Publ. Mat. **60** (2016), 221–234
DOI: 10.5565/PUBLMAT_60116_08

ON THE GALOIS CORRESPONDENCE THEOREM IN SEPARABLE HOPF GALOIS THEORY

Teresa Crespo, Anna Rio, and Montserrat Vela

Abstract: In this paper we present a reformulation of the Galois correspondence theorem of Hopf Galois theory in terms of groups carrying farther the description of Greither and Pareigis. We prove that the class of Hopf Galois extensions for which the Galois correspondence is bijective is larger than the class of almost classically Galois extensions but not equal to the whole class. We show as well that the image of the Galois correspondence does not determine the Hopf Galois structure.

2010 Mathematics Subject Classification: Primary: 12F10; Secondary: 13B05, 16T05.

Key words: Hopf algebra, Hopf Galois theory, Galois correspondence.

1. Introduction

A finite field extension K/k is a Hopf Galois extension if there exists a finite cocommutative k-Hopf algebra H such that K is an H-module algebra and the k-linear map $j\colon K \otimes_k H \to \operatorname{End}_k(K)$, defined by $j(s \otimes h)(t) = s(ht)$ for $h \in H$, $s, t \in K$, is bijective. Clearly a finite Galois extension K/k with Galois group G is a Hopf Galois extension with Hopf algebra the group algebra $k[G]$.

The concept of Hopf Galois extension was introduced by Chase and Sweedler to study inseparable extensions. For a Hopf Galois extension K/k with Hopf algebra H, they prove that the map from the set of sub-Hopf algebras of H to the set of intermediate fields of K/k sending a sub-Hopf algebra H' of H to the subfield of K fixed by H' is inclusion reversing and injective [**3**, Theorem 7.6].

Greither and Pareigis [**8**, Theorem 2.1] give a characterization and classification of Hopf Galois structures on separable field extensions, achieved by transforming the problem into a group-theoretic one involving the Galois group G of the Galois closure of the field extension

T. Crespo acknowledges support by grants MTM2012-33830, Spanish Science Ministry, and 2009SGR 1370; A. Rio and M. Vela acknowledge support by grants MTM2012-34611, Spanish Science Ministry, and 2009SGR 1220.

considered. They introduce the subclass of almost classically Galois extensions, which can be given a Hopf Galois structure such that the Galois correspondence is bijective, prove that all extensions of degree smaller than five are almost classically Galois, and provide an example of a Hopf Galois extension which is not almost classically Galois, namely a degree 16 extension of a quadratic number field (see [**8**, §4]). In [**6**], we checked that all Hopf Galois extensions of degree up to 7 are almost classically Galois and we presented an example of a degree 8 extension of $\mathbf{Q}$ which is Hopf Galois but not almost classically Galois (*loc. cit.* Example 2.1).

In [**5**], Childs uses Hopf Galois structures to obtain arithmetic properties of wildly ramified extensions. A more detailed account of concepts and achievements in Hopf Galois theory can be found in [**7**].

In contrast to what happens in the Galois case, the Hopf Galois structure is not unique in general. This fact raises the question on the number of different Hopf Galois structures which can be given to a Galois extension (see e.g. [**1**], [**2**]). A different question which has hardly been considered concerns the image of the Galois correspondence for each of the Hopf Galois structures, i.e. which intermediate fields are fixed fields of a sub-Hopf algebra of the Hopf algebra. In this context we may ask whether the class of Hopf Galois extensions admitting a Hopf Galois structure for which the Galois correspondence is bijective is bigger than the class of almost classically extensions, if different Hopf Galois structures may have Galois correspondences with the same image or more generally which are the sublattices of the lattice of intermediate fields of the extension corresponding to some Hopf Galois structure.

In this paper we give a reformulation of the Galois correspondence theorem in term of groups, carrying farther the description of Greither and Pareigis. We approach the question on the image of the Galois correspondence by studying two different families of field extensions. For the first one, we consider extensions whose Galois closure has Galois group the Frobenius group $F_{p(p-1)}$, for p prime. We obtain non almost classically Galois extensions which may be given a Hopf Galois structure for which the Galois correspondence is bijective and different Hopf Galois structures giving the same image for the Galois correspondence. For the second family, we consider Galois extensions with Galois group the dihedral group D_{2p}. In this case, each of the Hopf Galois structures provides a different sublattice of the lattice of intermediate extensions. The fact that there are non almost classically Galois extensions which may be endowed with a Hopf Galois structure giving a bijective Galois correspondence raises the question whether all Hopf Galois extensions may be endowed with such a Hopf Galois structure. In the last section we answer this question negatively by exhibiting a Hopf Galois extension for which no Hopf Galois structure gives a bijective Galois correspondence.

