Computing Integral Closure Workshop

notes by Enric Nart and Claudiu Raicu

MSRI, July 26-30, 2010

Contents

Chapter 1

The Talks

1 Okutsu-Montes Representations of Prime Ideals in Global Fields (overview)

(talk by Enric Nart)

Setting: K is a *local field* (i.e. a field which is complete with respect to some discrete valuation) with finite residue field. We denote by $\mathcal{O}$ the ring of integers, $\mathfrak{m}$ its maximal ideal and π some uniformizer.

Montes' algorithm:

Input: $f \in \mathcal{O}[x]$ a monic, separable (i.e. has no multiple factors over $\overline{K}$) polynomial.

Output: A family $\mathbf{t}_1, \cdots, \mathbf{t}_g$ of *f-complete optimal types* (to be defined later), parametrizing the irreducible factors $F_1, \cdots, F_g$ of $f(x)$ in $\mathcal{O}[x]$.

We fix an irreducible factor F of f for the rest of the section. Let $\theta \in K^{sep}$ be a root of F, $L = K(\theta)$. We write $\mathbf{t}$ for the type corresponding to F,

$$\mathbf{t} = [\phi_1, \cdots, \phi_r; \phi_{r+1}] \quad (+ \text{ extra data})$$

where $\phi_i \in \mathcal{O}[x]$ are monic, irreducible, separable polynomials with

$$\deg(\phi_1)|\deg(\phi_2)|\cdots|\deg(\phi_{r+1}) = \deg(F)$$

and

$$\deg(\phi_1) < \deg(\phi_2) < \cdots < \deg(\phi_r)$$

(note that the degree of ϕ_{r+1} is allowed to be equal to that of ϕ_r).

One should think of ϕ_{r+1} as a "sufficiently good" approximation of F.

Remarks on Montes' algorithm:

1. The factorization is "detected" but never carried out. Only certain auxiliary polynomials are factorized and all the factorizations occur only over finite fields.
2. The type $\mathbf{t}$ encodes a lot of information about the extension (L/K).

The type $\mathbf{t}$ is structured on $r+1$ "levels" (we call r *the order* of $\mathbf{t}$). At each level $1 \leq i \leq r+1$ one has invariants

$$e_i, f_i, h_i, \lambda_i, \mu_i \text{ etc.}$$

Question 1.1. What information can one recover from these invariants?

- Valuations:
$$v(\phi_i(\theta)) = \frac{|\lambda_i| + \mu_i}{e_1 \cdots e_{i-1}}.$$
- Ramification index:
$$e(L/K) = e_1 \cdots e_r.$$
- Residual degree:
$$f(L/K) = \deg(\phi_1) \cdot f_1 \cdots f_r.$$

In the tamely ramified case, we get a tower of extensions

$$K \subset K_1 \subset \cdots \subset K_r \subset L$$

where $K_i = K(\alpha_i)$ for roots α_i of ϕ_i. In this case, e_i (f_i) represent the ramification index (residual degree) of the intermediate extension $K_i \subset K_{i+1}$ (we let $K_{r+1} = L$).

Definition 1.2. Given an irreducible factor F of f, we define the exponent of F by

$$\exp(F) = \min\{i : \pi^i \mathcal{O}_L \subset \mathcal{O}[\theta]\}$$

One can recover $\exp(F)$ from the invariants of the type $\mathbf{t}$:

$$\exp(F) = \sum_{i=1}^{r} (e_i f_i \cdots e_r f_r - 1) \cdot \frac{h_i}{e_1 \cdots e_i}$$

1.1 How to compute an integral basis of $\mathcal{O}_L$ over $\mathcal{O}$?

Let n denote the degree of F. We construct an integral basis of $\mathcal{O}_L$ over $\mathcal{O}$, of the form

$$1, \frac{g_1(\theta)}{\pi^{\nu_1}}, \cdots, \frac{g_{n-1}(\theta)}{\pi^{\nu_{n-1}}}$$

as follows. For each $0 \leq m < n$ there exists a unique expression of m as

$$m = j_0 + j_1 \cdot \deg(\phi_1) + \cdots + j_r \cdot \deg(\phi_r), \quad \text{with } 0 \leq j_k < \frac{\deg(\phi_{k+1})}{\deg(\phi_k)}.$$

Define g_m and ν_m via the formulas

$$g_m(x) = x^{j_0}\phi_1^{j_1} \cdots \phi_r^{j_r},$$
$$\nu_m = \lfloor j_1 \cdot v(\phi_1(\theta)) + \cdots + j_r \cdot v(\phi_r(\theta)) \rfloor.$$

Remark. The polynomial ϕ_{r+1} is not used for the computation of the integral basis, but will be useful in other algorithms.

Questions:

1. Does this work for plane curves?
2. Are the invariants encoded by $\mathbf{t}$ also invariants of the order $\mathcal{O}[\theta]$, or just of the defining polynomial F?
3. Can we compute the Galois group of $K(\theta)/K$ from the invariants of $\mathbf{t}$? Or at least the degree of the normal closure?
4. In the wildly ramified case, is it possible to choose the ϕ_i's so that the intermediate fields K_i form a tower (as in the tamely ramified case)?

2 Tameness + Anisotropy $\Rightarrow \widetilde{A}/A = \mathrm{lr}(A^\dagger/A)$

(talk by Hendrik Lenstra)

References: Little Groups (from last year's workshop) + Kosters' thesis

Summary: Given an order A over a Dedekind domain R, we would like to determine its integral closure $\widetilde{A}$. In general $\widetilde{A}/A$ has strong finiteness properties (e.g. it is a finite group in the number field case). If we impose the conditions of *tameness* and *anisotropy* on the order A, then we obtain the following direct description of its integral closure:

$$\widetilde{A}/A = \mathrm{lr}(A^\dagger/A)$$

where lr stands for "*lower root*" (to be explained below).

2.1 Lower Roots

Given a positive integer n, one defines the *lower root* of n by

$$\mathrm{lr}(n) := \max\{d \in \mathbb{Z} : d^2 | n\}.$$

Explicitly, if

$$n = \prod_p p^{a_p}$$

then

$$\mathrm{lr}(n) = \prod_p p^{\lfloor a_p/2 \rfloor}.$$

One can extend this notion to finite abelian groups as follows. We define the *lower root* functor on finite abelian groups to be the unique functor with the following properties:

- If M is a cyclic group, then $\mathrm{lr}(M)$ is the unique subgroup of M of order $\mathrm{lr}(\#M)$.
- lr preserves direct sums

$$\mathrm{lr}(M_1 \oplus M_2) = \mathrm{lr}(M_1) \oplus \mathrm{lr}(M_2).$$

The uniqueness of such a functor is easy, and for exitence one can check that the functor defined by

$$\mathrm{lr}(M) = \sum_{k \in \mathbb{Z}} (kM \cap M[k])$$

satisfies the two conditions above. (Here kM and $M[k]$ denote the image and kernel respectively, of the multiplication by k map on M)

Even more generally, given a Dedekind domain R and a finite length R-module M, we define the *lower root* of M to be the submodule

$$\mathrm{lr}(M) = \sum_{r \in R} (rM \cap M[r])$$

of M (where rM and $M[r]$ are defined as before).

2.2 Orders over Dedekind rings

Given a Dedekind ring R, we let $K = Q(R)$ denote its fraction field, and consider a finite (commutative) K-algebra E which is a product of separable field extensions of K. We call

such an algebra *étale*. Alternatively, one can define E to be a finite K-algebra, with the property that the *trace map*

$$Tr_{E/K} : E \to K$$

defines a nondegenerate bilinear pairing

$$\langle\ ,\ \rangle : E \times E \to K, \quad \langle x, y\rangle = Tr_{E/K}(xy).$$

(by definition, a pairing is said to be *nondegenerate* if its radical

$$E^{\perp} = \{x \in E : \langle x, E\rangle = 0\}$$

consists only of the zero element: $E^{\perp} = \{0\}$)

Given R and E, we say that an R-algebra $A \subset E$ is an *order* if it is finitely generated as a module over R, and generates E as an algebra (module) over K:

$$K \cdot A = E.$$

Note that since E has no R-torsion, the same is true about A, so A must be a projective R-module. In particular, if R is a dvr, then A is free. For an order A as above, we let $\widetilde{A}$ denote its integral closure in E (which coincides with the integral closure of R in E).

We define an $R - lattice$ in E to be a finitely generated R-module $L \subset E$ with the property that

$$K \cdot L = E.$$

Given a lattice L, its *dual* is defined by

$$L^{\dagger} = \{x \in E : \langle x, L\rangle \subset R\}.$$

This is a sub-R-module of E which is abstractly isomorphic to

$$\mathrm{Hom}_R(L, R),$$

and one has the equality

$$L^{\dagger\dagger} = L.$$

It is clear that an order A is a lattice, as well as its integral closure $\widetilde{A}$.

Since the trace of R-integral elements is contained in R, we obtain the inclusions

$$A \subseteq \widetilde{A} \subseteq \widetilde{A}^{\dagger} \subseteq A^{\dagger}.$$

With R, E and A fixed for the rest of the section, we consider the module

$$B = A^{\dagger}/A.$$

This is an $R-$ and $A-$ module of finite length, thus admits decompositions

$$B = \bigoplus_{\mathfrak{p} \subset R} B_{\mathfrak{p}} = \bigoplus_{\mathfrak{p}} \bigoplus_{\mathfrak{p} \subset \mathfrak{m} \subset A} B_{\mathfrak{m}}$$

where $\mathfrak{p}$ and $\mathfrak{m}$ denote maximal ideals of R and A respectively. Here $B_{\mathfrak{p}}$ denotes the localization of B at $\mathfrak{p}$ which, since B has finite length, we can think of as the sections of B suported at $\mathfrak{p}$

$$B_{\mathfrak{p}} = \{x \in B : \exists n \in \mathbb{Z}_{\geq 0} \text{ s.t. } \mathfrak{p}^n \cdot x = 0\}.$$

A similar description holds for $B_{\mathfrak{m}}$. The module $\widetilde{A}/A$ is also of finite length, so we obtain similar decompositions as for B.

The structure of finite length modules over Dedekind rings is (just as for $\mathbb{Z}$) very simple: they're all sums of $R/\mathfrak{p}^i$. We can thus write

$$B_{\mathfrak{m}} \simeq_R \bigoplus_{i \geq 1} (R/\mathfrak{p}^i)^{n(i,\mathfrak{m})},$$

where $n(i, \mathfrak{m})$ are nonnegative integers. More is true: since

$$\mathfrak{p}^{i-1} B_{\mathfrak{m}} / \mathfrak{p}^i B_{\mathfrak{m}} \simeq (R/\mathfrak{p})^{n(i,\mathfrak{m})}$$

has a filtration whose quotients that are $A/\mathfrak{m}$-modules, we must have that $[A/\mathfrak{m} : R/\mathfrak{p}]$ divides $n(i, \mathfrak{m})$:

$$n(i, \mathfrak{m}) \in [A/\mathfrak{m} : R/\mathfrak{p}] \cdot \mathbb{Z}_{\geq 0}.$$

2.3 A Concrete Theorem

Theorem 2.1 (Concrete Theorem)**.** *One has*

$$(\widetilde{A}/A)_{\mathfrak{m}} = \mathrm{lr}(B)_{\mathfrak{m}}$$

for each $\mathfrak{m}$ *satisfying the following two conditions*

1. *char*$(A/\mathfrak{m}) = 0$ *or* *char*$(A/\mathfrak{m}) > \sum_{i \geq 1} n(i, \mathfrak{m})$.
2. *There exist* $i_1, i_2 \in \mathbb{Z}_{>1}$ *such that*
   - $i_1 \neq i_2 \bmod 2$.
   - $n(i, \mathfrak{m}) = 0$ *for all* $i \notin \{1, i_1, i_2\}$.
   - $n(i, \mathfrak{m}) \in \{0, [A/\mathfrak{m} : R/\mathfrak{p}]\}$ *for* $i \in \{i_1, i_2\}$.

Remarks.

1. The first condition in the theorem above corresponds to *tameness*.
2. Since $A^\dagger_\mathfrak{p}$ is free of rank $\dim_K(E)$ over $R_\mathfrak{p}$, $B_\mathfrak{m}$ is minimally generated by $\dim_K(E)$ elements, so
$$\sum_i n(i,\mathfrak{m}) \leq \dim_K(E).$$
Therefore, if $\mathrm{char}(A/\mathfrak{m}) > \dim_K(E)$, condition (1) is automatically satisfied.
3. In general we don't expect any inclusions between
$$\mathrm{lr}(A^\dagger/A) \text{ and } \widetilde{A}/A.$$
4. One would be interesting to look at examples over $R = k[x]$.
5. For vector spaces over an algebraically closed field, anisotropy ($\langle x, x\rangle \neq 0$ for $x \neq 0$) is not an interesting notion since it can only occur on 1-dimensional spaces.

2.4 Tameness

Let k be a field and e a finite k-algebra (not necessarily étale). Consider the pairing

$$\langle\ ,\ \rangle : e \times e \to k, \quad \langle x, y\rangle = \mathrm{Tr}_{e/k}(xy).$$

We always have the inclusion
$$\sqrt{0_e} \subset e^\perp$$
(since nilpotent elements have trace zero). We say that e is *tame* (over k) if this inclusion is an equality:
$$\sqrt{0_e} = e^\perp.$$

Equivalently, since tameness in the above definition is local, we have that e is tame if and only if $e_\mathfrak{m}$ is tame for all maximal ideals $\mathfrak{m}$. This latter condition is in turn equivalent to
$$\begin{cases} e/\mathfrak{m} \text{ separable over } k \\ \mathrm{char}(k) \nmid \mathrm{length}_{e_\mathfrak{m}}(e_\mathfrak{m}) \end{cases}.$$

If an algebra is not tame, then we say it is *wild*.

We can see that this notion of tameness corresponds to the more familiar one in the case of Dedekind rings. Indeed, if $R \subset T$ are Dedekind rings, and $\mathfrak{p} \subset R$ a prime of R, then

$$\mathfrak{p}T = \prod_{\mathfrak{q}} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})}$$

and we say that $T/\mathfrak{p}T$ is tame over $R/\mathfrak{p}$ if and only if for all $\mathfrak{q}|\mathfrak{p}$ we have

$$\begin{cases} T/\mathfrak{q} \text{ separable over } R/\mathfrak{p} \\ \text{char}(R/\mathfrak{p}) \nmid e(\mathfrak{q}/\mathfrak{p}) \end{cases}.$$

Tameness for an order. More generally, given an order A over R and a maximal ideal $\mathfrak{m} \subset A$ lying over $\mathfrak{p} \subset R$, we say that

- $\mathfrak{m}$ is *tame over* $\mathfrak{p}$ if $(A/\mathfrak{p}A)_{\mathfrak{m}}$ is tame over $R/\mathfrak{p}$.
- A is *tame over* R at $\mathfrak{p}$ if $A/\mathfrak{p}A$ is tame over $R/\mathfrak{p}$.

Further topics: a Less Concrete Theorem, some proofs, examples.

3 Van Hoeij's Algorithm for Curves

(talk by Mike Stillman)

Setting: k is a field (we'll be mainly interested in the case $k = \mathbb{F}_q$) and $f \in k[x, y]$ is a polynomial satisfying the following properties

1. f is monic of degree n in the y variable (assume also irreducible for simplicity).
2. The discriminant
$$\Delta = \text{res}_y \left(f, \frac{\partial f}{\partial y} \right) \in k[x]$$
is nonzero.

Let $\mathcal{O}$ denote the integral closure of $k[x]$ inside $F = k(x)[y]/(f)$. We would like to obtain a basis of $\mathcal{O}$ over $k[x]$. For an irreducible polynomial P of $k[x]$ we will write $\mathcal{O}_P$ for the integral closure of $k[x]_{(P)}$ inside F (which is also the localization of $\mathcal{O}$ at the ideal (P)).

Strategy: divide and conquer. For each irreducible P for which $P^2|\Delta$ we construct a *local basis* of $\mathcal{O}_P$ over $k[x]_{(P)}$, and then we glue together all these bases to get a basis for $\mathcal{O}$ over $k[x]$.

Example 3.1. There is a polynomial f of the form

$$f = y^{21} + \cdots \in \mathbb{F}_2[x, y],$$

having degree 25 in x and discriminant

$$\Delta(x) = x^{22} \cdot (x+1)^{72} \cdot (\text{cubic})^2 \cdot (\text{cubic})^4 \cdot (\deg\ 7)^2 \cdot (\deg\ 17)^2 \cdot (\deg\ 58)^2 \cdot (\deg\ 112)^2.$$

The Van Hoeij algorithm seems to work significantly better than other known algorithms on this example.

Main ingredients:

- Use the Frobenius map to compute $\mathcal{O}_{P(x)}$.
- If P has small multiplicity in Δ we can sometimes use a different strategy to avoid computations.

Reduction: We only need to consider the case when $P(x) = x$. If P has degree at least two, we consider α a root of P and work over $k(\alpha)$. We compute $\mathcal{O}_{x-\alpha}$, the integral closure of $k(\alpha)[x]$ in $F \otimes_k k(\alpha)$ and then use the trace map

$$\text{tr} : k(\alpha)[x] \to k[x]$$

to obtain a basis for $\mathcal{O}_P$.

From now on we're in the following situation: $P(x) = x$, $f \in k[x, y]$ and m is maximal with the property that $x^{2m} | \Delta(f)$. The goal is to compute a local basis of $\mathcal{O}_x \subset F$.

Definition 3.2. A partial basis (or stem) B of $\mathcal{O}_x$ consists of the following data:

$$B = [(d_1, b_1), (d_2, b_2), \cdots, (d_r, b_r)]$$

for some $r \geq 0$, where

1. $1 \leq d_1 < d_2 < \cdots$ are positive integers.
2. $b_i = b_i(x, y) \in k[x, y]$ are monic polynomials in y of degree e_i.
3. $1 \leq e_1 < e_2 < \cdots < e_r \leq n - 1$.
4. $B_i = \dfrac{b_i}{x^{d_i}} \in \mathcal{O}$ for all $i = 1, \cdots, r$.

We denote by $L(B)$ the $k[x]_x$-span of

$$\{1, y, \cdots, y^{e_1-1}, B_1, yB_1, \cdots, y^{e_2-e_1-1}B_1, \cdots, B_r, yB_r, \cdots y^{n-e_r-1}B_r\}.$$

For example, if $B = [\,]$ is empty, then $L(B) = k[x,y]/(f)$.

Let $F = \mathrm{frac}k[x,y]/(f)$, $k = \mathbb{F}_q$ and consider the Frobenius map

$$\sigma : F \to F,\ g \mapsto g^p.$$

Suppose we have constructed a stem B preserved by σ ($\sigma(L(B)) \subset L(B)$). σ restricts then to a map

$$\sigma : \frac{1}{x}L(B) \to \frac{1}{x^p}L(B)$$

which in turn induces a map

$$\overline{\sigma} : L_1(B) = \frac{1}{x}L(B)/L(B) \to L_*(B) = \frac{1}{x^p}L(B)/L(B).$$

Note that $L_1(B)$ and $L_*(B)$ are finite dimensional vector spaces of dimensions n and n^p respectively. $\overline{\sigma}$ is a twisted k-linear map, i.e. it satisfies

$$\overline{\sigma}(u+v) = \overline{\sigma}(u) + \overline{\sigma}(v) \text{ for } u, v \in L_1(B),$$

$$\overline{\sigma}(au) = a^p\overline{\sigma}(u),\ \text{for } a \in k,\ u \in L_1(B).$$

Therefore, one can compute the kernel of this map readily.

We have the following

Lemma 3.3. *If $a \in \frac{1}{x}L(B)$ and $\overline{\sigma}(\overline{a}) = 0$ then $a \in \mathcal{O}$.*

Proof. $a^p \in L(B) \subset \mathcal{O}$ so a is integral over $k[x]$. □

Now the algorithm loops through the following procedure: given a stem B and $\overline{\sigma} : L_1(B) \to L_*(B)$ we compute the kernel of $\overline{\sigma}$. If this is nonzero we extend B so that $L_1(B)$ contains the elements of this kernel.

What happens if $ker(\overline{\sigma}) = 0$?

The answer is given by the following

Proposition 3.4. *Suppose $ker(\overline{\sigma}) = 0$. Then $\mathcal{O}_x \subset \frac{1}{x}L(B)$.*

Proof. The $k[x]_{(x)}$ module $\mathcal{O}_x/L(B)$ has finite length, so $x^N\mathcal{O}_x \subset L(B)$ for $N >> 0$. Assume that $\mathcal{O}_x$ is not contained in $\frac{1}{x}L(B)$ and choose some $a \in \mathcal{O}_x \setminus \frac{1}{x}L(B)$. Consider the function $g : \mathcal{O}_x \to \mathcal{O}_x$ given by

$$g(t) = \begin{cases} xt & \text{if } t \notin \frac{1}{x}L(B) \\ t^p & \text{if } t \in \frac{1}{x}L(B) \end{cases}.$$

We claim that if $t \notin L(B)$ then $g(t) \notin L(B)$. In particular $g^{(N)}(a) \notin L(B)$ for all N, but $g^{(N)}(a)$ is easily seen to be contained in $x^N\mathcal{O}_x$, which in turn is a subset of $L(B)$ for $N >> 0$, a contradiction.

