On the OM algorithm

Adrien Poteaux*

*: CFHP - CO2 - CRIStAL - Université de Lille

joint work with Weimann, Nart et al...

June 19th, 2026

CAIPI, Caen

Context

- (K, v) a value field.

  $\rightsquigarrow v$ of rank 1 *not necessarily discrete*

$$v(0) = \infty$$

$$\forall a, b \in K, v(a\,b) = v(a) + v(b)$$

$$v(a + b) \geq \min(v(a), v(b))$$

Context

- (K, v) a value field.

  $\rightsquigarrow v$ of rank 1 *not necessarily discrete*

- $\mathbb{A}$ the completion of the valuation ring. $\{a \in K \mid v(a) \geq 0\}$

$$v(0) = \infty$$

$$\forall a, b \in K, v(a\,b) = v(a) + v(b)$$

$$v(a + b) \geq \min(v(a), v(b))$$

Context

- (K, v) a value field.

  $\rightsquigarrow v$ of rank 1 *not necessarily discrete*

- $\mathbb{A}$ the completion of the valuation ring. $\{a \in K \mid v(a) \geq 0\}$
- $\mathbb{F}$ the residue field. $\mathfrak{m} = \{a \in K \mid v(a) > 0\}$; $\mathbb{F} = \mathbb{A}/\mathfrak{m}$

$$v(0) = \infty$$

$$\forall a, b \in K, v(a\,b) = v(a) + v(b)$$

$$v(a + b) \geq \min(v(a), v(b))$$

Context

- (K, v) a value field.

  $\rightsquigarrow v$ of rank 1 *not necessarily discrete*

- $\mathbb{A}$ the completion of the valuation ring. $\{a \in K \mid v(a) \geq 0\}$
- $\mathbb{F}$ the residue field. $\mathfrak{m} = \{a \in K \mid v(a) > 0\}$; $\mathbb{F} = \mathbb{A}/\mathfrak{m}$

K	v	$\mathbb{A}$	$\mathbb{F}$
$\mathbb{K}(t)$	ord_t	$\mathbb{K}[[t]]$	$\mathbb{K}$
$\mathbb{Q}$	ord_p	$\mathbb{Z}_p$	$\mathbb{F}_p$
$\mathbb{K}(t_1, t_2)$	$\begin{cases} v(t_1) = 1 \\ v(t_2) = \sqrt{2} \end{cases}$	$\underbrace{\mathbb{K}[[t_1, t_2]]^{++}}_{\frac{t_2}{t_1} \in \mathbb{A}}$	$\mathbb{K}$

$v(0) = \infty$

$\forall a, b \in K, v(a\,b) = v(a) + v(b)$

$v(a + b) \geq \min(v(a), v(b))$

Context

- (K, v) a value field.

  $\rightsquigarrow v$ of rank 1 *not necessarily discrete*

- $\mathbb{A}$ the completion of the valuation ring. $\{a \in K \mid v(a) \geq 0\}$
- $\mathbb{F}$ the residue field. $\mathfrak{m} = \{a \in K \mid v(a) > 0\}$; $\mathbb{F} = \mathbb{A}/\mathfrak{m}$

K	v	$\mathbb{A}$	$\mathbb{F}$
$\mathbb{K}(t)$	ord_t	$\mathbb{K}[[t]]$	$\mathbb{K}$
$\mathbb{Q}$	ord_p	$\mathbb{Z}_p$	$\mathbb{F}_p$
$\mathbb{K}(t_1, t_2)$	$\begin{cases} v(t_1) = 1 \\ v(t_2) = \sqrt{2} \end{cases}$	$\underbrace{\mathbb{K}[[t_1, t_2]]^{++}}_{\frac{t_2}{t_1} \in \mathbb{A}}$	$\mathbb{K}$

Problem

1. $P \in \mathbb{A}[x]$ irreducible ?
2. Factorisation in $\mathbb{A}[x]$? (up to a given precision)

Context

- (K, v) a value field.

  $\rightsquigarrow v$ of rank 1 *not necessarily discrete*

- $\mathbb{A}$ the completion of the valuation ring. $\{a \in K \mid v(a) \geq 0\}$
- $\mathbb{F}$ the residue field. $\mathfrak{m} = \{a \in K \mid v(a) > 0\}$; $\mathbb{F} = \mathbb{A}/\mathfrak{m}$
- $\overline{v}$ the extension of v to $\overline{K}$.

K	v	$\mathbb{A}$	$\mathbb{F}$
$\mathbb{K}(t)$	ord_t	$\mathbb{K}[[t]]$	$\mathbb{K}$
$\mathbb{Q}$	ord_p	$\mathbb{Z}_p$	$\mathbb{F}_p$
$\mathbb{K}(t_1, t_2)$	$\begin{cases} v(t_1) = 1 \\ v(t_2) = \sqrt{2} \end{cases}$	$\underbrace{\mathbb{K}[[t_1, t_2]]^{++}}_{\frac{t_2}{t_1} \in \mathbb{A}}$	$\mathbb{K}$

Problem

1. $P \in \mathbb{A}[x]$ irreducible ?
2. Factorisation in $\mathbb{A}[x]$? (up to a given precision)

Successive factorisations (residual polynomial dissection)

1. dissection according to residual polynomials,
2. factorisation via a generalised Hensel lemma.

Augmented valuations: chains $\mu_0 < \mu_1 < \cdots < w_P$ (P irreducible).

Key polynomials: $\phi_k \in K[x]$ "representative" of μ_k ; $\deg(\phi_k) \leq \deg(\phi_{k+1})$

- $\mu_k(\phi_{k-1}) = w_P(\phi_{k-1})$
- "Optimal" chain: $\deg(\phi_k) < \deg(\phi_{k+1})$

Approximate roots: "optimal" key polynomials $\rightsquigarrow$ $\begin{array}{l} \mathrm{Char}(\mathbb{F}) = 0 \\ \mathrm{Char}(\mathbb{F}) \nmid \deg(P) \end{array}$

Algorithms for number fields ($\mathbb{A} = \mathbb{Z}_p$)

- Ore (1920's): prime ideal decomposition of p in $\mathbb{Q}[x]/(g)$:
  1. computing Newton polygons of g according to a valuation of $\mathbb{Q}[x]$,
  2. factorisation of residual polynomials of g (slope of the polygon).
- MacLane (1930's): *augmented valuations* of v in $K[x]/(g)$.
  - chains $\mu_0 < \mu_1 < \cdots < \mu_n < \cdots < \mu$ (one by factor of g),
  - using *key polynomials* associated to μ_k.
- Okutsu (1982): integral bases, no valuation / key polynomial.
- Montes (1999): OM-algorithm - Ore, MacLane, Okutsu, Montes.

  Nart et al (2010'): discriminant computation, integral basis...
- Vaquié / Herrera - Olalla - Mahboub - Spivakosky (2000's):

  generalisation of MacLane for any value field.
- cluster roots / Berkovich skeletons (P. Vaccon Weimann 2025 & 2026)

Algebraic curves / Functions fields ($\mathbb{A} = \mathbb{K}[[t]]$)

- Singularity of plane algebraic curves.
  - Newton–Puiseux algorithm (Duval, P., Rybowicz, Weimann)
  - valuations and Puiseux expansions (Abhyankhar, P., Weimann)
  - equisingularity types (P. & Weimann)
- genus computation (Riemann-Hurwitz formula).
- computing Riemann-Roch spaces (Hess, Darkaoui & Weimann).
- Factorisation in $\mathbb{K}[t, x]$ (Weimann).

Valuations of $K[x]$

A tree of valuations

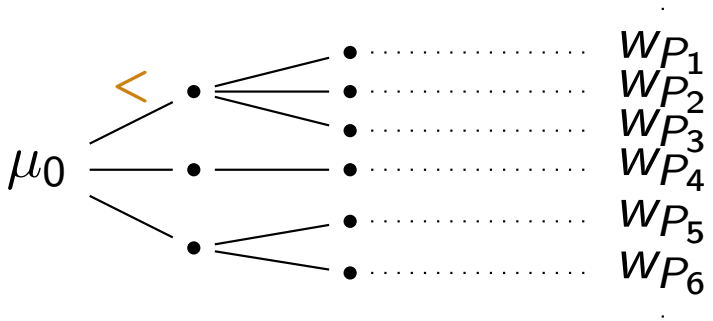
Definition (order on valuations)

- $\mu \leq \mu'$ *if* $\mu(g) \leq \mu'(g)$ *for all* $g \in K[x]$,
- $\mu < \mu'$ *if* $\mu \leq \mu'$ *and* $\mu \neq \mu'$.

