Canad. J. Math. Vol. **58** (3), 2006 pp. 580–599

Annihilators for the Class Group of a Cyclic Field of Prime Power Degree, II

Cornelius Greither and Radan Kučera

Abstract. We prove, for a field K which is cyclic of odd prime power degree over the rationals, that the annihilator of the quotient of the units of K by a suitable large subgroup (constructed from circular units) annihilates what we call the non-genus part of the class group. This leads to stronger annihilation results for the whole class group than a routine application of the Rubin–Thaine method would produce, since the part of the class group determined by genus theory has an obvious large annihilator which is not detected by that method; this is our reason for concentrating on the non-genus part. The present work builds on and strengthens previous work of the authors; the proofs are more conceptual now, and we are also able to construct an example which demonstrates that our results cannot be easily sharpened further.

1 Introduction and Statement of Results

In this paper we provide a generalization of the results in our paper [GK2]. We begin with a rapid overview. As in [GK2], we are concerned with a cyclic extension $K/\mathbb{Q}$ of odd prime power degree $l = p^k$; the added generality consists in replacing the hypothesis that all ramified primes in the cyclic field K have to be totally ramified by the condition that all ramified primes have full decomposition group. The main result can be described as follows (the complete statement is given in 1.3 below): Let E denote the group of units in K; fix a generator σ of the Galois group G of $K/\mathbb{Q}$. We construct a certain element $\varepsilon \in K$ by extracting a high $(\sigma - 1)$-power root from a circular unit η; in general ε will not be a unit, but $\varepsilon^{\sigma-1}$ is. We then proved in [GK2] that the $\mathbb{Z}[G]$-annihilator of $E/\langle \varepsilon^{\sigma-1} \rangle$ annihilates the p-part of $(\sigma-1)\mathcal{C}l(K)$. We will reprove it here in greater generality by a different approach.

The proof in [GK2] consisted of two stages: in the first we extracted, as said above, the deep root from a Sinnott circular unit and proved some important facts about it, and in the second stage the machinery of Thaine and Rubin was adapted to our purpose, in order to produce annihilators. This two-stage approach remains in force, but what we redo more generally in this paper is almost exclusively the first stage, by means of a more conceptual approach which comes from work of Burns and Hayward (see [H]). Not much will have to be said for the second stage because almost all that is required has already been done in [GK2].

We then conclude the paper by providing evidence that our main result would no longer be true if the assumptions are weakened further; at the very end we briefly comment on quite recent work of Burns and Hayward [BH].

Received by the editors May 9, 2004; revised February 1, 2005.

The second author was supported under Project Nr. 201/04/0381 of the Grant Agency of the Czech Republic.

AMS subject classification: 11R33, 11R20, 11Y40.

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

To explain the significance of our main result (for more details and for references, see [GK2]) we use a bit of not necessarily standard terminology. The "genus part" $\mathcal{C}l(K)_p/(\sigma-1)\mathcal{C}l(K)_p$ is completely known to us as the Galois group of the genus field of K over K. In particular it is annihilated by $(\sigma-1)$. Therefore the interesting object to be annihilated is the "non-genus part" $(\sigma-1)\mathcal{C}l(K)_p$; we succeed in finding an annihilator of this part which is in some sense best possible. If $\alpha \in \mathbb{Z}[G]$ annihilates that module, then $(\sigma-1)\alpha$ annihilates the whole of $\mathcal{C}l(K)_p$. Hence our main result and a little algebra imply that $\mathcal{C}l(K)_p$ is annihilated by the annihilator of $E/\langle\varepsilon^{(\sigma-1)^2}\rangle$. If at least three primes ramify in K, the latter annihilator is always larger than the annihilator of $E/\langle\eta^{\sigma-1}\rangle$, which is what the method of Rubin and Thaine, applied directly, would yield as an annihilator for $\mathcal{C}l(K)_p$. See the precise definition of ε in Theorem 1.1.

We now discuss our setup and our results in detail.

We suppose that $K/\mathbb{Q}$ is a cyclic extension of degree $l = p^k$, where p is an odd prime, such that the conductor m of K is not a prime power. Let χ be a generator of the group of Dirichlet characters corresponding to K. Let us decompose $\chi = \chi_{p_1}\cdots\chi_{p_s}$, where χ_{p_i} is a nontrivial Dirichlet character whose conductor is a power of a prime p_i. Let p^{k_i} be the order of χ_{p_i}. We fix an ordering of $p_1,\dots,p_s$ in such a way that $k_1 \geq \cdots \geq k_s \geq 1$, so $k_1 = k$ and $s > 1$. Hence $p_1,\dots,p_s$ are precisely the primes which ramify in K and p^{k_i} is the ramification index of p_i. Let ζ be a fixed l-th primitive root of unity and let σ be the generator of $G = \mathrm{Gal}(K/\mathbb{Q})$ satisfying $\chi(\sigma) = \zeta$ (as usual, χ is defined on G via the canonical isomorphism between $(\mathbb{Z}/m)^\times$ and the Galois group of the m-th cyclotomic field).

Let $I = \{1,\dots,s\}$. We define an $s \times s$ matrix $A = (a_{ij})_{i,j\in I}$ over $\mathbb{Z}/l\mathbb{Z}$ in the following way: the non-diagonal entries are given by the condition $\chi_{p_j}(p_i) = \zeta^{a_{ij}}$ and the diagonal entries are chosen such that the matrix A has zero row sums: $a_{ii} = -\sum_{j\in I,\, j\neq i} a_{ij}$. It is clear that the above condition is equivalent to the following one: Let K_j be the abelian field corresponding to χ_{p_j} and let σ_j be the generator of $\mathrm{Gal}(K_j/\mathbb{Q})$ determined by $\chi_{p_j}(\sigma_j) = \zeta^{q_j}$ with $q_j = lp^{-k_j}$. Then for any $i \neq j$ we have $q_j | a_{ij}$ and $\sigma_j^{a_{ij}/q_j}$ is the Frobenius automorphism of p_i in K_j.

For any $i \in I$ let ζ_i be a fixed p_i-th primitive root of unity if $p_i \neq p$ and a fixed p^{1+k_i}-th primitive root of unity if $p_i = p$. Then $\zeta_I = \prod_{i\in I}\zeta_i$ is a primitive m-th root of unity and $\eta = \mathrm{N}_{\mathbb{Q}(\zeta_I)/K}(1-\zeta_I)$ is the "Sinnott circular unit of conductor level" of K. Let $A_i \in \mathbb{Z}$ be the lift of the (i,i)-th minor of the matrix A satisfying $0 \leq A_i < l$. The first goal of this paper is the following theorem, which gives back [GK2, Theorem 1] in the case that every ramified prime of K is totally ramified:

Theorem 1.1 *There is a unique $\varepsilon \in K$ satisfying $\varepsilon^{(\sigma-1)^{s-1}} = \eta$ and having absolute norm*

$$\mathrm{N}_{K/\mathbb{Q}}(\varepsilon) = \prod_{i=1}^{s} p_i^{(-1)^{s-1}A_i}.$$

Moreover, $\varepsilon^{\sigma-1}$ is a unit of K.

This result will be proved in §4. We remark here that the cyclicity of $K/\mathbb{Q}$ is essential; for more on this see §8.

Let us mention that the existence of such an element $\varepsilon \in K$ was proved by D. Burns and A. Hayward under the assumption that the decomposition group for each of the ramified primes $p_1, \dots, p_s$ equals G (see [BH]). Theorem 1.1 may be proved by a modification of the argument in [GK2] with the following advantage: as a by-product we obtain that ε is a circular number in the m-th cyclotomic field. But we shall use the approach of Burns and Hayward since it gives a proof which is somewhat more conceptual and much less technical, see §4. It should also be pointed out that the proof presented here gives an alternative approach to the results of [GK2].

Let $l' > 1$ be a divisor of l and K' be the subfield of K of absolute degree l'. Let $\chi' = \chi^{l/l'}$, $\zeta' = \zeta^{l/l'}$, and

$$r = \max\{i \in I; q_i < l'\}.$$

Then $p_1, \dots, p_r$ are precisely the primes which ramify in K'. Let us denote $I' = \{1, \dots, r\}$ and define $\zeta_{I'} = \prod_{i \in I'} \zeta_i$ and $\eta' = \mathrm{N}_{\mathbb{Q}(\zeta_{I'})/K'}(1 - \zeta_{I'})$. Then

$$\mathrm{N}_{K/K'}(\eta) = (\eta')^{\prod_{i=r+1}^{s}(\mathrm{Frob}(p_i, K') - 1)},$$

where $\mathrm{Frob}(p_i, K')$, for $i > r$, means the Frobenius automorphism of p_i in K'. So $\mathrm{Frob}(p_i, K')$ is the restriction to K' of the Frobenius automorphism of p_i in the compositum $K_1 \cdots K_r$, which is $\prod_{j=1}^{r} \sigma_j^{a_{ij}/q_j}$. Here, by abuse of notation, we understand by σ_j the extension of the previous σ_j which is the identity on all K_t, $t \neq j$. But the restriction of σ_j to K is σ^{q_j}, so

$$\mathrm{Frob}(p_i, K') = (\sigma|_{K'})^{a_{i1} + \cdots + a_{ir}} = (\sigma|_{K'})^{-a_{ii}}$$

because $l' | a_{ij}$ for all $j > r$, $j \neq i$. Let $t_i = \sum_{c=0}^{b_i - 1} \sigma^c$, where $0 \leq b_i < l'$ is the lift of $-a_{ii}$ modulo l'. Then $\mathrm{Frob}(p_i, K') - 1$ is the restriction of $(\sigma - 1)t_i$ to K' and

$$\mathrm{N}_{K/K'}(\varepsilon)^{(\sigma-1)^{s-1}} = \left((\varepsilon')^{\prod_{i=r+1}^{s} t_i}\right)^{(\sigma-1)^{s-1}}$$

where ε' is given by Theorem 1.1 considered for K'. Notice that we have assumed in Theorem 1.1 that $s > 1$ but this remains true also for $s = 1$ (when $\varepsilon = \eta$ and $A_1 = 1$). If $0 \neq \alpha \in K$ satisfies $\alpha^{(\sigma-1)^2} = 1$, then $\alpha^{\sigma-1} = a \in \mathbb{Q}$, so $\alpha^{\sigma} = \alpha a$. Then $\alpha^{\sigma^i} = \alpha a^i$ for any positive integer i. Thus $\alpha = \alpha^{\sigma^l} = \alpha a^l$ which gives $\alpha^{\sigma-1} = a = 1$. Therefore

$$\mathrm{N}_{K/K'}(\varepsilon^{\sigma-1}) = \left((\varepsilon')^{\sigma-1}\right)^{\prod_{i=r+1}^{s} t_i}.$$

