ARCHIVUM MATHEMATICUM (BRNO)
Tomus 49 (2013), 209–222

ANNIHILATORS OF THE CLASS GROUP OF A COMPOSITUM OF QUADRATIC FIELDS

Jan Herman

Abstract. This paper is devoted to a construction of new annihilators of the ideal class group of a tamely ramified compositum of quadratic fields. These annihilators are produced by a modified Rubin's machinery. The aim of this modification is to give a stronger annihilation statement for this specific type of fields.

Introduction

In [4] K. Rubin fundamentally generalized F. Thaine's method [6] to construct annihilators of the ideal class group. These annihilators are obtained as images of so-called special units in certain linear maps, whose codomain is the group ring over the Galois group. For a real abelian extension of rationals, circular units are the usual source of the special units.

C. Greither and R. Kučera in [1] have followed [4] in the special case of a cyclic extension of $\mathbb{Q}$ whose degree is the power of an odd prime. The group of special units of this field was enlarged to the group of so-called semispecial units. The authors have found a semispecial unit that is not circular and proved that images of semispecial units in the above mentioned linear maps annihilate ideal class group, too.

This paper follows [4] in a similar way in the special case of the compositum of tamely ramified quadratic fields. We introduce the notion of semispeciality in these fields and show that units obtained in [2] as roots of circular units are semispecial. Further we show that semispecial units can be used as an input for Rubin's machinery.

To be more precise, let us compare the main results of this paper (Theorems 10 and 2) with the result of the paper [4] applied to our situation:

Let $k/\mathbb{Q}$ be a compositum of quadratic fields having an odd conductor n. Let K be the genus field of k in the narrow sense, suppose $K \neq k$. Let further M be a "large" power of 2, $\eta = N_{\mathbb{Q}(\zeta_n)/k}(1-\zeta_n)$ and V a G-submodule of $\mathcal{O}_k^\times/(\mathcal{O}_k^\times)^M$, such that $\eta \in V$, where $\zeta_n = e^{2\pi i/n}$, $G = \mathrm{Gal}(k/\mathbb{Q})$ and $\mathcal{O}_k^\times$ is the group of units of k.

2010 *Mathematics Subject Classification*: primary 11R20; secondary 11R27, 11R29.
Key words and phrases: annihilators, class group, circular (cyclotomic) units, compositum of quadratic fields.
Received November 6, 2012, revised October, 2013. Editor C. Greither.
DOI: 10.5817/AM2013-4-209

If $\alpha : V \to \mathbb{Z}/M\mathbb{Z}[G]$ is a G-linear map satisfying $\alpha(\{\pm 1\} \cap V) = 0$, then Rubin's Theorem 1.3 in [4] gives that $4\alpha(\eta)$ annihilates $Cl(k)/M\, Cl(k)$.

In [2] the existence of $\omega \in k$ satisfying $\omega^{\frac{[K:k]}{2}} = \eta$ was shown. In Theorem 2 we show that this ω is semispecial (however it needn't be special in Rubin's sense) and so Theorem 10 gives that $4\alpha(\omega) = \frac{8}{[K:k]}\alpha(\eta)$ annihilates $Cl(k)/M'\, Cl(k)$, where $M' = \frac{M}{[K:k]}$. Roughly speaking, the annihilator given by [4] is $\frac{[K:k]}{2}$ times our annihilator and so our result is stronger if $[K : k] > 2$.

1. Notation

Kučera in [2] constructs new explicit units of a compositum of quadratic fields by taking power-of-two roots of circular units. We will use these roots to produce annihilators of the class group of the given field.

Let us resume what we need from the paper [2].

At first some definitions:

Let k be a compositum of quadratic fields and let K be the genus field of k in narrow sense. Assume that $i = \sqrt{-1}, \sqrt{2}, \sqrt{-2} \notin K$, i.e. the prime 2 does not ramify in k (this is a special case of the one described in [2]). Define also the set

$$J = \{p \in \mathbb{Z};\ p \equiv 1 \pmod 4, |p| \text{ is prime and ramifies in } k\}\,.$$

We can describe the fields k and K as follows: $k = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, \dots, \sqrt{m_l})$, where the numbers m_j are square-free integers, all congruent to 1 modulo 4, and $K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r})$, where p_j runs through all signed primes congruent to 1 modulo 4 dividing $\prod_{j=1}^{l} m_j$.

Let us also suppose $|J| \geq 2$ (otherwise we have $k = \mathbb{Q}$ or the case of a quadratic field with a prime discriminant).

For a positive integer n define $\zeta_n = e^{2\pi i/n}$.

For any $p \in J$ define $K_{\{p\}} = \mathbb{Q}(\sqrt{p})$ and $n_{\{p\}} = |p|$.

For $\emptyset \neq S \subseteq J$ define $K_S = \prod_{p \in S} K_{\{p\}}$, $n_S = \prod_{p \in S} n_{\{p\}}$ and $\mathbb{Q}_S = \mathbb{Q}(\zeta_{n_S})$. Define also $K_\emptyset = \mathbb{Q}$, $n_\emptyset = 1$.

In each subfield K_S of K we can define a circular unit:

$$\varepsilon_S = \begin{cases} 1 & \text{for} \quad S = \emptyset\,, \\ \frac{1}{\sqrt{p}} N_{\mathbb{Q}_S/K_S}(1 - \zeta_{n_S}) & \text{for} \quad S = \{p\}\,, \\ N_{\mathbb{Q}_S/K_S}(1 - \zeta_{n_S}) & \text{for} \quad \#S > 1\,. \end{cases}$$

It is easy to see that for each $S \subseteq J$, ε_S is really a unit of K_S. By the norm map we can translate these units to get units in k:

$\eta_S = N_{K_S/k_S}(\varepsilon_S)$, where $k_S = K_S \cap k$.

Again, η_S is obviously a unit in k_S for each $S \subseteq J$.

In [2, Proposition 2.1] it is shown that for each $S \subseteq J$ there exists a unit

$$\varkappa_S \in \big\langle \{\varepsilon_T, T \subseteq S\} \big\rangle$$

such that

$$\varkappa_S^{[K_S:k_S]} = \pm \eta_S\,.$$

Denote $\omega_S = \varkappa_S^2$. Since the only power-of-two roots of unity in k_S are ± 1 it is easy to prove that $\omega_S \in k_S$, see [2, Corollary 3.1].

2. Semispecial units

In order to produce annihilators of the class group of k, we will introduce the notion of semispecial units — a slight modification of the concept of special units given by Rubin in [4].

Let $M \geq 8$ be a power of 2 divisible by $[K:k]$. We denote $M' = M/[K:k]$.

Denote by $\mathcal{Q}_M$ the set of all primes $q \equiv 1 + 2M (\mathrm{mod}\ M^2)$ such that q splits completely in k and for each $p \in J$ the absolute value of p is an M-th power modulo q.

