Hopf-Galois Structures and a Characterization of Dihedral Extensions

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

AUBURN
MONTGOMERY

May 23, 2018

This is joint work with:

Alan Koch
Agnes Scott College, Decatur, GA

Timothy Kohl
Boston University, MA

Paul J. Truman
Keele University, Staffordshire, UK

1. Introduction

Assume $\mathbb{Q} \subseteq K$ and let L/K be a Galois extension with non-abelian group G.

Then L/K admits both a classical and canonical non-classical Hopf-Galois structure via the Hopf algebras $K[G]$ and H_λ, respectively.

By a theorem of C. Greither, $K[G] \cong H_\lambda$ as K-algebras.

In this talk we apply Greither's result to the case $K = \mathbb{Q}$, $G = D_3$ to yield a characterization of Galois extensions with group D_3.

In the case $G = D_4$, Greither's theorem has implications for a result of A. Ledet.

2. Hopf Galois theory

We recall the notion of a Hopf algebra, a Hopf-Galois extension, and the Greither-Pareigis classification.

A **bialgebra** over a field K is a K-algebra B together with K-algebra maps $\Delta : B \to B \otimes_K B$ (comultiplication) and $\varepsilon : B \to K$ (counit) which satisfy the conditions

$$(I \otimes \Delta)\Delta = (\Delta \otimes I)\Delta,$$

$$\mathrm{mult}(I \otimes \varepsilon)\Delta = I = \mathrm{mult}(\varepsilon \otimes I)\Delta,$$

where $\mathrm{mult} : B \otimes_K B \to B$ is the multiplication map of B and I is the identity map on B.

A **Hopf algebra** over K is a K-bialgebra H with a K-linear map $\sigma : H \to H$ which satisfies

$$\mathrm{mult}(I \otimes \sigma)\Delta(h) = \varepsilon(h)1_H = \mathrm{mult}(\sigma \otimes I)\Delta(h),$$

for all $h \in H$.

A K-Hopf algebra H is **cocommutative** if $\Delta = \tau \circ \Delta$, where $\tau : H \otimes_K H \to H \otimes_K H$, $a \otimes b \mapsto b \otimes a$ is the twist map.

Let L be a finite extension of K and let $\mathrm{m} : L \otimes_K L \to L$ denote multiplication in L.

Let H be a finite dimensional, cocommutative K-Hopf algebra and suppose there is a K-linear action of H on L which satisfies

$$h \cdot (xy) = (\mathrm{m} \circ \Delta)(h)(x \otimes y)$$
$$h \cdot 1 = \varepsilon(h)1$$

for all $h \in H,\ x, y \in L$, and that the K-linear map

$$j : L \otimes_K H \to \mathrm{End}_K(L),\ j(x \otimes h)(y) = x(h \cdot y)$$

is an isomorphism of vector spaces over K. Then we say H provides a **Hopf-Galois structure** on L/K.

Example 1. Suppose L/K is Galois with Galois group G. Let $H = K[G]$ be the group algebra, which is a Hopf algebra via $\Delta(g) = g \otimes g,\ \varepsilon(g) = 1$, $\sigma(g) = g^{-1}$, for all $g \in G$. The action

$$\left(\sum r_g g\right) \cdot x = \sum r_g(g(x))$$

provides the “usual” Hopf-Galois structure on L/K which we call the **classical** Hopf-Galois structure.

In general, the process of finding a Hopf algebra and constructing an action may seem daunting, but in the separable case C. Greither and B. Pareigis [4] have provided a complete classification of such structures.

Let L/K be separable with normal closure E. Let $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$, and $X = G/G'$. Denote by $\mathrm{Perm}(X)$ the group of permutations of X.

A subgroup $N \leq \mathrm{Perm}(X)$ is **regular** if $|N| = |X|$ and $\eta[xG'] \neq xG'$ for all $\eta \neq 1_N, xG' \in X$.

Let $\lambda : G \to \mathrm{Perm}(X)$, $\lambda(g)(xG') = gxG'$, denote the left translation map. A subgroup $N \leq \mathrm{Perm}(X)$ is **normalized** by $\lambda(G) \leq \mathrm{Perm}(X)$ if $\lambda(G)$ is contained in the normalizer of N in $\mathrm{Perm}(X)$.

