Power integral bases in families of number fields

doktori (PhD) értekezés

Olajos Péter

Debreceni Egyetem

Debrecen, 2004

Köszönetnyilvánítás

Ezúton is szeretnék köszönetet mondani mindazoknak, akik közvetve vagy közvetlenül hozzájárultak a disszertációm elkészítéséhez.

Szüleimnek, akik felneveltek, segítettek és elindítottak az életben,

Témavezetőmnek, Dr. Gaál Istvánnak, aki megszerettette velem a számelméletet, azért a rengeteg hasznos tanácsért, útmutatásért, kitartásért és segítségért, amely nélkül ez a dolgozat nem készülhetett volna el,

Tanáraimnak, Dr. Győry Kálmánnak és Dr. Pethő Attilának, akiktől nagyon sokat tanultam és tanulok,

Doktorandusz társaimnak, debreceni és egri kollégáimnak,
Járási Istvánnak, Nyul Gábornak, Rakaczki Csabának, Pink Isvánnak,
Dr. Hajdu Lajosnak, Dr. Pintér Ákosnak, Dr. Turjányi Sándornak,
Dr. Liptai Kálmánnak, Dr. Mátyás Ferencnek, akikhez bármikor segítségért fordulhattam.

Contents

Introduction

This thesis consists of three chapters, all containing recent publications [30], [15], [10], [31] and [32] of the author. Before giving an overview of the contents of the chapters, we would like to emphasize the main subject of our thesis.

Consider an algebraic number field K of degree n with ring of integers $\mathbb{Z}_K$. An interesting problem in algebraic number theory is to decide if there exists an element α in K such that

$$1, \alpha, \alpha^2, ..., \alpha^{n-1}$$

is an integral basis, that is a *power integral basis*. The ring $\mathbb{Z}_K$ of integers is called *monogenic*, if K admits power integral bases. Another problem is to find all elements α which generate power integral bases in K.

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

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

Then we have

$$I(\alpha) = \frac{\prod_{1 \le j < k \le n} |\alpha^{(j)} - \alpha^{(k)}|}{\sqrt{|D_K|}}, \tag{1}$$

where D_K is the discriminant of K.

As it is well known α generates a power integral basis if and only if $I(\alpha) = 1$.

Let $\{1, \omega_2, ..., \omega_n\}$ be an arbitrary integral basis of K. Then the discriminant of the linear form

$$l(x) = x_1 + x_2\omega_2 + ... + x_n\omega_n$$

is equal to

$$D_{K/\mathbb{Q}}(l(x)) = \prod_{1 \le i < j \le n} (l^{(i)}(x) - l^{(j)}(x))^2 = I(x_2, ..., x_n)^2 D_K,$$

where $x = (x_1, x_2, ..., x_n) \in \mathbb{Z}^n$ and $I(x_2, ..., x_n)$ is a homogeneous form of degree $\frac{n(n-1)}{2}$ in $n-1$ variables with coefficients in $\mathbb{Z}$ called *the index form* corresponding to the integral basis $\{1, \omega_2, ..., \omega_n\}$.

Representing any α of $\mathbb{Z}_K$ in the form $\alpha = x_1 + \omega_2 x_2 + ... + \omega_n x_n$ we have

$$I(\alpha) = |I(x_2, ..., x_n)|,$$

that is the index of α is independent from the first coordinate of α. That is we have to solve the following equation to find all generators of power integral bases:

$$I(x_2, ..., x_n) = \pm 1 \text{ (in } x_2, \ldots, x_n \in \mathbb{Z}). \tag{2}$$

In 1976 K. Győry (see [18], [20] and [19]) gave the first general effective upper bounds for the solutions of index form equations using Baker's method (see also [21] for recent improvements). It means that we have only finitely many solutions of the equation (2).

In the last decade several authors were interested in constructing algorithms for solving index form equations. There are efficient algorithms for determining all generators of power integral bases in lower degree number fields cf. I. Gaál and N. Schulte [16] for cubic fields, I. Gaál, A. Pethő and M. Pohst [11] for quartic fields. A general algorithm for quintic and sextic fields was given by I. Gaál and K. Győry [9] and Y. Bilu, I. Gaál and K. Győry [1], which already requires several hours of CPU time. For algorithms for solving index form equations in certain special sextic, octic, nonic fields see I. Gaál [3], I. Gaál [5], I. Gaál and M. Pohst [13], I. Járási [22]. A complete description of algorithms for solving equation (2) and several connected results can be found in the monograph I. Gaál [8].

I

For higher degree number fields this problem is very complicated because of the high degree and large number of variables in equation (2). The resolution of the equation (2) is only hopeful if K is a composite of certain subfields, because in this case the index form is reducible. Interesting and well applicable necessary conditions are known for the existence of power integral bases. The purpose of the first chapter is to give a summary of these results in composite fields. We consider several applications of these results.

II

In this chapter we give all generators of power integral bases in the infinite parametric family of simplest quartic fields.

Let $t \in \mathbb{Z}$ and α be a root of $P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1$ and consider the infinite parametric family of number fields $K_t = K = \mathbb{Q}(\alpha)$. These fields K are totally real cyclic number fields of degree 4 and are called "simplest" quartic fields. Several authors have considered the infinite parametric family of simplest quartic fields K(see [17],[26] and [28]). The generators of power integral bases of the polynomial ring $\mathbb{Z}[\alpha]$ have already been described. In our case under certain conditions on t we explicitly give all generators of power integral bases in the ring of integers $\mathbb{Z}_K$ of K.

III

In the third chapter similarly to the first chapter we consider a parametric family of degree 6 which has a special structure. We know that if a sextic field has a quadratic subfield, then a factor of the index form leads to a relative Thue equation over the quadratic subfield. Algorithms for the resolution of index form equations in totally real cyclic sextic fields are developed by I. Gaál [4], in sextic fields with an imaginary quadratic subfield by I. Gaál and M. Pohst [13].

In this chapter we analyse the problem of determining elements of given index in a special infinite parametric family of sextic number fields with imaginary quadratic subfields, having also a totally real cubic subfield. Using results of I. Gaál [3] our problem can be reduced to solving cubic Thue inequalities over $\mathbb{Z}$. Fast algorithms are known for solving cubic (or higher degree) Thue equations or inequalities (see [2]). Moreover, using direct computations we also deal with those fields in the family which correspond to small parameters and are not covered by the main theorem.

Chapter 1

Composite fields

1.1 Coprime discriminants

Let L be a number field of degree r with integral basis $\{l_1 = 1, l_2, \ldots, l_r\}$ and discriminant D_L. Denote the index form corresponding to the integral basis $\{l_1 = 1, l_2, \ldots, l_r\}$ of L by $I_L(x_2, \ldots, x_r)$. Similarly, let M be a number field of degree s with integral basis $\{m_1 = 1, m_2, \ldots, m_s\}$ and discriminant D_M. Denote the index form corresponding to the integral basis $\{m_1 = 1, m_2, \ldots, m_s\}$ of M by $I_M(x_2, \ldots, x_s)$. Let $K = LM$ the composite of L and M. As it is known, if $(D_L, D_M) = 1$ the discriminant of K is

$$D_K = D_L^s \cdot D_M^r$$

and an integral basis of K is given by

$$\{l_i \cdot m_j : 1 \leq i \leq r,\ 1 \leq j \leq s\}.$$

Hence, any integer α of K can be represented in the form

$$\alpha = \sum_{i=1}^{r} \sum_{j=1}^{s} x_{ij} \cdot l_i \cdot m_j \tag{1.1}$$

with $x_{ij} \in \mathbb{Z}$ $(1 \leq i \leq r,\ 1 \leq j \leq s)$.

I. Gaál [5] formulated a general necessary condition for $\alpha \in \mathbb{Z}_K$ to be a generator of a power integral basis of K.

Theorem 1. *(I. Gaál, [5])*
Assume $(D_L, D_M) = 1$. *If* α *of (1.1) generates a power integral basis in* $K = LM$ *then*

$$N_{M/Q}\left(I_L\left(\sum_{i=1}^{s} x_{2i}\cdot m_i,\ldots,\sum_{i=1}^{s} x_{ri}\cdot m_i\right)\right) = \pm 1 \tag{1.2}$$

and

$$N_{L/Q}\left(I_M\left(\sum_{i=1}^{r} x_{i2}\cdot l_i,\ldots,\sum_{i=1}^{r} x_{is}\cdot l_i\right)\right) = \pm 1. \tag{1.3}$$

1.1.1 Applications of Theorem 1

Example: Field of degree nine with cubic subfields (see I. Gaál [7]).

Let f, g be monic, irreducible cubic polynomials with integer coefficients. Denote one of the roots of f and g by ϕ and ψ, respectively. Let us consider the algebraic number fields $L = \mathbb{Q}(\phi)$ and $M = \mathbb{Q}(\psi)$. Using the assumptions above the following cases were considered in [7]:

1. $f(x) = x^3 - x + 1,\ D_L = -23, \quad g(x) = x^3 - 2x + 2,\ D_M = -76$
2. $f(x) = x^3 + x + 1,\ D_L = -31, \quad g(x) = x^3 + x^2 + x + 2,\ D_M = -83$
3. $f(x) = x^3 + 2x + 1,\ D_L = -59, \quad g(x) = x^3 + x^2 - 2x - 3.\ D_M = -87$

Using Theorem 1 it was shown that there are no generators of power integral bases in the composite field $K = LM$. In these cases (1.2) and (1.3) yield relative Thue equations.

1.2 Notation

In the subsections below we will use the following notation:
Let $f, g \in \mathbb{Z}[x]$ be distinct monic irreducible polynomials (over $\mathbb{Q}$) of degrees m and n, respectively. Let φ be a root of f and let ψ be a root of g. Set $L = \mathbb{Q}(\varphi)$, $M = \mathbb{Q}(\psi)$ and assume that the composite field $K = LM$ has degree mn. Denote by $d(f)$ and $d(g)$ the discriminants of the polynomials f and g, respectively.

Consider the order $\mathcal{O}_f = \mathbb{Z}[\varphi]$ of the field L, the order $\mathcal{O}_g = \mathbb{Z}[\psi]$ of the field M and the composite order $\mathcal{O}_{fg} = \mathcal{O}_f\mathcal{O}_g = \mathbb{Z}[\varphi, \psi]$ in the composite field $K = ML$. Note that $\{1, \varphi, \dots, \varphi^{m-1}\}$, $\{1, \psi, \dots, \psi^{n-1}\}$ and

$$\{1, \varphi, \dots, \varphi^{m-1}, \psi, \varphi\psi, \dots, \varphi^{m-1}\psi, \dots, \psi^{n-1}, \varphi\psi^{n-1}, \dots, \varphi^{m-1}\psi^{n-1}\},$$

are $\mathbb{Z}$-bases of $\mathcal{O}_f$, $\mathcal{O}_g$ and $\mathcal{O}_{fg}$, respectively.

1.3 Non-coprime discriminants

If the condition of Theorem 1 is satisfied then we have to solve equations (1.2) and (1.3) which can be very complicated. But we can give other sufficient conditions for the non-existence of power integral basis.

Assume that there is a prime number q, $(q > 2)$ such that both f and g have a multiple linear factor (at least square) mod q, that is, there exist a_f and a_g in $\mathbb{Z}$ such that

$$\begin{array}{rcccl} f(a_f) & \equiv & f'(a_f) & \equiv & 0 \pmod{q}, \\ g(a_g) & \equiv & g'(a_g) & \equiv & 0 \pmod{q}. \end{array} \tag{1.4}$$

Remark 1. Our assumption implies that q divides both the discriminant $d(f)$ of the polynomial f and the discriminant $d(g)$ of g.

Remark 2. In [5] we considered fields that are composites of subfields with coprime discriminants. According to the remark above in our case the fields we consider are composites of subfields whose discriminants are not necessarily coprime. This is the case in many interesting examples some of which we list at the end of this section.

Our result is the following (see [15]):

Theorem 2. *(I. Gaál, P. Olajos, M. Pohst, [15])*
Under the assumptions above the index of any primitive element of the order $\mathcal{O}_{fg}$ is divisible by q.

As a consequence we have:

Theorem 3. *(I. Gaál, P. Olajos, M. Pohst, [15])*
Under the assumptions above the order $\mathcal{O}_{fg}$ has no power integral bases.

1.3.1 Proof of Theorem 2

Denote the conjugates of $\varphi \in L$ by $\varphi^{(i)}$ $(1 \le i \le m)$ and the conjugates of $\psi \in M$ by $\psi^{(j)}$ $(1 \le j \le n)$. Denote by $\gamma^{(i,j)}$ the conjugate of any element $\gamma \in K$ under the automorphism mapping φ to $\varphi^{(i)}$ and ψ to $\psi^{(j)}$ $(1 \le i \le m, 1 \le j \le n)$.

The discriminants of the polynomials f and g are

$$\begin{aligned} d(f) &= \prod_{1 \le i < j \le m} (\varphi^{(i)} - \varphi^{(j)})^2 \\ d(g) &= \prod_{1 \le i < j \le n} (\psi^{(i)} - \psi^{(j)})^2. \end{aligned} \tag{1.5}$$

These are also the discriminants of the bases $\{1, \varphi, \ldots, \varphi^{m-1}\}$ of the order $\mathcal{O}_f$ and $\{1, \psi, \ldots, \psi^{n-1}\}$ of the order $\mathcal{O}_g$, respectively. The discriminant of the order $\mathcal{O}_{fg}$ is

$$D(\mathcal{O}_{fg}) = d(f)^n \cdot d(g)^m. \tag{1.6}$$

We can represent any element $\alpha \in \mathcal{O}_{fg}$ in the form

$$\alpha = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \varphi^i \psi^j \tag{1.7}$$

with $x_{ij} \in \mathbb{Z}$. The index of α corresponding to the order $\mathcal{O}_{fg}$ (that is $(\mathcal{O}_{fg}^+ : \mathcal{O}_{fg}^+[\alpha])$) is

$$I_{\mathcal{O}_{fg}}(\alpha) = \frac{1}{\sqrt{|D(\mathcal{O}_{fg})|}} \prod_{(i_1,j_1)<(i_2,j_2)} \left| \alpha^{(i_1,j_1)} - \alpha^{(i_2,j_2)} \right|$$

where the pairs of indices are ordered lexicographically. Now we rearrange the factors in the product above. Using (1.5) and (1.6) we have

$$\begin{aligned} I_{\mathcal{O}_{fg}}(\alpha) &= \prod_{i=1}^{m} \prod_{1 \le j_1 < j_2 \le n} \left| \frac{\alpha^{(i,j_1)} - \alpha^{(i,j_2)}}{\psi^{(j_1)} - \psi^{(j_2)}} \right| \cdot \\ &\quad \prod_{j=1}^{n} \prod_{1 \le i_1 < i_2 \le m} \left| \frac{\alpha^{(i_1,j)} - \alpha^{(i_2,j)}}{\varphi^{(i_1)} - \varphi^{(i_2)}} \right| \cdot \\ &\quad \prod_{\substack{(i_1,j_1)<(i_2,j_2) \\ i_1 \ne i_2,\ j_1 \ne j_2}} \left| \alpha^{(i_1,j_1)} - \alpha^{(i_2,j_2)} \right|. \end{aligned} \tag{1.8}$$

Obviously, the factors that appear in (1.8) are algebraic integers.