For an arbitrary number field l let $\mathcal{O}_l$ denote the ring of algebraic integers in l; having any $q \in \mathcal{Q}_M$ let $l(q)$ be the compositum of l and the unique cyclic field $\mathbb{Q}(q)$ of degree M and conductor q. Denote also by $\tilde{q}_l$ the product of all distinct primes of $l(q)$ above q. If q splits completely in l then the ring $\mathcal{O}_{l(q)}/\tilde{q}_l$ is a product of $[l:\mathbb{Q}]$ copies of the field with q elements where Galois group $\mathrm{Gal}(l/\mathbb{Q})$ permutes these copies. The group of units $(\mathcal{O}_{l(q)}/\tilde{q}_l)^\times$ of this ring is therefore a product of $[l:\mathbb{Q}]$ copies of the cyclic group of order $q-1$. For an abelian group A and a positive integer N let A/N mean the quotient group A/A^N in multiplicative or A/NA in aditive notation. We will use this shorthand also if A is a ring, then A/N is a ring, too.

Definition 1. A number $\delta \in k^\times$ is called M-semispecial if for all but finitely many $q \in \mathcal{Q}_M$ there exists a unit $\delta_q \in k(q)^\times$ such that

- $N_{k(q)/k}(\delta_q) = 1$ (norm condition),
- δ^2 and δ_q have the same image in $(\mathcal{O}_{k(q)}/\tilde{q})^\times/M'$ (congruence condition).

Theorem 2. *The unit ω_J is M-semispecial.*

We will postpone the proof for a while. Fix a prime $q \in \mathcal{Q}_M$. At first for each nonempty $S \subseteq J$ let us define an auxiliary unit

$$\varepsilon_{S,q} = N_{\mathbb{Q}_S(\zeta_q)/K_S(q)}(1 - \zeta_{n_S}\zeta_q).$$

Put $\varepsilon_{\emptyset,q} = 1$. We shall show that these units have similar properties as ε_S (compare with [2, Lemma 2.2]).

Lemma 3. *Let $p \in S \subseteq J$. Then*

$$N_{K_S(q)/K_{S-\{p\}}(q)}(\varepsilon_{S,q}) = \varepsilon_{S-\{p\},q}^{1-\mathrm{Frob}(|p|,K_{S-\{p\}}(q))}.$$

Proof. The well-known norm relation for circular units gives

$$\begin{aligned} N_{K_S(q)/K_{S-\{p\}}(q)}(\varepsilon_{S,q}) &= N_{\mathbb{Q}_S(\zeta_q)/K_{S-\{p\}}(q)}(1 - \zeta_{n_S}\zeta_q) \\ &= N_{\mathbb{Q}_{S-\{p\}}(\zeta_q)/K_{S-\{p\}}(q)}\big(N_{\mathbb{Q}_S(\zeta_q)/\mathbb{Q}_{S-\{p\}}(\zeta_q)}(1 - \zeta_{n_S}\zeta_q)\big) \\ &= N_{\mathbb{Q}_{S-\{p\}}(\zeta_q)/K_{S-\{p\}}(q)}\big((1 - \zeta_{n_{S-\{p\}}}\zeta_q)^{1-\mathrm{Frob}(|p|,\mathbb{Q}_{S-\{p\}}(\zeta_q))^{-1}}\big) \\ &= \varepsilon_{S-\{p\},q}^{1-\mathrm{Frob}(|p|,K_{S-\{p\}}(q))^{-1}}. \end{aligned}$$

Since $|p|$ is an M-th power modulo q, $\mathrm{Frob}(|p|, K_{S-\{p\}}(q)) \in \mathrm{Gal}(K_{S-\{p\}}(q)/\mathbb{Q}(q))$. As q ramifies totally in $\mathbb{Q}(q)/\mathbb{Q}$ and splits completely in $k/\mathbb{Q}$, this Galois group is isomorphic to $\mathrm{Gal}(K_{S-\{p\}}/\mathbb{Q})$, which is 2-elementary. The lemma follows. $\square$

Lemma 4. *Let $S \subseteq J$. Then for arbitrary $\sigma \in \mathrm{Gal}(K(q)/\mathbb{Q}(q))$ the following holds:*

$$\varepsilon_{S,q}^{1-\sigma} = \prod_{T \subseteq S} \varepsilon_{T,q}^{2b_T}$$

for suitable $b_T \in \mathbb{Z}$.

Proof. We will prove the lemma by induction on S. For $S = \emptyset$, we have $\varepsilon_{S,q} = 1$, so the statement holds. Let us suppose that $S \neq \emptyset$ and that for each proper subset of S the lemma has been proven.

The Galois group $\mathrm{Gal}(K(q)/\mathbb{Q}(q))$ is isomorphic to $\mathrm{Gal}(K/\mathbb{Q})$, hence we can write $\sigma = \prod_{p \in R} \sigma_p$ for a suitable $R \subseteq J$, where σ_p denotes the non-trivial automorphism in $\mathrm{Gal}(K(q)/K_{J-\{p\}}(q))$. So $\varepsilon_{S,q}^{\sigma} = \varepsilon_{S,q}^{\prod_{p \in R \cap S} \sigma_p}$.

We will continue by induction on $R \cap S$. If $R \cap S = \emptyset$, then $\varepsilon_{S,q}^{\sigma} = \varepsilon_{S,q}$ and the statement holds. If $R \cap S = \{p\}$ we get using Lemma 3

$$\varepsilon_{S,q}^{1-\sigma} = \varepsilon_{S,q}^{1-\sigma_p} = \varepsilon_{S,q}^{2} \cdot (\varepsilon_{S,q}^{1+\sigma_p})^{-1} = \varepsilon_{S,q}^{2} \cdot \left(\varepsilon_{S-\{p\},q}^{1-\mathrm{Frob}(|p|, K_{S-\{p\}}(q))}\right)^{-1}.$$

The expression in parentheses satisfies the induction hypothesis, because $|p|$ is an M-th power modulo q, hence $\mathrm{Frob}(|p|, K_{S-\{p\}}(q)) \in \mathrm{Gal}(K_S(q)/\mathbb{Q}(q))$. Now we will suppose that $|R \cap S| \geq 2$ and that for each proper subset of $R \cap S$ the assertion holds. If we take a prime $p \in R \cap S$, we have $\sigma\sigma_p = \prod_{t \in R-\{p\}} \sigma_t$ and

$$\varepsilon_{S,q}^{1-\sigma} = \varepsilon_{S,q}^{1-\sigma_p} \cdot \left(\varepsilon_{S,q}^{1-\sigma\sigma_p}\right)^{\sigma_p}.$$

For each factor we can apply the induction hypothesis for $R \cap S$, so we get

$$\varepsilon_{S,q}^{1-\sigma} = \prod_{T \subseteq S} \varepsilon_{T,q}^{2b'_T} \cdot \Big(\prod_{T \subseteq S} \varepsilon_{T,q}^{2b''_T}\Big)^{\sigma_p} = \prod_{T \subseteq S} \varepsilon_{T,q}^{2(b'_T + b''_T)} \cdot \prod_{T \subseteq S} \left(\varepsilon_{T,q}^{\sigma_p - 1}\right)^{2b''_T}.$$

We can use the induction hypothesis for each factor in the latter product and the lemma follows. $\square$

Since we can write $\varepsilon_{S,q}^{1+\sigma} = \varepsilon_{S,q}^{2} \cdot \varepsilon_{S,q}^{\sigma-1}$ we get another version of the lemma, which will be used later on.