Theorem 2. (Greither-Pareigis) *Let L/K be a finite separable extension. There is a one-to-one correspondence between Hopf Galois structures on L/K and regular subgroups of $\mathrm{Perm}(X)$ that are normalized by $\lambda(G)$.*

One direction of this correspondence works by Galois descent: Let N be a regular subgroup 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.,

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

For simplicity, we will denote the conjugation action of $\lambda(g) \in \lambda(G)$ on $\eta \in N$ by ${}^g\eta$.

We then define

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

The action of H on L/K is thus

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

see [2, Proposition 1].

The fixed ring H is an n-dimensional K-Hopf algebra, $n = [L : K]$, and L/K has a Hopf Galois structure via H [4, p. 248, proof of 3.1 (b)$\Longrightarrow$ (a)], [1, Theorem 6.8, pp. 52-54].

By [4, p. 249, proof of 3.1, (a) $\Longrightarrow$ (b)],

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

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

Theorem 2 can be applied to the case where L/K is Galois with group G (thus, $E = L$, $G' = 1_G$, $G/G' = G$). In this case the Hopf Galois structures on L/K correspond to regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$, where $\lambda : G \to \mathrm{Perm}(G)$, $\lambda(g)(h) = gh$, is the left regular representation.

Example 3. Suppose L/K is a Galois extension, $G = \mathrm{Gal}(L/K)$. Let $\rho : G \to \mathrm{Perm}(G)$ be the right regular representation defined as $\rho(g)(h) = hg^{-1}$ for $g, h \in G$. Then $\rho(G)$ is a regular subgroup normalized by $\lambda(G)$, since $\lambda(g)\rho(h)\lambda(g^{-1}) = \rho(h)$ for all $g, h \in G$; N corresponds to a Hopf-Galois structure with K-Hopf algebra $H = L[\rho(G)]^G = K[G]$, the usual group ring Hopf algebra with its usual action on L. Consequently, $\rho(G)$ corresponds to the **classical** Hopf Galois structure.

Example 4. Again, suppose L/K is Galois with group G. Let $N = \lambda(G)$. Then N is a regular subgroup of $\mathrm{Perm}(G)$ which is normalized by $\lambda(G)$, and $N = \rho(G)$ if and only if N abelian. We denote the corresponding Hopf algebra by H_λ. If G is non-abelian, then $\lambda(G)$ corresponds to the **canonical non-classical** Hopf-Galois structure.

3. Isomorphism Classes

It is of interest to determine how $K[G]$ and H_λ fall into K-Hopf algebra and K-algebra isomorphism classes. We have:

Theorem 5. (Koch, Kohl, Truman, U.) *Assume that G is non-abelian. Then $H_\lambda \ncong K[G]$ as K-Hopf algebras.*

Proof. Over L, $K[G]$ and H_λ are isomorphic to $L[G]$ as Hopf algebras, thus their duals $K[G]^*$ and H_λ^* are finite dimensional as algebras over K and separable (as defined in [8, 6.4, page 47]). Using the classification of such K-algebras [8, 6.4, Theorem], we conclude that $K[G]^*$ and H_λ^* are not isomorphic as K-Hopf algebras, and so neither are $K[G]$ and H_λ. In fact, by [8, 6.3, Theorem], $K[G]^*$ and H_λ^* are not isomorphic as K-algebras, and consequently, $K[G]$ and H_λ are not isomorphic as K-coalgebras. $\square$

On the other hand, C. Greither has shown that following.

Theorem 6. (Greither) *$H_\lambda \cong K[G]$ as K-algebras.*

Proof. (Sketch.)

Step 1. Obtain the Wedderburn-Artin decomposition of $K[G]$, thus:

$$K[G] \cong A_1 \times A_2 \times \cdots \times A_m,$$

where $A_i = \mathrm{Mat}_{n_i}(E_i)$ for division rings E_i.

Step 2. Show that the action of G on $L[G]$ restricts to an action on the components $L \otimes A_i$ of $L[G] \cong L \otimes_K K[G]$, and hence each component $L \otimes A_i$ descends to a component S_i in the Wedderburn-Artin decomposition of H_λ; (supressing subscripts) S is an L-form of A.

Step 3. L-forms of A are classified by the pointed set $H^1(G, \mathrm{Aut}(L \otimes_K A))$. Let $[\hat{f}]$ be the class corresponding to the class of S.

Step 4. There exists a map in cohomology

$$\Psi : H^1(G, GL_n(L \otimes_K E)) \to H^1(G, \mathrm{Inn}(L \otimes_K A))$$

with $[\hat{f}] \in H^1(G, \mathrm{Inn}(L \otimes_K A))$. Moreover, there exists a class $[\hat{q}] \in H^1(G, GL_n(L \otimes_K E))$ with $\Psi([\hat{q}]) = [\hat{f}]$.

