Hatvány egész bázisok számtestek családjaiban

Power integral bases in families of number fields

doktori (PhD) értekezés tézisei

Olajos Péter

Témavezető: Dr. Gaál István

Debreceni Egyetem

Debrecen, 2004

Bevezetés

Legyen K n-ed fokú algebrai számtest, jelölje $\mathbb{Z}_K$ az egészek gyűrűjét. Az algebrai számelmélet egy klasszikus problémája annak eldöntése, hogy létezik-e olyan K-beli α elem, hogy

$$1, \alpha, \alpha^2, ..., \alpha^{n-1}$$

egész bázis. Az ilyen egész bázisokat *hatvány egész bázisnak* nevezzük. A $\mathbb{Z}_K$ egészek gyűrűjét *monogénnek* nevezzük, ha K rendelkezik hatvány egész bázissal. Egy további probléma megtalálni az összes olyan α elemet, amely hatvány egész bázist generál K-ban.

Egy $\alpha \in \mathbb{Z}_K$ primitív elem indexe

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

Ez felírható

$$I(\alpha) = \frac{\prod_{1 \le j < k \le n} |\alpha^{(j)} - \alpha^{(k)}|}{\sqrt{|D_K|}}, \tag{1}$$

alakban is, ahol D_K a K test diszkriminánsa.

Nyilvánvalóan az α pontosan akkor generál hatvány egész bázist, ha $I(\alpha) = 1$.

Legyen az $\{1, \omega_2, ..., \omega_n\}$ egy tetszőleges egész bázisa a K-nak. Ekkor a

$$l(x) = x_1 + x_2\omega_2 + ... + x_n\omega_n$$

lineáris forma diszkriminánsára teljesül, hogy

$$D_{K/\mathbb{Q}}(l(x)) = \prod_{1 \le i < j \le n} (l^{(i)}(x) - l^{(j)}(x))^2 = I(x_2, ..., x_n)^2 D_K,$$

ahol $x = (x_1, x_2, ..., x_n) \in \mathbb{Z}^n$ és az $I(x_2, ..., x_n)$ egy $\frac{n(n-1)}{2}$ fokú, $n-1$ változós, egész együtthatós homogén forma, melyet az $\{1, \omega_2, ..., \omega_n\}$ egész bázishoz tartozó *index formának* nevezünk.

Tetszőleges $\mathbb{Z}_K$-beli α elemet az $\alpha = x_1 + \omega_2 x_2 + ... + \omega_n x_n$ formában reprezentálva kapjuk, hogy az

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

mely független az α első koordinátájától. Azaz, a hatvány egész bázisok generátor elemeinek megkereséséhez meg kell oldanunk a következő diofantikus egyenletet:

$$I(x_2, ..., x_n) = \pm 1 \ (x_2, \ldots, x_n \in \mathbb{Z}). \tag{2}$$

1976-ban Győry K. ([18], [20] és [19]) a Baker módszer felhasználásával adott effektív felső korlátot az index forma egyenletek megoldására (lásd még [21] a legújabb javítások). Ez azt jelenti, hogy csak véges sok megoldása van a (2) egyenletnek.

Az elmúlt évtizedben számos szerző foglalkozott index forma egyenletek megoldására vonatkozó algoritmusok konstruálásával. Vannak hatékony algoritmusok

alacsony fokszámú számtestekben az összes hatvány egész bázis generátor meghatározására: Gaál I. és N. Schulte [16] a harmadfokú testekre, Gaál I., Pethő A. és M. Pohst [11] a negyedfokú testekre. Az ötöd és hatodfokú testekre Gaál I. és Győry K. [9] ill. Y. Bilu, Gaál I. és Győry K. [1] adtak általános algoritmusokat, melyek már több órás CPU időt igényelnek. Bizonyos speciális hatod-, nyolcad-, és kilencedfokú testek esetén dolgoztak ki módszereket az indexforma egyenlet megoldására: Gaál I. [3], Gaál I. [5], Gaál I. és M. Pohst [13], Járási I. [22]. A (2) egyenlet megoldására vonatkozó algoritmusok részletes leírása és számos ezzel kapcsolatos eredmény megtalálható Gaál I. [8] könyvében.

I

Magasabb fokszámú testekben ez a probléma nagyon komplikált, a (2) egyenlet magas fokszáma és a változók nagy száma miatt. A (2) egyenlet megoldása csak akkor reményteljes, ha a K bizonyos résztestek kompozítuma, mert ebben az esetben az indexforma reducibilis. Érdekes és jól alkalmazható szükséges feltételek ismertek a hatvány egész bázis létezésére vonatkozóan. Az első fejezet célja ezen eredmények összegzése kompozit testekben. Ezen eredmények számos alkalmazását is bemutatjuk.

II

A II. fejezetben a legegyszerűbb negyedfokú testek végtelen parametrikus családjában megadjuk az összes hatvány egész bázis generátor elemét.

Legyen $t \in \mathbb{Z}$ paraméter, α a $P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1$ gyöke és tekintsük a $K_t = K = \mathbb{Q}(\alpha)$ számtestek végtelen parametrikus családját. Ezeket a teljesen valós, ciklikus, negyedfokú testeket a "legegyszerűbb" negyedfokú testeknek nevezik.
Számos szerző foglalkozott a K legegyszerűbb negyedfokú testek végtelen parametrikus családjával (lásd [17],[26] és [28]). A $\mathbb{Z}[\alpha]$ polinomgyűrű hatvány egész bázisainak generátorai már ismertek. A mi esetünkben bizonyos$t$-re vonatkozó feltételek mellett a K test $\mathbb{Z}_K$ egészeinek gyűrűjében adjuk meg explicit módon az összes hatvány egész bázis generátor elemet.

III

A III. fejezetben az elsőhöz hasonlóan speciális struktúrájú hatodfokú parametrikus családot tekintünk. Tudjuk, hogy ha egy hatodfokú test rendelkezik egy másodfokú résztesttel, akkor az index egyik faktora a másodfokú résztest feletti relatív Thue egyenletre vezet. Teljesen valós, ciklikus hatodfokú testekben index forma egyenletek megoldásával kapcsolatos algoritmusokat fejlesztett ki: Gaál I. [4] és Gaál I. és M. Pohst [13].

Ebben a fejezetben adott indexű elemek meghatározásának problémáját vizsgáljuk olyan képzetes másodfokú résztesttel rendelkező hatodfokú testek egy végtelen parametrikus családjában, melyek egy harmadfokú, teljesen valós résztesttel is rendelkeznek. Felhasználva Gaál I. [3] eredményét a problémánk $\mathbb{Z}$ feletti harmadfokú

Thue egyenlőtlenségek megoldására redukálódik, ha a paraméter nem túl kicsi. Ismertek gyors algoritmusok harmad- (vagy magasabb fokú) Thue egyenletek vagy egyenlőtlenségek megoldására (lásd [2]). Továbbá direkt számítások felhasználásával azokat a testeket is vizsgáltuk, melyek a kis paraméter értékhez tartoznak és ezért a fő tétel nem vonatkozik rájuk.

1. Kompozit testek

1.1. Relatív prím diszkriminánsok

Legyen L egy r-edfokú számtest $\{l_1 = 1, l_2, \ldots, l_r\}$ egész bázissal és D_L diszkriminánssal. Jelölje $I_L(x_2, \ldots, x_r)$-lel az L $\{l_1 = 1, l_2, \ldots, l_r\}$ egész bázisához tartozó index formát. Hasonlóan, legyen M egy s-edfokú számtest $\{m_1 = 1, m_2, \ldots, m_s\}$ egész bázissal és D_M diszkriminánssal. Jelölje $I_M(x_2, \ldots, x_s)$-lel az M $\{m_1 = 1, m_2, \ldots, m_s\}$ egész bázisához tartozó index formát. Legyen $K = LM$ az L és M kompozítuma. Ismert, hogy ha $(D_L, D_M) = 1$, akkor a K diszkriminánsa

$$D_K = D_L^s \cdot D_M^r$$

és a K egy egész bázisa

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

alakban adható meg. Így tetszőleges α K-beli egész reprezentálható az

$$\alpha = \sum_{i=1}^{r} \sum_{j=1}^{s} x_{ij} \cdot l_i \cdot m_j \tag{3}$$

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

Gaál I. [5] megfogalmazott egy általános szükséges feltételt, hogy egy $\alpha \in \mathbb{Z}_K$ elem milyen esetben generál K-ban hatvány egész bázist.

1. Tétel. *(Gaál I., [5])*
Feltételezzük, hogy $(D_L, D_M) = 1$. Ha az (3) formában megadott α hatvány egész bázist generál $K = LM$-ban, akkor

$$N_{M/Q}\left(I_L\left(\sum_{i=1}^{s} x_{2i} \cdot m_i, \ldots, \sum_{i=1}^{s} x_{ri} \cdot m_i\right)\right) = \pm 1 \tag{4}$$

és

$$N_{L/Q}\left(I_M\left(\sum_{i=1}^{r} x_{i2} \cdot l_i, \ldots, \sum_{i=1}^{r} x_{is} \cdot l_i\right)\right) = \pm 1. \tag{5}$$

1.1.1. Az 1. Tétel alkalmazásai

Példa: Kilenced fokú test harmadfokú résztestekkel (lásd Gaál I. [7]).

Legyenek az f, g egyváltozós, irreducibilis, egész együtthatós harmadfokú polinomok. Jelölje rendre az f és g egy-egy gyökét ϕ és ψ. Tekintsük az $L = \mathbb{Q}(\phi)$ és $M = \mathbb{Q}(\psi)$ algebrai számtesteket. Az 1. Tétel alkalmazásaként a következő példákat vizsgálták a [7]-ben:

1. $f(x) = x^3 - x + 1,\ D_L = -23, \quad g(x) = x^3 - 2x + 2,\ D_M = -76$
2. $f(x) = x^3 + x + 1,\ D_L = -31, \quad g(x) = x^3 + x^2 + x + 2,\ D_M = -83$
3. $f(x) = x^3 + 2x + 1,\ D_L = -59, \quad g(x) = x^3 + x^2 - 2x - 3.\ D_M = -87$

Felhasználva a 1. Tételt megmutatták, hogy a $K = LM$ kompozit testben nincs hatvány egész bázis egyik esetben sem. Megjegyezzük, hogy ha L és M harmadfokú testek, akkor az (4) és az (5) harmadfokú, relatív Thue egyenletek a harmadfokú testek felett.

1.2. Jelölések

Az alábbi fejezetekben a következő jelöléseket fogjuk használni:
Legyenek az $f, g \in \mathbb{Z}[x]$ különböző, egyváltozós, irreducibilis rendre m és n fokú polinomok ($\mathbb{Q}$ felett). Legyen a φ az f egyik gyöke és legyen a ψ a g egyik gyöke. Legyen az $L = \mathbb{Q}(\varphi)$, $M = \mathbb{Q}(\psi)$ és feltételezzük, hogy a $K = LM$ kompozit test foka mn. Jelölje $d(f)$ és $d(g)$ rendre az f és g polinomok diszkriminánsait.

Tekintsük az L test $\mathcal{O}_f = \mathbb{Z}[\varphi]$, az M test $\mathcal{O}_g = \mathbb{Z}[\psi]$ rendjeit és a $K = ML$ kompozit testben az $\mathcal{O}_{fg} = \mathcal{O}_f\mathcal{O}_g = \mathbb{Z}[\varphi, \psi]$ rendet. Megjegyezzük, hogy az $\{1, \varphi, \ldots, \varphi^{m-1}\}$, $\{1, \psi, \ldots, \psi^{n-1}\}$ és az

$$\{1, \varphi, \ldots, \varphi^{m-1}, \psi, \varphi\psi, \ldots, \varphi^{m-1}\psi, \ldots, \psi^{n-1}, \varphi\psi^{n-1}, \ldots, \varphi^{m-1}\psi^{n-1}\},$$

rendre $\mathbb{Z}$ bázisok az $\mathcal{O}_f$, $\mathcal{O}_g$ és az $\mathcal{O}_{fg}$ rendekben.

1.3. Nem relatív prím diszkriminánsok

Ha a 1. Tétel feltétele teljesül, akkor a hatvány egész bázisok generátor elemeinek megkereséséhez meg kell oldanunk az (4) és (5) egyenleteket, amelyek sokszor nagyon komplikáltak. Az alábbiakban egyszerű elégséges feltételeket adunk meg, mely feltételek teljesülése mellett a vizsgált rendben nincs hatvány egész bázis.