Corollary 5. *Let $S \subseteq J$. Then for arbitrary $\sigma \in \mathrm{Gal}(K(q)/\mathbb{Q}(q))$ the following holds:*

$$\varepsilon_{S,q}^{1+\sigma} = \prod_{T \subseteq S} \varepsilon_{T,q}^{2c_T}$$

for suitable $c_T \in \mathbb{Z}$.

Similarly as before let us define units $\eta_{S,q} = N_{K_S(q)/k_S(q)}(\varepsilon_{S,q})$.

Lemma 6. *For each* $S \subseteq J$ *there exists* $\varkappa_{S,q} \in \langle \varepsilon_{T,q}; T \subseteq S\rangle \subseteq K_S(q)$*, such that*

$$\eta_{S,q} = \varkappa_{S,q}^{2^r},$$

where $2^r = [K_S : k_S] = [K_S(q) : k_S(q)]$.

Proof. $\mathrm{Gal}(K_S(q)/k_S(q))$ is 2-elementary, let $\beta_1, \dots, \beta_r$ be its independent generators. Then

$$\eta_{S,q} = N_{K_S(q)/k_S(q)}(\varepsilon_{S,q}) = \varepsilon_{S,q}^{(1+\beta_1)(1+\beta_2)\dots(1+\beta_r)}$$

and the previous corollary gives the result by means of induction on r. □

Since the only power-of-two roots of unity in $K_S(q)$ are ± 1 (the conductor of the field $K_S(q)$ is odd) we get that $\varkappa_{S,q}^2$ lies in $k_S(q)$, we will call it $\omega_{S,q}$. Denote also $\varkappa_q := \varkappa_{J,q}$, $\omega_q := \omega_{J,q}$, $\eta_q := \eta_{J,q}$ and $\varepsilon_q := \varepsilon_{J,q}$.

Proof of Theorem 2. We will prove that ω_q satisfies the conditions in the definition of M-semispeciality for the unit ω_J.

At first we will prove the norm condition. We have

$$\begin{aligned} N_{K(q)/K}(\varkappa_q)^{[K:k]} &= N_{k(q)/k}\left(\varkappa_q^{[K:k]}\right) \\ &= N_{k(q)/k}(\eta_q) = N_{\mathbb{Q}_J(\zeta_q)/k}(1-\zeta_{n_J}\zeta_q) \\ &= N_{\mathbb{Q}_J/k}\left(N_{\mathbb{Q}_J(\zeta_q)/\mathbb{Q}_J}(1-\zeta_{n_J}\zeta_q)\right) \\ &= N_{\mathbb{Q}_J/k}\left((1-\zeta_{n_J})^{\mathrm{Frob}(q,\mathbb{Q}_J)-1}\right) \\ &= \eta_J^{\mathrm{Frob}(q,k)-1} = 1\,, \end{aligned}$$

where the last equality follows from the fact that q splits completely in k, therefore its Frobenius in $\mathrm{Gal}(k/\mathbb{Q})$ is trivial. Since the only power-of-two roots of unity in K are ± 1, it means $N_{K(q)/K}(\varkappa_q) = \pm 1$, hence $N_{k(q)/k}(\omega_q) = N_{K(q)/K}(\varkappa_q^2) = 1$.

To prove the congruence condition, we will step by step derive congruences.

Obviously

$$1-\zeta_{n_J} \equiv 1-\zeta_{n_J}\zeta_q \pmod{1-\zeta_q} \text{ in } \mathcal{O}_{\mathbb{Q}_J(\zeta_q)}\,.$$

Taking norms to $K(\zeta_q)$ gives

$$\varepsilon_J = N_{\mathbb{Q}_J(\zeta_q)/K(\zeta_q)}(1-\zeta_{n_J}) \equiv N_{\mathbb{Q}_J(\zeta_q)/K(\zeta_q)}(1-\zeta_{n_J}\zeta_q) \pmod{1-\zeta_q} \text{ in } \mathcal{O}_{K(\zeta_q)}\,.$$

Therefore

$$\varepsilon_J^{\frac{q-1}{M}} = N_{K(\zeta_q)/K(q)}(\varepsilon_J) \equiv N_{\mathbb{Q}_J(\zeta_q)/K(q)}(1-\zeta_{n_J}\zeta_q) = \varepsilon_q \pmod{\tilde{q}_K} \text{ in } \mathcal{O}_{K(q)}$$

and so

$$\eta_J^{\frac{q-1}{M}} = N_{K(q)/k(q)}(\varepsilon_J^{\frac{q-1}{M}}) \equiv N_{K(q)/k(q)}(\varepsilon_q) = \eta_q \pmod{\tilde{q}_k} \text{ in } \mathcal{O}_{k(q)}\,.$$

As $\frac{q-1}{M} \equiv 2 \pmod{M}$ we see that η_J^2 and η_q have the same image in the quotient $(\mathcal{O}_{k(q)}/\tilde{q}_k)^\times/M$. Using $\omega_J^{[K:k]/2} = \eta_J$ and $\omega_q^{[K:k]/2} = \eta_q$ we obtain that ω_J^2 and ω_q have the same image in $(\mathcal{O}_{k(q)}/\tilde{q}_k)^\times/M'$, because $M' = M/[K:k]$. Thus ω_J is M-semispecial as we wanted to prove.

□

3. Annihilators of the class group

Let us now formulate some technical lemmas that will be used later on.

Lemma 7. *Let F be an abelian field, $i \notin F$. If R is an abelian field containing F and $\gamma \in R$ satisfies $\gamma^4 \in F$ then either $\gamma^2 \in F$ or $i\gamma^2 \in F$.*

Proof. Let us assume that $\gamma^2 \notin F$ and $i\gamma^2 \notin F$. Then

$$x^4 - \gamma^4 = (x-\gamma)(x+\gamma)(x-i\gamma)(x+i\gamma)$$

is an irreducible polynomial over F and so $[F(\gamma) : F] = 4$. Since $R/\mathbb{Q}$ is abelian, $F(\gamma)/F$ is a Galois extension and so $i \in F(\gamma)$. It is easy to see that both $F(\gamma^2)$ and $F(i\gamma^2)$ are quadratic subextensions of it and that Kummer theory together with $i \notin F$ implies $F(\gamma^2) \neq F(i\gamma^2)$. Hence $\mathrm{Gal}(F(\gamma)/F)$ is the noncyclic group of order 4 and the third quadratic subextension is $F(i)$. The minimal polynomial of γ over $F(i)$ is quadratic and divides $x^4 - \gamma^4$ but each of the three possibilities gives a contradiction. For example if the minimal polynomial were $(x-\gamma)(x+\gamma)$, then we would get $-\gamma^2 \in F(i)$, which contradicts $F(\gamma^2) \neq F(i)$. The other two cases are quite similar. □

