MATHEMATICS OF COMPUTATION
Volume 70, Number 236, Pages 1641–1659
S 0025-5718(01)01306-0
Article electronically published on March 8, 2001

ON THE COMPUTATION OF ALL EXTENSIONS OF A p-ADIC FIELD OF A GIVEN DEGREE

SEBASTIAN PAULI AND XAVIER-FRANÇOIS ROBLOT

ABSTRACT. Let $\mathbf{k}$ be a p-adic field. It is well-known that $\mathbf{k}$ has only finitely many extensions of a given finite degree. Krasner has given formulae for the number of extensions of a given degree and discriminant. Following his work, we present an algorithm for the computation of generating polynomials for all extensions $\mathbf{K}/\mathbf{k}$ of a given degree and discriminant.

1. INTRODUCTION

Let p be a fixed prime number. Let $\mathbb{Q}_p$ denote the field of p-adic rational numbers and fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. For $\mathbf{k}$ a finite extension of $\mathbb{Q}_p$ the description of the lattice of extensions of $\mathbf{k}$ in $\overline{\mathbb{Q}}_p$ is an important problem in the theory of p-adic fields.

If we restrict to Abelian extensions, then this description is complete and given by Local Class Field Theory (see [Se63] for instance). In the general case, such a description is not yet known. However, since the number of p-adic extensions of a given degree is finite, it is still possible to ask for a formula that gives the number of extensions of a given degree, and for methods to compute them. Krasner gives such a formula [Kr66], using his famous lemma as a main tool. Indeed, his proof is constructive. It is possible to adapt his methods to get a set of polynomials defining all of these extensions. This is the aim of our paper.

Note that in [Se78] Serre computes the number of extensions using a different method in the proof of his famous "mass formula" (which can also be proved by Krasner's method [Kr79]).

Let $m > 1$, $d \geq 0$ be two integers, and $\mathfrak{p}$ the prime ideal of $\mathbf{k}$. In this paper, we give an algorithm to compute all extensions of degree m and discriminant $\mathfrak{p}^d$. In section 2, we explain how the general case can be reduced essentially to the computation of totally ramified extensions. In section 3, we state Ore's conditions, which give all possible discriminants $\mathfrak{p}^d$ of totally ramified extensions of degree m. In section 4, we introduce an ultrametric distance on the set of Eisenstein polynomials of degree m. This distance is used in the construction of a set of

Received by the editor May 24, 1999 and, in revised form, January 14, 2000.
2000 *Mathematics Subject Classification.* Primary 11S15, 11S05; Secondary 11Y40.
Key words and phrases. p-adic fields, wildly ramified extensions, Eisenstein polynomials.
The work of the first author was supported in part by ISM and FCAR/CICMA (Québec).
The work of the second author was supported in part by NSERC (Canada) and FCAR/CICMA (Québec).
We would like to thank David Ford for his careful reading of the original manuscript and for his useful comments.

©2001 American Mathematical Society

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

polynomials defining all totally ramified extensions of degree m in section 5. In section 6, we give explicit formulae for the number of totally ramified extensions. In section 7, we describe the construction of totally and tamely ramified extensions, since this construction is easier than in the general case. In section 8, we give the algorithms for the computation of a minimal set of polynomials generating all the extensions of degree m and discriminant $\mathfrak{p}^d$. Section 9 contains two examples, and in section 10 we discuss future developments.

From now on, v_p denotes the unique valuation over $\overline{\mathbb{Q}}_p$ such that $v_p(p) = 1$. The corresponding non-archimedian absolute value is $|x| := p^{-v_p(x)}$. We denote the absolute Galois group of $\overline{\mathbb{Q}}_p/\mathbf{k}$ by G.

2. The general case

Let $\mathbf{K}/\mathbf{k}$ be an extension of degree m and of discriminant $\mathfrak{p}^d$, where $\mathfrak{p}$ is the prime ideal of $\mathbf{k}$. We can split this extension uniquely into a tower of extensions $\mathbf{K}/\mathcal{K}/\mathbf{k}$, where $\mathbf{K}/\mathcal{K}$ is totally ramified, and $\mathcal{K}/\mathbf{k}$ unramified. Thus the computation of all such extensions $\mathbf{K}/\mathbf{k}$ can be split into three steps, namely:

1. Find all the suitable unramified extensions $\mathcal{K}/\mathbf{k}$.
2. For any such extension $\mathcal{K}$, compute all the suitable totally ramified extensions $\mathbf{K}/\mathcal{K}$.
3. Deduce all the extensions $\mathbf{K}/\mathbf{k}$ from the previous two steps.

The second step will be discussed at length in the following sections, because it is the most difficult step and forms the core of this paper. The first and third steps are easy and are described below. The computations of the first and third steps are described algorithmically in section 8.

Assume that $l := [\mathcal{K} : \mathbf{k}]$ and $n := [\mathbf{K} : \mathcal{K}]$, so that $[\mathbf{K} : \mathbf{k}] = m = ln$. For each finite value of l, there exists a unique unramified extension of $\mathbf{k}$ of degree l. To find a polynomial generating this extension, we look at random monic polynomials of degree l over the residue field of $\mathbf{k}$ until we find an irreducible one, say $f_l(x)$. Then any monic lift of this polynomial to $\mathbf{k}[x]$ will define $\mathcal{K}$ over $\mathbf{k}$. Since easy estimations give that the ratio of the number of monic irreducible polynomials to the number of all monic polynomials of degree l is about $1/l$, this method is adequate for the values of l we are going to deal with. Now, let $\mathcal{P}^{v_1}$ be the discriminant of $\mathbf{K}/\mathcal{K}$, where $\mathcal{P}$ is the prime ideal of $\mathcal{K}$. Then the discriminant of $\mathbf{K}/\mathbf{k}$ is $\mathfrak{p}^{lv_1}$, so l must divide $\gcd(m, d)$. Further v_1 must satisfy Ore's conditions (proposition 3.1) since $\mathbf{K}/\mathcal{K}$ is totally ramified.

Hence, in order to compute step 1, check for any positive l dividing $\gcd(m, d)$ if m/l satisfies Ore's conditions; if so, add the field generated by the polynomial $f_l(x)$ to the list of unramified extensions of $\mathbf{k}$ to be considered.

For step 3, let $\mathcal{K}/\mathbf{k}$ be an unramified extension, as computed in step 1, defined over $\mathbf{k}$ by the polynomial $f(x)$, and let $\mathbf{K}/\mathcal{K}$ be a totally ramified extension, as computed in step 2, defined over $\mathcal{K}[x]$ by the polynomial $g(x)$. Let θ be a root of f. Then we can write

$$g(x) = \sum_{i=0}^{n} g_i(\theta)x^i,$$

where $g_i(x) \in \mathbf{k}[x]$. We define the polynomial h to be the resultant in the variable y of the two polynomials $f(y)$ and $\sum_i g_i(y)(x-y)^i$. It is a polynomial of degree m in the variable x, and it is the characteristic polynomial in $\mathbf{K}/\mathbf{k}$ of $\theta + \alpha$, where α is a root of g. Since by construction α is a prime element of $\mathbf{K}$ (see below) and θ

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

generates the residue field of $\mathbf{K}$, it follows that $\theta + \alpha$ generates $\mathbf{K}$ over $\mathbf{k}$ and the valuation ring of $\mathbf{K}$ is $\mathcal{O}_{\mathbf{k}}[\theta + \alpha]$. Hence h is irreducible.

3. Ore's conditions

Note that for the rest of the paper we focus on the totally ramified extension $\mathbf{K}/\mathcal{K}$ of degree n. Let $\mathcal{P}$ and e be the prime ideal and the absolute ramification index of $\mathcal{K}/\mathbb{Q}_p$ respectively. Indeed, e is also the ramification index of $\mathbf{k}/\mathbb{Q}_p$. Let $v_{\mathcal{P}}$ denote the unique valuation defined by $v_{\mathcal{P}}(x) := e \cdot v_p(x)$, and π an uniformizer of $\mathcal{K}$ for which $v_{\mathcal{P}}(\pi) = 1$. Let q denote the cardinality of the residue class field of $\mathcal{K}$.

The possible discriminants for $\mathbf{K}/\mathcal{K}$ are given by the following criterion (see [Or26]).

Proposition 3.1 (Ore's conditions)**.** *Let $\mathcal{K}$ be a finite extension of $\mathbb{Q}_p$ with maximal ideal $\mathcal{P}$. Given $j \in \mathbb{Z}$, let $a, b \in \mathbb{Z}$ be such that $j = an + b$ and $0 \leq b < n$. Then there exist totally ramified extensions $\mathbf{K}/\mathcal{K}$ of degree n and discriminant $\mathcal{P}^{n+j-1}$ if and only if*

$$\min\{v_{\mathcal{P}}(b)n, v_{\mathcal{P}}(n)n\} \leq j \leq v_{\mathcal{P}}(n)n.$$

Let j be an integer satisfying Ore's conditions with respect to n, so $0 \leq j \leq v_{\mathcal{P}}(n)n$, and let $j = an + b$ be the Euclidean division of j by n. The following is trivial but crucial:

$$n \mid j \iff b = 0 \iff j = v_{\mathcal{P}}(n)n \iff a = v_{\mathcal{P}}(n).$$

We now fix such an integer j and turn to the more specific problem of the construction of all totally ramified extensions $\mathbf{K}/\mathcal{K}$ of degree n and discriminant $\mathcal{P}^{n+j-1}$. We denote by $\mathbf{K}_{n,j}$ the set of all these extensions. Ore's result tells us that this set is not empty.

