Illinois Journal of Mathematics
Volume 55, Number 2, Summer 2011, Pages 623–639
S 0019-2082

ON THE RESTRICTED HILBERT–SPEISER AND LEOPOLDT PROPERTIES

NIGEL P. BYOTT, JAMES E. CARTER, CORNELIUS GREITHER AND HENRI JOHNSTON

Abstract. Let G be a finite abelian group. A number field K is called a Hilbert–Speiser field of type G if, for every tame G-Galois extension L/K, the ring of integers $\mathcal{O}_L$ is free as an $\mathcal{O}_K[G]$-module. If $\mathcal{O}_L$ is free over the associated order $\mathcal{A}_{L/K}$ for every G-Galois extension L/K, then K is called a Leopoldt field of type G. It is well known (and easy to see) that if K is Leopoldt of type G, then K is Hilbert–Speiser of type G. We show that the converse does not hold in general, but that a modified version does hold for many number fields K (in particular, for $K/\mathbb{Q}$ Galois) when $G = C_p$ has prime order. We give examples with $G = C_5$ to show that even the modified converse is false in general, and that the modified converse can hold when the original does not.

1. Introduction

Let L/K be a finite abelian extension of number fields with Galois group G. The associated order is defined to be $\mathcal{A}_{L/K} := \{x \in K[G] : x(\mathcal{O}_L) \subseteq \mathcal{O}_L\}$. In the case $K = \mathbb{Q}$, Leopoldt's theorem [17] shows that the ring of integers $\mathcal{O}_L$ of L is free as a module over $\mathcal{A}_{L/\mathbb{Q}}$. (A simplified proof of this result can be found in [18].) More generally, we say that a number field K is Leopoldt if, for every finite abelian extension L/K, the ring of integers $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ (note that this differs from the definition of Leopoldt given in [15]). Since $\mathcal{A}_{L/K} = \mathcal{O}_K[G]$ if and only if L/K is tame, Leopoldt's theorem implies the celebrated Hilbert–Speiser theorem: Every tame finite abelian extension L of $\mathbb{Q}$ has a normal integral basis, that is, $\mathcal{O}_L$ is free as a $\mathbb{Z}[G]$-module. (In this paper, we shall take "tame" to mean "at most tamely ramified".) A number field

Received November 4, 2009; received in final form March 10, 2010.
2010 *Mathematics Subject Classification.* 11R33, 11R29.

©2013 University of Illinois

K is called a Hilbert–Speiser field if, for every tame finite abelian extension L/K, the ring of integers $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$; in particular, $\mathbb{Q}$ is such a field. The same reasoning as above shows that if K is Leopoldt then K is Hilbert–Speiser. The converse follows from Leopoldt's theorem and the result proven in [13] that $\mathbb{Q}$ is the only Hilbert–Speiser field. Hence, we have the following observation.

THEOREM 1.1. *Let K be a number field. Then K is a Hilbert–Speiser field if and only if K is a Leopoldt field.*

The question arises as to whether a similar result holds when one fixes the group G.

DEFINITION 1.2. Let G be a finite abelian group and let K be a number field. Then K is a *Hilbert–Speiser field of type* G if, for every tame G-Galois extension L/K, the ring of integers $\mathcal{O}_L$ is free as an $\mathcal{O}_K[G]$-module. Furthermore, K is a *Leopoldt field of type* G if, for every G-Galois extension L/K, the ring of integers $\mathcal{O}_L$ is free as an $\mathcal{A}_{L/K}$-module.

The following conjecture was stated in [8], and proved there in the case in which $G = C_p$ is cyclic of prime order p and K contains a primitive pth root of unity ζ_p (see [8, Theorem 1.2]).

CONJECTURE 1.3. *Let K be a number field and let G be a finite abelian group. Then K is a Hilbert–Speiser field of type G if and only if K is a Leopoldt field of type G. We denote this statement by* HS-L(K, G).

Miyata [21] has investigated the integral Galois module structure of wildly ramified extensions L/K of number fields of prime degree. A careful reading of his paper suggests that one should expect the $\mathcal{O}_K$-ideal $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ to be a global obstruction to the freeness of $\mathcal{O}_L$ over $\mathcal{A}_{L/K}$. It is therefore natural to consider the adjusted module $\mathrm{Tr}_{L/K}(\mathcal{O}_L)^{-1}\mathcal{O}_L$ in place of $\mathcal{O}_L$ itself. We mention also a related situation where a similar adjustment is known to be necessary: see for example [26, Chapter III, Section 3]. Let K be a number field, G a finite abelian group, and $\mathcal{H}$ a Hopf order in $K[G]$. If L is a Galois extension of K with group G whose associated order $\mathcal{A}_{L/K}$ coincides with $\mathcal{H}$, then $\mathcal{O}_L$ is locally free over $\mathcal{H}$. Moreover $\mathcal{O}_L$ can be regarded (under a mild hypothesis on $\mathcal{H}$) as a principal homogeneous space over the dual Hopf order $\mathcal{H}^*$ to $\mathcal{H}$. There is a "class invariant" homomorphism from the group of principal homogeneous spaces over $\mathcal{H}^*$ into the locally free class group $\mathrm{Cl}(\mathcal{H})$. This associates to $\mathcal{O}_L$ the class $(\mathcal{H}^*)^{-1}(\mathcal{O}_L) = (\mathrm{Tr}_{L/K}(\mathcal{O}_L)^{-1}\mathcal{O}_L)$. On the other hand, the map which simply associates to $\mathcal{O}_L$ its class $(\mathcal{O}_L)$ in $\mathrm{Cl}(\mathcal{H})$ need not be a homomorphism. This lends further support to the idea that, in general, the class $(\mathrm{Tr}_{L/K}(\mathcal{O}_L)^{-1}\mathcal{O}_L)$ may be a more natural object to study than $(\mathcal{O}_L)$ itself.

In the light of these observations, we consider in this article the following modified versions of Definition 1.2 and Conjecture 1.3.

DEFINITION 1.4. Let G be a finite abelian group and let K be a number field. Then K is said to satisfy the *modified Leopoldt condition of type* G if, for every G-Galois extension L/K, the adjusted ring of integers $\mathrm{Tr}_{L/K}(\mathcal{O}_L)^{-1}\mathcal{O}_L$ is free as an $\mathcal{A}_{L/K}$-module.

CONJECTURE 1.5. *Let K be a number field and let G be a finite abelian group. If K is a Hilbert–Speiser field of type G, then K satisfies the modified Leopoldt condition of type G. We denote this statement by* mHS-L(K, G).

