New York Journal of Mathematics

New York J. Math. **31** (2025) 238–258.

Galois extensions and Hopf-Galois structures

Timothy Kohl and Robert Underwood

Abstract. Let K be a field and let N be a finitely generated group with finite automorphism group F. As shown by Haggenmüller and Pareigis, there is a bijection

$$\Theta : \mathcal{G}al(K,F) \to \mathcal{F}orm(K[N])$$

from the collection of F-Galois extensions of K to the collection of forms of the Hopf algebra $K[N]$. In the case that K is a finite field extension of $\mathbb{Q}$ and H is the Hopf algebra of a Hopf-Galois structure on a Galois extension E/K, we construct the preimage of H under Θ. We give criteria to determine the Hopf algebra isomorphism classes of the Hopf algebras attached to the Hopf-Galois structures on E/K. Examples are included throughout the paper.

Contents

1. Introduction

Hopf-Galois theory, specifically, the study of Hopf-Galois structures on Galois extensions of number fields, was introduced by C. Greither and B. Pareigis in 1987 as a way to generalize classical Galois theory [7]. In subsequent years, Hopf-Galois structures have been studied extensively by numerous authors. In this paper we consider Hopf-Galois theory in the broader context of the Galois extensions of S. U. Chase, D. K. Harrison, and A. Rosenberg [5]. A fundamental result is the bijection

$$\Theta : \mathcal{G}al(K,F) \to \mathcal{F}orm(K[N])$$

of R. Haggenmüller and B. Pareigis [9, Theorem 5], which gives a 1-1 correspondence between F-Galois extensions of K and forms of the K-Hopf algebra

Received August 10, 2023.
2010 *Mathematics Subject Classification.* 16T05.
Key words and phrases. Galois extension, Hopf algebra form, Hopf-Galois structure.

ISSN 1076-9803/2025

$K[N]$, where N is a finitely generated group with finite automorphism group $F = \mathrm{Aut}(N)$. For an F-Galois extension A of K, the map Θ is given explicitly as the fixed ring

$$\Theta(A) = (A[N])^F,$$

where F acts on A through the Galois action and on N as automorphisms. The fixed ring $(A[N])^F$ is an A-form of $K[N]$ and so belongs to $\mathcal{F}orm(K[N])$. The map Θ has been used to classify all of the Hopf algebra forms of the group ring Hopf algebra $K[N]$ in the cases when $N = \mathbb{Z}, C_3, C_4$, or C_6 [9, Theorem 6].

There is a natural connection between Θ and Hopf-Galois theory. Let K be a finite field extension of $\mathbb{Q}$. Let E/K be a Galois extension of fields with group G and let $(H, \cdot)$ be a Hopf-Galois structure of type N on E/K. Using (Morita-theoretic) Galois descent [2, (2.12)], the K-Hopf algebra H is given as the fixed ring $(E[N])^G$, where G acts on E as the Galois group and on N as automorphisms given by conjugation. Now, H is an E-form of $K[N]$ and the K-Hopf algebra isomorphism class of H is an element of $\mathcal{F}orm(K[N])$. Thus, there exists an F-Galois extension B of K, $F = \mathrm{Aut}(N)$, for which

$$\Theta(B) = (B[N])^F = H.$$

A main goal of this paper is to give an explicit description of the preimage B (see Section 4).

Using the preimage, in Section 5 we give criteria for determining the Hopf algebra isomorphism classes of the Hopf algebras attached to Hopf-Galois structures. Essentially, let $(H, \cdot)$ and $(H', \cdot')$ be Hopf Galois structures on E/K of type N and suppose that $\Theta(A) = H$ and $\Theta(A') = H'$ for some F-Galois extensions A, A', with $F = \mathrm{Aut}(N)$. Then $H \cong H'$ as Hopf algebras if and only if $A \cong A'$ as F-Galois extensions of K. In this manner, we extend [13, Theorem 2.2].

We apply our results to work of S. Taylor and P. J. Truman [15]. In that paper, the authors consider the case where E/K is a quaternionic extension and the Hopf-Galois structures are of type D_4, the dihedral group of order 8. An extensive discussion of this case is also given in [4, Chapter 9, Section 9.2.3].

As shown in [15, Lemma 2.5], there are 6 distinct Hopf-Galois structures on E/K of type D_4, which yield 6 pairwise non-isomorphic K-Hopf algebras. We compute all 6 preimages under Θ of these Hopf algebras; the preimages are necessarily pairwise non-isomorphic as F-Galois extensions of K; here, $F = \mathrm{Aut}(D_4) \cong D_4$. We find that 3 of these non-isomorphic F-Galois extensions are isomorphic as K-algebras.

The authors are indebted to the referee whose thoughtful comments and suggestions have improved this paper.

2. Galois extensions

Let R be a commutative ring with unity.

The notion of a Galois extension of R is due to M. Auslander and O. Goldman [1]. Let A be a commutative R-algebra and let $\mathrm{End}_R(A)$ denote the R-algebra of R-linear maps $\phi : A \to A$. Let $\mathrm{Aut}_R(A)$ denote the group of R-algebra automorphisms of A and let F be a finite subgroup of $\mathrm{Aut}_R(A)$. The *fixed ring* of A under F is $A^F = \{x \in A \mid f(x) = x, \forall f \in F\}$.

Let $D(A, F)$ denote the collection of sums $\sum_{g\in F} a_g g$, $a_g \in A$. On $D(A, F)$ endow an R-module structure as follows: for $r \in R$, $\sum_{g\in F} a_g g$, $\sum_{g\in F} b_g g \in D(A, F)$, $r(\sum_{g\in F} a_g g) = \sum_{g\in F} r a_g g$, and

$$(\sum_{g\in F} a_g g) + (\sum_{g\in F} b_g g) = \sum_{g\in F} (a_g + b_g) g.$$

Define a multiplication on $D(A, F)$ as follows:

$$(\sum_{g\in F} a_g g)(\sum_{h\in F} b_h h) = \sum_{g,h\in F} a_g g(b_h) gh,$$

where gh is the group product in F. The resulting R-algebra $D(A, F)$ is the *crossed product algebra* of A by F.

Let

$$j : D(A, F) \to \mathrm{End}_R(A)$$

be the map defined as $j(\sum_{g\in F} a_g g)(t) = \sum_{g\in F} a_g g(t)$, for $a_g, t \in A$. Then j is a homomorphism of R-algebras.

The question of whether j is an isomorphism of R-algebras is a key part of the definition of a Galois extension.

Definition 2.1. Let R be a commutative ring with unity and let A be a commutative R-algebra. Let F be a finite subgroup of $\mathrm{Aut}_R(A)$ with $R = A^F$. Then A is an *F-Galois extension of R* if

(a) A is a finitely generated, projective R-module,
(b) the map $j : D(A, F) \to \mathrm{End}_R(A)$ is an isomorphism of R-algebras.

Remark 2.2. There are a number of other ways to define an F-Galois extension of R that are equivalent to Definition 2.1, see [5, Definition 1.4, Theorem 1.3]. For instance, from [5, Theorem 1.3], A is an F-Galois extension of R if F is a finite subgroup of $\mathrm{Aut}_R(A)$, $R = A^F$, and A is a separable R-algebra in which the action of F on A is *strongly distinct*, that is, for distinct elements f, g in F, and any idempotent e of A, there exists an element $x \in A$ for which $f(x)e \neq g(x)e$.

The notion of F-Galois extension generalizes the usual definition of a Galois extension of fields.

Example 2.3. Let $R = K$ be a finite field extension of $\mathbb{Q}$. Let L be a (classical) Galois extension of K with group G. Then $\mathrm{Aut}_K(L) = G$, $L^G = K$, and L is separable over K. Thus by [5, Theorem 1.3, (a)⇔(c)], the map

$$j : D(L, G) \to \mathrm{End}_K(L)$$

defined as $j(a_g g)(x) = a_g g(x)$, for $a_g, x \in L$, $g \in G$, is an isomorphism of K-algebras. Thus L is a G-Galois extension of K.

Let A, A' be F-Galois extensions of R. Then *A is isomorphic to A'* as F-Galois extensions of R if there exists an isomorphism of commutative R-algebras $\theta : A \to A'$ for which $\theta(g(x)) = g(\theta(x))$ for all $g \in F$, $x \in A$. We let $\mathcal{G}al(R,F)$ denote the set of isomorphism classes of F-Galois extensions of R.

Let $\mathrm{Map}(F,R)$ denote the R-algebra of maps $\phi : F \to R$. Then $\mathrm{Map}(F,R)$ is the *trivial F-Galois extension* of R with action defined as

$$g(\phi)(h) = \phi(g^{-1}h)$$

for $g, h \in F$, $\phi \in \mathrm{Map}(F,R)$.

For the remainder of this section, we assume that $R = K$ is a field. In this case the Galois extensions are completely determined.

