DE TTK

1949

Algebrai számtestek egész bázisa és monogenitása

Egyetemi doktori (PhD) értekezés

a szerző neve: Remete László
témavezető neve: Dr Gaál István

Debreceni Egyetem
Természettudományi és Informatikai Doktori Tanács
Matematika- és számítástudományok doktori iskola
Debrecen, 2021

Ezen értekezést a Debreceni Egyetem Természettudományi Doktori Tanács Matematika- 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, 2021. június 10. .....

a jelölt aláírása

Tanúsítom, hogy Remete László doktorjelölt 2017-2021 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, 2021. június 10. .....

a témavezető aláírása

Algebrai számtestek egész bázisa és monogenitása

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

Írta: Remete László okleveles matematikus

Készült a Debreceni Egyetem Matematika- és Számítástudományok doktori iskolája (Explicit módszerek az algebrai számelméletben programja) keretében

Témavezető: Dr. Gaál István

Az értekezés bírálói:

Dr. Pink István .....

Dr. Szalay László .....

A bírálóbizottság:

elnök: Dr. Győry Kálmán .....

tagok: Dr. Hajdu Lajos .....

Dr. Pongrácz András .....

Dr. Liptai Kálmán .....

Dr. Zábrádi Gergely .....

Az értekezés védésének várható időpontja: 2021. szeptember

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Dr. Gaál Istvánnak a rengeteg segítséget és támogatást, amit az egyetemi éveim során kaptam. A tanácsainak és az útmutatásainak hála megismerkedhettem az algebrai számelmélet egy nagyon izgalmas és szerteágazó területével, és abban eleinte közösen, majd pedig önállóan is publikálható kutatási eredményeket érhettem el. Nélküle ez a dolgozat sokkal szegényebb lenne.

Tartalomjegyzék

1. Bevezetés **1**

2. Algebrai számelméleti alapok **5**

2.1. Egész bázisok kiszámítása, hasznos eszközök és módszerek 7

2.1.1. Egész bázis kiszámítása: a favágó módszer 7

2.1.2. Hermite normál alakú egész bázis 9

2.1.3. Az index becslése I: Duális bázis 11

2.1.4. Az index becslése II: Newton poligonok 12

2.1.5. Periodikus egész bázisok 15

2.2. Monogenitás, hatvány egész bázis 19

2.2.1. Az indexforma faktorai 20

3. Végtelen parametrikus számtestek egész bázisai **23**

3.1. Gyökbővítések egész bázisai 23

3.2. Legegyszerűbb testek általánosításai és egész bázisai 40

3.3. Kompozitum testek egész bázisai 61

4. Végtelen parametrikus számtestek monogenitása **69**

4.1. Gyökbővítések monogenitása 74

4.2. Legegyszerűbb testek monogenitása 85

4.3. Kompozitum számtestek monogenitása 89

Összefoglaló **97**

Summary **100**

Irodalomjegyzék **105**

1. fejezet

Bevezetés

Disszertációm fő vizsgálati tárgyai az algebrai számtestek egész bázisai. Adott algebrai számtest egy egész bázisának megkonstruálása egyszerű dolog. Érdekesebb a kérdés, ha nem egy bizonyos algebrai számtestről van szó, hanem számtestek egy végtelen családjáról.

A disszertációban számtestek olyan végtelen parametrikus családjaival foglalkozunk, melyeket polinomok végtelen parametrikus családjainak gyökei generálnak. Erre jó példát szolgáltatnak a másodfokú számtestek, melyeket az $f_m(X) = X^2 - m$ polinomok gyökei generálnak, ahol m négyzetmentes egész. Ezen másodfokú testek esetén ismeretesek az egész bázisok, formájuk az m paraméter 4-el való osztási maradékától függ. Ha $m \equiv 2, 3 \pmod 4$, akkor $(1, \sqrt{m})$, ha pedig $m \equiv 1 \pmod 4$, akkor $\left(1, \frac{1+\sqrt{m}}{2}\right)$ egész bázist alkot $\mathbb{Q}(\sqrt{m})$-ben.

