On the computation of norm residue symbols

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. dr. ir. drs. H. Bijl,
volgens besluit van het College voor Promoties
te verdedigen op 19 mei 2021
klokke 10.00 uur

door

Johannes Bouw

geboren te Sliedrecht
in 1950

Promotor	Prof. dr. R. M. van Luijk
Copromotor	Prof. dr. H. W. Lenstra jr.
Copromotor	dr. M. F. Kosters (Acorn, Irvine, CA)

Samenstelling van de promotiecommissie:

Prof. dr. F. A. van der Duijn Schouten
Prof. dr. B. de Smit
Prof. dr. E. Bayer-Fluckiger (École Polytechnique Fédérale de Lausanne)
Prof. dr. J. M. Voight (Dartmouth College, Hanover, NH)

On the computation of norm residue symbols

Jan Bouw

Typeset using LaTeX

Printed by Haveka, Alblasserdam

ISBN: 978-90-3610654-2

Design cover/bookmark: Hendrik Bouw

Contents

Chapter 1

Introduction

Let p be a prime number, denote by $\mathbf{Q}_p$ the field of p-adic numbers, and by $\bar{\mathbf{Q}}_p$ an algebraic closure of $\mathbf{Q}_p$. Let F be a finite extension of $\mathbf{Q}_p$ inside $\bar{\mathbf{Q}}_p$ and let F^{ab} be the maximal abelian extension of F inside $\bar{\mathbf{Q}}_p$. Local class field theory gives us a group homomorphism $\phi_F : F^* \longrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F)$, the *reciprocity map.* For an extensive treatment of the reciprocity map and the broader context of local class field theory, we refer to [**2**], part 2 or [**18**], Teil 2.

Let m be a positive integer and let F contain the m-th roots of unity, which are the elements of $\mu_m = \{x \in \bar{\mathbf{Q}}_p : x^m = 1\}$. The m-th *norm residue symbol* is the map $(\cdot, \cdot)_m : F^* \times F^* \longrightarrow \mu_m$ defined on every pair of elements $\alpha, \beta \in F^*$ by

$$(\alpha, \beta)_m = \frac{\phi_F(\alpha)(\sqrt[m]{\beta})}{\sqrt[m]{\beta}}.$$

The main purpose of this thesis is to prove the following theorems.

THEOREM 1.1. *There is a polynomial-time algorithm that, given a prime number p, a positive integer m and a finite extension F of $\mathbf{Q}_p$ containing a primitive m-th root of unity and also given two elements $\alpha, \beta \in F^*$, computes the norm residue symbol $(\alpha, \beta)_m$.*

At the end of the present introduction we shall describe how the field F and its elements α and β are supposed to be "given" to the algorithm, and how the output is represented. All this will necessarily be done in finite precision, and, as discussed below, this precision should be large enough to guarantee that the output of the algorithm is well-defined. The same comments apply to Theorems 1.2 and 1.4 below. The proof of Theorem 1.1 is found in Section 5 of Chapter 5.

Algorithms for computing norm residue symbols are useful in several contexts. In local class field theory, the norm residue symbol detects which elements are norms from certain extensions (see Remark 5.2). In algebraic number theory, they can be used in the computation of higher power residue symbols in algebraic number fields, see [**4**]. Norm residue symbols are also encountered in arithmetic geometry. For example, the quadratic norm residue symbol $(\alpha, \beta)_2$, which is known as the *Hilbert symbol*, is equal to 1 if and only if the conic $\alpha x^2 + \beta y^2 = z^2$ has an F-rational point. For general m, the norm residue symbol can be used to compute elements in Brauer groups, as explained in [**15**, Section 15]. This can be helpful in detecting the presence of so-called Brauer-Manin obstructions in arithmetic geometry (see [**20**, Chapter 8, Section 2]).

It is hard to find a computer algebra system that allows the possibility of computing norm residue symbols, especially in the case that $m > 2$. In some systems one can approach the problem in an indirect manner, which does not in all cases work out efficiently. We expect that the algorithm that underlies Theorem 1.1 is perfectly suitable for actual implementation.

THEOREM 1.2. *There is a polynomial-time algorithm that, given a prime number p, a positive integer n, and a finite extension F of $\mathbf{Q}_p$, decides whether F contains a primitive p^n-th root of unity and if so, computes such a root of unity.*

The proof of Theorem 1.2 can be found in the last section of Chapter 4. We remark that if $n = 1$, the decision whether F contains a primitive p-th root of unity is a simple verification (see Algorithm 4.13), but if $n > 1$ we perform extensive computations (see Algorithms 4.23 and 4.24) in order to decide whether the required root of unity exists and if so compute it. It is an interesting question whether there exists a faster algorithm than ours in the case that $n > 1$.

The computation of an m-th norm residue symbol can be reduced to two special cases, the *tame* one in which the prime number p does not divide m and the *wild* case in which m is a power of p. In the tame case (see Section 3 of Chapter 5), there is a formula usable in practice to compute the norm residue symbol and also good enough to prove Theorem 1.1. In this thesis we will mainly consider the wild case (see Section 4 of Chapter 5). In that case there are also formulas that can be used to compute the norm residue symbol (see [**7**]), but it remains a challenge to decide whether these formulas can be evaluated in polynomial time and to compare the efficiency of such a computation with the efficiency of our algorithm.

Let p be a prime number, let n be a positive integer and let the field F be a finite extension of $\mathbf{Q}_p$ containing μ_{p^n}. We denote by $\mathrm{ord}_F : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ the surjective valuation function on F. A *prime element* π of F is defined by the property $\mathrm{ord}_F(\pi) = 1$. In the appendix of Milnor's "Introduction to Algebraic K-theory", see [**15**], a *distinguished unit* δ in F is defined by the following properties:

i. $\mathrm{ord}_F(\delta - 1) = \frac{p \cdot \mathrm{ord}_F(p)}{p-1}$,
ii. $\delta \notin (F^*)^p$.

Such a distinguished unit δ has the property that for every unit u of the ring of integers $\mathcal{O}_F$ of F, the norm residue symbol $(u, \delta)_{p^n}$ is a p-th power in the group of p^n-th roots of unity, so $(u, \delta)_{p^n}^{p^{n-1}} = 1$, without δ itself being a p-th power.

The algorithm underlying Theorem 1.1 in the wild case is motivated by a theorem of Moore (see [**15**], Appendix, Theorem A.14). This theorem implies that for any prime element π of F and any distinguished unit δ the symbol $(\pi, \delta)_{p^n}$ generates the cyclic group μ_{p^n}. It also implies that for every pair of elements $\alpha, \beta \in F^*$ the integer $i \in \mathbb{Z}/p^n\mathbb{Z}$ for which $(\alpha, \beta)_{p^n} = (\pi, \delta)_{p^n}^i$ can be computed if $F, p, n, \alpha, \beta, \pi$ and δ are given. Only a few arithmetic rules, which hold for all elements in F^*, are used in the computation. These rules are the following:

i. $(\alpha, \beta)_{p^n} = 1$ if $\alpha + \beta = 1$,
ii. $(\alpha, \beta)_{p^n}^{p^n} = 1$,
iii. $(\alpha_1 \cdot \alpha_2, \beta)_{p^n} = (\alpha_1, \beta)_{p^n} \cdot (\alpha_2, \beta)_{p^n}$,
iv. $(\alpha, \beta_1 \cdot \beta_2)_{p^n} = (\alpha, \beta_1)_{p^n} \cdot (\alpha, \beta_2)_{p^n}$.

In his article “On Computations in Kummer Extensions” (see [**6**]) Daberkow was the first to use these ideas. The proof of Moore’s theorem, as given in [**15**], offered him an algorithm to compute the integer i. With this result there are two problems left in the computation of the norm residue symbol.

The first problem is the polynomiality of the algorithm, which is not a part of the discussion in Daberkow’s article. Our own algorithm for computing i, while still inspired by [**15**], is very different from Daberkow’s, and it does run in polynomial time. It makes use of a presentation for the group $U_1 = \{u \in F : \mathrm{ord}_F(u-1) > 0\} = 1 + \mathfrak{m}$ of *principal units* of F, where $\mathfrak{m} = \pi\mathcal{O}_F$ is the maximal ideal of $\mathcal{O}_F$. The algorithm that proves Theorem 1.2 depends on the same presentation.

The second problem is that knowing the value of i is not the same as knowing the norm residue symbol $(\alpha,\beta)_{p^n} = (\pi,\delta)_{p^n}^i$ as long as we do not know the value of $(\pi,\delta)_{p^n}$. Daberkow does not address this issue. In Chapter 5 of this thesis we compute the true value of the norm residue symbol by using a functorial property of the reciprocity map.

In Chapter 6 we prove the existence of a distinguished unit ϵ with the additional property that $(u,\epsilon)_{p^n} = 1$ if u a unit, which for $n > 1$ is not necessarily the case with a distinguished unit as defined above. Such a distinguished unit will be called a *strongly distinguished unit.*

One can show that a distinguished unit ϵ is strongly distinguished if and only if the field extension $F(\sqrt[p^n]{\epsilon})$ of F, which has degree p^n, is unramified (see Lemma 6.2). In addition, among all elements $\alpha \in F$ for which $F(\sqrt[p^n]{\alpha})$ is unramified of degree p^n over F, the strongly distinguished units are exactly those that are as close as possible to 1. This is a consequence of the following theorem, which also implies that strongly distinguished units exist. It is proved in Chapter 6.

Theorem 1.3. *Let p be a prime number and n a positive integer. Let F be a finite extension of the field $\mathbf{Q}_p$ containing ζ_{p^n}, a primitive p^n-th root of unity. Then there exists $\epsilon \in F$ such that*

i. $\mathrm{ord}_F(\epsilon - 1) = \frac{p}{p-1} \cdot \mathrm{ord}_F(p)$,
ii. *$F(\sqrt[p^n]{\epsilon})$ is an unramified field extension of F of degree p^n.*

There does not exist $\epsilon \in F$ satisfying (ii) *and* $\mathrm{ord}_F(\epsilon - 1) > \frac{p}{p-1} \cdot \mathrm{ord}_F(p)$.

A second result, which is also proved in Chapter 6, tells us that a strongly distinguished unit can be computed in polynomial time.

Theorem 1.4. *There is a polynomial-time algorithm that, given a prime number p, a positive integer n, and a finite extension F of $\mathbf{Q}_p$ containing the p^n-th roots of unity, computes an element ϵ of F satisfying conditions* (i) *and* (ii) *from Theorem 1.3.*

Once a strongly distinguished unit ϵ is available, one may simplify the algorithm underlying Theorem 1.1 by using a formula (see Chapter 6, Lemma 6.3ii) that depends on the property that $(u,\epsilon)_{p^n} = 1$ for every unit u. Thus, if one needs to compute a large number of norm residue symbols in the same field F, it may be of advantage to start by computing a strongly distinguished unit once and for all, using Theorem 1.4.

Moreover, the norm residue symbol $(\pi, \epsilon)_{p^n}$ can also be computed once and for all, and its value is independent of the choice of the prime element π (see Lemma 6.3i).

As announced earlier we will now explain how our field F is given to the algorithms of Theorem 1.1, 1.2 and 1.4, and how we are able to specify the input α, β to the algorithm of Theorem 1.1 using only a finite number of bits. Likewise we will specify in which manner and to which precision the roots of unity and the strongly distinguished units computed by our algorithms are represented.

Let F be any finite extension of $\mathbf{Q}_p$, with no assumptions on roots of unity. We summarize some facts from the standard theory of local fields (see [**24**], Chapter 3). Let f be the degree of the residue class field $\mathcal{O}_F/\mathfrak{m}$ over the prime field $\mathbf{F}_p$ and let $\mathbf{Z}_p$ denote the ring of p-adic integers. There is a monic polynomial $g \in \mathbf{Z}_p[X]$ of degree f that is irreducible modulo p,with the following property: adjoining a root γ of g to $\mathbf{Q}_p$ gives the maximal unramified subfield $E = \mathbf{Q}_p(\gamma)$ of F and $\mathcal{O}_E = \mathbf{Z}_p[\gamma]$ is its ring of integers. There is also a polynomial $h \in \mathbf{Z}_p[X, Y]$ such that $h(\gamma, Y) \in E[Y]$ is a monic and irreducible polynomial of degree $e = \operatorname{ord}_F(p)$ with the following properties: first, it satisfies specific conditions on its coefficients (see Chapter 3, Section 3) that make it into an *Eisenstein polynomial*; and second, it has a zero π in F. Then it is automatic that $F = E(\pi)$, that F is totally ramified over E with prime element π, and that $\mathcal{O}_F = \mathbf{Z}_p[\gamma, \pi] \cong \mathbf{Z}_p[X, Y]/(g, h)$.

Because F is the field of fractions of $\mathcal{O}_F$, it suffices to “give” $\mathcal{O}_F$ instead of F. However, in algorithms we cannot work with elements of $\mathcal{O}_F$ in infinite precision, so we use an approximation of $\mathcal{O}_F$, good enough for our purposes. This approximation is the finite ring $\mathcal{O}_N = \mathcal{O}_F/\mathfrak{m}^N$, where $N \in \mathbf{Z}_{>0}$ is the precision, to be chosen large enough as discussed below. If the polynomials g_N and h_N satisfy $g_N \equiv g \pmod{p^{\lceil \frac{N}{e} \rceil}}$ and $h_N \equiv h \pmod{p^{\lceil \frac{N}{e} \rceil}}$ then we have $\mathcal{O}_N \cong (\mathbf{Z}/p^{\lceil \frac{N}{e} \rceil}\mathbf{Z})[X, Y]/(g_N, h_N, Y^N)$, with γ and π corresponding to X and Y respectively (see Chapter 3, Section 4.1). Then our field is “given” in precision N by p, g_N and h_N.

Any element $x \in \mathcal{O}_N$ is represented by a sum of the form $\sum_{i=0}^{N-1} c_i \pi_i$, where π_i is a certain element with $\operatorname{ord}_F(\pi_i) = i$ (see Definition 2.3), and where each c_i belongs to the set $\mathcal{C} = \{\sum_{j=0}^{f-1} d_j \gamma^j : d_j \in \{0, 1, \ldots, p-1\} \,\text{for each}\, j\}$ of *digits* (see Definition 2.2). Observe that each coset of $\mathcal{O}_F/\mathfrak{m}$ contains exactly one digit. The elements of $(\mathcal{O}_N)^*$ are characterised by the property that $c_0 \neq 0$. This representation of elements of $(\mathcal{O}_N)^*$ will be used below, and it also applies to the roots of unity and strongly distinguished units that are computed by our algorithms. Note that $O(N \log q)$ bits suffice to represent any element of $\mathcal{O}_N$, where $q = p^f = \#\mathcal{C}$ is the number of elements of the residue field $\mathcal{O}_F/\mathfrak{m}$. Every arithmetical operation performed in our algorithms takes place in $\mathcal{O}_N$ for some N or in the ring $\mathbf{Z}$.

We will specify α and β in Theorem 1.1 using the analogue for F^* of *scientific notation.* This will do justice to the multiplicative nature of the norm residue symbol and also accommodate elements that do not belong to $\mathcal{O}_F^*$. Just as every positive real number can be uniquely written as $u \cdot 10^a$ with $u \in [1, 10)$ and $a \in \mathbf{Z}$, so can each element of F^* be uniquely written as $u \cdot \pi^a$ with $u \in (\mathcal{O}_F)^*$ and $a \in \mathbf{Z}$. We need to turn this notation into one that uses only a finite number of bits.

As in Theorem 1.1, let $m \in \mathbf{Z}_{>0}$ be such that $\mu_m \subset F$. Since the value of $(\alpha, \beta)_m$ depends only on the cosets $\alpha(F^*)^m$, $\beta(F^*)^m \in F^*/(F^*)^m$ (see Chapter 5, Proposition

5.1), it will for our purposes suffice to represent elements of $F^*/(F^*)^m$, and this is what can be done with a finite number of bits, as follows. If $u \cdot \pi^a \in F^*$ is as above, then knowing the coset $u \cdot \pi^a \cdot (F^*)^m$ is clearly equivalent to knowing a modulo $m\mathbf{Z}$ and u modulo $(\mathcal{O}_F^*)^m$. Now assume that our precision satisfies $N \geq 1$ in the tame case (see Algorithm 5.4) and $N \geq \frac{e}{p-1} + \mathrm{ord}_F(m) + 1$ otherwise. Then the group $1 + \mathfrak{m}^N$ is contained in $(\mathcal{O}_F^*)^m$ (see Chapter 4, Corollary 4.9), so we have a surjective group homomorphism

$$(\mathcal{O}_N)^* = \mathcal{O}_F^*/(1 + \mathfrak{m}^N) \to \mathcal{O}_F^*/(\mathcal{O}_F^*)^m.$$

Hence we can represent elements of $F^*/(F^*)^m$ by pairs $(\bar{a}, \bar{u}) \in \mathbf{Z}/m\mathbf{Z} \times (\mathcal{O}_N)^*$ with $(\bar{a}, \bar{u})$ representing the coset $u \cdot \pi^a (F^*)^m$, and that is what we shall do (see Chapter 5, section 2). The total number of bits used is $O(N \log q + \log m)$.

In Theorem 1.2 we choose the precision N in which our field F is given such that the inequality $N \geq \frac{e}{p-1} + e \cdot n + 1$ is satisfied. The precision of the output is $N - e \cdot n$ (see Algorithm 4.24, Proposition 4.25 and Theorem 4.26). We remark that due to the fact that in our algorithm p-th roots of principal units are computed, the precision of the output will be smaller than the precision of the input. In fact, the precision of the output is just large enough to distinguish between different p^n-th roots of unity and therefore the root of unity computed by the algorithm is well-defined. In Theorem 1.4 the precision of the input is also required to satisfy $N \geq \frac{e}{p-1} + e \cdot n + 1$, and the precision of the output is N itself (see Algorithm 6.8 and Proposition 6.9). In Theorem 1.1 we have to distinguish two cases. In the tame case, we require $N \geq 1$ for the precision of the input, and the precision of the output equals N (see Algorithm 5.4 and Proposition 5.5). In the other case, we choose the precision N of the input such that $N \geq 3(r+1)e + 1$, where r is the integer for which $p^r \mid\mid e$ and the precision of the output is $N - (r+1)e$ (see Algorithm 5.24, Proposition 5.25 and Theorem 5.26).

Chapter 2

Local fields: facts and notation

Let p be a prime. Let F be a finite field extension of $\mathbf{Q}_p$ and let d be its degree. We will call such a field F a *local field.* Let $\mathcal{O}$ be its ring of integers with maximal ideal $\mathfrak{m}$, residue field $k = \mathcal{O}/\mathfrak{m}$ and unit group $U = \mathcal{O}^*$. We write $^- : \mathcal{O} \to k$ for the residue map. For $i \in \mathbf{Z}_{\geq 1}$ we set $U_i = 1 + \mathfrak{m}^i$. We call U_1 the group of *principal units.* By $v : F^* \to \mathbf{Z}$ we denote the surjective valuation. Sometimes we denote v by ord. Let $f = [k : \mathbf{F}_p]$ be its residue field degree and let $e = d/f = v(p)$ be its ramification index. If $(p-1)|e$, define $r \in \mathbf{Z}_{\geq 0}$ by $p^r \mid\mid e/(p-1)$, that is, $p^r \mid e/(p-1)$, but $p^{r+1} \nmid e/(p-1)$. We denote a root of unity of order p^s, with $s \in \mathbf{Z}_{\geq 1}$, by ζ_{p^s}. Note that if $\zeta_{p^s} \in F$, then $s \leq r + 1$. We set $q = p^f = |k|$. Let $\gamma \in \mathcal{O}$ such that $\mathcal{B} = \{1, \overline{\gamma}, \overline{\gamma}^2, \ldots, \overline{\gamma}^{f-1}\}$ is a basis of k over $\mathbf{F}_p$. Let π be a prime element of F, so $v(\pi) = 1$. We emphasize that we make a fixed choice of γ and π. As explained in the introduction, these elements are used to represent the elements of F. We define $u_0 \in \mathcal{O}^* = U$ by

$$p = -u_0\pi^e.$$

Set $\mu_{q-1} = \{x \in F : x^{q-1} = 1\}$.

Definition 2.1. The map $\omega : k^* \longrightarrow \mu_{q-1}$, such that $\omega(a)$ with $a \in k^*$ is the unique $(q-1)$-th root of unity with the property that $\omega(a) \equiv a \pmod{\mathfrak{m}}$, is called the *Teichmüller character* and $\omega(a)$ is called the *Teichmüller representative* of a. We also define $\omega(0) = 0$.

For the proof of the existence of the Teichmüller character we refer to [**21**, Ch. 3, section 4.4]. The map ω is a multiplicative, so for $a, b \in k$ we have $\omega(a)\cdot\omega(b) = \omega(a\cdot b)$.

Definition 2.2. A *digit* is an element of $\mathcal{O}$ of the form $\sum_{j=0}^{f-1} d_j\gamma^j \in \mathcal{O}$ with $d_j \in \mathbf{Z}$ and $0 \leq d_j < p$. The set of digits is denoted by $\mathcal{C}$. The digits represent the elements of the residue field of F, that is, the reduction map $\mathcal{C} \to k$ is a bijection.

Definition 2.3. Let $m \in \mathbf{Z}$ and $m = e\cdot h + l$ with h and l integers and $0 \leq l < e$. We define $\pi_m = \pi^l \cdot p^h \in F^*$. Note that $v(\pi_m) = m$.

Proposition 2.4. *Every element $x \in F^*$ can be represented by an expression of the form $\sum_{n=t}^{\infty} c_n\pi_n$ with $t \in \mathbf{Z}$, $c_n \in \mathcal{C}$ and $c_t \neq 0$. This representation is unique. Any element of the ring of integers $\mathcal{O}$ of F has a unique representation of the form $\sum_{n=0}^{\infty} c_n\pi_n$ with $c_n \in \mathcal{C}$.*

Proof. This is a standard fact of local fields. □

For each $i \in \mathbf{Z}_{\geq 1}$ we have $\mathbf{F}_p$-linear isomorphisms

$$\begin{aligned} \sigma_i : k &\to U_i/U_{i+1} \\ c &\mapsto \overline{1+\omega(c)\pi_i} \end{aligned}$$

and

$$\begin{aligned} \sigma_i' : k &\to U_i/U_{i+1} \\ c &\mapsto \overline{1+\omega(c)\pi^i}. \end{aligned}$$

Proposition 2.5.

i. *The sequence* $1 \to U_1 \to \mathcal{O}^* \to k^* \to 1$ *is exact and splits uniquely. The map* $U_1 \times k^* \to \mathcal{O}^*$ *with* $(v, w) \to v \cdot \omega(w)$ *is a group isomorphism.*
ii. *The sequence* $1 \to \mathcal{O}^* \to F^* \to \mathbf{Z} \to 0$ *is exact and every choice of a prime element gives a splitting.*
iii. *The multiplicative group* U_1 *is a* $\mathbf{Z}_p$*-module.*

Proof. (i) The inclusion map $U_1 \to \mathcal{O}^*$ is injective and the map $\mathcal{O}^* \to k^*$ is a surjection. A splitting $k^* \to \mathcal{O}^*$ has image in μ_{q-1} and one easily sees that the Teichmüller character splits the sequence uniquely. See also [**15**, Appendix].

(ii) Follows easily.

(iii) In [**9**, Teil II, section 15.2], expressions of the form η^g with $\eta \in U_1$ and $g \in \mathbf{Z}_p$ are defined as follows: $\eta^g = \lim_{n\to\infty} \eta^{g(n)}$ where $g(n)$ is a sequence of positive integers converging to g in $\mathbf{Z}_p$. One can prove that for every pair of principal units η_1 and η_2 and for every $g, g' \in \mathbf{Z}_p$ we have: $(\eta_1 \cdot \eta_2)^g = \eta_1^g \cdot \eta_2^g$ and $\eta^{g+g'} = \eta^g \cdot \eta^{g'}$ and finally $\eta^{gg'} = (\eta^g)^{g'}$. From this it follows that U_1 has a $\mathbf{Z}_p$-module structure. □

Corollary 2.6. *The map*

$$\begin{aligned} \mathbf{Z} \times k^* \times U_1 &\mapsto F^* \\ (M, c, u) &\mapsto \pi^M \cdot \omega(c) \cdot u \end{aligned}$$

is an isomorphism of groups.

Proof. This follows from Proposition 2.5. □

In order to do computations in the uncountable field F, one needs to approximate elements. Let $N \in \mathbf{Z}_{\geq 1}$. We set $\mathcal{O}_N = \mathcal{O}/\mathfrak{m}^N$, which is a finite ring of cardinality q^N. By abuse of notation, we often denote the reduction map $\mathcal{O} \to \mathcal{O}_N$ by $\bar{\ }$. We can write an element in $\mathcal{O}_N$ uniquely as $\sum_{h=0}^{N-1} c_h\pi_h$ (by abuse of notation), with $c_h \in \mathcal{C}$. We say that we approximate an element of $x \in \mathcal{O}$ in precision N if its reduction in $\mathcal{O}_N$ is given.

We remark that for $N \geq 1$ Corollary 2.6 induces isomorphisms $F^*/U_N \cong \mathbf{Z} \times \mathcal{O}_N^* \cong \mathbf{Z} \times k^* \times U_1/U_N$.

We use subscripts to stress which field we are working in. For example, $\mathcal{O}_F$ will denote the ring of integers of F.

Chapter 3

A computational model for local fields

1. Introduction

Let F be a finite extension of $\mathbf{Q}_p$. This is an uncountable field and hence it is not obvious how to do arithmetic in such a field. Just as in the field $\mathbf{R}$, we need to work with a 'precision' to make all our computations take place in finite sets. In this chapter, we answer the following questions:

- How can one represent F with a finite amount of data?
- How can one represent elements of F in a finite precision?
- How can one do basic arithmetic in F?

We answer the above questions, and compute bit complexities for many of the basic algorithms. In the next section, we discuss the main results. One can use these results as a black box for local fields. In the final section we answer the above questions.

In this chapter, we follow the notation of Chapter 2.

