Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Journal de Théorie des Nombres
de Bordeaux **28** (2016), 557–582

Hopf-Galois module structure of tame $C_p \times C_p$ extensions

par Paul J. TRUMAN

Résumé. Soient p un nombre premier impair, K un corps de nombres contenant une racine primitive p-ième de l'unité, et L une extension galoisienne de K de groupe de Galois group isomorphe à $C_p \times C_p$. Nous étudions en détail les structures locale et globale de l'anneau des entiers $\mathfrak{O}_L$ en tant que module sur son ordre associé $\mathfrak{A}_H$ dans chacune des algèbres de Hopf H induisant une structure de Hopf-Galois non classique sur l'extension, complétant le cas $p = 2$ considéré dans [12]. Pour une telle algèbre de Hopf H, nous montrons que $\mathfrak{O}_L$ est localement libre sur $\mathfrak{A}_H$, calculons des générateurs locaux, et déterminons des conditions nécessaires et sufficiantes pour que $\mathfrak{O}_L$ soit libre sur $\mathfrak{A}_H$.

Abstract. Let p be an odd prime number, K a number field containing a primitive p^{th} root of unity, and L a Galois extension of K with Galois group isomorphic to $C_p \times C_p$. We 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 nonclassical Hopf-Galois structures on the extension, complementing the $p = 2$ case considered in [12]. For each Hopf algebra giving a nonclassical Hopf-Galois structure on L/K we show that $\mathfrak{O}_L$ is locally free over its associated order $\mathfrak{A}_H$ in H, compute local generators, and determine necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$.

1. Introduction

This paper is a sequel to [12], in which we studied the nonclassical Hopf-Galois module structure of rings of algebraic integers in tamely ramified biquadratic extensions of number fields, and to [11], in which we studied a larger class of tamely ramified extensions. In the introductions to those papers, we described how the use of nonclassical Hopf-Galois structures

Manuscrit reçu le 18 juin 2014, révisé le 11 août 2014, accepté le 5 septembre 2014.

Mathematics Subject Classification. 11R33, 11S23, 16T05.

Mots-clefs. Hopf-Galois theory, Galois module structure, tame extension.

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.

has proven to be a fruitful generalization of the classical Galois module theory of algebraic integers, and posed questions about the applications of these techniques to tamely ramified extensions in particular. Since in this paper we are concerned with extensions of number fields, we summarize the classical theory briefly in this context; a thorough survey can be found in [10]. If L/K is a finite Galois extension of number fields with Galois group G then classically one studies 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 $\mathfrak{O}_L$ is locally free over $\mathfrak{O}_K[G]$ (and therefore $\mathfrak{A}_{K[G]} = \mathfrak{O}_K[G]$) if and only if L/K is at most tamely ramified [7, Theorem 3]. In this case, therefore, $\mathfrak{O}_L$ defines a class in the locally free class group $\mathrm{Cl}\,(\mathfrak{O}_K[G])$, and Fröhlich's Hom Description of this group allows us to compute this class and determine the global structure of $\mathfrak{O}_L$ over $\mathfrak{O}_K[G]$, at least up to stable isomorphism. In the case that $K = \mathbb{Q}$, the Hilbert-Speiser theorem [8] asserts that $\mathfrak{O}_L$ is free over $\mathbb{Z}[G]$ if G is abelian, and in general Taylor's proof of Fröhlich's conjecture [9] identifies the obstruction to freeness of $\mathfrak{O}_L$ over $\mathbb{Z}[G]$ in terms of analytic invariants.

Hopf-Galois theory generalises the classical situation described above (see [5] for a survey). If L/K is a finite separable extension of fields, we say that a K-Hopf algebra 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 obvious K-linear map

$$L \otimes_K H \to \mathrm{End}_K(L)$$

is an isomorphism of K-vector spaces (see [5, Definition 2.7]). A finite Galois extension of fields L/K admits at least one Hopf-Galois structure, with Hopf algebra $K[G]$, and we call this the classical structure. We call any other Hopf-Galois structures admitted by the extension nonclassical. If L/K is an extension of local or global fields then within a Hopf algebra H giving a Hopf-Galois structure on the extension L/K we define the associated order of $\mathfrak{O}_L$ as follows:

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

and study the structure of $\mathfrak{O}_L$ as an $\mathfrak{A}_H$-module. This approach has proven fruitful in the study of wildly ramified extensions (see [3], for example), but in [11] we considered tamely ramified extensions and investigated the following natural generalization of Noether's theorem: If L/K is a finite separable extension of number fields which is at most tamely ramified and H is a Hopf algebra giving a Hopf-Galois structure on the extension, is $\mathfrak{O}_L$ locally free over $\mathfrak{A}_H$, its associated order in H? We proved the following partial result:

Theorem 1.1. Let L/K be a finite extension of number fields which is H-Galois for some commutative Hopf algebra H, and suppose that no prime lying above a prime number dividing $[L:K]$ is ramified in L/K (i.e. the extension is *domestic*). Then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.

Proof. See [11, Theorem 5.9]. □

As a particular case of this, we have:

Corollary 1.2. Let L/K be a finite extension of number fields which is H-Galois for some commutative Hopf algebra H, and suppose that L/K has prime-power degree. Then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.

In [12], we studied in detail the local and global Hopf-Galois module structure of tamely ramified Galois extensions of number fields L/K with group $G \cong C_2 \times C_2$. We used Corollary (1.2) to show that $\mathfrak{O}_L$ is locally free over its associated order $\mathfrak{A}_H$ in any Hopf algebra H giving a Hopf-Galois structure on the extension, and determined necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$. In the present paper we perform a similar analysis of tamely ramified Galois extensions of number fields L/K with group $G \cong C_p \times C_p$ for an odd prime number p, under the assumption that K contains a primitive p^{th} root of unity. In Section 2, we characterise these extensions and determine explicit integral bases of $\mathfrak{O}_{L,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$. In Section 3 we quote results of Byott, who enumerated and described all the Hopf-Galois structures admitted by such an extension, and give the Wedderburn decompositions of the Hopf algebras. In Section 4 we calculate, for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$, an explicit $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{A}_{H,\mathfrak{p}}$ and an explicit generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. Finally, in Section 5 We use the detailed local information from Section 4 to describe the locally free class group $\mathrm{Cl}(\mathfrak{A}_H)$ using a weak version of Fröhlich's Hom-Description ([6, §49]) and derive necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$.

2. Tame $C_p \times C_p$ Extensions

Let p be an odd prime number, and let K be a number field containing a primitive p^{th} root of unity ζ. A Galois extension L of K with group isomorphic to $C_p \times C_p$ has the form $L = K(\alpha, \beta)$, where $\alpha^p = a$ and $\beta^p = b$ are coset representatives of linearly independent elements of the $\mathbb{F}_p$-vector space $K^\times/(K^\times)^p$. In this section we establish congruence conditions on a and b which are equivalent to the extension L/K being tamely ramified, and for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ we calculate an explicit integral basis of the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$. Many of the results in this section are straightforward generalizations of the corresponding results in Section 2 of [12], so we omit the details of the proofs. In particular here, as there, when we take completions with respect to an absolute value arising from a prime $\mathfrak{p}$ of $\mathfrak{O}_K$, we shall often tacitly be working not with local fields or discrete valuation rings but with finite products of these objects, and so should regard our elements as tuples.

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

Proof. This is very similar to the proof of [12, Proposition 2.1]. The extension L/K is tamely ramified if and only if both the subextensions $K(\alpha)/K$ and $K(\beta)/K$ are tamely ramified, so it suffices to consider the subextension $K(\alpha)/K$. By [5, (24.2)] this is tamely ramified if and only if we can choose α such that $\alpha^p \equiv 1 \pmod{(\zeta-1)^p\mathfrak{O}_{K,\mathfrak{p}}}$ for each prime $\mathfrak{p}$ lying above p. By adjusting by the p^{th} power of an integral element and using the Chinese Remainder Theorem, we arrive at the criterion in the proposition. □

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

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

Proposition 2.3. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which does not lie above p, 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 $\mathfrak{O}_{L,\mathfrak{p}}$.

$$\left\{ \frac{\alpha^i\beta^j}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a^ib^j)}} \;\middle|\; 0 \leq i,j \leq p-1 \right\}$$

Proof. This is a straightforward generalization of the proof of [12, Proposition 2.3]. □

Definition 2.4. For each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ which lies above p, we shall write $e_\mathfrak{p} = v_\mathfrak{p}(p)$. Often, if there is no danger of confusion, we shall surpress the subcript and simply write e. This is divisible by $p-1$, and we shall write $e' = e/(p-1)$. We note that $e' = v_\mathfrak{p}(\zeta-1)$.

