Galois Extensions, Forms, and Hopf-Galois Theory

Robert G. Underwood
Department of Mathematics
Department of Computer Science
Auburn University at Montgomery
Montgomery, Alabama

June 3, 2022

Contents

1. Introduction

2. Galois Extensions

3. Hopf Algebras

4. Galois Extensions and Forms of $R[N]$

5. Connection to Hopf-Galois Theory

6. The Hopf Algebra Isomorphism Problem

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 the paper [GP87] as a way of generalizing classical Galois theory.

Since the appearance of this important paper, Hopf-Galois structures have been studied extensively by many authors, including N. Byott, L. Childs, T. Crespo, C. Greither, A. Koch, T. Kohl, D. Muñoz, A. Rio, P. J. Truman, S. Taylor, and U.

Some of these researchers have focused on the following problem: Given a (classical) Galois extension of number fields E/K, enumerate the number of Hopf-Galois structures on E/K of each possible type N.

Other authors have addressed the question: How does one determine the Hopf algebra isomorphism classes of the Hopf algebras that arise from the Hopf-Galois structures on a Galois extension of number fields?

In this talk we show how the bijection of R. Haggenmüller and B. Pareigis [HP86]

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

from the collection of Galois extensions to the collection of forms of the Hopf algebra $R[N]$, is related to the Hopf algebra isomorphism problem.

This is joint work with Timothy Kohl.

2. Galois Extensions

Let R be a commmutative ring with unity. The notion of a Galois extension of R is due to M. Auslander and O. Goldman [AG59].

Let A be a commutative R-algebra. 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 $\mathrm{Aut}_R(A)$. 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: For $r \in R$, $r(\sum_{g \in F} a_g g) = \sum_{g \in F} r a_g g$.

Define a multiplication on $D(A,F)$: For $\sum_{g \in F} a_g g$, $\sum_{h \in G} b_h h \in D(A,F)$, let

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

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 since j is R-linear and

$$\begin{aligned} j(ag \cdot bh)(t) &= j(ag(b)gh)(t) \\ &= ag(b)g(h(t)) \\ &= ag(bh(t)) \\ &= (j(ag) \circ j(bh))(t), \end{aligned}$$

for $a, b, t \in A$, $g, h \in F$.

The question of whether j is an *isomorphism* of R-algebras determines whether A is a Galois extension.

Definition 2.1.

Let R be a commmutative ring with unity and let A be a commutative R-algebra. Then A is an F-**Galois extension of** R if

(i) A is a finitely generated, projective module over R,

(ii) the map

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

defined as

$$j(\sum_{g \in F} a_g g)(x) = \sum_{g \in F} a_g g(x),$$

for all $x \in A$, $a_g \in A$, is an isomorphism of R-algebras.

□

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

Example 2.2.

Take $R = K$, where K is 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 [CHR65, 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' if there exists an isomorphism of commutative R-algebras

$$\psi : A \to A'$$

for which $\psi(g(x)) = g(\psi(x))$ 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.

There is a trivial object in $\mathcal{G}al(R, F)$. Let $\mathrm{Map}(F, R)$ denote the R-algebra of maps $\phi : F \to R$. Then $\{\phi_g\}_{g \in F}$, with $\phi_g(h) = \delta_{g,h}$, $g, h \in F$, is an R-basis for $\mathrm{Map}(F, R)$. We have

$$\mathrm{Map}(F, R) = \bigoplus_{g \in F} R\phi_g \cong \underbrace{R \times R \times \cdots \times R}_{|F|}.$$

There is an action of F on $\mathrm{Map}(F, R)$ given as

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

for $g, h \in F$, $\phi \in \mathrm{Map}(F, R)$. For the basis element ϕ_h, we have

$$g(\phi_h)(k) = \phi_h(g^{-1}k) = \delta_{h,g^{-1}k} = \delta_{gh,k} = \phi_{gh}(k),$$

for all $k \in F$, thus $g(\phi_h) = \phi_{gh}$. Through this action, F is a finite subgroup of $\mathrm{Aut}_R(\mathrm{Map}(F, R))$.

