Hopf-Galois module structure of monogenic cubic number fields

Daniel Gil Muñoz

University of Barcelona

Atlanta, May 2026

Table of contents

Table of contents

Let L be a number field and suppose that $L/\mathbb{Q}$ is H-Galois.

The associated order of $\mathcal{O}_L$ in H is defined as

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

Problem

Find a necessary and sufficient condition for $\mathcal{O}_L$ being $\mathfrak{A}_H$-free.

If $L/\mathbb{Q}$ is Galois and H is the classical Galois structure, then Leopoldt's theorem provides a neat sufficient condition.

Theorem (Leopoldt, 1959)

Let L be an abelian number field. Then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.

Fact

Leopoldt's theorem does not hold for non-classical structures.

The problem for non-classical structures was first tackled by Truman, using techniques related with the theory of idèles.

Theorem (Truman, 2012)

Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ be a tamely ramified biquadratic number field. Let H be the Hopf-Galois structure on $L/\mathbb{Q}$ constructed from $\mathbb{Q}(\sqrt{m})$. Call $d = \gcd(m, n)$.

The ring $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if at least one of the equations $x^2 + my^2 = \pm 4d$ has some solution $(x, y) \in \mathbb{Z}^2$.

Later, Rio and the author provided a computational approach.

Reference

G., Rio (2022):

- Method to study the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$.
- Characterization of freeness at all Hopf-Galois structures on quartic Galois number fields.

In almost all the non-classical cases, the freeness is characterized by the solvability of a generalized Pell equation.

Aim of the talk

Problem

Let L be a cubic number field and let H be its Hopf-Galois structure. Find a necessary and sufficient condition for $\mathcal{O}_L$ being $\mathfrak{A}_H$-free.

To be honest: I only reached a complete solution when $\mathcal{O}_L = \mathbb{Z}[\alpha]$ for some root α of a parametric polynomial.

To not restrict the cubic number fields L for which the solution applies, we can consider the problem for $\mathbb{Z}$-orders in L, not just $\mathcal{O}_L$.

Table of contents

Let L be an H-Galois number field and let $\mathcal{O}$ be a $\mathbb{Z}$-order of L.

Definition

The associated order of $\mathcal{O}$ in H is defined as

$$\mathfrak{A}_H(\mathcal{O}) = \{h \in H \mid h \cdot \mathcal{O} \subset \mathcal{O}\}.$$

As in the case $\mathcal{O} = \mathcal{O}_L$, $\mathfrak{A}_H(\mathcal{O})$ is the only $\mathbb{Z}$-order of H over which $\mathcal{O}$ can be possibly free.

Problem

Let L be a cubic number field and let H be its Hopf-Galois structure. Let $\mathcal{O}$ be a $\mathbb{Z}$-order in L. Find a necessary and sufficient condition for $\mathcal{O}$ being $\mathfrak{A}_H(\mathcal{O})$-free.

The method to study the freeness over the associated order remains valid for this case.

Call $n = [L : \mathbb{Q}]$. Let $W = \{w_i\}_{i=1}^n$ be a $\mathbb{Q}$-basis of H and let $B = \{\gamma_j\}_{j=1}^n$ be a $\mathbb{Z}$-basis of $\mathcal{O}$.

$$w_i \cdot \gamma_j = \sum_{k=1}^{n} m_{ij}^{(k)}(H, L)\gamma_k, \qquad m_{ij}^{(k)}(H, L) \in \mathbb{Q}.$$

$$M_j(H, L) = (m_{ij}^{(k)}(H, L))_{k,i=1}^n \in \mathcal{M}_n(\mathbb{Q}).$$

Definition

The matrix of the action is

$$M(H, L) = \left(\begin{array}{c} M_1(H, L) \\ \hline \vdots \\ \hline M_n(H, L) \end{array}\right) \in \mathcal{M}_{n^2 \times n}(\mathbb{Q}).$$

It is the matrix of the linear map $\rho\colon H \longrightarrow \mathrm{End}_K(L)$, $\rho(h)(x) = h \cdot x$.