2. A reformulation of the Galois correspondence theorem in terms of groups

In the sequel, we shall use the following notation. K/k denotes a separable extension, n its degree, $\widetilde{K}/k$ its Galois closure, $G = \mathrm{Gal}(\widetilde{K}/k)$, and $G' = \mathrm{Gal}(\widetilde{K}/K)$.

In the separable case the Hopf algebras giving a Hopf Galois structure are forms of some group algebra. More precisely they are Hopf algebras of the form $\widetilde{K}[N]^G$ with N as in [**8**, Theorem 2.1]. The result in the following proposition seems to be well-known. However, since neither the authors nor the experts consulted know a reference for it we are including a short proof. We thank Akira Masuoka for sending it to us.

Proposition 2.1. *Let k be a field and G a group. The sub-Hopf algebras of $k[G]$ are the group algebras $k[H]$, with H a subgroup of G.*

Proof: Given a non-empty set X, it spans a coalgebra $C = k[X]$, in which every element of X is grouplike. Every subcoalgebra D of C is spanned by grouplikes. For, if an element $d = \sum_{y\in Y} a_y y$ is in D, where Y is a finite subset of X, and a_y is a non-zero element in k, then one sees $y \in D$ from $(p_y \otimes \mathrm{id})\Delta(d) \in D$, where $p_y\colon C \to ky$ is the natural projection. Thus we have $D = k[G(D)]$, where $G(D) = \{\text{grouplikes of } C \text{ contained in } D\}$. If X is a monoid (or a group), D is a sub-bialgebra (or a Hopf subalgebra) if and only if $G(D)$ is a sub-monoid (or a subgroup) of X. □

For G and G' as above, we denote by λ the morphism from G into the symmetric group S_n given by the action of G on the left cosets G/G' by left translation. The result in the next proposition is implicitly contained in the proof of Theorem 5.2 in [**8**]. For the reader's convenience, we include a complete proof of it.

Proposition 2.2. *Let N be a regular subgroup of S_n normalized by $\lambda(G)$. There is a bijection between the set of k-sub-Hopf algebras of $\widetilde{K}[N]^G$ and the set of subgroups of N stable under the action of $\lambda(G)$ by conjugation.*

Proof: To a subgroup N' of N we assign the k-sub-Hopf algebra $\widetilde{K}[N']^G$ of $\widetilde{K}[N]^G$ and observe that for $\overline{N'} = \cap_{\sigma\in G}\lambda(\sigma)N'\lambda(\sigma)^{-1}$, we have $\widetilde{K}[N']^G = \widetilde{K}[\overline{N'}]^G$.

Now, if H is a k-sub-Hopf algebra of $\widetilde{K}[N]^G$, then $H \otimes \widetilde{K}$ is a $\widetilde{K}$-sub-Hopf algebra of $\widetilde{K}[N]^G \otimes \widetilde{K} \simeq \widetilde{K}[N]$ and so $H \otimes \widetilde{K} \simeq \widetilde{K}[N']$ for some subgroup N' of N. Since H is a k-algebra, we have $H = (H \otimes \widetilde{K})^G = \widetilde{K}[N']^G$.

If N' is a subgroup of N, stable under the action of $\lambda(G)$, the elements in $\widetilde{K}[N']^G$ are precisely the elements of the form $\sum_C a_C(\sum_{\tau \in C} \tau)$, where C runs over the conjugation classes of S_n having nonempty intersection with N'. Hence each k-sub-Hopf algebra of $\widetilde{K}[N]^G$ determines uniquely a stable subgroup of N. □

Now, the Galois correspondence theorem can be reformulated in the following way.

Theorem 2.3. *If K/k is a Hopf Galois extension with Hopf algebra $H = \widetilde{K}[N]^G$ for a regular subgroup N of* $\mathrm{Perm}(G/G')$*, then the map*

$$\begin{aligned} \mathcal{F}_N : \{\textit{Subgroups } N' \subseteq N \textit{ stable under } \lambda(G)\} &\longrightarrow \{\textit{Fields } E \mid k \subseteq E \subseteq K\} \\ N' &\longmapsto K^{\widetilde{K}[N']^G} \end{aligned}$$

is injective and inclusion reversing.

