COLLOQUIUM MATHEMATICUM

VOL. 108 2007 NO. 2

SOME REMARKS ON HILBERT–SPEISER AND LEOPOLDT FIELDS OF GIVEN TYPE

BY

JAMES E. CARTER (Charleston, SC)

Abstract. Let p be a rational prime, G a group of order p, and K a number field containing a primitive pth root of unity. We show that every tamely ramified Galois extension of K with Galois group isomorphic to G has a normal integral basis if and only if for every Galois extension L/K with Galois group isomorphic to G, the ring of integers O_L in L is free as a module over the associated order $\mathcal{A}_{L/K}$. We also give examples, some of which show that this result can still hold without the assumption that K contains a primitive pth root of unity.

1. Introduction. Throughout the present article p is a rational prime, the ring of integers in a number field F is denoted by O_F, and $Cl(O_F)$ denotes the ideal class group of F of order h_F. If F is a finite extension of the p-adic numbers $\mathbb{Q}_p$, then O_F denotes the valuation ring in F, and O_N denotes the integral closure of O_F in a finite extension N/F of F.

Now let G be a finite group and let K be a number field. If L/K is a Galois extension with Galois group G then O_L is a module over the integral group ring O_KG by way of the Galois action of G on L. If O_L is free as an O_KG-module, necessarily of rank one, we say L/K has a *normal integral basis*. It is well known that L/K has such a basis only if L/K is *tame*, that is, at most tamely ramified. If L/K is not tame, we can still ask for a freeness result. To do this we consider the associated order $\mathcal{A}_{L/K}$ contained in the K-algebra KG. It consists of all elements α of KG such that $\alpha O_L \subseteq O_L$. Of course $O_KG \subseteq \mathcal{A}_{L/K}$ and, as is well known, L/K is tame if and only if $O_KG = \mathcal{A}_{L/K}$. Moreover, for L/K tame or otherwise, it may happen that O_L is a free $\mathcal{A}_{L/K}$-module.

2000 *Mathematics Subject Classification*: Primary 11R33.

Key words and phrases: Galois module structure, normal integral basis, associated order, Hilbert–Speiser field, Leopoldt field.

The author would like to thank C. Greither for focusing the author's attention on Kummer extensions of prime degree.

This paper was written while the author was visiting the Université de Bordeaux 1 while on sabbatical leave during the academic year 2006–2007. He would like to thank the members of Laboratoire A2X, and, in particular, M. Olivier, for the kind hospitality extended to him during his visit.

Let us now consider all finite abelian extensions of K. If for each such extension L/K, O_L is free as a module over $\mathcal{A}_{L/K}$, then we call K a *Leopoldt field*. In [10] Leopoldt showed that the rational field $\mathbb{Q}$ is such a field. A simplified version of the proof of this result can be found in [11]. Note that if K is a Leopoldt field then it has the property that for any finite abelian group G and any tame Galois extension L/K with Galois group G, O_L is a free $O_K G$-module. Thus we recover the famous result of Hilbert and Speiser: Every tame finite abelian extension of $\mathbb{Q}$ has a normal integral basis. Any number field sharing this property with $\mathbb{Q}$ is called a *Hilbert–Speiser field*. From [7] we know that $\mathbb{Q}$ is the only such field. In other words, we have the following theorem.

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.*

Evidently, freeness for all tame finite abelian extensions is enough to guarantee freeness for all finite abelian extensions. This result suggests a conjecture regarding a restricted case of its statement which we next explain.

Let G be a finite abelian group. A number field K is called a *Leopoldt field of type G* if O_L is a free $\mathcal{A}_{L/K}$-module whenever L/K is a Galois extension with Galois group isomorphic to G. If K satisfies the condition that all of its tame Galois extensions with Galois group isomorphic to G have a normal integral basis, then we call K a *Hilbert–Speiser field of type G*. These fields have been studied, for instance, in [3], [4], [8], [9] and [15].

CONJECTURE 1.1. *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 and only if K is a Leopoldt field of type G.*

We will provide some limited evidence in support of Conjecture 1.1 in the form of the following theorem and some examples in Section 4.

THEOREM 1.2. *If G is a finite group of order p and K is a number field which contains a primitive pth root of unity, then K is a Hilbert–Speiser field of type G if and only if K is a Leopoldt field of type G.*

The nontrivial implication of Theorem 1.1 follows from the fact that $\mathbb{Q}$ is a Leopoldt field, and the fact proved in [7] that $\mathbb{Q}$ is the only Hilbert–Speiser field. Using results of [7], the following result is proved in [8] (see [8, Proposition 1]).

