CANONICAL NONCLASSICAL HOPF-GALOIS MODULE STRUCTURE OF NONABELIAN GALOIS EXTENSIONS

PAUL J. TRUMAN

Abstract. Let L/K be a finite Galois extension of local or global fields in any characteristic with nonabelian Galois group G, and let $\mathfrak{B}$ be an ambiguous ideal of L. We show that $\mathfrak{B}$ is free over its associated order in $K[G]$ if and only if it is free over its associated order in the Hopf algebra giving the canonical nonclassical Hopf-Galois structure on the extension.

1. Introduction and Statement of Results

Hopf-Galois module theory is a generalization of the classical Galois module theory of algebraic integers. Classically, we consider a finite Galois extension of local or global fields L/K with Galois group G. The group algebra $K[G]$ acts on L by

$$\left(\sum_{g\in G} c_g g\right)\cdot x = \sum_{g\in G} c_g g[x] \quad (c_g \in K,\ x \in L), \tag{1}$$

and the Normal Basis Theorem states that L is a free $K[G]$-module of rank 1. Motivated by this, we study the structure of the ring of algebraic integers (or valuation ring) $\mathfrak{O}_L$ as a module over its associated order in $K[G]$:

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

More generally, given any ambiguous ideal $\mathfrak{B}$ of L (i.e. a G-stable fractional ideal of L) we can define its associated order in $K[G]$ and study

2000 *Mathematics Subject Classification.* Primary 11R33; Secondary 11S23.

Key words and phrases. Hopf-Galois structure, Hopf-Galois module theory, Galois module structure, Associated order, Nonabelian extension.

the structure of $\mathfrak{B}$ as a module over its associated order. A survey of this topic can be found in [8].

The group algebra $K[G]$ is a Hopf algebra, and the action of $K[G]$ on L/K is an example of a so-called *Hopf-Galois structure* on the extension. If H is a K-Hopf algebra, then we say that H gives a Hopf-Galois structure on the extension L/K if L is an H-module algebra (see [3, §2]) and the K-linear map

$$j : L \otimes_K H \to \mathrm{End}_K L$$

defined by

$$j(s \otimes h)(t) = s(h \cdot t)$$

is a bijection. We call the Hopf-Galois structure given by $K[G]$ the classical structure. There may be a number of other K-Hopf algebras that give Hopf-Galois structures on L/K, and we call these nonclassical structures. Each of these Hopf-Galois structures provides a different context in which we can study the extension and its ambiguous ideals. A survey of this topic, focussing mainly on the consequences for $\mathfrak{O}_L$, can be found in [3]. If H is a Hopf algebra giving a Hopf-Galois structure on L/K then L is a free H-module of rank one [3, Theorem 2.15]; this a generalization of the classical Normal Basis Theorem and motivates us to ask analogous questions at integral level. Given an ambiguous ideal $\mathfrak{B}$ of L we can define within H the associated order of $\mathfrak{B}$:

$$\mathfrak{A}_H(\mathfrak{B}) = \{h \in H \mid h \cdot x \in \mathfrak{B} \text{ for all } x \in \mathfrak{B}\},$$

and study the structure of $\mathfrak{B}$ as a module over this associated order.

If the extension L/K admits a number of Hopf-Galois structures then we can compare the structure of $\mathfrak{B}$ as a module over its associated orders in the various Hopf algebras, and it is possible that we may achieve a more satisfactory description of $\mathfrak{B}$ as a module over some of these associated orders than over others. The most striking results in this direction are due to Byott [1], who exhibited examples of wildly

ramified Galois extensions L/K of p-adic fields for which $\mathfrak{O}_L$ is not free over its associated order in $K[G]$ but is free over its associated order in some Hopf algebra giving a nonclassical Hopf-Galois structure on the extension.

On the other hand, there are examples of extensions L/K of p-adic fields for which $\mathfrak{O}_L$ is free over its associated order in each of the Hopf-Galois structures admitted by the extension, or at least in certain families of these. For example, if L/K is unramified then $\mathfrak{O}_L$ is free over its associated order in each of the Hopf-Galois structures admitted by the extension [9, Theorem 1.1]. If the residue characteristic of K does not divide $[L : K]$ then L is free over its associated order in any commutative Hopf algebra giving a Hopf-Galois structure on L/K [9, Theorem 1.2]. If L/K is tamely ramified then $\mathfrak{O}_L$ is free over its associated order in any Hopf-Galois structure satisfying an additional technical hypothesis [11, Theorem 1.2]. Indeed, we are not aware of an example of a tamely ramified Galois extension of local fields L/K for which $\mathfrak{O}_L$ is not free over its associated order in each of the Hopf-Galois structures admitted by the extension.

