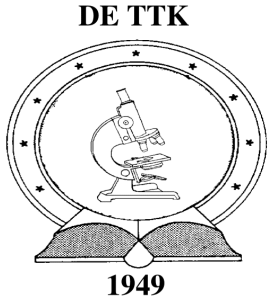

Algebrai számtestek monogenitása az abszolút és a relatív esetben

Egyetemi doktori (PhD) értekezés

Szabó Tímea
Témavezető: Dr. Gaál István

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

Ezen értekezést a Debreceni Egyetem Természettudományi Doktori Tanács Matematika- és Számítástudományok Doktori Iskola *Explicit módszerek az algebrai számelméletben* programja keretében készítettem a Debreceni Egyetem természettudományi doktori (PhD) fokozatának elnyerése céljából.
Nyilatkozom arról, hogy a tézisekben leírt eredmények nem képezik más PhD disszertáció részét.

Debrecen, 2017.

Szabó Tímea
jelölt

Tanúsítom, hogy Szabó Tímea doktorjelölt 2013 - 2016 között a fent megnevezett Doktori Iskola *Explicit módszerek az algebrai számelméletben* programjának keretében irányításommal végezte munkáját. Az értekezésben foglalt eredményekhez a jelölt önálló alkotó tevékenységével meghatározóan hozzájárult.
Nyilatkozom továbbá arról, hogy a tézisekben leírt eredmények nem képezik más PhD disszertáció részét.
Az értekezés elfogadását javasolom.

Debrecen, 2017.

Gaál István
témavezető

Algebrai számtestek monogenitása az abszolút és a relatív esetben

Értekezés a doktori (Ph.D.) fokozat megszerzése érdekében
a Matematika- és Számítástudományok tudományágban

Írta: Szabó Tímea okleveles matematikus

Készült a Debreceni Egyetem Matematika- és Számítástudományok
Doktori Iskolája (Explicit módszerek az algebrai számelméletben
programja) keretében.

Témavezető: Dr. Gaál István

A doktori szigorlati bizottság:

elnök: Dr. Hajdu Lajos .....
tagok: Dr. Szalay László .....
Dr. Tengely Szabolcs .....

A doktori szigorlat időpontja: 2016. december 9.

Az értekezés bírálói:

Dr. .....
Dr. .....

A bírálóbizottság:

elnök: Dr. .....
tagok: Dr. .....
Dr. .....
Dr. .....
Dr. .....

Az értekezés védésének időpontja: 2017. .....

Köszönetnyilvánítás

Köszönetemet fejezem ki mindenkinek, aki valamilyen módon támogatott és hozzájárult ezen dolgozat elkészítéséhez.

Elsősorban témavezetőmnek, *Dr. Gaál István*nak szeretnék köszönetet mondani egyetemi éveim alatt nyújtott segítségéért, és a disszertációm elkészítéséhez nyújtott szakmai tanácsaiért.

Szeretném megköszönni általános- és középiskolai, illetve egyetemi oktatóimnak, hogy hozzájárultak szellemi és szakmai fejlődésemhez, illetve megmutatták a matematika szépségeit.

Végezetül szeretnék köszönetet mondani szüleimnek és családomnak, hogy az évek alatt mindig támogatták célkitűzéseimet.

Tartalomjegyzék

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.

Az első példát olyan számtestre, melyben nem létezik hatvány egész bázis, Dedekind [7] adta 1878-ban. Az 1960-as években Hasse [34] vetette fel a hatvány egész bázissal rendelkező számtestek aritmetikai jellemzésének kérdését.

Jól ismert, hogy a hatvány egész bázisok meghatározásának problémája ekvivalens az indexforma egyenlet megoldásának problémájával. Így az indexforma egyenlet megoldásaira kapott eredmények segítségünkre lehetnek a hatvány egész bázisok meghatározásakor.

A Baker módszer [1] megjelenése után 1976-ban Győry Kálmán [32] effektív felső korlátot adott indexforma egyenletek megoldására. Ebből tetszőleges számtest esetén következett a hatvány egész bázisok számának végessége (ekvivalencia erejéig), sőt elméleti algoritmust is adott a megoldások meghatározására, 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 megjelenése (lásd [2]) és annak továbbfejlesztése az LLL algoritmus felhasználásával (lásd [37]) 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 [28] foglalta táblázatba a kis diszkriminánsú harmadfokú számtestek hatvány egész bázisait.

Gaál István, Pethő Attila és M. Pohst [22] tetszőleges negyedfokú

számtestek indexforma egyenletének megoldására adott hatékony algoritmust, visszavezetve azt harmad- és negyedfokú Thue egyenletekre.

Ötödfokú számtestek esetén Gaál István és Győry Kálmán [15], hatodfokú számtestek esetén Y. Bilu, Gaál István és Győry Kálmán [3] adtak algoritmust az indexforma egyenlet megoldására, de ezek az algoritmusok már jelentős számolásigénnyel rendelkeznek.

Magasabb fokú számtestek esetén csak speciális esetekben (pl. résztestek létezése esetén) sikerült algoritmust adni az indexforma egyenlet megoldására, lásd Gaál István [13].

Hatvány egész bázisok problémakörét relatív bővítésekben is vizsgálták. Gaál István [12] harmadfokú relatív bővítésekben, Gaál István és M. Pohst [25] negyedfokú relatív bővítésekben adott algoritmust a relatív hatvány egész bázisok generátorainak kiszámítására.

Ezen túlmenően rendkívül érdekes problémát jelent, ha hasonló számításokat elvégzünk adott fokú számtestek végtelen parametrikus családjában. Ekkor nemcsak egy konkrét indexforma egyenletet, hanem indexforma egyenletek egy végtelen parametrikus családját kell megoldani. Ilyen jellegű számításokat végzett Gaál István [11], Gaál István és M. Pohst [24], Gaál István és G. Lettl [16], [17], stb.

Értekezésem 1.1. Fejezetében tárgyaljuk az algebrai számelméleti alapokat a könnyebb érthetőség kedvéért.

A 2.1. Fejezetben vizsgáljuk harmadfokú gyökbővítésekben a hatvány egész bázisok létezésének relatív gyakoriságát és a minimális indexek viselkedését, melyeket mindeddig külön nem tanulmányoztak. Majd a 2.2. Fejezetben relatív harmadfokú testek esetén határozzuk meg és listázzuk ki a hatvány egész bázisok generátorait.

A 3. Fejezet tárgyalja negyedfokú és relatív negyedfokú bővítések végtelen parametrikus családjaiban az abszolút és a relatív hatvány egész bázisok létezését. A 3.1. Fejezetben negyedfokú bikvadratikus testek végtelen parametrikus családjaiban meghatározzuk a hatvány egész bázisok generátorait. Ez az első eset, amikor számtestek *két paraméter*étől függő végtelen családjában sikerül megoldani az indexforma egyenletet. A 3.2. Fejezetben relatív negyedfokú bővítések

esetén meghatározzuk a relatív hatvány egész bázisok generátorait, majd ezt felhasználva az (abszolút) hatvány egész bázisok generátorait is. Ez az első eredmény hatvány egész bázisok kiszámítására relatív bővítések végtelen parametrikus családjaiban.

Eredményeink az algebrai számelmélet klasszikus fejezetébe, az algebrai számtestek monogenitásának vizsgálatába tartoznak. Vizsgáljuk a harmadfokú gyökbővítések korábban nem vizsgált osztályát, valamint a monogenitás kérdését harmadfokú és negyedfokú számtestek végtelen parametrikus családjaiban. Vizsgálataink kiterjednek harmad- és negyedfokú relatív bővítésekre is. Vizsgáljuk egyrészt számtestek végtelen parametrikus családjait, másrészt konkrét számtestek esetén hatékony algoritmusokat implementálunk a hatvány egész bázisok generátorainak kiszámítására. Az ismertetett módszerek, algoritmusok felhasználhatóak lesznek számtestek más osztályai esetén is.

1.1. Algebrai számelméleti alapok

Ebben a fejezetben a könnyebb érthetőség kedvéért ismertetjük mindazon fogalmakat, melyeket a dolgozatban használni fogunk. A fogalmak és a tételek, illetve azok bizonyítása megtalálható a [13] könyvben.

Legyen ϑ n-edfokú algebrai egész szám, legyen $K = \mathbb{Q}(\vartheta)$ algebrai számtest, és jelölje $\mathbb{Z}_K$ a K test egészeinek gyűrűjét.

Azt mondjuk, hogy a K algebrai számtestnek $\{\omega_1 = 1, \omega_2, \ldots, \omega_n\}$ *egész bázis*a, ha bázis $\mathbb{Q}$ fölött, azaz minden $\alpha \in K$ esetén egyértelműen léteznek $x_1, \ldots, x_n \in \mathbb{Q}$, hogy

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

és $\alpha \in \mathbb{Z}_K$ pontosan akkor, ha $x_1, \ldots, x_n \in \mathbb{Z}$.

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

diszkriminánsa:

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

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

Az $\alpha \in K$ *elem 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 ($1 \leq i \leq n$).

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:

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

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 *ekvivalens*eknek nevezzük.

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.

Az $\{1, \alpha, \dots, \alpha^{n-1}\}$ alakú egész bázisokat *hatvány egész bázis*oknak nevezzük. Ilyen esetben az α elemet a hatvány egész bázis generátor elemének nevezzük. Nyilvánvaló, hogy α pontosan akkor generál hatvány egész bázist, ha $I(\alpha) = 1$. Mivel az index $\mathbb{Z}$-beli elemekkel történő eltolással szemben invariáns, ezért, ha α hatvány egész bázist generál, akkor ugyanez igaz minden vele ekvivalens elemre. Tehát a

hatvány egész bázisok generátor elemeit elegendő ekvivalencia erejéig meghatározni. $I(\alpha) = 1$ pontosan azt jelenti, hogy $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. Ezért, ha a K számtestben létezik hatvány egész bázis, akkor azt mondjuk, hogy K *monogén*.

A K *számtest indexe* (testindexe) alatt az

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

számot értjük.

A K számtest *minimális indexe* alatt az

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

számot értjük.

Ha K-ban van hatvány egész bázis, akkor vannak 1 indexű elemek, így $m_K = 1$ és $i_K = 1$. Ellenkező esetben érdekes és fontos probléma K minimális indexét és a minimális indexű elemeket kiszámítani. A minimális index akkor is lehet 1-nél nagyobb, ha $i_K = 1$.

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

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

$(i = 1, 2, \ldots, n)$. 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.

Tetszőleges $\alpha = x_1 + \omega_2 x_2 + \ldots + \omega_n x_n$ esetén

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

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 fentiek értelmében az m indexű elemeket ($0 < m \in \mathbb{Z}$) az

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

diofantikus egyenlet, úgynevezett *indexforma egyenlet* megoldásaiként kapjuk meg. Speciálisan, a hatvány egész bázisok generátorait $m = 1$ választás mellett kapjuk a fenti egyenlet megoldásával.

Győry Kálmán 1976-os [32] tétele szerint: Az (1) egyenletnek csak véges sok megoldása van.

Ezen eredmény különböző számelméleti vonatkozásban megtalálható a [9] és [10] könyvekben is.

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

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.

Azokat az $\mathcal{O}$-beli elemeket, melyek csak egy M-beli egységszorzóban vagy egy $\mathbb{Z}_M$-beli elemmel történő eltolásban különböznek, *relatív ekvivalens*eknek nevezzük M felett. Relatív ekvivalens elemek relatív indexe azonos. Relatív ekvivalencia erejéig a relatív hatvány egész bázisoknak csak véges sok generátora létezik.

A 3. Fejezetben foglalkozunk relatív bővítésekkel, és a relatív hatvány egész bázisok ismeretében szeretnénk meghatározni az (abszolút) hatvány egész bázis generátorokat. Az alábbiakban az ehhez kapcsolódó fogalmakat és összefüggéseket részletezzük (lásd [27]).

