An intution on the OM algorithm: computing residual polynomials

Note associated to the talk given at the CAIPI symposium in Caen

Adrien Poteaux

June 18th

Example 1. *Is $P = (x^2-2)^2 - 2\,t^2$ irreducible over $\mathbb{Q}[[t]][x]$? One can easily factorise it over $\mathbb{Q}(\sqrt{2})[[t]][x]$ as $P = (x^2 - 2 - \sqrt{2}\,t)\,(x^2 - 2 + \sqrt{2}\,t)$, but deciding if a factorisation occurs or not over $\mathbb{Q}[[t]][x]$ is not as obvious. We will answer it using valuation theory, and the so called OM algorithm.*

The OM algorithm can be seen on two different point of views: finding extensions of a valuation v on a field $\mathbb{K}$ that are valuations on $\mathbb{K}(x)$ for some indeterminate x, or equivalently how to factorise above $\mathbb{K}^h[x]$, where $\mathbb{K}^h \subset \overline{\mathbb{K}}$ denotes the henselisation of $(\mathbb{K}, v)$. The second being more intuitive for someone not used to valuation theory, we will mainly take this point of view in this document.

Note that we do not present the OM algorithm in the most classical way. While it has been historically introduced as a double "dissection" algorithm (first dissection using some Newton polygon, second dissection according to the residual polynomial), we will rather see it as follows (terms in italic will be defined later on). Given some polynomial of $\mathbb{K}[x]$ and some valuation μ above $\mathbb{K}[x]$ (starting with the *Gauss valuation*):

1. Compute and factorise some *residual polynomial* $R_\mu(P)$ of P associated to the valuation μ,
2. Run a *valuated Hensel lifting* (variant of the classical Hensel lifting) to lift the above factorisation. For each factor:
   - The residual polynomial is now R^N, a power of an irreducible element. If $N = 1$, we proved the irreducibility of the factor in $\mathbb{K}^h[x]$ (and stop here). Otherwise, we compute a *key polynomial* ϕ of μ that has R as a residual polynomial.
   - From the *ϕ-adic expansion* of P, we compute its *generalised Newton polygon* and will *augment* the valuation μ with $\mu(\phi) = \gamma$ where $-\gamma$ is a slope of the Newton polygon, and go back to Step 1 with this new valuation and the current factor.

As we can see, the only "dissection" here is Step 1. The valuated Hensel lifting will not be detailed in this note: we are going to follow some examples, and concentrate of these notions of residual polynomial, key polynomial and augmentation of valuations, providing some definitions along the process.

Let us fix some notations. We consider a value field $(\mathbb{K}, v)$ with value group $\Gamma = v(\mathbb{Q}^\times)$ and residue field $\mathbb{F}$ (defined as the quotient of elements of $\mathbb{K}$ with positive valuation and elements of non negative valuation). Here are some examples:

$\mathbb{K}$	v	Γ	$\mathbb{F}$
$K(t)$	ord_t	$\mathbb{Z}$	K
$\mathbb{Q}$	ord_p	$\mathbb{Z}$	$\mathbb{F}_p$
$K(t_1, t_2)$	$v(t_1) = 1,\ v(t_2) = \sqrt{2}$	$\mathbb{Z} + \sqrt{2}\mathbb{Z}$	K

The last example corresponds to a rank 1 *non discrete* valuation ; the proper definition for v here is classical: $v(\sum_{i,j} a_{ij} t_1^i t_2^j)$ is the minimum of the $i + j\sqrt{2}$ among the $a_{ij} \neq 0$, and $v(P/Q) = v(P) - v(Q)$.

1 The Gauss valuation

The OM algorithm considers valuations above $\mathbb{K}[x]$, as the well known Gauss valuation:

$$\begin{array}{rccc} \mu_0 : & \mathbb{K}[x] & \to & \Gamma \\ & \sum_i a_i\, x^i & \mapsto & \min_i v(a_i) \end{array}$$

The residual polynomial associated to μ_0 corresponds to the classical "reduction modulo a primitive element" effect. It enables to initialise the classical Hensel lifting.

