Bull. Aust. Math. Soc. **93** (2016), 420–432
doi:10.1017/S0004972715001410

ON NUMBER FIELDS WITHOUT A UNIT PRIMITIVE ELEMENT

T. ZAÏMI, M. J. BERTIN✉ and A. M. ALJOUIEE

(Received 5 August 2015; accepted 29 August 2015; first published online 11 January 2016)

Abstract

We characterise number fields without a unit primitive element, and we exhibit some families of such fields with low degree. Also, we prove that a noncyclotomic totally complex number field K, with degree $2d$ where d is odd, and having a unit primitive element, can be generated by a reciprocal integer if and only if K is not CM and the Galois group of the normal closure of K is contained in the hyperoctahedral group B_d.

2010 *Mathematics subject classification*: primary 11R06; secondary 11R32.

Keywords and phrases: primitive elements, Pisot numbers, units, CM-fields, reciprocal integers.

1. Introduction

In its simplest form, the primitive element theorem asserts that any algebraic number field (or, simply, any number field) K may be generated over $\mathbb{Q}$ by a single element, that is, there is a complex number θ such that the set $\{1, \theta, \ldots, \theta^{d-1}\}$ is a basis of the $\mathbb{Q}$-vector space K. The number θ is called a primitive element (or a generator) of K and the field K is denoted by $\mathbb{Q}(\theta)$. Multiplying such an algebraic number θ by a certain rational integer we easily obtain a primitive element of K which is an algebraic integer. Five years ago, Miller [12] asked the following question:

QUESTION 1.1. Does there exist a primitive element of K which is a unit?

In response to Question 1.1, Brooks exhibited some families of biquadratic number fields K without a unit primitive element. Poonen signalled that there is a positive (respectively, a negative) answer to Question 1.1 when K is not a CM-field (respectively, when K belongs to a certain class of CM-fields), without giving details. Recall that the field K is called a CM-field (we also say that K is CM) if it is a totally nonreal quadratic extension of a totally real number field, say R_K, which is unique. These answers of Brooks and Poonen, respectively, are contained in Corollary 1.7 and in Theorem 1.4 below. In fact, Theorem 1.4 is a corollary of the next theorem, which is, itself, a complete answer to the following question, related to some special units generating a given number field.

QUESTION 1.2. Let K be a real (respectively, a nonreal) number field. Can we find a primitive element of K which is a Pisot (respectively, a complex Pisot) unit?

A Pisot number is a real algebraic integer greater than 1 whose other conjugates are of modulus less than one, and a complex Pisot number is a nonreal algebraic integer with modulus greater than 1 whose other conjugates, except its complex conjugate, are of modulus less than one. Clearly, a positive answer to Question 1.2 yields a positive answer to Question 1.1.

Throughout, when we speak about conjugates and degree of an algebraic number field K without mentioning the basic field, this is meant over $\mathbb{Q}$. Similarly, if the extension $K : \mathbb{Q}$ is normal (respectively, cyclic), then we say that K is normal (respectively, cyclic). Also, we denote, by Ω_K, G_K, D and d, respectively, the group of roots of unity in K, the Galois group of the normal closure of K (that is, the normal closure of the extension $K : \mathbb{Q}$), a negative square-free rational integer and a positive rational integer.

It is clear that we have a negative answer to Question 1.2 when $K = \mathbb{Q}$ or when K is a nonreal quadratic field, since the units of K, in these two cases, belong to Ω_K. The following theorems collect some known answers to Question 1.2; the first one is due to Pisot (see for instance [2, 5, 13]) and the other may easily be deduced from the results of [3].

THEOREM 1.3.

(i) *A real number field with degree greater than one can be generated by a Pisot unit.*

(ii) *Let K be a nonreal number field satisfying $K \notin \{\mathbb{Q}(i), \mathbb{Q}(i\sqrt{3})\}$. Then, K is generated by a complex Pisot unit if and only if K is not CM or $\Omega_K \neq \{\pm 1\}$, or $K = \mathbb{Q}(i\sqrt{\beta})$ for some totally positive Pisot unit β (generating R_K), where $i^2 = -1$.*

As mentioned above, the first consequence of Theorem 1.3 is a characterisation of number fields without a unit primitive element.

THEOREM 1.4. *The number field K is generated by a unit if and only if K satisfies one of the following conditions:*

(i) *K is not CM;*

(ii) *K is CM and $\Omega_K \neq \{\pm 1\}$;*

(iii) *K is CM, $\Omega_K = \{\pm 1\}$ and $K = \mathbb{Q}(i\sqrt{\beta})$ where β is a totally positive Pisot unit (generating R_K).*

We refer frequently to the following theorem easily deduced from Theorem 1.4.

THEOREM 1.5. *Let K be a CM field whose only roots of unity are ± 1 and let R_K be its maximal totally real subfield. If all totally positive units in R_K that generate R_K are squares in R_K then K has no unit primitive element.*

On the other hand, if R is a totally real field that contains a totally positive unit β that is not a square in R and generates R, then the CM field $K = \mathbb{Q}(i\sqrt{\beta})$ has a unit primitive element $(i\sqrt{\beta})$, and $R_K = R$.

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

The question of which totally real number fields R contain a totally positive unit that is not a square in R has been investigated by various authors (see, for example, [7]).

Here we are concerned, in the proofs of Theorem 1.10 and Proposition 3.2, with totally real number fields R all of whose totally positive units are squares in R. The referee suggested Proposition 1.6 below which uniformises and thus simplifies the subsequent proofs.

To state this result, let $f_1 = -1, f_2, \ldots, f_d$ be a set of fundamental units of the totally real number field R with $[R : \mathbb{Q}] = d$. Form the $d \times d$ 'matrix of signs' of all d embeddings of $f_1, \ldots, f_d$ into $\mathbb{R}$. Thus, all entries in the first column will be -1, while for $j > 1$ the (i, j)th entry will be the sign (± 1) of f_j in the ith embedding of R into $\mathbb{R}$. Now, map these matrix entries into $\mathbb{F}_2$ by mapping $1 \mapsto 0 \in \mathbb{F}_2$ and $-1 \mapsto 1 \in \mathbb{F}_2$. (This is a kind of logarithmic map, being an isomorphism between the multiplicative group $\{-1, 1\}$ and the additive group $\mathbb{F}_2^+$.) Denote the resulting matrix by M_R.

