ACTA ARITHMETICA
138.4 (2009)

On totally real Hilbert–Speiser fields of type C_p

by

Cornelius Greither (München) and Henri Johnston (Oxford)

1. Introduction. Let L/K be a finite Galois extension of number fields with Galois group G. Then by a theorem of Noether it is well known that the ring of integers $\mathcal{O}_L$ is a projective module over the group ring $\mathcal{O}_K G$ if and only if L/K is tamely ramified. If $\mathcal{O}_L$ is in fact free (necessarily of rank 1) over $\mathcal{O}_K G$, then L/K is said to have a *normal integral basis*.

A number field K is called a *Hilbert–Speiser field* if every finite abelian tamely ramified extension L/K has a normal integral basis. The celebrated Hilbert–Speiser Theorem says that $\mathbb{Q}$ is such a field, and the main result of [GRRS99] is that $\mathbb{Q}$ is in fact the only such field. By fixing a finite abelian group G one can consider a finer problem: given a number field K, does every tame G-Galois extension L/K have a normal integral basis? If so, K is said to be a *Hilbert–Speiser field of type G*. The simplest case to consider is when $G = C_p$, the cyclic group of prime order p. This has been studied, for instance, in [Car03], [Car04], [Her05], [Ich02], [Ich04], [Ich07a], [Ich07b] and [IST07]. We continue the investigation of this case by establishing the following result, the proof of which is based on a detailed analysis of locally free class groups and ramification indices.

Theorem 1.1. *Let K be a totally real number field and let $p \geq 5$ be prime. Suppose that $K/\mathbb{Q}$ is ramified at p. If $p = 5$ and $[K(\zeta_5) : K] = 2$, assume further that there exists a prime $\mathfrak{p}$ of K above p such that the ramification index of $\mathfrak{p}$ in $K/\mathbb{Q}$ is at least 3. Then K is not Hilbert–Speiser of type C_p.*

Remark 1.2. Some extra conditions in the case $p = 5$ and $[K(\zeta_5) : K] = 2$ are required because, for example, as noted in [Ich07a, Remark 1], $K = \mathbb{Q}(\sqrt{5})$ is in fact Hilbert–Speiser of type C_5.

2000 *Mathematics Subject Classification*: Primary 11R33.
Key words and phrases: Galois module structure, normal integral basis, Hilbert–Speiser field.

DOI: 10.4064/aa138-4-3

Theorem 1.1 can be seen as an analogue of the following result of Herreng (see [Her05, §3]). The authors are grateful to Nigel P. Byott for pointing out that the original hypothesis that $K/\mathbb{Q}$ is Galois can be weakened as below.

THEOREM 1.3 (Herreng). *Let K be a totally imaginary number field and let p be an odd prime. Suppose that every prime $\mathfrak{p}$ of K above p is ramified. If*

(a) $p > [K : \mathbb{Q}]$, *or*
(b) $p \geq 5$ *and* $\zeta_p \in K$, *or*
(c) $p \geq 7$ *and the ramification index in $K/\mathbb{Q}$ of every prime $\mathfrak{p}$ of K above p is at least* 3,

then K is not Hilbert–Speiser of type C_p.

Combining Theorems 1.1 and 1.3(a) we immediately obtain the following result, which in many (but not all) respects is a significant sharpening of [Ich07a, Theorems 1 and 2].

THEOREM 1.4. *Let K be a Hilbert–Speiser field of type C_p for some odd prime p. If either*

(a) *K is totally real and $p \geq 7$, or*
(b) *K is totally imaginary and $p > [K : \mathbb{Q}]$,*

then $K \cap \mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}$ for all $n \geq 1$.

2. Realizable classes. We briefly recall the work of McCulloh on realizable classes in the special case of cyclic extensions of prime degree (see [McC83] for further details).

Let K be a number field and let p be a prime. Let $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ be the group of automorphisms of C_p. Then the locally free class group $\mathrm{Cl}(\mathcal{O}_K C_p)$ is a Δ-module. As L/K varies over all tame C_p-Galois extensions of K, the class $(\mathcal{O}_L)$ of $\mathcal{O}_L$ varies over a subset $R(\mathcal{O}_K C_p)$ of $\mathrm{Cl}(\mathcal{O}_K C_p)$. This subset is in fact a subgroup which can be described explicitly.

