# $\mathbb{Z}$-basis for the orders generated by the conjugates of algebraic integers

Stéphane R. LOUBOUTIN
Aix Marseille Université, CNRS, Centrale Marseille, I2M,
Marseille, FRANCE
stephane.louboutin@univ-amu.fr

June 26, 2018

## Contents

# 1 Abstract

Let

$$D_\alpha := \prod_{1\leq i<j\leq n} (\alpha_j - \alpha_i)^2 \in \mathbb{Z} \setminus \{0\}$$

be the discriminant of the minimal polynomial

$$\Pi_\alpha(X) = X^n - a_{n-1}X^{n-1} + \cdots + (-1)^n a_0 \in \mathbb{Z}[X]$$

of an algebraic integer $\alpha$ of degree $n$, where $\alpha_1, \cdots, \alpha_n$ are the $n$ distinct complex roots of $\Pi_\alpha(X)$.
We consider

$$\mathbb{M}_\alpha = \mathbb{Z}[\alpha_1, \cdots, \alpha_n],$$

and order of

$$\mathbb{L}_\alpha = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$$

be the normal closure of $\mathbb{Q}(\alpha)$.
It is a free $\mathbb{Z}$-module of rank

$$r = (\mathbb{L}_\alpha : \mathbb{Q}) \geq (\mathbb{Q}(\alpha) : \mathbb{Q}) = n.$$

If $\mathbb{M}$ is an order of a number field, let $D_\mathbb{M} \in \mathbb{Z}$ denote its discriminant. Notice that $D_{\mathbb{Z}[\alpha]} = D_\alpha$.

The goal is to determine a $\mathbb{Z}$-basis and the discriminant $D_{\mathbb{M}_\alpha}$ of $\mathbb{M}_\alpha$ and to give various applications of these determinations.

Let us explain how one usually constructs parametrized families of number fields of known discriminants and regulators. One usually starts from explicit parametrized families of monic polynomials with integral coefficients and constant coefficient equal to $\pm 1$, so that their complex roots are algebraic units.

Let us for example consider the simplest cubic fields $\mathbb{Q}(\alpha)$, where $\Pi_\alpha(X) = X^3 - aX^2 + (a-3)X + 1$, $a \geq 2$. Since $D_\alpha = (a^2 - 3a + 9)^2$ is a square, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois cyclic cubic extension and since $\Pi_\alpha(X) = (X - \alpha)$ $(X - (-\alpha^2 + (a-1)\alpha + 2))(X - (\alpha^2 - a\alpha + a - 2))$, the order $\mathbb{Z}[\alpha]$ is Galois invariant. Moreover, the three conjugates $\alpha$, $\alpha'$ and $\alpha''$ of $\alpha$ are algebraic units. Since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is of prime degree, any 2 of these conjugates are multiplicatively independent in the group of units $\mathbb{Z}[\alpha]^\times$ of the order $\mathbb{Z}[\alpha]$. In fact, for the simplest cubic fields we have $\mathbb{Z}[\alpha]^\times = \langle -1, \alpha, \alpha' \rangle$. Hence, in the cases that $\mathbb{Z}[\alpha]$ is equal to the ring of algebraic integers $\mathbb{Z}_\mathbb{K}$ of the number field $\mathbb{K}$, we end up with cyclic cubic fields of known discriminants and regulators. Now, since $D_\alpha = (\mathbb{Z}_\mathbb{K} : \mathbb{Z}[\alpha])^2 d_\mathbb{K}$ and $d_\mathbb{K} > 1$, it follows that if $a^2 - 3a + 9 = p$ is prime then $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[\alpha]$. Since the class number of $\mathbb{K}$ divides the class number $h_p^+$ of the real cyclotomic field $\mathbb{Q}(\zeta_p)^+$, we easily end up with with examples of prime numbers $p > 3$ for which $h_p^+ > 1$ (see [CW]).

