3rd *BYMAT Conference* (2020)

Constructing normal integral bases of Hopf Galois extensions

Daniel Gil Muñoz
Universitat Politècnica de Catalunya
daniel_gilmu@hotmail.com

Abstract: A Hopf Galois extension is an extension of fields that has attached a Hopf algebra together with an action on the top field, called a Hopf Galois structure. Every Galois extension is Hopf Galois, but the converse does not hold. For an extension of local or global fields, we recall the definition of associated order in a Hopf Galois structure and use it to generalize the concept of normal integral basis of a Galois extension to Hopf Galois extensions. We shall present a method to construct effectively a normal integral basis of a Hopf Galois extension and apply it to the Hopf Galois non-Galois extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Resumen: Una extensión Hopf Galois es una extensión de cuerpos que tiene asociada un álgebra de Hopf junto con una acción en el cuerpo superior, llamado una estructura Hopf Galois. Toda extensión de Galois es Hopf Galois, pero el recíproco no es cierto. Para una extensión de cuerpos locales o globales, recordamos la definición de orden asociado y la usamos para generalizar el concepto de base normal entera de una extensión de Galois a extensiones Hopf Galois. Presentamos un método para construir de manera efectiva una base normal entera de una extensión y la aplicamos a la extensión Hopf Galois no Galois $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Keywords: Hopf Galois extension, associated order, normal integral basis.

MSC2010: 11R32, 12F10, 16T05.

Acknowledgements: This work is based in some of the main lines of my first article with my PhD advisor Anna Rio, so it would not have been possible without her help. I also want to thank my university for the PhD funding.

Reference: Gil Muñoz, Daniel. "Constructing normal integral bases of Hopf Galois extensions". In: *TEMat monográficos*, 2 (2021): *Proceedings of the 3rd BYMAT Conference*, pp. 47-50. ISSN: 2660-6003. URL: https://temat.es/monograficos/article/view/vol2-p47.

1. Introduction: Hopf Galois extensions

Galois theory establishes a connection between field theory and group theory: for extensions of fields L/K with the property that every polynomial $f \in K[X]$ with a root in L has $\deg(f)$ roots in L (the so called Galois extensions), it is possible to read these extensions algebraically in terms of their Galois group $G := \mathrm{Gal}(L/K)$, the group of all K-automorphisms of L. This theory was introduced by French mathematician Évariste Galois to characterize the solvability by radicals of polynomial equations, and it has been proved as an essential tool in modern algebraic number theory.

The theory of Hopf Galois extensions establishes a similar link between the theory of fields and the one of Hopf algebras. Let L/K be a finite extension of fields and and let G be a group that acts on L by automorphisms. There is a natural group representation of G

$$\begin{array}{rccc} \rho_G: & G & \longrightarrow & \mathrm{Aut}_K(L) \\ & \sigma & \longmapsto & y \mapsto \sigma(y). \end{array}$$

Now, we can extend this map by K-linearity to a map $\rho_{K[G]}: K[G] \to \mathrm{End}_K(L)$ which is a linear representation of the K-group algebra $K[G]$. But $K[G]$ is a K-Hopf algebra and this structure is compatible with its action on L (concretely, L is a $K[G]$-module algebra, see the book [4] for a definition).

Let L/K be a finite extension and assume that H is a K-Hopf algebra that endows L with left H-module algebra structure. Similarly we have a linear representation

$$\begin{array}{rccc} \rho_H: & H & \longrightarrow & \mathrm{End}_K(L) \\ & h & \longmapsto & x \mapsto h \cdot x \end{array}$$

of the K-Hopf algebra H. We can construct a canonical map $(1, \rho_H): L \otimes_K H \to \mathrm{End}_K(L)$ defined by sending each $x \otimes h \in L \otimes_K H$ to the endomorphism $y \mapsto x(h \cdot y)$.

Definition 1. Let L/K be a finite extension of fields. A *Hopf Galois structure* of L/K is a pair $(H, \cdot)$ where H is a K-Hopf algebra and $\cdot: H \otimes_K L \to L$ is a K-linear action of H on L which endows it with K-module algebra structure and such that $(1, \rho_H)$ is an isomorphism of K-vector spaces. A *Hopf Galois extension* is an extension L/K that admits some Hopf Galois structure. If $(H, \cdot)$ is a Hopf Galois structure of L/K, we will also say that L/K is H-Galois. ◂

By construction, every Galois extension is Hopf Galois, because the K-group algebra $K[G]$ of its Galois group together with the evaluation action is a Hopf Galois structure. However, the converse does not hold: for instance, the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is a Hopf Galois extension that is not Galois. This example was used by Greither and Pareigis in their article [3] to nicely illustrate the notion of Hopf Galois extension.