4. Eisenstein polynomials

A polynomial $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_0$ with coefficients in the valuation ring $\mathcal{O}_{\mathcal{K}}$ of $\mathcal{K}$ is called an Eisenstein polynomial if $v_{\mathcal{P}}(f_j) \geq 1$ for $1 \leq j \leq n-1$ and $v_{\mathcal{P}}(f_0) = 1$. It is well-known that such polynomials are irreducible and generate totally ramified extensions. Furthermore, the discriminant of the field generated by such a polynomial is exactly the discriminant of the polynomial. Conversely, if $\mathbf{K}/\mathcal{K}$ is a totally ramified extension of degree n, then every prime element of $\mathbf{K}$ is a generating element over $\mathcal{K}$ and a root of an Eisenstein polynomial (see [Se63, chapter I, §6]).

Let $\mathbf{E}_{n,j}$ denote the set of all Eisenstein polynomials over $\mathcal{K}$ of degree n and discriminant $\mathcal{P}^{n+j-1}$. By the above discussion, the roots of the polynomials in $\mathbf{E}_{n,j}$ generate all the extensions $\mathbf{K} \in \mathbf{K}_{n,j}$.

For two elements f and g of $\mathbf{E}_{n,j}$, we set $d(f,g) := |f(\beta)|$, where β is a root of g. Let β' be any root of g and let $\sigma \in G$ be such that $\sigma(\beta) = \beta'$. Since σ is isometric, we have

$$|f(\beta)| = |\sigma(f(\beta))| = |f(\sigma(\beta))| = |f(\beta')|;$$

hence $d(f,g)$ does not depend on the choice of β. Observe that

$$|f(\beta)|^n = \prod_i |f(\beta_i)| = \prod_{i,j} |\beta_i - \alpha_j|,$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

where β_i (resp. α_j) denote the roots of g (resp. f). The last formula is symmetric with respect to f and g. Thus for any root α of f, the equality $|f(\beta)| = |g(\alpha)|$ follows since $|f(\alpha)|, |f(\beta)| \in \mathbb{R}^+$. Hence, $d(f,g) = d(g,f)$.

Fix a root α of f and assume that β is chosen among the roots of g such that the distance $|\beta - \alpha|$ is minimal. Notice that this distance does not depend on the choice of α. We have

$$d(f,g) = |f(\beta)| = \prod_{i=1}^{n} |\beta - \alpha_i|.$$

Now, if $|\beta - \alpha_i| \neq |\beta - \alpha|$ then $|\beta - \alpha_i| > |\beta - \alpha|$ and $|\alpha - \alpha_i| = |\alpha - \beta + \beta - \alpha_i| = |\beta - \alpha_i|$. We have proved that

$$d(f,g) = \prod_{i=1}^{n} \max\{|\beta - \alpha|, |\alpha - \alpha_i|\}.$$

Let $h \in \mathbf{E}_{n,j}$. Assume that γ (resp. γ') is a root of h such that the distance $|\beta - \gamma|$ (resp. $|\alpha - \gamma'|$) is minimal. Then

$$\begin{aligned}
d(f,h) &= \prod_{i=1}^{n} \max\{|\alpha - \gamma'|, |\alpha - \alpha_i|\} \\
&\leq \prod_{i=1}^{n} \max\{|\alpha - \gamma|, |\alpha - \alpha_i|\} \\
&\leq \prod_{i=1}^{n} \max\{\max\{|\alpha - \beta|, |\beta - \gamma|\}, |\alpha - \alpha_i|\} \\
&\leq \max\Big\{ \prod_{i=1}^{n} \max\{|\alpha - \beta|, |\alpha - \alpha_i|\}, \prod_{i=1}^{n} \max\{|\beta - \gamma|\}, |\alpha - \alpha_i|\} \Big\} \\
&\leq \max\{d(f,g), d(g,h)\}.
\end{aligned}$$

Thus d satisfies the ultrametric inequality. It is clear that $d(f,g) = 0$ if and only if $f = g$. The following result summarizes the properties of d.

Proposition 4.1. *Let f, g be two polynomials from the set $\mathbf{E}_{n,j}$ of Eisenstein polynomials of degree n and discriminant $\mathcal{P}^{n+j-1}$ over $\mathcal{K}$. Then $d(f,g) := |f(\beta)| = |g(\alpha)|$, where α (resp. β) is any root of f (resp. g), defines an ultrametric distance over $\mathbf{E}_{n,j}$. Furthermore, let f, g be two elements of $\mathbf{E}_{n,j}$, $\alpha = \alpha_1, \ldots, \alpha_n$ the roots of f, and β one of the roots of g which is closest to α. Then*

$$d(f,g) = \prod_{i=1}^{n} \max\{|\beta - \alpha|, |\alpha - \alpha_i|\}.$$

The distance $d(f,g)$ is easily calculated using the following lemma.

Lemma 4.2. *Write $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_0$ and $g(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_0$, and set*

$$w := \min_{0 \leq i \leq n-1} \left\{ v_{\mathcal{P}}(g_i - f_i) + \frac{i}{n} \right\}.$$

Then $d(f,g) = |\mathcal{P}|^w$.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Proof. Observe that

$$g(\alpha) = g(\alpha) - f(\alpha) = \sum_{i=0}^{n-1} (g_i - f_i)\alpha^i,$$

and since α is a prime element, $v_{\mathcal{P}}(\alpha) = 1/n$. Thus in the above sum all the terms have different valuations. It follows that the valuation of $g(\alpha)$ is the minimum of those. □

5. Construction of generating polynomials

In this section, we construct a finite set of polynomials that generate all the extensions in $\mathbf{K}_{n,j}$. Let Γ be the Galois group of the abelian extension $\mathcal{K}/\mathbf{k}$.

Let $m \geq l \geq 1$ be two integers, and $\mathcal{R}_{l,m}$ a fixed Γ-stable system of representatives of the quotient

$$\mathcal{P}^l/\mathcal{P}^m.$$

We denote by $\mathcal{R}^*_{l,m}$ the subset of those elements of $\mathcal{R}_{l,m}$ whose $v_{\mathcal{P}}$-valuation is exactly l. Thus $\mathcal{R}_{l,m}$ is also Γ-stable.

For $1 \leq i \leq n-1$, define

$$l(i) := \begin{cases} \max\{2 + a - v_{\mathcal{P}}(i), 1\} & \text{if } i < b, \\ \max\{1 + a - v_{\mathcal{P}}(i), 1\} & \text{if } i \geq b. \end{cases}$$

Let c be any integer such that

$$c > 1 + 2a + \frac{2b}{n} = \frac{n + 2j}{n}.$$

The reason for choosing these values of $l(i)$ and c will become clear presently.

Let Ω be the set of n-tuples $(\omega_0, \ldots, \omega_{n-1}) \in \mathcal{K}^n$ satisfying

$$\omega_i \in \begin{cases} \mathcal{R}^*_{1,c} & \text{if } i = 0, & (1) \\ \mathcal{R}_{l(i),c} & \text{if } 1 \leq i \leq n-1 \text{ and } i \neq b, & (2) \\ \mathcal{R}^*_{l(b),c} & \text{if } i = b \neq 0. & (3) \end{cases}$$

To each element $\omega := (\omega_0, \ldots, \omega_{n-1}) \in \Omega$, we associate the polynomial $A_\omega(x) \in \mathcal{O}_{\mathcal{K}}[x]$ given by

$$A_\omega(x) := x^n + \omega_{n-1}x^{n-1} + \cdots + \omega_1 x + \omega_0.$$

Lemma 5.1. *The polynomials A_ω are Eisenstein polynomials of discriminant $\mathcal{P}^{n+j-1}$.*

Proof. Since $l(i) \geq 1$ for all i, we have $v_{\mathcal{P}}(\omega_i) \geq 1$, and (1) gives $v_{\mathcal{P}}(\omega_0) = 1$. Thus, A_ω is an Eisenstein polynomial.

Let $\varkappa$ be a root of A_ω. Since the discriminant of A_ω is the norm from $\mathcal{K}(\varkappa)/\mathcal{K}$ of $A'_\omega(\varkappa)$, the second assertion is equivalent to

$$v_{\mathcal{P}}(A'_\omega(\varkappa)) = \frac{n + j - 1}{n} = 1 + a + \frac{b-1}{n}.$$

But $A'_\omega(\varkappa) = n\varkappa^{n-1} + (n-1)\omega_{n-1}\varkappa^{n-2} + \cdots + \omega_1$ and $v_{\mathcal{P}}(A'_\omega(\varkappa))$ is the minimum of these valuations, since they are all different.

It is straightforward to see by (2) that for $i \neq b$

$$v_{\mathcal{P}}(i\omega_i\varkappa^{i-1}) > 1 + a + \frac{b-1}{n},$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

and for $i = b \neq 0$

$$v_{\mathcal{P}}(b\omega_b \varkappa^{b-1}) = 1 + a + \frac{b-1}{n}.$$

If $b = 0$, then for $1 \leq i \leq n-1$ we have

$$v_{\mathcal{P}}(n\varkappa^{n-1}) = v_{\mathcal{P}}(n) + (n-1)/n < v_{\mathcal{P}}(i\omega_i \varkappa^{i-1})$$

and therefore $v_{\mathcal{P}}(A'_\omega(\varkappa)) = 1 + v_{\mathcal{P}}(n) - 1/n$, as required. If $b \neq 0$, then by Ore's conditions

$$v_{\mathcal{P}}(n\varkappa^{n-1}) > v_{\mathcal{P}}(b\omega_b \varkappa^{b-1});$$

hence $v(A'_\omega(\varkappa)) = 1 + a + (b-1)/n$. □

Theorem 5.2 (Krasner)**.** *The set $\mathbf{E}_{n,j}$ is the disjoint union of the closed discs $D_{\mathbf{E}_{n,j}}(A_\omega, r)$ with center A_ω and radius $r := |\mathcal{P}^c|$ as ω runs through Ω.*

Proof. Lemma 5.1 proves that the polynomials A_ω are indeed elements of $\mathbf{E}_{n,j}$.