2. Main results

We will now discuss the conventions regarding the complexity of certain algorithms. The complexity of the algorithms below is given in bit complexity (not in terms of field operations in say $\mathbf{F}_p$). We usually use the big O notation, in the parameters e, f, p and N. We also use the $\tilde{O}$ notation as follows: here $h' \in \tilde{O}(h)$ means that there is an integer s such that $h' \in O(h \cdot (\log h)^s)$. In this thesis we use the following convention for complexity. If we write that the complexity is $O((N \log q)^{1[+1]})$ (or briefly just $(N \log q)^{1[+1]}$ in the tables below), it means that the complexity is $O((N \log q)^2)$ and also $\tilde{O}(N \log q)$. The faster complexity is usually obtained by using fast arithmetic.

Let $\mathbb{F}$ be a field, and $\mathcal{D}$ a basis of a finite dimensional vector space V over $\mathbb{F}$. If $T : V \to V$ is a linear map, we denote by $[T]_{\mathcal{D}}$ the matrix of T with respect to the basis $\mathcal{D}$. Furthermore, if $x \in V$ we denote by $[x]_{\mathcal{D}}$ the coordinates of x with respect to the basis $\mathcal{D}$. Finally, if $c \in \mathcal{O}_1$ we denote by $[\cdot c]_{\mathcal{B}}$ the matrix of the linear map $\cdot c : \mathcal{O}_1 \to \mathcal{O}_1$ with $x \to c \cdot x$ with respect to the basis $\mathcal{B}$. The ring of $n \times n$ matrices over a ring R is denoted by $\mathrm{Mat}_n(R)$.

Definition 3.1. Let F be a local field and let $N \in \mathbf{Z}_{\geq 1}$. A *model* of F in precision N is a finite sequence of bits that specifies the ring $\mathcal{O}_N$, together with a representation of its elements; such a representation is defined to be a bijection from a set of finite sequences of bits to $\mathcal{O}_N$.

We remark that all O-constants are absolute, in particular independent of F and N.

Theorem 3.2. *For every local field F and $N \in \mathbf{Z}_{\geq 1}$ there is a model of F in precision N such that the length of the sequence of bits that specifies $\mathcal{O}_N$ and the lengths of the sequences of bits that represent its elements are $O(N \log q)$, and such that one has the following algorithms for basic arithmetic:*

Algorithm	***Input***	***Output***	***Complexity***
Addition	$\mathcal{O}_N$, $x, y \in \mathcal{O}_N$	$x + y \in \mathcal{O}_N$	$N \log q$
Subtraction	$\mathcal{O}_N$, $x, y \in \mathcal{O}_N$	$x - y \in \mathcal{O}_N$	$N \log q$
Multiplication	$\mathcal{O}_N$, $x, y \in \mathcal{O}_N$	$x \cdot y \in \mathcal{O}_N$	$(N \log q)^{1[+1]}$
Powering	$\mathcal{O}_N$, $x \in \mathcal{O}_N$, $r \in \mathbf{Z}_{\geq 0}$	$x^r \in \mathcal{O}_N$	$\log(r+2)\cdot$ $(N \log q)^{1[+1]}$
Inversion	$\mathcal{O}_N$, $x \in \mathcal{O}_N^*$	$1/x \in \mathcal{O}_N$	$(N \log q)^{1[+1]}$
Division	$\mathcal{O}_N$, $x \in \mathcal{O}_N$, $y \in \mathcal{O}_N^*$	$x/y \in \mathcal{O}_N$	$(N \log q)^{1[+1]}$
Equality	$\mathcal{O}_N$, $x, y \in \mathcal{O}_N$	$\begin{cases} \text{True} & \textit{if } x = y \\ \text{False} & \textit{if } x \neq y \end{cases}$	$N \log q$
Unit?	$\mathcal{O}_N$, $x \in \mathcal{O}_N$	$\begin{cases} \text{True} & \textit{if } x \in \mathcal{O}_N^* \\ \text{False} & \textit{if } x \notin \mathcal{O}_N^* \end{cases}$	$N \log q$

One can obtain constants as follows:

Algorithm	***Input***	***Output***	***Complexity***
$0, 1, \pi, \gamma$	$\mathcal{O}_N$	$0, 1, \overline{\pi}, \overline{\gamma} \in \mathcal{O}_N$	$N \log q$
p, f, N	$\mathcal{O}_N$	p, f, N	$N \log q$
$N > e$?	$\mathcal{O}_N$	$\begin{cases} \text{True} & \textit{if } N > e \\ \text{False} & \textit{if } N \leq e \end{cases}$	$N \log q$
e	$\mathcal{O}_N$ *with* $N > e$	e	$N \log q$
$\mathcal{O}_M$	$\mathcal{O}_N$, $M \leq N$	$\mathcal{O}_M$	$N \log q$

Additionally, one has the following algorithms:

Algorithm	***Input***	***Output***	***Complexity***
Reducing	$\mathcal{O}_N$, $x \in \mathcal{O}_N$, $M \leq N$	$\mathcal{O}_M$, $\overline{x} \in \mathcal{O}_M$	$N \log q$
Lifting	$M \geq N$, $\mathcal{O}_M$, $\mathcal{O}_N$ $x \in \mathcal{O}_N$	$x' \in \mathcal{O}_M$ *with* $\overline{x'} = x$	$M \log q$
σ_{N-1}^{-1}	$\mathcal{O}_N$ *with* $N \geq 2$, $x \in \mathcal{O}_N \cap \overline{U_{N-1}}$	$\mathcal{O}_1$, $\sigma_{N-1}^{-1}(x) \in \mathcal{O}_1$	$N \log q$
σ_{N-1}	$\mathcal{O}_N$ *with* $N \geq 2$, $c \in \mathcal{O}_1$	$\sigma_{N-1}(c) \in \mathcal{O}_N$	$N \log q$
u_0	$\mathcal{O}_N$ *with* $N > e$	$\mathcal{O}_{N-e}$, $\overline{u_0} \in \mathcal{O}_{N-e}$	$N \log q+$ $((N-e)\log q)^{1[+1]}$
Teichmüller	$\mathcal{O}_N$, $c \in \mathcal{O}_1$	$\overline{\omega(c)} \in \mathcal{O}_N$	$\big(N + ((N/e)\log q)^{1[+1]}\big)\cdot$ $\log q$

Furthermore, one has the following algorithms regarding $k = \mathcal{O}_1$:

Algorithm	***Input***	***Output***	***Complexity***
$[x]_{\mathcal{B}}$	$\mathcal{O}_1,\ x \in \mathcal{O}_1$	$(a_b)_{b\in\mathcal{B}} \in \mathbf{F}_p^f$ *s.t.* $x = \sum_{b\in\mathcal{B}} a_b b$	$\log q$
$[\cdot c]_{\mathcal{B}}$	$\mathcal{O}_1,\ c \in \mathcal{O}_1$	$[\cdot c]_{\mathcal{B}} \in \mathrm{Mat}_f(\mathbf{F}_p)$	$f(\log q)^{1[+1]}$
$[x \mapsto x^p]_{\mathcal{B}}$	$\mathcal{O}_1$	$[x \mapsto x^p]_{\mathcal{B}} \in \mathrm{Mat}_f(\mathbf{F}_p)$	$(f + \log p)(\log q)^{1[+1]}$

The proof of the above theorem can be found in Section 4.

Remark 3.3. Given a model $\mathcal{O}_N$, it is not the case that we can reconstruct F up to isomorphism. For example, if $N \le e$ the ring $\mathcal{O}_N$ can come from different fields with different e. If N is big enough, then at least the isomorphism class of the field F is uniquely determined (Lemma 3.6). Hence properties of F can be read off from $\mathcal{O}_N$ for large enough N.

Let us explain how we handle the non-uniqueness of F in certain algorithms. One of the algorithms outputs $\overline{u_0} \in \mathcal{O}_{N-e}$, when given $\mathcal{O}_N$ with $N > e$ as input. Note that in this specific algorithm, we lose some precision. This means that our algorithm computes $\overline{u_0}$, and that the answer does not depend on the possible choice of F giving rise to $\mathcal{O}_N$.

Remark 3.4. Once we can work with the rings $\mathcal{O}_N$, we can also work with F^*/U_N for any $N \in \mathbf{Z}_{\ge 1}$ as follows. By Corollary 2.6 one has $F^*/U_N \cong \mathbf{Z} \times \mathcal{O}_N^* \cong \mathbf{Z} \times k^* \times U_1/U_N$. Furthermore, we have an inclusion $U_1/U_N \to \mathcal{O}_N$. If $x = \pi^M \omega(c) v \pmod{U_N}$ corresponds to the (M, c, v), and y corresponds to (M', c', v'), then xy corresponds to $(M + M', cc', vv')$. The complexity of various operations, such as multiplication, now directly follows from the complexity of the operations in Theorem 3.2. With operations like addition, one has to be careful, since precision might be lost. Later in this thesis we usually work in quotients $F^*/(F^*)^m$, which are actually finite groups and hence we will not spend too much time on working out complexities for F^*/U_N.

3. Representing local fields

In this section we explain which data are used to represent a local field, and this will later motivate our construction for representing $\mathcal{O}_N$. We make use of two propositions, the first of which reads as follows.

Proposition 3.5. *Let p be a prime number, e and f positive integers and let $g \in \mathbf{Z}_p[X]$ and $h \in \mathbf{Z}_p[X, Y]$ be polynomials with the following properties.*

i. *g is monic in X of degree f and irreducible modulo p.*

ii. *h has the form*

$$h = Y^e + \sum_{j=0}^{f-1} \sum_{i=0}^{e-1} h_{ij} X^j Y^i$$

with $h_{ij} \in p\mathbf{Z}_p$ for all i, j and $h_{0j} \notin p^2\mathbf{Z}_p$ for at least one j.

Then $F = \mathbf{Q}_p[X, Y]/(g, h)$ is a field, and $F/\mathbf{Q}_p$ has ramification index e and residue class degree f and $E = \mathbf{Q}_p[X]/(g)$ is the largest unramified subfield of F. One has $\mathcal{O}_E = \mathbf{Z}_p[X]/(g)$ and $\mathcal{O}_F = \mathbf{Z}_p[X, Y]/(g, h)$. Finally, set $\gamma = \overline{X}$ and $\pi = \overline{Y}$. Then π

is a prime element of F and $\mathcal{B} = \{1, \overline{\gamma}, \ldots, \overline{\gamma}^{f-1}\}$ forms a basis of the residue field of F over $\mathbf{F}_p$.

Proof. The ideal (g) is a prime ideal in $\mathbf{Q}_p[X]$ because g is irreducible modulo p. It follows that $E = \mathbf{Q}_p[X]/(g)$ is a field. This field E is an unramified extension of $\mathbf{Q}_p$ of degree f (see [**24**, section 3.2, Theorem 3–2–6]. The field E has $\mathcal{O}_E = \mathbf{Z}_p[\gamma] \cong \mathbf{Z}_p[X]/(g)$ as its ring of integers (see [**24**, Ch. 3, section 3–2, Theorem 3–2–6(ii)]). The polynomial $h(\gamma, Y) \in E[Y]$ is an Eisenstein polynomial, so $F = E[Y]/(h)$ is a field. The field extension F/E is totally ramified of degree e (see [**24**, Theorem 3–3–1]). The field F has $\mathcal{O}_F = \mathcal{O}_E[\pi] = \mathbf{Z}_p[\gamma, \pi]$ as ring of integers (see [**24**, Ch. 3, Corollary 3–3–2]). So we have $\mathcal{O}_F = \mathbf{Z}_p[X, Y]/(g, h)$. Finally, π is a prime element of F (see [**24**, Ch. 3, section 3-3, Theorem 3–3–1(ii)]). The last statement follows easily (see [**24**, Ch. 3, Theorem 3-2-6]). □

We will now show that any local field F can be represented as in Proposition 3.5, and that we can make the defining coefficients small. Before we state and prove the second proposition we treat a lemma. We will alter apply the lemma below to $E = \mathbf{Q}_p[X]/(g)$ from Proposition 3.5.

Lemma 3.6. *Suppose the field E is an unramified extension of $\mathbf{Q}_p$ and h_1 and h_2 are monic Eisenstein polynomials of degree e in $\mathcal{O}_E[Y]$ where $\mathcal{O}_E$ is the ring of integers of E. Suppose further that l is the largest positive integer such that $p^l \mid (p \cdot e)^2$. Then, if $p^l \mid h_1 - h_2$, we have $E[Y]/(h_1) \cong E[Y]/(h_2)$.*

Proof. Suppose $\pi \in \overline{E}$, an algebraic closure of E, is a zero of the polynomial h_1. Since h_1 is Eisenstein, π is a prime element of $E(\pi)$.

First we will prove that $\mathrm{ord}_{E(\pi)} h_2(\pi) > 2 \cdot \mathrm{ord}_{E(\pi)} h_2'(\pi)$ where h_2' denotes the derivative of h_2. Since $p^l \mid h_1 - h_2$, we have

$$\mathrm{ord}_{E(\pi)} h_2(\pi) = \mathrm{ord}_{E(\pi)} (h_2 - h_1)(\pi) \geq e \cdot l.$$

Further we have

$$\mathrm{ord}_{E(\pi)} h_2'(\pi) \leq \mathrm{ord}_{E(\pi)} (e \cdot \pi^{e-1}),$$

because all terms of $h_2'(\pi)$ that are unequal to zero have different valuations. Hence we have

$$\begin{aligned} 2 \cdot \mathrm{ord}_{E(\pi)} h_2'(\pi) &\leq 2e \cdot \mathrm{ord}_p(e) + 2(e-1) \\ &< 2e \cdot (\mathrm{ord}_p(e) + 1) = 2e \cdot \mathrm{ord}_p(pe) \\ &= e \cdot l \leq \mathrm{ord}_{E(\pi)} h_2(\pi). \end{aligned}$$

With Newton's method and π as initial value we can now compute a zero π^* of h_2 in $E(\pi)$ (see [**24**, section 3-1]). We have $E(\pi^*) \subset E(\pi)$. Because the polynomials h_1 and h_2 are irreducible of the same degree, we conclude that the field extensions $E(\pi)/E$ and $E(\pi^*)/E$ have the same degree too. So $E(\pi) = E(\pi^*)$. This proves the assertion. □

The second proposition gives not only the converse of Proposition 3.5 but also includes the statement that we may choose the coefficients of g and h from a bounded interval in $\mathbf{Z}$ instead of from $\mathbf{Z}_p$.

Proposition 3.7. *Let p be a prime number and F a finite extension of $\mathbf{Q}_p$ with ramification index e and residue class degree f. Suppose l is the largest positive integer for which p^l divides $(pe)^2$. Then there exist polynomials $g \in \mathbf{Z}[X]$ and $h \in \mathbf{Z}[X,Y]$ such that*

i. *g is monic in X of degree f and irreducible modulo p, and the coefficients g_i of g satisfy $0 \le g_i \le p-1$,*
ii. *h has the form*
$$h = Y^e + \sum_{j=0}^{f-1}\sum_{i=0}^{e-1} h_{ij}X^jY^i$$
with $h_{ij} \in p\mathbf{Z}$ and $0 \le h_{ij} \le p^l - 1$ for all i,j, and $h_{0j} \notin p^2\mathbf{Z}$ for at least one j,
iii. *$F \cong \mathbf{Q}_p[X,Y]/(g,h)$.*

Proof. Let $g = \sum_{i=0}^{f} g_iX^i \in \mathbf{Z}_p[X]$ of degree f which is irreducible modulo p and satisfies condition (i) (such g exists by the theory of finite fields). It is well known that the maximal unramified subextension E of F is isomorphic to $\mathbf{Q}_p[X]/(g)$. Fix such an isomorphism. Then pick a prime element π of F and note that $E(\pi) = F$. Consider the minimum polynomial of π over E, viewed over $\mathbf{Q}_p[X]/(g)$. This minimum polynomial h is an Eisenstein polynomial of the form as in (ii), except that the h_{ij} are in $p\mathbf{Z}_p$. Apply Lemma 3.6 to replace h with a polynomial of the required form. □

Examples 3.8. The following example of a field F illustrates how we present a field. Let $F \supset \mathbf{Q}_2$ be the field given by the triple $(p,g,h) = (2, X^2+X+1, Y^2-(2+2X)Y-2X)$. We denote the unramified part of F by $E = \mathbf{Q}_2(\gamma)$, where γ is a zero of $g(X) = X^2+X+1$. If we adjoin a zero of the Eisenstein polynomial $h(\gamma, Y)$ to E we obtain our field F, which is a totally ramified extension of E. Throughout this thesis we give examples where F is the field from this example.

If we choose a prime number p and polynomials $g = X$ and $h = Y - p$, we obtain the field $F_1 = \mathbf{Q}_p$.

The next example shows that one may naturally encounter polynomials that do not satisfy the conditions on their coefficients. Let F_2 be the cyclotomic field $\mathbf{Q}_p(\zeta_{p^k})$, with k a positive integer. This extension is totally ramified of degree $e = p^{k-1}(p-1)$ and $\zeta_{p^k} - 1$ is a prime element. The integer l from Proposition 3.7 satisfies $l = 2k$. One has $F \cong \mathbf{Q}_p[X]/(g,h)$ where $g(X) = X$ and
$$h(Y) = \frac{(Y+1)^{p^k}-1}{(Y+1)^{p^{k-1}}-1} = \sum_{i=0}^{p-1}(Y+1)^{ip^{k-1}} = Y^e + \ldots + (\sum_{j=0}^{p-1} jp^{k-1})Y + p.$$
For almost all pairs (p,k), the coefficient of the term of the polynomial h with $Y^{\frac{e}{2}}$ (if $p \ne 2$ or $k > 1$) fails to satisfy the inequality from Proposition 3.7ii. This is illustrated by choosing for example $p = 2$ and $k = 5$ because then the coefficients of the terms Y^t of $h(Y)$ with $4 \le t \le 12$ are bigger than $2^{10} - 1$.

Remark 3.9. Let p, g, h and F be as in Proposition 3.7. Furthermore let d be the extension degree of the field F over $\mathbf{Q}_p$ and let L be the bit length of p, g, and h. Then we have

i. $L \geq d$.
ii. $L = O(d \log(pd))$.
iii. $L = O(d \log(2d))$ if F contains a primitive p-th root of unity.

Assertion (i) follows from the fact that we have to write down h and for each of its $d+1$ coefficients at least one bit is needed.

The f coefficients of the polynomial g can be written down in at most $f \cdot \log_2 p \leq d \cdot \log_2 p$ bits. The coefficients of the polynomial h are integers in the interval $[0, p^l - 1]$ with l as in Proposition 3.7. Hence h can be written down using at most $O(e \cdot f \cdot \log(p^l)) \leq O(d \cdot \log((pe)^2)) \leq O(d \cdot \log((pd)^2)) = O(d \cdot \log(pd))$ bits. Because the prime number p can be written down by $O(\log p)$ bits, we obtain the inequality $L = O(d \log(pd))$ bits. This proves assertion (ii).

If F contains a primitive p-th root of unity we have $d = [F : \mathbf{Q}_p] \geq p - 1$ and so $p \leq d + 1 \leq 2d$. If we take this into account, we obtain $L = O(d \log(2d))$. This proves assertion (iii).

4. Proof of main theorem

4.1. Representing $\mathcal{O}_N$ and its elements. Let F be a local field and let $N \in \mathbf{Z}_{\geq 1}$. Let us now discuss the data which define $\mathcal{O}_N = \mathcal{O}/\mathfrak{m}^N$. We call N the *precision* of the ring $\mathcal{O}_N$. Note that F can be given as in Proposition 3.5 by a triple (p, g, h), and we will define $\mathcal{O}_N$ with only a part of this information. Recall that $g \in \mathbf{Z}[X]$ and $h = Y^e + \sum_{j=0}^{f-1} \sum_{i=0}^{e-1} h_{ij} X^j Y^i \in \mathbf{Z}[X, Y]$.

The data for $\mathcal{O}_N$ for $N \geq 1$ are the following. The first part of the data is p and N. The second part of the information is a bit telling whether $N \leq e$ or $N > e$.The third part of the data is

$$g_N \equiv g \pmod{p^{\lceil \frac{N}{e} \rceil}} \in \left(\mathbf{Z}/p^{\lceil \frac{N}{e} \rceil}\mathbf{Z}\right)[X]$$

(if $N \leq e$, this is a polynomial in $(\mathbf{Z}/p\mathbf{Z})[X]$). Additionally, if $N > e$, we are given:

$$h_N \equiv h \pmod{p^{\lceil \frac{N}{e} \rceil}} = Y^e + \sum_{j=0}^{f-1} \sum_{i=0}^{e-1} h_{ij} X^j Y^i \bmod p^{\lceil \frac{N}{e} \rceil} \in \left(\mathbf{Z}/p^{\lceil \frac{N}{e} \rceil}\mathbf{Z}\right)[X, Y].$$

Proposition 3.10. *One has:*

$$\mathcal{O}_N \cong \mathbf{Z}_p[X, Y]/(g, h, Y^N) \cong \begin{cases} \left(\mathbf{Z}/p^{\lceil \frac{N}{e} \rceil}\mathbf{Z}\right)[X, Y]/(g_N, h_N, Y^N) & \textit{if } N > e \\ (\mathbf{Z}/p\mathbf{Z})[X, Y]/(g_N, Y^N) & \textit{if } N \leq e \end{cases}$$

Proof. The first isomorphism follows since $\overline{Y}$ is a prime element. The second isomorphism follows since we know that $p^{\lceil \frac{N}{e} \rceil} \in \mathfrak{m}^N$. Note that in the second case h_N is already in the ideal generated by g_N and Y^N. □

The data representing $\mathcal{O}_N$ in all cases have $O(N \log q)$ bits.

We will now discuss how elements of $\mathcal{O}_N$ are represented. Let π be the class of Y and γ be the class of X in $\mathcal{O}_N$. Note that any $x \in \mathcal{O}_N$ can be written uniquely as $\sum_{i=0}^{N-1} c_i \pi_i$ (recall Definition 2.3) with $c_i \in \mathcal{C}$, that is, we write $c_i = \sum_{j=0}^{f-1} d_{ij} \gamma^j$ with $0 \leq d_{ij} < p$. This is how we represent elements of $\mathcal{O}_N$ in $O(N \log q)$ bits.

4.2. Algorithms for a local field. In this section, we will explain the algorithms in Theorem 3.2. We assume that $\mathcal{O}_N$ is given as in the previous subsection, in $O(N \log q)$ bits. Hence elements in $\mathcal{O}_N$ are written as $\sum_{h=0}^{N-1} c_h \pi_h$ with $c_h \in \mathcal{C}$ and take up $O(N \log q)$ bits.

REMARK 3.11. In the rest of this thesis, we use that we can compute determinants and reduced row echelon forms, basis of kernel, cokernel, inverse, image of an $n \times n$ matrix over $\mathbf{F}_p$ in complexity $n^C (\log p)^{1[+1]}$, with $2 \leq C < 3$, where C is a "feasible matrix multiplication exponent"(see [**8**, Chapter 12], section 1).

Furthermore, we will use that we can do addition and subtraction in $\mathbf{Z}/p^m\mathbf{Z}$ in $O(\log(p^m))$ bit operations and multiplication and inversion in time $O((\log(p^m))^{1[+1]})$ bit operations (see [**8**, Chapter 5]).

Finally, we can compute determinants of $n \times n$ matrices over $\mathbf{Z}/p^m\mathbf{Z}$ in time $n^3 (\log(p^m))^{1[+1]}$ (by using row reductions). The latter can be improved, but we leave this to the reader.

The next lemma treats the complexity of some of the easy algorithms in Theorem 3.2.

LEMMA 3.12. *There algorithms for the following entries Theorem 3.2 run in the time as in Theorem 3.2:*

- *Equality;*
- *Unit?;*
- $0, 1, \pi, \gamma$*;*
- p, f, N*;*
- $N > e$*?;*
- e*;*
- $\mathcal{O}_M$*.*

PROOF. Only two algorithms require an explanation. For 'Unit?', an element $x = \sum_{h=0}^{N-1} c_h \pi_h \in \mathcal{O}_N$ is a unit if and only if $c_0 \neq 0$. For '$\mathcal{O}_M$', reduce the equations of $\mathcal{O}_N$ modulo the right power of p to obtain the model of $\mathcal{O}_M$. □

We have some other easy algorithms.

LEMMA 3.13. *There algorithms for the following entries Theorem 3.2 run in the time as in Theorem 3.2:*

- *Reducing;*
- *Lifting;*
- σ_{N-1}^{-1}*;*
- σ_{N-1}*.*

PROOF. Lifting and reducing are easy. The map σ_{N-1}^{-1} just sends $1 + c_{N-1}\pi_{N-1}$ to c_{N-1}. The map σ_{N-1} sends c to $1 + c\pi_{N-1}$. □

The next Lemma summarizes the discussion in [**8**, Chapter 2], on arithmetic operations in polynomial rings.

Lemma 3.14. *Let R be a finite ring whose elements can be represented as finite sequences of bits and for which there are algorithms for the operations addition, subtraction and multiplication. Let $z \in R[T]$ be a monic polynomial of degree l. If an upper bound for the number of bit operations of an addition/subtraction and a multiplication in R is respectively denoted by t and u, then an addition/subtraction and a multiplication in $R[T]/(z)$, can be performed in respectively $O(lt)$ and $O(l^{1[+1]}(t+u))$ bit operations.*

Proof. It is an easy verification that adding two elements of $R[T]/(z)$ comes down to l additions in R or $O(lt)$ bit operations. A multiplication of two elements of $R[T]/(z)$ requires $O(l^2)$ multiplications and additions of elements of R or $O(l^2(t+u))$ bit operations. Moreover the result of such a multiplication is a polynomial of degree at most $2l-2$ which is reduced by polynomial division by z. This division requires $l(l-1)(t+u)$ bit operations. Therefore the total cost of a multiplication in $R[T]/(z)$ is $O(l^2(t+u))$ bit operations. Using fast arithmetic one can reduce the factor l^2 in the runtime to $l^{1[+1]}$. □

The above lemma and its proof give a (standard) algorithm for computing in quotient rings and we apply this algorithm in our situation. We get the following result.