Example 2. *Consider $\mathbb{K} = \mathbb{Q}$ together with the 3-adic valuation $v = \mathrm{ord}_3$. Let $P = x^2 + 3\,x + 5 \in \mathbb{Q}[x]$, and take $R_{\mu_0}(P) = y^2 + 2 \in \mathbb{F}_3[y]$ its reduction modulo 3. As $y^2 + 2 = (y+1)\,(y+2)$ in $\mathbb{F}_3[y]$, the Hensel lemma ensures us that one can factorise P as*

$$P = (x + 1 + \mathcal{O}(3))\,(x + 2 + \mathcal{O}(3))$$

and this factorisation can be lifted quadratically to any aimed precision thanks to the well-known Newton–Hensel lifting algorithm [1, Section 15.4].

The Hensel lemma is a first step, but is not sufficient:

Example 3. *Keep $(\mathbb{K}, v) = (\mathbb{Q}, \mathrm{ord}_3)$ and consider $P = x^4 - 10\,x^2 + 27\,x + 16 \in \mathbb{Q}[x]$ Then $R_{\mu_0}(P) = y^4 + 2\,y + 1 = (y^2 + 1)^2$. As $y^2 + 1$ is irreducible over $\mathbb{F}_3[y]$, we do not have two coprime factors here. The Hensel lemma does nothing.*

To be slightly more precise, the computation of $R_{\mu_0}(P)$ for $P = \sum_i a_i\, x^i$ can be done as follows: for each a_i with valuation $\mu_0(P)$, take $\bar{a}_i$ an element of $\mathbb{F}$ such that $a_i = \bar{a}_i\, c$ up to elements of valuation $> \mu_0(P)$, with c an element of $\mathbb{K}$ with valuation $\mu_0(P)$ (we must take the same c for each a_i). Then $R_{\mu_0}(P) = \sum_i \bar{a}_i\, y^i$, letting $\bar{a}_i = 0$ when $v(a_i) > \mu_0(P)$.

Example 4. *Let* $\mathbb{K} = K(t_1, t_2)$ *with the valuation* $v(t_1) = 1$, $v(t_2) = \sqrt{2}$ *defined above. Consider*

$$P = (t_1^4\, t_2 + t_1^5)\, x^3 + (t_1\, t_2^3 + t_2^4)x^2 + \frac{8}{3}\, t_1^5\, x + 2\, t_1^5 + 3\, t_1^3\, t_2 + 4\, t_1\, t_2^3$$

Then $\mu_0(P) = 5$, *and we get* $R_{\mu_0}(P) = y^3 + \frac{8}{3}\, y + 2$.

2 Augmenting the Gauss valuation

After applying the Hensel lemma, we can always assume to have $R_{\mu_0}(P) = R^N$ for some irreducible polynomial R above $\mathbb{F}[y]$. In order to factorise further, more tools are needed. The first ones are representants and ϕ-adic expansions, that will enable us to find a "pertinent" augmentation of the valuation μ_0. By pertinent, we mean an augmentation that will enable us to either find some partial factorisation, prove irreducibility, or get another representant and valuation augmentation, with a converging process.

Representant of a residual polynomial. We postpone the notion of key polynomial associated to a valuation to the end of Section 3. For the moment, let us consider a polynomial $\phi \in \mathbb{K}[x]$ such that $R_{\mu_0}(\phi) = R$. We call it a *representant* of R according to the valuation μ_0 (several choices are possible).

Example 3 (continued)**.** $\phi = x^2 + 1$ *is such a representant. We could also have taken* $\phi = x^2 + 4$ *for instance.*

Note that when initialising the valuated Hensel lifting, we will consider representants for other polynomials than irreducible factor of $R_\mu(P)$ (when we have two coprime factors, we will compute Bézout cofactors and need to consider their representants).

ϕ-adic expansions.

