Acta Scientiarum Mathematicarum (2023) 89:3–12
https://doi.org/10.1007/s44146-023-00081-y
Published online April 28, 2023

Acta Scientiarum Mathematicarum

Monogenity in totally real extensions of imaginary quadratic fields with an application to simplest quartic fields

István Gaál

Dedicated to Professor Michael Pohst on his 75th birthday.

Abstract. We describe an efficient algorithm to calculate generators of power integral bases in composites of totally real fields and imaginary quadratic fields with coprime discriminants. We show that the calculation can be reduced to solving index form equations in the original totally real fields. We illustrate our method by investigating monogenity in the infinite parametric family of imaginary quadratic extensions of the simplest quartic fields.

Mathematics Subject Classification. Primary 11R04, 11R16; Secondary 11Y50.

Keywords. Monogenity, Power integral basis, Totally real fields, Simplest quartic fields, Calculating the solutions.

1. Introduction

There is an extensive literature of monogenity of number fields and power integral bases, see [4,12]. A number field K of degree n is *monogenic* if its ring of integers $\mathbb{Z}_K$ is a simple ring extension of $\mathbb{Z}$, that is there exists $\alpha \in \mathbb{Z}_K$ with $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. In this case $(1, \alpha, \ldots, \alpha^{n-1})$ is an integral basis of K, called *power integral basis*. We also call α the *generator* of this power integral basis. The algebraic integer α generates a power integral basis if and only if its *index*

$$I(\alpha) = \sqrt{\left| \frac{D(\alpha)}{D_K} \right|}$$

is equal to 1, where $D(\alpha)$ is the discriminant of α.

Birkhäuser

The calculation of generators of power integral bases can be reduced to the resolution of certain diophantine equations, called *index form equations*, cf. [4].

There exist general algorithms for solving index form equations in cubic, quartic, quintic, sextic fields, however the general algorithms for quintic and sextic fields are already quite tedious, see [4]. Therefore it is worthy to develop efficient methods for the resolution of special types of higher degree number fields, cf. [4,8].

In some cases we considered monogenity in composites of fields, see [3,9]. In these cases the index form factorizes that makes the resolution of the index form equation easier.

On the other hand, considering totally real relative Thue equations over imaginary quadratic fields, it has turned out, that the relative Thue equations can be reduced to absolute Thue equations (over $\mathbb{Z}$), cf. [6]. A similar idea was used in [2,5].

In the present paper we study composites $K = LM$ of a totally real fields L and imaginary quadratic fields M. We show that in this case the resolution of the index form equation in K can be reduced to solving the index form equation in L. If L is of degree n, then the index form equation of L is of degree $n(n-1)/2$ in $n-1$ variables, but the index form equation in K is of degree $2n(2n-1)/2$ in $2n-1$ variables. Therefore our statement simplifies a lot the calculation of generators of power integral bases in fields of type K of degree $2n$.

Surprisingly the proofs of our statements are quite simple. However, they provide a powerful tool. Our Theorem 2 immediately implies some results of [3] (see our remarks after the proof of Theorem 2).

The strengh and usefulness of our results is aslo demonstrated in the application given in Sect. 4, where we consider composites of the so called simplest quartic fields and imaginary quadratic fields.

2. Composites of totally real fields and imaginary quadratic fields

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n having all roots $\xi = \xi^{(1)}, \ldots, \xi^{(n)}$ in $\mathbb{R}$. The field $L = \mathbb{Q}(\xi)$ is then totally real. Assume that L has integral basis $(\ell_1 = 1, \ell_2, \ldots, \ell_n)$ and discriminant D_L. We shall denote by $\gamma^{(j)}$ the conjugates of any $\gamma \in L$ $(j = 1, \ldots, n)$. The index form corresponding to the basis $(\ell_1 = 1, \ell_2, \ldots, \ell_n)$ is defined by

$$I_L(x_2, \ldots, x_n) = \frac{1}{\sqrt{|D_L|}} \prod_{1 \le j_1 < j_2 \le n} \left(x_2 \left(\ell_2^{(j_1)} - \ell_2^{(j_2)} \right) + \ldots + x_n \left(\ell_n^{(j_1)} - \ell_n^{(j_2)} \right) \right).$$