To prove the claim, consider $t \notin L(B)$. If $t \notin \frac{1}{x}L(B)$ then $g(t) = xt \notin L(B)$. On the other hand, if $t \in \frac{1}{x}L(B)$ then $g(t) = t^p$ can't be in $L(B)$ because $\overline{\sigma}$ is injective. □

With this result, we can now finish our calculation of the local basis. We let $V_0 = L_1(B)$ and define V_i recursively as follows. We consider the induced map

$$\overline{\sigma} : V_i \to L_*(B)/V_i$$

and define

$$V_{i+1} = \ker(\overline{\sigma}).$$

We get a decreasing chain of subspaces

$$L_1(B) = V_0 \supset V_1 \supset \cdots \supset V_s = V_{s+1} = \cdots$$

which eventually stabilizes. It is then easy to check that $\mathcal{O}_x$ is the inverse image of V_s via the projection map

$$\frac{1}{x}L(B) \to L_1(B).$$

4 A Generalization of Anisotropy

(talk by Michiel Kosters)

4.1 Anisotropy of vector spaces

Let V be a finite dimensional vector space over a field k and let W be a 1-dimensional k-vector space. Let $\langle\ ,\ \rangle : V \times V \to W$ be a symmetric k-bilinear form.

Definition 4.1. The form $\langle\ ,\ \rangle$ is called *non-degenerate* if the map

$$\begin{aligned} \varphi : V &\to \mathrm{Hom}_k(V, W) \\ v &\mapsto \langle v, \cdot \rangle \end{aligned}$$

is an isomorphism. Remark that this is equivalent to φ being injective or surjective.

The form $\langle\ ,\ \rangle$ is called *anisotropic* if $\langle v, v \rangle = 0$ implies that $v = 0$. If the form is not anisotropic, it is called *isotropic*.

Remark 4.2. An anisotropic form is automatically non-degenerate.

4.2 Uniserial rings

We want to extend this definition of anisotropy to symmetric bilinear forms over modules over a certain class of rings.

Definition 4.3. A ring R is called uniserial if R is a zero-dimensional local principal ideal ring.

Such a uniserial ring R has the following struture. Let $\mathfrak{m} = (\pi)$ be the maximal ideal. As R is zero-dimensional and local, there is a smallest $n \in \mathbf{Z}_{\geq 1}$ such that $\mathfrak{m}^n = 0$. Then R has a composition series $R \supset \mathfrak{m} \supset \ldots \supset \mathfrak{m}^n = 0$ of length n and these ideals are the only ideals of R.

Remark 4.4. How do these rings arise in practice? Take a Dedekind domain and mod out by a nonzero ideal. One then has a zero-dimensional principal ideal ring and as this ring is Artinian, it is the product of uniserial rings. If R is a Dedekind domain and $\mathfrak{p}$ is a prime ideal of R, then $R/\mathfrak{p}^i$ for $i \in \mathbf{Z}_{\geq 1}$ is an example of such a ring. Remark that a field is also a uniserial ring.

These rings tend to have a lot of structures and modules over such rings also have a lot of structure.

Theorem 4.5. *Let $(R, \mathfrak{m})$ be a uniserial ring of length n. Let M be an R-module. Then*

$$M \cong \bigoplus_{i=1}^{n} \left(R/\mathfrak{m}^i\right)^{(n_i)}$$

where the n_i are uniquely determined cardinal numbers.

Corollary 4.6. *Let R be a uniserial ring and let M be a finitely generated R-module. Then $M \cong \mathrm{Hom}_R(M, R)$.*

This last corollary gives the possibility for non-degenerate forms over such modules.

4.3 Anisotropy

Let $(R, \mathfrak{m})$ be a uniserial ring of length n, let M be a finitely generated R-module, N be a free rank 1 R-module and finally let $\langle\ ,\ \rangle : M \times M \to N$ be a symmetric bilinear form. Our task will be to define the notion of anisotropy. First of all, this should be a generalization of the well-known concept in the vector space case.

Definition 4.7 (Try 1 (complete fail, works only in the vector space case))**.** $\langle\ ,\ \rangle$ is called anisotropic if $\langle x, x\rangle = 0$ implies that $x = 0$.

This definition fails terribly. Consider the form on $\mathbf{Z}/p^2\mathbf{Z}$ over $\mathbf{Z}/p^2\mathbf{Z}$ given by [1]. Then $\langle p, p\rangle = 0$, but this form looks anisotropic somehow. The problem comes from the fact that there is a submodule $\mathrm{lr}(M) \subset M$ (which is 0 iff the space is a vector space), such that $\langle \mathrm{lr}(M), \mathrm{lr}(M)\rangle = 0$. We can now modify our definition. First we define this lower root and the upper root.

Definition 4.8. We define the lower root respectively the upper root of M as

$$\begin{aligned} \mathrm{lr}(M) &= \sum_{i=0}^{n} \left(\mathfrak{m}^i M \cap M[\mathfrak{m}^i]\right) \\ \mathrm{ur}(M) &= \bigcap_{i=0}^{n} \left(\mathfrak{m}^i M + \mathrm{M}[\mathfrak{m}^i]\right). \end{aligned}$$

This looks like a terrible definition, but once one knows the decomposition of M into cyclic groups, one can easily calculate it (example).

Definition 4.9 (Try 2 (fail in characteristic 2, even if we ask for non-degeneracy))**.** $\langle\ ,\ \rangle$ is called anisotropic if $\langle x, x\rangle = 0$ implies that $x \in \mathrm{lr}(M)$.

This definition seems very reasonable, but it is not clear how one can check if it holds (this is just too much work). Secondly, I don't know if it implies that the form is non-degenerate, which we want as an analogue. For the final definition we first need to define two maps. We have $\langle \mathrm{lr}(M), \mathrm{ur}(M)\rangle = 0$ and $\mathfrak{m} \cdot \mathrm{ur}(M) \subseteq \mathrm{lr}(M) \subseteq \mathrm{ur}(M)$.

Definition 4.10. First define

$$\begin{aligned} \langle\ ,\ \rangle_{\mathrm{odd}} : \mathrm{ur}(M)/\mathrm{lr}(M) \times \mathrm{ur}(M)/\mathrm{lr}(M) &\to N \\ ([x], [y]) &\mapsto \langle x, y\rangle \end{aligned}$$

Let

$$\langle\ ,\ \rangle' : M/M[\mathfrak{m}] \times M/\mathfrak{m}[\mathfrak{m}] \to N/N[\mathfrak{m}].$$

Finally define

$$\langle\ ,\ \rangle_{\text{even}} = \langle\ ,\ \rangle'_{\text{odd}}.$$

(Give some random example)

This definition looks rather abstract. First remark that these odd and even forms are actually forms on vector spaces (with images in $N[\mathfrak{m}]$ respectively $N[\mathfrak{m}^2]/N[\mathfrak{m}]$). We should also remark that one can calculate this form explicitly without much trouble.

Definition 4.11 (Good one!)**.** The form $\langle\ ,\ \rangle$ is called anisotropic if $\langle\ ,\ \rangle_{\text{odd}}$ and $\langle\ ,\ \rangle_{\text{even}}$ are anisotropic (as forms over vector spaces).

If the even and odd forms are non-degenerate, then so is the original one. We have the following theorem.

Theorem 4.12. *Consider the following statements.*

1. $\langle\ ,\ \rangle$ *is anisotropic;*
2. *the form* $\langle\ ,\ \rangle$ *is non-degenerate and for any submodule* $L \subseteq M$ *with* $L \subseteq L^{\perp}$ *we have* $L \subseteq \operatorname{lr}(M)$ *and* $\operatorname{lr}(L^{\perp}/L) = \operatorname{lr}(M)/L$.
3. *the form* $\langle\ ,\ \rangle$ *is non-degenerate and if* $x \in M$ *satisfies* $\langle x, x\rangle = 0$*, then* $x \in \operatorname{lr}(M)$.

Then i $\iff$ *ii* $\implies$ *iii and all are equivalent if* $\operatorname{char}(R/\mathfrak{m}) \neq 2$.

This second statement is given so one can see the connection with quasi-anisotropy as given in the previous lecture by Hendrik Lenstra. Actually, there is another equivalent notion of anisotropy which is related to the integral closure, but it doesn't look very natural.

Remark that non-degenerate forms on 1-dimensional vector spaces are automatically anisotropic and we obtain the following theorem directly.

Theorem 4.13. *Suppose that* $\langle\ ,\ \rangle : M \times M \to N$ *is non-degenerate. The following statements hold.*

1. *If* M *is cyclic, then* $\langle\ ,\ \rangle$ *is anisotropic.*
2. *Suppose that* M *is generated by* 2 *elements and suppose that* $\operatorname{length}_R(M)$ *is odd. Then* $\langle\ ,\ \rangle$ *is anisotropic.*

4.4 Quasi-anisotropy

For calculating the integral closure the statement that the odd and even forms are anisotropic is too strong. The notion of quasi-anisotropy is a bit weaker and has no analogue in the vector space case.

Theorem 4.14. *The following statements are equivalent for a non-degenerate form* $\langle\ ,\ \rangle$*:*

1. *The induced form* $\langle\ ,\ \rangle' : M/M[\mathfrak{m}] \times M/M[\mathfrak{m}] \to R/R[\mathfrak{m}]$ *is anisotropic;*
2. *For any* $L \subseteq \mathrm{lr}(M)$ *we have* $\mathrm{lr}(L^\perp/L) = \mathrm{lr}(M)/L$.

If one of these statements hold, the form is called quasi-anisotropic.

One sees that anisotropy implies quasi-anisotropy and one sees the connection with the anisotropic case.

4.5 Bonus

Another equivalent definition of being anisotropic is that the unique submodule $L \subset M$ satisfying $\mathfrak{m}L^\perp \subseteq L \subseteq L^\perp$ is $\mathrm{lr}(M)$. This is the definition which we first used and has a nice application in the calculation of the ring of integers. For this it is also important to know $\bigcap_{L\subset M:\mathfrak{m}L^\perp\subseteq L\subseteq L^\perp} L$. We can calculate this in the case that $\mathrm{char}(R/\mathfrak{m}) \neq 2$, but what happens in the other case?

5 The Factorization Algorithm

(talk by Enric Nart)

Recall our setting: K is a *local field* with valuation v and ring of integers $\mathcal{O}$, $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$ and π an uniformizer. We assume that the residue field $\mathbb{F}_0 = \mathcal{O}/\mathfrak{m}$ is perfect and that v is normalized so that $v(\pi) = 1$.

Consider the discrete valuation v_1 on $K(x)$ defined by

$$v_1\left(\sum_{0\leq s} a_s x^s\right) = \min_{0\leq s}\{v(a_s)\},$$

and the reduction map

$$R_0 : K[x] \to \mathbb{F}_0[y], \quad g(x) \mapsto \overline{\frac{g(y)}{\pi^{v_1(g)}}} \text{ for } g \neq 0, \quad 0 \mapsto 0.$$

This is easily seen to be a semigroup homomorphism.

Our AIM: To "factorize" any given monic separable polynomial $f(x) \in \mathcal{O}[x]$.

Fix one such f for the rest of the talk. The first step is to factorize $R_0(f)(y)$ over $\mathbb{F}_0$. We write

$$R_0(f)(y) = \varphi_1(y)^{a_1} \cdots \varphi_k(y)^{a_k}$$

for some irreducible polynomials $\varphi_i \in \mathbb{F}_0[y]$. Via Hensel's lemma, we can lift this to a factorization

$$f = F_1 \cdots F_k \text{ in } \mathcal{O}[x],$$

with $R_0(F_j) = \varphi_j^{a_j}$.

We shall construct a "tree of types" for each of the irreducible factors φ_i appearing in the above decomposition. From now on, we fix one of the irreducible factors φ_i, and denote it by ψ_0. The leaves of the tree corresponding to ψ_0 will be in one-to-one correspondece with the irreducible factors of $F := F_i$.

We consider $\phi_1 \in \mathcal{O}[x]$ some monic separable lift of ψ_0 (i.e. ϕ_1 has $R_0(\phi_1) = \psi_0$).

We define a *type of order* 0 to be a list consisting of a separable polynomial whose reduction modulo $\mathfrak{m}$ is irreducible and separable (separability is automatic under the assumption that $\mathbb{F}_0$ is perfect). $[\phi_1]$ is an example of a type of order 0.

The factorization of F will be done in parallel with the branching of the tree with root $\mathbf{t} = [\phi_1]$. Any refinement of the factorization of F will correspond to introducing new types as vertices of this tree.

5.1 Invariants and operators associated to a type

The fundamental invariants that get attached to a type $\mathbf{t}$ are a slope

$$\lambda_i = -h_i/e_i$$

for positive coprime integers h_i, e_i, and a monic irreducible polynomial

$$\psi_i(y) \in \mathbb{F}_i[y].$$

The fields $\mathbb{F}_i$ are obtained recursively starting with $\mathbb{F}_0$ via

$$\mathbb{F}_{i+1} = \mathbb{F}_i[y]/(\psi_i(y)).$$

We denote by z_i the class of y in $\mathbb{F}_{i+1}$, so that we have

$$\mathbb{F}_{i+1} = \mathbb{F}_i(z_i) = \cdots = \mathbb{F}_0(z_0, \cdots, z_i).$$

From the fundamental invariants one constructs new invariants f_i, m_i by

$$f_i = \deg(\psi_i) \text{ and } m_i = \deg(\phi_i).$$

Along with the above invariants, we associate to the type $\mathbf{t}$ operators v_i, N_i, R_λ as follows. For $i \geq 1$ v_i will be a discrete valuation on $K(x)$ (we've already seen v_1). For $i \geq 0$ we introduce Newton polygon operators $N_i : K[x] \to 2^{\mathbb{R}^2}$ which associate to a polynomial its Newton polygon of order i. For $\lambda \in \mathbb{Q}^-$ we define reduction maps $R_\lambda : K[x] \to \mathbb{F}_i[y]$. We let $R_i := R_{\lambda_i}$.

At this point we have $\lambda_0 = 0$, $e_0 = 1$, $f_0 = \deg(\psi_0)$.

Definition 5.1. Given a type $\mathbf{t}$ of order 0 and a polynomial $g \in \mathcal{O}[x]$, we define the *order of* $\boldsymbol{t}$ *in* g to be

$$\mathrm{ord}_{\mathbf{t}}(g) := \mathrm{ord}_{\psi_0}(R_0(g)).$$

5.2 The Newton polygon operator in order 1

Given a polynomial $g \in \mathcal{O}[x]$, we consider its ϕ_1-expansion

$$g(x) = \sum_{0 \leq s} a_s(x) \cdot \phi_1^s, \quad \text{with } \deg(a_s) < m_1.$$

We define the Newton polygon $N_1(g)$ of g of order 1 to be the lower convex hull of the set of points

$$(s, v_1(a_s \phi_1^s)).$$

It is clear that $v_1(\phi_1) = 1$ because ϕ_1 is monic, so $v_1(a_s \phi_1^s) = v_1(a_s)$ and we denote this by u_s.

We are only interested in the *principal part* of the Newton polygon of f. This is by definition the subset $N_1^-(f) \subset N_1(f)$ consisting of the union of the negative slopes in $N_1(f)$. For a polygon N, we define the *length* of N to be the length of the projection of N to the horizontal axis, and we denote it by $l(N)$.

Remarks:

- $l(N_1^-(g)) = \mathrm{ord}_{\mathbf{t}}(g)$.
- The most expensive part of the algorithm consists of the divisions with remainder performed to obtain the ϕ_i-expansions of f.

5.3 Residual polynomial operators

To the polygon $N := N_1^-(f)$ one can associate certain *residual coefficients*

$$c_s = \begin{cases} 0 & \text{if } (s, u_s) \text{ lies above N,} \\ R_0(a_s)(z_0) & \text{if } (s, u_s) \text{ lies on N.} \end{cases}$$

It is clear that c_s is always nonzero in the second case.

Consider any $\lambda \in \mathbb{Q}^-$ and define

$$S_\lambda = \{(x, y) \in N : y + x|\lambda| \text{ is minimal}\}.$$

Then one sees that

$$S_\lambda = \begin{cases} \text{vertex} & \text{if } \lambda \text{ is not a slope of } N, \\ \text{side} & \text{if } \lambda \text{ is a slope of } N. \end{cases}$$

We write

$$\lambda = -\frac{h_\lambda}{e_\lambda}$$

with h_λ, e_λ coprime and define the degree of S_λ by

$$\deg(S_\lambda) = \frac{l(S_\lambda)}{e_\lambda} = \#(\text{integral points on } S_\lambda) - 1.$$

Define the residual polynomial of f with respect to λ to be

$$R_\lambda(f) := c_{s_0} + c_{s_0+e_\lambda} y + \cdots + c_{s_1} y^d \in \mathbb{F}_1[y],$$

where s_0, s_1 are the abscissae of the endpoints of S_λ, and d is the degree of S_λ.

The following three results are due to Ore, and appear in his PhD thesis from 1923.

Theorem 5.2 (Theorem of the Product)**.**

$$\begin{cases} N_1^-(gh) = N_1^-(g) + N_1^-(h) \\ R_\lambda(gh) = R_\lambda(g) \cdot R_\lambda(h) \end{cases}$$

Theorem 5.3 (Theorem of the Polygon)**.** *Let $F_{\boldsymbol{t}} \in \mathcal{O}[x]$ be the (unknown) factor of $f(x)$ attached to ψ_0 by Hensel's lemma. Then there exist unique polynomials $F_\lambda \in \mathcal{O}[x]$ with the properties*

1. $F_{\boldsymbol{t}}(x) = \prod_{\lambda \in slopes(N_1^-(f))} F_\lambda(x).$

2. *F_λ is monic, $N_1(F_\lambda)$ is one-sided with slope λ and $R_\lambda(F_\lambda) \sim R_\lambda(f)$ (here $\sim$ denotes equality up to a nonzero scalar).*

If these conditions hold, then one also has that

3. *$v(\phi_1(\theta)) = |\lambda|$ for any root θ of $F_\lambda(x)$.*

Theorem 5.4 (Theorem of the Residual Polynomial)**.** *If we write*

$$R_\lambda(f) \sim \prod_\psi \psi(y)^{a_\psi}$$

with $\psi \in \mathbb{F}_1[y]$ monic irreducible polynomials and a_ψ integers, then there exists a factorization

$$F_\lambda(x) = \prod_\psi F_{\lambda,\psi}(x) \text{ in } \mathcal{O}[x],$$

where each $F_{\lambda,\psi}$ is monic with $R_\lambda(F_{\lambda,\psi}) = \psi^{a_\psi}$.

It follows from the Theorem of the Product that $N_1(F_{\lambda,\psi})$ in the last theorem is one-sided with slope λ.

Note If $\mathrm{ord}_{\mathbf{t}}(f) = 1$ then $F_{\mathbf{t}}$ is irreducible by the Theorem of the Product and we stop the algorithm. Otherwise, we start branching the tree of types as described in the next section.

5.4 Branching of types

Corresponding to the factor $F_{\lambda,\psi}$ of F_λ we introduce a new node in the tree of types, and label it by the type of order one $\mathbf{t}' = [\phi_1, \phi_{\lambda,\psi}]$. We join $\mathbf{t}(= [\phi_1])$ and $\mathbf{t}'$ by an edge.

We define (analogously to the type zero case) the order in f of a type $\mathbf{t}'$ of order one by

$$\mathrm{ord}_{\mathbf{t}'}(f) = \mathrm{ord}_\psi(R_\lambda(f)).$$

In our case, this is equal to a_ψ. As before, if $\mathrm{ord}_{\mathbf{t}'}(f)$ is equal to 1, then $F_{\lambda,\psi}$ is irreducible and we stop.

At this point we have a polynomial $F_{\lambda,\psi}$ satisfying the following properties:

- $R_0(F_{\lambda,\psi}) \sim \psi_0^r \in \mathbb{F}_0[y]$ for some $r > 0$.
- $N_1(F_{\lambda,\psi})$ is one-sided with slope λ.

- $R_\lambda(F_{\lambda,\psi}) \sim \psi_0^r \in \mathbb{F}_1[y]$ for some $r > 0$.

The next step in the algorithm is to construct a polynomial $\phi_{\lambda,\psi}$ minimal with the above properties. The first property follows automatically from the other two, so what we're really looking for is a polynomial satisfying

$$\begin{cases} N_1(\phi_{\lambda,\psi}) \text{ is one sided wrt } \lambda, \\ R_\lambda(\phi_{\lambda,\psi}) \sim \psi, \\ \deg(\phi_{\lambda,\psi}) = e_\lambda f_\psi m_1. \end{cases}$$

How to construct $\phi_{\lambda,\psi}$?

We write

$$\psi(y) = c_0 + c_1 y + \cdots + y^d \in \mathbb{F}_1[y]$$

where each coefficient c_i can be written as

$$c_i = \alpha_0 + \alpha_1 z_0 + \cdots + \alpha_{f_0-1} z_0^{f_0-1}, \text{ for } \alpha_i \in \mathbb{F}_0.$$

We lift these coefficients c_i to polynomials $c_i \in \mathcal{O}[x]$,

$$c_i(x) = a_0 + a_1 x + \cdots + a_{f_0-1} x^{f_0-1},$$

where $a_i \in \mathcal{O}$ reduce modulo $\mathfrak{m}$ to α_i. Then the polynomial $\phi_{\lambda,\psi}$ defined by

$$\phi_{\lambda,\psi}(x) = \sum_{i=0}^{d} \pi^{h_\lambda \cdot (d-i)} c_i(x) \phi_1(x)^{i e_\lambda},$$

is the desired one.