Let $\mathrm{Cl}(\mathcal{O}_K)$ denote the ideal class group of K and let $\mathrm{Cl}'(\mathcal{O}_K C_p)$ be the kernel of the map $\mathrm{Cl}(\mathcal{O}_K C_p) \to \mathrm{Cl}(\mathcal{O}_K)$ induced by augmentation. Let $\mathcal{J}$ be the Stickelberger ideal in $\mathbb{Z}\Delta$ (the definition of $\mathcal{J}$ will be given later). The key result of relevance to the present paper is that $R(\mathcal{O}_K C_p)$ is the subgroup $\mathrm{Cl}'(\mathcal{O}_K C_p)^{\mathcal{J}}$ of $\mathrm{Cl}(\mathcal{O}_K C_p)$ where $\mathrm{Cl}'(\mathcal{O}_K C_p)^{\mathcal{J}} = \{c^\alpha : c \in \mathrm{Cl}'(\mathcal{O}_K C_p), \alpha \in \mathcal{J}\}$.

3. The proof of Theorem 1.1. Let K be a totally real number field and let $p \geq 5$ be prime. Let $\mathfrak{p}$ be some prime of K above p and let e denote the ramification index of $\mathfrak{p}$ in $K/\mathbb{Q}$. We will assume that p is ramified in $K/\mathbb{Q}$ and so $\mathfrak{p}$ can be chosen such that $e \geq 2$. Under these hypotheses we

shall show that K is not Hilbert–Speiser of type C_p (note that in the case $p = 5$ and $[K(\zeta_p) : K] = 2$ we shall have to assume that $e \geq 3$).

The basic idea of the proof will be to construct certain $\mathcal{O}_K$-algebras Γ and S such that $\Gamma \subseteq S$ with $S/\Gamma \simeq \mathcal{O}_K/\mathfrak{p}$ as $\mathcal{O}_K$-modules. Together, S and Γ will be used to construct a non-trivial subgroup of the realizable classes $R(\mathcal{O}_K C_p) = \mathrm{Cl}'(\mathcal{O}_K C_p)^{\mathcal{J}}$ described in Section 2, thereby giving the desired result. At all primes $\mathfrak{q} \neq \mathfrak{p}$ of K the completions $S_\mathfrak{q}$ and $\Gamma_\mathfrak{q}$ will be equal, so the essential part of the argument will be local at $\mathfrak{p}$.

Let $\phi_p(z)$ be the pth cyclotomic polynomial. Then $\Gamma := \mathcal{O}_K[z]/(\phi_p(z))$ is an $\mathcal{O}_K$-algebra, but is a domain if and only if $[K(\zeta_p) : K] = p - 1$. The group $\Delta := (\mathbb{Z}/p\mathbb{Z})^\times$ acts on Γ in the following way: to each $\bar{a} \in \Delta$ we associate an automorphism σ_a of Γ defined by $\sigma_a(z) = z^a$, where the image of z in Γ is again written z. Let $\omega : \Delta \to \mathbb{Z}_p^\times$ be the Teichmüller character, so that $\omega(\sigma_a) = \tilde{a}$ where $\tilde{a}^{p-1} = 1$, and $\tilde{a} \equiv a \pmod{p}$.

There exists an element λ such that $\mathbb{Z}_p[\zeta_p] = \mathbb{Z}_p[\lambda]$ with $\lambda^{p-1} = -p$, $\lambda \equiv 1 - \zeta_p \pmod{(1-\zeta_p)^2}$ (see, for example, [Lan90, Chapter 14, Lemma 3.1]). Furthermore, Δ acts on $\lambda^i\mathbb{Z}_p$ through the character ω^i with $i \in \{0, \ldots, p-2\}$. Note that $\Gamma_\mathfrak{p} = \mathcal{O}_{K_\mathfrak{p}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\zeta_p]$, for which $\{1, \lambda, \lambda^2, \ldots, \lambda^{p-2}\}$ is an $\mathcal{O}_{K_\mathfrak{p}}$-basis. Let π denote a parameter of $\mathcal{O}_{K_\mathfrak{p}}$ and define the element $x := (1/\pi) \otimes \lambda^{p-2}$ in $K_\mathfrak{p} \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(\zeta_p) = K_\mathfrak{p}\Gamma$ (we will abuse notation and write $x = \lambda^{p-2}/\pi$).

