Acta Scientiarum Mathematicarum
https://doi.org/10.1007/s44146-023-00092-9

Acta Scientiarum Mathematicarum

On the monogenity of pure quartic relative extensions of $\mathbb{Q}(i)$

István Gaál and László Remete

Abstract. We consider pure quartic relative extensions of the number field $\mathbb{Q}(i)$ of type $K = \mathbb{Q}(\sqrt[4]{a+bi})$, where $a, b \in \mathbb{Z}$ and $b \neq 0$, such that $a+bi \in \mathbb{Z}[i]$ is square-free. We describe integral bases of these fields. The index form equation is reduced to a relative cubic Thue equation over $\mathbb{Q}(i)$ and some corresponding quadratic form equations. We consider monogenity of K and relative monogenity of K over $\mathbb{Q}(i)$. We shall show how our former method based on the factors of the index form can be used in the relative case to exclude relative monogenity in some cases.

Mathematics Subject Classification. Primary 11Y50; Secondary 11R04, 11R16, 11R21, 11D41, 11D57, 11Y40.

Keywords. Monogenity, Power integral bases, Relative quartic extensions, Relative power integral bases, Index form equation.

1. Monogenity: basic concepts

Let ϑ be an algebraic integer of degree n, set $K = \mathbb{Q}(\vartheta)$. Denote by $\mathbb{Z}_K$ the ring of integers of K and by D_K the discriminant of K. The number field K is called *monogenic* if there exists $\alpha \in \mathbb{Z}_K$ such that $(1, \alpha, \ldots, \alpha^{n-1})$ is an integral basis, called *power integral basis* (for a detailed discussion of monogenity and power integral bases of number fields see [3]).

The *index* of a primitive element $\alpha \in \mathbb{Z}_K$ is defined as

$$I(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha]).$$

α *generates a power integral basis* if and only if $I(\alpha) = 1$. Denoting by $\alpha^{(j)}$ $(j = 1, \ldots, n)$ the conjugates of α, we have

$$I(\alpha) = \frac{1}{\sqrt{|D_K|}} \prod_{1 \leq i < j \leq n} \left| \alpha^{(i)} - \alpha^{(j)} \right|,$$

Research supported by the ÚNKP-21-4-I new national excellence program of the ministry for innovation and technology from the source of the national research, development and innovation fund and in part by the Eötvös Loránd Research Network (ELKH).

Published online: 14 June 2023

for a primitive element $\alpha \in \mathbb{Z}_K$.

If $\alpha, \beta \in \mathbb{Z}_K$ and $\beta = \pm\alpha + a$ with $a \in \mathbb{Z}$, then α and β are called *equivalent*. Equivalent algebraic integers have the same indices.

If K contains a proper subfield M, then for a primitive algebraic integer α in K we have

$$I(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha]) = (\mathbb{Z}_K : \mathbb{Z}_M[\alpha]) \cdot (\mathbb{Z}_M[\alpha] : \mathbb{Z}[\alpha]),$$

where

$$I_{K/M}(\alpha) = (\mathbb{Z}_K : \mathbb{Z}_M[\alpha])$$

is called the *relative index* of α over M (cf. [3]). $\alpha, \beta \in \mathbb{Z}_K$ are called *relative equivalent* if $\alpha = \varepsilon\beta + a$ where ε is a unit in M and $a \in \mathbb{Z}_M$. Relative equivalent algebraic integers have the same relative indices.

If $(1, \omega_2, \ldots, \omega_n)$ is an integral basis in K, then the discriminant of the linear form $L(\underline{x}) = x_1 + \omega_2 x_2 + \ldots + \omega_n x_n$ can be written as

$$D(L(\underline{x})) = I(x_2, \ldots, x_n)^2 \cdot D_K,$$

where D_K is the discriminant of K and $I(x_2, \ldots, x_n)$ is a homogeneous polynomial of degree $n(n-1)/2$ having the property that for any $\alpha = x_1 + x_2\omega_2 + \ldots + x_n\omega_n \in \mathbb{Z}_K$ the equation $I(\alpha) = |I(x_2, \ldots, x_n)|$ is satisfied. Therefore, determining generators of power integral bases leads to the Diophantine equation

$$I(x_2, \ldots, x_n) = \pm 1 \text{ in } x_2, \ldots, x_n \in \mathbb{Z},$$

called the *index form equation* corresponding to the integral basis $(1, \omega_2, \ldots, \omega_n)$, see [3].

To determine all inequivalent generators of power integral bases is a complicated problem, leading to the resolution of index form equations.

There are efficient methods for the resolution of index form equations in cubic and quartic number fields. However, this problem is only partially solved for higher degree fields, since in those cases the index form equation becomes much more complicated (cf. [3]).

2. The purposes of the present paper

In the present paper we consider pure quartic relative extensions of the number field $M = \mathbb{Q}(i)$. These fields are of type $K = \mathbb{Q}(\sqrt[4]{a+bi})$ where $a, b \in \mathbb{Z}$ and $b \neq 0$, such that $a + bi$ is not a square in $\mathbb{Z}_M$. We describe the integral bases of these fields and characterize their absolute and relative monogenity for the case that $a + bi$ is square-free.

Remark that formerly in [7] we considered monogenity of number fields $K = \mathbb{Q}(i, \sqrt[4]{m})$. Those are also octic fields containig $\mathbb{Q}(i)$ as a subfield, but those fields are composites of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt[4]{m})$ allowing a much easier investigation. In the present paper we study quartic relative extensions of $\mathbb{Q}(i)$, which are not composites of $\mathbb{Q}(i)$ with a quartic field.

To construct an integral basis in $K = \mathbb{Q}(\sqrt[4]{a+bi})$ we shall apply an extension of Lemma 2.17 of Narkiewicz [8] stating that if an algebraic integer

is defined by a minimal polynomial which is p-Eisenstein with respect to the prime p, then its index is not divisible by p.

