Canad. Math. Bull. Vol. **41** (2), 1998 pp. 158–165

POWER INTEGRAL BASES IN COMPOSITS OF NUMBER FIELDS

ISTVÁN GAÁL

ABSTRACT. In the present paper we consider the problem of finding power integral bases in number fields which are composits of two subfields with coprime discriminants. Especially, we consider imaginary quadratic extensions of totally real cyclic number fields of prime degree. As an example we solve the index form equation completely in a two parametric family of fields of degree 10 of this type.

1**. Introduction.** Let K be an algebraic number field of degree n with integral basis $\{b_1 = 1, b_2, \ldots, b_n\}$ and discriminant D_K. The discriminant of the linear form $L(\underline{x}) = x_2b_2, \ldots, x_nb_n$ can be rewritten in the form

$$D_K(x_2, \ldots, x_n) = \big(I_K(x_2, \ldots, x_n)\big)^2 D_K. \tag{1}$$

The index form $I_K(x_2, \ldots, x_n)$ corresponding to the integral basis $\{b_1 = 1, b_2, \ldots, b_n\}$ of K is a homogeneous polynomial of degree $n(n-1)/2$ with rational integer coefficients. Obviously, an algebraic integer

$$\alpha = x_1 + x_2b_2 + \cdots + x_nb_n$$

generates a *power integral basis* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ if and only if $x_1 \in \mathbb{Z}$ and $(x_2, \ldots, x_n)$ is a solution of the *index form equation*

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

Hence, to determine power integral bases (*cf.* Hasse's problem) one has to solve the above index form equation.

Algorithms for the resolution of index form equations in cubic fields were given by Gaál and Schulte [9], and in quartic fields by Gaál, Pethő and Pohst [5], [6]. For certain sextic fields see Gaál [3], [4] and Gaál and Pohst [7].

It has turned out that for higher degree number fields the resolution of index form equations becomes very difficult because of the high degree and the number of variables. For this reason, the results of Section 2 of this paper can be very useful. We consider index form equations over fields which are composits of two subfields with coprime discriminants. For such fields we derive an important consequence of the index form

Received by the editors October 22, 1996.

Research supported in part by Grants 16791 and 16975 from the Hungarian National Foundation for Scientific Research.

AMS subject classification: Primary: 11D57: secondary: 11R21.

https://doi.org/10.4153/CMB-1998-025-3 Published online by Cambridge University Press

equation, which throws also some light on the connection of the solutions of the index form equation in the composite field with the solutions of the index form equation in the subfields.

In Section 3 we specialize the general results of Section 2 to composits of imaginary quadratic fields with totally real cyclic fields of prime degree. For such fields we reduce the resolution of the index form equation in the composite field to the resolution of the index form equation in the totally real cyclic subfield. Our arguments have something common with the argument of [4] where we considered composits of imaginary quadratic fields with totally real cubic fields.

As an application of the explicit results of Section 3, in Section 4 we compose imaginary quadratic fields with a totally real cyclic quintic family of fields, first considered by Emma Lehmer [11]. Recently Gaál and Pohst [8] solved the index form equation completely in this quintic family. Using their result we solve completely the index form equation in the composite field of degree 10. We show that none of the fields in this two parametric family admits a power integral basis.

2. Power integral bases in composits of number fields of 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 $I_M(x_2, \ldots, x_s)$.

Assume, that the discriminants are coprime, that is

$$(D_L, D_M) = 1. \tag{2}$$

Denote by $K = LM$ the composite of L and M. As it is known (*cf.* [12]) the discriminant of K is

$$D_K = D_L^s D_M^r \tag{3}$$

and an integral basis of K is given by

$$\{l_i m_j : 1 \leq i \leq r, 1 \leq j \leq s\}. \tag{4}$$

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

$$\alpha = \sum_{i=1}^{r} \sum_{j=1}^{s} x_{ij} l_i m_j \tag{5}$$

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

In this section we formulate a general necessary condition for $\alpha \in \mathbb{Z}_K$ to be generator of a power integral basis of K.

