

COMMUTING HOPF-GALOIS STRUCTURES ON A SEPARABLE EXTENSION

PAUL J. TRUMAN

ABSTRACT. Let L/K be a finite separable extension of local or global fields in any characteristic, let H_1, H_2 be two Hopf algebras giving Hopf-Galois structures on the extension, and suppose that the actions of H_1, H_2 on L commute. We show that a fractional ideal \mathfrak{B} of L is free over its associated order in H_1 if and only if it is free over its associated order in H_2 . We also study which properties these associated orders share.

1. INTRODUCTION AND STATEMENT OF RESULTS

This paper is a sequel to [8]. In the introduction to that paper, we described one of the ways in which Hopf-Galois module theory generalizes the classical Galois module theory of algebraic integers: if L/K is a finite Galois extension of local or global fields with Galois group G then the action of the group algebra $K[G]$ on L is an example of a *Hopf-Galois structure* on the extension L/K ([2, Definition 2.7]), but the extension may admit a number of other Hopf-Galois structures, and each of these provides a different context in which we can ask module theoretic questions about the extension and its fractional ideals. If H is a Hopf algebra giving a Hopf-Galois structure on L/K then L is a free H -module of rank 1 ([2, Proposition 2.15]), and if \mathfrak{B} is a fractional ideal of L then we can define the associated order of \mathfrak{B} in H :

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

and compare the structure of \mathfrak{B} as a module over its associated orders in the various Hopf algebras. The most interesting case is $\mathfrak{B} = \mathfrak{D}_L$, the ring of algebraic integers of L , since there exist Galois extensions L/K of p -adic fields for which \mathfrak{D}_L is not free over its associated order in the group algebra $K[G]$ but is free over its associated order in some Hopf algebra giving a different Hopf-Galois structure on the extension ([1]). On the other hand, there exist extensions admitting multiple Hopf-Galois structures for which \mathfrak{D}_L is free over its associated

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

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

order in each of the corresponding Hopf algebras ([6]). Another way in which Hopf-Galois module theory generalizes classical Galois module theory is that a finite separable, but non-normal, extension L/K of local or global fields may admit Hopf-Galois structures; here of course the techniques of classical Galois module theory are not available, but these Hopf-Galois structures allow us to study such extensions and their fractional ideals, as described above. The results of this paper are concerned with comparing the structure of a fractional ideal \mathfrak{B} of L as a module over its associated orders in the various Hopf algebras giving Hopf-Galois structures on L/K .

A theorem of Greither and Pareigis ([4, Theorem 3.1] or [2, Theorem 6.8]) enumerates and describes all of the Hopf-Galois structures admitted by a given finite separable extension of fields L/K , as follows: let E/K be the Galois closure of L/K , $G = \text{Gal}(E/K)$, and $G_L = \text{Gal}(E/L)$. Now let X be the left coset space of G_L in G , and $B = \text{Perm}(X)$. Then the Hopf-Galois structures on L/K are in bijective correspondence with the regular subgroups of B normalized by the image of G under the embedding $\lambda : G \rightarrow B$ defined by $\lambda(\sigma)gG_L = \sigma gG_L$. (Recall that a subgroup of B is called *regular* if it has the same order as X and is transitive on X .) Furthermore, the Hopf algebra corresponding to a regular subgroup N is $E[N]^G$, where G acts on E as Galois automorphisms and on N by conjugation via the embedding λ :

$$(1) \quad {}^g\eta = \lambda(g)\eta\lambda(g^{-1}) \text{ for all } g \in G, \eta \in N.$$

Finally, such a Hopf algebra acts on L by

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

where $\bar{1}$ denotes the coset G_L in X .

If L/K is a Galois extension then in the notation above $X = G$ and λ is the left regular embedding of G into $\text{Perm}(G)$. In this case, one example of a regular subgroup of $\text{Perm}(G)$ normalized by $\lambda(G)$ is $\rho(G)$, the image of G under the right regular embedding. Since $\lambda(G)$ centralizes $\rho(G)$ inside $\text{Perm}(G)$, the Hopf-Galois structure corresponding to the regular subgroup $\rho(G)$ has Hopf algebra isomorphic to $K[G]$, and from equation (2) we recover the usual action of $K[G]$ on L ([2, Proposition 6.10]). We call this Hopf-Galois structure the *classical*