Proposition

There is some unimodular matrix $U \in GL_{n^2}(\mathbb{Z})$ and an invertible matrix $D \in \mathcal{M}_n(\mathbb{Q})$ such that

$$UM(H, L) = \begin{pmatrix} D \\ \hline O \end{pmatrix}.$$

Any such a matrix D is called a **reduced matrix**.

Theorem

- Let D be a reduced matrix. The vectors whose coordinates with respect to W are the columns of D^{-1} form a $\mathbb{Z}$-basis of $\mathfrak{A}_H(\mathcal{O})$.
- The absolute value of $\det(D)$ does not depend on the reduced matrix D. It is denoted by $I_W(\mathcal{O})$.

Let $\beta = \sum_{j=1}^{n} \beta_j \gamma_j \in \mathcal{O}$, where $\beta_j \in \mathbb{Z}$.

Definition

The matrix associated to β is defined as

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

Theorem

An element $\beta \in \mathcal{O}$ is an $\mathfrak{A}_H(\mathcal{O})$-free generator of $\mathcal{O}$ if and only if

$$|\det(M_\beta(H, L))| = I_W(\mathcal{O}).$$

Equivalently, $\det(M_\beta(H, L)) = \pm\det(D)$ for some (any) reduced matrix D.

Table of contents

Let L be a cubic number field. Then $L = \mathbb{Q}(\alpha)$, α root of

$$f(x) = x^3 - ax + b,$$

where $a, b \in \mathbb{Z}$ are such that $v_p(a) \leq 2$ or $v_p(b) \leq 3$ for all prime number p.

We shall consider the $\mathbb{Z}$-order $\mathcal{O} = \mathbb{Z}[\alpha]$.

Main results

- Characterization (in terms of a and b) of the $\mathfrak{A}_H(\mathbb{Z}[\alpha])$-freeness of $\mathbb{Z}[\alpha]$.
- Explicit specialization of these criteria to the case $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

We shall make use of the method above.

- A $\mathbb{Q}$-basis of H.

Let $G = \mathrm{Gal}(L/\mathbb{Q})$. We know $G \cong C_3$ or D_3, depending on whether the discriminant of f

$$\Delta := 4a^3 - 27b^2$$

is a square or not. Call $z := \sqrt{\Delta}$.

Proposition

Let $\sigma \in G$ be a 3-cycle. Then the elements

$$w_1 = \mathrm{Id}, \quad w_2 = z(\sigma - \sigma^2), \quad w_3 = \sigma + \sigma^2$$

form a $\mathbb{Q}$-basis W of H.

- A $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$.

Trivially, $B = \{1, \alpha, \alpha^2\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$.

Proposition

The action of W on B is given by the following table.

	1	α	α^2
w_1	1	α	α^2
w_2	0	$6a\alpha^2 + 9b\alpha - 4a^2$	$-9b\alpha^2 - 2a^2\alpha + 6ab$
w_3	2	$-\alpha$	$-\alpha^2 + 2a$

Proof:

Let $\alpha_1 = \alpha$, α_2, α_3 be the roots of f.

- The action of w_3:

$$w_3 \cdot \alpha = \alpha_2 + \alpha_3 = -\alpha,$$

$$w_3 \cdot \alpha^2 = \alpha_2^2 + \alpha_3^2 = -\alpha^2 + \Big(\sum_{i=1}^{3} \alpha_i\Big)^2 - 2\Big(\sum_{1 \le i < j \le 3} \alpha_i \alpha_j\Big) = -\alpha^2 + 2a.$$

- The action of w_2:

$$f(x) = x^3 - ax + b = (x - \alpha)(x^2 + \alpha x + \alpha^2 - a).$$

$\rightsquigarrow \alpha_2 = \frac{-\alpha+\sqrt{d}}{2}$ and $\alpha_3 = \frac{-\alpha-\sqrt{d}}{2}$, where $d := -3\alpha^2 + 4a$.

