The Structure of Hopf Algebras Acting on Galois Extensions

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

AUBURN
MONTGOMERY

June 7, 2016

Abstract

Let L/K be a Galois extension with group G. Let λ denote the left regular representation of G in $\mathrm{Perm}(G)$. Then by Greither-Pareigis theory, 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 $\lambda(G)$. All of the Hopf algebras thus constructed are finite dimensional algebras over K. In this talk, we discuss the Wedderburn-Malcev decompositions of these Hopf algebras.

1. The Jacobson Radical

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

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

eventually stops: there exists an integer $N \geq 1$ for which

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

Example 1.1. *Every finite dimensional algebra over a field K is left artinian as a ring.*

A left ideal L of R is a **maximal left ideal** 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 the intersection of all of the maximal left ideals of R.

Example 1.2. $J(\mathbb{Z}_p) = p\mathbb{Z}_p$.

A ring R is **Jacobson semisimple** if $J(R) = 0$.

Example 1.3. *For any field K, $J(\mathrm{Mat}_n(K)) = 0$ for $n \geq 1$.*

For an arbitrary ring R, the Jacobson radical $J(R)$ seems difficult to calculate. Here is an alternate characterization:

Proposition 1.4. *$J(R)$ consists of precisely those elements $x \in R$ for which $1 - rx$ has a left inverse for all $r \in R$.*

Proof. See [6, Propositon 8.31]. □

Further properties...

Proposition 1.5. *$J(R)$ is a two-sided ideal of R.*

Proof. See [6, Corollary 8.35(i)]. □

Proposition 1.6. *$J(R/J(R)) = 0$, that is, $R/J(R)$ is Jacobson semisimple.*
Proof. See [6, Corollary 8.35(ii)]. □

So, for a given ring R, is $J(R)$ the smallest two-sided ideal of R for which $R/J(R)$ is Jacobson semisimple?

Proposition 1.7. *If R is left artinian, then $J(R)$ is nilpotent.*

Proof. See [6, Proposition 8.34]. □

Proposition 1.8. *Suppose that R is a commutative algebra which is finitely generated over a field. Then $J(R)$ is the nilradical of R.*

Proof. By [6, Corollary 8.33], the nilradical of R is contained in $J(R)$. But since $J(R)$ is nilpotent, $J(R)$ consists of nilpotent elements, hence $J(R)$ is contained in the nilradical of R. □

2. Semisimple Rings

A left ideal L of R is a **minimal left ideal** 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.

Example 2.1. *Let K be a field, then*

$$K^n = \underbrace{K \times K \times \cdots \times K}_{n}$$

is left semisimple for $n \geq 1$.

Proposition 2.2. *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 [6, Theorem 8.42]. □

Proposition 2.3. (Maschke's Theorem) *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. (Sketch) In view of Proposition 2.2, we show that every left ideal L of KG is a direct summand. As vector spaces over K,

$$KG = L \oplus V,$$

so there is a K-map $\psi : KG \to L$ with $\psi(x) = x, \forall x \in L$. Now let $\Psi : KG \to KG$ be defined as

$$\Psi(x) = \frac{1}{|G|} \sum_{g \in G} g\psi(g^{-1}x).$$

Then $\mathrm{im}(\Psi) \subseteq L$, $\Psi(x) = x, \forall x \in L$, and Ψ is a KG-map. It follows that L is a direct summand as a KG-module. □

Proposition 2.4. *A ring R is left semisimple if and only if it is left artinian and $J(R) = 0$.*

Proof. See [6, Theorem 8.45]. □

Corollary 2.5. *Let G be a finite group and let K be a field whose characteristic does not divide $|G|$. Then $J(KG) = 0$.*

So, in view of Proposition 1.4, for any non-zero x in KG, there must be an element $r \in KG$ for which $1 - rx$ has no left inverse.

Proposition 2.6. (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. (Sketch of "only if") Suppose that R is a direct sum of minimal left ideals,

$$R = L_1 \oplus L_2 \oplus \cdots \oplus L_q.$$

We may assume without loss of generality, that the first m summands, L_i, $1 \le i \le m \le q$, represent the isomorphism classes of all of the L_i, $1 \le i \le q$. Let

$$B_1 = \sum_{L_i \cong L_1} L_1,\ B_2 = \sum_{L_i \cong L_2} L_2,\ \ldots,\ B_m = \sum_{L_i \cong L_m} L_m.$$

Then

$$R = B_1 \oplus B_2 \oplus \cdots \oplus B_m.$$

Let n_i be the number of summands in B_i, $1 \le i \le m$.

Now,

$$\begin{aligned} R^{\mathrm{opp}} &\cong \mathrm{End}_R(B_1) \times \mathrm{End}_R(B_2) \times \cdots \times \mathrm{End}_R(B_m) \\ &\cong \mathrm{Mat}_{n_1}(\mathrm{End}_R(L_1)) \times \mathrm{Mat}_{n_2}(\mathrm{End}_R(L_2)) \times \cdots \\ &\quad \cdots \times \mathrm{Mat}_{n_m}(\mathrm{End}_R(L_m)) \\ &\cong \mathrm{Mat}_{n_1}(C_1) \times \mathrm{Mat}_{n_2}(C_2) \times \cdots \times \mathrm{Mat}_{n_m}(C_m), \end{aligned}$$

for division rings $C_1, C_2, \ldots, C_m$.