Feltételezzük, hogy van olyan q ($q > 2$) prím szám, hogy mind az f, mind a g rendelkezik többszörös (legalább kétszeres) gyökkel $\bmod q$, azaz léteznek olyan a_f és a_g egész számok, úgy hogy

$$\begin{array}{rcccl} f(a_f) & \equiv & f'(a_f) & \equiv & 0 \pmod{q}, \\ g(a_g) & \equiv & g'(a_g) & \equiv & 0 \pmod{q}. \end{array} \tag{6}$$

1. Megjegyzés. A feltételeinkből következik, hogy a q egyszerre osztja az f polinom $d(f)$ és a g polinom $d(g)$ diszkriminánsát is.

2. Megjegyzés. Az [5]-ben olyan testeket tekintettünk, amelyek két relatív prím diszkriminánsú résztest kompozítumai. A fenti megjegyzés alapján a mi eseteinkben a vizsgált testek olyan kompozit testek, melyek diszkriminánsai nem szükségszerűen

relatív prímek. Ez az eset áll elő sok érdekes példa során, amelyek közül néhányat ezen szakasz végén felsorolunk.

Az eredményünk a következő (lásd [15]):

2. Tétel. *(Gaál I., Olajos P., M. Pohst, [15])*
A fenti feltételek mellett az $\mathcal{O}_{fg}$ rend minden primitív elemének indexe oszthatóq-val.

Következményként kapjuk, hogy:

3. Tétel. *(Gaál I., Olajos P., M. Pohst, [15])*
A fenti feltételek mellett az $\mathcal{O}_{fg}$ rendben nincs hatvány egész bázis.

1.3.1. A 3. Tétel alkalmazásai

I. Példa Egy ciklikus hatodfokú test

Tekintsük a K hatodfokú testet, amelyet a $h(x) = x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1$ egyik gyöke generál. Ez egy teljesen valós, ciklikus, hatodfokú test $D_K = 453789 = 3^3 7^5$ diszkriminánssal. Ennek harmadfokú részteste az $L = \mathbb{Q}(\varphi)$ (49 diszkriminánssal), ahol a φ az $f(x) = x^3 + 4x^2 + 3x - 1$ gyöke. Az L testben az $\{1, \varphi, \varphi^2\}$ elemek egész bázist generálnak. A $q = 7$ prímszámmal teljesül, hogy $f(x) \equiv (x+6)^3 \pmod 7$. A másodfokú résztest az $M = \mathbb{Q}(\sqrt{21})$. A $g(x) = x^2 - x - 5$ polinomnak gyöke a $\psi = (1 + \sqrt{21})/2$ és nyilvánvalóan az $\{1, \psi\}$ egy egész bázis az M-ben. A $q = 7$ prímszámmal teljesül, hogy $g(x) \equiv (x - 1/2)^2 \pmod 7$. A 2. Tételből következik, hogy az $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$ rend primitív elemeinek indexe mind osztható 7-tel, így a rendben nincs hatvány egész bázis.

II. Példa Egy nem ciklikus hatodfokú test

Tekintsük a K hatodfokú testet, amelyet a $h(x) = x^6 - 12190x^4 + 256565x^2 - 12167$ egyik gyöke generál. Ez teljesen valós, hatodfokú test D_6 Galois csoporttal, $D_K = 2^6 17^2 23^3 647^2$ diszkriminánssal. Ennek harmadfokú részteste az $L = \mathbb{Q}(\varphi)$ ($252977 = 17 \cdot 23 \cdot 647$ diszkriminánssal és S_3 Galois csoporttal), ahol a φ is az $f(x) = x^3 - 22x^2 - 23x - 1$ gyöke. Az L testben az $\{1, \varphi, \varphi^2\}$ elemek egy egész bázist alkotnak. A $q = 23$ prímszámmal teljesül, hogy $f(x) \equiv (x+15)(x+16)^2 \pmod{23}$. A másodfokú test az $M = \mathbb{Q}(\sqrt{23})$. A $g(x) = x^2 - 23$ polinom gyöke a $\psi = \sqrt{23}$ és nyilvánvalóan az $\{1, \psi\}$ egy egész bázis az M-ben. A $q = 23$ prímszámmal teljesül, hogy $g(x) \equiv x^2 \pmod{23}$. A 2. Tételből következik, hogy az $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$ rend primitív elemeinek indexe mind osztható 23-mal, így a rendben nincs hatvány egész bázis.

III. Példa Legegyszerűbb hatodfokú testek parametrikus családja

Legyen t egész paraméter, melyre $3 \nmid t$, $t \neq -8, -5$. Legyen β_t gyöke a

$$h_t(x) = x^6 - 2tx^5 - (5t + 15)x^4 - 20x^3 + 5tx^2 + (2t + 6)x + 1.$$

polinomnak és tekintsük hatodfokú testek $K_t = \mathbb{Q}(\beta_t)$ családját.

Ezt a családot "legegyszerűbb hatodfokú testeknek" nevezik, amely rendelkezik néhány érdekes tulajdonsággal, részletezve ld. [27]-ben. Ezek a testek teljesen valós, ciklikus testek. Legyen $q = t^2 + 3t + 9$. Ezt felhasználva kapjuk, hogy $d(h_t) = 6^6 q^5$. Megjegyezzük, hogy a $h_t(x) \equiv (x - t/3)^6 \pmod{q}$ (a "legegyszerűbb ötödfokú testek" hasonló tulajdonsággal rendelkeznek, vö. [14]).

A K_t test L_t harmadfokú résztestét az

$$f_t = x^3 - tx^2 - (t+3)x - 1$$

egyik φ gyöke generálja, ahol $d(f_t) = q^2$. Ezek pontosan a "legegyszerűbb harmadfokú testek", melyek teljesen valósak, ciklikusak. Ekkor nyilvánvalóan az $\{1, \varphi, \varphi^2\}$ egész bázisa az L_t-nek. Megjegyezzük, hogy $f_t(x) \equiv (x - t/3)^3 \pmod{q}$.

A K_t másodfokú részteste az $M_t = \mathbb{Q}(\sqrt{q})$.
Ha $q \equiv 2, 3 \pmod 4$, akkor legyen a $g_t(x) = x^2 - q$, ahol $d(g_t) = 4q$ és a $\psi = \sqrt{q}$ az egyik gyöke. Ebben az esetben $g_t(x) \equiv x^2 \pmod{q}$.
Ha $q \equiv 1 \pmod 4$, akkor legyen $g_t(x) = x^2 - x - (q-1)/4$, ahol $d(g_t) = q$ és a $\psi = (1 + \sqrt{q})/2$ az egyik gyöke. Ebben az esetben $g_t(x) \equiv (x - 1/2)^2 \pmod{q}$.
Mindkét esetben az $\{1, \psi\}$ egész bázisa az M_t-nek.

Tekintsük most az $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$ rendet. A 2. Tétel felhasználásával az $\mathcal{O}_{fg}$ rend primitív elemeinek indexe mind osztható q-val, ezért az $\mathcal{O}_{fg}$ rendben nincs hatvány egész bázis.

IV. Példa Magasabb fokú testek I.

A következőkben egy olyan példát mutatunk be, amely szemlélteti, hogy adott esetben az eredményünk könnyen alkalmazható bizonyos magasabb fokszámú testekre is.

Legyen a φ az $f(x) = x^5 - 2x^4 + 7x^2 + 6x + 5$ gyöke. Az $L = \mathbb{Q}(\varphi)$ ötödfokú test nem rendelkezik nem-triviális résztestekkel. Legyen ψ az $g(x) = x^8 + 13x^7 + 55x^6 + 75x^5 + 2x^3 - x^2 - 143x - 525$ gyöke. Az $M = \mathbb{Q}(\psi)$ nyolcadfokú test ugyancsak nem rendelkezik nem-triviális résztestekkel. A $q = 17$ prímszámmal teljesül, hogy

$$\begin{aligned} f(x) &\equiv (x+16)^2(x^3 + 16x + 5) \pmod{17}, \\ g(x) &\equiv (x+5)^2(x^3 + 12x^2 + 2x + 14)(x^3 + 8x^2 + 4x + 7) \pmod{17}, \end{aligned}$$

ezért a 2. Tétel alkalmazható. Tekintsük a $K = \mathbb{Q}(\varphi, \psi)$ 40-ed fokú test $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ rendjét. Tetszőleges $\alpha \in \mathcal{O}_{fg}$ megadható az

$$\alpha = \sum_{i=0}^{4} \sum_{j=0}^{7} x_{ij} \varphi^i \psi^j$$

alakban, ahol $x_{ij} \in \mathbb{Z}$. A 2. Tétel felhasználásával az $\mathcal{O}_{fg}$ rend összes primitív elemének az indexe osztható 17-tel, ezért az $\mathcal{O}_{fg}$ rendben nincs hatvány egész bázis.

V. Példa Magasabb fokú testek II.

Legyen a φ az $f(x) = x^5 + 17x^4 + 446x^3 + 2232x^2 + 6048x + 24192$ gyöke. Legyen a ψ a $g(x) = x^4 + 21x^3 - 3x^2 - 8x - 4$ gyöke. A $q = 19$ prímszámmal teljesül, hogy

$$\begin{aligned} f(x) &\equiv (x+12)^3(x+9)(x+10) \pmod{19}, \\ g(x) &\equiv (x+1)^2(x+2)(x+17) \pmod{19}, \end{aligned}$$

ezért a 2. Tétel alkalmazható. Tekintsük a $K = \mathbb{Q}(\varphi, \psi)$ 20-ad fokú test $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ rendjét. Tetszőleges $\alpha \in \mathcal{O}_{fg}$ megadható az

$$\alpha = \sum_{i=0}^{4} \sum_{j=0}^{3} x_{ij} \varphi^i \psi^j$$

alakban, ahol $x_{ij} \in \mathbb{Z}$. A 2. Tétel alapján az $\mathcal{O}_{fg}$ rend összes primitív elemeinek indexe osztható 19-cel, ezért az $\mathcal{O}_{fg}$ rendben nincs hatvány egész bázis.

VI. Példa Magasabb fokú testek III.

A fentiekhez hasonló jelöléseket használva legyen a φ az

$$\begin{aligned} f(x) = x^9 - 8x^8 + 73926x^7 + 5470524x^6 + 151807041x^5 + \\ 14x^4 + 6216x^3 + 1034964x^2 + 76587336x + 2125298574. \end{aligned}$$

gyöke. Legyen a ψ a

$$\begin{aligned} g(x) = x^8 - 58x^7 + 1210x^6 + 13324x^5 + 73975x^4 + \\ 177991x^3 + 186340x^2 + 1024870x + 2254714. \end{aligned}$$

gyöke. A $q = 113$ prímszámmal teljesül, hogy

$$\begin{aligned} f(x) &\equiv (x+111)^4(x+81)(x^4 + 32x^3 + 7x^2 + 111x + 49) \pmod{113}, \\ g(x) &\equiv (x+11)^5(x+56)(x^2 + 57x + 85) \pmod{113}, \end{aligned}$$

ezért a 2. Tétel alkalmazható. Tekintsük a $K = \mathbb{Q}(\varphi, \psi)$ 72-ed fokú test $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ rendjét. Tetszőleges $\alpha \in \mathcal{O}_{fg}$ megadható az

$$\alpha = \sum_{i=0}^{8} \sum_{j=0}^{7} x_{ij} \varphi^i \psi^j$$

alakban, ahol $x_{ij} \in \mathbb{Z}$. A 2. Tétel alapján a $\mathcal{O}_{fg}$ rend minden primitív elemének indexe osztható 113-mal, ezért az $\mathcal{O}_{fg}$ rendben nincs hatvány egész bázis.

1.4. Kongruencia feltételek I

Bizonyos speciális esetekben, amikor a 3. Tétel feltételei nem teljesülnek, meg tudunk adni egy elégséges kongruencia feltételt, melynek teljesülése esetén a megfelelő rendek

kompozítumaiban nincs hatvány egész bázis. A következő szakaszokban két ilyen tipusú eredményt részletezünk.