Proposition 3.15. *There is an algorithm which on input $x, y \in \mathcal{O}_N$ computes $x+y \in \mathcal{O}_N$ and $x-y \in \mathcal{O}_N$ in time $O(N\log q)$, and $x \cdot y \in \mathcal{O}_N$ in time $O((N\log q)^{1[+1]})$.*

Proof. Recall that

$$\mathcal{O}_N = \begin{cases} \left(\mathbf{Z}/p^{\lceil \frac{N}{e} \rceil}\mathbf{Z}\right)[X,Y]/(g_N, h_N, Y^N) & \text{if } N > e \\ \mathbf{Z}/p\mathbf{Z}[X,Y]/(g_N, Y^N) & \text{if } N \leq e. \end{cases}$$

In the second case, we can apply Lemma 3.14 twice to obtain the result.

In the first case, the situation is a bit trickier. We consider the ring

$$\mathcal{O}_{e\lceil \frac{N}{e} \rceil} = \left(\mathbf{Z}/p^{\lceil \frac{N}{e} \rceil}\mathbf{Z}\right)[X,Y]/(g_N, h_N, Y^{e\lceil \frac{N}{e} \rceil}) = \left(\mathbf{Z}/p^{\lceil \frac{N}{e} \rceil}\mathbf{Z}\right)[X,Y]/(g_N, h_N).$$

Lemma 3.14 allows us to do addition in time $O(N\log q)$ and multiplication in time $O((N\log q)^{1[+1]})$. Truncating the computations (reducing modulo Y^N, i.e. throwing away terms of the form $c_i\pi_i$ when $i \geq N$) allows us to do computations in $\mathcal{O}_N$ in the required time. □

Using repeated squaring, one can now compute the powers ('powering') of elements in $\mathcal{O}_N$ in the stated time.

We will now discuss an algorithm for computing inverses, with the help of a Newton iteration.

Algorithm 3.16 (Inverses).
Input: $u \in \mathcal{O}_N^*$.
Output: $u^{-1} \in \mathcal{O}_N$.
Steps:

```
i. Set $\overline{u} \in \mathcal{O}_1$.
ii. Compute $v_0 = \overline{u}^{-1} \in \mathcal{O}_1$ with the extended Euclidean algorithm.
```

iii. Compute $v_i \in \mathcal{O}_{\min(2^i,N)}$ for $1 \le i \le \lceil \log_2 N \rceil = j$ by $v_i = v'_{i-1} \cdot (2 - u \cdot v'_{i-1}) \in \mathcal{O}_{\min(2^i,N)}$ where v'_{i-1} is a lift of v_{i-1} to $\mathcal{O}_{\min(2^i,N)}$.
iv. Return $v = v_j \in \mathcal{O}_N$.

Proposition 3.17. *Algorithm 3.16 is correct and has bit complexity* $O((N \log q)^{1[+1]})$.

Proof. Computing $\overline{u}$ costs $O(N \log q)$ by Lemma 3.13. Applying the extended Euclidean Algorithm costs $O((\log q)^{1[+1]})$ bit operations. We refer to [**8**, Corollary 4.6] for this. In [**8**, Theorem 9.2] we find the proof that we can compute the inverse of a unit u by applying Newton iteration to the expression $f(x) = \frac{1}{ux} - 1$. The iteration gives the formula as in step iii and v_i is the inverse of u modulo $\mathfrak{m}^{\min(N,2^i)}$. The complexity of step iii is $O(\sum_{i=1}^{\lceil \log_2 N \rceil} (\min(2^i, N) \cdot \log q)^{1[+1]}) = O((N \log q)^{1[+1]})$ (Proposition 3.15, Lemma 3.13). This gives the required complexity. □

Note that for $x \in \mathcal{O}_N$, $y \in \mathcal{O}_N^*$ one has $x/y = x \cdot 1/y$. Hence we can now do division in the claimed time as well.

Recall that u_0 is defined by $p = -u_0 \pi^e$.

Algorithm 3.18 (u_0).
Input: $\mathcal{O}_N$ with $N > e$.
Output: $\overline{u_0} \in \mathcal{O}_{N-e}$.
Steps:

i. Compute $w = \sum_{i=0}^{e-1} \sum_{j=0}^{f-1} \frac{h_{ij}}{p} \gamma^j \pi^i \in \mathcal{O}_{N-e}$.
ii. Return $\overline{u_0} = w^{-1}$.

Proposition 3.19. *Algorithm 3.18 is correct and its complexity is* $O(N \log q + ((N-e) \log q)^{1[+1]})$.

Proof. If $h = Y^e + \sum_{j=0}^{f-1} \sum_{i=0}^{e-1} h_{ij} X^j Y^i$, then one has

$$1/u_0 = -\pi^e/p = \sum_{i=0}^{e-1} \sum_{j=0}^{f-1} \frac{h_{ij}}{p} \gamma^j \pi^i.$$

This formula allows us to compute $1/\overline{u_0} \in \mathcal{O}_{N-e}$ in time $O(N \log q)$ (we lose precision because of the division by p). We then invert $1/\overline{u_0}$ to get $\overline{u_0}$ in time $O(((N-e) \log q)^{1[+1]})$ (Algorithm 3.16).

□

Let us now discuss the complexity of the algorithms regarding the field k.

Lemma 3.20. *There are algorithms for* $[x]_{\mathcal{B}}$, $[\cdot c]_{\mathcal{B}}$ *and* $[x \mapsto x^p]_{\mathcal{B}}$ *as in Theorem 3.2 which run in the times as stated in Theorem 3.2.*

Proof. Since we work with digits, $[x]_{\mathcal{B}}$ is easy to compute.

To compute $[\cdot c]_{\mathcal{B}}$, we compute $c\overline{\gamma}^i$ for $i = 0, \ldots, f-1$ using f multiplications in $\mathcal{O}_1 = k$, in time $f(\log q)^{1[+1]}$. After that we compute $[c\overline{\gamma}^i]_{\mathcal{B}}$ for $i = 0, \ldots, f-1$ in time $f \log q$.

To compute $[x \mapsto x^p]_{\mathcal{B}}$, one raises $\overline{\gamma}$ to the p-th power and then compute $(\overline{\gamma}^p)^i$ for $i = 0, 1, \dots, f-1$. This requires $f + \log p$ multiplications in k and this costs $O((f + \log p)(\log q)^{1[+1]})$. □

Let us finally discuss how to do Teichmüller lifts. To compute $\omega(c) \in \mathcal{O}_N$, it suffices to do computations in the unramified part E of F, that is, in the ring

$$\mathcal{O}_{E,\lceil \frac{N}{e} \rceil} = \left(\mathbf{Z}/p^{\lceil \frac{N}{e} \rceil}\mathbf{Z}\right)[X]/(g_N) = \left(\mathbf{Z}/p^{\lceil \frac{N}{e} \rceil}\mathbf{Z}\right)[X,Y]/(g_N, Y-p) \subseteq \mathcal{O}_N.$$

Algorithm 3.21 (Teichmüller).
Input: $\underline{c \in \mathcal{O}_1}$.
Output: $\overline{\omega(c)} \in \mathcal{O}_N$.
Steps:

i. If $c = 0$ or $N \leq e$ return $\sum_{h=0}^{N-1} c_h \pi_h$ with $c_0 = c$ and $c_h = 0$ for $1 \leq h \leq N-1$ and terminate.
ii. Compute $(1-q)^{-1} = \sum_{i=0}^{\lceil \frac{N}{ef} \rceil - 1} p^{if} \in \mathcal{O}_{E,\lceil \frac{N}{e} \rceil}$.
iii. Put $x_0 = c \in k$ and for $1 \leq i \leq \lceil \log_2(N/e) \rceil = l$ compute $x_i = \frac{x'^q_{i-1} - q x'_{i-1}}{1-q} \in \mathcal{O}_{E,\min(2^i, N/e)}$ where x'_{i-1} is a lift of x_{i-1} to $\mathcal{O}_{E,\min(2^i,N/e)}$.
iv. Return $x_l \in \mathcal{O}_{E,\lceil \frac{N}{e} \rceil} \subset \mathcal{O}_N$.

Proposition 3.22. *Algorithm 3.21 is correct and its bit complexity is* $O\left(\left(N + ((N/e)\log q)^{1[+1]}\right) \cdot \log q\right)$.

Proof. If $N \leq e$ or $c = 0$, then $\overline{\omega(c)}$ is a lift of c to $\mathcal{O}_N$, which can be computed in time $O(N \log q)$. If $N > e$ step ii costs $O((N/e)\log q)$, step iv costs $O(N \log q)$ and the complexity of this algorithm is dominated by the third step. For the Newton iteration procedure with $x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$ we choose $f(x) = 1 - x^{1-q}$ and obtain the formula of the third step of the algorithm. In every step the precision doubles so x_{i+1} is computed modulo $p^{2^{i+1}}$. The complexity of the last iteration x_l of the third step of Algorithm 3.21 dominates the cost of all the other iterations together and for this iteration we compute a q-th power requiring $O(((N/e)\log q)^{1[+1]} \cdot \log q)$ bit operations. The rest of this step has smaller complexity.

We conclude that Algorithm 3.21 has a complexity of $O\big(\big(N + ((N/e)\log q)^{1[+1]}\big) \cdot \log q)$ bit operations. □

Chapter 4

On the structure of the unit group

1. Introduction

Let F be a finite extension of $\mathbf{Q}_p$. In this chapter we solve the following problems:

- When is $\zeta_p \in F^*$?
- What is the maximal s such that $\mu_{p^s} \subset F^*$, and how can we find $\zeta_{p^s} \in F^*$?

We will read off the answer to the first question from $\overline{u_0}$. To solve the second problem, we develop the theory of exponential representations. Moreover we will prove Theorem 1.2 and we introduce the group morphism χ, which plays an important role in our algorithms to compute the norm residue symbol.

2. Theory

Let F be a finite extension of $\mathbf{Q}_p$. We follow the notation of Chapter 2. The main problem of this section is to determine the structure of $U = \mathcal{O}^*$. The map $k^* \times U_1 \to U$, $(c, u) \mapsto \omega(c)u$ is an isomorphism (Proposition 2.5i). The finite group k^* is cyclic of order $q - 1$. Furthermore, one easily sees that U_1 is a $\mathbf{Z}_p$-module (Proposition 2.5iii). We denote by $\overline{F}$ an algebraic closure of F and for an integer $n \in \mathbf{Z}_{\geq 1}$ we set $\mu_n = \{x \in \overline{F} : x^n = 1\}$. We first detect if there is torsion in U_1, or equivalently, if μ_p is contained in F.

2.1. Detecting ζ_p. Recall that $u_0 \in \mathcal{O}^*$ is defined by $p = -u_0\pi^e$. Let us look at the p-th power map

$$\begin{aligned} U_1 &\to U_1 \\ x &\mapsto x^p. \end{aligned}$$

Take $1 + a \in U_i \setminus U_{i+1}$ with $a \in \mathfrak{m}^i \setminus \mathfrak{m}^{i+1}$. Then one has:

$$(1 + a)^p - 1 = a^p + pa^{p-1} + \ldots + pa.$$

The terms have valuation $pi, e + (p-1)i, e + (p-2)i, \ldots, e + i$ and the smallest value is among pi and $e + i$. Note that $pi \leq e + i$ iff $i \leq e/(p-1)$. Set

$$\rho(i) = \min\{pi, e + i\}.$$

Then for each $i \in \mathbf{Z}_{\geq 1}$ the p-th powering map gives a map $U_i \longrightarrow U_{\rho(i)}$, which we denote by κ_i. Note that any $j \in \mathbf{Z}_{\geq 1}$ can uniquely be written as $j = \rho^m(i)$ for some $m \in \mathbf{Z}_{\geq 0}$ and $1 \leq i < pe/(p-1)$, $p \nmid i$. For $j \in \mathbf{Z}_{\geq 1}$ we set $z(j) = (m, i)$ if $j = \rho^m(i)$.

For $i \geq 1$ we have the $\mathbf{F}_p$-linear map

$$\begin{aligned} \tau_i : U_i/U_{i+1} \to & U_{\rho(i)}/U_{\rho(i)+1} \\ \overline{v} \mapsto & \overline{v^p}. \end{aligned}$$

Recall for $i \in \mathbf{Z}_{\geq 1}$ we have $\mathbf{F}_p$-linear isomorphisms $\sigma_i' : k \to U_i/U_{i+1}$ defined by $c \mapsto \overline{1 + \omega(c)\pi^i}$. The above computations give us the following lemma.

Lemma 4.1. *For $x \in k$ one has*

$$k \ni \sigma_{\rho(i)}'^{-1} \circ \tau_i \circ \sigma_i'(x) = \begin{cases} x^p & \text{if } i < e/(p-1) \\ -\overline{u_0}x & \text{if } i > e/(p-1) \\ x^p - \overline{u_0}x & \text{if } i = e/(p-1). \end{cases}$$

From the above lemma we see that τ_i is an isomorphism of $\mathbf{F}_p$-vector spaces if $i \neq e/(p-1)$.

Remark 4.2. Let $i > e/(p-1)$. One can show that the map

$$\begin{aligned} \mathcal{O} &\to U_i \\ x &\mapsto \exp(\pi^i x) = \sum_{j \geq 0} (\pi^i x)^j / j! \end{aligned}$$

is an isomorphism of $\mathbf{Z}_p$-modules, with the inverse given by a logarithm map. It turns out to be slightly more subtle to understand the group U_1, since it might contain torsion.

Proposition 4.3. *Let $F \supset \mathbf{Q}_p$ be a local field. Then the following holds:*

i. *$\mu_p \subset F$ if and only if $p-1 \mid e$ and $N_{k/\mathbf{F}_p}(\overline{u_0}) = 1$.*
ii. *For all $i > e/(p-1)$ the p-th powering map $\kappa_i : U_i \longrightarrow U_{i+e}$ is an isomorphism, and if $\mu_p \not\subset F$, then κ_i is an isomorphism for all $i \geq e/(p-1)$*
iii. *$\mu_p \subset F$ if and only if $p-1 \mid e$ and $\tau_{e/(p-1)}$ has a kernel and a cokernel that are one-dimensional vector spaces over $\mathbf{F}_p$.*
iv. *All the maps τ_i are isomorphisms if and only if $\mu_p \not\subset F$.*

Proof. (i) If we identify the domain and codomain of $\tau_{e/(p-1)}$ with k, the corresponding map sends x to $x^p - \overline{u_0}x$ (Lemma 4.1). The equation $X^p - \overline{u_0}X = 0$ has a nonzero solution in k if and only if $\overline{u_0} \in (k^*)^{p-1}$ if and only if $N_{k/\mathbf{F}_p}(\overline{u_0}) = 1$. Note that if $\operatorname{ord}(\zeta_p - 1) = i$, the p-th powering map $\tau_i : U_i/U_{i+1} \longrightarrow U_{\rho(i)}/U_{\rho(i)+1}$ gives $\tau_i(\overline{\zeta_p}) = 1$, so τ_i is not an isomorphism. Hence we have $i = \frac{e}{p-1}$ and $p-1 \mid e$.

(ii) Let $i > e/(p-1)$. Then the p-th power map $U_i/U_{i+1} \to U_{i+e}/U_{i+e+1}$ is an isomorphism. With induction, one shows that for $j > i$ the map $U_i/U_j \to U_{i+e}/U_{j+e}$ is an isomorphism. By taking a projective limit, this shows that $\kappa_i : U_i \to U_{i+e}$ is an isomorphism. If $\mu_p \not\subset F$ and $p-1 \mid e$, the map $\kappa_{e/(p-1)}$ is an isomorphism so in that case κ_i is an isomorphism for all $i \geq e/(p-1)$.

(iii) One has the following commutative diagram with exact rows, where all vertical maps are p-th powering maps:

$$\begin{tikzcd}
1 \arrow[r] & U_{e/(p-1)+1} \arrow[r] \arrow[d, "\psi_1"] & U_{e/(p-1)} \arrow[r] \arrow[d, "\psi_2"] & U_{e/(p-1)}/U_{e/(p-1)+1} \arrow[r] \arrow[d, "\tau_{e/(p-1)}"] & 1 \\
1 \arrow[r] & U_{pe/(p-1)+1} \arrow[r] & U_{pe/(p-1)} \arrow[r] & U_{pe/(p-1)}/U_{pe/(p-1)+1} \arrow[r] & 1.
\end{tikzcd}$$

Note that ψ_1 is a bijection by what we have seen before, and that ψ_2 has kernel precisely equal to $\mu_p \cap F$. By the snake lemma, we get an isomorphism $\mu_p \cap F \to \ker(\tau_{e/(p-1)})$. The result follows.

(iv) From (iii) it follows that τ_i is not an isomorphism if and only if $\mu_p \subset F$ and $i = \frac{e}{p-1}$ with $p-1 \mid e$. □

Corollary 4.4. *Let $m \in \mathbf{Z}_{\geq 1}$. Write $m = p^{b_0}c$ with $b_0 \in \mathbf{Z}_{\geq 0}$ and $c \in \mathbf{Z}_{>0}$ such that $(c,p) = 1$. One has:*

i. *$U_1 \subseteq (F^*)^m$ if $b_0 = 0$.*
ii. *Assume $\mu_p \subset F$ and $b_0 > 0$. Then: $U_N \subseteq (F^*)^m$ if $N \geq \frac{e}{p-1} + b_0 \cdot e + 1$.*
iii. *Assume $\mu_p \not\subset F$ and $b_0 > 0$. Then: $U_N \subseteq (F^*)^m$ if $N \geq \frac{e}{p-1} + b_0 \cdot e$.*

Proof. (i) Since U_1 is a $\mathbf{Z}_p$-module and $c \in \mathbf{Z}_p^*$, one has $U_1 = U_1^c$.

(ii) If $N \geq \frac{e}{p-1} + b_0 \cdot e + 1$, then $N - l \cdot e > \frac{e}{p-1}$ if $l \leq b_0$ and so the p-th powerings $U_{N-b_0\cdot e} \longrightarrow U_{N-(b_0-1)\cdot e} \longrightarrow \ldots \longrightarrow U_N$ are isomorphisms. Therefore we have $U_N = U_{N-b_0\cdot e}^{p^{b_0}} \subset (F^*)^{p^{b_0}}$.

(iii) The proof is analogous to the proof of (ii), where we use the p-th powering map $U_{\frac{e}{p-1}}/U_{\frac{e}{p-1}+1} \longrightarrow U_{\frac{pe}{p-1}}/U_{\frac{pe}{p-1}+1}$ which is an isomorphism. The rest follows easily from Proposition 4.3 and its proof. □

Definition 4.5. Assume $\mu_p \subset F$. An element $\delta \in U_{pe/(p-1)}$ such that $\{\overline{\delta}\}$ is a basis for the cokernel of $\tau_{e/(p-1)}$ is called a *distinguished unit.* Equivalently, δ is a distinguished unit if $\overline{\delta} \in U_{pe/(p-1)}/U_{pe/(p-1)+1}$ satisfies

$$\overline{\delta} \notin \operatorname{im}\left(\tau_{e/(p-1)}\right)$$

(Proposition 4.3), which is equivalent to the definition given in the introduction.

Example 4.6. Let the field $F \supset \mathbf{Q}_2$ be given by the triple $(p,g,h) = (2, X^2 + X + 1, Y^2 - (2+2X)Y - 2X)$. Let us first compute $\overline{u_0}$. One has

$$\frac{\pi^2}{(1+\gamma)\pi + \gamma} = 2.$$

Hence $\overline{u_0} = -1/\overline{\gamma} = 1 + \overline{\gamma}$. The map $\tau_{e/(p-1)}$ is essentially given by $\mathbf{F}_4 \to \mathbf{F}_4$, $x \mapsto x^2 - (1+\overline{\gamma})x$. The image under this map is $\{0, \overline{\gamma}\}$. Hence, $\delta = 1 - \pi^4$ (or $1 + \pi^4$) is a distinguished unit.

2.2. Exponential representation and roots of unity. We will now discuss how to compute primitive p-th power roots of unity. We will introduce the so-called exponential representation for this purpose. With our application to the norm residue symbol in mind, we restrict ourselves to a special case (in the formulas below, we restrict to $\omega(b)$ for $b \in \mathcal{B}$, with $\mathcal{B} = \{\overline{1}, \overline{\gamma}, \ldots, \overline{\gamma}^{f-1}\}$, but other choices also work).

Let π' be a prime element of F. For i with $1 \leq i < pe/(p-1)$, $p \nmid i$ set

$$T_{\pi',i} = \{1 - \omega(b)\pi'^i : b \in \mathcal{B}\} \subseteq U_i.$$

One easily sees that $T_{\pi',i}$ is a basis of U_i/U_{i+1} over $\mathbf{F}_p$. Set

$$T_{\pi'} = \bigcup_{i:\ 1 \leq i < pe/(p-1),\ p \nmid i} T_{\pi',i}.$$

Assume, until the next lemma, that $\mu_p \subset F$ and let δ be a distinguished unit. Set

$$T_{\pi',\delta} = \{\delta\} \sqcup T_{\pi'}.$$

Recall that $r \in \mathbf{Z}_{\geq 0}$ is defined by $p^r \parallel e/(p-1)$. Note that $T^{p^{r+1}}_{\pi',e/(p^r(p-1))}$ in the quotient group $U_{pe/(p-1)}/U_{pe/(p-1)+1}$ is dependent over $\mathbf{F}_p$ and spans a subspace of codimension 1, by Proposition 4.3 and the discussion before this proposition. Furthermore, $T^{p^{r+1}}_{\pi',e/(p^r(p-1))} \cup \{\delta\}$ spans $U_{pe/(p-1)}/U_{pe/(p-1)+1}$ over $\mathbf{F}_p$. For $b \in \mathcal{B}$ set $w_b = 1 - \omega(b)\pi'^{e/(p^r(p-1))}$. Let $b' \in \mathcal{B}$ such that

$$S_{\pi',\delta,b'} = \left(T_{\pi',e/(p^r(p-1))} \setminus \{w_{b'}\}\right)^{p^{r+1}} \sqcup \{\delta\}$$

is a basis of $U_{pe/(p-1)}/U_{pe/(p-1)+1}$ over $\mathbf{F}_p$. We call (π', δ, b') a *distinguished triple.*

Lemma 4.7. *Let $t \in \mathbf{Z}_{\geq 1}$ and consider the $\mathbf{Z}_p$-module $M = \mathbf{Z}_p^t/b\mathbf{Z}_p$ for some $b \in \mathbf{Z}_p^t$, $b \neq 0$. Let s be maximal such that $b \in p^s \cdot \mathbf{Z}_p^t$. Then one has $M \cong \mathbf{Z}_p^{t-1} \oplus M_{\mathrm{tor}}$ as $\mathbf{Z}_p$-modules with $M_{\mathrm{tor}} = (b/p^s)\mathbf{Z}_p/b\mathbf{Z}_p \cong \mathbf{Z}/p^s\mathbf{Z}$.*

Proof. Left as an exercise. □

Proposition 4.8.

i. *Assume $\mu_p \not\subset F$. Let π' be a prime element. Then the map*

$$\begin{aligned} \varphi_{\pi'} : \mathbf{Z}_p^{T_{\pi'}} &\to U_1 \\ (a_t)_{t \in T_{\pi'}} &\mapsto \prod_{t \in T_{\pi'}} t^{a_t} \end{aligned}$$

is an isomorphism of $\mathbf{Z}_p$-modules.

ii. *Assume that $\mu_p \subset F$. Let π' be a prime element and let δ be a distinguished unit. Then the map*

$$\begin{aligned} \varphi_{\pi',\delta} : \mathbf{Z}_p^{T_{\pi',\delta}} &\to U_1 \\ (a_t)_{t \in T_{\pi',\delta}} &\mapsto \prod_{t \in T_{\pi',\delta}} t^{a_t} \end{aligned}$$

is surjective $\mathbf{Z}_p$-linear and the kernel is of the form $b\mathbf{Z}_p$ for some $b \in p\mathbf{Z}_p^{T_{\pi',\delta}}$. The largest integer s such that $\mu_{p^s} \subset F$ is equal to the largest integer s with $b \in p^s\mathbf{Z}_p^{T_{\pi',\delta}}$, and $\varphi_{\pi',\delta}(b/p^s)$ is a primitive p^s-th root of unity.

More specifically, let (π', δ, b) be a distinguished triple. Set

$$A_{b'} = \{(a_t)_{t\in T_{\pi',\delta}} \in \mathbf{Z}_p^{T_{\pi',\delta}},\ a_{w_{b'}} \in \mathbf{Z},\ 0 \le a_{w_{b'}} < p^{r+1}\}.$$

Then $\varphi_{\pi',\delta}|_{A_{b'}}$ is a bijection $A_{b'} \mapsto U_1$, say with inverse ψ, and one can take

$$b = \psi(w_{b'}^{p^{r+1}}) - p^{r+1}\psi(w_{b'}).$$

Proof. One easily sees that both maps are well-defined, because U_1 is a $\mathbf{Z}_p$-module. Recall for $j \in \mathbf{Z}_{\ge 1}$ we set $z(j) = (m, i)$ if $j = \rho^m(i)$.

i: For any $j \in \mathbf{Z}_{\ge 1}$ with $z(j) = (m, i)$ we define

$$T_{\pi',j} = T_{\pi',i}^{p^m}.$$

Note that $T_{\pi',j}$ is a basis of U_j/U_{j+1}, because the p-th powering maps are all isomorphisms. Hence one easily sees that any $x \in U_1$ can be written uniquely as $x = \prod_{i=1}^{\infty} \prod_{t\in T_{\pi',i}} t^{a_t}$ with $a_t \in \{0, 1, \ldots, p-1\}$. If one reorders this description, one gets a unique way of writing $x = \prod_{t\in T_{\pi'}} t^{a'_t}$ with $a'_t \in \mathbf{Z}_p$.

ii: Fix a distinguished triple (π', δ, b'). We define for $j \in \mathbf{Z}_{\ge 1}$

$$T_{\pi',\delta,b',j} = \begin{cases} S_{\pi',\delta,b'}^{p^m} & \text{if } j = pe/(p-1) + me \ (m \in \mathbf{Z}_{\ge 0}), \\ T_{\pi',i}^{p^m} & \text{else, where } z(j) = (m, i). \end{cases}$$

By construction, for $j \in \mathbf{Z}_{\ge 1}$, the set $T_{\pi',\delta,b',j}$ is a basis of U_j/U_{j+1} over $\mathbf{F}_p$. One can follow the same proof as for i, and after grouping one gets a unique way of writing $x \in U_1$ as $x = \prod_{t\in T_{\pi',\delta}} t^{a'_t}$ with $a'_t \in \mathbf{Z}_p$ and $0 \le a'_{w_{b'}} < p^{r+1}$. Furthermore, one can write $w_{b'}^{p^{r+1}} = w_{b'}^{c'_{w_{b'}}} \prod_{t\in T_{\pi',\delta},\ t\neq w_{b'}} t^{b'_t}$ such that $c'_{w_{b'}} \in \mathbf{Z}$ and $0 \le c'_{w_{b'}} < p^{r+1}$. Since our previous way of writing was unique, this gives the generating relation $b = (b'_t)_{T_{\pi',\delta}}$ with $b'_{w_{b'}} = c'_{w_{b'}} - p^{r+1}$. The result follows from Lemma 4.7. □

Definition 4.9. Let $x \in U_1$.