Step 5. By Hilbert's Theorem 90 (or its generalization) $H^1(G, GL_n(L \otimes_K E))$ is trivial, hence $[\hat{f}]$ is trivial, so $S \cong A$ as K-algebras, thus $H_\lambda \cong K[G]$ as K-algebras. $\square$

4. Dihedral Extensions

Let D_n denote the dihedral group of order $2n$ for $n \geq 3$. Explicitly, we write

$$D_n = \langle \sigma, \tau : \sigma^n = \tau^2 = \sigma\tau\sigma\tau = 1 \rangle.$$

Let L/K be a Galois extension with group D_n.
By Example 3 and Example 4 we have regular subgroups $\rho(D_n),\ \lambda(D_n)$ normalized by $\lambda(D_n)$.

These regular subgroups give rise to the classical and canonical non-classical Hopf-Galois structures on L/K via the K-Hopf algebras $K[D_n]$ and H_λ, respectively.

Example 7. In the case L/K is Galois with group D_n, the classical Hopf-Galois structure on L/K has K-Hopf algebra

$$K[D_n] = \left\{ \sum_{i=0}^{n-1} \sum_{j=0}^{1} a_{i,j}\sigma^i\tau^j : \ a_{i,j} \in K \right\}.$$

Example 8. In the case L/K is Galois with group D_3, then by [1, Example 6.12], the canonical non-classical Hopf-Galois structure on L/K has K-Hopf algebra

$$H_\lambda = \{a_0 + a_1\sigma + \tau(a_1)\sigma^2 + b_0\tau + \sigma(b_0)\tau\sigma + \sigma^2(b_0)\tau\sigma^2 :$$

$$a_0 \in \mathbb{Q}, a_1 \in L^{\langle\sigma\rangle}, b_0 \in L^{\langle\tau\rangle}\}.$$

Lemma 9. *Let $L/\mathbb{Q}$ be a Galois extension with group D_4. Then H_λ consists of elements of the form*

$$h = a_0 + a_1\sigma + a_2\sigma^2 + \tau(a_1)\sigma^3 + b_0\tau + b_1\tau\sigma + \sigma(b_0)\tau\sigma^2 + \sigma(b_1)\tau\sigma^3,$$

where $a_0, a_2 \in \mathbb{Q}$, $a_1 \in L^{\langle\sigma\rangle}$, $b_0 \in L^{\langle\sigma^2,\tau\rangle}$, and $b_1 \in L^{\langle\sigma^2,\tau\sigma^3\rangle}$.

Proof. Following [1, Example 6.12], let

$$x = a_0 + a_1\sigma + a_2\sigma^2 + a_3\sigma^3 + b_0\tau + b_1\tau\sigma + b_2\tau\sigma^2 + b_3\tau\sigma^3$$

be an element of LD_4 for some $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in L$. Then the elements in H_λ are precisely those x for which $\tau(x) = x$ and $\sigma(x) = x$. □

5. Application to D_3

Let $L/\mathbb{Q}$ be a Galois extension with group D_3. Necessarily, $L = \mathbb{Q}(\alpha, \sqrt{\mathcal{D}})$, where α is a root of a reduced irreducible cubic $p(x) = x^3 + bx - c$ over $\mathbb{Q}$, and $\mathcal{D} = -4b^3 - 27c^2$ is the discriminant of $p(x)$. Note that $\mathcal{D}$ is not a square in $\mathbb{Q}$.

We have two Hopf-Galois structures on $L/\mathbb{Q}$, one is the classical Hopf-Galois structure via the $\mathbb{Q}$-Hopf algebra $\mathbb{Q}[D_3]$, and the other is the canonical Hopf-Galois structure via the $\mathbb{Q}$-Hopf algebra H_λ.

By Theorem 6, $H_\lambda \cong \mathbb{Q}[D_3]$ as $\mathbb{Q}$-algebras.

And by a well-known result, the Wedderburn-Artin decomposition of $\mathbb{Q}[D_3]$ is

$$\mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

Thus, the decomposition of H_λ is

$$\mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

So, H_λ contains a non-trivial nilpotent element h of index 2 (corresponding to the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ in the component $\mathrm{Mat}_2(\mathbb{Q})$.)