At this point we call $\phi_{\lambda,\psi} =: \phi_2$ and write $[\phi_1, \phi_2]$ for the type $\mathbf{t}'$. We let $\lambda_1 = \lambda$ and $\psi_1 = \psi$ be the fundamental invariants of $\mathbf{t}'$.

6 Radical Rings

(talk by Hendrik Lenstra)

Setting: R is a dvr with maximal ideal $\mathfrak{p}$ and field of fractions K, E is an étale algebra over K and $A \subset E$ an R-order.

$$\begin{array}{ccc} A & \subset & E \\ \cup & & \cup \\ R & \subset & K \end{array}$$

We have the usual pairing on E given by

$$\langle x, y\rangle = \mathrm{Tr}_{E/K}(xy),$$

and

$$A^\dagger = \{x \in E : \langle x, A\rangle \subset R\}.$$

Since $\left\langle A, A^\dagger\right\rangle \subset R$ we get an induced pairing on $B = A^\dagger/A$

$$\langle\ ,\ \rangle : B \times B \to K/R,$$

whose image is $(\mathrm{ann}_R B)^{-1}/R$. This is a perfect duality inducing an isomorphism

$$B \xrightarrow{\sim} \mathrm{Hom}_R(B, K/R).$$

The correspondence between our objects and those from Michiel's talk (Section 4) is as follows:

$$M \longleftrightarrow B$$

$$R_{\text{Michiel}} \longleftrightarrow R/(\mathrm{ann}_R B)$$

$$N \longleftrightarrow (\mathrm{ann}_R B)^{-1}/R$$

Recall that A is *tame* if and only if the induced pairing

$$A/\mathfrak{p}A \times A/\mathfrak{p}A \xrightarrow{\langle\ ,\ \rangle} R/\mathfrak{p}$$

satisfies

$$(A/\mathfrak{p}A)^\perp = \mathfrak{r}/\mathfrak{p}A,$$

where $\mathfrak{r}$ denotes the Jacobson radical of A

$$\mathfrak{r} = \bigcap_{\mathfrak{m}\subset A \text{ maximal}} \mathfrak{m}.$$

We will see later that if A is tame over R, then we have the equivalences

$$A = \widetilde{A} \iff \mathfrak{p}B = 0 \iff (\mathfrak{r} : \mathfrak{r}) = A,$$

and also

$$(\mathfrak{r} : \mathfrak{r})/A = (\mathfrak{p}B)[\mathfrak{r}] \subset (\mathfrak{p}B)[\mathfrak{p}] \subset \mathrm{lr}(B).$$

Note: The equivalence $A = \widetilde{A} \iff (\mathfrak{r} : \mathfrak{r}) = A$ follows from Theorem 8.1, without any tameness assumption.

6.1 Radical algebras over a field K

Let $t \in \mathbb{Z}_{\geq 0}$, $n_1, n_2, \cdots, n_t \in \mathbb{Z}_{>1}$ and $a_1, \cdots, a_t \in K$. Consider the K-algebra

$$E = K[x_1, \cdots, x_t]/(x_1^{n_1} - a_1, \cdots, x_t^{n_t} - a_t).$$

We have $\dim_K(E) = n = n_1 \cdots n_t$ and a basis of E/K

$$\mathcal{B} = \{\prod_{i=1}^{k} \overline{x_i}^{j_i} : 0 \leq j_i < n_i\}.$$

It's easy to see that

$$\mathrm{Tr}_{E/K}\left(\prod_{i=1}^{k} \overline{x_i}^{j_i}\right) = \begin{cases} n \cdot 1 & \text{if all } j_i = 0, \\ 0 & \text{otherwise.} \end{cases}$$

As a consequence, we get

$$E \text{ is tame over } K \iff \mathrm{char}(K) \nmid n,$$

$$E \text{ is finite étale over } K \iff \begin{cases} \mathrm{char}(K) \nmid n \\ \alpha_i \in K^* \text{ for all } i \end{cases}.$$

From now on, we shall assume that E is finite étale over K.

We define the *group of radicals* to be the subgroup $\mathcal{G} = \langle \overline{x_1}, \cdots, \overline{x_t} \rangle \cdot K^*$ of E^*. We have an exact sequence

$$1 \longrightarrow K^* \longrightarrow \mathcal{G} \longrightarrow \oplus_{i=1}^{t} \mathbb{Z}/n_i\mathbb{Z} \longrightarrow 0,$$

where the last map sends an element $a\overline{x_1}^{i_1} \cdots \overline{x_t}^{i_t}$ to $(\overline{i_1}, \cdots, \overline{i_t})$.

6.2 Preferred alternative description of E

We start from a field K and an exact sequence

$$1 \longrightarrow K^* \xrightarrow{\iota} \mathcal{G} \xrightarrow{\varphi} H \longrightarrow 1$$

of abelian groups with $\#H = n < \infty$ and $\mathrm{char}(K) \nmid n$. Define E to be the K-algebra

$$E = K[\mathcal{G}]/(\alpha \cdot 1 - 1 \cdot \imath(\alpha) : \alpha \in K^*) = K[\mathcal{G}] \otimes_{K[K^*]} K,$$

where the map $K[K^*] \to K[\mathcal{G}]$ is induced by ι, and the map $K[K^*] \to K$ by the inclusion of $K^* \subset K$. Clearly, $\mathcal{G} \subset E^*$.

For $h \in H$, we let $E_h = (\varphi^{-1}h) \cup \{0\}$. This is a 1-dimensional K-subspace of E, and we have the decomposition

$$E = \bigoplus_h E_h.$$

Note that the restriction of $\mathrm{Tr}_{E/K}$ is multiplication by n on E_1 and 0 on E_h for $h \neq 1$.

Let now $v : K^* \twoheadrightarrow \mathbb{Z}$ be a discrete valuation, with valuation ring R having maximal ideal $\mathfrak{p}$, and assume that $v(n \cdot 1) = 0$. v induces a map $\mathcal{G} \to \mathbb{Q}$ (which we also denote by v) given by

$$g \mapsto \frac{1}{n} \cdot v(g^n).$$

(we used the fact that $g^n \in K^*$ since $nH = 0$). We get a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^* & \longrightarrow & \mathcal{G} & \longrightarrow & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle v} & & \vdots{\scriptstyle \overline{v}} & & \\ 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where the arrow $\overline{v}$ is induced by v.

In what follows, we will be interested in orders $A \subset E$ with the property that A is generated by $A \cap \mathcal{G}$ as an R-module (in which case we get a direct sum decomposition $A = \bigoplus_{h \in H} R \cdot \langle A \cap E_h \rangle$).

The only R-lattices in E that we shall consider will have the form

$$\bigoplus_{h \in H} R \cdot e_h, \text{ with each } e_h \in E_h, \quad e_h \neq 0.$$

Let

$$\mathcal{S} = \{s : H \to \mathbb{Q} : s \text{ is a lift of } \overline{v}, \qquad \begin{array}{ccc} & & H \\ & {\scriptstyle s}\swarrow & \downarrow{\scriptstyle \overline{v}} \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array} \}.$$

There is a bijection between the set $\mathcal{S}$ and the collection of lattices described above, given by

$$s \mapsto L_s = \bigoplus_{h \in H} I_{h,s(h)},$$

where

$$I_{h,q} = \{x \in E_h : v(x) \geq q\} \cup \{0\}.$$

If $s \in \mathcal{G}$ then L_s is an order if and only if

$$\begin{cases} s(1) = 0 \\ \text{for all } h, h' \in H,\ s(h) + s(h') \geq s(hh') \end{cases}.$$

Given such s, we write A_s for the corresponding order. The orders constructed in this way are *Hendrik's radical rings.*

Properties of A_s:

- A_s is finite étale over R (i.e. $\Delta_{A_s/R} = (1)$) if and only if $s = 0$. If this is the case, then $\overline{v} = 0$ and $A_s = \widetilde{A}_s$.
- A_s is tame over R.
- $A_s = \widetilde{A}_s \iff s(H) \subset [0, 1)$.

It turns out that the lattices $\mathfrak{r}A_s$ and $L_s^\dagger$ are easy to describe, and are both lattices of the type considered. More precisely,

$$\mathfrak{r}A_s = L_{s'}$$

where

$$s'(h) = \begin{cases} s(h) & \text{if } s(h) > 0 \\ 1 & \text{if } s(h) = 0 \end{cases}$$

and

$$L_s^\dagger = L_{\overline{s}},\ \text{where } \overline{s}(h) = -s(h^{-1}).$$

Consider now an order A_s and write

$$A_s = \bigoplus_{h \in H} I_{h,s(h)}, \quad A_s^\dagger = \bigoplus_{h \in H} I_{h,-s(h^{-1})}.$$

We can then compute B as

$$B_s = A_s^\dagger / A_s = \bigoplus_{h \in H} I_{h,-s(h^{-1})} / I_{h,s(h)} \simeq_R \bigoplus_{h \in H} (R/\mathfrak{p})^{s(h)+s(h^{-1})}.$$

As an inner product space, B_s is the orthogonal sum of one copy of

$$I_{h,-s(h)} / I_{h,s(h)}$$

for each $h \in H[2]$ and one copy of

$$I_{h,-s(h^{-1})}/I_{h,s(h)} \oplus I_{h^{-1},-s(h)}/I_{h^{-1},s(h^{-1})}$$

for each $\{h, h^{-1}\} \in (H \setminus H[2])/\{\pm\}$ (where $\pm$ is the equivalence relation identifying h with h^{-1}).

Let $h \in H[2]$. We get

$$\mathrm{lr}(I_{h,-s(h)}/I_{h,s(h)}) = \begin{cases} I_{h,0}/I_{h,s(h)} & \text{if } s(h) \in \mathbb{Z} \\ I_{h,\frac{1}{2}}/I_{h,s(h)} & \text{if } s(h) \in \frac{1}{2} + \mathbb{Z} \end{cases}.$$

From this, we conclude that the following implication holds:

$$H = H[2] \Longrightarrow \widetilde{A_s}/A_s = \mathrm{lr}(B_s).$$

It's easy to check that if B_s is anisotropic then $A_s = \widetilde{A_s}$ or $H = H[2]$.

Example 6.1. Take $n = 2m$ an even integer, H a cyclic group of order n and set

$$\mathcal{G} = K^* \cdot \langle g \rangle,$$

with $v(g^{2m}) = 2$. Let π be an uniformizer of R and consider

$$A = R\left[g, \frac{g^{m+1}}{\pi}\right].$$

Then

$$\widetilde{A} = R\left[g, \frac{g^m}{\pi}\right]$$

and

$$B = (R/\mathfrak{p}^2) \oplus (R/\mathfrak{p})^{2(m-1)}.$$

It follows that $B/B[\mathfrak{p}] \simeq R/\mathfrak{p}$, hence B is quasi-anisotropic, but not anisotropic.

7 Some Proofs

(talk by Michiel Kosters)

Fix $(R, \mathfrak{m})$ a uniserial ring, M a finitely generated R-module, and $N \simeq_R R$. We will try to prove the following

Theorem 7.1. *Let $\langle\ ,\ \rangle : M \times M \to N$ be a nondegenerate form. The following are equivalent:*

1. *$\langle\ ,\ \rangle_{odd}$ and $\langle\ ,\ \rangle_{even}$ are anisotropic (recall that, by definition, this is equivalent to $\langle\ ,\ \rangle$ being anisotropic).*
2. *There exists a unique $L \subset M$ with the property that $\mathfrak{m}L^\perp \subset L \subset L^\perp$.*
3. *For all $L \subset M$ with $L \subset L^\perp$ we have that $L \subset \mathrm{lr}(M)$ and $\mathrm{lr}(L^\perp/L) = \mathrm{lr}(M)/L$.*

We first introduce a reduction process called *shaving*, which will turn out to be useful in our proofs. Let r be such that $\mathrm{Ann}_R(M) = \mathfrak{m}^r$, and assume that $r \geq 2$. Define the *shaving* of M to be the module

$$\mathrm{Sh}(M) = M[\mathfrak{m}^{r-1}]/\mathfrak{m}^{r-1}M.$$

The bilinear form $\langle\ ,\ \rangle$ on M induces a pairing

$$\langle\ ,\ \rangle' : \mathrm{Sh}(M) \times \mathrm{Sh}(M) \to N,$$

and this has the property that $\langle\ ,\ \rangle_{\mathrm{odd}}$ and $\langle\ ,\ \rangle_{\mathrm{even}}$ are the same for M and $\mathrm{Sh}(M)$ as long as $r \geq 3$.

We will prove the implications (1) $\Rightarrow$ (2) and (2) $\Longleftrightarrow$ (3) in Theorem 7.1, and leave the implication (2) $\Rightarrow$ (1) as an exercise. We start with a

Lemma 7.2. *Let $L \subset M$ be a submodule with the property that $L \subset L^\perp$. Then there exists $L' \supset L$ such that*

$$\mathfrak{m}L'^\perp \subset L' \subset L'^\perp.$$

Proof. Consider a maximal submodule L' of M with the property that $L \subset L' \subset L'^\perp$. We claim that it has the desired properties. Assume that this isn't the case and consider the pairing

$$\langle\ ,\ \rangle'' : L'^\perp/L' \times L'^\perp/L' \to N$$

induced by $\langle\ ,\ \rangle$. Our assumption says that $\mathfrak{m}$ doesn't kill $L'^\perp/L'$, so its lower root is nontrivial. The lift of $\mathrm{lr}(L'^\perp/L')$ to M yields a module bigger than L' which kills itself, contradicting the maximality of L'. □

Proof of Theorem 7.1. (2) $\Rightarrow$ (1). Assume $\langle\ ,\ \rangle_{\mathrm{odd}}$ is isotropic, i.e. that there exists $x \in M \setminus \mathrm{lr}(M)$ with the property that $\langle x, x\rangle = 0$. Let $L = Rx$, which is clearly contained in $L^\perp$. The preceding lemma allows us to find an $L' \supset L$ such that $\mathfrak{m}L'^\perp \subset L' \subset L'^\perp$. The uniqueness of (2) implies that $L' = \mathrm{lr}(M)$, which is not possible.

Suppose now that $\langle\ ,\ \rangle_{\mathrm{even}}$ is isotropic. Then we use induction as follows

- For $r = 0, 1$ $\langle\ ,\ \rangle_{\text{even}}$ can't be isotropic.
- For $r = 2$ one checks the statement by an explicit calculation.
- For $r \geq 3$ the statement follows by induction using shaving.

(2) $\Rightarrow$ (1). Exercise.

(2) $\Rightarrow$ (3). Suppose $L \subset L^\perp$ and consider the induced pairing

$$\langle\ ,\ \rangle'' : L^\perp/L \times L^\perp/L \to N,$$

which still satisfies (2). There is a bijection between the sets

$$A = \{L' \supset L : \mathfrak{m}L'^\perp \subset L' \subset L'^\perp\}$$

and

$$B = \{S \subset L^\perp/L : \mathfrak{m}S^\perp \subset S \subset S^\perp\}.$$

The uniqueness in (2) says that $\#A \leq 1$, while the lower root of $L^\perp/L$ provides an element of B, so $\#B \geq 1$. This shows that $A = B$ and

$$\mathrm{lr}(M)/L = \mathrm{lr}(L^\perp/L).$$

(3) $\Rightarrow$ (2). Suppose that L is such that

$$\mathfrak{m}L^\perp \subset L \subset L^\perp.$$

It follows that $\mathfrak{m}$ kills $L^\perp/L$ and therefore $\mathrm{lr}(L^\perp/L) = 0$. Condition (3) then implies that $\mathrm{lr}(M)/L = 0$, i.e. $L = \mathrm{lr}(M)$ is the unique module with $\mathfrak{m}L^\perp \subset L \subset L^\perp$. □

8 Day 3, Round 2

(talk by Anurag Singh)

8.1 The method of Grauert-Remmert/de Jong

Let R be a reasonable (excellent) reduced ring and denote by $\mathrm{frac}(R)$ its total ring of fractions. Let $\widetilde{R}$ be the integral closure of R inside $\mathrm{frac}(R)$.

Suppose that $J \subset R$ is an ideal containing a non-zero-divisor. We have inclusions

$$R \hookrightarrow \mathrm{Hom}_R(J, J) \hookrightarrow \mathrm{frac}(R),$$

where the first map sends $r \in R$ to the multiplication by r map, and the second map sends φ to $\varphi(x)/x$ for some non-zero-divisor x.

By the Cayley-Hamilton theorem, we have an inclusion $\mathrm{Hom}_R(J,J) \subset \widetilde{R}$, hence we obtain a series of containments

$$R \subset \mathrm{Hom}_R(J,J) \subset \widetilde{R} \cap \mathrm{Hom}_R(J,R) \subset \mathrm{Hom}_R(J,\sqrt{J}),$$

of which only the last one requires an explanation. To prove it, consider $h \in \widetilde{R} \cap \mathrm{Hom}_R(J,R)$ and write down some integral equation with R-coefficients satisfied by h:

$$h^n + r_1 h^{n-1} + \cdots + r_n = 0, \qquad \text{with } r_i \in R.$$

For any $j \in J$ we can multiply this equation by j^n to obtain

$$(hj)^n + j r_1 (hj)^{n-1} + \cdots + j^n r_n = 0.$$

Starting at the second term, all terms are elements of J, so $(hj)^n$ must also be contained in J, i.e. $hj \in \sqrt{J}$.

Using these facts, we can prove the following

Theorem 8.1. *Let J be an ideal containing a non-zero-divisor such that*

1. *$J = \sqrt{J}$.*
2. *$V(J) \supset$ non-normal locus of R.*

Then $R = \widetilde{R}$ if and only if $Hom_R(J,J) = R$.

Proof. "$\Rightarrow$" is clear since $R \subset \mathrm{Hom}_R(J,J) \subset \widetilde{R}$.

"$\Leftarrow$" Condition (2) says that we can find N with the property that $J^N \widetilde{R} \subset R$. Fix such an N. The inclusion $J \cdot J^{N-1}\widetilde{R} \subset R$ can be rewritten as

$$J^{N-1}\widetilde{R} \subset \mathrm{Hom}_R(J,R),$$

from which we get

$$J^{N-1}\widetilde{R} \subset \widetilde{R} \cap \mathrm{Hom}_R(J,R) \subset \mathrm{Hom}_R(J,\sqrt{J}) = \mathrm{Hom}_R(J,J) = R.$$

This shows that $J^{N-1}\widetilde{R} \subset R$ and repeating the argument $N-1$ more times we get that $\widetilde{R} \subset R$. □

This theorem gives us an algorithm for computing $\widetilde{R}$: find J satisfying (1) and (2) and consider $\mathrm{Hom}_R(J,J)$. If this is larger than R then replace R by $\mathrm{Hom}_R(J,J)$ and repeat.

Another way of "making progress" towards the normalization is given by the following result of Lipman:

Theorem 8.2 (Lipman)**.** *Let R be a finitely generated algebra over a field k of characteristic zero. Then*

$$R = \widetilde{R} \text{ if and only if } Hom(J^{-1}, J^{-1}) = R,$$

where $J^{-1} = Hom_R(J_{R/k}, R)$ is the dual of the Jacobian ideal $J_{R/k}$.

8.2 A Frobenius based algorithm (Leonard-Pellikaan, Singh-Swanson)

Assume now that R is a reduced ring containing a field of characteristic $p > 0$. Let D be an element of the conductor which is a non-zero-divisor. We set

$$V_0 = \frac{1}{D}R \subset \mathrm{frac}(R), \quad V_0 \supset \widetilde{R}.$$

Now we proceed analogously to the last part of the Van Hoeij's algorithm. We define inductively for $e \geq 0$

$$V_{e+1} = \{f \in V_e : f^p \in V_e\}.$$

This gives a decreasing sequence of submodules $V_0 \supset V_1 \supset V_2 \cdots$.

Theorem 8.3. *This descending chain stabilizes and $\widetilde{R}$ is the stabilization.*

Proof. We have

$$V_e = \{f \in V_0 : f^{p^i} \in V_0 \text{ for all } i \leq e\}.$$

Clearly if $f \in \widetilde{R}$ then $f^{p^i} \in \widetilde{R}$, so $f \in V_e$ for all e. We thus have the inclusion $\widetilde{R} \subset V_e$ for all e.

Consider the Rees valuations $v_1, \cdots, v_k$ of the principal ideal (D) (which are by definition the valuations corresponding to the minimal primes of the ideal $D\widetilde{R} \subset \widetilde{R}$). Pick an e so that $p^e > v_i(D)$ for $1 \leq i \leq k$. Suppose that $\frac{r}{D} \in V_e$ for some $r \in R$. It follows that

$$\left(\frac{r}{D}\right)^{p^e} \in V_0 = \frac{1}{D}R$$

which we can rewrite as

$$r^{p^e} \in D^{p^e-1}R.$$

Taking valuations, we obtain

$$p^e v_i(r) \geq (p^e - 1)v_i(D) \Longleftrightarrow v_i(r) \geq v_i(D) - \frac{v_i(D)}{p^e}.$$

Since $v_i(D) < p^e$ is an integer, we must have $v_i(r) \geq v_i(D)$. This holds for all i, so $\frac{r}{D} \in \widetilde{R}$, and we get the inclusion $V_e \subset \widetilde{R}$. We already have the reverse inclusion, so in fact $V_e = \widetilde{R}$. □

9 Tameness + Anisotropy $\Rightarrow \widetilde{A}/A = \mathrm{lr}(A^\dagger/A)$ (contd.)

(talk by Hendrik Lenstra)

Recall our setting: R is a Dedekind domain with field of fractions K, E is a finite étale K-algebra, A an R-order and $\widetilde{A}$ the integral closure of A in E. The pairing on E defined from the trace map $\mathrm{Tr}_{E/K}$ induces a perfect pairing

$$\langle\ ,\ \rangle : B \times B \longrightarrow K/R, \text{ where } B = A^\dagger/A,\ A^\dagger = \{e \in E : \mathrm{Tr}_{E/K}(eA) \subset R\}.$$

We shall sketch the proofs of the following "less concrete" theorems.