LEMMA 3.1. *We have* $x^2, x^3, \lambda x, \pi x \in \Gamma_\mathfrak{p}$.

Proof. Since $e \geq 2$, we have $p/\pi^2 \in \mathcal{O}_{K_\mathfrak{p}}$. Hence

$$x^2 = \frac{\lambda^{2p-4}}{\pi^2} = \frac{-p\lambda^{p-3}}{\pi^2} \quad \text{and} \quad x^3 = \frac{(-p)^2\lambda^{p-4}}{\pi^3}$$

are both in $\Gamma_\mathfrak{p}$ (we have used $p \geq 5$ here). Furthermore, it is clear that

$$\lambda x = \frac{\lambda^{p-1}}{\pi} = \frac{-p}{\pi} \quad \text{and} \quad \pi x = \lambda^{p-2}$$

are both in $\Gamma_\mathfrak{p}$. ∎

We shall now consider three cases, the first two of which overlap.

3.1. *The case* $[K(\zeta_p) : K] > 2$. A consequence of Lemma 3.1 is that the $\mathcal{O}_{K_\mathfrak{p}}$-module $T := \Gamma_\mathfrak{p} + x\mathcal{O}_{K_\mathfrak{p}}$ is in fact an $\mathcal{O}_{K_\mathfrak{p}}$-algebra. Furthermore, we have

$$\pi T = \pi\Gamma_\mathfrak{p} + \lambda^{p-2}\mathcal{O}_{K_\mathfrak{p}} \subseteq \Gamma_\mathfrak{p} \subseteq T$$

since λ^{p-2} is part of an $\mathcal{O}_{K_\mathfrak{p}}$-basis of $\Gamma_\mathfrak{p}$. We now let S be the $\mathcal{O}_K$-order defined by

$$S_\mathfrak{q} = \Gamma_\mathfrak{q} \quad (\mathfrak{q} \neq \mathfrak{p}), \qquad S_\mathfrak{p} = T.$$

We find that $\Gamma \subseteq S$ and $\pi S \subseteq \Gamma$ (note that we have abused notation in the obvious way here). Furthermore, the ring $\bar{S} := S/\pi S$ is isomorphic to

$S_\mathfrak{p}/\pi S_\mathfrak{p} = T/\pi T$. Let $\bar{\Gamma}$ be the image of Γ under the canonical map $S \to \bar{S}$. We have a Milnor square

$$\begin{array}{ccc} \Gamma & \hookrightarrow & S \\ \downarrow & & \downarrow \\ \bar{\Gamma} & \hookrightarrow & \bar{S} \end{array}$$

where the horizontal arrows are the natural inclusions and the vertical arrows are the natural projections (note that this is a special case of a fiber product). Note that we have $\delta(\lambda^{p-2}) \equiv \omega^{p-2}(\delta)\lambda^{p-2}$ modulo $p\mathbb{Z}_p[\zeta_p]$ for every $\delta \in \Delta$, so $\delta(x) \in x + \Gamma \subset S$. Hence Δ acts on S and so acts on each of the rings in the Milnor square. By [CR87, p. 242] we have the following exact sequence

$$\mathrm{K}_1(S) \times \mathrm{K}_1(\bar{\Gamma}) \to \mathrm{K}_1(\bar{S}) \to \mathrm{Cl}(\Gamma) \to \mathrm{Cl}(S) \to 0.$$

As all the rings above are commutative, this becomes

$$S^\times \times \bar{\Gamma}^\times \to \bar{S}^\times \to \mathrm{Cl}(\Gamma) \to \mathrm{Cl}(S) \to 0.$$

Hence we have an embedding of Δ-modules

$$N := \frac{\bar{S}^\times}{\bar{\Gamma}^\times \cdot \mathrm{im}(S^\times)} \hookrightarrow \mathrm{Cl}(\Gamma),$$

where $\mathrm{im}(S^\times)$ is the image of $S^\times$ under the map $S \to \bar{S}$.

