On the computation of norm residue symbols

Bouw, J.

Citation

Bouw, J. (2021, May 19). *On the computation of norm residue symbols*. Retrieved from https://hdl.handle.net/1887/3176464

Author: Bouw, J.
Title: On the computation of norm residue symbols
Issue Date: 2021-05-19

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.