Hopf Forms and Hopf-Galois Theory

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

May 30, 2020

1. Introduction

Let K be a field containing $\mathbb{Q}$ and let N be a finite group with automorphism group $F = \mathrm{Aut}(N)$. R. Haggenmüller and B. Pareigis have shown that there is a bijection

$$\Theta : \mathcal{G}al(K, F) \to \mathcal{H}opf(KN)$$

from the collection of F-Galois extensions of K to the collection of Hopf forms of the group ring KN. In more detail, if L is an F-Galois extension of K, then the corresponding K-Hopf form is the fixed ring

$$\Theta(L) = H = (LN)^F$$

[6, Theorem 5].

Let $N = C_n$ denote the cyclic group of order n. If $n = 2$, then F is trivial and KC_2 is the only Hopf form of KC_2. For the cases $n = 3, 4, 6$,

$$F = \mathrm{Aut}(C_n) = \mathbb{Z}_n^* = C_2.$$

The C_2-Galois extensions of K are completely classified as the quadratic extensions $L = K[x]/(x^2 - b)$, where $b \in K^\times$ [13]. Thus the result of Haggenmüller and Pareigis yields an explicit description of all Hopf forms of KC_n for the cases $n = 3, 4, 6$ [6, Theorem 6].

In the cases $n \neq 2, 3, 4, 6$, the F-Galois extensions of K (and consequently) the Hopf forms of KC_n seem difficult to compute.

So it is of interest to investigate the structure of Hopf forms of KC_n for $n \geq 2$.

Two special Hopf forms of KC_n can be identified.

1. The trivial Hopf form KC_n, which is the image under Θ of the trivial F-Galois extension $\mathrm{Map}(F, K)$ of K; if $L = \mathrm{Map}(F, K)$, then

$$\Theta(L) = KC_n.$$

2. The linear dual $(KC_n)^*$, which is the absolutely semisimple Hopf form of KC_n. If $L = K[x]/(\Phi_n(x))$, where $\Phi_n(x)$ is the nth cyclotomic polynomial, then L is a $\mathbb{Z}_n^*$-Galois extension of K and

$$\Theta(L) = (KC_n)^*.$$

In the case that $K = \mathbb{Q}$ and $n = p$ is prime, we obtain an explicit description of $(\mathbb{Q}C_p)^*$.

The Hopf form $(\mathbb{Q}C_p)^*$ is the ring of regular functions on an affine variety in $\mathbb{Q}^{p-1}$. The variety is isomorphic to C_p as a group of points, which could be of interest in other applications.

There is a natural application of Θ to Hopf-Galois theory:

Let $(H, \cdot)$ be a Hopf-Galois structure of type N on the Galois extension of fields E/K. Then H is a Hopf form of KN and thus

$$\Theta(L) = H$$

for some F-Galois extension L of K, $F = \mathrm{Aut}(N)$.

We show how to construct L as a subfield of E under certain conditions.

We identify necessary conditions for the Galois extension $E/\mathbb{Q}$ with group G, $n = |G|$, to admit the Hopf-Galois structure $((\mathbb{Q}C_n)^*, \cdot)$ of type C_n.

I would like to thank Tim Kohl for discussions regarding papers [6], [12].

2. Hopf Forms of KN

Let F be a finite group. An F-**Galois extension** of K is a commutative K-algebra L that satisfies

(i) F is a subgroup of $\mathrm{Aut}_K(L)$,

(ii) L is a finitely generated, projective K-module,

(iii) $F \subseteq \mathrm{End}_K(L)$ is a free generating system over K.

The notion of F-Galois extension generalizes the usual definition of a Galois extension of fields.

The K-algebra of maps $\mathrm{Map}(F,K)$ is the **trivial F-Galois extension** of K where the action of F on $\mathrm{Map}(F,K)$ is given as

$$g(\phi)(h)=\phi(g^{-1}h)$$

for $g,h\in F$, $\phi\in\mathrm{Map}(F,K)$.

We let $\mathcal{G}al(K,F)$ denote the collection of all F-Galois extensions of K.

Let N be a finite group. Then the group ring KN is a K-Hopf algebra.

Let L be a faithfully flat K-algebra. An L-**Hopf form** of KN is a K-Hopf algebra H for which

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

as L-Hopf algebras.

A **Hopf form** of KN is a K-Hopf algebra H for which there exists a faithfully flat K-algebra L with

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

as L-Hopf algebras.

The **trivial Hopf form** of KN is KN.

Let $\mathcal{H}opf(KN)$ denote the collection of all Hopf forms of KN.

R. Haggenmüller and B. Pareigis [6, Theorem 5] have classified all Hopf forms of KN.

Theorem 1 (Haggenmüller and Pareigis).

Let N be a finite group and let $F = \mathrm{Aut}(N)$. There is a bijection

$$\Theta : \mathcal{G}al(K, F) \to \mathcal{H}opf(KN)$$

which associates to each F-Galois extension L of K, the Hopf form $H = \Theta(L)$ of KN defined as

$$H = (LN)^F,$$

where the action of F on N is through the automorphism group $F = \mathrm{Aut}(N)$ and the action of F on L is the Galois action. The Hopf form H is an L-Hopf form of KN with isomorphism $\psi : L \otimes_K H \to LN$ defined as $\psi(x \otimes h) = xh$.

Proposition 2.

