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
June 16, 2021

Plan

Plan

Plan

The ring of Puiseux series (1/9)

Definition

- For $m \geq 1$, there is an injective homomorphism
$$\mathbb{C}[[X]] \to \mathbb{C}[[T]],\ X \mapsto T^m.$$
- We regard this as a ring extension
$$\mathbb{C}[[X]] \subseteq \mathbb{C}[[T]] \equiv \mathbb{C}[[X^{\frac{1}{m}}]]$$
- If $m = kn$, there are injections
$$\begin{array}{l} \mathbb{C}[[X]] \to \mathbb{C}[[T]] \to \mathbb{C}[[S]], \\ X \mapsto T^n.\ T \mapsto S^k, \\ X \mapsto (S^k)^n = S^m. \end{array}$$
which can be regarded as inclusions
$$\mathbb{C}[[X]] \subseteq \mathbb{C}[[X^{\frac{1}{n}}]] \subseteq \mathbb{C}[[X^{\frac{1}{m}}]].$$
- Continuing in this way, we define
$$\mathbb{C}[[X^*]] \ = \ \bigcup_{n=1}^{\infty} \mathbb{C}[[X^{\frac{1}{n}}]].$$
- This is an integral domain that contains all *formal Puiseux series*.

Definition

For a fixed $\varphi \in \mathbb{C}[[X^*]]$, there is an $n \in \mathbb{N}$ such that $\varphi \in \mathbb{C}[[X^{\frac{1}{n}}]]$. Hence

$$\varphi = \sum_{m=0}^{\infty} a_m X^{\frac{m}{n}}, \quad \text{where} \quad a_m \in \mathbb{C}.$$

and we call *order of* φ the rational number defined by

$$\mathrm{ord}(\varphi) \; = \; \min\{\tfrac{m}{n} \;\mid\; a_m \neq 0\} \geq 0.$$

The ring of Puiseux series (3/9)

Notation

We denote by $\mathbb{C}((X^*))$ the quotient field of $\mathbb{C}[[X^*]]$.

Definition

Let $\varphi \in \mathbb{C}[[X^*]]$ and $n \in \mathbb{N}$ minimum with the property that $\varphi \in \mathbb{C}[[X^{\frac{1}{n}}]]$ holds. We say that the Puiseux series φ is *convergent* if we have $\varphi \in \mathbb{C}\langle X \rangle$. Convergent Puiseux series form an integral domain denoted by $\mathbb{C}\langle X^* \rangle$ and whose quotient field is denoted by $\mathbb{C}(\langle X^* \rangle)$.

Proposition

For every element $\varphi \in ((X^*))$, there exist $n \in \mathbb{Z}$, $r \in \mathbb{N}_{>0}$ and a sequence of complex numbers $a_n, a_{n+1}, a_{n+2}, \ldots$ such that

$$\varphi \; = \; \sum_{m=n}^{\infty} a_m X^{\frac{m}{r}} \;\; \text{and} \;\; a_n \neq 0.$$

and we define $\operatorname{ord}(\varphi) = \frac{n}{r}$.

Proof

The proof, easy, uses power series inversion.

Remark

- Formal Puiseux series can be defined over an arbitrary field $\mathbb{K}$.
- One essential property of Puiseux series is expressed by the following theorem, attributed to Puiseux for $\mathbb{K} = \mathbb{C}$ but which was implicit in Newton's use of the Newton polygon as early as 1671 and therefore known either as Puiseux's theorem or as the NewtonPuiseux theorem.
- In its modern version, this theorem requires only $\mathbb{K}$ to be algebraically closed and of characteristic zero. See corollary 13.15 in D. Eisenbud's *Commutative Algebra with a View Toward Algebraic Geometry*.

The ring of Puiseux series (6/9)

Theorem (Nowak's formulation of Puiseux' Theorem)

If $\mathbb{K}$ is an algebraically closed field of characteristic zero, then the field $\mathbb{K}((X^*))$ of formal Puiseux series over $\mathbb{K}$ is the algebraic closure of the field of formal Laurent series over $\mathbb{K}$. Moreover, if $\mathbb{K} = \mathbb{C}$, then the field $\mathbb{C}(\langle X^* \rangle)$ of convergent Puiseux series over $\mathbb{C}$ is algebraically closed as well.

