ON INDUCED HOPF GALOIS STRUCTURES AND LOCAL
HOPF GALOIS MODULES

DANIEL GIL AND ANNA RIO

ABSTRACT. In this paper we study the Hopf Galois module structure of the valuation ring of an extension of $p$-adic fields and we focus in the induced Hopf Galois structures, i.e, those given by Hopf Galois structures in a tower of extensions. We express Hopf Galois actions in terms of matrices and present a method to compute a basis of the associated order in every Hopf Galois structure. We see that for an induced Hopf Galois structure the corresponding algebra is a tensor product and the corresponding matrix is a Kronecker product. In the local case we prove that an analog equality holds for the corresponding associated order. Finally, we obtain conditions to assure the freeness of the valuation ring over the associated order in an induced Hopf Galois structure.

1. Introduction

A finite extension of fields $L/K$ is said to be Hopf Galois if there is a $K$-Hopf algebra $H$ and a $K$-linear action $\cdot : H \otimes_K L \rightarrow L$ which endows $L$ with $H$-module structure, such that the induced map $j : H \otimes_K L \rightarrow \text{End}_K(L)$ is bijective. In that case, the pair $(H, \cdot)$ is said to be a Hopf Galois structure of $L/K$. We also say that $L/K$ is $H$-Galois. This notion was introduced by Chase and Sweedler in their book [1] and it generalizes the one of Galois extension since the group algebra of the Galois group together with the Galois action is a Hopf Galois structure.

Although Hopf Galois structures are difficult to compute in general, the ones of separable extensions can be labelled by objects of group theory thank to Greither-Pareigis theorem. This result was introduced by Greither and Pareigis in their article [5] and translated the determination of Hopf Galois structures of a separable extension to a question of group theory. If $L/K$ is a separable extension, let $\bar{L}$ be its normal closure, $G = \text{Gal}(\bar{L}/K)$, $G' = \text{Gal}(\bar{L}/L)$ and $X = G/G'$. Let $\lambda, \rho : G \rightarrow \text{Perm}(X)$ be the left and right translation embeddings of $G$ into $\text{Perm}(X)$.

Theorem 1.1 (Greither-Pareigis). Hopf Galois structures of $L/K$ are in one-to-one correspondence with regular (i.e, simply transitive) subgroups of $\text{Perm}(X)$ normalized by $\lambda(G)$. Moreover, if $N$ is some such subgroup, the corresponding Hopf Galois structure is given by the $K$-Hopf algebra $\bar{L}[N]^G$ and its action over $L$ defined by

$$\left(\sum_{i=1}^{r} c_i n_i\right) \cdot x = \sum_{i=1}^{r} c_i n_i^{-1}(\lambda(G)(x))$$

Date: October 15, 2019.

2010 Mathematics Subject Classification. 11R32, 12F10, 16T05.

Key words and phrases. Induced Hopf Galois action, associated order.

Supported by grant MTM2015-66180-R.
If a Hopf Galois structure \((H, \cdot)\) corresponds to a group \(N\), the type of \(H\) is defined as the isomorphism class of \(N\) among the groups of order \(n\).

Hopf Galois theory can be used to generalize Galois module theory, giving rise to a Hopf Galois module theory. In the approach introduced by Leopoldt, Galois module theory studies the structure of the valuation ring \(O_L\) of a Galois extension \(L/K\) of \(p\)-adic fields over its associated order \(\mathfrak{A}_{K[G]}\), defined as the maximal \(O_K\)-order in \(K[G]\) that acts over \(O_L\). If \(L/K\) is \(H\)-Galois, the associated order of \(O_L\) in \(H\) is defined as

\[
\mathfrak{A}_H = \{ \alpha \in H \mid \alpha \cdot x \in O_L \text{ for every } x \in O_L \}.
\]

It is interesting to determine the freeness of \(O_L\) as \(\mathfrak{A}_H\)-module as \(H\) runs through the different Hopf Galois structures of \(L/K\).

Let \(L/K\) be a Galois extension and let \(E\) be an intermediate field of \(L/K\) such that \(\text{Gal}(L/E)\) has a normal complement in \(\text{Gal}(L/K)\). Crespo, Rio and Vela proved in their paper [4] that it is possible to induce a Hopf Galois structure of \(L/K\) from a Hopf Galois structure of \(L/E\) and a Hopf Galois structure of \(E/K\). This is what we call an induced Hopf Galois structure. The main goal in this paper is to explore induced Hopf Galois structures at the integral level, i.e., for every induced Hopf Galois structure \(H\), to determine the associated order \(\mathfrak{A}_H\) and study the freeness of \(O_L\) as \(\mathfrak{A}_H\)-module.

Let \(L/K\) be a degree \(n\) Hopf Galois extension of \(p\)-adic fields with Galois group \(G = J \rtimes G'\). Let \(E = L^{G'}\) and \(F = L^J\). We will prove in Section 3 that every induced Hopf Galois structure of \(L/K\) is of the form

\[
H = H_1 \otimes_K \mathfrak{T},
\]

where \(H_1\) is a Hopf Galois structure of \(E/K\) and \(\mathfrak{T}\) is a Hopf Galois structure of \(F/K\) (see Proposition 3.2). Hence, we have a diagram:

- \(\xymatrix{ & L \\
  & H \\
 E \ar[ru] \ar[rd] & \mathfrak{T} \\
 K \ar[ru] \ar[rd] & F \ar[ru] \ar[rd] & \mathfrak{A}_H \ar[ru] \ar[rd] & \mathfrak{A}_{H_1} \ar[ru] \ar[rd] & \mathfrak{A}_{\mathfrak{T}} \ar[ru] \ar[rd] \\
 & H_1 \ar[ru] & \mathfrak{T} \ar[ru] & \mathfrak{A}_H \ar[ru] \ar[rd] & \mathfrak{A}_{H_1} \ar[ru] \ar[rd] \ar[ru] & \mathfrak{A}_{\mathfrak{T}} \ar[ru] \ar[rd]}
\]

We want to explore the relation between \(\mathfrak{A}_H\), \(\mathfrak{A}_{H_1}\) and \(\mathfrak{A}_{\mathfrak{T}}\) as well as the relation between the freeness of \(O_L\), \(O_E\) and \(O_F\) over their respective associated orders.

Since \(H\) is the tensor product of \(H_1\) and \(\mathfrak{T}\), we can ask ourselves whether an analog relation holds with the associated orders. The answer is affirmative, as we will prove in Section 4.

**Theorem 1.2.** Let \(L/K\) be an \(H\)-Galois extension of \(p\)-adic fields, with \(H = H_1 \otimes_K \mathfrak{T}\) induced. Then,

\[
\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes \mathfrak{A}_{\mathfrak{T}}.
\]

This result provides explicitly an \(O_K\)-basis of \(\mathfrak{A}_H\) in terms of \(O_K\)-bases of \(\mathfrak{A}_{H_1}\) and \(\mathfrak{A}_{\mathfrak{T}}\). This allows us to take advantage of the fact that for every \(t \in O_L\), \(t\) is a generator of \(O_L\) as \(\mathfrak{A}_H\)-module if and only if the Hopf Galois conjugates of \(t\) under
an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$ form an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. In Section 5 we will use this property to prove the following:

**Theorem 1.3.** Let $L/K$ be an $H$-Galois extension of $p$-adic fields, with $H = H_1 \otimes_K \mathbb{P}$ induced. If $\mathcal{O}_E$ is $\mathfrak{A}_H$-free $\mathcal{O}_F$ is $\mathfrak{A}_\mathbb{P}$-free, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. In such case, if $\gamma$ is an $\mathfrak{A}_H$-generator of $\mathcal{O}_E$ and $\delta$ is an $\mathfrak{A}_\mathbb{P}$-generator of $\mathcal{O}_F$, then $\gamma\delta$ is an $\mathfrak{A}_H$-generator of $\mathcal{O}_L$.

We will also study the behaviour of the associated order when tensoring with a $K$-linearly disjoint extension, obtaining the following result:

**Theorem 1.4.** Let $L/K$ be an $H$-Galois extension of $p$-adic fields, with $H = H_1 \otimes_K \mathbb{P}$ induced. Then, $\mathcal{O}_E$ is $\mathfrak{A}_H$-free if and only if $\mathcal{O}_L$ is $\mathfrak{A}_{H_1 \otimes_K F}$-free.

Theorems 1.3 and 1.4 lead us to the following:

**Corollary 1.5.** Let $L/K$ be an $H$-Galois extension of $p$-adic fields, with $H = H_1 \otimes_K \mathbb{P}$ induced. If $\mathcal{O}_L$ is $\mathfrak{A}_{H_1 \otimes_K F}$-free and $\mathcal{O}_F$ is $\mathfrak{A}_\mathbb{P}$-free, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

The utility of this result is that $L/F$ is Galois while $E/K$ is not, and in some situations, freeness is easier to study in Galois extensions.

2. **Matrix of a Hopf Galois Action**

Let $L/K$ be a separable degree $n$ $H$-Galois extension of fields. Let $W = \{w_i\}_{i=0}^{n-1}$ be a $K$-basis of $H$ and let $B = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}$ be a $K$-basis of $L$. Since $H$ acts $K$-linearly over $L$, the elements $w_i \cdot \gamma_j$, $0 \leq i, j \leq n - 1$, are $K$-linear combinations of the elements of $B$. That is, given $0 \leq i, j \leq n - 1$,

$$w_i \cdot \gamma_j = \sum_{k=0}^{n-1} m_{ij}^{(k)} (H_W, L_B) \gamma_k$$

for certain scalars $m_{ij}^{(k)} (H_W, L_B) \in K$. We can gather the information as in the following table:

| $w_0$ | $\sum_{k=0}^{n-1} m_{00}^{(k)} (H_W, L_B) \gamma_k$ | $\ldots$ | $\sum_{k=0}^{n-1} m_{0, n-1}^{(k)} (H_W, L_B) \gamma_k$ | $\gamma_0$ | $\ldots$ | $\gamma_{n-1}$ |
|------|---------------------------------|---|---------------------------------|---|---|---|
| $w_1$ | $\sum_{k=0}^{n-1} m_{10}^{(k)} (H_W, L_B) \gamma_k$ | $\ldots$ | $\sum_{k=0}^{n-1} m_{1, n-1}^{(k)} (H_W, L_B) \gamma_k$ |
| $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ |
| $w_{n-1}$ | $\sum_{k=0}^{n-1} m_{n-1,0}^{(k)} (H_W, L_B) \gamma_k$ | $\ldots$ | $\sum_{k=0}^{n-1} m_{n-1, n-1}^{(k)} (H_W, L_B) \gamma_k$ |

These elements determine completely the action of $H$ over $L$: if $h \in H$ and $x \in L$, we write $h = \sum_{i=0}^{n-1} h_i w_i$ and $x = \sum_{j=0}^{n-1} x_j \gamma_j$, and we have

$$h \cdot x = \sum_{i, j=0}^{n-1} h_i x_j (w_i \cdot \gamma_j).$$

What we do is to gather the coefficients of the linear combinations in the previous table in a matrix, which subsequently provides full information about the action.
First, we take the coefficients of 1 in the entries of the previous table, and we transpose them, obtaining the matrix $M^{(0)}(H_W, L_B)$

$$
\begin{pmatrix}
  m_{00}^{(0)}(H_W, L_B) & m_{10}^{(0)}(H_W, L_B) & \cdots & m_{n-1,0}^{(0)}(H_W, L_B) \\
  m_{01}^{(0)}(H_W, L_B) & m_{11}^{(0)}(H_W, L_B) & \cdots & m_{n-1,1}^{(0)}(H_W, L_B) \\
  \cdots & \cdots & \cdots & \cdots \\
  m_{0,n-1}^{(0)}(H_W, L_B) & m_{1,n-1}^{(0)}(H_W, L_B) & \cdots & m_{n-1,n-1}^{(0)}(H_W, L_B)
\end{pmatrix}.
$$

We do the same with the elements $\gamma_1, \ldots, \gamma^{n-1}$ to obtain matrices $M^{(1)}(H_W, L_B), \ldots, M^{(n-1)}(H_W, L_B)$.

