The Structure of Greither-Pareigis Hopf Algebras

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

AUBURN
MONTGOMERY

June 6, 2017

This is joint work with:

Alan Koch
Agnes Scott College

Timothy Kohl
Boston University

Paul Truman
Keele University

with an acknowledgement to **Cornelius Greither**.

1.1 Semisimplicity. Let R be any ring. Then R is **left artinian** if it has the DCC for left ideals, that is, for each decreasing sequence of left ideals

$$L_1 \supseteq L_2 \supseteq L_3 \supseteq \cdots$$

there exists an integer $N \geq 1$ for which

$$L_N = L_{N+1} = L_{N+2} = \cdots$$

A left ideal L of R is **maximal** if $L \neq R$ and there is no left ideal J with $L \subset J \subset R$.

The **Jacobson radical** $J(R)$ of a ring R is the intersection of the maximal left ideals of R.

A left ideal L of R is **minimal** if $L \neq 0$ and there is no left ideal J with $0 \subset J \subset L$.

A ring R is **left semisimple** if it is a direct sum of minimal left ideals.

Proposition 1. *A ring R is left semisimple if and only if every left ideal of R is a direct summand as a left R-module.*

Proof. See [12, Theorem 8.42]. □

Proposition 2 (Maschke). *Let G be a finite group and let K be a field whose characteristic does not divide $|G|$. Then the group ring KG is a left semisimple ring.*

Proof. Use Proposition 1. □

Proposition 3. *A ring R is left semisimple if and only if it is left artinian and $J(R) = 0$.*

Proof. See [12, Theorem 8.45]. □

Corollary 4. *Let G be a finite group and let K be a field whose characteristic does not divide $|G|$. Then $J(KG) = 0$.*

Proposition 5. (Wedderburn-Artin) *A ring R is left semisimple if and only if it is isomorphic to the direct product of matrix rings over division rings.*

Proof. See [12, Theorem 8.56]. □

1.2 Commutator Ideals. Let K be a field, let A be a finite dimensional K-algebra. Let $[A, A]$ denote the ideal of A generated by the set of commutators $xy - yx$ for $x, y \in A$. The **abelian part** of A is the quotient K-algebra $A_{ab} = A/[A, A]$.

For example, $[\mathrm{Mat}_n(K), \mathrm{Mat}_n(K)] = \mathrm{Mat}_n(K)$, for $n \geq 2$, hence $\mathrm{Mat}_n(K)_{ab} = 0$, for $n \geq 2$.

Lemma 6. Let A, B be K-algebras. Then $(A \times B)_{ab} \cong A_{ab} \times B_{ab}$.

Proof. One has $(A \times B)_{ab} = (A \times B)/[A \times B, A \times B] =$ $(A \times B)/([A, A] \times [B, B]) \cong A_{ab} \times B_{ab}$. $\square$

Lemma 7. Let L/K be a finite field extension. Then $L \otimes_K A_{ab} \cong (L \otimes_K A)_{ab}$.

Proof. Since L is a flat K-module, the short exact sequence $0 \to [A, A] \to A \to A_{ab} \to 0$ yields the short exact sequence $0 \to L \otimes_K [A, A] \to L \otimes_K A \to L \otimes_K A_{ab} \to 0$. We have $L \otimes_K [A, A] = [L \otimes_K A, L \otimes_K A]$. It follows that

$$L \otimes_K A_{ab} \cong (L \otimes_K A)/(L \otimes_K [A, A])$$

$$= (L \otimes_K A)/[L \otimes_K A, L \otimes_K A] = (L \otimes_K A)_{ab}.$$

□

Lemma 8. Let G be any finite group, and let KG be the group ring over K. Let $G^{ab} = G/[G, G]$, where $[G, G]$ is the commutator subgroup of G. Then $(KG)_{ab} \cong KG^{ab}$.

Proof. One has $(KG)_{ab} = KG/[KG, KG] = KG/K[G, G] \cong KG^{ab}$.
□

2.1 The Basics. Let L/K be a Galois extension with group G. Let H be a finite dimensional Hopf algebra over K.

Then L is an H-**Galois extension** of K if L is an H-module algebra and the K-linear map

$$j : L \otimes_K H \to \mathrm{End}_K(L),$$

given as $j(a \otimes h)(x) = ah(x)$ for $a, x \in L$, $h \in H$, is bijective.

If L is an H-Galois extension for some H, then L is said to have a **Hopf-Galois structure** via H.

Example 9 (Classical Hopf-Galois Structure). *Let L/K be a Galois extension with group G. Let KG be the group ring K-Hopf algebra. Then L is a KG-Galois extension of K; L admits the classical Hopf-Galois structure via KG.*

But are there other Hopf-Galois structures on L/K?