Theorem 2.4. *Let K be a field, let F be a finite group and let A be an F-Galois extension of K. Then*

$$A = \underbrace{L \times L \times \cdots \times L}_{n}$$

where L is a U-Galois field extension of K for some subgroup U of F of index n. (L is a Galois extension of K with group U in the usual sense.)

Proof. See [14, Theorem 4.2]. □

Example 2.5. Let K be a field. Let C_4 denote the cyclic group of order 4. Then a C_4-Galois extension of K is of the form A, where A is a C_4-Galois field extension of K, or

$$A = L \times L,$$

where L is a C_2-Galois field extension of K, or

$$A = K \times K \times K \times K$$

(the trivial C_4-extension of K).

There is a converse to Theorem 2.4.

Theorem 2.6. *Let F be a finite group and suppose that L is a Galois field extension of K with group $U \leq F$, $n = [F : U]$. Then there exists an F-Galois extension of K of the form*

$$A = \underbrace{L \times L \times \cdots \times L}_{n}.$$

Proof. Let $T = \{g_1, g_2, \dots, g_n\}$ be a left transversal for U in F and let $A = \underbrace{L \times L \times \cdots \times L}_{n}$ with minimal orthogonal idempotents $e_1, e_2, \dots, e_n$. Let $\varsigma : F \to S_n$ be defined as $\varsigma(g)(i) = j$ if $gg_iU = g_jU$. Define an action of F on A on each component as

$$g(me_i) = (g^{-1}_{\varsigma(g)(i)}gg_i)(m)e_{\varsigma(g)(i)},$$

for $m \in L$, $1 \leq i \leq n$. Then A is an F-Galois extension of K. For details see [14, Theorem 4.2]. □

Remark 2.7. Theorem 2.4 and Theorem 2.6 appear in a paper of B. Pareigis as [14, Theorem 4.2]. However, Theorem 2.4 (at least when F is abelian) is probably due to H. Hasse [11]. Theorem 2.6 was probably also known to Hasse.

Given an F-Galois extension A, Theorem 2.4 shows that A determines a subgroup $U \leq F$ and a classical Galois field extension L/K with group U. By Theorem 2.6, the same subgroup U and the field L determine an F-Galois extension A'. We have $A \cong A'$ as F-Galois extensions of K, i.e., the F-Galois extension A arises from the field L by induction from the subgroup U up to the whole group F. In the case that F is abelian, the element A in the Harrison set $T(F, K)$ is the image of L under the map $T(i, K) : T(U, K) \to T(F, K)$, see [10, Theorem 7].

Example 2.8. Let $F = S_3$, with presentation

$$S_3 = \langle a, b \mid a^3 = 1, b^2 = 1, ba = a^2 b \rangle.$$

Let $U = \{1, a, a^2\} \cong C_3$. Let ζ denote a primitive 3rd root of unity, let $K = \mathbb{Q}(\zeta)$ and let $L = K(\omega)$, where $\omega = \sqrt[3]{2}$. Then L is a Galois field extension of K with group U; the U-Galois action is given as

$$1(\omega) = \omega, \quad a(\omega) = \zeta\omega, \quad a^2(\omega) = \zeta^2\omega.$$

Using Theorem 2.6, we compute the corresponding F-Galois extension of K. Let $T = \{g_1, g_2\}$ be a left transversal for U in F. We may take $g_1 = 1, g_2 = b$, so that the distinct left cosets are $\{U, bU\}$.

Let S_2 denote the group of permutations on the set $\{1, 2\}$. There is an action $\varsigma : F \to S_2$ given as

$$\varsigma(a^i)(1) = 1, \quad \varsigma(a^i)(2) = 2, \quad \varsigma(ba^i)(1) = 2, \quad \varsigma(ba^i)(2) = 1,$$

for $0 \leq i \leq 2$. Let

$$A = L \times L \cong Le_1 \oplus Le_2,$$

and write a typical element of A as

$$(c_0 + c_1\omega + c_2\omega^2)e_1 + (d_0 + d_1\omega + d_2\omega^2)e_2,$$

$c_0, c_1, c_2, d_0, d_1, d_2 \in K$. Now, A is an F-Galois extension of K with F-Galois action given as:

$$\begin{aligned} & a((c_0 + c_1\omega + c_2\omega^2)e_1 + (d_0 + d_1\omega + d_2\omega^2)e_2) \\ = \;& a(c_0 + c_1\omega + c_2\omega^2)e_1 + a^2(d_0 + d_1\omega + d_2\omega^2)e_2 \\ = \;& (c_0 + c_1\zeta\omega + c_2\zeta^2\omega^2)e_1 + (d_0 + d_1\zeta^2\omega + d_2\zeta\omega^2)e_2, \end{aligned}$$

$$\begin{aligned} & b((c_0 + c_1\omega + c_2\omega^2)e_1 + (d_0 + d_1\omega + d_2\omega^2)e_2) \\ = \;& 1(c_0 + c_1\omega + c_2\omega^2)e_2 + 1(d_0 + d_1\omega + d_2\omega^2)e_1 \\ = \;& (c_0 + c_1\omega + c_2\omega^2)e_2 + (d_0 + d_1\omega + d_2\omega^2)e_1. \end{aligned}$$

3. Galois extensions and forms of $K[N]$

Let K be a field and let B be a finite dimensional, commutative K-algebra. (Hence, B is faithfully flat over K.) Let C be an object over K in some category. A *B-form* of C is a K-object A in the same category for which

$$B \otimes_K A \cong B \otimes_K C$$

as B-objects in the category. A *form* of C is a K-object for which there exists a commutative, finite dimensional K-algebra B with

$$B \otimes_K A \cong B \otimes_K C$$

as B-objects in the category. The *trivial form* of C is C. Let $\mathcal{F}orm(B/K, C)$ denote the collection of the isomorphism classes of the B-forms of C and let $\mathcal{F}orm(C)$ denote the collection of the isomorphism classes of the forms of C.

Let $\mathbf{Aut}(C)$ denote the automorphism group functor of C on the category of finite dimensional commutative K-algebras, defined as follows: for a finite dimensional commutative K-algebra B, $\mathbf{Aut}(C)(B) = \mathrm{Aut}(B \otimes_K C)$, which denotes the group of automorphisms of $B \otimes_K C$ as a B-object. It is well-known that $\mathcal{F}orm(B/K, C)$ is classified by $\mathrm{H}^1(B/K, \mathbf{Aut}(C))$ [16, Section 17.6, Theorem]. If B/K is a Galois extension of fields with group G, we may pass to Galois descent to compute the B-forms of C as $\mathrm{H}^1(G, \mathbf{Aut}(C)(B))$ [16, Section 17.7, Theorem].

Let N be a finitely generated group with finite automorphism group $F = \mathrm{Aut}(N)$ and let $K[N]$ denote the group ring K-Hopf algebra.

Theorem 3.1 (Haggenmüller and Pareigis)**.** *There is a bijection*

$$\Theta : \mathcal{G}al(K, F) \to \mathcal{F}orm(K[N])$$

defined as follows: Let A be an F-Galois extension of K. Then $\Theta(A)$ is the fixed ring $(A[N])^F$, where the action of F on N is through the automorphism group F and the action of F on A is the Galois action. The image $\Theta(A) = (A[N])^F$ is an A-form of $K[N]$ with isomorphism $\psi : A \otimes_K (A[N])^F \to A[N]$, defined as $\psi(x \otimes h) = xh$, for $x \in A$, $h \in (A[N])^F$.

Details of the proof of Theorem 3.1 can be found in [9, Corollary 4, Theorem 5]. We remark that a key element of the proof of Theorem 3.1 is a result from R. Haggenmüller's dissertation [9, Proposition 3], [8, Proposition 2.14], which to our knowledge has not appeared in the literature. For the convenience of the reader, we include a proof here.

Let $\mathbf{G}(K[F])$ denote the grouplike functor of the K-Hopf algebra $K[F]$ from the category of commutative K-algebras to the category of groups, that is, for a commutative K-algebra B, $\mathbf{G}(K[F])(B)$ consists of the grouplike elements in the B-Hopf algebra $B \otimes_K K[F] \cong B[F]$.

Proposition 3.2 (Haggenmüller)**.** *Let B be a finite dimensional, commutative K-algebra. Then*

$$\mathbf{Aut}(\mathrm{Map}(F, K))(B) \cong \mathbf{G}(K[F])(B).$$

Proof. By [16, Section 6.2, Lemma],

$$B = B_1 \times B_2 \times \cdots \times B_m,$$

where each B_i, $1 \le i \le m$, is a K-algebra with no non-trivial idempotents. We have

$$\begin{aligned}\mathbf{Aut}(\mathrm{Map}(F,K))(B) &= \mathbf{Aut}(\mathrm{Map}(F,K))(\prod_{i=1}^{m} B_i)\\ &= \prod_{i=1}^{m} \mathbf{Aut}(\mathrm{Map}(F,K))(B_i) = \prod_{i=1}^{m} \mathrm{Aut}(\mathrm{Map}(F,B_i)).\end{aligned}$$

Fix an integer i, $1 \le i \le m$, and let $\sigma_i \in \mathrm{Aut}(\mathrm{Map}(F,B_i))$. Then σ_i is an isomorphism of B_i-algebras that respects the F-action on $\mathrm{Map}(F,B_i)$. A B_i-basis for $\mathrm{Map}(F,B_i)$ is $X = \{e_g\}_{g\in F}$, with $e_g(h) = \delta_{g,h}$, $h \in F$.

