JOURNAL
de Théorie des Nombres
de BORDEAUX
*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Sebastian PAULI

**Constructing class fields over local fields**

Tome 18, n° 3 (2006), p. 627-652.

<http://jtnb.cedram.org/item?id=JTNB_2006__18_3_627_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **18** (2006), 627-652

# Constructing class fields over local fields

par Sebastian PAULI

***Dedicated to Michael Pohst on his 60th Birthday***

Résumé. Soit $K$ un corps $\mathfrak{p}$-adique. Nous donnons une caractérisation explicite des extensions abéliennes de $K$ de degré $p$ en reliant les coefficients des polynômes engendrant les extensions $L/K$ de degré $p$ aux exposants des générateurs du groupe des normes $N_{L/K}(L^*)$. Ceci est appliqué à un algorithme de construction des corps de classes de degré $p^m$, ce qui conduit à un algorithme de calcul des corps de classes en général.

Abstract. Let $K$ be a $\mathfrak{p}$-adic field. We give an explicit characterization of the abelian extensions of $K$ of degree $p$ by relating the coefficients of the generating polynomials of extensions $L/K$ of degree $p$ to the exponents of generators of the norm group $N_{L/K}(L^*)$. This is applied in an algorithm for the construction of class fields of degree $p^m$, which yields an algorithm for the computation of class fields in general.

## 1. Introduction

Local class field theory gives a complete description of all abelian extensions of a $\mathfrak{p}$-adic field $K$ by establishing a one-to-one correspondence between the abelian extensions of $K$ and the open subgroups of the unit group $K^*$ of $K$. We describe a method that, given a subgroup of $K^*$ of finite index, returns the corresponding abelian extension.

There are two classic approaches to the construction of abelian extensions: Kummer extensions and Lubin-Tate extensions. Kummer extensions are used in the construction of class fields over global fields [Fie99, Coh99]. The theory of Lubin-Tate extensions explicitly gives generating polynomials of class fields over $\mathfrak{p}$-adic fields including the Artin map.

The goal of this paper is to give an algorithm that constructs class fields as towers of extensions from below thus avoiding the computation of a larger class field and the determination of the right subfield. The wildly ramified

Manuscrit reçu le 31 décembre 2005.

part of a class field is constructed as a tower of extensions of degree $p$ over the tamely ramified part of the class field.

Our approach allows the construction of class fields of larger degree than the approach with Lubin-Tate or Kummer extensions. Given a subgroup $G$ of $K^*$ these methods provide a class field $L_H$ that corresponds to a subgroup $H$ of $G$ and that contains the class field corresponding to $G$. In general the degree of $L_H$ is very large and the computation of the corresponding subfield expensive. Our approach does not yield a construction of the Artin map though.

We start by recalling the structure of the unit groups of $\mathfrak{p}$-adic fields (section 2). In section 3 we state the main results of local class field theory and the explicit description of tamely ramified class fields. It follows that we can restrict our investigation to cyclic class fields of degree $p^m$. We begin our investigation by constructing a minimal set of generating polynomials of all extensions of $K$ of degree $p$ (section 4). In section 5 we relate the coefficients of the polynomials generating extensions of degree $p$ to the exponents of the generators of their norm groups. This yields an algorithm for computing class fields of degree $p$. Section 6 contains an algorithm for computing class fields of degree $p^m$. In section 7 we give several examples of class fields.

Given a fixed prime number $p$, $\mathbb{Q}_p$ denotes the completion of $\mathbb{Q}$ with respect to the $p$-adic valuation $|\cdot| = p^{-\nu_p(\cdot)}$, $K$ is a finite extension of degree $n$ over $\mathbb{Q}_p$ complete with respect to the extension of $|\cdot|$ to $K$, and $\mathcal{O}_K = \{\alpha \in K \mid |\alpha| \leqslant 1\}$ is the valuation ring of $K$ with maximal ideal $\mathfrak{p}_K = \{\alpha \in K \mid |\alpha| < 1\} = (\pi_K)$. The residue class field is defined by $\underline{K} := \mathcal{O}_K/\mathfrak{p}_K$ and $f = f_K$ is the degree of $\underline{K}$ over the finite field with $p$ elements $\mathbb{F}_p$. For $\gamma \in \mathcal{O}_K$ the class $\gamma + \mathfrak{p}_K$ is denoted by $\underline{\gamma}$. The ramification index of $\mathfrak{p}_K$ is denoted by $e = e_K$ and we recall that $ef = n$. By $\mathrm{d}_K$ we denote the discriminant of $K$ and by $\mathrm{d}_\varphi$ the discriminant of a polynomial $\varphi$.

## 2. Units

It is well known that the group of units of a $p$-adic field $K$ can be decomposed into a direct product

$$K^* = \langle \pi_K \rangle \times \langle \zeta_K \rangle \times (1 + \mathfrak{p}_K) \cong \pi_K^{\mathbb{Z}} \times \underline{K}^* \times (1 + \mathfrak{p}_K),$$

where $\zeta_K \in K$ a $(\#\underline{K} - 1)$-th root of unity. The multiplicative group $1 + \mathfrak{p}_K$ is called the group of principal units of $K$. If $\eta \in 1 + \mathfrak{p}_K$ is a principal unit with $v_\mathfrak{p}(\eta - 1) = \lambda$ we call $\lambda$ the level of $\eta$.

A comprehensive treatment of the results presented in this section can be found in [Has80, chapter 15].

**Lemma 2.1** ($p$-th power rule)**.** *Let $\alpha$ be in $\mathcal{O}_K$. Let $p = -\pi_K^{e_K}\varepsilon$ be the factorization of $p$ where $\varepsilon$ is a unit. Then the $p$–th power of $1+\alpha\pi_K^{\lambda}$ satisfies*

$$(1+\alpha\pi^{\lambda})^p \equiv \begin{cases} 1+\alpha^p\pi_K^{p\lambda} & \mod \mathfrak{p}_K^{p\lambda+1} \quad \text{if} \quad 1 \leqslant \lambda < \frac{e_K}{p-1} \ , \\ 1+(\alpha^p-\varepsilon\alpha)\pi_K^{p\lambda} & \mod \mathfrak{p}_K^{p\lambda+1} \quad \text{if} \quad \lambda = \frac{e_K}{p-1} \ , \\ 1-\varepsilon\alpha\pi_K^{\lambda+e} & \mod \mathfrak{p}_K^{\lambda+e+1} \quad \text{if} \quad \lambda > \frac{e_K}{p-1} \ . \end{cases}$$

*The maps $h_1 : \alpha+\mathfrak{p} \longmapsto \alpha^p+\mathfrak{p}_K$ and $h_3 : \alpha+\mathfrak{p}_K \longmapsto -\varepsilon\alpha+\mathfrak{p}_K$ are automorphisms of $\underline{K}^+$, whereas $h_2 : \alpha+\mathfrak{p}_K \longmapsto \alpha^p-\varepsilon\alpha+\mathfrak{p}_K$ is in general only a homomorphism. The kernel of $h_2$ is of order 1 or $p$.*

As $(1+\mathfrak{p}_K^{\lambda})/(1+\mathfrak{p}_K^{\lambda+1}) \cong \mathfrak{p}_K^{\lambda}/\mathfrak{p}_K^{\lambda+1} \cong \underline{K}^+$, it follows that if $\eta_{\lambda,1},\dots,\eta_{\lambda,f_K}$ is a system of generators for the level $\lambda < \frac{e_K}{p-1}$ (for the level $\lambda > \frac{e_K}{p-1}$), then $\eta_{\lambda,1}^p,\dots,\eta_{\lambda,f}^p$ is a system of generators for the level $p\lambda$ (for the level $\lambda+e_K$). If $(p-1) \mid e_K$ the levels based on the level $\lambda = \frac{e_K}{p-1}$ need to be discussed separately.

We define the set of fundamental levels

$$F_K := \{\lambda \mid 0 < \lambda < \tfrac{pe_K}{p-1}, p \nmid \lambda\}.$$

All levels can be obtained from the fundamental levels via the substitutions presented above. The cardinality of $F_K$ is

$$\#F_K = \left\lfloor \tfrac{pe}{p-1} \right\rfloor - \left\lfloor \tfrac{pe}{p(p-1)} \right\rfloor = e + \left\lfloor \tfrac{e}{p-1} \right\rfloor - \left\lfloor \tfrac{e}{p-1} \right\rfloor = e.$$

If $K$ does not contain the $p$-th roots of unity then principal units of the fundamental levels generate the group of principal units:

**Theorem 2.2** (Basis of $1+\mathfrak{p}_K$, $\mu_p \not\subset K$)**.** *Let $\omega_1,\dots,\omega_f \in \mathcal{O}_K$ be a fixed set of representatives of an $\mathbb{F}_p$-basis of $\underline{K}$. If $p-1$ does not divide $e_K$ or if $h_2$ is an isomorphism, that is, $K$ does not contain the $p$-th roots of unity, then the elements*

$$\eta_{\lambda,i} := 1+\omega_i\pi^{\lambda} \ \text{ where } \lambda \in F_K, 1 \leqslant i \leqslant f_K$$

*are a basis of the group of principal units $1+\mathfrak{p}_K$.*

If $K$ contains the $p$-th roots of unity we need one additional generator:

**Theorem 2.3** (Generators of $1+\mathfrak{p}_K$, $\mu_p \subset K$)**.** *Assume that $(p-1) \mid e_K$ and $h_2$ is not an isomorphism, that is, $K$ contains the $p$-th roots of unity. Choose $e_0$ and $\mu_0$ such that $p$ does not divide $e_0$ and such that $e_K = p^{\mu_0-1}(p-1)e_0$. Let $\omega_1,\dots,\omega_f \in \mathcal{O}_K$ be a fixed set of representatives of a $\mathbb{F}_p$-basis of $\underline{K}$ with $\omega_1$ chosen such that $\omega_1^{p^{\mu_0}} - \varepsilon\omega_1^{p^{\mu_0-1}} \equiv 0 \bmod \mathfrak{p}_K$ and $\omega_1 \not\equiv 0 \bmod \mathfrak{p}_K$. Choose $\omega_* \in \mathcal{O}_K$ such that $x^p - \varepsilon x \equiv \omega_* \bmod \mathfrak{p}_K$ has no solution. Then the group of principal units $1+\mathfrak{p}_K$ is generated by*

$$\eta_* := 1+\omega_*\pi_K^{p^{\mu_0}e_0} \ \text{ and } \ \eta_{\lambda,i} := 1+\omega_i\pi_K^{\lambda} \ \text{ where } \lambda \in F_K,\ 1 \leqslant i \leqslant f_K.$$

Algorithms for the computation of the multiplicative group of residue class rings of global fields and the discrete logarithm therein are presented in [Coh99] and [HPP03]. They can be easily modified for the computation of the unit group of a $\mathfrak{p}$-adic field modulo a suitable power of the maximal ideal $\mathfrak{p}$.

## 3. Class Fields

We give a short survey over local class field theory (see [Ser63] or [Iwa86]). Yamamoto [Yam58] proofs the isomorphy and the ordering and uniqueness theorems of local class field theory in a constructive way. He does not show that there is a canonical isomorphism.

**Theorem 3.1** (Isomorphy)**.** *Let $L/K$ be an abelian extension, then there is a canonical isomorphism*

$$K^*/\mathrm{N}_{L/K}(L^*) \cong \mathrm{Gal}(L/K).$$

**Theorem 3.2** (Ordering and Uniqueness)**.** *If $L_1/K$ and $L_2/K$ are abelian extensions, then*

$$\mathrm{N}_{(L_1\cap L_2)/K}\left((L_1 \cap L_2)^*\right) = \mathrm{N}_{L_1/K}(L_1^*)\mathrm{N}_{L_2/K}(L_2^*)$$

*and*

$$\mathrm{N}_{(L_1L_2)/K}\left((L_1L_2)^*\right) = \mathrm{N}_{L_1/K}(L_1^*) \cap \mathrm{N}_{L_2/K}(L_2^*).$$

*In particular an abelian extension $L/K$ is uniquely determined by its norm group $\mathrm{N}_{L/K}(L^*)$.*

The latter result reduces the problem of constructing class fields to the construction of cyclic extensions whose compositum then is the class field. The construction of tamely ramified class fields, which is well known and explicit, is given below. In order to prove the existence theorem of local class field theory, it remains to prove the existence of cyclic, totally ramified class fields of degree $p^m$ ($m \in \mathbb{N}$). We give this proof by constructing these fields (algorithm 6.1). The existence theorem for class fields of finite degree follows:

**Theorem 3.3** (Existence)**.** *Let $G \subset K^*$ be a subgroup of finite index. There exists a finite abelian extension $L/K$ with*

$$\mathrm{N}_{L/K}(L^*) = G.$$

**Tamely Ramified Class Fields.** An extension $L/K$ is called tamely ramified if $p \nmid e_{L/K}$. Tamely ramified extensions are very well understood. It is well known that the results of local class field theory can be formulated explicitly for this case.

