New York Journal of Mathematics

New York J. Math. **25** (2019) 219–237.

The structure of Hopf algebras giving Hopf-Galois structures on quaternionic extensions

Stuart Taylor and **Paul J. Truman**

Abstract. Let L/F be a Galois extension of fields with Galois group isomorphic to the quaternion group of order 8. We describe all of the Hopf-Galois structures admitted by L/F, and determine which of the Hopf algebras that appear are isomorphic as Hopf algebras. In the case that F has characteristic not equal to 2 we also determine which of these Hopf algebras are isomorphic as F-algebras and explicitly compute their Wedderburn-Artin decompositions.

Contents

1. Introduction

Let L/F be a finite Galois extension of fields with group G. The group algebra $F[G]$, with its usual action on L, is an example of a *Hopf-Galois structure* on the extension. If H is a finite dimensional F-Hopf algebra, then we say that H gives a Hopf-Galois structure on L/F if and only if the following conditions hold:

- L is an H-module algebra; that is: L is an H-module with action $h(x)$ for $h \in H$ and $x \in L$ where, for $y \in L$,

$$h(xy) = \sum_{(h)} h_{(1)}(x)h_{(2)}(y)$$

(Sweedler notation) and $h(1) = \epsilon(h)(1)$;

Received November 14, 2018.

2010 *Mathematics Subject Classification.* 16T05.

Key words and phrases. Hopf Galois structure, Hopf algebra, Galois extension, Wedderburn-Artin decomposition.

ISSN 1076-9803/2019

- the F-linear map $j : L \otimes_F H \to \mathrm{End}_K(L)$ given by $j(l \otimes h)(x) = lh(x)$ for $l, x \in L$, $h \in H$, is bijective.

We note that in this definition L/F may be taken to be merely an extension of commutative rings. However, in this paper we will be concerned exclusively with fields, specifically the case where L/F is Galois (in the usual sense).

Since a Hopf-Galois structure on an extension L/F consists of a Hopf algebra H and an action of H on L, it is possible for distinct Hopf-Galois structures on L/F to involve Hopf algebras that are isomorphic, either as F-Hopf algebras or as F-algebras. These phenomena have recently been studied in papers such as [11] and [10]. In particular, [10] studies in detail the Hopf-Galois structures admitted by a dihedral extension of fields of degree $2p$, where p is an odd prime. In this paper we perform a similar analysis of the Hopf-Galois structures admitted by a Galois extension of fields with Galois group isomorphic to Q_8, the quaternion group of order 8. We call such extensions *quaternionic*. In addition to continuing and complementing the work begun in the papers cited above, our results have applications in the study of the Hopf-Galois module structure of rings of algebraic integers in quaternionic extensions of local or global fields. Since such extensions have been important in the history of Galois module structure (see [13], for example), this has the potential to be a fruitful line of inquiry, which we intend to pursue in a future paper.

A theorem of Greither and Pareigis ([8, Theorem 3.1], see also [3, Theorem 6.8]) classifies all of the Hopf-Galois structures admitted by a finite separable extension of fields. We state it here in a weakened form applicable to finite Galois extensions. Consider the group of permutations on the underlying set of G, $\mathrm{Perm}(G)$, and let $\lambda : G \hookrightarrow \mathrm{Perm}(G)$ be the left regular representation. A subgroup N of $\mathrm{Perm}(G)$ is said to be *regular* if $|N| = |G|$, the stabiliser $\mathrm{Stab}_N(g) = \{\eta \in N \,|\, \eta \cdot g = g\}$ is trivial for all $g \in G$, and N acts transitively on G (any two of these properties imply the third). The theorem of Greither and Pareigis states that there is a bijection between regular subgroups N of $\mathrm{Perm}(G)$ normalised by $\lambda(G)$ and Hopf-Galois structures on L/F. Furthermore, if N is a regular subgroup of $\mathrm{Perm}(G)$ normalised by $\lambda(G)$ then the Hopf algebra giving the Hopf-Galois structure corresponding to N is $L[N]^G$, the fixed ring of the group algebra $L[N]$, where G acts on $L[N]$ by acting on L as Galois automorphisms and on N by ${}^g\eta = \lambda(g)n\lambda(g^{-1})$ for all $\eta \in N$, $g \in G$. For a Hopf algebra $H = L[N]^G$ giving a Hopf-Galois structure on L/F, we refer to N as the *underlying group* of H and its isomorphism class as the *type* of H, or the structure given by H.

Example 1.1. *Let $\rho : G \hookrightarrow Perm(G)$ be the right regular representation. Suppose $g, h \in G$ and $x \in G$. Then $\lambda(g)\rho(h)[x] = gxh^{-1} = \rho(h)[gx] = \rho(h)\lambda(g)[x]$. That is: $\lambda(g)\rho(h) = \rho(h)\lambda(g)$ for all $g, h \in G$. Thus the action of G on $\rho(G)$ is trivial, and so the Hopf algebra $L[\rho(G)]^G$ is in fact the group*

algebra $F[G]$ as in the original discussion. The Hopf-Galois structure for which $N = \rho(G)$ is the underlying group is called the classical *structure.*

Example 1.2. *It is clear that the action of G on $\lambda(G)$ gives G-orbits equal to the conjugacy classes. When G is not abelian (so that the $\rho(G) \neq \lambda(G)$) the structure for which $N = \lambda(G)$ is the underlying group is called the* canonical non-classical *structure.*

The theorem of Greither and Pareigis is the cornerstone of almost all of the work concerned with the enumeration, description, and application of Hopf-Galois structures on separable extensions of fields. In particular, via a theorem of Byott [2, Proposition 1], it reveals a connection between the theory of Hopf-Galois structures and the theory of *left skew braces*, which is described in detail in the appendix to [15]. This appendix contains an enumeration of the Hopf-Galois structures admitted by a quaternion extension L/F [15, Table A.1]. In section 2 below we compute the regular subgroups corresponding to these Hopf-Galois structures, and in section 3 we determine which of the Hopf algebras that appear are isomorphic as Hopf algebras. In section 4 we study the F-algebra structure of these Hopf algebras: under the assumption that F has characteristic not equal to 2, we find explicit bases for each Hopf algebra, compute their Artin-Wedderburn decompositions, and identify which are isomorphic as F-algebras.

The first named author acknowledges funding support from the Faculty of Natural Sciences at Keele University. We are grateful to Prof. Alan Koch for his comments on an early draft of this paper, and to the anonymous referee for improvements to the exposition and interpretation of our results.

2. Structures on the extension

Let L/F be a Galois extension of fields with Galois group G isomorphic to the quaternion group of order 8. Let G have generators σ and τ, that is

$$G = \langle \sigma, \tau | \sigma^4 = \tau^4 = 1, \sigma^2 = \tau^2, \sigma\tau = \tau\sigma^{-1} \rangle.$$

There are 5 isomorphism types of groups of order 8: the elementary abelian group $C_2 \times C_2 \times C_2$, $C_4 \times C_2$, the cyclic group C_8, the dihedral group D_4 and the quaternion group Q_8. As mentioned in the introduction, [15, Table A.1] includes a count of the Hopf-Galois structures admitted by L/F, which we reproduce in Table 1 below. The same count appears in work of Crespo and Salguero [4, Table 3], as an application of an algorithm written in the computational algebra system Magma which gives all Hopf-Galois structures on separable field extensions of a given degree.

We now determine the regular subgroups of $\mathrm{Perm}(G)$ corresponding to these Hopf-Galois structures. We start with the subgroups corresponding to the Hopf-Galois structures of type $C_2 \times C_2 \times C_2$.

