ALGEBRA, LOGIC AND NUMBER THEORY
BANACH CENTER PUBLICATIONS, VOLUME 121
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2020

ON THE ORDER GENERATED BY THE CONJUGATES OF AN ALGEBRAIC INTEGER

STÉPHANE R. LOUBOUTIN

Aix Marseille Université, CNRS, Centrale Marseille, I2M
Marseille, France
ORCID: 0000-0001-9236-049X E-mail: stephane.louboutin@univ-amu.fr

Abstract. Let α be an algebraic integer of degree $n \geq 3$. Assume that the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Let $\mathbb{Z}[\mathrm{conj}(\alpha)]$ be the order of $\mathbb{Q}(\alpha)$ generated by the n complex conjugates of α. Apart from the case that $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is the symmetric group $\mathfrak{S}_n$, only for the cyclic cubic case are an explicit $\mathbb{Z}$-basis and the discriminant of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ known. Here, we prove that there always exists a $\mathbb{Z}$-basis of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ containing 1 and α. We deduce a new proof of the cyclic cubic case. We hope that this new approach could be helpful to settle the unsolved Galois quartic case. Finally, for α an algebraic integer of any degree $n \geq 2$, it is known that the discriminants of the orders $\mathbb{Z}[\alpha^k]$ go to infinity as k goes to infinity (without assuming that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois). Then, in the Galois cubic and quartic cases, we propose several conjectures related to the apparent behavior of the orders $\mathbb{Z}[\mathrm{conj}(\alpha^k)]$ as k goes to infinity. In particular, the orders $\mathbb{Z}[\mathrm{conj}(\alpha^k)]$ seem to behave completely differently from the orders $\mathbb{Z}[\alpha^k]$, as $k \geq 1$ goes to infinity.

1. Introduction. Throughout the paper, let α be an algebraic integer of degree n. Let

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

be the discriminant of its minimal polynomial

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

where $\mathrm{conj}(\alpha) = (\alpha_1, \ldots, \alpha_n)$ are the complex conjugates of α, i.e. are the n distinct complex roots of $\Pi_\alpha(X)$. We will consider the order

$$\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}[\alpha_1, \ldots, \alpha_n],$$

of the normal closure $\mathbb{Q}(\mathrm{conj}(\alpha)) = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ of $\mathbb{K} = \mathbb{Q}(\alpha)$.

2010 *Mathematics Subject Classification*: Primary 11R04; Secondary 11R16, 11R20.
Key words and phrases: discriminants, orders of number fields, cubic fields, quartic fields.
The paper is in final form and no version of it will be published elsewhere.

DOI: 10.4064/bc121-10

Let $\sigma_1, \dots, \sigma_n$, be the complex imbeddings of a number field $\mathbb{K}$ of degree n. The discriminant $D_{\mathbb{M}}$ of an order $\mathbb{M}$ of $\mathbb{K}$ is defined by

$$D_{\mathbb{M}} := D(\omega_1, \dots, \omega_n) = \Delta(\omega_1, \dots, \omega_n)^2 \in \mathbb{Z} \setminus \{0\}, \tag{1}$$

where

$$\Delta(\omega_1, \dots, \omega_n) := \det\bigl([\sigma_i(\omega_j)]_{1 \le i,j \le n}\bigr) \in \mathbb{C} \setminus \{0\} \tag{2}$$

and $\Omega = \{\omega_k \colon 1 \le k \le n\}$ is any $\mathbb{Z}$-basis of $\mathbb{M}$. It does not depend on the $\mathbb{Z}$-basis of $\mathbb{M}$ (see e.g. [Nar, Chapter II] or [Coh, Chapter 4]). If $\mathbb{K} = \mathbb{Q}(\alpha)$ and α is an algebraic integer, then $D_{\mathbb{Z}[\alpha]} = D(1, \alpha, \dots, \alpha^{n-1}) = D_\alpha$. The discriminant of the ring of algebraic integers $\mathbb{Z}_{\mathbb{K}}$ of $\mathbb{K}$, i.e. the discriminant of $\mathbb{K}$, is denoted by $D_{\mathbb{K}}$. Let $\mathbb{M}$ be an order of $\mathbb{K}$. The index $(\mathbb{Z}_{\mathbb{K}} : \mathbb{M})$ is finite and $D_{\mathbb{M}} = (\mathbb{Z}_{\mathbb{K}} : \mathbb{M})^2 D_{\mathbb{K}}$. In particular, $D_\alpha = (\mathbb{Z}_{\mathbb{K}} : \mathbb{Z}[\alpha])^2 D_{\mathbb{K}}$ if $\mathbb{K} = \mathbb{Q}(\alpha)$ and $\alpha \in \mathbb{Z}_{\mathbb{K}}$. We let $\mathbb{M}^\times$ denote the multiplicative group of units of an order $\mathbb{M}$.

Our goal is to determine a $\mathbb{Z}$-basis for the order $\mathbb{Z}[\mathrm{conj}(\alpha)]$ and its discriminant $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]}$ and to give various applications of these determinations. To date, the only cases where a $\mathbb{Z}$-basis for $\mathbb{Z}[\mathrm{conj}(\alpha)]$ has been obtained are the quadratic case (easy), the symmetric case (Theorem 8) and the cyclic cubic case (Theorem 17). The present paper which gives a new proof of Theorem 17 based on Theorem 13, might prove useful for solving the Galois quartic case. In Section 6 we raise many questions to which we have presently no answer on the behaviors of the orders $\mathbb{Z}[\alpha^k]$ and $\mathbb{Z}[\mathrm{conj}(\alpha^k)]$ as k goes to infinity.

Assume that $\mathbb{K}/\mathbb{Q} = \mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Then $\mathbb{Z}_{\mathbb{K}}$ is always Galois-invariant. Since $\mathbb{Z}[\alpha]$ is seldom Galois-invariant whereas $\mathbb{Z}[\mathrm{conj}(\alpha)]$ is always Galois-invariant, we are much more likely to have $\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[\mathrm{conj}(\alpha)]$ than to have $\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[\alpha]$. This makes the study of these $\mathbb{Z}[\mathrm{conj}(\alpha)]$ worthwhile. To measure this intuition, at least in the cyclic cubic case, we computed Table 1. Let $N_{\mathrm{cyclic}}(B)$ be the number of $\mathbb{Q}$-irreducible cubic monic polynomials $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ with $0 \le a, |b|, |c| \le B$ whose discriminants $D_\alpha = f_\alpha^2$ are squares in $\mathbb{Z}$. (By changing $\Pi(X)$ into $-\Pi(-X)$ if necessary, we can indeed assume that $a \ge 0$.) Set $\mathbb{K} = \mathbb{Q}(\alpha)$. Let $N_{\mathrm{monogenic}}(B)$ be the number of these polynomials for which $\mathbb{Z}[\alpha] = \mathbb{Z}_{\mathbb{K}}$, i.e. for which $D_\alpha = D_{\mathbb{K}}$. Let $N_{\mathrm{inv}}(B) \ge N_{\mathrm{monogenic}}(B)$ be the number of these polynomials for which $\mathbb{Z}[\alpha]$ is Galois invariant, i.e. for which $\mathbb{Z}[\alpha] = \mathbb{Z}[\mathrm{conj}(\alpha)]$, i.e. for which f_α divides $3b - a^2$ and $3ac - b^2$ (Theorem 17). Let $N_{\mathrm{conj}}(B)$ be the number of these polynomials for which $\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}_{\mathbb{K}}$, i.e. for which $\Delta_\alpha^2 = D_{\mathbb{K}}$ (Theorem 17). (The computation of the columns for $N_{\mathrm{cyclic}}(B)$ and $N_{\mathrm{inv}}(B)$ took 54370 seconds with Maple on a MacBook Air laptop computer. The computation of Table 1 on a Mac mini desk computer using the PARI/GP software for algebraic number theory computations took 37h40min.)

Question 1. *Table* 1 *raises three questions*: *is it true that*

$$\rho_{\mathrm{monogenic}}(B) = N_{\mathrm{monogenic}}(B)/N_{\mathrm{cyclic}}(B) \text{ and } \rho_{\mathrm{inv}}(B) = N_{\mathrm{inv}}(\alpha)/N_{\mathrm{cyclic}}(B)$$

tend to 0 *whereas* $\rho_{\mathrm{conj}}(B) = N_{\mathrm{conj}}(B)/N_{\mathrm{cyclic}}(B)$ *tends to a positive limit as* B *tends to infinity?*

B	$N_{\rm cyclic}(B)$	$N_{\rm monogenic}(B)$	$N_{\rm inv}(B)$	$N_{\rm conj}(B)$
10	62	30 (48.3%)	36 (58.0%)	44 (70.9%)
20	190	64 (33.6%)	77 (40.5%)	137 (72.1%)
40	613	136 (22.1%)	161 (26.2%)	431 (70.3%)
80	1762	277 (15.7%)	330 (18.7%)	1180 (66.9%)
160	5133	565 (11.0%)	667 (12.9%)	3378 (65.8%)
320	13904	1145 (8.2%)	1350 (9.7%)	9030 (64.9%)
640	37529	2283 (6.0%)	2715 (7.2%)	23903 (63.6%)
1280	97451	4616 (4.7%)	5475 (5.6%)	61412 (63.0%)

Table 1

2. Four families of parametrized number fields. To construct parametrized families of Galois number fields $\mathbb{K}_m = \mathbb{Q}(\varepsilon_m)$ of a given degree $n \geq 2$ of known discriminants and regulators, one usually starts from explicit parametrized families of $\mathbb{Q}$-irreducible monic polynomials $\Pi_m(X) \in \mathbb{Z}[X]$ of a given degree n and of constant coefficient equal to ± 1, where ε_m is any complex root of $\Pi_m(X)$. The conjugates of ε_m are algebraic units and one may hope to extract from them a system of fundamental units for the order $\mathbb{Z}[\mathrm{conj}(\varepsilon_m)]$. This is usually done by using Cusick's method developed in [Cus], as in [LL14], [LL16, Section 2], [Bal, Section 3] and [BW, Section 6]. It requires an estimation of $D_{\mathbb{Z}[\mathrm{conj}(\varepsilon_m)]}$.

Assume moreover that we are dealing with a family for which the extensions $\mathbb{K}_m/\mathbb{Q}$ are abelian and for which the discriminants $D_{\mathbb{Z}[\mathrm{conj}(\varepsilon_m)]} = f_m^{n-1}$ are known beforehand to be perfect $(n-1)$-th-powers, as in Propositions 3, 4 and 5. In that case, for the probably/conjecturally infinite occurrences for which $f_m = p$ is prime, the number field $\mathbb{K}_m$ is of conductor p, discriminant p^{n-1} and has ring of algebraic integers $\mathbb{Z}[\mathrm{conj}(\varepsilon_m)]$. Indeed, since $p^{n-1} = D_{\mathbb{Z}[\mathrm{conj}(\varepsilon_m)]} = (\mathbb{Z}_{\mathbb{K}_m} : \mathbb{Z}[\mathrm{conj}(\varepsilon_m)])^2 D_{\mathbb{K}_m}$ we infer that $D_{\mathbb{K}_m} > 1$ is a power of p, hence that p^{n-1} divides $D_{\mathbb{K}_m}$ by the conductor-discriminant formula, hence that $(\mathbb{Z}_{\mathbb{K}_m} : \mathbb{Z}[\mathrm{conj}(\varepsilon_m)]) = 1$. In that case, the class number of $\mathbb{K}_m$ divides the class number h_p^+ of the real cyclotomic field $\mathbb{Q}(\zeta_p)^+$ and we end up with examples of prime numbers $p > 3$ for which h_p^+ is large (see [CW], [SW], [Lou04] and [Lou07]).

