Ramification Groups of Nonabelian Kummer Extensions*

Romyar T. Sharifi

Department of Mathematics
The University of Chicago
5734 S. University Ave.
Chicago, IL 60637

sharifi@math.uchicago.edu

March 1996

Abstract

The reciprocity law of Coleman for the Hilbert norm residue symbol has allowed the computation of the conductors of the abelian Kummer extensions $\mathbf{Q}_p\big(\sqrt[p^n]{a}, \zeta_{p^n}\big)/\mathbf{Q}_p(\zeta_{p^n})$ with $a \in \mathbf{Q}_p$ and ζ_{p^n} a primitive p^nth root of unity for a fixed prime p and all positive integers n. From these conductors, we compute the ramification groups of the nonabelian Kummer extension $\mathbf{Q}_p\big(\sqrt[p^\infty]{\mathbf{Q}_p^\times}\big)/\mathbf{Q}_p$ obtained from adjoining to $\mathbf{Q}_p$ all p-power roots of its elements. More generally, given a similar nonabelian Kummer extension of complete discrete valuation fields, we have a method of computing its ramification groups from the conductors of the abelian Kummer extensions and knowledge of the ramification groups of the cyclotomic extensions.

1 Introduction

The availability of several explicit reciprocity laws in local class field theory has made possible the computation of the conductors of Kummer extensions of local fields containing the proper roots of unity. Given these conductors, one is able to determine the ramification groups of certain two-step metabelian extensions of local fields of characteristic 0. In particular, given a finite extension K of $\mathbf{Q}_p$, a subgroup Δ of the multiplicative group $K^\times$, and a positive integer n, we can compute the

*I would like to thank Professors Robert Coleman and Hendrik Lenstra for suggesting this problem to me.

ramification groups of the extension $K\big(\sqrt[p^n]{\Delta}\big)$ of K obtained by adjoining all the p^nth roots of elements of Δ. We shall first prove some simple theorems which make this job easier. Then, from the conductors computed by Coleman and McCallum in [2] and Prapavessi in [4][1] using the reciprocity law of Coleman in [1], we shall determine the ramification groups of the extensions $\mathbf{Q}_p\big(\sqrt[p^n]{\mathbf{Q}_p^\times}\big)/\mathbf{Q}_p$.

Let G_n denote the Galois group of $\mathbf{Q}_p\big(\sqrt[p^n]{\mathbf{Q}_p^\times}\big)/\mathbf{Q}_p$. Take $G = \varprojlim G_n$, where the inverse limit is taken with respect to the restriction maps. That is,

$$G = \mathrm{Gal}\big(\mathbf{Q}_p\big(\sqrt[p^\infty]{\mathbf{Q}_p{}^\times}\big)/\mathbf{Q}_p\big).$$

Then G^r shall denote the rth ramification group of this extension in the upper numbering. Note $G^r = \varprojlim G_n^r$, where G_n^r is the rth upper ramification group of G_n.

If p is odd, let V be the unit group of $\mathbf{Z}_p$. If $p = 2$, set $V = \sqrt{U_2}$, where U_2 is the set of units of $\mathbf{Z}_2$ which are congruent to 1 modulo 4. Then we have the following subgroups of G:

$$G(i,j,k) = \mathrm{Gal}\big(\mathbf{Q}_p\big(\sqrt[p^\infty]{\mathbf{Q}_p{}^\times}\big)/\mathbf{Q}_p\big(\zeta_{p^i}, \sqrt[p^j]{V}, \sqrt[p^k]{(1-p)p^p}\big)\big)$$

where i,j,and k are natural numbers[2] and ζ_{p^i} denotes a primitive p^ith root of unity. We obtain the following result in Section 3 for odd p and in Section 4 for $p = 2$.