Először, tegyük fel, hogy léteznek olyan négyzetmentes $p, q \in \mathbb{Z}$ számok, hogy

$$f(x) \equiv x^m \pmod{p}, \tag{7}$$

vagy

$$g(x) \equiv x^n \pmod{q}. \tag{8}$$

Ekkor a következő tételt kapjuk (lásd [10]):

4. Tétel. *(Gaál I., Olajos P., [10])*
Feltételezzük, hogy az $\mathcal{O}_{fg}$ rendben létezik hatvány egész bázis.
Ha a (7) teljesül, akkor

$$(d(g))^{m(m-1)/2} \equiv \pm 1 \pmod{p}. \tag{9}$$

Ha (8) teljesül, akkor

$$(d(f))^{n(n-1)/2} \equiv \pm 1 \pmod{q}. \tag{10}$$

5. Tétel. *(Gaál I., Olajos P., [10])*
Ha a (7) és a (8) feltételek teljesülnek és a (9) és a (10) feltételek közül valamelyik nem teljesül, akkor $\mathcal{O}_{fg}$ rendben nincs hatvány egész bázis.

3. Megjegyzés. Ez a tétel egy egyszerű szükséges feltételt ad meg hatvány egész bázis létezésével kapcsolatban. Ha a (9) és a (10) kongruenciák teljesülnek és a diszkriminánsok relatív prímek (ez azt jelenti, hogy nem alkalmazhatjuk a 3. Tételt), akkor az elemek megkereséséhez alkalmaznunk kell a 1. Tételt. De sok esetben, amikor a 4. Tétel teljesül és a diszkriminánsok relatív prímek, megtakarítunk sok számolást, mert nem kell megoldanunk a 1. Tétel (4) és (5) egyenleteit.

1.4.1. A 5. Tétel alkalmazásai

A példákban ugyanolyan értelemben használjuk az $\mathcal{O}_L$ és az $\mathcal{O}_M$ polinomrendeket, mint a 2. Tételben, és hasonlóan az $\mathcal{O}_K = \mathcal{O}_L\mathcal{O}_M$.

I. Példa

Legyenek a p, q négyzetmentes egészek (≥ 2). Az egyik leglényegesebb és leggyakoribb alkalmazása a 5. Tételnek az az eset, amikor $f(x) = x^m - p$ és $g(x) = x^n - q$. Feltételezzük, hogy a $K = \mathbb{Q}(\sqrt[m]{p}, \sqrt[n]{q})$ test foka mn. Ebben az esetben a

$$\begin{aligned} d(f) &= (-1)^{(m-1)(m-2)/2} \cdot m^m \cdot p^{m-1}, \\ d(g) &= (-1)^{(n-1)(n-2)/2} \cdot n^n \cdot q^{n-1}. \end{aligned}$$

A 5. Tétel felhasználásval, ha a

$$\left(n^n \cdot q^{n-1}\right)^{m(m-1)/2} \equiv \pm 1 \pmod{p},$$

$$\left(m^m \cdot p^{m-1}\right)^{n(n-1)/2} \equiv \pm 1 \pmod{q}$$

kongruenciák közül valamelyik nem teljesül, akkor az $\mathcal{O}_K = \mathbb{Z}[\sqrt[m]{p}, \sqrt[n]{q}]$ rendben nincs hatvány egész bázis.

I.1. Abban a speciális esetben, ha $m = 3,\ n = 2$, a $K = LM$ test egy hatodfokú algebrai számtest. Ekkor a $d(f) = D_{\mathcal{O}_L} = -27 \cdot p^2, d(g) = D_{\mathcal{O}_M} = 4 \cdot q$.

A fenti kongruenciák a

$$\begin{aligned} 64 \cdot q^3 &\equiv \pm 1 \pmod{p}, \\ -27 \cdot p^2 &\equiv \pm 1 \pmod{q} \end{aligned}$$

alakúak.

Ha például a $p = 7,\ q = 5$, akkor

$$(D_{\mathcal{O}_L}, D_{\mathcal{O}_M}) = 1,$$

ezért a 1. Tétel alkalmazható lenne. Ekkor a

$$\begin{aligned} 64 \cdot 5^3 = 8000 \equiv 6 \equiv -1 \pmod{7}, \\ -27 \cdot 7^2 = -1323 \equiv 2 \equiv -3 \pmod{5}. \end{aligned}$$

A 5. Tételből következik, hogy nincs hatvány egész bázis az $\mathcal{O}_K$-ban.

I.2. Abban a speciális esetben, amikor $m = 22,\ n = 15$ és $[K : \mathbb{Q}] = 22 \cdot 15 = 330$ azt kapjuk, hogy

$$d(f) = D_{\mathcal{O}_L} = 22^{22} \cdot p^{21},\ \ d(g) = D_{\mathcal{O}_M} = -15^{15} \cdot q^{14}.$$

Ha például a $p = 31,\ q = 17$, akkor

$$(D_{\mathcal{O}_L}, D_{\mathcal{O}_M}) = 1,$$

ezért a 1. Tétel alkalmazható lenne. De a 5. Tétel alkalmazásával, vagy a

$$(-15^{15} \cdot 17^{14})^{231} \equiv 4 \equiv -27 \pmod{31}$$

vagy a

$$(22^{22} \cdot 31^{21})^{105} \equiv 10 \equiv -7 \pmod{17}$$

kongruenciából következik, hogy nincs hatvány egész bázis az $\mathcal{O}_K$-ban.

II. Példa

Tekintsünk egy a fentitől különböző példát: legyen $f(x) = x^5 - p^3x^3 - p^2x^2 - px - p$ and $g(x) = x^3 - q^2x^2 - qx - q$ $(m = 5,\ n = 3)$. Ha az $\mathcal{O}_K$ rendelkezik hatvány egész bázissal, akkor a következő kongruenciáknak kell teljesülniük:

$$d(g)^{10} \equiv \pm 1 \pmod{p},$$

$$d(f)^3 \equiv \pm 1 \pmod{q},$$

ahol a

$$d(g) = -q^2(-4q - q^4 + 18q^2 + 4q^5 + 27)$$

és

$$d(f) = -p^4(108p^{13} - 56p^{12} + 12p^{11} + 75p^8 - 38p^7 + 11p^6 - 3750p^4 + 4250p^3 - 1600p^2 + 256p - 3125).$$

Ha ezen kongruenciák valamelyike nem teljesül, akkor az $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$ (az α és a β rendre gyökei az f, g-nek) rendben nincs hatvány egész bázis.

II.1. Legyen a $p = 7,\ q = 29$. Ekkor $[K : \mathbb{Q}] = 5 \cdot 3 = 15$, és ekkor azt kapjuk, hogy

$$d(f) = D_{\mathcal{O}_L} = -23320969892806663 = -(7)^4(11)^2(5208131)(15413),$$

$$d(g) = D_{\mathcal{O}_M} = -68417338124 = -(2)^2(29)^2(41)(496051)$$

és

$$(D_{\mathcal{O}_L}, D_{\mathcal{O}_M}) = 1,$$

ezért a 1. Tétel alkalmazható lenne. De a 5. Tétel alkalmazásával, vagy a

$$d(g)^{10} \equiv 2 \equiv -5 \pmod{7}$$

vagy a

$$d(f)^3 \equiv 6 \equiv -23 \pmod{29}$$

kongruenciából következik, hogy nincs hatvány egész bázis az $\mathcal{O}_K$-ban.

1.5. Kongruencia feltételek II

Ebben a szakaszban feltételezzük, hogy létezik egy olyan négyzetmentes$q$ egész szám, hogy az f egy teljes hatvány modulo q, azaz

$$f(x) \equiv (x - t)^m \pmod{q} \tag{11}$$

valamilyen $t \in \mathbb{Z}$-re.

Az eredményünk a következő:

6. Tétel. *(Olajos P., [31])*
Ha létezik hatvány egész bázis az $\mathcal{O}_{fg}$-ben, akkor teljesül a

$$(d(g))^{m(m-1)} \equiv \pm 1 \pmod{q} \tag{12}$$

kongruencia.

Következményként kapjuk, hogy:

7. Tétel. *(Olajos P., [31])*
Ha teljesül a (11) és nem teljesül a (12), akkor az $\mathcal{O}_{fg}$ rendben nincs hatvány egész bázis.

4. Megjegyzés. Ha a $(d(g), d(f)) = 1$, akkor az 1.1 szakasz alkalmazása komplikált magasabb fokú testekre. Ha teljesül a (11) feltétel, akkor magasabb fokú testekben is le tudunk vonni következtetést hatvány egész bázis létezésére vonatkozóan.

5. Megjegyzés. A $d = (d(f), d(g)) \neq 1$ esetet már vizsgáltuk az 1.3 szakaszban. Ebben az esetben az f és g rendelkezik egy többszörös gyökkel modulo q, ahol a q egy prímosztója a d-nek. A fenti eredmény egy szükséges feltételt ad hatvány egész bázis létezésére vonatkozóan abban az esetben, amikor a 3. Tétel nem alkalmazható.

1.5.1. A 7. Tétel alkalmazásai

I. Példa Teljesen valós, ciklikus, hatodfokú testek egy parametrikus családja.

A 7. Tétel egyik legérdekesebb alkalmazása az az eset, amikor

$$f(x) = x^3 - (a+1)x^2 + (a+2)x + 1,$$

$$g(x) = x^2 - ax - 1$$

ahol $a \in \mathbb{Z}$ paraméter $(m = 3, n = 2)$. Ezt a családot O. Lecacheux [24] vizsgálta, amely a jelenlegi eredményünkhöz kiindulásként szolgált. Ekkor azt kapjuk, hogy

$$d(f) = (a^2 - a + 7)^2,$$

$$d(g) = a^2 + 4.$$

Tekintsük az f polinomot. Ebben az esetben teljesül, hogy

$$f(x) - \left(x - \frac{a+1}{3}\right)^3 = \frac{1}{27} \cdot (a^2 - a + 7) \cdot (a + 4 - 9x).$$

Legyen $q = a^2 - a + 7$ és tegyük fel, hogy q négyzetmentes. Ha az $a \equiv 2 \pmod 3$, akkor a $(q, 9) = 9$. Emiatt azt a családot vizsgáljuk, amikor $a \equiv 0, 1 \pmod 3$. Ekkor $(q, 3) = 1$, amely azt jelenti, hogy az

$$f(x) \equiv \left(x - \frac{a+1}{3}\right)^3 \pmod{q}. \tag{13}$$

Felhasználva a (13) kongruenciát és a 6. Tételt, ha létezik hatvány egész bázis az $\mathcal{O}_{fg}$-ban, akkor teljesül a következő:

$$(a^2+4)^6 \equiv (a-3)^6 \equiv \pm 1 \pmod{q}. \tag{14}$$

A megoldások megtalálására a Maple-t alkalmazva kapjuk a következőt:

ha az $a \notin [-840, 840]$, akkor nem teljesül a (14), ezért a 7. Tétel alapján nincs hatvány egész bázis az $\mathcal{O}_{fg}$-ban.

Megvizsgálva az $|a| < 840$ értékeket, a (12) csak akkor teljesülhet, ha

$$a = -15, -2, 1, 4.$$

II. Példa

Egy másik alkalmazása a 7. Tételnek az az eset, amikor

$$f(x) = x^5 + a^2x^4 - (2a^3 + 6a^2 + 10a + 10)x^3 +$$

$$(a^4 + 5a^3 + 11a^2 + 15a + 5)x^2 + (a^3 + 4a^2 + 10a + 10)x + 1,$$

$$g(x) = x^2 - ax - 1$$

ahol $a \in \mathbb{Z}$ paraméter ($m = 5, n = 2$). Az f egyik gyöke által generált teljesen valós, ciklikus, ötödfokú családot E. Lehmer [25] vizsgálta, lásd még vö. Gaál I. és M. Pohst [14]. Ebben az esetben

$$d(g) = a^2 + 4.$$

Tekintsük az f polinomot. Legyen a $q = a^4 + 5a^3 + 15a^2 + 25a + 25$ és tegyük fel, hogy a q négyzetmentes. Ekkor teljesül, hogy

$$f(x) \equiv \left(x + \frac{a^2}{5}\right)^5 \pmod{q}. \tag{15}$$

Felhasználva a (15) kongruenciát és a 6. Tételt, ha létezik hatvány egész bázis az $\mathcal{O}_{fg}$-ben, akkor teljesül az

$$(a^2+4)^{20} \equiv \pm 1 \pmod{q} \tag{16}$$

kongruencia. A Maple felhasználásával azt kapjuk, hogy ha $a > 2.4 \cdot 10^{16}$, akkor nem teljesül a (16), ezért a 7. Tétel miatt nincs hatvány egész bázis az $\mathcal{O}_{fg}$-ben.