**Definition 2.1.** We define the **matrix of the action of $H$ over $L$** with respect to the $K$-basis $W$ of $H$ and the $K$-basis $B$ of $L$ as the matrix defined by blocks as

$$
M(H_W, L_B) = \begin{pmatrix}
  M^{(0)}(H_W, L_B) \\
  \vdots \\
  M^{(n-1)}(H_W, L_B)
\end{pmatrix}.
$$

**Remark 2.2.** We will usually omit the explicit mentions to the bases of $H$ and $L$ chosen and denote $M(H, L) = M(H_W, L_B)$, $m_{ij}^{(k)}(H, L) = m_{ij}^{(k)}(H_W, L_B)$.

With this definition, the coordinates of $w_i \cdot \gamma_j$ with respect to the $K$-basis $\{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}$ are the entries $(j, i)$ at each block $M^{(k)}(H_W, L_B)$. These two rules to define the matrix $M(H_W, L_B)$ may seem bizarre: why don’t we put the coordinates of each $w_i \cdot \gamma_j$ in the same row? Why don’t we take the matrix obtained from the table without transposing? Both questions are answered in Section 4. There, we will show that this definition is suitable to study the associated order of bases from $H$ to $L$ when $L/K$ is an extension of $p$-adic fields (see Theorem 4.1). By taking the transpose, we work by rows instead of by columns.

Let us establish the relation of the matrix of the action with respect to different bases.

**Proposition 2.3.** Let $W = \{w_i\}_{i=0}^{n-1}$ and $W' = \{w'_i\}_{i=0}^{n-1}$ be $K$-bases of $H$ and let $B = \{\gamma_j\}_{j=0}^{n-1}$ and $B' = \{\gamma'_j\}_{j=0}^{n-1}$ be $K$-bases of $L$. Let $P_W^{W'} = (a_{ij})$ be the matrix of the change of bases from $W' \to W$ and let $P_B^{B'} = (b_{ij})$ be the matrix of the change of bases from $B' \to B$. Let $P_B^{W'} = (b'_{ij})$. Given $0 \leq i, j, c \leq n-1$,

$$
m_{ij}^{(c)}(H_W, L_B') = \sum_{k=0}^{n-1} a_{ki} b_{ij} \sum_{d=0}^{n-1} b'_c m_{kd}^{(d)}(H_W, L_B).
$$

**Proof.** By definition of matrix of the action,

$$
w_i' \cdot \gamma_j' = \sum_{c=0}^{n-1} m_{ij}^{(c)}(H_W, L_B') \gamma_c'.
$$

On the other hand, by definition of matrix of the change of basis, $w_i' = \sum_{k=0}^{n-1} a_{ki} w_k$ and $\gamma_j' = \sum_{l=0}^{n-1} b_{lj} \gamma_l$. Then,
\[ w'_i \cdot \gamma'_j = \left( \sum_{k=0}^{n-1} a_{ki} w_k \right) \cdot \left( \sum_{l=0}^{n-1} b_{lj} \gamma_l \right) = \sum_{k,l=0}^{n-1} a_{ki} b_{lj} w_k \cdot \gamma_l \]

\[ = \sum_{k,l=0}^{n-1} a_{ki} b_{lj} \sum_{d=0}^{n-1} \gamma_d m_{kl}^{(d)} (H_W, L_B) \gamma_d \]

\[ = \sum_{k,l=0}^{n-1} a_{ki} b_{lj} \sum_{d=0}^{n-1} \gamma_d m_{kl}^{(d)} (H_W, L_B) \sum_{c=0}^{n-1} \gamma'_c \]

\[ = \sum_{c=0}^{d-1} \left( \sum_{k,l=0}^{n-1} a_{ki} b_{lj} \gamma'_c m_{kl}^{(d)} (H_W, L_B) \right) \gamma_c. \]

The statement follows from the uniqueness of coordinates. \( \square \)

**Example 2.4.** Let \( L/K \) be a finite degree \( n \) Galois extension of arbitrary fields and let \( G \) be its Galois group. Let us find the matrix of the classical Galois action over \( L \).

Let us write \( G = \{ \sigma_1, ..., \sigma_n \} \). Then, the elements \( \sigma_1, ..., \sigma_n \) form a \( K \)-basis of \( K[G] \). On the other hand, take a primitive element \( \alpha \) of \( L/K \) such that its Galois conjugates \( \alpha_1, ..., \alpha_n \) form a \( K \)-basis of \( L \) (such an element exists because of normal basis theorem). Since each \( \sigma \in G \) permutes the \( \alpha_i \), \( G \) can be seen as a subgroup of \( S_n \) and the action of \( K[G] \) over \( L \) is given by:

\[
\begin{array}{cccc}
\sigma_1 & \alpha_1 & \alpha_2 & \cdots & \alpha_n \\
\sigma_2 & \alpha_{\sigma_1(1)} & \alpha_{\sigma_1(2)} & \cdots & \alpha_{\sigma_1(n)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\sigma_n & \alpha_{\sigma_n(1)} & \alpha_{\sigma_n(2)} & \cdots & \alpha_{\sigma_n(n)} \\
\end{array}
\]

Hence, for every \( 0 \leq k \leq n-1 \), \( M^{(k)}(K[G], L) \) is the matrix whose \( i \)-th row is the \( \sigma_i^{-1}(k) \)-th vector of the canonical basis of \( K^n \). In particular, each block is obtained from exchanging two or more rows in the identity matrix.

**Example 2.5.** In the previous example, assume that \( G \cong C_n \). Let \( \sigma \) be a generator of \( G \). Then, \( \{1, \sigma, ..., \sigma^{n-1}\} \) is a \( K \)-basis of \( K[G] \). By normal basis theorem, there is a primitive element \( \alpha \) of \( L/K \) such that \( \{\alpha, \sigma(\alpha), ..., \sigma^{n-1}(\alpha)\} \) is a \( K \)-basis of \( L \). The action of \( K[G] \) over \( L \) is given by:

\[
\begin{array}{cccc}
\alpha & \sigma(\alpha) & \cdots & \sigma^{n-1}(\alpha) \\
1 & \alpha & \sigma(\alpha) & \cdots & \sigma^{n-1}(\alpha) \\
\sigma & \sigma(\alpha) & \sigma^2(\alpha) & \cdots & \alpha \\
\ldots & \ldots & \ldots & \ddots & \ldots \\
\sigma^{n-1} & \sigma^{n-1}(\alpha) & \alpha & \cdots & \sigma^{n-2}(\alpha) \\
\end{array}
\]

Then, for every \( 0 \leq k \leq n-1 \), \( M^{(k)}(K[G], L) \) is the matrix with rows \( e_{k+1}, e_k, ..., e_1, e_n, ..., e_{k+2} \), where \( e_i \) is the \( i \)-th vector of the canonical basis of \( K^n \).
If \( n = 2 \) (i.e., the extension is quadratic), we have

\[
M(K[G], L) = \begin{pmatrix}
1 & 0 \\
0 & 1 \\
0 & 0 \\
1 & 0
\end{pmatrix}
\]

**Example 2.6.** Let \( E = \mathbb{Q}_3(\alpha) \), where \( \alpha \) is a root of the polynomial \( f(x) = x^3 + 3 \in \mathbb{Q}_3[x] \). Then \( E/\mathbb{Q}_3 \) is a non-Galois extension with normal closure \( L = E(z) \), \( z = \sqrt[3]{-3} \).

The roots of \( f \) are \( \alpha, \xi \alpha, \xi^2 \alpha \), where \( \xi = \frac{-1 + \sqrt[3]{-3}}{2} \). Let \( r \) be the \( \mathbb{Q}_3 \)-automorphism of \( L \) given by \( r(\alpha) = \xi \alpha \) and \( r(z) = z \), and let \( s \) be the one given by \( s(z) = -z \) and \( s(\alpha) = \alpha \). As permutations of the roots of \( f \), \( r = (\alpha, \xi \alpha, \xi^2 \alpha) \) and \( s = (\xi \alpha, \xi^2 \alpha) \). These two elements generate the Galois group \( G \) of \( E/\mathbb{Q}_3 \). Additionally, \( s \) generates the group \( G' = \text{Gal}(L/E) \).

Let \( X = G/G' \) and consider the left translation \( \lambda: G \rightarrow \text{Perm}(X) \). By using Greither-Pareigis, one can check that the unique Hopf Galois structure of \( E/\mathbb{Q}_3 \) is given by the \( K \)-Hopf algebra \( H_1 \) with \( K \)-basis

\[
w_0 = \text{Id}, \ w_1 = (\mu - \mu^{-1})z, \ w_2 = \mu + \mu^{-1},
\]

where \( \mu = \lambda(r) \). The action of \( H_1 \) over \( E \) is given by

\[
\begin{array}{c|ccc}
 & 1 & \alpha & \alpha^2 \\
\hline
w_0 & 1 & \alpha & \alpha^2 \\
w_1 & 0 & 3\alpha & -\alpha^2 \\
w_2 & 2 & -\alpha & -3\alpha^2
\end{array}
\]

Then,

\[
M(H_1, E) = \begin{pmatrix}
1 & 0 & 2 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 1 & 3 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
1 & -1 & -3
\end{pmatrix}
\]

**Example 2.7.** Now we consider \( E = \mathbb{Q}_3(\alpha) \) with \( \alpha \) a root of \( f(x) = x^3 + 3x + 3 \in \mathbb{Q}_3[x] \). The normal closure of \( E/\mathbb{Q}_3 \) is

\( L = E(z) \), \( z = \sqrt[3]{-3} \cdot 3 \).

