JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Paul J. TRUMAN

Hopf-Galois module structure of tame biquadratic extensions

Tome 24, n° 1 (2012), p. 173-199.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_1_173_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 173-199

Hopf-Galois module structure of tame biquadratic extensions

par Paul J. TRUMAN

Résumé. Dans [14], nous avons étudié la structure de Hopf-Galois module non classique des anneaux d'entiers dans des extensions modérément ramifiées de corps locaux et globaux, et avons prouvé une généralisation partielle du théorème de Noether dans ce contexte. Dans le présent article, nous considérons des extensions galoisiennes modérées de corps de nombres L/K de groupe $G \cong C_2 \times C_2$ et étudions en détail la structure locale et globale de l'anneau des entiers $\mathfrak{O}_L$ comme module sur son ordre associé $\mathfrak{A}_H$ dans chacune des algèbres de Hopf H donnant une structure de Hopf-Galois non classique sur l'extension. Les résultats de [14] impliquent que $\mathfrak{O}_L$ est localement libre sur chaque $\mathfrak{A}_H$, et nous en tirons des conditions nécessaires et suffisantes pour que $\mathfrak{O}_L$ soit libre sur chaque $\mathfrak{A}_H$. En particulier, nous considérons le cas $K = \mathbb{Q}$, et construisons des extensions possédant une grande diversité de comportement global, ce qui implique que l'analogue direct du théorème d'Hilbert-Speiser n'est pas vrai.

Abstract. In [14] we studied the nonclassical Hopf-Galois module structure of rings of algebraic integers in some tamely ramified extensions of local and global fields, and proved a partial generalisation of Noether's theorem to this setting. In this paper we consider tame Galois extensions of number fields L/K with group $G \cong C_2 \times C_2$ and study in detail the local and global structure of the ring of integers $\mathfrak{O}_L$ as a module over its associated order $\mathfrak{A}_H$ in each of the Hopf algebras H giving a nonclassical Hopf-Galois structure on the extension. The results of [14] imply that $\mathfrak{O}_L$ is locally free over each $\mathfrak{A}_H$, and we derive necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over each $\mathfrak{A}_H$. In particular, we consider the case $K = \mathbb{Q}$, and construct extensions exhibiting a variety of global behaviour, which implies that the direct analogue of the Hilbert-Speiser theorem does not hold.

Manuscrit reçu le 14 janvier 2010.
This work is based on the author's PhD thesis "Hopf-Galois Module Structure of Some Tamely Ramified Extensions" (University of Exeter, 2009). I would like to express my gratitude to Dr. Nigel Byott for his guidance during my studies.

1. Introduction

Let L/K be a finite Galois extension of number fields with group G and rings of algebraic integers $\mathfrak{O}_L, \mathfrak{O}_K$ respectively. Classical Galois module theory seeks to describe the structure of $\mathfrak{O}_L$ as a module over the integral group ring $\mathfrak{O}_K[G]$ or, more generally, over the associated order

$$\mathfrak{A}_{K[G]} = \{\alpha \in K[G] \mid \alpha \cdot x \in \mathfrak{O}_L \text{ for all } x \in \mathfrak{O}_L\}.$$

Noether's theorem asserts that if L/K is at most tamely ramified then $\mathfrak{A}_{K[G]} = \mathfrak{O}_K[G]$ and conversely, and in this case $\mathfrak{O}_L$ is *locally free* over $\mathfrak{A}_{K[G]}$ [10, Theorem 3]. That is, for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$, the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K,\mathfrak{p}} \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$ is a free module (of rank 1) over the completed associated order $\mathfrak{A}_{K[G],\mathfrak{p}} = \mathfrak{O}_{K,\mathfrak{p}} \otimes_{\mathfrak{O}_K} \mathfrak{A}_{K[G]}$. For wildly ramified extensions, we seek conditions for $\mathfrak{O}_L$ to be free or locally free over $\mathfrak{A}_{K[G]}$. The group algebra $K[G]$ is a Hopf algebra, and we can exploit this fact to yield information about the local structure of $\mathfrak{O}_L$ over $\mathfrak{A}_{K[G]}$. Childs [6] showed that if L/K is a finite Galois extension of p-adic fields with group G and the associated order $\mathfrak{A}_{K[G]}$ is a Hopf order in $K[G]$ then $\mathfrak{O}_L$ is free over $K[G]$. A consequence of this for Galois extensions of number fields L/K is that if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ and the completed associated order $\mathfrak{A}_{K[G],\mathfrak{p}}$ is a Hopf order in $K_{\mathfrak{p}}[G]$ then the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{K[G],\mathfrak{p}}$.

Hopf-Galois theory generalises the situation described above. The notion of a Hopf-Galois structure is defined for certain extensions of commutative rings, but we shall be interested mainly in studying Hopf-Galois structures on finite extensions L/K of number fields. Let H be a finite dimensional K-Hopf algebra, with counit $\varepsilon : H \to K$ and comultiplication $\Delta : H \to H \otimes_K H$. We use Sweedler notation to represent the image under Δ of an element $h \in H$:

$$\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}.$$

If L is an H-module then we say that L is an *H-module algebra* if for $h \in H$ and $s, t \in L$ we have:

$$h \cdot (st) = \sum_{(h)} (h_{(1)} \cdot s)(h_{(2)} \cdot t)$$
$$h \cdot 1 = \varepsilon(h)1.$$

We say that H gives a *Hopf-Galois structure on L/K* (or that L/K is an *H-Galois extension*) if L is an H-module algebra and additionally the K-linear map

$$j : L \otimes_K H \to End_K(L)$$

defined by

$$j(s \otimes h)(t) = s(h \cdot t) \quad \text{for} \quad s, t \in L, \quad h \in H$$

is an isomorphism of K-vector spaces.

We shall be concerned with finite Galois extensions L/K of number fields. Such extensions admit at least one Hopf-Galois structure, with Hopf algebra $K[G]$, and we call this the classical structure. The extension may also admit a number of other Hopf-Galois structures, which we call nonclassical. A theorem of Greither and Pareigis allows for the enumeration of all Hopf-Galois structures admitted by a finite separable extension of fields, and a gives a characterisation of the associated Hopf algebras. We state it here in a weakened form applicable to finite Galois extensions. For a finite set X we write $\mathrm{Perm}(X)$ for the group of permutations of X. A subgroup N of $\mathrm{Perm}(X)$ is called regular if $|N| = |X|$ and N acts transitively on X. We define an embedding $\lambda : G \to \mathrm{Perm}(G)$ by left translation:

$$\lambda(g)(x) = gx \text{ for } g, x \in G.$$

Then we have:

Theorem 1.1 (Greither and Pareigis). *There is a bijection between regular subgroups N of $Perm(G)$ normalised by $\lambda(G)$ and Hopf-Galois structures on L/K. If N is such a subgroup, then G acts on the group algebra $L[N]$ by acting simultaneously on the coefficients as the Galois group and on the group elements by conjugation via the embedding λ. The Hopf algebra giving the Hopf-Galois structure corresponding to the subgroup N is*

$$H = L[N]^G = \{z \in L[N] \mid {}^g z = z \text{ for all } g \in G\}.$$

Such a Hopf algebra then acts on the extension L/K as follows:

$$\left(\sum_{n\in N} c_n n\right) \cdot x = \sum_{n\in N} c_n(n^{-1}(1_G))x. \tag{1.1}$$

Proof. See [7, Theorem 6.8]. □

If L/K is an H-Galois extension of fields then L is a free H-module of rank 1 (see [7, (2.16)]) - this is a Hopf-Galois analogue of the normal basis theorem. In the case of local or global fields it is natural to investigate analogous results at integral level, and so we define within H an associated order:

$$\mathfrak{A}_H = \{h \in H \mid h \cdot x \in \mathfrak{O}_L \text{ for all } x \in \mathfrak{O}_L\},$$

and study the structure of $\mathfrak{O}_L$ as an $\mathfrak{A}_H$-module. We are particularly interested in establishing whether $\mathfrak{O}_L$ is a free or locally free $\mathfrak{A}_H$-module. The consequence of Childs' theorem described above generalises to this setting: if L/K is an H-Galois extension of number fields and $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ then $\mathfrak{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{H,\mathfrak{p}}$ if the latter is a Hopf order in the Hopf algebra $H_{\mathfrak{p}}$. If the extension L/K admits a number of Hopf-Galois structures, we can compare the structure of $\mathfrak{O}_L$ as a module over the associated orders

in the various Hopf algebras. The use of nonclassical Hopf-Galois structures has interesting consequences for wildly ramified extensions - $\mathfrak{O}_L$ may not be free or locally free over $\mathfrak{A}_{K[G]}$, but may be free or locally free over its associated order $\mathfrak{A}_H$ within some Hopf algebra H giving a nonclassical Hopf-Galois structure on the extension (see for example [4]). However, this approach also raises questions about tamely ramified extensions. If L/K is an extension of number fields which is at most tamely ramified then Noether's theorem asserts that $\mathfrak{A}_{K[G]} = \mathfrak{O}_K[G]$ and that $\mathfrak{O}_L$ is locally free over $\mathfrak{O}_K[G]$, and results such as the Hilbert-Speiser theorem [12] describe the global structure of $\mathfrak{O}_L$ over $\mathfrak{O}_K[G]$ in certain cases. It is not known whether analogous results hold in general for any nonclassical Hopf-Galois structures admitted by the extension. In [14] we studied some problems of this type, and proved some local results for certain classes of extensions which are at most tamely ramified. In particular we obtained the following results for completions of extensions of number fields:

Theorem 1.2. *Let L/K be a finite extension of number fields with group G, and suppose that L/K is H-Galois for the Hopf algebra $H = L[N]^G$. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which is unramified in $\mathfrak{O}_L$. Then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$, this is a Hopf order in $H_{\mathfrak{p}}$, and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.*

Proof. See [14, Theorem 5.4]. □

Theorem 1.3. *Let L/K be a finite Galois extension of number fields, and suppose that L/K is H-Galois for some commutative Hopf algebra H. Suppose that $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ lying above a prime number $p \nmid [L : K]$. Then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$, this is the unique maximal order in $H_{\mathfrak{p}}$, and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.*

Proof. See [14, Theorem 5.8]. □

Combining these, we obtained the following result concerning domestic extensions. (We call a Galois extension of number fields L/K *domestic* if no prime $\mathfrak{p}$ of $\mathfrak{O}_K$ lying above a prime number $p \mid [L : K]$ is ramified in $\mathfrak{O}_L$.)