Proposition 1.6. *If* $\det(M_R) = 0$*, the totally real number field* R *is generated by a totally positive unit which is not a square in* R*.*

On the other hand, if $\det(M_R) = 1$*, all totally positive units in the totally real number field* R *are squares.*

Recall that when K is a quartic CM-field, the real quadratic field R_K contains a unique (fundamental) unit greater than 1, say f_K, such that any unit in R_K is of the form εf_K^k, where $\varepsilon = \pm 1$ and $k \in \mathbb{Z}$. In this case, we deduce from Theorem 1.4 the following consequence.

Corollary 1.7. *Let* K *be a quartic field. Then,* K *has no unit primitive element if and only if the following conditions all hold:*

(1) K *is CM;*
(2) $\{i, i\sqrt{3}, e^{i2\pi/5}\} \cap K = \emptyset$*; and*
(3) f_K *has norm* -1*, or* f_K *has norm* 1 *and* $K \neq \mathbb{Q}(i\sqrt{f_K})$.

A simple calculation (see also the proof of Corollary 1.7) shows that the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{D})$, where $D < -3$, is a quartic CM-field, $K \cap \{i, i\sqrt{3}, e^{i2\pi/5}\} = \emptyset$ and $f_K = 1 + \sqrt{2}$. It follows from Corollary 1.7 that K cannot be generated by a unit, since f_K has norm -1. For the same reason (see, for instance, [15]) any quartic CM-field K satisfying the conditions $K \cap \{i, i\sqrt{3}, e^{i2\pi/5}\} = \emptyset$ and $R_K = \mathbb{Q}(\sqrt{a^2 + 4})$, where a is a positive rational integer, has no unit generator. Similarly, there is no totally nonreal quadratic extension K of $\mathbb{Q}(\sqrt{6})$ which is generated by a unit, since $f_K = 5 + 4\sqrt{6}$ and $\frac{1}{2}(1 + i\sqrt{3}) \in \mathbb{Q}\left(i\sqrt{5 + 4\sqrt{6}}\right)$. Also, from Corollary 1.7, the field $\mathbb{Q}\left(i\sqrt{2 + \sqrt{3}}\right) = \mathbb{Q}(\sqrt{3}, i\sqrt{2})$ is the unique quartic CM-field K having a unit primitive element and such that $\sqrt{3} \in K$ and $\Omega_K = \{\pm 1\}$, since the norm of $f_K = 2 + \sqrt{3}$ is 1. From this computation another question arises.

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

Question 1.8. Let R be a totally real number field. Does there exist a CM-field (or do there exist infinitely many CM-fields) K without a unit primitive element and satisfying $R_K = R$?

Clearly, we have a positive answer to Question 1.8 when $R = \mathbb{Q}$, since each quadratic field $\mathbb{Q}(\sqrt{D})$, where $D \notin \{-1, -3\}$, has no unit generator. Also, we may deduce from Corollary 1.7 a positive answer to Question 1.8 when R is quadratic.

Corollary 1.9. *Let R be a real quadratic field. Then there are infinitely many biquadratic CM-fields K without a unit primitive element and such that $R_K = R$.*

We are unable to answer Question 1.8 when the degree of R is greater than 2. Using the following result, we can prove a positive answer to Question 1.8 when R belongs to certain classes of number fields, and from this we deduce some families of number fields without a unit generator.

Theorem 1.10. *Let K be a CM-field with $\Omega_K = \{\pm 1\}$. Suppose that there is a fundamental set of units of R_K whose elements $f_1, \ldots, f_{d-1}$ are positive, and such that for each embedding σ of R_K into $\mathbb{R}$, other than the identity of K, there is one and only one element of the set $\{1, \ldots, d-1\}$, say j_σ, such that $\sigma(f_{j_\sigma}) < 0$. If the correspondence $\sigma \mapsto j_\sigma$ is one-to-one, then K has no unit primitive element.*

A remarkable class of the set of units is formed by reciprocal integers. An algebraic integer α is said to be reciprocal if $1/\alpha$ is a conjugate of α. Then, the inverse of each conjugate of α is also a conjugate of α, the degree of α is even, except when $\alpha = \pm 1$ and the Galois group $G_{\mathbb{Q}(\alpha)}$ is contained in the hyperoctahedral group $B_d = \mathbb{Z}/2 \wr S_d$, where $\mathbb{Z}/2$ is the cyclic group with order 2, S_d is the the symmetric group on d letters, and each $\sigma \in G_{\mathbb{Q}(\alpha)}$ is identified, for an appropriate ordering of the conjugates $\alpha_1, \ldots, \alpha_{2d}$ of α, with an element $\widetilde{\sigma}$ of S_{2d}, defined by the equalities $\sigma(\alpha_j) = \alpha_{\widetilde{\sigma}(j)}$ for all $j \in \{1, \ldots, 2d\}$. The following question has been considered by Lalande [11].

Question 1.11. Let K be a number field having a unit primitive element and such that $G_K \subseteq B_d$, where $2d$ is the degree of K. Is K generated by a reciprocal integer?

Here the notation $G_K \subseteq B_d$ means that $G_{\mathbb{Q}(\theta)} \subseteq B_d$ for a certain primitive element θ of K, with an appropriate ordering of the conjugates of θ. Lalande [11] obtained a positive answer to Question 1.11 when the field K has at least one real conjugate. (In this case, the condition 'having a unit primitive element' may be removed.) To complete this result it remains to consider the case where K is totally complex. Clearly, we have a positive answer to Question 1.11 when K is cyclotomic, that is, when K is generated by a root of unity, and, in particular, when K is a nonreal quadratic field, because in this last case $K = \mathbb{Q}((1 + i\sqrt{3})/2)$ or $K = \mathbb{Q}(i)$. The theorem below gives some partial answers to Question 1.11.

Theorem 1.12.