A tree of valuations

Definition (order on valuations)

- $\mu \leq \mu'$ *if* $\mu(g) \leq \mu'(g)$ *for all* $g \in K[x]$,
- $\mu < \mu'$ *if* $\mu \leq \mu'$ *and* $\mu \neq \mu'$.



- Gauss valuation: $\mu_0(\sum_i a_i x^i) := \min_i v(a_i)$.
- P irreducible: $w_P(g) := \overline{v}(g(\theta))$ with $P(\theta) = 0$.

Computing w_P from μ_0: one example

$$P = ((x-2)^2 - 27)^5 + 3^{15}(x-2) \in \mathbb{Q}[x] \quad ; \quad v = \mathrm{ord}_3$$

- $\theta = 2 + 3^{\frac{3}{2}} + \frac{1}{2}3^{\frac{9}{5}} + \cdots$

Some valuations:

- $w_P(x) = \overline{v}(\theta) = \overline{v}(2) = 0$
- $\phi_0 = x - 2$; $w_P(\phi_0) = \overline{v}(\theta - 2) = \overline{v}(3^{\frac{3}{2}}) = \frac{3}{2}$
- $\phi_1 = (x-2)^2 - 27$; $w_P(\phi_1) = \overline{v}(3^{\frac{3}{2}}3^{\frac{9}{5}}) = \frac{33}{10}$

We will show how to construct:

$$\mu_0 \text{ ——— } \mu_1(\phi_0) = \tfrac{3}{2} \text{ ——— } \mu_2(\phi_1) = \tfrac{33}{10} \text{ ——— } w_P$$

Residual and key polynomials

associated to μ_0

$$P = ((x-2)^2 - 27)^5 + 3^{15}(x-2) \qquad \mu_0(P) = 0$$

- $\mathrm{in}_{\mu_0}(P) = (x-2)^{10}$.

$$R_{\mu_0}(P)(y) = (y-2)^{10}$$

Residual and key polynomials

associated to μ_0

$$P = ((x-2)^2 - 27)^5 + 3^{15}(x-2) \qquad \mu_0(P) = 0$$

- $\mathrm{in}_{\mu_0}(P) = (x-2)^{10}$.

$$R_{\mu_0}(P)(y) = (y-2)^{10}$$

- Representative: $\phi_0 := x - 2 \in \mathrm{KP}(\mu_0)$.

Residual and key polynomials

associated to μ_0

$$P = ((x-2)^2 - 27)^5 + 3^{15}(x-2) \qquad \mu_0(P) = 0$$

- $\mathrm{in}_{\mu_0}(P) = (x-2)^{10}$.

$$R_{\mu_0}(P)(y) = (y-2)^{10}$$

- Representative: $\phi_0 := x - 2 \in \mathrm{KP}(\mu_0)$.

$$\mu_0(\phi_0) = 0 < w_P(\phi_0) = \tfrac{3}{2}.$$ Getting $\frac{3}{2}$?

Generalised Newton polygon

associated to μ_0, ϕ_0

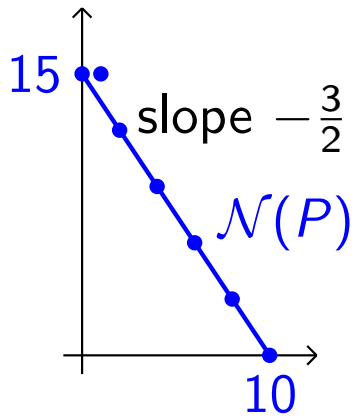
- (μ, ϕ) a *type*, i.e. $\phi \in \mathrm{KP}(\mu)$.
- Taylor expansion: $g = \sum_i a_i \phi^i$ with $\deg(a_i) < \deg(\phi)$.
- Generalised Newton polygon: $\mathcal{N}_{\mu,\phi}(g) = \mathrm{Conv}\{(i, \mu(a_i))\}$.

Generalised Newton polygon

associated to μ_0, ϕ_0

- (μ, ϕ) a *type*, i.e. $\phi \in \mathrm{KP}(\mu)$.
- Taylor expansion: $g = \sum_i a_i \phi^i$ with $\deg(a_i) < \deg(\phi)$.
- Generalised Newton polygon: $\mathcal{N}_{\mu,\phi}(g) = \mathrm{Conv}\{(i, \mu(a_i))\}$.

$$P = (\phi_0^2 - 27)^5 + 3^{15}\,\phi_0$$



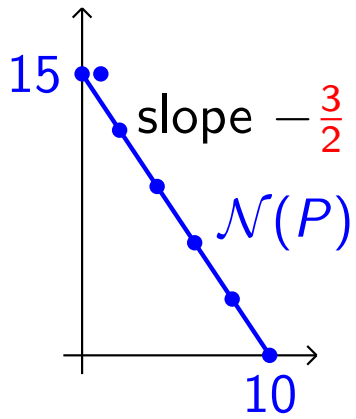
Generalised Newton polygon

associated to μ_0, ϕ_0

- (μ, ϕ) a *type*, i.e. $\phi \in \mathrm{KP}(\mu)$.

$$P = (\phi_0^2 - 27)^5 + 3^{15}\,\phi_0$$

- Taylor expansion: $g = \sum_i a_i\,\phi^i$ with $\deg(a_i) < \deg(\phi)$.
- Generalised Newton polygon: $\mathcal{N}_{\mu,\phi}(g) = \mathrm{Conv}\{(i, \mu(a_i))\}$.



- $\mu_1 = [\mu_0; \phi_0, \frac{3}{2}]$: $\mu_1(\sum_i a_i \phi_0^i) := \min_i v(a_i) + \frac{3}{2}\,i$

$$\mu_0 \text{ ——— } \mu_1(x-2) = \tfrac{3}{2} \text{ ..... } w_P$$

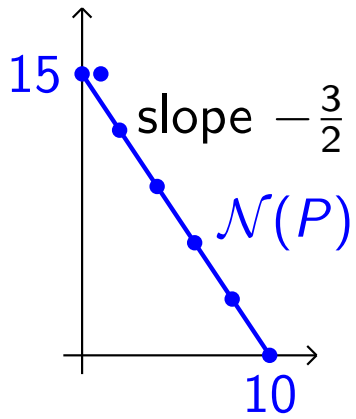
Generalised Newton polygon

associated to μ_0, ϕ_0

- (μ, ϕ) a *type*, i.e. $\phi \in \mathrm{KP}(\mu)$.

$P = (\phi_0^2 - 27)^5 + 3^{15}\,\phi_0$

- Taylor expansion: $g = \sum_i a_i\,\phi^i$ with $\deg(a_i) < \deg(\phi)$.
- Generalised Newton polygon: $\mathcal{N}_{\mu,\phi}(g) = \mathrm{Conv}\{(i, \mu(a_i))\}$.



- $\mu_1 = [\mu_0; \phi_0, \frac{3}{2}]$: $\mu_1(\sum_i a_i\phi_0^i) := \min_i v(a_i) + \frac{3}{2}\,i$
- $\mu_1' = [\mu_0; \phi_0, \lambda]$ with $\lambda \neq \frac{3}{2}$?
  - $\lambda > \frac{3}{2}$: $\mu_1' \not\sim w_P$ ✗
  - $\lambda < \frac{3}{2}$: $\mu_1' < \mu_1$ ∼

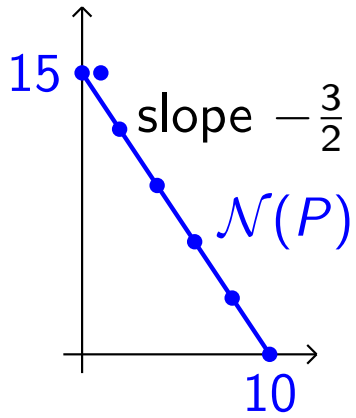
μ_0 ——— $\mu_1(x-2) = \frac{3}{2}$ ····· w_P

Generalised Newton polygon

associated to μ_0, ϕ_0

- (μ, ϕ) a *type*, i.e. $\phi \in \mathrm{KP}(\mu)$.
- Taylor expansion: $g = \sum_i a_i \phi^i$ with $\deg(a_i) < \deg(\phi)$.
- Generalised Newton polygon: $\mathcal{N}_{\mu,\phi}(g) = \mathrm{Conv}\{(i, \mu(a_i))\}$.