Let N be a finite group, let $F = \mathrm{Aut}(N)$, and let $L = \mathrm{Map}(F, K)$. Then

$$\Theta(L) = (LN)^F \cong KN.$$

Proof (Sketch).

$H = (LN)^F$ has a K-basis consisting of group-like elements. Hence, $H = KN'$ for some finite group N'. Since $L \otimes_K H = L \otimes_K KN' \cong LN$ as Hopf algebras, we conclude that $N' \cong N$. □

Remark 3.

The proposition above shows that

$$\mathrm{Map}(F, K) = \Theta^{-1}(KN).$$

In general, given a Hopf form H of KN it is not clear (at least to this author) how to explicitly construct an element $L \in \mathcal{G}al(K, F)$ for which $\Theta(L) = H$.

3. The Absolutely Semisimple Hopf Form of KC_n

Let $N = C_n$. By Maschke's theorem, KC_n is semisimple. Extending scalars to $\mathbb{C}$ yields the Wedderburn-Artin decomposition

$$\mathbb{C}C_n = \mathbb{C} \otimes_K KC_n \cong \underbrace{\mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C}}_{n}.$$

Let L be a separable K-algebra. Then any L-Hopf form of KC_n is also semisimple. An L-Hopf form H of KC_n is **absolutely semisimple** if

$$H = \underbrace{K \times K \times \cdots \times K}_{n}.$$

Absolutely semisimple Hopf forms of KC_n always exist [12, Theorem 4.3].

Theorem 4 (Pareigis).

KC_n has a uniquely determined absolutely semisimple Hopf form $H = (KC_n)^*$, where $(KC_n)^*$ is the linear dual of KC_n.

As a Hopf form of KC_n, $(KC_n)^*$ comes from some F-Galois extension L. Here is how we can find L.

Proposition 5.

Let $\Phi_n(x)$ denote the nth cyclotomic polynomial and let $F = \mathrm{Aut}(C_n) = \mathbb{Z}_n^*$. Then $L = K[x]/(\Phi_n(x))$ is an F-Galois extension of K and

$$\Theta(L) = (LC_n)^F = (KC_n)^* = \underbrace{K \times K \times \cdots \times K}_{n}.$$

Proof (Sketch).

We have

$$LC_n \cong \underbrace{L \times L \times \cdots \times L}_{n}.$$

The action of F fixes each idempotent, and so,

$$(LC_n)^F \cong \underbrace{K \times K \times \cdots \times K}_{n}.$$

(See the discussion after the proof of [12, Theorem 4.3].) □

Remark 6.
$K[x]/(\Phi_n(x))$ is not necessarily a field. For example, if $K = \mathbb{Q}(\zeta_3)$, then

$$K[x]/(\Phi_{15}(x)) \cong K(\zeta_{15}) \times K(\zeta_{15}).$$

The faithfully flat (separable) K-algebra $K(\zeta_{15}) \times K(\zeta_{15})$ is an $F = \mathbb{Z}_{15}^* = (C_2 \times C_4)$-Galois extension of K corresponding to $(KC_{15})^*$.

If $K = \mathbb{Q}$, then $\mathbb{Q}[x]/(\Phi_n(x))$ is a field, isomorphic to $\mathbb{Q}(\zeta_n)$; $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$ with group $\mathbb{Z}_n^*$. In the case that $n = p$ is a prime, we restate Proposition 5 and give a detailed proof.

Proposition 7.

Let ζ_p denote a primitive pth root of unity and let $L = \mathbb{Q}(\zeta_p)$. Then

$$\Theta(L) = (LC_p)^F = (\mathbb{Q}C_p)^*,$$

where $F = \mathrm{Aut}(C_p) = \mathbb{Z}_p^*$.

Proof.

Let $C_p = \langle \sigma \rangle$ and let $r \in \mathbb{Z}_p^*$ be a primitive root modulo p. Let $\zeta = \zeta_p$. Then $L = \mathbb{Q}(\zeta)$ is Galois with group $\mathbb{Z}_p^* \cong C_{p-1} = \langle g \rangle$.

The Galois action is given as $g^i(\zeta) = \zeta^{r^i}$ and the action of $\mathbb{Z}_p^* = \mathrm{Aut}(C_p)$ on C_p is given as $g^i(\sigma) = \sigma^{r^i}$.

A typical element of LC_p is $\sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-2} \alpha_{ij} \zeta^j \right) \sigma^i$ for $\alpha_{ij} \in \mathbb{Q}$. To be in $(LC_p)^F$, we require that

$$g^k\left(\sum_{i=0}^{p-1}\left(\sum_{j=0}^{p-2}\alpha_{ij}\zeta^j\right)\sigma^i\right)=\sum_{i=0}^{p-1}\left(\sum_{j=0}^{p-2}\alpha_{ij}\zeta^{r^kj}\right)\sigma^{r^ki}=\sum_{i=0}^{p-1}\left(\sum_{j=0}^{p-2}\alpha_{ij}\zeta^j\right)\sigma^i,$$

for $0 \le k \le p-2$.

Thus, $(LC_p)^F$ is generated as a $\mathbb{Q}$-algebra by the quantities

$$X_i=\sum_{j=0}^{p-2}\zeta^{ir^j}\sigma^{r^j}$$

for $0 \le i \le p-2$.
And as is well-known, the quantities

$$\{(1+X_0)/p,(1+X_1)/p,\ldots,(1+X_{p-2})/p,(1-X_0-X_1-\cdots-X_{p-2})/p\}$$

are the p minimal orthogonal idempotents for $(\mathbb{Q}C_p)^*$.

