THE ADDITIVE UNIT STRUCTURE OF COMPLEX BI-QUADRATIC FIELDS

VOLKER ZIEGLER

Abstract. We determine which rings of the form $\mathbb{Z}[\alpha]$ are generated by there units, where α is a root of the polynomial $X^4 - BX^2 + D$ such that α and all its conjugates are complex.

1. Introduction

It seems that Zelinsky [11] was the first who investigated the additive unit structure of rings, i.e. Zelinsky proved, if V is a vector space over a division ring D, then every linear transformation can be written as the sum of two automorphisms unless $\dim V = 1$ and D is the field of two elements. Zelinsky's work gave rise to many investigations of rings that are generated by their units (see [9] for an overview). These investigations led Goldsmith, Pabst and Scott [4] to the following definition:

Definition 1. *Let R be a ring (with identity). An element r is called k-good if $r = e_1 + \cdots + e_k$, with $e_1, \ldots, e_k \in R^*$. If every element of R is k-good we call also the ring k-good.*

The unit sum number $u(R)$ is defined as $\min\{k \ : \ R \ \text{ is } \ k - \text{good}\}$. If the minimum does not exist but the units generate R additively we set $u(R) = \omega$. If the units do not generate R we set $u(R) = \infty$.

Although this topic has a history of more than 50 years, the interest in algebraic integers was marginal. In 1964 Jacobson [5] asked which quadratic fields have the property that every (algebraic) integer can be written as the sum of distinct units. The problem was solved by Śliwa [7]. The cubic and quartic case was considered by Belcher [2, 3]. Moreover, Belcher [2] characterized all quadratic fields whose rings of integers are generated by their units. About thirty years later Ashrafi and Vámos [1], Jarden and Narkiewicz [6] and Tichy and Ziegler [8] resumed this topic. In particular Ashrafi and Vámos showed that the ring of integers of quadratic fields, complex cubic fields and fields of the form $\mathbb{Q}(\zeta_{2^n})$, with ζ_{2^n} is a 2^n-th primitive root of unity, do not have finite unit sum number. This was generalized to all number fields by Jarden and Narkiewicz. Tichy and Ziegler characterized all purely cubic number fields whose ring of integers are generated by their units. Note that the case of quadratic fields has been rediscovered by Ashrafi and Vámos [1].

For the rest of the paper $f(X) = X^4 - BX^2 + D$ is irreducible and all its roots are complex, i.e. $4D > B^2$ or $-B, D > 0$. Let α be one of the roots of $f(X)$.

1991 *Mathematics Subject Classification.* 11R16,11R27,11A67.

Key words and phrases. biquadratic fields, unit sum number.

The author gratefully acknowledges support from the Austrian Science Fund (FWF) under project Nr. P18079-N12.

Then we investigate the additive unit structure of $\mathbb{Z}[\alpha]$. In particular we prove the following theorem.

Theorem 1. *$\mathbb{Z}[\alpha]$ is generated by its units if and only if $D = \pm 1$ or B, D fulfill one of the cases listed in table 1. In particular, if $\mathbb{Z}[\alpha]$ is generated by its units, then $D = \pm 1$ or $B^2 - 4D = -4, -3$.*

TABLE 1. List of unit bases for $\mathbb{Z}[\alpha]$, where $\rho = \frac{-1+\sqrt{-3}}{2}$ and $i = \sqrt{-1}$.

B	D	ϵ	Basis
$2n^2$	n^4+1	$n+\alpha$	$\{1, i, \epsilon, \epsilon i\}$
$-2n^2$	n^4+1	$n^3+\alpha+n\alpha^2$	$\{1, i, \epsilon, \epsilon i\}$
$2n^2+1$	n^4+n^2+1	$n+\alpha$	$\{1, \rho, \epsilon, \epsilon\rho\}$
$2n^2-1$	n^4-n^2+1	$n+\alpha$	$\{1, \rho, \epsilon, \epsilon\rho\}$
$-6n^2+1$	$9n^4-3n^2+1$	$(3n^3-2n)+2n^2\alpha+n\alpha^2+\alpha^3$	$\{1, \rho, \epsilon, \epsilon\rho\}$
$-6n^2-1$	$9n^4+3n^2+1$	$(3n^3+2n)+2n^2\alpha+n\alpha^2+\alpha^3$	$\{1, \rho, \epsilon, \epsilon\rho\}$
-3	3	$1+\alpha+\alpha^3$	$\{1, \rho, \epsilon, \epsilon\rho\}$

In table 1 we denote by n an arbitrary integer. The case $D = \pm 1$ can be excluded in our further investigations, since in this case α is a unit and $\mathbb{Z}[\alpha]$ is by trivial reasons generated by its units. Also the case $D = 0$ can be ignored, since otherwise $f(X)$ is reducible.

Before we start with the proof of the theorem, we have to determine the unit structure of the rings under consideration, in particular we have to determine, which roots of unity may appear (see section 2). The proof of Theorem 1 is divided into two cases. In the first case we assume that the "discriminant" $\Delta := B^2 - 4D$ is positive. In this case it turns out that the field $\mathbb{Q}(\alpha)$ is a CM-field, i.e. a totally complex field which is the quadratic extension of a totally real field. Since in CM-fields the unit structure is well known we will succeed in this case (see section 3). In section 4 we are concerned with the case of $\Delta < 0$. In this case we will see that the Diophantine equation $X^2 - \Delta Y^2 = \pm 4$ is closely related to our problem and leeds us to systems of equations, which are solved by using Groebner Basis. We discuss also some corollaries to Theorem 1 (see section 6).

In tables we assume that the signs must not be mixed, i.e. in one row we have to choose always the upper case sign or the lower case sign for all entries. In some tables, especially if we list units that generate rings of integers, mixed signs are allowed. Those tables are labeled with "mixed signs".

2. Roots of unity and unit bases

In this section we determine in which cases roots of unity appear. By ζ_n we denote a primitive n-th root of unity. Before we start to investigate the unit structure we have to determine the Galois group of the polynomial $X^4 - BX^2 + D$.