For every Δ-module X, let X^- and $X^{\omega^{-1}}$ denote the minus part and the ω^{-1}-part of $\mathbb{Z}_p \otimes_\mathbb{Z} X$, respectively. Then $X^{\omega^{-1}} \subseteq X^-$. We will show that $N^{\omega^{-1}}$ contains a submodule M of order p. Note that by the definition of x and the action of Δ, we have $x \in S^{\omega^{-1}}$. We define $\bar{x} \in \bar{S}$ to be the image of $x \in T$ under the natural projection $T \to T/\pi T \simeq \bar{S}$ and note that $\bar{x} \in \bar{S}^{\omega^{-1}}$.

Let $[\exp](z) := \sum_{i=0}^{p-1}(1/i!)z^i$ denote the truncated exponential series. Whenever the ideal (a, b) generated by a and b satisfies $(a, b)^p = 0$, we have $[\exp](a + b) = [\exp](a) \cdot [\exp](b)$ (see the proof of [CGM+98, p-elementary group schemes—constructions and Raynaud's theory, Remark 1.1]). Let $y := [\exp](\bar{x}) \in \bar{S}$. Since $y^p = [\exp](p\bar{x}) = [\exp](0) = 1$, we have $y \in \bar{S}^\times$. We note that $y \notin \bar{\Gamma}$ (the summand with $i = 1$ is $\bar{x}$ and hence plainly outside $\bar{\Gamma}$, and all other summands are in $\bar{\Gamma}$ by Lemma 3.1). Moreover, as [exp] is compatible with the Δ-action, we have $y \in (\bar{S}^\times)^{\omega^{-1}} = \bar{S}^\times \cap \bar{S}^{\omega^{-1}}$.

LEMMA 3.2. *We have* $(\bar{\Gamma}^\times \cdot \mathrm{im}(S^\times))^{\omega^{-1}} = (\bar{\Gamma}^\times)^{\omega^{-1}}$.

Proof. Let $\mathfrak{M}$ denote the maximal order in $KS = K\Gamma$. Then $\mathfrak{M} = \mathrm{ind}_{\Delta_0}^{\Delta} \mathcal{O}_{K(\zeta_p)}$ with $\Delta_0 = \mathrm{Gal}(K(\zeta_p)/K)$. We consider $S^{\times -} \subseteq \mathfrak{M}^{\times -}$; since K is totally real, complex conjugation $j \in \Delta_0$ acts on each factor of $\mathfrak{M}$ separately, and we see that $\mathcal{O}_{K(\zeta_p)}^{\times -}$ is the multiplicative group of roots of unity $\langle \zeta_{p^f} \rangle$ for some $f \geq 1$ (see [Was97, Theorem 4.12]). Hence $\mathfrak{M}^{\times -} = \mathrm{ind}_{\Delta_0}^{\Delta} \langle \zeta_{p^f} \rangle$.

Suppose that $f = 1$. Then Δ_0 acts on ζ_p via $\omega|_{\Delta_0}$, and from the Frobenius reciprocity theorem one deduces that $\mathrm{ind}_{\Delta_0}^{\Delta}\langle\zeta_p\rangle$ has non-trivial ω^{-1}-part if and only if $\omega^{-1}|_{\Delta_0} = \omega|_{\Delta_0}$, that is, if and only if ω^2 is trivial on Δ_0. But this is not the case since $[K(\zeta_p) : K] = |\Delta_0| > 2$ by hypothesis. Now suppose $f > 1$. Then considering the short exact sequence

$$1 \to \mathrm{ind}_{\Delta_0}^{\Delta}\langle\zeta_{p^{f-1}}\rangle \to \mathrm{ind}_{\Delta_0}^{\Delta}\langle\zeta_{p^f}\rangle \to \mathrm{ind}_{\Delta_0}^{\Delta}\langle\zeta_p\rangle \to 1,$$

we see that the middle term has trivial ω^{-1}-part if and only if the same is true of both the outer terms. It now follows by induction on f that $\mathfrak{M}^{\times -} = \mathrm{ind}_{\Delta_0}^{\Delta}\langle\zeta_{p^f}\rangle$ has trivial ω^{-1}-part. Hence $(S^\times)^{\omega^{-1}}$ is trivial, and the lemma is proved. ∎

