New ideas for computing integral bases

J. Guàrdia
(joint work with J. Montes & E. Nart)

Introduction

Statement of the problem

Given $K = \mathbb{Q}(\vartheta)$, $F(x) = \mathrm{Irr}(\vartheta, K, \mathbb{Q})$, $n = \deg F$

determine $\omega_1, \ldots, \omega_n$

such that $\mathbb{Z}_K = \mathbb{Z} < \omega_1, \ldots, \omega_n >$.

Example: $K = \mathbb{Q}(i)$, $\mathbb{Z}_K = \mathbb{Z}<1, i>$

Main problems of computational algebraic number theory

4.9.3 Conclusion: the Main Computational Tasks of Algebraic Number Theory

From the preceding definitions and results, it can be seen that the main computational problems for a number field $K = \mathbb{Q}(\theta)$ are the following:

(1) Compute an integral basis of $\mathbb{Z}_K$, determine the decomposition of prime numbers in $\mathbb{Z}_K$ and $\mathfrak{p}$-adic valuations for given ideals or elements.

(3) Compute a system of fundamental units of K and/or the regulator $R(K)$. Note that these two problems are not completely equivalent, since for many applications, only the approximate value of the real number $R(K)$ is desired. In most cases, by the Brauer-Siegel theorem, the fundamental units are too large even to write down, at least in a naïve manner (see Section 5.8.3 for a representation which avoids this problem).

(4) Compute the class number and the structure of the class group $Cl(K)$. It is essentially impossible to do this without also computing the regulator.

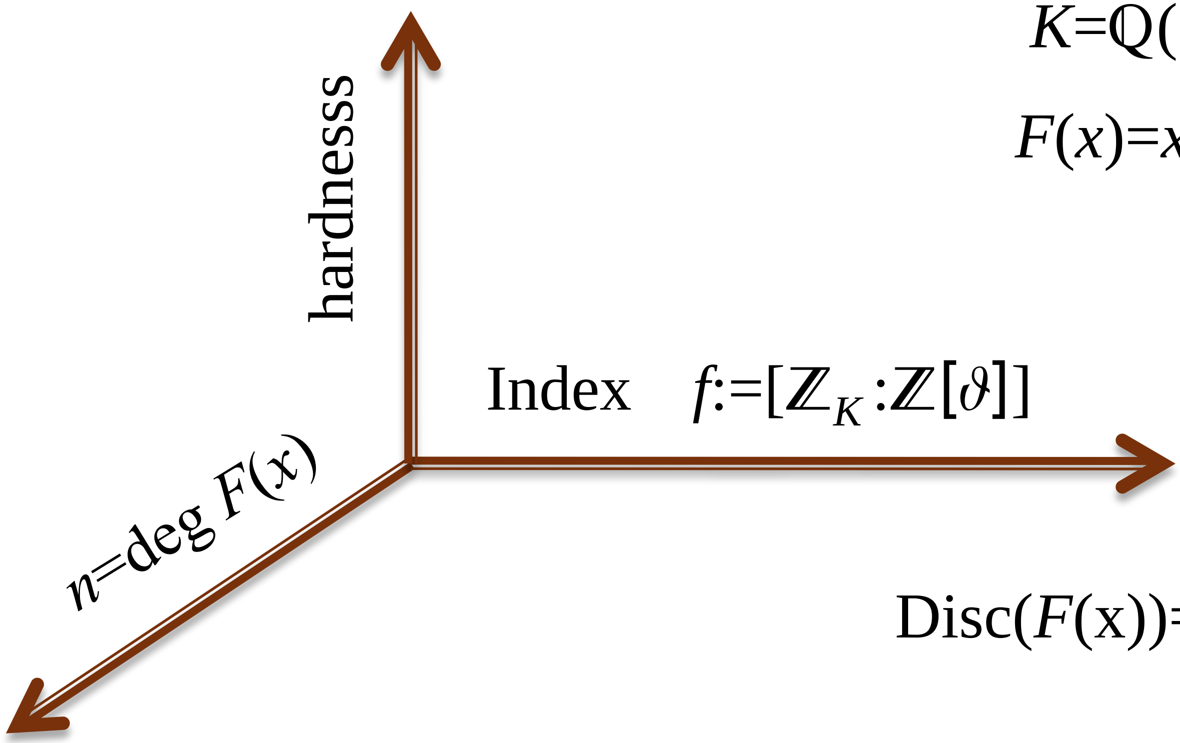
(5) Given an ideal of $\mathbb{Z}_K$, determine whether or not it is principal, and if it is, compute $\alpha \in K$ such that $I = \alpha\mathbb{Z}_K$.

H. Cohen
A course in Computational Algebraic Number Theory, GTM 138

It is not that easy!

$K=\mathbb{Q}(i)$

$F(x)=x^2+2^{10000}3^{10000}$



$\mathrm{Disc}(F(\mathrm{x}))=\mathrm{Disc}(K)\cdot f^2$

$F(x)=x^{10000}+\ldots\ 2^{9941}-1$

We must factor Disc(F(x))

Assume we can do it!

Think Globally Act Locally!

- For every $p \mid \mathrm{Disc}(F(x))$:
  Compute a triangular p-integral basis of K,
  i.e. a $\mathbb{Z}_{(p)}$ -basis of $\mathbb{Z}_K \otimes \mathbb{Z}_{(p)}$

- Glue all the local bases
  (with Chinese remainder theorem).

Ancient history

- Kummer–Dedekind $\longrightarrow$ Factor $\bmod p$
- Bauer–Ore $\longrightarrow$ Newton polygons
- Zassenhaus' Round 2 $\longrightarrow$ Enlarge p –radicals
- Zassenhaus' Round 4 $\longrightarrow$ p–adic Hensel lifting

(MAGMA, MAPLE, KANT)

Modern history

- Montes–Nart (99) $\longrightarrow$ Higher Newton polygons for prime ideal decomposition
- Ford–Pauli–Roblot (02) $\longrightarrow$ Improved Round 4