Lemma 1. *The polynomial $X^4 - BX^2 + D$ is reducible if and only if $B^2 - 4D$ is a square or $D = d^2$ and $B = b^2 - 2d$ for some integers b and d.*

Assume $X^4 - BX^2 + D$ is irreducible. The Galois group G corresponding to $X^4 - BX^2 + D$ is either $\mathbb{Z}_2 \times \mathbb{Z}_2$ if and only if D is a square in $\mathbb{Z}$, $\mathbb{Z}_4$ if and only if $D = \frac{B^2}{4+k^2}$ with D not a square in $\mathbb{Z}$ or D_4 otherwise. In the case D not a square, $M = \mathbb{Q}(\sqrt{B^2 - 4D})$ is the unique quadratic subfield of $\mathbb{Q}(\alpha)$.

Proof. First, we prove the irreducibility statement. If B^2-4D is a square it is obvious that X^4-BX^2+D is reducible. Therefore we assume B^2-4D is not a square. Assume X^4-BX^2+D is reducible. Since B^2-4D is not a square no root of X^4-BX^2+D is a rational. Therefore we have

$$X^4-BX^2+D=(X^2+b_1X+d_1)(X^2+b_2X+d_2),$$

with $b_1,b_2,d_1,d_2\in\mathbb{Z}$. By comparing coefficients we find $b_1=-b_2=b$. Note that $b\neq 0$ since otherwise X^2-BX+D is reducible which yields B^2-4D is a square. Moreover, we find $B=b^2-d_1-d_2$, $0=b_2d_1+b_1d_2$ and $D=d_1d_2$, i.e. $d_1=d_2=d$, $D=d^2$ and $B=b^2-2d$.

Next, we compute the Galois group. First we note that the only transitive subgroups of S_4 are $S_4,A_4,D_4,\mathbb{Z}_4$ and $\mathbb{Z}_2\times\mathbb{Z}_2$ up to conjugacy classes. Let $\alpha_1,\dots,\alpha_4$ be the roots of X^4-BX^2+D in a suitable order. Then we have

$$\alpha_1+\alpha_2=\alpha_3+\alpha_4=0 \tag{1}$$

and $\alpha_i+\alpha_j\neq 0$ for $i<j$ and $(i,j)\neq(1,2),(3,4)$. One sees at once that the cyclic permutation $(1,2,3)$ of the indices of α does not induce an automorphisms. Therefore $G=\mathrm{Gal}(\mathbb{Q}(\alpha),\mathbb{Q})$ is not S_4 nor A_4. Note that the only cyclic permutations of length 4, which leave (1) fixed, are $(1,3,2,4)$ and $(1,4,2,3)$. Note that in the case $\alpha_1\alpha_3=\sqrt{D}\in\mathbb{Z}$, the field $\mathbb{Q}(\alpha)$ is Galois and the Galois group can not be cyclic, since the only admissible cyclic permutations yield automorphisms with $\sqrt{D}\mapsto-\sqrt{D}$. Note that the Galois group $\mathbb{Z}_2\times\mathbb{Z}_2$ is exactly the transitive group such that (1) and $\alpha_1\alpha_3$ stays invariant. If $\sqrt{D}\in\mathbb{Q}(\alpha)\setminus\mathbb{Z}$ then $\mathbb{Q}(\alpha)$ is Galois and there exists an automorphism with $\sqrt{D}\mapsto-\sqrt{D}$, i.e. $G\neq\mathbb{Z}_2\times\mathbb{Z}_2$ and therefore $G=\mathbb{Z}_4$. In the case of $\sqrt{D}\notin\mathbb{Q}(\alpha)$ the field $\mathbb{Q}(\alpha)$ is not Galois and therefore has Galois group D_4.

If D is not a square in $\mathbb{Z}$ then $\mathbb{Q}(\alpha)$ has Galois group $\mathbb{Z}_4$ or D_4. It is an immediate consequence of Galois theory that fields with such Galois groups have a unique quadratic subfield. Since obviously $\mathbb{Q}(\sqrt{B^2-4D})$ is a quadratic subfield of $\mathbb{Q}(\alpha)$ it is unique. □

Let ζ_n be a primitive n-th root of unity. Then we prove:

Proposition 1. *The field $\mathbb{Q}(\alpha)$ may contain fourth and sixth roots of unity only in the following cases:*

- *If $B^2-4D=-4m^2$ with $m\in\mathbb{Z}$, then $\zeta_4=\frac{-B+2\alpha^2}{2m}$;*
- *If $B^2-4D=-3m^2$ with $m\in\mathbb{Z}$, then $\zeta_6=\frac{m-B+2\alpha^2}{2m}$;*
- *If $D=d^2$ and $B+2d=-m^2$, with $d,m\in\mathbb{Z}$, then $\zeta_4=\frac{-(B+d)\alpha+\alpha^3}{Bm}$ provided $B\neq 0$ and $\zeta_4=\frac{d\alpha-\alpha^3}{dm}$ otherwise;*
- *If $D=d^2$ and $B+2d=-3m^2$, with $d,m\in\mathbb{Z}$, then $\zeta_6=\frac{Bm-(B+d)\alpha+\alpha^3}{2Bm}$ provided $B\neq 0$ and $\zeta_6=\frac{dm+d\alpha-\alpha^3}{2dm}$ otherwise.*

Before we prove the proposition let us remark that the case $m=0$ is impossible, since otherwise we obtain in all cases $B^2-4D=0$. But this implies X^4-BX^2+D is reducible.

Proof. Let us assume D is not a perfect square and $\zeta_n\in\mathbb{Q}(\alpha)$ with $n=4,6$. Then the only quadratic subfield of $\mathbb{Q}(\alpha)$ is $\mathbb{Q}(\sqrt{B^2-4D})=\mathbb{Q}(\zeta_n)$. We consider the case $n=4$ first. Therefore we conclude $B^2-4D=-m'^2$ or equivalently $B^2+m'^2=4D$.

Assuming m' odd, we obtain $0 \equiv B^2 + m'^2 \equiv 1, 2 \mod 4$ which is a contradiction. Therefore $m' = 2m$ and we have $B^2 - 4D = -4m^2$. In the case of $n = 6$ we obtain $B^2 - 4D = -3m^2$ similarly.