We observe immediately that $\mathrm{Tr}_{L/K}(\mathcal{O}_L)^{-1}\mathcal{O}_L$ is *locally* free over $\mathcal{A}_{L/K}$ if and only if $\mathcal{O}_L$ is. Moreover, $\mathrm{Tr}_{L/K}(\mathcal{O}_L)^{-1}\mathcal{O}_L$ and $\mathcal{O}_L$ are isomorphic as $\mathcal{A}_{L/K}$-modules if and only if $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is a principal $\mathcal{O}_K$-ideal. Thus, for a number field K which is Hilbert–Speiser of type G, there are potentially two ways in which Conjecture 1.3 (respectively, Conjecture 1.5) might fail. On the one hand, it might fail locally, so that there is some G-Galois extension L of K for which $\mathcal{O}_L$ (and hence also $\mathrm{Tr}_{L/K}(\mathcal{O}_L)^{-1}\mathcal{O}_L$) is not even locally free over $\mathcal{A}_{L/K}$. On the other hand, genuinely global failure may occur, so that there is a G-Galois extension L of K for which $\mathcal{O}_L$ (respectively, $\mathrm{Tr}_{L/K}(\mathcal{O}_L)^{-1}\mathcal{O}_L$) is locally free over $\mathcal{A}_{L/K}$, but not free over $\mathcal{A}_{L/K}$.

We shall show that neither conjecture is true in general, and indeed that both local and global failure can occur. We shall prove, nevertheless, that Conjecture 1.5 holds in many interesting cases. Specifically, we show first that both conjectures can fail locally if G is the elementary abelian group $C_2 \times C_2$.

THEOREM 1.6. *Let K be a number field such that the ray class group $\mathrm{Cl}_4(\mathcal{O}_K)$ modulo $4\mathcal{O}_K$ is trivial, and such that some prime $\mathfrak{p}$ of K above 2 has absolute ramification index at least 3. Let $G = C_2 \times C_2$. Then K is Hilbert–Speiser of type G, but there exists a G-Galois extension L of K such that $\mathcal{O}_L$ is not locally free over $\mathcal{A}_{L/K}$.*

COROLLARY 1.7. HS-L$(K, C_2 \times C_2)$ *does not hold if K is any of the three real cubic fields $\mathbb{Q}(\alpha_i)$, $1 \le i \le 3$, where α_1, α_2, α_3 is a zero of $x^3 + x^2 - 3x - 1$, $x^3 - x^2 - 5x - 1$, $x^3 + x^2 - 5x - 3$, respectively.*

We shall then specialise to the case where $G = C_p$ is cyclic of prime order p, as in [8]. The above-mentioned work of Miyata allows us to prove the following key proposition, which in particular shows that global failure of mHS-L(K, C_p) cannot occur.

PROPOSITION 1.8. *A number field K satisfies the modified Leopoldt condition of type C_p if and only if*

(a) *K is Hilbert–Speiser of type C_p; and*
(b) *for every wildly ramified C_p-Galois extension L/K, the ring of integers $\mathcal{O}_L$ is locally free over its associated order $\mathcal{A}_{L/K}$.*

Hence, mHS-L(K, C_p) *holds if and only if either* (a) *does not hold or* (b) *does hold.*

With this in mind, we point out the main result of [12]. Its proof is based on a detailed analysis of locally free class groups and ramification indices.

THEOREM 1.9. *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 with absolute ramification index at least* 3. *Then K is not Hilbert–Speiser of type C_p.*

We can often verify part (b) of Proposition 1.8 by using the results of [1] and [2]. In other cases, we can quote existing results in the literature showing that K is not Hilbert–Speiser of type C_p (see [12], [14]). Combining all of these results gives the following theorem.

THEOREM 1.10. *Let p be a prime and let K be a number field. Suppose that at least one of the following conditions holds*:

(a) $p = 2$ *or* 3,
(b) $K/\mathbb{Q}$ *is unramified at* p,
(c) K *is totally real*, *or*
(d) K *is* (*totally*) *imaginary and* $K/\mathbb{Q}$ *is Galois.*

Then mHS-L(K, C_p) *holds.*

COROLLARY 1.11. *Let p be a prime and let K be a number field such that $K/\mathbb{Q}$ is Galois. Then* mHS-L(K, C_p) *holds.*

REMARK 1.12. Since the only primes of K which divide $\mathrm{Tr}_{L/K}(\mathcal{O}_K)$ are those which are wildly ramified in L/K, the conjectures mHS-L(K, C_p) and HS-L(K, C_p) coincide if every prime of K above p is principal. In this case (for instance, if p remains prime in K, or if K has class number 1) one can replace "mHS-L(K, C_p)" with "HS-L(K, C_p)" in the conclusions of Theorem 1.10 and Corollary 1.11.

We end the paper with some explicit examples. Firstly, we exhibit a sextic field which is not Galois over $\mathbb{Q}$, and for which mHS-L(K, C_5) (and also HS-L(K, C_5)) does not hold. This suggests that one should not expect any significant strengthening of Theorem 1.10 to be possible. Secondly, we justify the introduction of the conjecture mHS-L(K, G) in place of HS-L(K, G) by giving several examples of quartic fields K satisfying condition (b) of Theorem 1.10, so that mHS-L(K, C_5) holds, but for which HS-L(K, C_5) does *not* hold.

2. Local failure for elementary abelian extensions of degree 4

In this section, we prove Theorem 1.6 and Corollary 1.7. We first need a criterion which, for a G-Galois extension N/M of p-adic fields, guarantees

that the valuation ring $\mathcal{O}_N$ of N is *not* free over its associated order $\mathcal{A}_{N/M}$. Such a criterion is given by [5, Theorem 3.13]. It is valid for any abelian p-group G, and in fact applies not just to $\mathcal{O}_N$ but to any power $\mathfrak{P}^h$ of the maximal ideal $\mathfrak{P}$ of $\mathcal{O}_N$. Specialising to the case $p=2$, $G=C_2\times C_2$, N/M is totally ramified, and $h=0$, this result reads as follows.

LEMMA 2.1. *Let M be a finite extension of $\mathbb{Q}_2$ with absolute ramification index e. Let N/M be a totally ramified $C_2\times C_2$-Galois extension with ramification numbers $t_1\le t_2$ (in the lower numbering). Suppose further that*

$$t_2-\left\lfloor\frac{t_2}{2}\right\rfloor<2e. \tag{1}$$

Let w be the valuation of the different of N/M, and for $a\in\mathbb{Z}$ let $\overline{a}$ denote the least non-negative residue of a modulo 4. Then $\mathcal{O}_N$ is not *free over $\mathcal{A}_{N/M}$ if, for at least one value of $i\in\{1,2\}$, we have*

$$3>\overline{t}_i>\overline{w}. \tag{2}$$

By Hilbert's formula for the different [25, Chapter IV, Section 1, Proposition 4], we have $w=3(t_1+1)+(t_2-t_1)$. Since t_1 and t_2 must both be odd [25, Chapter IV, Section 2, Proposition 11 and Exercise 3(f)], it follows that

$$\overline{w}=3-\overline{t}_2. \tag{3}$$

We now turn to the question of recognising Hilbert–Speiser fields of type $C_2\times C_2$.