Definition 1. *Given* $P, \phi \in \mathbb{K}[x]$, *there is a unique expansion*

$$P = \sum_i a_i(x)\, \phi^i$$

with $a_i \in \mathbb{K}[x]$ *satisfying* $\deg(a_i) < \deg(\phi)$. *We call it the* ϕ-adic expansion *of* P, *also known as generalised Taylor expansion [1, Section 9.2].*

It can be computed by successive Euclidean divisions, with an almost linear complexity when using a divide and conquer approach.

Example 3 (continued)**.** *We have* $P = \phi^2 - 12\, \phi + 27\, (x + 1)$.

Finding a good valuation augmentation using the generalised Newton polygon. The next idea is to "homogenise" this expansion, so that at least two "monomials" of the ϕ-adic expansion have the same valuation, and no other monomial have a smaller valuation.

By monomial here, we mean any $a_i(x)\,\phi^i$ of the ϕ-adic expansion. The idea is to set some value $\gamma > \mu_0(\phi)$ to the valuation of ϕ so that we get the homogenisation described above. Doing so, we define a new valuation μ, augmenting μ_0 (since $\gamma > \mu_0(\phi)$) as: for any $P \in \mathbb{K}[x]$ with ϕ-adic expansion $P = \sum_i a_i(x)\,\phi^i$, we let

$$\mu(P) = \min_i \mu_0(a_i) + i\,\gamma$$

We write in short $\mu(\phi) = \gamma$, or $\mu = [\mu_0; \phi, \gamma]$.

Example 3 (continued)**.** *Remember* $P = \phi^2 - 12\,\phi + 27\,(x+1)$ *with* $\phi = x^2 + 1$ *and* $(\mathbb{K}, v) = (\mathbb{Q}, \mathrm{ord}_3)$*. We have* $\mu_0(1) = 0$*,* $\mu_0(12) = 1$ *and* $\mu_0(27\,(x+1)) = 3$*. In order to get two monomials with same valuation, we see two choices:* $\mu(\phi) = 2$ *and* $\mu(\phi) = 1$*. Note that* $\mu(\phi) = \frac{3}{2}$ *would not be correct, since then* $\mu(12\,\phi)$ *would be* $\frac{5}{2}$*, less than* $\mu(\phi^2) = \mu(27\,(x+1)) = 3$*.*

One can see that the value γ we are looking for will correspond to some slope of some Newton polygon. If P has a ϕ-adic expansion $\sum_i a_i\,\phi^i$, then the *generalised Newton polygon* $\mathcal{N}_{\mu_0,\phi}(P)$ of P is defined as the lower convex hull of the set of points $(i, \mu_0(a_i))$.

Example 3 (continued)**.** *We have* $\mathcal{N}_{\mu_0,\phi}(P) = ((0,3),(1,1),(2,0))$*.*

3 Key polynomials and residual polynomial computation.

Before providing some more formal definitions, let us finish to analyse the factorisation of Example 3.

Example 3 (continued)**.** *Let us choose* $\gamma = 1$ *to define the augmentation* $\mu = [\mu_0; \phi = x^2 + 1, 1]$*. Then, the monomials of the* ϕ*-adic expansion* $P = \phi^2 - 12\,\phi + 27\,(x+1)$ *with minimum valuation are* ϕ^2 *and* $-12\,\phi$*. As* $-12\,\phi$ *can be decomposed* $-3\,\phi - 9\,\phi$*, two "monomials" of different valuations, we can also say that the monomials of minimum valuation are* ϕ^2 *and* $-3\,\phi$*. We will define this below as the* initial terms *of* P *for the valuation* μ*:* $in_\mu(P) \sim_\mu \phi^2 - 3\,\phi$*. Note that we could also have taken* $\phi^2 + 6\,\phi$*: this definition is made modulo any element of valuation* $> \mu(P)$*.*

Now, the idea is to express $in_\mu(P)$ *as an element of valuation* $2 = \mu(P)$ *not involving* ϕ*, times a polynomial in some* ξ *of valuation* 0*. Here, we get* $in_\mu(P) \sim_\mu 9\,(\xi^2 - \xi)$ *with* $\xi = \frac{\phi}{3}$*.*