2. The theory of Hopf Galois modules

If F is a number (resp. p-adic) field, we will denote by $\mathcal{O}_F$ its ring of integers, i.e, the elements of K which are roots of monic polynomials with coefficients in $\mathbb{Z}$ (resp. $\mathbb{Z}_p$). From now on, we will deal only with extensions of number or p-adic fields L/K such that $\mathcal{O}_K$ is a principal ideal domain (actually, this is always satisfied when the fields are p-adic). Under this hypothesis, it follows that $\mathcal{O}_L$ is free as $\mathcal{O}_K$-module, and any basis of that module is called an integral basis of L.

One of the applications of Galois theory is the theory of Galois modules, which studies the structure of $\mathcal{O}_L$ as module over its associated order $\mathfrak{A}_{L/K}$ in $K[G]$, where $G = \mathrm{Gal}(L/K)$. This is defined as the maximal $\mathcal{O}_K$-order in $K[G]$ such that its evaluation action on L leaves $\mathcal{O}_L$ invariant. The notion of associated order can be easily generalized to the setting of Hopf Galois theory.

Definition 2. Let L/K be an H-Galois extension of fields as above. The *associated order* of $\mathcal{O}_L$ in H is defined as

$$\mathfrak{A}_H = \{h \in H \mid h \cdot x \in \mathcal{O}_L \ \forall x \in \mathcal{O}_L\}.$$ ◂

The associated order is indeed an $\mathcal{O}_K$-order in H, and in particular it is free as $\mathcal{O}_K$-module. Let $V = \{v_i\}_{i=1}^n$ be an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$. If in addition $\mathcal{O}_L$ is $\mathfrak{A}_H$-free of rank one with generator β, then $\{v_i \cdot \beta \mid 1 \le i \le n\}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$, called a *normal integral basis*. Thus, once computed a basis of $\mathfrak{A}_H$, the key point turns to whether $\mathcal{O}_L$ is free over $\mathfrak{A}_H$. We present a constructive method to answer both questions.

3. The reduction method

Let L/K be an H-Galois extension of number or p-adic fields. The reduction method provides a way to find effectively an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ and determine whether $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. The idea behind the method is the same as in representation theory: instead of working with the elements of the Hopf algebra, we use the matrices representing them. We present the main definitions and results (see the paper [2] for more details).

Definition 3. Let $W = \{w_i\}_{i=1}^n$ and $B = \{\gamma_j\}_{j=1}^n$ be K-bases of H and L respectively. Given $1 \leq j \leq n$, we denote

$$M_j(H,L) = \begin{pmatrix} | & | & \cdots & | \\ w_1 \cdot \gamma_j & w_2 \cdot \gamma_j & \cdots & w_n \cdot \gamma_j \\ | & | & \cdots & | \end{pmatrix} \in \mathcal{M}_{n^2 \times n}(K),$$

that is, $M_j(H,L)$ is the matrix whose i-th column is the column vector of the coordinates of $w_i \cdot \gamma_j$ with respect to the basis B. Then, the *matrix of the action* is defined as

$$M(H,L) = \left(\begin{array}{c} M_1(H,L) \\ \hline \cdots \\ \hline M_n(H,L) \end{array}\right).$$

The key step of the reduction method is to reduce $M(H,L)$ to an invertible matrix by linear transformations, but preserving the integral structure (i.e., multiplying by an unimodular matrix). This can be achieved by considering the Hermite normal form of $M(H,L)$, whose definition is well known for matrices with coefficients in $\mathbb{Z}$ and can be consulted in the book [1] for a general PID. However, $M(H,L)$ may have coefficients out of the ring, but in any case in its field of fractions. What we do in practice is to drop out of the matrix the least common multiple of the denominators and consider as Hermite normal form of $M(H,L)$ the fractional part times the Hermite normal form of the matrix with integral coefficients. In the language of polynomials, the first part would be the content and the second one, the principal part.