For any $1 \le i_1 < i_2 \le m$ and $1 \le j_1 < j_2 \le n$ we have

$$\left(\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_1)}\right) + \left(\alpha^{(i_2,j_1)} - \alpha^{(i_2,j_2)}\right) + \left(\alpha^{(i_2,j_2)} - \alpha^{(i_1,j_1)}\right) = 0$$

which implies the equation

$$\left(\varphi^{(i_1)} - \varphi^{(i_2)}\right)\varepsilon + \left(\psi^{(j_1)} - \psi^{(j_2)}\right)\eta + \rho = 0 \tag{1.9}$$

with

$$\varepsilon = \frac{\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_1)}}{\varphi^{(i_1)} - \varphi^{(i_2)}}, \quad \eta = \frac{\alpha^{(i_2,j_1)} - \alpha^{(i_2,j_2)}}{\psi^{(j_1)} - \psi^{(j_2)}}, \quad \rho = \alpha^{(i_2,j_2)} - \alpha^{(i_1,j_1)}.$$

Since these elements are factors in (1.8), hence they are algebraic integers lying in the $\mathbb{Z}$-order $\mathcal{O} = \mathcal{O}_{i_1,i_2,j_1,j_2} = \mathbb{Z}[\varphi^{(i_1)}, \varphi^{(i_2)}, \psi^{(j_1)}, \psi^{(j_2)}]$.

Let us fix those indices $1 \le i_1 < i_2 \le m$ and $1 \le j_1 < j_2 \le n$ for which $\varphi^{(i_1)} \equiv \varphi^{(i_2)} \pmod q$ and also $\psi^{(j_1)} \equiv \psi^{(j_2)} \pmod q$. Consider equation (1.9) modulo q.

By our assumptions $\varphi^{(i_1)} - \varphi^{(i_2)} \equiv 0 \pmod q$ and $\psi^{(j_1)} - \psi^{(j_2)} \equiv 0 \pmod q$, hence by equation (1.9) we get $\rho = \alpha^{(i_2,j_2)} - \alpha^{(i_1,j_1)} \equiv 0 \pmod q$. This is one of the algebraic integer factors of $I(\alpha)$, hence $q | I(\alpha)$. □

1.3.2 Applications of Theorem 3

Example I. A cyclic sextic field

Consider the sextic field K generated by a root of $h(x) = x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1$. This is a totally real cyclic sextic field with discriminant $D_K = 453789 = 3^3 7^5$. Its cubic subfield is $L = \mathbb{Q}(\varphi)$ (with discriminant 49) where φ is a root of $f(x) = x^3 + 4x^2 + 3x - 1$. In the field L the elements $\{1, \varphi, \varphi^2\}$ form an integral basis. We have $f(x) \equiv (x+6)^3 \pmod 7$. The quadratic subfield is $M = \mathbb{Q}(\sqrt{21})$. The polynomial $g(x) = x^2 - x - 5$ has $\psi = (1 + \sqrt{21})/2$ as a root, and obviously $\{1, \psi\}$ is an integral basis in M. We have $g(x) \equiv (x - 1/2)^2 \pmod 7$. Theorem 2 implies that the indices of the primitive elements of the order $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$ are all divisible by 7, hence it has no power integral basis.

Example II. A non-cyclic sextic field

Consider the sextic field K generated by a root of $h(x) = x^6 - 12190x^4 + 256565x^2 - 12167$. This is a totally real sextic field with Galois group D_6, discriminant $D_K = 2^6 17^2 23^3 647^2$. Its cubic subfield is $L = \mathbb{Q}(\varphi)$ (with discriminant $252977 = 17 \cdot 23 \cdot 647$ and Galois group S_3) where φ is a root of $f(x) = x^3 - 22x^2 - 23x - 1$. In the field L the elements $\{1, \varphi, \varphi^2\}$ form an integral basis. We have $f(x) \equiv (x + 15)(x + 16)^2 \pmod{23}$. The quadratic subfield is $M = \mathbb{Q}(\sqrt{23})$. The polynomial $g(x) = x^2 - 23$ has $\psi = \sqrt{23}$ as a root, and obviously $\{1, \psi\}$ is an integral basis in M. We have $g(x) \equiv x^2 \pmod{23}$. Theorem 2 implies that the indices of the primitive elements of the order $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$ are all divisible by 23, hence it has no power integral basis.

Example III. The parametric family of simplest sextic fields

Let $t \in \mathbb{Z}$ with $3 \nmid t$, $t \neq -8, -5$. Let us consider the family of sextic fields K_t generated by a root β_t of the polynomial

$$h_t(x) = x^6 - 2tx^5 - (5t + 15)x^4 - 20x^3 + 5tx^2 + (2t + 6)x + 1.$$

This family of fields is called the "simplest sextic fields", having some attractive properties, detailed in [27]. These fields are totally real cyclic fields. Let $q = t^2 + 3t + 9$. We have $d(h_t) = 6^6 q^5$. Note that $h_t(x) \equiv (x - t/3)^6 \pmod{q}$ (the "simplest quintic fields" have a similar property, cf. [14]).

The cubic subfield L_t of K_t is generated by a root φ of

$$f_t = x^3 - tx^2 - (t + 3)x - 1$$

with $d(f_t) = q^2$. These are the "simplest cubic fields", totally real, cyclic. It is well known that $\{1, \varphi, \varphi^2\}$ is an integral basis of L_t. Note that
$f_t(x) \equiv (x - t/3)^3 \pmod{q}$.

The quadratic subfield of K_t is $M_t = \mathbb{Q}(\sqrt{q})$.
If $q \equiv 2, 3 \pmod 4$ then set $g_t(x) = x^2 - q$ with $d(g_t) = 4q$ and with a root $\psi = \sqrt{q}$. In this case $g_t(x) \equiv x^2 \pmod{q}$.
If $q \equiv 1 \pmod 4$ then set $g_t(x) = x^2 - x - (q - 1)/4$ with $d(g_t) = q$ and with a root $\psi = (1 + \sqrt{q})/2$. In this case $g_t(x) \equiv (x - 1/2)^2 \pmod{q}$.
In both cases $\{1, \psi\}$ is an integral basis of M_t.

Consider now the order $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$. By Theorem 2 the indices of the primitive elements of $\mathcal{O}_{fg}$ are all divisible by q, hence $\mathcal{O}_{fg}$ has no power integral bases.

Example IV. A field of higher degree I.

This is an example to illustrate that our results are easily applicable also to suitable fields of higher degrees.

Let φ be a root of $f(x) = x^5-2x^4+7x^2+6x+5$. The quintic field $L = \mathbb{Q}(\varphi)$ has no non-trivial subfields. Let ψ be a root of $g(x) = x^8 + 13x^7 + 55x^6 + 75x^5 + 2x^3 - x^2 - 143x - 525$. The octic field $M = \mathbb{Q}(\psi)$ has no non-trivial subfields, either. We have

$$\begin{aligned} f(x) &\equiv (x+16)^2(x^3+16x+5) \pmod{17} \\ g(x) &\equiv (x+5)^2(x^3+12x^2+2x+14)(x^3+8x^2+4x+7) \pmod{17} \end{aligned}$$

hence our Theorem 2 applies. Consider the order $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ of the field $K = \mathbb{Q}(\varphi, \psi)$ of degree 40. Any $\alpha \in \mathcal{O}_{fg}$ can be represented in the form

$$\alpha = \sum_{i=0}^{4} \sum_{j=0}^{7} x_{ij} \varphi^i \psi^j$$

with $x_{ij} \in \mathbb{Z}$. By Theorem 2 the indices of all primitive elements of $\mathcal{O}_{fg}$ are divisible by 17, hence $\mathcal{O}_{fg}$ admits no power integral bases.

Example V. A field of higher degree II.

Let φ be a root of $f(x) = x^5 + 17x^4 + 446x^3 + 2232x^2 + 6048x + 24192$. Let ψ be a root of $g(x) = x^4 + 21x^3 - 3x^2 - 8x - 4$. We have

$$\begin{aligned} f(x) &\equiv (x+12)^3(x+9)(x+10) \pmod{19} \\ g(x) &\equiv (x+1)^2(x+2)(x+17) \pmod{19} \end{aligned}$$

hence our Theorem 2 applies. Consider the order $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ of the field $K = \mathbb{Q}(\varphi, \psi)$ of degree 20. Any $\alpha \in \mathcal{O}_{fg}$ can be represented in the form

$$\alpha = \sum_{i=0}^{4} \sum_{j=0}^{3} x_{ij} \varphi^i \psi^j$$

with $x_{ij} \in \mathbb{Z}$. By Theorem 2 the indices of all primitive elements of $\mathcal{O}_{fg}$ are divisible by 19, hence $\mathcal{O}_{fg}$ admits no power integral bases.

Example VI. A field of higher degree III.

Using similar notation as above let φ be a root of

$$\begin{aligned} f(x) = x^9 - 8x^8 + 73926x^7 + 5470524x^6 + 151807041x^5 + \\ 14x^4 + 6216x^3 + 1034964x^2 + 76587336x + 2125298574. \end{aligned}$$

Let ψ be a root of

$$g(x) = x^8 - 58x^7 + 1210x^6 + 13324x^5 + 73975x^4 + 177991x^3 + 186340x^2 + 1024870x + 2254714.$$

We have

$$\begin{aligned} f(x) &\equiv (x+111)^4(x+81)(x^4+32x^3+7x^2+111x+49) \pmod{113} \\ g(x) &\equiv (x+11)^5(x+56)(x^2+57x+85) \pmod{113} \end{aligned}$$

hence our Theorem 2 applies. Consider the order $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ of the field $K = \mathbb{Q}(\varphi, \psi)$ of degree 72. Any $\alpha \in \mathcal{O}_{fg}$ can be represented in the form

$$\alpha = \sum_{i=0}^{8} \sum_{j=0}^{7} x_{ij} \varphi^i \psi^j$$

with $x_{ij} \in \mathbb{Z}$. By Theorem 2 the indices of all primitive elements of $\mathcal{O}_{fg}$ are divisible by 113, hence $\mathcal{O}_{fg}$ admits no power integral bases.

1.4 Congruence conditions I

In the case when the assumptions of Theorem 3 are not satisfied then in certain special cases we can formulate a sufficient congruence condition for the non-existence of power integral basis in the composite of the corresponding orders. In the following subsections we detail two results of this type.

First, assume that there exist square-free integers $p, q \in \mathbb{Z}$ such that

$$f(x) \equiv x^m \pmod{p}, \tag{1.10}$$

or

$$g(x) \equiv x^n \pmod{q}. \tag{1.11}$$

Then we have the following theorem (see [10]):

Theorem 4. *(I. Gaál, P. Olajos, [10])*
Assume that there exist a power integral basis in $\mathcal{O}_{fg}$.

If (1.10) is satisfied, then

$$(d(g))^{m(m-1)/2} \equiv \pm 1 \pmod{p}. \tag{1.12}$$

If (1.11) is satisfied, then

$$(d(f))^{n(n-1)/2} \equiv \pm 1 \pmod{q}. \tag{1.13}$$

Theorem 5. *(I. Gaál, P. Olajos, [10])*
If both (1.10) and (1.11) are valid and any of (1.12) and (1.13) is not satisfied, then $\mathcal{O}_{fg}$ does not admit any power integral basis.

Remark 3. This theorem gives a simple necessary condition for the existence of power integral bases. If the congruences (1.12) and (1.13) are valid and the discriminants are coprime (this means that we can't use Theorem 3) then we have to use Theorem 1 for finding these elements. But in many cases when Theorem 4 is satisfied and the discriminants are coprime, we save a lot of calculations, because we don't have to solve equations (1.2) and (1.3) of Theorem 1.

1.4.1 Proof of Theorem 4

For simplicity's sake in this proof only we will use lower indices for the conjugates of algebraic integers. In this case we denote the conjugates of $\vartheta \in \mathbb{Z}_K$ corresponding to the conjugate α_k of α and β_l of β by ϑ_{kl} instead of $\vartheta^{(k,l)}$ as above. This helps to avoid confusion of conjugates and exponents.

If ϑ generates a power integral basis in K, then we have

$$I(\vartheta) = \frac{1}{\sqrt{|D_{\mathcal{O}_K}|}} \cdot \prod_{(k_1,l_1)<(k_2,l_2)} |\vartheta_{k_1 l_1} - \vartheta_{k_2 l_2}| = 1. \tag{1.14}$$

where the pairs $(k_1, l_1) < (k_2, l_2)$ are ordered lexicographically.

This product splits into three factors taking integer values. The first and second are the following:

$$F_1 = \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \frac{\vartheta_{kl_1} - \vartheta_{kl_2}}{\beta_{l_1} - \beta_{l_2}},$$

$$F_2 = \prod_{l=1}^{n} \prod_{1 \le k_1 < k_2 \le m} \frac{\vartheta_{k_1 l} - \vartheta_{k_2 l}}{\alpha_{k_1} - \alpha_{k_2}}.$$

The factors in these products are algebraic integers. By using symmetric polynomials we can see that both F_1 and F_2 are complete norms, hence $F_1, F_2 \in \mathbb{Z}$.

These factors absorb completely the discriminant $\sqrt{|D_{\mathcal{O}_K}|}$, thus the third factor F_3 consist of the remaining factors $(\vartheta_{k_1l_1} - \vartheta_{k_2l_2})$ of the product (1.14), and also takes integer value.

Denote by N the smallest normal extension of K, let p_0 be a prime factor of p and let $\mathfrak{p}_0$ be a prime ideal of N lying above p_0. Since $f(x) \equiv x^m \pmod{p_0}$, hence $f(x) = \prod_{j=1}^{m}(x - \alpha_j) \equiv x^m \pmod{\mathfrak{p}_0}$. This means that for any root α_j we have $0 = f(\alpha_j) \equiv \alpha_j^m \pmod{\mathfrak{p}_0}$ that is the roots of f are zero modulo $\mathfrak{p}_0$.