However, still assuming that $\alpha$ is an algebraic unit such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ Galois cyclic of prime degree $p \geq 3$,

whereas the order $\mathbb{Z}[\alpha]$ is not generally Galois invariant, the order $\mathbb{M}_\alpha$ is always Galois invariant. Hence it would be much more satisfactory to have families of parametrized polynomials for which $D_{\mathbb{M}_\alpha}$ would be known and for which any $p-1$ of the $p$ conjugates of $\alpha$ would form a system of fundamental units of the order $\mathbb{M}_\alpha$. In this respect we proved:

**Theorem 1** *(See [LL14, Theorem 1.2]). Let $\varepsilon$, $\varepsilon'$ and $\varepsilon''$ be the three real roots of any one of the following parametrized families of $\mathbb{Q}$-irreducible cubic polynomials of discriminants a square:*

$$\Phi_n(X) = X^3 - n(n^2+n+3)(n^2+2)X^2 - (n^3+2n^2+3n+3)X - 1 \quad n \in \mathbb{Z},$$

$$\Xi_n(X) = X^3 - (n^3-2n^2+3n-3)X^2 - n^2X - 1 \quad 1,\ 2 \neq n \in \mathbb{Z},$$

$$\Psi_n(X) = X^3 + (n^8+2n^6-3n^5+3n^4-4n^3+5n^2-3n+3)X^2 - (n^3-2)n^2X - 1 \quad n \in \mathbb{Z}.$$

*Then, $\{1, \varepsilon, \varepsilon^2\varepsilon'\}$ is a $\mathbb{Z}$-basis of the totally real cubic order $\mathbb{Z}[\varepsilon, \varepsilon']$ and $\{\varepsilon, \varepsilon'\}$ is a system of fundamental units of this cubic order $\mathbb{Z}[\varepsilon, \varepsilon']$.*

Indeed, in these three cases $3ac - b^2$ divides $D_\alpha$ and $3b - a^2$. Hence the results on the $\mathbb{Z}$-basis follow from Theorem 7.

## 2 A $\mathbb{Z}$-generating system of $\mathbb{M}_\alpha$

**Proposition 2** *(See [Lou16b]). The set*

$$\Omega_\alpha := \{\alpha_1^{e_1} \cdots e_n^{e_n};\ 0 \leq e_k \leq n-k\}$$

*is a $\mathbb{Z}$-generating system (with $n!$ elements) of $\mathbb{M}_\alpha$.*

**Proof.** Let us prove Proposition 2 for $n = 3$.
We must show that

$$\Omega_\alpha = \{1, \alpha, \alpha^2, \alpha', \alpha\alpha', \alpha^2\alpha'\}$$

is a $\mathbb{Z}$-generating system of the order $\mathbb{M}_\alpha = \mathbb{Z}[\alpha, \alpha', \alpha'']$, where $\alpha$, $\alpha'$ and $\alpha''$ are the complex roots of the minimal polynomial $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$.
Since $a = \alpha + \alpha' + \alpha'' \in \mathbb{Z}$, we have

$$\mathbb{M}_\alpha = \mathbb{Z}[\alpha, \alpha'].$$

Now, $\alpha'$ being a root of

$$\frac{\Pi_\alpha(X)}{X - \alpha} = X^2 - (a - \alpha)X + (\alpha^2 - a\alpha + b) \in \mathbb{Z}[\alpha][X],$$

it is integral over $\mathbb{Z}[\alpha]$ and we have

$$\mathbb{M}_\alpha = \mathbb{Z}[\alpha, \alpha'] = \mathbb{Z}[\alpha][\alpha'] = \mathbb{Z}[\alpha] + \alpha'\mathbb{Z}[\alpha].$$

Since

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2,$$

the desired result follows. •

## 3 A $\mathbb{Z}$-basis of $\mathbb{M}_\alpha$ in the worst case

**Theorem 3** *(See [Lou16b]). Assume that* $\mathrm{Gal}(\mathbb{L}_\alpha/\mathbb{Q})$ *is isomorphic to the symmetric group* $\mathfrak{S}_n$*. Then* $\mathbb{M}_\alpha$ *is a free* $\mathbb{Z}$*-module of rank* $n!$*,*

$$\Omega_\alpha := \{\alpha_1^{e_1} \cdots \alpha_n^{e_n};\ 0 \leq e_k \leq n-k\}$$