Remark 2.4. If the regular subgroup N of S_n normalized by $\lambda(G)$ is not contained in the alternating group A_n, then the subgroup $N_1 := N \cap A_n$ is stable under conjugation by $\lambda(G)$ and has index 2 in N. We have $\dim_k \widetilde{K}[N]^G = n$ and $\dim_k \widetilde{K}[N_1]^G = n/2$. The field $\mathcal{F}_N(N_1)$ is then a quadratic extension of k. Thus, if $N \not\subset A_n$, we get at least one nontrivial intermediate field in the image of the Galois correspondence.

3. A family of Hopf Galois extensions

We consider an extension K_0/k of prime degree $p \geq 5$ with Galois closure $\widetilde{K}$ such that the Galois group G of $\widetilde{K}|k$ is the Frobenius group $F_{p(p-1)}$. The group $\mathrm{Gal}(\widetilde{K}/K_0)$ is a Frobenius complement of $F_{p(p-1)}$. Let d be a divisor of $p-1$, $1 < d < p-1$, G' the subgroup of $\mathrm{Gal}(\widetilde{K}/K_0)$ with index d, and $K = \widetilde{K}^{G'}$ the subfield of $\widetilde{K}$ fixed by G'. We shall study the extensions $K|k$. Let us note that over $k = \mathbf{Q}$ the polynomial $X^p - a$, where $a \in \mathbf{Q}$ is not a p-th power, has Galois group $F_{p(p-1)}$, hence the extension $K_0/\mathbf{Q}$ obtained by adjoining a root of this polynomial satisfies the above conditions.

3.1. Hopf Galois character.

Proposition 3.1. *The extension $K|k$ is Hopf Galois, for all prime $p \geq 5$.*

Proof: We consider the tower of fields $k \subset K_0 \subset K \subset \widetilde{K}$. The extension K_0/k is Hopf Galois, since it is a prime degree extension such that its Galois closure has a solvable group (see [**4**]); the extension K/K_0 is Galois since $\widetilde{K}/K_0$ is cyclic. This implies that K/k is Hopf Galois by [**6**, Theorem 6.1]. □

Let us see now if K/k is almost classically Galois. Let us recall that the group $F_{p(p-1)}$ can be seen as a subgroup of $\mathrm{GL}(2,p)$, namely

$$F_{p(p-1)} = \left\{ \begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} : b \in \mathbf{F}_p,\ c \in \mathbf{F}_p^* \right\} \subset \mathrm{GL}(2,p).$$

For each divisor d of $p-1$, $F_{p(p-1)}$ has a unique normal subgroup F_{pd} corresponding to the unique subgroup C_d of order d of $\mathbf{F}_p^*$:

$$F_{pd} = \left\{ \begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} : b \in \mathbf{F}_p,\ c \in C_d \right\}.$$

Since G' has order $(p-1)/d$, the only candidate to be a normal complement for G' in G is F_{pd}. This group contains all elements of order ℓ in $F_{p(p-1)}$, for every divisor ℓ of d, which are of the form $\left(\begin{smallmatrix} 1 & b \\ 0 & c \end{smallmatrix}\right)$, with c of order ℓ in $\mathbf{F}_p^*$. We obtain then two cases, depending on $D := \gcd((p-1)/d, d)$.

- If $D \neq 1$, let ℓ be a prime number dividing D. The group G' has some element of order ℓ, since ℓ is a prime number dividing $|G'|$. Therefore, G' and F_{pd} have nontrivial intersection, G' has no normal complement in G, and K/k is not almost classically Galois.
- If $D = 1$, the subgroups F_{pd} and G' intersect in 0, hence G' has a normal complement, the extension K/k is almost classically Galois, and the structure is given by F_{pd}.

We state what we have proved so far in the following proposition.

Proposition 3.2. *Let $p \geq 5$ be a prime number, d a nontrivial divisor of $p-1$. An extension K/k of degree pd such that its Galois closure $\widetilde{K}$ has Galois group over k the Frobenius group $F_{p(p-1)}$ is almost classically Galois if and only if* $\gcd((p-1)/d, d) = 1$.