Jelölje $D_{\mathcal{O}}$ illetve D_M az $\mathcal{O}$ illetve M résztest diszkriminánsát. (Abban az esetben, ha $\mathcal{O} = \mathbb{Z}_K$, akkor $D_{\mathcal{O}} = D_K$, ahol D_K a K test diszkriminánsa.) Egy $\alpha \in \mathcal{O}$ elem $\mathcal{O}$-beli indexére fennáll

$$I_{\mathcal{O}}(\alpha) = (\mathcal{O}^+ : \mathbb{Z}[\alpha]^+) = \frac{\sqrt{|D_{K/\mathbb{Q}}(\alpha)|}}{\sqrt{|D_{\mathcal{O}}|}}. \tag{2}$$

Illetve azt is tudjuk, hogy

$$I_{\mathcal{O}}(\alpha) = (\mathcal{O}^+ : \mathbb{Z}_M[\alpha]^+) \cdot (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+), \tag{3}$$

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

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

Jelölje $D_{\mathcal{O}/M}$ az $\mathcal{O}$ relatív diszkriminánsát M felett. Ismert, hogy

$$D_{\mathcal{O}} = N_{M/\mathbb{Q}}(D_{\mathcal{O}/M}) \cdot D_M^{[K:M]}. \tag{4}$$

Jelölje $\gamma^{(i)}$ egy $\gamma \in M$ elem konjugáltjait ($i = 1, \dots, m$). Legyen $\delta^{(i,j)}$ a $\delta \in \mathcal{O}$ elem $\mathcal{O}$ azon automorfizmusa általi képe, amely az $M^{(i)}$ konjugált testeket elemenként fixen hagyja ($j = 1, \dots, n$). Ekkor egy $\alpha \in \mathcal{O}$ elem esetén

$$I_{\mathcal{O}/M}(\alpha) = \frac{\sqrt{|N_{M/\mathbb{Q}}(D_{\mathcal{O}/M}(\alpha))|}}{\sqrt{|N_{M/\mathbb{Q}}(D_{\mathcal{O}/M})|}} = \\ = \frac{1}{\sqrt{|N_{M/\mathbb{Q}}(D_{\mathcal{O}/M})|}} \cdot \prod_{i=1}^{m} \prod_{1 \le j_1 < j_2 \le n} \left|\alpha^{(i,j_1)} - \alpha^{(i,j_2)}\right|. \qquad (5)$$

Továbbá a (2), (3), (4) és (5) felhasználásával kapjuk, hogy

$$J(\alpha) = (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+) = \\ = \frac{1}{\sqrt{|D_M|}^{[K:M]}} \cdot \prod_{1 \le i_1 < i_2 \le m} \prod_{j_1=1}^{n} \prod_{j_2=1}^{n} \left|\alpha^{(i_1,j_1)} - \alpha^{(i_2,j_2)}\right|. \qquad (6)$$

Az α elem pontosan akkor generál hatvány egész bázist $\mathcal{O}$-ban, ha $I_{\mathcal{O}}(\alpha) = 1$. A (3) kifejezésben $I_{\mathcal{O}}(\alpha) = 1$ csak akkor teljesülhet, ha a (3) kifejezés mindkét faktora 1. Ezért az $\alpha \in \mathcal{O}$ elem pontosan akkor generál hatvány egész bázist $\mathcal{O}$-ban, ha

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

és

$$J(\alpha) = (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+) = 1. \qquad (7)$$

egyszerre teljesülnek.

Ebből következik, hogy ha α hatvány egész bázist generál $\mathcal{O}$-ban, akkor relatív hatvány egész bázist is generál $\mathcal{O}$-ban M felett.

Ismert, hogy a relatív hatvány egész bázisokat relatív ekvivalencia erejéig határozzuk meg, azaz M-beli egységgel történő szorzástól és $\mathbb{Z}_M$-beli elemmel történő eltolástól eltekintve.

1. Állítás. *Ha α hatvány egész bázist generál $\mathcal{O}$-ben, akkor*

$$\alpha = A + \varepsilon \cdot \alpha_0, \qquad (8)$$

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

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 harmadfokú gyökbővítésekben.

Külön figyelmet érdemelnek adott fokú számtestek speciális osztályai, végtelen parametrikus családjai, melyekben érdekes eredményekre vezet, ha tanulmányozzuk a hatvány egész bázisok létezése relatív gyakoriságának, vagy a minimális index nagyságának a tendenciáját valamely paraméter, vagy a számtestek diszkriminánsának a függvényében. Ilyen jellegű számításokat végzett Gaál István, Pethő Attila és M. Pohst [18] negyedfokú számtestek bizonyos osztályai esetén.

Az ilyen jellegű vizsgálatokból mindeddig kimaradtak a **harmadfokú gyökbővítések**, bár szinte a legegyszerűbb osztályát alkotják a legalább harmadfokú számtesteknek. Ezen számtestek egy végtelen parametrikus családnak tekinthetőek, melyek viselkedését mindeddig külön nem tanulmányozták.

Legyen $1 < n \in \mathbb{Z}$ köbmentes egész, $K = \mathbb{Q}(\sqrt[3]{n})$. A harmincas években M. Hall [33] megmutatta, hogy harmadfokú gyökbővítések esetén a minimális index tetszőlegesen nagy lehet. A közelmúltban El Fadil [8] megmutatta, hogy ha $n \not\equiv \pm 1 \pmod 9$ és $n = \pm\ell^2, \pm\ell(\ell+1)^2, \pm(\ell+1)\ell^2$ alakú, vagy négyzetmentes, akkor létezik K-ban hatvány egész bázis, azaz $m_K = 1$. Könnyen megmutatható az is, hogy minden harmadfokú gyökbővítésben $i_K = 1$.

Jelölje D_K a K számtest diszkriminánsát. Dolgozatunkban meghatározzuk azon számtestek hatvány egész bázisainak generátorait, melyekre $|D_K| < 12 \cdot 10^6$, majd jellemezzük a hatvány egész bázisok létezésének relatív gyakoriságát. Emellett meghatározzuk a minimális indexet és a minimális indexű elemeket azon számtestekben, melyekre $|D_K| < 3 \cdot 10^6$, és vizsgáljuk a minimális indexek átlagának viselkedését.

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 harmadfokú gyökbővítések esetén n tulajdonságaitól függően az egész bázis kétféle lehet, ennek megfelelően K diszkriminánsa és az egész bázishoz tartozó indexforma is különböző a két esetben.

Legyen $n > 1$ egy köbmentes egész, azaz $n = hk^2$, ahol $(h, k) = 1$, h és k négyzetmentesek. Legyen α gyöke az $f(x) = x^3 - n$ irreducibilis polinomnak. Ekkor a $K = \mathbb{Q}(\alpha)$ harmadfokú számtest egész bázisa (lásd Marcus [38]):

$$\text{I. eset}: \quad \left\{1, \alpha, \frac{\alpha^2}{k}\right\}, \quad \text{ha} \quad n \not\equiv \pm 1 \pmod 9$$

$$\text{II. eset}: \quad \left\{1, \alpha, \frac{\alpha^2 \pm k^2\alpha + k^2}{3k}\right\}, \quad \text{ha} \quad n \equiv \pm 1 \pmod 9.$$

A két esetnek megfelelően K diszkriminánsa:

$$\begin{aligned} &\text{I. eset}: \quad D_K = -27h^2k^2 \\ &\text{II. eset}: \quad D_K = -3h^2k^2 \end{aligned}$$

Az $\{1, \omega_2, \omega_3\}$ egész bázishoz tartozó indexforma:

$$I(X, Y) = \frac{1}{\sqrt{|D_K|}} \prod_{1 \le i < j \le 3} \left(X\left(\omega_2^{(i)} - \omega_2^{(j)}\right) + Y\left(\omega_3^{(i)} - \omega_3^{(j)}\right)\right)$$

ahol $\omega_i^{(j)}$ az $\omega_i \in K$ elem konjugáltjai ($i = 2, 3,\ j = 1, 2, 3$). A két esetben a szimmetrikus polinomok alaptételének felhasználásával ki tudjuk számítani az indexforma explicit alakját:

$$\text{I. eset}: \quad I(X, Y) = kX^3 - hY^3$$

$$\text{II. eset}: \quad I(X,Y) = 3kX^3 \pm 3k^2X^2Y + k^3XY^2 + \frac{1}{9}(\pm k^4 - h)Y^3$$

A kongruencia tulajdonságok miatt a II. esetben is természetesen egész együtthatós az indexforma.

2.1.1. Az elvégzendő számítások

A dolgozat ezen fejezetének célja harmadfokú gyökbővítésekben a hatvány egész bázisok relatív gyakoriságának és a minimális index változásának leírása a diszkrimináns függvényében.

Adott C korlát esetén a következőképpen határozzuk meg a $|D_K| < C$ tulajdonságú harmadfokú gyökbővítéseket. Vesszük azon $h < k$ relatív prím négyzetmentes pozitív egészeket, melyekre $3\sqrt{3}hk < \sqrt{C}$ (I. eset), vagy $\sqrt{3}hk < \sqrt{C}$ (II. eset), az $n = hk^2$ modulo 9 viselkedésétől függően. ($h > k$-ra ugyanazon testeket kapjuk.)

A dolgozatban a következő számítások eredményeit értékeljük.

A. Kiszámítjuk a hatvány egész bázisok generátorait a

$$|D_K| < 12 \cdot 10^6$$

diszkriminánsú harmadfokú gyökbővítésekben. Ehhez a fenti tulajdonságú 1352 db számtestben megoldjuk az

$$I(x,y) = \pm 1 \quad (x,y \in \mathbb{Z})$$

harmadfokú Thue egyenleteket.

B. Kiszámítjuk a minimális indexű elemeket a

$$|D_K| < 3 \cdot 10^6$$

diszkriminánsú harmadfokú gyökbővítésekben. Ehhez megkeressük a legkisebb olyan pozitív egész m-et, melyre az

$$I(x,y) = \pm m \quad (x,y \in \mathbb{Z})$$

egyenlet megoldható és kiszámítjuk ezek megoldásait. A legkisebb ilyen m lesz a minimális index, a megoldások pedig a minimális indexű

elemeket adják.
Ez 629 darab számtestet jelent, melyekben általában több indexforma egyenletet meg kell oldanunk, mire a minimális indexet megtaláljuk.

A 629 számtestben összesen kb 2000 indexforma egyenlet megoldása szükséges. Ez indokolja, hogy a minimális indexek vizsgálatát kevesebb számtestre végezzük.

A harmadfokú Thue egyenletek megoldását a KASH [6] algebrai számelméleti programcsomaggal végezzük. A legtöbb egyenlet megoldása néhány másodpercig tart.

2.1.2. Hatvány egész bázisok relatív gyakorisága

A hatvány egész bázisok relatív gyakoriságának jellemzéséhez az A. kategóriába eső ($|D_K| < 12 \cdot 10^6$) számtesteket $|D_K|$ szerint sorba rendezzük, majd a számtesteket csoportokra bontjuk úgy, hogy az $[1, 12 \cdot 10^6]$ intervallumot egyenlő részekre osztjuk, és a számtesteket akkor soroljuk egy csoportba, ha diszkriminánsuk abszolút értéke ugyanazon részintervallumba esik. Ezt követően kiszámítjuk az azonos csoportba eső számtestekben a hatvány egész bázisok relatív gyakoriságát, vagyis a hatvány egész bázissal rendelkező csoportbeli számtestek számát osztjuk a csoportbeli számtestek számával. Vizsgáljuk a relatív gyakoriságok tendenciáját.

A következő táblázatban az $[1, 12 \cdot 10^6]$ intervallumot 10 azonosan hosszúságú részre osztjuk fel. A második oszlopban a részintervallumhoz tartozó összes testek száma szerepel.

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 diszkrimináns növekedésével.

2.1.3. A minimális indexek átlagos viselkedése

A minimális indexeket a $|D_K| < 3 \cdot 10^6$ tulajdonságú testekre vizsgáljuk (B.). Ezen számtesteket $|D_K|$ szerint sorba rendezzük. Az $[1, 3 \cdot 10^6]$ intervallumot egyenlő részekre osztjuk. A számtesteket akkor soroljuk egy csoportba, ha diszkriminánsuk abszolút értéke ugyanazon intervallumba esik. Ezt követően kiszámítjuk az azonos csoportba eső számtestekben a minimális indexek átlagát. Vizsgáljuk az átlagok tendenciáját.

A következő táblázatban az $[1, 3 \cdot 10^6]$ intervallumot diszkrimináns szerint 10 egyforma hosszúságú részre osztjuk fel.

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). Ennek oka az, hogy az egész bázisok különböző struktúrája miatt az I. és II. típusú számtestek különbözőféleképpen viselkednek. Ezért célszerű őket külön megvizsgálni.

2.1.4. Az I. és II. eset vizsgálata

Az alább látható táblázatban az $[1, 3 \cdot 10^6]$ intervallumot osztottuk fel 10 részre a diszkriminánsok szerint, és külön vizsgáltuk az I., illetve II. esethez tartozó számtesteket. A táblázatban láthatóak az intervallumok, az adott intervallumba eső számtestek száma, a hatvány egész bázissal rendelkező számtestek relatív gyakorisága, illetve a minimális indexek átlaga.

I. eset

D_K	testek száma	rel gyak	min index
$0 \leq \lvert D_K \rvert < 3 \cdot 10^5$	92	0.62	1.82
$3 \cdot 10^5 \leq \lvert D_K \rvert < 2 \cdot 3 \cdot 10^5$	43	0.56	2.14
$2 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 3 \cdot 3 \cdot 10^5$	30	0.43	3.53
$3 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 4 \cdot 3 \cdot 10^5$	35	0.51	2.26
$4 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 5 \cdot 3 \cdot 10^5$	29	0.41	2.90
$5 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 6 \cdot 3 \cdot 10^5$	26	0.54	2.46
$6 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 7 \cdot 3 \cdot 10^5$	17	0.47	2.94
$7 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 8 \cdot 3 \cdot 10^5$	22	0.45	2.41
$8 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 9 \cdot 3 \cdot 10^5$	14	0.64	2.43
$9 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 3 \cdot 10^6$	25	0.4	3.08

II. eset

D_K	testek száma	rel gyak	min index
$0 \leq \lvert D_K \rvert < 3 \cdot 10^5$	83	0.17	2.81
$3 \cdot 10^5 \leq \lvert D_K \rvert < 2 \cdot 3 \cdot 10^5$	37	0.16	3.30
$2 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 3 \cdot 3 \cdot 10^5$	30	0.17	3.27
$3 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 4 \cdot 3 \cdot 10^5$	25	0.04	4.28
$4 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 5 \cdot 3 \cdot 10^5$	25	0.04	4.44
$5 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 6 \cdot 3 \cdot 10^5$	24	0.04	4.04
$6 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 7 \cdot 3 \cdot 10^5$	20	0	6.30
$7 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 8 \cdot 3 \cdot 10^5$	15	0.13	3.53
$8 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 9 \cdot 3 \cdot 10^5$	19	0.05	4.37
$9 \cdot 3 \cdot 10^5 \leq \lvert D_K \rvert < 3 \cdot 10^6$	18	0.06	5.56

Ezekben a táblázatokban jól megfigyelhető, hogy mennyire különbözik az I., illetve II. eset. *Az I. esetben az egyes relatív gyakoriságok nagyobbak és a minimális indexek átlaga kisebb, mint a II. esetben*, ez összhangban van azzal, hogy az I. esetben az indexforma kiszámításához használt Thue-egyenlet egyszerűbb, mint a II. esetben használt Thue-egyenlet.