Now let us assume $D = d^2$. Then there are 3 non-isomorphic quadratic subfields of $\mathbb{Q}(\alpha)$. These are beside $\mathbb{Q}(\sqrt{B^2 - 4D})$ the fields $\mathbb{Q}(\sqrt{B \pm 2d})$. If $\zeta_n \notin \mathbb{Q}(\sqrt{B^2 - 4D})$, then $\zeta_n \in \mathbb{Q}(\sqrt{B + 2d})$. Indeed, if $\zeta_n \notin \mathbb{Q}(\sqrt{B + 2d})$ then make the change $d \to -d$. The case $\zeta_n \in \mathbb{Q}(\sqrt{B^2 - 4D})$ has been treated above. Therefore we conclude $B + 2d = -m^2, -3m^2$ depending on n.

Now we have to compute the roots of unity. Let us note $\alpha = \pm\sqrt{\frac{B \pm \sqrt{B^2 - 4D}}{2}}$. Therefore we have $-B + 2\alpha^2 = \pm\sqrt{B^2 - 4D}$. If we substitute $B^2 - 4D = -4m^2$, $-3m^2$ respectively we obtain the first two cases. Note that $\pm\sqrt{-1}$ respectively $(1 \pm \sqrt{-3})/2$ is for either sign a fourth respectively sixth root of unity.

Now assume $D = d^2$ and $B + 2d = -m^2, -3m^2$. In this case we can write

$$\alpha = (e_1\sqrt{B + 2d} + e_2\sqrt{B - 2d})/2,$$

with $e_1, e_2 \in \{\pm 1\}$. By a simple computation we find

$$\alpha^3 = (e_1(B - d)\sqrt{B + 2d} + e_2(B + d)\sqrt{B - 2d})/2.$$

Therefore $\frac{-(B+d)\alpha + \alpha^3}{B} = e_1\sqrt{B + 2d}$ provided $B \neq 0$. Inserting $B + 2d = -m^2$, respectively $B+2d = -3m^2$ yields the third and fourth statement of the proposition. The case $B = 0$ can be proved similarly. □

If $\zeta_n \in \mathbb{Q}(\alpha)$ we have $\phi(n)|4$, i.e. $n = 1, 2, 3, 4, 5, 6, 8, 10, 12$. Since for n odd with $\zeta_{2n} = -\zeta_n$ it sufficies to consider the case n is even.

Proposition 2. *We have the following relations:*

$$\begin{aligned} \zeta_4 \in \mathbb{Z}[\alpha] &\iff B^2 - 4D = -4 \ \text{or} \ B = D = 1; \\ \zeta_6 \in \mathbb{Z}[\alpha] &\iff B^2 - 4D = -3; \\ \zeta_8 \in \mathbb{Z}[\alpha] &\iff B = 0, \ D = 1; \\ \zeta_{12} \in \mathbb{Z}[\alpha] &\iff B = D = 1. \end{aligned}$$

Moreover, $\zeta_1 0 \notin \mathbb{Z}[\alpha]$ *for any* α.

Proof. Assume $\zeta_4 \in \mathbb{Z}[\alpha]$. Because of Proposition 1 either $B^2 - 4D = -4m^2$, with $m = \pm 1$ or $B + 2d = -m^2$, where $Bm = \pm 1$. In the first case we obtain $B^2 - 4D = -4$ and in the second case we get $\pm 1 + 2d = -1$, i.e $B = -1$ and $d = 0$ or $B = 1$ and $d = 1$. This yields the first statement. Note that $d = 0$ yields $D = 0$ which has been excluded.

If $\zeta_6 \in \mathbb{Z}[\alpha]$, then we have $B^2 - 4D = -3m^2$ with $m = \pm 1$ or $B + 2d = -3m^2$ with $2Bm = \pm 1$. The first case yields $B^2 - 4D = -3$ and the second case is a contradiction.

In the case of $n = 8, 10, 12$ we have $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\alpha)$ and $\zeta_n \in \mathbb{Z}[\alpha]$ implies that $\mathbb{Z}[\alpha]$ is the maximal order. Computing discriminants we see that $\delta_{\mathbb{Z}[\alpha]} = 16(B^2 - 4D)^2 D$ and $\delta_n = 2^8, 5^3, 2^4 3^2$ for $n = 8, 10, 12$ where δ_n denotes the discriminant of $\mathbb{Q}(\zeta_n)$. Note if $\mathbb{Z}[\alpha]$ is the maximal order of $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_n)$ we have $\delta_{\mathbb{Z}[\alpha]} = \delta_n$. For $n = 8$ we deduce $(B^2 - 4D)^2 D = 16$ which yields $B = 0$ and $D = 1$, for $n = 10$ we have $16|5^3$, a contradiction, and for $n = 12$ we obtain $(B^2 - 4D)^2 D = 9$ which yields $B = D = 1$. □

Next we want to show, if the ring $\mathbb{Z}[\alpha]$ is generated by its units, then we already know a basis for $\mathbb{Z}[\alpha]$ consisting only of units. Let us prove following variation of [8, Lemma 1].

Lemma 2. *Let α be an algebraic integer of degree 4, totally complex, i.e all its conjugates are complex, and let $\zeta \in \mathbb{Z}[\alpha]$ be an n-th root of unity, with n maximal. Then the ring $\mathbb{Z}[\alpha]$ is generated by its units if and only if it is generated by $\{1, \zeta, \zeta^2, \dots, \zeta^{n-1}, \epsilon, \zeta\epsilon, \dots, \zeta^{n-1}\epsilon^3\}$, where ϵ is the fundamental unit of $\mathbb{Z}[\alpha]$.*

Proof. By Dirichlet's unit theorem we may assume $\mathbb{Z}[\alpha]$ is generated by

$$\{\zeta^{k_1}\epsilon^{l_1}, \zeta^{k_2}\epsilon^{l_2}, \zeta^{k_3}\epsilon^{l_3}, \zeta^{k_4}\epsilon^{l_4}\}.$$

Since ϵ is an algebraic integer of degree four, $\zeta^k\epsilon^l$ can be written as a linear combination of $\zeta^k, \zeta^k\epsilon, \zeta^k\epsilon^2, \zeta^k\epsilon^3$, which already proves the lemma. □

By Lemma 2 we can prove following propostion:

Proposition 3. *Let $|D| > 1$, and assume $\mathbb{Z}[\alpha]$ is generated by its units. Then there exists a unit $\epsilon \in \mathbb{Z}[\alpha]^*$ such that:*

- *The basis $\{1, \epsilon, \epsilon^2, \epsilon^3\}$ generates $\mathbb{Z}[\alpha]$ if $B^2 - 4D \neq -3, -4$;*
- *The basis $\{1, \zeta_6, \epsilon, \epsilon\zeta_6\}$ generates $\mathbb{Z}[\alpha]$ if $B^2 - 4D = -3$;*
- *The basis $\{1, \zeta_4, \epsilon, \epsilon\zeta_4\}$ generates $\mathbb{Z}[\alpha]$ if $B^2 - 4D = -4$.*

Moreover, in each case the basis, where ϵ is replaced by ϵ^{-1}, also generates $\mathbb{Z}[\alpha]$.