TABLE 1. The number of Hopf-Galois structures on a quaternionic extension

Type	Number of structures
$C_2 \times C_2 \times C_2$	2
$C_4 \times C_2$	6
C_8	6
Q_8	2
D_4	6

Lemma 2.1. *Let $s, t \in \{\sigma, \tau\}$ with $s \neq t$ and let $E_{s,t}$ be generated by $\lambda(s)\rho(t), \lambda(s^2)$, and $\lambda(t)\rho(st)$. Then $E_{s,t}$ is a regular subgroup of Perm(G) that is normalized by $\lambda(G)$ and isomorphic to $C_2 \times C_2 \times C_2$. The groups $E_{\sigma,\tau}$ and $E_{\tau,\sigma}$ are distinct, and are the underlying groups of the 2 Hopf-Galois structures of type $C_2 \times C_2 \times C_2$ on L/F.*

Proof. The elements of $E_{s,t}$ are

$$1, \lambda(s^2), \lambda(s)\rho(t), \lambda(s^{-1})\rho(t), \lambda(t)\rho(st), \lambda(t^{-1})\rho(st), \lambda(st)\rho(s), \lambda((st)^{-1})\rho(s).$$

All of the non-identity elements above have order 2, so $E_{s,t}$ is isomorphic to $C_2 \times C_2 \times C_2$. It is clear that $E_{s,t} \subset \mathrm{Perm}(G)$ and $E_{s,t} \cdot 1_G = G$; hence $E_{s,t}$ is a regular subgroup of Perm(G). To show that $E_{s,t}$ is normalized by $\lambda(G)$, it is sufficient to show that it is normalized by $\lambda(s)$ and $\lambda(t)$. Using the fact that $\lambda(G)$ and $\rho(G)$ commute inside Perm(G) we have for example

$$^{s}\lambda(s)\rho(t) = \lambda(sss^{-1})\rho(t) = \lambda(s)\rho(t)$$
$$^{t}\lambda(s)\rho(t) = \lambda(tst^{-1})\rho(t) = \lambda(s^{-1})\rho(t).$$

Similar calculations apply to the other elements, and so $E_{s,t}$ is normalized by $\lambda(G)$. Finally, we have $E_{s,t} \neq E_{t,s}$ since $\lambda(t)\rho(s)$ lies in $E_{t,s}$ but not in $E_{s,t}$. Referring to Table 1 we see that $E_{\sigma,\tau}$ and $E_{\tau,\sigma}$ are the underlying groups of the two Hopf-Galois structures of type $C_2 \times C_2 \times C_2$ on L/F. □

We now find the subgroups corresponding to the Hopf-Galois structures of type $C_4 \times C_2$ using a similar technique.

Lemma 2.2. *Let $s, t \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$ and let $A_{s,t}$ be generated by the permutations $\lambda(s)$ and $\rho(t)$. Then $A_{s,t}$ is a regular subgroup of Perm(G) that is normalized by $\lambda(G)$ and isomorphic to $C_4 \times C_2$. The 6 choices of the pair s, t yield distinct groups, and these are the underlying groups of the 6 structures of type $C_4 \times C_2$ on L/F.*

Proof. We have $\langle \rho(t), \lambda(s) \rangle \cong C_4 \times C_2$ since $\rho(t)$ and $\lambda(s)$ are both of order 4, commute with each other, and share the same square. It is clear that $A_{s,t} \subset \mathrm{Perm}(G)$ and that for $g, h \in G$ we have $\lambda(g)\rho(h) \cdot 1_G = gh^{-1}$; hence

$A_{s,t}$ is a regular subgroup of $\mathrm{Perm}(G)$. The verification that it is normalized by $\lambda(G)$ is very similar to the verification in Lemma 2.1, using the fact that $\rho(G)$ and $\lambda(G)$ commute inside $\mathrm{Perm}(G)$. To show that the six choices of the pair s, t yield distinct groups, note that for each such pair the group $A_{s,t}$ is the only one that contains $\lambda(s)$ and $\rho(t)$. Hence, by Table 1, the groups $A_{s,t}$ are the underlying groups of the 6 Hopf-Galois structures of type $C_4 \times C_2$. □

The subgroups corresponding to the Hopf-Galois structures of type C_8 cannot be described in terms of combinations of elements from $\lambda(G)$ and $\rho(G)$, since the order of any such element is at most 4.

Lemma 2.3. *Let $s, t \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$ and let $C_{s,t}$ be generated by the permutation $\eta_{s,t}$ defined in cycle notation by*

$$\eta_{s,t} = (1\ s\ t\ (st)^{-1}\ s^2\ s^{-1}\ t^{-1}\ (st)).$$

Then $C_{s,t}$ is a regular subgroup of Perm(G) that is normalized by $\lambda(G)$ and isomorphic to C_8. The 6 choices of the pair s, t yield distinct groups, and these are the underlying groups of the 6 structures of type C_8 on L/F.

Proof. It is clear that $C_{s,t}$ is a subgroup of $\mathrm{Perm}(G)$ isomorphic to C_8. Moreover, we have $C_{s,t} \cdot 1_G = G$ since $\eta_{s,t}^k \cdot 1_G = 1_G$ if and only if $k \equiv 0 \pmod 8$. Thus $C_{s,t}$ is a regular subgroup of $\mathrm{Perm}(G)$. To show that $C_{s,t}$ is normalized by $\lambda(G)$, it is sufficient to show that it is normalized by $\lambda(s)$ and $\lambda(t)$. We have

$$\begin{aligned}\lambda(s)\eta_{s,t}\lambda(s^{-1}) &= (1\ s\ s^2\ s^{-1})(t\ st\ t^{-1}\ (st)^{-1}) \\ &\qquad (1\ s\ t\ (st)^{-1}\ s^2\ s^{-1}\ t^{-1}\ st)(1\ s^{-1}\ s^2\ s)(t\ (st)^{-1}\ t^{-1}\ st) \\ &= (1\ (st)^{-1}\ t^{-1}\ s\ s^2\ st\ t\ s^{-1}) \\ &= \eta_{s,t}^3,\end{aligned}$$

and similarly, $\lambda(t)\eta_{s,t}\lambda(t^{-1}) = \eta_{s,t}$. Therefore $C_{s,t}$ is normalized by $\lambda(G)$. It may be verified that each of the 6 choices of the pair s, t gives a permutation that differs from all powers of those of the other choices. Hence, by Table 1, the groups $C_{s,t}$ are the underlying groups of the 6 Hopf-Galois structures of type C_8. □

Having found the abelian underlying groups of the corresponding Hopf-Galois structures on our extension L/F we now find the structures of quaternionic type which we saw earlier.

Lemma 2.4. *$\rho(G)$ and $\lambda(G)$ are the underlying groups of the two Hopf-Galois structures of type Q_8.*

Proof. As G is non-abelian, $\rho(G)$ and $\lambda(G)$ are distinct regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$. By Table 1, they are the underlying groups of the 2 Hopf-Galois structures of type Q_8. □

Finally, the subgroups corresponding to the Hopf-Galois structures of type D_4, the dihedral group of order 8, have a similar description to the groups $E_{s,t}$ and $A_{s,t}$.