2.1.5. Egy érdekes indexforma egyenlet

Ebben a részben azt szemléltetjük, hogy az indexforma egyenletek még ilyen testek esetén is bonyolultak lehetnek.

Legyen $n = 729620$, $h = 5$, $k = 382$ és $D_K = -10944300$. Az indexforma egyenletként az alábbi Thue-egyenletet kapjuk:

$$1146x^3 - 437772x^2y + 55742968xy^2 - 2365979309y^3 = \pm 1 \quad (x, y \in \mathbb{Z}).$$

Megszorozva az egyenletet 1146^2-nel és behelyettesítve $x = x_1/1146$-ot kapjuk az

$$x_1^3 - 437772x_1^2y + 63881441328x_1y^2 - 3107278482178644y^3 = \pm 1313316$$

egyenletet. A $K = \mathbb{Q}(\sqrt[3]{n})$ testet az

$$f(x) = x^3 - 437772x^2 + 63881441328x - 3107278482178644$$

polinom α gyöke generálja. A KASH [6] számításai szerint az $\{1, \alpha, \alpha^2/1146\}$ egész bázis. Az η alapegység együtthatói az egész bázisra vonatkozóan:

$$(-30162380429849338166685586548524287077586628684490115377400266235434667\backslash$$
$$79117346804431700196793325250691306434665191562987243376389437215167037469,$$
$$41352592835814110458946538472304995916562410371066709813866136578737620 9\backslash$$
$$21743789397814487241474004443267737148717341697017371040949980185459,$$
$$-16242939536519220298444101751231295836702001517805039425639564428516371\backslash$$
$$00512970017791331929852412887711551116957146300361999099905860563 3).$$

Három nem-asszociált μ_1, μ_2, μ_3 algebrai egész elem létezik ± 1313316 normával, ezek egész bázisra vonatkozó együtthatói:

$$(34334381069350325160454141144156928995623699439996969083993477034 38,$$
$$-47072401461571907087302882904575551018261769543174307883248091,$$
$$18489630718315727563756003224711034601510766929068014357564 2),$$
$$(29729390657862186190853772851556415545611983878 4,$$
$$-40758964299608219126602418812806302217931 79,$$
$$16009767400033649045655740491199579701228)$$
$$(945780024486523272, -12956701496843, 50853796986).$$

Az alapegységet szintén a KASH [6] algebrai programcsomaggal számoltuk ki, de a μ_1, μ_2, μ_3 kiszámításához szükségünk volt a Magma programcsomag [4] alkalmazására.

Mindezen bonyolult input adatok ellenére a Magma programcsomag gyorsan megoldotta az egyenletet.

2.2. Hatodfokú számtestek másodfokú résztesttel

Másodfokú résztesttel rendelkező hatodfokú testek hatvány egész bázisainak kiszámítása harmadfokú relatív Thue egyenletek megoldására vezet (lásd [23]). Ezek megoldása általában nagyon időigényes feladat, felhasználja a hatodfokú testek alapegységeinek és adott normájú elemeinek ismeretét, melyek kiszámítása önmagában nehézségekbe ütközhet.

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 megoldását.

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].

Korábban Gaál István és M. Pohst [23] vizsgálta képzetes másodfokú résztesttel rendelkező hatodfokú számtestek hatvány egész bázisait. Mivel a fellépő relatív Thue egyenlet teljes megoldása nagyon időigényes volt, csak néhány számtestben határozták meg a hatvány egész bázisokat.

Ezen fejezet célja, hogy a relatív Thue egyenletek "kis" megoldásainak kiszámítására adott [14] módszer felhasználásával ezen számításokat kiterjesszük és a korábbinál jóval több hatodfokú számtestben kiszámítsuk azon hatvány egész bázisok generátorait, melyek egész bázisra vonatkozó koordinátái "kicsik", jellemzően $C = 10^{250}$-nél kisebbek. 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.

A "kis" koordinátájú hatvány egész bázis generátor elemek nagy valószínűséggel teljes megoldást adnak, de biztosan szolgáltatják azon megoldásokat, melyek további gyakorlati számításokra alkalmasak.

2.2.1. Az indexforma egyenlet struktúrája

A most következő fejezetben bemutatjuk, hogyan is vezethető vissza egy másodfokú résztesttel rendelkező hatodfokú test hatvány egész bázisainak kiszámítása harmadfokú relatív Thue egyenlet megoldására.

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] cikkében a diszkrimináns abszolút értéke növekvő sorrendjében kilistázta az első ezer hatodfokú számtestet, melyek valós, illetve melyek képzetes másodfokú résztestekkel rendelkeznek. A 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. Számításainkban csak ilyen testekkel foglalkozunk. Tehát K minden α egész eleme felírható

$$\alpha = x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2, \tag{9}$$

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

Feladatunk tehát az, hogy megoldjuk az

$$I(x_1, x_2, y_0, y_1, y_2) = \pm 1, \quad x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z} \tag{10}$$

indexforma egyenletet, ahol $I(x_1, x_2, y_0, y_1, y_2)$ a fenti egész bázishoz tartozó indexforma.

Jelölje $\vartheta = \vartheta^{(1)}, \vartheta^{(2)}, \vartheta^{(3)}$ a ϑ M feletti konjugáltjait, $\vartheta^{(4)}, \vartheta^{(5)}, \vartheta^{(6)}$ pedig az $\overline{f}(x) = 0$ gyökeit, melyek éppen $\vartheta^{(1)}, \vartheta^{(2)}, \vartheta^{(3)}$ komplex konjugáltjai. Jelölje $\overline{\omega}$ az ω konjugáltját. Legyen $\varrho = -\vartheta^{(1)} - \vartheta^{(2)} = \gamma_2 + \vartheta^{(3)}$. Legyen $\omega^{(i)} = \omega$ $(i = 1, 2, 3)$, $\omega^{(i)} = \overline{\omega}$ $(i = 4, 5, 6)$ és legyenek

$$\alpha^{(i)} = x_0 + x_1\vartheta^{(i)} + x_2(\vartheta^{(i)})^2 + y_0\omega^{(i)} + y_1\omega^{(i)}\vartheta^{(i)} + y_2\omega^{(i)}(\vartheta^{(i)})^2,$$

$(i = 1, \ldots, 6)$ az α konjugáltjai.

Egyszerű számítással adódik, hogy

$$\sqrt{|D_K|} = |(\omega-\overline{\omega})^3| \\ \times|N_{M/\mathbb{Q}}\big((\vartheta^{(1)}-\vartheta^{(2)})(\vartheta^{(2)}-\vartheta^{(3)})(\vartheta^{(3)}-\vartheta^{(1)})\big)|.$$

Tegyük fel, hogy egy (9) formában felírt α a K egy hatvány egész bázisát generálja. Ekkor

$$I(\alpha) = \frac{\big|\prod_{1\le j<k\le 6}(\alpha^{(j)}-\alpha^{(k)})\big|}{\sqrt{|D_K|}} = \pm 1. \tag{11}$$

Nyilvánvalóan igaz $(j,k) = (1,2),(2,3),(1,3)$ esetén, hogy

$$\alpha^{(j)}-\alpha^{(k)} = (\vartheta^{(j)}-\vartheta^{(k)})\big((x_1+\omega y_1)+(\vartheta^{(j)}+\vartheta^{(k)})(x_2+\omega y_2)\big),$$

illetve $(j,k) = (4,5),(5,6),(4,6)$ esetén, hogy

$$\alpha^{(j)}-\alpha^{(k)} = (\vartheta^{(j)}-\vartheta^{(k)})\big((x_1+\overline{\omega} y_1)+(\vartheta^{(j)}+\vartheta^{(k)})(x_2+\overline{\omega} y_2)\big).$$

Emiatt $(j,k) = (1,2),(2,3),(1,3),(4,5),(5,6),(4,6)$ választás mellett az $|\alpha^{(j)}-\alpha^{(k)}|$ tényezők szorzata egyenlő az alábbi kifejezéssel:

$$\Big|N_{M/\mathbb{Q}}\big((\vartheta^{(1)}-\vartheta^{(2)})(\vartheta^{(2)}-\vartheta^{(3)})(\vartheta^{(3)}-\vartheta^{(1)})\big)\Big| \\ \times\Big|N_{K/\mathbb{Q}}\big((x_1+\omega y_1)-\varrho(x_2+\omega y_2)\big)\Big|.$$

Ezt beírva a (11) kifejezésbe és beosztva $\sqrt{|D_K|}$-val, az első faktor kiesik. A második faktor egy egész együtthatós polinom, így osztja $I(\alpha)$-t $\mathbb{Z}[x_1,x_2,y_0,y_1,y_2]$-ben.

Jelölje $F(x_1,x_2,y_0,y_1,y_2)$ a megmaradó kilenc $|\alpha^{(j)}-\alpha^{(k)}|$ tényező szorzatát osztva $|(\omega-\overline{\omega})^3|$-tal. Tehát $I(\alpha)$ egyenlő $N_{K/\mathbb{Q}}\big((x_1+\omega y_1)-\varrho(x_2+\omega y_2)\big)$ és $F(x_1,x_2,y_0,y_1,y_2)$ szorzatával. És mivel ez utóbbi egész együtthatós polinom, ezért F egy y_0-ban 9-edfokú racionális együtthatós polinom. Tehát, ha tudjuk, hogy $I(\alpha) = 1$, akkor következésképpen

$$N_{K/\mathbb{Q}}\big((x_1+\omega y_1)-\varrho(x_2+\omega y_2)\big) = \pm 1 \quad (x_1,x_2,y_1,y_2\in\mathbb{Z})$$

és

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

Tehát kimondható, hogy a (9) formában felírt α pontosan akkor generálja K egy hatvány egész bázisát (azaz $(x_1, x_2, y_0, y_1, y_2)$ egy megoldása a (10) egyenletnek), ha $X = x_1 + \omega y_1$, $Y = x_2 + \omega y_2$ kielégíti az

$$N_{K/M}(X - \varrho Y) = \nu \quad (X, Y \in \mathbb{Z}_M) \tag{12}$$

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

$$F(x_1, x_2, y_0, y_1, y_2) = \pm 1, \quad (x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}). \tag{13}$$

2.2.2. Hatodfokú számtestek képzetes másodfokú résztesttel

Ebben a fejezetben feltételezzük, hogy M komplex másodfokú test. Számításaink M. Olivier [41] cikkében lévő adatokon alapszanak.

Gaál István és M. Pohst [23] meghatározták az első 25 darab ilyen számtest esetén a hatvány egész bázisok generátorait. A fejezet célja, hogy a relatív Thue egyenletek "kis" megoldásaira vonatkozó [14] gyors algoritmus felhasználásával vizsgálatainkat kiterjesszük az első 100 ilyen típusú testre, meghatározva azon hatvány egész bázisok generátorait, melyek egész bázisra vonatkozó koordinátái 10^{250}-nél kisebbek.

A [41] táblázatában adva van a hatodfokú K test D_K diszkriminánsa, az M képzetes másodfokú résztest D_M diszkriminánsa és a K test M feletti ϑ generátorának harmadfokú $f(x)$ minimálpolinomja.

Legyen $C = 10^{250}$. Célunk a K hatodfokú test azon (9) alakú α elemeinek a meghatározása, melyek hatvány egész bázist generálnak és

$$max(|x_1|, |x_2|, |y_0|, |y_1|, |y_2|) < C. \tag{14}$$

Ehhez először meg kell határoznunk x_1, x_2, y_1, y_2-t (12) egyenletből. Abban az esetben, ha M képzetes másodfokú résztest, ezen egyenlet jobb oldalán csak véges sok egység léphet fel. A számítást minden

ilyen egységre elvégezzük. Ezt követően (12) minden x_1, x_2, y_1, y_2 megoldásához meghatározzuk y_0-t (13)-ból ($x_0 \in \mathbb{Z}$ tetszőleges).

Amíg [23]-ban az átlagos számítási idő 20 perc volt számtestenként, addig jelen algoritmusunk 1-2 percig futott számtestenként. Ezzel csak a (14) tulajdonságú "kis" megoldásokat kapjuk meg, de számításainkat 100 számtestre könnyen ki tudtuk terjeszteni, és tapasztalataink szerint ilyen jellegű problémák csak "kis" megoldásokkal rendelkeznek.

Számításaink eredményei a Függelék 4.2. Fejezetében láthatóak.

A megoldásaink listája tartalmazza nagy valószínűséggel az összes megoldást, de biztosan az összeset, mely még gyakorlati számításokhoz használható.