We will repeatedly use

Lemma 2. *A primitive Dirichlet character χ of order $n > 1$ coprime with its conductor f is of square-free conductor.*

Proof. Assume that $f = d^2F$ is not square-free, where $d > 1$. Take n^* such that $nn^* \equiv 1 \pmod{f}$. Since f divides $(f/d)^k$ for $k \geq 2$, we have $x \equiv y^n \pmod{f}$ and $\chi(x) = \chi^n(y) = 1$ whenever $x = 1 + \lambda\frac{f}{d} \equiv 1 \pmod{f/d}$, where $y = 1 + \lambda n^* \frac{f}{d}$. This contradicts the primitivity of χ modulo f. ∎

Now, let us start with the nicest situation:

Proposition 3. *Let α, α' and α'' be the three complex roots of the cubic polynomial $\Pi_\alpha(X) = X^3 - mX^2 + (m-3)X + 1 \in \mathbb{Z}[X]$, $\mathbb{Q}$-irreducible and of discriminant $D_m = f_m^2$, where $f_m = m^2 - 3m + 9$. The* simplest cubic field $\mathbb{K} = \mathbb{Q}(\alpha)$ *is cyclic with* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle$, *where $\sigma(\alpha) = -\alpha^2 + (m-1)\alpha + 2$. Hence, the cubic order $\mathbb{Z}[\alpha]$*

is $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*-invariant. Moreover,* $\mathbb{Z}[\alpha]^\times = \langle -1, \alpha, \alpha'\rangle$*, i.e.* $\{\alpha, \alpha'\}$ *is a system of fundamental units for the order* $\mathbb{Z}[\alpha]$*. Finally, if* $3 \nmid m$*, then the order* $\mathbb{Z}[\alpha]$ *is equal to the ring of algebraic integers* $\mathbb{Z}_\mathbb{K}$ *of* $\mathbb{K}$ *if and only if* f_m *is square-free. This happens infinitely many often with positive probability.*

Proof. Proofs of the assertion on the unit group $\mathbb{Z}[\alpha]^\times$ can be found in [Tho, Theorem (3.10)] or [LL14, Theorem 1]. Let us prove the assertion on $\mathbb{Z}_\mathbb{K}$. Let $f_\mathbb{K}$ be the conductor of $\mathbb{K}$. Assume that $3 \nmid m$ and $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[\alpha]$. Then, $3 \nmid f_m$ and $f_\mathbb{K}^2 = D_\mathbb{K} = D_m = f_m^2$. Hence, $f_m = f_\mathbb{K}$ is square-free, by Lemma 2. Conversely, if $3 \nmid m$ and f_m is square-free, then $\mathbb{K}$ is of conductor f_m, by [Lou07, Theorem 8], hence of discriminant $D_\mathbb{K} = f_\mathbb{K}^2 = f_m^2$ (by the conductor-discriminant formula). Now, $D_\mathbb{K} = f_m^2 = D_m = (\mathbb{Z}[\alpha] : \mathbb{Z}_\mathbb{K})^2 D_\mathbb{K}$ yields $(\mathbb{Z}[\alpha] : \mathbb{Z}_\mathbb{K}) = 1$ and $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[\alpha]$. See also [Wa1, Proposition 1 and Corollary] for an alternative proof. The last assertion follows from [Ric]. ■

However, we are very unlikely to find usually ourselves in such a nice setting. Usually the order $\mathbb{Z}[\alpha]$ will not be Galois-invariant, in which case we expect more satisfactory results by working with $\mathbb{Z}[\mathrm{conj}(\alpha)]$ instead, the smallest Galois-invariant order containing $\mathbb{Z}[\alpha]$. For example, we have:

Proposition 4. *Let* α *be a root of the quartic polynomial* $\Pi_\alpha(x) = X^4 - mX^3 - 6X^2 + mX + 1 \in \mathbb{Z}[X]$*, with* $m \neq -3, 0, 3$*,* $\mathbb{Q}$*-irreducible and of discriminant* $D_m = 4f_m^3$*, where* $f_m = m^2 + 16$*. The* simplest quartic field $\mathbb{K} = \mathbb{Q}(\alpha)$ *is a totally real cyclic quartic field with* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle$*, where*

$$\sigma(\alpha) = \frac{\alpha - 1}{\alpha + 1} = \big(-\alpha^3 + (m+1)\alpha^2 - (m-5)\alpha - 3\big)/2.$$

Hence, $\mathbb{Z}[\alpha]$ *which is not* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*-invariant is never equal to* $\mathbb{Z}_\mathbb{K}$*. The* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*-invariant quartic order* $\mathbb{Z}[\mathrm{conj}(\alpha)]$ *admits* $\{1, \alpha, \alpha^2, \sigma(\alpha)\}$ *as a* $\mathbb{Z}$*-basis and is of discriminant* $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = f_m^3$*. Finally, if* m *is odd, then* $\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}_\mathbb{K}$ *if and only if* f_m *is square-free. This happens infinitely many often with positive probability.*

Proof. Since $\sigma^2(\alpha) = \alpha^3 - m\alpha^2 - 6\alpha + m$ and $\sigma^3(\alpha) = m - \alpha - \sigma(\alpha) - \sigma^2(\alpha)$, we have $\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}[\alpha, \sigma(\alpha)] = \mathbb{Z}[\alpha][\sigma(\alpha)]$. Since $\sigma(\alpha)^2 - (m-2)\sigma(\alpha) - (\alpha^2 - (m+2)\alpha + m) = 0$, we have $\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}[\alpha] + \mathbb{Z}[\alpha]\sigma(\alpha)$. Hence, $\{1, \alpha, \alpha^2, \alpha^3, \sigma(\alpha), \alpha\sigma(\alpha), \alpha^2\sigma(\alpha), \alpha^3\sigma(\alpha)\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\mathrm{conj}(\alpha)]$. Since α^3, $\alpha\sigma(\alpha)$, $\alpha^2\sigma(\alpha)$ and $\alpha^3\sigma(\alpha)$ are $\mathbb{Z}$-linear combinations of 1, α, α^2 and $\sigma(\alpha)$, the first assertion follows. Let us now prove the assertion on $\mathbb{Z}_\mathbb{K}$. Assume that m is odd and $f_m = m^2 + 16$ is square-free. Since $\alpha - 1/\alpha \in \mathbb{Z}[\alpha]$ is a root of $X^2 - mX - 4$ of discriminant f_m, the real quadratic field $\mathbb{K}_2 = \mathbb{Q}(\sqrt{f_m})$ is a subfield of conductor f_m of $\mathbb{K}$ and f_m^3 divides $D_\mathbb{K}$ (by the conductor-discriminant formula). Since $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = f_m^3 = (\mathbb{Z}_\mathbb{K} : \mathbb{Z}[\mathrm{conj}(\alpha)])^2 D_\mathbb{K}$, we have $(\mathbb{Z}_\mathbb{K} : \mathbb{Z}[\mathrm{conj}(\alpha)]) = 1$ and $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[\mathrm{conj}(\alpha)]$. (An alternative proof would be to use the fact that if f_m is square-free, then $\mathbb{K}_2$ is clearly of conductor f_m whereas $\mathbb{K}$ is also of conductor f_m by [Lou07, Theorem 14]. Hence, the conductor-discriminant formula gives $D_\mathbb{K} = f_{\mathbb{K}_2} f_\mathbb{K}^2 = f_m^3 = D_{\mathbb{Z}[\mathrm{conj}(\alpha)]}$ and $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[\mathrm{conj}(\alpha)]$.) Conversely, assume that m is odd and $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[\mathrm{conj}(\alpha)]$. Then $D_\mathbb{K} = D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = f_m^3$ is odd and $D_\mathbb{K} = f_{\mathbb{K}_2} f_\mathbb{K}^2$, by the conductor-discriminant formula, where the conductor $f_{\mathbb{K}_2}$ of the quadratic subfield of $\mathbb{K}$ divides $f_\mathbb{K}$. Hence $f_\mathbb{K}$ is odd and square-free, by Lemma 2. It follows that $f_{\mathbb{K}_2} f_\mathbb{K}^2 = f_m^3$ is divisible by no fourth power of any prime and we deduce that f_m is square-free. ■

Proposition 5. *Let α be a root of the quintic polynomial $\Pi_\alpha(x) = X^5 + m^2X^4 - 2(m^3+3m^2+5m+5)X^3 + (m^4+5m^3+11m^2+15m+5)X^2 + (m^3+4m^2+10m+10)X + 1 \in \mathbb{Z}[X]$, $\mathbb{Q}$-irreducible for $m \in \mathbb{Z}$ and of discriminant $D_m = \delta_m^2 f_m^4$, where $\delta_m = m^3+5m^2+10m+7$ and $f_m = m^4+5m^3+15m^2+25m+25$. The* simplest quintic field $\mathbb{K} = \mathbb{Q}(\alpha)$ *is cyclic with* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle$, *where*

$$\sigma(\alpha) = \frac{-\alpha^2 + m\alpha + (m+2)}{(m+2)\alpha + 1}.$$

The quintic order $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*-invariant if and only if $m = -2$ and is never equal to $\mathbb{Z}_\mathbb{K}$. The* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*-invariant quintic order $\mathbb{Z}[\mathrm{conj}(\alpha)]$ admits $\{1,\alpha,\alpha^2,\sigma^2(\alpha),\sigma^4(\alpha)\}$ as a $\mathbb{Z}$-basis, is of discriminant $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = f_m^4$ and $\mathbb{Z}[\mathrm{conj}(\alpha)]^\times = \langle -1,\alpha,\sigma(\alpha),\sigma^2(\alpha),\sigma^3(\alpha)\rangle$, i.e. $\{\sigma^k(\alpha)\colon 0 \le k \le 3\}$ is a system of fundamental units for the order $\mathbb{Z}[\mathrm{conj}(\alpha)]$. Finally, if $5 \nmid m$ then $\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}_\mathbb{K}$ if and only if f_m is square-free. Conjecturally, this happens infinitely many often with positive probability.*

