Factoring polynomials over discrete valuation rings

Adrien Poteaux[⋆] & Martin Weimann[✈]

⋆: CFHP - CO2 - CRIStAL - Université de Lille

✈: GAATI - Université de Polynésie Française

7 février 2019

Journées Nationales de Calcul Formel

CIRM, Luminy

One example

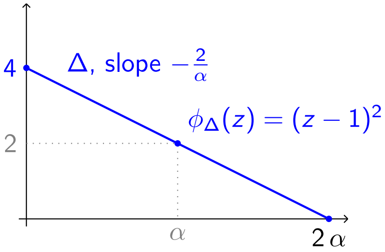
$$F = (y^\alpha - x^2)^2 + x^\alpha \in \mathbb{A}[y] \text{ with } \mathbb{A} = \mathbb{C}[[x]]$$

- $d = \deg(F) = 2\,\alpha$,
- $\delta = \upsilon_x(\mathrm{Disc}(F)) = 2\,\alpha^2 - 4\,\alpha + 4$.
- Assume $\alpha > 4$ odd.

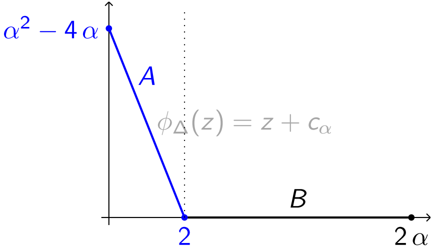
Is F irreducible in $\mathbb{C}[[x]][y]$?

Using the Newton-Puiseux algorithm.

$$F = (y^\alpha - x^2)^2 + x^\alpha$$



1. $G \leftarrow F(x^\alpha, x^2(y+1))/x^{4\,\alpha}$,
2. Hensel: $G = A \cdot B$,
3. Recursive call with A

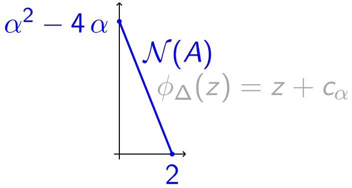


Polynomial	size
F	$\Theta(\alpha^2) = \Theta(\delta)$
G	$\Theta(\alpha^3) = \Theta(d\,\delta)$
A	$\Theta(\alpha^2) = \Theta(\delta)$

Answer: Yes complexity: $\Theta(d\,\delta)$ Answer in $\mathcal{O}(\delta)$?

Another way ?

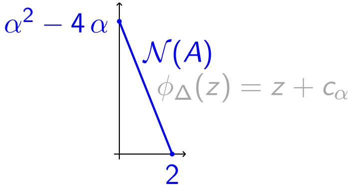
$$F = (y^\alpha - x^2)^2 + x^\alpha$$



- Writing $\psi = y^\alpha - x^2$, we have $F = \psi^2 + x^\alpha$,
  - Can we "guess" the second Newton polygon from $\psi^2 + x^\alpha$?
  - Can we "read" ϕ_Δ ?

Another way ?

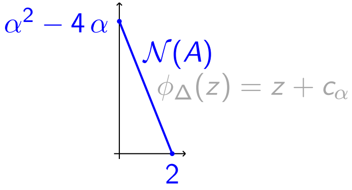
$$F = (y^\alpha - x^2)^2 + x^\alpha$$



- Writing $\psi = y^\alpha - x^2$, we have $F = \psi^2 + x^\alpha$,
  - Can we "guess" the second Newton polygon from $\psi^2 + x^\alpha$?
  - Can we "read" ϕ_Δ ?
- Key ingredients:
  - $\psi = \sqrt[2]{F}$ is an approximate root of F,
  - $F = \psi^2 + x^\alpha$ is the ψ-adic expansion of F.

Another way ?

$$F = (y^\alpha - x^2)^2 + x^\alpha$$



- Writing $\psi = y^\alpha - x^2$, we have $F = \psi^2 + x^\alpha$,
  - Can we “guess” the second Newton polygon from $\psi^2 + x^\alpha$?
  - Can we “read” ϕ_Δ ?
- Key ingredients:
  - $\psi = \sqrt[2]{F}$ is an approximate root of F,
  - $F = \psi^2 + x^\alpha$ is the ψ-adic expansion of F.
- Questions:
  - Why x^α corresponds to $\alpha^2 - 4\,\alpha$?
  - How to recover the correct characteristic polynomial ?