Let ω, ω' be two distinct elements of Ω and let i be such that $\omega_i \neq \omega'_i$. Then

$$v_{\mathcal{P}}(\omega_i - \omega'_i) + \frac{i}{n} \leq c - 1 + \frac{i}{n} < c,$$

and thus, by lemma 4.2, $d(A_\omega, A_{\omega'}) > r$, and by the ultrametric property of d the discs D_ω and $D_{\omega'}$ are disjoint.

Now, let f be an element of $\mathbf{E}_{n,j}$ and write $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_0$. Since f is an Eisenstein polynomial, $v_{\mathcal{P}}(f_0) = 1$ and there exists $\omega_0 \in \mathcal{R}^*_{1,c}$ such that

$$f_0 \equiv \omega_0 \pmod{\mathcal{P}^c}.$$

By reasoning as in lemma 5.1, we find that $v_{\mathcal{P}}(f_i) \geq l(i)$ for all $i > 0$ and that there exists ω_i satisfying (2) or (3) such that

$$f_i \equiv \omega_i \pmod{\mathcal{P}^c}.$$

Let $\omega := (\omega_0, \ldots, \omega_{n-1})$. We claim that $f \in D_\omega$. We have $v_{\mathcal{P}}(f_i - \omega_i) \geq c$ for $i = 0, \ldots, n-1$. Thus, for all i

$$v_{\mathcal{P}}(f_i - \omega_i) + \frac{i}{n} \geq c,$$

which by lemma 4.2 proves the claim. □

Corollary 5.3. *Let ω be an element of Ω and let $\varkappa$ be a root of $A_\omega(x)$. Then the extension $\mathcal{K}(\varkappa)/\mathcal{K}$ is a totally ramified extension of degree n and discriminant $\mathcal{P}^{n+j-1}$. Conversely, if $\mathbf{K}/\mathcal{K}$ is a totally ramified extension of degree n and discriminant $\mathcal{P}^{n+j-1}$, then there exist $\omega \in \Omega$ and a root $\varkappa$ of $A_\omega(x)$ such that $\mathbf{K} = \mathcal{K}(\varkappa)$.*

Proof. The first claim is clear since the polynomials A_ω belong to $\mathbf{E}_{n,j}$. For the second, let α be a prime element in $\mathbf{K}$ and denote its irreducible polynomial over $\mathcal{K}$ by f. Let $\alpha = \alpha_1, \ldots, \alpha_n$ denote the roots of f and let Δf be the minimal distance between α and any other root of f. Then

$$|f'(\alpha)| = \prod_{i=2}^{n} |\alpha - \alpha_i| \leq \Delta f \cdot \left|\mathcal{P}^{(n-2)/n}\right|,$$

since the α_i are prime elements. But

$$|f'(\alpha)| = \left|\mathcal{P}^{(n+j-1)/n}\right|,$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

and thus

$$\Delta f \geq \left|\mathcal{P}^{(j+1)/n}\right|.$$

Now, let $\omega \in \Omega$ be such that $d(f, A_\omega) \leq r = |\mathcal{P}^c|$ and let $\varkappa$ denote a root of A_ω such that $|\varkappa - \alpha|$ is minimal. Then we claim that $|\varkappa - \alpha| < \Delta f$. Indeed, otherwise

$$\begin{aligned} d(f, A_\omega) &= \prod_{i=1}^{n} \max\{|\alpha - \varkappa|, |\alpha - \alpha_i|\} \\ &\geq \prod_{i=1}^{n} \max\{\Delta f, |\alpha - \alpha_i|\} \\ &\geq \Delta f \prod_{i=2}^{n} |\alpha - \alpha_i| = \Delta f |f'(\alpha)| \\ &\geq \left|\mathcal{P}^{(n+2j)/n}\right|. \end{aligned}$$

This contradicts $|\mathcal{P}^{(n+2j)/n}| > r$ by the particular choice of c. Hence $|\varkappa - \alpha| < \Delta f$, and it follows by Krasner's lemma (see below) that $\mathbf{K} = \mathcal{K}(\varkappa)$. □

Theorem 5.4 (Krasner's lemma)**.** *Let β, γ be two elements of the algebraic closure of $\mathcal{K}$ such that the distance between β and γ is strictly smaller than the distance between γ and any of its conjugates. Then $\gamma \in \mathcal{K}(\beta)$.*

See [Ca86] for a proof.

6. Number of extensions in $\mathbf{K}_{n,j}$

We have constructed a finite set of polynomials that generate all the extensions in $\mathbf{K}_{n,j}$, namely the set $\{A_\omega : \omega \in \Omega\}$. Nevertheless, for each extension, there are in general several polynomials A_ω that generate the same extension. So the number of extensions is in fact smaller than the number of elements in Ω.

The aim of this section is to prove exact formulae for the number of extensions in $\mathbf{K}_{n,j}$. These formulae are interesting in their own right, but will also be useful in getting a more efficient algorithm (see section 8 for details).

Theorem 6.1 (Krasner)**.** *Let $\mathcal{K}$ be a finite extension of $\mathbb{Q}_p$, let $\mathcal{P}$ be the prime ideal of $\mathcal{K}$ with e its ramification index, and let q be the number of elements in the residue field of $\mathcal{K}$. Let $j = an + b$, where $0 \leq b < n$, be an integer satisfying Ore's conditions. Then the number of totally ramified extensions of $\mathcal{K}$ of degree n and discriminant $\mathcal{P}^{n+j-1}$ is*

$$\#\mathbf{K}_{n,j} = \begin{cases} n\, q^{\sum_{i=1}^{\lfloor a/e \rfloor} en/p^i} & \text{if } b = 0, \\ n\,(q-1)\, q^{\sum_{i=1}^{\lfloor a/e \rfloor} en/p^i + \left\lfloor (j - \lfloor a/e \rfloor en - 1)/p^{\lfloor a/e \rfloor + 1} \right\rfloor} & \text{if } b > 0 \end{cases}$$

We will prove this theorem in two steps.

Lemma 6.2. *The number of polynomials A_ω, where $\omega \in \Omega$, or (equivalently by theorem 5.2) the number of disjoint closed discs of radius $r := |\mathcal{P}^c|$ in $\mathbf{E}_{n,j}$,*

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

is given by

$$\#D_{\mathbf{E}_{n,j}}(r) = \begin{cases} (q-1)\, q^{nc-n-j-1+\sum_{i=1}^{\lfloor a/e\rfloor} en/p^i} & \text{if } b=0, \\ (q-1)^2\, q^{nc-n-j-1+\sum_{i=1}^{\lfloor a/e\rfloor} en/p^i + \left\lfloor (j-\lfloor a/e\rfloor en-1)/p^{\lfloor a/e\rfloor+1}\right\rfloor} & \text{if } b>0. \end{cases}$$

Proof. The number of elements in $\mathcal{R}^*_{1,c}$ is $(q-1)\,q^{c-2}$. For $\nu \neq b$, the number of elements in $\mathcal{R}_{l(\nu),c}$ is $q^{c-l(\nu)}$ and the number of elements in $\mathcal{R}^*_{l(b),c}$ is $(q-1)\,q^{c-l(b)-1}$. So we have

$$\#D_{\mathbf{E}_{n,j}}(r) = \begin{cases} (q-1)\, q^{c-2+(n-1)c-\sum_{\nu=1}^{n-1} l(\nu)} & \text{if } b=0, \\ (q-1)^2\, q^{c-2+(n-1)c-\sum_{\nu=1}^{n-1} (l(\nu)-1)} & \text{if } b>0. \end{cases}$$

It remains to compute the sum $\sum_{\nu=1}^{n-1} l(\nu)$. For $b>0$, we get

$$\sum_{\nu=1}^{n-1} l(\nu) = n-1+\sum_{\nu=1}^{b-1}\max\{1+a-v_{\mathcal{P}}(\nu),0\}+\sum_{\nu=b}^{n-1}\max\{a-v_{\mathcal{P}}(\nu),0\}.$$

Let $\tau \geq \sigma$ be two positive integers and let $\rho \geq 0$ be a real number. Then

$$\begin{aligned} \sum_{\nu=\sigma}^{\tau}\max\{\rho-v_{\mathcal{P}}(\nu),0\} &= \sum_{i\geq 0}\sum_{\substack{\nu=\sigma \\ v_p(\nu)=i}}^{\tau}\max\{\rho-ei,0\} \\ &= \sum_{i=0}^{\lfloor \rho/e\rfloor}\sum_{\substack{\nu=\sigma \\ v_p(\nu)=i}}^{\tau}(\rho-ei) \\ &= \sum_{i=0}^{\lfloor \rho/e\rfloor}(\rho-ei)\left(\left\lfloor\frac{\tau}{p^i}\right\rfloor-\left\lfloor\frac{\tau}{p^{i+1}}\right\rfloor-\left\lfloor\frac{\sigma-1}{p^i}\right\rfloor+\left\lfloor\frac{\sigma-1}{p^{i+1}}\right\rfloor\right). \end{aligned}$$

Using this formula, we find that

$$\begin{aligned} \sum_{\nu=1}^{n-1} l(\nu) \quad = \quad & n-1+\sum_{i=0}^{\lfloor \frac{a+1}{e}\rfloor}(1+a-ei)\left(\left\lfloor\frac{b-1}{p^i}\right\rfloor-\left\lfloor\frac{b-1}{p^{i+1}}\right\rfloor\right) \\ & +\sum_{i=0}^{\lfloor a/e\rfloor}(a-ei)\left(\left\lfloor\frac{n-1}{p^i}\right\rfloor-\left\lfloor\frac{n-1}{p^{i+1}}\right\rfloor-\left\lfloor\frac{b-1}{p^i}\right\rfloor+\left\lfloor\frac{b-1}{p^{i+1}}\right\rfloor\right). \end{aligned}$$