Less is known concerning extensions of global fields, but in [10] we gave examples of tame abelian extensions $L/\mathbb{Q}$ for which $\mathfrak{O}_L$ is locally, but not globally, free over its associated order in some of the nonclassical Hopf-Galois structures admitted by the extension, demonstrating that the naïve generalization of the Hilbert-Speiser Theorem to nonclassical Hopf-Galois structures does not hold.

A theorem of Greither and Pareigis [3, Theorem 6.8] allows for the enumeration and description of all the Hopf-Galois structures admitted by a given Galois extension of fields. In fact, their theorem applies to field extensions which are separable but not necessarily normal, but in this paper we shall only consider Galois extensions. Let L/K be such

an extension, with Galois group G. Let $\mathrm{Perm}(G)$ denote the group of permutations of G, and let $\lambda : G \hookrightarrow \mathrm{Perm}(G)$ be the left regular embedding. Then the theorem of Greither and Pareigis asserts that the Hopf-Galois structures on L/K are in bijective correspondence with the regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$, that the Hopf algebra corresponding to a regular subgroup N is $H = L[N]^G$, where G acts on L as Galois automorphisms and on N by conjugation via the image of the embedding λ into $\mathrm{Perm}(G)$, and that such a Hopf algebra acts on L by

$$\left(\sum_{\eta\in N} c_\eta \eta\right) \cdot x = \sum_{\eta\in N} c_\eta \eta^{-1}(1_G)[x] \quad (c_\eta \in L,\ x \in L). \tag{2}$$

In general, the extension L/K may admit a number of nonclassical Hopf-Galois structures, and the corresponding regular subgroups N of $\mathrm{Perm}(G)$ need not all be isomorphic to G. Two examples of regular subgroups that are isomorphic to G are $\lambda(G)$ itself and $\rho(G)$, the image of G under the right regular embedding. The action of G on $\rho(G)$ by conjugation via the image of the embedding λ into $\mathrm{Perm}(G)$ is trivial, so $L[\rho(G)]^G \cong K[G]$, and from Equation (2) we recover the usual action of $K[G]$ on L, as described in (1) (see [3, Proposition 6.10]). If G is abelian then $\lambda(G)$ coincides with $\rho(G)$, but if G is nonabelian then these subgroups of $\mathrm{Perm}(G)$ are distinct and $\lambda(G)$ corresponds to nonclassical Hopf-Galois structure on L/K. We will call this the *Canonical Nonclassical Structure* and denote the corresponding Hopf algebra by H_λ. Since every nonabelian Galois extension admits a canonical nonclassical structure, and such a structure has close relationship with G, they are natural objects to study.

In this paper we will consider finite nonabelian Galois extensions of local and global fields and compare the descriptions provided by the classical structure and the canonical nonclassical structure. Our main result is the following:

Theorem 1.1. Let L/K be a finite nonabelian Galois extension of local fields or global fields in any characteristic with group G, and let $\mathfrak{B}$ be an ambiguous ideal of L. Then $\mathfrak{B}$ is free over its associated order in $K[G]$ if and only if it is free over its associated order in H_λ.

Retaining the hypotheses and notation of the theorem, we can state and prove the following corollaries:

Corollary 1.2. Suppose that L/K is an extension of local fields and is at most tamely ramified. Then $\mathfrak{O}_L$ is free over its associated order in H_λ.

Proof. In this case $\mathfrak{O}_L$ is a free $\mathfrak{O}_K[G]$-module by Noether's Theorem [5, Theorem 3], so $\mathfrak{A}_{K[G]} = \mathfrak{O}_K[G]$ and Theorem 1.1 applies. □

Corollary 1.3. Suppose that L/K is an extension of global fields and is at most tamely ramified. Then $\mathfrak{O}_L$ is locally free over its associated order in H_λ.