$\square$

Proposition 8.

Let $(\mathbb{Q}C_p)^*$ be the absolutely semisimple Hopf form of $\mathbb{Q}C_p$.

(i) As $\mathbb{Q}$-algebras,

$$(\mathbb{Q}C_p)^* \cong \mathbb{Q}[X_0, X_1, \ldots, X_{p-2}]/I$$

where I is the ideal of $\mathbb{Q}[X_0, X_1, \ldots, X_{p-2}]$ generated by

$$\{(X_i - (p-1))(X_i + 1)\}, \quad 0 \leq i \leq p-2$$

and

$$\{(X_i + 1)(X_j + 1)\}, \quad 0 \leq i, j \leq p-2, \quad i < j.$$

(ii) *The $\mathbb{Q}$-Hopf algebra structure of $(\mathbb{Q}C_p)^*$ is given as*

$$\varepsilon(X_0) = p - 1,$$

$$\varepsilon(X_1) = \varepsilon(X_2) = \cdots = \varepsilon(X_{p-2}) = -1,$$

$$S(X_0) = X_0,$$

$$S(X_1) = -\sum_{i=0}^{p-2} X_i,$$

$$S(X_i) = X_{p-i}, \quad 2 \le i \le p-2,$$

and, with $X_{p-1} = S(X_1)$,

$$\Delta(X_i) = \left(\frac{1}{p}\sum_{j=0}^{p-1}(1 + X_{p-j}) \otimes (1 + X_{i+j})\right) - (1 \otimes 1),$$

for $0 \le i \le p-2$, where the subscripts are taken modulo p.

Proof.

For (i): The linear dual $(\mathbb{Q}C_p)^*$ is generated as a $\mathbb{Q}$-algebra by $X_0, X_1, \ldots, X_{p-2}$. For $0 \le i \le p-2$,

$$\left(\frac{X_i+1}{p}\right)\left(\frac{X_i+1}{p}\right) = \frac{X_i+1}{p}.$$

Thus

$$(X_i+1)(X_i+1) = p(X_i+1),$$

hence

$$(X_i-(p-1))(X_i+1) = 0, \quad 0 \le i \le p-2.$$

For $0 \le i,j \le p-2$, $i<j$,

$$\left(\frac{X_i+1}{p}\right)\left(\frac{X_j+1}{p}\right) = 0,$$

hence

$$(X_i+1)(X_j+1) = 0, \quad 0 \le i,j \le p-2, i<j.$$

For (ii): The dual $(\mathbb{Q}C_p)^*$ is a $\mathbb{Q}$-Hopf form of $\mathbb{Q}C_p$ with Hopf structure induced from that of LC_p, $L = \mathbb{Q}(\zeta_p)$.

Example 9.

Let $C_5 = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4\}$. Then

$$\mathrm{Aut}(C_5) = C_4 = \langle g \rangle = \{1, g, g^2, g^3\},$$

with action given as

$$1(\sigma) = \sigma, \quad g(\sigma) = \sigma^2, \quad g^2(\sigma) = \sigma^4, \quad g^3(\sigma) = \sigma^3.$$

Let $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ be the 5th cyclotomic polynomial. Then

$$L = \mathbb{Q}[x]/(\Phi_5(x)) = \mathbb{Q}(\zeta_5);$$

L is Galois with group C_4, with Galois action given as $g(\zeta) = \zeta^2$. The absolutely semisimple Hopf form of $\mathbb{Q}C_5$ is

$$\Theta(L) = (LC_5)^{C_4} = (\mathbb{Q}C_5)^*.$$

As a $\mathbb{Q}$-algebra, $(\mathbb{Q}C_5)^*$ is generated by

$$X_0 = \sigma + \sigma^2 + \sigma^4 + \sigma^3, \quad X_1 = \zeta\sigma + \zeta^2\sigma^2 + \zeta^4\sigma^4 + \zeta^3\sigma^3,$$

$$X_2 = \zeta^2\sigma + \zeta^4\sigma^2 + \zeta^3\sigma^4 + \zeta\sigma^3, \quad X_3 = \zeta^3\sigma + \zeta\sigma^2 + \zeta^2\sigma^4 + \zeta^4\sigma^3.$$

We have

$$(\mathbb{Q}C_5)^* = \mathbb{Q}[X_0, X_1, X_2, X_3]/I,$$

where the ideal I is generated by

$$(X_0-4)(X_0+1), \quad (X_1-4)(X_1+1), \quad (X_2-4)(X_2+1), \quad (X_3-4)(X_3+1),$$

$$(X_0+1)(X_1+1), \quad (X_0+1)(X_2+1), \quad (X_0+1)(X_3+1),$$

$$(X_1+1)(X_2+1), \quad (X_1+1)(X_3+1),$$

$$(X_2+1)(X_3+1).$$

The Hopf algebra structure of $(\mathbb{Q}C_5)^*$ is given by

$$\varepsilon(X_0) = 4, \quad \varepsilon(X_1) = \varepsilon(X_2) = \varepsilon(X_3) = -1,$$

