ACTA ARITHMETICA
104.1 (2002)

Nontrivial tame extensions over Hopf orders

by

Daniel R. Replogle (Morristown, NJ) and
Robert G. Underwood (Montgomery, AL)

1. Introduction. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$, let G be a finite abelian group, and let l be an odd prime. Consider a Galois extension L/K with $\mathrm{Gal}(L/K) = G$. There is a natural action of G on $\mathcal{O}_L$, and $\mathcal{O}_L$ may be viewed as an $\mathcal{O}_K[G]$-module. We say that L/K has a *trivial Galois module structure* if $\mathcal{O}_L$ is free as an $\mathcal{O}_K[G]$-module, that is, $\mathcal{O}_L$ has a normal integral basis over $\mathcal{O}_K$. A number field K is *Hilbert–Speiser* if each tame abelian extension L/K is so that L/K has trivial Galois module structure (see [5, §1]). The Hilbert–Speiser Theorem states that $\mathbb{Q}$ is Hilbert–Speiser, and in [5] the authors determine that $\mathbb{Q}$ is the only Hilbert–Speiser number field.

It is well known that $\mathcal{O}_K[G]$ can be endowed with the structure of an $\mathcal{O}_K$-Hopf order in $K[G]$, and that in many instances, there are a number of other $\mathcal{O}_K$-Hopf orders in $K[G]$, all containing $\mathcal{O}_K[G]$ (see [6, Proposition 3.2, Proposition 7.3]). We denote an $\mathcal{O}_K$-Hopf order in $K[G]$ by Λ. The counit map is denoted by $\epsilon : \Lambda \to \mathcal{O}_K$. $\mathcal{L}_\Lambda$ is the space of left integrals of Λ. The linear dual of Λ, denoted by $\mathcal{B}$, is an $\mathcal{O}_K$-Hopf order in the algebra $\mathrm{Map}(G, K)$. The counit map of $\mathcal{B}$ is given by $\epsilon : \mathcal{B} \to \mathcal{O}_K$, and $\mathcal{L}_\mathcal{B}$ is the space of left integrals of $\mathcal{B}$.

There is a notion of "tame Λ-extension" found in [2, §1]. The $\mathcal{O}_K$-algebra M is a *tame Λ-extension* (of $\mathcal{O}_K$) if M is a Λ-module algebra, faithful as a Λ-module, $\mathrm{rank}_{\mathcal{O}_K}(M) = \mathrm{rank}_{\mathcal{O}_K}(\Lambda)$ as projective $\mathcal{O}_K$-modules, and $\mathcal{L}_\Lambda M = M^\Lambda = \mathcal{O}_K$. If we specialize to the case where L/K is an abelian extension with group G and $\Lambda = \mathcal{O}_K[G]$, then $\mathcal{O}_L$ is a tame $\mathcal{O}_K[G]$-extension if and only if L/K is tamely ramified ([2, §1]). Thus the Hilbert–Speiser

2000 *Mathematics Subject Classification*: 11R18, 11R29, 11R33, 13C05.

The authors would like to thank N. Byott for his many suggestions and comments which improved this paper considerably. Specifically, Theorem 2.2 is due to Byott. In addition, the authors thank the referee whose comments improved the presentation and content of this paper.

property may be recast as follows: A number field K is Hilbert–Speiser if each tame $\mathcal{O}_K[G]$-extension of the form $\mathcal{O}_L$ for an abelian extension L/K with group G is so that $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module. To say that a field K is not Hilbert–Speiser means that for some finite abelian group G there exists a tame $\mathcal{O}_K[G]$-extension which is not a free $\mathcal{O}_K[G]$-module. Thus for any field $K \neq \mathbb{Q}$, there exists a finite abelian group G, and a tame $\mathcal{O}_K[G]$-extension which is not a free $\mathcal{O}_K[G]$-module. Moreover, this tame $\mathcal{O}_K[G]$-extension is the ring of integers of some Galois extension L/K with group G.

We wonder: for a given field K, and an $\mathcal{O}_K$-Hopf order Λ in $K[G]$, $\Lambda \neq \mathcal{O}_K[G]$, can one find a tame Λ-extension which is not a free Λ-module? If so, what is the structure of such a tame Λ-extension?

In this paper we show how to find nontrivial tame extensions over Hopf orders. We assume that G is an l-elementary abelian group of order l^n, which we denote by C_l^n. To find nontrivial tame Λ-extensions, we extend the technique used by the authors in [5] to show that no field $K \neq \mathbb{Q}$ is Hilbert–Speiser. The key step is to generalize the authors' lower bound on the collection of "Galois module classes" to Hopf orders other than $\mathcal{O}_K[C_l^n]$ ([5, Corollary 7]). We use our lower bound to give explicit examples of $\mathcal{O}_K$-Hopf orders Λ in $K[C_l^n]$ for which there exist tame Λ-extensions which are not free over Λ. These nontrivial tame Λ-extensions are not necessarily the full ring of integers of some Galois extension L/K with group C_l^n, however. They have the structure of certain tame Λ-extensions which locally, at primes above $l\mathcal{O}_K$, are principal homogeneous spaces over $\mathcal{B}$. We call these tame Λ-extensions "semilocal principal homogeneous spaces over $\mathcal{B}$" (see [1, §3]). These semilocal principal homogeneous spaces play the role of the rings of integers in the integral group ring case; the collection of their classes in the locally free classgroup $Cl(\Lambda)$ generalizes the set of Galois module classes.

For the convenience of the reader, we review the integral group ring case of [5]. Let L/K be a Galois extension with group C_l^n. It is well known that L/K is tamely ramified (tame) if and only if $\mathcal{O}_L$ is a locally free $\mathcal{O}_K[C_l^n]$-module. $\mathcal{O}_L$ then determines a *Galois module class*, $(\mathcal{O}_L)$, in the locally free classgroup $Cl(\mathcal{O}_K[C_l^n])$. Let $R(\mathcal{O}_K[C_l^n])$ denote the set of classes in $Cl(\mathcal{O}_K[C_l^n])$ which are realizable as Galois module classes of rings of integers of tame Galois extensions L/K with group C_l^n. For any abelian group G, McCulloh [8] has shown that $R(\mathcal{O}_K[G])$ is a subgroup of $Cl(\mathcal{O}_K[G])$, and describes $R(\mathcal{O}_K[G])$ explicitly for the case $G = C_l^n$ in [7].

Let $\mathcal{M}$ denote the maximal integral order in $K[C_l^n]$. The homomorphism $f : \mathcal{O}_K[C_l^n] \to \mathcal{M}$ induces a homomorphism of classgroups $f_* : Cl(\mathcal{O}_K[C_l^n]) \to Cl(\mathcal{M})$, defined by $(M) \mapsto (\mathcal{M} \otimes_{\mathcal{O}_K[C_l^n]} M)$. The kernel of f_* is called the *kernel group* of $Cl(\mathcal{O}_K[C_l^n])$, and is denoted by $D(\mathcal{O}_K[C_l^n])$.

The space of left integrals of the $\mathcal{O}_K$-Hopf order $\mathcal{O}_K[C_l^n]$ in $K[C_l^n]$ is $\mathcal{L}_{\mathcal{O}_K[C_l^n]} = \mathcal{O}_K\Sigma_n$, where Σ_n denotes the sum of the elements in C_l^n. Thus $\epsilon(\mathcal{L}_{\mathcal{O}_K[C_l^n]}) = l^n\mathcal{O}_K$. A *Swan module* is the $\mathcal{O}_K[C_l^n]$-module defined by $\langle r, \Sigma_n\rangle = r\mathcal{O}_K[C_l^n] + \Sigma_n\mathcal{O}_K[C_l^n]$, where $r \in \mathcal{O}_K$ is relatively prime to $l^n\mathcal{O}_K$. Each Swan module $\langle r, \Sigma_n\rangle$ is a locally free $\mathcal{O}_K[C_l^n]$-module and thus corresponds to a class $(\langle r, \Sigma_n\rangle)$ in $Cl(\mathcal{O}_K[C_l^n])$. The collection of classes of Swan modules forms a subgroup of $Cl(\mathcal{O}_K[C_l^n])$ which is called the *Swan subgroup* of $Cl(\mathcal{O}_K[C_l^n])$. The Swan subgroup is denoted by $T(\mathcal{O}_K[C_l^n])$.

Put $\overline{\mathcal{O}}_K = \mathcal{O}_K/l^n\mathcal{O}_K$. Let S^* denote the multiplicative group of units of a ring S. Let $V_{l^n} = \overline{\mathcal{O}}_K^*/\sigma(\mathcal{O}_K^*)$, where $\sigma(\mathcal{O}_K^*)$ is the image of $\mathcal{O}_K^*$ under the canonical surjection $\sigma : \mathcal{O}_K \to \overline{\mathcal{O}}_K$. Then there is a surjection of groups $T(\mathcal{O}_K[C_l^n]) \to V_{l^n}^{l^n-1}$. Moreover, the power $T(\mathcal{O}_K[C_l^n])^{l^{n-1}(l-1)/2}$ is contained in $R(\mathcal{O}_K[C_l^n]) \cap D(\mathcal{O}_K[C_l^n])$. These facts yield the following lower bound for $R(\mathcal{O}_K[C_l^n]) \cap D(\mathcal{O}_K[C_l^n])$ ([5, Corollary 7]).

THEOREM 1.0. *Let K be an algebraic number field, and let C_l^n be an l-elementary abelian group of order l^n. If $V_{l^n}^{(l^n-1)l^{n-1}(l-1)/2}$ is nontrivial, then $R(\mathcal{O}_K[C_l^n]) \cap D(\mathcal{O}_K[C_l^n])$ is nontrivial.*

Thus, if $V_{l^n}^{(l^n-1)l^{n-1}(l-1)/2}$ is nontrivial, there exists a Galois module class $(\mathcal{O}_L)$ for some tame extension L/K, for which $\mathcal{O}_L$ is not free over $\mathcal{O}_K[C_l^n]$. Specifically, for any $K \neq \mathbb{Q}$, there exists an odd prime l for which $V_l^{(l-1)^2/2}$ is nontrivial. Thus there exists a tame degree l Galois extension L/K for which $\mathcal{O}_L$ is not a free $\mathcal{O}_K[C_l]$-module, that is, $\mathcal{O}_L$ is a tame $\mathcal{O}_K[C_l]$-extension which is not free over $\mathcal{O}_K[C_l]$. In this manner the authors [5] show that no field $K \neq \mathbb{Q}$ is Hilbert–Speiser.

