ON ρ-CONJUGATE HOPF-GALOIS STRUCTURES

PAUL J. TRUMAN

Abstract. The Hopf-Galois structures admitted by a Galois extension of fields L/K with Galois group G correspond bijectively with certain subgroups of $\mathrm{Perm}(G)$. We use a natural partition of the set of such subgroups to obtain a method for partitioning the set of corresponding Hopf-Galois structures, which we term *ρ-conjugation*. We study properties of this construction, with particular emphasis on the Hopf-Galois analogue of the Galois correspondence, the connection with skew left braces, and applications to questions of integral module structure in extensions of local or global fields. In particular, we show that the number of distinct ρ-conjugates of a given Hopf-Galois structure is determined by the corresponding skew left brace, and that if H, H' are Hopf algebras giving ρ-conjugate Hopf-Galois structures on a Galois extension of local or global fields L/K then an ambiguous ideal $\mathfrak{B}$ of L is free over its associated order in H if and only if it is free over its associated order in H'. We exhibit a variety of examples arising from interactions with existing constructions in the literature.

1. Introduction

A *Hopf-Galois structure* on a finite extension of fields L/K consists of a cocommutative K-Hopf algebra H making L into an H-module algebra satisfying a certain non-degeneracy condition (see [6, (2.7) Definition] for the full definition). The motivating example is a Galois extension L/K with Galois group G: in this case the group algebra $K[G]$ (with its usual action on L) gives a Hopf-Galois structure on the extension. Hopf-Galois structures allow many results from Galois theory to be generalized to extensions which are inseparable or non-normal, but there is also considerable interest in their applications to Galois extensions: various authors have studied the number of Hopf-Galois structures admitted by particular extensions, the structure of the Hopf algebras involved, and questions concerning the Hopf-Galois analogue of the Galois correspondence. We highlight two applications in particular. Firstly, it has recently been discovered that each Hopf-Galois structure on a Galois extension yields a *skew left brace*; these objects are intensively studied because they can be used to generate set-theoretic solutions of the Yang-Baxter equation. The translation of existence, classification, and structural results between Hopf-Galois theory and skew brace theory has enriched both disciplines. Secondly, Hopf-Galois theory has been applied fruitfully to questions originating in Galois module theory: if L/K is a finite extension of local or global fields and H is

1991 *Mathematics Subject Classification.* Primary 16T05; Secondary 12F10, 11S23, 20N99.

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

a Hopf algebra giving a Hopf-Galois structure on the extension then we may study each fractional ideal $\mathfrak{B}$ of L as a module over its *associated order* in H. This raises the possibility of comparing the structure of $\mathfrak{B}$ as a module over its associated orders in the various Hopf-Galois structures admitted by the extension. We refer the reader to [9] for a recent survey of these and other related topics.

A theorem of Greither and Pareigis [12] classifies the Hopf-Galois structures admitted by a finite separable extension of fields L/K. In the special case of Galois extension with Galois group G their theorem implies that Hopf-Galois structures admitted by L/K correspond bijectively with regular subgroups N of $\mathrm{Perm}(G)$ that are normalized by the image of the left regular representation $\lambda : G \hookrightarrow \mathrm{Perm}(G)$. In [15] it is noted that such a subgroup N need not be normalized by the image of the *right* regular representation $\rho : G \hookrightarrow \mathrm{Perm}(G)$, and that for each $g \in G$ the subgroup $\rho(g)N\rho(g)^{-1}$ is again regular and normalized by $\lambda(G)$, and therefore corresponds to a Hopf-Galois structure on L/K. Following [18] we call this method of partitioning the set of Hopf-Galois structures on L/K *ρ-conjugation*. We review existing results concerning ρ-conjugate Hopf-Galois structures in more detail in Section 2 of this paper.

In Section 3 we study the Hopf-Galois analogue of the Galois correspondence, showing that the lattices of subfields realized by ρ-conjugate Hopf-Galois structures are intimately related to one another. Section 4 concerns the skew braces corresponding to ρ-conjugate Hopf-Galois structures; we show that the number of distinct ρ-conjugates of a given Hopf-Galois structure is determined by the corresponding skew brace, and obtain a criterion for a Hopf-Galois structure to have no nontrivial ρ-conjugates.

In Section 5 we suppose that L/K is a Galois extension of local or global fields and study questions of integral module structure. We show that if an ambiguous ideal $\mathfrak{B}$ of L is free over its associated order in a particular Hopf-Galois structure then it is free over its associated order in each of the Hopf-Galois structures that are ρ-conjugate to the original one. Finally, in Section 6 we study how ρ-conjugation interacts with other constructions in the literature, including Hopf-Galois structures arising from fixed point free pairs of homomorphisms (due to Byott and Childs), those arising from abelian maps (instigated by Childs and generalized by Koch), and induced Hopf-Galois structures (due to Crespo, Rio, and Vela).

Acknowledgements: I am grateful to Prof. Anna Rio for the suggestion to study the interaction between ρ-conjugate Hopf-Galois structures and induced Hopf-Galois structures, to Prof. Alan Koch for comments on an early draft of this paper, and to the anonymous referee for numerous improvements to the exposition and interpretation of the results.

Statement of competing interests: The author declares that there are no competing interests.

2. ρ-conjugate Hopf-Galois structures

In this section we recall the definition of ρ-conjugate Hopf-Galois structures and some of their known properties.

Let L/K be a Galois extension of fields with Galois group G. As mentioned in Section 1, a theorem of Griether and Pareigis [12] implies that the Hopf-Galois structures admitted by L/K correspond bijectively with regular subgroups N of $\mathrm{Perm}(G)$ that are normalized by the image of G under the left regular representation $\lambda : G \hookrightarrow \mathrm{Perm}(G)$. The normalization condition is equivalent to requiring that N is stable under the action of G on $\mathrm{Perm}(G)$ given by $g * \eta = \lambda(g)\eta\lambda(g)^{-1}$ for all $\eta \in \mathrm{Perm}(G)$ and all $g \in G$; accordingly, we shall refer to the subgroups of interest as *G-stable regular subgroups*. To ease notation when dealing with long compositions of permutations we shall write $\eta[g]$ for the effect of a permutation $\eta \in \mathrm{Perm}(G)$ on an element $g \in G$.

In general, a G-stable regular subgroup N of $\mathrm{Perm}(G)$ need not be normalized by the image of the right regular representation $\rho : G \hookrightarrow \mathrm{Perm}(G)$. This motivates the following (see also [15, Example 2.7]).

Proposition 2.1. Let N be a G-stable regular subgroup of $\mathrm{Perm}(G)$, and let $g \in G$. Then $N_g := \rho(g)N\rho(g)^{-1}$ is a G-stable regular subgroup of $\mathrm{Perm}(G)$.