PROPOSITION 2.2. *Let K be a number field such that $\mathrm{Cl}_4(\mathcal{O}_K)$ is trivial. Then K is Hilbert–Speiser of type $C_2\times C_2$.*

Proof. For any finite group G, the ring of integers $\mathcal{O}_L$ in a tame G-Galois extension L of K is a locally free $\mathcal{O}_K[G]$-module of rank 1. Moreover, if G is abelian, then a locally free $\mathcal{O}_K[G]$-module is determined up to isomorphism by its rank and its class in the locally free class group $\mathrm{Cl}(\mathcal{O}_K[G])$. Thus, if $\mathrm{Cl}(\mathcal{O}_K[G])$ is trivial, then $\mathcal{O}_L$ is necessarily free for any such L, and K is Hilbert–Speiser of type G.

We now take $G=C_2\times C_2$. By [20, Section 2] (or, more explicitly, [6, Proposition 2.4]), $\mathrm{Cl}(O_K[G])$ is isomorphic to a certain quotient of 4 copies of $\mathrm{Cl}_4(O_K)$. Thus, the triviality of $\mathrm{Cl}_4(\mathcal{O}_K)$ implies that of $\mathrm{Cl}(\mathcal{O}_K[G])$. □

Proof of Theorem 1.6. Let K be as in the statement of the theorem, and let $G=C_2\times C_2$. Then K is Hilbert–Speiser of type G by Proposition 2.2.

Now let $\pi\in K$ be a local parameter at $\mathfrak{p}$, let $M=K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$, and let $e\ge 3$ be the absolute ramification index of $\mathfrak{p}$. Let $E_1=K(\sqrt{1+\pi^{2e-5}})$, $E_2=K(\sqrt{\pi})$, and $L=E_1E_2$. The completions of E_1 and E_2 at $\mathfrak{p}$ are quadratic extensions F_1, F_2 of M with ramification numbers $u_1=5$, $u_2=2e$ respectively. Using standard results on the upper and lower ramification filtrations (see [25, Chapter IV, Section 3]), we find that the

completion of L at $\mathfrak{p}$ is the totally ramified biquadratic extension $N = F_1F_2$ of M with *upper* ramification numbers $u_1 < u_2$, and hence with lower ramification numbers $t_1 = u_1 = 5$ and $t_2 = u_1 + 2(u_2 - u_1) = 4e - 5$. We apply Lemma 2.1 to the G-Galois extension N/M. Firstly, (1) holds since $t_2 - \lfloor \frac{t_2}{2} \rfloor = (4e-5) - (2e-3) = 2e-2$. Secondly, (2) holds for $i = 1$ as $t_1 \equiv 1 \pmod 4$, and $w \equiv 0 \pmod 4$ by (3). This shows that the valuation ring $\mathcal{O}_N$ is not free over $\mathcal{A}_{N/M}$. But since $\mathfrak{p}$ is totally ramified in L/K, we have $\mathcal{A}_{L/K,\mathfrak{p}} = \mathcal{A}_{N/M}$. Hence $\mathcal{O}_L$ is not locally free over $\mathcal{A}_{L/K}$. □

Proof of Corollary 1.7. A list of all real cubic fields of discriminant ≤ 3132 is given by Cohen [9, Table B.4]. From this, we read off that the fields $K = \mathbb{Q}(\alpha_i)$ for $i = 1, 2, 3$ are real cubic fields: in fact, they are the unique such fields (up to Galois conjugacy) of discriminant 148, 404, 564, respectively, and none of them is normal over $\mathbb{Q}$. In each case, $\mathcal{O}_K = \mathbb{Z}[\alpha_i]$. By factoring the given polynomial over $\mathbb{F}_2$, we check that 2 is totally ramified in K. Thus the unique prime of K above 2 has ramification index $e = 3$.

It remains to verify that $\mathrm{Cl}_4(\mathcal{O}_K)$ is trivial. This can be done either using PARI [23], or as follows. We observe that the canonical map $\mathrm{Cl}_4(\mathcal{O}_K) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_K)$ is injective if and only if the natural map $\mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K/4\mathcal{O}_K)^\times$ is surjective. In each of the three cases, we can check the surjectivity of the latter map by hand, using the fundamental units given in Cohen's table. This table also tells us that K has class number 1. Thus $\mathrm{Cl}_4(\mathcal{O}_K) = 1$ as required. □

3. Realisable classes and the Proof of Proposition 1.8

Let K be a number field and let p be a prime. Let $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times$ 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 $\mathrm{Cl}(\mathcal{O}_K[C_p])$. 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 $\mathrm{Cl}(\mathcal{O}_K[C_p]) \longrightarrow \mathrm{Cl}(\mathcal{O}_K)$ induced by augmentation. Let $\mathcal{J}$ be the Stickelberger ideal in $\mathbb{Z}[\Delta]$. In [20], it is shown that $R(\mathcal{O}_K[C_p])$ is the subgroup $\mathrm{Cl}'(\mathcal{O}_K[C_p])^{\mathcal{J}}$ of $\mathrm{Cl}(\mathcal{O}_K[C_p])$ generated by $\{c^\alpha : c \in \mathrm{Cl}'(\mathcal{O}_K[C_p]), \alpha \in \mathcal{J}\}$.

Now assume that p is odd, and let Σ be the element $\Sigma_{g \in C_p} g$ in the group ring $K[C_p]$. For any wildly ramified C_p-Galois extension L/K, there is an integral $\mathcal{O}_K$-ideal $\mathfrak{b}$ such that $\mathfrak{b}(\mathcal{A}_{L/K} \cap K\Sigma) = \mathcal{O}_K\Sigma$, and it is easy to see that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathfrak{b}$. Miyata [21] associates to $\mathcal{O}_L$ a class $\mathrm{cl}(\mathcal{O}_L)$ in the locally free class group $\mathrm{Cl}(\mathcal{A}_{L/K})$, and then investigates the behaviour of this class as L varies over extensions with the same associated order. Note however that in general $\mathcal{O}_L$ need not be locally free over $\mathcal{A}_{L/K}$, so $\mathrm{cl}(\mathcal{O}_L)$ should not be interpreted simply as "the class of" the $\mathcal{A}_{L/K}$-module $\mathcal{O}_L$. In the case that $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K}$, one sees from [21, p. 160] that $\mathrm{cl}(\mathcal{O}_L)$ is the class in $\mathrm{Cl}(\mathcal{A}_{L/K})$ of the locally free module $\mathfrak{b}^{-1}\mathcal{O}_L$, and not of $\mathcal{O}_L$ itself.