(i) *Let K be a noncyclotomic totally complex number field having a unit primitive element of degree $2d$, where d is odd. Then, K is generated by a reciprocal integer if and only if $G_K \subseteq B_d$ and K is not CM.*

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

(ii) *Let K be a quartic totally complex field having a unit primitive element. Then, K is generated by a reciprocal integer if and only if $G_K \subseteq B_2$.*

(iii) *Let K be a CM-field with $\Omega_K = \{\pm 1\}$. Then, K is generated by a reciprocal integer if and only if there is a totally positive reciprocal integer β such that $\mathbb{Q}(\beta) = R_K$ and $K = \mathbb{Q}(i\sqrt{\beta})$.*

Dubickas in [6] recently considered the problem of whether a number field can be generated by a nonreciprocal unit satisfying certain conditions related to the distribution of its conjugates in the complex plane.

The proofs of Theorem 1.12 and some related lemmas, presented in the last section, use Theorem 1.3, Kronecker's theorem, asserting that an algebraic integer is a root of unity when its conjugates belong to the unit circle, and a well-known characterisation of CM-fields which says that a nonreal number field K is CM if and only if K is closed under the complex conjugation, and each embedding of K into $\mathbb{C}$ commutes with the complex conjugation (see, for instance, [4]). In the next section, we easily deduce Theorem 1.4 from Theorem 1.3. The corollaries, Theorem 1.10 and two auxiliary results, proved in the third section, allow us to obtain families of number fields with degree at most 10 and without a unit generator. Theorem 1.10 is, in fact, a consequence of Theorem 1.4. All computations are done using the systems PARI [1] and SAGE [14].

2. Proof of Theorem 1.4

The direct implication in the equivalence, K is not CM, or $\Omega_K \neq \{\pm 1\}$ or $K = \mathbb{Q}(i\sqrt{\beta})$ for some totally positive Pisot unit β (generating R_K) if and only if K is generated by a unit, follows trivially from Theorem 1.3, since a real or a complex Pisot unit is a unit, and the fields $\mathbb{Q}$, $\mathbb{Q}(i)$ and $\mathbb{Q}(i\sqrt{3})$ are, respectively, generated by the units 1, $i = e^{i2\pi/4}$ and $(-1 + i\sqrt{3})/2 = e^{i2\pi/3}$. To prove the converse, suppose that K is generated by a unit u and K is CM (if K is not CM, then there is nothing to show). Let $u_1, \overline{u_1}, \ldots, u_d, \overline{u_d}$ be the conjugates of u and let θ be a Pisot unit generating the real field R_K; such an element θ exists by Theorem 1.3(i). If $\theta_1, \ldots, \theta_d$ are the corresponding conjugates of θ, then the conjugates of the algebraic integer $u\theta^n$, where $n \in \mathbb{N}$, are $u_1\theta_1^n, \overline{u_1}\theta_1^n, \ldots, u_d\theta_d^n$, $\overline{u_d}\theta_d^n$ and the result follows immediately from Theorem 1.3(ii), since $u\theta^n$ is a complex Pisot unit generating K, when n is sufficiently large.

3. Families of number fields without a unit generator

Throughout this section, we always take for D a negative integer.

Proof of Theorem 1.5. Let K be a CM field with $\Omega_K = \{\pm 1\}$ and such that all totally positive units generating R_K are squares in R_K. Assuming on the contrary that K is generated by a unit, we have, from Theorem 1.4, that $K = \mathbb{Q}(i\sqrt{\beta})$ for some totally positive (Pisot) unit β generating R_K. Then, $\sqrt{\beta} \in R_K$, $i = i\sqrt{\beta}/\sqrt{\beta} \in K$ and this last relation leads to a contradiction, since K does not contain nonreal roots of unity. □

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

Proof of Proposition 1.6. Since $\det(M_R) \in \mathbb{F}_2$, it is either 0 or $1 \in \mathbb{F}_2$. If it is 0, then some sum of columns is the 0 vector, so that the corresponding product of distinct f_j is totally positive. Clearly, this product is not a square in R, as it could be taken to be a fundamental unit.

On the other hand, if the determinant is 1, then no such product is totally positive, so that the only totally positive units in R are squares. □

Proof of Corollary 1.7. Let K be a quartic field. If $K \neq \mathbb{Q}(u)$ for all units $u \in K$ then we deduce from Theorem 1.4 that K is CM, and $\Omega_K = \{\pm 1\}$ implies $i \notin K$, $(-1 + i\sqrt{3})/2 \notin K$ and $e^{i2\pi/5} \notin K$; thus, $K \cap \{i, i\sqrt{3}, e^{i2\pi/5}\} = \emptyset$. Also, the case where f_K has norm 1 and $K = \mathbb{Q}(i\sqrt{f_K})$ cannot hold because f_K is a totally positive Pisot unit generating R_K.

To prove the converse, notice first when $\xi \in \Omega_K$ and $\xi \neq \pm 1$ that a conjugate of ξ belongs to the set $\{e^{i2\pi/3}, e^{i2\pi/4} = i, e^{i2\pi/6}\}$ when ξ is quadratic, or to the set $\{e^{i2\pi/5}, e^{i2\pi/8}, e^{i2\pi/10}, e^{i2\pi/12}\}$ when ξ is quartic. It follows from the equalities $(e^{i2\pi/6})^2 = e^{i2\pi/3} = (-1 + i\sqrt{3})/2$, $(e^{i2\pi/10})^2 = e^{i2\pi/5}$ and $(e^{i2\pi/8})^2 = (e^{i2\pi/12})^3 = i$, that the relation $\{i, i\sqrt{3}, e^{i2\pi/5}\} \cap K = \emptyset$ implies $\Omega_K = \{\pm 1\}$. Now, assume on the contrary that the CM-field K, satisfying the two conditions $\{i, i\sqrt{3}, e^{i2\pi/5}\} \cap K = \emptyset$ and f_K has norm -1 (respectively, has norm 1 and $K \neq \mathbb{Q}(i\sqrt{f_K})$), is generated by a unit. It follows from Theorem 1.5 that there is a totally positive Pisot unit β such that $R_K = \mathbb{Q}(\beta)$ and $K = \mathbb{Q}(i\sqrt{\beta})$. Hence, $\beta = f_K^{2(l+1)}$ (respectively, $\beta = f_K^{2(l+1)}$ or $\beta = f_K^{2l+1}$) for some nonnegative rational integer l and so $\sqrt{\beta} = f_K^{(l+1)} \in R_K$ (respectively $\sqrt{\beta} = f_K^{(l+1)} \in R_K$ or $i\sqrt{\beta} = i f_K^l \sqrt{f_K} \in \mathbb{Q}(i\sqrt{f_K})$, which implies $K \subseteq \mathbb{Q}(i\sqrt{f_K})$). This leads immediately to a contradiction, since $i = i\sqrt{\beta}/\sqrt{\beta} \in K$ (respectively, since $i = i\sqrt{\beta}/\sqrt{\beta} \in K$ or $K = \mathbb{Q}(i\sqrt{f_K})$). □