structure. If G is abelian then in fact $\lambda(G) = \rho(G)$, but if G is non-abelian then they are distinct, and $\lambda(G)$ is another example of a regular subgroup of $\text{Perm}(G)$ normalized by $\lambda(G)$, and therefore corresponds to a different Hopf-Galois structure on L/K . In [8] we called this the *canonical nonclassical structure*, and denoted the corresponding Hopf algebra $L[\lambda(G)]^G$ by H_λ . We proved two theorems concerning the relationship between the classical structure and the canonical nonclassical structure: an element $x \in L$ generates L as a $K[G]$ module if and only if it generates L as an H_λ -module ([8, Theorem 2.1]), and, assuming that \mathfrak{D}_K is a principal ideal domain, an ambiguous (i.e. G -stable) ideal of L is free over its associated order in $K[G]$ if and only if it is free over its associated order in H_λ ([8, Theorem 1.1] and its correction, [9]). The proofs of these results exploited the fact that

$$h \cdot g(x) = g(h \cdot x) \text{ for all } h \in H_\lambda, g \in G, x \in L$$

([8, Lemma 3.3]). In this paper we generalize the results of [8] to a pair of Hopf algebras H_1, H_2 giving Hopf-Galois structures on a given separable (but not necessarily Galois) extension whose actions on L commute, by which we mean that

$$h_1 \cdot (h_2 \cdot x) = h_2 \cdot (h_1 \cdot x) \text{ for all } h_1 \in H_1, h_2 \in H_2, x \in L.$$

Furthermore, our results apply to all fractional ideals of L (not just to ambiguous ideals), and we can remove the hypothesis that \mathfrak{D}_K is a principal ideal domain.

Our results are as follows:

Theorem 1.1. Let L/K be a finite separable extension of fields and let H_1, H_2 be two Hopf algebras giving Hopf-Galois structures on L/K whose actions on L commute. Then an element $x \in L$ generates L as an H_1 -module if and only if it generates L as an H_2 -module.

Theorem 1.2. Retain the notation and hypotheses of Theorem 1.1, and assume that L/K is an extension of local or global fields (in any characteristic). Let \mathfrak{B} be a fractional ideal of L , and let $\mathfrak{A}_1(\mathfrak{B}), \mathfrak{A}_2(\mathfrak{B})$ be the associated orders of \mathfrak{B} in H_1, H_2 respectively. Then \mathfrak{B} is a free $\mathfrak{A}_1(\mathfrak{B})$ -module if and only if it is a free $\mathfrak{A}_2(\mathfrak{B})$ -module.

Corollary 1.3. If L/K is an extension of global fields then \mathfrak{B} is a locally free $\mathfrak{A}_1(\mathfrak{B})$ -module if and only if it is a locally free $\mathfrak{A}_2(\mathfrak{B})$ -module.

Proof. The proof of Theorem 1.2 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{D}_K

(a Galois algebra). To say that \mathfrak{B} is locally free over $\mathfrak{A}_1(\mathfrak{B})$ is to say that for each prime \mathfrak{p} of \mathfrak{D}_K , we have that $\mathfrak{B}_{\mathfrak{p}} = \mathfrak{D}_{K,\mathfrak{p}} \otimes_{\mathfrak{D}_K} \mathfrak{B}$ is a free $\mathfrak{D}_{K,\mathfrak{p}} \otimes_{\mathfrak{D}_K} \mathfrak{A}_1(\mathfrak{B})$ -module. By Theorem 1.2 this is equivalent to saying that for each prime \mathfrak{p} , $\mathfrak{B}_{\mathfrak{p}}$ is a free $\mathfrak{D}_{K,\mathfrak{p}} \otimes_{\mathfrak{D}_K} \mathfrak{A}_2(\mathfrak{B})$ -module, which is saying that \mathfrak{B} is a locally free $\mathfrak{A}_2(\mathfrak{B})$ -module. \square

In section 2 we characterize Hopf-Galois structures on a given separable extension whose actions commute, using the theorem of Greither and Pareigis. In section 3 we generalize some of the results of [8, Section 2], and use these to prove Theorems 1.1 and 1.2. Finally, in section 4 we ask, under the hypotheses of Theorem 1.2, which algebraic properties the associated orders $\mathfrak{A}_1(\mathfrak{B})$ and $\mathfrak{A}_2(\mathfrak{B})$ share. We show that $\mathfrak{A}_1(\mathfrak{B})$ is a maximal order in H_1 if and only if $\mathfrak{A}_2(\mathfrak{B})$ is a maximal order in H_2 (Proposition 4.3), but that it is possible for $\mathfrak{A}_1(\mathfrak{B})$ to be a Hopf order but for $\mathfrak{A}_2(\mathfrak{B})$ not to have this property (Example 4.1).

