Efficient Enumeration of Extensions of Local Fields with Bounded Discriminant

Sebastian Pauli

A Thesis

in

The Department

of

Mathematics and Statistics

Presented in Partial Fulfilment of the Requirements
for the Degree of Doctor of Philosophy at
Concordia University
Montreal, Quebec, Canada

June 2001

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By:	Mr. Sebastian Pauli
Entitled:	Efficient Enumeration of Extensions of Local Fields with Bounded Discriminant

and submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy (Mathematics)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Dr. S. Misra	Chair
Dr. J. Labute	External Examiner
Dr. C. David	Examiner
Dr. H. Kisilevsky	Examiner
Dr. F. Thaine	Examiner
Dr. D. Ford	Thesis Supervisor

Approved by	Dr. C. Cummins Graduate Program Director
Sept. 24th 2001	Dr. M. Singer Dean of Faculty

Abstract

Efficient Enumeration of Extensions of Local Fields with Bounded Discriminant

Sebastian Pauli, Ph.D.

Concordia University, 2001

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 [1966] gives 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. We also present canonical sets of generating polynomials of extensions of degree p^m. Some methods from the proof of the number of extensions of a given degree and discriminant can also be used for the determination of a bound that gives a considerably improved estimate of the complexity of polynomial factorization over local fields. We use this bound in an efficient new algorithm for factoring a polynomial Φ over a local field $\mathbf{k}$. For every irreducible factor $\varphi(x)$ of $\Phi(x)$ our algorithm returns an integral basis for $\mathbf{k}[x]/\varphi(x)\mathbf{k}[x]$ over $\mathbf{k}$.

Table of Contents

List of Symbols

$\alpha^{(i)}$	i-th conjugate of α	Section 1.2
$\|\alpha\|$	absolute value of alpha	Definition 1.1.1
$\alpha \equiv \beta$	$v(\alpha-\beta) > \max\{v(\alpha), v(\beta)\}$ or $\alpha=\beta=0$	
$(\alpha) = \alpha\mathcal{O}_{\mathbf{k}}$	ideal generated by $\alpha \in \mathcal{O}_{\mathbf{k}}$	
$\#A$	number of elements in a set A	
$A_\omega(x)$		Section 3.3
$\mathsf{C}(n)$		Section 1.4
$\chi_\vartheta(y)$	Characteristic polynomial of $\vartheta(x)$	Definition 2.3.2
$d(\varphi,\psi)$	ultrametric distance on $\mathbf{E}_{n,j}$	Proposition 3.2.3
$D_M(a,r)$	disc of radius r with center a in M	Section 3.4
$\#D_{\mathbf{E}_{n,j}}(r)$		Lemma 3.4.3
$\mathrm{disc}\,(\varphi)$	discriminant of the polynomial φ	Definition 1.2.4
$\mathrm{disc}\,(\mathbf{K}/\mathbf{k})$	discriminant of the extension $\mathbf{K}/\mathbf{k}$	Definition 1.2.5
$e_{\mathbf{K}/\mathbf{k}}$	ramification index of $\mathbf{K}/\mathbf{k}$	Definition 1.2.8
$e = e_{\mathbf{k}/\mathbb{Q}_p}$	ramification index of $\mathbf{k}/\mathbb{Q}_p$	
E_ϑ		Definition 2.4.1
$\mathbf{E}_{n,j}$	set of Eisenstein polynomials of degree n and discriminant $\mathfrak{p}^{n+j-1}$	Section 3.2
$f_{\mathbf{K}/\mathbf{k}}$	inertia degree of $\mathbf{K}/\mathbf{k}$	Definition 1.2.8
$f = f_{\mathbf{k}/\mathbb{Q}_p}$	inertia degree of $\mathbf{k}/\mathbb{Q}_p$	
F_ϑ		Definition 2.4.1
$\mathbb{F}_q$	finite field with q elements	
$\mathbb{F}_q(t)$	function field in t over $\mathbb{F}_q$	
$\mathbb{F}_q((t))$	field of Laurent series over $\mathbb{F}_q$	
$\mathrm{Gal}(\varphi)$	Galois group of the splitting field of the polynomial $\varphi(x)$	Definition 1.2.2
$\mathrm{Gal}(\mathbf{K},\mathbf{k})$	Galois group of $\mathbf{K}/\mathbf{k}$	Definition 1.2.2

$\gcd(a,b)$	greatest common divisor of a and b	
$j = an + b$		Section 3.1
$\mathbf{k}$	a local field	Definition 1.1.7
$\mathbf{k}[x]$	ring of polynomials over $\mathbf{k}$	
$\underline{\mathbf{k}} = \mathcal{O}_{\mathbf{k}}/\mathfrak{p}$	residue class field of $\mathbf{k}$	Definition 1.1.9
$\overline{\mathbf{k}}$	algebraic closure of $\mathbf{k}$	
$\mathbf{K}_{n,j}$	set of all extensions of $\mathbf{k}$ of degree n and discriminant $\mathfrak{p}^{n+j-1}$	Definition 3.2.1
$\#\mathbf{K}_{n,j}$	number of elements in $\mathbf{K}_{n,j}$	Theorem 3.4.2
$l(i)$		Section 3.3
$L(i)$		Sections 3.6, 3.7
$\operatorname{lcm}(a,b)$	least common multiple of a and b	
$\mathsf{M}(n)$		Section 1.4
$\mu(\alpha)$	minimal polynomial of α	Lemma 3.4.1
$\mathrm{N}(\alpha)$	norm of an element α	Section 1.2
$\mathrm{N}(\varphi)$	norm of a polynomial $\varphi(x)$	Definition 2.3.9
$\nu_{\vartheta}(y)$		Definition 2.3.3
$O(\cdot)$	big-O	Definition 1.4.1
$\mathcal{O}_{\mathbf{k}}$	valuation ring of $\mathbf{k}$	Definition 1.1.9
$\mathsf{P}(n,f)$		Section 1.4
$\mathfrak{p} = (\pi)$	the maximal ideal of $\mathcal{O}_{\mathbf{k}}$	Definition 1.1.9
$\varphi^{\#}(x)$		Lemma 2.1.2
π	prime element of $\mathcal{O}_{\mathbf{k}}$	
$\Pi_{n,j}$		Lemma 3.4.1
$\mathbb{Q}_p$	field of p-adic numbers	Example 1.1.8
$\mathcal{R}$	multiplicative set of representatives of $\underline{\mathbf{k}}$ in $\mathbf{k}$	Sections 3.6, 3.7
$\mathcal{R}_{l,m}$, $\mathcal{R}^*_{l,m}$		Section 3.3
$\operatorname{res}_x(\varphi,\vartheta)$	resultant of the polynomials φ and ϑ in x	
$\mathsf{T}(m,n)$		Section 1.4
$v(\alpha)$	exponential valuation of α	Definition 1.1.2
$v_\alpha(\beta)$	exponential valuation, normalized such that $v_\alpha(\alpha) = 1$	Definition 1.1.9
$v(\varphi)$	minimum of the valuations of the coefficients of a polynomial $\varphi(x)$	Lemma 2.1.2
$v^*_{\mathfrak{p}}(\varphi)$	$v_{\mathfrak{p}}$-star valuation of a polynomial $\varphi(x)$	Definition 2.3.3

Introduction

Let $\mathbf{k}$ be a local field, *i.e.*, a field complete with respect to a discrete prime divisor $\mathfrak{p}$, and fix an algebraic closure $\overline{\mathbf{k}}$ of $\mathbf{k}$.

Most results in chapter 2 hold for a local field in general; this includes local fields with infinite residue class field.

In chapter 3 the field $\mathbf{k}$ will be a finite extension of the p-adic numbers $\mathbb{Q}_p$ for some prime number p.

For $\mathbf{K}$ a finite extension of $\mathbf{k}$ the description of the lattice of extensions of $\mathbf{K}$ in $\overline{\mathbf{k}}$ is an important problem in the theory of $\mathfrak{p}$-adic fields.

If we restrict our attention to Abelian extensions then this description is complete and is given by Local Class Field Theory (see *e.g.* [Serre, 1963] or [Fesenko and Vostokov, 1993]). In the general case, such a description is not yet known. But if we restrict ourselves to local fields with finite residue class field the number of extensions of a given degree and discriminant is finite. It is even possible to ask for a formula that gives the number of extensions of a given degree, and for methods to compute them. Krasner [1966] gives such a formula, 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.

Note that Serre [1978] 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 [Krasner, 1979]).

In chapter 3 we give a new proof of Krasner's formula for the number of extensions of a $\mathfrak{p}$-adic field of a given degree and discriminant. We use the formulae for the number of extensions to compute a minimal set of polynomials that generate all extensions of a $\mathfrak{p}$-adic field of degree p and give an algorithm for the computation of all extensions of a given degree.

Some methods from the proof of the number of extensions of a given degree and discriminant can also be used for the determination of a bound that gives a considerably improved estimate of the complexity of polynomial factorization over local fields.

The factorization of polynomials over local fields is closely related to the computation of integral bases of local and global fields and can be applied to the factorization of ideals in global fields. Several polynomial factorization algorithms have been published:

- The Round Four algorithm of Zassenhaus [Ford, 1978, 1987, Ford and Letard, 1994] was originally conceived as an algorithm for the computation of integral bases of algebraic number fields and is fast in most cases. In some cases however a branch of the algorithm with exponential complexity is needed.
- Chistov [1991] proved the existence of a polynomial-time algorithm for factoring polynomials over local fields.
- The algorithm for factoring ideals of Buchmann and Lenstra described by Cohen [1993, section 6.2] can be used for factoring polynomials over a local field in polynomial time. (However, it needs an integral basis as an input.)
- The algorithm by Montes [1999] is formulated as an algorithm for the decomposition of ideals over number fields and is based on ideas of Ore [1926]. He does not provide a complexity analysis.
- The improved Round Four algorithm by Ford et al. [2000] is considerably faster than the original Round Four algorithm. Formulated as an algorithm for factoring a polynomial $\Phi(x)$ over $\mathbb{Q}_p$, it returns a local integral basis (in fact, a power basis) for $\mathbb{Q}_p[x]/\varphi(x)\mathbb{Q}_p[x]$ for each irreducible factor $\varphi(x)$ of $\Phi(x)$. The algorithm terminates in polynomial time.
- Cantor and Gordon [2000] have developed an algorithm for deriving an irreducible factor of a polynomial $\Phi(x) \in \mathbf{k}[x]$ of degree N over an extension $\mathbf{k}$ of degree k over $\mathbb{Q}_p$. In their talk at the fourth Algorithmic Number Theory Symposium in July 2000 they announced that they had reduced the expected number of bit

operations to

$$O(N^{4+\varepsilon} v_{\mathfrak{p}}(\operatorname{disc} \Phi)^{2+\varepsilon} \log^{1+\varepsilon} p^k).$$

The algorithm presented chapter 2 has its origins in the Round Four algorithm. It returns all irreducible factors $\varphi(x)$ of a polynomial $\Phi(x)$ over the valuation ring of a local field $\mathbf{k}$ together with an integral basis for $\mathbf{k}[x]/\varphi(x)\mathbf{k}[x]$. If $\mathbf{k}$ is a finite extension of $\mathbb{Q}_p$ of degree k, our algorithm derives a complete factorization of a polynomial $\Phi(x)$ of degree N with the expected number of bit operations being

$$O\big(N^{3+\varepsilon} v_{\mathfrak{p}}(\operatorname{disc} \Phi)^{1+\varepsilon} \log^{1+\varepsilon} p^k + N^{2+\varepsilon} v_{\mathfrak{p}}(\operatorname{disc} \Phi)^{2+\varepsilon} \log^{1+\varepsilon} p^k\big).$$

Parts of this thesis have been published in [Pauli and Roblot, 2001] and [Pauli, 2001].

Acknowledgements

I would like to thank

- David Ford for his support during the last three and a half years,
- David Cantor and Dan Gordon for convincing me that working over unramified extensions is more efficient,
- Xavier Roblot for the fruitfull colaboration,
- Frances Clerk and Robert Juricevic for their careful reading of this thesis and their useful suggestions,
- John Cannon and Claus Fieker for inviting me to Sydney to implement the polynomial factorization algorithm in the computer algebra system Magma [Bosma and Cannon, 1995],
- Masakazu Yamagishi for his hospitality during my stay in Nagoya, his useful suggestions, and the table of the number of Galois extensions of degree p^2 of $\mathfrak{p}$-adic fields.

Chapter 1

Preliminaries

1.1 Local Fields

We recall definitions and fundamental results in the theory of local fields. More detailed exposition can be found in [Fesenko and Vostokov, 1993] and [Hasse, 1963].

Definition 1.1.1. A function $|\cdot|$ from a field $\mathbf{k}$ into the nonnegative reals such that

(i) $|\alpha| = 0 \iff \alpha = 0$,

(ii) $|\alpha\beta| = |\alpha|\cdot|\beta|$,

(iii) $|\alpha + \beta| \leqslant \max\{|\alpha|, |\beta|\}$.

is called a *non-archimedean* or *ultrametric absolute value* on $\mathbf{k}$.

Definition 1.1.2. A function v from a field $\mathbf{k}$ into $\mathbb{Q} \cup \{\infty\}$ such that

(i) $v(\alpha) = \infty \iff \alpha = 0$,

(ii) $v(\alpha\beta) = v(\alpha) + v(\beta)$,

(iii) $v(\alpha + \beta) \geqslant \min\{v(\alpha), v(\beta)\}$.

is said to be a (an *exponential*) *valuation* on $\mathbf{k}$.

Note that if v is an exponential valuation on a field $\mathbf{k}$ and if $r \in \mathbb{R}$, $0 < r < 1$, then

$$|a| := \begin{cases} 0 & \text{if } a = 0 \\ r^{v(a)} & \text{otherwise} \end{cases}$$

is a non-archimedian absolute value on $\mathbf{k}$.

Example 1.1.3. Let p be a prime number. Every $a \in \mathbb{Q}$ can be uniquely represented by $a = p^m(r/s)$ with $m, r \in \mathbb{Z}$, $s \in \mathbb{N}$ and p, r, s pairwise relatively prime. The map $v_p : a \mapsto m$ is a exponential valuation on $\mathbb{Q}$. The map $|\cdot|_p : a \mapsto p^{-m}$ is a non-archimedian absolute value on $\mathbb{Q}$. We call $v_p(\cdot)$ the p-adic exponential valuation and $|\cdot|_p$ the p-adic absolute value.

Remark 1.1.4. The absolute value $|\cdot|_\infty$, defined by

$$|a|_\infty := \begin{cases} \alpha & \text{if } \alpha \geqslant 0 \\ -\alpha & \text{if } \alpha < 0 \end{cases}$$

fulfills the weaker triangle inequality

(iii)$'$ $|\alpha + \beta| \leqslant |\alpha| + |\beta|$

instead of the ultrametric inequality (iii). Absolute values which fulfill (iii)$'$ but not (iii) are called archimedean absolute values.

Theorem 1.1.5 (Ostrowski). *An absolute value on $\mathbb{Q}$ either coincides with $(|\cdot|_\infty)^r$ for some $r \in \mathbb{R}$, or with $(|\cdot|_p)^r$ for some prime p and some $r \in [0, 1]$.*

Example 1.1.6. Let $\mathbf{k}(t)$ be the rational function field over $\mathbf{k}$.

(i) For $\beta(t), \gamma(t) \in \mathbf{k}[t]$ with $\beta(t) \neq 0$ set $\deg(\beta/\gamma) = \deg(\beta) - \deg(\gamma)$. Then

$$v_\infty(\alpha) := \begin{cases} \infty & \text{if } \alpha(t) = 0 \\ \deg \alpha & \text{otherwise} \end{cases}$$

defines a valuation on $\mathbf{k}(t)$.

(ii) Let $\psi(t)$ be a monic, irreducible polynomial in $\mathbf{k}[t]$. Every $\alpha(t) \in \mathbf{k}(t)$ has a unique representation $\alpha(t) = \psi(t)^m \dfrac{\beta(t)}{\gamma(t)}$ with $m \in \mathbb{Z}$, $\beta(t), \gamma(t) \in \mathbf{k}[t]$ and $\gcd(\psi(t), \beta(t)) = 1$, $\gcd(\psi(t), \gamma(t)) = 1$, $\gamma(t)$ monic and $\gcd(\beta(t), \gamma(t)) = 1$. The map $v_{\psi(t)} : \alpha \mapsto m$ is a valuation on $\mathbf{k}(t)$.

Definition 1.1.7. We call a field a *local field* if it is complete with respect to a discrete (non-archimedean) absolute value.

Example 1.1.8. Let $|\cdot|_p$ be the p-adic absolute value defined in example 1.1.3. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is denoted by $\mathbb{Q}_p$.

Let $\mathbf{k}$ be a field with an exponential valuation v. Denote the completion of $\mathbf{k}$ by $\widehat{\mathbf{k}}$. The field $\widehat{\mathbf{k}}$ is a discrete valued field with exponential valuation $\widehat{v}(\lim_{i\to\infty}\alpha_n) := \lim_{i\to\infty} v(\alpha_n)$ where $(\alpha_n)_{n\in\mathbb{N}}$ is a Cauchy sequence. We usually denote $\widehat{v}$ by v as well.

Definition 1.1.9. Let $\mathbf{k}$ be a local field, with absolute value $|\cdot|$. We call

$$\mathcal{O}_{\mathbf{k}} := \{\alpha \in \mathbf{k} \mid |\alpha| \leqslant 0\}$$

the *valuation ring* of $\mathbf{k}$. $\mathcal{O}_{\mathbf{k}}$ is a local ring with maximal ideal

$$\mathfrak{p} := \{\alpha \in \mathbf{k} \mid |\alpha| < 0\},$$

which is principal. We denote by π a generator of $\mathfrak{p}$. The element π is called a prime element of $\mathbf{k}$.

We write $v_{\mathfrak{p}}$ or v_π for the exponential valuation on $\mathbf{k}$ which is normalized such that $v_{\mathfrak{p}}(\pi) = v_\pi(\pi) = 1$.

We call $\underline{\mathbf{k}} := \mathcal{O}_{\mathbf{k}}/\mathfrak{p}$ the *residue class field* of $\mathbf{k}$. For $\gamma \in \mathbf{k}$ we denote by $\underline{\gamma}$ the class $\gamma + \mathfrak{p}$ in $\underline{\mathbf{k}}$.

1.2 Extensions of local fields

Definition 1.2.1. Let $\mathbf{k}$ be a field. We call a polynomial $\varphi(x) \in \mathbf{k}[x]$ *separable* if every irreducible factor of $\varphi(x)$ has simple roots over its splitting field. Otherwise $\varphi(x)$ is called *inseparable.*

Let $\mathbf{k}$ be a local field and let $\varphi(x) \in \mathbf{k}[x]$ be a separable, monic, and irreducible polynomial of degree n. We obtain an algebraic extension $\mathbf{K}$ of $\mathbf{k}$ by adjoining a root α of $\varphi(x)$ to $\mathbf{k}$:

$$\mathbf{K} = \mathbf{k}(\alpha) \cong \mathbf{k}[x]/\varphi(x)\mathbf{k}[x].$$

We say $\mathbf{K}/\mathbf{k}$ is an extension of degree $[\mathbf{K} : \mathbf{k}] = n$. Denote the roots of $\varphi(x)$ in an algebraic closure $\overline{\mathbf{k}}$ of $\mathbf{k}$ by $\alpha = \alpha^{(1)}, \ldots, \alpha^{(n)}$. We call $\alpha^{(l)}$ the *l-th conjugate* of α. The field $\mathbf{K}$ is a vector space of dimension n over $\mathbf{k}$, and the n-tuple $(1, \alpha, \ldots, \alpha^{n-1})$ is a basis of $\mathbf{K}$ over $\mathbf{k}$. Thus every element $\beta \in \mathbf{K}$ has a unique representation $\beta = \sum_{i=0}^{n-1} \gamma_i \alpha^i$ with $\gamma_i \in \mathbf{k}$ for $0 \leqslant i \leqslant n-1$. The conjugates of β are $\beta^{(l)} = \sum_{i=0}^{n-1} \gamma_i \left(\alpha^{(l)}\right)^i$ for $1 \leqslant i \leqslant n$.

We define the *norm* $\mathrm{N}(\beta)$ of β by $\mathrm{N}(\beta) = \prod_{l=1}^{n} \beta^{(l)}$.

Definition 1.2.2. Let $\mathbf{K}$ be an algebraic extension of $\mathbf{k}$. We denote the group of automorphisms of $\mathbf{K}$ by $\mathrm{Aut}(\mathbf{K})$. We call

$$\mathrm{Gal}(\mathbf{K}/\mathbf{k}) := \{\sigma \in \mathrm{Aut}(\mathbf{K}) \mid \sigma(\alpha) = \alpha \text{ for all } \alpha \in \mathbf{k}\}$$

the *Galois group of* $\mathbf{K}/\mathbf{k}$.

If $\varphi(x)$ is a non-constant polynomial in $\mathbf{k}[x]$ and $\mathbf{K}$ is the splitting field of $\varphi(x)$ then we call $\mathrm{Gal}(\varphi) := \mathrm{Gal}(\mathbf{K}/\mathbf{k})$ the *Galois group of* $\varphi(x)$.

If $\mathbf{K} \cong \mathbf{k}[x]/\varphi(x)\mathbf{k}[x]$ is the splitting field of $\varphi(x) \in \mathbf{k}[x]$ we say that the extension $\mathbf{K}/\mathbf{k}$ is Galois.

Theorem 1.2.3. *Let $\mathbf{K}$ be a finite algebraic extension of degree n of a local field $\mathbf{k}$ with exponential valuation $v_{\mathfrak{p}}(\cdot)$. Then there exists one and only one prolongation $\widetilde{v}_p$ of the exponential valuation $v_{\mathfrak{p}}$ to an exponential valuation $\widetilde{v}_p : \mathbf{K} \to \mathbb{Q} \cup \{\infty\}$ with $\widetilde{v}_p|_{\mathbf{k}} = v_{\mathfrak{p}}$. This prolongation $\widetilde{v}_p$ is defined by $\widetilde{v}_p(\alpha) = v_{\mathfrak{p}}(\mathrm{N}(\alpha))/n$ for $\alpha \in \mathbf{K}$. The field $\mathbf{K}$ is complete with respect to $\widetilde{v}_p$.*

Let $\overline{\mathbf{k}}$ be an algebraic closure of $\mathbf{k}$. The prolongations of $|\cdot|$ and $v_{\mathfrak{p}}$ to $\overline{\mathbf{k}}$ or any intermediate field $\widehat{\mathbf{k}}$ will also be denoted by $|\cdot|$ and $v_{\mathfrak{p}}$, respectively.

Definition 1.2.4. Let $\psi(x) \in \mathbf{k}[x]$ be monic with $\psi(x) = \prod_{l=1}^{n}(x - \xi_l)$ where $\xi_l \in \overline{\mathbf{k}}$. We define $\mathrm{disc}\,(\psi) := \prod_{l<k}(\xi_l - \xi_k)^2 = \prod_{l\neq k}(-1)^{(n^2-n)/2}(\xi_l - \xi_k)$.

If $\psi(x)$ is irreducible and ξ is any root of $\psi(x)$ then $\mathrm{disc}\,(\psi) = \mathrm{N}(\psi'(\xi))$.

Let $\mathbf{K}/\mathbf{k}$ be an algebraic extension of degree n. Then $\mathcal{O}_{\mathbf{K}}$ is a free $\mathcal{O}_{\mathbf{k}}$-module of degree n. We call a basis of $\mathcal{O}_{\mathbf{K}}$ over $\mathcal{O}_{\mathbf{k}}$ an integral basis of $\mathbf{K}/\mathbf{k}$.

Definition 1.2.5. Let $(\delta_0, \dots, \delta_{n-1})$ be an integral basis of $\mathbf{K}/\mathbf{k}$. We call $\mathrm{disc}\,(\mathbf{K}/\mathbf{k}) := \det((\delta_k^{(l)})_{0\leqslant k\leqslant n-1, 1\leqslant l\leqslant n})^2$ the discriminant of $\mathbf{K}/\mathbf{k}$.

Definition 1.2.6. Let $\mathbf{K}$ be a finite algebraic extension of $\mathbf{k}$. We say $\mathbf{K}/\mathbf{k}$ is *unramified* if $[\mathbf{K} : \mathbf{k}] = [\underline{\mathbf{K}} : \underline{\mathbf{k}}]$.

For every positive integer 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 $\varphi_l(x)$. Then any (monic) lift of this polynomial to $\mathbf{k}[x]$ will define $\mathbf{K}$ over $\mathbf{k}$. Since easy estimates give that the ratio of the number of monic irreducible polynomials over $\underline{\mathbf{k}}$ to the number of all monic polynomials of degree l is about $1/l$, this method is adequate for the values of l we will deal with in this thesis.

If $\mathbf{K}/\mathbf{k}$ is an unramified extension given by a root of such a polynomial $\varphi_l(x)$ then $v_\mathfrak{p}(\mathrm{disc}\,(\varphi_l)) = v_\mathfrak{p}(\mathrm{disc}\,(\mathbf{K}/\mathbf{k})) = 0$.

Definition 1.2.7. Let $\mathbf{K}$ be an algebraic extension of $\mathbf{k}$. We say $\mathbf{K}/\mathbf{k}$ is *totally ramified* if $[\underline{\mathbf{K}} : \underline{\mathbf{k}}] = 1$.

A polynomial $\varphi(x) = x^n + \varphi_{n-1}x^{n-1} + \cdots + \varphi_0$ with coefficients in the valuation ring $\mathcal{O}_\mathbf{k}$ of $\mathbf{k}$ is called an *Eisenstein polynomial* if $v_\mathfrak{p}(\varphi_j) \geqslant 1$ for $1 \leqslant j \leqslant n-1$ and $v_\mathfrak{p}(\varphi_0) = 1$. It is well known that such polynomials are irreducible and define totally ramified extensions. Furthermore, the exponential valuation of the discriminant of the field generated by such a polynomial is exactly the exponential valuation discriminant of the polynomial. Conversely, if $\mathbf{K}/\mathbf{k}$ is a totally ramified extension of degree n, then every prime element of $\mathbf{K}$ is a generating element over $\mathbf{k}$ and is a root of an Eisenstein polynomial (see [Serre, 1963, Chap. I, §6]).

Let $\mathbf{K}$ be an extension of $\mathbf{k}$. We can split this extension uniquely into a tower of extensions $\mathbf{K}/\mathbf{K}_T/\mathbf{k}$ where $\mathbf{K}/\mathbf{K}_T$ is totally ramified and $\mathbf{K}_T/\mathbf{k}$ is unramified. In section 2.4 we show how we can obtain an integral basis of $\mathbf{K}_T/\mathbf{k}$ and $\mathbf{K}/\mathbf{K}_T$ from a defining polynomial of $\mathbf{K}/\mathbf{k}$.

Definition 1.2.8. Let $\mathbf{K}$ be a finite algebraic extension of degree n of a local field $\mathbf{k}$. We denote the maximal unramified subfield of $\mathbf{K}/\mathbf{k}$ by $\mathbf{K}_T$. We call $\mathbf{K}_T$ the *inertia field* of $\mathbf{K}/\mathbf{k}$, $f_{\mathbf{K}/\mathbf{k}} := [\mathbf{K}_T : \mathbf{k}]$ the *inertia degree* of $\mathbf{K}/\mathbf{k}$, and $e_{\mathbf{K}/\mathbf{k}} := [\mathbf{K}/\mathbf{K}_T]$ the *ramification index* of $\mathbf{K}/\mathbf{k}$.

$\mathbf{K} = \mathbf{k}(\Gamma, \Pi)$

totally ramified extension of degree
$e_{\mathbf{K}/\mathbf{k}} = e_{\mathbf{K}/\mathbf{K}_T}$ generated by a root Π
of an Eisenstein polynomial $A_\omega(x)$

extension of degree
$n = e_{\mathbf{K}/\mathbf{k}} f_{\mathbf{K}/k}$

$\mathbf{K}_T = \mathbf{k}(\Gamma)$

unramified extension of degree $f_{\mathbf{K}/\mathbf{k}} = f_{\mathbf{K}_T/\mathbf{k}}$
generated by a root Γ of a monic polynomial $\varphi(x)$ with
$\underline{\varphi}(x) \in \underline{\mathbf{k}}[x]$ irreducible

$\mathbf{k}$

Let p be the characteristic of the residue class field of $\mathbf{k}$. We say $\mathbf{K}/\mathbf{k}$ is *tamely ramified* if $p \nmid e_{\mathbf{K}/\mathbf{k}}$. Extensions $\mathbf{K}/\mathbf{k}$ with $p \mid e_{\mathbf{K}/\mathbf{k}}$ are called *wildly ramified.* Every totally ramified extension $\mathbf{K}/\mathbf{k}$ can be split into a tower $\mathbf{K}/\mathbf{K}_0/\mathbf{k}$ where $\mathbf{K}/\mathbf{K}_0$ is wildly ramified and $\mathbf{K}_0/\mathbf{k}$ is tamely ramified. See section 3.5 for a proof.