Let $\mathrm{Perm}(G)$ denote the permutation group of G. Let $\lambda(G)$ denote the image of the **left regular representation**

$$\lambda : G \to \mathrm{Perm}(G),\ \lambda(g)(g') = gg'$$

of G in $\mathrm{Perm}(G)$. Then $\lambda(G) \le \mathrm{Perm}(G)$. Let $\rho(G)$ denote the image of the **right regular representation**

$$\rho : G \to \mathrm{Perm}(G),\ \lambda(g)(g') = g'g^{-1}$$

of G in $\mathrm{Perm}(G)$. Then $\rho(G) \le \mathrm{Perm}(G)$.

A subgroup $N \le \mathrm{Perm}(G)$ is **normalized** by $\lambda(G)$ if $\lambda(G)$ is in the normalizer of N in $\mathrm{Perm}(G)$.

A subgroup $N \le \mathrm{Perm}(G)$ is **regular** if $|N| = |G|$ and

$$\mathrm{Stab}_N(g) = \{l \in N :\ l(g) = g\} = 1,\ \forall g \in G.$$

Proposition 10 (Greither-Pareigis [8]). *Let L/K be a Galois extension with group G with $n = [L : K]$. There is a one-to-one correspondence between Hopf-Galois structures on L/K and regular subgroups of $\mathrm{Perm}(G)$ that are normalized by $\lambda(G)$.*

One direction of this result works as follows.

Let N be a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$. Assume that G acts on LN by as the Galois group on L, and by conjugation via $\lambda(G)$ on N. Denote this action by "$\cdot$".

Let

$$H = (LN)^G = \{x \in LN : \ g \cdot x = x, \forall g \in G\}.$$

Then H is an n-dimensional K-Hopf algebra and L has a **Greither-Pareigis Hopf Galois structure via** H, hereafter referred to as a **Hopf Galois structure via** H**.**

One consequence is that

$$H \otimes_K L \cong KN \otimes_K L \cong LN,$$

that is, H is an L-**form** of KN.

So to find Hopf Galois structures on L/K we look for regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$.

In this way the search for Hopf Galois structures has been reduced to a problem in group theory.

Example 11. *It is known that* $\rho(G)$ *is a regular subgroup of* $\mathrm{Perm}(G)$ *normalized by* $\lambda(G)$. *In this case*

$$H = (L\rho(G))^G = K\rho(G) \cong KG,$$

and the corresponding Hopf-Galois structure on L *is the classical Hopf Galois structure.*

Example 12. *It is known that* $\lambda(G)$ *is a regular subgroup of* $\mathrm{Perm}(G)$ *normalized by* $\lambda(G)$. *Assume that* G *is non-abelian, and let*

$$H = (L\lambda(G))^G.$$

Then L/K *has a non-classical Hopf-Galois structure via* H.

3. Counting Results

Let L/K be Galois with group G. We review various results that count the number of Hopf Galois structures on L/K. It is enough to count the number of regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$.

3.1 The Case $|G| = p$, p prime. In this case, $G = C_p$. If N is any regular subgroup of $\mathrm{Perm}(G)$, then $|N| = |G| = p$, and so $N \cong C_p$.

This case is settled by a result of Childs [5].

Proposition 13 (Childs). *Let L/K be a Galois extension with group C_p. Then L/K has a unique Hopf Galois structure, namely the classical Hopf Galois structure.*

In other words, there is exactly one regular subgroup $N = \rho(C_p) \leq \mathrm{Perm}(C_p)$ normalized by $\lambda(C_p) = \rho(C_p)$.

3.2 The Case $|G| = p^2$. In this case, G is abelian and either $G = C_{p^2}$ or $G = C_p \times C_p$.

This case is handled by a result of Byott [3].

Proposition 14 (Byott). *If $G = C_{p^2}$, then there are p Hopf Galois structures on L/K. If $G = C_p \times C_p$, then there are p^2 Hopf Galois structures on L/K.*

In other words, if $G = C_{p^2}$, there are exactly p regular subgroups $N \leq \mathrm{Perm}(C_{p^2})$ normalized by $\lambda(C_{p^2})$, and if $G = C_p \times C_p$, there are exactly p^2 regular subgroups $N \leq \mathrm{Perm}(C_p \times C_p)$ normalized by $\lambda(C_p \times C_p)$.

3.3 The Case $|G| = pq$, $p > q$. If $p \not\equiv 1 \bmod q$, then $G = C_{pq}$, and if $p \equiv 1 \bmod q$, then either $G = C_{pq}$, or $G = C_p \rtimes C_q$.