We shall use the result of Gaál and Pohst [4], see also Chapter 14.1 of Gaál [3], reducing the index form equations in relative quartic extensions to a cubic relative Thue equation and to some corresponding relative quadratic form equations, similarly as in [5] in the absolute case.

Further, in our proofs we shall give a *relative analogue of another method, based on the factors of the index form.* If the index form as a polynomial with integer coefficients in $x_2, \dots, x_n$ has factors F_1, F_2 (also polynomials with integer coefficients in $x_2, \dots, x_n$) and there exists an element of index 1 (a generator of power integral basis), then there exist $y_2, \dots, y_n \in \mathbb{Z}$ such that $I(y_2, \dots, y_n) = \pm 1$, therefore $F_1(y_2, \dots, y_n) = \pm 1$ and $F_2(y_2, \dots, y_n) = \pm 1$. However, in some cases it can be shown that e.g. $F_1 - aF_2^2$ is divisible by some constant b ($a, b \in \mathbb{Z} \setminus \{0\}$). If b does not divide $\pm 1 - a$ with neither of the possible choices of the sign, then it contradicts the existence of a generator of a power integral basis with coordinates $y_2, \dots, y_n \in \mathbb{Z}$ in the integral basis. This method was used e.g. in [6,7] to exclude monogenity of the corresponding fields in the absolute case. In our present paper we show how a relative analogue of this method can be used to exclude the existence of relative power integral bases in relative extensions. This version of the method is used here for the first time. We believe it will have several further applications in the study of monogenity of higher degree number fields.

3. Pure quartic extensions of $M = \mathbb{Q}(i)$: preliminaries

We shall consider number fields of type $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt[4]{a + bi}$, where $a, b \in \mathbb{Z}$, $b \neq 0$ and $a + bi$ is square-free in the ring of Gaussian integers $\mathbb{Z}[i]$. α is a root of the polynomial

$$f(X) = X^8 - 2aX^4 + a^2 + b^2 \in \mathbb{Z}[X], \tag{1}$$

and the conjugates of α are

$$\pm\sqrt[4]{a + bi}, \qquad \pm i\sqrt[4]{a + bi}, \qquad \pm\sqrt[4]{a - bi}, \qquad \pm i\sqrt[4]{a - bi}.$$

In the proof of our theorem on the integral basis of the number field K we need the following Lemma. This is a slight extension of Lemma 2.17 [8] to the relative case, when the ground field is M instead of $\mathbb{Q}$. Our proof strictly follows the arguments of Lemma 2.17 [8]. The same arguments seem to remain valid also for any ground field having unique factorization in its ring of integers.

Lemma 1. *Let $M = \mathbb{Q}(i)$ and $K = M(\alpha)$, where α is an algebraic integer. If the minimal polynomial over M of α is π-Eisenstein for a prime $\pi \in \mathbb{Z}_M$, i.e. it has the form*

$$X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}_M[X],$$

with $a_0, a_1, \dots, a_{n-1}$ divisible by π and $\pi^2 \nmid a_0$, then there is no algebraic integer $\xi \in \mathbb{Z}_K$, such that $\xi \notin \mathbb{Z}_M[\alpha]$, but $\pi \cdot \xi \in \mathbb{Z}_M[\alpha]$. I.e. $\mathbb{Z}_M[\alpha]$ is π-maximal.

Proof. The π-Eisenstein property of the minimal polynomial of α over M implies that α^n/π is an algebraic integer, and $\pi^2 \nmid N_{K/M}(\alpha) = a_0$. Assume that there exists an algebraic integer $\xi \in \mathbb{Z}_K$, such that $\xi \notin \mathbb{Z}_M[\alpha]$, but $\pi \cdot \xi \in \mathbb{Z}_M[\alpha]$:

$$\xi = \frac{\beta_0 + \beta_1\alpha + \ldots + \beta_{n-1}\alpha^{n-1}}{\pi}, \qquad \beta_i \in \mathbb{Z}_M, \xi \notin \mathbb{Z}_M[\alpha].$$

Let j be the minimal index with $\pi \nmid \beta_j$. Then

$$\frac{\beta_0 + \beta_1\alpha + \ldots + \beta_{j-1}\alpha^{j-1}}{\pi} \in \mathbb{Z}_M[\alpha],$$

so

$$\begin{aligned}\eta &= \xi - \frac{\beta_0 + \beta_1\alpha + \ldots + \beta_{j-1}\alpha^{j-1}}{\pi} \\ &= \frac{\beta_j\alpha^j + \beta_{j+1}\alpha^{j+1} + \ldots + \beta_{n-1}\alpha^{n-1}}{\pi} \in \mathbb{Z}_K.\end{aligned}$$

Therefore,

$$\zeta = \alpha^{n-j-1} \cdot \eta - \frac{\alpha^n}{\pi} \cdot (\beta_{j+1} + \beta_{j+2}\alpha + \ldots + \beta_{n-1}\alpha^{n-j-2}) = \frac{\beta_j\alpha^{n-1}}{\pi} \in \mathbb{Z}_K.$$

This implies

$$\pi^n N_{K/M}(\zeta) = N_{K/M}(\pi\zeta) = N_{K/M}(\beta_j\alpha^{n-1}) = \beta_j^n N_{K/M}(\alpha)^{n-1}$$

hence π has to divide β_j, contrary to the choice of j. □

We shall also use the result of Gaál and Pohst [4], see also Theorem 14.1 of Gaál [3]. We briefly detail the lemma here, because it is an essential tool for the proof of Theorem 4. Let K be a quartic extension of M, generated by an α with relative minimal polynomial $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 \in \mathbb{Z}_M[x]$. Denote by n the relative index of α over M.

