ACTA ARITHMETICA
112.2 (2004)

Annihilators for the class group of a cyclic field of prime power degree

by

C. Greither (Neubiberg) and R. Kučera (Brno)

Introduction. It is well known that the theory of Euler systems produces bounds on the size of the class group of suitable number fields K. The word "size" means here just the order of the class group, or the order of the χ-part of the p-primary part of the class group of K, where χ is a character of the Galois group G of the field K over some other field, and the order of G is prime to p. We are interested in a more general situation where p may divide the order of G. The first substitute for the "size" that comes to mind is the $\mathbb{Z}_p[G]$-Fitting ideal of the p-part of the class group, but it is doubtful whether the standard method of Kolyvagin and Rubin (see for instance [R2]) is able to produce bounds on Fitting ideals in general, the main problem being that the inductive step of Kolyvagin amounts to a reduction to the case of a module which is cyclic over $\mathbb{Z}_p[G]$, and in general one cannot calculate Fitting ideals by multiplicativity and reduction to the cyclic case.

On the other hand, the first step in the Euler system method, in other words, Thaine's construction [Th] of annihilators (as generalized by Rubin [R1]) works over $\mathbb{Z}_p[G]$ from the very start and thus produces $\mathbb{Z}_p[G]$-annihilators when given so-called special units as input. Again, the standard source of special units are cyclotomic units (and elliptic units). So what else is there to say on annihilators?

In this paper we study G-abelian extensions $K/\mathbb{Q}$ for which the obvious choice of a special unit (to wit, the conductor-level Sinnott unit) would lead to an annihilation statement that is far too weak. The main reason for this is that in our examples the class group has a big predictable piece which is a G-trivial module, by genus theory. So we try to find better special units (or rather numbers), by extracting certain deep roots of the obvious special unit.

2000 *Mathematics Subject Classification*: 11R20, 11R27, 11R29.

Key words and phrases: annihilators, class group, cyclotomic units, cyclic fields.

The second author was supported by the project MSM 143100009 of the Ministry of Education of the Czech Republic.

Our main result seems to be optimal in general. This is to say that we cannot expect anything better if the non-genus part of the class group is cyclic. If that group is non-cyclic, it is reasonable to expect that its annihilator will be strictly larger than the lower bound given by our theorem.

The construction of these new special numbers is non-obvious and tricky; it goes back to methods of [GK], and we give full details for the reader's convenience, even in places where the changes with respect to [GK] are small. We are actually forced to work with a somewhat clumsy weakened notion of specialness, since our new numbers are not special in Rubin's sense, and even the proof of the weaker property requires some work. Finally the standard machinery of Thaine and Rubin has (of course) to be adapted in several places. In particular one has to be very careful in the choice of the map α (notation of [R1]) and in the application of Chebotarev's theorem; loosely speaking, we are but just able to make it. To conclude, let us remark that we really have to work with special numbers that are not units; Rubin raised the question in [R1] whether there was any need for such non-units, remarking that there were no such cases known at that time.

Our setting and our results will be explained in detail presently, in Section 1. Notation will be introduced as needed, but we mention here a frequently used shorthand: for any abelian group X, by X/M we mean X/X^M, if X is written multiplicatively, and we mean X/MX, if X is written additively. This is used as well when X is a ring; then of course X/M is again a ring.

1. Formulation of the problem and the result. Let p be an odd prime, $l = p^k$ with k an arbitrary positive integer, $s \geq 2$, $p_1, \ldots, p_s$ be different primes all congruent to 1 modulo l. Suppose that $K/\mathbb{Q}$ is a cyclic extension of degree l, totally ramified at each p_i, unramified outside $\{p_1, \ldots, p_s\}$.

Let $\mathcal{C}l(K)$ be the class group of K and $h(K) = |\mathcal{C}l(K)|$ the class number, let $\mathcal{C}l(K)_p$ and $h(K)_p$ denote the corresponding p-parts. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ be the Galois group of K and $\sigma \in G$ a fixed generator. Let $\mathfrak{p}_i$ be the prime of K above p_i for any $i = 1, \ldots, s$. Let $\mathrm{N} = \sum_{\tau \in G} \tau$ be the norm operator. The ring S is defined to be $S = \mathbb{Z}_p[G]/(\mathrm{N})$.

Let $E = \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K^*$ be the p-adic completion of the group of units of K. Let η denote the "Sinnott circular unit of conductor level", i.e.

$$\eta = \mathrm{N}_{\mathbb{Q}(\zeta_{p_1 \ldots p_s})/K}(1 - \zeta_{p_1} \ldots \zeta_{p_s}),$$

where ζ_n means a fixed nth root of unity. By abuse of notation we shall denote by η also its image in E. By $\langle \eta \rangle$ we understand the $\mathbb{Z}_p[G]$-span of η in E.

For any $i = 1, \ldots, s$, let K_i be the unique absolute degree l field of conductor p_i. Let $\overline{K}$ be the compositum of these fields for $i = 1, \ldots, s$. By

considering ramification indices over $\mathbb{Q}$, it is easy to see that $\overline{K}$ is the genus field of K. For any $i = 1, \ldots, s$, let $\sigma_i \in \mathrm{Gal}(\overline{K}/\mathbb{Q})$ be the automorphism determined by the following conditions: σ_i has trivial restriction to each K_j, $j \neq i$, and the restriction of σ_i to K is σ. Then the restriction of σ_i to K_i generates $\mathrm{Gal}(K_i/\mathbb{Q})$. We define an $s \times s$ matrix $A = (a_{ij})_{1 \leq i,j \leq s}$ over $\mathbb{Z}/l\mathbb{Z}$ in the following way: the non-diagonal entries are given by the condition that the restriction of $\sigma_j^{a_{ij}}$ is the Frobenius automorphism of p_i in K_j. The diagonal entries are chosen such that the matrix A has zero row sums: $a_{ii} = -\sum_{j \neq i} a_{ij}$.

Definition. We say that K satisfies the *Minors Condition* if $A_i = 0$ for each $i = 1, \ldots, s$, where $A_i \in \mathbb{Z}$ is the lift of the (i,i)th minor of the matrix A satisfying $0 \leq A_i < l$.

Theorem 1. *There is $\varepsilon \in K^*$ which is a unit outside of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ such that*

$$\varepsilon^{(\sigma-1)^{s-1}} = \eta$$

and

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

Moreover $\varepsilon \in \mathcal{O}_K^*$ if and only if the Minors Condition holds for K.

In both cases, i.e. whether the Minors Condition holds true for K or not, we have $\varepsilon^{\sigma-1} \in E$, so we can consider $E/\langle \varepsilon^{\sigma-1} \rangle$. We remind the reader that for any S-module X, the ideal $\mathrm{Ann}_S(X)$ is just the set $\{s \in S : sX = 0\}$. We shall prove the following

Theorem 2. $\mathrm{Ann}_S(E/\langle \varepsilon^{\sigma-1} \rangle) \subseteq \mathrm{Ann}_S((\sigma-1)\mathcal{C}\ell(K)_p)$.

Comment. One may call $(\sigma-1)\mathcal{C}\ell(K)_p$ the non-genus part of $\mathcal{C}\ell(K)_p$, and one may ask whether the S-Fitting ideal of $(\sigma-1)\mathcal{C}\ell(K)_p$ is equal to $\mathrm{Ann}_S(E/\langle \varepsilon^{\sigma-1} \rangle)$. We have

$$\mathrm{Ann}_S(E/\langle \varepsilon^{\sigma-1} \rangle) = \mathrm{Fit}_S(E/\langle \varepsilon^{\sigma-1} \rangle),$$
$$\mathrm{Ann}_S((\sigma-1)\mathcal{C}\ell(K)_p) \supseteq \mathrm{Fit}_S((\sigma-1)\mathcal{C}\ell(K)_p),$$

where the second formula is a general property of Fitting ideals and the first formula will be explained in the following Remark. If $(\sigma-1)\mathcal{C}\ell(K)_p$ is cyclic, then equality holds in the second formula as well, and we shall see in the following Remark that in this case the inclusion of Theorem 2 is also an equality. Taking all this together we infer that if $(\sigma-1)\mathcal{C}\ell(K)_p$ is cyclic, we do get equality of the Fitting ideals of $(\sigma-1)\mathcal{C}\ell(K)_p$ and $E/\langle \varepsilon^{\sigma-1} \rangle$. Similarly, we have this equality of Fitting ideals if $l = p$, since in this case S is a discrete valuation ring, and the two modules involved have the same

cardinality, as explained in the following Remark. But we have no idea how to approach this question in general.