2. Legegyszerűbb negyedfokú testek

2.1. Legegyszerűbb negyedfokú testek

Legyen $t \in \mathbb{Z} \setminus \{0, \pm 3\}$ és tekintsük a

$$P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1. \tag{17}$$

polinom $\xi = \xi_t$ gyökét. A $K_t = K = \mathbb{Q}(\xi)$ végtelen parametrikus családot *legegyszerűbb negyedfokú testeknek* nevezik. A K legegyszerűbb negyedfokú test egy teljesen valós, ciklikus, negyedfokú test. Ha a $t = 0$ vagy a $t = \pm 3$, akkor a $P_t(x)$ nem irreducibilis a $\mathbb{Q}$ felett.

Ha a ξ gyöke a (17)-nak, akkor a $\frac{\xi-1}{\xi+1}$ is gyöke a (17)-nak. Így az $x \mapsto \frac{x-1}{x+1}$ racionális leképezés permutálja a (17) gyökeit és a $K = \mathbb{Q}(\xi)$ egy negyedfokú valós számtest, melynek ciklikus Galois csoportja a $G = \langle \sigma \rangle$, amelyet a $\sigma : \xi \mapsto \frac{\xi-1}{\xi+1}$ automorfizmus generál. A "legegyszerűbb" negyedfokú számtestet vizsgálták: M. N. Gras [17], lásd még G. Lettl és A. Pethő [26] és G. Lettl, A. Pethő és P. Voutier [28].

Ennek a fejezetnek az a célja, hogy a K_t-ben parametrikus formában megadjuk az összes hatvány egész bázist.

2.2. Hatvány egész bázis a legegyszerűbb negyedfokú testekben

Legyen ismét a $\xi = \xi_t$ a $P_t(x)$ gyöke a (17)-ban és a $K = K_t = \mathbb{Q}(\xi_t)$.

A legegyszerűbb negyedfokú testek összes hatvány egész bázis generátor elemének megtalálásához két lemmára van szükségünk.

Megjegyezzük, hogy a $\mathbb{Q}(\alpha) = \mathbb{Q}(-\alpha)$ (α egy algebrai egész), azaz feltételezzük, hogy a $t > 0$ és a $t \neq 3$. A továbbiakban tegyük fel azt is, hogy a t^2+16 nem osztható egy páratlan négyzetszámmal. Továbbá jelölje a $v_2(t)$ a t 2-szerinti értékelését. A K egész bázisát az utóbbi időben explicite meghatározták.

1. Lemma. *(H. K. Kim and J. S. Kim, [23])*
A $K = K_t$ egy egész bázisa a következő módon adható meg.

$$\mathcal{O}_{\mathcal{K}} = \begin{cases} [1, \xi, \xi^2, \frac{1+\xi^3}{2}] & \text{if } v_2(t) = 0, \\ [1, \xi, \frac{1+\xi^2}{2}, \frac{\xi+\xi^3}{2}] & \text{if } v_2(t) = 1, \\ [1, \xi, \frac{1+\xi^2}{2}, \frac{1+\xi+\xi^2+\xi^3}{4}] & \text{if } v_2(t) = 2, \\ [1, \xi, \frac{1+2\xi-\xi^2}{4}, \frac{1+\xi+\xi^2+\xi^3}{4}] & \text{if } v_2(t) \geq 3. \end{cases}$$

Ezen fejezet legfontosabb eredménye:

8. Tétel. *(Olajos P., [32]) A $K = K_t$ legegyszerűbb negyedfokú testek $\mathbb{Z}_K$ egészeinek gyűrűje csak a $t = 2$ és a $t = 4$ esetén rendelkezik hatvány egész bázissal. Ezekben az esetekben az összes hatvány egész bázis generátor elem a következö:*

$t = 2,\ \alpha = x \cdot \xi + y \cdot \frac{1+\xi^2}{2} + z \cdot \frac{\xi+\xi^3}{2}$, *ahol*
$(x, y, z) = (4, 2, -1), (-13, -9, 4), (-2, 1, 0), (1, 1, 0), (-8, -3, 2),$
$(-12, -4, 3), (0, -4, 1), (6, 5, -2), (-1, 1, 0), (0, 1, 0).$

$t = 4,\ \alpha = x \cdot \xi + y \cdot \frac{1+\xi^2}{2} + z \cdot \frac{1+\xi+\xi^2+\xi^3}{4}$, *ahol*
$(x, y, z) = (3, 2, -1), (-2, -2, 1), (4, 8, -3), (-6, -7, 3), (0, 3, -1),$
$(1, 3, -1).$

A fő tétel bizonyításához a következő, negyedfokú testekben hatvány egész bázis megtalálására vonatkozó általános módszert alkalmazzuk.

Jelölje az $f(x) = x^4+a_1x^3+a_2x^2+a_3x+a_4$ a $K = \mathbb{Q}(\xi)$ a negyedfokú test generáló elemének minimál polinomját. Feltételezzük, hogy tetszőleges$\alpha \in \mathbb{Z}_K$ megadható az

$$\alpha = \frac{a + x\xi + y\xi^2 + z\xi^3}{g} \tag{18}$$

alakban, ahol $a, x, y, z \in \mathbb{Z}$, és a $g \in \mathbb{Z}$ rögzített, közös nevező. Legyen

$$\begin{aligned} F(u,v) &= u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3, \\ Q_1(x,y,z) &= x^2 - a_1xy + a_2y^2 + (a_1^2 - 2a_2)xz + \\ &+ (a_3 - a_1a_2)yz + (-a_1a_3 + a_2^2 + a_4)z^2, \\ Q_2(x,y,z) &= y^2 - xz - a_1yz + a_2z^2, \end{aligned}$$

és tekintsük az

$$I(\alpha) = m \tag{19}$$

egyenletet, ahol $\alpha \in \mathbb{Z}_K,\ m \in \mathbb{Z}$.

2. Lemma. *(Gaál I., Pethő I., M. Pohst, [11], lásd még [8])*
Az $\alpha \in \mathbb{Z}_K$ elem, amely a (18) alakban van megadva akkor és csak akkor megoldása a (19)-nak , ha létezik egy olyan $(u, v) \in \mathbb{Z}^2$ megoldása az

$$F(u,v) = \pm\frac{g^6m}{I(\xi)} = \pm i_m \tag{20}$$

egyenletnek, hogy a

$$Q_1(x,y,z) = u, \tag{21}$$

$$Q_2(x,y,z) = v. \tag{22}$$

3. Hatodfokú parametrikus család

3.1. Korábbi eredmények

Legyen a ϑ egy teljesen valós, harmadfokú algebrai egész és legyen az m egy négyzetmentes pozitív egész szám. Tekintsük a $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ hatodfokú testet, jelölje a D_K a test diszkriminánst és $\mathbb{Z}_K$ egészek gyűrűjét. Legyen az $M = \mathbb{Q}(i\sqrt{m})$ és az $L = \mathbb{Q}(\vartheta)$ a K résztestei. Legyen

$$\omega = \begin{cases} (1+\mathrm{i}\sqrt{m})/2, & \text{if } -m \equiv 1 \pmod 4 \\ \mathrm{i}\sqrt{m}, & \text{if } -m \equiv 2,3 \pmod 4. \end{cases} \tag{23}$$

Tetszőleges $\alpha \in \mathbb{Z}_K$ elemet megadhatunk az

$$\alpha = \frac{x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2}{g} \tag{24}$$

alakban, ahol $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$ és a $g \in \mathbb{Z}$ rögzített, közös nevező.
Legyen az $\mathcal{O} = \mathbb{Z}[1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2]$ és jelölje a $D_\mathcal{O}$ ezen rend diszkriminánsát. Vizsgálni fogjuk a hatvány egész bázis létezését és még általánosabban adott indexű elemek létezését az $\mathcal{O}$ rendben, amely gyakran egybeesik a $\mathbb{Z}_K$-val. Ekkor teljesül, hogy

$$\frac{g^6\sqrt{|D_K|}}{\sqrt{|D_\mathcal{O}|}} \in \mathbb{Z}.$$

Tekintsük az I_0 nem nulla, pozitív egész számot és az

$$I(\alpha) = I_0 \tag{25}$$

egyenlet $\alpha \in \mathbb{Z}_K$ megoldásait.

Legyen

$$I_1 = \frac{g^{15} I_0 \sqrt{|D_K|}}{\sqrt{|D_\mathcal{O}|}} \in \mathbb{Z}.$$

Jelölje a ϑ_i $(1 \le i \le 3)$ a ϑ M feletti konjugáltjait és legyen $\rho = -\vartheta_2 - \vartheta_3$.

3. Lemma. *(Gaál I., [3])*
Ha az $\alpha \in \mathbb{Z}_K$ az (25) egyenlet megoldása és az $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$ az α (24)-beli megadásának együtthatói, akkor

$$N_{K/M}((x_1 + \omega y_1) - \rho(x_2 + \omega y_2)) = \mu, \tag{26}$$
$$N_{L/Q}(y_0 + y_1\vartheta + y_2\vartheta^2) = d, \tag{27}$$

ahol a $\mu \in \mathbb{Z}_M$, $d \in \mathbb{Z}$, melyekre $d \cdot N_{M/Q}(\mu)$ osztja I_1-et.

A K testre vonatkozó feltételek mellett, jelölje a $\rho = \rho_1,\ \rho_2,\ \rho_3$ a ρ L feletti konjugáltjait és legyen az $X = x_1 + \omega y_1,\ Y = x_2 + \omega y_2$ egy tetszőleges , de rögzített megoldása az (26)-nek. Válasszuk meg az $\{r,\ s,\ t\} = \{1,\ 2,\ 3\}$ indexeket aszerint, hogy teljesüljön a következő:

$$|X - \rho_r Y| \leq |X - \rho_s Y| \leq |X - \rho_t Y|. \tag{28}$$

Legyen

$$c_m = \begin{cases} 2, & \text{if } -m \equiv 1 \pmod 4 \\ 1, & \text{if } -m \equiv 2, 3 \pmod 4 \end{cases}$$

$$\begin{aligned} c_1 &= 9c_m^3|\mu|, \\ c_2 &= \min(|\rho_r - \rho_s|,\ |\rho_r - \rho_t|), \\ c_3 &= |\rho_r - \rho_s| \cdot |\rho_r - \rho_t| \end{aligned}$$

$$c_4 = \max\left\{ \frac{2|\mu|^{1/3}}{c_2}, \frac{4c_m|\mu|}{c_3\sqrt{m}} \right\}, c_5 = \left(\frac{8|\mu|}{c_2 c_3} \right)^{1/3}.$$

Végül legyen

$$F(x, y) = \prod_{j=1}^{3} (x - \rho_j y) \in \mathbb{Z}[x, y].$$

Ezen feltételek mellett érvényes a következő állítás:

4. Lemma. *(Gaál I.,[3])*
Legyen az $X = x_1 + \omega y_1,\ Y = x_2 + \omega y_2 \in \mathbb{Z}_M$ az (26) egy megoldása a (28) szerint. Feltételezzük, hogy $|Y| > c_4$. Ekkor teljesül, hogy

$$x_1 y_2 = x_2 y_1.$$

Továbbá, az $-m \equiv 1 \pmod 4$ esetben:

$$\begin{cases} \text{if } |2x_2 + y_2| \geq 2c_5, & \text{then } |F(2x_1 + y_1, 2x_2 + y_2)| \leq c_1 \\ \text{if } |y_2| \geq 2c_5/\sqrt{m}, & \text{then } |F(y_1, y_2)| \leq c_1/(\sqrt{m})^3, \end{cases}$$

és a $-m \equiv 2, 3 \pmod 4$ esetben:

$$\begin{cases} \text{if } |x_2| \geq 2c_5, & \text{then } |F(x_1, x_2)| \leq c_1, \\ \text{if } |y_2| \geq c_5/\sqrt{m}, & \text{then } |F(y_1, y_2)| \leq c_1/(\sqrt{m})^3. \end{cases}$$

6. Megjegyzés. A [3]-ban olyan $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ testeket vizsgáltak, ahol a ϑ az $f(x) = x^3 - ax^2 - (a + 3)x - 1$ gyöke és az m egy négyzetmentes, pozitív egész. A [3]-nak a Theorem 3.1 felhasználásával kapjuk, hogy ha az $a \geq 3$ és $m \geq m_0$, akkor a K $\mathcal{O}$ rendjében nincs hatvány egész bázis.