Theorem 1. *Let $r \geq -1$. Then*

$$G^r = \begin{cases} G & \text{if } r = -1, \\ G(0,0,0) & \text{if } -1 < r \leq 0 \\ G(1,0,0) & \text{if } 0 < r \leq \frac{1}{p-1}, \\ G(i,i,i) & \text{if } i - 1 + \frac{1}{p-1} < r \leq i, \qquad i \geq 1, \\ G(i+1,i,i) & \text{if } i < r \leq i + \frac{1}{p(p-1)}, \qquad i \geq 1, \\ G(i+1,i,i+1) & \text{if } i + \frac{1}{p(p-1)} < r \leq i + \frac{1}{p-1}, \quad i \geq 1. \end{cases}$$

2 Kummer Theory

We now study the ramification groups of nonabelian Kummer extensions of complete discrete valuation fields. Our primary interest is in local fields. Take a local field F of characteristic not equal to a prime p. Assume for a moment that F is <u>not</u> a finite extension of $\mathbf{Q}_p$ and look at an extension of it by the p^nth roots of some subgroup of $F^\times$. Then we easily see that its ramification groups are trivial beyond the 0th group [3, Ch. 2]. Hence, when we later study $F = \mathbf{Q}_p$, we shall interest ourselves only with the wildly ramified case of adjoining to it the p^nth roots of elements of $\mathbf{Q}_p^\times$.

[1] Two corrections to [4] are supplied in an appendix to this paper.

[2] We remark that there are some equalities among the differently labeled $G(i,j,k)$'s and that these equalities differ in the two cases p odd and $p = 2$.

Let p be a prime number and K a complete discrete valuation field with characteristic prime to p. Given a nonnegative integer n, we let μ_{p^n} denote the group of p^nth roots of unity in the algebraic closure $\overline{K}$ of K. In μ_{p^n} we fix a primitive p^nth root of unity ζ_{p^n}. For a subgroup Δ of $K^\times$, we define $\sqrt[p^n]{\Delta} = \{x \in \overline{K} \mid x^{p^n} \in \Delta\}$.

We refer the reader to [3, Ch. 7] or [5, Chs. IV and XV] for definitions and properties of the objects for which we supply notations in this paragraph. For K and n as above, let $\mathfrak{p}_n$ denote the maximal ideal of the valuation ring of $K(\zeta_{p^n})$. Then given $a \in K^\times$, we will let $f = f_n(a)$ denote the unique nonnegative integer such that $\mathfrak{p}_n^f$ is the conductor of the extension $K\big(\zeta_{p^n}, \sqrt[p^n]{a}\big)/K(\zeta_{p^n})$. For a finite Galois extension L/K with Galois group G, we let G^r denote the rth upper ramification group for all real numbers $r \geq -1$. The map $\psi_{L/K}$ will denote the increasing function which takes the upper numbering of the ramification groups to the lower numbering.

Now fix a subgroup Δ of $K^\times$. For $n \geq 0$ set $G_n = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Delta}\big)/K\big)$ and $N_n = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Delta}\big)/K(\zeta_{p^n})\big)$. Define $\Delta_{n,r} = \{a \in \Delta \mid f_n(a) - 1 < r\}$ for real $r > -1$. Set $\Delta_{n,-1} = \Delta \cap K(\zeta_{p^n})^{\times p^n}$.

We begin with the following theorem.

Theorem 2. *For $r \geq -1$ we have $N_n^r = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Delta}\big)/K\big(\sqrt[p^n]{\Delta_{n,r}}\big)\big)$.*

Proof. Let us drop the subscript n from the notation and deal only with the nontrivial case $r > -1$. Set $I = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Delta_r}\big)/K(\zeta_{p^n})\big)$. For $a \in \Delta_r$, we let

$$H = H(a) = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Delta_r}\big)/K\big(\zeta_{p^n}, \sqrt[p^n]{a}\big)\big),$$
$$H' = H'(a) = \mathrm{Gal}\big(K\big(\zeta_{p^n}, \sqrt[p^n]{a}\big)/K(\zeta_{p^n})\big).$$

Then

$$I^r H/H = (I/H)^r = H'^r = 1,$$

since $f(a) - 1 < r$. Hence $I^r \subset H(a)$ for all $a \in \Delta_r$, which means $I^r = 1$. Set $J = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Delta}\big)/K\big(\sqrt[p^n]{\Delta_r}\big)\big)$. We have

$$N^r J/J = (N/J)^r = I^r = 1,$$

or $N^r \subset J$.