Proof. By Proposition 2 we know, if $|D| > 1$ roots of unity other than ± 1 occur in $\mathbb{Z}[\alpha]$ if and only if $B^2 - 4D = -3, -4$. Since $\mathbb{Q}(\alpha)$ is totally complex and of degree four we have by Dedekind's unit theorem, that in the case of $B^2 - 4D \neq -3, -4$ all units are of the form $\pm\epsilon^k$, where ϵ is a fundamental unit. Therefore the first case is proved.

Assume $B^2 - 4D = -4, -3$. By Lemma 2 we know that if $\mathbb{Z}[\alpha]$ is generated by its units then there exists a subset of $E = \{1, \zeta, \epsilon, \epsilon\zeta, \epsilon^2, \epsilon^2\zeta, \epsilon^3, \epsilon^3\zeta\}$ with four elements which is a basis for $\mathbb{Z}[\alpha]$. By ζ we denote ζ_4 respectively ζ_6 depending on $B^2 - 4D = -4, -3$. Indeed, since $\zeta_6^3 = \zeta_4^2 = -1$ and $\zeta_6^2 = \zeta_6 - 1$ we only have to consider subsets of E. A subset $\mathcal{B} = \{\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4\}$ is a basis of $\mathbb{Z}[\alpha]$ if and only if the Matrix M corresponding to the base change from $\mathcal{B}$ to $\{1, \alpha, \alpha^2, \alpha^3\}$ has determinant ± 1. Let us write $\epsilon = x + y\alpha + z\alpha^2 + w\alpha^3$. Moreover let $\epsilon_i = x_i + y_i\alpha + z_i\alpha^2 + w_i\alpha^3 \in E$, then $\mathbb{Z}[\alpha]$ has basis $\{\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4\}$ if and only if

$$\det M = \det \begin{pmatrix} x_1 & y_1 & z_1 & w_1 \\ x_2 & y_2 & z_2 & w_2 \\ x_3 & y_3 & z_3 & w_3 \\ x_4 & y_4 & z_4 & w_4 \end{pmatrix} = \pm 1.$$

If we compute for all 70 possible cases the determinant, we find that each determinant has the factor $Dw^2 + Bwy + y^2$. Therefore we have in any case $Dw^2 + Bwy + y^2 = \pm 1$. But the determinant corresponding to the basis $\{1, \zeta, \epsilon, \epsilon\zeta\}$ is exactly $Dw^2 + Bwy + y^2$. Therefore the case $B^2 - 4D = 3, 4$ is proved.

Now we prove the last statement of the proposition. Obviously a basis of $\mathbb{Z}[\alpha]$ remains a basis if each of its elements is multiplied by the same unit ϵ. Therefore we conclude, if $\{1, \epsilon, \epsilon^2, \epsilon^3\}$ is a basis then also $\{\epsilon^{-3}, \epsilon^{-2}, \epsilon^{-1}, 1\}$ (multiplication by ϵ^{-3}) is also a basis. Similar we find that with $\{1, \zeta, \epsilon, \epsilon\zeta\}$ also $\{\epsilon^{-1}, \epsilon^{-1}\zeta, 1, \zeta\}$ (multiplication by ϵ^{-1}) is a basis. □

3. The case $B^2 - 4D > 0$

This section is devoted to the case $B^2-4D>0$. In this case $\mathbb{Q}(\alpha)$ is a CM-field, i.e. a field that is a totally complex extension of a totally real number field. The following theorem yields a tool to prove Theorem 1 for this case (see [10, Theorem 4.12]).

Theorem 2. *Let K be a CM-field and let R be an order of K, E the unit group of R, K^+ the maximal real subfield of K, E^+ the unit group of $R \cap K^+$ and W the roots of unity lying in R. Then*

$$[E : WE^+] = 1, 2.$$

Proof. The proof of this theorem can be taken word by word from [10, Theorem 4.12]. Note that Washington proved this theorem in the case of R is the maximal order but this property is not needed for the proof. □

Because of Proposition 2 we know that $\mathbb{Z}[\alpha]$ contains no roots of unity other than ± 1. Let $\epsilon \in \mathbb{Z}[\alpha]^*$. Then we conclude by Theorem 2 that either ϵ or ϵ^2 is real. In the case of ϵ is real obviously $\mathbb{Z}[\alpha]$ is not generated by $1, \epsilon, \epsilon^2$ and ϵ^3. Therefore we assume that ϵ is not real but ϵ^2 is real. Let us write

$$\epsilon = x + y\alpha + z\alpha^2 + w\alpha^3.$$

We compute

$$\epsilon^2 = (x^2 - 2Dwy - Dz^2 - BDw^2) + 2(xy - Dwz)\alpha + ((Bw+y)^2 + Bz^2 + 2xz - Dw^2)\alpha^2 + 2(wx + Bwz + yz)\alpha^3.$$

Since α and α^3 are purely imaginary and linear independent we conclude

$$xy = Dwz, \qquad wx + Bwz + yz = 0. \tag{2}$$

Multiplying the second equation by y yields $z(Dw^2 + Bwy + y^2) = 0$. Since $Dw^2 + Bwy + y^2 = 0$ implies $\mathbb{Q}(\alpha)$ is not quartic, we deduce $z = 0$, hence $wx = xy = 0$. Therefore either $x = 0$ or $w = y = 0$. In the case of $x = 0$, we deduce that α is a unit, hence $D = \pm 1$. In the case of $w = y = 0$ we get $\epsilon = x = \pm 1$. But obviously ± 1 does not generate $\mathbb{Z}[\alpha]$.