3.2. Eredmények

Legyen az

$$f_n(x) = x^3 - nx^2 - (n+1)x - 1, \tag{29}$$

ahol $n \in \mathbb{N}$. Ha az $n \geq 3$, akkor az $f_n(x)$ teljesen valós. Legyen a $\vartheta = \vartheta_n$ az $f_n(x)$ gyöke és legyen az m egy négyzetmentes, pozitív egész. Tekintsük a teljesen komplex, hatodfokú testek kétparaméteres $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ családját. Definiáljuk az ω-t, úgy mint a (23)-ban és legyen az $\mathcal{O} = \mathbb{Z}[1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2]$ rend diszkriminánsa a $D_{\mathcal{O}}$, mint korábban. Használjuk az $L = \mathbb{Q}(\vartheta)$ és az $M = \mathbb{Q}(i\sqrt{m})$ jelöléseket is. Legyen az

$$m_0 = \begin{cases} 36, & \text{if } -m \equiv 1 \pmod 4, \\ 9, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

9. Tétel. *(Olajos P., [30])*
Tegyük fel, hogy az $n \geq 7$ és az $m \geq m_0$. Ekkor az $\mathcal{O}$ rendben nincs hatvány egész bázis.

Ezen tétel bizonyítása a [3]-hoz hasonló módszert használ, de mi a kis paramétereket is vizsgáljuk. Ez azt jelenti, hogy foglalkozni fogunk azokkal az esetekkel, amelyek nem teljesítik az $n \geq 7$-et vagy az $m \geq m_0(n)$-et. Megjegyezzük, hogy ha az $n \leq 2$, akkor a (29) nem teljesen valós, így végül is csak azokkal az esetekkel kell foglalkoznunk, amikor az $n = 3,\ 4,\ 5,\ 6$. A 9. Tétel bizonyításában felhasznált hasonló eszközökkel megmutatható, hogy az $m \geq m_o(n)$ esetben az $\mathcal{O}$ rendben nincs hatvány egész bázis.

10. Tétel. *(Olajos P., [30])*
Legyen

$$m_0(3) = \begin{cases} 143, & \text{if } -m \equiv 1 \pmod 4, \\ 36, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

$$m_0(4) = \begin{cases} 59, & \text{if } -m \equiv 1 \pmod 4, \\ 15, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

$$m_0(5) = \begin{cases} 42, & \text{if } -m \equiv 1 \pmod 4, \\ 11, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

$$m_0(6) = \begin{cases} 36, & \text{if } -m \equiv 1 \pmod 4, \\ 9, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

Az $n = 3,\ 4,\ 5,\ 6$, $m \geq m_o(n)$ esetben az $\mathcal{O}$ rendben nincs hatvány egész bázis.

Továbbá, az $n = 3,\ 4,\ 5,\ 6$ esetben az m kis értékeire vonatkozó közvetlen számolás eredményeképpen kapjuk:

11. Tétel. *(Olajos P., [30])*
Ha az $n = 3,\ 4,\ 5,\ 6$ és a $2 \leq m_0 < m_0(n)$, akkor az $\mathcal{O}$ rendben nincs hatvány egész bázist .

Introduction

Consider an algebraic number field K of degree n with ring of integers $\mathbb{Z}_K$. An interesting problem in algebraic number theory is to decide if there exists an element α in K such that

$$1, \alpha, \alpha^2, ..., \alpha^{n-1}$$

is an integral basis, that is a *power integral basis*. The ring $\mathbb{Z}_K$ of integers is called *monogenic*, if K admits power integral bases. Another problem is to find all elements α which generate power integral bases in K.

The index of a primitive element $\alpha \in \mathbb{Z}_K$ is defined by

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

Then we have

$$I(\alpha) = \frac{\prod_{1 \le j < k \le n} |\alpha^{(j)} - \alpha^{(k)}|}{\sqrt{|D_K|}}, \tag{1}$$

where D_K is the discriminant of K.

As it is well known α generates a power integral basis if and only if $I(\alpha) = 1$.

Let $\{1, \omega_2, ..., \omega_n\}$ be an arbitrary integral basis of K. Then the discriminant of the linear form

$$l(x) = x_1 + x_2\omega_2 + ... + x_n\omega_n$$

is equal to

$$D_{K/\mathbb{Q}}(l(x)) = \prod_{1 \le i < j \le n} (l^{(i)}(x) - l^{(j)}(x))^2 = I(x_2, ..., x_n)^2 D_K,$$

where $x = (x_1, x_2, ..., x_n) \in \mathbb{Z}^n$ and $I(x_2, ..., x_n)$ is a homogeneous form of degree $\frac{n(n-1)}{2}$ in $n-1$ variables with coefficients in $\mathbb{Z}$ called *the index form* corresponding to the integral basis $\{1, \omega_2, ..., \omega_n\}$.

Representing any α of $\mathbb{Z}_K$ in the form $\alpha = x_1 + \omega_2 x_2 + ... + \omega_n x_n$ we have

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

that is the index of α is independent from the first coordinate of α. That is we have to solve the following equation to find all generators of power integral bases:

$$I(x_2, ..., x_n) = \pm 1 \text{ (in } x_2, \ldots, x_n \in \mathbb{Z}). \tag{2}$$

In 1976 K. Győry (see [18], [20] and [19]) gave the first general effective upper bounds for the solutions of index form equations using Baker's method (see also [21] for recent improvements). It means that we have only finitely many solutions of the equation (2).

In the last decade several authors were interested in constructing algorithms for solving index form equations. There are efficient algorithms for determining all generators of power integral bases in lower degree number fields cf. I. Gaál and N. Schulte [16] for cubic fields, I. Gaál, A. Pethő and M. Pohst [11] for quartic fields. A general algorithm for quintic and sextic fields was given by I. Gaál and K. Győry [9] and Y. Bilu, I. Gaál and K. Győry [1], which already requires several hours of CPU time. For algorithms for solving index form equations in certain special sextic, octic, nonic fields see I. Gaál [3], I. Gaál [5], I. Gaál and M. Pohst [13], I. Járási [22]. A complete description of algorithms for solving equation (2) and several connected results can be found in the monograph I. Gaál [8].

I

For higher degree number fields this problem is very complicated because of the high degree and large number of variables in equation (2). The resolution of the equation (2) is only hopeful if K is a composite of certain subfields, because in this case the index form is reducible. Interesting and well applicable necessary conditions are known for the existence of power integral bases. The purpose of the first chapter is to give a summary of these results in composite fields. We consider several applications of these results.

II

In this chapter we give all generators of power integral bases in the infinite parametric family of simplest quartic fields.

Let $t \in \mathbb{Z}$ and α be a root of $P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1$ and consider the infinite parametric family of number fields $K_t = K = \mathbb{Q}(\alpha)$. These fields K are totally real cyclic number fields of degree 4 and are called "simplest" quartic fields. Several authors have considered the infinite parametric family of simplest quartic fields K(see [17],[26] and [28]). The generators of power integral bases of the polynomial ring $\mathbb{Z}[\alpha]$ have already been described. In our case under certain conditions on t we explicitly give all generators of power integral bases in the ring of integers$\mathbb{Z}_K$ of K.

III

In the third chapter similarly to the first chapter we consider a parametric family of degree 6 which has a special structure. We know that if a sextic field has a quadratic subfield, then a factor of the index form leads to a relative Thue equation over the quadratic subfield. Algorithms for the resolution of index form equations in totally real cyclic sextic fields are developed by I. Gaál [4], in sextic fields with an imaginary quadratic subfield by I. Gaál and M. Pohst [13].

In this chapter we analyse the problem of determining elements of given index in a special infinite parametric family of sextic number fields with imaginary quadratic

subfields, having also a totally real cubic subfield. Using results of I. Gaál [3] our problem can be reduced to solving cubic Thue inequalities over $\mathbb{Z}$. Fast algorithms are known for solving cubic (or higher degree) Thue equations or inequalities (see [2]). Moreover, using direct computations we also deal with those fields in the family which correspond to small parameters and are not covered by the main theorem.

1 Composite fields

1.1 Coprime discriminants

Let L be a number field of degree r with integral basis $\{l_1 = 1, l_2, \ldots, l_r\}$ and discriminant D_L. Denote the index form corresponding to the integral basis $\{l_1 = 1, l_2, \ldots, l_r\}$ of L by $I_L(x_2, \ldots, x_r)$. Similarly, let M be a number field of degree s with integral basis $\{m_1 = 1, m_2, \ldots, m_s\}$ and discriminant D_M. Denote the index form corresponding to the integral basis $\{m_1 = 1, m_2, \ldots, m_s\}$ of M by $I_M(x_2, \ldots, x_s)$. Let $K = LM$ the composite of L and M. As it is known, if $(D_L, D_M) = 1$ the discriminant of K is

$$D_K = D_L^s \cdot D_M^r$$

and an integral basis of K is given by

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

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

$$\alpha = \sum_{i=1}^{r} \sum_{j=1}^{s} x_{ij} \cdot l_i \cdot m_j \tag{3}$$

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

I. Gaál [5] formulated a general necessary condition for $\alpha \in \mathbb{Z}_K$ to be a generator of a power integral basis of K.

Theorem 1. *(I. Gaál, [5])*
Assume $(D_L, D_M) = 1$. *If* α *of (3) generates a power integral basis in* $K = LM$ *then*

$$N_{M/Q}\left(I_L\left(\sum_{i=1}^{s} x_{2i} \cdot m_i, \ldots, \sum_{i=1}^{s} x_{ri} \cdot m_i\right)\right) = \pm 1 \tag{4}$$

and

$$N_{L/Q}\left(I_M\left(\sum_{i=1}^{r} x_{i2} \cdot l_i, \ldots, \sum_{i=1}^{r} x_{is} \cdot l_i\right)\right) = \pm 1. \tag{5}$$

1.1.1 Applications of Theorem 1

Example: Field of degree nine with cubic subfields (see I. Gaál [7]).

Let f, g be monic, irreducible cubic polynomials with integer coefficients. Denote one of the roots of f and g by ϕ and ψ, respectively. Let us consider the algebraic number fields $L = \mathbb{Q}(\phi)$ and $M = \mathbb{Q}(\psi)$. Using the assumptions above the following cases were considered in [7]:

1. $f(x) = x^3 - x + 1,\ D_L = -23, \quad g(x) = x^3 - 2x + 2,\ D_M = -76$
2. $f(x) = x^3 + x + 1,\ D_L = -31, \quad g(x) = x^3 + x^2 + x + 2,\ D_M = -83$
3. $f(x) = x^3 + 2x + 1,\ D_L = -59, \quad g(x) = x^3 + x^2 - 2x - 3.\ D_M = -87$

Using Theorem 1 it was shown that there are no generators of power integral bases in the composite field $K = LM$. In these cases (4) and (5) yield relative Thue equations.

1.2 Notation

In the subsections below we will use the following notation:
Let $f, g \in \mathbb{Z}[x]$ be distinct monic irreducible polynomials (over $\mathbb{Q}$) of degrees m and n, respectively. Let φ be a root of f and let ψ be a root of g. Set $L = \mathbb{Q}(\varphi)$, $M = \mathbb{Q}(\psi)$ and assume that the composite field $K = LM$ has degree mn. Denote by $d(f)$ and $d(g)$ the discriminants of the polynomials f and g, respectively.

Consider the order $\mathcal{O}_f = \mathbb{Z}[\varphi]$ of the field L, the order $\mathcal{O}_g = \mathbb{Z}[\psi]$ of the field M and the composite order $\mathcal{O}_{fg} = \mathcal{O}_f\mathcal{O}_g = \mathbb{Z}[\varphi, \psi]$ in the composite field $K = ML$. Note that $\{1, \varphi, \ldots, \varphi^{m-1}\}$, $\{1, \psi, \ldots, \psi^{n-1}\}$ and

$$\{1, \varphi, \ldots, \varphi^{m-1}, \psi, \varphi\psi, \ldots, \varphi^{m-1}\psi, \ldots, \psi^{n-1}, \varphi\psi^{n-1}, \ldots, \varphi^{m-1}\psi^{n-1}\},$$

are $\mathbb{Z}$-bases of $\mathcal{O}_f$, $\mathcal{O}_g$ and $\mathcal{O}_{fg}$, respectively.