We can represent any $\vartheta \in \mathbb{Z}_K$ in the form

$$\vartheta = \frac{A + X\alpha + Y\alpha^2 + Z\alpha^3}{d} \tag{2}$$

where $A, X, Y, Z \in \mathbb{Z}_M$ and $d \in \mathbb{Z}$ is a common denominator.

Then

$$F(U,V) = U^3 - a_2U^2V + (a_1a_3 - 4a_4)UV^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)V^3$$

is a binary cubic form over $\mathbb{Z}_M$ and

$$\begin{aligned}Q_1(X,Y,Z) &= X^2 - a_1XY + a_2Y^2 + (a_1^2 - 2a_2)XZ \\ &\quad + (a_3 - a_1a_2)YZ + (-a_1a_3 + a_2^2 + a_4)Z^2, \\ Q_2(X,Y,Z) &= Y^2 - XZ - a_1YZ + a_2Z^2\end{aligned}$$

are ternary quadratic forms over $\mathbb{Z}_M$.

Lemma 2 (Gaál and Pohst [4]). *If ϑ of (2) generates a power integral basis of K over M, then there is a unit $\varepsilon \in M$, a $\gamma \in \mathbb{Z}_M$ of norm $\pm d^{12}/n$ and a solution $(U,V) \in \mathbb{Z}_M^2$ of*

$$F(U,V) = \varepsilon \cdot \gamma, \tag{3}$$

such that

$$U = Q_1(X, Y, Z),$$
$$V = Q_2(X, Y, Z). \tag{4}$$

In our case $a_1 = a_2 = a_3 = 0$ and $a_4 = -(a + bi)$.

4. Integral bases

Let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[4]{a + bi}$, $b \neq 0$ and $a + bi$ is square-free in $\mathbb{Z}_M$, as above.

Theorem 3. *An integral basis of K is given by the following table:*

	a (mod 8)	b (mod 8)	*Integral basis*
1.	0, 1, 2, 3, 4, 5, 6, 7	1, 3, 5, 7	$\left(1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\right)$
2.	1	0	$\left(1, \alpha, \frac{1+\alpha^2}{2}, \frac{1+\alpha+\alpha^2+\alpha^3}{4}, i, \frac{1+\alpha+i+i\alpha}{2}, \frac{1+2\alpha+\alpha^2+3i+i\alpha^2}{4}, \frac{1+2\alpha+\alpha^2+2i+i\alpha+i\alpha^3}{4}\right)$
3.	1, 5	2, 6	$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1+\alpha+\alpha^3+i}{2}, \frac{1+\alpha+\alpha^2+i\alpha}{2}, \frac{\alpha+\alpha^2+\alpha^3+i\alpha^2}{2}, \frac{1+\alpha^2+\alpha^3+i\alpha^3}{2}\right)$
4.	1	4	$\left(1, \alpha, \frac{1+\alpha^2}{2}, \frac{\alpha+\alpha^3}{2}, \frac{1+3\alpha+\alpha^2+\alpha^3+2i}{4}, \frac{3+\alpha+\alpha^2+\alpha^3+2i\alpha}{4}, \frac{3+2\alpha+\alpha^2+i+i\alpha^2}{4}, \frac{2+3\alpha+\alpha^3+i\alpha+i\alpha^3}{4}\right)$
5.	3, 7	0, 4	$\left(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^2+i}{2}, \frac{\alpha^3+i\alpha}{2}, \frac{1+i\alpha^2}{2}, \frac{\alpha+i\alpha^3}{2}\right)$
6.	3, 7	2, 6	$\left(1, \alpha, \alpha^2, \frac{1+\alpha+\alpha^2+\alpha^3}{2}, i, i\alpha, \frac{1+\alpha^2+i+i\alpha^2}{2}, \frac{1+\alpha^2+i\alpha+i\alpha^3}{2}\right)$
7.	5	0, 4	$\left(1, \alpha, \frac{1+\alpha^2}{2}, \frac{\alpha+\alpha^3}{2}, i, \frac{1+\alpha+i+i\alpha}{2}, \frac{i+i\alpha^2}{2}, \frac{1+\alpha+\alpha^2+\alpha^3+i+i\alpha+i\alpha^2+i\alpha^3}{4}\right)$

Proof of Theorem 3. Obviously,

$$\left(1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\right)$$

is a basis of $K = \mathbb{Q}(\alpha)$ over $\mathbb{Q}$ containing algebraic integers. The discriminant of this basis is $2^{24}(a^2 + b^2)^3$. Therefore the discriminant D_K of the field K divides $2^{24}(a^2 + b^2)^3$.

Considering the tower of fields $\mathbb{Q} \subset M = \mathbb{Q}(i) \subset K$, we obtain

$$D_K = 4^4 \cdot N_{M/\mathbb{Q}}(D_{K/M}),$$

where $D_{K/M}$ is the relative discriminant of K over M (see [8] Chapter IV., Proposition 4.15).

The minimal polynomial of α over $M = \mathbb{Q}(i)$ is $X^4 - (a + bi)$ with discriminant $4^4(a + bi)^3$. Since we assumed $a + bi \in \mathbb{Z}[i]$ to be square-free, for any prime π of $\mathbb{Z}_M$ dividing $a + bi$ the minimal polynomial of α is π-Eisenstein. By Lemma 1, this implies that for any prime $\pi \mid a + bi$, the basis $(1, \alpha, \alpha^2, \alpha^3)$ of K over M is π-maximal, i.e. $(a + bi)^3 \mid D_{K/M}$, hence $(a^2 + b^2)^3 \mid D_K$. Therefore we have:

$$2^8(a^2 + b^2)^3 \mid D_K \mid 2^{24}(a^2 + b^2)^3,$$

so the only prime which may divide the index of α is 2.