If $\varphi(x) \in \mathbf{k}[x]$ is insepararable then $\operatorname{disc}(\varphi) = 0$. If $\varphi(x) \in \mathbf{k}[x]$ is irreducible and $\operatorname{disc}(\varphi) = 0$ then $\varphi(x)$ is inseparable.

If $\mathbf{k}$ is a finite extension of $\mathbb{Q}_p$ we call $\mathbf{k}$ a $\mathfrak{p}$-*adic field.* Setting $e = e_{\mathbf{k}/\mathbb{Q}_p}$ and $f = f_{\mathbf{k}/\mathbb{Q}_p}$, we have the following situation.

$\mathbf{k} = \mathbb{Q}_p(\zeta, \pi)$

totally ramified extension of degree e
generated by a root π
of an Eisenstein polynomial

extension of degree ef
with inertia degree f,
ramification index e

$\mathbf{k}_T = \mathbb{Q}_p(\zeta)$

unramified extension of degree f
generated by a root ζ of a
monic polynomial $\varphi(x)$ with
$\underline{\varphi}(x) \in \mathbb{F}_p[x]$ irreducible

$\mathbb{Q}_p$

1.3 Krasner's Lemma

Proposition 1.3.1 (Krasner's Lemma). *Let $\mathbf{k}$ be a field complete with respect to a non-archimedean absolute value $|\cdot|$ and let $\alpha, \beta \in \overline{\mathbf{k}}$ with α separable over $\mathbf{k}$. If*

$$|\beta - \alpha| < |\alpha' - \alpha|$$

for all conjugates $\alpha' \neq \alpha$ of α then $\alpha \in \mathbf{k}(\beta)$.

Proof. Let $\mathbf{K}/\mathbf{k}(\beta)$ be the normal closure of $\mathbf{k}(\alpha, \beta)/\mathbf{k}(\beta)$. Let $\tau \in \mathrm{Gal}(\mathbf{K}/\mathbf{k}(\beta))$. Then

$$|\beta - \tau(\alpha)| = |\tau(\alpha - \beta)| = |\beta - \alpha| < |\alpha' - \alpha|.$$

Therefore

$$|\alpha - \tau(\alpha)| = |\alpha - \beta + \beta - \tau(\alpha))| \leqslant \max\big\{|\alpha - \beta|, |\beta - \tau(\alpha)|\big\} < |\alpha' - \alpha|$$

for all conjugates α' of α. This implies that τ is the identity; thus $\mathbf{k}(\alpha, \beta) = \mathbf{k}(\beta)$. □

1.4 Complexity Analysis

In analyzing the complexity of algorithms, it is convenient and usually sufficiently informative to specify computing times only up to order of magnitude, *i.e.*, up to a constant factor. The "big-O" notation lets us do this.

Definition 1.4.1. *Let $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{N} \to \mathbb{R}$. We write $f(n) = O(g(n))$ if there is a constant C such that $|f(n)|_\infty \leqslant Cg(n)$ for all $n \in \mathbb{N}$.*

As the algorithms we present are formulated over a general local field $\mathbf{k}$, their complexities are given in terms of arithmetic operations in $\mathbf{k}$. We fix the following notation.

- We write $\mathsf{P}(n, f)$ for the number of steps required to factorize a polynomial of degree n over an extension of the residue class field $\underline{\mathbf{k}}$ of $\mathbf{k}$ of degree f.
- We denote by $\mathsf{M}(n)$ the number of ring operations needed for multiplying two polynomials of degree at most n in $\mathbf{k}[x]$. Schönhage and Strassen [1971] have shown that $\mathsf{M}(n) = O(n \log n \log \log n)$.

- Let β, γ be in the algebraic closure $\overline{\mathbf{k}}$ of $\mathbf{k}$ with $[\underline{\mathbf{k}}(\underline{\beta}) : \underline{\mathbf{k}}] \leqslant n$ and $[\underline{\mathbf{k}}(\underline{\gamma}) : \underline{\mathbf{k}}] \leqslant n$ for some $n \in \mathbb{N}$. We denote by $\mathsf{C}(n)$ the number of arithmetic operations in $\mathbf{k}$ needed to compute an element $\delta \in \overline{\mathbf{k}}$ such that $\underline{\delta}$ is a primitive element of the compositum $\underline{\mathbf{k}}(\underline{\beta}, \underline{\gamma})$.
- We denote by $\mathsf{T}(m, n)$ the number of ring operations required for triangularizing a $m \times n$ matrix over the valuation ring $\mathcal{O}_{\mathbf{k}}$ of $\mathbf{k}$.
- We denote by $\mathsf{R}(m, n)$ the number of ring operations needed for computing the resultant in x of two polynomials in $\mathbf{k}[t][x]$ of degree in x at most n and of degree in t at most m. There exists an algorithm such that $\mathsf{R}(m, n) = O(n\mathsf{M}(nm)\log(nm))$.

The extended euclidian algorithm for two polynomials of degree at most n is of complexity $O(\mathsf{M}(n)\log n)$.

See von zur Gathen and Gerhard [1999] and the references cited therein for the relevant algorithms.

Chapter 2

Polynomial Factorization

We first present a root-finding algorithm, which we will use in an algorithm for the computation of all totally ramified extensions of a p-adic field in section 3.8. We will also use it in the construction of a minimal set of generating polynomials of degree p in section 3.6 and in the construction of a set of independent generating polynomials of degree p^m in section 3.7. This algorithm can also be found in Panayi [1995].

Secondly, we describe the polynomial factoring algorithm mentioned in the introduction.

Throughout this chapter we assume that the polynomial $\Phi(x)$ which is to be factored is squarefree and separable. If $\Phi(x)$ is not squarefree this can be easily remedied by dividing Φ by $\gcd(\Phi, \Phi')$, where $\Phi'(x)$ is the formal derivative of $\Phi(x)$. In some cases it is also possible to use the following much faster criterion to check whether $\Phi(x)$ is squarefree.

Lemma 2.0.2. *Let $\Phi(x) = c_N x^N + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in \mathbf{k}[x]$ with $v_\mathfrak{p}(c_N) < v_\mathfrak{p}(c_i)$ and $v_\mathfrak{p}(c_0) \leqslant v_\mathfrak{p}(c_i)$ for $i \in \{0, \ldots, N-1\}$. Then $\Phi(x)$ is squarefree.*

Proof. Without loss of generality we can assume $v_\mathfrak{p}(c_N) = 0$. Now $v_\mathfrak{p}(\xi) = v_\mathfrak{p}(c_0)/N$ for all roots $\xi \in \overline{\mathbf{k}}$ of $\Phi(x)$. The roots of the formal derivative $\Phi'(x)$ of $\Phi(x)$ have valuation at least $v_\mathfrak{p}(ic_i)/(N-i)$ for some $i \in \{1, \ldots, N-1\}$. But $v_\mathfrak{p}(c_0) \leqslant v_\mathfrak{p}(c_i)$ and $N > N - i$ for all $i \in \{1, \ldots, N-1\}$. Thus $v_\mathfrak{p}(\xi) < v_\mathfrak{p}(\xi')$ for all roots ξ of $\Phi(x)$ and all roots ξ' of $\Phi'(x)$. Therefore $\Phi(x)$ is squarefree. $\square$

Unless restricted otherwise in this chapter $\mathbf{k}$ will be a local field as specified in definition 1.1.7.

2.1 Root-Finding Algorithm

Lemma 2.1.1 (Hensel). *Let $\mathbf{k}$ be a field complete with respect to a non-archimedian absolute value $|\cdot|$, with $\mathcal{O}_{\mathbf{k}}$ its valuation ring and $\mathfrak{p}$ its prime ideal. Let $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ and assume there exists $\alpha \in \mathcal{O}_{\mathbf{k}}$ satisfying $|\Phi(\alpha)| < |\Phi'(\alpha)|^2$. Then Φ has a root in $\mathcal{O}_{\mathbf{k}}$ congruent to α modulo $\mathfrak{p}$.*

A constructive proof of this lemma can be found in [Cassels, 1986]. Panayi's root-finding algorithm relies on the following result.

Lemma 2.1.2. *Let $\Phi(x) = c_n x^n + \cdots + c_0 \in \mathcal{O}_{\mathbf{k}}[x]$. Denote the minimum of the valuations of the coefficients of $\Phi(x)$ by $v_{\mathfrak{p}}(\Phi) := \min\{v_{\mathfrak{p}}(c_0), \ldots, v_{\mathfrak{p}}(c_n)\}$ and define $\Phi^{\#}(x) := \Phi(x)/\pi^{v_{\mathfrak{p}}(\Phi)}$. For $\alpha \in \mathcal{O}_{\mathbf{k}}$, denote its representative in the residue class field $\underline{\mathbf{k}} = \mathcal{O}_{\mathbf{k}}/\mathfrak{p}$ by $\underline{\alpha}$, and for $\beta \in \mathcal{O}_{\mathbf{k}}/\mathfrak{p}$, denote a lift of β to $\mathcal{O}_{\mathbf{k}}$ by $\widehat{\beta}$.*

a) *If α is a zero of $\Phi(x)$ then $\underline{\alpha}$ is a zero of $\underline{\Phi}(x)$.*

b) *α is a zero of $\Phi(x\pi + \widehat{\beta})$ if and only if $\alpha\pi + \widehat{\beta}$ is a zero of $\Phi(x)$.*

c) *α is a zero of $\Phi(x)$ if and only if α is a zero of $\Phi^{\#}(x)$.*

d) *Let β be a zero of $\underline{\Phi}(x)$ and let $\psi(x) := \Phi(x\pi + \widehat{\beta})$. Then $\deg(\underline{\psi^{\#}}) \leqslant \deg(\underline{\Phi^{\#}})$.*

e) *If $\deg(\underline{\Phi^{\#}}) = 0$ then $\Phi(x)$ has no zero in $\mathcal{O}_{\mathbf{k}}$.*

f) *If $\deg(\underline{\Phi^{\#}}) = 1$ then $\Phi(x)$ has a zero in $\mathcal{O}_{\mathbf{k}}$.*

g) *If $\underline{\Phi^{\#}}(x) = (x-\beta)^m h(x)$ where $\gcd((x-\beta), h(x)) = 1$ and if $\psi(x) := \Phi(x\pi + \widehat{\beta})$ then $\deg(\underline{\psi^{\#}}) \leqslant m$*

Proof. The statements a) to c) are obvious.

d) Let $d = \deg(\underline{\Phi^{\#}})$. Then $v_{\mathfrak{p}}(c_d) \leqslant v_{\mathfrak{p}}(c_\nu)$ for all $\nu \leqslant d$ and $v_{\mathfrak{p}}(c_d) < v_{\mathfrak{p}}(c_\nu)$ for all $\nu > d$. Now $\psi = b_n x^n + \cdots + b_0$ with $b_i = \sum_{j=i}^{n} \binom{j}{i} c_j \pi^i \widehat{\beta}^{j-i}$. Because $\binom{i}{i} = 1$ we have $v_{\mathfrak{p}}(b_d) = v_{\mathfrak{p}}(c_d) + d$ and $v_{\mathfrak{p}}(b_\nu) \geqslant v_{\mathfrak{p}}(c_d) + \nu$ for all $\nu > d$. Hence, $\deg(\underline{\psi^{\#}}) \leqslant \deg(\underline{\Phi^{\#}})$.

e) Clear from a), b), and c).

f) We denote the coefficients of $\Phi^{\#}(x)$ by $c_\nu^{\#}$. Let β be a root of $\underline{\Phi^{\#}}(x)$. Since $\deg(\underline{\Phi^{\#}}) = 1$, $v_{\mathfrak{p}}(c_1^{\#}) = 0$ and $v_{\mathfrak{p}}(c_\nu^{\#}) \geqslant 1$ for $\nu > 1$. So $\Phi^{\#'}(\widehat{\beta}) \not\equiv 0 \bmod \mathfrak{p}$ and $\Phi^{\#}(\widehat{\beta}) \equiv 0 \bmod \mathfrak{p}$. Thus $\Phi^{\#}(x)$ has a root by lemma 2.1.1, and by c) $\Phi(x)$ has a root as well.

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

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

As $\underline{\varPhi}(x) = (x - \beta)^m h(x)$, we have $v_{\mathfrak{p}}(\varPhi^{(m)}(\widehat{\beta})/m!) = 0$. Also $v_{\mathfrak{p}}(\varPhi^{(i)}(\widehat{\beta})\pi^i/i!) \geqslant i > v_{\mathfrak{p}}(\varPhi^{(m)}(\widehat{\beta})/m!)\pi^m = m$ for $i > m$. Hence $\deg(\underline{\psi^{\#}}) \leqslant m$.

□

Assume $\varPhi(x)$ has a root β modulo $\mathfrak{p}$ and define two sequences $(\varPhi_\nu(x))_\nu$ and $(\delta_\nu)_\nu$ in the following way:

- $\varPhi_0(x) := \varPhi^{\#}(x)$,
- $\delta_0 := \widehat{\beta}$,
- $\varPhi_{\nu+1}(x) := \varPhi_\nu^{\#}(x\pi + \widehat{\beta}_\nu)$ where β is a root of $\underline{\varPhi^{\#}}(x)$,
- $\delta_{\nu+1} := \widehat{\beta}_\nu \pi^{\nu+1} + \delta_\nu$ where β_ν is a zero of $\underline{\varPhi_\nu^{\#}}(x)$ if there are any.

At each step, one can find such a root if indeed $\varPhi(x)$ has a root (in $\mathcal{O}_{\mathbf{k}}$) congruent to β modulo $\mathfrak{p}$ and δ_ν is congruent to this root modulo increasing powers of $\mathfrak{p}$. At some point, one of the following cases must happen:

- $\deg(\underline{\varPhi_\nu}) \leqslant 1$ and one uses 2.1.2 e) or f) to conclude;
- $\underline{\varPhi_\nu^{\#}}$ has no roots and thus $\delta_{\nu-1}$ is not an approximation of a root of $\varPhi(x)$;
- $\nu \geqslant v_{\mathfrak{p}}(\mathrm{disc}\,(\varPhi))$ and then lemma 2.1.3 below tells us that lemma 2.1.2 e) or f) applies.

While constructing this sequence it may happen that $\underline{\varPhi_\nu}(x)$ has more than one root. In this case we split the sequence and consider one sequence for each root. Lemma 2.1.2 g) tells that there are never more than $\deg(\varPhi)$ candidate roots. Notice that if the conditions of lemma 2.1.2 f) or lemma 2.1.3 are satisfied, the construction used in the proof of lemma 2.1.1 can be used to compute an arbitrarily close approximation of the root faster than with the root-finding algorithm.

Lemma 2.1.3. *If* $\nu \geqslant v_{\mathfrak{p}}(\mathrm{disc}\,(\varPhi))$, *then* $\deg(\underline{\varPhi_\nu}) \leqslant 1$.

Proof. Assume $\deg(\underline{\Phi_\nu}) \geqslant 2$. Since $\Phi_\nu(x) = \Phi_\nu^{\#}(x)$ by construction, it follows by considering the Taylor expansion

$$\Phi_{\nu+1}(x) = \Phi(\pi^{\nu+1}x + \delta_\nu) = \sum_{i=0}^{n} \frac{\Phi^{(i)}(\delta_\nu)}{i!} \pi^{(\nu+1)i} x^i$$

that $\Phi(\delta_\nu)$ and $\Phi'(\delta_\nu)\pi^{\nu+1}$ must have a $v_\mathfrak{p}$-valuation greater than or equal to the valuation of $\pi^{2(\nu+1)}$. So $v_\mathfrak{p}(\Phi(\delta_\nu)) \geqslant 2(\nu+1)$ and $v_\mathfrak{p}(\Phi'(\delta_\nu)) \geqslant \nu+1$. In particular, $\Phi(x)$ has (at least) a double root modulo $\mathfrak{p}^{\nu+1}$. But, the discriminant of $\Phi(x)$ modulo $\mathfrak{p}^{\nu+1}$ is nonzero by hypothesis, thus this is impossible. So $\deg(\underline{f_\nu}) < 2$. ☐

The following algorithm returns the number of zeroes of a polynomial f over a local field $\mathbf{k}$. We use the notation from lemma 2.1.2.

Algorithm 2.1.4 (Root Finding).

Input: A local field $\mathbf{k}$ with prime element π, a polynomial $\Phi(x) \in \mathbf{k}[x]$, and a desired precision N

Output: A set G of approximations of the roots of $\Phi(x)$ over $\mathbf{k}$

- Set $C \leftarrow \{(\Phi^{\#}(x), 0, 0)\}$.
- Set $G \leftarrow \{\ \}$.
- While C is not empty:
  - For all $(\psi(x), \delta, s)$ in C:
    - $C \leftarrow C \setminus \{(\psi(x), \delta, s)\}$.
    - $R \leftarrow \{\beta \mid \beta \text{ is a root of } \underline{\psi}(x) \text{ in } \underline{\mathbf{k}}\ \}$.
    - For all β in R:
      - Set $\psi(x) \leftarrow \psi(\pi x + \widehat{\beta})$.
      - Replace $\psi(x) \leftarrow \psi^{\#}(x)$.
      - If $\deg \underline{\psi} = 1$ then
        - derive an approximation δ of a root of $\Phi(x)$ using lemma 2.1.1.
        - $G \leftarrow G \cup \{\delta\}$.
      - If $\deg \underline{\psi} > 1$ then
        - $C \leftarrow C \cup \{(\psi(x), \delta + \pi^s\beta, s+1)\}$.
- Return G.

Corollary 2.1.5. *Let $\mathbf{k}$ be a local field and let $\Phi(x) \in \mathbf{k}[x]$ be a polynomial of degree N. Algorithm 2.1.4 returns approximations to all roots of a polynomial $\Phi(x) \in \mathbf{k}[x]$*

in at most

$$O\big(N v_{\mathfrak{p}}(\operatorname{disc}(\Phi)) \cdot (\mathsf{P}(N) + N\mathsf{M}(N))\big)$$

operations in $\mathbf{k}$.

Proof. At any time there are no more than $N = \deg \Phi$ candidate roots. By lemma 2.1.3 the algorithm terminates after at most $v_{\mathfrak{p}}(\operatorname{disc}\Phi)$ iterations. In each iteration of the inner loop a polynomial of degree at most N is factored over the residue class field of $\mathbf{k}$ and $\Psi(\pi x + \widehat{\beta})$ is evaluated. This can be done in $\mathsf{P}(N)$, respectively $N\mathsf{M}(N)$, operations in $\mathbf{k}$. □

2.2 Polynomial Factorization

Let $\Phi(x)$ be a monic, separable, squarefree polynomial of degree N in $\mathcal{O}_{\mathbf{k}}[x]$. In order to find a proper factorization of $\Phi(x)$ or to prove its irreducibility, we construct a polynomial $\varphi(x) \in \mathbf{k}[x]$ with $\deg \varphi$ less than or equal to the degree of every irreducible factor of $\Phi(x)$. The polynomial $\varphi(x)$ is iteratively modified such a way that $|\varphi(\xi)|$ decreases strictly for all roots $\xi \in \overline{\mathbf{k}}$ of $\Phi(x)$.

In section 2.3 we describe how a proper factorization of $\Phi(x)$ can be derived if $|\varphi(\xi_i)| \neq |\varphi(\xi_j)|$ for some roots ξ_i and ξ_j of $\Phi(x)$. In section 2.4 we describe how an integral basis of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$ over $\mathbf{k}$ can be obtained from the data computed in the algorithm. In section 2.5 we show that $\Phi(x)$ is irreducible if $|\varphi(\xi)|^N < |\operatorname{disc}\Phi|^2$ for some root ξ of $\Phi(x)$. In section 2.6 we present an algorithm that returns a proper factorization of $\Phi(x)$ over $\mathcal{O}_{\mathbf{k}}$ if one exists or an integral basis of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$ over $\mathbf{k}$ otherwise. In section 2.8 we analyse the complexity of the algorithm.

2.3 Reducibility

Hensel lifting gives a very efficient method for approximating factors of a polynomial over a local field if the polynomial has at least two relatively prime factors over the residue class field.

Proposition 2.3.1 (Quadratic Hensel Lifting). *Let* R *be a commutative ring with* 1*, let* $\mathfrak{b}$ *be an ideal of* R*, and let* $\Psi(x)$*,* $\Psi_{1,0}(x)$*,* $\Psi_{2,0}(x)$ *be monic, non-constant* *polynomials in* $R[x]$ *such that*

$$\Psi(x) \equiv \Psi_{1,0}(x)\Psi_{2,0}(x) \bmod \mathfrak{b}.$$

Assume there exist $\gamma_{1,0}(x)$, $\gamma_{2,0}(x) \in R[x]$ *and* $\gamma_{0,0}(x) \in \mathfrak{b}[x]$ *with*

$$\gamma_{1,0}(x)\Psi_{1,0}(x) + \gamma_{2,0}(x)\Psi_{2,0}(x) = 1 + \gamma_{0,0}(x).$$

Then for every $m \in \mathbb{N}$ *there exist* $\Psi_{1,m}(x)$, $\Psi_{2,m}(x)$ *satisfying*

$$\Psi(x) \equiv \Psi_{1,m}(x)\Psi_{2,m}(x) \bmod \mathfrak{b}^{2^m}$$

and

$$\Psi_{1,m}(x) \equiv \Psi_{1,0}(x) \bmod \mathfrak{b},$$
$$\Psi_{2,m}(x) \equiv \Psi_{2,0}(x) \bmod \mathfrak{b}.$$

Also there exist $\gamma_{1,m}(x)$, $\gamma_{2,m}(x) \in R[x]$ *and* $\gamma_{0,m}(x) \in \mathfrak{b}[x]$ *with*

$$\gamma_{1,m}(x)\Psi_{1,m}(x) + \gamma_{2,m}(x)\Psi_{2,m}(x) = 1 + \gamma_{0,m}(x).$$

For a proof see Pohst and Zassenhaus [1989].

We present two criteria which, if they are fulfilled, allow us to apply Hensel lifting to the problem of factoring $\Phi(x)$.

Definition 2.3.2. Let $\Phi(x) = \prod_{j=1}^{N}(x - \xi_j) \in \mathcal{O}_{\mathbf{k}}[x]$. For $\vartheta(x) \in \mathbf{k}[x]$ we define

$$\chi_\vartheta(y) := \prod_{i=1}^{N}(y - \vartheta(\xi_i)) = \operatorname{res}_x(\Phi(x), y - \vartheta(x)).$$

Definition 2.3.3. Let $\vartheta(x) \in \mathbf{k}[x]$ with $\chi_\vartheta(y) = y^N + c_1 y^{N-1} + \cdots + c_N \in \mathcal{O}_{\mathbf{k}}[y]$.

We say $\vartheta(x)$ *passes the Hensel test* if $\underline{\chi}_\vartheta(y) = \underline{\nu}_\vartheta(y)^s$ for some $s \geqslant 1$, where $\underline{\nu}_\vartheta(y)$ is monic and irreducible in $\underline{\mathbf{k}}[y]$.

We define further $v_{\mathfrak{p}}^*(\vartheta) := \min\limits_{1 \leqslant i \leqslant N} \dfrac{v_{\mathfrak{p}}(c_i)}{i}$.

We say the polynomial $\vartheta(x)$ *passes the Newton test* if $\dfrac{v_{\mathfrak{p}}(c_N)}{N} = v_{\mathfrak{p}}^*(\vartheta)$.

Note that $v_{\mathfrak{p}}(\vartheta(\xi_1)) = \cdots = v_{\mathfrak{p}}(\vartheta(\xi_N)) = v_{\mathfrak{p}}(c_N)/N$ if $\vartheta(x)$ passes the Newton test.

Proposition 2.3.4. *Let* $\gamma(x) \in \mathbf{k}[x]$ *with* $\chi_\gamma(y) \in \mathcal{O}_{\mathbf{k}}[y]$. *If* $\gamma(x)$ *fails the Hensel test then* $\Phi(x)$ *is reducible in* $\mathcal{O}_{\mathbf{k}}[x]$.

Proof. As $\gamma(x)$ fails the Hensel test, $\underline{\chi}_\gamma(y)$ has at least two irreducible factors. Hensel's lemma gives relatively prime monic polynomials $\chi_1(y)$ and $\chi_2(y)$ in $\mathcal{O}_{\mathbf{k}}[y]$ with $\chi_1(y)\chi_2(y) = \chi_\gamma(y)$. Reordering the roots of $\Phi(x)$ if necessary, we may write

$$\chi_1(y) = (y - \gamma(\xi_1)) \cdots (y - \gamma(\xi_r)) \text{ and } \chi_2(y) = (y - \gamma(\xi_{r+1})) \cdots (y - \gamma(\xi_N)),$$

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

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

is a proper factorization of $\Phi(x)$. □

Corollary 2.3.5. *Let $\vartheta(x) \in \mathbf{k}[x]$ with $\chi_\vartheta(y) = y^N + c_1 y^{N-1} + \cdots + c_N \in \mathcal{O}_{\mathbf{k}}[y]$. If $\vartheta(x)$ fails the Newton test then $\Phi(x)$ is reducible in $\mathcal{O}_{\mathbf{k}}[x]$.*

Proof. If $\vartheta(x)$ fails the Newton test we have $v_{\mathfrak{p}}^*(\vartheta) = r/s < v_{\mathfrak{p}}(c_N)/N$. Setting $\gamma(x) := \vartheta(x)^s/\pi^r$ we get

$$\min\{v_{\mathfrak{p}}(\gamma(\xi_1)), \ldots, v_{\mathfrak{p}}(\gamma(\xi_N))\} = 0 < \max\{v_{\mathfrak{p}}(\gamma(\xi_1)), \ldots, v_{\mathfrak{p}}(\gamma(\xi_N))\}.$$

Consequently $\gamma(x)$ fails the Hensel test and it follows from proposition 2.3.4 that $\Phi(x)$ is reducible. □

In general it is not possible to compute exactly the greatest common divisor of two polynomials over a local field. The following result from Ford and Letard [1994] (also see Ford et al. [2000]) provides a method for approximating the greatest common divisor to any desired precision.

The *Sylvester matrix* $S_{\Phi,\Psi}$ of the polynomials $\Phi(x) = c_0 x^N + \cdots + c_N$ and $\Psi(x) = b_0 x^M + \cdots + b_M$ is the $(M+N) \times (M+N)$ matrix

$$\begin{pmatrix} b_0 & \cdots & b_M & & 0 \\ & \ddots & & \ddots & \\ 0 & & b_0 & \cdots & b_M \\ c_0 & \cdots & c_N & & 0 \\ & \ddots & & \ddots & \\ 0 & & c_0 & \cdots & c_N \end{pmatrix}.$$

Proposition 2.3.6 (Ford). *Let $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ be monic. Let relatively prime polynomials $\Psi_1(x)$ and $\Psi_2(x)$ in $\mathcal{O}_{\mathbf{k}}[x]$ and $r_0 \in \mathbb{N}$ be given, such that*

$$\Phi(x) \mid \Psi_1(x)\Psi_2(x) \quad \textit{and} \quad \mathfrak{p}^{r_0} = \big(\Psi_1(x)\mathcal{O}_{\mathbf{k}}[x] + \Psi_2(x)\mathcal{O}_{\mathbf{k}}[x]\big) \cap \mathcal{O}_{\mathbf{k}}.$$

Choose $m \in \mathbb{N}$, $m > r_0$. For $j = 1, 2$ let S_{Φ,Ψ_j} be the Sylvester matrix of $\Phi(x)$ and $\Psi_j(x)$. Let $\pi^{r_j}\Phi_j(x)$ with $\Phi_j(x)$ monic, $r_j \in \mathbb{N}$, be the polynomial given by the last non-zero row of the matrix obtained by row reduction of S_{Φ,Ψ_j} modulo $\mathfrak{p}^m$. Then

$$\Phi_j(x) \equiv \gcd\big(\Phi(x), \Psi_j(x)\big) \bmod \mathfrak{p}^{m-r_0}.$$

Proof. Define

$$G_1(x) := \gcd\big(\Phi(x), \Psi_1(x)\big),\ H_1(x) := \Psi_1(x)/G_1(x),$$
$$G_2(x) := \gcd\big(\Phi(x), \Psi_2(x)\big),\ H_2(x) := \Psi_2(x)/G_2(x),$$

so that

$$\Phi(x) = G_1(x)G_2(x),$$

and let

$$p^{s_1}\mathcal{O}_{\mathbf{k}} = \big(G_2(x)\mathcal{O}_{\mathbf{k}}[x] + H_1(x)\mathcal{O}_{\mathbf{k}}[x]\big) \cap \mathcal{O}_{\mathbf{k}},$$
$$p^{s_2}\mathcal{O}_{\mathbf{k}} = \big(G_1(x)\mathcal{O}_{\mathbf{k}}[x] + H_2(x)\mathcal{O}_{\mathbf{k}}[x]\big) \cap \mathcal{O}_{\mathbf{k}}.$$

Because $\Psi_1(x) = G_1(x)H_1(x)$ and $\Psi_2(x) = G_2(x)H_2(x)$ we have $s_1 \leqslant r_0$ and $s_2 \leqslant r_0$.