This formula can be simplified if l' divides a_{ii} for some $r < i \leq s$. Then the corresponding $t_i = 0$ and $\mathrm{N}_{K/K'}(\varepsilon^{\sigma-1}) = 1$. On the other hand, if a_{ii} is not divisible by p for each $r < i \leq s$ (which is the case if and only if the decomposition group of each of $p_{r+1}, \dots, p_s$ equals G), then all t_i are invertible in $\mathbb{Z}[G]$ and $(\varepsilon')^{\sigma-1}$ belongs to the $\mathbb{Z}[G]$-span $\langle \varepsilon^{\sigma-1} \rangle$ of $\varepsilon^{\sigma-1}$.

Now we may consider all subfields $\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_k = K$ with $[L_i : \mathbb{Q}] = p^i$. For each $1 \leq i \leq k$, let s_i be the number of ramified primes in L_i and let η_i and ε_i mean η' and ε' for $K' = L_i$. Let $\varkappa_i$ be η_i if $s_i > 1$ and $\eta_i^{\sigma-1}$ if $s_i = 1$. Then $C' = \langle -1, \varkappa_1, \dots, \varkappa_k \rangle$ is the Sinnott group of circular units of K. Let $C = \langle -1, \varepsilon_1^{\sigma-1}, \dots, \varepsilon_k^{\sigma-1} \rangle \supseteq C'$. The following technical result is going to be proved in §2:

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

Proposition 1.2 *The index of C in the full group E of units of K is given by the formula*

$$[E:C] = 2^{l-1} h_K \prod_{i=1}^{k} p^{1-s_i},$$

where h_K is the class number of K. As a consequence, the p-part of this index is equal to the cardinality of the non-genus part $(\sigma-1)\mathcal{C}l(K)_p$ of the p-Sylow subgroup $\mathcal{C}l(K)_p$ of the class group of K:

$$[E:C]_p = |(\sigma-1)\mathcal{C}l(K)_p|.$$

In the special case when the decomposition group for each of the ramified primes $p_1, \dots, p_s$ equals G (or equivalently if no ramified prime is divisible by two different prime ideals of K) we have the following generalization of [GK2, Theorem 2], provided we also retain the condition that $K/\mathbb{Q}$ is tame from [GK2]. Note that this simply means that p is not among the ramified primes $p_1, \dots, p_s$.

Theorem 1.3 *Assume that the decomposition group of any prime ramified in $K/\mathbb{Q}$ is equal to G. Then $C = \langle -1, \varepsilon^{\sigma-1} \rangle$ with ε given by Theorem 1.1. If, in addition, the extension $K/\mathbb{Q}$ is tame, then*

$$\mathrm{Ann}_R((E \otimes \mathbb{Z}_p)/\langle \varepsilon^{\sigma-1} \rangle_R) \subseteq \mathrm{Ann}_R((\sigma-1)\mathcal{C}l(K)_p),$$

where $R = \mathbb{Z}_p[G]/(\mathrm{N}_G)$ and $\mathrm{N}_G = \sum_{\sigma\in G} \sigma$ is the norm operator.

This is the central result of the present paper; the proof will be given in §5 after some preparations on Gorenstein rings (§3) and circular units (§4).

Under the same assumption as in Theorem 1.3, we can give the following easy criterion (to be proved in §6) whether the Hilbert p-class field coincides with the genus field $\overline{K}$ of K by means of the minors of the matrix A introduced before Theorem 1.1:

Proposition 1.4 *Assume that the decomposition group of any prime ramified at $K/\mathbb{Q}$ equals G. Then the non-genus part $(\sigma-1)\mathcal{C}l(K)_p$ of the p-Sylow subgroup of the class group of K is trivial if and only if at least one of the A_i $(i = 1, \dots, s)$ is not divisible by p.*

It is natural to ask whether the decomposition assumption in Theorem 1.3 and Proposition 1.4 can be removed, taking $C \otimes \mathbb{Z}_p$ instead of $\langle \varepsilon^{\sigma-1} \rangle_R$ in Theorem 1.3. The following examples and results show that this is not possible. Details of the first example below will be given in §7.

Example 1.5 There is a cyclic field K of degree 9 with three ramified primes $p_1 = 19$, $p_2 = 577$, $p_3 = 37$ such that $E/C \cong (\mathbb{Z}/3)^2$ with the trivial action of σ, while $(\sigma-1)\mathcal{C}l(K)_p \cong R/(\sigma+2)$ as R-modules. Therefore, for this field K, $(\sigma-1)$ annihilates E/C but does not annihilate $(\sigma-1)\mathcal{C}l(K)_p$. In this example, 19 and 577 are totally ramified; the prime 37 has ramification degree 3 and is totally split in the cubic subfield of K.

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

Next, in order to show that the non-decomposition hypothesis is essential in Proposition 1.4, we shall use the following observation.

Proposition 1.6 *If there is a ramified prime whose decomposition group at $K/\mathbb{Q}$ is not equal to G, then all minors A_i ($i = 1, \dots, s$) are divisible by p.*

Proof Let us assume that there is a ramified prime p_j whose decomposition group at $K/\mathbb{Q}$ is not equal to G. Let K' and K'' be the fixed fields of the inertia and decomposition groups of p_j, respectively. So $d = [K'' : \mathbb{Q}]$ is divisible by p. We have computed that

$$\mathrm{N}_{K/K'}(\varepsilon^{\sigma-1}) = \left((\varepsilon')^{\sigma-1}\right)^{\prod_{i=r+1}^{s} t_i},$$

where ε and ε' are given by Theorem 1.1 for K and K', respectively, $t_i = \sum_{c=0}^{b_i-1} \sigma^c$, and $0 \le b_i < l'$ is the lift of $-a_{ii}$ modulo $l' = [K' : \mathbb{Q}]$. We know that $d|a_{jj}$ and so $d|b_j$. Let $\nu = \sum_{c=0}^{d-1} \sigma^c$, then $t_j = \nu \cdot \sum_{c=0}^{(b_j/d)-1} \sigma^{cd}$ and we have obtained $\prod_{i=r+1}^{s} t_i = \nu t$ for a suitable $t \in \mathbb{Z}[G]$. Therefore

$$\mathrm{N}_{K/K''}(\varepsilon)^{\sigma-1} = \mathrm{N}_{K'/K''}(\varepsilon')^{(\sigma-1)\nu t} = \left(\mathrm{N}_{K'/\mathbb{Q}}(\varepsilon')^t\right)^{\sigma-1} = 1,$$

because ν acts on K'' as the absolute norm. Hence, $a = \mathrm{N}_{K/K''}(\varepsilon)$ is in $\mathbb{Q}$, and $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)= a^d$ is a p-th power in $\mathbb{Q}$. Theorem 1.1 gives that all minors A_i ($i = 1, \dots, s$) are divisible by p. ■

The following example now demonstrates that the condition concerning full decomposition groups in Proposition 1.4 may not be omitted.

Example 1.7 The class numbers of both cyclic fields of degree 9 with two ramified primes $p_1 = 19$ and $p_2 = 7$ are equal to 3, and so the Hilbert class field of either of them is equal to their common genus field, while the corresponding minors A_1 and A_2 are all divisible by 3.

The system PARI was used in checking this example. One should note that 7 splits in the cubic field of conductor 19, which is the cubic subfield of either of the degree 9 fields in the example, so the assumption of Proposition 1.4 is not satisfied here.

