Constructing Splitting Fields of Polynomials over Local Fields

Jonathan Milstead, Sebastian Pauli, and Brian Sinclair

Abstract We present an algorithm that finds the splitting field of a polynomial over a local field. Our algorithm is an OM algorithm modified for this task.

1 Introduction

Let K be a local field. We present an algorithm that given a polynomial $\Phi \in \mathscr{O}_{\mathsf{K}}[x]$ computes the splitting field L of Φ, that is $\mathsf{K}(\theta_1, \ldots, \theta_N)$ where $\theta_1, \ldots, \theta_N$ are the roots of Φ.

Our algorithm is a variation of an OM algorithm [2], that is specialized to the computation of splitting fields. OM algorithms are named after Ore-MacLane or Okutsu-Montes and are algorithms that compute the OM invariants of a polynomial Φ [15, 9] which can be used to compute the factorization of Φ, an integral basis of the fields generated by the irreducible factors of Φ, their inertia degree and ramification index, and the decomposition of primes in the maximal order of the global field generated by Φ. Several algorithms have been developed for these tasks, for example by MacLane [12] (prime decomposition), Ford and Zassenhaus [5] (integral bases), Okutsu [15] (integral bases), and Montes [14] (prime decomposition). All of them compute the OM invariants more or less explicitly. Our algorithm is based on Montes' algorithm [14, 8, 18].

Our method for computing splitting fields uses the information about the extension generated by the roots of Φ computed in each iteration of the OM algorithm to construct subfields of L of Φ until the splitting field is obtained. In particular we extend our approximation L to the splitting field as soon as we find inertia or that the splitting field contains a certain tamely ramified subextension. We generate wildly ramified subfields of L as soon as we have found an irreducible factor of Φ generating such an extension. In our representation of the algorithm we follow the approach in [19]. An application of our algorithm can be found in [1]. It can also be modified into an root separation algorithm.

A method, similar to ours, is available in Magma [3]. It makes multiple calls to a variant of the Round 4 algorithm, but does not make use of all the information computed internally. The Round 4 algorithm is an OM algorithm that is less efficient than the algorithms based on Montes' methods [14]. The implementation of the Round 4 algorithm (a combination of the algorithms described in [6] and [17]) in Magma returns the factorization of a polynomial over a local field and in addition the extensions generated by the irreducible factors of the polynomial. In the computation of splitting fields, an initial call to Round 4 is used to generate the unramified extension whose degree is the least common multiple of the inertia degrees of the extensions generated by the irreducible factors of Φ. Then Φ is considered over

Jonathan Milstead
Department of Mathematics and Statistics, University of North Carolina Greensboro, NC 27402, e-mail: jmmilste@uncg.edu

Sebastian Pauli
Department of Mathematics and Statistics, University of North Carolina Greensboro, NC 27402, e-mail: s_pauli@uncg.edu

Brian Sinclair
Department of Mathematics and Statistics, University of North Carolina Greensboro, NC 27402, e-mail: basincla@uncg.edu

the extended field. After each subsequent call to Round 4, the field is extended using one of the irreducible factors of Φ over the current approximation to the splitting field until Φ splits into linear factors.

1.1 Overview

Section 2 contains a description of situations when factorizations of polynomials can be derived. Although we do not use these methods directly (they are used in the Round 4 algorithm), they make understanding the algorithm easier. In Section 3 we give some results about tamely ramified extensions and composites of tamely ramified extensions. The general strategy of the splitting field algorithm is outlined in section 4 with technical details provided in section 5 and 6. We present the splitting field algorithm and some auxiliary algorithms in section 7.

1.2 Notation

Let K be a local field, that is a field complete with respect to a non-archimedian exponential valuation v with finite residue class field $\underline{\mathsf{K}} \cong \mathbb{F}_q$ of characteristic p. We denote the multiplicative group of K by $\mathsf{K}^\times$. Let $\mathscr{O}_\mathsf{K}$ be the valuation ring of K and let $\Phi(x) \in \mathscr{O}_\mathsf{K}[x]$. For our purposes, $v = v_\mathsf{K}$ is normalized such that $v_\mathsf{K}(\pi_\mathsf{K}) = 1$ where $\pi = \pi_\mathsf{K}$ is a uniformizing element in $\mathscr{O}_\mathsf{K}$. For $\gamma \in \mathscr{O}_\mathsf{K}$ we denote by $\underline{\gamma}$ the class $\gamma + (\pi)$ in $\underline{\mathsf{K}}$. The unique extension of v to an algebraic closure $\overline{\mathsf{K}}$ of K (or to any intermediate field) is also denoted v. If L/K is a finite extension then v_L denotes the valuation that is normalized such that $v_\mathsf{L}(\pi_\mathsf{L}) = 1$ where π_L is a uniformizing element of L.

Definition 1. For $\gamma \in \overline{\mathsf{K}}^\times$ and $\delta \in \overline{\mathsf{K}}^\times$ we write $\gamma \sim \delta$ if

$$v(\gamma - \delta) > v(\gamma)$$

and impose the supplementary condition $0 \sim 0$. For $\varphi(x) = \sum_{i=0}^n c_i x^i$ and $\psi(x) = \sum_{i=0}^n b_i x^i$ in $\overline{\mathsf{K}}[x]$ we write $\varphi \sim \psi$ if

$$\min_{0 \le i \le n} v(c_i - d_i) \; > \; \min_{0 \le i \le n} v(c_i).$$

It follows immediately that the relation $\sim$ is symmetric, transitive, and reflexive. Let L be a finite extension of K with uniformizing element π_L. Two elements $\gamma = \gamma_0 {\pi_\mathsf{L}}^u \in \mathsf{L}$ and $\delta = \delta_0 {\pi_\mathsf{L}}^w \in \mathsf{L}$ with $v(\gamma_0) = v(\delta_0) = 0$ are equivalent with respect to $\sim$ if and only if $u = w$ and $\gamma_0 \equiv \delta_0 \bmod (\pi_\mathsf{L})$.

2 Hensel Lifting and Newton Polygons

Hensel lifting yields a factorization of polynomials over local fields in certain cases and Newton polygons give valuable information about the roots of polynomials. We show how these two tools can be used to obtain proper factorizations in more general cases.

Theorem 1 (Hensel's Lemma). *Let $\Phi \in \mathscr{O}_\mathsf{K}[x]$ be monic. If $\Phi \equiv \varphi_1 \varphi_2 \mod (\pi)$ where φ_1 and φ_2 are coprime modulo π, then there is a factorization $\Phi = \Phi_1 \Phi_2$ with $\Phi_1 \equiv \varphi_1 \bmod (\pi)$ and $\Phi_2 \equiv \varphi_2 \bmod (\pi)$.*

For an example of an efficient Hensel lifting algorithm that lifts a factorization modulo (π) to a factorization modulo $(\pi)^s$ for any given s, see [20]. We can also obtain an approximation to a factorization of Φ if Hensel lifting can be applied to the characteristic polynomial of an element $\varphi + (\Phi)$ in $\mathscr{O}_\mathsf{K}[x]/(\Phi)$.

Definition 2. Let $\Phi(x) = \prod_{j=1}^N (x - \theta_j) \in \mathscr{O}_\mathsf{K}[x]$. For $\varphi \in \mathsf{K}[x]$ we define

$$\chi_\varphi(y) := \prod_{i=1}^N (y - \varphi(\theta_i)) = \operatorname{res}_x(\Phi(x), y - \varphi(x)) \in \mathsf{K}[y].$$

Proposition 1. *Let $\gamma \in \mathsf{K}[x]$ with $\chi_\gamma \in \mathscr{O}_\mathsf{K}[y]$. If $\underline{\chi}_\gamma$ has at least two distinct irreducible factors then Φ is reducible in $\mathscr{O}_\mathsf{K}[x]$.*

Proof. Suppose $\underline{\chi}_\gamma$ has at least two irreducible factors. Then, Hensel's lemma gives relatively prime monic polynomials $\chi_1 \in \mathscr{O}_\mathsf{K}[y]$ and $\chi_2 \in \mathscr{O}_\mathsf{K}[y]$ with $\chi_1\chi_2 = \chi_\gamma$. Reordering the roots $\theta_1, \ldots, \theta_N$ of Φ if necessary, we may write

$$\chi_1(y) = (y - \gamma(\theta_1)) \cdots (y - \gamma(\theta_r)) \text{ and } \chi_2(y) = (y - \gamma(\theta_{r+1})) \cdots (y - \gamma(\theta_N)),$$

where $1 \leq r < N$. It follows that

$$\Phi = \gcd(\Phi, \chi_1(\gamma)) \cdot \gcd(\Phi, \chi_2(\gamma))$$

is a proper factorization of Φ.

Definition 3 (Newton Polygon). Let $\Phi(x) = \sum_{i=0}^{N} c_i x^i$. The lower convex hull of $\{(i, v(c_i)) \mid 0 \leq i \leq N\}$ is the Newton polygon of Φ.

The negatives of the slopes of the segments of the Newton polygon of Φ are the valuations of the roots of Φ. The length of the segment (in x-direction) is the number of roots with this valuation. The negatives of the slopes of the Newton polygon of the characteristic polynomial χ_φ of $\varphi + (\Phi)$ are the valuations $v(\varphi(\theta))$ for the roots θ of Φ. Proposition 1 yields a constructive method for finding a factorization of Φ if χ_φ has more than one segment:

Corollary 1. *Let $\varphi \in \mathsf{K}[x]$ with $\chi_\varphi \in \mathscr{O}_\mathsf{K}[y]$. If there are roots θ and θ' of Φ such that $v(\varphi(\theta)) \neq v(\varphi(\theta'))$ then we can find two proper factors of $\Phi(x)$ over $\mathscr{O}_\mathsf{K}[x]$.*

Proof. Let Θ be the set of roots of Φ and let $h/e = \min\{v(\varphi(\theta)) \mid \theta \in \Theta\}$. Setting $\gamma := \varphi^e/\pi^h$ we get

$$\max\{v(\gamma(\theta)) \mid \theta \in \Theta \text{ and } \gamma(\theta) = 0\} > \min\{v(\gamma(\theta)) \mid \theta \in \Theta \text{ and } \gamma(\theta) = 0\} = 0.$$

Thus Proposition 1 yields a factorization of Φ.

3 Tamely Ramified Extensions

For all $f \in \mathbb{N}$ there is, up to isomorphism, a unique unramified extension of K of degree f. Such an extension can be generated by any monic polynomial of degree f that is irreducible over $\underline{\mathsf{K}}$.

