Stéphane R. Louboutin

When is the order generated by a cubic, quartic or quintic algebraic unit Galois invariant: three conjectures

Czechoslovak Mathematical Journal, Vol. 70 (2020), No. 4, 905–919

Persistent URL: http://dml.cz/dmlcz/148400

Czechoslovak Mathematical Journal, 70 (145) (2020), 905–919

WHEN IS THE ORDER GENERATED BY A CUBIC, QUARTIC OR QUINTIC ALGEBRAIC UNIT GALOIS INVARIANT: THREE CONJECTURES

Stéphane R. Louboutin, Marseille

Received January 15, 2019. Published online March 30, 2020.

Abstract. Let ε be an algebraic unit of the degree $n \geqslant 3$. Assume that the extension $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois. We would like to determine when the order $\mathbb{Z}[\varepsilon]$ of $\mathbb{Q}(\varepsilon)$ is $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$-invariant, i.e. when the n complex conjugates $\varepsilon_1, \ldots, \varepsilon_n$ of ε are in $\mathbb{Z}[\varepsilon]$, which amounts to asking that $\mathbb{Z}[\varepsilon_1, \ldots, \varepsilon_n] = \mathbb{Z}[\varepsilon]$, i.e., that these two orders of $\mathbb{Q}(\varepsilon)$ have the same discriminant. This problem has been solved only for $n = 3$ by using an explicit formula for the discriminant of the order $\mathbb{Z}[\varepsilon_1, \varepsilon_2, \varepsilon_3]$. However, there is no known similar formula for $n > 3$. In the present paper, we put forward and motivate three conjectures for the solution to this determination for $n = 4$ (two possible Galois groups) and $n = 5$ (one possible Galois group). In particular, we conjecture that there are only finitely many cyclic quartic and quintic Galois-invariant orders generated by an algebraic unit. As a consequence of our work, we found a parametrized family of monic quartic polynomials in $\mathbb{Z}[X]$ whose roots ε generate bicyclic biquadratic extensions $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ for which the order $\mathbb{Z}[\varepsilon]$ is $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$-invariant and for which a system of fundamental units of $\mathbb{Z}[\varepsilon]$ is known. According to the present work it should be difficult to find other similar families than this one and the family of the simplest cubic fields.

Keywords: unit; algebraic integer; cubic field; quartic field; quintic field

MSC 2020: 11R27, 11R16, 11R20

1. Introduction

Let G be a given finite group of the order n. We would like to find monic $\mathbb{Q}$-irreducible polynomials $\Pi_G(X) \in \mathbb{Z}[X]$ of the degree n with constant terms $\Pi_G(0) \in \{\pm 1\}$ such that (i) $\mathbb{K}_G := \mathbb{Q}(\varepsilon_G)$ is a normal number field with Galois group G and (ii) the order $\mathbb{Z}[\varepsilon_G]$ is G-invariant, where ε_G is any complex root of $\Pi_G(X)$. The idea is that ε_G and its complex conjugates, which are algebraic units, might in this situation generate a subgroup of finite index in the group of

DOI: 10.21136/CMJ.2020.0019-19

units $\mathbb{Z}[\varepsilon_G]^\times$ of the order $\mathbb{Z}[\varepsilon_G]$, see Proposition 3.1 and Theorem 4.2. They might even form a system of fundamental units of this order, see Theorems 4.2 and 4.3, and Conjecture 4.2.

For example, the primitive nth root of unity $\zeta_n = \exp(2\pi\mathrm{i}/n)$, $n > 2$, is a totally complex algebraic unit such that the order $\mathbb{Z}[\zeta_n]$ is $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$-invariant with $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. More interestingly, consider the ring of algebraic integers $\mathbb{Z}[2\cos(2\pi/n)]$ of $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\cos(2\pi/n))$ (see [7] and [14]). In Proposition 2.1 we prove that there exists an algebraic unit $\varepsilon_n \in \mathbb{Z}[2\cos(2\pi/n)]$ such that $\mathbb{Z}[\varepsilon_n] = \mathbb{Z}[2\cos(2\pi/n)]$. In particular, the order $\mathbb{Z}[\varepsilon_n]$ is $\mathrm{Gal}(\mathbb{Q}(\varepsilon_n)/\mathbb{Q})$-invariant with $\mathrm{Gal}(\mathbb{Q}(\varepsilon_n)/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*/\{\pm 1\}$.

In Section 4, we consider a slightly different problem. For a given small degree $n \geqslant 3$ we would like to characterize and determine the minimal polynomials of algebraic units ε of the degree n for which $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois and $\mathbb{Z}[\varepsilon]$ is $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$-invariant (the problem is trivial for $n = 2$). In Theorem 4.2, we recall the only presently known situation in which this problem has been solved: the cyclic cubic units. Then, having performed some extended numerical computation, we conjecture the solution to this problem for the quartic and quintic units. In particular, we conjecture that there are only finitely many cyclic quartic and cyclic quintic Galois-invariant orders generated by an algebraic unit. We refer the reader to [12] for another problem of the same nature.

In Section 6, we try to generalize to the bicyclic biquadratic case the already known necessary and sufficient condition for the order generated by a cyclic cubic algebraic integer to be Galois-invariant (see Theorem 4.1). We have only found a necessary condition (see Proposition 6.1). However, having performed some numerical computation, we conjecture that it is in fact a necessary and sufficient condition (see Conjecture 6.1).

2. The case of real cyclotomic fields

Proposition 2.1. *Set $\alpha_n = 2\cos(2\pi/n)$, $n > 4$ and $n \neq 6$. Then*

$$\varepsilon_n := \begin{cases} -1 + \alpha_n & \text{if } n \text{ is a prime power,} \\ -2 + \alpha_n & \text{otherwise,} \end{cases}$$

is a totally real algebraic unit and the order $\mathbb{Z}[\varepsilon_n] = \mathbb{Z}[\alpha_n]$ is $\mathrm{Gal}(\mathbb{Q}(\varepsilon_n)/\mathbb{Q})$-invariant with $\mathrm{Gal}(\mathbb{Q}(\varepsilon_n)/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*/\{\pm 1\}$.

P r o o f. The first assertion follows from more precise Lemma 2.1. As for the second assertion, notice that for any $m \in \mathbb{Z}$, the order $\mathbb{Z}[\alpha_n] = \mathbb{Z}[m + \alpha_n]$ is the ring of algebraic integers of $\mathbb{Q}(\alpha_n) = \mathbb{Q}(\zeta_n)^+$ by [7] or [14]. □

Lemma 2.1. *Set $\alpha_n = 2\cos(2\pi/n)$, $n > 4$ and $n \neq 6$. Then $\alpha_n \notin \mathbb{Q}$ and $m + \alpha_n$, $m \in \mathbb{Z}$, is an algebraic unit if and only if we have one of the following cases:*

(1) *$m = 0$ and n is not of the form $n = 4p^k$ for any prime power $p^k > 1$.*
(2) *$m = 1$ and n is not of the form $n = 3p^k$ for any prime power $p^k > 2$.*
(3) *$m = -1$ and n is not of the form $n = 6p^k$ for any prime power $p^k > 1$.*
(4) *$m = 2$ and n is not of the form $n = 2p^k$ for any prime power $p^k > 3$.*
(5) *$m = -2$ and n is not of the form $n = p^k$ for any prime power $p^k > 4$.*

P r o o f. Since $2\cos((k+1)t) = (2\cos t)(2\cos(kt)) - 2\cos((k-1)t)$, $k \geqslant 1$, we have $2\cos(kt) = P_k(2\cos t)$ for some monic polynomial $P_k(t) \in \mathbb{Z}[X]$ and the order $\mathbb{Z}[\alpha_n]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha_n)/\mathbb{Q})$-invariant.