Proof. The proof of Theorem 1.1 does not depend on the fact that L is a field, so we may replace L with its completion at some prime $\mathfrak{p}$ of $\mathfrak{O}_K$ (a Galois algebra). In this case, for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ we have that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{O}_{K,\mathfrak{p}}[G]$-module by Noether's Theorem, so as above $\mathfrak{A}_{K[G],\mathfrak{p}} = \mathfrak{O}_{K,\mathfrak{p}}[G]$ for each prime. Hence Theorem 1.1 applies at each prime, and so $\mathfrak{O}_L$ is locally free over its associated order in H_λ. □

Corollary 1.4. Suppose that $K = \mathbb{Q}$, that $L/\mathbb{Q}$ is tamely ramified and that $[L : \mathbb{Q}]$ is not divisible by 4. Then $\mathfrak{O}_L$ is free over its associated order in H_λ.

Proof. In this case $\mathfrak{O}_L$ is a free $\mathbb{Z}[G]$-module by Taylor's Theorem [7], so $\mathfrak{A}_{K[G]} = \mathbb{Z}[G]$ and Theorem 1.1 applies. □

Corollary 1.5. Suppose that L/K is an extension of p-adic fields which is weakly ramified. Then $\mathfrak{O}_L$ is free over its associated order in H_λ.

Proof. In this case $\mathfrak{O}_L$ is free over its associated order in $K[G]$ by a Theorem of Johnston [6], so Theorem 1.1 applies. □

We will prove Theorem 1.1 in section 4, using properties of the canonical nonclassical Hopf-Galois structure H_λ that will be developed in sections 2 and 3. In section 2 we show that an element $x \in L$ generates L as a $K[G]$-module if and only if it generates L as an H_λ-module. In section 3 we study the relationship between the action of H_λ on L and the action of G on L, and in particular connections with the trace form on L/K.

2. Normal Basis Generators

In this section we continue to assume that L/K is a finite Galois extension of fields with Galois group G, but we do not assume that the extension is of local or global fields. Although we will be primarily interested in the canonical nonclassical Hopf-Galois structure on a nonabelian extension, many of the results in this section are valid more generally, and so we will only assume that G is nonabelian when it is necessary to do so. If H is a Hopf algebra giving a Hopf-Galois structure on L/K then, as noted in the introduction, L is a free H-module of rank one. However, to our knowledge the only results comparing explicit generators of L as a module over the various Hopf algebras giving Hopf-Galois structures on L/K are those appearing in [2], which are concerned with the valuation criterion for normal basis generators in characteristic p. We shall prove the following theorem:

Theorem 2.1. Suppose that G is nonabelian and let $x \in L$. Then x is a $K[G]$-generator of L if and only if x is an H_λ-generator of L.

To do this, we recall some elements of the proof of the theorem of Greither and Pareigis, as detailed in [3, §6]. Let $M = \mathrm{Map}(G, L)$, and let $\{u_g \mid g \in G\}$ be an L-basis of mutually orthogonal idempotents. That is:

$$u_g(\sigma) = \delta_{g,\sigma} \text{ for all } g, \sigma \in G.$$

It can be shown [3, Theorem 6.3] that the L-Hopf algebras giving Hopf-Galois structures on the extension of rings M/L are precisely the group

algebras LN of regular subgroups N of $\mathrm{Perm}(G)$, where the group N acts on M by permuting the subscripts of the idempotents u_g:

$$\eta \cdot u_g = u_{\eta(g)} \text{ for any } \eta \in N \text{ and } g \in G.$$

If in addition N is normalized by $\lambda(G)$ then the group G acts on $L[N]$ by acting on L as Galois automorphisms and on N by conjugation via the image of the embedding λ into $\mathrm{Perm}(G)$. It also acts on M by acting on L as Galois automorphisms and on the idempotents u_g by left translation of the subscripts. Now by Galois descent we obtain that the K-Hopf algebra $L[N]^G$ gives a Hopf-Galois structure on the extension of rings M^G/K. Note also that $L \otimes_K L[N]^G = L[N]$ and $L \otimes_K M^G = M$. Finally, we may identify L with the fixed ring M^G via the K-algebra isomorphism $L \xrightarrow{\sim} M^G$ defined by

$$x \mapsto f_x = \sum_{g \in G} g(x) u_g \text{ for all } x \in L,$$

and so $L[N]^G$ gives a Hopf-Galois structure on L/K, with the action of $L[N]^G$ on L as given in equation (2). The theorem of Greither and Pareigis asserts that all the Hopf-Galois structures admitted by L/K occur in this way and, as we have already remarked, provides a similar classification of Hopf-Galois structures on separable but non-normal extensions.

With this notation to hand, we establish two lemmas concerning normal basis generators and then prove Theorem 2.1.