For $j = 1, 2$ let S_{Φ,Ψ_j} be the Sylvester matrix of Φ and Ψ_j. It is clear that row-reduction of S_{Φ,Ψ_j} over $\mathbf{k}$ gives the coefficients of $G_j(x)$ in its last non-zero row. It follows (because the rank is invariant) that row-reduction of S_{Φ,Ψ_j} over $\mathcal{O}_{\mathbf{k}}$ gives the coefficients of $p^{r_j}G_j(x)$ in its last non-zero row, for some $r_j \geqslant 0$. Since

$$p^{s_j}G_j(x) \in \Phi(x)\mathcal{O}_{\mathbf{k}}[x] + \Psi_j(x)\mathcal{O}_{\mathbf{k}}[x]$$

it follows that $r_j \leqslant s_j$, and since

$$p^{r_j} \in \frac{\Phi(x)}{G_j(x)}\mathcal{O}_{\mathbf{k}}[x] + \frac{\Psi_j(x)}{G_j(x)}\mathcal{O}_{\mathbf{k}}[x]$$

it follows that $s_j \leqslant r_j$; hence $r_j = s_j$.

If $m > r_0$ then row-reduction of S_{Φ,Ψ_j} over $\mathcal{O}_{\mathbf{k}}$ performed modulo p^m gives in its last non-zero row the coefficients of $p^{s_j}\Phi_j(x)$, with $\Phi_j(x)$ in $\mathcal{O}_{\mathbf{k}}[x]$, $\Phi_j(x)$ monic, and

$$\Phi_j(x) \equiv G_j(x) \pmod{p^{m-s_j}\mathcal{O}_{\mathbf{k}}[x]}.$$

It follows that

$$\Phi_1(x) \equiv \gcd \Phi(x), \Psi_1(x) \bmod \pi^{m-r_0}\mathcal{O}_{\mathbf{k}}[x],$$
$$\Phi_2(x) \equiv \gcd \Phi(x), \Psi_2(x) \bmod \pi^{m-r_0}\mathcal{O}_{\mathbf{k}}[x].$$

$\square$

Remark 2.3.7. In the construction of $\Phi_1(x)$ and $\Phi_2(x)$ it is sufficient to have approximations to $\Phi(x)$, $\Psi_1(x)$, and $\Psi_2(x)$ that are correct modulo $\mathfrak{p}^m$.

Remark 2.3.8. Let $\gamma(x)$ be a polynomial in $\mathbf{k}[x]$ such that $\chi_1(y)\chi_2(y) = \chi_\gamma(y) \in \mathcal{O}_\mathbf{k}[y]$ where $\gcd(\underline{\chi}_1(y), \underline{\chi}_2(y)) = 1$. There exist $\alpha_1(y), \alpha_2(y) \in \mathcal{O}_\mathbf{k}[y]$ with

$$\underline{\alpha}_1(y)\underline{\chi}_1(y) + \underline{\alpha}_2(y)\underline{\chi}_2(y) = 1.$$

Because the index of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$ in its maximal order is at most $\mathfrak{p}^d$, where $d = \lfloor v_\mathfrak{p}(\operatorname{disc}\Phi)/2\rfloor$, and

$$\pi^d\alpha_1(\gamma(x))\pi^d\chi_1(\gamma(x)) + \pi^d\alpha_2(\gamma(x))\pi^d\chi_2(\gamma(x)) \equiv \pi^{2d} \bmod \mathfrak{p}^{2d+1},$$

it follows that $r_0 \leqslant 2d \leqslant v_\mathfrak{p}(\operatorname{disc}\Phi)$.

Both criteria for finding a proper factorization of $\Phi(x)$ need a factorization of the polynomial over the residue class field before Hensel lifting can be applied. If the residue class field $\underline{\mathbf{k}}$ is finite we can use the algorithms of Berlekamp [1970], Cantor and Zassenhaus [1981], or one of their many improvements.

If $\mathbf{k}$ is the completion of a function field over a number field then polynomials over $\underline{\mathbf{k}}$ can be factored using the algorithms for factoring polynomials over number fields by Trager [1976], Pohst [1999], Roblot [2000], or Fieker and Friedrichs [2000].

We will see that it is convenient to factor the polynomial $\Phi(x)$ over an unramified extension $\widehat{\mathbf{k}}$ of $\mathbf{k}$. Then the norms of the factors of $\Phi(x)$ over $\widehat{\mathbf{k}}$ can be used to derive a factorization of $\Phi(x)$ over $\mathbf{k}$. For more on the norm of a polynomial see Pohst and Zassenhaus [1989, section 5.4].

Definition 2.3.9. Let $\widehat{\mathbf{k}}$ be an algebraic extension of $\mathbf{k}$ of degree n. Let $\vartheta(x) \in \widehat{\mathbf{k}}[x]$ and $\vartheta^{(j)}(x) \in \widehat{\mathbf{k}}^{(j)}[x]$ $(1 \leqslant j \leqslant n)$ be the corresponding polynomials over the conjugate fields obtained by applying conjugation to the coefficients of $\vartheta(x)$ only. Then the norm of $\vartheta(x)$ is defined by $\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta) := \prod_{j=1}^n \vartheta^{(j)}(x)$.

Remark 2.3.10. Note that $\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta(x)) \in \mathbf{k}[x]$ and that

$$\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta_1(x)\vartheta_2(x)) = \mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta_1(x))\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta_2(x))$$

for all $\vartheta_1(x)$, $\vartheta_2(x) \in \widehat{\mathbf{k}}[x]$.

Remark 2.3.11. Let $\nu(y) \in \mathcal{O}_{\mathbf{k}}[y]$ be irreducible and let $\widehat{\mathbf{k}} := \mathcal{O}_{\mathbf{k}}[y]/\nu(y)\mathcal{O}_{\mathbf{k}}[y]$. Let $\varphi(x) = \sum_{i=0}^{n} c_i(y)x^n$ be a polynomial in $\widehat{\mathbf{k}}[x]$. Denote by C_i a lift of c_i from $\mathcal{O}_{\mathbf{k}}[y]/\nu(y)\mathcal{O}_{\mathbf{k}}[y]$ to $\mathcal{O}_{\mathbf{k}}[y]$. Then $\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\varphi(x)) = \mathrm{res}_y\big(\nu(y), \sum_{i=0}^{n} C_i(y)x^n\big)$.

2.4 Two-Element Certificates and Integral Bases

For a polynomial $\vartheta(x) \in \mathbf{k}[x]$ the values E_ϑ and F_ϑ defined below give lower bounds for the ramification indices and the inertia degrees respectively of the extensions $\mathbf{k}(\xi)$ for all roots ξ of $\Phi(x)$.

Definition 2.4.1. Let $\vartheta(x) \in \mathbf{k}[x]$, with $\chi_\vartheta(y) \in \mathcal{O}_{\mathbf{k}}[y]$, such that $\vartheta(x)$ passes the Hensel and Newton tests. We define $\nu_\vartheta(y)$ to be an arbitrary monic polynomial in $\mathcal{O}_{\mathbf{k}}[y]$, with $\underline{\nu}_\vartheta(y)$ irreducible in $\underline{\mathbf{k}}[y]$, such that $\underline{\chi}_\vartheta(y) = \underline{\nu}_\vartheta(y)^s$ for some $s \geqslant 1$. We set $F_\vartheta := \deg \underline{\nu}_\vartheta$. We define E_ϑ to be the (positive) denominator of the rational number $v_{\mathfrak{p}}^*(\vartheta)$ in lowest terms.

Definition 2.4.2. Let $\Phi(x)$ be a monic polynomial in $\mathcal{O}_{\mathbf{k}}[x]$. Let ξ be a root of $\Phi(x)$ Let $\Gamma(x) \in \mathbf{k}[x]$ with $\chi_\Gamma(y) \in \mathcal{O}_{\mathbf{k}}[y]$ and $\Pi(x) \in \mathbf{k}(\Gamma(\xi))[x]$ with $\chi_\Pi(y) \in \mathcal{O}_{\mathbf{k}(\Gamma(\xi))}[y]$ such that $\Gamma(x)$ passes the Hensel test and $\Pi(x)$ passes the Newton test. We call the pair $(\Gamma(x), \Pi(x))$ a *two-element certificate for* $\Phi(x)$ if $v_{\mathfrak{p}}^*(\Pi) = 1/E_\Pi$ and $F_\Gamma E_\Pi = \deg \Phi$.

Proposition 2.4.3. *Let $\Phi(x)$ be a monic polynomial in $\mathcal{O}_{\mathbf{k}}[x]$. If a two-element certificate $(\Gamma(x), \Pi(x))$ exists for $\Phi(x)$ then $\Phi(x)$ is irreducible over* $\mathbf{k}$. *Moreover an integral basis of the extension $\mathbf{K}/\mathbf{k}$ generated by a root ξ of $\Phi(x)$ is given by the elements $\Gamma(\xi)^i\Pi(\xi)^j$ with $0 \leqslant i \leqslant F_\Gamma - 1$ and $0 \leqslant j \leqslant E_\Pi - 1$.*

Proof. The polynomial $\Phi(x)$ is irreducible because every root of Φ generates an extension of degree $F_\Gamma E_\Pi = \deg \Phi$ over $\mathbf{k}$. Denote the inertia field of $\mathbf{K}/\mathbf{k}$ by $\mathbf{K}_T$. Let γ be a root of $\nu_\Gamma(x)$ such that $\gamma \equiv \Gamma(\xi)$. Then $\mathbf{K}_T = \mathbf{K}(\gamma)$ and $\mathcal{O}_{\mathbf{K}_T/\mathbf{k}} = \mathcal{O}_{\mathbf{k}}[\gamma]$. As $v_{\mathfrak{p}}^*(\Pi) = 1/E_\Pi$ we have $\mathcal{O}_{\mathbf{K}/\mathbf{k}} = \mathcal{O}_{\mathbf{K}_T/\mathbf{k}}[\Pi(\xi)] = \mathcal{O}_{\mathbf{k}}[\gamma, \Pi(\xi)]$. The elements $\gamma^i\Pi(\xi)^j$ with $0 \leqslant i \leqslant F_\Gamma - 1$ and $0 \leqslant j \leqslant E_\Pi - 1$ form an integral basis of $\mathbf{K}/\mathbf{k}$. Because $\Gamma(\xi) \equiv \gamma \bmod \Pi(\xi)$ the elements $\Gamma(\xi)^i\Pi(\xi)^j$ with $0 \leqslant i \leqslant F_\Gamma - 1$ and $0 \leqslant j \leqslant E_\Pi - 1$ are an integral basis of $\mathbf{K}/\mathbf{k}$ as well. $\square$

Let $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ be irreducible and let E be the ramification index and F the inertia degree of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$. Set $\widehat{\mathbf{k}}_0 := \mathbf{k}$. Assume we are given a tower of unramified extensions

$$\begin{aligned}
\widehat{\mathbf{k}}_r &:= \widehat{\mathbf{k}}_{r-1}[y_r]/\nu_{\gamma_{r-1}}\widehat{\mathbf{k}}_{r-1}[y_r] \\
&\vdots \\
\widehat{\mathbf{k}}_2 &:= \widehat{\mathbf{k}}_1[y_2]/\nu_{\gamma_1}(y_2)\widehat{\mathbf{k}}_1[y_2] \\
\widehat{\mathbf{k}}_1 &:= \widehat{\mathbf{k}}_0[y_1]/\nu_{\gamma_0}(y_1)\widehat{\mathbf{k}}_0[y_1] \\
\widehat{\mathbf{k}}_0 &:= \mathbf{k}
\end{aligned}$$

with $\gamma_i(x) \in \widehat{\mathbf{k}}_i[x]$, such that $\widehat{\mathbf{k}}_r$ is isomorphic to the inertia field of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$. Denote by $\widetilde{\gamma}_i(x)$ a lift of $\gamma_i(x)$ to $\mathbf{k}[y_1,\ldots,y_i][x]$ and by ξ a root of $\Phi(x)$. Define a sequence $\delta_i(x) \in \mathbf{k}[x]$ by $\delta_0(x) := \widetilde{\gamma}_0(x)$ and $\delta_i(x) := \widetilde{\gamma}\big(\delta_0(x),\ldots,\delta_{i-1}(x)\big)(x)$ for $1 \leqslant i \leqslant r$. Then the inertia field of $\mathbf{k}(\delta_0(\xi),\ldots,\delta_i(\xi))$ is isomorphic to $\widehat{\mathbf{k}}_i$.

Let $\Gamma(x) \in \mathbf{k}[x]$ be such that $\underline{\Gamma(\xi)}$ is a primitive element of $\underline{\widehat{\mathbf{k}}_r}$ over $\underline{\mathbf{k}}$. Then $F_\Gamma = F$. Assume that a polynomial $\psi(x) \in \widehat{\mathbf{k}}_r[x]$ with $\chi_\psi(y) \in \mathcal{O}_{\widehat{\mathbf{k}}_r}[y]$ and $v_{\mathfrak{p}}^*(\psi) = 1/E$ is known. Denote by $\widetilde{\psi}(x)$ a lift of $\psi(x)$ to $\mathbf{k}[y_1,\ldots,y_i][x]$ and set

$$\Pi(x) = \widetilde{\psi}\big(\delta_0(x),\ldots,\delta_r(x)\big)(x).$$

Then $(\Gamma(x),\Pi(x))$ is a two-element certificate for $\Phi(x)$.

If the residue class field $\underline{\mathbf{k}}$ of $\mathbf{k}$ is finite the following lemma can be used to find a primitive element of $\underline{\widehat{\mathbf{k}}_r}$.

Lemma 2.4.4. *Let $\mathbb{F}_q$ be the field with q elements. Let $\underline{\beta}$ and $\underline{\gamma}$ be elements of an algebraic closure of $\mathbb{F}_q$. Let $F_\beta := [\mathbb{F}_q(\underline{\beta}) : \mathbb{F}_q]$, $F_\gamma := [\mathbb{F}_q(\underline{\gamma}) : \mathbb{F}_q]$ and $F := \operatorname{lcm}(F_\beta, F_\gamma)$. Let $\underline{\delta} \in \mathbb{F}_q(\underline{\beta},\underline{\gamma})$ be randomly chosen. Then the probability that $\mathbb{F}_q(\underline{\delta}) = \mathbb{F}_q(\underline{\beta},\underline{\gamma})$ is at least* $1/2$.

Proof. The number of elements of $\mathbb{F}_{q^F}$ generating a proper subfield of $\mathbb{F}_{q^F}$ is at most

$$\sum_{\substack{l \text{ prime} \\ l<F,\, l|F}} q^{F/l} \leqslant (\log_2 F) q^{F/2}.$$

Therefore the probability that a randomly chosen element of $\mathbb{F}_{q^F}$ belongs to a proper subfield of $\mathbb{F}_{q^F}$ is at most

$$\frac{(\log_2 F) q^{F/2}}{q^F} = \frac{\log_2 F}{q^{F/2}} \leqslant \frac{\log_2 F}{2^{F/2}} \leqslant \frac{1}{2}. \qquad \square$$

For the case that $\mathbf{k}$ is the completion of a function field over a number field, the residue class field $\underline{\mathbf{k}}$ is a number field. Cohen [1999, section 2.1] presents an algorithm for computing a primitive element of the compositum of two number fields.

2.5 Irreducibility

The following proposition gives an upper bound for the number of steps needed in our algorithm either to derive a proper factorization of $\Phi(x)$ or to produce a two-element certificate of the irreducibility of $\Phi(x)$.

Proposition 2.5.1. *Let $\xi_1, \ldots, \xi_N$, $\alpha_1, \ldots, \alpha_n$ be elements of an algebraic closure of $\mathbf{k}$ and assume the following hypotheses hold.*

- $\Phi(x) := \prod_{j=1}^{N}(x - \xi_j)$ *is a squarefree polynomial in* $\mathcal{O}_{\mathbf{k}}[x]$.
- $\varphi(x) := \prod_{i=1}^{n}(x - \alpha_i)$ *is a polynomial in* $\mathbf{k}[x]$.
- $|\varphi(\xi_j)|^N < |\operatorname{disc} \Phi|^2$ *for* $1 \leqslant j \leqslant N$.
- *The degree of any irreducible factor of $\Phi(x)$ is greater than or equal to n.*

Then $N = n$ and $\Phi(x)$ is irreducible over $\mathbf{k}$.

To prove of this proposition we need a few lemmas.

Lemma 2.5.2. *Let $\Phi(x) = \prod_{j=1}^{N}(x - \xi_j) \in \mathbf{k}[x]$. Let α be an element of the algebraic closure of $\mathbf{k}$ and assume $\widetilde{\xi}$ is chosen among the roots of $\Phi(x)$ such that $|\alpha - \widetilde{\xi}|$ is minimal. Then*

$$|\Phi(\alpha)| = \prod_{i=1}^{N} \max\{|\alpha - \widetilde{\xi}|, |\widetilde{\xi} - \xi_i|\}.$$

Proof. We have $|\Phi(\alpha)| = \prod_{i=1}^{N} |\alpha - \xi_i|$ and $|\alpha - \xi_i| = |\alpha - \widetilde{\xi} + \widetilde{\xi} - \xi_i| \leqslant \max\{|\alpha - \widetilde{\xi}|, |\widetilde{\xi} - \xi_i|\}$. If $|\alpha - \widetilde{\xi}| < |\widetilde{\xi} - \xi_i|$ then $|\alpha - \xi_i| = |\widetilde{\xi} - \xi_i|$, and if $|\alpha - \widetilde{\xi}| \geqslant |\widetilde{\xi} - \xi_i|$ then $|\alpha - \xi_i| = |\widetilde{\xi} - \alpha|$. $\square$

Lemma 2.5.3. *Assume the hypotheses of proposition 2.5.1 hold. Then $\varphi(x)$ belongs to $\mathcal{O}_{\mathbf{k}}[x]$ and $\varphi(x)$ is irreducible over $\mathbf{k}$. Furthermore there exist a root ξ of $\Phi(x)$ and* *a root α of $\varphi(x)$ such that $\mathbf{k}(\xi) = \mathbf{k}(\alpha)$, so that the minimal polynomial of ξ over $\mathbf{k}$ is an irreducible factor of $\Phi(x)$ of degree n.*

Proof. Let $\Phi_i(x) = \prod_{j=1}^{N_i}(x - \xi_{i,j})$, $1 \leqslant i \leqslant m$, denote the m irreducible factors of $\Phi(x)$. Let $\mathcal{G}_i$ be the Galois group of the extension $\mathbf{k}[\xi_{i,1}, \ldots, \xi_{i,N_i}]/\mathbf{k}$. Let $\Delta\Phi_i$ be the minimal distance between two distinct zeroes of $\Phi_i(x)$. Let $\widetilde{\xi}_{i,j}$ denote a root of $\Phi_i(x)$ such that $|\alpha_j - \widetilde{\xi}_{i,j}|$ is minimal. Assume that $|\alpha_j - \widetilde{\xi}_{i,j}| \geqslant \Delta\Phi_i$. Then for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$, using lemma 2.5.2, we get

$$\begin{aligned}
|\Phi_i(\alpha_j)| &= \prod_{k=1}^{N_i} |\alpha_j - \xi_{i,k}| = \prod_{k=1}^{N_i} \max\{|\alpha_j - \widetilde{\xi}_{i,j}|, \, |\widetilde{\xi}_{i,j} - \xi_{i,k}|\} \\
&\geqslant \prod_{k=1}^{N_i} \max\{\Delta\Phi_i, \, |\widetilde{\xi}_{i,j} - \xi_{i,k}|\} \\
&= \Delta\Phi_i \prod_{\xi_{i,k} \neq \widetilde{\xi}_{i,j}} \max\{\Delta\Phi_i, \, |\widetilde{\xi}_{i,j} - \xi_{i,k}|\} = \Delta\Phi_i \prod_{\xi_{i,k} \neq \widetilde{\xi}_{i,j}} |\widetilde{\xi}_{i,j} - \xi_{i,k}|.
\end{aligned}$$

Without loss of generality, we may assume that $\Delta\Phi_i = |\xi_{i,1} - \xi_{i,2}|$. Choose $\sigma_{i,1}, \ldots, \sigma_{i,n} \in \mathcal{G}_i$ so that $\widetilde{\xi}_{i,1}^{\sigma_{i,1}}, \ldots, \widetilde{\xi}_{i,1}^{\sigma_{i,n}}$ are distinct and choose $\tau_{i,1}, \ldots, \tau_{i,n} \in \mathcal{G}_i$ so that $\widetilde{\xi}_{i,1}^{\tau_{i,1}}, \ldots, \widetilde{\xi}_{i,n}^{\tau_{i,n}}$ are distinct. Then $\Delta\Phi_i = |\xi_{i,1}^{\sigma_{i,j}} - \xi_{i,2}^{\sigma_{i,j}}|$ for $1 \leqslant j \leqslant n$ and $|\widetilde{\xi}_{i,j} - \xi_{i,k}| = |\widetilde{\xi}_{i,j}^{\tau_{i,j}} - \xi_{i,k}^{\tau_{i,j}}|$ for $1 \leqslant j \leqslant n$ and $1 \leqslant k \leqslant N_i$. Hence

$$\begin{aligned}
\prod_{j=1}^{n} |\Phi_i(\alpha_j)| &\geqslant \prod_{j=1}^{n} \Bigg(\Delta\Phi_i \prod_{\xi_{i,k} \neq \widetilde{\xi}_{i,j}} |\widetilde{\xi}_{i,j} - \xi_{i,k}| \Bigg) \\
&= \Bigg(\prod_{j=1}^{n} |\xi_{i,1}^{\sigma_{i,j}} - \xi_{i,2}^{\sigma_{i,j}}| \Bigg) \Bigg(\prod_{j=1}^{n} \prod_{\xi_{i,k} \neq \widetilde{\xi}_{i,j}} |\widetilde{\xi}_{i,j}^{\tau_{i,j}} - \xi_{i,k}^{\tau_{i,j}}| \Bigg) \geqslant |\operatorname{disc} \Phi_i|^2.
\end{aligned}$$

Now

$$\begin{aligned}
\max_{1 \leqslant k \leqslant N} |\varphi(\xi_k)|^N &\geqslant \prod_{k=1}^{N} |\varphi(\xi_k)| = \prod_{j=1}^{n} |\Phi(\alpha_j)| = \prod_{i=1}^{m} \prod_{j=1}^{n} |\Phi_i(\alpha_j)| \\
&\geqslant \prod_{i=1}^{m} |\operatorname{disc} \Phi_i|^2 \geqslant |\operatorname{disc} \Phi|^2.
\end{aligned}$$

Thus if $\max_{k=1}^{N} |\varphi(\xi_k)|^N < |\operatorname{disc} \Phi|^2$ then there exist i, j with $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$ such that $|\alpha_j - \widetilde{\xi}_{i,j}| < \Delta\Phi_i$. It follows from Krasner's lemma (proposition 1.3.1) that $\mathbf{k}(\widetilde{\xi}_{i,j}) \subseteq \mathbf{k}(\alpha_j)$. As $\deg \varphi = n \leqslant \deg \Phi_i = N_i$ we get $\mathbf{k}(\widetilde{\xi}_{i,j}) = \mathbf{k}(\alpha_j)$. Therefore $N_i = n$, and $\Phi_i(x)$, which is the minimal polynomial of $\widetilde{\xi}_{i,j}$ over $\mathbf{k}$, is an irreducible factor of $\Phi(x)$ of degree n. Because $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ and $|\alpha_j - \widetilde{\xi}_{i,j}| < \Delta\Phi_i$ it follows that $\varphi(x) \in \mathcal{O}_{\mathbf{k}}[x]$. $\square$

Lemma 2.5.4. *Assume the hypotheses of proposition 2.5.1 hold. Then* $\mathbf{k}(\xi) \cong \mathbf{k}(\alpha)$ *for every root* ξ *of* $\Phi(x)$ *and every root* α *of* $\varphi(x)$.