  (PARI, SAGE)
- GMN (09) $\longrightarrow$ Extended use of higher Newton polygons

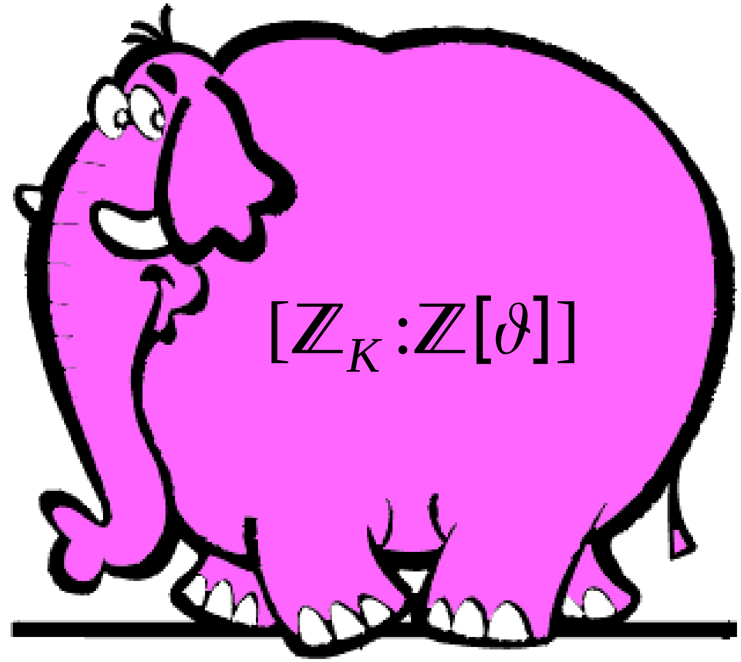
Some commercials

Graphical description

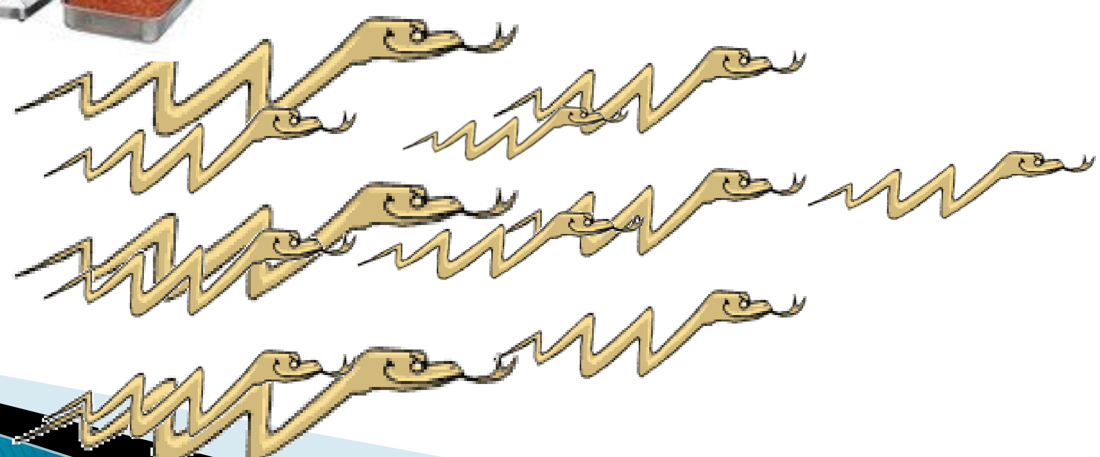
Round 2

Round 4

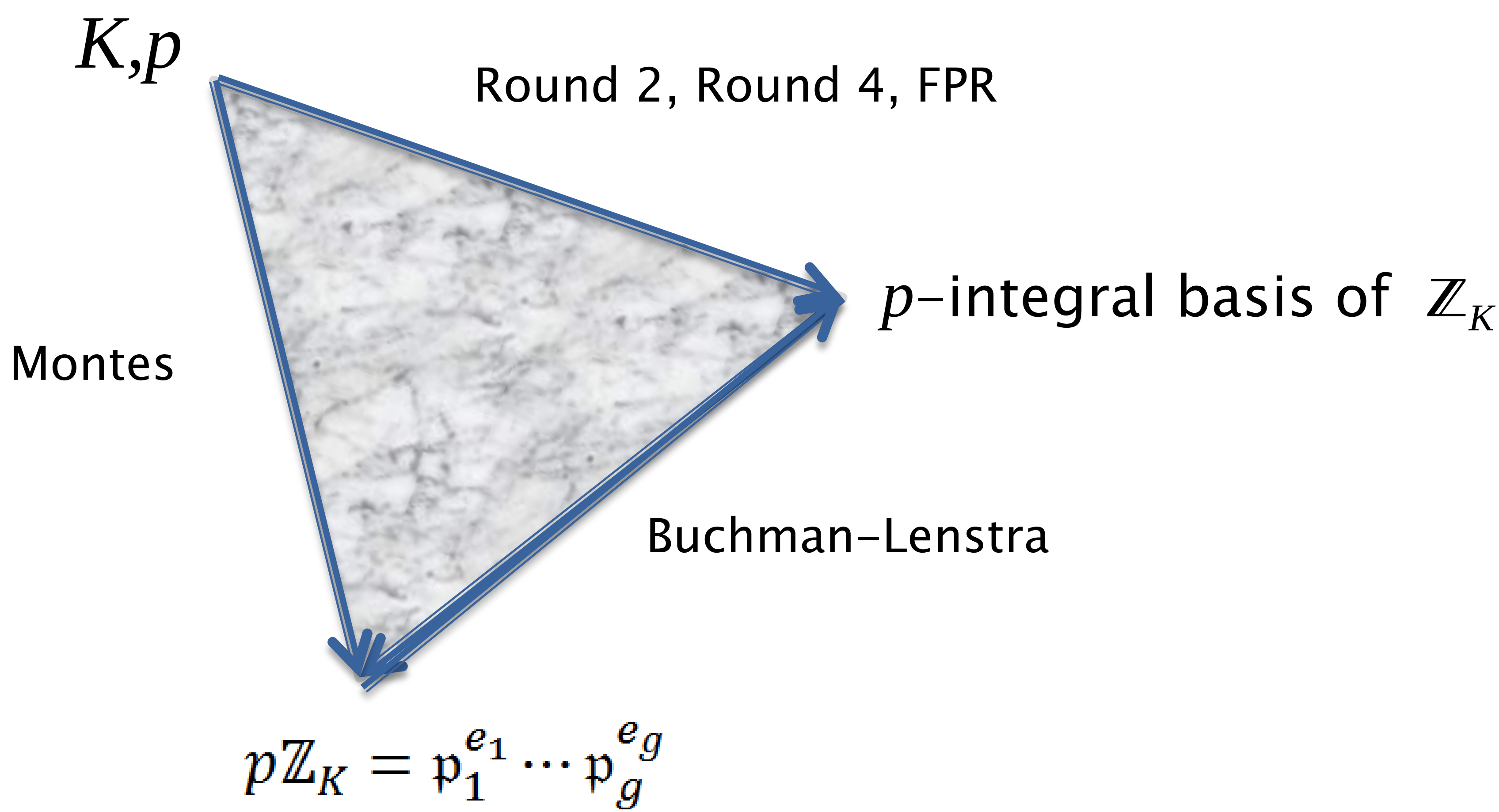
FPR



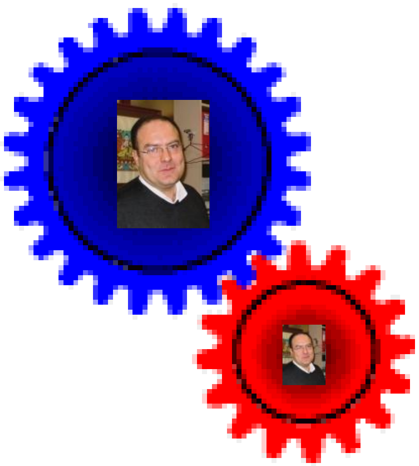
Montes



Change your mind!



