On the computation of norm residue symbols

Bouw, J.

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 $(\pi',\pi)_p\neq1$. 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 $(\pi',\pi'')_p\neq1$ and $(\pi'',\pi)_p\neq1$, 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 ${}^rm$. 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.

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

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

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

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

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 $\phi_{\mathbf{Q}_p} \circ N_{F/\mathbf{Q}_p} = \operatorname{Res} \circ \phi_F$ where $\operatorname{Res} : \operatorname{Gal}(F(\sqrt[m]{\zeta_{p^s}})/F) \longrightarrow \operatorname{Gal}(\mathbf{Q}_p(\sqrt[m]{\zeta_{p^s}})/\mathbf{Q}_p)$ is the restriction map.

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

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 $\mathcal{D} = \{\overline{\gamma^i \pi^j} : \ 0 \le i < f, \ 0 \le j < e\} \subset \mathcal{O}_{Me}$.
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 $s \ge 1$ 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 $T = \{(i, j) \in \mathbf{Z}^2 : 0 \le j < f, 1 \le i < \frac{pe}{p-1}, p \nmid i\}$.
ii. Compute $(z, \zeta_{p^s})_p$ for $z \in Z$ and let $z' \in Z$ such that $(z', \zeta_{p^s})_p \ne 1$ (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. □