$P = (\phi_0^2 - 27)^5 + 3^{15}\,\phi_0$



- $\mu_1 = [\mu_0; \phi_0, \frac{3}{2}]$: $\mu_1(\sum_i a_i \phi_0^i) := \min_i v(a_i) + \frac{3}{2}\, i$
- $\mu_1' = [\mu_0; \phi_0, \lambda]$ with $\lambda \neq \frac{3}{2}$?
  - $\lambda > \frac{3}{2}$: $\mu_1' \not\sim w_P$ ✗
  - $\lambda < \frac{3}{2}$: $\mu_1' < \mu_1$ ∼

$\mu_1(\phi_0^2 - 27) = 3 < \frac{33}{10}$

μ_0 ——— $\mu_1(x-2) = \frac{3}{2}$ ····· w_P

Next residual polynomial

associated to $\mu_1 = [\mu_0; \phi_0, \frac{3}{2}]$

$$P = (\phi_0^2 - 27)^5 + 3^{15}\,\phi_0 \qquad \mu_1(P) = 15$$

$$\Gamma_{\mu_0} = \mathbb{Z}\ ;\ \Gamma_{\mu_1} = \frac{1}{2}\mathbb{Z} \rightsquigarrow e = 2$$

- $\mathrm{in}_{\mu_1}(P) = (\phi_0^2 - 27)^5 = 3^{15}\,(\xi_1 - 1)^5$ with $\xi_1 = \frac{\phi_0^2}{27}$.

$$R_{\mu_1}(P)(y) = (y-1)^5$$

Next residual polynomial

associated to $\mu_1 = [\mu_0; \phi_0, \frac{3}{2}]$

$$P = (\phi_0^2 - 27)^5 + 3^{15}\,\phi_0 \qquad \mu_1(P) = 15$$

$$\Gamma_{\mu_0} = \mathbb{Z}\ ;\ \Gamma_{\mu_1} = \frac{1}{2}\mathbb{Z} \rightsquigarrow e = 2$$

- $\mathrm{in}_{\mu_1}(P) = (\phi_0^2 - 27)^5 = 3^{15}\,(\xi_1 - 1)^5$ with $\xi_1 = \frac{\phi_0^2}{27}$.

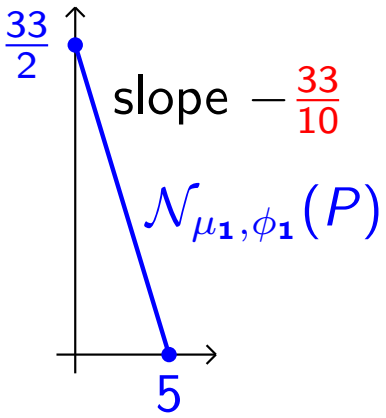
$$R_{\mu_1}(P)(y) = (y-1)^5$$

- Representative: $\phi_1 := (x-2)^2 - 27 \in \mathrm{KP}(\mu_1)$.

$$\mu_1(\phi_1) = 3 < w_P(\phi_1) = \frac{33}{10}.$$ Getting $\frac{33}{10}$?

Next Newton polygon and residual polynomial

$$P = \phi_1^5 + 3^{15}\,\phi_0$$



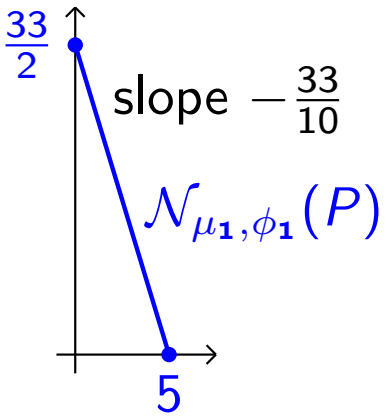
- $\mu_2 = [\mu_1; \phi_1, \frac{33}{10}]$

  $\mu_2(\sum_i a_i \phi_1^i) := \min_i \mu_1(a_i) + \frac{33}{10}\, i$

$$\mu_0 \text{ ——— } \mu_1(\phi_0) = \tfrac{3}{2} \text{ ——— } \mu_2(\phi_1) = \tfrac{33}{10} \text{ ..... } w_P$$

Next Newton polygon and residual polynomial

$$P = \phi_1^5 + 3^{15}\,\phi_0$$



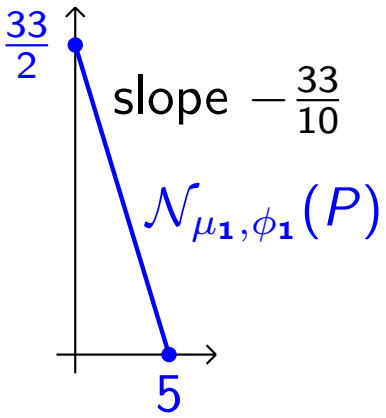
- $\mu_2 = [\mu_1; \phi_1, \frac{33}{10}]$

  $\mu_2(\sum_i a_i\phi_1^i) := \min_i \mu_1(a_i) + \frac{33}{10}\,i$
- $\mathrm{in}_{\mu_2}(P) = 3^{15}\,\phi_0\,(\xi_2 + 1)$ with $\xi_2 = \frac{\phi_1^5}{3^{15}\,\phi_0}$
- $R_{\mu_2}(P)(y) = \ y + 1$

$$\mu_0 \text{ ——— } \mu_1(\phi_0) = \tfrac{3}{2} \text{ ——— } \mu_2(\phi_1) = \tfrac{33}{10} \cdots\cdots\cdots\cdots\cdots w_P$$

Next Newton polygon and residual polynomial

$$P = \phi_1^5 + 3^{15}\,\phi_0$$



- $\mu_2 = [\mu_1; \phi_1, \frac{33}{10}]$

  $\mu_2(\sum_i a_i \phi_1^i) := \min_i \mu_1(a_i) + \frac{33}{10}\, i$
- $\mathrm{in}_{\mu_2}(P) = 3^{15}\,\phi_0\,(\xi_2 + 1)$ with $\xi_2 = \frac{\phi_1^5}{3^{15}\,\phi_0}$
- $R_{\mu_2}(P)(y) = (y+1)^1$

$$\mu_0 \text{ ——— } \mu_1(\phi_0) = \tfrac{3}{2} \text{ ——— } \mu_2(\phi_1) = \tfrac{33}{10} \text{ ——— } w_P$$

We proved: P irreducible, $w_P(x-2) = \frac{3}{2}$, $w_P((x-2)^2 - 27) = \frac{33}{10}$

Factorisation in $\mathbb{A}[x]$

- Dissection according to residual polynomials,
- Generalisation of the Hensel lemma.

Dissection according to the residual polynomial.

$F \in \mathbb{A}[x]$, μ a valuation computed from F.

Theorem

If $R_\mu(F)(y) = h_1^{N_1} \cdots h_m^{N_m}$, *then*

$$F = F_1 \cdots F_m$$

with $R_\mu(F_i) = h_i^{N_i}$.

Hensel lifting

Modern Computer Algebra, chapter 15.4

$$\underbrace{x^4 - 1}_{f} = (\underbrace{x - 2}_{g})(\underbrace{x^3 + 2x^2 - x - 2}_{h}) \mod 5$$

Hensel lifting

Modern Computer Algebra, chapter 15.4

$$\underbrace{x^4-1}_{f} = (\underbrace{x-2}_{g})(\underbrace{x^3+2x^2-x-2}_{h}) \mod 5$$

Euclide: $s\,g + t\,h = 1 \mod 5 \rightsquigarrow s = -2\ ;\ t = 2x^2 - 2x - 1.$

Hensel lifting

Modern Computer Algebra, chapter 15.4

$$\underbrace{x^4-1}_{f} = (\underbrace{x-2}_{g})(\underbrace{x^3+2x^2-x-2}_{h}) \mod 5$$

Euclide: $s\,g + t\,h = 1 \mod 5 \rightsquigarrow s = -2\ ;\ t = 2x^2 - 2x - 1.$

$$\begin{cases} e &= f - g\,h = 5x^2 - 5 \\ \hat{g} &= g + t\,e = 10x^4 - 9x^3 - 13x^2 + 9x + 3 \\ \hat{h} &= h + s\,e = -10x^2 + x + 8 \end{cases}$$

$$f - \hat{g}\,\hat{h} = 25 \cdot (4x^6 - 4x^5 - 8x^4 + 7x^3 + 5x^2 - 3x - 1) = 0 \mod 25$$

Hensel lifting

Modern Computer Algebra, chapter 15.4

$$\underbrace{x^4-1}_{f} = (\underbrace{x-2}_{g})(\underbrace{x^3+2x^2-x-2}_{h}) \mod 5$$

Euclide: $s\,g + t\,h = 1 \mod 5 \rightsquigarrow s = -2\ ;\ t = 2x^2 - 2x - 1.$

$$\begin{cases} e &= f - g\,h = 5x^2 - 5 \\ \hat{g} &= g + t\,e = 10x^4 - 9x^3 - 13x^2 + 9x + 3 \\ \hat{h} &= h + s\,e = -10x^2 + x + 8 \end{cases}$$

$$f - \hat{g}\,\hat{h} = 25 \cdot (4x^6 - 4x^5 - 8x^4 + 7x^3 + 5x^2 - 3x - 1) = 0 \mod 25$$

Non increasing degrees ? Add euclidean divisions

Lemma

If $f = q\,g + r$ *with* $\deg(r) < \deg(g)$, g *monic and* $f = 0 \mod m$, *then* $q = 0 \mod m$ *and* $r = 0 \mod m$

Hensel step

Input: $f = g\,h \mod \pi^{n+1}$ and $s\,g + t\,h = 1 \mod \pi^{n+1}$.