Proof. Let us prove the assertions on the $\mathbb{Z}$-basis and discriminant. Since $\sigma^3(\alpha) = -m^2 - \alpha - \sigma(\alpha) - \sigma^2(\alpha) - \sigma^4(\alpha)$ and $\sigma(\alpha) + (m+2)\sigma^2(\alpha) + (m+2)\sigma^4(\alpha) \in \mathbb{Z}[\alpha]$, we have $\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}[\alpha,\sigma^2(\alpha),\sigma^4(\alpha)]$. Set $\alpha_1 = 1$, $\alpha_2 = \alpha$, $\alpha_3 = \alpha^2$, $\alpha_4 = \sigma^2(\alpha)$ and $\alpha_5 = \sigma^4(\alpha)$. It remains to check that the $\mathbb{Z}$-module $\mathbb{M} := \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_5$ is a subring of $\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}[\alpha,\sigma^2(\alpha),\sigma^4(\alpha)]$, i.e. that $\alpha_i\alpha_j \in \mathbb{M}$ for $2 \le i \le j \le 5$. For $\beta,\gamma \in \mathbb{Q}[\theta]$, we write $\beta \sim \gamma$ whenever $\beta = \gamma + P(\alpha)$ for some quadratic polynomial $P(X) \in \mathbb{Z}[X]$. Hence, $\gamma \in \mathbb{M}$ and $\beta \sim \gamma$ imply $\beta \in \mathbb{M}$. Then, using any symbolic manipulation language like Maple, one can check that

$$\begin{aligned}
\alpha_2\alpha_3 &= \alpha^3 \sim (m+1)\sigma^2(\alpha) + (2m+3)\sigma^4(\alpha),\\
\alpha_2\alpha_4 &= \alpha\sigma^2(\alpha) \sim -(m+2)\sigma^4(\alpha),\\
\alpha_2\alpha_5 &= \alpha\sigma^4(\alpha) \sim -\sigma^2(\alpha) + m\sigma^4(\alpha)
\end{aligned}$$

are in $\mathbb{M}$. Therefore, $\alpha\mathbb{M} \subseteq \mathbb{M}$ and $\alpha_i\alpha_j \in \mathbb{M}$, $2 \le i \le j \le 5$ and $2 \le i \le 3$. Moreover, for $4 \le i \le j \le 5$, one can check that

$$\begin{aligned}
\alpha_4^2 &= (\sigma^2(\alpha))^2 \sim (m+1)\sigma^2(\alpha) + (m+1)^2\sigma^4(\alpha),\\
\alpha_4\alpha_5 &= \sigma^2(\alpha)\sigma^4(\alpha) \sim (m+1)\sigma^2(\alpha) + (2m+3)\sigma^4(\alpha),\\
\alpha_5^2 &= (\sigma^4(\alpha))^2 \sim (m+2)\sigma^2(\alpha) - (m^2+m)\sigma^4(\alpha)
\end{aligned}$$

are in $\mathbb{M}$. Moreover, using $\delta_m\sigma^2(\alpha) \sim -(2m^3+4m^2+3m+2)\alpha^3 - (2m+3))\alpha^4$, $\delta_m\sigma^4(\alpha) \sim (m^3+2m^2+3m+3)\alpha^3 + (m+1)\alpha^4$ and

$$\det\begin{pmatrix} -(2m^3+4m^2+3m+2) & m^3+2m^2+3m+3 \\ -(2m+3) & m+1 \end{pmatrix} = \delta_m,$$

we obtain $D_\mathbb{M} = D_m/\delta_m^2$. Finally, if $m \neq -2$ then $(\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha]) = |\delta_m| > 1$ and not being equal to $\mathbb{Z}[\mathrm{conj}(\alpha)]$, the order $\mathbb{Z}[\alpha]$ is not $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$-invariant. For $m = -2$ we have $\sigma(\alpha) = -\alpha^2 - 2\alpha \in \mathbb{Z}[\alpha]$ and $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$-invariant. (Our result implies [GP, Lemma 2]. Indeed, with their notation we have $\alpha^3 \sim (m+1)\sigma^2(\alpha) + (2m+3)\sigma^4(\alpha)$ and $\omega_5 \sim -\sigma^2(\alpha) - 2\sigma^4(\alpha)$. Hence, $\{1,\alpha,\alpha^2,\alpha^3,\omega_5\}$ is also a $\mathbb{Z}$-basis of $\mathbb{Z}[\mathrm{conj}(\alpha)]$.)

The assertion on $\mathbb{Z}[\mathrm{conj}(\alpha)]^\times$ follows from [SW, Theorem (3.5)] and [Jean, Theorem 2.2.2], once we notice that the crucial point of their proofs is not that they are working with $\mathbb{Z}_{\mathbb{K}}$ but with a Galois-invariant order of $\mathbb{K}$. (See also the imprecise statement in [GP, Lemma 3] where they should have made the same assumption on m as in their Lemma 1.)

The proof of the last assertion is similar to the proof of the cubic case given in the proof Proposition 3, by using [Lou07, Lemma 21] or [Jean, Théorème 1] instead of [Lou07, Theorem 14]. ∎

Even working with $\mathbb{Z}[\mathrm{conj}(\alpha)]$ is sometimes not satisfactory enough (notice that the $\mathbb{Z}$-basis of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ and $\mathbb{M}'$ in the following Proposition 6 are of the type considered in Proposition 10):

Proposition 6. *As in* [Wa2]*, let α be a root of the quartic polynomial $\Pi_\alpha(x) = X^4 - m^2X^3 - (m^3+2m^2+4m+2)X^2 - m^2X + 1 \in \mathbb{Z}[X]$, with $-1 \neq m \in \mathbb{Z}$ odd, $\mathbb{Q}$-irreducible of odd discriminant $D_m = (m+2)^4 f_m F_m^2$, where $f_m = m^2+4$ and $F_m = m(m+2)(m^2+4)$. Set $\beta = (\alpha-1)^2/(m+2)$ and $\gamma = (\alpha-1)^3/(m+2)$. Then $\mathbb{K} = \mathbb{Q}(\alpha)$ is a totally real cyclic quartic field with* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle\sigma\rangle$*, where*

$$\sigma(\alpha) = \alpha^3 - (m^2-m+2)\alpha^2 - m(m^2+m+3)\alpha + m - \gamma. \tag{3}$$

Hence, $\mathbb{Z}[\alpha]$ which is not $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*-invariant is never equal to $\mathbb{Z}_{\mathbb{K}}$. The* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*-invariant quartic order* $\mathbb{Z}[\mathrm{conj}(\alpha)]$ *admits $\{1, \alpha, \alpha^2, \sigma(\alpha)\}$ as a $\mathbb{Z}$-basis and $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = (m+2)^2 f_m F_m^2$. The module $\mathbb{M}' := \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma$ is a* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*-invariant order of $\mathbb{K}$ and $D_{\mathbb{M}'} = f_m F_m^2$. Hence,* $\mathbb{Z}[\mathrm{conj}(\alpha)]$ *is never equal to $\mathbb{Z}_{\mathbb{K}}$. Finally, $\mathbb{M}' = \mathbb{Z}_{\mathbb{K}}$ if and only if F_m is square-free. This happens infinitely many often with positive probability.*

Proof. Set $\mathbb{M} := \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \mathbb{Z}\gamma$. Then $\mathbb{Z}[\alpha] \subseteq \mathbb{M} \subseteq \mathbb{Z}[\mathrm{conj}(\alpha)]$. Now, $\alpha\gamma = (m^2-3)\gamma + \delta \in \mathbb{M}$, where $\delta \in \mathbb{Z}[\alpha]$, and $\gamma^2 \in \mathbb{Z}[\alpha] \subseteq \mathbb{M}$. Hence $\mathbb{M}$ is a subring of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ containing α, $\sigma(\alpha)$, by (3), $\sigma^2(\alpha) = 1/\alpha \in \mathbb{Z}[\alpha]$ and $\sigma^3(\alpha) = m^2 - \alpha - \sigma(\alpha) - \sigma^2(\alpha)$. Therefore, we do have $\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{M} = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \mathbb{Z}\sigma(\alpha)$. Hence, $(\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha]) = m+2$ and $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = D_\alpha/((\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha]))^2 = (m+2)^2 f_m F_m^2$.

Now, $\beta^2 - (m-2)\alpha\beta - m\alpha^2 = 0$. Hence, $\beta \in \mathbb{Z}_{\mathbb{K}}$ and $\mathbb{M}' \subseteq \mathbb{Z}_{\mathbb{K}}$. Since one can check that $\sigma(\alpha) \in \mathbb{M}'$, by (3), $\sigma(\beta) + (m^4 - 3m^2 + m - 1)\beta - m^2\gamma \in \mathbb{Z}[\alpha] \subseteq \mathbb{M}'$ and $\sigma(\gamma) - (m^4 + m^3 + 2m - 1)\gamma \in \mathbb{Z}[\alpha] \subseteq \mathbb{M}'$, the module $\mathbb{M}'$ is indeed $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$-invariant. Finally, it is easy to check that $\mathbb{M}'$ is multiplicatively closed.

For the last assertion, we notice that $\mathbb{K}_2 = \mathbb{Q}(\alpha + 1/\alpha) = \mathbb{Q}(\sqrt{m^2+4})$ is the quadratic subfield of $\mathbb{K}$. Hence, if $\mathbb{M}' = \mathbb{Z}_{\mathbb{K}}$, then $D_{\mathbb{K}} = D_{\mathbb{M}'} = f_m F_m^2$ is odd. Therefore, by the conductor-discriminant formula we have $f_m F_m^2 = D_{\mathbb{K}} = f_{\mathbb{K}_2} f_{\mathbb{K}}^2$, where $f_{\mathbb{K}_2}$ and $f_{\mathbb{K}}$ are square-free, by Lemma 2. It follows that F_m is square-free. Conversely, if F_m is square-free, it is proved in [Wa2, Section 1] that $D_{\mathbb{K}} = f_m F_m^2$. Hence, $D_{\mathbb{K}} = D_{\mathbb{M}'}$ and $\mathbb{Z}_{\mathbb{K}} = \mathbb{M}'$. ∎

Question 7. *Throughout his paper L. C. Washington assumes that F_m is square-free and determines a system of fundamental units for $\mathbb{Z}_{\mathbb{K}}$, see* [Wa2, Theorem page 766]*. It would be worth checking whether his proof gives a stronger result, the determination of a system of fundamental units for the order $\mathbb{M}'$. The same question applies to the simplest quartic fields considered in Proposition* 4 *and* [Gras] *and also to the recent paper* [BW].

3. A $\mathbb{Z}$-generating system of $\mathbb{Z}[\mathrm{conj}(\alpha)]$.

To date, the only cases where a $\mathbb{Z}$-basis for $\mathbb{Z}[\mathrm{conj}(\alpha)]$ has been obtained are the quadratic case (easy), the symmetric case (Theorem 8) and the cyclic cubic case (Theorem 17):

THEOREM 8 (see [Lou16]). *Let α be an algebraic integer of degree n. Then $\Omega_\alpha := \{\alpha_1^{e_1}\cdots\alpha_n^{e_n} : 0 \leq e_k \leq n-k\}$ is a $\mathbb{Z}$-generating system (with $n!$ elements) of $\mathbb{Z}[\mathrm{conj}(\alpha)]$. In particular, if $\mathrm{Gal}(\mathbb{Q}(\mathrm{conj}(\alpha))/\mathbb{Q})$ is isomorphic to the symmetric group $\mathfrak{S}_n$, then Ω_α is a $\mathbb{Z}$-basis of the order $\mathbb{Z}[\mathrm{conj}(\alpha)]$ of $\mathbb{Q}(\mathrm{conj}(\alpha))$ and the discriminant of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ is $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = D_\alpha^{n!/2}$.*

REMARKS 9. Assume that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Then $\mathbb{Z}[\mathrm{conj}(\alpha)]$ is a Galois invariant order of $\mathbb{Q}(\alpha)$ and the matrix M_α of the coordinates of the $n!$ elements of Ω_α in the canonical $\mathbb{Q}$-basis $\mathcal{B}_\alpha = \{1,\alpha,\dots,\alpha^{n-1}\}$ of $\mathbb{Q}(\alpha)$ is in $M_{n,n!}(\mathbb{Q})$. Consequently, it is not difficult to develop an algorithm for constructing a $\mathbb{Z}$-basis for the order $\mathbb{Z}[\mathrm{conj}(\alpha)]$ and for computing its discriminant $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]}$. These computations suggested us Theorem 13 below.