4. The case of $B^2 - 4D < -4$

Because of Proposition 3 (see also [8, Lemma 1]) we may assume $\{1, \epsilon, \epsilon^2, \epsilon^3\}$ generates $\mathbb{Z}[\alpha]$. Let the notations be as above and write

$$\epsilon^2 = x_2 + y_2\alpha + z_2\alpha^2 + w_2\alpha^3,$$
$$\epsilon^3 = x_3 + y_3\alpha + z_3\alpha^2 + w_3\alpha^3,$$

with

$$x_2 = -BDw^2 + x^2 - 2Dwy - Dz^2, \qquad y_2 = 2xy - 2Dwz,$$
$$z_2 = B^2w^2 - Dw^2 + 2Bwy + y^2 + 2xz + Bz^2, \qquad w_2 = 2wx + 2Bwz + 2yz$$

and

$$\begin{aligned} x_3 =& x(x^2-3Dw(Bw+2y))-3Dz(w^2(B^2-D)+2Bwy+y^2)\\ &-3Dxz^2-BDz^3,\\ y_3 =& D^2w^3-B^2Dw^3+3x^2y-3BDw(wy+z^2)\\ &-3D(wy^2+2wxz+yz^2),\\ z_3 =& 3x(w^2(B^2-D)+2Bwy+y^2)+3z(x^2+(Bw+y)(B^2w-2Dw+By))\\ &+3Bxz^2+z^3(B^2-D),\\ w_3 =& B^3w^3-2BDw^3+3wx^2+3B^2w^2y-3Dw^2y+3Bwy^2+y^3\\ &+6xz(Bw+y)+3z^2(B^2w-Dw+By)z. \end{aligned}$$

Then $\{1,\epsilon,\epsilon^2,\epsilon^3\}$ generates $\mathbb{Z}[\alpha]$ if and only if

$$\det M = \det \begin{pmatrix} 1 & 0 & 0 & 0\\ x & y & z & w\\ x_2 & y_2 & z_2 & w_2\\ x_3 & y_3 & z_3 & w_3 \end{pmatrix} = \pm 1$$

(see [8] or proof of Proposition 3). A computation shows

$$\begin{aligned} \det M =& \left(\left(y+B\frac{w}{2}\right)^2-\frac{\Delta}{4}w^2\right)\times\\ &(((B^2-D)w^2+2Bwy+y^2)^2+(B^2-4D)z^4\\ &-2(B(B^2-3D)w^2+2(B^2-2D)wy+By^2)z^2), \end{aligned} \tag{3}$$

i.e. $(2y+Bw)^2-\Delta w^2=\pm 4$. Since $\Delta = B^2-4D < -4$, we conclude $w=0$ and $y=\pm 1$. But with $\{1,\epsilon,\epsilon^2,\epsilon^3\}$ also $\{1,\epsilon^{-1},\epsilon^{-2},\epsilon^{-3}\}$ generates $\mathbb{Z}[\alpha]$. Because of $w=0, y=\pm 1$ and ϵ a unit we obtain

$$\epsilon^{-1} = x_{-1}+y_{-1}\alpha+z_{-1}\alpha^2+w_{-1}\alpha^3,$$

with $w_{-1}=0$ and $y_{-1}=\pm 1$. On the other hand we have

$$x_{-1} = -Bx+x^3-Dz+2Bx^2z+(B^2+D)xz^2+BDz^3,$$
$$y_{-1} = \pm(B-x^2-2Bxz-B^2z^2+Dz^2), \qquad z_{-1} = x-x^2z-Bxz^2-Dz^3,$$
$$w_{-1} = \pm(Bz^2+2xz-1).$$

Since we have $w_{-1}=0$, we find $1=z(Bz+2x)$, which yields $z=e=\pm 1$ and $x=e(1-B)/2$. Furthermore, we obtain $y_{-1}=\frac{(B-1)^2-4D}{4}=\pm 1$. Therefore $B=1\pm 2\sqrt{\pm 1+D}$. We can write $B=1+e_1 2n$ and $D=n^2+e_2$ with $n\in\mathbb{Z}$ and $e_1,e_2\in\{\pm 1\}$. Therefore we conclude $\epsilon=\pm(n+\alpha^2)\pm\alpha$ with mixed signs. But a short computation shows that $|\det M| = 4 \neq 1$, a contradiction.

5. The cases $B^2-4D=-3,-4$

We start with the case $B^2-4D=-4$. Obviously B has to be even and we write $B=2b$ and $D=b^2+1$. By the proof of Proposition 3 we know that we have to investigate the equation $Dw^2+Bwy+y^2=\pm 1$, i.e. we have

$$(y+bw)^2+w^2=1. \tag{4}$$

Therefore we conclude $w=0, y=\pm 1$ or $w=1, y=-b$ or $w=-1, y=b$. By Proposition 3 also the coefficients of ϵ^{-1} have to satisfy an analogous relation. Let us write $\epsilon^{-1}=x_{-1}+y_{-1}\alpha+z_{-1}\alpha^2+w_{-1}\alpha^3$. The formulas for y_{-1} and w_{-1} are computed in table 2.

Hence we obtain 16 systems of equations. For each system we compute a Groebner basis (see table 3) with respect to the lexicographic term order induced by $x \succ z \succ b$.