*is a* $\mathbb{Z}$*-basis of* $\mathbb{M}_\alpha$ *and the discriminant of* $\mathbb{M}_\alpha$ *is*

$$D_{\mathbb{M}_\alpha} = D_\alpha^{n!/2}.$$

Now, of particular interest is the case where $\mathbb{Q}(\alpha)$ is a normal number field. In that case $\mathbb{M}_\alpha$ is a Galois invariant order of $\mathbb{Q}(\alpha)$ and $r = n$. The matrix $M_\alpha$ of the coordinates of the $n!$ elements of $\Omega_\alpha$ in the canonical $\mathbb{Q}$-basis $\mathcal{B}_\alpha = \{1, \alpha, \cdots, \alpha^{n-1}\}$ of $\mathbb{Q}(\alpha)$ is in $M_{n,n!}(\mathbb{Q})$. Consequently, it is rather easy to develop and algorithm for constructing a $\mathbb{Z}$-basis of $\mathbb{M}_\alpha$ and to compute $D_{\mathbb{M}_\alpha}$. However, from a theorytical point of view, in the Galois case, we present the only cases where a $\mathbb{Z}$-basis of $\mathbb{M}_\alpha$ has been obtained: the quadratic and cubic cases.

## 4 Remark on the $\mathbb{Z}$-basis of $\mathbb{M}_\alpha$

**Lemma 4** *Let $\{\omega_1, \cdots, \omega_r\}$ be a $\mathbb{Z}$-basis of a free $\mathbb{Z}$-module $\mathbb{M}$ of rank $r \geq 1$. There exists a $\mathbb{Z}$-basis of $\mathbb{M}$ containing a given $\omega = a_1\omega_1 + \cdots + a_r\omega_r \in \mathbb{M}$ if and only if $\gcd(a_1, \cdots, a_r) = 1$.*
*Consequently, if $1 \in \mathbb{M}$ and $\mathbb{M} \cap \mathbb{Q} = \mathbb{Z}$, e.g. if $\mathbb{M}$ is an order of a number field of degree $r$, then there exists a $\mathbb{Z}$-basis of $\mathbb{M}$ of the form $\{1, \omega_2, \cdots, \omega_r\}$.*

**Proof.** Clearly, the condition is necessary.
Conversely, assume that $\gcd(a_1, \cdots, a_r) = 1$.
Let $u_1, \cdots, u_r \in \mathbb{Z}$ be such that $a_1u_1 + \cdots + a_ru_r = 1$ (Bézout).
Define a $\mathbb{Z}$-linear map $\phi : \mathbb{M} \longrightarrow \mathbb{Z}$ by

$$x = x_1\omega_1 + \cdots + x_r\omega_r \in \mathbb{M} \mapsto \phi(x) = u_1x_1 + \cdots + u_rx_r \in \mathbb{Z}.$$

Since $x = \phi(x)\omega + (x - \phi(x)\omega)$ for $x \in \mathbb{M}$, we have $\mathbb{M} = \mathbb{Z}\omega \oplus \ker\phi$.
Hence, there exist $\omega_2', \cdots, \omega_r' \in \mathbb{M}$ such that $\{\omega, \omega_2', \cdots, \omega_r'\}$ is a $\mathbb{Z}$-basis of $\mathbb{M}$. •

**Proposition 5** *There exists a $\mathbb{Z}$-basis of $\mathbb{M}_\alpha$ of the form $\{1, \alpha, \omega_3, \cdots, \omega_r\}$.*

## 5 A $\mathbb{Z}$-basis of $\mathbb{M}_\alpha$ in the cyclic cubic case

**Corollary 6** *Let $\alpha$ ba a cubic algebraic integer. Assume that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, i.e. assume that $D_\alpha = D^2$ is a square. Then*

$$D_{\mathbb{M}_\alpha} = (D/(\mathbb{M}_\alpha : \mathbb{Z}[\alpha])^2$$

*and the index $(\mathbb{M}_\alpha : \mathbb{Z}[\alpha])$ is equal to the least $d \geq 1$ such that $d\mathbb{M}_\alpha \subseteq \mathbb{Z}[\alpha]$, i.e. is equal to the least common multiple of the denominators of the entries of the matrix $M_\alpha$ of the coordinates in the $\mathbb{Q}$-basis $\mathcal{B}_\alpha = \{1, \alpha, \alpha^2\}$ of any $\mathbb{Z}$-generating system of $\mathbb{M}_\alpha$.*