We shall now endow the extension K/k with two different Hopf Galois structures. We consider two groups of order pd, the cyclic group C_{pd} and the Frobenius group F_{pd}. Let us note that for a prime d, these are the unique groups of order pd. We fix a generator ζ of $\mathbf{F}_p^*$ and write

$$S = \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then

$$G = \langle S, T\rangle = \left\{ S^i T^j = \begin{pmatrix} 1 & j \\ 0 & \zeta^i \end{pmatrix} \right\}_{j \bmod p,\, i \bmod p-1}.$$

We take $G' = \langle S^d \rangle$ and the left transversal of G/G'

$$T^x S^m = \begin{pmatrix} 1 & x\zeta^m \\ 0 & \zeta^m \end{pmatrix}, \quad x \in \mathbf{F}_p, \quad 0 \leq m < d.$$

Let us note that the element $\left(\begin{smallmatrix} 1 & b \\ 0 & \zeta^i \end{smallmatrix}\right)$ of G is in the class determined by $m = i \bmod d$, $x = b\zeta^{-i}$. Let us identify the set G/G' with $X = (\mathbf{Z}/(d)) \times \mathbf{F}_p$ by $(m, x) \leftrightarrow T^x S^m$. By computation of the action of the generators T, S of G on G/G', we obtain that the image $\lambda(G)$ of G in $S_{pd} = \mathrm{Perm}(X)$ is generated by

$$\sigma_1 \colon (m, x) \mapsto (m, x+1), \quad \sigma_2 \colon (m, x) \mapsto (m+1, x\zeta^{-1}).$$

The subgroup F of G isomorphic to F_{pd} is $F = \langle S^{\frac{p-1}{d}}, T\rangle$. It can be seen as a regular subgroup of the symmetric group S_{pd} via the action on itself by left translation. We identify F with the set $X = (\mathbf{Z}/(d)) \times \mathbf{F}_p$ by $(m, x) \leftrightarrow S^{m\frac{p-1}{d}} T^x$. By computation of the action of the generators T and $S^{\frac{p-1}{d}}$, we obtain that the image N_1 of F in $\mathrm{Perm}(X)$ is generated by

$$\tau_1 \colon (m, x) \mapsto (m, x + \zeta^{m\frac{p-1}{d}}), \quad \tau_2 \colon (m, x) \mapsto (m+1, x).$$

Let us see now that $\lambda(G)$ normalizes N_1. By computation, we obtain

$$\sigma_1 \tau_1 \sigma_1^{-1} = \tau_1, \qquad \sigma_1 \tau_2 \sigma_1^{-1} = \tau_2,$$

$$\sigma_2 \tau_1 \sigma_2^{-1} = \tau_1^{\zeta^{-1-\frac{p-1}{d}}}, \quad \sigma_2 \tau_2 \sigma_2^{-1} = \tau_2.$$

We consider now the cyclic group $C := C_{pd}$ of order pd. It can be seen as a regular subgroup of the symmetric group S_{pd} via the action on itself by left translation. We have $C = C_d \times C_p$, so we may identify it with the set $X = (\mathbf{Z}/(d)) \times \mathbf{F}_p$ in the obvious way. By computing the action of the generator $(1,1)$ of C, we obtain that the image N_2 of C in $\mathrm{Perm}(X)$ is generated by

$$\tau \colon (m, x) \mapsto (m+1, x+1).$$

Let us see now that $\lambda(G)$ normalizes N_2. By computation, we obtain

$$\sigma_1 \tau \sigma_1^{-1} = \tau, \quad \sigma_2 \tau \sigma_2^{-1} = \tau^k,$$

where k is the integer in the range $[0, pd-1]$ determined by $k \equiv 1 \pmod{d}$, $k \equiv \zeta^{-1} \pmod{p}$.

We have then obtained the following result.

Theorem 3.3. *Let $p \geq 5$ be a prime number, d a nontrivial divisor of $p-1$. An extension K/k of degree pd such that its Galois closure $\widetilde{K}$ has Galois group over k the Frobenius group $F_{p(p-1)}$ has (at least) two Hopf Galois structures given by the cyclic and Frobenius groups, respectively. The extension K/k is almost classically Galois if and only if* $\gcd((p-1)/d, d) = 1$ *and in this case the structure is given by the group F_{pd}.*

3.2. The Galois correspondence.

We may determine the intermediate fields of the extension K/k by classical Galois theory applied to the Galois extension $\widetilde{K}/k$. Since K is the subfield of $\widetilde{K}$ fixed by a cyclic group G' of G, the intermediate fields of K/k are in one-to-one correspondence to the subgroups of $G = F_{p(p-1)}$ containing G'. Writing again

$$F_{p(p-1)} = \langle S, T \rangle,$$

we shall describe the subgroups of $F_{p(p-1)}$. These are

- The subgroups
$$F_{pd} = \left\langle S^{\frac{p-1}{d}}, T \right\rangle,$$
which are all normal subgroups and satisfy $F_{pd_1} \subset F_{pd_2}$ if and only if $d_1 | d_2$. In particular, for $d = 1$, we obtain the p-Sylow subgroup.
- For each divisor d of $p-1$ we have p cyclic subgroups $C_d(b)$, $b \in \mathbf{F}_p$, of order d which are all conjugate:
$$C_d(b) = \left\langle S^{\frac{p-1}{d}} T^b \right\rangle.$$
We have $C_{d_1}(b) \subset C_{d_2}(b)$ if and only if $d_1 | d_2$; $C_d(b_1) \cap C_d(b_2) = 1$ if $b_1 \neq b_2$ and $C_d(b) \subset F_{pd}$, for all $b \in \mathbf{F}_p$.