PROPOSITION 1.1. *Let G be a group of order p and let K be a number field containing a primitive pth root of unity. If $p \geq 5$ then K is not a Hilbert–Speiser field of type G.*

It follows from Proposition 1.1 that Theorem 1.2 is true for all p such that $p \geq 5$. In what follows we will show that it is true in the remaining two cases as well.

2. Realizable classes. Let G be a finite group and let K be any number field. Let L/K vary over all tame Galois extensions of K with Galois group isomorphic to G. Then the class of O_L in the locally free class group $Cl(O_K G)$ varies over a subset $R(O_K G)$ of realizable classes of $Cl(O_K G)$. In [14] it is shown that when G is abelian then $R(O_K G)$ is a subgroup of $Cl(O_K G)$. Hence, for a finite abelian group G we deduce that K is a Hilbert–Speiser field of type G if and only if $R(O_K G)$ is the trivial subgroup of $Cl(O_K G)$.

Now suppose G is an elementary abelian group and K is any number field. In [13], $R(O_K G)$ is determined in terms of the kernel of a certain map defined on $Cl(O_K G)$. When G has order 2 or 3 this result is the following proposition, which is Theorem 1 of [3].

PROPOSITION 2.1. *Let G be a group of order 2 or 3. Then*

$$R(O_K G) = Cl'(O_K G)$$

where $Cl'(O_K G)$ is the kernel of the map $\varepsilon_* : Cl(O_K G) \to Cl(O_K)$ which is induced by the augmentation map $\varepsilon : O_K G \to O_K$.

From now on C_p is a group of order p. Let K be a number field and let $\mathfrak{M}$ be the maximal O_K-order in KC_p. The inclusion map $O_K C_p \to \mathfrak{M}$ induces a map from $Cl(O_K C_p)$ onto the locally free class group $Cl(\mathfrak{M})$ giving rise to the well-known exact sequence

$$0 \to D(O_K C_p) \to Cl(O_K C_p) \to Cl(\mathfrak{M}) \to 0. \tag{1}$$

The following result due to C. Greither is presented on pp. 268–269 of [3]. We slightly modify its statement and proof here in order to adapt them to our present needs.

PROPOSITION 2.2. *Let K be a number field which contains a primitive pth root of unity. If p equals 2 or 3 then there is an exact sequence*

$$0 \to D(O_K C_p) \to R(O_K C_p) \to \bigoplus_{i=1}^{p-1} Cl(O_K) \to 0.$$

Proof. Since K contains a primitive pth root of unity we have $Cl(\mathfrak{M}) \simeq \bigoplus_{i=1}^{p} Cl(O_K)$. From this and (1) we obtain an exact sequence

$$0 \to D(O_K C_p) \to Cl(O_K C_p) \to \bigoplus_{i=1}^{p} Cl(O_K) \to 0. \tag{2}$$

Also, in the notation of Proposition 2.1, there is an exact sequence

$$0 \to Cl'(O_K C_p) \to Cl(O_K C_p) \to Cl(O_K) \to 0. \tag{3}$$

Finally, we have the exact sequence

$$0 \to \bigoplus_{i=1}^{p-1} Cl(O_K) \to \bigoplus_{i=1}^{p} Cl(O_K) \to Cl(O_K) \to 0 \tag{4}$$

where the maps are the appropriate inclusion and projection maps. The sequences (2), (3), and (4) yield the following diagram:

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ & & & & Cl'(O_K C_p) & & \bigoplus_{i=1}^{p-1} Cl(O_K) & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \to & D(O_K C_p) & \to & Cl(O_K C_p) & \to & \bigoplus_{i=1}^{p} Cl(O_K) & \to & 0 \\ & & & & \downarrow & & \downarrow & & \\ & & & & Cl(O_K) & = & Cl(O_K) & & \\ & & & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \end{array} \tag{5}$$

One easily verifies that (5) is commutative. Hence there is a unique map $\alpha : Cl'(O_K C_p) \to \bigoplus_{i=1}^{p-1} Cl(O_K)$ completing the diagram. Applying the snake lemma to the two vertical exact sequences and maps between them gives an exact sequence

$$0 \to \ker(\alpha) \to D(O_K C_p) \to 0 \to \operatorname{coker}(\alpha) \to 0.$$

Hence, α is surjective with kernel $D(O_K C_p)$. Finally, if $p = 2$ or $p = 3$ we have $Cl'(O_K C_p) = R(O_K C_p)$ by Proposition 2.1. ∎

Corollary 2.1 (cf. [8, Proposition 2]). *Let K be a number field which contains a primitive pth root of unity. If p equals 2 or 3 then the following are equivalent*:

(i) *K is a Hilbert–Speiser field of type C_p.*
(ii) *$h_K = 1$ and $D(O_K C_p)$ is trivial.*
(iii) *$Cl(O_K C_p)$ is trivial.*

Proof. This is an immediate consequence of Proposition 2.2 and (2). ∎

3. Main result. Let G be a finite abelian group and K a number field, or a finite extension of the field of p-adic numbers $\mathbb{Q}_p$. Let L/K be a Galois extension with Galois group G. Many authors have considered the problem of determining when O_L is free as a module over $\mathcal{A}_{L/K}$, or, in the global case, at least locally free over $\mathcal{A}_{L/K}$. In addition to the references already cited, see, for instance, [5] and [12] and the appropriate references listed in these papers. Some of these results lead to a proof of the following proposition.