Main properties of Montes *algorithm*



- Based on higher Newton polygons
- No Hensel lifting nor p-adic factorization required
- Main task: factorization of polynomials over finite fields
- Computes maximal order, index and prime ideal factorization
- Low memory-requirements
- Excellent (heuristic) running time
- The computation of maximal orders relies on a conjecture that it is proven only in some cases, but:
  - It checks the validity of the result by itself (with no extra cost)
  - We have made thousands of tests, with no fail.

The Montes package

- www.ma4.upc.edu/~guardia/MontesAlgorithm.html
  (Google: "Montes Algorithm")

- Implemented in Magma

- Includes routines to
  - Compute p–maximal orders
  - Compute p–index
  - Factor $p\mathbb{Z}_K$ *formally (*ramification indices and residuals degrees)
  - Factor $p\mathbb{Z}_K$ *completely* (generators of the prime ideals)
  - Compute global maximal orders
  - Build examples of polynomials of arbitrary *order*

- Use it for your big polynomials and/or send them to us.

Some examples

```
Magma V2.11-10
Type ? for help.
>  Attach("montes.
>
>  Z:=Integers();
>  ZX<x>:=Polynomi
>
>  pol:=x^32+16;
>
>  Factorization(I
[ <2, 284> ]
>
>
>   time OK:=Maxin
Time: 3.180
>
>
>   time basis,ind
Time: 0.010
>
>
> time basis,index
Time: 106.140
>
>
> index;
[
    [ 2, 79925 ],
    [ 5, 0 ],
    [ 257, 0 ]
]
```

```
(09:54) gp > allocatemem()
  *** allocatemem: Warning: doubling stack size; new stack = 32768000000 (31250.
000 Mbytes).
  *** allocatemem: Warning: not enough memory, new stack 16384000000.
(09:54) gp > #
   timer = 1 (on)
(09:54) gp > f=x^800+2^50*x^600+2^100*x^400+2^200;
time = 0 ms.
(09:54) gp >
(09:54) gp > d=poldisc(f);
time = 3,292 ms.
(09:54) gp >
(09:54) gp > v=valuation(d,2);
time = 0 ms.
(09:54) gp >
(09:54) gp > v3=valuation(d,257);
time = 4 ms.
(09:54) gp >
(09:54) gp > v5=valuation(d,5);
time = 0 ms.
(09:54) gp >
(09:54) gp >  ZK=nfbasis(f,,[2,v; 257,v3; 5,v5]);

time = 2h, 10mn, 17,388 ms.
(12:05) gp >
```

Some bigger examples

$$
\begin{aligned}
\phi_1 &= x^2 + 4x + 16;\\
\phi_2 &= \phi_1^2 + 16x\phi_1 + 1024;\\
\phi_3 &= \phi_2^2 + 2^{11}u\phi_2 + 2^{18}x\phi_1;\\
\phi_4 &= \phi_3^2 + 2^{25}x\phi_3 + 2^{35}\phi_1\phi_2;\\
\phi_5 &= \phi_4^3 + 2^{29}\phi_3\phi_4^2 + 2^{139}\phi_3 + 2^{153}\phi_2;\\
\phi_6 &= \phi_5^2 + 2^{141}\phi_3\phi_5 + 2^{279}\phi_4;\\
\phi_7 &= \phi_6^3 + 2^{998}\phi_1 + 2^{1003};\\
\phi_8 &= \phi_7^2 + 2^{1505}(\phi_5 + 2^{167})\phi_6;\\
\phi_9 &= \phi_8^2 + (((2^{683}(xv\phi_2 + 2^{13}w)\phi_3 + 2^{710}(w\phi_2 + 2^{11}xv))\phi_4^2 +\\
&\quad 2^{743}(x(\phi_2 + 2^7v)\phi_3 + 2^{25}(u\phi_2 + 2^7(u\phi_1 + 64)))\phi_4 +
\end{aligned}
$$

ϕ_j	deg ϕ_j	ind(ϕ_j)	2-basis	2-stem	PARI 2.3.4	MAGMA 2.11	SAGE 3.2.3
ϕ_2	4	12	0.00	0.01	0.00	0.01	0.01
ϕ_3	8	72	0.00	0.01	0.004	0.02	0.01
ϕ_4	16	352	0.00	0.02	0.016	4.67	0.05
ϕ_5	48	3696	0.03	0.6	2.4	42747	4.06
ϕ_6	96	15408	0.08	0.38	101	$> 72h$	196
ϕ_7	288	142416	0.97	16	47157	$> 72h$	119047
ϕ_8	576	573696	6.8	M	$> 72h$	$> 72h$	$> 72h$
ϕ_9	1152	2303520	34.5	M	$> 72h$	$> 72h$	$> 72h$

Some tables (I):

$f^k(x) := (x^2 + x + 1)^2 - p^{2k+1} \quad p \equiv 1 \pmod 3$

- Small degree
- *Medium* index
- *Large* coefficients

p	ind(f^k)	p-stem	PARI 2.3.4	MAGMA 2.11	SAGE 3.2.3
7	1000	0.41	2.14	0.89	2.4
7	2000	1.14	15.03	3.35	16.4
7	4000	4.02	111.7	15.6	121
7	8000	18.9	747	84.6	841
7	16000	105	5573	486	6374
7	20000	187	11520	859	12242
13	1000	0.5	3.8	1.37	4.4
13	2000	1.5	27.4	5.16	30.7
13	10000	53.7	2585	231	3071
19	10000	65.7	3444	284	4213
31	10000	86.5	4741	364	6000
37	10000	93.7	5238	395	6715
43	10000	100.6	5689	422	7370
103	10000	140	9120	596	11913
1009	1000	0.99	27.9	3.65	37
1009	2000	4.49	189	19.6	266.2
1009	4000	24.5	1380	112	2032
10^9+9	1000	3.94	188	23.2	519
10^9+9	2000	22.9	1409	133	4085
10^9+9	4000	139	10608	763	42790
$10^{69}+9$	100	1.59	12.4	5.61	165
$10^{69}+9$	200	4.14	88.5	30.1	1322
$10^{69}+9$	400	14.3	688	167	10802

