RECENT RESULTS ON POWER INTEGRAL BASES OF COMPOSITE FIELDS

István Gaál and Péter Olajos (Debrecen, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. We consider the problem of existence of power integral bases in orders of composite fields. Completing our former results we show that under certain congruence conditions on the defining polynomial of the generating elements of the fields, the composite of the polynomial orders does not admit power integral basis. As applications we provide several examples involving also infinite parametric families of fields.

AMS Classification Number: 11D57, 11Y50

Keywords and phrases: power integral basis, composite field, index form equations.

1. Introduction

Let K be an algebraic number field of degree n with ring of integers $\mathbb{Z}_K$. It is a classical problem in algebraic number theory to decide if there is an element α in K such that

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

is an integral basis. Such an integral basis is called *power integral basis*. A further problem is to find all elements which generate power integral bases.

The index of a primitive algebraic integer α of K is defined as the module-index

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

Obviously α generates a power integral basis if and only if $I(\alpha) = 1$.

Note that

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

Research of the first author is supported by Grants T-037367 and T-042985, of the second author by Grant T-037367 from the Hungarian National Foundation for Scientific Research.

where $\alpha^{(i)}$ $(i = 1, \dots, n)$ are the conjugates of α and D_K is the discriminant of K.

Let $\{1, \omega_2, \dots, \omega_n\}$ be an integral basis of K. Then the discriminant of the linear form $l(X) = X_1 + \omega_2 X_2 + \dots + \omega_n X_n$ can be written as

$$D_{K/\mathbb{Q}}(l(X)) = I(x_2, \dots, x_n)^2 \cdot D_K,$$

where $I(x_2, \dots, x_n)$ is the *index form* corresponding to the integral basis $\{1, \omega_2, \dots, \omega_n\}$ (see I. Gaál [4]).

For any

$$\alpha = x_1 + \omega_2 x_2 + \dots + \omega_n x_n \in \mathbb{Z}_K$$

we have

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

Hence if we want to determine all generators of power integral bases, we have to solve the *index form equation*

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

Using Baker's method the first effective upper bounds for the solutions of (2) were given by K. Győry [10]. This upper bound implies that (2) has only finitely many solutions.

There are efficient algorithms for determining all generators of power integral bases in lower degree number fields cf. I. Gaál and N. Schulte [9] for cubic, I. Gaál, A. Pethő and M. Pohst [7] for quartic fields. A general algorithm for quintic fields was given by I. Gaál and K. Győry [5], 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 [1], [3], I.Gaál and M. Pohst [8], I. Járási [11]. For a more complete overview on the topic see the monograph [4].

For higher degree number fields this problem is very complicated because of the high degree and the large number of variables of equation (1). The resolution of this equation is only hopeful if K has proper subfields, because in this case the index form is reducible.

Higher degree fields having subfields are very often given as composites of certain subfields. This is the case that we investigated in [2] and [6]. The purpose of this paper is to add some recent results to this area. In order to make it easier for the reader to compare our (old and new) results, we first summarize our former results, then we detail the new results that can be used in some important cases not covered by our former statements.

2. Coprime discriminants

In [2] we considered the problem of existence of power integral bases in case K is the composite of two subfields L and M with coprime discriminants. Let L be of degree r with integral basis $\{l_1 = 1, l_2, \dots, l_r\}$ and discriminant D_L. Denote the index form corresponding to the integral basis $\{l_1 = 1, l_2, \dots, l_r\}$ of L by $I_L(x_2, \dots, x_r)$. Similarly, let M be of degree s with integral basis $\{m_1 = 1, m_2, \dots, m_s\}$ and discriminant D_M. Denote the index form corresponding to the integral basis $\{m_1 = 1, m_2, \dots, m_s\}$ of M by $I_M(x_2, \dots, x_s)$. Assume, that the discriminants are coprime, that is $\gcd(D_L, D_M) = 1$.

Set $K = L \cdot M$ the composite of L and M. As it is known (cf. W. Narkiewicz [12]) the discriminant of K is $D_K = D_L^s \cdot D_M^r$ and an integral basis of K is given by $\{l_i \cdot m_j : 1 \le i \le r,\ 1 \le j \le s\}$. Hence, any integer α of K can be represented in the form

$$\alpha = \sum_{i=1}^{r} \sum_{j=1}^{s} x_{ij} \cdot l_i \cdot m_j \tag{3}$$

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

I. Gaál [2] 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, [2]) *Assume* $\gcd(D_L, D_M) = 1$. *If* α *of (3) generates a power integral basis in* $K = L \cdot M$ *then*

$$N_{M/Q}\left(I_L\left(\sum_{i=1}^{s} x_{2i} \cdot m_i, \dots, \sum_{i=1}^{s} x_{ri} \cdot m_i\right)\right) = \pm 1 \tag{4}$$

and

$$N_{L/Q}\left(I_M\left(\sum_{i=1}^{r} x_{i2} \cdot l_i, \dots, \sum_{i=1}^{r} x_{is} \cdot l_i\right)\right) = \pm 1. \tag{5}$$

This statement was applied e.g. for nonic fields [3].