Proof of Corollary 1.9. Set $R = \mathbb{Q}(\sqrt{N})$, where N is a square-free rational integer greater than one. Then, each biquadratic field K of the form $R(\sqrt{D}) = \mathbb{Q}(\sqrt{N}, \sqrt{D})$ is a normal CM-field such that G_K is the Klein group, $R_K = R$ and $e^{i2\pi/5} \notin K$, since $\mathbb{Q}(e^{i2\pi/5})$ is cyclic. Letting (for instance) $|D|$ run through the set of prime numbers greater than $\max\{3, N\}$, we see that the quadratic subfields of K are $\mathbb{Q}(\sqrt{N})$, $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{ND})$ and so $\{i, i\sqrt{3}\} \cap K = \emptyset$. The result follows immediately, from Corollary 1.7. □

Proof of Theorem 1.10. With the above notation, let $R = R_K$ with K a CM-field satisfying $\Omega_K = \{\pm 1\}$. By reordering, if necessary, the embeddings of R into $\mathbb{R}$, we see that M_R is an upper triangular matrix with only 1 on its diagonal. Hence, $\det(M_R) = 1$ and the result follows immediately from Proposition 1.6 and Theorem 1.5. □

The following consequence of Theorem 1.10 allows us to answer Question 1.8, in some particular cases, and also to obtain families of sextic cyclic CM-fields without a unit generator.

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

COROLLARY 3.1. *Let R be a normal real number field with odd prime degree d. If there is an element of R all of whose conjugates, except one, have the same sign and form a fundamental set of units of R, then there are infinitely many cyclic CM-fields K of the form $R(\sqrt{D})$ without a unit primitive element and such that $R_K = R$.*

PROOF. Notice first that if θ generates the totally real number field R, then $\theta + \sqrt{D}$ is a primitive element of the field $K := R(\sqrt{D})$. Hence, K is CM, $R_K = R$ and K is normal, as R is so. By considering the element σ of G_K which sends $\sqrt{D}$ to $-\sqrt{D}$ and whose restriction to R is a generator of G_R (R is cyclic because its degree d is prime), we obtain from the relations $\sigma^j(\theta) = \theta$ if and only if $j \equiv 0 \pmod{d}$ and $\sigma^j(\sqrt{D}) = \sqrt{D}$ if and only if $j \equiv 0 \pmod{2}$ where $j \in \mathbb{Z}$, that the order of σ is $2d$, and so K is cyclic.

In order to apply Theorem 1.10, we first prove that the equality $\Omega_K = \{\pm 1\}$ holds, when D is sufficiently small. Indeed, let $\zeta \in \Omega_K$, satisfying $\zeta \neq \pm 1$. Then the degree of ζ is 2 or $2d$. Since K is cyclotomic when the degree of ζ is $2d$, and since there are at most a finite number of cyclotomic fields with a given degree, we immediately see that the degree of ζ is not $2d$ when D is sufficiently small. Notice also that a calculation similar to the one in the proof of Corollary 1.7 shows that the degree of ζ cannot be equal to 2 when $\{i, i\sqrt{3}\} \cap K = \emptyset$. Because the cyclic field K contains one and only one quadratic field, namely $\mathbb{Q}(\sqrt{D})$, the condition $D \notin \{-1, -3\}$ implies immediately $\{i, i\sqrt{3}\} \cap K = \emptyset$ and so the claim is proved. To conclude, consider the conjugates, say $u_1, \ldots, u_d$ of a unit u of R satisfying the second assumption in Corollary 3.1. By replacing, if necessary, u by $-u$, we may reorder these numbers so that $u_1 > 0, \ldots, u_{d-1} > 0$ and $u_d < 0$. Also, we may suppose without loss of generality that $\{u_1, \ldots, u_{d-1}\}$ is a fundamental set of units of R. Now, let φ_j be the unique automorphism of R sending u_d to u_j, where $j \in \{1, 2, \ldots, d\}$. Then $G_R = \{\varphi_1, \ldots, \varphi_d\} = \{\sigma_1, \ldots, \sigma_d\}$, where $\sigma_j := \varphi_j^{-1}$ for $j \in \{1, \ldots, d\}$ and so for each σ_j with $\sigma_j \neq \sigma_d$ (σ_d is the identity of R) there is one and only one element j_σ ($j_d = j$) of the set $\{1, \ldots, d-1\}$ such that $\sigma_j(u_{j_\sigma}) < 0$, since $\sigma_j(u_j) = u_d$. The results follow immediately from Theorem 1.10, since the above-mentioned correspondence between the group G_R and the set $\{1, \ldots, d\}$ is trivially one-to-one. □

Using Corollary 3.1, one can easily deduce a positive answer to Question 1.8 when R runs through the normal cubic fields $C_n := \mathbb{Q}(\theta_n)$ defined by the conditions $\theta_n^3 - n\theta_n + n = 0$, where n is a square-free positive rational integer, the residue (mod 3) of each prime divisor of n is 1 and $4n - 27$ is the square of a rational integer.

This family of normal cubic fields has been investigated by Francisca [8], who has also shown that each field C_n contains a unit, say u, such that the set $\{u, u'\}$, where u' is a conjugate of u, is a fundamental set of units of C_n and the conjugates of u do not have the same sign. Thus, each C_n satisfies the condition of Corollary 3.1, and so there are infinitely many CM-fields of the form $C_n(\sqrt{D})$ without a unit primitive element. In fact, using the approach of Gras [10] to show Godwin's conjecture [9], a fundamental set of units of C_n is explicitly given in [8]. The following proposition exhibits two examples of families of CM-fields having degrees 8 and 10 without a unit generator.

