On Norm Residue Symbols and Conductors

Romyar T. Sharifi

April 1998

Abstract

Using the norm residue symbol and a reciprocity law of Artin-Hasse, we determine the conductors of Kummer extensions of the form $K(\sqrt[p^n]{a}, \zeta_n)/K(\zeta_n)$ for any unramified extension K of $\mathbf{Q}_p$, element $a \in K^*$ and primitive p^nth root of unity ζ_n. We are able to do this without more recent and general reciprocity laws, which were needed in earlier proofs of the case $K = \mathbf{Q}_p$.

1 Introduction

We are interested in determining the conductors of Kummer extensions of the form $K(\sqrt[p^n]{a}, \zeta_n)/K(\zeta_n)$ for an unramified extension K of $\mathbf{Q}_p$, an element $a \in K^*$ and a primitive p^nth root of unity ζ_n. These are exactly the conductors of the p^nth norm residue symbols $(a, \cdot\,)_{p^n, K(\zeta_n)}$. Using a complete explicit reciprocity law of Coleman's [1], the conductors of these symbols have been computed in the case of $K = \mathbf{Q}_p$ by Coleman and McCallum in [2] for odd primes p and by Prapavessi in [8] for $p = 2$ (see also [9]). The author has also used Coleman's method to compute the conductors for any unramified K with p odd (unpublished). The same conductors were also computed by Miki in [6] and [7] using Iwasawa's reciprocity law [5] and ramification theory. Aside from revealing certain generalizations of classical reciprocity laws, knowledge of the conductors has been used by the aforementioned authors to compute the conductors of Jacobi sum Hecke characters.

Our proof of this somewhat more general case depends nevertheless on no more than the most basic of the classical reciprocity laws of Artin and Hasse [3]. Hence, this paper could have been written in the first half of this century. We do not appeal to heavy mathematical machinery. Even the use of ramification theory is avoided for the most part, though it would perhaps shorten some arguments.

Let p be a prime number and n a positive integer. In the next two sections, we shall assume that either p is odd or $n \geq 2$, as the quadratic case is somewhat exceptional and easily handled. In the following, $(\,\cdot\,,\,\cdot\,)$ will be understood to mean the p^nth norm residue symbol for the field $K(\zeta_n)$. We denote by v the normalized additive valuation on K and by v_n the normalized additive valuation on $K(\zeta_n)$. Let $\mathcal{O}$ denote

the valuation ring of K, $\mathcal{O}_n$ the valuation ring of $K(\zeta_n)$ and $\mathfrak{p}$ and $\mathfrak{p}_n$ their maximal ideals, respectively. We let $\zeta_k = \zeta_n^{p^{n-k}}$ and $\lambda_k = 1 - \zeta_k$ for all $1 \leq k \leq n$. For $a \in K^*$, let $\mathfrak{f}(a)$ denote the conductor of $(a, \cdot\,)$. Let q be the order of the residue field of K, and let μ_{q-1} denote the set of $(q-1)$st roots of unity in K. Furthermore, for L/K Galois, let $\mathrm{Tr}_{L/K}$ denote the trace from L to K. In particular, we set $\mathrm{Tr}_n = \mathrm{Tr}_{K(\zeta_n)/\mathbf{Q}_p}$. Let $\eta \in \mu_{q-1}$ be such that $\mathrm{Tr}_{K/\mathbf{Q}_p}(\eta) \equiv 1 \bmod p$ (by lifting an element with trace 1 from the residue field of K). Finally, let φ denote the Frobenius automorphism of $K/\mathbf{Q}_p$.

2 Symbols of the Form $(\alpha, 1 - \alpha^{p^k})$

We first concern ourselves with the evaluation of symbols of the form $(\alpha, 1 - \alpha^{p^k})$ with $\alpha \in \mathfrak{p}_n$ and $1 \leq k \leq n$. Factoring $1 - \alpha^{p^k}$, we obtain

$$(\alpha, 1 - \alpha^{p^k}) = (\alpha, \prod_{j=1}^{p^k}(1 - \alpha\zeta_k^{-j})) = \prod_{j=1}^{p^k}(\zeta_k^j, 1 - \alpha\zeta_k^{-j}),$$

and so we have

$$(\alpha, 1 - \alpha^{p^k}) = (\zeta_k, \prod_{j=1}^{p^k}(1 - \alpha\zeta_k^{-j})^j). \tag{1}$$

The following law of Artin-Hasse [3, p. 94] is one of the classical laws of explicit reciprocity.