Proposition 15. *If $p \not\equiv 1 \bmod q$, then L/K has exactly one Hopf Galois structure, namely the classical Hopf Galois structure.*

Proof. Note that $\gcd(pq, \phi(pq)) = 1$, and so, pq is a Burnside number. Thus by Byott [2], L/K has a unique Hopf Galois structure. □

Proposition 16 (Byott). *Assume $p \equiv 1 \bmod q$. If $G = C_{pq}$, then there are $2q - 1$ Hopf Galois structures on L/K. If $G = C_p \rtimes C_q$, then there are $2 + p(2q - 3)$ Hopf Galois structures on L/K.*

Proof. See [4], [11, Theorem 4.1]. □

4. The Structure of $H = (LN)^G$.

Let N be a regular subgroup of $\mathrm{Perm}(G)$ nomalized by $\lambda(G)$. Let $H = (LN)^G$ be the K-Hopf algebra acting on the Hopf-Galois extension L/K (H is a Greither-Pareigis Hopf algebra). We ultimately want to study the structure of H as both a K-algebra and a K-Hopf algebra.

To this end, we state the following results.

Proposition 17. *Let $\mathcal{G}(H)$ denote the set of grouplike elements in H. Then $\mathcal{G}(H) = N \cap \rho(G)$.*

Proof. See [10, Corollary 1.3]. □

Let N, N' be regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$. An isomorphism of groups $\phi : N \to N'$ is $\lambda(G)$-**invariant** if

$$\phi(x \cdot n) = x \cdot \phi(n)$$

for all $x \in \lambda(G)$, $n \in N$.

Proposition 18. *Suppose $\phi : N \to N'$ is a $\lambda(G)$-invariant isomorphism of groups. Then $(LN)^G \cong (LN')^G$ as K-Hopf algebras.*

Proof. By linearity, ϕ extends to an L-Hopf algebra isomorphism (also denoted by ϕ), $\phi : LN \to LN'$. Let $\sum r_i n_i \in (LN)^G$. Then for all $x \in G$, $\phi(\sum r_i n_i) = \phi(x \cdot \sum r_i n_i) = x \cdot \phi(\sum r_i n_i)$, and so, ϕ restricts to an injection $\phi : (LN)^G \to (LN')^G$. Since $\dim_K((LN)^G) = \dim_K((LN')^G)$, ϕ is a bijection, and hence an isomorphism of K-Hopf algebras. □

Proposition 19. *Suppose L/K is an H-Galois extension for some finite dimensional K-Hopf algebra $H = (LN)^G$ arising from the Greither-Pareigis construction of Proposition 10. Assume $char(K) = 0$. Then H is left semisimple.*

Proof. We know that H is an L-form of KN, that is, $H \otimes_K L \cong KN \otimes_K L = LN$. Since LN is left semisimple, $J(H \otimes_K L) = 0$. By [1, Theorem 1], $J(H) \otimes_K L = 0$. Since L is faithfully flat over K, the map $H \to H \otimes_K L \cong LN$, given as $h \mapsto h \otimes 1$ is an injection. Consequently, $J(H)$ injects into $J(H) \otimes_K L = 0$, thus $J(H) = 0$, and so, H is left semisimple by Proposition 3. □

Recall that, if H is a Greither-Pareigis Hopf algebra, then

$$H \otimes_K L \cong KN \otimes_K L \cong LN,$$

that is, H is an L-**form** of KN.

For $N \cong C_4$, $N \cong C_6$, Haggenmüller and Pareigis [9, Theorem 6] have characterized all of the Hopf algebra forms of KN.

Proposition 20 (Haggenmüller-Pareigis). *Let c, s be indeterminates. The Hopf algebra forms of KC_4 are*

$$H = K[c, s]/(s^2 - asc - bc^2 + u, c(ac - 2s)).$$

The Hopf algebra forms of KC_6 are

$$H = K[c, s]/(s^2 - asc - bc^2 + u, (c-2)(c-1)(c+1)(c+2),$$
$$(c-1)(c+1)(sc - 2a)).$$

In both cases, $a, b \in K$, $u \in K^\times$, with $a^2 + 4b = u$. Moreover, these forms are split by $K[x]/(x^2 - ax - b)$.

Proof. See [9]. □

5. Examples: $|G| = n$, $2 \leq n \leq 6$

In what follows, we fix the base field $K = \mathbb{Q}$. For various Galois extensions $L/\mathbb{Q}$ with group G, $2 \leq |G| \leq 6$, we compute the Greither-Pareigis Hopf algebras $H = (LN)^G$, as $\mathbb{Q}$-algebras, and as $\mathbb{Q}$-Hopf algebras.

By Proposition 19, all H are left semisimple.

5.1 Case $|G| = 2$. In this case $G = C_2$, and $L/\mathbb{Q}$ is a quadratic extension. By Proposition 13, $L/\mathbb{Q}$ has only the classical Hopf Galois structure via $H = \mathbb{Q}C_2$. The Wedderburn-Artin decomposition is

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

5.2 Case $|G| = 3$. In this case $G = C_3$, and $L/\mathbb{Q}$ is a cubic extension. By Proposition 13, $L/\mathbb{Q}$ has only the classical Hopf Galois structure via $H = \mathbb{Q}C_3$. The Wedderburn-Artin decomposition is

$$H \cong \mathbb{Q} \times \mathbb{Q}(\zeta_3),$$

where ζ_3 is a primitive 3rd root of unity.