Proof. Clearly N_g is a subgroup of $\mathrm{Perm}(G)$ that is isomorphic to N. Since N acts transitively on G, we have

$$N_g[g] = (N[e_G])g^{-1} = Gg^{-1} = G,$$

so N_g acts transitively on G. Therefore N_g is a regular subgroup of $\mathrm{Perm}(G)$. To show G-stability, we note that $\lambda(G)$ and $\rho(G)$ centralize one another inside $\mathrm{Perm}(G)$; hence for $h \in G$ and $\eta \in N$ we have

$$\begin{aligned} h * \rho(g)\eta\rho(g)^{-1} &= \lambda(h)\rho(g)\eta\rho(g)^{-1}\lambda(h)^{-1} \\ &= \rho(g)\lambda(h)\eta\lambda(h)^{-1}\rho(g)^{-1} \\ &= \rho(g)(h * \eta)\rho(g)^{-1}. \end{aligned}$$

We have $h * \eta \in N$ because N is G-stable; hence $\rho(g)(h * \eta)\rho(g)^{-1} \in N_g$, and so N_g is G-stable. □

Definition 2.2. We shall call two G-stable regular subgroups N, N' of $\mathrm{Perm}(G)$ *ρ-conjugate* to mean that $N' = N_g$ for some $g \in G$. In this case we shall also say that the Hopf-Galois structures corresponding to N, N' are ρ-conjugate to one another.

It is clear that ρ-conjugation is an equivalence relation on the set of G-stable regular subgroups of $\mathrm{Perm}(G)$, and so yields an equivalence relation on the set of Hopf-Galois structures admitted by L/K. Given a G-stable regular subgroup N, we have $N_g = N_h$ if and only if $\rho(g^{-1}h) \in \mathrm{Norm}_{\mathrm{Perm}(G)}(N)$. In particular, if G is abelian then $\rho(G) = \lambda(G)$, and since N is G-stable we have $N_g = N$ for all $g \in G$. We shall return to the question of determining the number of distinct ρ-conjugates of a given G-stable regular subgroup in Section 4.

Example 2.3. Let p, q be prime numbers with $p \equiv 1 \pmod{q}$ and let L/K be a Galois extension whose Galois group G is isomorphic to the metacyclic group of

order pq:

$$G = \langle s, t \mid s^p = t^q = e,\ tst^{-1} = s^d \rangle,$$

where d is a positive integer of multiplicative order q modulo p. Let $\eta = \lambda(s)\rho(t) \in \mathrm{Perm}(G)$ and $N = \langle \eta \rangle$. It is routine to verify that N is G-stable and regular. We find that $N_t = N$ and that

$$N_{s^i} = \langle \lambda(s)\rho(s^{i(1-d)}t) \rangle$$

for each $i = 0, \ldots, p-1$. These subgroups are all distinct, and so we obtain a family of p mutually ρ-conjugate Hopf-Galois structures on L/K.

Example 2.4. Let n be an even natural number and let L/K be a Galois extension whose Galois group G is isomorphic to the dihedral group of order $2n$:

$$G = \langle r, s \mid r^n = s^2 = e,\ srs^{-1} = r^{-1} \rangle.$$

Let $N = \langle \lambda(r)\rho(s), \lambda(s) \rangle$. Then N is G stable, regular, and isomorphic to D_{2n}. We find that $N_s = N$ and that

$$N_{r^k} = \langle \lambda(r)\rho(r^{2k}s), \lambda(s) \rangle$$

for each $k = 0, \ldots, n/2 - 1$. These subgroups are all distinct, and so we obtain a family of $n/2$ mutually ρ-conjugate Hopf-Galois structures on L/K.

Byott [4] enumerates the Hopf-Galois structures admitted by a Galois extension of degree pq. In particular, [4, Theorem 6.2] implies that the Hopf-Galois structures corresponding to the G-stable regular subgroups constructed in Example 2.3 are all of those for which the corresponding subgroup of $\mathrm{Perm}(G)$ is cyclic (that is: those of cyclic *type*). On the other hand, Kohl [19], enumerates the Hopf-Galois structures of dihedral type admitted by a Galois extension whose Galois group is isomorphic to the dihedral group of order $2n$; the precise formula depends upon the congruence class of n modulo 8, but if n is even there are at least $(n/2+1)|\Upsilon_n|$, where $|\Upsilon_n|$ is the number of square roots of 1 modulo n. The Hopf-Galois structures corresponding to the G-stable regular subgroups constructed in Example 2.4 account for less than half of these. Similarly, it is known that a Galois extension with Galois group isomorphic to the quaternion group of order 8 admits 22 Hopf-Galois structures [21, Table A.1]. Using the descriptions of the corresponding G-stable regular subgroups found in [23] we find that the 6 cyclic subgroups fall into 3 pairs under ρ-conjugation, whereas each of the remaining 16 subgroups is normalized by $\rho(G)$. We expect that situation of Example 2.3, in which all of the G-stable regular subgroups of a given type are mutually ρ-conjugate, to be rare.

We shall shed more light on these examples, and construct others, in Section 6.

In Greither and Pareigis's original paper classifying Hopf-Galois structures on separable extensions [12] they show that if N is a G-stable regular subgroup of $\mathrm{Perm}(G)$ then so too is

$$N^{opp} = \mathrm{Cent}_{\mathrm{Perm}(G)}(N).$$

In [17] the Hopf-Galois structure corresponding to N^{opp} is called the *opposite* of the one corresponding to N, and [18, Corollary 7.2] shows that for each $g \in G$ we

have $(N_g)^{opp} = (N^{opp})_g$. We shall see fruitful applications of this interaction in Section 5.

Example 2.5. Recall the hypotheses and notation of Example 2.4 above. The opposite of the subgroup N constructed in that example is the subgroup generated by $\rho(s)$ and the permutation μ_0 defined by

$$\mu_0[r^i s^j] = r^{i+(-1)^{i+j}} s^j.$$

Exploiting the interaction between opposite subgroups and ρ-conjugation, we find that for each $k = 0, \ldots, n/2 - 1$ the opposite of the subgroup N_{r^k} is generated by $\rho(s)$ and the permutation μ_k defined by

$$\mu_k[r^i s^j] = r^{i+(-1)^{i+j+k}} s^j.$$

The Hopf algebra giving the Hopf-Galois structure corresponding to a G-stable regular subgroup N is the fixed ring $L[N]^G$, where G acts on L via the usual Galois action and on N via $g * \eta = \lambda(g)\eta\lambda(g)^{-1}$. It is possible for two distinct Hopf-Galois structures on L/K to involve isomorphic Hopf algebras, and it is well known (see [15, Corollary 2.3], for example) that we have $L[N]^G \cong L[N']^G$ if and only if there is a group isomorphism $\phi : N \xrightarrow{\sim} N'$ such that $h * \phi(\eta) = \phi(h * \eta)$ for all $\eta \in N$ and all $h \in G$. More explicitly: ϕ induces an isomorphism of L-Hopf algebras $\phi : L[N] \xrightarrow{\sim} L[N']$, which descends to an isomorphism of K-Hopf algebras $\phi : L[N]^G \xrightarrow{\sim} L[N']^G$.

Turning to ρ-conjugate subgroups we have (see also [15, Example 2.7])

Proposition 2.6. For each $g \in G$ we have $L[N]^G \cong L[N_g]^G$ as K-Hopf algebras.