Assume first that $\mu_p \not\subset F$. Let π' be a prime element. The sequence $a = (a_t)_{t\in T_{\pi'}} \in \mathbf{Z}_p^{T_{\pi'}}$ such that

$$x = \prod_{t\in T_{\pi'}} t^{a_t} = \varphi_{\pi'}(a)$$

is called the *exponential representation* of x with respect to π'.

Assume $\mu_p \subset F$ and let (π', δ, b') be a distinguished triple. The sequence $a = (a_t)_{t\in T_{(\pi',\delta)}} \in \mathbf{Z}_p^{T_{(\pi',\delta)}}$ with $a_{w_{b'}} \in \{0, 1, \ldots, p^{r+1} - 1\}$ and

$$x = \prod_{t\in T_{\pi',\delta}} t^{a_t} = \varphi_{\pi',\delta}(a)$$

is called the *exponential respresentation* of x with respect to (π', δ, b').

Definition 4.10. For $x \in U_1$ and $N \in \mathbf{Z}_{\geq 1}$ we set

$$\mu(x, N) = \min\{i \in \mathbf{Z}_{\geq 0} : x^{p^i} \in U_N\}.$$

Assume that $\mu_p \not\subset F$. Let $(a_t)_{t \in T_{\pi'}}$ be the exponential representation of x with respect to π'. We define the *exponential representation* of $\overline{x} \in \mathcal{O}_N \cap \overline{U_1}$ with respect to $\overline{\pi'}$ to be

$$(a_t \bmod p^{\mu(t,N)})_{t \in T_{\pi'}}.$$

Assume that $\mu_p \subset F$. Let $(a_t)_{t \in T_{\pi',\delta}}$ be the exponential representation with respect to (π', δ, b'). We define the *exponential representation* of $\overline{x} \in \overline{U_1}$ where $\overline{U_1}$ is the image of U_1 in $\mathcal{O}_N = \mathcal{O}/\mathfrak{m}^N$, with respect to $(\overline{\pi'}, \overline{\delta}, b')$, to be

$$(a_t \bmod p^{\mu(t,N)})_{t \in T_{\pi',\delta}}.$$

One has $x = \prod_t \overline{t}^{a_t \bmod p^{\mu(t,N)}} \in \mathcal{O}_N$, and this is the unique representation of x with the given restrictions (together with the restriction on $a_{w_{b'}}$ in the second case). Furthermore, in the second case, if $N \leq pe/(p-1)$, the representation does not depend on δ and b'.

Definition 4.11. Let s be maximal such that $\mu_{p^s} \subset F^*$. Assume $s \geq 1$. Let π' be a prime element of F and let δ be a distinguished unit. Let $T = T_{\pi',\delta}$. Let $x \in F^*$. By Corollary 2.6 and Proposition 4.8ii one can write

$$x = (-\pi')^{v(x)} \omega(c) \prod_{t \in T} t^{a_t},$$

with $c \in k^*$, $a_t \in \mathbf{Z}_p$, and $(a_t)_{t \in T} \in \mathbf{Z}_p^T$ is unique modulo $b\mathbf{Z}_p$ (as in Proposition 4.8), and in particular modulo $p^s \cdot \mathbf{Z}_p^T$. We set

$$\chi(x; \pi', \delta) = (a_\delta \bmod p^s) \in \mathbf{Z}/p^s\mathbf{Z},$$

which is uniquely determined (Proposition 4.8). This gives us a group morphism

$$\chi(\cdot; \pi', \delta) : F^* \to \mathbf{Z}/p^s\mathbf{Z}.$$

In Lemma 5.6 of the next Chapter it will become clear that the morphism $\chi(\cdot; \pi', \delta)$ plays an important part in the computation of the norm residue symbol.

Remark 4.12. In the next section, we give algorithms to efficiently compute $\zeta_{p^s} \in U_1$. Computing ζ_{q-1} is much harder. For this one needs to work in the residue field k and compute a primitive root. No deterministic polynomial time algorithm is known for this.

3. Algorithms

In this section we discuss the complexity of the algorithms accompanying the theory discussed in the previous sections. The constant C, occurring in the runtime of our algorithms, is the linear algebra constant from Remark 3.11.

Algorithm 4.13 (μ_p detection).
Input: $\mathcal{O}_N$ with $N = e + 1$.
Output: True if $\mu_p \subset F$ and False otherwise.
Steps:

```
i. If $p - 1 \nmid e$ return False and terminate.
ii. Compute $\overline{u_0} \in k^*$.
iii. Compute the matrix of $A = [\cdot\overline{u_0}]_{\mathcal{B}} \in \mathrm{Mat}_f(\mathbf{F}_p)$.
iv. Compute $\det(A) \in \mathbf{F}_p$.
v. If $\det(A) = 1$ output True, and output False otherwise.
```

Proposition 4.14. *Algorithm 4.13 is correct and its complexity is* $O(e \log q + f(\log q)^{1[+1]} + f^C(\log p)^{1[+1]})$ *with* C *as in Remark 3.11.*

Proof. The correctness follows from Proposition 4.3. Step i takes time $O(\log e \cdot \log p)$. Step ii takes time $O(e \log q + (\log q)^{1[+1]})$ and step iii takes time $O(f(\log q)^{1[+1]})$ (Theorem 3.2). Step iv takes $O(f^C(\log p)^{1[+1]})$. This gives the required complexity. □

Algorithm 4.15 (Distinguished unit).
Input: $\mathcal{O}_N$ for $N \geq pe/(p-1) + 1$ such that $\mu_p \subset F$.
Output: $\overline{\delta} \in \mathcal{O}_N$, where δ is a distinguished unit.
Steps:

```
i. Compute $\overline{u_0} \in k^*$.
ii. Compute $A = [x \mapsto x^p - \overline{u_0}x]_{\mathcal{B}} \in \mathrm{Mat}_f(\mathbf{F}_p)$.
iii. Compute $c \in k$ which generates the cokernel of $A$ over $\mathbf{F}_p$.
iv. Compute $r_0 = \overline{1 + (c/\overline{-u_0}^j)\pi_{pe/(p-1)}} \in \mathcal{O}_{pe/(p-1)+1}$ where $j = 1$ if $p \neq 2$
    and $j = 2$ when $p = 2$.
v. Return a lift $\overline{\delta}$ of $r_0$ to $\mathcal{O}_N$.
```

Proposition 4.16. *Algorithm 4.15 is correct and its complexity is* $O((f + \log p)(\log q)^{1[+1]} + f^C(\log p)^{1[+1]} + N \log q)$.

Proof. The correctness follows from Proposition 4.8 and the discussion before this proposition. For step iv, note that if $p > 2$, one has

$$\pi^{pe/(p-1)} = \pi^e \pi^{e/(p-1)} = (-p/u_0)\pi^{e/(p-1)} = (-1/u_0)\pi_{pe/(p-1)}.$$

Similarly, if $p = 2$, one finds $\pi^{pe/(p-1)} = p^2/(u_0)^2 = \pi_{pe/(p-1)}/u_0^2$. This gives us

$$\overline{\delta} = \overline{1 + c \cdot \pi^{pe/(p-1)}} = \overline{1 + (c/\overline{-u_0}^j)\pi_{pe/(p-1)}} \in \mathcal{O}_{pe/(p-1)+1}$$

where $j = 1$ if $p \neq 2$ and $j = 2$ when $p = 2$. Moreover $\overline{\delta}$ is a distinguished unit and is computed by the algorithm mod $\pi^{pe/(p-1)+1}$.

Step i costs $O(N \log q + (\log q)^{1[+1]})$ (Theorem 3.2 by computing $\overline{u_0}$ for $N - e = 1$). Step ii costs $O((f + \log p)(\log q)^{1[+1]})$ (Theorem 3.2). The third step costs $O(f^C(\log p)^{1[+1]})$ by Remark 3.11. Step iv costs $O(N \log q + (\log q)^{1[+1]})$ by Theorem 3.2. Step v costs $O(N \log q)$ by Theorem 3.2. □

Algorithm 4.17 (Distinguished triple).
Input: $\mathcal{O}_N$ for $N \geq pe/(p-1) + 1$ such that $\mu_p \subset F$ and $\overline{\pi'} \in \mathcal{O}_N$ where π' is a prime

element.
Output: $b' \in \mathcal{B}$ and $\overline{\delta} \in \mathcal{O}_N$ such that (π', δ, b') is a distinguished triple as defined in section 2.2 of the present chapter.
Steps:

```
i. Compute $\overline{\delta} \in \mathcal{O}_N$ (Algorithm 4.15).
ii. Compute $\overline{u_0} \in k^*$.
iii. Compute $A = [x \mapsto x^p - \overline{u_0}x]_{\mathcal{B}} \in \mathrm{Mat}_f(\mathbf{F}_p)$.
iv. Compute $B = [x \mapsto x^p]_{\mathcal{B}} \in \mathrm{Mat}_f(\mathbf{F}_p)$
v. Compute $D = AB^{r \bmod f}$.
vi. Compute the kernel of $D$, and $b' \in \mathcal{B}$ occurring with a non-zero coefficient
    in a generator of the kernel of $D$ and return $b'$ and $\overline{\delta}$.
```

Proposition 4.18. *Algorithm 4.17 is correct and its complexity is* $O(N \log q + (f + \log p)(\log q)^{1[+1]} + f^C(\log p)^{1[+1]})$.

Proof. The correctness follows from the discussion before Proposition 4.8 and the fact that B has order f.

Step i costs $O((f + \log p)(\log q)^{1[+1]} + f^C(\log p)^{1[+1]} + N \log q)$. Step ii costs $O(N \log q + \log q^{1[+1]})$ (Theorem 3.2). The total cost of the steps iii and iv is $O((f + \log p)(\log q)^{1[+1]})$ according to Theorem 3.2. Step v requires the computation of the integer r and of $r \bmod f$ and this can be done in time $O(e\cdot(\log p + \log f)) < O(N \log q)$. The computation of D costs $O(f^C \cdot (\log p)^{1[+1]})$. Step vi costs $O(f^C(\log p)^{1[+1]})$ by 3.11. □

Remark 4.19. Optionally, one can as input have $\overline{\delta} \in \mathcal{O}_N$ and skip the first step of Algorithm 4.17. The complexity remains the same.

We will now discuss algorithms to compute the exponential representation. One can come up with algorithms with various complexities, and we have chosen ones which work well if q is large. Furthermore, to simplify the descriptions, we assume that $N > pe/(p-1)$. The algorithms below can easily be adjusted to work for all N.

Algorithm 4.20 (Exponential representation 1).
Input: $\mathcal{O}_N$ with $N > pe/(p-1)$ such that $\mu_p \not\subset F$ and $x \in \mathcal{O}_N \cap \overline{U_1}$, $\overline{\pi'} \in \mathcal{O}_N$ where π' is a prime element.
Output: the exponential representation of x with respect to $\overline{\pi'}$.
Steps:

```
i. Compute $\pi'^i \in \mathcal{O}_N$ for $i = 1, 2, \ldots, N-1$.
ii. Compute $t_{i,b} = \overline{1 - \omega(b)\pi'^i} \in \mathcal{O}_N$ for $1 \leq i < pe/(p-1)$, $p \nmid i$ and $b \in \mathcal{B}$ and
    set $a_{i,b} = 0 \in \mathbf{Z}$.
iii. For $1 \leq j < N$ and $b \in \mathcal{B}$ compute $t_{j,b} = t_{i,b}^{p^m} \in \mathcal{O}_N$ where $z(j) = (m, i)$ .
iv. Set $x_1 = x$.
v. For $j = 1, \ldots, N-1$ do:
    • Write $z(j) = (m, i)$.
    • Compute $c \in k$ such that $\overline{x_j} = \overline{1 + \omega(c)\pi'^j} \in \mathcal{O}_{j+1}$.
    • Compute $c_b \in k$ for $b \in \mathcal{B}$ such that $\overline{t_{j,b}} = \overline{1 + \omega(c_b)\pi'^j} \in \mathcal{O}_{j+1}$.
    • Write $c = \sum_{b \in \mathcal{B}} d_b c_b$ with $0 \leq d_b < p$.
```

```
        • Replace $a_{i,b}$ by $a_{i,b} + p^m d_b$ for $b \in \mathcal{B}$.
        • Set $x'_j = \prod_{b\in\mathcal{B}} t_{j,b}^{d_b}$.
        • Set $x_{j+1} = x_j/x'_j \in \mathcal{O}_N \cap \overline{U_{j+1}}$.
  vi. Return all $a_{i,b}$ (the weight corresponding to $t_{i,b}$).
```

Algorithm 4.21 (Exponential representation 2).
Input: $\mathcal{O}_N$ with $N > pe/(p-1)$ such that $\mu_p \subset F$ and $x \in \mathcal{O}_N \cap \overline{U_1}$, $\overline{\pi'}, \overline{\delta} \in \mathcal{O}_N$ and $b' \in \mathcal{B}$ such that (π, δ, b') is a distinguished triple.
Output: the exponential representation of x with respect to $(\overline{\pi'}, \overline{\delta}, b')$.
Steps:

```
  i. Compute $\pi'^i \in \mathcal{O}_N$ for $i = 1, 2, \ldots, N-1$.
  ii. Compute $t_{i,b} = \overline{1 - \omega(b)\pi'^i} \in \mathcal{O}_N$ for $1 \le i < pe/(p-1)$, $p \nmid i$ and $b \in \mathcal{B}$ and
      set $a_{i,b} = 0 \in \mathbf{Z}$.
  iii. For $1 \le j < N$ and $b \in \mathcal{B}$ with $z(j) = (m, i)$ compute $t_{j,b} = t_{i,b}^{p^m} \in \mathcal{O}_N$.
  iv. Compute $\overline{\delta}^{p^i} \in \mathcal{O}_N$ for $i = 1, \ldots, \lfloor N/e \rfloor$ and set $a_\delta = 0$.
  v. Set $x_1 = x$.
  vi. For $j = 1, \ldots, N-1$ do:
        • Write $z(j) = (m, i)$.
        • Compute $c \in k$ such that $\overline{x_j} = \overline{1 + \omega(c)\pi'^j} \in \mathcal{O}_{j+1}$.
        • Compute $c_b \in k$ for $b \in \mathcal{B}$ such that $\overline{t_{j,b}} = \overline{1 + \omega(c_b)\pi'^j} \in \mathcal{O}_{j+1}$.
        • If $j = pe/(p-1) + el$ for some $l \ge 0$:
            – Compute $c' \in k$ such that $\overline{\delta}^{p^l} = \overline{1 + \omega(c')\pi'^j} \in \mathcal{O}_{j+1}$.
            – Write $c = d'c' + \sum_{b\in\mathcal{B}, b\ne b'} d_b c_b$ with $0 \le d_b, d' < p$.
            – Replace $a_{i,b}$ by $a_{i,b} + p^m d_b$ for $b \in \mathcal{B}, b \ne b'$ and replace $a_\delta$ by
              $a_\delta + p^l d'$.
            – Set $x'_j = \left(\overline{\delta}^{p^l}\right)^{d'} \cdot \prod_{b\in\mathcal{B}, b\ne b'} t_{j,b}^{d_b}$
          Else:
            – Write $c = \sum_{b\in\mathcal{B}} d_b c_b$ with $0 \le d_b < p$.
            – Replace $a_{i,b}$ by $a_{i,b} + p^m d_b$ for $b \in \mathcal{B}$.
            – Set $x'_j = \prod_{b\in\mathcal{B}} t_{j,b}^{d_b}$.
        • Set $x_{j+1} = x_j/x'_j \in \mathcal{O}_N \cap \overline{U_{j+1}}$.
  vii. Return all $a_{i,b}$ (the weight corresponding to $t_{i,b}$) and $a_\delta$ (the weight corre-
       sponding to $\overline{\delta}$).
```

Proposition 4.22. *Algorithm 4.20 and Algorithm 4.21 are correct and both their complexities are* $O((N \log q)^{2[+1]} + N f^C (\log p)^{1[+1]})$.

Proof. Let us discuss the complexity of Algorithm 4.20. The analysis of Algorithm 4.21 is similar. The correctness follows from Proposition 4.8.

Step i: Requires $O(N \cdot (N \log q)^{1[+1]})$ (Theorem 3.2).

Step ii: Requires at most $O(ef)$ multiplications and additions in $\mathcal{O}_N$ in time $O(ef \cdot (N \log q)^{1[+1]})$ by Theorem 3.2. Furthermore, it requires us to compute $\overline{\omega(\gamma)} \in \mathcal{O}_N$ in time $O((N + (N/e \log q)^{1[+1]}) \log q)$ by Theorem 3.2.

Step iii: Requires at most $fN \log p$ multiplications in $\mathcal{O}_N$ in time $O(fN \log p \cdot (N \log q)^{1[+1]})$ by Theorem 3.2.

Step iv: No added complexity.

Step v: This step requires analysis, and is done N times. Part 1 is easy. Part 2 costs $O(N \log q + (\log q)^{1[+1]})$ (Theorem 3.2). Part 3 costs $O(fN \log q + f(\log q)^{1[+1]})$ (Theorem 3.2). Part 4 is linear algebra over $\mathbf{F}_p$ and takes time $O(f^C (\log p)^{1[+1]})$. Part 5 has a small complexity. Part 6 requires $O(f \log p)$ multplications in time $O(f \log p \cdot (N \log q)^{1[+1]}$ (Theorem 3.2). Step 7 requires $O((N \log q)^{1[+1]})$ (Theorem 3.2).

Step vi: No added complexity.

□

Algorithm 4.23 (p^s-th primitive root of unity).
Input: $\mathcal{O}_N$ with $N > e$, and $N \geq pe/(p-1) + 1 + er$ if $p - 1 \mid e$.
Output: largest $s \in \mathbf{Z}_{\geq 0}$ such that $\mu_{p^s} \subset F$, and $\overline{\zeta_{p^s}} \in \mathcal{O}_{N-es}$ where ζ_{p^s} is a primitive p^s-th root of unity.
Steps:

```
i.   Check if $\mu_p \subset F$ (Algorithm 4.13). If no, output $s = 0$ and $\overline{\zeta_1} = \overline{1} \in \mathcal{O}_N$ and terminate.
ii.  Compute $\overline{\pi}, \overline{\delta} \in \mathcal{O}_N$ and $b' \in \mathcal{B}$ such that $(\pi, \delta, b')$ is a distinguished triple (Algorithm 4.17).
iii. Compute the exponential representation $(a_t)_{t \in T_{\pi', \delta, b'}}$ of $\overline{w_{b'}}^{p^{r+1}}$ with respect to $(\overline{\pi'}, \overline{\delta}, b')$ (Algorithm 4.21).
iv.  Let $s$ be maximal such that $p^s | a_t$ for all $t$.
v.   Compute $\overline{\zeta_{p^s}} = \frac{\prod_{t \in T_{\pi', \delta, b'}} \overline{t}^{a_t/p^s}}{\overline{w_{b'}}^{p^{r+1}/p^s}} \in \mathcal{O}_{N-es}$.
vi.  Return $s$ and $\overline{\zeta_{p^s}} \in \mathcal{O}_{N-es}$.
```

A slight variation gives us smaller order roots of unity.

Algorithm 4.24 (p^n-th primitive root of unity).
Input: $m = p^n > 1$, $\mathcal{O}_N$ with $N \geq e/(p-1) + ne + 1$.
Output: If $\mu_{p^n} \subset F$ output YES and $\overline{\zeta_{p^n}} \in \mathcal{O}_{N-en}$. Otherwise, output NO.
Steps:

```
i.   If $n > r + 1$, output NO and terminate.
ii.  Check if $\mu_p \subset F$ (Algorithm 4.13). If no, output NO and terminate.
iii. Compute $\overline{\pi}, \overline{\delta} \in \mathcal{O}_N$ and $b' \in \mathcal{B}$ such that $(\pi, \delta, b')$ is a distinguished triple (Algorithm 4.17).
iv.  Compute the exponential representation $(a_t)_{t \in T_{\pi', \delta, w}}$ of $\overline{w_{b'}}^{p^{r+1}}$ with respect to $(\overline{\pi'}, \overline{\delta}, b')$ (Algorithm 4.21).
v.   If not $a_t \equiv 0 \pmod{p^n}$ for all $t$, output NO and terminate.
vi.  Compute $\overline{\zeta_{p^n}} = \frac{\prod_{\in T_{\pi', \delta, b'}} \overline{t}^{a_t/p^n}}{\overline{w_{b'}}^{p^{r+1}/p^n}} \in \mathcal{O}_{N-en}$.
vii. Return YES and $\overline{\zeta_{p^n}} \in \mathcal{O}_{N-en}$.
```

Proposition 4.25. *Algorithm 4.23 and Algorithm 4.24 are correct and their complexity is* $O((N \log q)^{2[+1]} + N f^C (\log p)^{1[+1]})$.

Proof. We will only discuss Algorithm 4.23, the other algorithm is similar.

Note that we know $s \leq r+1$, by looking at the ramification. The correctness follows from Proposition 4.8. Let us briefly discuss why the input needs to be in such high precision, and why we lose precision in the output. We need to compute the exponential representation of $w_{b'}^{p^{r+1}}$, all coefficients modulo p^{r+1}. The 'hardest' coefficient is the one for δ, which requires us to work in $U_{pe/(p-1)+re}$, i.e., to work in $\mathcal{O}_N$ with $N \geq pe/(p-1)+1+er$. Note also that after dividing by p^s, we get the exponential representation of ζ in $\mathcal{O}_{N-es}$ (note that $\mathcal{O}_N$ also does not have more information about the precise value of ζ_{p^s}).

Let us discuss the complexity of the various steps.

Step i: Algorithm 4.13 takes $O(e \log q + f^C(\log p)^{1[+1]} + f(\log q)^{1[+1]} + N \log q)$, where the last term relates to getting $\mathcal{O}_{e+1}$ from $\mathcal{O}_N$.

Step ii: Algorithm 4.17 has complexity
$O(N\log q + (f+\log p)(\log q)^{1[+1]} + f^C(\log p)^{1[+1]})$.

Step iii: Algorithm 4.21 has complexity $O((N\log q)^{2[+1]} + Nf^C(\log p)^{1[+1]})$.

Step iv: Smaller complexity than step iii.

Step v: Has a small complexity dominated by $O((N\log q)^{2[+1]})$.

Hence step ii and iii dominates the complexity and the result follows.

□

Theorem 4.26. *There is a polynomial-time algorithm that, given a prime number p, a positive integer N given in unary, a finite extension F of $\mathbf{Q}_p$ in precision N and a positive integer n, with $N \geq \frac{e}{p-1} + ne + 1$, decides whether F contains a primitive p^n-th root of unity and if so, computes such a root of unity in precision $N - e\cdot n \in \mathbf{Z}_{>0}$.*

Proof. We have Algorithm 4.24 and Proposition 4.25 with its proof and we are done.

□

Example 4.27. We give an example of the computation of primitive roots of unity. Let $F \supset \mathbf{Q}_2$ be given by the triple $(p,g,h) = (2, X^2+X+1, Y^2-(2+2X)Y-2X)$. We have $e=2, f=2$ and $q=4$. The element γ is a zero of g and the prime element π is a zero of $h(\gamma, Y)$. The group U_1 is generated as a $\mathbf{Z}_2$-module by the elements of $\{\delta, 1-\pi, 1-\gamma\pi, 1-\pi^3, 1-\gamma\pi^3\}$ with $\delta = 1+\pi^4$ a distinguished unit (see Example 4.6). We have $F^* = \pi^{\mathbf{Z}} \cdot \mu_3 \cdot U_1$ with $\mu_3 = \{1, \gamma, \gamma^2\}$, the group of roots of unity of order $p^f - 1 = 3$ and $\omega(\gamma^j) = \gamma^j$ for all $j \in \{0,1,2\}$. Let 2^k with $k \in \mathbf{Z}_{>0}$ be the maximum 2-power order of roots of unity contained in F, then $k \leq 1 + \mathrm{ord}_p e = 2$. We choose the precision $N = e/(p-1) + 2e + 1 = 7$ and apply Algorithm 4.23. With Algorithm 4.17 we compute $b' = \gamma$, so $w_{b'} = 1 - \gamma\cdot\pi$, and (π, δ, γ) is a distinguished triple. Next we compute the exponential representation of $\overline{w_{b'}}^4$ with respect to $(\overline{\pi}, \overline{\delta}, \gamma)$ and find $(1-\gamma\cdot\pi)^4 \equiv (1-\pi)^8 \bmod \pi^7$. It follows that $(1-\gamma\cdot\pi)^{-4}\cdot(1-\pi)^8 \equiv 1 \bmod \pi^7$. We have $a_{1,1} = 8$ and $a_{1,\gamma} = a_\delta = 0$. So F contains a primitive fourth root of unity and $\zeta_4 \equiv (1-\gamma\cdot\pi)^{-1}\cdot(1-\pi)^2 \bmod \pi^3$ or $\zeta_4 \equiv 1 + \gamma\cdot\pi + \gamma\cdot\pi^2 \bmod \pi^3$. Note that the result is given in precision $N = 7 - 2\cdot 2 = 3$.

Chapter 5

Norm residue symbols

1. Introduction

Let F be a finite extension of $\mathbf{Q}_p$. In this chapter, we will first discuss properties of the norm residue symbol. After that, we will use the exponential representation to compute a symbol which is isomorphic to the norm residue symbol. Then we will discuss how one can compute the exact value of the norm residue symbol.