If both a and b are odd, then $1 + i \mid a + bi$, so by Lemma 1, the basis $(1, \alpha, \alpha^2, \alpha^3)$ of K over M is $1+i$-maximal and 2 does not divide the relative index of α over $\mathbb{Q}(i)$. In this case $(1, \alpha, \alpha^2, \alpha^3)$ is a relative power integral basis of K over M and therefore

$$\left(1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\right)$$

is an integral basis of K over $\mathbb{Q}$.

If a is even, and b is odd, then the minimal polynomial of $\alpha - 1$, $(X + 1)^4 - (a + bi)$ is also $(1 + i)$-Eisenstein. Hence by Lemma 1, $\mathbb{Z}_M[\alpha - 1]$ is $1 + i$-maximal, and so is $\mathbb{Z}_M[\alpha]$. We obtain again that $(1, \alpha, \alpha^2, \alpha^3)$ is a relative power integral basis of K over M and therefore

$$\left(1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\right)$$

is an integral basis of K over $\mathbb{Q}$.

The interesting case is when a is odd and b is even. (They can not be both even, because $a+bi$ is square-free.) This case splits into 6 subcases. The integral bases are listed in the table of the Theorem, as cases 2–7.

In these cases we showed, that the elements listed in the corresponding bases are always algebraic integers. These cases are very similar, we detail only one of them.

If $a = 8k + 1$ and $b = 8l + 4$, then

$$\beta = \frac{3 + \alpha + \alpha^2 + \alpha^3 + 2i\alpha}{4}$$

is an algebraic integer, because it is a root of the integer polynomial

$$\begin{aligned}
&X^8 - 6X^7 + (19 - 6k + 8l)X^6 + (-8k^2 + 8l^2 + 28k - 24l - 34)X^5 \\
&\quad + (-4k^3 + 12kl^2 + 49k^2 + 12kl + l^2 - 46k + 52l + 41)X^4 \\
&\quad + (36k^3 + 32k^2l - 12kl^2 + 32l^3 - 70k^2 - 4kl + 10l^2 + 44k - 54l - 32)X^3 \\
&\quad + (28k^4 + 32k^3l + 32k^2l^2 + 32kl^3 + 4l^4 - 36k^3 \\
&\quad + 6k^2l + 44kl^2 - 26l^3 + 59k^2 + 12kl + 3l^2 - 22k + 40l + 17)X^2 \\
&\quad + (16k^5 + 32k^3l^2 + 16kl^4 - 20k^4 + 20l^4 + 16k^3 \\
&\quad - 6k^2l - 16kl^2 + 42l^3 - 28k^2 - 8kl + 8l^2 + 4k - 16l - 6)X \\
&\quad + (4k^2 + 4l^2 + 4l + 1)(k^4 + 2k^2l^2 + l^4 + 2k^2l + 2l^3 + 3k^2 - l^2 - 2l + 1).
\end{aligned}$$

Furthermore, we checked that the given bases are 2-maximal by calculating the minimal polynomial of each element of the form

$$\frac{\lambda_1 B_1 + \lambda_2 B_2 + \lambda_3 B_3 + \lambda_4 B_4 + \lambda_5 B_5 + \lambda_6 B_6 + \lambda_7 B_7 + \lambda_8 B_8}{2},$$

where B is the basis given in the table, $\lambda_i \in \{0, 1\}$, $(i = 1, \dots, 8)$, $a = 8k + r$, $b = 8l + s$, $(k, l = 0, \dots, 255)$ with the corresponding remainders r, s modulo 8. For example, if $a = 8k+1$ and $b = 8l+4$, then by the theorem on symmetric polynomials, the minimal polynomial of

$$\beta = \lambda_1 B_1 + \lambda_2 B_2 + \lambda_3 B_3 + \lambda_4 B_4 + \lambda_5 B_5 + \lambda_6 B_6 + \lambda_7 B_7 + \lambda_8 B_8$$

is a polynomial of the form

$$X^8 + P_1(k,l)X^7 + P_2(k,l)X^6 + P_3(k,l)X^5 + P_4(k,l)X^4 \\ + P_5(k,l)X^3 + P_6(k,l)X^2 + P_7(k,l)X + P_8(k,l),$$

where $P_i \in \mathbb{Z}[X, Y]$. (If β is not primitive, then it is a power of its minimal polynomial, but it does not affect the proof.) Therefore, $\beta/2$ is an algebraic integer if and only if $P_i(k,l)/2^i \in \mathbb{Z}$ for all $i = 1, \dots, 8$. Since the P_i-s are integer polynomials, if $k \equiv k' \pmod{2^8}$ and $l \equiv l' \pmod{2^8}$, then $2^8 \mid P_i(k,l) - P_i(k',l')$. This means, that the integrality of $\beta/2$ depends only on the remainder of k and l modulo 2^8.

We did not find any algebraic integers in this form, which proves the 2-maximality. □

Remark. We do not use the assumption $b = 0$ in the proof of Theorem 3, so the given integral bases are valid also for the case $b = 0$ and for $K = \mathbb{Q}(\alpha, i)$. Cases 2. and 7. extends the results of [7] to the case $m \equiv 1 \pmod 4$.

5. Monogenity, relative monogenity

We investigate the relative and absolute monogenity of the field K in the seven distinct cases corresponding to the table of Theorem 3.

Theorem 4. *(1) If $b \equiv 1, 3, 5, 7 \pmod 8$ then K is relatively monogenic over M and there are infinitely many parameters a, b, for which K is absolutely monogenic. Moreover, there exists infinitely many paramters a, b, for which K admits at least 2 inequivalent generators of power integral bases.*

(2) If $a \equiv 1 \pmod 8$ and $b \equiv 0 \pmod 8$ then K is not relatively monogenic over M.

(3) If $a \equiv 1, 5 \pmod 8$ and $b \equiv 2, 6 \pmod 8$ then K is absolutely monogenic for $a = 1, b = \pm 2$, otherwise K is not relatively monogenic over M.