Hasonlóan vizsgálhatunk más parametrikus polinomcsaládok gyökei által definiált számtesteket. Példaként tekintsük a legegyszerűbb hatodfokú számtesteket, melyeket az

$$f_m(X) = X^6 - 2mX^5 - 5(m+3)X^4 - 20X^3 + 5mX^2 + 2(m+3)X + 1$$

polinom gyökei generálnak, ahol $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$.

Ezek vizsgálata során kiderült, hogy ha $m^2 + 3m + 9$ négyzetmentes, akkor az m paraméter 36-al való osztási maradékától függően 19 esetet tudunk megkülönböztetni. Például, ha α az $f_m(X)$ gyöke és $m \equiv 1 \pmod{36}$, akkor

$$\left(1, \alpha, \alpha^2, \frac{1+\alpha+\alpha^3}{2}, \frac{4+\alpha+3\alpha^2+\alpha^4}{6}, \frac{11+3\alpha+13\alpha^2+6\alpha^3+2\alpha^4+\alpha^5}{18}\right)$$

egész bázisa $\mathbb{Q}(\alpha)$-nak. Ha $m \equiv 2 \pmod{36}$, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1+\alpha^3+\alpha^4}{3}, \frac{1+7\alpha+6\alpha^2+2\alpha^3+\alpha^5}{9}\right)$$

egész bázisa $\mathbb{Q}(\alpha)$-nak, és így tovább (ld. [28]). Ilyen esetben azt mondjuk, hogy a számtestcsalád egész bázisai periodikusan ismétlődnek.

Ez a jelenség a másodfokú testeken kívül eddig csak nagyon kevés számtestben volt ismert (pl. harmadfokú [12] és negyedfokú gyökbővítések [19], legegyszerűbb negyedfokú testek [49]). A dolgozatban három végtelen parametrikus számtestcsalád esetén igazoljuk az egész bázis periodikusságát, ráadásul tetszőleges fokszámokra, ami azt jelenti, hogy valójában végtelen sok parametrikus számtestcsaládot vizsgálunk. A kapcsolódó eredmények a [26], [28], [58] és [59] cikkekben jelentek meg.

Algebrai számtestek egész bázisai között kitüntetett szerepet töltenek be az $(1, \alpha, \ldots, \alpha^{n-1})$ alakú hatvány egész bázisok. Ha az n-edfokú K algebrai számtestben létezik ilyen α algebrai egész szám, akkor az egészek gyűrűjét $\mathbb{Z}$ felett egyetlen elem generálja, $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, azaz $\mathbb{Z}_K$ mono-generált, más néven *monogén* gyűrű.

A számtestek monogenitásának vizsgálata és a hatvány egész bázisok meghatározása az algebrai számelmélet klasszikus problémaköre, mely Dedekind [12] és Hasse [40] munkásságáig nyúlik vissza. Birch és Merriman [5] eredményeiből következően kiderült, hogy egy algebrai számtestben ekvivalencia erejéig véges sok hatvány egész bázis generátor létezhet, amit tőlük függetlenül A. Baker [2] módszerét felhasználva Győry Kálmán [36] effektív formában is bebizonyított. Az effektív eredmények (részletesebben ld. Evertse - Győry Kálmán [17]), egy véges, de gyakorlatban a nagyon nagy korlátok miatt nem kivitelezhető algoritmust adnak a hatvány egész bázisok generátorainak meghatározására. Többek között redukciós és leszámlálási algoritmusok konstruálása volt szükséges ahhoz, hogy viszonylag kis fokszámú testekben ténylegesen meg lehessen határozni a generátorokat, ld. Gaál István [22]. Általános, hatékony algoritmusok léteznek harmadfokú (ld. Gaál István, N. Schulte [30]) és negyedfokú számtestekre (ld. Gaál István, Pethő Attila, M. Pohst [24]). Ezeknél a számítási idő pár másodperc. Létezik általános eljárás ötödfokú számtestek (ld. Gaál István, Győry Kálmán [23]), átlagos számítógépen kb 8 óra futási idővel, és hatodfokú számtestek esetén is (ld. Y. Bilu, Gaál István, Győry Kálmán [4]), kb 5 hónap gépidővel. Speciális hatodfokú, nyolcadfokú stb. testek esetén léteznek ugyancsak hatékony eljárások, ld. Gaál István [22].

