Monogenitási vizsgálatok algebrai számtestekben

Monogenity of algebraic number fields

doktori (PhD) értekezés tézisei

Nyul Gábor

Debreceni Egyetem

Debrecen, 2007

1. Bevezetés

A számelmélet két fejezete, a diofantikus egyenletek elmélete és az algebrai számelmélet szoros kapcsolatban állnak egymással, például diofantikus egyenletek megoldásakor gyakran lehet algebrai számelméleti eszközöket használni. Az értekezés tárgya az algebrai számelmélet egy klasszikus területének, az algebrai számtestek monogenitásának és ezzel rokon kérdéseknek a vizsgálata, mely ekvivalens bizonyos szétesőforma diofantikus egyenletek, úgynevezett index forma egyenletek megoldásával.

Legyen K egy n-edfokú algebrai számtest és jelölje $\mathbb{Z}_K$ a K-beli algebrai egészek gyűrűjét. Nyilvánvaló, hogy ha $\alpha \in K$ primitív eleme K-nak, azaz $K = \mathbb{Q}(\alpha)$, akkor $(1, \alpha, \ldots, \alpha^{n-1})$ bázisa K-nak $\mathbb{Q}$ felett. Ugyancsak jól ismert, hogy minden algebrai számtestben létezik egész bázis. Az algebrai számelmélet egy klasszikus kérdése annak vizsgálata, hogy létezik-e K-ban a fenti két tulajdonsággal egyszerre rendelkező bázis, azaz létezik-e olyan $\alpha \in \mathbb{Z}_K$ elem, hogy $(1, \alpha, \ldots, \alpha^{n-1})$ egész bázisa K-nak. Az ilyen alakú egész bázist **hatvány egész bázis**nak, α-t pedig a hatvány egész bázis **generátor**ának nevezzük. K-t akkor hívjuk **monogén**nek, ha van hatvány egész bázisa. Egy algebrai számtest monogenitásának eldöntése mellett ugyancsak fontos probléma, hogy monogén testekben hogyan határozhatjuk meg az összes hatvány egész bázist generáló elemet.

Belátható, hogy ha $\alpha \in \mathbb{Z}_K$ primitív eleme K-nak, akkor $\mathbb{Z}[\alpha]^+$ véges indexű részcsoportja a $\mathbb{Z}_K^+$ additív csoportnak és ebben az esetben $I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+)$-t α **index**ének nevezzük. Látható, hogy α pontosan akkor generál hatvány egész bázist K-ban, ha $I(\alpha) = 1$.

A K algebrai számtest m_K **minimális index**e, illetve i_K **testindex**e rendre a K-beli primitív algebrai egészek indexeinek minimuma, illetve legnagyobb közös osztója. Világos, hogy $i_K \mid m_K$, továbbá K-ban akkor és csak akkor létezik hatvány egész bázis, ha $m_K = 1$, és így monogén K esetén $i_K = 1$. (Az utolsó állítás megfordítása nem igaz.)

Legyen $(\omega_1 = 1, \omega_2, \ldots, \omega_n)$ egész bázisa K-nak, $l(\underline{x}) = x_1 + x_2\omega_2 + \ldots + x_n\omega_n$ és $l^{(i)}(\underline{x}) = x_1 + x_2\omega_2^{(i)} + \ldots + x_n\omega_n^{(i)}$, ahol $\omega_j^{(i)}$ jelöli ω_j-nek az i-edik relatív konjugáltját K-ban $(i, j = 1, \ldots, n)$. Ekkor ehhez az egész bázishoz tartozó **diszkriminánsforma**

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

Legyen D_K a K számtest diszkriminánsa. A diszkrimináns forma felírható

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

alakban, ahol $I(x_2, \ldots, x_n)$ egy racionális egész együtthatós, $n(n-1)/2$-edfokú homogén polinom (lsd. például [11], Lemma 1.1.2.). Ezt a polinomot az $(\omega_1 = 1, \omega_2, \ldots, \omega_n)$ egész bázishoz tartozó **index formá**nak nevezzük.

Bebizonyítható (lsd. például [11], Lemma 1.1.3.), hogy ha $\alpha = x_1 + x_2\omega_2 + \ldots + x_n\omega_n \in \mathbb{Z}_K$ $(x_1, x_2, \ldots, x_n \in \mathbb{Z})$ primitív eleme K-nak, akkor $I(\alpha) = |I(x_2, \ldots, x_n)|$. Következésképpen A indexű primitív $\mathbb{Z}_K$-beli elemek keresése (A adott természetes szám) ekvivalens az

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

index forma egyenlet, speciálisan a hatvány egész bázisok keresése ekvivalens a ± 1 jobb oldalú index forma egyenlet megoldásával.

A fentiek alapján a minimális index és a testindex is megadható az index forma segítségével, mivel

$$m_K = \min\{|I(x_2, \ldots, x_n)| \mid x_2, \ldots, x_n \in \mathbb{Z} \text{ és } I(x_2, \ldots, x_n) \neq 0\}$$

és

$$i_K = \text{lnko}\{I(x_2, \ldots, x_n) \mid x_2, \ldots, x_n \in \mathbb{Z}\}.$$

Az $\alpha, \beta \in \mathbb{Z}_K$ elemek **$\mathbb{Z}$-ekvivalens**ek, ha $\alpha - \beta \in \mathbb{Z}$. Ebben az esetben $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, ezért ha $\alpha, \beta \in \mathbb{Z}_K$ $\mathbb{Z}$-ekvivalens primitív elemek, akkor $I(\alpha) = I(\beta)$. Speciálisan ha $\alpha, \beta \in \mathbb{Z}_K$ $\mathbb{Z}$-ekvivalensek és α hatvány egész bázist generál, akkor β is.

Legyenek $p_1, \ldots, p_s$ különböző rögzített prímszámok. Ekkor az index forma egyenlet **p-adikus változat**a az

$$I(x_2, \ldots, x_n) = \pm p_1^{t_1} \cdot \ldots \cdot p_s^{t_s}$$

egyenlet, ahol az ismeretlenek $x_2, \ldots, x_n \in \mathbb{Z}$ az $\text{lnko}(x_2, \ldots, x_n) = 1$ feltétellel és $0 \leq t_1, \ldots, t_s \in \mathbb{Z}$. Ennek megoldása ekvivalens az olyan K-beli primitív algebrai egészek meghatározásával, melyek indexe csak a rögzített prímekkel osztható.

Megjegyezzük, hogy a fenti fogalmak és azok tulajdonságai egyszerűen megfogalmazhatók $\mathbb{Z}_K$ helyett tetszőleges $\mathcal{O} \subseteq \mathbb{Z}_K$ rend esetén is.

Győry K. [26] bebizonyította, hogy az index forma egyenleteknek csak véges sok megoldásuk van, a megoldások abszolút értékére pedig effektív felső korlátot vezetett le. (A felső korlát legjobb ismert javítása [29]-ben található.) A bizonyítást az index forma egyenlet egységegyenletekre történő visszavezetésével és a Baker-módszert alkalmazva nyerte. Következményként adódik, hogy $\mathbb{Z}$-ekvivalenciától eltekintve csak véges sok adott indexű primitív $\mathbb{Z}_K$-beli elem létezik, speciálisan $\mathbb{Z}$-ekvivalenciától eltekintve csak véges sok hatvány egész bázis generátor van.

Az eredmény effektív volta algoritmuselméleti szempontból azt jelenti, hogy az index forma egyenletek megoldása, adott indexű primitív algebrai egész elemek keresése, hatvány egész bázis generátorok keresése elvben elvégezhető, ha a korlátig végignézzük az ismeretlenek összes lehetséges értékét. A felső korlátok azonban még a kis fokszámú testek esetén is olyan nagyok, hogy a gyakorlatban ez a módszer önmagában nem kivitelezhető, így hatékony algoritmusok keresése továbbra is fontos feladat maradt.

Az index forma egyenlet p-adikus változata esetén szintén *Győry K.* [27] adott a megoldásokra effektív felső korlátot, melyre ugyancsak elmondhatók az előbb leírtak.

Az elmúlt évtizedekben többen értek el jelentős eredményeket az index forma egyenlet, illetve az ehhez kapcsolódó algebrai számelméleti problémák megoldására vonatkozó hatékony algoritmusok keresésében (lsd. [11]). Igazán hatékony algoritmus csak harmadfokú (*Gaál I.*, *N. Schulte* [23]), negyedfokú (*Gaál I.*, *Pethő A.*, *M. Pohst* [19], [22]) és néhány speciális magasabbfokú számtest esetén ismert. Létezik továbbá általános algoritmus ötödfokú (*Gaál I.*, *Győry K.* [12]) és hatodfokú (*Y. Bilu*, *Gaál I.*, *Győry K.* [4]) számtestekre, melyek kivitelezhetők ugyan, de még nem tekinthetők igazán hatékonynak.

A másik lehetséges irány szerint algebrai számtestek egy családjában (például egy parametrikus családban) kell megoldani ezeket a problémákat. Ez azt jelenti, hogy a megoldást a család összes teste esetén egyszerre keressük.

Az értekezés további fejezetei mind az eddig ismertetett problémák valamelyikével foglalkoznak bizonyos algebrai számtestek esetén. Most röviden áttekintjük ezeket az eredményeket.

A 2. fejezetben egy gyors algoritmust adunk, ami adott valós másodfokú számtest esetén megadja az összes olyan vegyes szignatúrájú diéder negyedfokú számtestet, melyben van hatvány egész bázis és melynek részteste az adott másodfokú test, egyúttal ezekben meghatározza az összes hatvány egész bázis generátort.

A 3. fejezet célja, hogy a teljesen komplex eset vizsgálatával teljessé tegye a monogenitás vizsgálatát bikvadratikus számtestekben. Egyszerűen ellenőrizhető szükséges és elégséges feltételt adunk hatvány egész bázis létezésére és leírjuk az összes hatvány egész bázist generáló elemet.

A 4. fejezet olyan hatékony algoritmust ismertet, mely bikvadratikus számtestekben az index forma egyenlet p-adikus változatát oldja meg.

Az értekezés 5. fejezetében multikvadratikus számtestekben mutatjuk meg különböző feltételek mellett, hogy a testbeli algebrai egészek gyűrűjében, illetve egy bizonyos rendben nincs hatvány egész bázis.

Az utolsó fejezetben algebrai számtestek két parametrikus családja, a Kishi-féle harmadfokú testek és a legegyszerűbb negyedfokú testek esetén határozzuk meg a testindexet.