$$S(X_0) = X_0, \quad S(X_1) = -X_0 - X_1 - X_2 - X_3,$$

$$S(X_2) = X_3, \quad S(X_3) = X_2,$$

and

$$\begin{aligned}\Delta(X_0) &= \frac{1}{5}(1+X_0)\otimes(1+X_0) + \frac{1}{5}(1-X_0-X_1-X_2-X_3)\otimes(1+X_1)\\ &+ \frac{1}{5}(1+X_3)\otimes(1+X_2) + \frac{1}{5}(1+X_2)\otimes(1+X_3)\\ &+ \frac{1}{5}(1+X_1)\otimes(1-X_0-X_1-X_2-X_3) - 1\otimes 1,\end{aligned}$$

$$\begin{aligned}\Delta(X_1) &= \frac{1}{5}(1+X_0)\otimes(1+X_1) + \frac{1}{5}(1-X_0-X_1-X_2-X_3)\otimes(1+X_2)\\ &+ \frac{1}{5}(1+X_3)\otimes(1+X_3) + \frac{1}{5}(1+X_2)\otimes(1-X_0-X_1-X_2-X_3)\\ &+ \frac{1}{5}(1+X_1)\otimes(1+X_0) - 1\otimes 1,\end{aligned}$$

$$
\begin{aligned}
\Delta(X_2) \quad = \quad & \frac{1}{5}(1+X_0)\otimes(1+X_2)+\frac{1}{5}(1-X_0-X_1-X_2-X_3)\otimes(1+X_3) \\
& + \frac{1}{5}(1+X_3)\otimes(1-X_0-X_1-X_2-X_3)+\frac{1}{5}(1+X_2)\otimes(1+X_0) \\
& \quad + \frac{1}{5}(1+X_1)\otimes(1+X_1)-1\otimes 1,
\end{aligned}
$$

$$
\begin{aligned}
\Delta(X_3) \quad = \quad & \frac{1}{5}(1+X_0)\otimes(1+X_3) \\
& +\frac{1}{5}(1-X_0-X_1-X_2-X_3)\otimes(1-X_0-X_1-X_2-X_3) \\
& + \frac{1}{5}(1+X_3)\otimes(1+X_0)+\frac{1}{5}(1+X_2)\otimes(1+X_1) \\
& \quad + \frac{1}{5}(1+X_1)\otimes(1+X_2)-1\otimes 1.
\end{aligned}
$$

4. The Group of Points

Let

$$(\mathbb{Q}C_p)^* = \mathbb{Q}[X_0, X_1, \ldots, X_{p-2}]/I$$

be the absolutely semisimple Hopf form of $\mathbb{Q}C_p$. Let V be the set of common zeros of the polynomials in the ideal I.

V consists of p points of $\mathbb{Q}^{p-1}$

$$P_1, P_2, \ldots, P_{p-1}, P_p$$

where for $1 \leq i \leq p-1$, P_i is the point that has $p-1$ in the ith component and -1 elsewhere, and P_p has -1 in each component.

Let

$$\mathrm{G} = \mathrm{Hom}_{\mathbb{Q}\text{-alg}}((\mathbb{Q}C_p)^*, -)$$

be the $\mathbb{Q}$-group scheme represented by $(\mathbb{Q}C_p)^*$.

It is well-known that there is a group isomorphism

$$\mathrm{G}(\mathbb{Q}) = V \cong C_p$$

defined by $\overline{X}_i \mapsto x_i$, where x_i is the ith component of $P \in V$, $1 \leq i \leq p-1$ [14, Section 1.2, Theorem], [14, Section 2.3].

In more detail: V is endowed with a binary operation (point addition) induced from comultiplication. Point addition is defined as follows.

For $P = (x_0, x_1, \ldots, x_{p-2})$, $Q = (y_0, y_1, \ldots, y_{p-1})$ in V,

$$P + Q = R = (z_0, z_1, \ldots, z_{p-2}),$$

where

$$z_0 = \frac{1}{p}((1 + x_0)(1 + y_0) + (1 - \sum_{i=0}^{p-2} x_i)(1 + y_1) + (1 + x_{p-2})(1 + y_2)$$

$$+ \cdots + (1 + x_2)(1 + y_{p-2}) + (1 + x_1)(1 - \sum_{i=0}^{p-2} y_i) - 1,$$

$$\vdots$$

$$z_{p-2} = \frac{1}{p}((1 + x_0)(1 + y_{p-2}) + (1 - \sum_{i=0}^{p-2} x_i)(1 - \sum_{i=0}^{p-2} y_i) + (1 + x_{p-2})(1 + y_0)$$

$$+(1 + x_{p-3})(1 + y_1) + \cdots + (1 + x_1)(1 + y_{p-3})) - 1.$$

The identity element in V is the point

$$O = P_1 = (\varepsilon(X_0), \varepsilon(X_1), \varepsilon(X_2), \ldots, \varepsilon(X_{p-2}))$$

$$= (p-1, -1, -1, \ldots, -1);$$

the inverse of the point $P = (x_0, x_1, x_2, \ldots, x_{p-3}, x_{p-2}) \in V$ is

$$-P = (S(X_0), S(X_1), S(X_2), \ldots, S(X_{p-2})$$

$$= (x_0, -\sum_{i=0}^{p-2} x_i, x_{p-2}, x_{p-3}, \ldots, x_3, x_2),$$

where we identify $S(X_i)$ with its image under the $\mathbb{Q}$-algebra homomorphism $\overline{X}_i \mapsto x_i$.