Proposition 2.5. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above p, 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 $\mathfrak{O}_{K(\alpha),\mathfrak{p}}$:

$$\left\{ \left(\frac{\alpha-1}{\pi_\mathfrak{p}^{e'}}\right)^i \;\middle|\; 0 \leq i \leq p-1 \right\},$$

and the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$:

$$\left\{ \left(\frac{\alpha-1}{\pi_\mathfrak{p}^{e'}}\right)^i \left(\frac{\beta-1}{\pi_\mathfrak{p}^{e'}}\right)^j \;\middle|\; 0 \leq i,j \leq p-1 \right\}.$$

Proof. This is a straightforward generalization of the proof of [12, Proposition 2.4]. The stated $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{K(\alpha),\mathfrak{p}}$ is computed in [5, (24.4)], and a similar argument applies to $\mathfrak{O}_{K(\beta),\mathfrak{p}}$. Noting that the subextensions $K(\alpha)/K$ and $K(\beta)/K$ are arithmetically disjoint at $\mathfrak{p}$ yields the description of $\mathfrak{O}_{L,\mathfrak{p}}$ in the proposition. □

3. Hopf-Galois Structures On Tame $C_p \times C_p$ Extensions

A theorem of Greither and Pareigis allows for the enumeration of all Hopf-Galois structures admitted by any 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 L/K with Galois group G. Let $\mathrm{Perm}(G)$ be group of permutations of G, and let $\lambda : G \to \mathrm{Perm}(G)$ be the left regular embedding. Call a subgroup N of $\mathrm{Perm}(G)$ *regular* if $|N| = |G|$ and N acts transitively on G. Then we have:

Theorem 3.1 (Greither and Pareigis). There is a bijection between regular subgroups N of $\mathrm{Perm}(G)$ 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:

$$\left(\sum_{n\in N} c_n n\right) \cdot x = \sum_{n\in N} c_n (n^{-1}(1_G))x. \tag{3.1}$$

Proof. See [5, Theorem 6.8]. □

In [2] and [4], Byott enumerated all the Hopf-Galois structure admitted by a Galois extension L/K with group $G \cong C_p \times C_p$ and, under the assumption that $\zeta \in K$, described the corresponding Hopf algebras. These are all commutative and, since in our case K has characteristic zero, they are therefore separable (see [13, (11.4)]). This implies that each contains a unique maximal $\mathfrak{O}_K$-order. In this section we express each of the Hopf algebras giving nonclassical Hopf-Galois structures on L/K as a product of fields, and hence describe the unique maximal order in each of them. Finally, we derive formulae for the action of each Hopf algebra on the extension L/K.

Theorem 3.2 (Byott). Let L/K be a Galois extension of fields with group $G \cong C_p \times C_p$. Let $T \leq G$ have order p, let $d \in \{0, 1, \ldots, p-1\}$, and fix $\sigma, \tau \in G$ satisfying:

$$T = \langle \tau \rangle, \qquad \sigma^p = 1, \qquad G = \langle \sigma, \tau \rangle.$$

There are well defined elements $\rho, \eta \in \mathrm{Perm}(G)$ determined by:

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

We have $\rho\eta = \eta\rho$ and $\rho^p = \eta^p = 1$. Now set $N = N_{T,d} = \langle \rho, \eta \rangle$. Then $N \cong G$. Futhermore, N is regular on G and is normalised by $\lambda(G)$, and so N gives rise to a Hopf-Galois structure on L/K, with Hopf Algebra $H = H_{T,d} = L[N_{T,d}]^G$. If $d = 0$ then $N = \lambda(G)$, giving the classical structure regardless of the choice of T. If $d \neq 0$ then the $p-1$ possible choices of d, together with the $p+1$ possible choices of T, yield $p^2 - 1$ distinct groups N, each giving rise to a nonclassical structure on L/K. These are all the Hopf-Galois structures on L/K.

Proof. For the enumeration of Hopf-Galois structures, see [2, Corollary to Theorem 1, part (iii) (corrected)]. For the determination of the permutations η and ρ, see [4, Theorem 2.5]. □

Since the choice $d = 0$ gives the classical Hopf-Galois structure on L/K regardless of the choice of subgroup T, we shall henceforth assume that $d \neq 0$, so as to consider only nonclassical structures. Beyond this, we will not specify a choice of either T or d, and will therefore work with an arbitrary Hopf algebra $H = H_{T,d}$ giving a nonclassical structure on the extension. Next we seek a more explicit description of the Hopf algebra. Since $\zeta \in K$, the group algebra $K[\rho]$ has a basis of mutually orthogonal idempotents:

$$e_s = \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{-ks}\rho^k \qquad \text{for } 0 \leq s \leq p-1,$$

satisfying

$$\rho e_s = \zeta^s e_s.$$

The subfield L^T of L is cyclic of degree p over K. Fix $v \in \left(L^T\right)^\times$ satisfying

$$\sigma(v) = \zeta^{-d} v,$$

and set

$$a_v = \sum_{s=0}^{p-1} v^s e_s \in L^T[\rho].$$

Then we have:

Proposition 3.3 (Byott). With the above notation, for $d \neq 0$, we have $H = K[\rho, a_v\eta]$.

Proof. See [4, Lemma 2.10]. □

Proposition 3.4. With the above notation we have, for $d \neq 0$ and any choice of T, the following isomorphism of K-algebras.

$$H \cong K^p \times K(v)^{p-1}.$$

Proof. The following set is a basis of H:

$$\omega = \{e_s(a_v\eta)^t \mid 0 \leq s, t \leq p-1\}.$$

Clearly we have

$$(e_s(a_v\eta)^t)(e_{s'}(a_v\eta)^{t'}) = 0$$

whenever $s \neq s'$. By examining elements of the form $e_0(a_v\eta)^t$, we find that

$$e_0H \cong K[\eta],$$

and by forming orthogonal idempotents within $K[\eta]$ we have $K[\eta] \cong K^p$. The orthogonal idempotents in $K[\eta]$ correspond in e_0H to the elements

$$\frac{1}{p}\sum_{k=0}^{p-1} \zeta^{kdt} e_0(a_v\eta)^k.$$

Now considering elements of the form $e_s(a_v\eta)^t$ for $s \neq 0$, we calculate

$$(e_s(a_v\eta))^p = v^{ps}e_s,$$

so we see that $e_sH \cong K(v^s) \cong K(v)$. Thus we have

$$H \cong K^p \times K(v)^{p-1}. \qquad \square$$

Definition 3.5. For $r = 0, \ldots, p-1$, we shall adopt the following notation for the idempotents defined in the proof of Proposition (3.4):

$$E_r = \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{kdr} e_0(a_v\eta)^k.$$

Using the notation introduced in Definition (3.5), we can exhibit an explicit K-algebra isomorphism $\Phi : K^p \times K(v)^{p-1} \to H$:

Definition 3.6. Given an element

$$(z_0, \ldots, z_{p-1}, y_1, \ldots, y_{p-1}) \in K^p \times K(v)^{p-1},$$

write $y_s = \sum_{t=0}^{p-1} w_{s,t}v^{st}$ with $w_{s,t} \in K$ for $s = 1, \ldots, p-1$ and $t = 0, \ldots, p-1$. Let $\Phi : K^p \times K(v)^{p-1} \to H$ be the map defined by

$$\Phi(z_0, \ldots, z_{p-1}, y_1, \ldots, y_{p-1}) = \sum_{r=0}^{p-1} z_rE_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} w_{s,t}e_s(a_v\eta)^t.$$

A consequence of the description of H given in Proposition (3.4) is that we can identify the unique maximal $\mathfrak{O}_K$-order in H. Here, and subsequently, whenever $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ we write $\pi_{\mathfrak{p}}$ for a uniformiser of $K_{\mathfrak{p}}$.

Corollary 3.7. We have the following description of the unique maximal $\mathfrak{O}_K$-order $\mathfrak{M}_H$ in H.

$$\mathfrak{M}_H \cong \mathfrak{O}_K^p \times \mathfrak{O}_{K(v)}^{p-1}.$$

It is possible to choose the element v such that in the notation of Proposition (2.1) we have $v = \alpha^i\beta^j$ for some nonnegative integers i, j, and we shall always assume that we have done so. Choosing v in this way we have $V = v^p \equiv 1 \pmod{(\zeta - 1)^p\mathfrak{O}_L}$, which allows us to use Propositions (2.3) and (2.5) to describe locally the unique maximal $\mathfrak{O}_K$-order $\mathfrak{M}_H$.

