial x = 0$; however, $\partial f / \partial t = -\varphi' \in \mathbb{F}_p[t]$ is non-zero (otherwise f would be a pth power). Then, φ' is a common denominator for f; in this case, there is no need to take resultants, since φ' is already in $\mathbb{F}_p[t]$. For instance, the polynomial $Y^p - t$ factors modulo f as

$$Y^p - t = \left(Y - \frac{G(t, x)}{\varphi'} \right)^p,$$

with $G(t, x)$ in $\mathbb{F}_p[t, x]$.

The rest of this section is devoted to prove the former proposition. Let Z be a new indeterminates, and define $\mathbb{A}$ as the residue class ring $\mathbb{S}[\mathbf{t}, \mathbf{x}, Z]/\langle f_1^\star, \ldots, f_k^\star, 1 - hZ \rangle$. One easily checks that $\mathbb{A}$ is an integral domain, with field of fractions $\mathbb{L} = \mathbb{K}(\mathbf{t})[\mathbf{x}]/\langle f_1, \ldots, f_k \rangle$.

Let $\mathbb{B} \subset \mathbb{L}$ be the integral closure of $\mathbb{A}$. The *conductor* $\mathfrak{C} \subset \mathbb{A}$ of the extension $\mathbb{A} \to \mathbb{B}$ is the annihilator of the $\mathbb{A}$-module $\mathbb{B}/\mathbb{A}$; that is, $\delta \in \mathbb{A}$ is in $\mathfrak{C}$ if and only if any b in $\mathbb{B}$ can be written as $b = a/\delta$, with a in $\mathbb{A}$. Following [5], the following classical result in the vein of Gauss' Lemma relates the conductor to our denominator problem.

Lemma 1. *Any* δ *in* $\mathfrak{C} \cap \mathbb{S}[\mathbf{t}] - \{0\}$ *is a common denominator for* $(f_1, \ldots, f_k)$*.*

Proof. Consider $A, B, C \in \mathbb{K}(\mathbf{t})[\mathbf{x}, Y]$ and $\alpha \in \mathbb{S}[\mathbf{t}]$ that satisfy assumptions $1 - 4$. Thus, αA is in $\mathbb{S}[\mathbf{t}, \mathbf{x}, Y]$, and its residue class in $\mathbb{L}[Y]$ is actually in $\mathbb{A}[Y]$. Following the proof of [5, Lemma 7.1], we deduce that αB and αC are in $\mathbb{B}[Y]$, so that $\alpha \delta B$ and $\alpha \delta C$ are in $\mathbb{A}[Y] \subset \mathbb{B}[Y]$.

Considering B, this means that there exists a polynomial β in $\mathbb{S}[\mathbf{t}, \mathbf{x}, Z, Y]$ such that the residue classes of β and $\alpha \delta B$ coincide in $\mathbb{L}[Y]$. Since the normal form of β in $\mathbb{L}$ admits a power of h as a denominator, there exists $b \geq 0$ such that $\alpha \delta h^b B$ is in $\mathbb{S}[\mathbf{t}, \mathbf{x}, Y]$. ∎

The following result exhibits elements in the conductor. It is a direct consequence of the Lipman-Sathaye theorem [3] when $\mathbb{S} = \mathbb{Z}$, and is in [4, Remark 1.5] when $\mathbb{S} = \mathbb{F}_q$.

Lemma 2. *Any $(k+1) \times (k+1)$-minor of the Jacobian matrix of $(f_1^\star, \dots, f_k^\star, 1 - hZ)$ with respect to $(t_1, \dots, t_n, x_1, \dots, x_k, Z)$ is in $\mathfrak{C}$.*

From this, one can exhibit an element in the conductor using only data obtained from $(f_1, \dots, f_k)$.

