Polynomials over Power Series and their Applications to Limit Computations (tutorial version)

Marc Moreno Maza
University of Western Ontario
IBM Center for Advanced Studies

CASC 2018 Tutorial
Université de Lille
Bâtiment M^3
May 28, 2021

Plan

Plan

Plan

Notations

- Let $\mathcal{M}' = \langle X_1, \ldots, X_{n-1} \rangle$ be the maximal ideal of $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle$.
- Let $p = X_n^k + a_1 X_n^{k-1} + \cdots + a_k \in \mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle [X_n]$ be a Weierstrass polynomial of degree k. Thus $a_1, \ldots, a_k \in \mathcal{M}'$ holds.

Proposition 4

The following properties are equivalent

(i) $k = 0$,

(ii) p is a unit in $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle [X_n]$,

(iii) p is a unit in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n \rangle$.

Proof

- The equivalence $(i) \iff (iii)$ is trivial.
- The equivalence $(i) \iff (ii)$ follows from $k = \deg(p, X_n)$, $1 = \mathrm{lc}(p, X_n)$ and the fact that $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle$ is integral.

Factorization Properties (2/9)

Proposition 5

Let $f, g, h \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ be polynomials s. t. $f = gh$. Then

(i) if g, h are Weierstrass polynomials then so is f,

(ii) if f is a Weierstrass polynomial, then there exist units $\lambda, \mu \in \langle X_1, \ldots, X_{n-1}\rangle$ s. t. λg and μh are Weierstrass polynomials.

Proof

- Claim (i) is clear.
- To prove (ii), we write $g = b_0 X_n^\ell + \cdots + b_\ell$ and $h = c_0 X_n^m + \cdots + c_m$. We observe that $c_0 b_0 = 1$ holds. So we choose $\lambda = c_0$ and $\mu = b_0$.
- W.l.o.g. we assume $c_0 = b_0 = 1$. Thus, each of the following power series belongs to $\mathcal{M}'$

$$b_\ell c_m, b_\ell c_{m-1} + b_{\ell-1} c_m, b_\ell c_{m-2} + b_{\ell-1} c_{m-1} + b_{\ell-2} c_m, \ldots$$

- Since $\mathcal{M}'$ is a prime ideal then each coefficient $b_1, b_2, \ldots, b_\ell, c_1, c_2, \cdots, c_m$ belong to $\mathcal{M}'$

Lemma 2

Let $\mathbb{A}$ be a commutative ring and let $f = \sum_{s=0}^{k} a_s X^s$, $g = \sum_{i=0}^{\ell} b_i X^i$ and $h = \sum_{j=0}^{m} c_j X^j$ be polynomials s.t. a_0, b_0, c_0 units of $\mathbb{A}$ and $f = g\,h$ holds. Let $\mathcal{P}$ be a prime ideal s.t. $a_1, \ldots, a_k \in \mathcal{P}$ Then, we have $b_1, \ldots, b_\ell, c_1, \ldots, c_m \in \mathcal{P}$.

Proof (1/2)

- Consider a rectangular grid G where the points are indexed by the Cartesian Product $\{0, \ldots, \ell\} \times \{0, \ldots, m\}$.
- The point of G of coordinates (i, j) is mapped to $b_i c_j$ such that the sum of all points along a line $i + j = q$ equal a_q.
- There exists at least one such "line" consisting of a unique point. $b_i c_j$.

Proof (2/2)

- If there is only one such point then, this is $(0,0)$ and G reduces to that point and we are done.
- If there are two such points, then for one of them, either $i > 0$ or $j > 0$ holds. Consider a point of that latter type. Since $\mathcal{P}$ is prime, either $b_i \in \mathcal{P}$ (provided $i > 0$) or $c_j \in \mathcal{P}$ (provided $j > 0$) holds. W.l.o.g., assume $b_i \in \mathcal{P}$ and erase from G all points of the form b_i-*something*.
- If G is not empty, we go back two steps above.
- It is not hard to see that this procedure will erase all rows $b_1, b_2, \ldots, b_\ell$ and all columns $c_1, c_2, \ldots, c_m$, which proves the lemma.