As it is known, $I_L(x_2, \ldots, x_n) \in \mathbb{Z}[x_2 \ldots, x_n]$ and for any $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ the algebraic integer element

$$\alpha = x_1 + x_2 \ell_2 + \ldots x_n \ell_n$$

generates a power integral basis $(1, \alpha, \ldots, \alpha^{n-1})$ if and only if

$$I_L(x_2, \ldots, x_n) = \pm 1.$$

Let $0 < d \in \mathbb{Z}$ be a square-free integer, set

$$\omega = \begin{cases} i\sqrt{d} & \text{if } d \equiv 1, 2 \pmod 4, \\ \dfrac{1 + i\sqrt{d}}{2} & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

The conjugates of ω are $\omega^{(1)} = \omega, \omega^{(2)} = \overline{\omega}$ (the complex conjugate of ω). Let $M = \mathbb{Q}(i\sqrt{d})$ with discriminant D_M.

Our purpose is to investigate the composite field $K = L \cdot M$ of degree 2ℓ and discriminant D_K. We assume $(D_L, D_M) = 1$. Then $(1, \ell_2, \ldots, \ell_n, \omega, \omega\ell_2, \ldots, \omega\ell_n)$ is an integral basis of K and $D_K = D_M^n \cdot D_L^2$ (cf. [12]).

In the ring of integers $\mathbb{Z}_K$ of K any element α can be represented as

$$\alpha = x_1 + x_2\ell_2 + \ldots x_n\ell_n + y_1\omega + y_2\omega\ell_2 + \ldots + y_n\omega\ell_n = X_1 + X_2\ell_2 + \ldots + X_n\ell_n, \tag{1}$$

with $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{Z}$ and $X_j = x_j + \omega y_j$ are elements in the ring $\mathbb{Z}_M$ of algebraic integers of M.

We shall use the following consequence of Theorem 1 of [3]:

Lemma 1. *If α of (1) generates a power integral basis in K then*

$$N_{M/Q}(I_L(X_2, \ldots, X_n)) = \pm 1 \tag{2}$$

and

$$N_{L/Q}(y_1 + y_2\ell_2 + \ldots + y_n\ell_n) = \pm 1. \tag{3}$$

The conjugates of α of (1) are obtained obviously as

$$\alpha^{(j,k)} = x_1 + x_2\ell_2^{(j)} + \ldots x_n\ell_n^{(j)} + y_1\omega^{(k)} + y_2\omega^{(k)}\ell_2^{(j)} + \ldots + y_n\omega^{(k)}\ell_n^{(j)},$$

for $j = 1, \ldots, n, k = 1, 2$. Note that the index form corresponding to the basis $(1, \ell_2, \ldots, \ell_n, \omega, \omega\ell_2, \ldots, \omega\ell_n)$ has three factors, two of them are the polynomials on the left hand sides of equations (2), (3). The third factor is

$$F(x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) = \prod_{1 \le j_1, j_2 \le n, j_1 \ne j_2} (\alpha^{(j_1,1)} - \alpha^{(j_2,2)}), \tag{4}$$

(cf. [3,4]). This is also a polynomial with coefficients in $\mathbb{Z}$. Equations (2), (3) together with

$$F(x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) = \pm 1 \tag{5}$$

are already equivalent to α generating a power integral basis.

In our main result we reduce the resolution of the relative index form equation (2) to the resolution of absolute equations, i.e. absolute inequalities. This makes the resolution of (2) much easier.

Theorem 2. *Assume α of (1) generates a power integral basis in K.*
If $d \equiv 1, 2 \pmod 4$, then

$$|I_L(x_2, \ldots, x_n)| \le 1 \tag{6}$$

and

$$|I_L(y_2,\dots,y_n)| \le \frac{1}{(\sqrt{d})^{n(n-1)/2}}. \tag{7}$$

If $d \equiv 3 \pmod 4$, *then*

$$|I_L(2x_2+y_2,\dots,2x_n+y_n)| \le 2^{n(n-1)/2} \tag{8}$$

and

$$|I_L(y_2,\dots,y_n)| \le \left(\frac{2}{\sqrt{d}}\right)^{n(n-1)/2}. \tag{9}$$

Proof of Theorem 2. According to the arguments in the proof of Theorem 1 of [3] we have

$$|N_{M/Q}(I_L(X_2,\dots,X_n))| = \prod_{k=1}^{2}\left(\frac{1}{\sqrt{|D_L|}}\prod_{1\le j_1<j_2\le n}\left|\alpha^{(j_1,k)}-\alpha^{(j_2,k)}\right|\right). \tag{10}$$