Lemma 2.5. *Let $s, t \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$. Let $D_{s,\lambda}$ be generated by $\lambda(s)$ and $\lambda(t)\rho(s)$, and let $D_{s,\rho}$ be generated by $\rho(s)$ and $\lambda(s)\rho(t)$. Then $D_{s,\lambda}$ and $D_{s,\rho}$ do not depend upon the choice of t, and are regular subgroups of Perm(G) that are normalized by $\lambda(G)$ and isomorphic to D_4. The 3 choices of s yield 6 distinct groups, and these are the underlying groups of the Hopf-Galois structures of type D_4 on L/F.*

Proof. For a fixed choice of t the elements of $D_{s,\lambda}$ are

$$1,\ \lambda(s),\ \lambda(s^2),\ \lambda(s^{-1}),\ \lambda(t)\rho(s),\ \lambda(st)\rho(s),\ \lambda(t^{-1})\rho(s),\ \lambda((st)^{-1})\rho(s).$$

We see immediately that using st in place of t yields the same group, that $\lambda(s)$ has order 4, $\lambda(t)\rho(s)$ has order 2, and that these elements anticommute. Therefore $D_{s,\lambda} \cong D_4$. It is clear that $D_{s,\lambda} \subset \mathrm{Perm}(G)$ and that $D_{s,\lambda} \cdot 1_G = G$; hence $D_{s,\lambda}$ is a regular subgroup of Perm(G). The verification that it is normalized by $\lambda(G)$ is very similar to the verifications in Lemma 2.1 and Lemma 2.2, using the fact that $\rho(G)$ and $\lambda(G)$ commute inside Perm(G). Similarly, $D_{s,\rho}$ is a regular subgroup of Perm(G) that is isomorphic to D_4 and normalized by $\lambda(G)$. To show that the 3 choices of s yield 6 distinct groups, note that for each s the group $D_{s,\lambda}$ is the only one that contains $\lambda(s)$ and that $D_{s,\rho}$ is the only one that contains $\rho(s)$. Hence, by Table 1, the groups $D_{s,\lambda}$ and $D_{s,\rho}$ are the underlying groups of the 6 Hopf-Galois structures of type D_4. □

Remark 2.6. *For every regular subgroup N of Perm(G) corresponding to a Hopf-Galois structure on L/F we have $\rho(\sigma^2) \in N$, and so $Z(\rho(G)) \subseteq \rho(G) \cap N$. Clearly this is the case for $N = \rho(G)$ and $N = \lambda(G)$, and it is easy to verify that it holds for $N = E_{s,t}, A_{s,t}, D_{s,\lambda}$, and $D_{s,\rho}$ (for all valid choices of s, t) from the definitions of these groups. Finally, we can verify that it holds for the groups $C_{s,t}$ (for all valid choices of s, t) by computing $\eta_{s,t}^4 = \rho(\sigma^2)$ in these cases.*

3. Hopf algebra isomorphisms

In this section we determine which of the Hopf algebras giving Hopf-Galois structures on L/F are isomorphic as F-Hopf algebras. In [11, Theorem 2.2] Koch, Kohl, Underwood and the second named author outline the following criterion for two Hopf algebras arising from the Greither-Pareigis correspondence to be isomorphic as Hopf algebras: let N_1 and N_2 be underlying groups of two Hopf-Galois structures on L/F. Then $L[N_1]^G \cong L[N_2]^G$ as F-Hopf algebras if and only if there exists a G-equivariant isomorphism $f : N_1 \xrightarrow{\sim} N_2$. In particular, no two Hopf algebras of different types may be isomorphic as F-Hopf algebras.

We now determine which of our Hopf algebras are isomorphic. We consider the isomorphism classes of the underlying groups individually. We start with the elementary abelian groups.

Lemma 3.1. *The Hopf algebras giving the two Hopf-Galois structures of type $C_2 \times C_2 \times C_2$ are isomorphic to each other as Hopf algebras. That is, $L[E_{\sigma,\tau}]^G \cong L[E_{\tau,\sigma}]^G$ as Hopf algebras.*

Proof. Recall the definition of $E_{s,t}$ from Lemma 2.1. The non-trivial G-orbits of $E_{s,t}$ are

$$\{\lambda(s)\rho(t), \lambda(s^{-1})\rho(t)\},\ \{\lambda(t)\rho(st), \lambda(t^{-1})\rho(st)\},\ \{\lambda(st)\rho(s), \lambda((st)^{-1})\rho(s)\},$$

with stabilisers $\langle s\rangle$, $\langle t\rangle$ and $\langle st\rangle$ respectively. The map $f : E_{s,t} \to E_{t,s}$ defined by

$$f : \begin{cases} \lambda(s)\rho(t) & \mapsto & \lambda(s)\rho((st)^{-1}) \\ \lambda(s^2) & \mapsto & \lambda(s^2) \\ \lambda(t)\rho(st) & \mapsto & \lambda(t)\rho(s). \end{cases}$$

is a G-equivariant isomorphism. □

Now we find that for the Hopf-Galois structures of type $C_4 \times C_2$ the Hopf algebra isomorphism classes are determined by the choice of s.

Lemma 3.2. *Let $s, s', t, t' \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$ and $s' \neq t'$. We have $L[A_{s,t}]^G \cong L[A_{s',t'}]^G$ if and only if $s = s'$.*

Proof. Recall the definition of $A_{s,t}$ from Lemma 2.2. The non-trivial G-orbits of $A_{s,t}$ (that is, those of length greater than one) are $\{\lambda(s), \lambda(s^{-1})\}$, $\{\lambda(s)\rho(t), \lambda(s^{-1})\rho(t)\}$ both with stabiliser $\langle s\rangle$. Therefore if $s \neq s'$ then there cannot be a G-equivariant isomorphism between $A_{s,t}$ and $A_{s',t'}$ for any choices of t, t'. For fixed s and t, t' satisfying $s \neq t$ and $s \neq t'$ the map $f : A_{s,t} \to A_{s,t'}$ defined by

$$f : \begin{cases} \lambda(s) & \mapsto & \lambda(s) \\ \rho(t) & \mapsto & \rho(t'). \end{cases}$$

is a G-equivariant isomorphism: □

With a nearly identical argument we now give the result for Hopf-Galois structures of type C_8.

Lemma 3.3. *Let $s, s', t, t' \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$ and $s' \neq t'$. We have $L[C_{s,t}]^G \cong L[C_{s',t'}]^G$ as Hopf algebras if and only if $t = t'$.*

Proof. Recall the definition of $C_{s,t}$ from Lemma 2.3. The nontrivial G-orbits of $C_{s,t}$ are $\{\eta_{s,t}, \eta_{s,t}^3\}$, $\{\eta_{s,t}^2, \eta_{s,t}^6\}$ and $\{\eta_{s,t}^5, \eta_{s,t}^7\}$, all with stabiliser $\langle t\rangle$. Therefore if $t \neq t'$ then there cannot be a G-equivariant isomorphism between $C_{s,t}$ and $C_{s',t'}$ for any choices of s, s'. For fixed t and s, s' satisfying

$s \neq t$ and $s' \neq t$ let $\eta_{s,t}$ and $\eta_{s',t}$ be generators of $C_{s,t}$ and $C_{s',t}$ respectively; then the map $f : C_{s,t} \to C_{s',t}$ defined by

$$f : \eta_{s,t} \mapsto \eta_{s',t}.$$

is a G-equivariant isomorphism. □

The result for the Hopf-Galois structures of type Q_8 is an instance of a well known result (see [11, Example 2.4], for example).

Lemma 3.4. *The Hopf algebras $L[\lambda(G)]^G$ and $L[\rho(G)]^G$ are not isomorphic as Hopf algebras.*

Proof. The G-action on $\rho(G)$ is trivial since $\lambda(G)$ and $\rho(G)$ commute. However, the G-action on $\lambda(G)$ is conjugation so that the G-orbits are the conjugacy classes. Therefore no G-equivariant isomorphism can exist. □

Finally, we can give the result for the Hopf-Galois structures of type D_4.