Lemma 3

For the Weierstrass polynomial
$p = X_n^k + a_1 X_n^{k-1} + \cdots + a_k \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ the following properties are equivalent

(i) p is irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$,

(ii) p irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.

Proof of $(i) \Rightarrow (ii)$ (1/2)

- We proceed by contradiction. Assume that p reducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.
- So let $f_1, f_2 \in \mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$ be non-units s. t. $p = f_1 f_2$.
- Since p is general in X_n (that is, $p \not\equiv 0 \mod \mathcal{M}'$) we can assume that both f_1, f_2 are general in X_n.
- Applying the preparation theorem, we have $f_1 = \alpha_1 q_1$ and $f_2 = \alpha_2 q_2$, where α_1, α_2 are units and q_1, q_2 are Weierstrass polynomials.

Factorization Properties (6/9)

Proof of $(i) \Rightarrow (ii)$ (2/2)

- Thus, $p = \alpha_1 \alpha_2 q_1 q_2$. Observe that $q_1 q_2$ is a Weierstrass polynomial.
- Uniqueness from the preparation theorem implies $\alpha_1 \alpha_2 = 1$ and $p = q_1 q_2$, which is a factorization of p in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$.
- Recall that we assume that p irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ and that we aim at contradicting p reducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.
- So, one of the polynomials q_i must be a unit in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ This would imply $q_i = 1$, that is, $f_i = \alpha_i$. A contradiction.

Proof of $(ii) \Rightarrow (i)$

- We assume that p irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$ and proceeding by contradiction, we assume p reducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$. Thus let $p_1, p_2 \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ such that $p = p_1 p_2$ holds.
- We know that p_1, p_2 are Weierstrass polynomials of positive degree. Thus p is reducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$, a contradiction.

Factorization Properties (7/9)

Theorem 7

The ring $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$ is a unique factorization domain (UFD).

Proof of the Theorem (1/3)

- The proof is by induction on n.
- For $n = 0$, this is clear since any field is a UFD.
- By induction hypothesis, we assume that $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle$ is a UFD.
- It follows from Gauss Theorem that $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ is a UFD as well.
- Next, we show that every $f \in \mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$ has a factorization into irreducibles, unique up to order and units.
- We may assume that f is general in X_n. By the preparation theorem, we have $f = \alpha p$ with α a unit and $p \in \mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ a Weierstrass polynomial.

Proof of the Theorem (2/3)

- Since $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ is a UFD, there is a factorization
$$p = p_1 \cdots p_r$$
into irreducible elements, which is unique up to order, after $p_1, \ldots, p_r$ have been normalized to be Weierstrass polynomials.
- By the previous lemma,
$$f = \alpha p_1 \cdots p_r$$
is a factorization into irreducibles of $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.
- Let $f = f_1 \cdots f_s$ be another such factorization into irreducibles of $\mathbb{K}\langle X_1, \ldots, X_{n-1}, X_n\rangle$.
- We apply the preparation theorem to $f_1, \ldots, f_s$, leading to $f_1 = \alpha_i q_1$, $\ldots$, $f_s = \alpha_s q_s$, where $\alpha_1, \ldots, \alpha_s$ are units and $q_1, \ldots, q_s$ are Weierstrass polynomials of positive degrees.

Proof of the Theorem (3/3)

- By uniqueness in the preparation theorem, we have
$$p_1 \cdots p_r = q_1 \cdots q_s.$$
- Finally, since $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$ is a UFD, we deduce $r = s$ and $\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}$.

Remarks

- Following the techniques of the above proof and using the preparation theorem, one can prove that $\mathbb{K}\langle X_1, \ldots, X_n\rangle$ is a Noetherian ring.
- One can prove the preparation theorem in $\mathbb{K}[[X_1, \ldots, X_n]]$ (instead of $\mathbb{K}\langle X_1, \ldots, X_n\rangle$).
- As a result, the results of this section can also be established in $\mathbb{K}[[X_1, \ldots, X_n]]$ (instead of $\mathbb{K}\langle X_1, \ldots, X_n\rangle$).
- In particular, one can prove that $\mathbb{K}[[X_1, \ldots, X_n]]$ is a UFD.