If $d \equiv 1,2 \pmod 4$, then

$$\mathrm{Re}(\alpha^{(j_1,k)}-\alpha^{(j_2,k)}) = x_2(\ell_2^{(j_1)}-\ell_2^{(j_2)})+\dots+x_n(\ell_n^{(j_1)}-\ell_n^{(j_2)})$$

and

$$\mathrm{Im}(\alpha^{(j_1,k)}-\alpha^{(j_2,k)}) = \sqrt{d}\cdot\left(y_2(\ell_2^{(j_1)}-\ell_2^{(j_2)})+\dots+y_n(\ell_n^{(j_1)}-\ell_n^{(j_2)})\right).$$

We have

$$\begin{aligned}
|I_L(x_2,\dots,x_n)|^2 &= |N_{M/Q}(I_L(x_2,\dots,x_n))| \\
&= \prod_{k=1}^{2}\left(\frac{1}{\sqrt{|D_L|}}\prod_{1\le j_1<j_2\le n}\left|x_2(\ell_2^{(j_1)}-\ell_2^{(j_2)})+\dots+x_n(\ell_n^{(j_1)}-\ell_n^{(j_2)})\right|\right) \\
&= \prod_{k=1}^{2}\left(\frac{1}{\sqrt{|D_L|}}\prod_{1\le j_1<j_2\le n}\left|\mathrm{Re}(\alpha^{(j_1,k)}-\alpha^{(j_2,k)})\right|\right) \\
&\le \prod_{k=1}^{2}\left(\frac{1}{\sqrt{|D_L|}}\prod_{1\le j_1<j_2\le n}\left|\alpha^{(j_1,k)}-\alpha^{(j_2,k)}\right|\right) \\
&= |N_{M/Q}(I_L(X_2,\dots,X_n))|,
\end{aligned}$$

whence by (2) we obtain (6). Similarly,

$$\left(\sqrt{d}\right)^{n(n-1)}|I_L(y_2,\ldots,y_n)|^2=\left(\sqrt{d}\right)^{n(n-1)}|N_{M/Q}(I_L(y_2,\ldots,y_n))|$$
$$=\prod_{k=1}^{2}\left(\frac{1}{\sqrt{|D_L|}}\prod_{1\le j_1<j_2\le n}\sqrt{d}\left|y_2(\ell_2^{(j_1)}-\ell_2^{(j_2)})+\ldots+y_n(\ell_n^{(j_1)}-\ell_n^{(j_2)})\right|\right)$$
$$=\prod_{k=1}^{2}\left(\frac{1}{\sqrt{|D_L|}}\prod_{1\le j_1<j_2\le n}\left|\mathrm{Im}(\alpha^{(j_1,k)}-\alpha^{(j_2,k)})\right|\right)$$
$$\le\prod_{k=1}^{2}\left(\frac{1}{\sqrt{|D_L|}}\prod_{1\le j_1<j_2\le n}\left|\alpha^{(j_1,k)}-\alpha^{(j_2,k)}\right|\right)$$
$$=|N_{M/Q}(I_L(X_2,\ldots,X_n))|,$$

whence by (2) we obtain (7).

If $d\equiv 3 \pmod 4$, then

$$\mathrm{Re}(\alpha^{(j_1,k)}-\alpha^{(j_2,k)})=\frac{2x_2+y_2}{2}\cdot(\ell_2^{(j_1)}-\ell_2^{(j_2)})+\ldots+\frac{2x_n+y_n}{2}\cdot(\ell_n^{(j_1)}-\ell_n^{(j_2)})$$

and

$$\mathrm{Im}(\alpha^{(j_1,k)}-\alpha^{(j_2,k)})=\sqrt{d}\cdot\left(\frac{y_2}{2}\cdot(\ell_2^{(j_1)}-\ell_2^{(j_2)})+\ldots+\frac{y_n}{2}\cdot(\ell_n^{(j_1)}-\ell_n^{(j_2)})\right).$$