2 Proof of Proposition 1.2

We begin by computing the index $[C : C']$. Let r be the smallest positive integer satisfying $s_r > 1$. Then $\varepsilon_i^{\sigma-1} = \varkappa_i$ for each $i < r$. We shall prove by induction on $j = 0, 1, \dots, k$ that

$$\left[\langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_j^{\sigma-1}\rangle : \langle \varkappa_1, \dots, \varkappa_j\rangle\right] = \prod_{i=r}^{j} p^{s_i-2}.$$

The statement is clear for $j < r$. Let us suppose that $j \geq r$ and that the statement has been proved for $j-1$. Then

$$\mathrm{N}_{L_j/L_{j-1}}(\varkappa_j) \in \langle \varkappa_1, \dots, \varkappa_{j-1} \rangle \subseteq \langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_{j-1}^{\sigma-1} \rangle$$

and the previous computations give

$$\mathrm{N}_{L_j/L_{j-1}}(\varepsilon_j^{\sigma-1}) \in \langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_{j-1}^{\sigma-1} \rangle.$$

Moreover, $\varkappa_j = \varepsilon_j^{(\sigma-1)^{s_j-1}}$ and so

$$\begin{aligned} &\bigl[\langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_j^{\sigma-1} \rangle : \langle \varkappa_1, \dots, \varkappa_j \rangle\bigr] \\ &\qquad = \bigl[\langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_j^{\sigma-1} \rangle : \langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_{j-1}^{\sigma-1}, \varepsilon_j^{(\sigma-1)^{s_j-1}} \rangle\bigr] \\ &\qquad\quad \cdot \bigl[\langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_{j-1}^{\sigma-1}, \varkappa_j \rangle : \langle \varkappa_1, \dots, \varkappa_j \rangle\bigr]. \end{aligned}$$

The norm operator of L_j/L_{j-1} is $1 + \sigma^{p^{j-1}} + \cdots + \sigma^{(p-1)p^{j-1}}$. Therefore taking $\varkappa_j, \varkappa_j^{\sigma}, \dots, \varkappa_j^{\sigma^{(p-1)p^{j-1}-1}}$ together with a $\mathbb{Z}$-basis of $\langle \varkappa_1, \dots, \varkappa_{j-1} \rangle$ produces a $\mathbb{Z}$-basis of $\langle \varkappa_1, \dots, \varkappa_j \rangle$, and similarly for $\langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_{j-1}^{\sigma-1}, \varkappa_j \rangle$. Therefore the induction hypothesis gives

$$\bigl[\langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_{j-1}^{\sigma-1}, \varkappa_j \rangle : \langle \varkappa_1, \dots, \varkappa_j \rangle\bigr] = \prod_{i=r}^{j-1} p^{s_i-2}.$$

Moreover,

$$\begin{aligned} &\bigl[\langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_j^{\sigma-1} \rangle : \langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_{j-1}^{\sigma-1}, \varepsilon_j^{(\sigma-1)^{s_j-1}} \rangle\bigr] \\ &\qquad = \prod_{u=1}^{s_j-2} \bigl[\langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_{j-1}^{\sigma-1}, \varepsilon_j^{(\sigma-1)^u} \rangle : \langle \varepsilon_1^{\sigma-1}, \dots, \varepsilon_{j-1}^{\sigma-1}, \varepsilon_j^{(\sigma-1)^{u+1}} \rangle\bigr] \\ &\qquad = \prod_{u=1}^{s_j-2} \bigl|\mathbb{Z}[x]/(1-x, 1+x^{p^{j-1}}+\cdots+x^{(p-1)p^{j-1}})\bigr| = p^{s_j-2}, \end{aligned}$$

which completes the induction step.

Using Sinnott's formula for the index of the Sinnott group of circular units C' [S, Theorem 4.1, Theorem 5.3], we obtain

$$[E : C'] = 2^{l-1} \cdot \frac{p^{r-1}}{l} \cdot h_K,$$

hence

$$[E : C] = [E : C']/[C : C'] = 2^{l-1} h_K \cdot p^{r-1-k} \prod_{i=r}^{k} p_i^{2-s_i} = 2^{l-1} h_K \prod_{i=1}^{k} p^{1-s_i},$$

which was to be proved. The second statement of the proposition follows from the fact that the absolute degree of the genus field of K is $\prod_{i=1}^{k} p^{s_i}$.

3 Algebraic Preliminaries

Throughout this section, let G denote a cyclic group of order $l = p^k$ with generator σ, and let $R = \mathbb{Z}_p[G]/(\mathrm{N}_G)$.

Lemma 3.1 *The ring R is local and Gorenstein.*

Proof The group ring $\mathbb{Z}_p[G]$ is local with maximal ideal $(p, \sigma - 1)$, because p is in the radical and the factor ring $(\mathbb{Z}/p)[G]$ is local. The ring R has grade 1 since it has Krull dimension 1 and p is a nonzerodivisor. Kaplansky [Ka1, Exercise 1, p. 163] shows that every local ring of grade 1 whose maximal ideal is generated by two elements is Gorenstein. Alternatively one may also exhibit R as the quotient of a power series ring $\mathbb{Z}_p[[y]]$ by a nonzerodivisor and use [Ka1, Exercise 13, p. 164]. ■

Proposition 3.2 *Let M be any nonzero R-module without $\mathbb{Z}$-torsion and $x \in M$. Then $x \in (\sigma - 1)M$ if and only if for all $\phi \in \mathrm{Hom}_R(M, R)$ we have $\phi(x) \in (\sigma - 1)R$.*

Proof "Only if" is obvious. For "if", let us argue indirectly: let $\overline{M} = M/(\sigma - 1)M$, write $x \mapsto \overline{x}$ for the canonical map $M \to \overline{M}$, and assume that $\overline{x}$ is nonzero. The ring $\overline{R} = R/(\sigma - 1)R$ is Gorenstein and zero-dimensional, hence self-injective (the self-injectiveness of a zero-dimensional Gorenstein ring is well known and follows, *e.g.*, from [Ka2, Theorems III.12, III.20].) It is obvious that the finite ring $\overline{R}$ contains a minimal nonzero ideal I; this must be simple (*i.e.*, without proper subideal), hence cyclic, so of the form $z\overline{R}$, and I must be isomorphic to $\overline{R}/J$, where J is the maximal ideal of $\overline{R}$. So the annihilator of z is the maximal ideal J. Hence if $\overline{x}$ is not zero, the $\overline{R}$-homomorphism $f \colon R\overline{x} \to \overline{R}$ sending $\overline{x}$ to z is well-defined. By self-injectivity, f is the restriction of some $\overline{R}$-homomorphism $\phi_0 \colon \overline{M} \to \overline{R}$. Let ϕ_1 be the composite of the canonical map $M \to \overline{M}$ and ϕ_0. Then $\phi_1(x)$ is nonzero.

We claim: ϕ_1 can be lifted through the canonical surjection $\pi \colon R \to \overline{R}$, *i.e.*, there is an R-map ϕ such that $\pi\phi = \phi_1$. If this claim can be established, then $\phi(x)$ goes to $\phi_1(x) \neq 0$ under reduction modulo $(\sigma - 1)$, so $\phi(x)$ is not in $(\sigma - 1)R$, and we will be done.

Proof of claim: The sequence

$$\cdots \to \mathrm{Hom}_R(M, R) \to \mathrm{Hom}_R(M, \overline{R}) \to \mathrm{Ext}^1_R(M, (\sigma - 1)R) \to \cdots$$

is exact, and $R \cong (\sigma - 1)R$ because $(\sigma - 1)$ is a nonzerodivisor in R, so it suffices to show that $\mathrm{Ext}^1_R(M, R)$ is zero. This follows from [Ka1, Theorem 217]: we put $A = R$ and $B = M$ and we recall that the grade $G(M)$ is the length of a maximal R-sequence $x_1, \dots, x_g \in \mathrm{Rad}(R)$ on M. Here everything is rather simple: M has grade 1 since it is nonzero and has no $\mathbb{Z}$-torsion, and $n = G(R)$ in [Ka1, Theorem 217] is also 1, so the statement of "$\mathrm{Ext}^r_R(M, R)$ vanishes for all $r > n - G(B)$" [Ka1, Theorem 217] gives exactly what we want. ■

Corollary 3.3 *If M is as in Proposition 3.2, $x \in M$ and n is a natural number, then $x \in (\sigma - 1)^n M$ if and only if, for all $\phi \in \mathrm{Hom}_R(M, R)$, we have $\phi(x) \in (\sigma - 1)^n R$.*

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

Proof One direction is again trivial. The other direction follows from the corresponding implication in Proposition 3.2 by induction on n and using that $\sigma - 1$ is a nonzerodivisor on R. ■

Proposition 3.4 *Let $i\colon R \to \mathbb{Z}_p[G]$ denote the G-linear injection induced by $1 \mapsto \sigma - 1$, n a natural number, and M as before. Let N be any $\mathbb{Z}_p[G]$-module containing M such that N/M has no $\mathbb{Z}$-torsion. Let $x \in M$. Then the following three statements are equivalent:*

(a) $\forall \phi \in \operatorname{Hom}_R(M, R) : \phi(x) \in (\sigma - 1)^n R$;
(b) $\forall \phi' \in \operatorname{Hom}_{\mathbb{Z}_p[G]}(M, \mathbb{Z}_p[G]) : \phi'(x) \in (\sigma - 1)^{n+1}\mathbb{Z}_p[G]$;
(c) $\forall \phi'' \in \operatorname{Hom}_{\mathbb{Z}_p[G]}(N, \mathbb{Z}_p[G]) : \phi''(x) \in (\sigma - 1)^{n+1}\mathbb{Z}_p[G]$.

Proof (a) implies (b): Every ϕ' must be of the form $i\phi$ for some $\phi\colon M \to R$, since M is annihilated by N_G and hence the image of ϕ' is automatically contained in $(\sigma - 1)\mathbb{Z}_p[G]$. The statement $\phi(x) \in (\sigma - 1)^n R$ immediately translates to $\phi'(x) \in (\sigma - 1)^{n+1}\mathbb{Z}_p[G]$.

(b) implies (a): Given ϕ, let $\phi' = i\phi$, and use that

$$(\sigma - 1)^{n+1}\mathbb{Z}_p[G] = (\sigma - 1)^n \operatorname{Im}(i).$$

(b) implies (c): Obvious, by looking at ϕ'' restricted to M.

(c) implies (b): It suffices to show that every ϕ' extends to a homomorphism $\phi''\colon N \to \mathbb{Z}_p[G]$. Indeed, the obstruction to extending ϕ is in $\operatorname{Ext}^1_R(N/M, R)$, and this is zero by the same reasoning as in the proof of Proposition 3.2. ■

Comment The preceding proposition will be applied with M being a module of units and N a module of S-units in some abelian field.