As in the previous paragraph, $\mathrm{Cl}(\mathcal{A}_{L/K})$ is a Δ-module and [21, Corollary to Theorem 2] shows that $\mathrm{cl}(\mathcal{O}_L)$ lies in $\mathrm{Cl}'(\mathcal{A}_{L/K})^{\mathcal{J}}$, where $\mathrm{Cl}'(\mathcal{A}_{L/K})$ is defined analogously to $\mathrm{Cl}'(\mathcal{O}_K[C_p])$ and $\mathcal{J}$ is again the Stickelberger ideal in $\mathbb{Z}[\Delta]$. Moreover, there is a surjective Δ-homomorphism

$$f\colon \mathrm{Cl}'\big(\mathcal{O}_K[C_p]\big)^{\mathcal{J}} \longrightarrow \mathrm{Cl}'(\mathcal{A}_{L/K})^{\mathcal{J}}. \tag{4}$$

Proof of Proposition 1.8. If K satisfies the modified Leopoldt condition of type C_p, then it is clear that (a) and (b) hold once one recalls that $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$, and that $\mathcal{A}_{L/K} = \mathcal{O}_K[C_p]$ if and only if L/K is a tame C_p-Galois extension.

Suppose conversely that (a) and (b) both hold. Since K is a Hilbert–Speiser field of type C_p, the subgroup $\mathrm{Cl}'(\mathcal{O}_K[C_p])^{\mathcal{J}}$ is trivial by [20, Theorem, p. 103]. Now let L/K be any wildly ramified Galois extension with Galois group isomorphic to C_p. Since $\mathcal{O}_L$ is a locally free $\mathcal{A}_{L/K}$-module, it follows from the discussion above that the class $\mathrm{cl}(\mathcal{O}_L) = (\mathfrak{b}^{-1}\mathcal{O}_L)$ lies in $\mathrm{Cl}'(\mathcal{A}_{L/K})^{\mathcal{J}}$. However, $\mathrm{Cl}'(\mathcal{A}_{L/K})^{\mathcal{J}}$ is trivial by (4), so $\mathfrak{b}^{-1}\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$. $\square$

By [7, Theorem 2], we know that a Hilbert–Speiser field K of type C_p must have class number $h_K = 1$ if either $p = 2$, or $p = 3$ and K contains a primitive cube root of unity ζ_3. The condition $\zeta_3 \in K$ can be removed by Lemma 3.2 below. But if $h_K = 1$ then HS-L(K, C_p) and mHS-L(K, C_p) coincide, so we obtain the following additional corollary to Theorem 1.10.

Corollary 3.1. *Let $p = 2$ or 3, and let K be any number field. Then* HS-L(K, C_p) *holds.*

We will see in Section 6.3 below that there exist Hilbert–Speiser fields of type C_5 having class number 2.

Lemma 3.2. *If K is Hilbert–Speiser of type C_3 and $\zeta_3 \notin K$, then $h_K = 1$.*

Proof. Let $M = K(\zeta_3)$. Then $h_M = 1$ by [7, Theorem 2(ii)]. If the quadratic extension M/K is ramified (either at a prime above 3 or at an infinite prime), then the norm $\mathrm{Cl}(\mathcal{O}_M) \longrightarrow \mathrm{Cl}(\mathcal{O}_K)$ is surjective [27, Theorem 10.1], so $h_K = 1$. If M/K is everywhere unramified, then K is totally imaginary and each prime $\mathfrak{p}$ of K above 3 has absolute ramification index $e_{\mathfrak{p}} \geq 2$. We claim that in this case K cannot be Hilbert–Speiser of type C_3.

To prove the claim, we apply Herreng's formula [14, Proposition 3.2] for the 3-rank $d_3((\mathcal{O}_K/3\mathcal{O}_K)^\times)$ of the unit group of the residue ring $\mathcal{O}_K/3\mathcal{O}_K$. Writing $f_{\mathfrak{p}}$ for the inertia degree of $\mathfrak{p}$, this yields

$$d_3\big((\mathcal{O}_K/3\mathcal{O}_K)^\times\big) = \sum_{\mathfrak{p}|3} f_{\mathfrak{p}}\left(e_{\mathfrak{p}} - 1 - \left\lceil \frac{e_{\mathfrak{p}} - 3}{3} \right\rceil\right).$$

To show K is not Hilbert–Speiser of type C_3, it suffices by [13, Theorem 1] to show that $V_3(K) := (\mathcal{O}_K/3\mathcal{O}_K)^\times / \mathrm{im}(\mathcal{O}_K^\times)$ has exponent divisible by 3. This

will certainly hold if

$$d_3\big((\mathcal{O}_K/3\mathcal{O}_K)^\times\big) > d_3\big(\mathcal{O}_K^\times\big) = \frac{1}{2}[K:\mathbb{Q}] - 1. \tag{5}$$

(The equality holds since K is totally imaginary and $\zeta_3 \notin K$.) But we calculate

$$\begin{aligned} &2\big(d_3\big((\mathcal{O}_K/3\mathcal{O}_K)^\times\big) - d_3\big(\mathcal{O}_K^\times\big)\big) \\ &\quad = 2\sum_{\mathfrak{p}} f_{\mathfrak{p}}\left(e_{\mathfrak{p}} - 1 - \left\lceil \frac{e_{\mathfrak{p}}-3}{3}\right\rceil\right) - \left(\sum_{\mathfrak{p}} f_{\mathfrak{p}} e_{\mathfrak{p}} - 2\right) \\ &\quad = \sum_{\mathfrak{p}} f_{\mathfrak{p}}\left(e_{\mathfrak{p}} - 2 - 2\left\lceil \frac{e_{\mathfrak{p}}-3}{3}\right\rceil\right) + 2 \\ &\quad \geq 2, \end{aligned}$$

since $e_{\mathfrak{p}} \geq 2$ for each $\mathfrak{p}$. Hence (5) holds, as required. □

4. Local freeness for C_p-Galois extensions

Let p be prime and let N/M be a wildly ramified Galois extension of p-adic fields of degree p. In this section, we briefly review the results of [1] and [2], which give necessary and sufficient conditions for $\mathcal{O}_N$ to be free over $\mathcal{A}_{N/M}$ in this case.

Let e denote the ramification index of $M/\mathbb{Q}_p$ and let t denote the ramification number of N/M. From [25, Chapter IV, Section 2, Exercise 3] and the assumption that N/M is wildly ramified, we have $1 \leq t \leq \frac{pe}{p-1}$. Define n to be the "length" of the continued fraction expansion

$$\frac{t}{p} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}} = [a_0, a_1, a_2, \ldots, a_n], \quad \text{with } a_n > 1.$$

Let a be the unique integer such that $0 \leq a \leq p-1$ and $a \equiv t \bmod p$ (and so $t = a_0 p + a$).

THEOREM 4.1 ([1], [2]). *The ring of integers $\mathcal{O}_N$ is free over $\mathcal{A}_{N/M}$ if and only if*

(a) $a = 0$, *or*
(b) $t < \frac{pe}{p-1} - 1$ *and* $a \mid (p-1)$, *or*
(c) $\frac{pe}{p-1} - 1 \leq t$ *and* $n \leq 4$.