Thus,

$$\begin{aligned} R &\cong (\mathrm{Mat}_{n_1}(C_1))^{\mathrm{opp}} \times (\mathrm{Mat}_{n_2}(C_2))^{\mathrm{opp}} \times \cdots \times (\mathrm{Mat}_{n_m}(C_m))^{\mathrm{opp}} \\ &\cong \mathrm{Mat}_{n_1}(C_1^{\mathrm{opp}}) \times \mathrm{Mat}_{n_2}(C_2^{\mathrm{opp}}) \times \cdots \times \mathrm{Mat}_{n_m}(C_m^{\mathrm{opp}}) \\ &\cong \mathrm{Mat}_{n_1}(D_1) \times \mathrm{Mat}_{n_2}(D_2) \times \cdots \times \mathrm{Mat}_{n_m}(D_m), \end{aligned}$$

for division rings $D_1, D_2, \ldots, D_m$. □

Proposition 2.7. (Wedderburn-Malcev) *Let A be a finite dimensional algebra over a field K, and let $J(A)$ be its Jacobson radical. Then*

$$A/J(A) \cong \mathrm{Mat}_{n_1}(D_1) \times \ \mathrm{Mat}_{n_2}(D_2) \times \cdots \times \mathrm{Mat}_{n_m}(D_m),$$

for integers $n_1, n_2, \ldots, n_m$ and division rings $D_1, D_2, \ldots, D_m$.

Proof. First note that $J(A/J(A)) = 0$ by Proposition 1.6. Moreover, $A/J(A)$ is finite dimensional over K, and so it is left artinian. Hence by Proposition 2.4, $A/J(A)$ is left semisimple. Now by Proposition 2.6, the result follows. □

3. Greither-Pareigis Theory

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 3.1. (Classical Hopf-Galois Structure) *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?

Theorem 3.2. (Greither-Pareigis) *Let L/K be a Galois extension with group G with $n = [L : K]$. Let λ denote the left regular representation of G in $\mathrm{Perm}(G)$. 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 remarkable 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. 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 Hopf-Galois structure via H.

Example 3.3. *Let* $\rho : G \to \mathrm{Perm}(G)$ *be the right regular representation of* G *in* $\mathrm{Perm}(G)$. *Then* $\rho(G)$ *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 structure.*

Proposition 3.4. (Koch, Kohl, Truman, U.) *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. *Then* H *is a group ring if and only if* $N = \rho(G)$, *that is,* H *is a group ring if and only if* L *has the classical Hopf-Galois structure.*

Proof. See [5, Proposition 1.2].

Corollary 3.5. (Koch, Kohl, Truman, U.) *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. Let $G(H)$ denote the set of grouplike elements in H. Then*

$$G(H) = N \cap \rho(G).$$

Proof. See [5, Corollary 1.3].

In general, to construct Hopf-Galois structures on L we search for regular subgroups normalized by $\lambda(G)$.

But: what is the structure of the K-Hopf algebras that arise from this construction?

How do they fall into K-algebra isomorphism classes?

How do they fall into K-Hopf algebra isomorphism classes?

Are they left semisimple as rings?

What are their Wedderburn-Malcev decompositions?

Proposition 4.1. (Koch, Kohl, Truman, U.) *Let L/K be a Galois extension with group G of degree $n = [L : K]$. Let $\alpha \in L$ be a normal basis generator satisfying $\mathrm{tr}(\alpha) = 1$. Let N be a regular subgroup of $\mathrm{Perm}(G)$ that is normalized by $\lambda(G)$. For $n \in N$, set*

$$v_n = \sum_{g \in G} g(\alpha)\lambda(g)n\lambda(g)^{-1}.$$

Then $\{v_n\}_{n \in N}$ is a K-basis for $(LN)^G$.

Proof. See [5, Proposition 2.1]. □

Example 4.2. *If $N = \rho(G)$, then since $\lambda(G)$ commutes with $\rho(G)$, we have*

$$v_n = \sum_{g \in G} g(\alpha)\lambda(g)n\lambda(g)^{-1} = \sum_{g \in G} g(\alpha)n = n.$$

Thus, as expected, $\{v_n\}_{n \in N}$ is the standard basis for the group ring KG.

Proposition/Conjecture 4.3. *$H = (LN)^G$ is a left semisimple ring.*

For $N = \rho(G)$: yes, of course, this it true by Maschke's Theorem.

For N abelian (H commutative): yes, the conjecture holds, since in this case $J(H)$ is the nilradical of H, which is trivial. The reason $J(H)$ is trivial is that $J(LN)$ is trivial and any nontrivial element of $J(H)$ would lift to a nontrivial element of $J(LN)$, a contradiction.

The following result might also be helpful in proving the conjecture.