Some tables (II): Random tests

$$p = 2$$

Order	Tests	Mean Degree	Mean Index	Mean Time
3	1800	65	6735	1.065
4	5054	117	25774	3.936
5	300	172	67411	19.605

$$1 < p < 1024$$

Order	Tests	Mean Degree	Mean Index	Mean Time
1	20000	7	33	0.002
2	10000	25	777	0.151
3	6000	65	6605	4.09

$$\mathbb{t}_r = \{\phi_1(x), S_1, \phi_2(x), S_2, \ldots, \phi_r(x), S_r, \psi_r(y)\}$$

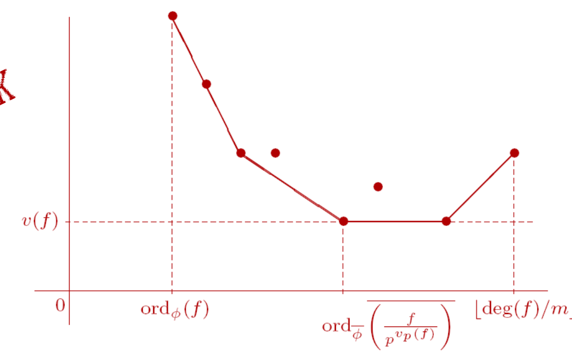
$$\mathrm{ind}_{\mathbb{t}_r}(F) := f_0 \cdots f_r \, \mathrm{ind}(N^{r+1}_{\phi_{r+1}}(F))$$

$$R_S(f)(y) := \sum_{(i,u_i)\in S} \overline{\left(\frac{a_i(x)}{p^{u_i}}\right)} \, y^{\frac{s-i}{e}} \in \mathbb{F}_\psi[y]$$

$$\psi_k(y) := cR^k_{S_k}(\phi_{k+1})(y) \in \mathbb{F}_k[y]$$

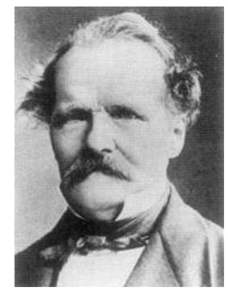
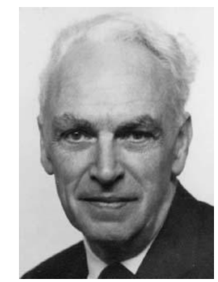
The mathematics of Montes algorithm

$\psi \,|\, R^{r+1}_S(\mathrm{Irr}(\theta, K, \mathbb{Q}))(y)$ irred. $\longrightarrow \mathfrak{a}_\psi \,|\, p\mathbb{Z}_K$



$$N_\phi(fg) = N_\phi(f) + N_\phi(g)$$

$$R_S(fg)(y) = R_S(f)(y) R_S(g)(y)$$

1. From  to 

Zur allgemeinen Theorie der algebraischen Größen.

Von Herrn *Michael Bauer* in Budapest.

§ I.

1. Es sei die Gleichung

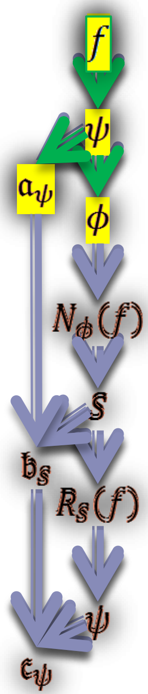
(I.) $$z^n + c_1 z^{n-1} + \cdots + c_k z^{n-k} + \cdots + c_n = 0$$

gegeben, deren Koeffizienten rationale ganze Größen irgend eines holoiden Bereiches $[(A), x_1, x_2, \dots x_m]$ bezw. $[[1], x_1, x_2, \dots x_m]$ sind.*) Es sei ferner P eine rationale Primgröße des Bereiches; w eine Wurzel der Gleichung (I.), die den Gattungsbereich (I') bestimmt. Es sollen in bezug auf den Gattungsbereich die Zerlegungen

(2.) $$\begin{cases} P = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_r^{e_r}, \\ w = \mathfrak{P}_1^{a_1}\mathfrak{P}_2^{a_2}\dots\mathfrak{P}_r^{a_r}\mathfrak{Q},\ (P, \mathfrak{Q}) = 1 \end{cases}$$

bestehen, wo $\mathfrak{P}_i$ ein Primideal, die Zahl e_i eine positive und die Zahl a_i eine nicht negative rationale ganze Zahl bedeuten.

Kummer–Dedekind's criterion



$$f(x) := \mathrm{Irr}(\theta, K, \mathbb{Q})$$

$$f(x) \equiv \psi_1(x)^{e_1} \cdots \psi_g(x)^{e_g} \pmod{p} \longrightarrow p\mathbb{Z}_K = \mathfrak{a}_1 \cdots \mathfrak{a}_g$$

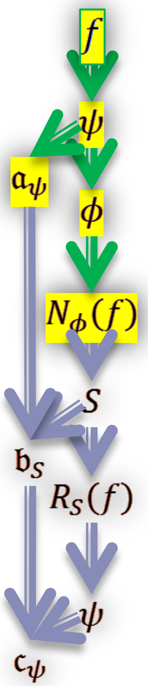
$$\psi_k(x) \in \mathbb{F}_p[x] \xrightarrow{\mathit{lifting}} \phi_k(x) \in \mathbb{Z}[x]$$

$$e_k = 1 \quad \text{or } \phi_k \nmid (f - \phi_1^{e_1} \cdots \phi_g^{e_g})/p \quad \Longrightarrow \mathfrak{a}_k = \mathfrak{p}_k^{e_k}$$

$$\mathfrak{p}_k = (p, \phi_k(\theta)),\ e(\mathfrak{p}_k/p) = e_k,\ \ f(\mathfrak{p}_k/p) = \deg \psi_k$$

$1, \theta, \ldots, \theta^{n-1}$ p–integral basis of K

Bauer–Ore: Newton polygon (I)