Finally, the residual polynomial $R_\mu(P)$ *can be obtained by replacing* ξ *by* y *and taking the reduction in* $\mathbb{F}_3$ *of each coefficient of the polynomial* $\xi^2 - \xi$*. This gives us* $R_\mu(P) = y^2 + 2\,y$*, which factorises as* $y\,(y+2)$*. To conclude, we take representants of* y *and* $y+2$*, for instance* ϕ *and* $\phi+6$*, and we can check that* $\mu(P - \phi\,(\phi+6)) = \mu(-18\,\phi + 27\,(x+1)) = 3 > 2 = \mu(P)$*. We found the beginning of a factorisation for* P*, that can be lifted using some* valuated *Hensel lifting.*

We are now defining more precisely this notion of initial terms of a polynomial for some valuation μ. Remember that we consider a valued field $(\mathbb{K}, v)$ with value group $\Gamma = v(\mathbb{K}^\star)$ and residue field $\mathbb{F}$. We will assume the group Γ to be non trivial. We consider a valuation μ over $\mathbb{K}[x]$ extending v (the restriction of μ to $\mathbb{K}$ is equal to v), and denote Γ_μ and $\mathbb{F}_\mu$ respectively its value group and residue field. Finally, we will assume μ to have trivial support, i.e. that μ is the restriction to $\mathbb{K}[x]$ of some valuation on the field $\mathbb{K}(x)$.

Graded algebra and Initial term mapping. For any $\alpha \in \Gamma_\mu$, we let

$$\mathcal{P}_\alpha = \{g \in \mathbb{K}[x] \mid \mu(g) \geq \alpha\} \supset \mathcal{P}_\alpha^+ = \{g \in \mathbb{K}[x] \mid \mu(g) > \alpha\}.$$

and define $\mathcal{G}_\mu := \bigoplus_{\alpha \in \Gamma_\mu} \mathcal{P}_\alpha / \mathcal{P}_\alpha^+$ the *graded algebra* of μ over $\mathbb{K}[x]$. The initial term mapping mentionned above is then defined as

$$\begin{array}{rccl} \mathrm{in}_\mu : & \mathbb{K}[x] & \to & \mathcal{G}_\mu \\ & 0 & \mapsto & 0 \\ & P \neq 0 & \mapsto & P + \mathcal{P}^+_{\mu(P)} \in \mathcal{P}_{\mu(P)} / \mathcal{P}^+_{\mu(P)} \end{array}$$

Key polynomials of the valuation μ. In order to define the notion of key polynomial, we need to translate properties of the action of μ on $\mathbb{K}[x]$ into algebraic relationships in $\mathcal{G}_\mu$.

Definition 2. *Consider $G, H \in \mathbb{K}[x]$. We say that:*

- *G and H are μ-equivalent ($G \sim_\mu H$) if $in_\mu(G) = in_\mu(H)$.*
- *G is μ-divisible by H ($H \mid_\mu G$) if $in_\mu(H) \mid in_\mu(G)$ in $\mathcal{G}_\mu$.*
- *G is μ-irreducible if $in_\mu(G)\mathcal{G}_\mu$ is a non-zero prime ideal.*
- *G is μ-minimal if $G \nmid_\mu F$ for any non zero $F \in \mathbb{K}[x]$ with $\deg(F) < \deg(G)$.*

Note that the first point can also be written as $\mu(G - H) < \mu(G)$, while the property of μ-minimality can be expressed as follows [2, Proposition 2.3]:

Lemma 1. *Let $\phi \in \mathbb{K}[x]$ be a non constant polynomial. Then ϕ is μ-minimal if and only if $\mu(P) = \min_i \mu(a_i\, \phi^i)$ for any $P \in \mathbb{K}[x]$, where the ϕ-adic expansion of P is $\sum_i a_i\, \phi^i$.*

Definition 3. *A* key polynomial *for μ is a monic polynomial in $\mathbb{K}[x]$ which is simultaneously μ-minimal and μ-irreducible. The set of key polynomials for μ is denoted $KP(\mu)$. All key polynomials are irreducible in $\mathbb{K}[x]$.*

In particular, representants of an irreducible polynomial taken above are key polynomials [2, Section 4.3].