Since we seek nontrival tame Λ-extensions for $\Lambda \neq \mathcal{O}_K[C_l^n]$, it is natural to seek an analogue of Theorem 1.0 for $\mathcal{O}_K$-Hopf orders Λ in $K[C_l^n]$. We require that our $\mathcal{O}_K$-Hopf orders satisfy a technical condition which we describe as follows. Let $\mathbb{F}_{l^n}^+$ denote the additive group of the finite field of order l^n. Then $C_l^n \cong \mathbb{F}_{l^n}^+$ and $C \cong \mathbb{F}_{l^n}^*$ is a group of automorphisms of C_l^n. The $\mathcal{O}_K$-Hopf order Λ in $K[C_l^n]$ *admits* C if these automorphisms map Λ into itself. Such Λ are *Raynaud orders*, that is, $\mathcal{O}_K$-Hopf algebra orders Λ in $K[C_l^n]$ which admit a group of automorphisms of C_l^n isomorphic to $\mathbb{F}_{l^n}^*$. (Equivalently: the corresponding group scheme $\operatorname{Spec}\Lambda$ is provided with an action of $\mathbb{F}_{l^n}$; see [9], [4, §4].) One sees immediately that $\mathcal{O}_K[C_l^n]$ is a Raynaud order.

We shall generalize Theorem 1.0 to $\mathcal{O}_K$-Hopf orders Λ in $K[C_l^n]$ which admit C. We give the (somewhat expected) analogues for $D(\mathcal{O}_K[C_l^n])$, $T(\mathcal{O}_K[C_l^n])$, and V_{l^n}, which we denote by $D(\Lambda)$, $T(\Lambda)$, and $V_{\epsilon(\mathcal{L}_\Lambda)}$, respectively. The proper analogue for $R(\mathcal{O}_K[C_l^n])$ is $\mathcal{R}(\Lambda)$, which we define to be the set of classes in the locally free classgroup $Cl(\Lambda)$ of the form $(\mathcal{X})$

where $\mathcal{X}$ is a semilocal principal homogeneous space over $\mathcal{B}$. The analogue of Theorem 1.0 is the following:

Main Theorem (Theorem 2.12). *Let C_l^n be an elementary abelian group of order l^n, let K be an algebraic number field, and let Λ be an $\mathcal{O}_K$-Hopf order in $K[C_l^n]$ which admits C. Suppose $\epsilon(\mathcal{L}_{\mathcal{B}})$ is a principal ideal in $\mathcal{O}_K$. If $V_{\epsilon(\mathcal{L}_\Lambda)}^{(l^n-1)l^{n-1}(l-1)/2}$ is nontrivial, then $\mathcal{R}(\Lambda)\cap D(\Lambda)$ is nontrivial.*

We apply our Main Theorem to the case $K=\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive l^mth root of unity, $m\ge 1$, and Λ is a Raynaud order in $K[C_l^n]$, $n=1,2$, which is a Larson order (cf. [6]). For these Raynaud orders we show that the group $V_{\epsilon(\mathcal{L}_\Lambda)}^{(l^n-1)l^{n-1}(l-1)/2}$ is nontrivial. Hence there exist tame Λ-extensions which are not free Λ-modules. These nontrivial tame Λ-extensions are semilocal principal homogeneous spaces over $\mathcal{B}$.

2. Construction of the lower bound. In this section we prove our Main Theorem. Throughout, we assume that Λ is an $\mathcal{O}_K$-Hopf order in $K[C_l^n]$ which admits C. We first develop an analogue for the collection of Galois module classes $R(\mathcal{O}_K[C_l^n])$. Let $\mathcal{O}_K^{\mathrm{c}}$ denote the integral closure of $\mathcal{O}_K$ in some fixed algebraic closure K^{c} of K. Let $\mathcal{X}$ be an $\mathcal{O}_K$-algebra which is finitely generated and projective as an $\mathcal{O}_K$-module. Suppose C_l^n acts on $\mathcal{X}$ as $\mathcal{O}_K$-algebra automorphisms. Then $\mathcal{X}$ is a *principal homogeneous space over* $\mathcal{B}$ if the action of C_l^n extends to an action of Λ on $\mathcal{X}$, and if for some homomorphism $\tau:\mathcal{X}\to\mathcal{O}_K^{\mathrm{c}}$ of $\mathcal{O}_K$-algebras, the $\mathcal{O}_K$-linear map

$$\varrho:\mathcal{X}\otimes_{\mathcal{O}_K}\mathcal{O}_K^{\mathrm{c}}\to\mathcal{B}\otimes_{\mathcal{O}_K}\mathcal{O}_K^{\mathrm{c}}=\mathrm{Hom}_{\mathcal{O}_K}(\Lambda,\mathcal{O}_K^{\mathrm{c}}),$$

defined by $\varrho(x\otimes r)(h)=\tau(h\cdot x)r$, for $x\in\mathcal{X}$, $r\in\mathcal{O}_K^{\mathrm{c}}$ and $h\in\Lambda$, is bijective. $\mathcal{X}$ is a principal homogeneous space over $\mathcal{B}$ if and only if $\mathcal{X}$ is a Galois Λ-extension of $\mathcal{O}_K$ in the sense of [2, §1]. We denote the collection of principal homogeneous spaces over $\mathcal{B}$ by $\mathrm{PH}(\mathcal{B})$.

Now let $\mathcal{O}_l$ denote the semilocalization of $\mathcal{O}_K$ at the ideal $l\mathcal{O}_K$. (Here we are surpressing the subscript K for convenience of notation.) Let $\mathcal{B}_l=\mathcal{B}\otimes_{\mathcal{O}_K}\mathcal{O}_l$. The definition of principal homogeneous space over $\mathcal{B}$ extends to the domain $\mathcal{O}_l$, and we let $\mathrm{PH}(\mathcal{B}_l)$ denote the collection of principal homogeneous spaces over the $\mathcal{O}_l$-Hopf order $\mathcal{B}_l$ in $\mathrm{Map}(C_l^n,K)$. Let $\mathcal{X}^{(l)}$ be a principal homogeneous space in $\mathrm{PH}(\mathcal{B}_l)$. Let $X=K\mathcal{X}^{(l)}$ and let $\mathcal{O}^X$ denote the integral closure of $\mathcal{O}_K$ in X. A *semilocal principal homogeneous space over* $\mathcal{B}$ is an order $\mathcal{X}$ of the form $\mathcal{X}^{(l)}\cap\mathcal{O}^X$ ([1, §3]). The set of isomorphism classes of such orders is denoted by $\mathrm{SPH}(\mathcal{B})$. The linear dual $\mathcal{B}$ is a semilocal principal homogeneous space over itself. Observe that $\mathcal{X}^{(l)}$ is the semilocalization $\mathcal{X}_l=\mathcal{X}\otimes_{\mathcal{O}_K}\mathcal{O}_l$. Moreover, each $\mathcal{X}\in\mathrm{SPH}(\mathcal{B})$ is a Λ-module (see [1, §3]).

Let $\mathcal{X} = \mathcal{X}^{(l)} \cap \mathcal{O}^X$ be a given element of $\mathrm{SPH}(\mathcal{B})$ for some $\mathcal{X}^{(l)} \in \mathrm{PH}(\mathcal{B}_l)$. Put $\Lambda_l = \Lambda \otimes_{\mathcal{O}_K} \mathcal{O}_l$. Then $\mathcal{X}_l$ is a Galois Λ_l-extension of $\mathcal{O}_l$. Thus by [3, Proposition 2.3], $\mathcal{X}_l$ is a tame Λ_l-extension of $\mathcal{O}_l$. It follows that $\mathcal{X}_l$ is Λ_l-faithful, and $\mathrm{rank}_{\mathcal{O}_l}(\mathcal{X}_l) = \mathrm{rank}_{\mathcal{O}_l}(\Lambda_l)$. Thus $\mathcal{X}$ is Λ-faithful, and $\mathrm{rank}_{\mathcal{O}_K}(\mathcal{X}) = \mathrm{rank}_{\mathcal{O}_K}(\Lambda)$. Moreover,

$$\mathcal{L}_\Lambda \mathcal{X} = \mathcal{L}_\Lambda(\mathcal{X}_l \cap \mathcal{O}^X) = \mathcal{L}_{\Lambda_l}\mathcal{X}_l \cap \mathcal{O}^X = \mathcal{X}_l^{\Lambda_l} \cap \mathcal{O}^X = \mathcal{X}^\Lambda$$

and

$$\mathcal{L}_\Lambda \mathcal{X} = \mathcal{L}_\Lambda(\mathcal{X}_l \cap \mathcal{O}^X) = \mathcal{L}_{\Lambda_l}\mathcal{X}_l \cap \mathcal{O}^X = \mathcal{O}_l \cap \mathcal{O}^X = \mathcal{O}_K.$$

Hence each $\mathcal{X} \in \mathrm{SPH}(\mathcal{B})$ is a tame Λ-extension.

Let ϖ be the element of $\mathrm{Map}(C_l^n, K)$ defined by $\varpi(g) = 1$ if $g = 1$, and $\varpi(g) = 0$ if $g \neq 1$. Then by [1, Lemma 1.3(ii)], $\mathcal{L}_\mathcal{B} = \mathcal{I}\varpi$ for some ideal $\mathcal{I} \subseteq \mathcal{O}_K$. Note $\epsilon(\mathcal{L}_\mathcal{B}) = \epsilon(\mathcal{I}\varpi) = \mathcal{I}$, hence $\mathcal{L}_\mathcal{B} = \epsilon(\mathcal{L}_\mathcal{B})\varpi$. By [1, Proposition 3.4], each $\mathcal{X} \in \mathrm{SPH}(\mathcal{B})$ is a locally free rank one Λ-module, and $\mathrm{Tr}(\mathcal{X}) = \epsilon(\mathcal{L}_\mathcal{B})$, where Tr denotes the trace map.