Let \( \alpha_0 = \alpha, \alpha_1 \) and \( \alpha_2 \) be the roots of \( f \). Then \( G = \langle r, s \rangle \) with \( r = (\alpha_0, \alpha_1, \alpha_2) \) and \( s = (\alpha_1, \alpha_2) \). Let \( \mu = \lambda(r) \). Again by Greither-Pareigis theory, we obtain that \( E/K \) has an unique Hopf Galois structure whose \( K \)-Hopf algebra \( H_1 \) has \( K \)-basis

\[
w_0 = \text{Id}, \ w_1 = (\mu - \mu^{-1})z, \ w_2 = \mu + \mu^{-1}.
\]
We can see that the action of $H_1$ over $E$ is given by

\begin{align*}
\begin{array}{c|ccc}
 & 1 & \alpha & \alpha^2 \\
 w_0 & 1 & \alpha & \alpha^2 \\
 w_1 & 0 & -3 + 27\alpha - 3\alpha^2 & -9 - 27\alpha^2 \\
 w_2 & 2 & -\alpha & -1 - \alpha^2 \\
\end{array}
\end{align*}

Then,

\[
M(H_1, E) = \begin{pmatrix}
1 & 0 & 2 \\
0 & -3 & 0 \\
0 & -9 & -1 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & -3 & 0 \\
1 & -27 & -1
\end{pmatrix}
\]

We finish the section with the following useful result.

**Proposition 2.8.** Let $L/K$ be a degree $n$ $H$-Galois extension. Then, the matrix $M(H, L)$ has rank $n$.

**Proof.** The columns of $M(H, L)$ are

\[
((m_{ij}^{(k)}(H, L))^n_{i=0})_{k=0}^{n-1}, 0 \leq i \leq n - 1.
\]

Let $\lambda_0, \ldots, \lambda_{n-1} \in K$ such that

\[
\sum_{i=0}^{n-1} \lambda_i m_{ij}^{(k)}(H, L) = 0, 0 \leq j, k \leq n - 1.
\]

Given $0 \leq j \leq n - 1$,

\[
\left(\sum_{i=0}^{n-1} \lambda_i w_i\right) \cdot \gamma_j = \sum_{i=0}^{n-1} \lambda_i \sum_{k=0}^{n-1} m_{ij}^{(k)}(H, L) \gamma_k = \sum_{k=0}^{n-1} \left(\sum_{i=0}^{n-1} \lambda_i m_{ij}^{(k)}(H, L)\right) \gamma_k = 0
\]

Since $\{\gamma_k\}_{k=0}^{n-1}$ is $K$-basis of $L$, $\sum_{i=0}^{n-1} \lambda_i w_i = 0$. But $\{w_i\}_{i=0}^{n-1}$ is $K$-basis of $H$, therefore $\lambda_i = 0$ for all $0 \leq i \leq n - 1$. Then, the columns of $M(H, L)$ are linearly independent, that is, the rank of $M(H, L)$ is $n$. \qed

3. **Induced Hopf Galois structures revisited**

Let $L/K$ be a finite Galois extension of fields with Galois group $G = \text{Gal}(L/K)$. Greither-Pareigis theorem applied to this situation gives that Hopf Galois structures of $L/K$ are of the form

\[H = L[N]^G,\]

where $N$ is a regular subgroup of $\text{Perm}(G)$ normalized by $\lambda(G)$. Assume that $G$ decomposes as a semidirect product

\[G = J \rtimes G',\]
where \( J \) is a normal subgroup of \( G \). Let us call \( E = L^{G'} \), \( F = L^J \), \( r = [E : K] \), \( u = [F : K] \). We have a lattice of intermediate fields

\[
\begin{array}{c}
\text{L} \\
\text{E} \\
\text{K} \\
\text{F}
\end{array}
\]

Since \( L/K \) is Galois, \( L/E \) is Galois with Galois group \( G' \). By Greither-Pareigis theorem, Hopf Galois structures of \( L/E \) are in one-to-one correspondence with regular subgroups of \( \text{Perm}(G') \) normalized by \( \lambda(G') \). On the other hand, Hopf Galois structures of \( E/K \) are in one-to-one correspondence with regular subgroups of \( \text{Perm}(X) \) normalized by \( \lambda(G) \), where \( X = \text{Gal}(\bar{E}/K) / \text{Gal}(\bar{E}/E) \). But fundamental theorem of Galois theory gives us the isomorphisms

\[
\text{Gal}(\bar{E}/K) \cong \text{Gal}(L/K) / \text{Gal}(L/\bar{E}),
\]

\[
\text{Gal}(\bar{E}/E) \cong \text{Gal}(L/E) / \text{Gal}(L/\bar{E}).
\]

Hence, there is a canonical bijection \( X \cong \text{Gal}(L/K) / \text{Gal}(L/E) \). Since \( |X| = [E : K] = [L : F] \), \( \text{Perm}(X) \cong \text{Perm}(J) \). We construct a Hopf Galois structure of \( L/K \) from Hopf Galois structures of \( L/E \) and \( E/K \) as follows.

**Theorem 3.1 (Induction).** Assume that \( N_1 \leq \text{Perm}(X) \) gives \( E/K \) a Hopf Galois structure and \( N_2 \leq \text{Perm}(G') \) gives \( L/E \) a Hopf Galois structure. Then, \( L/K \) has a Hopf Galois structure of type \( N_1 \times N_2 \).

**Proof.** See \cite{4} Theorem 3].

Let us add some clarifications to the statement. Hopf Galois structures of \( L/K \) are given by the regular subgroups of \( \text{Perm}(G) \) normalized by \( \lambda(G) \). We embed the group \( N_1 \times N_2 \) as a subgroup of \( \text{Perm}(G) \) by means of

\[
(\varphi, \psi) \mapsto \varphi \psi := \sigma \tau \mapsto \varphi(\sigma) \psi(\tau), \ \sigma \in J, \tau \in G'.
\]

Since \( J \cap G' = \{\text{Id}\} \), in each coset of \( X = G/G' \) there is a unique element of \( J \). Then, we define \( \varphi(\sigma) \) as the unique element of \( J \) in the coset \( \varphi(\sigma) \). We have

\[
\varphi(\sigma_1) = \varphi(\sigma_2) \implies \sigma_1 = \sigma_2 \implies \sigma_1 \sigma_2^{-1} \in G' \cap J = \{1\} \implies \sigma_1 = \sigma_2.
\]

Although in Theorem 3.1 giving a regular subgroup of \( \text{Perm}(G) \) normalized by \( \lambda(G) \) is enough to completely determine a Hopf Galois structure of \( L/K \) by Greither-Pareigis theorem, we can give a more precise description of the Hopf algebra and the Hopf action of an induced Hopf Galois structure. These results will show better how induction works.

**3.1. Hopf algebras involved.** Our first aim is to establish the relationship between the Hopf algebra of the induced Hopf Galois structure of \( L/K \) and the Hopf algebras of the Hopf Galois structures of \( E/K \) and \( F/K \).

Let \( N_1 \) (resp. \( N_2 \)) give \( E/K \) (resp. \( L/E \)) a Hopf Galois structure, so \( N = N_1 \times N_2 \) gives \( L/K \) a Hopf Galois structure. Translated to Hopf algebras, this says
that the Hopf Galois structures \( H_1 = L[N_1]^G \) of \( E/K \) and \( H_2 = L[N_2]^G \) of \( L/E \) give \( L/K \) the Hopf Galois structure \( H = L[N_1 \times N_2]^G \).

\[
\begin{array}{c}
E \\
\downarrow \\
H_1 \\
H \\
\downarrow \\
F \\
\downarrow \\
K \\
\end{array}
\]

In \[6\], Kohl, Koch, Truman and Underwood established an injective map

\[
\Psi : \{ \text{G-stable subgroups of } N \} \rightarrow \{ \text{Subgroups of } G \} \quad P \rightarrow \text{Gal}(L/L^P)^G .
\]

In our case, \( N_1 \) is a \( G \)-stable subgroup of \( N \). By the injective correspondence with intermediate fields of \( L/K \) (see \[3\] Theorem 2.3), it corresponds to the intermediate field \( L^{H_1} = (E \otimes_K F)^{H_1} = F \). Hence, its image under \( \Psi \) is \( \text{Gal}(L/F) = J \). By \[6\] Theorem 3.1, there is a short exact sequence of \( K \)-Hopf algebras

\[
1 \longrightarrow H_1 \longrightarrow H \longrightarrow \overline{\mathcal{H}} \longrightarrow 1 ,
\]

where \( \overline{\mathcal{H}} = F[N_2]^{G/J} \). By \[6\] Theorem 2.9, \( \overline{\mathcal{H}} \) gives \( F/K \) a Hopf Galois structure.

Hence we have obtained that the Hopf algebra of an induced Hopf Galois structure fits a short exact sequence with the Hopf Galois structures \( H_1 \) and \( \overline{\mathcal{H}} \) from which it is induced. But there is a deeper relation: \( H \) is actually the tensor product \( H_1 \otimes_K \overline{\mathcal{H}} \).

**Proposition 3.2.** Let \( H = L[N]^G \) be a Hopf algebra of the Hopf Galois structure of \( L/K \) induced by \( H_1 = L[N_1]^G \) and \( H_2 = L[N_2]^G \). Let \( \overline{\mathcal{H}} = F[N_2]^{G/J} \). Then, there is an isomorphism of \( K \)-Hopf algebras

\[
H \cong H_1 \otimes_K \overline{\mathcal{H}} .
\]

**Proof.** We have that \( L[N_1 \times N_2] \cong L[N_1] \otimes_L L[N_2] \) by means of the isomorphism (of \( K \)-Hopf algebras) given by \( n_1 n_2 \mapsto n_1 \otimes n_2 \) and extended by \( L \)-linearity. On the other hand, the action of \( G \) over \( N = N_1 \times N_2 \) is given by

\[
g(n_1 n_2) = gn_1 n_2 g^{-1} = gn_1 g^{-1} n_2 g^{-1} = g(n_1) g(n_2), \quad g \in G, \quad n_1, n_2 \in N .
\]

Hence, \( G \) acts through the previous isomorphism over \( L[N_1] \otimes_L L[N_2] \) as

\[
g(n_1 \otimes n_2) = g(n_1) \otimes g(n_2), \quad g \in G, \quad n_1, n_2 \in N ,
\]

which says that \( (L[N_1] \otimes_L L[N_2])^G \cong L[N_1]^G \otimes_K L[N_2]^G \). Then, taking fixed algebras in the previous isomorphism, we obtain

\[
L[N_1 \times N_2]^G \cong L[N_1]^G \otimes_K L[N_2]^G = L[N_1]^G \otimes_K F[N_2]^{G/J} .
\]

\( \square \)
It is trivial that, conversely, any such Hopf Galois structure is induced. Then, we can summarize the information obtained up to this point in the following.

**Corollary 3.3.** Let $L/K$ be a finite Galois extension of fields whose Galois group admits some decomposition as a semidirect product. The Hopf algebras of induced Hopf Galois structures of $L/K$ are those of the form

$$H = H_1 \otimes_K \mathcal{H},$$

where $H_1$ (resp. $\mathcal{H}$) comes from a Hopf Galois structure of $L^{G'}/K$ (resp. $L^J/K$), and $(J,G')$ is any pair such that $G = J \rtimes G'$, $J$ normal subgroup of $G$.