TABLE 2. The values of y_{-1} and w_{-1} in the case of $B^2-4D=-4$.

y	w	y_{-1} and w_{-1}
1	0	$y_{-1}=-x^2+z^2-3b^2z^2+b(2-4xz)$ $w_{-1}=-1+2xz+2bz^2$
-1	0	$y_{-1}=x^2-z^2+3b^2z^2-b(2-4xz)$ $w_{-1}=1-2xz-2bz^2$
$-b$	1	$y_{-1}=-1-2xz+b^3z^2+b^2(1+2xz)+b(x^2-3z^2)$ $w_{-1}=-b-x^2-2bxz+z^2-b^2z^2$
b	-1	$y_{-1}=1+2xz-b^3z^2-b^2(1+2xz)-b(x^2-3z^2)$ $w_{-1}=b+x^2+2bxz-z^2+b^2z^2$

TABLE 3. The Groebner bases.

y	w	y_{-1}	w_{-1}	Groebner basis
± 1	0	± 1	0	$1+4z^2-4bz^2-4z^4, x+2z-bz-2z^3$
± 1	0	∓ 1	0	$1-4z^2-4bz^2-4z^4, x-2z-bz-2z^3$
$\pm b$	∓ 1	$\pm b$	∓ 1	$1+4z^2+4bz^2-4z^4, x+2z+bz-2z^3$
$\pm b$	∓ 1	$\mp b$	± 1	$1+4z^2-4bz^2+4z^4, x+2z-bz+2z^3$
± 1	0	$\pm b$	∓ 1	$bz+z^3, xz+bz^2, b-x^2+z^2+b^2z^2$
$\pm b$	∓ 1	± 1	0	$bz-z^3, xz+bz^2, b+x^2-z^2-b^2z^2$
± 1	0	$\mp b$	± 1	$1-bz^2-z^4, x-z^3$
$\pm b$	∓ 1	∓ 1	0	$1+bz^2-z^4, x+z^3$

The first four Groebner bases do not yield solutions since otherwise we would obtain $4|1$. The last two Groebner bases yield $b=\pm(z^2-1/z^2)$, hence $z^2=1$ and therefore $b=0$ and $D=-1$ which yields a trivial case. The fifth (sixth) Groebner basis yields either $z=0$ and $b=x^2$ ($z=0$ and $b=-x^2$) or $z\neq 0$ and $b=-z^2$, $x=z^3$ ($z\neq 0$ and $b=z^2$, $x=-z^3$). Let us put $x=n$ in the case of $z=0$ and $z=n$ in the other case, where $n\in\mathbb{Z}$ arbitrary. These two cases yield all possible ϵ for which $\mathbb{Z}[\alpha]$ is generated by $\{1,\zeta_4,\epsilon,\epsilon\zeta_4\}$. These ϵ are listed in table 4. It is easy to check that in each case ϵ is a unit (one has just to compute the norm $\mathrm{N}_{K/\mathbb{Q}}(\epsilon)$ for each possible ϵ).

Now we consider the case $B^2-4D=-3$. In this case B has to be odd and therefore we write $B=2b-1$ and $D=b^2-b+1$. By Proposition 3 we have to investigate the equation $\det M=(y+wB/2)^2+3w^2/4=\pm 1$ or equivalently

$$(2y+2wb-w)^2+3w^2=\pm 4. \tag{5}$$

Equation (5) has exactly 6 solutions namely $(y,w)=(\pm 1,0),(\pm b,\mp 1),(\pm(1-b),\pm 1)$. As in the case of $B^2-4D=-4$ we know that the coefficients of ϵ^{-1}

TABLE 4. Units ϵ such that $\{1,\zeta_4,\epsilon,\epsilon\zeta_4\}$ generates $\mathbb{Z}[\alpha]$. (mixed signs)

B	D	ϵ
$2n^2$	n^4+1	$\pm n\pm\alpha$ $\pm(n^3+n\alpha^2)\pm(n^2\alpha-\alpha^3)$
$-2n^2$	n^4+1	$\pm n\pm(n^2\alpha+\alpha^3)$ $\pm(n^3+n\alpha^2)\pm\alpha$

also have to satisfy relation (5), i.e. $(2y_{-1}+2w_{-1}b-w_{-1})^2+3w_{-1}^2=\pm4$. In order to find more relations we compute y_{-1} and w_{-1} (see table 5).

TABLE 5. The values of y_{-1} and w_{-1} in the case of $B^2-4D=-3$.

y	w	y_{-1} and w_{-1}
1	0	$y_{-1}=-1+2b-x^2+2xz-4bxz+3bz^2-3b^2z^2$ $w_{-1}=-1+2xz+(2b-1)z^2$
-1	0	$y_{-1}=1-2b+x^2-2xz+4bxz-3bz^2+3b^2z^2$ $w_{-1}=1-2xz-(2b-1)z^2$
$-b$	1	$y_{-1}=b(b-2+x^2)+2(b^2-1)xz+(1-3b+b^3)z^2$ $w_{-1}=1-b-x^2-2bxz+z^2-b^2z^2$
$1-b$	1	$y_{-1}=(b-1)(1+b+x^2)+2(b-2)bxz+(b^3-3b^2+1)z^2$ $w_{-1}=x(2z-x)-b(1+2xz+(b-2)z^2)$
b	-1	$y_{-1}=b(2-b-x^2)-2(b^2-1)xz-(1-3b+b^3)z^2$ $w_{-1}=x^2+b-1+2bxz-z^2+b^2z^2$
$b-1$	-1	$y_{-1}=(1-b)(1+b+x^2)-2(b-2)bxz-(b^3-3b^2+1)z^2$ $x(x-2z)+b(1+2xz+(b-2)z^2)$

Similar as in the case of $B^2-4D=-4$ we find 36 systems of equations. We compute for each system a Groebner basis with respect to the lexicographic term order $x\succ z\succ b$. The first element of each Groebner basis is given in table 6.

Let us investigate the case $z=0$. In this case the first elements of the Groebner bases, get polynomials in b. Only in the cases $y=\pm1, w=0, y_{-1}=\pm b, w_{-1}=\mp1$ and $y=\pm1, w=0, y_{-1}=\pm(b-1), w_{-1}=\mp1$ the considered element vanishes unconditionally. In these cases the corresponding systems turn into

$$\pm(-1+2b-x^2)=\pm(b-1),\qquad \mp1=\mp1, \tag{6}$$

$$\pm(-1+2b-x^2)=\pm b,\qquad \mp1=\mp1. \tag{7}$$

System (6) yields $b=x^2$ and (7) yields $b=x^2+1$. Let $x=n$ then we obtain $B=2n^2-1$, $D=n^4+n^2+1$ and $\epsilon=\pm n\pm\alpha$ respectively $B=2n^2+1$, $D=n^4-n^2+1$ and $\epsilon=\pm n\pm\alpha$ with mixed signs. By computing norms we see that these ϵ's are indeed units. See also table 1.