We may assume that $\Omega_\alpha = \{1, \alpha, \alpha^2, \alpha', \alpha\alpha', \alpha^2\alpha'\}$ with $\alpha'$ such that its coordinates in the canonical $\mathbb{Q}$-basis $\mathcal{B}_\alpha = \{1, \alpha, \alpha^2\}$ of $\mathbb{Q}(\alpha)$ are given by the fourth column of the following matrix $M_\alpha$ (see [Lou12, Proposition 10]):

$$\begin{pmatrix} 1 & 0 & 0 & \frac{a^2b+3ac-4b^2+Da}{2D} & \frac{(2a^2-6b)c}{2D} & \frac{(ab-9c-D)c}{2D} \\ 0 & 1 & 0 & \frac{-2a^3+7ab-9c-D}{2D} & \frac{-a^2b+3ac+2b^2+aD}{2D} & \frac{2a^2c-ab^2+3bc+bD}{2D} \\ 0 & 0 & 1 & \frac{2a^2-6b}{2D} & \frac{ab-9c-D}{2D} & \frac{-6ac+2b^2}{2D} \end{pmatrix}$$

Letting $n_{i,j}$ denote the numerator of the coefficient $(i, j)$ of $M_\alpha$, we have $d := (\mathbb{M}_\alpha : \mathbb{Z}[\alpha]) = 2D/\gcd(n_{i,j})$ and

$$D_{\mathbb{M}_\alpha} = (D/d)^2 = \left(\frac{1}{2} \gcd_{4\leq j\leq 6} (n_{3,j})\right)^2,$$

$$D_{\mathbb{M}_\alpha} = \gcd\left(D_\alpha, (a^2-3b)^2, (b^2-3ac)^2\right).$$

**Theorem 7** *(See [LL16]). Assume that the* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *is Galois, i.e. assume that* $D_\alpha = D^2$ *is a square in* $\mathbb{Z}$. *Set*

$$\Delta = \gcd(D, 3b - a^2, 3ac - b^2),$$

*where* $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$.
*Let* $x, y, z \in \mathbb{Z}$ *be such that*

$$\Delta = xD + y(3b - a^2) + z(3ac - b^2).$$

*Then*

$$\{1, \alpha_1, \eta = x\alpha_1^2 + y\alpha_2 + z\alpha_2\alpha_1^2\}$$

*is a* $\mathbb{Z}$*-basis of the order* $\mathbb{M}_\alpha = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ *and*

$$D_{\mathbb{M}_\alpha} = \Delta^2 = \gcd(D_\alpha, (3b - a^2)^2, (3ac - b^2)^2).$$

**Corollary 8** *Under the assumptions of Theorem 7, the cubic order* $\mathbb{Z}[\alpha]$ *is* $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$*-invariant if and only if* $D$ *divides* $3b - a^2$ *and* $3ac - b^2$.

**Conjecture 9** *Under the assumptions of Theorem 7, if* $\mathbb{Z}[\alpha]$ *is* $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$*-invariant then* $c$ *is odd.*

If one could prove this conjecture, then using [Coh, Theorem 6.4.6] one could obtain cyclic cubic number fields with non-monogenic rings of algebraic integers.

## 6 When is the order $\mathbb{Z}[\varepsilon]$ Galois-invariant?

**Theorem 10** *Let $\varepsilon$ be an algebraic cubic unit. Assume that $\Pi_\varepsilon(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$, $c \in \{\pm 1\}$, is reduced, i.e. that $|b| \leq a$.*
*Then $\mathbb{Q}(\varepsilon)$ is Galois and the order $\mathbb{Z}[\varepsilon]$ is Galois invariant if and only if we are in one of the following cases:*