Theorem 4. *Assume that $B = \{\gamma_j\}_{j=1}^n$ is an integral basis of L. Let D be the Hermite normal form of the matrix $M(H,L)$ and call $D^{-1} = (d_{ij})_{i,j=1}^n$. Then, the elements*

$$v_i = \sum_{l=1}^{n} d_{li} w_l$$

form an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$. Moreover, a given element $\beta = \sum_{j=1}^n \beta_j \gamma_j$ is a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module if and only if the matrix

$$M_\beta(H,L) = \sum_{j=1}^{n} \beta_j M_j(H,L) D^{-1}$$

is unimodular.

4. An example of application

We apply Theorem 4 to study the example of the extension $L/\mathbb{Q}$ with $L = \mathbb{Q}(\omega)$, where $\omega = \sqrt[3]{2}$. Let c and s be the $\mathbb{Q}$-endomorphisms of L defined by the relations

$$\begin{aligned} c(1) &= 1, & c(\omega) &= -\frac{1}{2}\omega, & c(\omega^2) &= -\frac{1}{2}\omega^2, \\ s(1) &= 0, & s(\omega) &= \frac{1}{2}\omega, & s(\omega^2) &= -\frac{1}{2}\omega^2. \end{aligned}$$

In the aforementioned article [3], it is shown that $L/\mathbb{Q}$ has an unique Hopf Galois structure, given by the Hopf algebra

$$H = \mathbb{Q}(c,s)/\langle 3s^2 + c^2 - \mathrm{Id}_L, (2c + \mathrm{Id}_L)s, (2c + \mathrm{Id}_L)(c - \mathrm{Id}_L)\rangle$$

together with the evaluation action on L. Taking $\{\mathrm{Id}_L, c, s\}$ as $\mathbb{Q}$-basis of H and $\{1, \omega, \omega^2\}$ as $\mathbb{Q}$-basis of L, the blocks of the matrix of the action $M(H,L)$ are

$$M_1(H,L) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad M_2(H,L) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 \end{pmatrix}, \quad M_3(H,L) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

Joining these blocks as in Definition 3 gives the matrix of the action $M(H,L)$. Its Hermite normal form and inverse are

$$D = \frac{1}{2}\begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & -1 \\ 0 & 0 & 2 \end{pmatrix}, \qquad D^{-1} = \begin{pmatrix} 1 & \frac{1}{3} & -\frac{1}{3} \\ 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & 0 & 1 \end{pmatrix}.$$

Following Theorem 4, the associated order $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

$$V = \left\{\mathrm{Id}_L, \frac{\mathrm{Id}_L + 2c}{3}, \frac{-\mathrm{Id}_L + c + 3s}{3}\right\}.$$

Let us check whether $\mathcal{O}_L$ is $\mathfrak{A}_H$-free or not. For $\beta = \beta_1 + \beta_2\omega + \beta_3\omega^2$, we have

$$M_\beta(H,L) = \begin{pmatrix} \beta_1 & \beta_1 & 0 \\ \beta_2 & 0 & 0 \\ \beta_3 & 0 & -\beta_3 \end{pmatrix},$$

whose determinant is $\beta_1\beta_2\beta_3$. Then, taking $\beta = 1 + \omega + \omega^2 \in \mathcal{O}_L$, the determinant is 1, and then $M_\beta(H,L)$ is unimodular. Thus, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free of rank one and β is a generator. Consequently, $\mathcal{O}_L$ has a normal integral basis:

$$\left\{\mathrm{Id}_L(\beta), \frac{\mathrm{Id}_L + 2c}{3}(\beta), \frac{-\mathrm{Id}_L + c + 3s}{3}(\beta)\right\}.$$

References

[1] Adkins, W. A. and Weintraub, S. H. *Algebra: An Approach Via Module Theory*. Graduate Texts in Mathematics. Springer, 1992.

[2] Gil-Muñoz, D. and Rio, A. "On Induced Hopf Galois Structures and their Local Hopf Galois Modules". In: *arXiv e-prints* (2019). arXiv: 1910.06083 [math.NT].

[3] Greither, C. and Pareigis, B. "Hopf Galois theory for Separable Field Extensions". In: *Journal of algebra* 106 (1987), pp. 239–258.

[4] Underwood, R. G. *Fundamentals of Hopf Algebras*. 1st ed. Universitext. Springer International Publishing, 2015. isbn: 978-3-319-18990-1, 978-3-319-18991-8.