Algebraic Structure of the Canonical Non-classical Hopf Algebra

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

AUBURN
MONTGOMERY

June 12, 2019

1. Introduction

Let K be a field containing $\mathbb{Q}$, 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By an (unpublished) theorem of C. Greither, $K[G] \cong H_\lambda$ as K-algebras.

Various proofs of Greither's result have been found in certain cases.

For instance, S. Taylor and P. J. Truman [TT19] have shown that $K[G] \cong H_\lambda$ when G is the quaternion group Q_8.

U. has shown that $K[G] \cong H_\lambda$ for the cases $G = D_4$ and $G = D_3$.

In this talk we review these results; we examine the D_3 case in detail to find explicit formulas for the matrix units in H_λ.

2. Hopf Galois theory

We review some of the basic notions of Hopf-Galois theory.

Let L be a finite extension of a field K.

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 of H on L that satisfies

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

$$h \cdot 1 = \varepsilon(h)1$$

for all $h \in H,\ x, y \in L$, where $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$ is Sweedler notation.

Suppose also, 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 H together with this action provides a **Hopf-Galois structure** on L/K.

Example 2.1. 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 the separable case C. Greither and B. Pareigis [GP87] 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 2.2. (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 [Ch11, 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 [GP87, p. 248, proof of 3.1 (b)$\Longrightarrow$ (a)], [Ch00, Theorem 6.8, pp. 52-54].

By [GP87, 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 2.2 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 2.3. 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 2.4. 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 3.1. (Koch, Kohl, Truman, U. [KKTU19]) *Assume that G is non-abelian. Then $H_\lambda \not\cong K[G]$ 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 [Wa79, 6.4, page 47]). Using the classification of such K-algebras [Wa79, 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 [Wa79, 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. $\square$

Here is an another proof for Theorem 3.1.

Proof. By [Ko15, Corollary 1.3], the group-like elements of H_λ are computed as $G(H_\lambda) = \lambda(G) \cap \rho(G)$, which cannot be all of $\rho(G)$ since G is non-abelian. Thus $H_\lambda \ncong K[G]$ as K-Hopf algebras. $\square$

For the moment, we fix G, and the base field K, and allow L/K to vary.

Proposition 3.2. *Let L/K and L'/K be Galois extensions with non-abelian group G with $L \ncong L'$. Let H_λ and $H_{\lambda'}$ be the corresponding canonical non-classical Hopf algebras. Let E be the compositum of L, L', with Galois group Γ. Assume that $E^{Z(\Gamma)} \not\subseteq L \cap L'$, where $Z(\Gamma)$ denotes the center of Γ. Then $H_\lambda \ncong H_{\lambda'}$ as K-Hopf algebras.*

Proof. By way of contradiction, assume that $H_\lambda \cong H_{\lambda'}$ as K-Hopf algebras. Then

$$L \otimes_K H_\lambda \cong L[\lambda(G)] \cong L[G] \cong L \otimes_K H_{\lambda'}$$

as L-Hopf algebras. Thus $L \otimes_K H_{\lambda'}$ has exactly $|G|$ group-like elements.

Now tensoring over L with E yields

$$E \otimes_L L[G] \cong E \otimes_L (L \otimes_K H_{\lambda'}) \cong E[G].$$

So, the group-likes in $L \otimes_K H_{\lambda'}$ are the group elements in G. This is a contradiction since $E^{Z(\Gamma)} \nsubseteq L \cap L'$.

$\square$

We next consider K-algebra structure.

Theorem 3.3. (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. $\square$

For details in the case $G = D_p$, p an odd prime, see [KKTU19, Theorem 4].

Recently, P. J. Truman has given the following generalization.

Theorem 3.4. (Truman) *Let N be given and let N' be the centralizer of N in $\mathrm{Perm}(G)$. Then $(L[N])^G \cong (L[N'])^G$ as K-algebras.*

4. Greither's Theorem for $G = Q_8$

Let

$$Q_8 = \langle \sigma, \tau : \sigma^4 = \tau^4 = 1, \sigma^2 = \tau^2, \sigma\tau = \tau\sigma^3 \rangle$$

denote the quaternion group. Let L/K be a Galois extension with group Q_8.