Weierstrass preparation theorem for formal power series (1/8)

Lemma 4

Assume $n \geq 2$. Let $f, g, h \in \mathbb{K}[[X_1, \ldots, X_{n-1}]]$ such that $f = gh$ holds. Let $\mathcal{M}$ be the maximal ideal of $\mathbb{K}[[X_1, \ldots, X_{n-1}]]$. We write $f = \sum_{i=0}^{\infty} f_i$, $g = \sum_{i=0}^{\infty} g_i$ and $h = \sum_{i=0}^{\infty} h_i$, where $f_i, g_i, h_i \in \mathcal{M}^i \setminus \mathcal{M}^{i+1}$ holds for all $i > 0$, with $f_0, g_0, h_0 \in \mathbb{K}$. We note that these decompositions are uniquely defined. Let $r \in \mathbb{N}$. We assume that $f_0 = 0$ and $h_0 \neq 0$ both hold. Then the term g_r is uniquely determined by $f_1, \ldots, f_r, h_0, \ldots, h_{r-1}$.

Proof (1/2)

- Since $g_0 h_0 = f_0 = 0$ and $h_0 \neq 0$ both hold, the claim is true for $r = 0$.
- Now, let $r > 0$. By induction hypothesis, we can assume that $g_0, \ldots, g_{r-1}$ are uniquely determined by $f_1, \ldots, f_{r-1}, h_0, \ldots, h_{r-2}$.
- Observe that for determining g_r, it suffices to expand $f = gh$ modulo $\mathcal{M}^{r+1}$.

Weierstrass preparation theorem for formal power series (2/8)

Proof (2/2)

- Modulo $\mathcal{M}^{r+1}$, we have

$$\begin{array}{rcl} f_1 + f_2 + \cdots + f_r & = & (g_1 + g_2 + \cdots + g_r)(h_0 + h_1 + \cdots + h_r) \\ & = & g_1 h_0 + \\ & & g_2 h_0 + g_1 h_1 + \\ & & \vdots \\ & & g_r h_0 + g_{r-1} h_1 + \cdots + g_1 h_{r-1} \end{array}$$

- The conclusion follows.

Weierstrass preparation theorem for formal power series (3/8)

Notations

- Assume $n \geq 1$. Denote by $\mathbb{A}$ the ring $\mathbb{K}[[X_1, \ldots, X_{n-1}]]$ and by $\mathcal{M}$ be the maximal ideal of $\mathbb{A}$.
- Note that $n = 1$ implies $\mathcal{M} = \langle 0 \rangle$.
- Let $f \in \mathbb{A}[[X_n]]$, written as $f = \sum_{i=0}^{\infty} a_i X_n^i$ with $a_i \in \mathbb{A}$ for all $i \in \mathbb{N}$.

Theorem 8

We assume $f \not\equiv 0 \mod \mathcal{M}[[X_n]]$. Then, there exists a unit $\alpha \in \mathbb{A}[[X_n]]$, an integer $d \geq 0$ and a monic polynomial $p \in \mathbb{A}[X_n]$ of degree d such that we have

1. $p = X_n^d + b_{d-1} X_n^{d-1} + \cdots + b_1 X_n + b_0$, for some $b_{d-1}, \ldots, b_1, b_0 \in \mathcal{M}$,
2. $f = \alpha p$.

Further, this expression for f is unique.

Proof (1/5)

- Let $d \geq 0$ be the smallest integer such that $a_d \notin \mathcal{M}$. Clearly d exists since we assume that $f \not\equiv 0 \mod \mathcal{M}[[X_n]]$ holds.
- If $n = 1$, then writing $f = \alpha X_n^d$ with $\alpha = \sum_{i=0}^{\infty} a_{i+d} X_n^i$ proves the existence of the claimed decomposition.
- From now on, we assume $n \geq 2$.
- Let us write $\alpha = \sum_{i=0}^{\infty} c_i X_n^i$ with $c_i \in \mathbb{A}$ for all $i \in \mathbb{N}$.
- Since we require α to be a unit, we have $c_0 \notin \mathcal{M}$. Note that c_0 is also a unit modulo $\mathcal{M}$.