2. Diéder negyedfokú számtestek monogenitása

2.1. Negyedfokú számtestek monogenitása

Negyedfokú algebrai számtestekben az index forma egyenlet megoldásával, hatvány egész bázis keresésével *Gaál I.*, *Pethő A.* és *M. Pohst* [17], [18], [19], [20], [21], [22] egy cikksorozatban foglalkoztak részletesen. Ezek közül [19] és [22] tetszőleges negyedfokú számtest esetén alkalmazható hatékony algoritmust ismertet.

Legyen $K = \mathbb{Q}(\xi)$ egy tetszőleges negyedfokú algebrai számtest, ahol $\xi \in \mathbb{Z}_K$ definiáló polinomja $f(t) = t^4 + a_1t^3 + a_2t^2 + a_3t + a_4 \in \mathbb{Z}[t]$ és ξ indexe $m = I(\xi)$. Valamilyen $a, x, y, z \in \mathbb{Z}$ számokkal és $d \in \mathbb{Z}$ rögzített közös nevezővel bármely $\alpha \in \mathbb{Z}_K$ elem felírható az alábbi alakban:

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

A 2.1.1. tétel (*Gaál I., Pethő A., M. Pohst* [19], Theorem 2.1.) szerint α indexe pontosan akkor A, ha az

$$F(u,v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3 = \pm\frac{d^6A}{m} \quad (1)$$

egyenletnek van olyan $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ megoldása, hogy az x, y, z együtthatók teljesítik a következő egyenlőségeket:

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

Ha $F(u, v)$ reducibilis $\mathbb{Q}$ felett, akkor (1) egyszerűen megoldható, amúgy egy harmadfokú Thue-egyenlet. Ezután az (1) egyenlet összes (u, v) megoldására tekintenünk kell a (2) egyenletrendszert. Ennek megoldása [19] és [22]-t követve negyedfokú Thue-egyenletre vezethető vissza. Ha $F(u, v)$ irreducibilis, akkor az (1) Thue-egyenletet, illetve a fellépő negyedfokú Thue-egyenletet *Y. Bilu* és *G. Hanrot* [5] módszerével lehet gyorsan megoldani.

2.2. Diéder negyedfokú számtestek

A $K = \mathbb{Q}(\xi)$ negyedfokú algebrai számtestet **diéder negyedfokú számtest**nek nevezzük, ha ξ definiáló polinomjának Galois-csoportja nyolcad-

rendű diéder csoport. Ezeknek egyetlen M másodfokú résztestük van.

A. C. Kable [33] diéder negyedfokú számtestekben adott szükséges és elégséges feltételt hatvány egész bázis létezésére. Számunkra tételének két következménye lesz fontos. A 2.2.1. lemma (*A. C. Kable* [33], Corollary 1.) azt állítja, hogy ha K monogén, akkor az előjel megfelelő választásával $D_K \pm 4D_M^3$ négyzetszám.

Amennyiben K vegyes szignatúrájú diéder negyedfokú számtest, akkor $D_K < 0$, M pedig valós másodfokú számtest, ezért $D_M > 0$. Így adódik a 2.2.2. lemma (*A. C. Kable* [33], Corollary 2.) állítása, mely szerint ha K vegyes szignatúrájú és van benne hatvány egész bázis, akkor $|D_K| \leq 4D_M^3$.

2.3. Az algoritmus

A 2.2.2. lemma szerint adott M valós másodfokú számtest esetén csak véges sok olyan monogén, vegyes szignatúrájú diéder negyedfokú számtest létezik, melynek másodfokú részteste M. Ebben a részben ezek meghatározására adunk gyors algoritmust.

A fentiek értelmében a K vegyes szignatúrájú diéder negyedfokú számtestek közül elég csak azokat vizsgálni, melyekre $|D_K| \leq 4D_M^3$ teljesül. Ha M részteste K-nak, akkor $D_M^2 \mid D_K$ ellenőrzése tovább szűkíti a szóba jöhető testek körét. Az így megmaradó testek közül a 2.1. részben ismertetett eljárással választjuk ki azokat, amelyekben valóban van hatvány egész bázis, egyúttal meghatározzuk a hatvány egész bázist generáló elemeket is. (Megjegyezzük, hogy diéder negyedfokú testek esetén az (1) egyenlet bal oldala reducibilis, ezért egyszerűen megoldható.)

2.4. Numerikus példák

Az algoritmust példaként azokban az esetekben alkalmaztuk, amikor $M = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$. Például $M = \mathbb{Q}(\sqrt{5})$ esetén az alábbi három vegyes szignatúrájú diéder negyedfokú számtest adódik:

$D_K = -275, f(t) = t^4 - t^3 + 2t - 1, d = 1$
$(x, y, z) = (0, 0, 1), (1, 0, 0), (2, -2, 1), (1, 2, -4), (0, 1, -1)$

$D_K = -400, f(t) = t^4 - t^2 - 1, d = 1$
$(x, y, z) = (1, 0, 0), (0, 1, 1), (1, 0, -1), (0, 1, -1)$

$D_K = -475, f(t) = t^4 - t^3 - 2t^2 - 2t - 1, d = 1$
$(x, y, z) = (1, 0, 0), (0, 2, -1), (2, 1, -1)$

3. Bikvadratikus számtestek monogenitása

3.1. Bikvadratikus számtestek

Egy testet **bikvadartikus számtest**nek nevezünk, ha $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ alakú negyedfokú algebrai számtest, ahol $m, n \in \mathbb{Z} \setminus \{0, 1\}$ különböző négyzetmentes racionális egész számok. A továbbiak során legyen $l = \text{lnko}(m, n) > 0$ és m_1, n_1 az $m = lm_1$ és $n = ln_1$ egyenlőségekkel definiálva.

Bikvadratikus számtestek monogenitásával és ehhez kapcsolódó problémákkal többen is foglalkoztak: *T. Nakahara* [43], *Gaál I.*, *Pethő A.* és *M. Pohst* [16], [21], *T. Funakura* [8], *M.-N. Gras* és *F. Tanoé* [25], *Y. Motoda* [41]. Kiemeljük ezek közül, hogy *Gaál I.*, *Pethő A.* és *M. Pohst* [21] teljesen valós bikvadratikus számtestek esetén szimultán Pell-egyenletekre vezető hatékony algoritmust adtak az index forma egyenlet megoldására. Módszerük illusztrálására az összes 10^6-nál kisebb diszkriminánsú, teljesen valós bikvadratikus számtest esetén kiszámították a minimális indexet és meghatározták az összes ilyen indexű elemet.

3.2. Teljesen komplex bikvadratikus testek monogenitása

A továbbiakban az lesz a célunk, hogy a teljesen komplex eset vizsgálatával teljessé tegyük a monogenitás témakörét bikvadratikus számtestekben. A $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ bikvadratikus számtest pontosan akkor teljesen komplex, ha m és n közül legalább az egyik negatív szám.

K. S. Williams [53] megállapította, hogy minden bikvadratikus számtest esetén meg lehet m, n, m_1, n_1-et úgy választani, hogy azok a 4-gyel való oszthatóság szempontjából öt eset valamelyikébe tartozzanak. A teljesen komplex esetben az előjelekre is ügyelve az adódik, hogy m és n választható úgy, hogy a következő esetek valamelyike álljon fenn:

1. eset: $m > 0$, $n < 0$, $m \equiv 1 \pmod 4$, $n \equiv 1 \pmod 4$, $m_1 \equiv 1 \pmod 4$, $n_1 \equiv 1 \pmod 4$
2. eset: $m > 0$, $n < 0$, $m \equiv 1 \pmod 4$, $n \equiv 1 \pmod 4$, $m_1 \equiv 3 \pmod 4$, $n_1 \equiv 3 \pmod 4$
3/A. eset: $m > 0$, $n < 0$, $m \equiv 1 \pmod 4$, $n \equiv 2 \pmod 4$
3/B. eset: $m < 0$, $n > 0$, $m \equiv 1 \pmod 4$, $n \equiv 2 \pmod 4$
4/A. eset: $m > 0$, $n < 0$, $m \equiv 2 \pmod 4$, $n \equiv 3 \pmod 4$
4/B. eset: $m < 0$, $n > 0$, $m \equiv 2 \pmod 4$, $n \equiv 3 \pmod 4$

5/A. eset: $m > 0$, $n < 0$, $m \equiv 3 \pmod 4$, $n \equiv 3 \pmod 4$
5/B. eset: $m < 0$, $n < 0$, $m \equiv 3 \pmod 4$, $n \equiv 3 \pmod 4$

K. S. Williams [53] (Theorem 2., 3.) mindegyik esetben parametrikus formában meghatározott egy egész bázist és megadta a test diszkriminánsát. Ezeket az eredményeket felhasználva *Gaál I.*, *Pethő A.* és *M. Pohst* [16] esetenként kiszámították az egész bázishoz tartozó index formákat:

1. eset:

$$\left(l(x_2+\frac{x_4}{2})^2-\frac{n_1}{4}x_4^2\right)\left(l(x_3+\frac{x_4}{2})^2-\frac{m_1}{4}x_4^2\right)\left(n_1(x_3+\frac{x_4}{2})^2-m_1(x_2+\frac{x_4}{2})^2\right)$$

2. eset:

$$\left(l(x_2-\frac{x_4}{2})^2-\frac{n_1}{4}x_4^2\right)\left(l(x_3+\frac{x_4}{2})^2-\frac{m_1}{4}x_4^2\right)\left(n_1(x_3+\frac{x_4}{2})^2-m_1(x_2-\frac{x_4}{2})^2\right)$$

3. eset:

$$\left(lx_2^2-n_1x_4^2\right)\left(l(x_3+\frac{x_4}{2})^2-\frac{m_1}{4}x_4^2\right)\left(n_1(2x_3+x_4)^2-m_1x_2^2\right)$$

4. eset:

$$\left(\frac{l}{2}(2x_2+x_4)^2-\frac{n_1}{2}x_4^2\right)\left(2lx_3^2-\frac{m_1}{2}x_4^2\right)\left(2n_1x_3^2-\frac{m_1}{2}(2x_2+x_4)^2\right)$$

5. eset:

$$\left(l(2x_2+x_3)^2-n_1x_4^2\right)\left(lx_3^2-m_1x_4^2\right)\left(\frac{n_1}{4}x_3^2-m_1(x_2+\frac{x_3}{2})^2\right)$$

A következő tételben olyan szükséges és elégséges feltételt adunk a teljesen komplex bikvadratikus számtestek monogenitására, mely alapján könnyen ellenőrizhető, hogy egy adott testben van-e hatvány egész bázis. Továbbá amikor létezik hatvány egész bázis, akkor leírjuk az összes hatvány egész bázist generáló elemet. Kiderül, hogy a generátoroknak az egész bázisra vonatkozó együtthatói minden esetben a paraméterektől nem függő, konstans vektorok egy kis elemszámú halmazából kerülnek ki.