Let $q = \#\underline{K}$. If $G$ is a subgroup of $K^*$ with $1 + \mathfrak{p}_K \subset G$ then

$$G = \langle \pi_K^F \zeta_K^S,\, \zeta_K^E \rangle \times (1 + \mathfrak{p}_K)$$

for some integers $E \mid q-1$, $F$, and $S$. There exists a unique tamely ramified extension $L/K$ with $\mathrm{N}_{L/K}(L^*) = G$, $e_{L/K} = E$, and $f_{L/K} = F$.

Denote by $T$ the inertia field of $L/K$. There exists a primitive $(q^F-1)$-th root of unity $\zeta_L \in L$, a prime element $\pi_L$ of $L$ and automorphisms $\sigma$, $\tau$ in $\mathrm{Gal}(L/K)$ such that

- $\mathrm{N}_{T/K}(\zeta_L) = \zeta_K$ and $\mathrm{N}_{L/T}(\pi_L) = \zeta_L^S \pi_K$ where $0 \leqslant t \leqslant e-1$,
- $\zeta_L^\sigma = \zeta_L^q$ and $\pi_L^{\sigma-1} \equiv \zeta_L^{\frac{q-1}{e}S} \mod \mathfrak{p}_L$,
- $\zeta_L^\tau = \zeta_L$ and $\pi_L^{\tau-1} = \zeta_K^{\frac{q-1}{e}}$.

The Galois group of $L/K$ is generated by $\sigma$ and $\tau$:

$$\mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle \cong \langle s, t \mid st = ts,\, s^F = t^{-S},\, t^E = \mathrm{id} \rangle.$$

The Galois group $\mathrm{Gal}(L/K)$ is isomorphic to $K^*/\mathrm{N}_{L/K}(L^*)$ by the map:

$$\pi_K \mapsto \sigma,\ \zeta_K \mapsto \tau,\ \eta \mapsto \mathrm{id} \text{ for all } \eta \in 1 + \mathfrak{p}_K.$$

**Wildly Ramified Class Fields.** We have seen above that subgroups of $\langle \pi_K \rangle$ correspond to unramified extensions and that subgroups of $\langle \zeta_K \rangle$ correspond to tamely ramified extensions. Subgroups of $K^*$ that do not contain all of $1 + \mathfrak{p}_K$ correspond to wildly ramified extensions.

**Lemma 3.4.** *Let $L/K$ be an abelian and wildly ramified extension, that is, $[L : K] = p^m$ for some $m \in \mathbb{N}$. Then*

$$K^*/\mathrm{N}_{L/K}(L^*) \cong (1 + \mathfrak{p}_K)/\mathrm{N}_{L/K}(1 + \mathfrak{p}_L).$$

## 4. Generating Polynomials of Ramified Extensions of Degree $p$

Let $K$ be an extension of $\mathbb{Q}_p$ of degree $n = ef$ with ramification index $e$, prime ideal $\mathfrak{p}$, and inertia degree $f$. Set $q := p^f = \#\underline{K}$. For $\alpha, \beta \in \mathcal{O}_K$ we write $\alpha \equiv \beta$ if $\nu_K(\alpha - \beta) > \nu_K(\alpha)$.

In this section we present a canonical set of polynomials that generate all extensions of $K$ of degree $p$. These were first determined by Amano [Ama71] using different methods. MacKenzie and Whaples [MW56, FV93] use $\mathfrak{p}$-adic Artin-Schreier polynomials in their description of extensions of degree $p$.

There are formulas [Kra66, PR01] for the number of extensions of a $\mathfrak{p}$-adic field of a given degree and discriminant given by:

**Theorem 4.1** (Krasner)**.** *Let $K$ be a finite extension of $\mathbb{Q}_p$, and let $j = aN + b$, where $0 \leqslant b < N$, be an integer satisfying Ore's conditions:*

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

*Then the number of totally ramified extensions of $K$ of degree $N$ and discriminant $\mathfrak{p}^{N+j-1}$ is*

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

*There are no totally ramified extensions of degree $N$ with discriminant $\mathfrak{p}_K^{N+j-1}$, if $j$ does not satisfy Ore's conditions.*

Let $j = ap + b$ satisfy Ore's conditions for ramified extensions of degree $p$ then

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

We give a set of canonical generating polynomials for every extension in $\mathbf{K}_{p,j}$ with $j$ satisfying Ore's conditions.

First, we recall Panayi's root finding algorithm [Pan95, PR01] which we apply in the proofs in this section. Second, we determine a set of canonical generating polynomials for pure extensions of degree $p$ of a $\mathfrak{p}$-adic field, that is, for the case $b = 0$. Third, 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.

**Root finding.** We use the notation from [PR01]. Let $\varphi(x) = c_n x^n + \cdots + c_0 \in \mathcal{O}_K[x]$. Denote the minimum of the valuations of the coefficients of $\varphi(x)$ by $\nu_K(\varphi) := \min\{\nu_K(c_0), \ldots, \nu_K(c_n)\}$ and define $\varphi^{\#}(x) := \varphi(x)/\pi^{\nu_K(\varphi)}$. For $\alpha \in \mathcal{O}_K$, denote its representative in the residue class field $\underline{K}$ by $\underline{\alpha}$, and for $\beta \in \underline{K}$, denote a lift of $\beta$ to $\mathcal{O}_K$ by $\widehat{\beta}$.

In order to find a root of $\varphi(x)$, we define two sequences $(\varphi_i(x))_i$ and $(\delta_i)_i$ in the following way:

- set $\varphi_0(x) := \varphi^{\#}(x)$ and
- let $\delta_0 \in \mathcal{O}_K$ be a root of $\varphi_0(x)$ modulo $\mathfrak{p}_K$.

If $\underline{\varphi_i^{\#}}(x)$ has a root $\beta_i$ then

- $\varphi_{i+1}(x) := \varphi_i^{\#}(x\pi + \widehat{\beta}_i)$ and
- $\delta_{i+1} := \widehat{\beta}_i \pi^{i+1} + \delta_i$.

If indeed $\varphi(x)$ has a root (in $\mathcal{O}_K$) congruent to $\beta$ modulo $\mathfrak{p}$, then $\delta_i$ is congruent to this root modulo increasing powers of $\mathfrak{p}$. At some point, one of the following cases must occur:

(a) $\deg(\underline{\varphi_i^{\#}}) = 1$ and $\delta_{i-1}$ is an approximation of one root of $\varphi(x)$.

(b) $\deg(\underline{\varphi_i^{\#}}) = 0$ and $\delta_{i-1}$ is not an approximation of a root of $\varphi(x)$.

(c) $\underline{\varphi_i^{\#}}$ has no roots and thus $\delta_{i-1}$ is not an approximation of a root of the polynomial $\varphi(x)$.

While constructing this sequence it may happen that $\underline{\varphi_i}(x)$ has more than one root. In this case we split the sequence and consider one sequence for each root. One shows that the algorithm terminates with either (a), (b), or (c) after at most $\nu_K(\mathrm{d}\varphi)$ iterations.

**Extensions of $\mathfrak{p}$-adic fields of discriminant $\mathfrak{p}^{p+pe-1}$.** Let $\zeta$ be a $(q-1)$-th root of unity and set $\mathcal{R} = (\rho_0, \dots, \rho_{q-1}) = (0, 1, \zeta, \zeta^2, \dots, \zeta^{q-2})$. The set $\mathcal{R}$ is a multiplicative system of representatives of $\underline{K}$ in $K$.

**Theorem 4.2.** *Let $J := \{r \in \mathbb{Z} \mid 1 \leqslant r < pe/(p-1),\ p \nmid r\}$. Each extension of degree $p$ of $K$ of discriminant $\mathfrak{p}^{p+ep-1}$ is generated by a root of exactly one of the polynomials of the form*

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

*where $\delta \in \mathcal{O}_K$ is chosen such that $x^p - x + \underline{\delta}$ is irreducible over $\underline{K}$ 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 $K$ contains the $p$-th roots of unity.*

It is obvious that a pure extension can be Galois only if $K$ contains the $p$-th roots of unity. We prepare for the proof with some auxiliary results.

**Lemma 4.3.** *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 $\mathbb{F}_q$. □

**Lemma 4.4.** *Let*

$$\varphi_t(x) = x^p + \pi + \sum_{r\in J} \rho_{c_{t,r}}\pi^{r+1} + k_t\delta\pi^{v+1} \in \mathcal{O}_K[x] \ \ (t \in \{1, 2\})$$

*where $\rho_{c_{t,r}} \in \mathcal{R}$, $v \geqslant pe/(p-1)$, and $\delta \in \mathcal{O}_K$. Let $\alpha_1$ be a zero of $\varphi_1$ and $\alpha_2$ be a zero of $\varphi_2$ in an algebraic closure of $K$.*

**(a)** *If $c_{1,r} \neq c_{2,r}$ for some $r \in J$, then $K(\alpha_1) \ncong K(\alpha_2)$.*

**(b)** *If $c_{1,r} = c_{2,r}$ for all $r \in J$, if $K$ contains the $p$-th roots of unity, $\delta$ is chosen such that $x^p - x + \underline{\delta}$ is irreducible, $v = pe/(p-1)$, and $k_1 \neq k_2$ then $K(\alpha_1) \ncong K(\alpha_2)$.*

*Proof.* Let $L_1 := K(\alpha_1)$ and let $\mathfrak{p}_1$ denote the maximal ideal of $L_1$.
**(a)** We use Panayi's root-finding algorithm to show that $\varphi_2(x)$ does not have any roots over $K(\alpha_1)$. As $\varphi_2(x) \equiv x^p \bmod (\pi)$, we set $\varphi_{2,1}(x) := \varphi_2(\alpha_1 x)$. Then

$$\begin{aligned}\varphi_{2,1}(x) &= \alpha_1^p x^p + \pi + \sum_{r\in J} \rho_{c_{2,r}} \pi^{r+1} + k_2\delta\pi^{v+1} \\ &= \Big(-\pi - \sum_{r\in J} \rho_{c_{1,r}} \pi^{r+1} - k_1\delta\pi^{v+1}\Big) x^p + \pi + \sum_{r\in J} \rho_{c_{2,r}} \pi^{r+1} + k_2\delta\pi^{v+1} \\ &\equiv \pi(-x^p + 1).\end{aligned}$$

Hence $\varphi_{2,1}^{\#}(x) = \varphi_{2,1}(x)/\pi \equiv -x^p + 1$ and we set

$$\begin{aligned}\varphi_{2,2}(x) &:= \varphi_{2,1}^{\#}(\alpha_1 x + 1) \\ &= \Big(-1 - \sum_{r\in J} \rho_{c_{1,r}} \pi^{r} - k_1\delta\pi^{v}\Big)(\alpha_1 x + 1)^p + 1 + \sum_{r\in J} \rho_{c_{2,r}} \pi^{r} + k_2\delta\pi^{v} \\ &\equiv \Big(-1 - \sum_{r\in J} \rho_{c_{1,r}} \pi^{r} - k_1\delta\pi^{v}\Big)\alpha_1^p x^p + 1 + \sum_{r\in J} \rho_{c_{2,r}} \pi^{r} + k_2\delta\pi^{v}.\end{aligned}$$

Let $\underline{\beta_i}$ be a root of $\varphi_{2,i+2}^{\#}$. Let $m$ be minimal with $c_{1,m} = c_{2,m}$. Then $\beta_m \neq 0$. Let $m < u < pe/(p-1)$. Assume that the root-finding algorithm does not terminate with $\deg \varphi_{2,w}^{\#} = 0$ for some $m \leqslant w \leqslant u$. After $u$ iterations of the root-finding algorithm, we have

$$\begin{aligned}\varphi_{2,u+1}(x) = \Big(-1 - \sum_{r\in J} &\rho_{c_{1,r+1}} \pi^{r} - k_1\delta\pi^{v}\Big) \\ &\cdot\ (\alpha_1^u x + \beta_{u-1}\alpha_1^{u-1} + \cdots + \beta_m\alpha_1^m + 1)^p \\ &+\ 1 + \sum_{r\in J} \rho_{c_{2,r+1}} \pi^{i} + + k_2\delta\pi^{v-1} \\ \equiv -\alpha_1^{pu} x^p - p\alpha_1^u x - p\beta_m\alpha_1^m &+ \sum_{r\in J, r\geqslant m} (\rho_{c_{2,r+1}} - \rho_{c_{1,r+1}})\pi^r.\end{aligned}$$

The minimal valuation of the coefficients of $\varphi_{2,u+1}(x)$ is either $\nu_{L_1}(\alpha_1^{pu}) = pu$ or $\nu_{L_1}(p\beta_m\alpha_1^m) = pe + m$. As $\gcd(p, m) = 1$ and $m < pe/(p-1)$, there exists $u \in \mathbb{N}$ such that the polynomial $\varphi_{2,u+1}^{\#}(x)$ is constant. Thus the root-finding algorithm terminates with the conclusion that $\varphi_2(x)$ is irreducible over $K(\alpha_1)$.
**(b)** We set $\varphi_{2,1}(x) := \varphi_2(\alpha_1 x)$ and $\varphi_{2,2}(x) := \varphi_1^{\#}(\alpha_1 x + 1)$. After $v+$

1 iterations of the root-finding algorithm we obtain $\varphi_{2,v+2}(x) \equiv -\alpha_1^{vp}x^p - p\alpha_1^v x + (k_2 - k_1)\delta\pi^v$. By lemma 4.3 $\underline{\varphi^{\#}_{2+v}(x)}$ is irreducible for $k_1 \neq k_2$. Therefore, $\varphi_2(x)$ has no root in $K(\alpha_1)$ and $\varphi_1(x)$ and $\varphi_2(x)$ generate non-isomorphic extensions over $K$. □

*Proof of theorem 4.2.* We will show that the number of extensions given by the polynomials $\varphi(x)$ is greater then or equal to the number of extensions given by theorem 4.1. The number of elements in $J$ is $e$ (see section 2).