Theorem 1 (Artin-Hasse). *For $\beta \equiv 1 \bmod (\lambda_n)$ and $1 \leq k \leq n$, we have*

$$(\zeta_k, \beta) = \zeta_k^{\frac{1}{p^n}\mathrm{Tr}_n(\log \beta)} \qquad \text{for } p \text{ odd},$$
$$(\zeta_k, \beta) = \zeta_k^{\frac{1+2^{n-1}}{2^n}\mathrm{Tr}_n(\log \beta)} \qquad \text{for } p = 2 \text{ and } n \geq 2,$$

where Tr_n denotes the trace from $K(\zeta_n)$ to $\mathbf{Q}_p$ and log *denotes the logarithm defined by the usual power series.*

Let us apply the Artin-Hasse law to (1). First, we have

$$\log\big(\prod_{j=1}^{p^k}(1 - \alpha\zeta_k^{-j})^j\big) = -\sum_{i=1}^{\infty}\frac{\alpha^i}{i}\sum_{j=1}^{p^k} j\zeta_k^{-ij}. \tag{2}$$

In the case p^k divides i, we obtain merely $p^k(p^k + 1)/2$ as the sum over j. Let us assume now p^k does not divide i. We have, in fact,

$$\sum_{j=1}^{p^k} j\zeta_k^{-ij} = \zeta_k^{-i}\sum_{j=1}^{p^k} j(\zeta_k^{-i})^{j-1}, \tag{3}$$

where the latter sum is recognizable as the derivative of a geometric sum evaluated at ζ_k^{-i}. We evaluate

$$\frac{d}{dX}\left(\sum_{j=1}^{p^k} X^j\right) = \frac{d}{dX}\left(\frac{X^{p^k+1}-1}{X-1} - 1\right) = \frac{(p^k+1)X^{p^k}(X-1) - X^{p^k+1}+1}{(X-1)^2}.$$

Letting $X = \zeta_k^{-i}$, we obtain by (3) that

$$\sum_{j=1}^{p^k} j\zeta_k^{-ij} = \zeta_k^{-i}\frac{p^k}{\zeta_k^{-i}-1} = \frac{p^k}{1-\zeta_k^i}.$$

By (2), we conclude that evaluating (1) amounts to determining

$$-\frac{1+\delta}{p^n}\Big(\sum_{p^k \not| i} \mathrm{Tr}_n\big(\frac{\alpha^i}{i}\frac{1}{1-\zeta_k^i}\big) + \frac{p^k+1}{2}\sum_{p^k \mid i} \mathrm{Tr}_n(\frac{\alpha^i}{i})\Big) \bmod \mathbf{Z}_p, \tag{4}$$

where $\delta = 0$ if p is odd and $\delta = 2^{n-1}$ if $p = 2$.

Let us concentrate on evaluating the terms of the first sum in (4).

Lemma 2. *Let $\beta \in \mathcal{O}_n$ and set*

$$A_k = \frac{1}{p^n}\mathrm{Tr}_n\big(\frac{\beta}{\lambda_k}\big)$$

for $1 \le k \le n$.

a. *If p is odd or if $\beta \equiv 0 \bmod (2)$, then we have $A_k \in p^{-1}\mathbf{Z}_p$. Otherwise we have $A_k \in 4^{-1}\mathbf{Z}_2$.*

b. *If $\beta \equiv 0 \bmod (\lambda_1\lambda_k)$, then we have $A_k \in \mathbf{Z}_p$.*

c. *Let $1 \le l \le n$ and*

$$\beta = \eta\frac{\lambda_1\lambda_k}{\lambda_l}.$$

(Recall $\eta \in \mu_{q-1}$ is such that $Tr_{K/\mathbf{Q}_p}(\eta) \equiv 1 \bmod p$.) Then we have $A_k \equiv -1 \bmod p^{-1}\mathbf{Z}_p$.

Proof. Parts (a) and (b) are immediate from the fact that the different of the extension $K(\zeta_n)/\mathbf{Q}_p$ is $(p^n\lambda_1^{-1})$. For β as in part (c), we have

$$\frac{1}{p^n}\mathrm{Tr}_n\big(\frac{\eta\lambda_1}{\lambda_l}\big) = \mathrm{Tr}_{K/\mathbf{Q}_p}(\eta)\frac{1}{p^n}\mathrm{Tr}_{\mathbf{Q}_p(\zeta_n)/\mathbf{Q}_p}(1+\zeta_l+\cdots+\zeta_l^{p^{l-1}-1}) \equiv \frac{p-1}{p} \bmod \mathbf{Z}_p.$$

since the cyclotomic trace of any p-power root of unity of order at least p^2 is 0. □

We will also need the following easy lemma which gives us useful congruences for p-powers of certain elements.