Now, the algebraic integer $m + \alpha_n = m + \zeta_n + \zeta_n^{-1}$ is a unit if and only if the norm

$$0 \leqslant G_m(n) := N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(m + \zeta_n + \zeta_n^{-1}) = \prod_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} (m + \zeta_n^k + \zeta_n^{-k}) \in \mathbb{Z}$$

is equal to 1. Since $\zeta_n^k \neq \pm 1$ and $|m + \zeta_n^k + \zeta_n^{-k}| > |m| - 2$ for $\gcd(k,n) = 1$, we have $G_m(n) > 1$ for $|m| \geqslant 3$. It remains to look at the five cases $m \in \{0, 1, -1, 2, -2\}$. Recall that the cyclotomic polynomials satisfy

$$X^n - 1 = \prod_{d|n} \Phi_d(X) = (X-1) \prod_{1 \neq d|n} \Phi_d(X),$$

which implies $\Phi_n(X) \in \mathbb{Z}[X]$ for $n \geqslant 1$ and

$$X^n - 1 = (X^2 - 1) \prod_{1,2 \neq d|n} \Phi_d(X) \quad (n \text{ even}).$$

It follows that $n = \prod_{1 \neq d|n} \Phi_d(1)$ for $n > 1$, $1 = \prod_{1 \neq d|n} \Phi_d(-1)$ for $n > 1$ odd and $n/2 = \prod_{1,2 \neq d|n} \Phi_d(-1)$ if $n > 2$ is even. We deduce that

$$\Phi_n(1) = \begin{cases} 1 & \text{if } n > 1 \text{ is not of the form } n = p^k \text{ for any prime } p \geqslant 2, \\ p & \text{if } n > 1 \text{ is of the form } n = p^k \text{ for some prime } p \geqslant 2, \end{cases}$$

$$\Phi_n(-1) = 1 \text{ if } n > 1 \text{ is odd, } m = \prod_{1 \neq d|m} \Phi_{2d}(-1) \text{ if } n = 2m > 2 \text{ is even,}$$

$$\Phi_n(-1) = \begin{cases} 1 & \text{if } n > 2 \text{ is not of the form } n = 2p^k \text{ for any prime } p \geqslant 2, \\ p & \text{if } n > 2 \text{ is of the form } n = 2p^k \text{ for some prime } p \geqslant 2. \end{cases}$$

Case 1: $m = -2$. Since $-2 + \zeta_n + \zeta_n^{-1} = -(1 - \zeta_n)(1 - \zeta_n^{-1})$ we have $G_{-2}(n) = \Phi_n(1)^2$ and the case $m = -2$ follows.

Case 2: $m = 1$. If $3 \nmid n$, then $1 + \zeta_n + \zeta_n^{-1} = \zeta_n^{-1}(1 - \zeta_n^3)/(1 - \zeta_n)$ is the ratio of two conjugated elements of $\mathbb{Q}(\zeta_n)$. Therefore, $G_1(n) = 1$. Now, assume that $3 \mid n$. Then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n/3})] = \varphi(n)/\varphi(n/3) \in \{2, 3\}$ and

$$G_1(n) = \frac{N_{\mathbb{Q}(\zeta_{n/3})/\mathbb{Q}}(N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/3})}(1 - \zeta_{n/3}))}{N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1 - \zeta_n)} = \Phi_{n/3}(1)^{\varphi(n)/\varphi(n/3)}/\Phi_n(1).$$

The case $m = 1$ follows.

Case 3: $m = -1$. If n is odd, then $-1+\zeta_n+\zeta_n^{-1} = (1+\zeta_n^2+\zeta_n^{-2})/(1+\zeta_n+\zeta_n^{-1})$ is the ratio of two conjugated elements of $\mathbb{Q}(\zeta_n)$. Therefore $G_{-1}(n) = 1$. Now, assume that n is even. Then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{n/2})] = \varphi(n)/\varphi(n/2) \in \{1, 2\}$,

$$G_{-1}(n) = \frac{N_{\mathbb{Q}(\zeta_{n/2})/\mathbb{Q}}(N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n/2})}(1 + \zeta_{n/2} + \zeta_{n/2}^{-1}))}{N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1 + \zeta_n + \zeta_n^{-1})} = G_1(n/2)^{\varphi(n)/\varphi(n/2)}/G_1(n)$$

and the case $m = -1$ follows from the case $m = 1$, where we proved that for $n > 3$ we have $G_1(n) = p^2$ if $n = 3p^k$ with $p^k \geqslant 2$ and $G_1(n) = 1$ otherwise.

Case 4: $m = 0$. If n is odd then $\zeta_n(\zeta_n+\zeta_n^{-1}) = (1-\zeta_n^4)/(1-\zeta_n^2)$ is the ratio of two conjugated elements of $\mathbb{Q}(\zeta_n)$ and we have $G_0(n) = 1$. If $n = 2m > 2$ is even, then $\zeta_n(\zeta_n + \zeta_n^{-1}) = 1 + \zeta_{n/2}$ and hence $G_0(n) = \Phi_{n/2}(-1)^{\varphi(n)/\varphi(n/2)}$. The case $m = 0$ follows.

Case 5: $m = 2$. We have

$$2 + \zeta_n + \zeta_n^{-1} = (\zeta_{2n} + \zeta_{2n}^{-1})^2, \quad [\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}(\zeta_n)] = \varphi(2n)/\varphi(n) \in \{1, 2\},$$

and

$$G_2(n)^{\varphi(2n)/\varphi(n)} = N_{\mathbb{Q}(\zeta_{2n})/\mathbb{Q}}(\zeta_{2n} + \zeta_{2n}^{-1})^2 = G_0(2n)^4.$$

The case $m = 2$ follows. □

3. Multiplicatively independent units

We would like to thank Radan Kučera who in June 2018 commented our first version of the present proof of the following result:

Proposition 3.1. *Let ε be an algebraic unit of the degree $n \geqslant 3$. Assume that $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois. Let $\mu_\infty(\mathbb{Q}(\varepsilon))$ denote the finite group of complex roots of unity in $\mathbb{Q}(\varepsilon)$. Let r_ε denote the rank of the multiplicative group $\mathbb{U}_\varepsilon$ of units generated by $\mu_\infty(\mathbb{Q}(\varepsilon))$ and the n complex conjugates of ε.*

(1) *If n is an odd prime, then $\mu_\infty(\mathbb{Q}(\varepsilon)) = \{\pm 1\}$ and $r_\varepsilon = n - 1$.*

(2) *Assume that* $n = 4$ *and* $\mu_\infty(\mathbb{Q}(\varepsilon)) = \{\pm 1\}$. *Letting* $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Z}[X]$ *be the* $\mathbb{Q}$*-irreducible minimal polynomial of* ε *(with* $d \in \{\pm 1\}$*), then* $r_\varepsilon = n - 1 = 3$, *unless* $d = 1$ *and* $c = \delta a$ *for some* $\delta \in \{\pm 1\}$, *in which case* $r_\varepsilon = 2$ *if* $a \neq 0$ *and* $r_\varepsilon = 1$ *if* $a = 0$.

P r o o f. Set $\mathbb{K} = \mathbb{Q}(\varepsilon)$. Throughout the proof we assume that $\mu_\infty(\mathbb{K}) = \{\pm 1\}$, which is the case if $n \geqslant 3$ is prime. (The third point of Conjecture 4.2 shows that Proposition 3.1 may not hold true if $n = 4$ but $\mu_\infty(\mathbb{Q}(\varepsilon)) \neq \{\pm 1\}$.) Since $N_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = \pm 1$, the group $\mathbb{U}_\varepsilon$ is generated by -1 and any $n-1$ of the n conjugates of ε. Hence, $r_\varepsilon \leqslant n - 1$. Moreover, if $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is abelian, the group ring $\mathbb{Z}[G]$ acts on $\mathbb{U}_\varepsilon$ by $\Big(\sum\limits_{i=1}^{k} a_i g_i\Big) \cdot \eta = \prod\limits_{i=1}^{k} (g_i(\eta))^{a_i}$, where $g_1, \ldots, g_k \in G$, $a_1, \ldots, a_k \in \mathbb{Z}$ and $\eta \in \mathbb{U}_\varepsilon$.