Lemma 3. *Let $\Delta \in \mathbb{K}(\mathbf{t})[\mathbf{x}]$ be a $k \times k$-minor of the Jacobian matrix of $(f_1, \dots, f_k)$ with respect to $(t_1, \dots, t_n, x_1, \dots, x_k)$. Then, there exists an integer $d \geq 0$ such that $h^d \Delta$ is $\mathbb{S}[\mathbf{t}, \mathbf{x}]$, and in $\mathfrak{C}$.*

Proof. Let us define the following matrices:

- $J_{\mathbf{f}}$ is the Jacobian matrix of $(f_1, \dots, f_k)$ with respect to $(t_1, \dots, t_n, x_1, \dots, x_k)$,
- $J_{\mathbf{f}^\star}$ is the Jacobian matrix of $(f_1^\star, \dots, f_k^\star)$ with respect to $(t_1, \dots, t_n, x_1, \dots, x_k)$,
- $K_{\mathbf{f}^\star}$ is the Jacobian matrix of $(f_1^\star, \dots, f_k^\star, 1 - hZ)$ with respect to $(t_1, \dots, t_n, x_1, \dots, x_k, Z)$.

Let next $I \subset \{1, \dots, n\}$ and $J \subset \{1, \dots, k\}$ be such that Δ is built on columns of $J_{\mathbf{f}}$ indexed by $(t_i, i \in I)$ and $(x_j, j \in J)$, and let $\Delta^\star$ be the $k \times k$-minor of $J_{\mathbf{f}^\star}$ built on the same columns. Consider the equalities

$$\frac{\partial f_i^\star}{\partial t_j} = \frac{\partial h_i}{\partial t_j} f_i + h_i \frac{\partial f_i}{\partial t_j} \quad \text{and} \quad \frac{\partial f_i^\star}{\partial x_j} = h_i \frac{\partial f_i}{\partial x_j}.$$

It follows that in $\mathbb{K}(\mathbf{t})[\mathbf{x}]$, $\Delta^\star$ equals $h\Delta$ modulo $\langle f_1, \dots, f_k \rangle$. Multiplying by a large enough power of h to clear all denominators, we obtain that $h^c \Delta^\star = h^{c+1} \Delta \bmod \langle f_1^\star, \dots, f_k^\star \rangle$ holds in $\mathbb{S}[\mathbf{t}, \mathbf{x}]$, for some integer $c \geq 0$.

Let finally Γ be the $(k+1) \times (k+1)$-minor of $K_{\mathbf{f}^\star}$ built on columns indexed by Z, $(t_i, i \in I)$ and $(x_j, j \in J)$. Since the column of $J_{\mathbf{f}^\star}$ indexed by Z only contains the non-zero entry h, we deduce that $\Gamma = \pm h \Delta^\star$. This implies that $h^c \Gamma = \pm h^{c+2} \Delta \bmod \langle f_1^\star, \dots, f_k^\star \rangle$ holds in $\mathbb{S}[\mathbf{t}, \mathbf{x}]$. By the previous lemma, Γ, and thus $h^c \Gamma$, are in $\mathfrak{C}$. Thus, $h^{c+2} \Delta$ is in $\mathfrak{C}$ too. ☐

Let $\Delta \in \mathbb{S}[\mathbf{t}, \mathbf{x}]$ be in $\mathfrak{C}$. If Δ is already in $\mathbb{S}[\mathbf{t}]$, we are essentially done. In general, though, Δ may not be in $\mathbb{S}[\mathbf{t}]$ but in $\mathbb{S}[\mathbf{t}, \mathbf{x}]$; the next lemma provides the classical workaround.

Lemma 4. *Let $\Delta \in \mathbb{S}[\mathbf{t}, \mathbf{x}]$ be in $\mathfrak{C}$. Then*

$$\delta = \operatorname{res}(\cdots \operatorname{res}(\Delta, f_k^\star, x_k), \cdots, f_1^\star, x_1)$$

is either zero, or a common denominator of $(f_1, \dots, f_k)$.