Let us consider the factors F_1 and $F_3 \pmod{\mathfrak{p}_0}$. Using $\alpha_j \equiv 0 \pmod{\mathfrak{p}_0}$ for $j = 1, \ldots, m$ we have

$$\begin{aligned}
F_1 &= \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \left(\frac{\vartheta_{kl_1} - \vartheta_{kl_2}}{\beta_{l_1} - \beta_{l_2}} \right) \\
&= \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \frac{1}{\beta_{l_1} - \beta_{l_2}} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot (\alpha_k^i \cdot \beta_{l_1}^j - \alpha_k^i \cdot \beta_{l_2}^j) \\
&\equiv \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \frac{1}{\beta_{l_1} - \beta_{l_2}} \sum_{j=0}^{n-1} x_{0j} \cdot (\beta_{l_1}^j - \beta_{l_2}^j) \\
&= \left(\prod_{1 \le l_1 < l_2 \le n} \sum_{j=0}^{n-1} x_{0j} \cdot \left(\frac{\beta_{l_1}^j - \beta_{l_2}^j}{\beta_{l_1} - \beta_{l_2}} \right) \right)^m \pmod{\mathfrak{p}_0}.
\end{aligned}$$

For similar reasons for F_3 we have

$$\begin{aligned}
F_3 &= \prod_{k_1 \ne k_2} \prod_{1 \le l_1 < l_2 \le n} (\vartheta_{k_1l_1} - \vartheta_{k_2l_2}) \\
&= \prod_{k_1 \ne k_2} \prod_{1 \le l_1 < l_2 \le n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot (\alpha_{k_1}^i \cdot \beta_{l_1}^j - \alpha_{k_2}^i \cdot \beta_{l_2}^j) \\
&\equiv \prod_{k_1 \ne k_2} \prod_{1 \le l_1 < l_2 \le n} \sum_{j=0}^{n-1} x_{0j} \cdot (\beta_{l_1}^j - \beta_{l_2}^j) \\
&= \prod_{k_1 \ne k_2} \prod_{1 \le l_1 < l_2 \le n} (\beta_{l_1} - \beta_{l_2}) \cdot \sum_{j=0}^{n-1} x_{0j} \cdot \left(\frac{\beta_{l_1}^j - \beta_{l_2}^j}{\beta_{l_1} - \beta_{l_2}} \right)
\end{aligned}$$

$$= (D_{\mathcal{O}_M})^{m(m-1)/2} \cdot \left(\prod_{1 \le l_1 < l_2 \le n} \sum_{j=0}^{n-1} x_{0j} \cdot \left(\frac{\beta_{l_1}^j - \beta_{l_2}^j}{\beta_{l_1} - \beta_{l_2}} \right) \right)^{m^2-m}$$

$$= (d(g))^{m(m-1)/2} \cdot \left(\prod_{1 \le l_1 < l_2 \le n} \sum_{j=0}^{n-1} x_{0j} \cdot \left(\frac{\beta_{l_1}^j - \beta_{l_2}^j}{\beta_{l_1} - \beta_{l_2}} \right) \right)^{m^2-m} \pmod{\mathfrak{p}_0}.$$

In the case when $\vartheta \in \mathcal{O}_K$ generates a power integral basis in $\mathcal{O}_K$ then this means that $F_i = \varepsilon_i \quad (i = 1, 2, 3)$, where $\varepsilon_i = 1$ or -1. This implies

$$F_1 \equiv \varepsilon_1 \pmod{\mathfrak{p}_0},\ F_2 \equiv \varepsilon_2 \pmod{\mathfrak{p}_0},\ F_3 \equiv \varepsilon_3 \pmod{\mathfrak{p}_0}.$$

Comparing the above congruences for F_1 and $F_3 \pmod{\mathfrak{p}_0}$ we conclude

$$(d(g))^{m(m-1)/2} \cdot \varepsilon_1^{m-1} \equiv \varepsilon_3 \pmod{\mathfrak{p}_0}.$$

But this is a congruence with integers, hence it must also hold modulo p_0 in $\mathbb{Z}$ (if an integer is divisible by a prime ideal then by taking norms it follows that a certain power of the prime number under the prime ideal divides a power of the integer, that is the prime number divides the integer):

$$(d(g))^{m(m-1)/2} \cdot \varepsilon_1^{m-1} \equiv \varepsilon_3 \pmod{p_0}.$$

This is satisfied for all prime factors p_0 of (the square-free) p hence we become

$$(d(g))^{m(m-1)/2} \cdot \varepsilon_1^{m-1} \equiv \varepsilon_3 \pmod{p},$$

that is

$$(d(g))^{m(m-1)/2} \equiv \pm 1 \pmod{p}.$$

If (1.11) is satisfied performing similar calculation for F_2 and $F_3 \pmod{q}$ we obtain

$$(d(f))^{n(n-1)/2} \equiv \pm 1 \pmod{q}.$$

□

1.4.2 Applications of Theorem 5

In the examples we use the polynomial orders $\mathcal{O}_L$ and $\mathcal{O}_M$ in the same meaning as in Theorem 2, and similarly $\mathcal{O}_K = \mathcal{O}_L \mathcal{O}_M$.

Example I.

Let p, q be square-free integers (≥ 2). One of the most straightforward and frequently used applications of Theorem 5 is the case when $f(x) = x^m - p$ and $g(x) = x^n - q$. Assume that $K = \mathbb{Q}(\sqrt[m]{p}, \sqrt[n]{q})$ is of degree mn. We have

$$\begin{aligned} d(f) &= (-1)^{(m-1)(m-2)/2} \cdot m^m \cdot p^{m-1}, \\ d(g) &= (-1)^{(n-1)(n-2)/2} \cdot n^n \cdot q^{n-1}. \end{aligned}$$

By Theorem 5 if one of the congruences

$$\left(n^n \cdot q^{n-1}\right)^{m(m-1)/2} \equiv \pm 1 \pmod{p}$$

$$\left(m^m \cdot p^{m-1}\right)^{n(n-1)/2} \equiv \pm 1 \pmod{q}.$$

is not satisfied, then $\mathcal{O}_K = \mathbb{Z}[\sqrt[m]{p}, \sqrt[n]{q}]$ has no power integral basis.

I.1. In the special case if $m = 3,\ n = 2$, the field $K = LM$ is an algebraic number field of degree 6. We have $d(f) = D_{\mathcal{O}_L} = -27 \cdot p^2, d(g) = D_{\mathcal{O}_M} = 4 \cdot q$.

The above congruences are of the form

$$\begin{aligned} 64 \cdot q^3 &\equiv \pm 1 \pmod{p}, \\ -27 \cdot p^2 &\equiv \pm 1 \pmod{q}. \end{aligned}$$

If for example we take $p = 7,\ q = 5$ then

$$\gcd(D_{\mathcal{O}_L}, D_{\mathcal{O}_M}) = 1,$$

hence Theorem 1 would be applicable. We have

$$\begin{aligned} 64 \cdot 5^3 = 8000 \equiv 6 \equiv -1 \pmod{7}, \\ -27 \cdot 7^2 = -1323 \equiv 2 \equiv -3 \pmod{5}. \end{aligned}$$

Theorem 5 implies that there is no power integral basis in $\mathcal{O}_K$.

I.2. In the special case when $m = 22,\ n = 15$ and $[K : \mathbb{Q}] = 22 \cdot 15 = 330$, we have

$$d(f) = D_{\mathcal{O}_L} = 22^{22} \cdot p^{21},\ \ d(g) = D_{\mathcal{O}_M} = -15^{15} \cdot q^{14}.$$

If for example we take $p = 31,\ q = 17$ then

$$\gcd(D_{\mathcal{O}_L}, D_{\mathcal{O}_M}) = 1,$$

hence Theorem 1 would be applicable. But by applying Theorem 5, either

$$(-15^{15} \cdot 17^{14})^{231} \equiv 4 \equiv -27 \pmod{31}$$

or

$$(22^{22} \cdot 31^{21})^{105} \equiv 10 \equiv -7 \pmod{17}$$

implies that there exist no power integral basis in $\mathcal{O}_K$.

Example II.

To consider a different example let $f(x) = x^5 - p^3x^3 - p^2x^2 - px - p$ and $g(x) = x^3 - q^2x^2 - qx - q$ $(m = 5,\ n = 3)$. If $\mathcal{O}_K$ has power integral bases, then the following congruences must be satisfied:

$$d(g)^{10} \equiv \pm 1 \pmod{p},$$

$$d(f)^3 \equiv \pm 1 \pmod{q},$$

where

$$d(g) = -q^2(-4q - q^4 + 18q^2 + 4q^5 + 27)$$

and

$$d(f) = -p^4(108p^{13} - 56p^{12} + 12p^{11} + 75p^8 - 38p^7 + 11p^6 - 3750p^4 +$$
$$4250p^3 - 1600p^2 + 256p - 3125).$$

If one of these congruences is not satisfied, $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$ (α and β are being roots of f, g respectively) has no power integral basis.

II.1. Let $p = 7,\ q = 29$. Then $[K : \mathbb{Q}] = 5 \cdot 3 = 15$, and we have

$$d(f) = D_{\mathcal{O}_L} = -23320969892806663 = -(7)^4(11)^2(5208131)(15413),$$

$$d(g) = D_{\mathcal{O}_M} = -68417338124 = -(2)^2(29)^2(41)(496051)$$

and

$$\gcd(D_{\mathcal{O}_L}, D_{\mathcal{O}_M}) = 1,$$

hence Theorem 1 would be applicable. But by applying Theorem 5, either

$$d(g)^{10} \equiv 2 \equiv -5 \pmod{7}$$

or

$$d(f)^3 \equiv 6 \equiv -23 \pmod{29}$$

implies that there exist no power integral basis in $\mathcal{O}_K$.

1.5 Congruence conditions II

In this subsection we assume that there exists a square-free integer q, such that f is a perfect power modulo q, that is

$$f(x) \equiv (x-t)^m \pmod{q} \tag{1.15}$$

with some $t \in \mathbb{Z}$.

Our result is the following:

Theorem 6. *(P. Olajos, [31])*
If there exists a power integral basis in $\mathcal{O}_{fg}$, then the congruence

$$(d(g))^{m(m-1)} \equiv \pm 1 \pmod{q} \tag{1.16}$$

is satisfied.

As a consequence we have:

Theorem 7. *(P. Olajos, [31])*
If (1.15) is valid and (1.16) is not satisfied, then $\mathcal{O}_{fg}$ does not admit any power integral bases.

Remark 4. If $\gcd(d(g), d(f)) = 1$, then the results of Section 1.1 are hardly applicable for higher degree number fields. If condition (1.15) is satisfied, we can draw a conclusions on the existence of power integral bases even in higher degree fields.

Remark 5. The case $d = \gcd(d(f), d(g)) \neq 1$ have already been considered in Section 1.3 . In this case both f and g have a multiple linear factor modulo q, where q is a prime divisor of d. The result given above gives a necessary condition for the existence of power integral basis in case when Theorem 3 is not applicable.

1.5.1 Proof of Theorem 6

Denote by N the smallest normal extension of K and let $\mathfrak{q}_0$ be a prime ideal of N lying above a prime divisor q_0 of q.

Since $f(x) \equiv (x-t)^m \pmod{q}$, hence $f(x) = \prod_{j=1}^{m}(x-\varphi_j)$
$\equiv (x-t)^m \pmod{\mathfrak{q}_0}$, that is $\varphi_j \equiv t \pmod{\mathfrak{q}_0}$, where $1 \leq j \leq m$.

The discriminants of the polynomials f and g are

$$d(f) = \prod_{1\le i<j\le m} (\varphi^{(i)} - \varphi^{(j)})^2$$
$$d(g) = \prod_{1\le i<j\le n} (\psi^{(i)} - \psi^{(j)})^2.$$

These are also the discriminants of the bases $\{1, \varphi, \ldots, \varphi^{m-1}\}$ of the order $\mathcal{O}_f$ and $\{1, \psi, \ldots, \psi^{n-1}\}$ of the order $\mathcal{O}_g$, respectively. As it is known (cf. W.Narkiewicz [33]) the discriminant of the order $\mathcal{O}_{fg}$ is

$$D(\mathcal{O}_{fg}) = d(f)^n \cdot d(g)^m. \tag{1.17}$$

We can represent any element $\alpha \in \mathcal{O}_{fg}$ in the form

$$\alpha = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \varphi^i \psi^j \tag{1.18}$$

with $x_{ij} \in \mathbb{Z}$. The index of α corresponding to the order $\mathcal{O}_{fg}$ (that is $(\mathcal{O}_{fg}^+ : \mathcal{O}_{fg}^+[\alpha])$) is

$$I_{\mathcal{O}_{fg}}(\alpha) = \frac{1}{\sqrt{|D(\mathcal{O}_{fg})|}} \prod_{(i_1,j_1)<(i_2,j_2)} \left|\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_2)}\right|$$

where the pairs of indices are ordered lexicographically. Now we rearrange the factors in the product above. Using (1.17) and (1.18) we have

$$I_{\mathcal{O}_{fg}}(\alpha) = I_1 \cdot I_2 \cdot I_3,$$

where

$$\begin{aligned}
I_1 &= \prod_{i=1}^{m} \prod_{1\le j_1<j_2\le n} \left|\frac{\alpha^{(i,j_1)} - \alpha^{(i,j_2)}}{\psi^{(j_1)} - \psi^{(j_2)}}\right|, \\
I_2 &= \prod_{j=1}^{n} \prod_{1\le i_1<i_2\le m} \left|\frac{\alpha^{(i_1,j)} - \alpha^{(i_2,j)}}{\varphi^{(i_1)} - \varphi^{(i_2)}}\right|, \\
I_3 &= \prod_{\substack{(i_1,j_1)<(i_2,j_2) \\ i_1\neq i_2,\ j_1\neq j_2}} \left|\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_2)}\right|.
\end{aligned} \tag{1.19}$$

Obviously, the factors of I_1, I_2, I_3 appearing in (1.19) are algebraic integers. Further, using symmetric polynomials we can see that $I_1, I_2, I_3 \in \mathbb{Z}$. If α generates a power integral basis in $\mathcal{O}_{fg}$, then the index of α is 1, hence by $I_1 \cdot I_2 \cdot I_3 = \pm 1$ we also have $I_1, I_2, I_3 = \pm 1$ which implies that the factors of I_1, I_2, I_3 are in fact units.

For any $1 \leq i_1 \neq i_2 \leq m$ and $1 \leq j_1 \neq j_2 \leq n$ we have

$$\left(\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_1)}\right) + \left(\alpha^{(i_2,j_1)} - \alpha^{(i_2,j_2)}\right) + \left(\alpha^{(i_2,j_2)} - \alpha^{(i_1,j_1)}\right) = 0$$

which implies the equation

$$\left(\varphi^{(i_1)} - \varphi^{(i_2)}\right) \varepsilon_{i_1 i_2 j_1 j_2} + \left(\psi^{(j_1)} - \psi^{(j_2)}\right) \eta_{i_1 i_2 j_1 j_2} + \rho_{i_1 i_2 j_1 j_2} = 0 \qquad (1.20)$$

with

$$\begin{aligned} \varepsilon_{i_1 i_2 j_1 j_2} &= \frac{\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_1)}}{\varphi^{(i_1)} - \varphi^{(i_2)}}, \\ \eta_{i_1 i_2 j_1 j_2} &= \frac{\alpha^{(i_2,j_1)} - \alpha^{(i_2,j_2)}}{\psi^{(j_1)} - \psi^{(j_2)}}, \\ \rho_{i_1 i_2 j_1 j_2} &= \alpha^{(i_2,j_2)} - \alpha^{(i_1,j_1)}. \end{aligned}$$

By the above arguments these elements are units in

$$\mathcal{O} = \mathbb{Z}[\varphi^{(i_1)}, \varphi^{(i_2)}, \psi^{(j_1)}, \psi^{(j_2)}]$$

where

$$[\mathbb{Q}[\varphi^{(i_1)}, \varphi^{(i_2)}, \psi^{(j_1)}, \psi^{(j_2)}] : \mathbb{Q}] \leq m(m-1)n(n-1).$$

Consider equation (1.20) modulo $\mathfrak{q}_0$.

