

Hatvány egész bázisok
negyedfokú és relatív negyedfokú bővítések
végtelen parametrikus családjaiban

Szabó Tímea
II. matematikus MSC

Témavezető: Gaál István

Debreceni Egyetem
TTK, Matematikai Intézet

2012. december 30.

A publikáció elkészítését a TÁMOP-4.2.2/B-10/1-2010-0024 számú projekt támogatta.

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósult meg.



SZÉCHENYI TERV

1. Bevezetés

A hatvány egész bázisok létezésének kérdése az algebrai számelmélet klasszikus problémaköre. Jól ismert, hogy ha egy számtestnek létezik hatvány egész bázisa, akkor annak ekvivalencia erejéig véges sok generátora létezik. (ld. Győry Kálmán [20])

Gazdag irodalma van speciális számtestekben a hatvány egész bázisok összes generátorának kiszámításának. A hatvány egész bázisok generátorainak meghatározása ekvivalens az *indexforma egyenlet* megoldásának problémájával (ld. [7]).

Hatvány egész bázisok probléma körét relatív bővítésekben is vizsgálták. Gaál István [6] harmadfokú relatív bővítésekben, Gaál István és Michael Pohst [16] negyedfokú relatív bővítésekben adott algoritmust a relatív hatvány egész bázisok generátorainak kiszámítására.

Különösen érdekes problémát jelent, ha hasonló számításokat elvégezzünk adott fokú számtestek végtelen parametrikus családjában, ahol az indexforma egyenlet parametrikus formában adott. Ilyen jellegű számításokat végzett Gaál István [5], Gaál István és M.Pohst [15], Gaál István és G.Letl [9], [10], stb.

Hasonló eredmények, relatív bővítések végtelen parametrikus családjai esetén a relatív hatvány egész bázisok kiszámítására korábban nem születtek.

Dolgozatunkban negyedfokú és másodfokú számtestek feletti relatív negyedfokú bővítések végtelen parametrikus családjai esetén határozzuk meg a (relatív) hatvány egész bázisok összes generátorát.

A megoldás módszere Gaál István, Pethő Attila és M. Pohst [12] tételén, a relatív esetben Gaál István és M. Pohst [16] tételén alapul. A [16]-ban bebizonyított tétel a [12]-ben szereplő állítás általánosítása a relatív esetre, formailag nagyon hasonló, de technikailag jóval bonyolultabb. Mindkét állítás lényege, hogy negyedfokú (relatív negyedfokú) bővítésekben az index forma egyenlet visszavezethető egy harmadfokú és néhány hozzá kapcsolódó negyedfokú Thue egyenletre (relatív Thue egyenletre).

A dolgozat 2.Fejezetében ismertetjük a hatvány egész bázisokkal kapcsolatos algebrai számelméleti tudnivalókat. A negyedfokú bővítések végtelen parametrikus családjaira vonatkozó eredményeinket a 3.Fejezetben részletezzük, ezek megjelentek Gaál István és Szabó Tímea [18] cikkében. A relatív negyedfokú bővítések végtelen parametrikus családjaira vonatkozó eredményeinket a 4.Fejezetben ismertetjük, ezek publikálás alatt állnak Gaál István és Szabó Tímea [19] cikkében.

2. Algebrai számelméleti alapok

2.1. Az abszolút eset

Ebben a fejezetben az érthetőség kedvéért bevezetjük mindazon fogalmakat, melyeket a dolgozatban használni fogunk. A fogalmak és a tételek bizonyítása megtalálható a [7] könyvben.

Legyen α n -edfokú algebrai egész szám, $K = \mathbb{Q}(\alpha)$ algebrai számtest. Jelölje $\mathbb{Z}_K$ a K test egészeinek gyűrűjét.

1. Definíció. A K algebrai számtestnek $\{\omega_1 = 1, \omega_2, \dots, \omega_n\}$ egész bázisa, ha bázis $\mathbb{Q}$ fölött, és minden $\alpha \in \mathbb{Z}_K$ esetén létezik $x_1, \dots, x_n \in \mathbb{Z}$:

$$\alpha = \sum_{i=1}^n x_i \omega_i.$$

2. Definíció. Legyen $\{\omega_1 = 1, \omega_2, \dots, \omega_n\}$ egész bázisa K -nak. Ekkor K diszkriminánsa:

$$D_K = \det \begin{pmatrix} 1 & \omega_2^{(1)} & \dots & \omega_n^{(1)} \\ 1 & \omega_2^{(2)} & \dots & \omega_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_2^{(n)} & \dots & \omega_n^{(n)} \end{pmatrix}^2$$

ahol $\omega_i^{(j)}$ az ω_i (relatív) konjugáltjait jelöli ($1 \leq i, j \leq n$).

3. Definíció. Az $\alpha \in K$ diszkriminánsa

$$D_{K/\mathbb{Q}}(\alpha) = \prod_{1 \leq i < j \leq n} (\alpha^{(i)} - \alpha^{(j)})^2$$

ahol $\alpha^{(i)}$ az α (relatív) konjugáltjait jelöli ($1 \leq i \leq n$).

4. Definíció. Ha $\alpha \in \mathbb{Z}_K$ a K primitív eleme (azaz $K = \mathbb{Q}(\alpha)$), akkor az α indexe alatt a $\mathbb{Z}[\alpha]$ polinomgyűrű additív csoportjának indexét értjük $\mathbb{Z}_K$ additív csoportjában:

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

Megjegyzés: könnyen látható, hogy $a \in \mathbb{Z}$ esetén $I(\alpha) = I(a + \alpha)$, azaz az index $\mathbb{Z}$ -beli elemekkel történő eltolással szemben invariáns. Ha $\alpha \in \mathbb{Z}_K$, akkor a $\beta = \pm\alpha + a$ ($a \in \mathbb{Z}$) elemeket α -val *ekvivalenseknek* nevezzük.