Then, induced Hopf Galois structures of $L/K$ correspond to decompositions of $G$ as semidirect product (however this correspondence is not bijective because intermediate fields may have several Hopf Galois structures). From now on, every time we take an induced Hopf Galois structure with $H = H_1 \otimes_K \mathcal{H}$ of $L/K$ we will assume implicitly that $G = J \rtimes G'$ with $J$ normal subgroup of $G$, $E = L^{G'}/K$ is $H_1$-Galois and $F = L^J/K$ is $\mathcal{H}$-Galois.

**Example 3.4.** Let us assume that $G \cong D_{2p}$, the dihedral group of order $2p$ with $p$ an odd prime, and let us fix a presentation

$$G = \langle r, s \mid r^p = s^2 = 1, sr = r^{-1}s \rangle.$$

Then $G = J \rtimes G'$ with $J = \langle r \rangle$ the unique order $p$ subgroup of $G$ and $G'$ any of the $p$ different order 2 subgroups $G' = \langle r^d s \rangle$ with $0 \leq d \leq p - 1$. Therefore, $F = L^J/K$ is the unique degree 2 subextension of $L/K$, while there are $p$ possible degree $p$ subextensions $E_d/K$ of $L/K$, $E_d = L^{(r^d s)}$. Hence, $L/K$ has $p$ induced Hopf Galois structures, which are those of the having

$$H = L[^{(\lambda(r))}^G] \otimes_K F[^{(\rho(r^d s))}^{G'}], \ 0 \leq d \leq p - 1.$$

3.2. Hopf actions involved. In this section we study the Hopf action of an induced Hopf Galois structure $H = L[N]^G$ of $L/K$ in terms of the action of $H_1 = L[N_1]^G$ over $E$ and the action of $\mathcal{H} = F[N_2]^{G/J}$ over $F$.

**Proposition 3.5.** Let $\alpha, z$ be primitive elements of $E/K$, $F/K$ respectively. Let $w \in H_1$ and $\eta \in \mathcal{H}$. Then,

$$(w\eta) \cdot (\alpha^k z^l) = (w \cdot \alpha^k)(\eta \cdot z^l).$$

**Proof.** As $w \in L[N_1]^G$ and $\eta \in F[N_2]^{G/J}$, let us write

$$w = \sum_{i=1}^{r} c_i n_i^{(1)}, \ c_i \in L, \ \ \eta = \sum_{j=1}^{u} d_j n_j^{(2)}, \ d_j \in F,$$

where $N_1 = \{n_i^{(1)}\}_{i=1}^{r}$ and $N_2 = \{n_j^{(2)}\}_{j=1}^{u}$. Then, elements of $N = N_1 \times N_2$ can be written as

$$n_i^{(1)} n_j^{(2)}, \ 1 \leq i \leq r, \ 1 \leq j \leq u.$$
Theorem 3.6. Consider an induced Hopf Galois structure of \( L/K \). They act over elements of \( H \leq 0 \) \( \gamma \) let us call \( M \) above notation. Let \( H \), \( L \)

\[
\begin{align*}
(w\eta) \cdot (\alpha^k z^l) &= \left( \sum_{i=1}^{r} \sum_{j=1}^{u} c_i d_j n_i^{(1)} n_j^{(2)} \right) \cdot (\alpha^k z^l) \\
&= \sum_{i=1}^{r} \sum_{j=1}^{u} c_i d_j (n_i^{(1)} n_j^{(2)})^{-1} (\text{Id})(\alpha^k z^l) \\
&= \sum_{i=1}^{r} \sum_{j=1}^{u} c_i d_j (n_i^{(1)})^{-1} (n_j^{(2)})^{-1} (\text{Id})(\alpha^k z^l)
\end{align*}
\]

Let us determine how suitable linear combinations of \( n_i^{(1)} n_j^{(2)} \) act over \( \alpha^k z^l \). They act over elements of \( G \) as embedded elements of \( N_1 \times N_2 \). In particular,

\[
(n_i^{(1)})^{-1}(n_j^{(2)})^{-1}(\text{Id}) = (n_i^{(1)})^{-1}(\text{Id})(n_j^{(2)})^{-1}(\text{Id}).
\]

Now, \( (n_i^{(1)})^{-1}(\text{Id}) \in J \) fixes \( z^l \) and \( (n_j^{(2)})^{-1}(\text{Id}) \in G' \) fixes \( \alpha^k \), so

\[
(n_i^{(1)})^{-1}(\text{Id})(n_j^{(2)})^{-1}(\text{Id})(\alpha^k z^l) = (n_i^{(1)})^{-1}(\text{Id})(\alpha^k)(n_j^{(2)})^{-1}(\text{Id})(z^l).
\]

Hence,

\[
\begin{align*}
(w\eta) \cdot (\alpha^k z^l) &= \sum_{i=1}^{r} \sum_{j=1}^{u} c_i d_j (n_i^{(1)})^{-1}(\text{Id})(n_j^{(2)})^{-1}(\text{Id})(\alpha^k z^l) \\
&= \sum_{i=1}^{r} \sum_{j=1}^{u} c_i d_j (n_i^{(1)})^{-1}(\text{Id})(\alpha^k)(n_j^{(2)})^{-1}(\text{Id})(z^l) \\
&= \left( \sum_{i=1}^{r} c_i (n_i^{(1)})^{-1}(\text{Id})(\alpha^k) \right) \left( \sum_{j=1}^{u} d_j (n_j^{(2)})^{-1}(\text{Id})(z^l) \right) \\
&= \left( \sum_{i=1}^{r} c_i n_i \right) \cdot \alpha^k \left( \sum_{j=1}^{u} d_j n_j \right) \cdot z^l = (w \cdot \alpha^k)(\eta \cdot z^l).
\end{align*}
\]

Once we have this, we can study the matrix of an induced Hopf action.

\textbf{Theorem 3.6.} Let \( L/K \) be a finite Galois extension of fields of degree \( n \). We consider an induced Hopf Galois structure of \( L/K \) with \( H = H_1 \otimes_K \mathbb{P} \), in the above notation. Let \( M^{(c)}(H, L) = (m^{(c)}_{\zeta \theta})(H, L) \) be the \( c \)-th block of the matrix \( M(H, L) \), \( 0 \leq c \leq n - 1 \). Then,

\[
m^{(c)}_{\zeta \theta}(H, L) = m^{(a)}_{ik}(H_1, E) m^{(b)}_{jl}(\mathbb{P}, F),
\]

where, for each \( 0 \leq \zeta, \theta, c \leq n - 1 \), \( \zeta = i + rj \), \( \theta = k + rl \) and \( c = a + rb \) are the euclidean divisions by \( r \).

\textbf{Proof.} Let \( \{ w_i \}_{i=0}^{r-1} \) be a \( K \)-basis of \( H_1 \) and let \( \{ \eta_j \}_{j=0}^{u-1} \) be a \( K \)-basis of \( \mathbb{P} \). Since \( H = H_1 \otimes_K \mathbb{P} \), \( \{ w_i \eta_j | 0 \leq i \leq r - 1, 0 \leq j \leq u - 1 \} \) is a \( K \)-basis of \( H \). Given \( 0 \leq \zeta = i + rj \leq n - 1 \), let us call \( w_\zeta = w_i \eta_j \). On the other hand, since \( L = E \otimes_K F \), \( \{ \alpha^k z^l | 0 \leq k \leq r - 1, 0 \leq l \leq u - 1 \} \) is a \( K \)-basis of \( L \). For each \( 0 \leq \theta = k + rl \leq n - 1 \), let us call \( \gamma_\theta = \alpha^k z^l \).
Given $0 \leq \zeta, \theta \leq n - 1$, the action of $H$ over $L$ is described by

$$w_{\zeta} \cdot \gamma_{\theta} = \sum_{c=0}^{n-1} m_{\zeta \theta}^c (H, L) \gamma_c.$$ 

But we can obtain an alternative expression using Proposition 3.5 as follows:

$$w_{\zeta} \cdot \gamma_{\theta} = (w_i \gamma_j) \cdot (\alpha_k^a \cdot z^b) = (w_i \cdot \alpha_k^a)(\eta_j \cdot z^b)$$

$$= \left( \sum_{a=0}^{r-1} m_{ik}^a (H_1, E) \alpha^a \right) \left( \sum_{b=0}^{u-1} m_{jl}^b (\overline{H}, F) z^b \right)$$

$$= \sum_{a=0}^{r-1-1} \sum_{b=0}^{u-1} m_{ik}^a (H_1, E) m_{jl}^b (\overline{H}, F) \alpha^a z^b$$

$$= \sum_{c=0}^{n-1} m_{ik}^c (H_1, E) m_{jl}^c (\overline{H}, F) \gamma_c,$$ 

the last equality due to the fact that $a + rb$ runs through $\{0, ..., n - 1\}$ as $a$ runs through $\{0, ..., r - 1\}$ and $b$ runs through $\{0, ..., u - 1\}$.

Since $\{\gamma_c\}_{c=0}^{n-1}$ is a $K$-basis of $L$, uniqueness of coordinates gives the desired equalities. \hfill \Box

**Corollary 3.7.** The matrix $M(H, L)$ is the Kronecker product of $M(H_1, E)$ and $M(\overline{H}, F)$, that is

$$M(H, L) = M(H_1, E) \otimes M(\overline{H}, F).$$

**Example 3.8.** We consider again Example 2.6. In that case, we have the diagram

```
      L
     /\  
    E \  /  H \  /  F
   /    \    /    /
  H_1  K  \overline{H}
```

where $E = \mathbb{Q}_3(\alpha)$, $\alpha$ root of $f$, and $F = \mathbb{Q}_3(\sqrt{-3}) = \sqrt{-3}$. After deleting the zero rows, $M(H_1, E)$ becomes the matrix

$$\begin{pmatrix}
1 & 0 & 2 \\
1 & 3 & -1 \\
1 & -1 & 3
\end{pmatrix}.$$ 

On the other hand, the matrix $M(\overline{H}, F)$ after deleting the zero rows becomes the matrix

$$\begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix}.$$
Hence, $M(H, L)$ after deleting the zero rows is the Kronecker product
\[
\begin{pmatrix}
1 & 0 & 2 \\
1 & 3 & -1 \\
1 & -1 & 3 \\
1 & 0 & 2 \\
1 & 3 & -1 \\
1 & -1 & 3
\end{pmatrix}
\begin{pmatrix}
1 & 0 & 2 \\
1 & 3 & -1 \\
1 & -1 & 3 \\
1 & 0 & 2 \\
1 & 3 & -1 \\
1 & -1 & 3
\end{pmatrix}.
\]

4. Associated order to a Hopf Galois action

Let $L/K$ be an $H$-Galois extension of $p$-adic fields. The associated $\mathcal{O}_K$-order to $\mathcal{O}_L$ in $H$ is
\[
\mathfrak{A}_H = \{ \alpha \in H \mid \alpha \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L \}.
\]

In this section we establish a general method to compute an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$. Then, we assume that the Hopf Galois structure is induced and we combine the actions of $H_1$ over $E$ and $\mathcal{H}$ over $M$ in order to obtain an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.