Lemma 8. *Let F be an abelian field, $i \notin F$. Let n be a positive integer. If $\beta \in F$ is a 2^n-th power in an abelian field R containing F then β or $-\beta$ is a 2^{n-1}-th power in F.*

Proof. Let us use induction with respect to n. If $n = 1$ the statement is void; for $n = 2$ choose $\gamma \in R$ such that $\gamma^4 = \beta$ and use Lemma 7. Let us suppose that $n > 2$ and that the statement has been proven for $n-1$. We have $\delta \in R$ such that $\beta = \delta^{2^n}$. Lemma 7 for $\gamma = \delta^{2^{n-2}}$ gives that either $\delta^{2^{n-1}} \in F$ or $i\delta^{2^{n-1}} \in F$. Since $i\delta^{2^{n-1}} = (\zeta_{2^{n+1}}\delta)^{2^{n-1}}$ and $R(\zeta_{2^{n+1}})$ is an abelian field, the induction hypothesis gives that there is $\eta \in F$ such that either $\eta^{2^{n-2}} = \delta^{2^{n-1}}$ or $\eta^{2^{n-2}} = i\delta^{2^{n-1}}$. Each of the two cases implies $\eta^{2^{n-1}} = \pm\delta^{2^n} = \pm\beta$. □

Lemma 9. *Let F be an abelian field, $i \notin F$, $\sqrt{2} \notin F$, $i\sqrt{2} \notin F$. Let M be a power of 2 such that $8 \mid M$. Then the canonical map*

$$\rho\colon\ F^\times/(F^\times)^M \ \to\ F(\zeta_M)^\times/(F(\zeta_M)^\times)^M$$

has a kernel of order 2, more precisely

$$\ker(\rho) = \{(F^\times)^M, 2^{M/2}\cdot(F^\times)^M\}\,.$$

Proof. Since $2^{M/2} = (1+i)^M$, we see that $2^{M/2}\cdot(F^\times)^M \in \ker\rho$. Let us assume for a moment that there is $c \in F$ such that $2^{M/2} = c^M$. Then $(\frac{1}{2}c^2)^{M/2} = 1$ and $i \notin F$ gives $\frac{1}{2}c^2 = \pm 1$. Hence $c = \pm\sqrt{2}$ or $c = \pm i\sqrt{2}$, which is a contradiction. Therefore we know that ρ is not injective and to prove the lemma we need to show that its kernel does not contain any other element.

Let $a \in F^\times$ satisfy $a\cdot(F^\times)^M \in \ker\rho$. Then there is $b \in F(\zeta_M)^\times$ such that $a = b^M$. If $b \in F$ then $a\cdot(F^\times)^M = (F^\times)^M$ and there is nothing to prove. So we shall assume $b \notin F$.

Lemma 8 gives $c \in F^\times$ such that $c^{M/2} = \pm a$. Hence $(\frac{b^2}{c})^{M/2} = \pm 1$ and $\frac{b^2}{c}$ is an M-th root of unity, so $\frac{b^2}{c} = \zeta_M^u$ for a suitable $u \in \mathbb{Z}$. Changing b to $b \cdot \zeta_M^{[u/2]}$ allows us to assume that $u \in \{0, 1\}$.

The assumption $i \notin F$, $\sqrt{2} \notin F$, $i\sqrt{2} \notin F$ implies that $\mathbb{Q}(\zeta_M) \cap F = \mathbb{Q}$ and so $\mathrm{Gal}(F(\zeta_M)/F) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$.

At first, let us deal with the case $u = 1$. So we have $b^2 = c \cdot \zeta_M$. Let $\sigma \in \mathrm{Gal}(F(\zeta_M)/F)$ be determined by $\sigma(\zeta_M) = \zeta_M^{1+M/2}$. Then $\sigma^2(\zeta_M) = \zeta_M$ and so σ^2 is the identity. We have $\sigma(b^2) = \sigma(c \cdot \zeta_M) = c \cdot \zeta_M^{1+M/2} = b^2 \cdot \zeta_M^{M/2}$. It means that there is $v \in \{0, 1\}$ such that $\sigma(b) = (-1)^v \cdot b \cdot \zeta_M^{M/4}$ and so

$$b = \sigma^2(b) = (-1)^v \cdot \sigma(b) \cdot \zeta_M^{(1+M/2)M/4} = b \cdot \zeta_M^{M/2} = -b,$$

a contradiction.

Therefore $u = 0$ and $b^2 = c$. Since $b \notin F$ we have that $F(b)$ is one of the three quadratic subextensions of $F(\zeta_M)/F$, namely $F(i)$, $F(\sqrt{2})$, or $F(i\sqrt{2})$. Kummer theory gives that $b = d \cdot e$, where $d \in \{i, \sqrt{2}, i\sqrt{2}\}$ and $e \in F^\times$. Then $a = b^M = d^M \cdot e^M \in \{e^M, 2^{M/2} \cdot e^M\}$ and the lemma follows. $\square$

Now let us formulate the main theorem of the paper.

Recall that $G = \mathrm{Gal}(k/\mathbb{Q})$.

Theorem 10. *Fix a large power of 2, denote it M. Let δ be an M-semispecial unit of k, W a finitely generated $\mathbb{Z}[G]$-submodule of $k^\times/M$ such that $\delta(k^\times)^M \in W$. Let*

$$\alpha \colon W \to \mathbb{Z}/M[G]$$

be a $\mathbb{Z}[G]$-linear map whose kernel contains $W \cap (\mathbb{Q}^\times(k^\times)^M/(k^\times)^M)$. Then $4\alpha(\delta)$ annihilates $Cl(k)/M'$ where $M' = \frac{M}{[K:k]}$.

Remark 11. If M is large enough, then the quotient $Cl(k)/M'$ becomes the whole $Cl(k)_2$, the 2-part of $Cl(k)$.

The rest of the article proves the main theorem.

The proof follows Rubin's original proof in [4] and its adaptation in [1].

The annihilator of $Cl(k)/M'$ is constructed by means of Rubin's theorem (see [4, Theorem 5.1]). We produce infinitely many auxiliary primes q with prescribed properties using Chebotarev density theorem (similarly to [4, Theorem 5.5] and [1, Theorem 17]) and this allows to use the given M-semispecial unit as an input for Rubin's theorem.

The auxiliary primes q are constructed by the following theorem.