2. Properties

In this chapter we follow the notation as introduced in Chapter 2. The integers e and f denote respectively the ramification index and the residue class degree of a finite field extension F of $\mathbf{Q}_p$ where p is a prime number. The element $\pi \in F$ is a prime element and γ is defined as in Chapter 2. By $\omega(c)$ we denote the Teichmüller representative of $c \in \mathcal{C}$. Let F^{ab} denote the maximal abelian extension of F inside an algebraic closure of F. The map ϕ_F denotes the homomorphism $\phi_F : F^* \longrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F)$ which is called the *reciprocity map*, coming from class field theory. Let m be a positive integer and suppose that F contains the m-th roots of unity. For $\alpha, \beta \in F^*$ the m-th norm residue symbol $(\alpha, \beta)_m$ is the m-th root of unity defined by

$$(\alpha, \beta)_m = \frac{\phi_F(\alpha)(\sqrt[m]{\beta})}{\sqrt[m]{\beta}}.$$

The integer m will be called the *order* of the norm residue symbol. We state a number of properties of the m-th norm residue symbol.

Proposition 5.1. *Let m be a positive integer and let F be as above. Then for all α, α_1, α_2 and $\beta \in F^*$ we have:*

i. $(\alpha_1\alpha_2, \beta)_m = (\alpha_1, \beta)_m \cdot (\alpha_2, \beta)_m$.
ii. $(\alpha, \beta)_m = (\beta, \alpha)_m^{-1}$.
iii. $(\alpha, 1-\alpha)_m = 1$ *if* $\alpha \neq 1$.
iv. $(\alpha, -\alpha)_m = 1$.
v. $(\alpha, \gamma)_m = 1$ *for every* $\gamma \in F^* \Leftrightarrow \alpha \in (F^*)^m$.
vi. $(\alpha, \beta)_m = 1 \Leftrightarrow \alpha \in N_{E/F}(E^*)$ *with* $E = F(\sqrt[m]{\beta})$.
vii. $F(\sqrt[m]{\beta})/F$ *is unramified if and only if* $(\alpha', \beta)_m = 1$ *for all* $\alpha' \in \mathcal{O}_F^*$.
viii. *Let* $m = d_1 \cdot d_2$ *with* $d_1, d_2 \in \mathbf{Z}_{\geq 1}$*, then* $(\alpha, \beta)_m^{d_1} = (\alpha, \beta)_{d_2}$.
ix. *Let* $m = m_1 \cdot m_2$ *with* m_1 *and* m_2 *relatively prime positive integers,* $x = m_2^{-1} \bmod m_1$ *and* $y = m_1^{-1} \bmod m_2$ *then*

$$(\alpha, \beta)_m = (\alpha, \beta)_{m_1}^x \cdot (\alpha, \beta)_{m_2}^y.$$

x. *Let $m = p$ and let δ be a distinguished unit, then $(u, \delta)_p = 1$ for every $u \in \mathcal{O}_F^*$.*

Proof. For a proof of the first six items of Proposition 5.1 we refer to [**17**, Ch. 3, section 5]. We will prove the last four items.

vii: If E/F is a finite, abelian extension, then E/F is unramified if and only if $N_{E/F}(\mathcal{O}_E^*) = \mathcal{O}_F^*$. See [**13**, Chapter 11, section 4]. The result follows from part vi.

viii: We have $(\alpha, \beta)_m^{d_1} = (\alpha, \beta^{d_1})_m = \frac{\phi_F(\alpha)((\sqrt[m]{\beta})^{d_1})}{(\sqrt[m]{\beta})^{d_1}} = \frac{\phi_F(\alpha)(\sqrt[d_2]{\beta})}{\sqrt[d_2]{\beta}} = (\alpha, \beta)_{d_2}$.

ix: Because m_1 and m_2 are relatively prime, there are positive rational integers x and y with $xm_2 + ym_1 = 1$. So $xm_2 \equiv 1 \pmod{m_1}$ and $x = m_2^{-1} \pmod{m_1}$ and in the same way $y = m_1^{-1} \pmod{m_2}$. By (7) we have $(\alpha, \beta)_m = (\alpha, \beta)_m^{xm_2 + ym_1} = (\alpha, \beta)_m^{xm_2} \cdot (\alpha, \beta)_m^{ym_1} = (\alpha, \beta)_{m_1}^x \cdot (\alpha, \beta)_{m_2}^y$ and we are done.

x: The equation $\delta x^p + uy^p = 1$ has a solution $(x, y) \in (\mathcal{O}_F \setminus \{0\})^2$. For a proof of this fact we refer to [**15**, Appendix, proof of Lemma A.11]. Applying Proposition 5.1i, ii and iii gives $(u, \delta)_p = (x, u)_p^p \cdot (\delta, y)_p^p \cdot (x, y)_p^{p^2} = 1$. □

Remark 5.2. Proposition 5.1vi implies that for $\alpha_1, \alpha_2, \beta \in F^*$, one has $(\alpha_1, \beta)_m = (\alpha_2, \beta)_m$ if and only if the "residue classes" of α_1 and α_2 modulo the norm group $N_{E/F}(E^*)$, where $E = F(\sqrt[m]{\beta})$, coincide. This explains the term "norm residue symbol".

As an application of Proposition 5.1viii we can write an m-th norm residue symbol, with $m = m_0 \cdot p^n$ and $p \nmid m_0$, as a product of a norm residue symbol of order m_0 and one of order p^n. If the prime number p does not divide m, the m-th norm residue symbol is called *tame*. In the tame case we have the formula of the next proposition to compute the norm residue symbol. We remark that $m \mid q - 1$ because we assume that $\zeta_m \in F$ and $p \nmid m$.

Since the left and right kernel of $(\ ,\ )_m$ are $(F^*)^m$ by Proposition 5.1v, it is natural to view $(\ ,\ )_m$ as a symbol

$$(\ ,\ )_m : F^*/(F^*)^m \times F^*/(F^*)^m \to \mu_m.$$

The group $F^*/(F^*)^m$ is finite. Algorithmically, it is hard to work with $F^*/(F^*)^m$, and instead we choose to work with a group surjecting to $F^*/(F^*)^m$.

Let $m \in \mathbf{Z}_{\geq 1}$. Write $m = p^t b$ with $(b, p) = 1$. Note that the map

$$\begin{aligned} \mathbf{Z}/m\mathbf{Z} \times U/U^m &\to F^*/(F^*)^m \\ (\overline{a}, \overline{b}) &\mapsto \pi^a b (F^*)^m \end{aligned}$$

is an isomorphism. Let $N \in \mathbf{Z}_{\geq 1}$ with $N \geq e/(p-1) + te + 1$ if $t \geq 1$ and $N \geq 1$ otherwise. One has $U_N \subset U^m \subset (F^*)^m$ by Corollary 4.4. Note that we have an exact sequence $0 \to U_N \to U \to \mathcal{O}_N^* \to 0$. Hence we have a surjective map $\mathcal{O}_N^* \to U/U_N \to U/U^m$. We obtain a surjective map

$$\begin{aligned} (F^*/(F^*)^m)_N := \mathbf{Z}/m\mathbf{Z} \times \mathcal{O}_N^* &\to F^*/(F^*)^m \\ (\overline{a}, \overline{u}) &\mapsto \pi^a u (F^*)^m. \end{aligned}$$

Hence we represent elements of $F^*/(F^*)^m$ in a non-unique way by finite sets $\mathbf{Z}/m\mathbf{Z} \times \mathcal{O}_N^* \subset \mathbf{Z}/m\mathbf{Z} \times \mathcal{O}_N$ where N is large enough.

3. Computing the tame norm residue symbol

In this section, we will explain how to compute the tame norm residue symbol. The computation of this symbol turns out to be quite simple.

PROPOSITION 5.3. *Let $m \in \mathbf{Z}_{\geq 1}$ and let F be a finite extension of $\mathbf{Q}_p(\zeta_m)$ such that $p \nmid m$. Let further $\alpha, \beta \neq 0$ be elements of the field F, and put $\mathrm{ord}_F \alpha = a$ and $\mathrm{ord}_F \beta = b$. Let q denote the number of elements of the residue class field of F. Then we have $q \equiv 1 \bmod m$ and*

$$(\alpha, \beta)_m = \omega\left((-1)^{a \cdot b} \cdot \frac{\beta^a}{\alpha^b}\right)^{\frac{q-1}{m}}.$$

PROOF. See [**17**, Ch. 3, section 5]. □

ALGORITHM 5.4.
Input: $\mathcal{O}_N$, an integer $m \in \mathbf{Z}_{\geq 1}$, and $\alpha = (a, u), \beta = (b, v) \in (F^*/(F^*)^m)_N$ such that $m \mid (q-1)$.
Output: $\overline{(\alpha, \beta)_m} \in \mathcal{O}_N$.
Steps:

```
i. Compute $g = ab \cdot \frac{q-1}{m} \bmod (q-1)$, $h = a \cdot \frac{q-1}{m} \bmod (q-1)$, $k = b \cdot \frac{q-1}{m} \bmod (q-1)$.
ii. Compute $c = (-1)^g \cdot \frac{v^h}{u^k} \bmod \mathfrak{m}$.
iii. Compute $x = \omega(c) \bmod \mathfrak{m}^N$.
iv. Return $x$.
```

PROPOSITION 5.5. *Algorithm 5.4 computes correctly the tame norm residue symbol in time $O(\big(N + (((N/e) + 1) \log q)^{1[+1]}\big) \cdot \log q)$.*

PROOF. The first and second step each take $O(\log q \cdot (\log q)^{1[+1]})$ (Theorem 3.2). The Teichmüller lift takes time $O(\big(N + ((N/e) \log q)^{1[+1]}\big) \cdot \log q)$ (Theorem 3.2). □

4. Computing the wild norm residue symbol

Assume $m = p^n$ with $n \geq 1$ and $\mu_{p^n} \subset F^*$. We will now compute $(\ ,\ )_m$. Let s be maximal such that $\mu_{p^s} \subset F^*$.

The next lemma shows the relation between the exponential representation and the norm residue symbol. Recall the definition of $\chi(x; \pi', \delta)$ in Definition 4.11 in Chapter 4.

LEMMA 5.6. *Let π' be a prime element of F and let (π', δ, b') be a distinguished triple. Then $(\pi', \delta)_m$ is a primitive m-th root of unity and for $x \in F^*$ one has*

$$(\pi', x)_m = (\pi', \delta)_m^{\chi(x; \pi', \delta)}.$$

PROOF. Note that for $c \in k^*$, $z \in F^*$ we have

$$(\omega(c), z)_{p^s} = 1$$

since $\omega(c) \in (F^*)^m$ (Proposition 5.1). This gives for $i \in \mathbf{Z}$ (Proposition 5.1)

$$1 = (\omega(c)\pi'^i, 1 - \omega(c)\pi'^i)_m = (\pi', 1 - \omega(c)\pi'^i)_m^i.$$

Hence if $(i,p)=1$, we find

$$1=(\pi',1-\omega(c)\pi'^i)_m,$$

so $(\pi',t)_m=1$ for all $t\in T_{\pi'}$. Write

$$x=\omega(c)(-\pi')^{v(x)}\delta^d\prod_{t\in T_{\pi',\delta},\ t\neq\delta}t^{a_t}$$

with $c\in k^*$, $a_t\in\mathbf{Z}_p$, $d\in\mathbf{Z}_p$, so that $d\equiv\chi(x;\pi',\delta)\pmod m$. One finds using Proposition 5.1

$$(\pi',x)_m=(\pi',\omega(c))_m(\pi',-\pi')_m^{v(x)}(\pi',\delta)_m^d\prod_{t\in T_{\pi',\delta},\ t\neq\delta}(\pi',t)_m^{a_t}=(\pi',\delta)_m^d.$$

We conclude that $(\pi',F^*)_{p^s}=(\pi',\delta)_{p^s}^{\mathbf{Z}}$. Since π' is not a p-th power, it follows that $(\pi',F^*)_{p^s}=\mu_{p^s}$ by Proposition 5.1. Hence $(\pi',\delta)_{p^s}$ is a primitive p^s-th root of unity and by Proposition 5.1viii it follows that $(\pi',\delta)_m$ has order $m=p^n$. □

Lemma 5.7. *Let $x,y\in F^*$. Write $x=\omega(a)\pi^{v(x)}w'$ with $w'\in U_1$ and $a\in k^*$. Set $\pi'=w'\pi$. Let $\delta\in F^*$ be a distinguished unit. Then one has*

$$(x,y)_m=(\pi,\delta)_m^{(v(x)-1)\chi(y;\pi,\delta)}\cdot(\pi',\delta)_m^{\chi(y;\pi',\delta)}.$$

Proof. One has by Lemma 5.6

$$\begin{aligned}(x,y)_m&=(\omega(a)\pi^{v(x)}w',y)_m=(\omega(a),y)_m(\pi,y)_m^{v(x)-1}(\pi',y)_m\\&=(\pi,\delta)_m^{(v(x)-1)\chi(y;\pi,\delta)}\cdot(\pi',\delta)_m^{\chi(y;\pi',\delta)}.\end{aligned}$$

□

If $m=p$, then the formula in Lemma 5.7 simplifies considerably, because from 5.1x it follows immediately that $(\pi',\delta)_p=(\pi,\delta)_p$. For the general case $m=p^n$, we like to write $(\pi',\delta)_m$ as a power of $(\pi,\delta)_m$. We shall see that this is easy to do if $(\pi',\pi)_p\neq 1$. In the case $(\pi',\pi)_p=1$, we shall pass from π to π' by using the intermediate prime element $\pi''=-\delta\pi'$, which turns out to satisfy $(\pi',\pi'')_p\neq 1$ and $(\pi'',\pi)_p\neq 1$, unless $m=p=2$.

Let us now introduce some notation which makes our computations nicer.

Definition 5.8. Let M be a free R-module of rank 1 over a commutative ring R with basis $\{b\}$. We assume that the group operation on M is written multiplicatively. Furthermore, write the action of R on M exponentially, that is, the action of $r\in R$ on $m\in M$ is denoted as ${}^r m$. For $a\in M$ we define $a\!\downarrow\! b\in R$ by

$$a={}^{a\downarrow b}b.$$

One may think of $a\!\downarrow\! b$ as the logarithm of a to the base b.

Remark 5.9.

$$\begin{aligned}aa'\!\downarrow\! b&=a\!\downarrow\! b+a'\!\downarrow\! b\\({}^r a)\!\downarrow\! b&=r(a\!\downarrow\! b).\end{aligned}$$

Hence one has $1 \downarrow b = 0$ and $a^{-1} \downarrow b = -a \downarrow b$. One obviously has $b \downarrow b = 1$. Finally, if $\{b'\}$ is also a basis for M, then one has

$$a \downarrow b = a \downarrow b' \cdot b' \downarrow b.$$

We will apply the definition above to $R = \mathbf{Z}/m\mathbf{Z}$ and $M = \mu_m$, which is a free $\mathbf{Z}/m\mathbf{Z}$-module of rank one. For the basis element b we shall always take an element of the form $(\pi', \delta)_m$, with π' a prime element and δ a distinguished unit, which can be done by Lemma 5.6. By the same lemma, we can express the function χ in arrow notation as

$$\chi(x; \pi', \delta) = (\pi', x)_m \downarrow (\pi', \delta)_m.$$

with x, π', δ as in Lemma 5.6.

Proposition 5.10. *Let π' be a prime element and set $\pi'' = -\delta\pi'$. Then one has*

$$(\pi', \delta)_m \downarrow (\pi, \delta)_m = \begin{cases} 1 & \textit{if } m = 2 \\ -\dfrac{\chi(\pi'; \pi, \delta)}{\chi(\pi; \pi', \delta)} & \textit{if } \chi(\pi; \pi', \delta) \in (\mathbf{Z}/m\mathbf{Z})^* \\ \dfrac{\chi(\pi''; \pi, \delta) \cdot \chi(\pi'; \pi'', \delta)}{\chi(\pi; \pi'', \delta)} & \textit{all other cases.} \end{cases}$$

Proof. The condition $\chi(\pi; \pi', \delta) \in (\mathbf{Z}/m\mathbf{Z})^*$ in the second case is equivalent to $(\pi', \pi)_m$ being a primitive m-th root of unity, which by proposition 5.1 viii (with $d_2 = p$) is in turn equivalent to $(\pi', \pi)_p \neq 1$. Hence, in our arrow notation, the statement to be proved is

$$(\pi', \delta)_m \downarrow (\pi, \delta)_m = \begin{cases} 1 & \text{if } m = 2 \\ -\dfrac{(\pi, \pi')_m \downarrow (\pi, \delta)_m}{(\pi', \pi)_m \downarrow (\pi', \delta)_m} & \text{if } (\pi', \pi)_p \neq 1 \\ \dfrac{(\pi, \pi'')_m \downarrow (\pi, \delta)_m \cdot (\pi'', \pi')_m \downarrow (\pi'', \delta)_m}{(\pi'', \pi)_m \downarrow (\pi'', \delta)_m} & \text{all other cases.} \end{cases}$$

In the first case we have $m = 2$. Since $(\pi, \delta)_m$ and $(\pi', \delta)_m$ are of order m, we then have $(\pi, \delta)_m = (\pi', \delta)_m = -1$ and the result follows.

For the second case, using Proposition 5.1ii, one finds

$$-(\pi, \pi')_m \downarrow (\pi, \delta)_m = (\pi', \pi)_m \downarrow (\pi, \delta)_m = (\pi', \pi)_m \downarrow (\pi', \delta)_m \cdot (\pi', \delta)_m \downarrow (\pi, \delta)_m$$

and the result follows.

In the third case we have $m > 2$ and $(\pi', \pi)_p = 1$. As announced above, we shall use $\pi'' = -\delta\pi'$ as an intermediate prime element, and apply the second case with π'' first in the role of π', and next in the role of π. We have

$$(\pi'', \pi)_p = (-1, \pi)_p \cdot (\pi', \pi)_p \cdot (\delta, \pi)_p.$$

Here we have $(-1, \pi)_p = 1$ because $m > 2$ implies that -1 is a p-th power; $(\pi', \pi)_p = 1$ because we are in the third case; and $(\delta, \pi)_p = (\pi, \delta)_p^{-1} \neq 1$ by Proposition 5.1ii and

Lemma 5.6. Altogether, we have $(\pi'', \pi)_p \neq 1$, so the second case implies

$$(\pi'', \delta)_m \downarrow (\pi, \delta)_m = -\frac{(\pi, \pi'')_m \downarrow (\pi, \delta)_m}{(\pi'', \pi)_m \downarrow (\pi'', \delta)_m}.$$

Next we have $(\pi', \pi'')_m = (\pi', -\delta\pi')_m = (\pi', \delta)_m$, so we have

$$\chi(\pi'', \pi', \delta) = (\pi', \pi'')_m \downarrow (\pi', \delta) = 1.$$

Therefore the second case implies

$$(\pi', \delta)_m \downarrow (\pi'', \delta)_m = -(\pi'', \pi')_m \downarrow (\pi'', \delta)_m.$$

Combining the last two results, we obtain

$$(\pi', \delta)_m \downarrow (\pi, \delta)_m = (\pi', \delta)_m \downarrow (\pi'', \delta)_m \cdot (\pi'', \delta)_m \downarrow (\pi, \delta)_m =$$
$$= \frac{(\pi'', \pi')_m \downarrow (\pi'', \delta)_m \cdot (\pi, \pi'')_m \downarrow (\pi, \delta)_m}{(\pi'', \pi)_m \downarrow (\pi'', \delta)_m},$$

as required. □

We can finally give a formula for the norm residue symbol.

Theorem 5.11. *Let $x, y \in F^*$. Write $x = \omega(a)\pi^{v(x)}w'$ with $w' \in U_1$ and $a \in k$. Set $\pi' = w'\pi$. Let $\delta \in F^*$ be a distinguished unit and set $\pi'' = -\delta\pi'$. One has*

$$(x, y)_m = (\pi, \delta)_m^j$$

where $j \in \mathbf{Z}/m\mathbf{Z}$ is defined by

$$j = (v(x) - 1)\chi(y; \pi, \delta) + \chi(y; \pi', \delta) \cdot j' \text{ with}$$

$$j' = \begin{cases} 1 & \text{if } m = 2 \\ -\frac{\chi(\pi'; \pi, \delta)}{\chi(\pi; \pi', \delta)} & \text{if } m \neq 2, \chi(\pi; \pi', \delta) \in (\mathbf{Z}/m\mathbf{Z})^* \\ \frac{\chi(\pi''; \pi, \delta)\chi(\pi'; \pi'', \delta)}{\chi(\pi; \pi'', \delta)} & \text{all other cases.} \end{cases}$$

Proof. This follows directly from Lemma 5.7 and Proposition 5.10. □

For the next algorithms, recall how we represent elements in $(F^*/(F^*)^m)_N$ (see the end of section 2 of this chapter) .

Algorithm 5.12 (χ).
Input: $\overline{x} = (a, u') \in (F^*/(F^*)^m)_N$ where $m = p^n > 1$ such that $\mu_m \subset F^*$ and such that $N \geq e/(p-1) + ne + 1$, and $\overline{\delta} \in \mathcal{O}_N$ where δ is a distinguished unit and $\overline{v} \in \mathcal{O}_N^*$.
Output: $\chi(x; v\pi, \delta) \pmod{m}$.
Steps:

i. Compute $b' \in \mathcal{B}$ such that $(v\pi, \delta, b')$ is a distinguished triple (Algorithm 4.17).
ii. Compute $u'' = \frac{1}{(-\overline{v})^a} u' \in \mathcal{O}_N$.
iii. Compute $u''' = u''/\overline{\omega(\overline{u''})} \in \mathcal{O}_N$.
iv. Compute the exponential representation $(a_t)_t$ of $u''' \in \mathcal{O}_N$ with respect to $(\overline{v\pi}, \overline{\delta}, b')$ (Algorithm 4.21).
v. Return $a_\delta \pmod{m}$.

Proposition 5.13. *Algorithm 5.12 is correct and its complexity is* $O((N\log q)^{2[+1]} + (Nf^C)\cdot(\log p)^{1[+1]})$

Proof. The correctness follows from the definitions of χ and the exponential representation. In more detail, in the first steps we just write $\overline{\pi^a}u' = \overline{(-v\pi)^a\omega(\overline{u''})}u''' \in \mathcal{O}_N$. We then work with high enough precision to compute the exponent of the exponential representation of u''' modulo m at δ.

Let us compute the complexity. Step i, with Algorithm 4.17 (see Remark 4.19), has complexity $O(N\log q+(f+\log p)(\log q)^{1[+1]}+f^C(\log p)^{1[+1]})$. Step ii costs $O(\log m\cdot (N\log q)^{1[+1]})$ (Theorem 3.2) and step iii costs $O(\big(N+(N/e\log q)^{1[+1]}\big)\cdot\log q + (N\log q)^{1[+1]})$. Step iv has complexity $O((N\log q)^{2[+1]}+Nf^C(\log p)^{1[+1]})$ (Algorithm 4.21). □

Example 5.14. Let $F\supset \mathbf{Q}_2$ be given by $(p,g,h) = (2, X^2+X+1, Y^2-(2+2X)Y-2Y)$. As we have computed in Example 4.27 we have $m=4, \mu_4\subset F^*$ and further $b'=\gamma$ and $\delta = 1+\pi^4$.We choose $\bar{x} = (a,u') = (0, 1-\gamma\pi^3+\gamma^2\pi^6)$ and $v=1$ and compute $\chi(1-\gamma\pi^3+\gamma^2\pi^6,\pi,\delta)$. We follow the steps of Algorithm 5.12 and find $u'''=u''=u'=\bar{x}$. With Algorithm 4.21 we compute the exponential representation of $\bar{x}$ with respect to $(\bar{\pi}, \overline{1+\pi^4},\gamma)$ and find that $1-\gamma\pi^3+\gamma^2\pi^6 \equiv \delta^2(1-\gamma\pi^3) \bmod \pi^7$. So $a_\delta \equiv 2 \bmod m$ and we have $\chi(1-\gamma\pi^3+\gamma^2\pi^6;\pi,\delta) = 2 \bmod 4$.

Algorithm 5.15 (Symbol isomorphic to wild symbol).
Input: $\overline{x} = (a,u'), \overline{y} = (b,v') \in (F^*/(F^*)^m)_N$ where $m=p^n>1$ such that $\mu_m\subset F^*$ and such that $N\geq e/(p-1)+ne+1$, and $\overline{\delta}\in\mathcal{O}_N$ where δ is a distinguished unit.
Output: $j\in\mathbf{Z}/m\mathbf{Z}$ such that $(x,y)_m = (\pi,\delta)_m^j$.
Steps:

i. Compute $\overline{w'} = u'/\overline{\omega(\overline{u'})}\in\mathcal{O}_N^*$ and for notation set $\pi' = w'\pi$.
ii. Compute $\chi(y;\pi,\delta)$, $\chi(y;\pi',\delta)$, $\chi(\pi;\pi',\delta)\in\mathbf{Z}/m\mathbf{Z}$ (Algorithm 5.12).
If $m\neq 2$ and $\chi(\pi;\pi',\delta)\in(\mathbf{Z}/m\mathbf{Z})^*$, compute $\chi(\pi';\pi,\delta)\in\mathbf{Z}/m\mathbf{Z}$.
If $m\neq 2$ and $\chi(\pi;\pi',\delta)\notin(\mathbf{Z}/m\mathbf{Z})^*$, compute $\overline{w''} = -\overline{\delta w'}\in\mathcal{O}_N^*$ and for notation set $\pi'' = w''\pi$ and compute $\chi(\pi'';\pi,\delta)$, $\chi(\pi';\pi'',\delta)$, $\chi(\pi;\pi'',\delta)\in\mathbf{Z}/m\mathbf{Z}$ (Algorithm 5.12).
iii. Return

$$j = (a-1)\chi(y;\pi,\delta)+\chi(y;\pi',\delta)\cdot j' \textit{ with}$$

$$j' = \begin{cases} 1 & \text{if } m=2\\ -\frac{\chi(\pi';\pi,\delta)}{\chi(\pi;\pi',\delta)} & \text{if } m\neq 2, \chi(\pi;\pi',\delta)\in(\mathbf{Z}/m\mathbf{Z})^*\\ \frac{\chi(\pi'';\pi,\delta)\chi(\pi';\pi'',\delta)}{\chi(\pi;\pi'',\delta)} & \text{all other cases.}\end{cases}$$

Proposition 5.16. *Algorithm 5.15 is correct and has complexity* $O((N\log q)^{2[+1]}+Nf^C(\log p)^{1[+1]})$.