We calculate

$$\sqrt{d} = \frac{1}{z}(6a\alpha^2 + 9b\alpha - 4a^2).$$

Then,

$$w_2 \cdot \alpha = z(\alpha_2 - \alpha_3) = z\sqrt{d} = 6a\alpha^2 + 9b\alpha - 4a^2,$$

$$w_3 \cdot \alpha^2 = z(\alpha_2^2 - \alpha_3^2) = z(\alpha_2 - \alpha_3)(\alpha_2 + \alpha_3) = -\alpha(6a\alpha^2 + 9b\alpha - 4a^2).$$

We obtain the matrix of the action

$$M(H,L)=\begin{pmatrix}1 & 0 & 2\\ 0 & 0 & 0\\ 0 & 0 & 0\\ 0 & -4a^2 & 0\\ 1 & 9b & -1\\ 0 & 6a & 0\\ 0 & 6ab & 2a\\ 0 & -2a^2 & 0\\ 1 & -9b & -1\end{pmatrix}.$$

We find a reduced matrix so as to study the structure of $\mathbb{Z}[\alpha]$ as an $\mathfrak{A}_H(\mathbb{Z}[\alpha])$-module.

After some elementary operations, we get

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 2a^2 & 0 \\ 0 & 6a & 0 \\ 0 & 9b & -3 \\ 0 & 0 & 2a \\ 0 & 0 & 6 \end{pmatrix}.$$

Call $g_1 = \gcd(2a^2, 6a)$, $g_2 = \gcd(2a, 6)$.

$$g_1 = \begin{cases} 2a & \text{if } 3 \nmid a, \\ 6a & \text{if } 3 \mid a, \end{cases} \qquad g_2 = \begin{cases} 2 & \text{if } 3 \nmid a, \\ 6 & \text{if } 3 \mid a \end{cases}.$$

If $3 \nmid a$, we get

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2a & 0 \\ 0 & 9b & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Otherwise, we obtain

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 6a & 0 \\ 0 & 9b & 3 \\ 0 & 0 & 6 \end{pmatrix}.$$

When we apply Euclid's algorithm for the second column, what happens in the third column?

Let $x, y \in \mathbb{Z}$ with $y \neq 0$, $\lambda, \gamma \in \mathbb{Z}$ and

$$A = \begin{pmatrix} x & \lambda \\ y & \gamma \end{pmatrix}.$$

We apply Euclid's algorithm on x and y.

$$\begin{cases} r_{-1} := x,\ r_0 := y, \\ r_i = a_{i+1} r_{i+1} + r_{i+2} \text{ for } -1 \leq i \leq n-1, \\ r_n = \gcd(x, y),\ r_{n+1} = 0. \end{cases}$$

Define recursively sequences $\{\mu_i\}_i$ and $\{\nu_i\}_i$ by

$$\begin{cases} \mu_0 = 0,\ \mu_1 = 1, \\ \mu_i = -a_{i-1}\mu_{i-1} + \mu_{i-2},\ i \geq 2 \end{cases} \qquad \begin{cases} \nu_0 = 1,\ \nu_1 = -a_0, \\ \nu_i = -a_{i-1}\nu_{i-1} + \nu_{i-2},\ i \geq 2 \end{cases}$$

If we apply Euclid's algorithm on the first column of the matrix

$$A = \begin{pmatrix} x & \lambda \\ y & \gamma \end{pmatrix},$$

at the i-th step we have (up to reordering of rows)

$$\begin{pmatrix} r_{i-1} & \mu_{i-1}\lambda + \nu_{i-1}\gamma \\ r_i & \mu_i\lambda + \nu_i\gamma \end{pmatrix}.$$

Corollary

The Hermite normal form of A is (essentially)

$$\begin{pmatrix} r_n & \mu_n\lambda + \nu_n\gamma \\ 0 & \mu_{n+1}\lambda + \nu_{n+1}\gamma \end{pmatrix}.$$

Back to our case (for a moment)

If $3 \nmid a$, calling $h := \gcd(2a, 9b)$,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2a & 0 \\ 0 & 9b & 1 \\ 0 & 0 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & h & \mu_n \\ 0 & 0 & \mu_{n+1} \\ 0 & 0 & 2 \end{pmatrix}.$$

If $3 \mid a$, calling $h := \gcd(6a, 9b)$,

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 6a & 0 \\ 0 & 9b & 3 \\ 0 & 0 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 2 \\ 0 & h & 3\mu_n \\ 0 & 0 & 3\mu_{n+1} \\ 0 & 0 & 6 \end{pmatrix}.$$

We need the parity of μ_n and μ_{n+1}.