Theorem 12. *Let M be a fixed large power of 2 divisible by $[K : k]$, let $W \subseteq k^\times/(k^\times)^M$ a finitely generated $\mathbb{Z}[G]$-submodule and let $\alpha \colon W \to \mathbb{Z}/M[G]$ be a $\mathbb{Z}[G]$-linear map whose kernel contains $W \cap (\mathbb{Q}^\times(k^\times)^M/(k^\times)^M)$. Then for each class $\mathfrak{c} \in Cl(k)_2$ there exist infinitely many unramified primes $\mathfrak{q}$ in k of absolute degree 1 such that:*

- *$[\mathfrak{q}] = \mathfrak{c}^2$, where $[\mathfrak{q}]$ is the projection of the ideal class of $\mathfrak{q}$ into $Cl(k)_2$;*
- *$q \equiv 1 + 2M \pmod{M^2}$, where q is the rational prime below $\mathfrak{q}$;*
- *for each $p \in J$, $|p|$ is an M-th power modulo q;*

– *W has a set of generators coprime to q and there exists a $\mathbb{Z}[G]$-linear map $\varphi\colon (\mathcal{O}_k/q)^\times/M \to \mathbb{Z}/M[G]$ such that the following diagram commutes (ψ being the reduction map)*

$$\begin{tikzcd} W \arrow[r, "2\alpha"] \arrow[d, "\psi"'] & \mathbb{Z}/M[G] \\ (\mathcal{O}_k/q)^\times/M \arrow[ur, dotted, "\varphi"'] & \end{tikzcd}$$

Proof. Let $V \subseteq k(\zeta_M)^\times/(k(\zeta_M)^\times)^M$ denote the image of W under the canonical map $\rho\colon k^\times/(k^\times)^M \to k(\zeta_M)^\times/(k(\zeta_M)^\times)^M$. Lemma 9 gives

$$\ker(\rho) = \{(k^\times)^M, 2^{\frac{M}{2}} \cdot (k^\times)^M\}.$$

Since $\ker(\rho) \subseteq \mathbb{Q}^\times(k^\times)^M/(k^\times)^M \subseteq \ker(\alpha)$, there exists a map $\alpha'\colon V \to \mathbb{Z}/M[G]$, such that the following diagram commutes:

$$\begin{tikzcd} W \arrow[r, "\alpha"] \arrow[d, "\rho"'] & \mathbb{Z}/M[G] \\ V \arrow[ur, dotted, "\alpha'"'] & \end{tikzcd}$$

It is easy to see that $\ker(\alpha')$ contains $V \cap (\mathbb{Q}^\times(k(\zeta_M)^\times)^M/(k(\zeta_M)^\times)^M)$.

Consider the following diagram of fields:

$$\begin{tikzcd}[column sep=small] & & & k''' \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ H \arrow[ddddrrr, dash] & & k''(\zeta_{M^2}) \arrow[d, dash] \arrow[dr, dash] & k''L \arrow[dl, dash] \arrow[dr, dash] & L(\zeta_{M^2}) \arrow[dl, dash] \arrow[d, dash] \\ & & k'' \arrow[d, dash] & k(\zeta_{M^2}) \arrow[dd, dash] & L \arrow[ddl, dash] \\ & & k' \arrow[dr, dash] & & \\ & & & k(\zeta_M) \arrow[d, dash] & \\ & & & k & \end{tikzcd}$$

In the diagram, H is the 2-Hilbert class field of k,

$k' = k(\zeta_M, \ker(\alpha')^{\frac{1}{M}})$,
$k'' = k(\zeta_M, V^{\frac{1}{M}})$,
$L = k(\zeta_M, P^{\frac{1}{M}})$,
$k''' = k''L(\zeta_{M^2})$,

where $P = \pm\prod_{p\in J} p^{\mathbb{Z}}$.

Notice that $\zeta_{2M} \in L$.

Lemma 13. (a) *Let A' be the largest subfield of $k''L$ that is abelian over k. Then* $\mathrm{Gal}(A'/k(\zeta_M))$ *is* 2*-elementary.*

(b) *Let A'' be the largest subfield of $Hk''L$ that is abelian over H. Then the Galois group* $\mathrm{Gal}(A''/H(\zeta_M))$ *is* 2*-elementary.*

Proof. (a) Consider the following exact sequence of Galois groups:

$$1 \to \mathrm{Gal}(k''L/k(\zeta_M)) \to \mathrm{Gal}(k''L/k) \to \mathrm{Gal}(k(\zeta_M)/k) \to 1\,.$$

Since k has an odd conductor,

$$\mathrm{Gal}(k(\zeta_M)/k) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q}) \cong (\mathbb{Z}/M)^\times\,.$$

Kummer theory gives that $\mathrm{Gal}(k''L/k(\zeta_M))$ is an abelian 2-group whose exponent divides M. The action of $(\mathbb{Z}/M)^\times$ on $\mathrm{Gal}(k''L/k(\zeta_M))$ is the cyclotomic one, hence the one given by exponentiating. We will prove that each square in $\mathrm{Gal}(k''L/k(\zeta_M))$ is a commutator of $\mathrm{Gal}(k''L/k)$. Let $u \in \mathrm{Gal}(k(\zeta_M)/k)$ be the automorphism that corresponds to 3 in $(\mathbb{Z}/M)^\times$. Take its extension $\bar{u}$ to $\mathrm{Gal}(k''L/k)$. Then for each $\sigma \in \mathrm{Gal}(k''L/k(\zeta_M))$ the following holds

$$\bar{u}\sigma\bar{u}^{-1}\sigma^{-1} = \sigma^3 \cdot \sigma^{-1} = \sigma^2.$$

Hence the group of squares in $\mathrm{Gal}(k''L/k(\zeta_M))$ is a subgroup of the commutator group of $\mathrm{Gal}(k''L/k)$ and therefore $\mathrm{Gal}(A'/k(\zeta_M))$ is 2-elementary.

(b) Consider the exact sequence

$$1 \to \mathrm{Gal}\big(Hk''L/H(\zeta_M)\big) \to \mathrm{Gal}(Hk''L/H) \to \mathrm{Gal}\big(H(\zeta_M)/H\big) \to 1\,.$$

The primes above 2 are unramified in H/k and also in $k/\mathbb{Q}$ and so they are totally ramified in $k(\zeta_M)/k$. Hence $k(\zeta_M) \cap H = k$, $k(\zeta_M)H = H(\zeta_M)$ and

$$\mathrm{Gal}\big(H(\zeta_M)/H\big) \cong \mathrm{Gal}\big(k(\zeta_M)/k\big) \cong \mathrm{Gal}\big(\mathbb{Q}(\zeta_M)/\mathbb{Q}\big) \cong (\mathbb{Z}/M)^\times\,.$$

The rest can be done in the same way as above. □

Now we will continue the proof of Theorem 12 by constructing an automorphism $\tau \in \mathrm{Gal}(Hk'''/k)$ as an input for Chebotarev density theorem to produce infinitely many primes q that satisfy all properties claimed in the theorem.

For the given class $\mathfrak{c} \in Cl(k)_2$ take the corresponding $\tau_1 \in \mathrm{Gal}(H/k)$. Since $k(\zeta_M) \cap H = k$ as mentioned in the proof of Lemma 13(b), we can glue τ_1 together with $\mathrm{id}_{k(\zeta_M)} \in \mathrm{Gal}(k(\zeta_M)/k)$ to get $\tau_2 \in \mathrm{Gal}(H(\zeta_M)/k(\zeta_M))$ such that $\tau_2|_H = \tau_1$.