Theorem 9.1 (€)**.** *If $\widetilde{A}$ is tame over R and B is anisotropic, then $\widetilde{A}/A = \mathrm{lr}(B)$.*

Theorem 9.2 (£)**.** *If every order between A and $\widetilde{A}$ is tame over R and B is quasi-anisotropic, then $\widetilde{A}/A = \mathrm{lr}(B)$.*

Assume for simplicity that R is a dvr with maximal ideal $\mathfrak{p}$, and let

$$\mathfrak{r} = \bigcap_{0 \neq \mathfrak{m} \in \mathrm{Spec}(A)} \mathfrak{m}$$

be the Jacobson radical of A. A is tame over R if and only if

$$\mathfrak{r}/\mathfrak{p}A = \sqrt{0_{A/\mathfrak{p}A}}.$$

We have

(1) $A \neq \widetilde{A}$ if and only if $(\mathfrak{r} : \mathfrak{r}) \supsetneq A$.

($) If A is tame over R then $(\mathfrak{r} : \mathfrak{r})/A = (\mathfrak{p}B)[\mathfrak{r}]$.

(3) If A is tame over R, then $A = \widetilde{A}$ if and only $\mathfrak{p}B = 0$.

(1) follows from Theorem 8.1. Notice that $\mathfrak{p}B = 0$ if and only if $(\mathfrak{p}B)[\mathfrak{r}] = 0$, so (3) follows from (1) and (\$).

Proof of (\$). "$\subset$": Consider the diagram

$$\begin{array}{ccc} A/\mathfrak{p}A \times A/\mathfrak{p}A & \xrightarrow{\langle\ ,\ \rangle} & R/\mathfrak{p} \\ \downarrow & & \downarrow \\ A/\mathfrak{r} \times A/\mathfrak{r} & \xrightarrow{\langle\ ,\ \rangle} & R/\mathfrak{p} \\ \downarrow & \nearrow_{\langle\ ,\ \rangle} & \\ \frac{(\mathfrak{r}:\mathfrak{r})}{\mathfrak{r}} \times \frac{(\mathfrak{r}:\mathfrak{r})}{\mathfrak{r}} & & \end{array}$$

where the pairings $\langle\ ,\ \rangle$ are all induced by $\mathrm{Tr}_{E/K}$ ($\langle \overline{x}, \overline{y} \rangle = \overline{\mathrm{Tr}_{E/K}(xy)}$).

Since A is tame over R, the pairing on $A/\mathfrak{r}$ is nondegenerate. It follows that

$$\frac{(\mathfrak{r}:\mathfrak{r})}{\mathfrak{r}} = \frac{A + \{x \in (\mathfrak{r}:\mathfrak{r}) : \langle x, A \rangle \subset \mathfrak{p}\}}{\mathfrak{r}} = \frac{A}{\mathfrak{r}} \bigoplus \frac{(\mathfrak{r}:\mathfrak{r}) \cap \mathfrak{p}A^\dagger + A}{A},$$

so

$$\frac{(\mathfrak{r}:\mathfrak{r})}{A} = \frac{(\mathfrak{r}:\mathfrak{r}) \cap \mathfrak{p}A^\dagger + A}{A} \subset \frac{\mathfrak{p}A^\dagger + A}{A} = \mathfrak{p}B.$$

Clearly $\mathfrak{r}$ kills $(\mathfrak{r}:\mathfrak{r})$, so

$$\frac{(\mathfrak{r}:\mathfrak{r})}{A} \subset \mathfrak{p}B \cap B[\mathfrak{r}] = (\mathfrak{p}B)[\mathfrak{r}].$$

Sketch of proof of "$\supset$": Assume for simplicity that A is local with maximal ideal $\mathfrak{r} = \mathfrak{m}$.

<u>*Case 1*</u>: $A \neq \widetilde{A}$. We have the inclusions

$$\mathfrak{p}B[\mathfrak{m}] \subset B[\mathfrak{m}] \subset \frac{(A:\mathfrak{m})}{A} = \frac{(\mathfrak{m}:\mathfrak{m})}{A},$$

of which only the last equality requires an explanation. We have that

$$\mathfrak{m} \subset (A:\mathfrak{m}) \cdot \mathfrak{m} \subsetneq A,$$

where the last inclusion is strict because $\mathfrak{m}$ is not invertible (if it were, A would be a dvr, hence $A = \widetilde{A}$). The first inclusion must then be an equality, so $\mathfrak{m} = (A:\mathfrak{m}) \cdot \mathfrak{m}$, yielding $(A:\mathfrak{m}) \subset (\mathfrak{m}:\mathfrak{m})$.

<u>*Case 2*</u>: $A = \widetilde{A}$. Since A doesn't kill itself, $A \not\subset \mathfrak{p}A^\dagger$, thus $\mathfrak{p}A^\dagger \subset A$ (A is a dvr, so the fractional ideals in $\mathrm{frac}(A)$ are totally ordered) and therefore $\mathfrak{p}B = 0$. $\square$

Recall from Michiel's talk (Theorems 4.12 and 4.14) that

- B anisotropic $\iff$ $\mathrm{lr}(B)$ is the only submodule $L \subset B$ satisfying $\mathfrak{p}L^\perp \subset L \subset L^\perp$.
- B is quasi-anisotropic $\iff$ for all $L \subset \mathrm{lr}(B)$ we have

$$\mathrm{lr}(L^\perp/L) = \mathrm{lr}(B)/L.$$

Proof of (€). Consider $L = \widetilde{A}/A$. Clearly $L^\perp = \widetilde{A}^\dagger/A$, and $\widetilde{A}^\dagger \supset \widetilde{A}$ because $\left\langle \widetilde{A}, \widetilde{A} \right\rangle \subset R$. The picture of the inclusions is as follows:

$$\begin{array}{cc} A^\dagger & B \\ | & | \\ \widetilde{A}^\dagger & L^\perp \\ | & | \\ \widetilde{A} & L \\ | & | \\ A & \{0\} \end{array}$$

It follows that $L \subset L^\perp$, so in order to prove that $L = \mathrm{lr}(B)$ it suffices (by the anisotropy assumption on B) to show that $\mathfrak{p}L^\perp \subset L$. But this follows from remark (3) preceding the proof of \$: apply the remark to $\widetilde{A}$ which is tame over R to get that $\mathfrak{p}B_{\widetilde{A}} = \mathfrak{p}\widetilde{A}^\dagger/\widetilde{A} = 0$, i.e.

$$\mathfrak{p}\widetilde{A}^\dagger \subset \widetilde{A} \iff \mathfrak{p}L^\perp \subset L.$$

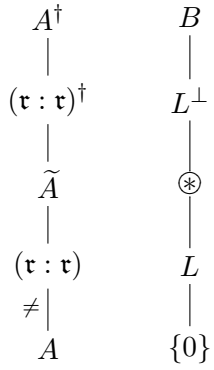
□

Proof of (£). We prove the theorem by induction on $\mathrm{length}_R(\widetilde{A}/A)$.

If $A = \widetilde{A}$, since A is tame over R, (3) shows that $\mathfrak{p}B = 0$ which yields $\mathrm{lr}(B) = 0$.

Suppose now $A \neq \widetilde{A}$, and take $L = (\mathfrak{r} : \mathfrak{r})/A$. By (1), $A \subsetneq (\mathfrak{r} : \mathfrak{r})$, or equivalently

$L \neq 0$. We have towers of inclusions



and we'd like to show that $\circledast$ is $\mathrm{lr}(B)$. By induction, we have

$$\circledast/L = \mathrm{lr}(L^\perp/L) = \widetilde{A}/(\mathfrak{r} : \mathfrak{r}),$$

thus

$$L = (\mathfrak{r} : \mathfrak{r})/A \overset{\$}{=} (\mathfrak{p}B)[\mathfrak{r}] \subset (\mathfrak{p}B)[\mathfrak{p}] \subset \mathrm{lr}(B).$$

Using now that B is quasi-anisotropic, we get that

$$\mathrm{lr}(L^\perp/L) = \mathrm{lr}(B)/L,$$

hence $\circledast = \mathrm{lr}(B)$, as desired. □

10 Construction of Valuations

(talk by David Eisenbud)

References: [McL36, McL36b]

Throughout this talk K will be a field, and for a given (non-archimedian) valuation v of K we shall denote by $\mathcal{O}_v$ and $\mathbb{F}_v$ its ring of integers and residue-class field respectively.

Goal: Construct the valuations on $K[x]$ from those on K. In particular, we'll be interested in the case when all non-archimedean valuations on K are discrete.

Given a valuation W on $K[x]$ with $W(x) \geq 0$, we let $v = W|_K$, so that $\mathcal{O}_W \supset \mathcal{O}_v[x]$.

Definition 10.1. A *key polynomial* $\phi \in \mathcal{O}_v[x]$ and *value* $\mu \in \mathbb{R}$ of W is a pair (ϕ, μ) such that

1. ϕ is monic, of positive degree.

2. $\mathrm{in}_W(\phi)$ is a prime or unit of $\mathrm{gr}_W\mathcal{O}_v[x]$, where the associated graded ring is taken with respect to the filtration on $\mathcal{O}_v[x]$ induced by W.

   In Mac Lane's terminology (2) translates into

(2') ϕ is *equivalence-irreducible* with respect to W. More precisely, one introduces an equivalence relation on poylnomials by saying that $f, g \in \mathcal{O}_v[x]$ are equivalent ($f \sim g$) with respect to W if $v(f) = v(g) < v(f-g)$. One says that a polynomial ϕ *equivalence-divides* f and write $\phi \underset{W}{\mid} f$ if $f \sim \phi\psi$ for some ψ.

3. ϕ is *minimal*, i.e. if $\mathrm{in}(\phi)|\mathrm{in}(g)$ for some $g \in \mathcal{O}_v[x] \setminus \{0\}$, then $\deg_x(g) \geq \deg_x(\phi)$ (here $\deg_x$ denotes the degree of a polynomial with respect to x; from now on, we shall write deg for $\deg_x$).

4. $\mu > W(\phi)$.

Remark 10.2. One should think of $W(\phi) - \mu$ as the negative slope occuring in the *Montes-Nart* setting.

Example 10.3. Consider $W = v_1$, where v_1 is given by

$$v_1(g(x)) = \min_i\{v(g_i)\}, \text{ for } g = \sum g_i x^i.$$

We have

$$\mathrm{gr}_{v_1}\mathcal{O}_v[x] = (\mathrm{gr}_v\mathcal{O}_v)[x] = \mathbb{F}_v[\pi][x],$$

a polynomial ring in two variables. $(x, 1)$ is a key pair of W.

We construct an extension $V = (W, (\phi, \mu))$ as follows. For $g(x) \in \mathcal{O}_v[x]$, write

$$g = \sum_{i=0}^{n} a_i \phi^i, \quad \deg(a_i) < \deg(\phi),$$

and define

$$V(g) = \min_i\{W(a_i) + i\mu\}.$$

Proposition 10.4. *1. V is a valuation.*

2. $V(g) \geq W(g)$ with equality if and only if g is not equivalence-divisible by ϕ ($\phi \underset{W}{\nmid} g$).

Definition 10.5. An *inductive valuation* is a (possibly infinte) sequence of valuations which we think of as a sequence $V = (v, (\phi_1, \mu_1), (\phi_2, \mu_2), \cdots)$, where each truncation $V_i = (v, (\phi_1, \mu_1), \cdots, (\phi_i, \mu_i))$ represents a valuation which is obtained from V_{i-1} and the V_{i-1}-key pair (ϕ_i, μ_i) via the procedure described above.

Consider a valuation V_∞ on $K[x]$, with values in $\mathbb{Q} \cup \infty$ (we allow V_∞ to take the value ∞ at non-zero polynomials). We assume that $V_\infty(x) \geq 0$ and let $v = V_\infty|_K$.

We define v_1 as above ($v_1(g) = \min_i(v(g_i))$) and consider ϕ_1 a monic polynomial of lowest degree with the property that

$$\mu_1 := V_\infty(\phi_1) \neq v_1(\phi_1).$$

Proposition 10.6. *(ϕ_1, μ_1) is a key pair for v_1.*

We construct $V_1 = (v_1, (\phi_1, \mu_1))$ and define recursevely key pairs (ϕ_i, μ_i) and valuations V_i via the same procedure: ϕ_i is minimal with the property

$$\mu_i := V_\infty(\phi_i) \neq V_{i-1}(\phi_i)$$

and $V_i = (V_{i-1}, (\phi_i, \mu_i))$.

Theorem 10.7. *The sequence of valuations $(V_i)_{i \geq 1}$ converges to V_∞.*

Our central example is the following:

Example 10.8. $K \subset L = K(\theta)$ is a finite field extension and $G(x) \in K[x]$ is the minimal polynomial of θ. Then valuations on L correspond to valuations on $K[x]$ with $v(G(x)) = \infty$.

Consider then a valuation V_∞ on L corresponding to a valuation on $K[x]$ (which we also denote by V_∞) with $V_\infty(G(x)) = \infty$, and run the previously described procedure for approximating it. At each stage we construct a new key pair (ϕ_i, μ_i), $\deg(\phi_{i-1}) \leq \deg(\phi_i)$. Eventually the degrees of ϕ_i stabilize to $\deg(G)$, and if we consider the ϕ_i–expansion of G:

$$G = \sum_j a_j \phi_i^j, \text{ with } \deg(a_j) < \deg(\phi_i),$$

then the minimum of the values $V_\infty(a_0), V_\infty(a_1\phi_i), \cdots$ is attained only at two consecutive terms. In this case G is a key polynomial and we can take $(\phi_{i+1}, \mu_{i+1}) = (G, \infty)$, which determines V_∞.

11 S_2-ification

(talk by Anurag Singh)

11.1 A characterization of normality

Definition 11.1. Let R be a Noetherian domain. R is said to be *normal* if the following equivalent conditions hold:

1. R is integrally closed in $\mathrm{frac}(R)$.
2. R is an intersection of discrete valuation rings.
3. $\begin{cases} R_1 : R_{\mathfrak{p}} \text{ is a dvr for each height one prime } \mathfrak{p}. \\ S_2 : \text{Every associated prime of a non-zero principal ideal has height one.} \end{cases}$

Example 11.2. Let K be a field, $R = K[s^4, s^3t, st^3, t^4] \subset K[s,t]$. If $\mathfrak{p}$ is a height 1 prime, one of s^4, t^4 must lie outside $\mathfrak{p}$, say $t^4 \notin \mathfrak{p}$. We get that $R_{\mathfrak{p}} = K[t^4, \frac{s}{t}]_{\mathfrak{p}}$ is a localization of a polynomial ring, hence regular. Therefore R has (R_1) but is not normal:

$$s^2t^2 = \frac{(s^3t)^2}{s^4} \in \mathrm{frac}(R) \setminus R, \text{ and it is a root of } T^2 - s^4t^4.$$

A presentation of R is given by

$$R \simeq K[w,x,y,z]/(wz - xy, x^3 - yw^2, y^3 - xz^2, wy^2 - x^2z),$$

with (w,x,y,z) mapping to (s^4, s^3t, st^3, t^4). The primary decomposition of the ideal $(x) \subset R$ is

$$(x) = (w, x^2) \cap (z, w)$$

where

$$\sqrt{(w,x^2)} = (w,x,y) \text{ has height 1, while } \sqrt{z,w} = (z,w,x,y) \text{ has height 2,}$$

so S_2 fails.

Note that $wy^2 = x^2z$, so

$$\frac{x^2}{w} = \frac{y^2}{z} (= s^2t^2).$$

Since $\frac{x}{w} \cdot \frac{y}{z} = 1$, any valuation ring containing R also contains one of x/w, y/z, hence also s^2t^2. So we see that, at least in this case, the integral closure of R is contained in the intersection of the dvrs containing R.

Definition 11.3. A collection $x_1, \cdots, x_m$ of elements of R form a *regular sequence* on a module M if the following conditions hold:

- $(x_1, \cdots, x_m)M \neq M$.
- x_1 is a non-zero-divisor on M and for $k = 2, \cdots, m-1$, x_{k+1} is a non-zero-divisor on $M/(x_1, \cdots, x_k)M$.

Let M be a finitely generated module over a local Noetherian ring $(R, \mathfrak{m})$. We define the *depth* of M by

$$\text{depth}(M) = \sup\{d : \exists x_1, \cdots, x_d \in \mathfrak{m} \text{ forming a regular sequence on M}\}.$$

We have that

$$\text{depth}(M) \leq \dim(M) = \dim(R/\text{ann } M).$$

Definition 11.4. For a Noetherian ring R, we say that M has the property S_i if for all $\mathfrak{p} \in \text{Spec}(R)$

$$\text{depth}_{M_\mathfrak{p}} \geq \min\{i, \dim(M_\mathfrak{p})\}.$$

Suppose now that R is a local ring of dimension 2, with $w, z \in R$ two elements generating an ideal of height 2. Then we have

$$w, z \text{ is a regular sequence on } R \iff \begin{cases} w \text{ is a non-zero-divisor on } R, \\ z \text{ is a non-zero-divisor on } R/(w). \end{cases}$$

The condition that z is not a zero-divisor on $R/(w)$ is equivalent to the following: if $\alpha z \in wR$ for some $\alpha \in R$ then $\alpha \in wR$. In example 11.2 we had $x^2 z \in wR$, but $x^2 \notin wR$, so z, w did not form a regular sequence.

We have the following

Proposition 11.5. *A Noetherian domain R has the S_2 property if and only if for every non-zero $a \in R$, and for every $\mathfrak{p} \in ass(R/a)$, the height of $\mathfrak{p}$ is equal to* 1.

11.2 S_2-ification

Suppose that R is a ring which is a finitely generated module over a Gorenstein ring $A \subset R$. We set

$$\omega = \text{Hom}_A(R, A)$$

the *canonical module* of R. This does not depend on the choice of A! (More generally, if S is Gorenstein and R an S-algebra which is a finite module over the image of S in R, then we define the canonical module by

$$\omega = \mathrm{Ext}^n_S(R, S)$$

where $n = \dim(S) - \dim(R)$.)

Fact: $\omega = \mathrm{Hom}_A(R, A) = R^*$ is S_2 (as is the dual $M^* = \mathrm{Hom}_S(M, S)$ of any module M over an S_2-ring S). Moreover,

$$\mathrm{Hom}_R(\omega, \omega) \simeq R^{**} \text{ is also } S_2.$$

The natural map

$$R \to \mathrm{Hom}_A(\omega, \omega)$$

is called the S_2-*ification* of R. This is universal, in the sense that any finite birational map of R to an S_2-ring factors through the S_2-ification.

Note: S_2-ification doesn't change the property of being R_1!

12 Invertibility of Fractional Ideals

(talk by David Eisenbud and Hendrik Lenstra)

12.1 The one-dimensional case (HL)

Let R be a one-dimensional Noetherian domain with field of fractions K, and let $J \subset K$ a *fractional R-ideal*, i.e. a non-zero finitely generated R-submodule of K. We say that J is *invertible* if there exists some fractional ideal I with the property that $IJ = R$. If J is invertible, then $(J : J) = R$ (since for any x with $xJ \subset J$, $xIJ = xR \subset IJ = R$). We have the following characterization of invertible ideals:

Theorem 12.1. *J is an invertible ideal if and only if $(R : J) : (R : J) = R$.*

Proof. "⇒" If J is invertible then $(R : J)$ is also invertible, and the remark preceding the theorem shows that $(R : J) : (R : J) = R$.

"⇐" The question is local, so we may assume that R is local with maximal ideal $\mathfrak{m}$. We claim that $(R : \mathfrak{m}) \supsetneq R$. To see this, take $0 \neq a \in \mathfrak{m}$. The ideal $\mathfrak{m}$ is nilpotent modulo a, say with order of nilpotence k. Let $x \in \mathfrak{m}^{k-1} \setminus Ra$. This is clearly contained in $(Ra : \mathfrak{m})$, so we have $(Ra : \mathfrak{m}) \supsetneq Ra$, and dividing by a proves our claim.

Suppose now that J is not invertible. Then $J \cdot (R : J) \subsetneq R$, so $J \cdot (R : J) \subset \mathfrak{m}$. This shows that

$$(R : J) : (R : J) = R : (J \cdot (R : J)) \supset (R : \mathfrak{m}) \supsetneq R,$$

as desired. □

12.2 The higher-dimensional case (DE)

Let R be a noetherian local domain, and $I \subset R$ a non-zero ideal. We have the following equivalences:

$$I^{-1} \supsetneq R \Longleftrightarrow \mathrm{Ext}^1_R(R/I, R) \neq 0 \Longleftrightarrow \mathrm{depth}(I) = 1,$$

where the latter is a well-known characterization of depth and the former follows by applying $\mathrm{Hom}(-, R)$ to the exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0.$$

One gets

$$0 = \mathrm{Hom}(R/I, R) \longrightarrow R \longrightarrow I^{-1} = \mathrm{Hom}(I, R) \longrightarrow \mathrm{Ext}^1(R/I, R) \longrightarrow 0 = \mathrm{Ext}^1(R, R),$$

so indeed $R \subsetneq I^{-1}$ if and only if $\mathrm{Ext}^1(R/I, R) \neq 0$.