Proposition 4.4. (Clark) *Let* $\phi : R \to S$ *be a ring homomorphism. Suppose that there exists a finite set* $\{x_1, \ldots, x_n\}$ *of left* R*-module generators of* S *such that each* x_i *lies in the commutant* $C_S(\phi(R))$*. Then* $\phi(J(R)) \subseteq J(S)$*.*

Proof. See [2, Proposition 3.23] □

Proposition 4.4 could be used to prove Conjecture 4.3 by applying it to the case $R = H$, $S = LN$, where $\phi : H \to LN$ is the inclusion. Then if appropriate generators $\{x_1, x_2, \ldots, x_n\}$ could be found, then $J(H)$ would be trivial since $J(LN)$ is trivial.

5. Examples: Galois Group: Rank 4 Elementary Abelian

In what follows, we explicitly construct some $(LN)^G$, aka "Greither-Pareigis" Hopf algebras.

Let K be the splitting field of the polynomial $p(x) = x^4 - 10x^2 + 1$ over $\mathbb{Q}$. Then $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, and K is Galois with group $G \cong C_2 \times C_2$, $G = \{1, \sigma, \tau, \sigma\tau\}$, $\sigma^2 = \tau^2 = 1$.

The Galois action is given as

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

Note that

$$\alpha = \frac{1}{4}\left(1 + \sqrt{2} + \sqrt{3} + \sqrt{6}\right)$$

is a normal basis generator for $K/\mathbb{Q}$ with $\mathrm{tr}(\alpha) = 1$.

Example 5.1. *The subgroup* $\rho(G)$ *is a regular subgroup of* $\mathrm{Perm}(G)$ *normalized by* $\lambda(G) = \rho(G)$. *K is a Hopf-Galois extension of* $\mathbb{Q}$*; K has the classical Hopf-Galois structure via* $H = (K\rho(G))^G = \mathbb{Q}G$. *A basis for* $\mathbb{Q}G$ *is* $\{1, \sigma, \tau, \sigma\tau\}$.

Proposition 5.2. $\mathbb{Q}G$ *is left semisimple as a ring. Its Wedderburn-Artin decomposition is*

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

Proof. By Maschke's Theorem, $\mathbb{Q}G$ is a left semisimple ring. Hence by Wedderburn-Artin,

$$\mathbb{Q}G \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_m}(D_m),$$

where $n_i \geq 1$ are integers and the D_i are division rings, $1 \leq i \leq m$.

Over $\mathbb{C}$, G has exactly 4 one-dimensional irreducible representations

$$\rho_i : G \to \mathrm{GL}(W_i),$$

$\dim_{\mathbb{C}}(W_i) = 1$, given in the tables:

x	$\rho_0(x)$
1	1
σ	1
τ	1
$\sigma\tau$	1

x	$\rho_1(x)$
1	1
σ	1
τ	-1
$\sigma\tau$	-1

x	$\rho_2(x)$
1	1
σ	-1
τ	1
$\sigma\tau$	-1

x	$\rho_3(x)$
1	1
σ	-1
τ	-1
$\sigma\tau$	1

Let χ_i be the character of ρ_i. Then

$$b_1 = \frac{1}{4}\sum_{x\in G}\chi_0(x^{-1})x = \frac{1}{4}\left(1+\sigma+\tau+\sigma\tau\right),$$

$$b_2 = \frac{1}{4}\sum_{x\in G}\chi_1(x^{-1})x = \frac{1}{4}\left(1+\sigma-\tau-\sigma\tau\right),$$

$$b_3 = \frac{1}{4}\sum_{x\in G}\chi_0(x^{-1})x = \frac{1}{4}\left(1-\sigma+\tau-\sigma\tau\right),$$

$$b_4 = \frac{1}{4}\sum_{x\in G}\chi_1(x^{-1})x = \frac{1}{4}\left(1-\sigma-\tau+\sigma\tau\right),$$

are pairwise orthogonal idempotents in $\mathbb{C}G$ with

$$b_1+b_2+b_3+b_4=1,$$

cf. [7, Exercise 6.4].

Now, each irreducible representation extends to a $\mathbb{C}$-algebra homomorphism:

$$\tilde{\rho}_i : \mathbb{C}G \rightarrow \mathrm{End}_{\mathbb{C}}(W_i) \cong \mathbb{C},$$

$0 \leq i \leq 3$.

There is an isomorphism

$$\tilde{\rho} : \mathbb{C}G \rightarrow \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$$

given as:

$$\tilde{\rho}(x) = (\tilde{\rho}_0(x), \tilde{\rho}_1(x), \tilde{\rho}_2(x), \tilde{\rho}_3(x)).$$

One has

$$\begin{aligned} \tilde{\rho}(b_1) &= (1,0,0,0), \\ \tilde{\rho}(b_2) &= (0,1,0,0), \\ \tilde{\rho}(b_3) &= (0,0,1,0), \\ \tilde{\rho}(b_4) &= (0,0,0,1), \end{aligned}$$

cf. [7, Proposition 10].

Since $\{b_1, b_2, b_3, b_4\}$ is also a $\mathbb{Q}$-basis for $\mathbb{Q}G$, one has

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

$\square$

Example 5.3. (Byott) *Let $\eta \in \mathrm{Perm}(G)$ be defined as*

$$\eta(\sigma^k\tau^l) = \sigma^{k-1}\tau^{l+k-1},\ 0 \leq k, l \leq 1.$$

Then $\langle\eta\rangle \cong C_4$ is a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$.