By our assumptions $\varphi^{(i_1)} - \varphi^{(i_2)} \equiv 0 \pmod{\mathfrak{q}_0}$, hence by equation (1.20) we get

$$\psi^{(j_1)} - \psi^{(j_2)} \equiv -\rho_{i_1 i_2 j_1 j_2} \cdot \eta_{i_1 i_2 j_1 j_2}^{-1} \pmod{\mathfrak{q}_0} \qquad (1.21)$$

where $-\rho_{i_1 i_2 j_1 j_2} \cdot \eta_{i_1 i_2 j_1 j_2}^{-1}$ is also a unit in $\mathcal{O}$. This can be done for all $i_1 \neq i_2$, $j_1 \neq j_2$, so multiplying the left and right sides of equation (1.21) (for all $i_1 \neq i_2$ and $j_1 \neq j_2$) we become

$$(d(g))^{m(m-1)} \equiv \pm 1 \pmod{\mathfrak{q}_0} \qquad (1.22)$$

since on the right side a power of the norm of a unit appears. This is a congruence with rational integers, hence as a consequence we also have

$$(d(g))^{m(m-1)} \equiv \pm 1 \pmod{q_0}. \tag{1.23}$$

We can prove (1.23) for all prime divisor q_0 of q, that is (1.16) must be satisfied. □

1.5.2 Applications of Theorem 7

Example I. A parametric family of totally real cyclic sextic fields

One of the most interesting application of Theorem 7 is the case when

$$f(x) = x^3 - (a+1)x^2 + (a+2)x + 1,$$

$$g(x) = x^2 - ax - 1$$

with parameter $a \in \mathbb{Z}$ ($m = 3, n = 2$). This family was investigated by O. Lecacheux [24] which has initialed our present result. We have

$$d(f) = (a^2 - a + 7)^2,$$

$$d(g) = a^2 + 4.$$

Let us consider the polynomial f. We get

$$f(x) - \left(x - \frac{a+1}{3}\right)^3 = \frac{1}{27} \cdot (a^2 - a + 7) \cdot (a + 4 - 9x).$$

Set $q = a^2 - a + 7$ and assume that q is square free. If $a \equiv 2 \pmod 3$, then $\gcd(q, 9) = 9$. Because of it we consider the family when $a \equiv 0, 1 \pmod 3$. Then we have $\gcd(q, 3) = 1$ which means

$$f(x) \equiv \left(x - \frac{a+1}{3}\right)^3 \pmod{q}. \tag{1.24}$$

Using congruence (1.24), by Theorem 6 if there exists a power integral basis in $\mathcal{O}_{fg}$ the following is satisfied:

$$(a^2 + 4)^6 \equiv (a - 3)^6 \equiv \pm 1 \pmod{q}. \tag{1.25}$$

Using Maple for finding solutions we have the following:

if $a \notin [-840, 840]$, then (1.25) is not satisfied, so by Theorem 7 there exist no power integral bases in $\mathcal{O}_{fg}$.

Considering the values $|a| < 840$, (1.16) can only be satisfied for

$$a = -15, -2, 1, 4.$$

Example II.

As another application of Theorem 7 is the case when

$$f(x) = x^5 + a^2x^4 - (2a^3 + 6a^2 + 10a + 10)x^3 +$$

$$(a^4 + 5a^3 + 11a^2 + 15a + 5)x^2 + (a^3 + 4a^2 + 10a + 10)x + 1,$$

$$g(x) = x^2 - ax - 1$$

with parameter $a \in \mathbb{Z}$ ($m = 5, n = 2$). The totally real cyclic quintic family generated by a root of f was investigated by E. Lehmer [25], see also cf. I. Gaál and M. Pohst [14]. We have

$$d(g) = a^2 + 4.$$

Let us consider the polynomial f. Set $q = a^4 + 5a^3 + 15a^2 + 25a + 25$ and assume that q is square free. Then we have

$$f(x) \equiv \left(x + \frac{a^2}{5}\right)^5 \pmod{q}. \tag{1.26}$$

Using congruence (1.26), by Theorem 6 if there exists a power integral basis in $\mathcal{O}_{fg}$, then

$$(a^2 + 4)^{20} \equiv \pm 1 \pmod{q} \tag{1.27}$$

is satisfied. Using Maple we have that if $a > 2.4 \cdot 10^{16}$, then (1.27) is not satisfied, so by Theorem 7 there exist no power integral bases in $\mathcal{O}_{fg}$.

Chapter 2

Simplest quartics

2.1 Simplest quartic fields

For $t \in \mathbb{Z} \setminus \{0, \pm 3\}$ let

$$P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1. \tag{2.1}$$

Let $\xi = \xi_t$ be a root of $P_t(x)$, then the infinite parametric family of number fields $K_t = K = \mathbb{Q}(\xi)$ is called *simplest quartic fields*. The simplest quartic field K is a totally real cyclic number field of degree 4. If $t = 0$ or $t = \pm 3$ then $P_t(x)$ is not irreducible over $\mathbb{Q}$ (see also Definition 1 and Lemma 1).

If ξ is a root of (2.1), then $\frac{\xi-1}{\xi+1}$ is also one of the roots of (2.1). Thus the rational map $x \mapsto \frac{x-1}{x+1}$ permutes the roots of (2.1) and $K = \mathbb{Q}(\xi)$ is a real quartic number field with cyclic Galois group $G = \langle \sigma \rangle$ generated by the automorphism $\sigma : \xi \mapsto \frac{\xi-1}{\xi+1}$. The family of "simplest" quartic number fields were investigated by M. N. Gras in [17], see also G. Lettl and A. Pethő in [26] and G. Lettl, A. Pethő and P. Voutier in [28].

The purpose of this chapter is to describe all generators of power integral bases in K_t, in a parametric form.

2.1.1 Remarks on simplest families of number fields

Before giving our results on power integral bases in the family of simplest quartic fields, for the sake of completeness, we give an overview of the simplest families of fields.

Let $t \in \mathbb{Z}$ and consider the polynomials

$$\begin{aligned} F_t^3(x,y) &= x^3 - tx^2y - (t+3)xy^2 - y^3, \\ F_t^4(x,y) &= x^4 - tx^3 - 6x^2y^2 + txy^3 + y^4, \\ F_t^6(x,y) &= x^6 - 2tx^5y - (5t+15)x^4y^2 \\ &\quad -20x^3y^3 + 5tx^2y^4 + (2t+6)xy^5 + y^6. \end{aligned}$$

For $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$ and $F \in \mathbb{Q}[x,y]$ we put $F^A = F(ax+by, cx+dy) \in \mathbb{Q}[x,y]$. This defines an isomorphism between $\mathrm{GL}_2(\mathbb{Q})$ and the group of homogeneous automorphisms of $\mathbb{Q}[x,y]$. We call forms $F, G \in \mathbb{Z}[x,y]$ *equivalent* if there exist some $A \in \mathrm{GL}_2(\mathbb{Q})$ and $q \in \mathbb{Q}^*$ (that is $q \neq 0$) with $qG = F^A$. This defines an equivalence relation on the set of all rational forms.

If $F, G \in \mathbb{Z}[x,y]$ are equivalent forms, there is some $A \in \mathrm{GL}_2(\mathbb{Q})$ with integer entries and some $q \in \mathbb{Q}^*$ such that $qG = F^A$. Then for any $K' > 0$, any solution $(x', y') \in \mathbb{Z}^2$ of $|G(x', y')| \leq K'$ can be obtained from some solution $(x, y) \in \mathbb{Z}^2$ of $|F(x,y)| \leq K$ with $K = |q|K'$ by $x = ax' + by', y = cx' + dy'$. Therefore it sufficies to solve the diophantine inequality $|F(x,y)| \leq K$ in $(x,y) \in \mathbb{Z}^2$ with arbitrary K for one F in each class of equivalent forms.

Definition 1. *(see e.g. [28]) A form $F \in \mathbb{Q}[x,y]$ is called simple if F is irreducible over $\mathbb{Q}$ with $\deg(F) \geq 3$ and if there exists some non-trivial $A \in \mathrm{PGL}_2 = \mathrm{GL}_2/\mathbb{Q}^* \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ such that $\psi_A : z \to Az = \frac{az+b}{cx+d}$ permutes the zeros of the underlying polynomial $P(x) = F(x,1)$ transitively. Here $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$ represents A.*

Remark 6. (see also [28]) Let F be a simple form and assume that ψ_A permutes the roots of P. Then there is some $q \in \mathbb{Q}^*$ with $F^A = qF$. For any $B \in \mathrm{GL}_2(\mathbb{Q})$, F^B is also simple and $B^{-1}AB$ permutes the roots of $P^B = F^B(x,1)$.

Remark 7. Definition 1 implies that the roots of P generate a cyclic number field of degree $\deg(F)$, where the Galois action on the roots of P is given by ψ_A. These fields are well known and some of them are the so-called "simplest" number fields.

Lemma 1. *(see [28])*

A. Each non-trivial torsion element of $\mathrm{PGL}_2(\mathbb{Q})$ has order 2,3,4 or 6 and is conjugated to some power of $\left(\begin{smallmatrix} 0 & 1 \\ c & 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & -1 \\ 1 & m \end{smallmatrix}\right)$ with $c \in \mathbb{Q}^*, m \in \{0,1,2\}$.

B. Up to equivalence – the only simple forms in $\mathbb{Q}[x,y]$ are

$$\begin{array}{ll} F_t^3(x,y) & with \quad t \in \mathbb{Z}, \\ F_t^4(x,y) & with \quad t \in \mathbb{Z} \setminus \{-3,0,3\} \\ F_t^6(x,y) & with \quad t \in \mathbb{Z} \setminus \{-8,-3,0,5\}. \end{array}$$

Remarks 8. In the paper [28] Thue inequalities of the form

$$|F_t^6(x,y)| \leq k(t),$$

were investigated for certain simple polynomials $k(t)$ (see [28]). From the results proved there, it follows that for $t \geq 89$ and $t \leq -92$ the only solutions of the family of Thue equations

$$|F_t^6(x,y)| = 1 \text{ resp. } = 27$$

with $\gcd(x,y) = 1$ and $-\dfrac{y}{2} < x \leq y$ are $(1,1)$ resp. $(0,1)$. Later in [27] the result above was extended for all $t \in \mathbb{Z}$.

Remarks 9. Denote by β_i the roots of polynomial $F_t^6(x,1)$, that is $F_t^6(x,1) = \prod_{i=1}^{6}(x-\beta_i)$ and consider the cyclic number field $K = \mathbb{Q}(\beta_1)$ of degree 6 over $\mathbb{Q}$. Then K has a cubic and a quadratic subfield denoted by k_3 and k_2, respectively (see also Example III of section 1.3.2 for details). Let us consider the order $\mathcal{D} = \mathbb{Z}[\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6] \subset K$. In [27] $\mathbb{Z}$-bases are found for the order $\mathcal{D}$ and the corresponding orders in the subfields.

2.2 Power integral bases in simplest quartic fields

Let again $\xi = \xi_t$ be a root of $P_t(x)$ in (2.1) and $K = K_t = \mathbb{Q}(\xi_t)$.

For finding all generators of power integral bases of the simplest quartics we need two lemmas.

Note that $\mathbb{Q}(\alpha) = \mathbb{Q}(-\alpha)$ (α an algebraic integer), that is we can assume that $t > 0$ and $t \neq 3$. In the following we assume also that $t^2 + 16$ is not divisible by an odd square. Further denote by $v_2(t)$ the 2-adic valuation of t. Recently the integral basis of K was explicitly given.

Lemma 2. *(H. K. Kim and J. S. Kim, [23])*
An integral bases of $K = K_t$ is given as follows.

$$\mathcal{O}_{\mathcal{K}} = \begin{cases} [1, \xi, \xi^2, \frac{1+\xi^3}{2}] & \text{if } v_2(t) = 0, \\ [1, \xi, \frac{1+\xi^2}{2}, \frac{\xi+\xi^3}{2}] & \text{if } v_2(t) = 1, \\ [1, \xi, \frac{1+\xi^2}{2}, \frac{1+\xi+\xi^2+\xi^3}{4}] & \text{if } v_2(t) = 2, \\ [1, \xi, \frac{1+2\xi-\xi^2}{4}, \frac{1+\xi+\xi^2+\xi^3}{4}] & \text{if } v_2(t) \geq 3. \end{cases}$$

The main result of this chapter is:

Theorem 8. *(P. Olajos, [32]) The ring of integers $\mathbb{Z}_K$ of the simplest quartic field $K = K_t$ admits power integral bases only for $t = 2$ and $t = 4$. In these cases all generators of power integral bases are the following:*

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

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

To prove our main result we apply the following general argument for finding power integral bases in quartic fields.

Denote by $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ the minimal polynomial of the generating element of a quartic field $K = \mathbb{Q}(\xi)$. Assume, that any $\alpha \in \mathbb{Z}_K$ can be represented in the form

$$\alpha = \frac{a + x\xi + y\xi^2 + z\xi^3}{g} \tag{2.2}$$

with $a, x, y, z \in \mathbb{Z}$, and with fixed common denominator $g \in \mathbb{Z}$. Set

$$\begin{aligned} F(u, v) &= u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3, \\ Q_1(x, y, z) &= x^2 - a_1xy + a_2y^2 + (a_1^2 - 2a_2)xz + \\ &+ (a_3 - a_1a_2)yz + (-a_1a_3 + a_2^2 + a_4)z^2, \\ Q_2(x, y, z) &= y^2 - xz - a_1yz + a_2z^2, \end{aligned}$$

and consider the equation

$$I(\alpha) = m \tag{2.3}$$

where $\alpha \in \mathbb{Z}_K,\ m \in \mathbb{Z}$.