We have the following

Proposition 12.2. *Let R be an S_2-domain, and $J \subset frac(R)$ a fractional ideal. Then the following are equivalent*

1. *$J_{\mathfrak{p}}$ is invertible for all $\mathfrak{p} \subset R$ prime ideal such that $R_{\mathfrak{p}}$ has depth 1 (or equivalently, codimension 1).*
2. *$(J^{-1} : J^{-1}) = R$.*

Proof. (1) ⇒ (2) : (1) together with Theorem 12.1 show that $R \subset (J^{-1} : J^{-1})$ coincide in codimension 1. But since R is S_2, $J^{-1} = \mathrm{Hom}_R(J, R)$ is also S_2, thus $(J^{-1} : J^{-1}) = \mathrm{Hom}_R(J^{-1}, J^{-1})$ is S_2 as well. Now sections of S_2-modules extend uniquely in codimension 2, so we must have $(J^{-1} : J^{-1}) = R$. (more formally, suppose there exists a minimal prime $\mathfrak{p}$ in the support of $(J^{-1} : J^{-1})/R$ and write down an exact sequence

$$0 \longrightarrow R_{\mathfrak{p}} \longrightarrow (J^{-1} : J^{-1})_{\mathfrak{p}} \longrightarrow Q \longrightarrow 0,$$

with Q an $R_{\mathfrak{p}}$ module of finite length. The long exact sequence in local cohomology shows that $(Q =) H^0_{\mathfrak{p}}(Q) = 0$, contradicting the choice of $\mathfrak{p}$.)

(2) ⇒ (1) : This follows from Theorem 12.1, since everything commutes with localization. □

Chapter 2

Okutsu-Montes Representations of Prime Ideals of One-Dimensional Integral Closures

Introduction

In 1923, Øystein Ore found a method to construct the prime ideals of a number field, dividing a given prime number p, in terms of a defining equation $f(x) \in \mathbf{Z}[x]$, provided that this equation satisfies certain *p-regularity* condition [Ore23]. The idea was to detect first a p-adic factorization of $f(x)$ according to the sides of certain Newton polygon $N(f)$, and then, to detect a further factorization of each of these factors according to the different irreducible polynomials that divide certain residual polynomials $R_\lambda(f)$ with coefficients in a finite field, for λ running on the slopes of the different sides of $N(f)$.

He raised then the question of the existence of an iterative procedure to compute the prime ideals in the p-irregular case, based on the consideration of similar Newton polygons $N_i(f)$ and residual polynomials $R_{\lambda,i}(f)$ of *higher order* $i \geq 1$.

Saunders MacLane attacked this problem in 1936 from the point of view of valuations. Given any discrete valuation v on a field k, he parametrized all discrete valuations of the rational function field $k(x)$ that extend v. Then, given an irreducible polynomial $f(x) \in k[x]$, he characterized all valuations of the field $k[x]/(f(x))$ that extend v, as limits of infinite families of valuations of $k[x]$ whose value on $f(x)$ grows to infinity. Finally, he gave a criterion to decide when a valuation of $k[x]$ was sufficiently close to a valuation of $k[x]/(f(x))$, to uniquely represent it [McL36, McL36b].

In 1999, Jesús Montes developed an algorithm that carries out Ore's program [Mon99]. The algorithm follows MacLane's pattern, but the introduction of the right concept of residual polynomial of higher order makes the whole theory constructive and well adapted to computational applications. The algorithm is highly recursive: each computation in order i requires auxiliary computations in all previous orders $1, \dots, i-1$. This led Montes, for purely computational reasons, to optimize the algorithm so that it does not work at certain order i until this is absolutely unavoidable; it turns out that the optimized algorithm has an output with unexpected canonical properties, linked to invariants of extensions of local fields that had been studied by Kousaku Okutsu in 1982 [Oku82].

Therefore, the algorithm of Montes computes what we call *Okutsu-Montes representations* of prime ideals of one-dimensional integral closures. These computational representations single out the prime ideals and they carry on essential data of the corresponding extensions of local fields. Moreover, these objects have proved to be an efficient and malleable tool for a computational resolution of several arithmetic tasks concerning prime ideals.

In this survey notes I explain the structure of Montes algorithm and describe some of its applications, with special emphasis on the computation of integral closures. Most of this material is joint work with Jordi Guàrdia and Jesús Montes. This survey grew out from the notes of a seminar delivered at the MSRI in Berkeley, California, as part of the workshop *Computation of integral closures*, that took place during the week of 26th to 30th of july 2010. We thank the organizer, David Eisenbud, for giving us the opportunity to present these results, and the participants for the charming atmosphere and the fruitful exchange of ideas that contributed to a substantial improvement of the final write up.

1 Overview

1.1 Local fields

Let K be a local field with perfect residue class field. Let $\mathcal{O}$ be its ring of integers, $\mathfrak{m}$ the maximal ideal, $\pi \in \mathfrak{m}$ a generator of $\mathfrak{m}$, and $v\colon \overline{K}^* \longrightarrow \mathbf{Q}$, the canonical extension of the discrete valuation of K to an algebraic closure, normalized by $v(K^*) = \mathbf{Z}$. Let $K^{\mathrm{sep}} \subseteq \overline{K}$ be the separable closure of K in $\overline{K}$.

Montes algorithm. [HN08, GMN08]

Input: A monic separable polynomial $f(x) \in \mathcal{O}[x]$.

Output: A family $\mathbf{t}_1, \dots, \mathbf{t}_g$ of *f-complete and optimal types*, parameterizing the monic irreducible factors $F_1(x), \dots, F_g(x)$ of $f(x)$ in $\mathcal{O}[x]$.

For local fields with finite residue class field, there have been recent estimations for the complexity of this algorithm by Veres [Ver09], Ford-Veres [FV10], and Pauli [Pau10]. The finer estimation is $O(n^{2+\epsilon}\delta^{2+\epsilon})$ bit operations, where $\delta = v(\mathrm{disc}(f))$.

Let $F(x)$ be one of these irreducible factors, $\theta \in K^{\mathrm{sep}}$ a root of F, $L = K(\theta)$ the corresponding finite separable extension of K, and $\mathcal{O}_L$ its ring of integers.

Let $\mathbf{t}$ be the type corresponding to F. For simplicity, we represent

$$\mathbf{t} = [\phi_1, \ldots, \phi_{r+1}]$$

as a sequence of monic irreducible separable polynomials in $\mathcal{O}[x]$ satisfying certain technical conditions. Among them let us just mention that

$$\deg \phi_1 \mid \cdots \mid \deg \phi_r \mid \deg \phi_{r+1} = \deg F, \qquad \deg \phi_1 < \cdots < \deg \phi_r.$$

It turns out that the polynomial $\phi_{r+1}(x)$ is an *Okutsu approximation* to $F(x)$, so that it is sufficiently close to $F(x)$ for certain purposes (see section 3). Thus, Montes algorithm is a kind of polynomial factorization algorithm. Actually, a rather peculiar one, in two senses:

1. It is based on a series of generalizations of Hensel lemma, so that successive factorizations of $f(x)$ are *detected*, but never carried out. Only certain auxiliary polynomials over finite extensions of the residue class field are factorized.

2. Besides computing an approximation to each irreducible factor F, the output of the algorithm provides as well a lot of arithmetic information about the finite extension L/K determined by F.

The type $\mathbf{t}$ is structured in $r+1$ *levels*, and r is called the *order* of $\mathbf{t}$. At each level i, $\mathbf{t}$ stores several combinatorial and arithmetic invariants

$$e_i,\ f_i,\ h_i,\ \lambda_i,\ \rho_i,\ \text{etc.}$$

linked to Newton polygons of higher order of $f(x)$. Let us briefly mention some properties of L/K determined by these invariants.

$$v(\phi_i(\theta)) = \frac{|\lambda_i| + \rho_i}{e_1 \cdots e_{i-1}}.$$

$$e(L/K) = e_1 \cdots e_r, \quad f(L/K) = f_0 f_1 \cdots f_r. \tag{2.1}$$

$$\exp(F) = \sum_{i=1}^{r} (e_i f_i \cdots e_r f_r - 1) \frac{h_i}{e_1 \cdots e_i},$$

where $\exp(F)$ is the *exponent* of F; that is, the least positive integer such that $\pi^{\exp(F)}\mathcal{O}_L \subseteq \mathcal{O}[\theta]$.

The type $\mathbf{t}$ determines as well an easy computation of the integral closure of $\mathcal{O}$ inside L. In fact, let $n = \deg F = [L\colon K]$; then, for each integer $0 \leq m < n$, we express m in a unique way as:

$$m = j_0 + j_1 \deg \phi_1 + \cdots + j_r \deg \phi_r, \quad 0 \leq j_i < (\deg \phi_{i+1}/\deg \phi_i),$$

where $\phi_0(x) := x$, and we consider the following polynomial of degree m:

$$g_m(x) := \phi_0(x)^{j_0}\phi_1(x)^{j_1}\cdots\phi_r(x)^{j_r}. \tag{2.2}$$

As shown above, the data of $\mathbf{t}$ allow us to compute

$$\nu_m := \lfloor j_1 v(\phi_1(\theta)) + \cdots + j_r v(\phi_r(\theta)) \rfloor.$$

Then, the following family is an $\mathcal{O}$-basis of $\mathcal{O}_L$:

$$1, \frac{g_1(\theta)}{\pi^{\nu_1}}, \ldots, \frac{g_{n-1}(\theta)}{\pi^{\nu_{n-1}}}.$$

Thus, we may say that Montes algorithm provides the computation of all the integral closures of $\mathcal{O}$ in the different extensions determined by the irreducible factors of the input polynomial $f(x)$, almost as a by-product. We need only to include in the algorithm an efficient computation of the polynomials $g_m(x)$ [1].

1.2 Applications to global fields

Let us illustrate the applications to number fields. For function fields of curves the results are completely analogous, but no implementation has been made yet.

Let $K = \mathbf{Q}[x]/(f(x))$ be now the number field defined by a monic irreducible polynomial $f(x)$ with integer coefficients and degree n. Let $\theta \in \overline{\mathbf{Q}}$ be a root of $f(x)$ and $\mathbf{Z}_K$ the ring of integers.

For any prime number p, the prime ideals of K dividing p are in one-to-one correspondence with the monic irreducible factors of $f(x)$ over $\mathbf{Z}_p[x]$. In fact, such a prime ideal determines a topological embedding $\iota_{\mathfrak{p}}\colon K \hookrightarrow K_{\mathfrak{p}} \hookrightarrow \overline{\mathbf{Q}}_p$, and the corresponding irreducible factor $F_{\mathfrak{p}}$ is the minimal polynomial of $\iota_{\mathfrak{p}}(\theta)$ over $\mathbf{Q}_p$.

[1] The polynomials ϕ_i are shared by different types. Thus, some of the partial products of (2.2) need to be computed as long as the ϕ_i are constructed, in order to avoid the repetition of these multiplications.

Hence, by applying Montes algorithm to $f(x)$ over $\mathbf{Z}_p$, one obtains what we call an *Okutsu-Montes representation* (OM representation) of all prime ideals of K dividing p:

$$\mathfrak{p} = [p; \phi_1, \ldots, \phi_r; \phi_{\mathfrak{p}}], \text{ where } \phi_{\mathfrak{p}} := \phi_{r+1}.$$

The polynomials ϕ_i have all integer coefficients. It turns out that all invariants contained in the corresponding type $\mathbf{t}$ are the essential data that is necessary for a computational treatment of the prime ideal. For instance, the following tasks in the group of fractional ideals can be based on the data (and operators) of the OM representations:

1. Compute the $\mathfrak{p}$-adic valuation, $v_{\mathfrak{p}}\colon K^* \longrightarrow \mathbf{Z}$.
2. Compute the prime ideal factorization of a fractional ideal.
3. Compute a two-element representation of a fractional ideal.
4. Add, multiply and invert fractional ideals.
5. Compute the reduction map, $\mathbf{Z}_K \longrightarrow \mathbf{Z}_K/\mathfrak{p}$, and a section of this map (a lifting map).
6. Solve Chinese remainder problems.
7. Compute a p-integral basis of K.

We have implemented a '+Ideals' package in Magma that contains routines for all these tasks [GMN10],[GMN10b].

Recall that a p-integral basis is a $\mathbf{Q}$-basis of K, made of integral elements $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}_K$, that satisfy any of the following equivalent conditions:

(a) $\alpha_1 \otimes 1, \ldots, \alpha_n \otimes 1$ are a $\mathbf{Z}_p$-basis of $\mathbf{Z}_K \otimes_{\mathbf{Z}} \mathbf{Z}_p$.

(b) $\alpha_1 \otimes 1, \ldots, \alpha_n \otimes 1$ are an $\mathbb{F}_p$-basis of $\mathbf{Z}_K \otimes_{\mathbf{Z}} \mathbb{F}_p$.

(c) p does not divide the index $(\mathbf{Z}_K\colon \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbf{Z}})$.

Since $\mathbf{Z}_K \otimes_{\mathbf{Z}} \mathbb{F}_p$ has dimension n as an $\mathbb{F}_p$-vector space, in practice it suffices to check that $\alpha_1, \ldots, \alpha_n$ determine $\mathbb{F}_p$-linearly independent elements in this $\mathbb{F}_p$-algebra.

It is well-known how to compute a p-integral basis of K from the local $\mathbf{Z}_p$-bases of all local rings $\mathbf{Z}_{K_{\mathfrak{p}}}$, for $\mathfrak{p}|p$. One needs only to compute multipliers $b_{\mathfrak{p}} \in \mathbf{Z}_K$ satisfying:

$$v_{\mathfrak{p}}(b_{\mathfrak{p}}) = 0, \quad v_{\mathfrak{q}}(b_{\mathfrak{p}}) \geq (\exp(F_{\mathfrak{p}}) + 1)e(\mathfrak{q}/p), \ \forall, \mathfrak{q}|p, \ \mathfrak{q} \neq \mathfrak{p}.$$

These multipliers can be easily computed from the data of the OM representations. If $\{\mathcal{B}_\mathfrak{p}\}_{\mathfrak{p}|p}$ are the local bases, then $\bigcup_{\mathfrak{p}|p} b_\mathfrak{p}\mathcal{B}_\mathfrak{p}$ is a p-integral basis of K.

Finally, an integral basis of K (a $\mathbf{Z}$-basis of $\mathbf{Z}_K$) can be computed as follows:

1. Factorize the discriminant $\mathrm{disc}(f)$.
2. For each prime $p|\,\mathrm{disc}(f)$, compute a p-integral basis of K in Hermite Normal Form.
3. Glue these data into a global basis by a simple application of the CRT.

1.3 Some remarks

1. The standard packages that manipulate number fields need to compute an integral basis as a preliminary step. This makes them totally useless for many number fields of large degree, or number fields defined by an equation with large coefficients, because of the impossibility to factorize the discriminant.

The routines based on the OM representations of the prime ideals do not require the factorization of $\mathrm{disc}(f)$ and they work very efficiently for "big" number fields [GMN10b][2].

Of course, the bottleneck is again integer factorization: we can deal only with fractional ideals whose norm may be factorized.

2. The routines based on the OM representations have a completely different nature than the classical ones. It often occurs, when dealing with some problem, that once a direct connexion with the data contained in the OM representations is found, the outcoming routine is much faster than the routine that would be inspired in the classical ones.

3. We do not know how to test if an ideal is principal. To this end it would be necessary to combine the OM representations with some kind of LLL reduction routine (preferably not based on the lattice $\mathbf{Z}_K$).

Question. Is there a theoretical reason that makes it hopeless to design such a test without factorizing the discriminant?

[2]We do not claim too much originality on this fact. Many researchers who need to work with number fields of large degree develop their own routines to deal with concrete problems, avoiding the computation of the maximal order. But we do claim on efficiency: our routines run extremely fast in practice.

4. Suppose the discriminant of the defining equation $f(x)$ may be factorized. Then, how do our routines behave with respect to the classical ones? Let us discuss this comparison at two levels.

1. The OM routines compute an integral basis much faster than the ordinary routines of Magma or Pari. We saw that the computation of the local bases is almost a by-product of Montes algorithm.

2. Once the maximal order of K has been computed, the OM routines still run (slightly) faster than the ordinary ones of Magma or Pari, for number fields whose degree is not too small (say $n \geq 16$). One reason for this is that the OM techniques avoid the use of linear algebra. The standard methods compute $\mathbf{Z}$-basis of the prime ideals, expressed in coordinates with respect to the integral basis. We get in this way $n \times n$ matrices, and the linear algebra procedures to manipulate them (like the computation of Hermite Normal Forms) dominate the complexity for n large.

5. Suppose the discriminant of the defining equation $f(x)$ may be factorized. We mentioned already that we also need the HNF routine to patch the different p-integral bases of K, for the primes p dividing $\mathrm{disc}(f)$, into a global integral basis. This routine is the bottleneck for the whole process, if n is large.

2 The Algorithm of Ore, MacLane and Montes

Let K be a local field, $\mathcal{O}$ its ring of integers, $\mathfrak{m}$ the maximal ideal, $\pi \in \mathfrak{m}$ a generator of $\mathfrak{m}$, and $\mathbb{F}_0 = \mathcal{O}/\mathfrak{m}$ the residue class field, which is supposed to be perfect. Let $v\colon \overline{K}^* \longrightarrow \mathbf{Q}$ be the canonical extension to $\overline{K}$ of the discrete valuation of K, normalized by $v(K^*) = \mathbf{Z}$. Let $K^{\mathrm{sep}} \subseteq \overline{K}$ be the separable closure of K in $\overline{K}$.

We extend v to a discrete valuation v_1 of the field $K(x)$, by letting it act on $K[x]$ as follows:

$$v_1\left(\sum\nolimits_{0\leq s} a_s x^s\right) := \min\{v(a_s) \mid 0 \leq s\}.$$

Also, we consider the 0-th *residual operator*:

$$R_0\colon \mathcal{O}[x] \longrightarrow \mathbb{F}_0[y], \quad g(x) \mapsto R_0(g) := \overline{g(y)/\pi^{v_1(g)}}.$$

Note that for monic polynomials, R_0 is the ordinary reduction map.

Our aim is to describe the monic irreducible factors of a given monic separable polynomial $f(x) \in \mathcal{O}[x]$. The starting point of the algorithm is Hensel lemma. From a factorization

of $R_0(f)(y)$ into a product of monic irreducible polynomials in $\mathbb{F}_0[y]$:

$$R_0(f)(y) = \varphi_1(y)^{n_1} \cdots \varphi_k(y)^{n_k},$$

we detect (but not compute) a factorization of $f(x)$ in $\mathcal{O}[x]$: $f = F_1 \cdots F_k$, into a product of monic (not necessarily irreducible) polynomials satisfying $R_0(F_i)(y) = \varphi_i(y)^{n_i}$.

We start then to construct a *tree $\mathcal{T}$ of types*. Actually, $\mathcal{T}$ is the disjoint union of k connected trees, one for each irreducible factor of $R_0(f)$. The initial node of each connected tree is a *type of order zero*, which we are going to describe now.

Let us fix one of the irreducible factors of $R_0(f)$, that we denote from now on by $\psi_0(y) \in \mathbb{F}_0[y]$. The subindex 0 emphasizes that we are working *at order zero*. We choose (non-canonically) a monic lift $\phi_1(x) \in \mathcal{O}[x]$ of ψ_0 and we denote

$$\mathbf{t} := [\phi_1].$$

This object is the type of order zero that labels the initial node of the tree.

Let $F_{\mathbf{t}}(x) \in \mathcal{O}[x]$ be the (unknown) monic factor of $f(x)$ attached by Hensel lemma to ψ_0; recall that $R_0(F_{\mathbf{t}}) = \psi_0^{\ell_0}$, for certain integer $\ell_0 > 0$.

Our initial node, labelled by $\mathbf{t}$, is supposed to sprout several branches labelled by types of order one, obtained by adding a different polynomial ϕ_2 for each branch, in a process to be explained later in more detail. Clearly, if $\ell_0 = 1$ then $F_{\mathbf{t}}$ is already irreducible and the initial node is already a leave of the tree $\mathcal{T}$ (an end node that has no further branching).

A type of order zero supports certain invariants of the irreducible factors of $F_{\mathbf{t}}$:

$$\begin{aligned}
&\psi_0(y) \in \mathbb{F}_0[y],\\
&f_0 := \deg \psi_0,\\
&m_1 := \deg \phi_1 = f_0,\\
&\mathbb{F}_1 := \mathbb{F}_0[y]/(\psi_0(y)),\\
&z_0 := \text{ class of } y \text{ in } \mathbb{F}_1.
\end{aligned}$$

Note that $\psi_0(z_0) = 0$ and $\mathbb{F}_1 = \mathbb{F}_0[z_0]$. This seemingly innocuous object $\mathbf{t}$ has hidden powers. It determines a *Newton polygon operator* of the first order:

$$N_1 := N_{\phi_1, v_1} \colon \mathcal{O}[x] \longrightarrow 2^{\mathbf{R}^2},$$

and, for every negative rational number $\lambda \in \mathbf{Q}^-$, a *residual polynomial operator* of the first order:

$$R_{\lambda,1} := R_{\phi_1, v_1, \lambda} \colon \mathcal{O}[x] \longrightarrow \mathbb{F}_1[y].$$

Let us describe all these operators in some detail.