Lemma 2.2. Let N be a regular subgroup of $\mathrm{Perm}(G)$, so that $L[N]^G$ is a K-Hopf algebra giving a Hopf-Galois structure on M^G/K. An element $f_x \in M^G$ is an $L[N]^G$-generator of M^G if and only if it is an $L[N]$-generator of M.

Proof. Let $\{h_1, \ldots, h_n\}$ be a K-basis of $L[N]^G$, and note that since $L[N] = L \otimes_K L[N]^G$, it is also an L-basis of $L[N]$. Suppose first that f_x is an $L[N]^G$ generator of M^G. Then the K-span of the elements $h_1 \cdot f_x, \ldots, h_n \cdot f_x$ is M^G, so the L-span of these elements is $L \otimes_K M^G =$

M. By considering dimensions we see that they must form an L-basis of M. Conversely, suppose that f_x is an $L[N]$-generator of M. Then the elements $h_1 \cdot f_x, \ldots, h_n \cdot f_x$ are linearly independent over L, so they are linearly independent over K, and since M^G is an $L[N]^G$-module they all lie in M^G. Considering dimensions again, we conclude that they must form a K-basis of M^G. □

Lemma 2.3. Fix orderings of the groups G and N. For $x \in L$, the element f_x is an $L[N]$-generator of M if and only if the matrix

$$T_N(x) = (\eta(g)[x])_{\eta \in N,\, g \in G}$$

is nonsingular.

We note that the definition of the matrix $T_N(x)$ depends on the orderings of G and N, but the question of whether it is nonsingular does not.

Proof. The set $\{u_g \mid g \in G\}$ is an L-basis of M. For $x \in L$ and $\eta \in N$, we have

$$\begin{aligned} \eta \cdot f_x &= \eta \cdot \left(\sum_{g \in G} g(x) u_g \right) \\ &= \sum_{g \in G} g(x) u_{\eta(g)} \\ &= \sum_{g \in G} \eta^{-1}(g)[x] u_g. \end{aligned}$$

Therefore the transition matrix from the set $\{u_g \mid g \in G\}$ to the set $\{\eta \cdot f_x \mid \eta \in N\}$ is row equivalent to the matrix $T_N(x)$ defined above, and so f_x is an $L[N]$-generator of M if and only if this matrix is nonsingular. □

Proof of Theorem 2.1. Recall that G is assumed to be nonabelian. By the theorem of Greither and Pareigis the classical Hopf-Galois structure on L/K corresponds to the regular subgroup $\rho(G)$ of $\mathrm{Perm}(G)$ and the canonical nonclassical Hopf-Galois structure corresponds to the regular subgroup $\lambda(G)$. By Lemma 2.2, it is sufficient to show that for a fixed

$x \in L$, the element f_x is an $L[\lambda(G)]$-generator of M if and only if it is an $L[\rho(G)]$-generator of M. For any $\sigma, \tau \in G$ we have $\lambda(\sigma)\tau = \sigma\tau$ and $\rho(\sigma)\tau = \tau\sigma^{-1}$. Therefore for any $x \in L$, the matrix $T_{\lambda(G)}(x)$ is row equivalent to the transpose of the matrix $T_{\rho(G)}(x)$, so the result follows by Lemma 2.3. □

3. The action of H_λ on L

In this section we assume that L/K is a nonabelian Galois extension of fields with group G, and let H_λ denote the Hopf algebra giving the canonical nonclassical Hopf-Galois structure on L/K, acting via equation (2). Henceforth, we reserve the symbol $\cdot$ for the action of an element $h \in H_\lambda$ on an element $x \in L$, viz. $h \cdot x$, and use parentheses for Galois actions and the action of an element $z \in K[G]$ on an element $x \in L$, viz. $z(x)$. Recall that the trace from L to K induces a nondegenerate associative symmetric K-bilinear form on L, and so given any K-basis of L we may form a dual basis with respect to the trace form. Identities involving the trace form will play an important part in the proof of Theorem 1.1 in section 4. The first two lemmas of this section concern the dual basis of a normal basis with respect to the trace form.

Lemma 3.1. Let x be a $K[G]$-generator of L, so that $\{\sigma(x) \mid \sigma \in G\}$ is a K-basis of L, and let $\{\widehat{\sigma(x)} \mid \sigma \in G\}$ be the dual basis with respect to the trace form on L/K. Then, for each $\sigma \in G$, we have $\widehat{\sigma(x)} = \sigma(\widehat{x})$.