(4) If $a \equiv 1 \pmod 8$ and $b \equiv 4 \pmod 8$ then K is absolutely monogenic for $a = 1, b = \pm 4$, otherwise K is not relatively monogenic over M.

(5) If $a \equiv 3, 7 \pmod 8$ and $b \equiv 0, 4 \pmod 8$ then K is not relatively monogenic over M.

(6) If $a \equiv 3, 7 \pmod 8$ and $b \equiv 2, 6 \pmod 8$ then there are infinitely many parameters a, b, for which K admits a generator of a relative power integral basis over M.

(7) If $a \equiv 5 \pmod 8$ *and* $b \equiv 0, 4 \pmod 8$ *then* K *is relatively monogenic over* M.

Remarks:

- In the cases (6) and (7) we conjecture that K is not absolutely monogenic.
- The absolute monogenity of K implies the relative monogenity of K over M, but not conversely. Therefore, the cases (2), (3), (4) and (5) are interesting in the sense that in these cases K is absolutely monogenic if and only if it is relatively monogenic over M.

Proof of Theorem 4. In all cases we will use Lemma 2 with $a_1 = a_2 = a_3 = 0$ and $a_4 = -(a+bi)$. So to check whether some algebraic integer $\vartheta \in K$ of the form

$$\vartheta = \frac{A + X\alpha + Y\alpha^2 + Z\alpha^3}{d}, \qquad A, X, Y, Z \in \mathbb{Z}[i],\ d \in \mathbb{Z}, \tag{5}$$

generates a power integral basis, we have to solve the equations

$$\left(U^2 + 4(a+bi)V^2\right) \cdot U = \varepsilon \cdot \gamma, \tag{6}$$

$$X^2 - (a+bi)Z^2 = U, \tag{7}$$

$$Y^2 - XZ = V. \tag{8}$$

where ε is a unit in $\mathbb{Z}[i]$, and $\gamma \in \mathbb{Z}[i]$ is of norm $d^{12}/I_{K/M}(\alpha)$. We intend to use also the representation of $\vartheta \in \mathbb{Z}_K$ of the form

$$\vartheta = c_1 + c_2B_2 + c_3B_3 + c_4B_4 + c_5B_5 + c_6B_6 + c_7B_7 + c_8B_8, \qquad c_i \in \mathbb{Z}, \tag{9}$$

where $(1, B_2, B_3, B_4, B_5, B_6, B_7, B_8)$ is the integral basis given in Theorem 3. Considering these integral bases, we can see that for case (1) we have $d = 1$, for cases (3),(5) and (6) we have $d = 2$ and for cases (2),(4) and (7) we have $d = 4$. Furthermore, if S is the transition matrix form the basis $(1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3)$ to the basis $(1, B_2, B_3, B_4, B_5, B_6, B_7, B_8)$, then

$$A = d \cdot (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) \cdot S \cdot (1, 0, 0, 0, i, 0, 0, 0)^T, \tag{10}$$

$$X = d \cdot (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) \cdot S \cdot (0, 1, 0, 0, 0, i, 0, 0)^T, \tag{11}$$

$$Y = d \cdot (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) \cdot S \cdot (0, 0, 1, 0, 0, 0, i, 0)^T, \tag{12}$$

$$Z = d \cdot (c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) \cdot S \cdot (0, 0, 0, 1, 0, 0, 0, i)^T. \tag{13}$$

Assuming $b \neq 0$ we have $b \cdot i = \alpha^4 - a \in \mathbb{Z}[\alpha]$, so $(\mathbb{Z}_M[\alpha] : \mathbb{Z}[\alpha]) = b^4$, and therefore the square of the relative index of α is

$$I_{K/M}(\alpha)^2 = \frac{I(\alpha)^2}{b^8} = \frac{D(f)}{D_K \cdot b^8},$$

where $D(f) = 2^{24} \cdot (a^2+b^2) \cdot b^8$ is the discriminant of the minimal polynomial $f(x)$ of α and we applied the well-known fact $D(f) = I(\alpha)^2 \cdot D_K$. Since the discriminant of the basis $(1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3)$ is $2^{24}(a^2+b^2)$, which is equal to $D(f)/b^8$, and

$$D_K = \det(S)^2 \cdot 2^{24}(a^2+b^2),$$

then we have

$$I_{K/M}(\alpha) = \left| \frac{1}{\det(S)} \right|.$$

□

Proof of (1). In the first case $(1, \alpha, \alpha^2, \alpha^3)$ is a relative power integral basis of K over M. The relative index of α is $I_{K/M}(\alpha) = 1$ and we can choose $d = 1$, so γ is also a unit and the right hand side of equation (6) is ε. This equation implies $N_{M/\mathbb{Q}}(U) = 1$, $V = 0$. So, by Eq. (7), X and Z are coprime Gaussian integers, and therefore by Eq. (8) either $X \cdot Z = 0$ or both X and Z are associates of squares in $\mathbb{Z}[i]$.

If $X = 0$, then both $a + bi$ and Z are units, i.e. $a = 0, b = \pm 1$. In this case α generates an absolute power integral basis, not only a relative power integral basis in K. We note that this field K is the algebraic number field generated by the 16th roots of unity.

If $Z = 0$, then $Y = 0$ and X is a unit ε_X. This yields the solutions $\vartheta = A + \varepsilon_X \alpha$, which are relative equivalent to α, so they also generates a relative power integral basis in K over M. This ϑ also generates an absolute power integral basis if $b = \pm 1$, but otherwise we conjecture that the absolute index of ϑ is greater than 1.