REMARK. Since all primes which ramify in K are totally and tamely ramified, the intersection of any cyclotomic field with K equals either K or $\mathbb{Q}$. Therefore the Sinnott group of circular units is generated by -1 and by all conjugates of η. Sinnott's Class Number Formula (see [S, Theorem 4.1, p. 207]) gives

$$(E : \langle\eta\rangle) = l^{-1}h(K)_p,$$

where we have used Theorem 5.3 on p. 221 of [S] to see that the index $(R : U) = 1$ since K is cyclic. Since $\langle\varepsilon^{\sigma-1}\rangle$ is a free S-module of rank one,

$$(\langle\varepsilon^{\sigma-1}\rangle : \langle\eta\rangle) = (\langle\varepsilon^{\sigma-1}\rangle : \langle\varepsilon^{(\sigma-1)^{s-1}}\rangle) = (S : (\sigma-1)^{s-2}) = l^{s-2}.$$

Hence

$$(E : \langle\varepsilon^{\sigma-1}\rangle) = l^{1-s}h(K)_p. \tag{1}$$

Let H be the p-class field of K, so $\mathrm{Gal}(H/K) \cong \mathcal{C}l(K)_p$. Since the degree of the genus field $\overline{K}$ over K is a p-power, $\overline{K}$ is a subfield of H. On the other hand, the largest subfield of H which is absolutely abelian corresponds to the largest quotient of $\mathrm{Gal}(H/K)$ on which G acts trivially, that is, to $\mathcal{C}l(K)_p/(\sigma-1)\mathcal{C}l(K)_p$. Therefore

$$\mathrm{Gal}(H/\overline{K}) = (\sigma-1)\,\mathrm{Gal}(H/K) \cong (\sigma-1)\mathcal{C}l(K)_p.$$

Thus

$$\begin{aligned}|(\sigma-1)\mathcal{C}l(K)_p| &= |\mathrm{Gal}(H/\overline{K})| = [H:K]/[\overline{K}:K] = [H:K]/l^{s-1}\\ &= l^{1-s}h(K)_p.\end{aligned}$$

Consequently, the two modules involved in Theorem 2 have the same cardinality. This shows the theorem is in some sense optimal. If $(\sigma-1)\mathcal{C}l(K)_p$ is S-cyclic, we can be more specific:

$$(S : \mathrm{Ann}_S((\sigma-1)\mathcal{C}l(K)_p)) = |(\sigma-1)\mathcal{C}l(K)_p|.$$

Moreover the Pontryagin dual of $E/\langle\varepsilon^{\sigma-1}\rangle$ is S-cyclic. (This follows from [Sch, Theorem 2.2]; let us briefly give the argument. Let $B = E/\langle\varepsilon^{\sigma-1}\rangle$ and pick $M \in \mathbb{Z}$ large enough so that $MB = 0$. A quick application of the snake lemma shows that B is isomorphic to the kernel of the obvious map $i : C/M \to E/M$ where C is short for $\langle\varepsilon^{\sigma-1}\rangle$. Now the ring S/M is Gorenstein, and C/M is free cyclic over it. Taking Pontryagin duals shows that B^{du} is isomorphic to the cokernel of i^{du}, and the target module of i^{du} is $(C/M)^{\mathrm{du}}$ which is again free cyclic over S/M by the Gorenstein property.) Therefore we obtain

$$(S : \mathrm{Ann}_S(E/\langle\varepsilon^{\sigma-1}\rangle)) = |E/\langle\varepsilon^{\sigma-1}\rangle|$$

as well. Hence the inclusion of Theorem 2 becomes an equality in this case.

Let for the moment $X = E/\langle\varepsilon^{\sigma-1}\rangle$. Then X and X^{du} have the same annihilator, and they also have the same Fitting ideal over S, since they have the same Fitting ideal over $\mathbb{Z}_p[G]$ by cyclicity of G (see Eisenbud's appendix in [MW]). This and the cyclicity of X^{du} imply that $\mathrm{Ann}_S(X) = \mathrm{Fit}_S(X)$, which was already used in the Comment after Theorem 2.

Let us conclude this Remark by saying that $\mathcal{C}l(K)_p$ is cyclic if and only if $s \le 2$; actually it is zero for $s = 1$.

Theorem 2 will be proved by showing the equivalent statement

$$(\sigma - 1)\,\mathrm{Ann}_S(E/\langle\varepsilon^{\sigma-1}\rangle) \subseteq \mathrm{Ann}_S(\mathcal{C}l(K)_p). \tag{2}$$

We now prepare for the proof of (2). The main ingredients come from the annihilation theorems of Thaine and Rubin. In particular we need a technical variant of Rubin's special units.

Definition. 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 $\varepsilon' \in K^*$ will be 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 $\widetilde{q}$ is the product of all primes of $K(q)$ dividing q, then ε' and ε_q have the same image in $(\mathcal{O}_{K(q)}/\widetilde{q})^*/(M/l^{s-1})$ ("congruence condition").

Remark. Rubin's special units are M-semispecial for any p-power M that is divisible by l^{s-1}.

We want to prove:

Theorem 3. *ε (see Theorem 1) is M-semispecial for all p-powers M with $l^{s-1} \mid M$.*

We mention that if the Minors Condition above fails, then ε is a non-unit, and that Rubin remarked in [R1] that so far special non-units apparently had not come in useful.

Theorem 4. *Let $\varepsilon' \in K^*$ be a unit outside of $\{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ and M-semispecial for all sufficiently large p-powers M. Let $E/\langle(\varepsilon')^{\sigma-1}\rangle$ be finite. If $\beta \in \mathrm{Ann}_S(E/\langle(\varepsilon')^{\sigma-1}\rangle)$, then $(\sigma - 1)\beta$ annihilates $\mathcal{C}l(K)_p$.*

These two theorems taken together with (1) prove (2) and hence Theorem 2.

2. Cyclotomic units. Fix an odd prime p, some p-power $l = p^k$, integers $1 < s \le s'$ and a high power L of p such that $l \mid L$. Let $p_1, \dots, p_{s'}$ be different primes all congruent to 1 modulo l. Put $I = \{1, \dots, s\}$ and $I' = \{s+1, \dots, s'\}$. Assume that $p_i \equiv 1 \pmod{L}$ for each $i \in I'$. There is a reason for this non-symmetry: later on we shall apply results of this section to a situation, where the primes $p_1, \dots, p_s$ will be given, while I' will either be empty or contain just one auxiliary prime.

For any $i \in I \cup I'$ let ζ_i be a fixed p_ith primitive root of unity. For any $i \in I$ let K_i be the unique degree l subfield of $\mathbb{Q}(\zeta_i)$, while for any $i \in I'$ we let K_i be the unique degree L subfield of $\mathbb{Q}(\zeta_i)$. For any subset $J \subseteq I \cup I'$ we define $\zeta_J = \prod_{i \in J} \zeta_i$. Let C be the group of circular numbers of $\mathbb{Q}(\zeta_{I \cup I'})$, i.e., the subgroup of $\mathbb{Q}(\zeta_{I \cup I'})^\times$ generated by all non-zero $1 - \zeta_{I \cup I'}^a$ with $a \in \mathbb{Z}$. (Thus the intersection of C and the group E of all units of $\mathbb{Q}(\zeta_{I \cup I'})$ is the group of circular units of $\mathbb{Q}(\zeta_{I \cup I'})$.) Let $\widetilde{G} = \mathrm{Gal}(\mathbb{Q}(\zeta_{I \cup I'})/\mathbb{Q})$. For any $i \in I \cup I'$ let $\sigma_i \in \widetilde{G}$ be a fixed generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_{I \cup I'})/\mathbb{Q}(\zeta_{(I \cup I') - \{i\}}))$.

Let

$$R = \prod_{i \in I'} \sum_{b=1}^{(p_i - 1)/L} \sigma_i^{bL},$$

so $R = 1$ if $I' = \emptyset$. For any $i \in I$ we define

$$T_i = \sum_{b=1}^{(p_i - 1)/l} \sigma_i^{bl}, \qquad \mathrm{N}_i = \sum_{a=1}^{l} \sigma_i^a.$$

It is easy to see that R can be understood as the norm operator from $\mathbb{Q}(\zeta_{I'})$ to the compositum K' of all fields K_j, $j \in I'$. Similarly, for each $i \in I$, the norm operator from $\mathbb{Q}(\zeta_i)$ to K_i is T_i.

For any $J \subset I$ such that $J \cup I' \neq \emptyset$ let

$$\alpha_J = \mathrm{N}_{\mathbb{Q}(\zeta_{J \cup I'})/K' \prod_{i \in J} K_i} (1 - \zeta_{J \cup I'}) = (1 - \zeta_{J \cup I'})^{R \prod_{i \in J} T_i}.$$

We define the polynomial $f(t) \in \mathbb{Z}[x]$ by means of the sequence d_c, defined in [GK, p. 740], as follows:

$$f(t) = \sum_{i=1}^{s-1} (-l)^{i-1} d_{s-1-i} \binom{t+i-1}{i}.$$

Let $f^{(n)}(t)$ be the nth difference of $f(t)$, i.e. $f^{(n)}(t) = f^{(n-1)}(t) - f^{(n-1)}(t-1)$ for any positive integer n, and $f^{(0)}(t) = f(t)$. For any $J \subseteq J_1 \subseteq I$ let

$$\varrho_{J_1, J}^{(n)} = \sum_{x \colon J_1 \to \{0, 1, \dots, l-1\}} (-1)^n f^{(n)} \Big(\sum_{i \in J} x(i) \Big) \prod_{i \in J_1} \sigma_i^{x(i)} \in \mathbb{Z}[G].$$

Recall the definition of the $s \times s$ matrix $A = (a_{ij})_{1 \le i,j \le s}$. The non-diagonal entries are given by the condition that the restriction of $\sigma_j^{a_{ij}}$ is the

Frobenius automorphism of p_i in K_j. The diagonal entries are chosen so as the matrix A has zero row sums: $a_{ii} = -\sum_{j\neq i} a_{ij}$.