Corollary 3.8. If $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which does not lie above p, then an $\mathfrak{O}_{K,\mathfrak{p}}$ basis of $\mathfrak{M}_{H,\mathfrak{p}}$ is:

$$\{E_r \mid 0 \leq r \leq p-1\} \cup \left\{ \frac{e_s(a_v\eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \;\middle|\; \begin{array}{l} 1 \leq s \leq p-1, \\ 0 \leq t \leq p-1 \end{array} \right\}.$$

Corollary 3.9. If $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which lies above p, then an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{K(v^s),\mathfrak{p}}$ is

$$\left\{ \left(\frac{v^s - 1}{\pi_{\mathfrak{p}}^{e'}} \right)^t \;\middle|\; 0 \leq t \leq p-1 \right\},$$

which implies that an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{M}_{H,\mathfrak{p}}$ is

$$\{E_r \mid 0 \leq r \leq p-1\} \cup \left\{ \left(\frac{e_s(a_v\eta) - e_s}{\pi_{\mathfrak{p}}^{e'}} \right)^t \;\middle|\; \begin{array}{l} 1 \leq s \leq p-1, \\ 0 \leq t \leq p-1 \end{array} \right\}.$$

In addition to the notation established in the previous sections, we now write S for the subgroup $\langle\sigma\rangle$ of G, and fix an element $x \in \left(L^S\right)^\times$ satisfying $\tau(x) = \zeta x$. Once again, it is possible to choose the element x such that in the notation of Proposition (2.1) we have $x = \alpha^i\beta^j$ for some nonnegative integers i, j, which implies that $X = x^p \equiv 1 \pmod{(\zeta - 1)^p\mathfrak{O}_L}$. Then $L = K(x, v)$, 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 the action of H on L is given by equation (3.1). We calculate:

$$\rho^r\eta^t(\sigma^k\tau^l) = 1_G \text{ if and only if } k = t \text{ and } l = r - dt(t-1)/2,$$

and so

$$(\rho^r\eta^t)^{-1}(1_G) = \sigma^t\tau^{r-(dt(t-1))/2} \tag{3.2}$$

Proposition 3.10. For $s = 0, \ldots, p-1$ we have

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

Proof. Each $e_s \in H$, so we use equation (3.2) to calculate $e_s(x^i v^j)$.

$$\begin{aligned} e_s \cdot (x^i v^j) &= \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{-ks}\rho^k \cdot (x^i v^j) \\ &= \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{-ks}\tau^k (x^i v^j) \\ &= \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{-ks}\zeta^{ki} x^i v^j \\ &= \frac{x^i v^j}{p}\sum_{k=0}^{p-1} \zeta^{k(i-s)} \\ &= \begin{cases} x^i v^j & \text{if } s = i \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$ □

Proposition 3.11. For $t = 0, \dots, p-1$ we have

$$(a_v \eta)^t \cdot (x^i v^j) = \zeta^{-dtj}\zeta^{-dit(t-1)/2} x^i v^{j+it}.$$

Proof. First we observe that

$$(a_v \eta)^t = \left(\sum_{s=0}^{p-1} v^s e_s \eta\right)^t = \sum_{s=0}^{p-1} v^{st} e_s \eta^t$$

since the e_s are orthogonal idempotents. Now each $(a_v \eta)^t \in H$, so we use equation (3.2) to calculate $(a_v \eta)^t \cdot (x^i v^j)$.

$$\begin{aligned} (a_v \eta)^t \cdot (x^i v^j) &= \sum_{s=0}^{p-1} v^{st} e_s \eta^t \cdot (x^i v^j) \\ &= \frac{1}{p}\sum_{s=0}^{p-1}\sum_{k=0}^{p-1} v^{st}\zeta^{-ks}\rho^k \eta^t \cdot (x^i v^j) \\ &= \frac{1}{p}\sum_{s=0}^{p-1}\sum_{k=0}^{p-1} v^{st}\zeta^{-ks}\sigma^t \tau^{k-dt(t-1)/2}(x^i v^j) \\ &= \frac{1}{p}\sum_{s=0}^{p-1}\sum_{k=0}^{p-1} v^{st}\zeta^{-ks}\zeta^{-dtj}\zeta^{ki-dit(t-1)/2} x^i v^j \\ &= \frac{\zeta^{-dtj}\zeta^{-dit(t-1)/2} x^i v^j}{p}\sum_{s=0}^{p-1}\sum_{k=0}^{p-1} \zeta^{k(i-s)} v^{st} \\ &= \zeta^{-dtj}\zeta^{-dit(t-1)/2} x^i v^{j+it}. \end{aligned}$$ □

Combining Propositions (3.10) and (3.11) yields:

Corollary 3.12. For $s = 0, \dots, p-1$ and $t = 0, \dots, p-1$, we have

$$e_s(a_v\eta)^t \cdot (x^i v^j) = \begin{cases} \zeta^{-dtj}\zeta^{-dit(t-1)/2}x^i v^{j+it} & \text{if } i = s \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 3.13. For $r = 0, \dots, p-1$, we have

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

Proof. Recall from Definition (3.5) that

$$E_r = \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{kdr} e_0(a_v\eta)^k,$$

so it is clear from Corollary (3.12) that $E_r \cdot (x^i v^j) = 0$ unless $i = 0$. In this case we have

$$\begin{aligned} E_r \cdot (v^j) &= \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{kdr} e_0(a_v\eta)^k \cdot (v^j) \\ &= \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{kdr}\zeta^{-kdj} v^j \\ &= \frac{v^j}{p}\sum_{k=0}^{p-1} \zeta^{kd(j-r)} \\ &= \begin{cases} v^r & \text{if } j = r \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

□

4. Local Freeness

We retain the notation of the previous sections: p is an odd prime number, K is a number field containing a primitive p^{th} root of unity ζ, and L is a tamely ramified Galois extension of K with group $G \cong C_p \times C_p$. Additionally, H is a Hopf algebra giving a nonclassical Hopf-Galois structure on the extension. This is determined by a choice of subgroup T of G having degree p and a choice of integer $d \in \{1, \dots, p-1\}$. We have not made a particular choice of either T or d, so as to work with an arbitrary Hopf algebra giving a Hopf-Galois structure on the extension. To describe the extension relative to this Hopf algebra, we have written $G = \langle \sigma, \tau \rangle$, where τ generates T, and have fixed an element $v \in \left(L^T\right)^\times$ satisfying $\sigma(v) = \zeta^{-d}v$ and an element $x \in \left(L^S\right)^\times$ satisfying $\tau(x) = \zeta x$.

In this section we establish that $\mathfrak{O}_L$ is locally free over its associated order $\mathfrak{A}_H$ in H, and for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ we find an explicit $\mathfrak{O}_{K,\mathfrak{p}}$-basis of the completed associated order $\mathfrak{A}_{H,\mathfrak{p}}$ and a generator of $\mathfrak{O}_L$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module. In the final section, we shall use this detailed local information to establish necessary and sufficient conditions for $\mathfrak{O}_L$ to be (globally) free over $\mathfrak{A}_H$.

Proposition 4.1. The associated order $\mathfrak{A}_H$ is the $\mathfrak{O}_K$-order $\mathfrak{O}_L[N]^G$ and $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$.

Proof. Since L/K is a tame extension of number fields, $[L : K] = p^2$, and H is commutative, we may apply [11, Theorem 5.10]. More precisely, if $\mathfrak{p}$ lies above p then $\mathfrak{p}$ must be unramified in L, so $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a Hopf order in $H_\mathfrak{p}$ ([11, Proposition 5.3]) and coincides with $\mathfrak{A}_{H,\mathfrak{p}}$ ([11, Proposition 5.4]). Now ([5, (12.7)]) implies that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$-module. If $\mathfrak{p}$ does not lie above p then the characteristic of the residue field $\mathfrak{O}_K/\mathfrak{p}$ does not divide $[L : K]$, so $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is the unique maximal order in $H_\mathfrak{p}$ ([11, Proposition 5.6]) and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$-module. Since $\mathfrak{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ we must have $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ for each $\mathfrak{p}$, and therefore $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$. □

Proposition 4.2. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which does not lie above p. Then an $\mathfrak{O}_K$-basis of $\mathfrak{A}_{H,\mathfrak{p}}$ is given by:

$$\{E_r \mid 0 \leq r \leq p-1\} \cup \left\{ \frac{e_s(a_v\eta)^t}{\pi_\mathfrak{p}^{r_\mathfrak{p}(V^{st})}} \;\middle|\; \begin{array}{c} 1 \leq s \leq p-1, \\ 0 \leq t \leq p-1 \end{array} \right\}.$$

Proof. Since $\mathfrak{p}$ does not lie above p we have $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G = \mathfrak{M}_{H,p}$, the unique maximal order in $H_\mathfrak{p}$, and we computed an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of this in Proposition (3.8). □

Proposition 4.3. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above p. For $0 \leq i \leq p-1$ and $1 \leq t \leq p-1$ define

$$\omega_{i,t} = \sum_{k=0}^{p-1} \sigma^k \left(\frac{v^t - 1}{\pi_\mathfrak{p}^{e'}} \right)^i {}^{\sigma^k}\eta^t.$$

Then an $\mathfrak{O}_{K,\mathfrak{p}}$-basis for $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is given by

$$\{\rho^k \mid 0 \leq k \leq p-1\} \cup \left\{ \omega_{i,t} \;\middle|\; \begin{array}{c} 0 \leq i \leq p-1, \\ 1 \leq t \leq p-1 \end{array} \right\}.$$