Proof. The correctness follows from Theorem 5.11.

Step i costs $O(\big(N+((N/e)\log q)^{1[+1]}\big)\cdot\log q + (N\log q)^{1[+1]})$ (Theorem 3.2). For step ii, use Algorithm 5.12 in time $O((N\log q)^{2[+1]}+Nf^C(\log p)^{1[+1]})$. Step iii has low complexity. □

5. Computing the exact value of the wild norm residue symbol

In the previous section, we have described an algorithm for computing a symbol which is isomorphic to the norm residue symbol. In this section we explain how to compute the true value of the residue symbol. These true values are often of importance if one computes local norm residue symbols in the context of global class field theory. In this section we use the same notation as in section two of the present chapter. Moreover we put $m = p^n$ with $n \in \mathbf{Z}_{>0}$.

For $x \in F^*$, define $x^* \in \mathbf{Z}_p^*$ by $N_{F/\mathbf{Q}_p}(x) = x^* p^c$ with $x^* \in \mathbf{Z}_p^*$ and $c \in \mathbf{Z}$.

PROPOSITION 5.17. *Let $s \in \mathbf{Z}_{>0}$ be maximal such that $\mu_{p^s} \subset F^*$. Let ζ_{p^s} be a primitive p^s-th root of unity. Let $x \in F^*$. Then m divides p^s and one has $x^* \in 1+p^s\mathbf{Z}_p$ and*

$$(x, \zeta_{p^s})_m = \zeta_{p^s}^{\frac{1-x^*}{m}}.$$

Finally, there exists $y \in F^*$ with $y^* \in 1 + p^s\mathbf{Z}_p \setminus 1 + p^{s+1}\mathbf{Z}_p$.

PROOF. By definition we have $(x, \zeta_{p^s})_m = \frac{\phi_F(x)(\sqrt[m]{\zeta_{p^s}})}{\sqrt[m]{\zeta_{p^s}}}$. As follows from the commutative diagram below [see **17**, Chapter 2, Proposition (5.4)], we have $\phi_{\mathbf{Q}_p} \circ N_{F/\mathbf{Q}_p} = \mathrm{Res} \circ \phi_F$ where $\mathrm{Res} : \mathrm{Gal}(F(\sqrt[m]{\zeta_{p^s}})/F) \longrightarrow \mathrm{Gal}(\mathbf{Q}_p(\sqrt[m]{\zeta_{p^s}})/\mathbf{Q}_p)$ is the restriction map.

$$\begin{tikzcd}
F^* \arrow[r, "\phi_F"] \arrow[d, "N_{F/\mathbf{Q}_p}"] & \mathrm{Gal}(F(\sqrt[m]{\zeta_{p^s}})/F) \arrow[d, "\mathrm{Res}"] \\
\mathbf{Q}_p^* \arrow[r, "\phi_{\mathbf{Q}_p}"] & \mathrm{Gal}(\mathbf{Q}_p(\sqrt[m]{\zeta_{p^s}})/\mathbf{Q}_p)
\end{tikzcd}$$

According to the easy description of $\phi_{\mathbf{Q}_p}$ as in [**17**, Chapter 3, Theorem (4.4)], we have

$$(x, \zeta_{p^s})_m = \frac{\phi_{\mathbf{Q}_p}(N_{F/\mathbf{Q}_p}(x))(\sqrt[m]{\zeta_{p^s}})}{\sqrt[m]{\zeta_{p^s}}} = \left(\sqrt[m]{\zeta_{p^s}}\right)^{(x^*)^{-1}-1} = \zeta_{p^s}^{\frac{(x^*)^{-1}-1}{m}}.$$

Since $(x, \zeta_{p^s})_m \in \mu_m$, it follows that $x^* \in 1 + p^s\mathbf{Z}_p$. Since ζ_{p^s} is not a p-th power, it follows that there exists $y \in F^*$ with $y^* \in 1 + p^s\mathbf{Z}_p \setminus 1 + p^{s+1}\mathbf{Z}_p$ (see Proposition 5.1 (v) with $m = p$). Furthermore we have $(x^* - 1)^2 \equiv 0 \bmod p^{2s}$ and so $(x^*)^2 - x^* \equiv x^* - 1 \bmod p^{2s}$. Division by x^* gives $x^* - 1 \equiv 1 - (x^*)^{-1} \bmod p^{2s}$ and we have $\frac{1-x^*}{m} \equiv \frac{(x^*)^{-1}-1}{m} \bmod p^s$. □

By the above proposition we can use y as in the proposition to gauge our isomorphic norm residue symbol (Algorithm 5.15). To find a suitable y, it is enough to compute y^* for a generating set of $F^*/(F^*)^p$ as $\mathbf{F}_p$-vector space.

We can finally describe the norm algorithm we need to compute the exact norm residue symbol. Note that the norm map $N_{\mathcal{O}/\mathbf{Z}_p} : \mathcal{O} \to \mathbf{Z}_p$ induces for $M \in \mathbf{Z}_{\geq 1}$ maps

$$N_M : \mathcal{O}_{Me} = \mathcal{O}/p^M\mathcal{O} = \mathcal{O} \otimes_{\mathbf{Z}_p} (\mathbf{Z}_p/p^M\mathbf{Z}_p) \to \mathbf{Z}/p^M\mathbf{Z}.$$

ALGORITHM 5.18 (Norm).
Input: $x \in \mathcal{O}_{Me}$ with $M \in \mathbf{Z}_{\geq 1}$.

Output: $N_M(x) \in \mathbf{Z}/p^M\mathbf{Z}$.
Steps:

```
i. Compute $\mathcal{D} = \{\overline{\gamma^i\pi^j} : \ 0 \leq i < f, \ 0 \leq j < e\} \subset \mathcal{O}_{Me}$.
ii. Compute $A = [\cdot x]_{\mathcal{D}} \in \mathrm{Mat}_{ef}(\mathbf{Z}/p^M\mathbf{Z})$.
iii. Return $\det(A) \in \mathbf{Z}/p^M\mathbf{Z}$.
```

Proposition 5.19. *Algorithm 5.18 is correct and has complexity* $O((ef)^3(\log p^M)^{1[+1]})$.

Proof. The algorithm is obviously correct. Step i and ii cost $O(ef{\cdot}Me(\log q)^{1[+1]})$ by Theorem 3.2. Step iii costs $O((ef)^3(\log p^M)^{1[+1]})$. □

Example 5.20. Let $F \supset \mathbf{Q}_2$ be given by $(p, g, h) = (2, X^2 + X + 1, Y^2 - (2 + 2X)Y - 2X)$. We have $\mathcal{D} = \{\overline{1}, \overline{\gamma}, \overline{\pi}, \overline{\gamma\pi}\}$. We choose $M = 5$ and compute $N_{10}(1 - \gamma\pi^3)$. Using the identities $\gamma^2 = -\gamma - 1$ and $\pi^2 = (2 + 2\gamma)\pi + 2\gamma$ we find that

- $1 - \gamma\pi^3 = 1 + 4\gamma + 6\pi + 6\gamma\pi$
- $\gamma(1 - \gamma\pi^3) = -4 - 3\gamma - 6\pi$
- $\pi(1 - \gamma\pi^3) = -12 + \pi + 16\gamma\pi$
- $\gamma\pi(1 - \gamma\pi^3) = -12\gamma - 16\pi - 15\gamma\pi$

This gives the matrix $A = \begin{pmatrix} 1 & 4 & 6 & 6 \\ -4 & -3 & -6 & 0 \\ -12 & 0 & 1 & 16 \\ 0 & -12 & -16 & -15 \end{pmatrix}$ with $\det(A) = 613 \equiv 5 \bmod 32$. We have $N_{10}(1 - \gamma\pi^3) \in 1 + 4\mathbf{Z}_2 \setminus 1 + 8\mathbf{Z}_2$ and so $1 - \gamma\pi^3$ is a suitable element of $F^*/(F^*)^2$ to gauge the isomorphic norm residue symbol of fourth order.

Let us discuss how we can use the above proposition to compute the exact value of the norm residue symbol.

Algorithm 5.21 (Computing an exact norm residue symbol value).
Input: $\mathcal{O}_N$ with $s \geq 1$ such that $\mu_{p^s} \subset F$ but $\mu_{p^{s+1}} \not\subset F$ and $N = 2se + 1$, $\overline{\zeta_{p^s}} \in \mathcal{O}_N$, $\overline{\delta} \in \mathcal{O}_N$ where δ is a distinguished unit.
Output: $c \in \mathbf{Z}/p^s\mathbf{Z}$ such that $(\pi, \delta)_{p^s} = \zeta_{p^s}^c$.
Steps:

```
i. Compute $Z = \{\overline{\pi}, \overline{\delta}\} \cup \{\overline{1 - \gamma^j\pi^i} : (i, j) \in T\} \subset \mathcal{O}_N$ where $T = \{(i, j) \in \mathbf{Z}^2 : 0 \leq j < f, 1 \leq i < \frac{pe}{p-1}, p \nmid i\}$.
ii. Compute $(z, \zeta_{p^s})_p$ for $z \in Z$ and let $z' \in Z$ such that $(z', \zeta_{p^s})_p \neq 1$ (Algorithm 5.15).
iii. Compute $z'^* = (1 - N_{2s}(\overline{z'}))/p^s \in (\mathbf{Z}/p^s\mathbf{Z})^*$ (Algorithm 5.18).
iv. Compute $j \in (\mathbf{Z}/p^s\mathbf{Z})^*$ such that $(z', \zeta_{p^s})_{p^s} = (\pi, \delta)_{p^s}^j$ (Algorithm 5.15).
v. Return $c = z'^*/j$.
```

Proposition 5.22. *Algorithm 5.21 is correct and has complexity* $O((ef)^{3[+1]}(\log e)^{2[+1]})$.

Proof. The map $x \mapsto x^*$ induces a group homomorphism $F^*/(F^*)^p \longrightarrow (1 + p^s\mathbf{Z}_p)/(1 + p^{s+1}\mathbf{Z}_p)$ that by Proposition 5.17 is non-trivial, and since Z generates $F^*/(F^*)^p$ it contains an element $z'^* \in (1 + p^s\mathbf{Z}_p)/(1 + p^{s+1}\mathbf{Z}_p)$. From this it follows that $\frac{1-z'^*}{p^s} \notin p\mathbf{Z}_p$ so $\zeta_{p^s}^{\frac{1-z^*}{p}} \neq 1$ which is, according to Proposition 5.17, equivalent to $(z'^*, \zeta_{p^s})_p \neq 1$. This explains the second step. Further we remark that in the third step of the Algorithm working in $\mathcal{O}_M$ with $M = 2s$ is necessary, because of the division by p^s. With Algorithm 5.15 the integer $j \in (\mathbf{Z}/p^s\mathbf{Z})^*$ is computed for which $(z'^*, \zeta_{p^s})_{p^s} = (\pi, \delta)_{p^s}^j$. If we combine the results of step iii and step iv it follows that $c = z'^*/j$. This proves the correctness

Step i costs $O(ef \cdot (N \log q)^{1[+1]})$ by Theorem 3.2. For step ii we apply Algorithm 5.15 and the cost is $O((ef) \cdot ((N \log q)^{2[+1]} + Nf^C(\log p)^{1[+1]}))$. For step iii we use Algorithm 5.18 and the cost is $O((ef)^3(\log p^{2s})^{1[+1]})$. For Step iv, we use Algorithm 5.15 again. The last step has low complexity. Furthermore $O(N \log q) = O(fN \log p) = O(sef \log p) = O(fe \cdot \log e)$. The dominating term in the complexity is therefore $O(ef \cdot (N \log q)^{2[+1]}) = O((ef)^{3[+1]} \cdot (\log e)^{2[+1]})$. Note that we have $N = 2se + 1 \geq e/(p-1) + se + 1$, so we can apply the algorithm. □

Example 5.23. Let $F \supset \mathbf{Q}_2$ again be given by $(p, g, h) = (2, X^2 + X + 1, Y^2 - (2 + 2X)Y - 2X)$ and let $\delta = 1 + \pi^4$ be our distinguished unit. We compute the true value of $(\pi, \delta)_4$. In Example 5.20 we computed $N_{F/\mathbf{Q}_p}(1 - \gamma\pi^3) = \overline{5} \in \mathbf{Z}/2^5\mathbf{Z}$. From this it follows that $\frac{N_{F/\mathbf{Q}_p}(1-\gamma\pi^3)^* - 1}{4} = 1$ and $(\zeta_4, 1 - \gamma\pi^3)_4 = \zeta_4$.

The norm residue symbol $(\zeta_4, 1 - \gamma\pi^3)_4$ can also be computed by Algorithm 5.15 of Chapter 5. We have $\zeta_4 = (1 - \gamma\pi)^{-1} \cdot (1 - \pi)^2 \bmod \pi^7$ and further with Algorithm 5.15 we obtain $(1-\gamma\pi, 1-\gamma\pi^3)_4 \downarrow (\pi, \delta)_4 = 1$ and $(1-\pi, 1-\gamma\pi^3)_4 \downarrow (\pi, \delta)_4 = 2$ (see the table in Example 6.11). Taking everything together we have $(\zeta_4, 1 - \gamma\pi^3)_4 \downarrow (\pi, \delta)_4 = -1 \cdot 1 + 2 \cdot 2 \equiv 3 \bmod 4$. This gives $(\pi, \delta)_4^3 = \zeta_4$ and $(\pi, \delta)_4 = \zeta_4^3$.

With the above algorithm one can now finally compute the true norm residue symbol.

Algorithm 5.24 (Wild norm residue symbol).
Input: $\mathcal{O}_N$ with $N \geq 3(r+1)e + 1$ and $x, y \in (F^*/(F^*)^m)_N$ where $m = p^n > 0$ with $n \leq r + 1$ and r as in Chapter 2.
Output: $s \in \mathbf{Z}_{\geq 0}$ maximal such that $\mu_{p^s} \subset F$; $\overline{\zeta_{p^s}} \in \mathcal{O}_{N-es}$ where ζ_{p^s} is some primitive p^s-th root of unity; $\overline{(x,y)_m} \in \mathcal{O}_{N-es}$ if $n \leq s$.
Steps:

```
i. Compute $s \in \mathbf{Z}_{\geq 0}$ and $\overline{\zeta_{p^s}} \in \mathcal{O}_{N-es}$ (Algorithm 4.23).
ii. If $n \leq s$:
    • Compute $\overline{\delta} \in \mathcal{O}_N$ where $\delta$ is a weakly distinguished unit (Algorithm 4.15).
    • Compute $j$ such that $(x, y)_m = (\pi, \delta)_m^j$ (Algorithm 5.15).
    • Compute $c \in \mathbf{Z}/p^s\mathbf{Z}$ such that $(\pi, \delta)_{p^s} = \zeta_{p^s}^c$ (Algorithm 5.21).
    • Compute $\overline{(x,y)_m} = \overline{\zeta_{p^s}}^{jcp^{s-n}} \in \mathcal{O}_{N-es}$.
iii. Return $s$, $\overline{\zeta_{p^s}}$ and if $n \leq s$ the value $\overline{(x,y)_m}$.
```

Proposition 5.25. *Algorithm 5.24 is correct and has complexity*

$$O((ef)^{3[+1]} \cdot (\log e)^{2[+1]} + (r+1) \log p \cdot (N \log q)^{1[+1]}).$$

Proof. The correctness follows easily. Step i: Algorithm 4.23 costs $O((N\log q)^{2[+1]}+ Nf^C(\log p)^{1[+1]})$. Step ii: Part 1: Note that $N \geq pe/(p-1)+1+er$. Algorithm 4.15 costs $O((f+\log p)(\log q)^{1[+1]}+f^C(\log p)^{1[+1]}+N\log q)$. Part 2: Note that $N-es\geq 2se+1$. Algorithm 5.15 costs $O((N\log q)^{2[+1]}+Nf^C(\log p)^{1[+1]})$ (we can replace N by $N-es$ here). Part 3: Note that $N\geq pe/(p-1)+1$. Algorithm 5.21 costs $O((ef)^{3[+1]}\cdot(\log e)^{2[+1]})$. Part 4: This costs $O((r+1)\log p\cdot(N\log q)^{1[+1]})$ by Theorem 3.2. □

In the introduction of this thesis we stated the next theorem.

Theorem 5.26. *There is a polynomial-time algorithm that, given a prime number p, a positive integer m and a finite extension F of $\mathbf{Q}_p$ containing a primitive m-th root of unity and also given two elements $\alpha,\beta\in F^*/(F^*)^m$, computes the norm residue symbol $(\alpha,\beta)_m$.*

Proof. There are two different cases to distinguish. In the tame case, where $p\nmid m$, we have Proposition 5.3, the proof of which is found in [**17**, Ch.3, section 5], and Algorithm 5.4. In the wild case, where $p\mid m$, we have Theorem 5.11 and the Algorithms 5.12 and 5.15. The true value of the norm residue symbol in the wild case is computed with Algorithm 5.24 where we use Proposition 5.17 and Algorithm 5.21. □

Chapter 6

Strongly distinguished units

1. Introduction

We defined a distinguished unit in a field $F \supseteq \mathbf{Q}_p(\zeta_p)$ to be a principal unit in $U_{pe/(p-1)}$ having no p-th root in $U_{e/(p-1)}$. Such a unit plays an important role in the exponential representation of principal units. In this section we introduce the notion of a strongly distinguished unit. Throughout this chapter p is a prime number and n is a positive integer. We let F be a finite extension of $\mathbf{Q}_p$ with $\mu_{p^n} \subset F$. We denote the ramification index of F over $\mathbf{Q}_p$ by e.

Definition 6.1. A *strongly distinguished unit of degree* $n \in \mathbf{Z}_{\geq 1}$ is a principal unit $\epsilon_n \in U_1$ with the property that $\mathrm{ord}_F(\epsilon_n - 1) = \frac{pe}{p-1}$ and such that $F(\sqrt[p^n]{\epsilon_n})$ is an unramified extension of F of degree p^n.

As we explained in Chapter 1, it may be of advantage to compute a strongly distinguished unit once and for all if a large number of norm residue symbols in the same field F has to be computed. If a strongly distinguished unit is used, the formula of Lemma 5.7 for the norm residue symbol of order p^n can be simplified, as we will see in Lemma 6.3ii below.

We give a few results that are almost immediate consequences of Definition 6.1 and the results of Chapter 5.

Lemma 6.2. *Let $\epsilon \in U_1$ with $\mathrm{ord}_F(\epsilon - 1) = pe/(p-1)$. Then ϵ is a strongly distinguished unit of degree n if and only if $\epsilon \notin F^{*p}$ and $(u, \epsilon)_{p^n} = 1$ for every $u \in \mathcal{O}_F^*$.*

Proof. From Proposition 5.1 of Chapter 5, part vii with $\beta = \epsilon, m = p^n$ and $\alpha' = u \in \mathcal{O}_F^*$, it follows that $(u, \epsilon)_{p^n} = 1$ for every $u \in \mathcal{O}_F^*$ if and only if the extension $F(\sqrt[p^n]{\epsilon_n})$ is unramified. Moreover $\epsilon \notin F^{*p}$ is equivalent to $[F(\sqrt[p^n]{\epsilon_n}) : F] = p^n$. □

Lemma 6.3. *Let $\epsilon_n \in U_1$ be a strongly distinguished unit of degree n. Then:*

i. *Let π, π' be prime elements of F. Then: $(\pi, \epsilon_n)_{p^n} = (\pi', \epsilon_n)_{p^n}$.*

ii. *Let $x, y \in F^*$. Write $x = \omega(a)\pi^{v(x)}w'$ with $w' \in U_1$ and $a \in k^*$. Set $\pi' = w'\pi$. Then one has*

$$(x, y)_{p^n} = (\pi, \epsilon_n)_{p^n}^{(v(x)-1)\chi(y;\pi,\epsilon_n)+\chi(y;\pi',\epsilon_n)}.$$

Proof. i: Follows from Lemma 6.2.

ii: Follows from i and Lemma 5.7 from Chapter 5. □

Lemma 6.4.

i. *Every strongly distinguished unit of degree $n \in \mathbf{Z}_{\geq 1}$ is a distinguished unit.*
ii. *Let $\delta \in F$. Then δ is a strongly distinguished unit of degree* 1 *if and only if δ is a distinguished unit.*

Proof. i: From Lemma 6.2 it follows that a strongly distinguished unit of degree n is not a p-th power.

ii: Let δ be a distinguished unit, then we have according to Proposition 5.1x, that $(u, \delta)_p = 1$ for every unit u, and then Proposition 5.1vii, with $m = p$, $\alpha' = u$ and $\beta = \delta$, says that $F(\sqrt[p]{\delta})$ is an unramified extension of F. The degree of this extension equals p, because $\delta \notin (F^*)^p$. Moreover we have $\mathrm{ord}_F(\delta - 1) = \frac{pe}{p-1}$, so δ is a strongly distinguished unit of degree 1. The other implication follows from i. □

In this Chapter we will prove Theorem 1.3 and Theorem 1.4 from Chapter 1. We prove the existence of strongly distinguished units in section 2. In section 3 we exhibit a uniquely solvable system of linear equations over $\mathbf{Z}/p^n\mathbf{Z}$ with the property that its unique solution gives rise to a strongly distinguished unit. This result leads, in section 4, to a polynomial-time algorithm that computes strongly distinguished units. Finally we give an example in section 5.

2. Existence

Lemma 6.5. *There exists $\epsilon \in U_1$ with* $\mathrm{ord}_F(\epsilon - 1) \geq p^n > 0$ *such that $F(\sqrt[p^n]{\epsilon})$ is an unramified extension of F of degree p^n.*

Proof. It is a well-known fact that there is a (unique) unramified extension L of F of degree p^n. By Kummer theory there is an element $\alpha \in F$ such that $L = F(\sqrt[p^n]{\alpha})$. There are an integer $i \in \mathbf{Z}$, an element $\beta \in \mathcal{O}_F/\mathfrak{m}_F$ and a principal unit $\epsilon \in U_1$ such that $\alpha = \pi^i \cdot \omega(\beta) \cdot \epsilon$. We have $p^n \mid i$ because the extension $F(\sqrt[p^n]{\alpha})/F$ is unramified. Furthermore $\omega(\beta) \in (F^*)^{p^n}$. This proves that there is a principal unit ϵ such that $L = F(\sqrt[p^n]{\epsilon})$. Because L is an unramified extension of F we have $\mathrm{ord}_F(1-\epsilon) = \mathrm{ord}_L(1-\epsilon)$. There are elements $a_i \in L$ such that $X^{p^n} - \epsilon = \prod_{i=1}^{p^n}(X - a_i)$, a product of p^n factors. Note that $\mathrm{ord}_L(1 - a_i) \geq 1$ since a_i is a principal unit. If we substitute $X = 1$ we obtain

$$\mathrm{ord}_F(1-\epsilon) = \mathrm{ord}_L(1-\epsilon) = \sum_{i=1}^{p^n} \mathrm{ord}_L(1 - a_i) \geq p^n \cdot 1 = p^n.$$

□

The theorem below proves the existence of strongly distinguished units.

Theorem 6.6. *There exists $\epsilon \in F$ such that*

i. $\mathrm{ord}_F(\epsilon - 1) = e_{F/\mathbf{Q}_p(\zeta_{p^n})} \cdot p^n = \frac{pe}{p-1}$,
ii. *$F(\sqrt[p^n]{\epsilon})$ is an unramified field extension of F of degree p^n.*

There does not exist $\epsilon \in F$ satisfying ii *and* $\mathrm{ord}_F(\epsilon - 1) > \frac{pe}{p-1}$.

Proof. Let E be the unique maximal subextension of F which is unramified over $\mathbf{Q}_p(\zeta_{p^n})$. Let $\epsilon \in E$ with $\mathrm{ord}_E(\epsilon - 1) \geq p^n > 0$ such that $E(\sqrt[p^n]{\epsilon})$ is an unramified extension of E of degree p^n (Lemma 6.5). As a consequence, $F(\sqrt[p^n]{\epsilon})$ is an unramified field extension of F of degree p^n. Note that $e_{E/\mathbf{Q}_p} = e_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p} = p^{n-1}(p-1)$. Also ϵ is a p-th power in E if $\mathrm{ord}_E(\epsilon - 1) > p \cdot p^{n-1}(p-1)/(p-1) = p^n$ (Corollary 4.4). Hence $\mathrm{ord}_E(\epsilon - 1) = p^n$. It follows that

$$\mathrm{ord}_F(\epsilon - 1) = e_{F/E} \cdot \mathrm{ord}_E(\epsilon - 1) = e_{F/\mathbf{Q}_p(\zeta_{p^n})} \cdot \mathrm{ord}_E(\epsilon - 1) = e_{F/\mathbf{Q}_p(\zeta_{p^n})} \cdot p^n.$$

This proves the first result.

By Corollary 4.4 from Chapter 4, any $\epsilon \in U_1$ with $\mathrm{ord}_F(\epsilon - 1) > \frac{pe}{p-1}$ is a p-th power in F. Hence such an ϵ cannot satisfy condition ii. □

Now we have also proven Theorem 1.3.

3. Constructing a unique strongly distinguished unit

Let δ be a distinguished unit and let π be a prime element. We refer to section 2.2 of Chapter 4, where the set $T_{\pi',\delta}$ is defined with π' is a prime element, and to Definition 4.10 where $\mu(x, N)$ is defined. We also refer to Definition 4.11 where the morphism $\chi(\cdot; \pi', \delta) : F^* \longrightarrow \mathbf{Z}/p^s\mathbf{Z}$ is defined. In the next lemma we take $s = n$. Remember that $(\pi, \delta)_{p^n}$ is a primitive p^n-th root of unity (Lemma 5.6). We shall write

$$T^*_{\pi,\delta} = \{z \in T_{\pi,\delta} : \mu(z, pe/(p-1)) \leq n - 1\},$$

which by section 2.1 of Chapter 4 is equal to $\{z \in T_{\pi,\delta} : \mathrm{ord}_F(z-1) \geq e/((p-1)p^{n-2})\}$.