Let $J \subseteq I$ and let T be a tree on J with root $r \in J$ (i.e., a directed graph with the set of vertices J without circuits such that the out-degree of r is 0 and out-degree of any other vertex equals 1). We denote the root r of T by $\sqrt{T}$ and define

$$A(T) = \prod_{(i,j)\in E(T)} a_{ij},$$

where (i,j) means the edge going from i to j and runs through the set $E(T)$ of all edges of T.

Let us make the following

ASSUMPTION 5. *For each $i \in I$ and $j \in I'$, the Frobenius automorphism of p_i is trivial on K_j.*

LEMMA 6. *If $s > 1$ then the $(s-1)$th difference of $f(t)$ is a constant polynomial $f^{(s-1)}(t) = (-l)^{s-2}$ and*

$$f(t) - f(t-l) = l^{s-1} \sum_{n=0}^{s-2} (-1)^n \binom{t}{n} \binom{l-n-1}{s-2-n}. \tag{3}$$

Proof. An easy observation shows that for any integers a, b with $b \geq 1$ we have

$$\binom{t+a}{b}^{(1)} = \binom{t+a-1}{b-1} \quad \text{and} \quad \binom{t+a}{0}^{(1)} = 0.$$

So

$$f^{(s-1)}(t) = \sum_{i=1}^{s-1} (-l)^{i-1} d_{s-1-i} \binom{t+i-1}{i}^{(s-1)} = (-l)^{s-2}.$$

The proof of (3) is given by induction with respect to s. Since we need to consider the polynomial $f(t)$ for different s at the same time, we shall write $f_s(t)$ instead of $f(t)$ during the proof. Suppose first that $s = 2$. Then $f_2(t) = t$, so $f_2(t) - f_2(t-l) = l$, which equals the right hand side of (3).

We shall suppose now that $s > 2$ and that (3) has been proved for $s-1$. Let us compute the first difference of $f_s(t)$:

$$\begin{aligned} f_s^{(1)}(t) &= \sum_{i=1}^{s-1} (-l)^{i-1} d_{s-1-i} \binom{t+i-2}{i-1} = d_{s-2} + \sum_{i=1}^{s-2} (-l)^i d_{s-2-i} \binom{t+i-1}{i} \\ &= d_{s-2} - l f_{s-1}(t). \end{aligned}$$

Therefore $f_s^{(1)}(t) - f_s^{(1)}(t-l) = -lf_{s-1}(t) + lf_{s-1}(t-l)$ and the induction hypothesis gives

$$\begin{aligned}
f_s^{(1)}(t) - f_s^{(1)}(t-l) &= -l^{s-1}\sum_{n=0}^{s-3}(-1)^n\binom{t}{n}\binom{l-n-1}{s-3-n} \\
&= -l^{s-1}\binom{l-1}{s-3} - l^{s-1}\sum_{n=1}^{s-3}(-1)^n\left(\binom{t-1}{n-1}+\binom{t-1}{n}\right)\binom{l-n-1}{s-3-n} \\
&= -l^{s-1}\sum_{n=1}^{s-3}(-1)^n\binom{t-1}{n-1}\binom{l-n-1}{s-3-n} \\
&\quad - l^{s-1}\sum_{n=1}^{s-2}(-1)^{n-1}\binom{t-1}{n-1}\binom{l-n}{s-2-n} \\
&= l^{s-1}\sum_{n=1}^{s-3}(-1)^n\binom{t-1}{n-1}\left(-\binom{l-n-1}{s-3-n}+\binom{l-n}{s-2-n}\right) \\
&\quad + l^{s-1}(-1)^{s-2}\binom{t-1}{n-1} \\
&= l^{s-1}\sum_{n=1}^{s-2}(-1)^n\binom{t-1}{n-1}\binom{l-n-1}{s-2-n} \\
&= \left(l^{s-1}\sum_{n=0}^{s-2}(-1)^n\binom{t}{n}\binom{l-n-1}{s-2-n}\right)^{(1)}.
\end{aligned}$$

Therefore there is a constant c such that

$$f_s(t) - f_s(t-l) = c + l^{s-1}\sum_{n=0}^{s-2}(-1)^n\binom{t}{n}\binom{l-n-1}{s-2-n}. \tag{4}$$

To finish the proof of (3) we need to show that $c = 0$. Let us substitute $t = l-1$ into (4). It is easy to see that

$$f_s(-1) = \sum_{i=1}^{s-1}(-l)^{i-1}d_{s-1-i}\binom{i-2}{i} = -d_{s-2}$$

and using Lemma 3 of [GK] we obtain

$$f_s(l-1) = \sum_{i=1}^{s-1}(-l)^{i-1}d_{s-1-i}\binom{l+i-2}{i}$$

$$= (l-1)d_{s-2} + \sum_{i=0}^{s-3} (-l)^{i+1} d_{s-3-i} \binom{l+i}{i+2}$$
$$= (l-1)d_{s-2} + (-l)d_{s-2} = -d_{s-2}.$$

Now, let us compute the sum on the right hand side of (4) for $t = l-1$. If $n \geq l$ then $\binom{l-1}{n} = 0$. If $n < l$ and $s > l+1$ then $\binom{l-n-1}{s-2-n} = 0$. So the sum equals zero if $s > l+1$. Let us now consider the case $s \leq l+1$:

$$\sum_{n=0}^{s-2} (-1)^n \binom{l-1}{n} \binom{l-n-1}{s-2-n}$$
$$= \sum_{n=0}^{s-2} (-1)^n \frac{(l-1)!(l-1-n)!}{n!(l-1-n)!(s-2-n)!(l-s+1)!}$$
$$= \sum_{n=0}^{s-2} (-1)^n \frac{(s-2)!(l-1)!}{n!(s-2-n)!(s-2)!(l-s+1)!}$$
$$= \binom{l-1}{s-2} \sum_{n=0}^{s-2} (-1)^n \binom{s-2}{n} = 0.$$

The lemma is proved. ∎

Corollary 7. *For any integer a and any $n \geq 0$ we have*

$$f^{(n)}(a) \equiv f^{(n)}(a-l) \pmod{l^{s-1}}.$$

Definition. Define

$$T = \prod_{i \in I} T_i, \quad \Gamma = \sum_{\substack{(j_1,\dots,j_s) \in \{0,1,\dots,l-1\}^s \\ l \mid j_1+\dots+j_s}} \prod_{i \in I} \sigma_i^{j_i}, \quad \Delta = \sum_{a=1}^{l-1} a\sigma_1^a.$$

Remark. Γ can be understood as the norm operator from $K' \prod_{i \in I} K_i$ to $K'K$, where K is the subfield of $\prod_{i \in I} K_i$ determined by $\mathrm{Gal}(\prod_{i \in I} K_i / K) = \langle \sigma_i \sigma_1^{-1};\ i \in I \rangle$.

Theorem 8. *Suppose that Assumption 5 holds and $s > 1$. Define $\beta = (1 - \zeta_{I \cup I'})^{RT\Gamma\Delta^{s-1}}$. If $I' \neq \emptyset$ then $\beta \in C^{l^{s-1}}$. If $I' = \emptyset$ then*

$$\beta \equiv \prod_{i \in I} p_i^{(-l)^{s-2} A_i} \pmod{C^{l^{s-1}}},$$

where A_i is a lift of the (i,i)th minor of matrix A.

Proof. We have $\beta = \alpha_I^{\Gamma\Delta^{s-1}}$. Consider the identity given by Lemma 7 of [GK] for $c = s-1$:

$$\Gamma\Delta^{s-1} = (-l)^{s-1}\Gamma_{s-1} - \frac{1}{l}\left(d_{s-1} - \binom{l}{2}^{s-1}\right)\Phi_0 + \sum_{i=1}^{s-1}(-l)^{i-1}d_{s-1-i}\Phi_i,$$

where

$$\Phi_0 = \sum_{t=0}^{s(l-1)} S_t \quad \text{and} \quad \Phi_i = \sum_{t=0}^{s(l-1)} S_t\binom{t+i-1}{i}$$

with

$$S_t = \sum_{\substack{(j_1,\dots,j_s)\in\{0,1,\dots,l-1\}^s \\ j_1+\dots+j_s=t}} \prod_{i=1}^{s}\sigma_i^{j_i}.$$

We have $\alpha_I^{(-l)^{s-1}\Gamma_{s-1}} \in C^{l^{s-1}}$ because $\Gamma_{s-1} \in \mathbb{Z}[G]$. Moreover $\Phi_0 = \prod_{i\in I} \mathrm{N}_i$, so $s > 1$ gives $\alpha_I^{\Phi_0} = 1$, where we have used Assumption 5 if $I' \neq \emptyset$. Finally,

$$\sum_{i=1}^{s-1}(-l)^{i-1}d_{s-1-i}\Phi_i = \varrho_{I,I}^{(0)}.$$

Therefore

$$\beta \equiv \alpha_I^{\varrho_{I,I}^{(0)}} \pmod{C^{l^{s-1}}}. \tag{5}$$

Let us begin by the easy observation that for any non-zero $a \in \mathbb{Z}$ and any non-constant polynomial $g(t) \in \mathbb{Z}[t]$ of degree d, the polynomial $g(t)-g(t-a)$ is of degree $d-1$. Therefore, since $f^{(s-1)}(t)$ is a constant non-zero polynomial by Lemma 6, for any $0 \le n < s-1$ the polynomial $f^{(n)}(t)$ is of degree $s-1-n$.