For $e_g \in X$, $\sigma_i(e_g) = e_h$ for some $e_h \in X$. Thus σ_i restricts to a 1-1 correspondence $\sigma_i : X \to X$, i.e., $\sigma_i \in \mathrm{Perm}(X)$. There is a 1-1 correspondence $F \to X$, given as $g \mapsto e_g$, and thus $\mathrm{Perm}(X) \cong \mathrm{Perm}(F)$, as groups. Thus we may view σ_i as an element of $\mathrm{Perm}(F)$. For $g \in F$, we have

$$\sigma_i(e_g) = e_h \;\Leftrightarrow\; \sigma_i(g) = h.$$

The F-action on X can be translated to F: for $g \in F$, $e_h \in X$,

$$g(e_h) = e_{gh} \;\Leftrightarrow\; g(h) = gh.$$

This F-action on F is actually the action of F on F through the left regular representation $\lambda : F \to \mathrm{Perm}(F)$, defined as $\lambda_g(h) = gh$.

Since σ_i respects the F-action on X, it also respects the F-action on F. For $g \in F$, $h \in F$,

$$\sigma_i(g(h)) = g(\sigma_i(h)).$$

Thus,

$$(\sigma_i \circ \lambda_g)(h) = (\lambda_g \circ \sigma_i)(h),$$

and so, $\sigma_i \in \mathrm{Cent}_{\mathrm{Perm}(F)}(\lambda(F))$. By [17, Chapter 1, Section 4],

$$\rho(F) = \mathrm{Cent}_{\mathrm{Perm}(F)}(\lambda(F)),$$

where $\rho : F \to \mathrm{Perm}(F)$, $\rho_g(h) = hg^{-1}$, is the right regular representation. Thus $\sigma_i \in \rho(F)$.

Certainly, any element of $\rho(F)$ defines an element of $\mathrm{Aut}(\mathrm{Map}(F,B_i))$. Thus,

$$F \cong \rho(F) = \mathrm{Aut}(\mathrm{Map}(F,B_i)).$$

It follows that $\mathbf{Aut}(\mathrm{Map}(F,K))(B) \cong \underbrace{F \times F \times \cdots \times F}_{m}$. Moreover,

$$\mathbf{G}(K[F])(B) = \mathbf{G}(K[F])(\prod_{i=1}^{m} B_i) = \prod_{i=1}^{m} \mathbf{G}(K[F])(B_i) = \underbrace{F \times F \times \cdots \times F}_{m},$$

since each B_i contains no non-trivial idempotents. The result follows.

□

Example 3.3. Recall Example 2.8 in which we constructed an F-Galois extension

$$A = Le_1 \oplus Le_2,$$

with

$$F = S_3 = \langle a, b \mid a^3 = 1, b^2 = 1, ba = a^2 b \rangle,$$

$K = \mathbb{Q}(\zeta)$, ζ a primitive 3rd root of unity, and $L = K(\omega)$, where $\omega = \sqrt[3]{2}$; the Galois group of L/K is $U = \{1, a, a^2\} \leq F$.

Now, with $N = C_2 \times C_2 = \{\epsilon, \sigma, \tau, \sigma\tau\}$, we have $S_3 = F = \mathrm{Aut}(N)$; the automorphisms in S_3 are generated by the premutations in cycle notation: $a = (\sigma, \tau, \sigma\tau), b = (\tau, \sigma\tau)$.

We compute the image of A under the map $\Theta : \mathcal{G}al(K, F) \to \mathcal{F}orm(K[N])$, i.e., the fixed ring $\Theta(A) = H = (A[C_2 \times C_2])^F$, which is an A-form of $K[C_2 \times C_2]$. By direct computation,

$$\Theta(A) = H = (A[C_2 \times C_2])^F = \bigoplus_{i=1}^{4} K h_i,$$

where

$$h_1 = \epsilon, \quad h_2 = \sigma + \tau + \sigma\tau,$$
$$h_3 = (\omega e_1 + \omega e_2)\sigma + (\zeta\omega e_1 + \zeta^2\omega e_2)\tau + (\zeta^2\omega e_1 + \zeta\omega e_2)\sigma\tau$$
$$h_4 = (\omega^2 e_1 + \omega^2 e_2)\sigma + (\zeta^2\omega^2 e_1 + \zeta\omega^2 e_2)\tau + (\zeta\omega^2 e_1 + \zeta^2\omega^2 e_2)\sigma\tau.$$

Since $h_2^2 = 2h_2 + 3$, the K-subalgebra $K \oplus Kh_2$ of H is isomorphic to $K \times K$ with idempotents $f_1 = \frac{1}{4}(3 - h_2)$, $f_2 = \frac{1}{4}(1 + h_2)$ corresponding to the first and second copies of K, respectively.

Now, f_2 annihilates h_3, h_4. Moreover, $h_3^3 f_1 = 16 f_1$, thus h_1 is a root of the polynomial $x^3 - 16$ over K. Thus H is isomorphic, as an algebra, to a product

$$\Theta(A) = H = (A[C_2 \times C_2])^F \cong K \times K \times K(\omega) = K \times K \times L.$$

The Hopf algebra structure of H is given as: $\Delta(h_1) = h_1 \otimes h_1$,

$$\Delta(h_2) = \frac{1}{6} h_3 \otimes h_4 + \frac{1}{6} h_4 \otimes h_3 + \frac{1}{3} h_2 \otimes h_2,$$

$$\Delta(h_3) = \frac{1}{6} h_4 \otimes h_4 + \frac{1}{3} h_2 \otimes h_3 + \frac{1}{3} h_3 \otimes h_2,$$

$$\Delta(h_4) = \frac{1}{3} h_3 \otimes h_3 + \frac{1}{3} h_2 \otimes h_4 + \frac{1}{3} h_4 \otimes h_2,$$

$$\varepsilon(h_1) = 1,\ \varepsilon(h_2) = 3,\ \varepsilon(h_3) = \varepsilon(h_4) = 0.$$

The coinverse map $S : H \to H$ is induced from the coinverse map on $A[C_2 \times C_2]$.

The K-Hopf algebra H is a form of the group ring Hopf algebra $K[C_2 \times C_2]$.

In the next section we consider the inverse map

$$\Theta^{-1} : \mathcal{F}orm(K[N]) \to \mathcal{G}al(K,F)$$

in the case that the forms are given as Hopf algebras of Hopf-Galois structures on a (classical) Galois extension of K.

4. Connection to Hopf-Galois theory

For the remainder of this paper, we take K to be a finite field extension of $\mathbb{Q}$.

4.1. Review of Greither-Pareigis theory. Let E/K be a Galois extension with group G. Let H be a finite dimensional, cocommutative K-Hopf algebra with comultiplication $\Delta : H \to H \otimes_R H$, counit $\varepsilon : H \to K$ and coinverse $S : H \to H$. Suppose there is a K-linear action $\cdot$ of H on E that satisfies

$$h \cdot (xy) = \sum_{(h)} (h_{(1)} \cdot x)(h_{(2)} \cdot y), \quad h \cdot 1 = \varepsilon(h)1$$

for all $h \in H$, $x, y \in E$, where $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$ is Sweedler notation. Suppose also that the K-linear map

$$j : E \otimes_K H \to \mathrm{End}_K(E),$$

given as $j(x \otimes h)(y) = x(h \cdot y)$, is an isomorphism of vector spaces over K. Then H together with this action, denoted as $(H, \cdot)$, provides a *Hopf-Galois structure* on E/K. Two Hopf-Galois structures $(H, \cdot)$, $(H', \cdot')$ on E/K are *isomorphic* if there is a Hopf algebra isomorphism $f : H \to H'$ for which $h \cdot x = f(h) \cdot' x$ for all $x \in E$, $h \in H$ (see [6, Introduction]).

C. Greither and B. Pareigis [7] have given a complete classification of Hopf-Galois structures up to isomorphism. Let $\lambda : G \to \mathrm{Perm}(G)$ denote the left regular representation. A subgroup $N \leq \mathrm{Perm}(G)$ is *regular* if it is semiregular (i.e., only the identity acts with fixed points) and transitive. A subgroup $N \leq \mathrm{Perm}(G)$ is *normalized* by $\lambda(G) \leq \mathrm{Perm}(G)$ if $\lambda(G)$ is contained in the normalizer of N in $\mathrm{Perm}(G)$.