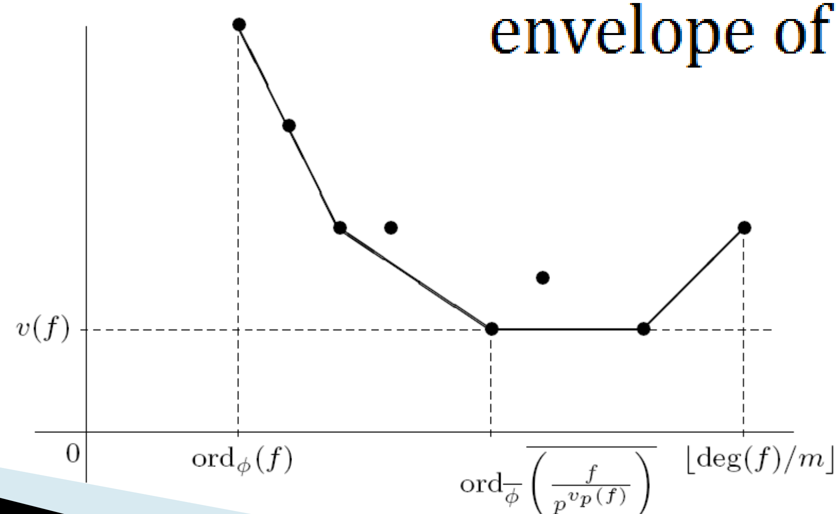


$$v\left(\sum a_i\, x^i\right) = \min_i\{v_p(a_i)\}$$

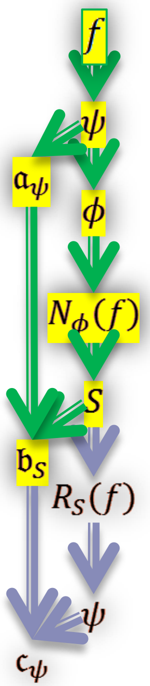
$\phi(x) \in \mathbb{Z}[x]$ monic and irreducible mod p

$$f(x) = \sum a_i(x)\, \phi(x)^i$$

$N_\phi(f) =$ principal part of the lower convex envelope of $\{(i, v(a_i(x))\}_i$

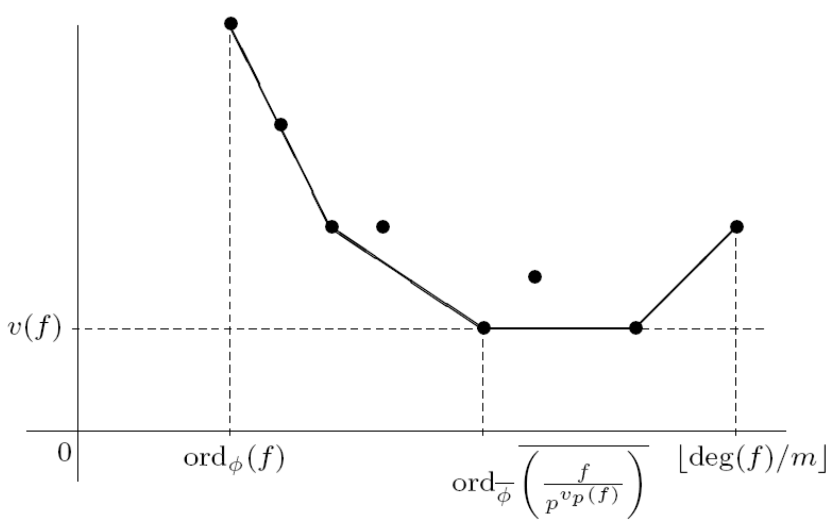


Bauer–Ore: Newton polygon (II)



$f(x) := \mathrm{Irr}(\theta, K, \mathbb{Q})$ escaping Dedekind's criterion

Fix $\psi = \psi_k,\quad \mathfrak{a}_\psi = \mathfrak{a}_k,\quad \phi = \phi_k(x)$

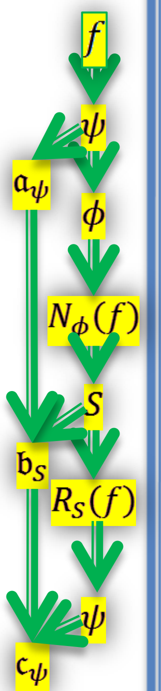


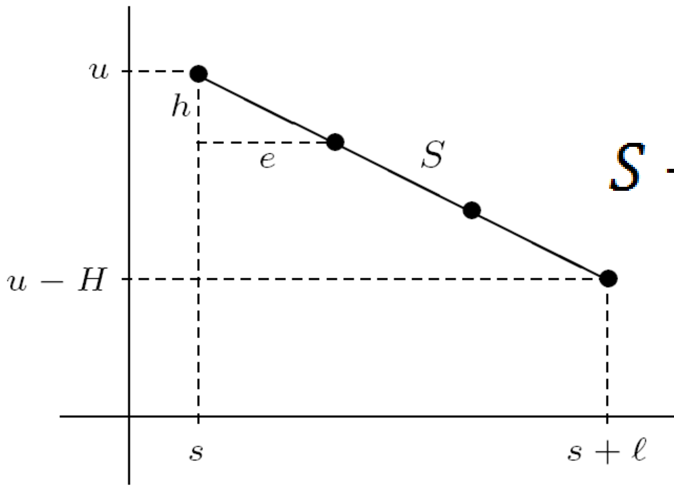
$$N_\phi(f) = S_1 + \cdots + S_r$$

$$\downarrow$$

$$\mathfrak{a}_\psi = \mathfrak{b}_1 \cdots \mathfrak{b}_r$$

Bauer–Ore: Residual polynomial





$$S \longrightarrow \begin{cases} \lambda = -h/e & \text{slope} \\ d = l/e = H/h & \text{degree} \end{cases}$$

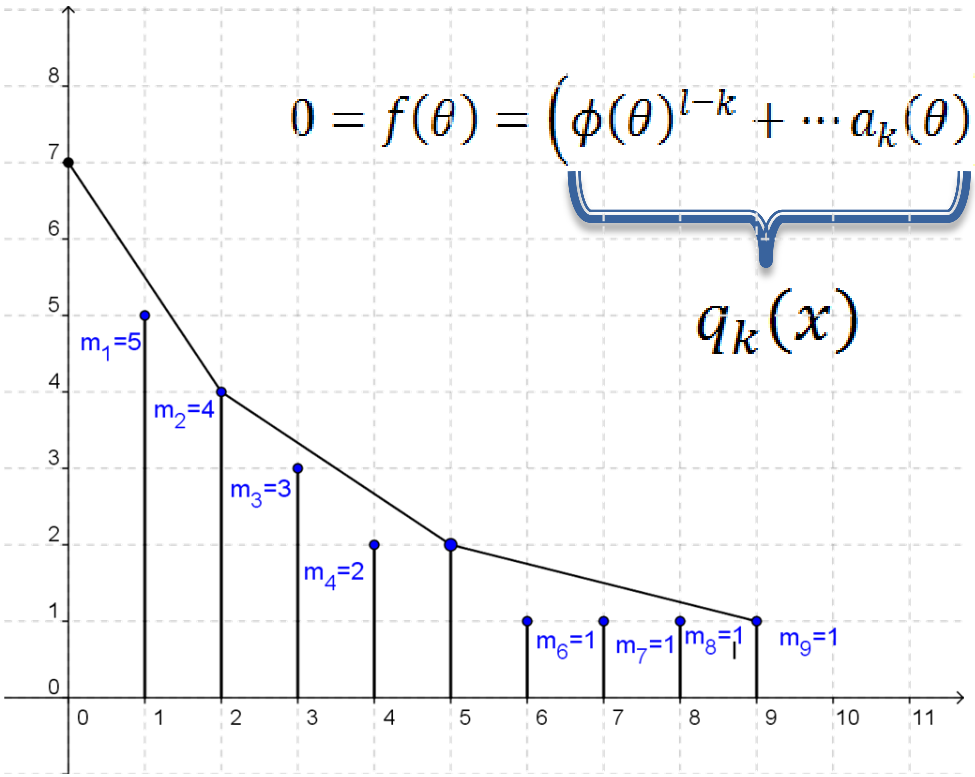
$$(i,u_i) \in S \Rightarrow p^{u_i} \mid a_i(x)$$