Let $\emptyset \neq J_1 \subseteq I$. For any polynomial $g(t) \in \mathbb{Z}[t]$ of degree d, we easily show by induction that for any mapping $x : J_1 \to \mathbb{Z}$,

$$\sum_{J\subseteq J_1}(-1)^{|J|}g\Big(t + \sum_{i\in J} x(i)\Big)$$

is a polynomial of degree at most $d - |J_1|$. Therefore

$$\sum_{J\subseteq J_1}(-1)^{|J|}f^{(s-|J_1|)}\Big(\sum_{i\in J} x(i)\Big) = 0,$$

which gives

$$\sum_{J\subseteq J_1}(-1)^{|J|}\varrho_{J_1,J}^{(s-|J_1|)}$$
$$= \sum_{x:\, J_1\to\{0,1,\dots,l-1\}}\Big(\prod_{i\in J_1}\sigma_i^{x(i)}\Big)\sum_{J\subseteq J_1}(-1)^{s-|J_1|+|J|}f^{(s-|J_1|)}\Big(\sum_{i\in J} x(i)\Big) = 0.$$

Suppose that $J \subsetneq J_1$. We have $\varrho_{J_1,J}^{(s-|J_1|)} = \varrho_{J,J}^{(s-|J_1|)} \prod_{i\in J_1-J} \mathrm{N}_i$. If $J \cup I' \neq \emptyset$ then

$$\alpha_{J_1}^{\varrho_{J_1,J}^{(s-|J_1|)}} = \alpha_{J_1}^{\varrho_{J,J}^{(s-|J_1|)} \prod_{i\in J_1-J} \mathrm{N}_i} = \alpha_J^{\varrho_{J,J}^{(s-|J_1|)} \prod_{i\in J_1-J} (\mathrm{Frob}(p_i)-1)}.$$

Therefore, by Assumption 5, if $J = \emptyset$ and $I' \neq \emptyset$ then

$$\alpha_{J_1}^{\varrho_{J_1,\emptyset}^{(s-|J_1|)}} = 1.$$

If $J = I' = \emptyset$ and $|J_1| > 1$ then

$$\alpha_{J_1}^{\varrho_{J_1,\emptyset}^{(s-|J_1|)}} = \alpha_{J_1}^{\varrho_{\emptyset,\emptyset}^{(s-|J_1|)} \prod_{i\in J_1} \mathrm{N}_i} = 1.$$

Finally, if $J = I' = \emptyset$ and $J_1 = \{i\}$ then

$$\varrho_{J_1,J}^{(s-|J_1|)} = \varrho_{\{i\},\emptyset}^{(s-1)} = (-1)^{s-1} f^{(s-1)}(0)\mathrm{N}_i = -l^{s-2}\mathrm{N}_i,$$

due to Lemma 6, and

$$\alpha_{J_1}^{\varrho_{J_1,J}^{(s-|J_1|)}} = p_i^{-l^{s-2}}$$

in this case.

We have thus obtained the following result: if $I' \neq \emptyset$ or $|J_1| > 1$ then

$$\alpha_{J_1}^{\varrho_{J_1,J_1}^{(s-|J_1|)}} = \prod_{\emptyset\neq J\subsetneq J_1} \alpha_J^{(-1)^{1+|J_1-J|}\varrho_{J,J}^{(s-|J_1|)} \prod_{i\in J_1-J} (\mathrm{Frob}(p_i)-1)}.$$

Now, suppose that $\emptyset \neq J \subsetneq J_1$. Assumption 5 gives

$$\varrho_{J,J}^{(s-|J_1|)} \prod_{i\in J_1-J} (\mathrm{Frob}(p_i) - 1) = \varrho_{J,J}^{(s-|J_1|)} \prod_{i\in J_1-J} \sum_{j\in J} a'_{i,j}(\sigma_j - 1)$$

for suitable $a'_{i,j} \in \mathbb{Z}[G]$, which are mapped to $a_{i,j}$ by the augmentation map (see [GK, p. 748]). Hence

$$\varrho_{J,J}^{(s-|J_1|)} \prod_{i\in J_1-J} (\mathrm{Frob}(p_i) - 1) = \varrho_{J,J}^{(s-|J_1|)} \sum_{y\colon J_1-J\to J} \prod_{i\in J_1-J} a'_{i,y(i)}(\sigma_{y(i)} - 1)$$

or, writing $y^{-1}(j) = \{i \in J_1 - J : y(i) = j\}$, we have

$$\varrho_{J,J}^{(s-|J_1|)} \prod_{i\in J_1-J} (\mathrm{Frob}(p_i) - 1) = \varrho_{J,J}^{(s-|J_1|)} \sum_{y\colon J_1-J\to J} \Big(\prod_{i\in J_1-J} a'_{i,y(i)} \Big) \prod_{j\in J} (\sigma_j - 1)^{|y^{-1}(j)|}.$$

For any $j \in J$ and any $n \geq s - |J_1|$,

$$\begin{aligned}\sigma_j \varrho_{J,J}^{(n)} &= \sum_{x\colon J \to \{0,1,\dots,l-1\}} (-1)^n f^{(n)}\Big(\sum_{i\in J} x(i)\Big)\sigma_j \prod_{i\in J} \sigma_i^{x(i)} \\ &= \sum_{x\colon J \to \{0,1,\dots,l-1\}} (-1)^n f^{(n)}\Big(\sum_{i\in J} x(i)\Big)\sigma_j^{x(j)+1} \prod_{i\in J-\{j\}} \sigma_i^{x(i)} \\ &= \sum_{x\colon J \to \{0,1,\dots,l-1\}} (-1)^n f^{(n)}\Big(-1+\sum_{i\in J} x(i)\Big) \prod_{i\in J} \sigma_i^{x(i)} \\ &\quad + \sum_{x\colon J-\{j\} \to \{0,1,\dots,l-1\}} (-1)^n d_x \prod_{i\in J-\{j\}} \sigma_i^{x(i)},\end{aligned}$$

where

$$d_x = f^{(n)}\Big(l-1+\sum_{i\in J-\{j\}} x(i)\Big) - f^{(n)}\Big(-1+\sum_{i\in J-\{j\}} x(i)\Big) \equiv 0 \pmod{l^{s-1}}$$

by Corollary 7. Hence

$$(\sigma_j - 1)\varrho_{J,J}^{(n)} \equiv \varrho_{J,J}^{(n+1)} \pmod{l^{s-1}}.$$

Repeating the argument $\sum_{j\in J} |y^{-1}(j)| = |J_1 - J|$ times, we arrive at

$$\varrho_{J,J}^{(s-|J_1|)} \prod_{i\in J_1-J} (\mathrm{Frob}(p_i) - 1) \equiv \varrho_{J,J}^{(s-|J|)} \sum_{y\colon J_1-J\to J} \prod_{i\in J_1-J} a'_{i,y(i)} \pmod{l^{s-1}}.$$

Putting things together, we have obtained: if $I' \neq \emptyset$ or $|J_1| > 1$ then

$$\alpha_{J_1}^{\varrho_{J_1,J_1}^{(s-|J_1|)}} \equiv \prod_{\emptyset\neq J\subsetneq J_1} \alpha_J^{(-1)^{1+|J_1-J|}\varrho_{J,J}^{(s-|J|)}\sum_{y\colon J_1-J\to J}\prod_{i\in J_1-J} a'_{i,y(i)}} \pmod{C^{l^{s-1}}}, \tag{6}$$

while if $I' = \emptyset$ and $J_1 = \{i\}$ then

$$\alpha_{J_1}^{\varrho_{J_1,J_1}^{(s-|J_1|)}} = \alpha_{J_1}^{\varrho_{J_1,\emptyset}^{(s-|J_1|)}} = p_i^{-l^{s-2}} \tag{7}$$

in this case.