Proof of the Theorem (1/3)

- We restrict the proof to the case $\mathbb{K} = \mathbb{C}$. Hence, we prove that $\mathbb{C}((X^*))$ and $\mathbb{C}(\langle X^* \rangle)$ are algebraically closed. We follow the elegant and short proof of K. J. Nowak which relies only on Hensel's lemma.
- It suffices to prove that any monic polynomial $f \in \mathbb{C}((X^*))[Y]$ (resp. $f \in \mathbb{C}(\langle X^* \rangle)[Y]$)
$$f(X, Y) = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)$$
of degree $n > 1$ is reducible.

Proof of the Theorem (2/3)

- Making use of Tschirnhausen transformation $\widetilde{Y} = Y - \frac{1}{n}a_1(X)$, we can assume that the coefficient $a_1(X)$ is identically zero. W.l.o.g., we assume $a_n(X)$ not identically zero.
- For each $k = 1, \ldots, n$, define $r_k = \operatorname{ord}(a_k(X)) \in \mathbb{Q}$, unless a_k is identically zero.
- Define $r := \min\{r_k/k\}$. Obviously, we have $r_k/k - r \geq 0$, with equality for at least one k.
- Take a positive integer q so large that all Puiseux series $a_k(X)$ are of the form $f_k(X^{1/q})$ for $f_k \in \mathbb{C}[[Z]]$ (resp. $f_k \in \mathbb{C}\langle Z\rangle$). Let $r := p/q$ for an appropriate $p \in \mathbb{Z}$.
- After the transformation of variables $X = w^q,\ Y = U \cdot w^p$, we get
$$f(X,Y) = w^{np} \cdot Q(w,U), \quad \text{where}$$
$$Q(w,U) = U^n + b_2(w)U^{n-2} + \cdots + b_n(w) \ \text{ and } \ b_k(w) = a_k(w^q)w^{-kp}.$$

The ring of Puiseux series (8/9)

Proof of the Theorem (3/3)

- Observe that $\operatorname{ord}(b_k(w)) \in \mathbb{Z}$ and satisfies in fact
$$\operatorname{ord}(b_k(w)) = q \cdot r_k - k \cdot p = q \cdot k(r_k/k - r) \geq 0.$$
- Therefore $Q(w, U)$ is a polynomial in $\mathbb{C}[[w]][U]$ (resp. $\mathbb{C}\langle w\rangle[U]$).
- Furthermore we have $\operatorname{ord}(b_k(w)) = 0$ for at least one k. Thus, for every such k, we have $b_k(0) \neq 0$.
- Therefore, the complex polynomial
$$Q(0, U) = U^n + b_2(0)U^{n-2} + \cdots + b_n(0) \not\equiv (U - c)^n$$
for any $c \in \mathbb{C}$.
- Hence, $Q(0, U)$ is the product of two coprime polynomials in $\mathbb{C}[U]$.
- By Hensel's lemma, $Q(w, U)$ is the product of two polynomials $Q_1(w, U)$ and $Q_2(w, U)$ in $\mathbb{C}[[w]][U]$ (resp. $\mathbb{C}\langle w\rangle[U]$).
- Finally, we have
$$f(X, Y) = X^{nr} \cdot Q_1(X^{1/q}, X^{-r}Y) \cdot Q_2(X^{1/q}, X^{-r}Y).$$

The ring of Puiseux series (9/9)

Remark

- Nowak's formulation of Puiseux' Theorem yields an algorithm provided that for each coefficient $a_1(X), \ldots, a_n(X)$, one can compute its order. This is the case if each of $a_1(X), \ldots, a_n(X)$ is a rational function in X.
- Since the input polynomial f belongs to $\mathbb{C}((X^*))[Y]$, we can always reduce to the case where f is monic provided that the leading coefficient $a_0(X)$ is also a rational function in X.
- Because Nowak's algorithm makes two recursive calls on polynomial of Y-degrees n_1 and n_2, with $n_1 + n_2 = n$, it is easy to check that the main cost is the "first" call to Hensel's lemma. Therefore, the cost of Nowak's algorithm is essentially that of Hensel's lemma.

Corollary

Every monic polynomial of $\mathbb{C}\langle X\rangle[Y]$ splits into linear factors in $\mathbb{C}[[X^*]][Y]$.