3. Non-coprime discriminants

A sufficient condition for the non-existence of power integral bases in K was formulated by I. Gaál, P. Olajos and M. Pohst [6] in the case when D_L and D_M are usually not coprime.

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. We also assume that there is a prime number q, $(q \geq 2)$ such that both f and g have a multiple linear factor (at least square) modulo q, that is, there exist a_f and a_g in $\mathbb{Z}$ such that

$$\begin{cases} f(a_f) \equiv f'(a_f) \equiv 0 & \pmod q, \\ g(a_g) \equiv g'(a_g) \equiv 0 & \pmod q. \end{cases} \tag{6}$$

Note that our assumption implies that q divides both the discriminant $d(f)$ of the polynomial f and the discriminant $d(g)$ of g. In our case the fields we consider are composites of subfields whose discriminants are usually not coprime. This is the case in many interesting examples.

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.

Theorem 2. (I. Gaál, P. Olajos, M. Pohst [6]) *Under the above assumptions 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 [6]) *Under the above assumptions the order $\mathcal{O}_{fg}$ has no power integral basis.*

In [6] we applied the above theorem to the parametric family of simplest sextic fields.

4. New results on composite fields

We are going to formulate a further sufficient condition for the non-existence of power integral bases in composite fields.

Let $f, g \in \mathbb{Z}[x]$ be monic, irreducible polynomials of degrees $m, n \in \mathbb{Z}$, respectively. Let α be a root of f, and let β be a root of g. Denote the discriminants of these polynomials by $d(f), d(g)$. The conjugates of α and β will be denoted by α_k $(k = 1, \dots, m)$ and β_l $(l = 1, \dots, n)$, respectively. Further, let $L = \mathbb{Q}(\alpha)$, $\mathcal{O}_{\mathcal{L}} = \mathbb{Z}[\alpha]$ with discriminant $D_{\mathcal{O}_{\mathcal{L}}} = d(f)$ and $M = \mathbb{Q}(\beta)$, $\mathcal{O}_{\mathcal{M}} = \mathbb{Z}\S^{\Updownarrow}[\beta]$ with discriminant $D_{\mathcal{O}_{\mathcal{M}}} = d(g)$. We assume that there are square-free numbers $p, q \in \mathbb{Z}$ $(p, q \geq 2)$ such that

$$(A) \qquad f(x) \equiv x^m \pmod{p},$$

or

$$(B) \qquad g(x) \equiv x^n \pmod{q}.$$

This condition is of course restrictive, but (as we can see in the examples) it holds in many cases which are important for the applications.

Let $K = L \cdot M$ and $\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathcal{L}} \cdot \mathcal{O}_{\mathcal{M}} = \mathbb{Z}[\alpha, \beta]$. Then $D_{\mathcal{O}_{\mathcal{K}}} = D^n_{\mathcal{O}_{\mathcal{L}}} \cdot D^m_{\mathcal{O}_{\mathcal{M}}}$ and any $\vartheta \in \mathcal{O}_{\mathcal{K}}$ can be written in the form

$$\vartheta = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot \alpha^i \cdot \beta^j$$

with conjugates

$$\vartheta_{kl} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot \alpha_k^i \cdot \beta_l^j$$

$(1 \le k \le m,\ 1 \le l \le n)$.

Our main result is the following:

Theorem 4. *Assume that there exists a power integral basis in $\mathcal{O}_{\mathcal{K}}$. If (A) is satisfied, then*

$$(d(g))^{m(m-1)/2} \equiv \pm 1 \pmod{p}. \tag{7}$$

If (B) is satisfied, then

$$(d(f))^{n(n-1)/2} \equiv \pm 1 \pmod{q}. \tag{8}$$

As a consequence we have:

Theorem 5. *If (A) is satisfied, but (7) does not hold, then $\mathcal{O}_{\mathcal{K}}$ does not admit any power integral basis. If (B) is satisfied, but (8) does not hold, then $\mathcal{O}_{\mathcal{K}}$ does not admit any power integral basis.*

Proof of Theorem 4. If ϑ generates a power integral basis in K, then we have

$$I(\vartheta) = \frac{1}{\sqrt{|D_{\mathcal{O}_{\mathcal{K}}}|}} \cdot \prod\nolimits_{(k_1,l_1)<(k_2,l_2)} |\vartheta_{k_1 l_1} - \vartheta_{k_2 l_2}| = 1. \tag{9}$$

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 $(\vartheta_{k_1 l_1} - \vartheta_{k_2 l_2})$ of the product (9), and also takes integer value.