We have:

$$h^2 = 0, \quad h \neq 0.$$

But as we have seen in Example 8 above, this element must be of the form

$$h = a_0 + a_1\sigma + \tau(a_1)\sigma^2 + b_0\tau + \sigma(b_0)\tau\sigma + \sigma^2(b_0)\tau\sigma^2,$$

for some $a_0 \in \mathbb{Q}$, $a_1 \in L^{\langle\sigma\rangle}$, $b_0 \in L^{\langle\tau\rangle}$.

From this we obtain:

Theorem 10.(Koch, Kohl, Truman, U.) *Let $L/\mathbb{Q}$ be a Galois extension with group D_3. Then L is the splitting field of an irreducible cubic $x^3 + bx - c$ where $-b\mathcal{D}$ is a square in $\mathbb{Q}$.*

Proof. As we have seen above, H_λ contains a non-trivial element h with $h^2 = 0$. By direct computation
$h^2 =$

$$
\begin{aligned}
& a_0^2 + a_0 a_1 \sigma + a_0 \tau(a_1)\sigma^2 + a_0 b_0 \tau + a_0 \sigma(b_0)\tau\sigma + a_0 \sigma^2(b_0)\tau\sigma^2 \\
& + a_0 a_1 \sigma + a_1^2 \sigma^2 + a_1 \tau(a_1) + a_1 b_0 \tau\sigma^2 + a_1 \sigma(b_0)\tau + a_1 \sigma^2(b_0)\tau\sigma \\
& + a_0 \tau(a_1)\sigma^2 + a_1 \tau(a_1) + \tau(a_1^2)\sigma + b_0 \tau(a_1)\tau\sigma + \tau(a_1)\sigma(b_0)\tau\sigma^2 \\
& \qquad + \tau(a_1)\sigma^2(b_0)\tau \\
& + a_0 b_0 \tau + a_1 b_0 \tau\sigma + b_0 \tau(a_1)\tau\sigma^2 + b_0^2 + b_0 \sigma(b_0)\sigma + b_0 \sigma^2(b_0)\sigma^2 \\
& + a_0 \sigma(b_0)\tau\sigma + a_1 \sigma(b_0)\tau\sigma^2 + \sigma(b_0)\tau(a_1)\tau + b_0 \sigma(b_0)\sigma^2 + \sigma(b_0^2) \\
& \qquad + \sigma(b_0)\sigma^2(b_0)\sigma \\
& + a_0 \sigma^2(b_0)\tau\sigma^2 + a_1 \sigma^2(b_0)\tau + \tau(a_1)\sigma^2(b_0)\tau\sigma + b_0 \sigma^2(b_0)\sigma \\
& \qquad + \sigma(b_0)\sigma^2(b_0)\sigma^2 + \sigma^2(b_0^2).
\end{aligned}
$$

Hence,

$$h^2 = Z_1 + Z_\sigma \sigma + Z_{\sigma^2}\sigma^2 + Z_\tau \tau + Z_{\tau\sigma}\tau\sigma + Z_{\tau\sigma^2}\tau\sigma^2 = 0,$$

where

$$\begin{aligned}
Z_1 &= a_0^2 + 2a_1\tau(a_1) + b_0^2 + \sigma(b_0^2) + \sigma^2(b_0^2) \\
Z_\sigma &= 2a_0a_1 + \tau(a_1^2) + b_0\sigma(b_0) + \sigma(b_0)\sigma^2(b_0) + b_0\sigma^2(b_0) \\
Z_{\sigma^2} &= 2a_0\tau(a_1) + a_1^2 + b_0\sigma(b_0) + \sigma(b_0)\sigma^2(b_0) + b_0\sigma^2(b_0) \\
Z_\tau &= 2a_0b_0 + (a_1 + \tau(a_1))\sigma(b_0) + (a_1 + \tau(a_1))\sigma^2(b_0) \\
Z_{\tau\sigma} &= 2a_0\sigma(b_0) + (a_1 + \tau(a_1))b_0 + (a_1 + \tau(a_1))\sigma^2(b_0) \\
Z_{\tau\sigma^2} &= 2a_0\sigma^2(b_0) + (a_1 + \tau(a_1))b_0 + (a_1 + \tau(a_1))\sigma(b_0).
\end{aligned}$$

Thus

$$Z_1 = Z_\sigma = Z_{\sigma^2} = Z_\tau = Z_{\tau\sigma} = Z_{\tau\sigma^2} = 0,$$

and from this system, the result follows. □

Example 11. Let L be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Then $L/\mathbb{Q}$ is Galois with group D_3. Here, $\mathcal{D} = -108$ which is not a square in $\mathbb{Q}$. However, $-b\mathcal{D} = 0 \cdot -108 = 0$ is a square in $\mathbb{Q}$.