3.2.1. Tétel (Nyul G. [45])
Legyen $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ *a felsorolt esetek valamelyikébe tartozó teljesen komplex bikvadratikus számtest.*
Az 1., 2. és 3/A. esetben K *nem monogén.*
A további esetekben K*-ban a hatvány egész bázis létezésének szükséges és elégséges feltétele:*
3/B. eset: $m_1 = -1$, $l - 4n_1 = -1$ *(és a feltétel miatt* $n_1 > 0$*).*

4/A. eset: $m_1 = 2$, $n_1 = -1$, $l = 1$, *azaz* $m = 2$ *és* $n = -1$.
4/B. eset: $m_1 = -2$, $l - n_1 = \pm 2$ *(és a feltétel miatt* $n_1 > 0$*).*
5/A. eset: $n_1 = -1$, $4l - m_1 = 1$ *(és a feltétel miatt* $m_1 > 0$*).*
5/B. eset: $l = 1$, $n_1 - m_1 = \pm 4$ *(és a feltétel miatt* $m_1, n_1 < 0$*).*

Ha K monogén, akkor a megfelelő index formával vett $I(x_2, x_3, x_4) = \pm 1$ *index forma egyenlet megoldásai:*
3/B. eset: $(x_2, x_3, x_4) = \pm(1, 1, -2), \pm(1, -1, 2)$
4/A. eset: $(x_2, x_3, x_4) = \pm(0, 0, 1), \pm(1, 0, -1)$
4/B. eset: $(x_2, x_3, x_4) = \pm(0, 0, 1), \pm(1, 0, -1)$
5/A. eset: $m_1 = 3$, $n_1 = -1$, $l = 1$, *azaz* $m = 3$, $n = -1$ *esetén*
$(x_2, x_3, x_4) = \pm(1, -2, 1), \pm(1, -2, -1), \pm(0, 1, 0), \pm(1, -1, 0)$
A többi 5/A. esetbeli testre $(x_2, x_3, x_4) = \pm(1, -2, 1), \pm(1, -2, -1)$
5/B. eset: $(x_2, x_3, x_4) = \pm(0, 1, 0), \pm(1, -1, 0)$

3.3. Teljesen komplex bikvadratikus számtestek táblázata

A 3.2.1. tétel bizonyításának fontos eleme, hogy bikvadratikus számtestek esetén az index forma minden esetben három egész együtthatós kvadratikus forma szorzatára bomlik, a teljesen komplex esetben pedig ezen tényezők között mindig van definit kvadratikus forma. Ezen a módon teljesen komplex bikvadratikus számtestekben tetszőleges jobb oldalú index forma egyenletet is meg lehet oldani. Ezt alkalmazva a teljesen valós esetnél említetthez hasonló táblázatot készítünk, melyben összefoglaljuk a 10^3-nál (az értekezésben a 10^4-nél) kisebb diszkriminánsú teljesen komplex bikvadratikus számtesteket, kiszámolva i_K testindexüket, m_K minimális indexüket és az $I(x_2, x_3, x_4) = \pm m_K$ egyenlet összes megoldását.

D_K	m_1	n_1	l	i_K	m_K	(x_2, x_3, x_4)
144	3	−1	1	1	1	$(1,-2,1),(1,-1,0),(0,1,0),(1,-2,-1)$
225	−3	5	1	2	2	$(0,1,-1),(0,0,1),(1,0,-1),(1,1,-1)$
256	2	−1	1	1	1	$(0,0,1),(1,0,-1)$
400	−1	−5	1	1	1	$(0,1,0),(1,-1,0)$
441	−1	7	3	2	2	$(0,1,-1),(1,0,1),(1,-1,1),(0,0,1)$
576	−3	2	1	1	4	$(0,1,-1),(0,0,1)$
576	−1	2	3	1	3	$(1,1,-1),(1,0,-1),(1,0,1),(1,-1,1)$
784	7	−1	1	1	2	$(1,-1,0),(0,1,0)$

4. Az index forma egyenlet p-adikus változata bikvadratikus számtestekben

4.1. A módszer rövid ismertetése

Ebben a fejezetben az index forma egyenlet p-adikus változatának megoldásával foglalkozunk bikvadratikus számtestekben. Megjegyezzük, hogy eltekintve egy *N. P. Smart* [49] által megoldott példától (egy teljesen komplex ciklikus negyedfokú számtestben, a 2 és 3 prímeket használva) p-adikus index forma egyenletet eddig még nem oldottak meg.

Legyenek $p_1, \ldots, p_s$ különböző rögzített prímszámok és tekintsük az

$$I(x_2, x_3, x_4) = \pm p_1^{t_1} \cdot \ldots \cdot p_s^{t_s} \tag{3}$$

p-adikus index forma egyenletet, ahol $x_2, x_3, x_4 \in \mathbb{Z}$, $0 \leq t_1, \ldots, t_s \in \mathbb{Z}$ az ismeretlenek az $\text{lnko}(x_2, x_3, x_4) = 1$ feltétel mellett.

A továbbiakhoz vezessük be az alábbi új, egész értékű paramétereket és ismeretleneket:

eset	u_1	u_2	u_3	a	b	c	d	f	g	t	x	y	z
1.	m_1	n_1	l	n_1	4	m_1	4	n_1	4	1	x_4	$2x_2 + x_4$	$2x_3 + x_4$
2.	m_1	n_1	l	n_1	4	m_1	4	n_1	4	1	x_4	$2x_2 - x_4$	$2x_3 + x_4$
3.	m_1	$4n_1$	l	n_1	1	m_1	4	n_1	1	1	x_4	x_2	$2x_3 + x_4$
4.	m_1	n_1	l	n_1	2	$m_1/2$	1	$2n_1$	1	2	x_4	$2x_2 + x_4$	x_3
5.	m_1	n_1	$4l$	n_1	1	m_1	1	n_1	4	1	x_4	$2x_2 + x_3$	x_3

A megfelelő index forma i-edik tényezőjének abszolút értékét jelöljük $F_i = F_i(x_2, x_3, x_4)$-gyel ($i = 1, 2, 3$). Ekkor a 4.1.1. lemma (*Gaál I., Pethő A., M. Pohst* [21], Lemma 1.) szerint

$$\pm u_1 F_1 \pm u_2 F_2 = \pm u_3 F_3. \tag{4}$$

Az index forma tényezőire fennáll a következő egyenletrendszer is:

$$\begin{aligned} (ax)^2 - ny^2 &= \pm abF_1 \\ (cx)^2 - mz^2 &= \pm cdF_2 \\ (fz)^2 - m_1 n_1 y^2 &= \pm fgF_3 \end{aligned}$$

Ennek bal oldalai lineáris formák szorzatára bomlanak a bikvadratikus számtest másodfokú résztesteiben, melyeket az alábbi azonosság kapcsol

össze:

$$tc(ax - \sqrt{n}y) - ta(cx - \sqrt{m}z) = \sqrt{m}(fz - \sqrt{m_1 n_1}y) \tag{5}$$

A 4.4.2. lemmának köszönhetően a (3) p-adikus index forma egyenlet megoldásához az esetek jelentős részében elegendő a (4)-ből származó $\mathbb{Z}$ feletti S-egység egyenletet megoldani, kivéve amikor az egyenlet jobb oldalán álló prímszámok valamelyike két különböző prímideál szorzatára bomlik fel a bikvadratikus számtest mindhárom másodfokú résztestében. Ekkor még meg kell oldanunk egy (5)-ből következő S-egység egyenletet a negyedfokú test felett is.

Az S-egység egyenletek megoldásakor a felső korlátok meghatározásához *K. Yu* [54] p-adikus és *A. Baker*, *G. Wüstholz* [2] komplex logaritmusok lineáris formáira vonatkozó becslését használjuk. A korlátok redukcióját egyrészt a *B. M. M. de Weger* [52] egy ötletén alapuló 4.3.1. lemma (*Gaál I., Járási I., F. Luca* [13], Lemma 4.1.), másrészt a 4.7.1. lemma (ez [11] Lemma 2.2.2. egy kis módosítással adódó vátozata) alapján végezzük el.

4.2. Három megoldott példa

Algoritmusunk illusztrálásaként három konkrét p-adikus index forma egyenletet is megoldunk.

Első példaként a $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ teljesen komplex bikvadratikus számtest esetén a $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ prímszámokkal végül 276 darab megoldás adódik.

Következő példaként a $\mathbb{Q}(\sqrt{5}, \sqrt{2})$ teljesen valós bikvadratikus számtestben a $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ prímszámok mellett 280 darab megoldást kapunk.

Utolsóként pedig ha a $\mathbb{Q}(\sqrt{19}, \sqrt{7})$ teljesen valós bikvadratikus számtestet tekintjük és a p-adikus index forma egyenlet jobb oldalán szereplő prímek $p_1 = 2$, $p_2 = 3$, akkor a megoldások száma 104.

Az első két példában a $\mathbb{Z}$ feletti S-egység egyenlet megoldásával lényegében már célt érünk. A harmadik példa esetén azonban a 3 a bikvadratikus számtest mindhárom másodfokú résztestében két különböző prímideál szorzatára esik szét, ezért ebben az esetben meg kell oldani még egy S-egység egyenletet a negyedfokú test felett is.

5. Multikvadratikus számtestek monogenitása

5.1. Multikvadratikus számtestek

A bikvadratikus számtestek természetes általánosításai a multikvadratikus számtestek. Legyen $n \in \mathbb{N}$, továbbá $k_1, \ldots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ páronként különböző négyzetmentes egész számok. Ekkor a $\mathbb{Q}(\sqrt{k_1}, \ldots, \sqrt{k_n})$ testet **multikvadratikus számtest**nek hívjuk.

Multikvadratikus számtestekben $n \geq 3$ esetén index forma egyenletekkel és a monogenitás problémájával kapcsolatban a közelmúltig nem születtek eredmények. Az alább ismertetendő tételeken kívül újabban *Y. Motoda* és *T. Nakahara* [42] értek el erre vonatkozó további eredményeket.