Proof. δ is in $\mathbb{S}[\mathbf{t}]$ by construction. A direct induction shows that δ there exists a polynomial β in $\mathbb{S}[\mathbf{t}, \mathbf{x}]$ such that $\Delta\beta = \delta$ in $\mathbb{A}$. Since Δ is in the conductor $\mathfrak{C}$, δ is in $\mathfrak{C}$ as well, so by Lemma 1, it is a common denominator for $(f_1, \dots, f_k)$. ☐

We can now prove Proposition 1. Let $\Delta \in \mathbb{K}(\mathbf{t})[\mathbf{x}]$ be a $k \times k$-minor of the Jacobian matrix of $(f_1, \dots, f_k)$ with respect to $(t_1, \dots, t_n, x_1, \dots, x_k)$. By Lemma 3, there exists an integer $d \geq 0$ such that $h^d \Delta$ is $\mathbb{S}[\mathbf{t}, \mathbf{x}]$ and in $\mathfrak{C}$. By the previous lemma

$$\gamma = \mathrm{res}(\cdots \mathrm{res}(h^d \Delta, f_k^\star, x_k), \cdots, f_1^\star, x_1)$$

is either zero, or a common denominator of $(f_1, \dots, f_k)$; we will assume it is not zero. Taking the factors $h_1, \dots, h_k, h$ out, we see that the polynomial δ can be rewritten as

$$\gamma = h_1^{e_1} \cdots h_k^{e_k} h^e \mathrm{res}(\cdots \mathrm{res}(\Delta, f_k, x_k), \cdots, f_1, x_1),$$

for some non-negative integers $e_1, \dots, e_k, e$; using the notation of Proposition 1, this can be rewritten as $\gamma = h_1^{e_1} \cdots h_k^{e_k} h^e \delta$. Multiplying by suitable powers of $h_1, \dots, h_k$, we deduce

$$h_1^{\ell_1} \cdots h_k^{\ell_k} \gamma = h^\ell \delta,$$

for some non-negative integers $\ell_1, \dots, \ell_k, \ell$. Since $h_1^{\ell_1} \cdots h_k^{\ell_k} \gamma$ is still a common denominator for $(f_1, \dots, f_k)$, we are done.

2 Application

As an application, we consider the following situation. As before, we start from the base ring $\mathbb{S}$, with either $\mathbb{S} = \mathbb{Z}$ or $\mathbb{S} = \mathbb{F}_q$. We still let $\mathbb{K}$ be the fraction field of $\mathbb{S}$, and we consider a triangular family of polynomials $g_1, \dots, g_k$ in $\mathbb{K}(\mathbf{t})[\mathbf{x}]$, with g_i in $\mathbb{K}(\mathbf{t})[x_1, \dots, x_i]$, monic in x_i and reduced with respect to $(g_1, \dots, g_{i-1})$ for all i; we do not assume that the ideal $\langle g_1, \dots, g_k \rangle$ is maximal. Besides, we consider the following data:

- if $\mathbb{S} = \mathbb{Z}$, let $\mathbb{S}' = \mathbb{F}_p$, for some prime p, and let $\tau_1, \dots, \tau_n$ and $\xi_1, \dots, \xi_k$ be in $\mathbb{F}_p$;
- if $\mathbb{S} = \mathbb{F}_q$, let $\mathbb{S}' = \mathbb{F}_q$ and let $\tau_1, \dots, \tau_n$ and $\xi_1, \dots, \xi_k$ be in $\mathbb{F}_q$.

For $0 \leq i \leq k$, let φ_i be the evaluation map

$$\begin{array}{rcccl} \varphi_i : & \mathbb{S}[\mathbf{t}][\mathbf{x}] & \to & \mathbb{S}'[\mathbf{x}] & \\ & t_i & \mapsto & \tau_i & \\ & x_j & \mapsto & \xi_j & j \leq i \\ & x_j & \mapsto & x_j & j > i; \end{array}$$

In particular, φ_0 only evaluates the $\mathbf{t}$ variables, and φ_n evaluates all $\mathbf{t}$ and $\mathbf{x}$ variables. We let D_0 be the following subring of $\mathbb{K}(\mathbf{t})$: $f \in \mathbb{K}(\mathbf{t})$ is in D_0 if and only if it can be written as a/b, with a and b in $\mathbb{S}[\mathbf{t}]$, and with $\varphi_0(b) \neq 0$. If we let $D = D_0[\mathbf{x}]$, all φ_i remain defined at D. Then, we make the following assumptions:

H$_1$. The polynomials $g_1, \dots, g_k$ are in D.

