The Structure of the Greither-Pareigis Hopf Algebra $(L\lambda(S_3))^{S_3}$

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

AUBURN
MONTGOMERY

May 24, 2017

1. Introduction

Let $L/\mathbb{Q}$ be a Galois extension with group S_3. Let $H = (L\lambda(S_3))^{S_3}$ be the Greither-Pareigis Hopf algebra determined by the regular subgroup $\lambda(S_3) \leq \mathrm{Perm}(S_3)$ normalized by $\lambda(S_3)$. In this talk we prove the following proposition.

Proposition 1.

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

if and only if L is the splitting field of an irreducible cubic $x^3 + bx - c$ where either $b = 0$, or $-\frac{1}{b}\mathcal{D}$ is a square in $\mathbb{Q}$ ($\mathcal{D} = -4b^3 - 27c^2$ is the discriminant).

2. Proof of Proposition 1

We first need a lemma.

Lemma 2. *Let $L/\mathbb{Q}$ be a Galois extension with group S_3. Let $H = (L\lambda(S_3))^{S_3}$ be the Greither-Pareigis Hopf algebra determined by the regular subgroup $\lambda(S_3)$. If H contains a non-trivial nilpotent element of index 2, then L is the splitting field of an irreducible cubic $x^3 + bx - c$ where either $b = 0$, or $-\frac{1}{b}\mathcal{D}$ is a square in $\mathbb{Q}$.*

Proof. By [1, Example 6.12], H 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 $a_0 \in \mathbb{Q}$, $a_1 \in L^{\langle\sigma\rangle}$, and $b_0 \in L^{\langle\tau\rangle}$.

By direct computation,

$$h^2 = U + V\sigma + W\sigma^2 + X\tau + Y\tau\sigma + Z\tau\sigma^2,$$

where

$$\begin{aligned}
U &= a_0^2 + 2a_1\tau(a_1) + n \\
V &= 2a_0a_1 + \tau(a_1^2) + m \\
W &= 2a_0\tau(a_1) + a_1^2 + m \\
X &= 2a_0b_0 + (a_1 + \tau(a_1))\sigma(b_0) + (a_1 + \tau(a_1))\sigma^2(b_0) \\
Y &= 2a_0\sigma(b_0) + (a_1 + \tau(a_1))b_0 + (a_1 + \tau(a_1))\sigma^2(b_0) \\
Z &= 2a_0\sigma^2(b_0) + (a_1 + \tau(a_1))b_0 + (a_1 + \tau(a_1))\sigma(b_0),
\end{aligned}$$

with

$$\begin{aligned}
m &= b_0\sigma(b_0) + \sigma(b_0)\sigma^2(b_0) + b_0\sigma^2(b_0), \\
n &= b_0^2 + \sigma(b_0^2) + \sigma^2(b_0^2), \\
2m + n &= (b_0 + \sigma(b_0) + \sigma^2(b_0))^2.
\end{aligned}$$

Now suppose that H contains an element

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

with $h^2 = 0$, $h \neq 0$, for some $a_0 \in \mathbb{Q}$, $a_1 \in L^{\langle\sigma\rangle}$, and $b_0 \in L^{\langle\tau\rangle}$. Since H is flat over $\mathbb{Q}$ and $\{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ is an L-basis for LS_3, $U = V = W = X = Y = Z = 0$.

Case I. $a_0 \in \mathbb{Q}$**,** $a_1 \in L^{\langle\sigma\rangle}$**,** $b_0 \in \mathbb{Q}$**.** In this case, we have two possibilites: $a_1 \in \mathbb{Q}$ or $a_1 \in L^{\langle\sigma\rangle}\backslash\mathbb{Q}$.

(i) $a_1 \in \mathbb{Q}$. From $U = 0$, we obtain $a_0^2 + 2a_1^2 + 3b_0^2 = 0$, and so, $a_0 = a_1 = b_0 = 0$. Thus $h = 0$, and so, (i) is not possible.