Then L/K has a unique biquadratic extension $K(\alpha, \beta)$ with $\alpha^2 = a \in K$, $\beta^2 = b \in K$ corresponding to the unique subgroup $\langle \sigma^2 \rangle$ of order 2.

For $x, y \in K^\times$, let $(x, y)_K$ denote the quaternion algebra with K-basis $\{1, u, v, w\}$, satisfying the relations $u^2 = x$, $v^2 = y$, $uv = w$, $vu = -w$.

We have the following result due to S. Taylor and P. J. Truman [NYJM19]

Proposition 4.1. (Taylor and Truman)

$$K[Q_8] \cong K \times K \times K \times K \times (-1, -1)_K,$$

and

$$H_\lambda \cong K \times K \times K \times K \times (-a, -b)_K.$$

What is not immediate is whether $(-1, -1)_K \cong (-a, -b)_K$ as K-algebras.

Proposition 4.2. (Taylor and Truman) $(-1,-1)_K \cong (-a,-b)_K$ *as K-algebras.*

Consequently, $H_\lambda \cong K[Q_8]$ as K-algebras.

In the decomposition

$$K[Q_8] \cong K \times K \times K \times K \times (-1,-1)_K,$$

the 4-dimensional K-algebra $(-1,-1)_K$ could either be a division ring or isomorphic to $Mat_2(K)$.

Proposition 4.3. *If K is real, then $(-1,-1)_K$ is a division ring.*

Proof. Let $q = a + bu + cv + dw \in (-1,-1)_K$ for $a, b, c, d \in K$ not all 0. Since K is real, one can compute the inverse

$$q^{-1} = (a - bu - cv - dw)/(a^2 + b^2 + c^2 + d^2).$$

$\square$

Proposition 4.4. *If K contains i then $(-1,-1)_K \cong Mat_2(K)$.*

Proof. The map $\phi : (-1,-1)_K \to Mat_2(K)$ defined as

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ u \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ v \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ w \mapsto \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

is an isomorphism of K-algebras. See [Ro17, Example C-2.114]. □

5. Greither's Theorem for $G = D_4$

Our methods here share similarities with the Q_8 case.

Let

$$D_4 = \langle \sigma, \tau : \sigma^4 = \tau^2 = \sigma\tau\sigma\tau = 1 \rangle$$

denote the dihedral group of order 8. Let L/K be a Galois extension with group D_4.

Then L/K has a unique biquadratic extension $K(\alpha, \beta)$ with $\alpha^2 = a \in K$, $\beta^2 = b \in K$ corresponding to the subgroup $\langle \sigma^2 \rangle$ of order 2.

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

The lattice of fixed fields is:

$$
\begin{tikzcd}
 & & L \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
L^{\langle\tau\rangle} \arrow[dr, dash] & L^{\langle\tau\sigma^2\rangle} \arrow[d, dash] & L^{\langle\sigma^2\rangle} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & L^{\langle\tau\sigma^3\rangle} \arrow[d, dash] & L^{\langle\tau\sigma\rangle} \arrow[dl, dash] \\
 & L^{\langle\sigma^2,\tau\rangle} \arrow[dr, dash] & L^{\langle\sigma\rangle} \arrow[d, dash] & L^{\langle\sigma^2,\tau\sigma^3\rangle} \arrow[dl, dash] & \\
 & & K & &
\end{tikzcd}
$$

By [CR81, Example 7.39]

$$K[D_4] \cong K \times K \times K \times K \times Mat_2(K).$$

And by character theory,

$$H_\lambda \cong K \times K \times K \times K \times Mat_n(D)$$

where $1 \leq n \leq 2$ and D is some division algebra over K.

We proceed to compute the component $Mat_n(D)$. (We intend to show that $Mat_n(D) \cong Mat_2(K)$.)

We begin by characterizing the elements in H_λ.