Thus V is a group with p elements, which must be isomorphic to C_p.

Example 10.

From Example 9

$$(\mathbb{Q}C_5)^* = \mathbb{Q}[X_0, X_1, X_2, X_3]/I$$

is the absolutely semisimple Hopf form of $\mathbb{Q}C_5$. The set of common zeros of the polynomials in I is

$$V = \{(4, -1, -1, -1), (-1, 4, -1, -1), (-1, -1, 4, -1),$$

$$(-1, -1, -1, 4), (-1, -1, -1, -1)\},$$

with $V \cong C_5$, where V is endowed with point addition.

The identity element is $O = P_1 = (4, -1, -1, -1)$, the inverse of $P_2 = (-1, 4, -1, -1)$ is $P_5 = (-1, -1, -1, -1)$, and the inverse of $P_3 = (-1, -1, 4, -1)$ is $P_4 = (-1, -1, -1, 4)$.

For instance,

$$\begin{aligned} P_3 + O &= (-1,-1,4,-1) + (4,-1,-1,-1) \\ &= (-1,-1,4,-1) \\ &= P_3, \end{aligned}$$

and

$$\begin{aligned} 2P_2 &= 2(-1,4,-1,-1) \\ &= (-1,4,-1,-1) + (-1,4,-1,-1) \\ &= (-1,-1,4,-1) \\ &= P_3. \end{aligned}$$

5. Connection to Hopf-Galois Theory

5.1 Brief Review of Greither-Pareigis

Let E/K be a Galois extension with group G. Let H be a finite dimensional, cocommutative K-Hopf algebra.

Suppose there is a K-linear action $\cdot$ of H on E that satisfies

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

for all $h \in H,\ x, y \in E$, where $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$ is Sweedler notation. Suppose also that the K-linear map

$$j : E \otimes_K H \to \mathrm{End}_K(E),\ j(x \otimes h)(y) = x(h \cdot y)$$

is an isomorphism of vector spaces over K. Then H together with this action, denoted as $(H, \cdot)$, provides a **Hopf-Galois structure** on E/K.

Two Hopf-Galois structures $(H_1, \cdot_1)$, $(H_2, \cdot_2)$ on E/K are **isomorphic** if there is a Hopf algebra isomorphism $f : H_1 \to H_2$ for which $h \cdot_1 x = f(h) \cdot_2 x$ for all $x \in E$, $h \in H$ (see [4, Introduction]).

C. Greither and B. Pareigis [5] have given a complete classification of Hopf-Galois structures up to isomorphism.

Theorem 11 (Greither and Pareigis).

Let E/K be a Galois extension with group G. There is a one-to-one correspondence between isomorphism classes of Hopf Galois structures on E/K and regular subgroups of $\mathrm{Perm}(G)$ that are normalized by $\lambda(G)$.

One direction of this correspondence works by Galois descent:

Let N be a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$; G acts on the group algebra EN through the Galois action on E and conjugation by $\lambda(G)$ on N, i.e.,

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

where ${}^{g}\eta$ denotes the conjugation action of $\lambda(g) \in \lambda(G)$ on $\eta \in N$.

Let

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

be the fixed ring H under the action of G. Then H is an n-dimensional E-Hopf algebra, $n = [E : K]$, and E/K admits the Hopf Galois structure $(H, \cdot)$.

By [5, p. 249, proof of 3.1, (a) $\Longrightarrow$ (b)],

$$E \otimes_K H \cong E \otimes_K KN \cong EN,$$

as E-Hopf algebras, so H is an E-form of KN.

Let N be a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$, and let $(H, \cdot)$ be the corresponding Hopf-Galois structure. If N is isomorphic to the abstract group N', then we say that the Hopf-Galois structure $(H, \cdot)$ on E/K is of **type** N'.

5.2 Hopf Forms and Hopf-Galois Structures

If $(H, \cdot)$ is a Hopf-Galois structure on E/K of type N, then the Hopf algebra H is a Hopf form of KN. Thus H can be recovered via Theorem 1. In other words, with $F = \mathrm{Aut}(N)$, there is an F-Galois extension L of K with

$$\Theta(L) = H = (LN)^F.$$

As we have noted (Remark 3), it is not clear how to compute the required L; the inverse map

$$\Theta^{-1} : \mathcal{H}opf(KN) \to \mathcal{G}al(K, F)$$

is not given explicitly.

Here is one way to find L.

Proposition 12.

Let E/K be a Galois extension with group G. Let $(H, \cdot)$ be a Hopf-Galois structure corresponding to regular subgroup N. Let $F = \mathrm{Aut}(N)$, let

$$W = \{g \in \lambda(G) : \ {}^{g}\eta = \eta, \forall \eta \in N\},$$

and let $L = E^W$. If W is a normal subgroup of $\lambda(G)$ with $\lambda(G)/W \cong F$, then $\Theta(L) = H$.

Proof.

By the Fundamental theorem of Galois theory, $L = E^W$ is Galois with group $F \cong \lambda(G)/W$, so L is an F-Galois extension. Now,

$$H = (EN)^G = (LN)^F,$$

and so, $\Theta(L) = H$. □

Example 13.