THEOREM 1. *Assume* $(D_L, D_M) = 1$. *If* α *of (5) generates a power integral basis in* $K = LM$ *then*

$$N_{M/Q}\left(I_L\left(\sum_{i=1}^{s} x_{2i} m_i, \ldots, \sum_{i=1}^{s} x_{ri} m_i\right)\right) = \pm 1 \tag{6}$$

https://doi.org/10.4153/CMB-1998-025-3 Published online by Cambridge University Press

and

$$N_{L/Q}\left(I_M\left(\sum_{i=1}^{r} x_{i2}l_i,\dots,\sum_{i=1}^{r} x_{is}l_i\right)\right)=\pm 1. \tag{7}$$

PROOF. Assume that α generates a power integral basis in K, that is the coefficients x_{ij} satisfy the index form equation corresponding to the basis (4). We show that in the present situation the index form corresponding to the integral basis (4) of K factorizes, and two factors imply equations (6) and (7). The conjugates of α are given by

$$\alpha^{(p,q)}=\sum_{i=1}^{r}\sum_{j=1}^{s} x_{ij}l_i^{(p)}m_j^{(q)}$$

$(1\le p\le r, 1\le q\le s)$. We have

$$\frac{1}{\sqrt{|D_K|}}\prod_{(1,1)\le(p_1,q_1)<(p_2,q_2)\le(r,s)}\left(\alpha^{(p_1,q_1)}-\alpha^{(p_2,q_2)}\right)=\pm 1$$

where the pairs are ordered lexicographically. A factor of the above index form is obtained by building the symmetric polynomial

$$\begin{aligned}\prod_{n=1}^{s}\prod_{1\le i<j\le r}\left(\alpha^{(i,n)}-\alpha^{(j,n)}\right)&=\prod_{n=1}^{s}\prod_{1\le i<j\le r}\left(\sum_{p=1}^{r}\sum_{q=1}^{s}\left(l_p^{(i)}m_q^{(n)}-l_p^{(j)}m_q^{(n)}\right)x_{pq}\right)\\&=\prod_{n=1}^{s}\prod_{1\le i<j\le r}\left(\sum_{p=1}^{r}\left(\left(l_p^{(i)}-l_p^{(j)}\right)\sum_{q=1}^{s}x_{pq}m_q^{(n)}\right)\right)\\&=\left(\sqrt{|D_L|}\right)^{s}N_{M/Q}\left(I_L\left(\sum_{q=1}^{s}x_{2q}m_q,\dots,\sum_{q=1}^{s}x_{rq}m_q\right)\right)\end{aligned}\tag{8}$$

Similarly,

$$\begin{aligned}\prod_{n=1}^{r}\prod_{1\le i<j\le s}\left(\alpha^{(n,i)}-\alpha^{(n,j)}\right)&=\prod_{n=1}^{r}\prod_{1\le i<j\le s}\left(\sum_{p=1}^{r}\sum_{q=1}^{s}\left(l_p^{(n)}m_q^{(i)}-l_p^{(n)}m_q^{(j)}\right)x_{pq}\right)\\&=\prod_{n=1}^{r}\prod_{1\le i<j\le s}\left(\sum_{q=1}^{s}\left(\left(m_q^{(i)}-m_q^{(j)}\right)\sum_{p=1}^{r}x_{pq}l_p^{(n)}\right)\right)\\&=\left(\sqrt{|D_M|}\right)^{r}N_{L/Q}\left(I_M\left(\sum_{p=1}^{r}x_{p2}l_p,\dots,\sum_{p=1}^{r}x_{ps}l_p\right)\right)\end{aligned}\tag{9}$$

The factors containing the discriminants D_L, D_M cancel by dividing by $\sqrt{|D_K|}$ because of (3). The remaining two polynomials have integer coefficients. Since these two factors, as well as the remaining factor of the index form attain integer values, and their product is equal to ±1, hence (8) and (9) imply (6) and (7) respectively. ■

3. **Power integral bases in imaginary quadratic extensions of totally real cyclic fields of prime degree.** In the following p will denote an odd prime. Let L be a totally real cyclic number field of degree p, with integral basis $\{l_1 = 1, l_2, \ldots, l_p\}$, and discriminant D_L. Denote by $I_L(x_2, \ldots, x_p)$ the index form corresponding to the integral basis $\{l_1 = 1, l_2, \ldots, l_p\}$. Also, let $0 < m \in \mathbb{Z}$ be square free with $m \neq 1, 3$ and let $M = \mathbb{Q}(i\sqrt{m})$. An integral basis of M is given by $\{1, \omega\}$ with

$$\omega = \begin{cases} (1 + i\sqrt{m})/2 & \text{if } -m \equiv 1 \bmod 4 \\ i\sqrt{m} & \text{if } -m \equiv 2, 3 \bmod 4 \end{cases} \tag{10}$$