Proposition 5.1. *Let L/K 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 $a_0, a_2 \in K$, $a_1 \in L^{\langle\sigma\rangle}$, $b_0 \in L^{\langle\sigma^2,\tau\rangle}$, and $b_1 \in L^{\langle\sigma^2,\tau\sigma^3\rangle}$.

Proof. Following [Ch00, 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 $L[D_4]$ 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 $\sigma(x) = x$. □

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

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

Let M be the subalgebra of H_λ corresponding to the component $\mathrm{Mat}_n(D)$ in the decomposition of H_λ.

Proposition 5.2. *M has K-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 K in the decomposition of H_λ are $e_i = \frac{1}{8}\sum_{s\in D_4}\chi_i(s^{-1})s$, $1 \leq i \leq 4$, 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 $e_i \in H_\lambda$).

The idempotent corresponding to the component $\mathrm{Mat}_n(D)$ is

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

By Proposition 5.1, 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 $a_0, a_2 \in K$, $a_1 \in L^{\langle\sigma\rangle}$, $b_0 \in L^{\langle\sigma^2,\tau\rangle}$, and $b_1 \in L^{\langle\sigma^2,\tau\sigma^3\rangle}$.

And so, a typical element of M 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 $q, a_{1,2}, b_{0,2}, b_{1,2} \in K$. Thus

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

is a K-basis for M. $\square$

Let $1 = (1-\sigma^2)/2$, $X = \alpha(\sigma - \sigma^3)$, $Y = \beta(\tau - \tau\sigma^2)$, 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	$-2\alpha^2 Y$	$-2\beta^2 X$	$4\alpha^2\beta^2$

Thus M is isomorphic as a K-algebra to the quaternion algebra $(-4a, 4b)_K$ with the quaternionic basis $\{1, X, Y, -2Z\}$.

Proposition 5.3. $M \cong (-4a, 4b)_K \cong (b, ba)_K$.

Proof. By [Co19, (4), (1), (2)],

$$M \cong (-4a, 4b)_K \cong (-a, b)_K \cong (b, -a)_K \cong (b, ba)_K.$$

$\square$

Proposition 5.4. $M \cong (b, ba)_K \cong Mat_2(K)$.

Proof. As in [Le01], L/K is a solution to the "Galois theoretical embedding problem" given by $K(\alpha, \beta)/K$ and the short exact sequence

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

So by [Le01, 0.4], ba is a norm in $K(\beta)/K$, that is, there exist $s, t \in K$ so that

$$s^2 - bt^2 = ba. \tag{1}$$

Thus by [Co19, Theorem 4.16], $M \cong (b, ba)_K \cong Mat_2(K)$. $\square$

Alternative ending of proof. From (1), we have

$$s^2 = ba + bt^2, \quad \text{or}$$
$$as^2 = a^2 b + abt^2.$$

Then

$$sX + aY + tZ$$

is a non-trivial nilpotent of index 2 in H_λ, thus $M \cong \mathrm{Mat}_2(K)$.

$\square$

Our conclusion is that

$$H_\lambda \cong K[D_4] \cong K \times K \times K \times K \times \mathrm{Mat}_2(K).$$

6. Greither's Theorem for $G = D_3$

Our method now differs from the Q_8 and D_4 cases.

Let

$$D_3 = \langle \sigma, \tau : \sigma^3 = \tau^2 = \sigma\tau\sigma\tau = 1 \rangle$$

denote the dihedral group of order 6. Let L/K be a Galois extension with group D_3.

L/K is the splitting field of some irreducible cubic $p(X) = X^3 + qX + r$ over K with discriminant $\mathcal{D} = -4q^3 - 27r^2$, not a square in K.

By [Ro15, Proposition A-5.69], $L^{\langle \sigma \rangle} = K(\sqrt{\mathcal{D}})$.

By [Ro15, Theorem A-1.2], the roots of $p(X)$ are

$$s+t, \quad s\zeta+t\zeta^2, \quad s\zeta^2+t\zeta$$

with $s=\sqrt[3]{(-r+\sqrt{R})/2}$, $t=-q/(3s)$, $R=r^2+(4/27)q^3$, and ζ a primitive 3rd root of unity. Note that $st=-q/3$ and $s^3+t^3=-r$.