We consider the splitting field E of the polynomial $x^4 - 10x^2 + 1$ over $\mathbb{Q}$. One has $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$; $E/\mathbb{Q}$ is Galois with group $C_2 \times C_2 = \{1, \sigma, \tau, \tau\sigma\}$ with Galois action

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

By [1], there are three Hopf-Galois structures on $E/\mathbb{Q}$ of type C_4, each of which is determined by a regular subgroup $N \cong C_4$ normalized by $\lambda(C_2 \times C_2)$. One such N is given as

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

where $1 := 1$, $2 := \sigma$, $3 := \tau$, $4 := \tau\sigma$, and

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

N is a regular subgroup of $\mathrm{Perm}(C_2 \times C_2)$ normalized by $\lambda(C_2 \times C_2)$ with $N \cong C_4$.

Let $(H, \cdot)$ be the corresponding Hopf-Galois extension with $H = (EN)^G$.

As one can check

$$W = \{g \in \lambda(C_2 \times C_2) : {}^g\eta = \eta, \forall \eta \in N\} = \{(1), (1,2)(3,4)\} = \{1, \sigma\}.$$

We have $G/W \cong F = \mathrm{Aut}(C_4) \cong C_2$, and the fixed field $L = E^W = \mathbb{Q}(\sqrt{2})$ is an F-Galois extension of $\mathbb{Q}$.

So by Proposition 12, $\Theta(L) = H$.

6. Absolutely Semisimple Hopf-Galois Structures

Let $E/\mathbb{Q}$ be Galois with group G, $n = |G|$.

When does $E/\mathbb{Q}$ admit a Hopf-Galois structure whose Hopf algebra is the absolutely semisimple Hopf form $(\mathbb{Q}C_n)^*$ of $\mathbb{Q}C_n$?

Proposition 14.

Let $E/\mathbb{Q}$ be a Galois extension with group G, $n = |G|$. Suppose $E/\mathbb{Q}$ admits the Hopf-Galois structure $((\mathbb{Q}C_n)^*, \cdot)$. Then $\phi(n) \mid n$, where ϕ is Euler's function.

Proof.

Let N be the regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$ that corresponds to $((\mathbb{Q}C_n)^*, \cdot)$. Then

$$E \otimes_{\mathbb{Q}} (\mathbb{Q}C_n)^* \cong EN$$

as Hopf algebras. Thus $(\mathbb{Q}C_n)^*$ is an E-Hopf form of $\mathbb{Q}N$ and $E \otimes_{\mathbb{Q}} (\mathbb{Q}C_n)^* \cong (EC_n)^* \cong EN$, as E-Hopf algebras. The dual $(EC_n)^*$ decomposes as $\underbrace{E \times E \times \cdots \times E}_{n}$, thus

$EN \cong \underbrace{E \times E \times \cdots \times E}_{n}$, and so, $(EN)^* \cong EN$, as Hopf algebras.

Hence, $EN \cong EC_n$ as E-Hopf algebras, and so, $C_n \cong N$. We conclude that E contains $\mathbb{Q}[x]/(\Phi_n(x))$. Thus E contains a subfield of degree $\phi(n)$ over $\mathbb{Q}$. Hence $\phi(n) \mid n$.

□

Proposition 15.

Let $n > 2$. Then $\phi(n) \mid n$ if and only if $n = 2^a 3^b$ where $a > 0$, $b \geq 0$.

Proof.

Suppose that $\phi(n) \mid n$. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where p_i are distinct primes, and $e_i > 0$. Then

$$\phi(n) = (p_1 - 1)p_1^{e_1 - 1}(p_2 - 1)p_2^{e_2 - 1} \cdots (p_k - 1)p_k^{e_k - 1}.$$

Since $n > 2$, $\phi(n)$ is even, and so, n is even. Thus, $p_1 = 2$ in the prime factorization of n. Suppose that n has two odd prime factors p_i, p_j. Since $e_i, e_j > 0$, both $p_i - 1$ and $p_j - 1$ are even, and so, $2^{e_1+1} \mid \phi(n)$, hence $2^{e_1+1} \mid n$, which is a contradiction. Thus, n has only one odd prime factor, say p, hence $n = 2^{e_1} p^e$, $e > 0$. Now, $(p - 1) \mid \phi(n)$, thus $(p - 1) \mid n$. Consequently, $(p - 1) = 2^r$ for some $r > 0$ and $2^{e_1 - 1 + r} \mid \phi(n)$, thus $2^{e_1 - 1 + r} \mid n$. It follows that $r = 1$ and so $p = 3$. Hence $n = 2^a 3^b$ where $a, b > 0$.

For the converse, suppose that $n = 2^a 3^b$, $a > 0$, $b \geq 0$. If $b = 0$, then $\phi(n) = 2^{a-1}$ which divides n. If $b > 0$, then $\phi(n) = 2^{a-1} \cdot 2 \cdot 3^{b-1} = 2^a 3^{b-1}$ which divides n.

$\square$

Proposition 14 and Proposition 15 yield necessary conditions for the Galois extension $E/\mathbb{Q}$ with group G, $n = |G|$, to admit the Hopf-Galois structure $((\mathbb{Q}C_n)^*, \cdot)$, namely,

(i) $n = 2^a 3^b$, $a > 0$, $b \geq 0$,
(ii) $E/\mathbb{Q}$ admits a Hopf-Galois structure of type C_n.