I would like to express my gratitude to Prof. Nigel Byott, who first suggested to me that it might be possible to generalize the results of [8] in this way.

2. COMMUTING HOPF-GALOIS STRUCTURES

Let L/K be a finite separable extension of fields. In this section we use the theorem of Greither and Pareigis to characterize pairs of Hopf-Galois structures on L/K whose actions on L commute. Although we are principally interested in extensions of local or global fields, we do not impose this hypothesis since the results of this section are valid more generally. We retain the hypotheses and notation used in the theorem of Greither and Pareigis, as described in section 1: E/K is the Galois closure of L/K , $G = \text{Gal}(E/K)$, $G_L = \text{Gal}(E/L)$, $X = \{gG_L \mid g \in G\}$, $B = \text{Perm}(X)$, and $\lambda : G \rightarrow B$ is defined by $\lambda(\sigma)gG_L = \sigma gG_L$. We shall always think of a Hopf algebra produced by the theorem of Greither and Pareigis as acting via equation (2); hence we may refer without ambiguity to *the* Hopf-Galois structure given by a particular Hopf algebra. In the introduction we noted that if L/K is a Galois extension with Galois group G then $\lambda(G)$ and $\rho(G)$ are both regular subgroups of B normalized by $\lambda(G)$, and therefore correspond to Hopf-Galois structures on L/K . We also noted that $\lambda(G)$ centralizes $\rho(G)$ inside B ; in fact $\lambda(G) = \text{Cent}_B(\rho(G))$. This relationship between $\lambda(G)$ and $\rho(G)$ in the Galois case is a particular example of a more general phenomenon:

Lemma 2.1. If N is a regular subgroup of B which is normalized by $\lambda(G)$, then so is $\text{Cent}_B(N)$.

Proof. The subgroup $\text{Cent}_B(N)$ is explicitly constructed in [4, Lemma 2.4.2] as follows: since N is regular on X , for each coset $\bar{g} \in X$ there is a unique element $\mu_{\bar{g}} \in N$ such that $\mu_{\bar{g}}(\bar{1}) = \bar{g}$. For each $\eta \in N$ define $\phi_\eta \in B$ by $\phi_\eta(\bar{g}) = \mu_{\bar{g}}(\eta(\bar{1}))$; then $\text{Cent}_B(N) = \{\phi_\eta \mid \eta \in N\}$. From this it is easy to verify that $\text{Cent}_B(N)$ is a regular subgroup of B . The proof that N' is normalized by $\lambda(G)$ appears as part of the proof of [4, Theorem 2.5]. These facts are also established in [5, Proposition 3.2, Corollary 3.9]. \square

Definition 2.2. If N is a regular subgroup of X normalized by $\lambda(G)$, and H is the Hopf algebra giving the corresponding Hopf-Galois structure, let $N' = \text{Cent}_B(N)$ and $H' = E[N']^G$.

We record some properties of the relationships between the regular subgroups N and N' and between the Hopf algebras H and H' :

Lemma 2.3. Let N be a regular subgroup of B which is normalized by $\lambda(G)$. Then:

- i) we may identify N' with N^{opp} (the group with the same underlying set as N but with the multiplication reversed);
- ii) $N' \cong N$;
- iii) $(N')' = N$;
- iv) $(H')' = H$;
- v) $N = N'$ if and only if N is abelian;
- vi) the Hopf-Galois structures given by H and H' coincide if and only if H is commutative.

Proof.

- i) See [4, Lemma 2.4.2].
- ii) In the notation of the proof of Lemma 2.1, the map $\eta \mapsto \phi_{\eta^{-1}}$ is an isomorphism from N to N' .
- iii) See [5, Lemma 3.5].
- iv) This follows from part (iii) and the definition of H' .
- v) If N is abelian then $N \subseteq N'$, but these groups have the same order, so in fact $N = N'$. For the converse, we recall from [5, Proposition 3.3] that $N \cap N' = Z(N)$, the center of N , so if $N = N'$ then N is abelian.
- vi) This follows from part (v) and the definition of H' .