Proof. Consider the isomorphism $\phi : N \to N_g$ defined by $\phi(\eta) = \rho(g)\eta\rho(g)^{-1}$ for all $\eta \in N$. By the proof of Proposition 2.1 we have $h*\phi(\eta) = \phi(h*\eta)$ for all $\eta \in N$ and all $h \in G$, so ϕ yields an isomorphism of K-Hopf algebras $\phi : L[N]^G \xrightarrow{\sim} L[N_g]^G$. Explicitly, we have

$$\phi\left(\sum_{\eta\in N} c_\eta \eta\right) = \sum_{\eta\in N} c_\eta \rho(g)\eta\rho(g)^{-1}. \tag{1}$$

□

3. The Hopf-Galois correspondence

If a Hopf algebra H gives a Hopf-Galois structure on a finite extension of fields L/K then each Hopf subalgebra H' of H has a corresponding fixed field

$$L^{H'} = \{x \in L \mid z \cdot x = \varepsilon(z)x \text{ for all } z \in H'\},$$

where $\varepsilon : H \to K$ denotes the counit map of H. In analogy with the classical Galois correspondence, we have $[L : L^{H'}] = \dim_K(H')$. The correspondence from Hopf subalgebras of H to intermediate fields of the extension L/K is inclusion reversing and injective, but not surjective in general; we say that an intermediate field M is *realizable with respect to* H to mean that there is a Hopf subalgebra H' of H such that $L^{H'} = M$. The proportion of the intermediate fields of the extension L/K that

are realizable with respect to H has been called the *Galois correspondence ratio* for H, and has been studied by several authors in recent years, with particular interest in situations for which it is equal to 1 (see [8], [9, Chapter 7], or [22], for example).

Specializing to the case in which L/K is a Galois extension, we have seen that each Hopf algebra giving a Hopf-Galois structure on L/K has the form $L[N]^G$ with N some G-stable regular subgroup of $\mathrm{Perm}(G)$; in this case the Hopf subalgebras of $L[N]^G$ are precisely the sets $L[P]^G$ with P a subgroup of N that is itself G-stable (see [10, Theorem 2.3] or [9, Theorem 7.2]). Abusing notation, we write L^P in place of of $L^{L[P]^G}$; since $\dim_K(L[P]^G) = |P|$, we then have $[L : L^P] = |P|$.

Turning to ρ-conjugate subgroups we have

Proposition 3.1. For each $g \in G$ the lattices of intermediate fields of L/K realizable with respect to the Hopf-Galois structures given by $L[N]^G$ and $L[N_g]^G$ are isomorphic.

Proof. By virtue of the Hopf algebra isomorphism $\phi : L[N]^G \xrightarrow{\sim} L[N_g]^G$ constructed in Proposition 2.6 the lattices of Hopf subalgebras of $L[N]^G$ and $L[N_g]^G$ are isomorphic. The result then follows from the discussion above. □

As a consequence of this, the Galois correspondence ratios for the Hopf-Galois structures given by $L[N]^G$ and $L[N_g]^G$ are the same for all $g \in G$. In fact, we can identify precisely how the intermediate fields realizable with respect to $L[N]^G$ and $L[N_g]^G$ are related to one another. As a first step, we study the actions of these Hopf algebras on the field L.

It follows from the theorem of Greither and Pareigis that the action of an element $\sum_{\eta\in N} c_\eta\eta \in L[N]^G$ on L is given by

$$\left(\sum_{\eta\in N} c_\eta\eta\right)\cdot x = \sum_{\eta\in N} c_\eta\eta^{-1}[e_G](x) \text{ for all } x \in L \tag{2}$$

(see [9, Proposition 4.14], for example). The action of $L[N_g]^G$ on L is given by an analogous formula. We describe how the isomorphism ϕ interacts with these actions.

Proposition 3.2. Let $x \in L$. Then for all $z \in L[N]^G$ we have

$$\phi(z)\cdot x = g(z\cdot g^{-1}(x)).$$

Proof. Write $z = \sum_{\eta\in N} c_\eta\eta$ with $c_\eta \in L$. Since $z \in L[N]^G$ we have $z = h * z$ for all $h \in G$. In particular,

$$z = g * z = \sum_{\eta\in N} g(c_\eta)\lambda(g)\eta\lambda(g)^{-1},$$

and so

$$\begin{aligned}\phi(z) &= \sum_{\eta\in N} g(c_\eta)\rho(g)\lambda(g)\eta\lambda(g)^{-1}\rho(g)^{-1}\\ &= \sum_{\eta\in N} g(c_\eta)\lambda(g)\rho(g)\eta\rho(g)^{-1}\lambda(g)^{-1}\end{aligned}$$

since $\lambda(G)$ and $\rho(G)$ centralize each other inside $\mathrm{Perm}(G)$. Therefore

$$\begin{aligned}
\phi(z)\cdot x &= \left(\sum_{\eta\in N} g(c_\eta)\lambda(g)\rho(g)\eta\rho(g)^{-1}\lambda(g)^{-1}\right)\cdot x\\
&= \sum_{\eta\in N} g(c_\eta)\lambda(g)\rho(g)\eta^{-1}\rho(g)^{-1}\lambda(g)^{-1}[e_G](x)\\
&= \sum_{\eta\in N} g(c_\eta)\lambda(g)\rho(g)\eta^{-1}[g^{-1}g](x)\\
&= \sum_{\eta\in N} g(c_\eta)g\eta^{-1}[e_G]g^{-1}(x)\\
&= g\left(\sum_{\eta\in N} c_\eta\eta^{-1}[e_G]g^{-1}(x)\right)\\
&= g\left(\sum_{\eta\in N} c_\eta\eta\right)\cdot g^{-1}(x)\\
&= g\left(z\cdot g^{-1}(x)\right),
\end{aligned}$$

as claimed. □

Now we have the following:

Theorem 3.3. An intermediate field M of L/K is realizable with respect to $L[N]^G$ if and only if the intermediate field $g(M)$ is realizable with respect to $L[N_g]^G$.