(1) Assume that $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is cyclic of the order n. Let σ be a generator. Then, $r_\varepsilon < n-1$ if and only if $\{\varepsilon, \sigma(\varepsilon), \ldots, \sigma^{n-2}(\varepsilon)\}$ are multiplicatively dependent, hence if and only if $P(\sigma) \cdot \varepsilon \in \{\pm 1\}$ for some $0 \neq P(X) \in \mathbb{Z}[X]$ of the degree $\leqslant n-2$. Set $N(X) = 1 + X + \ldots + X^{n-1}$ and $D(X) = \gcd(N(X), P(X)) \in \mathbb{Z}[X]$. There exist $U(X), V(X) \in \mathbb{Z}[X]$ and $k \in \mathbb{Z}_{\geqslant 1}$ such that $U(X)N(X) + V(X)P(X) = kD(X)$ by Bézout's identity in $\mathbb{Q}[X]$. Since $N(\sigma) \cdot \varepsilon = N_{\mathbb{K}/\mathbb{Q}}(\varepsilon) \in \{\pm 1\}$, it follows that $D(\sigma) \cdot \varepsilon \in \{\pm 1\}$. Notice that $N(X) = \prod\limits_{1 \neq d \mid n} \Phi_d(X)$ in $\mathbb{Z}[X]$, a factorization into irreducible polynomials.

Therefore, $r_\varepsilon < n - 1$ if and only if there exist I with $\emptyset \subsetneq I \subsetneq \{d > 1 \colon d \mid n\}$ and $\delta \in \{\pm 1\}$ such that $D_I(\sigma) \cdot \varepsilon = \delta$, where $D_I(X) = \prod\limits_{d \in I} \Phi_d(X)$.

If n is prime, there does not exist such a nonempty proper subset I.

If $n = 4$, then (i) $I = \{2\}$ and $D_I(X) = \Phi_2(X) = X + 1$, or (ii) $I = \{4\}$ and $D_I(X) = \Phi_4(X) = X^2 + 1$. In case (i), $\sigma(\varepsilon) = \delta/\varepsilon$, hence $\sigma^2(\varepsilon) = \varepsilon$ and ε is a quadratic unit, a contradiction. In case (ii), $\sigma^2(\varepsilon) = \delta/\varepsilon$. Hence, $r_\varepsilon \leqslant 2$, $\sigma^3(\varepsilon) = \delta/\sigma(\varepsilon)$, $d = \prod\limits_{k=0}^{3} \sigma^k(\varepsilon) = +1$ and $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - \delta a X + 1$. If we had $r_\varepsilon = 1$, we would have $\sigma(\varepsilon)^k = \delta' \varepsilon^l$ for some $\delta' \in \{\pm 1\}$ and nonzero $k, l \in \mathbb{Z}$, which would give $(\delta/\varepsilon)^{k^2} = (\sigma^2(\varepsilon))^{k^2} = \sigma(\sigma(\varepsilon)^k)^k = \sigma(\delta' \varepsilon^l)^k = \delta'^k \sigma(\varepsilon^k)^l = \delta'^k (\delta' \varepsilon^l)^l$ and the contradiction $\varepsilon^{k^2 + l^2} \in \{\pm 1\}$.

(2) Assume that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \tau, \sigma\tau\}$ of order 4 is not cyclic and that $r_\varepsilon < 3$. Then ε, $\sigma(\varepsilon)$ and $\tau(\varepsilon)$ are multiplicatively dependent and $(u + v\sigma + w\tau) \cdot \varepsilon \in \{\pm 1\}$ for some $(0,0,0) \neq (u,v,w) \in \mathbb{Z}^3$. Set $S = u + v\sigma + w\tau$ and $N = \mathrm{Id} + \sigma + \tau + \sigma\tau$. We have $S \cdot \varepsilon \in \{\pm 1\}$ and $N \cdot \varepsilon = N_{\mathbb{K}/\mathbb{Q}}(\varepsilon) \in \{\pm 1\}$. Hence, $((\mathrm{Id} + \sigma)S - wN) \cdot \varepsilon = (u + v - w)(\mathrm{Id} + \sigma) \cdot \varepsilon$, $((\mathrm{Id} + \tau)S - vN) \cdot \varepsilon = (u - v + w)(\mathrm{Id} + \tau) \cdot \varepsilon$, and $((\sigma + \tau)S - uN) \cdot \varepsilon = (-u + v + w)(\mathrm{Id} + \sigma\tau) \cdot \varepsilon$ are in $\{\pm 1\}$. Since $u + v - w \neq 0$, or $u - v + w \neq 0$, or $-u + v + w \neq 0$, one of the conjugates $\sigma(\varepsilon)$, $\tau(\varepsilon)$ or $\sigma\tau(\varepsilon)$ of ε, say $\sigma(\varepsilon)$, is equal to δ/ε with $\delta \in \{\pm 1\}$. The other two conjugates being $\tau(\varepsilon)$ and $\tau\sigma(\varepsilon) = \tau(\delta/\varepsilon) = \delta/\tau(\varepsilon)$,

we have $r_\varepsilon \leqslant 2$, $d = (\varepsilon\delta/\varepsilon)\tau(\varepsilon)\delta/\tau(\varepsilon) = +1$ and $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - \delta aX + 1$. Now, assume that $r_\varepsilon = 1$. Take $f \in \mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$. Then $f(\varepsilon)^k = \delta'\varepsilon^l$ for some $\delta' \in \{\pm 1\}$ and nonzero $k, l \in \mathbb{Z}$. If $l = -k$, then $(f(\varepsilon)\varepsilon)^k \in \{\pm 1\}$. Hence, $f(\varepsilon) \in \{\pm 1/\varepsilon\}$. If $l \neq -k$, then $\varepsilon^k = f(f(\varepsilon)^k) = f(\delta'\varepsilon^l) = \delta' f(\varepsilon)^l$, using $f \circ f = \mathrm{Id}$. Hence,

$$\Big(\frac{f(\varepsilon)}{\varepsilon}\Big)^{k+l} = \frac{f(\varepsilon)^k}{\varepsilon^k}\frac{f(\varepsilon)^l}{\varepsilon^l} = \frac{\delta'\varepsilon^l}{\delta' f(\varepsilon)^l}\frac{f(\varepsilon)^l}{\varepsilon^l} = 1$$

and $f(\varepsilon) \in \{\pm\varepsilon\}$. Therefore, $\pm\varepsilon$ and $\pm 1/\varepsilon$ are the four conjugates of ε and $\Pi_\varepsilon(X) = X^4 + bX^2 + 1$. □

4. When is $\mathbb{Z}[\varepsilon]$ Galois invariant?

Let ε be an algebraic unit of the degree $n \geqslant 2$. Let $\Pi_\varepsilon(X) = X^n - a_{n-1}X^{n-1} + \ldots + (-1)^n a_0 \in \mathbb{Z}[X]$ of the discriminant $0 \neq D_\varepsilon \in \mathbb{Z}$ be its minimal polynomial. Assume that $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois. We consider the following problem: can the order $\mathbb{Z}[\varepsilon]$ be $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$-invariant? If $n = 2$ then $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois and $\mathbb{Z}[\varepsilon]$ is $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$-invariant. Hence, we assume that $n \geqslant 3$. Since $\mathbb{Z}[\varepsilon] = \mathbb{Z}[-\varepsilon] = \mathbb{Z}[1/\varepsilon] = \mathbb{Z}[-1/\varepsilon]$ and $D_\varepsilon = D_{-\varepsilon} = D_{1/\varepsilon} = D_{-1/\varepsilon}$, we may assume that $|a_{n-1}| \leqslant a_1$, in which case we say that ε and $\Pi_\varepsilon(X)$ are *reduced*.