5.2. Három másodfokú számtest kompozitumának monogenitása

Az ebben a részben vizsgált multikvadratikus számtestek három másodfokú résztestük kompozitumaként állnak elő, ahol feltételeink biztosítani fogják, hogy a másodfokú testek diszkriminánsai páronként relatív prímek. Ezért egy egész bázisuk és diszkriminánsuk az 5.2.1. lemma ([44] Theorem 4.26.) alkalmazásával kapható, majd vizsgálható az ehhez tartozó index forma.

5.2.2. Tétel (Nyul G. [46], Theorem 3.)

Legyenek $k, l, m \in \mathbb{Z} \setminus \{0, 1\}$ páronként relatív prímek, négyzetmentesek, $k < 0$ és $l \equiv m \equiv 1 \pmod 4$. Ekkor az $N = \mathbb{Q}(\sqrt{k}, \sqrt{l}, \sqrt{m})$ nyolcadfokú számtestben nincs hatvány egész bázis.

5.3. Testindex multikvadratikus számtestekben

Most páratlan diszkriminánsú multikvadratikus számtestek esetén igazoljuk, hogy a testindex páros, amiből következik, hogy maximális rendjükben nincs hatvány egész bázis. A bizonyítás *R. Dedekind* ([44] Theorem 4.34.) tételén alapszik és felhasználjuk, hogy 2 különböző prímideálok szorzatára esik szét testünkben.

5.3.1. Tétel (Nyul G. [46], Theorem 1.)

Legyenek $n \in \mathbb{N}$, $n \geq 3$ és $k_1, \ldots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ páronként különböző négyzetmentes számok úgy, hogy $K = \mathbb{Q}(\sqrt{k_1}, \ldots, \sqrt{k_n})$ egy 2^n-edfokú algebrai

számtest és D_K páratlan. Ekkor K testindexe páros, következésképpen K-ban nincs hatvány egész bázis.

MEGJEGYZÉS Az 5.2.2. tétel állítása $k \equiv 1 \pmod 4$ esetén az 5.3.1. tételből is következik, ugyanis ekkor D_N páratlan.

5.4. Monogenitás multikvadratikus számtestek egy rendjében

A most következő eredmény tetszőleges multikvadratikus számtest esetén teljesül, a monogenitást azonban a maximális rend helyett a $\mathbb{Z}[\sqrt{k_1}, \ldots, \sqrt{k_n}]$ rendben vizsgáljuk. Mielőtt igazolnánk, hogy ebben a rendben minden elem indexe osztható 2-nek egy nagy kitevős hatványával, meghatározzuk a rend diszkriminánsát, hogy majd vizsgálni tudjuk az index formát.

5.4.1. LEMMA (Nyul G. [46], Lemma 1.)

Ha $n \in \mathbb{N}$, $k_1, \ldots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ páronként különböző négyzetmentes egész számok és $\mathbb{Q}(\sqrt{k_1}, \ldots, \sqrt{k_n})$ egy 2^n-edfokú algebrai számtest, akkor az $\mathcal{O} = \mathbb{Z}[\sqrt{k_1}, \ldots, \sqrt{k_n}]$ rend diszkriminánsa $D_{\mathcal{O}} = (k_1 \cdot \ldots \cdot k_n)^{2^{n-1}} \cdot 2^{n \cdot 2^n}$.

5.4.2. TÉTEL (Nyul G. [46], Theorem 2.)

Az 5.4.1. lemma jelölései és feltételei mellett az $\mathcal{O}$ rendben minden elem indexe osztható $2^{2^{n-1}(2^n-n-1)}$-gyel.

Mivel $n \geq 2$ esetén a tételbeli kitevő 1-nél nagyobb, így adódik az alábbi következmény.

5.4.3. KÖVETKEZMÉNY *Az 5.4.1. lemma jelölései és feltételei mellett, $n \geq 2$ esetén az $\mathcal{O}$ rendben nincs hatvány egész bázis.*

6. Algebrai számtestek testindexe

6.1. Testindex

Algebrai számtestek testindexével kapcsolatban többen értek el eredményeket: *M. Bauer* [3], *E. von Żyliński* [55], *H. T. Engstrom* [7]. Megmutatható, hogy a tiszta harmadfokú számtestek testindexe 1, tiszta negyedfokú számtestekben *T. Funakura* [8], bikvadratikus számtestekben *T. Nakahara* [43] illetve *Gaál I.*, *Pethő A.* és *M. Pohst* [16], ciklikus negyedfokú számtestekben *B. K. Spearman* és *K. S. Williams* [51] vizsgálták a testindexet.

6.2. Kishi-féle harmadfokú testek

Legyen α gyöke a $t^3-a(a^2+a+3)(a^2+2)t^2-(a^3+2a^2+3a+3)t-1 \in \mathbb{Z}[t]$ polinomnak, ahol $a \in \mathbb{Z}$. A $K = K_a = \mathbb{Q}(\alpha)$ **Kishi-féle harmadfokú testek** teljesen valós, ciklikus harmadfokú számtestek.

Legyen

$$\delta_1 = \begin{cases} 0 & \text{ha } 2 \mid a \\ 1 & \text{ha } 2 \nmid a \end{cases}, \quad \delta_2 = \begin{cases} 0 & \text{ha } a \equiv 2 \pmod 3 \\ 1 & \text{ha } a \not\equiv 2 \pmod 3 \end{cases},$$

továbbá

$$B = \frac{(a^2+3)(a^4+a^3+4a^2+3)}{4^{\delta_1} \cdot 9^{\delta_2}}.$$

Y. Kishi [36] négyzetmentes B esetén keresett alapegységrendszert K-ban, valamint a 6.2.1. lemma ([36], Corollary 1.4.) szerint megadta K diszkriminánsát.

A továbbiakhoz a Kishi-féle harmadfokú testeket az a paramétertől függően a következő hat esetbe soroljuk:

1. eset: $a \equiv 0, 2 \pmod 6$ vagy $a \equiv 4, 10 \pmod{18}$
2. eset: $a \equiv 34, 52 \pmod{54}$
3. eset: $a \equiv 3, 5 \pmod 6$ vagy $a \equiv 1, 13 \pmod{18}$
4. eset: $a \equiv 7, 25 \pmod{54}$
5. eset: $a \equiv 16 \pmod{54}$
6. eset: $a \equiv 43 \pmod{54}$

Az alábbiakban meghatározzuk a Kishi-féle harmadfokú testek egy egész bázisát, majd az ehhez tartozó index forma kiszámítása után belátjuk, hogy ezen számtestcsalád minden elemének testindexe 1.

6.2.2. Tétel

Ha B négyzetmentes, akkor a $K = \mathbb{Q}(\alpha)$ Kishi-féle harmadfokú test egy egész bázisa

1. eset: $\left(1, \alpha, \dfrac{-a+(-a+1)\alpha+\alpha^2}{a^2+1}\right)$

2. eset: $\left(1, \alpha, \dfrac{a^2-a+1+(2a^2-a+3)\alpha+\alpha^2}{3(a^2+1)}\right)$

3. eset: $\left(1, \dfrac{1+\alpha}{2}, \dfrac{-a+(-a+1)\alpha+\alpha^2}{2(a^2+1)}\right)$

4. eset: $\left(1, \dfrac{1+\alpha}{2}, \dfrac{4a^2-a+4+(2a^2-a+3)\alpha+\alpha^2}{6(a^2+1)}\right)$

5. eset: $\left(1, \dfrac{2+\alpha}{3}, \dfrac{4a^2-a+4+(2a^2-a+3)\alpha+\alpha^2}{9(a^2+1)}\right)$

6. eset: $\left(1, \dfrac{5+\alpha}{6}, \dfrac{4a^2-a+4+(2a^2-a+3)\alpha+\alpha^2}{18(a^2+1)}\right)$

Ehhez az egész bázishoz tartozó index forma például a 3. esetben

$$\begin{aligned} I(x_2,x_3) &= \left(-\frac{1}{2}a^2-\frac{1}{2}\right)x_2^3+\left(-a^5-a^4-5a^3-2a^2-\frac{9}{2}a-\frac{3}{2}\right)x_2^2x_3 \\ &\quad+\left(-\frac{1}{2}a^8-a^7-5a^6-6a^5-\frac{27}{2}a^4-10a^3-\frac{21}{2}a^2-\frac{15}{2}a\right)x_2x_3^2 \\ &\quad+\left(\frac{1}{2}a^7+\frac{1}{2}a^6+\frac{7}{2}a^5+a^4+\frac{13}{2}a^3-a^2+\frac{9}{2}a+\frac{3}{2}\right)x_3^3. \end{aligned}$$

6.2.3. Tétel

Ha B négyzetmentes, akkor a K Kishi-féle harmadfokú test testindexe 1.

6.3. Legegyszerűbb negyedfokú testek

Legyen $a \in \mathbb{Z} \setminus \{0\}$ és tegyük fel, hogy a^2+16 nem osztható 1-nél nagyobb páratlan négyzetszámmal. Az $f_a(t) = t^4 - at^3 - 6t^2 + at + 1 \in \mathbb{Z}[t]$ polinom felbontási testeként előálló $K = K_a$ testeket a **legegyszerűbb negyedfokú testek** családjának nevezzük. Ezek teljesen valós, ciklikus negyedfokú számtestek. *M.-N. Gras* [24] megmutatta, hogy a legegyszerűbb negyedfokú testek családja végtelen sok testből áll. A 6.3.1. lemmában összefoglalt módon *A. J. Lazarus* [37] (Table 4.1.) ezen testek diszkriminánsát, *H. K. Kim* és *J. S. Kim* [35] (Theorem 2.3.) pedig egy egész bázisát adták meg.

A hatvány egész bázisokat a legegyszerűbb negyedfokú testek $\mathbb{Z}[\alpha]$ rendjében ($\alpha \in \mathbb{Z}_K$ az $f_a(t)$ egy gyöke) *G. Lettl* és *Pethő A.* [38], míg a K-beli algebrai egészek gyűrűjében *Olajos P.* [47] írta le.

A 2.1.1. tétel felhasználásával igazoljuk, hogy a legegyszerűbb negyedfokú testek testindexe a paritásától függően 1 vagy 2. Eredményünkkel páratlan a esetén új bizonyítást nyerünk *Olajos P.* [47] tételére.

6.3.2. Tétel *A K legegyszerűbb negyedfokú test testindexe*

$$i_K = \begin{cases} 1 & ha \;\; a \equiv 0 \pmod 2 \\ 2 & ha \;\; a \equiv 1 \pmod 2). \end{cases}$$

1. Introduction

Two major branches of number theory, the theory of diophantine equations and algebraic number theory are closely related. For example when solving diophantine equations, we often use algebraic number theoretical tools. The subject of our thesis is a classical field of algebraic number theory, namely we investigate monogenity of algebraic number fields and related topics which are equivalent to solving certain diophantine equations, called index form equations.

