Egyetemi doktori (PhD) értekezés tézisei

Algebrai számtestek monogenitása az abszolút és a relatív esetben

Szabó Tímea
Témavezető: Dr. Gaál István

Debreceni Egyetem
Természettudományi Doktori Tanács
Matematika- és Számítástudományok Doktori Iskola
Debrecen, 2017

1. Bevezetés

A **hatvány egész bázisok** létezésének és kiszámításának kérdése az algebrai számelmélet klasszikus problémaköre.

A kérdés megoldottnak tekinthető alacsonyabb fokú számtestekben, harmad- és negyedfokú testek esetén hatékony eljárások, ötöd- és hatodfokú testek esetén komplikáltabb, de még használható általános algoritmusok léteznek a hatvány egész bázisok generátorainak kiszámítására.

Hatvány egész bázisok problémakörét *relatív bővítés*ekben is vizsgálták. Ezen felül érdekes problémát jelent, ha hasonló számításokat végzünk adott fokú *számtestek végtelen parametrikus családjá*ban, ahol az indexforma egyenlet parametrikus formában adott.

Értekezésem 1. Fejezetében a szükséges algebrai számelméleti alapfogalmakat tárgyaljuk a könnyebb érthetőség kedvéért. Legyen α n-edfokú algebrai egész szám, $K = \mathbb{Q}(\alpha)$ algebrai számtest.

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

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

Ha $\alpha \in \mathbb{Z}_K$, akkor a $\beta = \pm\alpha + a$ $(a \in \mathbb{Z})$ elemeket α-val *ekvivalens*eknek nevezzük.

Minden $\alpha \in \mathbb{Z}_K$ esetén

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

ahol D_K a K test diszkriminánsa, $D_{K/\mathbb{Q}}(\alpha)$ pedig az α diszkriminánsa.

Az $\{1, \alpha, \ldots, \alpha^{n-1}\}$ alakú egész bázisokat *hatvány egész bázis*oknak nevezzük. Ilyen esetben a α elemet a hatvány egész bázis generátor elemének nevezzük.

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

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

$(i = 1, 2, \ldots, n)$, ahol az $\omega_j^{(i)}$ az ω_j konjugáltja. Akkor

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

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

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

alakba írható, ahol $I(X_2, \ldots, X_n)$ egy $n(n-1)/2$ fokú, ugyancsak egész együtthatós homogén polinom. Az $I(X_2, \ldots, X_n)$ formát az $\{\omega_1 = 1, \omega_2, \ldots, \omega_n\}$ egész bázishoz tartozó *indexformá*nak nevezzük.

A K számtest *minimális index*e alatt az

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

számot értjük.

Az index és a hatvány egész bázis fogalma a *relatív eset*re is kiterjeszthető, számtestek relatív bővítéseire. Legyen M egy m-edfokú számtest és K az M véges bővítése, n relatív fokkal. Ekkor $[K : \mathbb{Q}] = n \cdot m$. Legyen $\mathbb{Z}_M$ az M egészeinek gyűrűje és legyen $\mathcal{O}$ rend $\mathbb{Z}_K$-ban, mely lehet egyenlő is $\mathbb{Z}_K$-val.

Azt mondjuk, hogy $\mathcal{O}$-nak $\{\omega_1 = 1, \omega_2, \ldots, \omega_n\}$ *relatív egész bázis*a M fölött, ha minden $\alpha \in \mathcal{O}$ esetén egyértelműen léteznek $x_1, \ldots, x_n \in \mathbb{Z}_M$, hogy

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

(Ha $\mathcal{O} = \mathbb{Z}_K$, akkor $\mathbb{Z}_K$ relatív egész bázisát M fölött K relatív egész bázisának is nevezzük M fölött.)

Az $\{1, \alpha, \ldots, \alpha^{n-1}\}$ $(\alpha \in \mathcal{O})$ alakú relatív egész bázisokat *relatív hatvány egész bázis*oknak nevezzük.

A továbbiakban feltételezzük, hogy $\mathcal{O}$-nak van relatív egész bázisa M felett.

Ha $\alpha \in \mathcal{O}$ egy primitív eleme K-nak M felett (tehát $K = M(\alpha)$), akkor az α *relatív index*e M-ben

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

A relatív index pontosan akkor egyenlő 1-gyel, ha $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *relatív hatvány egész bázis*a $\mathcal{O}$-nak $\mathbb{Z}_M$ felett.

A dolgozat egyik fejezetében foglalkozunk relatív bővítésekkel, és a relatív hatvány egész bázisok ismeretében szeretnénk meghatározni az (abszolút) hatvány egész bázis generátorokat. Ismeretes, hogy

$$I_{\mathcal{O}}(\alpha) = (\mathcal{O}^+ : \mathbb{Z}[\alpha]^+) = \\ = (\mathcal{O}^+ : \mathbb{Z}_M[\alpha]^+) \cdot (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+), \qquad (1)$$

ahol a megfelelő gyűrűk additív csoportjainak indexét ismerjük. Az első faktor az α relatív indexe:

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

Azt mondhatjuk, hogy egy $\alpha \in \mathcal{O}$ elem pontosan akkor generál hatvány egész bázist $\mathcal{O}$-ban, ha

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

és

$$J(\alpha) = (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+) = 1$$

teljesülnek. Következésképpen ha α hatvány egész bázist generál $\mathcal{O}$-ban, akkor relatív hatvány egész bázist generál $\mathcal{O}$-ban M felett.

A relatív hatvány egész bázisokat ekvivalencia erejéig határozzuk meg, azaz M-beli egységgel történő szorzástól és $\mathbb{Z}_M$-beli elemmel történő eltolástól eltekintve. Tehát ha α (abszolút) hatvány egész bázist generál $\mathcal{O}$-ben, akkor

$$\alpha = A + \varepsilon \cdot \alpha_0, \qquad (2)$$

ahol α_0 relatív hatvány egész bázist generál $\mathcal{O}$-ban M felett, ε egy M-beli egység és $A \in \mathbb{Z}_M$.

A dolgozat eredményei a 2. és 3. Fejezetben találhatóak.

A 2. Fejezetben vizsgáltuk harmadfokú gyökbővítésekben a hatvány egész bázisok létezését és a minimális indexek relatív gyakoriságát. Ezt követően relatív harmadfokú testek esetén határozzuk meg a hatvány egész bázis generátorokat.

A 3. Fejezet tárgyalja negyedfokú és relatív negyedfokú bővítések végtelen parametrikus családjaiban az abszolút és a relatív hatvány egész bázisok létezését.