Proof. Suppose that M is realizable with respect to $L[N]^G$. Then $M = L^P$ for some G-stable subgroup P of N. We have $\phi(L[P]^G) = L[P_g]^G$, a Hopf subalgebra of $L[N_g]^G$, and for $x \in L$ we have

$$\begin{aligned}
x \in L^{P_g} &\Leftrightarrow \phi(z)\cdot x = \varepsilon(z)x \text{ for all } z \in L[P]^G\\
&\Leftrightarrow g(z\cdot g^{-1}(x)) = \varepsilon(z)x \text{ for all } z \in L[P]^G, \text{ by Proposition 3.2}\\
&\Leftrightarrow z\cdot g^{-1}(x) = \varepsilon(z)g^{-1}(x) \text{ for all } z \in L[P]^G\\
&\Leftrightarrow g^{-1}(x) \in L^P = M\\
&\Leftrightarrow x \in g(M).
\end{aligned}$$

Hence $g(M)$ is realizable with respect to $L[N_g]^G$. For the converse statement we replace N by N_g and g by g^{-1} in the argument above. □

Example 3.4. Recall the hypotheses and notation of Example 2.3 above. Each of the subgroups N_{s^i} is cyclic of order pq, and therefore has a unique subgroup P_i of order p and a unique subgroup Q_i of order q; by uniqueness, each of these is G-stable. Since N_{s^i} is generated by $\lambda(s)\rho(s^{i(1-d)}t)$, we see that $P_i = \langle\lambda(s)\rangle$ regardless of i, and that $Q_i = \langle\rho(s^{i(1-d)}t)\rangle$. Therefore $L^{P_i} = L^{\langle s\rangle}$ (the unique intermediate field of degree p over K) and $L^Q = L^{\langle s^{i(1-d)}t\rangle}$. Thus each of this family of ρ-conjugate Hopf-Galois structures realizes the intermediate fields $L, K, L^{\langle s\rangle}$, and a

unique intermediate field of degree q over K, and each intermediate field of degree q over K is realized by exactly one Hopf-Galois structure in this family.

4. Skew braces

A (left) skew brace is a triple $(B, \star, \circ)$ where B is a set and $\star, \circ$ are binary operations on B, each making B into a group, such that

$$x \circ (y \star z) = (x \circ y) \star x^{-1} \star (x \circ z) \text{ for all } x, y, z \in B. \tag{3}$$

Here x^{-1} denotes the inverse of x with respect to $\star$; we denote the inverse of x with respect to $\circ$ by $\overline{x}$. We call Equation 3 the *left skew brace relation*; the right skew brace relation is analogous. We call a skew brace *two-sided* if both the left and right skew brace relations hold for all triples of elements of B. Skew braces with underlying set B yield solutions of the set theoretic Yang-Baxter equation on B; we can then obtain solutions of the Yang-Baxter equation over any field by using B as the basis for a vector space (see [16, §2], for example).

The connection between skew braces and Hopf-Galois structures on Galois extensions follows from an observation by Bachiller [1, Remark 2.6]. One formulation is as follows: a finite skew brace $(B, \star, \circ)$, yields two left regular representation maps $\lambda_\star, \lambda_\circ : B \hookrightarrow \mathrm{Perm}(B)$; we find that $\lambda_\star(B)$ is a $(B, \circ)$-stable regular subgroup of $\mathrm{Perm}(B)$, and so corresponds to a Hopf-Galois structure on a Galois extension with Galois group $(B, \circ)$. Conversely, if $G = (G, \circ)$ is a finite group and N is a G-stable regular subgroup of $\mathrm{Perm}(G)$ then the map $\eta \mapsto \eta[e_G]$ is a bijection from N to G; we use this to define a second binary operation $\star$ on G by

$$\eta[e_G] \star \mu[e_G] = \eta\mu[e_G].$$

Then $(G, \star) \cong N$, and the fact that N is G-stable implies that $(G, \star, \circ)$ is a skew brace. As noted in [20, Proposition 2.1] and [18, Proposition 3.1], two G-stable regular subgroups $N, N' \leq \mathrm{Perm}(G)$ yield isomorphic skew braces if and only if $N' = \varphi^{-1} N \varphi$ for some $\varphi \in \mathrm{Aut}(G, \circ)$, and yield the same skew brace if and only if $N' = \varphi^{-1} N \varphi$ for some $\varphi \in \mathrm{Aut}(G, \star, \circ)$ (the group of automorphisms of $(G, \circ)$ that also respect $\star$). Since these results involve conjugation by *automorphisms* of $(G, \circ)$, the following alternative formulation of ρ-conjugate subgroups is useful when studying connections with skew braces (see also [18, Proposition 4.1]). We note, however, that this formulation is less suitable for studying results such as Proposition 2.6 and Proposition 3.2, whose proofs depend heavily on the fact that $\lambda(G)$ and $\rho(G)$ centralize each other inside $\mathrm{Perm}(G)$.

Proposition 4.1. Let N be a G-stable regular subgroup of $\mathrm{Perm}(G)$, and let $g \in G$. Then $N_g = \varphi_g N \varphi_g^{-1}$, where φ_g is the inner automorphism of G corresponding to g.

Proof. We may write $\varphi_g = \rho(g)\lambda(g)$, and we then have

$$\begin{aligned} \varphi_g N \varphi_g^{-1} &= \rho(g)\lambda(g) N \lambda(g)^{-1} \rho(g)^{-1} \\ &= \rho(g) N \rho(g)^{-1} \text{ since } N \text{ is } G\text{-stable} \\ &= N_g. \end{aligned}$$

□

This observation immediately implies that ρ-conjugate Hopf-Galois structures yield isomorphic skew braces under the correspondence described above ([18, Corollary 4.1]).

The number of distinct ρ-conjugates of a given G-stable regular subgroup N of $\mathrm{Perm}(G)$ can be studied via the corresponding skew brace.

Theorem 4.2. Let N be a G-stable regular subgroup of $\mathrm{Perm}(G)$, let $(G, \star, \circ)$ be the corresponding skew brace, and let $g \in G$. The following are equivalent:

i) The G-stable regular subgroup N is normalized by $\rho(g)$;
ii) The inner automorphism φ_g of $\mathrm{Aut}(G, \circ)$ is an element of $\mathrm{Aut}(G, \star, \circ)$;
iii) We have $(y \star z) \circ g = (y \circ g) \star g^{-1} \star (z \circ g)$ for all $y, z \in G$.

Corollary 4.3. Let $G' = \{g \in G \mid \varphi_g \in \mathrm{Aut}(G, \star, \circ)\}$. Then the G-stable regular subgroup N has $|G|/|G'|$ distinct ρ-conjugates.

Corollary 4.4. The G-stable regular subgroup N is normalized by $\rho(G)$ if and only if $(G, \star, \circ)$ is a two-sided skew brace.

Proof of Theorem 4.2. By Proposition 4.1 we have $N_g = \varphi_g N \varphi_g^{-1}$, and the discussion above then implies that $N_g = N$ if and only if $\varphi_g \in \mathrm{Aut}(G, \star, \circ)$. Hence (i) and (ii) are equivalent.

Now suppose that (ii) holds. By the left skew brace relation (3), for all $y, z \in G$ we have

$$g \circ (y \star z) = (g \circ y) \star g^{-1} \star (g \circ z).$$

Since $\varphi_g \in \mathrm{Aut}(G, \star, \circ)$, so is $\varphi_g^{-1} = \varphi_{\overline{g}}$. Applying this to the equation above yields

$$\begin{aligned}
& \varphi_{\overline{g}}(g \circ (y \star z)) = \varphi_{\overline{g}}((g \circ y) \star g^{-1} \star (g \circ z)) \\
\Rightarrow \quad & \varphi_{\overline{g}}(g \circ (y \star z)) = \varphi_{\overline{g}}(g \circ y) \star \varphi_{\overline{g}}(g^{-1}) \star \varphi_{\overline{g}}(g \circ z) \\
\Rightarrow \quad & \overline{g} \circ g \circ (y \star z) \circ g = (\overline{g} \circ g \circ y \circ g) \star \varphi_{\overline{g}}(g)^{-1} \star (\overline{g} \circ g \circ z \circ g) \\
\Rightarrow \quad & (y \star z) \circ g = (y \circ g) \star g^{-1} \star (z \circ g);
\end{aligned}$$

Hence (iii) holds.