We now come back to the initial example:

Example 1 (continued). *Remember* $P = (x^2-2)^2 - 2\,t^2 \in \mathbb{Q}[[t]][x]$. *We get* $R_{\mu_0}(P) = (y^2-2)^2 \in \mathbb{Q}[y]$. y^2-2 *being irreducible in* $\mathbb{Q}[y]$, *an associated key polynomial can be* $\phi = x^2-2$. $\mathcal{N}_{\mu_0,\phi}(P) = ((0,2),(2,0))$ *has a single edge with slope* $-\gamma$ *with* $\gamma = 1$. *We get no factorisation, and augment* μ_0 *with* $\mu_1(\phi) = 1$. *As* $P = \phi^2 - 2\,t^2$, *we get* $in_{\mu_1} \sim_{\mu_1} t^2 \left(\left(\frac{\phi}{t}\right)^2 - 2\right)$, *leading to* $R_{\mu_1}(P) = y^2-2$. *Here the situation is different from the Gauss valuation. Because* $R_{\mu_0}(\phi) = y^2-2$, *the residue field of* μ_1 *now contains* $\sqrt{2}$, *so that* $R_{\mu_1}(P)$ *factorises as* $(y-\sqrt{2})\,(y+\sqrt{2})$. *In order to lift this residual factorisation, we need to find a representative for* $\sqrt{2}$. *As* $x^2 = \phi + 2$, *we get* $in_{\mu_1}(x^2) \sim_{\mu_1} 2$. in_{μ_1} *being multiplicative, we get* $in_{\mu_1}(x) \sim_{\mu_1} \sqrt{2}$ *(another way to see the presence of* $\sqrt{2}$ *in the residue field):* x *is our representant for* $\sqrt{2}$. *This enables us to conclude that* $P = (\phi - t\,x)\,(\phi + t\,x) + h.o.t$[1]. *Indeed,* $P - (\phi - t\,x)\,(\phi + t\,x) = -t^2\,(x^2-2) = -t^2\,\phi$ *has* μ_1*-valuation* $3 > 2$. *In particular,* P *is not irreducible above* $\mathbb{Q}[[t]][x]$.

4 Dissection of higher order (Montes, 1999)

We can generalise recursively the strategy above by successive augmentations of the valuation. The next example will illustrate another important point of the algorithm, which is the detection of ramification, that we see from the value group of the valuation.

Example 5 (Kuo). *Let* $P = (x^2 - t^3)^2 - t^7 \in \mathbb{Q}[[t]][x]$ *with* $v = \mathrm{ord}_t$. *We have* $R_{\mu_0}(P) = y^4$, *not getting any factorisation from the Gauss valuation, and introducing the key polynomial* $\phi_0 = x$. *We then compute* $\mathcal{N}_{\mu_0,\phi_0}(P) = ((0,6),(4,0))$ *(because* $\phi_0 = x$, *this is the classical Newton polygon). It has a single edge with slope* $-\gamma = -\frac{3}{2}$. *We define* $\mu_1 = [\mu_0; \phi_0 = x, \frac{3}{2}]$. *Note that this time,* $\gamma \notin \mathbb{Z}$, *the value groupe of* v.

Definition 4. *The ramification of* $\nu = [\mu; \phi, \gamma]$ *is the least integer* e *such that* $e\,\gamma \in \Gamma_\mu$.

Example 5 (continued). *We then have* $in_{\mu_1}(P) \sim_{\mu_1} (\phi_0^2 - t^3)^2 = t^6\,(\xi-1)^2$, *using* $\xi = \frac{\phi_0^2}{t^3}$ *as a transcendental element. This leads to* $R_{\mu_1}(P) = (y-1)^2$. *Once again, we do not get any factorisation from the residual polyomial: augmenting the Gauss valuation is not enough. But we can apply the same strategy starting from* μ_1*: we build a key polynomial as a representant of* $y-1$ *of valuation* 3, *i.e.* $\phi_1 = t^3\,(\xi-1) = \phi_0^2 - t^3$. *We then compute the* ϕ_1*-adic valuation* $P = \phi_1^2 - t^7$, *leading to a generalised Newton polygon with a single slope* $-\frac{7}{2}$. *Finally, we augment* μ_1 *by fixing* $\mu_2(\phi_1) = \frac{7}{2}$