5. Állítás. Minden $\alpha \in \mathbb{Z}_K$ esetén

$$D_{K/\mathbb{Q}}(\alpha) = (I(\alpha))^2 D_K.$$

Általában ezt az összefüggést használjuk az elemek indexének kiszámítására.

6. Definíció. Az $(1, \theta, \dots, \theta^{n-1})$ alakú egész bázisokat *hatvány egész bázisoknak* nevezzük. Ilyen esetben a θ elemet a *hatvány egész bázis generátor elemének* nevezzük.

Nyilvánvaló, hogy θ pontosan akkor generál hatvány egész bázist, ha $I(\theta) = 1$. Mivel ekvivalens elemek indexe azonos, ezért a hatvány egész bázisok generátor elemeit elegendő ekvivalencia erejéig meghatározni.

7. Definíció. A K számtest indexe (*testindexe*) alatt az

$$m_K = \text{lko}\{I(\alpha) \mid \alpha \in \mathbb{Z}_K, K = \mathbb{Q}(\alpha)\}$$

számot értjük.

Legyen $\{\omega_1 = 1, \omega_2, \dots, \omega_n\}$ egész bázisa K -nak, legyen

$$\ell^{(i)}(\underline{X}) = X_1 + X_2\omega_2^{(i)} + \dots + X_n\omega_n^{(i)}$$

($i = 1, 2, \dots, n$). Akkor

$$D_{K/\mathbb{Q}}(X_2, \dots, X_n) = \prod_{1 \leq i < j \leq n} (\ell^{(i)}(\underline{X}) - \ell^{(j)}(\underline{X}))^2$$

egy $n(n-1)$ fokú, egész együtthatós homogén polinom, mely

$$D_{K/\mathbb{Q}}(X_2, \dots, X_n) = (I(X_2, \dots, X_n))^2 \cdot D_K$$

alakba írható, ahol $I(X_2, \dots, X_n)$ egy $n(n-1)/2$ fokú, ugyancsak egész együtthatós homogén polinom.

8. Definíció. Az $I(X_2, \dots, X_n)$ polinomot az $\{\omega_1 = 1, \omega_2, \dots, \omega_n\}$ egész bázishoz tartozó indexformának nevezzük.

9. Állítás. Tetszőleges $\alpha = x_1 + \omega_2 x_2 + \dots + \omega_n x_n$ esetén

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

Megjegyzés: Az indexforma független az X_1 változótól, ami összhangban van azzal, hogy az elemek indexe $\mathbb{Z}$ -beli elemekkel történő eltolásra nézve invariáns.

A fenti tétel értelmében a $\mathbb{Z}_K$ gyűrű m indexű elemeit az

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

diofantikus egyenlet megoldásaiként kapjuk meg. Speciálisan $m = 1$ -re a hatvány egész bázisok generátorait kapjuk meg.

Győry Kálmán [20] tétele szerint:

10. Tétel. Az (1) egyenletnek csak véges sok megoldása van.

Ebből következően ekvivalencia erejéig csak véges sok hatvány egész bázis létezhet.

2.2. Hatvány egész bázisok kiszámítása

Az első példát olyan számtestre, melyben nem létezik hatvány egész bázis, Dedekind [4] adta 1878-ban. Az 1960-as években Hasse [21] vetette fel a hatvány egész bázissal rendelkező számtestek aritmetikai jellemzésének kérdését.

A Baker módszer [2] megjelenése után Győry Kálmán [20] effektív felső korlátot adott indexforma egyenletek megoldására. Ebből tetszőleges számtest esetén következett a hatvány egész bázisok számának végeessége, de a korlátok nagyságrendjük miatt a legegyszerűbb esetekben sem tették lehetővé az egyenletek megoldásainak tényleges kiszámítását és a hatvány egész bázisok meghatározását.

A redukciós módszer (ld. [1]) és annak továbbfejlesztése a következő évtizedekben lehetővé tette alacsony fokszámú testekben az indexforma egyenletek megoldását és a hatvány egész bázisok meghatározását.

Harmadfokú számtestek esetén az indexforma egyenlet egy harmadfokú Thue egyenlet, melyet megoldva Gaál István és N.Schulte [17] foglalta táblázatba a kis diszkriminánsú harmadfokú számtestek hatvány egész bázisait. Gaál István, Pethő Attila és M.Pohst [14] tetszőleges negyedfokú számtestek indexforma egyenletének megoldására adott hatékony algoritmust, visszavezetve azt harmad- és negyedfokú Thue egyenletekre. Ötödfokú számtestek esetén Gaál István és Győry Kálmán [8], hatodfokú számtestek esetén Y.Bilu, Gaál István és Győry Kálmán [3] adtak algoritmust az indexforma egyenlet megoldására, de ezek az algoritmusok már jelentős számolásiigénnyel rendelkeznek. Magasabb fokú számtestek esetén csak speciális esetekben (pl. résztestek létezése esetén) sikerült algoritmust adni az indexforma egyenlet megoldására, ld. Gaál István [7].

2.3. A relatív eset

Az index és a hatvány egész bázis fogalma a *relatív esetre* is kiterjedt, számtestek relatív bővítéseire. Relatív harmadfokú bővítésekkel foglalkozott I.Gaál és M.Pohst [6] illetve a relatív negyedfokú bővítésekkel I.Gaál és M.Pohst [16] (lásd még [7]).