Lemma 3.

a. *For $2 \leq l \leq n$, we have $\lambda_l^p \equiv \lambda_{l-1} \bmod (p)$.*

b. *We have*
$$\frac{\lambda_1^p}{p} \equiv -\lambda_1 \bmod (\lambda_1^2).$$

Proof. The first statement of part (a) is obvious from the binomial series expansion of $(1-\zeta_l)^p$. For part (b), note that $\zeta_1^i \equiv 1 \bmod (\lambda_1)$ for all i. Therefore we have

$$\frac{p}{\lambda_1^{p-1}} = \prod_{i=1}^{p-1} \frac{1-\zeta_1^i}{1-\zeta_1} = \prod_{i=1}^{p-1}(1+\zeta_1+\cdots+\zeta_1^{i-1}) \equiv (p-1)! \equiv -1 \bmod (\lambda_1),$$

where the last congruence is Wilson's theorem. □

The previous two lemmas lead to the following proposition.

Proposition 4.

a. *If $\alpha \equiv 0 \bmod (\lambda_1)$, then $(\alpha, 1-\alpha^{p^k})$ is a pth root of unity for all $1 \leq k \leq n$.*

b. *Let $1 \leq l \leq n$. If $\alpha \equiv 0 \bmod (\lambda_1\lambda_l)$, then we have $(\alpha, 1-\alpha^{p^k}) = 1$ for all $l \leq k \leq n$.*

c. *Let $1 \leq k \leq n$ and $k \leq l \leq n$, and set $\alpha = \pm\eta\lambda_1\lambda_k/\lambda_l$. Then we have that $(\alpha, 1-\alpha^{p^k}) = 1$ if and only if $k \geq 2$, or $p = 2$ and $k = l = 1$.*

d. *Let $p = 2$, $1 \leq k \leq n$ and $2 \leq l \leq n$, and set $\alpha = 4\eta/\lambda_l^2$. Then we have that $(\alpha, 1-\alpha^{2^k}) = 1$ if and only if $k \geq 2$.*

Proof. The symbols in question are evaluated using (4). We may assume throughout that $\alpha \equiv 0 \bmod (\lambda_1)$. Then $\alpha^i/i \equiv 0 \bmod (\lambda_1)$ for all $i \geq 1$ and $\alpha^i/i \equiv 0 \bmod (\lambda_1^2)$ for all $i \neq 1, p$. Part (a) now follows from Lemma 2a, and by Lemma 2b equation (4) reduces to

$$-\frac{1}{p^n}\big(\mathrm{Tr}_n\big(\frac{\alpha}{\lambda_k}\big) + \mathrm{Tr}_n\big(\frac{\alpha^p}{p\lambda_{k-1}}\big)\big) \bmod \mathbf{Z}_p \tag{5}$$

when $k \geq 2$,

$$-\frac{1}{p^n}\mathrm{Tr}_n\big(\frac{\alpha}{\lambda_1}\big) \bmod \mathbf{Z}_p \tag{6}$$

when $k = 1$ and p is odd, and

$$\frac{1}{2^n}\big(\mathrm{Tr}_n\big(\frac{\alpha}{2}\big) + \mathrm{Tr}_n\big(\frac{\alpha^2}{4}\big)\big) \bmod \mathbf{Z}_2 \tag{7}$$

when $k = 1$ and $p = 2$.

For part (b), we have $\alpha \equiv 0 \bmod (\lambda_1\lambda_k)$ and

$$\frac{\alpha^p}{p} \equiv 0 \bmod (\lambda_1\lambda_{k-1})$$

when $k > 1$. The result is then immediate from (5), (6), (7) and Lemma 2b.

For part (c), we must evaluate (5), (6) and (7). Lemma 2c tells us that the first term of each of these equations is $\mp p^{-1}$. When $k \geq 2$, there is a second term, and using Lemma 3 it is not hard to see that

$$\frac{\alpha^p}{p} \equiv \mp\eta^p \frac{\lambda_1\lambda_{k-1}}{\lambda_{l-1}} \bmod (\lambda_1^2).$$

As $\mathrm{Tr}_{K/\mathbf{Q}_p}(\eta^p) = \mathrm{Tr}_{K/\mathbf{Q}_p}(\varphi(\eta)) = \mathrm{Tr}_{K/\mathbf{Q}_p}(\eta)$, we easily see by Lemma 2b,c that this contribution is $\pm p^{-1}$. Finally, when $k = 1$ and $p = 2$, there is also a second term, but it vanishes unless $l = 1$, in which case it contributes 2^{-1}, which gives us part (c).