Lemma 3.5. *The Hopf algebras $L[D_{s,\lambda}]^G$ and $L[D_{s,\rho}]^G$ are pairwise non-isomorphic as Hopf algebras.*

Proof. Recall the definitions of $D_{s,\lambda}$ and $D_{s,\rho}$ from Lemma 2.5. The non-trivial G-orbits of $D_{s,\lambda}$ are

$$\{\lambda(s), \lambda(s^{-1})\}, \{\lambda(t)\rho(s), \lambda(t^{-1})\rho(s)\}, \text{ and } \{\lambda(st)\rho(s), \lambda((st)^{-1})\rho(s)\},$$

with stabilisers $\langle s\rangle$, $\langle t\rangle$, and $\langle st\rangle$ respectively. If $s \neq s'$ and $f : D_{s,\lambda} \to D_{s',\lambda}$ is a G-equivariant bijection then by considering stabilisers we see that $f(\lambda(s)) = \lambda(t')\rho(s')$ for some t'. But $\lambda(s)$ has order 4, whereas $\lambda(t')\rho(s')$ has order 2. Therefore f cannot be an isomorphism.

The non-trivial G-orbits of $D_{s,\rho}$ are

$$\{\lambda(s)\rho(t), \lambda(s^{-1})\rho(t)\} \text{ and } \{\lambda(s)\rho(st), \lambda(s^{-1})\rho(st)\}$$

both with stabiliser $\langle s\rangle$. Therefore if $s \neq s'$ then there cannot be a G-equivariant isomorphism between $D_{s,\lambda}$ and $D_{s',\lambda}$.

Finally, there cannot be a G-equivariant isomorphism between $D_{s,\lambda}$ and $D_{s',\rho}$ for any s, s', since these groups have different numbers of G-orbits. □

These results agree with the number of isomorphism classes of Hopf algebras for each type given in Table 1 of [4]. It may also be worth noting that our results imply that the Hopf-Galois structures of abelian type occur in pairs, with each pair arising from two different actions of a single Hopf algebra, and that, by contrast, each Hopf-Galois structure of nonabelian type arises from the action of a distinct Hopf algebra.

4. F-algebra isomorphisms

In this section we investigate the F-algebra structure of the Hopf algebras giving Hopf-Galois structures on L/F. We assume that the characteristic of F is not 2: this ensures the Hopf algebras are separable, hence semisimple, so that each has an Artin-Wedderburn decomposition (see section 3C of [5]).

We fix some notation. Since L/F is a quaternionic extension it has a unique biquadratic subextension K/F corresponding to the unique order 2 subgroup $\langle\sigma^2\rangle$ of G, so that $\mathrm{Gal}(K/F) = G/\langle\sigma^2\rangle$. Let $s, t \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$, and let α, β be elements of K such that $\alpha^2, \beta^2 \in F$, $s(\alpha) = \alpha, t(\alpha) = -\alpha, s(\beta) = -\beta$ and $t(\beta) = \beta$; note that $K = F(\alpha, \beta)$. We also fix an algebraic closure F^{alg} of F, and let $\Omega = \mathrm{Gal}(F^{\mathrm{alg}}/F)$.

If N is abelian then $H = L[N]^G$ is a commutative separable F-algebra, and hence, by [17, §6.3], corresponds to a finite Ω-set. Specifically, $L[N]^G$ corresponds to the Ω-set $\widehat{N} = \mathrm{Hom}(N, F^{\mathrm{alg}})$, where Ω acts on N by factoring through G, and on $\widehat{N}$ by $({}^{\omega}\chi)[\eta] = \omega(\chi({}^{\omega^{-1}}\eta))$ for all $\eta \in N$ (in fact, the action of Ω on $\widehat{N}$ factors through $\mathrm{Gal}(L'/K)$ for some cyclotomic extension L' of L). To make this correspondence explicit, let $\chi_1, \ldots, \chi_s \in \widehat{N}$ be a set of representatives for the Ω orbits of $\widehat{N}$, and for each $i \in \{1, \ldots, s\}$ let F_i be the fixed field of $\mathrm{Stab}_\Omega(\chi_i)$; then

$$H \cong \prod_{i=1}^{s} F_i \text{ as } F\text{-algebras.}$$

A result of Böltje and Bley [1, Lemma 2.2] shows how one may construct an F-basis of $L[N]^G$ corresponding to this decomposition: we have $L[N]^G = F^{\mathrm{alg}}[N]^\Omega$, and the group algebra $F^{\mathrm{alg}}[N]$ has a basis of mutually orthogonal idempotents, each corresponding to an element of $\widehat{N}$. The action of Ω on $F^{\mathrm{alg}}[N]$ permutes these idempotents, and by forming Ω-invariant linear combinations we obtain an F-basis of $L[N]^G$ corresponding to the decomposition above.

If $H = L[N]^G$ is a Hopf algebra whose underlying group N is isomorphic to $C_2 \times C_2 \times C_2$ then the values of the characters of N lie in F, so the action of Ω on $\widehat{N}$ factors through G. Using this observation we have:

Lemma 4.1. *Let $E_{s,t}$ be defined as in Lemma 2.1. Then we have*

$$L[E_{s,t}]^G \cong F^4 \times K \text{ as } F\text{-algebras.}$$

Proof. The dual group $\widehat{E}_{s,t}$ is generated by three characters:

$$\chi_1 : \begin{cases} \lambda(s)\rho(t) & \mapsto & -1 \\ \lambda(s^2) & \mapsto & 1 \\ \lambda(t)\rho(st) & \mapsto & 1 \end{cases},$$

$$\chi_2 : \begin{cases} \lambda(s)\rho(t) & \mapsto & 1 \\ \lambda(s^2) & \mapsto & -1 \\ \lambda(t)\rho(st) & \mapsto & 1 \end{cases},$$

and

$$\chi_3 : \begin{cases} \lambda(s)\rho(t) & \mapsto & 1 \\ \lambda(s^2) & \mapsto & 1 \\ \lambda(t)\rho(st) & \mapsto & -1 \end{cases}.$$

Let χ_0 denote the identity in $\widehat{E}_{s,t}$, and recall the G-orbit structure of $E_{s,t}$ in Lemma 3.1. It is easily verified that ${}^s\chi_2 = \chi_2\chi_3$, ${}^t\chi_2 = \chi_1\chi_2$ and ${}^{st}\chi_2 = \chi_1\chi_2\chi_3$ and that s and t act trivially on χ_0, χ_1, χ_3 and $\chi_1\chi_3$. Hence the orbits of G in $\widehat{E}_{s,t}$ are

$$\{\chi_0\}, \quad \{\chi_1\}, \quad \{\chi_3\}, \quad \{\chi_1\chi_3\}, \quad \{\chi_2, \chi_1\chi_2, \chi_2\chi_3, \chi_1\chi_2\chi_3\}.$$

The orbit representatives χ_0, χ_1, χ_3 $\chi_1\chi_3$ all have stabilizer G, and the orbit representative χ_2 has stabiliser $\langle s^2 \rangle$. Therefore we have $L[E_{s,t}]^G \cong F^4 \times K$, as claimed. □

For the remaining structures whose underlying group N is abelian there may exist characters of N whose values do not lie in the field F. In these cases the action of Ω on $\widehat{N}$ depends upon the intersection of L with certain cyclotomic extensions of F, and can be difficult to trace in detail. To overcome this problem we study the action of Ω on the group algebra $F^{\mathrm{alg}}[N]$, as in [1, Lemma 2.2]. As discussed above, we have $L[N]^G = F^{\mathrm{alg}}[N]^\Omega$, and the action of Ω factors through $\mathrm{Gal}(L'/K)$ for some cyclotomic extension L' of L. Thus, writing $G' = \mathrm{Gal}(L'/L)$, we have

$$L[N]^G = \left(L'[N]^{G'}\right)^G,$$

where the action of G' on $L'[N]$ is only on the coefficients. In the following two lemmas we suppress the details of this first step of the descent (if any), and begin with a convenient L-basis on $L[N]$ on which it is easy to follow the action of G. By forming G-invariant linear combinations of these basis elements we obtain a basis of $L[N]^G$ corresponding to its Artin-Wedderburn decomposition. Although working with bases in this way is rather cumbersome, it has the advantage of applying uniformly, whereas studying the orbits of Ω in $\widehat{N}$ can split into many cases, depending upon the roots of unity contained in L.