This talk

Context:

- $\mathbb{A}$ a discrete valuation ring (e.g. $\mathbb{K}((x))$, $\mathbb{Q}_p$),
- $v_{\mathbb{A}}$ valuation over $\mathbb{A}$ (e.g. v_x, v_p),
- $F \in \mathbb{A}[y]$ (monic).

Objective(s):

1. Irreducibility test in $\mathbb{A}[y]$,
2. Factorisation of F in $\mathbb{A}[y]$.
3. Case $\mathbb{A} = \mathbb{K}[[x]]$: Puiseux series of F ?

Notations: $d = \deg(F)$; $\delta = v_{\mathbb{A}}(\mathrm{Disc}(F))$

Approximate root of $F \in \mathbb{A}[y]$ monic [Ab10]

- Hyp: $\mathrm{char}(\mathbb{A})$ does not divide d,
- Let $N \in \mathbb{N}$ dividing d,

Proposition

There is an unique monic $\psi \in \mathbb{A}[y]$ such that:

- $\deg(\psi) = d/N$,
- $\deg(F - \psi^N) < d - d/N$,

$\rightsquigarrow$ $\psi = \sqrt[N]{F}$ is the N-th approximate root of F.

Example: $\psi = \sqrt[d]{F} = y + \dfrac{a_{d-1}}{d}$ is the d-th approximate root of F.

Valuations on $\mathbb{A}[y]$

- Gauss valuation:
  - $F = \sum_i a_i\, y^i$,
  - $v_0(F) = \min_i v_{\mathbb{A}}(a_i)$.
- Extended valuation: given $\psi \in \mathbb{A}[y]$ monic, $\frac{m}{q} \in \mathbb{Q}$:
  - $v_\psi = (v_0, \psi, \frac{m}{q})$ *extends* v_0.

    Defined by $v_\psi(\psi) = m\,q$, $v_\psi(y) = m$ and $v_\psi(x) = q$,
  - Expand $F = \sum_i a_i(y)\,\psi^i$ with $\deg(a_i) < \deg(\psi)$,
  - Generalised Newton polygon:

    $\mathcal{N}_\psi(F)$ is the lower convex hull of $(i, v_\psi(a_i\,\psi^i) - v_\psi(F))_i$.

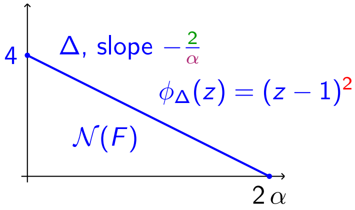
Improving the irreducibility test

generalisation of the work of Abhyankhar to $\mathbb{A}[y]$.

link with the Newton–Puiseux algorithm for $\mathbb{A} = \mathbb{K}((x))$

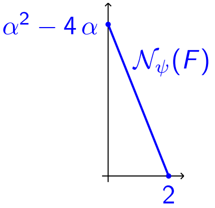
We get the second Newton polygon !

$$F = (y^\alpha - x^2)^2 + x^\alpha$$



With $m = 2$, $q = \alpha$, $\psi = \sqrt[2]{F}$, we get:

- $F = \psi^2 + x^\alpha$.
- $v_\psi(F) = 4\,\alpha$
- $v_\psi(\psi^2) - v_\psi(F) = 0$,
- $v_\psi(x^\alpha) - v_\psi(F) = \alpha^2 - 4\,\alpha$.



Reminder: $v_\psi(x) = \alpha \quad v_\psi(y) = 2 \quad v_\psi(\psi) = 2\,\alpha$

Complexity ?

- Computing $\sqrt[N]{F}$: $\mathcal{O}(\mathsf{M}(d)) = \tilde{\mathcal{O}}(d)$ op in $\mathbb{A}$.
  - $F_\infty = y^d\, F(1/y)$ the reciprocal polynomial of F,
  - $F_\infty(0) = 1 \rightsquigarrow \exists!\, \phi \in \mathbb{A}[[y]]$ s.t. $\phi(0) = 1$ and $\phi^N = F_\infty$,
  - ϕ is the root of $Z^N - F_\infty = 0 \rightsquigarrow$ Newton iteration !
  - ψ is the reciprocal polynomial of $\lceil \phi \rceil^{\frac{d}{N}}$

Complexity ?