Lemma 3. *(I. Gaál, A. Pethő, M. Pohst, [11], see also [8])*
The element $\alpha \in \mathbb{Z}_K$, represented in the form (2.2), is a solution of (2.3) if and only if there exists a solution $(u, v) \in \mathbb{Z}^2$ of

$$F(u,v) = \pm\frac{g^6 m}{I(\xi)} = \pm i_m \tag{2.4}$$

with

$$Q_1(x,y,z) = u, \tag{2.5}$$

$$Q_2(x,y,z) = v. \tag{2.6}$$

2.3 Proof of Theorem 8

Let $t \in \mathbb{Z}^+ \setminus \{3\}$ and $\xi = \xi_t$ be a root of $P_t(x)$ in (2.1) and let $K = K_t = \mathbb{Q}(\xi)$ be a simplest quartic field and $\{1, \omega_2, \omega_3, \omega_4\}$ be an integral basis of K according to Lemma 2. For simplicity we omit t, but all the formulas implicitly depend on t. In our case the index form (2) is a homogeneous form of degree 6 in 3 variables. Let us suppose that (x_0, y_0, z_0) is a solution of (2). Using Lemma 2 we can rewrite any $\alpha = x_0\omega_2 + y_0\omega_3 + z_0\omega_4$ in the form

$$\alpha = \frac{a + x_1\xi + y_1\xi^2 + z_1\xi^3}{g}.$$

Note that this implies a one-to-one correspondence between (x_0, y_0, z_0) and (x_1, y_1, z_1). The forms appearing in Lemma 3 have the following shape:

$$\begin{aligned}
F(u,v) &= u^3 + 6u^2v + (-t^2-4)uv^2 + (-24-2t^2)v^3 \\
&= (u+2v)(u^2+4uv-v^2t^2-12v^2), \\
Q_1(x_1,y_1,z_1) &= x_1^2 + tx_1y_1 - 6y_1^2 + (t^2+12)x_1z_1 - 5ty_1z_1 + (t^2+37)z_1^2, \\
Q_2(x_1,y_1,z_1) &= y_1^2 - x_1z_1 + ty_1z_1 - 6z_1^2.
\end{aligned}$$

Case I.: Set $\{1, \omega_2, \omega_3, \omega_4\} = \{1, \xi, \xi^2, \frac{1+\xi^3}{2}\}$, and $v_2(t) = 0$

In the first case $g = 2,\ I(\xi) = 2,\ m = \pm 1$, that is $i_m = \pm 2^5 = 32$. Using the factorization of $F(u, v)$, that is

$$u + 2v = 2^i$$

and

$$u^2 + 4uv - v^2t^2 - 12v^2 = \frac{i_m}{2^i},$$

where $i \in [0, 5]$ we have the following solutions (t, u, v) of equation $F(u, v) = i_m$:

$(t, u, v) = (1, \mp 12, \pm 2), (1, \pm 4, \pm 2), (5, \pm 22, \pm 5), (5, \pm 42, \mp 5)$.

Case II.: Set $\{1, \omega_2, \omega_3, \omega_4\} = \{1, \xi, \frac{1+\xi^2}{2}, \frac{\xi+\xi^3}{2}\}$, and $v_2(t) = 1$

In this case $g = 2,\ I(\xi) = 4,\ m = \pm 1$, that is $i_m = \pm 2^4 = 16$. Using similar calculations as above we have for solutions (t, u, v) of equation $F(u, v) = i_m$:

$(t, u, v) = (2, \pm 2, \pm 1), (2, \pm 6, \mp 1)$.

Case III.: $\{1, \omega_2, \omega_3, \omega_4\} = \{1, \xi, \frac{1+\xi^2}{2}, \frac{1+\xi+\xi^2+\xi^3}{4}\}$, and $v_2(t) = 2$

In this case $g = 4,\ I(\xi) = 8,\ m = \pm 1$, that is $i_m = \pm 2^9 = 512$. Using similar calculations as above we have for solutions (t, u, v) of equation $F(u, v) = i_m$:

$(t, u, v) = (4, \pm 4, \pm 2), (2, \pm 12, \mp 2), (4, \pm 10, \pm 3), (4, \pm 22, \mp 3), (t, \pm 8, 0)$.

Case IV.: $\{1, \omega_2, \omega_3, \omega_4\} = \{1, \xi, \frac{1+2\xi-\xi^2}{4}, \frac{1+\xi+\xi^2+\xi^3}{4}\}$, and $v_2(t) \geq 3$

In this case $g = 4,\ I(\xi) = 16,\ m = \pm 1$, that is $i_m = \pm 2^8 = 256$. Using similar calculations as above we have for solutions (t, u, v) of equation $F(u, v) = i_m$:

$(t, u, v) = (8, \pm 2, \pm 1), (8, \pm 6, \mp 1), (16, \pm 14, \pm 1), (16, \pm 18, \mp 1)$.

In each case we use similar calculations using ideas of [12]. For the sake of clarity we shortly explain the arguments of [12] for solving index form equations in quartic fields. We have to solve the system of equations

$$\begin{aligned} Q_1(x_1, y_1, z_1) &= u, \\ Q_2(x_1, y_1, z_1) &= v. \end{aligned} \tag{2.7}$$

where $x_1, y_1, z_1 \in \mathbb{Z}$. Obviously, any solution (x_1, y_1, z_1) of (2.7) satisfies

$$Q_0(x_1, y_1, z_1) = 0 \tag{2.8}$$

where

$$Q_0(x_1, y_1, z_1) = uQ_2(x_1, y_1, z_1) - vQ_2(x_1, y_1, z_1). \tag{2.9}$$

Consider a non-trivial solution (x_Q, y_Q, z_Q) of (2.8). Without loss of generality we assume that $z_Q \neq 0$. Following the arguments of [34] we write all solutions (x_1, y_1, z_1) of (2.8) in a parametric form

$$\begin{aligned} x_1 &= rx_Q &+ p \\ y_1 &= ry_Q &+ q \\ z_1 &= rz_Q \end{aligned} \tag{2.10}$$

with rational parameters r, p, q and substitute into (2.8). (x_Q, y_Q, z_Q) is a solution of (2.8), hence we get

$$r(c_1 p + c_2 q) = c_3 p^2 + c_4 pq + c_5 q^2,$$

where the integer parameters $c_1, \ldots, c_5$ are easily calculated. Then we multiply (2.10) by $(c_1 p + c_2 q)$. Further, we multiply these equations by the square of the common denominator of p, q to obtain integer parameters. We divide these equations by $\Big(\gcd(p,q)\Big)^2$ and obtain

$$\begin{aligned} k \cdot x_1 &= c_{11} p^2 + c_{12} pq + c_{13} q^2, \\ k \cdot y_1 &= c_{21} p^2 + c_{22} pq + c_{23} q^2, \\ k \cdot z_1 &= c_{31} p^2 + c_{32} pq + c_{33} q^2, \end{aligned} \tag{2.11}$$

where $k \in \mathbb{Z}$, $c_{ij} \in \mathbb{Z}$ $(1 \leq i, j \leq 3)$ and the parameters $p, q \in \mathbb{Z}$ are coprime.

In our cases we have the following constants:

$$\begin{aligned} c_1 &= -2vx_Q - uz_Q - 12vz_Q - vt^2 z_Q - vty_Q, \\ c_2 &= -vtx_Q + utz_Q + 2uy_Q + 12vy_Q + 5vtz_Q, \\ c_3 &= v, \\ c_4 &= vt, \\ c_5 &= -u - 6v. \end{aligned}$$

Substituting the relations (2.11) into equations (2.7) concerning Q_1 and Q_2, yields that we have to solve

$$\begin{aligned} Q_1(kx_1, ky_1, kz_1) &= Q_1(p,q) = k^2 \cdot u, \\ Q_2(kx_1, ky_1, kz_1) &= Q_2(p,q) = k^2 \cdot v \end{aligned} \tag{2.12}$$

in $p, q \in \mathbb{Z}$.

The matrix $C = (c_{ij})_{1\le i,j\le 3}$ is regular (see [12]). If we consider (2.11) as a system of linear equations in the variables p^2, pq, q^2 using Cramer's rule we have

$$\det(C)\cdot p^2 = k\cdot(\bar{c}_{11}x_1 + \bar{c}_{12}y_1 + \bar{c}_{13}z_1),$$
$$\det(C)\cdot q^2 = k\cdot(\bar{c}_{31}x_1 + \bar{c}_{32}y_1 + \bar{c}_{33}z_1),$$

where $C^{-1} = (\bar{c}_{ij}/\det(C))_{1\le i,j\le 3}$ with integer $\bar{c}_{ij}$. Because of these equations by $\gcd(p,q) = 1$ we can see that k divides $\det(C)/\gcd\{c_{ij}|1 \le i,j \le 3\}^2$. Let consider our **Cases I-IV** in which we calculated equation $Q_1(x_1,y_1,z_1)$ (or $Q_2(x_1,y_1,z_1)$), k and determined all solutions $(x_1,y_1,z_1) \in \mathbb{Z}^3$ of (2.7). In each case equation $Q_2(p,q) = k^2\cdot v$ is equal to equation $Q_1(p,q) = k^2\cdot u$ multiplied by a non-zero integer, that is we have to solve only one of the equations in (p,q). That is we have to solve Thue equations in (p,q) and it is easy to do by Kash [2].

Case I.:
A1. $(t,u,v) = (1,\pm 4,\pm 2)$:

$$Q_1(p,q) = 8(4p^4 - 14p^3q - 5p^2q^2 + 44pq^3 - 16q^4) = k^2\cdot u,\ k|8$$

and no solutions in (p,q).
A2. $(t,u,v) = (1,\mp 12,\pm 2)$:

$$Q_1(p,q) = 24(-p^4 - 13p^3q - 40p^2q^2 - 13pq^3 - q^4) = k^2\cdot u,\ k|8$$

and no solutions in (p,q).
A3. $(t,u,v) = (5,\pm 22,\pm 5)$:

$$Q_1(p,q) = 37p^4 + 24p^3q - 259p^2q^2 + 54pq^3 + 236q^4 = k^2\cdot u,\ k|32.$$

The solutions (p,q), (x_1,y_1,z_1) and parameter k are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1
22	5	± 5	± 3	± 16	± 19	± 9	∓ 2
-22	-5	± 49	± 31	± 8	± 7	± 3	∓ 1
-22	-5	± 1	∓ 1	± 8	± 43	± 47	∓ 9
-22	-5	± 98	± 62	± 32	± 7	± 3	∓ 1
-22	-5	± 2	∓ 2	± 32	± 43	± 47	∓ 9

Using these results we have no integral solutions (x_0,y_0,z_0) of equation (2).

A4. $(t, u, v) = (5, \pm 42, \mp 5)$:

$$Q_1(p, q) = 42(-23p^4 - 214p^3q - 539p^2q^2 - 184pq^3 + 16q^4) = k^2 \cdot u,\ k|32.$$

The solutions (p, q), (x_1, y_1, z_1) and parameter k are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1
42	-5	± 40	∓ 9	± 4	± 59	± 31	∓ 7
42	-5	0	± 1	± 4	± 9	∓ 19	± 3
42	-5	± 80	∓ 18	± 16	± 59	± 31	∓ 7
42	-5	0	± 2	± 16	± 9	∓ 19	± 3
-42	5	± 4	∓ 1	± 8	± 3	∓ 7	± 3
-42	5	± 8	∓ 2	± 32	± 3	∓ 7	± 3

Using these results we have no integral solutions (x_0, y_0, z_0) of equation (2).

Case II.:
B1. $(t, u, v) = (2, \pm 2, \pm 1)$:

$$Q_1(p, q) = 2(p^4 + 8p^3q + 4p^2q^2 - 48pq^3 + 16q^4) = k^2 \cdot u,\ k|16.$$

The solutions (p, q), parameter k, (x_1, y_1, z_1) and (x_0, y_0, z_0) are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1	x_0	y_0	z_0
2	1	± 1	0	± 1	± 59	± 31	∓ 7	± 4	± 2	∓ 1
2	1	± 6	∓ 1	± 4	± 22	± 9	∓ 4	± 13	± 9	∓ 4
2	1	± 4	∓ 1	± 4	± 4	∓ 1	0	± 2	∓ 1	0
2	1	± 2	± 1	± 4	± 2	± 1	0	± 1	± 1	0
2	1	0	± 1	± 4	± 14	± 3	∓ 2	± 8	± 3	∓ 2
2	1	± 4	0	± 16	± 59	± 31	∓ 7	± 4	± 2	∓ 1
2	1	± 12	∓ 2	± 16	± 22	± 9	∓ 4	± 13	± 9	∓ 4
2	1	± 8	∓ 2	± 16	± 4	∓ 1	0	± 2	∓ 1	0
2	1	± 4	± 2	± 16	± 2	± 1	0	± 1	± 1	0
2	1	0	± 2	± 16	± 14	± 3	∓ 2	± 8	± 3	∓ 2

In this case we have got solutions (x_0, y_0, z_0) of the index form equation (2).

B2. $(t,u,v)=(2,\pm 6,\mp 1)$:

$$Q_1(p,q)=-6(5p^4+40p^3q+100p^2q^2+80pq^3+16q^4)=k^2\cdot u,\ k|16.$$

The solutions (p,q), parameter k, (x_1,y_1,z_1) and (x_0,y_0,z_0) are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1	x_0	y_0	z_0
-6	1	± 3	∓ 1	± 1	± 21	± 4	∓ 3	± 12	± 4	∓ 3
-6	1	± 1	∓ 1	± 1	± 1	∓ 4	± 1	0	∓ 4	± 1
-6	1	± 6	∓ 2	± 4	± 21	± 4	∓ 3	± 12	± 4	∓ 3
-6	1	± 2	∓ 2	± 4	± 1	∓ 4	± 1	0	∓ 4	± 1
-6	1	± 4	∓ 1	± 4	± 10	± 5	∓ 2	± 6	± 5	∓ 2
-6	1	± 2	∓ 1	± 4	± 2	∓ 1	0	± 1	∓ 1	0
-6	1	0	± 1	± 4	0	± 1	0	0	± 1	0
-6	1	± 12	∓ 4	± 16	± 21	± 4	∓ 3	± 12	± 4	∓ 3
-6	1	± 4	∓ 4	± 16	± 1	∓ 4	± 1	0	∓ 4	± 1
-6	1	± 8	∓ 2	± 16	± 10	± 5	∓ 2	± 6	± 5	∓ 2
-6	1	± 4	∓ 2	± 16	± 2	∓ 1	0	± 1	∓ 1	0
-6	1	0	± 2	± 16	0	± 1	0	0	± 1	0

In this case we have got solutions (x_0,y_0,z_0) of the index form equation (2).