Let $\bar{y}$ denote the projection of y to N. If $\bar{y}$ were trivial in N, then y would have to be in $(\bar{\Gamma}^\times \cdot \mathrm{im}(S^\times))^{\omega^{-1}} = (\bar{\Gamma}^\times)^{\omega^{-1}}$. However, we have already noted that y is not even in $\bar{\Gamma}$. Hence $M := \langle\bar{y}\rangle$ is a non-trivial Δ-submodule of N with $M^{\omega^{-1}} = M$.

3.2. *The case $e \geq 4$.* Let $x_1 = x = \lambda^{p-2}/\pi = (1/\pi) \otimes \lambda^{p-2}$ be as above and define $x_2 = \lambda^{p-2}/\pi^2 = (1/\pi^2) \otimes \lambda^{p-2}$.

LEMMA 3.3. *We have $x_2^2, x_2^3, \lambda x_2, \pi^2 x_2, x_1 x_2, x_1^2 x_2, x_1 x_2^2 \in \Gamma_{\mathfrak{p}}$.*

Proof. We use the assumption that $p \geq 5$ without further mention. Since $e \geq 4$, we have $p/\pi^4 \in \mathcal{O}_{K_{\mathfrak{p}}}$. Hence

$$x_2^2 = \frac{\lambda^{2p-4}}{\pi^4} = \frac{-p\lambda^{p-3}}{\pi^4} \quad \text{and} \quad x_2^3 = \frac{p^2\lambda^{p-4}}{\pi^6}$$

are both in $\Gamma_{\mathfrak{p}}$. Furthermore, it is clear that

$$\lambda x_2 = \frac{\lambda^{p-1}}{\pi^2} = \frac{-p}{\pi^2} \quad \text{and} \quad \pi^2 x_2 = \lambda^{p-2}$$

are both in $\Gamma_{\mathfrak{p}}$. Finally,

$$x_1 x_2 = \frac{\lambda^{2p-4}}{\pi^3} = \frac{(-p)\lambda^{p-3}}{\pi^3}, \quad x_1^2 x_2 = \frac{\lambda^{3p-6}}{\pi^4} = \frac{(-p)^2\lambda^{p-4}}{\pi^4}, \quad \text{and}$$
$$x_1 x_2^2 = \frac{\lambda^{3p-6}}{\pi^5} = \frac{(-p)^2\lambda^{p-4}}{\pi^5}$$

are all in $\Gamma_{\mathfrak{p}}$. ∎

A consequence of Lemmas 3.1 and 3.3 is that the $\mathcal{O}_{K_{\mathfrak{p}}}$-module $T := \Gamma_{\mathfrak{p}} + x_1\mathcal{O}_{K_{\mathfrak{p}}} + x_2\mathcal{O}_{K_{\mathfrak{p}}}$ is in fact an $\mathcal{O}_{K_{\mathfrak{p}}}$-algebra. Furthermore, we have

$$\pi^2 T = \pi^2\Gamma_{\mathfrak{p}} + \pi\lambda^{p-2}\mathcal{O}_{K_{\mathfrak{p}}} + \lambda^{p-2}\mathcal{O}_{K_{\mathfrak{p}}} = \pi^2\Gamma_{\mathfrak{p}} + \lambda^{p-2}\mathcal{O}_{K_{\mathfrak{p}}} \subseteq \Gamma_{\mathfrak{p}} \subseteq T$$

since λ^{p-2} is part of an $\mathcal{O}_{K_{\mathfrak{p}}}$-basis of $\Gamma_{\mathfrak{p}}$. We now let S be the $\mathcal{O}_K$-order defined by

$$S_{\mathfrak{q}} = \Gamma_{\mathfrak{q}} \quad (\mathfrak{q} \neq \mathfrak{p}), \qquad S_{\mathfrak{p}} = T.$$