- Computing $\sqrt[N]{F}$: $\mathcal{O}(\mathsf{M}(d)) = \tilde{\mathcal{O}}(d)$ op in $\mathbb{A}$.
  - $F_\infty = y^d\, F(1/y)$ the reciprocal polynomial of F,
  - $F_\infty(0) = 1 \rightsquigarrow \exists!\, \phi \in \mathbb{A}[[y]]$ s.t. $\phi(0) = 1$ and $\phi^N = F_\infty$,
  - ϕ is the root of $Z^N - F_\infty = 0 \rightsquigarrow$ Newton iteration !
  - ψ is the reciprocal polynomial of $\lceil \phi \rceil^{\frac{d}{N}}$
- ψ-adic expansion: $\mathcal{O}(\mathsf{M}(d)\log(N)) = \tilde{\mathcal{O}}(d)$ op in $\mathbb{A}$.
  - $F = A\,\psi^{\frac{N}{2}} + B \rightsquigarrow \mathcal{O}(\mathsf{M}(d))$
  - Recursive call on A and B.

Complexity ?

- Computing $\sqrt[N]{F}$: $\mathcal{O}(\mathsf{M}(d)) = \tilde{\mathcal{O}}(d)$ op in $\mathbb{A}$.
  - $F_\infty = y^d\, F(1/y)$ the reciprocal polynomial of F,
  - $F_\infty(0) = 1 \rightsquigarrow \exists!\ \phi \in \mathbb{A}[[y]]$ s.t. $\phi(0) = 1$ and $\phi^N = F_\infty$,
  - ϕ is the root of $Z^N - F_\infty = 0 \rightsquigarrow$ Newton iteration !
  - ψ is the reciprocal polynomial of $\lceil \phi \rceil^{\frac{d}{N}}$
- ψ-adic expansion: $\mathcal{O}(\mathsf{M}(d)\log(N)) = \tilde{\mathcal{O}}(d)$ op in $\mathbb{A}$.
  - $F = A\,\psi^{\frac{N}{2}} + B \rightsquigarrow \mathcal{O}(\mathsf{M}(d))$
  - Recursive call on A and B.
- Truncation: $n = 2\,\delta/d$.

Total cost: $\delta\,\mathrm{plog}(d)$!

Miscellaneous

- More than one Newton–Puiseux recursive call ?
  - Compute successive approximate roots $\psi_0, \cdots, \psi_k$ $\qquad \psi_{-1} = x$
  - Recursive augmented valuations $\upsilon_k = (\upsilon_{k-1}, \psi_k, \frac{m_k}{q_k})$:

$$\begin{cases} \upsilon_k(\psi_i) = q_k \upsilon_{k-1}(\psi_i) & -1 \leq i < k-1 \\ \upsilon_k(\psi_{k-1}) = q_k \upsilon_{k-1}(\psi_{k-1}) + m_k \\ \upsilon_k(\psi_k) = q_k \upsilon_k(\psi_{k-1}) \end{cases}$$

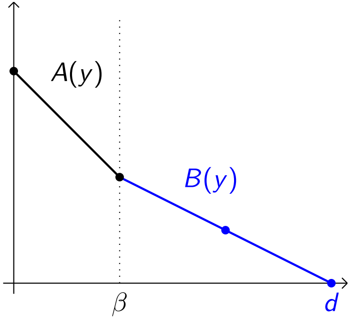
  - $\mathcal{N}_k(F)$ via generalised $(\psi_0, \cdots, \psi_k)$-adic expansions
- Compute the characteristic polynomials ?
  - The coefficients of the ψ-adic expansions must be *corrected*,
  - Compute some $\lambda_k(\psi_i) \in \mathbb{K}_k$ (tower of fields).
- Make a single (univariate) irreducibility test ?
  - Rely on dynamic evaluation.