Proposition 2.3. *The commutative R-algebra $\mathrm{Map}(F, R)$ is an F-Galois extension of R.*

Proof. Since $\mathrm{Map}(F, R)$ is free over R of rank $|F|$, condition (i) of Definition 2.1 holds. For (ii), we first show that $R = \mathrm{Map}(F, R)^F$. Since $F \leq \mathrm{Aut}_R(\mathrm{Map}(F, R))$, we have $R \subseteq \mathrm{Map}(F, R)^F$. For the reverse containment, let $\phi = \sum_{g \in F} r_g \phi_g \in \mathrm{Map}(F, R)$ for $r_g \in R$.

Then

$$\begin{aligned} h(\phi)(k) &= h(\sum_{g\in F} r_g\phi_g)(k) \\ &= (\sum_{g\in F} r_g h(\phi_g))(k) \\ &= (\sum_{g\in F} r_g\phi_{hg})(k) \\ &= (\sum_{g\in F} r_g\phi_g)(k) \end{aligned}$$

for all $h, k \in F$ if and only if the coefficients r_g are equal for all $g \in F$. Thus $\phi \in R$, which shows that $R = \mathrm{Map}(F, R)^F$.

Now, the elements $\{\phi_g\}_{g\in F}$ are so that

$$\sum_{g\in F} \phi_g h(\phi_g) = \phi_1(h) = \delta_{1,h},$$

for all $h \in F$. Thus by [CHR65, Theorem 1.3, (b)⇔(c)], the map

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

is an isomorphism of R-algebras. Thus $\mathrm{Map}(F, R)$ is an F-Galois extension of R.

□

The F-Galois extension $\mathrm{Map}(F, R)$ is the **trivial** F**-Galois extension** of R.

In the case that $R = K$ is a field, B. Pareigis [Pa90, Theorem 4.2] has completely characterized F-Galois extensions of K.

Theorem 2.4. (Pareigis) *Let K be a field and let F be a finite group. Then A is an F-Galois extension of K if and only if*

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

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

Proof. Let A be an F-Galois extension of K. By [CHR65, Theorem 1.3], A is a commutative, separable K-algebra and hence

$$A = M_1 \times M_2 \times \cdots \times M_n$$

where each M_i is a separable field extension of K. Let $\phi_1, \phi_2, \ldots, \phi_n$ be the minimal orthogonal idempotents. Then F acts transitively on the set $\{\phi_1, \phi_2, \ldots, \phi_n\}$.

We have $M_i \cong M_j, \forall i, j$, hence

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

where $M = M_1$. Let U be the stabilizer of ϕ_1 in F. Then M is Galois over K with group U and $[F : U] = n$.

Conversely, let $U \leq F$, $n = [F : U]$, and let M be a U-Galois field extension of K. Let

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

with minimal orthogonal idempotents $\phi_1, \phi_2, \cdots \phi_n$.

Let $g_1, g_2, \ldots, g_n$ be a left transversal for U in F and let $\rho : F \to S_n$ be defined as

$$\rho(g)(i) = j \text{ iff } gg_iU = g_jU.$$

Define an action of F on A on each component as

$$g(m\phi_i) = (g_{\rho(g)(i)}^{-1} gg_i)(m)\phi_{\rho(g)(i)},$$

for $m \in M$, $1 \leq i \leq n$. Then A is an F-Galois extension of K.

□

Remark 2.5. If one begins with an F-Galois extension

$$A = M_1 \times M_2 \times \cdots \times M_n,$$

together with a transitive action of F on the idempotents $X = \{\phi_1, \phi_2, \ldots, \phi_n\}$, then the stabilizer U of ϕ_1 in F is the isotropy subgroup F_{ϕ_1} of ϕ_1.