Implicit function theorem and local parametrization

Definition

Let $f \in \mathbb{K}\langle X, Y\rangle$ be minimal, with $f(0,0) = 0$. The branch $V(f)$ is called smooth if we have

$$\operatorname{grad} f := \left(\frac{\partial f}{\partial X}(0), \frac{\partial f}{\partial Y}(0)\right) \neq (0,0).$$

Remark

If $\partial f/\partial Y \neq 0$, the implicit function theorem gives us a local parametrization $x \mapsto \Phi(x) = (x, \varphi(x))$ of $V(f)$. That is, there exists a convergent power series $\varphi \in \mathbb{K}\langle X\rangle$ such that $f(x, \varphi(x)) = 0$ holds in a neighborhood of the origin.

Motivating the notion of Puiseux series

Example

Let $f := X^3 - Y^2$. The implicit function theorem does not apply to f. However, there is a parametrization:

$$t \mapsto \Phi(t) = (t^2, \varphi(t)), \text{ where } \varphi(t) = t^3.$$

Setting $t = x^{1/2}$, we obtain a parametrization of the cuspidal cubic with fractional exponents

$$x \mapsto \left(x, x^{\frac{3}{2}}\right).$$

Remark

We will show that locally any branch of a curve has a parametrization of the form

$$t \mapsto (t^n, \varphi(t)) \text{ or } x \mapsto \left(x, \varphi(x^{\frac{1}{n}})\right),$$

for some power series $\varphi \in \mathbb{C}\langle T \rangle$. Such φ are called Puiseux Series.

Theorem on Puiseux Series

Definition

Let $f(X, Y) \in \mathbb{C}[[X, Y]]$ be with $f(0, 0) = 0$. A pair (φ_1, φ_2) of series in $\mathbb{C}[[T]]$ is called a formal parametrization of f if we have:

1. $(\varphi_1, \varphi_2) \neq (0, 0)$,
2. $\varphi_1(0) = \varphi_2(0) = 0$ and
3. $f(\varphi_1(T), \varphi_2(T)) = 0$ holds in $\mathbb{C}[[T]]$.

Here, the substitution is the sense of power series composition.

Puiseux's Theorem (algebraic version)

Let the series $f \in \mathbb{C}[[X, Y]]$ be general in Y of order $k \geq 1$. Then there exists a natural number $n \geq 1$ and $\varphi \in \mathbb{C}[[T]]$ such that $\varphi(0) = 0$ and $f(T^n, \varphi(T)) = 0$ hold in $\mathbb{C}[[T]]$. Moreover, if f is convergent, then so is φ.

Proof (skipping the "Moreover")

- We apply Weierstrass Preparation Theorem so as to reduce to the case where f is a monic polynomial in Y.
- We apply Nowak's formulation of Puiseux' Theorem,

Proving convergence of the power series in Puiseux Theorem

Remark

- In the special case of the implicit function theorem, the convergence of φ can be derived easily from convergence of f, as a corollary of Weierstrass Preparation Theorem.
- The general case is more complicated.

Remark

The proof (to be presented hereafter) combines

- methods from complex analysis and topology to prove the existence of sufficiently many "convergent solutions", and
- an algebraic trick to show that the formally constructed series is equal to one of the convergent solutions.

Thus φ must be convergent.

Discriminant (recall)

Notation

Let A be a commutative ring and $f \in \mathbb{A}[Y]$ a non-constant polynomial. We denote by D_f the discriminant of f.

Proposition

Let $U \subset \mathbb{C}$ be a domain, let $A := \mathcal{O}(U)$ be the ring of holomorphic functions in U. For $f \in A[Y]$ monic and $x \in U$, we write

$$f_x := Y^k + a_1(x)Y^{k-1} + \cdots + a_k(x) \in \mathbb{C}[Y].$$

Then f_x has a multiple root in $\mathbb{C}$ if and only if $D_f(x) = 0$ holds.

Proof

- By the specialization property of resultants, we have $D_f(x) = D_{f_x}$.
- Then, the assertion follows from definition of discriminants of D_{f_x}.

Puiseuxs Theorem (geometric version)

Let $f(X,Y) = Y^k + a_1(X)Y^{k-1} + \cdots + a_k(X) \in \mathbb{C}\langle X\rangle[Y], k \geq 1$ be an irreducible Weierstrass polynomial. (Note that f could have irreducible factors that are not Weierstrass polynomials.) Let $\rho > 0$ be chosen such that

a) $a_1, \ldots, a_k$ converge in $U := \{x \in \mathbb{C} \mid |x| < \rho\}$,

b) $D_f(x) \neq 0$ in $U^* := U \setminus \{0\}$.