For part (d), we first consider $l \geq 3$. In this case $\alpha \equiv 0 \bmod (2\lambda_2)$, and so by part (b) we have that the symbol is 1 for all $2 \leq k \leq n$. Lemma 3a yields that

$$\frac{2}{\lambda_l^2} \equiv \frac{2}{\lambda_{l-1}} \bmod (2).$$

Using this to evaluate (7), it is clear that in this case (7) is congruent to the same formula with $\alpha = 4\eta/\lambda_{l-1}$, which by part (c) is nonzero. Now consider $l = 2$, in which case $\alpha = 2\eta\zeta_2$. For $k > 1$, we evaluate (5), which becomes

$$-\frac{1}{2^n}\big(\mathrm{Tr}_n\big(\eta\frac{2\zeta_2}{\lambda_k}\big) + \mathrm{Tr}_n\big(\eta^2\frac{-2}{\lambda_{k-1}}\big)\big) \equiv 2^{-1}(1+1) \equiv 0 \bmod \mathbf{Z}_2,$$

by Lemma 2c. If $k = 1$, we use (7), which is

$$-\frac{1}{2^n}\mathrm{Tr}_n(\eta\zeta_2 - \eta^2) \equiv 2^{-1} \bmod \mathbf{Z}_2,$$

and this finishes the proof. □

3 Symbols of the Form $(\alpha, 1 - a\alpha)$

We now concern ourselves with the evaluation of symbols of the form $(\alpha, 1-a\alpha)$ with $a \in \mathcal{O}$ and $\alpha \in \mathfrak{p}_n$. By letting α vary, the following simple fact becomes the key to our computations of conductors:

$$(a, 1 - a\alpha) = (\alpha, 1 - a\alpha)^{-1}. \tag{8}$$

First, we deal with the case $a \in \mathbf{Z}_p$. In $\mathbf{Z}_p[[X]]$, the polynomial $1 - aX$ may be expanded in a power series as

$$1 - aX = \prod_{i=1}^{\infty} (1 - X^i)^{\gamma_i(a)}, \tag{9}$$

with $\gamma_i(a) \in \mathbf{Z}_p$. The former power series will converge on $\mathfrak{p}_n$, and therefore we have

$$(\alpha, 1 - a\alpha) = \prod_{i=1}^{\infty} (\alpha, 1 - \alpha^i)^{\gamma_i(a)}. \tag{10}$$

It is in fact possible to determine the values of the $\gamma_i(a)$.

Lemma 5. *For each $i \geq 1$, the function $\gamma_i \colon \mathbf{Z}_p \to \mathbf{Z}_p$ defined by (9) is a polynomial*

$$\gamma_i(a) = \frac{1}{i} \sum_{d \,|\, i} \mu(d) a^{i/d},$$

where μ is the Möbius function.

Proof. Taking the negative of the logarithm of both sides of (9), we obtain

$$\sum_{n=1}^{\infty} \frac{a^n}{n} X^n = \sum_{i=1}^{\infty} \gamma_i(a) \sum_{d=1}^{\infty} \frac{X^{id}}{d} = \sum_{n=1}^{\infty} \sum_{d \,|\, n} \frac{\gamma_{n/d}(a)}{d} X^n.$$

Matching up terms of equal power, we obtain

$$a^n = \sum_{d \,|\, n} \gamma_{n/d}(a) \frac{n}{d} = \sum_{d \,|\, n} \gamma_d(a) d.$$

The result then follows immediately from the Möbius inversion formula applied to a^n viewed as a function of n [4], p. 20. □

Proposition 6. *Let $a \in \mathbf{Z}_p$.*

a. *For $\alpha \equiv 0 \bmod (\lambda_1)$, we have*

$$(\alpha, 1 - a\alpha) = \prod_{k=1}^{n} (\alpha, 1 - \alpha^{p^k})^{\gamma_{p^k}(a)}.$$

In fact, $(\alpha, 1 - \alpha^i) = 1$ unless $i = p^k$ with $1 \leq k \leq n$.

b. *Let $1 \leq l \leq n$. For $\alpha \equiv 0 \bmod (\lambda_1 \lambda_l)$, we have*

$$(\alpha, 1 - a\alpha) = \prod_{k=1}^{l-1} (\alpha, 1 - \alpha^{p^k})^{\gamma_{p^k}(a)}.$$

c. *For* $\alpha \equiv 0 \bmod (\lambda_1^2)$, *we have*

$$(\alpha, 1 - a\alpha) = 1.$$

Proof. For part (a), set $i = jp^k$ with j not divisible by p and $k \geq 0$, we have that

$$(\alpha, 1 - \alpha^i) = (\alpha^j, 1 - (\alpha^j)^{p^k})^{j^{-1}}.$$

If $k = 0$, the latter symbol is clearly 1. If $j > 1$ and $k \leq n$, then $\alpha^j \equiv 0 \bmod (\lambda_1^2)$ and so by Proposition 4b, $(\alpha, 1 - \alpha^i) = 1$. If $k > n$, then $1 - \alpha^i \equiv 0 \bmod (p^n \lambda_1 \lambda_n)$ (since $p^{n+k-1} \geq p^{2n} > p^{n-1}(n(p-1)+1)$) and so is a p^nth power. This shows again that the symbol is 1, proving part (a). Parts (b) and (c) now follow immediately by Proposition 4b. □

If $a = b\xi$ with $b \in \mathbf{Z}_p$ and $\xi \in \mu_{q-1}$ we have that $(\alpha, 1 - a\alpha) = (\xi\alpha, 1 - b\xi\alpha)$, allowing us to use Proposition 6 with α replaced by $\xi\alpha$. More generally, we wish to consider arbitrary $a \in \mathcal{O}$. The following proposition will be useful in this regard.