Proof. The result is an immediate consequence of lemma 2.5.3 if $n = N$, so we assume $n < N$. Let $\Phi_1(x) := \prod_{i=1}^{n}(x - \xi_{1,i})$ denote the irreducible factor of $\Phi(x)$ given by lemma 2.5.3 and write $\Phi_2(x) := \prod_{j=1}^{N-n}(x - \xi_{2,j}) = \Phi(x)/\Phi_1(x)$. Let $B = \max_{j=1}^{N} |\varphi(\xi_j)|$. By lemma 2.5.3 $\varphi(x)$ is an irreducible polynomial in $\mathcal{O}_{\mathbf{k}}[x]$; because

$$\prod_{i=1}^{n} |\Phi_1(\alpha_i)| = \prod_{j=1}^{n} |\varphi(\xi_{1,j})| \leqslant B^n \quad \text{and} \quad \prod_{i=1}^{n} |\Phi_2(\alpha_i)| = \prod_{j=1}^{N-n} |\varphi(\xi_{2,j})| \leqslant B^{N-n}$$

it follows that $|\Phi_1(\alpha)| \leqslant B$ and $|\Phi_2(\alpha)| \leqslant B^{(N-n)/n}$ for each root α of $\varphi(x)$. We have

$$|\operatorname{disc}\Phi_1|\,|\operatorname{res}(\Phi_1, \Phi_2)| \;=\; \prod_{i=1}^{n}\Bigg(\prod_{j\neq i} |\xi_{1,i} - \xi_{1,j}| \prod_{j=1}^{N-n} |\xi_{1,i} - \xi_{2,j}|\Bigg).$$

Let $\mathcal{G}$ be the Galois group of the extension $\mathbf{k}[\xi_{1,1}, \ldots, \xi_{1,n}]/\mathbf{k} = \mathbf{k}[\alpha_1, \ldots, \alpha_n]/\mathbf{k}$. For $1 \leqslant i \leqslant n$ let $\widetilde{\alpha}_i$ be a root of $\varphi(x)$ that is closest to $\xi_{1,i}$, and for $1 \leqslant j \leqslant n$ let $\sigma_{j,i}$ be a member of $\mathcal{G}$ such that $\xi_{1,j}^{\sigma_{j,i}} = \xi_{1,i}$. Then

$$|\widetilde{\alpha}_i - \xi_{1,i}| \leqslant |\widetilde{\alpha}_i^{\sigma_{j,i}} - \xi_{1,i}| = |\widetilde{\alpha}_i^{\sigma_{j,i}} - \xi_{1,j}^{\sigma_{j,i}}| = |\widetilde{\alpha}_i - \xi_{1,j}|$$

for $1 \leqslant j \leqslant n$. Thus

$$\begin{aligned}
A_i \;&:=\; \Bigg(\prod_{j\neq i} |\xi_{1,i} - \xi_{1,j}|\Bigg)\Bigg(\prod_{j=1}^{N-n} |\xi_{1,i} - \xi_{2,j}|\Bigg) \\
&=\; \Bigg(\prod_{j\neq i} |\xi_{1,i} - \widetilde{\alpha}_i + \widetilde{\alpha}_i - \xi_{1,j}|\Bigg)\Bigg(\prod_{j=1}^{N-n} |\xi_{1,i} - \widetilde{\alpha}_i + \widetilde{\alpha}_i - \xi_{2,j}|\Bigg) \\
&\leqslant\; \Bigg(\prod_{j\neq i} \max\{|\xi_{1,i} - \widetilde{\alpha}_i|, |\widetilde{\alpha}_i - \xi_{1,j}|\}\Bigg)\Bigg(\prod_{j=1}^{N-n} \max\{|\xi_{1,i} - \widetilde{\alpha}_i|, |\widetilde{\alpha}_i - \xi_{2,j}|\}\Bigg) \\
&=\; \Bigg(\prod_{j\neq i} |\widetilde{\alpha}_i - \xi_{1,j}|\Bigg)\Bigg(\prod_{j=1}^{N-n} \max\{|\xi_{1,i} - \widetilde{\alpha}_i|, |\widetilde{\alpha}_i - \xi_{2,j}|\}\Bigg).
\end{aligned}$$

If $|\xi_{1,i} - \widetilde{\alpha}_i| \geqslant |\widetilde{\alpha}_i - \xi_{2,j}|$ for some j then $A_i \leqslant |\Phi_1(\widetilde{\alpha}_i)| \leqslant B$, and if $|\xi_{1,i} - \widetilde{\alpha}_i| < |\widetilde{\alpha}_i - \xi_{2,j}|$ for all j then $A_i \leqslant \prod_{j=1}^{N-n} |\widetilde{\alpha}_i - \xi_{2,j}| = |\Phi_2(\widetilde{\alpha}_i)| \leqslant B^{(N-n)/n} \leqslant B$. Hence

$$B^N < |\operatorname{disc}\Phi|^2 = |\operatorname{disc}\Phi_1|^2|\operatorname{res}(\Phi_1,\Phi_2)|^4|\operatorname{disc}\Phi_2|^2 \leqslant B^n|\operatorname{disc}\Phi_2|^2.$$

It follows that $B^{N-n} < |\operatorname{disc}\Phi_2|^2$, and also that $N-n \geqslant n$ (otherwise $\Phi(x)$ would have an irreducible factor of degree less than n). Repeatedly applying lemma 2.5.3 in this manner we decompose $\Phi(x)$ as a product of irreducible polynomials each of degree n, and the result follows. □

Proof of proposition 2.5.1. By lemma 2.5.4 N must be a multiple of n. If $n = N$ we are done. But if $n < N$ then $\Phi(x)$ is the product of N/n irreducible polynomials, say $\Phi_1(x), \ldots, \Phi_{N/n}(x)$, each of degree n. For $1 \leqslant r \leqslant N/n$ let $\Phi_r(x) = \prod_{i=1}^n (x - \xi_{r,i})$, and for $1 \leqslant i \leqslant n$ let $\widetilde{\alpha}_{r,i}$ denote a root of $\varphi(x)$ that is closest to $\xi_{r,i}$. Arguing as in the proof of lemma 2.5.4 we have

$$\begin{aligned} A_{r,i} &:= \left(\prod_{j\neq i} |\xi_{r,i} - \xi_{r,j}|\right)\left(\prod_{s\neq r}\prod_{j=1}^{n} |\xi_{r,i} - \xi_{s,j}|\right) \\ &\leqslant \left(\prod_{j\neq i} \max\{|\xi_{r,i} - \widetilde{\alpha}_{r,i}|, |\widetilde{\alpha}_{r,i} - \xi_{r,j}|\}\right)\left(\prod_{s\neq r}\prod_{j=1}^{n} |\xi_{r,i} - \xi_{s,j}|\right) \\ &\leqslant \left(\prod_{j\neq i} |\widetilde{\alpha}_{r,i} - \xi_{r,j}|\right)\left(\prod_{s\neq r}\prod_{j=1}^{n} \max\{|\xi_{r,i} - \widetilde{\alpha}_{r,i}|, |\widetilde{\alpha}_{r,i} - \xi_{s,j}|\}\right) \\ &\leqslant B, \end{aligned}$$

hence

$$|\operatorname{disc}\Phi| = \prod_{r=1}^{N/n}\prod_{i=1}^{n} A_{r,i} \leqslant B^N < |\operatorname{disc}\Phi|^2,$$

which since $\operatorname{disc}\Phi \in \mathcal{O}_{\mathbf{k}}$ is impossible. □

2.6 Polynomial Factorization Algorithm

The following algorithm constructs a polynomial $\varphi(x)$ as described in section 2.2. We will use proposition 2.5.1 to show that the algorithm terminates; to do this we need to ensure that $\deg\varphi$ is less than or equal to the degree of any irreducible factor of $\Phi(x)$. As the algorithm progresses we accumulate polynomials $\varphi_i(x)$ with $E_{\varphi_i} > 1$ and use these for altering $\varphi(x)$ so that the valuation of $\varphi(x)$ evaluated at the roots of $\Phi(x)$ increases (see remarks 2.6.7 and 2.6.3). When we find an element γ with $F_\gamma > 1$ we ensure the condition on the degree of $\varphi(x)$ by determining an unramified extension $\widehat{\mathbf{k}}$ of $\mathbf{k}$ with $\widehat{\mathbf{k}} \subseteq \mathbf{k}(\xi)$ for every root ξ of $\Phi(x)$, finding a factor $\widehat{\Phi}(x)$ of $\Phi(x)$ with $\deg(\widehat{\Phi}) = \deg(\Phi)/F_\gamma$ over $\widehat{\mathbf{k}}$, then factoring $\widehat{\Phi}(x)$ itself over $\widehat{\mathbf{k}}$. As we collect more information about the fields generated by the roots of $\Phi(x)$, we enlarge the unramified extension $\widehat{\mathbf{k}}$.

Algorithm 2.6.1 (Polynomial Factorization).

Input: a monic, separable, squarefree polynomial $\Phi(x)$ over a local field $\mathbf{k}$

Output: a proper factorization of $\Phi(x)$ if one exists,
a two-element certificate for $\Phi(x)$ otherwise

- Initialize $\varphi(x) \leftarrow x$, $\widehat{\Phi}(x) \leftarrow \Phi(x)$, $\widehat{\mathbf{k}} \leftarrow \mathbf{k}$, $E \leftarrow 1$, $P \leftarrow \{\ \}$.
- Repeat:
  - **a**) If $\varphi(x)$ fails the Newton test then: [remark 2.6.2]
    - Return a proper factorization of $\Phi(x)$.
  - **b**) If $E_\varphi \nmid E$ then [**increase** E]: [remark 2.6.3]
    - $P \leftarrow P \cup \{\varphi\}$, $S \leftarrow \operatorname{lcm}(E, E_\varphi)/E$, $E \leftarrow SE$, $\varphi(x) \leftarrow \varphi(x)^S$.
    - If $E = \deg \widehat{\Phi}$ then: [remark 2.6.4]
      - Return a two-element certificate for $\Phi(x)$.
  - **c**) Find $\psi(x) = \pi^{c_0}\varphi_1(x)^{c_1}\varphi_2(x)^{c_2}\cdots\varphi_k(x)^{c_k}$ with: [remark 2.6.7]
    $v_{\mathfrak{p}}^*(\psi) = v_{\mathfrak{p}}^*(\varphi)$, $\varphi_i(x) \in P$, $c_0 \in \mathbb{Z}$, $c_i \in \mathbb{N}$ $(i > 0)$, $\deg \psi < E$.
  - **d**) Set $\gamma(x) \leftarrow \varphi(x)\psi^{-1}(x)$. [remark 2.6.5]
  - **e**) If $\gamma(x)$ fails the Hensel test then: [remark 2.6.2]
    - Return a proper factorization of $\Phi(x)$.
  - **f**) If $EF_\gamma = \deg \widehat{\Phi}$ then: [remark 2.6.4]
    - Return a two-element certificate for $\Phi(x)$.
  - **g**) If $F_\gamma > 1$ then [**extend the ground field**]: [remark 2.6.6]
    - Replace $\widehat{\mathbf{k}} \leftarrow \widehat{\mathbf{k}}[y]/\nu_\gamma(y)\widehat{\mathbf{k}}[y]$.
    - Derive a proper factorization $\widehat{\Phi}(x) = \widehat{\Phi}_1(x)\cdots\widehat{\Phi}_r(x)$ of $\widehat{\Phi}(x)$ over $\widehat{\mathbf{k}}$.
    - Replace $\widehat{\Phi}(x) \leftarrow \widehat{\Phi}_i(x)$, with $\deg \widehat{\Phi}_i = \big(\deg \widehat{\Phi}\big)/F_\gamma$.
  - **h**) Find $\delta \in \mathcal{O}_{\widehat{\mathbf{k}}}$ with $\delta \equiv \gamma(\xi) \bmod \pi\mathcal{O}_{\widehat{\mathbf{k}}}$ for all roots ξ of $\Phi(x)$.
  - **i**) Replace $\varphi(x) \leftarrow \varphi(x) - \delta\psi(x)$. [remark 2.6.3]

Remark 2.6.2. A proper factorization of $\widehat{\Phi}(x)$ over $\widehat{\mathbf{k}}$ can be derived by applying proposition 2.3.4 to $\widehat{\Phi}(x)$ and $\varphi(x)$ or corollary 2.3.5 to $\widehat{\Phi}(x)$ and $\gamma(x)$. From this factorization of $\widehat{\Phi}(x)$ over $\widehat{\mathbf{k}}$ a factorization of $\Phi(x)$ over $\mathbf{k}$ can be obtained using remark 2.3.10.

Remark 2.6.3. Replacing $\varphi(x)$ by $\varphi(x)^S$ ensures that $\deg\varphi = E$ when E is replaced by SE, and as $\deg\delta\psi < E$ the degree of $\varphi(x)$ remains equal to E when $\varphi(x)$ is replaced by $\varphi(x) - \delta\psi(x)$. As $\varphi(x) = x$ initially, $\varphi(x)$ remains monic.

Remark 2.6.4. If $E = \deg\widehat{\Phi}$ then every root ξ of $\widehat{\Phi}(x)$ generates an extension of degree $\deg\widehat{\Phi}$, and hence $\widehat{\Phi}(x)$ is irreducible. It follows from proposition 2.5.1 that $\deg\varphi = E = \deg\widehat{\Phi}$ if $\deg\widehat{\Phi}\cdot v_{\mathfrak{p}}^*(\varphi) > 2v_{\mathfrak{p}}(\operatorname{disc}\Phi)$. As $v_{\mathfrak{p}}^*(\varphi)$ increases strictly algorithm 2.6.1 terminates. There exist $c_0 \in \mathbb{Z}$ and $c_1, \ldots, c_s \in N$ such that $\Pi(x) := \varphi_1(x)^{c_1}\cdots\varphi_s(x)^{c_s}$ with $\varphi_i(x) \in P$ and $v_{\mathfrak{p}}^*(\Pi) = 1/E$. Following section 2.4 we construct a two-element certificate of $\Phi(x)$.

Remark 2.6.5. In practice we find $\widehat{\psi}(x) \in \widehat{\mathbf{k}}[x]$ such that $\widehat{\psi}(x)\psi(x) \equiv 1 \bmod \widehat{\Phi}(x)$ and set $\gamma(x) \leftarrow \varphi(x)\widehat{\psi}(x)$. Note that $v_{\mathfrak{p}}^*(\gamma) = 0$. As only the values of the polynomials $\gamma(x)$ and $\widehat{\psi}(x)$ at the roots of $\widehat{\Phi}(x)$ are of concern, these polynomials can be reduced modulo $\widehat{\Phi}(x)$.

Remark 2.6.6. As $F_\gamma > 1$, and as $\widehat{\Phi}(x)$ and therefore $\nu_\gamma(y)$ are separable, $\nu_\gamma(y)$ must have at least two distinct factors over $\widehat{\mathbf{k}}[y]/\nu_\gamma(y)\widehat{\mathbf{k}}[y]$, at least one of which is linear. Proposition 2.3.4 gives a factorization of $\widehat{\Phi}(x)$ over $\widehat{\mathbf{k}}[y]/\nu_\gamma(y)\widehat{\mathbf{k}}[y]$.

Remark 2.6.7. Let the elements in P be numbered so that the increase of E by the factor S_j due to $\varphi_j(x)$ is followed by the increase of E by the factor S_{j+1} due to $\varphi_{j+1}(x)$. As $E_\varphi \mid E$ there is an element $\psi(x) = \pi^{c_0}\varphi_1(x)^{c_1}\cdots\varphi_k(x)^{c_k}$ with $v_{\mathfrak{p}}^*(\psi) = v_{\mathfrak{p}}^*(\varphi)$. By construction of the $\varphi_j(x)$ we have the relations

$$v_{\mathfrak{p}}^*(\varphi_j^{S_j}) = v_{\mathfrak{p}}^*(\pi^{b_j}\varphi_1^{b_{j,1}}\cdots\varphi_{j-1}^{b_{j,j-1}})$$

with $b_j \in \mathbb{Z}$ and $b_{j,i} \in \mathbb{N}$; hence we can reduce the exponents $c_1, \ldots, c_k$ so that $0 \leqslant c_j < S_j$ for $1 \leqslant j \leqslant k$. We get

$$\begin{aligned}
\deg\psi &\leqslant (S_1 - 1) + (S_2 - 1)S_1 + (S_3 - 1)S_1S_2 + \cdots + (S_k - 1)S_1\cdots S_{k-1} \\
&= (-1 + S_1\cdots S_k) \;=\; E - 1.
\end{aligned}$$

The integers $c_0, c_1, \ldots, c_k$ can be computed using the following algorithm.

Algorithm 2.6.8.

Input: A list of pairs $\big(a_i/b_i,\, S_i\big)$, $1 \leqslant i \leqslant k$, with $a_i,\, b_i,\, S_i \in \mathbb{N}$, $\gcd(a_i,\, b_i) = 1$ and $\operatorname{lcm}(b_1, \ldots, b_{i-1}) \cdot S_i = \operatorname{lcm}(b_1, \ldots, b_i)$ for all $1 \leqslant i \leqslant k$, and a rational number $w = t/u$ where $\gcd(t,\, u) = 1$ and $u \leqslant \prod_{i=1}^{k} S_i$

Output: Positive integers $c_0, \ldots, c_k$ with $c_0 \in \mathbb{Z}$, $0 \leqslant c_i < S_i$ for $1 \leqslant i \leqslant k$, and $c_0 + \sum_{i=1}^{k} c_i \cdot a_i/b_i = w$.

- Set $T \leftarrow \prod_{i=1}^{k} S_i$.
- For i from 1 to k:
  - Replace $T \leftarrow T/S_i$ and set $d \leftarrow b_i/\gcd(b_i,\, T)$.
  - Set $r \leftarrow T \cdot d \cdot a_i/b_i$ and $s \leftarrow w \cdot e \cdot d$.
  - Find c_i so that $c_i \cdot r \equiv s \bmod d$ with $0 \leqslant x < d$.
  - Replace $w \leftarrow w - c_i \cdot a_i/b_i$.
- Set $c_0 \leftarrow w$.
- Return $c_0, \ldots, c_k$.

2.7 Examples

In the first example we show the irreducibility of a polynomial $\Phi(x)$ whose roots generate totally ramified extensions of $\mathbb{Q}_2$. We need to increase the ramification index bound E twice to show the irreducibility of $\Phi(x)$. From the polynomials collected in the set P we compile a certificate for the irreducibility of $\Phi(x)$.

In the second example a polynomial $\Psi(x)$ is factored over $\mathbb{Q}_3$. In the first iteration of the algorithm we discover that all extensions of $\mathbb{Q}_3$ generated by roots of $\Psi(x)$ contain an unramified extension $\widehat{\mathbf{k}}/\mathbb{Q}_3$. We derive a factorization of $\Psi(x)$ over $\widehat{\mathbf{k}}$ from which we obtain a factorization of $\Psi(x)$ over $\mathbb{Q}_3$.

In the third example we factor a polynomial over the field $\mathbb{F}_3\,((t))$.

Example 2.7.1. Let $\mathbf{k} = \mathbb{Q}_2$ and

$$\Phi(x) = x^6 + 3{\cdot}2x^4 + 2^5x^3 + 3{\cdot}2^2x^2 - 3{\cdot}2^6x + 33{\cdot}2^3.$$

Initially we set $P := \{\ \}$ and $\varphi(x) := x$, hence $\chi_\varphi(y) = \Phi(y)$. It follows that $\varphi(x)$ passes the Hensel and Newton tests. We find $v_2^*(\varphi) = 1/2$, thus $E_\varphi = 2$, and we set $E := 2$, $\varphi_1(x) := \varphi(x)$ and replace P by $\{\varphi_1(x)\}$.

We replace $\varphi(x)$ by x^2; thus $\psi(x) = 2$ and $\gamma(x) = \varphi(x)\psi^{-1}(x) = 2^{-1}x^2$ with $\underline{\chi}_\gamma(y) = y^6 - y^4 + y^2 - 1$. Hence $\nu_\gamma(y) = y + 1$.

We replace $\varphi(x)$ by $\varphi(x) - (-1)\psi(x) = x^2 + 2$. As

$$\chi_\varphi(y) = y^6 - 2^9 y^3 + 9{\cdot}2^{11}y^2 - 3{\cdot}2^{15}y + 3{\cdot}2^{16}$$

the polynomial $\varphi(x)$ passes the Hensel and Newton tests. We have $v_2^*(\varphi) = 8/3$ and $E_\varphi = 3$. We replace E by $\mathrm{lcm}(E, E_\varphi) = 6$, we set $\varphi_2(x) := \varphi(x)$, and we replace P by $\{\varphi_1(x),\, \varphi_2(x)\}$.

The ramification index of an extensions of $\mathbb{Q}_2$ generated by a root of $\Phi(x)$ must be at least $E = 6$. As the degree of $\Phi(x)$ is six, $\Phi(x)$ is irreducible. The irreducibility of $\Phi(x)$ is certified by the two-element certificate $(1,\, \Pi(x))$ with $\Pi(x) := 2^{-3}\varphi_1(x)\varphi_2(x) = 2^{-3}x^3 + 2^{-2}x$. Note that $v_2^*(\Pi) = 1/6$.

Example 2.7.2. Let $\mathbf{k} = \mathbb{Q}_3$ and

$$\Psi(x) = x^8 + 4x^6 + 2{\cdot}3x^4 + 7x^2 + 3^2x + 13.$$

We derive a factorization of $\Psi(x)$ over $\mathbb{Q}_3$ to a precision of twelve 3-adic digits.

Initially we set $\varphi(x) := x$. Then $\chi_\varphi(y) = \Psi(y)$ and $\nu_\varphi(y) = y^2 + 1$. Thus we continue our computation over the extended ground field $\widehat{\mathbf{k}} := \mathbf{k}[y]/\nu_\varphi(y)\mathbf{k}[y]$. Let α be a primitive element of $\widehat{\mathbf{k}}$. Hensel lifting gives the factors

$$\begin{aligned}\widehat{\Psi}(x) = x^4 &+ 435740\alpha x^3 + (-33734{\cdot}3^2\alpha - 59774{\cdot}3)x^2 \\ &+ (-89882\alpha + 8443{\cdot}3^2)x + (-5132{\cdot}3^2\alpha + 520585)\end{aligned}$$

and its conjugate

$$\begin{aligned}x^4 &- 435740\alpha x^3 + (33743{\cdot}3^2\alpha - 59774{\cdot}3)x^2 \\ &+ (89882\alpha + 8443{\cdot}3^2)x + (5132{\cdot}3^2\alpha + 520585)\end{aligned}$$

of Ψ over $\widehat{\mathbf{k}}$. We now factorize $\widehat{\Psi}(x)$ over $\widehat{\mathbf{k}}$.

Over $\widehat{\mathbf{k}}$ the polynomial $\varphi(x) = x$ has characteristic polynomial $\chi_\varphi(y) = \widehat{\Psi}(y)$. Hence $\varphi(x)$ passes the Hensel and Newton tests and $\nu_\varphi(y) = y + 2\alpha$.

Thus $\psi(x) = 1$, $\gamma(x) = \varphi_1(x)$, and $\delta = -2\alpha$. Replacing $\varphi(x)$ by $\varphi(x) - \delta\psi(x) = x + 2\alpha$. we get

$$\chi_\varphi(y) = y^4 \; + (145244{\cdot}3\alpha)y^3 + (-33734{\cdot}3^2\alpha - 24679{\cdot}3^2)y^2 \\ + (-116638{\cdot}3\alpha + 50654{\cdot}3^2)y + (53869{\cdot}3^2\alpha - 33559{\cdot}3^2);$$

thus $\varphi(x)$ fails the Newton test. Note that the valuations of the roots of $\chi_\varphi(y)$ are $1/3$ and 1. The polynomial $\vartheta(x) := \varphi(x)^3/3$ with

$$\chi_\vartheta(y) = y^4 \; + (-155281{\cdot}3\alpha + 16838{\cdot}3^2)y^3 + (-3793{\cdot}3^2\alpha + 60782{\cdot}3)y^2 \\ + (277066\alpha + 9565{\cdot}3^2)y + (8165{\cdot}3^2\alpha - 8350)$$

fails the Hensel test. Hensel lifting gives the factors

$$\chi_{\vartheta,1}(y) = y \; - (4151{\cdot}3^2\alpha + 57679{\cdot}3^2),$$
$$\chi_{\vartheta,2}(y) = y^3 + (-142828{\cdot}3\alpha + 5156{\cdot}3^3)y^2 + (-30373{\cdot}3^2\alpha + 150737{\cdot}3)y \\ + (-520028\alpha - 17123{\cdot}3^2)$$

of $\chi_\vartheta(y)$. We obtain the factors

$$\widehat{\Psi}_1(x) := \gcd(\widehat{\Psi}, \chi_{\vartheta,1}(\vartheta(x)) = x + 391409\alpha - 26500{\cdot}3,$$
$$\widehat{\Psi}_2(x) := \gcd(\widehat{\Psi}, \chi_{\vartheta,2}(\vartheta(x)) = x^3 + (14777{\cdot}3\alpha - 150647{\cdot}3)x^2 \\ + (158332{\cdot}3\alpha - 117802{\cdot}3)x + 188791\alpha - 185620$$

of $\widehat{\Psi}(x)$. As $\chi_\varphi(y)$ has a root of valuation $1/3$ at least one of the extensions given by roots of $\widehat{\Psi}(x)$ must have ramification index greater than or equal to three. Thus $\widehat{\Psi}_2(x)$ is irreducible. Computing the norm of $\widehat{\Psi}_1(x)$ and $\widehat{\Psi}_2(x)$ we get the irreducible factors of $\Psi(x)$ modulo 3^{12} over $\mathbf{k}$:

$$\Psi_1(x) := \mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\widehat{\Psi}_1) = x^2 - 53000{\cdot}3x + 204634$$
$$\Psi_2(x) := \mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\widehat{\Psi}_2) = x^6 - 124147{\cdot}3x^5 - 128147{\cdot}3x^4 + 120868{\cdot}3x^3 \\ + 28201{\cdot}3x^2 + 107405{\cdot}3x + 312880.$$

The two-element certificate $(\Gamma_1(x), \Pi_1(x)) = (x, 3)$ certifies $\Phi_1(x)$; the two-element certificate $(\Gamma_2(x), \Pi_2(x)) = (x, \mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(x + 2\alpha)) = (x, x^2 + 4)$ certifies $\Phi_2(x)$.

Example 2.7.3. Let $\mathbf{k} = \mathbb{F}_3((t))$ be the completion of $\mathbb{F}_3(t)$ with respect to $v_t(\cdot)$, normalized such that $v_t(t) = 1$. Let

$$\Phi(x) = x^6 + 2tx^4 + (t^7 + 2t)x^3 + t^2x^2 + (t^8 + 2t^2)x + t^2 \in \mathbb{F}_3((t))[x].$$

We derive a factorization of $\Psi(x) \in \mathbf{k} = \mathbb{F}_3((t))[x]$ to a precision of 32 digits. Initially we set $\varphi(x) := x$. Then $\chi_\varphi(y) = \Phi(y)$. Thus $\varphi(x) = x$ passes the Hensel and Newton tests and we obtain $v_t^*(\varphi) = 1/3$. Replacing $\varphi(x)$ by x^3 we get

$$\chi_\varphi(y) = y^6 + 2t^3y^4 + (t^{21} + 2t^3)y^3 + t^6y^2 + (t^{24} + 2t^6)y + t^6.$$

and therefore $v_t^*(\varphi) = 1$. Thus we set $\gamma(x) := \varphi(x)/t = x^3/t$. Now

$$\chi_\gamma(y) = y^6 + 2ty^4 + (t^{18} + 2)y^3 + t^2y^2 + (t^{19} + 2t)y + 1$$

with $\underline{\chi_\gamma}(y) = y^6 + 2y^3 + 1$ and $\nu_\gamma(y) = y + 1$. Hence we replace $\varphi(x)$ by $x^3 + t$. The characteristic polynomial

$$\chi_\varphi(y) = y^6 + 2t^3y^4 + (t^{21} + t^4)y^3 + t^6y^2 + (t^{24} + t^7)y + 2t^25 + 2t^24 + t^8$$

of φ passes the Hensel and Newton tests. As $v_t^*(\varphi) = 8/6 = 4/3$ we set $\psi(x) = tx$. The characteristic polynomial of $\gamma(x) = \varphi(x)\psi^{-1}(x)$ is

$$\begin{aligned}\chi_\gamma(y) = y^6 + t^6y^5 + t^6y^4 + (2t^11 + 2)y^3 + (2t^{17} + t^{11} + t^6)y^2\\ + (t^{17} + 2t^{11} + t^6)y + 2t^{17} + 2t^{16} + 1\end{aligned}$$

with $\nu_\gamma(y) = y + 1$. Replacing $\varphi(x)$ with $\varphi(x) - (-1)\psi(x) = x^3 + tx + t$ we get

$$\chi_\varphi(y) = y^6 + t^{21}y^3 + 2t^{24}.$$

Thus $\varphi(x)$ passes the Hensel and Newton tests.

As $v_t^*(\varphi) = 4$ we set $\gamma(x) := \varphi(x)/t^4 = (x^3 + tx + t)/t^4$ and get $\chi_\gamma(y) = y^6 + t^9y^3 + 2$. We have

$$\underline{\chi_\gamma}(y) = (y + \underline{1})^3(y + \underline{2})^3.$$

Hensel Lifting gives the factors

$$\begin{aligned}\chi_{\gamma,1}(y) &= y^3 + 2t^{18} + 2t^9 + 1 \text{ and}\\ \chi_{\gamma,2}(y) &= y^3 + t^{18} + 2t^9 + 2\end{aligned}$$

of $\chi_\gamma(y)$ modulo t^32. As the sum of the degrees of the polynomials

$$\chi_{\gamma,1}(\gamma(x)) \equiv (t^6 + 1)/t^4 \cdot x^3 + (t^6 + 1)/t^3 \cdot x + (2t^{21} + 2t^{12} + t^3 + 1)/t^3 \bmod \Phi(x),$$
$$\chi_{\gamma,2}(\gamma(x)) \equiv (t^6 + 1)/t^4 \cdot x^3 + (t^6 + 1)/t^3 \cdot x + (t^{21} + 2t^{12} + 2t^3 + 1)/t^3 \bmod \Phi(x)$$

is equal to the degree of Φ we only need to divide by the leading coefficients in order to derive a factorization of Φ. Thus the polynomials

$$\Phi_1(x) = x^3 + tx + 2t^{28} + t^{22} + t^{16} + 2t^{10} + 2t^7 + t^4 + t,$$
$$\Phi_2(x) = x^3 + tx + t^{28} + 2t^{22} + 2t^{16} + t^{10} + 2t^7 + 2t^4 + t$$

are the irreducible factors of $\Phi(x)$ to a precision of 32 digits. The two-element certificates $(\Gamma_1(x), \Pi_1(x)) = (1, x)$ and $(\Gamma_2(x), \Pi_2(x)) = (1, x)$ certify their irreducibility.

2.8 Complexity Analysis

Theorem 2.8.1. *Let* $\mathbf{k}$ *be a local field and let* $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ *be monic, separable, and squarefree of degree* N.

There exists an algorithm that derives a factorization of $\Phi(x)$ *into irreducible factors and returns an integral basis of* $\mathbf{k}[x]/\varphi(x)\mathbf{k}[x]$ *for every irreducible factor* $\varphi(x)$ *of* $\Phi(x)$ *with the number of arithmetic operations in* $\mathbf{k}$ *being*

$$O\big(\log N(\mathsf{P}(N,N) + \mathsf{T}(N,N) + \mathsf{C}(N)) + v_{\mathfrak{p}}(\operatorname{disc}\Phi)(\mathsf{R}(1,N) + \mathsf{P}(N,N))\big).$$

Lemma 2.8.2. *Let* $\mathbf{k}$ *be a local field and let* $\Phi(x) \in \mathbf{k}[x]$ *be monic, separable, and squarefree of degree* N. *Let* E_Φ *be the minimum of the ramification indices and* F_Φ *be the minimum of the inertia degrees of all extensions of* $\mathbf{k}$ *generated by roots of* $\Phi(x)$.