Theorem 1.4. *Let L/K be a finite domestic extension of number fields which is H-Galois for some commutative Hopf algebra $H = L[N]^G$. Then $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$ and $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.*

Proof. See [14, Theorem 5.9]. □

As a particular case of this, we have:

Corollary 1.5. *Let L/K be a Galois extension of number fields of prime power degree which is at most tamely ramified. Suppose that L/K is H-Galois for some commutative Hopf algebra H. Then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.*

The purpose of this paper is to study in detail the local and global Hopf-Galois module structure of a class of tamely ramified extensions L/K of number fields to which this theorem applies. Specifically, we study tamely ramified Galois extensions of number fields with group $G \cong C_2 \times C_2$. We begin by characterising these extensions and determining explicit integral bases of $\mathfrak{O}_{L,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$. In addition to the classical structure with Hopf algebra $K[G]$, biquadratic extensions admit 3 nonclassical Hopf-Galois structures, as detailed in [5]. The results of [14] imply that $\mathfrak{O}_L$ is locally free over its associated order $\mathfrak{A}_H$ in each Hopf-Galois structure admitted by the extension. We calculate an explicit $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{A}_{H,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ and also give explicit generators of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. We use idèles, together with this detailed local information, to describe the locally free class group $\mathrm{Cl}\,(\mathfrak{A}_H)$ ([9, §49]) and derive necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$. Finally, we consider the case where $K = \mathbb{Q}$, where these results have a very explicit form. We show that in this case freeness of $\mathfrak{O}_L$ over $\mathfrak{A}_H$ is connected to representability questions for certain quadratic forms. In the classical structure $\mathbb{Q}[G]$, the Hilbert-Speiser theorem [12] asserts that $\mathfrak{O}_L$ is free over $\mathbb{Z}[G]$. In contrast to this, we give examples of extensions exhibiting a variety of global behaviours with respect to the associated orders in nonclassical Hopf-Galois structures.

We shall study analogous problems for tamely ramified Galois extensions of number fields with group $C_p \times C_p$, where p is an odd prime number, in a forthcoming paper.

2. Tame biquadratic extensions

Let K be a number field. The Galois extensions of K with group $G \cong C_2 \times C_2$ are of the form $L = K(\alpha, \beta)$, where $\alpha^2 = a$ and $\beta^2 = b$ are elements of K whose images in the $\mathbb{F}_2$-vector space $K^\times/K^{\times 2}$ are linearly independent. We shall establish congruence conditions on a and b which are equivalent to the extension L/K being tamely ramified.

We shall frequently employ completion. If $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ lying above a prime number p then we write $K_\mathfrak{p}$ for the completion of the number fields K with respect to the discrete absolute value arising from $\mathfrak{p}$. The field $K_\mathfrak{p}$ is a p-adic field with ring of integers (valuation ring) $\mathfrak{O}_{K,\mathfrak{p}}$ and maximal ideal $\mathfrak{p}\mathfrak{O}_{K,\mathfrak{p}} = \pi_\mathfrak{p}\mathfrak{O}_{K,\mathfrak{p}}$. We write $L_\mathfrak{p}$ for the $K_\mathfrak{p}$-algebra $K_\mathfrak{p} \otimes_K L$; in general this is not a p-adic field but a product of p-adic fields. We have the isomorphism

$$L_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}\mathfrak{O}_L} L_\mathfrak{P},$$

where the product is taken over those primes $\mathfrak{P}$ of $\mathfrak{O}_L$ lying above $\mathfrak{p}$ and each factor on the right hand side is a p-adic field [11, (1.8)]. We have a similar decomposition of the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K,\mathfrak{p}} \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$

into a product of valuation rings. In particular, if more than one prime of $\mathfrak{O}_L$ lies above $\mathfrak{p}$ then we must regard the image in $L_\mathfrak{p}$ of an element of L as a tuple. We shall often tacitly make use of this in what follows. The rings $L_\mathfrak{p}$ and $\mathfrak{O}_{L,\mathfrak{p}}$ are examples of *Galois algebras*.

Proposition 2.1. *The extension $K(\alpha,\beta)/K$ is tamely ramified if and only if a and b can be chosen to satisfy $a \equiv b \equiv 1 \pmod{4\mathfrak{O}_K}$.*

Proof. Since $[K(\alpha,\beta) : K] = 4$, the extension is tamely ramified if and only if no prime $\mathfrak{p}$ of $\mathfrak{O}_K$ lying above 2 is ramified in $\mathfrak{O}_L$. Since L is the compositum of $K(\alpha)$ and $K(\beta)$, L/K is tamely ramified if and only if both the subextensions $K(\alpha)/K$ and $K(\beta)/K$ are tamely ramified. Consider the subextension $K(\alpha)/K$; the argument for the subextension $K(\beta)/K$ is similar. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2. Using [7, (24.2)] and the discussion of Galois algebras above, the extension $K(\alpha)/K$ is tamely ramified if and only if for each prime $\mathfrak{P}$ of $\mathfrak{O}_{K(\alpha)}$ lying above $\mathfrak{p}$, the completion $K(\alpha)_\mathfrak{P}/K_\mathfrak{p}$ is generated over $K_\mathfrak{p}$ by an element z satisfying $z^2 = 1 + 4u_\mathfrak{p}$, where $u_\mathfrak{p} \in \mathfrak{O}_{K,\mathfrak{p}}$. So the extension $K(\alpha)/K$ is tamely ramified if and only if we can choose $a = \alpha^2$ such that for each $\mathfrak{p} \mid 2\mathfrak{O}_K$ we have $a \equiv 1 \pmod{4\mathfrak{O}_{K,\mathfrak{p}}}$. If we can choose a in this way for each prime $\mathfrak{p}$ lying above 2 then by the Chinese Remainder Theorem we can choose a such that the condition is satisfied for all such $\mathfrak{p}$ simultaneously, i.e. $a \equiv 1 \pmod^{*} 4\mathfrak{O}_K$. Finally, we can adjust a by a square of an integral element (without affecting the congruence conditions above 2) to ensure that $a \in \mathfrak{O}_K$, i.e. $a \equiv 1 \pmod{4\mathfrak{O}_K}$. □

Next we calculate explicit integral bases of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$. For primes not lying above 2 the following function will be useful:

Definition 2.2. For $x \in K^\times$ and $\mathfrak{p}$ a prime of $\mathfrak{O}_K$, define $r_\mathfrak{p}(x)$ by

$$r_\mathfrak{p}(x) = \left\lfloor \frac{v_\mathfrak{p}(x)}{2} \right\rfloor = \max\left\{ n \in \mathbb{Z} \mid n \leq \frac{v_\mathfrak{p}(x)}{2} \right\}.$$

Proposition 2.3. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which does not lie above 2, and let $\pi_\mathfrak{p}$ be a uniformiser of $\mathfrak{O}_{K,\mathfrak{p}}$. Then the following is an $\mathfrak{O}_{K,\mathfrak{p}}$ basis of $\mathfrak{O}_{L,\mathfrak{p}}$.*

$$\left\{ 1, \frac{\alpha}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a)}}, \frac{\beta}{\pi_\mathfrak{p}^{r_\mathfrak{p}(b)}}, \frac{\alpha\beta}{\pi_\mathfrak{p}^{r_\mathfrak{p}(ab)}} \right\}$$

Proof. Let z be one of $\alpha, \beta, \alpha\beta$ and consider the subextension $K(z)/K$. Let ω denote the set $\left\{1, z/\pi_\mathfrak{p}^{r_\mathfrak{p}(z^2)}\right\}$. Note that $z/\pi_\mathfrak{p}^{r_\mathfrak{p}(z^2)} \in \mathfrak{O}_{K(z),\mathfrak{p}}$ since $2r_\mathfrak{p}(z^2) \leq v_\mathfrak{p}(z^2)$. If $v_\mathfrak{p}(z^2) \equiv 0 \pmod 2$ then we may calculate explicitly $\mathfrak{d}(\omega) \in \mathfrak{O}_{K,\mathfrak{p}}^\times$, so ω is an integral basis of $\mathfrak{O}_{K(z),\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$. If $v_\mathfrak{p}(z^2) \equiv 1 \pmod 2$ then we calculate $\mathfrak{d}(\omega) = \mathfrak{p}\mathfrak{O}_{K,\mathfrak{p}}$, so $K(z)_\mathfrak{p}/K_\mathfrak{p}$ is ramified and

therefore there exists a unique prime ideal $\mathfrak{P}$ of $\mathfrak{O}_{K(z)}$ such that $\mathfrak{p}\mathfrak{O}_{K(z)} = \mathfrak{P}^2$. We may then calculate that $v_{\mathfrak{P}}\left(z/\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(z^2)}\right) = 1$, so ω comprises an element of $\mathfrak{P}$-valuation 0 and an element of $\mathfrak{P}$-valuation 1, whence ω is an integral basis for $\mathfrak{O}_{K(z),\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$. To complete the proof of the proposition we apply the above to two different subextensions $K(z), K(y)$ of L/K. We may assume that at least one of $v_{\mathfrak{p}}\left(z^2\right), v_{\mathfrak{p}}\left(y^2\right)$ is congruent to 0 modulo 2. We then have that the extensions are arithmetically disjoint at $\mathfrak{p}$, and so $\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K(y),\mathfrak{p}}\mathfrak{O}_{K(z),\mathfrak{p}}$. □

Proposition 2.4. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above 2. Then the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$.*

$$\left\{1, \left(\frac{\alpha-1}{2}\right), \left(\frac{\beta-1}{2}\right), \left(\frac{(\alpha-1)(\beta-1)}{4}\right)\right\}.$$

Proof. Consider first the subextension $K(\alpha)/K$. By [7, (24.4)] and the discussion of Galois algebras above we have that an $\mathfrak{O}_{K,\mathfrak{p}}$ basis of $\mathfrak{O}_{K(\alpha),\mathfrak{p}}$ is

$$\left\{1, \left(\frac{\alpha-1}{2}\right)\right\},$$

and the local extension $K(\alpha)_{\mathfrak{p}}/K_{\mathfrak{p}}$ is unramified, so $\mathfrak{d}\left(K(\alpha)_{\mathfrak{p}}/K_{\mathfrak{p}}\right) = \mathfrak{O}_{K,\mathfrak{p}}$. Analogous results hold for the subextension $K(\beta)/K$. Since both the subextensions $K(\alpha)/K$ and $K(\beta)/K$ are unramified at $\mathfrak{p}$, they are arithmetically disjoint at $\mathfrak{p}$, and so we obtain

$$\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K(\alpha),\mathfrak{p}}\mathfrak{O}_{K(\beta),\mathfrak{p}},$$

which yields the description of $\mathfrak{O}_{L,\mathfrak{p}}$ in the proposition. □

From these propositions we can identify those primes of $\mathfrak{O}_K$ which are ramified in $\mathfrak{O}_L$. Recall that a prime $\mathfrak{p}$ is ramified in $\mathfrak{O}_L$ if and only if it divides the discriminant $\mathfrak{d}\left(L/K\right)$, and that for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ we have $\mathfrak{d}\left(L/K\right)_{\mathfrak{p}} = \mathfrak{d}\left(L_{\mathfrak{p}}/K_{\mathfrak{p}}\right)$. Since L/K is tamely ramified and $[L:K] = 4$, any prime $\mathfrak{p}$ lying above 2 is unramified in $\mathfrak{O}_L$. For primes not lying above 2, we refer to the discriminant calculations in the proof of Proposition 2.3, and conclude that $\mathfrak{p}$ is ramified in the subextension $K(\alpha)/K$ if and only if $v_{\mathfrak{p}}\left(a\right) \equiv 1 \pmod 2$, and similarly for the subextension $K(\beta)/K$. Therefore $\mathfrak{p}$ is ramified in the extension L/K if and only if $v_{\mathfrak{p}}\left(a\right) \equiv 1 \pmod 2$ or $v_{\mathfrak{p}}\left(b\right) \equiv 1 \pmod 2$.