\square

Since we may identify N' with N^{opp} , we may identify the group algebra $E[N']$ with the opposite ring $E[N]^{opp}$ (the ring with the same underlying set as $E[N]$ but with the multiplication reversed). However, we may not identify the Hopf algebra H' with the opposite ring H^{opp} , since the action of G on N^{opp} (see equation (1)) may not be compatible with its action on N . This is already apparent in the case that L/K is Galois, $N = \rho(G)$ and $N' = \lambda(G)$. Since $\lambda(G)$ is the centralizer of $\rho(G)$ in B , the action of G on $\rho(G)$ is trivial, and so $L[\rho(G)]^G = L^G[\rho(G)] \cong K[G]$. However, the action of G on $\lambda(G)$ is not trivial (the orbits are the conjugacy classes), and so $L[\lambda(G)]^G \neq K[\lambda(G)]$. Therefore in this case we may not identify $L[\lambda(G)]^G$ with $K[\rho(G)]^{opp}$.

We shall show that if H is a Hopf algebra giving a Hopf-Galois structure on L/K then the actions of H and H' on L commute (Proposition 2.4) and, conversely, that if H_1 and H_2 are two Hopf algebras giving Hopf-Galois structure on L/K whose actions on L commute then $H_2 = H_1'$ (Proposition 2.5). To do this, we recall some notation employed in the proof of the theorem of Greither and Pareigis, as detailed in [2, §6]. Let $M = \text{Map}(X, E)$, and let $\{u_{\bar{g}} \mid \bar{g} \in X\}$ be an E -basis of mutually orthogonal idempotents (where \bar{g} denotes the left coset $gG_L \in X$). That is:

$$u_{\bar{g}}(\bar{\sigma}) = \delta_{\bar{g}, \bar{\sigma}} \text{ for all } \bar{g}, \bar{\sigma} \in X.$$

It can be shown ([2, Theorem 6.3]) that the E -Hopf algebras giving Hopf-Galois structures on the extension of rings M/E are precisely the group algebras $E[N]$ of regular subgroups N of $\text{Perm}(G)$, where the group N acts on M by permuting the subscripts of the idempotents $u_{\bar{g}}$:

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

If in addition N is normalized by $\lambda(G)$ then the group G acts on $E[N]$ by acting on E as Galois automorphisms and on N via equation 1. It also acts on M by acting on E as Galois automorphisms and on the idempotents $u_{\bar{g}}$ by left translation of the subscripts. These actions are G -equivariant, so by Galois descent we obtain that $E[N]^G$ is a K -Hopf algebra giving a Hopf-Galois structure on the extension of rings M^G/K (and also that $E \otimes_K E[N]^G = E[N]$ and $E \otimes_K M^G = M$). Finally, we may identify L with the fixed ring M^G via the K -algebra isomorphism $L \xrightarrow{\sim} M^G$ defined by

$$(3) \quad x \mapsto f_x = \sum_{\bar{g} \in X} g(x)u_{\bar{g}} \text{ for all } x \in L.$$

(For $\bar{g} \in X$, the element $g(x)$ is well defined since $g_0(t) = t$ for all $g_0 \in G_L$ and $t \in L$).

Thus $E[N]^G$ gives a Hopf-Galois structure on L/K , with the action of $E[N]^G$ on L as given in equation (2).

With this notation to hand, we show that if H is a Hopf algebra giving a Hopf-Galois structure on L/K then the actions of H and H' on L commute. We then show that any pair of Hopf algebras giving Hopf-Galois structures on L/K whose actions on L commute arises in this way.

Proposition 2.4. Let H be a Hopf algebra giving a Hopf-Galois structure on L/K . Then the actions of H and H' on L commute.

Proof. Since $\eta'\eta = \eta\eta'$ for all $\eta \in N$ and $\eta' \in N'$, we have $z' \cdot (z \cdot f) = z \cdot (z' \cdot f)$ for all $z \in E[N]$, $z' \in E[N']$, and $f \in M$. Therefore it is certainly true that $h' \cdot (h \cdot f) = h \cdot (h' \cdot f)$ for all $h \in E[N]^G$, $h' \in E[N']^G$, and $f \in M^G$, and so the actions of H and H' on L commute. \square

Proposition 2.5. If $H_1 = E[N_1]^G$ and $H_2 = E[N_2]^G$ are two Hopf algebras giving Hopf-Galois structures on the extension L/K whose actions on L commute, then we have $N_2 = N_1'$.