4.1. Computing a basis of $\mathfrak{A}_H$. Let $L/K$ be a degree $n$ $H$-Galois extension of $p$-adic fields. Let us take a $K$-basis $\{w_0, ..., w_{n-1}\}$ of $H$. In order to compute an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$, we need an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. Take an element $\gamma \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\gamma]$ (for instance, $\gamma = \pi_L$). Then, $\{1, \gamma, ..., \gamma^{n-1}\}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. The element $\gamma$ is also a primitive element of $L/K$, so $\{1, \gamma, ..., \gamma^{n-1}\}$ is a $K$-basis of $L$. The action of $H$ over $L$ is given by
\[
w_i \cdot \gamma^j = \sum_{k=0}^{n-1} m_{ij}^{(k)}(H, L)\gamma^k,
\]
where $m_{ij}^{(k)}(H, L)$ are the entries of the matrix $M^{(k)}(H, L)$, the $k$-th block of $M(H, L)$.

**Theorem 4.1.** Let $h = \sum_{i=0}^{n-1} h_i w_i \in H$, $h_i \in K$. Then, $h \in \mathfrak{A}_H$ if and only if
\[
M(H, L) \begin{pmatrix} h_0 \\ \vdots \\ h_{n-1} \end{pmatrix} \in \mathcal{O}_K^n.
\]

**Proof.** By definition, $h \in \mathfrak{A}_H$ if and only if $h \cdot x \in \mathcal{O}_L$ for all $x \in \mathcal{O}_L$. Fix $x \in \mathcal{O}_L$. Since $\mathcal{O}_L = \mathcal{O}_K[\gamma]$, we can write $x = \sum_{j=0}^{n-1} x_j \gamma^j$, with $x_j \in \mathcal{O}_K$, $0 \leq j \leq n-1$. We compute
\[
h \cdot x = \left( \sum_{i=0}^{n-1} h_i w_i \right) \left( \sum_{j=0}^{n-1} x_j \gamma^j \right) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} h_i x_j w_i \cdot \gamma^j
\]
\[
= \sum_{k=0}^{n-1} \left( \sum_{j=0}^{n-1} x_j \left( \sum_{i=0}^{n-1} m_{ij}^{(k)}(H, L)h_i \right) \right) \gamma^k.
\]

Then, $h \in \mathfrak{A}_H$ if and only if $\sum_{i=0}^{n-1} x_j \left( \sum_{i=0}^{n-1} m_{ij}^{(k)}(H, L)h_i \right) \in \mathcal{O}_K$ for all $x_0, ..., x_{n-1} \in \mathcal{O}_K$ and all $0 \leq k \leq n-1$. This happens if and only if $\sum_{i=0}^{n-1} m_{ij}^{(k)}(H, L)h_i \in \mathcal{O}_K$ for all $0 \leq j, k \leq n-1$. □
Given \( h = \sum_{i=0}^{n-1} h_i w_i \in \mathbb{A}_H \), we would like to know an expression for the vector of coordinates \( h_0, \ldots, h_{n-1} \). The previous result says that it becomes a vector of integers in \( K \) when multiplied by \( M(H, L) \). If we had an invertible matrix instead of \( M(H, L) \), we would be able to express such vector as the inverse matrix applied to a vector of integers. We seek then to obtain an equivalent condition in which \( M(H, L) \) is replaced by an invertible \( n \times n \) matrix.

Recall that \( M(H, L) \) is a matrix with \( n^2 \) rows and \( n \) columns. Since it has rank \( n \), it can be reduced by Gauss method to a square matrix of order \( n \). Moreover, this can be done by using only elementary transformations \( f \) such that for \( x \in K \), \( x \in \mathcal{O}_K \) if and only if \( f(x) \in \mathcal{O}_K \). Such elementary transformations are called \textbf{integral}. The elementary transformations that are not integral are the following:

- Multiply a row by a non-integer of \( K \) or by a non-invertible element of \( \mathcal{O}_K \).
- Sum a non-integer multiple of a row to another row.

\textbf{Theorem 4.2 (Integer-preserving Gauss method).} Let \( K \) be a \( p \)-adic field and let \( M \) be a matrix of size \( n \times m \) with \( m \geq n \geq 1 \) and with rank \( n \). Then, there exists a finite sequence of integral elementary transformations such that when applied to \( M \), we obtain a square matrix \( \Phi \in \mathcal{M}_n(K) \).

\textbf{Proof.} By the standard Gauss method, we know that \( M \) can be reduced to a square matrix of order \( n \) by means of a finite sequence of elementary transformations. We introduce slight modifications in the method in order to prove that we only need integral elementary transformations.

Since \( \Phi \) has rank \( n \) and \( n \) columns, it must have some non-zero element in its first column. We may assume that it is in the \((0, 0)\) position by exchanging rows if necessary. It is enough to prove that there exist integral elementary transformations such that we obtain a non-zero element in the \((0, 0)\) position and zeroes in the remainder of the column. Indeed, if we are able to do this, we can repeat the procedure on the second column by placing a non-zero element in the \((1, 1)\) position and making zeroes below. At the end, we obtain a square matrix since \( M \) has rank \( n \).

This amounts to prove that if \( c \in K \) is in the \((i, 0)\) position of \( M \) and \( d \in K \) is in the \((j, 0)\), then there exists a sequence of integral elementary transformations by which we can make \( 0 \) in position \((i, 0)\) or \((j, 0)\). We can assume that \( c \) and \( d \) have the same denominator (otherwise we multiply the same element of \( \mathcal{O}_K \) both at numerator and denominator in such a way we obtain \( \text{lcm}(c, d) \) in the denominator).

Let us call \( a \in \mathcal{O}_K \) the numerator of \( c \) and \( b \in \mathcal{O}_K \) the numerator of \( d \). With the following distinction of cases we finish the proof:

- \textbf{Case 1:} \( a, b \in \mathcal{O}_K \). Then, \( b - (ba^{-1})a = 0 \), so \( F_j \rightarrow F_j - ba^{-1}F_i \) is an integral elementary transformation which gives a zero in \( F_j \).
- \textbf{Case 2:} \( a \in \mathcal{O}_K^* \) and \( b \in \pi_K \mathcal{O}_K \). Since \( \mathcal{O}_K \) is a PID, Bezout identity holds for elements of \( \mathcal{O}_K \), so there are \( r, s \in \mathcal{O}_K \) such that \( ra + sb = 1 \). Then, the sequence of integral elementary transformations \( F_i \rightarrow rF_i, F_i \rightarrow F_i + sF_j, F_j \rightarrow F_j - bF_i \) gives a zero in \( F_j \).
- \textbf{Case 3:} \( a, b \in \pi_K \mathcal{O}_K \). Then, \( a = p^{k_a}u_a \) and \( b = p^{k_b}u_b \) with \( k_a, k_b \in \mathbb{Z} \) and \( u_a, u_b \in \mathcal{O}_K^* \). Then, the sequence of integral elementary transformations \( F_i \rightarrow u_a^{-1}F_i, F_j \rightarrow u_b^{-1}F_j \) and \( F_i \rightarrow F_i - p^{k_a-b}F_j \) (resp. \( F_j \rightarrow F_j - p^{k_b-k_a}F_i \)) if \( k_a \geq k_b \) (resp. \( k_b \geq k_a \)) gives a zero in \( F_j \).

\( \square \)
Definition 4.3. A reduced matrix of the action of $H$ over $L$ is every square matrix of order $n$ obtained by applying a finite sequence of integral elementary transformations to $M(H, L)$.

We denote the set of reduced matrices of the action of $H$ over $L$ as $\text{Red}(H, L)$. Since all of them have rank $n$, they are invertible. The set of their inverses is denoted by $\text{Red}^{-1}(H, L)$.

**Proposition 4.4.** Let $L/K$ be a degree $n$ $H$-Galois extension of $p$-adic fields. Let $D = (d_{ij})_{i,j=0}^{n-1} \in \text{Red}^{-1}(H, L)$. Then, the elements

\[ v_i = \sum_{l=0}^{n-1} d_{il}w_l, \quad 0 \leq i \leq n - 1 \]

form an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$. The action of this basis over the fixed $\mathcal{O}_K$-basis of $\mathcal{O}_L$ is given by

\[ v_i \cdot \gamma^j = \sum_{k=0}^{n-1} \epsilon_{ij}^{(k)}(H, L)\gamma^k, \]

where we denote $D^k M^{(k)}(H, L) = (\epsilon_{ij}^{(k)}(H, L))$ for all $0 \leq k \leq n - 1$.

**Proof.** Let $h = \sum_{i=0}^{n-1} h_iw_i \in H$. By Theorem 4.1, $h \in \mathfrak{A}_H$ if and only if

\[ M(H, L)\begin{pmatrix} h_0 \\ \vdots \\ h_{n-1} \end{pmatrix} \in \mathcal{O}_K^n. \]

By Theorem 4.2, there exists a sequence of integral linear transformations that reduce $M(H, L)$ to an element of $\text{Red}(H, L)$. Moreover, by definition, every element of $\text{Red}(H, L)$ arises in this way. Hence, the last condition is equivalent to

\[ C\begin{pmatrix} h_0 \\ \vdots \\ h_{n-1} \end{pmatrix} \in \mathcal{O}_K^n \]

for every $C \in \text{Red}(H, L)$. This happens if and only if for every $D \in \text{Red}^{-1}(H, L)$ there exists a vector of integers $c_i^{(D)} \in \mathcal{O}_K$ such that

\[ \begin{pmatrix} h_0 \\ \vdots \\ h_{n-1} \end{pmatrix} = D\begin{pmatrix} c_0^{(D)} \\ \vdots \\ c_{n-1}^{(D)} \end{pmatrix}. \]

Let us fix $D = (d_{ij})_{i,j=0}^{n-1} \in \text{Red}^{-1}(H, L)$ and call $c_i^{(D)} = c_i$. If $h \in \mathfrak{A}_H$, then

\[ h_l = \sum_{i=0}^{n-1} d_{il}c_i, \quad 0 \leq i, l \leq n - 1, \]

which is equivalent to

\[ h = \sum_{l=0}^{n-1} \sum_{i=0}^{n-1} d_{il}c_iw_l = \sum_{i=0}^{n-1} c_i \left( \sum_{l=0}^{n-1} d_{il}w_l \right) = \sum_{i=0}^{n-1} c_iw_i \in \langle v_0, \ldots, v_{n-1} \rangle_{\mathcal{O}_K}. \]

Then $\{v_0, \ldots, v_{n-1}\}$ is a system of generators of $\mathfrak{A}_H$. Now, it is $K$-linearly independent because $D$ is invertible and $\{w_i\}_{i=0}^{n-1}$ is a $K$-basis, so it is also $\mathcal{O}_K$-linearly independent and hence an $\mathcal{O}_K$-basis for $\mathfrak{A}_H$. \qed
Example 4.5. Let us consider again Example 2.7, where we computed

\[ M(H_1, E) = \begin{pmatrix}
1 & 0 & 2 \\
0 & -3 & 0 \\
0 & -9 & -1 \\
0 & 0 & 0 \\
1 & 27 & -1 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & -3 & 0 \\
1 & -27 & -1 \\
\end{pmatrix}. \]

By integral linear transformations, it can be reduced to the matrix

\[ C = \begin{pmatrix}
1 & 0 & 2 \\
0 & 27 & -3 \\
0 & -9 & 0 \\
0 & 0 & 0 \\
9 & 6 & 18 \\
0 & 0 & -1 \\
0 & -3 & -9 \\
\end{pmatrix} ∈ \text{Red}(H_1, E). \]

Hence,

\[ D = \frac{1}{9} \begin{pmatrix}
2w_0 - 2w_2 \\
18w_0 - w_1 - 9w_2 \\
\end{pmatrix} ∈ \text{Red}^{-1}(H_1, E) \]

and, by Proposition 4.4,

\[ A_{H_1, H_1} = \mathbb{Z}_3 \left[ w_0, 2w_0 - 2w_2, \frac{18w_0 - w_1 - 9w_2}{9} \right]. \]

4.2. Induced associated order. Let \( L/K \) be a degree \( n \) \( H \)-Galois extension of \( p \)-adic fields with induced Hopf Galois structure. As proved in Section 3, \( L/K \) must be Galois and \( H \) corresponds to a certain decomposition \( G = J \rtimes G' \) of the Galois group with \( J \) normal subgroup of \( G \), in such a way that if \( E = L^{G'} \) and \( F = L^J \), \( E/K \) is \( H_1 \)-Galois and \( F/K \) is \( \overline{H} \)-Galois. Moreover, we have that \( H = H_1 \otimes_K \overline{H} \).