Each totally and tamely ramified extension of degree e can be generated by a polynomial of the form $x^e - \gamma\pi_\mathsf{K}$ where $v(\gamma) = 0$. In certain cases we can obtain a generating polynomial of a tamely ramified subextension from a polynomial generating a totally ramified extension.

Proposition 2 ([7, Proposition 2.1]). *Let $n = e_0 p^m$ with $p \nmid e_0$ and let*

$$\varphi(x) = x^n + \sum_{i=1}^{n-1} \varphi_i x^i + \varphi_0 \in \mathscr{O}_\mathsf{K}[x]$$

be a polynomial whose Newton polygon is a line of slope $-h/n$, where $\gcd(h,n) = 1$. Let α be a root of φ. The maximum tamely ramified subextension M of $\mathsf{L} = \mathsf{K}(\alpha)$ of degree e_0 can be generated by the Eisenstein polynomial $x^{e_0} - (-\psi_0)^b \pi^{e_0 a}$ where a and b are integers such that $ae_0 + bh = 1$ and $\psi_0 \in \mathscr{O}_\mathsf{K}[x]$ with $\psi_0 \equiv \varphi_0 \bmod (\pi^{h+1})$.

This proposition also yields the standard form for generating polynomials of tamely ramified extensions mentioned above.

Corollary 2. *Let $\varphi(x) = \sum_{i=0}^{e} \varphi_i x^i \in \mathscr{O}_\mathsf{K}[x]$ be an Eisenstein polynomial and assume $p \nmid e$. If $\psi(x) = x^e + \psi_0$ with $\psi_0 \equiv \varphi_0 \bmod (\pi^2)$, then the extensions generated by $\varphi(x)$ and $\psi(x)$ are isomorphic.*

In our algorithm we need to find the composite of several tamely ramified extension of the same degree.

Proposition 3. *Let $\varphi_1(x) = x^e - \gamma_1\pi \in \mathscr{O}_\mathsf{K}[y]$ and $\varphi_2(x) = x^e - \gamma_2\pi \in \mathscr{O}_\mathsf{K}[x]$ with $p \nmid e$ and $v(\gamma_1) = v(\gamma_2) = 0$. Let θ_1 and θ_2 be a roots of φ_1 and φ_2 respectively. Then the composite of $\mathsf{K}(\theta_1)$ and $\mathsf{K}(\theta_2)$ is the unramified extension of $\mathsf{K}(\theta_1)$ whose degree is the least common multiple f of the degrees of the irreducible factors of $z^e - \underline{\frac{\gamma_2}{\gamma_1}} \in \underline{\mathsf{K}}[z]$.*

Proof. We have

$$\varphi_2(\theta_1 x) = (\theta_1 x)^e - \gamma_2\pi = \theta_1^e x^e - \gamma_2\pi = (\gamma_1\pi)x^e - \gamma_2\pi.$$

Dividing by $\gamma_1\pi$ gives $x^e - \frac{\gamma_2}{\gamma_1} = 0$. So the composite of $\mathsf{K}(\theta_1)$ and $\mathsf{K}(\theta_2)$ is the extension of $\mathsf{K}(\theta_1)$ that contains the roots of $\tau(x) = x^e - \frac{\gamma_2}{\gamma_1}$. Since $\gcd(x^e - \frac{\gamma_2}{\gamma_1}, \frac{d}{dx}(x^e - \frac{\gamma_2}{\gamma_1})) = \gcd(x^e - \frac{\gamma_2}{\gamma_1}, ex^{e-1}) = 1$ the polynomial $\underline{\tau}(z) = z^e - \underline{\frac{\gamma_2}{\gamma_1}} \in \underline{K(\theta_1)}[z]$ is squarefree. Denote by f the least common multiple of the degrees of the irreducible factors of $\underline{\tau}$. Then τ splits into linear factors in the unramified extension of $\mathsf{K}(\theta_1)$ of degree f, which is the composite of $\mathsf{K}(\theta_1)$ and $\mathsf{K}(\theta_2)$.

4 Partitions of Zeros and Types

Let $\Phi(x) = x^N + \sum_{i=0}^{N-1} c_i x^i \in \mathscr{O}_\mathsf{K}[x]$ be separable and squarefree and let $\Theta_0 = \{\theta_1, \ldots, \theta_N\}$ be the set of zeros of Φ in $\overline{\mathsf{K}}$. We want to find the splitting field of Φ, that is the smallest extension L/K over which Φ splits into linear factors. We successively generate a tower of subfields of L until we have found L.

In this process we partition the set of the zeros of Φ until all partitions contain exactly one zero of Φ. We obtain a tree with root node Θ_0 whose leaves consist of the sets containing exactly one zero of Φ. Every time we find sufficient information about a subfield of L we continue over the corresponding extension.

In our description of the algorithm, we focus on one path from the root node Θ_0 to a leaf. We indicate where branching occurs, thus describing the construction of all root paths in the tree. The nodes of such a root path are subsets of Θ_0, where, if Θ_{u+1} is a child of Θ_u then $\Theta_{u+1} \subseteq \Theta_u$. To each node Θ_u we attach a subfield K_u of the splitting field such that

$$\mathsf{K} \subset \mathsf{K}_1 \subset \cdots \subset \mathsf{K}_u \subset \cdots \subset \mathsf{L}.$$

In our algorithm, we construct these extensions as soon as we find that L has a certain subfield. When we find a divisor f of the inertia degree of L/K, we continue over the unramified extension of degree f. Similarly we construct an unramified extension of degree e when we find $\varphi \in \mathscr{O}_{\mathsf{K}_i}$ with $v(\varphi(\theta)) = \frac{h}{ep^\mu}$ where $\gcd(h,e) = \gcd(e,p) = 1$ and $e \neq 1$. To find generating polynomials of wildly ramified extensions, in addition to the field K_u, we attach a polynomial φ_u to the node Θ_u that is an approximation to a polynomial that generates the wildly ramified part of $\mathsf{K}_u(\theta)/\mathsf{K}_u$ for $\theta \in \Theta_u$. When the degree of φ_u is the ramification index of $\mathsf{K}_u(\theta)/\mathsf{K}_u$ then φ_u is an approximation to a unique factor of Φ that can be lifted to a factor $\widehat{\varphi}_u$ of Φ over K_u. We continue working over $\mathsf{K}_u[x]/(\widehat{\varphi}_u)$.

We start the first iteration with a linear monic polynomial $\varphi_1 = x + \beta \in \mathscr{O}_\mathsf{K}[x]$. The negatives of the slopes of the segments of the Newton polygon of $\Phi(x-\beta)$ are the valuations of the roots of Φ. Then

$$L_1 = \{v(\varphi_1(\theta)) \mid \theta \in \Theta_0\}$$

is the set of negatives of the slopes of the segments of the Newton polygon of $\Phi(x-\beta)$. We obtain a partition of Θ_0 into the sets $\{\theta \in \Theta_0 \mid v(\varphi_1(\theta)) = \lambda\}$ for $\lambda \in L_1$. By Corollary 1 each of these sets corresponds to a factor of Φ. For some $\lambda_1 \in L_1$ we set

$$\Theta_1^* = \{\theta \in \Theta_0 \mid v(\varphi_1(\theta)) = \lambda_1\}. \tag{1}$$

Without computing Θ_1^* explicitly we investigate the extensions generated by the factor $\prod_{\theta\in\Theta_1^*}(x-\theta)$ of Φ further.

Let $\lambda_1 = h_1/d_1$ in lowest terms. Then $v(\varphi_1^{d_1}(\theta)/\pi^{h_1}) = 0$ for all $\theta \in \Theta_1^*$. We set

$$R_1 = \left\{\underline{\rho} \in \underline{\mathsf{K}}[z] \;\middle|\; \underline{\rho} \text{ irreducible and } \underline{\rho}\left(\underline{\varphi_1^{d_1}(\theta)/\pi^{h_1}}\right) = \underline{0} \text{ for } \theta \in \Theta_1^*\right\}.$$

Let $f_1 = \operatorname{lcm}\{\deg \underline{\rho} \mid \underline{\rho} \in R_1\}$ and let K_1^* be the unramified extension of K of degree f_1. Then $\mathsf{K}_1^* \subset \mathsf{L}$. Over $\underline{\mathsf{K}}_1^*$ the polynomials in R_1 split into linear factors. Let

$$\Gamma_1 = \{\underline{\varphi_1^{d_1}(\theta)/\pi^{h_1}} \in \underline{\mathsf{K}}_1^* \mid \theta \in \Theta_1^*\}$$

be the set of zeros of the polynomials in R_1. By Proposition 1 each $\underline{\gamma} \in \Gamma_1$ corresponds to a factor of Φ over K_1^*. We continue to construct the splitting field of this factor. For some $\underline{\gamma}_1 \in \Gamma_1$ let

$$\Theta_1 = \left\{\theta \in \Theta_1^* \mid \underline{\varphi_1^{d_1}(\theta)/\pi^{h_1}} = \underline{\gamma}_1\right\}. \tag{2}$$

If $|\Theta_1| = 1$ then we have reached a leaf of the tree of partitions. Otherwise we write $d_1 = p^{\mu_1} e_1$ with $p \not| e_1$. If $e_1 = 1$ we set $\mathsf{K}_1 = \mathsf{K}_1^*$.

If $e_1 > 1$, for each $\gamma \in \Gamma_1$ we obtain a tamely ramified extension of K_1^* that is a subfield of L and let K_1 be the composite of these extensions and the unramified extension of K_1^* that contains the e_1-th roots of unity.

Over K_1 we have $\varphi_1^{p^{\mu_1}}(\theta) \sim \delta$ for some $\delta \in \mathsf{K}_1$ for all $\theta \in \Theta_1$. The ramification index of $\mathsf{K}_1(\theta)/\mathsf{K}_1$ is divisible by p^{μ_1} and we use $\varphi_2 = \varphi_1^{p^{\mu_1}}(\theta) - \delta$ as a first approximation to an irreducible factor of Φ that generates a wildly ramified extension of K_1. All relevant information from the considerations above can be recovered from the tuple

$$(\varphi_1, \lambda_1, \pi^h, y - \underline{\gamma}_1) \in \mathscr{O}_{\mathsf{K}}[x] \times \mathbb{Q} \times \mathsf{K}[x] \times \underline{\mathsf{K}}_1[y].$$

In the second iteration of the algorithm we use φ_2 to investigate the subfield of L that contains the roots in Θ_1 further. The set $L_2 = \{v(\varphi_2(\theta)) \mid \theta \in \Theta_1\}$ contains the slopes of the Newton polygon of the characteristic polynomial $\varphi_2 + \Phi$ over K_1. Each $\lambda \in L_2$ corresponds to a proper factor of Φ (compare Corollary 1). Let $\lambda_2 \in L_2$ be the slope of a segment of the Newton polygon and $\Theta_2^* = \{\theta \in \Theta_1 \mid v(\varphi_2(\theta)) = \lambda_2\}$ be the corresponding subset of zeros of Φ. We write $\lambda_2 = h_2/d_2$ in lowest terms and $d_2 = p^{\mu_2^*} e_2$ with $p \nmid e_2$ and set $\mu_2 = \min\{\mu_2^* - \mu_1, 0\}$.