In all other cases we deduce $b=-1,0,1$ or 2. The case $b=0,1$ implies $D=-1$. Inserting $z=0, b=1$ respectively $z=0$, $b=2$ into table 5 yields the equations $1=0$, $x^2\pm1=0$ and $x^2\pm2=0$. Note that the equation $x^2-1=0$ appears only for $b=-1$,$y=\pm b, w=\mp1, y_{-1}=\pm(b-1)$, $w_{-1}=\mp1$, i.e. $-B=D=3$. Therefore we have $\epsilon=\pm1\pm(\alpha+\alpha^3)$ with mixed signs. Indeed this ϵ is a unit.

TABLE 6. The first element of the Groebner bases.

y	w	y_{-1}	w_{-1}	first element of the Groebner basis
±1	0	±1	0	$1+6z^2-4bz^2-3z^4$
±1	0	∓1	0	$1-2z^2-4bz^2-3z^4$
±1	0	$\pm(1-b)$	±1	$4+4z^2-4bz^2-3z^4$
±1	0	$\mp b$	±1	$4-4bz^2-3z^4$
±1	0	$\pm b$	∓1	$4z-4bz-3z^3$
±1	0	$\pm(b-1)$	∓1	$4bz+3z^3$
$\pm b$	∓1	±1	0	$1-2b+b^2-2z^2+2bz^2-3z^4$
$\pm b$	∓1	∓1	0	$1+2b+b^2-6z^2+2bz^2-3z^4$
$\pm b$	∓1	$\pm(1-b)$	±1	$1-2b+b^2-6z^2+2bz^2-3z^4$
$\pm b$	∓1	$\mp b$	±1	$b^2-8z^2+2bz^2-3z^4$
$\pm b$	∓1	$\pm b$	∓1	$b^2+2bz^2-3z^4$
$\pm b$	∓1	$\pm(b-1)$	∓1	$1+2b+b^2-2z^2+2bz^2-3z^4$
$\pm(b-1)$	∓1	±1	0	$b^2+2bz^2-3z^4$
$\pm(b-1)$	∓1	∓1	0	$4-4b+b^2+4z^2+2bz^2-3z^4$
$\pm(b-1)$	∓1	$\pm(1-b)$	±1	$1-2b+b^2-2z^2+2bz^2-3z^4$
$\pm(b-1)$	∓1	$\mp b$	±1	$4-4b+b^2+2bz^2-3z^4$
$\pm(b-1)$	∓1	$\pm b$	∓1	$b^2+4z^2+2bz^2-3z^4$
$\pm(b-1)$	∓1	$\pm(b-1)$	∓1	$1-2b+b^2+6z^2+2bz^2-3z^4$

Now we may assume $z \neq 0$. In each case we compute the zeros of the first element of the Groebner bases (see table 6) considered as a polynomial in b. The solutions can be found in table 7.

TABLE 7. Expressions for b.

y	w	y_{-1}	w_{-1}	b
±1	0	±1	0	$\frac{1}{4}\left(6+\frac{1}{z^2}-3z^2\right)$
±1	0	∓1	0	$\frac{1}{4}\left(-2+\frac{1}{z^2}-3z^2\right)$
±1	0	$\pm(1-b)$	±1	$1+\frac{1}{z^2}-\frac{3z^2}{4}$
±1	0	$\mp b$	±1	$\frac{1}{z^2}-\frac{3z^2}{4}$
±1	0	$\pm b$	∓1	$1-\frac{3z^2}{4}$
±1	0	$\pm(b-1)$	∓1	$-\frac{3z^2}{4}$
$\pm b$	∓1	±1	0	$1-3z^2, 1+z^2$
$\pm b$	∓1	∓1	0	$-1-z^2\pm2z\sqrt{z^2+2}$
$\pm b$	∓1	$\pm(1-b)$	±1	$1-z^2\pm2z\sqrt{z^2+1}$
$\pm b$	∓1	$\mp b$	±1	$-z^2\pm2z\sqrt{z^2+2}$
$\pm b$	∓1	$\pm b$	∓1	$-3z^2, z^2$
$\pm b$	∓1	$\pm(b-1)$	∓1	$-1-z^2\pm2z\sqrt{z^2+1}$
$\pm(b-1)$	∓1	±1	0	$-3z^2, z^2$
$\pm(b-1)$	∓1	∓1	0	$2-z^2\pm2z\sqrt{z^2-2}$
$\pm(b-1)$	∓1	$\pm(1-b)$	±1	$1-3z^2, 1+z^2$
$\pm(b-1)$	∓1	$\mp b$	±1	$2-z^2\pm2z\sqrt{z^2-1}$
$\pm(b-1)$	∓1	$\pm b$	∓1	$-z^2\pm2z\sqrt{z^2-1}$
$\pm(b-1)$	∓1	$\pm(b-1)$	∓1	$1-z^2\pm2z\sqrt{z^2-2}$

Table 7 shows that we have 18 different subcases. The first two cases yield $z^2 = 1$ since otherwise b would be not an integer. Therefore we obtain $b = 1$ and $b = -1$. But $b = 1$ yields $D = 1$ and we ignore this case. In the case of $b = -1$ the corresponding system turns into $(x - 3e_1)^2 = 1$ and $2xe_1 = 4$, where $z = e_1$ with $e_1 \in \{\pm 1\}$. Therefore we find $x = 2e_1$. We can easily check that the corresponding ϵ is indeed a unit. Note that $b = -1$ yields $B = -3$ and $D = 3$.

The cases 3 and 4 yield for integral z no integral b, hence we find for these two cases no solution.

Now let us consider the cases $5, 6, 7, 11, 13$ and 15. In the cases $7, 11, 13$ and 15 we see that for any integral z we obtain an integral b. Therefore we let $z = n$ where $n \in \mathbb{Z}$ is arbitrary. In the cases 5 and 6 we find that for every even z we have an integral b. Therefore we put $z = 2n$ with $n \in \mathbb{Z}$. Inserting these results into the equations given by table 5 we obtain systems of equations in x and n. Solving for x we find in each case an integral solution for x. Moreover, these solutions yield indeed units ϵ. We list these solutions in table 8.