Since \( H, H_1 \) and \( \overline{H} \) correspond to Hopf Galois structures of extensions of \( p \)-adic fields, we can consider the corresponding associated orders \( A_H, A_{H_1}, \) and \( A_{\overline{H}} \) of \( \mathcal{O}_L, \mathcal{O}_E, \) and \( \mathcal{O}_F \), respectively. Here we study the relationship between these objects, which turns out to be the analog of the situation at the level of fields: \( A_H \) is the \( \mathcal{O}_K \)-tensor product of \( A_{H_1} \) and \( A_{\overline{H}} \).

The idea of the proof is to use the method that we have just introduced to compute bases of the associated orders involved and prove that the product of a certain basis of \( A_{H_1} \) and a certain basis of \( A_{\overline{H}} \) is a basis of \( A_H \). We begin with the following technical result:

Proposition 4.6. Let \( K \) be a \( p \)-adic field. Let \( A ∈ \mathcal{M}_{n_A \times m_A}(K) \) with rank \( n_A \) and \( m_A ≥ n_A ≥ 1 \) and \( B ∈ \mathcal{M}_{n_B \times m_B}(K) \) with rank \( n_B \) and \( m_B ≥ n_B ≥ 1 \). Let \( f_A \) (resp. \( f_B \)) be a composition of linear integral transformations such that \( \Phi_A := f_A A ∈ \mathcal{M}_{n_A}(K) \) and \( \Phi_B := f_B B ∈ \mathcal{M}_{n_B}(K) \). Then, there exists a sequence of linear integral transformations by which the Kronecker product \( A ⊗ B \) can be reduced to \( \Phi_A ⊗ \Phi_B ∈ \mathcal{M}_{n_A n_B}(K) \).

Proof. First, we know that \( f_A \) and \( f_B \) exist because of Theorem 2.2. If we call \( A = (a_{ij})_{i,j=0}^{n_A-1} \), the matrix \( A ⊗ B \) can be written by blocks in the following way:
\[ A \otimes B = \begin{pmatrix}
  a_{00} B & a_{01} B & \cdots & a_{0,n_A-1} B \\
  a_{10} B & a_{11} B & \cdots & a_{1,n_A-1} B \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n_A-1,0} B & a_{n_A-1,1} B & \cdots & a_{n_A-1,n_A-1} B
\end{pmatrix} \]

We apply \( f_B \) to each row of blocks, and after deleting the zero rows, we obtain that \( A \otimes B \) can be reduced to the matrix

\[ A \otimes \Phi_B \begin{pmatrix}
  a_{00} \Phi_B & a_{01} \Phi_B & \cdots & a_{0,n_A-1} \Phi_B \\
  a_{10} \Phi_B & a_{11} \Phi_B & \cdots & a_{1,n_A-1} \Phi_B \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n_A-1,0} \Phi_B & a_{n_A-1,1} \Phi_B & \cdots & a_{n_A-1,n_A-1} \Phi_B
\end{pmatrix}. \]

Next, for \( 0 \leq i \leq n_A - 1 \), we apply \( f_A \) to the submatrices of this matrix formed by the \( i \)-th rows of each row of blocks. In such a submatrix, every element in the same column is multiplied by the same entry of \( A \), so they are invariant under integral linear transformations. As a consequence, the previous can be reduced to the matrix \( \Phi_A \otimes \Phi_B \).

\[ \square \]

**Remark 4.7.** 1. The proof is constructive in the sense that it provides a method to reduce a Kronecker product of matrices to a square one (if we consider the integral Gauss method implemented).

2. Although we have reduced first the right matrix in the Kronecker product and then the left one, we are able to do it in the opposite order. In fact, what the result says is that we can reduce a factor in a Kronecker product in such a way that the other one remains invariant.

In our situation, we know by Theorem 3.6 that \( M(H, L) = M(H_1, E) \otimes M(T, F) \), and we can apply the previous result.

**Corollary 4.8.** 1. If \( \Phi_E \in \text{Red}(H_1, E) \) and \( \Phi_F \in \text{Red}(T, F) \), then \( \Phi_E \otimes \Phi_F \in \text{Red}(H, L) \).

2. If \( \Psi_E \in \text{Red}^{-1}(H_1, E) \) and \( \Psi_F \in \text{Red}^{-1}(T, F) \), \( \Psi_E \otimes \Psi_F \in \text{Red}^{-1}(H, L) \).

**Proof.** 1. Let \( f_E \) and \( f_F \) be compositions of linear integral transformations such that \( \Phi_E = f_E M(H_1, E) \) and \( \Phi_F = f_F M(T, F) \). By Proposition 4.6, we can apply sequences of linear integral transformations built from \( f_E \) and \( f_F \) in such a way that \( M(H, L) \) is reduced to the matrix \( \Phi_E \otimes \Phi_F \), which subsequently is a reduced matrix.

2. Since matrices written by blocks may be multiplied by blocks with the usual rules applied to the entries, we have that when \( A \) and \( B \) are invertible, \( (A \otimes B) = A^{-1} \otimes B^{-1} \). Then the result follows immediately from 1. \[ \square \]

Now we apply the method of the previous part to obtain the decomposition of the associated order.

**Theorem 4.9.** Let \( L/K \) be an \( H \)-Galois extension of \( p \)-adic fields with \( H = H_1 \otimes_K \mathcal{P} \) induced. Then,

\[ \mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_K \mathfrak{A}_\mathcal{P}. \]
Proof. Let $\Psi_E = (\psi_{ik}^{(E)})_{i,k=0}^{r-1} \in \text{Red}^{-1}(H_1,E)$ and $\Psi_F = (\psi_{ij}^{(F)})_{j=0}^{u-1} \in \text{Red}^{-1}(\overline{T},F)$. By the previous corollary, $\Psi_E \otimes \Psi_F \in \text{Red}^{-1}(H,L)$. The entries of the matrix $\Psi_E \otimes \Psi_F$ can be described in a similar way as in Theorem 3.3

$$\psi_{\xi\eta}^{(L)} = \psi_{ik}^{(E)} \psi_{jl}^{(F)}, \ 0 \leq \xi, \eta \leq n-1,$$

where, for each $0 \leq \xi, \eta \leq n-1$, $\xi = i + rj$ and $\theta = k + rl$ are the euclidean divisions by $r$.

On the other hand, let $\{w_l\}_{l=1}^{r-1}$ be a $K$-basis of $H_1$ and $\{\eta_m\}_{m=0}^{u-1}$ be a $K$-basis of $\overline{T}$. Since $H = H_1 \otimes_K \overline{T}$, $\{\psi_{l\eta}m\}_{l,m}$ is a $K$-basis of $H$. By Theorem 1.3.

- The elements $v_i = \sum_{l=0}^{r-1} \psi_{li}^{(E)} w_l$, $0 \leq i \leq r-1$, form an $\mathcal{O}_K$-basis of $\mathfrak{A}_{H_1}$.
- The elements $\mu_j = \sum_{m=0}^{u-1} \psi_{mj}^{(F)} \eta_m$, $0 \leq j \leq u-1$, form an $\mathcal{O}_K$-basis of $\mathfrak{A}_{\overline{T}}$.
- The elements $u_{i+j} = \sum_{l=0}^{r-1} \sum_{m=0}^{u-1} \psi_{li}^{(E)} \psi_{mj}^{(F)} \psi_{l\eta}m$, form an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.

Since $u_{i+j} = v_i \mu_j$ for every $0 \leq i \leq r-1$ and every $0 \leq j \leq u-1$, the $\mathcal{O}_K$-basis of $\mathfrak{A}_H$ obtained is the product of the $\mathcal{O}_K$-bases of $\mathfrak{A}_{H_1}$ and $\mathfrak{A}_{\overline{T}}$.

5. Freeness over the associated order

In this part we deal with the problem of the structure of the valuation ring $\mathcal{O}_L$ in an extension of $p$-adic fields $L/K$ as module over its associated order in each Hopf Galois structure. Namely, we would like to find conditions for the freeness of such Hopf Galois module.

First, we find a necessary and sufficient condition for an element $\beta \in \mathcal{O}_L$ to be a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module. Next, we establish a relation between the associated order in a Hopf Galois structure and the one obtained by tensoring with a linearly disjoint field and prove Theorem 1.4. Finally, we consider again the associated order in a Hopf Galois structure and the one obtained by tensoring $\mathcal{O}_L$ in an extension of $L/K$.

We finish the section proving Theorem 1.3.

5.1. Characterization of freeness. Let $L/K$ be a $H$-Galois extension of $p$-adic fields. Let $\{w_l\}_{l=1}^{r-1}$ be a $K$-basis of $H$ and let $\gamma$ be a primitive element of $L/K$ such that $\mathcal{O}_L = \mathcal{O}_K[\gamma]$. Let $D = (d_{ij})_{i,j=0}^{n-1} \in \text{Red}^{-1}(H,L)$. We proved in Proposition 4.3 that the elements

$$v_i = \sum_{l=0}^{n-1} d_{i}w_l, \ 0 \leq i \leq n-1$$

form an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$. Standard linear algebra yields that an element $\beta \in \mathcal{O}_L$ is a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module if and only if the elements $v_i \cdot \beta \in \mathcal{O}_L$ are $\mathcal{O}_K$-linearly independent. This property will be used repeatedly throughout this section and will be the key to prove the main results. We will write it in a more explicit way using matrices.

**Definition 5.1.** We call the associated matrix to the element $\beta \in \mathcal{O}_L$ in $H$ (denoted by $D_\beta^{H}$) the matrix whose rows are the coordinates of $v_i \cdot \beta$ with respect to the basis $\{1, \gamma, ..., \gamma^{n-1}\}$.