By lemma 4.4 (a), the roots of two polynomials generate non-isomorphic extensions if the coefficients $\rho_{c_i}$ differ for at least one $i \in J$. For every $i$ we have the choice among $p^f = q$ values for $\rho_{c_i}$. This gives $q^e$ polynomials generating non-isomorphic extensions.

If $K$ does not contain the $p$-th roots of unity, then an extension generated by a root $\alpha$ 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 $K$. Thus our set of polynomials generates all $pq^e$ extensions.

If $K$ contains the $p$-th roots of unity, then lemma 4.4 (b) gives us $p-1$ additional extensions for each of the polynomials from lemma 4.4 (a). 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 4.5.** *Let* $J := \{r \in \mathbb{Z} \mid 1 \leqslant r < (ap+b)/(p-1),\ p \nmid (b+r)\}$ *and if* $(p-1) \mid (a+b)$, *set* $v = (ap+b)/(p-1)$. *Each extension of degree* $p$ *of* $K$ *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*

$$\varphi(x) = \begin{cases} x^p + \zeta^s \pi^{a+1} x^b + \pi + \sum\limits_{i \in J} \rho_{c_i} \pi^{i+1} + k\delta\pi^{v+1} & \text{if} \begin{cases} (p-1) \mid (a+b) \text{ and} \\ x^{p-1} + (-1)^{ap+1}\underline{\zeta^s b} \\ \text{has } p-1 \text{ roots}, \end{cases} \\ x^p + \zeta^s \pi^{a+1} x^b + \pi + \sum\limits_{i \in J} \rho_{c_i} \pi^{i+1} & \text{otherwise,} \end{cases}$$

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

**Lemma 4.6.** *Let*

$$x^p + \zeta^{s_t}\pi^{a+1}x^b + \pi + \sum_{r \in J} \rho_{c_{t,r}} \pi^{r+1} + k_t\delta_t\pi^{v+1} \in \mathcal{O}_K[x] \quad (t \in \{1,2\})$$

*where* $\rho_{t,r} \in \mathcal{R}$, $v \geqslant \frac{ap+b}{p-1}$, *and* $\delta_t \in \mathcal{O}_K$. *Let* $\alpha_1$ *be a zero of* $\varphi_1$ *and* $\alpha_2$ *be a zero of* $\varphi_2$ *in an algebraic closure of* $K$.

**(a)** *If* $s_1 \neq s_2$, *then* $K(\alpha_1) \ncong K(\alpha_2)$.

**(b)** *If $s_1 = s_2$ and $c_{1,r} \neq c_{2,r}$ for some $r \in J$ then $K(\alpha_1) \ncong K(\alpha_2)$.*

**(c)** *$K(\alpha_1)/K$ is Galois if and only if $a + b \equiv 0 \bmod (p-1)$ and $x^{p-1} + (-1)^{ap+1}\underline{\zeta^{s_1} b}$ is reducible over $\underline{K}$.*

**(d)** *Assume $s_1 = s_2$ and $c_{1,r} = c_{2,r}$ for all $r \in J$. If $(p-1) \mid (ap+b)$, then for $v = \frac{ap+b}{p-a}$ there exists $\delta \in \mathcal{O}_K$ such that $K(\alpha_1) \ncong K(\alpha_2)$ if $k_1 \neq k_2$.*

*Proof.* Let $L_1 := K(\alpha_1)$.
**(a)** For $t \in \{1, 2\}$ let $\gamma_t = \sum_{r \in J} \rho_{c_{t,r}} \pi^r + k_t \delta_t \pi^v$. Then $\alpha_1^p/\pi = -\zeta^{s_1} \pi^a \alpha^b - 1 - \gamma_1$. We use Panayi's root-finding algorithm to show that $\varphi_2(x)$ has no root over $L_1 = K(\alpha_1)$. As before, we get $\varphi_{2,1}(x) := \varphi_2(\alpha_1 x) \equiv \pi(-x^p + 1)$. Therefore we set

$$\begin{aligned}\varphi_{2,2}(x) &:= \varphi_{2,1}^{\#}(\alpha_1 x + 1) \\ &= (-\zeta^{s_1} \pi^a \alpha^b - 1 - \gamma_1)(\alpha_1 x + 1)^p + \zeta^{s_2} \pi^a \alpha^b (\alpha_1 x + 1)^b + 1 + \gamma_2.\end{aligned}$$

Let $2 \leqslant u \leqslant pe/(p-1)$. Let $\underline{\beta_i} \in \mathcal{R}$ be a root of $\underline{\varphi_{2,i}^{\#}(x)}$. Assume that the root-finding algorithm does not terminate with $\deg \underline{\varphi_{2,w}^{\#}} = 0$ for some $2 \leqslant w \leqslant u$ and let $m$ be minimal with $m < u < pe/(p-1)$ and $\beta_m \not\equiv 0 \bmod (\alpha)$. After $u$ iterations of the root-finding algorithm, we have

$$\begin{aligned}\varphi_{2,u+1}(x) = (-\zeta^{s_1} \pi^a \alpha_1^b - 1 - \gamma_1)(\alpha_1^u x + \beta_{u-1} \alpha_1^{u-1} + \cdots + \beta_m \alpha_1^m + 1)^p \\ + \zeta^{s_2} t \pi^a \alpha^b (\alpha_1^u x + \beta_{u-1} \alpha_1^{u-1} + \cdots + \beta_m \alpha_1^m + 1)^b + 1 + \gamma_2 \pi.\end{aligned}$$

Because $u \leqslant e$, $\nu_{L_1}(p) = pe$, and $a < e$, the minimal valuation of the coefficients of $\varphi_{2,u+1}(x)$ is either $\nu_{L_1}(-\alpha_1^{pu}) = pu$ or $\nu_{L_1}(\pi^a \alpha_1^b) = pa + b$. Hence the root-finding algorithm terminates with $\varphi_{2,u+1}(x) \equiv (\zeta^{s_2} - \zeta^{s_1}) \pi^a \alpha^b$ for some $u$ in the range $2 \leqslant u \leqslant e$.

**(b)** We show that $\varphi_2(x)$ does not have any roots over $L_1$. As $\varphi_2(x) \equiv x^p \bmod (\pi)$, we get $\varphi_{2,1}(x) := \varphi_2(\alpha x)$. Now $\varphi_{2,1}^{\#}(x) \equiv -x^p + 1$ and we set $\varphi_{2,2}(x) := \varphi_{2,1}^{\#}(\alpha_1 x + 1)$.

Denote by $\underline{\beta_r}$ a root of $\underline{\varphi_{2,r+1}^{\#}(x)}$. Let $m$ be minimal with $m < u < pe/(p-1)$ and $\beta_m \not\equiv 0 \bmod \underline{(\alpha)}$. Assume that the root-finding algorithm does not terminate earlier with $\deg \underline{\varphi_{2,w}^{\#}} = 0$ for some $w \leqslant u$. After $u$

iterations, we have

$$\begin{aligned}\varphi_{2,u+1}(x) &= \Big(-\zeta^{s_1}\pi^a\alpha_1^b - 1 - \sum_{r\in J}\rho_{c_{1,r+1}}\pi^i - \rho_{c_{1,a+2}}\pi^{a+1}\Big)\\ &\quad\cdot(\alpha_1^u x + \beta_{u-1}\alpha_1^{u-1} + \cdots + \beta_m\alpha_1^m + 1)^p\\ &\quad+\zeta^{s_1}\pi^a\alpha_1^b(\alpha^u x + \beta_{u-1}\alpha_1^{u-1} + \cdots + \beta_m\alpha_1^m + 1)^b + 1\\ &\quad+\sum_{r\in J}\rho_{c_{2,r+1}}\pi^r + \rho_{c_{2,a+1}}\pi^{a+1}\\ &\equiv -\alpha^{pu}x^p - p\alpha_1^u x - p\beta_m\alpha_1^m - \sum_{r\in J}\rho_{c_{1,r+1}}\pi^r(\beta_m\alpha_1^m)^p - (\beta_m\alpha_1^m)^p\\ &\quad+\zeta^{s_1}\pi^a\alpha_1^b b\alpha_1^u x + \zeta^{s_1}\pi^a\alpha_1^b b\beta_m\alpha^m + \sum_{r\in J}(\rho_{c_{2,r+1}} - \rho_{c_{1,r+1}})\pi^r,\end{aligned}$$

with $\beta_m \not\equiv 0 \bmod (\alpha_1)$.

The minimal valuation of the terms of $\varphi_{2,u+1}(x)$ is

$$\nu_{L_1}(\zeta^{s_1}\pi^a\alpha_1^b b\beta_m\alpha_1^m) = pa + b + m$$

or $\nu_{L_1}(\alpha_1^{pr}) = pr$. By the choice of $J$ we have $p \nmid (pa+b+m)$. Therefore, the root-finding algorithm terminates with $\varphi_{2,u}(x) \equiv \zeta^s\pi^a\alpha_1^b b\beta_m\alpha^m$ for some $u \in \mathbb{N}$.

**(c)** We show that $\varphi_1(x)$ splits completely over $L_1$ if and only if the conditions above are fulfilled. We set $\varphi_{1,1}(x) := \varphi_1(\alpha_1 x)$ and $\varphi_{1,2}(x) := \varphi_{1,1}^{\#}(\alpha x + 1)$. Thus

$$\begin{aligned}\varphi_{1,2}(x) &= \big(-\zeta^{s_1}\pi^a\alpha_1^b - 1 - \textstyle\sum_{r\in J}\rho_{c_{1,r}}\pi^r\big)(\alpha_1 x + 1)^p\\ &\quad+\zeta^{s_1}\pi^a\alpha^b(\alpha_1 x + 1)^b + 1 + \textstyle\sum_{r\in J}\rho_{c_{1,r}}\pi^r\\ &\equiv x(-\alpha_1^p x^{p-1} + \zeta^{s_1}\pi^a\alpha_1^{b+1}b).\end{aligned}$$

After $u+1$ iterations we get

$$\varphi_{1,u+1}(x) \equiv \begin{cases} -\alpha_1^{up}x^p & \text{if } up < pa+b+u,\\ x(-\alpha_1^{up}x^{p-1} + \zeta^{s_1}\pi^a\alpha_1^{b+u}b) & \text{if } up = pa+b+u,\\ \zeta^{s_1}\pi^a\alpha_1^{b+1}bx & \text{if } \begin{cases} up > pa+b+u \text{ and}\\ (p-1)\nmid(a+b).\end{cases}\end{cases}$$

In the third case, $\varphi_{1,u+1}^{\#}(x)$ is linear and therefore $\varphi_1(x)$ has only one root over $L_1$. In the second case,

$$\varphi_{u+1}(x) \equiv -\alpha_1^{up}x^p + \zeta^{s_1}\pi^a\alpha_1^{b+u}bx \equiv -\alpha_1^{up}x^p + \zeta^{s_1}(-\alpha_1)^{ap}\alpha^{b+u}x$$

and so $\varphi^{\#}_{1,u+1}(x) \equiv -x^p + (-1)^{ap}\zeta^{s_1} bx \bmod (\alpha_1)$. If $\underline{\varphi^{\#}_{u+1}}(x)$ has $p$ roots over $\underline{K}$ for every root $\underline{\beta}$ of $\underline{\varphi^{\#}_{1,u+1}}(x)$, we get

$$\begin{aligned}\varphi_{1,u+2}(x) &= \varphi_{1,u+1}(\alpha_1 x + \beta)\\ &\equiv -\alpha_1^{(u+1)p}x^p + (-1)^{ap}\alpha_1^{u+1}\beta\zeta^{s_1}\pi^a\alpha_1^b + (-1)^{ap}\alpha_1^{u+1}b\beta^b\zeta^{s_1}\pi^a\alpha_1^b x.\end{aligned}$$

But $up+p > u+1+pa+b$; thus $\underline{\varphi^{\#}_{1,u+2}}(x)$ is linear and $\varphi_1(x)$ has as many distinct roots as $\underline{\varphi^{\#}_{1,u+1}}(x)$.