Note that, in the first summation, we can replace $\lfloor (a+1)/e\rfloor$ by $\lfloor a/e\rfloor$, since these are the same if $e \nmid a+1$, and otherwise the term $i=(a+1)/e$ does not contribute to the sum since in this case $1+a-ei=0$. Rearranging and simplifying the sums, we obtain

$$\begin{aligned} \sum_{\nu=1}^{n-1} l(\nu) \quad = \quad & n+b+a(n-1)-2-\left\lfloor\frac{b-1}{p^{\lfloor a/e\rfloor+1}}\right\rfloor-a\left\lfloor\frac{n-1}{p^{\lfloor a/e\rfloor+1}}\right\rfloor \\ & +e\lfloor a/e\rfloor\left\lfloor\frac{n-1}{p^{\lfloor a/e\rfloor+1}}\right\rfloor-\sum_{i=1}^{\lfloor a/e\rfloor} e\left\lfloor\frac{n-1}{p^i}\right\rfloor. \end{aligned}$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Since $b > 0$, by Ore's conditions we find that $v_p(n) \geq \lfloor a/e \rfloor + 1$. It follows that for all $1 \leq i \leq \lfloor a/e \rfloor + 1$, one has $\lfloor (n-1)/p^i \rfloor = n/p^i - 1$. Thus,

$$\begin{aligned}\sum_{\nu=1}^{n-1} l(\nu) &= an + b + n - 2 - \frac{an}{p^{\lfloor a/e \rfloor + 1}} - \left\lfloor \frac{b-1}{p^{\lfloor a/e \rfloor + 1}} \right\rfloor + \frac{e\lfloor a/e \rfloor n}{p^{\lfloor a/e \rfloor + 1}} - \sum_{i=1}^{\lfloor a/e \rfloor} \frac{en}{p^i} \\ &= n + j - 2 - \left\lfloor \frac{j - \lfloor a/e \rfloor en - 1}{p^{\lfloor a/e \rfloor + 1}} \right\rfloor - \sum_{i=1}^{\lfloor a/e \rfloor} \frac{en}{p^i}\end{aligned}$$

The formula for $b = 0$ can be derived in a similar way. □

Lemma 6.3. *Let $t > j+1$ be an integer and let $s := \left|\mathcal{P}^{(n+j-1+t)/n}\right|$. Let $\#D_{\mathbf{E}_{n,j}}(s)$ denote the number of disjoint closed discs of radius s in $\mathbf{E}_{n,j}$. Then the number of elements in $\mathbf{K}_{n,j}$ is*

$$\#\mathbf{K}_{n,j} = \#D_{\mathbf{E}_{n,j}}(s) \frac{n}{(q-1)q^{t-2}}.$$

Proof. Let $\Pi_{n,j}$ denote the set of all prime elements of members of $\mathbf{K}_{n,j}$. Alternatively, $\Pi_{n,j}$ can be defined as the union of the sets $\mathfrak{P} \setminus \mathfrak{P}^2$, where $\mathfrak{P}$ is the prime ideal of some member $\mathbf{K}$ of $\mathbf{K}_{n,j}$. Let χ be the map from $\Pi_{n,j}$ to $\mathbf{E}_{n,j}$ that sends a prime element to its minimal polynomial over $\mathcal{K}$.

Let $u = |\mathcal{P}^t|^{1/n}$, and let α and β be two elements of $\Pi_{n,j}$ such that $|\alpha - \beta| \leq u$. Then α and β generate the same field $\mathbf{K} \in \mathbf{K}_{n,j}$ by Krasner's lemma. Observe we have $d(\chi(\alpha), \chi(\beta)) \leq u\,|\mathcal{P}^{n+j-1}|^{1/n} = s$ by the same reasoning as in the proof of corollary 5.3. Hence, $\chi(D_\Pi(\alpha, u)) \subset D_{\mathbf{E}_{n,j}}(\chi(\alpha), s)$, where $D_\Pi(\alpha, u)$ is the closed disc of center α and radius u in $\Pi_{n,j}$. Conversely, let $f \in \mathbf{E}_{n,j}$ and let α denote any root of f, so $f = \chi(\alpha)$. Then it is straightforward to prove, using the same methods, that $D_{\mathbf{E}_{n,j}}(\chi(\alpha), s) \subset \chi(D_\Pi(\alpha, u))$. Thus, for all $\alpha \in \Pi_{n,j}$

$$D_{\mathbf{E}_{n,j}}(\chi(\alpha), s) = \chi(D_\Pi(\alpha, u)).$$

Now, the map χ is clearly surjective and n-to-one. Furthermore, the inverse image of $\chi(\alpha)$ is the set of conjugates of α over $\mathcal{K}$, and since $t > j+1$, the closed discs of radius u centered at the conjugates of α are all disjoint. It follows that the inverse image of any closed disc of radius s in $\mathbf{E}_{n,j}$ is the disjoint union of n closed discs of radius u in $\Pi_{n,j}$. But, again by the remark above, any such disc is in fact contained in $\mathfrak{P} \setminus \mathfrak{P}^2$ for some $\mathbf{K} \in \mathbf{K}_{n,j}$. Thus, the number of disjoint closed discs of radius u in $\Pi_{n,j}$ is equal to $\#\mathbf{K}_{n,j}$ times the number of disjoint closed discs in $\mathfrak{P} \setminus \mathfrak{P}^2$, which does not depend on $\mathbf{K} \in \mathbf{K}_{n,j}$. This number is easily seen to be equal to $q^{t-1} - q^{t-2}$, and so

$$\#\mathbf{K}_{n,j}\, q^{t-2}\,(q-1) = n\,\#D_E(s),$$

and the result is proved. □

Theorem 6.1 is proven by choosing t such that $n + j - 1 + t = nc$ and applying the two previous lemmas.

7. Tamely ramified extensions

In this section we let $\mathbf{K}/\mathcal{K}$ be totally and tamely ramified, *i.e.*, p does not divide $n = [\mathbf{K} : \mathcal{K}]$. The description of totally and tamely ramified extensions of p-adic fields is well-known (see [Ha69, chapter 16] or theorem 7.2 below). The aim of this section is to recover this description using the methods developed in the previous

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

sections. Notice first the following result, whose proof follows directly from Ore's conditions.

Proposition 7.1. *Let $\mathbf{K}/\mathcal{K}$ be a totally and tamely ramified extension of degree n. Then $j = 0$, and thus the discriminant of this extension is $\mathcal{P}^{n-1}$, $a = b = 0$, and one can choose $c = 2$.*

The totally tamely ramified extensions of degree n of $\mathcal{K}$ are described by the following theorem.

Theorem 7.2. *Let ζ be a primitive $(q-1)$-th root of unity contained in $\mathcal{K}$, g the* gcd *of n and $q-1$, and $m := n/g$. Then there are exactly n totally and tamely ramified extensions $\mathbf{K}/\mathcal{K}$ of degree n. Furthermore, these extensions can be split into g classes of m $\mathcal{K}$-isomorphic extensions, all extensions in the same class being generated over $\mathcal{K}$ by the roots of the polynomial*

$$x^n + \zeta^r \pi$$

with $r = 0, \dots, g-1$.

Proof. We look at the set of generating polynomials defined in section 5. Proposition 7.1 tells us that $j = a = b = 0$, and the smallest possible value for c is 2. We choose $\mathcal{R}^*_{1,2} := \{\zeta^i \pi \text{ with } 0 \le i \le q-2\}$ and $\mathcal{R}_{1,2} := \mathcal{R}^*_{1,2} \cup \{0\}$. Then the roots of the polynomials $x^n + \omega_{n-1}x^{n-1} + \cdots + \omega_0$, where $\omega_i \in \mathcal{R}_{1,2}$ for $1 \le i \le n-1$ and $\omega_0 \in \mathcal{R}^*_{1,2}$, generate all these extensions $\mathbf{K}$.

We now turn to the extensions $\mathbf{K}$ generated by the roots of the polynomials $x^n + \zeta^i \pi$ (*i.e.*, we take $\omega_i = 0$ for $1 \le i \le n-1$). Let α be such a root. Then it is clear that for any integer h, $\zeta^h \alpha$ generates the same extension. The minimal polynomial of $\zeta^h \alpha$ is $x^n + \zeta^{nh+i}\pi$, and one can choose h such that $nh + i \equiv r \pmod{q-1}$ with $0 \le r < g$. Hence, it is enough to consider only the polynomials $x^n + \zeta^r \pi$ where $0 \le r \le g-1$.

Now, let $x^n + \zeta^r \pi$ and $x^n + \zeta^{r'} \pi$ be two such polynomials, where $0 \le r, r' \le g-1$ and $r \ne r'$, and let α (resp. α') be a root of $x^n + \zeta^r \pi$ (resp. $x^n + \zeta^{r'} \pi$). Then if α and α' generate the same field, it follows that this field contains an n-th root of $\zeta^{r-r'}$. But this is impossible, since this field contains only the $(q-1)$-th roots of unity and $r - r'$ is not a multiple of n modulo $q-1$. So α and α' generate two distinct extensions of $\mathcal{K}$. Furthermore, the conjugates of α over $\mathcal{K}$ are $\alpha, \rho\alpha, \dots, \rho^{n-1}\alpha$, where ρ is a primitive n-th root of unity in $\overline{\mathbb{Q}}_p$ such that $\rho^m = \zeta^{(q-1)/g}$ (recall that $m = n/g$). It is clear that $\alpha, \rho^m\alpha = \zeta^{(q-1)/g}\alpha, \dots, \rho^{(g-1)m}\alpha = \zeta^{(g-1)(q-1)/g}\alpha$ all generate the same field, whereas $\alpha, \rho\alpha, \dots, \rho^{m-1}\alpha$ all generate different extensions. Thus, the roots of the polynomial $x^n + \zeta^r \pi$ generate m distinct isomorphic extensions, and the roots of all of these polynomials generate $mg = n$ extensions. Since we know that this is exactly the number of totally ramified extensions of degree n of $\mathcal{K}$ by theorem 6.1, this proves that all the totally ramified extensions of degree n of $\mathcal{K}$ are obtained considering only these polynomials, and that the other polynomials are redundant. □

8. Algorithms

From the results of the previous sections we know how many extensions in $\mathbf{K}_{n,j}$ there are and we know how to find a set of polynomials generating all of them. In this section, we will describe how to use these results to compute a *minimal* set of polynomials generating these extensions. The first algorithm that we need is an

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

algorithm that will tell us how many distinct isomorphic extensions are generated by a given polynomial, and whether two polynomials generate isomorphic extensions or not.