We find $\psi_2 \in \mathsf{K}_1[x]$ with $\deg \psi_2 < \deg \varphi_2$ and $v_{\mathsf{K}_1}(\psi_2(\theta)) = h_2/p^{\mu_2^* - \mu_2}$. Let

$$R_2 = \left\{\underline{\rho} \in \underline{\mathsf{K}}_1[z] \;\middle|\; \underline{\rho} \text{ irreducible and } \underline{\rho}\left(\underline{\varphi_2^{e_2 p^{\mu_2}}(\theta)/\psi_2(\theta)}\right) = \underline{0} \text{ for } \theta \in \Theta_2^*\right\},$$

which is the set of irreducible factors of the characteristic polynomial $\varphi_2^{e_2 p^{\mu_2}}/\psi_2 + \Phi$ over $\underline{\mathsf{K}}_1$. By Proposition 1 each polynomial in R_2 corresponds to a factor of Φ. Let $f_2 = \operatorname{lcm}\{\deg \underline{\rho} \mid \underline{\rho} \in R_2\}$. The splitting field L of Φ contains the unramified extension K_2^* of degree f_2 of K_1. If $e_2 \neq 1$ L also contains the composite K_2 of certain tamely ramified extensions of K_2^* of degree e_2. Otherwise we set $\mathsf{K}_2 = \mathsf{K}_2^*$. Over K_2 the slope λ_2 of the segment becomes h_2/p^{μ_2}. Let

$$\Gamma_2 = \left\{\underline{\varphi_2^{p^{\mu_2}}(\theta)/\psi_2(\theta)} \in \underline{\mathsf{K}}_2^* \;\middle|\; \theta \in \Theta_2^*\right\}.$$

By Proposition 1 each $\gamma \in \Gamma_2$ corresponds to a factor of Φ over K_2 and a branch of in our tree of partitions. We follow the branch corresponding to some $\underline{\gamma}_2 \in \Gamma_2$ to the node

$$\Theta_2 = \left\{\theta \in \Theta_2^* \mid \underline{\varphi_2^{e_2 p^{\mu_2}}(\theta)/\psi_2(\theta)} = \underline{\gamma}_2\right\}.$$

If $|\Theta_2| = 1$, we do not need to investigate this branch of the tree of partitions further.

If $|\Theta_2| = \deg \varphi_2 = p^{\mu_1} > 1$ then φ_2 is an approximation to an irreducible factor of Φ of degree $\deg \varphi_2$ that defines a wildly ramified extension of K_2. We obtain this factor with single factor lifting [10], construct the corresponding wildly ramified extension, and start over at the root node Θ_0 over this extension with a linear polynomial φ_1.

Otherwise we use $\varphi_3 = \varphi_2^{p^{\mu_2}} - \gamma_2 \psi$ as the next approximation to an irreducible factor of Φ that generates a wildly ramified extension of K_2.

All the information obtained in this second iteration of the algorithm is included in or can be recovered from the information in

$$(\varphi_2, \lambda_2, \psi_2, z - \underline{\gamma}_2) \in \mathscr{O}_{\mathsf{K}_1}[x] \times \mathbb{Q} \times \mathsf{K}_1[x] \times \underline{\mathsf{K}}_2[z].$$

We inductively continue this process and keep track of the information computed in a sequence of such tuples called *types* (see [8, Definitions 1.21, 1.22 and section 2.1]). We generalize them insofar as we allow the coefficients of the polynomials in all tuples in a type to be in an extension of K.

Definition 4. Let $\Phi \in \mathscr{O}_{\mathsf{K}}[x]$ and let L/K be a finite. Let $t = (\varphi_i, \lambda_i, \psi_1, \underline{\rho}_i)_{1\le i\le u}$ where

(a) $\varphi_1 \in \mathscr{O}_{\mathsf{L}}[x]$ is linear, $\varphi_i \in \mathscr{O}_{\mathsf{L}}[x]$ is monic,
(b) $\lambda_i = h_i/d_i \in \mathbb{Q}$ in lowest terms,
(c) $\psi_i \in \mathsf{L}[x]$ with $\deg \psi_i < \deg \varphi_i$, and
(d) $\underline{\rho}_i \in \underline{\mathsf{L}}$ irreducible.

We call t an *extended type of Φ over* L, if for all θ in some subset Θ of the set of roots of Φ we have:

(e) $v(\varphi_i(\theta)) = \lambda_i$
(f) $v(\psi_i(\theta)) = e\lambda_i$ with $e = \frac{\operatorname{lcm}(d_1,\dots,d_i)}{\operatorname{lcm}(d_1,\dots,d_{i-1})}$,
(g) $\underline{\rho}_i(\underline{\varphi_i^e(\theta)/\psi_i(\theta)}) = \underline{0}$, and
(h) $v(\varphi_i(\theta)) > v(\varphi_{i-1}(\theta))$ and $\deg \varphi_i = e \cdot \deg \underline{\rho}_{i-1} \cdot \deg \varphi_{i-1}$ for $2 \le i \le u$.

We call $(\varphi_i, \lambda_i, \underline{\rho}_i)_{1\le i\le u}$ a type of Φ over L.

Definition 5. Let $t = (\varphi_i, \lambda_i, \psi_1, \underline{\rho}_i)_{1\le i\le u}$ be an extended type over L. We call t *optimal* if $\deg \varphi_{i-1} < \deg \varphi_i$ for $2 \le i \le u$ and *complete* if

$$\deg \varphi_u = p^{\max\{\mu_i | 1\le i\le u\}} \cdot \deg \underline{\rho}_1 \cdot \dots \cdot \underline{\rho}_u.$$

If $\deg \varphi_i$ is a power of p for all $1 \le i \le u$ then we call t a *wild type* of Φ over L.

A type t describes a root path in a tree of partitions of Θ_0. If $t = (\varphi_i, \lambda_i, \psi_i, \rho_i)_{1\le i\le u}$ a wild type over L with a corresponding subset of roots Θ_u, then $\lambda_i = h_i/\pi^{\mu_i^*}$ and $\operatorname{lcm}(p^{m_1}, \dots, p^{m_u}) = p^{\max\{m_1,\dots,m_u\}}$ divides the ramification index of $\mathsf{L}(\theta)$ for $\theta \in \Theta_u$. In our considerations all types are wild and the polynomials $\underline{\rho}$ are linear.

At the end of the u-th iteration of our algorithm we construct a polynomial φ_{u+1} of degree $p^{\max\{m_1,\dots,m_u\}}$ that is irreducible with $v(\varphi_{u+1}(\theta)) > v(\varphi_u(\theta))$ for $\theta \in \Theta_u$.

In the following sections we describe methods for constructing φ_{u+1}, finding $v(\varphi_{u+1}(\theta))$ for all $\theta \in \Theta_u$, constructing ψ_{u+1}, and finding $\underline{\rho}_{u+1}$. We will see that the sets $\Theta_0 \supset \Theta_1 \supset \dots \supset \Theta_u$ help in the understanding the algorithm, but will never be explicitly needed in actual computations.

If $t = (\varphi_i, \lambda_i, \psi_1, \underline{\rho}_i)_{1\le i\le u}$ is an extended type over L and $|\Theta_u| = p^{\max\{m_1,\dots,m_u\}}$, then φ_u is an approximation to a unique irreducible factor of Φ over L of degree $p^{\max\{m_1,\dots,m_u\}}$. Using the information in t, this approximation can be lifted to an approximation of arbitrary precision using single factor lifting (see [10]).

5 The First Iteration

We start our description of the construction of the splitting field of $\Phi \in \mathscr{O}_{\mathsf{K}}[x]$ of degree N with the first iteration. We have already gone through these steps in a more conceptual manner in the previous section. As before let $\varphi_1 \in \mathscr{O}_{\mathsf{K}}[x]$ be linear and monic, say $\varphi_1(x) = x + \beta$, and let Θ_0 denote the set of zeros of Φ in $\overline{\mathsf{K}}$. Although we use the zeros in Θ_0 in our exposition, they are not needed in any of the computations.

5.1 Newton Polygons I

The Newton polygon of $\Phi(x-\beta)$ yields the valuations of the zeros $\theta_1, \dots, \theta_N$ of Φ. Alternatively we can also use the φ_1-expansion of Φ:

Definition 6. Let $\Phi \in \mathcal{O}_{\mathsf{K}_u}[x]$ of degree N and $\varphi \in \mathcal{O}_{\mathsf{K}_u}[x]$ of degree n be monic polynomials. We call

$$\Phi = \sum_{i=0}^{\lceil N/n \rceil} a_i \varphi^i$$

with $\deg(a_i) < n$ the φ-expansion of Φ.

If $\Phi = \sum_{i=0}^{\lceil N/\deg \varphi_1 \rceil} a_i \varphi_1^i$ is the φ_1-expansion of Φ, then the polynomial $\chi_1(y) = \sum_{i=0}^{\lceil N/\deg \varphi_1 \rceil} a_i y^i$ has the zeros $\varphi_1(\theta)$ where $\theta \in \Theta_0$. We have

$$\chi_1(y) = \Phi(y-\beta) = \chi_{\varphi_1}(y) \tag{3}$$

with χ_{φ_1} as in Definition 2. The negatives of the slopes of the segments of the Newton polygon of χ_1 are the valuations of $\varphi_1(\theta)$ for $\theta \in \Theta_0$. We obtain a partition of Θ_0 into the sets

$$\{\theta \in \Theta \mid v(\varphi_1(\theta)) = \lambda\}$$

where λ is the negative of the slope of a segment of the Newton polygon of χ_1. To find the splitting field one continues the algorithm for each of the sets in this partition.