H_λ contains the non-trivial nilpotent element of index 2:

$$h = \sqrt[3]{2}\tau + \sqrt[3]{2}\zeta_3\tau\sigma + \sqrt[3]{2}\zeta_3^2\tau\sigma^2.$$

Example 12. Let L be the splitting field of $p(x) = x^3 + 23x - 529$ over $\mathbb{Q}$. As one can check, $p(x)$ is irreducible over $\mathbb{Q}$, and $\mathcal{D} = -7604375$ is not a square in $\mathbb{Q}$. Hence $L/\mathbb{Q}$ is Galois with group D_3. Now

$$-b\mathcal{D} = 174900625 = 13225^2.$$

The splitting field of $p(x)$ is $L = \mathbb{Q}(b_0, \sqrt{-23})$, where b_0 is a root of $p(x)$. Moreover, H_λ contains the non-trivial nilpotent index 2 element

$$h = \sqrt{-23}\sigma - \sqrt{-23}\sigma^2 + b_0\tau + \sigma(b_0)\tau\sigma + \sigma^2(b_0)\tau\sigma^2.$$

Example 13. Let $p(x) = x^3 - 4x + 1$. Then $p(x)$ is irreducible with $\mathcal{D} = 229$ and so the splitting field of $p(x)$ over $\mathbb{Q}$ is Galois with group D_3. However, $-b\mathcal{D} = 4 \cdot 229$, which is not a square in $\mathbb{Q}$.

By Theorem 6,

$$H_\lambda \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}),$$

and hence H_λ contains a non-trivial nilpotent element h with $h^2 = 0$.

Theorem 10 tells us how to construct from this h an irreducible cubic $x^3 + b'x - c'$ with discriminant $\mathcal{D}'$ whose splitting field is the same as that of $p(x)$, and which satisfies $-b'\mathcal{D}'$ a square in $\mathbb{Q}$.

6. Application to D_4

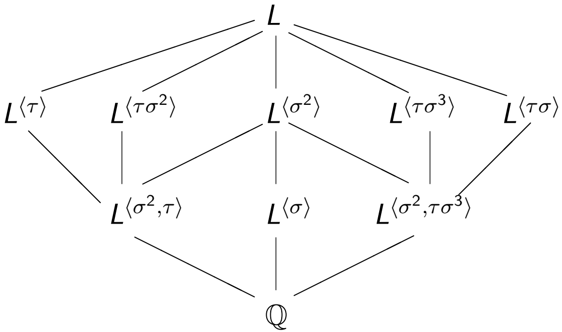
Let $L/\mathbb{Q}$ be Galois with group D_4. By (Curtis and Reiner)

$$\mathbb{Q}[D_4] \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}),$$

and so, by Theorem 6,

$$H_\lambda \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

The lattice of fixed fields is:



Note that $L^{\langle \sigma^2 \rangle}$ is the unique biquadratic extension of $\mathbb{Q}$ contained in L.

We have $L^{\langle \sigma^2 \rangle} = \mathbb{Q}(\alpha, \beta)$ with $L^{\langle \sigma^2, \tau \rangle} = \mathbb{Q}(\beta)$, $L^{\langle \sigma \rangle} = \mathbb{Q}(\alpha)$ and $L^{\langle \sigma^2, \tau\sigma^3 \rangle} = \mathbb{Q}(\alpha\beta)$.

Thus $b_0 = b_{0,1} + b_{0,2}\beta$, $a_1 = a_{1,1} + a_{1,2}\alpha$, and $b_1 = b_{1,1} + b_{1,2}\alpha\beta$ for some $b_{0,1}, b_{0,2}, a_{1,1}, a_{1,2}, b_{1,1}, b_{1,2} \in \mathbb{Q}$.

We have $\sigma(b_0) = b_{0,1} - b_{0,2}\beta$, $\sigma(b_1) = b_{1,1} - b_{1,2}\alpha\beta$, and $\tau(a_1) = a_{1,1} - a_{1,2}\alpha$.

Lemma 14. *The component* $\mathrm{Mat}_2(\mathbb{Q})$ *in the decomposition of* H_λ *has* $\mathbb{Q}$*-basis*

$$\{(1-\sigma^2)/2, \alpha(\sigma-\sigma^3), \beta(\tau-\tau\sigma^2), \alpha\beta(\tau\sigma-\tau\sigma^3)\}.$$

Proof. The idempotents corresponding to the 4 copies of $\mathbb{Q}$ in the decomposition of H_λ are $e_i = \frac{1}{8}\sum_{s\in D_4}\chi_i(s^{-1})s$, $1 \le i \le 4$, where χ_i are the characters of the 4 1-dimensional irreducible representations of D_4 (each e_i is in LD_4 and is fixed by D_4, hence $e_i \in H_{\lambda,4}$).