2.2.3. Hatodfokú számtestek valós másodfokú résztesttel

Ebben a fejezetben azon hatodfokú számtestek hatvány egész bázisait vizsgáljuk, melyek valós másodfokú résztesttel rendelkeznek (ezen eredmények publikálását későbbre tervezzük). Ezen számításokhoz ismét segítségül hívtuk M.Olivier [41] cikkét. Az előző esethez hasonlóban a táblázatában adva van a hatodfokú K test D_K diszkriminánsa, az M valós másodfokú résztest D_M diszkriminánsa és a K test M feletti ϑ generátorának a harmadfokú $f(x)$ minimálpolinomja.

Legyen $C = 10^{250}$. Célunk a K hatodfokú test azon (9) alakú α elemeinek a meghatározása, melyek hatvány egész bázist generálnak és

$$max(|x_1|, |x_2|, |y_0|, |y_1|, |y_2|) < C. \tag{15}$$

Ehhez újra a (12), (13) egyenletek (15)-t kielégítő megoldásait kell megkeresnünk.

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:

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

ahol ε az M valós másodfokú résztest alapegysége, $k \in \mathbb{Z}$. Legyen $k = 3m+r$, ahol $m, r \in \mathbb{Z}$, $r \in \{-1, 0, 1\}$. Az egyenlet mindkét oldalát ε^{3m}-nel osztva, $X_0 = \varepsilon^{-m}X$, $Y_0 = \varepsilon^{-m}Y$ helyettesítéssel az

$$N_{K/M}(X_0 - \varrho Y_0) = \pm\varepsilon^r, \quad (X_0, Y_0 \in \mathbb{Z}_M) \tag{16}$$

egyenlet adódik. A $max(|x_1|, |x_2|, |y_1|, |y_2|) < C$ korlát felhasználásával a fenti egyenletből korlátot nyerhetünk $|k|$-ra, abból korlát adódik $|m|$-re. Ezen $|m|$-re vonatkozó korlátot használjuk fel arra, hogy korlátot vezessünk le X_0, Y_0 méretére. Legyen

$$X_0 = x_{01} + y_{01}\omega$$
$$Y_0 = x_{02} + y_{02}\omega,$$

ahol $x_{01}, x_{02}, y_{01}, y_{02} \in \mathbb{Z}$. Az $|\overline{X_0}|, |\overline{Y_0}|$-re kapott felső korlátból felső becslést vezethetünk le $x_{01}, x_{02}, y_{01}, y_{02}$ abszolút értékeire:

$$max(|x_{01}|, |x_{02}|, |y_{01}|, |y_{02}|) < C'.$$

A [14]-ben adott gyors algoritmussal meghatározzuk (16) fenti tulajdonságú megoldásait. Végül, minden szóba jöhető m-re meghatározzuk X, Y komponenseit:

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

ahol $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. Minden (X_0, Y_0) esetén, minden m-re ezen x_1, x_2, y_1, y_2-höz megvizsgáljuk, hogy a (13) egyenletnek van-e megfelelő $y_0 \in \mathbb{Z}$ megoldása.

A relatív Thue egyenletek "kis" megoldásainak meghatározásánál [14] szerint a megoldások abszolút értékeire előre adott korlátot redukálnunk kell. Ahogy [14]-ben látható néhány példán keresztül, valós másodfokú résztesttel rendelkező számtestek esetében ezen redukció kevésbé hatékony, mint komplex másodfokú résztest esetében. Ezért ezen számtestek esetében a számítások számtestenként lényegesen több időt vettek igénybe, bizonyos esetekben néhány órát is. A függelékben található eredmények listája ezért is szűkebb.

Számításaink eredményeit a Függelék 4.3. Fejezete tartalmazza.

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.

A megoldás módszere Gaál István, Pethő Attila és M. Pohst [20] tételén, a relatív esetben Gaál István és M. Pohst [25] tételén alapul. A [25]-ben bebizonyított tétel a [20]-ban 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).

3.1. Hatvány egész bázisok negyedfokú bikvadratikus testek végtelen parametrikus családjaiban

Felhasználva a K.S. Williams [43] által megadott egész bázist, meg lehet konstruálni a $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ alakú *biciklikus bikvadratikus* negyedfokú számtestekben az indexforma egyenletet. Ez tette lehetővé, hogy ilyen típusú testek esetén a testindexeket teljesen jellemezni lehessen [19] és hasonló testek esetében általános módszer szülessen az indexforma egyenlet megoldására [21]. Teljesen komplex esetben Nyul Gábor [40] 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 [35] nemrég megadták a fentieknél általánosabb $\mathbb{Q}(\sqrt{a + b\sqrt{c}})$ 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. Bár a szerzők megadtak egy olyan elemet, mely hatvány egész bázist generál, de nem igazolták, hogy más (nem ekvivalens) hatvány egész bázist generáló elemek nem léteznek.

Ebben a fejezetben megoldottuk az indexforma egyenletet negyedfokú számtestek ezen két végtelen parametrikus családjában és megmutattuk, hogy a [35]-ben megadottakon kívül nincs más hatvány egész bázis ezekben a testekben. Ez az első olyan eredmény, amikor számtestek *két paraméter*től függő végtelen családjában sikerül megoldani az indexforma egyenletet. Eredményünk ráadásul lezáró jellegű eredmény abban az értelemben, hogy teljesen megválaszolja az adott testekben a hatvány egész bázisok meghatározásának kérdését.

3.1.1. Eredmények

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

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

illetve

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

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.

3.1.2. Segédtételek

Gaál István, Pethő Attila és M. Pohst [20] megmutatták, hogy az indexforma egyenlet megoldása negyedfokú testekben visszavezethető egy harmadfokú egyenletre (mely irreducibilis esetben Thue egyenlet) és néhány hozzá kapcsolódó negyedfokú Thue egyenletre.

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. Legyen

$$F(U, V) = U^3 - a_2U^2V + (a_1a_3 - 4a_4)UV^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)V^3,$$

$$\begin{aligned} Q_1(X, Y, Z) &= X^2 - XYa_1 + Y^2a_2 + XZ(a_1^2 - 2a_2) + YZ(a_3 - a_1a_2) \\ &\quad + Z^2(-a_1a_3 + a_2^2 + a_4), \end{aligned}$$

$$Q_2(X, Y, Z) = Y^2 - XZ - a_1YZ + Z^2a_2.$$

Alkalmazzuk [20] eredményét $\mathbb{Z}[\xi]$ rendjére, mivel esetünkben éppen ez az egészek gyűrűje.

2. Lemma (Gaál I., Pethő A. és M. Pohst [20]). *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 olyan $(u, v) \in \mathbb{Z}^2$ megoldása az*

$$F(u, v) = \pm 1 \tag{17}$$

harmadfokú Thue egyenletnek, hogy (x, y, z) kielégíti a

$$\begin{aligned} Q_1(x, y, z) &= u, \\ Q_2(x, y, z) &= v \end{aligned} \tag{18}$$

egyenleteket.

Gaál István, Pethő Attila és M. Pohst [22] cikkében ki van dolgozva egy általános módszer (18) típusú kvadratikus forma egyenletrendszerek megoldására. Ezen egyenletrendszerek negyedfokú Thue egyenletek megoldására vezethetők vissza. Teljesen komplex negyedfokú számtestek esetén a (18) rendszerből egy pozitív definit kvadratikus forma konstruálható (lásd [22]).

3. Lemma (Gaál I. [11]). *Legyen K teljesen komplex negyedfokú test. Ekkor az $R(x) = F(x,1)$ polinomnak három különböző valós gyöke van, $\lambda_1 < \lambda_2 < \lambda_3$. 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 $\lambda \in (-\lambda_2, -\lambda_1)$.

3.1.3. Bizonyítás

1. Tétel bizonyítása

I. Tudjuk, hogy ha $c \equiv 1 \pmod 4$, akkor $g_k = 4k+3, h_k = 2$. 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 2. Lemma jelöléseit használva kapjuk, hogy $a_1 = -2, a_2 = -2k, a_3 = 2k+1, a_4 = k^2 + k - \ell$. Ekkor a (17) egyenlet az alábbi alakú:

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

Innen 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

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

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

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

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 $v = -g_k/c$-t, amennyiben ez utóbbi egész. Ekkor az egyenletrendszer lehetséges megoldáspárjai: $(u, v) = (\pm 1, 0), ((2k + 1)g_k/c - 1, -g_k/c)$.

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

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

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 2. Lemmabeli kvadratikus formák:

$$\begin{aligned} Q_1(X, Y, Z) &= X^2 + 2XY - 2Y^2k + XZ(4 + 4k) + YZ(-2k + 1) \\ &\quad + Z^2(5k + 2 + 5k^2 - \ell), \\ Q_2(X, Y, Z) &= Y^2 - XZ + 2YZ - 2Z^2k. \end{aligned}$$

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 $\lambda = 2k+1+\varepsilon$ választható, tetszőleges kicsi pozitív ε-nal. Kapjuk, hogy a hatvány egész bázist generáló α elem $x, y, z \in \mathbb{Z}$ koordinátáira

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

tehát

$$\left(x + y + z\left(\frac{3}{2} + k - \frac{\varepsilon}{2}\right)\right)^2 + \varepsilon\left(y + \frac{3z}{2}\right)^2 + z^2\left(-\ell - \frac{1}{4} - \varepsilon k - \frac{3\varepsilon}{4} - \frac{\varepsilon^2}{4}\right) = u + \lambda v, \tag{19}$$

ahol $u + \lambda v$ vagy 1 vagy $1 + \varepsilon g_k/c$ vagy $-1 - \varepsilon g_k/c$, 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 (19)-ban nagyobb, mint 1, amiből kapjuk, hogy $z = 0$ és ekkor (19) 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 $u + \lambda v = 1 + \varepsilon g_k/c$, akkor $\ell < -1$ választással kellően kicsi ε-ra kapjuk, hogy $0.9 < 1 + \varepsilon g_k/c < 1$. z^2 együtthatója (19)-ben nagyobb, mint 1, amiből kapjuk, hogy $z = 0$. A (19) egyenlet ekkor az alábbi alakú:

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

tehát

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

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

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

ami lehetetlen, ha például ε irracionális.

Következésképpen csak $(x, y, z) = (\pm 1, 0, 0)$ megoldás, tehát csak ϑ generál hatvány egész bázist. $\square$

2. Tétel bizonyítása

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

$$f(X) = X^4 - 2g_k X^2 + g_k^2 - c.$$

Az 2. Lemma jelöléseivel most $a_1 = 0, a_2 = -2g_k, a_3 = 0, a_4 = g_k^2 - c$. A (17) harmadfokú egyenlet az alábbi alakú:

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

ami a következő egyenletrendszert jelenti:

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

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 $v = g_k/c$. Ha $c \equiv 2 \pmod 4$, akkor g_k páratlan, ha $c \equiv 3 \pmod 4$, akkor g_k páros, ezért $v = g_k/c$ nem egész.

Ha $i_1 = -1, i_2 = 1$, akkor lehetséges megoldásként kapjuk, hogy $v = 0$ vagy $v = -g_k/c$, 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

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

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

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

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

$$\begin{aligned} Q_1(X,Y,Z) &= X^2 - 2Y^2 g_k + 4XZg_k + Z^2(5g_k^2 - c), \\ Q_2(X,Y,Z) &= Y^2 - XZ - 2Z^2 g_k. \end{aligned}$$

A pozitív definit kvadratikus forma megkonstruálásához λ-t a következőképpen kell megválasztanunk: $\lambda \in (-\lambda_2, -\lambda_1) = (-x_1, -x_2) = (2g_k, 2g_k + \rho_2)$. Újra legyen $\lambda = 2g_k + \varepsilon$, tetszőleges kicsi pozitív ε-nal. Ha a tételbeli α elem hatvány egész bázist generál, akkor $x, y, z \in \mathbb{Z}$ koordinátáira fennáll

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

tehát

$$\left(x + z\left(g_k - \frac{\varepsilon}{2}\right)\right)^2 + \varepsilon y^2 + z^2\left(-c - \varepsilon g_k - \frac{\varepsilon^2}{4}\right) = u + \lambda v, \qquad (20)$$

ahol $u + \lambda v = 1$.

IV. Ha $u + \lambda v = 1$, akkor $c < 0$ mellett z^2 együtthatója (20)-ben nagyobb, mint 1, kellően kicsi ε esetén, ahonnan kapjuk, hogy $z = 0$ és (20) 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 csak $(x, y, z) = (\pm 1, 0, 0)$ megoldás, tehát ϑ az egyetlen generátora a hatvány egész bázisnak. □

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, ξ negyedfokú elem M felett és legyen és $K = M(\xi)$ az M relatív negyedfokú bővítése (tehát K nyolcadfokú). Célunk először is az, hogy meghatározzuk a relatív hatvány egész bázisát $\mathcal{O} = \mathbb{Z}_K$-nak $\mathbb{Z}_M$ 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 hatvány egész bázis generátor, de érdekes és fontos kérdés annak eldöntése, hogy van-e más olyan elem $Z_M[\xi]$-ben, ami hatvány egész bázist generál. Ezt követően ezeket az eredményeket felhasználva meghatározzuk az abszolút hatvány egész bázisokat.

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

A dolgozat ezen fejezetében szereplő tételek és bizonyításuk a [31], illetve a [27] cikkekben szerepelnek.