2. Harmadfokú és relatív harmadfokú testek

2.1. A minimális index viselkedése harmadfokú gyökbővítésekben

A dolgozat ezen fejezetének célja a hatvány egész bázisok és a minimális indexű elemek vizsgálata a $K = \mathbb{Q}(\sqrt[3]{n})$ alakú számtestekben ($1 < n \in \mathbb{Z}$ köbmentes), azaz a harmadfokú gyökbővítésekben. Ezen számtestek egy végtelen parametrikus családnak tekinthetőek (n a paraméter), melyek viselkedését mindeddig

külön nem tanulmányozták. Számításaink azt mutatják, hogy *ezen testek diszkriminánsának növekedésével tendenciózusan csökken a hatvány egész bázisok létezésének relatív gyakorisága, és tendenciózusan növekszik a minimális index.*

Eredményeink eléréséhez több mint 2000 indexforma egyenlet megoldása volt szükséges. Esetünkben ezek harmadfokú Thue egyenletek, melyek megoldásához a KASH [6] programcsomagot használtuk fel.

A következő számítások elvégzése volt szükséges:

A. Kiszámoljuk a hatvány egész bázisok generátorait a $|D_K| < 12 \cdot 10^6$ diszkriminánsú harmadfokú gyökbővítésekben.

B. Kiszámítjuk a minimális indexű elemeket a $|D_K| < 3 \cdot 10^6$ diszkriminánsú harmadfokú gyökbővítésekben.

A számítások elvégzése után jellemezzük a hatvány egész bázisok relatív gyakoriságát és a minimális indexű elemek átlagos viselkedését.

A következő táblázatban az $[1, 12 \cdot 10^6]$ intervallumot 10 azonosan hosszúságú részre osztjuk fel. Minden részintervallum esetén elosztottuk azon testek számát, melyekben létezik hatvány egész bázis és $|D_K|$ az intervallumba esik, azon összes testek számával, melyekre $|D_K|$ az intervallumba esik.

D_K			testek száma	relatív gyakoriság
0	$\leq \lvert D_K \rvert <$	$12 \cdot 10^5$	375	0.37
$12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$2 \cdot 12 \cdot 10^5$	178	0.27
$2 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$3 \cdot 12 \cdot 10^5$	137	0.27
$3 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$4 \cdot 12 \cdot 10^5$	122	0.27
$4 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$5 \cdot 12 \cdot 10^5$	116	0.25
$5 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$6 \cdot 12 \cdot 10^5$	97	0.26
$6 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$7 \cdot 12 \cdot 10^5$	86	0.24
$7 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$8 \cdot 12 \cdot 10^5$	80	0.26
$8 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$9 \cdot 12 \cdot 10^5$	80	0.20
$9 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$12 \cdot 10^6$	81	0.21

Mint látható, *a hatvány egész bázissal rendelkező testek relatív gyakorisága csökkenő tendenciát mutat.*

A következő táblázatban az $[1,\, 3 \cdot 10^6]$ intervallumot diszkrimináns szerint 10 egyforma hosszúságú részre osztjuk fel úgy, ahogy korábban már megtettük. Minden részintervallum esetén tekintjük azon testek minimális indexeinek átlagát, melyek esetén $|D_K|$ a részintervallumba esik.

D_K			testek száma	min index átlag
0	$\leq \lvert D_K \rvert <$	$3 \cdot 10^5$	175	2.29
$3 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$2 \cdot 3 \cdot 10^5$	80	2.68
$2 \cdot 3 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$3 \cdot 3 \cdot 10^5$	60	2.90
$3 \cdot 3 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$4 \cdot 3 \cdot 10^5$	60	3.10
$4 \cdot 3 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$5 \cdot 3 \cdot 10^5$	54	3.61
$5 \cdot 3 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$6 \cdot 3 \cdot 10^5$	50	3.22
$6 \cdot 3 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$7 \cdot 3 \cdot 10^5$	37	4.76
$7 \cdot 3 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$8 \cdot 3 \cdot 10^5$	37	2.86
$8 \cdot 3 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$9 \cdot 3 \cdot 10^5$	33	3.55
$9 \cdot 3 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$3 \cdot 10^6$	43	4.12

Látható, hogy $|D_K|$ *növekedésével a minimális indexek átlaga is növekszik*, bár ez a növekedés nem

teljesen monoton, ahogy az várható volna (ez durvább felosztás esetén következik csak be).

2.2. Hatodfokú számtestek másodfokú résztesttel

Másodfokú résztesttel rendelkező hatodfokú testek hatvány egész bázisainak kiszámítása harmadfokú relatív Thue egyenletek megoldására vezet (lásd [23]).

Rokon problémák megoldásában, amikor bonyolult, vagy nagy számú Thue egyenletet kellett megoldani, hatékonyan alkalmaztuk Pethő Attila [42] módszerét Thue egyenletek "kis" megoldásainak kiszámítására. Ez azt jelenti, hogy egy gyors algoritmus segítségével kiszámítjuk pl a $C = 10^{500}$- nál kisebb abszolút értékű megoldásokat. Mivel tapasztalataink szerint Thue egyenletek megoldásai általában kicsi számok, az eljárás nagy valószínűséggel az összes megoldást szolgáltatja, másrészt gyorsasága miatt lehetővé teszi nagyszámú egyenlet megoldást.

A közelmúltban Gaál István [14] hasonló gyors algoritmust adott relatív Thue egyenletek "kis" megoldásainak kiszámítására. Amíg Pethő Attila módszere a lánctört algoritmusra épül, addig Gaál István módszere az LLL algoritmust használja fel [37].

Célunk (lásd [26]) a korábbiaknál sokkal több szám-

testre kiterjeszteni a számításokat, meghatározni azon hatvány egész bázisok generátorait, melyek egész bázisra vonatkozó koordinátái "kicsik", jellemzően $C = 10^{250}$-nél kisebbek, felhasználva a relatív Thue egyenletek "kis" megoldásainak keresésére rendelkezésre álló módszert. Számításaink kiterjednek a [23]-ban szereplőknél jóval több képzetes másodfokú résztesttel rendelkező hatodfokú számtestre, valamint valós másodfokú résztesttel rendelkező hatodfokú számtestekre is, melyek a korábbi számításokban még egyáltalán nem szerepeltek.

Legyen M másodfokú számtest, melynek egész bázisa $\{1, \omega\}$. Legyen $f(X) = X^3 + \gamma_2 X^2 + \gamma_1 X + \gamma_0 \in \mathbb{Z}_M[X]$ a hatodfokú ϑ minimálpolinomja M felett és legyen $K = \mathbb{Q}(\vartheta)$. M.Olivier [41] táblázatában lévő ϑ-k 99%-os valószínűséggel olyanok, hogy relatív indexük M felett 1, amiből következik, hogy $\{1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2\}$ K egy egész bázisát alkotja. Tehát K minden α egész eleme felírható

$$\alpha = x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2 \qquad (3)$$

alakban, ahol $x_i, y_i \in \mathbb{Z}$ $(i = 0, 1, 2)$.