1. *$\Pi_\varepsilon(X) = X^3 - 4X^2 + 3X + 1$, $X^3 - 6X^2 + 5X - 1$ or $X^3 - 20X^2 - 9X - 1$, in which cases $d_\varepsilon = 7^2$, or $\Pi_\varepsilon(X) = X^3 - 9X^2 + 6X - 1$, in which case $d_\varepsilon = 9^2$.*
2. *$\Pi_\varepsilon(X) = X^3 - aX^2 + (a-3)X + 1$, $a \geq 2$, i.e. if $\mathbb{Q}(\varepsilon)$ is a so-called* **simplest cubic field**, *in which case $d_\varepsilon = (a^2 - 3a + 9)^2$.*

**Question 11** *Let $\alpha$ be a cubic algebraic integer for which $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. If $\mathbb{Z}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$ then the order $\mathbb{Z}[\alpha]$ is Galois invariant. This seldom happens (Theorem 10 and Table (1)).*
**Does anyone know a neccessary and sufficient condition on $\Pi_\alpha(X)$ for having $\mathbb{Z}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$?**
*In contrast, the order $\mathbb{M}_\alpha = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ is always Galois and we often have $\mathbb{Z}_{\mathbb{Q}(\alpha)} = \mathbb{M}_\alpha$ (Table (1)). It would be nice to have a necessary and sufficient condition on $\Pi_\alpha(X)$ for having $\mathbb{Z}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$.*

For a given bound $B$ we computed the number $N(B)$ of $\mathbb{Q}$-irreducible cubic polynomials $\Pi(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ with $0 \leq a, |b|, |c| \leq B$ and whose discriminants are squares in $\mathbb{Z}$. Let $\alpha$ denote any root of $\Pi(X)$ and $\alpha_1, \alpha_2, \alpha_3$ denote its three real roots. We computed the number $N(\alpha)$ of these polynomials for which $\mathbb{Z}[\alpha] = \mathbb{Z}_{\mathbb{Q}(\alpha)}$, i.e. for which $D_\alpha = D_{\mathbb{K}}$, the number $N_{inv}(\alpha)$ of these polynomials for which the order $\mathbb{Z}[\alpha]$ is Galois invariant, i.e. for which $D$ diivides $3b - a^2$ and $3ac - b^2$ (Corollary 8), and the number $N(\alpha_1, \alpha_2, \alpha_3)$ of these polynomials for which $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Z}_{\mathbb{Q}(\alpha)}$, i.e. for which $\Delta^2 = D_{\mathbb{K}}$ (Theorem 7).

| $B$ | $N(B)$ | $N(\alpha)$ | $N_{inv}(\alpha)$ | $N(\alpha_1, \alpha_2, \alpha_3)$ |
|---|---|---|---|---|
| 10 | 62 | 30 (48.4%) | 36 (58.1%) | 44 (71.0%) |
| 20 | 190 | 64 (33.7%) | 77 (40.5%) | 137 (72.1%) |
| 30 | 387 | 97 (25.1%) | 116 (30.0%) | 280 (72.4%) |
| 40 | 613 | 136 (22.2%) | 161 (26.3%) | 431 (70.3%) |
| 50 | 853 | 168 (19.7%) | 202 (23.7%) | 592 (69.4%) |
| 100 | 2506 | 351 (14.0%) | 414 (16.5%) | 1686 (67.3%) |
| 200 | 7125 | 713 (10.0%) | 840 (11.8%) | 4663 (65.4%) |
| 300 | 12762 | 1071 (8.4%) | 1261 (9.9%) | 8263 (64.7%) |
| 500 | 26349 | 1794 (6.8%) | 2117 (8.0%) | 16991 (64.5%) |
| 1000 | 69696 | 3603 (5.2%) | 4266 (6.1%) | 44005 (63.1%) |

(1)

**Conjecture 12** *Set* $\alpha = 2\cos(2\pi/11)$.
*Let* $\varepsilon$ *be an algebraic quintic unit.*
*Assume that* $\Pi_\varepsilon(X) = X^5 - aX^4 + bX^3 - cX^2 + dX - e \in \mathbb{Z}[X]$, $e \in \{\pm 1\}$, *is reduced, i.e. that* $|d| \leq a$.
*Then* $\mathbb{Q}(\varepsilon)$ *is a* **cyclic quintic number field** *and the order* $\mathbb{Z}[\varepsilon]$ *is Galois invariant if and only if we are in one of the following* 8 *cases:*