Proof (2/5)

We must solve for $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ s. t. for all $m \geq 0$ we have

$$\begin{array}{rcl}
a_0 & = & b_0 c_0 \\
a_1 & = & b_0 c_1 + b_1 c_0 \\
a_2 & = & b_0 c_2 + b_1 c_1 + b_2 c_0 \\
& \vdots & \\
a_{d-1} & = & b_0 c_{d-1} + b_1 c_{d-2} + \cdots + \cdots + b_{d-2} c_1 + b_{d-1} c_0 \\
a_d & = & b_0 c_d + b_1 c_{d-1} + \cdots + \cdots + b_{d-1} c_1 + c_0 \\
a_{d+1} & = & b_0 c_{d+1} + b_1 c_d + \cdots + \cdots + b_{d-1} c_2 + c_1 \\
& \vdots & \\
a_{d+m} & = & b_0 c_{d+m} + b_1 c_{d+m-1} + \cdots + \cdots + b_{d-1} c_{m+1} + c_m \\
& \vdots &
\end{array}$$

Proof (3/5)

- We will compute each of $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ modulo each of the successive powers of $\mathcal{M}$, that is, $\mathcal{M}, \mathcal{M}^2, \ldots, \mathcal{M}^r, \ldots$.
- We start by solving for each of $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ modulo $\mathcal{M}$.
- By definition of d, the left hand sides of the first d equations above are all $\equiv 0 \mod \mathcal{M}$.
- Since c_0 is a unit modulo $\mathcal{M}$, these first d equations taken modulo $\mathcal{M}$ imply that each of $b_0, b_1, \ldots, b_{d-1}$ is $\equiv 0 \mod \mathcal{M}$.
- Plugging this into the remaining equations we obtain $c_m \equiv a_{d+m} \mod \mathcal{M}$, for all $m \geq 0$.
- Therefore, we have solved for each of $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ modulo $\mathcal{M}$.

Proof (4/5)

- Let $r > 0$ be an integer. We assume that we have inductively determined each of $b_{d-1}, \ldots, b_1, b_0, c_0, c_1, \ldots, c_d, \ldots$ modulo each of $\mathcal{M}, \ldots, \mathcal{M}^r$. We wish to determine them modulo $\mathcal{M}^{r+1}$.
- Consider the first equation, namely $a_0 = b_0 c_0$, with $a_0, b_0, c_0 \in \mathbb{A}$. Recall that $a_0 \in \mathcal{M}$ and $c_0 \notin \mathcal{M}$ both hold. By assumption, b_0 and c_0 are known modulo each of $\mathcal{M}, \ldots, \mathcal{M}^r$. In addition, a_0 is known modulo each of $\mathcal{M}, \ldots, \mathcal{M}^r, \mathcal{M}^{r+1}$. Therefore, the previous lemma applies and we can compute b_0 modulo $\mathcal{M}^{r+1}$.
- Consider the second equation, that we re-write $a_1 - b_0 c_1 = b_1 c_0$. A similar reasoning applies and we can compute b_1 modulo $\mathcal{M}^{r+1}$.
- Continuing in this manner, we can compute each of $b_0, b_1, \ldots, b_{d-1}$ modulo $\mathcal{M}^{r+1}$ using the first d equations.
- Finally, using the remaining equations determine $c_m \mod \mathcal{M}^r$, for all $m \geq 0$.

Weierstrass preparation theorem for formal power series (8/8)

Proof (5/5)

- The induction is complete, and the existence of a factorization of f as claimed is proved.
- The uniqueness is obvious, because d is uniquely determined by f, and the unit α is uniquely determined as **the** coefficient of X_n^d in any two such factorizations.
- Finally, equating the coefficients of $X_n^{d-1}, \ldots, X_n, X_n^0$ in any two such factorizations determine p uniquely.