Proof. Since the actions of H_1, H_2 on L commute, the actions of H_1, H_2 on M^G commute. Since $E \otimes_K M^G = M$ and $E \otimes_K H_i = E[N_i]$ for $i = 1, 2$, this implies that the actions of $E[N_1], E[N_2]$ on M commute. Therefore for all $\eta_1 \in N_1, \eta_2 \in N_2$ we have

$$\begin{aligned} \eta_1\eta_2u_{\bar{g}} &= \eta_2\eta_1u_{\bar{g}} \text{ for all } \bar{g} \in X \\ \Rightarrow \eta_1^{-1}\eta_2^{-1}\eta_1\eta_2\bar{g} &= \bar{g} \text{ for all } \bar{g} \in X \\ \Rightarrow \eta_1^{-1}\eta_2^{-1}\eta_1\eta_2 &= 1 \\ \Rightarrow \eta_1\eta_2 &= \eta_2\eta_1. \end{aligned}$$

Therefore $N_2 \subseteq N_1'$. But N_2 and N_1' have the same order, so in fact they must be equal. \square

3. NORMAL BASIS GENERATORS AND INTEGRAL MODULE STRUCTURE

We continue to assume that L/K is a finite separable extension of fields, and retain the notation established in section 1 concerning the statement of the theorem of Greither and Pareigis, as well as the elements of its proof that we used in section 2. In this section we prove

Theorems 1.1 and 1.2, which are our main results. We require slight generalizations of two lemmas from [8]:

Lemma 3.1. Let N be a regular subgroup of $\text{Perm}(X)$ normalized by $\lambda(G)$, so that $E[N]^G$ is a K -Hopf algebra giving a Hopf-Galois structure on M^G/K . An element $f \in M^G$ is an $E[N]^G$ -generator of M^G if and only if it is an $E[N]$ -generator of M .

Proof. This is a slight generalization of [8, Lemma 2.2], with essentially the same proof. \square

Lemma 3.2. Fix an ordering of the set X , say $X = \{\overline{g}_1, \dots, \overline{g}_m\}$, and define an ordering on the group N , say $N = \{\eta_1, \dots, \eta_m\}$, by $\eta_j(\overline{g}_1) = \overline{g}_j$. For $x \in L$, the element f_x is an $E[N]$ -generator of M if and only if the matrix

$$T_N(x) = (\eta_i(\overline{g}_j)[x])$$

is nonsingular.

Proof. This is a slight generalization of [8, Lemma 2.3], with essentially the same proof. We note that although the definition of the matrix $T_N(x)$ depends on the ordering of X , the question of whether it is nonsingular does not. \square

We now use the characterization of commuting Hopf-Galois structures from section 2 to prove Theorem 1.1: which generalizes [8, Theorem 1.2]:

Proof of Theorem 1.1. By the theorem of Greither and Pareigis, $H_1 = E[N]^G$ for some regular subgroup N of X normalized by $\lambda(G)$, and by Proposition 2.5 we have $H_2 = H'_1 = E[N']^G$. Thus by Lemmas 3.1 and 3.2 it is sufficient to show that $T_N(x)$ is nonsingular if and only if $T_{N'}(x)$ is nonsingular. We have:

$$\begin{aligned} \det(T_N(x)) &= \det((\eta_i(\overline{g}_j)[x])) \\ &= \det((\eta_i(\eta'_j(\overline{g}_1))[x])) \\ &= \det((\eta'_j(\eta_i(\overline{g}_1))[x])) \text{ since } N, N' \text{ commute inside } B \\ &= \det((\eta'_j(\overline{g}_i)[x])) \\ &= \det(T_{N'}(x))^T \end{aligned}$$

Therefore $\det(T_N(x)) = \det(T_{N'}(x))$, and so $T_N(x)$ is nonsingular if and only if $T_{N'}(x)$ is nonsingular, which completes the proof. \square

The results we have established so far are valid for any finite separable extension of fields. We now turn to questions of integral Hopf-Galois

module structure in a finite separable extension of local or global fields L/K . Note, though, that we make no restriction on the characteristic of K . Using the notation established in section 2, we will prove Theorem 1.2, which generalizes [8, Theorem 1.1]. First we note that if H is a Hopf algebra giving a Hopf-Galois structure on L/K and \mathfrak{B} is a fractional ideal of L then \mathfrak{B} has an associated order in H : since L is a free H -module of rank 1 ([2, Proposition 2.15]), we can identify \mathfrak{B} with a full \mathfrak{O}_K -lattice in H , and the left multiplier ring of this lattice is an order in H ([11, Chapter 2, §8]), which we can identify with the associated order of \mathfrak{B} in H . Thus the assumption in [8, Theorem 1.1] that the fractional ideal \mathfrak{B} is an ambiguous ideal of L is superfluous.