As a locally free rank one Λ-module, the element $\mathcal{X} \in \mathrm{SPH}(\mathcal{B})$ corresponds to a class $(\mathcal{X}) \in Cl(\Lambda)$. We have the class invariant map $\Psi : \mathrm{SPH}(\mathcal{B}) \to Cl(\Lambda)$, defined by $\Psi(\mathcal{X}) = (\mathcal{X})(\mathcal{B})^{-1}$. Byott [1] has given a description of the image $\Psi(\mathrm{SPH}(\mathcal{B}))$ which we will presently state. We employ the characterization of the classgroup given in [7] and [1]. Let $\mathcal{O}'_K = \mathcal{O}_K[l^{-1}]$, and $\Lambda' = \Lambda \otimes_{\mathcal{O}_K} \mathcal{O}'_K$. Let $I(\Lambda')$ denote the free abelian group generated by the prime fractional ideals of Λ'. Let (Λ_l^*) denote the subgroup of principal ideals in $I(\Lambda')$. Any locally free rank one Λ-module M can be written in the form $M = \overline{\eta} \cdot x$ where x is a "semilocal generator for M", and where $\overline{\eta} = \eta \cap \Lambda_l$, with $\eta \in I(\Lambda')$ (see [1, §4]). There is an isomorphism

$$Cl(\Lambda) \cong I(\Lambda')/(\Lambda_l^*), \tag{2.0}$$

where the class (M) corresponds to the image of η in $I(\Lambda')/(\Lambda_l^*)$.

We now give Byott's characterization of $\Psi(\mathrm{SPH}(\mathcal{B}))$. The augmentation map $\epsilon : \Lambda \to \mathcal{O}_K$ induces a map of classgroups $\epsilon_* : Cl(\Lambda) \to Cl(\mathcal{O}_K)$, defined by $(M) \mapsto (\mathcal{O}_K \otimes_\Lambda M)$. Let $Cl_0(\Lambda)$ denote the kernel of ϵ_*. Via the isomorphism of (2.0), the action of C on Λ induces an action of C on $Cl_0(\Lambda)$. This action extends to an action of $\mathbb{Z}[C]$ on $Cl_0(\Lambda)$. Put $\theta = \sum_{\delta \in C} t(\delta)\delta^{-1}$ where $t(\delta)$ is the least nonnegative residue (mod l) of the image of δ under the trace map $\mathrm{Tr} : \mathbb{F}_{l^n} \to \mathbb{F}_l \cong \mathbb{Z}/l\mathbb{Z}$. Then $\mathcal{J} = \mathbb{Z}[C](\theta/l) \cap \mathbb{Z}[C]$ is the *Stickelberger ideal* in $\mathbb{Z}[C]$. Let $Cl_0(\Lambda)^\mathcal{J}$ denote the image of $Cl_0(\Lambda)$ under the Stickelberger ideal. We have the following theorem ([1, Theorem 5.2]):

THEOREM 2.1 (Byott). *Let $\mathcal{B}$ denote the dual of an $\mathcal{O}_K$-Hopf order Λ in $K[C_l^n]$. If Λ admits C, then the image of the map $\Psi : \mathrm{SPH}(\mathcal{B}) \to Cl(\Lambda)$ is precisely $Cl_0(\Lambda)^\mathcal{J}$.*

We now define an analogue for the Galois module classes. Let $\mathcal{R}(\Lambda)$ denote the collection of classes in $Cl(\Lambda)$ of the form $(\mathcal{X})$ where $\mathcal{X}$ is a semilocal principal homogeneous space over $\mathcal{B}$. For $\Lambda = \mathcal{O}_K[C_l^n]$, $\mathcal{R}(\Lambda)$ is the collection of classes $(\mathcal{X})$ where $\mathcal{X}$ is a semilocal principal homogeneous space over $\mathcal{O}_K[C_l^n]^D$, the linear dual of $\mathcal{O}_K[C_l^n]$. These semilocal principal homogeneous spaces consist of the integral closures of $\mathcal{O}_K$ in the Galois algebras over K with group C_l^n which are at most tamely ramified at every prime of $\mathcal{O}_K$ (cf. [1, p. 422]). $\mathcal{R}(\mathcal{O}_K[C_l^n])$ is therefore the collection of classes of these integral closures. On the other hand, $R(\mathcal{O}_K[C_l^n])$ denotes the set of classes in $Cl(\mathcal{O}_K[C_l^n])$ of the form $(\mathcal{O}_L)$ where $\mathcal{O}_L$ is the ring of integers of a tame Galois extension L/K with group C_l^n.

We claim that $\mathcal{R}(\mathcal{O}_K[C_l^n]) = R(\mathcal{O}_K[C_l^n])$. Indeed, since $\mathcal{O}_K[C_l^n]^D$ is a free $\mathcal{O}_K[C_l^n]$-module, the image of the class invarient map is $\mathcal{R}(\mathcal{O}_K[C_l^n])$. By the main result of McCulloh [7] we have $Cl_0(\mathcal{O}_K[C_l^n])^{\mathcal{J}} = R(\mathcal{O}_K[C_l^n])$. Thus by Theorem 2.1, $\mathcal{R}(\mathcal{O}_K[C_l^n]) = R(\mathcal{O}_K[C_l^n])$. We conclude that $\mathcal{R}(\Lambda)$ generalizes the collection of Galois module classes. In fact, if $\epsilon(\mathcal{L}_{\mathcal{B}})$ is a principal ideal in $\mathcal{O}_K$, then $\mathcal{R}(\Lambda)$ is the image of the class invarient map for any Λ which admits C.

THEOREM 2.2. *Let Λ be an $\mathcal{O}_K$-Hopf order in $K[C_l^n]$ which admits C, with linear dual $\mathcal{B}$. Suppose $\epsilon(\mathcal{L}_{\mathcal{B}})$ is a principal ideal in $\mathcal{O}_K$, then $\mathcal{R}(\Lambda) = \Psi(\mathrm{SPH}(\mathcal{B}))$.*

Proof. We claim that if $\epsilon(\mathcal{L}_{\mathcal{B}})$ is a principal ideal in $\mathcal{O}_K$, then the class $(\mathcal{B})$ is trivial in $Cl(\Lambda)$, thus $\Psi(\mathcal{X}) = (\mathcal{X})$. It is then immediate that $\Psi(\mathrm{SPH}(\mathcal{B})) = \mathcal{R}(\Lambda)$. Recall that $\mathcal{L}_{\mathcal{B}} = \epsilon(\mathcal{L}_{\mathcal{B}})\varpi$, where ϖ is the element of $\mathrm{Map}(C_l^n, K)$ defined previously. Since $\epsilon(\mathcal{L}_{\mathcal{B}})$ is principal, $\epsilon(\mathcal{L}_{\mathcal{B}}) = \mathcal{O}_K x$ for some element $x \in \mathcal{O}_K$. By [1, Lemma 1.3(iii)],

$$\mathcal{B} = \Lambda \cdot \mathcal{L}_{\mathcal{B}} = \Lambda \cdot \mathcal{O}_K x\varpi = \Lambda \cdot x\varpi,$$

thus $\mathcal{B}$ is a free Λ-module, and $(\mathcal{B})$ is trivial in $Cl(\Lambda)$. Hence $\Psi(\mathcal{X}) = (\mathcal{X})$ for each $\mathcal{X} \in \mathrm{SPH}(\mathcal{B})$. ∎

We next develop analogues for the kernel group and the Swan subgroup of $Cl(\mathcal{O}_K[C_l^n])$. The inclusion $f : \Lambda \to \mathcal{M}$ induces a homomorphism of class groups $f_* : Cl(\Lambda) \to Cl(\mathcal{M})$, given by $(M) \mapsto (\mathcal{M} \otimes_\Lambda M)$. The *kernel group* of $Cl(\Lambda)$, denoted by $D(\Lambda)$, is defined to be the kernel of f_*.

Let $r \in \mathcal{O}_K$ be relatively prime to $\epsilon(\mathcal{L}_\Lambda)$. *A Hopf–Swan module* is the Λ-module defined by $\langle r, \mathcal{L}_\Lambda\rangle = r\Lambda + \mathcal{L}_\Lambda$. When $\Lambda = \mathcal{O}_K[C_l^n]$ the Hopf–Swan module $\langle r, \mathcal{L}_\Lambda\rangle$ specializes to a Swan module.

The methods of [11, Proposition 2.4] apply to show that each Hopf–Swan module $\langle r, \mathcal{L}_\Lambda\rangle$ is a locally free rank one Λ-module. Let $\overline{\mathcal{O}}_K = \mathcal{O}_K/\epsilon(\mathcal{L}_\Lambda)$, and let σ denote the canonical surjection $\sigma : \mathcal{O}_K \to \overline{\mathcal{O}}_K$. Put $\Gamma = \Lambda/\mathcal{L}_\Lambda$, and let κ denote the canonical surjection $\kappa : \Lambda \to \Gamma$. Let $\overline{\epsilon} : \Gamma \to \overline{\mathcal{O}}_K$ be the map defined by $\overline{\epsilon}(h \bmod \mathcal{L}_\Lambda) = \epsilon(h) \bmod \epsilon(\mathcal{L}_\Lambda)$. There exists a fiber product

$$
\begin{array}{ccc}
\Lambda & \xrightarrow{\ \kappa\ } & \Gamma \\
\Big\downarrow{\scriptstyle \epsilon} & & \Big\downarrow{\scriptstyle \overline{\epsilon}} \\
\mathcal{O}_K & \xrightarrow{\ \sigma\ } & \overline{\mathcal{O}}_K
\end{array}
\tag{2.3}
$$

and we can identify Λ with the subring N of $\mathcal{O}_K \times \Gamma$ defined by

$$N = \{(s, \gamma) \in \mathcal{O}_K \times \Gamma : \sigma(s) = \overline{\epsilon}(\gamma)\}.$$

The element $h \in \Lambda$ corresponds to the pairing $(\epsilon(h), \kappa(h)) \in N$. Over K, the fiber product (2.3) yields the identification $K[C_l^n] = K \times K[C_l^n]/\Sigma_n K[C_l^n]$, and Λ may be viewed as an $\mathcal{O}_K$-order in $K \times K[C_l^n]/\Sigma_n K[C_l^n]$.