3. Hopf-Galois structures on tame biquadratic extensions

In this section we quote results of Byott, who enumerated all Hopf-Galois structures admitted by a biquadratic extension [3] and described the corresponding Hopf algebras [5]. These are all commutative K-Hopf algebras and so, since they are also separable K-algebras (see [15, (11.4)]), each has a unique maximal order. We determine the Wedderburn components of the

Hopf algebras giving nonclassical structures, which allows us to identify easily the unique maximal order in each Hopf algebra. Finally, we derive formulae for the action of each Hopf algebra on the extension.

Theorem 3.1 (Byott). *Let $T \leq G$ have order 2, let $d \in \{0,1\}$, and fix $\sigma, \tau \in G$ satisfying:*

$$T = \langle \tau \rangle, \quad \sigma^2 = 1, \quad G = \langle \sigma, \tau \rangle.$$

There are well defined permutations $\eta, \rho \in Perm(G)$ determined by:

$$\rho(\sigma^k \tau^l) = \sigma^k \tau^{l-1}$$
$$\eta(\sigma^k \tau^l) = \sigma^{k-1} \tau^{l+(k-1)d} \qquad \text{for } k, l \in \mathbb{Z}.$$

We have $\rho\eta = \eta\rho$ and $\rho^2 = 1$. Set $N = N_T = \langle \rho, \eta \rangle$. If $d = 0$ then $\eta^2 = 1$ and so $N \cong C_2 \times C_2$. If $d = 1$ then $\eta^2 = \rho$ and so $N \cong C_4$. In both cases N is regular on G and is normalised by $\lambda(G)$. Thus N gives rise to a Hopf-Galois structure on L/K, with Hopf algebra $H = H_T = L[N_T]^G$. If $d = 0$ then $H_T = K[G]$ regardless of the choice of T. If $d = 1$ then the 3 possible choices of T yield 3 distinct groups N, each giving rise to a nonclassical structure on L/K. These are all the Hopf-Galois structures admitted by L/K.

Proof. For the enumeration of Hopf-Galois structures, see [3, Corollary to Theorem 1, part (iii) (corrected)]. For the determination of the permtations η and ρ, see [5, Theorem 2.5] □

We shall henceforth assume that $d = 1$, and therefore consider only nonclassical Hopf-Galois structures admitted by the extension L/K. The Hopf algebras we will consider are therefore of the form $H = L[N]^G$ where $N = \langle \eta \rangle \cong C_4$ is a regular subgroup of $\mathrm{Perm}(G)$ which is normalised by $\lambda(G)$, corresponding to a choice of subgroup T of G having order 2. We note in particular that each such Hopf algebra is commutative. We will not specify a choice of T, and will therefore work with an arbitrary Hopf algebra giving a nonclassical Hopf-Galois structure on the extension.

Next we seek a more explicit description of the Hopf algebra $H = L[N]^G$. The group N has a unique subgroup of order 2, generated by η^2. The group algebra $K[\eta^2]$ has a basis of mutually orthogonal idempotents:

$$e_0 = \frac{1}{2}\left(1 + \eta^2\right), \quad e_1 = \frac{1}{2}\left(1 - \eta^2\right)$$

satisfying

$$\eta^2 e_s = (-1)^s e_s.$$

We write L^T for the subfield of L fixed by $T = \langle \tau \rangle$. Thus L^T/K is cyclic of degree 2. Fix $v \in \mathfrak{O}_L^T$ satisfying

$$\sigma(v) = -v.$$

Write $v^2 = V \in \mathfrak{O}_K$, and set

$$a_v = e_0 + ve_1 \in \mathfrak{O}_L^T[\eta^2].$$

Then we have

Proposition 3.2 (Byott). *With the above notation we have*

$$H = K[\eta^2, a_v\eta] \ .$$

Proof. See [5, Lemma 2.10]. □

Proposition 3.3. *With the above notation we have the following isomorphism of K-algebras:*

$$H \cong K^2 \times K(w),$$

where w is defined by $w^2 = -v^2 = -V$.

Proof. We make the following change of generators of $H = K[\eta^2, a_v\eta]$:

$$\{1, \eta^2, a_v\eta, \eta^2(a_v\eta)\} \mapsto \{e_0, e_1, e_0(a_v\eta), e_1(a_v\eta)\} = \omega$$

This is easily shown to be a change of basis. We shall examine properties of the basis ω. Clearly

$$(e_0(a_v\eta)^t)(e_1(a_v\eta)^{t'}) = 0$$

for any $t, t' \in \mathbb{Z}$, and so we have a decomposition $H = e_0H \times e_1H$. We note that $e_0(a_v\eta) = e_0\eta$ and form orthogonal idempotents within the K-algebra e_0H as follows:

$$\{e_0, e_0\eta\} \mapsto \left\{\frac{1}{2}(e_0 + e_0\eta), \frac{1}{2}(e_0 - e_0\eta)\right\}.$$

This implies that $e_0H \cong K^2$. Now we examine elements of the form $e_1(a_v\eta)^t$. We calculate

$$\begin{aligned}(e_1(a_v\eta))^2 &= (e_1v\eta)^2 \\ &= e_1(v\eta)^2 \\ &= e_1V\eta^2 \\ &= -e_1V \quad \text{(by definition of } e_1)\end{aligned}$$

Recall the definition of w from the statement of the proposition. If we make the identifications

$$\begin{aligned} e_1 &\mapsto 1 \\ e_1(a_v\eta) &\mapsto w, \end{aligned}$$

we see that $e_1H \cong K(w)$. This gives

$$H \cong K^2 \times K(w).$$

□

Corollary 3.4. *We have the following description of the unique maximal $\mathfrak{O}_K$-order $\mathfrak{M}_H$ in H:*

$$\mathfrak{M}_H \cong \mathfrak{O}_K^2 \times \mathfrak{O}_{K(w)}.$$

Definition 3.5. For $r = 0, 1$, we shall adopt the following notation for the idempotents defined in the proof of 3.3:

$$E_r = \frac{1}{2}\left(e_0 + (-1)^r e_0\eta\right).$$

It is possible to choose the element v such that we have $v = \alpha^i\beta^j$ for some nonnegative integers i, j, and we shall always assume that we have done so. We then have $v^2 = V \equiv 1 \pmod{4\mathfrak{O}_K}$, and so we may use the propositions of section 2 to calculate an explicit $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{M}_{H,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$.

Corollary 3.6. *If $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which does not lie above 2, then we may use Proposition 2.3 to obtain an explicit $\mathfrak{O}_{K,\mathfrak{p}}$ basis of $\mathfrak{M}_{H,\mathfrak{p}}$:*

$$\left\{E_0, E_1, e_1, \frac{e_1(a_v\eta)}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V)}}\right\}.$$

Proposition 3.7. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above 2, and write $2 = u\pi_{\mathfrak{p}}^e$ with $u \in \mathfrak{O}_{K,\mathfrak{p}}^\times$, so that $e = v_{\mathfrak{p}}(2)$. Then there exists $e/2 \leq q_{\mathfrak{p}} \leq e$ and $c_{\mathfrak{p}} \in \mathfrak{O}_{K,\mathfrak{p}}^\times$ such that the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{K(w),\mathfrak{p}}$.*

$$\left\{1, \left(\frac{c_{\mathfrak{p}}w - 1}{\pi_{\mathfrak{p}}^{q_{\mathfrak{p}}}}\right)\right\}$$

Proof. We omit the subscript $\mathfrak{p}$ and write simply c and q. We calculate that

$$w^2 = -V = 1 + u_1\pi_{\mathfrak{p}}^e$$

for some $u_1 \in \mathfrak{O}_{K,\mathfrak{p}}^\times$, and follow the proof of [7, (24.2) Case (ii)]. There exist some $c, u_c \in \mathfrak{O}_{K,\mathfrak{p}}^\times$ such that $(cw)^2 = 1 + u_c\pi_{\mathfrak{p}}^Q$ with either $Q < 2e$ and $Q \equiv 1 \pmod 2$ or $Q \geq 2e$. In the first case $K(w)_{\mathfrak{p}}/K_{\mathfrak{p}}$ is totally wildly ramified. Writing $Q = 2q + 1$ (so in particular $q < e$) the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{K(w),\mathfrak{p}}$:

$$\left\{1, \left(\frac{cw - 1}{\pi_{\mathfrak{p}}^q}\right)\right\}.$$

In the second case $K(w)_{\mathfrak{p}}/K_{\mathfrak{p}}$ is either unramified ($Q = 2e$) or not a proper extension ($Q > 2e$). Using Proposition 2.4, we have that the following is an $\mathfrak{O}_{K,\mathfrak{p}}$ basis of $\mathfrak{O}_{K(w),\mathfrak{p}}$:

$$\left\{1, \left(\frac{cw - 1}{\pi_{\mathfrak{p}}^q}\right)\right\}.$$

□

Corollary 3.8. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2. Then for $c = c_{\mathfrak{p}}$ and $q = q_{\mathfrak{p}}$ as defined above, the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{M}_{H,\mathfrak{p}}$:*

$$\left\{E_0, E_1, e_1, \frac{ce_1(a_v\eta) - e_1}{\pi_{\mathfrak{p}}^q}\right\}.$$

In addition to the notation established in the previous sections, we now fix an element $x \in \mathfrak{O}_L^{\langle\sigma\rangle}$ satisfying $\tau(x) = -x$. It is possible to choose the element x such that we have $x = \alpha^i\beta^j$ for some nonnegative integers i, j, and we shall always assume that we have done so. Then, writing $x^2 = X$, we have $X \equiv 1 \pmod{4\mathfrak{O}_K}$, and

$$L = K(x, v),$$

so to determine the action of the Hopf algebra H on L/K, we need only consider the action of each K-basis element of H on an arbitrary product x^iv^j. Recall that H has K-basis

$$\{E_0, E_1, e_1, e_1(a_v\eta)\},$$

and that the action of H on $x \in L$ is given by equation (1.1). We calculate:

$$\eta^t(\sigma^k\tau^l) = \sigma^{k-t}\tau^{l+tk-t(t+1)/2},$$

and so

$$\eta^t(\sigma^k\tau^l) = 1_G \text{ if and only if } k = t \text{ and } l = -\frac{t(t-1)}{2}.$$