3.2.1. Eredmények

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 bázisainak 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 bázisainak 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.*

3.2.2. Segédtételek

A fő eszköz, amelyet a relatív hatvány egész bázisok kiszámításához alkalmazni fogunk, Gaál István és Michael Pohst [25] cikkének módszere, amit alább részletezünk. Ez a módszer az indexforma egyenletet visszavezeti egy relatív harmadfokú egyenletre (mely irreducibilis esetben Thue egyenlet) és néhány relatív negyedfokú Thue egyenletre.

Legyen K egy negyedfokú bővítése az m-edfokú M számtestnek, melyet ξ generál. Legyen ξ relatív minimálpolinomja M felett $f(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4 \in \mathbb{Z}_M[X]$. Legyen $\mathcal{O} = \mathbb{Z}_K$ vagy $\mathcal{O} = \mathbb{Z}_M[\xi]$. Ekkor minden $\alpha \in \mathcal{O}$ elem egyértelműen felírható

$$\alpha = \frac{1}{d}\left(a + x\xi + y\xi^2 + z\xi^3\right) \tag{21}$$

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

$$F(U,V) = U^3 - a_2U^2V + (a_1a_3 - 4a_4)UV^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)V^3$$

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

$$\begin{aligned} Q_1(X,Y,Z) &= X^2 - XYa_1 + Y^2a_2 + XZ(a_1^2 - 2a_2) \\ &\quad + YZ(a_3 - a_1a_2) + Z^2(-a_1a_3 + a_2^2 + a_4) \\ Q_2(X,Y,Z) &= Y^2 - XZ - a_1YZ + Z^2a_2 \end{aligned}$$

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

4. Lemma (Gaál I. és M. Pohst [25]). *Ha α (21)-beli alakú és kielégíti az*

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

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

$$N_{M/\mathbb{Q}}(F(u,v)) = \pm\frac{d^{6m}}{i_0} \tag{22}$$

egyenletnek, melyre

$$\begin{aligned} u &= Q_1(x,y,z), \\ v &= Q_2(x,y,z). \end{aligned} \tag{23}$$

A (22) egy ismert u, v megoldása esetén meg kell oldanunk a (23) egyenletrendszert. Erre a célra L.J.Mordell [39] módszerét használjuk, azaz paraméterezzük a $Q_0(x,y,z) = uQ_2(x,y,z) - vQ_1(x,y,z) = 0$ kvadratikus forma egyenlet megoldásait. Ezen módszereket részletesen leírjuk a bizonyításunkban. Láthatólag a 4. Lemma formailag szinte teljes analógiában van az 2. Lemmával. A relatív eset azonban számos technikai problémát vet fel a 4. Lemma alkalmazása közben.

Végezetül, ahhoz, hogy meg tudjuk határozni $\mathcal{O}$-ban az összes (abszolút) hatvány egész bázis generátort, az alábbi lépéseket kell követnünk (lásd 1.1. Fejezetben (7), (8)):

I. Lépés *Ekvivalencia erejéig meghatározunk minden $\alpha_0 \in \mathcal{O}$ hatvány egész bázis generátort $\mathcal{O}$-ban M felett.*
Más szóval, meghatározunk minden 1 realtív indexű $\alpha_0 \in \mathcal{O}$-t:

$$I_{\mathcal{O}/M}(\alpha_0) = 1.$$

Megjegyezzük, hogy ha α_0 relatív indexe 1, akkor α minden (8) formában adott ekvivalensének is 1 a relatív indexe.

Az 1.1. Fejezet 1. Állítása szerint ha $\alpha \in \mathcal{O}$ hatvány egész bázist generál, akkor

$$\alpha = A + \varepsilon\alpha_0,$$

ahol α_0 a fenti, $A \in \mathbb{Z}_M$ és ε egység M-ben.

II. Lépés *Határozzuk meg ε és A értékét úgy, hogy*

$$J(\alpha) = 1$$

legyen.
Legyen $\mu_1 = 1, \mu_2, \ldots, \mu_m$ egy egész bázisa M-nek (esetünkben M másodfokú). Ekkor a fenti A az alábbi alakban írható:

$$A = a_1 + a_2\mu_2 + \ldots + a_m\mu_m, \tag{24}$$

ahol $a_1, \ldots, a_m \in \mathbb{Z}$.

Mivel az (abszolút) index invariáns a ± 1-gyel való szorzásra és $\mathbb{Z}$-beli elemmel való eltolásra, ezért az $a_2, \ldots, a_m$ (24)-beli értékeket elegendő előjeltől eltekintve meghatározni. A II. Lépés azt jelenti, hogy

kiszámítjuk azon ε és $a_2, \ldots, a_m$ értékeket, melyek teljesítik a $J(\alpha) = 1$ feltételt. A (6) értelmében ez azt jelenti, hogy meg kell oldanunk egy $n^2m(m-1)/2$ fokú egyenletet, mely függ ε-tól és $a_2, \ldots, a_m$-től.

Ez általában nagyon komplikált lehet. Azonban, ha M egy képzetes másodfokú számtest, akkor csak véges sok ε egység van M-ben és a_2-ben egyváltozós polinomegyenletet kapunk.

3.2.3. Bizonyítás

A fejezet első felében ismertetjük a relatív hatvány egész bázisokra vonatkozó eredmények bizonyítását, majd a későbbiekben az abszolút hatvány egész bázisokra vonatkozó eredményekét.

3. Tétel bizonyítása

A 4. Lemmába behelyettesítjük az $a_1 = 0,\ a_2 = -t^2,\ a_3 = 0,\ a_4 = 1$ értékeket. A (22) egyenlet az alábbi alakot veszi fel:

$$F(u,v) = (u-2v)(u+2v)(u+t^2v) = \varepsilon \quad (u,v \in \mathbb{Z}_M),$$

ahol $\varepsilon \in \mathbb{Z}_M$ egység. Ezért $F(u,v)$ minden tényezőjének szintén egységnek kell lennie $\mathbb{Z}_M$-ben, amelyből következik, hogy $v = 0$ és u egység $\mathbb{Z}_M$-ben.

Legyenek $x, y, z \in \mathbb{Z}_M$ a (21)-beli relatív hatvány egész bázist generáló α elem koordinátái. Akkor akkor

$$Q_0(x,y,z) = uQ_2(x,y,z) - vQ_1(x,y,z) = 0,$$

tehát

$$y^2 - xz - z^2t^2 = 0. \tag{25}$$

Ennek egy nem triviális megoldása: $x_0 = -t^2, y_0 = 0, z_0 = 1$. Ezért a (25) megoldása paraméterezhető az alábbi alakban:

$$\begin{aligned} x &= -t^2r + p \\ y &= q \\ z &= r, \end{aligned} \tag{26}$$

ahol $p, q, r \in M, r \neq 0$ (lásd [39], [25]). Ezt a kifejezést behelyettesítve (25)-be $rp = q^2$ adódik. Megszorozzuk a (26) minden egyenletét p-vel és rp-t helyettesítjük q^2-tel, így

$$\begin{aligned} kx &= -t^2q^2 + p^2 \\ ky &= pq \\ kz &= q^2, \end{aligned} \tag{27}$$

ahol $k \in M$. Ha $\mathbb{Z}_M$-ben van egyértelmű faktorizáció, beszorozzuk ezeket az egyenleteket p, q közös nevezőjének négyzetével és osztjuk őket p, q legnagyobb közös osztójának négyzetével. Ilyen módon a k, p, q paramétereket helyettesíteni tudjuk $\mathbb{Z}_M$-beli paraméterekkel. (Megjegyezzük, hogy ha $\mathbb{Z}_M$-ben nincs egyértelmű faktorizáció, akkor ugyanezt az érvelést használjuk $\mathbb{Z}_M$ ideáljainak bevonásával. A részletes eljárás megtalálható [25]-ben.)

[25] szerint k-nak osztania kell a kx, ky, kz (27)-beli előállításában a p^2, pq, q^2 együtthatóiból álló mátrix determinánsát. Innen következik, hogy k-nak is egységnek kell lennie (lásd [25]). Végül, a (27)-beli alakot $Q_1(x, y, z) = u$-ba helyettesítve adódik

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

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

Felhasználva V. Ziegler [44]-beli 2. Tételét le tudjuk írni ezen relatív negyedfokú Thue egyenletnek a megoldásait. Ezeket az alábbi táblázat tartalmazza (ahol $\omega_3 = (1 + i\sqrt{3})/2$):

p	q	k^2u		p	q	k^2u
0	1	1		$1-\omega_3$	$(1-\omega_3)t$	$\omega_3 - 1$
0	-1	1		$1-\omega_3$	$(\omega_3-1)t$	$\omega_3 - 1$
0	i	1		$\omega_3 - 1$	0	$\omega_3 - 1$
0	$-i$	1		$\omega_3 - 1$	$(1-\omega_3)t$	$\omega_3 - 1$
0	ω_3	$-\omega_3$		$\omega_3 - 1$	$(\omega_3-1)t$	$\omega_3 - 1$
0	$-\omega_3$	$-\omega_3$		$-\omega_3$	0	$-\omega_3$
0	$1-\omega_3$	$\omega_3 - 1$		$-\omega_3$	$\omega_3 t$	$-\omega_3$
0	$\omega_3 - 1$	$\omega_3 - 1$		$-\omega_3$	$-\omega_3 t$	$-\omega_3$
1	0	1		t	1	1

1	t	1		t	-1	1
1	$-t$	1		$-t$	1	1
-1	0	1		$-t$	-1	1
-1	t	1		it	i	1
-1	$-t$	1		it	$-i$	1
i	0	1		$-it$	i	1
i	it	1		$-it$	$-i$	1
i	$-it$	1		$\omega_3 t$	ω_3	$-\omega_3$
$-i$	0	1		$\omega_3 t$	$-\omega_3$	$-\omega_3$
$-i$	it	1		$(1-\omega_3)t$	$1-\omega_3$	ω_3-1
$-i$	$-it$	1		$(1-\omega_3)t$	ω_3-1	ω_3-1
ω_3	0	$-\omega$		$(\omega-1)t$	$1-\omega$	$\omega-1$
ω_3	$\omega_3 t$	$-\omega_3$		$(\omega_3-1)t$	ω_3-1	ω_3-1
ω_3	$-\omega_3 t$	$-\omega_3$		$-\omega_3 t$	ω_3	$-\omega_3$
$1-\omega_3$	0	ω_3-1		$-\omega_3 t$	$-\omega_3$	$-\omega_3$

A (p,q) megoldásokból (27) alapján ki tudjuk számolni x,y,z-t, amely a 3. Tétel bizonyítását adja. Megjegyezzük, hogy V. Ziegler [44]-beli tétele $|t|^2 > 245$-re érvényes. $\square$

5. Tétel bizonyítása

A 4. Lemmába behelyettesítjük az $a_1 = -4t,\ a_2 = 6t+2,\ a_3 = 4t,\ a_4 = 1$ értékeket. A (22) egyenlet az alábbi alakot veszi fel:

$$F(u,v) = (u+2v)(u-(2-2t)v)(u-(2+8t)v) = \varepsilon \quad (u,v \in \mathbb{Z}_M),$$

ahol $\varepsilon \in \mathbb{Z}_M$ egység. Ezért $F(u,v)$ minden tényezőjének szintén egységnek kell lennie $\mathbb{Z}_M$-ben, amelyből következik, hogy $v = 0$ és u egy egység $\mathbb{Z}_M$-ben.

Legyen újra $x,y,z \in \mathbb{Z}_M$ a (21)-beli relatív hatvány egész bázist generáló α elem koordinátái. Akkor akkor

$$Q_0(x,y,z) = uQ_2(x,y,z) - vQ_1(x,y,z) = 0,$$

tehát

$$y^2 - xz + 4tyz + (6t+2)z^2 = 0. \tag{28}$$

Ennek egy nem triviális megoldása $x_0 = 6t+2, y_0 = 0, z_0 = 1$. Ezért a (28) megoldása paraméterezhető az alábbi alakban:

$$\begin{aligned} x &= (6t+2)r + p \\ y &= q \\ z &= r, \end{aligned} \tag{29}$$

ahol $p, q, r \in M, r \neq 0$. Ezt a kifejezést behelyettesítve (28)-be $q^2 = r(p-4tq)$ adódik. Megszorozzuk a (29) minden egyenletét $p-4tq$-val és $r(p-4tq)$-t helyettesítjük q^2-tel, így

$$\begin{aligned} kx &= p^2 - 4tpq + (6t+2)q^2 \\ ky &= pq - 4tq^2 \\ kz &= q^2, \end{aligned} \tag{30}$$

ahol $k \in M$. Hasonlóképpen, mint a 3. Tétel bizonyításában, a k, p, q paramétereket helyettesítjük $\mathbb{Z}_M$-beli paraméterekkel. Ismét kapjuk, hogy k-nak egységnek kell lennie. Végül, a (30)-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, $Q_2(x, y, z) = v$ mindkét oldala ismét eltűnik.)