Hensel–Newton algorithm and extended valuations

Slope factorisation [CaRoVa16]

$$F(y) = \sum_{i=0}^{d} a_i\, y^i$$

- β a "break" of $\mathcal{N}(F)$,
- $A_0 = \sum_{i=0}^{\beta} a_i y^i,\ V_0 = 1,$



Newton iteration:

$$\begin{aligned} A_{k+1} &= A_k + (V_k\, F \% A_k) \\ B_{k+1} &= F \mathbin{/\!/} A_{k+1} \\ V_{k+1} &= (2\,V_k - V_k^2\, B_{k+1}) \% A_{k+1} \end{aligned}$$

Factorisation up to precision $n \rightsquigarrow \tilde{\mathcal{O}}(n\, d)$

Hensel lemma works with extended valuations

Lemma

Assume $B = \psi^b + \cdots$ *and* $v(B) = b\,v(\psi)$. *Then*

- $v(A\%B) \geq v(A)$,
- $v(A \mathbin{/\!\!/} B) \geq v(A) - v(B)$.

Hensel lemma works with extended valuations

Lemma

Assume $B = \psi^b + \cdots$ *and* $v(B) = b\,v(\psi)$. *Then*

- $v(A \% B) \geq v(A)$,
- $v(A \mathbin{/\!/} B) \geq v(A) - v(B)$.

Theorem

Assume

- $v(F - G\,H) \geq v(F) + n$ *and* $v(S\,G + T\,H - 1) \geq n$.

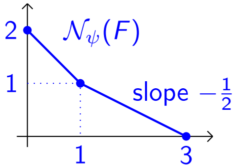
Then $\tilde{G}, \tilde{H}, \tilde{S}, \tilde{T} = \texttt{HenselStep}(F, G, H, S, T)$ *satisfies:*

- $v(F - \tilde{G}\,\tilde{H}) \geq v(F) + 2\,n$,
- $v(\tilde{S}\,\tilde{G} + \tilde{T}\,\tilde{H} - 1) \geq 2\,n$.

Good initialisation ?

$$F = \psi^3 + y^2 x^3 \psi + x^6 y \text{ with } \psi = y^3 - x^2$$

- $v_\psi(x) = 3$, $v_\psi(y) = 2$, $v_\psi(\psi) = 6$.
- Extend v_ψ with the lower edge:
  $v(x) = 6$, $v(y) = 4$, $v(\psi) = 13$

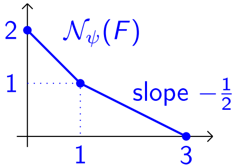


- $G_0 = \overbrace{\psi^2 + y^2 x^3}^{26}$, $H_0 = \overbrace{\psi}^{13} \Longrightarrow \overbrace{F}^{39} - G_0 H_0 = \overbrace{x^6 y}^{40}$

Good initialisation ?

$$F = \psi^3 + y^2 x^3 \psi + x^6 y \text{ with } \psi = y^3 - x^2$$

- $v_\psi(x) = 3$, $v_\psi(y) = 2$, $v_\psi(\psi) = 6$.
- Extend v_ψ with the lower edge:
  $v(x) = 6$, $v(y) = 4$, $v(\psi) = 13$



- $G_0 = \overbrace{\psi^2 + y^2 x^3}^{26}$, $H_0 = \overbrace{\psi}^{13} \implies \overbrace{F}^{39} - G_0 H_0 = \overbrace{x^6 y}^{40}$
- With $s_0 = 1$ and $t_0 = -T$, we have $s_0 (T^2 + 1) + t_0 T = 1$,
- $S_0 = \underbrace{x^{-5} y}_{-26}$, $T_0 = \underbrace{-x^{-5} y \psi}_{-13} \implies S_0 G_0 + T_0 H_0 - 1 = \underbrace{x^{-2}\psi}_{1}$

State of the art (sketch)

- Abhyankar-Moh [Ab06]: approximate roots,
- Mac Lane, Abhyankar [Ma36², Ab90, Ru14]: extended valuations,
- Montes et al [Mo99,GuMoNa11&12,BaNaSt13,GuNaPa12] $\mathcal{O}(d^2 + d\delta^2)$,
- Caruso et al [CaRoVa16]: slope factorisation,

Case $\mathbb{A} = \mathbb{K}[[x]]$:

- Sasaki et al [KaSa99,AlAtMa17]: Extended Hensel Construction at least $\mathcal{O}(d^2\,(\delta + d^2))$,
- Puiseux [PoRy15,PoWe]: Newton–Puiseux algorithm $\mathcal{O}(d\,\delta)$.