Theorem 4.1 (Greither and Pareigis)**.** *Let E/K be a Galois extension with group G. There is a* 1-1 *correspondence between isomorphism classes of Hopf Galois structures on E/K and regular subgroups of* $\mathrm{Perm}(G)$ *that are normalized by* $\lambda(G)$.

One direction of the correspondence in Theorem 4.1 is given as follows. Let N be a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$. Then G acts on the group algebra $E[N]$ through the Galois action on E and conjugation by $\lambda(G)$ on N, i.e.,

$$g(x\eta) = g(x)(\lambda(g)\eta\lambda(g^{-1})), g \in G,\ x \in E,\ \eta \in N.$$

We denote the conjugation action of $\lambda(g) \in \lambda(G)$ on $\eta \in N$ by ${}^g\eta$. Let H denote the fixed ring

$$(E[N])^G = \{x \in E[N] \mid g(x) = x, \forall g \in G\}.$$

Then H is an r-dimensional K-Hopf algebra, $r = [E : K]$, and E/K admits the Hopf Galois structure $(H, \cdot)$ [2, (6.8) Theorem, pp. 52-54]. The action of H on E/K is given as

$$\Big(\sum_{\eta\in N} r_\eta \eta\Big)\cdot x = \sum_{\eta\in N} r_\eta \eta^{-1}[1_G](x),$$

see [3, Proposition 1]. By Morita theory [2, (2.13) Lemma], the isomorphism

$$E \otimes_K H \cong E \otimes_K K[N] \cong E[N],$$

$x \otimes h \mapsto xh$ is an isomorphism of E-Hopf algebras. Thus H is an E-form of $K[N]$.

If N is isomorphic to the abstract group N', then the Hopf-Galois structure $(H, \cdot)$ on E/K is of *type* N'.

4.2. The preimage of a Hopf-Galois structure. If $(H, \cdot)$ is a Hopf-Galois structure on E/K of type N, then the Hopf algebra H is a Hopf form of $K[N]$. Thus by Theorem 3.1, with $F = \mathrm{Aut}(N)$, there is an F-Galois extension B of K with

$$\Theta(B) = (B[N])^F = H. \tag{1}$$

We have $B \otimes_K H \cong B[N]$ as B-Hopf algebras. Our goal is to give an explicit description of B.

By Theorem 2.4

$$B = \underbrace{L \times L \times \cdots \times L}_{m},$$

where L is a V-Galois field extension of K for some subgroup V of F of index $[F : V] = m$. By Remark 2.7, B arises from the pair V, L via Theorem 2.6.

Lemma 4.2. *There is an isomorphism of L-Hopf algebras*

$$L \otimes_K H \to L[N].$$

Proof. Let $\{h_1, h_2, \dots, h_r\}$ be a K-basis for H and let $\eta \in N$. Then there exist unique $b_1, b_2, \dots, b_r$ in B with $\eta = \sum_{i=1}^r b_i \otimes h_i$. Moreover, since H is an E-form of $K[N]$, there exist unique $x_i, x_2, \dots, x_r$ in E with $\eta = \sum_{i=1}^r x_i \otimes h_i$.

Let E' be any field extension of K containing both L and E and let $C = \underbrace{E' \times E' \times \cdots \times E'}_{m}$. Then

$$C \otimes_K H \cong C[N],$$

and $\sum_{i=1}^r (b_i - x_i) \otimes h_i = 0$ in $C \otimes_K H$. Thus $b_i = x_i$, $1 \le i \le r$, and so, $b_i \in E$, thus $b_i \in L$, for $1 \le i \le r$. Thus, $L \otimes_K H \cong L[N]$ as L-Hopf algebras.

□

Since E/K is Galois with group G, we may use Galois descent to describe $H \in \mathcal{F}orm(K[N])$. The E-form H of $K[N]$ corresponds to a 1-cocycle (homomorphism) $\varrho : G \to F$ in

$$\mathrm{H}^1(G, \mathbf{Aut}(K[N])(E)) = \mathrm{H}^1(G, F).$$

By [7, p. 249, Proof of 3.1, a $\Rightarrow$ b] or [2, (6.7) Proposition], $\varrho(g)$ is given as conjugation by elements of $\lambda(G)$, that is, for $g \in G, \eta \in N$,

$$\varrho(g)(\eta) = {}^{g}\eta = \lambda(g)\eta\lambda(g^{-1}).$$

The kernel of ϱ is a normal subgroup of G defined as

$$G_0 = \{g \in G \mid {}^{g}\eta = \eta, \forall \eta \in N\}.$$

The quotient group G/G_0 is isomorphic to a subgroup U of $F = \mathrm{Aut}(N)$.

Let $E_0 = E^{G_0}$. Then E_0 is Galois extension of K with group U. By Theorem 2.6, there exist an F-Galois extension of K of the form

$$A = \underbrace{E_0 \times E_0 \times \cdots \times E_0}_{n},$$

where $[F : U] = n$.

Theorem 4.3. *Let E/K be a Galois extension with group G and let $(H, \cdot)$ be a Hopf-Galois structure on E/K of type N. Let B be the preimage of H under Θ as in (1). Then $B = A$, that is,*

$$\Theta(A) = (A[N])^F = H.$$

Proof. By [7, Corollary 3.2], E_0 is the smallest field extension of K, contained in E with

$$E_0 \otimes H \cong E_0[N].$$

Thus H is an E_0-form of $K[N]$.

By [16, Section 17.6, Theorem], $\mathcal{F}orm(E_0/K, \mathrm{Map}(F, K))$ corresponds to

$$\mathrm{H}^1(E_0/K, \mathbf{Aut}(\mathrm{Map}(F, K))).$$

Thus by Proposition 3.2, $\mathcal{F}orm(E_0/K, \mathrm{Map}(F, K))$ corresponds to

$$\mathrm{H}^1(E_0/K, \mathbf{G}(K[F])).$$

Now, by [9, Theorem 2], $\mathrm{H}^1(E_0/K, \mathbf{G}(K[F]))$ can be identified with

$$\mathrm{H}^1(E_0/K, \mathbf{Aut}(K[N])).$$

Consequently, there is a bijection

$$\hat{\Theta} : \mathcal{F}orm(E_0/K, \mathrm{Map}(F, K)) \to \mathcal{F}orm(E_0/K, K[N]).$$

Now, $\mathcal{F}orm(\mathrm{Map}(F, K)) = \mathcal{G}al(K, F)$ by [9, Corollary 4].

Thus $\mathcal{F}orm(E_0/K, \mathrm{Map}(F, K))$, a subset of $\mathcal{F}orm(\mathrm{Map}(F, K))$, can be viewed as a subset of $\mathcal{G}al(K, F)$. Hence, the preimage of $H \in \mathcal{F}orm(E_0/K, K[N])$ under $\hat{\Theta}$ is precisely $\Theta^{-1}(H) = B$ (for this use the proof of [9, Corollary 4]).

It follows that B is an E_0-form of $\mathrm{Map}(F, K)$ and so,

$$E_0 \otimes_K (\underbrace{L \times L \times \cdots \times L}_{m}) \cong E_0 \otimes_K \mathrm{Map}(F, K) \cong \mathrm{Map}(F, E_0).$$

Write $L \cong K[x]/(f(x))$ for some minimal polynomial $f(x) \in K[x]$. Then

$$\begin{aligned} & E_0 \otimes_K (\underbrace{L \times L \times \cdots \times L}_{m}) \\ \cong\ & E_0 \otimes_K (\underbrace{K[x]/(f(x)) \times K[x]/(f(x)) \times \cdots \times K[x]/(f(x))}_{m}) \\ \cong\ & \underbrace{E_0[x]/(f(x)) \times E_0[x]/(f(x)) \times \cdots \times E_0[x]/(f(x)))}_{m} \\ \cong\ & \mathrm{Map}(F, E_0) \\ \cong\ & \underbrace{E_0 \times E_0 \times \cdots \times E_0}_{|F|}. \end{aligned}$$

Thus, all of the zeros of $f(x)$ must lie in E_0, hence $L \subseteq E_0$. Now by Lemma 4.2, $E_0 = L$ and $U = V$ since E_0 is minimal. Hence $\Theta(A) = H$, where $A = \underbrace{E_0 \times E_0 \times \cdots \times E_0}_{n}$, with $[F : U] = n$, $U \cong G/G_0$. □

Example 4.4. Let E/K be a Galois extension with group G. Let $\rho : G \to \mathrm{Perm}(G)$ denote the right regular representation. Then $N = \rho(G)$ is a regular subgroup of Perm(G) normalized by $\lambda(G)$; $\rho(G)$ corresponds to the classical Hopf-Galois structure on E/K with Hopf algebra $K[G]$ [2, (6.10) Proposition]. Since $\lambda(G)$ commutes with $\rho(G)$, we have

$$G_0 = \{g \in G \mid {}^g\eta = \eta, \forall \eta \in \rho(G)\} = G.$$

Thus $U \cong G/G_0 = 1$ and $E_0 = E^{G_0} = K$. Let $F = \mathrm{Aut}(\rho(G))$. Then $n = [F : U] = [F : 1] = |F|$. By Theorem 4.3, we have $\Theta(A) = K[\rho(G)]$, where $A = \underbrace{K \times K \times \cdots \times K}_{n}$. Of course, A is the trivial F-Galois extension of K, Map(F, K).