By induction we shall prove that for any $J \subseteq I$, $J \neq \emptyset$, we have $\alpha_J^{\varrho_{J,J}^{(s-|J|)}} \in C^{l^{s-1}}$ if $I' \neq \emptyset$, and

$$\alpha_J^{\varrho_{J,J}^{(s-|J|)}} \equiv \prod_{i\in J} p_i^{-l^{s-2}b_i} \pmod{C^{l^{s-1}}} \tag{8}$$

if $I' = \emptyset$, where

$$b_i = \sum_{T \text{ a tree on } J,\ \sqrt{T}=i} A(T),$$

the summation running over all trees T on J with root i.

Consider the $I'=\emptyset$ case first. If $J=\{i\}$ then there is just one tree T on J with $A(T)=1$, so the statement follows from (7). Suppose that $J_1 \subseteq I$, $|J_1|>1$ and that for all non-empty proper subsets of J_1 the statement has been proved. Using the induction hypothesis we make the substitution (8) on the right hand side of (6). We need to show that for each $i \in J_1$,

$$b_i \equiv \sum_{J \subsetneq J_1,\, i \in J} (-1)^{1+|J_1-J|} \sum_{\substack{T \text{ a tree on } J \\ \sqrt{T}=i}} A(T) \sum_{y\colon J_1-J \to J} \prod_{i \in J_1-J} a_{i,y(i)} \pmod{l^{s-1}}$$

(recall that $a'_{i,y(i)}$ goes to $a_{i,y(i)}$ under the augmentation map). It is clear that the function y describes how to add leaves to the tree T to obtain a new tree on the whole set J_1. Moreover, the same tree on J_1 can be obtained for different subsets J. Fix a tree T_1 on J_1 with the set J_0 of leaves. We see that we obtain T_1 from a unique subtree T on J for each $J \subsetneq J_1$ satisfying $J_1 - J \subseteq J_0$ and that the common summand of all these subtrees is

$$\sum_{J \subsetneq J_1,\, J_1-J \subseteq J_0} (-1)^{1+|J_1-J|} A(T_1) = A(T_1) \sum_{\emptyset \neq J_2 \subseteq J_0} (-1)^{1+|J_2|} = A(T_1).$$

The case $I'=\emptyset$ is proved. The other case can be proved similarly.

The theorem follows from (5), (8) for $J=I$, and, in the $I'=\emptyset$ case, the Kirchhoff–Tutte theorem as stated in [GK, p. 756]. ∎

3. Proof of Theorem 1. We shall use Theorem 8 for $I=\{1,\dots,s\}$ and $I'=\emptyset$. Then $\eta=\alpha_I^\Gamma$, and Theorem 8 implies that $\beta=\eta^{\Delta^{s-1}}$ satisfies

$$\beta \equiv \prod_{i=1}^{s} p_i^{(-l)^{s-2}A_i} \pmod{C^{l^{s-1}}},$$

where $A_i \in \mathbb{Z}$ is the lift of the (i,i)th minor of the matrix A satisfying $0 \le A_i < l$. Therefore there is $\varepsilon \in \mathbb{Q}(\zeta_{p_1 \dots p_s})$ such that

$$\beta = \varepsilon^{l^{s-1}} \prod_{i=1}^{s} p_i^{(-l)^{s-2}A_i}.$$

Since we work in an absolutely abelian field, l is odd, and $\beta \in K$, we have $\varepsilon \in K$. Since $\eta^{\mathrm{N}}=1$, we have $\eta^{(\sigma-1)\Delta}=\eta^{l-\mathrm{N}}=\eta^l$ and

$$\eta^{l^{s-1}} = \eta^{(\sigma-1)^{s-1}\Delta^{s-1}} = \beta^{(\sigma-1)^{s-1}} = \varepsilon^{l^{s-1}(\sigma-1)^{s-1}},$$

hence $\eta = \varepsilon^{(\sigma-1)^{s-1}}$. Moreover β is a unit, so ε is a unit outside of $\{\mathfrak{p}_1,\dots,\mathfrak{p}_s\}$, and is a unit if and only if K satisfies the Minors Condition. Taking norms gives

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

and Theorem 1 follows.

4. Proof of Theorem 3. Let M be a p-power divisible by l^{s-1}, let $q \in \mathcal{Q}_M$ and

$$\eta_q = \mathrm{N}_{\mathbb{Q}(\zeta_{p_1 \dots p_s}, \zeta_q)/K(q)}(1 - \zeta_{p_1} \dots \zeta_{p_s} \zeta_q).$$

The proof consists of two steps: first, we shall construct ε_q. We use Theorem 8 for $I = \{1, \dots, s\}$ and $I' = \{s+1\}$ with $p_{s+1} = q$ and $L = M$. Then $\eta_q = \alpha_I^{\Gamma}$ and Theorem 8 gives $\beta = \eta_q^{\Delta^{s-1}} \in C^{l^{s-1}}$. Therefore there is $\varepsilon_q \in \mathbb{Q}(\zeta_{p_1 \dots p_s}, \zeta_q)$ such that

$$\eta_q^{\Delta^{s-1}} = \varepsilon_q^{l^{s-1}}. \tag{9}$$

Since we work in an absolutely abelian field, l is odd, and $\eta_q \in \mathcal{O}^*_{K(q)}$, we have $\varepsilon \in \mathcal{O}^*_{K(q)}$.

Lemma 9. $\mathrm{N}_{K(q)/\mathbb{Q}(q)}(\eta_q) = 1$.

Proof. Since the p_i are Mth powers modulo q, their Frobenius is trivial on $\mathbb{Q}(q)$, so the norm relations for cyclotomic units give $\mathrm{N}_{K(q)/\mathbb{Q}(q)}(\eta_q) = 1$. ∎

Lemma 9 gives $\eta_q^{\mathrm{N}} = 1$, so we have $\eta_q^{(\sigma-1)\Delta} = \eta_q^{l-\mathrm{N}} = \eta_q^l$ and

$$\eta_q^{l^{s-1}} = \eta_q^{(\sigma-1)^{s-1}\Delta^{s-1}} = \varepsilon_q^{l^{s-1}(\sigma-1)^{s-1}},$$

so

$$\varepsilon_q^{(\sigma-1)^{s-1}} = \eta_q. \tag{10}$$

Second, we shall now verify that ε_q satisfies the norm condition and the congruence condition.

Remark. In (9) and (10), σ is given on K and acts trivially on the extension $\mathbb{Q}(q)$.

From the standard norm relations for cyclotomic units and the condition "q totally split in K" we obtain $\mathrm{N}_{K(q)/K}(\eta_q) = 1$. From (9) we get

$$\mathrm{N}_{K(q)/K}(\varepsilon_q)^{l^{s-1}} = 1$$

and so $\mathrm{N}_{K(q)/K}(\varepsilon_q) = 1$.

The congruence condition is slightly trickier: let $\widetilde{K} = \mathbb{Q}(\zeta_{p_1}, \dots, \zeta_{p_s})$. Since $\zeta_q \equiv 1$ modulo $\zeta_q - 1$, which generates the prime of $\mathbb{Q}(\zeta_q)$ over q, we have $1 - \zeta_{p_1} \dots \zeta_{p_s} \zeta_q \equiv 1 - \zeta_{p_1} \dots \zeta_{p_s}$ modulo every prime of $\widetilde{K}(\zeta_q)$ over q, so

$$\mathrm{N}_{\widetilde{K}(\zeta_q)/K(\zeta_q)}(1 - \zeta_{p_1} \dots \zeta_{p_s} \zeta_q) \equiv \mathrm{N}_{\widetilde{K}/K}(1 - \zeta_{p_1} \dots \zeta_{p_s}) = \eta$$

modulo every prime of $K(\zeta_q)$ over q, hence

$$\eta_q = \mathrm{N}_{K(\zeta_q)/K(q)}(\mathrm{N}_{\widetilde{K}(\zeta_q)/K(\zeta_q)}(1 - \zeta_{p_1} \dots \zeta_{p_s} \zeta_q)) \equiv \eta^{(q-1)/M}$$

modulo every prime of $K(q)$ over q, but $\eta^{(q-1)/M}$ equals η times an Mth power since $q \equiv 1+M \pmod{M^2}$. This shows: η_q and η have the same image in $X = (\mathcal{O}_{K(q)}/\widetilde{q})^*/M$.

Since $\mathcal{O}_{K(q)}/\widetilde{q} \cong \mathcal{O}_K/q\mathcal{O}_K$ and q is totally split in K, we get $X \cong \mathbb{Z}/M[G]$ as a $\mathbb{Z}[G]$-module. Write the map $\{x \in \mathcal{O}_{K(q)} : (q,x) = 1\} \to X \to \mathbb{Z}/M[G]$ by an overbar. So $\overline{\eta}_q = \overline{\eta}$, and Theorem 1 and (10) give $(\sigma-1)^{s-1}\overline{\varepsilon}_q = (\sigma-1)^{s-1}\overline{\varepsilon}$.

LEMMA 10. *Let $x \in \mathbb{Z}/M[G]$ be in the augmentation kernel and*

$$(\sigma-1)^{s-1}x = 0.$$

Then $x \equiv 0 \pmod{M/l^{s-1}}$.