Furthermore, let

$$\begin{aligned} V &:= \{t \in \mathbb{C} \mid |t| < \rho^{\frac{1}{k}}\}, \\ \mathcal{C} &:= \{(x,y) \in U \times \mathbb{C} : f(x,y) = 0\}. \end{aligned}$$

Then, there exists a series $\varphi \in \mathbb{C}\langle T\rangle$ that converges in V and has the following properties:

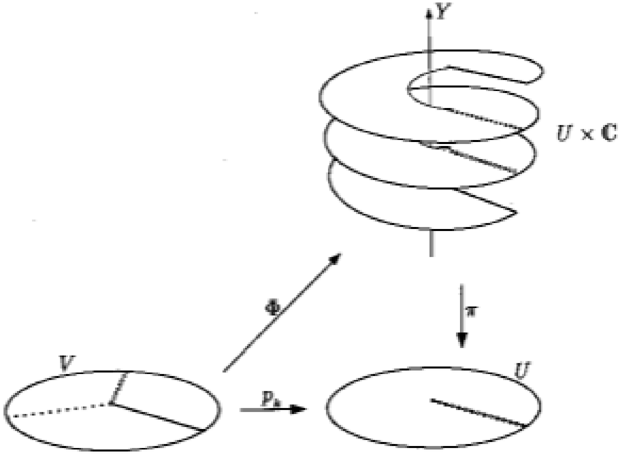
i) we have $f(t^k, \varphi(t)) = 0$ for all $t \in V$;

ii) the map $\Phi : V \to \mathcal{C},\ t \mapsto (t^k, \varphi(t))$, is bijective.

Illustration of the geometric version Puiseux's Theorem

The situation for $k = 3$ and $\rho = 1$ is illustrated in the following sketch. Only the real component of the Y-direction is drawn.

- $p_k : V \to U$ is given by $t \mapsto t^k$,
- $\pi : U \times \mathbb{C} \to U$, $(x, y) \mapsto x$, is projection.



Factoring Weierstrass polynomials (1/3)

Notations and hypotheses (recall)

- Let $f = Y^k + a_1(X)Y^{n-1} + \cdots + a_k(X) \in \mathbb{C}\langle X\rangle[Y]$ be an irreducible Weierstrass polynomial, with degree $k \geq 1$.
- Let $\rho > 0$ be chosen such that the series $a_1, \ldots, a_k$ converge in the open set $U := \{x \in \mathbb{C} \mid |x| < \rho\}$.
- The discriminant $\operatorname{discrim}(f, Y)(x)$ is not zero for all $x \in U \setminus \{0\}$.
- Let $V := \{t \in \mathbb{C} \mid |t| < \rho^{\frac{1}{k}}\}$.
- Let $\mathcal{C} := \{(x, y) \in U \times \mathbb{C} \mid f(x, y) = 0\}$.
- From the geometric version of Puiseux's theorem, there exists a power series $\phi \in \mathbb{C}\langle T\rangle$ that converges in V and has the following properties:
    1. for all $t \in V$, we have $f(t^k, \phi(t)) = 0$,
    2. $\Psi : V \to \mathcal{C},\ t \longmapsto (t^k, \phi(t))$ is bijective.

Factoring Weierstrass polynomials (2/3)

Proposition

Let $\zeta = \exp(2\pi\imath/k)$ be a k-th primitive root of unity. For all $i = 1, \ldots, k$, we define

$$\varphi_i = \varphi(\zeta^i t) \quad \text{and} \quad \Phi_i := (t^k, \varphi_i(t))$$

Then, $\Phi_1, \ldots, \Phi_k$ are distinct parametrizations of $\mathcal{C}$, that is, the series $\varphi_1, \ldots, \varphi_k$ are distinct.

Proof

- The maps $V \to V,\ t \longmapsto \zeta^i t$ are bijective. Moreover, they are distinct.
- Hence, the bijective maps $\Phi_1, \ldots, \Phi_k$ are distinct.

Remark

From a geometric point of view, the maps $\Phi_1, \ldots, \Phi_k$ differ from each other by permutations of the sheets of the covering map $\pi^* : \mathcal{C}^* \to U^*$. Thus, the roots of unity act as "covering transformations".