Since we fixed $G' = C_{(p-1)/d}(0)$, the subgroups of G containing G' are the groups $C_{(p-1)/d'}(0)$ and $F_{p(p-1)/d'}$, with d' running over the divisors of d. Hence, for each divisor d' of d, there is a field $L^1_{d'}$ such that $K_0 \subset L^1_{d'} \subset \widetilde{K}$ and $[L^1_{d'} : K_0] = d'$ and a field $L^2_{d'}$ such that $[L^2_{d'} : k] = d'$, $L^2_{d'} \cap K_0 = k$, and $L^2_{d'} \subset L^1_{d'}$. Moreover if $d_1 | d_2$, then $L^1_{d_1} \subset L^1_{d_2}$ and $L^2_{d_1} \subset L^2_{d_2}$.

Let us look now at the subgroups of the two groups N giving a Hopf Galois structure to K/k. For each d' dividing d, the cyclic group C_{pd} has exactly one subgroup of order pd' and exactly one of order d', namely the cyclic groups $C_{pd'}$ and $C_{d'}$, hence the Hopf Galois structure of type C_{pd} yields a bijective Galois correspondence if and only if all of them are stable under the action of G. This is clear by the fact that C_{pd} has a unique subgroup for each order. For each d' dividing d, the group F_{pd}

has a subgroup $F_{pd'}$ of order pd' and p conjugate subgroups $C_{d'}(b)$ of order d', hence the Hopf Galois structure of type F_{pd} yields a bijective Galois correspondence if, for each d', the subgroup $F_{pd'}$ and one of the subgroups $C_{d'}(b)$ are stable under the action of G. For $F_{pd'}$ this is clear. For $C_{d'}(b)$, since σ_1 normalizes N_1, it is enough to compute $\sigma_2\tau_2^e\tau_1^b\sigma_2^{-1}$, where $e = d/d'$. We obtain

$$\sigma_2\tau_2^e\tau_1^b\sigma_2^{-1} = \tau_2^e\tau_1^{b(\zeta^{-1}-\frac{p-1}{d})}.$$

Now the powers of $\tau_2^e\tau_1^b$ are $(\tau_2^e\tau_1^b)^k = \tau_2^{ke}\tau_1^{b(1+\eta^e+\cdots+\eta^{(k-1)e})}$, for $\eta = \zeta^{\frac{p-1}{d}}$, so the subgroup $C_{d'}(b)$ is stable exactly for $b = 0$.

We have then obtained the following result.

Theorem 3.4. *Let $p \geq 5$ be a prime number, d a nontrivial divisor of $p-1$. Let K/k be an extension of degree pd such that its Galois closure $\widetilde{K}$ has Galois group over k the Frobenius group $F_{p(p-1)}$. We can endow K/k with a non almost classically Galois Hopf Galois structure of type C_{pd} such that the Galois correspondence is one-to-one. We can also endow K/k with a Hopf Galois structure of type F_{pd}, which is almost classically Galois exactly when* $\gcd((p-1)/d, d) = 1$ *and such that the Galois correspondence is always one-to-one.*

Corollary 3.5. *There exist Hopf Galois extensions which are not almost classically Galois but may be endowed with a Hopf Galois structure such that the Galois correspondence is one-to-one.*

4. A family of Galois extensions

Let $p \geq 3$ be a prime number and K/k a Galois extension with Galois group $G = D_{2p}$, the dihedral group of order $2p$. The Hopf Galois structures of K/k are determined in [**2**, Theorem 6.2]. There are $2+p$ structures of which p are of type C_{2p} and the two others correspond to D_{2p} (the classical Galois one) and to its opposite group. We shall describe these Hopf Galois structures and see that the images of the corresponding Galois correspondences are all different.