Thus the set X is isomorphic to the F-set of left cosets F/F_{ϕ_1}, and the action of F on X is essentially the action of F on the set of left cosets F/F_{ϕ_1} given in the converse of the proof of Theorem 2.4.

□

Example 2.6. Let K be a field and let C_4 denote the cyclic group of order 4. Then the C_4-Galois extensions of K are of the form

$$A,$$

where A is a C_4-Galois field extension of K, or

$$A = M \times M,$$

where M 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.)

□

2.1 Forms of $\mathrm{Map}(F, R)$ and the direct limit

Let $\mathrm{Map}(F, R)$ be the trivial F-Galois extension of R. Let B be a faithfully flat commutative R-algebra. A B-**form** of $\mathrm{Map}(F, R)$ is an F-Galois extension A of R for which

$$B \otimes_R A \cong B \otimes_R \mathrm{Map}(F, R) = \mathrm{Map}(F, B)$$

as F-Galois extensions of B.

A **form** of $\mathrm{Map}(F, R)$ is an F-Galois extension A of R for which there exists a faithfully flat commutative R-algebra B with

$$B \otimes_R A \cong B \otimes_R \mathrm{Map}(F, R) \cong \mathrm{Map}(F, B)$$

as F-Galois extensions of B.

The **trivial form** of $\mathrm{Map}(F, R)$ is $\mathrm{Map}(F, R)$.

For a given faithfully flat commutative R-algebra B, we let

$$\mathcal{F}orm(B/R, \mathrm{Map}(F, R))$$

denote the collection of all B-forms of $\mathrm{Map}(F, R)$. We let $\mathcal{F}orm(\mathrm{Map}(F, R))$ denote the collection of all forms of $\mathrm{Map}(F, R)$.

We can view $\mathcal{F}orm(\mathrm{Map}(F, R))$ as a direct limit. The set $\{B/R\}$ of all faithfully flat commutative R-algebras B is partially ordered under inclusion and serves as the indexing set for the collection of objects

$$\{\mathcal{F}orm(B/R, \mathrm{Map}(F, R))_{B/R}\}.$$

Suppose that B/R, B'/R, are faithfully flat commutative R-algebras with $B \subseteq B'$. If A is a B-form of $\mathrm{Map}(F, R)$, then A is an B'-form of $\mathrm{Map}(F, R)$, thus there is a set morphism (an inclusion)

$$\varrho_{B,B'} : (B/R, \mathrm{Map}(F, R))_{B/R} \to (B'/R, \mathrm{Map}(F, R))_{B'/R}.$$

For all B/R, $\varrho_{B,B}$ is the identity map and

$$\varrho_{B',B''} \circ \varrho_{B,B'} = \varrho_{B,B''},$$

whenever $B \subseteq B' \subseteq B''$. So

$$\{\mathcal{F}orm(B/R, \mathrm{Map}(F,R))_{B/R}, \varrho_{B,B'}\}$$

is a direct system over $\{B/R\}$.

The direct limit $\varinjlim \mathcal{F}orm(B/R, \mathrm{Map}(F,R))_{B/R}$ exists and we have

$$\mathcal{F}orm(\mathrm{Map}(F,R)) = \varinjlim \mathcal{F}orm(B/R, \mathrm{Map}(F,R))_{B/R}. \tag{1}$$

3. Hopf Algebras

An R-**Hopf algebra** is a R-algebra H together with additional maps

$$\Delta_H : H \to H \otimes_R H \quad (\textbf{comultiplication}),$$
$$\varepsilon_H : H \to R \quad (\textbf{counit}),$$
$$S_H : H \to H \quad (\textbf{coinverse}),$$

where Δ_H, ε_H are R-algebra maps and S_H is a R-linear map, which satisfy the conditions:

$$(I_H \otimes \Delta_H)\Delta_H(h) = (\Delta_H \otimes I_H)\Delta_H(h), \tag{2}$$

$$(I_H \otimes \varepsilon_H)\Delta_H(h) = h \otimes 1, \quad (\varepsilon_H \otimes I_H)\Delta_H(h) = 1 \otimes h, \tag{3}$$

$$m_H(I_H \otimes S_H)\Delta_H(h) = \varepsilon_H(h)1_H = m_H(S_H \otimes I_H)\Delta_H(h), \tag{4}$$

for all $h \in H$.