4.1. The cyclic cubic case. In the cubic case, we know of a simple and useful necessary condition for the order $\mathbb{Z}[\varepsilon]$ to be Galois invariant and the problem is already solved:

Theorem 4.1 ([6], Theorem 2)**.** *Let α be a cubic algebraic integer α of the minimal polynomial $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ of the discriminant D_α. Assume that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, i.e. that $D_\alpha = \Delta_\alpha^2$ is a square. Then $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant if and only if Δ_α divides $3b - a^2$ and $3ac - b^2$.*

Conjecture 6.1 below is an analog of Theorem 4.1 for bicyclic biquadratic algebraic integers. Using Theorem 4.1 we have performed some numerical computation which makes the following Conjecture 4.1 very reasonable:

Conjecture 4.1. *Under the assumptions of Theorem* 4.1*, if $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant then $a + b$ and c are odd (notice that this necessary condition is invariant under the change $\alpha \mapsto \alpha + n$ with $n \in \mathbb{Z}$).*

Theorem 4.2 ([5], Theorem 1, Corollary 2, [6], Corollary 3)**.** *Let ε be a reduced cubic algebraic unit. Then $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ is Galois and $\mathbb{Z}[\varepsilon]$ is $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$-invariant if and only if one of the following cases takes place:*

(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* $D_\varepsilon = 7^2$ *and* $(\mathbb{Z}[\varepsilon]^\times : \mathbb{U}_\varepsilon) = 3$, 4, *and* 13, *respectively.*

(2) $\Pi_\varepsilon(X) = X^3 - 9X^2 + 6X - 1$, *in which case* $D_\varepsilon = 9^2$ *and* $(\mathbb{Z}[\varepsilon]^\times : \mathbb{U}_\varepsilon) = 4$.

(3) $\Pi_\varepsilon(X) = X^3 - aX^2 + (a-3)X + 1$, $a \geqslant 2$, *i.e.* $\mathbb{Q}(\varepsilon)$ *is the simplest cubic field, in which case* $D_\varepsilon = (a^2 - 3a + 9)^2$, $r_\varepsilon = 2$ *and the pair of conjugates* $\{\varepsilon,\ \varepsilon' = \varepsilon^2 - a\varepsilon + a - 2\}$ *is the system of fundamental units of the order* $\mathbb{Z}[\varepsilon]$ *by* [4], *Theorem* 1 *or* [13], *Theorem* 3.10.

4.2. The bicyclic biquadratic quartic case. (See [2], Chapter 13 and [3].) Let $\alpha_1 = \alpha, \alpha_2, \alpha_3, \alpha_4$ be the roots of a $\mathbb{Q}$-irreducible quartic polynomial $\Pi_\alpha(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Q}[X]$. Set $u_2 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $u_3 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, $u_4 = \alpha_1\alpha_4 + \alpha_2\alpha_3$ and let

$$R_\alpha(X) := (X - u_2)(X - u_3)(X - u_4) = X^3 - bX^2 + (ac - 4d)X - (a^2d - 4bd + c^2)$$

be its *cubic resolvent*. The extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois with the Galois group isomorphic to $C_2 \times C_2$ if and only if $R_\alpha(X)$ splits completely over $\mathbb{Q}$. In that case, $\beta_k = \alpha_1 + \alpha_k$ and $\beta'_k = \alpha_i + \alpha_j$ are the roots of $X^2 - aX + (b - u_k) \in \mathbb{Q}[X]$ for $k = 2, 3, 4$, where $\{1, k, i, j\} = \{1, 2, 3, 4\}$. Therefore, $\mathbb{Q}(\beta_k) = \mathbb{Q}(\sqrt{a^2 - 4b + 4u_k}) \subseteq \mathbb{Q}(\alpha)$ for $k = 2, 3, 4$. Finally, since $\beta_2 + \beta_3 + \beta_4 = 2\alpha + a$ we have $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{a^2 - 4b + 4u_2}, \sqrt{a^2 - 4b + 4u_3}, \sqrt{a^2 - 4b + 4u_4})$.

Lemma 4.1. *Let* α *be a quartic algebraic integer. If* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *is bicyclic biquadratic, then* $D_\alpha = \Delta_\alpha^2$ *is the square of an even integer* Δ_α.

P r o o f. Here $R_\alpha(X) \in \mathbb{Z}[X]$. Hence, $u_2, u_3, u_4 \in \mathbb{Z}$ and $D_\alpha = D_{\Pi_\alpha(X)} = D_{R_\alpha(X)} = \Delta_\alpha^2$, where $\Delta_\alpha = (u_2 - u_3)(u_3 - u_4)(u_4 - u_2) \in \mathbb{Z}$ is even (notice that $(u_2 - u_3) + (u_3 - u_4) + (u_4 - u_2) = 0$). □

Theorem 4.3. *For* $A \geqslant 2$, *consider the* $\mathbb{Q}$*-irreducible polynomial* $\Pi_\varepsilon(X) = X^4 - 2A^3X^3 + 5A^2X^2 - 4AX + 1 \in \mathbb{Z}[X]$ *of the discriminant* $D_\varepsilon = 16(A^4 - 4)^2$. *Set* $\eta = \varepsilon^3 - 2A^3\varepsilon^2 + 5A^2\varepsilon - 3A$ *with* $\Pi_\eta(X) = X^4 - A^2X^2 + 1$, $D_\eta = D_\varepsilon$ *and* $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\eta]$. *Then,* $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\sqrt{A^2 - 2}, \sqrt{A^2 + 2})$ *is totally real,* $r_\varepsilon = 3$ *and the four roots of* $\Pi_\varepsilon(X)$ *are* $\varepsilon = \eta^3 + A\eta^2$, $\varepsilon' = -\eta^3 + A\eta^2$, $\varepsilon'' = -A^2\eta^3 - A\eta^2 + (A^4 - 1)\eta + A^3$, *and* $\varepsilon''' = A^2\eta^3 - A\eta^2 - (A^4 - 1)\eta + A^3$. *Hence,* $\mathbb{Z}[\varepsilon]$ *is* $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$*-invariant. Moreover,* $\varepsilon\varepsilon' = \eta^2$ *and* $\{\varepsilon, \eta, \varepsilon''\}$ *is a system of fundamental units of the totally real quartic order* $\mathbb{Z}[\varepsilon]$ *for* $A > 2$.

P r o o f. Only the last assertion needs a proof. First, $\eta'_1 := \varepsilon\varepsilon' = -\eta^6 + A^2\eta^4 = \eta^2$, $\eta'_2 := \varepsilon\varepsilon''$ and $\eta'_3 := \varepsilon\varepsilon'''$ are roots of $X^2 - A^2X + 1$, $X^2 - 2(A^2 + 1)X + 1$ and