5.2 Residual Polynomial I

Residual (or associated) polynomials were first introduced by Ore [16, 13]. They yield information about the unramified part of the extension generated by the zeros of Φ. Let S be a segment of the Newton Polygon of $\chi_1(y) = \sum_{i=1}^{N} a_i y^i$ (see (3)), let m_1 be the length of S, $(k, v(a_k))$ and $(k+m_1, v(a_{k+m_1}))$ its endpoints, and $\lambda_1 = \frac{v(a_k)-v(a_{k+n})}{m_1} = \frac{h_1}{d_1}$ where $\gcd(h_1, d_1) = 1$ the negative of its slope. If

$$\Theta_1^* = \{\theta \in \Theta_0 \mid v(\varphi_1(\theta)) = \lambda_1\},$$

then $|\Theta_1^*| = m_1$. We evaluate χ_1 at $\varphi_1(\theta)y$ and obtain a polynomial whose Newton polygon has a horizontal segment of length m_1. For $\theta \in \Theta_1^*$ we consider $\chi_1(\varphi_1(\theta)y)$. Using the equivalence relation from Definition 1 we obtain

$$\chi_1(\varphi_1(\theta)y) = \sum_{i=0}^{N} a_i(\varphi_1(\theta)y)^i \sim \sum_{i=k}^{k+m_1} a_i \varphi_1^i(\theta) y^i \sim \sum_{j=0}^{m_1/d_1} a_{jd_1+k} \varphi_1^{jd_1+k}(\theta) y^{jd_1+k}$$

The last equivalence holds, because the x-coordinates of the points on the segment of the Newton polygon are of the form $k + jd_1$ with $0 \le j \le m_1/d_1$. Furthermore for $0 \le j \le m_1/d_1$ we have $v(a_{jd_1+k}\varphi_1^{jd_1+k}(\theta)) = v(a_k \varphi_1^k(\theta))$ and the polynomial is divisible by y^k. Dividing $\chi_1(\varphi_1(\theta)y)$ by $\pi^{v(a_k)}\varphi_1^k(\theta)y^k$ we obtain a polynomial of degree m_1/d_1 that is equivalent to a polynomial whose leading coefficient and constant coefficient have valuation zero:

$$\frac{\chi_1(\varphi_1(\theta)y)}{\pi^{v(a_k)}\varphi_1^k(\theta)y^k} \equiv \sum_{j=0}^{m_1/d_1} \frac{a_{jd_1+k}\varphi_1^{jd_1}(\theta)y^{jd_1}}{\pi^{v(a_k)}} \bmod (\pi).$$

For $\varepsilon = \varphi_1^{d_1}/\pi^{h_1}$ we have $v(\varepsilon(\theta)) = v(\varphi_1^{d_1}(\theta)/\pi^{h_1}) = 0$. Substitution of $\varphi_1^{d_1}$ by $\varepsilon\pi^{h_1}$ yields

$$\frac{\chi_1(\varphi_1(\theta)y)}{\pi^{v(a_k)}\varphi_1^k(\theta)y^k} \equiv \sum_{j=0}^{m_1/d_1} \frac{a_{jd_1+k}\pi^{jh_1}\varepsilon^j y^{jd_1}}{\pi^{v(a_k)}} \bmod (\pi).$$

Replacing εy^{d_1} by z and considering the resulting polynomial over $\underline{\mathsf{K}}$ yields the residual polynomial of S:

$$\underline{A}_1(z) := \sum_{j=0}^{m_1/d_1} \underline{a_{jd_1+k}\pi^{jh_1-v(a_k)}} z^j \in \underline{\mathsf{K}}[z].$$

For $\theta \in \Theta_1^*$ we have that $\underline{\varphi_1^{d_1}(\theta)/\pi^{h_1}} \in \overline{\underline{\mathsf{K}}}$ is a zero of $\underline{A}_1$.

5.3 Unramified Extension I

Let f_1 be the least common multiple of the degrees of the irreducible factors of $\underline{A}$. The unramified extension K_1^* of K of degree f_1 is a subfield of L and $\underline{A}$ splits into linear factors over the residue class field $\underline{\mathsf{K}}_1^*$ of K_1.

Let Γ_1 be the set of zeros of $\underline{A}_1$ in K_1. By Proposition 1 we can obtain a proper factor of Φ over K_1 for each $\gamma \in \Gamma_1$. For some $\gamma_1 \in \Gamma_1$ let

$$\Theta_1 = \{\theta \in \Theta_1^* \mid \underline{\varphi_1(\theta)^{d_1}/\pi^{h_1}} = \underline{\gamma}_1\}.$$

Our choice of γ_1 determines on which branch of the tree of partitions of Θ to follow.

5.4 Tamely Ramified Extension I

For all $\theta \in \Theta_1$ we have $v(\varphi_1(\theta)) = \lambda_1 = h_1/d_1 = h_1/(e_1 p^{\mu_1^*})$ where $\gcd(h_1, d_1) = \gcd(e_1, p) = 1$.

If $e_1 = 1$ is a power of p we set $\mathsf{K}_1 = \mathsf{K}_1^*$.

If $e_1 \neq 1$ is not a power of p, then the slope $-h_1/(e_1 p^{\mu_1^*})$ together with $\underline{\gamma}_1$ give enough information to provide a generating polynomial of a tamely ramified subfield $\mathsf{K}_1/\mathsf{K}_1^*$ of L. Let γ_1 be a lift $\underline{\gamma}_1$ to $\mathscr{O}_{\mathsf{K}_1}$. We have $\frac{\theta^{d_1}}{\pi^{h_1}} \sim \gamma_1$, so $\left(\theta^{p^{\mu_1}}\right)^{e_1} \sim \gamma_1 \pi^{h_1}$. Therefore for $\delta = \theta^{p^{\mu_1}}$, we have $\delta^{e_1} \sim \gamma_1 \pi^{h_1}$. The Newton polygon of $\tau^*(x) = x^{e_1} - \gamma_1 \pi^{h_1}$ is a line of slope $-h_1/e_1$ with $\gcd(h_1, e_1) = 1$. By Proposition 2, if a and b are integers such that $ae_1 + bh_1 = 1$, the extension generated by τ^* is generated by the Eisenstein polynomial

$$\tau = x^{e_1} + (-1)^b (\gamma_1 \pi^{h_1})^b \pi^{e_1 a} = x^{e_1} + (-1)^b \gamma_1^b \pi^{bh_1 + ae_1} = x^{e_1} + (-\gamma_1)^b \pi.$$

As the splitting field of τ contains the e_1-th roots of unity we continue the computations over the tamely ramified extension K_1 given by τ over the unramified extension of K_1^* that contains the e_1-th roots of unity. Using proposition 3 we can obtain the composite of the tamely ramified extensions of degree e_1 given by all $\gamma \in \Gamma_1$.

5.5 Next Approximation I

After the considerations in section 5.4 above we can assume $\lambda_1 = h_1/d_1 = h_1/p^{\mu_1}$, as either d_1 was a power of p already or, if K_1 is a tamely ramified extension of K_1^*, recomputing the Newton polygon gives a segment with slope $-\lambda = -h_1/p^{\mu_1}$. In the latter case we also need to recompute the residual polynomial $\underline{A}$ in 5.2, which will be of higher degree. Again let Γ_1 be the set of zeros of $\underline{A}$, and $\underline{\gamma}_1 \in \Gamma_1$. Denote by γ_1 a lift of $\underline{\gamma}_1$ to $\mathscr{O}_{\mathsf{K}_1}$ and set

$$\Theta_1 = \{\theta \in \Theta_1^* \mid \underline{\varphi_1^{d_1}(\theta)/\pi_{\mathsf{K}_1}^{h_1}} = \underline{\gamma}_1\}.$$

We have the relation $\varphi_1^{p^{\mu_1}}(\theta) \sim \gamma_1 \pi_{\mathsf{K}_1}^{h_1}$ for all $\theta \in \Theta_1$. Now

$$\varphi_2 = \varphi_1^{p^{\mu_1}} - \gamma_1 \pi_{\mathsf{K}_1}^{h_1}$$

is an approximation to a polynomial generating the wildly ramified subextension of $\mathsf{K}_1(\theta)$ with

$$v_{\mathsf{K}_1}(\varphi_2(\theta)) = v_{\mathsf{K}_1}(\varphi_1^{p^{\mu_1}}(\theta) - \gamma_1 \pi_{\mathsf{K}_1}^{h_1}) > h_1 \geq h_1/d_1 = v_{\mathsf{K}_1}(\varphi_1(\theta)).$$

5.6 Valuations I

Let $a = \sum_{j=0}^{d_1} a_j \varphi_1^j \in \mathsf{K}_1[x]$ with $\deg a < \deg \varphi_2 = d_1 = p^{\mu_1}$. As the valuations

$$v_{\mathsf{K}_1}(\varphi_1(\theta)) = \frac{h_1}{d_1}, \ldots, v_{\mathsf{K}_1}(\varphi_1^{d_1-1}(\theta)) = \frac{(d_1-1)h_1}{d_1}$$

are distinct (and not in $\mathbb{Z}$),

$$v_{\mathsf{K}_1}(a(\theta)) = \min_{0 \leq j \leq \deg d_1 - 1} v_{\mathsf{K}_1}(a_j(\theta)\varphi_1^j(\theta)) = \min_{0 \leq j \leq \deg d_1 - 1} v_{\mathsf{K}_1}(a_j(\theta)) + j(h_1/d_1).$$

Furthermore, if we only consider the terms with valuation $v_{\mathsf{K}_1}(a(\theta))$ we obtain a polynomial that at θ is equivalent to $a(x)$. That is, if $v_{\mathsf{K}_1}(a_j(\theta)) + j(h_1/d_1) = v_{\mathsf{K}_1}(a(\theta))$ then we have $a(\theta) \sim a_j(\theta) + \varphi_1^{j(h_1/d_1)}$ for $\theta \in \Theta_1$.

5.7 Polynomials with given Valuations I

The data computed in the first iteration allows us, given $c \in \mathbb{Z}$ and $d \in \mathbb{N}$ with $\gcd(c,d) = 1$ and $d \mid d_1 = p^{\mu_1}$, to find $\psi(x) \in \mathsf{K}[x]$ with $v(\psi(\theta)) = \frac{c}{d}$ for $\theta \in \Theta_1$ and $\deg \psi < d_1$.

If $d = 1$ then $\psi(x) := \pi_{\mathsf{K}_1}^{s_\pi}$ with $s_{\pi_{\mathsf{K}_1}} = c$ has the property $v_{\mathsf{K}_1}(\psi(\theta)) = \frac{c}{d}$ for all $\theta \in \Theta_1$.

Otherwise d is a proper divisor of d_1. Find $s_1 \in \mathbb{Z}$ such that $s_1 h_1 \equiv \frac{c}{d} d_1 \bmod d_1$ and let $s_0 = \frac{c}{d} - v(\varphi_1^{s_1}(\theta)) \in \mathbb{Z}$. Now for $\psi(x) := \pi_{\mathsf{K}_1}^{s_0} \varphi_1(x)^{s_1} \in \mathsf{K}[x]$ we have $v(\psi(\theta)) = \frac{c}{d}$ for $\theta \in \Theta_1$.