Proof. For $\sigma, \tau \in G$ we have:

$$\begin{aligned}
\mathrm{Tr}_{L/K}(\sigma(\widehat{x})\tau(x)) &= \sum_{g\in G} g(\sigma(\widehat{x})\tau(x)) \\
&= \sum_{g\in G} g\sigma(\widehat{x})g\tau(x) \\
&= \sum_{g\in G} (g\sigma)(\widehat{x})(g\sigma)\sigma^{-1}\tau(x) \\
&= \sum_{g\in G} (g\sigma)(\widehat{x}\sigma^{-1}\tau(x)) \\
&= \sum_{g\in G} g(\widehat{x}\sigma^{-1}\tau(x)) \\
&= \mathrm{Tr}_{L/K}(\widehat{x}\sigma^{-1}\tau(x)) \\
&= \delta_{1,\sigma^{-1}\tau} \\
&= \delta_{\sigma,\tau}.
\end{aligned}$$

Since the elements of the dual basis are uniquely determined by the equations

$$\mathrm{Tr}_{L/K}(\widehat{\sigma(x)}\tau(x)) = \delta_{\sigma,\tau},$$

we must have $\widehat{\sigma(x)} = \sigma(\widehat{x})$. This completes the proof. □

We might view the second lemma as an "inside out" version of the first:

Lemma 3.2. Retain the notation of Lemma 3.1. Then for any $\sigma, \tau \in G$ we have

$$\sum_{g\in G} \sigma g(\widehat{x})\tau g(x) = \delta_{\sigma,\tau}.$$

Proof. Enumerate the elements of G as $g_1, \ldots, g_n$, let X be the matrix with (i,j) entry $g_i g_j(x)$, and let $\widehat{X}$ be the matrix with (i,j) entry $g_j g_i(\widehat{x})$. Using Lemma 3.1 we have

$$\sum_{k=1}^{n} g_k g_i(\widehat{x}) g_k g_j(x) = \delta_{i,j},$$

so $\widehat{X}X = I$. But this implies that $X\widehat{X} = I$, and the (i, j) entry of this product is given by

$$\sum_{k=1}^{n} g_i g_k(x) g_j g_k(\widehat{x}),$$

so this must also equal $\delta_{i,j}$. The result follows on setting $\sigma = g_i$, $\tau = g_j$. □

The final lemma in this section concerns the relationship between the action of H_λ on L and the action of $K[G]$. Recall that $\lambda(G)$ is the image in $\mathrm{Perm}(G)$ of G under the left regular embedding and that Hopf algebra $H_\lambda = L[\lambda(G)]^G$ acts on L via equation (2). Therefore if $h = \sum_{g\in G} c_g \lambda(g) \in H_\lambda$ and $t \in L$ then

$$\begin{aligned} h \cdot t &= \left(\sum_{g\in G} c_g \lambda(g)\right) \cdot t \\ &= \sum_{g\in G} c_g \lambda(g)^{-1}(1_G)[t] \\ &= \sum_{g\in G} c_g g^{-1}[t]. \end{aligned} \tag{3}$$

Lemma 3.3. Let $t \in L$, $z \in K[G]$ and $h \in H_\lambda$. Then

$$h \cdot z(t) = z(h \cdot t).$$

Proof. Recall that G acts on $L[\lambda(G)]$ by acting on L as Galois automorphisms and on $\lambda(G)$ by conjugation via the image of the embedding λ into $\mathrm{Perm}(G)$. The map $T : L[\lambda(G)] \to L[\lambda(G)]^G = H_\lambda$ defined by

$$z \mapsto \sum_{g\in G} {}^g z$$

is K-linear and surjective, so it is sufficient to consider the case in which $h = T(y\lambda(\tau))$ for some $y \in L$ and $\tau \in G$, and $z = \sigma \in G$. In

this case we have:

$$\begin{aligned}
\sigma(T(y\lambda(\tau))\cdot t) &= \sigma\left(\sum_{g\in G} g(y)\,{}^g\lambda(\tau)\cdot t\right)\\
&= \sigma\left(\sum_{g\in G} g(y)\lambda(g\tau g^{-1})\cdot t\right)\\
&= \sigma\left(\sum_{g\in G} g(y)g\tau^{-1}g^{-1}(t)\right) \text{ by Equation (3)}\\
&= \sum_{g\in G} \sigma g(y)\sigma g\tau^{-1}g^{-1}(t)\\
&= \sum_{g\in G} \sigma g(y)\sigma g\tau^{-1}g^{-1}\sigma^{-1}\sigma(t)\\
&= \sum_{g\in G} \sigma g(y)\,{}^{(\sigma g)}\lambda(\tau)\cdot\sigma(t) \text{ by Equation (3)}\\
&= \sum_{g\in G} g(y)\,{}^g\lambda(\tau)\cdot\sigma(t)\\
&= T(y\lambda(\tau))\cdot\sigma(t),
\end{aligned}$$

as claimed. □

4. Proof of the Main Theorem

In this section we assume that L/K is a nonabelian Galois extension of local or global fields with group G. Note, however, that we make no restriction on the characteristic of K. Let $\mathfrak{B}$ be an ambiguous ideal of L. Write $\mathfrak{A}_{K[G]}$ for the associated order of $\mathfrak{B}$ in $K[G]$ and $\mathfrak{A}_\lambda$ for the associated order of $\mathfrak{B}$ in H_λ. We shall split the "if" and "only if" implications of Theorem 1.1 into two separate propositions.

Proposition 4.1. Suppose that $x \in \mathfrak{B}$ generates $\mathfrak{B}$ as an $\mathfrak{A}_{K[G]}$-module. Then x generates $\mathfrak{B}$ as a $\mathfrak{A}_\lambda$-module.

Proof. Since x generates $\mathfrak{B}$ as an $\mathfrak{A}_{K[G]}$-module, it generates L as a $K[G]$-module, so $\{\sigma(x) \mid \sigma \in G\}$ is a K-basis of L. By Lemma 3.1, there exists $\widehat{x} \in L$ such that $\{\sigma(\widehat{x}) \mid \sigma \in G\}$ is the dual basis to

$\{\sigma(x) \mid \sigma \in G\}$ with respect to the trace form. That is:

$$\sum_{g \in G} g\sigma(\widehat{x})g\tau(x) = \delta_{\sigma,\tau} \text{ for all } \sigma, \tau \in G.$$

Also, there exist $a_1, \ldots, a_n \in \mathfrak{A}_{K[G]}$ such that $\{a_1(x), \ldots, a_n(x)\}$ is an $\mathfrak{O}_K$-basis of $\mathfrak{B}$. For each $i = 1, \ldots, n$, write $x_i = a_i(x)$ and define an element $h_i \in L[\lambda(G)]$ by

$$h_i = \sum_{g \in G} \left(\sum_{\theta \in G} \theta(x_i) g^{-1} \theta(\widehat{x}) \right) \lambda(g).$$

For each $i = 1, \ldots, n$ we make three claims about the element h_i:

(a) $h_i \in L[\lambda(G)]^G = H_\lambda$, and so we may let h_i act on elements of L according to equation (2),
(b) $h_i \cdot x = x_i$,
(c) $h_i \in \mathfrak{A}_\lambda$.

If we can establish these three claims, then it will follow that $\{h_i \mid i = 1, \ldots, n\}$ is an $\mathfrak{O}_K$-basis of $\mathfrak{A}_\lambda$ and that $\mathfrak{B}$ is a free $\mathfrak{A}_\lambda$-module.

To prove (a), let $\tau \in G$. Then

$$\begin{aligned}
{}^{\tau}h_i &= {}^{\tau}\left(\sum_{g\in G}\left(\sum_{\theta\in G}\theta(x_i)g^{-1}\theta(\widehat{x})\right)\lambda(g)\right)\\
&= \sum_{g\in G}\tau\left(\sum_{\theta\in G}\theta(x_i)g^{-1}\theta(\widehat{x})\right){}^{\tau}\lambda(g)\\
&= \sum_{g\in G}\left(\sum_{\theta\in G}\tau\theta(x_i)\tau g^{-1}\theta(\widehat{x})\right)\lambda(\tau g\tau^{-1})\\
&= \sum_{g'\in G}\left(\sum_{\theta\in G}\tau\theta(x_i)(g')^{-1}\tau\theta(\widehat{x})\right)\lambda(g')\\
&\quad \text{(writing } g' = \tau g\tau^{-1}, \text{ so that } \tau g^{-1} = (g')^{-1}\tau)\\
&= \sum_{g\in G}\left(\sum_{\theta\in G}\tau\theta(x_i)g^{-1}\tau\theta(\widehat{x})\right)\lambda(g)\\
&\quad \text{(replacing } g' \text{ by } g)\\
&= \sum_{g\in G}\left(\sum_{\theta\in G}\theta(x_i)g^{-1}\theta(\widehat{x})\right)\lambda(g)\\
&\quad \text{(replacing } \tau\theta \text{ by } \theta)\\
&= h_i,
\end{aligned}$$

so $h_i \in L[\lambda(G)]^G = H_\lambda$.