Proof. We follow the method of [1, Lemma 2.1]. Firstly, we find the orbits of G in N. Recall from Proposition (3.2) that $N = \langle \rho, \eta \rangle$, and from Theorem (3.1) that G acts on N by conjugation via the embedding λ. We calculate ${}^g\rho = \rho$ for all $g \in G$ and ${}^\tau\eta = \eta, {}^\sigma\eta = \rho^d\eta$. The orbits of G in N are therefore

$$\{\rho^k\} \text{ for } 0 \leq k \leq p-1,$$

which each have length 1, and

$$\{\rho^k \eta^t \mid 0 \leq k \leq p-1\} \text{ for } 1 \leq t \leq p-1,$$

which each have length p. Each of the elements forming an orbit of length 1 is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis element of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$. For each of the $p-1$ orbits of length p, we construct p basis elements as follows: for $t = 1, \dots, p-1$ choose η^t as a representative of the orbit containing it, and note that the corresponding stabilizer is $T = \langle \tau \rangle$. Using Proposition (2.5), an integral basis of $L_{\mathfrak{p}}^T / K_{\mathfrak{p}}$ is given by

$$\left\{ \left(\frac{v^t - 1}{\pi_{\mathfrak{p}}^{e'}} \right)^i \,\middle|\, 0 \leq i \leq p-1 \right\},$$

and so, for each $i = 0, \dots, p-1$, the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis element of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$:

$$\omega_{i,t} = \sum_{k=0}^{p-1} \sigma^k \left(\frac{v^t - 1}{\pi_{\mathfrak{p}}^{e'}} \right)^i {}^{\sigma^k}\eta^t. \qquad \square$$

Finally, we find explicit generators of $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$-module for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$. In the case that $\mathfrak{p}$ does not lie above p, we first make the following definition:

Definition 4.4. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which does not lie above p. Define $0 \leq j_{\mathfrak{p}} \leq p-1$ as follows:

- If $v_{\mathfrak{p}}(X) \equiv 0 \pmod{p}$ or $v_{\mathfrak{p}}(V) \equiv 0 \pmod{p}$ then let $j_{\mathfrak{p}} = 0$.
- Otherwise, let $j_{\mathfrak{p}}$ be the unique integer in the range $1, \dots, p-1$ such that $v_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}}) \equiv 0 \pmod{p}$.

We note that $j_{\mathfrak{p}} \neq 0$ if and only if $(v_{\mathfrak{p}}(X), p) = (v_{\mathfrak{p}}(V), p) = 1$, that is, if and only if $\mathfrak{p}$ is ramified in both of the subextensions $K(x)/K$ and $K(v)/K$. Using this definition, we have:

Proposition 4.5. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which does not lie above p. Then the following element $\gamma_{\mathfrak{p}}$ is a generator for $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module:

$$\gamma_{\mathfrak{p}} = \sum_{j=0}^{p-1} \frac{v^j}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^j)}} + \sum_{s=1}^{p-1} \frac{x^s v^{s j_{\mathfrak{p}}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s V^{s j_{\mathfrak{p}}})}}.$$

Proof. It is easy to see from Proposition (2.3) that $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$. Since $\mathfrak{O}_{L,\mathfrak{p}}$ and $\mathfrak{A}_{H,\mathfrak{p}}$ are both free $\mathfrak{O}_{K,\mathfrak{p}}$-modules of rank p^2, 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 $\mathfrak{O}_{L,\mathfrak{p}}$. Recall the $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{A}_{H,\mathfrak{p}}$ from Proposition (4.2), and note that we have $\mathfrak{O}_{L,\mathfrak{p}} = \bigoplus_{s=0}^{p-1} e_s \mathfrak{O}_{L,\mathfrak{p}}$. For each $r = 0, \dots, p-1$, we have by (3.13) that

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

giving an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $e_0\mathfrak{O}_{L,\mathfrak{p}}$. For $s \neq 0$ and $t = 0, \dots, p-1$, we have by (3.12) that

$$\begin{aligned} \frac{e_s(a_v\eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \cdot \gamma_{\mathfrak{p}} &= \frac{e_s(a_v\eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \cdot \frac{x^s v^{sj_{\mathfrak{p}}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})}} \\ &\sim \frac{v^{st}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \frac{x^s v^{sj_{\mathfrak{p}}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})}} \\ &= \frac{x^s v^{sj_{\mathfrak{p}}+st}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}+st})}}, \end{aligned}$$

where $y \sim y'$ denotes that $y' = uy$ for some $u \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. The final equality above holds since by the choice of $j_{\mathfrak{p}}$ we have

$$r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}}) + r_{\mathfrak{p}}(V^{st}) = r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}+st}).$$

Therefore for each $s \neq 0$, the elements

$$\frac{e_s(a_v\eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \cdot \gamma_{\mathfrak{p}} \text{ for } 0 \leq t \leq p-1$$

are an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $e_s\mathfrak{O}_{L,\mathfrak{p}}$. Together with the basis of $e_0\mathfrak{O}_{L,\mathfrak{p}}$, we have an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$. □

If $\mathfrak{p}$ is a prime lying above p, then by [11, Proposition 5.3] $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a Hopf order in $H_{\mathfrak{p}}$ and by a straightforward generalization of [12, Proposition 4.3] it is a local ring, so we may use the method of Childs and Hurley to identify a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module (see [5, (14.7)]).

Proposition 4.6. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above p. Then a generator for $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module is:

$$\gamma_{\mathfrak{p}} = \frac{1}{p^2} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} x^i v^j.$$

Proof. We observe that the trace element

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

is a left integral of $\mathfrak{A}_{H,\mathfrak{p}}$ (see [5, §3]). Therefore by [5, (14.7)] $\gamma_{\mathfrak{p}}$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module if and only if $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$ and $\theta \cdot \gamma_{\mathfrak{p}} = 1$. To show that $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$, it is sufficient to show that

$$\left(\frac{1}{p} \sum_{i=0}^{p-1} x^i \right) \in \mathfrak{O}_{L,\mathfrak{p}}.$$

Recalling the $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$ given in Proposition (2.5), the element

$$\left(\frac{x-1}{\pi_{\mathfrak{p}}^{e'}}\right)^{p-1} \sim \frac{1}{p}\sum_{i=0}^{p-1}\binom{p-1}{i}(-1)^i x^i$$

lies in $\mathfrak{O}_{L,\mathfrak{p}}$. (Recall that $y \sim y'$ denotes that $y' = uy$ for some $u \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$.) But for $i = 0, \ldots, p-1$ we have

$$\binom{p-1}{i} \equiv (-1)^i \pmod{p},$$

so

$$\sum_{i=0}^{p-1}\binom{p-1}{i}(-1)^i x^i \equiv \sum_{i=0}^{p-1} x^i \pmod{p\mathfrak{O}_{L,\mathfrak{p}}},$$

and so

$$\left(\frac{1}{p}\sum_{i=0}^{p-1} x^i\right) \in \mathfrak{O}_{L,\mathfrak{p}}.$$

Therefore $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$. It is straightforward to verify that

$$\theta \cdot \gamma_{\mathfrak{p}} = \mathrm{Tr}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(\gamma_{\mathfrak{p}}) = 1. \qquad \square$$

5. Conditions for Global Freeness

In this section, we determine necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$. We have shown in Section 4 that $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$, and so it defines a class in the locally free class group $\mathrm{Cl}\,(\mathfrak{A}_H)$. Since H is a commutative Hopf algebra, $\mathfrak{A}_H$ has the locally free cancellation property (see [6, (§51)]), and so $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$ module if and only if it has trivial class in $\mathrm{Cl}\,(\mathfrak{A}_H)$. Furthermore, again since H is commutative, we have an isomorphism

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

where $\mathbb{J}(H)$ is the group of idèles of H, $H^{\times}$ is the subgroup of principal idèles, and $\mathbb{U}(\mathfrak{A}_H)$ is the group of unit idèles. (This is a weak form of Fröhlich's Hom Description, see [6, (§49)].) The class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$ corresponds under this isomorphism to the class of an idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ determined as follows: let Γ be a fixed generator of L over H, and for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ let $h_{\mathfrak{p}} \in H_{\mathfrak{p}}$ be an element such that $h_{\mathfrak{p}} \cdot \Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module. In this section we use the detailed local information we computed in Section 4 first to "sandwich" the locally free class group between products of ray class groups whose conductors are ideals divisible only by primes lying above p, and then to compute the idèle $h_{\mathfrak{p}}$, and hence give necessary and sufficient conditions for $\mathfrak{O}_L$ to have trivial class in $\mathrm{Cl}\,(\mathfrak{A}_H)$.