H$_2$. For $\ell \leq k$, $\varphi_n(g_\ell) = 0$.

- $\mathbf{H}_3$. For $\ell \leq k$, either g_ℓ is purely inseparable, or $\varphi_0(\partial g_\ell/\partial x_\ell)$ is invertible in the residue class ring $\mathbb{S}'[x_1, \ldots, x_\ell]/\langle \varphi_0(g_1), \ldots, \varphi_0(g_\ell)\rangle$.

For $\ell \leq k$, let J_ℓ be the Jacobian matrix of $(g_1, \ldots, g_\ell)$ with respect to $(t_1, \ldots, t_n, x_1, \ldots, x_\ell)$. Since all g_i are in D, all entries of J_ℓ are in D. Then, we can define $\varphi_0(J_\ell)$ in the obvious manner, applying φ_0 entrywise, and we make the following further assumption:

- $\mathbf{H}_4$. For $\ell \leq k$, there exists an $\ell \times \ell$ minor Δ_ℓ of J_ℓ such that $\varphi_0(\Delta_\ell)$ is invertible in $\mathbb{S}'[x_1, \ldots, x_\ell]/\langle \varphi_0(g_1), \ldots, \varphi_0(g_\ell)\rangle$.

Remark that if no g_i is purely inseparable, $\mathbf{H}_3$ implies $\mathbf{H}_4$. Under $\mathbf{H}_1, \ldots, \mathbf{H}_4$, our conclusion is the following.

Proposition 2. *Consider $\ell < k$, and suppose that $f_1, \ldots, f_\ell$ are polynomials in $\mathbb{K}(\mathbf{t})[\mathbf{x}]$ such that the following holds:*

1. *for $i \leq \ell$, f_i is in $\mathbb{K}(\mathbf{t})[x_1, \ldots, x_i]$, monic in x_i and reduced with respect to $(f_1, \ldots, f_{i-1})$;*
2. *for $i \leq \ell$, f_i is in D;*
3. *the ideal $\langle f_1, \ldots, f_\ell\rangle$ is maximal in $\mathbb{K}(\mathbf{t})[x_1, \ldots, x_\ell]$ and contains $\langle g_1, \ldots, g_\ell\rangle$.*

Let $f_{\ell+1} \in \mathbb{K}(\mathbf{t})[x_1, \ldots, x_{\ell+1}]$ be a monic factor of $g_{\ell+1}$ modulo $\langle f_1, \ldots, f_\ell\rangle$. Then, $f_{\ell+1}$ is in D.

Proof. We will establish the following claim below: *there exists a common denominator $\gamma \in \mathbb{S}[\mathbf{t}]$ of $(f_1, \ldots, f_\ell)$ such that $\varphi_0(\gamma) \neq 0$.* Taking it for granted, let $\alpha \in \mathbb{S}[\mathbf{t}]$ be such that $\varphi_0(\alpha) \neq 0$ and $\alpha g_{\ell+1}$ is in $\mathbb{S}[\mathbf{t}, x_1, \ldots, x_{\ell+1}]$. Then, applying the characteristic property of γ, we see that $\alpha\gamma h^e f_{\ell+1}$ is in $\mathbb{S}[\mathbf{t}, x_1, \ldots, x_{\ell+1}]$, for some integer $e \geq 0$, where $h = h_1 \cdots h_\ell \in \mathbb{S}[\mathbf{t}]$ and h_i is such that $h_i f_i$ is in $\mathbb{S}[\mathbf{t}, \mathbf{x}]$. Since f_i is in D, we can take h_i with $\varphi_0(h_i) \neq 0$. Since $\alpha\gamma$ is in $\mathbb{S}[\mathbf{t}]$ and satisfies $\varphi_0(\alpha\gamma) \neq 0$ as well, $f_{\ell+1}$ is in D, as requested.