Legyen $C = 10^{250}$. Célunk a K hatodfokú test azon (3) alakú α elemeinek a meghatározása, melyek hatvány egész bázist generálnak és melyekre fennáll

$$max(|x_1|, |x_2|, |y_0|, |y_1|, |y_2|) < C. \qquad (4)$$

Jelölje $\vartheta = \vartheta^{(1)}, \vartheta^{(2)}, \vartheta^{(3)}$ a ϑ M feletti relatív

konjugáltjait. Legyen $\varrho = -\vartheta^{(1)} - \vartheta^{(2)}$. A (3) formában felírt α pontosan akkor generálja K egy hatvány egész bázisát, ha $X = x_1 + \omega y_1,\ Y = x_2 + \omega y_2$ kielégíti az alábbi Thue egyenletet

$$N_{K/M}(X - \varrho Y) = \nu, \quad X, Y \in \mathbb{Z}_M \tag{5}$$

(ahol ν az M egy egysége) és x_1, x_2, y_0, y_1, y_2 egy megoldása az alábbi 9-edfokú polinomegyenletnek:

$$F(x_1, x_2, y_0, y_1, y_2) = \pm 1, \quad x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}. \tag{6}$$

Ezen F konstrukcióját lásd [26]-ban.

Legyen először is K olyan hatodfokú számtest, mely *képzetes másodfokú résztest*tel rendelkezik. Ha meg akarjuk határozni K összes hatvány egész bázisának generátorait (3) alakban, először is meg kell határoznunk az (5) egyenlet azon megoldásait, melyek kielégítik (4)-et. Abban az esetben, ha M képzetes másodfokú résztest, ν csak véges sokféle lehet. Ezt követően pedig ki kell számítanunk y_0-t (6)-ból ($x_0 \in \mathbb{Z}$ tetszőleges).

Mivel a módszer körülbelül példánként 2-5 perc alatt meghatározza a megoldásokat, ezért ez lehetővé teszi, hogy kilistázzuk a 100 legkisebb abszolút értékű számtestben az adott tulajdonságú hatvány egész bázisok generátorait.

Számításaink eredményei megtalálhatóak disszertáció Függelékének 4.2. Fejezetében.

Most pedig legyen K *valós másodfokú résztest*tel rendelkező hatodfokú számtest.

A feladat nehézsége ezen számtestek esetén az, hogy míg képzetes másodfokú résztest esetén az M-ben véges sok egység van, addig valós másodfokú résztest esetén végtelen sok van. Emiatt a feladat az alábbi alakot ölti ebben az esetben:

$$N_{K/M}(X - \varrho Y) = \pm\varepsilon^k, \quad X, Y \in \mathbb{Z}_M \tag{7}$$

ahol ε az M valós másodfokú résztest alapegysége, $k \in \mathbb{Z}$. Legyen $k = 3m + r$, ahol $m, r \in \mathbb{Z}$, $r \in \{-1, 0, 1\}$. A (4) korlátból a (7) egyenlet felhasználásával korlátot vezethetünk le $|k|$-ra, majd $|m|$-re. Legyen $X_0 = \varepsilon^{-m}X$, $Y_0 = \varepsilon^{-m}Y$, akkor X_0, Y_0 egész bázisbeli koordinátái is korlátosok. Az egyenlet mindkét oldalát leosztva ε^{3m}-nel, $X_0 = \varepsilon^{-m}X$, $Y_0 = \varepsilon^{-m}Y$ helyettesítéssel a feladat az alábbi alakot ölti: meg kell határoznunk az

$$N_{K/M}(X_0 - \varrho Y_0) = \pm\varepsilon^r, \quad X_0, Y_0 \in \mathbb{Z}_M$$

azon megoldásait, melyek az X_0, Y_0 komponenseire kapott korlát alatt vannak. Ezen egyenlet X_0, Y_0 megoldásai ismeretében minden szóba jöhető m-re az

$$\begin{aligned} x_1 + \omega y_1 = X = \varepsilon^{-m}X_0, \\ x_2 + \omega y_2 = Y = \varepsilon^{-m}Y_0 \end{aligned}$$

alapján kiszámítjuk x_1, x_2, y_1, y_2-t, majd (6)-ból y_0-t.

Számításaink eredményeit lásd a Függelék 4.3. Fejezetében.

3. Negyedfokú és relatív negyedfokú testek

A dolgozat ezen fejezetében negyedfokú számtestekben és másodfokú számtestek feletti relatív negyedfokú bővítésekben határozzuk meg a hatvány egész bázisok illetve relatív hatvány egész bázisok generátor elemeit. Tételeink nem egyszerű számtestekre, hanem negyedfokú és relatív negyedfokú számtestek végtelen parametrikus családjaira vonatkoznak.

3.1. Hatvány egész bázisok negyedfokú bikvadratikus testek végtelen parametrikus családjaiban

J.G.Huard, B.K.Spearman és K.S.Williams [35] nemrég megadták a $\mathbb{Q}(\sqrt{a+b\sqrt{c}})$ alakú bikvadratikus negyedfokú számtestekben az egész bázist explicit alakban. Dolgozatukban J.G.Huard, B.K.Spearman és K.S.Williams [35] 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.

Ebben a fejezetben megoldottuk az indexforma egyenletet negyedfokú számtestek ezen két végtelen parametrikus családjában és megmutattuk, hogy az

összes hatvány egész bázis a [35]-ban megadott. Ez az első olyan eredmény, amikor számtestek *két paraméter*étől függő végtelen családjában sikerül megoldani az indexforma egyenletet.

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

$$f_c(k) = 16k^2 + 24k + (9 - 4c),$$

$$g_k = 4k + 3,\ h_k = 2 \text{ ha } c \equiv 1 \pmod 4$$

$$f_c(k) = 4k^2 + 4(c+1)k + (c^2 + c + 1),$$

$$g_k = 2k + c + 1,\ h_k = 1 \text{ ha } c \equiv 2, 3 \pmod 4.$$

A [35] dolgozatból tudjuk, hogy minden c esetén $f_c(k)$ négyzetmentes végtelen sok k-ra. Jelölje S azon (c, k) párok halmazát, ahol $c < -3$, $k > |c|$ és $f_c(k)$ négyzetmentes. Ekkor S egy végtelen halmaz. Továbbá, az egyes c-k esetén $f_c(k) = g_k^2 - ch_k^2$ nagyobb, mint c, ezért $L_{c,k} = \mathbb{Q}(\sqrt{g_k + h_k\sqrt{c}})$ 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.

A következő állításokat bizonyítjuk be:

1. Tétel (Gaál I., Szabó T. [30]). *Legyen* $c \equiv 1 \pmod 4$. *Ekkor minden* $(c, k) \in S$ *esetén ekvivalencia erejéig az egyetlen hatvány egész bázist* $L_{c,k}$*-ban*

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

generálja.