Proposition 7. *Let* $a \in \mathcal{O}$ *and* $\alpha \equiv 0 \bmod (\lambda_1)$.

a. *If* $b \in \mathcal{O}$ *is such that* $a \equiv b \bmod (p^2)$ *then* $(\alpha, 1 - a\alpha^i) = (\alpha, 1 - b\alpha^i)$ *for all* $i \geq 1$.

b. *We have* $(\alpha, 1 - a\alpha^i) = 1$ *unless* $i = p^k$ *with* $0 \leq k \leq n$. *Furthermore, if* $\alpha \equiv 0 \bmod (\lambda_1 \lambda_l)$ *then* $(\alpha, 1 - a\alpha^i) = 1$ *for* $i \geq p^l$.

Proof. In general, we have that $1 - f(X)$ with $f \in \mathcal{O}[[X]]$ may be expanded as a product of terms of the form $1 - c\xi X^h$ with $c \in \mathbf{Z}_p$, $\xi \in \mu_{q-1}$ and $h \geq 1$. Set $h = jp^m$ with p not dividing j. Then by Proposition 6a we have that

$$(\alpha, 1 - c\xi\alpha^h) = \prod_{k=0}^{n-m} (\varphi^{-m}(\xi)\alpha^j, 1 - (\varphi^{-m}(\xi)\alpha^j)^{p^{k+m}})^{j^{-1}\gamma_{p^k}(c)}. \tag{11}$$

Note that $(1 - aX^i)(1 - bX^i)^{-1}$ has such an expansion with all $c \equiv 0 \bmod p^2$. In this case $\gamma_{p^k}(c)$ is divisible by p for all $k \geq 0$. By Proposition 4a the symbols are all pth roots of unity, which yields part (a).

For part (b), observe that in an expansion of $1 - aX^i$ each h is a multiple of i. Unless $i = p^k$ with $0 \leq k \leq n-m$, Proposition 6a then shows that each of the symbols in (11) is 1. The second statement follows from Proposition 6b, and we remark that terms of (11) will be 1 unless $0 \leq k < l - m$. □

4 Computation of the Conductors

We are now prepared to compute the conductors. Some of the arguments involved in this simplify when $K = \mathbf{Q}_p$. The interested reader might attempt to work out this case without use of Proposition 7. We begin with the case of p odd.

Theorem 8. *Let p be an odd prime. Let $a \in K^*$ and write $a = \epsilon p^b(1+c)$ with $\epsilon \in \mu_{q-1}$, $b \in \mathbf{Z}$, and $c \in \mathfrak{p}$. Let $w = \min\{v(b), v(c)\}$. Then*

$$\mathfrak{f}(a) = \begin{cases} (p\lambda_1^2) & \text{if } w = 0, \\ (\lambda_w^2) & \text{if } 1 \leq w < n \text{ and } v(b+c) = w, \\ (\lambda_w \lambda_{w+1}) & \text{if } w < n \text{ and } v(b+c) > w, \\ (\lambda_n^2) & \text{if } w = n = v(c), \\ (1) & \text{otherwise.} \end{cases}$$

Proof. Step 1: $\mathfrak{f}(p) = (p\lambda_1^2)$.

By Proposition 6c, $\mathfrak{f}(p) \mid (p\lambda_1^2)$. Take $\alpha = \eta\lambda_1^2/\lambda_n$. By (8) and Proposition 6b we have that

$$(p, 1 - p\alpha) = (\alpha, 1 - \alpha^p)^{-\gamma_p(p)}.$$

Since Lemma 5 tells us that $\gamma_p(p) \equiv -1 \bmod p$, we have by Proposition 4c that the division is actually an equality.

Step 2: $\mathfrak{f}(1+pu) = (\lambda_1^2)$ *for* $u \in \mathcal{O}^*$.

Let $\alpha \equiv 0 \bmod (\lambda_1^2\lambda_n^{-1})$. By Proposition 7a, it suffices to check this for $u = \xi \in \mu_{q-1}$. We perform the following expansion:

$$1 - (1+p\xi)X \equiv (1-X)\prod_{i=1}^{\infty}(1 - p\xi X^i) \bmod p^2\mathbf{Z}_p[[X]].$$

Employing both parts of Propostion 7, we see that

$$(\alpha, 1 - (1+p\xi)\alpha) = (\alpha, 1 - p\xi\alpha)(\alpha, 1 - p\xi\alpha^p).$$

By expanding as in (11) and using Proposition 6b, we see that the rightmost term is 1. As the other term is $(\xi\alpha, 1 - p\xi\alpha)^{-1}$, we are reduced to Step 1.