Therefore we have

$$(\eta^t)^{-1}(1_G) = \sigma^t\tau^{-(t(t-1))/2}. \tag{3.1}$$

Proposition 3.9. *For $s = 0, 1$ we have*

$$e_s(x^iv^j) = \begin{cases} x^iv^j & \text{if } s = i \\ 0 & \text{otherwise} \end{cases}$$

Proof. Each $e_s \in H$, so we use equation (3.1) to calculate $e_s(x^iv^j)$.

$$\begin{aligned} e_s(x^iv^j) &= \frac{1}{2}\left(1 + (-1)^s\eta^2\right)(x^iv^j) \\ &= \frac{1}{2}\left(1 + (-1)^s\tau\right)(x^iv^j) \\ &= \frac{x^iv^j}{2}\left(1 + (-1)^{i+s}\right) \\ &= \begin{cases} x^iv^j & \text{if } s = i \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

□

Proposition 3.10. *We have*

$$(a_v\eta)(x^iv^j) = (-1)^j x^i v^{j+i}.$$

Proof. The element $(a_v\eta) \in H$, so we use equation (3.1) to calculate $(a_v\eta)(x^iv^j)$.

$$\begin{aligned}(a_v\eta)(x^iv^j) &= (e_0 + ve_1)\,(x^iv^j)\\ &= v^i\eta(x^iv^j)\\ &= \sigma(x^iv^{j+i})\\ &= (-1)^j x^i v^{j+i}\end{aligned}$$

□

Combining Proposition 3.9 and Proposition 3.10, we have:

Corollary 3.11. *For $s = 0, 1$ and $t = 0, 1$ we have*

$$e_s(a_v\eta)^t(x^iv^j) = \begin{cases} (-1)^{jt}x^iv^{j+it} & \text{if } i = s\\ 0 & \text{otherwise.}\end{cases}$$

Corollary 3.12. *For $r = 0, 1$, we have*

$$E_r(x^iv^j) = \begin{cases} v^r & \text{if } i = 0, j = r\\ 0 & \text{otherwise}\end{cases}$$

4. Local freeness

We begin this section by applying the results of [14] to establish that $\mathfrak{O}_L$ is locally free over its associated order $\mathfrak{A}_H$ in each of the nonclassical Hopf-Galois structures admitted by the extension. We then collect the detailed local information which we shall require in order to use idèles to describe the locally free class group in section 5. For each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ we calculate an explicit $\mathfrak{O}_{K,\mathfrak{p}}$-basis of the completed associated order $\mathfrak{A}_{H,\mathfrak{p}}$ and an explicit generator of $\mathfrak{O}_{L,\mathfrak{p}}$ as a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.

Proposition 4.1. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$. Then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.*

Proof. We may simply apply Corollary 1.5. More explicitly, since L/K is at most tamely ramified and has degree 4, if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ lying above 2 then $\mathfrak{p}$ is unramified in $\mathfrak{O}_L$ and we may apply Theorem 1.2. This yields that $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a Hopf order in $H_{\mathfrak{p}}$ and that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module. On the other hand, if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which is ramified in $\mathfrak{O}_L$ then $\mathfrak{p}$ cannot lie above 2, and we may apply Theorem 1.3. This yields that $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is the unique maximal $\mathfrak{O}_{K,\mathfrak{p}}$-order in $H_{\mathfrak{p}}$, which implies that $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ and that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$-module. □

Proposition 4.2. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$. An $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is given by:*

$$\begin{cases} \{1, \eta^2, 2e_0(a_v\eta), (e_1(a_v\eta) - e_0(a_v\eta))\} & \text{if } \mathfrak{p} \mid 2\mathfrak{O}_K \\ \left\{E_0, E_1, e_1, \frac{e_1(a_v\eta)}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V)}}\right\} & \text{otherwise} \end{cases}$$

Proof. If $\mathfrak{p}$ does not lie above 2 then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G = \mathfrak{M}_{H,\mathfrak{p}}$ and so we may use the $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{M}_{H,\mathfrak{p}}$ given in Proposition 3.6. If $\mathfrak{p}$ lies above 2 then we use [1, Lemma (2.1)] to calculate an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$. We must first find the orbits of G in N. The action of G on N is by conjugation via the embedding λ. We calculate ${}^{\tau}\eta = \eta$ and ${}^{\sigma}\eta = \eta^3$, so the orbits of G in N are

$$\{1\}, \{\eta^2\}, \{\eta, \eta^3\}.$$

The orbits $\{1\}$ and $\{\eta^2\}$ both have stabiliser G, so [1, Lemma (2.1)] implies that $1, \eta^2$ are two of the $\mathfrak{O}_{K,\mathfrak{p}}$-basis elements of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$. The orbit $\{\eta, \eta^3\}$ has stabiliser $T = \langle\tau\rangle$. Following [1, Lemma (2.1)], we consider the quadratic extension L^T/K. Using Proposition 2.4, an integral basis of $L_{\mathfrak{p}}^T/K_{\mathfrak{p}}$ is given by

$$\left\{1, \frac{v-1}{2}\right\},$$

and so the remaining two $\mathfrak{O}_{K,\mathfrak{p}}$-basis elements of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ are given by

$$\eta + \eta^3 = 2e_0\eta$$

and

$$\begin{aligned} \frac{v-1}{2}\eta + \frac{-v-1}{2}\eta^3 &= \frac{v}{2}\left(\eta - \eta^3\right) - \frac{1}{2}\left(\eta + \eta^3\right) \\ &= e_1(a_v\eta) - e_0(a_v\eta), \end{aligned}$$

giving the description of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ in proposition. □

In the next section we will be particularly interested in the group of units $\mathfrak{A}_{H,\mathfrak{p}}^{\times} = \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^{\times}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$. If $\mathfrak{p}$ does not lie above 2 then by Proposition 4.2 we have

$$\left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^{\times} = \mathfrak{M}_{H,\mathfrak{p}}^{\times} \cong (\mathfrak{O}_{K,\mathfrak{p}}^{\times})^2 \times \mathfrak{O}_{K(w),\mathfrak{p}}^{\times}.$$

To determine $\left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^{\times}$ when $\mathfrak{p}$ lies above 2 we use the following proposition:

Proposition 4.3. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2. Then the associated order $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a local ring. Denote by $\mathfrak{a}$ the ideal $\mathfrak{p}\mathfrak{O}_{L,\mathfrak{p}}[N] + \ker\varepsilon$ of $\mathfrak{O}_{L,\mathfrak{p}}[N]$. Then $\mathfrak{a}^G$ is the unique maximal ideal of $\mathfrak{A}_{H,\mathfrak{p}}$.*

Proof. Note first that $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a finitely generated module over the complete discrete valuation ring $\mathfrak{O}_{K,\mathfrak{p}}$, so it is sufficient to show that $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ contains no nontrivial idempotents. We have an isomorphism

$$\mathfrak{O}_{L,\mathfrak{p}}[N] \cong \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_{L,\mathfrak{P}}[N],$$

and the G-action on each side yields

$$\mathfrak{O}_{L,\mathfrak{p}}[N]^G \cong \left(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_{L,\mathfrak{P}}[N] \right)^G.$$

Now each $\mathfrak{O}_{L,\mathfrak{P}}$ is a discrete valuation ring with residue field of characteristic 2, and $|N| = 4$, so each $\mathfrak{O}_{L,\mathfrak{P}}[N]$ is a local ring, and therefore has no nontrivial idempotents by ([8, (5.25)]). The first part of the result follows since by ([13, Chapter I, §9]) G permutes transitively the primes $\mathfrak{P}$ which lie above $\mathfrak{p}$ and so the components of the product above. For the second part, we consider the injection

$$\frac{\mathfrak{O}_{L,\mathfrak{p}}[N]^G}{\mathfrak{a}^G} \hookrightarrow \frac{\mathfrak{O}_{L,\mathfrak{p}}[N]}{\mathfrak{a}}$$

defined by

$$[z] = z + \mathfrak{a}^G \mapsto z + \mathfrak{a},$$

and the isomorphisms

$$\frac{\mathfrak{O}_{L,\mathfrak{p}}[N]}{\mathfrak{a}} \cong \prod_{\mathfrak{P}|\mathfrak{p}} \frac{\mathfrak{O}_{L,\mathfrak{P}}}{\mathfrak{P}} \cong \frac{\mathfrak{O}_{L,\mathfrak{p}}}{\mathfrak{p}}.$$

We have that $[z]$ corresponds to an element of $\mathfrak{O}_{L,\mathfrak{p}}/\mathfrak{p}$, but is also fixed by all $g \in G$, so in fact $[z]$ corresponds to an element of $\mathfrak{O}_{K,\mathfrak{p}}/\mathfrak{p}$, and we have

$$\frac{\mathfrak{O}_{L,\mathfrak{p}}[N]^G}{\mathfrak{a}^G} \cong \mathfrak{O}_{K,\mathfrak{p}}/\mathfrak{p}.$$

Therefore $\mathfrak{a}^G$ is a maximal ideal since $\mathfrak{O}_{K,\mathfrak{p}}/\mathfrak{p}$ is a field, and is unique since $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a local ring. □

Corollary 4.4. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2, and let $z \in \mathfrak{O}_{L,\mathfrak{p}}[N]^G$. Then $z \in (\mathfrak{O}_{L,\mathfrak{p}}[N]^G)^\times$ if and only if $\varepsilon(z) \in \mathfrak{O}_{K,\mathfrak{p}}^\times$.*

Finally, we calculate explicit generators of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$:

Proposition 4.5. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above 2. Then a generator for $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module is:*

$$\gamma_{\mathfrak{p}} = \frac{1}{4}(1 + v + x + xv).$$

Proof. By [14, Proposition 5.3] we have that $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a Hopf order and by Proposition 4.3 above it is a local ring. We observe that the trace element

$$\theta = \sum_{n \in N} n$$

is a left integral of $\mathfrak{A}_{H,\mathfrak{p}}$ (see [7, §3]). Therefore by [7, (14.7)] sufficient conditions for $\gamma_{\mathfrak{p}}$ to be a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ are that $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$ and $\theta(\gamma_{\mathfrak{p}}) = 1$. For the first, we recall the $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$ given in Proposition 2.4 and calculate:

$$\gamma_{\mathfrak{p}} = \frac{(x-1)(v-1)}{4} + \frac{x-1}{2} + \frac{v-1}{2} + 1,$$

so $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$. It is straightforward to verify that $\theta(\gamma_{\mathfrak{p}}) = \mathrm{Tr}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(\gamma_{\mathfrak{p}}) = 1$. □