Finally, suppose that (iii) holds. Then for all $y, z \in G$ we have

$$\begin{aligned}
\varphi_{\overline{g}}(y \star z) &= \overline{g} \circ (y \star z) \circ g \\
&= \overline{g} \circ ((y \circ g) \star g^{-1} \star (z \circ g)) \text{ by (iii)} \\
&= (\overline{g} \circ y \circ g) \star \overline{g}^{-1} \star (\overline{g} \circ g^{-1}) \star \overline{g}^{-1} \star (\overline{g} \circ z \circ g) \text{ by Equation 3.}
\end{aligned}$$

Now by a well known skew brace identity (see [13, Lemma 1.7, part (2)], for example) we have

$$\overline{g}^{-1} \star (\overline{g} \circ g^{-1}) \star \overline{g}^{-1} = (\overline{g} \circ g)^{-1} = e_G;$$

applying this to the final line above yields

$$\varphi_{\overline{g}}(y \star z) = (\overline{g} \circ y \circ g) \star (\overline{g} \circ z \circ g) = \varphi_{\overline{g}}(y) \star \varphi_{\overline{g}}(z),$$

and so $\varphi_{\overline{g}} \in \mathrm{Aut}(G, \star, \circ)$. Therefore $\varphi_g \in \mathrm{Aut}(G, \star, \circ))$, so (ii) holds. □

5. Integral module structure

We now suppose that L/K is a Galois extension of local or global fields (in any characteristic) with Galois group G. As discussed briefly in Section 1, Hopf-Galois structures can be used in this context to study the structure of fractional ideals $\mathfrak{B}$ of L. More precisely: if H is a Hopf algebra giving a Hopf-Galois structure on the extension then L is a free H-module of rank 1 (this is a Hopf-Galois analogue of the classical normal basis theorem), and we seek integral analogues of this result. Each fractional ideal $\mathfrak{B}$ of L has an *associated order* 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 we may study the structure of $\mathfrak{B}$ as an $\mathfrak{A}_H(\mathfrak{B})$-module, with particular emphasis on determining criteria for it to be free (necessarily of rank 1). By construction, $\mathfrak{A}_H(\mathfrak{B})$ is the largest subring of H for which $\mathfrak{B}$ is a module, and it is the only order in H over which $\mathfrak{B}$ can possibly be free.

The most famous results in this area are due to Byott [3], who exhibits Galois extensions L/K of p-adic fields for which the valuation ring $\mathfrak{O}_L$ is not free over $\mathfrak{A}_{K[G]}(\mathfrak{O}_L)$, but is free over $\mathfrak{A}_H(\mathfrak{O}_L)$ for some other Hopf algebra H giving a Hopf-Galois structure on the extension. On the other hand, in [24] and [25] we show that a fractional ideal $\mathfrak{B}$ of L is free over its associated order in a particular Hopf-Galois structure if and only if it is free over its associated order in the opposite Hopf-Galois structure. The main result of this section is in a similar vein. Recall that an *ambiguous ideal* of L is a fractional ideal of L that is invariant under the action of G. (In particular: the ring of algebraic integers $\mathfrak{O}_L$ is an ambiguous ideal of L, and if L/K is an extension of local fields then every fractional ideal of L is an ambiguous ideal.) We will prove:

Theorem 5.1. Let $L[N]^G$ give a Hopf-Galois structure on L/K, and let $g \in G$. Then an ambiguous ideal $\mathfrak{B}$ of L is free over its associated order in $L[N]^G$ if and only if it is free over its associated order in $L[N_g]^G$.

Corollary 5.2. An ambiguous ideal of L is free over its associated order in $L[N]^G$ if and only if it is free over its associated order in $L[N_g]^G$ for all $g \in G$.

The proof of Theorem 5.1 does not depend upon the fact that L is a field, so if L/K is an extension of global fields and $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$ then we may apply the theorem to the Galois algebra $L_\mathfrak{p} = K_\mathfrak{p} \otimes_K L$. This yields:

Corollary 5.3. If L/K is an extension of global fields then an ambiguous ideal of L is locally free over its associated order in $L[N]^G$ if and only if it is locally free over its associated order in $L[N_g]^G$ for all $g \in G$.

Proof of Theorem 5.1. Let $\mathfrak{A}$ denote the associated order of $\mathfrak{B}$ in $L[N]^G$, and let $\mathfrak{A}_g$ denote the associated order of $\mathfrak{B}$ in $L[N_g]^G$. Suppose that $\mathfrak{B}$ is a free $\mathfrak{A}$-module, with generator $x \in \mathfrak{B}$. We shall show that $\mathfrak{A}_g = \phi(\mathfrak{A})$ and that $\mathfrak{B}$ is a free $\mathfrak{A}_g$-module with generator $g(x)$ (note that $g(x) \in \mathfrak{B}$ because $\mathfrak{B}$ is an ambiguous ideal of L).

Since ϕ is an isomorphism of K-Hopf algebras, it is immediate that $\phi(\mathfrak{A})$ is an order in $L[N_g]^G$. Now let $y \in \mathfrak{B}$. Since $\mathfrak{B}$ is an ambiguous ideal of L we have $g^{-1}(y) \in \mathfrak{B}$, and since $\mathfrak{B}$ is a free $\mathfrak{A}$-module with generator x there exists a unique element $z \in \mathfrak{A}$ such that $z \cdot x = g^{-1}(y)$. Now consider the action of the element $\phi(z) \in \phi(\mathfrak{A})$ on the element $g(x) \in \mathfrak{B}$. We have:

$$\begin{aligned} \phi(z) \cdot g(x) &= g(z \cdot g^{-1}(g(x))) \text{ by Proposition 3.2} \\ &= g(g^{-1}(y)) \\ &= y. \end{aligned}$$

Hence given $y \in \mathfrak{B}$ there exists a unique element $\phi(z)$ of the order $\phi(\mathfrak{A})$ in $L[N_g]^G$ such that $\phi(z) \cdot g(x) = y$, and so $\mathfrak{B}$ is a free $\phi(\mathfrak{A})$-module with generator $g(x)$. Since $\mathfrak{A}_g$ is the only order in $L[N_g]^G$ over which $\mathfrak{B}$ can be free, we conclude that $\phi(\mathfrak{A}) = \mathfrak{A}_g$.

For the converse statement we replace N by N_g and g by g^{-1} in the argument above. □

The interaction between Theorem 5.1 and the previously mentioned results concerning integral module structure with respect to opposite Hopf-Galois structures can cause one instance of freeness to propagate to a whole family.