If $X \cdot Z \neq 0$, then let $X = \varepsilon_X(s_1 + s_2 i)^2, Z = \varepsilon_Z(t_1 + t_2 i)^2$ and $Y = \varepsilon_Y(s_1 + s_2 i)(t_1 + t_2 i)$, where $\varepsilon_X, \varepsilon_Y$ and ε_Z are units in $\mathbb{Z}[i]$, such that $\varepsilon_Y^2 = \varepsilon_X \cdot \varepsilon_Z$. Equation (8) shows that

$$(s_1 + i s_2)^4 \pm (a + bi)(t_1 + i t_2)^4$$

is a unit (with either $+$ or $-$). By considering the real and the imaginary parts of this expression, we obtain the system of equations

$$\begin{aligned} a t_1^4 - 6a t_1^2 t_2^2 + a t_2^4 - 4b t_1^3 t_2 + 4b t_1 t_2^3 - s_1^4 + 6 s_1^2 s_2^2 - s_2^4 &= j \\ 4a t_1^3 t_2 - 4a t_1 t_2^3 + b t_1^4 - 6b t_1^2 t_2^2 + b t_2^4 - 4 s_1^3 s_2 + 4 s_1 s_2^3 &= k \end{aligned} \tag{14}$$

or

$$\begin{aligned} a t_1^4 - 6a t_1^2 t_2^2 + a t_2^4 - 4b t_1^3 t_2 + 4b t_1 t_2^3 + s_1^4 - 6 s_1^2 s_2^2 + s_2^4 &= j \\ 4a t_1^3 t_2 - 4a t_1 t_2^3 + b t_1^4 - 6b t_1^2 t_2^2 + b t_2^4 + 4 s_1^3 s_2 - 4 s_1 s_2^3 &= k \end{aligned} \tag{15}$$

where either $j = \pm 1, k = 0$ or $j = 0, k = \pm 1$. If s_1, s_2, t_1, t_2 are rational integers, such that a and b are rational integer solutions of the system of linear equations above, then ϑ generates a relative power integral basis in K corresponding to the current parameters a and b.

For certain parameters a, b there exist trivial solutions. For example, if Z is a unit, i.e. $t_1^2 + t_2^2 = 1$, then

$$-(a + bi) = \frac{U - X^2}{Z^2} = \pm(U - X^2),$$

so if

$$a = \pm \Re\left(U - X^2\right),$$

$$b = \pm \Im\left(U - X^2\right),$$

then the algebraic integer

$$\vartheta = A + X\alpha + Y\alpha^2 + Z\alpha^3$$

generates a relative power integral basis in K over M.

Moreover, there exist infinitely many parameters a, b for which the field K is monogenic. The simplest example is when we set $b = \pm 1$, and then the absolute index of α is also 1, because the discriminant $2^{24}(a^2+1)$ of f is equal to the discriminant of K.

We can go further, there exist infinitely many paramters a, b for which K admits at least 2 inequivalent generators of power integral bases. Let q be an arbitrary rational integer, $a = q^4$ and $b = -1$, then the minimal polynomial of

$$\beta = (\alpha + q)(\alpha - q)(iq - \alpha)$$

is

$$X^8 + 16q^6X^6 + 48q^5X^5 + 68q^4X^4 + 56q^3X^3 + 28q^2X^2 + 8qX + 1$$

with discriminant $2^{24}(q^8+1) = 2^{24}(a^2+b^2) = D_K$, so β also generates a power integral basis in K.

In order to find all monogenic fields K, and all generators of power integral bases, we have to find all solutions of (14) or (15), and then determine the imaginary part of A, such that the discriminant of ϑ (which is a polynomial in $\Im(A)$) is equal to the discriminant of K. □

Proof of (2). In the second case the relative index of α is $I_{K/M}(\alpha) = 2^8$ and we can use the common denominator $d = 4$, so γ is an algebraic integer of norm $4^{12}/2^8 = 2^{16}$. Up to associates, we can choose $\gamma = 256$ and then equation (6) is of the form

$$\left(U^2 + 4(a+bi)V^2\right) \cdot U = \varepsilon \cdot 256.$$

On the other hand, Eqs. (10)–(13) give

$$\begin{aligned} A &= 4c_1 + 2c_3 + c_4 + 2c_6 + c_7 + c_8 + i(4c_5 + 2c_6 + 3c_7 + 2c_8), \\ X &= 4c_2 + c_4 + 2c_6 + 2c_7 + 2c_8 + i(2c_6 + c_8), \\ Y &= 2c_3 + c_4 + c_7 + c_8 + ic_7, \\ Z &= c_4 + ic_8. \end{aligned}$$

Substituting these expressions into the Eqs. (6), (7) and (8), we can see that $u = U/4, v = V/2$ and $(u^2 + (a+bi)v^2)/4$ are Gaussian integers, so Eq. (6) can be written as

$$\frac{u^2 + (a+bi)v^2}{4} \cdot u = \varepsilon.$$

Let $F_1 = \frac{u^2+(a+bi)v^2}{4}$ and $F_2 = u$. Since $F_1 \cdot F_2 = \varepsilon$, then both factors have to be a unit, such that $a + bi$ is a divisor of $4F_1 - F_2^2$. To sum up, if the relative index of ϑ is 1, then $a + bi$ divides $3, 5, 1 - 4i$ or $1 + 4i$. With $a \equiv 1 \pmod 8$ and $b \equiv 0 \pmod 8$, $b \neq 0$ it is not possible, so there is no such algebraic integer ϑ, and therefore K is not relatively monogenic over M, and also not monogenic over $\mathbb{Q}$. □

Proof of (3). In this case the relative index of α is $I_{K/M}(\alpha) = 2^4$ and we can use the common denominator $d = 2$, so γ is an algebraic integer of norm $2^{12}/2^4 = 2^8$. Up to associates, the only Gaussian integer of norm 256 is $\gamma = 16$, so Eq. (6) is of the form

$$\left(U^2 + 4(a + bi)V^2\right) \cdot U = \varepsilon \cdot 16.$$

Equations (10)–(13) give

$$\begin{aligned} A &= 2c_1 + c_5 + c_6 + c_8 + ic_5, \\ X &= 2c_2 + c_5 + c_6 + c_7 + ic_6, \\ Y &= 2c_3 + c_6 + c_7 + c_8 + ic_7, \\ Z &= 2c_4 + c_5 + c_7 + c_8 + ic_8. \end{aligned}$$