Dolgozatunk második felében a relatív negyedfokú bővítések végtelen parametrikus családjával foglalkozunk. Legyen M egy számtest és K az M egy testbővítése, n relatív fokkal. Jelölje $\mathbb{Z}_M$ illetve $\mathcal{O} = \mathbb{Z}_K$ az M illetve K egészeinek gyűrűjét. Ha $\alpha \in \mathcal{O}$ egy primitív eleme K -nak M felett (tehát $K = M(\alpha)$), akkor az α *relatív indexe* M -ben

$$I_{K/M}(\alpha) = (\mathcal{O}^+ : \mathbb{Z}_M[\alpha]^+).$$

A relatív index pontosan akkor egyenlő eggyel, ha $1, \alpha, \dots, \alpha^{n-1}$ *relatív hatvány egész bázisa* $\mathcal{O}$ -nak $\mathbb{Z}_M$ -ben.

Harmadfokú relatív bővítések hatvány egész bázisainak kiszámítására Gaál István [6], negyedfokú relatív bővítések hatvány egész bázisainak kiszámítására Gaál István és M. Pohst [16] adtak hatékony algoritmust.

3. Negyedfokú számtestek végtelen parametrikus családja

Használva K.S.Williams [26] által adott egész bázist, meg lehet konstruálni a $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ alakú másodfokú számtestekben az indexforma egyenletet. Ez tette lehetővé, hogy ilyen típusú testek esetén a testindexeket teljesen jellemezni tudjuk [11] és hasonló testek esetében általános módszert adjunk az indexforma egyenlet megoldására [13]. Teljesen komplex esetben Nyul Gábor [25] jellemezte az összes $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ típusú testet, explicit módon megadta a hatvány egész bázisok összes generátorát is. J.G.Huard, B.K.Spearman és K.S.Williams [22] nemrég megadták a $\mathbb{Q}(\sqrt{a+b\sqrt{c}})$ alakú negyedfokú számtestekben az egész bázist explicit alakban. Dolgozatukban J.G.Huard, B.K.Spearman és K.S.Williams [22] megvizsgálták $\mathbb{Q}(\sqrt{a+b\sqrt{c}})$ típusú testek két végtelen parametrikus családját két paraméter bevonásával. A szerzők bebizonyították, hogy ezen családok rendelkeznek hatvány egész bázissal.

Dolgozatunkban *megoldottuk az indexforma egyenletet negyedfokú számtestek ezen két végtelen parametrikus családjában* és megmutattuk, hogy az összes hatvány egész bázis a [22]-ban megadott. Ez az első eset, amikor számtestek *két paraméterétől* függő végtelen családjában sikerül megoldani az indexforma egyenletet.

Legyen $c < 0$ egész és pozitív egész k esetén legyen

$$f_c(k) = 16k^2 + 24k + (9 - 4c), \quad a_k = 4k + 3, \quad b_k = 2 \text{ ha } c \equiv 1 \pmod{4}$$

$$f_c(k) = 4k^2 + 4(c+1)k + (c^2 + c + 1), \quad a_k = 2k + c + 1, \quad b_k = 1 \text{ ha } c \equiv 2, 3 \pmod{4}.$$

A [22] dolgozatból nyilvánvaló, hogy minden c esetén $f_c(k)$ négyzetmentes végtelen sok k -ra. Jelölje S a (c, k) párok halmazát, ahol $c < -3$, $k > |c|$ és $f_c(k)$ négyzetmentes. Nyilvánvaló, hogy S egy végtelen halmaz. Továbbá, az egyes c -k esetén $f_c(k) = a_k^2 - cb_k^2$ nagyobb, mint c , ezért $L_{c,k} = \mathbb{Q}(\sqrt{a_k + b_k\sqrt{c}})$ egy negyedfokú bővítése $\mathbb{Q}$ -nak. $L_{c,k}$ tartalmazza a $\mathbb{Q}(\sqrt{c})$ komplex másodfokú testet, ezért ez egy teljesen komplex negyedfokú test.

Dolgozatunkban a következő két tétel bizonyítását mutatjuk meg, melyek megjelentek a [18] dolgozatban:

11. Tétel. *Legyen $c \equiv 1 \pmod{4}$. Ekkor minden $(c, k) \in S$ esetén ekvivalencia erejéig az egyetlen hatvány egész bázist $L_{c,k}$ -ban*

$$\vartheta = \frac{1}{2} \left(1 + \sqrt{a_k + 2\sqrt{c}} \right)$$

generálja.

12. Tétel. *Legyen $c \equiv 2, 3 \pmod{4}$. Ekkor minden $(c, k) \in S$ esetén ekvivalencia erejéig az egyetlen hatvány egész bázist $L_{c,k}$ -ban*

$$\vartheta = \sqrt{a_k + \sqrt{c}}$$

generálja.

J.G.Huard, B.K.Spearman és K.S.Williams [22] azt mutatták meg, hogy a fenti elemek hatvány egész bázist generálnak. Mi teljesen megoldottuk az indexforma-egyenletet és bizonyítottuk, hogy ekvivalencia erejéig nincs a hatvány egész bázisnak másik generátora.

3.1. Segédtelemek

Gaál István, Pethő Attila és M. Pohst [12]-ben megmutatták, hogy az indexforma-egyenlet negyedfokú testekben (három változóval és 6 fokszámmal) harmadfokú Thue egyenletté alakítható. Megmutattuk ezt az eredményt $\mathbb{Z}[\xi]$ rendjére mivel a mi alkalmazásunkban ez éppen a számtest egészeinek gyűrűje.

Legyen $K = \mathbb{Q}(\xi)$ egy negyedfokú számtest és $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 \in \mathbb{Z}[x]$ a ξ minimálpolinomja.