One can construct a collection of irreducible cubics whose Galois groups are C_3. For any integer m, let $b = m^2 + m + 7$, and let $p(x) = x^3 - bx + b$. Then $p(x)$ is irreducible over $\mathbb{Q}$ and the Galois group of the splitting field $L/\mathbb{Q}$ is C_3. See [6, Corollary 2.5].

5.3 Case $|G| = 4$. This is the first case where it gets interesting. If $G = C_4$, then by Proposition 14, there are 2 Hopf Galois structures on $L/\mathbb{Q}$, and if $G = C_2 \times C_2$, there are 4 Hopf Galois structures on $L/\mathbb{Q}$.

We only consider the case $G = C_2 \times C_2$, here. Specifically, we let $L/\mathbb{Q}$ be the splitting field of the irreducible quartic $p(x) = x^4 - 10x^2 + 1$, that is, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

$L/\mathbb{Q}$ is Galois with group $C_2 \times C_2 = \{1, \sigma, \tau, \tau\sigma\}$ with Galois action

$$\sigma(\sqrt{2} + \sqrt{3}) = \sqrt{2} - \sqrt{3}, \quad \tau(\sqrt{2} + \sqrt{3}) = -\sqrt{2} + \sqrt{3}.$$

Of the corresponding 4 regular subgroups of $\mathrm{Perm}(C_2 \times C_2)$ normalized by $\lambda(C_2 \times C_2)$, one $M_1 = \rho(C_2 \times C_2) = \lambda(C_2 \times C_2)$ is isomorphic to $C_2 \times C_2$, while three, N_1, N_2, N_3, are isomorphic to C_4.

Explicitly, with $1 := 1$, $2 := \sigma$, $3 := \tau$, $4 := \tau\sigma$,

$$M_1 = \lambda(C_2 \times C_2) = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

$$N_1 = \{(1), (1,3,2,4), (1,2)(3,4), (1,4,2,3)\}$$

$$N_2 = \{(1), (1,4,3,2), (1,3)(2,4), (1,2,3,4)\}$$

$$N_3 = \{(1), (1,2,4,3), (1,4)(2,3), (1,3,4,2)\}.$$

Now, M_1 corresponds to the classical Hopf Galois structure on $L/\mathbb{Q}$, hence $A_1 = (LM_1)^{C_2 \times C_2} \cong \mathbb{Q}(C_2 \times C_2)$, and the Wedderburn-Artin decomposition is

$$A_1 \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}.$$

We next treat the N_i. Let $B_1 = (LN_1)^{C_2 \times C_2}$.

Proposition 21. *Let c, s be indeterminates. Then $B_1 = \mathbb{Q}[c, s]/(s^2 - 2c^2 + 8, -2sc)$.*

Proof. As one can check

$$\{x \in \lambda(C_2 \times C_2) : \; x \cdot n = n, \forall n \in N_1\} = \{(1), (1,2)(3,4)\} = \{1, \sigma\}.$$

There is an induced action of $(C_2 \times C_2)/\{1, \sigma\}$ on LN_1. By the fundamental theorem of Galois theory, $(C_2 \times C_2)/\{1, \sigma\} \cong C_2$ is the group of the Galois extension $E_1/\mathbb{Q}$, $E_1 = \mathbb{Q}(\sqrt{2})$ (the fixed field of $\{1, \sigma\}$ is E_1). And so, there is an induced action of $(C_2 \times C_2)/\{1, \sigma\}$ on $E_1 N_1$.

Now, $(C_2 \times C_2)/\{1, \sigma\} \cong C_2$ can be viewed as the group of automorphisms of $N_1 \cong C_4$. Since L is a B_1-Galois extension of $\mathbb{Q}$, E_1 is a C_2-Galois extension of $\mathbb{Q}$ in the sense of [9, page 130]. We have

$$B_1 = (LN_1)^{C_2 \times C_2} = (E_1 C_4)^{C_2},$$

and so, by [9, Theorem 5], B_1 is a E_1-(Hopf algebra) form of $\mathbb{Q}C_4$. Since $E_1 = \mathbb{Q}[x]/(x^2 - 2)$, Proposition 20 applies to yield $B_1 = \mathbb{Q}[c, s]/(s^2 - 2c^2 + 8, -2sc)$. □

We want the Wedderburn-Artin decomposition of $B_1 = \mathbb{Q}[c,s]/(s^2 - 2c^2 + 8, -2sc)$. In B_1, $c^3 = 4c$, and so, there are three mutually orthogonal idempotents:

$$\frac{1}{4}c + \frac{1}{8}c^2, \quad -\frac{1}{4}c + \frac{1}{8}c^2, \quad 1 - \frac{1}{4}c^2.$$