By Theorem 3.2, K is a Hopf-Galois extension of $\mathbb{Q}$; K has a Hopf-Galois structure via the 4-dimensional $\mathbb{Q}$-Hopf algebra $H = (K\langle\eta\rangle)^G$.

By Proposition 4.1, a $\mathbb{Q}$-basis for H is $\{v_1, v_\eta, v_{\eta^2}, v_{\eta^3}\}$ with

$$\begin{aligned} v_1 &= 1, \\ v_\eta &= \frac{1}{2}\left(\eta + \eta^3\right) + \frac{\sqrt{3}}{2}\left(\eta - \eta^3\right) \\ v_{\eta^2} &= \eta^2 \\ v_{\eta^3} &= \frac{1}{2}\left(\eta + \eta^3\right) - \frac{\sqrt{3}}{2}\left(\eta - \eta^3\right). \end{aligned}$$

Proposition 5.4. *The $\mathbb{Q}$-Hopf algebra H of Example 5.3 is left semisimple as a ring. Its Wedderburn-Artin decomposition is*

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

Proof. H contains $\dfrac{1+\eta^2}{4}$ and $\pm\dfrac{\eta+\eta^3}{4}$, and so, H contains

$$b_1 = \frac{1}{4}\left(1+\eta+\eta^2+\eta^3\right),$$

$$b_2 = \frac{1}{4}\left(1-\eta+\eta^2-\eta^3\right),$$

and

$$b_3 = 1 - b_1 - b_2 = \frac{1-\eta^2}{4};$$

b_1, b_2, b_3 are mutually orthogonal idempotents.

Let

$$a = \left(\frac{1-\eta^2}{2}\right)\left(\frac{1}{2}(\eta+\eta^3) + \frac{\sqrt{3}}{2}(\eta-\eta^3)\right) = \frac{\sqrt{3}}{2}(\eta-\eta^2).$$

Then $\{b_1, b_2, b_3, a\}$ is a $\mathbb{Q}$-basis for H. Note that $a^2 = -3b_3$.

Now as a vector space over $\mathbb{Q}$,

$$H = \mathbb{Q}b_1 \oplus \mathbb{Q}b_2 \oplus \mathbb{Q}b_3 \oplus \mathbb{Q}a,$$

and as $\mathbb{Q}$-algebras,

$$\begin{aligned} H &\cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}b_3[a], \\ &\cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt{-3}), \end{aligned}$$

the isomorphism in the last component given as $b_3 \mapsto 1_{\mathbb{Q}(\sqrt{-3})}$, $a \mapsto \sqrt{-3}$. By Wedderburn-Artin, H is left semisimple. □

By direct calculation,

$$G(H) = N \cap \rho(G) = \{1, \eta^2\}.$$

6. Conclusions, I

Regarding the rank 4 elementary abelian example above:

In the case where K has the classical Hopf-Galois structure (Example 5.1),

$$H_1 = (K\rho(G))^G = \mathbb{Q}G \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q},$$

In the case where K has the non-classical Hopf-Galois structure (Example 5.3),

$$H_2 = (KN)^G \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\sqrt{-3}).$$

The two Hopf-Galois structures on K are distinct in that the two Hopf algebras are non-isomorphic as $\mathbb{Q}$-algebras, and hence, certainly non-isomorphic as Hopf algebras.

Moreover, both Hopf algebras are left semisimple, and thus by Proposition 2.4, both Jacobson radicals are trivial.

7. Examples: Galois Group: Symmetric Group on 3 Letters

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

Observe that

$$\beta = \frac{1}{3}(1 + \alpha + \alpha^2 + \omega + \omega\alpha + \omega\alpha^2)$$

is a normal basis generator for $K/\mathbb{Q}$ with $\mathrm{tr}(\beta) = 1$.

Example 7.1. *The subgroup* $\rho(S_3)$ *is a regular subgroup of* $\mathrm{Perm}(S_3)$ *normalized by* $\lambda(S_3)$*. K is a Hopf-Galois extension of* $\mathbb{Q}$*; K has the classical Hopf-Galois structure via* $H = (K\rho(S_3))^{S_3} = \mathbb{Q}S_3$*. A basis for* $\mathbb{Q}S_3$ *is* $\{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$*.*

Proposition 7.2. $\mathbb{Q}S_3$ *is left semisimple as a ring. Its Wedderburn-Artin decomposition is*

$$\mathbb{Q}S_3 \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

Proof. (Computer-free proof) By Maschke's Theorem, $\mathbb{Q}S_3$ is a left semisimple ring.

Hence by Wedderburn-Artin,

$$\mathbb{Q}S_3 \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_m}(D_m),$$

where $n_i \geq 1$ are integers and the D_i are division rings, $1 \leq i \leq m$.

Over $\mathbb{C}$, there are exactly two 1-dimensional representations of S_3,

$$\rho_0 : S_3 \to \mathrm{GL}(W_0),$$

given as $\rho_0(x) = 1, \forall x \in S_3$, and

$$\rho_1 : S_3 \to \mathrm{GL}(W_1),$$

defined as $\rho_1(\sigma^i) = 1$, and $\rho_1(\tau\sigma^i) = -1$ for $i = 0, 1, 2$.