5.8 Arithmetic I

We consider the arithmetic of polynomials of degree less than $d_1 = p^{\mu_1}$.

Let $a(x) = \sum_{i=0}^{d_1-1} a_i x^i$ and $\tau(x) = x^{s_1} \pi^{s_0}$ with $s_0, s_1 \in \mathbb{Z}$. Multiplication gives $a(x)\tau(x) = \sum_{i=0}^{d_1-1} a_i \pi_{\mathsf{K}_1}^{s_\pi} x^{i-s_1}$ which in general is a rational function or a polynomial of degree greater than $d_1 - 1$.

As $v(\varphi_1^{d_1}(\theta)/\pi_{\mathsf{K}_1}^{h_1} - \gamma_1) = 0$ we have the relation

$$\varphi_1^{d_1}(\theta) \sim \gamma_1 \pi_{\mathsf{K}_1}^{h_1}.$$

So by repeatedly substituting $\varphi_1^{d_1}$ by $\gamma_1 \pi_{\mathsf{K}_1}^{h_1}$ we obtain a polynomial $b(x) \in \mathsf{K}[x]$ with $\deg b < d_1$ such that $b(\theta) \sim a(\theta)\psi(\theta)$.

6 The u-th Iteration

We describe a general iteration of the algorithm. Let $t = (\varphi_i, \lambda_i, \psi_i, y - \gamma_i)_{1 \leq i \leq u-1}$ be a wild extended type of Φ over K_{u-1} that is not complete. We write $\lambda_i = h_i/p^{\mu_i^*}$ with $\gcd(h_i, e_i p) = \gcd(e_i, p) = 1$ and set $M_{u-1} = \max\{\mu_i^* | 1 \leq i \leq$

$u-1\}$ and $\mu_{u-1} = M_{u-1} - M_{u-2}$. Assume that we have found the next approximation $\varphi_u \in \mathcal{O}_{\mathsf{K}_{u-1}}[x]$ to a generator of a wildly ramified extension with $\deg \varphi_u = p^{M_{u-1}}$ and $v_{\mathsf{K}_u}(\varphi_u(\theta)) > v_{\mathsf{K}_u}(\varphi_{u-1}(\theta))$ for all $\theta \in \Theta_{u-1}$.

We assume that we have the following methods, which rely on the data computed in the previous steps. For each method the base case is described in section 5 and the general case in this section. Because of the recursive nature of the algorithm we use forward references in our representation.

`Valuation` given $a(x) \in \mathsf{K}_u[x]$ with $\deg a < \deg \varphi_u = p^{M_{u-1}}$ finds $v_{\mathsf{K}_u}(a(\theta))$ for $\theta \in \Theta_{u-1}$ (see sections 5.6, 6.7 and Algorithm 1).

`PolynomialWithValuation` given $c \in \mathbb{Z}$ and $d \in \mathbb{N}$ with $d \mid p^{M_u}$ finds $\psi(x) \in \mathsf{K}_u[x]$ with $\deg \psi < \deg \varphi_u = p^{M_{u-1}}$ such that $v_{\mathsf{K}_u}(\psi(\theta)) = \frac{c}{d}$ for all $\theta \in \Theta_{u-1}$ (see sections 5.7, 6.8 and Algorithm 3).

Furthermore we assume that we have methods for arithmetic and reduction of polynomials of degree less than p^{M_u} in their representations as sums of power products (see sections 5.8, 6.9 and Algorithm 4 `reduce`).

In the u-th iteration of the algorithm we investigate the properties of φ_u and construct the next approximation $\varphi_{u+1} \in \mathcal{O}_{\mathsf{K}_u}[x]$ to a polynomial defining a wildly ramified subfield of the splitting field.

6.1 Newton Polygon II

We use the φ_u-expansion of Φ to find the valuations $v_{\mathsf{K}_{u-1}}(\varphi_u(\theta))$ for $\theta \in \Theta_{u-1}$. Let $l_u = \lceil N/\deg \varphi_u \rceil$ and $\Phi = \sum_{i=0}^{l_u} a_i \varphi_u^i$ be the φ_u-expansion of Φ. For each root $\theta \in \Theta_{u-1}$ we have

$$\Phi(\theta) = \sum_{i=0}^{l_u} a_i(\theta)\varphi_u^i(\theta) = 0.$$

Hence

$$\chi_u = \sum_{i=0}^{l_u} a_i(\theta) y^i \in \overline{\mathsf{K}}[y]$$

has the zeros $\varphi_u(\theta)$ for $\theta \in \Theta_{u-1}$.

The method `Valuation` returns the valuations of the coefficients $a_i(\theta)$ of χ_u and with these the Newton polygon of χ_u yields the valuations of $\varphi_u(\theta)$ for $\theta \in \Theta_{u-1}$. We obtain a partition of Θ_{u-1} into the subsets $\{\theta \in \Theta_{u-1} \mid v(\varphi(\theta)) = \lambda\}$ where λ is the negative of the slope of a segment of the Newton polygon of χ_u. By Corollary 1 each segment of the Newton polygon of χ_u, and thus each set in the partition, corresponds to a factor of $\Phi(x)$.

Definition 7. The Newton polygon of χ_u is called the Newton polygon of Φ with respect to φ_u. It is also called a *Newton polygon of higher order* [14, 8].

6.2 Residual Polynomial II

Let S be a segment of the Newton Polygon of χ_u of length m_u with endpoints $(k, v_{\mathsf{K}_{u-1}}(a_k(\theta)))$ and $(k+m, v_{\mathsf{K}_{u-1}}(a_{k+m_u}(\theta)))$ for $\theta \in \Theta_{u-1}$. Let

$$\lambda_u = \frac{v_{\mathsf{K}_{u-1}}(a_k(\theta)) - v_{\mathsf{K}_{u-1}}(a_{k+n}(\theta))}{m_u} = \frac{h_u}{d_u},$$

where $\gcd(h_u, d_u) = 1$ and let $\Theta_u^* = \{\theta \in \Theta_{u-1} \mid v_{\mathsf{K}_{u-1}}(\varphi_u(\theta)) = \lambda_u\}$. We have $|\Theta_u^*| = m_u \deg \varphi_u$.

Let e_u and μ_u^* such that $d_u = e_u p^{\mu_u^*}$ with $\gcd(e_u, p) = 1$ and $M = \sum_{i=0}^{u-1} \mu_i = \max\{\mu_i^* \mid \mu_i^*\}$, $\nu = \min\{\mu^*, M\}$, and $\mu_u = \max\{\mu_u^* - M, 0\}$. The method `PolynomialWithValuation` gives $\psi_u \in \mathsf{K}_{u-1}[x]$ with

$$v_{\mathsf{K}_{u-1}}(\psi_u(\theta)) = v_{\mathsf{K}_{u-1}}\left(\varphi_u^{e_u p^{\mu_u}}\right) = e_u p^{\mu_u} \lambda_u = h_u / p^{\nu}$$

for $\theta \in \Theta_u^*$. We have

$$\chi_u(\varphi_u(\theta)) \sim \sum_{i=k}^{k+m} a_i(\theta)\varphi_u^i(\theta)x^i \sim \sum_{j=0}^{m/(e_u p^{\mu_u})} a_{je_u p^{\mu_u}+k}(\theta)\varphi_u^{je_u p^{\mu_u}+k}(\theta)x^{je_u p^{\mu_u}+k}$$

The last equivalence holds, because the x-coordinates of the points on the segment of the Newton polygon are of the form $k + je_u p^{\mu_u}$ ($0 \le j \le m/(e_u p^{\mu_u})$). Division by $\varphi_u^k y^k$ yields

$$\frac{\chi_u(\varphi_u(\theta))}{\varphi_u^k(\theta)y^k} \sim \sum_{j=0}^{m/(e_u p^{\mu_u})} a_{je_u p^{\mu_u}+k}(\theta)\varphi_u^{je_u p^{\mu_u}}(\theta)y^{je_u p^{\mu_u}}.$$

For $\gamma = \varphi_u \theta^{e_u p^{\mu_u}}/\psi_u(\theta)$ we have $v_{\mathsf{K}_{u-1}}(\gamma) = v_{\mathsf{K}_{u-1}}(\varphi_u^{e_u p^{\mu_u}}(\theta)/\psi_u(\theta)) = 0$. By substituting $\gamma\psi_u(\theta)$ for $\varphi_u^{e_u p^{\mu_u}}(\theta)$ we get

$$\frac{\chi(\varphi_u(\theta)y)}{\varphi_u^k(\theta)y^k} \sim \sum_{j=0}^{m/(e_u p^{\mu_u})} a_{je_u p^{\mu_u}+k}(\theta)(\gamma\psi_u^j(\theta))y^{je_u p^{\mu_u}}$$

The method `PolynomialWithValuation` gives a polynomial $\tau \in \mathsf{K}_{u-1}[x]$ with $v_{\mathsf{K}_{u-1}}(\tau(\theta)) = v_{\mathsf{K}_{u-1}}(a_k(\theta))$ for $\theta \in \Theta_{u-1}$. Replacing $\gamma y^{e_u p^{\mu_u}}$ by y and division by $\tau(\theta)$ yields

$$A(y) = \sum_{j=0}^{m/(e_u p^{\mu_u})} \frac{a_{je_u p^{\mu_u}+k}(\theta)\psi_u^j(\theta)}{\tau(\theta)} y^j.$$

By construction $v_{\mathsf{K}_{u-1}}\left(\frac{a_{je_u p^{\mu_u}+k}(\theta)\psi_u^j(\theta)}{\tau(\theta)}\right) \ge 0$, in particular $v_{\mathsf{K}_{u-1}}\left(\frac{a_k(\theta)\psi_u(\theta)}{\tau(\theta)}\right) = 0$ and $v_{\mathsf{K}_{u-1}}\left(\frac{a_{k+m}(\theta)\psi_u^{m/(e_u p^{\mu_u})}(\theta)}{\tau(\theta)}\right) = 0$. So the polynomial $\underline{A}(z) \in \underline{\mathsf{K}}_{u-1}[z]$ has degree $m_u/(e_u p^{\mu_u})$. It is called the residual polynomial of S.