Then $\Gamma \subseteq S$ and $\pi^2 S \subseteq \Gamma$. The same argument as in the previous case gives an embedding of Δ-modules

$$N := \frac{\bar{S}^\times}{\bar{\Gamma}^\times \cdot \mathrm{im}(S^\times)} \hookrightarrow \mathrm{Cl}(\Gamma).$$

By definition of x_1, x_2 and the action of Δ, we have $x_1, x_2 \in S^{\omega^{-1}}$. Let $y_1 = [\exp](\bar{x}_1)$, $y_2 = [\exp](\bar{x}_2) \in \bar{S} = S/\pi^2 S$. As in the previous case, both y_1, y_2 are elements of order p in $(\bar{S}^\times)^{\omega^{-1}}$.

LEMMA 3.4. *$(S^\times)^{\omega^{-1}}$ is cyclic.*

Proof. Let $\mathfrak{M}$ denote the maximal order in $KS = K\Gamma$. As $S \subseteq \mathfrak{M}$, we have $(S^\times)^{\omega^{-1}} \subseteq (\mathfrak{M}^\times)^{\omega^{-1}}$, and so it suffices to show that $(\mathfrak{M}^\times)^{\omega^{-1}}$ is a cyclic group.

By the same argument as for Lemma 3.2, we obtain $\mathfrak{M}^{\times -} = \mathrm{ind}_{\Delta_0}^{\Delta} \langle \zeta_{p^f} \rangle$. Furthermore, as ω^{-1} is an odd character, we have $(\mathfrak{M}^\times)^{\omega^{-1}} \subseteq \mathfrak{M}^{\times -}$. Now $\langle \zeta_{p^f} \rangle$ is trivially cyclic as a $\mathbb{Z}_p[\Delta_0]$-module; hence

$$\mathfrak{M}^{\times -} = \mathrm{ind}_{\Delta_0}^{\Delta} \langle \zeta_{p^f} \rangle = \mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p[\Delta_0]} \langle \zeta_{p^f} \rangle$$

is cyclic as a $\mathbb{Z}_p[\Delta]$-module. Thus $(\mathfrak{M}^\times)^{\omega^{-1}} = \mathbb{Z}_p(\omega^{-1}) \otimes_{\mathbb{Z}_p[\Delta]} \mathfrak{M}^{\times -}$ is cyclic as a $\mathbb{Z}_p(\omega^{-1})$-module, where $\mathbb{Z}_p(\omega^{-1})$ is the ring extension of $\mathbb{Z}_p$ obtained by adjoining the image of ω^{-1}. However, ω^{-1} takes its values in $\mathbb{Z}_p^\times$, and so $\mathbb{Z}_p(\omega^{-1}) = \mathbb{Z}_p$. Therefore $(\mathfrak{M}^\times)^{\omega^{-1}}$ is cyclic as a $\mathbb{Z}_p$-module, and hence is cyclic as a group. ∎