Proof of Theorem 1.2. Let $H_1 = H$; then by Proposition 2.5 we have $H_2 = H'$. Suppose that $x \in \mathfrak{B}$ generates \mathfrak{B} as an $\mathfrak{A}_H(\mathfrak{B})$ -module. Then x generates L as an H -module, and so by Theorem 1.1 it generates L as an H' -module. Therefore for each $a \in \mathfrak{A}_H(\mathfrak{B})$ we may define $z_a \in H'$ by $z_a \cdot x = a \cdot x$. We claim that

$$\mathfrak{A}_{H'}(\mathfrak{B}) = \{z_a \mid a \in \mathfrak{A}_H(\mathfrak{B})\}.$$

First we show that $z_a \in \mathfrak{A}_{H'}(\mathfrak{B})$ for each $a \in \mathfrak{A}_H(\mathfrak{B})$. Let $a \in \mathfrak{A}_H(\mathfrak{B})$ and $b \in \mathfrak{B}$. Since \mathfrak{B} is a free $\mathfrak{A}_H(\mathfrak{B})$ -module, there exists a unique $w \in \mathfrak{A}_H(\mathfrak{B})$ such that $b = w \cdot x$. Now we have:

$$\begin{aligned} z_a \cdot b &= z_a \cdot (w \cdot x) \\ &= w \cdot (z_a \cdot x) \text{ since the actions of } H, H' \text{ on } L \text{ commute} \\ &= w \cdot (a \cdot x), \end{aligned}$$

and this lies in \mathfrak{B} since $a, w \in \mathfrak{A}_H(\mathfrak{B})$. Therefore $z_a \in \mathfrak{A}_{H'}(\mathfrak{B})$.

On the other hand, if $z \in \mathfrak{A}_{H'}(\mathfrak{B})$ then $z \cdot x = z_a \cdot x$ for some $a \in \mathfrak{A}_H(\mathfrak{B})$, and this implies that $z = z_a$ because x generates L as a free H' -module. Therefore $\mathfrak{A}_{H'}(\mathfrak{B}) = \{z_a \mid a \in \mathfrak{A}_H(\mathfrak{B})\}$, as claimed.

Since $(H')' = H$, the converse statement follows by interchanging the roles of H, H' in the argument above. \square

In [8], we split the proof of Theorem 1.1 into two propositions: Proposition 4.1 and Proposition 4.2. In the proofs of those propositions we assumed that certain \mathfrak{O}_K orders in certain K -algebras possessed \mathfrak{O}_K -bases. Although this is automatically true if L/K is an extension of local fields, it need not be true if L/K is an extension of global fields. In order for these proofs to be correct as written, we therefore issued a correction ([9]) adding the hypothesis that \mathfrak{O}_K must be a principal

ideal domain. In the proof of Theorem 1.2 above, we made no such assumptions about \mathfrak{D}_K -bases, and so this hypothesis is no longer needed. In particular, [8, Theorem 1.1] is valid as stated.

4. SHARED PROPERTIES OF ASSOCIATED ORDERS

In this section we adopt the hypotheses of Theorem 1.2: L/K is a finite separable extension of local or global fields, \mathfrak{B} is a fractional ideal of L , H is a Hopf algebra giving a Hopf-Galois structure on L/K , and H' is the Hopf algebra whose action on L commutes with that of H . We have seen that \mathfrak{B} is free over $\mathfrak{A}_H(\mathfrak{B})$ if and only if it is free over $\mathfrak{A}_{H'}(\mathfrak{B})$, but we might wonder whether these orders share any algebraic properties. If K has characteristic zero, then the question of whether $\mathfrak{A}_H(\mathfrak{B})$ is a Hopf order in H is particularly interesting, since in this case \mathfrak{D}_L is locally free over $\mathfrak{A}_H(\mathfrak{B})$ by a theorem of Childs ([2, Theorem 13.4]). However, there are examples of extensions for which $\mathfrak{A}_H(\mathfrak{B})$ is a Hopf order but $\mathfrak{A}_{H'}(\mathfrak{B})$ is not:

Example 4.1. Let p, q, r be prime numbers with $r \equiv 1 \pmod{q}$ and $p \nmid qr$, and let L/K be a tamely ramified Galois extension of p -adic fields whose Galois group G is isomorphic to the metacyclic group of order qr . For a fixed integer d having order q modulo r , we may write

$$G = \langle \sigma, \tau \mid \sigma^r = \tau^q = 1, \tau\sigma = \sigma^d\tau \rangle.$$

The extension L/K is Galois with nonabelian Galois group, so it admits the classical Hopf-Galois structure, with Hopf algebra $K[G]$, and the canonical nonclassical structure, with Hopf algebra $H_\lambda = L[\lambda(G)]^G$. Since L/K is tamely ramified, Noether's Theorem implies that \mathfrak{D}_L is a free module over $\mathfrak{D}_K[G]$, which is a Hopf order in $K[G]$. By Theorem 1.2, \mathfrak{D}_L is free over its associated order $\mathfrak{A}_\lambda(\mathfrak{D}_L)$ in H_λ , but we shall show that this is not a Hopf order in H_λ .