Remark

- The assumption of the theorem, namely $f \not\equiv 0 \mod \mathcal{M}[[X_n]]$, can always be assumed. Indeed, one can reduce to this case by a suitable linear change of coordinates.
- From this Weierstrass preparation theorem for formal power series, one can show that $\mathbb{K}[[X_1, \ldots, X_{n-1}]]$ is a UFD and a Noetherian ring.

Definition

Let $D := \{x = (x_1, \dots, x_n) \in \mathbb{K}^n \ \mid \ |x_i| < \rho_i\}$ be a polydisk and let $M \subseteq D$. We say that M is a *principal analytic set* if there exists $f \in \mathbb{K}\langle X_1, \dots, X_n\rangle$ that converges throughout D and satisfies

$$M = V_D(f) \ \text{ where } \ V_D(f) := \{x \in D \ \mid \ f(x) = 0\}.$$

Given f, the set $V_D(f)$ may be empty or not, depending on D.

Definition

Let D_1 and D_2 be two polydisks of $\mathbb{K}^n$. Let $M_1 \subseteq D_1$ and $M_2 \subseteq D_2$ be two principal analytic sets. We say that M_1 and M_2 are *equivalent* if there exists a polydisk $D \subseteq D_1 \cap D_2$ such that we have

$$M_1 \cap D \ = \ M_2 \cap D.$$

An equivalence class of principal analytic sets is called a *germ of a principal analytic set*, or, when $n = 2$, a germ of a curve.

Notation for a germ

Given two equivalent principal analytic sets $M_1 = V_{D_1}(f_1)$ and $M_2 = V_{D_1}(f_2)$ there exists a polydisk D such that we have

$$\{x \in D_1 \mid f_1(x) = 0\} \cap D = \{x \in D_2 \mid f_2(x) = 0\} \cap D.$$

Therefore $f_1 = f_2$ holds and we simply write $V(f)$ for the equivalent class of M_1 and M_2. Indeed, if the set of zeros of an analytic function f has an accumulation point inside the domain of f, then f is zero everywhere on the connected component containing the accumulation point.

The empty germ

It follows that $V(f) = \emptyset$ means that $0 \notin V_D(f)$ for any representative $V_D(f) \in V(f)$. This implies $f(0) \neq 0$, that is, f is a unit in $\mathbb{K}\langle X_1, \ldots, X_n \rangle$. The converse is clearly true, so we have

$$V(f) = \emptyset \quad \Longleftrightarrow \quad f \not\equiv 0 \mod \mathcal{M}.$$

Binary operations on germs

An inclusion $V(f_1) \subseteq V(f_2)$ between two germs means that there exist representatives $V_{D_1}(f_1) \in V(f_1)$ and $V_{D_2}(f_2) \in V(f_2)$ together with a polydisk $D \subseteq D_1 \cap D_2$ such that we have

$$V_{D_1}(f_1) \cap D \ \subseteq \ V_{D_2}(f_2) \cap D.$$

We define $V(f_1) \cap V(f_2)$ and $V(f_1) \cup V(f_2)$ similarly.

Proposition 6

- For all $f, g \in \mathbb{K}\langle X_1, \ldots, X_n\rangle$ s.t f divides g, we have $V(f) \subseteq V(g)$.
- For all $f, f_1, \ldots, f_r \in \mathbb{K}\langle X_1, \ldots, X_n\rangle$ s.t. $f = f_1 \cdots f_r$ holds we have $V(f) = V(f_1) \cup \cdots \cup V(f_r)$.

Germs of curves (4/8)

Lemma (Study's Lemma)

Let $f, g \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ with f irreducible. If the germs $V(f), V(g)$ satisfy $V(f) \subseteq V(g)$ then f divides g in $\mathbb{K}\langle X_1, \ldots, X_n \rangle$.

Proof of Study's Lemma (1/3)

- We proceed by induction on n.
- The case $n = 0$ is trivial.
- Next, by induction hypothesis, we assume that the lemma holds in $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle$.
- By definition of $V(f) \subseteq V(g)$ and thanks to the preparation theorem, we can assume that f, g are Weierstrass polynomials in $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle[X_n]$. Thus we have

$$f = X_n^k + a_1 X_n^{k-1} + \cdots + a_k, \quad g = X_n^\ell + b_1 X_n^{\ell-1} + \cdots + b_\ell,$$

where $k, \ell \geq 1$ and each of $a_1, \ldots, a_k, b_1, \ldots, b_\ell$ is zero modulo $\mathcal{M}'$, where (as usual) $\mathcal{M}'$ is the maximal ideal of $\mathbb{K}\langle X_1, \ldots, X_{n-1} \rangle$.