Here $I_H : H \to H$ is the identity map and $m_H : H \otimes_K H \to H$ denotes multiplication in H.

Properties (2), (3), (4), are the **coassociative property**, **counit property**, and **coinverse property**, respectively.

Example 3.1. Let N be any group. Then the group ring $R[N]$ is a R-Hopf algebra with comultiplication map

$$\Delta_{R[N]} : R[N] \to R[N] \otimes_R R[N]$$

defined as $\eta \mapsto \eta \otimes \eta$, counit map

$$\varepsilon_{R[N]} : R[N] \to R,$$

given as $\eta \mapsto 1$, and coinverse map

$$S_{R[N]} : R[N] \to R[N]$$

defined by $\eta \mapsto \eta^{-1}$, for all $\eta \in N$.

Henceforth, when we write $R[N]$, we assume that $R[N]$ has this structure as a R-Hopf algebra.

3.1 Forms of $R[N]$ and the direct limit

Let N be a group and let B be a faithfully flat commutative R-algebra. A B-**form** of $R[N]$ is a R-Hopf algebra H for which

$$B \otimes_R H \cong B \otimes_R R[N] \cong B[N]$$

as B-Hopf algebras. A **form** of $R[N]$ is a R-Hopf algebra H for which there exists a faithfully flat commutative R-algebra B with

$$B \otimes_R H \cong B \otimes_R R[N] \cong B[N]$$

as B-Hopf algebras.

The **trivial Hopf form** of $R[N]$ is $R[N]$.

For a given faithfullly flat R-algebra B, we let $\mathcal{F}orm(B/R, R[N])$ denote the collection of all B-forms of $R[N]$. We let $\mathcal{F}orm(R[N])$ denote the collection of all forms of $R[N]$.

We can view $\mathcal{F}orm(R[N])$ as a direct limit. As in Section 2.1, $\{B/R, \subseteq\}$ is a directed set and

$$\{\mathcal{F}orm(B/R, R[N])_{B/R}, \varrho_{B,B'}\}$$

is a direct system over $\{B/R\}$ where

$$\varrho_{B,B'} : (B/R, R[N])_{B/R} \to \mathcal{F}orm(B'/R, R[N])_{B'/R}$$

is the inclusion map. The direct limit exists and satisfies

$$\mathcal{F}orm(R[N]) = \varinjlim \mathcal{F}orm(B/R, R[N])_{B/R}. \tag{5}$$

4. Galois Extensions and Forms of $R[N]$

Let N be a finitely generated group with finite automorphism group $F = \mathrm{Aut}(N)$.

R. Haggenmüller and B. Pareigis [HP86, Corollary 4] have shown that there is a bijective correspondence between $\mathcal{G}al(R, F)$ and $\mathcal{F}orm(R[N])$.

We first prove a lemma.

Lemma 4.1 *Let F be a finite group. Then*

$$\mathcal{G}al(R, F) = \mathcal{F}orm(\mathrm{Map}(F, R)).$$

Proof. Let A be an F-Galois extension of R. Then A is faithfully flat over R. Now, $A \otimes_R A$ is an A-algebra through $a(b \otimes c) = b \otimes ac$ for $a, b, c \in A$, and $A \otimes_R A$ is an F-Galois extension of A by the action $g(a \otimes b) = g(a) \otimes b$ for $g \in F$.

Let $\mathrm{Map}(F, A)$ denote the A-algebra of maps $F \to A$. Then $\mathrm{Map}(F, A)$ is the trivial F-Galois extension of A.