We now have $in_{\mu_2}(P) \sim_{\mu_2} \phi_1^2 - t^7$. *Now, because we have* $\frac{3}{2} = \mu_2(\phi_0)$ *in our value group, we whould not take* $\frac{\phi_1^2}{t^7}$ *as a transcendental element, but for instance* $\xi = \frac{\phi_1}{\phi_0\,t^2}$. *Another way of saying this is that* $\frac{7}{2} \in \Gamma_{\mu_2}$, *i.e. that there is no ramification* ($e = 1$) *involved. A third (similar) point of view is that it is possible to build a transcendental element* ξ *on the form* ϕ_1 *divided by the product of powers of* t *and* ϕ_0 *because of the different valuations of* ϕ_1, ϕ_0 *and* t.

[1] higher order terms

More generally, from the definition of the ramification, ξ will always be built as ϕ_k^e divided by a product of powers of the ϕ_i, $0 \le i < k$ times an element of $\mathbb{K}$. The valuation of this element of $\mathbb{K}$ and the exponents of the ϕ_i can be computed only by considering the valuations of the ϕ_i !

Example 5 (continued)**.** *We can now express our initial term polynomial as an element of valuation* 7 *times a polynomial in* $\xi = \frac{\phi_1}{t^2\,\phi_0}$*:*

$$in_{\mu_2}(P) \sim_{\mu_2} t^4\,x^2 \left(\left(\frac{\phi_1}{x\,t^2}\right)^2 - \frac{t^3}{x^2}\right) \sim_{\mu_2} t^7 \left(\left(\frac{\phi_1}{x\,t^2}\right)^2 - 1\right)$$

since $x^2 = \phi_1 + t^3 \sim_{\mu_2} t^3$*. This leads to* $R_{\mu_2}(P) = y^2 - 1$*, that factorises as* $(y-1)\,(y+1)$*. By taking representants as before, we get the factorisation* $P = (\phi_1 - t^2\,x + \cdots)\,(\phi_1 + t^2\,x + \cdots)$*, as indeed* $P - (\phi_1 - t^2\,x)\,(\phi_1 + t^2\,x) = t^4\,(x^2 - t^3) = t^4\,\phi_1$ *has* μ_2*-valuation* $7 + \frac{1}{2} > 7$*.*

5 Rank 1 non discrete examples

Let us conclude this note with two examples involving a non discrete valuation, that we can use for instance when computing multivariate Puiseux series. Additionally to this "non discrete" novelty, these examples use everything that has been sketched in the previous examples. This was not part of the talk, but might interest a reader wanting a more evolved example.

Example 6. *Consider* $\mathbb{K} = \mathbb{Q}(t_1, t_2)$ *with the valuation defined by* $v(t_1) = 1$ *and* $v(t_2) = \sqrt{2}$ *(thus* $\Gamma_v = \mathbb{Z} + \sqrt{2}\,\mathbb{Z}$*), and consider*

$$P = \left(\left((x-1)^4 - 2\,t_1^2\,t_2^2\right)^4 - 3\,t_2^{14}\right)^6 - t_1^{60}\,t_2^{35}\,(x-1)^2\,\left((x-1)^4 - 2\,t_1^2\,t_2^2\right)^2$$

Note that in practice, the polynomial is given in a dense representation. We start by computing $R_{\mu_0}(P) = (y-1)^{96}$*, thus taking* $\phi_0 = x - 1$*. We then get a Newton polygon with a single slope* $-\left(\frac{1}{2} + \frac{\sqrt{2}}{2}\right)$*, leading to* $\mu_1 = [\mu_0; \phi_0 = x-1, \gamma_0 = \frac{1}{2} + \frac{\sqrt{2}}{2}]$*.* γ_0 *does not belong to* Γ_v *but* $2\,\gamma_0$ *does, so that the first ramification index* e_1 *is* 2*. The groupe value* Γ_{μ_1} *is the one generated by* 1, $\sqrt{2}$ *and* γ_0*, i.e.* $\Gamma_{\mu_1} = (\frac{1}{2} + \frac{\sqrt{2}}{2})\,\mathbb{Z} + \sqrt{2}\,\mathbb{Z}$ *for instance. Note that neither* $\frac{1}{2}$ *nor* $\frac{\sqrt{2}}{2}$ *belong to* Γ_{μ_1}*.*