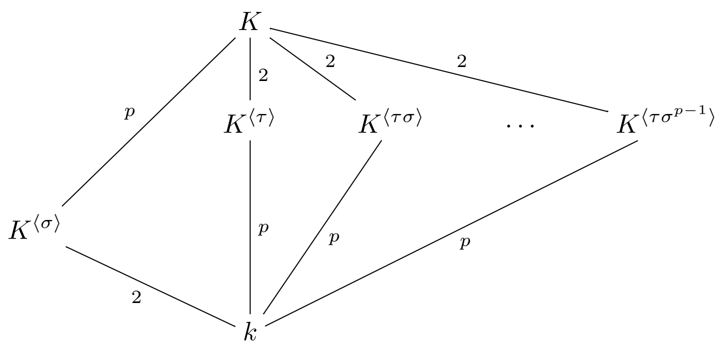
We shall work with the following presentation of D_{2p}.

$$\begin{aligned} D_{2p} &= \langle \sigma, \tau \mid \sigma^p = 1,\ \tau^2 = 1,\ \tau\sigma = \sigma^{p-1}\tau \rangle \\ &= \{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{p-1}\}. \end{aligned}$$

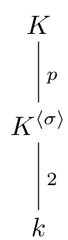
We consider the embedding of G in S_{2p} given by the action of G on itself by left translation.

$$\lambda\colon D_{2p} \hookrightarrow \mathrm{Perm}(D_{2p}) \simeq S_{2p}$$
$$g \mapsto \lambda(g)\colon x \mapsto gx.$$

The Galois structure corresponds to $\rho(D_{2p})$, where $\rho\colon D_{2p} \hookrightarrow \mathrm{Perm}(D_{2p}) \simeq S_{2p}$ is given by $\rho(g)(x) = xg^{-1}$. The image of the Galois correspondence is then the whole lattice of intermediate fields and is given by the fundamental theorem of Galois theory. Since D_{2p} has two conjugation classes of nontrivial subgroups, one class containing the normal subgroup of order p, which is generated by σ and another class of length p of subgroups of order 2 generated by the elements $\tau\sigma^k$, $k = 0, \dots, p-1$, the subfield lattice consists, besides k and K, in one normal extension of degree 2, and p conjugate extensions of degree p.



The nonclassical structure of type D_{2p} is given by $\lambda(G)$. In this case, the image of the Galois correspondence consists, besides k and K, in the normal extension of degree 2 (see [**8**, Theorem 5.3]).



In order to study the cyclic structures, we identify D_{2p} with the set $Y = \mathbf{F}_2 \times \mathbf{F}_p$ by $\tau^i\sigma^j \leftrightarrow (i,j)$ and S_{2p} with $\mathrm{Perm}(Y)$. We have then

$$\lambda(\sigma)(m,n) = (m, n+m), \quad \lambda(\tau)(m,n) = (m+1, n).$$

Let us now write $C_{2p} = C_2 \times C_p$ and identify it with Y. We have then p embeddings of C_{2p} in $\mathrm{Perm}(Y)$ given by sending a chosen generator of C_{2p} to the permutation

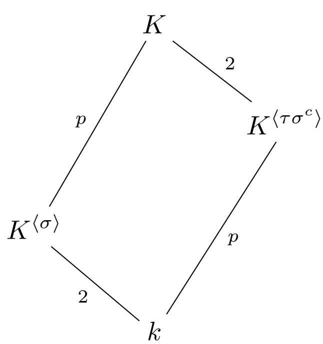
$$\pi_c\colon (m,n) \mapsto (m+1, n+1+(-1)^m c), \quad c = 0, \dots, p-1,$$

which is a $2p$-cycle. Let us denote $N_c = \langle \pi_c \rangle$. Each of the groups $N_c \simeq C_{2p}$ have just two proper nontrivial subgroups of orders 2 and p, which are normal. Since N_c is not contained in the alternating group A_{2p}, by Remark 2.4, the subgroup $N_c \cap A_{2p} = \langle \pi_c^2 \rangle$ is stable under conjugation by $\lambda(G)$. Then the field $K^{K[\langle \pi_c^2 \rangle]^G} = K^{\langle \sigma \rangle}$ is in the image of the Galois correspondence theorem for all Hopf Galois structures. The subgroup $\langle \pi_c^p \rangle$ is also stable under conjugation by $\lambda(G)$, since $\lambda(\sigma)\pi_c\lambda(\sigma^{-1}) = \pi_c^p$. It corresponds then to the intermediate field $K^{K[\langle \pi_c^p \rangle]^G}$, which has degree p over k. We have

$$\begin{aligned} K^{K[\langle \pi_c \rangle^p]^G} &= \{x \in K \mid \mu(h)(x) = \varepsilon(h)(x),\ \forall\, h \in k[\langle \pi_c^p \rangle]\} \\ &= \{x \in K \mid \mu(\pi_c^p)(x) = \varepsilon(\pi_c^p)(x) = x\} \\ &= \{x \in K \mid \tau\sigma^c(x) = x\} = K^{\langle \tau\sigma^c \rangle} \end{aligned}$$

since the action of μ is given by $\mu(\pi_c^p)(x) = \pi_c^{-p}(1_G)(x) = \tau\sigma^c(x)$, 1_G is identified with $(0,0) \in Y$ and $\pi_c^p(0,0) = (1,c)$ corresponds to $\tau\sigma^c$.