Algorithm `HenselStep`:

$e \leftarrow f - g\,h \mod \pi^{2n+1}$;

$q, r \leftarrow \mathtt{QuoRem}(s\,e, h)$;

$\hat{g} \leftarrow g + e\,t + q\,g \mod \pi^{2n+1}$;

$\hat{h} \leftarrow h + r \mod \pi^{2n+1}$;

Hensel step

Input: $f = g\,h \mod \pi^{n+1}$ and $s\,g + t\,h = 1 \mod \pi^{n+1}$.

Algorithm `HenselStep`:

$e \leftarrow f - g\,h \mod \pi^{2n+1}$;
$q, r \leftarrow \mathtt{QuoRem}(s\,e, h)$;
$\hat{g} \leftarrow g + e\,t + q\,g \mod \pi^{2n+1}$;
$\hat{h} \leftarrow h + r \mod \pi^{2n+1}$;
$b \leftarrow s\,\hat{g} + t\,\hat{h} - 1 \mod \pi^{2n+1}$;
$c, d \leftarrow \mathtt{QuoRem}(s\,b, \hat{h})$;
$\hat{s} \leftarrow s - d \mod \pi^{2n+1}$;
$\hat{t} \leftarrow t - b\,t - c\,\hat{g} \mod \pi^{2n+1}$;
return $\hat{h}$, $\hat{g}$, $\hat{s}$, $\hat{t}$

Output: $f = \hat{g}\,\hat{h} \mod \pi^{2\,n+1}$ and $\hat{s}\,\hat{g} + \hat{t}\,\hat{h} = 1 \mod \pi^{2\,n+1}$.

Hensel lemma works with μ

- (μ', ϕ) a type, $\lambda > \mu'(\phi)$.
- $\mu = [\mu'; \phi, \lambda]$.

Lemma

If $B = \phi^b + \cdots$ *et* $\mu(B) = b\,\mu(\phi)$, *then*

- $\mu(A\%B) \geq \mu(A)$,
- $\mu(A /\!\!/ B) \geq \mu(A) - \mu(B)$.

Hensel lemma works with μ

- (μ', ϕ) a type, $\lambda > \mu'(\phi)$.
- $\mu = [\mu'; \phi, \lambda]$.

Lemma

If $B = \phi^b + \cdots$ et $\mu(B) = b\,\mu(\phi)$, then

- $\mu(A\%B) \geq \mu(A)$,
- $\mu(A /\!/ B) \geq \mu(A) - \mu(B)$.

Notation:

$$\lceil F \rceil_\mu^n \rightsquigarrow \text{ we remove "terms" of valuation } > n$$

Example: $\lceil 4x - 8 \rceil_{\mu_1}^2 = x - 2$ since $4x - 8 = \underbrace{x - 2}_{3/2} + \underbrace{3(x-2)}_{5/2}$

Adaptation of the Hensel–Newton algorithm

Input: $\mu(F - G\,H) \geq \mu(F) + n$ and $\mu(S\,G + T\,H - 1) \geq n$.

Algorithm `HenselStep`:

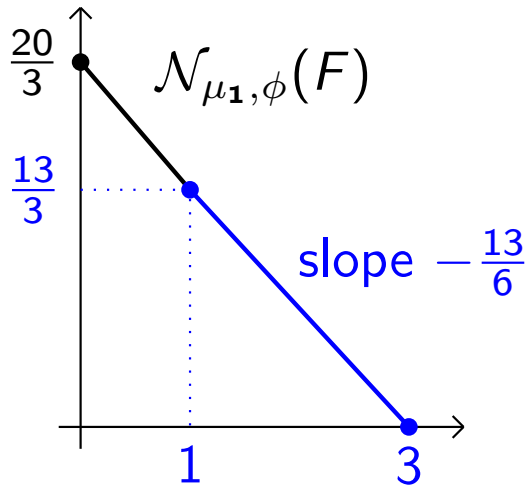
$E \leftarrow \lceil F - G\,H \rceil^{\mu(F)+2n}$;
$Q, R \leftarrow \lceil \mathtt{QuoRem}(S\,E, H) \rceil^{\mu(F)+2n}$;
$\tilde{G} \leftarrow \lceil G + E\,T + Q\,G \rceil^{\mu(G)+2n}$;
$\tilde{H} \leftarrow \lceil H + R \rceil^{\mu(H)+2n}$;
$B \leftarrow \lceil S\,\tilde{G} + T\,\tilde{H} - 1 \rceil^{2n}$;
$C, D \leftarrow \lceil \mathtt{QuoRem}(S\,B, \tilde{H}) \rceil^{2n}$;
$\tilde{S} \leftarrow \lceil S - D \rceil^{2n-\mu(G)}$;
$\tilde{T} \leftarrow \lceil T - B\,T - C\,\tilde{G} \rceil^{2n-\mu(H)}$;
return $\tilde{H}$, $\tilde{G}$, $\tilde{S}$, $\tilde{T}$

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

Initialisation: via $\mathrm{in}_\mu(F)$

$$F = \phi^3 + t^3\,x^2\,\phi + t^6\,x \in \mathbb{K}[[t]][x] \text{ with } \phi = x^3 - t^2$$

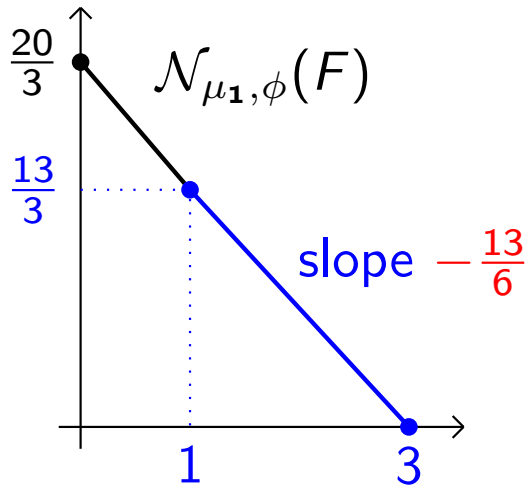
- $\mu_1 = \left[\mu_0; x, \frac{2}{3}\right]$,



Initialisation: via $\mathrm{in}_\mu(F)$

$$F = \phi^3 + t^3\,x^2\,\phi + t^6\,x \in \mathbb{K}[[t]][x] \text{ with } \phi = x^3 - t^2$$

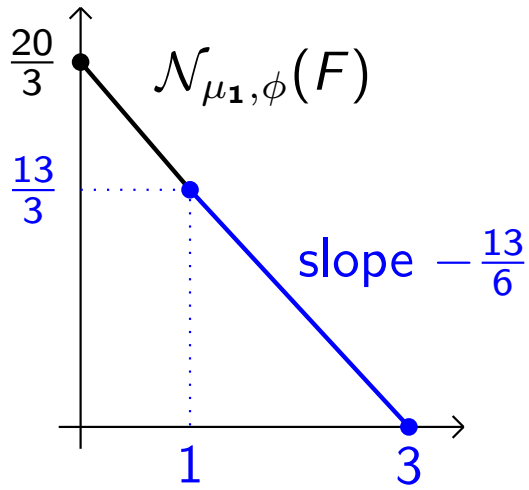
- $\mu_1 = \left[\mu_0; x, \frac{2}{3}\right]$,
- $\mu_2 := \left[\mu_1; \phi, \frac{13}{6}\right]$,