2. Tétel (Gaál I., Szabó T. [30]). *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*

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

generálja.

J.G.Huard, B.K.Spearman és K.S.Williams [35] 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.

A bizonyításhoz alkalmazzuk Gaál István, Pethő Attila és M. Pohst [20] eredményét a $\mathbb{Z}[\xi]$ rendre, mivel alkalmazásunkban éppen ez az egészek gyűrűje. Eszerint a hatvány egész bázis generátorok kiszámítása visszavezethető egy harmadfokú Thue egyenletre és egy kvadratikus forma egyenletrendszerre. Gaál István, Pethő Attila és M. Pohst [22] cikkében ki van dolgozva egy általános módszer ilyen típusú kvadratikus forma egyenletrendszerek megoldására. Ezen egyenletrendszerek negyedfokú Thue egyenletek megoldására vezethetők vissza. Teljesen komplex negyedfokú számtestek esetén a kvadratikus forma egyenletrendszerből egy pozitív definit kvadratikus forma konstruálható (lásd [11]).

3.2. Komplex másodfokú testek negyedfokú bővítéseinek végtelen parametrikus családjai: Relatív és abszolút hatvány egész bázisok

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

Legyen M másodfokú számtest, $K = M(\xi)$ az M relatív negyedfokú bővítése (tehát K nyolcadfokú). Célunk először is az, hogy meghatározzuk a relatív hatvány egész bázisát $\mathcal{O} = \mathbb{Z}_M[\xi]$-nek $\mathbb{Z}_M$ felett. Ezt követően ezeket az eredményeket felhasználva meghatározzuk az abszolút hatvány egész bázisokat.

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

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

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

3. Tétel (Gaál I., Szabó T. [31]). $|t|^2 > 245$ *esetén az* $\mathcal{O}$ *relatív hatvány egész bázisának összes nem ekvivalens generátorát* $\mathbb{Z}_M$ *felett megadja az alábbi formula:*

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

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

$D = -3$ esetén

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

is hatvány egész bázist generál, ahol $\omega_3 = (1+i\sqrt{3})/2$.

Az $\mathcal{O}$ gyűrű $\mathbb{Z}$ feletti (abszolút) hatvány egész bázisaira vonatkozóan kapjuk:

4. Tétel (Gaál I., Remete L., Szabó T. [27]). *$|t|^2 > 245$ feltétel mellett $\mathcal{O}$-nak nincs (abszolút) hatvány egész bázisa $\mathbb{Z}$ felett.*

Egy másik család esetén is sikerült hasonló eredményeket elérni:

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

$$f(X) = X^4 - 4tX^3 + (6t+2)X^2 + 4tX + 1 \in \mathbb{Z}_M[X]$$

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

5. Tétel (Gaál I., Szabó T. [31]). *$|t| > 1544803$ esetén az $\mathcal{O}$ relatív hatvány egész bázisának összes nem ekvivalens generátorát $\mathbb{Z}_M$ felett megadja az alábbi formula:*

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

Az $\mathcal{O}$ gyűrű $\mathbb{Z}$ feletti (abszolút) hatvány egész bázisaira vonatkozóan kapjuk:

6. Tétel (Gaál I., Remete L., Szabó T. [27]). $|t| > 1544803$ *feltétel mellett* $\mathcal{O}$*-nak nincs (abszolút) hatvány egész bázisa* $\mathbb{Z}$ *felett.*

A fő eszköz, amelyet a relatív hatvány egész bázisok kiszámításához alkalmazni fogunk, Gaál István és Michael Pohst [25] cikkének módszere. Ez a módszer az indexforma egyenletet visszavezeti relatív harmadfokú Thue egyenlet és néhányat relatív negyedfokú Thue egyenletre.

Ahhoz, hogy meg tudjuk határozni $\mathcal{O}$-ban az összes (abszolút) hatvány egész bázis generátort, az alábbi lépéseket kell követnünk:

I. Lépés *Ekvivalencia erejéig meghatározunk minden* $\alpha_0 \in \mathcal{O}$ *relatív hatvány egész bázis generátort* $\mathcal{O}$*-ban* M *felett.*

II. Lépés *Adott* α_0 *esetén határozzuk meg* $\varepsilon \in M$ *egység és* $A \in \mathbb{Z}_M$ *értékét úgy, hogy az* $\alpha = A + \varepsilon \cdot \alpha_0$ *elemre* $J(\alpha) = 1$ *teljesüljön.* (lásd (2))

1. Introduction

Monogentity of number fields and the calculation of generators of **power integral bases** is a classical topic of algebraic number theory.

We have general algorithms for calculating generators of power integral bases in lower degree number fields. In cubic and quartic fields there are efficient algorithms, in quintic and sextic fields there are more complicated but still usable algorithms for calculating the generators of the power integral bases.

The notion of index and power integral basis were extended also to the relative case, for *relative extensions* of number fields. It is a delicate problem to consider the same problem in *infinite parametric families* of number fields, when we are faced to solving the index form equation in a parametric form.

In the first chapter we consider some basic concepts of the algebraic number theory. Let α be az algebraic number of degree n and let $K = \mathbb{Q}(\alpha)$ an algebraic number field.

If $\alpha \in \mathbb{Z}_K$ is a primitive element of K (that is $K = \mathbb{Q}(\alpha)$), then the *index* of α is defined by the index of the additive group of $\mathbb{Z}[\alpha]$ in the additive group of $\mathbb{Z}_K$, that is

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

If $\alpha \in \mathbb{Z}_K$ then the elements $\beta = \pm\alpha + a$ $(a \in \mathbb{Z})$ are called *equivalent* with α.

For all $\alpha \in \mathbb{Z}_K$

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

where D_K is the discriminant of the field K and $D_{K/\mathbb{Q}}(\alpha)$ is the discriminant of the element α.

An integral basis of the form $\{1, \alpha, \ldots, \alpha^{n-1}\}$ we call *power integral basis*. In this case we call the element α the generator of the power integral basis.

Let $\{\omega_1 = 1, \omega_2, \ldots, \omega_n\}$ be an integral basis of K and

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

$(i = 1, 2, \ldots, n)$, where $\omega_j^{(i)}$ is a conjugate of ω_j. Then

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

is a homogeneous polynomial with integer coefficients of degree $n(n-1)$ that we can represent in the form

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

where $I(X_2, \ldots, X_n)$ is also a homogeneous polynomial with integer coefficients of degree $n(n-1)/2$. The form $I(X_2, \ldots, X_n)$ we call the *index form* belonging to the integral basis $\{\omega_1 = 1, \omega_2, \ldots, \omega_n\}$.