1. Lemma (Gaál I., Pethő A. és M.Pohst [12]). *Az $\alpha = a + x\xi + y\xi^2 + z\xi^3 \in \mathbb{Z}[\xi]$ (ahol $a, x, y, z \in \mathbb{Z}$) akkor és csak akkor generál hatvány egész bázist $\mathbb{Z}[\xi]$ -ben, ha van egy $(u, v) \in \mathbb{Z}^2$ megoldása az*

$$F(u, v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3 = \pm 1 \quad (2)$$

harmadfokú egyenletnek, oly módon, hogy (x, y, z) kielégíti az alábbiakat:

$$\begin{aligned} Q_1(x, y, z) &= x^2 - xy a_1 + y^2 a_2 + xz(a_1^2 - 2a_2) + yz(a_3 - a_1 a_2) \\ &\quad + z^2(-a_1 a_3 + a_2^2 + a_4) = u \quad , \\ Q_2(x, y, z) &= y^2 - xz - a_1 yz + z^2 a_2 = v \quad . \end{aligned} \quad (3)$$

Gaál István, Pethő Attila és M. Pohst [14] cikkében ki van dolgozva egy általános módszer (3) típusú kvadratikus forma egyenletrendszer megoldására. Ezen egyenletrendszerek negyedfokú Thue egyenletek megoldására vezethetők vissza. Teljesen komplex negyedfokú számtestek esetén a (3) rendszerből egy pozitív definit kvadratikus forma konstruálható (cf. [12]).

2. Lemma (Gaál I., Pethő A. és M.Pohst [14]). *Legyen K teljesen komplex negyedfokú test. Ekkor az $R(x) = F(x, 1)$ polinomnak van három különböző valós gyöke, $\lambda_1 < \lambda_2 < \lambda_3$. A $T_\lambda(x, y, z) = Q_1(x, y, z) + \lambda \cdot Q_2(x, y, z)$ forma akkor és csak akkor pozitív definit, ha $\lambda \in (-\lambda_2, -\lambda_1)$.*

3.2. Bizonyítás

3.2.1. 1.Tétel bizonyítása

I. Tudjuk, hogy ha $c \equiv 1 \pmod{4}$, akkor $a_k = 4k + 3, b_k = 2$ és írjuk fel c -t a következőképpen: $c = 4\ell + 1 < -3$ ($\ell < -1$). A ϑ definiáló polinomja ekkor

$$f(x) = x^4 - 2x^3 - 2kx^2 + (2k + 1)x + k^2 + k - \ell.$$

Innen az 1.Lemma jelöléseit használva kapjuk, hogy $a_1 = -2, a_2 = -2k, a_3 = 2k + 1, a_4 = k^2 + k - \ell$. Ekkor a (2) egyenlet az alábbi alakú:

$$F(u, v) = (u + (2k + 1)v)(u^2 - uv - v^2(4k^2 + 6k + 1 - 4\ell)) = \pm 1,$$

ahonnan a következő egyenletrendszert kapjuk:

$$\begin{aligned} u + (2k + 1)v &= i_1 \\ u^2 - uv - v^2(4k^2 + 6k + 1 - 4\ell) &= i_2, \end{aligned}$$

ahol $i_1, i_2 = \pm 1$. Fejezzük ki u -t az első egyenletből és helyettesítsük be a második egyenletbe. Ekkor v -re egy másodfokú egyenletet kapunk.

Ha $i_1 = i_2 = 1$, akkor kapjuk, hogy

$$v = \frac{a_k \pm \sqrt{a_k^2 - 8c}}{2c}.$$

Ebben a képletben $a_k^2 < a_k^2 - 8c < (a_k + 1)^2$, $k > |\ell|$ miatt, emiatt v -re nem kapunk egész értéket.

Ha $i_1 = 1, i_2 = -1$, akkor lehetséges megoldásként kapjuk $v = 0$ -t és $v = a_k/c$ -t, amennyiben ez utóbbi egész. Ekkor az egyenletrendszer lehetséges megoldaspárjai: $(u, v) = (\pm 1, 0), (-(2k + 1)a_k/c + 1, a_k/c)$.

Ha $i_1 = -1, i_2 = 1$, akkor a gyök alatt nem áll négyzetszám, hasonlóan az $i_1 = i_2 = 1$ esethez.

Ha $i_1 = i_2 = -1$, akkor lehetséges megoldásként kapjuk $v = 0$ -t és $v = -a_k/c$ -t, amennyiben ez utóbbi egész. Ekkor az egyenletrendszer lehetséges megoldaspárjai: $(u, v) = (\pm 1, 0), ((2k + 1)a_k/c - 1, -a_k/c)$.

II. Ezután kiszámoljuk az $R(x) = F(x, 1)$ gyökeit. Az adódik, hogy

$$\begin{aligned} x_1 &= \frac{1}{2}(1 - a_k) = -2k - 1 \\ x_2 &= \frac{1}{2}\left(1 + \sqrt{a_k^2 - 4c}\right) = 2k + 2 + \rho_2 \\ x_3 &= \frac{1}{2}\left(1 - \sqrt{a_k^2 - 4c}\right) = -2k - 1 - \rho_3, \end{aligned}$$

ahol ρ_2, ρ_3 pozitív számok, mivel $c < 0$. Következésképpen

$$\lambda_1 = x_3 < \lambda_2 = x_1 < \lambda_3 = x_2.$$

III. $a_1 = -2, a_2 = -2k, a_3 = 2k + 1, a_4 = k^2 + k - \ell$ esetén az 1.Lemmabeli kvadratikus formák:

$$\begin{aligned} Q_1(x, y, z) &= x^2 + 2xy - 2y^2k + xz(4 + 4k) + yz(-2k + 1) + z^2(5k + 2 + 5k^2 - \ell), \\ Q_2(x, y, z) &= y^2 - xz + 2yz - 2z^2k. \end{aligned}$$

A pozitív definit kvadratikus forma megkonstruálásához λ -t a következőképpen kell megválasztanunk: $\lambda \in (-\lambda_2, -\lambda_1) = (-x_1, -x_3) = (2k + 1, 2k + 1 + \rho_3)$. Következésképpen vehetjük $\lambda = 2k + 1 + \varepsilon$, tetszőleges kicsi pozitív ε -nal. Kapjuk, hogy

$$Q_1(x, y, z) + \lambda Q_2(x, y, z) = u + \lambda v,$$

tehát

$$\left(x + y + z\left(\frac{3}{2} + k - \frac{\varepsilon}{2}\right)\right)^2 + \varepsilon\left(y + \frac{3z}{2}\right)^2 + z^2\left(-\ell - \frac{1}{4} - \varepsilon k - \frac{3\varepsilon}{4} - \frac{\varepsilon^2}{4}\right) = u + \lambda v, \quad (4)$$

ahol $u + \lambda v$ vagy 1 vagy $1 + \varepsilon a_k/c$ vagy $-1 - \varepsilon a_k/c$, ez utóbbi pedig lehetetlen kellően kicsi ε -ra.