COROLLARY 4.2. *If $p = 3$, then $\mathcal{O}_N$ is always free over $\mathcal{A}_{N/M}$.*

Proof. Since $p = 3$, we must have $a \in \{0, 1, 2\}$. The case $a = 0$ is clear, so suppose $a \in \{1, 2\}$. Then a divides $2 = p - 1$ and either

$$\frac{t}{p} = a_0 + \frac{1}{3} \quad \text{or} \quad \frac{t}{p} = a_0 + \frac{2}{3} = a_0 + \frac{1}{1 + \frac{1}{2}},$$

so $n \leq 2$. Since either $t < \frac{pe}{p-1} - 1$ or $\frac{pe}{p-1} - 1 \leq t$, this completes the proof. □

We end this section with a global consequence of Theorem 4.1.

COROLLARY 4.3. *Let $p \geq 5$ be prime, and let $b(p)$ be the least positive integer not dividing $p-1$. Let K be a number field such that some prime $\mathfrak{p}$ of K above p has absolute ramification index $e > b(p)$. Then there is a C_p-Galois extension L of K such that $\mathcal{O}_L$ is* not *locally free over $\mathcal{A}_{L/K}$.*

Proof. Let $M = K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$. For any integer t such that $0 < t < pe/(p-1)$ and $t \not\equiv 0 \pmod{p}$, there is a (totally ramified) C_p-Galois extension N of M with ramification number t: see for instance [11, Chapter III, (2.5) Proposition]. We take $t = b(p)$. As $p \geq 5$, we have $0 < t < p-1$, so that $t \not\equiv 0 \pmod{p}$. Also, $t < \frac{pe}{p-1} - 1$ since $e \geq t+1$ by hypothesis. Thus, there exists a Galois C_p-extension N of M with ramification number t, and moreover $\mathcal{O}_N$ is not free over $\mathcal{A}_{N/M}$ by Theorem 4.1 and the definition of $b(p)$.

Having found the p-adic extension N/M, we observe that there exists a C_p-Galois extension L of the number field K such that $L_{\mathfrak{p}} = N$: this follows from the Grunwald–Wang theorem (see for example [22, (9.2.3) Corollary]; note we are not in the "special case" since p is odd). Then $\mathcal{O}_L$ is not locally free over $\mathcal{A}_{L/K}$, since $\mathcal{O}_N$ is not free over $\mathcal{A}_{N/M}$. □

5. Proof of Theorem 1.10

We now combine the results of previous sections and of [8], [14] to prove our main result.

Proof of Theorem 1.10. Assume that K is a Hilbert–Speiser field of type C_p. By Proposition 1.8, it suffices to show that if L/K is a wildly ramified C_p-Galois extension, then $\mathcal{O}_L$ is a locally free $\mathcal{A}_{L/K}$-module. To this end, let $M = K_{\mathfrak{p}}$ be the completion of K at some prime $\mathfrak{p}$ above p and let e be the ramification index of $M/\mathbb{Q}_p$. Let N/M be a C_p-Galois extension and assume that N/M is (wildly) ramified. Let t be the ramification number of N/M. From [25, Chapter IV, Section 2, Exercise 3] and the assumption that N/M is wildly ramified, we have $1 \leq t \leq \frac{pe}{p-1}$.

We always have $\zeta_2 = -1 \in K$, so the case $p = 2$ is given by [8, Theorem 1.2]. The case $p = 3$ follows from Corollary 4.2. So we may henceforth assume that $p \geq 5$.

Suppose that $K/\mathbb{Q}$ is unramified at p. Then $e = 1$ and so the above inequality becomes $1 \leq t \leq \frac{p}{p-1}$, which forces $a = t = 1$. It now follows from Theorem 4.1(c) that $\mathcal{O}_N$ is a free $\mathcal{A}_{N/M}$-module. So we may henceforth assume that $e \geq 2$.

Suppose that K is totally real. By Theorem 1.9, we are reduced to the case $p = 5$ and $e = 2$. We must have $a = t \in \{1, 2\}$. If $t = 1$, the result follows from Theorem 4.1(b); if $t = 2$, it follows from Theorem 4.1(c).

Suppose that K is (totally) imaginary and $K/\mathbb{Q}$ is Galois. By the end of the proof of [14, Proposition 3.4], we must have $e \leq \frac{2p}{p-2}$, since otherwise K would not be Hilbert–Speiser of type C_p. The inequalities $2 \leq e \leq \frac{2p}{p-2}$ and $1 \leq t \leq \frac{pe}{p-1}$ now leave several cases to consider. Since $p \geq 5$, we have $\frac{2p}{p-2} < 4$, so $e \in \{2,3\}$. If $e = 2$ then $a = t \in \{1,2\}$. If $t = 1$, the result follows from Theorem 4.1(b); if $t = 2$, it follows from Theorem 4.1(c) since

$$\frac{t}{p} = \frac{2}{p} = \frac{1}{(\frac{p-1}{2}) + \frac{1}{2}}.$$

Now assume $e = 3$. In this case we find $a = t \in \{1,2,3\}$. When $t \in \{1,2\}$ the result follows from Theorem 4.1(b). If $t = 3$, then either

$$\frac{t}{p} = \frac{3}{p} = \frac{1}{(\frac{p-1}{3}) + \frac{1}{3}} \quad \text{or} \quad \frac{t}{p} = \frac{3}{p} = \frac{1}{(\frac{p-2}{3}) + \frac{1}{1+\frac{1}{2}}},$$

and so the result follows from Theorem 4.1(c). □

6. Counterexamples for C_5

Most of this section is devoted to providing a counterexample to mHS-L(K, C_5) in the case that $K/\mathbb{Q}$ is not Galois. In this counterexample, mHS-L(K, C_5) fails locally. In the last part, we give some examples of fields K such that mHS-L(K, C_5) holds, but HS-L(K, C_5) does not; the failure of HS-L(K, C_5) is then necessarily a genuinely global phenomenon.

The counterexample will be a sextic field K over the rationals with signature $(2,2)$. The defining polynomial is $x^6 + 2x^4 - 5x - 5$. The field K has class number 1, and the prime 5 splits in K as the fourth power of a degree one prime $\mathfrak{p}_1$ times a degree two prime $\mathfrak{p}_2$. Applying Corollary 4.3, and noting that $b(5) = 3$, it follows that K has a C_5-Galois extension L/K for which $\mathcal{O}_L$ is not locally free over $\mathcal{A}_{L/K}$.

It is therefore left to prove that K is Hilbert–Speiser of type C_5. To do this, we must show that the subgroup of realisable classes in the class group of $\mathcal{O}_K[C_5]$ is trivial.

Since 5 ramifies in K, the calculation of the class group of $\mathcal{O}_K[C_5]$ is a little difficult, involving two fibre products, but not as difficult as one might expect since some relevant ray class groups are trivial and of order 2, respectively. The final outcome is that the class group of $\mathcal{O}_K[C_5]$ is of order 1 or 2. This implies, by an easy explicit argument, that $\mathrm{Cl}(\mathcal{O}_K[C_5])$ is annihilated by the Stickelberger ideal (note that the cyclic group $\mathrm{Aut}(C_5)$ of order 4 has to act trivially). Therefore K is Hilbert–Speiser of type C_5, by McCulloh's theorem on realisable classes in [20]. In fact, with extra effort one can show that the order of the whole class group is 1; but it is much simpler to use McCulloh's theorem.