Proposition 4.6. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which does not lie above 2. Define $j_{\mathfrak{p}} \in \{0,1\}$ by*

$$j_{\mathfrak{p}} = \begin{cases} 1 & \text{if } v_{\mathfrak{p}}(X) \equiv v_{\mathfrak{p}}(V) \equiv 1 \pmod 2 \\ 0 & \text{otherwise} \end{cases}$$

Then a generator for $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module is:

$$\gamma_{\mathfrak{p}} = 1 + \frac{v}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V)}} + \frac{xv^{j_{\mathfrak{p}}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}})}}.$$

Proof. Since $\mathfrak{O}_{L,\mathfrak{p}}$ and $\mathfrak{A}_{H,\mathfrak{p}}$ are both free $\mathfrak{O}_{K,\mathfrak{p}}$-modules of rank 4, it suffices to show that the images of $\gamma_{\mathfrak{p}}$ under the $\mathfrak{O}_{K,\mathfrak{p}}$-basis elements of $\mathfrak{A}_{H,\mathfrak{p}}$ form an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$. We note that we have $\mathfrak{O}_{L,\mathfrak{p}} = e_0\mathfrak{O}_{L,\mathfrak{p}} \bigoplus e_1\mathfrak{O}_{L,\mathfrak{p}}$. Using Proposition 2.3 we have that an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$ is given by

$$\left\{ 1, \frac{v}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V)}}, \frac{x}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X)}}, \frac{xv}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(XV)}} \right\}$$

We also have from Proposition 4.1 that $\mathfrak{O}_{L,\mathfrak{p}}$ admits the maximal order $\mathfrak{M}_{H,\mathfrak{p}}$, which by Proposition 3.6 has $\mathfrak{O}_{K,\mathfrak{p}}$-basis

$$\left\{ E_0, E_1, e_1, \frac{e_1(a_v\eta)}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V)}} \right\}.$$

Now for $r = 0, 1$, we have by Corollary 3.12 that

$$E_r\gamma_{\mathfrak{p}} = \frac{v^r}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^r)}},$$

so $\{E_0\gamma_\mathfrak{p}, E_1\gamma_\mathfrak{p}\}$ is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $e_0\mathfrak{O}_{L,\mathfrak{p}}$. We now consider $e_1\mathfrak{O}_{L,\mathfrak{p}}$. For $t = 0, 1$ we have by Corollary 3.11 that

$$\begin{aligned}\frac{e_1(a_v\eta)^t}{\pi_\mathfrak{p}^{r_\mathfrak{p}(V^t)}}\gamma_\mathfrak{p} &= \frac{e_1(a_v\eta)^t}{\pi_\mathfrak{p}^{r_\mathfrak{p}(V^t)}}\frac{xv^{j_\mathfrak{p}}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(XV^{j_\mathfrak{p}})}}\\ &= \frac{(-1)^{j_\mathfrak{p}t}xv^{j_\mathfrak{p}+t}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(V^t)}\pi_\mathfrak{p}^{r_\mathfrak{p}(XV^{j_\mathfrak{p}})}}\\ &= \frac{(-1)^{j_\mathfrak{p}t}xv^{j_\mathfrak{p}+t}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(XV^{j_\mathfrak{p}+t})}}\end{aligned}$$

the final equality holding since by the choice of $j_\mathfrak{p}$ we have

$$r_\mathfrak{p}(XV^{j_\mathfrak{p}}) + r_\mathfrak{p}(V^t) = r_\mathfrak{p}(XV^{j_\mathfrak{p}+t}).$$

So $\{e_1\gamma_\mathfrak{p}, e_1(a_v\eta)\gamma_\mathfrak{p}\}$ is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $e_1\mathfrak{O}_{L,\mathfrak{p}}$. Together with the basis of $e_0\mathfrak{O}_{L,\mathfrak{p}}$, we have an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$. □

5. Conditions for global freeness

Having established that $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$ in all of the nonclassical Hopf-Galois structures admitted by the extension L/K, we now seek conditions for global freeness. For each Hopf algebra H giving a nonclassical Hopf-Galois structure on the extension, $\mathfrak{O}_L$ determines a class in the locally free class group $\mathrm{Cl}\,(\mathfrak{A}_H)$, and since the Hopf algebras giving Hopf-Galois structures on L/K are all commutative, $\mathfrak{O}_L$ is free over an associated order $\mathfrak{A}_H$ if and only if this class is trivial (see [9, §51]). We shall describe $\mathrm{Cl}\,(\mathfrak{A}_H)$ in terms of idèles. We recall the definitions of the idèle group of H:

$$\mathbb{J}(H) = \prod_{\mathfrak{p}\lhd\mathfrak{O}_K}{}' H_\mathfrak{p}^\times = \left\{(h_\mathfrak{p})_\mathfrak{p} \mid h_\mathfrak{p} \in H_\mathfrak{p}^\times, h_\mathfrak{p} \in \mathfrak{A}_{H,\mathfrak{p}}^\times \text{ for almost all } \mathfrak{p}\right\},$$

and the group of unit idèles:

$$\mathbb{U}(\mathfrak{A}_H) = \prod_{\mathfrak{p}\lhd\mathfrak{O}_K} \mathfrak{A}_{H,\mathfrak{p}}^\times = \left\{(h_\mathfrak{p})_\mathfrak{p} \in \mathbb{J}(H) \mid h_\mathfrak{p} \in \mathfrak{A}_{H,\mathfrak{p}}^\times \text{ for all } \mathfrak{p}\right\}.$$

In each case, the product is taken over all primes $\mathfrak{p}$ of $\mathfrak{O}_K$. Since H is commutative, we have the following isomorphism ([9, Theorem (49.22)]):

$$\mathrm{Cl}\,(\mathfrak{A}_H) \cong \frac{\mathbb{J}(H)}{H^\times\mathbb{U}(\mathfrak{A}_H)}.$$

By Proposition 3.3 we have $\mathbb{J}(H) \cong \mathbb{J}(K)^2 \times \mathbb{J}(K(w))$ and $H^\times \cong (K^\times)^2 \times K(w)^\times$. It remains to describe the group

$$\mathbb{U}(\mathfrak{A}_H) = \prod_{\mathfrak{p}\lhd\mathfrak{O}_K} \mathfrak{A}_{H,\mathfrak{p}}^\times.$$

If $\mathfrak{p} \nmid 2\mathfrak{O}_K$ then from Proposition 4.2 we have that $\mathfrak{A}_{H,\mathfrak{p}}^{\times} = \mathfrak{M}_{H,\mathfrak{p}}^{\times} \cong (\mathfrak{O}_{K,\mathfrak{p}}^{\times})^2 \times \mathfrak{O}_{K(w),\mathfrak{p}}^{\times}$. If $\mathfrak{p} \mid 2\mathfrak{O}_K$ then we have that $\mathfrak{A}_{H,\mathfrak{p}}^{\times} = \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^{\times}$. In the following proposition we express z in terms of the $\mathfrak{O}_{K,\mathfrak{p}}$-basis elements of the maximal order $\mathfrak{M}_{H,\mathfrak{p}}$ and derive congruence conditions on the coefficients which are equivalent to $z \in \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^{\times}$.

Proposition 5.1. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above 2, and write $2 = u\pi_{\mathfrak{p}}^e \in \mathfrak{O}_{K,\mathfrak{p}}$, with $u \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. Let $z \in \mathfrak{M}_{H,\mathfrak{p}}$ and write*

$$z = a_0E_0 + a_1E_1 + a_{1,0}e_1 + a_{1,1}\frac{ce_1(a_v\eta) - e_1}{\pi_{\mathfrak{p}}^q}$$

with $a_0, a_1, a_{1,0}, a_{1,1} \in \mathfrak{O}_{K,\mathfrak{p}}$ and c, q as in Proposition 3.7. Then $z \in \mathfrak{A}_{H,\mathfrak{p}}^{\times}$ if and only if

i) $a_{1,1} \equiv 0 \pmod{\pi_{\mathfrak{p}}^q}$
ii) $a_0 - a_1 + 2\pi_{\mathfrak{p}}^{-q}ca_{1,1} \equiv 0 \pmod 4$
iii) $a_0 + a_1 - 2a_{1,0} + 2\pi_{\mathfrak{p}}^{-q}a_{1,1} \equiv 0 \pmod 4$
iv) $a_0 + a_1 + 2a_{1,0} - 2\pi_{\mathfrak{p}}^{-q}a_{1,1} \equiv 0 \pmod 4$
v) $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$

Proof. We rewrite z in terms of the basis elements of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ given in Proposition 4.2. By Corollary 4.4, we then have that $z \in \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^{\times}$ if and only if the coefficients of these basis elements lie in $\mathfrak{O}_{K,\mathfrak{p}}$ and $\varepsilon(z) \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. The details of the proof are routine. □

Our next aim is to "sandwich" the locally free class group $\mathrm{Cl}\,(\mathfrak{A}_H)$ between products of ray class groups whose conductors are ideals divisible only by primes lying above 2. For these primes we therefore seek necessary and sufficient conditions for $z \in \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^{\times}$ in terms of higher unit groups of $\mathfrak{O}_{K,\mathfrak{p}}$ and $\mathfrak{O}_{K(w),\mathfrak{p}}$.

Definition 5.2. Define an isomorphism

$$\Theta : (K^{\times})^2 \times K(w)^{\times} \cong H^{\times}$$

by composing the automorphism of $(K^{\times})^2 \times K(w)^{\times}$ defined by

$$(z_0, z_1, y_0) \mapsto (z_0, z_0z_1, z_0y_0)$$

with the isomorphism $K^2 \times K(w) \cong H$ defined in Proposition 3.3. We shall also write Θ for the induced isomorphism $(K_{\mathfrak{p}}^{\times})^2 \times (K(w)_{\mathfrak{p}})^{\times} \cong H_{\mathfrak{p}}^{\times}$, where $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$, and the isomorphism $\mathbb{J}(K)^2 \times \mathbb{J}(K(w)) \cong \mathbb{J}(H)$.