Since $I = N/J$, we have $N/N^r = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Gamma}\big)/K(\zeta_{p^n})\big)$ where we can choose $\Delta_r \subset \Gamma \subset \Delta$ by Kummer theory. For $a \in \Gamma$ set $M = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Delta}\big)/K\big(\zeta_{p^n}, \sqrt[p^n]{a}\big)\big)$. Then $N^r \subset M$, so $H' = H'(a)$ as above satisfies $H'^r = N^r M/M = 1$, which means $a \in \Delta_r$. Hence $\Delta_r = \Gamma$, or $N^r = J$. □

For any integer $n \geq 0$ let $A_n = \mathrm{Gal}\big(K(\zeta_{p^n})/K\big)$. Let $\psi_n = \psi_{K(\zeta_{p^n})/K}$. Then for $r \geq -1$ we define $\Delta_n^r \leq K^\times$ by $\Delta_n^r = \Delta_{n,\psi_n(r)}$.

Lemma 3. *For $r \geq -1$ such that $A_n^r = 1$ we have*

$$G_n^r = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Delta}\big)/K\big(\sqrt[p^n]{\Delta_n^r}\big)\big).$$

Proof. We drop the subscript n from the notation. As a property of the upper numbering of ramification groups, we have

$$G^r N/N = A^r \tag{1}$$

Setting $\psi' = \psi_{K(\sqrt[p^n]{\Delta})/K}$, we also have an equality with ramification groups in the lower numbering

$$N_{\psi'(r)} = G_{\psi'(r)} \cap N.$$

Its equivalent formulation in the upper numbering reads

$$N^{\psi(r)} = G^r \cap N. \tag{2}$$

Since $A^r = 1$, we have that $G^r \cap N = G^r$, so by Theorem 2 we conclude that $K\big(\sqrt[p^n]{\Delta^r}\big)$ is the fixed field of G^r, proving the lemma. □

Now let

$$i(n,r) = \max\{0 \le i \le n \mid A_n^r \subset \mathrm{Gal}\big(K(\zeta_{p^n})/K(\zeta_{p^i})\big)\}. \tag{3}$$

Note that if for some $k \ge 0$ we have $\mu_{p^k} \subset K$, then $i(n,r) \ge k$. Let L_n^r denote the fixed field of $N_n^{\psi_n(r)}$.

Theorem 4. *Let $r \ge -1$ be such that $A_n^r = \mathrm{Gal}\big(K(\zeta_{p^n})/K(\zeta_{p^i})\big)$ for $i = i(n,r)$. If $L_n^r = L_i^r(\zeta_{p^n})$, then the fixed field of G_n^r is L_i^r. That is,*

$$G_n^r = \mathrm{Gal}\big(K\big(\sqrt[p^n]{\Delta}\big)/K\big(\sqrt[p^i]{\Delta_i^r}\big)\big).$$

Proof. The last statement is clearly equivalent to the first by Theorem 2. Furthermore, by Lemma 3 the theorem is already proven in the case $i = n$. So assume $i < n$. Let F denote the fixed field of G_n^r. Note that our assumption on r implies by (1) and (3) that $F \cap K(\zeta_{p^n}) = K(\zeta_{p^i})$ and $\zeta_{p^{i+1}} \notin F$. Since (2) yields $F \subset L_n^r = L_i^r(\zeta_{p^n})$, we have that if $L_i^r \subset F$ then $L_i^r = F$.

Let $B = \mathrm{Gal}\big(K(\zeta_{p^n})/K(\zeta_{p^i})\big)$. Then for $s \ge -1$ we have $A_i^s = A_n^s B/B$, which implies that $i(i,s) = \min\{i, i(n,s)\}$. In particular $i(i,r) = i$. Hence we can apply Lemma 3 to see that the fixed field of G_i^r is L_i^r. Then, letting M be such that $G_n/M = G_i$, we have $G_n^r M/M = G_i^r$, and so $L_i^r \subset F$. □

Note that the condition on r in the above theorem holds whenever p is odd and $i = i(n,r) \ge 1$ or $p = 2$ and $i \ge 2$. This is a basic result in group theory upon recalling $A_n \hookrightarrow (\mathbf{Z}/p^n\mathbf{Z})^*$.