Substituting these expressions into the Eqs. (6), (7) and (8), we can see that $u = U/2, v = V$ and $(u^2 + (a + bi)v^2)/2$ are Gaussian integers, so Eq. (6) is equivalent to

$$F_1 \cdot F_2 = \frac{u^2 + (a + bi)v^2}{2} \cdot u = \varepsilon.$$

Therefore, $a + bi$ divides $2F_1 - F_2^2$, where F_1 and F_2 are units. With $a \equiv 1, 5 \pmod 8$ and $b \equiv 2, 6 \pmod 8$ it is possible only if $F_1 = i, a = 1$ and $b = \pm 2$. In these cases K is indeed monogenic. For example

$$\beta = \frac{1 - i + i\alpha + i\alpha^3}{2}$$

generates a power integral basis. If $a = 1, b = 2$, then the minimal polynomial of β is

$$X^8 - 4X^7 + 10X^6 - 12X^5 + 12X^4 - 8X^3 + 6X^2 - 4X + 1,$$

and if $a = 1, b = -2$, then the minimal polynomial of β is

$$X^8 - 4X^7 + 10X^6 - 20X^5 + 32X^4 - 36X^3 + 28X^2 - 12X + 2.$$

In both cases, the discriminant of the polynomials are $2^{16} \cdot 5^3 = D_K$, so β generates a power integral basis in K.

For other values of a and b, K is not relatively monogenic over M, and therefore, K is not monogenic over $\mathbb{Q}$. □

Proof of (4). It is almost the same as Case (2), except the expressions for A, X, Y and Z. The relative index of α over M is $I_{K/M}(\alpha) = 2^8$ and $d = 4$. Equation (6) is of the form

$$\left(U^2 + 4(a + bi)V^2\right) \cdot U = \varepsilon \cdot 256,$$

and Eqs. (10)–(13) give

$$\begin{aligned} A &= 4c_1 + 2c_3 + c_5 + 3c_6 + 3c_7 + 2c_8 + i(2c_5 + c_7), \\ X &= 4c_2 + 2c_4 + 3c_5 + c_6 + 2c_7 + 3c_8 + i(2c_6 + c_8), \\ Y &= 2c_3 + c_5 + c_6 + c_7 + ic_8, \\ Z &= 2c_4 + c_5 + c_6 + c_8 + ic_8. \end{aligned}$$

Substituting these expressions into the Eqs. (6), (7) and (8) we obtain the same equations and conditions as in Case (2). If the relative index of ϑ is 1, then $a+bi$ divides $3, 5, 1+4i$ or $1-4i$. With $a \equiv 1 \pmod 8$ and $b \equiv 4 \pmod 8$, it is possible only if $a = 1$ and $b = \pm 4$. In these cases K is indeed monogenic. For $a = 1, b = 4$ and

$$\beta = \frac{2 + \alpha + \alpha^3 - i + i\alpha^2}{4},$$

the minimal polynomial of β is

$$X^8 - 4X^7 + 7X^6 - 6X^5 + 3X^4 - 2X^3 + 3X^2 - 2X + 1,$$

with discriminant $2^8 \cdot 17^3 = D_K$. So β generates a power integral basis in K.

If $a = 1, b = -4$, then the corresponding β has the minimal polynomial

$$X^8 - 4X^7 + 7X^6 - 8X^5 + 8X^4 - 6X^3 + 4X^2 - 2X + 1$$

with the same discriminant, so K is monogenic in this case too.

For other values of a and b, K is not relatively monogenic over M, and therefore, K is not monogenic over $\mathbb{Q}$. □

Proof of (5). This case is similar to Case 3. The relative index of α is $I_{K/M}(\alpha) = 2^4$ and we can use the common denominator $d = 2$, so Eq. (6) is of the form

$$\left(U^2 + 4(a+bi)V^2\right) \cdot U = \varepsilon \cdot 16.$$

Equations (10)–(13) give

$$\begin{aligned} A &= 2c_1 + c_7 + ic_5, \\ X &= 2c_2 + c_8 + ic_6, \\ Y &= 2c_3 + c_5 + ic_7, \\ Z &= 2c_4 + c_6 + ic_8. \end{aligned}$$

Substituting these expressions into the Eqs. (6), (7) and (8) we obtain that $u = U/4$ and $v = V$ are Gaussian integers. Then Eq. (6) is equivalent to

$$F_1 \cdot F_2 = (4u^2 + (a+bi)v^2) \cdot u = \varepsilon.$$

Thus $a+bi$ divides $F_1 - 4F_2^2$, i.e. $a+bi$ divides $3, 5, 1-4i$ or $1+4i$. With $a \equiv 3, 7 \pmod 8$, $b \equiv 0, 4 \pmod 8$ and $b \neq 0$, it is possible only if $a = -1$ and $b = \pm 4$, and therefore $F_1 = \pm i$. However, if $b = \pm 4$, then the imaginary part of $F_1 = 4u^2 + (a+bi)v^2$ is even, so there is no solution of the equation above, K is not relatively monogenic over M, and therefore, K is not monogenic over $\mathbb{Q}$. □

Proof of (7). This is a slightly more interesting case. The relative index of α is $I_{K/M}(\alpha) = 2^3$ and we can use the common denominator $d = 2$, so Eq. (6) is of the form

$$\left(U^2 + 4(a+bi)V^2\right) \cdot U = \varepsilon \cdot 16(1+i).$$

Equations (10)–(13) give

$$\begin{aligned} A &= 2c_1 + c_4 + c_7 + c_8 + i(2c_5 + c_7), \\ X &= 2c_2 + c_4 + i(2c_6 + c_8), \\ Y &= 2c_3 + c_4 + c_7 + c_8 + ic_7, \\ Z &= c_4 + ic_8. \end{aligned}$$