The discriminant of M is

$$D_M = \begin{cases} -m & \text{if } -m \equiv 1 \bmod 4 \\ -4m & \text{if } -m \equiv 2, 3 \bmod 4 \end{cases} \tag{11}$$

As above, we assume that $(D_L, D_M) = 1$. Consider the field $K = LM$. The integers of K can be represented in the form

$$\alpha = x_1 + x_2 l_2 + \cdots + x_p l_p + y_1 \omega + y_2 \omega l_2 + \cdots + y_p \omega l_p \tag{12}$$

with $x_j, y_j \in \mathbb{Z}$, $(1 \leq j \leq p)$.

THEOREM 2. *Assume $m \neq 1, 3$ and $(D_L, D_M) = 1$. If the integer α of (12) generates a power integral basis in $K = LM$, then*

$$I_L(x_2, \ldots, x_p) = \pm 1, \tag{13}$$

$y_1 = \pm 1$ and $y_2 = \cdots = y_p = 0$.

In other words, α must be of the form $\alpha = \beta \pm \omega$ with $\beta \in L$, where β generates a power integral basis in L.

The converse of the assertion is of course not true: elements of the above type do not necessarily generate a power integral basis in K.

Before proving the theorem, we formulate an important consequence of it:

COROLLARY 1. *Let $p \geq 5$ and assume as above $m \neq 1, 3$ and $(D_L, D_M) = 1$. If L is not the maximal real subfield of a cyclotomic field, then the composite field $K = LM$ admits no power integral bases.*

PROOF OF THE COROLLARY. In view of a result of M. N. Gras [10], the cyclic field L of prime degree $p \geq 5$ can only have power integral bases if L is the maximal real subfield of a cyclotomic field. Hence equation (13) is unsolvable in other cases. ∎

Now we turn to the proof of Theorem 2.

https://doi.org/10.4153/CMB-1998-025-3 Published online by Cambridge University Press

PROOF OF THEOREM 2. Assume that α of (12) generates a power integral basis in K. Set $X_j = x_j + \omega y_j$ for $2 \le j \le p$. As an application of Theorem 1 we have

$$N_{M/Q}\bigl(I_L(X_2,\dots,X_p)\bigr) = \pm 1 \tag{14}$$

$$N_{L/Q}(y_1 + y_2 l_2 + \cdots + y_p l_p) = \pm 1 \tag{15}$$

By our assumption on m, the unit group of M is trivial, hence equation (14) implies

$$I_L(X_2,\dots,X_p) = \pm 1. \tag{16}$$

We shall now show, that the unit groups of K and L coincide. Obviously, the unit ranks are equal. By considering those n for which $\varphi(n)$ divides $2p = [K : \mathbb{Q}]$, one can see, that if $m \neq 1, 3$ and K is not the cyclotomic field of degree $2p$, where $p_1 = 2p + 1$ is prime, then apart from ± 1 there are no other torsion units in K. The assumption $(D_L, D_M) = 1$ excludes that K is the above cyclotomic field, for in that case both D_L and D_M were divisible by $p_1 = 2p + 1$. Denote by $\varepsilon_1,\dots,\varepsilon_{p-1}$ the fundamental units in L. It is sufficient to show that for any η of the form

$$\eta = \pm \varepsilon_1^{a_1} \cdots \varepsilon_{p-1}^{a_{p-1}} \tag{17}$$

with $0 \le a_j \le 1$ $(1 \le j \le p-1)$, the square root of η is not contained in K. Suppose on the contrary that $\sqrt{\eta} \in K$. Then there exist $\gamma, \delta \in L$ such that