3 Ramification Groups for p odd

Now let p be an odd prime and take the field K to be $\mathbf{Q}_p$. Let $\mathfrak{p}$ denote the maximal ideal of the ring of integers $\mathbf{Z}_p[\zeta_{p^n}]$ of $\mathbf{Q}_p(\zeta_{p^n})$. Then for $a \in \mathbf{Q}_p^\times$ we let $f_n(a)$ denote the nonnegative integer such that $\mathfrak{p}^{f_n(a)}$ is the conductor of the extension $\mathbf{Q}_p\big(\zeta_{p^n}, \sqrt[p^n]{a}\big)/\mathbf{Q}_p(\zeta_{p^n})$. Let v_p denote the p-adic valuation of $\mathbf{Q}_p$. We have the following theorem [2]:

Theorem 5 (Coleman). *Let p be an odd prime number. Let $a \in \mathbf{Q}_p^\times$, and write $a = \xi p^b (1-p)^c$ with $\xi \in \mu_{p-1}$, $b \in \mathbf{Z}$, and $c \in \mathbf{Z}_p$. Let $u = \min\{v_p(b), v_p(c)+1\}$. Then*

$$f_n(a) = \begin{cases} p^{n-u-1}(p+1) & \text{if } u = 0, \text{ or } u < n \text{ and } v_p(b-pc) > u, \text{ else :} \\ 2p^{n-u} & \text{if } 1 \le u < n \text{ or } u = n = v_p(c)+1, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\Delta = \langle 1-p, p\rangle$. Note that $\mathbf{Q}_p\big(\sqrt[p^n]{\Delta}\big) = \mathbf{Q}_p\big(\sqrt[p^n]{\mathbf{Q}_p^\times}\big)$. For $j \ge 0$, let $V_j = \langle (1-p)^{p^j}\rangle$ and $W_j = \langle (1-p)^{p^j} p^{p^{j+1}}\rangle$. From Theorem 5 we have

$$\Delta_r = \begin{cases} \Delta^{p^n} & \text{if } -1 \le r \le 1, \\ V_{n-i}W_{n-i} & \text{if } 2p^{i-1}-1 < r \le p^{i-1}(p+1)-1, \quad 1 \le i \le n, \\ V_{n-i}W_{n-i-1} & \text{if } p^{i-1}(p+1)-1 < r \le 2p^i - 1, \quad 1 \le i < n, \\ \Delta & \text{if } p^{n-1}(p+1)-1 < r, \end{cases}$$

where Δ_r is the $\Delta_{n,r}$ of Theorem 2.

Set $N = \mathrm{Gal}\big(\mathbf{Q}_p(\sqrt[p^n]{\mathbf{Q}_p^\times})/\mathbf{Q}_p(\zeta_{p^n})\big)$. We define certain subgroups of N by

$$N(j,k) = \mathrm{Gal}\big(\mathbf{Q}_p\big(\sqrt[p^n]{\mathbf{Q}_p{}^\times}\big)/\mathbf{Q}_p\big(\zeta_{p^n}, \sqrt[p^j]{1-p}, \sqrt[p^k]{(1-p)p^p}\big)\big)$$

for j and k satisfying $0 \le j,k \le n$. We can now write down the ramification groups of N. For $r \ge -1$,

$$N^r = \begin{cases} N & \text{if } -1 \le r \le 1, \\ N(i,i) & \text{if } 2p^{i-1}-1 < r \le p^{i-1}(p+1)-1, \quad 1 \le i \le n, \\ N(i+1,i) & \text{if } p^{i-1}(p+1)-1 < r \le 2p^i - 1, \quad 1 \le i < n, \\ 1 & \text{if } p^{n-1}(p+1)-1 < r. \end{cases}$$