We continue with the Hopf algebras giving the structures of type $C_4 \times C_2$.

Lemma 4.2. *Let $A_{s,t}$ be defined as in Lemma 2.2. Then we have*

$$L[A_{s,t}]^G \cong F^4 \times F(\alpha, \iota)^d \text{ as } F\text{-algebras,}$$

where $\iota \in F^{alg}$ is such that $\iota^2 = -1$ and $d = 2/[F(\alpha, \iota) : F(\alpha)]$.

Proof. Let

$$
\begin{aligned}
b_0 &= \frac{1}{8}\big(1+\lambda(s)+\lambda(s^2)+\lambda(s^{-1})+\rho(t)^{-1}+\lambda(s)^{-1}\rho(t)+\rho(t)+\lambda(s)\rho(t)\big),\\
b_1 &= \frac{1}{8}\big(1-\lambda(s)+\lambda(s^2)-\lambda(s^{-1})-\rho(t)^{-1}+\lambda(s)^{-1}\rho(t)-\rho(t)+\lambda(s)\rho(t)\big),\\
b_2 &= \frac{1}{8}\big(1+\lambda(s)+\lambda(s^2)+\lambda(s^{-1})-\rho(t)^{-1}-\lambda(s)^{-1}\rho(t)-\rho(t)-\lambda(s)\rho(t)\big),\\
b_3 &= \frac{1}{8}\big(1-\lambda(s)+\lambda(s^2)-\lambda(s^{-1})+\rho(t)^{-1}-\lambda(s)^{-1}\rho(t)+\rho(t)-\lambda(s)\rho(t)\big),\\
b_4 &= \frac{1}{4}\big(1-\lambda(s^2)+\lambda(s)^{-1}\rho(t)-\lambda(s)\rho(t)\big),\\
b_5 &= \frac{1}{4}\big(1-\lambda(s^2)-\lambda(s)^{-1}\rho(t)+\lambda(s)\rho(t)\big),\\
b_6 &= \frac{1}{4}\big(\lambda(s)-\lambda(s^{-1})-\rho(t)^{-1}+\rho(t)\big),\\
b_7 &= \frac{1}{4}\big(-\lambda(s)+\lambda(s^{-1})-\rho(t)^{-1}+\rho(t)\big).
\end{aligned}
$$

It is easily verified that these 8 elements of $L[A_{s,t}]$ are linearly independent over L and so form an L-basis of $L[A_{s,t}]$. Recall from Lemma 3.2 that the non-trivial G-orbits of $A_{s,t}$, are $\{\lambda(s),\lambda(s^{-1})\}$, $\{\lambda(s)\rho(t),\lambda(s^{-1})\rho(t)\}$, both with stabiliser $\langle s\rangle$. From this we see that b_0, b_1, b_2 and b_3 are fixed by G, that ${}^t b_4 = b_5$, and that ${}^t b_6 = b_7$. Therefore the following linear combinations of the above elements are all fixed by G, and in fact form a basis of $L[A_{s,t}]^G$ over F.

$$
\begin{aligned}
a_0 &= b_0,\\
a_1 &= b_1,\\
a_2 &= b_2,\\
a_3 &= b_3,\\
a_{4,0} &= b_4 + b_5 = \frac{1}{2}\big(1-\lambda(s^2)\big) = \mathfrak{e},\\
a_{4,1} &= \alpha(b_4 - b_5) = -\alpha\mathfrak{e}\lambda(s)\rho(t),\\
a_{4,2} &= b_6 + b_7 = \mathfrak{e}\rho(t),\\
a_{4,3} &= \alpha(b_6 - b_7) = \alpha\mathfrak{e}\lambda(s).
\end{aligned}
$$

We have $a_i a_j = \delta_{i,j} a_i$ for $i,j = 0,1,2,3$ and $a_{4,k}a_i = a_i a_{4,k} = 0$ for all $i = 0,1,2,3$ and $k = 0,1,2,3$. Finally, we consider the multiplication table of the $a_{4,k}$.

	$a_{4,0}$	$a_{4,1}$	$a_{4,2}$	$a_{4,3}$
$a_{4,0}$	$a_{4,0}$	$a_{4,1}$	$a_{4,2}$	$a_{4,3}$
$a_{4,1}$	$a_{4,1}$	$\alpha^2 a_{4,0}$	$a_{4,3}$	$\alpha^2 a_{4,2}$
$a_{4,2}$	$a_{4,2}$	$a_{4,3}$	$-a_{4,0}$	$-a_{4,1}$
$a_{4,3}$	$a_{4,3}$	$\alpha^2 a_{4,2}$	$-a_{4,1}$	$-\alpha^2 a_{4,0}$

From the table it is clear that we have the claimed decomposition. □

We use a similar process for the Hopf algebras giving the Hopf-Galois structures of type C_8.

Lemma 4.3. *Let $C_{s,t}$ be defined as in Lemma 2.3. Then we have*

$$L[C_{s,t}]^G \cong F^2 \times F(\beta\iota)^{d_1} \times F(r\iota, \beta\iota)^{d_1 d_2} \text{ as } F\text{-algebras,}$$

where $r, \iota \in F^{alg}$ such that $r^2 = 2$, $\iota^2 = -1$ and where $d_1 = 2/[F(\beta\iota) : F]$ and $d_2 = 2/[F(r\iota, \beta\iota) : F(\beta\iota)]$.

Proof. Let $\eta = \eta_{s,t}$ as defined in Lemma 2.3, so that $C_{s,t} = \langle\eta\rangle$, and let

$$\begin{aligned}
b_0 &= \frac{1}{8}\big(1 + \eta + \eta^2 + \eta^3 + \eta^4 + \eta^5 + \eta^6 + \eta^7\big),\\
b_1 &= \frac{1}{8}\big(1 - \eta + \eta^2 - \eta^3 + \eta^4 - \eta^5 + \eta^6 - \eta^7\big),\\
b_2 &= \frac{1}{4}\big(1 - \eta^2 + \eta^4 - \eta^6\big),\\
b_3 &= \frac{1}{4}\big(\eta - \eta^3 + \eta^5 - \eta^7\big),\\
b_4 &= \frac{1}{2}\big(1 - \eta^4\big),\\
b_5 &= \frac{1}{2}\big(\eta^3 - \eta^7\big),\\
b_6 &= \frac{1}{2}\big(\eta^2 - \eta^6\big),\\
b_7 &= \frac{1}{2}\big(\eta - \eta^5\big).
\end{aligned}$$

It is easily verified that these 8 elements of $L[C_{s,t}]$ are linearly independent over L and so form an L-basis of $L[C_{s,t}]$. Recall from Lemma 3.3 that the nontrivial G-orbits of $C_{s,t}$ are $\{\eta, \eta^3\}$, $\{\eta^2, \eta^6\}$ and $\{\eta^5, \eta^7\}$, all with stabiliser $\langle t\rangle$. From this we see that b_0, b_1, b_2 and b_4 are fixed by G, that ${}^s b_3 = -b_3$, ${}^s b_6 = -b_6$, and that ${}^s b_5 = b_7$. Therefore the following linear combinations of the above elements are all fixed by G, and in fact form a basis of $L[C_{s,t}]$ over L:

$$\begin{aligned}
a_0 &= b_0,\\
a_1 &= b_1,\\
a_{2,0} &= b_2,\\
a_{2,1} &= \beta b_3 = \beta b_2 \eta,\\
a_{3,0} &= b_4 = \mathfrak{e},\\
a_{3,1} &= \beta b_6 = \beta \mathfrak{e} \eta^2,\\
a_{3,2} &= (b_5 + b_7) = \mathfrak{e}(\eta^3 + \eta),\\
a_{3,3} &= \beta(b_5 - b_7) = \beta \mathfrak{e}(\eta^3 - \eta).
\end{aligned}$$

We have $a_i a_j = \delta_{i,j} a_i$ for $i, j = 0, 1$, $a_i a_{2,k} = 0$ for $i = 0, 1$ and $k = 0, 1$, $a_i a_{3,k} = 0$ for $i = 0, 1$ and $k = 0, 1, 2, 3$, and $a_{2,k} a_{3,l} = 0$ for $k = 0, 1$ and $l = 0, 1, 2, 3$. Finally, we consider the multiplication tables of the $a_{2,k}$ and the $a_{3,k}$.