Factoring Weierstrass polynomials (3/3)

Remark

The parametrizations $\varphi_1, \ldots, \varphi_k$ can be used to extend each factorization

$$f_x(Y) = (Y - c_1) \cdots (Y - c_n), \quad \text{where} \quad c_i \in \mathbb{C}$$

for $x \in U \setminus \{0\}$, to the entire U.

Corollary

Let $(T^k, \varphi(T))$ be a parametrization given by the geometric version of Puiseux's theorem. Let $\zeta, \varphi_1, \ldots, \varphi_k$ be as in the previous proposition. Then, the following holds in $\mathbb{C}\langle T \rangle[Y]$

$$f(T^k, Y) \;=\; (Y - \varphi_1(T)) \cdots (Y - \varphi_k(T)).$$

Proof

Each of $\varphi_1, \ldots, \varphi_k$ is a distinct root in $\mathbb{C}\langle T \rangle$ of the polynomial $f(T^k, Y) \in \mathbb{C}\langle T \rangle[Y]$.

Complement on the algebraic version Puiseux's theorem (1/3)

Notations

- Let $f \in \mathbb{C}\langle X, Y\rangle$ be general in Y.
- Let $n \in \mathbb{N}$ and $\varphi(S) \in \mathbb{C}[[S]]$ be defining a solution to the algebraic version Puiseux's theorem, that is, $f(S^n, \varphi(S)) = 0$ holds in $\mathbb{C}[[S]]$.
- By the preparation theorem, there exist a unit $\alpha \in \langle X, Y\rangle$ and irreducible Weierstrass polynomials $p_1, \ldots, p_r \in \mathbb{C}\langle X\rangle[Y]$ so that $f = \alpha p_1 \cdots p_r$

Observations

- Since $\alpha(S^n, \varphi(S)) \neq 0$, there exists $j \in \{1, \ldots, r\}$ such that $p_j(S^n, \varphi(S)) = 0$ holds.
- Therefore, w.l.o.g. one can assume that f is an irreducible Weierstrass polynomial of $\mathbb{C}\langle X\rangle[Y]$ of degree k and of which φ is a formal solution in the sense of the algebraic version Puiseux's theorem.

Complement on the algebraic version Puiseux's theorem (2/3)

Observations

- From the previous corollary, there exist $\varphi_1, \ldots, \varphi_k \in \mathbb{C}\langle T \rangle$ such that we have in $\mathbb{C}\langle T \rangle[Y]$
$$f(T^k, Y) \ = \ (Y - \varphi_1(T)) \cdots (Y - \varphi_k(T)).$$
- In the algebraic of version Puiseux's theorem, the *denominator* n can be as large as desired. Thus we can assume $n = \ell k$, for some ℓ.
- Therefore, we have in $\mathbb{C}[[S]][Y]$
$$f(S^n, Y) \ = \ (Y - \varphi_1(S^\ell)) \cdots (Y - \varphi_k(S^\ell)).$$
- Since $\varphi \in \mathbb{C}[[S]]$ is also a zero of $f(S^n, Y)$ and since $\mathbb{C}[[S]][Y]$ is an integral domain, we have $\varphi_i = \varphi$, for some i. Hence φ is convergent.

Corollary

If $f \in \mathbb{C}\langle X, Y \rangle$ is an irreducible power series, general in Y of order k, then there exists a convergent power series $\phi \in \mathbb{C}\langle T \rangle$ such that $f(T^k, \phi(T)) = 0$ holds in $\mathbb{C}\langle T \rangle$.

Complement on the algebraic version Puiseux's theorem (3/3)

Corollary

If $f \in \mathbb{C}\langle X, Y\rangle$ is irreducible in $\mathbb{C}\langle X, Y\rangle$, then it is also irreducible in $\mathbb{C}[[X, Y]]$. (Thus, for power series, there is no change in the divisibility theory in passing from convergent to formal power series.)

Proof of the corollary

- We may assume that f is a Weierstrass polynomial of degree k.
- Since it is irreducible in $\mathbb{C}\langle X, Y\rangle$, the geometric version of Puiseux's theorem applies. Thus, there exist convergent power series $\varphi_1, \ldots, \varphi_k$ such that we have

$$f(T^k, Y) = (Y - \varphi_1(T)) \cdots (Y - \varphi_k(T)).$$

- Since each factor on the right hand side of the above equality belongs to $\mathbb{C}\langle X, Y\rangle$ and since $\mathbb{C}[[X, Y]]$ is a unique factorization domain, it follows that all possible formal factor of f are necessarily convergent power series. This yields the conclusion.