1.3 Non-coprime discriminants

If the condition of Theorem 1 is satisfied then we have to solve equations (4) and (5) which can be very complicated. But we can give other sufficient conditions for the non-existence of power integral basis.

Assume that there is a prime number q, $(q > 2)$ such that both f and g have a multiple linear factor (at least square) $\bmod q$, that is, there exist a_f and a_g in $\mathbb{Z}$ such that

$$\begin{array}{rcccl} f(a_f) & \equiv & f'(a_f) & \equiv & 0 \pmod{q}, \\ g(a_g) & \equiv & g'(a_g) & \equiv & 0 \pmod{q}. \end{array} \tag{6}$$

Remark 1. Our assumption implies that q divides both the discriminant $d(f)$ of the polynomial f and the discriminant $d(g)$ of g.

Remark 2. In [5] we considered fields that are composites of subfields with coprime discriminants. According to the remark above in our case the fields we consider are composites of subfields whose discriminants are not necessarily coprime. This is the case in many interesting examples some of which we list at the end of this section.

Our result is the following (see [15]):

Theorem 2. *(I. Gaál, P. Olajos, M. Pohst, [15])*
Under the assumptions above the index of any primitive element of the order $\mathcal{O}_{fg}$ is divisible by q.

As a consequence we have:

Theorem 3. *(I. Gaál, P. Olajos, M. Pohst, [15])*
Under the assumptions above the order $\mathcal{O}_{fg}$ has no power integral bases.

1.3.1 Applications of Theorem 3

Example I. A cyclic sextic field

Consider the sextic field K generated by a root of $h(x) = x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1$. This is a totally real cyclic sextic field with discriminant $D_K = 453789 = 3^3 7^5$. Its cubic subfield is $L = \mathbb{Q}(\varphi)$ (with discriminant 49) where φ is a root of $f(x) = x^3 + 4x^2 + 3x - 1$. In the field L the elements $\{1, \varphi, \varphi^2\}$ form an integral basis. We have $f(x) \equiv (x+6)^3 \pmod 7$. The quadratic subfield is $M = \mathbb{Q}(\sqrt{21})$. The polynomial $g(x) = x^2 - x - 5$ has $\psi = (1 + \sqrt{21})/2$ as a root, and obviously $\{1, \psi\}$ is an integral basis in M. We have $g(x) \equiv (x - 1/2)^2 \pmod 7$. Theorem 2 implies that the indices of the primitive elements of the order $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$ are all divisible by 7, hence it has no power integral basis.

Example II. A non-cyclic sextic field

Consider the sextic field K generated by a root of $h(x) = x^6 - 12190x^4 + 256565x^2 - 12167$. This is a totally real sextic field with Galois group D_6, discriminant $D_K = 2^6 17^2 23^3 647^2$. Its cubic subfield is $L = \mathbb{Q}(\varphi)$ (with discriminant $252977 = 17 \cdot 23 \cdot 647$ and Galois group S_3) where φ is a root of $f(x) = x^3 - 22x^2 - 23x - 1$. In the field L the elements $\{1, \varphi, \varphi^2\}$ form an integral basis. We have $f(x) \equiv (x+15)(x+16)^2 \pmod{23}$. The quadratic subfield is $M = \mathbb{Q}(\sqrt{23})$. The polynomial $g(x) = x^2 - 23$ has $\psi = \sqrt{23}$ as a root, and obviously $\{1, \psi\}$ is an integral basis in M. We have $g(x) \equiv x^2 \pmod{23}$. Theorem 2 implies that the indices of the primitive elements of the order $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$ are all divisible by 23, hence it has no power integral basis.

Example III. The parametric family of simplest sextic fields

Let $t \in \mathbb{Z}$ with $3 \nmid t$, $t \neq -8, -5$. Let us consider the family of sextic fields K_t generated by a root β_t of the polynomial

$$h_t(x) = x^6 - 2tx^5 - (5t+15)x^4 - 20x^3 + 5tx^2 + (2t+6)x + 1.$$

This family of fields is called the "simplest sextic fields", having some attractive properties, detailed in [27]. These fields are totally real cyclic fields. Let $q = t^2 + 3t + 9$. We have $d(h_t) = 6^6 q^5$. Note that $h_t(x) \equiv (x - t/3)^6 \pmod q$ (the "simplest quintic fields" have a similar property, cf. [14]).

The cubic subfield L_t of K_t is generated by a root φ of

$$f_t = x^3 - tx^2 - (t+3)x - 1$$

with $d(f_t) = q^2$. These are the "simplest cubic fields", totally real, cyclic. It is well known that $\{1, \varphi, \varphi^2\}$ is an integral basis of L_t. Note that
$f_t(x) \equiv (x - t/3)^3 \pmod{q}$.

The quadratic subfield of K_t is $M_t = \mathbb{Q}(\sqrt{q})$.
If $q \equiv 2, 3 \pmod 4$ then set $g_t(x) = x^2 - q$ with $d(g_t) = 4q$ and with a root $\psi = \sqrt{q}$. In this case $g_t(x) \equiv x^2 \pmod{q}$.
If $q \equiv 1 \pmod 4$ then set $g_t(x) = x^2 - x - (q-1)/4$ with $d(g_t) = q$ and with a root $\psi = (1 + \sqrt{q})/2$. In this case $g_t(x) \equiv (x - 1/2)^2 \pmod{q}$.
In both cases $\{1, \psi\}$ is an integral basis of M_t.

Consider now the order $\mathcal{O}_{fg} = \mathbb{Z}[1, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi]$. By Theorem 2 the indices of the primitive elements of $\mathcal{O}_{fg}$ are all divisible by q, hence $\mathcal{O}_{fg}$ has no power integral bases.

Example IV. A field of higher degree I.

This is an example to illustrate that our results are easily applicable also to suitable fields of higher degrees.

Let φ be a root of $f(x) = x^5 - 2x^4 + 7x^2 + 6x + 5$. The quintic field $L = \mathbb{Q}(\varphi)$ has no non-trivial subfields. Let ψ be a root of $g(x) = x^8 + 13x^7 + 55x^6 + 75x^5 + 2x^3 - x^2 - 143x - 525$. The octic field $M = \mathbb{Q}(\psi)$ has no non-trivial subfields, either. We have

$$\begin{aligned} f(x) &\equiv (x+16)^2(x^3 + 16x + 5) \pmod{17} \\ g(x) &\equiv (x+5)^2(x^3 + 12x^2 + 2x + 14)(x^3 + 8x^2 + 4x + 7) \pmod{17} \end{aligned}$$

hence our Theorem 2 applies. Consider the order $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ of the field $K = \mathbb{Q}(\varphi, \psi)$ of degree 40. Any $\alpha \in \mathcal{O}_{fg}$ can be represented in the form

$$\alpha = \sum_{i=0}^{4} \sum_{j=0}^{7} x_{ij} \varphi^i \psi^j$$

with $x_{ij} \in \mathbb{Z}$. By Theorem 2 the indices of all primitive elements of $\mathcal{O}_{fg}$ are divisible by 17, hence $\mathcal{O}_{fg}$ admits no power integral bases.

Example V. A field of higher degree II.

Let φ be a root of $f(x) = x^5 + 17x^4 + 446x^3 + 2232x^2 + 6048x + 24192$. Let ψ be a root of $g(x) = x^4 + 21x^3 - 3x^2 - 8x - 4$. We have

$$\begin{aligned} f(x) &\equiv (x+12)^3(x+9)(x+10) \pmod{19} \\ g(x) &\equiv (x+1)^2(x+2)(x+17) \pmod{19} \end{aligned}$$

hence our Theorem 2 applies. Consider the order $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ of the field $K = \mathbb{Q}(\varphi, \psi)$ of degree 20. Any $\alpha \in \mathcal{O}_{fg}$ can be represented in the form

$$\alpha = \sum_{i=0}^{4} \sum_{j=0}^{3} x_{ij} \varphi^i \psi^j$$

with $x_{ij} \in \mathbb{Z}$. By Theorem 2 the indices of all primitive elements of $\mathcal{O}_{fg}$ are divisible by 19, hence $\mathcal{O}_{fg}$ admits no power integral bases.

Example VI. A field of higher degree III.

Using similar notation as above let φ be a root of

$$f(x) = x^9 - 8x^8 + 73926x^7 + 5470524x^6 + 151807041x^5 + 14x^4 + 6216x^3 + 1034964x^2 + 76587336x + 2125298574.$$

Let ψ be a root of

$$g(x) = x^8 - 58x^7 + 1210x^6 + 13324x^5 + 73975x^4 + 177991x^3 + 186340x^2 + 1024870x + 2254714.$$

We have

$$\begin{aligned} f(x) &\equiv (x+111)^4(x+81)(x^4+32x^3+7x^2+111x+49) \pmod{113} \\ g(x) &\equiv (x+11)^5(x+56)(x^2+57x+85) \pmod{113} \end{aligned}$$

hence our Theorem 2 applies. Consider the order $\mathcal{O}_{fg} = \mathbb{Z}[\varphi, \psi]$ of the field $K = \mathbb{Q}(\varphi, \psi)$ of degree 72. Any $\alpha \in \mathcal{O}_{fg}$ can be represented in the form

$$\alpha = \sum_{i=0}^{8} \sum_{j=0}^{7} x_{ij} \varphi^i \psi^j$$

with $x_{ij} \in \mathbb{Z}$. By Theorem 2 the indices of all primitive elements of $\mathcal{O}_{fg}$ are divisible by 113, hence $\mathcal{O}_{fg}$ admits no power integral bases.

1.4 Congruence conditions I

In the case when the assumptions of Theorem 3 are not satisfied then in certain special cases we can formulate a sufficient congruence condition for the non-existence of power integral basis in the composite of the corresponding orders. In the following subsections we detail two results of this type.

First, assume that there exist square-free integers $p, q \in \mathbb{Z}$ such that

$$f(x) \equiv x^m \pmod{p}, \tag{7}$$

or

$$g(x) \equiv x^n \pmod{q}. \tag{8}$$

Then we have the following theorem (see [10]):

Theorem 4. *(I. Gaál, P. Olajos, [10])*
Assume that there exist a power integral basis in $\mathcal{O}_{fg}$.

If (7) is satisfied, then

$$(d(g))^{m(m-1)/2} \equiv \pm 1 \pmod{p}. \tag{9}$$

If (8) is satisfied, then

$$(d(f))^{n(n-1)/2} \equiv \pm 1 \pmod{q}. \tag{10}$$

Theorem 5. *(I. Gaál, P. Olajos, [10])*
If both (7) and (8) are valid and any of (9) and (10) is not satisfied, then $\mathcal{O}_{fg}$ *does not admit any power integral basis.*

Remark 3. This theorem gives a simple necessary condition for the existence of power integral bases. If the congruences (9) and (10) are valid and the discriminants are coprime (this means that we can't use Theorem 3) then we have to use Theorem 1 for finding these elements. But in many cases when Theorem 4 is satisfied and the discriminants are coprime, we save a lot of calculations, because we don't have to solve equations (4) and (5) of
Theorem 1.

1.4.1 Applications of Theorem 5

In the examples we use the polynomial orders $\mathcal{O}_L$ and $\mathcal{O}_M$ in the same meaning as in Theorem 2, and similarly $\mathcal{O}_K = \mathcal{O}_L\mathcal{O}_M$.

Example I.

Let p, q be square-free integers (≥ 2). One of the most straightforward and frequently used applications of Theorem 5 is the case when $f(x) = x^m - p$ and $g(x) = x^n - q$. Assume that $K = \mathbb{Q}(\sqrt[m]{p}, \sqrt[n]{q})$ is of degree mn. We have

$$\begin{aligned} d(f) &= (-1)^{(m-1)(m-2)/2} \cdot m^m \cdot p^{m-1}, \\ d(g) &= (-1)^{(n-1)(n-2)/2} \cdot n^n \cdot q^{n-1}. \end{aligned}$$

By Theorem 5 if one of the congruences

$$\left(n^n \cdot q^{n-1}\right)^{m(m-1)/2} \equiv \pm 1 \pmod{p},$$

$$\left(m^m \cdot p^{m-1}\right)^{n(n-1)/2} \equiv \pm 1 \pmod{q}$$

is not satisfied, then $\mathcal{O}_K = \mathbb{Z}[\sqrt[m]{p}, \sqrt[n]{q}]$ has no power integral basis.