**(d)** We set $\varphi_{2,1}(x) := \varphi(\alpha x)$ and $\varphi_{2,2}(x) := \varphi^{\#}_{2,1}(\alpha x + 1)$. We obtain $\varphi_{2,v+1}(x) \equiv -\alpha_1^{vp}x^p + \zeta^{s_1}\pi^a\alpha_1^{b+v}bx + (k_1-k_2)\delta\pi^v$, hence $\underline{\varphi^{\#}_{v+1}(x)} = x^p + (-1)^{ap+1}\zeta^{s_1}bx + (k_1-k_2)\delta$. By lemma 4.3, there exists $\delta \in \mathcal{O}_K$ such that $\underline{\varphi^{\#}_{2,v+1}(x)}$ is irreducible. □

*Proof of theorem 4.5.* If $(p-1) \nmid (a+b)$, then

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

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

$$\#J = a + \tfrac{a+b}{p-1} - 1 - \left\lfloor \tfrac{a+b}{p} + \tfrac{a+b}{p(p-1)} - 1 \right\rfloor - \left\lfloor \tfrac{b}{p} \right\rfloor = a + \tfrac{a+b-1}{p-1} - \left\lfloor \tfrac{a+b-1}{p-1} \right\rfloor = a.$$

Using lemma 4.6 (a), we get $p^f - 1$ sets of generating polynomials. By lemma 4.6 (b), 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 the extension generated by any root is cyclic. In the latter case, we have $p-1$ additional polynomials generating one extension each by lemma 4.6 (d). Thus we obtain $(p^f-1)p^{af+1}$ distinct extensions. □

**Number of Galois Extensions.** The following result can also easily be deduced from class field theory.

**Corollary 4.7.** *Let $K$ be an extension of $\mathbb{Q}_p$ of degree $n$. If $K$ does not contain the $p$-th roots of unity, then the number of ramified Galois extensions of $K$ of degree $p$ is $p \cdot \frac{p^n-1}{p-1}$. If $K$ contains the $p$-th roots of unity then the number of ramified Galois extensions of $K$ of degree $p$ is $p \cdot \frac{p^{n+1}-1}{p-1}$.*

*Proof.* Let $\varphi(x)$ be as in theorem 4.5. We denote the inertia degree and the ramification index of $K$ by $f$ and $e$, respectively. The number of values of $s$ for which $x^{p-1} - \zeta^s$ is reducible is $(p^f-1)/(p-1)$. By Ore's conditions, $0 \leqslant a \leqslant e$. For every $a < e$, there is exactly one $b$ with $1 \leqslant b < p$ such that $(p-1) \mid (a+b)$. For every $a$, the set $J$ contains $a$ elements. This gives

$p^{fa}$ combinations of values of $c_i$, $i \in J$. We have $p$ choices for $k$. Thus the number of polynomials $\varphi(x)$ generating Galois extensions is

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

If $K$ contains the $p$-the roots of unity, $a = e$ also yields Galois extensions. By theorem 4.2, we obtain additional $p(p^f)^e = p^{n+1}$ extensions. □

## 5. Ramified Abelian Extensions of Degree $p$

Let $L/K$ be an abelian ramified extension of degree $p$. The ramification number (*Verzweigungszahl*) of $L/K$ is defined as $v = v_{L/K} = \nu_L(\pi_L^{\sigma-1} - 1)$, where $\sigma \in \mathrm{Gal}(L/K) \setminus \{\mathrm{id}\}$. The ramification number $v$ is independent of the choice of $\sigma$. If $\varphi$ is the minimal polynomial of $\pi_L$, then

$$\begin{aligned} \nu_L(\mathrm{d}(\varphi)) &= \sum_{i \neq j} \nu_L\big(\sigma^i(\pi_L) - \sigma^j(\pi_L)\big) \\ &= \sum_{i=1}^{p(p-1)} \nu_L\big(\sigma(\pi_L) - \pi_L\big) \;=\; p(p-1)(v+1). \end{aligned}$$

Hence, $\nu_K(\mathrm{d}_{L/K}) = (p-1)(v+1)$ for the discriminant of $L/K$ and $\mathcal{D}_{L/K} = \mathfrak{p}_L^{(p-1)(v+1)}$ for the different of the extension. It follows from Ore's conditions (see Theorem 4.1) that either $v = p\frac{e_K}{p-1}$ or $v = \frac{ap+b}{p-1} \in F_K$ where $j = ap + b$ satisfies Ore's conditions.

**Lemma 5.1.** *Let $L/K$ be a ramified extension of degree $p$. If $d := \nu_L(\mathcal{D}_{L/K}) = (p-1)(v+1)$, then*

$$\mathrm{T}_{L/K}(\mathfrak{p}_L^m) = \mathfrak{p}_K^{\left\lfloor \frac{m+d}{e_{L/K}} \right\rfloor}.$$

See [FV93, section 1.4] for a proof. We use Newton's relations to investigate the norm group of abelian extensions of degree $p$.

**Proposition 5.2** (Newton's relations)**.** *Let $\vartheta = \vartheta^{(1)}, \ldots, \vartheta^{(n)}$ be the roots of a monic polynomial $\varphi = \sum_{0 \leqslant i \leqslant n} \gamma_i x^i$. Then $\gamma_i = (-1)^{(n-i)} R_{n-i}(\vartheta)$ where $R_{n-i}(\vartheta)$ is the $(n-i)$-th symmetric function in $\vartheta^{(1)}, \ldots, \vartheta^{(n)}$. Set $S_k(\vartheta) = \sum_{i=1}^n \big(\vartheta^{(i)}\big)^k$ for each integer $k \geqslant 1$. Then*

$$S_k(\vartheta) = \begin{cases} -k\gamma_{n-k} - \sum_{i=1}^{k-1} \gamma_{n-i} S_{k-i}(\vartheta) & \text{for } 1 \leqslant k \leqslant n, \text{ and} \\ \qquad\quad - \sum_{i=1}^{n} \gamma_{n-i} S_{k-i}(\vartheta) & \text{for } k > n. \end{cases}$$

The following describes explicitly where and how the jump in the norm group takes place (c.f. [FV93, section 1.5]).

**Lemma 5.3.** *Let $L/K$ be ramified abelian of degree $p$ and let $v$ denote the ramification number of $L/K$. Let $\langle\sigma\rangle = \mathrm{Gal}(L/K)$. Assume that $\mathrm{N}_{L/K}(\pi_L) = \pi_K$. Let $\varepsilon \in K$ be chosen such that $\pi_L^{\sigma-1} \equiv 1 + \varepsilon\pi_L^v \bmod \mathfrak{p}^{v+1}$. Then*

$$\begin{aligned}
\mathrm{N}_{L/K}(1+\alpha\pi_L^i) &\equiv 1+\alpha^p\pi_K^i && \bmod \mathfrak{p}_K^{i+1} && \text{if } i<v,\\
\mathrm{N}_{L/K}(1+\alpha\pi_L^v) &\equiv 1+(\alpha^p-\varepsilon^{p-1}\alpha)\pi_K^v && \bmod \mathfrak{p}_K^{v+1}, && \text{and}\\
\mathrm{N}_{L/K}(1+\alpha\pi_L^{v+p(i-v)}) &\equiv 1-\varepsilon^{p-1}\alpha\pi_K^i && \bmod \mathfrak{p}_K^{i+1} && \text{if } i>v.
\end{aligned}$$

*The kernel of the endomorphism $\underline{K}^+ \to \underline{K}^+$ given by $\underline{\alpha} \mapsto \underline{\alpha}^p - \underline{\varepsilon}^{p-1}\underline{\alpha}$ has order $p$.*

*Proof.* We have

$$\mathrm{N}_{L/K}(1+\omega\pi_L^i) = 1 + \omega R_1(\pi_L^i) + \omega^2 R_2(\pi_L^i) + \cdots + \omega^p R_p(\pi_L^i),$$

where $R_k(\pi_L^i)$ denotes the $k$-th symmetric polynomial in $\pi_L^i, \pi_L^{\sigma i}, \ldots, \pi_L^{\sigma^{p-1}i}$. In particular $R_1(\pi_L^i) = \mathrm{T}_{L/K}(\pi_L^i)$ and $R_p(\pi_L^i) = \mathrm{N}_{L/K}(\pi_L)^i$. By lemma 5.1 and $\nu_L(\mathcal{D}_{L/K}) = (v+1)(p-1)$, we obtain

$$S_k(\pi_L^i) = \mathrm{T}_{L/K}(\pi_L^{ki}) \in \mathrm{T}_{L/K}(\mathfrak{p}_L^{ki}) \subset \mathfrak{p}_K^{\lambda_{ki}}$$

where

$$\lambda_{ki} = \left\lfloor \tfrac{(p-1)(v+1)+ki}{p} \right\rfloor = v+1+\left\lfloor \tfrac{-v-1+ki}{p} \right\rfloor = v+\left\lceil \tfrac{ki-v}{p} \right\rceil = v-\left\lfloor \tfrac{v-ki}{p} \right\rfloor.$$

(i) If $i<v$, then $i<\lambda_1 = v-\left\lfloor\frac{v-i}{p}\right\rfloor$ and $\nu_K(S_k(\pi_L^i)) \geqslant \lambda_k \geqslant \lambda_1 > i$. With Newton's relations we get $\nu_K(R_k(\pi_L^i)) > i$ for $1 \leqslant k \leqslant p-1$ and as $R_p(\pi_L^i) = \mathrm{N}_{L/K}(\pi_L)^i = \pi_K^i$, we obtain

$$\mathrm{N}_{L/K}(1+\alpha\pi_L^i) \equiv 1+\alpha^p\pi_K^i \mod \mathfrak{p}_K^{i+1}.$$

(ii) Assume $i=v$. By lemma 5.1 $\mathrm{T}_{L/K}(\mathfrak{p}_L^v) = \mathfrak{p}_K^{\lambda_v}$, and so $\mathrm{T}_{L/K}(\pi_L^v) \equiv \beta\pi_K^v \bmod \mathfrak{p}_K^{v+1}$ for some $\beta \in {\mathcal{O}_K}^*$. We have $\lambda_k = v+\left\lceil\frac{(k-1)v}{p}\right\rceil > v$. If $k \geqslant 2$ then $\nu_K(S_k(\pi_L^i)) \geqslant \lambda_k \geqslant v+1$. Hence with Newton's relations $\nu_K(R_k(\pi_L^i)) \geqslant \min(kv, v+1) \geqslant v+1$ for $2 \leqslant k \leqslant p-1$. Thus $\mathrm{N}_{L/K}(1+\alpha\pi_L^v) \equiv 1+\alpha\beta\pi_K^v + \alpha^p\pi_K^v \bmod \mathfrak{p}_K^{v+1}$ and $\mathrm{N}_{L/K}(1+\pi_L^v) \subset (1+\mathfrak{p}_K)^v$. By the definition of $\varepsilon$ and as $\mathrm{N}_{L/K}(\pi_L^{\sigma-1}) = 1$ we have $\mathrm{N}_{L/K}(1+\varepsilon\pi_L^v) \equiv 1 \bmod \mathfrak{p}_K^{v+1}$. Therefore $\beta \equiv -\varepsilon^{p-1} \bmod \mathfrak{p}_K$ and we conclude that

$$\mathrm{N}_{L/K}(1+\alpha\pi_L^v) \equiv 1+(\alpha^p-\varepsilon^{p-1}\alpha)\pi_K^v \mod \mathfrak{p}_K^{v+1}.$$

(iii) Let $i>v$. We have $\lambda_{v+p(i-v)} = i$ and $\lambda_{k(v+p(i-v))} > i$. By the considerations in (ii), we obtain

$$\mathrm{N}_{L/K}(1+\alpha\pi_L^{v+p(i-v)}) \equiv 1-\varepsilon^{p-1}\alpha\pi_K^i \mod \mathfrak{p}_K^{i+1}.$$

□

Next we investigate the relationship between the minimal polynomial of $\pi_L$, a uniformizer of the field $L$, and the norm group $\mathrm{N}_{L/K}(L^*)$. We start by choosing a suitable representation for subgroups of $K^*$ of index $p$. We begin with extensions of discriminant $\mathfrak{p}^{p+e_{L/K}-1}$, which are Galois if and only if $K$ contains the $p$-the roots of unity.