$X^2-2(A^2-1)X+1$, respectively. Hence, setting $d_1 = A^4-4$, $\eta_1 = \frac{1}{2}(A^2+\sqrt{A^4-4})$, $d_2 = A^2+2$, $\eta_2 = A^2+1+A\sqrt{A^2+2}$ and $d_3 = A^2-2$, $\eta_3 = A^2-1+A\sqrt{A^2-2}$, we have $\eta'_k \in \{\eta_k, \eta_k^{-1}\}$ for $1 \leqslant k \leqslant 3$. We claim that if $\xi \in \mathbb{Z}[\varepsilon]$ then $\xi\xi' \in \mathcal{O}_1 := \mathbb{Z}[\eta'_1]$, $\xi\xi'' \in \mathcal{O}_2 := \mathbb{Z}[\sqrt{d_2}]$ and $\xi\xi''' \in \mathcal{O}_3 := \mathbb{Z}[\sqrt{d_3}]$. Indeed, in the first case, it suffices to show that $\varepsilon^k\varepsilon'^l + \varepsilon^k\varepsilon'^l \in \mathbb{Z}[\eta'_1]$ for $k, l \geqslant 0$, hence that $s'_k := \varepsilon^k + \varepsilon'^k \in \mathbb{Z}[\eta'_1]$ for $k \geqslant 0$, which follows from $s'_1 = 2A\eta^2 = 2A\eta'_1$ and $s'_{k+1} = s'_1 s'_k - \varepsilon\varepsilon' s_{k-1} = s'_1 s'_k - \eta'_1 s_{k-1}$ for $k \geqslant 1$. In the second and third cases, $s''_1 = \varepsilon + \varepsilon''$ and $s'''_1 = \varepsilon + \varepsilon'''$, being roots of $X^2-2A^3X+3A^2-2$ and $X^2-2A^3X+3A^2+2$ of the discriminants $4(A^2-1)^2(A^2+2)$ and $4(A^2+1)^2(A^2-2)$, are in $\mathbb{Z}[\sqrt{d_2}]$ and $\mathbb{Z}[\sqrt{d_3}]$, respectively. Moreover, η_i is the fundamental unit of $\mathcal{O}_i$ for $1 \leqslant i \leqslant 3$. (Use continued fractions or look at the size of the coefficients of $\sqrt{d_i}$ of the powers of any $1 < \xi \in \mathbb{Z}[\eta_i]^\times$.) It follows that for $\xi \in \mathbb{V}_\varepsilon := \mathbb{Z}[\varepsilon]^\times$ we have $\xi^2 = \pm N_{\mathbb{Q}(\varepsilon)/\mathbb{Q}}(\xi)\xi^2 = \pm(\xi\xi')(\xi\xi'')(\xi\xi''') \in \langle -1, \eta_1, \eta_2, \eta_3\rangle$. Hence, $\mathbb{V}_\varepsilon^2 \subseteq \langle -1, \eta_1, \eta_2, \eta_3\rangle \subseteq \mathbb{V}_\varepsilon$. It remains to determine which of the units η_1, η_2, η_3, $\eta_1\eta_2$, $\eta_1\eta_3$, $\eta_2\eta_3$ they are and $\eta_1\eta_2\eta_3$ are squares in $\mathbb{Z}[\varepsilon]$. By [8], Corollary 3.2, items 2 and 3 for $A > 2$ we see that only η_1, $\eta_2\eta_3$ and hence $\eta_1\eta_2\eta_3$ are squares in $\mathbb{Q}(\varepsilon)$. In fact, there are squares in $\mathbb{Z}[\varepsilon]$, by noticing that $\eta'_1 = \eta^2$ and $\eta'_2\eta'_3 = (\varepsilon\varepsilon'')(\varepsilon\varepsilon''') = \varepsilon/\varepsilon' = (\varepsilon/\eta)^2$. Therefore, $\mathbb{V}_\varepsilon^2 \subseteq \langle -1, \eta_1, \eta_2, \eta_3\rangle = \langle -1, \eta'_1, \eta'_2, \eta'_3\rangle = \langle -1, \eta'_1, \eta'_2, \eta'_1\eta'_2\eta'_3\rangle = \langle -1, \eta^2, \eta'_2, \varepsilon^2\rangle$, where $\eta'_2 \in \{\eta_2, \eta_2^{-1}\}$ is not a square (we used $\eta'_1\eta'_2\eta'_3 = \varepsilon^2 N_{\mathbb{Q}(\varepsilon)/\mathbb{Q}}(\varepsilon) = \varepsilon^2$). Hence, $\mathbb{V}_\varepsilon = \langle -1, \eta, \eta'_2, \varepsilon\rangle = \langle -1, \eta, \varepsilon\varepsilon'', \varepsilon\rangle$ and the desired result follows. □

We used Lemma 4.1 to speed up our algorithm that checked Conjecture 4.2 up to the bound $H(\varepsilon) := \max(|a|, |b|, |c|, |d|) \leqslant 160$, where $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Z}[X]$, $d \in \{\pm 1\}$. The computation took 4 hours with Maple on a MacBook Air laptop computer. It gave 1291 reduced bicyclic biquadratic polynomials. Observe that $d = +1$ is positive in all cases in Conjecture 4.2. If proved to hold true beforehand, it would speed up our algorithm. Notice however that $\Pi_\alpha(X) = X^4 - 4X^3 + 2X^2 + 4X - 2$ with a negative constant coefficient is associated with a bicyclic biquadratic number field $\mathbb{Q}(\alpha)$ for which $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant. The occurrences $A = 2, 3, 4$ in this range made us come by with the family considered in Theorem 4.3.

Conjecture 4.2. *Let ε be a reduced quartic algebraic unit. Then $\mathbb{Q}(\varepsilon)$ is a bicyclic biquadratic number field and $\mathbb{Z}[\varepsilon]$ is $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$-invariant if and only if one of the following cases takes place:*

(1) $\Pi_\varepsilon(X) = X^4-4X^3+5X^2-2X+1$, *in which case* $D_\varepsilon = 144$, $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\sqrt{-1}, \sqrt{3})$ *and* $r_\varepsilon = 1$.

(2) $\Pi_\varepsilon(X) = X^4 + bX^2 + 1$, *where neither $-b-2$ nor $-b+2$ is a square, in which case* $D_\varepsilon = 16(b^2-4)^2$, $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\sqrt{-b-2}, \sqrt{-b+2})$ *and* $r_\varepsilon = 1$. *If $b \geqslant 3$, then ε is a fundamental unit of the totally imaginary quartic order $\mathbb{Z}[\varepsilon]$ (by* [9],

Theorem 18*). If* $b < -2$*, we know of a system of fundamental units of* $\mathbb{Z}[\varepsilon]$ *only for* $b = -A^2 < -4$ *by Theorem* 4.3.

(3) $\Pi_\varepsilon(X) = X^4 - 2A^3X^3 + 5A^2X^2 - 4AX + 1$ *for some* $A \geqslant 2$*, in which case* $D_\varepsilon = 16(A^4-4)^2$, $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\sqrt{A^2-2}, \sqrt{A^2+2})$, $r_\varepsilon = 3$*, and for* $A > 2$ *any* 3 *of the* 4 *conjugates of* ε *form a system of fundamental units of the totally real quartic order* $\mathbb{Z}[\varepsilon]$ *(see Theorem* 4.3*).*

4.3. The cyclic quartic case.

Conjecture 4.3. *Set* $\alpha_n = 2\cos(2\pi/n)$*, an algebraic integer. Let* $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\alpha_n)$ *denote the maximal real subfield of the cyclotomic number field* $\mathbb{Q}(\zeta_n)$*. Let* $\mathbb{Z}_\mathbb{K}$ *denote the ring of algebraic integers of a number field* $\mathbb{K}$*. Let* ε *be a reduced quartic algebraic unit. Then* $\mathbb{Q}(\varepsilon)$ *is a cyclic quartic number field and* $\mathbb{Z}[\varepsilon]$ *is* $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$*-invariant if and only if one of the following* 14 *cases takes place:*

(1) *In these two cases we have* $D_\varepsilon = 125$ *and* $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\zeta_5] = \mathbb{Z}_{\mathbb{Q}(\zeta_5)}$ *with* $\Pi_{\zeta_5}(X) = X^4 + X^3 + X^2 + X + 1$ *of discriminant* 125*.*
   (a) $\Pi_\varepsilon(X) = X^4 - X^3 + X^2 - X + 1 = \Pi_{-\zeta_5}(X)$.
   (b) $\Pi_\varepsilon(X) = X^4 - 3X^3 + 4X^2 - 2X + 1 = \Pi_{1+\zeta_5}(X)$.