We begin by studying the group of units of $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$:

Proposition 5.1. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$. If $\mathfrak{p}$ does not lie above p then

$$\mathfrak{A}^\times_{H,\mathfrak{p}} = \mathfrak{M}^\times_{H,p} \cong (\mathfrak{O}^\times_{K,\mathfrak{p}})^p \times (\mathfrak{O}^\times_{K(v),\mathfrak{p}})^{p-1}.$$

If $\mathfrak{p}$ lies above p then

$$\mathfrak{A}^\times_{H,\mathfrak{p}} = \{z \in \mathfrak{A}_{H,\mathfrak{p}} \mid \varepsilon(z) \in \mathfrak{O}^\times_{K,\mathfrak{p}}\}.$$

Proof. If $\mathfrak{p}$ does not lie above p then by [11, Proposition 5.6] $\mathfrak{A}_{H,\mathfrak{p}}$ is the unique maximal order in $H_\mathfrak{p}$, and Corollary (3.8) yields the stated description of the units. If $\mathfrak{p}$ lies above p then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a local ring whose unique maximal ideal is $(\mathfrak{p}\mathfrak{O}_{L,\mathfrak{p}}[N] + \ker\varepsilon)^G$ (a straightforward generalization of [12, Proposition 4.3]), and so an element $z \in \mathfrak{A}_{H,\mathfrak{p}}$ is a unit if and only if $\varepsilon(z) \in \mathfrak{O}^\times_{K,\mathfrak{p}}$. □

Proposition 5.2. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above p. Let $z \in \mathfrak{M}_{H,\mathfrak{p}}$ and write

$$z = \sum_{r=0}^{p-1} a_r E_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} a_{s,t}\left(\frac{e_s(a_v\eta) - e_s}{\pi_\mathfrak{p}^{e'}}\right)^t e_s$$

with $a_r, a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$ for $r,t = 0,\dots,p-1$ and $s = 1,\dots,p-1$. Then $z \in \mathfrak{A}^\times_{H,\mathfrak{p}}$ if and only if

(i) $$\sum_{s=i}^{p-1}\sum_{t=j}^{p-1}\binom{s}{i}\binom{t}{j}(-1)^{t-j}\pi_\mathfrak{p}^{-te'}a_{s,t} \equiv 0 \pmod{p\pi_\mathfrak{p}^{-ie'}\mathfrak{O}_{K,\mathfrak{p}}}$$

for $1 \le i,j \le p-1$,

(ii) $$\sum_{r=0}^{p-1}\zeta^{jdr}a_r + p\sum_{s=1}^{p-1}\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_\mathfrak{p}^{-te'}a_{s,t} \equiv 0 \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}}$$

for $0 \le j \le p-1$,

(iii) $$\sum_{r=0}^{p-1}a_r + p\sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{-ks}(-1)^t\pi_\mathfrak{p}^{-te'}a_{s,t} \equiv 0 \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}}$$

for $0 \le k \le p-1$,

(iv) $a_0 \in \mathfrak{O}^\times_{K,\mathfrak{p}}$.

Proof. We rewrite z in terms of the basis elements of $\mathfrak{A}_{H,\mathfrak{p}}$ given in Proposition (4.3), noting that for each $1 \le t \le p-1$ and $0 \le s \le p-1$ we have

$$e_s(a_v\eta)^t = \frac{1}{p}\sum_{i=0}^{s}\binom{s}{i}\pi_\mathfrak{p}^{ie'}\omega_{i,t}.$$

By Proposition (5.1), we then have that $z \in \mathfrak{A}^\times_{H,\mathfrak{p}}$ if and only if the coefficients of these basis elements lie in $\mathfrak{O}_{K,\mathfrak{p}}$ and $\varepsilon(z) \in \mathfrak{O}^\times_{K,\mathfrak{p}}$. The details of the proof are lengthy but routine. □

Proposition (5.2) is analogous to [12, Proposition 5.1]. Owing to differences in notation, condition (iii) of Proposition (5.2) corresponds to the union of conditions (iii) and (iv) of [12, Proposition 5.1]. Note also that the $j = 0$ case of the congruences in part (ii) of Proposition (5.2) is identical to the $k = 0$ case of the congruences in condition (iii).

We now seek necessary and sufficient conditions for $z \in \mathfrak{A}_{H,\mathfrak{p}}^{\times}$ in terms of higher unit groups of $\mathfrak{O}_{K,\mathfrak{p}}$ and $\mathfrak{O}_{K(v),\mathfrak{p}}$.

Definition 5.3. Define an isomorphism

$$\Theta : (K^{\times})^p \times (K(v)^{\times})^{(p-1)} \cong H^{\times}$$

by composing the automorphism of $(K^{\times})^p \times (K(v)^{\times})^{(p-1)}$ defined by

$$(z_0, z_1, \ldots, z_{p-1}, y_1, \ldots y_{p-1}) \mapsto (z_0, z_0 z_1, \ldots, z_0 z_{p-1}, z_0 y_1, \ldots, z_0 y_{p-1})$$

with the explicit isomorphism $\Phi : K^p \times K(v)^{(p-1)} \to H$ defined in Definition (3.6). Thus given an element $(z_0, \ldots, z_{p-1}, y_1, \ldots, y_{p-1}) \in K^p \times K(v)^{p-1}$, we write $y_s = \sum_{t=0}^{p-1} w_{s,t} v^{st}$ with $w_{s,t} \in K$ for $s = 1, \ldots, p-1$ and $t = 0, \ldots, p-1$, and then we have

$$\Theta(z_0, \ldots, z_{p-1}, y_1, \ldots, y_{p-1}) = z_0 E_r \sum_{r=1}^{p-1} z_0 z_r E_r + \sum_{s=1}^{p-1} \sum_{t=0}^{p-1} z_0 w_{s,t} e_s (a_v \eta)^t.$$

We shall also write Θ for the induced isomorphism

$$(K_{\mathfrak{p}}^{\times})^p \times (K(v)_{\mathfrak{p}}^{\times})^{(p-1)} \cong H_{\mathfrak{p}}^{\times},$$

where $\mathfrak{p}$ a prime of $\mathfrak{O}_K$, and the isomorphism

$$\mathbb{J}(K)^p \times \mathbb{J}(K(v))^{(p-1)} \cong \mathbb{J}(H).$$

Proposition 5.4. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above p. Then

$$\Theta\left(\mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + p^2 \mathfrak{O}_{K,\mathfrak{p}})^{(p-1)} \times (1 + p^2 \mathfrak{O}_{K(v),\mathfrak{p}})^{(p-1)}\right) \subseteq \mathfrak{A}_{H,\mathfrak{p}}^{\times}.$$

Proof. The image under Θ of an element of

$$\mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + p^2 \mathfrak{O}_{K,\mathfrak{p}})^{(p-1)} \times (1 + p^2 \mathfrak{O}_{K(v),\mathfrak{p}})^{(p-1)}$$

has the form

$$z = \sum_{r=0}^{p-1} a_r E_r + \sum_{s=1}^{p-1} \sum_{t=0}^{p-1} a_{s,t} \left(\frac{e_s(a_v \eta) - e_s}{\pi_{\mathfrak{p}}^{e'}} \right)^t e_s$$

with $a_r, a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$ for $r, t = 0, \ldots, p-1$ and $s = 1, \ldots, p-1$, and

(a) $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$.
(b) $a_r \equiv a_0 \pmod{p^2 \mathfrak{O}_{K,\mathfrak{p}}}$ for $1 \leq r \leq p-1$.
(c) $a_{s,0} \equiv a_0 \pmod{p^2 \mathfrak{O}_{K,\mathfrak{p}}}$ for $1 \leq s \leq p-1$.
(d) $a_{s,t} \equiv 0 \pmod{p^2 \mathfrak{O}_{K,\mathfrak{p}}}$ for $1 \leq s, t \leq p-1$.

We show that z satisfies the conditions of Proposition (5.2).

By (d) we have $\pi_{\mathfrak{p}}^{-te'} a_{s,t} \equiv 0 \pmod{p\mathfrak{O}_{K,\mathfrak{p}}}$ for $1 \leq s, t \leq p-1$. So

$$\sum_{s=i}^{p-1}\sum_{t=j}^{p-1}\binom{s}{i}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \equiv 0 \pmod{p\mathfrak{O}_{K,\mathfrak{p}}},$$

which is sufficient to ensure that condition (i) of Proposition (5.2) holds.

By (b) and (d) we have, for $1 \leq j \leq p-1$, that

$$\begin{aligned}\sum_{r=0}^{p-1}\zeta^{jdr}a_r + p\sum_{s=1}^{p-1}\sum_{j=1}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}&\\ &\equiv \sum_{r=0}^{p-1}\zeta^{jdr}a_0 \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}}\\ &\equiv a_0\sum_{r=0}^{p-1}\zeta^{jdr} \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}}\\ &\equiv 0 \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}},\end{aligned}$$

so condition (ii) of Proposition (5.2) holds.

For $0 \leq k \leq p-1$ we have by (b),(c) and (d) that

$$\begin{aligned}\sum_{r=0}^{p-1}a_r + p\sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{-ks}(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t}&\\ &\equiv \sum_{r=0}^{p-1}a_0 + p\sum_{s=1}^{p-1}\zeta^{-ks}a_{s,0} \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}}\\ &\equiv pa_0 + p\sum_{s=1}^{p-1}\zeta^{-ks}a_0 \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}}\\ &\equiv pa_0\sum_{s=0}^{p-1}\zeta^{-ks} \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}}\\ &\equiv 0 \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}},\end{aligned}$$

so condition (iii) of Proposition (5.2) holds.