	$a_{2,0}$	$a_{2,1}$
$a_{2,0}$	$a_{2,0}$	$a_{2,1}$
$a_{2,1}$	$a_{2,1}$	$-\beta^2 a_{2,0}$

	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$
$a_{3,0}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$
$a_{3,1}$	$a_{3,1}$	$-\beta^2 a_{3,0}$	$a_{3,3}$	$-\beta^2 a_{3,2}$
$a_{3,2}$	$a_{3,2}$	$a_{3,3}$	$-2a_{3,0}$	$-2a_{3,1}$
$a_{3,3}$	$a_{3,3}$	$-\beta^2 a_{3,2}$	$-2a_{3,1}$	$2\beta^2 a_{3,0}$

From these tables it is clear that we have the claimed decomposition. □

Comparing these results with those obtained in section 3, we see that two Hopf algebras giving Hopf-Galois structures of the same abelian type on L/F are isomorphic as Hopf algebras if and only if they are isomorphic as F-algebras. On the other hand, although Hopf algebras giving Hopf-Galois structures of different types are not isomorphic as Hopf algebras, in certain situations it is possible that they are isomorphic as F-algebras. For example: if $\beta = \iota$ then $L[E_{s,t}]^G \cong L[A_{s,t}]^G$ as F-algebras.

The remaining structures are of nonabelian type, and so we cannot employ the methods of [17, §6.3] or [1, Lemma 2.2]. We emulate the same process using the character table in place of the dual group of our underlying group. We write down a convenient L-basis of $L[N]$ and form G-invariant linear combinations of these basis elements. We find that certain quaternion algebras appear in the decompositions, and so we fix notation for these: for

$x, y \in F^\times$, let $(x, y)_F$ denote the quaternion algebra with F-basis $1, u, v, w$ satisfying the relations $u^2 = x$, $v^2 = y$, and $uv = w = -vu$. In addition, let $a = \alpha^2 \in F^\times$, $b = \beta^2 \in F^\times$, where $\alpha, \beta \in K$ are as defined at the beginning of this section.

We begin with the Hopf algebras giving the classical and canonical nonclassical structures of type Q_8.

Lemma 4.4. *We have*

$$L[\rho(G)]^G \cong K[G] \cong F^4 \times (-1, -1)_F \text{ as } F\text{-algebras}$$

and

$$L[\lambda(G)]^G \cong F^4 \times (-a, -b)_F \text{ as } F\text{-algebras.}$$

Proof. Let $\mu \in \{\rho, \lambda\}$. The character table for $\mu(G)$ is

	1	$\{\mu(s^2)\}$	$\{\mu(s), \mu(s^{-1})\}$	$\{\mu(t), \mu(t^{-1})\}$	$\{\mu(st), \mu((st)^{-1})\}$
χ_0	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	1	-1	1	-1
χ_3	1	1	-1	-1	1
ψ	2	-2	0	0	0

First we consider the case $\mu = \rho$, corresponding to the classical Hopf-Galois structure on L/F. For $k = 0, 1, 2, 3$, let e_k be the orthogonal idempotent corresponding to the character χ_k. The idempotent corresponding to the 2-dimensional representation is

$$e_\psi = \frac{1}{2}\Big(1 - \rho(s^2)\Big) = \mathfrak{e}.$$

The following is a set of 8 linearly independent elements of $L[\rho(G)]$, and each element is fixed by G since the action of G on $\rho(G)$ is trivial. It is therefore a basis of $L[\rho(G)]^G = F[\rho(G)]$ over F:

$$\{e_0, e_1, e_2, e_3, \mathfrak{e}, \mathfrak{e}\rho(s), \mathfrak{e}\rho(t), \mathfrak{e}\rho(st)\}.$$

The e_k are orthogonal idempotents, and each is also orthogonal to every element of the set $\{\mathfrak{e}, \mathfrak{e}\rho(s), \mathfrak{e}\rho(t), \mathfrak{e}\rho(st)\}$. This set spans a 4-dimensional F-algebra, which is isomorphic to the quaternion algebra $(-1, -1)_F$ via the F-algebra isomorphism defined by $\mathfrak{e}\rho(s) \mapsto u$, $\mathfrak{e}\rho(t) \mapsto v$. Therefore we have the claimed decomposition.

Now we consider the case $\mu = \lambda$, corresponding to the canonical nonclassical Hopf-Galois structure on L/F. As discussed in Lemma 3.4 the G-orbits of $\lambda(G)$ are the conjugacy classes. As above, for $k = 0, 1, 2, 3$ let e_k be the orthogonal idempotent corresponding to the character χ_k, and note that these are fixed by G. The idempotent $\mathfrak{e}$, corresponding to the 2-dimensional

representation of $\lambda(G)$, is also fixed by G. Now consider the L-linearly independent set $\{\mathfrak{e}, \mathfrak{e}\lambda(s), \mathfrak{e}\lambda(t), \mathfrak{e}\lambda(st)\}$. An element of the F-algebra generated by this set is of the form

$$x = a_0\mathfrak{e} + a_1\mathfrak{e}\lambda(s) + a_2\mathfrak{e}\lambda(t) + a_3\mathfrak{e}\lambda(st) \text{ with } a_k \in L \text{ for } k = 0, 1, 2, 3.$$

The element x is fixed by G if and only if $a_1 = a_1'\alpha$, $a_2 = a_2'\beta$ and $a_3 = a_3'\alpha\beta$ for some $a_0, a_1', a_2', a_3' \in F$. Thus the following set is an F-basis of $L[\lambda(G)]^G$:

$$\{e_0, e_1, e_2, e_3, \mathfrak{e}, \alpha\mathfrak{e}\lambda(s), \beta\mathfrak{e}\lambda(t), \alpha\beta\mathfrak{e}\lambda(st)\}.$$

As above, the e_k are orthogonal to each other and to every element of the set $\{\mathfrak{e}, \alpha\mathfrak{e}\lambda(s), \beta\mathfrak{e}\lambda(t), \alpha\beta\mathfrak{e}\lambda(st)\}$. This set spans a 4-dimensional F-algebra, which is isomorphic to the quaternion algebra $(-a, -b)_F$ via the F-algebra isomorphism defined by $\alpha\mathfrak{e}\lambda(s) \mapsto u, \beta\mathfrak{e}\lambda(t) \mapsto v$. Therefore we have the claimed decomposition. □

It may appear that the Hopf algebras giving the classical and canonical non-classical structures are not isomorphic as F-algebras. However, we have:

Lemma 4.5. *We have $(-a, -b)_F \cong (-1, -1)_F$ as F-algebras.*

Proof. By a result of Witt [9, Theorem I.1.1], the fact that $K = F(\alpha, \beta)$ embeds into a quaternionic extension of F implies that the quadratic form $ax_1^2 + bx_2^2 + abx_3^2$ is equivalent to the quadratic form $x_1^2 + x_2^2 + x_3^2$. These are the norm forms of the subspaces of pure quaternions of $(-a, -b)_F$ and $(-1, -1)_F$, respectively. Therefore these subspaces are isometric, and so (see [12, III, Theorem 2.5]) $(-a, -b)_F \cong (-1, -1)_F$ as F-algebras. □

Corollary 4.6. *We have $L[\rho(G)]^G \cong L[\lambda(G)]^G \cong F^4 \times (-1, -1)_F$ as F-algebras.*

In fact, this result follows from an unpublished theorem of Greither which states that if L/F is *any* Galois extension of fields then $F[G] \cong L[\lambda(G)]^G$ as F-algebras. See [10, Theorem 5.2] for more details.