The Galois action on L is defined by

$$\sigma(s+t)=s\zeta+t\zeta^2, \quad \sigma(s\zeta+t\zeta^2)=s\zeta^2+t\zeta, \quad \sigma(s\zeta^2+t\zeta)=s+t,$$

$$\tau(s+t)=s+t, \quad \tau(s\zeta+t\zeta^2)=s\zeta^2+t\zeta, \quad \tau(s\zeta^2+t\zeta)=s\zeta+t\zeta^2.$$

Let $\beta = s + t$, $v = 2\beta - \sigma(\beta) - \sigma^2(\beta)$, and $w = 2\beta^2 - \sigma(\beta^2) - \sigma^2(\beta^2)$.

Lemma 6.1.

(i) $v = 3s + 3t$,

(ii) $w = 3s^2 + 3t^2$,

(iii) $\sigma(s^2 + t^2) = s^2\zeta^2 + t^2\zeta$.

(iv) $\sigma(s^2\zeta + t^2\zeta^2) = s^2 + t^2$.

By [CR81, Example (7.39)],

$$K[D_3] \cong K \times K \times \mathrm{Mat}_2(K),$$

and by character theory,

$$H_\lambda \cong K \times K \times \mathrm{Mat}_n(D), \tag{2}$$

where $1 \leq n \leq 2$ and D is a division algebra over K.

We claim that $Mat_n(D) \cong Mat_2(K)$.

Let M be the subalgebra of H_λ corresponding to the component $\mathrm{Mat}_n(D)$ in the decomposition (2).

In order to show that $M \cong Mat_2(K)$, we first compute a K-basis for M.

By [Ch00, Example 6.12],

$$H_\lambda = \{a_0 + a_1\sigma + \tau(a_1)\sigma^2 + b_0\tau + \sigma(b_0)\tau\sigma + \sigma^2(b_0)\tau\sigma^2 :$$
$$a_0 \in K, a_1 \in L^{\langle\sigma\rangle}, b_0 \in L^{\langle\tau\rangle}\}.$$

Let $a_1 = q_0 + q_1\sqrt{\mathcal{D}}$ be a typical element of $L^{\langle\sigma\rangle} = K(\sqrt{\mathcal{D}})$, $q_0, q_1 \in K$. Note that $\tau(a_1) = q_0 - q_1\sqrt{\mathcal{D}}$.

Let $b_0 = r_0 + r_1\beta + r_2\beta^2$ a typical element of $L^{\langle\tau\rangle} = K(\beta)$, $r_0, r_1, r_2 \in K$.

Proposition 6.2. *A K-basis for M is*

$$\Big\{(2-\sigma-\sigma^2)/3, \sqrt{\mathcal{D}}(\sigma-\sigma^2), (v\tau+\sigma(v)\tau\sigma+\sigma^2(v)\tau\sigma^2)/3,$$

$$(w\tau+\sigma(w)\tau\sigma+\sigma^2(w)\tau\sigma^2)/3\Big\}.$$

Proof. The element $e_3 = (2-\sigma-\sigma^2)/3$ is the orthogonal idempotent corresponding to the component $M \cong \mathrm{Mat}_n(D)$ in the decomposition (2).

By Childs' result, H_λ consists of elements of the form

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

where $a_0 \in K$, $a_1 \in K(\sqrt{\mathcal{D}})$, and $b_0 \in K(\beta)$. Thus, the product $e_3 h$ is a typical element of M, which can be written as a linear combination of the claimed basis. □

We want to convert the basis of Proposition 6.2 into a quaternionic K-basis. We assume $q \neq 0$.

Lemma 6.3. *A K-basis for M is* $\{1, U, V, W\}$ *where* $1 = (2 - \sigma - \sigma^2)/3$, $U = \sqrt{\mathcal{D}}(\sigma - \sigma^2)$, $V = (w\tau + \sigma(w)\tau\sigma + \sigma^2(w)\tau\sigma^2)/3$, *and* $W = UV = \sqrt{\mathcal{D}}(\sigma - \sigma^2)(w\tau + \sigma(w)\tau\sigma + \sigma^2(w)\tau\sigma^2)/3$.