Initialisation: via $\mathrm{in}_\mu(F)$

$$F = \phi^3 + t^3\,x^2\,\phi + t^6\,x \in \mathbb{K}[[t]][x] \text{ with } \phi = x^3 - t^2$$

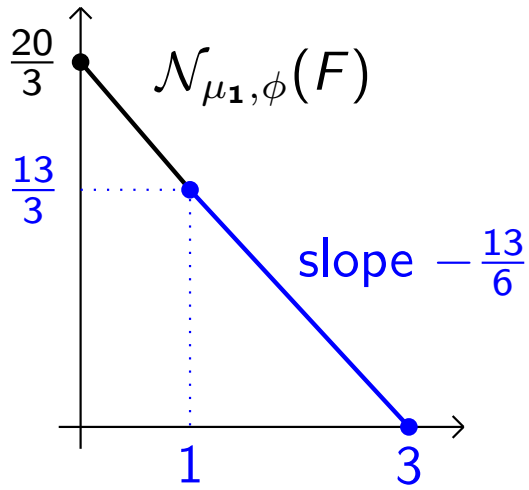
- $\mu_1 = \left[\mu_0; x, \frac{2}{3}\right]$,
- $\mu_2 := \left[\mu_1; \phi, \frac{13}{6}\right]$,
- $\mathrm{in}_{\mu_2}(F) = \phi^3 + t^3\,x^2\,\phi$,
- $\tilde{R}_{\mu_2}(F) = y\,(y^2+1)$.



- $H_0 = \phi,\ G_0 = \phi^2 + t^3\,x^2 \implies \overbrace{F}^{13/2} - H_0\,G_0 = \overbrace{t^6\,x}^{20/3}$

Initialisation: via $\mathrm{in}_\mu(F)$

$$F = \phi^3 + t^3\,x^2\,\phi + t^6\,x \in \mathbb{K}[[t]][x] \text{ with } \phi = x^3 - t^2$$



- $\mu_1 = \left[\mu_0; x, \frac{2}{3}\right]$,
- $\mu_2 := \left[\mu_1; \phi, \frac{13}{6}\right]$,
- $\mathrm{in}_{\mu_2}(F) = \phi^3 + t^3\,x^2\,\phi$,
- $\tilde{R}_{\mu_2}(F) = y\,(y^2+1)$.

- $H_0 = \phi,\ G_0 = \phi^2 + t^3\,x^2 \implies \overbrace{F}^{13/2} - H_0\,G_0 = \overbrace{t^6\,x}^{20/3}$

$\frac{20}{3} - \frac{13}{2} = \frac{1}{6}$

- If $s_0 = 1$ and $t_0 = -y$, then $s_0\,(y^2+1) + t_0\,y = 1$,
- $S_0 = \underbrace{t^{-5}x}_{-13/3},\ T_0 = \underbrace{-t^{-5}x\,\phi}_{-13/6} \implies S_0\,G_0 + T_0\,H_0 - 1 = \underbrace{t^{-2}\phi}_{1/6}$

Approximate roots of $F \in \mathbb{A}[x]$ monic

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

Proposition

There is a unique $\phi \in \mathbb{A}[x]$ monic such that:

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

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

$$F = \phi^N + a_{N-2}\,\phi^{N-2} + \cdots + a_0$$

They are "optimal" key polynomials

- Hyp: $\mathrm{char}(\mathbb{F})$ does not divide $d = \deg(F)$

Proposition

If $R_\mu = h^N$, then $\phi = \sqrt[N]{F} \in KP(\mu)$

$$F = \phi^N + a_{N-2}\,\phi^{N-2} + \cdots + a_0$$

Proposition

If $\mathcal{N}_{\mu,\phi}(F)$ has a unique slope λ, then $R_{[\mu;\phi,\lambda]}(F)(y) \neq (y+c)^N$.

- either we get a partial factorisation,
- either we consider $\sqrt[N']{F}$ with N' a proper divisor of N.

$\Longrightarrow$ logarithmic number of steps before we get a partial factorisation.

ϕ-adic expansion

- $F, \phi \in \mathbb{A}[x]$ with ϕ monic. $c = \deg(\phi)$, $d = \deg(F)$
- $k \neq 0$ a power of 2 such that $\frac{k}{2}\, c \leq d < k\, c$.

$$F = \sum_{i=0}^{k-1} a_i\, \phi^i \quad , \quad \deg(a_i) < c$$

1. If $k = 1$, return $a_0 = f$.
2. Compute $\phi^{\frac{k}{2}}$ by repeated squaring,
3. $q, r \leftarrow$ $\mathtt{QuoRem}(a, \phi^{\frac{k}{2}})$,
4. Recursive calls for q and r

ϕ-adic expansion

- $F, \phi \in \mathbb{A}[x]$ with ϕ monic. $c = \deg(\phi)$, $d = \deg(F)$
- $k \neq 0$ a power of 2 such that $\frac{k}{2}\, c \leq d < k\, c$.

$$F = \sum_{i=0}^{k-1} a_i\, \phi^i \quad , \quad \deg(a_i) < c$$

1. If $k = 1$, return $a_0 = f$. $\mathsf{C}(1) = 0$
2. Compute $\phi^{\frac{k}{2}}$ by repeated squaring,
3. $q, r \leftarrow \mathtt{QuoRem}(a, \phi^{\frac{k}{2}})$,
4. Recursive calls for q and r

$\mathsf{C}(k) =$

ϕ-adic expansion

- $F, \phi \in \mathbb{A}[x]$ with ϕ monic. $c = \deg(\phi)$, $d = \deg(F)$
- $k \neq 0$ a power of 2 such that $\frac{k}{2}\, c \leq d < k\, c$.

$$F = \sum_{i=0}^{k-1} a_i\, \phi^i \quad , \quad \deg(a_i) < c$$

1. If $k = 1$, return $a_0 = f$. $\mathsf{C}(1) = 0$
2. Compute $\phi^{\frac{k}{2}}$ by repeated squaring, $\mathsf{M}(k\, c)$
3. $q, r \leftarrow$ $\mathtt{QuoRem}(a, \phi^{\frac{k}{2}})$,
4. Recursive calls for q and r

$\mathsf{C}(k) =$

ϕ-adic expansion

- $F, \phi \in \mathbb{A}[x]$ with ϕ monic. $c = \deg(\phi)$, $d = \deg(F)$
- $k \neq 0$ a power of 2 such that $\frac{k}{2}\, c \leq d < k\, c$.

$$F = \sum_{i=0}^{k-1} a_i\, \phi^i \quad , \quad \deg(a_i) < c$$

1. If $k = 1$, return $a_0 = f$. $\mathsf{C}(1) = 0$
2. Compute $\phi^{\frac{k}{2}}$ by repeated squaring, $\mathsf{M}(k\, c)$
3. $q, r \leftarrow \texttt{QuoRem}(a, \phi^{\frac{k}{2}})$, $\mathsf{M}(k\, c)$
4. Recursive calls for q and r

$\mathsf{C}(k) =$

ϕ-adic expansion

- $F, \phi \in \mathbb{A}[x]$ with ϕ monic. $c = \deg(\phi)$, $d = \deg(F)$
- $k \neq 0$ a power of 2 such that $\frac{k}{2}\, c \leq d < k\, c$.

$$F = \sum_{i=0}^{k-1} a_i\, \phi^i \quad , \quad \deg(a_i) < c$$

1. If $k = 1$, return $a_0 = f$. $\mathsf{C}(1) = 0$
2. Compute $\phi^{\frac{k}{2}}$ by repeated squaring, $\mathsf{M}(k\, c)$
3. $q, r \leftarrow \mathtt{QuoRem}(a, \phi^{\frac{k}{2}})$, $\mathsf{M}(k\, c)$
4. Recursive calls for q and r $2\, \mathsf{C}(k/2)$

$\mathsf{C}(k) =$

ϕ-adic expansion

- $F, \phi \in \mathbb{A}[x]$ with ϕ monic. $c = \deg(\phi)$, $d = \deg(F)$
- $k \neq 0$ a power of 2 such that $\frac{k}{2}\, c \leq d < k\, c$.