Example 16.

Consider the splitting field E of the polynomial $x^4 - 2x^2 + 9$ over $\mathbb{Q}$. We show that $E/\mathbb{Q}$ admits the Hopf-Galois structure $((\mathbb{Q}C_4)^*, \cdot)$. We have $E = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$; $E/\mathbb{Q}$ is Galois with group $C_2 \times C_2 = \{1, \sigma, \tau, \tau\sigma\}$ with Galois action

$$\sigma(\sqrt{-1}) = \sqrt{-1}, \quad \sigma(\sqrt{2}) = -\sqrt{2},$$

$$\tau(\sqrt{-1}) = -\sqrt{-1}, \quad \tau(\sqrt{2}) = \sqrt{2}.$$

Note that $n = 4 = 2^2 3^0$. As in Example 13, there are three Hopf-Galois structures on $E/\mathbb{Q}$ of type C_4, one of them is given by the regular subgroup

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

Let $(H, \cdot)$ be the Hopf-Galois structure determined by N, $H = (EN)^{C_2 \times C_2}$.

As in Example 13,

$$W = \{g \in \lambda(C_2 \times C_2) : {}^g\eta = \eta, \forall \eta \in N\} = \{(1), (1,2)(3,4)\} = \{1, \sigma\}.$$

Thus W is a normal subgroup of $\lambda(C_2 \times C_2)$ with $G/W \cong C_2 \cong F = \mathrm{Aut}(C_4)$.

We have $L = E^W = \mathbb{Q}(\sqrt{-1})$, thus L is F-Galois. Hence by Proposition 12,

$$\Theta(L) = H.$$

But $L = \mathbb{Q}(\zeta_4)$, and so, $\Theta(L) = H = (\mathbb{Q}C_4)^*$ by Proposition 5.

Example 17.

We take $E/\mathbb{Q}$ to be the splitting field of $x^3 - 2$ over $\mathbb{Q}$, then $n = 6 = 2 \cdot 3$. As shown in [8, Section 7], $E/\mathbb{Q}$ admits a Hopf-Galois structure of type C_6 whose Hopf algebra is the absolutely semisimple Hopf form $(\mathbb{Q}C_6)^*$ of $\mathbb{Q}C_6$.

Remark 18.

Recently, T. Kohl [9] has determined whether or not a Galois extension with group G, $n = |G|$, admits a Hopf-Galois structure of type C_n for various G. For example, if $E/\mathbb{Q}$ is Galois with group A_4, then there are no Hopf-structures of type C_{12}. Thus $E/\mathbb{Q}$ cannot have a Hopf-Galois structure with Hopf algebra $(\mathbb{Q}C_{12})^*$.

Remark 19 (Galois theoretical embedding problem).

[10, Introduction]. Let $L = \mathbb{Q}(\zeta_n)$, $n > 2$, *be the Galois extension of* $\mathbb{Q}$ *with group* $\mathbb{Z}_n^* = \mathrm{Aut}(C_n)$. *Does there exist a Galois extension* $E/\mathbb{Q}$ *with group* G, *and a short exact sequence of groups*

$$1 \to T \to G \to \mathbb{Z}_n^* \to 1,$$

so that $E^T = \mathbb{Q}(\zeta_n)$? *If this is the case, suppose further that* $E/\mathbb{Q}$ *admits a Hopf-Galois structure corresponding to regular subgroup* $N \cong C_n$, *with*

$$W = \{g \in \lambda(G) : \, {}^g\eta = \eta, \forall \eta \in N\} = T.$$

Then $E/\mathbb{Q}$ *admits the Hopf-Galois structure* $((\mathbb{Q}C_n)^*, \cdot)$.

Remark 20.

Regarding Remark 19, perhaps the Galois theoretical embedding problem would be easier to solve if $n = 2 \cdot 3^b$*,* $b > 0$*. For then* $\mathbb{Z}_n^*$ *is cyclic of order* $\phi(n)$ *[7, Proposition 4.1.3].*

Question 21.

Consider the construction of the absolutely semisimple Hopf form $(\mathbb{Q}C_p)^*$ of Proposition 7. Suppose that the $\mathbb{Q}$-basis for $L = \mathbb{Q}(\zeta)$ is changed to the normal basis on the generator $-\zeta$, i.e.,

$$\{-\zeta, g(-\zeta), g^2(-\zeta), \ldots, g^{p-2}(-\zeta)\},$$

or to some other $\mathbb{Q}$-basis given by powers of $a + b\zeta$, $a, b \in \mathbb{Q}$. How does this change of basis affect the generators and relations of $(\mathbb{Q}C_p)^*$ and the points of the variety V?

Question 22.

Given two Hopf forms H, H' of KC_n when do we have $H \cong H'$ as K-Hopf algebras? as K-algebras? (This is analogous to the question for Hopf-Galois structures.)

Question 23 (Pareigis).

Let N be any finite group. By Maschke's theorem, $\mathbb{Q}N$ is semisimple. Extending scalars to $\mathbb{C}$ yields the Wedderburn-Artin decomposition

$$\mathbb{C}N \cong \mathrm{Mat}_{n_1}(\mathbb{C}) \times \mathrm{Mat}_{n_2}(\mathbb{C}) \times \cdots \times \mathrm{Mat}_{n_l}(\mathbb{C}).$$

A Hopf form H of $\mathbb{Q}N$ is **absolutely semisimple** *if*

$$H \cong \mathrm{Mat}_{n_1}(\mathbb{Q}) \times \mathrm{Mat}_{n_2}(\mathbb{Q}) \times \cdots \times \mathrm{Mat}_{n_l}(\mathbb{Q}).$$

For which groups N does $\mathbb{Q}N$ admit an absolutely semisimple Hopf form?