(2) *In these four cases we have* $D_\varepsilon = 1125$ *and* $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\alpha_{15}] = \mathbb{Z}_{\mathbb{Q}(\zeta_{15})^+}$ *with* $\Pi_{\alpha_{15}}(X) = X^4 - X^3 - 4X^2 + 4X + 1$ *of discriminant* 1125*.*
   (a) $\Pi_\varepsilon(X) = X^4 - 3X^3 - X^2 + 3X + 1 = \Pi_{-\alpha_{15}+1}(X)$.
   (b) $\Pi_\varepsilon(X) = X^4 - 4X^3 - 4X^2 + X + 1 = \Pi_{-1/\alpha_{15}}(X) = \Pi_{(\alpha_{15}-1)/(-\alpha_{15}+2)}(X)$.
   (c) $\Pi_\varepsilon(X) = X^4 - 24X^3 + 26X^2 - 9X + 1 = \Pi_{1/(\alpha_{15}+2)}(X)$.
   (d) $\Pi_\varepsilon(X) = X^4 - 8X^3 + 14X^2 - 7X + 1 = \Pi_{1/(-\alpha_{15}+2)}(X) = \Pi_{(\alpha_{15}-1)/\alpha_{15}}(X)$.

(3) *In these three cases we have* $D_\varepsilon = 2000$ *and* $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\alpha_{20}] = \mathbb{Z}_{\mathbb{Q}(\zeta_{20})^+}$ *with* $\Pi_{\alpha_{20}}(X) = X^4 - 5X^2 + 5$ *of discriminant* 2000*.*
   (a) $\Pi_\varepsilon(X) = X^4 - 6X^3 + X^2 + 4X + 1 = \Pi_{-1/(\alpha_{20}+1)}(X) = \Pi_{1/(\alpha_{20}-1)}(X)$.
   (b) $\Pi_\varepsilon(X) = X^4 - 8X^3 - 11X^2 - 2X + 1 = \Pi_{(-\alpha_{20}+1)/(\alpha_{20}+2)}(X)$.
   (c) $\Pi_\varepsilon(X) = X^4 - 12X^3 + 19X^2 - 8X + 1 = \Pi_{1/(\alpha_{20}+2)}(X) = \Pi_{-1/(\alpha_{20}-2)}(X)$.

(4) *In these two cases we have* $D_\varepsilon = 2048$ *and* $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\alpha_{16}] = \mathbb{Z}_{\mathbb{Q}(\zeta_{16})^+}$ *with* $\Pi_{\alpha_{16}}(X) = X^4 - 4X^2 + 2$ *of discriminant* 2048*.*
   (a) $\Pi_\varepsilon(X) = X^4 - 4X^3 - 2X^2 + 4X - 1 = \Pi_{\alpha_{16}^2+\alpha_{16}-1}(X)$.
   (b) $\Pi_\varepsilon(X) = X^4 - 4X^3 + 2X^2 + 4X - 1 = \Pi_{\alpha_{16}+1}(X) = \Pi_{-\alpha_{16}+1}(X)$.

(5) $\Pi_\varepsilon(X) = X^4 - 7X^3 + 9X^2 + 7X + 1$ *and* $D_\varepsilon = 6125$.

(6) $\Pi_\varepsilon(X) = X^4 - 11X^3 + 31X^2 - 11X + 1$ *and* $D_\varepsilon = 15125$.

(7) $\Pi_\varepsilon(X) = X^4 - 9X^3 + 19X^2 - 9X + 1$ *and* $D_\varepsilon = 19773$.

We checked Conjecture 4.3 up to the bound $H(\varepsilon) := \max(|a|, |b|, |c|, |d|) \leqslant 150$ on the coefficients of $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Z}[X]$, $d \in \{\pm 1\}$. The

computation took 52660 seconds on a Mac mini desk computer. It gave 401 reduced cyclic quartic polynomials.

4.4. The Galois quintic case.

Conjecture 4.4. *Set $\alpha = \alpha_{11} = 2\cos(2\pi/11)$, of the minimal polynomial $\Pi_\alpha(X) = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$. Let ε be a reduced quintic algebraic unit. Then $\mathbb{Q}(\varepsilon)$ is a cyclic quintic number field and $\mathbb{Z}[\varepsilon]$ is $\mathrm{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$-invariant if and only if one of the following 8 cases takes place:*

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

In these eight cases we have $D_\varepsilon = 14641 = 11^4$ and $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\alpha] = \mathbb{Z}_{\mathbb{Q}(\zeta_{11})^+}$.

If $\mathbb{Q}(\varepsilon)$ is a cyclic quintic number field, then D_ε is a square (see Theorem 5.1). This has sped up our algorithm used to check Conjecture 4.4 up to the bound $H(\varepsilon) := \max(|a|, |b|, |c|, |d|, |e|) \leqslant 200$, where $\Pi_\varepsilon(X) = X^5 - aX^4 + bX^3 - cX^2 + dX - e \in \mathbb{Z}[X]$, $e \in \{\pm 1\}$. The computation took 132365 seconds on a Mac mini desk computer. It gave 174 reduced cyclic quintic polynomials.

5. Remarks on discriminants

Let $\sigma_k, \ldots, \sigma_n$ be complex imbeddings of a number field $\mathbb{K}$ of the degree n. If $\Omega = \{\omega_k;\ 1 \leqslant k \leqslant n\}$ is a $\mathbb{Z}$-basis of a free $\mathbb{Z}$-module $\mathbb{M}$ of the rank n of $\mathbb{K}$, the *discriminant* $D_\mathbb{M} \in \mathbb{Q} \setminus \{0\}$ of $\mathbb{M}$ is defined by $D_\mathbb{M} = D(\omega_1, \ldots, \omega_n)^2$, which does not depend on the $\mathbb{Z}$-basis Ω of $\mathbb{M}$, where

$$D(\omega_1, \ldots, \omega_n) := \det\left([\sigma_i(\omega_j)]_{1 \leqslant i,j \leqslant n}\right) \in \mathbb{C} \setminus \{0\} \tag{5.1}$$

(see e.g. [1], Chapter 4 or [10], Chapter II). The discriminant of the ring of the algebraic integers $\mathbb{Z}_\mathbb{K}$ of $\mathbb{K}$ is called the discriminant of $\mathbb{K}$ and denoted by $D_\mathbb{K}$. Notice (i) that the *determinant* $D(\omega_1, \ldots, \omega_n)$ defined in (5.1) is not necessarily a rational number and (ii) that its sign depends on the choices of the labelings of the σ's and of the ω's. Indeed, if $\tau \in \mathfrak{S}_n$ is any permutation of $\{1, \ldots, n\}$, then $D(\omega_{\tau(1)}, \ldots, \omega_{\tau(n)}) = \varepsilon(\tau) D(\omega_1, \ldots, \omega_n)$, where $\varepsilon(\tau) \in \{\pm 1\}$ is the signature of τ.

Let $G = \{g_1, \dots, g_n\}$ be a given indexing of the elements of a finite group of the order n. For $g \in G$ we define a permutation $\widetilde{g}$ of G by $gg_i = g_{\widetilde{g}(i)}$, $1 \leqslant i \leqslant n$. If $\{g_{\tau(1)}, \dots, g_{\tau(n)}\}$ is another indexing of the elements of G, where $\tau \in \mathfrak{S}_n$ is a permutation of $\{1, \dots, n\}$, then $gg_{\tau(i)} = g_{\widetilde{g}\tau(i)} = g_{\tau\tau^{-1}\widetilde{g}\tau(i)}$, $1 \leqslant i \leqslant n$. Since $\widetilde{g}$ and $\tau^{-1}\widetilde{g}\tau$ have the same signature, the signature $\varepsilon(\widetilde{g}) \in \{\pm 1\}$ of $\widetilde{g}$ does not depend on the choice of the indexing of the elements of G.