Panayi's Root Finding Algorithm. Let f, $h \in \mathcal{O}_{\mathcal{K}}[x]$ be two irreducible polynomials of degree n. Let $\mathbf{K}$ be a field generated by a root of f. Any root of h generates a field isomorphic (over $\mathcal{K}$) to $\mathbf{K}$ if and only if h has a root in $\mathbf{K}$. Also, the number of isomorphic fields generated by the roots of f is n/r, where r is the number of roots of f in $\mathbf{K}$.

To count the number of roots in $\mathbf{K}$, we use Peter Panayi's root finding algorithm [Pa95].

Lemma 8.1 (Hensel)**.** *Let $\mathbf{K}$ be a field complete with respect to a non-archimedian absolute value $|\cdot|$, $\mathcal{O}_{\mathbf{K}}$ its valuation ring and $\mathfrak{P}$ its prime ideal. Let $f(x) \in \mathcal{O}_{\mathbf{K}}[x]$ and assume there exists $\alpha \in \mathcal{O}_{\mathbf{K}}$ satisfying $|f(\alpha)| < |f'(\alpha)|^2$. Then f has a root in $\mathcal{O}_{\mathbf{K}}$ congruent to α modulo $\mathfrak{P}$.*

A constructive proof of this lemma can be found in [Ca86]. Panayi's method relies on the following result.

Lemma 8.2. *Let $f(x) = f_n x^n + \ldots + f_0 \in \mathcal{O}_{\mathbf{K}}[x]$. Denote the minimum of the valuations of the coefficients of f by $v_{\mathfrak{P}}(f) := \min\left\{v_{\mathfrak{P}}(f_0), \ldots, v_{\mathfrak{P}}(f_n)\right\}$ and define $f^{\#} := f/\pi^{v_{\mathfrak{P}}(f)}$. For $\alpha \in \mathcal{O}_{\mathbf{K}}$, denote its representative in the residue field $\mathcal{O}_{\mathbf{K}}/\mathfrak{P}$ by $\overline{\alpha}$, and for $\beta \in \mathcal{O}_{\mathbf{K}}/\mathfrak{P}$, denote a lift of β to $\mathcal{O}_{\mathbf{K}}$ by $\hat{\beta}$.*

(a) *If α is a zero of $f(x)$ then $\overline{\alpha}$ is a zero of $\overline{f}(x)$.*
(b) *α is a zero of $f(x\pi + \hat{\beta})$ if and only if $\alpha\pi + \hat{\beta}$ is a zero of $f(x)$.*
(c) *α is a zero of $f(x)$ if and only if α is a zero of $f^{\#}(x)$.*
(d) *Let β be a zero of $\overline{f}$ and let $g(x) := f(x\pi + \hat{\beta})$. Then $\deg(\overline{g^{\#}}) \leq \deg(\overline{f^{\#}})$.*
(e) *If $\deg(\overline{f^{\#}}) = 0$ then f has no zero in $\mathcal{O}_{\mathbf{K}}$.*
(f) *If $\deg(\overline{f^{\#}}) = 1$ then f has a zero in $\mathcal{O}_{\mathbf{K}}$.*
(g) *If $\overline{f^{\#}}(x) = (x-\beta)^m h(x)$, where $((x-\beta), h(x)) = 1$, and if $g(x) := f(x\pi + \hat{\beta})$, then $\deg(\overline{g^{\#}}) \leq m$.*

Proof. Statements (a), (b), and (c) are obvious.

(d) Let $d = \deg(\overline{f^{\#}})$. Then $v_{\mathfrak{P}}(f_d) \leq v_{\mathfrak{P}}(f_\nu)$ for all $\nu \leq d$, and $v_{\mathfrak{P}}(f_d) < v_{\mathfrak{P}}(f_\nu)$ for all $\nu > d$. Now,

$$g_i = \sum_{j=i}^{n} \binom{j}{i} f_j \pi^i \hat{\beta}^{j-i};$$

therefore $v_{\mathfrak{P}}(g_d) = v_{\mathfrak{P}}(f_d) + d$ and $v_{\mathfrak{P}}(g_\nu) \geq v_{\mathfrak{P}}(f_d) + \nu$ for all $\nu > d$. Hence, $\deg(\overline{g^{\#}}) \leq \deg(\overline{f^{\#}})$.

(e) Clear in light of (a), (b), (c).

(f) Since $\deg(\overline{f^{\#}}) = 1$, we have $v_{\mathfrak{P}}(f_1^{\#}) = 0$ and $v_{\mathfrak{P}}(f_\nu^{\#}) \geq 1$ for $\nu > 1$. So $f^{\#\prime}(\hat{\beta}) \not\equiv 0 \pmod{\mathfrak{P}}$ and $f^{\#}(\hat{\beta}) \equiv 0 \pmod{\mathfrak{P}}$; thus $f^{\#}$ has a root by lemma 8.1, and f also by (c).

(g) Without loss of generality, we may assume that $f = f^{\#}$. Consider the Taylor expansion

$$f(\pi x + \hat{\beta}) = \sum_{i=0}^{n} \frac{f^{(i)}(\hat{\beta})}{i!} \pi^i x^i.$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

As $\overline{f}(x) = (x-\beta)^m h(x)$, we have $v_{\mathfrak{P}}(f^{(m)}(\hat{\beta})/m!) = 0$. It is also clear that $v_{\mathfrak{P}}(f^{(i)}(\hat{\beta})\pi^i/i!) \geq i > v_{\mathfrak{P}}(f^{(m)}(\hat{\beta})/m!)\pi^m = m$ for $i > m$. Hence $\deg(\overline{g^{\#}}) \leq m$. □

Assume f has a root β modulo $\mathfrak{P}$ and define two sequences $(f_\nu)_\nu$ and $(b_\nu)_\nu$ in the following way: $f_0 := f^{\#}$, $b_0 := \hat{\beta}$, and $f_{\nu+1}(x) := f_\nu^{\#}(x\pi + \hat{\beta}_\nu)$, $b_{\nu+1} := \hat{\beta}_\nu \pi^{\nu+1} + b_\nu$, where β_ν is a zero of $\overline{f_\nu}$, if there are any. At each step, one can find such a root if f has indeed a root (in $\mathcal{O}_{\mathbf{K}}$) congruent to β modulo $\mathfrak{P}$, and b_ν is congruent to this root modulo increasing powers of $\mathfrak{P}$. At some point, one of the following cases must occur: $\deg(\overline{f_\nu}) \leq 1$ and one uses 8.2 (e) or (f) to conclude; β_ν does not exist and thus b_ν is not an approximation of a root of f; $\nu \geq v_{\mathfrak{p}}(\mathrm{disc}(f))$ and then lemma 8.3 below tells us that lemma 8.2 (e) or (f) applies.

While constructing this sequence it may happen that $\overline{f_\nu}$ has more than one root. In this case we split the sequence and consider one sequence for each root. Lemma 8.2 (g) tells that there are never more than $\deg(f)$ candidate roots. Notice that if the conditions of lemma 8.2 (f) or lemma 8.3 are satisfied, the construction used in the proof of lemma 8.1 can be used to compute an arbitrarily good approximation of the root faster than with the root finding algorithm.

Lemma 8.3. *If $\nu \geq v_{\mathfrak{P}}(\mathrm{disc}(f))$, then $\deg(\overline{f_\nu}) \leq 1$.*

Proof. Assume $\deg(\overline{f_\nu}) \geq 2$. Since $f_\nu = f_\nu^{\#}$ by construction, it follows by considering the Taylor expansion

$$f_{\nu+1}(x) = f(\pi^{\nu+1}x + b_\nu) = \sum_{i=0}^{n} \frac{f^{(i)}(b_\nu)}{i!}\pi^{(\nu+1)i}x^i$$

that $f(b_\nu)$ and $f'(b_\nu)\pi^{\nu+1}$ must have a $v_{\mathfrak{P}}$-valuation greater than or equal to the valuation of $\pi^{2(\nu+1)}$. So $v_{\mathfrak{P}}(f(b_\nu)) \geq 2(\nu+1)$ and $v_{\mathfrak{P}}(f'(b_\nu)) \geq \nu+1$. In particular, f has (at least) a double root modulo $\mathfrak{P}^{\nu+1}$. But, the discriminant of f modulo $\mathfrak{P}^{\nu+1}$ is not zero by hypothesis; thus this is impossible. So $\deg(\overline{f_\nu}) < 2$. □

The following algorithm returns the number of zeroes of a polynomial f over a p-adic field $\mathbf{K}$. We use the notation from lemma 8.2.