We address this question for various groups. First we consider abelian groups, then non-abelian groups.

Example 24.

Let $N = C_n$, $n \geq 1$. By Theorem 4, $(\mathbb{Q}C_n)^* \cong \mathbb{Q}^n$ is the absolutely semisimple Hopf form of $\mathbb{Q}C_n$. By Proposition 5, $\Theta(L) = (\mathbb{Q}C_n)^*$, where $L = \mathbb{Q}(\zeta_n)$.

Example 25.

Let $N = C_p^n$, $p \geq 2$, $n \geq 1$; C_p^n is the elementary abelian group of order p^n. Then $\mathbb{Q}C_p^n$ admits the absolutely semisimple Hopf form

$$(\mathbb{Q}C_p^n)^* \cong \mathbb{Q}^{p^n}.$$

So there is an $\mathrm{Aut}(C_p^n)$-Galois extension $L/\mathbb{Q}$ for which

$$\Theta(L) = (\mathbb{Q}C_p^n)^*.$$

What is the structure of L?

Proposition 26.

Let

$$L = \mathbb{Q}(\zeta_p)^{\frac{\prod_{i=0}^{n-1}(p^n - p^i)}{p-1}}.$$

Then L is an $\mathrm{Aut}(C_p^n)$-Galois extension of $\mathbb{Q}$ with $\Theta(L) = (\mathbb{Q}C_p^n)^*$.

Proof.
(Sketch) $\mathrm{Aut}(C_p^n) = \mathrm{GL}_n(\mathbb{F}_p)$ and

$$|\mathrm{GL}_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1}(p^n - p^i).$$

For $1 \leq j \leq n$, there is a subgroup U_j of $\mathrm{GL}_n(\mathbb{F}_p)$ given as

$$U_j = \{\mathrm{diag}(1, \ldots, 1, a^{(j)}, 1, \ldots, 1) : \ a^{(j)} \in \mathbb{F}_p^*\} \cong \mathbb{F}_p^*.$$

The index is $[\mathrm{GL}_n(\mathbb{F}_p) : U_j] = (\prod_{i=0}^{n-1}(p^n - p^i))/(p-1)$; $\mathbb{Q}(\zeta_p)$ is a U_j-Galois extension of fields. Thus by [12, Theorem 4.2],

$$L = \mathbb{Q}(\zeta_p)^{\frac{\prod_{i=0}^{n-1}(p^n - p^i)}{p-1}}$$

is $\mathrm{GL}_n(\mathbb{F}_p)$-Galois. Moreover, $\Theta(L) = (\mathbb{Q}C_p^n)^*$.

$\square$

Example 27.

Let $N = D_3$. Then

$$\mathbb{Q}D_3 \cong \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

Thus $\mathbb{Q}D_3$ is an absolutely semisimple Hopf form of itself.

Example 28.

Let $N = D_4$. Then

$$\mathbb{Q}D_4 \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathrm{Mat}_2(\mathbb{Q}).$$

Thus $\mathbb{Q}D_4$ is an absolutely semisimple Hopf form of itself.

Example 29.

Let $N = Q_8$, the quaternion group. We have

$$\mathbb{C}Q_8 \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_2(\mathbb{C}),$$

yet

$$\mathbb{Q}Q_8 \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{H},$$

where $\mathbb{H}$ is the rational quaternions. Thus $\mathbb{Q}Q_8$ is not an absolutely semisimple form of itself.

Does $\mathbb{Q}Q_8$ admit an absolutely semisimple Hopf form?

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

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

3. L. N. Childs, Hopf Galois structures on Kummer extensions of prime power degree, *New York J. Math.*, **17**, 2011, 51-74.

4. T. Crespo, A. Rio, M. Vela, Non-isomorphic Hopf-Galois structures with isomorphic underlying Hopf algebras, *J. Algebra*, {bf 455, (2015), 270-276.

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

6. R. Haggenmüller, B. Pareigis, Hopf algebra forms on the multiplicative group and other groups, *manuscripta math.*, **55**, (1986), 121-135.

7. K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2ed., GTM, 84, Springer-Verlag, New York, 1990.

8. A. Koch, T. Kohl, P. Truman, R. Underwood, 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, (2019).

9. T. Kohl, Characteristic subgroup lattices and Hopf-Galois structures, *Int. J. of Alg. and Comp.*, **29**(02), 391-405 (2019).

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

11. B. Pareigis, Twisted group rings, *Comm. Alg.*, **17**(12), 1989, 2923-2939.

12. B. Pareigis, Forms of Hopf algebras and Galois theory, *Topics in Algebra*, Banach Center Publications, **26**, Part 1, PWN Polish Scientific Publishers, 1990.

13. C. Small, The Group of quadratic extensions, *J. Pure Appl. Alg.*, **2**, (1972), 83-105.

14. W. Waterhouse, Introduction to Affine Group Schemes, Springer-Verlag, New York, 1979.