Lemma 6.7.

i. *For $z, z' \in T_{\pi,\delta}$, define $b_{z',z} \in \mathbf{Z}/p^n\mathbf{Z}$ by $(z', z)_{p^n} = (\pi, \delta)_{p^n}^{b_{z',z}}$. Then the system of linear equations*

$$\begin{cases} \sum_{z \in T^*_{\pi,\delta}} b_{z',z} x_z = 0 & \text{for all } z' \in T_{\pi,\delta}, z \neq \delta \\ \qquad x_\delta = 1 \end{cases}$$

has a unique solution with all $x_z \in \mathbf{Z}/p^n\mathbf{Z}$.

ii. *The unique solution $(x_z)_{z \in T^*_{\pi,\delta}}$ from* i *satisfies $x_z \in p^{\mu(z,pe/(p-1))}\mathbf{Z}/p^n\mathbf{Z}$ for all z.*

iii. *If $(c_z)_{z \in T^*_{\pi,\delta}} \in \mathbf{Z}^{T^*_{\pi,\delta}}$ satisfies $(c_z \bmod p^n) = x_z$ for all z, with $(x_z)_{z \in T^*_{\pi,\delta}}$ as in* i, *then $\epsilon = \prod_{z \in T^*_{\pi,\delta}} z^{c_z}$ is a strongly distinguished unit of degree n.*

Proof. Let ϵ'_n be a strongly distinguished unit of degree n. By Lemma 6.4i and Lemma 5.6 each of $(\pi, \epsilon'_n)_{p^n}$ and $(\pi, \delta)_{p^n}$ has order p^n. So there is a positive integer a with $p \nmid a$ such that $(\pi, \delta)_{p^n} = (\pi, \epsilon'_n)^a_{p^n} = (\pi, \epsilon'^a_n)_{p^n}$. Choose $\epsilon_n = \epsilon'^a_n$, then ϵ_n is a strongly distinguished unit for which $\chi(\epsilon_n; \pi, \delta) = 1$. Write $\epsilon_n = \prod_{z \in T_{\pi,\delta}} z^{a_z}$ with $a_z \in \mathbf{Z}_p$ (Proposition 4.8ii). Then we have $(a_\delta \bmod p^n) = \chi(\epsilon_n; \pi, \delta) = 1$. From $\epsilon_n \in U_{pe/(p-1)}$ it follows that for every $z \in T_{\pi,\delta}$ we have $p^{\mu(z,pe/(p-1))} \mid a_z$. In particular $(a_z \bmod p^n) = 0$ if $\mu(z, pe/(p-1)) \geq n$ or equivalently if $z \notin T^*_{\pi,\delta}$. From

5.1vii and the fact that $F(\sqrt[p^n]{\epsilon_n})$ is an unramified extension of F, it follows that for every $z' \in T_{\pi,\delta}$ we have

$$1 = (z', \epsilon_n)_{p^n} = \prod_{z \in T_{\pi,\delta}} (z', z)_{p^n}^{a_z} = \prod_{z \in T^*_{\pi,\delta}} (z', z)_{p^n}^{a_z} = (\pi, \delta)_{p^n}^{\sum_{z \in T^*_{\pi,\delta}} b_{z',z} a_z}.$$

So for every $z' \in T_{\pi,\delta}$ we have $\sum_{z \in T^*_{\pi,\delta}} b_{z',z}(a_z \bmod p^n) = 0$ in $\mathbf{Z}/p^n\mathbf{Z}$, while we just proved $(a_\delta \bmod p^n) = 1$. Hence $x_z = (a_z \bmod p^n)$ is a solution to the system of linear equations in i, and this solution also satisfies ii.

To prove uniqueness, let $(x_z)_{z \in T^*_{\pi,\delta}}$ be any solution, and let $\epsilon = \prod_{z \in T^*_{\pi,\delta}} z^{c_z}$ be as in iii. Then $\chi(\epsilon; \pi, \delta) = (1 \bmod p^n)$, and for each $z' \in T_{\pi,\delta}$, we have

$$(z', \epsilon)_{p^n} = \prod_{z \in T^*_{\pi,\delta}} (z', z)_{p^n}^{c_z} = (\pi, \delta)_{p^n}^{\sum_{z \in T^*_{\pi,\delta}} b_{z',z} x_z} = (\pi, \delta)_{p^n}^0 = 1.$$

Let $\alpha' \in \mathcal{O}_F^*$. Since α' can by Proposition 4.8ii be written as $\alpha' = \omega(\alpha' \bmod \mathfrak{m}) \cdot \prod_{z' \in T^*_{\pi,\delta}} z'^{d_{z'}}$ with $d'_z \in \mathbf{Z}_p$ and $\omega(k^*) \subset (F^*)^{p^n}$, we obtain $(\alpha', \epsilon)_{p^n} = 1$. Hence Proposition 5.1vii implies that $F(\sqrt[p^n]{\epsilon})$ is an unramified extension of F. By Kummer theory we have $\epsilon = \epsilon_n^i \cdot u^{p^n}$ with $i \in \mathbf{Z}$ and $u \in U_1$. Then $1 = \chi(\epsilon; \pi, \delta) = i \cdot \chi(\epsilon_n; \pi, \delta) + p^n \cdot \chi(u; \pi, \delta) \equiv i \bmod p^n$. Using the exponential representation from Proposition 4.8ii for ϵ, ϵ_n, u we obtain

$$\prod_{z \in T^*_{\pi,\delta}} z^{c_z} = \prod_{z \in T_{\pi,\delta}} z^{i a_z} \cdot \prod_{z \in T_{\pi,\delta}} z^{p^n \cdot e_z}$$

(with $e_z \in \mathbf{Z}_p$). According to Proposition 4.8ii, corresponding exponents are congruent modulo p^n, so for all $z \in T^*_{\pi,\delta}$ we have

$$x_z = (c_z \bmod p^n) = (i a_z \bmod p^n) = (a_z \bmod p^n).$$

This proves that $(a_z \bmod p^n)_{z \in T^*_{\pi,\delta}}$ is the unique solution to our system.

To prove that ϵ is a strongly distinguished unit of degree n, we remark that $c_z \equiv a_z \equiv 0 \bmod p^{\mu(z, pe/(p-1))}$, for $z \in T^*_{\pi,\delta}$ it follows that $\epsilon \in U_{pe/(p-1))}$. Also, from $\chi(\epsilon; \pi, \delta) = 1 \bmod p^n$ it follows that $\epsilon \notin (F^*)^p$ so that in particular $\epsilon \notin U_{1+pe/(p-1)}$. □

4. Computation

Let us now discuss how to compute a strongly distinguished unit.

Algorithm 6.8 (Strongly distinguished unit).
Input: $\mathcal{O}_N$ with $\zeta_{p^n} \in F$ and with $N \geq e/(p-1) + ne + 1$.
Output: A strongly distinguished unit $\epsilon_n \in \mathcal{O}_N$ of degree n.
Steps:

i. Compute $\overline{\delta} \in \mathcal{O}_N$ where $\overline{\delta}$ is a distinguished unit (Algorithm 4.15). If $n = 1$ return $\overline{\epsilon}_1 = \overline{\delta}$ and terminate.
ii. Compute $\overline{T_{\pi,\delta}} = \{\overline{1 - \omega(\gamma^j)\pi^i} \in \mathcal{O}_N, (i,j) \in S\} \cup \{\overline{\delta}\} \subset \mathcal{O}_N$ where $S = \{(i,j) \in \mathbf{Z}^2 : 0 \leq j < f, 1 \leq i < \frac{pe}{p-1}, p \nmid i\}$.

iii. For $\overline{z}, \overline{z'} \in \overline{T_{\pi,\delta}}$ compute $b_{z',z} \in \mathbf{Z}/p^n\mathbf{Z}$ with $(z',z)_{p^n} = (\pi,\delta)_{p^n}^{b_{z',z}}$ (Algorithm 5.15).

iv. Find $\overline{c_z} \in \mathbf{Z}/p^n\mathbf{Z}$ for $z \in T_{\pi,\delta}$, such that $\overline{c_\delta} = 1$ and such that for all $z' \in T_{\pi,\delta}$ we have

$$\sum_{z \in T_{\pi,\delta}} b_{z',z}\overline{c_z} = 0 \in \mathbf{Z}/p^n\mathbf{Z}.$$

v. For every $z \in T_{\pi,\delta}$ choose $c_z \in \{0, 1, \ldots, p^n - 1\}$ such that $(c_z \bmod p^n) = \overline{c_z}$.

vi. Return $\overline{\epsilon_n} \in \mathcal{O}_N$ with $\overline{\epsilon}_n = \prod_{\overline{z} \in \overline{T_{\pi,\delta}}} \overline{z}^{\overline{c_z}}$.

Proposition 6.9. *Algorithm 6.8 is correct and its complexity is* $O((ef)^2 \cdot ((N \log q)^{2[+1]} + Nf^C(\log p)^{1[+1]}))$.

Proof. The correctness of the Algorithm follows from Lemma 6.7. Let us discuss the complexity of the algorithm. Note that $p^n = O(e)$ and $e = O(N)$. Step i costs $O((f + \log p)(\log q)^{1[+1]} + f^C(\log p)^{1[+1]} + N \log q)$ by Algorithm 4.15. Step ii costs less than step iii. Step iii costs $(ef)^2 \cdot O((N \log q)^{2[+1]} + Nf^C(\log p)^{1[+1]})$ (Algorithm 5.15). Step iv is solving an $ef \times ef$ system over $\mathbf{Z}/p^n\mathbf{Z}$, which costs $O((ef)^3(\log p^n)^{1[+1]})$. Step v costs $O(\log p^n \cdot ef \cdot (N \log q)^{1[+1]})$ (Theorem 3.2). □

Theorem 6.10. *There is a polynomial-time algorithm that, given a prime number p, a positive integer n, and a finite extension F of $\mathbf{Q}_p$ containing the p^n-th roots of unity, computes an element ϵ of F satisfying conditions* (i) *and* (ii) *from Theorem 1.3.*

Proof. In Theorem 6.4 we proved the existence of a strongly distinguished unit and in Algorithm 6.8, whose correctness is proven in Proposition 6.9, we gave a polynomial-time algorithm to compute such a unit. This concludes the proof and we have also proven Theorem 1.4 from Chapter 1. □

5. Examples

Example 6.11. Let, as in previous examples, $F \supset \mathbf{Q}_2$ be given by $(p, g, h) = (2, X^2 + X + 1, Y^2 - (2 + 2X)Y - 2Y)$. A distinguished unit, as we have seen Example 4.6, is $\delta = 1 + \pi^4$. We want to compute a strongly distinguished unit ϵ_2 for the 4-th norm residue symbol in F by using the following table where we have computed $(\alpha,\beta)_4 \downarrow (\pi,\delta)_4$ for every $\alpha, \beta \in T_{\pi,\delta} = \{\pi, \delta, 1 - \pi, 1 - \gamma \cdot \pi, 1 - \pi^3, 1 - \gamma \cdot \pi^3\}$. In this table α is in the first column and β is in the first row.

$(\alpha,\beta)_4 \downarrow (\pi,\delta)_4$	π	δ	$1-\pi$	$1-\gamma\pi$	$1-\pi^3$	$1-\gamma\pi^3$
π	0	1	0	0	0	0
δ	3	0	0	2	0	0
$1-\pi$	0	0	2	1	1	2
$1-\gamma\pi$	0	2	3	0	0	1
$1-\pi^3$	0	0	3	0	0	2
$1-\gamma\pi^3$	0	0	2	3	2	2

If we put $\epsilon_2 = \delta \cdot (1-\pi)^{x_2} \cdot (1-\gamma\cdot\pi)^{x_3} \cdot (1-\pi^3)^{x_4} \cdot (1-\gamma\cdot\pi^3)^{x_5}$, we derive from the table a system of linear congruences using the fact that $(\epsilon_2, z)_4 \equiv 0 \bmod 4$ for every $z \in T_{\pi,\delta}$. We have

$$\begin{aligned} 2x_3 &\equiv 0 \bmod 4 \\ 2x_2 + x_3 + x_4 + 2x_5 &\equiv 0 \bmod 4 \\ 3x_2 + x_5 &\equiv 2 \bmod 4 \\ 3x_2 + 2x_5 &\equiv 0 \bmod 4 \\ 2x_2 + 3x_3 + 2x_4 + 2x_5 &\equiv 0 \bmod 4. \end{aligned}$$

The solution is $x_2 = x_3 = x_4 = 0 \bmod 4$, and $x_5 = 2 \bmod 4$. So a strongly distinguished unit of degree two in this field is $\epsilon = \delta \cdot (1-\gamma\pi^3)^2$.

Example 6.12. Let p be a prime number, let $F = \mathbf{Q}_p(\zeta_p)$ and let $\pi = 1-\zeta_p$ be a prime element. Then F is a totally ramified extension of $\mathbf{Q}_p$ of degree $p-1$. We have $e = p-1$, $f = 1$ and a set of generators for the $F^*/(F^*)^p$ is $T_{\pi,\delta} = \{\pi, 1-\pi, 1-\pi^2, \ldots, 1-\pi^p\}$. The map $\tau_1 : U_1/U_2 \longrightarrow U_p/U_{p+1}$ is the trivial map, so the cokernel of τ_1 is generated by $\delta = 1-\pi^p$ which is a distinguished unit and also a strongly distinguished unit of degree 1.

Bibliography

[1] Arora, S. and Barak, B., *Computational Complexity.* Cambridge University Press, New York, 2009.

[2] Artin, E., *Algebraic numbers and algebraic functions.* AMS Chelsea Publishing, Providence, 2005.

[3] Bernstein, D.J., *Fast multiplication and its applications.* Cambridge University Press, Cambridge, 2008.

[4] Boer, K. de, *Computing the power residue symbol.* Master thesis, Radboud University, Nijmegen, 2016, available at `www.ru.nl/math/@1060430/algebra-topology/`.

[5] Cassels, J.W.S. and Fröhlich, A., *Algebraic number theory.* Thompson Book Company Inc., Washington D.C., 1967.

[6] Daberkow, M., *On computations in Kummer extensions.* Journal of Symbolic Computation, 31, 113–131, 2001.

[7] Fesenko I. B., Vostokov S. V., *Local fields and their extensions.* 2nd extended ed., Chapter 7, Amer. Math. Soc., 2002.

[8] Gathen, J. von zur and Gerhard, J., *Modern Computer Algebra.* Cambridge University Press, Cambridge, 2003.

[9] Hasse, H., *Zahlentheorie.* Akademie-Verlag, Berlin, 1963.

[10] Hensel, K., *Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers.* Journal für Mathematik, Bd. 146. Heft 4, 1913.

[11] Ireland, K. and Rosen, M., *A classical introduction to modern number theory.* Springer-Verlag, New York, 1990.

[12] Koblitz, N., *A course in number theory and cryptography.* Springer-Verlag, New York, 1994.

[13] Lang, S., *Algebraic Number Theory, second edition.* Springer-Verlag, New York, 1970.

[14] Milne, J.S., *Class Field Theory (v4.02).* 2013, available at `www.jmilne.org/math/`.

[15] Milnor, J.W., *Introduction to algebraic K-theory.* Princeton University Press, Princeton, 1971.

[16] Neukirch, J., *Algebraic number theory.* Springer-Verlag, Berlin, 1992.

[17] Neukirch, J., *Class field theory.* Berlin, Springer-Verlag, 1985.

[18] Neukirch, J., *Klassenkörpertheorie.* Hochschulskripten 713/713a^*, Bibliographisches Institut, Mannheim, 1969.

[19] Pagano, C. and Boer, K. de, *Calculating the power residue symbol and ibeta.* Proceedings of the International Symposium on Symbolic and Algebraic Computations, 117 - 124, 2017.

[20] Poonen, Bjorn, *Rational Points on Varieties.* Graduate studies in Mathematics 186, AMS, Providence Rhode Island, 2017.

[21] Robert, A., *A course in p-adic analysis.* Springer-Verlag, New York, 2000.

[22] Serre, J-P., *Local fields.* Springer-Verlag, New York-Berlin, 1979.

[23] Shallit, J. and Bach, E., *Algorithmic number theory.* Volume 1. MIT Press, Cambridge Massachusetts, 1997.

[24] Weiss, E., *Algebraic number theory.* McGraw-Hill Book Company, New York, 1963.

Samenvatting

1. Het Legendresymbool

In zijn “Essai sur la théorie des nombres” uit 1798 introduceerde de Franse wiskundige Legendre (1752–1833) het kwadratisch restsymbool dat ook wel Legendresymbool wordt genoemd. Dit symbool wordt voor een priemgetal $p > 2$ en een geheel getal a dat niet deelbaar is door p genoteerd als $(\frac{a}{p})$. Het symbool heeft de waarde 1 wanneer de congruentie $x^2 \equiv a \bmod p$ opgelost kan worden en de waarde -1 wanneer dit niet het geval is. Met het Legendresymbool wordt in feite een functie

$$\{a \in \mathbf{Z} : p \nmid a\} \longrightarrow \{-1, 1\}$$

gegeven die gedefinieerd wordt door

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Uit de congruentie $a^{p-1} \equiv 1 \bmod p$ volgt, dat

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \bmod p$$

dus $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ of $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Leonhard Euler (1707–1783) bewees dat beide definities gelijkwaardig zijn door aan te tonen dat de congruentie $x^2 \equiv a \bmod p$ kan worden opgelost wanneer geldt $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ en dat dit niet het geval is als $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Door zijn compactheid en de mogelijkheid om het op eenvoudige wijze aan te passen om er zo machtsrestsymbolen van hogere orde mee te noteren is het Legendresymbool een succesvolle notatie gebleken die het onderzoek naar de eigenschappen van kwadratische resten zeker heeft gestimuleerd.

We geven een voorbeeld van de berekening van een Legendresymbool. Kies $p = 17$ en bereken de kwadratische resten modulo 17. Dit zijn

$$1^2 \equiv 1 \bmod 17,\ 2^2 \equiv 4 \bmod 17,\ 3^2 \equiv 9 \bmod 17,\ 4^2 \equiv 16 \bmod 17,$$

$$5^2 \equiv 8 \bmod 17,\ 6^2 \equiv 2 \bmod 17,\ 7^2 \equiv 15 \bmod 17,\ 8^2 \equiv 13 \bmod 17.$$

De kwadraten van andere gehele getallen geven geen nieuwe kwadratische resten modulo 17, want er geldt

$$a^2 \equiv (17 - a)^2 \bmod 17$$

zodat $1^2 \equiv 16^2$, $2^2 \equiv 15^2$ enzovoorts. Een kwadratische rest modulo 17 is dus een element van de verzameling

$$R = \{1, 2, 4, 8, 9, 13, 15, 16\}.$$

Omdat 12 geen kwadratische rest is modulo 17, geldt $(\frac{12}{17}) = -1$. De congruentie $x^2 \equiv 12 \bmod 17$ heeft dan ook geen oplossing. Maar $\left(\frac{15}{17}\right) = 1$, want $15 \in R$ en de congruentie $x^2 \equiv 15 \bmod 17$ is oplosbaar. De oplossingen zijn $x \equiv 7 \bmod 17$ en $x \equiv 10 \bmod 17$.

2. Kwadratische reciprociteit

Er bestaat een verband tussen een Legendresymbool en, in zekere zin, het omgekeerde symbool. Dit verband wordt beschreven door de kwadratische reciprociteitswet en luidt als volgt:

als p en q verschillende, oneven priemgetallen zijn, dan geldt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^{-1} = \begin{cases} 1, & \text{als } p \equiv 1 \bmod 4 \text{ of } q \equiv 1 \bmod 4, \\ -1, & \text{als } p \equiv 3 \bmod 4 \text{ en } q \equiv 3 \bmod 4. \end{cases}$$

De kwadratische reciprociteitswet is een opmerkelijk resultaat, omdat het oplossen van kwadratische congruenties modulo een priemgetal p op het eerste gezicht niets te maken heeft met het oplossen van kwadratische congruenties modulo een ander priemgetal q.

De kwadratische reciprociteitswet heeft een tweetal aanvullingswetten:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{als } p \equiv 1 \bmod 4, \\ -1, & \text{als } p \equiv 3 \bmod 4, \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{als } p \equiv 1 \bmod 8 \text{ of } p \equiv -1 \bmod 8, \\ -1, & \text{als } p \equiv 3 \bmod 8 \text{ of } p \equiv -3 \bmod 8. \end{cases}$$

Legendre slaagde er niet in om een correct bewijs van de kwadratische reciprociteitswet te geven. Het eerste volledige bewijs werd in 1801 gegeven door de Duitse wiskundige Carl Friedrich Gauss (1777–1855), die in de loop der jaren zelfs op zijn minst zes verschillende bewijzen gaf.

De gevalsonderscheidingen modulo 4 en modulo 8 laten de kwadratische reciprociteitswet en zijn aanvullingswetten er niet bijzonder elegant uitzien. We kunnen hier wat aan doen door de invoering van het *Jacobisymbool* en een tweetal *normrestsymbolen*. Deze symbolen zullen ons in staat stellen alle genoemde wetten door een enkele formule uit te drukken. Een extra voordeel is dat deze herformulering ook goed werkt voor de zogenaamde “hogere” reciprociteitswetten uit de algebraïsche getaltheorie.

3. Jacobisymbolen

Voor gehele getallen $a, b \in \mathbf{Z}\backslash\{0\}$ die relatief priem zijn, kan het Jacobisymbool $\left(\frac{a}{b}\right)$ worden gedefinieerd, dat een product is van Legendresymbolen:

$$\left(\frac{a}{b}\right) = \prod_{p \text{ priem},\, p\neq 2,\, p|b} \left(\frac{a}{p}\right)^{\operatorname{ord}_p b}$$

waarbij $\operatorname{ord}_p b$ het aantal factoren p in de priemfactorisatie van b aangeeft. Dit symbool moet overigens niet verward worden met het zogenaamde Kroneckersymbool!

Het oorspronkelijke Jacobisymbool was beperkt tot het geval dat b positief en oneven is. In bovenstaande uitbreiding van het Jacobisymbool voor algemene b worden factoren 2 in b bij het product in het rechterlid genegeerd. Het is gebruikelijk om voor de uitgebreide definitie van het Jacobisymbool te kiezen, omdat de reciprociteitswet zich dan eenvoudig laat uitdrukken.

Met het Jacobisymbool kan een belangrijke uitbreiding worden gegeven aan de kwadratische reciprociteitswet en de beide aanvullingswetten. Deze wetten gelden namelijk niet alleen voor Legendresymbolen met oneven priemtallen p en q, maar ook voor Jacobisymbolen als a en b oneven zijn. Er geldt namelijk voor oneven, gehele getallen $a, b \in \mathbf{Z} \setminus \{0\}$ die copriem zijn en waarvoor bovendien geldt dat $a > 0$ of $b > 0$:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \begin{cases} 1, & \text{als } a \equiv 1 \bmod 4 \text{ of } b \equiv 1 \bmod 4, \\ -1, & \text{als } a \equiv 3 \bmod 4 \text{ en } b \equiv 3 \bmod 4. \end{cases}$$

En bovendien, als $b > 0$, dat

$$\left(\frac{-1}{b}\right) = \begin{cases} 1, & \text{als } b \equiv 1 \bmod 4, \\ -1, & \text{als } b \equiv 3 \bmod 4. \end{cases}$$

$$\left(\frac{2}{b}\right) = \begin{cases} 1, & \text{als } b \equiv 1 \bmod 8 \text{ of } b \equiv -1 \bmod 8, \\ -1, & \text{als } b \equiv 3 \bmod 8 \text{ of } b \equiv -3 \bmod 8. \end{cases}$$

We berekenen als voorbeeld het Jacobisymbool $\left(\frac{5}{24}\right)$. Omdat factoren 2 uit de priemfactorontbinding van het getal 24 worden weggelaten, geldt dat $\left(\frac{5}{24}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$, want 2 is geen kwadratische rest modulo 3. Een ander voorbeeld: $\left(\frac{7}{45}\right) = \left(\frac{7}{5}\right)^1 \cdot \left(\frac{7}{3}\right)^2 = \left(\frac{2}{5}\right) = -1$.

4. Normrestsymbolen

We gaan nu voor rationale getallen $a, b \in \mathbf{Q} \setminus \{0\}$ een tweetal normrestsymbolen definiëren, namelijk het symbool $(a, b)_\infty$ en het symbool $(a, b)_2$.

Het eerstgenoemde symbool is bijzonder eenvoudig. Schrijf $H_\infty = \mathbf{Q}_{>0}$, de verzameling van de positieve rationale getallen. Er geldt dat H_∞ een ondergroep is van $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$. De quotiëntgroep $\mathbf{Q}^*/H_\infty$ heeft precies twee elementen want $\mathbf{Q}^*$ is te schrijven als de vereniging van de twee disjuncte nevenklassen H_∞ en $-H_\infty$.

We definiëren nu het normrestsymbool $(a, b)_\infty$ voor $a, b \in \mathbf{Q}^*$ met $a \in (-1)^{a_0} \cdot H_\infty$ en $b \in (-1)^{b_0} \cdot H_\infty$ waarbij $a_0, b_0 \in \{0, 1\}$:

$$(a, b)_\infty = (-1)^{a_0 \cdot b_0}.$$

Kennelijk geldt dat:

$$(a, b)_\infty = \begin{cases} -1, & \text{als } a < 0 \text{ en } b < 0, \\ 1, & \text{anders.} \end{cases}$$

Bovendien is het symbool *bimultiplicatief.* Dit betekent dat

$$(a \cdot a', b)_\infty = (a, b)_\infty \cdot (a', b)_\infty$$

$$(a, b \cdot b')_\infty = (a, b)_\infty \cdot (a, b')_\infty$$

waarbij $a, a', b, b' \in \mathbf{Q}^*$. Ook is eenvoudig in te zien dat het symbool *symmetrisch* is:

$$(a, b)_\infty = (b, a)_\infty.$$

Met de definitie is het niet moeilijk na te gaan dat bijvoorbeeld $(3\frac{1}{2}, -5)_\infty = 1$ en dat $(-2, -\frac{1}{3})_\infty = -1$.