(ii) $a_1 \in L^{\langle\sigma\rangle}\backslash\mathbb{Q}$. From $U = V = 0$, we obtain

$$\begin{aligned} a_0^2 + 2a_1\tau(a_1) + 3b_0^2 &= 0 \\ 2a_0a_1 + \tau(a_1^2) + 3b_0^2 &= 0. \end{aligned}$$

Since $[L^{\langle\sigma\rangle} : \mathbb{Q}] = 2$ and $a_1 \in L^{\langle\sigma\rangle}\backslash\mathbb{Q}$, $a_1 = v + w\sqrt{d}$, where $v, w, d \in \mathbb{Q}$ with $w \neq 0$, $d \neq 0$. We have $\tau(\sqrt{d}) = -\sqrt{d}$.

Now, $a_0^2 + 2a_1\tau(a_1) = 2a_0a_1 + \tau(a_1^2)$, hence

$$a_0^2 + 2(v + w\sqrt{d})(v - w\sqrt{d}) = 2a_0(v + w\sqrt{d}) + (v - w\sqrt{d})^2,$$

thus

$$a_0^2 + 2v^2 - 2w^2d = 2a_0v + 2a_0w\sqrt{d} + v^2 - 2vw\sqrt{d} + w^2d,$$

and so, $2a_0w = 2vw$, and $a_0^2 + 2v^2 - 2w^2d = 2a_0v + v^2 + w^2d$.

Consequently, $a_0 = v$, and so, $3w^2d = 0$, which is not possible. So (ii) cannot happen.

Case II. $a_0 \in \mathbb{Q}$**,** $a_1 \in L^{\langle\sigma\rangle}$**,** $b_0 \in L^{\langle\tau\rangle}\backslash\mathbb{Q}$**.** Since $b_0 \in L^{\langle\tau\rangle}\backslash\mathbb{Q}$ and $[L^{\langle\tau\rangle} : \mathbb{Q}] = 3$, b_0 is a root of an irreducible cubic polynomial

$$p(x) = x^3 - ax^2 + bx - c$$

over $\mathbb{Q}$.

Since the roots of $p(x)$ are b_0, $\sigma(b_0)$ and $\sigma^2(b_0)$, $a = b_0 + \sigma(b_0) + \sigma^2(b_0)$ and $b = m$. Since $[L^{\langle\sigma\rangle} : \mathbb{Q}] = 2$, we write $a_1 = v + w\sqrt{d}$ for $v, w, d \in \mathbb{Q}$, $d \neq 0$. We have $\tau(\sqrt{d}) = -\sqrt{d}$.

From $X = Y = Z = 0$ we obtain the system of equations

$$\begin{aligned} 2a_0 b_0 + 2v\sigma(b_0) + 2v\sigma^2(b_0) &= 0 \\ 2a_0\sigma(b_0) + 2vb_0 + 2v\sigma^2(b_0) &= 0 \\ 2a_0\sigma^2(b_0) + 2vb_0 + 2v\sigma(b_0) &= 0, \end{aligned} \tag{1}$$

which in matrix form appears as $2Az = 0$, where $z = (b_0, \sigma(b_0), \sigma^2(b_0))^t$, and

$$A = \begin{pmatrix} a_0 & v & v \\ v & a_0 & v \\ v & v & a_0 \end{pmatrix}.$$

Now, $\det(A) = (2v + a_0)(v - a_0)^2$. If A is invertible, then $b_0 = 0$, which is impossible since $b_0 \notin \mathbb{Q}$. So, either $a_0 = -2v$, or $a_0 = v$. Note: if $w = 0$, then $a_1 = v$. We now have four possibilities to consider.

(i) $a_0 = -2v$ and $w = 0$ (so that $a_1 = v$). From $U = V = 0$, we obtain $(-2a_1)^2 + 2a_1^2 + n = 0$ and $2(-2a_1)a_1 + a_1^2 + m = 0$, so that $6a_1^2 + n = 0$ and $-3a_1^2 + m = 0$. It follows that

$$0 = 2m + n = (b_0 + \sigma(b_0) + \sigma^2(b_0))^2,$$

whence, $b_0 + \sigma(b_0) + \sigma^2(b_0) = 0$, hence $a = 0$.

Moreover, from (1),

$$2(-2a_1)b_0 + 2a_1\sigma(b_0) + 2a_1\sigma^2(b_0)$$

$$= -4a_1 b_0 + 2a_1\sigma(b_0) + 2a_1\sigma^2(b_0) = 0,$$

and so, $-6a_1 b_0 = 0$.