Now, if $\mathbb{K}/\mathbb{Q}$ is normal number field of the Galois group G, then for any $g \in G$ we have

$$g(D(\omega_1, \dots, \omega_n)) = \varepsilon(\widetilde{g})D(\omega_1, \dots, \omega_n). \tag{5.2}$$

Hence, $D(\omega_1, \dots, \omega_n) \in \mathbb{Z}$ if and only if $\varepsilon(\widetilde{g}) = +1$ for all $g \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

Theorem 5.1. *If G is a finite group, then $\varepsilon(\widetilde{g}) = +1$ for all $g \in G$ if and only if either G is of odd order or its 2-Sylow subgroups are not cyclic. Consequently, the discriminant of a normal number field is a square if and only if its degree is odd or the 2-Sylow subgroups of its Galois group are not cyclic.*

P r o o f. Let $\langle g\rangle = \{g^k \colon 0 \leqslant k \leqslant d-1\}$ be the cyclic subgroup generated by a given $g \in G$, which is of order d dividing the order n of G. Let

$$G = \bigcup_{1 \leqslant i \leqslant n/d} \langle g\rangle g_i = \{g_1, gg_1, \dots, g^{d-1}g_1, \dots, g_{n/d}, gg_{n/d}, \dots, g^{d-1}g_{n/d}\}$$

be a partition of G into n/d right cosets of $\langle g\rangle$. Clearly, $\widetilde{g}$ is a product of n/d cycles with disjoint supports ($\widetilde{g}$ permutes cyclically each block $g_k, gg_kg, \dots, g^{d-1}g_k$). Hence, $\varepsilon(\widetilde{g}) = \big((-1)^{d-1}\big)^{n/d} = (-1)^{n-n/d}$. It follows that $\varepsilon(\widetilde{g}) = +1$ if and only if $n = (n/d)d \equiv n/d \pmod 2$, hence if and only if either n is odd or n/d is even. The desired result follows.

Notice that since $g \mapsto \varepsilon(\widetilde{g})$ is a morphism, we readily recover that $\varepsilon(\widetilde{g}) = +1$ for all $g \in G$ whenever the order of G is odd. □

If $\mathbb{K}/\mathbb{Q}$ is not a normal number field, we have only a partial answer to the problem. Let $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$ be the Galois group of the normal closure $\mathbb{N}$ of $\mathbb{K}$. Set $H = \mathrm{Gal}(\mathbb{N}/\mathbb{K})$. Let g_i, $1 \leqslant i \leqslant n$, be n elements of G such that their restrictions to $\mathbb{K}$ are the n complex imbeddings σ_i, $1 \leqslant i \leqslant n$. Let $X = G/_gH$ be the set of n left cosets of H in G, i.e. $X = \{g_iH \colon 1 \leqslant i \leqslant n\}$. Then any $g \in G$ acts on X and gives rise to a permutation $\widetilde{g}$ of the elements in X. Since $g \mapsto \varepsilon(\widetilde{g})$ is a morphism, we obtain that $\varepsilon(\widetilde{g}) = +1$ for all $g \in G$ whenever the order of G is odd. Hence, we have:

Theorem 5.2. *If the degree of the normal closure of a number field $\mathbb{K}$ is odd, then the discriminant of $\mathbb{K}$ is a square.*

Remark 5.1. Lenstra wrote us on May 17, 2016 that the conclusion of Theorem 5.1 is certainly known, in fact he has known it since he was a student, but he was not sure that he ever saw an explicit reference. He also pointed out that we can rephrase Theorem 5.1 by saying that the image of the Cayley embedding of a finite group G in $\mathrm{Sym}(G)$ contains an odd permutation if and only if G has even order and contains an element of the order of the largest 2-power dividing $\#G$. It implies an interesting group-theoretic fact that the elements of odd order in a group with a cyclic Sylow-2 subgroup form a subgroup (obviously characteristic hence normal), see [11].

6. Necessary conditions for the order generated by an algebraic bicyclic biquadratic integer to be Galois invariant

Lemma 6.1. *Let α be a complex root of a $\mathbb{Q}$-irreducible quartic monic polynomial $\Pi_\alpha(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Z}[X]$ of the discriminant D_α. Assume that $\mathbb{Q}(\alpha)$ is a bicyclic biquadratic number field. Then $D_\alpha = \Delta_\alpha^2$ is the square of an even integer Δ_α. Moreover, if the quartic order $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant, then Δ_α divides $T := a^2d - c^2$ and $U := a^3 - 4ab + 8c$.*

P r o o f. For the first assertion, see Lemma 4.1 and Theorem 5.1. Set $\mathbb{K} = \mathbb{Q}(\alpha)$ and let $\sigma_1 = \mathrm{Id}$, $\sigma_2 = \sigma$, $\sigma_3 = \tau$ and $\sigma_4 = \sigma\tau$ be the four elements of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ with $\sigma^2 = \tau^2 = \mathrm{Id}$. If the ω_i's are in $\mathbb{K}$, it is easy to check that

$$D(\omega_1, \omega_2, \omega_3, \omega_4) = \det([\sigma_i(\omega_j)]_{1 \leqslant i,j \leqslant 4}) \in \mathbb{Q}(\alpha)$$

is $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$-invariant by (5.2), hence is in $\mathbb{Q}$ and in $\mathbb{Z}$ if the ω_i's are in $\mathbb{Z}_\mathbb{K}$. Therefore, the discriminant $D_\mathbb{M}$ of a submodule $\mathbb{M}$ of rank 4 of $\mathbb{Z}_\mathbb{K}$ is the square of an integer, say $D_\mathbb{M} = \Delta_\mathbb{M}^2$. In particular, $D_\alpha = \Delta_\alpha^2$ is a square and if $\mathbb{M} \subseteq \mathbb{Z}[\alpha]$, then $\Delta_\mathbb{M}^2 = D_\mathbb{M} = (\mathbb{Z}[\alpha] : \mathbb{M})^2 D_\alpha = (\mathbb{Z}[\alpha] : \mathbb{M})^2 \Delta_\alpha^2$ and Δ_α divides $\Delta_\mathbb{M}$. Now, assume that $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant. Taking $\omega_j = P_j(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, where $\alpha_k = \sigma_k(\alpha)$ and $P_j(X_1, X_2, X_3, X_4) \in \mathbb{Z}[X_1, X_2, X_3, X_4]$, we have $\mathbb{M} := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \mathbb{Z}\omega_3 + \mathbb{Z}\omega_4 \subseteq \mathbb{Z}[\alpha]$, hence D_α divides $D(\omega_1, \omega_2, \omega_3, \omega_4) = P(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ with

$$P(X_1, X_2, X_3, X_4) = \det \begin{pmatrix} L(X_1, X_2, X_3, X_4) \\ L(X_2, X_1, X_4, X_3) \\ L(X_3, X_4, X_1, X_2) \\ L(X_4, X_3, X_2, X_1) \end{pmatrix} \in \mathbb{Z}[X_1, X_2, X_3, X_4], \tag{6.1}$$

where the jth coefficient of the first line $L(X_1, X_2, X_3, X_4)$ of this square matrix is $P_j(X_1, X_2, X_3, X_4)$. The point is that if $P(X_1, X_2, X_3, X_4)$ is a symmetric polynomial, then $D(\omega_1, \omega_2, \omega_3, \omega_4)$ will be an explicit polynomial (with integral coefficients) in the coefficients a, b, c and d of $\Pi_\alpha(X)$.

Taking $L(X_1, X_2, X_3, X_4) = [1, X_1, X_1X_2, X_1X_2X_3]$, we obtain a symmetric polynomial $P(X_1, X_2, X_3, X_4) = -(X_1X_2 - X_3X_4)(X_1X_3 - X_2X_4)(X_1X_4 - X_2X_3) = \sigma_3^2 - \sigma_1^2\sigma_4$ and

$$D(1, \alpha, \alpha\sigma(\alpha), \alpha\sigma(\alpha)\tau(\alpha)) = c^2 - a^2d. \tag{6.2}$$

Taking $L(X_1, X_2, X_3, X_4) = [1, X_1, X_2, X_3]$, we obtain a symmetric polynomial $P(X_1, X_2, X_3, X_4) = -(X_1+X_2-X_3-X_4)(X_1-X_2+X_3-X_4)(X_1-X_2-X_3+X_4)$ $= -\sigma_1^3 + 4\sigma_1\sigma_2 - 8\sigma_3$ and

$$D(1, \alpha, \sigma(\alpha), \tau(\alpha)) = -a^3 + 4ab - 8c. \tag{6.3}$$

The desired result follows. □

Remark 6.1. Let $b \in \mathbb{Z}$, $D > 1$ be such that $b^2 - 4D^2$, $-b - 2D$ and $-b + 2D$ are not squares in $\mathbb{Z}$. Then $\Pi_\alpha(X) = X^4 + bX^2 + D^2$ is $\mathbb{Q}$-irreducible of the discriminant $D_\alpha = \Delta_\alpha^2$ being a square, where $\Delta_\alpha = 4D(b^2 - 4D^2)$, and $\mathbb{Q}(\varepsilon_b) = \mathbb{Q}(\sqrt{-b-2D}, \sqrt{-b+2D})$ is a bicyclic biquadratic field. Since $-D/\alpha = (\alpha^3 + b\alpha)/D$ is a root of $\Pi_\alpha(X)$, the order $\mathbb{Z}[\alpha]$ is not $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant. Since $T = U = 0$, the necessary condition in Lemma 6.1 is not sufficient. In the notation of Proposition 6.1, notice that Δ_α always divides $T = U = W = 0$ but does not divide $V + W = V - W = V = -4(b^2 - 4D^2)$.