Case III.:
C1. $(t,u,v)=(4,\pm 4,\pm 2)$:

$$Q_1(p,q)=4(p^4-16p^2q^2+32q^4)=k^2\cdot u,\ k|128.$$

The solutions (p,q), parameter k, (x_1,y_1,z_1) and (x_0,y_0,z_0) are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1	x_0	y_0	z_0
4	2	±1	0	±2	±11	±3	∓1	±3	±2	∓1
4	2	±2	0	±8	±11	±3	∓1	±3	±2	∓1
4	2	±4	0	±32	±11	±3	∓1	±3	±2	∓1
4	2	±8	0	±128	±11	±3	∓1	±3	±2	∓1
-4	-2	±2	±1	±8	±7	±3	∓1	±2	±2	∓1
-4	-2	±2	∓1	±8	±13	±13	∓3	±4	±8	∓3
-4	-2	±4	±2	±32	±7	±3	∓1	±2	±2	∓1
-4	-2	±4	∓2	±32	±13	±13	∓3	±4	±8	∓3
-4	-2	±8	±4	±128	±7	±3	∓1	±2	±2	∓1
-4	-2	±8	∓4	±128	±13	±13	∓3	±4	±8	∓3

In this case we have got solutions (x_0, y_0, z_0) of the index form equation (2).
C2. $(t, u, v) = (4, \pm12, \mp2)$:

$$Q_1(p, q) = -4(p^4 + 16p^3q + 80p^2q^2 + 128pq^3 + 32q^4) = k^2 \cdot u,\ k|128.$$

The solutions (p, q), parameter k, (x_1, y_1, z_1) and (x_0, y_0, z_0) are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1	x_0	y_0	z_0
12	-2	±6	∓1	±8	±21	±11	∓3	±6	±7	∓3
12	-2	±2	∓1	±8	±1	∓5	±1	0	±3	∓1
12	-2	±12	∓2	±32	±21	±11	∓3	±6	±7	∓3
12	-2	±4	∓2	±32	±1	∓5	±1	0	±3	∓1
12	-2	±24	∓4	±128	±21	±11	∓3	±6	±7	∓3
12	-2	±8	∓4	±128	±1	∓5	±1	0	±3	∓1
-12	2	±1	0	±2	±3	±5	∓1	±1	±3	∓1
-12	2	±2	0	±8	±3	±5	∓1	±1	±3	∓1
-12	2	±4	0	±32	±3	±5	∓1	±1	±3	∓1
-12	2	±8	0	±128	±3	±5	∓1	±1	±3	∓1

In this case we have got solutions (x_0, y_0, z_0) of the index form equation (2).

C3. $(t, u, v) = (t, \pm 8, 0)$:

$$Q_1(p, q) = 64(p^4 - tp^3q - 6p^2q^2 + tpq^3 + q^4) = k^2 \cdot u,\ k|8.$$

In this case if $k^2 = 1$ or $k^2 = 4$, then there is no solutions (p, q) of equation above. Let us consider the cases when $k^2 = 16$ and $k^2 = 64$.

If $k^2 = 16$, then we have to solve the equation

$$p^4 - tp^3q - 6p^2q^2 + tpq^3 + q^4 = \pm 2, \tag{2.13}$$

and if $k^2 = 64$, then we have to solve the equation

$$p^4 - tp^3q - 6p^2q^2 + tpq^3 + q^4 = \pm 8. \tag{2.14}$$

If we consider equations (2.13) and (2.14) modulo 2 (and repeat it a few times), then it is easily seen that these equations have no solutions in (p, q).

C4. $(t, u, v) = (4, \pm 10, \pm 3)$:

$$Q_1(p, q) = 10(p^4 + 24p^3q + 72p^2q^2 - 352pq^3 + 272q^4) = k^2 \cdot u,\ k|512.$$

The solutions (p, q), (x_1, y_1, z_1) and parameter k are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1
10	3	± 1	0	± 1	± 19	± 12	∓ 3
10	3	± 2	0	± 4	± 19	± 12	∓ 3
10	3	± 2	± 1	± 8	± 9	± 4	∓ 1
10	3	± 4	0	± 16	± 19	± 12	∓ 3
10	3	± 4	± 2	± 32	± 9	± 4	∓ 1
10	3	± 8	0	± 64	± 19	± 12	∓ 3
10	3	± 8	± 4	± 128	± 9	± 4	∓ 1
10	3	± 16	0	± 256	± 19	± 12	∓ 3
10	3	± 16	± 8	± 512	± 9	± 4	∓ 1

Using these results we have no integral solutions (x_0, y_0, z_0) of equation (2).

C5. $(t, u, v) = (4, \pm 22, \mp 3)$:

$$Q_1(p, q) = 22(31p^4 + 232p^3q - 72p^2q^2 - 3744pq^3 - 6928q^4) = k^2 \cdot u,\ k|512.$$

The solutions (p, q), (x_1, y_1, z_1) and parameter k are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1
-22	3	± 4	∓ 1	± 4	± 3	∓ 6	± 1
-22	3	± 18	∓ 5	± 8	± 13	± 2	∓ 1
-22	3	± 8	∓ 2	± 16	± 3	∓ 6	± 1
-22	3	± 36	∓ 10	± 32	± 13	± 2	∓ 1
-22	3	± 16	∓ 4	± 64	± 3	∓ 6	± 1
-22	3	± 72	∓ 20	± 128	± 13	± 2	∓ 1
-22	3	± 32	∓ 8	± 256	± 3	∓ 6	± 1
-22	3	± 144	∓ 40	± 512	± 13	± 2	∓ 1

Using these results we have no integral solutions (x_0, y_0, z_0) of equation (2).

Case IV.:
D1. $(t, u, v) = (8, \pm 2, \pm 1)$:

$$Q_1(p, q) = 2(5p^4 - 80p^2q^2 + 64q^4) = k^2 \cdot u,\ k|256.$$

The solutions (p, q), (x_1, y_1, z_1) and parameter k are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1
2	1	± 4	± 1	± 8	± 59	± 36	∓ 5
2	1	± 4	∓ 1	± 8	± 19	∓ 28	± 3
2	1	0	± 1	± 8	± 7	± 8	∓ 1
2	1	± 8	± 2	± 32	± 59	± 36	∓ 5
2	1	± 8	∓ 2	± 32	± 19	∓ 28	± 3
2	1	0	± 2	± 32	± 7	± 8	∓ 1
2	1	± 16	± 4	± 32	± 59	± 36	∓ 5
2	1	± 16	∓ 4	± 32	± 19	∓ 28	± 3
2	1	0	± 4	± 32	± 7	± 8	∓ 1

Using these results we have no integral solutions (x_0, y_0, z_0) of equation (2).

D2. $(t, u, v) = (8, \pm 6, \mp 1)$:

$$Q_1(p, q) = 6(11p^4 + 256p^3q + 1856p^2q^2 + 4096pq^3 - 1024q^4) = k^2 \cdot u,\ k|2048.$$

The solutions (p, q), (x_1, y_1, z_1) and parameter k are collected in the following table:

u	v	p	q	k	x_1	y_1	z_1
-6	1	± 16	∓ 3	± 32	± 40	± 65	∓ 8
-6	1	± 8	∓ 1	± 32	± 8	∓ 1	0
-6	1	0	± 1	± 32	0	± 1	0
-6	1	± 32	∓ 6	± 128	± 40	± 65	∓ 8
-6	1	± 16	∓ 2	± 128	± 8	∓ 1	0
-6	1	0	± 2	± 128	0	± 1	0
-6	1	± 64	∓ 12	± 512	± 40	± 65	∓ 8
-6	1	± 32	∓ 4	± 512	± 8	∓ 1	0
-6	1	0	± 4	± 512	0	± 1	0
-6	1	± 128	∓ 24	± 2048	± 40	± 65	∓ 8
-6	1	± 64	∓ 8	± 2048	± 8	∓ 1	0
-6	1	0	± 8	± 2048	0	± 1	0

Using these results we have no integral solutions (x_0, y_0, z_0) of equation (2).

D3. $(t, u, v) = (16, \pm 14, \pm 1)$:

$$Q_1(p, q) = 14(43p^4 + 112p^3q - 248p^2q^2 - 192pq^3 + 304q^4) = k^2 \cdot u,\ k|256$$

and no solutions in (p, q).

D4. $(t, u, v) = (16, \pm 18, \mp 1)$:

$$Q_1(p, q) = 36(p^4 + 64p^3q + 1264p^2q^2 + 8224pq^3 + 4336q^4) = k^2 \cdot u,\ k|256$$

and no solutions in (p, q).

Summarizing **Cases I-IV** we have the following generators of power integral bases in $\mathbb{Z}_K$:

Integral basis $\left\{1, \xi, \frac{1+\xi^2}{2}, \frac{\xi+\xi^3}{2}\right\}$			
t	x_0	y_0	z_0
2	± 4	± 2	∓ 1
2	± 13	± 9	∓ 4
2	± 2	∓ 1	0
2	± 1	± 1	0
2	± 8	± 3	∓ 2
2	± 12	± 4	∓ 3
2	0	± 4	∓ 1
2	± 6	± 5	∓ 2
2	± 1	∓ 1	0
2	0	± 1	0

Integral basis $\left\{1, \xi, \frac{1+\xi^2}{2}, \frac{1+\xi+\xi^2+\xi^3}{4}\right\}$			
t	x_0	y_0	z_0
4	± 3	± 2	∓ 1
4	± 2	± 2	∓ 1
4	± 4	± 8	∓ 3
4	± 6	± 7	∓ 3
4	0	± 3	∓ 1
4	± 1	± 3	∓ 1

These solutions are listed in **Theorem 8**. □

Chapter 3

A parametric family of degree 6

3.1 Auxiliary results

Let ϑ be a totally real cubic algebraic integer and let m be a square-free positive integer. Let us consider the sextic field $K = \mathbb{Q}(\vartheta, i\sqrt{m})$, with discriminant D_K and ring of integers $\mathbb{Z}_K$. Let $M = \mathbb{Q}(i\sqrt{m})$ and $L = \mathbb{Q}(\vartheta)$ be the subfields of K. Set

$$\omega = \begin{cases} (1+\mathrm{i}\sqrt{m})/2, & \text{if } -m \equiv 1 \pmod 4 \\ \mathrm{i}\sqrt{m}, & \text{if } -m \equiv 2, 3 \pmod 4. \end{cases} \tag{3.1}$$

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

$$\alpha = \frac{x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2}{g} \tag{3.2}$$

with $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$ and with a fixed common denominator $g \in \mathbb{Z}$. Set $\mathcal{O} = \mathbb{Z}[1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2]$ and denote by $D_{\mathcal{O}}$ the discriminant of this order. We are going to consider the existence of power integral basis, and more general the existence of elements of a given index, in the order $\mathcal{O}$ which often coincides with $\mathbb{Z}_K$. We have

$$\frac{g^6\sqrt{|D_K|}}{\sqrt{|D_{\mathcal{O}}|}} \in \mathbb{Z}.$$

Let I_0 be a given, non-zero positive integer and consider the solutions $\alpha \in \mathbb{Z}_K$ of

$$I(\alpha) = I_0. \tag{3.3}$$

Set

$$I_1 = \frac{g^{15} I_0 \sqrt{|D_K|}}{\sqrt{|D_{\mathcal{O}}|}} \in \mathbb{Z}.$$

Denote by ϑ_i $(1 \leq i \leq 3)$ the conjugates of ϑ over M and set $\rho = -\vartheta_2 - \vartheta_3$.

Lemma 4. *(I. Gaál, [3])*
If $\alpha \in \mathbb{Z}_K$ is a solution of equation (3.3), and $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$ are the coefficients of α in the representation (3.2), then

$$N_{K/M}((x_1 + \omega y_1) - \rho(x_2 + \omega y_2)) = \mu, \tag{3.4}$$

$$N_{L/Q}(y_0 + y_1\vartheta + y_2\vartheta^2) = d, \tag{3.5}$$

where $\mu \in \mathbb{Z}_M$, $d \in \mathbb{Z}$, such that $d \cdot N_{M/Q}(\mu)$ divides I_1.

Under our assumptions on the field K, denote by $\rho = \rho_1,\ \rho_2,\ \rho_3$ the conjugates of ρ over L and let $X = x_1 + \omega y_1,\ Y = x_2 + \omega y_2$ be an arbitrary, but fixed solution of (3.4). Choose the indices $\{r,\ s,\ t\} = \{1,\ 2,\ 3\}$ according to

$$|X - \rho_r Y| \leq |X - \rho_s Y| \leq |X - \rho_t Y|. \tag{3.6}$$

Set

$$c_m = \begin{cases} 2, & \text{if } -m \equiv 1 \pmod 4 \\ 1, & \text{if } -m \equiv 2, 3 \pmod 4 \end{cases}$$

$$\begin{aligned} c_1 &= 9c_m^3|\mu|, \\ c_2 &= \min(|\rho_r - \rho_s|,\ |\rho_r - \rho_t|), \\ c_3 &= |\rho_r - \rho_s| \cdot |\rho_r - \rho_t| \end{aligned}$$

$$c_4 = \max\left\{\frac{2|\mu|^{1/3}}{c_2}, \frac{4c_m|\mu|}{c_3\sqrt{m}}\right\}, c_5 = \left(\frac{8|\mu|}{c_2 c_3}\right)^{1/3}.$$

Finally put

$$F(x, y) = \prod_{j=1}^{3}(x - \rho_j y) \in \mathbb{Z}[x, y].$$

Under these assumptions we have the following statement:

Lemma 5. *(I. Gaál, [3])*
Let $X = x_1 + \omega y_1,\ Y = x_2 + \omega y_2 \in \mathbb{Z}_M$ be a solution of (3.4) according to (3.6). Suppose $|Y| > c_4$. We have

$$x_1 y_2 = x_2 y_1.$$

Further, in case $-m \equiv 1 \pmod 4$:

$$\begin{cases} \text{if } |2x_2 + y_2| \geq 2c_5, & \text{then } |F(2x_1 + y_1, 2x_2 + y_2)| \leq c_1 \\ \text{if } |y_2| \geq 2c_5/\sqrt{m}, & \text{then } |F(y_1, y_2)| \leq c_1/(\sqrt{m})^3, \end{cases}$$

and in case $-m \equiv 2, 3 \pmod 4$:

$$\begin{cases} \text{if } |x_2| \geq 2c_5, & \text{then } |F(x_1, x_2)| \leq c_1, \\ \text{if } |y_2| \geq c_5/\sqrt{m}, & \text{then } |F(y_1, y_2)| \leq c_1/(\sqrt{m})^3. \end{cases}$$

Remark 10. In [3] the fields $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ were considered, where ϑ is a root of $f(x) = x^3 - ax^2 - (a+3)x - 1$ and m is a square-free positive integer. By Theorem 3.1 of [3] if $a \geq 3$ and $m \geq m_0$, then there is no power integral basis in the order $\mathcal{O}$ of K.

3.2 Results

Let

$$f_n(x) = x^3 - nx^2 - (n+1)x - 1 \tag{3.7}$$

where $n \in \mathbb{N}$. If $n \geq 3$, then $f_n(x)$ is totally real. Let $\vartheta = \vartheta_n$ be a root of $f_n(x)$ and let m be a square-free positive integer. Consider the two-parametric family $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ of totally complex sextic fields. Define ω as in (3.1) and set $\mathcal{O} = \mathbb{Z}[1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2]$ with discriminant $D_{\mathcal{O}}$ as before. We also use $L = \mathbb{Q}(\vartheta)$ and $M = \mathbb{Q}(i\sqrt{m})$. Put

$$m_0 = \begin{cases} 36, & \text{if } -m \equiv 1 \pmod 4, \\ 9, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

Theorem 9. *(P. Olajos, [30])*
Assume that $n \geq 7$ and $m \geq m_0$. Then the order $\mathcal{O}$ has no power integral basis.

The proof of this theorem uses arguments similar to [3], but we will consider the small parameters, as well. It means that we will deal with the cases, which do not satisfy $n \geq 7$ or $m \geq m_0(n)$. Note that if $n \leq 2$, then (3.7) is not totally real, so we have to deal additionally only with the cases, when $n = 3,\ 4,\ 5,\ 6$. Using similar tools as in the proof of Theorem 9, we can show that for $m \geq m_o(n)$ the order $\mathcal{O}$ admits no power integral basis.