Theorem 5.4. Consider the Hopf-Galois structures given by $L[N_g]^G$ and $L[N_g^{opp}]^G$ as g runs through the elements of G. An ambiguous ideal $\mathfrak{B}$ of L is either free over its associated orders in all of these Hopf-Galois structures or in none of them.

Proof. By Corollary 5.2 the ambiguous ideal $\mathfrak{B}$ is free over its associated order in $L[N]^G$ if and only if it is free over its associated order in $L[N_g]^G$ for each $g \in G$. Now applying [25, Theorem 1.2] to each $L[N_g]^G$ we find that $\mathfrak{B}$ is free over its associated order in $L[N_g]^G$ if and only if it is free over its associated order in $L[N_g^{opp}]^G$. □

Example 5.5. Let p, q be odd primes with $p \equiv 1 \pmod{q}$ and let L/K be a Galois extension of local or global fields whose Galois group G is isomorphic to the metacyclic group of order pq

$$G = \langle s, t \mid s^p = t^q = e,\ tst^{-1} = s^d \rangle,$$

as in Example 2.3. For $k = 0, \ldots, p-1$ let

$$N_k = \langle \lambda(s), \lambda(t)\rho(s^k t) \rangle.$$

It is routine to verify that each N_k is distinct, G-stable, regular, and isomorphic to G. We find that $\rho(t)$ normalizes each N_k, and that $\rho(s)N_k\rho(s^{-1}) = N_{k+1-d}$. Hence the subgroups N_k are mutually ρ-conjugate, and by [18, Corollary 7.2] the same is true for their opposites N_k^{opp}. Thus we obtain a family of $2p$ Hopf-Galois structures on L/K. By Theorem 5.4, an ambiguous ideal $\mathfrak{B}$ of L is either free over its associated orders in all of these $2p$ Hopf-Galois structures or in none of them.

6. Interactions with existing constructions

In this section we study the interactions between ρ-conjugation and various results concerning the construction and enumeration of Hopf-Galois structures on a Galois extension L/K. (We no longer assume that L/K is an extension of local or global fields.)

6.1. **Byott's translation theorem and fixed-point free pairs of homomorphisms.** Many results concerning the construction and enumeration of Hopf-Galois structures on separable field extensions employ Byott's translation theorem [2] to address some of the combinatorial difficulties inherent to Greither-Pareigis theory. Specializing to the Galois case, Byott's theorem may be summarized as follows: let M be an abstract group of the same order as G, and consider *regular embeddings* $\alpha : M \to \mathrm{Perm}(G)$ (that is: embeddings with regular image). Such an embedding yields a bijection $a : M \to G$ defined by $a(\mu) = \alpha(\mu)[e_G]$ for all $\mu \in M$, and thence a regular embedding $\beta : G \to \mathrm{Perm}(M)$ defined by $\beta(g) = a^{-1}\lambda(g)a$ for all $g \in G$. Byott's theorem asserts that this construction yields a bijection between regular embeddings of M into $\mathrm{Perm}(G)$ and regular embeddings of G into $\mathrm{Perm}(M)$. Furthermore: $\alpha(M)$ is G-stable if and only if $\beta(G) \subseteq \mathrm{Hol}(M) = \lambda(M)\,\mathrm{Aut}(M) \subseteq \mathrm{Perm}(M)$, and $\alpha(M) = \alpha'(M)$ if and only if there exists $\theta \in \mathrm{Aut}(M)$ such that $\beta'(g) = \theta\beta(g)\theta^{-1}$ for all $g \in G$.

We can study ρ-conjugate Hopf-Galois structures from this perspective, using the reformulation expressed in Proposition 4.1. Given a regular embedding $\alpha : M \to \mathrm{Perm}(G)$ and an element $g \in G$, the map $\alpha_g : M \to \mathrm{Perm}(G)$ defined by $\alpha_g(\mu) = \varphi_g\alpha(\mu)\varphi_g^{-1}$ for all $\mu \in M$ is a regular embedding with image $\alpha(M)_g$. We then find the following:

Lemma 6.1. Let $\beta : G \to \mathrm{Hol}(M)$ be the embedding corresponding to α. Then the embedding $\beta_g : G \to \mathrm{Hol}(M)$ corresponding to α_g is given by $\beta_g = \beta\varphi_{g^{-1}}$.

Proof. The bijection $a_g : M \to G$ corresponding to α_g is given by

$$a_g(\mu) = \varphi_g\alpha(\mu)\varphi_{g^{-1}}[e_G] = \varphi_g\alpha(\mu)[e_G] = \varphi_g a(\mu).$$

Hence for $h \in G$ and $\mu \in M$ we have

$$\begin{aligned}
\beta_g(h)[\mu] &= a^{-1}\varphi_g^{-1}\lambda_G(h)\varphi_g a[\mu] \\
&= a^{-1}\varphi_g^{-1}(hga[\mu]g^{-1}) \\
&= a^{-1}(g^{-1}hga[\mu]g^{-1}g) \\
&= a^{-1}\lambda(\varphi_{g^{-1}}(h))a[\mu] \\
&= \beta(\varphi_{g^{-1}}(h))[\mu].
\end{aligned}$$

Hence $\beta_g = \beta\varphi_{g^{-1}}$, as claimed. □

As an application of Lemma 6.1 we study the interaction between ρ-conjugation and Hopf-Galois structures on Galois extensions arising from *fixed point free* pairs of homomorphisms, due to Byott and Childs [5]. Given finite groups G, M of the same order, a pair of homomorphisms $f_1, f_2 : G \to M$ is called fixed point free if

the only element $h \in G$ for which $f_1(h) = f_2(h)$ is $h = e_G$. Given such a pair of homomorphisms, the map $\beta_{f_1,f_2} : G \to \mathrm{Hol}(M)$ defined by

$$\beta_{f_1,f_2}(h) = \lambda(f_1(h))\rho(f_2(h)) \text{ for all } h \in G$$

is a regular embedding of G into $\mathrm{Hol}(M)$ (where λ, ρ denote the left and right regular representations of M), and therefore yields a Hopf-Galois structure of type M on a Galois extension with Galois group G. Applying Lemma 6.1 we obtain immediately

Proposition 6.2. Let $f_1, f_2 : G \to \mathrm{Hol}(M)$ be a fixed point free pair of homomorphisms, with corresponding regular embedding $\beta : G \to \mathrm{Hol}(M)$, and let $g \in G$. For $i = 1, 2$ let $f_{i,g} = f_i\varphi_g$. Then $f_{1,g}, f_{2,g}$ is a fixed point free pair of homomorphisms, and the corresponding embedding of G into $\mathrm{Hol}(M)$ is β_g.