Mindezek fényében érdekesek és fontosak azon eredményeink, melyeket a periodikus egész bázisok vonatkozásában vizsgált végtelen parametrikus számtest családok monogenitásával kapcsolatban nyertünk. Ezekhez az eredményekhez a fentiekkel ellentétben Dedekind [11] módszerét, a Newton poligonok elméletét (ld. [33], Chapter 6.4), Ø. Ore [56] index-tételét és az indexforma faktorait felhasználva jutunk el. A korábbi megközelítésekhez képest ez az irány egyfelől kicsivel korlátozottabb, más szempontból viszont általánosabb eredményekhez vezet. Számításaink során nem célunk meghatározni az összes hatvány egész bázis generátort, csupán azt igyekszünk eldönteni, hogy a mely paraméterek esetén lehet monogén a test. Arra törekszünk, hogy ha egy adott paraméter esetén a polinom gyöke nem generál hatvány egész bázist, akkor megmutassuk, hogy a test nem monogén. Az utóbbi években ez a kutatási irány egyre nagyobb népszerűségnek örvend, több olyan cikk született, ami végtelen parametrikus számtestek monogenitásával foglalkozik (ld. [44], [43], [29], [32], [61], [46], [28], [45], [31], [27], [26], [39], [48], [62], [7], [55], [6]). Ez a módszer a klasszikus megközelítésnél annyiban általánosabb, hogy egyszerre végtelen sok számtesttel kapcsolatban fogalmazunk meg állításokat.

Az általunk vizsgált esetek többségében ez ráadásul igen hatékonyan működik. A hatodfokú gyökbővítések esetében például sikerült megmutatnunk (ld. [26]), hogy ha az $X^6 - m$ polinom gyöke nem generál hatvány egész bázist, akkor a test nem is lehet monogén. Ez a feltétel pedig csupán m-nek a 36-os maradékától függ, tehát négyzetmentes m paraméterek esetén sikerült jellemezni az összes monogén hatodfokú gyökbővítést.

Az értekezés 2. fejezetében a felhasznált módszereket és állításokat gyűjtöttem össze. Az első részben az egész bázis meghatározásához, és a periodikus egész bázis igazolásához használt eljárásokat foglalom össze, majd a 2.1.5 részben precízen definiálom a periodikus egész bázis tulajdonságot. A fejezet második részében, az indexforma kiszámításához, és az egész együtthatós faktorizációjához kapcsolódó módszereket ismertetem.

A 3. és 4. fejezetekben találhatóak a három végtelen parametrikus számtestcsaládhoz kapcsolódó eredmények, melyek részben a [26], [27], [28], [29], [58] és [59] cikkekben jelentek meg.

A 3. fejezetben megmutatom, hogy az egész bázis mindhárom család esetben periodikusan ismétlődik. A megfelelő paraméterekhez tartozó gyökbővítések esetén megadjuk a legkisebb periódushosszt, a legegyszerűbb testek kétféle általánosítása esetén felső korlátot adunk a periódushosszra, illetve bizonyos kis fokszámokú esetekben ezeknél is megadjuk a legkisebb periódushosszt. A legegyszerűbb testek általánosításai esetén (ld. [59]), külön vizsgáljuk a felbontási testet, mivel tapasztalataink szerint az a tény, hogy az n-edfokú polinom felbontási teste, egy résztestének ciklikus n-edfokú bővítése, szoros kapcsolatban áll a periodikus egész bázis tulajdonsággal, illetve a monogenitás vizsgálatakor használt faktorok közötti összefüggésekkel. A gyökbővítések esetében ez a tulajdonság nyilvánvalóan teljesül. Ezek után igazoljuk, hogy megfelelő feltételek mellett a periodikus egész bázis tulajdonság öröklődik olyan testekre is, amelyek a már vizsgált számtestcsaládok közül kikerülő testek kompozítumaként állnak elő.