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

Table 1. Fundamental units for Case 1 of Proposition 3.2.

θ	$f_1(\theta)$	$f_2(\theta)$	$f_3(\theta)$	$f_4(\theta)$
$2\cos 2\pi/11$	$0.83\ldots$	$1.39\ldots$	$3.51\ldots$	$-0.76\ldots$
$2\cos 4\pi/11$	$-1.30\ldots$	$-1.08\ldots$	$0.2\ldots$	$-3.51\ldots$
$2\cos 6\pi/11$	$-1.91\ldots$	$0.54\ldots$	$-1.20\ldots$	$0.59\ldots$
$2\cos 8\pi/11$	$-0.28\ldots$	$0.37\ldots$	$-0.59\ldots$	$-0.52\ldots$
$2\cos 10\pi/11$	$1.68\ldots$	$-3.22\ldots$	$0.76\ldots$	$1.20\ldots$

Proposition 3.2. *If $R=\mathbb{Q}(\theta)$ where $\theta^4+\theta^3-3\theta^2-\theta+1=0$ (respectively, where $\theta^5+\theta^4-4\theta^3-3\theta^2+3\theta+1=0$), then there are infinitely many (respectively, infinitely many cyclic) CM-fields K of the form $R(\sqrt{D})$ without a unit primitive element and such that $R=R_K$.*

Proof.

Case 1: $R=\mathbb{Q}(\theta)$ *and* $\theta^5+\theta^4-4\theta^3-3\theta^2+3\theta+1=0$.

Replacing $(x+1/x)$ by x in the irreducible cyclotomic polynomial $(x^{11}-1)/(x-1)$, we see that $R=R_{\mathbb{Q}(e^{i2\pi/11})}$ is cyclic and the conjugates of θ are $2\cos 2\pi/11\simeq 1.68\ldots, 2\cos 4\pi/11\simeq 0.83\ldots, 2\cos 6\pi/11\simeq -0.28\ldots, 2\cos 8\pi/11\simeq -1.30\ldots$ and $2\cos 10\pi/11\simeq -1.91\ldots$.

With the same argument as in the first part of the proof of Corollary 3.1, each field K of the form $R(\sqrt{D})$, where $D\notin\{-1,-3,-11\}$, is a cyclic CM-field such that $R=R_K$ and $\Omega_K=\{\pm 1\}$ (recall that $\mathbb{Q}(\sqrt{-11})$ is the unique quadratic subfield of $\mathbb{Q}(e^{i2\pi/11})$). Using SAGE [14],

$$\{f_1(\theta)=\theta^2-2, f_2(\theta)=\theta^3-2\theta, f_3(\theta)=\theta^2+\theta-1, f_4(\theta)=\theta^4+\theta^3-3\theta^2-3\theta\}$$

is a fundamental set of units of R. Table 1 gives the approximate values of the elements of the corresponding four fundamental units of R.

We compute the corresponding matrix M_R:

$$M_R=\begin{pmatrix}1&0&0&0&1\\1&1&1&0&1\\1&1&0&1&0\\1&1&0&1&1\\1&0&1&0&0\end{pmatrix}.$$

Thus $\det(M_R)=1$ and the result follows from Proposition 1.6 and Theorem 1.5.

Case 2: $R=\mathbb{Q}(\theta)$ *and* $\theta^4+\theta^3-3\theta^2-\theta+1=0$.

Now, R is a totally real quartic field whose Galois group is the dihedral group D_4. Similarly to the proofs of Corollary 1.9 and Case 1, we find that $K:=R(\sqrt{D})$ is a CM-field with $\Omega_K=\{\pm 1\}$ for infinitely many D. Using SAGE [14],

$$\{f_1(\theta)=\theta, f_2(\theta)=\theta^3+\theta^2-2\theta, f_3(\theta)=\theta^3+2\theta^2-\theta-1\}$$

is a set of fundamental units of R. The approximate values of these units, together with their conjugates, are given in Table 2.

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

TABLE 2. Fundamental units for Case 2 of Proposition 3.2.

$\theta = f_1(\theta)$	$f_2(\theta)$	$f_3(\theta)$
1.35...	1.61...	3.81...
0.47...	−0.61...	−0.91...
−0.73...	1.61...	0.42...
−2.09...	−0.61...	0.67...

We conclude as in the previous case since the corresponding matrix M_R is

$$M_R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix},$$

and its determinant is 1. □

4. Proof of Theorem 1.12

To make clear the proof of Theorem 1.12, let us give some auxiliary results. The first one has already been proved in [11]; we prefer to give a different simple proof.

LEMMA 4.1 [11]. *Suppose that the conjugates $\theta_1, \theta_2, \ldots, \theta_{2d-1}, \theta_{2d}$ of an algebraic number θ are ordered so that $G_{\mathbb{Q}(\theta)} \subseteq B_d$. Then $\theta_{2j} \in \mathbb{Q}(\theta_{2j-1})$ for all $j \in \{1, \ldots, d\}$.*

PROOF. Let θ_k be a conjugate over the field $\mathbb{Q}(\theta_{2j-1})$ of the number θ_{2j} for some j and k. Then there is an embedding σ of $\mathbb{Q}(\theta_{2j-1}, \theta_{2j})$ into $\mathbb{C}$ sending θ_{2j-1} to θ_{2j-1} and θ_{2j} to θ_k (σ is an extension of the identity of $\mathbb{Q}(\theta_{2j-1})$). By considering an element of $G_{\mathbb{Q}(\theta)} \subseteq B_d$ whose restriction to $\mathbb{Q}(\theta_{2j-1}, \theta_{2j})$ is σ, we see that $\sigma(\theta_{2j-1}) = \theta_{2j-1}$, $\sigma(\theta_{2j}) = \theta_{2j}$, which implies $\theta_{2j} = \theta_k$. Thus, the only conjugate of θ_{2j} over $\mathbb{Q}(\theta_{2j-1})$ is θ_{2j} and so $\theta_{2j} \in \mathbb{Q}(\theta_{2j-1})$. □

The following result asserts that the Galois group of the normal closure of a CM-field is always contained in the hyperoctahedral group.