Now we know that it makes sense to let h_i act on $x \in L$ according

to equation (2), and so we can prove (b):

$$\begin{aligned} h_i \cdot x &= \left(\sum_{g \in G} \left(\sum_{\theta \in G} \theta(x_i) g^{-1} \theta(\widehat{x}) \right) \lambda(g) \right) \cdot x \\ &= \sum_{g \in G} \left(\sum_{\theta \in G} \theta(x_i) g^{-1} \theta(\widehat{x}) \right) g^{-1}(x) \\ &= \sum_{\theta \in G} \theta(x_i) \left(\sum_{g \in G} g^{-1} \theta(\widehat{x}) g^{-1}(x) \right) \\ &= \sum_{\theta \in G} \theta(x_i) \mathrm{Tr}_{L/K}(\theta(\widehat{x}) x) \\ &= \sum_{\theta \in G} \theta(x_i) \delta_{\theta,1} \text{ (using Lemma 3.1)} \\ &= x_i. \end{aligned}$$

Finally, we prove (c). It is sufficient to prove that $h_i \cdot x_j \in \mathfrak{B}$ for each $j = 1, \ldots, n$. Recall that $x_j = a_j(x)$ for some $a_j \in \mathfrak{A}_{K[G]}$. Using Lemma 3.3 we have:

$$\begin{aligned} h_i \cdot x_j &= h_i \cdot a_j(x) \\ &= a_j(h_i \cdot x) \\ &= a_j(x_i), \end{aligned}$$

and this lies in $\mathfrak{B}$ since $x_i \in \mathfrak{B}$ and $a_j \in \mathfrak{A}_{K[G]}$.

We have verified all three claims, and so the proof is complete. □

The next proposition is the converse of the previous one:

Proposition 4.2. Suppose that $x \in \mathfrak{B}$ generates $\mathfrak{B}$ as an $\mathfrak{A}_\lambda$-module. Then x generates $\mathfrak{B}$ as an $\mathfrak{A}_{K[G]}$-module.

Proof. Since x generates $\mathfrak{B}$ as an $\mathfrak{A}_\lambda$-module, it generates L as an H_λ-module, and so by Theorem 2.1 it generates L as a $K[G]$-module. Therefore $\{\sigma(x) \mid \sigma \in G\}$ is a K-basis of L and by Lemma 3.1 there exists $\widehat{x} \in L$ such that $\{\sigma(\widehat{x}) \mid \sigma \in G\}$ is the dual basis to $\{\sigma(x) \mid \sigma \in G\}$ with respect to the trace form. Analogously to the proof of Proposition 4.1, there exist $h_1, \ldots, h_n \in \mathfrak{A}_\lambda$ such that $\{h_1 \cdot x, \ldots, h_n \cdot x\}$

is an $\mathfrak{O}_K$-basis of $\mathfrak{B}$. For each $i = 1, \ldots, n$, write $x_i = h_i \cdot x$ and define an element $a_i \in K[G]$ by

$$a_i = \sum_{g \in G} \mathrm{Tr}_{L/K}(x_i g(\widehat{x}))g.$$

In this case it is clear that $a_i \in K[G]$, so a_i acts on elements of L, and we make two claims about each a_i:

(a) $a_i(x) = x_i$.

(b) $a_i \in \mathfrak{A}_{K[G]}$.

Analogously to the proof of Proposition 4.1, if we can establish these claims then it will follow that $\{a_i \mid i = 1, \ldots, n\}$ is an $\mathfrak{O}_K$-basis of $\mathfrak{A}_{K[G]}$ and that $\mathfrak{B}$ is a free $\mathfrak{A}_{K[G]}$-module.