Let $\tilde{y}_1, \tilde{y}_2 \in (\bar{S}^\times/\bar{\Gamma}^\times)^{\omega^{-1}}$ be the images of y_1, y_2 under the natural projection. Since $y_1, y_2 \notin \bar{\Gamma}$ (the summand with $i = 1$ is outside $\bar{\Gamma}$ and all others are in $\bar{\Gamma}$ by Lemmas 3.1 and 3.3), $\tilde{y}_1, \tilde{y}_2$ are also each of order p. Suppose that $\tilde{y}_1^{k_1} \tilde{y}_2^{k_2}$ is trivial for some $k_1, k_2 \in \{1, \ldots, p-1\}$. This would mean that $[\exp](k_1\bar{x}_1 + k_2\bar{x}_2)$ is in $\bar{\Gamma}$. By virtue of Lemma 3.3, we have $[\exp](k_1\bar{x}_1 + k_2\bar{x}_2) \equiv 1 + k_1\bar{x}_1 + k_2\bar{x}_2$ modulo $\bar{\Gamma}$. Therefore we would obtain $k_1\bar{x}_1 + k_2\bar{x}_2 \in \bar{\Gamma}$ and so $k_1x_1 + k_2x_2 \in \Gamma_\mathfrak{p}$, which is impossible. Hence the subgroup $\langle \tilde{y}_1, \tilde{y}_2 \rangle \simeq \langle y_1, y_2 \rangle \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is non-cyclic. Let $\bar{y}_1, \bar{y}_2$ be the projections of $\tilde{y}_1, \tilde{y}_2$ to N and let $M := \langle \bar{y}_1, \bar{y}_2 \rangle \subseteq N^{\omega^{-1}}$. Note that M is non-trivial because $(\mathrm{im}(S^\times))^{\omega^{-1}}$ is cyclic by Lemma 3.4, but $\langle \tilde{y}_1, \tilde{y}_2 \rangle$ is non-cyclic. Hence M is a non-trivial Δ-submodule of N with $M^{\omega^{-1}} = M$.

3.3. *The case $[K(\zeta_p) : K] = 2$ and $e = 2$ or 3.* Note that the condition $[K(\zeta_p) : K] = 2$ implies that $(p-1)/2$ divides e. Hence we are reduced to considering the cases $p = 5$ and $p = 7$ (since $p \geq 11$ forces $e \geq 5$). If $p = 5$, then e must be even and so in fact $e = 2$. However, this case is excluded by hypothesis. If $p = 7$, then we must have $e = 3$. In this case, we

let $x_1 = \lambda^5/\pi$, $x_2 = \lambda^5/\pi^2$ and $x_3 = \lambda^4/\pi$. It is straightforward to check that the $\mathcal{O}_{K_\mathfrak{p}}$-module $T := \Gamma_\mathfrak{p} + x_1\mathcal{O}_{K_\mathfrak{p}} + x_2\mathcal{O}_{K_\mathfrak{p}} + x_3\mathcal{O}_{K_\mathfrak{p}}$ is in fact an $\mathcal{O}_{K_\mathfrak{p}}$-algebra. The result is then given by a slight variant of the proof of the previous case (note that $x_1, x_2 \in S^{\omega^{-1}}$ but $x_3 \notin S^{\omega^{-1}}$).

3.4. *The proof of Theorem 1.1.* In each of the above cases, we have shown that there exists a non-trivial Δ-submodule M of $\mathrm{Cl}(\Gamma)$ such that $M^{\omega^{-1}} = M$.

Proof of Theorem 1.1. Recall that the Stickelberger ideal is defined to be $\mathcal{J} = \mathbb{Z}\Delta \cap \theta \cdot \mathbb{Z}\Delta = \mathrm{Ann}_\Delta(\langle\zeta_p\rangle) \cdot \theta$ where θ is the Stickelberger element $p^{-1}\sum_{j=1}^{p-2} j\sigma_j^{-1}$. Let $\mathcal{J}_p \subseteq \mathbb{Z}_p\Delta$ be the p-completion of $\mathcal{J}$. Then $\omega^{-1}(\mathcal{J}_p) = \omega^{-1}(\mathrm{Ann}_\Delta(\langle\zeta_p\rangle)) \cdot \omega^{-1}\theta$. The second factor of the last expression is the generalized Bernoulli number $B_{1,\omega}$. Since $p \geq 5$, the first factor is $\mathbb{Z}_p$. By [Was97, Corollary 5.15] we have $B_{1,\omega} \equiv B_2/2 = 1/12 \pmod p$. Hence, $M^\mathcal{J} = M^{\omega^{-1}(\mathcal{J}_p)} = M^{\mathbb{Z}_p} = M$ and therefore $\mathrm{Cl}(\Gamma)^\mathcal{J} \neq 0$.