Let p be a prime ideal of K, and let K_p denote the completion of K at the nontrivial discrete valuation of K corresponding to p. Let $\mathcal{O}_{K_p}$ be the ring of integers of K_p. Let $\Lambda_p = \mathcal{O}_{K_p} \otimes_{\mathcal{O}_K} \Lambda$, $\langle r, \mathcal{L}_\Lambda\rangle_p = \langle r, \mathcal{L}_{\Lambda_p}\rangle$, and $\Gamma_p = \Lambda_p/\mathcal{L}_{\Lambda_p}$. We have the completions of the maps ϵ, κ, $\overline{\epsilon}$, and σ, which we denote by $\epsilon_p : \Lambda_p \to \mathcal{O}_{K_p}$, $\kappa_p : \Lambda_p \to \Gamma_p$, $\overline{\epsilon}_p : \Gamma_p \to \overline{\mathcal{O}}_{K_p}$, and $\sigma_p : \mathcal{O}_{K_p} \to \overline{\mathcal{O}}_{K_p}$, respectively. Let $J(K \times K[C_l^n]/\Sigma_n K[C_l^n])$ be the *idèle group* of $K \times K[C_l^n]/\Sigma_n K[C_l^n]$ defined by

$$
\begin{aligned}
&J(K \times K[C_l^n]/\Sigma_n K[C_l^n]) \\
&\qquad = \Big\{(\alpha_p) \in \prod K_p^* \times (K_p[C_l^n]/\Sigma_n K_p[C_l^n])^* : \alpha_p \in \Lambda_p^* \ ,\ \text{a.e.}\Big\},
\end{aligned}
$$

where the product is over all prime ideals of $\mathcal{O}_K$. For any idèle α in $J(K \times K[C_l^n]/\Sigma_n K[C_l^n])$, let $\Lambda\alpha$ denote the locally free Λ-module defined by

$$\Lambda\alpha = \bigcap_p \, (\Lambda_p \alpha_p \cap (K \times K[C_l^n]/\Sigma_n K[C_l^n])).$$

THEOREM 2.4. *The Hopf–Swan module $\langle r, \mathcal{L}_\Lambda\rangle$ is a locally free rank one Λ-module equal to $\Lambda\alpha$, where α is the idèle in $J(K \times K[C_l^n]/\Sigma_n K[C_l^n])$ defined by $\alpha_p = 1$ if $p \nmid r\mathcal{O}_K$, and $\alpha_p = (1, r) \in \mathcal{O}_{K_p} \times \Gamma_p$ if $p \mid r\mathcal{O}_K$.*

Proof. Following the method of [11, Proposition 2.4(i)], we show that $\langle r, \mathcal{L}_\Lambda\rangle_p = \Lambda_p \alpha_p$ for all primes p of K. Suppose $p \nmid r\mathcal{O}_K$. Then r is a unit of $\mathcal{O}_{K_p}$, hence $\langle r, \mathcal{L}_\Lambda\rangle_p = \Lambda_p = \Lambda_p \alpha_p$. On the other hand, if $p \mid r\mathcal{O}_K$ then $p \nmid \epsilon(\mathcal{L}_\Lambda)$, since r is relatively prime to $\epsilon(\mathcal{L}_\Lambda)$. Thus the ideal $\epsilon(\mathcal{L}_{\Lambda_p})$ consists of units of $\mathcal{O}_{K_p}$, and hence, $\mathcal{O}_{K_p}/\epsilon(\mathcal{L}_{\Lambda_p})$ is trivial. The identification from the fiber product (2.3) then yields

$$\Lambda_p = \mathcal{O}_{K_p} \times \Gamma_p. \tag{2.5}$$

Now let $rh_1 + h_2$ be an element of $\langle r, \mathcal{L}_\Lambda\rangle_p$ with $h_1 \in \Lambda_p$, $h_2 \in \mathcal{L}_{\Lambda_p}$. Then $rh_1 + h_2$ is identified via (2.5) with the element $(r\epsilon_p(h_1) + \epsilon_p(h_2), r\kappa_p(h_1))$ in $\mathcal{O}_{K_p} \times \Gamma_p$. Since $\epsilon_p(h_2)$ is a unit in $\mathcal{O}_{K_p}$, $\langle r, \mathcal{L}_\Lambda\rangle_p$ corresponds to the cartesian product $\mathcal{O}_{K_p} \times r\Gamma_p$ under the identification of (2.5). Thus any element of $\langle r, \mathcal{L}_\Lambda \rangle_p$ can be viewed as an $(\mathcal{O}_{K_p} \times \Gamma_p)$-multiple of the generator $(1, r)$. It follows that $\langle r, \mathcal{L}_\Lambda \rangle_p = \Lambda_p \alpha_p$. ∎

In view of Theorem 2.4, the Hopf–Swan module $\langle r, \mathcal{L}_\Lambda \rangle$ corresponds to a class $(\langle r, \mathcal{L}_\Lambda \rangle)$ in $Cl(\Lambda)$. We seek an explicit description of the collection of Hopf–Swan classes in $Cl(\Lambda)$. Observe that the fiber product (2.3) yields the exact Mayer–Vietoris sequence

$$(2.6) \qquad 1 \to \Lambda^* \to \Gamma^* \times \mathcal{O}_K^* \to \overline{\mathcal{O}}_K^* \xrightarrow{\partial} D(\Lambda) \to D(\Gamma) \oplus D(\mathcal{O}_K) \to 0$$

(see [10, 1.10]). For an element $u = r \bmod \epsilon(\mathcal{L}_\Lambda) \in \overline{\mathcal{O}}_K^*$, let $\Lambda \cdot u$ denote the left Λ-module defined as

$$\Lambda \cdot u = \{(s, \gamma) \in \mathcal{O}_K \times \Gamma : \sigma(s)u = \overline{\epsilon}(\gamma)\}$$

(see [10, 4.19]). (Note that if $u = 1$, then $\Lambda \cdot 1 = \Lambda$ via the identification from the fiber product (2.3).) By [10, 4.20], $\Lambda \cdot u$ is a locally free rank one Λ-module, corresponding to the class $(\Lambda \cdot u) \in Cl(\Lambda)$. The boundary map $\partial : \overline{\mathcal{O}}_K^* \to D(\Lambda)$ is given as $\partial(u) = (\Lambda \cdot u)$. The image of the boundary map ∂ is precisely the collection of classes of Hopf–Swan modules.

Theorem 2.7. *Let ∂ be the boundary map given in* (2.6). *Then the image of ∂ is the collection of classes* $\{(\langle r, \mathcal{L}_\Lambda \rangle)\}$.

Proof. Following the method of [11, Proposition 2.4(ii)], let β be the element of $\prod \Lambda_p^*$ defined by $\beta_p = 1$ if $p \mid r\mathcal{O}_K$, and $\beta_p = r$ if $p \nmid r\mathcal{O}_K$. Let μ be the element of $\prod \mathcal{O}_{K_p}^* \times \Gamma_p^*$ defined by $\mu_p = 1$ if $p \mid r\mathcal{O}_K$, and $\mu_p = (r, 1)$ if $p \nmid r\mathcal{O}_K$. Then with $(1, r^{-1}) \in K \times K[C_l^n]/\Sigma_n K[C_l^n]$, we have $\alpha(1, r^{-1})\beta = \mu$. It follows that $\Lambda\mu \cong \Lambda\alpha = \langle r, \mathcal{L}_\Lambda \rangle$.

Since $\Lambda\mu$ is a projective Λ-module, we may apply the exact functor $- \otimes_\Lambda \Lambda\mu$ to the fiber product of (2.3) to obtain the fiber product

$$\begin{array}{ccc} \Lambda\mu & \longrightarrow & \Gamma \otimes_\Lambda \Lambda\mu \\ \downarrow & & \downarrow \\ \mathcal{O}_K \otimes_\Lambda \Lambda\mu & \longrightarrow & \overline{\mathcal{O}}_K \otimes_\Lambda \Lambda\mu \end{array}$$

Over K we obtain

$$\begin{array}{ccc} K\Lambda\mu & \longrightarrow & K[C_l^n]/\Sigma_n K[C_l^n] \otimes_\Lambda \Lambda\mu \\ \downarrow & & \downarrow \\ K \otimes_\Lambda \Lambda\mu & \longrightarrow & 0 \end{array}$$

and we may identify $K\Lambda\mu$ with

$$(K \otimes_\Lambda \Lambda\mu) \times (K[C_l^n]/\Sigma_n K[C_l^n] \otimes_\Lambda \Lambda\mu).$$

There is a natural embedding of $\Lambda\mu$ into the $K[C_l^n]$-module $K\Lambda\mu$. Let $\mathcal{O}_K\Lambda\mu$ denote the $\mathcal{O}_K$-submodule of $K\Lambda\mu$ generated by $\{x_1 : (x_1,x_2)\in\Lambda\mu\}$, and let $\Gamma\Lambda\mu$ denote the Γ-submodule of $K\Lambda\mu$ generated by $\{x_2 : (x_1,x_2)\in\Lambda\mu\}$. Then as in [10, §3], there are isomorphisms

$$\mathcal{O}_K\otimes_\Lambda \Lambda\mu\cong\mathcal{O}_K\Lambda\mu \quad\text{and}\quad \Gamma\otimes_\Lambda\Lambda\mu\cong\Gamma\Lambda\mu.$$