Let K be an algebraic number field of degree n and denote the ring of algebraic integers in K by $\mathbb{Z}_K$. Obviously if $\alpha \in K$ is a primitive element of K that is $K = \mathbb{Q}(\alpha)$, then $(1, \alpha, \ldots, \alpha^{n-1})$ is a basis of K over $\mathbb{Q}$. It is also well-known that each algebraic number field has integral bases. A classical problem of algebraic number theory is to decide if K admits bases satisfying these two properties simultaneously, in other words whether there exists $\alpha \in \mathbb{Z}_K$ with $(1, \alpha, \ldots, \alpha^{n-1})$ being an integral basis. Such integral basis is called a **power integral basis** and α the **generator** of it. K is called **monogeneous** if it has power integral bases. In addition to deciding the existence of power integral bases, another important problem is to find all generators of power integral bases in monogeneous number fields.

It can be proved that if $\alpha \in \mathbb{Z}_K$ is a primitive element of K, then $\mathbb{Z}[\alpha]^+$ is a subgroup with finite index of $\mathbb{Z}_K^+$ and in this case the **index** of α is defined by $I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+)$. This α generates a power integral basis in K if and only if $I(\alpha) = 1$.

We define the **minimal index** m_K and the **field index** i_K of K as the minimum and the greatest common divisor of the indices of all primitive algebraic integer elements in K, respectively. It is clear that $i_K \mid m_K$, K admits power integral bases if and only if $m_K = 1$, and so for monogeneous fields K we have $i_K = 1$. (The converse of the last statement is not true.)

Let $(\omega_1 = 1, \omega_2, \ldots, \omega_n)$ be an integral basis of K, $l(\underline{x}) = x_1 + x_2\omega_2 + \ldots + x_n\omega_n$ and $l^{(i)}(\underline{x}) = x_1 + x_2\omega_2^{(i)} + \ldots + x_n\omega_n^{(i)}$, where $\omega_j^{(i)}$ denotes the i-th relative conjugate of ω_j in K $(i, j = 1, \ldots, n)$. The **discriminant form** corresponding to this integral basis is

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

If the discriminant of K is D_K, then the discriminant form can be written

as

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

where $I(x_2, \ldots, x_n)$ is a homogeneous polynomial of degree $n(n-1)/2$ with integer coeffiecients (see [11], Lemma 1.1.2.). This polynomial is called the **index form** corresponding to the integral basis $(\omega_1 = 1, \omega_2, \ldots, \omega_n)$.

It can be shown (see [11], Lemma 1.1.3.) that if $\alpha = x_1 + x_2\omega_2 + \ldots + x_n\omega_n \in \mathbb{Z}_K$ $(x_1, x_2, \ldots, x_n \in \mathbb{Z})$ is a primitive element of K, then $I(\alpha) = |I(x_2, \ldots, x_n)|$. Hence determining primitive elements of $\mathbb{Z}_K$ with index A (where A is a given natural number) is equivalent to solving the **index form equation**

$$I(x_2, \ldots, x_n) = \pm A \quad (x_2, \ldots, x_n \in \mathbb{Z}).$$

Especially determining all power integral bases is equivalent to solving the index form equation with ± 1 on the right hand side.

The minimal index and the field index can also be given using the index form since

$$m_K = \min \{|I(x_2, \ldots, x_n)| \mid x_2, \ldots, x_n \in \mathbb{Z} \text{ és } I(x_2, \ldots, x_n) \neq 0\}$$

and

$$i_K = \gcd \{I(x_2, \ldots, x_n) \mid x_2, \ldots, x_n \in \mathbb{Z}\}.$$

The elements $\alpha, \beta \in \mathbb{Z}_K$ are called **$\mathbb{Z}$-equivalent**, if $\alpha - \beta \in \mathbb{Z}$. Then $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, hence if $\alpha, \beta \in \mathbb{Z}_K$ are $\mathbb{Z}$-equivalent primitive elements, then $I(\alpha) = I(\beta)$. Especially if $\alpha, \beta \in \mathbb{Z}_K$ are $\mathbb{Z}$-equivalent and α generates a power integral basis, then so does β.

Let $p_1, \ldots, p_s$ be given distinct prime numbers. The **p-adic version** of the index form equation is

$$I(x_2, \ldots, x_n) = \pm p_1^{t_1} \cdot \ldots \cdot p_s^{t_s}$$

where the unknowns are $x_2, \ldots, x_n \in \mathbb{Z}$ with $\gcd(x_2, \ldots, x_n) = 1$ and $0 \leq t_1, \ldots, t_s \in \mathbb{Z}$. Solving this equation is equivalent to determining the primitive algebraic integers in K of index divisible by the fixed primes only.

Remark that the above definitions and their properties can also be given in any order $\mathcal{O} \subseteq \mathbb{Z}_K$ instead of $\mathbb{Z}_K$.

K. Győry [26] proved that index form equations have only finitely many solutions and effective upper bounds can be given for the absolute values of

the solutions. (For the best known improved bounds see [29].) In the proof he reduced the index form equation to unit equations and used Baker's method. This result imply that up to $\mathbb{Z}$-equivalence there are only finitely many elements in $\mathbb{Z}_K$ with given index, especially up to $\mathbb{Z}$-equivalence there are only finitely many generators of power integral bases.

From a purely algorithmic point of view, the effectiveness of this result means that index form equations can be solved and primitive algebraic integer elements of given index, generators of power integral bases can be found by checking all possible values of the variables less than the upper bound. But these upper bounds are much too large for practical applications, even in number fields of small degree, so searching for efficient algorithms remained an important problem.

Also for the solutions of the p-adic analogue of index form equations *K. Győry* [27] gave an effective upper bound of the same nature.

In the last decades considerable effort was made to construct efficient algorithms for solving index form equations and answering the related questions (see [11]). Efficient algorithms are known for cubic (*I. Gaál*, *N. Schulte* [23]), for quartic (*I. Gaál*, *A. Pethő*, *M. Pohst* [19], [22]) and for some special higher degree number fields. There are general algorithms for quintic (*I. Gaál*, *K. Győry* [12]) and for sextic (*Y. Bilu*, *I. Gaál*, *K. Győry* [4]) fields, but they are not really efficient.

The other possible direction is to solve these problems in a family of algebraic number fields (for example in a parametric family). This means to find the solutions in each field of the family.

In the next chapters of our thesis we deal with some of the above problems in certain types of algebraic number fields. Now we briefly summarize these results.

In the second chapter we present a fast algorithm for finding all monogeneous mixed dihedral quartic number fields containing a given real quadratic field as a subfield. We also determine all generators of power integral bases.

To complete the theory of monogenity in biquadratic number fields, our purpose in the third chapter is to give a necessary and sufficient condition for the existence of power integral bases in totally complex biquadratic number fields which can be easily checked. We also describe all generators of power integral bases in totally complex biquadratic number fields.

In Chapter 4 we give an efficient algorithm to solve the p-adic version of index form equation in biquadratic number fields.

In Chapter 5 we prove for multiquadratic number fields that under different assumptions there exist no power integral bases in the ring of algebraic integers of the field or in a certain order.

In the last chapter we compute the field indices in two parametric families of algebraic number fields, the cubic fields of Kishi and the simplest quartic fields.

2. Monogenity of dihedral quartic number fields

2.1. Monogenity of quartic number fields

There is a series of papers about solving index form equations and finding power integral bases in quartic number fields by *I. Gaál*, *A. Pethő* and *M. Pohst* [17], [18], [19], [20], [21], [22]. In [19] and [22] they gave an efficient algorithm which can be used in any quartic field.

Let $K = \mathbb{Q}(\xi)$ be an arbitrary quartic number field where the minimal polynomial of $\xi \in \mathbb{Z}_K$ is $f(t) = t^4 + a_1t^3 + a_2t^2 + a_3t + a_4 \in \mathbb{Z}[t]$ and the index of ξ is $m = I(\xi)$. We can represent any $\alpha \in \mathbb{Z}_K$ in the form

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

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

Theorem 2.1.1. (*I. Gaál, A. Pethő, M. Pohst* [19], Theorem 2.1.) states that the index of α is A if and only if there exists a solution $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ of the cubic equation

$$F(u,v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3 = \pm\frac{d^6A}{m} \quad (6)$$

such that x, y, z satisfy the following equations:

$$\begin{aligned} Q_1(x,y,z) &= x^2 - a_1xy + a_2y^2 + (a_1^2 - 2a_2)xz + (a_3 - a_1a_2)yz \\ &\quad +(-a_1a_3 + a_2^2 + a_4)z^2 = u\ , \\ Q_2(x,y,z) &= y^2 - xz - a_1yz + a_2z^2 = v\ . \end{aligned} \quad (7)$$

If $F(u, v)$ is reducible over $\mathbb{Q}$, then (6) is easy to solve, otherwise it is a cubic Thue equation. Then for every solution (u, v) we have to determine the solutions of the system (7). It can be reduced to quartic Thue equations by [19] and [22]. If $F(u, v)$ is irreducible, then the Thue equation (6), and the resulting other quartic Thue equations can be solved by the method of *Y. Bilu* and *G. Hanrot* [5].

2.2. Dihedral quartic number fields

The quartic number field $K = \mathbb{Q}(\xi)$ is called a **dihedral quartic number field**, if the Galois group of the minimal polynomial of ξ is a dihedral group of order eight. These fields have a unique quadratic subfield M.

A. C. Kable [33] gave necessary and sufficient conditions for dihedral quartic fields to have power integral bases. For us two consequences of his theorem will be important. Lemma 2.2.1. (*A. C. Kable* [33], Corollary 1.) states that if K is monogeneous, then, with a suitable choice of sign, $D_K \pm 4D_M^3$ is a square.

In the case of dihedral quartic fields K with mixed signature we have $D_K < 0$, M is a real quadratic field, hence $D_M > 0$. Thus we get Lemma 2.2.2. (*A. C. Kable* [33], Corollary 2.) which asserts that if K is mixed and has a power integral basis, then $|D_K| \leq 4D_M^3$.

2.3. The algorithm

By Lemma 2.2.2. for a given real quadratic number field M there exist only finitely many monogeneous mixed dihedral quartic field containing M as a subfield. Now we present a fast algorithm for determining all such quartic fields.