Similarly as in [1, page 195] we see that $\mathrm{Gal}(k''/k')$ is a cyclic $\mathbb{Z}/M[G]$-module. Let τ_3 be its generator. We would like to extend τ_3 to $\tau_4 \in \mathrm{Gal}(k''L/k(\zeta_M))$ such that τ_4 is trivial on L. We need to show that τ_3 is trivial on $L \cap k''$. Let us denote $\widehat{P} = P(k(\zeta_M)^\times)^M/(k(\zeta_M)^\times)^M$. Kummer theory gives

$$L \cap k'' = k(\zeta_M, P^{\frac{1}{M}}) \cap k(\zeta_M, V^{\frac{1}{M}}) = k(\zeta_M, (\widehat{P} \cap V)^{\frac{1}{M}})$$

and $P \subseteq \mathbb{Q}$ implies $\widehat{P} \cap V \subseteq \ker(\alpha')$. Hence $L \cap k'' \subseteq k(\zeta_M, \ker(\alpha')^{\frac{1}{M}}) = k'$ and since $\tau_3 \in \mathrm{Gal}(k''/k')$ we can extend.

The field $H(\zeta_M) \cap k''L$ is abelian over k and so by Lemma 13(a) the group

$$\mathrm{Gal}(H(\zeta_M) \cap k''L/k(\zeta_M))$$

is 2-elementary. Hence

$$\tau_2^2 \in \mathrm{Gal}\left(H(\zeta_M)/H(\zeta_M) \cap k''L\right)$$

and

$$\tau_4^2 \in \mathrm{Gal}\left(k''L/H(\zeta_M) \cap k''L\right).$$

This implies that there exists a unique automorphism

$$\tau_5 \in \mathrm{Gal}\left(Hk''L/H(\zeta_M) \cap k''L\right) \subseteq \mathrm{Gal}\left(Hk''L/k(\zeta_M)\right),$$

such that $\tau_5|_{H(\zeta_M)} = \tau_2^2$ and $\tau_5|_{k''L} = \tau_4^2$.

In order to glue τ_5 together with a suitable $\tau_6 \in \mathrm{Gal}(k(\zeta_{M^2})/k(\zeta_{2M}))$ we need to determine the intersection $k(\zeta_{M^2}) \cap Hk''L$.

Since $H(\zeta_{M^2}) \cap Hk''L/H$ is an abelian subextension of $Hk''L/H$, Lemma 13(b) gives $H(\zeta_{M^2}) \cap Hk''L \subseteq A''$ and $\mathrm{Gal}(H(\zeta_{M^2}) \cap Hk''L/H(\zeta_M))$ is 2-elementary.

Similarly as in the proof of Lemma 13(b) we have $\mathrm{Gal}(H(\zeta_{M^2})/H) \cong (\mathbb{Z}/M^2)^\times$. Its subgroup $\mathrm{Gal}(H(\zeta_{M^2})/H(\zeta_M))$ corresponds to the subgroup of $(\mathbb{Z}/M^2)^\times$ generated by the class containing $1+M$. Thus $\mathrm{Gal}(H(\zeta_{M^2})/H(\zeta_M))$ is cyclic and the intersection $Hk''L \cap H(\zeta_{M^2})$ is a subextension of cyclic extension $H(\zeta_{M^2})/H(\zeta_M)$, hence also cyclic. Taking together, $Hk''L \cap H(\zeta_{M^2})/H(\zeta_M)$ has degree at most 2. As $\zeta_{2M} \in k''L$ we get $Hk''L \cap H(\zeta_{M^2}) = H(\zeta_{2M})$, which implies $\zeta_{4M} \notin Hk''L$ and $Hk''L \cap k(\zeta_{M^2}) = k(\zeta_{2M})$.

Let us calculate $\tau_5(\zeta_{2M}) = \tau_4^2(\zeta_{2M})$. We have $\tau_4 \in \mathrm{Gal}(k''L/k(\zeta_M))$, which gives $\tau_4(\zeta_M) = \zeta_M$ and $\tau_4(\zeta_{2M}) = e \cdot \zeta_{2M}$, where $e \in \{1, -1\}$. Hence

$$\tau_4^2(\zeta_{2M}) = \tau_4(e \cdot \zeta_{2M}) = e^2 \cdot \zeta_{2M} = \zeta_{2M}$$

and so $\tau_5 \in \mathrm{Gal}(Hk''L/k(\zeta_{2M}))$.

Let $\tau_6 \in \mathrm{Gal}(k(\zeta_{M^2})/k(\zeta_{2M}))$ be determined by $\tau_6(\zeta_{M^2}) = \zeta_{M^2}^{1+2M}$. We have shown that there exists an automorphism $\tau \in \mathrm{Gal}(Hk'''/k(\zeta_{2M}))$ satisfying

$$\tau|_{Hk''L} = \tau_5 \text{ and } \tau|_{k(\zeta_{M^2})} = \tau_6\,.$$

Now we can finish the proof of Theorem 12.

Due to Chebotarev density theorem, there exist infinitely many degree one primes of k relatively prime to a generating set of W, not over primes ramified in $k/\mathbb{Q}$, not over 2 such that the primes of Hk''' above them have their Frobenius automorphism in the conjugation class of τ.

Choose any of them and denote it $\mathfrak{q}$. We will show that $\mathfrak{q}$ satisfies all properties claimed in Theorem 12.

Let q be the rational prime below $\mathfrak{q}$.

Since $\tau|_H = \tau_1^2$, the class $[\mathfrak{q}]$ corresponds to the class $\mathfrak{c}^2$.

We have constructed τ to satisfy $\tau(\zeta_{M^2}) = \zeta_{M^2}^{1+2M}$. On the other hand, $\tau|_{k(\zeta_{M^2})}$ is the Frobenius of $\mathfrak{q}$, so $\tau(\zeta_{M^2}) = \zeta_{M^2}^{q}$. Putting these two equalities together, we get $q \equiv 1 + 2M \pmod{M^2}$.

The prime q splits completely in $L/\mathbb{Q}$, because $\tau|_L = \mathrm{id}_L$ and q splits completely in $k/\mathbb{Q}$. For each $p \in J$, $|p|$ is an M-th power in L, hence also in $\mathcal{O}_L$. Denote $\mathfrak{Q}$ a prime ideal in L over $\mathfrak{q}$. Then

$$\mathcal{O}_L/\mathfrak{Q} \cong \mathbb{Z}/q$$

and $|p|$ is an M-th power in $\mathbb{Z}/q$.