4 Extracting Roots of Circular Units

We keep all the notation introduced in §1. Our first aim is to prove Theorem 1.1. Since we intend to use Hayward's result, we recall his notation first. For any $i \in I = \{1, 2, \dots, s\}$, let $\mathfrak{p}_i$ be a prime of $\mathbb{Q}(\zeta_I)$ above p_i and let $f_{p_i}(x)$ denote the Artin symbol $(x, \mathbb{Q}(\zeta_I)_{\mathfrak{p}_i}/\mathbb{Q}_{p_i})$ for all nonzero $x \in \mathbb{Z}$. For $i, j \in I$, $i \neq j$, the (i, j)-th entry of Hayward's group-ring-valued reciprocity matrix A^I is equal to $f_{p_j}(p_i) - 1$, while the diagonal entries of A^I are determined by the condition that A^I has zero row sums. For any $i \in I$, A^I_i denotes the (i, i)-th minor of A^I, while $\overline{A^I_i}$ denotes its image in $\mathbb{Z}[G]$. We need to explain the ϕ^1 notation: $\phi^1(u)$ is the coefficient of the identity id $\in G$ in the element $\phi(u) \in \mathbb{Z}[G]$ for any G-homomorphism $\phi\colon M \to \mathbb{Z}[G]$ and any $u \in M$. Consequently, by G-linearity of ϕ,

$$\phi(u) = \sum_{g \in G} \phi^1(g^{-1}u)g.$$

Let $S = \{p_1, \dots, p_s\}$ and $\mathcal{O}_{K,S}$ be the ring of S-integers of K.

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

Proposition 4.1 (Hayward) *For all G-linear $\phi : \mathcal{O}^*_{K,S} \to \mathbb{Z}[G]$ we have*

$$\phi(\eta) \equiv \sum_{i=1}^{s} \phi^1(p_i)\overline{A_i^I} \pmod{I_G^s},$$

where I_G is the augmentation ideal of $\mathbb{Z}[G]$.

Proof This follows from [H, Proposition 5.5] and his "lowering the top field" argument given in the proof of [H, Proposition 3.2]. Alternatively, one may quote [H, Proposition 5.7], inserting the expressions for the regulators given by [H, Proposition 5.6]. ■

Let us now establish the connection with our notation. If $j, h \in I$, $j \neq h$, then the restriction of $f_{p_h}(p_j)^{-1}$ to the genus field $\overline{K}$ of K is $\sigma_h^{a_{jh}/q_h}$, with σ_h, q_h and a_{jh} being defined in §1 (e.g., by [H, Lemma 5.4]). Therefore the restriction of $f_{p_h}(p_j)$ to K equals $\sigma^{-a_{jh}}$ and so the image $\overline{A_i^I}$ in $\mathbb{Z}[G]$ of the (i,i)-th minor A_i^I is equal to the (i,i)-th minor of the zero-row-sum matrix that has, for $j \neq h$, the (j,h)-th entry equal to $\sigma^{-a_{jh}} - 1 = (\sigma - 1)\cdot\sum_{t=0}^{b_{jh}-1} \sigma^t$, where b_{jh} is a positive representative of $-a_{jh}$. Hence we can divide each row of the latter minor by $\sigma - 1$. But $\sum_{t=0}^{b_{jh}-1} \sigma^t \equiv b_{jh} \pmod{\sigma - 1}$ and so

$$\overline{A_i^I} \equiv (\sigma - 1)^{s-1} \cdot (-1)^{s-1} \cdot A_i \pmod{(\sigma - 1)^s},$$

where we have used $(\sigma - 1)^{s-1} \cdot l \equiv 0 \pmod{(\sigma - 1)^s}$, which follows from $(\sigma - 1)\cdot l \equiv (\sigma - 1)\cdot(1 + \sigma + \cdots + \sigma^{l-1}) = 0 \pmod{(\sigma - 1)^2}$ and $s > 1$.

Consequently, Proposition 4.1 just reads

$$(*) \qquad \phi(\eta) \equiv \sum_{i=1}^{s} \phi^1(p_i)(-1)^{s-1}A_i(\sigma - 1)^{s-1} \pmod{(\sigma - 1)^s}.$$

We note that an element of the finitely generated $\mathbb{Z}[G]$-module O_K^* is a $(\sigma - 1)^n$-th power if and only if this is true after p-completion. We let N be the p-completion of the group $O^*_{K,S}$. Now $(*)$ gives that $\phi(\eta)$ is divisible by $(\sigma - 1)^{s-1}$, which, together with Proposition 3.4, implies that there exists a unit ε_1 of K with $\varepsilon_1^{(\sigma-1)^{s-2}} = \eta$. But $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon_1) = \pm 1$, so, changing the sign of ε_1 if necessary, we can suppose that $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon_1) = 1$. Using Hilbert's Theorem 90 we find a nonzero $x \in K$ such that $x^{\sigma-1} = \varepsilon_1$. Since all ramified primes belong to S, multiplying x by a suitable rational number we obtain an S-unit ε with $\varepsilon^{\sigma-1} = \varepsilon_1$ and so $\varepsilon^{(\sigma-1)^{s-1}} = \eta$. We even may suppose that e_i, the exponent of p_i in $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)$, has sign $(-1)^{s-1}$ or zero and absolute value $< l$. In order to prove Theorem 1.1, we have only to establish that $e_i = (-1)^{s-1}A_i$. For this, fix $i \in I$. Let V denote the p-completion of the multiplicative span of $p_1, \ldots, p_s$, so $V \subset N$, and it is easily seen that N/V has no torsion. By the same reasoning as in the proof of Proposition 3.4, one sees that there exists $\phi \colon N \to \mathbb{Z}_p[G]$ which maps p_i to the norm element N_G and all other p_j to zero. Thus $\phi^1(p_j) = \delta_{ij}$ (Kronecker's delta). Moreover ϕ can be chosen as the continuous

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

extension of some G-homomorphism $\phi_0\colon O^*_{K,S} \to \mathbb{Z}[G]$; we can apply $(*)$ to this and obtain

$$(\sigma-1)^{s-1}\phi(\varepsilon) = \phi(\eta) \equiv (-1)^{s-1}A_i(\sigma-1)^{s-1} \pmod{(\sigma-1)^s}.$$

Now multiplication by $(\sigma-1)^{s-1}$ induces an isomorphism

$$\mathbb{Z}_p/l\mathbb{Z}_p \cong \mathbb{Z}_p[G]/(\mathrm{N}_G, (\sigma-1)) \to (\sigma-1)^{s-1}\mathbb{Z}_p[G]/(\sigma-1)^s\mathbb{Z}_p[G].$$

Thus, $\phi(\varepsilon) \equiv (-1)^{s-1}A_i \pmod{(l, \sigma-1)}$. On the other hand, we can calculate as follows:

$$\phi(\varepsilon) = \sum_{g\in G}\phi^1(g^{-1}\varepsilon)\,g \equiv \sum_{g\in G}\phi^1(g^{-1}\varepsilon) = \phi^1(\mathrm{N}_{K/\mathbb{Q}}\varepsilon) = e_i \pmod{(l, \sigma-1)}.$$

Thus $e_i \equiv (-1)^{s-1}A_i$ modulo l, and we get equality since both are in the same range of length l. This concludes the proof of Theorem 1.1.

Now we shall prove the corresponding generalization of [GK2, Theorem 3]. At first, let us recall the definition of semispecialness:

Let M be any p-power divisible by l^{s-1}. For any prime $q \equiv 1 \pmod{M}$ let $K(q)$ be the compositum of K with the cyclic field $\mathbb{Q}(q)$ of absolute degree M and conductor q. Let

$$\mathcal{Q}_M = \{q \text{ prime};\ q \text{ totally split in } K,\ q \equiv 1 + M \pmod{M^2},$$
$$p_i \text{ is an } M\text{-th power modulo } q \text{ for } i = 1, \dots, s\}.$$

A number $\varepsilon' \in K^*$ is called *M-semispecial* if for all but finitely many q in $\mathcal{Q}_M$, there exists $\varepsilon_q \in \mathcal{O}^*_{K(q)}$ satisfying

- $\mathrm{N}_{K(q)/K}(\varepsilon_q) = 1$ (*norm condition*).
- If $\tilde{q}$ is the product of all primes of $K(q)$ dividing q, then ε' and ε_q have the same image in $(\mathcal{O}_{K(q)}/\tilde{q})^*/(M/l^{s-1})$ (*congruence condition*).

Theorem 4.2 *The number ε constructed in Theorem 1.1 is M-semispecial for all p-powers M with $l^{s-1}|M$.*

Proof Let us fix M and take any $q \in \mathcal{Q}_M$ and, similarly to [GK2], for a fixed primitive q-th root of unity ζ_q put

$$\eta_q = \mathrm{N}_{\mathbb{Q}(\zeta_l,\zeta_q)/K(q)}(1-\zeta_l\zeta_q).$$

Here one should note that G is naturally a direct factor of $\mathrm{Gal}(K(q)/\mathbb{Q})$, so it acts on all data associated with the extension $K(q)/\mathbb{Q}$. We only need to know that there is $\varepsilon_q \in O^*_{K(q)}$ such that $\eta_q = \varepsilon_q^{(\sigma-1)^{s-1}}$. Indeed, let us show that if such ε_q exists then it can be chosen in such a way that it also satisfies the norm condition. From the standard norm relations for cyclotomic units and the condition "q totally split in K"

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

we obtain $\mathrm{N}_{K(q)/K}(\eta_q) = 1$ and so $\alpha = \mathrm{N}_{K(q)/K}(\varepsilon_q) \in K$ satisfies $\alpha^{(\sigma-1)^{s-1}} = 1$. We know (see the paragraph above Proposition 1.2) that this already forces $\alpha^{\sigma-1} = 1$ and so $\alpha \in \mathbb{Q}$. But α is a unit and so $\alpha = \pm 1$. Then, choosing $\alpha\varepsilon_q$ instead of ε_q we have both $\eta_q = \varepsilon_q^{(\sigma-1)^{s-1}}$ and the norm condition. From this point onward, the proof of Theorem 4.2 proceeds in the same way as in [GK2, §4, Proof of Theorem 3].