The *minimal index* of K is

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

We also consider monogenity and power integral bases in the relative case. Let M be an algebraic number field of degree m and K an extension of M with $[K : M] = n$. Then we have $[K : \mathbb{Q}] = n \cdot m$. Denote by $\mathbb{Z}_M$ the ring of integers of M. Let $\mathcal{O}$ be either the ring of integers $\mathbb{Z}_K$ of K or an order in $\mathbb{Z}_K$. We assume that there exist a relative power integral basis of $\mathcal{O}$ over M. If $\alpha \in \mathcal{O}$ is a primitive element of K over M (that is $K = M(\alpha)$), then the *relative index* of α over M is

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

The relative index is equal to 1 if and only if $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a *relative power integral basis* of $\mathcal{O}$ over $\mathbb{Z}_M$.

In Chapter 3 we calculated the (absolute) power integral bases by using relative power integral bases. We have

$$\begin{aligned} I_{\mathcal{O}}(\alpha) &= (\mathcal{O}^+ : \mathbb{Z}[\alpha]^+) = \\ &= (\mathcal{O}^+ : \mathbb{Z}_M[\alpha]^+) \cdot (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+), \end{aligned} \tag{1}$$

where the indices of the additive groups of the corresponding rings are calculated. The first factor is just the relative index of α:

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

$I_{\mathcal{O}}(\alpha) = 1$ can only be satisfied if both factors of (1) are equal to 1. Therefore a primitive element $\alpha \in \mathcal{O}$ generates a power integral basis of $\mathcal{O}$ if and only if

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

and

$$J(\alpha) = (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+) = 1.$$

Hence if α generates a power integral basis of $\mathcal{O}$, then it generates a relative power integral basis of $\mathcal{O}$ over M.

It is well known that generators or relative power integral bases are determined up equivalence, that is up to multiplication by a unit in M and up to translation by element of $\mathbb{Z}_M$. If α generates a power integral basis of $\mathcal{O}$, then

$$\alpha = A + \varepsilon \cdot \alpha_0, \tag{2}$$

where α_0 is a generator of a relative power integral basis of $\mathcal{O}$ over M, ε is a unit in M and $A \in \mathbb{Z}_M$.

The results of the thesis can be found in Chapter 2 and Chapter 3.

In Chapter 2 we study the existence of the power integral bases and the behaviour of minimal indices of pure cubic fields. Then we calculate power integral bases in sextic fields with a quadratic subfield.

In Chapter 3 we consider parametric families of biquadratic fields and infinite parametric families of

octic field that are quartic extensions of quadratic fields. We investigated the existence of power integral bases in the absolute and in the relative case, as well.

2. Cubic and relative cubic fields

2.1. On the behaviour of minimal indices of pure cubic fields

Using standard techniques, we studied the existence of power integral bases and the behaviour of minimal indices of pure cubic fields of type $K = \mathbb{Q}(\sqrt[3]{n})$ (n is a cube-free positive integer) up to discriminant $|D_K| < 3 \cdot 10^6$ and $|D_K| < 12 \cdot 10^6$, respectively. Such calculations for these special fields are performed here for the first time. This yields to solve cubic Thue equations, that may have extreme coefficients in some examples. Based on our computational results on index form equations in these fields, we consider the frequency of fields with power integral bases and the average behaviour of minimal indices. Our computations shows, that *the frequency of fields with power integral bases decreases and the average value of the minimal index increases as the field discriminant increases.*

To achieve our results we needed to solve more then 2000 index form equations. To solve the index form equations (cubic Thue equations), we used KASH [6].

The following calculations were required:

A. Calculating all elements generating power integral bases in pure cubic fields up to discriminant $|D_K| < 12 \cdot 10^6$.

B. Calculating the minimal indices and all elements with minimal index in pure cubic fields up to discriminant $|D_K| < 3 \cdot 10^6$.

After making the calculations, we characterize the frequency of the existence of the power integral bases and the average behaviour of minimal indices.

To construct the following table, we split the interval $[1,\, 12 \cdot 10^6]$ into 10 parts of equal length. For each subinterval, we divide the number of fields having $|D_K|$ in that interval admitting power integral basis by the total number of fields with $|D_K|$ in that interval.

D_K			number of fields	frequency
0	$\leq \lvert D_K \rvert <$	$12 \cdot 10^5$	375	0.37
$12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$2 \cdot 12 \cdot 10^5$	178	0.27
$2 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$3 \cdot 12 \cdot 10^5$	137	0.27
$3 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$4 \cdot 12 \cdot 10^5$	122	0.27
$4 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$5 \cdot 12 \cdot 10^5$	116	0.25
$5 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$6 \cdot 12 \cdot 10^5$	97	0.26
$6 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$7 \cdot 12 \cdot 10^5$	86	0.24
$7 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$8 \cdot 12 \cdot 10^5$	80	0.26
$8 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$9 \cdot 12 \cdot 10^5$	80	0.20
$9 \cdot 12 \cdot 10^5$	$\leq \lvert D_K \rvert <$	$12 \cdot 10^6$	81	0.21

It is seen that the frequency of fields with power integral bases is decreasing.

To construct the following table, we split the interval $[1, 3 \cdot 10^6]$ into 10 parts of equal length. In each subinterval we calculate the arithmetical mean of the minimal indices of the fields having $|D_K|$ in that interval.

D_K			number of fields	average min index
0	$\leq \|D_K\| <$	$3 \cdot 10^5$	175	2.29
$3 \cdot 10^5$	$\leq \|D_K\| <$	$2 \cdot 3 \cdot 10^5$	80	2.68
$2 \cdot 3 \cdot 10^5$	$\leq \|D_K\| <$	$3 \cdot 3 \cdot 10^5$	60	2.90
$3 \cdot 3 \cdot 10^5$	$\leq \|D_K\| <$	$4 \cdot 3 \cdot 10^5$	60	3.10
$4 \cdot 3 \cdot 10^5$	$\leq \|D_K\| <$	$5 \cdot 3 \cdot 10^5$	54	3.61
$5 \cdot 3 \cdot 10^5$	$\leq \|D_K\| <$	$6 \cdot 3 \cdot 10^5$	50	3.22
$6 \cdot 3 \cdot 10^5$	$\leq \|D_K\| <$	$7 \cdot 3 \cdot 10^5$	37	4.76
$7 \cdot 3 \cdot 10^5$	$\leq \|D_K\| <$	$8 \cdot 3 \cdot 10^5$	37	2.86
$8 \cdot 3 \cdot 10^5$	$\leq \|D_K\| <$	$9 \cdot 3 \cdot 10^5$	33	3.55
$9 \cdot 3 \cdot 10^5$	$\leq \|D_K\| <$	$3 \cdot 10^6$	43	4.12

It is seen that the minimal index increases in average as $|D_K|$ increases.

2.2. Sextic fields with quadratic subfield

Calculating power integral bases in sextic fields with a quadratic subfield leads to resolution of cubic relative Thue equations (cf. [23]).