The above arguments lead us to

$$\left|I_L\left(\frac{2x_2+y_2}{2},\ldots,\frac{2x_n+y_n}{2}\right)\right|\le 1$$

and

$$\left|I_L\left(\frac{y_2}{2},\ldots,\frac{y_n}{2}\right)\right|\le\frac{1}{(\sqrt{d})^{n(n-1)/2}},$$

whence we obtain (8) and (9), accordingly. □

Remark. Our Theorem 2 immediately implies the result of [3] on monogenity of composites of totally real cyclic fields of prime degree and imaginary quadratic fields, as well as on monogenity of composites of Lehmer's quintics and imaginary quadratic fields. In the next section we show that our result implies that the above statements of [3] hold for any composite of a totally real number field and an imaginary quadratic field.

3. Applying Theorem 2

Let $d\equiv 1,2$ (mod4). If $d=1$, then left hand side of both (6) and (7) is 1. Concerning inequality (6) this yields that either $I_(x_2,\ldots,x_n)=0$, that is $x_2=\ldots=x_n=0$ or $I_(x_2,\ldots,x_n)=\pm 1$, that is $\beta=x_2\ell_2+\ldots+x_n\ell_n$ generates a power integral basis in L. Similary, inequality (7) implies either $y_2=\ldots=y_n=0$, or $\gamma=y_2\ell_2+\ldots+y_n\ell_n$ generates a power integral basis in L. For given $y_2,\ldots,y_n$ we calculate y_1 from (3). We test all these $x_2,\ldots,x_n,y_1,y_2,\ldots,y_n$ in (5). Note that $x_2=\ldots=x_n=0$, and simultaneously $y_2 = \ldots = y_n = 0$ is not possible, since ω does not generate K.

If $d \neq 1$, then (7) gives $y_2 = \ldots = y_n = 0$ and (3) gives $y_1 = \pm 1$. The values of $x_2, \ldots, x_n$ are obtained from (6). If $I_L(x_2, \ldots, x_n) = 0$ then $x_2 = \ldots x_n = 0$ and $\alpha = \pm\omega$ which is again impossible, since ω does not generate K. Hence we have to take those $x_2, \ldots, x_n$ for which $I_L(x_2, \ldots, x_n) = \pm 1$, that is $\beta = x_2\ell_2 + \ldots + x_n\ell_n$ generates a power integral basis in L. We test all these $x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ in (5).

Let now $d \equiv 3 \pmod 4$.

If $d = 3$, then the right hand side of (8) is $2^{n(n-1)/2}$, the right hand side of (9) is $(2/\sqrt{3})^{n(n-1)/2}$. Hence we have to determine the elements $\beta = z_2\ell_2 + \ldots + z_n\ell_n$ having index $\leq 2^{n(n-1)/2}$ and to select from those the elements $\gamma = y_2\ell_2 + \ldots + y_n\ell_n$ having index $\leq (2/\sqrt{3})^{n(n-1)/2}$. We test if there exist $x_i \in \mathbb{Z}$ with $x_i = (z_i - y_i)/2$ for all $i = 2, \ldots, n$. For given $y_2, \ldots, y_n$ we calculate y_1 from (3). We test all possible $x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ in (5).

Otherwise, if $d \neq 3$, Eq (9) has left hand side < 1, therefore $y_2 = \ldots y_n = 0$ and (3) gives $y_1 = \pm 1$. In this case inequality (8) implies $|I_L(x_2, \ldots, x_n)| \leq 1$. $I_L(x_2, \ldots, x_n) = 0$ implies $x_2 = \ldots = x_n = 0$ which is not possible again. The equation $I_L(x_2, \ldots, x_n) = \pm 1$ yields that $\beta = x_2\ell_2 + \ldots + x_n\ell_n$ generates a power integral basis in L. We test all these $x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ in (5).

This means that for calculating generators of power integral basis in K we only need the generators of power integral bases in L and, in case $d = 3$, elements of small indices of L. This is easy to calculate in lower degree (cubic, quartic) fields, therefore we obtain an efficient method to calculate generators of power integral bases in sextic, octic fields, that are composites of totally real cubic, quartic fields and imaginary quadratic fields.