Note that the function $\psi_n = \psi_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p}$ is given by

$$\psi_n(r) = \begin{cases} r & \text{if } -1 \le r \le 0, \\ p^{i-1}(1+(p-1)(r-i+1))-1 & \text{if } i-1 < r \le i, \quad 1 \le i < n, \\ p^{n-1}(1+(p-1)(r-n+1))-1 & \text{if } n-1 < r, \end{cases} \tag{4}$$

where furthermore $i(n,r) = \min\{\lceil r \rceil, n\}$ for $r > -1$ and the condition on r of Theorem 4 is satisfied. This follows for instance from Proposition 7.10 of [3, p. 109]. We then have

$$N^{\psi_n(r)} = \begin{cases} N & \text{if } -1 \le r \le \frac{1}{p-1}, \\ N(i,i) & \text{if } i-1+\frac{1}{p-1} < r \le i+\frac{1}{p(p-1)}, \quad 1 \le i < n, \\ N(i+1,i) & \text{if } i+\frac{1}{p(p-1)} < r \le i+\frac{1}{p-1}, \quad 1 \le i < n, \\ N(n,n) & \text{if } n-1+\frac{1}{p-1} < r \le n+\frac{1}{p-1}, \\ 1 & \text{if } n+\frac{1}{p-1} < r. \end{cases}$$

Let $G_n = \mathrm{Gal}\big(\mathbf{Q}_p\big(\sqrt[p^n]{\overline{\mathbf{Q}_p^{\times}}}\big)/\mathbf{Q}_p\big)$ and let

$$G_n(i,j,k) = \mathrm{Gal}\big(\mathbf{Q}_p\big(\sqrt[p^n]{\overline{\mathbf{Q}_p{}^{\times}}}\big)/\mathbf{Q}_p\big(\zeta_{p^i}, \sqrt[p^j]{V}, \sqrt[p^k]{(1-p)p^p}\big)\big), \tag{5}$$

where i,j,and k range from 0 to n and V denotes the unit group of $\mathbf{Z}_p$. Applying Theorem 4 to G_n, we obtain the following ramification groups.

Theorem 6. *Let $r \ge -1$. Then*

$$G_n^r = \begin{cases} G_n & \text{if } -1 \le r \le 0, \\ G_n(1,0,0) & \text{if } 0 < r \le \frac{1}{p-1}, \\ G_n(i,i,i) & \text{if } i-1+\frac{1}{p-1} < r \le i, \quad 1 \le i < n, \\ G_n(i+1,i,i) & \text{if } i < r \le i+\frac{1}{p(p-1)}, \quad 1 \le i < n, \\ G_n(i+1,i,i+1) & \text{if } i+\frac{1}{p(p-1)} < r \le i+\frac{1}{p-1}, \quad 1 \le i < n, \\ G_n(n,n,n) & \text{if } n-1+\frac{1}{p-1} < r \le n+\frac{1}{p-1}, \\ 1 & \text{if } n+\frac{1}{p-1} < r. \end{cases}$$

The groups of Theorem 1 are now the inverse limits of these G_n^r with respect to n. We remark that if $\mathbf{Q}_p$ is replaced by any (finite) unramified extension K of $\mathbf{Q}_p$ and V by the unit group of the valuation ring of K in equation (5), then one can show by computing the necessary conductors that Theorem 6 holds with these changes and hence so does Theorem 1.

4 Ramification Groups for $p = 2$

We now let $p = 2$ and keep the notations for conductors $f_n(a)$ and the 2-adic valuation v_2. We have the following theorem, which is a corrected form of that in [4] (see Appendix).

Theorem 7 (Prapavessi). *Let $a \in \mathbf{Q}_2^\times$, and write $a = \xi 2^b(-3)^c$ with $\xi = \pm 1$, $b \in \mathbf{Z}$, and $c \in \mathbf{Z}_2$. Let $u = \min\{v_2(b), v_2(c)+2\}$. If $\xi = 1$ then*

$$f_n(a) = \begin{cases} 3\cdot 2^{n-1} & \text{if } u = 0, \\ 2^n & \text{if } u = 1 \text{ and } n \geq 2, \\ 2^{n-u+1} & \text{if } 2 \leq u \leq n \text{ and } u = v_2(c)+2, \\ 3\cdot 2^{n-u-1} & \text{if } 2 \leq u \leq n-2 \text{ and } u \leq v_2(c)+1, \\ 2 & \text{if } 2 \leq u = n-1 \text{ and } u = v_2(c)+1, \\ 0 & \text{otherwise.} \end{cases}$$