We have then obtained that for each of the Hopf Galois cyclic structures of K/k there is exactly one extension of degree p in the image of the Galois correspondence. Its image gives the lattice



for c an integer, $1 \le c \le p$.

5. A Hopf Galois extension with non bijective Galois correspondence

In this section we exhibit a Hopf Galois extension such that the Galois correspondence is not bijective for any of its Hopf Galois structures. The extension considered is a separable field extension K/k of degree 12 such that the Galois group G of its normal closure $\widetilde{K}$ over k is isomorphic to $S_3 \times S_3$, the direct product of two copies of the symmetric group on three letters. Let us note that the group $S_3 \times S_3$ has exactly one conjugation class of non-normal subgroups of order 3. Hence K is the subfield of $\widetilde{K}$ fixed by a subgroup G' in this conjugation class. As an example of such an extension we can take $k = \mathbf{Q}$ and K to be the field obtained by adjoining to $\mathbf{Q}$ a root of the polynomial

$$x^{12} - 2x^{11} - 2x^9 + 15x^8 - 4x^7 - 12x^6 - 4x^5 + 15x^4 - 2x^3 - 2x + 1.$$

Proposition 5.1. *Let K/k be a separable field extension of degree 12 such that the Galois group $G = \mathrm{Gal}(\widetilde{K}/k)$ of its normal closure is isomorphic to $S_3 \times S_3$. Then, K/k is a Hopf Galois extension non almost classically Galois.*

Proof: The extension K/k is not almost classically Galois since $S_3 \times S_3$ has no normal subgroups of order 12.

Since all transitive subgroups of S_{12} isomorphic to $S_3 \times S_3$ lie in the same conjugacy class, there is an enumeration of the left cosets G/G' such that the embedding λ of G in S_{12} obtained via the action on those left cosets is

$$\lambda(G) = \langle \sigma, \tau \rangle,$$

where

$$\sigma = (1,2,3,4,5,6)(7,8,9,10,11,12),$$
$$\tau = (1,9)(2,10)(3,7)(4,8)(5,11)(6,12)$$

and such that G' is the stabilizer of 1.

The group

$$N = \langle (1,11,5,9,3,7)(2,12,6,10,4,8), (1,10)(2,9)(3,8)(4,7)(5,12)(6,11) \rangle,$$

isomorphic to the dihedral group $D_{2\cdot 6}$, is a regular subgroup of S_{12} such that $\lambda(G) \subset \mathrm{Norm}_{S_{12}}(N)$. Therefore N provides a Hopf Galois structure for K/k. □

We look now for a regular subgroup $N \subset S_{12}$ normalized by $\lambda(G)$ and such that the lattice of its subgroups stable under the action of $\lambda(G)$

by conjugation is in one-to-one correspondence with the lattice of intermediate fields of K/k. That is, we want to know whether K/k may be endowed with a Hopf Galois structure such that the Galois correspondence is bijective.

By classical Galois theory, the lattice of intermediate fields of K/k corresponds to the subgroups of G containing G'. This gives

Subgroups of G containing G'	Intermediate fields of K/k
G'	K
3 subgroups of order 6	3 extensions of k of degree 6
1 subgroups of order 9	1 biquadratic extension of k
3 subgroups of order 18	3 quadratic extensions of k
G	k

Checking over the 5 isomorphism classes of groups of order 12, we see that only the dihedral group has enough subgroups to be in bijective correspondence with such a subfield lattice. Therefore, the question becomes:

> *Is there any regular subgroup $N \subset S_{12}$ isomorphic to the dihedral group $D_{2\cdot 6}$ such that $\lambda(G) \subset \mathrm{Norm}_{S_{12}}(N)$ and N has 3 subgroups of order 2, 1 subgroup of order 3, 3 subgroups of order 6, all of them stable under conjugation by $\lambda(G)$?*