As a consequence of the above arguments we have

Theorem 3. *Under the above conditions, for $d \neq 1, 3$ the composite field $K = LM$ can only be monogenic if the totally real field L is monogenic. Additionally, if $d \neq 1, 3$ then all generators of power integral bases of K are of the form*

$$\alpha = x + \beta \pm \omega$$

where β generates a power integral basis in L and $x \in \mathbb{Z}$ is arbitrary.

Remark. Our Theorem 3 implies Theorem 2 of [3] on generators of power integral bases in composites of totally real cyclic fields of prime degree and imaginary quadratic fields.

4. Composites of the simplest quartic fields and imaginary quadratic fields

In this section we shall give an application to an infinite parametric family of number fields, that shows the strength of our method.

Let a be an integer with $a \neq 0, \pm 3$. Let ξ be a root of

$$f(x) = x^4 - ax^3 - 6x^2 + ax + 1.$$

The parametric family of fields $L = \mathbb{Q}(\xi)$ is called *simplest quartic fields*, see Gras [10]. She showed that for $a \neq 0, \pm 3$ the polynomial f is irreducible and $\mathbb{Q}(\xi) = \mathbb{Q}(-\xi)$, so we can assume $a > 0$ and $a \neq 3$. In the following we shall also assume that a^2+16 is not divisible by an odd square. This condition was needed by Kim and Lee [11] to determine an integral basis of L. (Gras [10] showed that $a^2 + 16$ represents infinitely many square free integers.) Using the discriminant

$$D(f) = 4(a^2 + 16)^3$$

of the polynomial we obtain the discriminant of L. Let $v_2(x)$ denote the exponent of 2 in the prime power decomposition of the integer x.

Lemma 4. *Under the above assumptions on the parameter a an integral basis and the discriminant of L is given by*

$$\begin{aligned}
\left(1, \xi, \xi^2, \tfrac{1+\xi^3}{2}\right), \; D_L &= (a^2+16)^3, \text{ if } v_2(a) = 0,\\
\left(1, \xi, \tfrac{1+\xi^2}{2}, \tfrac{\xi+\xi^3}{2}\right), \quad D_L &= \tfrac{(a^2+16)^3}{4}, \quad \text{if } v_2(a) = 1,\\
\left(1, \xi, \tfrac{1+\xi^2}{2}, \tfrac{1+\xi+\xi^2+\xi^3}{4}\right), \quad D_L &= \tfrac{(a^2+16)^3}{16}, \quad \text{if } v_2(a) = 2,\\
\left(1, \xi, \tfrac{1+2\xi-\xi^2}{4}, \tfrac{1+\xi+\xi^2+\xi^3}{4}\right), \quad D_L &= \tfrac{(a^2+16)^3}{64}, \quad \text{if } v_2(a) \geq 3.
\end{aligned}$$

Olajos [13] determined all generators of power integral bases (up to sign and translation by elements of $\mathbb{Z}$).

Lemma 5. *Under the above assumptions on the parameter a a power integral basis in L exists only for $a = 2$ and $a = 4$. All generators of power integral bases are given by*

- $a = 2$, $\alpha = x\xi + y\frac{1+\xi^2}{2} + z\frac{\xi+\xi^3}{2}$ *where*
  $(x, y, z) = (4, 2, -1), (-13, -9, 4), (-2, 1, 0), (1, 1, 0),$
  $(-8, -3, 2), (-12, -4, 3), (0, -4, 1), (6, 5, -2), (-1, 1, 0), (0, 1, 0)$
- $a = 4$, $\alpha = x\xi + y\frac{1+\xi^2}{2} + z\frac{1+\xi+\xi^2+\xi^3}{4}$ *where*
  $(x, y, z) = (3, 2, -1), (-2, -2, 1), (4, 8, -3), (-6, -7, 3),$
  $(0, 3, -1), (1, 3, -1).$

Note also that Gaál and Petrányi [7] calculated the minimal indices and all elements of minimal index for all parameters a.

Our purpose is to study composites of simplest quartic fields with imaginary quadratic fields.

Let d be a squarefree positive integer, $M = \mathbb{Q}(i\sqrt{d})$. Set

$$\omega = i\sqrt{d} \;\text{ if }\; d \equiv 1, 2 \pmod 4 \;\text{ and }\; \omega = \frac{1 + i\sqrt{d}}{4} \;\text{ if }\; d \equiv 3 \pmod 4.$$

We assume that $(D_M, D_L) = 1$. If $v_2(a) \geq 1$ then D_L is even, hence in that case we must have $d \equiv 3 \pmod 4$, since $D_M = -4d$ if $d \equiv 1, 2 \pmod 4$.