$$F = \sum_{i=0}^{k-1} a_i\, \phi^i \quad , \quad \deg(a_i) < c$$

1. If $k = 1$, return $a_0 = f$. $\mathsf{C}(1) = 0$
2. Compute $\phi^{\frac{k}{2}}$ by repeated squaring, $\mathsf{M}(k\, c)$
3. $q, r \leftarrow \mathtt{QuoRem}(a, \phi^{\frac{k}{2}})$, $\mathsf{M}(k\, c)$
4. Recursive calls for q and r $2\, \mathsf{C}(k/2)$

$$\mathsf{C}(k) = 2\, \mathsf{C}(k/2) + \mathcal{O}(\mathsf{M}(k\, c))$$

ϕ-adic expansion

- $F, \phi \in \mathbb{A}[x]$ with ϕ monic. $c = \deg(\phi)$, $d = \deg(F)$
- $k \neq 0$ a power of 2 such that $\frac{k}{2}\, c \leq d < k\, c$.

$$F = \sum_{i=0}^{k-1} a_i\, \phi^i \quad , \quad \deg(a_i) < c$$

1. If $k = 1$, return $a_0 = f$. $\mathsf{C}(1) = 0$
2. Compute $\phi^{\frac{k}{2}}$ by repeated squaring, $\mathsf{M}(k\, c)$
3. $q, r \leftarrow \mathtt{QuoRem}(a, \phi^{\frac{k}{2}})$, $\mathsf{M}(k\, c)$
4. Recursive calls for q and r $2\, \mathsf{C}(k/2)$

$$\mathsf{C}(k) = 2\, \mathsf{C}(k/2) + \mathcal{O}(\mathsf{M}(k\, c)) \rightsquigarrow \mathsf{C}(k) = \mathcal{O}(\mathsf{M}(k\, c)\, \log(k)) \subset \mathcal{O}^{\sim}(d)$$

Computing a valuation

- $\nu = [\mu; \phi, \gamma]$ is defined as:

$$\nu(g) = \min\{\mu(a_i) + i\,\gamma \mid 0 \leq i\},$$

(we start from the *Gauss valuation* $\mu_0(\sum_i a_i\, x^i) = \min_i v(a_i)$)

- Computation of $\nu(g)$:

1. compute the ϕ-adic expansion of g
2. compute recursively the $\mu(a_i)$

Computing a valuation

- $\nu = [\mu; \phi, \gamma]$ is defined as:

$$\nu(g) = \min\{\mu(a_i) + i\,\gamma \mid 0 \leq i\},$$

(we start from the *Gauss valuation* $\mu_0(\sum_i a_i\, x^i) = \min_i v(a_i)$)

- Computation of $\nu(g)$:

1. compute the ϕ-adic expansion of g $\quad \mathcal{O}(\mathsf{M}(d)\log(d))$
2. compute recursively the $\mu(a_i)$ $\quad \mathsf{C}(\deg(a_i))$

- Total : $\sum_i \deg(a_i) \leq \deg(g)$

$$\rightsquigarrow \mathsf{C}(d) = \mathcal{O}(\mathsf{M}(d)\,\log^2(d)) \subset \mathcal{O}^{\sim}(d) \text{ op. in } \mathbb{A}.$$

NB: assuming we have less than $\log_2(d)$ "successive" valuations

Generalised Newton polygon computation

The computation of $\mathcal{N}_{\mu,\phi}(F)$ is done as follows:

1. compute $F = \sum_i a_i \phi^i$,
2. compute the $\mu(a_i)$.

Generalised Newton polygon computation

The computation of $\mathcal{N}_{\mu,\phi}(F)$ is done as follows:

1. compute $F = \sum_i a_i \phi^i$, $\mathcal{O}(\mathrm{M}(d)\log(d))$
2. compute the $\mu(a_i)$. $\mathrm{M}(\deg(a_i)\log(\deg(a_i))^2)$

Total: $\mathcal{O}(\mathrm{M}(d)\log(d)^2) \subset \mathcal{O}^{\sim}(d)$ operations in $\mathbb{A}$

Remark: convex hull in $\mathcal{O}(d\ \log(d))$ op. in $\mathbb{Z}$ (*no op in* $\mathbb{A}$)

Residual polynomial computation

- $\mu = [\nu; \phi, \gamma]$; $\mathbb{F}_\mu = \mathbb{F}[z]$; $f = [\mathbb{F}_\mu : \mathbb{F}]$; $I = \{i_0, i_0 + e, ..., i_0 + n\,e\}$

$$R_\mu(G) = \sum_{i \in I} z^{\tau_i} R_\nu(a_i)(z)\, y^{\frac{i-i_0}{e}}$$

1. get the a_i, "monomials" with valuation $\mu(G)$,
2. recursive call for all $R_\nu(a_i)(y)$,
3. Compute the $z^{\tau_i}\, R_\nu(a_i)(z)$.

Residual polynomial computation

- $\mu = [\nu; \phi, \gamma]$; $\mathbb{F}_\mu = \mathbb{F}[z]$; $f = [\mathbb{F}_\mu : \mathbb{F}]$; $I = \{i_0, i_0 + e, ..., i_0 + n\,e\}$

$$R_\mu(G) = \sum_{i \in I} z^{\tau_i} R_\nu(a_i)(z)\, y^{\frac{i-i_0}{e}}$$

1. get the a_i, "monomials" with valuation $\mu(G)$,
2. recursive call for all $R_\nu(a_i)(y)$,
3. Compute the $z^{\tau_i}\, R_\nu(a_i)(z)$.

- a_i, τ_i: given while computing $\mathcal{N}_{\nu,\phi}(G)$,
- $\tau_i \in \mathcal{O}(\delta) \rightsquigarrow \log(\delta)$ op. in $\mathbb{F}_\mu$ $\quad \tilde{\mathcal{O}}(f\ \log(\delta))$
- Remaining: $n\,\mathrm{C}(f) + f + 1$ mult. in $\mathbb{F}_\mu$ $\quad n\,\mathrm{C}(f) + \tilde{\mathcal{O}}(f^2)$

Residual polynomial computation

- $\mu = [\nu; \phi, \gamma]$; $\mathbb{F}_\mu = \mathbb{F}[z]$; $f = [\mathbb{F}_\mu : \mathbb{F}]$; $I = \{i_0, i_0 + e, ..., i_0 + n\,e\}$

$$R_\mu(G) = \sum_{i \in I} z^{\tau_i} R_\nu(a_i)(z)\, y^{\frac{i-i_0}{e}}$$

1. get the a_i, "monomials" with valuation $\mu(G)$,
2. recursive call for all $R_\nu(a_i)(y)$,
3. Compute the $z^{\tau_i}\, R_\nu(a_i)(z)$.

- a_i, τ_i: given while computing $\mathcal{N}_{\nu,\phi}(G)$,
- $\tau_i \in \mathcal{O}(\delta) \rightsquigarrow \log(\delta)$ op. in $\mathbb{F}_\mu$ $\qquad \tilde{\mathcal{O}}(f\ \log(\delta))$
- Remaining: $n\,\mathsf{C}(f) + f + 1$ mult. in $\mathbb{F}_\mu$ $\qquad n\,\mathsf{C}(f) + \tilde{\mathcal{O}}(f^2)$

$n\,f \leq 2\,d \rightsquigarrow \mathsf{C}(d) \leq n\,\mathsf{C}(f) + \tilde{\mathcal{O}}(d\,f)$: $\mathsf{C}(d) \in \tilde{\mathcal{O}}(d\,f)$ op. in $\mathbb{F}$

Computing representatives.

- $\mu = [\nu; \phi, \gamma]$; residue field $\mathbb{F}_\mu$; e relative ramification index
- $g = \sum_{i=0}^{n} g_i\, y^i \in \mathbb{F}_\mu[y]$,
- N "targeted" valuation. $\qquad G \in \mathrm{KP}(\mu) : N = \mu(G)$
- $G \in K[x]$ s. t. $\mu(G) = N$ and $R_\mu(G) = g$?

Computing representatives.

- $\mu = [\nu; \phi, \gamma]$; residue field $\mathbb{F}_\mu$; e relative ramification index
- $g = \sum_{i=0}^{n} g_i\, y^i \in \mathbb{F}_\mu[y]$,
- N "targeted" valuation. $\qquad G \in \mathrm{KP}(\mu) : N = \mu(G)$
- $G \in K[x]$ s. t. $\mu(G) = N$ and $R_\mu(G) = g$?

1. Use $N' = N - \lfloor N \rfloor + n\,\gamma$ $\qquad H \in \mathbb{A}[x]$

$$H = \phi^s \sum_{i=0}^{n} H_i(x)\, \phi^{i\,e} \text{ with } R_\nu(H_i) = g_i, \nu(H_i) = N' - i\,\gamma$$

2. Return $G = \pi^{\lfloor N \rfloor - n\,\mu(\phi)}\, H$

Computing representatives.