We conclude by showing how to obtain the required common denominator γ of $(f_1, \ldots, f_\ell)$. Let $J_{\mathbf{g},\ell}$ (resp. $J_{\mathbf{f}}$) be the Jacobian matrix of $(g_1, \ldots, g_\ell)$ (resp. $(f_1, \ldots, f_\ell)$) with respect to $(t_1, \ldots, t_n, x_1, \ldots, x_\ell)$. As said before, all entries of both $J_{\mathbf{g},\ell}$ and $J_{\mathbf{f}}$ are in D. Besides, by assumption, there exists an $\ell \times \ell$ minor Δ_ℓ of $J_{\mathbf{g},\ell}$ such that $\varphi_0(\Delta_\ell)$ is invertible modulo $\langle \varphi_0(g_1), \ldots, \varphi_0(g_\ell)\rangle$.

As a consequence, we claim that there exists an $\ell \times \ell$ minor Δ'_ℓ of $J_{\mathbf{f}}$ such that $\varphi_0(\Delta'_\ell)$ is invertible modulo $\langle \varphi_0(f_1), \ldots, \varphi_0(f_\ell)\rangle$. Indeed, remember that $\langle f_1, \ldots, f_\ell\rangle$ contains $\langle g_1, \ldots, g_\ell\rangle$. Differentiating the corresponding membership equalities, this shows that J_ℓ factors as $J_\ell = AJ_{\mathbf{f}}$ modulo $\langle f_1, \ldots, f_\ell\rangle$, where A is a square $\ell \times \ell$ matrix; applying φ_0 and considering the columns contributing to the minor Δ_ℓ proves our claim. As previously, we define

$$\delta = \mathrm{res}(\cdots \mathrm{res}(\Delta'_\ell, f_\ell, x_\ell), \cdots, f_1, x_1) \in \mathbb{K}(\mathbf{t});$$

remark that δ is in D. Then, we claim that $\varphi_0(\delta)$ is non-zero. Indeed, since all f_i are monic, one can (up to sign) commute the application of φ_0 and the resultant, so that

$$\varphi_0(\delta) = \mathrm{res}(\cdots \mathrm{res}(\varphi_0(\Delta'_\ell), \varphi_0(f_\ell), x_\ell), \cdots, \varphi_0(f_1), x_1) \in \mathbb{S}'.$$

If the latter is zero, $\varphi_0(\Delta'_\ell)$ would be a zero-divisor modulo $\langle \varphi_0(f_1^\star), \ldots, \varphi_0(f_\ell^\star)\rangle$, a contradiction. In particular, δ itself is non-zero. By Proposition 1, there exists $d \geq 0$ such that $h^d\delta$ is a common denominator for $(f_1, \ldots, f_\ell)$, where $h = h_1 \cdots h_\ell \in \mathbb{S}[\mathbf{t}]$ and h_i is such that $h_i f_i$ is in $\mathbb{S}[\mathbf{t}, \mathbf{x}]$. Since f_i is in D, we can take h_i with $\varphi_0(h_i) \neq 0$. Letting $\gamma = h^d\delta$ proves our conclusion. ☐

Corollary 1. *Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_L$ be the maximal ideals containing $\langle g_1, \ldots, g_k\rangle$, and for $j \leq L$, let $(f_{j,1}, \ldots, f_{j,n})$ be the reduced Gröbner basis of $\mathfrak{m}_j$ for the lexicographic order $x_1 < \cdots < x_n$, Then all $f_{j,\ell}$ are in D.*

Proof. The proof is an easy induction on $\ell = 1, \ldots, k$, since $f_{j,\ell}$ is a factor of g_ℓ modulo $\langle f_{j,1}, \ldots, f_{j,\ell-1}\rangle$. ☐

Corollary 2. *There exists a unique set of polynomials $(f_1, \ldots, f_k)$ such that the following holds:*