Algorithm 8.4 (Root Counting)**.**
Input: $\mathbf{K}$, f
Output: *the number m of zeroes of f over* $\mathbf{K}$

- $C \leftarrow \{f^{\#}\}$.
- $m \leftarrow 0$.
- *While C is not empty:*
  - *For all c in C:*
    - $C \leftarrow C \setminus \{c\}$.
    - $R \leftarrow \{$*roots of* $\overline{c}$ *in* $\mathcal{O}_{\mathbf{K}}/\mathfrak{P}\}$.
    - *For all β in R:*
      - $h(x) \leftarrow c(\pi x + \hat{\beta})$.
      - $h \leftarrow h^{\#}$.
      - *If* $\deg \overline{h} = 1$ *then* $m \leftarrow m+1$.
      - *If* $\deg \overline{h} > 1$ *then* $C \leftarrow C \cup \{h\}$.
- *Return m.*

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

In order to prove that two irreducible polynomials f, h of the same degree generate the same field, it is possible to modify this algorithm so that it terminates as soon as it is known that one root of h belongs to the field $\mathbf{K}$ defined by f.

Computing Totally Ramified Extensions. Let $\mathcal{K}$ be a finite extension of $\mathbb{Q}_p$ with maximal ideal $\mathcal{P}$. Let n and j be such that they satisfy Ore's conditions. The following algorithm finds a minimal set of polynomials generating all totally ramified extensions of degree n and discriminant $\mathcal{P}^{n+j-1}$ using the polynomials A_ω defined in section 5.

Algorithm 8.5.
Input: $\mathcal{K}$, n, j
Output: *A minimal set of polynomials generating all totally ramified extensions of* $\mathbf{K}$ *of degree* n *and discriminant* $\mathcal{P}^{n+j-1}$

- *Compute* $\#\mathbf{K}_{n,j}$ *using theorem 6.1.*
- $L \leftarrow \emptyset$.
- $l \leftarrow 0$.
- *For* $\omega \in \Omega$*:*
  - *Let* $\varkappa$ *be a root of* $A_\omega(x)$.
  - *If no* $h \in L$ *has a root in* $\mathcal{K}(\varkappa)$ *then:*
    - $L \leftarrow L \cup \{A_\omega\}$.
    - *Let* r *be the number of roots of* A_ω *in* $\mathcal{K}(\varkappa)$.
    - $l \leftarrow l + n/r$.
  - *If* $l = \#\mathbf{K}_{n,j}$ *then return* L.

Notice that we could test all the polynomials A_ω for isomorphism and keep only the ones defining non-isomorphic extensions. However, since the number of these polynomials is far greater than the number of extensions, it is better to proceed as above, that is, to compute the number of extensions at the beginning and to stop when enough polynomials to generate all these extensions have been found. This explains why it is useful to know the number of such extensions before the construction.

There are several improvements that can be made to this algorithm. If p does not divide n, one can use theorem 7.2 to get directly a minimal set of polynomials generating all extensions. Also, the computation becomes faster if one enumerates the elements of Ω in such a way that the distance between polynomials in L and the next A_ω is maximal. Another way to improve the computation time is to use the following results, which enable us to compute the subfield lattice at the same time.

Proposition 8.6. *Let* $\mathbf{K}/\mathcal{K}$ *be a totally ramified field extension of degree* n *and discriminant* $\mathcal{P}^{n+j-1}$*. Let* n_0*,* n_1 *be two positive integers such that* $n = n_0 n_1$*. Then* $\mathbf{K}/\mathbf{k}$ *may have an intermediate field* $\mathbf{K}_0$ *of degree* n_0 *and discriminant* $\mathcal{P}^{n_0+j_0-1}$ *only if there exist integers* j_0, j_1 *such that* $j = j_0 n_1 + j_1$ *and such that* n_0, j_0 *and* n_1, j_1 *satisfy Ore's conditions.*

Proof. Assume that $\mathbf{K}/\mathcal{K}$ admits a sub-extension $\mathbf{K}_0/\mathcal{K}$ of degree n_0. Let $\mathfrak{P}_0$ be the prime ideal of $\mathbf{K}_0$ and let $\mathfrak{P}^{n_0+j_0-1}$ (resp. $\mathfrak{P}_0^{n_1+j_1-1}$) be the discriminant of $\mathbf{K}_0/\mathcal{K}$ (resp. $\mathbf{K}/\mathbf{K}_0$). Then n_0, j_0 and n_1, j_1 must satisfy Ore's conditions. Furthermore, by the formula for discriminants in a tower of extensions, we have

$$\mathrm{disc}_{\mathbf{K}/\mathcal{K}} = (\mathrm{disc}_{\mathbf{K}_0/\mathcal{K}})^{n_1} \cdot \mathbf{N}_{\mathbf{K}_0/\mathcal{K}}(\mathrm{disc}_{\mathbf{K}/\mathbf{K}_0}).$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Now, since $\mathbf{K}_0/\mathcal{K}$ is totally ramified, it follows that

$$\mathcal{P}^{n+j-1} = \mathcal{P}^{(n_0+j_0-1)n_1}\mathcal{P}^{n_1+j_1-1},$$

which proves the result. □

Proposition 8.7. *Let $\mathbf{K}$ be a totally ramified extension of $\mathcal{K}$ of degree n and discriminant $\mathcal{P}^{j+n-1}$, with $n = n_0p^s$ and $\gcd(n_0, p) = 1$. Then $\mathbf{K}$ has a tamely ramified subfield $\mathbf{K}_0$ of degree n_0 over $\mathcal{K}$ with discriminant $\mathcal{P}^{n_0-1}$.*

Proof. By proposition 8.6, $\mathbf{K}$ can only have subfields of degree n_0 over $\mathcal{K}$ with discriminant $\mathcal{P}^{n_0-1}$. Assume such a subfield $\mathbf{K}_0$ exists; then $\mathrm{disc}_{\mathbf{K}/\mathbf{K}_0} = \mathfrak{P}_0^{p^s+j_1-1}$, where $j_1 = j = a(n_0p^s) + b$ and $\mathfrak{P}_0$ is the prime ideal of $\mathbf{K}$. Using theorem 6.1, we obtain

$$\#\mathcal{K}_{n,j} = \#\mathcal{K}_{n_0,0}\,\#(\mathbf{K}_0)_{n_1,j}.$$

Hence either all extensions $\mathbf{K}$ have such a subfield of degree n_0, or some of the extensions $\mathbf{K}$ have two or more non-isomorphic subfields of degree n_0.

Let π be a uniformizer of $\mathcal{K}$. Assume $\mathbf{K}_0$ and $\mathbf{K}_1$ are non-isomorphic subfields of degree n_0 over $\mathcal{K}$, generated by the polynomials

$$f_0(x) = x^{n_0} + \zeta^{r_0}\pi \quad \text{and} \quad f_1(x) = x^{n_0} + \zeta^{r_1}\pi$$

respectively, see theorem 7.2. Let $\varkappa_0$ be a root of f_0; then

$$h(x) := -\frac{f_1(\varkappa_0 x)}{\pi^{n_0}} = x^{n_0} - \zeta^{r_1-r_0}$$

has a root in $\mathbf{K}$. If h has a root in $\mathcal{K}$ then $\mathbf{K}_0 \cong \mathbf{K}_1$, which contradicts the assumption $\mathbf{K}_0 \ncong \mathbf{K}_1$. Otherwise the extension $\mathbf{K}/\mathcal{K}$ has inertia degree greater than one, and this contradicts the assumption that $\mathbf{K}/\mathcal{K}$ is totally ramified. □

One way to improve the above algorithm using these results is first to compute all suitable sub-extensions $\mathbf{K}_0/\mathcal{K}$, and then to construct the absolute extensions $\mathbf{K}/\mathcal{K}$ which are relative extensions of $\mathbf{K}_0$. Since the number of polynomials to be considered is much smaller in the relative case and one has to look for roots of polynomials with smaller degree and discriminant, this improves the computation time considerably, especially in the case treated in proposition 8.7.

The proof of lemma 6.3 can also be used to compute a minimal set of polynomials in a different way. We use the notations of the proof of lemma 6.3. In addition to the map χ that sends a prime element α in $\Pi_{n,j}$ to its irreducible polynomial $\chi(\alpha)$ over $\mathcal{K}$, we define a map $\widetilde{\chi}$ from $\Pi_{n,j}$ to Ω that sends this prime element to the unique element $\omega \in \Omega$ such that $d(\chi(\alpha), A_\omega) \le r$. Also, for such a prime element α, we define the set $\mathcal{A}(\alpha)$ to be a (fixed) set of representatives of the prime elements of $\mathcal{K}(\alpha)$ modulo $\mathfrak{P}_\alpha^t$, where $\mathfrak{P}_\alpha$ is the prime ideal of $\mathcal{K}(\alpha)$. For example, one can choose $\mathcal{A}(\alpha)$ to be the set of elements $\alpha(\zeta_0 + \zeta_1\alpha + \cdots + \zeta_{t-2}\alpha^{t-2})$, where the ζ_j's range through a set of representatives of $\mathcal{O}_\mathcal{K}/\mathcal{P}$ and $\zeta_0 \not\equiv 0 \pmod{\mathcal{P}}$.

Proposition 8.8. *Let α be an element $\Pi_{n,j}$. Then the set $\{\widetilde{\chi}(\beta)\colon \beta \in \mathcal{A}(\alpha)\}$ is exactly the set of $\omega \in \Omega$ such that α and any root of A_ω define a $\mathcal{K}$-isomorphic extension.*

Moreover, for any such ω, the number m of $\beta \in \mathcal{A}(\alpha)$ such that $\widetilde{\chi}(\beta) = \omega$ is independent of ω and is the number of $\mathcal{K}$-automorphisms of $\mathcal{K}(\alpha)$; so, in particular, the number of conjugate fields over $\mathcal{K}$ of $\mathcal{K}(\alpha)$ is n/m.

Proof. This is a direct application of the proofs of corollary 5.3 and lemma 6.3. □

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

This gives us the following algorithm.