6.1. The class group of a certain nonmaximal order R in $M = K(\zeta_5)$. Let $K = \mathbb{Q}(\theta)$ with $\theta^6 + 2\theta^4 - 5\theta - 5 = 0$. We check using PARI [23] that $5\mathcal{O}_K = \mathfrak{p}_1^4\mathfrak{p}_2$, where $\mathfrak{p}_1$ has degree 1 and $\mathfrak{p}_2$ has degree 2. We let $M = K(\zeta_5)$. Calculation shows that $\mathfrak{p}_1\mathcal{O}_M$ is again prime.

Remark 6.1. M has very large degree (24), but the polynomial defining M, afforded by the PARI command `polcomposite`, is not as unwieldy as one might expect. We then calculated `bnfinit` of M, which contains all the information we need on (ray) class groups of M.

Some remarks on the length and the reliability of our calculations: The algorithm `bnfinit` took seconds or minutes, depending on the choice of governing parameters. We used the parameters $c = 0.3$, $c2 = 12$, which yield a rigorous result under the assumption GRH. (It seems illusory to eliminate GRH for a field of this size, in particular a call of `bnfcertify` results in an instantaneous refusal, because the Minkowski constant is much too large.) The inbuilt check number was 1, as it should be. Some more plausibility checks were done, such as repeating the calculation with another defining polynomial afforded by `polred`, or on different machines.

Another partial justification of correctness is as follows. All the units produced by [23] were double-checked (a quick way is to take the principal ideal generated by a hypothetical unit and factor it; if one gets the empty factorisation, we indeed have a unit). Now if we accept the statement that the class number h_M of M is 1 (produced by `bnfinit`) as true, then the triviality of a certain ray class group (established below) is rigorously true as well: The unlikely case that PARI missed some units of M would only mean that our number for the order of the ray class group might be too high, but we already obtain order 1 using the supply of units found by [23].

The main task in this section is a comparison of the rings $R = \mathcal{O}_K[\zeta_5] \cong \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_5]$, which is *not* the maximal order of M, on the one side, and the ring $S = \mathcal{O}_M$ on the other side. By [23], S has class number 1. We want to establish that $\mathrm{Cl}(R)$ is trivial as well.

For this, we need some analysis of the inclusion $R \subset S$. Since S disagrees with R at most at primes which are ramified both in K and in $\mathbb{Q}(\zeta_5)$, the only prime at which we expect disagreement is $\mathfrak{p}_1$. Let π be a local parameter at $\mathfrak{p}_1$ in K, and let $\lambda = \zeta_5 - 1$. Since 5 is (tamely) ramified with ramification index 4 both in $K_{\mathfrak{p}_1}$ and in $\mathbb{Q}_5(\zeta_5)$, the rings $\mathcal{O}_{M,\mathfrak{p}_1}$ and $\mathbb{Z}_5[\pi,\lambda]$ cannot be equal. But one has the following local description at $\mathfrak{p}_1$.

Lemma 6.2. *The element $\xi := \lambda/\pi$ is integral. The ring $S_{\mathfrak{p}_1} = \mathcal{O}_{M,\mathfrak{p}_1}$ is the (free) $\mathcal{O}_{K,\mathfrak{p}_1}$-span of $1, \xi, \xi^2, \xi^3$, and the length of $\mathcal{O}_{M,\mathfrak{p}_1}/\mathbb{Z}_5[\pi,\lambda]$ is 6. Moreover, $\pi^3 S_{\mathfrak{p}_1}$ is contained in $R_{\mathfrak{p}_1} = \mathbb{Z}_5[\pi,\lambda]$.*

Proof. The integrality of ξ is clear, by looking at valuations. (Recall that π is also a parameter for the extended ideal $\mathfrak{p}_1\mathcal{O}_M$.) The $\mathcal{O}_K$-module T defined

as the $\mathcal{O}_K$-span of $1, \xi, \xi^2, \xi^3$ has the easily seen property that $T/\mathbb{Z}_5[\pi, \lambda]$ is of length 6 $(= 1 + 2 + 3)$ over $\mathcal{O}_K/\mathfrak{p}_1$, that is, of order 5^6. By comparing the discriminants of the algebras R and S (given by [23] and Schachtelungsformel), one sees that $\mathcal{O}_{M,\mathfrak{p}_1}/\mathbb{Z}_5[\pi, \lambda]$ also has order 5^6. Hence, we have equality. The last statement follows from the definitions. □

COROLLARY 6.3. *We also have the global inclusion* $\mathfrak{p}_1^3 S \subset R$.

This corollary produces a fibre product arising as follows. If we let $\bar{S}$ stand for $S/\mathfrak{p}_1^3 S$ and $\bar{R}$ for the image of R in $\bar{S}$, we obtain the fibre product

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

where the horizontal arrows are the natural inclusions and the vertical arrows are the natural projections. By [10, Theorem 42.13] and the fact that all rings are commutative, we have the following exact sequence

$$S^\times \times \bar{R}^\times \longrightarrow \bar{S}^\times \longrightarrow \mathrm{Cl}(R) \longrightarrow \mathrm{Cl}(S) \oplus \mathrm{Cl}(\bar{R}).$$

Since $\bar{R}$ has trivial class group (being semilocal), and since the class group of S is also trivial, the class group $\mathrm{Cl}(R)$ is an epimorphic image of $U := \bar{S}^\times/(\bar{R}^\times \cdot \mathrm{im}(S^\times))$. It thus suffices to establish that U is trivial. In fact, we will check that $U' := \bar{S}^\times/\mathrm{im}(S^\times)$ is already trivial. But U' is precisely the ray class group modulo $\mathfrak{p}_1^3$ of M. By [23], we find that this ray class group is trivial, so we are done. (It is perhaps interesting to mention that the ray class number of M modulo $5\mathcal{O}_M$ is relatively large, being equal to $15{,}625 = 5^6$.)

We sum up: $R = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_5]$ has class number 1. We note that, in principle, this calculation could also be performed using the algorithm of [16].

6.2. The class group of the integral group ring. To calculate the class group of $\mathcal{O}_K[C_5]$, we now have to look at a second fibre product with $\mathcal{O}_K[C_5]$ at the upper left; the upper right and lower left corners are occupied by $R = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_5]$ and $\mathcal{O}_K$, respectively. Finally, the lower right-hand corner has the ring $T = R/\lambda R = \mathcal{O}_K/5\mathcal{O}_K$. (Recall $\lambda = 1 - \zeta_5$.) The class group of R is trivial (see previous section), and so is the class group of $\mathcal{O}_K$ [23]. Hence, applying [10, Corollary 49.28], we find that the class group of $\mathcal{O}_K[C_5]$ is an epimorphic image of the group $X := T^\times/(\mathrm{im}(R^\times) \cdot \mathrm{im}(\mathcal{O}_K^\times))$. Our final claim will follow, if we can establish that X is of order 1 or 2. But, reasoning as above, X is an epimorphic image of $T^\times/\mathrm{im}(\mathcal{O}_K^\times)$, the ray class group of K modulo $5\mathcal{O}_K$. By [23] this group has order 2. This is safe, since we ran `bnfcertify` on K, which confirmed the whole output of `bnfinit`. We mention in passing that the fundamental units of K have remarkably small coefficients. Let us also remark that we cannot expect ray class number 1 here, because of the existence of the quadratic extension $K(\sqrt{5})/K$. (Getting

back to a remark made at the beginning: it is possible, but not easy, to show that X is of order 1. We also note that, in principle, this calculation can be performed using the algorithm of [3].)