We often used the method of A.Pethő [42], based on the continued fraction algorithm, which gave an efficient way to calculate "small" solutions of Thue equations. "Small" yields here an upper bound, say

10^{500} for the absolute values of the solutions. This was very much faster than the complete resolution of the equation, and gave all solutions with very high probability, certainly all that can be used in practice.

Recently István Gaál [14] developed such a fast algorithm to calculate "small" solutions (e.g. with sizes less than 10^{500}) of relative Thue equations. The algorithm is based on the LLL reduction algorithm [37] as one could expect. Since in higher degree number fields even the calculation of basic field data (integral basis, fundamental units) can become a hard and time consuming problem, this algorithm seems to have several useful applications.

In [26] we extend the list of [23] by calculating generators of power integral bases of sextic fields with quadratic subfields having "small" coordinates (i.e. $< 10^{250}$ in absolute value). We use the input data of M.Olivier [41].

Let M be a quadratic field with integral basis $\{1, \omega\}$. Let $f(X) = X^3 + \gamma_2 X^2 + \gamma_1 X + \gamma_0 \in \mathbb{Z}_M[X]$ be the cubic minimal polynomial of ϑ over M genarting the field $K = \mathbb{Q}(\vartheta)$. In the tables of M.Olivier [41], in about 99% of the cases this ϑ can be chosen so that ϑ has relative index 1 over M, which implies, that $\{1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2\}$ is an integral basis of K. So all integral elements of K can be written in the form

$$\alpha = x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2, \qquad (3)$$

with $x_i, y_i \in \mathbb{Z}$ $(i = 0, 1, 2)$.

Let $C = 10^{250}$. Our purpose is to determine all elements α of (3), generating a power integral basis and setisfying

$$max(|x_1|, |x_2|, |y_0|, |y_1|, |y_2|) < C. \tag{4}$$

Denote by $\vartheta = \vartheta^{(1)}, \vartheta^{(2)}, \vartheta^{(3)}$ the conjugates of ϑ over M. Let $\varrho = -\vartheta^{(1)} - \vartheta^{(2)}$. The element α of (3) generates a power integral basis of K if and only if the quadratic integers $X = x_1 + \omega y_1$, $Y = x_2 + \omega y_2$ satisfy the relative Thue equation

$$N_{K/M}(X - \varrho Y) = \nu, \quad X, Y \in \mathbb{Z}_M \tag{5}$$

(with a unit ν of M) and x_1, x_2, y_0, y_1, y_2 is a solution of a degree 9 polynomial equation

$$F(x_1, x_2, y_0, y_1, y_2) = \pm 1, \quad x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}. \tag{6}$$

For the construction of F see [23].

First of all let K be a sextic field with *imaginary quadratic subfeld*. In order to determine all generators of power integral bases (3) satisfying (4) of K one has to determine x_1, x_2, y_1, y_2 by solving the relative Thue equation (5). In case M is an imaginary quadratic subfield ν can take finitely many values. For each solution x_1, x_2, y_1, y_2 of (5) we calculate y_0 from (6) ($x_0 \in \mathbb{Z}$ is arbitrary).

The running time was about 2-5 minutes per example, therefore it made possible to list the results for the first 100 number fields of smallest discriminants in absolute value.

The list of our calculations can be found in Chapter 4.2.

Now let K be a sextic field with a *real quadratic subfield*. In order to determine all generators of power integral bases (3) setisfying (4) of K one has to determine x_1, x_2, y_1, y_2 by solving the relative Thue equation (5).

The difficulty of the task in these is that real quadratic fields admits infinitely many units. Therefore we obtain

$$N_{K/M}(X - \varrho Y) = \pm\varepsilon^k, \quad X, Y \in \mathbb{Z}_M \tag{7}$$

where ε is the fundamental unit of the real quadratic field M, $k \in \mathbb{Z}$. Let $k = 3m + r$, where $m, r \in \mathbb{Z}$, $r \in \{-1, 0, 1\}$. The bound (4) implies an upper bound for $|k|$ and then for $|m|$, as well. Set $X_0 = \varepsilon^{-m}X$, $Y_0 = \varepsilon^{-m}Y$. From the bounds on $|m|$ and from (4) we obtain bounds for the components of X_0 and Y_0 in the integral basis. Therefore we have to determine the solutions of

$$N_{K/M}(X_0 - \varrho Y_0) = \pm\varepsilon^r, \quad X_0, Y_0 \in \mathbb{Z}_M,$$

under this bound. Using

$$x_1 + \omega y_1 = X = \varepsilon^{-m} X_0,$$
$$x_2 + \omega y_2 = Y = \varepsilon^{-m} Y_0$$

for each possible m and for each X_0, Y_0 we calculate x_1, x_2, y_1, y_2 and by (6) we calculate y_0.

The list of the results can be found in Chapter 4.3.

3. Quartic and relative quartic fields

In this chapter we calculate power integral bases in quartic fields and calculate relative and absolute power integral bases in quartic extensions of imaginary quadratic fields.

3.1. Power integral bases in parametric families of biquadratic fields

J.G.Huard, B.K.Spearman and K.S.Williams [35] recently gave explicitly the integral bases in biquadratic number fields of type $\mathbb{Q}(\sqrt{a+b\sqrt{c}})$. In their paper J.G.Huard, B.K.Spearman and K.S.Williams [35] also considered two infinite parametric families of fields of type $\mathbb{Q}(\sqrt{a+b\sqrt{c}})$ involving two parameters. The

authors proved that these families admit power integral bases.

We solve completely the index form equation in these two parametric families of biquadratic fields and show that all power integral bases are those given in [35]. This is the first time that the index form equation is completely solved in infinite parametric families of number fields, involving *two parameters*.

Let $c < 0$ be an integer and for positive integers k set

$$f_c(k) = 16k^2 + 24k + (9 - 4c),$$

$$g_k = 4k + 3,\ h_k = 2 \text{ ha } c \equiv 1 \pmod 4$$

$$f_c(k) = 4k^2 + 4(c+1)k + (c^2 + c + 1),$$

$$g_k = 2k + c + 1,\ h_k = 1 \text{ ha } c \equiv 2, 3 \pmod 4.$$

Following the arguments of [35] we conclude that for each c, $f_c(k)$ is square-free for infinitely many k. We denote by S the set of pairs (c, k) with $c < -3$, $k > |c|$ and $f_c(k)$ square-free. Obviously, S is an infinite set. Further, for each c we have $f_c(k) = g_k^2 - ch_k^2$ greater than c, hence $L_{c,k} = \mathbb{Q}(\sqrt{g_k + b_k\sqrt{c}})$ is a quartic extension of $\mathbb{Q}$. $L_{c,k}$ contains the complex quadratic field $\mathbb{Q}(\sqrt{c})$ hence it is a totally complex quartic field.