Lemma 5.2. *The three subgroups of order 2 of N stable under conjugation by G must be the subgroups $\langle \omega_i \rangle$ where*

$$\omega_1 = (1,7)(2,8)(3,9)(4,10)(5,11)(6,12),$$

$$\omega_2 = (1,9)(2,10)(3,11)(4,12)(5,7)(6,8),$$

$$\omega_3 = (1,11)(2,12)(3,7)(4,8)(5,9)(6,10).$$

Proof: Since N is regular, its elements of order 2 have no fixed point and then must be the product of six disjoint transpositions. Looking for an element ω which is the product of 6 disjoint transpositions and is stable under conjugation by $\lambda(G)$ amounts to look for a set of 6 disjoint transpositions which are permuted by conjugation of the two generators of $\lambda(G)$. By performing the computation, we obtain the result in the lemma. □

Proposition 5.3. *There is no regular subgroup $N \subset S_{12}$ isomorphic to the dihedral group $D_{2\cdot 6}$ such that $\lambda(G) \subset \mathrm{Norm}_{S_{12}}(N)$ and N has 3 subgroups of order 2 and 3 subgroups of order 6 all of them stable under conjugation by $\lambda(G)$.*

Proof: Let N be a regular subgroup of S_{12} isomorphic to the dihedral group $D_{2\cdot 6}$. The dihedral group $D_{2\cdot 6} = \langle r, s \mid r^6 = s^2 = 1, rs = sr^5 \rangle$ has exactly 3 subgroups of order 6 and one of them is the cyclic group $\langle r \rangle$. If N has 3 subgroups of order 6 stable under conjugation by $\lambda(G)$, then, in particular, its cyclic subgroup of order 6 must be. This implies that the center of N is stable under $\lambda(G)$. Now, if N has 3 subgroups of order 2 stable under conjugation by $\lambda(G)$, according to the lemma, these must be generated by ω_1, ω_2, and ω_3, respectively. Then one of the elements ω_i should commute with the other two, which does not hold. ☐

As a corollary, we obtain the following result.

Theorem 5.4. *There exist separable Hopf Galois extensions K/k such that the Galois correspondence is not bijective for any of its Hopf Galois structures.*

References

[1] N. P. Byott, Uniqueness of Hopf Galois structure for separable field extensions, *Comm. Algebra* **24(10)** (1996), 3217–3228. DOI: 10.1080/00927879608825743; Corrigendum, *Comm. Algebra* **24(11)** (1996), 3705. DOI: 10.1080/00927879608825779.

[2] N. P. Byott, Hopf-Galois structures on Galois field extensions of degree pq, *J. Pure Appl. Algebra* **188(1–3)** (2004), 45–57. DOI: 10.1016/j.jpaa.2003.10.010.

[3] S. U. Chase and M. E. Sweedler, *"Hopf algebras and Galois theory"*, Lecture Notes in Mathematics **97**, Springer-Verlag, Berlin-New York, 1969. DOI: 10.1007/BFb0101433.

[4] L. N. Childs, On the Hopf Galois theory for separable field extensions, *Comm. Algebra* **17(4)** (1989), 809–825. DOI: 10.1080/00927878908823760.

[5] L. N. Childs, *"Taming wild extensions: Hopf algebras and local Galois module theory"*, Mathematical Surveys and Monographs **80**, American Mathematical Society, Providence, RI, 2000. DOI: 10.1090/surv/080.

[6] T. Crespo, A. Rio, and M. Vela, From Galois to Hopf Galois: theory and practice, in: *"Trends in Number Theory"*, Contemp. Math. **649**, Amer. Math. Soc., Providence, RI, 2015, pp. 29–46. DOI: 10.1090/conm/649/13018.

[7] T. Crespo, A. Rio, and M. Vela, The Hopf Galois property in subfield lattices, *Comm. Algebra* **44(1)** (2016), 336–353. DOI:10.1080/00927872.2014.982809.

[8] C. Greither and B. Pareigis, Hopf Galois theory for separable field extensions, *J. Algebra* **106(1)** (1987), 239–258. DOI: 10.1016/0021-8693(87)90029-9.

Teresa Crespo:
Departament d'Àlgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
E-08007 Barcelona
Spain
E-mail address: teresa.crespo@ub.edu

Anna Rio and Montserrat Vela:
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya
C/Jordi Girona, 1–3, Edifici Omega
E-08034 Barcelona
Spain
E-mail address: ana.rio@upc.edu
E-mail address: montse.vela@upc.edu

Primera versió rebuda el 28 d'abril de 2014,
darrera versió rebuda el 28 de maig de 2014.