We consider monogenity of the composite field $K = LM$ of degree 8. This is an infinite parametric family of octic fields, depending on the parameters d, a.

We show:

Theorem 6. *Under the above conditions for $d \neq 3$ the field K is not monogenic.*

Proof of Theorem 6. For a given parameter a denote by $(1, \ell_2, \ell_3, \ell_4)$ an integral basis of L. Denote by $I_L(x_2, x_3, x_4)$ the index form corresponding to this integral basis. The condition $(D_L, D_M) = 1$ implies that an integral basis of K is given by $(1, \ell_2, \ell_3, \ell_4, \omega, \omega\ell_2, \omega\ell_3, \omega\ell_4)$. Represent any $\alpha \in \mathbb{Z}_K$ in the form

$$\alpha = x_1 + x_2\ell_2 + x_3\ell_3 + x_4\ell_4 + y_1\omega + y_2\omega\ell_2 + y_3\omega\ell_3 + y_4\omega\ell_4$$

with integer coefficients x_i, y_i $(1 \leq i \leq 4)$.

I. Assume $d \neq 1$. In this case, by Theorem 3 and Lemma 5, the field K can only be monogenic if $a = 2$ or $a = 4$. Since in both cases we have $v_2(a) \geq 1$, then we must have $d \equiv 1 \pmod 4$. Further, by Theorem 3, if α generates a power integral basis in K, then $y_2 = y_3 = y_4 = 0, y_1 = \pm 1$ and $\beta = x_2\ell_2 + x_3\ell_3 + x_4\ell_4$ generates a power integral basis in L. By Lemma 5, for $a = 2$ and $a = 4$ all possible x_2, x_3, x_4 are known.

Now, we consider the third factor (5) of the index form equation of K for $d \equiv 1 (\text{mod } 4)$, $d \neq 1$. In both cases $a = 2$ and $a = 4$ we substitute the possible x_2, x_3, x_4 and $y_2{=}y_3{=}y_4{=}0, y_1{=}\pm 1$ into $F(x_2, x_3, x_4, y_1, y_2, y_3, y_4)$. In all cases we obtain a polynomial of degree 6 in $d > 1$ with positive coefficients, implying that $F(x_2, x_3, x_4, y_1, y_2, y_3, y_4) = \pm$ is not possible.

II. Let now $d = 1$. As we showed at the beginning of Sect. 3, in this case all generators of power integral bases in K can be written in the form

$$\alpha = x_1 + y_1\omega + \varepsilon_1\beta + \varepsilon_2\gamma\omega \tag{11}$$

where $\beta = x_2\ell_2 + x_3\ell_3 + x_4\ell_4$ and $\gamma = y_2\ell_2 + y_3\ell_3 + y_4\ell_4$ are generators of power integral bases in L, $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$, $(\varepsilon_1, \varepsilon_2) \neq (0, 0)$ and $x_1 \in \mathbb{Z}$ is arbitrary. Therefore, by Lemma 5 the field K can be monogenic only if $a = 2$ or $a = 4$. Since, in both cases $a = 2$ and $a = 4$ all possible x_2, x_3, x_4 and y_2, y_3, y_4 are given in Lemma 5, we have to consider Eq (5) in the following three cases:

a. If $(\varepsilon_1, \varepsilon_2) = (1, 0)$ then the possible x_2, x_3, x_4 corresponding to $a = 2$ and $a = 4$ are listed in Lemma 5, $y_2 = y_3 = y_4 = 0$ and (3) gives $y_1 = \pm 1$. We substitute the possible values of the variables into $F(x_2, x_3, x_4, y_1, y_2, y_3, y_4)$ and find that in all cases it takes huge values, not ± 1.

b. If $(\varepsilon_1, \varepsilon_2) = (0, 1)$ then $x_2 = x_3 = x_4 = 0$ and the possible y_2, y_3, y_4 corresponding to $a = 2$ and $a = 4$ are listed in Lemma 5. We substitute the possible values of the variables into $F(x_2, x_3, x_4, y_1, y_2, y_3, y_4)$ and obtain a polynomial of degree 12 in y_1. Solving $F(x_2, x_3, x_4, y_1, y_2, y_3, y_4) = \pm 1$ in y_1 we never get integer solutions for y_1.