We claim that $\mathcal{O}_K\Lambda\mu=\mathcal{O}_K$ and $\Gamma\Lambda\mu=\Gamma$. Suppose $p\,|\,r\mathcal{O}_K$. In this case

$$\Lambda_p\mu_p=\Lambda_p=\mathcal{O}_{K_p}\times\Gamma_p,$$

hence, locally at p, $\mathcal{O}_{K_p}\Lambda_p\mu_p=\mathcal{O}_{K_p}$, and $\Gamma_p\Lambda_p\mu_p=\Gamma_p$. If $p\nmid r\mathcal{O}_K$, then $\Lambda_p\mu_p=N_p(r,1)$ where $N_p=\{(s,\gamma)\in\mathcal{O}_{K_p}\times\Gamma_p:\sigma_p(s)=\overline{\epsilon}_p(\gamma)\}$, and $r\in\mathcal{O}_{K_p}^*$. Now since $(r^{-1},r^{-1})\in N_p$ we have $(1,r^{-1})\in\Lambda_p\mu_p$. Thus $\mathcal{O}_{K_p}\Lambda_p\mu_p=\mathcal{O}_{K_p}$. Since $(1,1)\in N_p$, we have $(r,1)\in\Lambda_p\mu_p$. It follows that $\Gamma_p\Lambda_p\mu_p=\Gamma_p$. We conclude $\mathcal{O}_K\Lambda\mu=\mathcal{O}_K$ and $\Gamma\Lambda\mu=\Gamma$, which yields the isomorphisms

$$\mathcal{O}_K\otimes_\Lambda\Lambda\mu\cong\mathcal{O}_K\quad\text{and}\quad\Gamma\otimes_\Lambda\Lambda\mu\cong\Gamma.$$

By [10, Lemma 4.20(iv)], $\Lambda\mu\cong\Lambda\cdot v$ for some $v\in\overline{\mathcal{O}}_K^*$, hence $\langle r,\mathcal{L}_\Lambda\rangle\cong\Lambda\mu\cong\Lambda\cdot v$. Since the collection of Hopf–Swan modules $\{\langle r,\mathcal{L}_\Lambda\rangle\}$ is in a one-to-one correspondence with the elements of $\overline{\mathcal{O}}_K^*$, it follows that the image of ∂ is $\{(\langle r,\mathcal{L}_\Lambda\rangle)\}$. ■

In view of Theorem 2.7, we define the *Hopf–Swan subgroup of* $Cl(\Lambda)$, denoted by $T(\Lambda)$, to be the image of ∂. We consider $T(\Lambda)$ as an additive abelian subgroup of $Cl(\Lambda)$. For a positive integer w, let $(\langle r,\mathcal{L}_\Lambda\rangle)^w$ denote the sum of w copies of the class $(\langle r,\mathcal{L}_\Lambda\rangle)\in T(\Lambda)$. Define $T(\Lambda)^w$ to be those elements $(\langle s,\mathcal{L}_\Lambda\rangle)\in T(\Lambda)$ of the form $(\langle r,\mathcal{L}_\Lambda\rangle)^w$ for some class $(\langle r,\mathcal{L}_\Lambda\rangle)\in T(\Lambda)$.

At this point we can begin the construction of our lower bound for $\mathcal{R}(\Lambda)\cap D(\Lambda)$. Let $\sigma(\mathcal{O}_K^*)$ denote the image of $\mathcal{O}_K^*$ under the canonical surjection $\sigma:\mathcal{O}_K\to\overline{\mathcal{O}}_K=\mathcal{O}_K/\epsilon(\mathcal{L}_\Lambda)$. Put $V_{\epsilon(\mathcal{L}_\Lambda)}=\overline{\mathcal{O}}_K^*/\sigma(\mathcal{O}_K^*)$. We claim that there is a surjection of groups $T(\Lambda)\to V_{\epsilon(\mathcal{L}_\Lambda)}^{l^n-1}$. From the exact sequence (2.6) we obtain

$$T(\Lambda)\cong\overline{\mathcal{O}}_K^*/(\sigma(\mathcal{O}_K^*)\cdot\overline{\epsilon}(\Gamma^*)). \tag{2.8}$$

We assert that the (l^n-1)st power of $\overline{\epsilon}(\Gamma^*)$ is in $\sigma(\mathcal{O}_K^*)$.

LEMMA 2.9. *Suppose Λ is an $\mathcal{O}_K$-Hopf order in $K[C_l^n]$ which admits C. Recall $\Gamma=\Lambda/\mathcal{L}_\Lambda$. If $\gamma\in\Gamma^*$, then $\overline{\epsilon}(\gamma)^{l^n-1}\in\sigma(\mathcal{O}_K^*)$.*

Proof. Since C is a group of automorphisms of C_l^n, C is a group of automorphisms of Λ and Γ. By [1, Lemma 1.3(i)], $\mathcal{L}_\Lambda=I(\Sigma_n/l^n)$, for some integral ideal I. Thus $\epsilon(\mathcal{L}_\Lambda)=\epsilon(I(\Sigma_n/l^n))=I$. It follows that $\mathcal{L}_\Lambda=\epsilon(\mathcal{L}_\Lambda)(\Sigma_n/l^n)$. Write ς for the identity of C_l^n. C fixes ς, and permutes the remaining elements of C_l^n transitively, hence $\Lambda^C = \mathcal{O}_K\varsigma + \mathcal{L}_\Lambda$. Now the C-cohomology of the short exact sequence

$$0 \to \mathcal{L}_\Lambda \to \Lambda \to \Gamma \to 0,$$

yields the exact sequence $0 \to \mathcal{O}_K\varsigma \to \Gamma^C \to H^1(C, \mathcal{L}_\Lambda)$. Since C acts trivially on $\mathcal{L}_\Lambda$, $H^1(C, \mathcal{L}_\Lambda) = \mathrm{Hom}(C, \mathcal{L}_\Lambda)$. Note $\mathrm{Hom}(C, \mathcal{L}_\Lambda) = 0$ since C is a torsion group and $\mathcal{L}_\Lambda$ is torsion-free as an abelian group. Thus we identify Γ^C with $\mathcal{O}_K$.

Now let N be the norm map $N : \Gamma^* \to \mathcal{O}_K^*$, defined by $N(\gamma) = \prod_{\delta \in C} \gamma^\delta$. For $\gamma = h + \mathcal{L}_\Lambda \in \Gamma$, and $\delta \in C$,

$$\overline{\epsilon}(\gamma^\delta) = \epsilon(h^\delta) \bmod \epsilon(\mathcal{L}_\Lambda) = \epsilon(h) \bmod \epsilon(\mathcal{L}_\Lambda) = \overline{\epsilon}(\gamma),$$

since δ permutes the elements of C_l^n, and $\epsilon(g) = 1$ for all $g \in C_l^n$. Thus

$$\overline{\epsilon}(N(\gamma)) = \overline{\epsilon}\Big(\prod_{\delta \in C} \gamma^\delta\Big) = \prod_{\delta \in C} \overline{\epsilon}(\gamma^\delta) = \overline{\epsilon}(\gamma)^{l^n - 1}.$$

Now for $u \in (\Gamma^C)^* \cong \mathcal{O}_K^*$, $\overline{\epsilon}(u) = u \bmod \epsilon(\mathcal{L}_\Lambda)$, since $\epsilon(u) = u$ for $u \in \mathcal{O}_K$. Thus $\overline{\epsilon}(N(\gamma)) \in \sigma(\mathcal{O}_K^*)$, which yields $\overline{\epsilon}(\gamma)^{l^n-1} \in \sigma(\mathcal{O}_K^*)$. ■

LEMMA 2.10. *Let Λ be an $\mathcal{O}_K$-Hopf order in $K[C_l^n]$ which admits C, and let $T(\Lambda)$ be the Hopf–Swan subgroup of $Cl(\Lambda)$. Recall $V_{\epsilon(\mathcal{L}_\Lambda)} = \overline{\mathcal{O}}_K^*/\sigma(\mathcal{O}_K^*)$. Then there is a surjective map $T(\Lambda) \to V_{\epsilon(\mathcal{L}_\Lambda)}^{l^n-1}$.*

Proof. From (2.8) we have

$$T(\Lambda) \cong \overline{\mathcal{O}}_K^*/\sigma(\mathcal{O}_K^*) \cdot \overline{\epsilon}(\Gamma^*) \cong V_{\epsilon(\mathcal{L}_\Lambda)}/(\overline{\epsilon}(\Gamma^*)/\sigma(\mathcal{O}_K^*)).$$

Now by Lemma 2.9, $\overline{\epsilon}(\Gamma^*)/\sigma(\mathcal{O}_K^*)$ is contained in the kernel of the $(l^n - 1)$st power map $V_{\epsilon(\mathcal{L}_\Lambda)} \to V_{\epsilon(\mathcal{L}_\Lambda)}$, hence there is a surjection $T(\Lambda) \to V_{\epsilon(\mathcal{L}_\Lambda)}^{l^n-1}$. ■

The next step in the construction of a lower bound for $\mathcal{R}(\Lambda) \cap D(\Lambda)$ is to relate $T(\Lambda)$ and $\mathcal{R}(\Lambda) \cap D(\Lambda)$.