Algorithm 8.9.
Input: $\mathcal{K}$, n, j
Output: *A minimal set of polynomials generating all totally ramified extensions of* $\mathbf{K}$ *of degree* n *and discriminant* $\mathcal{P}^{n+j-1}$

- *Let* $\{\omega_1, \ldots, \omega_l\}$ *be the elements of* Ω.
- *For* $1 \leq i \leq l$, *set* $B_i \leftarrow 0$.
- $L \leftarrow \emptyset$.
- $c \leftarrow 1$.
- *While* $c \leq l$:
  - *if* $B_c = 0$:
    - $L \leftarrow L \cup \{A_{\omega_c}\}$.
    - *Let* $\varkappa$ *be a root of* A_{ω_c}.
    - *For all* d *such that* $\omega_d \in \widetilde{\chi}^{-1}(\mathcal{A}(\varkappa))$:
      - $B_d \leftarrow 1$.
  - $c \leftarrow c + 1$.
- *Return* L.

Since the basic operation in algorithm 8.9 is the computation of characteristic polynomials whereas the basic operation in algorithm 8.5 is the root finding algorithm, this algorithm seems faster than the latter. But this is not true in general. The reason is that the number of elements in $\mathcal{A}(\alpha)$ is $(q-1)q^{t-2}$, and so the number of such basic operations quickly becomes large. Furthermore, if in algorithm 8.5 the polynomials A_ω to consider are chosen cleverly, it can rapidly find polynomials defining all non-isomorphic extensions and thus be able to conclude using the root finding algorithm only a few times.

Computing All Extensions. We use the previous algorithms and the discussion of section 2 to write an algorithm computing all extensions of a given degree and discriminant. However, note that the minimal set of polynomials given by our algorithms might give the same extensions of $\mathbf{k}$ several times, since it is still possible that two extensions non-isomorphic over $\mathcal{K}$ are isomorphic over $\mathbf{k}$.

Since the extension $\mathcal{K}/\mathbf{k}$ is unramified, it is an abelian extension. Let Γ be its Galois group; it acts on Ω in the natural way: let $\sigma \in \Gamma$ and $\omega = (\omega_0, \ldots, \omega_{n-1})$, then $\sigma \cdot \omega = (\sigma(\omega_0), \ldots, \sigma(\omega_{n-1}))$. This action is well-defined since the sets $\mathcal{R}_{l,m}$, $\mathcal{R}^*_{l,m}$ are stable under the action of Γ. For $\omega \in \Omega$, define $\mathcal{B}(\omega)$ to be the set of elements $\omega' \in \Omega$ such that A_ω and A'_ω define $\mathcal{K}$-isomorphic extensions. Let α be a root of A_ω; it follows by proposition 8.8 that

$$\mathcal{B}(\omega) = \{\omega' \in \Omega : A_{\omega'} = \tilde{\chi}(\beta) \text{ for some } \beta \in \mathcal{A}(\alpha)\}.$$

Theorem 8.10. *Let* $\omega, \omega' \in \Omega$ *and let* α *(resp.* α'*) be any root of* A_ω *(resp.* $A_{\omega'}$*). Then the fields* $\mathcal{K}(\alpha)$ *and* $\mathcal{K}(\alpha')$ *are* $\mathbf{k}$*-isomorphic if and only if there exists* $\sigma \in \Gamma$ *such that*

$$\mathcal{B}(\sigma \cdot \omega) \cap \mathcal{B}(\omega') \neq \emptyset.$$

Furthermore, in this case, we have

$$\mathcal{B}(\sigma \cdot \omega) = \mathcal{B}(\omega').$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Proof. First note that the last assertion follows directly from the first one. Assume that $\mathcal{K}(\alpha)$ and $\mathcal{K}(\alpha')$ are $\mathbf{k}$-isomorphic extensions and let $\tilde{\sigma}$ be the $\mathbf{k}$-isomorphism sending $\mathcal{K}(\alpha)$ on $\mathcal{K}(\alpha')$. Let $\beta = \tilde{\sigma}(\alpha)$, and let $\sigma \in \Gamma$ denote the restriction of $\tilde{\sigma}$ to $\mathcal{K}$. Then $\tilde{\sigma}(A_\omega(\alpha)) = A_{\sigma\cdot\omega}(\beta) = 0$, so $\sigma \cdot \omega \in \mathcal{B}(\omega')$ since $\mathcal{K}(\beta) \cong \mathcal{K}(\alpha')$.

Now, let $\omega_1 \in \mathcal{A}(\omega)$ be such that $\sigma \cdot \omega_1 \in \mathcal{A}(\omega')$. Let α_1 be a root of A_{ω_1} and let $\tilde{\sigma}$ be any element of G extending σ. Then $\tilde{\sigma}(\alpha_1)$ is a root of $A_{\sigma\cdot\omega_1}$ and thus defines an extension of $\mathcal{K}$ isomorphic to $\mathcal{K}(\alpha')$ over $\mathcal{K}$ (and hence also over $\mathbf{k}$). Thus $\mathcal{K}(\alpha_1)$ is $\mathbf{k}$-isomorphic to $\mathcal{K}(\alpha')$, but $\mathcal{K}(\alpha_1)$ is $\mathcal{K}$-isomorphic to $\mathcal{K}(\alpha)$ since $\omega_1 \in \mathcal{A}(\omega)$, and therefore $\mathcal{K}(\alpha)$ and $\mathcal{K}(\alpha')$ are $\mathbf{k}$-isomorphic. □

Algorithm 8.11.

Input: $\mathbf{k}$, m, d

Output: *A minimal set of polynomials generating all extensions of* $\mathbf{k}$ *of degree* m *and discriminant* $\mathfrak{p}^d$

- $M \leftarrow \emptyset$.
- *For every positive divisor* l *of* m*:*
  - $n \leftarrow m/l$.
  - $j \leftarrow d/l - n + 1$.
  - *If* n, j *fulfill Ore's conditions then:*
    - *Let* $f(x) \in \mathcal{O}_{\mathbf{k}}[x]$ *be a monic polynomial of degree* l *that is irreducible over* $\mathcal{O}_{\mathbf{k}}/\mathfrak{p}[x]$.
    - *Let* $\mathcal{K}$ *be the field generated over* $\mathbf{k}$ *by a root* ζ *of* f.
    - *Using algorithm 8.5 or algorithm 8.9, compute a minimal set* L *of polynomials generating all totally ramified extensions of* $\mathcal{K}$ *of degree* n *and discriminant* $\mathcal{P}^{n+j-1}$.
    - *Using theorem 8.10, remove the polynomials defining* $\mathbf{k}$*-isomorphic fields.*
    - *For every* $h \in L$*:*
      - *Compute the characteristic polynomial* g *over* $\mathbf{k}$ *of* $\zeta + \varkappa$*, where* $\varkappa$ *is any root of* h.
      - $M \leftarrow M \cup \{g\}$,
- *Return* M.

These methods have been implemented in the computer algebra systems KASH [Da96] and PARI [Ba99]. They will be available in a future release of these systems.

9. Examples

Example 9.1 (Extensions of degree 9 and discriminant 3^{12} over $\mathbb{Q}_3$)**.** There are 54 extensions of degree 9 and discriminant 3^{9+4-1} over $\mathbb{Q}_3$. We compute all these as absolute extensions over $\mathbb{Q}_3$. We find the following generating polynomials, each of them defining 9 isomorphic extensions:

$$\begin{array}{ll} F_1(x) = x^9 + 3x^4 + 6x^3 + 3 & F_2(x) = x^9 + 3x^4 + 6 \\ F_3(x) = x^9 + 3x^4 + 3x^3 + 3 & F_4(x) = x^9 + 3x^4 + 3x^3 + 6 \\ F_5(x) = x^9 + 3 & F_6(x) = x^9 + 3x^4 + 6x^3 + 6 \end{array}$$

Following proposition 8.6, we compute the subfields of degree 3 and discriminant 3^{3+j_0-1}, where $j_0 = 1$. Notice that these are the only possible subfields. We find that there are six such subfields, generated by the roots of the two polynomials $f_1(x) = x^3 + 6x + 3$ and $f_2(x) = x^3 + 3x + 3$. Let π_1 and π_2 be zeroes of f_1 and f_2 respectively. Each of the fields $\mathbb{Q}_3(\pi_\nu)$ admits six totally ramified extensions of

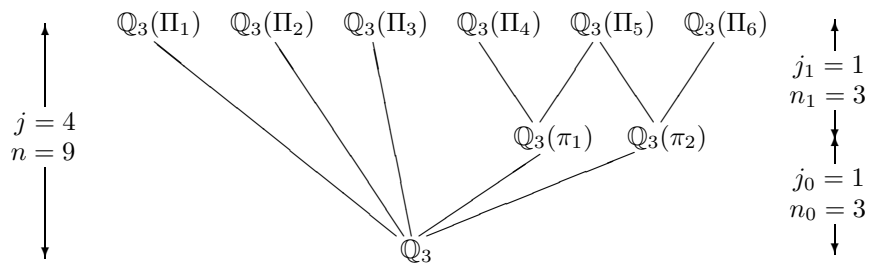
License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

degree $n_1 = 3$ and discriminant $(\pi_\nu)^{3+j_1-1}$, where $j_1 = 1$. These extensions are generated by $g_{\nu 1}(x) = x^3 + \pi_\nu x + \pi_\nu$ and $g_{\nu 2}(x) = x^3 + 2\pi_\nu x + \pi_\nu$ over $\mathbb{Q}_3(\pi_\nu)$.