If $K$ contains the $p$-th roots of unity then

$$K^* = \langle \zeta_K \rangle \times \langle \pi_K \rangle \times \langle \eta_{\lambda,i} \mid \lambda \in F_K, 1 \leqslant i \leqslant f_K; \eta_* \rangle$$

Let $G$ be a subgroup of $K^*$ of index $p$ with $\eta_* \notin G$. Let $(g_1, ..., g_{e_K f_K+3})$ be generators of $G$. Let $n = e_K f_K$ and $B \in \mathbb{Z}^{n+3 \times n+3}$ such that

$$(g_1, ..., g_{e_K f_K+3})^T = B(\zeta_K, \pi_K,\ \eta_{\lambda,i} \mid \lambda \in F_K, 1 \leqslant i \leqslant f_K, \eta_*)^T$$

be a representation matrix of $G$. Let $A$ be the row Hermite normal form of $B$. Then

$$A = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 & a_\pi \\ 0 & 1 & 0 & & & 0 & 0 \\ \vdots & 0 & 1 & 0 & \cdots & 0 & a_{1,1} \\ \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & & \ddots & \ddots & 0 & \vdots \\ \vdots & & & & \ddots & 1 & a_{v-1,f} \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & p \end{pmatrix}.$$

Thus

$$G = \langle \pi_K \eta_*^{a_\pi};\ \zeta_K;\ \eta_{\lambda,i} \eta_*^{a_{\lambda,i}} \mid \lambda \in F_K, 1 \leqslant i \leqslant f_K;\ \eta_*^p \rangle \ \ (t \in \{1,2\}).$$

**Theorem 5.4.** *Assume that $K$ contains the $p$-th roots of unity. Let*

$$\varphi_t(x) = x^p + \pi + \sum_{r \in J} \rho_{c_{t,r}} \pi^{r+1} + k_t \delta \pi^{v+1} \in \mathcal{O}_K[x] \ \ (t \in \{1,2\})$$

*be polynomials as in theorem 4.2. If $L_1 := K[x]/(\varphi_1)$ and $L_2 := K[x]/(\varphi_2)$, then $v = v_{L_1/K} = v_{L_2/K} = pe_K/(p-1)$. Hence*

$$\mathrm{N}(L_t^*) = \langle \pi_K \eta_*^{a_{t,\pi}};\ \zeta_K;\ \eta_{\lambda,i} \eta_*^{a_{t,\lambda,i}} \mid \lambda \in F_K, 1 \leqslant i \leqslant f_K;\ \eta_*^p \rangle \ \ (t \in \{1,2\}).$$

**(a)** *Let $w \in J = \{1 \leqslant r \leqslant pe/(p-1) \mid p \nmid r\}$. We have $c_{1,r} = c_{2,r}$ for $1 \leqslant r < w$, $r \in J$ if and only if $a_{1,v-r,i} = a_{2,v-r,i}$ for all $1 \leqslant r < w$, $r \in J$ and all $1 \leqslant i \leqslant f_K$.*

**(b)** *If $c_{1,r} = c_{2,r}$ for all $r \in J$, then $k_1 = k_2$ if and only if $a_{1,\pi} = a_{2,\pi}$.*

*Proof.* **(a)** We show one implication directly. The other implication follows by a counting argument.

(i) As $p \mid (v - \lambda)$ if and only if $p \mid \lambda$ we have $v - r \in F_K$ if and only if $r \in J$.

(ii) Let $\pi_t$ be a root of $\varphi_t$. We write $\varphi_t = x^p - \gamma_t$. The minimal polynomial of $\pi_t^\lambda$ over $K$ is $x^p - \gamma_t^\lambda$. The characteristic polynomial of $\omega \pi_t^\lambda$ is

$x^p+\omega^p\gamma_t^\lambda$. The characteristic polynomial of $1+\omega\pi_t^\lambda$ is $(x-1)^p-\alpha^p\omega^\lambda$. Thus $\mathrm{N}_{L_t/K}(1+\omega\pi_t^\lambda)=(-1)^p-\omega^p\gamma_t^\lambda$. If $\gamma_1=\gamma_2+\alpha\pi_K^{w+1}$ for some $\alpha\in{\mathcal{O}_K}^*$ then for $r\leqslant w$ we obtain

$$\gamma_1^{v-r}=(\gamma_2+\pi_K^{w+1}\alpha)^{v-r}\equiv\gamma_2^{v-r}+(v-r)\gamma_2^{v-r-1}\alpha\pi_K^{w+1}\mod\mathfrak{p}_K^{v+1}.$$

(iii) Assume that $c_{1,r}=c_{2,r}$ for all $1\leqslant r<w$. For all $r\leqslant w-1$ we obtain

$$\mathrm{N}_{L_1/K}(1+\omega\pi_{L_1}^{v-r})=(-1)^p+\omega^p\gamma_1^{v-r}\equiv\mathrm{N}_{L_2/K}(1+\omega\pi_{L_1}^{v-r})\mod\mathfrak{p}_K^{v+1}$$

which implies $a_{1,v-r,i}=a_{2,v-r,i}$ for all $1\leqslant r<w$ and $1\leqslant i\leqslant f_K$.
(iv) If $c_{1,w}\neq c_{2,w}$ for $r=w$ we have

$$\mathrm{N}_{L_2/K}(1+\omega\pi_{L_2}^{v-w})=(-1)^p+\omega^p\gamma_2^{v-w}$$

and

$$\mathrm{N}_{L_1/K}(1+\omega\pi_{L_1}^{v-w})\equiv(-1)^p+\omega^p(\gamma_2^{v-w}+(v-w)\gamma_2^{v-w-1}\pi_K^{w+1}\alpha)\mod\mathfrak{p}_K^{v+1}.$$

By (i), $p\nmid(v-w)$ and as $\nu_K(\gamma_2)=1$, it follows that $a_{1,w,i}\neq a_{2,w,i}$.
(v) There are $p^f$ choices for each $\rho_{c_{t,r}}$. On the corresponding level $\lambda=v-r$ there are $f$ generating principal units $\eta_{\lambda,1},\dots,\eta_{\lambda,1}$ with in total $p^f$ choices for the exponents $a_{t,\lambda,1},\dots,a_{t,\lambda,f}$. This shows the equivalence.
**(b)** We have

$$\mathrm{N}_{L_t/K}(\pi_{L_t})\equiv\pi_K+\sum_{r\in J}\rho_{c_{t,r}}\pi_K^{r+1}+k_t\delta\pi_K^{v+1}\equiv\pi_K\left(\prod_{\lambda,i}\eta_{\lambda,i}^{a_{t,\lambda,i}}\cdot\eta_*^{a_{t,\pi}}\right)\mod\mathfrak{p}_K^{v+2}.$$

Since $c_{1,r}=c_{2,r}$ for all $r\in J$, we have $a_{1,\lambda,i}=a_{2,\lambda,i}$ for all $\lambda\in F_{L_t}$, $1\leqslant i\leqslant f$. Thus $k_1=k_2$ is equivalent to $a_{1,\pi}=a_{2,\pi}$. □

If $K$ does not contain the $p$-th roots of unity then

$${K^*}=\langle\pi_K\rangle\times\langle\zeta_K\rangle\times\prod_{\lambda\in F_K}\prod_{1\leqslant i\leqslant f_K}\langle\eta_{\lambda,i}\rangle.$$

Let $G$ be a subgroup of ${K^*}$ of index $p$ and let $A$ be the row Hermite normal form of the representation matrix of $G$. There are values $\lambda_0\in F_K$,

$1 \leqslant i_0 \leqslant f_K$, $a_\pi \in \{0, \dots, p-1\}$, $a_{\lambda,i} \in \{0, \dots, p-1\}$ for $(\lambda, i) \in F_K \times \{1, \dots, f_K\} \setminus \{(\lambda_0, i_0)\}$ with $\lambda \leqslant \lambda_0$, $i \leqslant i_0$ and $a_{\lambda_0,i_0} = p$, such that

$$A = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 & a_\pi & 0 & \cdots & 0 \\ 0 & 1 & 0 & & & 0 & 0 & 0 & & \vdots \\ \vdots & 0 & 1 & 0 & \cdots & 0 & a_{1,1} & 0 & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ \vdots & & & \ddots & \ddots & 0 & \vdots & \vdots & & \vdots \\ \vdots & & & & \ddots & 1 & \vdots & \vdots & & \vdots \\ \vdots & & & & & 0 & a_{\lambda_0,i_0} & 0 & & \vdots \\ \vdots & & & & & & 0 & 1 & \ddots & \vdots \\ \vdots & & & & & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

Thus $G$ can be generated as follows

$$G = \langle \pi_K \eta_{\lambda_0,i_0}^{a_\pi};\ \zeta_K;\ \eta_{\lambda,i} \eta_{\lambda_0,i_0}^{a_{\lambda,i}} \mid \lambda \in F_K, \lambda < \lambda_0, 1 \leqslant i \leqslant f_K;$$

$$\eta_{\lambda_0,i} \eta_{\lambda_0,i_0}^{a_{\lambda_0,i}} \mid 1 \leqslant i < i_0;\ \eta_{\lambda_0,i_0}^{p};\ \eta_{\lambda_0,i} \mid i_0 < i \leqslant f_K;$$

$$\eta_{\lambda,i} \mid \lambda \in F_K, \lambda_0 < \lambda, 1 \leqslant i \leqslant f_K \rangle.$$

By lemma 5.3, we have $\lambda_0 = v_{L/K}$ if $G = \mathrm{N}_{L/K}(L^*)$.

**Theorem 5.5.** *Let*

$$\varphi_t(x) = x^p + \zeta^{s_t} \pi^{a+1} x^b + \pi + \sum_{r \in J} \rho_{c_{t,r}} \pi^{i+1} + k_t \delta \pi^{v+1} \in \mathcal{O}_K[x] \ (t \in \{1, 2\})$$

*be polynomials as in theorem 4.5 such that $L_1 := K[x]/(\varphi_1)$ and $L_2 := K[x]/(\varphi_2)$ are Galois. Then $v = v_{L_1/K} = v_{L_2/K} = (ap+b)/(p-1)$. If $K$ does not contain the $p$-th roots of unity,*

$$\mathrm{N}(L_t^*) = \langle \pi_K \eta_{v,i_t}^{a_{t,\pi}};\ \zeta_K;\ \eta_{\lambda,i} \eta_{v,i_t}^{a_{t,\lambda,i}} \mid \lambda \in F_K, \lambda < v, 1 \leqslant i \leqslant f_K;$$

$$\eta_{v,i} \eta_{v,i_t}^{a_{t,v,i}} \mid 1 \leqslant i < i_t;\ \eta_{v,i_t}^{p};\ \eta_{v,i} \mid i_t < i \leqslant f_K;$$

$$\eta_{\lambda,i} \mid \lambda \in F_K, v < \lambda, 1 \leqslant i \leqslant f_K \rangle.$$

*If $K$ contains the $p$-th roots of unity then $\eta_*$ is an additional generator of $\mathrm{N}(L_t^*)$.*

**(a)** *$s_1 \neq s_2$ if and only if there exists $1 \leqslant i < i_t$ with $a_{1,v,i} \neq a_{2,v,i}$.*

**(b)** *Let $w \in J = \{r \in \mathbb{Z} \mid 1 \leqslant r < (ap+b)/(p-1),\ p \nmid (b+r)\}$. We have $c_{1,r} = c_{2,r}$ for $1 \leqslant r < w$, $r \in J$ if and only if $a_{1,v-r,i} = a_{2,v-r,i}$ for*

$1 \leqslant r < w$, $r \in J$ *and all* $1 \leqslant i \leqslant f_K$.
**(c)** *If* $c_{1,r} = c_{2,r}$ *for all* $r \in J$, *then* $k_1 = k_2$ *if and only if* $a_{1,\pi} = a_{2,\pi}$.