1. *for $i \leq k$, f_i is in $\mathbb{K}(\mathbf{t})[x_1, \ldots, x_i]$, monic in x_i and reduced with respect to $\langle f_1, \ldots, f_{i-1}\rangle$;*
2. *for $i \leq k$, f_i is in D and $\varphi_n(f_i) = 0$;*
3. *the ideal $\langle f_1, \ldots, f_k\rangle$ is maximal in $\mathbb{K}(\mathbf{t})[x_1, \ldots, x_k]$ and contains $\langle g_1, \ldots, g_k\rangle$.*

Proof. Suppose that we have proved the following property, written $\mathbf{P}(\ell)$: there exist unique polynomials $(f_1, \ldots, f_\ell)$ that satisfy

1. for $i \leq \ell$, f_i is in $\mathbb{K}(\mathbf{t})[x_1, \ldots, x_i]$, monic in x_i and reduced with respect to $\langle f_1, \ldots, f_{i-1}\rangle$;
2. for $i \leq \ell$, f_i is in D and $\varphi_n(f_i) = 0$;
3. the ideal $\langle f_1, \ldots, f_\ell\rangle$ is maximal in $\mathbb{K}(\mathbf{t})[x_1, \ldots, x_\ell]$ and contains $\langle g_1, \ldots, g_\ell\rangle$.

We prove that $\mathbf{P}(\ell + 1)$ holds; then by induction, we get $\mathbf{P}(k)$, which is the claim of the corollary.

Since the ideal $\langle f_1, \ldots, f_\ell\rangle$ is maximal in $\mathbb{K}(\mathbf{t})[x_1, \ldots, x_\ell]$, the polynomial $g_{\ell+1}$ factors uniquely into a product of powers of monic irreducible polynomials $f_{\ell+1,1}, \ldots, f_{\ell+1,N}$ in $\mathbb{L}[x_{\ell+1}]$, where $\mathbb{L}$ is the field $\mathbb{K}(\mathbf{t})[x_1, \ldots, x_\ell]/\langle f_1, \ldots, f_\ell\rangle$.

Then, for any $j \leq N$, $(f_1, \ldots, f_{\ell+1,j})$ satisfy points 1 and 3 of $\mathbf{P}(\ell + 1)$. Conversely, any polynomial $f_{\ell+1}$ such that $(f_1, \ldots, f_{\ell+1})$ satisfy $\mathbf{P}(\ell + 1)$ must be one of the $f_{\ell+1,j}$. Hence, we are left to prove that there exists a unique j such that $f_{\ell+1,j}$ satisfies point 2.

Proposition 2 shows that for all $j \leq N$, $f_{\ell+1,j}$ is in D. We conclude by proving that there exists a unique j such that $\varphi_n(f_{\ell+1,j}) = 0$. Recall that $f_{\ell+1,1}^{e_1} \cdots f_{\ell+1,N}^{e_N} = g_{\ell+1}$ holds modulo $\langle f_1, \ldots, f_\ell\rangle$, for some positive integer exponents e_i Since all polynomials involved are in D, and since $\Phi(g_{\ell+1}) = 0$, we deduce that $\varphi_n(f_{\ell+1,1}^{e_1} \cdots f_{\ell+1,N}^{e_1}) = 0$. Thus, since all $f_{\ell+1,j}$ are in D, we have $\varphi_n(f_{\ell+1,j}) = 0$ for at least one $j \leq N$. It remains to prove that this j is unique:

- If g_i is purely inseparable, then $N = 1$, so we are done.

- Else, ξ_ℓ is a root of $\varphi_{\ell-1}(g_\ell)$ of multiplicity 1. Since $\varphi_{\ell-1}(g_\ell) = \varphi_{\ell-1}(f_{\ell+1,i})^{e_1} \cdots \varphi_{\ell-1}(f_{\ell+1,i})^{e_N}$, the uniqueness of j follows (and $e_j = 1$).