LEMMA 2.11. *Let K be an algebraic number field with ring of integers $\mathcal{O}_K$ and let Λ be an $\mathcal{O}_K$-Hopf order in $K[C_l^n]$ which admits C. Suppose $\epsilon(\mathcal{L}_\mathcal{B})$ is a principal ideal in $\mathcal{O}_K$. Then $T(\Lambda)^{l^{n-1}(l-1)/2} \subseteq \mathcal{R}(\Lambda) \cap D(\Lambda)$.*

Proof. We use the method of [5, Proposition 4], where the theorem is proved for the case $\Lambda = \mathcal{O}_K[C_l^n]$. For $\delta \in C$, one has $(\langle r, \mathcal{L}_\Lambda \rangle)^\delta = (\langle r, \mathcal{L}_\Lambda \rangle)$, thus $T(\Lambda)$ is a $\mathbb{Z}[C]$-submodule of $D(\Lambda)$. Let $\epsilon_*^\mathcal{M} : Cl(\mathcal{M}) \to Cl(\mathcal{O}_K)$ denote the map of classgroups induced by the augmentation $\epsilon^\mathcal{M} : \mathcal{M} \to \mathcal{O}_K$. Then $\epsilon_*^\mathcal{M} \circ f_* = \epsilon_*$ where f_* is the homomorphism of class groups $f_* : Cl(\Lambda) \to Cl(\mathcal{M})$ defined by $(M) \mapsto (\mathcal{M} \otimes_\Lambda M)$. Hence $D(\Lambda) \subseteq Cl_0(\Lambda)$. Let $T(\Lambda)^\mathcal{J}$ denote the image of $T(\Lambda)$ under the action of $\mathcal{J}$. Then

$$T(\Lambda)^\mathcal{J} \subseteq Cl_0(\Lambda)^\mathcal{J} \cap D(\Lambda),$$

and hence

$$T(\Lambda)^{\mathcal{J}} \subseteq \Psi(\mathrm{SPH}(\mathcal{B})) \cap D(\Lambda),$$

by Theorem 2.1. Since $\epsilon(\mathcal{L}_{\mathcal{B}})$ is a principal ideal,

$$T(\Lambda)^{\mathcal{J}} \subseteq \mathcal{R}(\Lambda) \cap D(\Lambda),$$

by Theorem 2.2.

The group of automorphisms C is finite and we may list its elements $\delta_1, \ldots, \delta_m$. Let $(\langle r, \mathcal{L}_\Lambda\rangle)$ be a class in $T(\Lambda)$, and let $\alpha = \sum_{i=1}^m a_i\delta_i$ be an element in $\mathcal{J} \subseteq \mathbb{Z}[C]$. Let $\varepsilon : \mathbb{Z}[C] \to \mathbb{Z}$ denote the augmentation map defined by $\varepsilon(\delta_i) = 1$ for $i = 1, \ldots, m$. Then

$$\begin{aligned}(\langle r, \mathcal{L}_\Lambda\rangle)^{\alpha} &= (\langle r, \mathcal{L}_\Lambda\rangle)^{a_1\delta_1} + (\langle r, \mathcal{L}_\Lambda\rangle)^{a_2\delta_2} + \ldots + (\langle r, \mathcal{L}_\Lambda\rangle)^{a_m\delta_m}\\ &= (\langle r, \mathcal{L}_\Lambda\rangle)^{a_1} + (\langle r, \mathcal{L}_\Lambda\rangle)^{a_2} + \ldots + (\langle r, \mathcal{L}_\Lambda\rangle)^{a_m}\\ &= (\langle r, \mathcal{L}_\Lambda\rangle)^{\varepsilon(\alpha).}\end{aligned}$$

Thus $T(\Lambda)^{\mathcal{J}} = T(\Lambda)^{\varepsilon(\mathcal{J})}$. Now by [5, Lemma 3], $T(\Lambda)^{\varepsilon(\mathcal{J})} = T(\Lambda)^{l^{n-1}(l-1)/2}$. It follows that $T(\Lambda)^{l^{n-1}(l-1)/2} \subseteq \mathcal{R}(\Lambda) \cap D(\Lambda)$. ∎

We are now in a position to prove our Main Theorem.

THEOREM 2.12. *Let C_l^n be an l-elementary abelian group, let K be an algebraic number field, and let Λ be an $\mathcal{O}_K$-Hopf order in $K[C_l^n]$, which admits C. Suppose $\epsilon(\mathcal{L}_{\mathcal{B}})$ is a principal ideal in $\mathcal{O}_K$. If $V_{\epsilon(\mathcal{L}_\Lambda)}^{(l^n-1)l^{n-1}(l-1)/2}$ is nontrivial, then $\mathcal{R}(\Lambda) \cap D(\Lambda)$ is nontrivial.*

Proof. Suppose $V_{\epsilon(\mathcal{L}_\Lambda)}^{(l^n-1)l^{n-1}(l-1)/2}$ is nontrivial. Then by Lemma 2.10, $T(\Lambda)^{l^{n-1}(l-1)/2}$ is nontrivial. It follows that $\mathcal{R}(\Lambda) \cap D(\Lambda)$ is nontrivial by Lemma 2.11. ∎

3. Applications to cyclotomic fields. In this section we find a collection of fields $K/\mathbb{Q}$ and Raynaud orders Λ in $K[C_l^n]$, $n = 1, 2$, for which the corresponding group $V_{\epsilon(\mathcal{L}_\Lambda)}^{(l^n-1)l^{n-1}(l-1)/2}$ is nontrivial. We then apply Theorem 2.12 to show the existence of tame Λ-extensions which are not free Λ-modules. These tame Λ-extensions are semilocal principal homogeneous spaces over $\mathcal{B}$.

Assume $n = 1$, and let $l > 3$ be a prime which satisfies *Vandiver's conjecture*, that is, $l \nmid h^+(\mathbb{Q}(\zeta_1))$, where $h^+(\mathbb{Q}(\zeta_1))$ is the class number of the maximal real subfield of $\mathbb{Q}(\zeta_1)$, and ζ_1 is a primitive lth root of unity. Vandiver's conjecture is known to be true for primes $l < 4000000$ (see [12]).

Let ζ_m denote a primitive l^mth root of unity, $m \geq 1$. We set $K = \mathbb{Q}(\zeta_m)$, then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$. The ideal $l\mathbb{Z}[\zeta_m]$ decomposes as $l\mathbb{Z}[\zeta_m] = (1-\zeta_m)^{l^{m-1}(l-1)}\mathbb{Z}[\zeta_m]$. Each integer j with $0 \leq j \leq l^{m-1}$, gives rise to an

$\mathbb{Z}[\zeta_m]$-Hopf order in $K[C_l]$ of the form

$$\Lambda_j = \mathbb{Z}[\zeta_m][\{(g-1)(1-\zeta_m)^{-j}\mathbb{Z}[\zeta_m]\}],$$

where the g runs through all the nontrivial elements of C_l. Such Hopf orders are called *Larson orders in* $K[C_l]$ ([6, Proposition 3.2]). It is easy to see that each Λ_j admits C. The space of left integrals $\mathcal{L}_{\Lambda_j}$ is so that $\epsilon(\mathcal{L}_{\Lambda_j}) = (1-\zeta_m)^{(l^{m-1}-j)(l-1)}\mathbb{Z}[\zeta_m]$ (cf. [6, Lemma 4.2]). For convenience, put $S = \mathbb{Z}[\zeta_m]$. For each j, $0 \le j \le l^{m-1}$, let $\overline{S}_j = S/(1-\zeta_m)^{(l^{m-1}-j)(l-1)}S$, and let $\sigma_j : S \to \overline{S}_j$ denote the canonical surjection. Put $V_{\epsilon(\mathcal{L}_{\Lambda_j})} = \overline{S}_j^*/\sigma_j(S^*)$. We shall employ Theorem 2.12 to show that $\mathcal{R}(\Lambda_j) \cap D(\Lambda_j)$ is nontrivial for $0 \le j \le l^{m-1}-1$. We begin with a lemma.

LEMMA 3.0. *For each j, $0 \le j \le l^{m-1}-1$, there is a surjective map of groups,*

$$V_{\epsilon(\mathcal{L}_{\Lambda_j})} \to V_{\epsilon(\mathcal{L}_{\Lambda_{l^{m-1}-1}})}.$$

Proof. Since $(1-\zeta_m)^{(l^{m-1}-j)(l-1)}S \subseteq (1-\zeta_m)^{l-1}S$, there is a surjection

$$\beta_j : \overline{S}_j \to \overline{S}_{l^{m-1}-1}.$$

We claim that β_j restricts to a surjection of multiplicative groups,

$$\beta_j : \overline{S}_j^* \to \overline{S}_{l^{m-1}-1}^*.$$

We have

$$S \cong \mathbb{Z} \oplus (1-\zeta_m)\mathbb{Z} \oplus (1-\zeta_m)^2\mathbb{Z} \oplus \ldots \oplus (1-\zeta_m)^{l^{m-1}(l-1)-1}\mathbb{Z},$$

so that $\overline{S}_{l^{m-1}-1} = S/(1-\zeta_m)^{l-1}S$ is isomorphic to C_l^{l-1} as additive groups. Let

$$v = a_0 + a_1(1-\zeta_m) + \ldots + a_{l-2}(1-\zeta_m)^{l-2},$$

$a_r \in C_l$, be an element of $\overline{S}_{l^{m-1}-1}^*$. Necessarily, $(a_0, l) = 1$. Consequently, there exists an element $w \in \overline{S}_j^*$ for which $\beta_j(w) = v$, thus $\beta_j : \overline{S}_j^* \to \overline{S}_{l^{m-1}-1}^*$ is a surjection of multiplicative groups.