Proposition 5.3. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2. Then*

$$\Theta\left(\mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + 4\mathfrak{O}_{K,\mathfrak{p}}) \times (1 + 4\mathfrak{O}_{K(w),\mathfrak{p}})\right) \subseteq \mathfrak{A}_{H,\mathfrak{p}}^{\times},$$

Proof. The image under Θ of an element of

$$\mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + 4\mathfrak{O}_{K,\mathfrak{p}}) \times (1 + 4\mathfrak{O}_{K(w),\mathfrak{p}})$$

has the form

$$z = a_0 E_0 + a_1 E_1 + a_{1,0} e_1 + a_{1,1} \frac{ce_1(a_v \eta) - e_1}{\pi_{\mathfrak{p}}^q}$$

with $a_0, a_1, a_{1,0}, a_{1,1} \in \mathfrak{O}_{K,\mathfrak{p}}$ and

a) $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$
b) $a_1 \equiv a_0 \pmod{4\mathfrak{O}_{K,\mathfrak{p}}}$
c) $a_{1,0} \equiv a_0 \pmod{4\mathfrak{O}_{K,\mathfrak{p}}}$
d) $a_{1,1} \equiv 0 \pmod{4\mathfrak{O}_{K,\mathfrak{p}}}$

It is easily verified that these congruences imply those in Proposition 5.1. □

Proposition 5.4. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2, and let $e_{\mathfrak{p}} = v_{\mathfrak{p}}(2)$. Then*

$$\Theta^{-1}\left(\mathfrak{A}_{H,\mathfrak{p}}^{\times}\right) \subseteq \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + 2\mathfrak{O}_{K,\mathfrak{p}}) \times (1 + \pi_{\mathfrak{p}}^{\left\lceil \frac{e_{\mathfrak{p}}}{2} \right\rceil} \mathfrak{O}_{K(w),\mathfrak{p}}),$$

where

$$\left\lceil \frac{e_{\mathfrak{p}}}{2} \right\rceil = \min\left\{ n \in \mathbb{Z} \mid n \geq \frac{e_{\mathfrak{p}}}{2} \right\}.$$

Proof. Let

$$z = a_0 E_0 + a_1 E_1 + a_{1,0} e_1 + a_{1,1} \frac{ce_1(a_v \eta) - e_1}{\pi_{\mathfrak{p}}^q}$$

with $a_0, a_1, a_{1,0}, a_{1,1} \in \mathfrak{O}_{K,\mathfrak{p}}$, and suppose that $z \in \mathfrak{A}_{H,\mathfrak{p}}^{\times}$. In particular, $a_0, a_1, a_{1,0}$ and $a_{1,1}$ satisfy conditions (i)-(v) of Proposition 5.1. We shall show that this implies

$$\Theta^{-1}(z) \in \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + 2\mathfrak{O}_{K,\mathfrak{p}}) \times (1 + \pi_{\mathfrak{p}}^{\left\lceil \frac{e_{\mathfrak{p}}}{2} \right\rceil} \mathfrak{O}_{K(w),\mathfrak{p}}).$$

Adding (iii) and (iv) yields $2a_0 + 2a_1 \equiv 0 \pmod 4$, which implies that $a_0 \equiv a_1 \pmod 2$. Adding (ii) and (iii) yields

$$2a_0 - 2a_{1,0} + 2(c+1)\pi_{\mathfrak{p}}^{-q} a_{1,1} \equiv 0 \pmod 4,$$

which implies that

$$a_0 - a_{1,0} + (c+1)\pi_{\mathfrak{p}}^{-q} a_{1,1} \equiv 0 \pmod 2.$$

Now $\pi_{\mathfrak{p}}^{-q} a_{1,1} \in \mathfrak{O}_{K,\mathfrak{p}}$ by (i), and by examining the proof of Proposition 3.7 we see that $v_{\mathfrak{p}}(c+1) \geq \left\lceil \frac{e_{\mathfrak{p}}}{2} \right\rceil$, so we obtain $a_{1,0} \equiv a_0 \pmod{\pi_{\mathfrak{p}}^{\left\lceil \frac{e_{\mathfrak{p}}}{2} \right\rceil}}$. Since we also have from (i) that $a_{1,1} \equiv 0 \pmod{\pi_{\mathfrak{p}}^q}$ and from (v) that $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$, the result follows. □

Combining Proposition 5.3 and Proposition 5.4, we can now "sandwich" the locally free class group $\mathrm{Cl}\,(\mathfrak{A}_H)$:

Corollary 5.5. *Define an ideal* $\mathfrak{e}$ *of* $\mathfrak{O}_K$ *by*

$$\mathfrak{e} = \prod_{\mathfrak{p}|2\mathfrak{O}_K} \mathfrak{p}^{\left\lceil \frac{e_\mathfrak{p}}{2} \right\rceil},$$

where $e_\mathfrak{p} = v_\mathfrak{p}(2)$. *Then there are injections:*

$$\begin{array}{ccccc} \mathbb{U}(\mathfrak{O}_K) & \times & \mathbb{U}_4(\mathfrak{O}_K) & \times & \mathbb{U}_4(\mathfrak{O}_{K(w)}) \\ & & \downarrow & & \\ & & \mathbb{U}(\mathfrak{A}_H) & & \\ & & \downarrow & & \\ \mathbb{U}(\mathfrak{O}_K) & \times & \mathbb{U}_2(\mathfrak{O}_K) & \times & \mathbb{U}_\mathfrak{e}(\mathfrak{O}_{K(w)}) \end{array}$$

and therefore surjections:

$$\begin{array}{ccccc} Cl\,(\mathfrak{O}_K) & \times & Cl_4(\mathfrak{O}_K) & \times & Cl_4(\mathfrak{O}_{K(w)}) \\ & & \downarrow & & \\ & & Cl\,(\mathfrak{A}_H) & & \\ & & \downarrow & & \\ Cl\,(\mathfrak{O}_K) & \times & Cl_2(\mathfrak{O}_K) & \times & Cl_\mathfrak{e}(\mathfrak{O}_{K(w)}) \end{array}$$

Next we turn to the idèle whose class in $\mathbb{J}(H)/H^\times\mathbb{U}(\mathfrak{A}_H)$ corresponds to the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$. We construct this idèle as follows: Let Γ be a generator of L over H - such a generator exists by the Hopf-Galois analogue of the normal basis theorem (see [7, (2.16)]). Then for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ let $\gamma_\mathfrak{p}$ be a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$, and define $h_\mathfrak{p} \in H_\mathfrak{p}$ by $h_\mathfrak{p}\Gamma = \gamma_\mathfrak{p}$. Then the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$ corresponds to the class of the idèle $(h_\mathfrak{p})_\mathfrak{p}$ in the quotient above. We also interpret this class as a triple of fractional ideals so that we can use Proposition 5.5 to determine whether $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$.

Proposition 5.6. *The class of* $\mathfrak{O}_L$ *in the locally free class group*

$$Cl\,(\mathfrak{A}_H) \cong \frac{\mathbb{J}(H)}{H^\times\mathbb{U}(\mathfrak{A}_H)}$$

corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$*, where* $h_{\mathfrak{p}}$ *is defined by*

$$h_{\mathfrak{p}} = \begin{cases} E_0 + E_1 + e_1 + e_1(a_v\eta) & \text{if } \mathfrak{p} \mid 2\mathfrak{O}_K \\ E_0 + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)} E_1 + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}})} e_1(a_v\eta)^{j_{\mathfrak{p}}} & \text{if } \mathfrak{p} \mid XV\mathfrak{O}_K \\ 1 & \text{otherwise} \end{cases}$$

and where (see Proposition 4.6):

$$j_{\mathfrak{p}} = \begin{cases} 1 & \text{if } v_{\mathfrak{p}}(X) \equiv v_{\mathfrak{p}}(V) \equiv 1 \pmod 2 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Define

$$\Gamma = \frac{1}{4}(1 + v + x).$$

Using the formulae for the action of the K-basis elements of H on those of L in Corollary 3.11 and Corollary 3.12, we see that Γ is a generator of L over H. To show that the class of $\mathfrak{O}_L$ in $\mathrm{Cl}(\mathfrak{A}_H)$ corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ in $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$ we must show that for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$, the element $h_{\mathfrak{p}}\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. We recall the local generators $\gamma_{\mathfrak{p}}$ given in Proposition 4.5 and Proposition 4.6:

$$\gamma_{\mathfrak{p}} = \begin{cases} \frac{1}{4}(1 + x + v + xv) & \text{if } \mathfrak{p} \mid 2\mathfrak{O}_K \\ 1 + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)} v + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}})} xv^{j_{\mathfrak{p}}} & \text{otherwise} \end{cases}$$

Suppose first that $\mathfrak{p} \nmid 2XV\mathfrak{O}_K$. Then $h_{\mathfrak{p}} = 1$ and so

$$h_{\mathfrak{p}}\Gamma = \frac{1}{4}(1 + v + x),$$

whereas by Proposition 4.5

$$\gamma_{\mathfrak{p}} = 1 + v + x.$$

We note that $\mathfrak{p} \nmid 2\mathfrak{O}_K$ and so $4 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. Therefore we have that $h_{\mathfrak{p}}\Gamma$ and $\gamma_{\mathfrak{p}}$ differ only by an element of $\mathfrak{O}_{K,\mathfrak{p}}^{\times}$, and so $h_{\mathfrak{p}}\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. Next suppose that $\mathfrak{p} \mid XV\mathfrak{O}_K$. Then

$$\begin{aligned} h_{\mathfrak{p}}\Gamma &= E_0\Gamma + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)} E_1\Gamma + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}})} e_1(a_v\eta)^{j_{\mathfrak{p}}}\Gamma \\ &= \frac{1}{4}\left(1 + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)} v + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}})} xv^{j_{\mathfrak{p}}}\right) \end{aligned}$$

whereas by Proposition 4.5

$$\gamma_{\mathfrak{p}} = 1 + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)} v + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}})} xv^{j_{\mathfrak{p}}}.$$

Again, since $\mathfrak{p} \nmid 2\mathfrak{O}_K$ we have that $4 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. Therefore $h_{\mathfrak{p}}\Gamma$ and $\gamma_{\mathfrak{p}}$ differ only by an element of $\mathfrak{O}_{K,\mathfrak{p}}^{\times}$, and so $h_{\mathfrak{p}}\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$.