The idempotent corresponding to the component $\mathrm{Mat}_2(\mathbb{Q})$ is

$$e = 1 - \sum_{i=1}^{4} e_i = \frac{1-\sigma^2}{2}.$$

By Lemma 9, a typical element of H_λ appears as

$$h = a_0 + a_1\sigma + a_2\sigma^2 + \tau(a_1)\sigma^3 + b_0\tau + b_1\tau\sigma + \sigma(b_0)\tau\sigma^2 + \sigma(b_1)\tau\sigma^3,$$

where $a_0, a_2 \in \mathbb{Q}$, $a_1 \in L^{\langle\sigma\rangle}$, $b_0 \in L^{\langle\sigma^2,\tau\rangle}$, and $b_1 \in L^{\langle\sigma^2,\tau\sigma^3\rangle}$.

Thus a typical element of $\mathrm{Mat}_2(\mathbb{Q})$ is

$$\begin{aligned} eh &= \left(\frac{1-\sigma^2}{2}\right)\big(a_0 + a_1\sigma + a_2\sigma^2 + \tau(a_1)\sigma^3 + b_0\tau + b_1\tau\sigma \\ &\quad + \sigma(b_0)\tau\sigma^2 + \sigma(b_1)\tau\sigma^3\big) \\ &= q\left(\frac{1-\sigma^2}{2}\right) + a_{1,2}\alpha(\sigma-\sigma^3) + b_{0,2}\beta(\tau-\tau\sigma^2) \\ &\quad + b_{1,2}\alpha\beta(\tau\sigma-\tau\sigma^3), \end{aligned}$$

for $q, a_{1,2}, b_{0,2}, b_{1,2} \in \mathbb{Q}$. Thus

$$\{(1-\sigma^2)/2, \alpha(\sigma-\sigma^3), \beta(\tau-\tau\sigma^2), \alpha\beta(\tau\sigma-\tau\sigma^3)\}$$

is a $\mathbb{Q}$-basis for $\mathrm{Mat}_2(\mathbb{Q})$. $\square$

Theorem 15. *Let $L/\mathbb{Q}$ be a Galois extension with group D_4. Then there exists a non-trivial solution (b, c, d) in $\mathbb{Q}$ of the equation*

$$b^2\alpha^2 = c^2\beta^2 + d^2\alpha^2\beta^2, \tag{1}$$

where $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ is the unique biquadratic extension contained in L, with $\alpha^2, \beta^2 \in \mathbb{Q}$.

Proof. By Lemma 14, the component $\mathrm{Mat}_2(\mathbb{Q})$ has $\mathbb{Q}$-basis

$$\{(1-\sigma^2)/2, \alpha(\sigma-\sigma^3), \beta(\tau-\tau\sigma^2), \alpha\beta(\tau\sigma-\tau\sigma^3)\}.$$

Put $1 := (1-\sigma^2)/2$, $X := \alpha(\sigma-\sigma^3)$, $Y := \beta(\tau-\tau\sigma^2)$, and $Z := \alpha\beta(\tau\sigma-\tau\sigma^3)$.

Then we have the multiplication table:

	1	X	Y	Z
1	1	X	Y	Z
X	X	$-4\alpha^2$	$-2Z$	$2\alpha^2 Y$
Y	Y	$2Z$	$4\beta^2$	$2\beta^2 X$
Z	Z	$-2\alpha^2 Y$	$-2\beta^2 X$	$4\alpha^2\beta^2$

Clearly, $\mathrm{Mat}_2(\mathbb{Q}) \subseteq H_\lambda$ contains an element $h \in$ with $h^2 = 0$ and $h \neq 0$. Write

$$h = a + bX + cY + dZ,$$

for $a, b, c, d \in \mathbb{Q}$. Then

$$\begin{aligned} h^2 &= (a + bX + cY + dZ)(a + bX + cY + dZ) \\ &= (a^2 - 4b^2\alpha^2 + 4c^2\beta^2 + 4d^2\alpha^2\beta^2) + 2abX + 2acY + 2adZ \\ &= 0, \end{aligned}$$

and so,

$$
\begin{aligned}
a^2 + 4c^2\beta^2 + 4d^2\alpha^2\beta^2 &= 4b^2\alpha^2 \\
2ab &= 0 \\
2ac &= 0 \\
2ad &= 0.
\end{aligned}
$$