If $n = [F : U] = 1$, then $A = E_0$ and A is a F-Galois field extension of K.

Example 4.5. Let E/K be a Galois extension with group G where G is a non-abelian complete group (i.e., G has trivial center and $G \cong \mathrm{Aut}(G)$). For instance, $G = S_n$, for $n \neq 2, 6$, is a non-abelian complete group.

The subgroup $N = \lambda(G)$ is a regular subgroup of Perm(G) normalized by itself and corresponds to the canonical non-classical Hopf-Galois structure with Hopf algebra H_λ. In this case G_0 is trivial since the center of $\lambda(G)$ is trivial, and so $E^{G_0} = E_0 = E$ and $G/G_0 \cong G \cong \mathrm{Aut}(N) = F$. Thus

$$[F : U] = |\mathrm{Aut}(N)|/[G : G_0] = |\mathrm{Aut}(N)|/|G| = 1.$$

By Theorem 4.3, $\Theta(E_0) = H_\lambda$.

We can have $n = 1$ with G_0 non-trivial.

Example 4.6. In the table below we list every group G of order ≤ 42 in which there exists a Galois extension of fields E/K with group G with at least one Hopf-Galois structure H on E/K of type M with $n = [F : U] = 1$. Consequently, for each case indicated by the table, $\Theta(E_0) = H$.

G	M	$\lvert G_0 \rvert$	$[G : G_0]$
C_2	C_2	2	1
$C_2 \times C_2$	C_4	2	2
S_3	C_6	3	2
S_3	S_3	1	6
D_4	$C_4 \times C_2$	1	8
$C_4 \times C_2$	C_8	2	4
D_6	C_{12}	3	4
D_6	$C_3 \rtimes C_4$	1	12
$C_8 \rtimes C_2$	C_{16}	2	8
$C_8 \times C_2$	C_{16}	2	8
$C_5 \rtimes C_4$	$C_5 \rtimes C_4$	1	20
$C_2 \times C_2 \times S_3$	$C_4 \times S_3$	1	24
S_4	$C_2 \times A_4$	1	24
S_4	S_4	1	24
$C_7 \rtimes C_6$	$C_2 \times (C_7 \rtimes C_3)$	1	42
$C_7 \rtimes C_6$	$C_7 \rtimes C_6$	1	42

Example 4.7. Let E/K be a Galois extension of fields with quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. S. Taylor and P. Truman [15] have enumerated the Hopf-Galois structures on E/K of each possible type [15, Table 1]. There are 6 Hopf-Galois structures on E/K of type D_4, corresponding to 6 regular subgroups that are normalized by $\lambda(Q_8) = \langle \lambda(i), \lambda(j) \rangle$:

$$D_{i,\lambda} = \langle \lambda(i), \lambda(j)\rho(i) \rangle, \quad D_{j,\lambda} = \langle \lambda(j), \lambda(i)\rho(j) \rangle, \quad D_{k,\lambda} = \langle \lambda(k), \lambda(i)\rho(k) \rangle,$$

$$D_{i,\rho} = \langle \rho(i), \lambda(i)\rho(j) \rangle, \quad D_{j,\rho} = \langle \rho(j), \lambda(j)\rho(i) \rangle, \quad D_{k,\rho} = \langle \rho(k), \lambda(k)\rho(i) \rangle$$

[15, Lemma 2.5].

We consider the case $N = D_{i,\lambda}$. Let $H_{i,\lambda}$ denote the K-Hopf algebra attached to the Hopf-Galois structure on E/K that corresponds to $D_{i,\lambda}$. Let $F = \mathrm{Aut}(D_{i,\lambda})$. We compute the F-Galois extension A of K for which $\Theta(A) = H_{i,\lambda}$ and give the explicit Hopf algebra structure of $H_{i,\lambda}$ as the fixed ring $(A[D_{i,\lambda}])^F$.

We have

$$G_0 = \{g \in Q_8 \mid {}^g\eta = \eta, \forall \eta \in D_{i,\lambda}\} = \{1, -1\},$$

with

$$Q_8/G_0 \cong \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\} = C_2 \times C_2.$$

Let $E_0 = E^{G_0}$. Then E_0/K is the unique biquadratic subfield of E. There exist elements α, β in E_0 satisfying $\alpha^2 \in K, \beta^2 \in K$ with $E_0 = K(\alpha, \beta)$; E_0/K is Galois with group $C_2 \times C_2$.

We have $F = D_4$, with presentation

$$D_4 = \langle a, b \mid a^4 = b^2 = 1, ab = ba^3 \rangle.$$

The action of D_4 on $D_{i,\lambda}$ is given as

$$a(\lambda(i)) = \lambda(i), \quad a(\lambda(j)\rho(i)) = \lambda(i)\lambda(j)\rho(i),$$
$$b(\lambda(i)) = \lambda(j)\rho(i)\lambda(i)\lambda(j)\rho(i) = \lambda(-i),$$
$$b(\lambda(j)\rho(i)) = \lambda(j)\rho(i)\lambda(j)\rho(i)\lambda(j)\rho(i) = \lambda(j)\rho(i).$$

We identify $C_2 \times C_2$ with the subgroup $U = \{1, a^2, b, ba^2\}$ of F. The Galois action is given as

$$a^2(\alpha) = \alpha, \quad b(\alpha) = -\alpha, \quad a^2(\beta) = -\beta, \quad b(\beta) = \beta.$$

The set $T = \{1, ba\}$ is a left transversal for U in F; the left cosets are $\{U, baU\}$.

By Theorem 2.6, E_0 and U determine an F-Galois extension of K,

$$A = E_0 \times E_0 \cong E_0e_1 \oplus E_0e_2.$$

The F-Galois action on A is given as follows: for $c_i, d_i \in K$, $0 \leq i \leq 3$,

$$a((c_0 + c_1\alpha + c_2\beta + c_3\alpha\beta)e_1 + (d_0 + d_1\alpha + d_2\beta + d_3\alpha\beta)e_2)$$

$$\begin{aligned} &= (ba^2)(c_0 + c_1\alpha + c_2\beta + c_3\alpha\beta)e_2 + (b)(d_0 + d_1\alpha + d_2\beta + d_3\alpha\beta)e_1 \\ &= (c_0 - c_1\alpha - c_2\beta + c_3\alpha\beta)e_2 + (d_0 - d_1\alpha + d_2\beta - d_3\alpha\beta)e_1, \end{aligned}$$

$$b((c_0 + c_1\alpha + c_2\beta + c_3\alpha\beta)e_1 + (d_0 + d_1\alpha + d_2\beta + d_3\alpha\beta)e_2)$$

$$\begin{aligned} &= (b)(c_0 + c_1\alpha + c_2\beta + c_3\alpha\beta)e_1 + (ba^2)(d_0 + d_1\alpha + d_2\beta + d_3\alpha\beta)e_2 \\ &= (c_0 - c_1\alpha + c_2\beta - c_3\alpha\beta)e_1 + (d_0 - d_1\alpha - d_2\beta + d_3\alpha\beta)e_2. \end{aligned}$$

By Theorem 4.3,

$$\Theta(E_0e_1 \oplus E_0e_2) = ((E_0e_1 \oplus E_0e_2)[D_{i,\lambda}])^F \cong H_{i,\lambda}.$$

To find the explicit structure of the K-Hopf algebra $H_{i,\lambda}$, set $r = \lambda(i)$, $s = \lambda(j)\rho(i)$, so that

$$D_{i,\lambda} = \langle r, s \mid r^4 = s^2 = 1, rs = sr^3 \rangle \cong D_4.$$

By direct computation,

$$(A[D_{i,\lambda}])^F = \bigoplus_{i=1}^{8} Kh_i,$$

where

$$h_1 = 1, \quad h_2 = \frac{1}{2}(r + r^3), \quad h_3 = r^2, \quad h_4 = \frac{1}{2}(\alpha(e_1 - e_2)r - \alpha(e_1 - e_2)r^3),$$
$$h_5 = \frac{1}{2}(e_1s + e_2sr + e_1sr^2 + e_2sr^3), \quad h_6 = \frac{1}{2}(\beta e_1s + \beta e_2sr - \beta e_1sr^2 - \beta e_2sr^3),$$

$$h_7 = \frac{1}{2}(e_2s + e_1sr + e_2sr^2 + e_1sr^3),$$
$$h_8 = \frac{1}{2}(\alpha\beta e_2s + \alpha\beta e_1sr - \alpha\beta e_2sr^2 - \alpha\beta e_1sr^3).$$