Proof. We have

$$\begin{aligned}
&\sqrt{\mathcal{D}}(\sigma - \sigma^2)(w\tau + \sigma(w)\tau\sigma + \sigma^2(w)\tau\sigma^2)/3 \\
&\quad = \sqrt{\mathcal{D}}((\sigma(w) - \sigma^2(w))\tau + (\sigma^2(w) - w)\tau\sigma + (w - \sigma(w))\tau\sigma^2)/3) \\
&\qquad = \sqrt{\mathcal{D}}((\sigma(w) - \sigma^2(w))\tau + \sigma(\sigma(w) - \sigma^2(w))\tau\sigma \\
&\qquad\qquad + \sigma^2(\sigma(w) - \sigma^2(w))\tau\sigma^2)/3).
\end{aligned}$$

And, $\sqrt{\mathcal{D}}((\sigma(w) - \sigma^2(w))$

$$\begin{aligned} &= (s^3 - t^3)(\zeta(1-\zeta^2)(1-\zeta)^2(3\sigma(\beta^2) - 3\sigma^2(\beta^2)) \\ &= 9(s^3 - t^3)(2\zeta + 1)(s^2 - t^2)(\zeta^2 - \zeta) \\ &= 27(s^3 - t^3)(s^2 - t^2) \\ &= 27(s^5 + t^5) - q^2 v \\ &= -9rw - 2q^2 v. \end{aligned}$$

And so, the matrix that converts the basis of Proposition 6.2 to the set $\{1, U, V, W\}$ is invertible, hence $\{1, U, V, W\}$ is a basis.

$\square$

In fact, the K-basis $\{1, U, V, W\}$ is quaternionic. We need some lemmas.

Let $\mathrm{Tr}_{L^{\langle\tau\rangle}/K} : L^{\langle\tau\rangle} \to K$ and $\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/K} : L^{\langle\sigma\tau\rangle} \to K$ and denote the trace maps.

Lemma 6.4. $\mathrm{Tr}_{L^{\langle\tau\rangle}/K}(w^2) = -2\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/K}(w\sigma(w))$.

Proof. We have $\mathrm{Tr}_{L^{\langle\tau\rangle}/K}(w) = 0$. Thus

$$\begin{aligned}
0 &= (w + \sigma(w) + \sigma^2(w))^2 \\
&= w^2 + \sigma(w^2) + \sigma^2(w^2) + 2w\sigma(w) + 2\sigma(w)\sigma^2(w) + 2w\sigma^2(w) \\
&= \mathrm{Tr}_{L^{\langle\tau\rangle}/K}(w^2) + 2\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/K}(w\sigma(w)).
\end{aligned}$$

Lemma 6.5. $\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/K}(w\sigma(w)) = -3q^2$.

Proof. We have

$$
\begin{aligned}
\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/K}(w\sigma(w)) = \mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}(9(s^2+t^2)(s^2\zeta^2+t^2\zeta))
\end{aligned}
$$

$$
\begin{aligned}
&= 9\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}((s^2+t^2)(s^2\zeta^2+t^2\zeta)) \\
&= 9\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}(s^4\zeta^2+s^2t^2\zeta+s^2t^2\zeta^2+t^4\zeta) \\
&= 9\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}(s^4\zeta^2+t^4\zeta-s^2t^2) \\
&= 9\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}(s^4\zeta^2+t^4\zeta-(q^2/9)) \\
&= -3q^2.
\end{aligned}
$$

Lemma 6.6.
$((w\tau + \sigma(w)\tau\sigma + \sigma^2(w)\tau\sigma^2)/3)^2 = q^2(2 - \sigma - \sigma^2)/3.$