Substituting these expressions into the Eqs. (6), (7) and (8) we can see that $u = U/(2-2i)$ and $v = V/2$ are Gaussian integers. Thus,

$$F_1 \cdot F_2 = (u^2 + 2i(a+bi)v^2) \cdot u = \varepsilon.$$

Hence, $N_{M/\mathbb{Q}}(u) = 1$ and $2i(a+bi)$ divides $F_1 - F_2^2$. It is possible only if $F_1 - F_2^2 = 0$, i.e. $v = 0$. Similarly to the first case, there exist infinitely many solutions of the equations above. For example, if $Z = 1, U = 2 \pm 2i$ and $Y^2 = X$, where Y is not a multiple of $1+i$, then

$$a + bi = Y^4 - U.$$

Since $U = 2 \pm 2i$, and Y is not a multiple of $1+i$, then $a = \Re(Y^4 - U) \equiv 3 \pmod 4$ and $b = \Im(Y^4 - U) \equiv 2 \pmod 4$ as it is required in this case. Thus, there exist infinitely many parameters a, b, for which there exists an algebraic integer ϑ with relative index equal to 1. Despite the existence of generators of relative power integral bases, we could not find any parameters for which K is monogenic. □

Proof of (8). In the last case the relative index of α is $I_{K/M}(\alpha) = 2^6$ and we can use the common denominator $d = 4$, so γ is an algebraic integer of norm $4^{12}/2^6 = 2^{18}$. Up to associates, we can choose $\gamma = 512$ and then Eq. (6) is of the form

$$\left(U^2 + 4(a+bi)V^2\right) \cdot U = \varepsilon \cdot 512.$$

On the other hand, Eqs. (10)–(13) give

$$\begin{aligned} A &= 4c_1 + 2c_3 + 2c_6 + c_8 + i(4c_5 + 2c_6 + 2c_7 + c_8), \\ X &= 4c_2 + 2c_4 + 2c_6 + c_8 + i(2c_6 + c_8), \\ Y &= 2c_3 + c_8 + i(2c_7 + c_8), \\ Z &= 2c_4 + c_8 + ic_8. \end{aligned}$$

Substituting these expressions into the Eq. (6), (7) and (8), we can see that $u = U/8$ and $v = V/4$ are Gaussian integers, so Eq. (6) is equivalent to

$$F_1 \cdot F_2 = (u^2 + (a+bi)v^2) \cdot u = \varepsilon.$$

Hence, $N_{M/Q}(u) = 1$ and $(a+bi)$ divides $F_1 - F_2^2$. It is possible only if $F_1 - F_2^2 = 0$, i.e. $v = 0$. For any a and b

$$X = (1+i)^3, Y = 0, Z = 0$$

is a solution of (6),(7) and (8). These values give us

$$c_2 = -1, \quad c_3 = 0, \quad c_4 = 0, \quad c_6 = 1, \quad c_7 = 0, \quad c_8 = 0.$$

Therefore, $A = 4c_1 + 2 + i(4c_5 + 2)$, so for any a and b (with $a \equiv 5 \pmod 8$, $b \equiv 0, 4 \pmod 8$, $a^2 + b^2$ square-free),

$$\vartheta = \frac{4c_1 + 2 + i(4c_5 + 2) + (1 + i)^3\alpha}{4} = c_1 + ic_5 + \frac{i - \alpha}{1 + i}, \qquad c_1, c_5 \in \mathbb{Z},$$

generates a relative power integral basis in K over M. Despite the existence of generators of relative power integral bases, we could not find any parameters for which K is monogenic. □

6. Computational remarks

All calculations were perfomed on Maple [1] and were executed on a 12th Gen Intel Core i7 PC. The checking of the 2-maximality of the given bases required about 4 min. All other calculations took only some seconds.

Funding Information Open access funding provided by University of Debrecen.

Data availibility Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

[1] Char, B.W., Geddes, K.O., Gonnet, G.H., Monagan, M.B., Watt, S.M. (eds.): MAPLE. Watcom Publications, Waterloo, Canada, Reference Manual (1988)

[2] Gaál, I.: Power integral bases in composites of number fields. Can. Math. Bull. **41**(2), 158–165 (1998)

[3] Gaál, I.: Diophantine equations and power integral bases. Theory and algorithms, 2nd ed. Birkhäuser, Boston (2019)

[4] Gaál, I., Pohst, M.: Computing power integral bases in quartic relative extensions. J. Number Theory **85**, 201–219 (2000)

[5] Gaál, I., Remete, L.: Binomial Thue equations and power integral bases in pure quartic fields. JP J. Algebra Number Theory Appl. **32**(1), 49–61 (2014)

[6] Gaál, I., Remete, L.: Integral bases and monogenity of pure fields. J. Number Theory **173**, 129–146 (2017)

[7] Gaál, I., Remete, L.: Non-monogenity in a family of octic fields. Rocky Mt. J. Math. **47**(3), 817–824 (2017)

[8] Narkiewicz, W.: Elementary and analytic theory of algebraic numbers, 3rd edn. Springer Monogr, Math (2004)

István Gaál(✉) and László Remete
University of Debrecen, Mathematical Institute
Pf. 400, Debrecen 4002
Hungary
e-mail: gaal.istvan@unideb.hu

László Remete
e-mail: remete.laszlo@science.unideb.hu

László Remete
ELKH-DE Equations, Functions, Curves and their Applications Research Group
Debrecen
Hungary

Received: January 19, 2023.
Accepted: May 19, 2023.