Proof of Study's Lemma (2/3)

- Since $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle$ is a UFD, it follows from resultant theory that f and g have a common divisor of positive degree ii and only if the resultant $\operatorname{res}(f, g)$ is not zero.
- Since f is also irreducible in $\mathbb{K}\langle X_1, \ldots, X_{n-1}\rangle[X_n]$, proving $\operatorname{res}(f, g) \neq 0$ would do what we need.
- Let $D = \{x = (x_1, \ldots, x_n) \in \mathbb{K}^n \ \mid \ |x_i| < \rho_\}$ be a polydisk throughout which f and g are convergent.
- Define $D' = \{x = (x_1, \ldots, x_{n-1}) \in \mathbb{K}^{n-1} \ \mid \ |x_i| < \rho_i\}$.
- For each $x' \in D'$, we denote by $f_{x'}$ and $g_{x'}$ the univariate polynomials of $\mathbb{K}[X_n]$ obtained by specializing $X_1, \ldots, X_{n-1}$ to x' into f, g.
- In particular, we have $f_0 = X_n^k$ and $g = X_n^\ell$, so $V(f_0) = V(g_0) = \{0\}$.

Proof of Study's Lemma (3/3)

- Since the roots of $f_{x'}$ and $g_{x'}$ depends continuously on x', one can choose the polydisk $D = \{x = (x_1, \ldots, x_n) \in \mathbb{K}^n \mid |x_i| < \rho_i\}$ (and thus D') such that for all $x' \in D'$ each root x_n of $f_{x'}$ and $g_{x'}$ satisfies $|x_n| < \rho_n$.
- For the same continuity argument, and since $V(f) \subseteq V(g)$ holds, the polydisk D can be further refined such that $V(f_{x'}) \subseteq V(g_{x'})$ holds for all $x' \in D'$.
- Hence, for all $x' \in D'$, the univariate polynomials $f_{x'}$ and $g_{x'}$ have a common prime factor, that is, $\mathrm{res}(f_{x'}, g_{x'}) = 0$.
- Finally, using the specialization property of the resultant, we conclude that $\mathrm{res}(f, g)(x') = 0$ holds for all $x' \in D'$.

Definition

A germ of a principal analytic set $V(f)$ is called *reducible* if there exist two germs of a principal analytic set $V(f_1)$ and $V(f_2)$ such that we have $V(f) = V(f_1) \cup V(f_2)$, $V(f_1) \neq \emptyset$, $V(f_2) \neq \emptyset$ and $V(f_1) \neq V(f_2)$. Otherwise, $V(f)$ is called irreducible.

Lemma 5

A germ of a principal analytic set $V(f)$ is irreducible if and only if there exists $g \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ and $k \in \mathbb{N}^*$ such that $f = g^k$ holds.

Theorem 9

Let $V(f)$ be a germ of a principal analytic set. Then, $V(f)$ admits a decomposition

$$V(f) = V(f_1) \cup \cdots \cup V(f_r).$$

where $V(f_1), \ldots, V(f_r)$ are irreducible. This decomposition is unique up to the order in which the components appear.

Germs of curves (8/8)

Definition

We call a series $f \in \mathbb{K}\langle X_1, \ldots, X_n \rangle$ *minimal* if every prime factor f_i of f occurs only once, that is, $f = f_1 \cdots f_r$.

- Then, for a curve (that is $n = 2$) the sets $V(f_1), \ldots, V(f_r)$ are called the branch of the curve at the origin.
- This notion can be translated at any point of the curve by an appropriate change of coordinates.
- If f is minimal, we call

  $$\mathrm{Ord}(V(f)) \; = \; \mathrm{ord}(f)$$

  the order of the germ.