Finally, we have the Hopf algebras giving the structures of type D_4.

Lemma 4.7. *Let $D_{s,\lambda}$ and $D_{s,\rho}$ be defined as in Lemma 2.5. Then we have*

$$L[D_{s,\lambda}]^G \cong F^4 \times (-a, b)_F \text{ as } F\text{-algebras}$$

and

$$L[D_{s,\rho}]^G \cong F^4 \times (-1, a)_F \text{ as } F\text{-algebras.}$$

Proof. In order to control the size of the table below, let us write

$$O_1 = \{\lambda(s), \lambda(s^{-1})\}, \qquad O_2 = \{\lambda(t)\rho(s), \lambda(t^{-1})\rho(s)\},$$

and

$$O_3 = \{\lambda(st)\rho(s), \lambda((st)^{-1})\rho(s)\}.$$

Then the character table for $D_{s,\lambda}$ is the following:

	1	$\{\lambda(s^2)\}$	O_1	O_2	O_3
χ_0	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	1	-1	1	-1
χ_3	1	1	-1	-1	1
ψ	2	-2	0	0	0

As in the proof of Lemma 4.4, for $k = 0, 1, 2, 3$ let e_k be the orthogonal idempotent corresponding to the character χ_k, and note that the idempotent corresponding to the 2-dimensional representation is $\mathfrak{e}$. Recall from Lemma 3.5 that the non-trivial G-orbits of $D_{s,\lambda}$ are O_1, O_2, and O_3 with stabilisers $\langle s\rangle$, $\langle t\rangle$, and $\langle st\rangle$ respectively. Hence each e_k is fixed by G. Now consider the L-linearly independent set $\{\mathfrak{e}, \mathfrak{e}\lambda(s), \mathfrak{e}\lambda(t)\rho(s), \mathfrak{e}\lambda(st)\rho(s)\}$. An element of the F-algebra generated by these elements is of the form

$$x = a_0\mathfrak{e} + a_1\mathfrak{e}\lambda(s) + a_2\mathfrak{e}\lambda(t)\rho(s) + a_3\mathfrak{e}\lambda(st)\rho(s) \text{ with } a_k \in L \text{ for } k = 0, 1, 2, 3.$$

The element x is fixed by G if and only if $a_1 = a_1'\alpha$, $a_2 = a_2'\beta$ and $a_3 = a_3'\alpha\beta$ for some $a_0, a_1', a_2', a_3' \in F$. The set

$$\{e_0, e_1, e_2, e_3, \mathfrak{e}, \alpha\mathfrak{e}\lambda(s), \beta\mathfrak{e}\lambda(t)\rho(s), \alpha\beta\mathfrak{e}\lambda(st)\rho(s)\}$$

is therefore an F-basis of $L[D_{s,\lambda}]^G$. The e_k are orthogonal to each other and to every element of the set $\{\mathfrak{e}, \alpha\mathfrak{e}\lambda(s), \beta\mathfrak{e}\lambda(t)\rho(s), \alpha\beta\mathfrak{e}\lambda(st)\rho(s)\}$. This set spans a 4-dimensional F-algebra, which is isomorphic to the quaternion algebra $(-a, b)_F$ via the F-algebra isomorphism defined by $\alpha\mathfrak{e}\lambda(s) \mapsto u, \beta\mathfrak{e}\lambda(t)\rho(s) \mapsto v$. Therefore we have the claimed decomposition.

We determine the structure of $L[D_{s,\rho}]^G$ by essentially the same method, and so we omit some of the details. In notation analogous to that employed above, we find that the set

$$\{e_0, e_1, e_2, e_3, \mathfrak{e}, \mathfrak{e}\rho(s), \alpha\mathfrak{e}\lambda(s)\rho(t), \alpha\mathfrak{e}\lambda(s)\rho(st)\}$$

is an F-basis of $L[D_{s,\lambda}]^G$. The final four elements span a 4-dimensional F-algebra, which is isomorphic to the quaternion algebra $(-1, a)_F$ via the F-algebra isomorphism defined by $\mathfrak{e}\rho(s) \mapsto u, \alpha\mathfrak{e}\lambda(s)\rho(t) \mapsto v$. Therefore we have the claimed decomposition. □

As in the case of the Hopf algebras giving the Hopf-Galois structures of Q_8 type, some of the quaternion algebras appearing in the decompositions above are isomorphic:

Lemma 4.8. *We have $(-a, b)_F \cong (-1, a)_F$ as F-algebras.*

Proof. Write $[-a, -b], [-1, a]$ for the classes of $(-a, b)_F, (-1, a)_F$ in the Brauer group $\mathrm{Br}(F)$. It is sufficient to show that $[-a, -b] = [-1, a]$. We refer to [12, Chapters III and IV] for properties of quaternion algebras over F

and their classes in $\mathrm{Br}(F)$. Using the result of Lemma 4.5 we have $[-a,-b] = [-1,-1]$, and so in $\mathrm{Br}(F)$ we have

$$\begin{aligned}
[-a,b][-a,-b] &= [-a,-b^2] \text{ by [12, III, Theorem 2.11]} \\
&= [-a,-1] \text{ by [12, III, Proposition 1.1]} \\
&= [-1,-a] \\
&= [-1,a][-1,-1] \text{ by [12, III, Theorem 2.11]} \\
&= [-1,a][-a,-b].
\end{aligned}$$

Cancelling $[-a,-b]$, we obtain $[-a,b] = [-1,a] = [a,-1]$, as claimed. Therefore $(-a,b)_F \cong (-1,a)_F$ as F-algebras. □

Corollary 4.9. *We have*

$$L[D_{s,\rho}]^G \cong L[D_{s,\lambda}]^G \cong F^4 \times (-1,a)_F \text{ as } F\text{-algebras.}$$

In order to better understand the F-algebra structure of the Hopf algebras $L[D_{s,\rho}]^G$, we investigate the relationships between $(-1,a)_F, (-1,b)_F$ and $(-1,ab)_F$.

Lemma 4.10. *Let $x,y \in \{a,b,ab\}$ with $x \neq y$. Then we have $(-1,x)_F \cong (-1,xy)_F$ as F-algebras if and only if $(-1,y)_F \cong M_2(F)$ as F-algebras.*

Proof. In $\mathrm{Br}(F)$ we have $[-1,xy] = [-1,x][-1,y]$, so $[-1,x] = [-1,xy]$ if and only if $[-1,y] = [-1,1]$. That is, $(-1,x)_F \cong (-1,xy)_F$ as F-algebras if and only if $(-1,y)_F \cong (-1,1)_F \cong M_2(F)$ as F-algebras. □

Lemma 4.10 suggests three scenarios for the quaternion algebras $(-1,a)_F$, $(-1,b)_F$, and $(-1,ab)_F$: all three are isomorphic to matrix rings, exactly one is isomorphic to a matrix ring and the other two are isomorphic to the same division algebra, or each is isomorphic to a distinct division algebra. We conclude with examples illustrating that each of these three cases does occur.

Example 4.11. *Suppose that -1 is a square in F. Then for $x \in \{a,b,ab\}$ we have that -1 occurs as the norm of an element of the field $F(x)$, and so $(-1,x)_F \cong (-1,1)_F \cong M_2(F)$* [9, Proposition I.1.6]. *Therefore in this case we have*

$$L[D_{s,\rho}]^G \cong L[D_{t,\rho}]^G \cong L[D_{st,\rho}]^G \cong F^4 \times M_2(F)$$

as F-algebras.