IV.1. Ha $u + \lambda v = 1$, akkor $\ell < -1$ választással kellően kicsi ε -ra z^2 együtthatója (4)-ben nagyobb, mint 1, amiből kapjuk, hogy $z = 0$ és ekkor (4) az alábbi alakú:

$$(x + y)^2 + \varepsilon y^2 = 1.$$

ε kicsi értéke esetén a bal oldal csak akkor egész, ha $y = 0$, ezért $x = \pm 1$.

IV.2. Ha $u + \lambda v = 1 + \varepsilon a_k/c$, akkor $\ell < -1$ választással kellően kicsi ε -ra kapjuk, hogy $0.9 < 1 + \varepsilon a_k/c < 1$. z^2 együttthatója (4)-ben nagyobb, mint 1, amiből kapjuk, hogy $z = 0$. A (4) egyenlet ekkor az alábbi alakú:

$$(x + y)^2 + \varepsilon y^2 = 1 + \varepsilon a_k/c,$$

tehát

$$(x + y)^2 - 1 = \varepsilon \left(\frac{a_k}{c} - y^2 \right).$$

Most $\varepsilon > 0, a_k/c < 0$ és $-y^2 \leq 0$, ezért a jobb oldali kifejezés negatív. Ez csak úgy lehetséges, ha a bal oldalon $x + y = 0$. Ekkor kapjuk, hogy

$$\varepsilon \left(y^2 - \frac{a_k}{c} \right) = 1,$$

ami lehetetlen, ha például ε irracionális.

Következésképpen csak ϑ generál hatvány egész bázist.

3.2.2. 2.Tétel bizonyítása

I. A 2.Tétel bizonyítása hasonlóan történik, mint az 1.Tétel bizonyítása. Ebben az esetben $a_k = 2k + c + 1, b_k = 1$ és $c \equiv 2, 3 \pmod{4}$. A ϑ elem definiáló polinomja

$$f(x) = x^4 - 2a_k x^2 + a_k^2 - c.$$

Az 1.Lemma jelöléseivel most $a_1 = 0, a_2 = -2a_k, a_3 = 0, a_4 = a_k^2 - c$. A (2) harmadfokú egyenlet az alábbi alakú:

$$F(u, v) = (u + 2a_k v)(u^2 + 4v^2(c - a_k^2)) = \pm 1,$$

ami a következő egyenletrendszert jelenti:

$$\begin{aligned} u + 2a_k v &= i_1 \\ u^2 + 4v^2(c - a_k^2) &= i_2, \end{aligned}$$

ahol $i_1, i_2 = \pm 1$. Kifejezve u -t az első egyenletből és behelyettesítve azt a másodikba, kapunk egy másodfokú egyenletet v -re.

Ha $i_1 = i_2 = 1$, akkor lehetséges megoldásként kapjuk, hogy $v = 0$ vagy $v = a_k/c$. Ha $c \equiv 2 \pmod{4}$, akkor a_k páratlan, ha $c \equiv 3 \pmod{4}$, akkor a_k páros, ezért $v = a_k/c$ nem egész.

Ha $i_1 = -1, i_2 = 1$, akkor lehetséges megoldásként kapjuk, hogy $v = 0$ vagy $v = -a_k/c$, ez utóbbi nem lehetséges, hasonlóan az $i_1 = i_2 = 1$ esethez.

Ha $i_1 = 1, i_2 = -1$ és $i_1 = i_2 = -1$, akkor nincs megoldás a kongruencia-tulajdonságok miatt.

Ezért a lehetséges megoldáspár csak az $(u, v) = (1, 0)$ lehet.

II. Ezután kiszámoljuk az $R(x) = F(x, 1)$ gyökeit. Az adódik, hogy

$$\begin{aligned} x_1 &= -2a_k \\ x_2 &= -2\sqrt{a_k^2 - c} = -2a_k - \rho_2 \\ x_3 &= 2\sqrt{a_k^2 - c} = 2a_k + \rho_3, \end{aligned}$$

ahol ρ_2, ρ_3 pozitív számok, mivel $c < 0$. Következésképpen

$$\lambda_1 = x_2 < \lambda_2 = x_1 < \lambda_3 = x_3.$$

III. $a_1 = 0, a_2 = -2a_k, a_3 = 0, a_4 = a_k^2 - c$ esetén az 1.Lemmabeli kvadratikus formák:

$$\begin{aligned} Q_1(x, y, z) &= x^2 - 2y^2a_k + 4xza_k + z^2(5a_k^2 - c), \\ Q_2(x, y, z) &= y^2 - xz - 2z^2a_k. \end{aligned}$$

A pozitív definit kvadratikus forma megkonstruálásához λ -t a következőképpen kell megválasztanunk: $\lambda \in (-\lambda_2, -\lambda_1) = (-x_1, -x_2) = (2a_k, 2a_k + \rho_2)$. Újra vehetjük $\lambda = 2a_k + \varepsilon$, tetszőleges kicsi pozitív ε -nal. Innen

$$Q_1(x, y, z) + \lambda Q_2(x, y, z) = u + \lambda v,$$

tehát

$$\left(x + z \left(a_k - \frac{\varepsilon}{2}\right)\right)^2 + \varepsilon y^2 + z^2 \left(-c - \varepsilon a_k - \frac{\varepsilon^2}{4}\right) = u + \lambda v, \quad (5)$$

ahol $u + \lambda v = 1$.