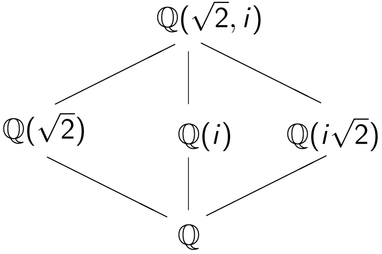
If $a \neq 0$, then $b = c = d = 0$, hence $a^2 = 0$, which is impossible. So we assume that $a = 0$.

It follows that $h^2 = 0$, $h \neq 0$, implies that there is a non-trivial solution (b, c, d) to

$$b^2\alpha^2 = c^2\beta^2 + d^2\alpha^2\beta^2.$$

Moreover, h is non-trivial if and only if (b, c, d) is non-trivial. $\square$

Example 16. Let L be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. By [3, Corollary 4.5], the Galois group is D_4. We have $L = \mathbb{Q}(\sqrt[4]{2}, i)$ with $\sigma(i) = i$, $\sigma(\sqrt[4]{2}) = -i\sqrt[4]{2}$, $\tau(i) = -i$, and $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$. The lattice of the unique biquadratic extension is



where $L^{\langle\sigma^2\rangle} = \mathbb{Q}(\sqrt{2}, i)$ is the unique biquadratic extension in L with quadratic subfields $L^{\langle\sigma^2,\tau\rangle} = \mathbb{Q}(\sqrt{2})$, $L^{\langle\sigma\rangle} = \mathbb{Q}(i)$, and $L^{\langle\sigma^2,\tau\sigma^3\rangle} = \mathbb{Q}(i\sqrt{2})$. We choose $\beta = \sqrt{2}$, $\alpha = i$. Then equation (1) is

$$-b^2 = 2c^2 - 2d^2,$$

which has a non-trivial solution $(b, c, d) = (0, 1, 1)$. The corresponding element $h \in \mathrm{Mat}_2(\mathbb{Q})$ is

$$h = \sqrt{2}(\tau - \tau\sigma^2) + i\sqrt{2}(\tau\sigma - \tau\sigma^3),$$

which satisfies $h^2 = 0$, $h \neq 0$.

Example 17. Let $f(x) = x^4 - 4x^2 - 3$. Then $p(x) = f(x-1)$ is irreducible over $\mathbb{Q}$, by the Eisenstein criterion, and hence $f(x)$ is irreducible over $\mathbb{Q}$. By [3, Corollary 4.5] the Galois group of the splitting field of $f(x)$ is D_4. Note that the discriminant satisfies

$$\mathcal{D} = -37632 = -3 \cdot 12544 = -3 \cdot 112^2 = -147 \cdot 16^2.$$

The roots of $f(x)$ are

$$\sqrt{2+\sqrt{7}},\ \sqrt{2-\sqrt{7}},\ -\sqrt{2+\sqrt{7}},\ -\sqrt{2-\sqrt{7}}.$$

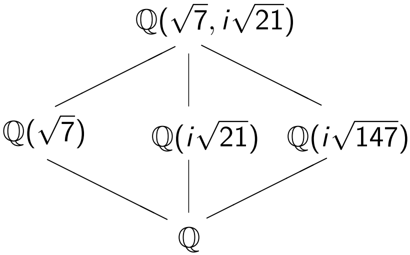
The splitting field over $\mathbb{Q}$ is $L = \mathbb{Q}(\sqrt{2+\sqrt{7}}, i\sqrt{3})$. The Galois action is given by

$$\sigma\left(\sqrt{2+\sqrt{7}}\right) = \sqrt{2-\sqrt{7}},\ \ \sigma\left(\sqrt{2-\sqrt{7}}\right) = -\sqrt{2+\sqrt{7}},$$

$$\tau\left(\sqrt{2+\sqrt{7}}\right) = \sqrt{2+\sqrt{7}},\ \ \tau\left(\sqrt{2-\sqrt{7}}\right) = -\sqrt{2-\sqrt{7}},$$

$$\sigma(i\sqrt{3}) = \tau(i\sqrt{3}) = -i\sqrt{3}.$$

The unique biquadratic extension contained in L is $\mathbb{Q}(\sqrt{7}, i\sqrt{3}) = \mathbb{Q}(\sqrt{7}, i\sqrt{21})$, with lattice