Consider the continued fraction expansion

$$\frac{x}{y} = [a_0; a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}},$$

and, for $1 \leq i \leq n$, let $\frac{p_i}{q_i} = [a_0; a_1, \ldots, a_i]$ be the i-th convergent.

Proposition

Given $1 \leq i \leq n+1$, we have:

- $\mu_i = (-1)^{i-1} q_{i-1}$.
- $\nu_i = (-1)^i p_{i-1}$.

How to sum up a long story

This way we determine a reduced matrix in all cases.

Recall that in order to study the freeness we need the value of the index $I_W(\mathbb{Z}[\alpha])$.

Proposition

Let $g = \gcd(a, b)$. Then

$$I_W(\mathbb{Z}[\alpha]) = \begin{cases} 2g & \text{if } v_3(a) = 0, \\ 18g & \text{if } 1 \leq v_3(a) \leq v_3(b), \\ 54g & \text{if } v_3(a) > v_3(b). \end{cases}$$

We can move to the next stage of the method.

Let $\beta = \sum_{j=1}^{3} \beta_j \alpha^{j-1} \in \mathbb{Z}[\alpha]$ and call $D_\beta(H, L) := \det(M_\beta(H, L))$.

$$D_\beta(H, L) = 2(3\beta_1 + 2a\beta_3)(3a\beta_2^2 - 9b\beta_2\beta_3 + a^2\beta_3^2).$$

We compare this with the already calculated index $I_W(\mathbb{Z}[\alpha])$.

If $3 \mid a$, we get $D_\beta(H, L) = \pm 2g$, which is equivalent to

$$\begin{cases} 3\beta_1 + 2a\beta_3 = r, \\ 3\frac{a}{g}\beta_2^2 - 9\frac{b}{g}\beta_2\beta_3 + \frac{a^2}{g}\beta_3^2 = s. \end{cases}$$

with $r, s \in \{-1, 1\}$.

Treating the second one as a second degree equation on β_2, it has discriminant

$$\delta = \frac{-3\Delta\beta_3^2 + 12ags}{g^2}.$$

This is a perfect square if and only if the equation $x^2 + 3\Delta y^2 = 12ags$ has some solution on $\mathbb{Z}^2$.

Main theorem

Let L be a cubic number field, and let α be such that $L = \mathbb{Q}(\alpha)$ and with minimal polynomial $f(x) = x^3 - ax + b$, where $a, b \in \mathbb{Z}$ and $v_p(a) \leq 2$ or $v_p(b) \leq 3$ for all prime p.

The $\mathbb{Z}$-order $\mathbb{Z}[\alpha]$ of L is $\mathfrak{A}_H(\mathbb{Z}[\alpha])$-free if and only if there exist integers $x, y \in \mathbb{Z}$ such that:

- $x^2 + 3\Delta y^2 = \pm 12ag$, $6a \mid 9by \pm x$ and $3 \nmid y$, if $v_3(a) = 0$.
- $x^2 + 3\Delta y^2 = \pm 36ag$ and $6a \mid 9by \pm x$, if $1 \leq v_3(a) \leq v_3(b)$.
- $x^2 + 3\Delta y^2 = \pm 108ag$ and $6a \mid 9by \pm x$, if $v_3(a) > v_3(b)$.

As in the case of Galois quartic fields, the freeness is characterized with the solvability of certain generalized Pell equations.

When does $\mathcal{O}_L = \mathbb{Z}[\alpha]$?

Equivalently: When is $\{1, \alpha, \alpha^2\}$ an integral basis of L?

Reference

Alaca (1998): Determination of an integral basis for a cubic field through a p-integral basis for each prime number p.

Definition

Let L be a degree n number field.