6.3 Unramified Extension II

Let f_u be the least common multiple of the degrees of the irreducible factors of $\underline{A}$ and let K_u^* be the unramified extension of K_{u-1} of degree f_u. Over $\underline{\mathsf{K}}_u^*$ the residual polynomial $\underline{A}$ splits into linear factors. We denote by Γ_u the set of lifts of zeros of $\underline{A}$ to K_u and partition Θ_u^* into the sets of the form

$$\Theta_u = \left\{ \theta \in \Theta_u^* \;\middle|\; \underline{\frac{\varphi_u^{e_u p^{\mu_u}}}{\psi_u}}(\theta) = \underline{\gamma}_u \right\}. \tag{4}$$

where $\gamma_u \in \Gamma_u$. We have $|\Theta_u| = g \deg \varphi_u$, where g is the multiplicity of $\underline{\gamma}_u$ as a zero of $\underline{A}$.

6.4 Tamely Ramified Extension II

For $\theta \in \Theta_u$, we have $\underline{\left(\varphi_u^{e_u p^{\mu_u}}/\psi_u\right)}(\theta) = \underline{\gamma_u}$, and therefore $\left(\varphi_u^{p^{\mu^u}}(\theta)\right)^{e_u} \sim \gamma_u\psi_u(\theta)$. For $\widetilde{\varphi} = \varphi^{p^{\mu_u}}$ we have $\widetilde{\varphi}^{e_u}(\theta) \sim \gamma_u\psi(\theta)$. As in section 6.2 let $\nu = \min\{\mu_u^*, M_{u-1}\} = \mu_u^* - \mu_u$. Since

$$v_{\mathsf{K}_{u-1}}(\psi_u^{p^\nu}(\theta)) = p^\nu(e_u p^{\mu_u}\lambda_u) = p^{\mu_u^*-\mu_u} e_u p^{\mu_u} \frac{h_u}{e_u p^{\mu_u^*}} = h_u,$$

there is $\delta \in \mathcal{O}_{\mathsf{K}_{u-1}}^{\times}$ such that $\psi_u^{p^{\mu_u^*-\mu_u}}(\theta) \sim \delta \pi_{\mathsf{K}_{u-1}}^{h_u}$. With $\widehat{\varphi} = \widetilde{\varphi}^{p^v}$ we get

$$\widehat{\varphi}^{e_u}(\theta) = \widetilde{\varphi}^{p^v} \sim \gamma_u^{p^v} \psi^{p^{v_u}}(\theta) \sim \gamma_u^{p^v} \delta \pi^{h_u}.$$

Thus the roots of $\tau^*(x) = x^{e_u} - \gamma_u^{p^v} \delta \pi^{h_u}$ are in the splitting field L. Since the Newton polygon of τ^* is a line of slope $-h_u/e_u$ where $\gcd(h_u, e_u) = 1$, the polynomial τ^* defines a tamely ramified extension of K_u^* of degree e_u. By Proposition 2 it is generated by the Eisenstein polynomial

$$\tau(x) = x^{e_u} + (-1)^b (\gamma_u^{p^v} \delta \pi^{h_u})^b \pi^{e_u a} = x^{e_u} + (-1)^b \gamma_u^{bp^v} \delta^b \pi^{bh_u + ae_u} = x^{e_u} + (-\gamma_u^{p^v} \delta)^b \pi$$

where a and b are integers such that $ae_u + bh_u = 1$.

6.5 Wildly Ramified Extension

Now either d_u was a power of p already or, after extending K_u^* the slope of the segment of the Newton polygon of χ_u corresponding to S now is $-h_u/p^{\mu_u^*}$ over K_u. If K_u is a tamely ramified extension of K_u^* we would need to recompute the associated polynomial $\underline{A}$ and to obtain a residual polynomial of higher degree. Hence we assume $\lambda_u = h_u/d_u = h_u/p^{\mu_u^*}$.

If $|\Theta_u| = \deg \varphi_u = 1$ we have reached a leaf of the tree of partitions.

If $|\Theta_u| > \deg \varphi_u$ we continue with constructing a next approximation to a polynomial that generates the wildly ramified part of $\mathsf{K}_u(\theta)$ for $\theta \in \Theta_u$.

If $|\Theta_u| = \deg \varphi_u = p^{M_{u-1}} \neq 1$ then φ_u is an approximation to a unique irreducible factor $\widehat{\varphi}$ of degree $p^{M_{u-1}}$ of Φ over K_u. We obtain $\widehat{\varphi}$ using single factor lifting [10], which generates a totally and wildly ramified extension M of K_u over which Φ has at least one linear factor. Now for $1 \leq i \leq u-1$ with $\mu_i > 0$ the data in $t = (\varphi_i, \lambda_i, \psi_i, y - \gamma_i)_{1 \leq i \leq u-1}$ and the slopes $-\lambda_i$, and thus ψ_i and $\underline{A}_i$ are not correct over M. Thus we continue our computations with the type $t = (\varphi_i, \lambda_i, \psi_i, y - \gamma_i)_{1 \leq i \leq j}$ over M, where $1 \leq j \leq u-1$ is such that $\mu_i = 0$ for $1 \leq i \leq j$.

6.6 The Next Approximation II

As above in section 6.5 we assume that $\lambda_u = h_u/d_u = h_u/p^{\mu_u^*}$ and as in section 6.2 let $\psi_u \in \mathsf{K}_{u-1}[x]$ with $v(\psi_u(\theta)) = h_u/p^{\mu_u^*}$ for $\theta \in \Theta_u \subseteq \Theta_{u-1}$. If Γ_u denotes the set of zeros of the residual polynomial and $\gamma_u \in \Gamma_u$, then $\varphi_u^{p^{\mu_u^*}}(\theta) \sim \gamma_u \psi_u$ for all $\theta \in \Theta_u$. The polynomial

$$\varphi_{u+1} = \varphi_u^{p^{\mu_u^*}} - \gamma_u \psi_u$$

is an approximation to a polynomial that generates the wildly ramified subextension of $\mathsf{K}_u(\theta)$ with

$$v_{\mathsf{K}_u}(\varphi_u(\theta)) = v_{\mathsf{K}_u}(\varphi_u^{p^{\mu_u^*}}(\theta) - \gamma_u \psi_u) = v_{\mathsf{K}_u}(\psi_u) = h_u/p^v \geq h_u/d_u = v_{\mathsf{K}_u}(\varphi_u(\theta))$$

for all $\theta \in \Theta_u$.

6.7 Valuations II

For $b(x) \in \mathsf{K}_{u-1}[x]$ with $\deg b < p^{M_{u-1}}$ the method `Valuation` yields $v_{\mathsf{K}_{u-1}}(a(\theta))$ for $\theta \in \Theta_u \subset \Theta_{u-1}$. Let $a \in \mathsf{K}_u[x]$ with $\deg a < p^{M_u}$ and $m = \lceil \deg a / \deg \varphi_u \rceil$. Let $a = \sum_{j=0}^{m} a_j \varphi_u^j$ with $\deg a_j < \deg \varphi_u = p^{M_{u-1}}$ be the φ_u-expansion of a. As the valuations

$$v_{\mathsf{K}_u}(\varphi_u(\theta)) = \frac{h_1}{d_u}, \ldots, v_{\mathsf{K}_u}(\varphi_u^{p^{\mu_u}-1}(\theta)) = \frac{(p^{\mu_u}-1)h_u}{d_u}$$

are distinct (and not in $\frac{1}{p^{M_{u-1}}}\mathbb{Z}$) we have

$$v_{\mathsf{K}_u}(a(\theta)) = \min_{0\le j\le m} v_{\mathsf{K}_u}\left(a_j(\theta)\varphi_u^j(\theta)\right) = \min_{0\le j\le m} v_{\mathsf{K}_u}\left(a_j(\theta) + j(h_u/p^{\mu_u})\right).$$

Furthermore, if we only consider the terms with valuation $v_{\mathsf{K}_u}(a(\theta))$ we obtain a polynomial that at θ is equivalent to $a(x)$. That is, for $J = \{j \mid v_{\mathsf{K}_u}(a_j) + jh_u/d_u = v_{\mathsf{K}_u}(a(\theta))\}$ and $b(x) = \sum_{j\in J} a_j(x)\varphi_u^j(x)$ we have $a(\theta) \sim b(\theta)$ for $\theta \in \Theta_u$.

6.8 Polynomials with given Valuations II

Let $c \in \mathbb{Z}$ and $d \in \mathbb{N}$ with $d \le M_u$. We describe how $\psi(x) \in \mathsf{K}_u[x]$ with $v_{\mathsf{K}_u}(\psi(\theta)) = \frac{c}{p^d}$ and $\deg\psi < \deg\varphi_u = p^{M_{u-1}}$ can be constructed. Assume that for $c' \in \mathbb{Z}$ and $d' \in \mathbb{N}$ with $d' < M_{u-1}$ we can find $\psi'(x) \in \mathsf{K}[x]$ with $v_{\mathsf{K}_u}(\psi'(\theta)) = \frac{c'}{p^{d'}}$ for $\theta \in \Theta_u \subseteq \Theta_{u-1}$.

If $d < M_{u-1}$ then we can find $\psi(x)$ by our assumption. Otherwise we have $M_{u-1} < d \le M_u$ and we find $s_u \in \mathbb{Z}$, $0 \le s_u < p^{\mu_u}$ such that

$$s_u h_u \equiv c p^{M_u - d} \bmod p^{\mu_u}$$

and set $\frac{c'}{p^{d'}} = \frac{c}{p^d} - s_u v_{\mathsf{K}_u}(\varphi_u)$ in lowest terms. As $d' < M_{u-1}$ the assumption yields $\psi'(x) \in \mathsf{K}_u[x]$ with $v_{\mathsf{K}_u}(\psi'(\theta)) = \frac{c'}{p^{d'}}$. Thus we get $\psi(x) = \varphi_u^{s_u}(x)\psi'(x)$ with $v_{\mathsf{K}_u}(\psi(\theta)) = \frac{c}{p^d}$ and $\deg\psi < p^{M_u}$.

6.9 Arithmetic II

We consider the arithmetic of polynomials of degree less than p^{M_u}. Clearly addition and subtraction of two such polynomials again yield polynomials of degree less than p^{M_u}. We assume that methods for handling polynomials of degree less than $p^{M_{u-1}}$ are available. That is, given $a(x) \in \mathsf{K}_{u-1}$ and $b(x) \in \mathsf{K}_{u-1}$ we can find a polynomial $c \in \mathsf{K}_{u-1}[x]$ with $\deg c < p^{M_{u-1}}$ such that $c(\theta) \sim a(\theta)b(\theta)$ for $\theta \in \Theta_u \subseteq \Theta_{u-1}$.