c. If $(\varepsilon_1, \varepsilon_2) = (1, 1)$ then x_2, x_3, x_4 and y_2, y_3, y_4 (corresponding to $a = 2$ or $a = 4$) may run independently through the possible triplets listed in Lemma 5. In all cases, we substitute x_2, x_3, x_4 and y_2, y_3, y_4 into $F(x_2, x_3, x_4, y_1, y_2, y_3, y_4)$ and obtain a polynomial of degree 12 in y_1.

Solving $F(x_2, x_3, x_4, y_1, y_2, y_3, y_4) = \pm 1$ in y_1 we never get integer solutions for y_1.

□

Remark. The case $a = 3$ is not covered by Theorem 6. In this case we have

$$|I_L(2x_2 + y_2, 2x_3 + y_3, 2x_4 + y_4)| \leq 64$$

and

$$|I_L(y_2, y_3, y_4)| \leq 2.$$

According to [7] we have minimal index 2 in L for infinitely many parameters a. Especially the elements of index ≤ 64 seems very difficult to determine. This could be the subject of a further research.

Remark. Note that in [9] we obtained conditions on the monogenity of composites of fields, among others of simplest quartic fields and quadratic fields. We did not assume that the discriminants are relative prime and involved also real quadratic fields. However we only obtained certain divisibility conditions on the parameters as a consequence of monogenity.

5. One more example

We also provide a positive example to show that such composite fields may happen to be monogenic. Consider the totally real quartic field L generated by a root ξ of the polynomial $f(x) = x^4 - 4x^2 - x + 1$. In this field $(1, \xi, \xi^2, \xi^2)$ is an integral basis and $D_L = 1957$. Let $M = \mathbb{Q}(i)$ with $D_M = -4$, coprime to D_L. The composite field $K = LM$ can be generated e.g. by $\alpha = i\xi$ having minimal polynomial $g(x) = x^8 + 8x^6 + 18x^4 + 9x^2 + 1$. In K the element α generates a power integral basis. Note that the generator $\alpha = i\xi$ is of the form (11) with $(\varepsilon_1, \varepsilon_2) = (0, 1)$.

6. Computational aspects

All calculations connected with the above examples were performed in Maple [1]. Our procedures were executed on an average laptop running under Windows. The CPU time took all together some seconds.

Acknowledgements

The author is grateful to the anonymous referee whose valuable comments have considerably improved the quality of the paper.

References

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

[2] Gaál, I.: Computing elements of given index in totally complex cyclic sextic fields. J. Symbolic Comput. **20**(1), 61–69 (1995)

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

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

[5] Gaál, I.: Monogenity in totally complex sextic fields, revisited. J. Pure Appl. Math. **47**(1), 87–98 (2020)

[6] Gaál, I., Jadrijević, B., Remete, L.: Totally real Thue inequalities over imaginary quadratic fields. Glasnik Mathematicki **53**(2), 229–238 (2018)

[7] Gaál, I., Petrányi, G.: Calculating all elements of minimal index in the infinite parametric family of simplest quartic fields. Czech. Math. J. **64**(2), 465–475 (2014)

[8] Gaál, I., Remete, L.: Power integral bases in a family of sextic fields with quadratic subfields. Tatra Mt. Math. Publ. **64**, 59–66 (2015)

[9] Gaál, I., Remete, L.: Integral bases and monogenity of composite fields. Exp. Math. **28**(2), 209–222 (2019)

[10] Gras, M.N.: Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$, Publ. Math. Fac. Sci. Besancon, Théor. Nombres, Année 1977-1978, Fasc. 2, (1978). (In French.)

[11] Kim, H.K., Lee, J.H.: Evaluation of the Dedekind zeta function at $s = -1$ of the simplest quartic fields. Trends Math. New Ser. Inf. Center Math. Sci. **11**, 63–79 (2009)

[12] Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers, 3rd edn. Springer, Berlin (2004)

[13] Olajos, P.: Power integral bases in the family of simplest quartic fields. Exp. Math. **14**(2), 129–132 (2005)

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

Received: September 8, 2020.
Accepted: February 1, 2022.