On the computation of norm residue symbols

Bouw, J.

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*

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

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 $p^r \mid\mid e/(p-1)$. 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 $M \cong \mathbf{Z}_p^{t-1} \oplus M_{\text{tor}}$ as $\mathbf{Z}_p$-modules with $M_{\text{tor}} = (b/p^s)\mathbf{Z}_p/b\mathbf{Z}_p \cong \mathbf{Z}/p^s\mathbf{Z}$.*

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 $w_{b'}^{p^{r+1}} = w_{b'}^{c'_{w_{b'}}} \prod_{t\in T_{\pi',\delta},\ t\ne w_{b'}} t^{b'_t}$ 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 $\overline{\pi'^i} \in \mathcal{O}_N$ 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 $i = 1, 2, \dots, N-1$.
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 $i = 1, \dots, \lfloor N/e \rfloor$ and set $a_\delta = 0$.
v.    Set $x_1 = x$.
vi.   For $j = 1, \dots, N-1$ 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 (π,δ,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 $\overline{\zeta_{p^s}}=\dfrac{\prod_{t\in T_{\pi',\delta,b'}}\overline{t}^{a_t/p^s}}{\overline{w_{b'}}^{p^{r+1}/p^s}}\in\mathcal{O}_{N-es}$.
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 (π,δ,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 $\overline{\zeta_{p^n}}=\dfrac{\prod_{\in T_{\pi',\delta,b'}}\overline{t}^{a_t/p^n}}{\overline{w_{b'}}^{p^{r+1}/p^n}}\in\mathcal{O}_{N-en}$.
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* $O((N\log q)^{2[+1]}+Nf^C(\log p)^{1[+1]})$.

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 $N = 7-2\cdot 2 = 3$.