- $\mu = [\nu; \phi, \gamma]$; residue field $\mathbb{F}_\mu$; e relative ramification index
- $g = \sum_{i=0}^{n} g_i\, y^i \in \mathbb{F}_\mu[y]$,
- N "targeted" valuation. $\qquad G \in \mathrm{KP}(\mu) : N = \mu(G)$
- $G \in K[x]$ s. t. $\mu(G) = N$ and $R_\mu(G) = g$?

1. Use $N' = N - \lfloor N \rfloor + n\,\gamma$ $\qquad H \in \mathbb{A}[x]$

$$H = \phi^s \sum_{i=0}^{n} H_i(x)\, \phi^{i\,e} \text{ with } R_\nu(H_i) = g_i, \nu(H_i) = N' - i\,\gamma$$

2. Return $G = \pi^{\lfloor N \rfloor - n\,\mu(\phi)}\, H$

$\mathrm{C}(d) = n\,\mathrm{C}(\deg(\phi)) + \mathscr{O}(d) \rightsquigarrow \mathrm{C}(d) = \mathscr{O}(d)$ op. in $\mathbb{A}$.

Precision $n\,\mu(\phi)$ (to compute H) $\rightsquigarrow \mathscr{O}(d\,n\,\mu(\phi))$ op. in $\mathbb{F}$.

Computing $\phi = \sqrt[N]{F}$

$\mathcal{O}^{\sim}(d^2)$ op. in $\mathbb{A}$ via the Tschirnhausen transform

$\mathcal{O}(\mathsf{M}(d)) = \mathcal{O}^{\sim}(d)$ op. in $\mathbb{A}$ via Newton iteration.

- $F_\infty = x^d\, F(1/x)$ the reciprocal polynomial of F,
- $F_\infty(0) = 1 \rightsquigarrow \exists!\ \psi \in \mathbb{A}[[x]]$ s.t. $\psi(0) = 1$ and $\psi^N = F_\infty$,
- ψ is the root of $z^N - F_\infty = 0 \rightsquigarrow$ Newton iteration !
- ϕ is the reciprocal polynomial of $\lceil \psi \rceil^{\frac{d}{N}}$

Finding μ that factorise F or prove irreductibility

- Write $R_{\mu_0}(F) = h^N$ - or return (False, μ_0) $\quad \mathcal{O}(d\,f)$
- $\mu \leftarrow \mu_0$
- While $N > 1$
  - $\phi \leftarrow \sqrt[N]{F}$ $\quad \mathcal{O}(d)$
  - $\mathcal{N}_{\mu,\phi}(F)$ has a unique slope λ and $R_{[\mu;\phi,\lambda]}(F) = h^N$

    - or return (False, μ) $\quad \mathcal{O}(d)$
  - $\mu \leftarrow [\mu; \phi, \lambda]$
- Return (True, μ).

$\Longrightarrow$ at most $\log_2(\deg(F))$ iterations

precision $\frac{\delta}{d}$; $d\,f \leq 2\,\delta\,\ell_0 \rightsquigarrow \mathcal{O}(\delta\ell_0)$

A (first) factorisation algorithm.

1. Get (μ, ϕ) that factorises F (or F irreducible) $\quad \mathcal{O}(\delta\, \ell_0)$
2. Factorise $\tilde{R}_{[\mu;\phi,\lambda]}(F) = h_0 h_1 \cdots h_r$ in $\mathbb{F}_k[y]$.
3. Multi-factor Hensel: $F = F_0 F_1 \cdots F_r$. $\quad \mathcal{O}(d\, n)$
4. Back to step 1 for each F_i.

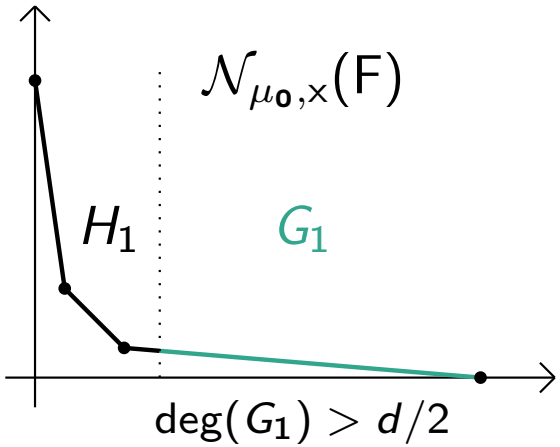
$\Longrightarrow$ at most $\deg(F)$ iterations at maximal precision

Precision $\delta \rightsquigarrow \mathcal{O}(d^2\, \delta)$ + univariate factorisations

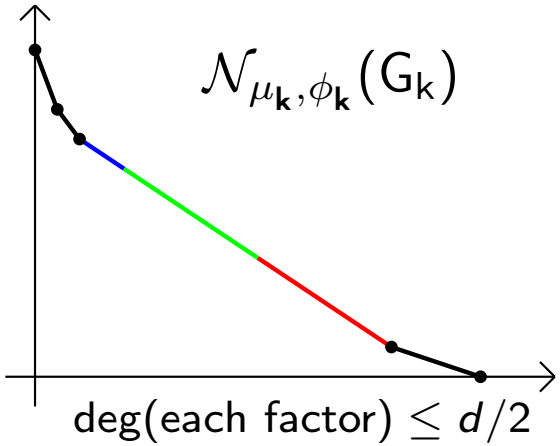
A divide and conquer algorithm

$\mathcal{O}(d\,\delta)$

Step 1: "small" precision.



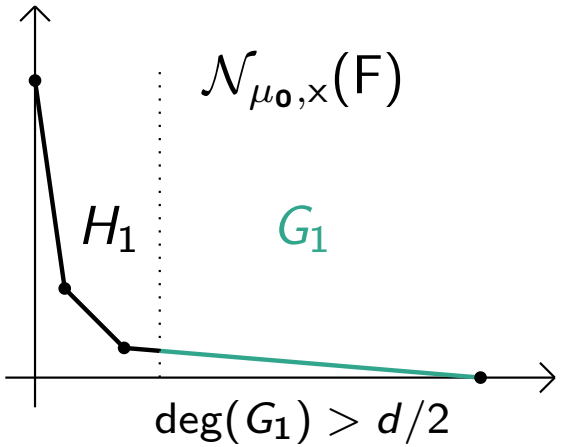
$(\cdots)$



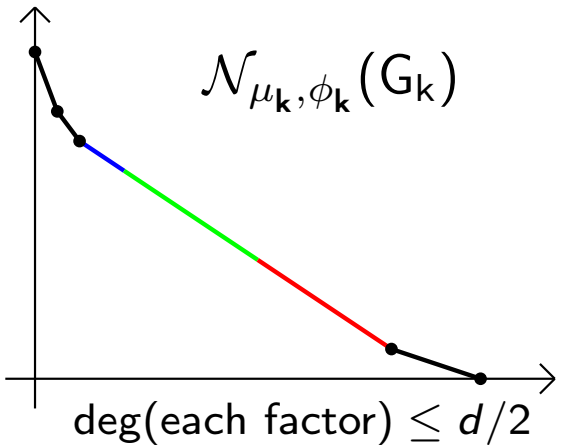
A divide and conquer algorithm

$\mathcal{O}(d\,\delta)$

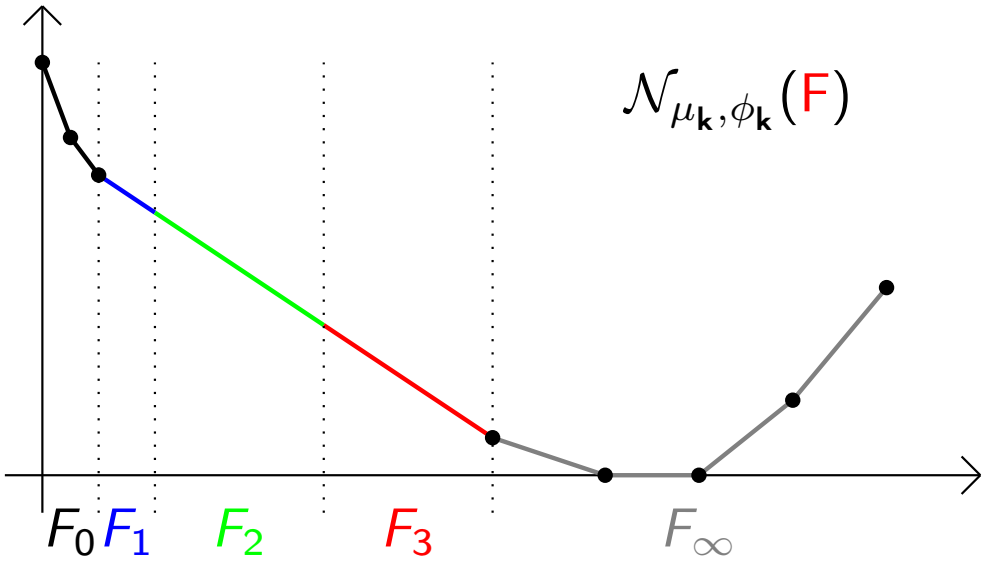
Step 1: "small" precision.