Algorithm 2.6.1 derives a proper factorization of $\Phi(x)$ *or a two-element certificate for* $\Phi(x)$ *with the number of arithmetic operations in* $\mathbf{k}$ *being*

$$O\Big(\log F_\Phi\big(\mathsf{P}(N,F_\Phi) + \mathsf{C}(F_\Phi) + \mathsf{T}(N,N)\big) + E_\Phi \frac{v_{\mathfrak{p}}(\operatorname{disc}\Phi)}{N}\big(\mathsf{R}(1,N) + \mathsf{P}(N,F_\Phi)\big)\Big).$$

Proof. Let $\widehat{\mathbf{k}}$ be an unramified extension of $\mathbf{k}$ contained in $\mathbf{k}(\xi)$ for all roots ξ of $\Phi(x)$ and let $F = [\widehat{\mathbf{k}} : \mathbf{k}]$. Then $v_{\mathfrak{p}}(\operatorname{disc}\Phi) \geqslant F v_{\mathfrak{p}}(\operatorname{disc}\widehat{\Phi})$, where $\widehat{\Phi}(x)$ is a factor of degree N/F of $\Phi(x)$ over $\widehat{\mathbf{k}}$. Therefore extending the ground field does not increase the number of repetitions of the main loop, *i.e.*, steps **a**), **c**) to **f**) and **i**) are repeated at most $2(E_\Phi/N)v_{\mathfrak{p}}(\operatorname{disc}\Phi)$ times by proposition 2.5.1. Note that two polynomials of degree $(\deg\Phi)/F$ over an extension $\widehat{\mathbf{k}}$ of degree F of $\mathbf{k}$ can be multiplied in $\mathsf{M}(F \cdot N/F) = \mathsf{M}(N)$ operations in $\mathbf{k}$.

a) The resultant in the Hensel test needs $\mathsf{R}(1,N)$ arithmetic operations in $\mathbf{k}$.

b) [**increase** E] An increase of E can occur at most $\log_2 E_\Phi$ times. Computing $\varphi(x)^S$ is of complexity $\mathsf{M}(N)\log E_\Phi$.

c) The extended euclidian algorithm needed for the computation of ψ^{-1} is of complexity $O(\mathsf{M}(N)\log N)$.

e) The resultant in the Newton test needs $\mathsf{R}(1,N)$ arithmetic operations in $\mathbf{k}$.

g) [**extend the ground field**] The ground field can be extended at most $\log_2 F_\Phi$ times. Factoring $\chi_\gamma(y)$ over the residue class field is of complexity $\mathsf{P}(N/F,F)$. The construction of a primitive element of a compositum of two residue class field is of complexity $\mathsf{C}(F_\Phi)$. Deriving a proper factorization requires approximating the greatest common divisor (see proposition 2.3.6) and computing the norm of $\widehat{\Phi}(x)$ over $\mathbf{k}$ (see remark 2.3.11). This can be achieved in $\mathsf{T}(N,N)$, respectively $\mathsf{R}(F,N/F)$, operations in $\mathbf{k}$.

h) The factorization of $\chi_\gamma(y)$ over the residue class field is of complexity $\mathsf{P}(N/F,F)$.

Thus a proper factorization of $\Phi(x)$ or a two-element certificate for $\Phi(x)$ can be derived with the number of arithmetic operations in $\mathbf{k}$ being

$$\begin{aligned}
&O\Big(\log F_\Phi\big(\mathsf{R}(1,N)+\mathsf{P}(N,F_\Phi)+\mathsf{C}(F_\Phi)+\mathsf{T}(N,N)\big)+\log E_\Phi\big(\mathsf{M}(N)\log(N)\big)\\
&\qquad\qquad+E_\Phi\frac{v_\mathfrak{p}(\operatorname{disc}\Phi)}{N}\big(\mathsf{R}(1,N)+\mathsf{P}(N,F_\Phi)\big)\Big)\\
&=O\Big(\log F_{\Phi_i}\big(\mathsf{P}(N,F_{\Phi_i})+\mathsf{C}(F_\Phi)+\mathsf{T}(N,N)\big)+E_{\Phi_i}\frac{v_\mathfrak{p}(\operatorname{disc}\Phi)}{N}\big(\mathsf{R}(1,N)+\mathsf{P}(N,F_{\Phi_i})\big)\Big).
\end{aligned}$$

□

Proof of theorem 2.8.1. Denote by $\Phi_1(x),\dots,\Phi_m(x)$ the irreducible factors of $\Phi(x)$. Let F_{Φ_i} be the inertia degree of the field given by $\Phi_i(x)$. Let E_{Φ_i} be the ramification index of the field given by $\Phi_i(x)$. It follows from 2.8.2 that the number of arithmetic operations required for deriving a factorization of $\Phi(x)$ into irreducible factors is

$$\begin{aligned}
&\sum_{i=1}^m O\Big(\log F_{\Phi_i}\big(\mathsf{P}(N,F_{\Phi_i})+\mathsf{C}(F_\Phi)+\mathsf{T}(N,N)\big)+E_{\Phi_i}\frac{v_\mathfrak{p}(\operatorname{disc}\Phi)}{N}\big(\mathsf{R}(1,N)+\mathsf{P}(N,F_{\Phi_i})\big)\Big)\\
&\qquad=O\big(\log N(\mathsf{P}(N,N)+\mathsf{C}(N)+\mathsf{T}(N,N))+v_\mathfrak{p}(\operatorname{disc}\Phi)(\mathsf{R}(1,N)+\mathsf{P}(N,N))\big).
\end{aligned}$$

□

Note that there are algorithms for factoring a polynomial of degree N over $\mathbb{F}_q$ with the expected number of bit operations being $O(N^2 \log q)$ (see Kaltofen and Shoup [1998]).

If the residue class field of $\mathbf{k}$ is finite then lemma 2.4.4 implies that the expected number of resultants needed to find an element δ such that $\underline{\delta}$ is a primitive element of the compositum $\underline{\mathbf{k}}(\underline{\beta}, \underline{\gamma})$ is $O(1)$. Therefore, in this case, the expected value of $\mathsf{C}(N)$ is $O(N\mathsf{M}(N)\log(N))$ operations in $\mathbf{k}$.

It follows from proposition 2.5.1 and remark 2.3.8 that throughout the algorithm a precision of $2v_\mathfrak{p}(\operatorname{disc}\Phi)$ digits in the ground field is sufficient. Thus $\mathfrak{p}^{2v_\mathfrak{p}(\operatorname{disc}\Phi)}$ can be used as a modulus for the triangulization of the matrices occuring in the computation of the approximations of the greatest common divisor. Noting that the triangularization is done over a local ring and to a fixed precision, it is easily seen that $\mathsf{T}(N, N) = O(N^3)$.

Corollary 2.8.3. *Let $\mathbf{k}$ be a finite extension of $\mathbb{Q}_p$ of degree k. Let $\Phi(x) \in \mathcal{O}_\mathbf{k}[x]$ be a monic, separable, and squarefree polynomial. There exists an algorithm that*

- *derives a factorization of $\Phi(x)$ into irreducible factors and*
- *returns an integral basis of $\mathbf{k}[x]/\varphi(x)\mathbf{k}[x]$ for every irreducible factor $\varphi(x)$ of $\Phi(x)$*

with the expected number of bit operations being

$$O\big(N^{3+\varepsilon} v_\mathfrak{p}(\operatorname{disc}\Phi)^{1+\varepsilon} \log^{1+\varepsilon} p^k + N^{2+\varepsilon} v_\mathfrak{p}(\operatorname{disc}\Phi)^{2+\varepsilon} \log^{1+\varepsilon} p^k\big).$$

Chapter 3

Totally Ramified Extensions

Let $\mathbf{k}$ be a $\mathfrak{p}$-adic field. Let $n > 1$, $d \geqslant 0$ be integers, and let $\mathfrak{p}$ be the prime ideal of $\mathbf{k}$. In this chapter, we give an algorithm to compute all extensions of degree n and discriminant $\mathfrak{p}^d$.

In section 3.1 we state Ore's conditions, which give all possible discriminants $\mathfrak{p}^d$ of totally ramified extensions of degree n. In section 3.2 we introduce an ultrametric distance on the set of Eisenstein polynomials of degree n. This distance is used in section 3.3 in the construction of a set of polynomials defining all totally ramified extensions of degree n. In section 3.4 we give explicit formulae for the number of totally ramified extensions. In section 3.8 we describe the construction of totally and tamely ramified extensions since this construction is easier than in the general case. It is also possible to construct a set of generating polynomials for all extensions of degree p in general (see section 3.6) and of extensions of degree p^m with some restrictions. (see section 3.7). Section 3.10 contains two examples.

Note that similar formulas can also be given for local fields of characteristic $p \neq 0$. The following result shows us that these are not particularly interesting.

Theorem 3.0.4. *Assume that* $\operatorname{char} \mathbf{k} = \operatorname{char} \underline{\mathbf{k}} = p \neq 0$ *and that* $\underline{\mathbf{k}}$ *is perfect.*

Then $\mathbf{k}$ *is isomorphic to* $\mathbf{k} \cong \underline{\mathbf{k}}((\pi))$, *the field of all power series in one indeterminate* π *over* $\underline{\mathbf{k}}$ *with the exponential valuation given by the exponent of the lowest power of* π*.*

Thus for the rest of our discussion we focus on the totally ramified extension $\mathbf{K}$ of degree n of a $\mathfrak{p}$-adic field $\mathbf{k}$. Let $\mathfrak{p}$ and e be the prime ideal and the absolute ramification index of $\mathbf{k}/\mathbb{Q}_p$ respectively. We denote the uniformizer of $\mathfrak{p}$ by π.

Let $v_\mathfrak{p}$ denote the unique prolongation of v_p to $\mathbf{k}$ such that $v_\mathfrak{p}(\pi) = 1$. Let q denote the cardinality of the residue class field of $\mathbf{k}$.

3.1 Discriminants

The possible discriminants for totally ramified extensions of $\mathbf{k}$ are given by the following criterion from Ore [1926].

Proposition 3.1.1 (Ore's Conditions). *Let $\mathbf{k}$ be a finite extension of $\mathbb{Q}_p$ with maximal ideal $\mathfrak{p}$. Given $j \in \mathbb{Z}$ let $a, b \in \mathbb{Z}$ be such that $j = an + b$ and $0 \leqslant b \leqslant n-1$. Then there exist totally ramified extensions $\mathbf{K}/\mathbf{k}$ of degree n and discriminant $\mathfrak{p}^{n+j-1}$ if and only if*

$$\min\{v_\mathfrak{p}(b)n, v_\mathfrak{p}(n)n\} \leqslant j \leqslant v_\mathfrak{p}(n)n.$$

Proof. Every totally ramified extension $\mathbf{K}$ of $\mathbf{k}$ can be generated by a root ξ of an Eisenstein polynomial $\varphi(x) = x^n + \varphi_{n-1}x^{n-1} + \ldots + \varphi_0$. We have $\operatorname{disc}(\mathbf{K}/\mathbf{k}) = \operatorname{disc}(\varphi)$ and $v_\mathfrak{p}(\operatorname{disc}(\varphi))/n = v_\mathfrak{p}(\varphi'(\xi))$. Because $v_\mathfrak{p}(\xi) = 1/n$ the valuations of $i\varphi_i\xi^{i-1}$ for $1 \leqslant i < n$ and $n\xi^{n-1}$ are all different, we get

$$\begin{aligned} v_\mathfrak{p}(\varphi'(\xi)) &= v_\mathfrak{p}(n\xi^{n-1} + (n-1)\varphi_{n-1}\xi^{n-2} + \ldots + \varphi_1) \\ &= \min_{1 \leqslant i \leqslant n-1} \left\{ v_\mathfrak{p}(n) + \frac{n-1}{n}, v_\mathfrak{p}(i) + v_\mathfrak{p}(\varphi_i) + \frac{i-1}{n} \right\} \\ &= \min_{1 \leqslant i \leqslant n-1} \left\{ \frac{nv_\mathfrak{p}(n)}{n}, \frac{n(v_\mathfrak{p}(i) + v_\mathfrak{p}(\varphi_i) - 1) + i}{n} \right\} + \frac{n-1}{n} \end{aligned}$$

Setting $j := v_\mathfrak{p}(\operatorname{disc}(\varphi)) - n + 1 = nv_\mathfrak{p}(\varphi'(\xi)) - n + 1$ gives

$$j = \min_{1 \leqslant i \leqslant n-1} \{nv_\mathfrak{p}(n), n(v_\mathfrak{p}(i) + v_\mathfrak{p}(\varphi_i) - 1) + i\}.$$

Thus either $j = nv_\mathfrak{p}(n)$ or $j = n(v_\mathfrak{p}(b) + v_\mathfrak{p}(\varphi_b) - 1) + b$ for some $1 \leqslant b \leqslant n-1$. Fix $b \in \mathbb{Z}$ with $1 \leqslant b \leqslant n-1$. Set $a := v_\mathfrak{p}(b) + v_\mathfrak{p}(\varphi_b) - 1$. As $v_\mathfrak{p}(\varphi_b) - 1 \geqslant 0$ we get $nv_\mathfrak{p}(b) + b \leqslant j = an + b$. Because $n \nmid b$ we can simplify this condition to $nv_\mathfrak{p}(b) \leqslant j = an + b$. Combining this case with $j = nv_\mathfrak{p}(n)$ we get $\min\{nv_\mathfrak{p}(b), nv_\mathfrak{p}(n)\} \leqslant j \leqslant nv_\mathfrak{p}(n)$.

It is clear from the discussion above that for every $j = an + b$ with

$$\min\{nv_{\mathfrak{p}}(b), nv_{\mathfrak{p}}(n)\} \leqslant j \leqslant nv_{\mathfrak{p}}(n)$$

we can construct an Eisenstein polynomial $\varphi(x)$ such that $\operatorname{disc}(\varphi) = \mathfrak{p}^{n+j-1}$. $\square$

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

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

Proposition 3.1.2. *Let $\mathbf{k}$ be a finite extension of $\mathbb{Q}_p$ with maximal ideal $\mathfrak{p}$. Let $\mathbf{K}/\mathbf{k}$ be a totally ramified field extension of degree n and discriminant $\mathfrak{p}^{n+j-1}$. Let n_0, n_1 be two positive integers such that $n = n_0 n_1$. Suppose $\mathbf{K}/\mathbf{k}$ has an intermediate field $\mathbf{K}_0$ of degree n_0 and discriminant $\mathfrak{p}^{n_0+j_0-1}$. Then 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 $\mathbf{K}/\mathbf{k}$ admits a sub-extension $\mathbf{K}_0/\mathbf{k}$ 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 $\mathbf{K}_0/\mathbf{k}$ (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

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

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

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

which proves the result. $\square$

3.2 Eisenstein Polynomials

We now fix an integer j fulfilling Ore's conditions (proposition 3.1.1) and turn to the more specific problem of the construction of all totally ramified extensions $\mathbf{K}/\mathbf{k}$ of degree n and discriminant $\mathfrak{p}^{n+j-1}$.

Definition 3.2.1. Let $\mathbf{k}$ be a local field with maximal ideal $\mathfrak{p}$. We denote by $\mathbf{K}_{n,j}$ the set of all extensions of $\mathbf{k}$ of degree n and discriminant $\mathfrak{p}^{n+j-1}$.

Let $\mathbf{E}_{n,j}$ denote the set of all Eisenstein polynomials over $\mathbf{k}$ of degree n and discriminant $\mathfrak{p}^{n+j-1}$. The roots of the polynomials in $\mathbf{E}_{n,j}$ generate all the extensions $\mathbf{K} \in \mathbf{K}_{n,j}$.

For two elements $\varphi(x)$ and $\psi(x)$ of $\mathbf{E}_{n,j}$, we set $d(\varphi, \psi) := |\varphi(\beta)|$ where β is a root of $\psi(x)$. Let β' be any root of $\psi(x)$ and let $\sigma \in \mathrm{Gal}(\psi)$ over $\mathbf{k}$ such that $\sigma(\beta) = \beta'$. Since σ is an isometry, we have $|\varphi(\beta)| = |\sigma(\varphi(\beta))| = |\varphi(\sigma(\beta))| = |\varphi(\beta')|$ hence $d(\varphi, \psi)$ does not depend on the choice of β. Observe that

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

where β_i (respectively α_j) denote the roots of $\psi(x)$ (respectively $\varphi(x)$). The last formula is symmetric with respect to $\varphi(x)$ and $\psi(x)$. Thus for any root α of $\varphi(x)$ we obtain the equality $|\varphi(\beta)| = |\psi(\alpha)|$. Hence, $d(\varphi, \psi) = d(\psi, \varphi)$.

The distance $d(\varphi, \psi)$ is easily calculated using the following lemma.

Lemma 3.2.2. *Write $\varphi(x) = x^n + \varphi_{n-1}x^{n-1} + \cdots + \varphi_0$ and $\psi(x) = x^n + \psi_{n-1}x^{n-1} + \cdots + \psi_0$ and set*

$$w := \min_{0 \leqslant i \leqslant n-1} \left\{ v_{\mathfrak{p}}(\psi_i - \varphi_i) + \frac{i}{n} \right\}.$$

Then $d(\varphi, \psi) = |\pi|^w$.

Proof. Observe that

$$\psi(\alpha) = \psi(\alpha) - \varphi(\alpha) = \sum_{i=0}^{n-1} (\psi_i - \varphi_i)\alpha^i,$$

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

Let $\varphi(x) = x^n + \varphi_{n-1}x^{n-1} + \cdots + \varphi_0$, $\psi(x) = x^n + \psi_{n-1}x^{n-1} + \cdots + \psi_0$, and $\vartheta(x) = x^n + \vartheta_{n-1}x^{n-1} + \cdots + \vartheta_0$ be polynomials in $\mathbf{E}_{n,j}$. We have

$$
\begin{aligned}
&\min_{0\leqslant i\leqslant n-1}\left\{v_{\mathfrak{p}}(\varphi_i-\psi_i)+\frac{i}{n}\right\}\\
&\geqslant \min_{0\leqslant i\leqslant n-1}\left\{\min\left\{v_{\mathfrak{p}}(\varphi_i-\vartheta_i),v_{\mathfrak{p}}(\vartheta_i-\psi_i)\right\}+\frac{i}{n}\right\}\\
&= \min_{0\leqslant i\leqslant n-1}\left\{\min\left\{v_{\mathfrak{p}}(\varphi_i-\vartheta_i)+\frac{i}{n},v_{\mathfrak{p}}(\vartheta_i-\psi_i)+\frac{i}{n}\right\}\right\}\\
&= \min\left\{\min_{0\leqslant i\leqslant n-1}\left\{v_{\mathfrak{p}}(\varphi_i-\vartheta_i)+\frac{i}{n}\right\},\min_{0\leqslant i\leqslant n-1}\left\{v_{\mathfrak{p}}(\vartheta_i-\psi_i)+\frac{i}{n}\right\}\right\}.
\end{aligned}
$$

Thus $d(\varphi,\psi)\leqslant\max\{d(\varphi,\vartheta),d(\vartheta,\psi)\}$, *i.e.*, d satisfies the ultrametric inequality. It is clear that $d(\varphi,\psi)=0$ if and only if $\varphi(x)=\psi(x)$. The following result summarizes the properties of d.

Proposition 3.2.3. *Let $\varphi(x)$ and $\psi(x)$ be two polynomials from the set $\mathbf{E}_{n,j}$ of Eisenstein polynomials of degree n and discriminant $\mathfrak{p}^{n+j-1}$ over $\mathbf{k}$. Then $d(\varphi,\psi):=|\varphi(\beta)|=|\psi(\alpha)|$ where α (respectively β) is any root of $\varphi(x)$ (respectively $\psi(x)$) defines an ultrametric distance over $\mathbf{E}_{n,j}$. Furthermore, let $\varphi(x)$, ψ be two elements of $\mathbf{E}_{n,j}$, $\alpha=\alpha_1,\dots,\alpha_n$ the roots of $\varphi(x)$, and β one of the roots of $\psi(x)$ which is closest to α. Then*

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

3.3 Generating Polynomials

In this section, we construct a set of polynomials that generate all the extensions in $\mathbf{K}_{n,j}$.

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

$$\mathfrak{p}^l/\mathfrak{p}^m.$$

We denote by $\mathcal{R}^*_{l,m}$ the subset of those elements of $\mathcal{R}_{l,m}$ whose $v_{\mathfrak{p}}$-valuation is exactly l.

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

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

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 $(\omega_0, \ldots, \omega_{n-1}) \in \mathbf{k}^n$ satisfying

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

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

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

Lemma 3.3.1. *The polynomials $A_\omega(x)$ are Eisenstein polynomials of discriminant $\mathfrak{p}^{n+j-1}$.*

Proof. Since $l(i) \geqslant 1$ for all i, we have $v_\mathfrak{p}(\omega_i) \geqslant 1$ and (1) gives $v_\mathfrak{p}(\omega_0) = 1$. Thus, $A_\omega(x)$ is an Eisenstein polynomial.

Let $\varkappa$ be a root of $A_\omega(x)$. Since the discriminant of $A_\omega = \mathrm{N}_{\mathbf{k}(\varkappa)/\mathbf{k}}(A'_\omega(\varkappa))$, the second assertion is equivalent to

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

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

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

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

and for $i = b \neq 0$

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

If $b \neq 0$ then by Ore's conditions

$$v_\mathfrak{p}(n\varkappa^{n-1}) > v_\mathfrak{p}(b\omega_b\varkappa^{b-1}).$$

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

If $b = 0$, then for $1 \leqslant i \leqslant n-1$ we have $a = v_\mathfrak{p}(n)$, thus

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

and therefore $v_{\mathfrak{p}}(A'_\omega(\varkappa)) = 1 + v_{\mathfrak{p}}(n) - 1/n$ as required. □

Theorem 3.3.2 (Krasner). *Let c be an integer such that $c > 1+2a+2b/n$. 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 $r := |\mathfrak{p}^c|$ as ω runs through Ω.*

Proof. Lemma 3.3.1 proves that the polynomials A_ω are indeed elements of $\mathbf{E}_{n,j}$.

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

$$v_{\mathfrak{p}}(\omega_i - \omega'_i) + \frac{i}{n} \leqslant c - 1 + \frac{i}{n} < c$$

and thus by lemma 3.2.2, $d(A_\omega, A_{\omega'}) > r$ and by the ultrametric property of d the discs D_ω and $D_{\omega'}$ are disjoint.

Now, let φ be an element of $\mathbf{E}_{n,j}$ and write $\varphi(x) = x^n + \varphi_{n-1}x^{n-1} + \cdots + \varphi_0$. Since f is an Eisenstein polynomial, $v_{\mathfrak{p}}(\varphi_0) = 1$ and there exists $\omega_0 \in \mathcal{R}^*_{1,c}$ such that

$$\varphi_0 \equiv \omega_0 \bmod \mathfrak{p}^c.$$

By reasoning as in lemma 3.3.1, we find that $v_{\mathfrak{p}}(\varphi_i) \geqslant l(i)$ for all $i > 0$ and there exists ω_i satisfying (2) or (3) such that

$$\varphi_i \equiv \omega_i \bmod \mathfrak{p}^c.$$

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

$$v_{\mathfrak{p}}(\varphi_i - \omega_i) + \frac{i}{n} \geqslant c$$

which by lemma 3.2.2 proves the claim. □

Corollary 3.3.3. *Let ω be an element of Ω and let $\varkappa$ be a root of $A_\omega(x)$. Then the extension $\mathbf{k}(\varkappa)/\mathbf{k}$ is a totally ramified extension of degree n and discriminant $\mathfrak{p}^{n+j-1}$. Conversely, if $\mathbf{K}/\mathbf{k}$ is a totally ramified extension of degree n and discriminant $\mathfrak{p}^{n+j-1}$ then there exist $\omega \in \Omega$ and a root $\varkappa$ of $A_\omega(x)$ such that $\mathbf{K} = \mathbf{k}(\varkappa)$.*

Proof. The first claim is clear since the polynomials $A_\omega(x)$ belong to $\mathbf{E}_{n,j}$. For the second, let α be a prime element in $\mathbf{K}$ and denote its irreducible polynomial over $\mathbf{k}$

by $\varphi(x)$. We denote by $\alpha_1, \ldots, \alpha_n$ the roots of $\varphi(x)$. Let $\alpha \in \{\alpha_1, \ldots, \alpha_n\}$ and let $\Delta\varphi$ be the minimal distance between α and any other root of $\varphi(x)$. Then

$$|\varphi'(\alpha)| = \prod_{i=2}^{n} |\alpha - \alpha_i| \leqslant \Delta\varphi \left|\mathfrak{p}^{(n-2)/n}\right|$$

since the α_i are prime elements. But

$$|\varphi'(\alpha)| = \left|\mathfrak{p}^{(n+j-1)/n}\right|$$

and thus

$$\Delta\varphi \geqslant \left|\mathfrak{p}^{(j+1)/n}\right|.$$

Now let $\omega \in \Omega$ be such that $d(\varphi, A_\omega) \leqslant r = |\mathfrak{p}^c|$ where $c > 1+2a+2b/n = (n+2j)/n$ and let $\varkappa$ denote a root of A_ω such that $|\varkappa - \alpha|$ is minimal. Then we claim that $|\varkappa - \alpha| < \Delta\varphi$, since otherwise

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

This contradicts $|\mathfrak{p}^{(n+2j)/n}| > r$ by the particular choice of c. Hence $|\varkappa - \alpha| < \Delta\varphi$ and it follows by Krasner's lemma (proposition 1.3.1) that $\mathbf{K} = \mathbf{k}(\varkappa)$. $\square$

3.4 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 $\{A_\omega \mid \omega \in \Omega\}$. Nevertheless, for each extension, there are in general several polynomials A_ω that generate the same extension. Hence 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 by themselves, but will also be useful to get a more efficient algorithm for the computation of all totally ramified extensions of a given degree and discriminant (see section 3.8 for details). We also use them as a tool in the computation of canonical generating polynomials of degree p in section 3.6.

We will need the following lemma.

Lemma 3.4.1. *Let $t > j+1$ be an integer and let $s := \left|\mathfrak{p}^{(n+j-1+t)/n}\right|$. 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 $\mathfrak{P}\backslash\mathfrak{P}^2$ where $\mathfrak{P}$ is the prime ideal of some member of $\mathbf{K}_{n,j}$. Let μ be the map from $\Pi_{n,j}$ to $\mathbf{E}_{n,j}$ that sends a prime element to its minimal polynomial over $\mathbf{k}$.

Let $u = |\mathfrak{p}^{t/n}|$ and let α and β be two elements of $\Pi_{n,j}$ such that $|\alpha - \beta| \leqslant u$. Then α and β generate the same field $\mathbf{K} \in \mathbf{K}_{n,j}$ by Krasner's lemma (proposition 1.3.1). Observe that we have $d(\mu(\alpha), \mu(\beta)) \leqslant u \left|\mathfrak{p}^{(n+j-1)/n}\right| = s$ by the same reasoning as in the proof of corollary 3.3.3. Hence $\mu(D_\Pi(\alpha, u)) \subseteq D_{\mathbf{E}_{n,j}}(\mu(\alpha), s)$, 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 $f = \mu(\alpha)$. Then it is straightforward to prove, using the same methods, that $D_{\mathbf{E}_{n,j}}(\mu(\alpha), s) \subset \mu(D_\Pi(\alpha, u))$. Thus, $D_{\mathbf{E}_{n,j}}(\mu(\alpha), s) = \mu(D_\Pi(\alpha, u))$ for all $\alpha \in \Pi_{n,j}$.

Now, the map μ is clearly surjective and n-to-one. Furthermore, the inverse image of $\mu(\alpha)$ is the set of conjugates of α over $\mathbf{k}$, 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. $\square$

Theorem 3.4.2. *Let* $\mathbf{k}$ *be a finite extension of* $\mathbb{Q}_p$*, let* $\mathfrak{p}$ *be the prime ideal of* $\mathbf{k}$ *with* e *its ramification index, and let* q *be the number of elements in the residue field of* $\mathbf{k}$*. Let* $j = an + b$*, where* $0 \leqslant b < n$*, be an integer satisfying Ore's conditions. Then the number of totally ramified extensions of* $\mathbf{k}$ *of degree* n *and discriminant* $\mathfrak{p}^{n+j-1}$ *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 compute the number of elements in the closed disc $D_{\mathbf{E}_{n,j}}(r)$ of radius $|\mathfrak{p}^c|$ and then apply lemma 3.4.1 to obtain $\#\mathbf{K}_{n,j}$.