Finally suppose that $\mathfrak{p} \mid 2\mathfrak{O}_K$. Then

$$\begin{aligned} h_{\mathfrak{p}}\Gamma &= E_0\Gamma + E_1\Gamma + e_1\Gamma + e_1(a_v\eta)\Gamma \\ &= \frac{1}{4}(1 + v + x + xv) \\ &= \gamma_{\mathfrak{p}} \end{aligned}$$

So in this case $h_{\mathfrak{p}}\Gamma$ coincides with the generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ given in Proposition 4.5. This completes the proof. □

Definition 5.7. For $y \in K$, define the fractional ideal

$$I_y = \prod_{\mathfrak{p} \mid y\mathfrak{O}_K} \mathfrak{p}^{r_{\mathfrak{p}}(y)}.$$

Proposition 5.8. *Under the composition of maps*

$$\mathbb{J}(H) \to \mathbb{J}(K)^2 \times \mathbb{J}(K(w)) \to Cl(\mathfrak{O}_K) \times Cl_4(\mathfrak{O}_K) \times Cl_4(\mathfrak{O}_{K(w)}),$$

the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ *is mapped to the triple of classes of fractional ideals*

$$\left(\mathfrak{O}_K, I_V^{-1}, \left(I_X^{-1} \prod_{\substack{\mathfrak{P} \mid (1+w) \\ \mathfrak{P} \nmid 2\mathfrak{O}_{K(w)}}} \mathfrak{P}^{-v_{\mathfrak{P}}(1+w)} \prod_{\substack{v_{\mathfrak{p}}(V) \equiv 1 \pmod 2 \\ v_{\mathfrak{p}}(X) \equiv 1 \pmod 2 \\ \mathfrak{P} \mid \mathfrak{p}\mathfrak{O}_{K(w)}}} \mathfrak{P}^{-1} \right) \right).$$

Proof. Under the isomorphism

$$\Theta^{-1} : \mathbb{J}(H) \cong \mathbb{J}(K)^2 \times \mathbb{J}(K(w))$$

the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ is mapped to the triple of idèles

$$\left((1)_{\mathfrak{p}}, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)} \right)_{\mathfrak{p}}, (y_{\mathfrak{p}})_{\mathfrak{p}} \right),$$

where

$$y_{\mathfrak{p}} = \begin{cases} 1 + w & \mathfrak{p} \mid 2\mathfrak{O}_K \\ \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(XV)} w & v_{\mathfrak{p}}(X) \equiv v_{\mathfrak{p}}(V) \equiv 1 \pmod 2 \\ \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X)} & \text{otherwise.} \end{cases}$$

since by definition we have $j_{\mathfrak{p}} = 1$ if $v_{\mathfrak{p}}(X) \equiv v_{\mathfrak{p}}(V) \equiv 1 \pmod 2$ and $j_{\mathfrak{p}} = 0$ otherwise. If $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ then for each prime $\mathfrak{P}$ of $\mathfrak{O}_{K(w)}$ lying above $\mathfrak{p}$ we obtain from $y_{\mathfrak{p}}$ elements $y_{\mathfrak{P}} \in K(w)_{\mathfrak{P}}$ as follows: If $\mathfrak{P}$ is the only prime of $\mathfrak{O}_{K(w)}$ lying above $\mathfrak{p}$ then $y_{\mathfrak{P}} = y_{\mathfrak{p}}$. If two primes of $\mathfrak{O}_{K(w)}$ lie above $\mathfrak{p}$ then we label one of them $\mathfrak{P}$; the other is then $\delta\mathfrak{P}$, where δ is a generator for the Galois group of $K(w)/K$. We then set $y_{\mathfrak{P}} = y_{\mathfrak{p}}$ and $y_{\delta\mathfrak{P}} = \delta y_{\mathfrak{p}}$. Thus the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ corresponds to the triple of idèles

$$\left((1)_{\mathfrak{p}}, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)} \right)_{\mathfrak{p}}, \left((1+w) y'_{\mathfrak{P}} \right)_{\mathfrak{P}} \right),$$

where

$$y'_{\mathfrak{P}} = \begin{cases} 1 & \mathfrak{P} \mid 2\mathfrak{O}_{K(w)} \\ (1+w)^{-1}\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X)} & \mathfrak{P} \mid (1+w)\mathfrak{O}_{K(w)}, \mathfrak{P} \nmid 2\mathfrak{O}_{K(w)} \\ \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(XV)} w & v_{\mathfrak{p}}(X) \equiv v_{\mathfrak{p}}(V) \equiv 1 \pmod 2 \text{ and } \mathfrak{P} \mid \mathfrak{p} \\ \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X)} & \text{otherwise} \end{cases}$$

Since $(1+w) \in K(w)^{\times}$, this triple of idèles has the same class in the product $\mathrm{Cl}(\mathfrak{O}_K) \times \mathrm{Cl}_4(\mathfrak{O}_K) \times \mathrm{Cl}_4(\mathfrak{O}_{K(w)})$ as the triple of idèles

$$\left((1)_{\mathfrak{p}}, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)}\right)_{\mathfrak{p}}, \left(y'_{\mathfrak{P}}\right)_{\mathfrak{P}}\right).$$

We now map this triple of idèles to a triple of fractional ideals. We see immediately that the first component corresponds to the trivial ideal, and that the second component corresponds to the fractional ideal I_V^{-1}. In the third component we calculate:

$$v_{\mathfrak{P}}\left(y'_{\mathfrak{P}}\right) = \begin{cases} 0 & \mathfrak{P} \mid 2\mathfrak{O}_{K(w)} \\ -v_{\mathfrak{P}}(1+w) - v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X)}\right) & \mathfrak{P} \mid (1+w)\mathfrak{O}_{K(w)}, \mathfrak{P} \nmid 2\mathfrak{O}_{K(w)} \\ -v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X)}\right) - 1 & \begin{cases} v_{\mathfrak{p}}(X) \equiv v_{\mathfrak{p}}(V) \equiv 1 \pmod 2 \\ \text{and } \mathfrak{P} \mid \mathfrak{p} \end{cases} \\ -v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X)}\right) & \text{otherwise} \end{cases}$$

since if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which does not lie above 2 and $\mathfrak{P}$ is a prime of $\mathfrak{O}_{K(w)}$ lying above $\mathfrak{p}$ then $v_{\mathfrak{P}}(w) = v_{\mathfrak{p}}(V)$. Therefore this component corresponds to the fractional ideal

$$\left(I_X^{-1} \prod_{\substack{\mathfrak{P} \mid (1+w)\mathfrak{O}_{K(w)} \\ \mathfrak{P} \nmid 2\mathfrak{O}_{K(w)}}} \mathfrak{P}^{-v_{\mathfrak{P}}(1+w)} \prod_{\substack{v_{\mathfrak{p}}(V) \equiv 1 \pmod 2 \\ v_{\mathfrak{p}}(X) \equiv 1 \pmod 2 \\ \mathfrak{P} \mid \mathfrak{p}\mathfrak{O}_{K(w)}}} \mathfrak{P}^{-1} \right).$$

□

Proposition 5.9. *A sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$ is that the triple of fractional ideals given in Proposition 5.8 has trival class in the product of ray class groups*

$$Cl(\mathfrak{O}_K) \times Cl_4(\mathfrak{O}_K) \times Cl_4(\mathfrak{O}_{K(w)}).$$

A necessary condition is that the same triple has trivial class in the product of ray class groups

$$Cl(\mathfrak{O}_K) \times Cl_2(\mathfrak{O}_K) \times Cl_4(\mathfrak{O}_{K(w)}).$$

Proof. By Proposition 5.6, the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$ corresponds to the class of the idèle $(h_\mathfrak{p})_\mathfrak{p}$ in $\mathbb{J}(H)/H^\times\mathbb{U}(\mathfrak{A}_H)$. Recalling the surjections of Corollary 5.5, the result follows. □

If we make additional assumptions about the ray class numbers $h_4(K)$ and $h_4(K(v))$ then we can obtain a more precise result:

Proposition 5.10. *Let K be a number field such that $h_4(K)$ is odd. Define an ideal $\mathfrak{t}$ of $\mathfrak{O}_K$ by*

$$\mathfrak{t} = \prod_{\mathfrak{p}|2\mathfrak{O}_K} \mathfrak{p}.$$

Then

$$Cl_4(\mathfrak{O}_K) \cong Cl_\mathfrak{t}(\mathfrak{O}_K).$$

Proof. This proposition differs only slightly from [2, Lemma 4.1]. □

Corollary 5.11. *Suppose that $h_4(K)$ and $h_4(K(w))$ are both odd. Then*

$$Cl(\mathfrak{A}_H) \cong Cl(\mathfrak{O}_K) \times Cl_2(\mathfrak{O}_K) \times Cl_\mathfrak{t}(\mathfrak{O}_{K(w)}),$$

and so $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ if and only if the triple of fractional ideals given in Proposition 5.8 has trival class in this product of ray class groups.

6. Extensions of $\mathbb{Q}$

In this section we take $K = \mathbb{Q}$. A tame biquadratic extension L of $\mathbb{Q}$ has the form $L = \mathbb{Q}(\alpha, \beta)$, where $\alpha^2 = a, \beta^2 = b$ and a, b are squarefree integers both congruent to 1 modulo 4 whose images in the $\mathbb{F}_2$-vector space $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ are linearly independent. We recall the results of section 2 describing the 3 nonclassical Hopf-Galois structures admitted by the extension, and retain the notation of that section. We note in particular that we are free to replace the element x by $xv/\gcd(X, V)$ (corresponding to replacing the element $\sigma \in G$ by $\sigma\tau$); this does not affect the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$. We may assume without loss of generality that $x^2 = X$ and $v^2 = V$ are squarefree integers.

Let H be a Hopf algebra giving a nonclassical Hopf-Galois structure on $L/\mathbb{Q}$. By Proposition 3.3 we have the following isomorphism of $\mathbb{Q}$-algebras:

$$H \cong \mathbb{Q}^2 \times \mathbb{Q}(w),$$

where $w^2 = -V$. We shall write $F = \mathbb{Q}(w)$. Since $V \equiv 1 \pmod 4$, we have $-V \equiv -1 \pmod 4$. Thus $\mathfrak{d}\,(F) = -4V$, and so $F/\mathbb{Q}$ is wildly ramified at 2. Also $\mathfrak{O}_F = \mathbb{Z}[w]$.

Proposition 6.1. *A necessary condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$ is that there exist integers m_0, m_1 satisfying*

$$m_0^2 + Vm_1^2 = \pm 2\gcd(X, V). \tag{6.1}$$

A sufficient condition is that there exist integers $m_0 \equiv m_1 \equiv 1 \pmod 8$ *satisfying (6.1).*

Proof. Recall from Definition 5.7 that for $y \in \mathbb{Q}$ we define the fractional ideal I_y by

$$I_y = \prod_{p|y} p^{r_p(y)}.$$

Since X, V are squarefree integers we have $v_p(X) \equiv v_p(V) \equiv 1 \pmod 2$ if and only if $p \mid \gcd(X, V)$, and so by Proposition 5.9, a sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$ is that the triple of fractional ideals

$$\left(\mathbb{Z}, I_V^{-1}, \left(I_X^{-1} \prod_{\substack{\mathfrak{P}|(1+w)\mathfrak{O}_F \\ \mathfrak{P}\nmid 2\mathfrak{O}_F}} \mathfrak{P}^{-v_{\mathfrak{P}}(1+w)} \prod_{\substack{p|\gcd(X,V) \\ \mathfrak{P}|p\mathfrak{O}_F}} \mathfrak{P}^{-1}\right)\right)$$

has trivial class in the product of ray class groups

$$\mathrm{Cl}(\mathbb{Z}) \times \mathrm{Cl}_4(\mathbb{Z}) \times \mathrm{Cl}_4(\mathfrak{O}_F).$$