There is exactly one 2-dimensional representation

$$\rho_2 : S_3 \to \mathrm{GL}(W_2),$$

defined as $\rho_2(\sigma^i) = \begin{pmatrix} \omega^i & 0 \\ 0 & \omega^{2i} \end{pmatrix}$, and $\rho_2(\tau\sigma^i) = \begin{pmatrix} 0 & \omega^{2i} \\ \omega^i & 0 \end{pmatrix}$, for $i = 0, 1, 2$, where ω is a primitive 3rd root of unity, [7, §2.4, §2.5, §5.3].

Let χ_i be the character of ρ_i. Then

$$b_1 = \frac{1}{6}\sum_{x\in S_3}\chi_0(x^{-1})x = \frac{1}{6}\left(1+\sigma+\sigma^2+\tau+\tau\sigma+\tau\sigma^2\right),$$

$$b_2 = \frac{1}{6}\sum_{x\in S_3}\chi_1(x^{-1})x = \frac{1}{6}\left(1+\sigma+\sigma^2-\tau-\tau\sigma-\tau\sigma^2\right),$$

and

$$b_3 = \frac{1}{3}\sum_{x\in S_3}\chi_2(x^{-1})x = \frac{1}{3}\left(2-\sigma-\sigma^2\right)$$

are pairwise orthogonal idempotents in $\mathbb{C}S_3$ with

$$b_1+b_2+b_3=1,$$

cf. [7, Exercise 6.4].

Now, each irreducible representation extends to a $\mathbb{C}$-algebra homomorphism:

$$\tilde{\rho}_i : \mathbb{C}S_3 \to \mathrm{End}_{\mathbb{C}}(W_i) \cong \mathrm{Mat}_{n_i}(\mathbb{C}),\ \ n_i = \dim_{\mathbb{C}}(W_i),$$

$0 \leq i \leq 2$.
There is an isomorphism

$$\tilde{\rho} : \mathbb{C}S_3 \to \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_2(\mathbb{C})$$

given as:

$$\tilde{\rho}(x) = (\tilde{\rho}_0(x), \tilde{\rho}_1(x), \tilde{\rho}_2(x)).$$

One has

$$\tilde{\rho}(b_1) = \left(1, 0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right),$$

$$\tilde{\rho}(b_2) = \left(0, 1, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right),$$

$$\tilde{\rho}(b_3) = \left(0, 0, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right).$$

cf. [7, Proposition 10].

We seek 4 elements of $\mathbb{C}S_3$ which correspond to a basis for the simple component $\mathrm{Mat}_2(\mathbb{C})$.

We find elements $b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2} \in \mathbb{C}S_3$ which satisfy the multiplication table

	$b_{1,1}$	$b_{1,2}$	$b_{2,1}$	$b_{2,2}$
$b_{1,1}$	$b_{1,1}$	$b_{1,2}$	0	0
$b_{1,2}$	0	0	$b_{1,1}$	$b_{1,2}$
$b_{2,1}$	$b_{2,1}$	$b_{2,2}$	0	0
$b_{2,2}$	0	0	$b_{2,1}$	$b_{2,2}$

(1)

We require that

$$b_{1,1} + b_{2,2} = b_3 = \frac{1}{3}(2 - \sigma - \sigma^2),$$

with $b_{1,1}^2 = b_{1,1}$ and $b_{2,2}^2 = b_{2,2}$, and so we guess that

$$b_{1,1} = \frac{1}{3}\left(1 - \sigma + \tau\sigma - \tau\sigma^2\right),$$

and

$$b_{2,2} = \frac{1}{3}\left(1 - \sigma^2 - \tau\sigma + \tau\sigma^2\right).$$

(Note: I used trial and error, but one could probably solve a non-linear system to get this.)

Now for $b_{1,2}$ and $b_{2,1}$: We require that

$$(b_{1,2} + b_{2,1})^2 = b_{1,1} + b_{2,2} = \frac{1}{3}(2 - \sigma - \sigma^2),$$

and so, we could guess that

$$b_{1,2} + b_{2,1} = \frac{1}{3}\tau\left(2 - \sigma - \sigma^2\right)$$

since $\frac{1}{3}(2 - \sigma - \sigma^2)$ is idempotent and $\tau^2 = 1$.

But we also know that $b_{1,2}$ satisfies the equation $b_{2,2}X = 0$, which converts to a 6×6 linear homogeneous system with many solutions, one of which is

$$b_{1,2} = -\frac{1}{3}\left(\sigma - \sigma^2 - \tau + \tau\sigma^2\right).$$

With this choice for $b_{1,2}$, then

$$b_{2,1} = \frac{1}{3}\left(\sigma - \sigma^2 + \tau - \tau\sigma\right).$$

Now (as one can check) a $\mathbb{C}$-basis for $\mathbb{C}S_3$ is

$$B' = \{b_1, b_2, b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2}\},$$

with

$$\begin{aligned}
b_1 &= \frac{1}{6}(1+\sigma+\sigma^2+\tau+\tau\sigma+\tau\sigma^2),\\
b_2 &= \frac{1}{6}(1+\sigma+\sigma^2-\tau-\tau\sigma-\tau\sigma^2),\\
b_{1,1} &= \frac{1}{3}(1-\sigma+\tau\sigma-\tau\sigma^2),\\
b_{1,2} &= -\frac{1}{3}(\sigma-\sigma^2-\tau+\tau\sigma^2),\\
b_{2,1} &= \frac{1}{3}(\sigma-\sigma^2+\tau-\tau\sigma),\\
b_{2,2} &= \frac{1}{3}(1-\sigma^2-\tau\sigma+\tau\sigma^2).
\end{aligned}$$