Használva B. Jadrijević és V. Ziegler [36]-beli 2. Tételét le tudjuk írni ezen relatív negyedfokú Thue egyenletnek a megoldásait, melyek: $(p, q) \in \{(0, \pm 1), (\pm 1, 0)\}$. A (p, q) megoldásokból (30) alapján kapjuk x, y, z-re a lehetséges megoldásokat, amely az 5. Tétel bizonyítását adja. Megjegyezzük, hogy B. Jadrijević és V. Ziegler [36]-beli eredménye $|t| > 1544803$-ra érvényes. □

4. Tétel bizonyítása

Jelölje α_0 a relatív hatvány egész bázis egy lehetséges generátorát $\mathcal{O}$-ban $\mathbb{Z}_M$ felett, legyen ez most például

$$\alpha_0 = (1 - t^4)\xi + t\xi^2 + t^2\xi^3,$$

ahol $t = t_1 + t_2 i\sqrt{d}$ a paraméter $(t_1, t_2 \in \mathbb{Z})$. Megjegyezzük, hogy mivel a ξ elem $\mathbb{Z}_M$ feletti minimálpolinomja függ a $t \in \mathbb{Z}_M$ paramétertől,

ezért ξ függ t-től és d-től is. Legyen $\varepsilon = \pm 1$ és írjuk fel α-t az alábbi formában

$$\alpha = a_1 + a_2 i\sqrt{d} + \varepsilon\alpha_0,$$

ahol $a_1, a_2 \in \mathbb{Z}$. Ezután kiszámítjuk $J(\alpha)$ értékét. Ez egy nagyon bonyolult 16-odfokú polinom, mely nem csak az a_2-től függ, de függ t_1, t_2, d értékektől is. Szimmetrikus polinomok használatával és a formula egyszerűsítésével kapjuk, hogy $J(\alpha)$ osztható 16-tal. Ezért nincs $\mathcal{O}$-nak α_0-hoz tartozó hatvány egész bázisa. A bizonyítás a megmaradt α_0 jelöltek esetén is hasonlóan megy, illetve a II. család esetén is ugyanezeket a számításokat kell elvégeznünk és hasonló eredményre jutunk. A Maple számítások 10-60 másodpercet vettek igénybe esetenként. □

6. Tétel bizonyítása

A bizonyítás hasonlóan végezhető el, mint a 4. Tétel bizonyítása. □

4. Függelék

4.1. Harmadfokú gyökbővítések minimális indexű elemeinek listája

Az alábbi táblázatban összefoglaljuk a harmadfokú gyökbővítések alapvető adatait $|D_K| \leq 118803$ diszkriminánsig.

Táblázatunkban szerepel D_K, az I. ill. II. eset jelzése (az egyszerűség kedvéért arab számmal), n, h, k értékei, a minimális index m_K értéke, valamint a minimális indexű elemek (x, y) koordinátái. Ennek megfelelően a minimális indexű elemek

$$\alpha = \pm(a + x\omega_2 + y\omega_3)$$

alakúak, ahol $a \in \mathbb{Z}$, $\{1, \omega_2, \omega_3\}$ az egész bázis (az I. ill. II. eseteknek megfelelően), és (x, y) az utolsó oszlopbeli számpárok.

D_K	eset	n	h	k	m_K	(x, y)
-108	1	4	1	2	1	$(0,-1),(1,1)$
-243	1	9	1	3	1	$(0,-1)$
-300	2	100	1	10	1	$(-3,1)$
-588	2	98	2	7	1	$(-5,-2),(-2,-1)$
-675	1	25	1	5	1	$(0,-1)$
-867	2	289	1	17	1	$(-11,2)$
-972	1	36	1	6	1	$(0,-1)$
-972	1	18	2	3	1	$(1,1)$
-1083	2	361	1	19	2	$(-6,1)$
-1323	1	49	1	7	1	$(-1,-2),(0,-1)$
-1452	2	242	2	11	1	$(4,1)$
-2028	2	676	1	26	2	$(-17,2)$
-2700	1	50	2	5	2	$(0,-1),(14,19)$
-3267	1	121	1	11	1	$(0,-1)$
-3675	2	1225	1	35	3	$(-23,2),(35,-3)$
-4107	2	1369	1	37	3	$(37,-3),(49,-4),(367,-30)$

-4563	1	169	1	13	1	$(0,-1)$
-5292	1	196	1	14	1	$(0,-1)$
-6075	1	225	1	15	1	$(0,-1)$
-6075	1	75	3	5	2	$(1,1)$
-6348	2	2116	1	46	2	$(61,-4)$
-8427	2	2809	1	53	3	$(53,-3)$
-9075	2	3025	1	55	1	$(73,-4)$
-10092	2	1682	2	29	2	$(-49,-5)$
-11532	2	3844	1	62	3	$(62,-3)$
-11907	1	441	1	21	1	$(0,-1)$
-11907	1	147	3	7	3	$(-3,-4),(0,-1)$
-12675	2	845	5	13	2	$(-4,-1)$
-13068	1	484	1	22	1	$(0,-1)$
-14283	1	529	1	23	1	$(0,-1)$
-14700	2	980	5	14	1	$(5,1)$
-15123	2	5041	1	71	3	$(71,-3)$
-15987	2	5329	1	73	1	$(-97,4)$
-17787	2	847	7	11	2	$(4,-1)$
-18252	1	338	2	13	2	$(0,-1)$
-20172	2	6724	1	82	2	$(-109,4)$
-22188	2	3698	2	43	3	$(29,2)$
-22707	1	841	1	29	1	$(0,-1)$
-23763	2	7921	1	89	3	$(89,-3)$
-24300	1	900	1	30	1	$(0,-1)$
-24300	1	450	2	15	1	$(-1,-2)$
-24300	1	300	3	10	1	$(-2,-3)$
-24300	1	180	5	6	1	$(1,1)$
-24843	2	8281	1	91	3	$(-121,4),(91,-3),(817,-27)$
-25947	1	961	1	31	1	$(0,-1)$
-26508	2	4418	2	47	5	$(16,1)$
-29403	1	1089	1	33	1	$(0,-1)$
-29403	1	363	3	11	3	$(0,-1)$
-31212	1	1156	1	34	1	$(0,-1)$
-31212	1	578	2	17	1	$(1,2)$
-33075	1	245	5	7	2	$(1,1)$
-34347	2	11449	1	107	2	$(178,-5)$
-35643	2	11881	1	109	3	$(109,-3)$

-36300	2	2420	5	22	2	$(-15,-2)$
-38988	1	1444	1	38	1	$(0,-1)$
-38988	1	722	2	19	2	$(0,-1)$
-39675	2	2645	5	23	2	$(8,1)$
-41067	1	1521	1	39	1	$(0,-1)$
-41067	1	507	3	13	3	$(0,-1)$
-41772	2	13924	1	118	3	$(118,-3)$
-44652	2	7442	2	61	2	$(-511,-25)$
-45387	1	1681	1	41	1	$(0,-1)$
-47628	1	1764	1	42	1	$(0,-1)$
-47628	1	882	2	21	2	$(0,-1)$
-47628	1	588	3	14	3	$(0,-1),(3,5)$
-47628	1	294	6	7	1	$(1,1)$
-48387	2	16129	1	127	3	$(127,-3)$
-49923	1	1849	1	43	1	$(0,-1),(2,7)$
-50700	2	8450	2	65	6	$(-65,-3)$
-53868	2	17956	1	134	1	$(-223,5)$
-57132	1	1058	2	23	2	$(0,-1)$
-59643	1	2209	1	47	1	$(0,-1)$
-61347	2	20449	1	143	2	$(-238,5)$
-63075	2	21025	1	145	3	$(145,-3)$
-70227	1	2601	1	51	1	$(0,-1)$
-70227	1	867	3	17	3	$(0,-1)$
-71148	2	23716	1	154	3	$(154,-3)$
-72075	2	4805	5	31	1	$(-21,-2)$
-74892	2	12482	2	79	6	$(-185,-7),(-79,-3)$
-77763	2	25921	1	161	3	$(161,-3)$
-79707	2	26569	1	163	3	$(163,-3),(597,-11)$
-81675	1	605	5	11	5	$(0,-1)$
-82668	2	13778	2	83	5	$(-111,-4)$
-86700	2	28900	1	170	3	$(170,-3)$
-86700	2	2890	10	17	3	$(6,-1)$
-87723	1	3249	1	57	1	$(0,-1)$
-87723	1	1083	3	19	3	$(0,-1)$
-90828	1	3364	1	58	1	$(0,-1)$
-93987	1	3481	1	59	1	$(0,-1)$
-96123	2	32041	1	179	3	$(179,-3)$

-98283	2	32761	1	181	3	$(181, -3)$
-99372	2	2548	13	14	3	$(-178, 41), (-13, 3), (5, -1)$
-100467	1	3721	1	61	1	$(0, -1)$
-103788	1	1922	2	31	2	$(-2, -5), (0, -1)$
-108300	2	36100	1	190	3	$(190, -3)$
-108300	2	3610	10	19	1	$(-6, 1)$
-112908	2	18818	2	97	6	$(-97, -3)$
-114075	1	4225	1	65	1	$(0, -1), (1, 4)$
-116427	2	38809	1	197	3	$(197, -3)$
-117612	1	4356	1	66	1	$(0, -1)$
-117612	1	2178	2	33	2	$(0, -1)$
-117612	1	1452	3	22	2	$(-1, -2)$
-117612	1	726	6	11	5	$(1, 1)$
-118803	2	39601	1	199	3	$(199, -3)$

4.2. Képzetes másodfokú résztesttel rendelkező hatodfokú számtestek hatvány egész bázisainak listája

Az alábbi táblázat azon 100 komplex másodfokú résztesttel rendelkező hatodfokú számtestre vonatkozik, melyek diszkriminánsának abszolút értéke a legkisebb. A táblázat tartalmazza a K számtest D_K diszkriminánsát, az M képzetes másodfokú résztest $\{1, \omega\}$ egész bázisát, és a K M feletti ϑ generátorának $f(X)$ relatív minimálpolinomját. Az eredmények tartalmazzák azon $(x_1, x_2, y_1, y_2, y_0)$ értékeket, melyekre

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

hatvány egész bázist generál K-ban és $max(|x_1|, |x_2|, |y_0|, |y_1|, |y_2|) < 10^{250}$.

$D_K = -9747$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2+\omega X+(1-\omega)$
Megoldások: (0 1 -2 0 1), (0 0 -2 1 1), (0 0 -1 0 0), (0 0 -1 0 1), (0 0 -1 1 0), (0 1 -1 0 0), (0 -1 0 1 0), (0 1 0 0 1), (1 0 -2 1 1), (1 0 -1 1 0), (1 0 -1 0 0), (1 0 -1 0 1), (1 -1 -1 1 0), (1 0 0 0 -1), (1 0 0 0 0), (1 -1 0 0 0), (1 -1 0 1 0), (1 -1 1 0 -1), (2 -1 -2 1 2), (2 0 -2 1 -1), (2 -1 -1 1 0).

$D_K = -10816$, $\omega = i$, $f(X) = X^3 - (1+\omega)X^2 + 5\omega X - (1+4\omega)$
Megoldások: (0 2 -3 0 6), (0 2 -3 0 7), (0 1 -2 0 3), (0 1 -1 0 3), (0 0 -1 0 1), (1 0 0 1 -1), (1 0 0 1 0), (1 -1 2 1 -4), (1 -1 2 1 -3), (1 -2 3 1 -7), (1 -2 3 1 -6), (2 2 -3 1 6), (2 1 -1 1 2), (2 0 0 1 -1), (2 0 0 1 0), (3 1 -1 2 2), (3 0 0 2 -1), (3 -1 2 2 -5), (3 -1 2 2 -4), (5 2 -3 3 4), (5 2 -2 3 5).

$D_K = -11691$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - (1+\omega)X^2 + (-2+2\omega)X + 1$
Megoldások: (0 0 -2 1 1), (0 1 -2 1 1), (0 0 -1 1 0), (1 0 -2 1 0), (1 1 -1 0 0), (1 0 -1 0 0), (1 0 -1 0 1), (1 -1 -1 1 -1), (1 0 -1 1 -1), (1 0 -1 1 0), (1 0 0 0 0), (1 -1 0 0 -1), (1 -1 0 0 0), (1 -1 0 1 -2), (1 -1 0 1 -1), (1 -1 1 0 -2), (1 -1 1 0 -1), (2 -1 -2 1 -1), (2 -1 -1 1 -1), (2 -2 0 1 -3).

$D_K = -12167$, $\omega = (1 + i\sqrt{23})/2$, $f(X) = X^3 - (1 + \omega)X^2 + (-2 + \omega)X + 1$
Megoldások: (0 1 -1 0 0), (1 0 0 0 0), (1 -1 1 0 -1).

$D_K = -14283$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 + (1 - \omega)X - 1$
Megoldások: (0 -1 -1 0 0), (0 0 -1 0 0), (0 0 -1 0 1), (0 -1 -1 1 1), (0 0 -1 -1 -1), (0 -1 0 0 1), (0 1 0 -1 -1), (1 0 0 0 -1), (1 0 0 0 0), (1 1 0 -1 0), (1 0 0 -1 1), (1 1 0 0 -1), (2 -3 -3 0 4), (3 3 -2 -3 -4).

$D_K = -16551$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2+2X+(-1+\omega)$
Megoldások: (0 1 -2 0 0), (0 0 -1 0 0), (1 1 -4 1 3), (1 0 -1 0 1), (1 0 -1 1 1), (1 -1 0 1 1), (1 -1 1 0 0), (2 0 -2 1 1), (2 -1 -1 1 1), (2 -1 0 1 0), (3 0 -3 2 1).

$D_K = -16807$, $\omega = (1 + i\sqrt{7})/2$, $f(X) = X^3 - \omega X^2 + (-1 + \omega)X + 1$
Megoldások: (0 1 -1 0 1), (0 -1 0 0 0), (1 1 -1 0 0), (1 0 -1 1 0), (1 -2 0 1 -1), (1 -1 0 1 0), (1 0 0 0 0), (1 -1 0 0 -1), (2 -1 -1 1 0).