Moreover, since $s^2 - 2c^2 + 8 = 0$ implies that

$$\left(\frac{s}{2}\right)^2 = -2\left(1 - \frac{1}{4}c^2\right),$$

$$B_1 \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt{-2}).$$

Next, let

$$B_2 = (LN_2)^{C_2 \times C_2}, \quad B_3 = (LN_3)^{C_2 \times C_2}.$$

In a similar manner, one obtains

$$B_1 = \mathbb{Q}[c, s]/(s^2 - 3c^2 + 12, -2sc), \quad B_2 = \mathbb{Q}[c, s]/(s^2 - 6c^2 + 24, -2sc),$$

and

$$B_2 \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt{-3}).$$

$$B_3 \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt{-6}).$$

5.4 Case $|G| = 5$. In this case $G = C_5$, and $L/\mathbb{Q}$ is a quintic extension. By Proposition 13, $L/\mathbb{Q}$ has only the classical Hopf Galois structure via $H = \mathbb{Q}C_5$. The Wedderburn-Artin decomposition is

$$H \cong \mathbb{Q} \times \mathbb{Q}(\zeta_5),$$

where ζ_5 is a primitive 5rd root of unity.

For example, let $p(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$. Then $p(x)$ is the minimal polynomial for $\zeta_{11} + \zeta_{11}^{-1}$. The splitting field $L/\mathbb{Q}$ is Galois with group C_5.

5.5 Case $|G| = 6$. Note that $6 = 3 \cdot 2$ with $3 \equiv 1 \bmod 2$, and so, by Proposition 16, there are 3 Hopf Galois structures on $L/\mathbb{Q}$ if $G = C_6$, and there are 5 Hopf Galois structures on $L/\mathbb{Q}$ if $G = C_3 \rtimes C_2 = S_3$.

We only consider the case $G = S_3$, here. Specifically, let L be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Let ω denote a primitive 3rd root of unity and let $\alpha = \sqrt[3]{2}$.

Then $L = \mathbb{Q}(\alpha, \omega)$ 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 $\sigma(\alpha) = \omega\alpha$, $\sigma(\omega) = \omega$, $\tau(\alpha) = \alpha$, $\tau(\omega) = \omega^2$.

By Proposition 16, there are 5 Hopf Galois structures on $L/\mathbb{Q}$. But since the corresponding regular subgroups $N \leq \mathrm{Perm}(S_3)$ satisfy $|N| = |S_3| = 6$, we conclude that some of the N may be isomorphic to S_3, and some may be isomorphic to C_6.

In fact, by a result of Kohl [11], of the 5, there are 2 regular subgroups isomorphic to S_3, namely, $M_1 = \rho(S_3)$ and $M_2 = \lambda(S_3)$, and 3 regular subgroups isomorphic to C_6, namely, N_1, N_2 and N_3.

We compute the structure of the corresponding Greither-Pareigis Hopf algebras in turn.

Proposition 22. *Let* $A_1 = (LM_1)^{S_3} = (L\rho(S_3))^{S_3} \cong \mathbb{Q}S_3$*. Then* A_1 *is left semisimple as a ring. Its Wedderburn-Artin decomposition is*

$$A_1 \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

Proof. By Proposition 2, A_1 is left semisimple with decomposition

$$A_1 \cong \mathrm{Mat}_{n_1}(D_1) \times \mathrm{Mat}_{n_2}(D_2) \times \cdots \times \mathrm{Mat}_{n_l}(D_l),$$

for integers n_i and division rings D_i, $1 \leq i \leq l$.

By Lemma 8, $(A_1)_{ab} \cong \mathbb{Q}C_2$ since $S_3/[S_3, S_3] \cong C_2$.

Hence $(A_1)_{ab} \cong \mathbb{Q} \times \mathbb{Q}$, and so,

$$A_2 \cong \mathbb{Q} \times \mathbb{Q} \times R,$$

where $\dim_{\mathbb{Q}}(R) = 4$ and one of the following cases must hold:

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

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

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

However, as one check, $\mathbb{Q}S_3$ contains the non-zero nilpotent element $a = \sigma - \sigma^2 + \tau - \tau\sigma$, $a^2 = 0$.

Thus the first two cases are impossible, for if $a = (a_1, a_2, a_3, a_4)$ with $a_1, a_2 \in \mathbb{Q}$, $a_3 \in S$, $a_4 \in T$, as in 1), then $0 = a^2 = (a_1^2, a_2^2, a_3^2, a_4^2) = (0, 0, 0, 0)$, thus $a = 0$.