I.1. In the special case if $m = 3,\ n = 2$, the field $K = LM$ is an algebraic number field of degree 6. We have $d(f) = D_{\mathcal{O}_L} = -27 \cdot p^2, d(g) = D_{\mathcal{O}_M} = 4 \cdot q$.

The above congruences are of the form

$$64 \cdot q^3 \equiv \pm 1 \pmod{p},$$
$$-27 \cdot p^2 \equiv \pm 1 \pmod{q}.$$

If for example we take $p = 7,\ q = 5$ then

$$\gcd(D_{\mathcal{O}_L}, D_{\mathcal{O}_M}) = 1,$$

hence Theorem 1. would be applicable. We have

$$64 \cdot 5^3 = 8000 \equiv 6 \equiv -1 \pmod{7},$$
$$-27 \cdot 7^2 = -1323 \equiv 2 \equiv -3 \pmod{5}.$$

Theorem 5 implies that there is no power integral basis in $\mathcal{O}_K$.

I.2. In the special case when $m = 22,\ n = 15$ and $[K : \mathbb{Q}] = 22 \cdot 15 = 330$, we have

$$d(f) = D_{\mathcal{O}_L} = 22^{22} \cdot p^{21},\ \ d(g) = D_{\mathcal{O}_M} = -15^{15} \cdot q^{14}.$$

If for example we take $p = 31,\ q = 17$ then

$$\gcd(D_{\mathcal{O}_L}, D_{\mathcal{O}_M}) = 1,$$

hence Theorem 1 would be applicable. But by applying Theorem 5, either

$$(-15^{15} \cdot 17^{14})^{231} \equiv 4 \equiv -27 \pmod{31}$$

or

$$(22^{22} \cdot 31^{21})^{105} \equiv 10 \equiv -7 \pmod{17}$$

implies that there exist no power integral basis in $\mathcal{O}_K$.

Example II.

To consider a different example let $f(x) = x^5 - p^3x^3 - p^2x^2 - px - p$ and $g(x) = x^3 - q^2x^2 - qx - q$ $(m = 5,\ n = 3)$. If $\mathcal{O}_K$ has power integral bases, then the following congruences must be satisfied:

$$d(g)^{10} \equiv \pm 1 \pmod{p},$$

$$d(f)^3 \equiv \pm 1 \pmod{q},$$

where

$$d(g) = -q^2(-4q - q^4 + 18q^2 + 4q^5 + 27)$$

and

$$d(f) = -p^4(108p^{13} - 56p^{12} + 12p^{11} + 75p^8 - 38p^7 + 11p^6 - 3750p^4 +$$

$$4250p^3 - 1600p^2 + 256p - 3125).$$

If one of these congruences is not satisfied, $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$ (α and β are being roots of f, g respectively) has no power integral basis.

II.1. Let $p = 7,\ q = 29$. Then $[K : \mathbb{Q}] = 5 \cdot 3 = 15$, and we have

$$d(f) = D_{\mathcal{O}_L} = -23320969892806663 = -(7)^4(11)^2(5208131)(15413),$$

$$d(g) = D_{\mathcal{O}_M} = -68417338124 = -(2)^2(29)^2(41)(496051)$$

and

$$\gcd(D_{\mathcal{O}_L}, D_{\mathcal{O}_M}) = 1,$$

hence Theorem 1 would be applicable. But by applying Theorem 5, either

$$d(g)^{10} \equiv 2 \equiv -5 \pmod 7$$

or

$$d(f)^3 \equiv 6 \equiv -23 \pmod{29}$$

implies that there exist no power integral basis in $\mathcal{O}_K$.

1.5 Congruence conditions II

In this subsection we assume that there exists a square-free integer q, such that f is a perfect power modulo q, that is

$$f(x) \equiv (x - t)^m \pmod q \tag{11}$$

with some $t \in \mathbb{Z}$.

Our result is the following:

Theorem 6. *(P. Olajos, [31])*
If there exists a power integral basis in $\mathcal{O}_{fg}$, then the congruence

$$(d(g))^{m(m-1)} \equiv \pm 1 \pmod q \tag{12}$$

is satisfied.

As a consequence we have:

Theorem 7. *(P. Olajos, [31])*
If (11) is valid and (12) is not satisfied, then $\mathcal{O}_{fg}$ does not admit any power integral bases.

Remark 4. If $\gcd(d(g), d(f)) = 1$, then the results of Section 1.1 are hardly applicable for higher degree number fields. If condition (11) is satisfied, we can draw a conclusions on the existence of power integral bases even in higher degree fields.

Remark 5. The case $d = \gcd(d(f), d(g)) \neq 1$ have already been considered in Section 1.3 . In this case both f and g have a multiple linear factor modulo q, where q is a prime divisor of d. The result given above gives a necessary condition for the existence of power integral basis in case when Theorem 3 is not applicable.

1.5.1 Applications of Theorem 7

Example I. A parametric family of totally real cyclic sextic fields

One of the most interesting application of Theorem 7 is the case when

$$f(x) = x^3 - (a+1)x^2 + (a+2)x + 1,$$

$$g(x) = x^2 - ax - 1$$

with parameter $a \in \mathbb{Z}$ $(m = 3, n = 2)$. This family was investigated by O. Lecacheux [24] which has initialed our present result. We have

$$d(f) = (a^2 - a + 7)^2,$$

$$d(g) = a^2 + 4.$$

Let us consider the polynomial f. We get

$$f(x) - \left(x - \frac{a+1}{3}\right)^3 = \frac{1}{27} \cdot (a^2 - a + 7) \cdot (a + 4 - 9x).$$

Set $q = a^2 - a + 7$ and assume that q is square free. If $a \equiv 2 \pmod 3$, then $\gcd(q, 9) = 9$. Because of it we consider the family when $a \equiv 0, 1 \pmod 3$. Then we have $\gcd(q, 3) = 1$ which means

$$f(x) \equiv \left(x - \frac{a+1}{3}\right)^3 \pmod q. \tag{13}$$

Using congruence (13), by Theorem 6 if there exists a power integral basis in$\mathcal{O}_{fg}$ the following is satisfied:

$$(a^2 + 4)^6 \equiv (a - 3)^6 \equiv \pm 1 \pmod q. \tag{14}$$

Using Maple for finding solutions we have the following:

if $a \notin [-840, 840]$, then (14) is not satisfied, so by Theorem 7 there exist no power integral bases in $\mathcal{O}_{fg}$.

Considering the values $|a| < 840$, (12) can only be satisfied for

$$a = -15, -2, 1, 4.$$

Example II.

As another application of Theorem 7 is the case when

$$f(x) = x^5 + a^2x^4 - (2a^3 + 6a^2 + 10a + 10)x^3 +$$

$$(a^4 + 5a^3 + 11a^2 + 15a + 5)x^2 + (a^3 + 4a^2 + 10a + 10)x + 1,$$

$$g(x) = x^2 - ax - 1$$

with parameter $a \in \mathbb{Z}$ $(m = 5, n = 2)$. The totally real cyclic quintic family generated by a root of f was investigated by E. Lehmer [25], see also cf. I. Gaál and M. Pohst [14]. We have

$$d(g) = a^2 + 4.$$

Let us consider the polynomial f. Set $q = a^4 + 5a^3 + 15a^2 + 25a + 25$ and assume that q is square free. Then we have

$$f(x) \equiv \left(x + \frac{a^2}{5}\right)^5 \pmod{q}. \tag{15}$$

Using congruence (15), by Theorem 6 if there exists a power integral basis in $\mathcal{O}_{fg}$, then

$$(a^2 + 4)^{20} \equiv \pm 1 \pmod{q} \tag{16}$$

is satisfied. Using Maple we have that if $a > 2.4 \cdot 10^{16}$, then (16) is not satisfied, so by Theorem 7 there exist no power integral bases in $\mathcal{O}_{fg}$.

2 Simplest quartics

2.1 Simplest quartic fields

For $t \in \mathbb{Z} \setminus \{0, \pm 3\}$ let

$$P_t(x) = x^4 - tx^3 - 6x^2 + tx + 1. \tag{17}$$

Let $\xi = \xi_t$ be a root of $P_t(x)$, then the infinite parametric family of number fields $K_t = K = \mathbb{Q}(\xi)$ is called *simplest quartic fields*. The simplest quartic field K is a totally real cyclic number field of degree 4. If $t = 0$ or $t = \pm 3$ then $P_t(x)$ is not irreducible over $\mathbb{Q}$.

If ξ is a root of (17), then $\frac{\xi-1}{\xi+1}$ is also one of the roots of (17). Thus the rational map $x \mapsto \frac{x-1}{x+1}$ permutes the roots of (17) and $K = \mathbb{Q}(\xi)$ is a real quartic number field with cyclic Galois group $G = \langle \sigma \rangle$ generated by the automorphism $\sigma : \xi \mapsto \frac{\xi-1}{\xi+1}$. The family of "simplest" quartic number fields were investigated by M. N. Gras in [17], see also G. Lettl and A. Pethő in [26] and G. Lettl, A. Pethő and P. Voutier in [28].

The purpose of this chapter is to describe all generators of power integral bases in K_t, in a parametric form.

2.2 Power integral bases in simplest quartic fields

Let again $\xi = \xi_t$ be a root of $P_t(x)$ in (17) and $K = K_t = \mathbb{Q}(\xi_t)$.

For finding all generators of power integral bases of the simplest quartics we need two lemmas.

Note that $\mathbb{Q}(\alpha) = \mathbb{Q}(-\alpha)$ (α an algebraic integer), that is we can assume that $t > 0$ and $t \neq 3$. In the following we assume also that $t^2 + 16$ is not divisible by an

odd square. Further denote by $v_2(t)$ the 2-adic valuation of t. Recently the integral basis of K was explicitly given.

Lemma 1. *(H. K. Kim and J. S. Kim, [23])*
An integral bases of $K = K_t$ is given as follows.

$$\mathcal{O}_{\mathcal{K}} = \begin{cases} [1, \xi, \xi^2, \frac{1+\xi^3}{2}] & \text{if } v_2(t) = 0, \\ [1, \xi, \frac{1+\xi^2}{2}, \frac{\xi+\xi^3}{2}] & \text{if } v_2(t) = 1, \\ [1, \xi, \frac{1+\xi^2}{2}, \frac{1+\xi+\xi^2+\xi^3}{4}] & \text{if } v_2(t) = 2, \\ [1, \xi, \frac{1+2\xi-\xi^2}{4}, \frac{1+\xi+\xi^2+\xi^3}{4}] & \text{if } v_2(t) \geq 3. \end{cases}$$

The main result of this chapter is:

Theorem 8. *(P. Olajos, [32]) The ring of integers $\mathbb{Z}_K$ of the simplest quartic field $K = K_t$ admits power integral bases only for $t = 2$ and $t = 4$. In these cases all generators of power integral bases are the following:*

$t = 2,\ \alpha = x \cdot \xi + y \cdot \frac{1+\xi^2}{2} + z \cdot \frac{\xi+\xi^3}{2}$ *where*
$(x, y, z) = (4, 2, -1), (-13, -9, 4), (-2, 1, 0), (1, 1, 0), (-8, -3, 2),$
$(-12, -4, 3), (0, -4, 1), (6, 5, -2), (-1, 1, 0), (0, 1, 0).$

$t = 4,\ \alpha = x \cdot \xi + y \cdot \frac{1+\xi^2}{2} + z \cdot \frac{1+\xi+\xi^2+\xi^3}{4}$ *where*
$(x, y, z) = (3, 2, -1), (-2, -2, 1), (4, 8, -3), (-6, -7, 3), (0, 3, -1),$
$(1, 3, -1).$

To prove our main result we apply the following general argument for finding power integral bases in quartic fields.

Denote by $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ the minimal polynomial of the generating element of a quartic field $K = \mathbb{Q}(\xi)$. Assume, that any $\alpha \in \mathbb{Z}_K$ can be represented in the form

$$\alpha = \frac{a + x\xi + y\xi^2 + z\xi^3}{g} \tag{18}$$

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

$$\begin{aligned} F(u, v) &= u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3, \\ Q_1(x, y, z) &= x^2 - a_1xy + a_2y^2 + (a_1^2 - 2a_2)xz + \\ &+ (a_3 - a_1a_2)yz + (-a_1a_3 + a_2^2 + a_4)z^2, \\ Q_2(x, y, z) &= y^2 - xz - a_1yz + a_2z^2, \end{aligned}$$

and consider the equation

$$I(\alpha) = m \tag{19}$$

where $\alpha \in \mathbb{Z}_K,\ m \in \mathbb{Z}$.