Let $\gamma_{\nu\mu}$ denote a root of $f_{\nu\mu}$. Using algorithm 8.4, we get that

$$\mathbb{Q}_3(\pi_1)(\gamma_{12}) \cong \mathbb{Q}_3(\pi_2)(\gamma_{21})$$

and that the other fields are distinct. So we have found 27 extensions of degree 9 that have subfields of degree 3. Let Π_ν be a root of F_ν; then we obtain $\mathbb{Q}_3(\Pi_5) \cong \mathbb{Q}_3(\pi_1)(\gamma_{21}) \cong \mathbb{Q}_3(\pi_2)(\gamma_{12})$, $\mathbb{Q}_3(\Pi_6) \cong \mathbb{Q}_3(\pi_1)(\gamma_{22})$, and $\mathbb{Q}_3(\Pi_4) \cong \mathbb{Q}_3(\pi_2)(\gamma_{11})$. The lattice of subfields (up to isomorphism) is depicted below:



Example 9.2 (All extensions of degree 10 of $\mathbb{Q}_5$)**.** There is one unramified extension of degree 10; it is generated over $\mathbb{Q}_5$ by the roots of $g(x) = x^{10} + 2x^8 + 3$.

There are two extensions with residue degree 5 and ramification index 2. The unramified part $\mathcal{K}/\mathbb{Q}_5$ is defined by $g(x) = x^5 + 3x^3 + 3$ and the tamely ramified part $\mathbf{K}/\mathcal{K}$ by $h_\nu(x) = x^2 + 5\nu$, where $\nu = 1, 2$.

There are 605 extensions with residue degree 2 and ramification index 5. These extensions $\mathbf{K}$ are generated over the unramified field $\mathcal{K} := \mathbb{Q}_5(\rho)$, $\rho^2 + 2 = 0$, by the polynomials in the following table. The roots of each polynomial generate N distinct isomorphic extensions. Together, the polynomials in each line generate a total of $\#\mathbf{K}$ extensions of absolute discriminant 5^{5+j-1}.

j	generating polynomials	N	$\#\mathbf{K}$
1	$x^5 + 5(h_1 + h_2\rho)x + 5 \qquad h_1,\ h_2 \in \{0,1,2,3,4\},\ (h_1,h_2) \neq (0,0)$	5	120
2	$x^5 + 5(h_1 + h_2\rho)x^2 + 5 \qquad h_1,\ h_2 \in \{0,1,2,3,4\},\ (h_1,h_2) \neq (0,0)$	5	120
3	$x^5 + 5(h_1 + h_2\rho)x^3 + 5 \qquad h_1,\ h_2 \in \{0,1,2,3,4\},\ (h_1,h_2) \neq (0,0)$	5	120
4	$x^5 + 5(h_1 + h_2\rho)x^4 + 5 \qquad h_1,\ h_2 \in \{0,1,2,3,4\}$ $(h_1,h_2) \notin \{(0,0),(1,0),(2,1),(2,4),(3,1),(3,4),(4,0)\}$	5	90
4	$x^5 + 5(h_1 + h_2\rho)x^4 + 5 + 25h_0\rho \qquad h_0 \in \{0,1,2,3,4\}$ $(h_1,h_2) \in \{(1,0),(2,1),(2,4),(3,1),(3,4)\}$	1	25
4	$x^5 + 4 \cdot 5x^4 + 5 + 25h_0 \qquad h_0, \in \{0,1,2,3,4\}$	1	5
5	$x^5 + 5 + 25(h_1 + h_2\rho) \qquad h_1,\ h_2 \in \{0,1,2,3,4\}$	5	125

There are 1210 totally ramified extensions of degree 10 of $\mathbb{Q}_5$. Using proposition 8.7, we find that they are relative extensions over one of the two tamely ramified extensions of degree 2 defined by $g_\nu(x) = x^2 + 5\nu$, where $\nu = 1, 2$. Let π_ν be a root of g_ν. The wildly ramified part is generated by the polynomials in the following table over $\mathbb{Q}_5(\pi_\nu)$. The roots of each polynomial generate N distinct isomorphic

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

extensions. Together, the polynomials in each line generate $\#\mathbf{K}$ extensions of absolute discriminant 5^{10+j-1}.

j	generating polynomials		N	$\#\mathbf{K}$
1	$x^5 + h_1\pi_\nu x + \pi_\nu$	$h_1 \in \{1,2,3,4\}$	5	20
2	$x^5 + h_2\pi_\nu x^2 + \pi_\nu$	$h_2 \in \{1,2,3,4\}$	5	20
3	$x^5 + h_3\pi_\nu x^3 + \pi_\nu$	$h_3 \in \{1,2,3,4\}$	5	20
4	$x^5 + h_4\pi_\nu x^4 + \pi_\nu$	$h_4 \in \{1,2,3\}$	5	15
4	$x^5 + 4\pi_\nu x^4 + (\pi_\nu + h_0\pi_\nu^2)$	$h_0 \in \{0,1,2,3,4\}$	1	5
6	$x^5 + h_1\pi_\nu^2 x + (\pi_\nu + h_0\pi_\nu^2)$	$h_1 \in \{1,2,3,4\}$, $h_0 \in \{0,1,2,3,4\}$	5	100
7	$x^5 + h_1\pi_\nu^2 x^2 + (\pi_\nu + h_0\pi_\nu^2)$	$h_1 \in \{1,2,3,4\}$, $h_0 \in \{0,1,2,3,4\}$	5	100
8	$x^5 + h_1\pi_\nu^2 x^3 + (\pi_\nu + h_0\pi_\nu^2)$	$h_1 \in \{1,2,4\}$, $h_0 \in \{0,1,2,3,4\}$	5	75
8	$x^5 + 3\pi_\nu^2 x^3 + (\pi_\nu + h_0\pi_\nu^2 + h_1\pi_\nu^3)$	$h_0,\ h_1 \in \{0,1,2,3,4\}$	1	25
9	$x^5 + h_1\pi_\nu^2 x^4 + (\pi_\nu + h_0\pi_\nu^2)$	$h_1 \in \{1,2,3,4\}$, $h_0 \in \{0,1,2,3,4\}$	5	100
10	$x^5 + (\pi_\nu + h_2\pi_\nu^2 + h_3\pi_\nu^3)$	$h_2,\ h_3 \in \{0,1,2,3,4\}$	5	125

This gives 605 extensions of degree 5 over $\mathbb{Q}(\pi_1)$ (resp. $\mathbb{Q}(\pi_2)$). Hence there are 1818 extensions of degree 10 of $\mathbb{Q}_5$. Note that there are only 293 non-isomorphic extensions of degree 10 of $\mathbb{Q}_5$.

10. Future developments

The methods described above work fine for small examples, *i.e.*, when the number $\#D_{\mathbf{E}_{n,j}}$ of polynomials A_ω with $\omega \in \Omega$ is small.

The number of polynomials can easily be reduced by using, in addition to the degree and discriminant invariants, indices of inseparability (see [He94]). The indices of inseparability can be translated directly into conditions on the coefficients on the polynomials.

Furthermore, our algorithm can be refined to the computation of all p-extensions (*i.e.*, finite, normal, separable extensions, whose degrees are powers of the prime p) with a given Galois group using the formulas for the number of such extensions given by I. R. Shafarevich [Sh47] for the case that $\mathbf{k}$ does not contain the p-th roots of unity and by M. Yamagishi [Ya95] for the general case. Here the main obstacle is filtering out the polynomials with the right Galois group.

These approaches are subjects of ongoing research.

References

[Ba99] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier. *The Computer Algebra System PARI-GP*, Université Bordeaux I, 1999, `ftp://megrez.math.u-bordeaux.fr/pub/pari/`

[Ca86] J.W.S. Cassels. *Local Fields*, London Mathematical Society Students Text **3**, Cambridge University Press, 1986. MR **87i:**11172

[Da96] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, KANT V4, J. Symb. Comp. **11** (1996), 267–283; also see `http://www.math.tu-berlin.de/~kant/`. MR **99g:**11150

[Ha69] H. Hasse, *Number Theory*, Grundlehren der mathematischen Wissenschaften **229**, Springer-Verlag, Berlin, 1980. MR **81c:**12001

[He94] V. Heiermann, *De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux*, J. Number Theory **59** (1994), 159–202. MR **97e:**11148

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

[Kr66] M. Krasner, *Nombre des extensions d'un degré donné d'un corps* $\mathfrak{p}$*-adique*, Les Tendances Géométriques en Algèbre et Théorie des Nombres, Ed. CNRS, Paris, 1966, pp. 143–169. MR **37:**1349

[Kr79] M. Krasner, *Remarques au sujet d'une note de J.-P. Serre*, C. R. Acad. Sci. Paris **288** (1979), 863–865. MR **80k:**12023

[Or26] Ö. Ore, *Bemerkungen zur Theorie der Differente*, Math. Zeitschr. **25** (1926), pp. 1–8.

[Pa95] P. Panayi, *Computation of Leopoldt's p-adic regulator*, PhD thesis, University of East Anglia, 1995, `http://www.mth.uea.ac.uk/~h090/`.

[Se63] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1963. MR **27:**133

[Se78] J.-P. Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris **286** (1978), A1031–A1036. MR **80a:**12018

[Sh47] I. R. Shafarevich, *On p-extensions* , Mat. Sb., Nov. Ser. **20(62)** (1947), 351–363; English Transl., AMS Transl. II. Ser. **4** (1956), 59–72. MR **8:**560e

[Ya95] M. Yamagishi, *On the number of Galois p-extensions of a local field*, AMS Proc. 123 (1995), 2375–2380. MR **95j:**11109

Centre Interuniversitaire en Calcul Mathématique Algébrique, Concordia University, 1455 de Maisonneuve Blvd. W., Montréal, Québec, H3G 1M8, CANADA

E-mail address: `pauli@cicma.concordia.ca`

Institut Girard Desargues, Université Claude Bernard (Lyon 1), 43, boulevard du 11 Novembre 1918, 69622 Villeurbanne cedex, France

E-mail address: `roblot@desargues.univ-lyon1.fr`

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use