$$\sqrt{\eta} = \gamma + \delta i \sqrt{m}$$

that is

$$\eta = \gamma^2 - m\delta^2 + 2i\gamma\delta\sqrt{m}.$$

By comparing the imaginary parts, it follows that $\gamma\delta = 0$. If $\delta = 0$ then $\sqrt{\eta} = \gamma \in L$ contradicts to the fact, that $\varepsilon_1,\dots,\varepsilon_{p-1}$ are fundamental units in L. Assume now that $\gamma = 0$, and let $d \in \mathbb{Z}$ be such that $\delta_0 = d\delta$ is integer in L. Then we get

$$\eta = -m\frac{\delta_0^2}{d^2}$$

hence

$$a = -\frac{d^2}{m} = \frac{\delta_0^2}{\eta}$$

is an integer in $\mathbb{Z}$ because the right hand side is an integer. By taking norm it follows that

$$a^p = \pm\bigl(N_{L/Q}(\delta_0)\bigr)^2$$

which is impossible for $p > 2$ except for $a = \pm 1$ in which case $\eta = \pm\delta_0^2$ contradicts again to the fact that $\varepsilon_1,\dots,\varepsilon_{p-1}$ are fundamental units in L.

Consider now equation (16). As it is known, the index form $I_L(X_2,\dots,X_p)$ can be factorized into linear factors $f_j(X_2,\dots,X_p)$ $(1 \le j \le p(p-1)/2)$ with algebraic integer

https://doi.org/10.4153/CMB-1998-025-3 Published online by Cambridge University Press

coefficients. The field L being cyclic, the coefficients of the linear forms are contained in L. If α is a generator of a power integral basis in K, then

$$\prod_{j=1}^{p(p-1)/2} f_j(X_2,\dots,X_p) = \pm 1.$$

Hence each linear factor is a unit in K. But the unit groups of K and L coincide, hence each linear factor is also a unit in L:

$$f_j(X_2,\dots,X_p) = \eta_j \quad \bigl(1 \le j \le p(p-1)/2\bigr).$$

with some units $\eta_j \in L$. Subtracting the conjugate over M of each linear factor from itself we obtain

$$f_j(y_2,\dots,y_p) = 0 \quad \bigl(1 \le j \le p(p-1)/2\bigr).$$

As it is known, the rank of the system of linear forms f_j, $1 \le j \le p(p-1)/2$ is $p-1$, hence the above system of equations implies $y_2 = \cdots = y_p = 0$. By this and equation (16) we get (13). Also, $y_1 = \pm 1$ follows from (15). ■

4. **An example.** Let n be an integer parameter and consider the family of totally real cyclic quintic fields $L = \mathbb{Q}(\vartheta)$ generated by a root of the polynomial

$$(18)\qquad \begin{aligned} f_n(x) = x^5 + n^2x^4 - (2n^3+6n^2+10n+10)x^3 \\ + (n^4+5n^3+11n^2+15n+5)x^2 + (n^3+4n^2+10n+10)x + 1. \end{aligned}$$

This family of fields was first considered by Emma Lehmer [11], then by Schoof and Washington [13] and by Darmon [2]. Let

$$c = n^4 + 5n^3 + 15n^2 + 25n + 25, \qquad d = n^3 + 5n^2 + 10n + 7.$$

In a recent paper Gaál and Pohst [8] proved:

LEMMA 1 ([8]). *Assume that c is square-free. Then an integral basis of L is given by $\{1, \vartheta, \vartheta^2, \vartheta^3, \omega_5\}$ with*

$$\omega_5 = \frac{1}{d}\bigl((n+2) + (2n^2+9n+9)\vartheta + (2n^2+4n-1)\vartheta^2 + (-3n-4)\vartheta^3 + \vartheta^4\bigr),$$

the discriminant of L is

$$D_L = c^4.$$

For $n \ne -1, -2$ there exist no power integral bases in L. For $n = -1, -2$ we get the same field. For $n = -1$ all solutions of the index form equation corresponding to the integral basis $\{1, \vartheta, \vartheta^2, \vartheta^3, \vartheta^4\}$ of L are $(x_2, x_3, x_4, x_5) = (0,1,0,0)$, $(0,3,0,-1)$, $(0,4,0,-1)$, $(1,-4,0,1)$, $(1,-3,0,1)$, $(1,-2,-1,1)$, $(1,-1,-1,0)$, $(1,0,0,0)$, $(1,1,0,0)$, $(2,-1,-1,0)$, $(2,0,-1,0)$, $(2,1,-2,-1)$, $(2,1,-1,0)$, $(2,3,-1,-1)$, $(2,4,-1,-1)$, $(2,8,-1,-2)$, $(3,-1,-1,0)$, $(3,0,-1,0)$, $(3,3,-1,-1)$, $(3,4,-1,-1)$, $(4,-4,-1,1)$, $(5,-11,-1,3)$, $(5,2,-2,-1)$, $(5,13,-2,-3)$, $(11,5,-4,-2)$.