$(\cdots)$



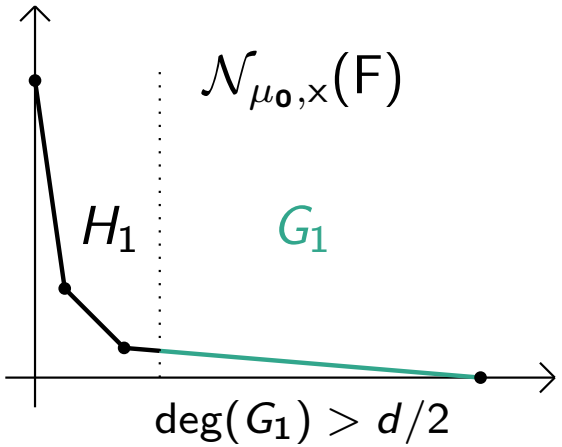
Step 2: required precision.



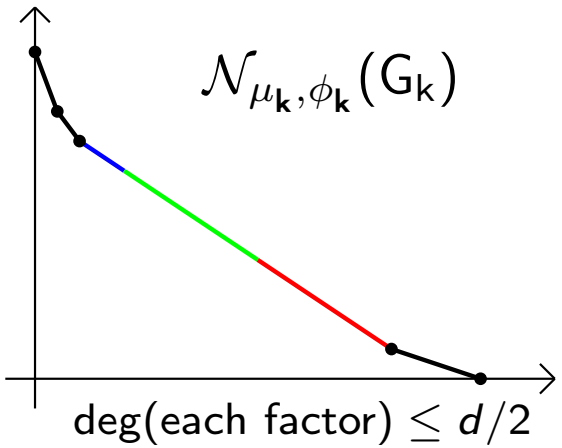
A divide and conquer algorithm

$\mathcal{O}(d\,\delta)$

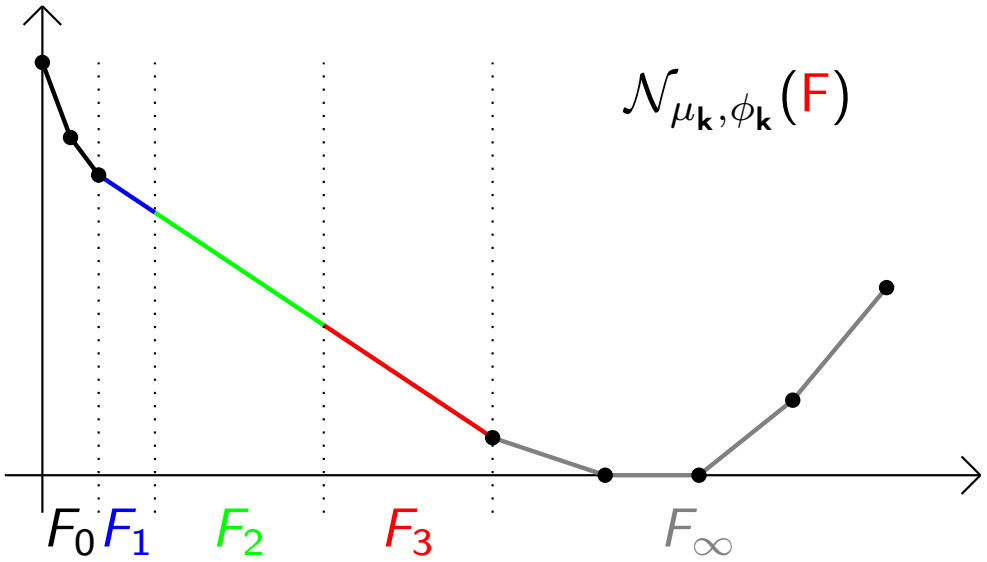
Step 1: "small" precision.



$(\cdots)$



Step 2: required precision.



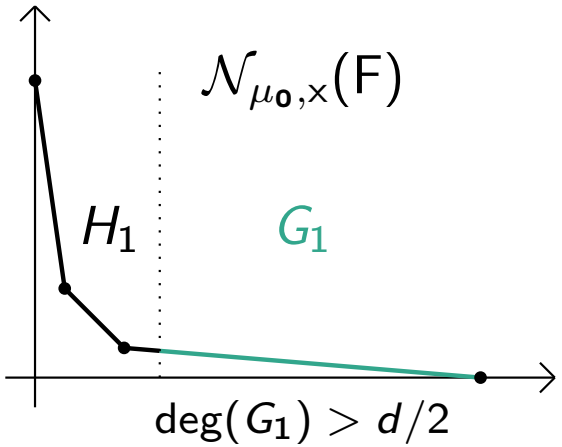
Step 3: recursive call for each F_i.

$\deg(F_i) \leq d/2$ *for all* i.

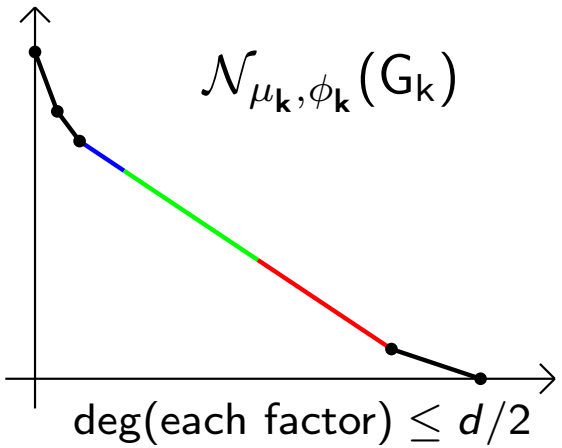
A divide and conquer algorithm

$\mathcal{O}(d\,\delta)$

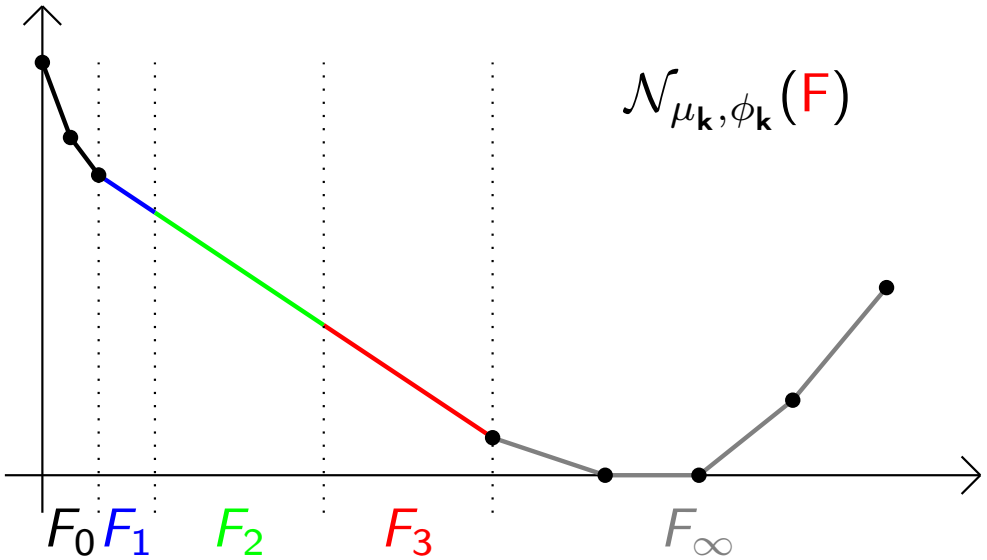
Step 1: "small" precision.



$(\cdots)$



Step 2: required precision.



Step 3: recursive call for each F_i.

$$\deg(F_i) \leq d/2 \text{ for all } i.$$

Other divide and conquer approach : van der Hoeven & Lecerf.

Thank you !