Hopf-Galois Structures and Binary Quadratic Forms

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

March 23, 2019

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

Let $L/\mathbb{Q}$ be a Galois extension with group

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

the dihedral group of order 6. Then $L/\mathbb{Q}$ admits a canonical non-classical Hopf-Galois structure with Hopf algebra H_λ.

By a theorem of C. Greither, $H_\lambda \cong \mathbb{Q}[D_3]$ as $\mathbb{Q}$-algebras.

In this talk we show that up to scalar multiplication, nilpotent elements in H_λ correspond to rational points on a certain conic over $\mathbb{Q}$. Using this we give a new proof of Greither's theorem.

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 group G. Let $H = K[G]$ be the group algebra, which is a Hopf algebra via $\Delta(g) = g \otimes g,\ \varepsilon(g) = 1$, $S(g) = g^{-1}$, for all $g \in G$. The action of $K[G]$ on L given as

$$\Big(\sum_{g \in G} r_g g\Big) \cdot x = \sum_{g \in G} r_g(g(x))$$

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

In the case that L/K is separable, C. Greither and B. Pareigis have given a complete classification of Hopf-Galois 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.,

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

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

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

The fixed ring H is an n-dimensional K-Hopf algebra, $n = [L : K]$, and L/K has a Hopf Galois structure via H.

Moreover,

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

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 $N = \rho(G)$ is a regular subgroup normalized by $\lambda(G)$, since $\lambda(g)\rho(h)\lambda(g^{-1}) = \rho(h)$ for all $g, h \in G$.

$N = \rho(G)$ corresponds to a Hopf-Galois structure with K-Hopf algebra

$$H_\rho = (L[\rho(G)])^G = K[G],$$

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. The corresponding Hopf algebra is the fixed ring

$$H_\lambda = (L[\lambda(G)])^G.$$

If G is non-abelian, then $N = \lambda(G)$ corresponds to the *canonical non-classical* Hopf-Galois structure. □

3. The Case $K = \mathbb{Q}$, $G = D_3$

For the remainder of this talk, we specialize to the case where the base field $K = \mathbb{Q}$, and the Galois group is the dihedral group of order 6,

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

Let $L/\mathbb{Q}$ be a Galois extension with group D_3. By Example 2.3, and Example 2.4, we have regular subgroups $\rho(D_3)$, $\lambda(D_3)$ normalized by $\lambda(D_3)$.

These regular subgroups give rise to the classical and canonical non-classical Hopf-Galois structures on $L/\mathbb{Q}$ via the $\mathbb{Q}$-Hopf algebras $\mathbb{Q}[D_3]$ and H_λ, respectively.

The classical Hopf-Galois structure on $L/\mathbb{Q}$ has $\mathbb{Q}$-Hopf algebra

$$\mathbb{Q}[D_3] = \left\{ a_{0,0} + a_{0,1}\sigma + a_{0,2}\sigma^2 + a_{1,0}\tau + a_{1,1}\tau\sigma + a_{1,2}\tau\sigma^2 : \; a_{i,j} \in \mathbb{Q} \right\}.$$

And, due to L. Childs, the canonical non-classical Hopf-Galois structure on $L/\mathbb{Q}$ has $\mathbb{Q}$-Hopf algebra

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

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

It is of interest to determine how $\mathbb{Q}[D_3]$ and H_λ fall into isomorphism classes as algebras and Hopf algebras.

Proposition 3.1. *H_λ and $\mathbb{Q}[D_3]$ are not isomorphic as $\mathbb{Q}$-Hopf algebras.*

Proof. See [KKTU19, Proposition 4]. □

The situation is different as algebras.

Theorem 3.2. [C. Greither] *$H_\lambda \cong \mathbb{Q}[D_3]$ as $\mathbb{Q}$-algebras.*

Proof. This is shown in [KKTU19, Theorem 4]. Note: Greither's theorem holds for any Galois extension L/K, $\mathbb{Q} \subseteq K$, with group G, that is, we always have $H_\lambda \cong K[G]$ as K-algebras. □

Since $\mathbb{Q}$ has characteristic 0, both H_λ and $\mathbb{Q}[D_3]$ are left semisimple and decompose into a product of matrix rings over division rings.

By [CR81, Example (7.39)],

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

as $\mathbb{Q}$-algebras. And so, by Theorem 3.2

$$H_\lambda \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}), \tag{1}$$

as $\mathbb{Q}$-algebras.

Let M be the subalgebra of H_λ corresponding to the component $\mathrm{Mat}_2(\mathbb{Q})$ in the decomposition (1).

We compute a $\mathbb{Q}$-basis for $M \subseteq H_\lambda$.

Let $\alpha \in L$ be so that $L^{\langle\sigma\rangle} = \mathbb{Q}(\alpha)$, $\alpha^2 \in \mathbb{Q}$, and let $a_1 = q_0 + q_1\alpha$ be a typical element of $\mathbb{Q}(\alpha)$, $q_0, q_1 \in \mathbb{Q}$. Note that $\tau(a_1) = q_0 - q_1\alpha$.