A similar agrument shows that 2) cannot happen either. Thus

$$A_1 \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

□

Proposition 23. *Let* $A_2 = (LM_2)^{S_3} = (L\lambda(S_3))^{S_3}$*. Then* A_2 *is left semisimple as a ring. Its Wedderburn-Artin decomposition is*

$$A_2 \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

Proof. By Proposition 19, A_2 is left semisimple with decomposition

$$A_2 \cong \mathrm{Mat}_{n_1}(D_1) \times \mathrm{Mat}_{n_2}(D_2) \times \cdots \times \mathrm{Mat}_{n_l}(D_l),$$

for n_i and D_i.

We have $L \otimes_{\mathbb{Q}} A_2 \cong LS_3$, thus $\dim_L((L \otimes_{\mathbb{Q}} A_2)_{ab}) = 2$, by Lemma 8.

Now, by Lemma 7, $\dim_{\mathbb{Q}}((A_2)_{ab}) = 2$. Thus the decomposition is

$$A_2 \cong Q \times R,$$

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

$$(A_2)_{ab} = ((LM_2)^{S_3})_{ab} = ((LM_2)_{ab})^{S_3} \cong (LC_2)^{S_3} = \mathbb{Q}C_2,$$

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

$$A_2 \cong \mathbb{Q} \times \mathbb{Q} \times R.$$

So it remains to determine R.

To this end, note that either case 1), 2), or 3) holds exactly as in the proof of Proposition 22. But since A_2 contains the non-trivial nilpotent element $b = \alpha\tau + \alpha\omega\tau\sigma + \alpha\omega^2\tau\sigma^2$, $b^2 = 0$, the only possibility is case 3): $R = \mathrm{Mat}_2(\mathbb{Q})$. Thus

$$A_2 \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

□

Proposition 24. A_1 and A_2 are isomorphic as $\mathbb{Q}$-algebras, but not as $\mathbb{Q}$-Hopf algebras.

As shown above, both A_1 and A_2 have the same Wedderburn-Artin decomposition, thus $A_1 \cong A_2$ as $\mathbb{Q}$-algebras.

On the other hand, by Proposition 17,
$\mathcal{G}(A_1) = M_1 \cap \rho(S_3) = \rho(S_3)$, while $\mathcal{G}(A_2) = M_2 \cap \rho(S_3) = \{1\}$.
Thus $A_1 \not\cong A_2$ as Hopf algebras. □

Proposition 25. *Let $B_i = (LN_i)^{S_3}$, for $i = 1, 2, 3$. Then B_i, $i = 1, 2, 3$, are in the same isomorphism class as $\mathbb{Q}$-Hopf algebras, and hence as $\mathbb{Q}$-algebras.*

Proof. We show there exists a $\lambda(S_3)$-invariant isomorphism between any two B_i, and then apply Proposition 18.

To this end, with $1 := 1$, $2 := \sigma$, $3 := \sigma^2$, $4 := \tau$, $5 := \tau\sigma$, $6 := \tau\sigma^2$, we have

$$\lambda(S_3) = \langle (1, 2, 3)(4, 6, 5), (1, 4)(2, 5)(3, 6) \rangle ,$$

and

$$N_1 = \langle (1, 6, 2, 5, 3, 4) \rangle ,$$

$$N_2 = \langle (1, 4, 2, 6, 3, 5) \rangle ,$$

$$N_3 = \langle (1, 5, 2, 4, 3, 6) \rangle .$$

For each $i = 1, 2, 3$,

$$\lambda(S_3) \cap N_i = \langle (1,2,3)(4,6,5) \rangle ,$$

is the unique 3-Sylow subgroup of both $\lambda(S_3)$ and N_i.

Now,

$$N_1 = \langle (1,2,3)(4,6,5)(1,5)(2,4)(3,6) \rangle ,$$
$$N_2 = \langle (1,2,3)(4,6,5)(1,6)(2,5)(3,4) \rangle ,$$
$$N_3 = \langle (1,2,3)(4,6,5)(1,4)(2,6)(3,5) \rangle .$$

Define a map $\phi : N_1 \to N_2$ by the rule

$$(1,2,3)(4,6,5)(1,5)(2,4)(3,6) \mapsto (1,2,3)(4,6,5)(1,6)(2,5)(3,4).$$

Then as one can check ϕ is a $\lambda(S_3)$-invariant isomorphism. In a similar manner, there is a $\lambda(S_3)$-invariant isomorphism between N_1 and N_3. □

So we need only to consider B_1.

Proposition 26. *Let c, s be indeterminates. Then $B_1 = \mathbb{Q}[c,s]/I$, with*

$$I = (s^2+sc+c^2-3, (c-2)(c-1)(c+1)(c+2), (c-1)(c+1)(sc+2)).$$

Proof. As one can check $\{x \in \lambda(S_3) : \ x \cdot n = n, \forall n \in N_1\}$ is precisely the 3-Sylow subgroup $\langle (1,2,3)(4,6,5) \rangle$ which we can identify with the commutator subgroup $[S_3, S_3]$.