Example 4.12. *Let $F = \mathbb{Q}$, $\alpha = \sqrt{11}$, $\beta = \sqrt{2}$. Then by* [7] *$K = \mathbb{Q}(\alpha,\beta)$ can be embedded in a quaternionic extension L of $\mathbb{Q}$. In this case we have $(-1,b)_{\mathbb{Q}} \cong (-1,1)_{\mathbb{Q}} \cong M_2(\mathbb{Q})$ as $\mathbb{Q}$-algebras since 2 is the norm of the element $1+i \in \mathbb{Q}(i)$, and so by Lemma 4.10 we have $(-1,a)_{\mathbb{Q}} \cong (-1,ab)_{\mathbb{Q}}$ as $\mathbb{Q}$-algebras. However, $(-1,a)_{\mathbb{Q}} \ncong M_2(\mathbb{Q})$, since no element of $\mathbb{Q}(i)$ has norm 11. Therefore in this case we have $L[D_{t,\rho}]^G \cong \mathbb{Q}^4 \times M_2(\mathbb{Q})$ and*

$$L[D_{s,\rho}]^G \cong L[D_{st,\rho}]^G \cong \mathbb{Q}^4 \times (-1,a) \ncong \mathbb{Q}^4 \times M_2(\mathbb{Q})$$

as $\mathbb{Q}$-algebras.

Example 4.13. *Let* $F = \mathbb{Q}$, $\alpha = \sqrt{11}$, $\beta = \sqrt{6}$. *Then by* [16, Example 4.4] $K = \mathbb{Q}(\alpha, \beta)$ *can be embedded in a quaternionic extension* L *of* $\mathbb{Q}$. *In this case none of* $(-1, a)_{\mathbb{Q}}, (-1, b)_{\mathbb{Q}}, (-1, ab)_{\mathbb{Q}}$ *is isomorphic to* $M_2(\mathbb{Q})$ *as a* $\mathbb{Q}$*-algebra, since none of* $6, 11, 66$ *occurs as the norm of an element of* $\mathbb{Q}(i)$. *Therefore by Lemma 4.10 these quaternion algebras are all nonisomorphic as* $\mathbb{Q}$*-algebras, and so we have*

$$L[D_{s,\rho}]^G \ncong L[D_{t,\rho}]^G \ncong L[D_{st,\rho}]^G$$

as $\mathbb{Q}$*-algebras.*

References

[1] Bley, Werner; Boltje, Robert. Lubin–Tate formal groups and module structure over Hopf orders. *J. Théor. Nombres Bordeaux* **11** (1999), no. 2, 269–305. MR1745880, Zbl 0979.11053, doi: 10.5802/jtnb.251. 227, 228, 231

[2] Byott, N. P. Uniqueness of Hopf Galois structure for separable field extensions. *Comm. Algebra* **24** 1996, no. 10, 3217–3228. MR1402555, Zbl 0878.12001, doi: 10.1080/00927879608825743. 221

[3] Childs, Lindsay N. Taming wild extensions: Hopf algebras and local Galois module theory. Mathematical Surveys and Monographs, 80. *American Mathematical Society, Providence, RI*, 2000. viii+215 pp. ISBN: 0-8218-2131-8. MR1767499, Zbl 0944.11038, doi: 10.1090/surv/080. 220

[4] Crespo, Teresa; Salguero, Marta. Computation of Hopf Galois structures on low degree separable extensions and classification of those for degrees p^2 and $2p$. Preprint, 2018. arXiv:1802.09948. 221, 226

[5] Curtis, Charles W.; Reiner, Irving. Methods of representation theory. I. With applications to finite groups and orders. Pure and Applied Mathematics. A Wiley-Interscience Publication. *John Wiley & Sons, Inc., New York*, 1981. xxi+819 pp. ISBN: 0-471-18994-4. MR0632548, Zbl 0469.20001. 227

[6] Fröhlich, A. Artin root numbers and normal integral bases for quaternion fields. *Invent. Math.* **17** (1972), 143–166. MR0323759, Zbl 0261.12008, doi: 10.1007/BF01418937.

[7] Fujisaki, Genjiro. An elementary construction of Galois quaternion extension. *Proc. Japan Acad. Ser. A Math. Sci.* **66** (1990), no. 3, 80–83. MR1051598, Zbl 0707.11077, doi: 10.3792/pjaa.66.80. 235

[8] Greither, Cornelius; Pareigis, Bodo. Hopf Galois theory for separable field extensions. *J. Algebra* **106** (1987), no. 1, 239–258. MR0878476, Zbl 0615.12026, doi: 10.1016/0021-8693(87)90029-9. 220

[9] Jensen, Christian U.; Yui, Noriko. Quaternion extensions. *Algebraic geometry and commutative algebra, Vol. I*, 155–182. *Kinokuniya, Tokyo*, 1988. MR0977759, Zbl 0691.12011. 233, 235

[10] Koch, Alan; Kohl, Timothy; Truman, Paul J.; Underwood, Robert. The structure of Hopf algebras acting on Galois extensions with dihedral groups. Preprint, 2017. To appear in *C. Pillen, e. a. (Ed.) Advances in Algebra: Research from the Southern Regional Algebra Conference. Proc. in Math. Stat. Springer.* arXiv:1708.09822. 220, 233

[11] Koch, Alan; Kohl, Timothy; Truman, Paul J.; Underwood, Robert. Isomorphism problems for Hopf–Galois structures on separable field extensions. *J. Pure Appl. Algebra* **223** (2019), no. 5, 2230–2245. MR3906546, Zbl 1403.16031, arXiv:1711.05554, doi: 10.1016/j.jpaa.2018.07.014. 220, 224, 226

[12] Lam, Tsit-Yuen. Introduction to quadratic forms over fields. Graduate Studies in Mathematics, 67. *American Mathematical Soc., Providence, RI*, 2005. xxii+550 pp. ISBN: 0-8218-1095-2. MR2104929, Zbl 1068.11023, doi: 10.1090/gsm/067. 233, 234, 235

[13] Martinet, Jacques. Modules sur l'algèbre du groupe quaternionien. *Ann. Sci. École Norm. Sup* (4) **4** (1971), 399–408. MR0291208, Zbl 0219.12012, doi: 10.24033/asens.1216. 220

[14] Martinet, Jacques. Sur les extensions à groupe de Galois quaternionien. *C.R. Acad. Sci. Paris Sér. A–B* **274** (1972), A933–A935. MR0299593, Zbl 0235.12005.

[15] Smoktunowicz, Agata; Vendramin, Leandro. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra* **2** (2018), no. 1, 47–86. MR3763907, Zbl 06857320, arXiv:1705.06958, doi: 10.4171/JCA/2-1-3. 221

[16] Vaughan, Theresa P. Constructing quaternionic fields. *Glasgow Math. J.* **34** (1992), no. 1, 43–54. MR1145631, Zbl 0746.12003, doi: 10.1017/S0017089500008533. 236

[17] Waterhouse, William C. Introduction to affine group schemes. Graduate Texts in Mathematics, 66. *Springer-Verlag, New York-Berlin*, 1979. xi+164 pp. ISBN: 0-387-90421-2. MR0547117, Zbl 0442.14017, doi: 10.1007/978-1-4612-6217-6. 227, 231

(Stuart Taylor) School of Computing and Mathematics, Colin Reeves Building, Keele University, Staffordshire, ST5 5BG, UK.
S.J.Taylor@Keele.ac.uk

(Paul Truman) School of Computing and Mathematics, Colin Reeves Building, Keele University, Staffordshire, ST5 5BG, UK.
P.J.Truman@Keele.ac.uk

This paper is available via http://nyjm.albany.edu/j/2019/25-13.html.