LEMMA 4.2. *If K is a CM-field with degree $2d$, then $G_K \subseteq B_d$.*

PROOF. Let θ be a primitive element of the CM-field K. Suppose that the conjugates $\theta_1, \ldots, \theta_{2d}$ of θ are ordered so that $\theta_{2j} = \overline{\theta_{2j-1}}$ for all $j \in \{1, \ldots, d\}$ and let $\sigma \in G_{\mathbb{Q}(\theta)}$ satisfy $\sigma(\theta_{2j}) = \theta_{2l}$ (respectively, $\sigma(\theta_{2j}) = \theta_{2l-1}$) for some j and l. Since the restriction of σ to the CM-field $\mathbb{Q}(\theta_{2j})$ commutes with the complex conjugation, that is, $\sigma(\overline{\theta_{2j}}) = \overline{\sigma(\theta_{2j})}$, we see that $\sigma(\theta_{2j-1}) = \theta_{2l-1}$ (respectively, that $\sigma(\theta_{2j-1}) = \theta_{2l}$). In a similar manner, when $\sigma(\theta_{2j-1}) = \theta_{2l}$ (respectively, $\sigma(\theta_{2j-1}) = \theta_{2l-1}$), we find $\sigma(\theta_{2j}) = \theta_{2l-1}$ (respectively, $\sigma(\theta_{2j}) = \theta_{2l}$). Thus $G_{\mathbb{Q}(\theta)} \subseteq B_d$ and so $G_K \subseteq B_d$. □

The lemma below may be viewed as a converse of Lemma 4.2.

LEMMA 4.3. *Let K be a totally complex number field of degree $2d$ such that $G_{\mathbb{Q}(\theta)} \subseteq B_d$ for some primitive element θ of K and where the conjugates are ordered so that $\theta_{2j} = \overline{\theta_{2j-1}}$ for all $j \in \{1, \ldots, d\}$. Then K is a CM-field.*

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

PROOF. From Lemma 4.1, $\theta_{2j} \in \mathbb{Q}(\theta_{2j-1})$ and so K is closed with respect to complex conjugation. Set $\theta := \theta_1$ and let φ be an embedding of $\mathbb{Q}(\theta)$ into $\mathbb{C}$ sending θ to some θ_{2j} (respectively, some θ_{2j-1}). By considering an element of $G_{\mathbb{Q}(\theta)}$ whose restriction to K is φ, we deduce in the two cases that $\varphi(\overline{\theta}) = \varphi(\theta_2) = \theta_{2j-1} = \overline{\theta_{2j}}$ (respectively, $\varphi(\overline{\theta}) = \varphi(\theta_2) = \theta_{2j} = \overline{\theta_{2j-1}}$) and $\varphi(\overline{\theta}) = \overline{\varphi(\theta)}$, and so φ commutes with the complex conjugation. Hence, K is a CM-field. □

The following result is an analogue of Theorem 1.3(ii), for reciprocal generators.

LEMMA 4.4. *Let α be a reciprocal integer generating a CM-field K. If $\alpha \notin \Omega_K$, then the degree of α is a multiple of 4 and there is a totally positive reciprocal integer $\beta \in R_K$ such that $\alpha^2 = \zeta\beta$ and $\zeta \in \Omega_K \backslash \{1\}$.*

PROOF. Let $\alpha_1 := \alpha, \ldots, \alpha_{2d}$ be the conjugates of α, ordered so that $\alpha_{2j} = \overline{\alpha_{2j-1}}$ for all $j \in \{1, \ldots, d\}$. Then, as in the proof of Theorem 1.3(ii) (see [3]), the conjugates of α over R_K are α and $\overline{\alpha}$, and the conjugates of the algebraic integer $\beta := |\alpha|^2 \in R_K$ (over $\mathbb{Q}$) are the numbers $|\alpha_1|^2, |\alpha_3|^2, \ldots, |\alpha_{2d-1}|^2$. It follows that there is no $j \in \{1, \ldots, d\}$ such that $|\alpha_{2j-1}|^2 = 1$, since otherwise all conjugates of α belong to the unit circle and so, by Kronecker's theorem, $\alpha \in \Omega_K$. Hence, if α_k is a conjugate of α, then so are all the distinct numbers $\alpha_k, \overline{\alpha_k}, 1/\alpha_k$ and $1/\overline{\alpha_k}$, and consequently $1/\beta$ is a conjugate of β; thus, β is a totally positive reciprocal integer (having even degree) and the degree of R_K is even, and so the degree of K is a multiple of 4. Moreover, since β is a unit and the conjugates of the algebraic integer $\alpha^2/\beta \in K$ are the numbers $\alpha_1^2/|\alpha_1|^2, \ldots, \alpha_{2d}^2/|\alpha_{2d}|^2$, all of modulus 1, we have again by Kronecker's theorem that $\alpha^2/\beta \in \Omega_K$ and so $\alpha^2 = \zeta\beta$, for some $\zeta \in \Omega_K \backslash \{1\}$. □

The lemma below allows us to obtain a complete answer to Question 1.11 in the quartic case.