If $\xi = -1$ then

$$f_n(a) = \begin{cases} 3\cdot 2^{n-1} & \text{if } u = 0, \\ 3\cdot 2^{n-2} & \text{if } u = 1 \text{ and } n \geq 3, \\ 0 & \text{if } u = 1,\ n = 2, \text{ and } v_2(c) \geq 1, \\ 2 & \text{if } u = 1,\ n = 2, \text{ and } v_2(c) = 0, \text{ or} \\ & \text{if } u = 1 \text{ and } n = 1, \\ 2^n & \text{if } u \geq 2. \end{cases}$$

Take $\Delta = \langle -1, 3, 2\rangle$. Then $\mathbf{Q}_2\big(\sqrt[2^n]{\Delta}\big) = \mathbf{Q}_2\big(\sqrt[2^n]{\mathbf{Q}_2^\times}\big)$. From Theorem 7 we have

$$\Delta_{1,r} = \begin{cases} \Delta^2 & \text{if } r = -1, \\ \langle -3, 4\rangle & \text{if } -1 < r \leq 1, \\ \langle -1, 3, 4\rangle & \text{if } 1 < r \leq 2, \\ \Delta & \text{if } 2 < r \end{cases}$$

and for $n \geq 2$,

$$\Delta_{n,r} = \begin{cases} \langle 3^{2^n}, (-4)^{2^{n-2}}\rangle & \text{if } r = -1, \\ \langle 3^{2^{n-1}}, (-4)^{2^{n-2}}\rangle & \text{if } -1 < r \leq 1, \\ \langle (-3)^{2^{n-2}}, (-4)^{2^{n-2}}\rangle & \text{if } 1 < r \leq 3, \\ \langle (-3)^{2^{n-i-1}}, (-4)^{2^{n-i}}\rangle & \text{if } 2^i - 1 < r \leq 3\cdot 2^{i-1} - 1, \quad 2 \leq i < n, \\ \langle (-3)^{2^{n-i-1}}, (-4)^{2^{n-i-1}}\rangle & \text{if } 3\cdot 2^{i-1} - 1 < r \leq 2^{i+1} - 1, \quad 2 \leq i < n, \\ \langle -1, 3, 4\rangle & \text{if } 2^n - 1 < r \leq 3\cdot 2^{n-1} - 1, \\ \Delta & \text{if } 3\cdot 2^{n-1} - 1 < r. \end{cases}$$

Now take $N = \mathrm{Gal}\big(\mathbf{Q}_2\big(\sqrt[2^n]{\mathbf{Q}_2^\times}\big)/\mathbf{Q}_2(\zeta_{2^n})\big)$. Note that $\psi_n = \psi_{\mathbf{Q}_2(\zeta_{2^n})/\mathbf{Q}_2}$ satisfies equation (4) with $p = 2$. Let us define subgroups of N by

$$N(i,j) = \mathrm{Gal}\big(\mathbf{Q}_2\big(\sqrt[2^n]{\mathbf{Q}_2{}^\times}\big)/\mathbf{Q}_2\big(\zeta_{2^n}, \sqrt[2^{i+1}]{-3}, \sqrt[2^j]{-4}\big)\big)$$

for natural numbers i and j such that $i \leq n-1$ and $j \leq n$. We also define

$$N(n) = \mathrm{Gal}\big(\mathbf{Q}_2\big(\sqrt[2^n]{\mathbf{Q}_2{}^{\times}}\big)/\mathbf{Q}_2\big(\zeta_{2^{n+1}}, \sqrt[2^n]{3}, \sqrt[2^{n-1}]{2}\big)\big).$$