$$R_S(f)(y) := \sum_{(i,u_i)\in S} \overline{\left(\frac{a_i(x)}{p^{u_i}}\right)}\, y^{\frac{i-s}{e}} \in \mathbb{F}_\psi[y]$$

$$R_S(f)(y) = \psi_1(y)^{e_1} \cdots \psi_g(y)^{e_g} \longrightarrow \mathfrak{b}_S = \mathfrak{c}_1 \cdots \mathfrak{c}_g$$

$$e_k = 1 \Longrightarrow \mathfrak{c}_k = \mathfrak{p}_k^e,\quad e(\mathfrak{p}_k/p) = e,\quad f(\mathfrak{p}_k/p) = m \deg \psi_k$$

p–Integral basis in order 1



$$0 = f(\theta) = \underbrace{\Big(\phi(\theta)^{l-k} + \cdots a_k(\theta)\Big)}_{q_k(x)}\phi(\theta)^k + \underbrace{a_{k-1}(\theta)\phi(\theta)^{k-1} + \cdots + a_0(\theta)}_{v_p(\;) \geq m_k}$$

p–integral basis of K:

$$\left\{ \frac{q_j(\theta)\theta^k}{p^{m_j}} : 1 \leq j \leq l, 0 \leq k < \deg \phi \right\}_{\phi}$$

Theoretical background

Theorem of the product:

$$N_\phi(fg) = N_\phi(f) + N_\phi(g)$$

$$R_S(fg)(y) = R_S(f)(y)R_S(g)(y)$$

Theorem of the polygon

Theorem of the residual polynomial

p-adic reciprocals

Generalizing the lifting

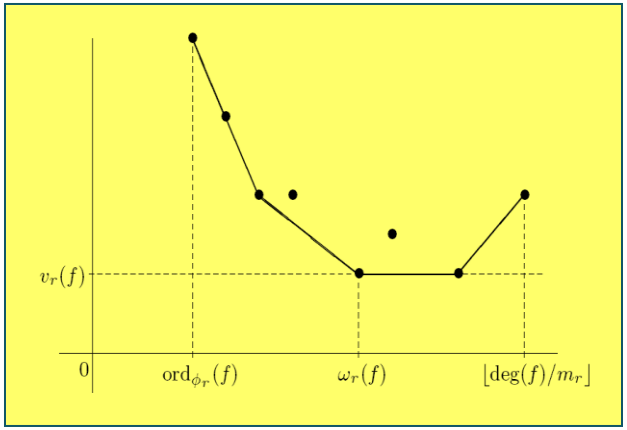
Proposition: Given

$$\phi(x) \in \mathbb{Z}[x], S, \psi(y) \in \mathbb{F}_{\overline{\phi}}[y]$$

we can easily compute a monic irreducible polynomial $F \in \mathbb{Z}[x]$ with

$$N_\phi(F) = S \qquad R_S(F)(y) = c\,\psi(y)$$

F is a representative of the order one type $\mathfrak{t} = \{\phi, S, \psi\}$



2. Higher Newton Polygons (Montes)

Outline

- Higher order types
- Higher valuations
- Higher Newton polygons
- Generalized theorems:
  - of the product
  - of the polygon
  - of the residual polynomial
- Finiteness results: control of the index

Recursive definitions and proofs!

Higher order types

A type of order r is

$$\mathbb{t}_r = \{\phi_1(x), S_1, \phi_2(x), S_2, \ldots, \phi_r(x), S_r, \psi_r(y)\}$$

where

$$\phi_k(x) \in \mathbb{Z}[x] \text{ monic, } \phi_k(x) \text{ irred. mod } p$$

$$N^k_{\phi_k}(\phi_{k+1}) = S_k \text{ side with slope } \lambda_k := -h_k/e_k$$

$$\psi_k(y) := cR^k_{S_k}(\phi_{k+1})(y) \in \mathbb{F}_k[y] \quad 0 \le k \le r-1$$

monic and irreducible

$$\psi_0(y) := \phi_1(y) \bmod p$$

$$\mathbb{F}_0 := \mathbb{F}_p \qquad \mathbb{F}_{k+1} = \mathbb{F}_k(z_k) \qquad \psi_k(z_k) = 0.$$

$\psi_r(y) \in \mathbb{F}_r[y]$ monic, irreducible, free

General "lifting"

Theorem: Given any type $\mathbb{t}_r$ we can effectively construct a monic irreducible polynomial $\phi_{r+1} \in \mathbb{Z}[x]$ such that:

$$N_{\phi_k}^{k}(\phi_{r+1}) = S_k, \qquad 1 \le k \le r$$

$$R_{S_k}^{k}(\phi_{r+1})(y) = c_k R_{S_k}^{k}(\phi_{k+1})(y) \quad 0 \le k \le r-1$$

$$R_{S_r}^{r}(\phi_{r+1})(y) = c\,\psi_r(y)$$

$$\mathbb{t}_r = \{\phi_1(x), S_1, \phi_2(x), S_2, \dots, \phi_r(x), S_r, \psi_r(y)\}$$

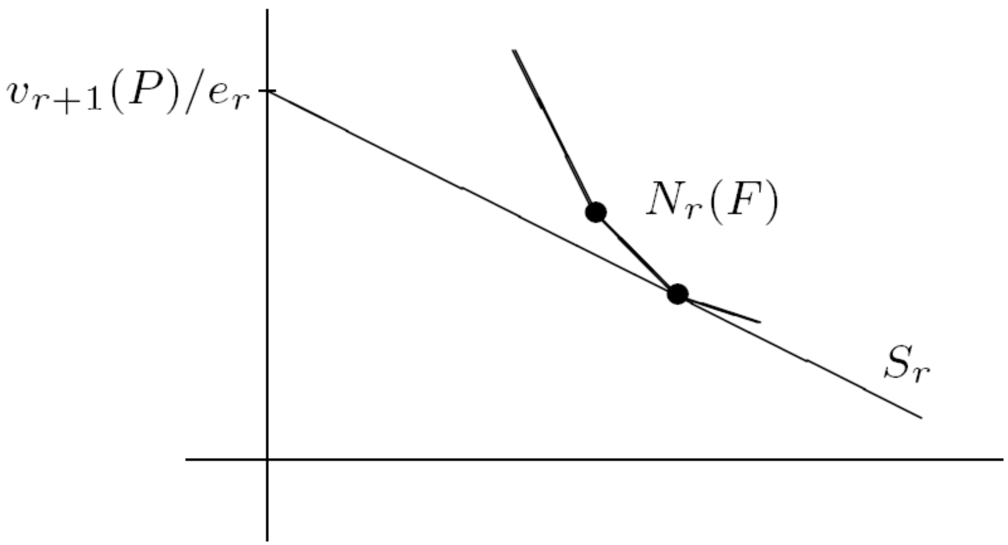
$$\Downarrow$$

$$\mathbb{t}_{r+1} = \{\phi_1(x), S_1, \phi_2(x), S_2, \dots, \phi_r(x), S_r, \phi_{r+1}(x), S_{r+1}, \psi_{r+1}(y)\}$$