Lemma 2. *(I. Gaál, A. Pethő, M. Pohst, [11], see also [8])*
The element $\alpha \in \mathbb{Z}_K$, represented in the form (18), is a solution of (19) if and only if there exists a solution $(u, v) \in \mathbb{Z}^2$ of

$$F(u,v) = \pm\frac{g^6 m}{I(\xi)} = \pm i_m \tag{20}$$

with

$$Q_1(x,y,z) = u, \tag{21}$$

$$Q_2(x,y,z) = v. \tag{22}$$

3 A parametric family of degree 6

3.1 Auxiliary results

Let ϑ be a totally real cubic algebraic integer and let m be a square-free positive integer. Let us consider the sextic field $K = \mathbb{Q}(\vartheta, i\sqrt{m})$, with discriminant D_K and ring of integers $\mathbb{Z}_K$. Let $M = \mathbb{Q}(i\sqrt{m})$ and $L = \mathbb{Q}(\vartheta)$ be the subfields of K. Set

$$\omega = \begin{cases} (1+\mathrm{i}\sqrt{m})/2, & \text{if } -m \equiv 1 \pmod 4 \\ \mathrm{i}\sqrt{m}, & \text{if } -m \equiv 2,3 \pmod 4. \end{cases} \tag{23}$$

We represent any $\alpha \in \mathbb{Z}_K$ in the form

$$\alpha = \frac{x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2}{g} \tag{24}$$

with $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$ and with a fixed common denominator $g \in \mathbb{Z}$.
Set $\mathcal{O} = \mathbb{Z}[1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2]$ and denote by $D_\mathcal{O}$ the discriminant of this order. We are going to consider the existence of power integral basis, and more general the existence of elements of a given index, in the order $\mathcal{O}$ which often coincides with $\mathbb{Z}_K$. We have

$$\frac{g^6\sqrt{|D_K|}}{\sqrt{|D_\mathcal{O}|}} \in \mathbb{Z}.$$

Let I_0 be a given, non-zero positive integer and consider the solutions $\alpha \in \mathbb{Z}_K$ of

$$I(\alpha) = I_0. \tag{25}$$

Set

$$I_1 = \frac{g^{15} I_0\sqrt{|D_K|}}{\sqrt{|D_\mathcal{O}|}} \in \mathbb{Z}.$$

Denote by ϑ_i $(1 \le i \le 3)$ the conjugates of ϑ over M and set $\rho = -\vartheta_2 - \vartheta_3$.

Lemma 3. *(I. Gaál, [3])*
If $\alpha \in \mathbb{Z}_K$ is a solution of equation (25), and $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$ are the coefficients of α in the representation (24), then

$$N_{K/M}((x_1 + \omega y_1) - \rho(x_2 + \omega y_2)) = \mu, \tag{26}$$

$$N_{L/Q}(y_0 + y_1\vartheta + y_2\vartheta^2) = d, \tag{27}$$

where $\mu \in \mathbb{Z}_M$, $d \in \mathbb{Z}$, such that $d \cdot N_{M/Q}(\mu)$ divides I_1.

Under our assumptions on the field K, denote by $\rho = \rho_1,\ \rho_2,\ \rho_3$ the conjugates of ρ over L and let $X = x_1 + \omega y_1,\ Y = x_2 + \omega y_2$ be an arbitrary, but fixed solution of (26). Choose the indices $\{r,\ s,\ t\} = \{1,\ 2,\ 3\}$ according to

$$|X - \rho_r Y| \le |X - \rho_s Y| \le |X - \rho_t Y|. \tag{28}$$

Set

$$c_m = \begin{cases} 2, & \text{if } -m \equiv 1 \pmod 4 \\ 1, & \text{if } -m \equiv 2, 3 \pmod 4 \end{cases}$$

$$\begin{aligned} c_1 &= 9c_m^3|\mu|, \\ c_2 &= \min(|\rho_r - \rho_s|,\ |\rho_r - \rho_t|), \\ c_3 &= |\rho_r - \rho_s| \cdot |\rho_r - \rho_t| \end{aligned}$$

$$c_4 = \max\left\{\frac{2|\mu|^{1/3}}{c_2}, \frac{4c_m|\mu|}{c_3\sqrt{m}}\right\}, c_5 = \left(\frac{8|\mu|}{c_2c_3}\right)^{1/3}.$$

Finally put

$$F(x, y) = \prod_{j=1}^{3}(x - \rho_j y) \in \mathbb{Z}[x, y].$$

Under these assumptions we have the following statement:

Lemma 4. *(I. Gaál, [3])*
Let $X = x_1 + \omega y_1,\ Y = x_2 + \omega y_2 \in \mathbb{Z}_M$ be a solution of (26) according to (28). Suppose $|Y| > c_4$. We have

$$x_1y_2 = x_2y_1.$$

Further, in case $-m \equiv 1 \pmod 4$:

$$\begin{cases} \text{if } |2x_2 + y_2| \ge 2c_5, & \text{then } |F(2x_1 + y_1, 2x_2 + y_2)| \le c_1 \\ \text{if } |y_2| \ge 2c_5/\sqrt{m}, & \text{then } |F(y_1, y_2)| \le c_1/(\sqrt{m})^3, \end{cases}$$

and in case $-m \equiv 2, 3 \pmod 4$:

$$\begin{cases} \text{if } |x_2| \ge 2c_5, & \text{then } |F(x_1, x_2)| \le c_1, \\ \text{if } |y_2| \ge c_5/\sqrt{m}, & \text{then } |F(y_1, y_2)| \le c_1/(\sqrt{m})^3. \end{cases}$$

Remark 6. In [3] the fields $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ were considered, where ϑ is a root of $f(x) = x^3 - ax^2 - (a+3)x - 1$ and m is a square-free positive integer. By Theorem 3.1 of [3] if $a \geq 3$ and $m \geq m_0$, then there is no power integral basis in the order $\mathcal{O}$ of K.

3.2 Results

Let

$$f_n(x) = x^3 - nx^2 - (n+1)x - 1 \tag{29}$$

where $n \in \mathbb{N}$. If $n \geq 3$, then $f_n(x)$ is totally real. Let $\vartheta = \vartheta_n$ be a root of $f_n(x)$ and let m be a square-free positive integer. Consider the two-parametric family $K = \mathbb{Q}(\vartheta, i\sqrt{m})$ of totally complex sextic fields. Define ω as in (23) and set $\mathcal{O} = \mathbb{Z}[1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2]$ with discriminant $D_{\mathcal{O}}$ as before. We also use $L = \mathbb{Q}(\vartheta)$ and $M = \mathbb{Q}(i\sqrt{m})$. Put

$$m_0 = \begin{cases} 36, & \text{if } -m \equiv 1 \pmod 4, \\ 9, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

Theorem 9. *(P. Olajos, [30])*
Assume that $n \geq 7$ and $m \geq m_0$. Then the order $\mathcal{O}$ has no power integral basis.

The proof of this theorem uses arguments similar to [3], but we will consider the small parameters, as well. It means that we will deal with the cases, which do not satisfy $n \geq 7$ or $m \geq m_0(n)$. Note that if $n \leq 2$, then (29) is not totally real, so we have to deal additionally only with the cases, when $n = 3,\ 4,\ 5,\ 6$. Using similar tools as in the proof of Theorem 9, we can show that for $m \geq m_o(n)$ the order $\mathcal{O}$ admits no power integral basis.

Theorem 10. *(P. Olajos, [30])*
Set

$$m_0(3) = \begin{cases} 143, & \text{if } -m \equiv 1 \pmod 4, \\ 36, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

$$m_0(4) = \begin{cases} 59, & \text{if } -m \equiv 1 \pmod 4, \\ 15, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

$$m_0(5) = \begin{cases} 42, & \text{if } -m \equiv 1 \pmod 4, \\ 11, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

$$m_0(6) = \begin{cases} 36, & \text{if } -m \equiv 1 \pmod 4, \\ 9, & \text{if } -m \equiv 2,\ 3 \pmod 4. \end{cases}$$

For $n = 3,\ 4,\ 5,\ 6$, $m \geq m_o(n)$, the order $\mathcal{O}$ has no power integral basis.

Further, for $n = 3,\ 4,\ 5,\ 6$ by performing direct computation for the small values of m we get:

Theorem 11. *(P. Olajos, [30])*
If $n = 3,\ 4,\ 5,\ 6$ and $2 \leq m_0 < m_0(n)$, then $\mathcal{O}$ has no power integral basis.

References

[1] Y. Bilu, I. Gaál and K. Győry, *Index form equations in sextic fields: a hard computation*, Acta Arithm., to appear.

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

[3] I. Gaál, *Computing elements of given index in totally complex cyclic sextic fields*, J.Symbolic Comp., **20**(1995), 61–69.

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

[5] I. Gaál, *Power integral bases in composits of number fields*, Canad. Math. Bulletin **41**(1998), 158–165.

[6] I. Gaál, *Power integral bases in algebraic number fields*, Ann. Univ. Sci. Budapest, Sect. Comp., **18**(1999), 61–87.

[7] I. Gaál, *Solving index form equations in fields of degree nine with cubic subfields*, J.Symbolic Comput., **30**(2000), 181–193

[8] I. Gaál, Diophantine equations and power integral bases, Birkhäuser, Boston, (2002).

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

[10] I. Gaál and P. Olajos, *Recent results on power integral bases of composite fields*, Acta Acad. Paed. Agr. Eger, **30**(2003), 45–54.

[11] 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.

[12] I. Gaál, A. Pethő and M. Pohst, *Simultaneous Representation of Integers by a Pair of Ternary Quadratic Forms–With an Application to Index Form Eqautions in Quadratic Number Fields*, J. Number Theory, **57**(1996), 90–104.

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

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

[15] I. Gaál, M. Pohst and P. Olajos, *Power integral bases in orders of composite fields*, Experimental Math., **11**(2002), 87–90.

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

[17] M. N. Gras, *Table numerique du nombre de classes et des unites des extensions cycliques reelles de degré 4 in* $\mathbb{Q}$, Publ. Math. Fac. Sci. Besançon, (1977-1978) fasc. 2.

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

[19] K. Győry, *On polynomials with integer coefficients and given discriminant, IV*, Publ. Math. (Debrecen), **25**(1978), 155–167.

[20] K. Győry, Résultats effectifs sur la représentation des entiers par des formes décomposables, Queen's Papers in Pure and Applied Math., No. **56**, Kingston, Canada, (1980).

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

[22] I. Járási, *Power integral bases in sextic fields with a cubic subfield*, Acta Sci. Math. (Szeged), **XX**(2003), 291–303.

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

[24] O. Lecacheux, *Unités d´une famille de corps cycliques réels de degré 6 liés à la courbe modulaire* $X_1(13)$, J. Number Theory, **31**(1989), 54–63.

[25] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comput., **50**(1988), 535–541.

[26] G. Lettl and A. Pethő, *Complete Solution of a Family of Quartic Thue Equations*, Abh. Math. Sem. Univ. Hamburg, **65**(1995), 365–383.

[27] G. Lettl, A. Pethő, P. Voutier, *On the arithmetic of simplest sextic fields and related Thue equations*, in Number Theory, eds. K.Győry, A.Pethő, V.T.Sós, Walter de Gruyter, Berlin-New York, 1998, 331–348.

[28] G. Lettl, A. Pethő and P. Voutier *Simple families of Thue inequalities*, Trans. Am. Math. Soc., **351**(1999), 1871–1894.

[29] M. Mignotte and N. Tzanakis, *On a family of cubic*, J. Number Theory, **39**(1991),41–49.

[30] P. Olajos, *Power integral bases in a parametric family of sextic fields*, Publ. Math. Debrecen, **58**(2000), 779–790.

[31] P. Olajos, *Power integral bases in orders of composite fields II*, Annales Sci. Math., to appear.

[32] P. Olajos, *Power integral bases in the family of simplest quartic fields*, Experimental Math., submitted.

[33] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Springer, (1974).

[34] L. J. Mordell, Diophantine Equations, Academic Press, New York London, 1969.