Lemma 3.4.3. *The number of polynomials* A_ω *where* $\omega \in \Omega$*, or equivalently by theorem 3.3.2 the number of disjoint closed discs of radius* $r := |\mathfrak{p}^c|$ *in* $\mathbf{E}_{n,j}$*, 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 $i \neq b$, the number of elements in $\mathcal{R}_{l(i),c}$ is $q^{c-l(i)}$ and the number of elements in $\mathcal{R}^*_{l(b),c}$ is $(q-1)\,q^{c-l(b)-1}$. So we have

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

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

$$\sum_{i=1}^{n-1} l(i) = n - 1 + \sum_{i=1}^{b-1} \max\{1 + a - v_\mathfrak{p}(i), 0\} + \sum_{i=b}^{n-1} \max\{a - v_\mathfrak{p}(i), 0\}.$$

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

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

Thus, using this formula, we find

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

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

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

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

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

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

Theorem 3.4.2 is proven by choosing t such that $n + j - 1 + t = nc$ and applying lemma 3.4.3 and lemma 3.4.1.

3.5 Tamely Ramified Extensions

In this section let $\mathbf{K}/\mathbf{k}$ be totally and tamely ramified, *i.e.*, p does not divide $n = [\mathbf{K} : \mathbf{k}]$. The description of totally and tamely ramified extensions of p-adic fields is well-known (see [Hasse, 1963, Chapter 16] or theorem 3.5.2 below). The aim of this section is to recover this description using the methods developed in the previous sections. Note first the following result the proof of which follows directly from proposition 3.1.1.

Proposition 3.5.1. *Let $\mathbf{K}/\mathbf{k}$ be a totally and tamely ramified extension of degree n. Then $j = 0$ and thus the discriminant of this extension is $\mathfrak{p}^{n-1}$, $a = b = 0$, and $c = 2$.*

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

Theorem 3.5.2. *Let ζ be a primitive $(q-1)$-th root of unity contained in $\mathbf{k}$, let g be the* gcd *of n and $q-1$, and let $m := n/g$. Then there are exactly n totally and tamely ramified extensions $\mathbf{K}/\mathbf{k}$ of degree n. Furthermore, these extensions can be split into g classes of m $\mathbf{k}$-isomorphic extensions, the extensions in a given class being generated over $\mathbf{k}$ by the roots of the polynomial*

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

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

Proof. We look at the set of generating polynomials defined in section 3.3. Proposition 3.5.1 tells us that $j = a = b = 0$, and that the smallest value for c is 2. We choose $\mathcal{R}^*_{1,2} := \{\zeta^i \pi \mid 0 \leqslant i \leqslant q-2\}$ 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 $1 \leqslant i \leqslant n-1$ 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 $1 \leqslant i \leqslant n-1$). Let α be such a root. Then it is clear that for any integer h, $\zeta^h \alpha$ generates the same extension. Furthermore, 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 $0 \leqslant r < g$. So in fact it is enough to consider only the polynomials $x^n + \zeta^r \pi$ with $0 \leqslant r \leqslant g-1$.

Now let $x^n + \zeta^r\pi$ and $x^n + \zeta^{r'}\pi$ be two such polynomials, with $0 \leqslant r, r' \leqslant g-1$ and $r \neq r'$, and let α (respectively α') be a root of $x^n+\zeta^r\pi$ (respectively $x^n+\zeta^{r'}\pi$). 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 not possible, 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 $\mathbf{k}$. Furthermore, the conjugates of α over $\mathbf{k}$ are $\alpha, \rho\alpha, \ldots, \rho^{n-1}\alpha$ 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 $\alpha, \rho^m\alpha = \zeta^{(q-1)/g}\alpha, \ldots, \rho^{(g-1)m}\alpha = \zeta^{(g-1)(q-1)/g}\alpha$ all generate the same field, whereas $\alpha, \rho\alpha, \ldots, \rho^{m-1}\alpha$ all generate different extensions. Thus, the roots of the polynomial $x^n + \zeta^r\pi$ generate m isomorphic but distinct 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 $\mathbf{k}$ by theorem 3.4.2, this proves that all the totally ramified extensions of degree n of $\mathbf{k}$ are obtained considering only these polynomials, and that any other polynomials are redundant. $\square$

Proposition 3.5.3. *Let $\mathbf{K}$ be a totally ramified extension of $\mathbf{k}$ of degree n and discriminant $\mathfrak{p}^{j+n-1}$, 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 $\mathbf{k}$ with discriminant $\mathfrak{p}^{n_0-1}$.*

Proof. By proposition 3.1.2, all the subfields of degree n_0 of $\mathbf{K}$, provided they exist, have discriminant $\mathfrak{p}^{n_0-1}$. Assume such a subfield $\mathbf{K}_0$ exists. Then $\operatorname{disc}_{\mathbf{K}/\mathbf{K}_0} = \mathfrak{P}_0^{p^s+j_1-1}$, where $j_1 = j = a(n_0p^s)+b$ and $\mathfrak{P}_0$ is the prime ideal of $\mathbf{K}$. Using theorem 3.4.2 we obtain

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

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 $\mathbf{k}$. Assume $\mathbf{K}_0$ and $\mathbf{K}_1$ are non-isomorphic subfields of degree n_0 over $\mathbf{k}$, generated by the polynomials

$$\varphi_0(x) = x^{n_0} + \zeta^{r_0}\pi \quad \text{and} \quad \varphi_1(x) = x^{n_0} + \zeta^{r_1}\pi$$

respectively (see theorem 3.5.2). Let $\varkappa_0$ be a root of φ_0, then

$$\psi(x) := -\frac{\varphi_1(\varkappa_0 x)}{\pi^{n_0}} = x^{n_0} - \zeta^{r_1-r_0}$$

has a root in $\mathbf{K}$. If ψ has a root in $\mathbf{k}$ then $\mathbf{K}_0 \cong \mathbf{K}_1$ which contradicts the assumption that $\mathbf{K}_0 \not\cong \mathbf{K}_1$, and if ψ has no root on $\mathbf{k}$ then the extension $\mathbf{K}/\mathbf{k}$ has inertia degree greater than 1, which contradicts the assumption that $\mathbf{K}/\mathbf{k}$ is totally ramified. $\square$

3.6 Extensions of Degree p

Let $\mathbf{k}$ be an extension of $\mathbb{Q}_p$ of degree ef with ramification index e, prime ideal $\mathfrak{p}$, and inertia degree f. Set $q := p^f$. In this section we present a canonical set of polynomials that generate all extensions of $\mathbf{k}$ of degree p. Note that similar polynomials have been given by Amano [1971], although our results are more explicit.

Let $j = ap + b$. By theorem 3.4.2 the number of extensions of $\mathbf{k}$ of degree p and discriminant $\mathfrak{p}^{n+j-1}$ is

$$\#\mathbf{K}_{p,j} = \begin{cases} pq^e & \text{if } b = 0 \\ p(q-1)q^a & \text{if } b \neq 0. \end{cases}$$

We will give a set of canonical polynomials for every possible value of $j = ap + b$. Let ζ be a $(q-1)$-th root of unity, and set $\mathcal{R} = (\rho_0, \ldots, \rho_{q-1}) = (0, 1, \zeta, \zeta^2, \ldots, \zeta^{q-2})$, then $\mathcal{R}$ is a multiplicative system of representatives of $\underline{\mathbf{k}}$ in $\mathbf{k}$.

First we will compute a set of canonical generating polynomials for pure extensions of degree p of a $\mathfrak{p}$-adic field that is, for the case $b = 0$. Secondly we give a set of canonical generating polynomials for extensions of degree p of discriminant $\mathfrak{p}^{p+ap+b-1}$ where $b \neq 0$ of a $\mathfrak{p}$-adic field. We use the notation from section 2.1.

Extensions of $\mathfrak{p}$-adic fields of discriminant $\mathfrak{p}^{p+pe-1}$

Theorem 3.6.1. *Let $L(0) := \{r \in \mathbb{Z} \mid 1 \leqslant r < pe/(p-1),\ p \nmid r\}$. Then each extension of degree p of $\mathbf{k}$ of discriminant $\mathfrak{p}^{p+ep-1}$ is generated by a root of exactly one of the polynomials of the form*

$$\varphi(x) = \begin{cases} x^p + \pi + \sum_{i \in L(0)} \rho_{c_i} \pi^{i+1} + k\delta\pi^{pe/(p-1)+1} & \text{if } \begin{array}{l}(p-1) \mid e \text{ and} \\ x^{p-1} + \underline{(p/\pi^e)} \text{ is reducible,}\end{array} \\ x^p + \pi + \sum_{i \in L(0)} \rho_{c_i} \pi^{i+1} & \text{otherwise,} \end{cases}$$

where δ is chosen such that $x^p - x + \underline{\delta}$ is irreducible over $\underline{\mathbf{k}}$ and $0 \leqslant k < p$. These extensions are Galois if and only if $(p-1) \mid e$ and $x^{p-1} + \underline{p/\pi^e}$ is reducible, i.e., if $\mathbf{k}$ contains the p-th roots of unity.

Lemma 3.6.2. *Let*

$$\varphi(x) = x^p + \pi + \sum_{i \in L(0)} \rho_{c_i} \pi^{i+1} + \pi^R \gamma$$

and

$$\psi(x) = x^p + \pi + \sum_{i \in L(0)} \rho_{d_i} \pi^{i+1} + \pi^R \delta.$$

where ρ_{c_i}, $\rho_{d_i} \in \mathcal{R}$, $R \geqslant pe/(p-1)$, and γ, $\delta \in \mathcal{O}_{\mathbf{k}}$. Let α be a zero of f and β be a zero of g in an algebraic closure of $\mathbf{k}$. If $c_i \neq d_i$ for some $i \in L(0)$ then $\mathbf{k}(\alpha) \not\cong \mathbf{k}(\beta)$.

Proof. We will use Panayi's root-finding algorithm (algorithm 2.1.4) to show that $\psi(x)$ does not have any roots over $\mathbf{k}(\alpha)$. As $\psi(x) \equiv x^p \bmod (\pi)$ we set $\psi_1(x) := \psi(\alpha x)$. Then

$$\begin{aligned}
\psi_1(x) &= \alpha^p x^p + \pi + \sum_{i \in L(0)} \rho_{d_i} \pi^{i+1} + \pi^R \delta \\
&= (-\pi - \sum_{i \in L(0)} \rho_{c_i} \pi^{i+1} - \pi^R \gamma) x^p + \pi + \sum_{i \in L(0)} \rho_{d_i} \pi^{i+1} + \pi^R \delta \\
&\equiv \pi(-x^p + 1)
\end{aligned}$$

Hence $\psi_1^{\#}(x) = \psi_1(x)/\pi \equiv -x^p + 1$ and we set $\psi_2(x) := g_1^{\#}(\alpha x + 1)$.

Let $\underline{\beta_i}$ be a root of $\underline{g_{i+2}^{\#}}$. Let $2 \leqslant r < pe/(p-1)$. Assume that the root-finding algorithm does not terminate with $\deg \underline{\psi_j^{\#}} = 0$ for some $2 \leqslant j \leqslant r$ and that there is $t < r < pe/(p-1)$ with $\beta_t \not\equiv 0 \bmod (\alpha)$. After r iterations of the root-finding algorithm we have

$$\begin{aligned}
\psi_{r+1}(x) &= \Big(-1 - \sum_{i \in L(0)} \rho_{c_{i+1}} \pi^i - \rho_{c_{a+2}} \pi^{a+1}\Big)(\alpha^r x + \beta_{r-1}\alpha^{r-1} + \cdots + \beta_t \alpha^t + 1)^p \\
&\quad + 1 + \sum_{i \in L(0)} \rho_{d_{i+1}} \pi^i + \rho_{d_{a+1}} \pi^{a+1} + \pi^{R-1}\delta \\
&\equiv -\alpha^{pr} x^p - p\alpha^r x - p\beta_t \alpha^t + \sum_{i \in L(0), i \geqslant t} (\rho_{d_{i+1}} - \rho_{c_{i+1}}) \pi^i.
\end{aligned}$$

The minimal valuation of the coefficients of $\psi_{r+1}(x)$ is either $v_\alpha(\alpha^{pr}) = pr$ or $v_\alpha(p\beta_t\alpha^t) = pe + t$. As $\gcd(p,t) = 1$ and $t < pe/(p-1)$ there exists $r \in \mathbb{N}$ such that the polynomial $\underline{g_{r+1}^{\#}}(x)$ is constant. Thus the root-finding algorithm terminates with the conclusion that $\psi(x)$ is irreducible over $\mathbf{k}(\alpha)$. $\square$

It is obvious that a pure extension can be Galois only if $\mathbf{k}$ contains the p-th roots of unity.

Lemma 3.6.3. *Assume that $\varphi(x) := x^{p-1} + c \in \mathbb{F}_q[x]$ has $p-1$ roots in $\mathbb{F}_q$. Then there exists $d \in \mathbb{F}_q$ such that $\psi_k(x) := x^p + cx - kd \in \mathbb{F}_q[x]$ is irreducible for all $1 \leqslant k < p$.*

Proof. Let $h(x) = x^p + cx \in \mathbb{F}_q[x]$. As $\varphi(x)$ splits completely over $\mathbb{F}_q$, there exists $d \in \mathbb{F}_q \setminus h(\mathbb{F}_q)$. Now $\psi_1(x) = x^p + cx - d$ is irreducible. It follows that

$$k\psi_1(x) = kx^p + ckx - kd = (kx)^p + c(kx) - kd$$

is irreducible. Replacing kx by y we find that $\psi_k(y) = y^p + cy - kd$ is irreducible over $\mathbb{F}_q$. $\square$

Lemma 3.6.4. *Assume $\mathbf{k}$ contains the p-th roots of unity and let $t = pe/(p-1)$. Then there exists $\delta \in \mathcal{O}_{\mathbf{k}}$ such that*

$$\varphi(x) = x^p + \pi + \sum_{i \in L(0)} \rho_{c_i} \pi^{i+1} + k\delta\pi^{t+1} \in \mathcal{O}_{\mathbf{k}}[x]$$

and

$$\psi(x) = x^p + \pi + \sum_{i \in L(0)} \rho_{c_i} \pi^{i+1} + l\delta\pi^{t+1} \in \mathcal{O}_{\mathbf{k}}[x]$$

generate non-isomorphic extensions over $\mathbf{k}$ if $l \neq k$.

Proof. Let α be a root of $\varphi(x)$. We set $\varphi_1(x) := \varphi(\alpha x)$ and $\varphi_2(x) := \varphi_1^{\#}(\alpha x + 1)$. After $t+1$ iterations of the root-finding algorithm we obtain $\varphi_{2+t}(x) \equiv -\alpha^{tp}x^p - p\alpha^t x + (l-k)\delta\pi^t$. By lemma 3.6.3 there exists $\delta \in \mathcal{O}_{\mathbf{k}}$ such that $\underline{\varphi_{2+t}^{\#}(x)}$ is irreducible for all $1 \leqslant k < p$ and all $1 \leqslant l < p$ with $k \neq l$. Therefore $\psi(x)$ has no root in $\mathbf{k}(\alpha)$. Thus $\varphi(x)$ and $\psi(x)$ generate non-isomorphic extensions over $\mathbf{k}$. $\square$

Proof of theorem 3.6.1. We will show that the number of extensions given by the polynomials $\varphi(x)$ is greater or equal to the number of extensions given by theorem 3.4.2. The number of elements in $L(0)$ is

$$\#L(0) = \left\lfloor \frac{pe}{p-1} \right\rfloor - \left\lfloor \frac{pe}{p(p-1)} \right\rfloor = e + \left\lfloor \frac{e}{p-1} \right\rfloor - \left\lfloor \frac{e}{p-1} \right\rfloor = e.$$

By lemma 3.6.2 the roots of two polynomials generate non-isomorphic extensions if the coefficients ρ_{c_i} differ for at least one $i \in L(0)$. For every i we have the choice among p^f values for ρ_{c_i}. This gives q^e polynomials generating non-isomorphic extensions.

If $\mathbf{k}$ does not contain the p-th roots of unity then an extension generated by a root α of a polynomial $\varphi(x)$ does not contain any of the other roots of $\varphi(x)$. Hence the roots of each polynomial give p distinct extensions of $\mathbf{k}$. Thus our set of polynomials generates all pq^e extensions.

If $\mathbf{k}$ contains the p-th roots of unity then lemma 3.6.4 gives us $p-1$ additional extensions for each of the polynomials from lemma 3.6.2. Thus our set of polynomials generates all pq^e extensions. □

Extensions of $\mathfrak{p}$-adic fields of discriminant $\mathfrak{p}^{p+ap+b-1}$, $b \neq 0$

Theorem 3.6.5. *Let $L(0) := \{r \in \mathbb{Z} \mid 1 \leqslant r < (ap+b)/(p-1),\, p \nmid (b+r)\}$ and if $(p-1) \mid (a+b)$ set $t := a + (a+b)/(p-1)$. Each extension of degree p of $\mathbf{k}$ of discriminant $\mathfrak{p}^{p+ap+b-1}$ with $b \neq 0$ is generated by a root of exactly one of the polynomials of the form*

$$\varphi(x) = \begin{cases} x^p + \zeta^s\pi^{a+1}x^b + \pi + \sum_{i\in L(0)} \rho_{c_i}\pi^{i+1} + k\delta\pi^{t+1} & \text{if } \begin{cases} (p-1) \mid (a+b) \text{ and} \\ x^{p-1} + (-1)^{ap+1}\underline{\zeta^s b} \\ \text{is reducible,} \end{cases} \\ x^p + \zeta^s\pi^{a+1}x^b + \pi + \sum_{i\in L(0)} \rho_{c_i}\pi^{i+1} & \text{otherwise,} \end{cases}$$

where $\rho \in \mathcal{R}$ and δ is chosen such that $x^p + (-1)^{ap+1}\underline{\zeta^s b}x + \underline{\delta}$ is irreducible in $\underline{\mathbf{k}}$ and $0 \leqslant k < p$. These extensions are Galois if and only if $(p-1) \mid (a+b)$ and $x^{p-1} - \underline{\zeta^s b} \in \underline{\mathbf{k}}[x]$ is reducible.

Lemma 3.6.6. *Let*

$$\varphi(x) = x^p + \zeta^s\pi^{a+1}x^b + \pi + \gamma\pi^2 \in \mathcal{O}_{\mathbf{k}}[t]$$

and

$$\psi(x) = x^p + \zeta^t\pi^{a+1}x^b + \pi + \delta\pi^2 \in \mathcal{O}_{\mathbf{k}}[t]$$

with $\gamma, \delta \in \mathcal{O}_{\mathbf{k}}$. If $s \neq t$ then the roots of $\varphi(x)$ and $\psi(x)$ generate non-isomorphic extensions of $\mathbf{k}$.

Proof. Let α be a root of $\varphi(x)$. Then $\alpha^p/\pi = -\zeta^s\pi^a\alpha^r - 1 - \gamma\pi$. We use Panayi's root-finding algorithm to show that $\psi(x)$ has no root over $\mathbf{k}(\alpha)$. As before we get $\psi_1(x) := \psi(\alpha x) \equiv \pi(-x^p + 1)$. Therefore we set

$$\psi_2(x) := \psi_1^{\#}(\alpha x+1) = (-\zeta^s\pi^a\alpha^b - 1 - \gamma\pi)(\alpha x+1)^p + \zeta^t\pi^a\alpha^b(\alpha x+1)^b + 1 + \delta\pi.$$

Let $2 \leqslant r \leqslant e$. Let $\underline{\beta_i} \in \mathcal{R}$ be a root of $\underline{\psi_i^{\#}}(x)$. Assume that the root-finding algorithm does not terminate with $\deg \underline{\psi_j^{\#}} = 0$ for some $2 \leqslant j \leqslant r$ and assume that there exists r such that $t < r < pe/(p-1)$ with $\beta_t \not\equiv 0 \bmod (\alpha)$. After r iterations of the root-finding algorithm we have

$$\begin{aligned}\psi_{r+1}(x) \;=\; & (-\zeta^s\pi^a\alpha^b - 1 - \gamma\pi)(\alpha^r x + \beta_{r-1}\alpha^{r-1} + \cdots + \beta_u\alpha^u + 0 + \cdots + 0 + 1)^p \\ & + \zeta^t\pi^a\alpha^b(\alpha^r x + \beta_{r-1}\alpha^{r-1} + \cdots + \beta_u\alpha^u + 0 + \cdots + 0 + 1)^b + 1 + \delta\pi.\end{aligned}$$

Because $r \leqslant e$, $v_\alpha(p) = pe$, and $a < e$, the minimal valuation of the coefficients of $\psi_{r+1}(x)$ is either $v_\alpha(-\alpha^{pr}) = pr$ or $v_\alpha(\pi^a\alpha^b) = pa + b$. Hence the root-finding algorithm terminates with $\psi_{r+1}(x) \equiv (\zeta^t - \zeta^s)\pi^a\alpha^b$ for some r in the range $2 \leqslant r \leqslant e$. $\square$

Lemma 3.6.7. *Let*

$$\varphi(x) = x^p + \zeta^s\pi^{a+1}x^b + \pi + \sum_{i\in L(0)} \rho_{c_i}\pi^{i+1} + \pi^R\gamma \in \mathcal{O}_{\mathbf{k}}[t]$$

and

$$\psi(x) = x^p + \zeta^s\pi^{a+1}x^b + \pi + \sum_{i\in L(0)} \rho_{d_i}\pi^{i+1} + \pi^R\delta \in \mathcal{O}_{\mathbf{k}}[t]$$

with ρ_{c_i}, $\rho_{d_i} \in \mathcal{R}$, $R \geqslant a + a + b/(p-1)$ and γ, $\delta \in \mathcal{O}_{\mathbf{k}}$. Let α be a zero of $\varphi(x)$ and β be a zero of $\psi(x)$ in a fixed algebraic closure of $\mathbf{k}$. If $c_i \neq d_i$ for some $i \in L(0)$ then $\mathbf{k}(\alpha) \not\cong \mathbf{k}(\beta)$.

Proof. We use Panayi's root-finding algorithm to show that $\psi(x)$ does not have any roots over $\mathbf{k}(\alpha)$. As $\psi(x) \equiv x^p \bmod (\pi)$, we get $\psi_1(x) := \psi(\alpha x)$. Now $\psi_1^{\#}(x) \equiv -x^p + 1$ and we set $\psi_2(x) := \psi_1^{\#}(\alpha x + 1)$.

Let $\underline{\beta_i}$ be a root of $\underline{\psi_{i+1}^{\#}}(x)$. Assume that the root-finding algorithm does not terminate earlier with $\deg \underline{\psi_j^{\#}} = 0$ for some $j \leqslant r$. After r iterations we have

$$
\begin{aligned}
\psi_{r+1}(x) &= \Big(-\zeta^s\pi^a\alpha^b - 1 - \sum_{i\in L(0)} \rho_{c_{i+1}}\pi^i - \rho_{c_{a+2}}\pi^{a+1}\Big) \\
&\quad \cdot (\alpha^r x + \beta_{r-1}\alpha^{r-1} + \cdots + \beta_t\alpha^t + 1)^p \\
&\quad + \zeta^s\pi^a\alpha^b(\alpha^r x + \beta_{r-1}\alpha^{r-1} + \cdots + \beta_t\alpha^t + 1)^b + 1 \\
&\quad + \sum_{i\in L(0)} \rho_{d_{i+1}}\pi^i + \rho_{d_{a+1}}\pi^{a+1} \\
&\equiv -\alpha^{pr}x^p - p\alpha^r x - p\beta_t\alpha^t - \sum_{i\in L(0)} \rho_{c_{i+1}}\pi^i(\beta_t\alpha^t)^p - (\beta_t\alpha^t)^p \\
&\quad + \zeta^s\pi^a\alpha^b b\alpha^r x + \zeta^s\pi^a\alpha^b b\beta_t\alpha^t + \sum_{i\in L(0)} (\rho_{d_{i+1}} - \rho_{c_{i+1}})\pi^i
\end{aligned}
$$

with $\beta_t \not\equiv 0 \bmod (\alpha)$. The minimal valuation of the terms of $\psi_{r+1}(x)$ is

$$
v_\alpha(\zeta^s\pi^a\alpha^b b\beta_t\alpha^t) = pa + b + t
$$

or $v_\alpha(\alpha^{pr}) = pr$. By the choice of $L(0)$ we have $p \nmid (pa + b + t)$. Therefore the root-finding algorithm terminates with $\psi_r(x) \equiv \zeta^s\pi^a\alpha^b b\beta_t\alpha^t$ for some $r \in \mathbb{N}$. $\square$

Lemma 3.6.8. *Let*

$$
\varphi(x) = x^p + \zeta^s\pi^{a+1}x^b + \sum_{i\in L(0)} \rho_{c_i}\pi^{i+1} + \pi \in \mathcal{O}_{\mathbf{k}}[x]
$$

with $\varphi(\alpha) = 0$ *for some* $\alpha \in \overline{\mathbf{k}}$*. Then* $\mathbf{k}(\alpha)/\mathbf{k}$ *is Galois if and only if* $a + b \equiv 0 \bmod (p-1)$ *and* $x^{p-1} + (-1)^{ap+1}\underline{\zeta^s b}$ *is reducible over* $\underline{\mathbf{k}}$*.*

Proof. We will show that $\varphi(x)$ splits completely over $\mathbf{k}(\alpha)$ if and only if the conditions above are fulfilled. Using the root-finding algorithm (algorithm 2.1.4) we set $\varphi_1(x) := \varphi(\alpha x)$ and $\varphi_2(x) := \varphi_1^{\#}(\alpha x + 1)$, *i.e.*

$$
\begin{aligned}
\varphi_2(x) &= \Big(-\zeta^s\pi^a\alpha^b - 1 - \sum_{i\in L(0)} \rho_{c_i}\pi^i\Big)(\alpha x + 1)^p + \zeta^s\pi^a\alpha^b(\alpha x + 1)^b + 1 + \sum_{i\in L(0)} \rho_{c_i}\pi^i \\
&\equiv x(-\alpha^p x^{p-1} + \zeta^s\pi^a\alpha^{b+1}b).
\end{aligned}
$$

After $r+1$ iterations we get

$$
\varphi_{r+1}(x) \equiv \begin{cases} -\alpha^{rp}x^p & \text{if } rp < pa + b + r, \\ x(-\alpha^{rp}x^{p-1} + \zeta^s\pi^a\alpha^{b+r}b) & \text{if } rp = pa + b + r, \\ \zeta^s\pi^a\alpha^{b+1}bx & \text{if } rp > pa + b + r \text{ and } (p-1) \nmid (a+b). \end{cases}
$$

In the third case $\underline{\varphi_{r+1}^{\#}}(x)$ is linear and therefore $\varphi(x)$ has only one root.

In the second case

$$\varphi_{r+1}(x) \equiv -\alpha^{rp}x^p + \zeta^s\pi^a\alpha^{b+r}bx \equiv -\alpha^{rp}x^p + \zeta^s(-\alpha)^{ap} + \alpha^{b+r}$$

thus $\varphi^{\#}_{r+1}(x) \equiv -x^{p-1} + (-1)^{ap}\zeta^s b \bmod (\alpha)$. If $\underline{\varphi^{\#}_{r+1}}(x)$ has p roots over $\underline{\mathbf{k}}$ for every root $\underline{\beta}$ of $\underline{\varphi^{\#}_{r+1}}(x)$ we get

$$\varphi_{r+2}(x) = \varphi_{r+1}(\alpha x+\beta) \equiv -\alpha^{(r+1)p}x^p + (-1)^{ap}\alpha^{r+1}\beta\zeta^s\pi^a\alpha^b + (-1)^{ap}\alpha^{r+1}b\beta^b\zeta^s\pi^a\alpha^b x.$$

But $rp+p > r+1+pa+b$; thus $\underline{\varphi^{\#}_{r+2}}(x)$ is linear and $\varphi(x)$ has as many distinct roots as $\underline{\varphi^{\#}_{r+1}}(x)$. $\square$

Lemma 3.6.9. *Assume that $a+b \equiv 0 \bmod (p-1)$ and $x^{p-1}+(-1)^{ap+1}\underline{\zeta^s b}$ is reducible over $\underline{\mathbf{k}}$. Then there exists $\delta \in \mathcal{O}_{\mathbf{k}}$ such that*

$$\varphi(x) = x^p + \zeta^s\pi^{a+1}x^b + \sum_{i\in L(0)} \rho_{c_i}\pi^{i+1} + k\delta\pi^{t+1} \in \mathcal{O}_{\mathbf{k}}[x]$$

and

$$\psi(x) = x^p + \zeta^s\pi^{a+1}x^b + \sum_{i\in L(0)} \rho_{c_i}\pi^{i+1} + l\delta\pi^{t+1} \in \mathcal{O}_{\mathbf{k}}[x]$$

(where $t = a+(a+b)/(p-1)$) generate non-isomorphic extensions over $\mathbf{k}$ if $l \neq k$.