PROPOSITION 3.1. *Let K be a number field which contains a primitive pth root of unity. Suppose L/K is a Galois extension with Galois group C_p. If p equals 2 or 3 then O_L is a locally free $\mathcal{A}_{L/K}$-module.*

Proof. If $p = 2$ then O_L is a locally free $\mathcal{A}_{L/K}$-module by [5, Theorems 2.1 and 17.3].

To finish the proof we consider the following situation. Let M be a finite extension of the field of 3-adic numbers $\mathbb{Q}_3$, and assume M contains a primitive cube root of unity. Let $\mathfrak{p}$ be the prime ideal of M with corresponding valuation ring O_M. Let N/M be a Galois extension with Galois group C_3 and assume $\mathfrak{p}$ ramifies in N/M. The proposition will follow if we can show that the integral closure O_N of O_M in N is a free $\mathcal{A}_{N/M}$-module. To this end let e be the absolute ramification index of M, and let t be the ramification number of N/M. Since M contains a primitive cube root of unity we have $e = 2e_1$ for some positive rational integer e_1. It is well known that $1 \leq t \leq 3e_1$. If $t \equiv 0 \pmod 3$ (resp. $1 \leq t < 3e_1 - 1$ and $t \not\equiv 0 \pmod 3$), then O_N is a free $\mathcal{A}_{N/M}$-module by part a (resp. part b) of the theorem appearing on p. 1333 of [2]. Finally, if $t = 3e_1 - 1$ then O_N is a free $\mathcal{A}_{N/M}$-module by [1, Theorem 1]. ∎

We can now prove our main result.

Proof of Theorem 1.2. As already noted, Theorem 1.2 is true if $p \geq 5$ by Proposition 1.1. Now suppose either $p = 2$ or $p = 3$. Let K be a number field containing a primitive pth root of unity and assume K is a Hilbert–Speiser field of type C_p. Let L/K be any Galois extension with Galois group isomorphic to C_p. By Proposition 3.1, O_L is a locally free $\mathcal{A}_{L/K}$-module. Since $Cl(O_K C_p)$ is trivial by Corollary 2.1 and maps onto $Cl(\mathcal{A}_{L/K})$ by [6, 49.25(iii)], it follows that $Cl(\mathcal{A}_{L/K})$ is trivial. So the class of O_L in $Cl(\mathcal{A}_{L/K})$ is trivial, which shows that O_L is a free $\mathcal{A}_{L/K}$-module. Hence, K is a Leopoldt field of type C_p. Since the other implication of Theorem 1.2 is clear this concludes the proof. ∎

4. Examples

EXAMPLE 4.1. Among all imaginary quadratic fields there are exactly three Hilbert–Speiser fields of type C_2 by [3, Corollary 3]. They are the fields $\mathbb{Q}(\sqrt{m})$ where $m \in \{-1, -3, -7\}$. Hence, by Theorem 1.2 these fields are Leopoldt fields of type C_2 as well. The fact that among all imaginary quadratic fields these fields are precisely the Leopoldt fields of type C_2 is also proved in [15].

EXAMPLE 4.2. Let $\mathbb{Z}$ be the ring of rational integers and let $m \in \mathbb{Z}$ with $m > 1$ and square free. Let ε_m be the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{m})$. Then either $\varepsilon_m = a + b\sqrt{m}$ or $\varepsilon_m = (a + b\sqrt{m})/2$ where $a, b \in \mathbb{Z}$, and the greatest common divisor $(2, ab)$ is 1. By [3, Corollary 4], $\mathbb{Q}(\sqrt{m})$ is a Hilbert–Speiser field of type C_2 exactly when its class number equals 1 and one of the following holds: (i) $m \equiv 1 \pmod 8$; (ii) $m \equiv 5 \pmod 8$ and $\varepsilon_m \notin \mathbb{Z}[\sqrt{m}]$; (iii) $m \equiv 2$ or $3 \pmod 4$ and $(2, b) = 1$. For $1 < m < 100$ such that the class number of $\mathbb{Q}(\sqrt{m})$ is 1 we find: m satisfies (i) if $m \in \{17, 33, 41, 57, 73, 89, 97\}$; m satisfies (ii) if $m \in \{5, 13, 21, 29, 37, 53, 61, 69, 77, 93\}$; m satisfies (iii) if $m \in \{2, 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 83\}$. Hence, for these values of m, $\mathbb{Q}(\sqrt{m})$ is a Leopoldt field of type C_2 by Theorem 1.2.