Proof. Recalling that $(\sigma-1)\Delta = l - \mathrm{N}$ in $\mathbb{Z}[G]$, where $\Delta = \sum_{i=1}^{l-1} i\sigma^i$ and $\mathrm{N} = \sum_{i=0}^{l-1}\sigma^i$, we see that $l^{s-1}x = \Delta^{s-1}(\sigma-1)^{s-1}x = 0$ in $\mathbb{Z}/M[G]$, since $\mathrm{N}x = 0$ in $\mathbb{Z}/M[G]$. ∎

LEMMA 11. $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)$ *is an Mth power modulo q.*

Proof. Theorem 1 gives

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

Since $q \in \mathcal{Q}_M$, the p_i are Mth powers modulo q, and the same holds true for $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon)$. ∎

Notice that $\overline{\varepsilon}_q$ and $\overline{\varepsilon}$ are in the augmentation kernel (for $\overline{\varepsilon}$ see Lemma 11, for $\overline{\varepsilon}_q$ Lemma 9) and Lemma 10 applied to $\overline{\varepsilon}_q - \overline{\varepsilon}$ shows that ε_q and ε have the same image in $X/(M/l^{s-1}) = (\mathcal{O}_{K(q)}/\widetilde{q})^*/(M/l^{s-1})$. Note that we lost the factor l^{s-1} in the passage from $\overline{\eta}_q$, $\overline{\eta}$ to $\overline{\varepsilon}_q$, $\overline{\varepsilon}$.

This concludes the proof of Theorem 3.

5. Proof of Theorem 4. We first translate Theorem 4 into a statement in the spirit of Rubin's Theorem. We keep the notation of the previous sections, so K is a cyclic field of absolute degree $l = p^k$, p being an odd prime, $p_1, \ldots, p_s$, with $s \geq 2$, are primes, which ramify totally and tamely in K, and K is unramified outside $\{p_1, \ldots, p_s\}$. Moreover, $\mathcal{C}l(K)$ is the class group of K and $E = \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K^*$ is the p-adic completion of the group of units of K.

For the rest of the paper, we will tacitly assume that l^{s-1} divides M, and we let $M' = M/l^{s-1}$, without further mention.

THEOREM 12. *Fix a large p-power M. Assume that $\varepsilon' \in K^*$ is M-semi-special, suppose that $V \subseteq K^*/M$ is a finitely generated $\mathbb{Z}_p[G]$-submodule, and that $\varepsilon' \in V$. Let $\alpha : V \to \mathbb{Z}/M[G]$ be a $\mathbb{Z}_p[G]$-linear map such that*

$\alpha(V \cap \mathbb{Q}) = 0$, *where* $V \cap \mathbb{Q}$ *means* $V \cap (\mathbb{Q}^* K^{*M}/K^{*M})$. *Then* $\alpha(\varepsilon')$ *annihilates* $\mathcal{C}l(K)_p/M'$.

Let us prove that Theorem 12 implies Theorem 4. Choose and fix $\beta \in \mathrm{Ann}_S(E/\langle(\varepsilon')^{\sigma-1}\rangle)$. Put $\pi = \varepsilon' \cdot p_1$ if ε' is a unit and $\pi = \varepsilon'$ otherwise. Notice that π is M-semispecial because p_1 is M-semispecial (to show that p_1 is really M-semispecial just take 1 as the corresponding ε_q). Then $\pi^{\sigma-1} = (\varepsilon')^{\sigma-1}$, π is not a unit, but π is a unit outside of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ and

$$E/\langle(\varepsilon')^{\sigma-1}\rangle = E/\langle\pi^{\sigma-1}\rangle = E/(E \cap \langle\pi\rangle) \cong \langle\pi\rangle E/\langle\pi\rangle.$$

So $\beta \in \mathrm{Ann}_S(\langle\pi\rangle E/\langle\pi\rangle)$.

LEMMA 13. *π is not annihilated by any non-zero element of $\mathbb{Z}_p[G]$.*

Proof. Suppose that $\pi^{\varrho} = 1$ for some $\varrho \in \mathbb{Z}_p[G]$. There are $r \in \mathbb{Z}_p$ and $\varrho' \in \mathbb{Z}_p[G]$ satisfying $\varrho = r + (\sigma - 1)\varrho'$. Then $\pi^r \in E$ and so $r = 0$. Let $u \in E$ be a Minkowski unit. Since $E/\langle(\varepsilon')^{\sigma-1}\rangle = E/\langle\pi^{\sigma-1}\rangle$ is finite, there is a positive integer c such that $u^c \in \langle\pi^{\sigma-1}\rangle$, hence there is $\gamma \in \mathbb{Z}_p[G]$ such that $u^c = \pi^{(\sigma-1)\gamma}$. Therefore

$$u^{c\varrho'} = \pi^{(\sigma-1)\varrho'\gamma} = \pi^{\varrho\gamma} = 1.$$

We have shown that ϱ' is a multiple of N and so $\varrho = 0$. ∎

Having $\beta \in \mathrm{Ann}_S(\langle\pi\rangle E/\langle\pi\rangle)$, we construct a map $\alpha_1 : \langle\pi\rangle E \to \mathbb{Z}_p[G]$ as follows: for any $u \in \langle\pi\rangle E$ we have $\beta u \in \langle\pi\rangle$ and the equation $\beta u = \alpha_1(u)\pi$ has a unique solution $\alpha_1(u)$ in $\mathbb{Z}_p[G]$ due to Lemma 13. It is obvious that α_1 is $\mathbb{Z}_p[G]$-linear and $\alpha_1(\pi) = \beta$. Let $\alpha_0 : (\langle\pi\rangle E)/M \to \mathbb{Z}/M[G]$ be the reduction of α_1 modulo M.

Let $\widetilde{V} = (\langle\pi\rangle E)/M$ and V be the image of $\widetilde{V}$ in K^*/M under the canonical mapping $j : \widetilde{V} \to V$.

LEMMA 14. *The kernel* $\ker(j)$ *is a trivial G-module.*

Proof. Let $x = \overline{\pi^z u} \in \ker(j)$, where $u \in E$ and $z \in \mathbb{Z}_p[G]$. Then $\pi^z u = y^M$ for a suitable $y \in K^*$, so

$$x^{\sigma-1} = \overline{\pi^{(\sigma-1)z} u^{\sigma-1}} = \overline{(y^{\sigma-1})^M}.$$

Looking at valuations we see that $y^{\sigma-1}$ is a unit. So $x^{\sigma-1}$ is the trivial element of $\widetilde{V}$. ∎

Recall that we are using Rubin's shorthand $V \cap \mathbb{Q} = V \cap (\mathbb{Q}^* K^{*M}/K^{*M})$.

LEMMA 15. *$V \cap \mathbb{Q}$ is contained in $j(\widetilde{V}^G)$.*

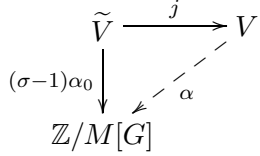
Proof. Let $x \in \langle\pi\rangle E$, $j(\overline{x}) \in V \cap \mathbb{Q}$. So there are $m \in \mathbb{Q}^*$, $y \in K^*$ with $x = m \cdot y^M$. This implies

$$x^{\sigma-1} = (y^{\sigma-1})^M,$$

and as in the last proof $y^{\sigma-1}$ must be a unit. This is enough to show that $\overline{x} \in (\langle\pi\rangle E)/M$ is fixed under σ. ∎

As a consequence we get

PROPOSITION 16. *If $\alpha_0 : \widetilde{V} \to \mathbb{Z}/M[G]$ is any $\mathbb{Z}[G]$-homomorphism, then $(\sigma-1)\alpha_0$ factors through a $\mathbb{Z}[G]$-homomorphism $\alpha : V \to \mathbb{Z}/M[G]$ which has the extra property that $\alpha(V \cap \mathbb{Q}) = 0$.*



Proof. We know that $(\sigma-1)\alpha_0$ annihilates $\ker(j)$ by Lemma 14. Hence α exists. Any $v \in V \cap \mathbb{Q}$ has the form $j(\widetilde{v})$ for some $\widetilde{v} \in \widetilde{V}^G$ by Lemma 15, so $\alpha(v) = \alpha j(\widetilde{v}) = (\sigma-1)\alpha_0(\widetilde{v}) = \alpha_0((\sigma-1)\widetilde{v}) = \alpha_0(0) = 0$. ∎

Now we can use Theorem 12 for the mapping $\alpha : V \to \mathbb{Z}/M[G]$ given by Proposition 16 for the mapping α_0 constructed above, and we deduce that

$$\alpha(\varepsilon') = (\sigma-1)\alpha_0(\varepsilon') = \alpha_0((\sigma-1)\varepsilon') = \alpha_0((\sigma-1)\pi) = (\sigma-1)\alpha_0(\pi),$$

which is the class of $(\sigma-1)\alpha_1(\pi) = (\sigma-1)\beta$ modulo M, annihilates $\mathcal{C}l(K)_p/M'$. We have proved that Theorem 4 follows from Theorem 12: it suffices to take M large enough that M' annihilates $\mathcal{C}l(K)_p$.