There is an isomorphism of A-algebras

$$\psi : A \otimes_R A \to \mathrm{Map}(F, A)$$

defined as $\psi(a \otimes b)(g) = g^{-1}(a)b$ for $a, b \in A$, $g \in F$. Moreover, ψ preserves the action of F since

$$\begin{array}{rcl} \psi(g(a \otimes b))(h) & = & \psi(g(a) \otimes b)(h) \\ & = & h^{-1}(g(a))b \\ & = & \psi(a \otimes b)(g^{-1}h) \\ & = & g(\psi(a \otimes b))(h), \end{array}$$

for all $h \in F$. Thus ψ is an isomorphism of F-Galois extensions of A.

Since $\mathrm{Map}(F, A) \cong A \otimes_R \mathrm{Map}(F, R)$, the R-algebra A is an A-form of $\mathrm{Map}(F, R)$.

This shows that $\mathcal{G}al(R, F) \subseteq \mathcal{F}orm(\mathrm{Map}(F, R))$.

By construction, every form of $\mathrm{Map}(F, R)$ is an F-Galois extension of R, thus $\mathcal{G}al(R, F) = \mathcal{F}orm(\mathrm{Map}(F, R))$.

□

Theorem 4.2 (Haggenmüller and Pareigis) *Let N be a finitely generated group with finite automorphism group $F = \mathrm{Aut}(N)$. Then there is a bijection*

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

Proof. Let B be a faithfully flat commutative R-algebra. By [Wa79, Section 17.6, Theorem], there is a bijective correspondence

$$\mathcal{F}orm(B/R, \mathrm{Map}(F, R)) \to \mathrm{H}^1(B/R, \mathbf{Aut}(\mathrm{Map}(F, R))) \qquad (6)$$

where $\mathbf{Aut}(\mathrm{Map}(F, R))$ denotes the automorphism group functor in the category of F-Galois extensions of R [Wa79, Section 7.6].

(For a commutative R-algebra B, $\mathbf{Aut}(\mathrm{Map}(F, R))(B)$ is the group of isomorphisms

$$B \otimes_R \mathrm{Map}(F, R) \to B \otimes_R \mathrm{Map}(F, R)$$

of F-Galois extensions of B.)

Let $\mathbf{G}(R[F])$ denote the **grouplike functor** from the category of faithfully flat commutative R-algebras to the category of groups, defined as follows: For a faithfully flat R-algebra B, $\mathbf{G}(R[F])(B)$ consists of the grouplike elements of the Hopf algebra

$$B \otimes_R R[F] \cong B[F].$$

(If $R = K$ is a field, and $B = L$ is a field extension of K, then $\mathbf{G}(K[F])(L) = F$.)

The automorphism group functor $\mathbf{Aut}(\mathrm{Map}(F, R))$ is isomorphic to the grouplike functor $\mathbf{G}(R[F])$ [Ha79, Proposition 2.14].

Thus, there is a bijective correspondence

$$\mathcal{F}orm(B/R, \mathrm{Map}(F, R)) \to \mathrm{H}^1(B/R, \mathbf{G}(R[F])). \tag{7}$$

By [Wa79, Section 17.6, Theorem], there is a bijective correspondence

$$\mathcal{F}orm(B/R, R[N]) \to \mathrm{H}^1(B/R, \mathbf{Aut}(R[N])) \tag{8}$$

where $\mathbf{Aut}(R[N])$ denotes the automorphism group functor in the category of R-Hopf algebras [Wa79, Section 7.6].

(For any commutative R-algebra B, $\mathbf{Aut}(R[N])(B)$ is the group of Hopf algebra isomorphisms $B \otimes_R R[N] \to B \otimes_R R[N]$.)

Now, $B \otimes_R R[N] \cong B[N]$, and Hopf algebra automorphisms of $B[N]$ are completely determined as the set of grouplike elements $\mathbf{G}(R[F])(B)$ of the group ring Hopf algebra $B[F]$, where $F = \mathrm{Aut}(N)$ [HP86, Theorem 2].