This proves uniquess in both cases. □

Lemma 5. *The ideal $\langle g_1, \ldots, g_k \rangle$ is radical in $\mathbb{K}(\mathbf{t})[\mathbf{x}]$.*

Proof. Let $h_1, \ldots, h_k$ and $g_1^\star, \ldots, g_k^\star$ be as before. These polynomials form a *regular chain* in $\overline{\mathbb{K}}[\mathbf{t}, \mathbf{x}]$. In particular, we write the primary decomposition of $\langle g_1^\star, \ldots, g_k^\star \rangle$ in $\overline{\mathbb{K}}[\mathbf{t}, \mathbf{x}]$ as

$$\langle g_1^\star, \ldots, g_k^\star \rangle = Q_1 \cap \cdots \cap Q_s \cap R_1 \cap \cdots \cap R_t,$$

where:

- all Q_i are n-dimensional, and contain no non-zero polynomial in $\overline{\mathbb{K}}[\mathbf{t}]$;
- all R_i contain a non-zero polynomial in $\mathbb{K}[\mathbf{t}]$, that divides a power of $h_1 \cdots h_k$.

We are going to prove that all Q_i are prime. As a consequence of $\mathbf{H}_4$, there exists a minor Δ of J_ℓ invertible in $\mathbb{K}(\mathbf{t})[\mathbf{x}]/\langle g_1, \ldots, g_k \rangle$. Thus, there exists non-zero polynomial $\delta \in \mathbb{K}[\mathbf{t}]$ such that if $\delta(\tau_1, \ldots, \tau_n) \neq 0$, Δ is invertible at all solutions of $g_1^\star(\tau, \mathbf{x}), \ldots, g_k^\star(\tau, \mathbf{x})$.

Since Q_i are n-dimensional, contains no non-zero polynomial in $\overline{\mathbb{K}}[\mathbf{t}]$, there exists a maximal ideal $\mathfrak{m} \subset \overline{\mathbb{K}}[\mathbf{t}, \mathbf{x}]$ containing $\langle g_1^\star, \ldots, g_k^\star \rangle$, at which Δ is invertible. If $(r_1, \ldots, r_m)$ are generators of Q_i, we deduce (by differentiating the membership identities) that the Jacobian matrix of $(r_1, \ldots, r_m)$ has rank at least k at $\mathfrak{m}$. The Jacobian criterion [2, Th. 16.19] implies that the localization $Q_{i\mathfrak{m}}$ is prime, and thus Q_i as well.

Let now $a \in \mathbb{K}(\mathbf{t})[\mathbf{x}]$ be such that a^r is in $\langle g_1, \ldots, g_k \rangle$, for some $r \geq 1$. Write $a = A/\alpha$, with $A \in \mathbb{K}[\mathbf{t}, \mathbf{x}]$ and $\alpha \in \mathbb{K}[\mathbf{t}]$. After clearing denominators, we obtain that βA^r is in $\langle g_1^\star, \ldots, g_k^\star \rangle \subset \mathbb{K}[\mathbf{t}, \mathbf{x}]$, for some non-zero $\beta \in \mathbb{K}[\mathbf{t}]$. Thus, βA^r is in each Q_i and since Q_i is prime and contains no non-zero polynomial in $\overline{\mathbb{K}}[\mathbf{t}]$, A is in Q_i.

Therefore, for u large enough, $(h_1 \cdots h_k)^u A$ is in the ideal generated by $\langle g_1^\star, \ldots, g_k^\star \rangle$ in $\overline{\mathbb{K}}[\mathbf{t}, \mathbf{x}]$, and thus in $\mathbb{K}[\mathbf{t}, \mathbf{x}]$. This is sufficient to conclude. □

Corollary 3. *For $\ell < k$, let $g'_{\ell+1} \in \mathbb{K}(\mathbf{t})[x_1, \ldots, x_{\ell+1}]$ be a monic factor of $g_{\ell+1}$ modulo $\langle g_1, \ldots, g_\ell \rangle$. Then, $g'_{\ell+1}$ is in D.*

Proof. Hereafter, all ideals are in $\mathbb{K}(\mathbf{t})[\mathbf{x}]$. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_L$ be the maximal ideals containing $\langle g_1, \ldots, g_\ell \rangle$, so that $\langle g_1, \ldots, g_\ell \rangle$ can be written as $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_L$ (by Lemma 5).