The proof of Theorem 12 is very much in the style of Rubin's paper [R1]. A rough outline is as follows:

• Thaine's idea gives principality statements on ideals in K, depending on existence and behaviour of certain units in $K(q)$ ([R1, Theorem 5.1]).

• Roughly speaking, Rubin's Theorem 5.5 (which uses the theorem of Chebotarev) produces enough primes q.

• Then one has to provide the connection between ε' and the units used in the first step ([R1, p. 525]).

Major changes only occur in the second step. We will formulate and prove our version of this second step first:

THEOREM 17. *Fix a p-power M, suppose that $V \subseteq K^*/M$ is a finitely generated $\mathbb{Z}_p[G]$-submodule; assume that $\alpha : V \to \mathbb{Z}/M[G]$ is $\mathbb{Z}_p[G]$-linear and $\alpha(V \cap \mathbb{Q}) = 0$. Then for any $\mathfrak{c} \in \mathcal{C}l(K)_p$ there are infinitely many unramified primes $\mathfrak{q}$ in K of absolute degree 1 satisfying the following conditions, where q is the rational prime below $\mathfrak{q}$:*

(i) $[\mathfrak{q}] = \mathfrak{c}$, *where* $[\mathfrak{q}]$ *is the projection of the ideal class of* $\mathfrak{q}$ *into* $\mathcal{C}l(K)_p$;

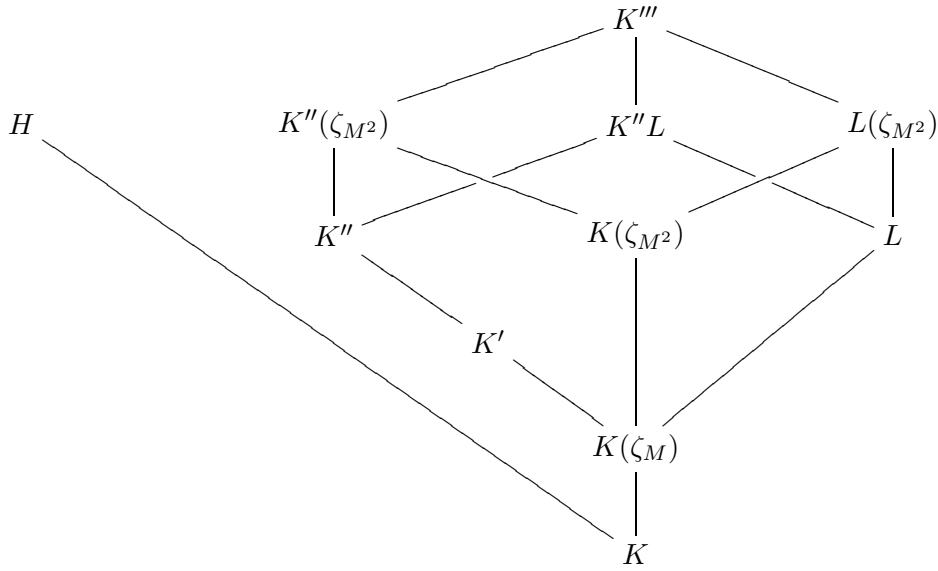
(ii) $q \equiv 1 + M \pmod{M^2}$;

(iii) p_i *is an* M*th power modulo* q *for each* $i = 1, \dots, s$;

(iv) *V has a set of generators whose support does not contain $\mathfrak{q}$, and there is a $\mathbb{Z}_p[G]$-linear map $\varphi : (\mathcal{O}_K/q)^*/M \to \mathbb{Z}/M[G]$ so that a commutative diagram arises (ψ being the reduction map)*

$$\begin{array}{ccc} V & \xrightarrow{\alpha} & \mathbb{Z}/M[G] \\ \downarrow{\scriptstyle \psi} & \nearrow_{\varphi} & \\ (\mathcal{O}_K/q)^*/M & & \end{array}$$

Proof. Let H be the p-Hilbert class field of K; let $K' = K(\zeta_M, \ker(\alpha)^{1/M})$, $K'' = K(\zeta_M, V^{1/M})$, and $L = K(\zeta_M, P^{1/M})$, where $P = p_1^{\mathbb{Z}} \dots p_s^{\mathbb{Z}}$, and finally $K''' = K''L(\zeta_{M^2})$. Consider the following diagram of fields.



Lemma 18. (a) *$K(\zeta_{M^2})$ is the largest subfield of K''' that is abelian over K.*

(b) *$K(\zeta_M)$ is the largest subfield of $K''L$ that is abelian over K.*

(c) *$K''' \cap H = K$.*

Proof. (a) We have an exact sequence of Galois groups

$$1 \to \mathrm{Gal}(K'''/K(\zeta_{M^2})) \to \mathrm{Gal}(K'''/K) \to \mathrm{Gal}(K(\zeta_{M^2})/K) \to 1,$$

where $\mathrm{Gal}(K(\zeta_{M^2})/K) \cong (\mathbb{Z}/M^2)^*$. We have $K''' = K(\zeta_{M^2})(V^{1/M}, P^{1/M})$. By Kummer theory, $B = \mathrm{Gal}(K'''/K(\zeta_{M^2}))$ is an abelian p-group and the action of $(\mathbb{Z}/M^2)^*$ is the cyclotomic one (i.e. the natural one, given by exponentiating: $(\mathbb{Z}/M^2)^* \times B \to B$ sends (u, ϱ) to ϱ^u). (Cf. [R1, Lemma 1.6].) So the coinvariants of B under the action vanish, and the largest abelian quotient of $\mathrm{Gal}(K'''/K)$ is $\mathrm{Gal}(K(\zeta_{M^2})/K)$.

(b) This can be proved by the same reasoning as (a).

(c) By (a) we only need to show that $K(\zeta_{M^2}) \cap H = K$. This is easy since $K(\zeta_{M^2})/K$ is totally ramified at p. ∎

By Chebotarev's theorem and Lemma 18(c) we find that for any $\tau \in \mathrm{Gal}(K'''/K)$ there exist infinitely many degree one primes $\mathfrak{q}$ of K whose Frobenius on K''' is τ and whose class is $\mathfrak{c}$. We shall built a suitable τ in three steps.

First step: Let $e_0 \in \mathrm{Hom}(\mathbb{Z}/M[G], \mu_M)$ be given by

$$e_0\Big(\sum_{i=0}^{l-1} a_i\sigma^i\Big) = \zeta_M^{a_0}.$$

Then e_0 generates $\mathrm{Hom}(\mathbb{Z}/M[G], \mu_M)$ as a $\mathbb{Z}[G]$-module: $\sigma^{-j}e_0$ maps $\sum_{i=0}^{l-1} a_i\sigma^i$ to $\zeta_M^{a_j}$. Therefore the $\mathbb{Z}$-span of the $\sigma^{-j}e_0$, where $j = 1, \dots, l$, is $\mathrm{Hom}(\mathbb{Z}/M[G], \mu_M)$. Moreover, by Kummer theory,

$$\begin{aligned}\mathrm{Gal}(K''/K') &\cong \ker(\mathrm{Hom}(V, \mu_M) \to \mathrm{Hom}(\ker(\alpha), \mu_M)) \\ &\cong \mathrm{Hom}(\mathrm{im}(\alpha), \mu_M),\end{aligned}$$

which is canonically an epimorphic image of $\mathrm{Hom}(\mathbb{Z}/M[G], \mu_M)$. Let τ_1 be the image of e_0 under this isomorphism; so τ_1 is a generator of $\mathbb{Z}[G]$-module $\mathrm{Gal}(K''/K')$.

Next step: We claim τ_1 can be extended to $\tau_2 \in \mathrm{Gal}(K''L/K(\zeta_M))$ so that τ_2 is trivial on L. For this we need that τ_1 is identity on $L \cap K''$. Now by Kummer theory

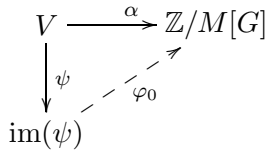
$$L \cap K'' = K(\zeta_M)(P^{1/M}) \cap K(\zeta_M)(V^{1/M}) = K(\zeta_M)((V \cap P)^{1/M}).$$

Since $V \cap P \subseteq V \cap \mathbb{Q}$, and we assumed $\alpha(V \cap \mathbb{Q}) = 0$, we get $L \cap K'' \subseteq K(\zeta_M, \ker(\alpha)^{1/M}) = K'$ as desired.

Last step: We note τ_2 is the identity on $K(\zeta_M)$; we want to extend τ_2 to $\tau \in \mathrm{Gal}(K'''/K)$ so that $\tau(\zeta_{M^2}) = \zeta_{M^2}^{1+M}$. For this it suffices to have $K''L \cap K(\zeta_{M^2}) = K(\zeta_M)$. Indeed, $K(\zeta_{M^2})$ is abelian over K, and by Lemma 18(b) any subfield of $K''L$ that is abelian over K must be contained in $K(\zeta_M)$.