Let $a(x) = \sum_{i=0}^{p^{M_u}-1} a_i(x)\varphi_u^i$ and $b = \varphi_u^s b'$ with $s \in \mathbb{Z}$, $b' \in \mathsf{K}_u[x]$ of degree less than $p^{M_{u-1}}$. Multiplication gives $a(x)b(x) = \sum_{i=0}^{p^{M_u}-1} a_i b' \varphi_u^{i+s}$ which in general is a rational function or a polynomial of degree greater than $p^{M_u} - 1$. We have $\underline{\varphi_u^{e_u}(\theta)/\psi_u(\theta)} = \underline{\gamma}_u$, thus

$$\varphi_u^{e_u}(\theta) \sim \gamma\psi_u(\theta)$$

for any $\gamma \in \mathsf{K}_u$ with $\underline{\gamma} = \underline{\gamma}_u$. Repeated substitution of $\varphi_u^{p^{\mu_u}}$ by $\gamma\psi_u$ reduces the exponents of φ_u to s' with $0 \le s' < p^{\mu_u}$. The coefficient of $\varphi_u^{s'}$ now is the product of polynomials of degree less than p^{M_u}, which can be reduced to a polynomial of degree less than p^{M_u} by our assumption. Thus we obtain a polynomial $b(x) \in \mathsf{K}[x]$ with $\deg b < p^{M_u}$ such that $b(\theta) \sim a(\theta)\psi_u(\theta)$. If $v_{\mathsf{K}_u}(a(\theta)) = 0$ recursive application of these reductions yield $\beta \in \mathsf{K}_u$ with $a(\theta) \sim \beta$.

7 Algorithms

In our formulation of the algorithm we add a fifth component to the extended types from Definition 4, making all the information from previous iterations of the algorithm needed in later iterations readily available. We denote the subfield of the splitting field of Φ over which we are working at all times by L. So in this section types are of the form

$$t = (\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1 \le i \le u} \tag{5}$$

with $\varphi_i \in \mathcal{O}_{\mathsf{L}}[x]$, $\lambda_i = \frac{h}{e_i p^{\mu_i^*}} \in \mathbb{Q}$ with $\gcd(h, e_i p) = \gcd(e_i, p) = 1$, $\gamma_i \in \underline{\mathsf{L}}$, $\mu_i \in \mathbb{N}$ such that $\mu_i = \max\{\mu_i^* - M_i, 0\}$ where $M_i = \max\{\mu_j^* \mid 1 \le j \le i-1\} = \sum_{j=1}^{i-1} \mu_j$. By $\Theta = \Theta_u$ we denote the set of zeros that corresponds to t as in (4).

In an implementation of the algorithm, the methods described below operate on representations of polynomials as nested φ_i-expansions ($1 \le i \le u$). To avoid having to write down these somewhat involved data structures, we use polynomials to formulate the input and the output of the methods. Sections 5.8 and 6.9 yield these methods:

`div`(t,a,b) Given $a \in \mathsf{K}[x]$ of degree less than p^{M_u} and $b(x) = \varphi_u^{s_u} \dots \varphi_1^{s_1} \pi^{s_\pi}$ where $s_i < e_i$ we find $c \in \mathsf{K}[x]$ with $\deg c < \deg \varphi_u$ such that $a(\theta)/b(\theta) \sim c(\theta)$ for all $\theta \in \Theta_u$

`mult`(t,a,b) Given $a, b \in \mathsf{K}[x]$ of degree less than p^{M_u} we find $c \in \mathsf{K}[x]$ with $\deg c < \deg \varphi_u$ such that $a(\theta)b(\theta) \sim c(\theta)$ for all $\theta \in \Theta_u$.

`pow`(t,a,n) Given $a \in \mathsf{K}[x]$ of degree less than p^{M_u} we find $c(x) \in \mathsf{K}[x]$ with $\deg c < \deg \varphi_u$ such that $a^n(\theta) \sim c(\theta)$ for all $\theta \in \Theta_u$.

Furthermore we write `divmod` for the function that for $a, b \in \mathbb{Z}$ returns the quotient and remainder of the division of a by b.

We first give auxiliary algorithms for the computation of $v_t(a) = v(a(\theta))$ for $\theta \in \Theta_u$, the Newton polygon of Φ with respect to φ, polynomials with given valuations, the reduction of elements represented as power products of polynomials, and the computation of residues and residual polynomials. This is followed by the algorithm for the splitting field.

We use Algorithm 1 `Valuation` to compute $v_{\mathsf{L}}(a(\theta))$ for $\theta \in \Theta_u$. It follows from the discussions in sections 5.6 and 6.7 that to find $v_{\mathsf{L}}(a(\theta))$ for $\theta \in \Theta_u$ we only need the type $t = (\varphi_i, \lambda_i, \rho_i)_{1 \le i \le u}$ and not θ. We thus obtain one of the valuations of polynomial rings as classified by MacLane in [11]. We write $v_t(a)$ for the valuation computed by the algorithm and have $v_t(a) = v_{KK_u}(a(\theta))$

Algorithm 1 `Valuation`

Input: A local field L, type $(\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1 \le i \le u}$ over L, and $a(x) \in \mathsf{L}[x]$.
Output: Valuation $v_t(a)$.

- If $a \in \mathsf{L}$: Return $v_{\mathsf{L}}(a)$.
- Find the φ_{u-1}-expansion of $a(x) = \sum_{j=0}^{\lceil \deg a / \deg \varphi_u \rceil} a_j(x) \varphi_u^j(x)$.
- Return $\min \left\{ \texttt{Valuation}\left(\mathsf{L}, (\varphi_j, \lambda_j, \psi_j, \gamma_j, \mu_j)_{1 \le j \le u-1}, a_j\right) + j\lambda_{u-1} \;\middle|\; 1 \le i \le \lceil \frac{\deg a}{\deg \varphi_{u-1}} \rceil \right\}$

Algorithm 2 `NewtonPolygonSegments` returns the set of segments of the Newton polygon of Φ with respect to φ as described in section 5.1 and 6.1.

Algorithm 2 `NewtonPolygonSegments`

Input: A local field L, $\Phi \in \mathsf{L}[x]$, a type $t = (\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1 \le i \le u}$ over L, and $\varphi \in \mathcal{O}_{\mathsf{L}}[x]$
Output: Set of Segments S of the Newton polygon of Φ with respect to φ.

- Find the φ-expansion $\Phi = \sum_{i=0}^{m} a_i \varphi^i$ where $m = \lceil \deg \Phi / \deg \varphi \rceil$.
- Find $v_i = \texttt{Valuation}(\mathsf{L}, t, a_i)$ for $0 \le i \le m$.
- Construct the lower convex hull of the set of points $\{(i, v_i) \mid 1 \le i \le m\}$.
- Return the set S of segments of this broken line.

Given a type t as in (5) and $w \in \frac{1}{p^{M_u}}\mathbb{Z}$, Algorithm 3 `PolynomialWithValuation` returns a polynomial ψ such that $v_t(\psi) = w$ as described in sections 5.7 and 6.8. See [19], [18, Algorithm 14] or [10, Section 4] for a general version of this algorithm.

Algorithm 3 `PolynomialWithValuation`

Input: A type $(\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1\le i\le u}$ and $\frac{c}{p^d} \in \mathbb{Q}$ with $d \le \sum_{i=1}^{u-1} \mu_i$.
Output: $\psi(x) \in \mathsf{K}[x]$ with $\deg\psi < \deg\varphi_u$ and $v_{\mathsf{L}}(\psi(\theta)) = \frac{c}{p^d}$.

- If $d = 0$: Return π^c.
- $M \leftarrow \sum_{i=1}^{u-2} \mu_i$.
- If $d \le M$: Return `PolynomialWithValuation` $\left((\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1\le i\le u-1}, \frac{c}{p^d}\right)$.
- Find $0 \le s < p^{\mu_{u-1}}$ such that $sh_{u-1} \equiv cp^{M+\mu_{u-1}-d} \bmod p^{\mu_{u-1}}$.
- Return $\varphi_u^s(x) \cdot$ `PolynomialWithValuation` $\left((\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1\le i\le u-1}, \frac{c}{p^d} - s\lambda_{u-1}\right)$.

In sections 5.8 and 6.9 we have described how a product $\prod_{i=1}^{u} \varphi_i^{s_i}(x)$ can be reduced such that $s_i < p^{\mu_i}$ for $1 \le i \le u$. Algorithm 4 `reduce` conducts this reduction recursively. Because, for $1 \le i \le u$ the valuations of $\varphi_i^{s_i}$ with $s_i < p^{\mu_i}$ are linearly independent, there is only one reduced representation of each class of some $a \in \mathsf{L}[x]$ with respect to the equivalence relation from Definition 1. Thus if $v_t(a) = 0$ then `reduce`$(a) \in \mathsf{L}$.

Algorithm 4 `reduce`

Input: A type $(\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1\le i\le u}$ and $a(x) = \varphi_u^{r_u} \cdot \prod_{i=1}^{u-1} \varphi_i^{r_i} \cdot \delta \in \mathsf{L}[x]$ with $\delta \in \mathsf{K}$.
Output: $b(x) = \varphi_u^{s_u} c(x) \in \mathsf{L}[x]$ with $\deg c < \deg\varphi_u$, $0 \le s_u < p^{\mu_u}$, and $a(\theta) \sim b(\theta)$ for $\theta \in \Theta_u$.

- If $a \in \mathsf{L}$: Return a.
- $s, d \leftarrow$ `divmod`(r_u, p^{μ_u})
- Return $\varphi_u^s \cdot \gamma_u^d \cdot \psi_u^d \cdot$ `reduce` $\left((\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1\le i\le u-1}, \prod_{i=1}^{u-1} \varphi_i^{r_i} \cdot \delta\right)$.

The residual polynomial of a segment of a Newton polygon of higher order is computed in Algorithm 5 `ResidualPolynomial`.

Algorithm 5 `ResidualPolynomial`

Input: A type $(\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1\le i\le u}$, a segment S of the Newton polygon of Φ with respect to φ, and ψ with $v_t(\psi) = \lambda_u = ep^{\min\{\mu, M_u\}}$ where $-h/(ep^{\mu})$ is the slope of S.
Output: The residual polynomial $\underline{A}$ of S.

- Let $\Phi = \sum_{i=0}^{\lceil N/\deg\varphi_u \rceil} a_i\varphi^i$ be the φ-expansion of $\Phi(x)$.
- Let m be the length of S.
- $\tau \leftarrow$ `PolynomialWithValuation`(t, ν) where ν is the y-coordinate of the first point of S.
- $\underline{A}(z) \leftarrow \sum_{j=0}^{m/e_u}$ `reduce`$(t,$ `mult`$(t, a_{k+e\cdot i}(x),$ `div`$(t,$ `pow`$(t, \psi(x), j), \tau(x))))y^j$.
- return $\underline{A}$.