Example 6.3. Let n be an even natural number and let $G = \langle r, s\rangle$ and $M = \langle \mu, \pi\rangle$ both be isomorphic to the dihedral group of order $2n$ (here r, μ have order n and s, π have order 2). Fix $0 \le k \le n/2 - 1$ and define $f_1 : G \to M$ by $f_1(r^i s^j) = \mu^i\pi^j$ and $f_2 : G \to M$ by $f_2(r^i s^j) = (\mu^{2k}\pi)^i$. Then f_1, f_2 form a fixed point free pair of homomorphisms, and the corresponding embedding $\beta : G \hookrightarrow \mathrm{Hol}(M)$ is given by

$$\beta(r) = \lambda(\mu)\rho(\mu^{2k}\pi), \quad \beta(s) = \lambda(\pi).$$

(Here λ, ρ denote the left and right regular representations of M.) We find that composing β with φ_s results in an equivalent embedding, whereas composing with each φ_{r^ℓ} for $0 \le \ell \le n/2 - 1$ gives an inequivalent embedding. Thus we obtain $n/2$ mutually ρ-conjugate Hopf-Galois structures of dihedral type on a Galois extension with Galois group isomorphic to G. In fact, these are the Hopf-Galois structures described in Example 2.4.

6.2. **Hopf-Galois structures arising from abelian maps.** An *abelian map* is a group endomorphism with abelian image. In [7] Childs shows that fixed point free abelian maps on a finite group G yield a family of Hopf-Galois structures on a Galois extension L/K with Galois group G. This approach is generalized by Koch [14], as follows: let $\psi : G \to G$ be an abelian map, and for each $h \in G$ define $\eta_\psi(h) \in \mathrm{Perm}(G)$ by

$$\eta_\psi(h) = \lambda(h\psi(h)^{-1})\rho(\psi(h)^{-1}).$$

Then $N_\psi = \{\eta_\psi(h) \mid h \in G\}$ is a G-stable regular subgroup of $\mathrm{Perm}(G)$ [14, Theorem 3.1], which therefore corresponds to a Hopf-Galois structure on L/K.

Proposition 6.4. Let ψ be an abelian map on G and let N_ψ be the corresponding G-stable regular subgroup of $\mathrm{Perm}(G)$. Then for each $g \in G$ the subgroup $N_{\psi,g}$ arises from an abelian map on G.

Proof. By Proposition 4.1 we have $N_{\psi,g} = \varphi_g N_\psi \varphi_g^{-1}$. It is shown in [18, Proposition 5.1] that if ψ is an abelian map on G and $\varphi \in \mathrm{Aut}(G)$ then the map $\varphi\psi\varphi^{-1}$ is also an abelian map on G, and $N_{\varphi\psi\varphi^{-1}} = \varphi N_\psi \varphi^{-1}$. Thus $N_{\psi,g}$ arises from the abelian map $\psi' = \varphi_g\psi\varphi_g^{-1}$ on G. □

Example 6.5. Let $n \geq 5$ and suppose that G is isomorphic to the symmetric group S_n. In [14, Example 3.7] Koch shows that the abelian maps on G correspond bijectively with elements $x \in S_n$ of order at most 2, as follows:

$$\psi_x(t) = \begin{cases} e & \text{if } t \in A_n \\ x & \text{if } t \notin A_n \end{cases}$$

Let N_x be the G-stable regular subgroup arising from the abelian map ψ_x. Applying Proposition 6.4 we see that for each $g \in G$ the subgroup $N_{\psi,g}$ arises from the abelian map $\varphi_g \psi_x \varphi_g^{-1}$, which behaves as follows

$$\varphi_g \psi_x \varphi_g^{-1}(t) = \begin{cases} e & \text{if } t \in A_n \\ gxg^{-1} & \text{if } t \notin A_n \end{cases}$$

Thus $\varphi_g \psi_x \varphi_g^{-1} = \psi_{gxg^{-1}}$, and so the ρ-conjugate subgroups correspond to conjugacy classes of elements of order at most 2 in G. In particular, the subgroups arising from transpositions are mutually ρ-conjugate.

6.3. **Induced Hopf-Galois structures.** The method of *induced* Hopf-Galois structures is due to Crespo, Rio, and Vela [11]: if T is a subgroup of G having a normal complement S in G then, given a Hopf-Galois structure on L/L^T and a Hopf-Galois structure on L^T/K, we can induce a Hopf-Galois structure on L/K. Note that T need not be a normal subgroup of G, and so the extension L^T/K need not be a Galois extension. In order to study Hopf-Galois structures on this extension, we need the full strength of the Greither-Pareigis classification. In this context, it implies that the Hopf-Galois structures on L^T/K correspond bijectively with regular subgroups of $\mathrm{Perm}(G/T)$ (the permutation group of the left coset space) that are G-stable in the sense that they are normalized by the image of G under the left translation map $\lambda : G \to \mathrm{Perm}(G/T)$ defined by $\lambda(h)[xT] = hxT$ for all $h \in G$ and $xT \in G/T$.

Given a G-stable regular subgroup $A \subset \mathrm{Perm}(G/T)$ and a T-stable regular subgroup $B \subset \mathrm{Perm}(T)$, we use the fact that G is the semidirect product of S and T to identify A with a regular subgroup of $\mathrm{Perm}(S)$, and then to define a map $\eta : A \times B \to \mathrm{Perm}(G)$ by

$$\eta(a, b)[st] = a[s]b[t] \text{ for all } s \in S \text{ and } t \in T.$$

It is easy to see that η is an embedding whose image N is a regular subgroup of $\mathrm{Perm}(G)$ isomorphic to $A \times B$; [11, Theorem 3] shows that N is G-stable, and hence corresponds to a Hopf-Galois structure on L/K. We say that the subgroup N is *induced* from the subgroups A and B, and that the Hopf-Galois structure on L/K corresponding to N is induced from those corresponding to A on L^T/K and B on L/L^T.

Now let $g \in G$ and let $\varphi = \varphi_g$ be the inner automorphism corresponding to g. Since S is normal in G we have $\varphi(S) = S$, and it is easily shown that G is the semidirect product of S and $\varphi(T)$. We shall show that the Hopf-Galois structure corresponding to N_g is induced from certain Hopf-Galois structures on $L^{\varphi(T)}/K$ and $L/L^{\varphi(T)}$.

Lemma 6.6. Let $g \in G$ and $\varphi = \varphi_g$. Then:

i) $\varphi A \varphi^{-1}$ identifies naturally with a G-stable regular subgroup of $\mathrm{Perm}(G/\varphi(T))$;
ii) $\varphi B \varphi^{-1}$ identifies naturally with a $\varphi(T)$-stable regular subgroup of $\mathrm{Perm}(\varphi(T))$.