Thus, the automorphism group functor $\mathbf{Aut}(R[N])$ is isomorphic to the grouplike functor $\mathbf{G}(R[F])$, and there is a bijective correspondence

$$\mathcal{F}orm(B/R, R[N]) \to \mathrm{H}^1(B/R, \mathbf{G}(R[F])). \tag{9}$$

Combining (7) and (9) yields a bijective correspondence

$$\mathcal{F}orm(B/R, \mathrm{Map}(F, R)) \to \mathcal{F}orm(B/R, R[N]).$$

Taking the direct limit of both sides yields the bijection

$$\mathcal{F}orm(\mathrm{Map}(F, R)) \to \mathcal{F}orm(R[N]).$$

Thus by Lemma 4.1, we obtain a bijection

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

□

In [HP86, Theorem 5], the authors given an explicit description of the map Θ.

Theorem 4.3 (Haggenmüller and Pareigis) *Let N be a finitely generated group with finite automorphism group $F = \mathrm{Aut}(N)$. Then the bijection $\Theta : \mathcal{G}al(R, F) \to \mathcal{F}orm(R[N])$ associates to each F-Galois extension A of R, the form $H = \Theta(A)$ of $R[N]$ defined as the fixed ring*

$$H = (A[N])^F,$$

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 form H is an A-form of $R[N]$ with isomorphism $\psi : A \otimes_R H \to A[N]$ defined as $\psi(x \otimes h) = xh$, for $x \in A$, $h \in H$.

□

As one might expect, the trivial form of $\mathrm{Map}(F, R)$ is mapped to the trivial form of $R[N]$.

Proposition 4.4 *Let N be a finitely generated group with finite automorphism group $F = \mathrm{Aut}(N)$. Let $A = \mathrm{Map}(F, R)$ denote the trivial F-Galois extension of R. Then $\Theta(A) = (A[N])^F \cong R[N]$.*

Proof. (Sketch) $H = (A[N])^F$ is free over R on a basis consisting of grouplike elements. Hence, $H = R[N']$ for some finite group N'. Since $A \otimes_R H = A \otimes_R R[N'] \cong A[N]$ as Hopf algebras, we conclude that $N' \cong N$.

□

Giving an explicit description of the inverse map

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

is more subtle.

In the next section, we give an explicit formula for Θ^{-1} in the case that the forms are given as the Hopf algebras of Hopf-Galois structures of a (classical) Galois extension of K.

5. Connection to Hopf-Galois Theory

For the remainder of this talk, we take $R = K$, where K is a finite field extension of $\mathbb{Q}$. There is a natural application of the map Θ to Hopf-Galois theory.

5.1 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 [CRV15, Introduction]).

C. Greither and B. Pareigis [GP87] have given a complete classification of Hopf-Galois structures up to isomorphism.

Denote by $\mathrm{Perm}(G)$ the group of permutations of G. A subgroup $N \leq \mathrm{Perm}(G)$ is **regular** if $|N| = |G|$ and $\eta(g) \neq g$ for all $\eta \neq 1_N$, $g \in G$. Let $\lambda : G \to \mathrm{Perm}(G)$, $\lambda(g)(h) = gh$, denote the left regular representation.

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

□

Let N be a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$. We compute the corresponding Hopf-Galois structure as follows: 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 shall denote the conjugation action of $\lambda(g) \in \lambda(G)$ on $\eta \in N$ by ${}^{g}\eta$.)

Let H denote the fixed ring

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

Then H is an n-dimensional E-Hopf algebra, $n = [E : K]$, and E/K admits the Hopf Galois structure $(H, \cdot)$ [GP87, p. 248, proof of 3.1 (b)⇒(a)], [Ch00, Theorem 6.8, 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 [Ch11, Proposition 1].