By [6, Proposition 2.5], we have $\mathfrak{D}_L[\lambda(G)]^G \subseteq \mathfrak{A}_\lambda(\mathfrak{D}_L)$. We begin by showing that $\mathfrak{D}_L[\lambda(G)]^G$ is not a Hopf order in H_λ . By [7, Corollary 2.2] $\mathfrak{D}_L[\lambda(G)]^G$ is a Hopf order in H_λ if and only if the inertia subgroup of G is contained in the center of G . Since G is nonabelian, the extension L/K is neither unramified nor totally ramified, and so the inertia subgroup must be the unique nontrivial normal subgroup of G , which is $\langle \sigma \rangle$. But it is easy to see that G has trivial center, so the inertia subgroup is not contained in the center of G , and so $\mathfrak{D}_L[\lambda(G)]^G$ is not a Hopf order in H_λ .

Next we suppose that $\mathfrak{A}_\lambda(\mathfrak{D}_L)$ is a Hopf order in H_λ properly containing $\mathfrak{D}_L[\lambda(G)]^G$. Then $\mathfrak{D}_L \otimes_{\mathfrak{D}_K} \mathfrak{A}_\lambda(\mathfrak{D}_L)$ is a Hopf order in $L \otimes_K L[\lambda(G)]^G = L[\lambda(G)]$ properly containing $\mathfrak{D}_L[\lambda(G)]$. But $|G| = qr$ and $p \nmid qr$, so $L[\lambda(G)]$ has no Hopf orders apart from $\mathfrak{D}_L[\lambda(G)]$, by [2, Corollary 20.3]. Therefore $\mathfrak{A}_\lambda(\mathfrak{D}_L)$ is not a Hopf order in H_λ .

This example illustrates that Theorem 1.2 has the potential to extend the scope of Childs' Theorem: if L/K is a finite separable extension of local or global fields in characteristic zero and H is a Hopf algebra giving a Hopf-Galois structure on the extension then \mathfrak{D}_L is locally free over its associated orders in both H and H' if either of these is a Hopf order.

The question of whether $\mathfrak{A}_H(\mathfrak{B})$ is a maximal order in H is also of interest, and this is the subject of our final result. We shall require H to be a separable K -algebra, so we first note a criterion for this to occur:

Lemma 4.2. The Hopf algebra H is a separable K -algebra if and only if the characteristic of K does not divide $[L : K]$.

Proof. By [3, Theorem 7] H is separable if and only if it is semisimple, and by [10, Theorem 5.1.8] H is semisimple if and only if $\varepsilon(I_H) \neq 0$, where I_H denotes the subspace of left integrals of H and $\varepsilon : H \rightarrow K$ denotes the counit map (recall that an element $\phi \in H$ is called a left integral of H if $h\phi = \varepsilon(h)\phi$ for all $h \in H$). To determine I_H , we note that the subspace of left integrals of a Hopf algebra over a field is one-dimensional ([2, Corollary 3.4]) and recall that, by the theorem of Greither and Pareigis, $H = E[N]^G$ for some group N of order $[L : K]$. The subspace of left integrals of $E[N]$ is equal to $E\theta$, where $\theta = \sum_{\eta \in N} \eta$. Recalling the action of G on N from the theorem of Greither and Pareigis, we see that in fact θ lies in $H = E[N]^G$, and so we deduce that $I_H = K\theta$. Therefore $\varepsilon(I_H) \neq 0$ if and only if $\varepsilon(\theta) \neq 0$. But $\varepsilon(\theta) = |N| = [L : K]$, so $\varepsilon(\theta) \neq 0$ if and only if the characteristic of K does not divide $[L : K]$. \square

Proposition 4.3. Suppose that the characteristic of K does not divide $[L : K]$. Let \mathfrak{B} be a fractional ideal of L , and let $\mathfrak{A}_H(\mathfrak{B})$, $\mathfrak{A}_{H'}(\mathfrak{B})$ be the associated orders of \mathfrak{B} in H , H' respectively. Then $\mathfrak{A}_H(\mathfrak{B})$ is a maximal order in H if and only if $\mathfrak{A}_{H'}(\mathfrak{B})$ is a maximal order in H' .