The K-algebra structure of $(A[D_{i,\lambda}])^F$ is given as follows. First note that $C = Kh_1 \oplus Kh_3$ is a K-subalgebra of $(A[D_{i,\lambda}])^F$, isomorphic to $K \times K$ with idempotents $f_1 = \frac{1}{2}(1 + h_3)$ and $f_2 = \frac{1}{2}(1 - h_3)$ corresponding to the first and second copies of K, respectively. Now, $\{f_2, h_4, h_6, -h_8\}$ is a K-basis for the quaternion algebra $(-\alpha^2, \beta^2)_K$. Since the the idempotent f_1 annihilates each element in this basis, we conclude that $(A[D_{i,\lambda}])^F$ contains the K-subalgebra $K \times (-\alpha^2, \beta^2)_K$. Moreover,

$$\{\frac{1}{4}(h_5 + f_1)(h_7 + f_1),\ \frac{1}{4}(h_5 - f_1)(h_7 - f_1),\ \frac{1}{4}(h_5 + f_1)(h_7 - f_1),$$
$$\frac{1}{4}(h_5 - f_1)(h_7 + f_1)\}$$

is a set of mutually orthogonal idempotents in $(A[D_{i,\lambda}])^F$ that are annihilated by f_2, thus

$$(A[D_{i,\lambda}])^F \cong K \times K \times K \times K \times (-\alpha^2, \beta^2)_K.$$

This description of $(A[D_{i,\lambda}])^F$ agrees with Truman and Taylor's decomposition found in [15, Lemma 4.7].

The Hopf algebra structure of $(A[D_{i,\lambda}])^F$ is given as:

$$\Delta(h_1) = h_1 \otimes h_1, \quad \Delta(h_2) = h_2 \otimes h_2 + \frac{1}{\alpha^2} h_4 \otimes h_4, \quad \Delta(h_3) = h_3 \otimes h_3,$$
$$\Delta(h_4) = h_2 \otimes h_4 + h_4 \otimes h_2, \quad \Delta(h_5) = h_5 \otimes h_5 + \frac{1}{\beta^2} h_6 \otimes h_6,$$
$$\Delta(h_6) = h_5 \otimes h_6 + h_6 \otimes h_5, \quad \Delta(h_7) = h_7 \otimes h_7 + \frac{1}{\alpha^2\beta^2} h_8 \otimes h_8,$$
$$\Delta(h_8) = h_7 \otimes h_8 + h_8 \otimes h_7,$$
$$\varepsilon(h_1) = 1, \quad \varepsilon(h_2) = 1, \quad \varepsilon(h_3) = 1, \quad \varepsilon(h_4) = 0, \quad \varepsilon(h_5) = 1,$$
$$\varepsilon(h_6) = 0, \quad \varepsilon(h_7) = 1, \quad \varepsilon(h_8) = 0,$$

and the coinverse $S : (A[D_{i,\lambda}])^F \to (A[D_{i,\lambda}])^F$ is induced from that of $A[D_{i,\lambda}]$.

5. The Hopf algebra isomorphism problem

Let E/K be a Galois extension with group G. Various authors have addressed the following question: what are the K-Hopf algebra isomorphism classes of the Hopf algebras that arise from the Hopf-Galois structures on E/K? See [6], [12, Section 4], [13, Theorem 2.2] and [15, Section 3]. We can use Theorem 4.3 to establish a criterion to compute these isomorphism classes.

Let $(H_N, \cdot_N)$ be a Hopf-Galois structure on E/K corresponding to a regular subgroup N of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$. Let $F_N = \mathrm{Aut}(N)$, and let

$$\Theta_N : \mathcal{G}al(K, F_N) \to \mathcal{F}orm(K[N])$$

be the Haggenmüller-Pareigis bijection, defined as $\Theta_N(A) = (A[N])^{F_N}$, where A is an F_N-Galois extension of K.

The Hopf algebra H_N is a form of $K[N]$, and we have already computed the preimage $A = \Theta^{-1}(H_N)$ in Theorem 4.3: Let

$$G_0(N) = \{g \in G \mid {}^g\eta = \eta, \forall \eta \in N\},$$

and put $E_0(N) = E^{G_0(N)}$. Then $E_0(N)$ is Galois over K with group $U_N = G/G_0(N) \le F_N$. By Theorem 2.6, $E_0(N)$ and U_N determine an F_N-Galois extension of K

$$A_{U_N} = \underbrace{E_0(N) \times E_0(N) \times \cdots \times E_0(N)}_{n},$$

$n = [F_N : U_N]$. By Theorem 4.3, $\Theta_N(A_{U_N}) = (A_{U_N}[N])^{F_N} = H_N$.

Since E/K is Galois with group G, by Galois descent the E-form H_N of $K[N]$ corresponds to a 1-cocycle (homomorphism) $\varrho_N : G \to F_N$ in

$$\mathrm{H}^1(G, \mathbf{Aut}(K[N])(E)) = \mathrm{H}^1(G, F_N).$$

The homomorphism $\varrho_N(g)$ is given as conjugation: $\eta \mapsto {}^g\eta$, for $g \in G, \eta \in N$; the kernel of ϱ_N is $G_0(N)$.

Now, suppose that $(H_{N'}, \cdot_{N'})$ is some other Hopf-Galois structure on the same E/K, corresponding to a regular subgroup N' of Perm(G), normalized by $\lambda(G)$. If $(H_N, \cdot_N)$ and $(H_{N'}, \cdot_{N'})$ are not of the same type, i.e., if $N \not\cong N'$, then $E[N] \not\cong E[N']$ as E-Hopf algebras. Thus $E \otimes_K H_N \not\cong E \otimes_K H_{N'}$ as E-Hopf algebras, and hence $H_N \not\cong H_{N'}$ as K-Hopf algebras. So the Hopf algebras attached to a Hopf-Galois structure can only be isomorphic as Hopf algebras if the structures are of the same type.

So we assume that N and N' are of the same type, i.e., there is a group isomorphism

$$\psi : N' \to N.$$

For later use, this isomorphism determines an isomorphism

$$\hat{\psi} : F_{N'} \to F_N,$$

given as $\hat{\psi}(f)(\eta) = (\psi f \psi^{-1})(\eta)$ for $f \in F_{N'}, \eta \in N$.

The isomorphism ψ extends to an isomorphism of E-Hopf algebras

$$\psi : E \otimes_K K[N'] \to E \otimes_K K[N].$$

Since $H_{N'}$ is an E-form of $K[N']$, there exists an isomorphism of E-Hopf algebras

$$\varphi' : E \otimes_K H_{N'} \to E \otimes_K K[N'],$$

thus there is an isomorphism

$$\psi\varphi' : E \otimes_K H_{N'} \to E \otimes_K K[N] \cong E[N].$$

So, $H_{N'}$ is an E-form of $K[N]$, i.e., $H_{N'}$ is an element of $\mathcal{F}orm(K[N])$. Consequently, $H_{N'}$ has a preimage under Θ_N, that is, there exists an F_N-Galois extension B of K for which

$$\Theta_N(B) = H_{N'}.$$

We compute B and its F_N-Galois structure. By descent theory, $H_{N'}$ corresponds to the 1-cocycle $d_1^0(\psi\varphi')(d_1^1(\psi\varphi'))^{-1}$ in $\mathrm{H}^1(E/K, \mathbf{Aut}(K[N])$ (d_1^i are the standard maps). We want to describe this 1-cocycle as a homomorphism in $\mathrm{H}^1(G, \mathbf{Aut}(K[N])(E))$. We have

$$\begin{aligned} d_1^0(\psi\varphi')(d_1^1(\psi\varphi'))^{-1} &= (d_1^0\psi)(d_1^0\varphi')((d_1^1\psi)(d_1^1\varphi'))^{-1} \\ &= (d_1^0\psi)((d_1^0\varphi')(d_1^1\varphi')^{-1})(d_1^1\psi)^{-1}. \end{aligned} \tag{2}$$

Now, the 1-cocycle $(d_1^0\varphi')(d_1^1\varphi')^{-1}$ corresponds to the homomorphism $\varrho_{N'}$ in $\mathrm{H}^1(G, \mathbf{Aut}(K[N'])(E))$, and we identify $d_1^0\psi = \psi \otimes id \otimes id$ with the map ψ and $(d_1^1\psi)^{-1} = \psi^{-1} \otimes id \otimes id$ with the map ψ^{-1}. So, it follows from (2) that the composition

$$\hat{\psi}\varrho_{N'} : G \to F_N, \quad G \xrightarrow{\varrho_{N'}} F_{N'} \xrightarrow{\hat{\psi}} F_N,$$

defined as

$$\hat{\psi}\varrho_{N'}(g)(\eta) = (\psi(\varrho_{N'}(g))\psi^{-1})(\eta), \quad g \in G, \eta \in N,$$

is the 1-cocycle in $\mathrm{H}^1(G, \mathbf{Aut}(K[N])(E))$ corresponding to $H_{N'}$.