Now we consider the remaining cases. In each expression for b we find the term $2z\sqrt{z^2 - k}$, with $k = 2, 1, -1$. Since we assume $z \neq 0$ the only possibility for b to be an integer is $k = -1$ and $z^2 = 1$. This corresponds to the cases 16 and 17. We obtain $b = 1$ (case 16) respectively $b = -1$ (case 17). Since $b = 1$ yields $D = 1$ we ignore this case. The other case yields $B = -3$, $D = 3$, $z = e_1$, $y = (1 - b)e_2 = 2e_2$ and $w = e_2$, where $e_1, e_2 \in \{\pm 1\}$. Using table 5 we find the system $(x - 3/2e_1)^2 = 1/4$, $(x - 2e_1)^2 = 1$, which yields $x = e_1$. Again the corresponding ϵ is a unit.

Table 8. Solutions for ϵ. (mixed signs)

B	D	ϵ
$2n^2+1$	n^4+n^2+1	$\pm n \pm \alpha$ $\pm\left(n^3+n-n\alpha^2\right) \pm \left((n^2+1)\alpha - \alpha^3\right)$ $\pm\left(\lvert n\rvert^3 - \lvert n\rvert\alpha^2\right) \pm \left(n^2\alpha - \alpha^3\right)$
$2n^2-1$	n^4-n^2+1	$\pm n \pm \alpha$ $\pm\left(n^3-n-n\alpha^2\right) \pm \left((n^2-1)\alpha - \alpha^3\right)$ $\pm\left(n^3 - n\alpha^2\right) \pm \left(n^2\alpha - \alpha^3\right)$
$-6n^2+1$	$9n^4-3n^2+1$	$\pm\left(6n^3-n+n\alpha^2\right) \pm \alpha$ $\pm\left(3n^3+n+n\alpha^2\right) \pm \left((3n^2-1)\alpha + \alpha^3\right)$ $\pm\left(3n^3-2n+n\alpha^2\right) \pm \left(3n^2\alpha + \alpha^3\right)$
$-6n^2-1$	$9n^4+3n^2+1$	$\pm\left(6n^3+n+n\alpha^2\right) \pm \alpha$ $\pm\left(3n^3-n+n\alpha^2\right) \pm \left((3n^2+1)\alpha + \alpha^3\right)$ $\pm\left(3n^3+2n+n\alpha^2\right) \pm \left(3n^2\alpha + \alpha^3\right)$
-3	3	$\pm 1 \pm (\alpha + \alpha^3)$ $\pm(2+\alpha^2) \pm \alpha$ $\pm(1+\alpha^2) \pm (2\alpha + \alpha^3)$

6. Two corollaries

In this section we want to prove two corollaries. The first corollary treats the case of purely quartic complex fields and the second corollary treats the case of rings of the form $\mathbb{Z}[\alpha]$ with $\alpha = \sqrt{a} + \sqrt{b}$.

Corollary 1. *Let $0 < D \in \mathbb{Z}$ and let α be a root of $X^4 + D$. The ring $\mathbb{Z}[\alpha]$ is generated by its units if and only if $D = 1$.*

Proof. Since Theorem 1 we know if $\mathbb{Z}[\alpha]$ is generated by its units, then $D = \pm 1$ or $B^2 - 4D = -4D = -4, -3,$. In any case we deduce $D = 1$ and this case is trivial, since this implies α is a unit. □

Corollary 2. *Let $a, b \in \mathbb{Z}$ such that $a < 0$ or $b < 0$, both not squares and assume $\mathbb{Q}(\sqrt{a} + \sqrt{b})$ is quartic. Then the ring $\mathbb{Z}[\sqrt{a} + \sqrt{b}]$ is not generated by its units except $a = b \pm 1$.*

Proof. First, we note that the field $\mathbb{Q}(\alpha)$ with $\alpha = \sqrt{a} + \sqrt{b}$ is totally complex. Next we compute the minimal polynomial of α. Since the conjugates of α are $\sqrt{a} + \sqrt{b}, \sqrt{a} - \sqrt{b}, -\sqrt{a} + \sqrt{b}, -\sqrt{a} - \sqrt{b}$, we find that $X^4 - 2(a + b)X^2 + (a - b)^2$ is the minimal polynomial of α. with $B = 2(a + b)$ and $D = (a - b)^2$ we find $B^2 - 4D = 4(a + b)^2 - 4(a - b)^2$. If $\mathbb{Z}[\alpha]$ is generated by its units either $D = \pm 1$ or $B^2 - 4D = -4, -3$. The first case yields $a = b \pm 1$ Since $4 | B^2 - 4D$ it remains to investigate the equation $(a + b)^2 - (a - b)^2 = -1$ or equivalently $4ab = -1$. Since $a, b \in \mathbb{Z}$ the last equation yields a contradiction. □

References

[1] N. Ashrafi and P. Vámos. On the unit sum number of some rings. *The Quarterly Journal of Mathematics*, 56(1):1–12, 2005.

[2] P. Belcher. Integers expressible as sums of distinct units. *Bull. Lond. Math. Soc.*, 6:66–68, 1974.

[3] P. Belcher. A test for integers being sums of distinct units applied to cubic fields. *J. Lond. Math. Soc., II. Ser.*, 12:141–148, 1976.

[4] B. Goldsmith, S. Pabst, and A. Scott. Unit sum numbers of rings and modules. *Q. J. Math., Oxf. II. Ser.*, 49(195):331–344, 1998.

[5] B. Jacobson. Sums of distinct divisors and sums of distinct units. *Proc. Am. Math. Soc.*, 15:179–183, 1964.

[6] M. Jarden and W. Narkiewicz. On sums of units. *Monatsh. Math.*, 150(4):327–336, 2007.

[7] J. Śliwa. Sums of distinct units. *Bull. Acad. Pol. Sci.*, 22:11–13, 1974.

[8] R. Tichy and V. Ziegler. Units generating the ring of integers of complex cubic fields. to appear in Colloquium Mathematicum.

[9] P. Vámos. 2-good rings. *The Quarterly Journal of Mathematics*, 56(3):417–430, 2005.

[10] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[11] D. Zelinsky. Every linear transformation is a sum of nonsingular ones. *Proc. Am. Math. Soc.*, 5:627–630, 1954.

V. Ziegler
Graz University of Technology
Institute of algorithmic number theory and analysis,
Steyrergasse 30,
A-8010 Graz, Austria
E-mail address: ziegler@finanz.math.tugraz.at