Thus either $a_1 = 0$ or $b_0 = 0$. But the latter case is not possible, and so, $a_1 = 0$. Now, since $V = 0$, $m = b = 0$. It follows that b_0 is a root of the irreducible polynomial $x^3 - c$. Consequently, L is the splitting field of $x^3 - c$ over $\mathbb{Q}$.

(ii) $a_0 = v$ and $w = 0$. From $U = V = 0$, we obtain $a_1^2 + 2a_1^2 + n = 0$ and $2a_1^2 + a_1^2 + m = 0$. Hence

$$9a_1^2 + 2m + n = 9a_1^2 + (b_0 + \sigma(b_0) + \sigma^2(b_0))^2 = 0,$$

so $a_0 = a_1 = 0$ and $b_0 + \sigma(b_0) + \sigma^2(b_0) = 0$. Again, this yields $m = 0$, and b_0 is a root of the irreducible polynomial $x^3 - c$. Hence, L is the splitting field of $x^3 - c$ over $\mathbb{Q}$.

(iii) $a_0 = -2v$ and $w \neq 0$. From $V = W = 0$ we obtain

$$2(-2v)(v+w\sqrt{d})+(v-w\sqrt{d})^2 = 2(-2v)(v-w\sqrt{d})+(v+w\sqrt{d})^2,$$

thus $12vw\sqrt{d} = 0$. And so, $v = 0$, thus $a_0 = 0$. Since $U = V = W = 0$, $2a_1\tau(a_1) + n = 0$, $\tau(a_1^2) + m = 0$, and $a_1^2 + m = 0$. Consequently,

$$2a_1\tau(a_1) + \tau(a_1^2) + a_1^2 + 2m + n$$

$$= (a_1 + \tau(a_1))^2 + (b_0 + \sigma(b_0) + \sigma^2(b_0))^2 = 0,$$

and so, $b_0 + \sigma(b_0) + \sigma^2(b_0) = 0$. Thus b_0 is a root of the cubic $p(x) = x^3 + bx - c$, $b = m$.

Let $\mathcal{D} = -4b^3 - 27c^2$ be the discriminant of $p(x)$. From [4, Proposition 4.59(i)], $L^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{\mathcal{D}})$.

Since $w \neq 0$, $a_1 \in L^{\langle\sigma\rangle} \backslash \mathbb{Q}$, with $a_1^2 + b = 0$. Consequently, $L^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{-b})$. Thus $\mathbb{Q}(\sqrt{\mathcal{D}}) = \mathbb{Q}(\sqrt{-b})$, and so, $\mathcal{D} = -bq^2$ for some $q \in \mathbb{Q}$.

(iv) $a_0 = v$ and $w \neq 0$. From $U = V = 0$, we obtain $3v^2 - 2w^2d + n = 0$ and $3v^2 + w^2d + m = 0$. Hence $v = a_0 = 0$ and $b_0 + \sigma(b_0) + \sigma^2(b_0) = 0$. Thus b_0 is a root of $x^3 + bx - c$, $b = m$, with $a_1^2 + m = 0$. As above, $\mathcal{D} = -bq^2$ for some $q \in \mathbb{Q}$.

So we have shown the following: if H contains a non-trivial element h with $h^2 = 0$, then L is the splitting field of an irreducible cubic $x^3 + bx - c$ where either $b = 0$, or $-\frac{1}{b}\mathcal{D}$ is a square in $\mathbb{Q}$. $\square$

We now prove Proposition 1.

Proposition 1. *Let $L/\mathbb{Q}$ be a Galois extension with group S_3. Let $H = (L\lambda(S_3))^{S_3}$ be the Greither-Pareigis Hopf algebra determined by the regular subgroup $\lambda(S_3)$ of $\mathrm{Perm}(S_3)$ normalized by $\lambda(S_3)$. Then*

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

if and only if L is the splitting field of an irreducible cubic $x^3 + bx - c$ over $\mathbb{Q}$ where either $b = 0$, or $-\frac{1}{b}\mathcal{D}$ is a square in $\mathbb{Q}$.