4. Existence of particular $\mathbb{Z}$-basis.

The following result applies to the orders $\mathbb{Z}[\mathrm{conj}(\alpha)]$:

PROPOSITION 10 (see [Coh, Corollary 4.7.6]). *Let $\mathbb{M}$ be an order in a number field $\mathbb{Q}(\alpha)$, where α is an algebraic integer of degree n. Assume that $\mathbb{Z}[\alpha] \subseteq \mathbb{M}$. There exist polynomials $P_k(X) \in \mathbb{Z}[X]$ with $\deg P_k(X) \leq k-1$ and positive integers $d_1 \mid \cdots \mid d_{n-1}$ such that $\left\{1, \frac{\alpha+P_1(\alpha)}{d_1},\dots,\frac{\alpha^{n-1}+P_{n-1}(\alpha)}{d_{n-1}}\right\}$ is a $\mathbb{Z}$-basis of $\mathbb{M}$. In that situation, we have $(\mathbb{M}:\mathbb{Z}[\alpha]) = d_1d_2\cdots d_{n-1}$.*

Proof. We give a short proof of this known result. Recall that a sub-module of a free $\mathbb{Z}$-module of rank $r \geq 1$ is a free $\mathbb{Z}$-module of rank less than or equal to r (e.g. see [ST, Theorem 1.16]).

Fix $d \geq 1$ such that $\mathbb{Z}[\alpha] \subseteq \mathbb{M} \subseteq \frac{1}{d}\mathbb{Z}[\alpha]$. For $1 \leq k \leq n$, set $\mathbb{M}_k = (\mathbb{Q}+\mathbb{Q}\alpha+\dots+\mathbb{Q}\alpha^{k-1}) \cap \mathbb{M} = \left(\frac{1}{d}\mathbb{Z}+\frac{1}{d}\mathbb{Z}\alpha+\dots+\frac{1}{d}\mathbb{Z}\alpha^{k-1}\right)\cap\mathbb{M}$. For $0 \leq k \leq n-1$, let $\lambda_k^* : \mathbb{Q}(\alpha) = \mathbb{Q}\oplus\mathbb{Q}\alpha\oplus\dots\oplus\mathbb{Q}\alpha^{n-1} \to \mathbb{Q}$ be the $\mathbb{Q}$-linear form defined by $\lambda_k^*(\sum_{i=0}^{n-1} x_i\alpha^i) = x_k$. Hence, $\lambda_k^*(\mathbb{M}) \subseteq \frac{1}{d}\mathbb{Z}$ and $\lambda_k^*(\alpha^i) \in \mathbb{Z}$ for $i \geq 0$.

Then $\mathbb{M}_n = \mathbb{M}$ is a free $\mathbb{Z}$-module of rank n. By induction on k decreasing from n to 1 we infer that $\mathbb{M}_k$ is a free $\mathbb{Z}$-module of rank k. Indeed, assume that $\mathbb{M}_k$ is free of rank k. Then $\mathbb{M}_k$ is not a sub-module of the free $\mathbb{Z}$-module $\frac{1}{d}\mathbb{Z}+\frac{1}{d}\mathbb{Z}\alpha+\dots+\frac{1}{d}\mathbb{Z}\alpha^{k-2}$ of rank $k-1$. Hence, $\lambda_{k-1}^* : \mathbb{M}_k \to \frac{1}{d}\mathbb{Z}$ is a non-trivial morphism of additive groups. Therefore, there exist $d_{k-1} \in \mathbb{Z}_{\geq 1}$ dividing d and $\omega_{k-1} \in \mathbb{M}_k$ such that $\lambda_{k-1}^*(\mathbb{M}_k) = \frac{1}{d_{k-1}}\mathbb{Z}$ and $\lambda_{k-1}^*(\omega_{k-1}) = 1/d_{k-1}$. Clearly, we have $\mathbb{M}_k = \mathbb{M}_{k-1}\oplus\mathbb{Z}\omega_{k-1}$ and $\mathbb{M}_{k-1}$ is free of rank $k-1$. Notice that since $\mathbb{Q}\cap\mathbb{M} = \mathbb{Z}$, we have $\omega_0 = 1$ and $d_0 = 1$.

Now, since $\alpha\omega_{k-2} \in \alpha\mathbb{M}_{k-1} \subseteq \mathbb{M}_k$ we have $\frac{1}{d_{k-2}} = \lambda_{k-2}^*(\omega_{k-2}) = \lambda_{k-1}^*(\alpha\omega_{k-2}) \in \lambda_{k-1}^*(\mathbb{M}_k) = \frac{1}{d_{k-1}}\mathbb{Z}$ and $d_{k-2} \mid d_{k-1}$. Moreover, $\{\omega_0,\dots,\omega_{n-1}\}$ is clearly a $\mathbb{Z}$-basis of $\mathbb{M}$ and $\omega_k = (\alpha^k+P_k(\alpha))/d_k$, where $P_k(X) = \sum_{i=0}^{k-1} p_{k,i}X^i \in \mathbb{Q}[X]$ is of degree less than k.

Finally, by induction on k increasing from 0 to $n-1$ we prove that $P_k(X) \in \mathbb{Z}[X]$. First, $0 = P_0(X) \in \mathbb{Z}[X]$. Now assume that $P_i(X) \in \mathbb{Z}[X]$ for $0 \leq i \leq k-1$. Then $\frac{d_k}{d_{k-1}}\omega_k - \alpha\omega_{k-1} = \frac{P_k(\alpha)-\alpha P_{k-1}(\alpha)}{d_{k-1}} \in \mathbb{M}\cap(\mathbb{Q}+\mathbb{Q}\alpha+\dots+\mathbb{Q}\alpha^{k-1}) = \mathbb{M}_k = \mathbb{Z}\omega_0+\dots+\mathbb{Z}\omega_{k-1}$. Since $P_{k-1}(X) \in \mathbb{Z}[X]$ and $d_{k-1}\omega_i = \frac{d_{k-1}}{d_i}d_i\omega_i \in \mathbb{Z}[\alpha]$ for $0 \leq i \leq k-1$, we do obtain $P_k(\alpha) \in \mathbb{Z}[\alpha]$. ∎

Corollary 11. *Let $\mathbb{Z}_{\mathbb{K}}$ be the ring of algebraic integers of a number field $\mathbb{K}$ of degree $n \geq 2$. There exists $\beta \in \mathbb{Z}_{\mathbb{K}}$ such that $\mathbb{K} = \mathbb{Q}(\beta)$ and such that $\mathbb{Z}_{\mathbb{K}}$ admits a $\mathbb{Z}$-basis of the form $\{1, \beta, \omega_3, \dots, \omega_n\}$.*

Proof. Notice that $\mathbb{K} = \mathbb{Q}(\beta)$ where $\beta = (\alpha + P_1(\alpha))/d_1$. ■

Lemma 12. *Let $\{\omega_1, \dots, \omega_r\}$ be a $\mathbb{Z}$-basis of a free $\mathbb{Z}$-module $\mathbb{M} \subseteq \mathbb{C}$ of rank $r \geq 1$. There exists a $\mathbb{Z}$-basis for $\mathbb{M}$ containing $\omega = a_1\omega_1 + \dots + a_r\omega_r \in \mathbb{M}$ if and only if* $\gcd(a_1, \dots, a_r) = 1$. *Consequently, assume $\mathbb{M} \cap \mathbb{Q} = \mathbb{Z}$, e.g. assume that $\mathbb{M}$ is an order of a number field. There exists a $\mathbb{Z}$-basis for $\mathbb{M}$ of the form $\{\omega_1 = 1, \omega_2, \dots, \omega_r\}$ and if $\omega = a_1 + \sum_{i=2}^r a_i\omega_i \in \mathbb{M}$, there exists a $\mathbb{Z}$-basis for $\mathbb{M}$ containing* 1 *and ω if and only if* $\delta := \gcd(a_2, \dots, a_r) = 1$.

Proof. Clearly, the condition is necessary.

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

$$x = x_1\omega_1 + \dots + x_r\omega_r \in \mathbb{M} \mapsto \phi(x) = x_1u_1 + \dots + x_ru_r \in \mathbb{Z}.$$

Then $\phi(\omega) = 1$ and $x = \phi(x)\omega + (x - \phi(x)\omega)$ for $x \in \mathbb{M}$. Therefore, $\mathbb{M} = \mathbb{Z}\omega \oplus \ker\phi$, where $\ker\phi$ is a free $\mathbb{Z}$-module of rank $r-1$ (e.g. see [ST, Theorem 1.16]). The first assertion follows. Let us prove the second assertion. If $\mathcal{B} = \{1, \omega, \omega_3', \dots, \omega_r'\}$ is a completed $\mathbb{Z}$-basis of $\mathbb{M}$, then $(\omega - a_1)/\delta = \sum_{i=2}^r \frac{a_i}{\delta}\omega_i$ being in $\mathbb{M}$ can be written as $(\omega - a_1)/\delta = b_1 + b\omega + (\sum_{i=3}^r b_i\omega_i')$, where b, $b_i \in \mathbb{Z}$. Multiplying by δ and using the $\mathbb{Z}$-linear independence of $\mathcal{B}$ we obtain $1 = b\delta$ and $\delta = b = 1$. Conversely, if $\delta = 1$, there exists a $\mathbb{Z}$-basis of $\mathbb{Z}\omega_2 + \dots + \mathbb{Z}\omega_r$ containing $\omega' := \sum_{i=2}^r a_i\omega_i$ (by the first assertion). Hence, the set $\{1, \omega'\}$ can be completed into a $\mathbb{Z}$-basis of $\mathbb{M}$. Since $\omega' := \omega - a_1$, the set $\{1, \omega\}$ can be completed into a $\mathbb{Z}$-basis of $\mathbb{M}$. ■

Theorem 13. *Let α be an algebraic integer of degree $n \geq 2$. There exists a $\mathbb{Z}$-basis of* $\mathbb{Z}[\mathrm{conj}(\alpha)]$ *containing* 1 *and α.*

Proof. The order $\mathbb{Z}[\mathrm{conj}(\alpha)]$ admits a $\mathbb{Z}$-basis of the form $\{1, \omega_2, \dots, \omega_r\}$, where $r = (\mathbb{Q}(\mathrm{conj}(\alpha)) : \mathbb{Q})$ (Lemma 12). Write $\alpha = a + \sum_{i=2}^r a_i\omega_i$, with a, $a_i \in \mathbb{Z}$. Let us prove that $\delta := \gcd(a_2, \dots, a_r) = 1$ (Lemma 12). Set $\mathbb{Z}_0[X_1, \dots, X_n] = \{P(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n] \colon P(0, \dots, 0) = 0\}$. Let $\beta_k = \alpha_k - a$ be the complex conjugates of $\beta = \alpha - a = \sum_{i=2}^r a_i\omega_i \in \delta\mathbb{Z}[\mathrm{conj}(\alpha)]$, $1 \leq k \leq n$. Since $\mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}[\beta_1, \dots, \beta_n]$, we have

$$\beta = \delta(a_0 + P(\beta_1, \dots, \beta_n)),$$

where $a_0 \in \mathbb{Z}$ and $P(X_1, \dots, X_n) \in \mathbb{Z}_0[X_1, \dots, X_n]$. Now, $\mathrm{Gal}(\mathbb{Q}(\mathrm{conj}(\alpha))/\mathbb{Q})$ acts transitively on the α_k's, hence acts transitively on the β_k's. Therefore, we obtain

$$\beta_k = \delta(a_0 + P_k(\beta_1, \dots, \beta_n)) \quad (1 \leq k \leq n),$$

where $P_k(X_1, \dots, X_n) \in \mathbb{Z}_0[X_1, \dots, X_n]$. By induction on l, it follows that

$$\beta_k = \delta(a_l + \delta^l P_{k,l}(\beta_1, \dots, \beta_n)) \quad (1 \leq k \leq n \text{ and } l \geq 0),$$

where $a_l \in \mathbb{Z}$, and $P_{k,l}(X_1, \dots, X_n) \in \mathbb{Z}_0[X_1, \dots, X_n]$. We obtain the contradiction $0 \neq \alpha_1 - \alpha_2 = \beta_1 - \beta_2 \in \delta^{l+1}\mathbb{Z}[\mathrm{conj}(\alpha)]$ for all $l \geq 0$. ■

Remarks 14. Take $\Pi_\alpha(X) = X^4+4(m^2+1)X^2+4(m^2+1)$, $m>1$, $\mathbb{Q}$-irreducible. The extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, $\alpha' = \frac{\alpha^3+2\alpha}{2m}+2m\alpha$ is a conjugate of α and $\alpha\alpha' - 2m = \frac{\alpha^2+2}{m} \in \mathbb{Z}[\mathrm{conj}(\alpha)]$, Hence, there do not exist $\mathbb{Z}$-bases of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ containing 1, α and α^2. However, if α is an algebraic integer of degree n such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois and if the index $(\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha])$ is prime, there exist $\mathbb{Z}$-bases of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ containing $1, \alpha, \dots, \alpha^{n-2}$, by Proposition 10.