We will prove that there exists a map φ' such that the following diagram commutes.

$$\begin{tikzcd} W \arrow[r, "2\alpha"] \arrow[d, "\psi"'] & \mathbb{Z}/M[G] \\ \mathrm{im}(\psi) \arrow[ur, dotted, "\varphi'"'] & \end{tikzcd}$$

It suffices to prove that $\ker(\psi) \subseteq \ker(2\alpha)$. Let us take any element $v \in k^\times$ such that $v \cdot (k^\times)^M \in \ker(\psi)$. Locally at every G-conjugate of $\mathfrak{q}$, v is an M-th power, so all G-conjugates of $\mathfrak{q}$ splits in $k(\zeta_M, v^{\frac{1}{M}})$, which implies that all G-conjugates of $\tau|_{k''} = \tau_3^2 \in \mathrm{Gal}(k''/k')$ act as the identity on $k(\zeta_M, v^{\frac{1}{M}})$.

Consider the fixed field T of $\mathrm{Gal}(k''/k')^2$, the group of squares in $\mathrm{Gal}(k''/k')$. Then $\mathrm{Gal}(T/k')$ is the largest quotient of $\mathrm{Gal}(k''/k')$ that is 2-elementary. Kummer theory gives $T = k(\zeta_M, C^{\frac{1}{M}})$, where C can be taken as a subgroup of V and $C/\ker(\alpha') \cong \mathrm{Gal}(T/k')$. Since $C/\ker(\alpha')$ is 2-elementary, we have $C^2 \subseteq \ker(\alpha')$. For any $c \in C$ it means $2\alpha'(c) = \alpha'(c^2) = 0$, i.e. $c \in \ker(2\alpha')$, so $C \subseteq \ker(2\alpha')$.

Recall that τ_3 generates the G-module $\mathrm{Gal}(k''/k')$, so τ_3^2 generates $\mathrm{Gal}(k''/T)$. Therefore for each $\sigma \in \mathrm{Gal}(k''/T)$ we have $\sigma(v^{\frac{1}{M}}) = v^{\frac{1}{M}}$, hence $v^{\frac{1}{M}} \in T$, which means

$$k(\zeta_M, v^{\frac{1}{M}}) \subseteq k(\zeta_M, C^{\frac{1}{M}}) \subseteq k\big(\zeta_M, \ker(2\alpha')^{\frac{1}{M}}\big)\,,$$

so $v \cdot (k(\zeta_M)^\times)^M \in \ker(2\alpha')$. Thus $v \cdot (k^\times)^M \in \ker(2\alpha)$ as was to be shown.

Finally, since the ring $\mathbb{Z}/M[G]$ is self-injective (see [3, page 162]), the homomorphism $\varphi'\colon\ \mathrm{im}(\psi) \to \mathbb{Z}/M[G]$ can be extended to the desired homomorphism $\varphi\colon (\mathcal{O}_k/q)^\times/M \to \mathbb{Z}/M[G]$.

The proof of Theorem 12 is done. $\square$

In order to prove Theorem 10 we will use the following slightly weaker version of Rubin's Theorem 5.1 published in [4].

Theorem 14 (Rubin)**.** *Let F be an abelian extension of $\mathbb{Q}$, $G = \mathrm{Gal}(F/\mathbb{Q})$. Let q be a rational prime which splits completely in F and let E be a finite extension of F, abelian over $\mathbb{Q}$, such that only primes above q ramify in E/F, but those ramify totally and tamely. Let $\tilde{q}$ be the product of all primes over q in E and let $\mathcal{A}$ be the $\mathbb{Z}/(q-1)[G]$-annihilator of the cokernel of the reduction map*

$$\big\{\varepsilon \in \mathcal{O}_E^\times; N_{E/F}(\varepsilon) = 1\big\} \to (\mathcal{O}_E/\tilde{q})^\times\,.$$

Write $w = \frac{q-1}{[E:F]}$. Then $\mathcal{A} \subseteq w\mathbb{Z}/(q-1)[G]$ and for any prime $\mathfrak{q}$ over q, $w^{-1}\mathcal{A}$ annihilates the ideal class $[\mathfrak{q}] \in Cl(F)/[E:F]$.

Proof of Theorem 10. Choose an arbitrary class $\mathfrak{c} \in Cl_2(k)$. It is possible to perceive $\mathfrak{c}$ as an element of the quotient $Cl(k)/M$.

The M-semispeciality of δ implies that for almost all $q \in \mathcal{Q}_M$ there exists a unit $\delta_q \in k(q)^\times$ satisfying $N_{k(q)/k}(\delta_q) = 1$, such that δ^2 and δ_q have the same image in $(\mathcal{O}_{k(q)}/\tilde{q})^\times/M'$.

For the given module W, the map $\alpha\colon W \to \mathbb{Z}/M[G]$ and the chosen class $\mathfrak{c}$ we use Theorem 12 to get a prime ideal $\mathfrak{q}$ of the field k, such that $\mathfrak{q}$ does not only fulfill all conditions of Theorem 12, but also that the prime q is not one of the finitely many exceptions in $\mathcal{Q}_M$, for which we do not have a unit δ_q.

We have a unit $\delta_q \in \mathcal{O}_k(q)^\times$, such that $N_{k(q)/k}(\delta_q) = 1$ and that δ_q and δ^2 have the same image in $(\mathcal{O}_{k(q)}/\tilde{q})^\times/M'$.

Denote $\mathcal{B} = (\mathcal{O}_{k(q)}/\tilde{q})^\times / \langle \mathrm{im}(\delta_q)\rangle_G$. Let $\mathcal{A}$ be the $\mathbb{Z}/(q-1)[G]$-annihilator of the module $\mathcal{B}$. Then every element $\beta \in \mathcal{A}$ annihilates also the module

$$(\mathcal{O}_{k(q)}/\tilde{q})^\times / \operatorname{im}\left(\{\varepsilon \in \mathcal{O}_{k(q)}^\times ; N_{k(q)/k}(\varepsilon) = 1\}\right).$$

We will use Theorem 14 for $F = k$ and $E = k(q)$, so $w = \frac{q-1}{M} \equiv 2 \pmod{M}$. We obtain that $\frac{1}{2}\beta$ annihilates the class $[\mathfrak{q}] = \mathfrak{c}^2$ in $Cl(k)/M$ and so β annihilates $\mathfrak{c}$ in $Cl(k)/M$.

Since $q \equiv 1 + 2M \pmod{M^2}$, the 2-part of the module $\mathcal{B}$ is equal to

$$\mathcal{B}/2M = ((\mathcal{O}_{k(q)}/\tilde{q})^\times/2M)/\langle \mathrm{im}(\delta_q)\rangle_G$$

and the projection $\mathcal{A}' \subseteq \mathbb{Z}/2M[G]$ of the annihilator $\mathcal{A}$ is the annihilator of $\mathcal{B}/2M$. Obviously every element of $\mathcal{A}'$ annihilates $\mathfrak{c}$ in $Cl(k)/M$, too.