As said above we now pick a degree one prime $\mathfrak{q}$ of K, not over any p_i or p, and such that V has generating set supported outside $\mathfrak{q}$, whose Frobenius in K''' is τ and whose class in $\mathcal{C}\ell(K)_p$ is $\mathfrak{c}$. This already satisfies (i). Let q be the rational prime below $\mathfrak{q}$. The property (ii) now follows from $\tau(\zeta_{M^2}) = \zeta_{M^2}^{1+M}$. For (iii), let $\mathfrak{Q}$ be a prime of $K(\zeta_M)$ above $\mathfrak{q}$; then $\mathfrak{Q}$ is again degree 1 since $\mathfrak{q}$ splits totally in $K(\zeta_M)$. Moreover, $\mathfrak{Q}$ has to split totally in L, by construction of $\mathfrak{q}$. Therefore every p_i has to be an Mth power in the completion $K(\zeta_M)_{\mathfrak{Q}}$ and so in $\mathcal{O}_{K(\zeta_M)}/\mathfrak{Q}$ which is just $\mathbb{Z}/q$. For (iv): Since $\mathbb{Z}/M[G]$ is self-injective, it suffices to find φ_0 which fills the

diagram



Obviously, φ_0 exists if and only if $\ker(\alpha) \supseteq \ker(\psi)$; let us check the latter inclusion. Let $v \in V$; we find

$$\begin{aligned} v \in \ker(\psi) &\Rightarrow \text{locally at every } G\text{-conjugate of } \mathfrak{q},\ v \text{ is an } M\text{th power} \\ &\Rightarrow \text{all } G\text{-conjugates of } \mathfrak{q} \text{ split in } K(\zeta_M, v^{1/M}) \\ &\Rightarrow \text{all } G\text{-conjugates of } \tau_1 \in \mathrm{Gal}(K''/K') \text{ are trivial} \\ &\quad \text{on } K(\zeta_M, v^{1/M}) \\ &\Rightarrow \mathrm{Gal}(K''/K') \text{ acts trivially on } K(\zeta_M, v^{1/M}); \end{aligned}$$

the last implication holds since τ_1 was chosen to be a $\mathbb{Z}[G]$-generator of $\mathrm{Gal}(K''/K')$. Now by Galois theory we obtain

$$\begin{aligned} v \in \ker(\psi) &\Rightarrow K(\zeta_M, v^{1/M}) \subseteq K' = K(\zeta_M, \ker(\alpha)^{1/M}) \\ &\Rightarrow v \in \ker(\alpha) \end{aligned}$$

as desired. Theorem 17 is thus proved. ∎

Before proving Theorem 12, we formulate the required result of Thaine (see [R1, Theorem 5.1]) in the case which we need.

THEOREM 19. *Let q be a rational prime which is totally split in K, and let L be a finite extension of K, abelian over $\mathbb{Q}$, such that only the primes above q in K ramify, but those ramify totally and tamely. Let $\widetilde{q}$ be the product of all primes over q in L, and let $\mathcal{A}$ be the $\mathbb{Z}/(q-1)[G]$-annihilator of the cokernel of the reduction map*

$$\{\overline{\varepsilon} \in \mathcal{O}_L^*;\ \mathrm{N}_{L/K}(\overline{\varepsilon}) = 1\} \to (\mathcal{O}_L/\widetilde{q})^*.$$

(Note that $(\mathcal{O}_L/\widetilde{q})^*$ is free cyclic over $\mathbb{Z}/(q-1)[G]$.) Then for every prime $\mathfrak{q}$ of K over q, $\mathcal{A}$ annihilates $[\mathfrak{q}] \in \mathcal{C}l(K)/[L:K]$.

The given statement is slightly weaker than [R1, Theorem 5.1]. We will apply it with $L = K(q)$.

In order to finally prove Theorem 12, suppose α and ε' are as in its statement. We must prove that the image of any class $\mathfrak{c} \in \mathcal{C}l(K)_p$ in $\mathcal{C}l(K)_p/M'$ is annihilated by $\alpha(\varepsilon')$. To this end we apply Theorem 17. This produces a rational prime q and a degree one prime $\mathfrak{q}$ of K above q, with properties (i)–(iv). Also, there are infinitely many possibilities for q.

Since ε' is supposed to be M-semispecial, we may assume by (ii) and (iii) in Theorem 17 the existence of a unit ε_q in $K(q)$ with $\mathrm{N}_{K(q)/K}(\varepsilon_q) = 1$, and

such that ε' and ε_q have the same image in $(\mathcal{O}_{K(q)}/\widetilde{q})^*/M' \cong (\mathcal{O}_K/q)^*/M'$. Here $K(q) = K\mathbb{Q}(q)$, $\mathbb{Q}(q)$ being the degree M subfield of $\mathbb{Q}(\zeta_q)$. By Theorem 19, the annihilator $\mathcal{A}$ of $\mathcal{B} = (\mathcal{O}_{K(q)}/\widetilde{q})^*/\langle \mathrm{im}(\varepsilon_q)\rangle$ annihilates the class of $\mathfrak{q}$ in $\mathcal{C}l(K)/M$. By property (ii), M is the exact p-power dividing $q-1$. So the p-part of $\mathcal{B}$ is

$$\mathcal{B}/M = ((\mathcal{O}_{K(q)}/\widetilde{q})^*/M)/\langle \mathrm{im}(\varepsilon_q)\rangle,$$

and the projection $\mathcal{A}_p$ of $\mathcal{A}$ to $\mathbb{Z}/M[G]$ is the annihilator of $\mathcal{B}/M$. So $\mathcal{A}_p$ again annihilates $[\mathfrak{q}]$ in $\mathcal{C}l(K)_p/M$.

From this it follows directly that $\mathcal{A}'$, the projection of $\mathcal{A}_p$ to $\mathbb{Z}/M'[G]$, annihilates $[\mathfrak{q}]$ in $\mathcal{C}l(K)_p/M'$. Since $(\mathcal{O}_{K(q)}/\widetilde{q})^*/M$ is free cyclic over $\mathbb{Z}/M[G]$, it is also clear that $\mathcal{A}'$ is the annihilator of $((\mathcal{O}_{K(q)}/\widetilde{q})^*/M')/\langle \mathrm{im}(\varepsilon_q)\rangle = \mathcal{B}/M'$.

Thus we are left with showing that $\alpha(\varepsilon')$ lies in $\mathcal{A}'$. But since ε_q and ε' have the same image in $(\mathcal{O}_{K(q)}/\widetilde{q})^*/M'$, $\mathcal{A}'$ is likewise the annihilator of

$$((\mathcal{O}_{K(q)}/\widetilde{q})^*/M')/\langle \mathrm{im}(\varepsilon')\rangle = ((\mathcal{O}_K/q)^*/M')/\langle \psi(\varepsilon')\rangle,$$

where ψ is the reduction map from Theorem 17 (now considered modulo M'). We look at the following diagram which arises by reading diagram (iv) in Theorem 17 modulo M':

$$\begin{array}{ccc} V/M' & \xrightarrow{\ \alpha\ } & \mathbb{Z}/M'[G] \\ \Big\downarrow{\scriptstyle \psi} & \nearrow{\scriptstyle \varphi} & \\ (\mathcal{O}_K/q)^*/M' & & \end{array}$$

Since $(\mathcal{O}_K/q)^*/M'$ is $\mathbb{Z}/M'[G]$-free cyclic, we have $\varphi(\psi(\varepsilon')) \in \mathcal{A}'$. (To see this, let T be the ring $\mathbb{Z}/M'[G]$, N the T-module $(\mathcal{O}_K/q)^*/M'$, and pick a T-isomorphism $i : T \to N$. Then putting $U = \langle \psi(\varepsilon')\rangle$, we find $N/U \cong T/i^{-1}(U)$, and comparing annihilators we see that $i^{-1}(U)$ is exactly the annihilator of N/U, so $i^{-1}(U) = \mathcal{A}'$. Hence $\varphi(\psi(\varepsilon')) \in \varphi i(\mathcal{A}')$, and this is contained in $\mathcal{A}'$ since φi is defined on the T-module T.) Therefore $\alpha(\varepsilon') \in \mathcal{A}'$ as was to be shown. ∎

References

[GK] 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.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. 76 (1984), 179–330.

[R1] K. Rubin, *Global units and ideal class groups*, ibid. 89 (1987), 511–526.

[R2] K. Rubin, *The Main Conjecture*, in: S. Lang, Cyclotomic Fields I and II (combined 2nd edition), Springer, 1990.

[Sch] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. 72 (2003), 913–937 (electronic).

[S] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181–234.

[Th] F. Thaine, *On the ideal class groups of real abelian number fields*, Ann. of Math. 128 (1988), 1–18.

Institut für theoretische Informatik und Mathematik
Fakultät für Informatik
Universität der Bundeswehr München
85577 Neubiberg, Germany
E-mail: greither@informatik.unibw-muenchen.de

Přírodovědecká fakulta
Masarykova univerzita
Janáčkovo nám. 2a
662 95 Brno, Czech Republic
E-mail: kucera@math.muni.cz

Received on 21.1.2003
and in revised form on 30.5.2003 (4448)