$D_K = -19683$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 + (-1 + \omega)$
Megoldások: (0 0 -1 0 0), (0 1 -1 0 1), (0 0 0 -1 0), (0 -1 0 1 0), (0 1 0 0 0), (1 0 -1 0 0), (1 1 -1 -1 -1), (1 0 0 0 0), (1 0 0 -1 1).

$D_K = -21168$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 + (1 - 2\omega)X + 1$
Megoldások: (0 0 -1 0 0), (0 0 -1 1 -1), (1 0 -2 1 0), (1 -1 -1 1 1), (1 0 -1 1 -1), (1 0 -1 0 0), (1 -1 0 0 1), (1 -1 0 1 0), (2 -1 -1 1 1).

$D_K = -21296$, $\omega = (1+i\sqrt{11})/2$, $f(X) = X^3-\omega X^2+(-1+\omega)X+1$
Megoldások: (0 1 -1 0 1), (0 1 -1 1 1), (1 2 -2 1 2), (1 0 -1 1 1), (1 1 -1 0 0), (1 0 0 0 0), (1 -1 0 0 -1), (1 -2 1 0 -1), (2 0 -1 1 0).

$D_K = -22592$, $\omega = i$, $f(X) = X^3 - (1 + \omega)X^2 + (1 + 2\omega)X - \omega$
Megoldások: (0 1 -1 0 1), (0 1 -1 1 2), (1 2 -3 3 6), (1 0 -1 1 0), (1 0 -1 1 1), (1 -1 0 0 0), (1 0 0 0 0), (1 -1 0 1 0), (1 0 0 1 0), (1 -1 1 0 -1).

$D_K = -22707$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + 2\omega X + (1 - 2\omega)$
Megoldások: (1 0 -1 1 1), (1 0 -1 0 0), (1 0 0 0 0), (1 -1 0 0 -1).

$D_K = -23031$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 + (-1 + \omega)$
Megoldások: (0 0 -1 1 0), (0 -1 0 1 -1), (0 0 0 -1 0), (1 0 -2 1 1), (1 -1 -1 1 0), (1 0 -1 0 0), (1 0 0 0 0), (1 0 0 -1 1).

$D_K = -24003$, $\omega(1 + i\sqrt{3})/2i$, $f(X) = X^3 - X^2 - X + (1 - \omega)$
Megoldások: (0 0 -1 0 0), (0 0 -1 0 1), (0 0 -1 1 -1), (0 1 -1 0 0), (0 1 0 -1 1), (0 0 0 1 -1), (1 0 -1 0 0), (1 -1 -1 1 -1), (1 0 0 0 0), (1 -1 0 0 0), (2 -1 -2 1 1).

$D_K = -25947$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 + X + 1$
Megoldások: (0 0 -1 0 0), (0 -1 -1 0 -1), (0 0 0 -1 -1), (0 -1 0 1 1), (1 0 -1 0 0), (1 0 -1 0 0), (1 1 -1 0 -1).

$D_K = -29791$, $\omega = (1 + i\sqrt{31})/2$, $f(X) = X^3 - (1 + \omega)X^2 + (-2 + \omega)X + 1$
Megoldások: (0 1 -1 0 0), (1 0 0 0 0), (1 -1 1 0 -1).

$D_K = -30976$, $\omega = i$, $f(X) = X^3 - X^2 + (2 - \omega)X - 1$
Megoldások: (0 -1 -1 1 2), (0 0 -1 0 0), (0 0 -1 1 1), (0 0 -1 1 2), (1 -1 0 -1 0), (1 -1 0 0 0), (1 -1 0 0 1), (1 0 0 0 0).

$D_K = -31347$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + 3\omega X - \omega$
Megoldások: (0 0 -1 0 1), (0 1 -1 0 2), (1 0 -1 0 1), (1 0 -1 1 1), (1 0 -1 1 2), (1 0 0 0 0), (1 -1 0 1 0), (1 -1 1 0 -2), (1 0 1 -1 0), (2 0 -1 1 0), (2 -1 -1 1 0).

$D_K = -33856$, $\omega = i$, $f(X) = X^3 + X - \omega$
Megoldások: (0 0 0 -1 -1), (0 0 0 -1 0), (1 0 0 -1 -1), (1 0 0 0 0), (1 -1 0 -1 0), (1 1 0 -1 0).

$D_K = -34371$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + (-1 + 4\omega)X + (2 - \omega)$
Megoldások: (0 0 -2 1 2), (0 0 -1 0 1), (1 -1 -1 1 0), (1 -1 0 0 -3),

(1 -1 0 0 -2), (2 -1 -3 2 2), (2 -1 -2 1 0), (3 -2 -4 2 0).

$D_K = -34992$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + 3\omega X + (1 - 2\omega)$
Megoldások: (0 0 -1 0 1), (1 -1 -1 1 0), (1 -1 0 1 0).

$D_K = -36963$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2+\omega X+(-1+\omega)$
Megoldások: (0 0 -1 0 1), (0 1 -1 0 0), (1 0 -2 1 1), (1 -1 -1 1 0), (1 0 -1 0 0), (1 0 -1 1 0), (1 0 0 0 0), (1 -1 0 0 0), (2 -1 -1 1 0).

$D_K = -40203$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + (-2 + 3\omega)X + (2 - \omega)$
Megoldások: (0 0 -1 0 1), (0 0 -1 1 0), (1 0 -1 0 0), (1 0 -1 1 0), (1 -1 0 0 -2).

$D_K = -41472$, $\omega = i\sqrt{2}$, $f(X) = X^3 + (1 - \omega)X - 1$
Megoldások: (0 -1 -1 -1 0), (0 -1 0 0 1), (1 -1 -1 -1 0), (1 0 0 0 0), (1 1 0 -1 -1), (1 0 0 -1 -1).

$D_K = -41823$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 + (5 - 5\omega)X + (-6 + 2\omega)$
Megoldások: (0 -2 -2 1 7), (0 -1 -1 1 3), (1 0 -1 -1 1), (1 1 0 -1 -3), (2 -1 -2 -1 5), (3 1 0 -3 -1).

$D_K = -44496$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + 2X - 2$
Megoldások: Nincs megoldás.

$D_K = -47680$, $\omega = i$, $f(X) = X^3 - \omega X - 1$
Megoldások: (0 0 -1 -1 -1), (0 -1 -1 0 1), (0 0 -1 0 0), (0 0 -1 0 1), (0 -1 0 0 1), (0 0 0 1 0), (1 0 0 0 0), (1 1 0 0 -1), (3 3 1 0 -1).

$D_K = -47979$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - X^2 - 2\omega X + (-1 + 2\omega)$
Megoldások: (0 0 -1 0 0), (0 -1 -1 -1 2), (0 -1 -1 1 0), (0 -1 0 0 1).

$D_K = -49408$, $\omega = i$, $f(X) = X^3 - X^2 + X + \omega$
Megoldások: (0 0 -1 1 1), (0 1 -1 0 1), (0 0 -1 0 0), (0 0 -1 0 1), (1 0 0 0 0), (1 0 0 1 0), (1 -1 0 0 0).

$D_K = -50139$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - X^2 - X + (-1+\omega)$
Megoldások: (0 0 -1 0 -1), (0 0 -1 1 -1), (1 -1 -1 1 0), (1 0 0 0 0), (2 -2 -2 1 0), (4 -2 -3 2 -1).

$D_K = -52272$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - (1+\omega)X^2 + (4-\omega)X + (-3-2\omega)$
Megoldások: (0 0 -1 1 2), (0 -1 -1 1 3), (1 -2 -1 1 5), (1 0 -1 0 0), (1 -1 0 0 1), (1 0 0 -1 -1).

$D_K = -53568$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - X^2 - \omega X - \omega$
Megoldások: Nincs megoldás.

$D_K = -53824$, $\omega = i$, $f(X) = X^3 - (1+\omega)X^2 + (2+2\omega)X - 1$
Megoldások: Nincs megoldás.

$D_K = -54675$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - (1+\omega)X^2 + (2-\omega)X + \omega$
Megoldások: (1 0 -1 0 0), (1 -1 1 0 1), (2 -1 -1 1 0), (2 -1 0 1 1).

$D_K = -57591$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - (1+\omega)X^2 + (3-3\omega)X + 1$
Megoldások: (1 0 -2 1 0), (1 0 -1 0 0), (1 0 0 0 1), (1 -2 4 0 3), (2 0 -3 1 1), (3 -1 -1 1 1).

$D_K = -59648$, $\omega = i$, $f(X) = X^3 - (1+\omega)X^2 + (-1+\omega)X + (1+\omega)$
Megoldások: (0 0 -1 0 0), (0 0 -1 1 -1), (0 0 -1 1 0), (1 0 -2 1 1), (1 -2 0 0 -1), (1 0 0 0 -1), (1 0 0 0 0), (1 0 0 1 -1), (1 -1 0 0 0).

$D_K = -59967$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - (1+2\omega)X - \omega$
Megoldások: (0 0 -1 0 -1), (0 0 -1 1 -2), (0 0 0 1 -2), (1 -1 0 0 1).

$D_K = -60992$, $\omega = i$, $f(X) = X^3 - X^2 - (1+\omega)X + 1$
Megoldások: (0 0 -2 1 1), (0 0 -1 0 -1), (0 0 -1 0 0), (0 0 -1 1 -1), (0 1 -1 1 -1), (0 0 0 -1 1), (1 0 0 0 0), (1 -1 0 1 0), (1 -1 0 0 0), (1 -1 0 0 1), (2 -1 0 0 1), (8 -4 1 0 1).

$D_K = -61504$, $\omega = i$, $f(X) = X^3 + X - 1$
Megoldások: (0 0 -1 0 0), (0 0 0 1 1), (1 0 0 1 0), (1 0 0 -1 0).

$D_K = -64827$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 - 2X + 1$
Megoldások: Nincs megoldás.

$D_K = -65600$, $\omega = i$, $f(X) = X^3 - (1 + \omega)X^2 - \omega X - 1$
Megoldások: (0 0 -1 0 0), (0 0 -1 1 0), (1 0 -1 1 0), (1 -1 0 0 1), (1 -1 1 0 0).

$D_K = -70659$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - 2X + (1 - \omega)$
Megoldások: (0 0 -1 0 0), (0 2 -1 -2 4), (0 0 -1 -1 2), (0 -1 0 0 0), (0 0 0 1 -2), (0 0 0 1 -1), (1 1 -1 -1 1), (1 0 0 0 0).

$D_K = -72716$, $\omega = (1+i\sqrt{7})/2$, $f(X) = X^3-(1+\omega)X^2+(-1+2\omega)x+1$
Megoldások: (1 0 -2 1 1), (1 -1 0 0 -1), (1 0 0 0 -1), (1 -1 1 0 -1), (3 -2 0 0 -1).

$D_K = -73008$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 + (3 - 2\omega)X - 1$
Megoldások: (0 0 -1 1 1), (1 0 -1 0 0), (1 0 0 -1 0).

$D_K = -73467$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 - 2\omega X + 1$
Megoldások: (0 0 -1 0 0), (0 0 -1 1 -1), (1 -1 -1 1 0).

$D_K = -82496$, $\omega = i$, $f(X) = X^3 - (1 + \omega)X^2 + 1$
Megoldások: (1 0 0 0 0), (1 -1 1 0 0).

$D_K = -82971$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + (2 + \omega)X + (-2 + \omega)$
Megoldások: (1 0 -1 1 1), (2 0 -2 1 2).

$D_K = -85131$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-X^2+(3-2\omega)X+(-1+\omega)$
Megoldások: (1 -1 -1 1 3), (1 0 -1 0 0).

$D_K = -86528$, $\omega = i\sqrt{2}$, $f(X) = X^3 - \omega X^2 - \omega X - 1$
Megoldások: (0 1 -1 0 0), (0 1 0 0 -1), (1 0 0 0 -1), (1 0 0 1 0), (1 2 0 0 -1), (2 -1 1 2 2).

$D_K = -87616$, $\omega = i$, $f(X) = X^3 - (1+\omega)X^2 + (-2+\omega)X + 1$
Megoldások: (0 1 -1 0 0), (0 0 -1 0 0), (0 0 -1 0 1), (1 0 -1 1 -2), (1 0 -1 1 -1), (1 0 0 0 0), (1 0 0 1 -2), (1 0 0 1 -1), (1 -1 1 0 -1).

$D_K = -87831$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2+2\omega X-(1+\omega)$
Megoldások: (0 1 -1 0 1), (1 0 0 0 0).

$D_K = -91719$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - (1+\omega)X^2 + (-1+4\omega)X - 2\omega$
Megoldások: (1 0 -1 1 1), (2 0 -1 1 1), (2 -2 1 1 -5).

$D_K = -92416$, $\omega = i$, $f(X) = X^3 - (1+\omega)X^2 + (-1+\omega)$
Megoldások: Nincs megoldás.

$D_K = -93987$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - 2\omega X + 1$
Megoldások: Nincs megoldás.

$D_K = -94311$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - X^2 - 3\omega X + (-1+4\omega)$
Megoldások: (0 1 0 0 -2), (1 0 -1 -1 3).

$D_K = -95607$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - X^2 + 2X + \omega$
Megoldások: (0 0 -1 0 0), (0 0 -1 1 2), (1 -1 -1 1 2), (1 -1 0 1 1), (1 0 0 0 0).