IV. Ha $u + \lambda v = 1$, akkor $c < 0$ mellett z^2 együtthatója (5)-ben nagyobb, mint 1, kellően kicsi ε esetén, ahonnan kapjuk, hogy $z = 0$ és (5) maga után vonja, hogy

$$x^2 + \varepsilon y^2 = 1.$$

ε kicsi értéke esetén a bal oldal csak $y = 0$ esetén egész, innen $x = \pm 1$.

Következésképpen ϑ az egyetlen generátora a hatvány egész bázisnak.

4. Relatív negyedfokú bővítések végtelen parametrikus családjai

Ebben a fejezetben ismertetjük eredményeinket relatív negyedfokú bővítések végtelen parametrikus családjainak relatív hatvány egész bázisaira vonatkozóan.

Tekintsük $K = M(\xi)$ alakú nyolcadfokú számtestek két végtelen parametrikus családját az M másodfokú résztestük felett. Célunk, hogy meghatározzuk a relatív hatvány egész bázisát vagy $\mathcal{O} = \mathbb{Z}_K$ -nek $\mathbb{Z}_M$ felett (ha K egész bázisa parametrikus formában ismert) vagy $\mathcal{O} = \mathbb{Z}_M[\xi]$ -nek $\mathbb{Z}_M$ felett. Megjegyezzük, hogy az utóbbi esetben ξ maga egy hatvány egész bázis generátora, de érdekes lenne megtudni, hogy van-e más generátora a hatvány egész bázisnak.

Azokat az $\mathcal{O}$ -beli elemeket, melyek csak egy egységszorzóban vagy egy $\mathbb{Z}_M$ -beli elemmel történő eltolásban különböznek, *ekvivalenseknek* nevezzük. Ekvivalens elemek indexe azonos. A relatív hatvány egész bázisoknak csak véges sok nem ekvivalens generátora létezik.

Megjegyezzük, hogy ez az első eredmény hatvány egész bázisok kiszámítására relatív bővítések végtelen parametrikus családjaiban.

A dolgozat ezen fejezetében szereplő két tétel a [19] cikkben szerepel.

I. Legyen $D > 0$ egy négyzetmentes egész, $M = \mathbb{Q}(\sqrt{-D})$, $t \in \mathbb{Z}_M$ egy paraméter és legyen ξ az

$$f(x) = x^4 - t^2x^2 + 1 \in \mathbb{Z}_M[x] \quad (6)$$

polinom gyöke. Legyen $K = M(\xi)$ és tekintsük az $\mathcal{O} = \mathbb{Z}_M[\xi]$ relatív hatvány egész bázisait $\mathbb{Z}_M$ felett.

13. Tétel. *$|t| > 245$ esetén az $\mathcal{O}$ hatvány egész bázisának összes nem ekvivalens generátorát $\mathbb{Z}_M$ felett megadja az alábbi formula:*

$$\alpha = \xi, -t^2\xi + \xi^3, (1-t^4)\xi + t\xi^2 + t^2\xi^3, (1-t^4)\xi - t\xi^2 + t^2\xi^3, t\xi^2 + \xi^3, -t\xi^2 + \xi^3.$$

Továbbá $D = -3$ esetén

$$\alpha = (1 - \omega_3^2 t)\xi + \omega_3 \xi^2 + \omega_3^2 \xi^3,$$

ahol $\omega_3 = (1 + i\sqrt{3})/2$.

II. Legyen $D > 0$ egy négyzetmentes egész, $M = \mathbb{Q}(\sqrt{-D})$, $t \in \mathbb{Z}_M$ egy paraméter és legyen ξ az

$$f(x) = x^4 - 4tx^3 + (6t + 2)x^2 + 4tx + 1 \in \mathbb{Z}_M[x] \quad (7)$$

polinom gyöke. Legyen $K = M(\xi)$ és tekintsük az $\mathcal{O} = \mathbb{Z}_M[\xi]$ relatív hatvány egész bázisait $\mathbb{Z}_M$ felett.

14. Tétel. $|t| > 1544803$ esetén az $\mathcal{O}$ hatvány egész bázisának összes nem ekvivalens generátorát $\mathbb{Z}_M$ felett megadja az alábbi formula:

$$\alpha = \xi, (6t + 2)\xi - 4t\xi^2 + \xi^3.$$

4.1. Segédtelemek

A fő eszköz, amelyet mindenütt alkalmazni fogunk, Gaál István és Michael Pohst [16] cikkének módszere, amit alább részletezünk. Ez a módszer a relatív indexforma egyenletet visszavezeti relatív harmadfokú egyenletre (irreducibilis esetben Thue egyenlet) és néhányat relatív negyedfokú Thue egyenletté. A mi két családunk esetén a harmadfokú egyenlet reducibilis. A negyedfokú Thue egyenlet megoldásához alkalmaznunk kell az eredményeket relatív Thue egyenletek végtelen parametrikus családjára vonatkozóan.