We note that since X and V are squarefree, we have $r_p(V) = r_p(X) = 0$ for all prime numbers p. So $I_V = I_X = \mathbb{Z}$, and therefore the first two terms of the triple of ideals above automatically have trivial class in $\mathrm{Cl}(\mathbb{Z}) \times \mathrm{Cl}_4(\mathbb{Z})$, and the third term reduces to the fractional ideal

$$J = \prod_{\substack{\mathfrak{P}|(1+w)\mathfrak{O}_F \\ \mathfrak{P}\nmid 2\mathfrak{O}_F}} \mathfrak{P}^{-v_{\mathfrak{P}}(1+w)} \prod_{\substack{p|\gcd(X,V) \\ \mathfrak{P}|p\mathfrak{O}_F}} \mathfrak{P}^{-1}.$$

Thus, using Poposition 5.9, a necessary condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$ is that J has trivial class in $\mathrm{Cl}_2(\mathfrak{O}_F)$. We show that this implies that equation (6.1) has a solution in integers. Recall from above that 2 is ramified in F, and write $2\mathfrak{O}_F = \mathfrak{P}_2^2$. Then $\mathfrak{P}_2 \mid\mid (1+w)\mathfrak{O}_F$, since $2 \mid\mid N_{F/\mathbb{Q}}(1+w)$ in $\mathbb{Z}$. Suppose that $J = \lambda\mathfrak{O}_F$ for some $\lambda \equiv 1 \pmod{^*} 2\mathfrak{O}_K$). Then we have

$$(1+w)\gcd(X,V)\lambda\mathfrak{O}_F = \mathfrak{P}_2 \prod_{\substack{p|\gcd(X,V) \\ \mathfrak{P}|p\mathfrak{O}_F}} \mathfrak{P}.$$

Taking norms, this is equivalent to the existence of an element $\mu = m_0 + m_1 w \in \mathfrak{O}_F$ satisfying

$$N_{F/\mathbb{Q}}(\mu)^2 = (2\gcd(X,V))^2$$

i.e.

$$m_0^2 + V m_1^2 = \pm 2\gcd(X,V).$$

Now suppose that equation (6.1) has an integer solution satisfying $m_0 \equiv m_1 \equiv 1 \pmod 8$. Consider the element $\mu = (1+w)\gcd(X,V)\lambda$ constructed

above. We have

$$\begin{aligned}
\mu \equiv 1 \pmod{8\mathfrak{O}_F} &\Rightarrow v_{\mathfrak{P}_2}\left((1+w)\gcd(X,V)\lambda - (1+w)\right) \geq 6 \\
&\Rightarrow v_{\mathfrak{P}_2}\left(1+w\right) + v_{\mathfrak{P}_2}\left(\gcd(X,V)\lambda - 1\right) \geq 6 \\
&\Rightarrow v_{\mathfrak{P}_2}\left(\gcd(X,V)\lambda - 1\right) \geq 5 \\
&\Rightarrow \gcd(X,V)\lambda \equiv 1 \pmod{^*\, 4\mathfrak{O}_F} \\
&\Rightarrow \pm\lambda \equiv 1 \pmod{^*\, 4\mathfrak{O}_F}
\end{aligned}$$

So, since λ is a generator for J, there exists a generator of J congruent to $1 \pmod{^*\, 4\mathfrak{O}_F}$. By Poposition 5.9, this is a sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$. □

7. Examples

If $L/\mathbb{Q}$ is a tame biquadratic extension, then by the Hilber-Speiser theorem ([12]) $\mathfrak{O}_L$ is free over the associated order $\mathfrak{A}_{\mathbb{Q}[G]} = \mathbb{Z}[G]$ in the classical Hopf-Galois structure $\mathbb{Q}[G]$. In this section we show that the analogous result does not hold for the 3 nonclassical Hopf-Galois structure admitted by the extension. Each of the three nonclassical structures admitted by $L/\mathbb{Q}$ corresponds to a choice of element $v \in \mathfrak{O}_L$, which appears in equation (6.1). We have some freedom in each case to make a convenient choice of the element $x \in \mathfrak{O}_L$ without affecting the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$.

Example 7.1. Let p, q be prime numbers satisfying $p \equiv q \equiv 1 \pmod 4$. Let $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Then $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in any of the three nonclassical Hopf-Galois structures admitted by the extension.

Proof. We consider the following 3 cases, each corresponding to the freeness of $\mathfrak{O}_L$ over $\mathfrak{A}_H$ in one of the nonclassical Hopf-Galois structures admitted by $L/\mathbb{Q}$:

i) The choices $v = \sqrt{p}, x = \sqrt{q}$ lead us to consider the equation $m_0^2 + pm_1^2 = \pm 2$. This has no solutions in integers since a solution (m_0, m_1) would satisfy $|m_0^2 + pm_1^2| = 2$, which is impossible.

ii) The choices $v = \sqrt{q}, x = \sqrt{p}$ lead us to consider the equation $m_0^2 + qm_1^2 = \pm 2$. This has no solutions in integers for similar reasons as equation (i).

iii) The choices $v = \sqrt{pq}, x = \sqrt{p}$ lead us to consider the equation $m_0^2 + pqm_1^2 = \pm 2p$. Suppose that (m_0, m_1) is an integer solution of this equation. Then $m_0^2 = \pm 2p - pqm_1^2$, which implies that $p \mid m_0^2$, and so $p \mid m_0$. Write $m_0 = pm_2$. Then (m_1, m_2) is an integer solution of the equation $pm_2^2 + qm_1^2 = \pm 2$. This implies that $|pm_2^2 + qm_1^2| = 2$ which is impossible.

Thus $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in any of the nonclassical Hopf-Galois structures admitted by the extension. □

Example 7.2. Let $L = \mathbb{Q}(\sqrt{-83}, \sqrt{-47})$. Then $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in precisely two of the three nonclassical Hopf-Galois structures admitted by the extension.

Proof. We show first that $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{83 \times 47}, x = \sqrt{-83}$. For this would imply that there exist integers m_0, m_1 satisfying

$$m_0^2 + (83 \times 47)m_1^2 = \pm 2 \times 83,$$

which would imply that there exist integers m_1, m_2 satisfying

$$|83m_2^2 + 47m_1^2| = 2,$$

which is impossible. In the Hopf-Galois structure corresponding to the choices $v = \sqrt{-83}, x = \sqrt{-47}$ we are led to consider the equation $m_0^2 - 83m_1^2 = \pm 2$. This has the solution $m_0 = 9, m_1 = 1$, which satisfies $m_0 \equiv m_1 \equiv 1 \pmod 8$. Similarly, in the Hopf-Galois structure corresponding to the choices $v = \sqrt{-47}, x = \sqrt{-83}$ we are led to consider the equation $m_0^2 - 47m_1^2 = \pm 2$. This has the solution $m_0 = -7, m_1 = 1$, which satisfies $m_0 \equiv m_1 \equiv 1 \pmod 8$. Thus $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in precisely two of the three nonclassical Hopf-Galois structures admitted by the extension. □

Example 7.3. Let r be a prime number satisfying $r \equiv 5 \pmod 8$ and let $L = \mathbb{Q}(\sqrt{-83}, \sqrt{-47r})$. Then $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in precisely one of the three nonclassical Hopf-Galois structures admitted by the extension.

Proof. By the argument presented above, $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{-83}, x = \sqrt{-47r}$. If $\mathfrak{O}_L$ were free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{83 \times 47r}, x = \sqrt{-83}$ then there would exist integers m_0, m_1 satisfying

$$m_0^2 + (83 \times 47r)m_1^2 = \pm 2 \times 83,$$

which would imply that there exist integers m_1, m_2 satisfying

$$83m_2^2 + 47rm_1^2 = \pm 2,$$

which is impossible. Finally we show that $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{-47r}, x = \sqrt{-83}$. This would imply that there exist integers m_0, m_1 satisfying

$$m_0^2 - 47rm_1^2 = \pm 2.$$

If we reduce this equation modulo r then we have a solution to

$$m_0^2 \equiv \pm 2 \pmod r.$$

But $r \equiv 5 \pmod 8$, so neither of ± 2 is a quadratic residue modulo r, and so this is impossible. Thus $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in precisely one of the three nonclassical Hopf-Galois structures admitted by the extension. □

Theorem 7.4. *Let $L/\mathbb{Q}$ be a tame biquadratic extension. Then $\mathfrak{O}_L$ is not simultaneously free over $\mathfrak{A}_H$ in all three of the nonclassical Hopf-Galois structures admitted by the extension.*

Proof. Write $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \in \mathbb{Z}/\mathbb{Z}^2$ and $a \equiv b \equiv 1 \pmod 4$. If $a > 0$ then $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{a}, x = \sqrt{b}$, and if $b > 0$ then $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{b}, x = \sqrt{a}$. But if $a < 0$ and $b < 0$ then $ab > 0$ and $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{ab}, x = \sqrt{a}$. □

Note added by the editors : this article was submitted for the issue dedicated to the Journées Arithmétiques 2009 in Saint-Étienne.

References

[1] Bley, W. and Boltje, R., *Lubin-Tate formal groups and module structure over Hopf orders*. J. Theor. Nombres Bordeaux **11** (1999), 269–305.

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

[3] Byott, N. P., *Uniqueness of Hopf-Galois structure for separable field extensions*. Communications in Algebra **24(10)** (1996), 3217–3228, corrigendum ibid 3705.

[4] Byott, N. P., *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications"*. Journal de Theorie des Nombres de Bordeaux **9** (1997), 201–219.

[5] Byott, N. P., *Integral Hopf-Galois Structures on Degree p^2 Extensions of $p-$adic Fields*. Journal of Algebra **248** (2002), 334–365.

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

[7] Childs, L. N., *Taming Wild Extensions: Hopf Algebras and local Galois module theory*. American Mathematical Society, 2000.

[8] Curtis, C. W. and Reiner, I., *Methods of Representation Theory with Applications to Finite Groups and Orders (Volume 1)*. Wiley, 1981.

[9] Curtis, C. W. and Reiner, I., *Methods of Representation Theory with Applications to Finite Groups and Orders (Volume 2)*. Wiley, 1981.

[10] Fröhlich, A., *Galois Module Structure of Algebraic Integers*. Springer, 1983.

[11] Fröhlich, A. and Taylor, M. J., *Algebraic Number Theory*. Cambridge University Press, 1991.

[12] Hilbert, D., *Die Theorie der algebraischen Zahlen*. Gesammelte Abhandlungen, 1965.

[13] Neukirch, J., *Algebraic Number Theory*. Springer, 1999.

[14] Truman, P. J., *Towards a Generalised Noether Theorem for Nonclassical Hopf-Galois Structures*. New York Journal of Mathematics **17** (2011), 799–810.

[15] Waterhouse, W.C., *Introduction to Affine Group Schemes*. Springer, 1997.

Paul J. Truman
School of Computing and Mathematics
Keele University,
ST5 5BG, UK
E-mail: P.J.Truman@keele.ac.uk