Each $\mathfrak{m}_j$ is defined by unique polynomials $f_{j,1}, \ldots, f_{j,\ell}$ that form a reduced Gröbner basis for the lexicographic order $x_1 < \cdots < x_n$. By Corollary 1, all $f_{j,i}$ are in D. Besides, by Proposition 2, $g'_{\ell+1}$ is a monic factor of $g_{\ell+1}$ modulo $\mathfrak{m}_j = \langle f_{j,1}, \ldots, f_{j,\ell} \rangle$, so that the normal form $g'_{\ell+1,j}$ of $g'_{\ell+1}$ modulo $\langle f_{j,1}, \ldots, f_{j,\ell} \rangle$ is in D. It remains to prove that $g'_{\ell+1}$ is in D too, using Chinese remaindering.

The inverse map of Chinese remaindering associates to a polynomial $a \in \mathbb{K}(\mathbf{t})[x_1, \ldots, x_\ell]$, reduced with respect to $\langle g_1, \ldots, g_\ell \rangle$, its normal forms modulo all $\langle f_{j,1}, \ldots, f_{j,\ell} \rangle$. The matrix of $\mathbf{M}$ this $\mathbb{K}(\mathbf{t})$-linear map (on the canonical bases) has entries in D; we want to prove that the inverse of $\mathbf{M}$ does as well.

Let us for the moment assume that we have proved that $\langle \varphi_0(f_{j,1}), \ldots, \varphi_0(f_{j,\ell}) \rangle$ are pairwise coprime. This implies that the matrix $\varphi_0(\mathbf{M})$ is invertible, so that $\det(\varphi_0(\mathbf{M})) = \varphi_0(\det(\mathbf{M}))$ is non-zero, which is sufficient to conclude.

So, we need to prove that the ideals $\langle \varphi_0(f_{j,1}), \ldots, \varphi_0(f_{j,\ell}) \rangle$ are pairwise coprime. Consider two such sequences $f_{j,1}, \ldots, f_{j,\ell}$ and $f_{j',1}, \ldots, f_{j',\ell}$. By construction, we have $f_{j,i} = f_{j',i}$ up to some $i_0 < \ell$, and f_{j,i_0+1} and f_{j',i_0+1} are two distinct irreducible factors of g_{i_0+1} modulo $\langle f_{j,1}, \ldots, f_{j,i_0} \rangle = \langle f_{j',1}, \ldots, f_{j',i_0} \rangle$.

In particular, g_{i_0+1} cannot be purely inseparable. Thus, $\mathbf{H_3}$ implies that $\varphi_0(\partial g_{i_0+1}/\partial x_{i_0+1})$ is a unit modulo $\langle \varphi_0(f_{j,1}), \ldots, \varphi_0(f_{j,i_0}), \varphi_0(g_{i_0+1}) \rangle$. This implies that $\varphi_0(f_{j,i_0+1})$ and $\varphi_0(f_{j',i_0+1})$ are coprime modulo $\langle \varphi_0(f_{j,1}), \ldots, \varphi_0(f_{j,i_0}) \rangle$, and finishes the proof. □

References

[1] J. Abbott. *On the factorization of polynomials over algebraic fields.* PhD thesis, University of Bath, 1988.

[2] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[3] J. Lipman and A. Sathaye. Jacobian ideals and theorem of Briançon-Skoda. *Michigan Math. J.*, 28:199–222, 1981.

[4] A. K. Singh and I. Swanson. An algorithm for computing the integral closure. arXiv:0901.0871, 2009.

[5] P. J. Weinberger and L. P. Rothschild. Factoring polynomials over algebraic number fields. *ACM Trans. Math. Soft.*, 2(4):335–350, 1976.