As $8 + 8\,\sqrt{2} < 14\,\sqrt{2}$*, we have:*

$$in_{\mu_1}(P) \sim_{\mu_1} \left(\phi_0^4 - 2\,t_1^2\,t_2^2\right)^{24} \sim_{\mu_1} t_1^{48}\,t_2^{48} \left(\left(\frac{\phi_0^2}{t_1\,t_2}\right)^2 - 2\right)^{24}$$

leading to $R_{\mu_1} = (y^2 - 2)^{24}$*, and the key polynomial* $\phi_1 = \phi_0^4 - 2\,t_2^2\,t_2^2$*. We compute* $P = (\phi_1^4 - 3\,t_2^{14})^6 - t_1^{60}\,t_2^{35}\,\phi_0^2\,\phi_1^2$*. To compute the next Newton polygon, one can check that* $\mu_1(\phi_1) = 2 + 2\,\sqrt{2}$ *and* $\mu_1(t_1^{60}\,t_2^{35}\,\phi_0^2\,\phi_1^2) = 60 + 35\,\sqrt{2} + 2\,(\frac{1}{2} + \frac{\sqrt{2}}{2}) + 2\,(2 + 2\,\sqrt{2}) =$

$65+40\sqrt{2} > 84\sqrt{2} = 6\cdot 14\sqrt{2}$ *(the highest valuation in* $(\phi_1^4 - 3\,t_2^{14})^6$*), so that* $\mathcal{N}_{\mu_1,\phi_1}(P)$ *has a single slope* $-\gamma_1$ *with* $\gamma_1 = \frac{7\sqrt{2}}{2}$*. As mentionned before,* γ_1 *does not belong to* Γ_{μ_1}*, but* $2\,\gamma_1$ *does, leading to ramification* $e_1 = 2$*. To get an transcendental element, one need to find a linear combination of* $1 = \mu_1(t_1)$*,* $\sqrt{2} = \mu_1(t_2)$ *and* $\frac{1}{2} + \frac{\sqrt{2}}{2} = \gamma_0 = \mu_1(\phi_0)$ *equal to* $2\,\gamma_1 = 7\sqrt{2}$*, getting* $\frac{\phi_1^2}{t_2^7}$*. As before, we define* μ_2 *via* $\mu_2(\phi_1) = \gamma_1$*. We now have* $\Gamma_{\mu_2} = \frac{1}{2}\,\mathbb{Z} + \frac{\sqrt{2}}{2}\,\mathbb{Z}$*.*

From the inequality on valuations in the previous paragraph, we have

$$in_{\mu_2}(P) \sim_{\mu_2} \left(\phi_1^4 - 3\,t_2^{14}\right)^6 \sim_{\mu_2} t_2^{84}\left(\left(\frac{\phi_1^2}{t_2^7}\right)^2 - 3\right)^6$$

leading to $R_{\mu_2}(P) = (y^2-3)^6$*. As* $y^2 - 3$ *is irreducible over* $\mathbb{Q}(\sqrt{2})[y]$*, we found no factorisation, and take* $\phi_2 = \phi_1^4 - 3\,t_2^{14}$ *as a key polynomial. We get a* (ϕ_0, ϕ_1, ϕ_2)*-adic expansion* $P = \phi_2^6 - t_1^{60}\,t_2^{35}\,\phi_0^2\,\phi_1^2$*, so that* $\mathcal{N}_{\mu_2,\phi_2}(P)$ *has a single edge with slope* $-\gamma_2$ *with* $\gamma_2 = \frac{61+43\sqrt{2}}{6}$*. Neither* γ_2 *nor* $2\,\gamma_2$ *belongs to* Γ_{μ_2}*, but* $3\,\gamma_2$ *does, getting ramification* $e_3 = 3$*. As* $\frac{61}{2} + \frac{43}{2}\sqrt{2} = 30 + 21\sqrt{2} + (\frac{1}{2} + \frac{\sqrt{2}}{2})$*, we take* $\frac{\phi_2^3}{t_1^{30}\,t_2^{21}\,\phi_0}$ *as a transcendental element. We define as usual* $\mu_3 = [\mu_2; \phi_2, \gamma_2]$