Legyen K egy negyedfokú bővítése az m -edfokú M számtestnek, melyet ξ generál és ξ relatív minimálpolinomja $f(x) = x^4 + a_1x^3 +$

$a_2x^2 + a_3x + a_4 \in \mathbb{Z}_M[x]$. Legyen $\mathcal{O}$ vagy $\mathbb{Z}_K$ vagy $\mathbb{Z}_M[\xi]$. Egy $\alpha \in \mathcal{O}$ elemet az alábbi alakban felírunk:

$$\alpha = \frac{1}{d} (a + x\xi + y\xi^2 + z\xi^3), \quad (8)$$

ahol $x, y, z \in \mathbb{Z}_M$ ($1 \leq i \leq 4$) és $d \in \mathbb{Z}$ közös nevező. Legyen $i_0 = I_{K/M}(\xi) = (\mathcal{O}^+ : \mathbb{Z}_M[\xi]^+)$,

$$F(u, v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3$$

egy kétváltozós harmadfokú polinom $\mathbb{Z}_M$ felett és

$$\begin{aligned} Q_1(x, y, z) &= x^2 - xy a_1 + y^2 a_2 + xz(a_1^2 - 2a_2) + yz(a_3 - a_1 a_2) + z^2(-a_1 a_3 + a_2^2 + a_4) \\ Q_2(x, y, z) &= y^2 - xz - a_1 yz + z^2 a_2 \end{aligned}$$

háromváltozós kvadratikus forma $\mathbb{Z}_M$ felett.

3. Lemma (Gaál I. és M.Pohst [16]). *Ha α a (8)-beli alakú és kielégíti*

$$I_{K/M}(\alpha) = 1$$

egyenletet, akkor létezik $(u, v) \in \mathbb{Z}_M$ megoldása az

$$N_{M/\mathbb{Q}}(F(u, v)) = \pm \frac{d^{6m}}{i_0} \quad (9)$$

egyenletnek oly módon, hogy

$$\begin{aligned} u &= Q_1(x, y, z), \\ v &= Q_2(x, y, z). \end{aligned} \quad (10)$$

A (9) egy ismert u, v megoldása esetén meg kell oldanunk a (10) egyenletrendszert. Erre a célra használjuk L.J.Mordell [24] módszerét, paraméterezzük a $Q_0(x, y, z) = uQ_2(x, y, z) - vQ_1(x, y, z) = 0$ kvadratikus forma egyenlet megoldásait, amelyet szintén érthetővé tesz [16]. Ezen módszereket részletesen leírjuk a bizonyításunkban. Láthatólag a 3.Lemma formailag szinte teljes analógiában van az 1.Lemmával. A relatív eset azonban számos technikai problémát vet fel a 3. Lemma alkalmazása közben.

4.2. Bizonyítás

4.2.1. 1.Tétel bizonyítása

A lemmánkba behelyettesítjük $a_1 = 0, a_2 = -t^2, a_3 = 0, a_4 = 1$. A (9) egyenlet az alábbi alakú:

$$F(u, v) = (u - 2v)(u + 2v)(u + t^2v) = \varepsilon,$$

ahol $\varepsilon \in M$ egy egysége. Ezért $F(u, v)$ minden tényezőjének szintén egységnek kell lennie M -ben, amelyből következik, hogy $v = 0$ és u egy egység M -ben. A $Q_0 = 0$ egyenletből következik, hogy $Q_2 = 0$, ezért

$$y^2 - xz - z^2t^2 = 0. \quad (11)$$

Ennek egy nem triviális megoldása: $x_0 = -t^2, y_0 = 0, z_0 = 1$. Ezért a (11) megoldása paraméterezhető az alábbi alakban:

$$\begin{aligned} x &= -t^2r + p \\ y &= q \\ z &= r, \end{aligned} \quad (12)$$

ahol $p, q, r \in M, r \neq 0$ (cf. [24], [16]). Ezt a kifejezést behelyettesítve (11)-ba $rp = q^2$ adódik. Megszorozzuk a (12) minden egyenletét p -vel és rp -t helyettesítjük q^2 -tel, így

$$\begin{aligned} kx &= -t^2q^2 + p^2 \\ ky &= pq \\ kz &= q^2, \end{aligned} \quad (13)$$

ahol $k \in M$. $\mathbb{Z}_M$ -ben van egyértelmű faktorizáció, beszorozzuk ezeket az egyenleteket p, q közös osztójának négyzetével és osztom őket p, q legnagyobb közös osztójának négyzetével. Ezzel a k, p, q paramétereket helyettesíteni tudjuk $\mathbb{Z}_M$ -beli paraméterekkel. (Megjegyezzük, hogy ha $\mathbb{Z}_M$ -ben nincs egyértelmű faktorizáció, akkor főként ugyanezt az érvelést használjuk $\mathbb{Z}_M$ ideáljainak bevonásával. A részletes eljárás megtalálható [16]-ben.)

Figyelembe véve a p^2, pq, q^2 együtthatóit a kx, ky, kz reprezentációjában (13)-ben és kiszámolva a megfelelő 3x3-as mátris determinánsát kapjuk, hogy k -nak is egésznek kell lennie (cf. [16]). Végül, a (13)-beli alakot $Q_1(x, y, z) = u$ -ba helyettesítve adódik

$$p^4 - t^2 p^2 q^2 + q^4 = k^2 u.$$

(A második egyenlet $Q_2(x, y, z) = v$ eltűnik mindkét oldalon.)

Használva a V.Ziegler [27]-beli 2.Tételt le tudjuk írni ezen relatív negyedfokú Thue egyenletnek a megoldásait, ezért x, y, z -t is (13)-ben, amely az 1.Tétel bizonyítását adja. Megjegyezzük, hogy V.Ziegler [27]-beli tétele $|t| > 245$ -re érvényes.