We have seen that it is enough to study those mixed dihedral quartic fields K for which $|D_K| \leq 4D_M^3$ holds. If M is a subfield of K, then checking $D_M^2 \mid D_K$ also decreases the number of the candidate fields. From the remaining fields we choose those having indeed power integral bases by the method discussed in Part 2.1. We also determine all generators of power integral bases. (Remark that in the case of dihedral quartic fields the left hand side of (6) is always reducible, hence it is easy to solve.)

2.4. Numerical examples

To illustrate our algorithm we performed computations for $M = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$. For example when $M = \mathbb{Q}(\sqrt{5})$, we got three mixed dihedral quartic fields:

$$D_K = -275, f(t) = t^4 - t^3 + 2t - 1, d = 1$$
$$(x, y, z) = (0, 0, 1), (1, 0, 0), (2, -2, 1), (1, 2, -4), (0, 1, -1)$$
$$D_K = -400, f(t) = t^4 - t^2 - 1, d = 1$$
$$(x, y, z) = (1, 0, 0), (0, 1, 1), (1, 0, -1), (0, 1, -1)$$
$$D_K = -475, f(t) = t^4 - t^3 - 2t^2 - 2t - 1, d = 1$$
$$(x, y, z) = (1, 0, 0), (0, 2, -1), (2, 1, -1)$$

3. Monogenity of biquadratic number fields

3.1. Biquadratic number fields

Quartic fields of type $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ are called **biquadratic number fields** where $m, n \in \mathbb{Z} \setminus \{0, 1\}$ are distinct square-free integers. In the sequel let $l = \gcd(m, n) > 0$ and let m_1, n_1 be defined by $m = lm_1$ and $n = ln_1$.

The monogenity of biquadratic number fields and related topics in these fields were considered by several authors cf. *T. Nakahara* [43], *I. Gaál*, *A. Pethő* and *M. Pohst* [16], [21], *T. Funakura* [8], *M.-N. Gras* and *F. Tanoé* [25], *Y. Motoda* [41]. We emphasize that *I. Gaál*, *A. Pethő* and *M. Pohst* [21] gave an efficient algorithm for solving index form equations in totally real biquadratic fields by solving simultanous Pellian equations. Using this method they determined the minimal indices and all elements with minimal index in totally real biquadratic fields having discriminant less than 10^6.

3.2. Monogenity of totally complex biquadratic fields

To complete the above theory of monogenity in biquadratic number fields, our purpose is to characterize totally complex biquadratic fields having power integral bases. The biquadratic field $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is totally complex if and only if at least one of m and n is negative.

K. S. Williams [53] established that m, n, m_1, n_1 can be chosen such that any biquadratic field belongs to one of five given cases. In the totally complex case, with respect to the signs, m and n can be chosen such that one of the following cases holds:

Case 1: $m > 0$, $n < 0$, $m \equiv 1 \pmod 4$, $n \equiv 1 \pmod 4$, $m_1 \equiv 1 \pmod 4$, $n_1 \equiv 1 \pmod 4$
Case 2: $m > 0$, $n < 0$, $m \equiv 1 \pmod 4$, $n \equiv 1 \pmod 4$, $m_1 \equiv 3 \pmod 4$, $n_1 \equiv 3 \pmod 4$
Case 3/A: $m > 0$, $n < 0$, $m \equiv 1 \pmod 4$, $n \equiv 2 \pmod 4$
Case 3/B: $m < 0$, $n > 0$, $m \equiv 1 \pmod 4$, $n \equiv 2 \pmod 4$
Case 4/A: $m > 0$, $n < 0$, $m \equiv 2 \pmod 4$, $n \equiv 3 \pmod 4$
Case 4/B: $m < 0$, $n > 0$, $m \equiv 2 \pmod 4$, $n \equiv 3 \pmod 4$
Case 5/A: $m > 0$, $n < 0$, $m \equiv 3 \pmod 4$, $n \equiv 3 \pmod 4$
Case 5/B: $m < 0$, $n < 0$, $m \equiv 3 \pmod 4$, $n \equiv 3 \pmod 4$

In each case *K. S. Williams* [53] (Theorem 2., 3.) described an integral basis and the discriminant of these fields. *I. Gaál*, *A. Pethő* and *M. Pohst* [16] formulated the corresponding index forms:

Case 1:

$$\left(l(x_2+\frac{x_4}{2})^2-\frac{n_1}{4}x_4^2\right)\left(l(x_3+\frac{x_4}{2})^2-\frac{m_1}{4}x_4^2\right)\left(n_1(x_3+\frac{x_4}{2})^2-m_1(x_2+\frac{x_4}{2})^2\right)$$

Case 2:

$$\left(l(x_2-\frac{x_4}{2})^2-\frac{n_1}{4}x_4^2\right)\left(l(x_3+\frac{x_4}{2})^2-\frac{m_1}{4}x_4^2\right)\left(n_1(x_3+\frac{x_4}{2})^2-m_1(x_2-\frac{x_4}{2})^2\right)$$

Case 3:

$$\left(lx_2^2-n_1x_4^2\right)\left(l(x_3+\frac{x_4}{2})^2-\frac{m_1}{4}x_4^2\right)\left(n_1(2x_3+x_4)^2-m_1x_2^2\right)$$

Case 4:

$$\left(\frac{l}{2}(2x_2+x_4)^2-\frac{n_1}{2}x_4^2\right)\left(2lx_3^2-\frac{m_1}{2}x_4^2\right)\left(2n_1x_3^2-\frac{m_1}{2}(2x_2+x_4)^2\right)$$

Case 5:

$$\left(l(2x_2+x_3)^2-n_1x_4^2\right)\left(lx_3^2-m_1x_4^2\right)\left(\frac{n_1}{4}x_3^2-m_1(x_2+\frac{x_3}{2})^2\right)$$

In the next theorem we give necessary and sufficient conditions for the monogenity of totally complex biquadratic number fields, which can be used to check easily the existence of power integral bases in such fields. We also describe all generators of power integral bases. It turns out that the coordinates of the generators are contained in a finite set of constant vectors.

THEOREM **3.2.1.** (G. Nyul [45])
Let $K=\mathbb{Q}(\sqrt{m},\sqrt{n})$ be a totally complex biquadratic number field represented in one of the cases listed above.
In cases 1, 2 and 3/A the field K is not monogeneous.
In the other cases the necessary and sufficient condition of the existence of power integral bases in K is:
Case 3/B: $m_1=-1$, $l-4n_1=-1$ (and by the assumption $n_1>0$).
Case 4/A: $m_1=2$, $n_1=-1$, $l=1$, so $m=2$ and $n=-1$.
Case 4/B: $m_1=-2$, $l-n_1=\pm 2$ (and by the assumption $n_1>0$).
Case 5/A: $n_1=-1$, $4l-m_1=1$ (and by the assumption $m_1>0$).
Case 5/B: $l=1$, $n_1-m_1=\pm 4$ (and by the assumption $m_1,n_1<0$).

If K is monogeneous, then the solutions of the index form equation $I(x_2,x_3,x_4)=\pm 1$ are:

Case 3/B: $(x_2, x_3, x_4) = \pm(1, 1, -2), \pm(1, -1, 2)$
Case 4/A: $(x_2, x_3, x_4) = \pm(0, 0, 1), \pm(1, 0, -1)$
Case 4/B: $(x_2, x_3, x_4) = \pm(0, 0, 1), \pm(1, 0, -1)$
Case 5/A: For $m_1 = 3$, $n_1 = -1$, $l = 1$ *that is for* $m = 3$, $n = -1$
$(x_2, x_3, x_4) = \pm(1, -2, 1), \pm(1, -2, -1), \pm(0, 1, 0), \pm(1, -1, 0)$
For the other fields of this case $(x_2, x_3, x_4) = \pm(1, -2, 1), \pm(1, -2, -1)$
Case 5/B: $(x_2, x_3, x_4) = \pm(0, 1, 0), \pm(1, -1, 0)$

3.3. Table of totally complex biquadratic number fields

It is important in the proof of Theorem 3.2.1. that the index form splits into three quadratic factors having integer coefficients in biquadratic fields, moreover in the totally complex case there is a definite quadratic form among these factors. Using this we can solve index form equations with arbitrary number on the right hand side. This way we can present a list of all totally complex biquadratic fields up to discriminant 10^3 (in the thesis up to 10^4) computing the field indices i_K, minimal indices m_K and all solutions of the equation $I(x_2, x_3, x_4) = \pm m_K$.

D_K	m_1	n_1	l	i_K	m_K	(x_2, x_3, x_4)
144	3	−1	1	1	1	$(1,-2,1),(1,-1,0),(0,1,0),(1,-2,-1)$
225	−3	5	1	2	2	$(0,1,-1),(0,0,1),(1,0,-1),(1,1,-1)$
256	2	−1	1	1	1	$(0,0,1),(1,0,-1)$
400	−1	−5	1	1	1	$(0,1,0),(1,-1,0)$
441	−1	7	3	2	2	$(0,1,-1),(1,0,1),(1,-1,1),(0,0,1)$
576	−3	2	1	1	4	$(0,1,-1),(0,0,1)$
576	−1	2	3	1	3	$(1,1,-1),(1,0,-1),(1,0,1),(1,-1,1)$
784	7	−1	1	1	2	$(1,-1,0),(0,1,0)$

4. The p-adic version of the index form equation in biquadratic number fields

4.1. Brief description of the method

In this chapter we present an efficient algorithm for solving the p-adic analogue of the index form equation in biquadratic number fields. Note that except from an example solved by *N. P. Smart* [49] (in a totally complex cyclic quartic field, using primes 2 and 3) no p-adic index form equations have been solved so far.