2.1 The Newton polygon operator

Any polynomial $g(x) \in \mathcal{O}[x]$ has a canonical ϕ_1-expansion:

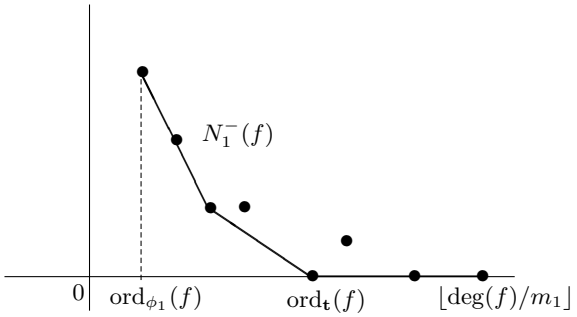
$$g(x) = \sum_{0 \le s} a_s(x)\phi_1(x)^s, \quad \deg a_s < m_1.$$

Then, $N_1(g)$ is the lower convex hull of the set of all points $(s, v_1(a_s))$ in $\mathbf{R}^2$. We are only interested in the *principal part* of this polygon, $N_1^-(g) \subseteq N_1(g)$, made of all sides with negative slope. The *length* $\ell(N)$ of a polygon N is, by definition, the length of its projection to the horizontal axis.

We denote:

$$\mathrm{ord}_{\mathfrak{t}}(g) := \mathrm{ord}_{\psi_0} R_0(g) = \ell(N_1^-(g)).$$

By construction, the type $\mathfrak{t}$ of order zero extracted from the factorization of $f(x)$ modulo $\mathfrak{m}$, had $\mathrm{ord}_{\mathfrak{t}}(f) = \ell_0 > 0$. Since our polynomial $f(x)$ is monic, the last point of $N_1(f)$ has ordinate zero. The typical shape of $N_1(f)$ is as shown below.



The polygon $N := N_1^-(f)$ has a *residual coefficient* c_s at each integer abscissa, $\mathrm{ord}_{\phi_1} f \le s \le \mathrm{ord}_{\mathfrak{t}}(f)$, defined as follows:

$$c_s := \begin{cases} 0, & \text{if } (s, v_1(a_s)) \text{ lies above } N, \\ R_0(a_s)(z_0) \in \mathbb{F}_1, & \text{if } (s, v_1(a_s)) \text{ lies on } N. \end{cases}$$

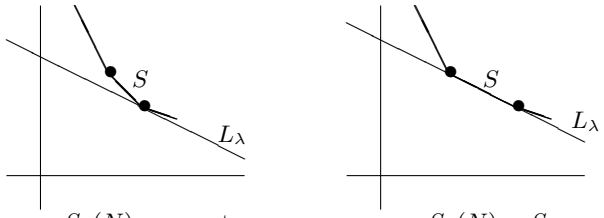
In the latter case, $c_s \neq 0$ because $\deg a_s < m_1 = f_0$.

2.2 The residual polynomial operators

We keep the notation $N = N_1^-(f)$. Denote by $\mathrm{Slopes}(N)$ the set of slopes of N. Given any $\lambda \in \mathbf{Q}^-$, we consider:

$$S_\lambda(N) := \{(x,y) \in N \mid y + x|\lambda| \text{ is minimal}\} = \begin{cases} \text{a vertex}, & \text{if } \lambda \notin \mathrm{Slopes}(N), \\ \text{a side}, & \text{if } \lambda \in \mathrm{Slopes}(N). \end{cases}$$

The following picture illustrates both possibilities. In this picture L_λ is the line of slope λ having first contact with N from below.

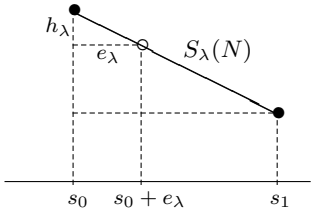


$S_\lambda(N) =$ a vertex $\qquad$ $S_\lambda(N) = S$

In any case, $S_\lambda(N)$ is a segment of $\mathbf{R}^2$ with end points having integer coordinates. Any such segment has a *degree*. If $\lambda = -h_\lambda/e_\lambda$ with h_λ, e_λ positive coprime integers, the degree of $S_\lambda(N)$ is defined as:

$$d := d(S_\lambda(N)) := \ell(S_\lambda(N))/e_\lambda.$$

Note that S_λ splits into d minimal subsegments whose end points have integer coordinates.



We define the *residual polynomial* of the first order of $f(x)$, with respect to λ, as:

$$R_{\lambda,1}(f)(y) := R_{\phi_1,v_1,\lambda}(f)(y) := c_{s_0} + c_{s_0+e_\lambda} y + \cdots + c_{s_1} y^d \in \mathbb{F}_1[y].$$

Note that $c_{s_0} c_{s_1} \neq 0$; thus, the degree of $R_{\lambda,1}(f)$ is always equal to d.

For any polynomial $g(x) \in \mathcal{O}[x]$ the definition of $R_{\lambda,1}(g)$ is completely analogous but taking $N = N_1^-(g)$.

2.3 Fundamental results of Ore

Theorem of the product. For any pair of polynomials $g(x), h(x) \in \mathcal{O}[x]$ and any $\lambda \in \mathbf{Q}^-$,

$$N_1^-(gh) = N_1^-(g) + N_1^-(h), \quad R_{\lambda,1}(gh) = R_{\lambda,1}(g)R_{\lambda,1}(h).$$

The sum of two polygons is the polygon obtained by taking as (left) starting point the sum of the two (left) starting points, and then joining to this starting point the sides of both polygons by increasingly ordered slopes.

Notation. Given a field $\mathcal{F}$ and two polynomials $\varphi(y), \psi(y) \in \mathcal{F}[y]$, we write $\varphi(y) \sim \psi(y)$ to indicate that there exists a constant $c \in \mathcal{F}^*$ such that $\varphi(y) = c\psi(y)$.

Theorem of the polygon. Let $f(x)$, ψ_0, $F_{\mathbf{t}}(x)$, N be as above. Then,

1. The polynomial $F_{\mathbf{t}}(x)$ factorizes in $\mathcal{O}[x]$ as:

   $$F_{\mathbf{t}}(x) = \prod\nolimits_{\lambda \in \mathrm{Slopes}(N)} F_\lambda(x),$$

   for some monic polynomials $F_\lambda(x) \in \mathcal{O}[x]$, whose Newton polygon $N_1(F_\lambda)$ is one-sided with slope λ, and $R_{\lambda,1}(F_\lambda) \sim R_{\lambda,1}(f)$.

2. For any root $\theta \in K^{\mathrm{sep}}$ of F_λ, we have $v(\phi_1(\theta)) = |\lambda|$.

Theorem of the residual polynomial. With the same notation, let $\lambda \in \mathrm{Slopes}(N)$ and let $R_{\lambda,1}(f)(y) = \prod_\psi \psi(y)^{\ell_\psi}$ be the factorization of $R_{\lambda,1}(f)$ into a product of monic irreducible polynomials in $\mathbb{F}_1[y]$. Then,

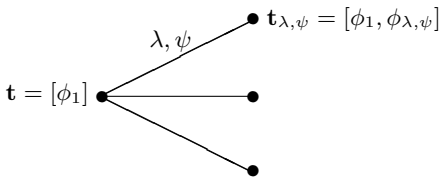
$$F_\lambda(x) = \prod\nolimits_\psi F_{\lambda,\psi}(x),$$

for some monic $F_{\lambda,\psi}(x) \in \mathcal{O}[x]$ such that $R_{\lambda,1}(F_{\lambda,\psi})(y) \sim \psi(y)^{\ell_\psi}$ in $\mathbb{F}_1[y]$.

This theorem is a kind of *Hensel lemma in order one*.

2.4 Branching of types

The theorems of Ore detect a (never computed) factorization of $F_{\mathbf{t}}$. The different (unknown) factors $F_{\lambda,\psi}$ are parameterized by certain *types of order one*. We can think that the node $\mathbf{t}$ sprouts several branches with end nodes labelled by types $\mathbf{t}_{\lambda,\psi} = [\phi_1, \phi_{\lambda,\psi}]$, where $\phi_{\lambda,\psi}(x) \in \mathcal{O}[x]$ is a monic separable polynomial of degree $m_{\lambda,\psi} := e_\lambda f_\psi m_1$, satisfying: $R_{\lambda,1}(\phi_{\lambda,\psi}) \sim \psi$. By the Theorem of the product, $\phi_{\lambda,\psi}$ is irreducible.



If $\ell_\psi = 1$, the Theorem of the product shows that $F_{\lambda,\psi}$ is irreducible, and the node $\mathbf{t}_{\lambda,\psi}$ becomes a leave of the tree of types. If $\ell_\psi > 1$ we need to analyze the node $\mathbf{t}_{\lambda,\psi}$ to detect further factorizations of $F_{\lambda,\psi}$, or show that it is irreducible.

By the Theorem of the product, all irreducible factors F of $F_{\lambda,\psi}$ satisfy:

$$\begin{aligned} &R_0(F)(y) = \psi_0(y)^{\ell_0(F)} \text{ in } \mathbb{F}_0[y], \\ &N_1(F) \text{ is one-sided with slope } \lambda, \\ &R_{\lambda,1}(F)(y) = \psi(y)^{\ell_1(F)} \text{ in } \mathbb{F}_1[y], \end{aligned}$$

for some positive integers $\ell_0(F)$, $\ell_1(F)$.

These properties motivate the use of the term *type*. A type is an object that collects some arithmetic features of irreducible polynomials. The polynomials that have these properties are of a certain "type". The last polynomial of a type is some sort of minimal object having these features; it is also called a *representative* of the type. Let us show how these representatives are constructed.

Construction of the polynomials $\phi_{\lambda,\psi}$

Let us denote for a while:

$$e := e_\lambda, \quad h := h_\lambda, \quad f := f_\psi.$$

Suppose that $\psi(y) = c_0 + c_1 y + \cdots + c_{f-1} y^{f-1} + y^f \in \mathbb{F}_1[y]$. The polynomial $\phi_{\lambda,\psi}(x)$ we are looking for must be of the form:

$$\pi^{hf} a_0(x) + \pi^{h(f-1)} a_e(x) \phi_1(x)^e + \cdots + \pi^{h(f-k)} a_{ek}(x) \phi_1(x)^{ek} + \cdots + \phi_1(x)^{ef},$$

with $R_0(a_{ek})(z_0) = c_k$, for all $0 \leq k < f$.

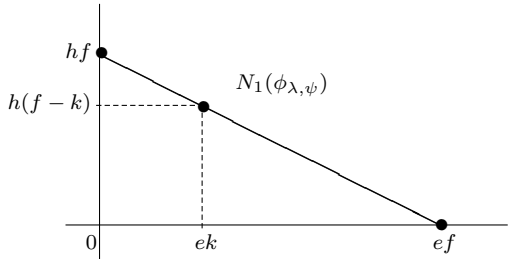
The condition on $a_{ek}(x)$ is easy to fulfill: if $c_k = 0$ we take $a_{ek}(x) = 0$, whereas for

$$c_k = u_0 + u_1 z_0 + \cdots + u_{f_0-1} z_0^{f_0-1} \in \mathbb{F}_1,$$

with $u_i \in \mathbb{F}_0$, we simply take arbitrary liftings of the u_i to $\mathcal{O}$ (which we denote by the same symbol $u_i \in \mathcal{O}$), and take

$$a_{ek}(x) = u_0 + u_1 x + \cdots + u_{f_0-1} x^{f_0-1} \in \mathcal{O}[x].$$

The Newton polygon of $\phi_{\lambda,\psi}$ is:



2.5 Types of order r

Definition. Let $r \geq 1$ be an integer, and $\mathbf{t} = [\phi_1, \ldots, \phi_{r+1}]$ a family of monic irreducible separable polynomials in $\mathcal{O}[x]$. We say that $\mathbf{t}$ is a *type of order* r if it satisfies the following properties:

1. $[\phi_1, \ldots, \phi_r]$ is a type of order $r - 1$.
2. $N_r(\phi_{r+1})$ is one-sided with negative slope (say) λ.
3. $R_{\lambda,r}(\phi_{r+1})(y) \in \mathbb{F}_r[y]$ is an irreducible polynomial.
4. $\deg \phi_r \mid \deg \phi_{r+1}$.

If $\mathbf{t}$ satisfies these conditions, we add two fundamental invariants at level r:

$$\begin{aligned}&\lambda_r := \text{ slope of } N_r(\phi_{r+1}),\\ &\psi_r(y) \in \mathbb{F}_r[y] \text{ monic such that } R_{\lambda_r,r}(\phi_{r+1}) \sim \psi_r,\end{aligned}$$

Convention. We shall denote from now on: $R_r := R_{\lambda_r,r}$.

Let us recall the subsequent invariants deduced from λ_r, ψ_r:

$$\begin{aligned}&\lambda_r = -h_r/e_r, \quad h_r,\, e_r \text{ positive coprime integers}\\ &f_r := \deg \psi_r,\\ &\mathbb{F}_{r+1} := \mathbb{F}_r[y]/(\psi_r(y)),\\ &z_r := \text{ class of } y \text{ in } \mathbb{F}_{r+1},\end{aligned}$$

so that $\psi_r(z_r) = 0$ and $\mathbb{F}_{r+1} = \mathbb{F}_r[z_r] = \mathbb{F}_0[z_0, \ldots, z_r]$.

In order to have a coherent definition, it is necessary to show that if $\mathbf{t}$ satisfies these properties, then $\mathbf{t}$ determines a Newton polygon operator of order $r+1$,

$$N_{r+1}\colon \mathcal{O}[x] \longrightarrow 2^{\mathbf{R}^2},$$

and residual polynomial operators of order $r+1$, for each $\lambda \in \mathbf{Q}^-$:

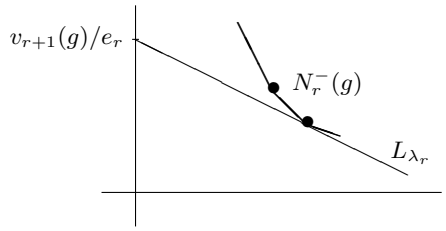
$$R_{\lambda,r+1}\colon \mathcal{O}[x] \longrightarrow \mathbb{F}_{r+1}[y],$$

satisfying analogous results to the three fundamental theorems of Ore.

The first (and essential) step is to construct a discrete valuation v_{r+1} of $K(x)$. Let us describe how it acts on polynomials. Given $g(x) \in K[x] \setminus \{0\}$, we compute $N := N_r^-(g)$ and we take any point $(x, y) \in N$ such that $y + x|\lambda_r|$ is minimal. Then, we define:

$$v_{r+1}(g) := e_r(y + x|\lambda_r|).$$

The following picture illustrates the situation. The line L_{λ_r} is the line of slope λ_r having first contact with N from below.



Note that v_{r+1} depends only on v_r, ϕ_r and λ_r. In MacLane's terminology, ϕ_r is a *key polynomial* over v_r and v_{r+1}/e_r is the *augmented valuation* attached to the pair $(\phi_r, v_r(\phi_r)+|\lambda|)$ [McL36, Sec.4]

Once we have the discrete valuation v_{r+1}, we can define a Newton polygon operator of order $r+1$ as before. If $g(x) = \sum_{0\leq s} a_s(x)\phi_{r+1}(x)^s$ is the ϕ_{r+1}-expansion of a polynomial $g(x)$, then $N_{r+1}(g) := N_{\phi_{r+1},v_{r+1}}(g)$ is defined as the lower convex hull of the set of points (s, u_s), where $u_s := v_{r+1}(a_s\phi_{r+1}^s)$.

Note that the ordinate of the points incorporates $v_{r+1}(\phi_{r+1}^s)$, which is a positive integer. This is necessary to keep the property:

$$\ell(N_{r+1}^-(g)) = \mathrm{ord}_{\psi_r}(R_r(g)).$$

In order one (for $r=0$), we had $v_1(\phi_1) = 0$, because ϕ_1 is monic; thus, the definition of N_1 is coherent with the general definition of the Newton polygons N_r for all $r \geq 1$.

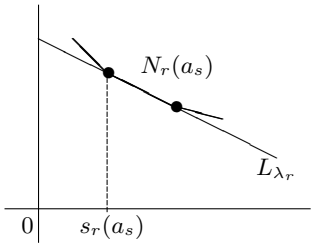
The residual operators of order $r+1$ are defined in a completely analogous way, except for the fact that the residual coefficients of $N := N_{r+1}^-(g)$ need to be twisted by certain powers of z_r. More precisely, for each integer abscissa s in the projection of N over the horizontal axis, we define

$$c_s := \begin{cases} 0, & \text{if } (s,u_s) \text{ lies above } N, \\ z_r^{t_s} R_r(a_s)(z_r) \in \mathbb{F}_{r+1}, & \text{if } (s,u_s) \text{ lies on } N, \end{cases}$$

The exponent t_s is defined to be:

$$t_s := \left(s_r(a_s) - h_r^{-1}u_s\right)/e_r,$$

where h_r^{-1} is any integer satisfying: $h_r^{-1}h_r \equiv 1 \pmod{e_r}$, and $s_r(a_s)$ is the abscissa of the left end point of the segment $S_{\lambda_r}(N_r(a_s))$.



With some effort, one is able to prove results completely analogous to the three fundamental results of Ore; that is, Theorems of the product, of the polygon and of the residual polynomial in order r [HN08, Secs.2+3].

Definition. Let $\mathbf{t}$ be a type of order r. For any $g(x) \in \mathcal{O}[x]$ we define

$$\mathrm{ord}_{\mathbf{t}}(g) := \mathrm{ord}_{\psi_r} R_r(g) = \ell(N_{r+1}^-(g)),$$

and we say that $\mathbf{t}$ is g-complete if $\mathrm{ord}_{\mathbf{t}}(g) = 1$.

By the Theorem of the product, $\mathrm{ord}_{\mathbf{t}}(gh) = \mathrm{ord}_{\mathbf{t}}(g) + \mathrm{ord}_{\mathbf{t}}(h)$.

2.6 Back to the factorization algorithm

Along the factorization algorithm, we construct types such that $\mathrm{ord}_{\mathbf{t}}(f)$ is positive. This means that there is some irreducible factor $F(x)$ of $f(x)$ in $\mathcal{O}[x]$, for which $\mathrm{ord}_{\mathbf{t}}(F) > 0$, and this implies that F has the features captured by the type $\mathbf{t}$:

$$R_i(F) \sim \psi_i^{\ell_i(F)}, \quad N_i(F) \text{ is one-sided with slope } \lambda_i, \ \forall\, 1 \le i \le r.$$

We denote by $F_{\mathbf{t}}(x) \in \mathcal{O}[x]$ the (unknown) product of all monic irreducible factors F of f such that $\mathrm{ord}_{\mathbf{t}}(F) > 0$; this notation is coherent with the previous way to consider $F_{\mathbf{t}}$ as an (unknown) factor of $f(x)$ detected by Hensel lemma or the results of Ore.

If $\mathbf{t}$ is f-complete, then $F_{\mathbf{t}}$ is already irreducible, and the node labelled by $\mathbf{t}$ is a leave of the tree of types. If $\mathbf{t}$ is not f-complete, that is, $\mathrm{ord}_{\mathbf{t}}(f) > 1$, it is clear that the extension of Ore's results to order r determines a completely analogous branching of the node of the tree $\mathcal{T}$ labelled by $\mathbf{t}$.

The construction of the polynomial $\phi_{\lambda,\psi}$ that enlarges the type at the next order is obtained by applying in a recursive way the procedure described in section 2.4. However, at order $r > 1$ one has to care about the powers of z_r that twist the residual coefficients of the polygons [HN08, Sec.2.3].

We conclude with a couple of remarks on the Theorem of the polygon and the computation of the residue class fields of the extensions determined by the irreducible factors.

2.7 Special features of the Theorem of the polygon in order r

Proposition. Suppose $\mathrm{ord}_{\mathbf{t}}(f) > 0$ and let $\theta \in K^{\mathrm{sep}}$ be a root of $F_{\mathbf{t}}$. Then, for any polynomial $g(x) \in \mathcal{O}[x]$,

$$v_{r+1}(g) \le e_1 \cdots e_r \, v(g(\theta)), \tag{2.3}$$

and equality holds if and only if $\mathrm{ord}_{\mathbf{t}}(g) = 0$.