There is an induced action of $S_3/[S_3, S_3]$ on LN_1. By the fundamental theorem of Galois theory, $S_3/[S_3, S_3] \cong C_2$ is the group of the Galois extension $K = \mathbb{Q}(\omega)/\mathbb{Q}$ (the fixed field of $[S_3, S_3]$ is $\mathbb{Q}(\omega)$). And so, there is an induced action of $S_3/[S_3, S_3]$ on KN_1.

Now, $S_3/[S_3, S_3] \cong C_2$ can be viewed as the group of automorphisms of $N_1 \cong C_6$. Since L is a B_1-Galois extension of $\mathbb{Q}$, K is a C_2-Galois extension of $\mathbb{Q}$ in the sense of [9, page 130]. We have

$$B_1 = (LN_1)^{S_3} = (KC_6)^{C_2},$$

and so, by [9, Theorem 5], B_1 is a K-(Hopf algebra) form of $\mathbb{Q}C_6$.

Since $K = \mathbb{Q}[x]/(x^2 + x + 1)$, Proposition 20 applies to yield $B_1 = \mathbb{Q}[c, s]/I$, with

$$I = (s^2+sc+c^2-3, (c-2)(c-1)(c+1)(c+2), (c-1)(c+1)(sc+2)).$$

□

Proposition 27. *Let $B_1 = (LN_1)^{S_3}$. Then B_1 is left semisimple as a ring. Its Wedderburn-Artin decomposition is*

$$B_1 \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}.$$

Proof. Observe that B_1 is left semisimple by Proposition 19.

The ideal I determines an affine variety in $\mathbb{Q}^2$ consisting of exactly six points:

$$P_1 = (-2, 1), P_2 = (-1, 2), P_3 = (1, 1),$$

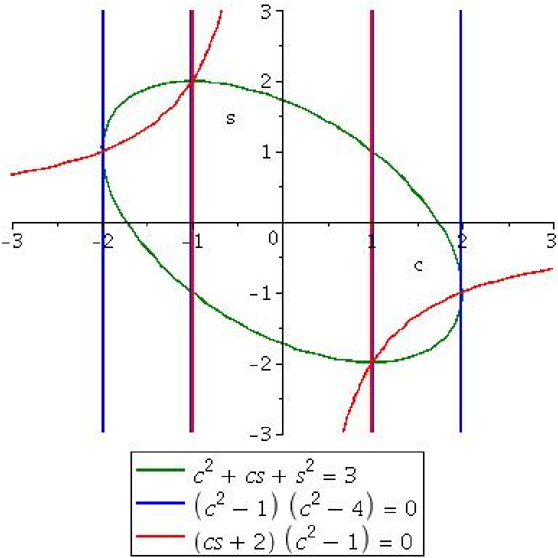
$$P_4 = (2, -1), P_5 = (1, -2), P_6 = (-1, -1),$$

This is the set of common zeros of the polynomials in I.

The graphs of the equations

$$\begin{aligned} s^2 + sc + c^2 - 3 &= 0 \\ (c-2)(c-1)(c+1)(c+2) &= 0 \\ (c-1)(c+1)(sc+2) &= 0 \end{aligned}$$

are:


s
c
-3
-2
-1
0
1
2
3
$c^2 + cs + s^2 = 3$
$(c^2 - 1)(c^2 - 4) = 0$
$(cs + 2)(c^2 - 1) = 0$

We construct a collection of six mutually orthogonal idempotents in B_1. Consequently, B_1 has the claimed form.

With respect to the set of monomials $\{1, c, c^2, s, sc, sc^2\}$, assume that

$$e_j = a_{1,j} + a_{2,j}c + a_{3,j}c^2 + a_{4,j}s + a_{5,j}sc + a_{6,j}sc^2,$$

$a_{i,j} \in \mathbb{Q}$, is an idempotent for $1 \leq j \leq 6$.

There exist evaluation homomorphisms $\Psi_{P_i} : B_1 \to \mathbb{Q}$, $1 \leq i \leq 6$. We have $\Psi_{P_i}(e_j) = \delta_{i,j}$ for $1 \leq i, j \leq 6$.

This yields the linear system $Ay_j = b_j$, where

$$A = \begin{pmatrix} 1 & -2 & 4 & 1 & -2 & 4 \\ 1 & -1 & 1 & 2 & -2 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & -1 & -2 & -4 \\ 1 & 1 & 1 & -2 & -2 & -2 \\ 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}, \quad y_j = \begin{pmatrix} a_{1,j} \\ a_{2,j} \\ a_{3,j} \\ a_{4,j} \\ a_{5,j} \\ a_{6,j} \end{pmatrix},$$

and b_j is the jth standard basis element for $\mathbb{Q}^6$ (in column form).