The subgroup $\sigma_j(S^*)$ of $\overline{S}_j^*$ then induces a surjection

$$\overline{S}_j^*/\sigma_j(S^*) \to \overline{S}_{l^{m-1}-1}^*/\beta_j(\sigma_j(S^*)).$$

Observing that $\beta_j(\sigma_j(S^*)) = \sigma_{l^{m-1}-1}(S^*)$ yields the desired surjection

$$V_{\epsilon(\mathcal{L}_{\Lambda_j})} \to V_{\epsilon(\mathcal{L}_{\Lambda_{l^{m-1}-1}})}. \blacksquare$$

THEOREM 3.1. *Let $l > 3$ be a prime which satisfies Vandiver's conjecture. Let $m \ge 1$, and let j be any integer $0 \le j \le l^{m-1}-1$. Then $\mathcal{R}(\Lambda_j) \cap D(\Lambda_j)$ is nontrivial.*

Proof. We show that for j, $0 \le j \le l^{m-1}-1$, the group $V_{\epsilon(\mathcal{L}_{\Lambda_j})}^{(l-1)^2/2}$ is nontrivial. For the moment we fix $j = l^{m-1}-1$. Our first step is to compute the group $\overline{S}^*_{l^{m-1}-1} = (S/(1-\zeta_m)^{l-1}S)^*$. Observe that $(S/(1-\zeta_m)^{l-1}S)^*$ has order $(l-1)l^{l-2}$ as a multiplicative group, and the elements

$$1+(1-\zeta_m),\quad 1+(1-\zeta_m)^2,\quad 1+(1-\zeta_m)^3,\ \ldots,\ 1+(1-\zeta_m)^{l-2},$$

have order l. It follows that

$$\overline{S}^*_{l^{m-1}-1} = (S/(1-\zeta_m)^{l-1}S)^* \cong C_{l-1}\times C_l^{l-2}.$$

We next characterize the subgroup $\sigma_{l^{m-1}-1}(S^*)$ of $(S/(1-\zeta_m)^{l-1}S)^*$. We employ the cyclotomic units of K^+ and K, where K^+ denotes the maximal real subfield of K. The *cyclotomic units* U^+ *of* K^+ are the elements of S^* generated by -1 and the quantities of the form

$$u_a = \zeta_m^{(1-a)/2}\,\frac{1-\zeta_m^a}{1-\zeta_m},\qquad 1<a<l^m/2,\ (a,l)=1.$$

The *cyclotomic units* U *of* K are the elements of S^* generated by ζ_m and the cyclotomic units of K^+ (cf. [12, Lemma 8.1]).

Let E^+ denote the full group of units of the maximal real subfield K^+. By Washington [12, Theorem 8.2], the index $[E^+:U^+]=h^+(K)$. Moreover, by [12, Corollary 4.13], $S^*=WE^+$, where W denotes the group of roots of unity in K. Now since $U=WU^+$ by definition,

$$[E^+:U^+]=[WE^+:WU^+]=[S^*:U],$$

thus the quotient group S^*/U is finite of order $h^+(K)$.

Consider the surjection of groups

$$\sigma_{l^{m-1}-1}: S^*\to \sigma_{l^{m-1}-1}(S^*).$$

The subgroup $U\le S^*$ induces a surjection of quotients

$$S^*/U\to \sigma_{l^{m-1}-1}(S^*)/\sigma_{l^{m-1}-1}(U).$$

Let $\overline{-\zeta_m}$ denote the residue class of $-\zeta_m$ modulo $(1-\zeta_m)^{l-1}S$, and let $\overline{u}_a$ denote the residue class of u_a modulo $(1-\zeta_m)^{l-1}S$ for $1<a<l^m/2$, $(a,l)=1$. We claim that the classes $\overline{-\zeta_m}$ and

$$\{\overline{u}_a \mid 1<a\le (l-1)/2\}$$

generate all the elements of $\sigma_{l^{m-1}-1}(U)$. Certainly this is true for the case $m=1$, so we assume that $m>1$. Observe that

$$1+\zeta_m+\ldots+\zeta_m^{l-1}\equiv 0 \bmod (1-\zeta_m)^{l-1}S,$$

hence for $1<a<l^m/2$, $(a,l)=1$, $a\equiv 1 \bmod l$,

$$u_a\equiv \zeta_m^{(1-a)/2} \bmod (1-\zeta_m)^{l-1}S,$$

that is,

$$\overline{u}_a = (\overline{\zeta}_m)^{(1-a)/2}.$$

For $a \not\equiv 1 \bmod l$, $a > l+1$, let k denote the least positive integer congruent to a modulo l. Then

$$u_a \equiv \zeta_m^{(1-a)/2} \zeta_m^{(k-1)/2} u_k \bmod (1-\zeta_m)^{l-1} S,$$

thus

$$\overline{u}_a = (\overline{\zeta}_m)^{(k-a)/2} \overline{u}_k.$$

We conclude that the classes $\{\overline{u}_a \mid 1 < a \leq l-1\}$ together with $\overline{-\zeta_m}$ generate $\sigma_{l^{m-1}-1}(U)$.

Similarly, one shows that the classes $\{\overline{u}_a \mid 1 < a \leq (l-1)/2\}$ together with $\overline{-\zeta_m}$ generate $\sigma_{l^{m-1}-1}(U)$. It follows that $\sigma_{l^{m-1}-1}(U)$ is a subgroup of $(S/(1-\zeta_m)^{l-1}S)^* \cong C_{l-1} \times C_l^{l-2}$ of the form

$$\sigma_{l^{m-1}-1}(U) = \langle \overline{-\zeta_m} \rangle \times \langle \overline{u}_2 \rangle \times \ldots \times \langle \overline{u}_{(l-1)/2} \rangle.$$

Thus $\sigma_{l^{m-1}-1}(U)$ can have at most $(l-1)/2$ copies of C_l in its cyclic decomposition. Now suppose $\sigma_{l^{m-1}-1}(S^*)$ had more than $(l-1)/2$ copies of C_l in its decomposition. Then l divides the order of $\sigma_{l^{m-1}-1}(S^*)/\sigma_{l^{m-1}-1}(U)$, and hence l divides $h^+(K)$, the order of the group S^*/U. By [12, Corollary 10.6], $l \mid h^+(\mathbb{Q}(\zeta_1))$, that is, Vandiver's conjecture does not hold for l. This contradicts our assumption that l satisfies Vandiver's conjecture.

It follows that $\sigma_{l^{m-1}-1}(S^*)$ can have at most $(l-1)/2$ copies of C_l in its cyclic decomposition. Hence $V_{\epsilon(\mathcal{L}_{\Lambda_{l^{m-1}-1}})} = \overline{S}^*_{l^{m-1}-1}/\sigma_{l^{m-1}-1}(S^*)$ must contain at least one copy of C_l in its cyclic decomposition, since for $l > 3$,

$$l-2 > (l-1)/2.$$

We conclude that $V^{l-1}_{\epsilon(\mathcal{L}_{\Lambda_{l^{m-1}-1}})}$ is nontrivial. Thus by Lemma 3.0, $V^{l-1}_{\epsilon(\mathcal{L}_{\Lambda_j})}$ is nontrivial for all j, $0 \leq j \leq l^{m-1}-1$, and all m, $m \geq 1$. Consequently, $V^{(l-1)^2/2}_{\epsilon(\mathcal{L}_{\Lambda_j})}$ is nontrivial for all j, $0 \leq j \leq l^{m-1}-1$, and all m, $m \geq 1$. Let $\mathcal{B}_j$ denote the linear dual of Λ_j. The ideal $\epsilon(\mathcal{L}_{\mathcal{B}_j})$ is divisor of lS, hence principal, since all ideals of the cyclotomic field K dividing lS are principal ideals. An application of Theorem 2.12 then shows that $\mathcal{R}(\Lambda_j) \cap D(\Lambda_j)$ is nontrivial. ■

It is immediate from Theorem 3.1 that for each j, $0 \leq j \leq l^{m-1}-1$, there exists a tame Λ_j-extension M which is not a free Λ_j-module. We know that M is a semilocal principal homogeneous space over $\mathcal{B}_j$. Thus locally, at the prime ideal $(1-\zeta_m)S$ lying above lS, M is a principal homogeneous space over $\mathcal{B}_j$.

We claim that there exists a nontrivial class $(M) \in \mathcal{R}(\Lambda_j)$ for which M is the full ring of integers of some Galois extension L/K with group C_l. To this end, put $w = 1 + (1-\zeta_m)^{l(l^{m-1}-j)+1}$. Then $L = K(z)$, $z = w^{1/l}$, is a Galois extension of degree l. By [2, Theorem 16.1], $\mathcal{O}_L$ is a Galois Λ_j-extension, thus $\mathcal{O}_L$ is a semilocal principal homogeneous space over $\mathcal{B}_j$. Hence there is some element of $\mathrm{SPH}(\mathcal{B}_j)$ which is integrally closed over S. Now let (M) be the nontrivial element of $\mathcal{R}(\Lambda_j)$ which exists via Theorem 3.1. Then by [1, Theorem 5.6], there exists an $\mathcal{X} \in \mathrm{SPH}(\mathcal{B}_j)$ with $(\mathcal{X}) = (M)$ for which $\mathcal{X}$ is the full ring of integers of some Galois extension of K with group C_l. Since $K[C_l]$ satisfies the Eichler condition ([10, p. 307]), $M \cong \mathcal{X}$, thus M is the full ring of integers of some Galois extension L/K with group C_l.

We next consider the case $n = 2$, and find a collection of Raynaud orders Λ in $K[C_l^2]$, $l > 3$, $K = \mathbb{Q}(\zeta_m)$, $S = \mathbb{Z}[\zeta_m]$, $m \geq 2$, for which there exists tame Λ-extensions which are not free over Λ.

Put $C_l^2 = C_l \times C_l'$. Let ν denote the nontrivial discrete valuation on K which corresponds to the prime ideal $(1-\zeta_m)S$. For each pair of integers i, j with $0 \leq i, j \leq l^{m-1}$, one may define an *l-adic order bounded group valuation ξ on $C_l \times C_l'$*, by setting $\xi(1,1) = \infty$, $\xi(h,1) = i$ for $h \in C_l$, $h \neq 1$, and $\xi(h,h') = j$, for $h \in C_l$, $h' \in C_l'$, $h' \neq 1$ ([6, Definition 1.1]). ξ gives rise to an S-Hopf order in $K[C_l \times C_l']$ of the form

$$\Lambda_{i,j} = S[\{(g-1)(1-\zeta_m)^{-\xi(g)}S\}],$$

where g runs through all the nontrivial elements of $C_l \times C_l'$ ([6, Proposition 3.2]). It is easy to see that $\Lambda_{i,j}$ is a Raynaud order if and only if $i = j$.