- An element $x \in L$ is said to be **p-integral** if $v_{\mathfrak{p}}(x) \geq 0$ for all $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_L)$ over p.
- A **p-integral basis** of L is a $\mathbb{Q}$-basis $B = \{\omega_j\}_{j=1}^n$ of L such
  - ω_j is p-integral for all j.
  - For each $x \in L$ p-integral, $\exists! x_j \in \mathbb{Q}$ p-integral such that $x = \sum_{j=1}^n x_j \omega_j$.

- The form of a p-integral basis for a cubic field is found for each prime number p (if $p > 3$, it has a uniform shape in terms of p).
- Using the Chinese Reminder Theorem, one can construct an integral basis for a collection of p-integral bases for p running through the prime numbers.
- In particular, $\{1, \alpha, \alpha^2\}$ is an integral basis if and only if it is a p-integral basis for each p.

Proposition

The equality $\mathcal{O}_L = \mathbb{Z}[\alpha]$ holds if and only if exactly one condition at each block holds.

$p = 2$

- $b \equiv 1 \pmod 2$,
- $a \equiv 0 \pmod 2$ and $b \equiv 2 \pmod 4$,
- $a \equiv 3 \pmod 4$ and $b \equiv 0 \pmod 4$,
- $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$.

$p > 3$

- $v_p(a) = 0$ and $v_p(b) \geq 1$,
- $v_p(a) \geq 1$ and $v_p(b) \leq 1$,
- $v_p(a) = v_p(b) = 0$ and $v_p(\Delta) \leq 1$.

$p = 3$

- $v_3(a) = 0$,
- $v_3(a) \geq 1$ and $v_3(b) = 1$,
- $v_3(a) \geq 1$, $a \not\equiv 3 \pmod 9$, $v_3(b) = 0$ and $b^2 \not\equiv a + 1 \pmod 9$,
- $a \equiv 3 \pmod 9$, $v_3(b) = 0$ and $b^2 \not\equiv 4 \pmod 9$.

Corollary

Let L be a cubic number field, and let α be such that $L = \mathbb{Q}(\alpha)$ and with minimal polynomial $f(x) = x^3 - ax + b$, where $a, b \in \mathbb{Z}$ and $v_p(a) \leq 2$ or $v_p(b) \leq 3$ for all prime p.

Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if there exist integers $x, y \in \mathbb{Z}$ such that:

- $x^2 + 3\Delta y^2 = \pm 12ag$, $6a \mid 9by \pm x$ and $3 \nmid y$, if $v_3(a) = 0$ and the conditions for $p = 2$ and $p > 3$ hold.
- $x^2 + 3\Delta y^2 = \pm 36ag$ and $6a \mid 9by \pm x$, if $v_3(a) = v_3(b) = 1$ and the conditions for $p = 2$ and $p > 3$ hold.
- $x^2 + 3\Delta y^2 = \pm 108ag$ and $6a \mid 9by \pm x$, if $v_3(a) > v_3(b)$ and the conditions for each prime p hold.

Table of contents

- The role of the **monogenity** of the cubic field is that it provides a simple integral basis to work with, but the conditions obtained do not rely on monogenity. In other words, *freeness is not linked with monogenity*.
- Instead, we know that freeness is closely tied with **ramification of primes**. The method we use allows to bypass the ramification to study the freeness, but in exchange, very explicit information of the field is required.
- One can use this approach to study arbitrary cubic number fields. Following Alaca's work, we can express any integral basis of L with respect to $\{1, \alpha, \alpha^2\}$, and change the basis to find the matrix of the action $M(H, L)$. The situation is much trickier, with many more parameters *(work in progress)*.

Bibliography

- S. Alaca; *p-integral bases of a cubic field*, Proceedings of the AMS 7, 146 (1998), p. 1949-1953.
- D. Gil-Muñoz; *Hopf-Galois module structure of monogenic orders in cubic number fields*, Preprint (2025).
- P. Truman; *Hopf-Galois module structure of tame biquadratic extensions*, Journal de Theorie de Nombres de Bordeaux 28, 2 (2016), p. 557-582.