The existence of ε_q can be proved by a similar approach as Theorem 1.1. It is enough to show that η_q is an $(\sigma - 1)^{s-1}$th power in the p-completion of $O^*_{K(q)}$. But, using Proposition 3.4 and Corollary 3.3, this is an easy consequence of the following Proposition 4.3. ■

Proposition 4.3 *For all $\phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(O^*_{K(q)} \otimes \mathbb{Z}_p, \mathbb{Z}_p[G])$ the value $\phi(\eta_q)$ is divisible by $(\sigma - 1)^s$.*

Proposition 4.3 is not yet amenable to an induction argument. But we shall show that Proposition 4.3 is a consequence of the following Proposition 4.4. Let $\overline{K}$ be the genus field of K, $\Gamma = \mathrm{Gal}(\overline{K}/\mathbb{Q})$ and

$$\beta_q = \mathrm{N}_{\mathbb{Q}(\zeta_I, \zeta_q)/\overline{K}(q)}(1 - \zeta_I\zeta_q),$$

the conductor level Sinnott unit of $\overline{K}(q)$.

Proposition 4.4 *For all $\phi \in \mathrm{Hom}_{\mathbb{Z}_p[\Gamma]}(O^*_{\overline{K}(q)} \otimes \mathbb{Z}_p, \mathbb{Z}_p[\Gamma])$, the value $\phi(\beta_q)$ lies in I_Γ^s, where I_Γ is the augmentation ideal of $\mathbb{Z}_p[\Gamma]$.*

Proof We use induction on s. This is very close to the proof of [H, Proposition 5.5], but in some sense simpler.

For $s = 1$ we must show $\phi(\beta_q) \equiv 0 \pmod{I_\Gamma}$. But this is quite easy:

$$\mathrm{N}_{\overline{K}(q)/\mathbb{Q}(q)}(\beta_q) = 1$$

since the Frobenius automorphism of p_1 on $\mathbb{Q}(q)$ is trivial, so $\phi(\beta_q)$ is annihilated by this norm N_Γ and has to lie in I_Γ.

We now copy the inductive step [H, p. 115]. Here $\overline{K} = \prod_{i=1}^s K_i$ is the compositum of the fields K_i introduced in §1, $\Gamma_i = \mathrm{Gal}(K_i/\mathbb{Q})$, $I = \{1, \dots, s\}$ corresponds to Hayward's $B = \{1, \dots, d+1\}$, g_i is a fixed generator of Γ_i. Hayward uses Eulerian relations: write $\beta_{J,q}$ for the conductor level unit in $K_J(q)$, where J is any nonempty subset of $\{1, \dots, s\}$ and K_J is the compositum of the K_i with $i \in J$. Note that for $I = \{1, \dots, s\}$ we recover $\beta_q = \beta_{I,q}$. All we need is that $\mathrm{N}_{\Gamma_i}\beta_q$ equals $\alpha_i\beta_{I\setminus\{i\}}$ for some element α_i of I_Γ, and that the total norm N_Γ kills β_q. The sum displayed three lines below formula (11) in [H] then reads with our simplified notation in our setting:

$$\sum_{\varnothing \neq J \subset I} (-1)^{s-|J|} \phi_J(\beta_{J,q}) \prod_{j \in I - J} \alpha_j.$$

It is in I_Γ^s exactly as in [H], and the maps ϕ_J are constructed from ϕ in a quite analogous fashion to [H]: they are Γ_J-linear, defined on $O^*_{K_J(q)}$ with target $\mathbb{Z}[\Gamma_J]$. All

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

summands of this term except the one with $J = I$ are then in I_Γ^s, since $\phi_J(\beta_{J,q})$ is in $I_\Gamma^{|J|}$, by the induction hypothesis, and the product of the α_j is visibly in $I_\Gamma^{s-|J|}$. The summand with $J = I$ is exactly $\phi(\beta_q)$, and the whole sum is in I_Γ^s. Therefore $\phi(\beta_q)$ is in I_Γ^s and the induction step is complete. ■

Proof of Proposition 4.3 Now we shall use the "lowering the top field" argument to prove that Proposition 4.4 implies Proposition 4.3. For any $\phi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(O^*_{K(q)} \otimes \mathbb{Z}_p, \mathbb{Z}_p[G])$ we obtain $\phi^1 \in \mathrm{Hom}_{\mathbb{Z}_p}(O^*_{K(q)} \otimes \mathbb{Z}_p, \mathbb{Z}_p)$. But $(O^*_{\overline{K}(q)} \otimes \mathbb{Z}_p)/(O^*_{K(q)} \otimes \mathbb{Z}_p)$ has no torsion, since $O^*_{\overline{K}(q)}/O^*_{K(q)}$ has no p-torsion (suppose there is $x \in \overline{K}(q)$ such that $x \notin K(q)$ but $x^p \in K(q)$; since $\overline{K}(q)$ is abelian over $K(q)$, this would force $K(q)$ to contain a primitive p-th root ζ_p of unity, and this is not the case, since the ramification index of p in $K(q)/\mathbb{Q}$ is a p-power hence odd). Therefore there is $\psi \in \mathrm{Hom}_{\mathbb{Z}_p}(O^*_{\overline{K}(q)} \otimes \mathbb{Z}_p, \mathbb{Z}_p)$, whose restriction to $O^*_{K(q)} \otimes \mathbb{Z}_p$ is ϕ^1. Now we can define $\psi' \in \mathrm{Hom}_{\mathbb{Z}_p[\Gamma]}(O^*_{\overline{K}(q)} \otimes \mathbb{Z}_p, \mathbb{Z}_p[\Gamma])$ by $\psi'(x) = \sum_{\vartheta \in \Gamma} \psi(\vartheta x)\vartheta^{-1}$ for any $x \in O^*_{\overline{K}(q)} \otimes \mathbb{Z}_p$. Then Proposition 4.4 gives $\psi'(\beta_q) \in I_\Gamma^s$, and so $\mathrm{res}_{\overline{K}(q)/K(q)}\psi'(\beta_q) \in I_G^s$. But

$$\begin{aligned}\mathrm{res}_{\overline{K}(q)/K(q)}\psi'(x) &= \sum_{\vartheta \in \Gamma} \psi(\vartheta x)\, \mathrm{res}_{\overline{K}(q)/K(q)}\vartheta^{-1} = \sum_{\tau \in G} \psi(\mathrm{N}_{\overline{K}(q)/K(q)}(\tau x))\tau^{-1} \\ &= \sum_{\tau \in G} \phi^1(\mathrm{N}_{\overline{K}(q)/K(q)}(\tau x))\tau^{-1} = \phi(\mathrm{N}_{\overline{K}(q)/K(q)}(x)),\end{aligned}$$

and so Proposition 4.3 follows from $\mathrm{N}_{\overline{K}(q)/K(q)}(\beta_q) = \eta_q$ and from the obvious fact that I_G^s is generated by $(\sigma - 1)^s$. ■

Hence, Proposition 4.3 is proved, and we are done with the proof of Theorem 4.2.

5 Proof of Theorem 1.3

Concerning Theorem 1.3, the fact $C = \langle -1, \varepsilon^{\sigma-1} \rangle$ has been proved by a direct computation in the first section. If we show that [GK2, Theorem 4] carries over to the setup of the present paper, then this theorem and Theorem 4.2 will give Theorem 1.3 just in the same way as [GK2, Theorem 4] plus [GK2, Theorem 3] imply [GK2, Theorem 2].

When we proved [GK2, Theorem 4], we worked under the assumption that all ramification in $K/\mathbb{Q}$ was total and tame. The only place in the proof of that theorem which actually uses these hypotheses on ramification is [GK2, Lemma 18]. We just have to explain why the lemma remains true if we allow non-total ramification (wild ramification still being excluded). In the proof of part (a), we used that $\mathrm{Gal}(K(\zeta_{M^2})/K) \cong (\mathbb{Z}/M^2)^*$. This remains true since p is unramified in K, so K and $\mathbb{Q}(\zeta_{M^2})$ are linearly disjoint over $\mathbb{Q}$. We are even able to say that $K(\zeta_{M^2})/K$ is totally ramified at all places above p. This shows that the claim in the proof of part (c) that "$K(\zeta_{M^2})$ and the Hilbert class field H of K are disjoint over K" also remains true. Since part (b) is quite analogous to part (a), we now have checked the validity of [GK2, Lemma 18] completely in our setting.

As was said before, this suffices to establish Theorem 1.3.

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

6 Proof of Proposition 1.4

In this section we assume that the decomposition group of any prime ramified at $K/\mathbb{Q}$ equals G. Let us say "K belongs to the genus case" if the non-genus part $(\sigma - 1)\mathcal{C}l(K)_p$ is trivial. (Equivalently: the Hilbert p-class field of K is equal to the genus field of K. In looser terms: $\mathcal{C}l(K)_p$ is just as large as forced by genus theory.) We show next that K belongs to the genus case if and only if at least one of A_i is not divisible by p.