Hence, $v_{r+1}/e_1 \cdots e_r$ has to be considered an approximation of the valuation v on the finite extension $K(\theta)/K$. The formula for the value of $v(\phi_{r+1}(\theta))$ given by the Theorem of the polygon gives an interpretation of the slopes of $N^-_{r+1}(f)$ as a measure of the inequality of (2.3), for the polynomial ϕ_{r+1}. More precisely, for any root $\theta \in K^{\mathrm{sep}}$ of the factor F_λ of $F_{\mathbf{t}}$ determined by some $\lambda \in \mathrm{Slopes}(N^-_{r+1}(f))$, the Theorem of the polygon states that:

$$v(\phi_{r+1}(\theta)) = \frac{|\lambda| + v_{r+1}(\phi_{r+1})}{e_1 \cdots e_r},$$

or equivalently:

$$e_1 \cdots e_r \, v(\phi_{r+1}(\theta)) - v_{r+1}(\phi_{r+1}) = |\lambda|.$$

2.8 Computation of the residue class fields of the extensions determined by the irreducible factors

If the type $\mathbf{t}$ of order r is f-complete, then the field $\mathbb{F}_{r+1}$ is a computational representation of the residue class field of the (unknown) irreducible factor F singled out by $\mathbf{t}$. If $\theta \in K^{\mathrm{sep}}$ is a root of F, $L = K(\theta)$ and $\mathbb{F}_L$ is the residue class field, there is an explicit isomorphism:

$$\gamma \colon \mathbb{F}_{r+1} = \mathbb{F}_0[z_0, \ldots, z_r] \longrightarrow \mathbb{F}_L, \quad z_i \mapsto \overline{\gamma_i(\theta)},$$

where $\gamma_i(x) \in K(x)$ are certain rational functions that can be expressed as a product of the ϕ polynomials of $\mathbf{t}$ with integer (positive or negative) exponents [HN08, Sec.2.4+(36)].

The computation of these rationals functions would be inefficient, so that along the flow of the algorihtm only these integer exponents are computed and stored, which is sufficient for all the applications where the residue class field $\mathbb{F}_L$ is involved.

2.9 Higher order indices

Why does this process terminate? Why all types become complete after a finite number of steps? Answer: because each node "swallows" a positive (and big!) integer portion of the absolute index of $f(x)$.

Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible separable polynomial, $L = K(\theta)$, where $\theta \in K^{\mathrm{sep}}$ is a root of F, and $\mathcal{O}_L$ the ring of integers. The *index* $\mathrm{ind}(F)$ is defined as:

$$\mathrm{ind}(F) := \mathrm{length}_{\mathcal{O}}(\mathcal{O}_L/\mathcal{O}[\theta]).$$

Recall the well-known relationship: $v(\mathrm{disc}(F)) = 2\,\mathrm{ind}(F) + v(\mathrm{disc}(L/K))$.

Let $f(x) \in \mathcal{O}[x]$ be a monic separable polynomial, and $f = F_1 \cdots F_g$ its factorization into a product of monic irreducible polynomials in $\mathcal{O}[x]$. Let $\mathcal{O}_f := \mathcal{O}[x]/(f(x))$. The index of f is by definition:

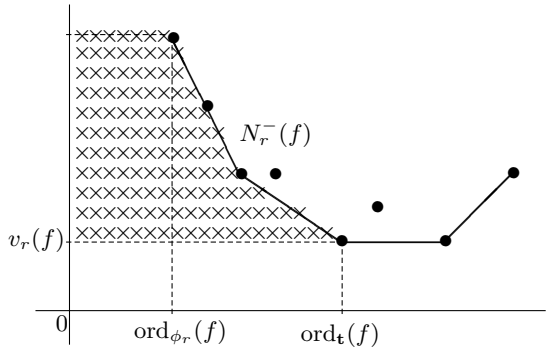
$$\mathrm{ind}(f) := \mathrm{length}_{\mathcal{O}}\left((\mathcal{O}_f)^{\sim}/\mathcal{O}_f\right) = \sum_{j=1}^{g} \mathrm{ind}(F_j) + \sum_{1 \le j < k \le g} v(\mathrm{Res}(F_j, F_k)),$$

where the superscript $(\ )^{\sim}$ indicates "integral closure".

Now, for each $\mathbf{t} \in \mathbf{t}$, we define:

$$\mathrm{ind}_{\mathbf{t}}(f) := f_0 f_1 \cdots f_r \,\mathrm{ind}(N_{r+1}^{-}(f)),$$

where r is the order of $\mathbf{t}$ and, for any polygon N, $\mathrm{ind}(N)$ is the number of points of integer coordinates that lie below or on N and the horizontal line passing through the (left) starting point of N, beyond the vertical axis and above the horizontal line having first contact with N from below.



Theorem. Let $\mathcal{T}$ be the tree of types considered at any stage of Montes algorithm. Then,

$$\sum_{\mathbf{t} \in \mathbf{t}} \mathrm{ind}_{\mathbf{t}}(f) \le \mathrm{ind}(f).$$

If all leaves of $\mathcal{T}$ are f-complete, then equality holds.

Corollary.

1. The factorization algorithm ends after a finite number of steps.

2. It computes $\mathrm{ind}(f)$ as a by-product.

It is not absolutely true that $\mathrm{ind}_{\mathbf{t}}(f)$ is always positive. However, if for some node $\mathbf{t}$ we have $\mathrm{ind}(N_r^-(f)) = 0$, then this polygon is one-sided and the projection of this side either to the horizontal or to the vertical axis has length one; hence, $\mathbf{t}$ is either complete, or it becomes complete after a unibranch step.

2.10 Optimization of Montes algorithm

Definition. The type $\mathbf{t} = [\phi_1, \dots, \phi_{r+1}]$ of order r is called *optimal* if either $r = 0$ or $\deg \phi_1 < \cdots < \deg \phi_r$. It is called *strongly optimal* if it is optimal and moreover $\deg \phi_r < \deg \phi_{r+1}$.

Montes algorithm is optimized in such a way that all nodes of the tree of types, except for the leaves, are strongly optimal. Hence, by the very definition, all nodes of the tree, including the leaves, are optimal.

Let us sketch the ideas of the optimization process. Suppose a node of the tree, $\mathbf{t} = [\phi_1, \dots, \phi_r]$ of order $r-1$, is strongly optimal and non-complete. Then, in principle, several branches sprout from $\mathbf{t}$, parameterized by pairs (λ, ψ), where λ is one of the slopes of $N_r^-(f)$ and ψ is one of the irreducible factors of $R_{\lambda,r}(f)$. For each one of these branches let us write,

$$\lambda = -h_\lambda/e_\lambda, \quad f_\psi := \deg \psi, \quad m_{\lambda,\psi} := e_\lambda f_\psi m_r,$$

where e_λ, h_λ are positive coprime integers. Denote by $\phi_{\lambda,\psi}$ the $(r+1)$-th ϕ-polynomial of degree $m_{\lambda,\psi}$ constructed by the general method, as explained in section 2.6. The type

$$\mathbf{t}_{\lambda,\psi} := [\phi_1, \dots, \phi_r, \phi_{\lambda,\psi}]$$

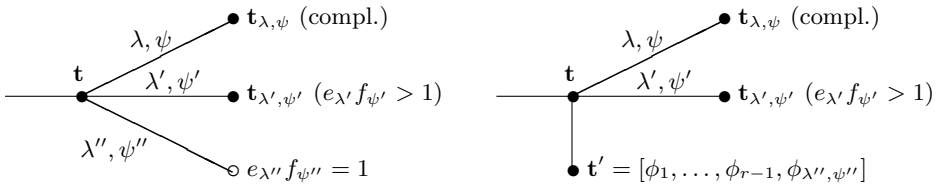
would be a new node of order r if no optimization were applied. Now there are three different possibilities for each branch:

(a) The type $\mathbf{t}_{\lambda,\psi}$ is complete. In this case, $\mathbf{t}_{\lambda,\psi}$ is a leave of the tree.

(b) The type $\mathbf{t}_{\lambda,\psi}$ is not complete, and $e_\lambda f_\psi > 1$. In this case, $\mathbf{t}_{\lambda,\psi}$ is strongly optimal and it is taken as a new node of order r of the tree.

(c) The type $\mathbf{t}_{\lambda,\psi}$ is not complete, and $e_\lambda f_\psi = 1$. In this case, $\mathbf{t}_{\lambda,\psi}$ is not strongly optimal.

In case (c), the polynomial $\phi_{\lambda,\psi}$ is a better representative of the original type $\mathbf{t}$ than ϕ_r; thus, we consider the type $\mathbf{t}' = [\phi_1, \dots, \phi_{r-1}, \phi_{\lambda,\psi}]$ as a new node of order $r-1$. This type $\mathbf{t}'$ is added to the tree and manipulated as any other type, but only slopes strictly less than λ (instead of strictly less than 0) are considered in the Newton polygon $N_{\mathbf{t}',r}(f)$. We call this replacement of a branch of order r by a new branch of order $r-1$, a *refinement step*.



Since all computations (v_r, N_r, $R_r, \dots$) are of a recursive nature, to proceed in order $r-1$ instead of order r causes a considerable improvement of the complexity.

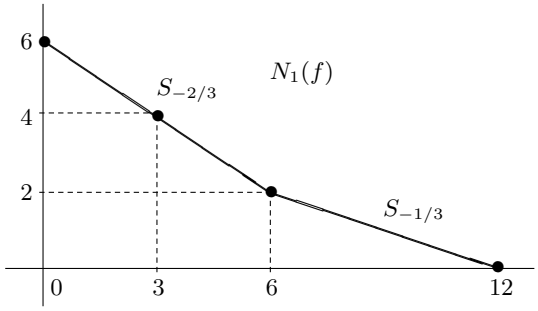
Note that the leaves of the tree, as nodes of complete branches, are not necessarily strongly optimal (in case (a) $e_\lambda f_\psi$ can be indistinctly equal to or greater than one). There will appear non-strongly optimal leaves if and only if there are irreducible factors of $f(x)$ that are one an *Okutsu approximation* to the other. In any case, the optimized algorithm always outputs f-complete and optimal types. Curiosly enough, this optimization motivated by pure practical reasons, provides the output of Montes algorithm with unexpected canonical properties.

The concept of Okutsu appoximation and the canonical properties of the output data of Montes algorithm will be discussed in section 3.

2.11 An example

Let us show how the algorithm works with an example. Take $f(x) = x^{12} + 4x^6 + 16x^3 + 64 \in \mathbf{Z}_2[x]$.

Since $f(x) \equiv x^{12} \pmod 2$, the tree of types will be connected and we can take $\mathbf{t}_0 = [x]$ as a root node. The Newton polygon of first order of $f(x)$ has two sides, with slopes $-2/3$ and $-1/3$, and $\mathrm{ind}_{\mathbf{t}_0}(f) = \mathrm{ind}(N_1(f)) = 23$.



The residual polynomials of the first order are:

$$R_{-2/3,1}(f)(y) = y^2 + y + 1, \quad R_{-1/3,1}(f)(y) = (y+1)^2.$$

Thus, the type $\mathbf{t}_0$ ramifies into two types of order one, with edges labelled by λ_1, $\psi_1(y)$, given by :

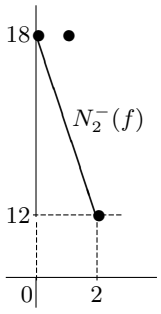
$$\begin{array}{ll} \mathbf{t} = [x, x^6 + 4x^3 + 16], & \lambda_1 = -2/3,\ \psi_1(y) = y^2 + y + 1, \\ \mathbf{t}' = [x, x^3 + 2], & \lambda_1 = -1/3,\ \psi_1(y) = y + 1. \end{array}$$

The type $\mathbf{t}$ is complete, and it singles out an (unknown) irreducible factor $F(x) \in \mathbf{Z}_2[x]$; let $L/\mathbf{Q}_2$ be the finite extension determined by F. We can apply (2.1) to get $e(L/\mathbf{Q}_2) = 3$, $f(L/\mathbf{Q}_2) = 2$. Also, we get an Okutsu approximation $x^6 + 4x^3 + 16$, to F.

The type $\mathbf{t}'$ is not complete: $\mathrm{ord}_{\mathbf{t}'}(f) = \mathrm{ord}_{\psi_1} R_1(f) = 2$, so that some more work in order two is required. Denote $\phi_2(x) = x^3 + 2$. We know that $N_2^-(f)$ will have length 2; hence, in order to compute this polygon we need only to compute the three last terms of the ϕ_2-adic development of $f(x)$:

$$f(x) = \phi_2(x)^4 + \cdots + 28\phi_2(x)^2 - 32\phi_2(x) + 64.$$

We have $v_2(\phi_2) = v_2(2) = 3$, so that $v_2(64) = 18$, $v_2(-32\phi_2(x)) = 18$, and $v_2(28\phi_2(x)^2) = 12$. The Newton polygon of secon order is:



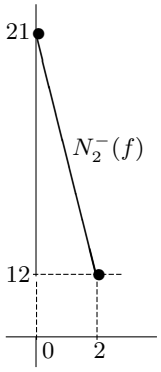
It has slope $\lambda := -3$ and residual polynomial of second order $R_{\lambda,2}(f)(y) = y^2 + 1 = (y+1)^2$, a power of $\psi(y) := y + 1$. Also, $\mathrm{ind}_{\mathbf{t}'}(f) = 3$. We want now to construct a polynomial $\phi_{\lambda,\psi}$ of minimal degree satisfying:

$$N_2(\phi_{\lambda,\psi}) \text{ one-sided with slope } -3, \quad R_{\lambda,2}(\phi_{\lambda,\psi}) \sim \psi.$$

Since $e_\lambda = f_\psi = 1$, this polynomial $\phi_{\lambda,\psi}$ will have again degree 3; we can take $\phi_{\lambda,\psi}(x) = x^3 + 6$. For the sake of optimization, instead of considering the (non-complete, non-strongly optimal) type $[x, x^3+2, x^3+6]$ of order 2, whose further enlargements will require to work in order 3, we replace the type $\mathbf{t}'$ by the type $\mathbf{t}'' = [x, x^3+6]$ of order 1. In this way, our next work will be done still in order 2. If we now take $\phi_2(x) := x^3 + 6$, the last three terms of the ϕ_2-adic development of $f(x)$ are:

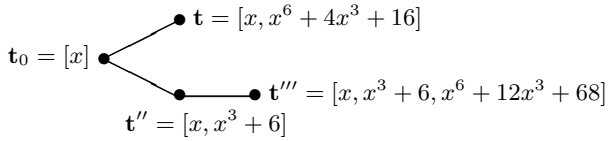
$$f(x) = \phi_2(x)^4 + \cdots + 220\phi_2(x)^2 - 896\phi_2(x) + 1408.$$

We have now $v_2(1408) = 21$, $v_2(896\phi_2) = 24$, $v_2(220\phi_2^2) = 12$, so that $N_2^-(f)$ is one-sided with slope $-9/2$:



and $\mathrm{ind}_{\mathbf{t}''}(f) = \mathrm{ind}(N_2^-(f)) = 4$. The residual polynomial of second order is already irreducible: $R_{-9/2,2}(f)(y) = y + 1$. Thus, $\mathbf{t}''$ is extended to a unique type of order two: $\mathbf{t}''' = [x, x^3+6, x^6+12x^3+68]$, which is already complete. It singles out another irreducible factor $G(x) \in \mathbf{Z}_2[x]$; let $M/\mathbf{Q}_2$ be the corresponding extension. By (2.1) we get $e(M/\mathbf{Q}_2) = 6$, $f(M/\mathbf{Q}_2) = 1$, and we have computed an Okutsu approximation $x^6 + 12x^3 + 68$, to $G(x)$.

The final tree $\mathcal{T}$ of types is:



The index $\mathrm{ind}(f)$ is equal to: $\mathrm{ind}(f) = \mathrm{ind}_{\mathfrak{t}_0}(f) + \mathrm{ind}_{\mathfrak{t}''}(f) = 23 + 4 = 27$.

3 Okutsu Frames and Optimal Types

As in the last section, we fix a local field K, with ring of integers $\mathcal{O}$, maximal ideal $\mathfrak{m}$, and uniformizer $\pi \in \mathfrak{m}$. Let $v\colon \overline{K}^* \longrightarrow \mathbf{Q}$, be the canonical extension of the discrete valuation of K to an algebraic closure, with the usual normalization $v(K^*) = \mathbf{Z}$. Let $K^{\mathrm{sep}} \subseteq \overline{K}$ be the separable closure of K in $\overline{K}$. For any $\eta \in \overline{K}$ we denote $\deg \eta := [K(\eta)\colon K]$.

All results of this section are extracted from [GMN09], which is a revision of the original paper by Okutsu [Oku82].

3.1 Okutsu frames

Let us fix a monic irreducible separable polynomial $F(x) \in \mathcal{O}[x]$, of degree n. Let $\theta \in K^{\mathrm{sep}}$ be a root of $F(x)$, $L = K(\theta)$, and $\mathcal{O}_L$ the ring of integers.

Denote $\mu_0 := 0$, $m_0 := 1$, and consider sequences, respectively of positive integers and non-negative rational numbers:

$$\begin{aligned} &0 < m_1 < m_2 < \cdots < m_R < m_{R+1} := n, \\ &0 < \mu_1 < \mu_2 < \cdots < \mu_R < \mu_{R+1} := \infty, \end{aligned}$$

recursively defined as follows:

$$\begin{aligned} m_i &:= \min\left\{ \deg \eta \;\middle|\; \eta \in \overline{K} \text{ satisfies } \; v(\theta - \eta) > \mu_{i-1} \right\}, \\ \mu_i &:= \max\left\{ v(\theta - \eta) \text{ among all } \eta \in \overline{K} \text{ of degree } m_i \right\}. \end{aligned}$$

We can choose separable integral elements $\alpha_i \in K^{\mathrm{sep}}$ satisfying

$$\deg \alpha = m_i, \quad v(\theta - \alpha) = \mu_i, \quad \forall\, 1 \leq i \leq R.$$

Let $F_i(x) \in \mathcal{O}[x]$ be the minimal polynomial of α_i over K, and denote $K_i = K(\alpha_i)$, for all $1 \leq i \leq R$. The fields K_i are not necessarily subfields of L, but we shall see soon that their maximal tamely ramified subextensions over K are always contained in L.

Definition. The sequence $[F_1, \ldots, F_R]$ is called an *Okutsu frame* of F, and R is called the *Okutsu depth* of F.

Although the polynomials F_i are not uniquely determined, we must consider an Okutsu frame as an essentially canonical object attached to F.

Definition. An $\eta \in K^{\text{sep}}$ such that $\deg \eta = n$ and $v(\theta - \eta) > \mu_R$ is called an *Okutsu approximation* to θ.

A monic irreducible separable polynomial $G(x) \in \mathcal{O}[x]$ is called an *Okutsu approximation* to F if $\deg G = n$ and $v(G(\theta)) > (n/m_R)v(F_R(\theta))$.

Remarks.

1. The values $v(F_i(\theta))$, $1 \leq i \leq R$ are independent of the choice of the Okutsu frame [GMN09, Cor.2.14].
2. $\eta \in K^{\text{sep}}$ is an Okutsu approximation to θ if and only if the minimal polynomial of η over K is an Okutsu approximation to $F(x)$ [GMN09, Lem.2.12].
3. The notion of Okutu approximation determines an equivalence relation on $\mathcal{O}_{K^{\text{sep}}}$, and on the set of monic irreducible separable polynomials in $\mathcal{O}[x]$ [GMN09, Lem.4.3].

Exercises. The following facts are an immediate consequence of the definitions:

1. $\text{depth}(F) = 0$ if and only if F is irreducible modulo $\mathfrak{m}$.
2. Suppose that $v(F(0)) = 0$ and let $[F_1, \ldots, F_R]$ be an Okutsu frame of F. Let $G(x) := \pi^{nm} F(x/\pi^m)$, for some positive integer m. Then, $[x, F_1(x), \ldots, F_R(x)]$ is an Okutsu frame of G, and $\mu_{i,G} = \mu_{i-1} + m$, for all $1 \leq i \leq R+1$.
3. Let $E(x)$ be an Eisenstein polynomial. Then $[x]$ is an Okutsu frame of E, and $\mu_1 = 1/n$.
4. Two Eisenstein polynomials $E(x)$, $E'(x)$, are one an Okutsu approximation to the other if and only if $v(E(0) - E'(0)) > 1$.

Suppose that $\text{depth}(F) = 0$ and take $G = \pi^n F(x/\pi)$. Let $E(x)$ be an Eisenstein polynomial of degree n. The polynomial E determines a totally ramified extension and the polynomial G determines an unramified extension. However, the exercises show that G and E have both $[x]$ as Okutsu frame. Hence, it has to be clear that an Okutsu frame is an object attached to an irreducible polynomial and it is by no means an invariant of the finite extension determined by this polynomial.

3.2 Okutsu invariants of finite extensions of K

In spite of what has been said, an Okutsu frame accompanied by an Okutsu approximation do contain a lot of information about the extension L/K and its subextensions.

All results of this section are extracted from [GMN09, Sec.2.1]. We fix throughout the section an Okutsu frame $[F_1, \dots, F_R]$ of F.

Lemma. Suppose that $\alpha, \eta \in K^{\text{sep}}$ satisfy:

$$v(\theta - \alpha) > \mu_{i-1}, \quad v(\theta - \eta) > \mu_{i-1},$$

for some $1 \leq i \leq R+1$. Then, for any polynomial $g(x) \in K[x]$ of degree less than m_i, we have

$$v(g(\eta) - g(\alpha)) > v(g(\alpha)).$$

Moreover, if $\deg \alpha = m_i$, then $e(K(\alpha)/K)$ divides $e(K(\eta)/K)$.