The $\mathbb{C}$-algebra isomorphism

$$\tilde{\rho} : \mathbb{C}S_3 \to \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_2(\mathbb{C})$$

is now given as

$$\begin{aligned}
\tilde{\rho}(b_1) &= \left(1, 0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right), \\
\tilde{\rho}(b_2) &= \left(0, 1, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right), \\
\tilde{\rho}(b_{1,1}) &= \left(0, 0, \frac{1}{3}\begin{pmatrix} 1-\omega & \omega^2-\omega \\ \omega-\omega^2 & 1-\omega^2 \end{pmatrix}\right), \\
\tilde{\rho}(b_{1,2}) &= \left(0, 0, \frac{1}{3}\begin{pmatrix} \omega^2-\omega & 1-\omega^2 \\ 1-\omega & \omega-\omega^2 \end{pmatrix}\right), \\
\tilde{\rho}(b_{2,1}) &= \left(0, 0, \frac{1}{3}\begin{pmatrix} \omega-\omega^2 & 1-\omega^2 \\ 1-\omega & \omega^2-\omega \end{pmatrix}\right), \\
\tilde{\rho}(b_{2,2}) &= \left(0, 0, \frac{1}{3}\begin{pmatrix} 1-\omega^2 & \omega-\omega^2 \\ \omega^2-\omega & 1-\omega \end{pmatrix}\right).
\end{aligned}$$

Now, B' is also a $\mathbb{Q}$-basis for $\mathbb{Q}S_3$. Hence, there is a $\mathbb{Q}$-algebra isomorphism

$$\phi : \mathbb{Q}S_3 \to \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q})$$

$$\begin{aligned}
\phi(b_1) &= \left(1, 0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right), \\
\phi(b_2) &= \left(0, 1, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right), \\
\phi(b_{1,1}) &= \left(0, 0, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right), \\
\phi(b_{1,2}) &= \left(0, 0, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right), \\
\phi(b_{2,1}) &= \left(0, 0, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right), \\
\phi(b_{2,2}) &= \left(0, 0, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right).
\end{aligned}$$

Example 7.3. *Let* $\lambda : S_3 \to \mathrm{Perm}(S_3)$ *denote the left regular representation of* S_3 *in* $\mathrm{Perm}(S_3)$*;* $\lambda(S_3)$ *is a subgroup of* $\mathrm{Perm}(S_3)$ *normalized by* $\lambda(S_3)$*. Then* K *is a Hopf-Galois extension of* $\mathbb{Q}$*;* K *has a Hopf-Galois structure via the* 6*-dimensional* $\mathbb{Q}$*-Hopf algebra* $H = (K\lambda(S_3))^{S_3}$*.*

Proposition 7.4. H *is left semisimple as a ring. Its Wedderburn-Artin decomposition is*

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

Proof. By [1, (6.12) Example, p. 55],

$$H = \{a_0 + a_1\sigma + \tau(a_1)\sigma^2 + b_0\tau + \sigma^2(b_0)\sigma\tau + \sigma(b_0)\sigma^2\tau\}$$

where $a_0 \in \mathbb{Q}$, $a_1 \in \mathbb{Q}(\omega)$, and $b_0 \in \mathbb{Q}(\alpha)$.

Write $a_1 = a_{1,0} + a_{1,1}\omega$, $b_0 = b_{0,0} + b_{0,1}\alpha + b_{0,2}\alpha^2$, for $a_{1,0}, a_{1,1}, b_{0,0}, b_{0,1}, b_{0,2} \in \mathbb{Q}$.

Then a typical element of H can be written as

$$\begin{aligned} &a_0 + (a_{1,0} + a_{1,1}\omega)\sigma + (a_{1,0} + a_{1,1}\omega^2)\sigma^2 + (b_{0,0} + b_{0,1}\alpha + b_{0,2}\alpha^2)\tau \\ &+ (b_{0,0} + b_{0,1}\alpha\omega^2 + b_{0,2}\alpha^2\omega)\sigma\tau + (b_{0,0} + b_{0,1}\alpha\omega + b_{0,2}\alpha^2\omega^2)\sigma^2\tau \\ &= a_0 + a_{1,0}(\sigma + \sigma^2) + a_{1,1}(\omega\sigma + \omega^2\sigma^2) + b_{0,0}(\tau + \sigma\tau + \sigma^2\tau) \\ &+ b_{0,1}(\alpha\tau + \alpha\omega^2\sigma\tau + \alpha\omega\sigma^2\tau) + b_{0,2}(\alpha^2\tau + \alpha^2\omega\sigma\tau + \alpha^2\omega^2\sigma^2\tau). \end{aligned}$$

Thus

$$C = \{v_1, v_2, v_3, v_4, v_5, v_6\},$$

with

$$\begin{aligned} v_1 &= 1 \\ v_2 &= \sigma + \sigma^2, \\ v_3 &= \omega\sigma + \omega^2\sigma^2, \\ v_4 &= \tau + \sigma\tau + \sigma^2\tau, \\ v_5 &= \alpha\tau + \alpha\omega^2\sigma\tau + \alpha\omega\sigma^2\tau, \\ v_6 &= \alpha^2\tau + \alpha^2\omega\sigma\tau + \alpha^2\omega^2\sigma^2\tau, \end{aligned}$$

is a $\mathbb{Q}$-basis for H; this is the "standard" basis for H.