Het tweede normrestsymbool is op analoge wijze gedefinieerd. Dit symbool wordt voor elk tweetal elementen $a, b \in \mathbf{Q}^*$ genoteerd als $(a, b)_2$. De multiplicatieve groep $\mathbf{Q}^*$ heeft $H_2 = \{4^l \cdot \frac{1+8n}{1+8m} : l, m, n \in \mathbf{Z}\}$ als ondergroep. De quotiënt groep $\mathbf{Q}^*/H_2$ heeft precies acht elementen, want $\mathbf{Q}^*$ is te schrijven als vereniging van de disjuncte nevenklassen $(-1)^{a_1} \cdot 2^{a_2} \cdot 5^{a_3} \cdot H_2$, waarbij $a_i \in \{0, 1\}$ voor $i = 1, 2$ en 3.
Voor $a, b \in \mathbf{Q}^*$ definiëren we nu het normrestsymbool $(a, b)_2$ als volgt:
als $a \in (-1)^{a_1} \cdot 2^{a_2} \cdot 5^{a_3} \cdot H_2$ en $b \in (-1)^{b_1} \cdot 2^{b_2} \cdot 5^{b_3} \cdot H_2$ dan is

$$(a, b)_2 = (-1)^{a_1 \cdot b_1 + a_2 \cdot b_3 + a_3 \cdot b_2}.$$

Eenvoudig is in te zien dat ook dit symbool symmetrisch en bimultiplicatief is.

We geven enkele voorbeelden. Stel, we willen het normrestsymbool $(29, 14)_2$ berekenen. Er geldt $29 = 5 \cdot \frac{145}{25} \in 5 \cdot H_2$, omdat 145 en 25 elementen van H_2 zijn. Daaruit volgt dat $a_1 = a_2 = 0$ en $a_3 = 1$. Verder hebben we $14 \in -1 \cdot 2 \cdot -7 \in -1 \cdot 2 \cdot H_2$, dus $b_1 = b_2 = 1$ en $b_3 = 0$. Als we de definitie toepassen, volgt dat $(29, 14)_2 = -1$.

5. Normrestsymbolen en de kwadratische reciprociteitswet

We kunnen nu voor coprieme getallen $a, b \in \mathbf{Z} \setminus \{0\}$ de kwadratische reciprociteitswet en de beide aanvullingswetten met één enkele formule weergeven:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = (b, a)_\infty \cdot (b, a)_2.$$

We geven enkele voorbeelden. Neem $a = 29$ en $b = 14$. Er geldt $(29, 14)_\infty = 1$ en $(29, 14)_2 = -1$. Verder is $(\frac{29}{14}) = (\frac{1}{14}) = 1$ en $(\frac{14}{29}) = -1$ want eenvoudig is door berekening na te gaan dat 14 geen kwadratische rest modulo 29 is omdat de kwadratische resten modulo 29 de getallen $1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25$ en 28 zijn. Eenvoudig volgt dan de juistheid van de kwadratische reciprociteitswet in dit geval.

Als voorbeeld controleren we verder nog de tweede aanvullingswet. Stel nu dat voor het oneven priemgetal p geldt dat $p \in (-1)^{b_1} \cdot 2^{b_2} \cdot 5^{b_3} \cdot H_2$, dan onderscheiden we vier verschillende gevallen voor p en berekenen in elk van die gevallen het normrestsymbool $(p, 2)_2$. Dit geeft de onderstaande tabel.

p mod 8	b_1	b_2	b_3	$(p, 2)_2$
1	0	0	0	1
3	1	0	1	-1
5	0	0	1	-1
7	1	0	0	1.

Het resultaat is als volgt samen te vatten:

$$(p,2)_2 = \begin{cases} 1, & \text{als } p \equiv 1 \bmod 8 \text{ of } p \equiv -1 \bmod 8, \\ -1, & \text{als } p \equiv 3 \bmod 8 \text{ of } p \equiv -3 \bmod 8. \end{cases}$$

Als we nu de kwadratische reciprociteitswet toepassen, dan krijgen we

$$\left(\frac{2}{p}\right)\left(\frac{p}{2}\right)^{-1} = (p,2)_\infty \cdot (p,2)_2.$$

Omdat $\left(\frac{p}{2}\right) = \left(\frac{1}{2}\right) = 1$ en $(p,2)_\infty = 1$ volgt er dat

$$\left(\frac{2}{p}\right) = (p,2)_2.$$

6. Reëele en 2-adische getallen

De definitie van $(a,b)_\infty$ die we in paragraaf 4 gegeven hebben, hangt alleen af van het teken van a en b en kan daarom zonder verandering ook voor reëele getallen a en b ongelijk nul gegeven worden. De rol van $H_\infty = \mathbf{Q}_{>0}$ wordt dan overgenomen door $\mathbf{R}_{>0}$, die samenvalt met de verzameling kwadraten $(\mathbf{R}^*)^2$ van elementen van $\mathbf{R}^*$.

Merk op dat geldt $H_\infty = \mathbf{Q}^* \cap (\mathbf{R}^*)^2$ en dat de functie

$$\mathbf{R}^* \times \mathbf{R}^* \longrightarrow \{-1,1\}, \quad (a,b) \mapsto (a,b)_\infty$$

in de gebruikelijke topologie continu is.

Wat zojuist is gezegd voor $(a,b)_\infty$, is ook van toepassing op het symbool $(a,b)_2$, wanneer we het lichaam $\mathbf{R}$ vervangen door het lichaam van de 2-*adische getallen*, waarvan we straks de constructie zullen schetsen. Er zal dan blijken dat geldt $H_2 = \mathbf{Q}^* \cap (\mathbf{Q}_2^*)^2$ en dat $(a,b)_2$ ook gedefinieerd kan worden voor $a,b \in \mathbf{Q}_2^*$. De functie

$$\mathbf{Q}_2^* \times \mathbf{Q}_2^* \longrightarrow \{-1,1\}, \quad (a,b) \mapsto (a,b)_2$$

is dan continu in de 2-*adische topologie.*

Het lichaam $\mathbf{Q}_2$ van de 2-adische getallen wordt precies zo geconstrueerd als het lichaam $\mathbf{R}$ van de reëele getallen, namelijk door naar Cauchyrijen van rationale getallen te kijken, met als enige verschil dat Cauchyrijen nu gedefinieerd worden ten opzichte van de 2-*adische metriek*, die als volgt wordt verkregen. Definieer

$$|x|_2 = 2^{-k}$$

voor

$$x = 2^k \cdot \frac{1+2l}{1+2m} \in \mathbf{Q}^*$$

met $k,l,m \in \mathbf{Z}$, en $|0|_2 = 0$, dan is de 2-adische afstand van de rationale getallen x en y gelijk aan $|x-y|_2$. In de 2-adische metriek geldt bijvoorbeeld $\lim_{n\to\infty} 2^n = 0$. Het lichaam $\mathbf{Q}_2$ wordt de *completering* van $\mathbf{Q}$ genoemd ten opzichte van de 2-adische metriek.

7. Rekenen met 2-adische getallen

Net zoals men een reëel getal meestal door middel van zijn decimale ontwikkeling representeert, gebruikt men voor een 2-adisch getal a doorgaans een binaire schrijfwijze. Deze ziet er als volgt uit:

$$a = \sum_{n \in \mathbf{Z}} c_n 2^n$$

met alle $c_n \in \{0,1\}$, zodanig dat er een $m \in \mathbf{Z}$ is met $c_n = 0$ voor alle $n < m$. Omgekeerd definieert elke dergelijke rij $\{c_n\}_{n \in \mathbf{Z}}$ een 2-adisch getal, namelijk de limiet van

$$\sum_{n=m}^{m+h} c_n 2^n$$

voor $h \to \infty$.

Voor $a \in \mathbf{Z}_{\geq 0}$ is dit de gebruikelijke schrijfwijze van a in het tweetallig stelsel, met $c_n = 0$ voor $n < 0$ en ook voor n voldoende groot.

Voor $a = -1 = \lim_{n \to \infty}(2^n - 1)$ krijgen we

$$-1 = 1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + \ldots$$

en in het algemeen geldt voor $a \in \mathbf{Z}_{<0}$, dat $c_n = 0$ voor $n < 0$ en $c_n = 1$ voor n voldoende groot.

Elementen van $\mathbf{Q}_2$ kunnen worden opgeteld, afgetrokken en vermenigvuldigd op de manier waarop in het tweetallig stelsel wordt gerekend. Als bijvoorbeeld $c = 1 + 2 + 2^3 + 2^4 + 2^6$ en $d = 2 + 2^2 + 2^5 + 2^7$ dan is

$$c + d \equiv 1 \bmod 2^8,$$
$$c \cdot d \equiv 2 \bmod 2^8.$$

Het is ook mogelijk om door elementen van $\mathbf{Q}_2^* = \mathbf{Q}_2 \setminus \{0\}$ te delen. Daarbij kan gebruik gemaakt worden van een alternatieve staartdeling, waarbij 2-adische getallen genoteerd worden als som van machten van twee, waarvan de exponenten van links naar rechts toenemen. Een voorbeeld:

$$\frac{c}{d} = 2^{-1} + 2^2 + 2^3 + 2^5 + 2^6 \bmod 2^7.$$

Rationale getallen zijn ook 2-adische getallen en kunnen dus binair worden geschreven als een som van machten van 2. Dit kunnen er eindig veel zijn, zoals $\frac{3}{4} = 2^{-2} + 2^{-1}$, of oneindig veel, zoals

$$\frac{3}{7} = 1 - \frac{4}{7} = 1 + \frac{4}{1-8} = 1 + 4(1 + 8 + 8^2 + 8^3 + \ldots) = 1 + 2^2 + 2^5 + 2^8 + \ldots.$$

Er kan worden aangetoond dat een element van $\mathbf{Q}_2^*$ een kwadraat is, dan en slechts dan als het van de vorm

$$4^k \cdot (1 + \sum_{l \geq 3} c_l 2^l)$$

is, met $c_l \in \{0,1\}$ en $k \in \mathbf{Z}$. Uiteraard zijn machten van 4 kwadraten in $\mathbf{Q}_2$, maar ook getallen $x \in \mathbf{Q}_2^*$ waarvoor geldt dat $x \equiv 1 \bmod 8$ zijn kwadraten, en ook producten van beide. Zo is bijvoorbeeld het getal -7 een kwadraat in $\mathbf{Q}_2$, want $-7 \equiv 1 \bmod 8$.

De getallen $\sqrt{-7}$ en $-\sqrt{-7}$ behoren dus tot $\mathbf{Q}_2$. Het oplossen van de congruentie $x^2 \equiv -7 \bmod 2$ geeft $x \equiv 1 \bmod 2$. Vervolgens kan de oplossing verfijnd worden door de congruentie $x^2 \equiv -7$ op te lossen modulo hogere machten van 2. Zo vinden we $\sqrt{-7} \equiv 1+2^2+2^4+2^6+2^7 \bmod 2^8$ en $-\sqrt{-7} \equiv 1+2+2^3+2^5 \bmod 2^8$. Dit voorbeeld illustreert dat $\mathbf{Q}_2$ een ander lichaam is dan het lichaam van de reële getallen.

8. Normrestsymbolen van 2-adische getallen

De definitie van H_2 zoals we die in paragraaf 4 hebben gegeven, lijkt op de definitie van de verzameling $(\mathbf{Q}_2^*)^2$. Het is niet moeilijk om met deze beschrijving van de kwadraten in $\mathbf{Q}_2^*$ aan te tonen dat $H_2 = \mathbf{Q}^* \cap (\mathbf{Q}_2^*)^2$ en dat $\mathbf{Q}^*/H_2$ isomorf is met $\mathbf{Q}_2^*/(\mathbf{Q}_2^*)^2$. Opnieuw bevat elke nevenklasse van $\mathbf{Q}_2^*$ modulo $(\mathbf{Q}_2^*)^2$ precies één element van de vorm

$$(-1)^{a_1} \cdot 2^{a_2} \cdot 5^{a_3}$$

met alle $a_i \in \{0,1\}$. De quotiëntgroep $\mathbf{Q}_2^*/(\mathbf{Q}_2^*)^2$ heeft dus acht elementen. Daarmee is duidelijk dat het normrestsymbool $(a,b)_2$ met $a,b \in \mathbf{Q}_2^*$ kan worden gedefinieerd zoals in paragraaf 4 voor elementen van $\mathbf{Q}^*$.

We geven enkele voorbeelden van de berekening van normrestsymbolen in $\mathbf{Q}_2^*$. Voor het normrestsymbool $(a,b)_2$ met

$$a = 1 + 2^2 + 2^3 + 2^4 + \dots$$

en

$$b = 2 + 2^2 + 2^3 + 2^5 + \dots$$

geldt dat $a \in 5 \cdot H_2$ en $b \in -1 \cdot 2 \cdot H_2$.

Merk op dat bij de beantwoording van de vraag tot welke nevenklasse de elementen van $\mathbf{Q}_2^*/(\mathbf{Q}_2^*)^2$ in het normrestsymbool behoren, het niet van belang is welke termen met hogere machten van 2 in de representatie van a en b op de plaats van de puntjes staan. Het 2-adische normrestsymbool is dan ook continu in beide argumenten: wanneer a of b wordt vervangen door een 2-adisch getal dat er in de 2-adische metriek dichtbij ligt, verandert de waarde van het symbool niet.

Voor de genoemde elementen a en b geldt dat $(a_1, a_2, a_3) = (0,0,1)$ en $(b_1, b_2, b_3) = (1,1,0)$. Daaruit volgt, dat $(a,b)_2 = (-1)^{a_1 \cdot b_1 + a_2 \cdot b_3 + a_3 \cdot b_2} = -1$.

Een ander voorbeeld. Als

$$a = 1 + 2 + 2^2 + 2^5 + \dots$$

en

$$b = 2 + 2^4 + 2^9 + 2^{11} + \dots$$

dan geldt dat $a \in -1 \cdot H_2$ en $b \in 2 \cdot H_2$. Dus $(a_1, a_2, a_3) = (1,0,0)$ en $(b_1, b_2, b_3) = (0,1,0)$. Daaruit volgt $(a,b)_2 = 1$.

9. Hogere machtsrestsymbolen

In de eerste paragraaf van deze samenvatting hebben we de oplosbaarheid besproken van de kwadratische congruentie $x^2 \equiv a \bmod p$, waarbij p een oneven priemgetal is en het gehele getal a niet deelbaar is door p. De congruentie is oplosbaar wanneer het Legendresymbool $\left(\frac{a}{p}\right) = 1$ en er is geen oplossing wanneer $\left(\frac{a}{p}\right) = -1$. De waarde van het Legendresymbool is dus een oplossing van de vergelijking $x^2 = 1$. Ook kan het m-de machtsrestsymbool gedefinieerd worden, waarbij het gehele getal m groter is dan twee. De uitkomst van het m-de machtsrestsymbool is een oplossing van de vergelijking $x^m = 1$. Deze vergelijking heeft in een geschikt gekozen lichaam m verschillende oplossingen, die m-de eenheidswortels worden genoemd. De m-de eenheidswortels zijn machten van een zogenaamde primitieve m-de eenheidswortel, die we aangeven met het symbool ζ_m. De oplossingen van de vergelijking $x^m = 1$ zijn dus de elementen van

$$\{(\zeta_m)^i : i \in \mathbf{Z}, 0 \leq i \leq m-1\}.$$

Voor $m > 2$ zijn deze oplossingen niet allemaal elementen van $\mathbf{Q}$. Als we m-de machtsrestsymbolen willen definiëren waarbij $m > 2$, dan ligt het voor de hand om te rekenen in een lichaam dat niet alleen de rationale getallen maar ook de m-de eenheidswortels bevat. Zo'n lichaam is het getallenlichaam $\mathbf{Q}(\zeta_m)$.

Als voorbeeld van hogere machtsrestsymbolen kiezen we het vierde machtsrestsymbool, waarbij de vierde eenheidswortels

$$\langle \mathrm{i} \rangle = \{\mathrm{i}^k : k \in \mathbf{Z}, 0 \leq k \leq 3\}$$

de mogelijke uitkomsten zijn.

De getallen die in het vierde machtsrestsymbool voorkomen, zijn getallen uit de zogenaamde ring van gehelen $\mathbf{Z}[\mathrm{i}] = \{a + b \cdot \mathrm{i}; a, b \in \mathbf{Z}\}$ van het lichaam $\mathbf{Q}(\mathrm{i})$. Wanneer $P = (\pi)$ een priemideaal is van de ring $\mathbf{Z}[\mathrm{i}]$, met π een irreducibel element, dan definieert men de norm van P, die genoteerd wordt als $N(P)$, als het aantal elementen van de eindige quotiëntring $\mathbf{Z}[\mathrm{i}]/P$. Er geldt dat $N(P) = \pi \cdot \bar{\pi}$ waarbij $\bar{\pi}$ de geconjugeerde is van π.

Het lichaam waarin we werken is

$$\mathbf{Q}(\mathrm{i}) = \{a + b \cdot \mathrm{i}; a, b \in \mathbf{Q}\}.$$

Het vierde machtsrestsymbool is voor $\alpha \in \mathbf{Z}[\mathrm{i}]$ en een priemideaal $P \neq (1+i)$, waarbij bovendien geldt dat $2 \notin P$ en $\alpha \notin P$, gedefinieerd als de vierde eenheidswortel $\left(\frac{\alpha}{P}\right)_4$, waarvoor geldt

$$\left(\frac{\alpha}{P}\right)_4 \equiv \alpha^{\frac{N(P)-1}{4}} \bmod P.$$

Merk op dat deze definitie veel lijkt op de definitie van kwadratische resten uit het begin van deze samenvatting. Volgens de kleine stelling van Fermat geldt $\alpha^{N(P)-1} \equiv 1 \bmod P$, waaruit volgt voor $\alpha \notin P$ dat

$$\alpha^{N(P)-1} - 1 = \prod_{j=0}^{3} (\alpha^{\frac{N(P)-1}{4}} - \mathrm{i}^j).$$

Voor precies één waarde $j \in \{0, 1, 2, 3\}$ geldt

$$\alpha^{\frac{N(P)-1}{4}} \equiv \mathrm{i}^j \bmod P.$$

We geven een voorbeeld:

$$\left(\frac{1+\mathrm{i}}{3+2\mathrm{i}}\right)_4 \equiv (1+\mathrm{i})^{\frac{13-1}{4}} \bmod (3+2\mathrm{i})$$

want $N(3+2\mathrm{i}) = 3^2 + 2^2 = 13$. Bovendien is $\mathbf{Z}[\mathrm{i}]/(3+2\mathrm{i})$ een eindig lichaam van dertien elementen dat isomorf is met $\mathbf{Z}/13\mathbf{Z}$. Het isomorfisme stuurt $3+2\mathrm{i}$ naar 0, en $2\mathrm{i}$ naar $-3 \equiv 10 \bmod 13$ en dus i naar 5. Daaruit volgt dat 5 een vierde eenheidswortel is in $\mathbf{Z}/13\mathbf{Z}$. Het isomorfisme geeft $\overline{a+b\mathrm{i}} \to a+5b \bmod 13$ en $1+\mathrm{i} \to 6$. Daaruit volgt dat $(1+\mathrm{i})^3 \to 6^3 \equiv 8 \bmod 13$. Omdat $8 \equiv 5^3 \bmod 13$ geldt dat

$$\left(\frac{1+\mathrm{i}}{3+2\mathrm{i}}\right)_4 = \mathrm{i}^3 = -\mathrm{i}.$$

Op een analoge wijze kunnen m-de machtsrestsymbolen worden gedefinieerd voor $m > 2$, waarbij we werken in een getallenlichaam $K \supset \mathbf{Q}(\zeta_m)$.

10. Hogere normrestsymbolen

In de vorige paragraaf gaven we een voorbeeld van een m-de machtsrestsymbool waarbij $m > 2$. Er kan ook een Jacobisymbool voor hogere machtsresten worden gedefinieerd. De analogie met het Legendresymbool beperkt zich niet tot definities, maar geldt ook voor de eigenschappen van hogere machtsrestsymbolen. Zo geldt er een reciprociteitswet die een generalisatie is van de reciprociteitswet van Legendresymbolen.

Voor algemene K en m is, anders dan voor $K = \mathbf{Q}$ en $m = 2$, de reciprociteitswet van de m-de machtsrestsymbolen niet goed te formuleren zonder gebruik te maken van normrestsymbolen. Hogere normrestsymbolen zijn door Hilbert (1862–1943) uitgevonden om er zijn reciprociteitswet voor hogere machtsrestsymbolen mee te kunnen formuleren.

Normrestsymbolen worden gedefinieerd in bepaalde completeringen van een lichaam K, zoals we eerder kwadratische normrestsymbolen definieerden in completeringen van $\mathbf{Q}$ zoals $\mathbf{R}$ en $\mathbf{Q}_2$. Zulke completeringen heten *lokale lichamen* en normrestsymbolen worden dan ook gedefinieerd in lokale lichamen. De introductie van *p-adische lichamen* door Hensel (1861–1941) en de ontwikkeling van de klassenlichamentheorie door o.a. Furtwängler (1869–1940) en Takagi (1875–1960), die de reciprociteitswet voor hogere machtsrestsymbolen bewees, maakte het mogelijk om reciprociteit te formuleren in de terminologie van deze theorie.

Het belangrijkste resultaat van dit proefschrift is een algoritme om in polynomiale tijd normrestsymbolen te berekenen in een lokaal lichaam dat een geschikte eenheidswortel bevat. Het belang van de algoritme is tweeërlei. In de eerste plaats is er een theoretisch belang, namelijk dat het mogelijk is om de waarde van normrestsymbolen uit te rekenen. In de tweede plaats is de algoritme onmisbaar wanneer men de reciprociteitswet van hogere machtsrestsymbolen praktisch wil toepassen voor getallenlichamen. Koen de Boer, promovendus bij het CWI te Amsterdam, gebruikt de algoritme om er hogere machtsrestsymbolen mee te berekenen.

Net als bij berekeningen in de numerieke analyse is er bij alle algoritmen in lokale lichamen steeds weer het probleem van de precisie waarmee moet worden gerekend om een voldoende nauwkeurig en correct resultaat te krijgen. Men kan immers niet rekenen met getallen die gerepresenteerd worden door een som van oneindig veel termen, maar elementen van lokale lichamen worden meestal wel op die manier gegeven.

Een stimulans voor dit onderzoek was een stelling van Moore over zwak continue Steinbergsymbolen uit de K-theorie. Normrestsymbolen zijn dergelijke symbolen en de waarde van zulke symbolen wordt bepaald door de bimultiplicatieve eigenschap en de eigenschap dat een symbool waarvan beide argumenten som 1 hebben de waarde 1 heeft. Tenslotte is de exacte waarde van het normrestsymbool het resultaat van een normalisatie door toepassing van een stelling uit de klassenlichamentheorie. De eenvoud van deze feiten was een uitdaging om op zoek te gaan naar een algoritme die de exacte waarde van normrestsymbolen berekent in polynomiale tijd.

Dankwoord

Dit proefschrift zou niet voltooid zijn zonder de jarenlange begeleiding van mijn begeleider en copromotor prof. dr. H.W. Lenstra. De inspirerende gesprekken over wiskunde, maar ook over andere onderwerpen, die we met regelmaat hadden en die vooral de laatste jaren een grotere frequentie kenden dan daarvoor, hebben veel bijgedragen aan het tot stand komen van het uiteindelijke resultaat. Daarom ben ik hem allereerst veel dank verschuldigd. Ook mijn tweede copromotor, Michiel Kosters, wil ik van harte danken. Met zijn kritische blik, zijn inhoudelijke bijdrage en zijn deskundigheid op het gebied van computervaardigheden heeft hij, zeker in de latere fasen van het promotietraject, substantieel bijgedragen aan het succesvol afronden van het proefschrift. Ik dank ook prof. dr. R. van Luijk voor de bereidheid om mijn promotor te zijn en voor zijn bijdrage die weliswaar hoofdzakelijk de laatste fase van het promotietraject betrof, maar daarom niet minder belangrijk is. Tenslotte dank ik allen die mij morele steun hebben gegeven door met regelmaat naar mijn vorderingen te informeren en mij zo inspireerden om door te gaan. Het maken van het proefschrift was in mijn beleving een werk van Herculische afmetingen, maar, zoals een bekende spreuk zegt, een onvermoeide arbeid komt alles te boven.

Curriculum vitae

Jan Bouw werd geboren op 28 juli 1950. Na het behalen van de hoofdakte aan de Pedagogische Academie Merwerode te Dordrecht werkte hij van 1971 tot 1976 als onderwijzer en behaalde in die periode de akten Wiskunde L.O. en Wiskunde M.O.-A.Vanaf 1976 werkte hij als leraar wiskunde aan de Christelijke Scholengemeenschap De Lage Waard te Papendrecht. In 1979 behaalde hij de akte Wiskunde M.O.-B. In de periode 1984 - 1988 studeerde hij, naast zijn betrekking als leraar, wiskunde aan de Vrije universiteit te Amsterdam en behaalde in 1988 het doctoraal examen. Bovendien gaf hij van 1986 tot 1998 les aan de tweedegraads opleiding Wiskunde van de Hogeschool Holland in de lesplaats Dordrecht. Van 1998 tot 2017 schreef hij als auteur mee aan de wiskunde methode Moderne Wiskunde voor het voortgezet onderwijs. In 2003 nam hij deel aan het NWO project om leraren in de gelegenheid te stellen om onderzoek te doen. Het ingediende projectvoorstel werd gehonoreerd en onder leiding van prof. dr. H. W. Lenstra jr werd in de periode 2003 tot 2005 door hem onderzoek gedaan naar Algoritmen in de klassenlichamentheorie. Na afloop van de tweejarige periode werd een verzoek aan NWO om voortzetting van de financiering van het onderzoek, dat in 2005 nog niet was afgerond, niet gehonoreerd. In overleg met prof. Lenstra werd besloten om toch verder te gaan met het onderzoek, maar dan in de hoedanigheid van promovendus. Het werd een project van vele jaren met als uiteindelijk resultaat dit proefschrift. Sinds augustus 2014 is hij gepensioneerd als docent wiskunde.