Proof. Let α be a root of $\varphi(x)$. Using the root finding algorithm we set $\varphi_1(x) := \varphi(\alpha x)$ and $\varphi_2(x) := \varphi_1^{\#}(\alpha x+1)$. We get $\varphi_{t+1}(x) \equiv -\alpha^{tp}x^p + \zeta^s\pi^a\alpha^{b+t}bx + (k-l)\delta\pi^t$ hence $\underline{\varphi^{\#}_{t+1}(x)} = x^p + (-1)^{ap+1}\zeta^s bx + (k-l)\delta$. By lemma 3.6.3 there exists $\delta \in \mathcal{O}_{\mathbf{k}}$ such that $\underline{\varphi^{\#}_{t+1}(x)}$ is irreducible. $\square$

Proof of theorem 3.6.5. If $(p-1) \nmid (a+b)$ then

$$\begin{aligned}\#L(0) &= a + \left\lfloor\frac{a+b}{p-1}\right\rfloor - \left\lfloor\frac{a+b}{p} + \frac{a+b}{p(p-1)}\right\rfloor - \left\lfloor\frac{b}{p}\right\rfloor \\ &= a + \left\lfloor\frac{a+b-1}{p-1}\right\rfloor - \left\lfloor\frac{a(p-1)+a+b(p-1)+b}{p(p-1)}\right\rfloor = a.\end{aligned}$$

If $(p-1) \mid (a+b)$ then

$$\begin{aligned}\#L(0) &= a + \frac{a+b}{p-1} - 1 - \left\lfloor\frac{a+b}{p} + \frac{a+b}{p(p-1)} - 1\right\rfloor - \left\lfloor\frac{b}{p}\right\rfloor \\ &= a + \frac{a+b-1}{p-1} - \left\lfloor\frac{a+b-1}{p-1}\right\rfloor = a.\end{aligned}$$

Using lemma 3.6.6 we get $p^f - 1$ sets of generating polynomials. By lemma 3.6.7 each of these sets contains p^{fa} polynomials that generate non-isomorphic fields. Now either the roots of one of the polynomials generate p distinct extensions or else the extension generated by any root is cyclic. In the latter case we have $p-1$ additional polynomials generating one extension each by lemma 3.6.9. Thus we obtain $(p^f - 1)p^{af+1}$ distinct extensions. □

Corollary 3.6.10. *Let* $\mathbf{k}$ *be an extension of* $\mathbb{Q}_p$ *of degree* n*. The number of Galois extensions of* $\mathbf{k}$ *of degree* p *and discriminant* $\mathfrak{p}^{p+ap+b-1}$ *is*

$$p \cdot \frac{p^n - 1}{p - 1}.$$

Proof. Let $\varphi(x)$ as in theorem 3.6.5. We denote the inertia degree and the ramification index of $\mathbf{k}$ by f and e respectively. The number of values of s s for which $x^{p-1} - \zeta^s$ is reducible is $(p^f - 1)/(p - 1)$. By Ore's Conditions $0 \leqslant a < e$. For every a there is exactly one b with $1 \leqslant b < p$ such that $(p - 1) \mid (a + b)$. For every a the set $L(0)$ contains a elements. This gives p^{fa} combinations of values of c_i, $i \in L(0)$. We have p choices for k. Thus the number of polynomials $\varphi(x)$ generating Galois extensions is

$$p \cdot \frac{p^f - 1}{p - 1} \cdot \sum_{a=0}^{e-1} p^{fa} = p \cdot \frac{p^f - 1}{p - 1} \cdot \frac{p^{fe} - 1}{p^f - 1} = p \cdot \frac{p^n - 1}{p - 1}.$$

□

3.7 Extensions of Degree p^m

Let $j = ap + b$. By theorem 3.4.2 the number of extensions of $\mathbf{k}$ of degree $n = p^m$ and discriminant $\mathfrak{p}^{p^m + emp^m - 1}$ is

$$\#\mathbf{k}_{p^m + emp^m - 1} = p^m q^{e \frac{p^m - 1}{p - 1}}$$

In the case of extensions of degree p^m with $m > 1$ we only give a set of polynomials generating independent extensions (but not – as before for extensions of degree p – a set of polynomials that give all extensions).

Lemma 3.7.1. *Let* p *be a prime number, let* $m \in \mathbb{N}$*, and let* $a < p^m$ *with* $p \nmid a$*. If* $1 \leqslant r \leqslant p^m - 1$ *then*

$$v_p\left(\binom{ap^m}{r}\right) = m - v_p(r).$$

Proof. For any $1 \leqslant s \leqslant p^m - 1$ we have $v_p\left(\frac{ap^m - s}{s}\right) = 0$. Hence

$$\begin{aligned}
v_p\left(\binom{ap^m}{r} r\right) &= v_p\left(\frac{(ap^m)!r}{r!(ap^m - r)!)}\right) = v_p\left(\frac{ap^m}{(r-1)!(ap^m - r)!)}\right) \\
&= v_p\left(\frac{ap^m(ap^m-1)\cdots(ap^m - r + 1)}{(r-1)(r-2)\cdots 1}\right) \\
&= m + v_p\left(\frac{ap^m - (r-1)}{r-1}\cdots\frac{ap^m - 1}{1}\right) = m.
\end{aligned}$$

□

Extensions of discriminant $\mathfrak{p}^{p^m + emp^m - 1}$

Proposition 3.7.2. *Let* $\mathbf{k}$ *be a* $\mathfrak{p}$*-adic field. Set*

$$\begin{aligned}
L(0) &:= \left\{ l \in \mathbb{Z} \;\middle|\; 1 \leqslant l \leqslant \frac{pe}{p-1} \text{ or } ep^{m-1} < l \leqslant \frac{ep^m}{p-1}, \text{ and } p \nmid l \right\}, \\
L(i) &:= \left\{ l \in \mathbb{Z} \;\middle|\; \begin{array}{l} em - ev_p(i) \leqslant l < em \text{ and } p^{m-h+1} \nmid i \text{ if} \\ \frac{ep^h}{p-1} < \frac{i}{p^{m-h}} + p^h(l - eh) \leqslant \frac{ep^{h+1}}{p-1} \text{ with } 1 \leqslant h \leqslant m-1 \end{array} \right\}
\end{aligned}$$

for $1 \leqslant i \leqslant p^m - 1$*. Let*

$$\varphi(x) = x^{p^m} + \sum_{i=1}^{p^{m-1}-1} x^i \sum_{l \in L(i)} \rho_{c_{i,l}} \pi^{l+1} + \sum_{l \in L(0)} \rho_{c_{0,l}} \pi^{l+1} + \pi$$

and

$$\psi(x) = x^{p^m} + \sum_{i=1}^{p^{m-1}-1} x^i \sum_{l \in L(i)} \rho_{d_{i,l}} \pi^{l+1} + \sum_{l \in L(0)} \rho_{d_{0,l}} \pi^{l+1} + \pi.$$

Assume $c_{i,l} \neq d_{i,l}$ *for some* $0 \leqslant i \leqslant p^{m-1} - 1$ *and some* $l \in L(i)$*. Let* $\alpha \in \overline{\mathbf{k}}$ *and* $\beta \in \overline{\mathbf{k}}$ *be roots of* $\varphi(x)$ *respectively* $\psi(x)$*. Then* $\mathbf{k}(\alpha) \ncong \mathbf{k}(\beta)$*.*

Note that $L(i) = \varnothing$ if $p \nmid i$.

Proof. We use Panayi's root-finding algorithm (algorithm 2.1.4) to prove that $\psi(x)$ does not have any roots over $\mathbf{k}(\alpha)$. As in the proofs of lemmas 3.6.2 and 3.6.7, we get

$$
\begin{aligned}
\psi_1^{\#}(x) &= \left(-\sum_{i=1}^{p^{m-1}-1} \alpha^{ip} \sum_{l\in L(i)} \rho_{c_{i,l}}\pi^l - \sum_{l\in L(0)} \rho_{c_{0,l}}\pi^l + 1\right) x^{p^m} \\
&\quad + \sum_{i=1}^{p^{m-1}-1} \alpha^{ip} x^{ip} \sum_{l\in L(i)} \rho_{d_{i,l}}\pi^l + \sum_{l\in L(0)} \rho_{d_{0,l}}\pi^l + 1.
\end{aligned}
$$

We denote by β_s a lift of a root of $\underline{\psi_{s+1}^{\#}}(x)$ to $\mathbf{k}(\alpha)$. Let t be the smallest integer such that $\beta_t \not\equiv 0 \bmod (\alpha)$ and let $r \leqslant ep^m/(p-1)$. Then

$$
\begin{aligned}
\psi_{r+1}(x) &= \left(-\sum_{i=1}^{p^{m-1}-1} \alpha^{ip} \sum_{l\in L(i)} \rho_{c_{i,l}}\pi^l - \sum_{l\in L(0)} \rho_{c_{0,l}}\pi^l - 1\right) \\
&\quad \cdot (\alpha^r x + \alpha^{r-1}\beta_{r-1} + \cdots + \alpha^t\beta_t + 0 + \cdots + 0 + 1)^{p^m} \\
&\quad + \sum_{i=1}^{p^m-1} \alpha^i (\alpha^r x + \alpha^{r-1}\beta_{r-1} + \cdots + \alpha^t\beta_t + 0 + \cdots + 0 + 1)^i \sum_{l\in L(i)} \rho_{d_{i,l}}\pi^l \\
&\quad + \sum_{l\in L(0)} \rho_{d_{0,l}}\pi^l + 1.
\end{aligned}
$$

Again we assume that the root-finding algorithm does not terminate earlier with $\deg\big(\underline{\psi_s^{\#}}(x)\big) = 0$ for $s < r$. It will become clear presently why the root-finding algorithm cannot terminate with $\deg\big(\underline{\psi_s^{\#}}(x)\big) = 1$ under the condition $r \leqslant ep^m/(p-1)$.

Consider the term $(\alpha^r x + 1)^{p^m}$. For every r the non-constant term with coefficient of lowest exponential valuation is one of

$$
\alpha^{rp^m} x^{p^m}, \ldots, p^h \alpha^{rp^{m-h}} x^{p^{m-h}}, \ldots, p^m \alpha^r x.
$$

The exponential valuations of the coefficients of these terms are

$$
v_\alpha(\alpha^{rp^m}) = rp^m, \ldots, v_\alpha(p^h\alpha^{rp^{m-h}}) = ehp^m + rp^{m-h}, \ldots, v_\alpha(p^m\alpha^r) = emp^m + r.
$$

We find that if $r > ep^{h+1}/(p-1)$ then

$$
hep^m + rp^{m-h} > (h+1)ep^m + rp^{m-h-1}.
$$

Thus for $ep^h/(p-1) < r \leqslant ep^{h+1}/(p-1)$ the valuation of the coefficient of the term $p^h\alpha^{rp^{m-h}}$ is lower than the valuations of the coefficients of any other non-constant term of $(\alpha^r x + 1)^{p^m}$. Therefore the degree of $\big((\alpha^r x + 1)^{p^m}\big)^{\#}$ is 1 if $r > ep^m/(p-1)$.

Consider the term $\alpha^i(\alpha^r x+1)^i\pi^{em-v_\mathfrak{p}(i)}$. By lemma 3.7.1 for every r the non-constant term with coefficient of lowest exponential valuation is of the form

$$\alpha^i p^g \alpha^{rp^{v_p(i)-g}} x^{p^{v_p(i)-g}} \pi^{em-ev_p(i)}$$

with $1 \leqslant g \leqslant v_p(i)$. The valuations of these terms are

$$v_\alpha(\alpha^i p^g \alpha^{rp^{v_p(i)-g}} x^{p^{v_p(i)-g}} \pi^{em-ev_p(i)}) = i + p^m(em - ev_p(i) + eg) + rp^{v_p(i)-g}.$$

If $r > ep^{m-v_p(i)+g+1}/(p-1)$ then

$$i + p^m(em - ev_p(i) + eg) + rp^{v_p(i)-g} > i + p^m(em - ev_p(i) + e(g+1)) + rp^{v_p(i)-(g+1)}.$$

Thus for $ep^{m-v_p(i)+g}/(p-1) < r \leqslant ep^{m-v_p(i)+g+1}/(p-1)$ the valuation of the coefficient of the term $\alpha^i p^g \alpha^{rp^{v_p(i)-g}} x^{p^{v_p(i)-g}} \pi^{em-ev_p(i)}$ is lower than the valuations of the coefficients of any other non-constant term of $\alpha^i(\alpha^r x+1)^i\pi^{em-v_\mathfrak{p}(i)}$.

We compare the non-constant terms with minimal valuation from $(\alpha^r x+1)^{p^m}$ and $\alpha^i(\alpha^r x+1)^i\pi^{em-v_\mathfrak{p}(i)}$ for a given $ep/(p-1) < r \leqslant ep^m/(p-1)$. Setting $h := m - v_p(i) + g$, we obtain

$$\begin{aligned} v_\alpha(p^h\alpha^{rp^{m-h}}) &= ehp^m + rp^{m-h} \\ &= e(m - v_p(i) + g)p^m + rp^{m-m+v_p(i)-g} \\ &< i + e(m - v_p(i) + g)p^m + rp^{v_p(i)-g} \\ &= v_\alpha(\alpha^i p^g \alpha^{rp^{v_p(i)-g}} x^{p^{v_p(i)-g}} \pi^{em-ev_p(i)}). \end{aligned}$$

Hence the non-constant term relevant in the root-finding algorithm is always of the form $p^h\left(\alpha^r x\right)^{p^{m-h}}$.

In step r where $ep^h/(p-1) < r \leqslant ep^{h+1}/(p-1)$ for some $1 \leqslant h \leqslant m-1$ we get $\beta_r \neq 0$ only if $v_\alpha(p^h\alpha^{rp^{m-h}}) = v_\alpha(\alpha^i + \pi^l)$ for some $1 \leqslant i \leqslant p^m - 1$ and $l \in L(i)$. It follows that

$$v_\alpha(p^h\alpha^{rp^{m-h}}) = ehp^m + rp^{m-h} = i + lp^m = v_\alpha(\alpha^i + \pi^l);$$

hence

$$\frac{ep^h}{p-1} < r = \frac{i}{p^{m-h}} + p^h(l - eh) \leqslant \frac{ep^{h+1}}{p-1}.$$

It is obvious that $p \mid r$ if and only if $p^{m-h+1} \mid i$.

Assume that $v_p(i) = m - h$; then $p \nmid r$. Set $s := ip^{-v_p(i)}$ and $d := l + v_p(i) - m$. We obtain

$$\frac{ep^h}{p-1} < r = s + p^h d \leqslant \frac{ep^{h+1}}{p-1}$$

and as $i < p^m$ we have $1 \leqslant i < p^h$, $p \nmid i$, and $0 \leqslant d < ev_p(i)$. Therefore

$$s + p^h d \leqslant p^h - 1 + p^h(ev_p(i) - 1) = p^h ev_p(i) - 1.$$

If $v_p(i) > 1$ we have $p^h ev_p(i) - 1 \geqslant ep^{h+1}/(p-1)$. Thus for every r with $ep^h/(p-1) < r \leqslant ep^{h+1}/(p-1)$ and $p \nmid r$ there exist $1 \leqslant i \leqslant p^m - 1$ and $l \in L(i)$ with $r = i/p^{m-h} + p^h(l - eh)$.

If $v_p(i) = 1$ then $h = m - 1$ and $ep^{m-1} - 1 < ep^m/(p-1)$. For every r with $ep^{m-1}/(p-1) < r \leqslant ep^{m-1} - 1$ and $p \nmid r$ there exist $1 \leqslant i \leqslant p^m - 1$ and $l \in L(i)$ with $r = i/p + p^{m-1}(l - em - e)$. For $ep^m - 1 < r \leqslant ep^m/(p-1)$ such elements i and l do not exist.

We have seen that for $r \leqslant ep^m/(p-1)$ all the valuations of all coefficients of non-constant terms with minimal valuation are divisible by p. The valuations of all constant terms of the form $\alpha^i + \pi^l \rho$ are divisible by p as $L(i) = \varnothing$ if $p \mid i$.

The valuations of the constant terms of the form $p^m \beta_t \alpha^t$ are not divisible by p. If $r > ep^m/(p-1)$ then $\deg\left(\underline{\psi_{r+1}^{\#}}\right) \leqslant 1$. The coefficient of the linear term of $\psi_{r+1}(x)$ has valuation $v_\alpha\left(p^m \alpha^r\right) = emp^m + r > emp^m ep^m/(p-1)$. As $t < ep^m/(p-1)$ the root-finding algorithm terminates with $\deg\left(\underline{\psi_{r+1}^{\#}}\right) = 0$ for some $1 \leqslant r \leqslant ep^m/(p-1)$. $\square$

Remark 3.7.3. Proposition 3.7.2 gives us a set $S \subset \mathbf{E}_{n,j}$ of polynomials whose roots define non-isomorphic fields extensions of $\mathbf{k}$.

- The number of integers l with $1 \leqslant l \leqslant ep/(p-1)$ or $ep^{m-1} < l \leqslant ep^m/(p-1)$ is

$$s_1 := \left\lfloor \frac{ep}{p-1} \right\rfloor + \left\lfloor \frac{ep^m}{p-1} - ep^{m-1} \right\rfloor = \left\lfloor \frac{ep}{p-1} \right\rfloor + \left\lfloor \frac{ep^{m-1}}{p-1} \right\rfloor.$$

- The number of integers l with $em - v_{\mathfrak{p}}(i) \leqslant l < em$ for i from 1 to $p^m - 1$ is

$$s_2 := \sum_{i=1}^{p^m-1} v_{\mathfrak{p}}(i) = e \sum_{i=1}^{p^m-1} v_p(i) = e\frac{p^m - 1}{p-1} - em.$$

- The number of integers r with $0 \leqslant r \leqslant ep^m/(p-1)$ with $p \mid r$ is

$$s_3 := \left\lfloor \frac{ep^m}{p(p-1)} \right\rfloor = \left\lfloor \frac{ep^{m-1}}{p-1} \right\rfloor .$$

- But there exist r with $p \mid r$ such that there is no i with $1 \leqslant i \leqslant p^m - 1$ and $l \in L(i)$ such that
$$\frac{ep^h}{p-1} < r = \frac{i}{p^{m-h}} + p^h(l - eh) \leqslant \frac{ep^{h+1}}{p-1},$$
or respectively
$$\frac{ep^{m-1}}{p-1} < r \leqslant ep^{m-1}.$$

  We have $v_p(i) \leqslant m-1$. Therefore $v_p(ip^{h-m}) \leqslant h-1$.

  If $h < m-1$ then the number of integers r with $ep^h/(p-1) < r \leqslant ep^{h+1}/(p-1)$ and $v_p(r) \geqslant h$ is
$$s_4 := \left\lfloor \frac{\lfloor ep^{h+1}/(p-1) \rfloor - \lfloor ep^h/(p-1) \rfloor}{p^h} \right\rfloor = e.$$

  The number of integers r with $ep^{m-1}(p-1) < r \leqslant ep^{m-1}$ and $v_p(r) \geqslant m-1$ is
$$s_5 := \left\lfloor \frac{ep^{m-1} - \lfloor ep^{m-1}/(p-1) \rfloor}{p^{m-1}} \right\rfloor = e - \left\lfloor \frac{e}{p-1} \right\rfloor .$$

We get

$$\begin{aligned} s &:= s_1 + s_2 - s_3 + (m-2)s_4 + s_5 \\ &= \left\lfloor \frac{ep}{p-1} \right\rfloor + \left\lfloor \frac{ep^{m-1}}{p-1} \right\rfloor + e\frac{p^m - 1}{p-1} - em - \left\lfloor \frac{ep^{m-1}}{p-1} \right\rfloor + (m-2)e + e - \left\lfloor \frac{e}{p-1} \right\rfloor \\ &= e\frac{p^m - 1}{p-1}. \end{aligned}$$

Thus the number of polynomials in S is

$$\#S = q^s = q^{e\frac{ep^m - 1}{p-1}}.$$

Note that if the roots of every polynomial in S generate p^m distinct extensions, then all extensions of degree $\mathfrak{p}^m$ and discriminant $\mathfrak{p}^{p^m + emp^m - 1}$ are given by the elements of S.

3.8 Computing Totally Ramified Extensions

Let $\mathbf{k}$ be a finite extension of $\mathbb{Q}_p$ with maximal ideal $\mathfrak{p}$. Let n and j be such that they satisfy the conditions of section 3.1.

The following algorithm finds a minimal set of polynomials generating all totally ramified extensions of degree n and discriminant $\mathfrak{p}^{n+j-1}$ using the polynomials A_ω defined in section 3.3.

Algorithm 3.8.1 (Totally Ramified Extensions).

Input: $\mathbf{k}$, n, j

Output: A minimal set of polynomials generating all totally ramified extensions of $\mathbf{k}$ of degree n and discriminant $\mathfrak{p}^{n+j-1}$

- Compute $\#\mathbf{K}_{n,j}$ using theorem 3.4.2.
- $L \leftarrow \varnothing$.
- $l \leftarrow 0$.
- For $\omega \in \Omega$:
  - Let $\varkappa$ be a root of $A_\omega(x)$.
  - If no $h \in L$ has a root in $\mathbf{k}(\varkappa)$ then:
    - $L \leftarrow L \cup \{A_\omega\}$.
    - Let r be the number of roots of A_ω in $\mathbf{k}(\varkappa)$.
    - $l \leftarrow l + n/r$.
  - 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 have been found to generate all these extensions. 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 3.5.2 to get directly a minimal set of polynomials generating all extensions.

- If $n = p$ one can use the complete description of extensions of degree p as given in section 3.6.
- If $n = p^m$ one can start with a set of polynomials defining distinct extensions (see section 3.7).
- 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.
- We can improve the computation time considerably by using propositions 3.1.2 and 3.5.3, which enable us to compute the subfield lattice at the same time. We first compute all suitable sub-extensions $\mathbf{K}_0/\mathbf{k}$ and then construct the absolute extensions $\mathbf{K}/\mathbf{k}$ 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 reduces the computation time considerably, especially in the case treated in proposition 3.5.3. Splitting up the construction of extensions this way enables us to apply theorem 3.5.2 and the results of sections 3.6 and 3.7.

The proof of lemma 3.4.1 can also be used to compute a minimal set of polynomials in a different way. We use the notation from the proof of lemma 3.4.1. In addition to the map μ that sends a prime element α in $\Pi_{n,j}$ to its irreducible polynomial $\mu(\alpha)$ over $\mathbf{k}$, we define a map $\widetilde{\mu}$ from $\Pi_{n,j}$ to Ω that sends this prime element to the unique element $\omega \in \Omega$ such that $d(\mu(\alpha), A_\omega) \leqslant r$. 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 $\mathbf{k}(\alpha)$ modulo $\mathfrak{P}_\alpha^t$ where $\mathfrak{P}_\alpha$ is the prime ideal of $\mathbf{k}(\alpha)$. 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 $\mathcal{O}_{\mathbf{k}}/\mathfrak{p}$ and $\zeta_0 \not\equiv 0 \pmod{\mathfrak{p}}$.

Proposition 3.8.2. *Let α be an element of $\Pi_{n,j}$. Then the set $\{\widetilde{\mu}(\beta) \colon \beta \in \mathcal{A}(\alpha)\}$ is exactly the set of $\omega \in \Omega$ such that α and any root of A_ω define $\mathbf{k}$-isomorphic extensions. Moreover, for any such ω the number m of $\beta \in \mathcal{A}(\alpha)$ such that $\widetilde{\mu}(\beta) = \omega$ is independent of ω and is the number of $\mathbf{k}$-automorphisms of $\mathbf{k}(\alpha)$; so, in particular, the number of conjugate fields over $\mathbf{k}$ of $\mathbf{k}(\alpha)$ is n/m.*

Proof. This is a direct application of the proofs of corollary 3.3.3 and lemma 3.4.1. □

This gives us the following algorithm.

Algorithm 3.8.3 (Totally Ramified Extensions).

Input: $\mathbf{k}$, n, j

Output: A minimal set of polynomials generating all totally ramified extensions of $\mathbf{K}$ of degree n and discriminant $\mathfrak{p}^{n+j-1}$

- Let $\{\omega_1, \ldots, \omega_l\}$ be the elements of Ω.
- For $1 \leqslant i \leqslant l$, set $B_i \leftarrow 0$.
- $L \leftarrow \varnothing$.
- $c \leftarrow 1$.
- While $c \leqslant l$:
  - 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 $\omega_d \in \widetilde{\mu}^{-1}(\mathcal{A}(\varkappa))$:
      - $B_d \leftarrow 1$.
  - $c \leftarrow c + 1$.
- Return L.

Since the basic operation in algorithm 3.8.3 is the computation of characteristic polynomials whereas the basic operation in algorithm 3.8.1 is the root finding algorithm, this algorithm seems faster than the latter. But this is not the case 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 3.8.1 the polynomials from A_ω are chosen cleverly, the algorithm can rapidly find polynomials defining all non-isomorphic extensions and thus can terminate after using the root finding algorithm only a few times.

3.9 Generating Polynomials of Galois Extensions

Shafarevich [1947] also gives a formula for the number of extensions of a $\mathfrak{p}$-adic field. Instead of Krasner's topological approach he chose a group-theoretic approach.

Theorem 3.9.1 (Shafarevich). *Let* $\mathbf{k}$ *be a finite extension of* $\mathbb{Q}_p$ *with* $[\mathbf{k} : \mathbb{Q}_p] = n$*. Let* G *be a group of order* p^m *with* $d \leqslant n+1$ *generators and* $\mathrm{Aut}(G)$ *the group of its automorphisms. The number extensions of* $\mathbf{k}$ *with Galois group* G *is*

$$\frac{1}{\#\mathrm{Aut}(G)}\left(\frac{\#G}{p^d}\right)^{n+1}\prod_{i=0}^{d-1}(p^{n+1}-p^i).$$

Yamagishi [1995] generalized Shafarevich's results to include the case when $\mathbf{k}$ includes the p-th roots of unity. The following proposition is a consequence of his work.

Denote by μ_p and μ_{p^2} the set of the p-th, respectively p^2-th, roots of unity.

Proposition 3.9.2 (Yamagishi). *The number of Galois extensions of degree p^2 of $\mathbf{k}$ with ramification index E and inertia degree F is given below.*

<table>
<tr><th rowspan="2">Galois group</th><th rowspan="2">E</th><th rowspan="2">F</th><th colspan="3">number of extensions of $\mathbf{k}$, if</th></tr>
<tr><th>$\mu_p \not\subset \mathbf{k}$</th><th>$\mu_p \subset \mathbf{k}$ and $\mu_{p^2} \not\subset \mathbf{k}$</th><th>$\mu_{p^2} \subset \mathbf{k}$</th></tr>
<tr><td rowspan="2">$C_p \times C_p$</td><td>p</td><td>p</td><td>$\frac{p^n-1}{p-1}$</td><td colspan="2">$\frac{p^{n+1}-1}{p-1}$</td></tr>
<tr><td>p^2</td><td>1</td><td>$p^2\,\frac{p^n-1}{p-1}\,\frac{p^{n-1}-1}{p^2-1}$</td><td colspan="2">$p^2\,\frac{p^{n+1}-1}{p-1}\,\frac{p^n-1}{p^2-1}$</td></tr>
<tr><td rowspan="3">C_{p^2}</td><td>1</td><td>p^2</td><td colspan="3">1</td></tr>
<tr><td>p</td><td>p</td><td>p^n-1</td><td colspan="2">$p^{n+1}-1$</td></tr>
<tr><td>p^2</td><td>1</td><td>$p^{n+1}\,\frac{p^n-1}{p-1}$</td><td>$p^{n+2}\,\frac{p^n-1}{p-1}$</td><td>$p^{n+2}\,\frac{p^{n+1}-1}{p-1}$</td></tr>
</table>

Denote by e and f the ramification index and inertia degree of $\mathbf{k}$. Let π be a prime element of $\mathbf{k}$ and let $\zeta \in \mathbf{k}$ be a (p^f-1)-th root of unity.