Let $\beta \in L$ be so that $L^{\langle\tau\rangle} = \mathbb{Q}(\beta)$ with $b_0 = r_0 + r_1\beta + r_2\beta^2$ a typical element of $\mathbb{Q}(\beta)$, $r_0, r_1, r_2 \in \mathbb{Q}$.

Let $v = 2\beta - \sigma(\beta) - \sigma^2(\beta)$, $w = 2\beta^2 - \sigma(\beta^2) - \sigma^2(\beta^2)$.

Proposition 3.3. *A $\mathbb{Q}$-basis for M is*

$$\left\{ \frac{2-\sigma-\sigma^2}{3}, \alpha(\sigma-\sigma^2), \frac{v\tau+\sigma(v)\tau\sigma+\sigma^2(v)\tau\sigma^2}{3}, \right.$$

$$\left. \frac{w\tau+\sigma(w)\tau\sigma+\sigma^2(w)\tau\sigma^2}{3} \right\}.$$

Proof. The element $e_3 = (2-\sigma-\sigma^2)/3$ is the orthogonal idempotent corresponding to the component $\mathrm{Mat}_2(\mathbb{Q})$ in the decomposition (1). 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 $a_0 \in \mathbb{Q}$, $a_1 \in \mathbb{Q}(\alpha)$, and $b_0 \in \mathbb{Q}(\beta)$. Thus, the product $e_3 h$ is a typical element of M, which can be written as a linear combination of the claimed basis. □

Since $\mathrm{Mat}_2(\mathbb{Q})$ has nilpotent elements, e.g. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, H_λ must have nilpotent elements, necessarily in the subalgebra M.

Here is how we find them.

Let $m \in M \subseteq H_\lambda$. By Proposition 3.3, there exists $a, b, c, d \in \mathbb{Q}$ so that

$$\begin{aligned} m &= a(2-\sigma-\sigma^2) + b\alpha(\sigma-\sigma^2) + c(v\tau + \sigma(v)\tau\sigma + \sigma^2(v)\tau\sigma^2) \\ &\quad + d(w\tau + \sigma(w)\tau\sigma + \sigma^2(w)\tau\sigma^2) \\ &= a(2-\sigma-\sigma^2) + b\alpha(\sigma-\sigma^2) \\ &\quad + ((cv+dw)\tau + \sigma(cv+dw)\tau\sigma + \sigma^2(cv+dw)\tau\sigma^2). \end{aligned}$$

Let $\mathrm{Tr}_{L^{\langle\tau\rangle}/\mathbb{Q}} : L^{\langle\tau\rangle} \to \mathbb{Q}$ and $\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}} : L^{\langle\sigma\tau\rangle} \to \mathbb{Q}$ and denote the trace maps. Let $\mathrm{N}_{L^{\langle\tau\rangle}/\mathbb{Q}} : L^{\langle\tau\rangle} \to \mathbb{Q}$ denote the norm map.

Lemma 3.4. *The element m is nilpotent of index 2 if and only if the following conditions hold:*

(i) $a = 0$,

(ii) $\mathrm{Tr}_{L^{\langle\tau\rangle}/\mathbb{Q}}((cv + dw)^2) = 2b^2\alpha^2$,

(iii) $\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}((cv + dw)\sigma(cv + dw)) = -b^2\alpha^2$.

Proof. We show directly that $m^2 = 0$ if and only if conditions (i), (ii), and (iii) hold. □

4. Application to Binary Quadratic Forms

Let $p(X) = X^3 + qX + r$ be an irreducible cubic over $\mathbb{Q}$ with discriminant $\mathcal{D} = -4q^3 - 27r^2$. Without loss of generality we can assume that $q, r \in \mathbb{Z}$.

Suppose $\mathcal{D}$ is not a square in $\mathbb{Q}$. Then the splitting field L of $p(X)$ is Galois over $\mathbb{Q}$ with group D_3.

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

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

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

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

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

Let H_λ be the $\mathbb{Q}$-Hopf algebra of the canonical non-classical Hopf Galois structure on $L/\mathbb{Q}$.

By Theorem 3.2,

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

Let M be the subalgebra of H_λ isomorphic to $\mathrm{Mat}_2(\mathbb{Q})$. Let m be a nilpotent element of M.

By Lemma 3.4(iii), there exist rationals x, y so that

$$\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}((xv + yw)\sigma(xv + yw)) = -\mathcal{D}. \qquad (2)$$

We claim that the right-hand side of (2) is a binary quadratic form in x, y over $\mathbb{Z}$.

To prove this we first need a lemma.

Lemma 3.5.