*Proof.* We have seen that there exists $v$ in $F_K$ and $1 \leqslant i_t \leqslant f_K$ such that $a_{t,v,i_t} = p$ for $t = 1, 2$.
**(a)** (i) If $\varepsilon_t \in \mathcal{O}_{L_t}^*$ is chosen such that $\pi_{L_t}^{\sigma-1} \equiv 1 + \varepsilon_t \pi_L^v \mod \mathfrak{p}_{L_t}^{v+1}$ then $\pi_{L_t}^{\sigma} = \pi_{L_t} + \varepsilon_t \pi_{L_t}^{v+1} \mod \mathfrak{p}_{L_t}^{v+2}$. By lemma 5.3,

$$\mathrm{N}_{L_t/K}(1 + \alpha\pi_{L_t}) \equiv 1 + (\alpha^p - \varepsilon_t^{p-1}\alpha^{p-1})\pi_K^v \mod \mathfrak{p}_K.$$

It follows from the proof of lemma 4.6(c) that modulo $\mathfrak{p}_K$ the unit $\varepsilon_t$ is congruent to one of the roots of $\varphi_{t,v}^{\#} \equiv -x^p + (-1)^{ap}\zeta_K^{s_t} b x \mod \mathfrak{p}_K$. Thus, $\varepsilon_t^{p-1} \equiv (-1)^{ap+1}\zeta_K^{s_t} b \mod \mathfrak{p}_K$. As the kernel of $\underline{\psi}_t : \underline{K}^+ \to \underline{K}^+$, $\underline{\alpha} \mapsto \underline{\alpha}^p - \underline{\varepsilon}_t^{p-1}\underline{\alpha}$ has order $p$, the intersection of the kernels of $\underline{\psi}_1$ and $\underline{\psi}_2$ is $\{0\}$. Therefore there exists $1 \leqslant i < f_K$ such that $a_{1,v,i} \neq a_{2,v,i}$.
(ii) By corollary 4.7, there are $\frac{p^f-1}{p-1}$ possible values for $s_t$. For any given $1 \leqslant i_t < f_K$ there are $p^{f_K - i_t}$ combinations of $0 \leqslant a_{t,v,i} < p$ where $1 \leqslant i < i_t$. In total this gives $\sum_{i_t=1}^{f} p^{f_K - i_t} = \frac{p^{f_K}-1}{p-1}$ combinations, the same number of choices as for the exponent $s_t$.
**(b)** (i) As $p$ divides $\big((ap+b)/(p-1) + b - \lambda\big) = \big((ap+bp)/(p-1) - \lambda\big)$ if and only if $p \mid \lambda$, we have $v - r \in F_K$ if and only if $r \in J$.
(ii) Assume that $\varphi_t = x^p + \beta x^b + \gamma_t$, with $\gamma_1 = \gamma_2 + \pi_K^w \alpha$ for some $\alpha \in \mathcal{O}_K^*$ with $\nu_L(R) = 0$. We have

$$\mathrm{N}_{L_t/K}(1 + \omega\pi_{L_t}^{\lambda}) = 1 + \omega R_1(\pi_{L_t}^{\lambda}) + \omega^2 R_2(\pi_{L_t}^{\lambda}) + \cdots + \omega^p R_p(\pi_{L_t}^{\lambda}),$$

where $R_i(\pi_{L_t}^{\lambda})$ denotes the $i$-th symmetric polynomial in $\pi_{L_t}^{\lambda}, \pi_{L_t}^{\sigma\lambda}, \ldots, \pi_{L_t}^{\sigma^{p-1}\lambda}$. In particular, $R_1(\pi_{L_t}^{\lambda}) = \mathrm{T}_{L_t/K}(\pi_{L_t}^{\lambda})$ and $R_p(\pi_{L_t}^{\lambda}) = \gamma_t^{\lambda}$. We have seen in the proof of theorem 5.4 (a)(ii) that $\gamma_1^{v-r} \equiv \gamma_2^{v-r} \mod \mathfrak{p}_K^v$ for $r \leqslant w - 1$. By Newton's relations (proposition 5.2) we see that

$$S_i(\pi_{L_t}) = \begin{cases} (p-b)\beta_t & \text{for } i = p - b, \\ (p-b)\beta_t^k & \text{for } i = k(p-b) < p, \\ p\gamma_t & \text{for } i = p, \\ -\beta_t S_{i-(p-b)}(\pi_{L_t}) - \gamma_t S_{i-p}(\pi_{L_t}) & \text{for } i > p, \\ 0 & \text{otherwise.} \end{cases}$$

We have $\nu_K(S_p(\pi_{L_t})) = \nu_K(p\gamma_t) = e + 1 > v$. By Newton's relations, $R_i(\pi_{L_t}^{\lambda})$ is a sum of the $S_i(\pi_{L_t})$, hence $\nu_K(R_i(\pi_{L_t}^{\lambda})) \geqslant \min(a+1, e+1) = a + 1 \geqslant v$ for $i < p$. Thus for all $r \leqslant w - 1$

$$\mathrm{N}_{L_1/K}(1 + \omega\pi_{L_1}^{v-r}) \equiv \mathrm{N}_{L_2/K}(1 + \omega\pi_{L_2}^{v-r}) \mod \mathfrak{p}_K^v.$$

(iii) See the proof of theorem 5.4 (a) (iv).
**(c)** See the proof of theorem 5.4 (b). □

Theorems 5.4 and 5.5 yield an algorithm for computing the class field $L$ over an extension $K$ of $\mathbb{Q}_p$ corresponding to a subgroup $G$ of $K^*$ of index $p$. The discriminant $\mathfrak{p}^{p+ap+b-1}$ of the extension can be directly read off from the Hermite normal form of the transformation matrix from the generators of $K^*$ to the generators of $G$. After determining the exponent for $\zeta$ one has a first approximation of a generating polynomial of $L$:

$$x^p + \zeta^s \pi^{a+1} x^b + \pi.$$

Now the constant term can be determined by computing the coefficients of $\pi$, $\pi^2, \ldots$ in its $\pi$-adic expansion step by step up to the coefficient of $\pi^{v+1} = \pi^{(ap+b)/(p-1)+1}$.

The existence theorem for ramified extensions of degree $p$ follows from the two theorems above by a counting argument. A change in a coefficient of the polynomial results in a change of an entry of the matrix. There are exactly $p$ choices for the indeces $c_r$ of the coefficients of $\pi$, $\pi^2, \ldots$ and for the entries $a_{\lambda,i}$ of the matrix. Likewise there are $p$ choices for the coefficient $k$ of the polynomials and the entry $a_\pi$ of the matrix. We obtain a one-to-one correspondence between generating polynomials of ramified normal extensions of degree $p$ and the matrices representing their norm groups.

The existence theorem for unramified extensions of degree $p$ is a special case of the existence theorem for tamely ramified extensions.

**Corollary 5.6.** *Let $G$ be a subgroup of $K^*$ of index $p$. Then there exists a unique abelian extension $L/K$ with $\mathrm{N}_{L/K}(L^*) = G$.*

## 6. Cyclic Totally Ramified Extensions of Degree $p^m$

We construct the class field corresponding to a subgroup $G \subset K^*$ with $K^*/G$ cyclic of order $p^m$ as a tower of extensions of degree $p$. In each step we determine a class field $L$ of degree $p$ and then find the class field over $L$ corresponding to the preimage of $G$ under the norm map.

**Norm Equations.** Let $L/K$ be a finite extension and let $\alpha \in K$. We are looking for a solution $\beta \in L^*$ of the norm equation

$$\mathrm{N}_{L/K}(\beta) = \alpha \in K$$

provided it exists. Let $L^* = \langle \pi_L \rangle \times \langle \zeta_L \rangle \times \langle \eta_{L,1}, \ldots, \eta_{L,r} \rangle$ be the unit group of $L$. Obviously $\mathrm{N}_{L/K}(\beta) = \alpha$ has a solution if $\alpha$ is in the subgroup

$$U := \langle \mathrm{N}_{L/K}(\pi_L), \mathrm{N}_{L/K}(\zeta_L), \mathrm{N}_{L/K}(\eta_{L,1}), \ldots, \mathrm{N}_{L/K}(\eta_{L,r}) \rangle$$

of $K^*$. We determine a solution $\beta$ $\mathrm{N}_{L/K}(\beta) = \alpha$ by representing $\alpha$ by the generators of $U$ given above. The set of all solutions is $\{\beta \cdot \gamma \mid \gamma \in \ker(\mathrm{N}_{L/K})\}$.

We find the preimage of a subgroup $A$ of $\mathrm{N}_{L/K}(L^*) \subset K^*$ in a similar way. We need to determine a subgroup $B$ of $L^*$ such that $\mathrm{N}_{L/K}(B) = A$.

As $A \subset \mathrm{N}_{L/K}(L^*)$ there exist $a_{\pi,l}, a_{\zeta_L,l}, a_{k,l} \in \mathbb{N}$ $(1 \leqslant k \leqslant r, 1 \leqslant l \leqslant r+2)$ such that

$$A = \langle \mathrm{N}_{L/K}(\pi_L)^{a_{\pi,l}} \mathrm{N}_{L/K}(\zeta_L)^{a_{\zeta_L,l}} \textstyle\prod_{k=1}^{r} \mathrm{N}_{L/K}(\eta_k)^{a_{k,l}} \mid 1 \leqslant l \leqslant r+2 \rangle.$$

Thus a solution of our problem is given by

$$B = \langle \pi_L^{a_{\pi,l}} \zeta_L^{a_{\zeta_L,l}} \textstyle\prod_{k=1}^{r} \eta_k^{a_{k,l}} \mid 1 \leqslant l \leqslant r+2 \rangle.$$

**Constructing Class Fields.** Let $G$ be a subgroup of $K^*$ with $K^*/G \cong (1+\mathfrak{p}_K)/(G \cap (1+\mathfrak{p}_K))$ cyclic and $[K^* : G] = p^m$. We describe an algorithm for constructing the class field over $K$ corresponding to $G$.

Let $\eta_1 \in K^*$ be such that $\langle \eta_1 G \rangle = K^*/G$. If $H_1 = \langle \eta_1^p, G \rangle$, then $H_1$ is the unique subgroup of $K^*$ of index $p$ with $H_1 \supset G$. We determine the class field $L_1/K$ corresponding to $H_1$ using the results of the previous section. Let $G_1 = \mathrm{N}_{L_1/K}^{-1}(G) \subset L_1^*$. Since $H_1 = \mathrm{N}_{L_1/K}(L_1^*)$, we have $[L_1^* : G_1] = p^{m-1}$. Now we determine the subgroup $H_2 \supset G_1$ with $[L_1^* : H_2] = p$ and compute the class field $L_2/L_1$ corresponding to $H_2$.

Next we show that $L_2/K$ is normal. If $L_2/K$ was not normal then we would have $\widehat{\sigma}(L_2) \neq L_2$ for an extension of an automorphism $\sigma \in \mathrm{Gal}_{L_1/K}$, and $\mathrm{N}_{\sigma(L_2)/K}(\sigma(L_2^*)) = \mathrm{N}_{L_2/K}(L_2^*) = \langle \eta_1^{p^2}, G \rangle$. But by its construction, $L_2/L_1$ is the unique abelian extension with $\mathrm{N}_{L_2/K}(L_2^*) = \langle \eta_1^{p^2}, G \rangle$. Thus $L_2/K$ is normal.

The Galois group of $L_2/K$ is either isomorphic to $C_p \times C_p$ or to $C_{p^2}$. Assume $\mathrm{Gal}_{L_2/K} \cong C_p \times C_p$. Then $L_2/K$ has at least two distinct subfields $L_1$ and $L_1'$ of degree $p$ with $\mathrm{N}_{L_1/K}(L_1^*) \supset G$ and $\mathrm{N}_{L_1'/K}(L_1'^*) \supset G$ and $\mathrm{N}_{L_1/K}(L_1^*) \neq \mathrm{N}_{L_1'/K}(L_1'^*)$ (otherwise $L_1 = L_1'$). But $H_1$ is the unique subgroup of $G$ of index $p$, therefore $\mathrm{Gal}_{L_2/K} \cong C_{p^2}$.