Proof. Since the characteristic of K does not divide $[L : K]$, Lemma 4.2 implies that H is a separable K -algebra. Therefore an \mathfrak{D}_K -order \mathfrak{A} in H is maximal if and only if for each prime \mathfrak{p} of \mathfrak{D}_K the order $\mathfrak{D}_{K,\mathfrak{p}} \otimes_{\mathfrak{D}_K} \mathfrak{A}$ is a maximal $\mathfrak{D}_{K,\mathfrak{p}}$ -order in the separable $K_{\mathfrak{p}}$ -algebra $K_{\mathfrak{p}} \otimes_K H$ ([11,

Corollaries 11.2 and 11.5]), and so we may reduce to the case in which K is a local field.

In this case, suppose that $\mathfrak{A}_{H'}(\mathfrak{B})$ is a maximal order but $\mathfrak{A}_H(\mathfrak{B})$ is not. Since H is a separable K -algebra, by [11, Corollary 10.4] $\mathfrak{A}_H(\mathfrak{B})$ is properly contained in some maximal order in H , say \mathfrak{M} . Since L is a free H' -module of rank 1 ([2, Proposition 2.15]) and $\mathfrak{A}_{H'}(\mathfrak{B})$ is a maximal order in H' , [11, Theorem 18.10] implies that \mathfrak{B} is a free $\mathfrak{A}_{H'}(\mathfrak{B})$ -module of rank 1. Let $x \in \mathfrak{B}$ generate \mathfrak{B} as an $\mathfrak{A}_{H'}(\mathfrak{B})$ module; by Theorem 1.2 it also generates \mathfrak{B} as an $\mathfrak{A}_H(\mathfrak{B})$ -module. Now let $\Delta = \mathfrak{M} \cdot x$. This is a full \mathfrak{O}_K -lattice in L which properly contains \mathfrak{B} , and a free \mathfrak{M} -module of rank 1, generated by x . Let $\mathfrak{A}_{H'}(\Delta)$ denote the associated order of Δ in H' . Similarly to the proof of Theorem 1.2, for each $\mu \in \mathfrak{M}$ define $z_\mu \in H'$ by $z_\mu \cdot x = \mu \cdot x$; we find that $\mathfrak{A}_{H'}(\Delta) = \{z_\mu \mid \mu \in \mathfrak{M}\}$. But $\mathfrak{A}_{H'}(\Delta) \supsetneq \mathfrak{A}_{H'}(\mathfrak{B})$ since

$$\Delta = \mathfrak{A}_{H'}(\Delta) \cdot x \supsetneq \mathfrak{A}_{H'}(\mathfrak{B}) \cdot x = \mathfrak{B}.$$

This contradicts the assumption that $\mathfrak{A}_{H'}(\mathfrak{B})$ is a maximal order in H' . Therefore $\mathfrak{A}_H(\mathfrak{B})$ is a maximal order in H .

Since $(H')' = H$, the converse statement follows by interchanging the roles of H, H' in the argument above. \square

REFERENCES

1. Nigel P. Byott, *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, (1997): 201-219.
2. Lindsay N. Childs, *Taming Wild Extensions: Hopf algebras and local Galois module theory*, American Mathematical Society, (2000).
3. Miriam Cohen and Davida Fishman, *Hopf algebra actions*, Journal of Algebra 100, (1986): 363-379.
4. Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, Journal of Algebra 1, (1987): 239-258.
5. Timothy Kohl, *Groups of order $4p$, twisted wreath products and Hopf-Galois theory*, Journal of Algebra 314, (2007): 42-74.
6. Paul J. Truman, *Towards a generalisation of Noethers Theorem to nonclassical Hopf-Galois structures*, New York J. Math 17, (2011): 799-810.
7. ———, *Integral Hopf-Galois structures for tame extensions*, New York J. Math 19, (2013): 647-655.
8. ———, *Canonical nonclassical Hopf-Galois module structure of nonabelian Galois extensions*, Communications in Algebra 44.3 (2016): 1119-1130.
9. ———, *Correction to: Canonical nonclassical Hopf-Galois module structure of nonabelian Galois extensions*, Communications in Algebra 45.9 (2017): 3892.
10. Moss E. Sweedler, *Hopf algebras*, Benjamin, New York, 1969.

11. Irving Reiner, *Maximal orders* Academic Press, (1975).

SCHOOL OF COMPUTING AND MATHEMATICS, KEELE UNIVERSITY, STAFFORD-
SHIRE, ST5 5BG, UK

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