We see that

$$N^{\psi_n(r)} = \begin{cases} N & \text{if } r = -1, \\ N(0,0) & \text{if } -1 < r \leq 1, \\ N(1,0) & \text{if } 1 < r \leq 2, \qquad n \geq 2, \\ N(i,i) & \text{if } i < r \leq i + \frac{1}{2}, \qquad 2 \leq i < n, \\ N(i,i+1) & \text{if } i + \frac{1}{2} < r \leq i+1, \quad 2 \leq i < n, \\ N(n) & \text{if } n < r \leq n+1, \\ 1 & \text{if } n+1 < r. \end{cases}$$

Let $G_n = \mathrm{Gal}\big(\mathbf{Q}_2\big(\sqrt[2^n]{\mathbf{Q}_2^{\times}}\big)/\mathbf{Q}_2\big)$ and let

$$G_n(i,j,k) = \mathrm{Gal}\big(\mathbf{Q}_2\big(\sqrt[2^n]{\mathbf{Q}_2{}^{\times}}\big)/\mathbf{Q}_2\big(\zeta_{2^i}, \sqrt[2^{j+1}]{-3}, \sqrt[2^k]{-4}\big)\big),$$

where i, j, k are natural numbers such that $i \leq n+1$, $j \leq n-1$, and $k \leq n$. We can as in the odd case apply Theorem 4 to G_n to obtain the following ramification groups.

Theorem 8. *Let $r \geq -1$. Then*

$$G_n^r = \begin{cases} G_n & \text{if } r = -1, \\ G_n(1,0,0) & \text{if } -1 < r \leq 1, \\ G_n(2,1,2) & \text{if } 1 < r \leq 2, \qquad n \geq 2, \\ G_n(i+1,i,i) & \text{if } i < r \leq i + \frac{1}{2}, \qquad 2 \leq i < n, \\ G_n(i+1,i,i+1) & \text{if } i + \frac{1}{2} < r \leq i+1, \quad 2 \leq i < n, \\ G_n(n+1,n-1,n) & \text{if } n < r \leq n+1, \\ 1 & \text{if } n+1 < r. \end{cases}$$

Note that $G_n(2,1,2) = G_n(2,1,1)$ for $n \geq 2$ and so can be combined with the next two cases by setting $i = 1$, but we have left it separate for clarity. Taking the inverse limit over n, we obtain Theorem 1 for $p = 2$.

Appendix

We work over the field $\mathbf{Q}_2$. Following [4], we let $h = \prod_{i=1}^{2^{n-1}} [2i-1]$. Also, we set $\pi_s = 1 - \zeta_{2^s}$ for all $s \geq 1$. It was seen in Lemma 9 of [4] that for $s \leq n$ we have

$$\frac{Dh}{h}(\pi_s) \equiv 2^{n-2}\zeta_2 \bmod 2^{n-1}, \tag{6}$$

and consequently for $b \in \mathbb{Z}$ and $h^b(\pi_n) = 2^b$ we have that the k_s of Corollary 3 of [4] are

$$k_s = \begin{cases} 3 - v_2(b) & \text{if } s = 1, \\ 2^{s-1}(n + 3 - v_2(b) - s) & \text{if } s \geq 2. \end{cases}$$

From this it is seen that

$$f_n(2^b) = \begin{cases} 3 \cdot 2^{n-1} & \text{if } v_2(b) = 0, \\ 2^n & \text{if } v_2(b) = 1 \text{ and } n \geq 2. \end{cases}$$

Since $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, we have furthermore that for $n \geq 3$ and $n \leq v_2(b) + 1$ the conductor $f_n(2^b)$ is 1. This leaves only $v = v_2(b) \geq 2$ and $n > v + 1$, in which case both k_{n-v+1} and k_{n-v+2} are maximal equaling 2^{n-v+1} with the next greatest k_i being $k_{n-v} = 3 \cdot 2^{n-v-1}$. Unfortunately, Lemma 10 of [4] is incorrect, and so we recompute the conductor in this case here.