Condition (iv) of Proposition (5.2) holds by (a). □

Proposition 5.5. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above p. Then

$$\Theta^{-1}(\mathfrak{A}_{H,\mathfrak{p}}^{\times}) \subseteq \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1+(\zeta-1)\mathfrak{O}_{K,\mathfrak{p}})^{(p-1)} \times \left(1+(\zeta-1)\mathfrak{O}_{K(v),\mathfrak{p}}\right)^{(p-1)}.$$

Proof. Let

$$z=\sum_{r=0}^{p-1}a_rE_r+\sum_{s=1}^{p-1}\sum_{t=0}^{p-1}a_{s,t}\left(\frac{e_s(a_v\eta)-e_s}{\pi_{\mathfrak{p}}^{e'}}\right)^t e_s\in\mathfrak{M}_{H,\mathfrak{p}}$$

with $a_r, a_{s,t}\in\mathfrak{O}_{K,\mathfrak{p}}$ for $r,t=0,\dots,p-1$ and $s=1,\dots,p-1$, and suppose that $z\in\left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times$. Then the a_r and $a_{s,t}$ satisfy the conditions of Proposition (5.2) and, in particular, $a_0\in\mathfrak{O}_{K,\mathfrak{p}}^\times$. We shall show that this implies

$$\Theta^{-1}(z)\in\mathfrak{O}_{K,\mathfrak{p}}^\times\times(1+(\zeta-1)\mathfrak{O}_{K,\mathfrak{p}})^{(p-1)}\times\left(1+(\zeta-1)\mathfrak{O}_{K(v),\mathfrak{p}}\right)^{(p-1)}.$$

It is sufficient to prove that

(a) $a_r\equiv a_0 \pmod{(\zeta-1)\mathfrak{O}_{K,\mathfrak{p}}}$ for $0\le r\le p-1$.
(b) $a_{s,0}\equiv a_0 \pmod{(\zeta-1)\mathfrak{O}_{K,\mathfrak{p}}}$ for $1\le s\le p-1$.
(c) $a_{s,t}\equiv 0 \pmod{(\zeta-1)\mathfrak{O}_{K,\mathfrak{p}}}$ for $1\le s,t\le p-1$.

For each $s=1,\dots,p-1$ and $j=0,\dots,p-1$, define

$$A_{s,j}=\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}.$$

Using this notation, condition (i) of Proposition (5.2) becomes

$$\sum_{s=i}^{p-1}\binom{s}{i}A_{s,j}\equiv 0 \pmod{p\pi_{\mathfrak{p}}^{-ie'}\mathfrak{O}_{K,\mathfrak{p}}} \text{ for } 1\le i,j\le p-1.$$

If we consider the case $i=p-1$ then this becomes

$$A_{p-1,j}\in\mathfrak{O}_{K,\mathfrak{p}} \text{ for } 1\le j\le p-1,$$

and if we further specialize to the case $j=p-1$ then we have

$$\pi_{\mathfrak{p}}^{-(p-1)e'}a_{p-1,p-1}\in\mathfrak{O}_{K,\mathfrak{p}},$$

which is equivalent to

$$a_{p-1,p-1}\equiv 0 \pmod{p\mathfrak{O}_{K,\mathfrak{p}}}.$$

Now by considering decreasing values of j in turn we obtain

$$a_{p-1,t}\equiv 0 \pmod{\pi_{\mathfrak{p}}^{te'}\mathfrak{O}_{K,\mathfrak{p}}} \text{ for } 1\le t\le p-1.$$

Finally, considering decreasing values of i in a similar way yields

$$a_{s,t}\equiv 0 \pmod{\pi_{\mathfrak{p}}^{te'}\mathfrak{O}_{K,\mathfrak{p}}} \text{ for } 1\le s,t\le p-1,$$

which is sufficient to establish (c). In fact, we have shown that $\pi_{\mathfrak{p}}^{-te'}a_{s,t}\in\mathfrak{O}_{K,\mathfrak{p}}$ for $1\le t\le p-1$.

Next we establish (a). Summing the congruences in part (ii) of Proposition (5.2) over j with appropriate coefficients we have, for each $0 \leq r' \leq p-1$,

$$\begin{aligned}
&\sum_{j=0}^{p-1} \zeta^{-jdr'} \left(\sum_{r=0}^{p-1} \zeta^{jdr} a_r + p \sum_{s=1}^{p-1} A_{s,j} \right) \equiv 0 \pmod{p^2 \mathfrak{O}_{K,\mathfrak{p}}} \\
&\qquad \Rightarrow \sum_{r=0}^{p-1} \sum_{j=0}^{p-1} \zeta^{jd(r-r')} a_r + p \sum_{s=1}^{p-1} \sum_{j=0}^{p-1} \zeta^{-jdr'} A_{s,j} \equiv 0 \pmod{p^2 \mathfrak{O}_{K,\mathfrak{p}}} \\
&\qquad \Rightarrow a_{r'} + \sum_{s=1}^{p-1} \sum_{j=0}^{p-1} \zeta^{-jdr'} A_{s,j} \equiv 0 \pmod{p \mathfrak{O}_{K,\mathfrak{p}}}.
\end{aligned}$$

To simplify the double summation, note that for each $s = 1, \ldots, p-1$ we have

$$\begin{aligned}
\sum_{j=0}^{p-1} \zeta^{-jdr'} A_{s,j} &= \sum_{j=0}^{p-1} \zeta^{-jdr'} \sum_{t=j}^{p-1} \binom{t}{j} (-1)^{t-j} \pi_{\mathfrak{p}}^{-te'} a_{s,t} \\
&= \sum_{t=0}^{p-1} \sum_{j=0}^{t} \binom{t}{j} \zeta^{-jdr'} (-1)^{t-j} \pi_{\mathfrak{p}}^{-te'} a_{s,t} \\
&= \sum_{t=0}^{p-1} (\zeta^{-dr'} - 1)^t \pi_{\mathfrak{p}}^{-te'} a_{s,t} \\
&\equiv a_{s,0} \pmod{(\zeta - 1) \mathfrak{O}_{K,\mathfrak{p}}},
\end{aligned}$$

since we showed above that $\pi_{\mathfrak{p}}^{-te'} a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$ for $1 \leq s, t \leq p-1$. Therefore we have

$$a_{r'} + \sum_{s=1}^{p-1} a_{s,0} \equiv 0 \pmod{(\zeta - 1) \mathfrak{O}_{K,\mathfrak{p}}}$$

for any $r' = 0, \ldots, p-1$, which implies that all of the $a_{r'}$ are congruent to a_0 modulo $(\zeta - 1)\mathfrak{O}_{K,\mathfrak{p}}$, as claimed in (a).

To help us establish (b), we note first that we may view the congruences in part (i) of Proposition (5.2) as follows: for $1 \leq i, j, k \leq p-1$ we have

$$(\zeta^{-k} - 1)^i \sum_{s=i}^{p-1} \sum_{t=j}^{p-1} \binom{s}{i} \binom{t}{j} (-1)^{t-j} \pi_{\mathfrak{p}}^{-te'} a_{s,t} \equiv 0 \pmod{p \mathfrak{O}_{K,\mathfrak{p}}}.$$

Summing these congruences over all $1 \leq i, j \leq p-1$ and rewriting the inner summations using the binomial theorem gives us

$$\sum_{s=1}^{p-1} \sum_{t=1}^{p-1} (\zeta^{-sk} - 1)(-1)^t \pi_{\mathfrak{p}}^{-te'} a_{s,t} \equiv 0 \pmod{p \mathfrak{O}_{K,\mathfrak{p}}} \text{ for } 1 \leq k \leq p-1. \tag{5.1}$$

Using this, we establish (b). Summing the congruences in part (ii) of Proposition (5.2) gives us

$$\sum_{j=1}^{p-1}\sum_{r=0}^{p-1}\zeta^{jdr}a_r + p\sum_{s=1}^{p-1}\sum_{j=1}^{p-1}\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \equiv 0 \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}},$$

which reduces to

$$\sum_{j=1}^{p-1}\sum_{r=0}^{p-1}\zeta^{jdr}a_r - p\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t} \equiv 0 \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}}.$$

Adding to this one of the congruences from part (iii) of Proposition (5.2) gives

$$\sum_{j=0}^{p-1}\sum_{r=0}^{p-1}\zeta^{jdr}a_r + p\sum_{s=1}^{p-1}\zeta^{-ks}a_{s,0} + p\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}(\zeta^{-ks}-1)(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t} \equiv 0 \pmod{p^2\mathfrak{O}_{K,\mathfrak{p}}}$$

for each $k = 0, \ldots, p-1$. If $k = 0$ then the final term is zero, and if $k \neq 0$ then it is congruent to 0 modulo $p^2\mathfrak{O}_{K,\mathfrak{p}}$ by congruence (5.1). So we have

$$a_0 + \sum_{s=1}^{p-1}\zeta^{-ks}a_{s,0} \equiv 0 \pmod{p\mathfrak{O}_{K,\mathfrak{p}}} \text{ for } 0 \leq k \leq p-1,$$

and so for each $k = 0, \ldots, p-1$ there exists $c_k \in \mathfrak{O}_{K,\mathfrak{p}}$ such that

$$a_0 + \sum_{s=1}^{p-1}\zeta^{-ks}a_{s,0} = pc_k.$$

We therefore have

$$a_0 = \sum_{k=0}^{p-1} c_k$$

and

$$a_{s,0} = \sum_{k=0}^{p-1}\zeta^{ks}c_k \text{ for } 1 \leq s \leq p-1,$$

and so we have

$$\begin{aligned} a_{s,0} - a_0 &= \sum_{k=0}^{p-1}(\zeta^{ks}-1)c_k \\ &\equiv 0 \pmod{(\zeta-1)\mathfrak{O}_{K,\mathfrak{p}}} \text{ for } 1 \leq s \leq p-1. \end{aligned}$$