So $L_2/K$ is the class field corresponding to $\mathrm{N}_{L_2/K}(L_2^*) = \langle \eta_1^{p^2}, G \rangle$. Next we set $G_2 = \mathrm{N}_{L_2/L_1}^{-1}(G_1) = \mathrm{N}_{L_2/K}^{-1}(G) \subset L_1^*$ and continue as above until we obtain $L_m/K$, the class field corresponding to $G$.

As the Galois group of all subextensions of $L_m/K$ of degree $p^2$ is isomorphic to $C_{p^2}$, we obtain $\mathrm{Gal}_{L_m/K} \cong C_{p^m}$. This yields the existence theorem for cyclic class fields of degree $p^m$.

**Algorithm 6.1** (Cyclic Class Fields of Degree $p^m$)**.**
Input: $K/\mathbb{Q}_p$, $G$ a subgroup of $K^*$ such that
$K^*/G \cong (1+\mathfrak{p}_K)/(G \cap (1+\mathfrak{p}_K))$ cyclic with $[K^* : G] = p^m$.
Output: $L_m/K$ cyclic of degree $p^m$ with $\mathrm{N}_{L_m/K}(L_m) = G$.

- Set $G_1 := G$ and $L_0 := K$.
- For $i$ from 1 to $m$:
  - **a.** Let $\eta_i \in L_{i-1}^*$. Set $H_1 = \langle \eta_i^p, G_i \rangle$, then $[K^* : H_i] = p$.
  - **b.** Determine $L_i/K$ class field corresponding to $H_i$.

**c.** Set $G_{i+1} = \mathrm{N}^{-1}_{L_i/L_{i-1}}(G_i) \subset L_i^*$, then $[L_i^* : G_{i+1}] = p^{m-i}$.

**Corollary 6.2.** *For every subgroup $G$ of $K^*$ with $K^*/G \cong (1+\mathfrak{p}_K)/(G \cap (1+\mathfrak{p}_K))$ cyclic of degree $p^m$ there exists an abelian extension $L/K$ of degree $p^m$ with $\mathrm{N}_{L/K}(L^*) = G$.*

The existence theorem of local class field theory for finite extensions (theorem 3.3) follows.

**Example 6.3.** Let $G_1 = \langle 3\rangle \times \langle -1\rangle \times \langle (1+3)^9\rangle \subset \mathbb{Q}_3^*$. We compute the class field corresponding to $G_1$ as follows (from bottom to top):

**b.** $\mathbb{Q}_3(\pi_2)$ with $\pi_2^3 + (-12\pi_1^2 - 6)\pi_2^2 - 372\pi_1^2 + 31\pi_1 - 183{=}0$

**a.** $H_2 = G_2$, as $[\mathbb{Q}_3(\pi_1)^* : G_2] = 3$

**c.** $G_2 = \mathrm{N}^{-1}_{\mathbb{Q}_3(\pi_1)/\mathbb{Q}_3}(G_1)$
$= \langle \pi_1, -1, (1+\pi_1)(1+\pi_1^4)^2, (1+\pi_1^2)(1+\pi_1^4), (1+\pi_1^4)^3\rangle$
$\mathbb{Q}_3(\pi_1)^* = \langle \pi_1\rangle \times \langle -1\rangle \times \langle 1+\pi_1, 1+\pi_1^2, 1+\pi_1^4\rangle$

**b.** $\mathbb{Q}_3(\pi_1)$ with $\pi_1^3 + 6\pi_1^2 + 3 = 0$

**a.** $H_1 = \langle 3\rangle \times \langle -1\rangle \times \langle (1+3)^3\rangle$, such that $[\mathbb{Q}_3^* : H_1] = 3$
$G_1 = \langle 3\rangle \times \langle -1\rangle \times \langle (1+3)^9\rangle$
$\mathbb{Q}_3^* = \langle 3\rangle \times \langle -1\rangle \times \langle 1+3\rangle$

$\mathbb{Q}_3$

## 7. Examples

The methods presented above have been implemented in the computer algebra system Magma [BC95] and released with Magma 2.12. In the tables below we give cyclic class fields over $\mathbb{Q}_p$ and some of their extensions for $p \in 2, 3, 5, 7, 11, 13$ of degree up to 343.

Let $K$ be a finite extension of $\mathbb{Q}_p$ with unit group

$$K^* = \langle \pi\rangle \times \langle \zeta\rangle \times \langle \eta_{\lambda,i} \mid \lambda \in F_K, 1 \leqslant i \leqslant f\rangle.$$

A cyclic class field $L$ of degree $d$ over a field $K$ is denoted by

$$L^{(a_\pi; a_\zeta; a_{1,1} \ldots, a_{v-1,f})}_{d,\nu_K(\mathrm{d}(L/K))}/K,$$

where $a_\pi, a_\zeta, a_{1,1} \ldots, a_{v-1,f}$ are the entries in the relevant column of the Hermite normal form of the transformation matrix mapping the basis of $K^*$ to generators of the norm group $\mathrm{N}_{L/K}(L^*)$ (compare the exposition before theorem 5.5). It is obvious that $0 \leqslant a_\pi < d$, $0 \leqslant a_\zeta < d$, and $0 \leqslant a_{\lambda,i} < d$ for $\lambda \in F_K$ and $1 \leqslant i \leqslant f_{K/\mathbb{Q}_p}$. If $d$ is a multiple of $p$ we leave out $a_\zeta = 0$.

In some tables the class fields are parameterized by the $a_{i,j}$. The $a_{i,j}$ in the naming scheme are always to be considered modulo $d$. Throughout this section we use $\{0,\dots,p-1\}$ as a set of representatives of $\mathbb{Z}_p/(p)$. As we compute class fields as towers of extensions and in order to facilitate representation we give their generating polynomials over a suitable subfield that can be found in one of the other tables. We use $\pi$ to denote a uniformizer of that ground field.

If $K$ contains the $p$-th roots of unity we have the additional generator $\eta_*$ for $K^*$ and an additional entry $a_*$ in the transformation matrix.

**Class Fields over $\mathbb{Q}_2$.** There are six totally ramified class fields of degree 2 over $\mathbb{Q}_2$. The parameter $k$ is equal to 0 or 1.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $K_{2,2}^{(k)}/\mathbb{Q}_2$ | $\langle 2\cdot 3^k, 3^2, 5\rangle$ | $\mathbb{Q}_2$ | $x^2+2x+2+k\cdot 4$ |
| $K_{2,3}^{(k,0)}/\mathbb{Q}_2$ | $\langle 2\cdot 5^k, 3, 5^2\rangle$ | $\mathbb{Q}_2$ | $x^2+2+k\cdot 8$ |
| $K_{2,3}^{(k+1,1)}/\mathbb{Q}_2$ | $\langle 2\cdot 5^{k+1}, 3\cdot 5, 5^2\rangle$ | $\mathbb{Q}_2$ | $x^2+2+4+k\cdot 8$ |

The following table contains 2 of the class fields of degree 64 over $\mathbb{Q}_2$ and its abelian subfields. The parameter $k$ is equal to 0 or 1.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $K_{4,11}^{(1,2)}/\mathbb{Q}_2$ | $\langle 2\cdot 5, 3\cdot 5, 5^4\rangle$ | $K_{2,3}^{(1,1)}$ | $x^2+\pi+\pi^2+\pi^4$ |
| $K_{8,31}^{(2;5)}/\mathbb{Q}_2$ | $\langle 2\cdot 5^2, 3\cdot 5^5, 5^8\rangle$ | $K_{4,11}^{(1,2)}$ | $x^2+\pi+\pi^4$ |
| $K_{16,79}^{(10;13)}/\mathbb{Q}_2$ | $\langle 2\cdot 5^{10}, 3\cdot 5^{13}, 5^{16}\rangle$ | $K_{8,31}^{(2;5)}$ | $x^2+\pi+\pi^8+\pi^{16}+\pi^{17}$ |
| $K_{32,191}^{(10;29)}/\mathbb{Q}_2$ | $\langle 2\cdot 5^{10}, 3\cdot 5^{29}, 5^{32}\rangle$ | $K_{16,79}^{(10;13)}$ | $x^2+\pi+\pi^{16}+\pi^{24}+\pi^{26}+\pi^{33}$ |
| $K_{64,447}^{(10+32k;29)}/\mathbb{Q}_2$ | $\langle 2\cdot 5^{10+32k}, 3\cdot 5^{29}, 5^{64}\rangle$ | $K_{32,191}^{(29;10)}$ | $x^2+\pi+\pi^{32}+\pi^{40}+\pi^{42}+\pi^{50}+\pi^{52}+\pi^{56}+\pi^{58}+\pi^{62}+k\pi^{65}$ |

**Ramified Class Fields of Degree $p$ over $\mathbb{Q}_p$ for $p$ odd.** If $p$ is an odd prime then $\mathbb{Q}_p^* = \langle p, \zeta, (1+p)\rangle$ where $\zeta$ is a $(p-1)$-th root of unity. Theorem 4.5 yields generating polynomials of totally ramified normal extensions of degree $p$ over $\mathbb{Q}_p$:

$$\varphi = x^p + (p-1)px^{p-1} + p + kp^2,$$

where $0 \leqslant k < p$. Let $K$ be the extension defined by a root of $\varphi$. The exponents of the generators of the norm groups follow immediately from the coefficients of the polynomial. We obtain

$$\mathrm{N}_{K/\mathbb{Q}_p}(K^*) = \langle p(1+p)^k, \zeta, (1+p)^p\rangle.$$

**Class Fields over $\mathbb{Q}_3$.** We start with the class fields of degree 2 and 3 over $\mathbb{Q}_3$. The parameter $k$ runs from 0 to 2.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $K_{2,0}/\mathbb{Q}_3$ | $\langle 3^2, -1, 4\rangle$ | $\mathbb{Q}_3$ | $x^2+1$ |
| $K_{2,1}^{(0)}/\mathbb{Q}_3$ | $\langle 3, 1, 4\rangle$ | $\mathbb{Q}_3$ | $x^2+3$ |
| $K_{2,1}^{(1)}/\mathbb{Q}_3$ | $\langle -3, 1, 4\rangle$ | $\mathbb{Q}_3$ | $x^2-3$ |
| $K_{3,0}/\mathbb{Q}_3$ | $\langle 3^3, -1, 4\rangle$ | $\mathbb{Q}_3$ | $x^3+2x+1$ |
| $K_{3,4}^{(k)}/\mathbb{Q}_3$ | $\langle 3\cdot 4^k, -1, 4^3\rangle$ | $\mathbb{Q}_3$ | $x^3+2\cdot 3x^2+3+k\cdot 3^2$ |

There are 12 ramified class fields of degree 3 over $K_{2,1}^{(1)}$. The fields $L_{3,6}^{(6)}$, $L_{3,6}^{(7)}$, and $L_{3,6}^{(8)}$ are normal over $\mathbb{Q}_3$. In addition to their norm groups in $K_{2,1}^{(1)}$, we give their norm groups in $\mathbb{Q}_3$. The parameter $k$ takes on values from 0 to 2.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $L_{3,4}^{(k)}/K_{2,1}^{(1)}$ | $\langle \pi(1+\pi)^k, -1, (1+\pi)^3, 4\rangle$ | $K_{2,1}^{(1)}$ | $x^3+2\pi x^2+\pi+k\pi^2$ |
| $L_{3,6}^{(k)}/K_{2,1}^{(1)}$ | $\langle \pi\cdot 4^k, -1, (1+\pi), 4^3\rangle$ | $K_{2,1}^{(1)}$ | $x^3+2\pi^2 x+\pi+\pi^2+k\pi^3$ |
| $L_{3,6}^{(3+k)}/K_{2,1}^{(1)}$ | $\langle \pi\cdot 4^k, -1, (1+\pi)4, 4^3\rangle$ | $K_{2,1}^{(1)}$ | $x^3+2\pi^2 x+\pi+2\pi^2+k\pi^3$ |
| $L_{3,6}^{(6+k)}/K_{2,1}^{(1)}/\mathbb{Q}_3$ | $\langle \pi\cdot 4^k, -1, (1+\pi)4^2, 4^3\rangle$<br>$\langle -3\cdot 4^{(3-k)}, 1, 4^3\rangle$ | $K_{2,1}^{(1)}$ | $x^3+2\pi^2 x+\pi+k\pi^3$ |