At first, let us suppose that all A_i are divisible by p. Let ε be as in Theorem 1.1. From Proposition 1.2 and Theorem 1.3 we know that

$$|(\sigma - 1)\mathcal{C}l(K)_p| = [E : \langle \varepsilon^{\sigma-1} \rangle]_p,$$

where E is the group of units of K. Let us distinguish two cases:

- $\varepsilon \in E$: It is easy to see that $\varepsilon^l = \varepsilon^{(\sigma-1)\Delta} \in \langle \varepsilon^{\sigma-1} \rangle$, where $\Delta = \sum_{a=1}^{l-1} a\sigma^a$. We have $p \mid [E : \langle \varepsilon^{\sigma-1} \rangle]$ since $\varepsilon \notin \langle \varepsilon^{\sigma-1} \rangle$. Indeed, if $\gamma \in \mathbb{Z}[G]$ satisfies $\varepsilon = \varepsilon^{(\sigma-1)\gamma}$, for a suitable $t \in \mathbb{Z}$ we obtain $1 = (\sigma - 1)\gamma + tN$, where $N = \sum_{a=0}^{l-1} \sigma^a$, and by considering the augmentation map we get $1 = tl$, which is a contradiction.
- $\varepsilon \notin E$: Let us denote $\rho = \varepsilon^{l/p} \cdot \prod_{i=1}^{s} p_i^{(-1)^s A_i/p}$. Theorem 1.1 gives that

$$\rho^p = \varepsilon^l \cdot \prod_{i=1}^{s} p_i^{(-1)^s A_i} = \varepsilon^l \cdot \mathrm{N}_{K/\mathbb{Q}}(\varepsilon)^{-1} = \varepsilon^{(\sigma-1)\Delta} \in \langle \varepsilon^{\sigma-1} \rangle.$$

  Therefore $\rho \in E$. We shall prove that $\rho \notin \langle \varepsilon^{\sigma-1} \rangle$. Indeed, supposing the contrary gives the existence of $\gamma \in \mathbb{Z}[G]$ such that $\rho = \varepsilon^{(\sigma-1)\gamma}$. Then $\varepsilon^{(\sigma-1)p\gamma} = \rho^p = \varepsilon^{(\sigma-1)\Delta}$ which means $(\sigma - 1)p\gamma = (\sigma - 1)\Delta = l - N$, giving $p|N$ in $\mathbb{Z}[G]$, which is a contradiction. Again we have $p|[E : \langle \varepsilon^{\sigma-1} \rangle]$.

In both cases we have obtained that p divides $|(\sigma - 1)\mathcal{C}l(K)_p|$ and so K does not belong to the genus case.

We shall suppose now that at least one of A_i, say A_t, where $1 \le t \le s$, is not divisible by p. Let $\overline{K}$ be the genus field of K. Let φ be the isomorphism mapping $\mathcal{C}l(K)_p/(\sigma - 1)\mathcal{C}l(K)_p$ onto the Galois group of $\overline{K}/K$ induced by the Artin map. Let $\mathcal{C}l(K)_p[\sigma - 1]$ mean the subgroup of $\mathcal{C}l(K)_p$ killed by $\sigma - 1$ and let ι be the mapping from $\mathcal{C}l(K)_p[\sigma - 1]$ to $\mathcal{C}l(K)_p/(\sigma - 1)\mathcal{C}l(K)_p$ induced by the inclusion. It is easy to see that $|\mathcal{C}l(K)_p[\sigma - 1]| = |\mathcal{C}l(K)_p/(\sigma - 1)\mathcal{C}l(K)_p|$ by considering the kernel and the cokernel of the mapping $\mathcal{C}l(K)_p \to \mathcal{C}l(K)_p$ given by the action of $\sigma - 1$. It is enough to show that ι is surjective, since then ι is an isomorphism. But then for any $x \in \mathcal{C}l(K)_p$ such that $(\sigma - 1)x \neq 0$ there is a positive integer n such that $(\sigma - 1)^n x \neq 0$ and $(\sigma - 1)^{n+1}x = 0$, which gives $0 \neq (\sigma - 1)^n x \in (\sigma - 1)\mathcal{C}l(K)_p \cap \mathcal{C}l(K)_p[\sigma - 1]$, a contradiction. Hence $(\sigma - 1)\mathcal{C}l(K)_p$ is trivial and K belongs to the genus case.

So it remains to prove that ι is surjective. We shall actually prove that $\varphi \circ \iota$ is surjective. At first, let us recall some notation. For any $i = 1, \dots, s$, the ramification index of p_i is p^{k_i}. Due to our assumption, the decomposition group of p_i is G and so the inertia degree of p_i is $q_i = lp^{-k_i}$. Recall that the cyclic field of absolute degree p^{k_i} ramified only at p_i is denoted by K_i. Then the genus field $\overline{K}$ is the compositum

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

of $K_1, \dots, K_s$. We have chosen generators $\sigma_1, \dots, \sigma_s$ of the Galois group $\mathrm{Gal}(\overline{K}/\mathbb{Q})$ such that $\sigma_j|_{K_i}$ is the identity if $i \neq j$ and $\sigma_j|_K = \sigma^{q_j}$. Any $\nu \in \mathrm{Gal}(\overline{K}/K)$ is of the form $\nu = \prod_{j=1}^s \sigma_j^{x_j}$, where the integers x_j are well-defined modulo p^{k_j} and we have $l \mid \sum_{j=1}^s q_j x_j$.

Let $\mathfrak{p}_i$ be the prime of K above p_i. Its class $[\mathfrak{p}_i]$ lies in $\mathcal{C}l(K)_p[\sigma - 1]$ and $\varphi \circ \iota([\mathfrak{p}_i])$ is the Artin symbol $(\mathfrak{p}_i, \overline{K}/K)$. We define integers b_{ij} by $\varphi \circ \iota([\mathfrak{p}_i]) = \prod_{j=1}^s \sigma_j^{b_{ij}}$. Hence the b_{ij} are well-defined modulo p^{k_j} and satisfy $l \mid \sum_{j=1}^s q_j b_{ij}$ for each i. We will relate the integers b_{ij} to the entries a_{ij} of A. Let $i \neq j$, then

$$\sigma_j^{b_{ij}} = (\mathfrak{p}_i, \overline{K}/K)|_{K_j} = (\mathfrak{p}_i, KK_j/K)|_{K_j} = (\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_i), K_j/\mathbb{Q}) = (p_i, K_j/\mathbb{Q})^{q_i}.$$

But $(p_i, K_j/\mathbb{Q})$ is the Frobenius automorphism of p_i on K_j, so it is equal to $\sigma_j^{a_{ij}/q_j}$ due to the definition of A. Therefore $b_{ij} \equiv q_i \frac{a_{ij}}{q_j} \pmod{p^{k_j}}$, which gives $q_j b_{ij} \equiv q_i a_{ij} \pmod{l}$, assuming $i \neq j$. But A has zero row sums, hence $q_i b_{ii} \equiv -\sum_{j \neq i} q_j b_{ij} \equiv -\sum_{j \neq i} q_i a_{ij} = q_i a_{ii} \pmod{l}$. Thus $a_{ii} \equiv b_{ii} \pmod{p^{k_i}}$. We have obtained that the matrix $B = (b_{ij})$ can be obtained from the matrix A by the following procedure: multiply each row (the i-th row is multiplied by q_i) and divide each column (the j-th column is divided by q_j). The described procedure does not change the (i,i)-th minors of the matrix, so we are assuming that there is $t \in \{1, \dots, s\}$ such that the (t,t)-th minor of B is not divisible by p. Let $x_1, \dots, x_s$ be any integers satisfying $l \mid \sum_{j=1}^s q_j x_j$. To prove that $\varphi \circ \iota$ is surjective we will show that there are integers $y_1, \dots, y_s$ such that

$$\sum_{i=1}^s y_i b_{ij} \equiv x_j \Big(\bmod \frac{l}{q_j}\Big)$$

is satisfied for each $j = 1, \dots, s$. For a moment, let us forget the congruence for $j = t$ and put $y_t = 0$. The obtained system of congruences is solvable since the matrix of the system is invertible over $\mathbb{Z}_p$ as its determinant, which is the (t,t)-th minor of B, is invertible. But then the congruence for $j = t$ is also satisfied:

$$\begin{aligned} q_t x_t &\equiv -\sum_{j \neq t} q_j x_j \equiv -\sum_{j \neq t} q_j \sum_{i=1}^s y_i b_{ij} = -\sum_{i=1}^s y_i \sum_{j \neq t} q_j b_{ij} \\ &\equiv \sum_{i=1}^s y_i q_t b_{it} = q_t \sum_{i=1}^s y_i b_{it} \pmod{l} \end{aligned}$$

and the proposition is proved. ■

7 Construction of Example 1.5

In presenting our example which disproves the validity of Theorem 1.3 without the decomposition hypothesis, one option would be to throw it at the reader and state that it has all required properties, checked by PARI. We feel however that this would not be very enlightening. At the expense of a few extra pages we prefer to explain how

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

we found our way to the counterexample, sticking to a general framework as long as possible. A little PARI calculation is only needed at the end when giving numerical values to our parameters. It appears that our construction should give infinite families of counterexamples, but it also appears that a rigorous proof, replacing the computer verification, would be very difficult. In view of this we proceed as follows.

We keep the notation K, l, s, and G from the beginning. At first no restrictions will be imposed; then we will set $k = 2$ (that is, degree p^2) and $s = 3$ (three ramified primes), also assuming a certain decomposition pattern. In this setting we will give a list of five conditions that imply (taken together) that K is a counterexample of the desired kind. It can be shown using Chebotarev's theorem that the first four conditions can be satisfied infinitely often for any fixed p. The fifth condition is more subtle. For a concrete example we will take $p = 3$, give explicit values to everything, and verify the validity of the fifth condition by computation.