Thus $a_{s,0} \equiv a_0 \pmod{(\zeta-1)\mathfrak{O}_{K,\mathfrak{p}}}$, as claimed in (b). This completes the proof. □

By combining Propositions (5.4) and (5.5), we can "sandwich" the group of unit idèles $\mathbb{U}(\mathfrak{A}_H)$ between products of groups of unit idèles of fields, and so "sandwich" the free class group $\mathrm{Cl}\,(\mathfrak{A}_H)$ between products of ray class groups of fields:

Corollary 5.6. There are injections:

$$\begin{tikzcd}
\mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_{p^2}(\mathfrak{O}_K)^{(p-1)} \times \mathbb{U}_{p^2}(\mathfrak{O}_{K(v)})^{(p-1)} \arrow[d] \\
\mathbb{U}(\mathfrak{A}_H) \arrow[d] \\
\mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_{(\zeta-1)}(\mathfrak{O}_K)^{(p-1)} \times \mathbb{U}_{(\zeta-1)}(\mathfrak{O}_{K(v)})^{(p-1)}
\end{tikzcd}$$

and therefore surjections:

$$\begin{tikzcd}
\mathrm{Cl}\,(\mathfrak{O}_K) \times \mathrm{Cl}_{p^2}(\mathfrak{O}_K)^{(p-1)} \times \mathrm{Cl}_{p^2}(\mathfrak{O}_{K(v)})^{(p-1)} \arrow[d] \\
\mathrm{Cl}\,(\mathfrak{A}_H) \arrow[d] \\
\mathrm{Cl}\,(\mathfrak{O}_K) \times \mathrm{Cl}_{(\zeta-1)}(\mathfrak{O}_K)^{(p-1)} \times \mathrm{Cl}_{(\zeta-1)}(\mathfrak{O}_{K(v)})^{(p-1)}.
\end{tikzcd}$$

Next we compute an idèle whose class in $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$ corresponds to the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$:

Proposition 5.7. The class of $\mathfrak{O}_L$ in the locally free class group

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

corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ where:

$$h_{\mathfrak{p}} = \begin{cases} \displaystyle\sum_{r=0}^{p-1} E_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} \zeta^{std(t-1)/2} \upsilon^{-pq_{s,t}} e_s(a_v\eta)^t & \text{if } \mathfrak{p} \mid p\mathfrak{O}_K \\ \displaystyle\sum_{r=0}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^r)} E_r + \sum_{s=1}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} e_s(a_v\eta)^{j_{\mathfrak{p}}} & \text{otherwise.} \end{cases}$$

Here $q_{s,t} = \left\lfloor \frac{st}{p} \right\rfloor$ for $0 \leq s, t \leq p-1$ and $j_{\mathfrak{p}}$ is as defined in Definition (4.4).

Proof. Define

$$\Gamma = \frac{1}{p^2}\left(\sum_{j=0}^{p-1}\upsilon^j + \sum_{s=1}^{p-1}x^s\right) \in L^\times$$

Using the formulae in Corollary (3.12) for the action on elements of L of the elements $e_s(a_\upsilon\eta)^t$ ($s = 1, \ldots, p-1$ and $t = 0, \ldots, p-1$) and those in Proposition (3.13) for the action of the elements E_r ($r = 0, \ldots, p-1$), 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 $h_\mathfrak{p}\cdot\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. First suppose that $\mathfrak{p} \mid p\mathfrak{O}_K$. Then

$$\begin{aligned}
h_\mathfrak{p}\cdot\Gamma &= \sum_{r=0}^{p-1}E_r\cdot\Gamma + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{std(t-1)/2}\upsilon^{-pq_{s,t}}e_s(a_\upsilon\eta)^t\cdot\Gamma \\
&= \frac{1}{p^2}\left(\sum_{r=0}^{p-1}\upsilon^r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{std(t-1)/2}\upsilon^{-pq_{s,t}}e_s(a_\upsilon\eta)^t\cdot x^s\right) \\
&= \frac{1}{p^2}\left(\sum_{r=0}^{p-1}\upsilon^r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{std(t-1)/2}\zeta^{-std(t-1)/2}x^s\upsilon^{st-pq_{s,t}}\right) \\
&= \frac{1}{p^2}\left(\sum_{r=0}^{p-1}\upsilon^r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}x^s\upsilon^{\overline{st}}\right),
\end{aligned}$$

where $\overline{st}$ denotes the least positive residue of st modulo p. So in this case $h_\mathfrak{p}\cdot\Gamma$ coincides with the generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ given in Proposition (4.6).

Now suppose that $\mathfrak{p} \nmid p\mathfrak{O}_K$. Then

$$\begin{aligned}
h_\mathfrak{p}\cdot\Gamma &= \sum_{r=0}^{p-1}\pi_\mathfrak{p}^{-r_\mathfrak{p}(V^r)}E_r\cdot\Gamma + \sum_{s=1}^{p-1}\pi_\mathfrak{p}^{-r_\mathfrak{p}(X^sV^{sj_\mathfrak{p}})}e_s(a_\upsilon\eta)^{j_\mathfrak{p}}\cdot\Gamma \\
&= \frac{1}{p^2}\sum_{r=0}^{p-1}\pi_\mathfrak{p}^{-r_\mathfrak{p}(V^r)}\upsilon^r + \frac{1}{p^2}\sum_{s=1}^{p-1}\zeta^{-sj_\mathfrak{p}d(j_\mathfrak{p}-1)/2}\pi_\mathfrak{p}^{-r_\mathfrak{p}(X^sV^{sj_\mathfrak{p}})}x^s\upsilon^{sj_\mathfrak{p}}
\end{aligned}$$

whereas from Proposition (4.5) we have that a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ is

$$\gamma_\mathfrak{p} = \sum_{j=0}^{p-1}\pi_\mathfrak{p}^{-r_\mathfrak{p}(V^j)}\upsilon^j + \sum_{s=1}^{p-1}\pi_\mathfrak{p}^{-r_\mathfrak{p}(X^sV^{sj_\mathfrak{p}})}x^s\upsilon^{sj_\mathfrak{p}}.$$

Comparing these two, we see that

$$p^2\left(\sum_{r=0}^{p-1}E_r+\sum_{s=1}^{p-1}\zeta^{sj_{\mathfrak{p}}d(j_{\mathfrak{p}}-1)/2}e_s\right)(h_{\mathfrak{p}}\cdot\Gamma)=\gamma_{\mathfrak{p}}.$$

Since both p^2 and the second factor lie in $\mathfrak{A}_{H,\mathfrak{p}}^{\times}$, we have that $h_{\mathfrak{p}}\cdot\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. This completes the proof. □

The idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ corresponds under the isomorphism

$$\mathbb{J}(H)\cong\mathbb{J}(K)^p\times\mathbb{J}(K(v))^{(p-1)}$$

to a tuple of idèles, and this tuple in turn corresponds to a tuple of classes of fractional ideals via the usual map

$$\mathbb{J}(K)^p\times\mathbb{J}(K(v))^{(p-1)}\to\mathrm{Cl}\left(\mathfrak{O}_K\right)^p\times\mathrm{Cl}\left(\mathfrak{O}_{K(v)}\right)^{(p-1)}$$

In order to use the surjections of class groups of Proposition (5.6) to determine necessary and sufficient conditions for $\mathfrak{O}_L$ to be a free $\mathfrak{A}_H$-module, we must identify this tuple of classes of fractional ideals. First we define some notation:

Definition 5.8. For any $y\in K$, define a fractional ideal of K by

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

For each $s=1,\dots,p-1$ define an element $U_s\in K(v)^{\times}$ by

$$U_s=\sum_{t=0}^{p-1}\zeta^{std(t-1)/2}V^{-q_{s,t}}v^{st}\in K(v)^{\times}.$$

For each $s=1,\dots,p-1$ define a fractional ideal J_s of $K(v)$ by

$$J_s=\left(I_{X^s}^{-1}\prod_{\mathfrak{P}\nmid p\mathfrak{O}_{K(v)}}\mathfrak{P}^{-v_{\mathfrak{P}}(U_s)}\prod_{\mathfrak{P}|V\mathfrak{O}_{K(v)}}\mathfrak{P}^{v_{\mathfrak{p}}\left(V^{sj_{\mathfrak{p}}}\right)-pr_{\mathfrak{p}}(V^{sj_{\mathfrak{p}}})-p}\right).$$