First we prove (a). We have:

$$\begin{aligned} a_i(x) &= \sum_{g \in G} \mathrm{Tr}_{L/K}(x_i g(\widehat{x}))g(x) \\ &= \sum_{g \in G} \sum_{\sigma \in G} \sigma(x_i)\sigma g(\widehat{x})g(x) \\ &= \sum_{\sigma \in G} \sigma(x_i) \sum_{g \in G} \sigma g(\widehat{x})g(x) \\ &= \sum_{\sigma \in G} \sigma(x_i)\delta_{\sigma,1} \text{ (using Lemma 3.2)} \\ &= x_i. \end{aligned}$$

To prove (b), it is sufficient to prove that $a_i(x_j) \in \mathfrak{B}$ for each $j = 1, \ldots, n$. Recall that $x_j = h_j \cdot x$ for some $h_j \in \mathfrak{A}_\lambda$. Using Lemma 3.3 we have:

$$\begin{aligned} a_i(x_j) &= a_i(h_j \cdot x) \\ &= h_j \cdot (a_i(x)) \\ &= h_j \cdot x_i, \end{aligned}$$

and this lies in $\mathfrak{B}$ since $x_i \in \mathfrak{B}$ and $h_j \in \mathfrak{A}_\lambda$.

We have verified both the claims, and so the proof is complete. □

By combining Propositions 4.1 and 4.2, we obtain Theorem 1.1.

5. Possible Generalizations and Further Questions

In the course of proving Theorem 1.1, we showed that if $\mathfrak{B}$ is free over one (and therefore both) of $\mathfrak{A}_{K[G]}$ and $\mathfrak{A}_\lambda$ then we can write down an $\mathfrak{O}_K$-basis for one of these orders in terms of an $\mathfrak{O}_K$-basis for the other. We might wonder what properties these orders share in this case. For example: if one is a maximal order or a Hopf order, must the other also have this property? This might be particularly interesting in the case of tame extensions, since in this case $\mathfrak{A}_{K[G]} = \mathfrak{O}_K[G]$, which is certainly a Hopf order in $K[G]$.

It is possible that L/K may admit a number of Hopf-Galois structures whose Hopf algebras are isomorphic to H_λ and which act on L via Equation (2). From a different point of view, we may consider each of these as a different action of the Hopf algebra H_λ on L. In particular, Childs [4] has shown that certain fixed point free endomorphisms of G yield different actions of H_λ on L. It would be natural to investigate whether Theorem 1.1 generalizes to these Hopf-Galois structures.

The focus of this paper has been on ambiguous ideals $\mathfrak{B}$ of L, since in this case the associated orders of $\mathfrak{B}$ in $K[G]$ and in H_λ are both defined. If L/K is a Galois extension of local fields then every fractional ideal of L is ambiguous, but in the case of global fields we might ask whether it is possible for a fractional ideal $\mathfrak{B}$ of L which is not ambiguous to have an associated order in H_λ. We are grateful to the referee for raising this question, as it suggests the potential broader applicability of nonclassical Hopf-Galois structures in this context.

References

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

2. Byott, N. P. (2011), A valuation criterion for normal basis generators of Hopf-Galois extensions in characteristic p. *Journal de théorie des nombres de Bordeaux* 23.1, 59-70.
3. Childs, L. N. (2000), *Taming Wild Extensions: Hopf algebras and local Galois module theory,* American Mathematical Society.
4. Childs, L. N. (2013), Fixed-point free endomorphisms and Hopf Galois structures. *Proceedings of the American Mathematical Society* 141.4, 1255-1265.
5. Fröhlich, A. (1983), *Galois Module Structure of Algebraic Integers*, Springer.
6. Johnstone, H., Explicit integral Galois module structure of weakly ramified extensions of local fields. *arXiv*:1204.2133v3 [math.NT].
7. Taylor, M. J. (1981), On Fröhlich's Conjecture for Rings of Integers of Tame Extensions. *Inventiones mathematicae* 63, 41-79.
8. Thomas, L. (2010), On the Galois module structure of extensions of local fields. *Publ. Math. Besançon*, 157-194.
9. Truman, P. J. (2011), Towards a generalisation of Noethers Theorem to non-classical Hopf-Galois structures. *New York J. Math*, 17, 799-810.
10. Truman, P. J. (2012), Hopf-Galois module structure of tame biquadratic extensions. *Journal de théorie des nombres de Bordeaux*, 24(1), 173-199.
11. Truman, P. J. (2013), Integral Hopf-Galois structures for tame extensions. *New York J. Math*, 19, 647-655.

School of Computing and Mathematics, Keele University, Staffordshire, ST5 5BG, UK

E-mail address: P.J.Truman@Keele.ac.uk