We consider only those Raynaud orders $\Lambda_{j,j}$ for which $2j \leq 2l^{m-1} - l$. We first compute the ideal $\epsilon(\mathcal{L}_{\Lambda_{j,j}})$. Note that each j satisfying the condition $2j \leq 2l^{m-1} - l$ corresponds to a Raynaud order Λ_j in $K[C_l]$. There exists an injection of K-Hopf algebras $A : K[C_l] \to K[C_l \times C_l']$ defined by $A(h) = (h,1)$, for $h \in C_l$. Let $K[C_l]^+$ denote the augmentation ideal of $K[C_l]$. Then

$$A(K[C_l]^+)K[C_l \times C_l'] = K[C_l \times C_l']A(K[C_l]^+),$$

thus the quotient ring $K[C_l \times C_l']/A(K[C_l]^+)K[C_l \times C_l']$ has the structure of a K-Hopf algebra, which is isomorphic to $K[C_l']$ as K-Hopf algebras.

It follows that there is a surjective map of K-Hopf algebras

$$B : K[C_l \times C_l'] \to K[C_l'].$$

Thus, in the sense of Larson ([6, §2]), there exists a short exact sequence of K-Hopf algebras

$$K[C_l] \xrightarrow{A} K[C_l \times C_l'] \xrightarrow{B} K[C_l'].$$

Observe that $\Lambda_j = A^{-1}(\Lambda_{j,j})$ and $\Lambda_j = B(\Lambda_{j,j})$. Thus by [6, Proposition 2.1] one has $\epsilon(\mathcal{L}_{\Lambda_{j,j}}) = (1-\zeta_m)^{(l-1)(2l^{m-1}-2j)}S$.

Let $\bar{S}_{j,j} = S/(1-\zeta_m)^{(l-1)(2l^{m-1}-2j)}S$, and let $\sigma_{j,j} : S \to \bar{S}_{j,j}$ denote the canonical surjection. Put $V_{\epsilon(\mathcal{L}_{\Lambda_{j,j}})} = \bar{S}^*_{j,j}/\sigma_{j,j}(S^*)$.

THEOREM 3.2. *Let $l > 3$ be a prime which satisfies Vandiver's conjecture, and let j be any integer for which $0 \leq 2j \leq 2l^{m-1} - l$, $m \geq 2$. Then $\mathcal{R}(\Lambda_{j,j}) \cap D(\Lambda_{j,j})$ is nontrivial.*

Proof. Consider the Raynaud (Larson) order $\Lambda_{l^{m-1}-l}$ in $K[C_l]$, and the corresponding canonical surjection $\sigma_{l^{m-1}-l} : S \to S/(1-\zeta_m)^{l(l-1)}S$. Using the method of Lemma 3.0 we have a surjection of groups

$$V_{\epsilon(\mathcal{L}_{\Lambda_{j,j}})} \to V_{\epsilon(\mathcal{L}_{\Lambda_{l^{m-1}-l}})} = (S/(1-\zeta_m)^{l(l-1)}S)^*/\sigma_{l^{m-1}-l}(S^*).$$

We seek to characterize the quotient $V_{\epsilon(\mathcal{L}_{\Lambda_{l^{m-1}-l}})}$. First observe that

$$S = \mathbb{Z} \oplus (1-\zeta_m)\mathbb{Z} \oplus (1-\zeta_m)^2\mathbb{Z} \oplus \ldots \oplus (1-\zeta_m)^{l^{m-1}(l-1)-1}\mathbb{Z},$$

thus $S/(1-\zeta_m)^{l(l-1)}S$ is isomorphic to $C_l^{l(l-1)}$ as additive groups. Consequently, there are $(l-1)l^{l(l-1)-1}$ elements in the unit group $(S/(1-\zeta_m)^{l(l-1)}S)^*$. The elements

$$1+(1-\zeta_m),\quad 1+(1-\zeta_m)^2,\quad 1+(1-\zeta_m)^3,\ \ldots,\ 1+(1-\zeta_m)^{l-2},$$

have order l^2 in $(S/(1-\zeta_m)^{l(l-1)}S)^*$. Moreover,

$$1+(1-\zeta_m)^{l-1},\quad 1+(1-\zeta_m)^{l},\quad 1+(1-\zeta_m)^{l+1},\ \ldots,\ 1+(1-\zeta_m)^{l(l-1)-1},$$

have order l in the unit group. Note that

$$(1+(1-\zeta_m)^r)^l \equiv 1+(1-\zeta_m)^{lr} \bmod (1-\zeta_m)^{l(l-1)}S,$$

for $r = 1,\ldots,l-2$. Thus the unit group $(S/(1-\zeta_m)^{l(l-1)}S)^*$ is generated by C_{l-1}, together with the elements $1+(1-\zeta_m)^r$, $r = 1,\ldots,l-2$, and the elements $1+(1-\zeta_m)^s$, for $l-1 \le s \le l(l-1)-1$, $(s,l) = 1$. It follows that

$$(S/(1-\zeta_m)^{l(l-1)}S)^* \cong C_{l-1} \times C_l^{l^2-3l+3} \times C_{l^2}^{l-2}.$$

We next characterize the image $\sigma_{l^{m-1}-l}(S^*)$. We know that the quotient group S^*/U is finite of order $h^+(K)$, where U denotes the cyclotomic units of K. The subgroup $U \le S^*$ induces a surjection of quotients

$$S^*/U \to \sigma_{l^{m-1}-l}(S^*)/\sigma_{l^{m-1}-l}(U).$$

Let $\overline{-\zeta_m}$ denote the residue class of $-\zeta_m$ modulo $(1-\zeta_m)^{l(l-1)}S$, and let $\overline{u}_a$ denote the residue class of u_a modulo $(1-\zeta_m)^{l(l-1)}S$ for $1 < a < l^m/2$, $(a,l) = 1$. By the method of the proof of Theorem 3.1, one sees that the classes $\{\overline{u}_a \mid 1 < a \le (l^2-1)/2\}$, $(a,l) = 1$, together with $\overline{-\zeta_m}$ generate $\sigma_{l^{m-1}-l}(U)$.

The important question is: What is the maximum number of copies of C_{l^2} that can occur in the cyclic decomposition of $\sigma_{l^{m-1}-l}(U)$? To answer this question, we consider the subgroup $(\sigma_{l^{m-1}-l}(U))^l$. Since

$$1+\zeta_m^l+\zeta_m^{2l}+\ldots+\zeta_m^{(l-1)l} \equiv 0 \bmod (1-\zeta_m)^{l(l-1)}S,$$

it is fairly obvious that the classes

$$\{(\overline{u}_a)^l \mid 1 < a \le (l-1)/2\},$$

together with $(\overline{-\zeta_m})^l$ generate $(\sigma_{l^{m-1}-l}(U))^l$. Thus there can be at most $(l-1)/2$ copies of C_l in the cyclic decomposition of $(\sigma_{l^{m-1}-l}(U))^l$. It follows that there can be at most $(l-1)/2$ copies of C_{l^2} in the cyclic decomposition of $\sigma_{l^{m-1}-l}(U)$.

If $\sigma_{l^{m-1}-l}(S^*)$ contains more than $(l-1)/2$ copies of C_{l^2} in its cyclic decomposition, then l^2, and hence l, divides the order of the quotient

$$\sigma_{l^{m-1}-l}(S^*)/\sigma_{l^{m-1}-l}(U).$$

It follows that l divides $h^+(K)$, the order of the group S^*/U. By [12, Corollary 10.6], $l \mid h^+(\mathbb{Q}(\zeta_1))$, that is, Vandiver's conjecture does not hold for l. This contradicts our assumption that l satisfies Vandiver's conjecture.

Thus $\sigma_{l^{m-1}-l}(S^*)$ contains at most $(l-1)/2$ copies of C_{l^2} in its cyclic decomposition. Now since $l > 3$,

$$(l-1)/2 < l-2,$$

thus $\sigma_{l^{m-1}-l}(S^*)$ has less than $l-2$ copies of C_{l^2} in its cyclic decomposition.

We conclude that $V_{\epsilon(\mathcal{L}_{\Lambda_{l^{m-1}-l}})} = \overline{S}^*_{l^{m-1}-l}/\sigma_{l^{m-1}-l}(S^*)$ contains at least one copy of C_{l^2} in its cyclic decomposition. It follows that $V^{l(l^2-1)(l-1)/2}_{\epsilon(\mathcal{L}_{\Lambda_{l^{m-1}-l}})}$ is nontrivial, and hence $V^{l(l^2-1)(l-1)/2}_{\epsilon(\mathcal{L}_{\Lambda_{j,j}})}$ is nontrivial. Let $\mathcal{B}_{j,j}$ denote the linear dual of $\Lambda_{j,j}$. Then the ideal $\epsilon(\mathcal{L}_{\mathcal{B}_{j,j}})$ is principal in the cyclotomic field K. Theorem 2.12 then applies to show the existence of a semilocal principal homogeneous space over $\mathcal{B}_{j,j}$ which is not a free $\Lambda_{j,j}$-module. ∎

References

[1] N. P. Byott, *Hopf orders and a generalisation of a theorem of L. R. McCulloh*, J. Algebra 177 (1995), 409–433.

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

[3] L. N. Childs and S. Hurley, *Tameness and local normal bases for objects of finite Hopf algebras*, ibid. 298 (1986), 763–778.

[4] C. Greither and L. N. Childs, *p-elementary group schemes—constructions and Raynaud's theory*, in: Hopf Algebras, Polynomial Formal Groups and Raynaud Orders, Mem. Amer. Math. Soc. 651 (1998).

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

[6] R. G. Larson, *Hopf algebra orders determined by group valuations*, J. Algebra 38 (1976), 414–452.

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

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

[9] M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France 102 (1974), 241–280.

[10] I. Reiner and S. V. Ullom, *A Mayer–Vietoris sequence for class groups*, J. Algebra 31 (1974), 305–342.

[11] S. V. Ullom, *Nontrivial lower bounds for class groups of integral group rings*, Illinois J. Math. 20 (1976), 361–371.

[12] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1997.

Department of Mathematics and Computer Science
College of Saint Elizabeth
Morristown, NJ 07960, U.S.A.
E-mail: dreplogle@liza.st-elizabeth.edu

Department of Mathematics
Auburn University Montgomery
Montgomery, AL 36124, U.S.A.
E-mail: underw@strudel.aum.edu

Received on 23.2.2001
and in revised form on 29.9.2001 (3983)