Step 3: $\mathfrak{f}(p^p(1+pd)) = (\lambda_1^2)$ *for* $d \in \mathcal{O}$, $d \not\equiv -1 \bmod (p)$.

Assume $n \geq 2$ and let $\alpha \equiv 0 \bmod (\lambda_1\lambda_2)$. We have

$$(p^p, 1-\alpha) = (p, (1-\alpha)^p) = (\alpha, 1-p\alpha)^{-1}, \tag{12}$$

the latter equality following from Step 1. By Step 2, we have

$$(1+pd, 1-\alpha) = (\alpha, 1-(1+pd)\alpha)^{-1}. \tag{13}$$

Combining these two equations, we obtain

$$(p^p(1+pd), 1-\alpha) = (\alpha, 1-p\alpha)^{-1}(\alpha, 1-(1+pd)\alpha)^{-1}.$$

However, this equals $(\alpha, 1-(1+p(d+1))\alpha)^{-1}$ by Proposition 7a and an argument similar to that of Step 2. If $d \equiv -1 \bmod p$, the symbol is 1 by Proposition 7a. Otherwise, Step 2 yields the desired conductor.

Step 4: $\mathfrak{f}(p^p(1-p)) = (\lambda_1\lambda_2)$.

Let $n \geq 2$ and $a = p^p(1-p)$. We have that $\mathfrak{f}(a) \,|\, (\lambda_1\lambda_2)$, and we want to show this is exact. Take

$$\alpha = \eta\frac{\lambda_1\lambda_2}{\lambda_n}.$$

Equation (13) is still valid, but since $\alpha^p \not\equiv 0 \bmod (p\lambda_1^2)$, we have that (12) must be replaced by

$$(p^p, 1-\alpha) = (p, 1-p\alpha)(p, 1-\alpha^p).$$

By Proposition 6a,

$$(p^p(1-p), 1-\alpha) = (p, 1-\alpha^p)\prod_{k=1}^{n}(\alpha, 1-\alpha^{p^k})^{-\gamma_{p^k}(p)-\gamma_{p^k}(1-p)}.$$

The symbols in the product are all pth roots of unity by Proposition 4a. And the powers are easily computed using Lemma 5, yielding

$$(p^p(1-p), 1-\alpha) = (p, 1-\alpha^p)\prod_{k=2}^{n}(\alpha, 1-\alpha^{p^k})^{-1}.$$

The second term is equal to 1 by Proposition 4c. By Lemma 3,

$$\frac{\alpha^p}{p} \equiv -\eta^p\frac{\lambda_1^2}{\lambda_{n-1}} \bmod (\lambda_1^2).$$

Let $\beta = -\eta^p\lambda_1^2/\lambda_{n-1}$. Then we have

$$(p, 1-\alpha^p) = (p, 1-p\beta) = (\beta, 1-\beta^p)$$

by Proposition 6a and the fact that $\gamma_{p^k}(p) \equiv 0 \bmod p$ for all $k > 1$. The final symbol is not 1 by Proposition 4c. Hence $(p^p(1-p), 1-\alpha) \neq 1$.

Step 5: general case.

Let $a = \epsilon p^b(1+c)$. Recall that $w = \min\{v(b), v(c)\}$. It is easy to see that we are done if $w = 0$, $w = 1$, or $w > n$. So assume $1 < w \leq n$. Then $a = (a')^{p^{w-1}}$ for some a' with $\mathfrak{f}(a') = (\lambda_1^2)$ or $(\lambda_1\lambda_2)$. Then clearly

$$(a, 1-\beta) = (a', 1-\beta^{p^{w-1}})$$

for any $\beta \in \mathfrak{p}_n$. We therefore conclude that $\mathfrak{f}(a)$ divides (λ_w^2) or $(\lambda_w\lambda_{w+1})$ in the two cases, respectively, with one exception: if $w = n = v(c)$ we can only say it divides (λ_n^2). Since $K(\sqrt[p]{1-p}, \zeta_n)/K(\zeta_n)$ is not unramified, we must in fact have equality.

So assume $1 < w < n$ and take

$$\beta = \varphi^{-w+1}(\eta)\frac{\lambda_w^2}{\lambda_n} \quad \text{or} \quad \beta = \varphi^{-w+1}(\eta)\frac{\lambda_w\lambda_{w+1}}{\lambda_n},$$

in the two respective cases. Similarly, letting

$$\alpha = \eta\frac{\lambda_1^2}{\lambda_{n-w+1}} \quad \text{or} \quad \alpha = \eta\frac{\lambda_1\lambda_2}{\lambda_{n-w+1}},$$

we have $\beta^{p^{w-1}} \equiv \alpha \bmod (\lambda_1^2)$ by Lemma 3a. Thus

$$(a', 1-\beta^{p^{w-1}}) = (a', 1-\alpha).$$

The same arguments as in the previous steps with these α replacing those used to prove exactness of the conductors now yield the result. □

We finish with the case of $p = 2$. This is somewhat more complicated due to the existence of a primitive pth root of unity in K, i.e. -1. This allows an unramified quadratic extension to occur. Furthermore, certain of the Kummer extensions of K are then contained inside cyclotomic extensions, causing the results to vary with n.