Question 15. *In the cyclic cubic case, $\{1,\alpha,\alpha^2\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ if and only if $\mathbb{Z}[\alpha]$ is Galois-invariant, hence if and only if f_α divides $3b-a^2$ and $3ac-b^2$, where $D_\alpha = f_\alpha^2$* (*Theorem* 17). *In the Galois quartic case, can anyone give a simple necessary and sufficient condition for the existence of $\mathbb{Z}$-basis of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ of the form $\{1,\alpha,\alpha^2,\omega_4\}$ that would readily apply to the simplest quartic fields* (*Proposition* 4) *where such $\mathbb{Z}$-basis do exist?*

Corollary 16. *Let α ba a cubic algebraic integer. Assume that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, i.e. assume that $D_\alpha = f_\alpha^2$ is a square. Then*

$$D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = D_\alpha/(\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha])^2 = \big(f_\alpha/(\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha])\big)^2$$

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

Proof. Let $\{1,\alpha,\omega_3 = (A+B\alpha+\alpha^2)/C\}$ be a $\mathbb{Z}$-basis of $\mathbb{Z}[\mathrm{conj}(\alpha)]$, where $A,B,C \in \mathbb{Q}$ (Theorem 13). Then $\alpha^2 = -A-B\alpha+C\omega_3 \in \mathbb{Z}[\mathrm{conj}(\alpha)] = \mathbb{Z}+\mathbb{Z}\alpha+\mathbb{Z}\omega_3$. Hence, $A,B,C \in \mathbb{Z}$, by the $\mathbb{Q}$-linear independence of $\{1,\alpha,\omega_3\}$, and $\mathbb{Z}[\alpha] = \mathbb{Z}+\mathbb{Z}\alpha+\mathbb{Z}\alpha^2 = \mathbb{Z}+\mathbb{Z}\alpha+\mathbb{Z}C\omega_3$ yields $(\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha]) = C$. Finally, $\min\{d\geq 1\colon d\mathbb{Z}[\mathrm{conj}(\alpha)] \subseteq \mathbb{Z}[\alpha]\} = \min\{d \geq 1\colon d\omega_3 \in \mathbb{Z}[\alpha]\} = C$. ■

5. The cyclic cubic case. Our motivation for proving Theorem 13 is that we knew it to hold in the symmetric case (Theorem 8) and in the cyclic cubic case (Theorem 17). Our aim in the present section is to give a new proof of Theorem 17, based on Corollary 16 to Theorem 13. We hope this new approach might be helpful to find an analog of Theorem 17 in the two possible Galois quartic cases: (i) in the bicyclic biquadratic case where we have not yet managed to adopt the method used in [LL16] and (ii) in the cyclic quartic case where the method used in [LL16] cannot work. In these two cases we presently only know of an improvement on Theorem 8 which gives a $\mathbb{Z}$-generating system with 24 elements. Indeed, by [LL16, Lemmas 7 and 8] we know beforehand $\mathbb{Z}$-generating subsets of $\mathbb{Z}[\mathrm{conj}(\alpha)]$ with 16 elements (cyclic quartic case) or 12 elements (biquadratic bicyclic case).

Theorem 17 (see [LL16, Theorem 2]). *Let $\Pi_\alpha(X) = X^3-aX^2+bX-c \in \mathbb{Z}[X]$ be the minimal polynomial of a cubic algebraic integer α. Assume that the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, i.e. that $D_\alpha = f_\alpha^2$ is a square. Then $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = \Delta_\alpha^2$, where*

$$\Delta_\alpha = \gcd(f_\alpha, a^2-3b, b^2-3ac).$$

In particular, the cubic order $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$*-invariant if and only if f_α divides a^2-3b and b^2-3ac. Moreover, let α' be any one of the two other conjugates of α and* *let* $x, y, z \in \mathbb{Z}$ *be such that*

$$xf_\alpha + y(a^2 - 3b) + z(b^2 - 3ac) = \Delta_\alpha = \gcd(f_\alpha, a^2 - 3b, b^2 - 3ac)$$

Then $\{1, \alpha, \eta = x\alpha^2 + y\alpha' + z\alpha'\alpha^2\}$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}[\mathrm{conj}(\alpha)]$.

Proof. We may assume that $f_\alpha = (\alpha - \alpha')(\alpha - \alpha'')(\alpha' - \alpha'')$. By Theorem 8, $\Omega_\alpha = \{1, \alpha, \alpha^2, \alpha', \alpha\alpha', \alpha^2\alpha'\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\mathrm{conj}(\alpha)]$. By [Lou12, Proposition 10], the matrix M_α of the coordinates of the elements of Ω_α in the $\mathbb{Q}$-basis $\mathcal{B}_\alpha = \{1, \alpha, \alpha^2\}$ is

$$M_\alpha = \begin{pmatrix} 1 & 0 & 0 & \frac{a^2b+3ac-4b^2+af_\alpha}{2f_\alpha} & \frac{(2a^2-6b)c}{2f_\alpha} & \frac{(ab-9c-f_\alpha)c}{2f_\alpha} \\ 0 & 1 & 0 & \frac{-2a^3+7ab-9c-f_\alpha}{2f_\alpha} & \frac{-a^2b+3ac+2b^2+af_\alpha}{2f_\alpha} & \frac{2a^2c-ab^2+3bc+bf_\alpha}{2f_\alpha} \\ 0 & 0 & 1 & \frac{2a^2-6b}{2f_\alpha} & \frac{ab-9c-f_\alpha}{2f_\alpha} & \frac{-6ac+2b^2}{2f_\alpha} \end{pmatrix}.$$

Indeed, it suffices to determine its fourth column, i.e. the coordinates of $\alpha' = ((\alpha' + \alpha'') + (\alpha' - \alpha''))/2$ in $\mathcal{B}_\alpha$, from which those of $\alpha\alpha'$ and $\alpha^2\alpha'$ follow. We notice that $\alpha' + \alpha'' = a - \alpha$ and that

$$\alpha' - \alpha'' = \frac{(\alpha - \alpha')(\alpha - \alpha'')(\alpha' - \alpha'')}{(\alpha - \alpha')(\alpha - \alpha'')} = \frac{f_\alpha}{\Pi'_\alpha(\alpha)} = \frac{f_\alpha}{3\alpha^2 - 2a\alpha + b},$$

i.e. that

$$\alpha' - \alpha'' = \frac{(2a^2 - 6b)\alpha^2 - (2a^3 - 7ab + 9c)\alpha + a^2b + 3ac - 4b^3}{f_\alpha}.$$

For $1 \leq i \leq 3$ and $4 \leq j \leq 6$, let $n_{i,j}/(2f_\alpha)$ be the (i,j)-coefficient of M_α, with $n_{i,j} \in \mathbb{Z}$. By Corollary 16, we have $(\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha]) = 2f_\alpha / \gcd(n_{i,j})$ and

$$D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = \left(\frac{f_\alpha}{(\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha])}\right)^2 = \left(\frac{1}{2} \gcd_{\substack{1 \leq i \leq 3 \\ 4 \leq j \leq 6}} (n_{i,j})\right)^2 = \left(\frac{1}{2} \gcd(n_{3,4}, n_{3,5}, n_{3,6})\right)^2,$$

where we have used

$$n_{1,4} = bn_{3,4} - an_{3,5} + n_{3,6}, \quad n_{1,5} = cn_{3,4}, \quad n_{1,6} = cn_{3,5},$$
$$n_{2,4} = -2an_{3,4} + n_{3,5}, \quad n_{2,5} = -an_{3,5} + n_{3,6} \quad \text{and} \quad n_{2,6} = cn_{3,4} - bn_{3,5}.$$

Noticing that $f_\alpha^2 = D_\alpha = -4a^3c - 4b^3 + a^2b^2 + 18abc - 27c^2$ we obtain

$$n_{3,5}^2 + n_{3,5}(2f_\alpha) + (2f_\alpha)^2 = (ab - 9c)^2 + 3f_\alpha^2 = n_{3,4}n_{3,6}$$

and

$$\gcd(n_{3,4}, n_{3,5}, n_{3,6}) = \gcd(n_{3,4}, 2f_\alpha, n_{3,6}) = \gcd(2a^2 - 6b, 2f_\alpha, -6ac + 2b^2),$$

by Lemma 18. The desired result on $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]}$ follows.

As for the last assertion, it follows from (1), (2) and

$$\begin{aligned} D(1, \alpha, \eta) &= \big(x\Delta(1, \alpha, \alpha^2) + y\Delta(1, \alpha, \alpha') + z\Delta(1, \alpha, \alpha'\alpha^2)\big)^2 \\ &= \big(-xf_\alpha + y(3b - a^2) + z(3ac - b^2)\big)^2 = \Delta_\alpha^2 = D_{\mathbb{Z}[\mathrm{conj}(\alpha)]}, \end{aligned}$$

where the σ_i's in (2) are chosen such that $\sigma_1(\alpha) = \alpha$, $\sigma_2(\alpha) = \alpha'$ and $\sigma_3(\alpha) = \alpha''$. ■

Lemma 18. *If* $A^2 + AB + B^2 = CD \neq 0$, *then*

$$\gcd(A, C, D) = \gcd(B, C, D) = \gcd(A, B, C, D).$$

Proof. By symmetry, it suffices to prove that $\gcd(A,C,D)$ divides B, hence that if p is prime and p^k divides A and p^{2k} divides $(A+B)B = CD - A^2$ then p^k divides B. This assertion is clear because if p^l is the highest power of p that divides B and $l < k$ then p^{2l} is the highest power of p that divides $(A+B)B$. This proof is simpler than the one of [LL16, Lemma 5] ■

Remarks 19. For the polynomials $P_{f,g}(X)$ introduced in [Bal], we have $\Delta_\alpha = \gcd(f_\alpha, 3\lambda - a^2, -3a - \lambda^2)$ with $f_\alpha = (f-g)(3a+\lambda^2)$ and $a^2 - 3\lambda = (f^2+g^2-fg)(3a+\lambda^2)$. Hence, $\Delta_\alpha = 3a + \lambda^2$ which is [Bal, Corollary 5.3]. In the same way, Theorem 17 proves in one fell swoop the assertion on the $\mathbb{Z}$-bases in [LL14, Theorem 1.2].