We prove:

1. Theorem (I. Gaál, T. Szabó [30]). *Let $c \equiv 1 \pmod 4$. Then for all $(c, k) \in S$ up to equivalence the*

only power integral basis in $L_{c,k}$ is generated by

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

2. Theorem (I. Gaál, T. Szabó [30]). *Let $c \equiv 2, 3 \pmod 4$. Then for all $(c, k) \in S$ up to equivalence the only power integral basis in $L_{c,k}$ is generated by*

$$\vartheta = \sqrt{g_k + \sqrt{c}}.$$

J.G.Huard, B.K.Spearman and K.S.Williams [35] showed that the above elements generate power integral bases. We completely solve the index form equation and prove that up to equivalence there are no other generators of power integral bases.

In the proof of the results we use the statements of István Gaál, Attila Pethő and M. Pohst [20]. According to this result the calculation of the generators of the power integral bases can be reduced to a cubic Thue equation and a system of equations with quadratic forms.

3.2. Infinite parametric families of quartic extensions of quadratic fields: Relative és absolute power integral bases

In this Chapter we describe our results on absolute and relative power integral bases in infinite parametric families of quartic extensions of quadratic fields.

We are going to consider two infinite parametric families of octic fields $K = M(\xi)$ over their quadratic subfield M. Our purpose is to describe the relative power integral bases of $\mathcal{O} = \mathbb{Z}_M[\xi]$. Then we use these results to calculate the absolute power integral bases of $\mathcal{O}$.

I. Let $D > 0$ be a square-free integer, $M = \mathbb{Q}(\sqrt{-D})$, $t \in \mathbb{Z}_M$ a parameter and let ξ be a root of

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

Let $K = M(\xi)$ and consider the relative power integral bases of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$.

3. Theorem (I. Gaál, T. Szabó [31]). *For* $|t|^2 > 245$ *all non-equivalent generators of power integral bases of* $\mathcal{O}$ *over* $\mathbb{Z}_M$ *are given by*

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

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

Moreover for $D = -3$ we also have

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

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

For the absolute power integral bases of $\mathcal{O}$ over $\mathbb{Z}$ we have

4. Theorem (I. Gaál, L. Remete, T. Szabó [27]). *Under the above conditions for* $|t|^2 > 245$ *the order* $\mathcal{O}$ *admits no power integral bases.*

II. Let $D > 0$ be a square-free integer, $M = \mathbb{Q}(\sqrt{-D})$, $t \in \mathbb{Z}_M$ a parameter and let ξ be a root of

$$f(X) = X^4 - 4tX^3 + (6t + 2)X^2 + 4tX + 1 \in \mathbb{Z}_M[X].$$

Let $K = M(\xi)$ and consider the relative power integral bases of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$.

5. Theorem (I. Gaál, T. Szabó [31]). *For* $|t| > 1544803$ *all non-equivalent generators of power integral bases of* $\mathcal{O}$ *over* $\mathbb{Z}_M$ *are given by*

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

For the absolute power integral bases of $\mathcal{O}$ over $\mathbb{Z}$ we have

6. Theorem (I. Gaál, L. Remete, T. Szabó [27]). *Under the above conditions for* $|t| > 1544803$ *the order* $\mathcal{O}$ *admits no power integral bases.*

Our main tool throughout is the application of the method of István Gaál, M. Pohst [25]. This reduces the relative index form equation to a relative cubic Thue equation and some relative quartic Thue equations.

In order to determine all generators of (absolute) power integral bases of $\mathcal{O}$ we have to perform the following steps:

Step 1 *Determine up to equivalence all generators* $\alpha_0 \in \mathcal{O}$ *of relative power integral bases of* $\mathcal{O}$ *over* M.

Step 2 *If* $I(\alpha) = 1$, *then* $\alpha = A + \varepsilon \cdot \alpha_0$, *where* $A \in \mathbb{Z}_M$, $\varepsilon \in U_M$. *Determine* A, ε *so that* $J(\alpha) = 1$ *is satisfied.*

Hivatkozások

[1] A. Baker, Transcendental number theory, Cambridge, 1990.

[2] 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.

[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] W. Bosma and J. Cannon, *Discovering mathematics with Magma. Reducing the abstract to the concrete*, Algorithms and Computation in Mathematics 19. Berlin, Springer, 2006.

[5] B.W. Char, K.O. Geddes, G.H. Gonnet, M.B. Monagan, S.M. Watt (eds.) *MAPLE, Reference Manual*, Watcom Publications, Waterloo, Canada, 1988.

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

[7] 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.

[8] L. El Fadil, *Computation of a power integral basis of a pure cubic number field*, Int. J. Contemp. Math. Sci., **2** (2007), 601–606.

[9] J.H. Evertse, K. Győry, Unit Equations in Diophantine Number Theory, Cambridge University Press, 2015.

[10] J.H. Evertse, K. Győry, Discriminant Equations in Diophantine Number Theory, Cambridge University Press, 2016.

[11] I. Gaál, *Power integral bases in orders of families of quartic fields*, Publ. Math. (Debrecen), **42** (1993), 253–263.

[12] I. Gaál, *Power integral bases in cubic relative extensions*, Experimental Math., **10** (2001), 133–139.

[13] I. Gaál, Diophantine equations and power integral bases, New Computational Methods, Birkhäuser Boston, 2002.

[14] I. Gaál, *Calculating "small" solutions of relative Thue equations*, Experimental Math., **24** (2015), 142–149.

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

[16] I. Gaál and G. Lettl, *A parametric family of quintic Thue equations*, Math. Comput., **69** (1999), 851–859.

[17] I. Gaál and G. Lettl, *A parametric family of quintic Thue equations II.*, Monatsh. Math., **131** (2000), 29–35.

[18] I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations*, Proc. of the 1991 International Symposium on Symbolic and Algebraic Computation, ed. by Stephen M. Watt, ACM Press, (1991), 185–186.

[19] 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.

[20] 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.

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

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

[25] I. Gaál and M. Pohst, *On the resolution of index form equations in relative quartic extensions*, J.Number Theory, **85** (2000), 201–219.

[26] I. Gaál, L. Remete and T. Szabó, *Calculating power integral bases by solving relative Thue equations*, Tatra Mt. Math. Publ. **59** (2014), 79–92.

[27] I. Gaál, L. Remete and T. Szabó, *Calculating power integral bases by using relative power integral bases*, Functiones et Approximatio **54.2** (2016), 141–149.

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

[29] I. Gaál and T. Szabó, *A note on the minimal indices of pure cubic fields*, JP Journal of Algebra, Number Theory and Applications, **19** (2010), 129–139.

[30] 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.

[31] 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, **29** (2013), 31–34.

[32] K. Győry, *Sur les polynomes a coefficients entiers et de discriminant donne, III*, Publ. Math. (Debrecen), **23** (1976), 141–165.