Theorem 10. *(P. Olajos, [30])*
Set

$$m_0(3) = \begin{cases} 143, & \text{if } -m \equiv 1 \pmod 4, \\ 36, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

$$m_0(4) = \begin{cases} 59, & \text{if } -m \equiv 1 \pmod 4, \\ 15, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

$$m_0(5) = \begin{cases} 42, & \text{if } -m \equiv 1 \pmod 4, \\ 11, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

$$m_0(6) = \begin{cases} 36, & \text{if } -m \equiv 1 \pmod 4, \\ 9, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

For $n = 3,\ 4,\ 5,\ 6$, $m \geq m_o(n)$, the order $\mathcal{O}$ has no power integral basis.

Further, for $n = 3,\ 4,\ 5,\ 6$ by performing direct computation for the small values of m we get:

Theorem 11. *(P. Olajos, [30])*
If $n = 3,\ 4,\ 5,\ 6$ and $2 \leq m_0 < m_0(n)$, then $\mathcal{O}$ has no power integral basis.

In the proof of our statements we shall use the result of M. Mignotte and N. Tzanakis [29] on the solutions of the Thue equations corresponding to the family (3.7). Note that in [29] the equation is solved only for sufficiently large parameters, but later on the result was extended to the range $n \geq 3$ (private communication).

Lemma 6. *(M. Mignotte and N. Tzanakis, [29])*
If $n \geq 3$, then all solutions of the equation

$$N_{L/Q}(x - \vartheta y) = \pm 1 \quad (x, y \in \mathbb{Z})$$

are $(x, y) = (\pm 1, 0), (0, \pm 1), (\pm 1, \mp 1), (\pm 1, \mp n), (\pm(n+1), \pm 1)$.

3.3 Proof of Theorem 9

In our situation we apply Lemma 4 and Lemma 5 with $I_0 = I_1 = 1$. Denote by $\vartheta = \vartheta_1 < \vartheta_2 < \vartheta_3$ the roots of (3.7) and put $\rho = -\vartheta_2 - \vartheta_3$ that is $\rho_j = \vartheta_j - n$ for $1 \le j \le 3$. We have

$$\begin{aligned} -\frac{n}{n+1} &\le \vartheta_1 \le -\frac{(n-1)}{n} \\ -\frac{1}{n-1} &\le \vartheta_2 \le -\frac{1}{n} \\ n+1 &\le \vartheta_3 \le n+2. \end{aligned}$$

The above inequalities imply:

$$\begin{aligned} \rho_2 - \rho_1 &= \vartheta_2 - \vartheta_1 \ge 1 - \left(\frac{1}{n-1} + \frac{1}{n}\right) \\ \rho_3 - \rho_2 &= \vartheta_3 - \vartheta_2 \ge n + 1 + \frac{1}{n} \\ c_2 &\ge 1 - \left(\frac{1}{n-1} + \frac{1}{n}\right) \\ c_3 &\ge (n+1)\left(1 - \left(\frac{1}{n-1} + \frac{1}{n}\right)\right) \\ c_4 &\le \max\left\{\frac{2}{c_2}, \frac{4c_m}{c_3\sqrt{m}}\right\} \le \max\left\{\frac{2}{c_2}; \frac{8}{c_3}\right\} \\ c_5 &\le \left(\frac{8}{c_2 c_3}\right)^{1/3} \end{aligned}$$

In case $n \ge 7$, we have $c_4 < 3$ and $c_5 < 1.3$.

Arrange the conjugates of any $\gamma \in K$ so that $\gamma^{(j+3)}$ is the conjugate of $\gamma^{(j)}$ over M (j=1, 2, 3), $\vartheta^{(j)} = \vartheta^{(j+3)} = \vartheta_j$ and $\omega^{(j)} = \omega,\ \omega^{(j+3)} = \bar{\omega}$ (conjugate of ω over M)(j=1, 2, 3).

Set

$$\beta = g \cdot \alpha,$$

$$\beta^{(j)} = x_0 + x_1\vartheta^{(j)} + x_2{\vartheta^{(j)}}^2 + y_0\omega^{(j)} + y_1\omega^{(j)}\vartheta^{(j)} + y_2\omega^{(j)}{\vartheta^{(j)}}^2,$$

$$\beta_{jk} = \beta^{(j)} - \beta^{(k)},\ 1 \le j,\ k \le 6.$$

The proof of Theorem 2.1 of [3] implies that the expressions

$$\begin{aligned} d_1 &= |\beta_{14}\beta_{25}\beta_{36}|, \\ d_2 &= |\beta_{12}\beta_{23}\beta_{31}\beta_{45}\beta_{56}\beta_{64}|, \\ d_3 &= \beta_{15}\beta_{16}\beta_{24}\beta_{26}\beta_{34}\beta_{35} \end{aligned} \tag{3.8}$$

attain integer values with $d_1 \cdot d_2 \cdot d_3 = \pm I_1$. In our case $I_1 = 1$, hence $d_1 = d_2 = 1$ (cf. equations (3.4),(3.5)) and $d_3 = \pm 1$.

A. Consider now the solutions with $|Y| \leq c_4$. In view of $m \geq m_0$ it implies $y_2 = 0$ and $|x_2| \leq 2$ both for $-m \equiv 1 \pmod 4$ and for $-m \equiv 2,\ 3 \pmod 4$. For $y_2 = 0$ equation (3.5) reduces to

$$N_{L/Q}(y_0 + y_1\vartheta) = \pm 1, \tag{3.9}$$

whence by Lemma 6 we have

$$(y_0, y_1) = (\pm 1, 0), (0, \pm 1), (\pm 1, \mp 1), (\pm 1, \mp n), (\pm(n+1), \pm 1).$$

A1. For $y_0 = \pm 1$, $y_1 = 0$ equation (3.4) becomes

$$N_{K/M}(x_1 - \rho x_2) = \pm 1.$$

Using again, Lemma 6 we obtain

$$(x_1, x_2) = (\pm 1, 0), (\mp n, \pm 1), (\pm(n+1), \mp 1), (\pm(n^2+1), \mp n), (\pm 1, \pm 1).$$

For these values we tested the third factor (3.8). Using symmetric polynomials we calculated coefficients of the third factor, and substituted the above five pairs of $(x_1,\ x_2)$.

A11. In case $-m \equiv 1 \pmod 4$:
1. For $y_0 = \pm 1,\ x_1 = \pm 1,\ x_2 = 0$ we have

$$\begin{aligned} d_3 &= -m^3 - 6m^2 - 9m + 23 + (-6m^2 - 18m + 6)n \\ &+ (-2m^2 - 15m + 5)n^2 + (-2 - 6m)n^3 + (-m - 1)n^4. \end{aligned}$$

2. For $y_0 = \pm 1,\ x_1 = \mp n,\ x_2 = \pm 1$ we have

$$\begin{aligned} d_3 &= -m^3 - 2m^2 - m + 23 + (2m^2 + 2m + 6)n \\ &+ (-2m^2 - 3m + 5)n^2 + (2m - 2)n^3 + (-m - 1)n^4. \end{aligned}$$

3. For $y_0 = \pm 1,\ x_1 = \pm(n+1),\ x_2 = \mp 1$ we have

$$\begin{aligned} d_3 &= -m^3 + 10m^2 - 25m + 23 + (-2m^2 + 10m + 6)n \\ &+ (-2m^2 + 9m + 5)n^2 + (-2m - 2)n^3 + (-m - 1)n^4. \end{aligned}$$

4. For $y_0 = \pm 1,\ x_1 = \pm(n^2+1),\ x_2 = \mp n$ we have

$$\begin{aligned} d_3 &= -m^3 - 6m^2 - 9m + 23 + (12m^2 + 36m + 6)n \\ &+ (-2m^2 - 42m + 5)n^2 + (4m^2 + 24m - 2)n^3 \\ &+ (-2m^2 - 31m - 1)n^4 + 16mn^5 - 6mn^6 + 4mn^7 - mn^8 \end{aligned}$$

5. For $y_0 = \pm 1,\ x_1 = \pm 1,\ x_2 = \pm 1$ we have

$$\begin{aligned} d_3 &= -m^3 - 26m^2 - 169m + 23 + (-36m^2 - 468m + 6)n \\ &+ (-26m^2 - 662m + 5)n^2 + (-12m^2 - 624m - 2)n^3 \\ &+ (-2m^2 - 411m - 1)n^4 - 192mn^5 - 62mn^6 - 12mn^7 - mn^8 \end{aligned}$$

A12. In case $-m \equiv 2,\ 3 \pmod 4$:

1. For $y_0 = \pm 1,\ x_1 = \pm 1,\ x_2 = 0$ we have

$$\begin{aligned} d_3 &= -64m^3 - 96m^2 - 36m + 23 + (-96m^2 - 72m + 6)n \\ &+ (-32m^2 - 60m + 5)n^2 + (-2 - 24m)n^3 + (-4m - 1)n^4. \end{aligned}$$

2. For $y_0 = \pm 1, x_1 = \mp n, x_2 = \pm 1$ we have

$$\begin{aligned} d_3 &= -64m^3 - 32m^2 - 4m + 23 + (32m^2 + 8m + 6)n \\ &+ (-32m^2 - 12m + 5)n^2 + (8m - 2)n^3 + (-4m - 1)n^4. \end{aligned}$$

3. For $y_0 = \pm 1,\ x_1 = \pm(n+1),\ x_2 = \mp 1$ we have

$$\begin{aligned} d_3 &= -64m^3 + 160m^2 - 100m + 23 + (-32m^2 + 40m + 6)n \\ &+ (-32m^2 + 60m + 5)n^2 + (-8m - 2)n^3 + (-4m - 1)n^4. \end{aligned}$$

4. For $y_0 = \pm 1,\ x_1 = \pm(n^2+1),\ x_2 = \mp n$ we have

$$\begin{aligned} d_3 &= -64m^3 - 96m^2 - 36m + 23 + (192m^2 + 144m + 6)n \\ &+ (-32m^2 - 168m + 5)n^2 + (64m^2 + 96m - 2)n^3 \\ &+ (-32m^2 - 124m - 1)n^4 + 64mn^5 - 24mn^6 + 16mn^7 - 4mn^8 \end{aligned}$$

5. For $y_0 = \pm 1,\ x_1 = \pm 1,\ x_2 = \pm 1$ we have

$$\begin{aligned} d_3 &= -64m^3 - 416m^2 - 676m + 23 + (-576m^2 - 1872m + 6)n \\ &+ (-416m^2 - 2648m + 5)n^2 + (-192m^2 - 2496m - 2)n^3 \\ &+ (-32m^2 - 1644m - 1)n^4 - 768mn^5 - 248mn^6 \\ &- 48mn^7 - 4mn^8 \end{aligned}$$

None of them can attain the values ± 1.

A2. For $y_1 = \varepsilon = \pm 1, \pm n,\ y_2 = 0$ equation (3.4) gets the form

$$N_{K/M}((x_1 + \varepsilon\omega) - \rho x_2) = \mu\ ,$$

where $x_1 \in \mathbb{Z};\ x_2 = 0,\ \pm 1,\ \pm 2;\ |\mu| = 1$. This equation can be written in the form

$$\prod_{i=1}^{3}((x_1 + \varepsilon\omega) - \rho_i x_2) = \mu.$$

Set $\gamma_i = x_1 + \varepsilon\omega - \rho_i x_2\ \ (i = 1,\ 2,\ 3)$. Then

$$\mathrm{Im}(\gamma_i) = \mathrm{Im}(\varepsilon\omega) = \begin{cases} \dfrac{\varepsilon\sqrt{m}}{2}, & \text{if } -m \equiv 1 \pmod 4 \\ \varepsilon\sqrt{m}, & \text{if } -m \equiv 2,\ 3 \pmod 4 \end{cases}$$

In view of $m \geq 9$ it implies $\dfrac{\sqrt{m}}{2} > 1$, so $|\mathrm{Im}(\gamma_i)| > 1$. Because of above condition $|\gamma_i| \geq |\mathrm{Im}(\gamma_i)| > 1\ \ (i = 1,\ 2,\ 3)$, thus $|\gamma_1\gamma_2\gamma_3| > 1$ contradicting $\gamma_1\gamma_2\gamma_3 \neq \mu$, if $|\mu| = 1$. We have no solutions in these cases, either.

B. We still have to check the solutions with $|Y| > c_4$. In case $-m \equiv 1 \pmod 4$ by Lemma 5 either $|y_2| < \dfrac{2c_5}{\sqrt{m}} < 1$, that is $y_2 = 0$, or in the opposite case if $|y_2| \geq \dfrac{2c_5}{\sqrt{m}} > 0$, then

$$|F(y_1, y_2)| \leq \frac{c_1}{\sqrt{m^3}} = \frac{9c_m^3}{\sqrt{m^3}} \leq \frac{72}{6^3} < 1$$

implying $y_1 = y_2 = 0$ (for $m \geq m_0$) and contradiction with $|y_2| > 2$. Hence $y_2 = 0$. We get the same result for $-m \equiv 2,\ 3 \pmod 4$ with $2c_5/\sqrt{m}$ replaced by $c_5/\sqrt{m}$. Now equation (3.5) reduces to

$$N_{L/Q}(y_0 + \vartheta y_1) = \pm 1$$

whence by Lemma 6 we conclude

$$(y_0, y_1) = (\pm 1, 0);\ (0, \pm 1);\ (\pm 1, \mp 1), (\pm 1, \mp n), (\pm(n+1), \pm 1).$$

B1. The case $y_0 = \pm 1,\ y_1 = 0$ was already considered in **A1**.