4.2.2. 2.Tétel bizonyítása

A lemmánkba behelyettesítjük $a_1 = -4t, a_2 = 6t + 2, a_3 = 4t, a_4 = 1$. A (9) egyenlet az alábbi alakú:

$$F(u, v) = (u + 2v)(u - (2 - 2t)v)(u - (2 + 8t)v) = \varepsilon,$$

ahol ε M egy egysége. Ezért $F(u, v)$ minden tényezőjének szintén egységnek kell lennie M -ben, amelyből következik, hogy $v = 0$ és u egy egység M -ben. Ismét $Q_0 = 0$ -ból következik, hogy $Q_2 = 0$, ezért

$$y^2 - xz + 4tyz + (6t + 2)z^2 = 0. \quad (14)$$

Ennek egy nem triviális megoldása $x_0 = 6t + 2, y_0 = 0, z_0 = 1$. Ezért a (14) megoldása paraméterezhető az alábbi alakban:

$$\begin{aligned} x &= (6t + 2)r + p \\ y &= q \\ z &= r, \end{aligned} \quad (15)$$

ahol $p, q, r \in M, r \neq 0$. Ezt a kifejezést behelyettesítve (14)-be $q^2 = r(p - 4tq)$ adódik. Megszorozzuk a (15) minden egyenletét $p - 4tq$ -val és $r(p - 4tq)$ -t helyettesítjük q^2 -tel, így

$$\begin{aligned} kx &= p^2 - 4tpq + (6t + 2)q^2 \\ ky &= pq - 4tq^2 \\ kz &= q^2, \end{aligned} \quad (16)$$

ahol $k \in M$. Hasonlóképpen, mint az 1.Tétel bizonyításában, a k, p, q paramétereket helyettesítjük $\mathbb{Z}_M$ -beli paraméterekkel. Ismét kapjuk, hogy k -nak egésznek kell lennie. Végül, a (16)-beli alakot $Q_1(x, y, z) = u$ -ba helyettesítve adódik

$$p^4 - 4tp^3q + (6t + 2)p^2q^2 + 4tpq^3 + q^4 = k^2u.$$

(A második egyenlet $Q_2(x, y, z) = v$ ismét eltűnik mindkét oldalon.)

Használva a B.Jadrijevič és V.Ziegler [23]-beli 2.Tételt le tudjuk írni ezen relatív negyedfokú Thue egyenletnek a megoldásait, ezért x, y, z -t is (16)-ben, amely a 2.Tétel bizonyítását adja. Megjegyezzük, hogy B.Jadrijevič és V.Ziegler [23]-beli eredménye $|t| > 1544803$ -ra érvényes.

Hivatkozások

- [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, *Transcendental Number Theory*, Cambridge, 1990.
- [3] Y.Bilu, I.Gaál and K.Győry, *Index form equations in sextic fields: a hard computation*, Acta Arithm., **115.1** (2004), 85–96.
- [4] R.Dedekind, *Über Zusammenhang zwischen der Theorie der Ideale und der Theorie der Höheren Kongruenzen*, Abh. König. Ges. der Wissen. zu Göttingen, **23**(1878), 1–23.
- [5] I.Gaál, *Power integral bases in orders of families of quartic fields*, Publ. Math. (Debrecen), **42** (1993), 253–263.
- [6] I.Gaál, *Power integral bases in cubic relative extensions*, Experimental Math., **10**(2001), 133–139.
- [7] I.Gaál, *Diophantine Equations and Power Integral Bases*, New Computational Methods, Birkhäuser Boston, 2002.
- [8] I.Gaál and K.Győry, *Index form equations in quintic fields*, Acta Arith., **89**(1999), 379–396.
- [9] I.Gaál and G.Lettl, *A parametric family of quintic Thue equations*, Math. Comput., **69**(1999), 851–859.
- [10] I.Gaál and G.Lettl, *A parametric family of quintic Thue equations II.*, Monatsh. Math., **131**(2000), 29–35.
- [11] I.Gaál, A.Pethő and M.Pohst, *On the indices of biquadratic number fields having Galois group V_4* , Archiv der Math., **57** (1991), 357–361.
- [12] I.Gaál, A.Pethő and M.Pohst, *On the resolution of index form equations in quartic number fields*, J. Symbolic Comput., **16** (1993), 563–584.

- [13] 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.
- [14] 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.
- [15] I.Gaál and M.Pohst, *Power integral bases in a parametric family of totally real quintics*, Math. Comput., **66**(1997), 1689–1696.
- [16] I.Gaál and M.Pohst, *On the resolution of index form equations in relative quartic extensions*, J.Number Theory, **85**(2000), 201–219.
- [17] I.Gaál and N.Schulte, *Computing all power integral bases of cubic number fields*, Math. Comput., **53**(1989), 689–696.
- [18] I.Gaál and T.Szabó, *Power integral bases in parametric families of biquadratic fields*, JP Journal of Algebra, Number Theory and Applications, **21**(2012), 105 - 114.
- [19] I.Gaál and T.Szabó, *Relative power integral bases in infinite families of quartic extensions of quadratic fields*, JP Journal of Algebra, Number Theory and Applications, manuscript.
- [20] K.Győry, *Sur les polynomes a coefficients entiers et de discriminant donne, III*, Publ. Math. (Debrecen), **23**(1976), 141–165.
- [21] H.Hasse, *Zahlentheorie*, Akademie-Verlag, Berlin, 1963.
- [22] 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.
- [23] B.Jadrijevič, V.Ziegler, *A system of relative Pellian equations and a related family of relative Thue equations*, Int. J. Number Theory **2**(2006), No. 4, 569-590.
- [24] L.J.Mordell, *Diophantine equations*, Pure and Applied Mathematics, 30. London-New York: Academic Press, 1969.

- [25] G.Nyul, *Power integral bases in mixed biquadratic number fields*, Acta Acad. Paed. Agriensis, Sect. Math. **28**(2001) 7986
- [26] K.S.Williams, *Integers of biquadratic fields*, Canad. Math. Bull., **13**(1970), 519-526.
- [27] V.Ziegler, *On a family of relative quartic Thue inequalities*, J. Number Theory **120**(2006), No. 2, 303-325.