$D_K = -96512$, $\omega = i$, $f(X) = X^3 - X^2 - X - \omega$
Megoldások: (0 0 -1 1 -1), (0 0 -1 0 0), (1 0 0 0 0), (1 -1 0 0 0).

$D_K = -96579$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-X^2+(1-\omega)X+(-2+\omega)$
Megoldások: (0 0 -1 0 0), (0 -1 0 0 1), (1 0 -2 1 1), (1 0 -1 0 0), (1 0 0 0 0), (1 0 0 -1 1).

$D_K = -96832$, $\omega = i$, $f(X) = X^3 - (1+\omega)X^2 + \omega X + \omega$
Megoldások: (0 0 -1 0 0), (1 0 -1 1 0), (1 0 0 0 0), (1 0 0 1 0), (1 -1 0 0 0), (1 -1 1 0 -1).

$D_K = -103383$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 + (3 - 3\omega)X + (-3 + 2\omega)$
Megoldások: (1 0 -1 0 0), (1 -1 -1 0 3).

$D_K = -104112$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + (-2 + 3\omega)X + (1 - 2\omega)$
Megoldások: (0 1 -1 0 2), (1 1 -1 0 1), (1 0 -1 0 0), (1 0 0 0 0).

$D_K = -104571$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 - (1 + 2\omega)X + 3\omega$
Megoldások: (0 -1 0 1 -1), (0 0 0 -1 2), (1 0 -1 0 1).

$D_K = -106560$, $\omega = i$, $f(X) = X^3 - (1 + \omega)X^2 - X - 1$
Megoldások: (1 0 0 0 0), (1 -1 1 0 0).

$D_K = -107163$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + (1 - 2\omega)X + (-2 + 3\omega)$
Megoldások: (0 0 -1 0 0), (0 1 -1 0 -1), (0 1 0 0 -3).

$D_K = -107811$, $\omega = (1+i\sqrt{11})/2$, $f(X) = X^3 - \omega X^2 + (-3+\omega)X + \omega$
Megoldások: (1 0 0 0 0), (1 -2 1 0 -1), (2 -2 1 0 -2).

$D_K = -108459$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 + (3 - 3\omega)X + (-2 + \omega)$
Megoldások: (0 -1 -1 2 2), (1 0 0 -1 0).

$D_K = -108544$, $\omega = i$, $f(X) = X^3 - (1+\omega)X^2 + (-2+\omega)X + (1+\omega)$
Megoldások: (0 0 -1 0 0), (1 0 0 0 0).

$D_K = -108731$, $\omega = (1 + i\sqrt{7})/2$, $f(X) = X^3 - (1 + \omega)X^2 - X + \omega$
Megoldások: (0 1 -1 0 -1), (0 1 -1 0 0), (1 0 -1 1 -1), (1 0 0 0 0), (2 -1 1 0 -1).

$D_K = -108800$, $\omega = i$, $f(X) = X^3 - X^2 + (1 - 2\omega)X + \omega$
Megoldások: (1 -1 0 0 1).

$D_K = -109539$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 + 3X - \omega$
Megoldások: (1 0 -1 0 0), (1 -1 -1 0 0), (1 -1 -1 1 3), (1 0 0 0 0),

(1 -1 0 0 0).

$D_K = -109744$, $\omega = (1 + i\sqrt{19})/2$, $f(X) = X^3 - (1+\omega)X^2 + (-2+\omega)X + 1$
Megoldások: (0 1 -1 0 0), (1 0 0 0 0), (1 -1 1 0 -1).

$D_K = -110079$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 + (1-2\omega)X + (2-\omega)$
Megoldások: (0 1 -1 0 -2), (0 -1 1 0 2), (1 0 -1 0 0), (1 0 -1 1 -1), (1 -1 0 0 1).

$D_K = -110144$, $\omega = i$, $f(X) = X^3 - (1+\omega)X^2 + (-3-\omega)X + (2+3\omega)$
Megoldások: (0 0 -1 0 1), (0 2 -1 0 -3), (0 0 0 -1 2), (0 -1 0 0 1), (1 1 0 1 -3).

$D_K = -112192$, $\omega = i$, $f(X) = X^3 - X^2 + (-2-3\omega)X - 2\omega$
Megoldások: (0 0 -2 1 -1), (1 -1 2 -1 3), (2 -1 -1 1 1), (4 -2 0 1 1).

$D_K = -114399$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 + (4-\omega)X + (1-3\omega)$
Megoldások: (0 -1 -1 0 0), (1 0 0 0 -1), (1 0 0 -1 -2), (2 -3 -3 0 4).

$D_K = -116800$, $\omega = i$, $f(X) = X^3 + (1-3\omega)X + (-2+\omega)$
Megoldások: (0 -1 -1 -1 1), (1 1 1 0 -2).

$D_K = -117207$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 - 2X + (1+\omega)$
Megoldások: (0 0 0 -1 2), (1 0 0 0 0).

$D_K = -118287$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 + (-2-\omega)X + \omega$
Megoldások: (0 -1 0 1 -2), (1 1 -1 -3 4), (1 0 0 0 0), (1 1 0 0 -1).

$D_K = -122256$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3 - (1+\omega)X^2 - X + (1-\omega)$
Megoldások: Nincs megoldás.

$D_K = -124848$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - 4\omega X + (-2+4\omega)$
Megoldások: (0 -1 -1 0 3), (0 0 -1 -1 3), (1 0 -4 -3 7), (1 0 -1 0 1), (1 0 0 0 -1), (1 3 3 0 -7).

$D_K = -129088$, $\omega = i$, $f(X) = X^3 - X^2 + (1 - 2\omega)X + (1 + \omega)$
Megoldások: (0 0 -1 0 0), (1 -1 1 0 1).

$D_K = -130032$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + (-5 + 5\omega)X + (6 - 5\omega)$
Megoldások: Nincs megoldás.

$D_K = -130304$, $\omega = i$, $f(X) = X^3 - (1 + \omega)X^2 + (-3 + 2\omega)X + 2\omega$
Megoldások: (0 0 -1 0 -1), (1 -1 2 -1 1), (4 -2 1 0 -3).

$D_K = -131787$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 + (2 - 3\omega)X + (-1 + \omega)$
Megoldások: (1 -1 -1 1 2), (1 0 -1 0 0), (1 -1 0 0 2).

$D_K = -133407$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2-(1+\omega)X-1$
Megoldások: (0 0 -1 0 0), (1 0 0 0 -1), (2 -1 -1 1 -1), (4 -2 -3 2 0).

$D_K = -133839$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - X^2 - (1 + \omega)X + 2$
Megoldások: (0 1 0 -1 1), (1 0 -1 -1 1), (1 0 -1 0 1), (1 0 -1 2 -5).

$D_K = -134811$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 + (2 - 2\omega)X - (1 + \omega)$
Megoldások: (0 -1 -1 0 1), (0 1 1 0 -1), (1 0 -1 0 0).

$D_K = -137200$, $\omega = (1+i\sqrt{7})/2$, $f(X) = X^3-\omega X^2+(-2+\omega)X+\omega$
Megoldások: (1 0 0 0 0), (1 -1 0 0 -1).

$D_K = -137403$, $\omega = (1 + i\sqrt{3})/2$, $f(X) = X^3 - (1 + \omega)X^2 + (-2 + 3\omega)X + (2 - 3\omega)$
Megoldások: Nincs megoldás.

$D_K = -139023$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2+(1+2\omega)X-2$
Megoldások: (0 0 -1 0 1), (0 1 -1 0 1), (2 -1 -1 0 1).

$D_K = -139520$, $\omega = i$, $f(X) = X^3 + (1 - \omega)X - (1 + \omega)$
Megoldások: (0 -1 -1 0 1), (0 0 -1 0 0).

$D_K = -139968$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2-(1+\omega)X+\omega$
Megoldások: Nincs megoldás.

$D_K = -141939$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2-X-\omega$
Megoldások: (0 0 -2 1 0), (0 0 -1 0 1), (2 -1 -1 1 -2).

$D_K = -143872$, $\omega = i\sqrt{2}$, $f(X) = X^3-\omega X^2-(1+\omega)X-1$
Megoldások: (0 1 -1 0 -1), (0 1 -1 0 0), (1 0 0 0 0), (1 0 0 1 0), (1 -1 1 0 0), (2 1 -1 2 -2).

$D_K = -143883$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2+\omega X-(1+\omega)$
Megoldások: Nincs megoldás.

$D_K = -144207$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-(1+\omega)X^2+(2-2\omega)X+(-2+\omega)$
Megoldások: (0 0 -1 1 -1), (1 0 -1 0 0), (2 0 -3 1 1).

$D_K = -144448$, $\omega = i$, $f(X) = X^3-(1+\omega)X^2-(1+\omega)X-1$
Megoldások: (1 0 0 0 -1).

$D_K = -147008$, $\omega = i$, $f(X) = X^3-(1+\omega)X^2-(1+2\omega)X+1$
Megoldások: (0 0 -1 0 0), (1 0 -1 1 1), (1 -1 0 0 -1).

$D_K = -147520$, $\omega = i$, $f(X) = X^3-(1+\omega)X^2+(-2+\omega)X+(2+\omega)$
Megoldások: (0 0 -1 0 0), (1 0 0 0 0), (1 0 0 1 -2).

$D_K = -149283$, $\omega = (1+i\sqrt{3})/2$, $f(X) = X^3-X^2+(3-\omega)X+(-2+\omega)$
Megoldások: (0 1 0 0 -1), (1 0 0 0 0).

4.3. Valós másodfokú résztesttel rendelkező hatodfokú számtestek hatvány egész bázisainak listája

Az alábbi táblázat azon 6 valós másodfokú résztesttel rendelkező hatodfokú számtestre vonatkozik, melyek diszkriminánsának abszolút értéke a legkisebb. A táblázat tartalmazza a K számtest D_K diszkriminánsát, az M képzetes másodfokú résztest $\{1, \omega\}$ egész bázisát, és a K M feletti ϑ generátorának $f(X)$ relatív minimálpolinomját. Az eredmények tartalmazzák azon $(x_1, x_2, y_1, y_2, y_0)$ értékeket, melyekre

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

hatvány egész bázist generál K-ban és $max(|x_1|, |x_2|, |y_0|, |y_1|, |y_2|) < 10^{300}$.

$D_K = 30125$, $\omega = (1+\sqrt{5})/2$, $f(X) = X^3 - (1+\omega)X^2 - (1+\omega)X + (3+5\omega)$
Megoldások: (12 -3 19 -4 -25).

$D_K = 35125$, $\omega = (1+\sqrt{5})/2$, $f(X) = X^3 - \omega X^2 + (-4+3\omega)X + (8-5\omega)$
Megoldások: Nincs megoldás.

$D_K = 49664$, $\omega = \sqrt{2}$, $f(X) = X^3 - (1+\omega)X^2 + 2X + (1-\omega)$
Megoldások: (2 -1 1 0 0).

$D_K = 51125$, $\omega = (1+\sqrt{5})/2$, $f(X) = X^3 - \omega X^2 + (-1+\omega)X + (-2+\omega)$
Megoldások: (0 0 1 0 0).

$D_K = 52625$, $\omega = (1+\sqrt{5})/2$, $f(X) = X^3 - (1+\omega)X^2 + (-1+2\omega)X + (-4+2\omega)$
Megoldások: (4 -3 6 -5 -3), (1 -1 3 -1 -1).

$D_K = 56125$, $\omega = (1+\sqrt{5})/2$, $f(X) = X^3 - \omega X^2 - X + (-3+3\omega)$
Megoldások: Nincs megoldás.

Összefoglalás

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.

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:

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

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

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

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

$(i = 1, 2, \ldots, n)$. 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. Ehhez 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 $\mathcal{O}$ vagy $\mathbb{Z}_K$ vagy egy rend $\mathbb{Z}_K$-ban. 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 2. Fejezetében egyik célunk volt 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 2. Fejezet másik felében olyan hatodfokú számtestekben határozzuk meg a hatvány egész bázisok generátorait, melyek másodfokú résztesttel rendelkeznek. Célunk a korábbiaknál sokkal több számtestre 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 számtest*re, valamint *valós másodfokú résztesttel rendelkező hatodfokú számtest*ekre is, melyek a korábbi számításokban még egyáltalán nem szerepeltek.

A dolgozat 3. 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.

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. Mi 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 eset, 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 a (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.

A fejezet második felében 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 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. 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.*

Summary

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 fileds there are effective algorithms, in quintic and sextic fileds there are more complicated but still usable algorithms for calculating the generators of the power integral bases.

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

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

The integral basis of the form $\{1, \theta, \dots, \theta^{n-1}\}$ we call *power integral basis*. In this case we call the element θ the generator of the power integral basis.

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

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

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

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

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

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

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

The *minimal index* of K is

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

We also considered 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 in 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 the firs part of Chapter 2 using standard techniques, we study the existance of power integral bases and the behaviour of minimal indices of pure cubic fields of type $K = \mathbb{Q}(\sqrt[3]{n})$, 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 is decreasing and the minimal index increases in average 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].

In Chapter 2 we calculate power integral bases in sextic fields with a quadratic subfield. 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].

In Chapter 3 we calculate power integral bases in quartic fields and calculate relative and absolute power integral bases in quartic extensions of imaginary quadratic 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*

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

In the second half of 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.*

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)