The multiplication table for the v_i is:

(2)

	1	v_2	v_3	v_4	v_5	v_6
1	1	v_2	v_3	v_4	v_5	v_6
v_2	v_2	$2v_2$	$-1-v_2-v_3$	$2v_4$	$-v_5$	$-v_6$
v_3	v_3	$-1-v_2-v_3$	$2+v_3$	$-v_4$	$-v_5$	$2v_6$
v_4	v_4	$2v_4$	$-v_4$	$3+3v_2$	0	0
v_5	v_5	$-v_5$	$2v_5$	0	0	$6-6v_2-6v_3$
v_6	v_6	$-v_6$	$-v_6$	0	$6+6v_3$	0

Now, as in Proposition 7.2, $c_1 = b_1 = \frac{1}{6}(1 + v_2 + v_4)$ and $c_2 = b_2 = \frac{1}{6}(1 + v_2 - v_4)$ form a pair of mutually orthogonal idempotents in H.

We search for matrix units satisfying table (1).

One has that

$$c_{1,1} = \frac{1}{3}(1 + v_3) = \frac{1}{3}(1 + \omega\sigma + \omega^2\sigma^2)$$

and

$$c_{2,2} = \frac{1}{3}(1 - v_2 - v_3) = \frac{1}{3}(1 + \omega^2\sigma + \omega\sigma^2)$$

are a pair of orthogonal idempotents.

A bit of trial and error using table (2) (really!) shows that the other matrix units are $c_{1,2} = \frac{1}{6}v_6$ and $c_{2,1} = \frac{1}{3}v_5$.

The set

$$C' = \{c_1, c_2, c_{1,1}, c_{1,2}, c_{2,1}, c_{2,2}\}$$

is a $\mathbb{Q}$-basis for H. There is a $\mathbb{Q}$-algebra isomorphism:

$$\psi : H \to \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}),$$

$$c_1 \mapsto \left(1, 0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right),$$

$$c_2 \mapsto \left(0, 1, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right),$$

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

$$c_{1,2} \mapsto \left(0, 0, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right),$$

$$c_{2,1} \mapsto \left(0, 0, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right),$$

$$c_{2,2} \mapsto \left(0, 0, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right).$$

Clearly, H is left semisimple. □

Recall that

$$\beta = \frac{1}{3}(1 + \alpha + \alpha^2 + \omega + \omega\alpha + \omega\alpha^2)$$

is a normal basis generator for $K/\mathbb{Q}$. By Proposition 4.1, there is another $\mathbb{Q}$-basis for H,

$$D = \{v_1 = 1, v_\sigma, v_{\sigma^2}, v_\tau, v_{\tau\sigma}, v_{\tau\sigma^2}\},$$

where

$$v_x = \sum_{g \in S_3} g(\beta)\lambda(g)\lambda(x)\lambda(g)^{-1},$$

for $x \in S_3$.

The basis matrix of D (with respect to C) is:

$$M_D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/3 & 1/3 & 1/3 \\ 0 & 0 & 0 & 1/3 & 1/3 & -2/3 \\ 0 & 0 & 0 & 1/3 & -2/3 & 1/3 \end{pmatrix}$$

One has

$$M_D v_D = v.$$

Now,

$$M_D^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 & 0 \end{pmatrix}$$

so that

$$M_D^{-1} v = v_D.$$

Thus, in terms of D, the basis C' computed above is

$$C' = \{\tfrac{1}{6}(1+v_\sigma+v_{\sigma^2}+v_\tau+v_{\tau\sigma}+v_{\tau\sigma^2}), \tfrac{1}{6}(1+v_\sigma+v_{\sigma^2}-v_\tau-v_{\tau\sigma}-v_{\tau\sigma^2}),$$

$$\tfrac{1}{3}(1-v_{\sigma^2}), \tfrac{1}{6}(v_\tau - v_{\tau\sigma}), \tfrac{1}{3}(v_\tau - v_{\tau\sigma^2}), \tfrac{1}{3}(1-v_\sigma)\}.$$

8. Conclusions, II

Regarding the S_3 examples above:

In the case where K has the classical Hopf-Galois structure (Example 7.1),

$$H_1 = (K\rho(S_3))^{S_3} = \mathbb{Q}S_3 \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}),$$

In the case where K has the non-classical Hopf-Galois structure (Example 7.3),

$$H_2 = (K\lambda(S_3))^{S_3} \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

By a direct computation (or use [1, (6.9) Example]),

$$G(H_2) = \lambda(S_3) \cap \rho(S_3) = \{1\}.$$

These two Hopf algebras are isomorphic as $\mathbb{Q}$-algebras, yet are non-isomorphic as Hopf algebras.