Hence the projection $\mathcal{A}'' \subseteq \mathbb{Z}/M'[G]$ of $\mathcal{A}$ is the annihilator of the module

$$\mathcal{B}/M' = \left((\mathcal{O}_{k(q)}/\tilde{q})^\times/M'\right)/\langle \mathrm{im}(\delta_q)\rangle_G \cong ((\mathcal{O}_k/q)^\times/M')/\langle \psi(\delta^2)\rangle_G\,,$$

where $\psi\colon W \to (\mathcal{O}_k/q)^\times/M'$ is the reduction map (it is the map ψ from Theorem 12 taken modulo M'). And again, every element of $\mathcal{A}''$ annihilates $\mathfrak{c}$ in $Cl(k)/M'$.

To finish the proof, we need to show that $4\alpha(\delta) \in \mathcal{A}''$. The diagram in Theorem 12 gives

$$\begin{tikzcd} W \arrow[r, "2\alpha"] \arrow[d, "\psi"'] & \mathbb{Z}/M'[G] \\ (\mathcal{O}_k/q)^\times/M' \arrow[ur, dotted, "\varphi"'] & \end{tikzcd}$$

Since $(\mathcal{O}_k/q)^\times/M'$ is free cyclic $\mathbb{Z}/M'[G]$ module, one can prove using the same reasoning as in [1, page 197] that $\varphi(\psi(\delta^2)) \in \mathcal{A}''$. Hence $4\alpha(\delta) = 2\alpha(\delta^2) \in \mathcal{A}''$ and the proof is complete. $\square$

Due to Theorem 2 we know that ω_J is M-semispecial. Thus Theorem 10 means that for any finitely generated $\mathbb{Z}[G]$-module $W \subseteq k^\times/M$ containing $\omega_J \cdot (k^\times)^M$ and any $\mathbb{Z}[G]$-homomorphism $\alpha\colon W \to \mathbb{Z}/M[G]$, which is trivial on all classes of W containing a rational number, we get an annihilator $4\alpha(\omega_J)$ of $Cl(k)/M'$.

If K — the genus field of k in narrow sense — is real then Theorem 2 can be stated in the following stronger form:

Theorem 15. *If K is real then the unit $\varkappa_J \in k$ is M-semispecial.*

Proof. Proposition 4.1 of [2] gives that $\varkappa_J \in k$. Let $q \in \mathcal{Q}_M$. Since $\frac{q-1}{M}$ is even, $\mathbb{Q}(q)$ is real. As we assume K being real, for any $S \subseteq J$ the field $K_S(q)$ is real, too. The unit $\varepsilon_{S,q}$ is the norm from the imaginary abelian field $\mathbb{Q}_S(\zeta_q)$ to its real subfield and so it is totally positive. Lemma 6 implies that $\varkappa_q = \varkappa_{J,q}$ is totally positive, too. For any $\sigma \in \mathrm{Gal}(K(q)/k(q))$ we have

$$(\varkappa_q^{\sigma-1})^{[K:k]} = (\varkappa_q^{[K:k]})^{\sigma-1} = \eta_q^{\sigma-1} = 1$$

and so $\varkappa_q^{\sigma-1} = \pm 1$. But $\varkappa_q$ is totally positive and so $\varkappa_q^{\sigma-1} = 1$. It means that $\varkappa_q \in k(q)$.

In the proof of Theorem 2 we have obtained that $N_{K(q)/K}(\varkappa_q) = \pm 1$ and that η_J^2 and η_q have the same image in $(\mathcal{O}_{k(q)}/\tilde{q}_k)^\times/M$. Since we know that $\varkappa_q \in k(q)$ is totally positive, this implies $N_{k(q)/k}(\varkappa_q) = 1$. Identities $\eta_J = \varkappa_J^{[K:k]}$ and $\eta_q = \varkappa_q^{[K:k]}$ give that $\varkappa_J^2$ and $\varkappa_q$ have the same image in $(\mathcal{O}_{k(q)}/\tilde{q}_k)^\times/M'$. □

Example 16. Let us apply our result to the case of a real quadratic field:

Let us consider $k = \mathbb{Q}(\sqrt{p_1 p_2 \dots p_r})$, where $p_1, p_2, \dots p_r$ are different odd primes, all of them congruent to 1 modulo 4, and $r \geq 2$. Let $\gamma > 1$ be the fundamental unit of k and h the class number of k. Consider the module $W = \mathcal{O}_k^\times/M$ and the map $\alpha\colon W \to \mathbb{Z}/M[G]$ determined by $\alpha(\pm\gamma) = 1 - \sigma$, where $G = \{1, \sigma\}$ and M is divisible by the 2-part of h.

Theorems 10 and 15 give that $4\alpha(\varkappa_J)$ annihilates the 2-class group $Cl(k)_2$ of k.

Notice that even stronger result is given by classical theory of quadratic fields:

The Sinnott group of circular units of k is generated by -1 and η_J; its index in $\mathcal{O}_k^\times$ is equal to h (see [5, Theorem 4.1]), so $\eta_J = \pm\gamma^{\pm h}$. Hence $\varkappa_j = \pm\gamma^{\pm h \cdot 2^{1-r}}$ and so $4\alpha(\varkappa_J) = \pm 4h \cdot 2^{1-r}(1-\sigma)$ annihilates $Cl(k)_2$. We have obtained an annihilator $2^{4-r} \cdot h$ of $Cl(k)_2$.

Genus theory gives that the $\mathbb{Z}_2$-rank of $Cl(k)_2$ is equal to $r-1$ and so $Cl(k)_2$ is annihilated by $2^{2-r} \cdot |\,Cl(k)_2|$, which is in fact the quarter of our annihilator.

In the situation of any real quadratic field with an odd discriminant divisible by a prime congruent to 3 modulo 4 the $\mathbb{Z}_2$-rank of $Cl(k)_2$ is equal to $r-2$ and $\varkappa_J^2$ is semispecial. The obtained annihilators are $2^{5-r} \cdot h$ by Theorem 10 and $2^{3-r} \cdot h$ by genus theory.

Therefore for a real quadratic field k and the obtained semispecial unit the constant 4 in the statement of Theorem 10 seems to be superfluous. For fields of a higher degree the question whether $2\alpha(\delta)$ is also an annihilator (see Theorem 10) remains open.

Acknowledgement. The author was supported under the project 201/09/H012 of the Czech Science Foundation.

References

[1] Greither, C., Kučera, R., *Annihilators for the class group of a cyclic field of prime power degree*, Acta Arith. **112** (2) (2004), 177–198.

[2] Kučera, R., *On the class number of a compositum of real quadratic fields: an approach via circular units*, Funct. Approx. Comment. Math. **39** (2008), 179–189.

[3] Lambek, J., *Lectures on rings and modules*, 3rd ed., Chelsea Publishing Co., New York, 1988.

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

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

[6] Thaine, F., *On the ideal class groups of real abelian number fields*, Ann. of Math. (2) **128** (1988), 1–18.

Faculty of Science, Masaryk University,
Kotlářská 2, 611 37 Brno, Czech Republic
E-mail: hermitko@mail.muni.cz