[33] M. Hall, *Indices in cubic fields*, Bull. Amer. Math. Soc. **43** (1937), 104–108.

[34] H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin, 1963.

[35] 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.

[36] B. Jadrijević, 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.

[37] A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), 515–534.

[38] D.A. Marcus, *Number fields*, Universitext, Springer, 1977.

[39] L.J. Mordell, Diophantine equations, Pure and Applied Mathematics, 30. London-New York: Academic Press, 1969.

[40] G. Nyul, *Power integral bases in mixed biquadratic number fields*, Acta Acad. Paed. Agriensis, Sect. Math. **28** (2001) 79–86.

[41] M. Olivier, *Corps sextiques contenant un corps quadratique (II)*, J. théorie des nombres de Bordeaux **1** (1990), 49-102.

[42] A. Pethő, *On the resolution of Thue inequalities*, J.Symbolic Comput., **4** (1987), 103–109.

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

[44] V. Ziegler, *On a family of relative quartic Thue inequalities*, J. Number Theory **120** (2006), No. 2, 303–325.

Publikációk/List of publications

- I. Gaál and T. Szabó, *A note on the minimal indices of pure cubic fields*, JP Journal of Algebra, Number Theory and Applications, **19** (2010), 129–139.

- 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.

- 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, **29** (2013), 31–34.

- I. Gaál, L. Remete and T. Szabó, *Calculating power integral bases by solving relative Thue equations*, Tatra Mt. Math. Publ. **59** (2014), 79–92.

- I. Gaál, L. Remete and T. Szabó, *Calculating power integral bases by using relative power integral bases*, Functiones et Approximatio **54.2** (2016), 141–149.

Előadások/List of talks

- *On the behaviour of minimal indices of number fields*, 20th Czech and Slovak International Conference on Number Theory, 2011. szeptember 5-9., Stará Lesná (Szlovákia)

- *Power integral bases in infinite families of quartic fields*, 21st Czech and Slovak International Conference on Number Theory, 2013. szeptember 2-6., Ostravice (Csehország)

- *Power integral bases in quartic fields and quartic extensions*, 29th Journées Arithmétiques 2015. július 6-10., Debrecen

- *Power integral bases in quartic fields and quartic extensions*, 22th Czech and Slovak International Conference on Number Theory, 2015. augusztus 30 - szeptember 4., Liptovsky Jan (Szlovákia)

- *Power integral bases in quartic fields and quartic extensions*, Computational Aspects of Diophantine Equations, 2016. február 15-19., Salzburg (Ausztria)

DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR

Nyilvántartási szám: DEENK/282/2017.PL
Tárgy: PhD Publikációs Lista

Jelölt: Szabó Tímea
Neptun kód: MI3XH1
Doktori Iskola: Matematika- és Számítástudományok Doktori Iskola
MTMT azonosító: 10051816

A PhD értekezés alapjául szolgáló közlemények

Idegen nyelvű tudományos közlemények külföldi folyóiratban (5)

1. Gaál, I., Remete, L., **Szabó, T.**: Calculating power integral bases by using relative power integral bases.
   Funct. Approx. Comment. Math. 54 (2), 141-149, 2016. ISSN: 0208-6573.
   DOI: http://dx.doi.org/10.7169/facm/2016.54.2.1
2. Gaál, I., Remete, L., **Szabó, T.**: Calculating power integral bases by solving relative Thue equations.
   Tatra Mt. Math. Publ. 59, 79-92, 2014. ISSN: 1210-3195.
   DOI: http://dx.doi.org/10.2478/tmmp-2014-0020
3. Gaál, I., **Szabó, T.**: Relative power integral bases in infinite families of quartic extensions of quadratic field.
   JP J. Algebra, Number Theory Appl. 29 (1), 31-43, 2013. ISSN: 0972-5555.
4. Gaál, I., **Szabó, T.**: Power integral bases in parametric families of biquadratic fields.
   JP J. Algebra, Number Theory Appl. 24 (1), 105-114, 2012. ISSN: 0972-5555.
5. Gaál, I., **Szabó, T.**: A note on the minimal indices of pure cubic fields.
   JP J. Algebra, Number Theory Appl. 19 (2), 129-139, 2010. ISSN: 0972-5555.

A DEENK a Jelölt által az iDEa Tudóstérbe feltöltött adatok bibliográfiai és tudománymetriai ellenőrzését a tudományos adatbázisok és a Journal Citation Reports Impact Factor lista alapján elvégezte.

Debrecen, 2017.09.19.

Cím: 4032 Debrecen, Egyetem tér 1. ¤ Postacím: 4010 Debrecen, Pf. 39. ¤ Tel.: (52) 410-443
E-mail: publikaciok@lib.unideb.hu ¤ Honlap: www.lib.unideb.hu

Registry number: DEENK/282/2017.PL
Subject: PhD Publikációs Lista

Candidate: Tímea Szabó
Neptun ID: MI3XH1
Doctoral School: Doctoral School of Mathematical and Computational Sciences
MTMT ID: 10051816

List of publications related to the dissertation

Foreign language scientific articles in international journals (5)

1. Gaál, I., Remete, L., **Szabó, T.**: Calculating power integral bases by using relative power integral bases.
   Funct. Approx. Comment. Math. 54 (2), 141-149, 2016. ISSN: 0208-6573.
   DOI: http://dx.doi.org/10.7169/facm/2016.54.2.1
2. Gaál, I., Remete, L., **Szabó, T.**: Calculating power integral bases by solving relative Thue equations.
   Tatra Mt. Math. Publ. 59, 79-92, 2014. ISSN: 1210-3195.
   DOI: http://dx.doi.org/10.2478/tmmp-2014-0020
3. Gaál, I., **Szabó, T.**: Relative power integral bases in infinite families of quartic extensions of quadratic field.
   JP J. Algebra, Number Theory Appl. 29 (1), 31-43, 2013. ISSN: 0972-5555.
4. Gaál, I., **Szabó, T.**: Power integral bases in parametric families of biquadratic fields.
   JP J. Algebra, Number Theory Appl. 24 (1), 105-114, 2012. ISSN: 0972-5555.
5. Gaál, I., **Szabó, T.**: A note on the minimal indices of pure cubic fields.
   JP J. Algebra, Number Theory Appl. 19 (2), 129-139, 2010. ISSN: 0972-5555.

The Candidate's publication data submitted to the iDEa Tudóstér have been validated by DEENK on the basis of Web of Science, Scopus and Journal Citation Report (Impact Factor) databases.

19 September, 2017

Address: 1 Egyetem tér, Debrecen 4032, Hungary Postal address: Pf. 39. Debrecen 4010, Hungary
Tel.: +36 52 410 443 Fax: +36 52 512 900/63847 E-mail: publikaciok@lib.unideb.hu, ◻ Web: www.lib.unideb.hu