1. $\Pi_\varepsilon(X) = X^5 - 3X^4 - 3X^3 + 4X^2 + X - 1 = \Pi_{\frac{-1}{\alpha}}(X)$.
2. $\Pi_\varepsilon(X) = X^5 - 4X^4 + 2X^3 + 5X^2 - 2X - 1 = \Pi_{1+\alpha}(X)$.
3. $\Pi_\varepsilon(X) = X^5 - 6X^4 - X^3 + 10X^2 - 6X + 1 = \Pi_{\frac{1}{1-\alpha}}(X)$.
4. $\Pi_\varepsilon(X) = X^5 - 6X^4 + 10X^3 - X^2 - 6X + 1 = \Pi_{1-\alpha}(X)$.
5. $\Pi_\varepsilon(X) = X^5 - 7X^4 + 13X^3 - 5X^2 - 2X + 1 = \Pi_{\frac{\alpha}{\alpha+1}}(X)$.
6. $\Pi_\varepsilon(X) = X^5 - 8X^4 + 19X^3 - 15X^2 + X + 1 = \Pi_{\frac{\alpha-1}{\alpha}}(X)$.
7. $\Pi_\varepsilon(X) = X^5 - 10X^4 - 15X^3 - 3X^2 + 3X + 1 = \Pi_{\frac{-\alpha-1}{\alpha+2}}(X)$.
8. $\Pi_\varepsilon(X) = X^5 - 15X^4 + 35X^3 - 28X^2 + 9X - 1 = \Pi_{\frac{1}{\alpha+2}}(X)$.

*In these* 8 *cases we have* $d_\varepsilon = 11^4$ *and* $\mathbb{Z}[\varepsilon] = \mathbb{Z}_{\mathbb{Q}(\zeta_{11})^+}$.

## 7 On the orders $\mathbb{Z}[\alpha^n]$ and $\mathbb{M}_{\alpha^n}$, $n \geq 1$

We would like to understand the behaviors of

$$D_{\alpha^k} \text{ and } \mathbb{Z}[\alpha^k], \text{ or of } D_{\mathbb{Z}[\alpha_1^k,\cdots,\alpha_n^k]} \text{ and } \mathbb{Z}[\alpha_1^k,\cdots,\alpha_n^k]$$

as $k \geq 1$ varies. Hence, $\mathbb{Z}[\alpha^m] \subseteq \mathbb{Z}[\alpha^n]$ and $\mathbb{M}_m \subseteq \mathbb{M}_n$ if $m$ is a multiple of $n$. Can it happen that for some $\alpha$'s we have $\mathbb{Z}[\alpha_n] = \mathbb{Z}[\alpha]$ or $\mathbb{M}_n = \mathbb{M}_1$ for infinitely many $n$'s? Or even for a positive proportion of $n$'s?

### 7.1 The case that $\alpha$ is an algebraic unit

**Theorem 13** *Let $\varepsilon$ be an algebraic* **unit**. *Assume that $\varepsilon$ is not a complex root of unity. Then $d_{\varepsilon^k}$ goes to infinity as $k$ goes to infinity.*

**Proof.** (J. Oesterlé, personal communication).
Since $\mathbb{Q}(\varepsilon)$ has only finitely many subfields, by considering subsequences if necessary, we may assume that $\mathbb{Q}(\varepsilon^k) = \mathbb{K}$ for all $k \geq 1$, where $\mathbb{K}$ is a given number field. Set $m = (\mathbb{K} : \mathbb{Q})$. Since $\varepsilon$ is not a complex root of unity, the $\varepsilon^k$'s are pairwise distinct elements of $\mathbb{Z}_{\mathbb{K}}^{\times}$. Therefore, it suffices to show that for any given $A > 0$ the set $X = \{\eta \in \mathbb{Z}_{\mathbb{K}}^{\times};\ \mathbb{Q}(\eta) = \mathbb{K} \text{ and } d_\eta \leq A\}$ is finite. Let $\overline{\mathbb{K}}$ be the normal closure of $\mathbb{K}$. Let $\sigma_i$, $1 \leq i \leq m$, be the complex embeddings of $\mathbb{K}$. Hence, $\sigma_i(\mathbb{K}) \subseteq \overline{\mathbb{K}}$. Let $S$ be the set of places of $\overline{\mathbb{K}}$ above the rational primes less than or equal to $A$. Set $Y = \{\eta \in \mathbb{Z}_{\overline{\mathbb{K}}}^{\times};\ \eta - 1 \text{ is a } S\text{-unit of } \mathbb{Z}_{\overline{\mathbb{K}}}\}$.