Notice also that Lemma 6.1 and Proposition 6.1 could be used to improve the speed of the algorithm used to check Conjecture 4.2.

Since the necessary condition obtained in Lemma 6.1 is not sufficient, we prove a more stringent one (by the end of Remark 6.1):

Proposition 6.1. *Let α be a complex root of a $\mathbb{Q}$-irreducible quartic monic polynomial $\Pi_\alpha(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Z}[X]$ of the discriminant D_α. Assume that $\mathbb{Q}(\alpha)$ is a bicyclic biquadratic number field. Then $D_\alpha = \Delta_\alpha^2$ is the square of an even integer Δ_α. Moreover, if the quartic order $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant, then Δ_α divides $T := a^2d - c^2$, $U := a^3 - 4ab + 8c$, $V + W$ and $V - W$, where $V := a^2b + 2ac - 4b^2 + 16d$ and $W := a^2c + 8ad - 4bc$.*

Proof. Since $\mathbb{Z}[\alpha + n] = \mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant for any $n \in \mathbb{Z}$ by Lemma 6.1, we have that Δ_α divides $P(n) := a'^2d' - c'^2 = Un^3 + Vn^2 + Wn + T$ and $Q(n) := a'^3 - 4a'b' + 8c' = a^3 - 4ab + 8c = U$, where $\Pi_{\alpha+n}(X) = \Pi_\alpha(X - n)$ $= X^4 - a'X^3 + b'X^2 - c'X + d'$. Now, $P(X) = UX^3 + VX^2 + WX + T \in \mathbb{Z}[X]$ is such that some $\Delta \in \mathbb{Z}$ dividing T and U divides all the $P(n)$'s for $n \in \mathbb{Z}$, if and only if Δ divides all the numbers $Vn^2 + Wn = (V + W)\frac{1}{2}(n^2 + n) + (V - W)\frac{1}{2}(n^2 - n)$ for $n \in \mathbb{Z}$, which amounts to asking that Δ divides $V + W$ and $V - W$. □

In the range $H(\alpha) := \max(|a|, |b|, |c|, |d|) \leqslant 80$, where $\Pi_\alpha(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Z}[X]$, $a \geqslant 0$, we have found no example where this necessary condition is not sufficient. The computation took 31662 seconds on a MacBook Air laptop computer. It gave 7841 reduced bicyclic biquadratic polynomials. Now, 1413 out of them comply with the necessary condition in Lemma 6.1 and 293 out of them comply with the necessary condition in Proposition 6.1. Moreover, in these 293 cases we have found that $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant. So we might have hit upon a necessary and sufficient condition (similar to the one obtained in Theorem 4.1 for cyclic cubic algebraic integers) for the order generated by a bicyclic biquadratic algebraic integer to be Galois-invariant. In fact, we have checked that these 293 occurrences comply with the slightly simpler and stronger following equivalence:

Conjecture 6.1. *Let α be a complex root of a $\mathbb{Q}$-irreducible quartic monic polynomial $\Pi_\alpha(X) = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{Z}[X]$ of the discriminant D_α. Assume that $\mathbb{Q}(\alpha)$ is a bicyclic biquadratic number field. Then $D_\alpha = \Delta_\alpha^2$ is the square of an even integer Δ_α. Moreover, the quartic order $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant, if and only if Δ_α divides $T := a^2d - c^2$, $U := a^3 - 4ab + 8c$, $V := a^2b + 2ac - 4b^2 + 16d$ and $W := a^2c + 8ad - 4bc$.*

Question. Let the hypotheses and notation be as in Proposition 6.1. Assume that $\mathbb{Z}[\alpha]$ is $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$-invariant. By (6.2) and (6.3), both T and U are determinants of free $\mathbb{Z}$-submodules of rank 4 of $\mathbb{Z}[\alpha]$, which explains why Δ_α divides T and U. A nice way to prove that Δ_α also divides $V + W$ and $V - W$ would be to show that they are determinants of free $\mathbb{Z}$-submodules of rank 4 of $\mathbb{Z}[\alpha]$. In fact, a nice way to prove the necessity in Conjecture 6.1 would be to show that V and W are determinants of free $\mathbb{Z}$-submodules of rank 4 of $\mathbb{Z}[\alpha]$.

Acknowledgements. We would like to thank H. Lenstra and R. Kučera for their comments on some parts of this paper (see Proposition 3.1 and Remark 5.1).

References

[1] *H. Cohen*: A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics 138, Springer, Berlin, 1993. zbl MR doi

[2] *D. A. Cox*: Galois Theory. Pure and Applied Mathematics. A Wiley-Interscience Series of Texts, Monographs, and Tracts, John Wiley & Sons, Chichester, 2004. zbl MR doi

[3] *L.-C. Kappe, B. Warren*: An elementary test for the Galois group of a quartic polynomial. Am. Math. Mon. *96* (1989), 133–137. zbl MR doi

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

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

[6] *J. H. Lee, S. R. Louboutin*: Discriminants of cyclic cubic orders. J. Number Theory *168* (2016), 64–71. zbl MR doi
[7] *J. J. Liang*: On the integral basis of the maximal real subfield of a cyclotomic field. J. Reine Angew. Math. *286/287* (1976), 223–226. zbl MR doi
[8] *S. R. Louboutin*: Hasse unit indices of dihedral octic CM-fields. Math. Nachr. *215* (2000), 107–113. zbl MR doi
[9] *S. R. Louboutin*: Fundamental units for orders generated by a unit. Publ. Math. Besançon, Algèbre et Théorie des Nombres. Presses Universitaires de Franche-Comté, Besançon, 2015, pp. 41–68. zbl MR
[10] *W. Narkiewicz*: Elementary and Analytic Theory of Algebraic Numbers. Springer Monographs in Mathematics, Springer, Berlin; PWN-Polish Scientific Publishers, Warszawa, 1990. zbl MR doi
[11] *P. Stevenhagen*: Algebra I. Universiteit Leiden, Technische Universiteit Delft, Leiden, Delft, 2017. Available at `http://websites.math.leidenuniv.nl/algebra/algebra1.pdf`. (In Dutch.)
[12] *F. Thaine*: On the construction of families of cyclic polynomials whose roots are units. Exp. Math. *17* (2008), 315–331. zbl MR doi
[13] *E. Thomas*: Fundamental units for orders in certain cubic number fields. J. Reine Angew. Math. *310* (1979), 33–55. zbl MR doi
[14] *K. Yamagata, M. Yamagishi*: On the ring of integers of real cyclotomic fields. Proc. Japan Acad., Ser. A *92* (2016), 73–76. zbl MR doi

Author's address: Stéphane R. Louboutin, Aix Marseille Université, CNRS, Centrale Marseille, I2M, 39, rue Frédéric Joliot-Curie, 13453 Marseille Cedex 13, France, e-mail: `stephane.louboutin@univ-amu.fr`.