This completes the proof that the class group of $\mathcal{O}_K[C_5]$ has order at most 2, and this implies, as explained at the beginning, that K is Hilbert–Speiser of type C_5.

6.3. Some examples and more counterexamples. In this section, we give some examples of fields K such that K has class number 2 and is Hilbert–Speiser of type C_5 (as mentioned after Corollary 3.1). The examples K will be quartic fields over the rationals with signature $(2,1)$. Moreover, $K/\mathbb{Q}$ will be unramified at 5, and K will contain a nonprincipal prime $\mathfrak{p}$ above 5. By Theorem 1.10 (b), mHS-L(K,C_5) holds. However, there exists a C_5-Galois extension L/K with $\mathrm{Tr}_{L/K}(\mathcal{O}_L)=\mathfrak{p}$. This follows from the Grunwald–Wang theorem as in the proof of Corollary 4.3, but we construct one such L explicitly in the Appendix. The existence of such an extension L shows that HS-L(K,C_5) does not hold: The class $(\mathfrak{p}^{-1}\mathcal{O}_L)$ in $\mathrm{Cl}(\mathcal{A}_{L/K})$ is trivial by mHS-L(K,C_5), so the class $(\mathcal{O}_L)$ in $\mathrm{Cl}(\mathcal{A}_{L/K})$ cannot be trivial.

In order to produce our fields K, we used [23] and [24] to generate lists of degree 4 polynomials f_i with coefficients of absolute value less than or equal to 20, and then successively sifted out along the following criteria:

(a) f_i irreducible
(b) the field K_i defined by f_i has signature (2, 1)
(c) 5 is unramified but not inert in K_i
(d) $h_{K_i}=2$
(e) at least one prime of K_i above 5 is nonprincipal
(f) the field $M_i=K_i(\zeta_5)$ has class number 2 which equals the ray class number of M_i modulo $(1-\zeta_5)$.

In fact, using [24], one quickly obtains 12,051 polynomials satisfying (a), (b), and (d). With some extra effort utilising [4] we then found that $x^4-x^3+3x^2-3x-4$ satisfies all the stated criteria. This example was then successfully checked using [23] on another machine.

Let $K=\mathbb{Q}(\theta)$ with $\theta^4-\theta^3+3\theta^2-3\theta-4=0$. Since 5 does not ramify in K, K is arithmetically disjoint to $\mathbb{Q}(\zeta_5)$, and hence $\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta_5]$ is the ring of integers in $M=K(\zeta_5)$. Since the ray class group of M modulo $(1-\zeta_5)$ has order 2, and $h_M=2$, it follows that the quotient $U':=(\mathcal{O}_M/(1-\zeta_5))^\times/\mathrm{im}(\mathcal{O}_M^\times)$ is trivial.

We have a fibre product with $\mathcal{O}_K[C_5]$ at the upper left, and with the upper right and lower left corners occupied by $\mathcal{O}_M=\mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta_5]$ and $\mathcal{O}_K$, respectively. Finally, the lower right-hand corner has the ring $\mathcal{O}_M/(1-\zeta_5)$. By [10, Theorem 42.13] and the fact that all rings are commutative we obtain an exact sequence which appears as the middle row in the following

diagram

$$\begin{array}{ccccc}
 & & 0 & & 0 \\
 & & \downarrow & & \downarrow \\
 & & \mathrm{Cl}'\big(\mathcal{O}_K[C_5]\big) & & \mathrm{Cl}(\mathcal{O}_M) \\
 & & \downarrow & & \downarrow \\
1 \to U & \to & \mathrm{Cl}\big(\mathcal{O}_K[C_5]\big) & \to & \mathrm{Cl}(\mathcal{O}_M) \oplus \mathrm{Cl}(\mathcal{O}_K) \\
 & & \downarrow & & \downarrow \\
 & & \mathrm{Cl}(\mathcal{O}_K) & = & \mathrm{Cl}(\mathcal{O}_K) \\
 & & \downarrow & & \downarrow \\
 & & 0 & & 0,
\end{array}$$

where the left and right vertical sequences are, respectively, the exact sequence of Section 3, and the exact sequence defined in terms of the natural maps. One easily verifies that this diagram is commutative so there is a unique map $\alpha:\ \mathrm{Cl}'(\mathcal{O}_K[C_5]) \to \mathrm{Cl}(\mathcal{O}_M)$ which makes the resulting diagram commute. Applying the snake lemma to the vertical sequences and maps between them, we obtain the exact sequence

$$0 \longrightarrow \ker(\alpha) \longrightarrow U \longrightarrow 0.$$

Hence, α has kernel U. That is, the following sequence is exact

$$1 \longrightarrow U \longrightarrow \mathrm{Cl}'\big(\mathcal{O}_K[C_5]\big) \xrightarrow{\alpha} \mathrm{Cl}(\mathcal{O}_M).$$

Since $U = U'/\operatorname{im}(\mathcal{O}_K^\times)$ is trivial, $\mathrm{Cl}'(\mathcal{O}_K[C_5])$ maps injectively into $\mathrm{Cl}(\mathcal{O}_M)$, and hence is of order 1 or 2. So it is annihilated by the Stickelberger ideal, and K is Hilbert–Speiser of type C_5. Furthermore, as explained above, mHS-L(K, C_5) holds, but HS-L(K, C_5) does not.