By [GP87, p. 249, proof of 3.1, (a)⇒(b)],

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

as E-Hopf algebras, so H is an E-form of $K[N]$.

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

5.2 Connection to the map Θ

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 H can be recovered via the Haggenmüller and Pareigis bijection (Theorem 4.2).

In other words, with $F = \mathrm{Aut}(N)$, there is an F-Galois extension A of K with

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

We seek a method to construct A.

From [GP87, p. 249, Proof of 3.2], the E-form H of $K[N]$ corresponds to the cocycle $\varrho : G \to F$, which is given by congugation by elements of $\lambda(G)$.

The kernel of ϱ is the normal subgroup of $\lambda(G)$ given as

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

The quotient group $\lambda(G)/G_0$ 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 2.4, 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 $[F : U] = n$.

Proposition 5.2.1 *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 G_0, E_0, and A be as above. Then*

$$\Theta(A) = H.$$

Proof. Since the map $\Theta : \mathcal{G}al(K, F) \to \mathcal{F}orm(K[N])$ is a bijection, and $H \in \mathcal{F}orm(K[N])$, there exists an F-Galois extension B of K for which $\Theta(B) = H$. By Theorem 2.4,

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

where M is a V-Galois field extension of K for some subgroup V of F of index $[F : V] = m$. We claim that $A = B$.

To this end, H is an B-form of $K[N]$, thus

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

given by $x \otimes h \mapsto xh$. The F-Galois extension B contains the field M and we have

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

and so, H is an M-form of $K[N]$.

By [GP87, 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 $K[N]$.

Since there is a bijection

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

we conclude that $\Theta^{-1}(H) = B$ is an E_0-form of $\mathrm{Map}(F, K)$.

So,

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

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

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

Thus, all of the zeros of $f(x)$ must lie in E_0, hence $M \subseteq E_0$. But since E_0 is minimal, $E_0 = M$ and $U = V$. Hence

$$\Theta(A) = H$$

where

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

where $[F : U] = n$, $U \cong \lambda(G)/G_0$.

□

Example 5.2.2. Let E/K be a Galois extension with group G. Let $\rho : G \to \mathrm{Perm}(G)$, $\lambda(g)(h) = hg^{-1}$, denote the right regular representation. Then $\rho(G)$ is a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$; $\rho(G)$ corresponds to the classical Hopf-Galois structure on E/K with Hopf algebra $K[G]$ [Ch00, (6.10) Proposition].

Since $\lambda(G)$ commutes with $\rho(G)$, we have

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

Thus $U = \lambda(G)/G_0 = 1$ and $E_0 = E^{G_0} = K$. Let $F = \mathrm{Aut}(G)$. Then

$$\Theta(A) = K[G]$$

where

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

with $n = [F : 1] = |F|$. Of course, A is the trivial F-Galois extension of K, $\mathrm{Map}(F, K)$.

6. The Hopf Algebra Isomorphism Problem

Let E/K be a Galois extension with group G. Various authors: [CRV15], [KKTU19a, Section 4], [KKTU19b, Theorem 2.2], [TT19, Section 3] have addressed the following question: what are the K-Hopf algebra isomorphism classes of the various Hopf algebras that arise from the Hopf-Galois structures on E/K?

We can use Proposition 5.2.1 to establish a partial result regarding the Hopf algebra isomorphism problem.

Let $(H, \cdot)$, $(H', \cdot')$ be Hopf-Galois structures on E/K corresponding to regular subgroups N, N' of $\mathrm{Perm}(G)$, respectively.

If $(H, \cdot)$ and $(H', \cdot')$ are not of the same type, i.e., if $N \ncong N'$, then $E[N] \ncong E[N']$ as Hopf algebras. Thus $E \otimes_K H \ncong E \otimes_K H'$ as Hopf algebras, and hence $H \ncong H'$ 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. In what follows we assume that $(H, \cdot)$ and $(H', \cdot')$ are of the same type $N \cong N'$.