6. The behavior of the orders $\mathbb{Z}[\alpha^k]$ and $\mathbb{Z}[\mathrm{conj}(\alpha^k)]$. Let α be an algebraic integer of degree n. Set

$$\begin{aligned}\mathcal{E}_\alpha &= \{k \geq 1\colon \mathbb{Q}(\alpha^k) = \mathbb{Q}(\alpha)\} = \{k \geq 1\colon (\mathbb{Q}(\alpha^k) : \mathbb{Q}) = n\},\\ E_\alpha &= \{k \in \mathcal{E}_\alpha\colon \mathbb{Z}[\alpha^k] = \mathbb{Z}[\alpha]\} = \{k \in \mathcal{E}_\alpha\colon D_{\alpha^k} = D_\alpha\}\end{aligned}$$

and

$$\mathcal{S}_\alpha = \{k \in \mathcal{E}_\alpha\colon \mathbb{Z}[\mathrm{conj}(\alpha^k)] = \mathbb{Z}[\mathrm{conj}(\alpha)]\} = \{k \in \mathcal{E}_\alpha\colon D_{\mathbb{Z}[\mathrm{conj}(\alpha^k)]} = D_{\mathbb{Z}[\mathrm{conj}(\alpha)]}\}.$$

As k varies in $\mathcal{E}_\alpha$, we would like to understand the behaviors of the $\mathbb{Z}[\alpha^k]$'s, orders of $\mathbb{Q}(\alpha)$, of the $\mathbb{Z}[\mathrm{conj}(\alpha^k)]$'s, orders of $\mathbb{Q}(\mathrm{conj}(\alpha)) = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$, and of their discriminants D_{α^k} and $D_{\mathbb{Z}[\mathrm{conj}(\alpha^k)]}$. For simplicity, we usually assume that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. In that case, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\mathrm{conj}(\alpha)]$ are orders of the number field $\mathbb{Q}(\alpha)$.

If ε is a root of unity of order n, then $\mathcal{E}_\varepsilon = \{k \geq 1\colon \gcd(k,n) = 1\}$ and $\mathbb{Z}[\varepsilon^k] = \mathbb{Z}[\varepsilon] = \mathbb{Z}[\mathrm{conj}(\varepsilon)] = \mathbb{Z}[\mathrm{conj}(\varepsilon^k)]$ for $k \in \mathcal{E}_\varepsilon$.

If $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a totally real cubic extension or more generally an extension with at least three real embeddings and no proper subfield, then $\mathcal{E}_\alpha = \mathbb{Z}_{\geq 1}$ (if $\mathbb{Q}(\alpha^k) \subsetneqq \mathbb{Q}(\alpha)$, then $\alpha^k = r \in \mathbb{Q}$ and all the real conjugates of α are solutions of the equation $x^k = r$ which has at most two real solutions).

In contrast, $\mathcal{E}_\alpha = \{k \geq 1\colon 3 \nmid k\}$ for the non-totally real cubic algebraic integer $\alpha = \sqrt[3]{2}$.

On the one hand, since D_{α^k} goes to infinity as k goes to infinity, see Theorem 20, the set E_α is always finite and it is reasonable to make guesses on the precise behavior of the $\mathbb{Z}[\alpha^k]$'s, see Conjecture 23.

On the other hand, it is natural to wonder whether for some α's or most α's we have $\mathbb{Z}[\mathrm{conj}(\alpha^k)] = \mathbb{Z}[\mathrm{conj}(\alpha)]$ for infinitely many k's in $\mathcal{E}_\alpha$, or even for a positive proportion

$$0 < \rho_\alpha := \lim_{K\to\infty} \frac{\#[1,K] \cap S_\alpha}{\#[1,K] \cap \mathcal{E}_\alpha}$$

of the k's in $\mathcal{E}_\alpha$.

The behaviors of the $D_{\mathbb{Z}[\mathrm{conj}(\alpha^k)]}$'s and $\mathbb{Z}[\mathrm{conj}(\alpha^k)]$'s seem hard to predict at the moment. To begin with, we know of only few cases for which a formula for the $D_{\mathbb{Z}[\mathrm{conj}(\alpha^k)]}$'s can help us study these behaviors, see Theorems 8 and 17. So we did extended computations in the Galois cubic and quartic cases. According to these computations, it seems that there are some cyclic cubic α's for which $k \mapsto D_{\mathbb{Z}[\mathrm{conj}(\alpha^k)]}$ is a strictly increasing sequence, see Question 25. However, for any cyclic cubic unit ε the sequence $k \mapsto D_{\mathbb{Z}[\mathrm{conj}(\epsilon^k)]}$ seems to come back to its first term with a positive probability, see Conjecture 26. For the Galois quartic cases the situation is less clear for it seems that for bicyclic biquadratic quartic units the sequence $k \mapsto D_{\mathbb{Z}[\mathrm{conj}(\epsilon^k)]}$ may never come back to its first term, see Conjecture 30.

In this final section, we start to investigate these questions. From a computational point of view, for a given bound K we only have access to $\mathcal{E}_\alpha(K) = [1, K] \cap \mathcal{E}_\alpha$ and

$$E_\alpha(K) = [1, K] \cap E_\alpha, \quad \mathcal{S}_\alpha(K) = [1, K] \cap \mathcal{S}_\alpha \text{ and } \rho_\alpha(K) = \frac{\#\mathcal{S}_\alpha(K)}{\#\mathcal{E}_\alpha(K)}. \tag{4}$$

6.1. The behavior of the orders $\mathbb{Z}[\alpha^k]$

Theorem 20 (see [Dub] and [Lou20]). *Let $\alpha \neq 0$ be an algebraic integer which is not a root of unity. Then the discriminants D_{α^k} go exponentially to infinity with k.*

In the cubic and totally imaginary quartic cases we have results much better than Theorem 20:

Theorem 21. *Let ε be a cubic* unit. *Then, $|D_{\varepsilon^k}| \geq h_\varepsilon^k/2$ for some explicit $h_\varepsilon > 1$, i.e. D_{ε^k} goes exponentially to infinity as k goes to infinity. Consequently, if $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is not Galois, i.e. if D_α is not a square in $\mathbb{Z}$, then $D_{\mathbb{Z}[\mathrm{conj}(\varepsilon^k)]} = D_{\varepsilon^k}^3$ also goes exponentially to infinity as k goes to infinity.*

Proof. Let η be a cubic unit.

1. (See [Lou10, Theorem 1] or [Lou15, Theorem 9].) If $D_\eta < 0$, letting η_1 be the real conjugate of η and η_2 and $\eta_3 = \bar{\eta}_2$ be the two complex conjugates of η, then $|D_\eta| \geq h_\eta/2$, where

$$h_\eta = \max(|\eta_1|, |\eta_1|^{-1}) = \max(|\eta_1|, |\eta_1|^{-1}, |\eta_2|^2, |\eta_2|^{-2}, |\eta_3|^2, |\eta_3|^{-2})^{3/2} > 1.$$

2. (See [Lou12] or [Lou15, Theorem 33].) If $D_\eta > 0$, letting η_1, η_2, η_3 be the three real conjugates of η, then $|D_\eta| \geq h_\eta/2$, where

$$h_\eta = \max(|\eta_1|, |\eta_1|^{-1}, |\eta_2|, |\eta_2|^{-1}, |\eta_3|, |\eta_3|^{-1})^{3/2} > 1.$$

By applying these bounds to ε^k and noticing that $h_{\varepsilon^k} = h_\varepsilon^k$, the first assertion follows. Now, if $\mathbb{Q}(\varepsilon^k)/\mathbb{Q} = \mathbb{Q}(\varepsilon)/\mathbb{Q}$ is not Galois, then $\mathrm{Gal}(\mathbb{Q}(\mathrm{conj}(\varepsilon^k)/\mathbb{Q}))$ is isomorphic to the symmetric group $\mathfrak{S}_3$ and $D_{\mathbb{Z}[\mathrm{conj}(\varepsilon^k)]} = D_{\varepsilon^k}^3$ (Theorem 8). ■

Theorem 22 (see [Lou10, Theorem 2]). *Let ε_1, $\bar{\varepsilon}_1$, ε_2 and $\bar{\varepsilon}_2$ be the complex conjugates of a totally imaginary quartic* unit *ε which is not a complex root of unity. Set $h_\varepsilon = \max(|\varepsilon_1|, |\varepsilon_1|^{-1}, |\varepsilon_2|, |\varepsilon_2|^{-1}) > 1$. Then, $|D_{\varepsilon^k}| \geq 7h_\varepsilon^k/10$ for $k \in \mathcal{E}_\varepsilon$, i.e. D_{ε^k} goes exponentially to infinity as $k \in \mathcal{E}_\varepsilon$ goes to infinity.*

6.2. The behavior of the cubic orders $\mathbb{Z}[\alpha^k]$. Let α be a cubic algebraic integer such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, i.e. whose discriminant $D_\alpha = f_\alpha^2$ is a square. Let $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ be its minimal polynomial. Set $H(\alpha) = \max(|a|, |b|, |c|)$. By changing α into $-\alpha$ is necessary, when doing computations we may and we will assume that $a \geq 0$. If α is assumed to be a cubic unit, we will denote it by ε instead. We computed the sets $E_\alpha(100)$ for the α's in the range $H(\alpha) \leq 200$ for which $\mathbb{Q}(\alpha)/\mathbb{Q}$ is cyclic. (The computation took 17176 seconds with Maple on a MacBook Air laptop computer and gave 7125 cyclic cubic extensions and 28 occurrences in Conjecture 23.) According to this computation, it seems reasonable to conjecture:

Conjecture 23. *Let α be a cyclic cubic algebraic integer. Then $\#E_\alpha \geq 2$ if and only if $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ with $|ab - c| = 1$, in which case $E_\alpha = \{1, 2\}$.*

At least, according to [Lou12, Theorem 1 and Lemma 5], this conjecture is true when restricted to algebraic units:

Theorem 24. *Let ε be a cyclic cubic unit. Then $\#E_\varepsilon \geq 2$ if and only if $\Pi_\varepsilon(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ with $|ab - c| = 1$, in which case $E_\varepsilon = \{1, 2\}$. Moreover, it happens only in the following* 8 *cases*:

$\Pi_\varepsilon(X)$	D_ε
$X^3 - X^2 - 2X - 1$	49
$X^3 + X^2 - 2X - 1$	49
$X^3 - 2X^2 - X + 1$	49
$X^3 + 2X^2 - X - 1$	49

$\Pi_\varepsilon(X)$	D_ε
$X^3 - 3X - 1$	81
$X^3 - 3X + 1$	81
$X^3 - 3X^2 + 1$	81
$X^3 + 3X^2 - 1$	81

The proof of Theorem 24 stems from the lowers bounds for discriminants of totally real cubic units used in the proof of Theorem 21. For algebraic integers we only have the weaker estimates obtained in the proof of Theorem 20. They are not good enough to prove Conjecture 23.