where $L^{\langle\sigma^2\rangle} = \mathbb{Q}(\sqrt{7}, i\sqrt{21})$, with quadratic subfields $L^{\langle\sigma^2,\tau\rangle} = \mathbb{Q}(\sqrt{7})$, $L^{\langle\sigma\rangle} = \mathbb{Q}(i\sqrt{21})$, and $L^{\langle\sigma^2,\tau\sigma^3\rangle} = \mathbb{Q}(i\sqrt{37632}) = \mathbb{Q}(i\sqrt{147}) = \mathbb{Q}(i\sqrt{3})$, see [3, proof of Theorem 4.1]. Let $\beta = \sqrt{7}$, $\alpha = i\sqrt{21}$. Then equation (1) is

$$-21b^2 = 7c^2 - 147d^2,$$

which has non-trivial solution $(b, c, d) = (1, 9, 2)$. Thus

$$i\sqrt{21}(\sigma - \sigma^3) + 9\sqrt{7}(\tau - \tau\sigma^2) + 2i\sqrt{147}(\tau\sigma - \tau\sigma^3)$$

is a non-trivial nilpotent element of index 2 in H_λ.

7. Application to a Result of Ledet

We obtain a new proof of the following result of A. Ledet [6, 0.4]:

Theorem 18.(Ledet) *Let $L/\mathbb{Q}$ be a Galois extension with group D_4. Let $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ be the unique biquadratic extension contained in L. Then $\beta^2\alpha^2$ is a norm in $\mathbb{Q}(\beta)/\mathbb{Q}$.*

Proof. By Theorem 15 there exists a non-trivial solution (b, c, d) in $\mathbb{Q}$ to the equation

$$b^2\alpha^2 = c^2\beta^2 + d^2\alpha^2\beta^2.$$

Assuming $c \neq 0$, $\alpha \neq 0$, we have

$$\frac{b^2}{c^2} - \frac{d^2}{c^2}\beta^2 = \frac{\beta^2}{\alpha^2},$$

thus $\frac{\beta^2}{\alpha^2}$ is a norm in $\mathbb{Q}(\beta)/\mathbb{Q}$. Consequently, $\beta^2\alpha^2$ is a norm in $\mathbb{Q}(\beta)/\mathbb{Q}$. □

Ledet's result also gives another proof of Greither's result (Theorem 6) in the case $G = D_4$:

Theorem 19. *Let $L/\mathbb{Q}$ be a Galois extension with group D_4. Then*

$$H_\lambda \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

Proof. Regardless of Greither's result, we always have

$$H_\lambda \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_r(R),$$

where $1 \leq r \leq 2$ and R is some division ring.

Now, $L/\mathbb{Q}$ is a solution to the "Galois theoretical embedding problem" given by $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ and the short exact sequence

$$1 \to \langle \sigma^2 \rangle \to D_4 \to C_2 \times C_2 \to 1.$$

So by [6, 0.4], $\beta^2\alpha^2$ is a norm in $\mathbb{Q}(\beta)/\mathbb{Q}$, that is, there exist $x, y \in \mathbb{Q}$ so that

$$x^2 - y^2\beta^2 = \beta^2\alpha^2.$$

Thus,

$$x^2 = \beta^2\alpha^2 + y^2\beta^2, \quad \text{or}$$
$$x^2\alpha^2 = \alpha^4\beta^2 + y^2\alpha^2\beta^2.$$

Let $b = x$, $c = \alpha^2$, $d = y$. Then

$$bX + cY + dZ$$

is a non-trivial nilpotent of index 2 in H_λ, thus

$$H_\lambda \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

□

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

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

K. Conrad, Galois groups of cubics and quartics (not in characteristic 2),
http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf

C. Greither and B. Pareigis.
Hopf Galois theory for separable field extensions.
J. Algebra, 106(1), 239–258, 1987.

A. Koch, T. Kohl, P. Truman, and R. Underwood.
The Structure of Hopf algebras acting on dihedral extensions.
in Advances in Algebra, *Proc. Math. Stats.*, Springer, to appear.

A. Ledet,
Embedding problems and equivalence of quadratic forms.
Math. Scand., 88, 279-302, 2001.

A. Koch, T. Kohl, P. Truman, and R. Underwood.
Isomorphism problems for Hopf-Galois structures on separable field extensions.
arXiv: 1711.05554, 2017.

W. C. Waterhouse.
Introduction to Affine Group Schemes.
Springer-Verlag, New York, 1979.