We need an analog of Theorem 7 (a version of the Rédei–Reichardt theorem) in [GK1], in order to control the size of $(\sigma - 1)\mathcal{C}l(K)_p$ in terms of a certain matrix. We have to redo some of the basics. Let us change notation slightly: the group of units of K will be written $\mathcal{O}_K^*$, and E will mean $\mathbb{Z}_p \otimes \mathcal{O}_K^*$. Likewise C will stand for the $\mathbb{Z}_p[G]$-span of $\varepsilon_1^{\sigma-1}, \dots, \varepsilon_s^{\sigma-1}$.

Lemma 7.1 *For $i = 1, \dots, s$, let $\mathfrak{p}_i$ be a prime ideal of K above p_i, and let $\mathfrak{a}_i$ be the product of all G-conjugates of $\mathfrak{p}_i$ without repetition. Then:*

(a) *$\mathcal{C}l(K)_p^G$ is generated by the classes $[\mathfrak{a}_i]$, $i = 1, \dots, s$.*

(b) *Let $\iota\colon \mathbb{Z}/(p^{k_1}) \times \cdots \times \mathbb{Z}/(p^{k_s}) \to \mathcal{C}l(K)_p^G$ be defined by mapping $(0, \dots, 1, \dots, 0)$ (the 1 at position i) to $[\mathfrak{a}_i]$. Then the kernel of ι has order $|G| = l = p^k$.*

Proof We note to begin with that $\mathfrak{a}_i^{p^{k_i}}$ is the ideal $p_i\mathcal{O}_K$, so the map ι makes sense (*cf.* also [RW, Lemma 2.1]).

Since E has no nontrivial G-fixed elements, the Tate cohomology group $\hat{\mathrm{H}}^0(G, E)$ is zero. Since $\mathbb{Q}E \cong \mathbb{Q}_p[G]/(\mathrm{N}_G)$, the Herbrand quotient of E is $1/|G|$, and therefore (by cyclicity of G) the order of $\mathrm{H}^1(G, E)$ is $|G|$. Let I_K be the ideal group of K tensored with $\mathbb{Z}_p$, and P_K the subgroup of principal ideals, tensored with $\mathbb{Z}_p$. From $0 \to E \to K^* \otimes \mathbb{Z}_p \to P_K \to 0$ and Hilbert's Theorem 90 we obtain $\mathrm{H}^1(G, P_K) = 0$. Thus $0 \to P_K \to I_K \to \mathcal{C}l(K)_p \to 0$ remains exact on taking G-invariants. Visibly, I_K^G is generated by the $\mathfrak{a}_i$ and all ideals extended from $\mathbb{Q}$, but the latter ones are all principal. Therefore part (a) follows. Taking G-invariants in the other sequence we get $0 \to E^G \to \mathbb{Q}^* \otimes \mathbb{Z}_p \to P_K^G \to \mathrm{H}^1(G, E) \to 0$. Give the label α to the map with target P_K^G in this sequence; so $\operatorname{coker}(\alpha)$ has order $|G|$. The map $(0, \dots, 1, \dots, 0) \mapsto \mathfrak{a}_i$ gives an identification of $\mathbb{Z}/(p^{k_1}) \times \cdots \times \mathbb{Z}/(p^{k_s})$ with the quotient $I_K^G/\operatorname{Im}(\alpha)$, and then $P_K^G/\operatorname{Im}(\alpha)$ gets identified with the kernel of ι. This proves (b). ■

The genus field $\overline{K}$ is the compositum of the fields $K_1, \dots, K_s$. The group $\mathrm{Gal}(\overline{K}/\mathbb{Q})$ is the direct product of the cyclic groups $\langle\sigma_i\rangle = \mathrm{Gal}(K_i/\mathbb{Q})$; moreover, the canonical epimorphism $\mathrm{Gal}(\overline{K}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ sends σ_i to σ^{q_i} for $i = 1, \dots, s$. If we identify $\mathrm{Gal}(\overline{K}/\mathbb{Q})$ with $W := \mathbb{Z}/(p^{k_1}) \times \cdots \times \mathbb{Z}/(p^{k_s})$ via its generators $\sigma_1, \dots, \sigma_s$, then

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

$\Delta := \operatorname{Gal}(\overline{K}/K)$ becomes identified with the kernel of the mapping $W \longrightarrow \mathbb{Z}/(p^k)$, $(c_1, \dots, c_s) \mapsto \sum_{j=1}^{s} q_j c_j$.

Proposition 7.2 *If we use the above description of Δ, then the Frobenius of $\mathfrak{p}_i$ in $\overline{K}/K$ is the row vector $(f_i a_{ij}/q_j)_j$, where f_i is the inertia degree of p_i in K. (The matrix $A = (a_{ij})$ over $\mathbb{Z}/(p^k)$ was defined in §1.) The Frobenius of $\mathfrak{a}_i$ is g_i times this row vector, with g_i the number of prime ideals above p_i in K.*

Proof The second statement is an easy consequence of the first, so it suffices to show that the Frobenius of $\mathfrak{p}_i$ in $\overline{K}/K$ is $\prod_{j=1}^{s} \sigma_j^{f_i a_{ij}/q_j}$. We have by construction of A that the Frobenius of p_i in $K_j/\mathbb{Q}$ is $\sigma_j^{a_{ij}/q_j}$; from this one deduces the desired formula exactly as in §6. The factor q_i coming up there corresponds to the factor f_i here. ■

From now on we assume that all inertia degrees $f_1, \dots, f_s$ are 1, that is, every prime p_i is fully decomposed in a subfield K' of K and fully ramified in K/K'. Thus we can forget about the factors f_i in the preceding proposition.

We now consider the map $f\colon I_K^G/P_K^G \rightarrow W$, $f([\mathfrak{a}_i]) = (g_i \cdot a_{ij}/q_j)_j$. The image of f is contained in V which is by definition the set of all $(c_1, \dots, c_s)$ such that $\sum_j q_j c_j = 0$. So $|V| = p^{k_1+\cdots+k_s-k}$. From Lemma 7.1 one sees that $I_K^G/P_K^G = \mathcal{C}l(K)_p^G$ has exactly the same order. We recall that there is also a canonical identification $V = \operatorname{Gal}(\overline{K}/K)$. Since f is essentially the Artin map according to the last proposition, we get a commutative diagram

$$\begin{tikzcd}
\mathcal{C}l(K)_p^G \arrow[r, "f"] \arrow[ddr, "f'"'] & V \arrow[d, "\cong"] \\
 & \Delta \arrow[d] \\
 & \mathcal{C}l(K)_p/(\sigma-1)\mathcal{C}l(K)_p
\end{tikzcd}$$

where f' is induced by the inclusion $\mathcal{C}l(K)^G \rightarrow \mathcal{C}l(K)$ and the lower vertical map is the isomorphism from genus field theory. Moreover,

$$\ker(f') = \mathcal{C}l(K)_p^G \cap (\sigma-1)\mathcal{C}l(K)_p = \bigl((\sigma-1)\mathcal{C}l(K)_p\bigr)^G.$$

We are interested in cases where the latter module is "minimal nonzero", that is, of order p. The point in this is as follows: We recall from §3 that R denotes the ring $\mathbb{Z}_p[G]/(\mathrm{N}_G)$, and we define a finite R-module X to be *taut* (not standard terminology!) if $|X| = [R : \operatorname{Ann}_R(X)]$. If X^G is a cyclic $\mathbb{Z}_p$-module, then the socle of X is simple. Therefore the Pontryagin dual $X^\vee$ has simple radical-factor module, so it is cyclic. Therefore $[R : \operatorname{Ann}_R(X^\vee)] = |X^\vee| = |X|$; and by dualizing again one sees that

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

$\mathrm{Ann}_R(X^\vee) = \mathrm{Ann}_R(X)$, so the outcome of this reasoning is: Whenever X^G is cyclic over $\mathbb{Z}_p$, then X is taut. This, applied to $X = (\sigma - 1)\mathcal{C}l(K)_p$, will be instrumental in finding our counterexample.

From here on we fix $k = 2$, $s = 3$ and assume $k_1 = k_2 = 2; k_3 = 1$. The choice of p is left open for yet awhile. Thus K is cyclic over $\mathbb{Q}$ of degree p^2. Let K' denote the subfield of degree p.

Theorem 7.3 *Suppose that K and K' satisfy the following list of conditions:*

(1) *All 2×2 principal minors of the matrix A are zero modulo p^2.*
(2) *All 1×1 principal minors of the matrix A' are zero modulo p, where A' is the analogous matrix to A for the degree p subfield K'; note that A' is a 2×2 matrix.*
(3) *The prime p_3 splits (totally) in K'.*
(4) *The image of f has order p^2.*
(5) *The only units in K' that are norms from K are p-th powers.*

Then $(\sigma-1)\mathcal{C}l(K)_p$ is a taut module, and $\mathrm{Ann}_R(E/C)$ *does not annihilate $(\sigma-1)\mathcal{C}l(K)_p$.*

Remark 7.4 The map f is essentially given by the matrix A, with the following modifications: the last column is divided by p (this is because $q_3 = p$), and the last row is multiplied by p (this is because $g_3 = p$).

Proof For the proof of Theorem 7.3 we first show that $(\sigma - 1)\mathcal{C}l(K)_p$ is taut. For this it suffices, by the above, to have $((\sigma - 1)\mathcal{C}l(K)_p)^G$ cyclic over $\mathbb{Z}_p$, and we actually claim it is of order p. Indeed, it is identified with the kernel of f'. The image of f' is of order p^2 by condition (4), and the domain of definition of f' has order $p^{2+2+1-2}$ as previously remarked in greater generality, which gives p^3, so we are done here.