$\Pi_\alpha(X)$	K	$\rho_\alpha(K)$
$X^3 - 3X^2 - 4X - 1$	10^2	0.49
$f_\alpha = 7$	10^3	0.479
	10^4	0.4645
	10^5	0.45166
$X^3 - 9X^2 + 6X + 1$	10^2	0.34
$f_\alpha = 3^2 \cdot 7$	10^3	0.308
	10^4	0.3068
	10^5	0.30272
$X^3 - 43X^2 + 40X + 1$	10^2	0.55
$f_\alpha = 7 \cdot 13 \cdot 19$	10^3	0.492
	10^4	0.4817
	10^5	0.47455
$X^3 - 31X^2 - 25X - 1$	10^2	0.30
$f_\alpha = 2^3 \cdot 7 \cdot 13$	10^3	0.305
	10^4	0.2968
	10^5	0.28942

$\Pi_\alpha(X)$	K	$\rho_\alpha(K)$
$X^3 - 54X^2 + 69X - 1$	10^2	0.18
$f_\alpha = 3^2 \cdot 5 \cdot 7 \cdot 11$	10^3	0.161
	10^4	0.1547
	10^5	0.15172
$X^3 - 24X^2 + 23X - 5$	10^2	0.65
$f_\alpha = 13^2$	10^3	0.621
	10^4	0.5938
	10^5	0.58007
$X^3 - 33X^2 + 32X - 7$	10^2	0.72
$f_\alpha = 331$	10^3	0.624
	10^4	0.5974
	10^5	0.57832
$X^3 - 9X + 9$	10^2	0.01
$f_\alpha = 27$	10^3	0.001
	10^4	0.0001
	10^5	0.00001

Table 2

6.3. The behavior of the cubic orders $\mathbb{Z}[\mathrm{conj}(\alpha^k)]$. We come back to a problem considered in [Lou16]. We stick to the notation introduced in (4). For various cyclic cubic algebraic integers α, we computed the approximations $\rho_\alpha(K)$ to the putative probability ρ_α that $\mathbb{Z}[\mathrm{conj}(\alpha^k)] = \mathbb{Z}[\mathrm{conj}(\alpha)]$, see Table 2. (If $\Pi_\alpha(X) = X^3 - aX^2 + bX - c$, then $\Pi_{\alpha^2}(X) = X^3 - (a^2 - 2b)X^2 + (b^2 - 2ac)X - c^2$ and $\Pi_{\alpha^k}(X) = X^3 - a_kX^2 + b_kX - c^k$ with $a_{k+3} = aa_{k+2} - ba_{k+1} + ca_k$ and $b_{k+3} = bb_{k+2} - acb_{k+1} + c^2b_k$. We then use Theorem 17 to compute the $D_{\mathbb{Z}[\mathrm{conj}(\alpha^k)]} = \Delta_{\alpha^k}$'s.) It would be nice to experimentally guess and understand the dependence of ρ_α on $\Pi_\alpha(X)$.

The case $f_\alpha = 27$ of Table 2 can be generalized to show that there are probably infinitely many cases where $\mathcal{E}_\alpha = \{1\}$:

Question 25. *Consider the polynomials $\Pi_\alpha(X) = X^3 - CX + C \in \mathbb{Z}[X]$, $\mathbb{Q}$-irreducible for $C \neq 0$. According to our computation we conjecture that $\gcd(D_{\alpha^k}, (3b_k - a_k^2)^2, (3a_kc_k - b_k^2)) = C^{2(k - \lfloor k/4 \rfloor)}$, both in $\mathbb{Z}$ and $\mathbb{Z}[C]$. If one could prove this, one would get an infinite family of cyclic cubic fields $\mathbb{Q}(\alpha)$ for which $k \mapsto D_{\mathbb{Z}[\mathrm{conj}(\alpha^k)]}$ would be strictly increasing, hence for which $\mathbb{Z}[\mathrm{conj}(\alpha^k)] = \mathbb{Z}[\mathrm{conj}(\alpha)]$ if and only if $k = 1$. Indeed, $D_\alpha = C^2(4C - 27)$ is a square if and only if $C = C'^2 + C' + 7$ for some $C' \in \mathbb{Z}$.*

Let now restrict ourselves to algebraic units ε. Setting

$$\rho_{\min}(B, K) := \min\{\rho_\varepsilon(K)\colon \mathbb{Q}(\varepsilon) \text{ cubic cyclic and } H(\varepsilon) \leq B\},$$

according to these computations, we have $\rho_{\min}(50, 10^3) = \rho_\varepsilon(10^3) = 0.249$, where $\Pi_\varepsilon(X) = X^3 - 10X^2 + 17X - 1$, and there are 159 polynomials $\Pi_\alpha(X)$ in this range with $a \geq 0$. (The computation took 2000 seconds with Maple on a MacBook Air laptop computer.) We also have $\rho_{\min}(10^3, 10^2) = \rho_\varepsilon(10^2) = 0.17$, where $\Pi_\varepsilon(X) = X^3 - 489X^2 + 534X - 1$, and there are 1310 polynomials $\Pi_\alpha(X)$ in this range with $a \geq 0$. (The computation took 900 seconds with Maple on a MacBook Air laptop computer.) Hence, contrary to the non-Galois cubic case (see Theorem 21), it seems reasonable to conjecture:

Conjecture 26. *If ε is a cyclic cubic unit, then $\mathbb{Z}[\mathrm{conj}(\varepsilon^k)] = \mathbb{Z}[\mathrm{conj}(\varepsilon)]$ for a positive proportion $\rho_\varepsilon > 0$ of the $k \in \mathcal{E}_\varepsilon = \{k \geq 1\}$.*

6.4. The abelian quartic case. Let α be a quartic algebraic integer. Assume that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Restrict k to range in $\mathcal{E}_\alpha$, in which case $\mathbb{Z}[\alpha^k]$ and $\mathbb{Z}[\mathrm{conj}(\alpha)]$ are orders of $\mathbb{Q}(\alpha)$. We did similar computations as those in Section 6.3. However, here we do not have anything analogous to Theorem 17 to compute the discriminants of the $\mathbb{Z}[\mathrm{conj}(\alpha)]$'s. Instead, we used Theorem 8 and wrote a program in Maple which from the matrix $M_\alpha \in M_{4,24}(\mathbb{Q})$ of the coordinates of the 24 elements of Ω_α in the canonical $\mathbb{Q}$-basis $\mathcal{B}_\alpha = \{1, \alpha, \alpha^2, \alpha^3\}$ of $\mathbb{Q}(\alpha)$ computes a matrix $P_\alpha \in \mathrm{GL}_4(\mathbb{Q})$ of the coordinates in $\mathcal{B}_\alpha$ of a $\mathbb{Z}$-basis of $\mathbb{Z}[\mathrm{conj}(\alpha)]$. Thus $P^{-1} \in M_{4,4}(\mathbb{Z})$ and $(\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha]) = \det P^{-1}$, which gives $D_{\mathbb{Z}[\mathrm{conj}(\alpha)]} = D_\alpha / (\mathbb{Z}[\mathrm{conj}(\alpha)] : \mathbb{Z}[\alpha])^2$. For a given K, we can thus determine $\mathcal{E}_\alpha(K)$, $\mathcal{S}_\alpha(K)$ and $\rho_\alpha(K)$, with the notation of (4).

6.5. Totally imaginary Galois quartic units. When dealing with totally imaginary quartic units ε for which $\mathbb{K}/\mathbb{Q} = \mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois, we have some information. Indeed, let $\mathbb{L}$ be the real quadratic subfield (fixed by the complex conjugation) of a totally imaginary quartic Galois field $\mathbb{K}$. Let $W_\mathbb{K}$ be the multiplicative group of the complex roots of unity in $\mathbb{K}$ and $\mathbb{U}_\mathbb{K}$ and $\mathbb{U}_\mathbb{L}$ be the unit groups of the rings of algebraic integers of $\mathbb{K}$ and $\mathbb{L}$. The Hasse unit index $Q_\mathbb{K} = (U_\mathbb{K} : W_\mathbb{K} U_\mathbb{L})$ is equal to 1 or 2 (see [Hasse, Satz 14] or [Lem, Proposition 1]).

First, assume that $\mathbb{K}/\mathbb{Q} = \mathbb{Q}(\varepsilon)/\mathbb{Q}$ *is cyclic quartic.* Then $Q_{\mathbb{K}} = 1$, by [Hasse, Satz 24] or [Lem, Point 5, page 352]. Therefore, to get a totally imaginary cyclic quartic unit we must have $W_{\mathbb{K}} \neq \{\pm 1\}$. Hence, $\mathbb{K} = \mathbb{Q}(\zeta_5)$ and $\varepsilon \in \mathbb{Z}[\zeta_5]^\times = \left\{\pm\zeta_5^k\left((1-\sqrt{5})/2\right)^l : k,\ l \in \mathbb{Z}\right\}$. According to our computation it is reasonable to conjecture the following:

Conjecture 27. *Let* ε *be a totally imaginary cyclic quartic unit. Thus* $\varepsilon \in \left\{\pm\zeta_5^k\left(\frac{1-\sqrt{5}}{2}\right)^l : 1 \leq k \leq 4,\ l \in \mathbb{Z}\right\}$ *and* $\mathcal{E}_\varepsilon = \{k \geq 1 \colon 5 \nmid k\}$. *Then* $\mathbb{Z}[\mathrm{conj}(\varepsilon^k)] = \mathbb{Z}[\mathrm{conj}(\varepsilon)]$ *for all* $k \in \mathcal{E}_\varepsilon$.

Second, assume that $\mathbb{K}/\mathbb{Q} = \mathbb{Q}(\varepsilon)/\mathbb{Q}$ *is bicyclic biquadratic.* Since for an algebraic unit ε we have $\mathbb{Z}[\mathrm{conj}(\varepsilon)] = \mathbb{Z}[\mathrm{conj}(\eta)]$ for $\eta \in \{\pm\varepsilon, \pm 1/\varepsilon\}$, we may suppose the minimal polynomial $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + 1 \in \mathbb{Z}[X]$ of a quartic unit ε is reduced, i.e. such that $|c| \leq a$. The minimal polynomials $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + 1 \in \mathbb{Z}[X]$ of totally imaginary quartic units satisfy $b \geq -1$ and $0 \leq |c| \leq a \leq \sqrt{4b+5}$ (e.g. see [Lou15, Lemma 15]). In the range $-1 \leq b \leq 10^3$ and $0 \leq |c| \leq a \leq \sqrt{4b+5}$ we found 1141 minimal polynomials of totally imaginary bicyclic biquadratic units. For each of them, with $K = 100$, we computed $\mathcal{E}_\varepsilon(K)$, $\mathcal{S}_\varepsilon(K)$ and $\rho_\varepsilon(K)$. (The computation took 28423 seconds with Maple on a MacBook Air laptop computer for $-1 \leq b \leq 10^3$.) There are only 6 out of these 1141 reduced units for which $\#\mathcal{S}_\varepsilon(100) > 1$: $\Pi_{\zeta_{12}}(X) = X^4 - X^2 + 1$, $\Pi_{\zeta_8}(X) = X^4 + 1$ and the 4 non-trivial ones in Table 3 for which we did more extended computation up to $K = 800$ to check that the conjecture on $\mathcal{S}_\varepsilon$ and hence the conjecture on ρ_ε given in this Table 3.