Let $p_1, \ldots, p_s$ be distinct fixed primes and consider the solutions $x_2, x_3, x_4 \in \mathbb{Z}$ with $\gcd(x_2, x_3, x_4) = 1$ and $0 \leq t_1, \ldots, t_s \in \mathbb{Z}$ of the equation

$$I(x_2, x_3, x_4) = \pm p_1^{t_1} \cdot \ldots \cdot p_s^{t_s}. \tag{8}$$

In order to be able to deal with all cases in a unique way introduce new integer parameters and variables:

eset	u_1	u_2	u_3	a	b	c	d	f	g	t	x	y	z
1.	m_1	n_1	l	n_1	4	m_1	4	n_1	4	1	x_4	$2x_2 + x_4$	$2x_3 + x_4$
2.	m_1	n_1	l	n_1	4	m_1	4	n_1	4	1	x_4	$2x_2 - x_4$	$2x_3 + x_4$
3.	m_1	$4n_1$	l	n_1	1	m_1	4	n_1	1	1	x_4	x_2	$2x_3 + x_4$
4.	m_1	n_1	l	n_1	2	$m_1/2$	1	$2n_1$	1	2	x_4	$2x_2 + x_4$	x_3
5.	m_1	n_1	$4l$	n_1	1	m_1	1	n_1	4	1	x_4	$2x_2 + x_3$	x_3

Denote by $F_i = F_i(x_2, x_3, x_4)$ the absolute value of the i-th factor of the index form ($i = 1, 2, 3$). Lemma 4.1.1. (*I. Gaál, A. Pethő, M. Pohst* [21], Lemma 1.) states that

$$\pm u_1 F_1 \pm u_2 F_2 = \pm u_3 F_3. \tag{9}$$

For the quadratic factors of the index form we have

$$\begin{aligned} (ax)^2 - ny^2 &= \pm abF_1 \\ (cx)^2 - mz^2 &= \pm cdF_2 \\ (fz)^2 - m_1 n_1 y^2 &= \pm fgF_3 \end{aligned}$$

The left hand sides of these equations split into linear factors in the quadratic subfields of the biquadratric field. The linear factors are connected according to the identity

$$tc(ax - \sqrt{n}y) - ta(cx - \sqrt{m}z) = \sqrt{m}(fz - \sqrt{m_1 n_1}y). \tag{10}$$

By Lemma 4.4.2. in most of the cases it is enough to solve the S-unit equation over $\mathbb{Z}$ coming from (9) to solve the p-adic index form equation (8) completely. But if there is a prime on the right hand side of our equation which splits into the product of two distinct prime ideals in all the three quadratic subfields of the biquadratic field, then we have to proceed by solving an S-unit equation based on (10) over the quartic field.

To compute upper bounds for the solutions of the S-unit equation, our method involves estimates for the linear forms of p-adic (*K. Yu* [54]) and complex (*A. Baker*, *G. Wüstholz* [2]) logarithms. The bounds are reduced by the reduction procedures using Lemma 4.3.1. (*I. Gaál, I. Járási, F. Luca* [13], Lemma 4.1. based on an idea of *B. M. M. de Weger* [52]) and Lemma 4.7.1. (which is a tiny modification of [11], Lemma 2.2.2).

4.2. Three examples

To illustrate our algorithm we solve three specific p-adic index form equations.

In the first example for the totally complex biquadratic field $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ and primes $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ we get 276 solutions.

In our next example there are 280 solutions, when considering the totally real biquadratic field $\mathbb{Q}(\sqrt{5}, \sqrt{2})$, the primes are $p_1 = 2$, $p_2 = 3$, $p_3 = 5$.

Finally if we consider the totally real biquadratic field $\mathbb{Q}(\sqrt{19}, \sqrt{7})$ and the primes $p_1 = 2$, $p_2 = 3$, then the p-adic index form equation has 104 solutions.

In the first two examples it was enough to solve an S-unit equation over $\mathbb{Z}$. But in the third example 3 is the product of two distinct prime ideals in each quadratic subfield, hence we have to solve an S-unit equation over the quartic field too.

5. Monogenity of multiquadratic number fields

5.1. Multiquadratic number fields

As the generalization of biquadratic number fields we get multiquadratic number fields. Let $n \in \mathbb{N}$ and $k_1, \ldots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ be pairwise distinct square-free integers. Then the field $\mathbb{Q}(\sqrt{k_1}, \ldots, \sqrt{k_n})$ is a **multiquadratic number field**.

For $n \geq 3$ in multiquadratic number fields index form equations and the problem of monogenity were not yet investigated. Beside the following theorems recently *Y. Motoda* and *T. Nakahara* [42] presented some other results.

5.2. Monogenity of the composite of three quadratic number fields

In this part we consider multiquadratic fields that are composites of three quadratic subfields, where by the assumptions the discriminants of the quadratic fields are pairwise coprime. An integral basis and the discriminant can be given using Lemma 5.2.1. ([44] Theorem 4.26.), then we can consider the corresponding index form.

THEOREM **5.2.2.** (G. Nyul [46], Theorem 3.)
Let $k, l, m \in \mathbb{Z} \setminus \{0, 1\}$ be pairwise coprime, square-free, $k < 0$ and $l \equiv m \equiv 1 \pmod 4$. Then the octic field $N = \mathbb{Q}(\sqrt{k}, \sqrt{l}, \sqrt{m})$ has no power integral bases.

5.3. Field index of multiquadratic number fields

In our next result we show that the field index of multiquadratic number fields with odd discriminant is even, from which it follows that there is no power integral bases in their maximal order. The proof of the following statement depends on a theorem of *R. Dedekind* ([44] Theorem 4.34.) and we shall utilize that 2 does not ramify in the field.

THEOREM **5.3.1.** (G. Nyul [46], Theorem 1.)
Let $n \in \mathbb{N}$, $n \geq 3$ and let $k_1, \ldots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ be pairwise distinct square-free integers, such that $K = \mathbb{Q}(\sqrt{k_1}, \ldots, \sqrt{k_n})$ is of degree 2^n with odd discriminant. Then the field index of K is even, hence K is not

monogeneous.

REMARK If $k \equiv 1 \pmod 4$, then Theorem 5.2.2. also follows from Theorem 5.3.1., because in that case D_N is odd.

5.4. Monogenity in an order of multiquadratic number fields

The following result deals with arbitrary multiquadratic fields, but we consider monogenity in the order $\mathbb{Z}[\sqrt{k_1}, \ldots, \sqrt{k_n}]$ of the field. In order to prove that the indices of the elements of this order are divisible by a high power of 2, we need to determine the discriminant of the order.

LEMMA **5.4.1.** (G. Nyul [46], Lemma 1.)
If $n \in \mathbb{N}$, $k_1, \ldots, k_n \in \mathbb{Z} \setminus \{0, 1\}$ are pairwise distinct square-free integers and $\mathbb{Q}(\sqrt{k_1}, \ldots, \sqrt{k_n})$ is of degree 2^n, then the discriminant of the order $\mathcal{O} = \mathbb{Z}[\sqrt{k_1}, \ldots, \sqrt{k_n}]$ is $D_{\mathcal{O}} = (k_1 \cdot \ldots \cdot k_n)^{2^{n-1}} \cdot 2^{n \cdot 2^n}$.

THEOREM **5.4.2.** (G. Nyul [46], Theorem 2.)
Using the notation and assumptions of Lemma 5.4.1. the index of any element of $\mathcal{O}$ is divisible by $2^{2^{n-1}(2^n-n-1)}$.

For $n \geq 2$ the power in this theorem is greater than 1, hence we have the following consequence.

COROLLARY **5.4.3.** *Using the notation and assumptions of Lemma 5.4.1., for $n \geq 2$ the order $\mathcal{O}$ has no power integral bases.*

6. Field index of algebraic number fields

6.1. Field index

Several authors considered field indices of algebraic number fields cf. *M. Bauer* [3], *E. von Żyliński* [55], *H. T. Engstrom* [7]. It can be shown that the field index of pure cubic fields is 1, in pure quartic fields *T. Funakura* [8], in biquadratic number fields *T. Nakahara* [43] and *I. Gaál*, *A. Pethő*, *M. Pohst* [16], in cyclic quartic fields *B. K. Spearman* and *K. S. Williams* [51] investigated the field indices.

6.2. Cubic fields of Kishi

Let α be a root of the polynomial $t^3 - a(a^2+a+3)(a^2+2)t^2 - (a^3+2a^2+3a+3)t - 1 \in \mathbb{Z}[t]$ where $a \in \mathbb{Z}$. We call the totally real cyclic cubic number fields $K = K_a = \mathbb{Q}(\alpha)$ the **cubic fields of Kishi**.

Let

$$\delta_1 = \begin{cases} 0 & \text{if } 2 \mid a \\ 1 & \text{if } 2 \nmid a \end{cases}, \quad \delta_2 = \begin{cases} 0 & \text{if } a \equiv 2 \pmod 3 \\ 1 & \text{if } a \not\equiv 2 \pmod 3 \end{cases}$$

and

$$B = \frac{(a^2+3)(a^4+a^3+4a^2+3)}{4^{\delta_1} \cdot 9^{\delta_2}}.$$

Y. Kishi [36] found a system of fundamental units in K and gave the discriminant of K in Lemma 6.2.1. ([36], Corollary 1.4.) when B is square-free.

In the sequel we will have the following six cases for the cubic fields of Kishi depending on the parameter a:

Case 1: $a \equiv 0, 2 \pmod 6$ or $a \equiv 4, 10 \pmod{18}$
Case 2: $a \equiv 34, 52 \pmod{54}$
Case 3: $a \equiv 3, 5 \pmod 6$ or $a \equiv 1, 13 \pmod{18}$
Case 4: $a \equiv 7, 25 \pmod{54}$
Case 5: $a \equiv 16 \pmod{54}$
Case 6: $a \equiv 43 \pmod{54}$

We describe an integral basis of the cubic fields of Kishi, compute the corresponding index form and using it we prove that the field index of these fields is 1.

THEOREM **6.2.2.**
If B is square-free, then an integral basis of the cubic field $K = \mathbb{Q}(\alpha)$ of Kishi is

Case 1: $\left(1, \alpha, \dfrac{-a+(-a+1)\alpha+\alpha^2}{a^2+1}\right)$

Case 2: $\left(1, \alpha, \dfrac{a^2-a+1+(2a^2-a+3)\alpha+\alpha^2}{3(a^2+1)}\right)$

Case 3: $\left(1, \dfrac{1+\alpha}{2}, \dfrac{-a+(-a+1)\alpha+\alpha^2}{2(a^2+1)}\right)$

Case 4: $\left(1, \dfrac{1+\alpha}{2}, \dfrac{4a^2-a+4+(2a^2-a+3)\alpha+\alpha^2}{6(a^2+1)}\right)$

Case 5: $\left(1, \dfrac{2+\alpha}{3}, \dfrac{4a^2-a+4+(2a^2-a+3)\alpha+\alpha^2}{9(a^2+1)}\right)$

Case 6: $\left(1, \dfrac{5+\alpha}{6}, \dfrac{4a^2-a+4+(2a^2-a+3)\alpha+\alpha^2}{18(a^2+1)}\right)$

The corresponding index form for example in Case 3 is

$$\begin{aligned} I(x_2, x_3) &= \left(-\frac{1}{2}a^2 - \frac{1}{2}\right)x_2^3 + \left(-a^5 - a^4 - 5a^3 - 2a^2 - \frac{9}{2}a - \frac{3}{2}\right)x_2^2 x_3 \\ &\quad + \left(-\frac{1}{2}a^8 - a^7 - 5a^6 - 6a^5 - \frac{27}{2}a^4 - 10a^3 - \frac{21}{2}a^2 - \frac{15}{2}a\right)x_2 x_3^2 \\ &\quad + \left(\frac{1}{2}a^7 + \frac{1}{2}a^6 + \frac{7}{2}a^5 + a^4 + \frac{13}{2}a^3 - a^2 + \frac{9}{2}a + \frac{3}{2}\right)x_3^3. \end{aligned}$$

THEOREM **6.2.3.**
If B is square-free, then the field index of the cubic field K of Kishi is 1.