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

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

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

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

Proposition 3.6.
$\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}((xv+yw)\sigma(xv+yw)) = 9qx^2 + 27rxy - 3q^2y^2.$

Proof. We have $(xv+yw)\sigma(xv+yw)$

$$\begin{aligned} = \ & 9x^2(s+t)(s\zeta+t\zeta^2) + 9xy((s+t)(s^2\zeta^2+t^2\zeta) \\ & + (s^2+t^2)(s\zeta+t\zeta^2)) + 9y^2(s^2+t^2)(s^2\zeta^2+t^2\zeta). \end{aligned}$$

Now, applying $\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}$ to each term above yields

$$\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}((xv+yw)\sigma(xv+yw)) = 9qx^2 + 27rxy - 3q^2y^2.$$

Now, in view of (2) and Proposition 3.6, the equation

$$E:\ 9qX^2 + 27rXY - 3q^2Y^2 = -\mathcal{D}$$

has a non-trivial solution (x, y) in the rationals (and hence an infinite number of rational solutions). The discriminant of the binary quadratic form is

$$\mathcal{D}' = (27r)^2 - 4(9q)(-3q^2) = -27\mathcal{D}.$$

If $\mathcal{D}' > 0$, then $\mathcal{D} < 0$. Thus if E is an hyperbola, then $p(X)$ has one real root and two non-real complex roots. Moreover, if $p(X)$ has three real roots, then E is an ellipse.

The nilpotent elements of H_λ (up to multiplication by a rational) correspond to rational points on the graph of E.

Example 3.7. Let $q(X) = X^3 + 3X + 1$. Then $q(X)$ is irreducible with $\mathcal{D} = -135$, and so its splitting field $L/\mathbb{Q}$ is Galois with group D_3. The roots of $q(X)$ are

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

where $s = \sqrt[3]{(-1+\sqrt{5})/2}$, $t = \sqrt[3]{(-1-\sqrt{5})/2}$. In this case,

$$E: \ 27X^2 + 27XY - 27Y^2 - 135 = 0,$$

with $\mathcal{D}' = -27(-135) = 3645$, and $\mathcal{D} = -135$. Thus E is a hyperbola and $X^3 + 3X + 1$ has exactly one real root.

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

By inspection, $(2, 1)$ is a solution to E. Thus

$$m = \sqrt{-135}(\sigma - \sigma^2) + (2v + w)\tau + \sigma(2v + w)\tau\sigma + \sigma^2(2v + w)\tau\sigma^2$$

is a nilpotent element of H_λ.

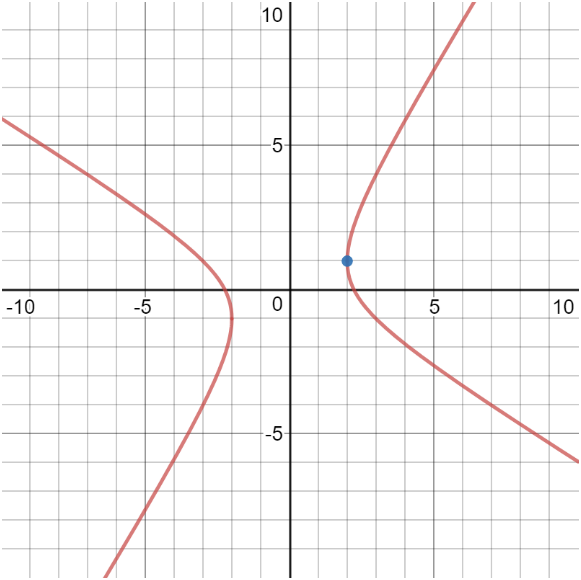

Fig. 1. Graph of hyperbola $27X^2 + 27XY - 27Y^2 - 135 = 0$ given by $X^3 + 3X + 1$. The point $(2, 1)$ corresponds to the nilpotent element $m \in H_\lambda$.

4. Another Proof of Greither's Theorem

Let $L/\mathbb{Q}$ be Galois with group D_3 and let y be a generator for the subfield $L^{\langle\tau\rangle}$ with minimal polynomial $p(X) = X^3 + qX + r$ and discriminant $\mathcal{D} = -4q^3 - 27r^2$.

In this section we give an alternate proof of Greither's theorem (Theorem 3.2).

Theorem 4.1. (Greither) *$H_\lambda \cong \mathbb{Q}[D_3]$ as $\mathbb{Q}$-algebras.*

Proof. By the theory of characters,

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

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

So to establish Greither's result, we show that $r = 2$ and $R = \mathbb{Q}$, and to do this it suffices to show that H_λ contains a non-trivial nilpotent element of index 2.

In order prove the existence of such an element, we show that

$$E: \; 9qX^2 + 27rXY - 3q^2Y^2 = -\mathcal{D} = 4q^3 + 27r^2.$$

has a non-trivial solution in the rationals. Then by Proposition 3.6, there are rationals x, y not both zero with

$$\mathrm{Tr}_{L^{\langle\sigma\tau\rangle}/\mathbb{Q}}((xv + yw)\sigma(xv + yw)) = -\mathcal{D}.$$

Consequently, by Lemma 3.4(iii), H_λ contains a non-trivial nilpotent of index 2, and so the decomposition is in fact

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

If $q = 0$, then E is easily solved since it reduces to $XY = r$. So we assume that $q \neq 0$.

If $q \neq 0$, one checks that $X = 2q/3$, $Y = 3r/q$ is a non-trivial rational solution to E. $\square$

References

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

[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.

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

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