$\Pi_\varepsilon(X) = X^4 - X^3 + 2X^2 + X + 1$ $D_\varepsilon = 2^2 \cdot 3^2 \cdot 5^2,\ \mathbb{K} = \mathbb{Q}(\sqrt{-3}, \sqrt{-15})$ $\varepsilon = \zeta_6\frac{1+\sqrt{5}}{2} = \frac{1+\sqrt{-3}+\sqrt{-15}+\sqrt{5}}{4}$	$\mathcal{E}_\varepsilon = \{k \geq 1 \colon 3 \nmid k\}$ $\mathcal{S}_\varepsilon = \{1, 2\}$ $\rho_\varepsilon = 0$
$\Pi_\varepsilon(X) = X^4 - 4X^3 + 5X^2 - 2X + 1$ $D_\varepsilon = 2^4 \cdot 3^2,\ \mathbb{K} = \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$ $\varepsilon = \zeta_{24}\sqrt{2+\sqrt{3}} = \frac{2+\sqrt{-1}+\sqrt{3}}{2}$	$\mathcal{E}_\varepsilon = \{k \geq 1 \colon 12 \nmid k\}$ $\mathcal{S}_\varepsilon = \{k \geq 1 \colon k \equiv \pm 1 \pmod 6\}$ $\rho_\varepsilon = 4/11$
$\Pi_\varepsilon(X) = X^4 - 14X^3 + 53X^2 - 4X + 1$ $D_\varepsilon = 2^4 \cdot 3^2 \cdot 13^2 \cdot 17^2,\ \mathbb{K} = \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$ $\varepsilon = \zeta_{24}\sqrt{(2+\sqrt{3})^3} = \frac{7+2\sqrt{-1}+\sqrt{-3}+4\sqrt{3}}{2}$	$\mathcal{E}_\varepsilon = \{k \geq 1 \colon 12 \nmid k\}$ $\mathcal{S}_\varepsilon = \{k \geq 1 \colon k \equiv \pm 1 \pmod 6\}$ $\rho_\varepsilon = 4/11$
$\Pi_\varepsilon(X) = X^4 - 52X^3 + 725X^2 - 14X + 1$ $D_\varepsilon = 2^4 \cdot 3^2 \cdot 181^2 \cdot 241^2,\ \mathbb{K} = \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$ $\varepsilon = \zeta_{24}\sqrt{(2+\sqrt{3})^5} = \frac{26+7\sqrt{-1}+4\sqrt{-3}+15\sqrt{3}}{2}$	$\mathcal{E}_\varepsilon = \{k \geq 1 \colon 12 \nmid k\}$ $\mathcal{S}_\varepsilon = \{k \geq 1 \colon k \equiv \pm 1 \pmod 6\}$ $\rho_\varepsilon = 4/11$

Table 3. ($\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = C_2 \times C_2$)

Conjecture 28. *Let* ε *be a totally imaginary bicyclic biquadratic unit which is not a complex root of unity. Then* $\#\mathcal{S}_\varepsilon > 1$ *if and only if either* (i) $\varepsilon \in \{\pm\zeta_6^k(2+\sqrt{3})^l : k, l \in \{\pm 1\}\}$, $\mathcal{E}_\varepsilon = \{k \geq 1 \colon 3 \nmid k\}$, $\mathcal{S}_\varepsilon = \{1, 2\}$ *and* $\rho_\varepsilon = 0$, *or* (ii) $\varepsilon \in \left\{\pm\sqrt{\zeta_{12}^k(2+\sqrt{3})^l} : k \in \{1, 5, 7, 11\},\ l \text{ odd}\right\}$, $\mathcal{E}_\varepsilon = \{k \geq 1 \colon 12 \nmid k\}$, $\mathcal{S}_\varepsilon = \{k \geq 1 \colon k \equiv \pm 1 \pmod 6\}$ *and* $\rho_\varepsilon = 4/11$.

Notice that the complex conjugates of $\sqrt{\zeta_{12}(2+\sqrt{3})^l}$ are $\sqrt{\zeta_{12}(2+\sqrt{3})^l}$, $\sqrt{\zeta_{12}^5(2+\sqrt{3})^{-l}}$, $\sqrt{\zeta_{12}^7(2+\sqrt{3})^{-l}}$ and $\sqrt{\zeta_{12}^{11}(2+\sqrt{3})^l}$.

6.6. Totally real Galois quartic units

First, assume that $\mathbb{K}/\mathbb{Q} = \mathbb{Q}(\varepsilon)/\mathbb{Q}$ *is cyclic quartic.* There are 138 reduced polynomials $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Z}[X]$, $d \in \{\pm 1\}$, in the range $H(\alpha) = \max(|a|, |b|, |c|) \leq 50$ for which $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is a totally real Galois cyclic extension. For these 138 reduced polynomials we found that $0.17 \leq \rho_\varepsilon(100) \leq 0.52$, see the excerpt of our computation given in Table 4. (The computation took 5427 seconds with Maple on a MacBook Air laptop computer.)

$\Pi_\varepsilon(X)$	K	$\#\mathcal{E}_\varepsilon(K)$	$\#\mathcal{S}_\varepsilon(K)$	$\rho_\varepsilon(K)$
$X^4 - 24X^3 + 26X^2 - 9X + 1$	100	100	17	0.17
$D_\varepsilon = 1125$	200	200	38	0.19
$\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = C_4$	400	400	74	0.185
$\mathbb{Q}(\varepsilon)$ totally real	800	800	143	0.17875
$X^4 - 39X^3 + 16X^2 + 16X + 1$	100	100	52	0.52
$D_\varepsilon = 674541125$	200	200	102	0.51
$\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = C_4$	400	400	202	0.505
$\mathbb{Q}(\varepsilon)$ totally real	800	800	395	0.49375

Table 4

Therefore, as in Conjecture 26, it seems reasonable to conjecture:

CONJECTURE 29. *If* ε *is a totally real cyclic quartic unit, then* $\mathcal{E}_\varepsilon = \{k \geq 1\}$ *and* $\mathbb{Z}[\mathrm{conj}(\varepsilon^k)] = \mathbb{Z}[\mathrm{conj}(\varepsilon)]$ *for a positive proportion* $\rho_\varepsilon > 0$ *of the* $k \in \mathcal{E}_\varepsilon$.

Second, assume that $\mathbb{K}/\mathbb{Q} = \mathbb{Q}(\varepsilon)/\mathbb{Q}$ *is bicyclic biquadratic.* There are 121 reduced polynomials $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Z}[X]$, $d \in \{\pm 1\}$, in the range $H(\alpha) = \max(|a|, |b|, |c|) \leq 30$ for which $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is a totally real Galois bicyclic biquadratic extension. For 95 out of these units ε we found that $\mathcal{E}_\varepsilon(100) = \{1\}$ and for the 26 remaining ones we found that $\mathcal{E}_\varepsilon(100) = \{1, \dots, 100\}$ and $0.17 \leq \rho_\varepsilon(100) \leq 0.29$, see the excerpt of our computation given in Table 5. (The computation took 2817 seconds with Maple on a MacBook Air laptop computer.)

$\Pi_\varepsilon(X)$	K	$\#\mathcal{E}_\varepsilon(K)$	$\#\mathcal{S}_\varepsilon(K)$	$\rho_\varepsilon(K)$
$X^4 - 46X^3 - 19X^2 + 4X + 1$	100	100	14	0.14
$D_\varepsilon = 110250000$	200	200	30	0.15
$\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = C_2 \times C_2$	400	400	52	0.13
$\mathbb{Q}(\varepsilon)$ totally real	800	800	105	0.13125
$X^4 - 13X^3 - 18X^2 + 11X - 1$	100	100	29	0.29
$D_\varepsilon = 8410000$	200	200	61	0.305
$\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = C_2 \times C_2$	400	400	115	0.2875
$\mathbb{Q}(\varepsilon)$ totally real	800	800	220	0.275

Table 5

Therefore, it seems reasonable to conjecture:

Conjecture 30. *If ε is a totally real bicyclic biquadratic unit, then either* (i) $\mathcal{E}_\varepsilon = \{1\}$ *or* (ii) $\mathcal{E}_\varepsilon = \{k \geq 1\}$*and* $\mathbb{Z}[\mathrm{conj}(\varepsilon^k)] = \mathbb{Z}[\mathrm{conj}(\varepsilon)]$ *for a positive proportion* $\rho_\varepsilon > 0$ *of the* $k \in \mathcal{E}_\varepsilon$.

Moreover, both cases have positive probability.

At least, it would be worth finding a necessary and sufficient condition on $\Pi_\varepsilon(X)$ for having $\mathcal{E}_\varepsilon = \{1\}$.

Acknowledgements. We would like to thank J.-R. Belliard for helpful discussions on modules while we were working on Section 4 and J. Oesterlé, J.-H. Evertse and K. Györy while we were working on Theorem 20.

References

[Bal] S. Balady, *Families of cyclic cubic fields*, J. Number Theory 167 (2016), 394–406.

[BW] S. Balady, L. C. Washington, *A family of cyclic quartic fields with explicit fundamental units*, Acta Arith. 187 (2019), 43–57.

[Coh] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, Berlin, 1993.

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

[Cus] T. W. Cusick, *Lower bounds for regulators*, in: Number Theory, Noordwijkerhout 1983, Lectures Notes in Math. 1068, Springer, Berlin, 1984, 63–73.

[Dub] A. Dubickas, *On the discriminant of the power of an algebraic number*, Studia Sci. Math. Hungar. 44 (2007), 27–34.

[GP] I. Gaál, M. Pohst, *Power integral bases in a parametric family of totally real cyclic quintics*, Math. Comp. 66 (1997), 1689–1696.

[Gras] M. N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré* 4 *de Q*, Publ. math. fasc. 2, Fac. Sci. Besançon, 1977/1978.

[Hasse] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.

[Jean] S. Jeannin, *Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer*, J. Théor. Nombres Bordeaux 8 (1996), 75–92.

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

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

[Lem] F. Lemmermeyer, *Ideal class groups of cyclotomic fields. I*, Acta Arith. 72 (1995), 347–359.

[Lou04] S. Louboutin, *Class numbers of real cyclotomic fields*, Publ. Math. Debrecen 64 (2004), 451–461.

[Lou07] S. Louboutin, *Efficient computation of root numbers and class numbers of parametrized families of real abelian number fields*, Math. Comp. 76 (2007), 455–473.

[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*, in: Publ. Math. Besançon Algèbre et Théorie des Nombres 2015, Presses Univ. Franche-Comté, Besançon, 2016, 41–68.

[Lou16] S. Louboutin, *Discriminants of $\mathfrak{S}_n$-orders*, Int. J. Number Theory 12 (2016), 1899–1905.

[Lou20] S. Louboutin, *On the discriminants of the powers of an algebraic integer*, Canad. Math. Bull. 63 (2020), 481–483.

[Nar] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, second ed., Springer, Berlin; PWN, Warsaw, 1990.

[Ric] C. Ricci, *Ricerche arithmetiche sui polinomi*, Rend. Circ. Mat. Palermo 57 (1933), 433–475.

[SW] R. Schoof, L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. 50 (1988), 543–556.

[ST] I. Stewart, D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, third ed., A K Peters, Natick, MA, 2002.

[Tho] E. Thomas, *Fundamental units for orders in certain cubic number fields*, J. Reine Angew. Math. 310 (1979), 33–55.

[Wa1] L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. 48 (1987), 371–384.

[Wa2] L. C. Washington, *A family of cyclic quartic fields arising from modular curves*, Math. Comp. 57 (1991), 763–775.