6.3. Simplest quartic fields

Let $a \in \mathbb{Z} \setminus \{0\}$ and suppose that $a^2 + 16$ is not divisible by any odd squares other than 1. The splitting fields $K = K_a$ of the polynomials $f_a(t) = t^4 - at^3 - 6t^2 + at + 1 \in \mathbb{Z}[t]$ are called the family of **simplest quartic fields**. These are totally real cyclic quartic fields. *M.-N. Gras* [24] proved that the family of simplest quartic fields is infinite. As summarized in Lemma 6.3.1. we know the discriminant by *A. J. Lazarus* [37] (Table 4.1.) and an integral basis by *H. K. Kim* and *J. S. Kim* [35] (Theorem 2.3.) of these fields.

In simplest quartic fields power integral bases were described in the order $\mathbb{Z}[\alpha]$ ($\alpha \in \mathbb{Z}_K$ is a root of $f_a(t)$) by *G. Lettl* and *A. Pethő* [38] and in the ring of integers of K by *P. Olajos* [47].

Using Theorem 2.1.1. we prove that the field index of a simplest quartic field is 1 or 2 depending on the parity of a. Our result gives a new proof of the theorem of *P. Olajos* [47] when a is odd.

THEOREM **6.3.2.** *The field index of the simplest quartic field K is*

$$i_K = \begin{cases} 1 & \text{if } a \equiv 0 \pmod 2 \\ 2 & \text{if } a \equiv 1 \pmod 2. \end{cases}$$

Irodalom

[1] A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford, **20** (1969), 129–137.

[2] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math., **442** (1993), 19–62.

[3] M. Bauer, *Über den ausserwesentlicher Diskriminantenteiler algebraischer Körper*, Math. Ann., **64** (1907), 573.

[4] Y. Bilu, I. Gaál and K. Győry, *Index form equations in sextic fields: a hard computation*, Acta Arith., **115** (2004), 85–96.

[5] Y. Bilu and G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory, **60** (1996), 373–392.

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

[7] H. T. Engstrom, *On the common index divisors of an algebraic field*, Trans. Amer. Math. Soc., **32** (1930), 223–237.

[8] T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ., **26** (1984), 27–41.

[9] I. Gaál, *Computing power integral bases in algebraic number fields*, in: Number Theory (eds. K. Győry, A. Pethő and V. T. Sós), Walter de Gruyter, 1998, 243–254.

[10] I. Gaál, *Power integer bases in algebraic number fields*, Annales Univ. Sci. Budapest., Sectio Comp., **18** (1999) 61–87.

[11] I. Gaál, Diophantine Equations and Power Integral Bases, Birkhäuser, 2002.

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

[13] I. Gaál, I. Járási and F. Luca, *A remark on prime divisors of lengths of sides of Heron triangles*, Experimental Math., **12** (2003), 303–310.

[14] I. Gaál and G. Nyul, *Computing all monogeneous mixed dihedral quartic extensions of a quadratic field*, J. Théorie Nombres Bordeaux, **13** (2001), 137–142.

[15] I. Gaál and G. Nyul, *Index form equations in biquadratic fields: the p-adic case*, Publ. Math. Debrecen, **68** (2006), 225–242.

[16] I. Gaál, A. Pethő and M. Pohst, *On the indices of biquadratic number fields having Galois group V_4*, Arch. Math., **57** (1991), 357–361.

[17] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in biquadratic number fields, I*, J. Number Theory, **38** (1991), 18–34.

[18] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in biquadratic number fields, II*, J. Number Theory, **38** (1991), 35–51.

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

[20] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in dihedral quartic number fields*, Experimental Math., **3** (1994), 245–254.

[21] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in biquadratic number fields, III. The bicyclic biquadratic case*, J. Number Theory, **53** (1995), 100–114.

[22] I. Gaál, A. Pethő and M. Pohst, *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.

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

[24] M.-N. Gras, *Table numérique du nombre de classes et des unites des extensions cycliques réelles de degré 4 de $\mathbb{Q}$*, Publ. Math. Fac. Sci. Besançon, Theor. Nombres, Annee 1977-1978, Fasc. 2.

[25] M.-N. Gras and F. Tanoé, *Corps biquadratiques monogénes*, Manuscripta Math., **86** (1995), 63–79.

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

[27] K. Győry, *On polynomials with integer coefficients and given discriminant V. p-adic generalizations*, Acta Math. Acad. Sci. Hungar., **32** (1978), 175–190.

[28] K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv., **54** (1979), 583–600.

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

[30] K. Győry, *Discriminant form and index form equations*, in: Algebraic Number Theory and Diophantine Analysis (eds. F. Halter-Koch and R. F. Tichy), Walter de Gruyter, 2000, 191–214.

[31] K. Győry, *Index form equations and their applications*, Proc. Inst. Math. NASB Belarus, **13** (2005), 83–93.

[32] J. G. Huard, B. K. Spearman and K. S. Williams, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory, **51** (1995), 87–102.

[33] A. C. Kable, *Power bases in dihedral quartic fields*, J. Number Theory, **76** (1999), 120–129.

[34] L.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly, **96** (1989), 133–137.

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

[36] Y. Kishi, *A family of cyclic cubic polynomials whose roots are systems of fundamental units*, J. Number Theory, **102** (2003), 90–106.

[37] A. J. Lazarus, *On the class number and unit index of simplest quartic fields*, Nagoya Math. J., **121** (1991), 1–13.

[38] G. Lettl and A. Pethő, *Complete solution of a family of quartic Thue equations*, Abh. Math. Sem. Univ. Hamburg, **65** (1995), 365–383.

[39] D. A. Marcus, Number Fields, Springer–Verlag, 1977.

[40] L. J. Mordell, Diophantine Equations, Academic Press, 1969.

[41] Y. Motoda, *On integral bases of certain real monogenic biquadratic fields*, Rep. Fac. Sci. Engrg. Saga Univ. Math., **33** (2004), 9–22.

[42] Y. Motoda and T. Nakahara, *Monogenesis of algebraic number fields whose Galois groups are 2-elementary abelian*, Proc. 2003 Nagoya Conf. „Yokoi-Chowla Conjecture and Related Problems" (eds. S. Katayama, C. Levesque and T. Nakahara), Furukawa Total Pr. Co., 2004, 91–99.

[43] T. Nakahara, *On the indices and integral bases of non–cyclic but abelian biquadratic fields*, Arch. Math., **41** (1983), 504–508.

[44] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Third Edition, Springer–Verlag, 2004.

[45] G. Nyul, *Power integral bases in totally complex biquadratic number fields*, Acta Acad. Paed. Agriensis, Sectio Math., **28** (2001), 79–86.

[46] G. Nyul, *Non-monogenity of multiquadratic number fields*, Acta Math. Inf. Univ. Ostraviensis, **10** (2002), 85–93.

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

[48] B. Schmal, *Diskriminanten, $\mathbb{Z}$-Ganzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern*, Arch. Math., **52** (1989), 245–257.

[49] N. P. Smart, *Solving a quartic discriminant form equation*, Publ. Math. Debrecen, **43** (1993), 29–39.

[50] N. P. Smart, The Algorithmic Resolution of Diophantine Equations, London Math. Soc., Cambridge University Press, 1998.

[51] B. K. Spearman and K. S. Williams, *The index of a cyclic quartic field*, Monatsh. Math., **140** (2003), 19–70.

[52] B. M. M. de Weger, Algorithms for diophantine equations, CWI Tract 65, Amsterdam, 1989.

[53] K. S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull., **13** (1970), 519–526.

[54] K. Yu, *Linear forms in p-adic logarithms*, Acta Arith., **53** (1989), 107–186.

[55] E. von Żyliński, *Zur Theorie der ausserwesentlichen Diskriminantenteiler algebraischer Körper*, Math. Ann., **73** (1913), 273–274.

Publikációk (List of publications)

1. I. Gaál and G. Nyul, *Computing all monogeneous mixed dihedral quartic extensions of a quadratic field*, Journal de Théorie des Nombres de Bordeaux, **13** (2001), 137–142.

2. G. Nyul, *Power integral bases in totally complex biquadratic number fields*, Acta Academie Paedagogicae Agriensis, Sectio Mathematicae, **28** (2001), 79–86.

3. G. Nyul, *Non-monogenity of multiquadratic number fields*, Acta Mathematica et Informatica Universitatis Ostraviensis, **10** (2002), 85–93.

4. G. Nyul, *A divisibility problem of binomial coefficients*, Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös nominatae, Sectio Mathematica, **47** (2004), 115–121.

5. I. Gaál and G. Nyul, *Index form equations in biquadratic fields: the p-adic case*, Publicationes Mathematicae Debrecen, **68** (2006), 225–242.

Előadások (List of talks)

1. *Power integral bases in biquadratic number fields*, The 15th Czech and Slovak International Conference on Number Theory, 2001. szeptember 3.–8., Ostravice (Csehország).

2. *Index forma egyenletek bikvadratikus számtestekben*, Számelméleti tudományos emlékülés Kiss Péter emlékére, 2002. november 22.–23., Eger.

3. *Index form equations in biquadratic and multiquadratic number fields*, Workshop on Computational Number Theory, 2003. október 20.–24., Debrecen.

4. *Binomiális együtthatók oszthatósága*, Soproni Diofantikus Nap, 2004. október 9., Sopron.

5. *Hatvány egész bázisok másodfokú számtestek kompozitumában*, Nyíregyházi Kriptográfiai és Diofantikus Nap, 2005. április 30., Nyíregyháza.

6. *The field index of some families of number fields*, The 17th Czech and Slovak International Conference on Number Theory, 2005. szeptember 5.–10., Malenovice (Csehország).

7. *Algebrai számtestek testindexe*, Berekfürdői Diofantikus és Kriptográfiai Napok, 2006. április 22., Berekfürdő.