Proof. Suppose $L/\mathbb{Q}$ is a Galois extension with group S_3, with L the splitting field of an irreducible cubic $x^3 + bx - c$ over $\mathbb{Q}$ where either $b = 0$, or $-\frac{1}{b}\mathcal{D}$ is a square in $\mathbb{Q}$. Let $H = (L\lambda(S_3))^{S_3}$ be the Greither-Pareigis Hopf algebra determined by the regular subgroup $\lambda(S_3) \leq \mathrm{Perm}(S_3)$ normalized by $\lambda(S_3)$.

By [5, Proposition 19], H is left semisimple with decomposition

$$H \cong \mathrm{Mat}_{n_1}(D_1) \times \mathrm{Mat}_{n_2}(D_2) \times \cdots \times \mathrm{Mat}_{n_l}(D_l),$$

where the n_i are integers, and the D_i are division algebras over $\mathbb{Q}$.

We have $L \otimes_{\mathbb{Q}} H \cong LS_3$, thus $\dim_L((L \otimes_{\mathbb{Q}} H)_{ab}) = 2$, by [5, Lemma 8]. Now, by [5, Lemma 7], $\dim_{\mathbb{Q}}((H)_{ab}) = 2$. Thus the decomposition is

$$H \cong Q \times R,$$

where Q is a 2-dimensional commutative $\mathbb{Q}$-algebra, and R is a 4-dimensional non-commutative $\mathbb{Q}$-algebra.

To determine Q, note that

$$H_{ab} = ((L\lambda(S_3))^{S_3})_{ab} = ((L\lambda(S_3))_{ab})^{S_3} \cong (LC_2)^{S_3} = \mathbb{Q}C_2,$$

since $[S_3, S_3]$ is a normal subgroup of S_3, that is, $[S_3, S_3]^{S_3} = [S_3, S_3]$. Thus, $Q = \mathbb{Q} \times \mathbb{Q}$, so that

$$H \cong \mathbb{Q} \times \mathbb{Q} \times R.$$

So it remains to determine R. To this end, note that one of following cases holds:

(1) $R = S \times T$, where S, T are division algebras with $\dim_{\mathbb{Q}}(S) = \dim_{\mathbb{Q}}(T) = 2$,

(2) $R = S$, where S is a division algebra with $\dim_{\mathbb{Q}}(S) = 4$,

(3) $R = \mathrm{Mat}_2(\mathbb{Q})$.

Assume $b = 0$. Then L is the splitting field of the irreducible cubic $x^3 - c$ over $\mathbb{Q}$.

Let ω denote a primitive 3rd root of unity and let $b_0 = \sqrt[3]{c}$. Then $L = \mathbb{Q}(b_0, \omega)$, and L is Galois with group $S_3 = \langle \sigma, \tau \rangle$ with $\sigma^3 = \tau^2 = 1$, $\tau\sigma = \sigma^2\tau$. The Galois action is given as $\sigma(b_0) = \omega b_0$, $\sigma(\omega) = \omega$, $\tau(b_0) = b_0$, $\tau(\omega) = \omega^2$.

Let $a_0 = a_1 = 0$. As one check, H contains the non-zero nilpotent element

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

of index 2.

Next, assume that $-\frac{1}{b}\mathcal{D}$ is a square in $\mathbb{Q}$. (Necessarily, $b \neq 0$ and b is not a square in $\mathbb{Q}$.)

Let $a_0 = 0$, $a_1 = \sqrt{-b}$. By [2, Theorem 2.6], $L = \mathbb{Q}(b_0, \sqrt{\mathcal{D}})$, where b_0 is a root of $x^3 + bx - c$. Thus $L = \mathbb{Q}(b_0, \sqrt{-b})$.

Now, H contains the non-zero nilpotent element

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

of index 2. Indeed, as one can check,
$U = V = W = X = Y = Z = 0$, and so $h^2 = 0$, $h \neq 0$.