Proof. To show (i), let $a \in A$ and $s\varphi(T) \in G/\varphi(T)$ (with $s \in S$). Then

$$\varphi a \varphi^{-1}[s\varphi(T)] = \varphi a[\varphi^{-1}(s)T] = s'\varphi(T)$$

for some element $s' \in S$. Hence $\varphi A \varphi^{-1}$ permutes $G/\varphi(T)$, and this action is regular because A acts regularly on G/T. To show G-stability, let $h \in G$ and consider

$$\begin{aligned} \lambda(h)\varphi a \varphi^{-1}\lambda(h^{-1})[s\varphi(T)] &= h\varphi a[\varphi^{-1}(h^{-1})\varphi^{-1}(s)T] \\ &= \varphi(\varphi^{-1}(h)a[\varphi^{-1}(h^{-1})\varphi^{-1}(s)T] \\ &= \varphi(\varphi^{-1}(h)a\varphi^{-1}(h^{-1})\varphi^{-1}[s\varphi(T)] \\ &= \varphi a'\varphi^{-1}[s\varphi(T)] \end{aligned}$$

for some $a' \in A$, since A is G-stable. Hence $\varphi A \varphi^{-1}$ is G-stable. The proof of (ii) is similar. □

Note that if $g \in T$ then the regular subgroup $\varphi B \varphi^{-1}$ of $\mathrm{Perm}(T)$ is ρ-conjugate to B.

Proposition 6.7. For A, B, N, and g as above, the subgroup $N_g \leq \mathrm{Perm}(G)$ is induced from $\varphi A \varphi^{-1} \leq \mathrm{Perm}(G/\varphi(T))$ and $\varphi B \varphi^{-1} \leq \mathrm{Perm}(\varphi(T))$.

Proof. Let $h \in G$, and write $h = s\varphi(t)$ with $s \in S$ and $t \in T$. Now let $\eta = \eta(a, b) \in N$ and consider

$$\begin{aligned} \varphi\eta\varphi^{-1}[s\varphi(t)] &= \varphi\eta[\varphi^{-1}(s)t] \\ &= \varphi(a[\varphi^{-1}(s)]b[t]) \text{ (note that } \varphi^{-1}(s) \in S) \\ &= (\varphi a[\varphi^{-1}(s)])(\varphi b[t]) \\ &= (\varphi a[\varphi^{-1}(s)])(\varphi b[\varphi^{-1}(\varphi(t))]) \\ &= \eta(\varphi a\varphi^{-1}, \varphi b\varphi^{-1})[s\varphi(t)]. \end{aligned}$$

Hence $N_g \leq \mathrm{Perm}(G)$ is induced from $\varphi A \varphi^{-1} \leq \mathrm{Perm}(G/\varphi(T))$ and $\varphi B \varphi^{-1} \leq \mathrm{Perm}(\varphi(T))$. □

We remark that the argument of Proposition 6.7 remains valid if φ is any automorphism of G that preserves S.

Example 6.8. Let p, q be odd primes with $p \equiv 1 \pmod{q}$ and let L/K be a Galois extension of fields whose Galois group G is isomorphic to the metacyclic group of order pq

$$G = \langle s, t \mid s^p = t^q = e,\ tst^{-1} = s^d \rangle,$$

as in Example 2.3. Let $T = \langle t \rangle$ and $S = \langle s \rangle$. Then the conjugates of T are precisely the subgroups $T_i = s^i T s^{-i}$, and S is a normal complement to each of these subgroups in G. For each i the extensions L/L^{T_i} and L^{T_i}/K have prime degree and each admits a unique Hopf-Galois structure (note that each L^{T_i}/K is non-normal). In each case, we can induce a Hopf-Galois structure on L/K from

these, and by Proposition 6.7 we obtain a family of p mutually ρ-conjugate Hopf-Galois structures on L/K. Referring to Example 2.3 we see that these are all of the Hopf-Galois structures of cyclic type admitted by L/K.

References

[1] D. Bachiller. Counterexample to a conjecture about braces. *J. Algebra*, 453:160–176, 2016.

[2] N. P. Byott. Uniqueness of Hopf Galois structure of separable field extensions. *Comm. Algebra*, 24:3217–3228, 3705, 1996.

[3] N. P. Byott. Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications. *J. Théor. Nombres Bordeaux*, 9:201–219, 1997.

[4] N. P. Byott. Hopf-Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra*, 188(1-3,2.2):45–57, 2004.

[5] N. P. Byott and L. N. Childs. Fixed point free pairs of homomorphisms and Hopf Galois structures. *New York J. Math.*, 18:707–731, 2012.

[6] L. N. Childs. *Taming Wild Extensions: Hopf algebras and local Galois module theory*, volume 80 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2000.

[7] L. N. Childs. Fixed-point free endomorphisms and Hopf Galois structures. *Proc. Amer. Math. Soc.*, 141:1255–1265, 2013.

[8] L. N. Childs. On the Galois correspondence for Hopf Galois structures. *New York J. Math.*, 23:1–10, 2017.

[9] L. N. Childs, C. Greither, K. P. Keating, A. Koch, T. Kohl, P. J. Truman, and R. Underwood. *Hopf algebras and Galois module theory*, volume 260 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2021.

[10] T. Crespo, A. Rio, and M. Vela. The Hopf Galois property in subfield lattices. *Comm. Algebra*, 44:336–353, 2016.

[11] T. Crespo, A. Rio, and M. Vela. On the Galois correspondence theorem in separable Hopf Galois theory. *Publ. Mat. (Barcelona)*, 60(1):221–234, 2016.

[12] C. Greither and B. Pareigis. Hopf Galois theory for separable field extensions. *J. Algebra*, 106:239–258, 1987.

[13] L. Guarneri and L. Vendramin. Skew braces and the Yang-Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.

[14] A. Koch. Abelian maps, bi-skew braces, and opposite pairs of Hopf-Galois structures. *Proc. Amer. Math. Soc.*, 8(16):189–203, 2021.

[15] A. Koch, T. Kohl, P. J. Truman, and R. Underwood. Isomorphism problems for Hopf-Galois structures on separable field extensions. *J. Pure Appl. Algebra*, 223:2230–2245, 2019.

[16] A. Koch, L. Stordy, and P. J. Truman. Abelian fixed point free endomorphisms and the yang-baxter equation. *New York J. Math.*, 26:1473–1492, 2020.

[17] A. Koch and P. J. Truman. Opposite skew left braces and applications. *J. Algebra*, 546:218–235, 2020.

[18] A. Koch and P. J. Truman. Skew left braces and isomorphism problems for Hopf-Galois structures on Galois extensions. *J. Algebra Appl.*, 2022.

[19] T. Kohl. Enumerating dihedral Hopf-Galois structures acting on dihedral extensions. *J. Algebra*, 542:93–115, 2020.

[20] K. Nejabati Zenouz. Skew braces and Hopf-Galois structures of Heisenberg type. *J. Algebra*, 524:187–225, 2019.

[21] A. Smoktunowicz and L. Vendramin. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra*, 2(1):47–86, 2018.

[22] L. Stefanello and S. Trappeniers. On the connection between Hopf-Galois structures and skew braces. arXiv:2206.07610 [math.NT].

[23] S. Taylor and P. J. Truman. The structure of Hopf algebras giving Hopf-Galois structures on quaternionic extensions. *New York J. Math.* 25:219–237, 2019.

[24] P. J. Truman. Canonical nonclassical Hopf–Galois module structure of nonabelian Galois extensions. *Comm. Algebra*, 44(3):1119–1130, 2016.

[25] P. J. Truman. Commuting Hopf-Galois structures on a separable extension. *Comm. Algebra*, 46(4):1420–1427, 2018.

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

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