LEMMA 4.5. *A quartic CM-field, having a unit primitive element, is generated by a reciprocal integer.*

PROOF. Let K be a quartic CM-field having a unit primitive element. Clearly, when there is a quartic element $\zeta \in \Omega_K$, the cyclotomic field K is generated by the reciprocal integer ζ. Notice also, when $\Omega_K = \{\pm 1\}$, that Corollary 1.7 yields $K = \mathbb{Q}(i\sqrt{f_K})$, where the fundamental unit f_K of R_K has norm 1. Hence, $1/f_K$ is a conjugate of f_K, the conjugates of $i\sqrt{f_K}$ are $i\sqrt{f_K}, -i\sqrt{f_K}, i/\sqrt{f_K}, -i/\sqrt{f_K} = 1/i\sqrt{f_K}$, and so $i\sqrt{f_K}$ is a reciprocal integer generating K. Finally, suppose that there is a quadratic element $\zeta \in \Omega_K$. Then the minimal polynomial of ζ over R_K is $(x - \zeta)(x - \overline{\zeta}) \in \mathbb{Z}[x]$, and since the real quadratic number f_K^2 is a reciprocal integer generating R_K, we deduce that the conjugates of ζf_K^2 are the four distinct numbers $\zeta f_K^2, \overline{\zeta} f_K^2, \zeta/f_K^2$ and $\overline{\zeta}/f_K^2 = 1/\zeta f_K^2$, and so ζf_K^2 is a reciprocal integer generating K. □

REMARK 4.6. We may also deduce from Lemma 4.5 the following answer to Question 1.1: a nonnormal quartic CM-field has no unit primitive element. Indeed, let K be a quartic CM-field, and suppose that K has a unit primitive element. Then,

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

Lemma 4.5 asserts that K is generated by a reciprocal integer, say α. If $\overline{\alpha} \neq 1/\alpha$, then K is a normal extension of $\mathbb{Q}$, because the conjugates of α are α, $1/\alpha$, $\overline{\alpha}$ and $1/\overline{\alpha}$. Otherwise, $\overline{\alpha} = 1/\alpha$ and there is a conjugate α' of α such that $\alpha' \notin \{\alpha, 1/\alpha\}$, and so the conjugates of α are α, $1/\alpha$, α' and $1/\alpha'$. It follows, in this last case, from the relation $\overline{\alpha'} \notin \{\alpha, 1/\alpha, \alpha'\}$ that $\overline{\alpha'} = 1/\alpha'$ and the conjugates of α are on the unit circle (α is a root of unity by Kronecker's theorem), and so the field K is (cyclotomic) normal.

Proof of Theorem 1.12. The proof is in three parts.

Proof of Part (i). Let K be a noncyclotomic totally complex number field having a unit primitive element and being of degree $2d$ where d is odd. The direct implication in Theorem 1.12 follows trivially from the introduction and the first assertion in Lemma 4.4, because K is not cyclotomic and $2d$ is not a multiple of 4. Notice also from Lemma 4.2 that the condition $G_K \subseteq B_d$ is always true when K is CM.

To prove the converse, suppose that K is not CM and $G_K \subseteq B_d$. Let θ be a primitive element of K such that $G_{\mathbb{Q}(\theta)} \subseteq B_d$, for an appropriate ordering, say $\theta_1, \theta_2, \ldots, \theta_{2d-1}, \theta_{2d}$, of the conjugates of θ. It follows by Lemma 4.3 that there is $j \in \{1, \ldots, d\}$ such that $\theta_{2j} \neq \overline{\theta_{2j-1}}$.

To simplify the notation, we may suppose, without loss of generality, that $j = 1$, since any conjugate of a reciprocal integer is reciprocal and each conjugate of K satisfies the same assumptions as K. Let α_1 be a complex Pisot unit generating K; such an element exists from Theorem 1.3(ii), since K is not CM (this does not affect the assumption $j = 1$). Let $\alpha_1, \alpha_2, \ldots, \alpha_{2d-1}, \alpha_{2d}$ be the corresponding conjugates of α_1. Then $\theta_2 \neq \overline{\theta_1}$ implies $\alpha_2 \neq \overline{\alpha_1}$ and we have from Lemma 4.1 that $\alpha_{2j} \in \mathbb{Q}(\alpha_{2j-1})$ for all $j \in \{1, \ldots, d\}$. Let c be the unique element of $\{3, \ldots, n\}$ such that $\overline{\alpha_1} = \alpha_c$ and consider the algebraic integer $\eta_1 := \alpha_1/\alpha_2 \in K$. The corresponding conjugates of η_1 are $\eta_1, \eta_2 := \alpha_2/\alpha_1 = 1/\eta_1, \ldots, \eta_{2d-1} := \alpha_{2d-1}/\alpha_{2d}$, $\eta_{2d} := \alpha_{2d}/\alpha_{2d-1}$, and so η_1 is a reciprocal integer. Now, we claim that η_1 is a primitive element of K. Indeed, let s be the degree of η_1 (over $\mathbb{Q}$) and let t be the degree of α_1 over $\mathbb{Q}(\eta_1)$. Then $st = 2d$ and the claim follows immediately when $t = 1$. Assume on the contrary that $t \geq 2$. Then η_1 is repeated t times in the set $\{\eta_1, \eta_2, \ldots, \eta_{2d}\}$. Notice also that if $\alpha_1/\alpha_2 = \eta_l = \alpha_l/\alpha_v$ for some $l \in \{2, \ldots, 2d\}$ and $v \in \{l-1, l+1\}$, then $\alpha_1\alpha_v = \alpha_l\alpha_2$, $1 \leq |\alpha_1\alpha_v| = |\alpha_l\alpha_2|$, because α_1 is a complex Pisot number, and so $1 < |\alpha_l|$, since $|\alpha_2| < 1$; thus, $\alpha_l = \overline{\alpha_1}$, $l = c$ and so $t = 2$. Hence, $s = d$, and this last equality leads to a contradiction, because d is odd and the degree s of the reciprocal integer η_1 is even ($|\eta_1| > |\alpha_1| > 1$ implies $\eta_1 \neq \pm 1$).