Thus, in either case ($b = 0$ or $-\frac{1}{b}\mathcal{D}$ is a square in $\mathbb{Q}$), H contains a non-trivial nilpotent element of index 2, and this shows that cases (1) and (2) above are impossible: For if $h = (c_1, c_2, c_3, c_4)$ for $c_1, c_2 \in \mathbb{Q}$, $c_3 \in S$, $c_4 \in T$, as in (1), then

$$0 = h^2 = (c_1^2, c_2^2, c_3^2, c_4^2) = (0, 0, 0, 0),$$

thus $h = 0$. A similar agrument shows that (2) cannot happen either. Thus

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

For the converse of Proposition 1, suppose that $L/\mathbb{Q}$ is Galois with group S_3 with $H = (L\lambda(S_3))^{S_3}$ and

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

Then H contains a non-trivial nilpotent element of index 2, namely, the element in H corresponding to

$$\left(0, 0, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)$$

in $\mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q})$. Thus by Lemma 2, L is the splitting field of an irreducible cubic $x^3 + bx - c$ where either $b = 0$, or $-\frac{1}{b}\mathcal{D}$ is a square in $\mathbb{Q}$. □

3. A Class of Splitting Fields

In this section we construct a collection of irreducible cubics $x^3 + bx - c$ in which $-\frac{1}{b}\mathcal{D}$ is a square in $\mathbb{Q}$.

Let $p(x) = x^3 + bx - b^2$, $b \in \mathbb{Q}$. Then $\mathcal{D} = -4b^3 - 27b^4$. We require that

$$\frac{-4b^3 - 27b^4}{-b} = q^2$$

for some $q \in \mathbb{Q}$. Thus $b^2(4 + 27b) = q^2$, and so, $4 + 27b = (q/b)^2$.

We seek z so that $z^2 = 4 + 27b$. Now, $b = (z^2 - 4)/27$, hence $z^2 \equiv 4 \bmod 27$, that is, we want 4 to be a quadratic residue mod 27.
Certainly, this happens if $z = 25$. Now, $b = (25^2 - 4)/27 = 23$, and $q^2 = (23)^2(4 + 27 \cdot 23) = 330625$, so that $q = 575$.

Now, put

$$p(x) = x^3 + 23x - 529.$$

As one can check, $p(x)$ is irreducible over $\mathbb{Q}$ with

$$-\frac{1}{b}\mathcal{D} = \frac{-4 \cdot 23^3 - 27 \cdot (-529)^2}{-23} = 330625 = (575)^2.$$

The splitting field of $p(x)$ is $L = \mathbb{Q}(b_0, \sqrt{-23})$, where b_0 is a root of $p(x)$. Moreover, $H = (L\lambda(S_3))^{S_3}$ contains the non-trivial nilpotent index 2 element

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

hence

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

as $\mathbb{Q}$-algebras.

4. An Application

Proposition 3. *Suppose that $L/\mathbb{Q}$ is a Galois extension with group S_3. Then $\mathbb{Q}S_3$ and $H = (L\lambda(S_3))^{S_3}$ have the same number of Wedderburn-Artin components.*

Proof. See [3, Corollary 4.9].

Now, we have already established that $\mathbb{Q}S_3 \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q})$, and so, H must have 3 Wedderburn-Artin components, two of which are copies of $\mathbb{Q}$. Thus

$$H \cong \mathbb{Q} \times \mathbb{Q} \times R$$

where either $R = \mathrm{Mat}_2(\mathbb{Q})$, or R is some 4-dimensional non-commutative division algebra over $\mathbb{Q}$.

But if $L/\mathbb{Q}$ is the splitting field of a cubic other than one of the form described in Proposition 1 (for instance $x^3 - 4x + 1$), then

$$H = (L\lambda(S_3))^{S_3} \cong \mathbb{Q} \times \mathbb{Q} \times R,$$

where R is some 4-dimensional division algebra over $\mathbb{Q}$.

- L. N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, AMS: Mathematical Surveys and Monographs, **80**, 2000.
- K. Conrad, Galois groups of cubics and quartics (not in characteristic 2), `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf`
- A. Koch, T. Kohl, P. Truman, R. Underwood, *On the Structure of Hopf algebras acting on separable extensions*, preprint, date: April 6, 2017.
- J. Rotman, *Advanced Modern Algebra*, Pearson, New Jersey, 2002.
- R. Underwood, The Structure of Greither-Pareigis Hopf Algebras, presented at Omaha 2017, University of Nebraska-Omaha, NE, May, 2017.