Proof.
$((w\tau + \sigma(w)\tau\sigma + \sigma^2(w)\tau\sigma^2)/3)^2$

$$\begin{aligned}
&= \frac{1}{9}\left(w^2 + \sigma(w^2) + \sigma^2(w^2)\right) \\
&\quad + \frac{1}{9}(w\sigma(w) + \sigma(w)\sigma^2(w) + w\sigma^2(w))\sigma \\
&\quad + \frac{1}{9}(w\sigma(w) + \sigma(w)\sigma^2(w) + w\sigma^2(w))\sigma^2 \\
&= -\frac{2}{9}\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/K}(w\sigma(w)) + \frac{1}{9}\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/K}(w\sigma(w))\sigma \\
&\quad + \frac{1}{9}\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/K}(w\sigma(w))\sigma^2 \\
&= -\frac{1}{3}\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/K}(w\sigma(w))(2 - \sigma - \sigma^2)/3 \\
&= q^2(2 - \sigma - \sigma^2)/3
\end{aligned}$$

Proposition 6.7. *A quaternionic K-basis for M is $\{1, U, V, W\}$ where $1 = (2 - \sigma - \sigma^2)/3$, $U = \sqrt{\mathcal{D}}(\sigma - \sigma^2)$, $V = (w\tau + \sigma(w)\tau\sigma + \sigma^2(w)\tau\sigma^2)/3$, and $W = UV = \sqrt{\mathcal{D}}(\sigma - \sigma^2)(w\tau + \sigma(w)\tau\sigma + \sigma^2(w)\tau\sigma^2)/3$.*

Proof. The set $\{1, U, V, W\}$ is linearly independent over K hence is a K-basis for M. Now, $U^2 = -3\mathcal{D}$, $V^2 = q^2$, and $UV = -VU$. Thus $M \cong (-3\mathcal{D}, q^2)_K$.

$\square$

Now we can show that $M \cong Mat_2(K)$ and hence $H_\lambda \cong K[D_3]$ as K-algebras.

Proposition 6.8. *$M \cong Mat_2(K)$.*

Proof. By [Co19, (4)], $M \cong (-3\mathcal{D}, q^2) \cong (-3\mathcal{D}, 1)_K$. Thus by [Co19, Theorem 4.3] $M \cong Mat_2(K)$.

$\square$

7. Matrix Units in H_λ: the $G = D_3$ Case

By Proposition 6.8, $M \cong Mat_2(K)$. We compute the matrix units in M.

By [Co19, Theorem 4.3], there is a K-algebra isomorphism $\phi : M \to Mat_2(K)$ given as

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ U \mapsto \begin{pmatrix} 0 & 1 \\ -3\mathcal{D} & 0 \end{pmatrix},\ V/q \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$UV/q \mapsto \begin{pmatrix} 0 & -1 \\ -3\mathcal{D} & 0 \end{pmatrix}.$$

Thus,

$$\frac{1}{2}U - \frac{1}{2}UV/q \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \frac{1}{2}1 - \frac{1}{2}V/q \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\frac{1}{2}1 + \frac{1}{2}V/q \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad -\frac{1}{6\mathcal{D}}U - \frac{1}{6\mathcal{D}}UV/q \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

References

[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.*, Vol 17, (2011), 51-74.

[Co19] K. Conrad, Quaternion algebras, `https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf`

[CR81] C. W. Curtis and I. Reiner, *Methods of Representation Theory, vol. 1*, Wiley, 1981.

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

[KKTU19] A. Koch, T. Kohl, P. J. Truman, R. Underwood. (2019) 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.

[Ko15], T. Kohl, Grouplike elements as Galois groups on Hopf-Galois extensions, *preprint: July 13, 2015*.

[Le01], A. Ledet, Embedding problems and equivalence of quadratic forms, *Math. Scand.*, 88, 279-302, 2001.

[Ro15] J. Rotman, *Advanced Modern Algebra*, Third Ed., Part 1, Amer. Math. Soc., 2015.

[Ro17] J. Rotman, *Advanced Modern Algebra*, Third Ed., Part 2, Amer. Math. Soc., 2017.

[Se77] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.

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

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