Assume that $f(x) \equiv x^m \pmod{p}$. 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

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

$$= \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \frac{1}{\beta_{l_1} - \beta_{l_2}} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot (\alpha_k^i \cdot \beta_{l_1}^j - \alpha_k^i \cdot \beta_{l_2}^j)$$

$$\equiv \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \frac{1}{\beta_{l_1} - \beta_{l_2}} \sum_{j=0}^{n-1} x_{0j} \cdot (\beta_{l_1}^j - \beta_{l_2}^j)$$

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

For similar reasons for F_3 we have

$$F_3 = \prod_{k_1 \ne k_2} \prod_{1 \le l_1 < l_2 \le n} (\vartheta_{k_1 l_1} - \vartheta_{k_2 l_2})$$

$$= \prod_{k_1 \ne k_2} \prod_{1 \le l_1 < l_2 \le n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot (\alpha_{k_1}^i \cdot \beta_{l_1}^j - \alpha_{k_2}^i \cdot \beta_{l_2}^j)$$

$$\equiv \prod_{k_1\neq k_2} \prod_{1\leq l_1<l_2\leq n} \sum_{j=0}^{n-1} x_{0j} \cdot (\beta_{l_1}^j - \beta_{l_2}^j)$$

$$= \prod_{k_1\neq k_2} \prod_{1\leq l_1<l_2\leq n} (\beta_{l_1} - \beta_{l_2}) \cdot \sum_{j=0}^{n-1} x_{0j} \cdot \left(\frac{\beta_{l_1}^j - \beta_{l_2}^j}{\beta_{l_1} - \beta_{l_2}} \right)$$

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

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

In the case when $\vartheta \in \mathcal{O}_{\mathcal{K}}$ generates a power integral basis in $\mathcal{O}_{\mathcal{K}}$ 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

$$(d(g))^{m(m-1)/2} \equiv \pm 1 \pmod{p}. \tag{10}$$

Performing a similar calculation in the case $g(x) \equiv x^n \pmod{q}$ for F_2 and $F_3 \pmod{q}$ we obtain

$$(d(f))^{n(n-1)/2} \equiv \pm 1 \pmod{q}. \tag{11}$$

This theorem gives a simple condition to exclude the existence of power integral bases in $\mathcal{O}_{\mathcal{K}}$. If the congruences (7) and (8) are both valid and the discriminants D_L, D_M are coprime (this means that we can not apply Theorem 4) then we have to use Theorem 1 for finding the generator elements. On the other hand, if the discriminants D_L, D_M are coprime and if Theorem 4 is applicable, then we can exclude the existence of power integral bases without any tedious computations.

5. Examples

In the examples we use the polynomial orders $\mathcal{O}_{\mathcal{L}}$ and $\mathcal{O}_{\mathcal{M}}$ in the same meaning as in Theorem 2, and similarly $\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathcal{L}}\mathcal{O}_{\mathcal{M}}$.

Example I. Let p, q be square-free integers (≥ 2). One of the most straightforward and frequently used applications of Theorem 4 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

$$d(f) = (-1)^{(m-1)(m-2)/2} \cdot m^m \cdot p^{m-1},$$

$$d(g) = (-1)^{(n-1)(n-2)/2} \cdot n^n \cdot q^{n-1}.$$

By Theorem 4 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 $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\sqrt[m]{p}, \sqrt[n]{q}]$ has no power integral basis.

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

The above congruences are of the form

$$64 \cdot q^3 \equiv \pm 1 \pmod{p}. \tag{12}$$

$$-27 \cdot p^2 \equiv \pm 1 \pmod{q}. \tag{13}$$

If for example $p = 7,\ q = 5$ then $\gcd(D_{\mathcal{O}_{\mathcal{L}}}, D_{\mathcal{O}_{\mathcal{M}}}) = 1$. We have

$$64 \cdot 5^3 = 8000 \equiv 6 \equiv -1 \pmod{7}, \tag{14}$$

$$-27 \cdot 7^2 = -1323 \equiv 2 \equiv -3 \pmod{5}. \tag{15}$$

Theorem 4 implies that there is no power integral basis in $\mathcal{O}_{\mathcal{K}}$.

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

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

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

$$\gcd(D_{\mathcal{O}_{\mathcal{L}}}, D_{\mathcal{O}_{\mathcal{M}}}) = 1,$$

hence Theorem 1 would be applicable. But by applying Theorem 4, 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 $\mathcal{O}_{\mathcal{K}}$.

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 $\mathcal{O}_{\mathcal{K}}$ 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, $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\alpha, \beta]$ (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

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

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

and

$$\gcd(D_{\mathcal{O}_{\mathcal{L}}}, D_{\mathcal{O}_{\mathcal{M}}}) = 1,$$

hence Theorem 1 would be applicable. But by applying Theorem 4, 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 $\mathcal{O}_{\mathcal{K}}$.

References

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

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

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

[4] Gaál, I., *Diophantine equations and power integral bases,* Birkhäuser, Boston, 2002.

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

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

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

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

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

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

[11] Járási, I., Power integral bases in sextic fields with a cubic subfield, *Acta Sci. Math. Szeged*, to appear.

[12] Narkiewicz, W., *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1974.

István Gaál
University of Debrecen
Institute of Mathematics
H–4010 Debrecen, P.O. Box 12.
Hungary
e-mail: igaal@math.klte.hu

Péter Olajos
University of Debrecen
Institute of Mathematics
H–4010 Debrecen, P.O. Box 12.
Hungary
e-mail: olaj@math.klte.hu