The $\mathcal{O}_K$-linear independence of the elements $v_i \cdot \beta$ is equivalent to the invertibility of $D_\beta^{H}$. This leads to the following.

**Corollary 5.2.** An element $\beta \in \mathcal{O}_L$ is a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module if and only if $D_\beta^{H} \in \mathcal{M}_n(\mathcal{O}_K)^*$. 


ON INDUCED HOPF GALOIS STRUCTURES AND LOCAL MODULES

Let \( \beta = \sum_{k=0}^{n-1} \beta_k \gamma^k \). Let us compute explicitly the entries of \( D^H_{\beta} \). This involves computing the coordinates of \( v_i \cdot \beta \) for all \( 0 \leq i \leq n - 1 \). We have:

\[
v_i \cdot \beta = \sum_{k=0}^{n-1} \beta_k v_i \cdot \gamma^k = \sum_{k=0}^{n-1} \gamma_k \sum_{l=0}^{n-1} \epsilon_{ik}^{(l)} (H, L) \gamma^l = \sum_{l=0}^{n-1} \beta_k \epsilon_{ik}^{(l)} (H, L) \gamma^l.
\]

Hence, \( D^H_{\beta} = \left( \sum_{k=0}^{n-1} \beta_k \epsilon_{ik}^{(l)} (H, L) \right)_{i,l=0}^{n-1} \).

Remark 5.3. Although it is not true that \( \epsilon_{il}^{(k)} (H, L) \in \mathcal{O}_K \) in general, we have \( \sum_{k=0}^{n-1} \beta_k \epsilon_{ik}^{(l)} (H, L) \in \mathcal{O}_K \) because \( v_i \cdot \beta \in \mathcal{O}_L \) as \( v_i \in \mathfrak{A}_H \) and \( \beta \in \mathcal{O}_L \).

Example 5.4. Let \( L/K \) be a quadratic extension of \( p \)-adic fields, which is known to have the classical Galois structure \( K[G] \) as its unique Hopf Galois structure. Since \( p \geq 3 \), \( L/K \) is tamely ramified and then \( \mathcal{O}_L \) is \( \mathfrak{A}_K[G] \)-free. Let \( z \in L \) such that \( z \notin K \) and \( z^2 \in K \). Let us prove that \( \mathcal{O}_L \) has free generator \( 1 + z \).

The elements of the Galois group \( G \) of \( L/K \) are the identity \( \text{Id}_L \) and the \( K \)-automorphism \( \sigma : L \rightarrow L \) given by \( \sigma(z) = -z \). These two elements form a \( K \)-basis of \( K[G] \). The action of this basis over \( L \) is given by

\[
\begin{pmatrix}
1 & z \\
1 & -z
\end{pmatrix},
\]

Then, after deleting the zero rows, \( M(K[G], L) \) is reduced to the matrix

\[
\Phi = \begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix} \in \text{Red}(K[G], L),
\]

which is a reduced matrix since it is quadratic. Its inverse is

\[
\Psi = \frac{1}{2} \begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix} \in \text{Red}^{-1}(K[G], L).
\]

By Theorem 4.4,

\[
\mathfrak{A}_K[G] = \mathcal{O}_K \left[ \frac{\text{Id}_L + \sigma}{2}, \frac{\text{Id}_L - \sigma}{2} \right].
\]

Since \( \mathcal{O}_L = \mathcal{O}_K[z] \), the action of this \( \mathcal{O}_K \)-basis over \( 1 + z \) is given by

\[
\frac{\text{Id}_L + \sigma}{2} \cdot (1 + z) = 1, \quad \frac{\text{Id}_L - \sigma}{2} \cdot (1 + z) = z.
\]

Thus,

\[
D^{[K[G]]}_{1+z} = \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix},
\]

which is clearly invertible, so \( 1 + z \) generates \( \mathcal{O}_L \) as \( \mathfrak{A}_K[G] \)-module.

Example 5.5. Let \( E/Q_3 \) be the extension in Example 2.7. We know by Example 4.3 that

\[
\mathfrak{A}_{H_1} = \mathbb{Z}_3 \left[ w_0, \frac{2w_0 - w_2}{3}, \frac{18w_0 - w_1 - 9w_2}{9} \right].
\]

Using the table (2) in Example 2.7, we compute the action of this matrix over \( \mathcal{O}_E \):
Thus, the associated matrix to $O_\gamma$ is

$$D^H_\gamma = \begin{pmatrix} \gamma_0 & \gamma_1 & \gamma_2 \\ \gamma_1 & \gamma_1 & \gamma_2 \\ 2\gamma_1 + 6\gamma_2 & 0 & \gamma_1 + 6\gamma_2 \end{pmatrix}.$$

In particular, if $\gamma = 1 + \alpha$ (i.e., $\gamma_0 = \gamma_1 = 1$ and $\gamma_2 = 0$), then $D^H_\gamma$ is invertible in $M_3(\mathcal{O}_K)$, so $\mathcal{O}_E = \mathfrak{A}_{H_1} \cdot \gamma$.

5.2. Associated orders and tensor products. Let $L/F$ be a degree $n$ $H$-Galois extension of $p$-adic fields with $H = H_1 \otimes_H \mathbb{F}$ induced. We particularize the previous questions on basis of the associated order and freeness of $O_L$ over the associated order to the situation where the Hopf Galois structure of $L/F$ is $H_1 \otimes_K F$. Note that this is actually a Hopf Galois structure of $L/F$ because $H_1$ is a Hopf Galois structure of $E/K$ and $F$ is $K$-faithfully flat. Moreover, the action of $H_1 \otimes_K F$ over $L$ is obtained by extending $F$-linearly the one of $H_1$ over $E$.

We study the relationship between $\mathfrak{A}_{H_1}$ and $\mathfrak{A}_{H_1} \otimes_K F$, as well as the $\mathfrak{A}_{H_1}$ freeness of $O_E$ and the $\mathfrak{A}_{H_1} \otimes_K F$-freeness of $O_L$. In order to do this, we need a suitable description of elements of $O_L$. We know that $L = K(\alpha, z)$, and as one can expect it is true that $O_L = O_K[\alpha, z]$. We make use of the following result.

**Lemma 5.6.** Let $R \rightarrow S$ be an étale ring map and let $R \rightarrow B$ be any ring map. Let $A \subset B$ be the integral closure of $R$ in $B$ and let $A' \subset S \otimes_R B$ be the integral closure of $S$ in $S \otimes_R B$. Then the canonical map $S \otimes_R A \rightarrow A'$ is an isomorphism.

**Proof.** See [7] Lemma 10.143. \qed

From this we can express $O_L$ as a tensor product.

**Proposition 5.7.** With the previous notation, $O_L = O_E \otimes_{O_F} O_F$.

**Proof.** By definition, $O_E$ is the integral closure of $O_K$ in $E$. Since $F/K$ is an extension of $p$-adic fields, the map of rings $O_K \rightarrow O_F$ is étale. Applying Lemma 4.6 with $R = O_K$, $S = O_F$, and $B = E$, the integral closure of $O_F$ in $O_F \otimes_{O_K} E = E \otimes_K F = L$ is $O_E \otimes_{O_K} O_F$. But such integral closure is known to be $O_L$, so we conclude that $O_L = O_E \otimes_{O_K} O_F$. \qed

The description is explicit when we take generators of the valuation rings as $O_K$-algebras.

**Corollary 5.8.** Let $\alpha, z$ be primitive elements of $E/K$, $F/K$ such that $O_E = O_K[\alpha]$ and $O_F = O_K[\alpha]$. Then, $O_L = O_K[\alpha, z]$. 

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
$w_0$ & 1 & $\alpha$ \\
\hline
$2w_0 - w_3$ & $\alpha$ & $\alpha^2$ \\
\hline
$18w_0 - 6w_3 - 9w_5$ & $\alpha^2 + 1$ & 6$\alpha^2 + 6$ \\
\hline
\end{tabular}
\caption{Matrix representation of $O_\gamma$}
\end{table}
As a consequence, every $\beta \in \mathcal{O}_L$ can be written as

$$\beta = \sum_{j=0}^{u-1} \beta^{(j)} z^j,$$

where $\beta^{(j)} \in \mathcal{O}_E$ for every $0 \leq j \leq u - 1$.

**Proposition 5.9.** With the previous notation, $\mathfrak{A}_{H_1 \otimes_K F} = \mathfrak{A}_{H_1 \otimes \mathcal{O}_K} \mathcal{O}_F$.

**Proof.** Call $H^{(1)} = H_1 \otimes_K F$. First, we prove that $\mathfrak{A}_{H_1 \otimes \mathcal{O}_K} \mathcal{O}_F \subset \mathfrak{A}_{H^{(1)}}$. It is clearly contained in $H_1 \otimes \mathcal{O}_K F = H_1 \otimes_K F = H^{(1)}$. On the other hand, it acts $\mathcal{O}_K$-linearly over $\mathcal{O}_L$ componentwise since $\mathcal{O}_L = \mathcal{O}_E \otimes \mathcal{O}_K \mathcal{O}_F$. This proves the claim.

For the other inclusion, let $h \in \mathfrak{A}_{H^{(1)}}$. Trivially, $h \in H^{(1)} = H_1 \otimes_K F$. Now, take a primitive element $z$ of $F/K$ such that $\mathcal{O}_F = \mathcal{O}_K[z]$ (for instance, $z = \pi_F$). Since $\{1, z, \ldots, z^{u-1}\}$ is a $K$-basis of $F$ and $H_1$ is $K$-flat, it is also an $H_1$-basis of $H^{(1)}$. Then,

$$h = \sum_{j=0}^{u-1} h^{(j)} z^j, \quad h^{(j)} \in H_1.$$

The result will follow from the fact that $h^{(j)} \in \mathfrak{A}_{H_1}$ for all $0 \leq j \leq u - 1$. In order to prove this, we may check that $h^{(j)} \cdot \gamma \in \mathcal{O}_E$ for all $\gamma \in \mathcal{O}_E$. Take any such $\gamma \in \mathcal{O}_E$. In particular $\gamma \in \mathcal{O}_L$, and since $h \in \mathfrak{A}_{H^{(1)}}$, we have that $h \cdot L \gamma \in \mathcal{O}_L$. But

$$h \cdot L \gamma = \left( \sum_{j=0}^{u-1} h^{(j)} z^j \right) \cdot L \gamma = \sum_{j=0}^{u-1} (h^{(j)} \cdot L \gamma) z^j \in \mathcal{O}_L.$$

By Corollary 5.8, $\mathcal{O}_L = \mathcal{O}_E[z]$. Hence, the previous expression yields that $h^{(j)} \cdot E \gamma \in \mathcal{O}_E$ for all $0 \leq j \leq u - 1$. \hfill $\square$

Now, we restate and prove Theorem 1.4.

**Theorem 5.10.** $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free if and only if $\mathcal{O}_L$ is $\mathfrak{A}_{H_1 \otimes_K F}$-free.