Using the techniques described above, we can find many more examples of such polynomials. We list three here, including our example above, along with the corresponding discriminant d_K:

$$\begin{aligned}
&x^4 - x^3 + 3x^2 - 3x - 4 \quad \big(d_K = -12{,}844 = -2^2 \cdot 13^2 \cdot 19\big),\\
&x^4 - x^3 + 4x^2 - 4x - 1 \quad \big(d_K = -17{,}051 = -17^2 \cdot 59\big),\\
&x^4 - 2x^3 + 3x^2 + x - 4 \quad \big(d_K = -17{,}231,\ \text{where } 17{,}231 \text{ is prime}\big).
\end{aligned}$$

Appendix

As mentioned above, a C_5-Galois extension L/K with $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathfrak{p}$ for the first example K in the short list at the end of Section 6 can actually be constructed explicitly. From [19], we find a polynomial

$$\begin{aligned}
g(x,t) &= x\big(x^2 - 25\big)^2 + \big(x^4 - 20x^3 - 10x^2 + 300x - 95\big)t^2 - 4(x-3)^2 t^4\\
&= x^5 + t^2 x^4 + \big(-20t^2 - 50\big)x^3 + \big(-4t^4 - 10t^2\big)x^2\\
&\quad + \big(24t^4 + 300t^2 + 625\big)x + \big(-36t^4 - 95t^2\big)
\end{aligned}$$

whose Galois group over $\mathbb{Q}(t)$ is the cyclic group C_5 of order 5. Whenever $\tau \in K$ is such that $g_\tau(x) = g(x,\tau)$ is irreducible over K, the specialised polynomial g_τ has Galois group C_5 over K. With some guesswork it is now possible to find a choice of τ such that the resulting extension $L = L_\tau$ is ramified at the degree one prime over 5 in K and unramified at the other prime over 5. We only give the outcome; everything has been verified by PARI, using a variety of double-checks, such as calculating discriminants both for the relative extension L/K and the absolute field L, and comparing via the Schachtelungsformel. Also the a priori fact that L/K is cyclic (which would be difficult to prove by PARI in full rigour) was tested by looking at the factorisation of several dozen prime ideals. Let θ denote a root of the defining polynomial for K, so $\theta^4 - \theta^3 + 3\theta^2 - 3\theta - 4 = 0$. We are now free again to use x as the variable for the polynomial defining L/K. We find

$$\begin{aligned} g_\tau = x^5 &+ \big(-9\theta^3 + 6\theta^2 + 15\theta + 8\big)x^4 + \big(180\theta^3 - 120\theta^2 - 300\theta - 210\big)x^3 \\ &+ \big(666\theta^3 - 8364\theta^2 + 5370\theta + 7728\big)x^2 \\ &+ \big(-6156\theta^3 + 51{,}624\theta^2 - 28{,}620\theta - 43{,}823\big)x \\ &+ \big(6039\theta^3 - 75{,}306\theta^2 + 48{,}255\theta + 69{,}512\big). \end{aligned}$$

Apart from the wild ramification at one prime above 5, L/K has tame ramification in two primes of norm 66,821 and 4,268,881 respectively. (These two numbers are prime.)

Acknowledgments. Carter would like to thank the members of Laboratoire A2X of the Université de Bordeaux I, and the members of the Mathematics Department of the Universität der Bundeswehr München for their kind hospitality during his visits in the 2006–2007 academic year.

Johnston would like to thank the Deutscher Akademischer Austausch Dienst (German Academic Exchange Service) for a grant allowing him to visit Greither at Universität der Bundeswehr München for the 2006–2007 academic year, and his hosts for making his stay most productive and enjoyable.

References

[1] F. Bertrandias and M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Ser. A-B **274** (1972), A1330–A1333. MR 0296047

[2] F. Bertrandias, J.-P. Bertrandias and M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Ser. A-B **274** (1972), A1388–A1391. MR 0296048

[3] W. Bley and R. Boltje, *Computation of locally free class groups*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 72–86. MR 2282916

[4] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265. MR 1484478

[5] N. P. Byott, *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications*, J. Théor. Nombres Bordeaux **9** (1997), 201–219. MR 1469668

[6] N. P. Byott and B. Sodaïgui, *Galois module structure for dihedral extensions of degree 8: Realizable classes over the group ring*, J. Number Theory **112** (2005), 1–19. MR 2131138

[7] J. E. Carter, *Normal integral bases in quadratic and cyclic cubic extensions of quadratic fields*, Arch. Math. **81** (2003), 266–271. MR 2013257; *Erratum*, ibid. **83** (2004), vi–vii. MR 2191482

[8] J. E. Carter, *Some remarks on Hilbert–Speiser and Leopoldt fields of given type*, Colloq. Math. **108** (2007), 217–223. MR 2291634

[9] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math., vol. 138, Springer-Verlag, New York, 1993. MR 1228206

[10] C. W. Curtis and I. Reiner, *Methods of representation theory, Vol. II. With applications to finite groups and orders*. Wiley, New York, 1987. MR 0892316

[11] I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions. A constructive approach*, American Mathematical Society, Providence, RI, 1993. MR 1218392

[12] C. Greither and H. Johnston, *On totally real Hilbert–Speiser fields of type C_p*, Acta Arith. **138** (2009), 329–336. MR 2534138

[13] C. Greither, D. R. Replogle, K. Rubin and A. Srivastav, *Swan modules and Hilbert–Speiser number fields*, J. Number Theory **79** (1999), 164–173. MR 1718724

[14] T. Herreng, *Sur les corps de Hilbert–Speiser*, J. Théor. Nombres Bordeaux **17** (2005), 767–778. MR 2212124

[15] H. Johnston, *Relative Galois module structure of rings of integers of absolutely abelian number fields*, J. Reine Angew. Math. **620** (2008), 85–103. MR 2427977

[16] J. Klüners and S. Pauli, *Computing residue class rings and Picard groups of orders*, J. Algebra **292** (2005), 47–64. MR 2166795

[17] H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119–149. MR 0108479

[18] G. Lettl, *The ring of integers of an abelian number field*, J. Reine Angew. Math. **404** (1990), 162–170. MR 1037435

[19] G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer, Berlin, 1999. MR 1711577

[20] L. R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra **82** (1983), 102–134. MR 0701039

[21] Y. Miyata, *Wildly ramified extensions of prime degree p and Stickelberger conditions*, Japan. J. Math. (N.S.) **15** (1989), 157–168. MR 1053635

[22] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, Springer-Verlag, Berlin, 2000. MR 1737196

[23] PARI/GP, version 2.3.4, Bordeaux, 2008; available at `http://pari.math.u-bordeaux.fr/`.

[24] QaoS, Querying Algebraic Object System; available at `http://qaos.math.tu-berlin.de/`.

[25] J.-P. Serre, *Local fields*, Graduate Texts in Math., vol. 67, Springer-Verlag, New York, 1979. MR 0554237

[26] M. J. Taylor, *Hopf orders and Galois module structure*, DMV Sem., vol. 18, Group rings and class groups, Birkhäuser, Basel, 1992, pp. 153–210. MR 1167451

[27] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Math., vol. 83, Springer-Verlag, New York, 1997. MR 1421575

Nigel P. Byott, Mathematics Research Institute, University of Exeter, Harrison Building, North Park Road, Exeter EX4 4QF, UK

E-mail address: `N.P.Byott@ex.ac.uk`

James E. Carter, Department of Mathematics, College of Charleston, 66 George Street, Charleston, SC 29424-0001, USA

E-mail address: carterj@cofc.edu

Cornelius Greither, Fakultät für Informatik, Institut für theoretische Informatik und Mathematik, Universität der Bundeswehr München, 85577 Neubiberg, Germany

E-mail address: cornelius.greither@unibw.de

Henri Johnston, St. John's College, Cambridge CB2 1TP, UK

E-mail address: H.Johnston@dpmms.cam.ac.uk

URL: http://www.dpmms.cam.ac.uk/~hlj31