Proof of Part (ii). From the introduction we know that the direct implication is true. To prove the converse, consider a primitive element θ of the totally complex quartic field K and suppose that the conjugates $\theta = \theta_1, \theta_2, \theta_3, \theta_4$ of θ are ordered so that $G_{\mathbb{Q}(\theta)} \subseteq B_2$. Recall, by Lemma 4.1, that $\theta_2 \in \mathbb{Q}(\theta_1)$ and $\theta_4 \in \mathbb{Q}(\theta_3)$. From Lemma 4.5, K is generated by a reciprocal integer when it is CM. This happens, in particular, when $\theta_2 = \overline{\theta_1}$, because in this case $\theta_4 = \overline{\theta_3}$, and so K is CM from Lemma 4.3. Suppose, now, that K is not CM (so $\theta_2 \neq \overline{\theta_1}$), and set, for instance, $\theta_3 = \overline{\theta_1}$. Then $\theta_4 = \overline{\theta_2}$, and by Theorem 1.3(ii), there is a complex Pisot unit α generating K. Let $\alpha_1 = \alpha, \alpha_2, \alpha_3, \alpha_4$

https://doi.org/10.1017/S0004972715001410 Published online by Cambridge University Press

be the corresponding conjugates of α. Then, $\alpha_2 \in \mathbb{Q}(\theta_2) = \mathbb{Q}(\theta_1) = \mathbb{Q}(\alpha_1)$, $\alpha_3 = \overline{\alpha_1}$ and $\alpha_4 = \overline{\alpha_2} \in \mathbb{Q}(\theta_3) = \mathbb{Q}(\alpha_3)$. Now we claim, similarly to the proof of Theorem 1.12(i), that the reciprocal integer $\eta := \alpha_1/\alpha_2$, whose conjugates are α_1/α_2, $\alpha_2/\alpha_1 = 1/\eta$, $\alpha_3/\alpha_4 = \overline{\eta}$ and $\alpha_4/\alpha_3 = 1/\overline{\eta}$, is a generator of K. Indeed, assuming the contrary, we see that η is quadratic, since $|\alpha_1| > 1 > |\alpha_2|$, and so $|\eta| > 1 > |1/\eta|$. Moreover, η is real, since $\eta = \overline{\eta}$. It follows, from the relations $\mathbb{Q} \subset \mathbb{Q}(\eta) \subset \mathbb{Q}(\eta)(\alpha) = \mathbb{Q}(\alpha)$, that α is quadratic over $\mathbb{Q}(\eta)$ and the minimal polynomial of α over the real field $\mathbb{Q}(\eta)$ is $(x-\alpha)(x-\overline{\alpha}) = (x-\alpha_1)(x-\alpha_3)$, and so the minimal polynomial of α_2 over $\mathbb{Q}(\eta)$ is $(x-\alpha_2)(x-\overline{\alpha_2}) = (x-\alpha_2)(x-\alpha_4)$. Hence, K is a quadratic totally nonreal extension of the totally real field $\mathbb{Q}(\eta)$, and this last assertion leads to a contradiction, since K is supposed to be non-CM.

Proof of Part (iii). Let K be a CM-field with $\Omega_K = \{\pm 1\}$. Suppose that there is a reciprocal integer α generating K. Then the second assertion in Lemma 4.4 implies that there is a totally positive reciprocal integer $\beta \in R_K$ such that $\alpha^2 = -\beta$. Hence, the degree of β is half the degree of α, β is a primitive element of $R_{\mathbb{Q}(\alpha)}$ and $K = \mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{\beta})$. The converse follows trivially from the fact that $i\sqrt{\beta}$ is a reciprocal integer generating the CM-field $\mathbb{Q}(i\sqrt{\beta})$ when β is a totally positive reciprocal integer. □

Acknowledgement

We thank very much the referee for his acute and pertinent remarks and suggestions which have contributed to the clarification and simplification of certain of our results.

References

[1] C. Batut, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to PARI-GP, Version 2.5.1* (Institut de Mathématiques de Bordeaux, 2012), pari.math.u-bordeaux.fr/pub/pari/manuals/2.5.1/users.pdf.
[2] M. J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse and J. P. Schreiber, *Pisot and Salem numbers* (Birkhäuser, Verlag, Basel, 1992).
[3] M. J. Bertin and T. Zaïmi, "Complex Pisot numbers in algebraic number fields", *C. R. Math. Acad. Sci. Paris* **353** (2015), doi:10.1016/j.crma.2015.09.007.
[4] P. E. Blanksby and J. H. Loxton, 'A note on the characterization of CM-fields', *J. Aust. Math. Soc.* **26** (1978), 26–30.
[5] Y. Bugeaud, *Distribution Modulo One and Diophantine Approximation*, Cambridge Tracts in Mathematics, 193 (Cambridge University Press, Cambridge, 2012).
[6] A. Dubickas, 'Nonreciprocal units in a number field with an application to Oeljeklaus–Toma manifolds (with an appendix by Laurent Battisti)', *New York J. Math.* **20** (2014), 257–274.
[7] H. M. Edgar, R. A. Mollin and B. L. Peterson, 'Class groups, totally positive units and squares', *Proc. Amer. Math. Soc.* **98**(1) (1986), 33–37.
[8] C. O. Francisca, 'On cyclic cubic fields', *Extracta Math.* **6** (1991), 28–30.
[9] H. J. Godwin, 'The determination of units in totally real cubic fields', *Math. Proc. Cambridge Philos. Soc.* **56** (1960), 318–321.
[10] M. N. Gras, 'Note à propos d'une conjecture de H. J. Godwin sur les unités des corps cubiques', *Ann. Inst. Fourier (Grenoble)* **30** (1980), 1–6.
[11] F. Lalande, 'Corps de nombres engendrés par un nombre de Salem', *Acta Arith.* **83** (1999), 191–200.
[12] V. Miller, 'Two questions about units in number fields', mathoverflow.net/questions/15260/two-questions-about-units-in-number-fields.

[13] C. Pisot, *Quelques aspects de la théorie des entiers algébriques*, Séminaire de mathématiques supérieures (Université de Montréal, Montréal, 1966).
[14] SAGE Mathematics Software, Version 3.4, http://www.sagemath.org.
[15] H. Yokoi, 'On real quadratic fields containing units with norm −1', *Nagoya Math. J.* **33** (1968), 139–152.

T. ZAÏMI, College of Science,
Al-Imam Mohammad Ibn Saud Islamic University,
PO Box 90950, Riyadh 11623, Saudi Arabia
e-mail: tmzaemi@imamu.edu.sa

M. J. BERTIN, Université Pierre et Marie Curie (Paris 6),
IMJ, 4 Place Jussieu, 75005 Paris, France
e-mail: marie-jose.bertin@imj-prg.fr

A. M. ALJOUIEE, College of Science,
Al-Imam Mohammad Ibn Saud Islamic University,
PO Box 90950, Riyadh 11623, Saudi Arabia
e-mail: amjouiee@imamu.edu.sa