Set $s = n - v + 1$. We wish to show (compare [4, p. 96]) that for all $f \in x^k \mathbf{Z}_2[[X]]$ with $k = 3 \cdot 2^{s-2}$ we have

$$T_s\left(f(\pi_s)\frac{Dh}{h}(\pi_s)\right) + T_{s+1}\left(f(\pi_{s+1})\frac{Dh}{h}(\pi_{s+1})\right) \equiv 0 \bmod 2^{n+s-1},$$

where T_s denotes the trace from $\mathbf{Q}_2(\zeta_{2^s})$ to $\mathbf{Q}_2$. By the above remark, this will prove $f_n(2^b) = 3 \cdot 2^{n-v-1}$. Since trace is additive, we can therefore attack instead the problem of showing that

$$T_s\left(\pi_s^k\frac{Dh}{h}(\pi_s)\right) + T_{s+1}\left(\pi_{s+1}^k\frac{Dh}{h}(\pi_{s+1})\right) \equiv 0 \bmod 2^{n+s-1}$$

for all $3 \cdot 2^{s-2} \leq k < 2^s$. Note that $T_{s+1}(2^{n-1}x) \equiv 0 \bmod 2^{n+s-1}$ for all $x \in \mathbf{Z}_2[\zeta_{2^s}]$ since the different of $\mathbf{Q}_2(\zeta_{2^{s+1}})/\mathbf{Q}_2$ is (2^s). Similarly, $T_s(\pi_s^k 2^{n-1}x) \equiv 0 \bmod 2^{n+s-1}$ for $k \geq 2^{s-1}$. By (6), we then only need show that

$$T_s(\pi_s^k\zeta_2) + T_{s+1}(\pi_{s+1}^k\zeta_2) \equiv 0 \bmod 2^{s+1}$$

for $3 \cdot 2^{s-2} \leq k < 2^s$. Let us begin:

$$\begin{aligned} &T_s(\pi_s^k\zeta_2) + T_{s+1}(\pi_{s+1}^k\zeta_2) \\ &= T_s\left(\zeta_2\sum_{i=0}^{k}\binom{k}{i}(-\zeta_{2^s})^i\right) + T_{s+1}\left(\zeta_2\sum_{i=0}^{k}\binom{k}{i}(-\zeta_{2^{s+1}})^i\right) \\ &= 2^{s-1}\sum_{i\geq 0}\binom{k}{2^{s-1}i + 2^{s-2}}(-1)^{i+1} + 2^s\sum_{i\geq 0}\binom{k}{2^s i + 2^{s-1}}(-1)^{i+1}, \end{aligned}$$

where the sums are taken over i such that the denominator of the binomial coefficient is less than or equal to the numerator. Noting that $3 \cdot 2^{s-2} \leq k < 2^s$, our problem is therefore reduced to showing that

$$\binom{k}{2^{s-2}} - \binom{k}{3 \cdot 2^{s-2}} \equiv 2\binom{k}{2^{s-1}} \bmod 4$$

for all such k. One checks that if $3 \cdot 2^{s-2} \leq k < 7 \cdot 2^{s-3}$ then the coefficients on the left are -1 and 1 mod 4, respectively, both switching signs for $7 \cdot 2^{s-3} \leq k < 2^s$. Furthermore, the binomial coefficient on the right is always odd. This proves the claim, so we have in this case $f_n(2^b) = 3 \cdot 2^{n-v-1}$.

Furthermore in equation (1.1) of [4, p. 86] the third case statement must be broken up into two parts as in Theorem 7. This is the actual result of taking the smallest of two conductors as stated at the top of [4, p. 98]. Note also that we have included in the proof of Theorem 7 the classical case $n = 1$, implicitly not included in Theorem 1 of [4].

References

[1] R. F. Coleman, The Dilogarithm and the Norm Residue Symbol, *Bulletin de la Société Mathématique de France*, **109** (1981), pp. 373-402.

[2] R. F. Coleman and W. McCallum, Stable Reduction of Fermat Curves and Jacobi Sum Hecke Characters, *Journal für die reine und angewandte Mathematik*, **385** (1988), pp. 41-101.

[3] K. Iwasawa, "Local Class Field Theory," Oxford University Press, New York, 1986.

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

[5] J.-P. Serre, "Local Fields," Springer-Verlag, New York, 1979.