The kernel of $\hat{\psi}\varrho_{N'}$ is $G_0(N')$ and the Galois group of $E_0(N')$ is $U_{N'} = G/G_0(N')$. As a subgroup of F_N, we take the Galois group of $E_0(N')$ to be $\hat{\psi}(U_{N'}) \le F_N$, which acts through $\hat{\psi}^{-1}$, i.e., $f(x) = \hat{\psi}^{-1}(f)(x)$ for $f \in \hat{\psi}(U_{N'})$, $x \in E_0(N')$.

By Theorem 2.6, $E_0(N')$ and $\hat{\psi}(U_{N'})$ determine an F_N-Galois extension of K

$$A_{\hat{\psi}(U_{N'})} = \underbrace{E_0(N') \times E_0(N') \times \cdots \times E_0(N')}_{n},$$

$n = [F_{N'} : U_{N'}] = [F_N : \hat{\psi}(U_{N'})]$. By Theorem 4.3,

$$\Theta_N(A_{\hat{\psi}(U_{N'})}) = (A_{\hat{\psi}(U_{N'})}[N])^{F_N} = H_{N'}.$$

We have proved the following.

Theorem 5.1. *Let E/K be a Galois extension with group G. Let $(H_N, \cdot_N)$, $(H_{N'}, \cdot_{N'})$ be Hopf-Galois structures on E/K corresponding to regular subgroups N, N' of* $\mathrm{Perm}(G)$*, respectively, of the same type N. Let $\psi : N' \to N$ be an isomorphism. Let A_{U_N}, $A_{\hat{\psi}(U_{N'})}$ be the F_N-Galois extensions of K as above. Then*

$$\Theta_N(A_{U_N}) = (A_{U_N}[N])^{F_N} = H_N,$$
$$\Theta_N(A_{\hat{\psi}(U_{N'})}) = (A_{\hat{\psi}(U_{N'})}[N])^{F_N} = H_{N'}.$$

An isomorphism criterion can now be given. This criterion extends [13, Theorem 2.2].

Theorem 5.2. *Let E/K be a Galois extension with group G. Let $(H_N, \cdot_N)$, $(H_{N'}, \cdot_{N'})$ be Hopf-Galois structures on E/K corresponding to regular subgroups N, N' of* $\mathrm{Perm}(G)$*, respectively, of the same type N. Let $\psi : N' \to N$ be an isomorphism. The following are equivalent:*

(a) $A_{U_N} \cong A_{\hat{\psi}(U_{N'})}$ *as* F_N*-Galois extensions of* K.
(b) $H_N \cong H_{N'}$ *as* K*-Hopf algebras.*
(c) *The* 1*-cocycle* $\varrho_N : G \to F_N$ *is cohomologous to the* 1*-cocycle* $\hat{\psi}\varrho_{N'} : G \to F_N$.
(d) *There exists a* $\lambda(G)$*-invariant map* $N' \to N$.

Proof. For (c)⇔(d): Suppose that $\xi : N' \to N$ is $\lambda(G)$-invariant. Then for all $g \in G, \eta' \in N'$,

$$ {}^g(\xi(\eta')) = \xi({}^g\eta'), $$

which is equivalent to

$$ \varrho_{H_N}(g)(\xi(\eta')) \quad = \quad \xi(\varrho_{H_{N'}}(g)(\eta')). $$

Note that $\xi = \nu\psi$ for some automorphism $\nu : N \to N$ (just set $\nu = \xi\psi^{-1}$).

Let $\eta' = \xi^{-1}(\eta)$ for some $\eta \in N$. Then we obtain

$$ \begin{aligned} \varrho_{H_N}(g)(\eta) &= \xi(\varrho_{H_{N'}}(g)(\xi^{-1}(\eta))). \\ &= ((\nu\psi)\varrho_{H_{N'}}(g)(\psi^{-1}\nu^{-1}))(\eta) \\ &= (\nu(\psi\varrho_{H_{N'}}(g)\psi^{-1})\nu^{-1})(\eta) \\ &= (\nu(\hat{\psi}\varrho_{H_{N'}})(g)\nu^{-1})(\eta), \end{aligned} $$

for all $g \in G$, and so ϱ_{H_N} is cohomologous to $\hat{\psi}\varrho_{H_{N'}}$.

Conversely, suppose that ϱ_{H_N} is cohomologous to $\hat{\psi}\varrho_{H_{N'}}$, i.e., suppose that there exists a fixed $\nu \in F_N$ for which

$$ \hat{\psi}\varrho_{H_{N'}}(g) = \nu\varrho_{H_N}(g)\nu^{-1} $$

for all $g \in G$. Then

$$ \psi\varrho_{H_{N'}}(g)\psi^{-1} = \nu\varrho_{H_N}(g)\nu^{-1}, $$

and so,

$$ (\nu^{-1}\psi)\varrho_{H_{N'}}(g) = \varrho_{H_N}(g)(\nu^{-1}\psi), \tag{3} $$

where $\nu^{-1}\psi : N' \to N$ is an isomorphism.

Now, from (3),

$$ (\nu^{-1}\psi)(\varrho_{H_{N'}}(g)(\eta')) = \varrho_{H_N}(g)((\nu^{-1}\psi)(\eta')). $$

for $g \in G, \eta' \in N'$, and so,

$$ (\nu^{-1}\psi)({}^g\eta') = {}^g((\nu^{-1}\psi)(\eta')). $$

Thus $\nu^{-1}\psi : N' \to N$ is $\lambda(G)$-invariant.

For (b)⇔(c): Use Galois descent.

For (a)⇔(b): This follows since $\Theta_N(A_{U_N}) = H_N$ and $\Theta_N(A_{\hat{\psi}(U_{N'})}) = H_{N'}$, where Θ_N is the Haggenmüller and Pareigis bijection. □

Example 5.3. We recall the details of Example 4.7: E/K is a Galois extension of fields with quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$; $K(\alpha, \beta)$ is the unique biquadratic subfield of E.

There are 6 Hopf-Galois structures on E/K of type D_4, corresponding to 6 regular subgroups that are normalized by $\lambda(Q_8)$: $D_{s,\lambda}$, $D_{s,\rho}$, for $s \in \{i, j, k\}$. Let $H_{s,\lambda}$, $H_{s,\rho}$, $s \in \{i, j, k\}$, be the corresponding K-Hopf algebras. By [15, Section 3], these Hopf algebras are pairwise non-isomorphic as K-Hopf algebras.

We recover this result using our criteria above and compute the 6 preimages under Θ of these Hopf algebras. The preimages are necessarily pairwise non-isomorphic as F-Galois extensions of K, $F = \mathrm{Aut}(D_4) \cong D_4$.

In what follows, the subgroup $D_{i,\lambda}$ plays the role of N and the other five subgroups will in turn play the role of N'. To simplify notation, we set $F_{i,\lambda} = \mathrm{Aut}(D_{i,\lambda})$. Let

$$\Theta_{D_{i,\lambda}} : \mathcal{G}al(K, F_{i,\lambda}) \to \mathcal{F}orm(K[D_{i,\lambda}])$$

be the Haggenmüller-Pareigis bijection.

By direct computation:

$$G_0(D_{i,\rho}) = \{1, -1, i, -i\}, \quad G_0(D_{j,\rho}) = \{1, -1, j, -j\},$$
$$G_0(D_{k,\rho}) = \{1, -1, k, -k\}.$$

We have

$$E_0(D_{i,\rho}) = E^{G_0(D_{i,\rho})} = K(\alpha), \quad E_0(D_{j,\rho}) = E^{G_0(D_{j,\rho})} = K(\beta),$$
$$E_0(D_{k,\rho}) = E^{G_0(D_{k,\rho})} = K(\alpha\beta),$$

with Galois groups

$$U_{i,\rho} = Q_8/G_0(D_{i,\rho}), \quad U_{j,\rho} = Q_8/G_0(D_{j,\rho}), \quad U_{k,\rho} = Q_8/G_0(D_{k,\rho}),$$

respectively. Let $\psi_{i,\rho} : D_{i,\rho} \to D_{i,\lambda}$ be an isomorphism, let $F_{i,\rho} = \mathrm{Aut}(D_{i,\rho})$ and let $\hat{\psi}_{i,\rho} : F_{i,\rho} \to F_{i,\lambda}$ be the induced isomorphism. By Theorem 2.6, $K(\alpha)$ and $\hat{\psi}_{i,\rho}(U_{i,\rho})$ determine an $F_{i,\lambda}$-Galois extension of K

$$A_{\hat{\psi}_{i,\rho}(U_{i,\rho})} = K(\alpha) \times K(\alpha) \times K(\alpha) \times K(\alpha).$$

By Theorem 5.1,

$$\Theta_{D_{i,\lambda}}(A_{\hat{\psi}_{i,\rho}(U_{i,\rho})}) = (A_{\hat{\psi}_{i,\rho}(U_{i,\rho})}[D_{i,\lambda}])^{F_{i,\lambda}} = H_{i,\rho}.$$

The preimages of $H_{j,\rho}$ and $H_{k,\rho}$ are computed in a similar manner and we obtain

$$A_{\hat{\psi}_{j,\rho}(U_{j,\rho})} = K(\beta) \times K(\beta) \times K(\beta) \times K(\beta)$$

and

$$A_{\hat{\psi}_{k,\rho}(U_{k,\rho})} = K(\alpha\beta) \times K(\alpha\beta) \times K(\alpha\beta) \times K(\alpha\beta),$$

respectively.