ϕ_{r+1} is a *representative* of $\mathbb{t}_r$

Higher valuations

$$v_{r+1}\left(\sum a_i(x)\,\phi_r(x)^i\right) = e_r \min_i \{v_r(a_i(x)\phi_r(x)^i) + i|\lambda_r|)\}$$



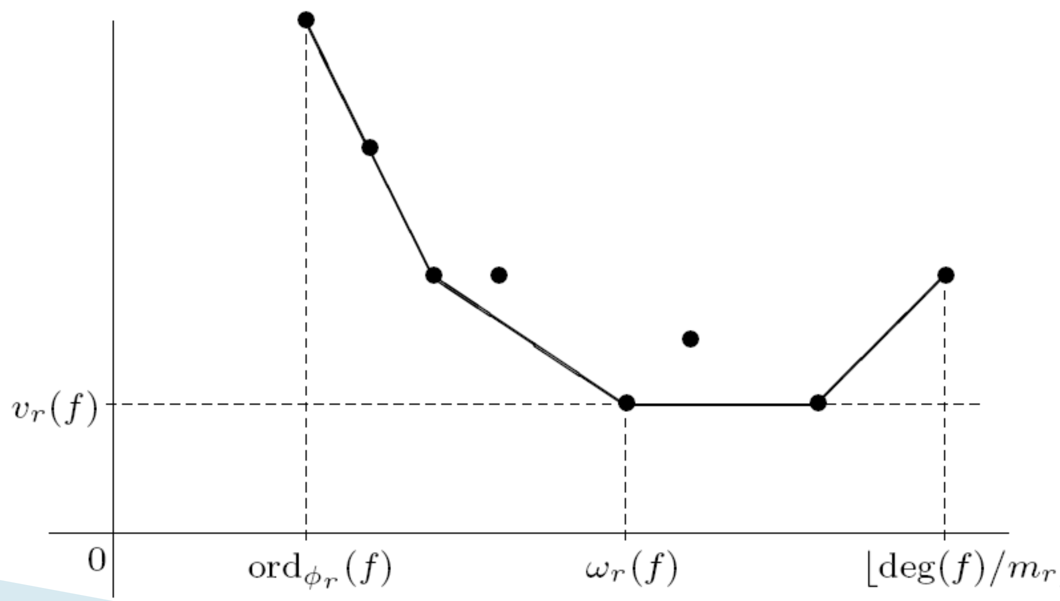
v_{r+1} extends v with index $e_1 \cdots e_r$

Higher Newton polygons

$$\mathfrak{t}_r \longrightarrow \phi_{r+1}$$

$$f(x) = \sum a_i(x)\,\phi_{r+1}(x)^i$$

$N^{r+1}_{\phi_{r+1}}(f) =$ principal part of the lower convex envelope of $\{(i, v_{r+1}(a_i(x)\phi_{r+1}(x)^i))\}_i$



Higher residual polynomials

Definition:

The residual polynomial in order *r*+1 attached to *S* is:

$$R_S^{r+1}(f)(y) = c_s + c_{s+e}y + \cdots + c_{s+(d-1)e}y^{d-1} + c_{s+de}y^d$$

$$c_i := z_r^{t_r(i)} R_S^r\big(a_i(x)\big)(z_r) \in \mathbb{F}_r$$

Higher order theorems

- Theorems of the product, of the polygon, of the residual polynomial:

$$\forall \mathfrak{t}_r \ \forall S \in N_{\phi_{r+1}}^{r+1}(\mathrm{Irr}(\theta, K, \mathbb{Q}))$$

$$\psi \,|\, R_S^{r+1}\big(\mathrm{Irr}(\theta, K, \mathbb{Q})\big)(y) \text{ irred.} \longrightarrow \mathfrak{a}_\psi \,|\, p\mathbb{Z}_K$$

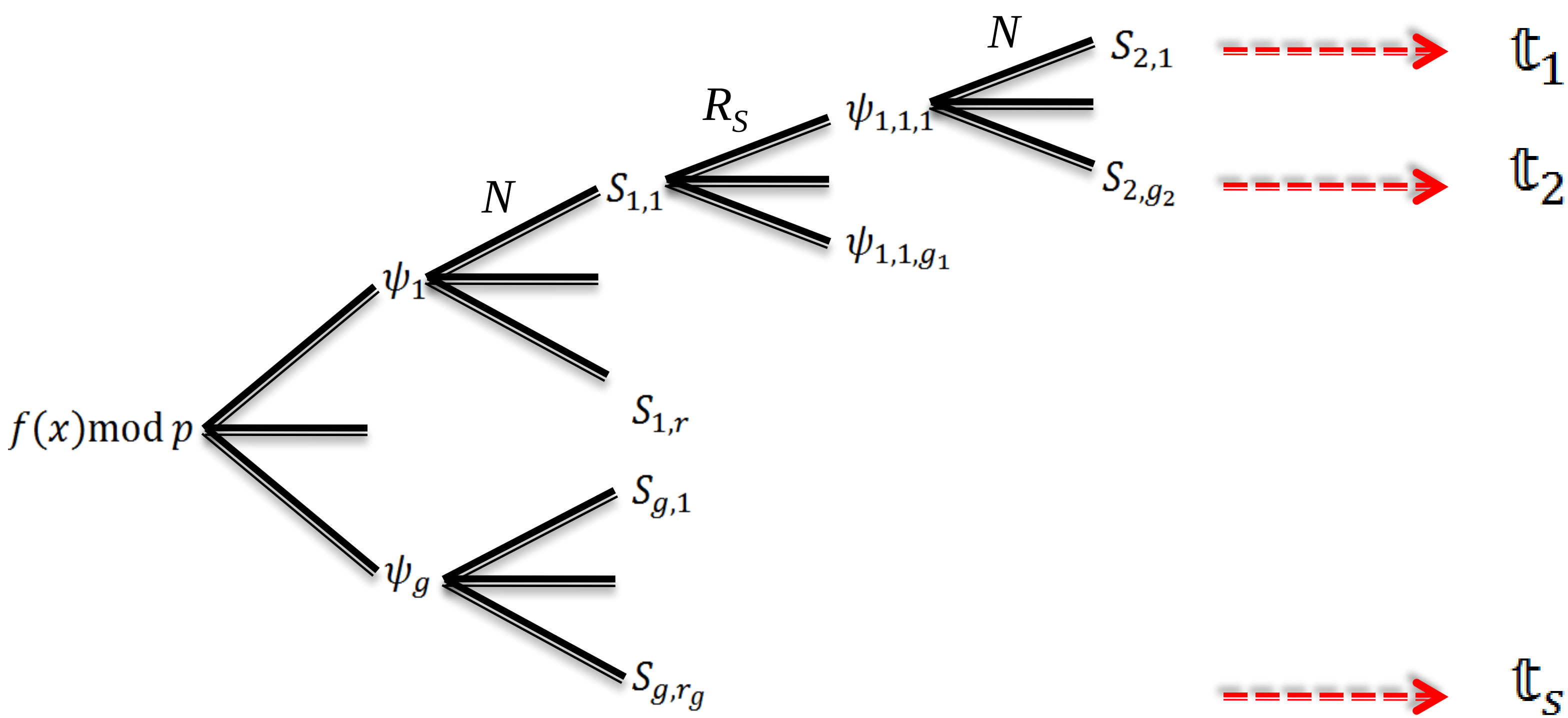
  - If ψ has exponent 1, then $\mathfrak{a}_\psi = \mathfrak{p}_\psi^e$ ($\mathfrak{t}_r$ is *complete*)
  - Otherwise, $S_{r+1} = S, \psi_{r+1} = \psi$ originate an extension of $\mathfrak{t}_r$:

$$\mathfrak{t}_r = \{\phi_1(x), S_1, \phi_2(x), S_2, \dots, \phi_r(x), S_r, \psi_r(y)\}$$

$$\Downarrow$$

$$\mathfrak{t}_{r+1} = \{\phi_1(x), S_1, \phi_2(x), S_2, \dots, \phi_r(x), S_r, \phi_{r+1}(x), S_{r+1}, \psi_{r+1}(y)\}$$

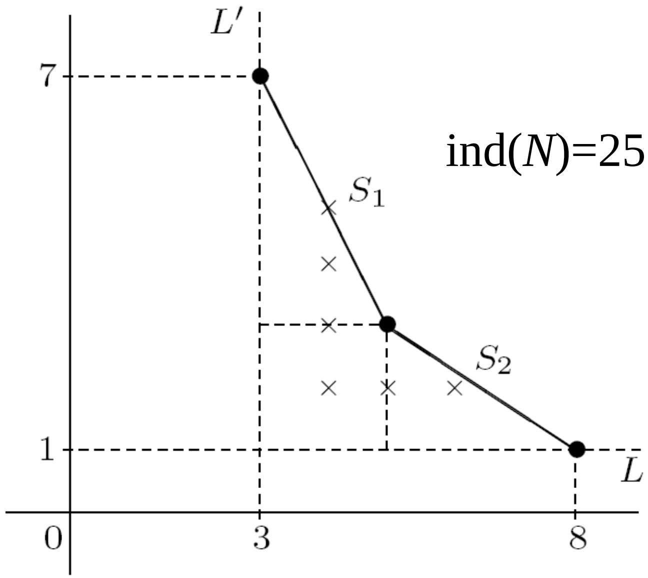
Types attached to a polynomial



- Every complete type $\mathfrak{t}$ determines a prime factor $\mathfrak{p}_{\mathfrak{t}}$ of $p\mathbb{Z}_K$.
- Every prime $\mathfrak{p}$ comes from a type.

Finiteness: Theorem of the index (I)

ind(N):= number of points of integral coordinates “below” N.



$$\mathbf{t}_r \dashrightarrow \operatorname{ind}_{\mathbf{t}_r}(F) := f_0 \cdots f_r \operatorname{ind}(N^{r+1}_{\phi_{r+1}}(F))$$

$$\operatorname{ind}_{r+1}(F) := \sum_{\mathbf{t}_r \in t_r(F)} \operatorname{ind}_{\mathbf{t}_r}(F)$$

Finiteness: Theorem of the index (II)

Theorem of the index

Let $f \in \mathbb{Z}[x]$ be a monic and separable polynomial.

a) $v_p(\mathrm{ind}(f)) \geq \mathrm{ind}_1(f)+...+\mathrm{ind}_r(f), \quad r \geq 1.$

b) Equality holds if and only if $\mathrm{ind}_{r+1}(f)=0$.

p–Integral basis in order r

$\mathfrak{t}_r = \{\phi_1(x), S_1, \phi_2(x), S_2, \dots, \phi_r(x), S_r, \psi_r(y)\}$ complete

Compute a representative ϕ_{r+1} of $\mathfrak{t}_r$

$$f(x) = Q(x)\phi_{r+1}(x) + a(x)$$

$$B_{\mathfrak{t}_r} = \left\{\frac{Q(\theta)q_{r,j_r}(\theta)q_{1,j_1}(\theta)\theta^{j_0}}{p^{m_{j_0,j_1,\dots,j_r}}}\right\}_{j_0,j_1,\dots,j_r}$$

Conjecture: $\bigcup_{\mathfrak{t}} B_{\mathfrak{t}}$ is a p – integral basis of K.

Proven when: $\max\{r\colon\ \mathfrak{t}_r\} = 1$ or $\mathrm{card}\{\mathfrak{t}_r\} = 1$.

Test: $v_p(ind(f)) = [\mathbb{Z}_K : \mathbb{Z}[\{B_{\mathfrak{t}}\}_{\mathfrak{t}}]]$

Complexity issues

What about the order of types?

- The running time of the algorithm is determined by the highest order of the involved types.

- The enlargement of a type is somewhat arbitrary, but Montes has designed a *refinement process* to :
  - 1. Eat as much index as possible in every order
  - 2. Assure that "$e_k f_k$">1" grows in every order.

$$\sum_{\mathfrak{t}} \prod_{k=1}^{r} e_k^{\mathfrak{t}} f_k^{\mathfrak{t}} = \deg f \implies \max\{r\colon \ \mathfrak{t}_r\} \ll \log_2 \deg f$$

- The number of types and its length should be related to the Galoisian structure of *K*.

Help. I need somebody (J. Lennon)

To do:

- Detailed analysis of the complexity of the algorithm

- Improvement of the diagonalization process (specific Gröbner basis computation).

- Implementation in Sage (requires factorization of polynomial over relative extensions of finite fields).