Algorithm 6 `SplittingField` computes the splitting field of a polynomial. If $\mu_u = 0$ and $\deg\varphi = 1$ and the multiplicity of the zero γ of $\underline{A}$ is one, then φ is an approximation to a linear factor and therefore discarded. In a type

we denote non-assigned components by $\cdot$. In each iteration we of the algorithm we start with a type whose last member has only the first component set and then fill in the other components. At the end of each iteration the last member of all types again only have the first component assigned. We start with $t = (x, \cdot, \cdot, \cdot, \cdot)$. The types in the algorithm are at all times optimal. In step **4i.** when the current iteration only yields a φ with a higher valuation at $\theta \in \Theta$ we replace the last component of the type t by the current $(\varphi, \cdot, \cdot, \cdot, \cdot)$; this is called an improvement step. If the degree of φ in increases we append $(\varphi, \cdot, \cdot, \cdot, \cdot)$ to t; this is called a Montes step.

Algorithm 6 `SplittingField`

Input: $\Phi \in \mathcal{O}_{\mathsf{K}}[x]$ monic and square-free
Output: Splitting field of Φ

- Initialize $\mathsf{L} \leftarrow \mathsf{K}$ and $T \leftarrow \{(x, \cdot, \cdot, \cdot, \cdot)\}$
- While T is non-empty:
  1. Choose a type $t = (\varphi_i, \lambda_i, \psi_i, \gamma_i, \mu_i)_{1 \le i \le u}$ from T.
  2. Remove t from T.
  3. $M \leftarrow \sum_{i=1}^{u-1} \mu_i$
  4. For $S \in$ `NewtonPolygonSegments`$(\Phi(x), t, \varphi_u(x))$:
     - **a.** Let $\lambda_u = \frac{h}{ep^{\mu^*}}$ with $\gcd(h, pe) = \gcd(e, p) = 1$ be the negative of the slope of S.
     - **b.** $\mu_u \leftarrow \max\{\mu^* - M, 0\}$ and $\nu \leftarrow \min\{\mu^*, M\}$
     - **c.** $\psi_u \leftarrow$ `PolynomialWithValuation`$(t, h/p^{\nu})$
     - **d.** $\underline{A} \leftarrow$ `ResidualPolynomial`(t, S, ψ)
     - **e.** Find f_0 minimal with $e \mid (|\underline{\mathsf{L}}^{f_0}| - 1)$.
     - **f.** If $f = \operatorname{lcm}\{f_0, \deg \underline{\rho} \mid \underline{\rho}$ irreducible factor of $\underline{A}\} > 1$:
       continue over unramified extension
       - Replace L by the unramified extension of L of degree f.
     - **g.** If the length of S is one and $\deg \varphi_u > 1$:
       continue over wildly ramified extension
       - Let $\widehat{\varphi}$ be a lift of φ_u to a factor of Φ.
       - Replace L by $\mathsf{L}[x]/(\widehat{\varphi})$.
       - Insert t into T.
       - Replace each $(\varphi_j, \lambda_j, \psi_j, \gamma_j, \mu_j)_j \in T$ by $(\varphi_1, \cdot, \cdot, \cdot, \cdot)$
       - Exit for loop.
     - **h.** If $e > 1$:
       continue over tamely ramified extension
       - Find $\delta \in \mathcal{O}_{\mathsf{K}}$ such that $\psi^{p^{\nu}} = \delta \pi^h$.
       - Find $a, b \in \mathbb{Z}$ be such that $ae + bh = 1$.
       - Replace L by the composite of $\mathsf{L}[x]/(x^e + (-\gamma^{p^{\nu}}\delta)^b \pi_L)$ where the γ are lifts of the roots of $\underline{A}$ in $\underline{\mathsf{L}}$.
       - Insert t into T.
       - Exit for loop.
     - **i.** For all roots $\underline{\gamma}$ of $\underline{A}$ in $\underline{\mathsf{L}}$:
       - Let γ be a lift of $\underline{\gamma}$ to $\mathcal{O}_{\mathsf{L}}$.
       - If $\mu_u > 0$:
         more wild ramification found, a Montes step
         - Insert t with $(\varphi_u^{\mu_u} - \gamma\psi_u, \cdot, \cdot, \cdot, \cdot)$ appended into T.
       - Else if $\deg \varphi > 1$ or the multiplicity of γ is greater than 1:
         valuation of φ increases, but not its degree, an improvement step
         - Insert t with its last member replaced by $(\varphi_u - \gamma\psi_u, \cdot, \cdot, \cdot, \cdot)$ into T.
- Return L.

Remark 1. For better readability of the algorithm we have excluded some obvious improvements. When we continue over a tamely ramified extension in **5h.**, instead of exiting the for loop and recomputing the Newton polygon in **4.** we can adjust the slopes of the segments of the Newton polygon, which over the tamely ramified extension of degree e do not have e in the denominator anymore and continue in **4c**. When choosing t from T in **1.** a speedup may be achieved by first processing the longest type as this avoids discarding information about wildly ramified extensions in

4h. If $\varphi \in \mathcal{O}_\mathsf{K}[x]$ is Eisenstein the maximal tamely ramified subfield of the splitting field of φ can be obtained from [7, Theorem 9.1].

7.1 Termination

The termination of the algorithm is assured by the following theorem.

Theorem 2 ([17, Proposition 4.1]). *Let $\Phi(x) \in \mathcal{O}_\mathsf{K}[x]$ be square-free and let Θ_0 be the set of zeros of $\Phi(x)$ in $\overline{\mathsf{K}}$. Let $\varphi(x) \in \mathsf{K}[x]$ such that the degree of any irreducible factor of $\Phi(x)$ is greater than or equal to $\deg\varphi$. If $(\deg\Phi) \cdot v(\varphi(\theta_j)) > 2v(\operatorname{disc}\Phi)$ for all $\theta \in \Theta_0$ then $\deg\varphi = \deg\Phi$ and $\Phi(x)$ is irreducible over K.*

By Theorem 2 the polynomial $\Phi(x)$ is irreducible if we find a monic $\varphi(x) \in \mathcal{O}_\mathsf{K}[x]$ such that $Nv(\varphi_u(\theta)) > 2v(\operatorname{disc}\Phi)$ for some $u \in \mathbb{N}$. In every iteration of the algorithm the increase from $v(\varphi_u)$ to $v(\varphi_{u+1})$ is at least $1/N$. Thus the algorithm terminates after at most $v(\operatorname{disc}\Phi)$ iterations.

7.2 Representation of Extensions

Extensions of local fields are often represented as a tower of an totally ramified extension over an unramified extension. Although some computer algebra systems (for example Magma [3]) allow the construction of arbitrary towers of extensions, in practice it is more efficient to work over smaller towers. We represent our extensions as a totally and wildly ramified extension over a totally and tamely ramified extension over an unramified extension and insert new extensions into the corresponding subfield in the tower.

Ramified extensions are usually given by Eisenstein polynomials, and indeed for the tamely ramified extensions in our algorithm we explicitly give these. For the wildly ramified extensions, lifting the approximation to an irreducible factor φ by single factor lifting yields a generating polynomial $\widehat{\varphi}$ that is not Eisenstein in general. Algorithm 3 can be used to compute $\Pi \in \mathsf{L}[x]$ with $v_t(\Pi) = 1/p^M$ where $p^M = \deg\varphi$. The characteristic polynomial (see Definition 2) of $\Pi \in \mathsf{L}[x]/(\widehat{\varphi})$ is the desired Eisenstein polynomial. It can be computed either using linear algebra methods as in [6] or, in the p-adic case, using Newton relations.

References

1. C. Awtrey, N. Miles, J. Milstead, C. Shill, and E. Strosnider, *Galois groups of degree 14 2-adic fields*, Involve, to appear.
2. J. Bauch, E. Nart, and D. Stainsby, *Complexity of OM Factorizations*, LMS Journal of Computation and Mathematics **16**, 139-171.
3. J. J. Cannon et al., *The computer algebra system Magma*, University of Sydney (2014) `http://magma.maths.usyd.edu.au/magma/`.
4. D. G. Cantor and D. M. Gordon, *Factoring polynomials over p-adic fields*, In Proc. ANTS IV, Lecture Notes in Comput. Sci. **1838**, Springer Verlag, 2000, 185–208.
5. D. Ford, *On the Computation of the maximal order in a Dedekind domain*, PhD Dissertation, Ohio State University, 1978.
6. D. Ford, S. Pauli, and X.-F. Roblot, *A Fast Algorithm for Polynomial Factorization over $\mathbb{Q}_p$*, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 151–169.
7. C. Greve and S. Pauli *Galois Groups of Eisenstein Polynomials whose Ramification Polygon has one Side*, Int. J. Number Theory **8** (2012), no. 6, 1401–1424.
8. J. Guàrdia, J. Montes, and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **354** (2012), no. 1, 361–416.
9. J. Guàrdia, J. Montes, E. Nart, *Okutsu Invariants and Newton Polygons*, Acta Arithmetica 145 (2010), 83–108.
10. J. Guardia, E. Nart, and S.Pauli, *Single-Factor Lifting and Factorization of Polynomials over Local Fields*, J. Symbolic Comput. **47** (2012), no. 11, 1318–1346.
11. S. MacLane, *A Construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc. **40** (1936), 363–395.
12. S. MacLane, *A Construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal **2** (1936), 493–510.

13. J. Montes and E. Nart, *On a Theorem of Ore*, Journal of Algebra **146** (1992), 318–334.
14. J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, PhD Thesis, Universitat de Barcelona, 1999.
15. K. Okutsu, *Construction of integral basis, I, II, III, and IV*, Proc. Jpn. Acad. Ser. A **58** (1982), 47–49, 87–89, 117-119, and 167–169.
16. Ö. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann **99** (1928), 84–117.
17. S. Pauli, *Factoring polynomials over local fields*, J. Symb. Comp. **32** (2001), 533–547.
18. S. Pauli, *Factoring polynomials over local fields II*, in G. Hanrot and F. Morain and E. Thomé, *Algorithmic Number Theory*, *9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010*, Lecture Notes in Comput. Sci. **6197**, Springer Verlag, 2010, 301–315.
19. S. Pauli and B. Sinclair, *A guide to OM algorithms*, in preparation, 2014.
20. H. Zassenhaus, *On Hensel factorization I*, J. Number Theory, **1** (1969), 291–311.