Clearly, $A_{\hat{\psi}_{i,\rho}(U_{i,\rho})}$, $A_{\hat{\psi}_{j,\rho}(U_{j,\rho})}$, and $A_{\hat{\psi}_{k,\rho}(U_{k,\rho})}$ are pairwise non-isomorphic as F-Galois extensions since they are pairwise non-isomorphic as K-algebras. Thus, $H_{i,\rho}$, $H_{j,\rho}$ and $H_{k,\rho}$ are pairwise non-isomorphic as K-Hopf algebras.

As shown in [15, Lemma 3.5], there is no $\lambda(G)$-invariant isomorphism $D_{s,\lambda} \to D_{t,\lambda}$ for $s, t \in \{i, j, k\}$, $s \neq t$. So by Theorem 5.2, (d)⇔(b), $H_{s,\lambda} \ncong H_{t,\lambda}$ for $s \neq t$.

We next consider the preimages of $H_{s,\lambda}$, $s \in \{i, j, k\}$, under $\Theta_{D_{i,\lambda}}$. We have

$$G_0(D_{i,\lambda}) = G_0(D_{j,\lambda}) = G_0(D_{k,\lambda}) = \{1, -1\},$$

thus

$$\begin{aligned} E_0(D_{i,\lambda}) = E^{G_0(D_{i,\lambda})} = E_0(D_{j,\lambda}) = E^{G_0(D_{j,\lambda})} \\ = E_0(D_{k,\lambda}) = E^{G_0(D_{k,\lambda})} = K(\alpha, \beta), \end{aligned}$$

with Galois groups

$$U_{i,\lambda} = U_{j,\lambda} = U_{k,\lambda} = Q_8/\{1, -1\} = C_2 \times C_2,$$

respectively.

We have already constructed the preimage of $H_{i,\lambda}$ under $\Theta_{D_{i,\lambda}}$ in Example 4.7: the $F_{i,\lambda}$-Galois extension of K, $A_{U_{i,\lambda}} = K(\alpha, \beta) \times K(\alpha, \beta)$ satisfies $\Theta_{D_{i,\lambda}}(A_{U_{i,\lambda}}) = H_{i,\lambda}$.

As for the preimage of $H_{j,\lambda}$, let $\psi_{j,\lambda} : D_{j,\lambda} \to D_{i,\lambda}$ be an isomorphism, let $F_{j,\lambda} = \mathrm{Aut}(D_{j,\lambda})$ and let $\hat{\psi}_{j,\lambda} : F_{j,\lambda} \to F_{i,\lambda}$ be the induced isomorphism. By Theorem 2.6, $K(\alpha, \beta)$ and $\hat{\psi}_{j,\lambda}(U_{j,\lambda})$ determine an $F_{i,\lambda}$-Galois extension of K, $A_{\hat{\psi}_{j,\lambda}(U_{j,\lambda})} = K(\alpha, \beta) \times K(\alpha, \beta)$, which satisfies $\Theta_{D_{i,\lambda}}(A_{\hat{\psi}_{j,\lambda}(U_{j,\lambda})}) = H_{j,\lambda}$.

The preimage of $H_{k,\lambda}$ is computed in a similar manner and is found to be $A_{\hat{\psi}_{k,\lambda}(U_{k,\lambda})} = K(\alpha, \beta) \times K(\alpha, \beta)$.

By Theorem 5.2 (a)⇔(b), $A_{U_{i,\lambda}} \ncong A_{\hat{\psi}_{j,\lambda}(U_{j,\lambda})} \ncong A_{\hat{\psi}_{k,\lambda}(U_{k,\lambda})}$ as $F_{i,\lambda}$-Galois extensions of K, though they are isomorphic as K-algebras. Theorem 5.2 (a)⇔(b) also implies that $H_{s,\lambda} \ncong H_{t,\rho}$ for $s, t \in \{i, j, k\}$.

References

[1] Auslander, M.; Goldman, O. The Brauer group of a commutative ring. *Trans. Amer. Math. Soc.* **97** no. 3 (1960), 367–409. MR0121392 (22 #12130) Zbl 0100.26304. 239

[2] Childs, L. 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 (2001e:11116) Zbl 0944.11038. 239, 247, 248, 249

[3] Childs, L. N. Hopf Galois structures on Kummer extensions of prime power degree. *New York J. Math.* **17** (2011), 51–74. MR2781908 (2012c:12006) Zbl 1233.12003. 247

[4] Childs, L. N.; Greither, C.; Keating, K.; Koch, A.; Kohl, T.; Truman, P. J.; Underwood, R. Hopf algebras and Galois module theory. Mathematical Surveys and Monographs, 260, *American Mathematical Society, Providence, RI*, 2021. vii+311 pp. ISBN: 978-1-4704-6516-2 MR4390798 Zbl 1489.16001. 239

[5] Chase, S. U.; Harrison, D. K.; Rosenberg, A. Galois theory and Galois cohomology of commutative rings. *Mem. Amer. Math. Soc.*, no. 52, (1965), 15–33. MR0195922 (33 #4118) Zbl 0143.05902. 238, 240

[6] Crespo, T.; Rio, A.; Vela, M. Non-isomorphic Hopf-Galois structures with isomorphic underlying Hopf algebras. *J. Algebra* **422** (2015), 270–276. MR3272077 Zbl 1319.16025. 246, 252

[7] Greither, C.; Pareigis, B. Hopf Galois theory for separable field extensions. *J. Algebra* **106** no. 1 (1987), 239–258. MR0878476 (88i:12006) Zbl 0615.12026. 238, 246, 248

[8] Haggenmüller, R. Über Invarianten separabler Galoiserweiterungen kommutativer Ringe, Dissertation, Universität München, 1979. 243

[9] Haggenmüller, R.; Pareigis, B. Hopf algebra forms of the multiplicative group and other groups. *manuscripta math.* **55** no. 2 (1986), 121–136. MR0833240 (87e:16026) Zbl 0604.16005. 238, 239, 243, 248

[10] Harrison, D. K. Abelian extensions of commutative rings. *Mem. Amer. Math. Soc.*, no. 52, (1965), 1–14. MR0195921 (33 #4117) Zbl 0143.06003. 242

[11] Hasse, H. Die Multiplikationsgruppe der abelschen Körper mit fester Galoisgruppe. *Abh. Math. Sem. Univ. Hamburg* **16** nos. 3-4 (1949), 29–40. MR0032597 (11,313d) Zbl 0039.26801. 242

[12] Koch, A.; Kohl, T.; Truman, P. J.; Underwood, R. Normality and short exact sequences of Hopf-Galois structures. *Comm. Algebra* **47** no. 5 (2019), 2086–2101. MR3977722 Zbl 1430.16034. 252

[13] Koch, A.; Kohl, T.; Truman, P. J.; Underwood, R. Isomorphism problems for Hopf-Galois structures on separable field extensions. *J. Pure and Appl. Algebra* **223** no. 5 (2019), 2230–2245. MR3906546 Zbl 1403.16031. 239, 252, 254

[14] Pareigis, B. Forms of Hopf algebras and Galois theory. *Topics in algebra, Part 1 (Warsaw, 1988)*, 75–93, Banach Center Publ., **26**, Part 1, *PWN, Warsaw*, 1990. MR1171227 (93f:16038) Zbl 0724.16019. 241, 242

[15] Taylor, S.; Truman, P. J. The Structure of Hopf algebras giving Hopf-Galois structures on quaternionic extensions. *New York J. Math.* **25** (2019), 219–237. MR3933762 Zbl 1466.16030. 239, 250, 252, 256, 257

[16] Waterhouse, W. 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 (82e:14003) Zbl 0442.14017. 243, 244, 248

[17] Wielandt, H. Finite permutation groups. *Academic Press, New York*, 1964. Zbl 0138.02501. 244

(Timothy Kohl) Department of Mathematics and Statistics, Boston University, 665 Commonwealth Avenue, Boston, MA 02215, USA
tkohl@math.bu.edu

(Robert Underwood) Department of Mathematics, Department of Computer Science, Auburn University at Montgomery, Montgomery, AL 36124, USA
runderwo@aum.edu

This paper is available via http://nyjm.albany.edu/j/2025/31-11.html.