Theorem 9. *Let $p = 2$. Let $a \in K^*$ and write $a = \epsilon 2^b(1+c)$ with $\epsilon \in \mu_{q-1}$, $b \in \mathbf{Z}$ and $c \in \mathfrak{p}$. Let $w = \min\{v(b), v(c)\}$. Then*

$$\mathfrak{f}(a) = \begin{cases} (8) & \text{if } w = 0, \\ (4) & \text{if } w = 1 = v(c) = n, \\ (4) & \text{if } w = 1,\ v(b+c) = 1 \text{ and } n \geq 2, \\ (2\lambda_2) & \text{if } w = 1,\ v(b+c) \geq 2 \text{ and } n \geq 3, \\ (2) & \text{if } w = 1 = v(b),\ v(c+2) = 2 \text{ and } n = 2, \\ (\lambda_{w-1}) & \text{if } 2 \leq w \leq n \text{ and } w = v(c), \\ (\lambda_w\lambda_{w+1}) & \text{if } 2 \leq w \leq n-2 \text{ and } w < v(c), \\ (\lambda_{n-1}) & \text{if } 2 \leq w = n-1 \text{ and } v(c) = n, \\ (1) & \text{otherwise.} \end{cases}$$

Proof. Step 1: $n = 1$.

Let $u \in \mathcal{O}^*$. Then $1+4u$ is either a square or its square root generates an unramified extension of K and so has conductor (1), $1+2u$ is neither a square nor does it yield an unramified extension and so has conductor (4), and 2 satisfies $(2, 1+4u) \neq 1$ for any u such that $1+4u$ is not a square and so has conductor (8). This implies the theorem when $n = 1$. In what follows, we assume $n \geq 2$.

Step 2: $\mathfrak{f}(2) = (8)$, $\mathfrak{f}(1+2u) = (4)$ *for* $u \in \mathcal{O}^*$, $\mathfrak{f}(4(1+2d)) = (4)$ *for* $d \not\equiv 1 \bmod (2)$.

These statements follow exactly as in Steps 1-3 of Theorem 8.

Step 3: $\mathfrak{f}(-4) = (2\lambda_2)$ *for* $n \geq 3$ *and* $\mathfrak{f}(-4) = (1)$ *for* $n = 2$.

This is very similar to Step 4 of Theorem 8. However, the statement of Proposition 4c requires that we make a minor adjustment. When $n = 2$, we have that $\beta = -2$ satisfies $(\beta, 1-\beta^2) = 1$. So in this case we cannot conclude from this $(-4, 1-\alpha) \neq 1$ for some $\alpha \equiv 0 \bmod (2)$. In fact, this is not the case. We remark that $(1+\zeta_2)^2 \in \mathbf{Q}_2(\zeta_2)$ is a fourth root of -4, and so we see that $\mathfrak{f}(-4) = (1)$ when $n = 2$.

Step 4: $\mathfrak{f}(1+4\xi) = (2)$ *for* $\xi \in \mu_{q-1}$.

For $\alpha \equiv 0 \bmod (2)$, we have by Propositon 7a that

$$(\alpha, 1-(1+4\xi)\alpha) = (\alpha, 1-\alpha) = 1,$$

so $\mathfrak{f}(1+4\xi) \,|\, (2)$.

Let $\alpha \equiv 0 \bmod (\lambda_2)$. Note that $1-(1+4\xi)\alpha$ can be written as a product of $1-\alpha$ and terms of the form $1-(4\xi)^i\alpha^j$ with $i, j > 0$. This can be expanded using (9) as

$$(\alpha, 1-(4\xi)^i\alpha^j) = \prod_{h=1}^{\infty} (\alpha, 1-\xi^{ih}\alpha^{jh})^{\gamma_h(4^i)}.$$

We make several observations about the terms on the right hand side. Note that $\gamma_h(4^i)$ is always even, and it is divisible by 4 if $i > 1$ or if h is odd or divisible by 4. If jh is odd, the symbol is clearly 1. If jh is even, note

$$(\alpha, 1-\xi^{ih}\alpha^{jh})^2 = (\alpha^2, 1-\xi^{ih}(\alpha^2)^{jh/2}).$$

Since $\alpha^2 \equiv 0 \bmod (2)$, this is 1 if jh is not a power of 2 greater than 2 and less than or equal 2^{n+1} by Proposition 6a. This symbol is always ± 1 by Proposition 4a, and so if $\gamma_h(4^i)$ is divisible by 4, the symbol is 1. This leaves us with $i = 1$, $h = 2$ and $j = 2^s$ with $1 \leq s \leq n$. Observing what the original product must be, we see that

$$(\alpha, 1-(1+4\xi)\alpha) = \prod_{k=2}^{n+1} (\alpha^2, 1-\xi^2\alpha^{2^k})^{-1}.$$

Let $\alpha = 2\varphi^{-1}(\eta)/\lambda_n$. Then we can apply Proposition 4d to see that the $k = 2$ term is nontrivial and is the only such term. We conclude that $\mathfrak{f}(1+4\xi) = (2)$.