Over $K_{3,4}^{(0)}$ there are 39 ramified cyclic extensions of degree 3 with 3 different discriminant. Both parameters $l$ and $k$ run from 0 to 2.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $L_{3,4}^{(k)}/K_{3,4}^{(0)}$ | $\langle 3^1\eta_1^k, \eta_1^3, \eta_2, \eta_3^1\rangle$ | $K_{3,4}^{(0)}$ | $x^3+2\pi x^2+\pi+k\pi^2$ |
| $L_{3,6}^{(k;l)}/K_{3,4}^{(0)}$ | $\langle 3^1\eta_2^k, \eta_2^2, \eta_2^3, \eta_3\rangle$ | $K_{3,4}^{(0)}$ | $x^3+l\pi^2 x+\pi+k\pi^3$ |
| $L_{3,10}^{(k+l+2;l,0)}/K_{3,4}^{(0)}$ | $\langle 3\eta_3^{k+l+2}, \eta_1\eta_3^l, \eta_2, \eta_3^3\rangle$ | $K_{3,4}^{(0)}$ | $x^3+2\pi^3x^2+\pi+\pi^3+l\pi^4+k\pi^5$ |
| $L_{3,10}^{(k+l+2;l,1)}/K_{3,4}^{(0)}$ | $\langle 3\eta_3^{k+l+2}, \eta_1\eta_3^l, \eta_2\eta_3, \eta_3^3\rangle$ | $K_{3,4}^{(0)}$ | $x^3+2\pi^3x^2+\pi+\pi^3+l\pi^4+k\pi^5$ |
| $L_{3,10}^{(k+l;l,2)}/K_{3,4}^{(0)}$ | $\langle 3\eta_3^{k+l}, \eta_1\eta_3^l, \eta_2\eta_3^2, \eta_3^3\rangle$ | $K_{3,4}^{(0)}$ | $x^3+2\pi^3x^2+\pi+l\pi^4+k\pi^5$ |

The three fields $L_{3,10}^{(k+1,2,0)}$ for $k=0,1$, and 2 are cyclic over $\mathbb{Q}_3$. They appear

as $K_{9,22}^{(3(2-k))}/\mathbb{Q}_3$ in the following table of all cyclic extensions of $\mathbb{Q}_3$ of degree 9. Let $\rho$ be denote a root of $x^3+2x+1$ and recall that $K_{3,0}=\mathbb{Q}_3(\rho)$.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $K_{9,0}/\mathbb{Q}_3$ | $\langle 3^9,-1,4\rangle$ | $K_{3,0}$ | $x^3+(2\rho+2)x^2+(2\rho^2+2\rho+2)x+2\rho$ |
| $K_{9,22}^{(3(2-k))}/\mathbb{Q}_3$ | $\langle 3\cdot 4^{3(2-k)},-1,4^9\rangle$ | $K_{3,4}^{(0)}$ | $x^3+2\pi^3x^2+\pi+\pi^3+2\pi^4+k\pi^5$ |
| $K_{9,22}^{(3(k-1)+1)}/\mathbb{Q}_3$ | $\langle 3\cdot 4^{3(k-1)+1},-1,4^9\rangle$ | $K_{3,4}^{(1)}$ | $x^3+2\pi^3x^2+\pi+\pi^3+\pi^4+k\pi^5$ |
| $K_{9,22}^{(3(k-1)+2)}/\mathbb{Q}_3$ | $\langle 3\cdot 4^{3(k-1)+2},-1,4^9\rangle$ | $K_{3,4}^{(2)}$ | $x^3+2\pi^3x^2+\pi+\pi^3+k\pi^5$ |
| $K_{9,48}^{(1)}/\mathbb{Q}_3$ | $\langle 3^34,-1,4^3\rangle$ | $K_{3,0}$ | $x^3+2\cdot 3x^2+3+2\rho^23^2$ |
| $K_{9,48}^{(2)}/\mathbb{Q}_3$ | $\langle 3^34^2,-1,4^3\rangle$ | $K_{3,0}$ | $x^3+2\cdot 3x^2+3+\rho^23^2$ |

The following table contains all cyclic extensions of $\mathbb{Q}_3$ of degree 27 containing $K_{9,22}^{(0)}$, all cyclic extensions of $\mathbb{Q}_3$ of degree 81 containing $K_{27,94}^{(0)}/$, and all cyclic extensions of $\mathbb{Q}_3$ of degree 243 containing $K_{81,364}^{(0)}$. The parameter $k$ runs from 0 to 2.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $K_{27,94}^{(9(k+1))}/\mathbb{Q}_3$ | $\langle 3\cdot 4^{9(k+2)},-1,4^{27}\rangle$ | $K_{9,22}^{(0)}$ | $x^3+2\pi^9x^2+\pi+\pi^7+\pi^9+\pi^{10}+2\pi^{12}+\pi^{13}+k\pi^{14}$ |
| $K_{81,364}^{(27(k+2))}/\mathbb{Q}_3$ | $\langle 3\cdot 4^{27(k+2)},\zeta,4^{81}\rangle$ | $K_{27,94}^{(0)}$ | $x^3+2\pi^{27}x^2+\pi+\pi^{19}+\pi^{27}+2\pi^{28}+\pi^{30}+2\pi^{31}+2\pi^{33}+2\pi^{34}+2\pi^{36}+2\pi^{37}+k\pi^{41}$ |
| $K_{243,29728}^{(81(k))}/\mathbb{Q}_3$ | $\langle 3\cdot 4^{81(k)},\zeta,4^{243}\rangle$ | $K_{81,364}^{(0)}$ | $x^3+2\pi^{81}x^2+\pi+\pi^{55}+\pi^{81}+\pi^{82}+2\pi^{84}+2\pi^{85}+2\pi^{87}+\pi^{88}+\pi^{90}+\pi^{96}+2\pi^{97}+2\pi^{99}+\pi^{102}+2\pi^{103}+\pi^{105}+2\pi^{108}+\pi^{109}+2\pi^{112}+\pi^{114}+2\pi^{115}+2\pi^{120}+\pi^{121}+k\pi^{122}$ |

**Class Fields over $\mathbb{Q}_5$.** There are 5 cyclic extensions of degree 25 over $\mathbb{Q}_5$ containing $K_{5,8}^{(0)}$ and 5 cyclic extensions of degree 125 over $\mathbb{Q}_5$ containing $K_{25,68}^{(0)}$. The parameter $k$ takes values from 0 to 4.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $K_{5,8}^{(k)}/\mathbb{Q}_5$ | $\langle 5\cdot 6^k,\zeta,6^5\rangle$ | $\mathbb{Q}_5$ | $x^5+4\cdot 5x^4+5+k\cdot 5^2$ |
| $K_{25,68}^{(5(1-k))}/\mathbb{Q}_5$ | $\langle 5\cdot 6^{5(1-k)},\zeta,6^{25}\rangle$ | $K_{5,8}^{(0)}$ | $x^5+4\pi^5x^4+\pi+\pi^5+4\pi^6+k\pi^7$ |
| $K_{125,468}^{(25(k+4))}/\mathbb{Q}_5$ | $\langle 5\cdot 6^{25(k+4)},\zeta,6^{125}\rangle$ | $K_{25,68}^{(0)}$ | $x^5+4\pi^{25}x^4+\pi+\pi^{21}+\pi^{25}+\pi^{26}+4\pi^{28}+3\pi^{29}+4\pi^{30}+\pi^{31}+k\pi^{32}$ |

**Class Fields over $\mathbb{Q}_7$.** Over $\mathbb{Q}_7$ there are 7 cyclic extensions of degree 49 containing $K_{7,12}^{(0)}$ and 7 cyclic extensions of degree 343 containing $K_{49,138}^{(0)}$. The parameter $k$ runs from 0 to 6.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $K_{7,12}^{(k)}/\mathbb{Q}_7$ | $\langle 7\cdot 8^k, \zeta, 8^7\rangle$ | $\mathbb{Q}_7$ | $x^5 + 6\cdot 7x^6 + 7 + k\cdot 7^2$ |
| $K_{49,138}^{(7(1-k))}/\mathbb{Q}_7$ | $\langle 7\cdot 8^{7(1-k)}, \zeta, 8^{49}\rangle$ | $K_{7,12}^{(0)}$ | $x^7+6\pi^7x^6+\pi+\pi^7+6\pi^8+k\pi^9$ |
| $K_{343,488}^{(49k)}/\mathbb{Q}_7$ | $\langle 7\cdot 8^{49k}, \zeta, 8^{343}\rangle$ | $K_{49,138}^{(0)}$ | $x^7+6\pi^{49}x^6+\pi+\pi^{43}+\pi^{49}+\pi^{50}+6\pi^{52}+6\pi^{53}$ $+6\pi^{54}+5\pi^{55}+6\pi^{56}+3\pi^{57}+k\pi^{58}$ |

**Class Fields over $\mathbb{Q}_{11}$.** There are 11 cyclic extensions of degree 121 over $\mathbb{Q}_{11}$ containing $K_{11,20}^{(4)}$. The parameter $k$ runs from 0 to 11.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $K_{11,20}^{(k)}/\mathbb{Q}_{11}$ | $\langle 11\cdot 12^k, \zeta, 12^{11}\rangle$ | $\mathbb{Q}_{11}$ | $x^{11} + 10\cdot 11x^{10} + 11 + k\cdot 11^2$ |
| $K_{121,350}^{(11(1-k))}/\mathbb{Q}_{11}$ | $\langle 11\cdot 12^{11(1-k)}, \zeta, 12^{121}\rangle$ | $K_{11,20}^{(4)}$ | $x^{11} + 10\pi^{11}x^{10} + \pi + \pi^{11} + 10\pi^{12} + k\cdot\pi^{13}$ |

**Class Fields over $\mathbb{Q}_{13}$.** There are 13 cyclic extensions of degree 169 over $\mathbb{Q}_{13}$ containing $K_{13,24}^{(9)}$. The parameter $k$ runs from 0 to 12.

| $L/K$ | $\mathrm{N}_{L/K}(L^*)$ | over | generated by |
|---|---|---|---|
| $K_{13,24}^{(k)}/\mathbb{Q}_{13}$ | $\langle 13\cdot 14^k, \zeta, 14^{13}\rangle$ | $\mathbb{Q}_{13}$ | $x^{13} + 12\cdot 13x^{12} + 13 + k\cdot 13^2$ |
| $K_{169,492}^{(-13k+9)}/\mathbb{Q}_{13}$ | $\langle 13\cdot 14^{-13k+9}, \zeta, 14^{169}\rangle$ | $K_{13,24}^{(9)}$ | $x^{13} + 12\pi^{13}x^{12} + \pi + \pi^{13} + 3\pi^{14} + k\pi^{15}$ |

## References


[Ama71] S. Amano, *Eisenstein equations of degree p in a* $\mathfrak{p}$*-adic field*. J. Fac. Sci. Univ. Tokyo Sect. IA Math. **18** (1971), 1–21.

[BC95] W. Bosma, J.J. Cannon, *Handbook of Magma functions*. School of Mathematics, University of Sydney, Sydney, 1995.

[Coh99] H. Cohen, *Advanced topics in computational number theory*. Springer Verlag, New York, 1999.

[Fie99] C. Fieker, *Computing class fields via the Artin map*. Math. Comp. **70** (2001), 1293–1303.

[FV93] I. B. Fesenko, S. V. Vostokov, *Local fields and their extensions*. Translations of Mathematical Monographs, vol. **121**, American Mathematical Society, 1993.

[Has80] H. Hasse, *Number Theory*. Springer Verlag, Berlin, 1980.

[HPP03] F. Hess, S. Pauli, M. E. Pohst, *Computing the multiplicative group of residue class rings*. Math. Comp. **72** (2003), no. 243, 1531–1548.

[Iwa86] K. Iwasawa, *Local class field theory*. Oxford University Press, New York, 1986.

[Kra66] M. Krasner, *Nombre des extensions d'un degré donné d'un corps* $\mathfrak{p}$*-adique* Les Tendances Géométriques en Algèbre et Théorie des Nombres, Paris, 1966, 143–169.

[MW56] R. E. MacKenzie, G. Whaples, *Artin-Schreier equations in characteristic zero*. Amer. J. Math. **78** (1956), 473–485. MR 19,834c

[Pan95] P. Panayi, *Computation of Leopoldt's p-adic regulator*. Dissertation, University of East Anglia, 1995.

[PR01] S. Pauli, X.-F. Roblot, *On the computation of all extensions of a p-adic field of a given degree*. Math. Comp. **70** (2001), 1641–1659.

[Ser63] J.-P. Serre, *Corps locaux*. Hermann, Paris, 1963.

[Yam58] K. Yamamoto, *Isomorphism theorem in the local class field theory*. Mem. Fac. Sci. Kyushu Ser. A **12** (1958), 67–103.

Sebastian Pauli
Department of Mathematics and Statistics
University of North Carolina Greensboro
Greensboro, NC 27402, USA
*E-mail*: pauli@math.tu-berlin.de