**Proof.** One of the implications is immediate: if $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free, since $\mathcal{O}_F$ is $\mathcal{O}_K$-flat, $\mathcal{O}_E \otimes \mathcal{O}_K \mathcal{O}_F = \mathcal{O}_L$ is $\mathfrak{A}_{H_1 \otimes \mathcal{O}_K \mathcal{O}_F}$-free by the previous result, $\mathfrak{A}_{H_1 \otimes \mathcal{O}_K \mathcal{O}_F} = \mathfrak{A}_{H_1 \otimes_K \mathcal{O}_F}$ and the claim follows.

Conversely, let us assume that $\mathcal{O}_L$ is $\mathfrak{A}_{H_1 \otimes_K F}$-free. As in the previous proof, we call $H^{(1)} = H_1 \otimes_K F$. Since both $\mathcal{O}_L$ and $\mathfrak{A}_{H^{(1)}}$ are $\mathcal{O}_K$-free of rank $n = [L : K]$, $\mathcal{O}_L$ must be $\mathfrak{A}_{H^{(1)}}$-free of rank 1. Let $t$ be a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_{H^{(1)}}$-module. By Corollary 5.8, we can write

$$t = \sum_{l=0}^{r-1} \left( \sum_{j=0}^{u-1} t_{lj} z^j \right) \alpha^l, \quad t_{lj} \in \mathcal{O}_K.$$

Let $D = (d_{ij})_{i,j=0}^{u-1} \in \text{Red}^{-1}(H, E)$. By Proposition 4.3, the elements

$$v_i = \sum_{l=0}^{n-1} d_{li} w_l, \quad 0 \leq i \leq r - 1$$
form an \(\mathcal{O}_K\)-basis of \(\mathfrak{A}_{H_1}\). Moreover, the action of this basis over \(\mathcal{O}_E\) is given by

\[
v_i \cdot \alpha^j = \sum_{k=0}^{r-1} c_{ij}^{(k)}(H_1, E) \alpha^k,
\]

where \(D^t M^{(k)}(H_1, E) = (c_{ij}^{(k)}(H_1, E))_{i,j=0}^{r-1}\).

Since \(\mathcal{O}_F\) is \(\mathcal{O}_K\)-flat, \(\{v_i\}_{i=0}^{r-1}\) is an \(\mathcal{O}_F\)-basis of \(\mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathcal{O}_F = \mathfrak{A}_{H_1(1)}\). Then, the system \(\{v_i \cdot t\}_{i=0}^{r-1}\) is \(\mathcal{O}_F\)-linearly independent. We compute the coordinates of such vectors with respect to the \(\mathcal{O}_K\)-basis \(\{1, \alpha, ..., \alpha^{r-1}\}:

\[
v_i \cdot t = v_i \cdot \left( \sum_{l=0}^{r-1} \left( \sum_{j=0}^{u-1} t_{lj} z^j \right) \alpha^l \right) = \sum_{l=0}^{r-1} \left( \sum_{j=0}^{u-1} t_{lj} z^j \right) c_{il}^{(k)}(H_1, E) \alpha^k
\]

Hence, the matrix \(\left( \sum_{i=0}^{r-1} \left( \sum_{j=0}^{u-1} t_{lj} z^j \right) c_{il}^{(k)}(H_1, E) \right)_{i,k=0}^{r-1}\) of the coordinates of \(v_i \cdot t\) has non-zero determinant. To compute the determinant we use repeatedly the property of the sum at each column, obtaining:

\[
\det \left( \sum_{i=0}^{r-1} \left( \sum_{j=0}^{u-1} t_{lj} z^j \right) c_{il}^{(k)}(H_1, E) \right)_{i,k=0}^{r-1} = \sum_{a=1}^{u^r} z^d_a D_a,
\]

where:

- \(D_a = \det \left( \sum_{i=0}^{r-1} s_a(l) c_{il}^{(k)}(H_1, E) \right)_{i,k=0}^{r-1}\).
- \(\{s_a\}_{a=1}^{u^r}\) is the set of maps \(s : \{0, ..., u - 1\} \rightarrow \prod_{j=0}^{r-1} \{t_{lj}\}_{i=0}^{r-1}\) such that \(s(l) \in \{t_{lj}\}_{i=0}^{r-1}\) for all \(0 \leq j \leq r - 1\).
- \(d_a = \sum_{x=1}^{u-1} x \# \{l \in \{0, ..., u - 1\} \mid s_a(l) = t_{lx} \}\). Now, the determinant is non-zero, so there exists some \(1 \leq a \leq u^r\) such that \(D_a \neq 0\). Let \(\gamma = \sum_{i=0}^{r-1} s_a(l) \alpha^i \in \mathcal{O}_E\). Then, given \(0 \leq i \leq r - 1\), we have that

\[
v_i \cdot \gamma = \sum_{l=0}^{r-1} s_a(l) v_i \cdot \alpha^l = \sum_{k=0}^{r-1} \left( \sum_{l=0}^{r-1} s_a(l) c_{il}^{(k)}(H_1, E) \right) \alpha^k.
\]

The determinant of the matrix with the coordinates of the vectors \(v_i \cdot \gamma\) with respect to the basis \(\{1, \alpha, ..., \alpha^{r-1}\}\) is \(D_a \neq 0\), so \(\gamma\) is a free generator of \(\mathcal{O}_E\) as \(\mathfrak{A}_{H_1}\)-module. In particular, \(\mathcal{O}_E\) is \(\mathfrak{A}_{H_1}\)-free. \(\square\)
5.3. Freeness over induced associated orders. Let $L/K$ be an $H$-Galois extension with $H = H_1 \otimes_K \overline{H}$ induced. Let $E/K$ be $H_1$-Galois and $F/K$ be $\overline{H}$-Galois. Our aim is to relate the freeness of $O_L$ as $\mathfrak{A}_H$-module with the freeness of $O_E$ as $\mathfrak{A}_{H_1}$-module and the freeness of $O_F$ as $\mathfrak{A}_{\overline{H}}$-module.

We prove that the first one is implied by the other two, which is Theorem 1.3.

Theorem 5.11. Let $L/K$ be an $H$-Galois extension of $p$-adic fields with $H = H_1 \otimes_K \overline{H}$ induced. If $O_E$ is $\mathfrak{A}_{H_1}$-free and $O_F$ is $\mathfrak{A}_{\overline{H}}$-free, then $O_L$ is $\mathfrak{A}_H$-free.

Moreover, if $\gamma$ is a $\mathfrak{A}_{H_1}$-free generator of $O_E$ and $\delta$ is a $\mathfrak{A}_{\overline{H}}$-free generator of $O_F$, then $\gamma \delta$ is a $\mathfrak{A}_H$-free generator of $O_L$.

Proof. Let $\{v_i\}_{i=0}^{r-1}$ be an $O_K$-basis of $\mathfrak{A}_{H_1}$ and let $\{\mu_j\}_{j=0}^{u-1}$ be an $O_K$-basis of $\mathfrak{A}_{\overline{H}}$. Then, $\{(v_i \cdot \gamma)\}_{i=0}^{r-1}$ is an $O_K$-basis of $O_E$ and $\{\mu_j \cdot \delta\}_{j=0}^{u-1}$ is an $O_K$-basis of $O_F$. Since $O_L = O_E \otimes_{O_K} O_F$, the product of these bases is an $O_K$-basis of $O_L$. But that basis is formed by the elements

$$(v_i \cdot \gamma)(\mu_j \cdot \delta) = (v_i \mu_j) \cdot (\gamma \delta), \ 0 \leq i \leq r - 1, \ 0 \leq j \leq u - 1.$$

Since $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{O_K} \mathfrak{A}_{\overline{H}}$, this amounts to say that $\gamma \delta$ is a $\mathfrak{A}_H$-free generator of $O_L$. \hfill \Box

6. An Application: Dihedral Extensions

The results in the previous sections allow to study the induced Hopf Galois structures of certain dihedral extensions.

Let $L/K$ be a dihedral degree $2r$ dihedral extension, with $r$ a Burnside number. Induced Hopf Galois structures of $L/K$ can be described as in the case $r = p$ in Example 3.4 since the structure of $G$ is similar. We obtain the $\mathfrak{A}_H$-freeness of $O_L$ by using Theorem 1.3.

Theorem 6.1. Let $L/K$ be a degree $2r$ dihedral extension of $p$-adic fields, where $r$ is a Burnside number. Let $H = H_1 \otimes_K \overline{H}$ be an induced Hopf Galois structure of $L/K$ corresponding to a decomposition $G = J \rtimes G'$ with $J \cong C_r$ and $G' \cong C_2$. Let $F = L^J$. If $O_L$ is $\mathfrak{A}_{F[J]}$-free, then $O_L$ is $\mathfrak{A}_H$-free.

Proof. First, $L/F$ has Galois group $J \cong C_r$ and hence it is of degree $r$. Since $r$ is Burnside, by Byott’s uniqueness theorem (see [2] (8.1)), $F[J]$ is the unique Hopf Galois structure of $L/F$. Since $H_1 \otimes_K F$ is also a Hopf Galois structure of $L/F$, we have that $H_1 \otimes_K F = F[J]$. By the hypothesis, $O_L$ is $\mathfrak{A}_{H_1 \otimes_K F}$-free. Moreover, since $F/K$ is quadratic, Example 5.4 tells us that $O_F$ is $\mathfrak{A}_{\overline{H}}$-free. The result follows by using Corollary 1.3. \hfill \Box

The case of dihedral degree $2p$ extensions is a particular case of the previous hypothesis since $p$ is a Burnside number. Then, for such extensions we have that the freeness in the classical Galois structure of $L/F$ implies the freeness in induced Hopf Galois structures of $L/K$. We study the Hopf Galois module structure of induced and non-induced Hopf Galois structures of these family of extensions in a forthcoming paper.

References

[1] S.U. Chase, M.E. Sweedler; *Hopf Algebras and Galois Theory*, Lecture Notes in Mathematics, Springer, 1969.
24 DANIEL GIL AND ANNA RIO

[2] L.N. Childs; Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, Mathematical Surveys and Monographs 80, American Mathematical Society, 1986.

[3] T. Crespo, A. Rio, M. Vela; On the Galois correspondence theorem in separable Hopf Galois theory, Publications Matemàtiques vol. 60 1 (2016), 221-234.

[4] T. Crespo, A. Rio, M. Vela; Induced Hopf Galois structures, Journal of Algebra 457 (2016), 312-322.

[5] C. Greither, B. Pareigis; Hopf Galois Theory for Separable Field Extensions, Mathematisches Institut der Universität München, Theresienstr. 39, 8000 Munich 2, West Germany, 1985.

[6] A. Koch, T. Kohl, P. Truman, R. Underwood; Normality and Short Exact Sequences of Hopf-Galois Structures, Communications in Algebra, DOI: 10.1080/00927872.2018.1529237.

[7] Stacks Project, available at: https://stacks.math.columbia.edu/tag/03ge

Universitat Politècnica de Catalunya
E-mail address: daniel.gil.munoz@upc.edu

Universitat Politècnica de Catalunya
E-mail address: ana.rio@upc.edu