EXAMPLE 4.3. Among all quadratic fields there are exactly twelve Hilbert–Speiser fields of type C_3 by [4, Corollary 5] or [9, 5.3]. They are the fields $\mathbb{Q}(\sqrt{m})$ where $m \in \{-11, -3, -2, -1, 2, 3, 5, 6, 17, 33, 41, 89\}$. By Theorem 1.2 the field $\mathbb{Q}(\sqrt{-3})$ is a Leopoldt field of type C_3. We next show that the remaining eleven fields are also Leopoldt fields of type C_3.

Let ω be a primitive cube root of unity and assume K is a number field satisfying $\omega \notin K$. After some routine changes, the proof of the $p = 3$ case of Proposition 2.2 becomes the argument on p. 268 of [3]. As shown there, that argument gives the exact sequences

$$0 \to D(O_K C_3) \to Cl(O_K C_3) \to Cl(O_K) \oplus Cl(O_{K(\omega)}) \to 0 \tag{6}$$

and

$$0 \to D(O_K C_3) \to R(O_K C_3) \to Cl(O_{K(\omega)}) \to 0. \tag{7}$$

Now suppose K is one of our eleven remaining fields. Since K is a Hilbert–Speiser field of type C_3 we see from (7) that $h_{K(\omega)} = 1$ and $D(O_K C_3)$ is trivial. Hence, $Cl(O_K C_3) \simeq Cl(O_K)$ by (6). Since $h_K = 1$ it follows that $Cl(O_K C_3)$ is trivial. So if K is one of our eleven remaining fields and L/K is any Galois extension with Galois group isomorphic to C_3,then $Cl(\mathcal{A}_{L/K})$ is trivial by [6, 49.25(iii)]. Therefore, the example will be complete once we prove the following proposition.

PROPOSITION 4.1. *Let K be a quadratic field and let L/K be a Galois extension with Galois group isomorphic to C_3. Then O_L is a locally free $\mathcal{A}_{L/K}$-module.*

Proof. The proof is similar to the proof of the $p = 3$ case of Proposition 3.1. Let M be a quadratic extension of the field of 3-adic numbers $\mathbb{Q}_3$, and let e be the absolute ramification index of M. Let $\mathfrak{p}$ be the prime ideal of M with corresponding valuation ring O_M. Let N/M be a Galois extension with Galois group isomorphic to C_3. Let O_N be the integral closure of O_M in N.

Assume $\mathfrak{p}$ ramifies in N/M and let t be the ramification number of N/M. We know that $1 \leq t \leq 3e/2$. If $e = 1$ then $t = 1$. Hence, O_N is a free $\mathcal{A}_{N/M}$-module by [1, Theorem 1]. If $e = 2$ then $t \in \{1, 2, 3\}$. If $t = 3$ (resp. $t = 1$) then O_N is a free $\mathcal{A}_{N/M}$-module by part a (resp. part b) of the theorem appearing on p. 1333 of [2]. If $t = 2$ then O_N is a free $\mathcal{A}_{N/M}$-module by [1, Theorem 1]. ∎

REFERENCES

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

[2] F. Bertrandias et M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, ibid., A1330–A1333.

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

[4] —, Erratum to [3], ibid. 83 (2004), no. 6, vi–vii.

[5] L. N. Childs, *Taming wild extensions with Hopf algebras*, Trans. Amer. Math. Soc. 304 (1987), 111–140.

[6] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. II, Wiley, New York, 1987.

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

[8] 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), no. 6, 76–79.

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

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

[11] G. Lettl, *The ring of integers of an abelian number field*, ibid. 404 (1990), 162–170.

[12] —, *Relative Galois module structure of integers of local abelian fields*, Acta Arith. 85 (1998), 235–248.

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

[14] —, *Galois module structure of abelian extensions*, J. Reine Angew. Math. 375/376 (1987), 259–306.

[15] A. Srivastav and S. Venkataraman, *Relative Galois module structure of quadratic extensions*, Indian J. Pure Appl. Math. 25 (1994), 473–488.

Department of Mathematics
College of Charleston
66 George Street
Charleston, SC 29424-0001, U.S.A.
E-mail: carterj@cofc.edu

Received 5 October 2006 (4799)