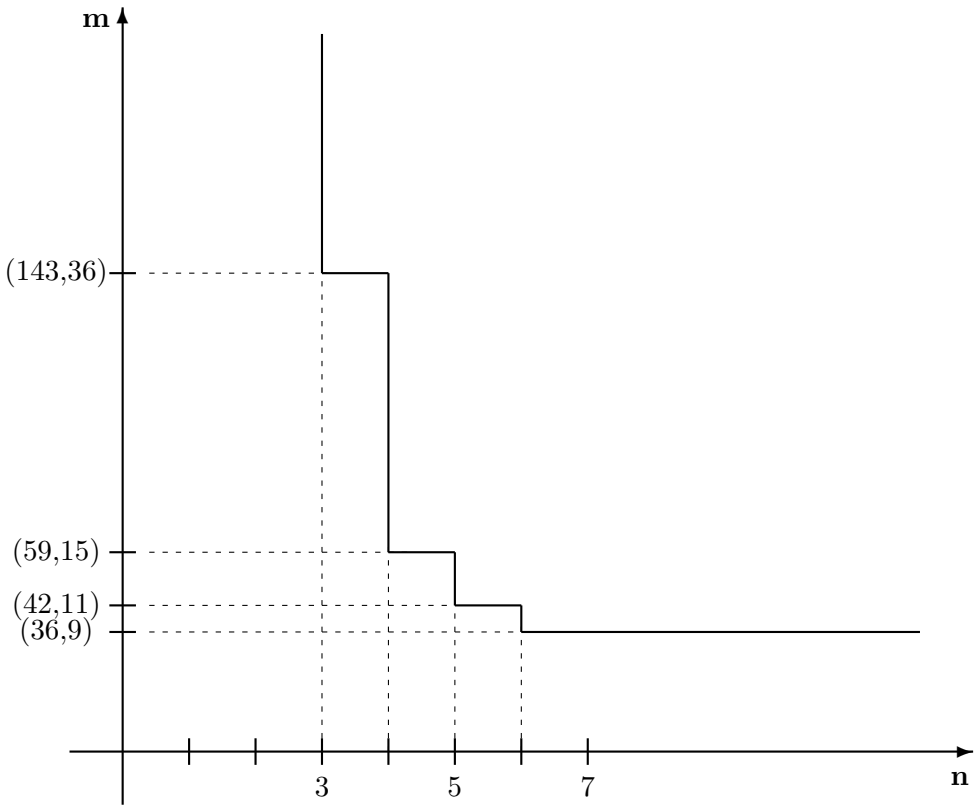
B2. If $y_1 = \varepsilon = \pm 1, \pm n,\ \ y_2 = 0$, then by Lemma 5 we get $x_2 = 0$. Then equation (3.4) becomes

$$N_{K/M}(x_1 + \varepsilon\omega) = \pm 1.$$

It means that $|x_1 + \varepsilon\omega| = 1$. Both for $-m \equiv 1 \pmod 4$ and for $-m \equiv 2,\ 3 \pmod 4$ we obtained the same result, namely the above equation has no solution over $\mathbb{Z}$. □

3.4 Small values of parameters

The proof of Theorem 10, in the cases $n = 3,\ 4,\ 5,\ 6$, $m \geq m_0(n)$ is similar to the proof of Theorem 9. This requires a simple, but tedious calculation and considering several cases, therefore we omit the details of the proof of Theorem 10. Consider now a coordinate system displaying the points $(m,\ n) \in \mathbb{Z}^2$. Note that for $n = 3,\ 4,\ 5,\ 6,\ n \geq 7$ we display the values of $m_0(n)$ which is different for $-m \equiv 1 \pmod 4$ and $-m \equiv 2,\ 3 \pmod 4$.



The shaded part of this diagram shows the pairs (m, n) covered by Theorems 9, 10.

It's a very interesting problem to examine the cases, when $n \geq 3$ and $m < m_0(n)$. Also in this case we apply Lemma 5.

In case $|Y| > c_4$ we have to solve the Thue inequalities of Lemma 5 . This can be done by Kash [2]. This way we get a couple of possible vectors $(x_1,\ x_2,\ y_1,\ y_2) \in \mathbb{Z}^4$. For fixed $y_1,\ y_2$ the corresponding value of y_0 can be found from equation (3.5) which is then a cubic polynomial equation in y_0.

In case $|Y| \leq c_4$ we can determine the possible values of $(x_2,\ y_2)$ by this condition. For fixed $Y = x_2 + \omega y_2$ equation (3.4) in Lemma 9 is a cubic polynomial equation in $X = x_1 + \omega y_1$, which can be solved by Maple. We were looking for the solutions of X, in which x_1 and y_1 are integers. The value of y_0 we can get from equation (3.5) similarly as above.

Finally, the possible tuples $(x_1,\ x_2,\ y_0,\ y_1,\ y_2)$ were tested if the corresponding $\alpha \in \mathcal{O}$ satisfies

$$I(\alpha) = 1.$$

This test eliminated all possible solutions.

3.5 Computational experiences

The computation involved in our results were performed in Maple, except for solving Thue equations which was done by Kash [2]. Note that the "thue" procedure of Maple is only supposed to find small (and not all) solutions of Thue inequalities, but unfortunately in some cases it failed to find even the small ones.

The total CPU time (used mainly for the proof of Theorem 11) was about 5 hours on an old IBM compatible 233MHZ Pentium II PC.

Summary

The thesis consists of three chapters.

In the first chapter we consider composite fields and give congruence conditions for existence of power integral basis. These conditions are well applicable also in investigations of infinite parametric families of number fields (see examples). The application of these results replaces tedious computation in solving norm or relative norm form equations of high degree. This chapter has four sections. In the first section we recall the results of I. Gaál [5] on composite fields with certain subfields with coprime discriminants. In the other sections we give different sufficient congruence conditions for the non-existence of power integral basis in composites of number fields. Considering the examples which are listed at the end of these sections we can see that all results have their own applications where they cannot be replaced by the other ones.

In the next chapter we consider the family of simplest quartic fields.
Let $t \in \mathbb{Z},\ t \neq 0, \pm 3$ and $\xi = \xi_t$ be a root of polynomial $P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1$. The infinite parametric family of number fields $K_t = K = \mathbb{Q}(\xi)$ is called *simplest quartic fields*. The simplest quartic fields K are totally real cyclic number fields of degree 4. (If $t = 0$ or $t = \pm 3$ then $P_t(x)$ is not irreducible over $\mathbb{Q}$.)
Several authors have considered the infinite parametric family of simplest quartic fields $K(\xi)$. The generators of power integral bases of the polynomial ring $\mathbb{Z}[\xi]$ have already been described. In this chapter under certain conditions on t we explicitly give all generators of power integral bases in the ring of integers $\mathbb{Z}_K$ of K. We use a well known general algorithm for calculating power

integral bases in quartic fields.

The purpose of the third chapter is to investigate power integral bases in a parametric family of totally complex sextic fields. These fields are composits of a complex quadratic subfield and a totally real cubic subfield. I. Gaál [3] studied a similar family of fields. Using his method we show that the fields of the family in question do not admit power integral bases if the parameters are not very small. Moreover, using direct computations we also deal with those fields in the family which correspond to small parameters and are not covered by the main theorem.

Összefoglaló

A disszertáció három fejezetből áll.

Az első fejezetben kompozit testekben adunk meg hatvány egész bázis létezésére vonatkozó kongruencia feltételeket. Ezek a feltételek számtestek végtelen parametrikus családjainak vizsgálatainál is jól alkalmazhatóak (lásd a példákat). Ezen eredmények alkalmazásával felesleges számolást kerülhetünk el, mert nem kell magas fokú norma vagy relatív norma forma egyenleteket megoldani. Ez a fejezet négy részből áll. Az első részben relatív prím diszkriminánsú kompozit testeket tekintünk, amely Gaál I. eredménye [5]. A további részekben különböző elégséges kongruencia feltételeket adunk meg számtestekben arra vonatkozóan, hogy ne létezzen hatvány egész bázis. Ezen részek végén felsorolt példák alapján látható, hogy az összes eredmény rendelkezik olyan saját alkalmazásokkal, melyeknél nem helyettesíthetőek más tételekkel.

A következő fejezetben a legegyszerűbb negyedfokú testek családját vizsgáljuk.
Legyen $t \in \mathbb{Z},\ t \neq 0, \pm 3$ és $\xi = \xi_t$ az egyik gyöke a $P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1$ polinomnak. A $K_t = K = \mathbb{Q}(\xi)$ számtestek végtelen parametrikus családját *legegyszerűbb negyedfokú testeknek* hívjuk. A legegyszerűbb negyedfokú K testek teljesen valós, ciklikus negyedfokú számtestek. (Ha $t = 0$ vagy $t = \pm 3$, akkor $P_t(x)$ nem irreducibilis a $\mathbb{Q}$ felett.)
Több szerző vizsgálta a $K(\xi)$ legegyszerűbb negyedfokú testek végtelen parametrikus családját. A $\mathbb{Z}[\xi]$ polinom gyűrű hatvány egész bázisainak generátorait már leírták. Ebben a fejezetben bizonyos t-re vonatkozó feltételek mellett a K test $\mathbb{Z}_K$ egészeinek gyűrűjében adjuk meg explicit módon az összes

hatvány egész bázis generátorait. Egy jól ismert általános algoritmust használunk, hogy kiszámoljuk a hatvány egész bázisokat a negyedfokú testekben.

A harmadik fejezet célja, hogy megvizsgáljuk a hatvány egész bázisokat teljesen komplex hatodfokú testek egy végtelen parametrikus családjában. Ezek a testek egy komplex másodfokú és egy teljesen valós harmadfokú résztestek kompozítumai. Gaál I. [3] testek egy hasonló családját vizsgálta. Felhasználva a módszerét megmutatjuk, hogy a kérdéses család testjeiben nincs hatvány egész bázis, ha a paraméterek nem túl kicsik. Továbbá direkt számítások felhasználásával azokat a testeket is vizsgáltuk, melyek a kis paraméter értékhez tartoznak és ezért a fő tétel nem vonatkozik rájuk.

Bibliography

[1] Y. Bilu, I. Gaál and K. Győry, *Index form equations in sextic fields: a hard computation*, Acta Arithm., to appear.

[2] M. Daberkow, C. Fieker, J. Klüners, M.Pohst, K.Roegner and K.Wildanger, KANT V4, J.Symbolic Comp., **24**(1997), 267–283.

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

[4] I. Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp., **65**(1996), 801–822.

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

[6] I. Gaál, *Power integral bases in algebraic number fields*, Ann. Univ. Sci. Budapest, Sect. Comp., **18**(1999), 61–87.

[7] I. Gaál, *Solving index form equations in fields of degree nine with cubic subfields*, J.Symbolic Comput., **30**(2000), 181–193

[8] I. Gaál, Diophantine equations and power integral bases, Birkhäuser, Boston, (2002).

[9] I. Gaál and K. Győry, *Index form equations in quintic fields*, Acta Arith., **89**(1999), 379–396.

[10] I. Gaál and P. Olajos, *Recent results on power integral bases of composite fields*, Acta Acad. Paed. Agr. Eger, **30**(2003), 45–54.

[11] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in quartic number fields*, J.Symbolic Comput., **16**(1993), 563–584.

[12] I. Gaál, A. Pethő and M. Pohst, *Simultaneous Representation of Integers by a Pair of Ternary Quadratic Forms–With an Application to Index Form Eqautions in Quadratic Number Fields*, J. Number Theory, **57**(1996), 90–104.

[13] I. Gaál and M. Pohst, *On the resolution of index form equations in sextic fields with an imaginary quadratic subfield*, J.Symbolic Computation, **22**(1996), 425–434.

[14] I. Gaál and M. Pohst, *Power integral bases in a parametric family of totally real quintics*, Math. Comp. **66**(1997), 1689–1696.

[15] I. Gaál, M. Pohst and P. Olajos, *Power integral bases in orders of composite fields*, Experimental Math., **11**(2002), 87–90.

[16] I. Gaál and N. Schulte, *Computing all power integral bases of cubic number fields*, Math. Comput., **53**(1989), 689–696.

[17] M. N. Gras, *Table numerique du nombre de classes et des unites des extensions cycliques reelles de degré 4 in* $\mathbb{Q}$, Publ. Math. Fac. Sci. Besançon, (1977-1978) fasc. 2.

[18] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné, III.*, Publ. Math. (Debrecen), **23**(1976), 141–165.

[19] K. Győry, *On polynomials with integer coefficients and given discriminant, IV.*, Publ. Math. (Debrecen), **25**(1978), 155–167.

[20] K. Győry, Résultats effectifs sur la représentation des entiers par des formes décomposables, Queen's Papers in Pure and Applied Math., No. **56**, Kingston, Canada, (1980).

[21] K. Győry, *Bounds for the solutions of decomposable form equations*, Publ. Math. (Debrecen), **52**(1998), 1–31.

[22] I. Járási, *Power integral bases in sextic fields with a cubic subfield*, Acta Sci. Math. (Szeged), **XX**(2003), 291–303.

[23] H. K. Kim and J. S. Kim, *Computation of the different of the simplest quartic fields*, (manuscript).

[24] O. Lecacheux, *Unités d´une famille de corps cycliques réels de degré 6 liés à la courbe modulaire $X_1(13)$*, J. Number Theory, **31**(1989), 54–63.

[25] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comput., **50**(1988), 535–541.

[26] G. Lettl and A. Pethő, *Complete Solution of a Family of Quartic Thue Equations*, Abh. Math. Sem. Univ. Hamburg, **65**(1995), 365–383.

[27] G. Lettl, A. Pethő, P. Voutier, *On the arithmetic of simplest sextic fields and related Thue equations*, in Number Theory, eds. K.Győry, A.Pethő, V.T.Sós, Walter de Gruyter, Berlin-New York, 1998, 331–348.

[28] G. Lettl, A. Pethő and P. Voutier *Simple families of Thue inequalities*, Trans. Am. Math. Soc., **351**(1999), 1871–1894.

[29] M. Mignotte and N. Tzanakis, *On a family of cubic*, J. Number Theory, **39**(1991),41–49.

[30] P. Olajos, *Power integral bases in a parametric family of sextic fields*, Publ. Math. Debrecen, **58**(2000), 779–790.

[31] P. Olajos, *Power integral bases in orders of composite fields II*, Annales Sci. Math., to appear.

[32] P. Olajos, *Power integral bases in the family of simplest quartic fields*, Experimental Math., submitted.

[33] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Springer, (1974).

[34] L. J. Mordell, Diophantine Equations, Academic Press, New York London, 1969.

Appendix A

List of papers of the author

1. P. Olajos, *Power integral bases in a parametric family of sextic fields*, Publ. Math. Debrecen, **58**(2000), 779–790.

2. I. Gaál, M. Pohst and P. Olajos, *Power integral bases in orders of composite fields*, Experimental Math. **11**(2002), 87–90.

3. I. Gaál and P. Olajos, *Recent results on power integral bases of composite fields*, Acta Acad. Paed. Agr. Eger, **30**(2003), 45–54.

4. P. Olajos, *Power integral bases in orders of composite fields II*, Annales Sci. Math., to appear.

5. P. Olajos, *Power integral bases in composite fields*, "On Yokoi-Chowla Conjecture and Related Problems", Furukawa Total Pr. Co., (2004), 86–95.

6. P. Olajos, *Power integral bases in the family of simplest quartic fields*, Experimental Math., submitted.

Appendix B

List of conference talks of the author

1. Power integral bases in a parametric family of sextic fields, 15th Czech and Slovak International Conference on Number Theory, Ostravice 2001.
2. Power integral bases in orders of composite fields, Explicit methods in number Theory, Leiden 2002.
3. Hatvány egész bázisok testek kompozítumaiban, Kiss Péter, az egri és debreceni számelmélész (Kiss Péter emlékére Számelméleti tudományos emlékülés), Eger 2002.
4. Recent results on power integral bases of composite fields, 16th Czech and Slovak International Conference on Number Theory, Bratislava 2003.
5. Recent results on power integral bases of composite fields, XXIIIrd Journées Arithmétiques, Graz 2003.
6. Recent results on power integral bases of composite fields, Diophantine Approximation, Leiden 2003.
7. Power integral bases in algebraic number fields, Yokoi-Chowla conjecture and related problems, Nagoya 2003.