Using GAP [7], one computes $y_j = A^{-1} b_j$, where

$$A^{-1} = \begin{pmatrix} -1/6 & 1/3 & 1/3 & -1/6 & 1/3 & 1/3 \\ 0 & -1/6 & 1/3 & 0 & 1/6 & -1/3 \\ 1/6 & -1/6 & 0 & 1/6 & -1/6 & 0 \\ -1/6 & 1/3 & 0 & 1/6 & -1/3 & 0 \\ 0 & -1/6 & 1/6 & 0 & -1/6 & 1/6 \\ 1/6 & -1/6 & 1/6 & -1/6 & 1/6 & -1/6 \end{pmatrix},$$

and so the idempotents are

$$e_1 = \frac{(c-1)(c+1)(s+1)}{6}, \quad e_2 = \frac{-(c-1)(c+2)(s+1)}{6}$$

$$e_3 = \frac{(c+1)(sc+2)}{6}, \quad e_4 = \frac{-(c-1)(c+1)(s-1)}{6}$$

$$e_5 = \frac{(c-2)(c+1)(s-1)}{6}, \quad e_6 = \frac{-(c-1)(sc+2)}{6}$$

□

We used the GAP [7] command `ReducedGroebnerBasis` to verify that these are indeed idempotents. For example, to show that $e_1^2 = e_1$ in $B_1 = \mathbb{Q}[c,s]/I$, we ran

```
gap> I:=[s^2+s*c+c^2-3,(c-2)*(c-1)*(c+1)*(c+2),
(c-1)*(c+1)*(sc+2)];

gap> ReducedGroebnerBasis(I,MonomialLexOrdering ( ));
[s^4-5*s^2+4,c*s^2+1/2*s^3-c-1/2*s,c^2+c*s+s^2-3]

gap> e1:=1/6*(c^2-1)*(s+1);

gap> J:=[s^2+s*c+c^b2-3,(c-2)*(c-1)*(c+1)*(c+2),
(c-1)*(c+1)*(sc+2),e1^2-e1];

gap> ReducedGroebnerBasis(J,MonomialLexOrdering ( ));
[s^4-5*s^2+4,c*s^2+1/2*s^3-c-1/2*s,c^2+c*s+s^2-3]
```

Thus $e_1^2 - e_1 \in I$.

The following table summarizes the case $G = S_3$ where $L/\mathbb{Q}$ is the splitting field of $x^3 - 2$, with Galois group S_3:

$N \leq \mathrm{Perm}(S_3)$	**Iso. Class**	**Wedderburn-Artin for $(LN)^{S_3}$**	**Hopf Alg. Iso. Class of $(LN)^{S_3}$**
$M_1 = \rho(S_3)$	S_3	$\mathbb{Q}^2 \times \mathrm{Mat}_2(\mathbb{Q})$	$[\mathbb{Q}S_3]$
$M_2 = \lambda(S_3)$	S_3	$\mathbb{Q}^2 \times \mathrm{Mat}_2(\mathbb{Q})$	$[(LM_2)^{S_3}] \neq [\mathbb{Q}S_3]$
$N_1 = \langle(1,6,2,5,3,4)\rangle$	C_6	$\mathbb{Q}^6$	$[(LN_1)^{S_3}]$
$N_2 = \langle(1,4,2,6,3,5)\rangle$	C_6	$\mathbb{Q}^6$	$[(LN_1)^{S_3}]$
$N_3 = \langle(1,5,2,4,3,6)\rangle$	C_6	$\mathbb{Q}^6$	$[(LN_1)^{S_3}]$

S. A. Amitsur,
The Radical of field extensions,
Bull. Res. Council Israel, Sect. F, **7F**(1), 1957/1958, 1-10.

N. P. Byott,
Uniqueness of Hopf Galois structure of separable field extensions,
Comm. Algebra, **24**, 1996, 3217-3228, 3705.

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

N. P. Byott,
Hopf-Galois structures on Galois field extensions of degree pq,
J. Pure Appl. Algebra, 1-3, 2004, 45-57.

L. N. Childs,
On the Hopf Galois theory for separable field extensions,
Comm. Algebra, **17**, 1989, 809-825.

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

The GAP System.

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

R. Haggenmüller, B. Pareigis,
Hopf algebra forms on the multiplicative group and other groups,
manuscripta math., **55**, 1986, 121-136.

A. Koch, T. Kohl, P. Truman, R. Underwood,
On the structure of Hopf algebras acting on separable algebras,
working draft: March 21, 2017.

T. Kohl,
Regular permutation groups of order *mp* and Hopf Galois structures,
Alg. Num. Theor., **7**(9), 2013, 2203-2240.

J. Rotman,
Advanced Modern Algebra,
Pearson, Upper Saddle River, New Jersey, (2002).