Step 5: $\mathfrak{f}(2^b) = (\lambda_w\lambda_{w+1})$ *for* $w = v(b)$ *with* $2 \leq w \leq n-2$.

Let $a = 2^b$ with $w = v(b)$ such that $2 \leq w \leq n-1$. Take $\beta \equiv 0 \bmod (\lambda_w\lambda_{w+1})$. Since $a = (-4)^{b/2}$, we have by Step 3 that

$$(2^b, 1-\beta) = (-4, 1-\beta^{2^{w-1}})^{b/2^w} = 1.$$

Next take

$$\beta = \varphi^{1-w}(\eta)\frac{\lambda_w\lambda_{w+1}}{\lambda_n} \quad \text{and} \quad \alpha = \eta\frac{2\lambda_2}{\lambda_{n-w+1}}.$$

Then since $\alpha \equiv \beta^{2^{w-1}} \bmod (2\lambda_2)$, we have that

$$(2^b, 1-\beta) = (-4, 1-\alpha)^{b/2^{w-1}}.$$

As before, this is not 1 except when $w = n-1$, in which case the conductor is (1).

Step 6: $\mathfrak{f}((1+4\xi)^d) = (\lambda_{w-1})$ *for* $w = v(d)+2$ *with* $2 \le w \le n$.

Let $a = (1+4\xi)^d$ with $0 \le v(d) \le n-1$. Take $\beta \equiv 0 \bmod (\lambda_{w-1})$. Then

$$((1+4\xi)^d, 1-\beta) = (1+4\xi, 1-\beta^{2^{w-1}})^{d/2^{w-2}} = 1.$$

Next assume $w \le n$ and take

$$\beta = \varphi^{2-w}(\eta)\frac{\lambda_{w-1}}{\lambda_n} \quad \text{and} \quad \alpha = \eta\frac{2}{\lambda_{n-w+2}}.$$

Then $\alpha \equiv \beta^{2^{w-2}} \bmod (2)$, so we have

$$((1+4\xi)^d, 1-\beta) = (1+4\xi, 1-\alpha)^{d/2^{w-2}}.$$

Finally, we note that this symbol is not trivial since

$$(1+4\xi, 1-\alpha) = (1+4\xi, 1-(1+4\xi)\alpha),$$

and as in Step 4, the last symbol is not 1. When $w = n+1$, the conductor is the conductor of the Kummer extension obtained by adjoining $\sqrt{1+4\xi}$ to $\mathbf{Q}_p(\zeta_n)$. Since this extension is unramified or trivial, the conductor is (1).

Step 7: general case.

Noting that the conductors of 2^b and $(1+4\xi)^d$ are never equal unless they are (1), we have only to combine the results of the previous steps to finish the proof of the theorem. That this matches the case statement is only a matter of going down the list, which we leave to the reader. □

References

[1] R. F. Coleman, The Dilogarithm and the Norm Residue Symbol, *Bull. Soc. Math. France* **109** (1981), 373–402.

[2] R. F. Coleman and W. McCallum, Stable Reduction of Fermat Curves and Jacobi Sum Hecke Characters, *J. Reine Angew. Math.* **385** (1988), 41–101.

[3] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetz, Physica-Verlag, Würzburg, 1965.

[4] M. Ireland and K. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Springer-Verlag, New York, 1990.

[5] K. Iwasawa, On Explicit Formulas for the Norm Residue Symbol, J. Math. Soc. Japan **20** (1968), 151–165.

[6] H. Miki, On the Calculation of Certain Hilbert Norm Residue Symbols and its Application, *J. Number Theory* **50** (1995), 87–105.

[7] H. Miki, Jacobi Sums and the Hilbert Symbol for a Power of Two, *J. Math. Soc. Japan* **48** No. 2 (1996), 367–407.

[8] D. T. Prapavessi, On the Conductor of 2-adic Hilbert Norm Residue Symbols, *J. Algebra* **149** (1992), 85–101.

[9] R. T. Sharifi, Ramification Groups of Nonabelian Kummer Extensions, *J. Number Theory* **65** (1997), 105–115.

Dept. of Mathematics, The University of Chicago, 5734 S. University Ave., Chicago, IL 60637
E-mail address: sharifi@math.uchicago.edu