Proposition 5.9. Under the composition of maps

$$\mathbb{J}(H)\cong\mathbb{J}(K)^p\times\mathbb{J}(K(v))^{(p-1)}\to\mathrm{Cl}\left(\mathfrak{O}_K\right)^p\times\mathrm{Cl}\left(\mathfrak{O}_{K(v)}\right)^{(p-1)},$$

the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ defined in Proposition (5.7) corresponds to the tuple of classes of fractional ideals

$$\left(\mathfrak{O}_K,I_V^{-1},\dots,I_{V^{(p-1)}}^{-1},J_1,\dots,J_{(p-1)}\right),$$

Proof. Under the isomorphism

$$\mathbb{J}(H)\to\mathbb{J}(K)^p\times\mathbb{J}(K(v))^{(p-1)}$$

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

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

where for $s = 1, \ldots, p-1$, the element $y_{s,\mathfrak{P}} \in K(v)_{\mathfrak{P}}$ is defined by

$$y_{s,\mathfrak{P}} = \begin{cases} \displaystyle\sum_{t=0}^{p-1} \zeta^{std(t-1)/2} V^{-q_{s,t}} v^{st} & \mathfrak{P} \mid p\mathfrak{O}_{K(v)} \\ \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} v^{sj_{\mathfrak{p}}} & \text{otherwise.} \end{cases}$$

Now for each $s = 1, \ldots, p-1$ we define an idèle $(y'_{s,\mathfrak{P}})_{\mathfrak{P}} \in \mathbb{J}(K(v))$ by

$$y'_{s,\mathfrak{P}} = U_s^{-1} y_{s,\mathfrak{P}} = \begin{cases} 1 & \mathfrak{P} \mid p\mathfrak{O}_{K(v)} \\ U_s^{-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} v^{sj_{\mathfrak{p}}} & \text{otherwise.} \end{cases}$$

Then the tuple of idèles

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

has the same class in the product $\mathrm{Cl}\,(\mathfrak{O}_K)^p \times \mathrm{Cl}\left(\mathfrak{O}_{K(v)}\right)^{(p-1)}$ as the tuple of idèles $\mathfrak{I}$. Mapping the tuple of idèles $\mathfrak{I}'$ to a tuple of fractional ideals, we see immediately that the first component is mapped to the trivial ideal, and that for $r = 2, \ldots, p$, the r^{th} component is mapped to the fractional ideal

$$I_{V^{r-1}}^{-1} = \prod_{\mathfrak{p} \mid V} \mathfrak{p}^{-r_{\mathfrak{p}}(V^{r-1})}.$$

To determine the images of the remaining components we calculate, for each $s \neq 0$ and $\mathfrak{P}$ a prime of $\mathfrak{O}_{K(v)}$, the valuation $v_{\mathfrak{P}}\left(y'_{s,\mathfrak{P}}\right)$. We have:

$$v_{\mathfrak{P}}\left(y'_{s,\mathfrak{P}}\right) = \begin{cases} 0 & \mathfrak{P} \mid p\mathfrak{O}_{K(v)} \\ -v_{\mathfrak{P}}\left(U_s\right) + v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} v^{sj_{\mathfrak{p}}} \right) & \text{otherwise.} \end{cases}$$

We observed after Definition (4.4) that $j_{\mathfrak{p}} \neq 0$ only if the prime $\mathfrak{p}$ of $\mathfrak{O}_K$ is ramified in the extension $K(v)/K$. In addition, we now observe that in this case we have

$$r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}}) = r_{\mathfrak{p}}(X^s) + r_{\mathfrak{p}}(V^{sj_{\mathfrak{p}}}) + 1,$$

and

$$pv_{\mathfrak{p}}\left(V\right) = v_{\mathfrak{P}}\left(V\right) = v_{\mathfrak{P}}\left(v^p\right) = pv_{\mathfrak{P}}\left(v\right).$$

Using these observations we see that if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ such that $j_{\mathfrak{p}} \neq 0$ and $\mathfrak{P}$ is a prime of $\mathfrak{O}_{K(v)}$ lying above $\mathfrak{p}$ then we have

$$\begin{aligned} v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} v^{sj_{\mathfrak{p}}}\right) &= -v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s)}\right) - v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{sj_{\mathfrak{p}}})+1}\right) + v_{\mathfrak{P}}\left(v^{sj_{\mathfrak{p}}}\right) \\ &= -v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s)}\right) - pr_{\mathfrak{p}}(V^{sj_{\mathfrak{p}}}) - p + v_{\mathfrak{p}}\left(V^{sj_{\mathfrak{p}}}\right). \end{aligned}$$

On the other hand, if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ such that $j_{\mathfrak{p}} = 0$ and $\mathfrak{P}$ is a prime of $\mathfrak{O}_{K(v)}$ lying above $\mathfrak{p}$ then we have

$$v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} v^{sj_{\mathfrak{p}}}\right) = v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s)}\right)$$

So we see that the idèle $(y'_{s,\mathfrak{P}})_{\mathfrak{P}}$ corresponds to the fractional ideal

$$J_s = \left(I_{X^s}^{-1} \prod_{\mathfrak{P} \nmid p\mathfrak{O}_{K(v)}} \mathfrak{P}^{-v_{\mathfrak{P}}(U_s)} \prod_{\mathfrak{P} | V\mathfrak{O}_{K(v)}} \mathfrak{P}^{v_{\mathfrak{p}}\left(V^{sj_{\mathfrak{p}}}\right) - pr_{\mathfrak{p}}(V^{sj_{\mathfrak{p}}}) - p} \right),$$

and so the tuple of idèles $\mathfrak{J}'$ corresponds to the tuple of fractional ideals

$$\left(\mathfrak{O}_K, I_V^{-1}, \ldots, I_{V^{(p-1)}}^{-1}, J_1, \ldots, J_{(p-1)}\right).$$

□

Proposition 5.10. A sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$ is that the tuple of fractional ideals

$$\left(\mathfrak{O}_K, I_V^{-1}, \ldots, I_{V^{(p-1)}}^{-1}, J_1, \ldots, J_{(p-1)}\right),$$

has trivial class in the product of ray class groups

$$\mathrm{Cl}\left(\mathfrak{O}_K\right) \times \mathrm{Cl}_{p^2}(\mathfrak{O}_K)^{(p-1)} \times \mathrm{Cl}_{p^2}(\mathfrak{O}_{K(v)})^{(p-1)}.$$

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

$$\mathrm{Cl}\left(\mathfrak{O}_K\right) \times \mathrm{Cl}_{(\zeta-1)}(\mathfrak{O}_K)^{(p-1)} \times \mathrm{Cl}_{(\zeta-1)}(\mathfrak{O}_{K(v)})^{(p-1)}.$$

Proof. By Proposition (5.7), the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\left(\mathfrak{A}_H\right)$ corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ in $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$, and by Proposition (5.9), this corresponds to the given tuple of fractional ideals. Recalling the surjections of Proposition (5.6), the result follows. □

References

[1] W. Bley & R. Boltje, "Lubin-Tate formal groups and module structure over Hopf orders", *J. Théor. Nombres Bordeaux* **11** (1999), no. 2, p. 269-305.

[2] N. P. Byott, "Uniqueness of Hopf Galois structure for separable field extensions", *Comm. Algebra* **24** (1996), no. 10, p. 3217-3228.

[3] ———, "Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications", *J. Théor. Nombres Bordeaux* **9** (1997), no. 1, p. 201-219.

[4] ———, “Integral Hopf-Galois structures on degree p^2 extensions of p-adic fields”, *J. Algebra* **248** (2002), no. 1, p. 334-365.

[5] L. N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000, viii+215 pages.

[6] C. W. Curtis & I. Reiner, *Methods of Representation Theory with Applications to Finite Groups and Orders (Volume 2)*, Pure and Applied Mathematics, John Wiley & Sons, 1987, XV+951 pages.

[7] A. Fröhlich, *Galois module structure of algebraic integers*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 1, Springer-Verlag, Berlin, 1983, x+262 pages.

[8] D. Hilbert, “Die Theorie der algebraischen Zahlkörper.”, *Jahresber. Dtsch. Math.-Ver.* **4** (1897), p. i-xviii + 175-546.

[9] M. J. Taylor, “On Fröhlich’s conjecture for rings of integers of tame extensions”, *Invent. Math.* **63** (1981), no. 1, p. 41-79.

[10] L. Thomas, “On the Galois module structure of extensions of local fields”, in *Actes de la Conférence “Fonctions L et Arithmétique”*, Publ. Math. Besançon Algèbre Théorie Nr., Lab. Math. Besançon, Besançon, 2010, p. 157-194.

[11] P. J. Truman, “Towards a generalisation of Noether’s theorem to nonclassical Hopf-Galois structures”, *New York J. Math.* **17** (2011), p. 799-810.

[12] ———, “Hopf-Galois module structure of tame biquadratic extensions”, *J. Théor. Nombres Bordeaux* **24** (2012), no. 1, p. 173-199.

[13] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York-Berlin, 1979, xi+164 pages.

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