Lemma 3.9.3. *Let $\vartheta(x) \in \mathbf{k}[x]$ be monic with* $\deg(\vartheta) = p$ *and $\underline{\varphi}(x)$ irreducible over $\underline{\mathbf{k}}[x]$. Let $j = ap+b$ such that they fulfill Ore's Conditions and such that $p-1$ divides $a+b$. Let*

$$\varphi(x) = x^p + \zeta^s\pi^{a+1}x^b + \pi + \sum_{i\in L(0)} \rho_{c_i}\pi^{i+1} \in \mathbf{k}[x]$$

with $x^{p-1}+(-1)^{ap+1}\underline{\zeta^s b}$ in $\underline{\mathbf{k}}[x]$ reducible. Denote by Γ and Π roots of $\vartheta(x)$ and $\varphi(x)$ respectively. Then $\mathbf{k}(\Gamma,\Pi)/\mathbf{k}$ is Galois with Galois group isomorphic to $C_p \times C_p$.

Proof. By theorem 3.6.5 $\mathbf{k}(\Pi)$ is Galois over $\mathbf{k}$. In the proof of corollary 3.6.10 we have seen that the number of polynomials of the form $\varphi(x)$ is $(p^n-1)(p-1)$. By theorem 3.6.5 these generate non-isomorphic extensions. As the coefficients of $\varphi(x)$ are fixed by all elements in $\mathrm{Gal}(\mathbf{k}(\varGamma)/\mathbf{k})$ the extension $\mathbf{k}(\varGamma, \varPi)$ is Galois over $\mathbf{k}$. $\square$

Remark 3.9.4. We use the notation from theorem 3.6.5. Fix a, b, s, and c_i, $i \in L(0)$. For $k \in \{1, \ldots, p\}$ set

$$\varphi_k(x) := x^p + \zeta^s \pi^{a+1} x^b + \pi + \sum_{i \in L(0)} \rho_{c_i} \pi^{i+1} + (k-1)\delta\pi^{t+1} \in \mathbf{k}[x].$$

Denote by $\varPi_k$ a root of φ_k in an algebraic closure of $\mathbf{k}$. Let $\vartheta(x) \in \mathbf{k}[x]$ be monic with $\deg(\vartheta) = p$ and $\underline{\varphi}(x)$ irreducible over $\underline{\mathbf{k}}[x]$. The lattice of subfields of $\mathbf{k}(\varGamma, \varPi_1) = \cdots = \mathbf{k}(\varGamma, \varPi_p)$ is:

$$\begin{tikzcd}
& & \mathbf{k}(\varGamma, \varPi_1) \arrow[dll, dash, "p"'] \arrow[d, dash] \arrow[drr, dash] & & \\
\mathbf{k}(\varGamma) \arrow[drr, dash, "p"'] & & \mathbf{k}(\varPi_1) \arrow[d, dash] & \cdots & \mathbf{k}(\varPi_p) \arrow[dll, dash] \\
& & \mathbf{k} & &
\end{tikzcd}$$

For $\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{k})$ and $\psi(x) = c_n x^n + \cdots + c_1 x + c_0 \in \mathbf{K}[x]$ denote by $\sigma(\psi)(x)$ the polynomial $\sigma(c_n)x^n + \cdots + \sigma(c_1)x + \sigma(c_0)$.

Lemma 3.9.5. *Let $\vartheta(x) \in \mathbf{k}[x]$ be monic with $\deg(\vartheta) = p$ and $\underline{\vartheta}(x)$ irreducible over $\underline{\mathbf{k}}[x]$. Denote by $\varGamma$ a root of $\vartheta(x)$. Let $j = ap+b$ such that they fulfill Ore's Conditions and such that $(p-1) \mid (a+b)$. Let*

$$\varphi(x) = x^p + \xi^s \pi^{a+1} x^b + \pi + \sum_{i \in L(0)} \rho_{c_i} \pi^{i+1} + k\delta\pi^t \in \mathbf{k}(\varGamma)[x]$$

with $x^{p-1} - \underline{\zeta^s b}$ reducible in $\underline{\mathbf{k}}[x]$ and $\delta \in \mathbf{k}(\varGamma)$ such that $x^p - \underline{\zeta^s b}x + \underline{\delta} \in \underline{\mathbf{k}(\varGamma)}[x]$ is irreducible. Let $\varPi$ be a root of $\varphi(x)$. Then $\mathbf{k}(\varGamma, \varPi)/\mathbf{k}$ is Galois with Galois group isomorphic to C_{p^2}.

Proof. All Galois extensions of degree p of $\mathbf{k}(\varGamma)$ are generated by the roots of polynomials of the form

$$\varphi(x) = x^p + \zeta^s \pi^{a+1} x^b + \pi + \sum_{i \in L(0)} \rho_{c_i} \pi^{i+1} + k\delta\pi^{t+1},$$

where $(p-1) \mid (a+b)$ and $x^{p-1} - \underline{\zeta^s b}$ is reducible in $\underline{\mathbf{k}}[x]$.

Let Π be a root of $\varphi(x)$. The extension $\mathbf{k}(\Gamma, \Pi)/\mathbf{k}$ is Galois if for every σ in $\mathrm{Gal}(\mathbf{k}(\Gamma)/\mathbf{k})$ the polynomial $\sigma(\varphi)(x)$ is reducible over $\mathbf{k}(\Gamma, \Pi)$. By lemma 3.6.6 the extension $\mathbf{k}(\Gamma, \Pi)/\mathbf{k}$ is not Galois if $\zeta^s \in \mathbf{k}(\Gamma) \setminus \mathbf{k}$. It follows from the proof of lemma 3.6.7 that $\mathbf{k}(\Gamma, \Pi)/\mathbf{k}$ is not Galois if $\rho_{c_i} \in \mathbf{k}(\Gamma) \setminus \mathbf{k}$. By Lemma 3.9.3 we have $\mathrm{Gal}(\mathbf{k}(\Gamma, \Pi)/\mathbf{k}) \cong C_p \times C_p$ if $k = 0$. This leaves

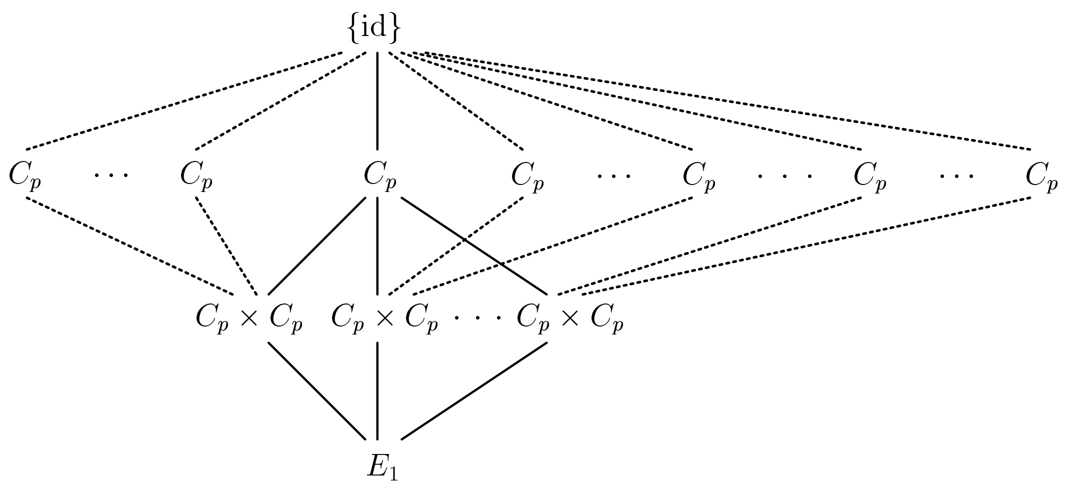
$$p\frac{p^n - 1}{p - 1} - \frac{p^n - 1}{p - 1} = p^n - 1$$

Galois extensions of $\mathbf{k}$ of degree p^2 with ramification index p and inertia degree p and Galois group not isomorphic to $C_p \times C_p$. $\square$

Proposition 3.9.6. *Let $\vartheta(x) \in \mathbb{Q}_p[x]$ be monic with $\deg(\vartheta) = p$ and $\underline{\vartheta}(x)$ irreducible over $\mathbb{F}_p[x]$. Let Γ be a root of $\vartheta(x)$. Let $\varphi(x) := x^p + (p-1)px^{p-1} + p \in \mathbb{Q}_p(\Gamma)$. Let π be a root of $\varphi(x)$. Let $\psi(x) := x^p + (p-1)\pi x^{p-1} + \pi$. Then $\mathbb{Q}_p(\Gamma, \pi, \Pi)$ is the unique Galois extension of $\mathbb{Q}_p$ with Galois group isomorphic to*

$$E_1 := \langle \sigma, \tau;\, \sigma^p = \tau^p = [\sigma, \tau]^p = 1,\, [\sigma, [\sigma, \tau]] = [\tau, [\sigma, \tau]] = 1 \rangle.$$

The lattice of subgroups of E_1 is shown below. The subgroups with dotted lines are not normal in E_1.



Proof. It follows from theorem 3.9.1 that there is only one Galois extension of $\mathbb{Q}_p$ with Galois group isomorphic to E_1.

First we show that $\mathbb{Q}_p(\mathit{\Gamma}, \pi, \mathit{\Pi})$ is Galois over $\mathbb{Q}_p$. As the coefficients of $\varphi(x)$ and $\psi(x)$ are fixed under the automorphisms of $\mathbb{Q}_p(\mathit{\Gamma})$ the extension $\mathbb{Q}_p(\mathit{\Gamma}, \pi, \mathit{\Pi})/\mathbb{Q}_p(\mathit{\Gamma})$ is Galois. It follows from the proof of lemma 3.6.8 that there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\mathit{\Gamma}, \pi)/\mathbb{Q}_p(\mathit{\Gamma})$ generating $\mathrm{Gal}(\mathbb{Q}_p(\mathit{\Gamma}, \pi)/\mathbb{Q}_p(\mathit{\Gamma})$, such that $\sigma(\pi) \equiv \pi + \pi^2 \bmod \pi^3$. This gives $\sigma(\psi)(x) \equiv x^p + (p-1)(\pi + \pi^2)x^{p-1} + \pi + \pi^2$. We use the root-finding algorithm to show that $\sigma(\psi)(x)$ has a root over $\mathbb{Q}_p(\mathit{\Gamma}, \pi, \mathit{\Pi})$. We get

$$\sigma(\psi)_2(x) \equiv \pi(x^p + (p-1)x + 1)$$

(*c.f.* proof of lemma 3.6.7) which has p roots over $\mathbb{Q}_p(\mathit{\Gamma}, \pi, \mathit{\Pi})$. It follows that $\sigma(\psi)(x)$ has p roots over $\mathbb{Q}_p(\mathit{\Gamma}, \pi, \mathit{\Pi})$. Thus $\mathbb{Q}_p(\mathit{\Gamma}, \pi, \mathit{\Pi})$ is Galois over $\mathbb{Q}_p$.

The extension of degree p^3 with Galois group isomorphic to E_1 is the only Galois extension of degree p^3 which has p^2 totally ramified subfields of degree p^2 that are not Galois over $\mathbb{Q}_p$.

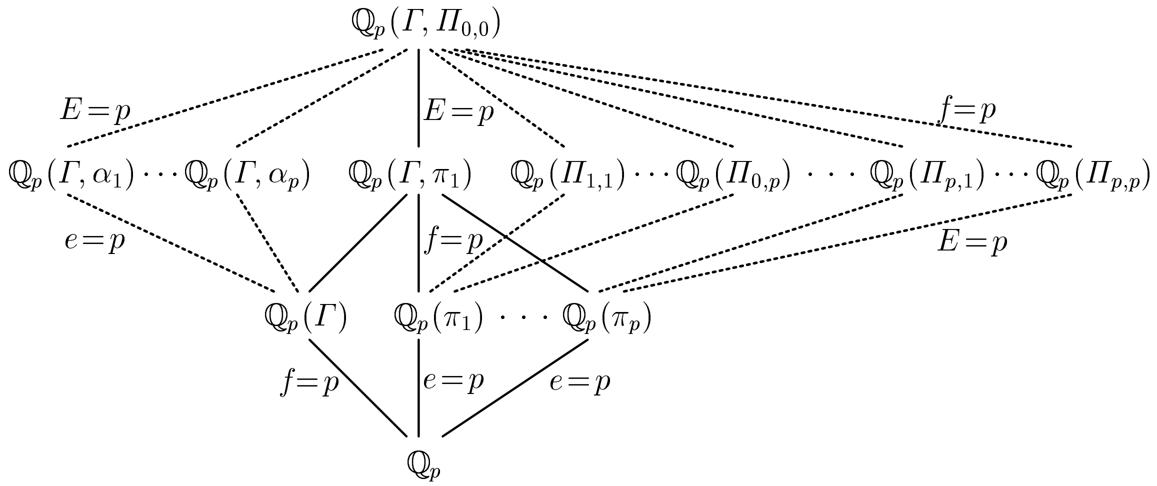
For $i \in \{0, \dots, p-1\}$ let $\varphi_i(x) := x^p + (p-1)px^{p-1} + p + ip^2 \in \mathbb{Q}_p[x]$ and denote by π_i a root of $\varphi_i(x)$. For $i \in \{0, \dots, p-1\}$ and $k \in \{0, \dots, p-1\}$ let $\psi_{ik}(x) := x^p + (p-1)\pi_i x^{p-1} + \pi_i + k\pi_i^2 \in \mathbb{Q}_p(\pi_i)$ and denote by $\mathit{\Pi}_{ik}$ a root of $\psi_{ik}(x)$.

We show that $\mathbb{Q}_p(\pi_i, \mathit{\Pi}_{ik})$ is not Galois over $\mathbb{Q}_p(\pi_i)$. It follows from the proof of lemma 3.6.8 that there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\pi_i)/\mathbb{Q}_p$ such that $\sigma(\pi) \equiv \pi_i + \pi_i^2 \bmod \pi_i^3$. This gives $\sigma(\psi_{ik})(x) \equiv x^p + (p-1)(\pi + \pi^2)x^{p-1} + \pi + \pi^2$. We use the root-finding algorithm to show that $\sigma(\psi_{ik})(x)$ has a root over $\mathbb{Q}_p(\mathit{\Gamma}, \pi, \mathit{\Pi})$. As in the proof of lemma 3.6.8 we get

$$\sigma(\psi)_2(x) \equiv \pi_i(x^p - (p-1)x + 1),$$

which is irreducible over $\mathbb{Q}_p(\pi_i, \mathit{\Pi}_{ik})$. Thus $\mathbb{Q}_p(\pi_i, \mathit{\Pi}_{ik})$ is not Galois over $\mathbb{Q}_p(\pi_i)$. $\square$

For $p \neq 2$ the lattice of subfields of the unique extensions of $\mathbb{Q}_p$ of degree p^3 with Galois group E_1 is depicted below. The elements $\mathit{\Gamma}$, π_i, and $\mathit{\Pi}_{k,l}$ with $i, k, l \in \{1, \dots, p\}$ are as in the proof of proposition 3.9.6. The elements $\alpha_1, \dots, \alpha_p$ are generators of the remaining degree-p extensions of $\mathbb{Q}_p(\mathit{\Gamma})$.



3.10 Examples

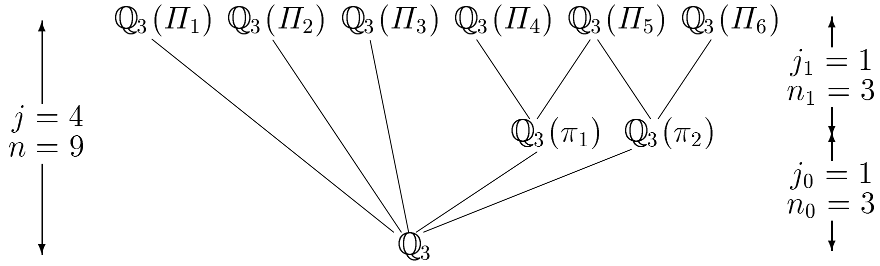
Example 3.10.1 (Extensions of degree 9 and discriminant 3^{12} over $\mathbb{Q}_3$). There are 54 extensions of degree 9 and discriminant 3^{9+4-1} over $\mathbb{Q}_3$. We compute all these as absolute extensions over $\mathbb{Q}_3$. We find the following generating polynomials, each of them defining 9 isomorphic extensions.

$$\begin{aligned}
\mathit{\Phi}_1(x) &= x^9 + 2 \cdot 3x^4 + 3 & \qquad \mathit{\Phi}_4(x) &= x^9 + 2 \cdot 3x^4 + 2 \cdot 3x^3 + 3 \\
\mathit{\Phi}_2(x) &= x^9 + 3x^4 + 2 \cdot 3x^3 + 3 & \qquad \mathit{\Phi}_5(x) &= x^9 + 3x^4 + 3 \\
\mathit{\Phi}_3(x) &= x^9 + 3x^4 + 3x^3 + 3 & \qquad \mathit{\Phi}_6(x) &= x^9 + 2 \cdot 3x^4 + x^3 + 3
\end{aligned}$$

Following proposition 3.1.2, 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 out that there are six such subfields generated by the roots of the two polynomials $\varphi_1(x) = x^3 + 6x + 3$ and $\varphi_2(x) = x^3 + 3x + 3$. Let π_1 and π_2 be zeroes of φ_1 and φ_2 respectively. Each of the fields $\mathbb{Q}_3(\pi_i)$ admits six totally ramified extensions of degree $n_1 = 3$ and discriminant $(\pi_i)^{3+j_1-1}$ where $j_1 = 1$. These extensions are generated by $\psi_{i1}(x) = x^3 + \pi_i x + \pi_i$ and $\psi_{i2}(x) = x^3 + 2\pi_i x + \pi_i$ over $\mathbb{Q}_3(\pi_i)$.

Let $\alpha_{i,k}$ denote a root of $\psi_{i,k}$. Using algorithm 2.1.4 we get that $\mathbb{Q}_3(\pi_1)(\alpha_{12}) \cong \mathbb{Q}_3(\pi_2)(\alpha_{21})$ and that the other fields are distinct. So we have found 27 extensions of degree 9 that have subfields of degree 3. Let $\mathit{\Pi}_i$ be a root of $\mathit{\Phi}_i$. We have $\mathbb{Q}_3(\mathit{\Pi}_5) \cong$

$\mathbb{Q}_3(\pi_1)(\alpha_{21}) \cong \mathbb{Q}_3(\pi_2)(\alpha_{12})$, $\mathbb{Q}_3(\Pi_6) \cong \mathbb{Q}_3(\pi_1)(\alpha_{22})$ and $\mathbb{Q}_3(\Pi_4) \cong \mathbb{Q}_3(\pi_2)(\alpha_{11})$. The lattice of subfields (up to isomorphism) is depicted below.



Example 3.10.2 (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 $\varphi(x) = x^{10} + 2x^8 + 3$.

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

There are 605 extensions with residue degree 2 and ramification index 5. These extensions $\mathbf{K}$ are generated over the unramified field $\mathbf{k} := \mathbb{Q}_5(\rho)$, $\rho^2 + 2 = 0$, 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	$x^5 + 5(h_1 + h_2\rho)x + 5$ $\quad h_1,\ h_2 \in \{0,1,2,3,4\}$, $(h_1, h_2) \neq (0,0)$	5	120
2	$x^5 + 5(h_1 + h_2\rho)x^2 + 5$ $\quad h_1,\ h_2 \in \{0,1,2,3,4\}$, $(h_1, h_2) \neq (0,0)$	5	120
3	$x^5 + 5(h_1 + h_2\rho)x^3 + 5$ $\quad h_1,\ h_2 \in \{0,1,2,3,4\}$, $(h_1, h_2) \neq (0,0)$	5	120
4	$x^5 + 5(h_1 + h_2\rho)x^4 + 5$ $\quad h_1,\ h_2 \in \{0,1,2,3,4\}$ $(h_1, h_2) \notin \{(0,0),(1,0),(2,1),(2,4),(3,1),(3,4),(4,0)\}$	5	90
4	$x^5 + 5(h_1 + h_2\rho)x^4 + 5 + 25h_0\rho$ $\quad h_0 \in \{0,1,2,3,4\}$ $(h_1, h_2) \in \{(1,0),(2,1),(2,4),(3,1),(3,4)\}$	1	25
4	$x^5 + 4 \cdot 5x^4 + 5 + 25h_0$ $\quad h_0, \in \{0,1,2,3,4\}$	1	5
5	$x^5 + 5 + 25(h_1 + h_2\rho)$ $\quad h_1,\ h_2 \in \{0,1,2,3,4\}$	5	125

There are 1210 totally ramified extensions of degree 10 of $\mathbb{Q}_5$. Using proposition 3.5.3, we find that they are relative extensions over one of the two tamely ramified extensions of degree 2 defined by $\varphi_i(x) = x^2 + 5i$ where $i = 1, 2$. Let π_i be a root of φ_i. The wildly ramified part is generated by the polynomials in the following table over $\mathbb{Q}_5(\pi_i)$. The roots of each polynomial generate N distinct isomorphic 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	$x^5 + h_1\pi_i x + \pi_i$	$h_1 \in \{1,2,3,4\}$	5	20
2	$x^5 + h_2\pi_i x^2 + \pi_i$	$h_2 \in \{1,2,3,4\}$	5	20
3	$x^5 + h_3\pi_i x^3 + \pi_i$	$h_3 \in \{1,2,3,4\}$	5	20
4	$x^5 + h_4\pi_i x^4 + \pi_i$	$h_4 \in \{1,2,3\}$	5	15
4	$x^5 + 4\pi_i x^4 + (\pi_i + h_0\pi_i^2)$	$h_0 \in \{0,1,2,3,4\}$	1	5
6	$x^5 + h_1\pi_i^2 x + (\pi_i + h_0\pi_i^2)$	$h_1 \in \{1,2,3,4\}$, $h_0 \in \{0,1,2,3,4\}$	5	100
7	$x^5 + h_1\pi_i^2 x^2 + (\pi_i + h_0\pi_i^2)$	$h_1 \in \{1,2,3,4\}$, $h_0 \in \{0,1,2,3,4\}$	5	100
8	$x^5 + h_1\pi_i^2 x^3 + (\pi_i + h_0\pi_i^2)$	$h_1 \in \{1,2,4\}$, $h_0 \in \{0,1,2,3,4\}$	5	75
8	$x^5 + 3\pi_i^2 x^3 + (\pi_i + h_0\pi_i^2 + h_1\pi_i^3)$	$h_0,\ h_1 \in \{0,1,2,3,4\}$	1	25
9	$x^5 + h_1\pi_i^2 x^4 + (\pi_i + h_0\pi_i^2)$	$h_1 \in \{1,2,3,4\}$, $h_0 \in \{0,1,2,3,4\}$	5	100
10	$x^5 + (\pi_i + h_2\pi_i^2 + h_3\pi_i^3)$	$h_2,\ h_3 \in \{0,1,2,3,4\}$	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 $\mathbb{Q}_5$.

3.11 Future Developments

This thesis can be regarded as a step towards a generalized, constructive class field theory for $\mathfrak{p}$-adic fields. The methods described above work well for small examples, *i.e.*, when the number $\#D_{\mathbf{E}_{n,j}}$ of polynomials A_ω with $\omega \in \Omega$ is small.

A complete description of extensions of degree p^m would speed up the computation considerably. Here the methods of Lbekkouri [1997] could be applied. He gives conditions on the coefficients of Eisenstein polynomials over $\mathbb{Q}_p$ of degree p^2, to decide whether the extensions defined by these are normal.

The number of polynomials can be easily reduced by using additional invariants of the extensions to be computed in addition to the degree and discriminant.

The indices of inseparability, introduced by Arf [1939] and refined by Heiermann [1996], could be easily used, as they can be translated directly into conditions on the coefficients of the defining polynomials of extensions.

It is ultimately desirable to refine the algorithm so that it returns all extensions of a $\mathfrak{p}$-adic field of a given degree, discriminant and Galois group. Once the description of extensions of degree p^2 has been completed (see section 3.9) it should be possible to construct totally ramified Galois extensions of $\mathbb{Q}_p$ using methods similar to those in the proof of proposition 3.9.6.

These approaches are subjects of ongoing research.

Bibliography

S. Amano. Eisenstein equations of degree p in a $\mathfrak{p}$-adic field. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 18, 1971.

C. Arf. Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper. *J. Reine Angew. Math.*, 181, 1939.

E. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.*, 24, 1970.

W. Bosma and J.J. Cannon. *Handbook of Magma functions.* School of Mathematics, University of Sydney, Sydney, 1995.

D. G. Cantor and D. Gordon. Factoring polynomials over p-adic fields. In W. Bosma, editor, *ANTS IV*, volume 1838 of *LNCS*. Springer Verlag, 2000.

D. G. Cantor and H. Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Math. Comp.*, 36, 1981.

J. W. S. Cassels. *Local Fields.* Cambridge University Press, Cambridge, 1986.

A. L. Chistov. Efficient factoring polynomials over local fields and its applications. In *ICM 1990.* Springer-Verlag, 1991.

H. Cohen. *A Course in Computional Algebraic Number Theory.* Springer Verlag, New York, 1993.

H. Cohen. *Advanced topics in computational number theory.* Springer Verlag, New York, 1999.

I. B. Fesenko and S. V. Vostokov. *Local Fields and Their Extensions*, volume 121 of *Translations of Mathematical Monographs.* American Mathematical Society, 1993.

C. Fieker and C. Friedrichs. On reconstruction of algebraic numbers. In W. Bosma, editor, *ANTS IV*, volume 1838 of *LNCS*. Springer Verlag, 2000.

D. Ford. *On the Computation of the Maximal Order in a Dedekind Domain.* Phd thesis, Ohio State University, 1978.

D. Ford. The construction of maximal orders over a Dedekind domain. *Journal of Symbolic Computation*, 4, 1987.

D. Ford and P. Letard. Implementing the round four maximal order algorithm. *Journal de Théorie des Nombres de Bordeaux*, 6, 1994.

D. Ford, S. Pauli, and X.-R Roblot. A guide to polynomial factorization over $\mathbb{Q}_p$. Technical Report 3, CICMA, Concordia Laval McGill, 2000.

H. Hasse. *Zahlentheorie*. Akademie Verlag, Berlin, 1963.

V. Heiermann. De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux. *Journal of Number Theory*, 59, 1996.

E. Kaltofen and V. Shoup. Subquadratic-time factoring of polynomials over finite fields. *Math. Comp.*, 67, 1998.

M. Krasner. Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique. In *Les Tendances Géométriques en Algèbre et Théorie des Nombres*. Paris, 1966.

M. Krasner. Remarques au sujet d'une note de J.-P. Serre. *C. R. Acad. Sci. Paris*, 288, 1979.

A. Lbekkouri. On extensions defined by Eisenstein polynomials over $\mathbb{Q}_p$. preprint, 1997.

J. Montes. *Polígonos de Newton de orden superior y aplicaciones aritméticas*. PhD thesis, Universitat de Barcelona, 1999.

Ö. Ore. Bemerkungen zur Theorie der Differente. *Math. Zeitschr.*, 25, 1926.

P. Panayi. *Computation of Leopoldt's p-adic regulator*. Dissertation, University of East Anglia, 1995.

S. Pauli. Factoring polynomials over local fields. to appear in J. Symb. Comp., 2001.

S. Pauli and X.-F. Roblot. On the computation of all extensions of a p-adic field of a given degree. *Math. Comp.*, 70, 2001.

M. E. Pohst. Factoring polynomials over global fields. submitted to J. Symb. Comp., 1999.

M. E. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*. Cambridge University Press, 1989.

X.-F. Roblot. Factorization algorithms over number fields. submitted to J. Symb. Comp., 2000.

A. Schönhage and V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7, 1971.

J.-P. Serre. *Corps Locaux*. Hermann, Paris, 1963.

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.

I. R. Shafarevich. On p-extensions. *Mat. Sb., Nov. Ser. 20*, 62, 1947.

B. M. Trager. Algebraic factoring and rational function integration. In *Symposium on Symbolic and Algebraic Computation*. ACM Press, 1976.

J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

M. Yamagishi. On the number of Galois p-extensions of a local field. *Proc. AMS*, 123, 1995.