By Siegel's theorem, $Y$ is finite. Now, let $\eta \in X$. Then $\sigma_i(\eta) - \eta$ divides $d_\eta$ in $\mathbb{Z}_{\mathbb{K}}$. Hence, $\sigma_i(\eta) - \eta$ is a $S$-unit and so is each $\sigma_i(\eta)/\eta$. Therefore,

$$\phi : \eta \in X \longrightarrow \phi(\eta) = \left(\frac{\sigma_1(\eta)}{\eta}, \cdots, \frac{\sigma_n(\eta)}{\eta}\right) \in Y^m$$

is well defined and $\phi(\eta) = \phi(\eta')$ if and only if $\eta'/\eta$ is invariant under the action of all the $\sigma_i$'s, hence if and only if $\eta' = \pm\eta$. Therefore, $X$ is finite and $\#X \leq 2(\#Y)^m$. •

**Question 14** *Can anyone prove the same result without assuming that the algebraic integer $\alpha$ is a unit?*

### 7.2 The non-normal cubic case

For non-totally real cubic units, we proved:

**Theorem 15** *(See [Lou10, Theorem 1]). Let $\alpha$ be a real cubic algebraic unit of negative discriminant $D_\alpha < 0$. Then*

$$|D_\alpha| \geq \max(|\alpha|, |\alpha|^{-1})^{3/2}/2.$$

*Consequently, $D_{\alpha^k}$ and $D_{\mathbb{Z}[\alpha_1^k, \alpha_2^k, \alpha_3^k]}$ go exponentially to infinity as $k$ goes to infinity.*

**Proof.** Since $\mathbb{Q}(\alpha^k)/\mathbb{Q} = \mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois, the group $\mathrm{Gal}(\mathbb{Q}(\alpha_1^k, \alpha_2^k, \alpha_3^k)/\mathbb{Q})$ is isomorphic to $\mathfrak{S}_3$ and $D_{\mathbb{M}_k} = D_{\mathbb{Z}[\alpha_1^k, \alpha_2^k, \alpha_3^k]} = D_{\alpha^k}^3$ (Theorem 3). •

For totally real cubic units, we proved:

**Theorem 16** *(See [Lou12] and [Lou15, Theorem 33]). Let $\alpha_1, \alpha_2, \alpha_3$ be the 3 real conjugates of a totally real cubic algebraic* **unit** *$\alpha$. Then*

$$D_\alpha \geq \max(|\alpha_1|, |\alpha_1|^{-1}, |\alpha_2|, |\alpha_2|^{-1}, |\alpha_3|, |\alpha_3|^{-1})^{3/2}/2.$$

*Consequently, $D_{\alpha^k}$ goes exponentially to infinity as $k$ goes to infinity and if $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois, i.e. if $D_\alpha$ is not a square in $\mathbb{Z}$, then $D_{\mathbb{Z}[\alpha_1^k, \alpha_2^k, \alpha_3^k]}$ goes exponentially to infinity as $k$ goes to infinity.*

### 7.3 The cyclic cubic case

Now, let us come back to the problem considered in [Lou16b]. We did some computation to determine

$$N(X) := \#\{n \in [1, X];\ \mathbb{M}_n = \mathbb{M}_1\}$$

for various cubic algebraic integers $\alpha$ such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois (we used Theorem 7 to compute $D_{\mathbb{M}_1}$ and the $D_{\mathbb{M}_n}$'s, and we notice that since $\mathbb{M}_n \subseteq \mathbb{M}_1$, we have $\mathbb{M}_n = \mathbb{M}_1$ if an only if $D_{\mathbb{M}_n} = D_{\mathbb{M}_1}$). According to these computations, and contrary to the non-Galois cubic case, it seems reasonable to conjecture that for any such $\alpha$ there is a positive proportion of $n$'s for which $\mathbb{M}_n = \mathbb{M}_1$:

| $\Pi_\alpha(X)$ | $f_\alpha$ | $X$ | $N(X)/X$ |
|---|---|---|---|
| $X^3-3X^2-4X-1$ | 7 | $10^2$ | 0.49 |
| | | $10^3$ | 0.479 |
| | | $10^4$ | 0.4645 |
| | | $10^5$ | 0.45166 |
| $X^3-X^2-4X-1$ | 13 | $10^2$ | 0.48 |
| | | $10^3$ | 0.464 |
| | | $10^4$ | 0.4553 |
| | | $10^5$ | 0.44489 |
| $X^3-10X^2+7X+1$ | 79 | $10^2$ | 0.47 |
| | | $10^3$ | 0.467 |
| | | $10^4$ | 0.4651 |
| | | $10^5$ | 0.45369 |
| $X^3-43X^2+40X+1$ | $7\cdot 13\cdot 19$ | $10^2$ | 0.55 |
| | | $10^3$ | 0.492 |
| | | $10^4$ | 0.4817 |
| | | $10^5$ | 0.47455 |
| $X^3-31X^2-25X-1$ | $2^3\cdot 7\cdot 13$ | $10^2$ | 0.30 |
| | | $10^3$ | 0.305 |
| | | $10^4$ | 0.2968 |
| | | $10^5$ | 0.28942 |
| $X^3-54X^2+69X-1$ | $3^2\cdot 5\cdot 7\cdot 11$ | $10^2$ | 0.18 |
| | | $10^3$ | 0.161 |
| | | $10^4$ | 0.1547 |
| | | $10^5$ | 0.15172 |
| $X^3-15X^2+14X-3$ | 61 | $10^2$ | 0.64 |
| | | $10^3$ | 0.587 |
| | | $10^4$ | 0.5655 |
| | | $10^5$ | 0.55305 |
| $X^3-24X^2+23X-5$ | $13^2$ | $10^2$ | 0.65 |
| | | $10^3$ | 0.621 |
| | | $10^4$ | 0.5938 |
| | | $10^5$ | 0.58007 |
| $X^3-33X^2+32X-7$ | 331 | $10^2$ | 0.72 |
| | | $10^3$ | 0.624 |
| | | $10^4$ | 0.5974 |
| | | $10^5$ | 0.57832 |

# References

[Coh] H. Cohen. *A course in computational algebraic number theory.* Graduate Texts in Mathematics **138**. Springer-Verlag, Berlin, 1993.

[CW] G. Cornell and L. C. Washington. Class numbers of cyclotomic fields. *J. Number Theory* **21** (1985), 260–274.

[LL14] Jun Ho Lee and S. Louboutin. On the fundamental units of some cubic orders generated by units. *Acta Arith.* **165** (2014), 283–299.

[LL15] J. H. Lee and S. Louboutin. Determination of the orders generated by a cyclic cubic unit that are Galois invariant. *J. Number Theory* **148** (2015), 33–39.

[LL16] J. H. Lee and S. Louboutin. Discriminants of cyclic cubic orders. *J. Number Theory* **168** (2016), 64–71.

[Lou10] S. Louboutin. On some cubic or quartic algebraic units. *J. Number Theory* **130** (2010), 956–960.

[Lou12] S. Louboutin. On the fundamental units of a totally real cubic order generated by a unit. *Proc. Amer. Math. Soc.* **140** (2012), 429–436.

[Lou15] S. Louboutin. Fundamental units for some orders generated by a unit. *Publ. Math. Besançon Algèbre et Théorie des Nombres* 2015, 41–68. Presses Univ. Franche-Comté, Besançon.

[Lou16a] S. Louboutin. Dedekind sums, mean square value of $L$-functions at $s = 1$ and upper bounds on relative class numbers. *Bull. Pol. Acad. Sci. Math.* **64** (2016), 165–174.

[Lou16b] S. Louboutin. Discriminants of $\mathfrak{S}_n$-orders. *Int. J. Number Theory* **12** (2016), 1899–1905.

[Mur] A. Murchio. Unités fondamentales pour les ordres générés par une unité (Fundamental units for orders generated by a unit). PhD Thesis, in preparation.