Let Σ denote the sum of the elements of C_p. Consider the following Milnor square:

$$\begin{array}{ccc} \mathcal{O}_K C_p & \xrightarrow{\alpha} & \mathcal{O}_K C_p/\mathcal{O}_K\Sigma =: \Lambda \\ \downarrow \beta & & \downarrow \gamma \\ \mathcal{O}_K & \to & \mathcal{O}_K/p\mathcal{O}_K \end{array}$$

where the horizontal maps are the natural projections, β is the augmentation map, and γ is the map induced by augmentation. The resulting map

$$\mathrm{Cl}(\mathcal{O}_K C_p) \xrightarrow{(\alpha,\beta)} \mathrm{Cl}(\Lambda) \times \mathrm{Cl}(\mathcal{O}_K)$$

is surjective (see, for instance, [CR87, Corollary 49.28]). It follows immediately that

$$\mathrm{Cl}'(\mathcal{O}_K C_p) \to \mathrm{Cl}(\Lambda)$$

is surjective. However, $\mathrm{Cl}(\Lambda) \simeq \mathrm{Cl}(\Gamma)$ since $\Lambda \simeq \Gamma$, and so $\mathrm{Cl}(\Lambda)^\mathcal{J} \neq 0$. Therefore $\mathrm{Cl}'(\mathcal{O}_K C_p)^\mathcal{J} = R(\mathcal{O}_K C_p) \neq 0$, and so K is not a Hilbert–Speiser field of type C_p. ∎

Acknowledgments. The authors are grateful to the Deutscher Akademischer Austausch Dienst (German Academic Exchange Service) for a grant allowing the second named author to visit the first for the 2006–07 academic year, thus making this collaboration possible.

The authors are indebted to James E. Carter for suggesting the original problem, to Nigel P. Byott for pointing out an error in an earlier version of this paper, and to both the aforementioned and the referee for several helpful comments and suggestions.

References

[Car03] J. E. Carter, *Normal integral bases in quadratic and cyclic cubic extensions of quadratic fields*, Arch. Math. (Basel) 81 (2003), 266–271.

[Car04] —, *Erratum to*: [Car03], ibid. 83 (2004), no. 6, vi–vii.

[CGM+98] L. N. Childs, C. Greither, D. J. Moss, J. Sauerberg, and K. Zimmermann, *Hopf algebras*, *polynomial formal groups*, *and Raynaud orders*, Mem. Amer. Math. Soc. 136 (1998), no. 651.

[CR87] C. W. Curtis and I. Reiner, *Methods of Representation Theory. With Applications to Finite Groups and Orders. Vol. II*, Pure Appl. Math. (New York), Wiley, New York, 1987.

[GRRS99] C. Greither, D. R. Replogle, K. Rubin, and A. Srivastav, *Swan modules and Hilbert–Speiser number fields*, J. Number Theory 79 (1999), 164–173.

[Her05] T. Herreng, *Sur les corps de Hilbert–Speiser*, J. Théor. Nombres Bordeaux 17 (2005), 767–778.

[Ich02] H. Ichimura, *Note on the ring of integers of a Kummer extension of prime degree. V*, Proc. Japan Acad. Ser. A Math. Sci. 78 (2002), 76–79.

[Ich04] —, *Normal integral bases and ray class groups*, Acta Arith. 114 (2004), 71–85.

[Ich07a] —, *Note on Hilbert–Speiser number fields at a prime p*, Yokohama Math. J. 54 (2007), 45–53.

[Ich07b] —, *Note on imaginary quadratic fields satisfying the Hilbert–Speiser condition at a prime p*, Proc. Japan Acad. Ser. A Math. Sci. 83 (2007), 88–91.

[IST07] H. Ichimura and H. Sumida-Takahashi, *Imaginary quadratic fields satisfying the Hilbert–Speiser type condition for a small prime p*, Acta Arith. 127 (2007), 179–191.

[Lan90] S. Lang, *Cyclotomic Fields I and II*, 2nd ed., Grad. Texts in Math. 121, Springer, New York, 1990.

[McC83] L. R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra 82 (1983), 102–134.

[Was97] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

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

St. Hugh's College
St. Margaret's Road
Oxford OX2 6LE, U.K.
E-mail: henri@maths.ox.ac.uk
http://people.maths.ox.ac.uk/henri

Received on 17.9.2008
and in revised form on 26.2.2009 (5730)