Both Hopf algebras are left semisimple, and thus by Proposition 2.4, both Jacobson radicals are trivial.

Fact 9.1. *Suppose* $\varphi : S \to G$ *is a bijection of sets with* G *a group. Then there is a unique group structure on* S *that makes* φ *an isomorphism of groups.*

For $x, y \in S$, define

$$xy = \varphi^{-1}(\varphi(x)\varphi(y)).$$

Proposition 9.2. *Let K be a field. Let $\varphi : A \to H$ be an isomorphism of K-algebras with H a K-Hopf algebra. Then there is a unique Hopf algebra structure on A that makes φ an isomorphism of K-Hopf algebras.*

Proof. Define $\Delta_A : A \to A \otimes_K A$ by the rule

$$\Delta_A(a) = (\varphi^{-1} \otimes \varphi^{-1})\Delta_H(\varphi(a)),$$

define $\epsilon_A : A \to K$ by the rule

$$\epsilon_A(a) = \epsilon_H(\varphi(a)),$$

and define $S_A : A \to A$ by the rule

$$S_A(a) = \varphi^{-1} S_H(\varphi(a)),$$

for $a \in A$.

Then $(A, m_A, \lambda_A, \Delta_A, \epsilon_A, S_A)$ is a K-Hopf algebra and φ is an isomorphism of K-Hopf algebras.

Now by Propositions 7.2 and 7.4, the composition of maps

$$\mathbb{Q}S_3 \stackrel{\phi}{\to} \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}) \stackrel{\psi^{-1}}{\to} H,$$

is an isomorphism of $\mathbb{Q}$-algebras.

Put $\varphi = \psi^{-1} \circ \phi$. Then by Proposition 9.2, there is a $\mathbb{Q}$-Hopf algebra structure on $\mathbb{Q}S_3$ with

$$\Delta_{\mathbb{Q}S_3}(a) = (\varphi^{-1} \otimes \varphi^{-1})\Delta_H(\varphi(a)),$$

$$\epsilon_{\mathbb{Q}S_3}(a) = \epsilon_H(\varphi(a)),$$

and

$$S_{\mathbb{Q}S_3}(a) = \varphi^{-1} S_H(\varphi(a)),$$

for $a \in \mathbb{Q}S_3$; φ is an isomorphism of $\mathbb{Q}$-Hopf algebras.

This $\mathbb{Q}$-Hopf algebra structure on $\mathbb{Q}S_3$ admits exactly one grouplike element (since H has only one grouplike).

Consequently, this $\mathbb{Q}$-Hopf algebra structure on $\mathbb{Q}S_3$ is distinct from the ordinary $\mathbb{Q}$-Hopf algebra structure on $\mathbb{Q}S_3$ (in which there are 6 grouplikes).

What is $\Delta_{\mathbb{Q}S_3}(\sigma)$?

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

[2] P. Clark,
Noncommutative Algebra
retreived from the internet, May 2016.

[3] R. Farnsteiner,
The Theorem of Wedderburn-Malcev: $H^2(A, N)$ and extensions,
retrieved from the internet, August 2015.

[4] C. Greither and B. Pareigis,
Hopf galois theory for separable field extensions,
J. Algebra, **106**, 239-258, (1987).

[5] A. Koch, T. Kohl, P. Truman, R. Underwood,
On the structure of Hopf algebras acting on separable algebras,
working draft: April 13, 2016.

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

[7] J.-P. Serre,
Linear Representations of Finite Groups
GTM 42, Springer-Verlag, New York, (1977).

[8] J. Wedderburn,
On hypercomplex numbers,
Proc. London Math. Soc., **6**, 77-118, (1908).

Appendix: Decomposition of $\mathbb{Q}S_3$ (Computer Solution)

```
gap> LoadPackage("wedderga");
 true

 gap> QG:=GroupRing(Rationals,SymmetricGroup(3));
 <algebra-with-one over Rationals, with 2 generators>

 gap> WedderburnDecomposition(QG);

[ Rationals, Rationals, <crossed product with center
Rationals over CF(3) of a group of size 2> ]

gap> WedderburnDecompositionInfo(QG);

[ [ 1, Rationals ], [ 1, Rationals ], [ 1, Rationals,
3, [ 2, 2, 0 ] ] ]
```

What this means is that

$$\mathbb{Q}S_3 \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\omega)[x : \ \omega x = x\omega^2, x^2 = 1],$$

where ω is a primitive 3rd root of unity; $\{1, \omega, x, \omega x\}$ is a $\mathbb{Q}$-basis for the component $\mathbb{Q}(\omega)[x : \ \omega x = x\omega^2, x^2 = 1]$.

Now, the companion matrix of the polynomial $x^2 + x + 1$ is $W = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, and the companion matrix of $x^2 - 1$ is $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Moreover, $WX = XW^2$.

As one can check, $\{I_2, W, X, WX\}$ is a $\mathbb{Q}$-basis for $\mathrm{Mat}_2(\mathbb{Q})$, thus as rings,

$$\mathbb{Q}(\omega)[x : \ \omega x = x\omega^2, x^2 = 1] \cong \mathrm{Mat}_2(\mathbb{Q}).$$

Thus,

$$\mathbb{Q}S_3 \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$