Proposition 6.1 *Let E/K be a Galois extension with group G. Let $(H, \cdot)$, $(H', \cdot')$ be Hopf-Galois structures on E/K corresponding to regular subgroups N, N' of $\mathrm{Perm}(G)$, respectively, with $N \cong N'$. Let*

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

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

Then $H \cong H'$ as K-Hopf algebras only if $G_0 = G_0'$.

Proof. Suppose that $H \cong H'$ as K-Hopf algebras. Let $F = \mathrm{Aut}(N)$. Then by Proposition 5.2.1, there exists F-Galois extensions A, A' of K with $\Theta(A) = H$ and $\Theta(A') = H'$, where $A \cong A'$ as F-Galois extensions.

Let $U = \lambda(G)/G_0$, $U' = \lambda(G)/G_0'$. We have

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

and

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

with $m = [F : U]$ and $n = [F : U']$. Since $A \cong A'$, $m = n$ and $E_0 \cong E_0'$. Since E_0 is Galois with group U and E_0' is Galois with group U', we must have $E_0 = E_0'$. Consequently, $G_0 = G_0'$.

□

Remark 6.2 Proposition 6.1 can be obtained from [KKTU19b, Theorem 2.2] using a G-equivariant isomorphism $N \to N'$.

□

References

[AG59] M. Auslander and O. Goldman, The Brauer group of a commutative ring, *Trans. Amer. Math. Soc.*, **81**, (1959), 749-765.

[By02] N. P. Byott, Integral Hopf-Galois structures on degree p^2 extensions of p-adic fields, *J. Algebra*, **248**, 2002, 334-365.

[Ch00] L. N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, AMS: Mathematical Surveys and Monographs, **80**, 2000.

[Ch11] L. N. Childs, Hopf Galois structures on Kummer extensions of prime power degree, *New York J. Math.*, **17**, 2011, 51-74.

[CHR65] S. U. Chase, D. K. Harrison, A. Rosenberg, *Galois Theory and Galois Cohomology of Commutative Rings*, Mem. Amer. Math. Soc., **52**, 1965. `/quaternionalg.pdf`

[CRV15] T. Crespo, A. Rio, M. Vela, Non-isomorphic Hopf-Galois structures with isomorphic underlying Hopf algebras, *J. Algebra*, **455**, (2015), 270-276.

[GP87] C. Greither and B. Pareigis, Hopf Galois theory for separable field extensions, *J. Algebra*, **106**, 1987, 239-258.

[Ha79] R. Haggenmüller, Über Invarianten separabler Galoiserweiterungen kommutativer Ringe, Dissertation, Universität München, 1979.

[HP86] R. Haggenmüller, B. Pareigis, Hopf algebra forms on the multiplicative group and other groups, *manuscripta math.*, **55**, (1986), 121-135.

[KKTU19a] A. Koch, T. Kohl, P. Truman, R. Underwood, The Structure of Hopf Algebras Acting on Dihedral Extensions. In: Feldvoss J., Grimley L., Lewis D., Pavelescu A., Pillen C. (eds) Advances in Algebra. SRAC 2017. Springer Proceedings in Mathematics & Statistics, vol 277. Springer, Cham, (2019).

[KKTU19b] A. Koch, T. Kohl, P. Truman, R. Underwood, Isomorphism problems for Hopf-Galois structures on separable field extensions, *J. Pure and Appl. Algebra*, **223**, (2019), 2230-2245.

[Pa90] B. Pareigis, Forms of Hopf algebras and Galois theory, *Topics in Algebra*, Banach Center Publications, **26**, Part 1, PWN Polish Scientific Publishers, 1990.

[TT19] S. Taylor, P. J. Truman, The Structure of Hopf algebras giving Hopf-Galois structures on quaternionic extensions, *New York J. Math.*, **25**, 2019, 219-237.

[Wa79] W. Waterhouse, *Introduction to Affine Group Schemes*, Springer-Verlag, New York, 1979.