We next show that the integral closure of R acts on E in a natural way. Let $\nu = 1 + \sigma^p + \cdots + \sigma^{(p-1)p}$; this is the relative norm from K to K'. The $\mathbb{Q}_p$-algebra $\mathbb{Q}R$ has two primitive idempotents $e' = \nu/p$ and $e'' = 1 - e'$. The maximal order T in $\mathbb{Q}R$ is $e'R \oplus e''R$, a product of two discrete valuations rings, the former isomorphic to $\mathbb{Z}_p[\zeta_p]$, the latter isomorphic to $\mathbb{Z}_p[\zeta_{p^2}]$. Now T acts naturally on the torsion-free module E if and only if e' acts, that is, if and only if every norm η^ν of a unit $\eta \in \mathcal{O}_K^*$ is a p-th power. But this holds, by our fifth condition. We claim that this implies: *The index of the annihilator J of E/C over R is strictly smaller than the order of E/C.* Once this is proved, it will follow at once that J is not contained in the R-annihilator of $(\sigma - 1)\mathcal{C}l(K)_p$ because the latter module has the same order as E/C and is taut.

We now justify the claim and begin by noting a few simple facts: T is a product of two discrete valuation rings and E is T-free cyclic for reasons of rank. Moreover, C is contained in $(\sigma - 1)E$ by conditions (1) and (2) and Theorem 1.1. Thus E/C is T-isomorphic to T/J' where J' is some T-ideal contained in the radical of T, and J' is the exact T-annihilator of E/C. Of course we then have $J = J' \cap R$. We also know that $|E/C| = |T/J'|$. To establish the claim we therefore must just show $[R : J] < [T : J']$. This inequality is equivalent to $[J' : J] < [T : R]$. But J is the kernel of the obvious map $j\colon J' \to T/R$, so $[J' : J]$ is the order of the image of j, and j cannot be surjective since its image is in the radical of the nonzero module T/R. Thus the above claim and the theorem are proved. ■

In order to arrive at a concrete counterexample, it only remains to realize all the conditions in the last theorem, and for this purpose we take $p = 3$. For the sake of simplicity let us agree that whatever p_i is, we take for χ_i the character that maps the least positive primitive root mod p_i to ζ_9 for $i = 1, 2$, respectively to ζ_9^3 for $i = 3$. It is straightforward to find many triplets (p_1, p_2, p_3) satisfying conditions (1)–(4). We give just one here which seems to be about as small as it can get, without having done an extensive search: $(p_1, p_2, p_3) = (37, 433, 97)$. The matrix A is:

$$\begin{pmatrix} 0 & 6 & 3 \\ 3 & 6 & 0 \\ 6 & 6 & 6 \end{pmatrix}.$$

The matrix A' is derived from A as follows: take the left upper 2×2 submatrix of A without the diagonal entries, fill the diagonal so as to make the row sums vanish, and reduce mod 3. The result is clearly the zero matrix. So condition (2) in the theorem is satisfied. Condition (1) is an easy consequence of the fact that every entry of A is a multiple of 3. Condition (3) (which will be needed below again) holds since p_3 already splits in the two cubic fields of conductor p_1 and p_2 individually, hence also in K'. The image of the map f is the span of the vectors $(0, 6, 1)$ and $(3, 6, 0)$ in $\mathbb{Z}/9 \times \mathbb{Z}/9 \times \mathbb{Z}/3$, hence of order $9 = p^2$, so condition (4) is satisfied.

The most interesting point is checking condition (5). This goes as follows. Using PARI one finds a pair of fundamental units η_1, η_2 for K': a generating polynomial is $f(x) = x^3 - x^2 - 5340x + 59337$, and the fundamental units are given by $\eta_1 = \frac{1}{5}(866265946\xi^2 + 68116106252\xi + 662120160917)$ and $\eta_2 = \frac{1}{9}(4041368488\xi^2 - 41877962210\xi - 21105076828281)$ where ξ is the image of x in K'. (Note: A little care is necessary in order to get the correct field of conductor $p_1 p_2$, since there are two of them.) Then one verifies that the natural map

$$\mathcal{O}_{K'}^*/3 \to (\mathcal{O}_{K'}/97\mathcal{O}_{K'})^*/3$$

is injective, as follows: Note that 97 is split in K', so any $\eta \in \mathcal{O}_{K'}^*$ gives rise to a triple of elements of $(\mathbb{Z}/97)^*$ (indeed η_1 maps to $(8, 92, 17)$ under some labeling of the three primes above 97 in K'), and the index map modulo any fixed primitive root g mod 97, $g = 5$ say, provides an isomorphism $\big((\mathbb{Z}/97)^* \times (\mathbb{Z}/97)^* \times (\mathbb{Z}/97)^*\big)/3 \to (\mathbb{Z}/3)^3$; the triple $(8, 92, 17)$ maps to $(0, 1, 2)$. Likewise, if we start with η_2, we obtain $(2, 0, 1)$.

The three primes above 97 are totally and tamely ramified in K/K'. Therefore, every norm from K to K' of an element prime to 97 maps to a cube modulo these three primes. From the above we infer that any unit which is a cube modulo these three primes is a cube itself. This establishes condition (5), and the construction of one counterexample is complete. Note that Example 1.5 given in the first section uses different prime numbers, but it was found by the same method, and as a double check, we calculated the two R-modules in question explicitly. Among the examples

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

we found, the field given in Example 1.5 is of smallest conductor, but we did not do an extensive search. A search without guidance from theory probably would not have led to any counterexample.

8 A Final Comment

In a recent preprint [BH], Burns and Hayward prove that in a different setting ($K/\mathbb{Q}$ noncyclic) the whole approach systematically fails because the conductor level Sinnott unit η_K is often not "divisible" at all, that is, not contained in $O^*_{K,S}$ to the power I_G. We will give a short argument here why this is so. (The point is not so much the shortness but that we use simpler ingredients.)

Let p be odd, K the compositum of K_1 and K_2 where K_i is cyclic of order p, (tamely) ramified exactly in p_i, and neither of the p_i splits in K. Let $E = \mathbb{Z}_p \otimes_{\mathbb{Z}} O^*_K$, and $E_S = \mathbb{Z}_p \otimes_{\mathbb{Z}} O^*_{K,S}$ with $S = \{\infty, p_1, p_2\}$. Because of the non-splitting of the p_i, η_K generates the full group of Sinnott units of K (maybe up to -1 which is irrelevant). Since Fröhlich [F, Theorem 5.2 II(b)] showed that p does not divide h_K, we know by Sinnott's class number formula (see [S, Theorem. 4.1, Theorem. 5.1]) that p does not divide the index of the Sinnott unit group in the full unit group. (There are no extra rational factors in that class number formula because K is its own genus field.) This implies, of course, that η_K generates E, so it cannot be contained in E^{I_G}. So we are almost done; it remains to show that η_K cannot even lie in $E_S^{I_G}$.

The ideal above p_i in K is principal ($i = 1, 2$), generated by $\eta_i = \mathrm{N}_{\mathbb{Q}(\zeta_{p_i})/K_i}(1 - \zeta_{p_i})$. Thus E_S is generated by E, η_1, and η_2. This shows that (switching to additive notation and letting $E_i = \mathbb{Z}_p \otimes_{\mathbb{Z}} O^*_{K_i}$)

$$I_G \cdot E_S \subset I_G \cdot E + E_1 + E_2.$$

Now E is free cyclic over $R = \mathbb{Z}_p[G]/(N_G)$. Hence it has a unique maximal submodule (the Jacobson radical). Clearly E_1 and E_2 are proper submodules of E. It is equally obvious that $I_G \cdot E$ is a proper submodule of E. Therefore the sum $I_G \cdot E + E_1 + E_2$ is a proper submodule of E again, which means that η_K, which generates E, cannot lie in this proper submodule, and therefore cannot be in $I_G \cdot E_S$.

References

[BH] D. Burns and A. Hayward, *Explicit units and the Equivariant Tamagawa number conjecture. II.* Preprint: http://www.mth.kcl.uk/staff/dj_burns/gk3/ps

[F] A. Fröhlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields.* Contemporary Mathematics 24, American Mathematical Society, Providence, RI, 1983.

[GK1] C. Greither and R. Kučera, *The lifted root number conjecture for fields of prime degree over the rationals: an approach via trees and Euler systems.* Ann. Inst. Fourier (Grenoble) **52**(2002), 735–777.

[GK2] ———, *Annihilators for the class group of a cyclic field of prime power degree.* Acta Arith. **112**(2004), no. 2, 177–198.

[H] A. Hayward, *A class number formula for higher derivatives of abelian L-functions.* Compositio Math. **140**(2004), no. 1, 99–129.

[Ka1] I. Kaplansky, *Commutative Rings.* Polygonal Publishing House, Washington, NJ, 1994.

[Ka2] ———, *Fields and Rings.* Second ed. Chicago Lectures in Mathematics, University of Chicago Press, Chicago 1972.

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press

[RW] J. Ritter and A. Weiss, *The lifted root number conjecture for some cyclic extensions of* $\mathbb{Q}$. Acta Arith. **90**(1999), no. 4, 313–340.

[S] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field.* Invent. Math. **62**(1980/81), no. 2, 181–234.

Institut für theoretische Informatik
und Mathematik
Fakultät für Informatik
Universität der Bundeswehr München
85579 Neubiberg
Germany
e-mail: cornelius.greither@unibw.de

Přírodovědecká fakulta
Masarykova univerzita
Janáčkovo nám. 2a
60200 Brno
Czech Republic
e-mail: kucera@math.muni.cz

https://doi.org/10.4153/CJM-2006-024-2 Published online by Cambridge University Press