Conclusion

- Irreducibility test in $\mathbb{A}[y]$ in $\mathcal{O}(\delta)$, $\leftarrow$ improved by a factor d !
- "direct" factorisation in $\mathbb{A}[y]$: $\mathcal{O}(\rho\, n\, d)$, $\leftarrow$ was $\mathcal{O}(n\, d^2)$
- Sage prototype,
- "Bivariate" computations above the *residue field* of $\mathbb{A}$ (no field extension).
- Puiseux series ?
  - $N_1 = d/2$: $\psi_1 = \psi_0^2 + X^{m_1} S_1(X)^2$

  $\rightsquigarrow$ $S_1(X)$ is an approximate root ($\rightsquigarrow$ Newton iteration !)
  - $q_1 > 2$? Solving some linear system ?

Example: if $S_1(x) = x^{\frac{1}{3}}\, P_1(x) + x^{\frac{2}{3}}\, P_2(x)$,

$$\psi_1 = \psi_0^3 - 3\, x\, P_1\, P_2\, \psi_0 - x\, P_1^3 - x^2\, P_2^3$$

Bibliographie

S. Abhyankar.
Irreducibility criterion for germs of analytic functions of two complex variables.
Adv. Mathematics, 35:190–257, 1989.

S. Abhyankar.
Algebraic Geometry for Scientists and Engineers, volume 35 of *Mathematical surveys and monographs*.
Amer. Math. Soc., 1990.

S. Abhyankar.
Lectures on Algebra.
Number vol. 1 in Lectures on Algebra. World Scientific, 2006.

P. Alvandi, M. Ataei, and M. Moreno Maza.
On the extended hensel construction and its application to the computation of limit points.
In ISSAC '17, pages 13–20.

J.-D. Bauch, E. Nart, and H. Stainsby.

Complexity of the OM factorizations of polynomials over local fields.
LMS Journal of Computation and Mathematics, 16:139–171, 2013.

X. Caruso, D. Roe, and T. Vaccon.
Division and slope factorization of p-adic polynomials.
In ISSAC '16, pages 159–166.

J. v. z. Gathen and J. Gerhard.
Modern Computer Algebra.
Cambridge University Press, New York, NY, USA, 3rd edition, 2013.

J. Guàrdia, J. Montes, and E. Nart.
Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields.
J. Théor. Nombres Bordx., 23(3):667–696, 2011.

J. Guàrdia, J. Montes, and E. Nart.

Newton polygons of higher order in algebraic number theory.
Transsactions of the American Mathematical Society, 364:361–416, 2012.

J. Guàrdia, E. Nart, and S. Pauli.
Single-factor lifting and factorization of polynomials over local fields.
Journal of Symbolic Computation, 47(11):1318 – 1346, 2012.

F. Kako and T. Sasaki.
Solving multivariate algebraic equations by Hensel construction.
Japan J. of Industrial and Applied Math., 16:257–285, 1999.

S. MacLane.
A construction for absolute values in polynomial rings.
Trans. Amer. Math. Soc., 40(3):363–395, 1936.

S. Mac Lane.

A construction for prime ideals as absolute values of an algebraic field.
Duke Math. J., 2(3):492–510, 1936.

J. Montes Peral.
Polígonos de newton de orden superior y aplicaciones aritméticas.
PhD thesis, Universitat de Barcelona, 1999.

A. Poteaux and M. Rybowicz.
Improving complexity bounds for the computation of puiseux series over finite fields.
ISSAC '15, pages 299–306

A. Poteaux and M. Weimann.
Computing Puiseux series: a fast divide and conquer algorithm.
arXiv:1708.09067, pages 1–27, 2017.

J. Rüth.
Models of curves and valuations.

PhD thesis, Universität Ulm, 2014.