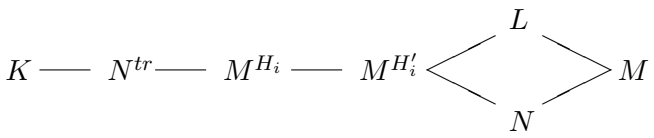
Proposition. Suppose that $\alpha \in K^{\text{sep}}$ satisfies

$$\deg \alpha = m_i, \quad v(\theta - \alpha) = \mu_i,$$

for some $1 \leq i \leq R+1$. Let $N = K(\alpha)$, M/K a finite Galois extension containg L and N, and $G = \text{Gal}(M/K)$. Consider the subgroups:

$$H_i := \{\sigma \in G \mid v(\theta - \sigma(\theta)) > \mu_{i-1}\} \supseteq H_i' := \{\sigma \in G \mid v(\theta - \sigma(\theta)) \geq \mu_i\},$$

and let $M^{H_i} \subseteq M^{H_i'} \subseteq M$ be the respective fixed fields. Finally, let N^{tr} be the maximal tamely ramified subextension of N/K. Then, $N^{tr} \subseteq M^{H_i} \subseteq M^{H_i'} \subseteq L \cap N$.



Corollaries. Let $K_i = K(\alpha_i)$, for $1 \leq i \leq R$.

1. The numbers $e(K_i/K)$, $f(K_i/K)$, do not depend on the chosen Okutsu frame.

2. $e(K_1/K) \,|\, \cdots \,|\, e(K_r/K) \,|\, e(L/K)$, and
   $f(K_1/K) \,|\, \cdots \,|\, f(K_r/K) \,|\, f(L/K)$. In particular, $m_1 \,|\, \cdots \,|\, m_r \,|\, n$.

3. The extension K_1/K is unramified and we have a chain of tamely ramified subfields of L:

$$\begin{array}{ccccccccccc} & & & & K_2 & & & & K_R & & \\ & & & & | & & & & | & & \\ K & - & K_1 & - & K_2^{tr} & - & \cdots & - & K_R^{tr} & - & L^{tr} & - & L \end{array}$$

4. If $G(x) \in \mathcal{O}[x]$ is an Okutsu approximation to F, it admits a root $\alpha \in K^{\mathrm{sep}}$ such that the field $K_{R+1} := K(\alpha)$ satisfies:

$$K_{R+1}^{tr} = L^{tr}, \quad e(K_{R+1}/K) = e(L/K), \quad f(K_{R+1}/K) = f(L/K).$$

5. If L/K is tamely ramified, then

$$\{v(\theta - \sigma(\theta)) \mid \sigma \in G\} = \begin{cases} \{\mu_1, \ldots, \mu_R, \infty\}, & \text{if } m_1 = 1, \\ \{0, \mu_1, \ldots, \mu_R, \infty\}, & \text{if } m_1 > 1. \end{cases}$$

   In particular, μ_R is Krasner's radius of $F(x)$. Moreover, for each $0 \le i \le R$, there are exactly $(n/m_i) - (n/m_{i+1})$ different roots θ' of F such that $v(\theta - \theta') = \mu_i$.

One might speculate that the fields K_i in Corollary (3) may not be subfields of L, but they eventually detect the presence of subfields of L with given ramification index and residual degree. Jürgen Klüners provided us with an example showing that is not the case either.

Example (Klüners). Let $F(x) = x^4 + 4x^2 - 4x + 4 \in \mathbf{Z}_2[x]$. This polynomial is separable, irreducible, and it determines a primitive extension L of $\mathbf{Q}_2$. Actually, the roots of F are the squares of the roots of the strongly Eisenstein polynomial $x^4 + 2x + 2$, whose Galois group is well-known. Now, it is easy to check that $[x, x^2 - 2]$ is an Okutsu frame of F, with Okutsu invariants $\mu_1 = 1/2$, $\mu_2 = 5/8$. Thus, the quadratic field $K_2 = \mathbf{Q}_2(\sqrt{2})$ does not correspond to any quadratic subfield of L. Even more, the normal closure of $L/\mathbf{Q}_2$ has a unique quadratic subextension, which is unramified, so that K_2 (which is totally ramified) cannot be connected to any quadratic subfield of this normal closure either.

3.3 Okutsu frames and integral closures

The next theorem shows a relevant property of the polynomials F_i that constitute an Okutsu frame of F.

Theorem. Take $F_0(x) = x$. For any integer $0 \leq m < n$, express m in a unique way as:

$$m = j_0 + j_1 m_1 + \cdots + j_R m_R, \quad 0 \leq j_i < (m_{i+1}/m_i),$$

and consider the following polynomial of degree m:

$$g_m(x) := F_0(x)^{j_0} F_1(x)^{j_1} \cdots F_R(x)^{j_R}.$$

Then, for any polynomial $g(x) \in \mathcal{O}[x]$ of degree m we have,

$$v(g_m(\theta)) \geq v(g(\theta)) - v_1(g(x)).$$

Corollary [Oku82, I,Thm.1]. If $\nu_m := \lfloor v(g_m(\theta)) \rfloor$, then

$$1, \frac{g_1(\theta)}{\pi^{\nu_1}}, \cdots, \frac{g_{n-1}(\theta)}{\pi^{\nu_{n-1}}}$$

is an $\mathcal{O}$-basis of $\mathcal{O}_L$.

3.4 Okutsu frames and optimal types

Theorem. Let $f(x) \in \mathcal{O}[x]$ be a monic separable polynomial. Let $\mathbf{t} = [\phi_1, \ldots, \phi_r, \phi_{r+1}]$ be an f-complete optimal type of order r, and let $F(x) \in \mathcal{O}[x]$ be the monic irreducible factor of $f(x)$ singled out by $\mathbf{t}$. Then,

1. The Okutsu depth of F is

$$R = \begin{cases} r, & \text{if } e_r f_r > 1, \\ r-1, & \text{if } e_r f_r = 1. \end{cases}$$

   In the first case, $[\phi_1, \ldots, \phi_r]$ is an Okutsu frame of F, and ϕ_{r+1} is an Okutsu approximation to F. In the second case, $[\phi_1, \ldots, \phi_{r-1}]$ is an Okutsu frame of F, and ϕ_r, ϕ_{r+1} are both Okutsu approximations to F.

2. $F(x) \equiv \phi_{r+1}(x) \pmod{\mathfrak{m}^\nu}$, where

$$\nu = \left\lceil \frac{h_1}{e_1} + \frac{h_2}{e_1 e_2} + \cdots \frac{h_r}{e_1 \cdots e_r} + \frac{h_{r+1}}{e(L/K)} \right\rceil.$$

Corollaries.

1. The optimized Montes algorithm outputs an essentially canonical representation of the irreducible factors.

2. All irreducible factors are parameterized by strongly optimal types if and only if these factors are pairwise inequivalent under the equivalence relation "to be an Okutsu approximation to".

3. The numerical invariants h_i, e_i, f_i, λ_i, for $1 \leq i \leq R$, and the discrete valuations $v_1, \ldots, v_{R+1}$ are invariants of $F(x)$.

4. In spite of the philosophy of Montes algorithm, that detects factorization but never computes it, the last polynomials of the output types are approximations to the irreducible factors, with a controlled precision. Therefore, the algorithm provides a factorization of the input polynomial indeed.

In a recent work with J. Guàrdia and S. Pauli [GNP10], we develop a *single-factor approximation* algorithm that improves each one of these approximations up to a prescribed precision. This algorithm has quadratic convergence and although it has the same complexity than the Hensel lift routine, it has a slightly better performance in practice.

4 Computation of Integral Closures in Global Fields

For simplicity, we discuss only the computation of the maximal order of a number field.

Let $K = \mathbf{Q}[x]/(f(x))$ be the number field defined by a monic irreducible polynomial $f(x)$ with integer coefficients and degree n. Let $\theta \in \overline{\mathbf{Q}}$ be a root of $f(x)$ and $\mathbf{Z}_K$ the ring of integers.

We already mentioned in section 1.2 that an integral basis of K (i.e. a $\mathbf{Z}$-basis of $\mathbf{Z}_K$) can be computed by an standard application of the Chinese remainder theorem, from a family of p-integral basis in Hermite Normal Form, for all prime numbers p dividing $\mathrm{disc}(f)$.

In this section we deal with the computation of a p-integral basis for a given prime number p. We saw in section 1.2 that Montes algorithm attaches to each prime ideal $\mathfrak{p}$ of K lying over p an OM representation:

$$\mathfrak{p} = [p; \phi_{1,\mathfrak{p}}, \dots, \phi_{r,\mathfrak{p}}; \phi_{\mathfrak{p}}],$$

where $\phi_{\mathfrak{p}}$ is just the $r+1$-th polynomial of the f-complete and optimal type attached to the p-adic irreducible factor of $f(x)$ corresponding to $\mathfrak{p}$. The common feature of the two methods we are about to present is the computation of a p-integral basis in terms of the data encoded by these OM representations.

4.1 Standard OM method

Let $\mathfrak{P}$ be the set of prime ideals of K dividing p. For each $\mathfrak{p} \in \mathfrak{P}$, we fix a topological embedding

$$\iota_{\mathfrak{p}} \colon K \hookrightarrow K_{\mathfrak{p}} \hookrightarrow \overline{\mathbf{Q}}_p,$$

and we denote $\tau_{\mathfrak{p}} := \iota_{\mathfrak{p}}(\theta)$. Let $F_{\mathfrak{p}}(x) \in \mathbf{Z}_p[x]$ be the minimal polynomial of $\tau_{\mathfrak{p}}$ over $\mathbf{Q}_p$, and denote by $n_{\mathfrak{p}} = e(\mathfrak{p}/p)f(\mathfrak{p}/p)$, its degree.

Recall that Montes algorithm can be slightly modified to compute a $\mathbf{Z}_p$-basis of the local ring of integers $\mathbf{Z}_{K_{\mathfrak{p}}}$, for all $\mathfrak{p} \in \mathfrak{P}$. Let us denote by:

$$\mathcal{B}_{\mathfrak{p}} = \left\{ 1, \frac{g_{1,\mathfrak{p}}(\tau_{\mathfrak{p}})}{p^{\nu_{1,\mathfrak{p}}}} \dots, \frac{g_{n_{\mathfrak{p}}-1,\mathfrak{p}}(\tau_{\mathfrak{p}})}{p^{\nu_{n_{\mathfrak{p}}-1,\mathfrak{p}}}} \right\}, \quad \mathfrak{p} \in \mathfrak{P}.$$

these $\mathfrak{p}$-integral bases. The exponents of the denominators were defined as $\nu_{m,\mathfrak{p}} := \lfloor j_1 v(\phi_{1,\mathfrak{p}}(\tau_{\mathfrak{p}})) + \cdots + j_r v(\phi_{r,\mathfrak{p}}(\tau_{\mathfrak{p}})) \rfloor$; thus, the Theorem of the polygon provides an explicit computation of these $\nu_{m,\mathfrak{p}}$ in terms of the data of the OM representation of $\mathfrak{p}$ (see section 2.7).

We compute multipliers $b_{\mathfrak{p}} \in \mathbf{Z}_K$ satisfying:

$$v_{\mathfrak{p}}(b_{\mathfrak{p}}) = 0, \quad v_{\mathfrak{q}}(b_{\mathfrak{p}}) \geq (\exp(F_{\mathfrak{p}}) + 1) e(\mathfrak{q}/p). \tag{2.4}$$

Proposition. **[Ore25]** The family $\bigcup_{\mathfrak{p} \in \mathfrak{P}} b_{\mathfrak{p}} \mathcal{B}_{\mathfrak{p}}$ is a p-integral basis of K.

Proof. Let us denote

$$\alpha_{m,\mathfrak{p}} := b_{\mathfrak{p}} \frac{g_{m,\mathfrak{p}}(\theta)}{p^{\nu_{m,\mathfrak{p}}}}, \quad \forall\, 0 \leq m < n_{\mathfrak{p}}.$$

Although $g_{m,\mathfrak{p}}(\theta)/p^{\nu_{m,\mathfrak{p}}}$ is not necessarily (globally) integral, the element $\alpha_{m,\mathfrak{p}}$ belongs to $\mathbf{Z}_K$ and, even more, it satisfies

$$v_{\mathfrak{q}}(\alpha_{m,\mathfrak{p}}) \geq e(\mathfrak{q}/p), \quad \forall\, \mathfrak{q} \in \mathfrak{P},\ \mathfrak{q} \neq \mathfrak{p}. \tag{2.5}$$

In fact, this is an immediate consequence of (2.4), because $\nu_{m,\mathfrak{p}} \leq \nu_{n_\mathfrak{p}-1,\mathfrak{p}} = \exp(F_\mathfrak{p})$, for all $m, \mathfrak{p}$.

Let us check that $\{\alpha_{m,\mathfrak{p}}\}_{m,\mathfrak{p}}$ is an $\mathbb{F}_p$-linearly independent family in $\mathbf{Z}_K \otimes_\mathbf{Z} \mathbb{F}_p$. Suppose that for certain integers $a_{m,\mathfrak{p}}$ we have

$$\sum_{m,\mathfrak{p}} a_{m,\mathfrak{p}}\alpha_{m,\mathfrak{p}} \in p\mathbf{Z}_K = \prod_{\mathfrak{p}\in\mathfrak{P}} \mathfrak{p}^{e(\mathfrak{p}/p)}.$$

Let us fix one of the primes $\mathfrak{p} \in \mathfrak{P}$. By (2.5),

$$\sum_{m} a_{m,\mathfrak{p}}\alpha_{m,\mathfrak{p}} \in \mathfrak{p}^{e(\mathfrak{p}/p)}.$$

Since $v_\mathfrak{p}(b_\mathfrak{p}) = 0$, if we apply $\iota_\mathfrak{p}$ to this identity, we get

$$\sum_{m} a_{m,\mathfrak{p}} \frac{g_{m,\mathfrak{p}}(\tau_\mathfrak{p})}{p^{\nu_{m,\mathfrak{p}}}} \in (\mathfrak{p}\mathbf{Z}_{K_\mathfrak{p}})^{e(\mathfrak{p}/p)} = p\mathbf{Z}_{K_\mathfrak{p}}.$$

This implies that all $a_{m,\mathfrak{p}}$ are multiples of p. □

The computation of the multipliers $b_\mathfrak{p}$ in terms of the data of the OM representations of the prime ideals is explained in [GMN10, Secs.3.2+4.2]. This computation requires to improve the approximations $\phi_\mathfrak{p}$ till $v_\mathfrak{p}(\phi_\mathfrak{p}(\theta))$ has a sufficiently large value. As mentioned at the end of the last section, this can be carried out with the single-factor approximation algorithm [GNP10].

4.2 Method of the quotients

Let $\mathbf{t} = [\phi_1, \ldots, \phi_i]$ be a type of order $i-1$ labelling one of the nodes of the tree $\mathcal{T}$ along the flow of Montes algorithm. Before computing $N_i^-(f)$, we know a priori the length of this polygon:

$$\ell := \ell(N_i^-(f)) = \mathrm{ord}_{\psi_{i-1}} R_{i-1}(f).$$

Hence, we need only to compute the first $\ell+1$ coefficients of the ϕ_i-adic expansion of $f(x)$:

$$\begin{aligned} f(x) &= \phi_i(x)q_{i,1}(x) + a_0(x), \\ q_{i,1}(x) &= \phi_i(x)q_{i,2}(x) + a_1(x), \\ \cdots &\quad \cdots \\ q_{i,\ell-1}(x) &= \phi_i(x)q_{i,\ell}(x) + a_{\ell-1}(x), \\ q_{i,\ell}(x) &= \phi_i(x)q_{i,\ell+1}(x) + a_\ell(x). \end{aligned}$$

The polynomials $q_{i,1}(x), \ldots, q_{i,\ell}(x)$ are called the *quotients of i-th order of $f(x)$ with respect to* $\mathbf{t}$. There are two relevant facts concerning these polynomials:

1. They are obtained at cost zero along the computation of the coefficients of the ϕ_i-development of $f(x)$ that are necessary to build up the principal polygon $N_i^-(f)$.

2. The element $q_{i,j}(\theta)/p^{\lfloor H_{i,j}\rfloor}$ is integral, for an easy computable rational number $H_{i,j}$. More precisely [GMN09a, Prop.10],

$$H_{i,j} = (Y_j - jv_i(\phi_i))/e_1 \cdots e_{i-1},$$

where Y_j is the ordinate of the point of abscissa j lying on $N_i(f)$.

Conjecture. *For each $\mathfrak{p} = [p; \phi_1, \ldots, \phi_r; \phi_{\mathfrak{p}}] \in \mathfrak{P}$, compute the family*

$$\mathcal{B}_{\mathfrak{p}} := \left\{ b_{\mathfrak{p}},\, b_{\mathfrak{p}} \frac{g_1(\theta)}{p^{\nu_1}},\, \cdots b_{\mathfrak{p}} \frac{g_{n_{\mathfrak{p}}-1}(\theta)}{p^{\nu_{n_{\mathfrak{p}}-1}}} \right\},$$

where now:

1. $b_{\mathfrak{p}} := q_{r+1,1}(\theta)$.

2. *For each $0 \leq m < n_{\mathfrak{p}}$, written in a unique way as:*

$$m = j_0 + j_1 m_1 + \cdots + j_r m_r, \quad 0 \leq j_i < (m_{i+1}/m_i),$$

take $g_m(x)$, ν_m to be:

$$g_m(x) := x^{j_0} q_{1,j_1}(x) \cdots q_{r,j_r}(x), \quad \nu_m := \lfloor H_{1,j_1} + \cdots + H_{r,j_r} + H_{r+1,1} \rfloor.$$

Then, $\bigcup_{\mathfrak{p}\in\mathfrak{P}} \mathcal{B}_{\mathfrak{p}}$ is a p-integral basis of K.

The advantage with respect to the standard method is twofold:

1. We replace the computation of the powers $\phi_i^{j_i}$ by a single polynomial $q_{i,j}$ that was obtained at zero cost.

2. We replace the whole construction of the multiplier $b_{\mathfrak{p}}$ by the consideration of the polynomial $q_{r+1,1}$, which is obtained at the cost of only one division with remainder: $f(x) = \phi_{\mathfrak{p}}(x) q_{r+1,1}(x) + a_0(x)$.

The disadvantage is that the polynomials $g_m(x)$ considered in the standard method have degree m, while those of the quotients method have, by nature, large degree.

In practice, the method of the quotients has a slightly better generic performance, and it is more regular, in the sense that in the examples where the standard method is faster, the difference of the times of execution is very small, while there are peak cases in which the quotients method is extremely faster than the standard one. Anyhow, no accurate analysis of the complexities of either method has been made yet.

In spite of being based on a conjecture, in the +Ideals package we compute integral closures by using the method of the quotients. Since Montes algorithm computes $\mathrm{ind}(f)$ as a by-product, it is easy to check a posteriori that $\bigcup_{\mathfrak{p}\in\mathfrak{P}} \mathcal{B}_{\mathfrak{p}}$ is a p-integral basis indeed. Thus, our implementation outputs an unconditional result. If the output contains no warning message, it means that the p-integral basis was correct. We have run this implementation in thousands of examples and got no counterexample.

Bibliography

[FV10] D. Ford, O. Veres, *On the complexity of the Montes Ideals Factorization Algorithm*, in G. Hanrot, F. Morain and E. Thomé (Eds.), ANTS-IX 2010, Lecture Notes in Computer Science, vol. 6197, pp. 174–185. Springer Verlag Berlin Heidelberg 2010.

[HN08] Guàrdia, J., Montes, J., Nart, E., *Newton polygons of higher order in algebraic number theory*, arXiv:0807.2620v2[math.NT].

[GMN08] Guàrdia, J., Montes, J., Nart, E., *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, arXiv:0807. 4065v3[math.NT].

[GMN09a] Guàrdia, J., Montes, J., Nart, E., *Higher Newton polygons and integral bases*, arXiv:0902. 4428v1[math.NT].

[GMN09] J. Guàrdia, J. Montes, E. Nart, *Okutsu invariants and Newton polygons*, Acta Arithmetica, to appear. arXiv:0911.0286v4[math.NT].

[GMN10] Guàrdia, J., Montes, J., Nart, E., *A new computational approach to ideal theory in number fields*, arXiv:1005.1156v1[math.NT].

[GMN10b] Guàrdia, J., Montes, J., Nart, E., *Arithmetic in big number fields: The '+Ideals' package*, arXiv:1005.4596v1[math.NT].

[GNP10] J. Guàrdia, E. Nart, S. Pauli, *Single-factor approximation for polynomials over local fields*, in preparation.

[McL36] S. MacLane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society, **40**(1936), pp. 363–395.

[McL36b] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal **2**(1936), pp. 492–510.

[Mon99] J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, Tesi Doctoral, Universitat de Barcelona 1999.

[Oku82] K. Okutsu, *Construction of integral basis, I, II*, Proceedings of the Japan Academy, **58**, Ser. A (1982), 47–49, 87–89.

[Ore23] Ø. Ore, *Zur Theorie der algebraischen Körper*, Acta Mathematica **44**(1923), pp. 219–314.

[Ore25] Ø. Ore, *Bestimmung der Diskriminanten algebraischer Körper*, Acta Mathematica **45**(1925), pp. 303–344.

[Pau10] S. Pauli, *Factoring polynomials over local fields, II*, in G. Hanrot, F. Morain and E. Thomé (Eds.), ANTS-IX 2010, Lecture Notes in Computer Science, vol. 6197, pp. 301–315. Springer Verlag Berlin Heidelberg 2010.

[Ver09] O. Veres, *On the Complexity of Polynomial Factorization Over P-adic Fields*, PhD Dissertation, Concordia University, 2009.