The computation of the residual polynomial is slightly more involved here. We have

$$in_{\mu_3}(P) \sim_{\mu_3} \phi_0^2\,t_1^{60}\,t_2^{42}\left(\left(\frac{\phi_2^3}{t_1^{30}\,t_2^{21}\,\phi_0}\right)^2 - \frac{\phi_1^2}{t_2^7}\right) \sim_{\mu_3} \phi_0^2\,t_1^{60}\,t_2^{42}\left(\left(\frac{\phi_2^3}{t_1^{30}\,t_2^{21}\,\phi_0}\right)^2 - \sqrt{3}\right)$$

since $\phi_2^4 \sim_{\mu_3} 3\,t_2^{14}$ *implies* $\phi_2^2 \sim_{\mu_3} \sqrt{3}\,t_2^7$*. We thus get* $R_{\mu_3}(P) = y^2 - \sqrt{3}$*, which is irreducible over* $Q(\sqrt{2}, \sqrt{3})[y]$*. We proved the irreducibility of* P*.*

Variante of Example 6

Example 7. *We keep the polynomials* $\phi_0 = x - 1$*,* $\phi_1 = \phi_0^4 - 2\,t_1^2\,t_2^2$ *and* $\phi_2 = \phi_1^4 - 3\,t_2^{14}$ *from Example 6 and let* $P = \phi_2^6 - 6\,t_1^{60}\,t_2^{42}\,\phi_0^2$*. We get the same chain of augmented valuations, and then*

$$in_{\mu_3}(P) \sim_{\mu_3} \phi_0^2\,t_1^{60}\,t_2^{42}\left(\left(\frac{\phi_2^3}{t_1^{30}\,t_2^{21}\,\phi_0}\right)^2 - 6\right)$$

and $R_{\mu_3}(P) = y^2 - 6$*, that factorises as* $(y - \sqrt{2}\,\sqrt{3})\,(y + \sqrt{2}\,\sqrt{3})$*. Setting*

$$P_1 = t_1^{30}\,t_2^{21}\,\phi_0\left(\frac{\phi_2^3}{t_1^{30}\,t_2^{21}\,\phi_0} - \frac{\phi_0^2}{t_1\,t_2}\,\frac{\phi_1^2}{t_2^7}\right) = \phi_2^3 - t_1^{29}\,t_2^{13}\,\phi_0^3\,\phi_1^2 \text{ and } P_2 = \phi_2^3 + t_1^{29}\,t_2^{13}\,\phi_0^3\,\phi_1^2$$

we get $P - P_1\,P_2 = (\phi_0^4\,\phi_1^4 - 6\,t_1^2\,t_2^{16})\,t_1^{58}\,t_2^{26}\,\phi_0^2 = ((\phi_1 + 2\,t_1^2\,t_2^2)\,(\phi_2 + 3\,t^{14}) - 6\,t_1^2\,t_2^{16})\,t_1^{58}\,t_2^{26}\,\phi_0^2$ *so that* $\mu_3(P - P_1\,P_2) = 59 + 27\sqrt{2} + \mu_3(\phi_1\,\phi_2 + 2\,t_1^2\,t_2^2\,\phi_2 + 3\,t^{14}\,\phi_1) = 59 + \frac{89}{2}\sqrt{2} > 61 + 43\sqrt{2} = \mu_3(P)$

References

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

[2] E. Nart. On the equivalence of types. *Journal de Théorie des Nombres de Bordeaux*, 28(3):743–771, 2016.