https://doi.org/10.4153/CMB-1998-025-3 Published online by Cambridge University Press

Let $0 < m \in \mathbb{Z}$ be square free with $m \not\equiv 1, 3$ and let $M = \mathbb{Q}(i\sqrt{m})$. Let ω and D_M be the same as in (10), (11).

THEOREM 3. *Assume that $m \not\equiv 1, 3$. Suppose c is square-free and coprime to D_M. Then the field $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ contains no power integral bases.*

PROOF. Under the above conditions the discriminants of L and M are coprime. An integral basis of K is given by $\{1, \vartheta, \vartheta^2, \vartheta^3, \omega_5, \omega, \omega\vartheta, \omega\vartheta^2, \omega\vartheta^3, \omega\omega_5\}$ where ω is the same as in (10).

Denote by $I_L(x_2, \ldots, x_5)$ the index form corresponding to the integer basis $\{1, \vartheta, \vartheta^2, \vartheta^3, \omega_5\}$ of L. By Theorem 2, if

$$\alpha = x_1 + x_2\vartheta + x_3\vartheta^2 + x_4\vartheta^3 + x_5\omega_5 + y_1\omega + y_2\omega\vartheta + y_3\omega\vartheta^2 + y_4\omega\vartheta^3 + y_5\omega\omega_5$$

$(x_i, y_i \in \mathbb{Z})$ generates a power integral basis in K, then

$$I_L(x_2, \ldots, x_5) = \pm 1 \quad \text{in } x_2, x_3, x_4, x_5 \in \mathbb{Z}$$

By Lemma 1 this equation is only solvable for $n = -1, -2$. Hence K can only have power integral bases for $n = -1, -2$. Since these are the same fields, let us fix $n = -1$. Again applying Theorem 2, if $\alpha \in K$ generates a power integral basis, then

$$\alpha = x_1 + x_2\vartheta + x_3\vartheta^2 + x_4\vartheta^3 + x_5\omega_5 \pm \omega$$

where $x_1 \in \mathbb{Z}$ is arbitrary and (x_2, x_3, x_4, x_5) is listed in Lemma 1. By using KANT (*cf.* [1]) we tested these values of α directly and obtained the assertion. ■

ACKNOWLEDGEMENTS. The author is thankful to Klaus Wildanger for the fruitful discussions about the topic during his stay in Debrecen.

REFERENCES

1. M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig and K. Wildanger, *Kant V4*. J. Symb. Comput. **24**(1997), 267–283.

2. H. Darmon, *Note on a polynomial of Emma Lehmer*. Math. Comp. **56**(1991), 795–800.

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

4. ______, *Computing elements of given index in totally complex cyclic sextic fields*. J. Symb. Comput., **20**(1995), 61–69.

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

6. ______, *Simultaneous representation of integers by a pair of ternary quadratic forms—with an application to index form equations in quartic number fields*. J. Number Theory **57**(1996), 90–104.

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

8. ______, *Power integral bases in a parametric family of totally real cyclic quintics*. Math. Comp. **66**(1997), 1689–1696.

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

10. M. N. Gras, *Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$*. J. Number Theory, **23**(1986), 347–353.

https://doi.org/10.4153/CMB-1998-025-3 Published online by Cambridge University Press

11. E. Lehmer, *Connection between Gaussian periods and cyclic units*. Math. Comp. **50**(1988), 535–541.

12. W. Narkiewicz, *Elementary and Analytic Theory of Algerbaic Numbers*. Second Edition, Springer Verlag, 1990.

13. R. Schoof and L. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*. Math. Comp. **50**(1988), 543–556.

Kossuth Lajos University
Mathematical Institute
H-4010 Debrecen Pf.12.
Hungary
e-mail: igaal@math.klte.hu

https://doi.org/10.4153/CMB-1998-025-3 Published online by Cambridge University Press