A 4. fejezetben, a periodikus egész bázis felhasználásával alacsonyabb fokszámok esetén megvizsgáljuk, hogy a három végtelen parametrikus számtestcsalád mely paraméterek mellett lehet monogén. Az esetek többségében, ezt néhány maradékosztálytól eltekintve, minden megfelelő paraméterre el tudjuk dönteni (ld. [26],[28]). A fejezet utolsó részében alacsonyabb fokú kompozit bővítések monogenitását vizsgáljuk az előző részekben is használt módszerek segítségével, és hasonló átfogó eredményeket nyerünk (ld. [29]). Következményként kapjuk, hogy az M.-L. Chang [6] által vizsgált $X^3 - m$ polinomhoz hasonlóan, néhány meghatározott értéktől eltekintve az $X^4 - m$ és az $X^6 - m$ polinomok felbontási testei sem lehetnek monogének.

Az egész bázisokkal, és az indexformákkal kapcsolatos számításainkat a Maple matematikai programcsomaggal végeztük, amely kiválóan használható az ilyen szimbolikus műveletekhez (ld. [3]).

2. fejezet

Algebrai számelméleti alapok

Egy $\alpha \in \mathbb{C}$ számot *n-edfokú algebrai számnak* nevezünk, ha α gyöke egy $f(X) \in \mathbb{Z}[X]$ egész együtthatós n-edfokú irreducibilis polinomnak. Ezt a polinomot α *egész együtthatós definiáló polinomjának* nevezzük. Ha a definiáló polinom főegyütthatója c és

$$f(X) = c \cdot \prod_{i=1}^{n} (X - \alpha^{(i)}),$$

akkor az $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ számokat az α *konjugáltjainak* nevezzük.

Egy $\mathbb{Q} \subset K \subset \mathbb{C}$ testet *algebrai számtestnek* nevezünk, ha a $K/\mathbb{Q}$ testbővítés véges. Ha $[K : \mathbb{Q}] = n$, akkor létezik olyan n-edfokú algebrai szám, hogy $K = \mathbb{Q}(\alpha)$. Ekkor a K test egy $\mathbb{Q}$ fölötti vektortérnek tekinthető, amelynek a dimenziója n, és egy bázisa $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$, azaz tetszőleges $\beta \in K$ szám egyértelműen írható fel

$$\beta = r_0 + r_1\alpha + r_2\alpha^2 + \ldots + r_{n-1}\alpha^{n-1}$$

alakban, ahol $r_0, r_1, \ldots, r_{n-1}$ racionális számok. A $\beta \in K$ *relatív konjugáltjai* alatt a

$$\beta^{(i)} = r_0 + r_1\alpha^{(i)} + r_2(\alpha^{(i)})^2 + \ldots + r_{n-1}(\alpha^{(i)})^{n-1}, \qquad (i = 1, \ldots, n)$$

számokat értjük.

A β számot *algebrai egésznek* nevezzük, ha a β egész együtthatós definiáló polinomjának főegyütthatója 1. A K-beli algebrai egészek halmaza gyűrűt alkot, melyet $\mathbb{Z}_K$-val jelölünk. Ekkor $\mathbb{Z}_K$ egy teljes modulus K-ban $\mathbb{Z}$ fölött, melynek egy bázisát a K test *egész bázisának* nevezzük. Ha tehát $(\omega_1 = 1, \omega_2, \ldots, \omega_n)$ a K egy egész bázisa, akkor tetszőleges $\beta \in \mathbb{Z}_K$ algebrai egész egyértelműen írható fel

$$\beta = z_1 + z_2\omega_2 + \ldots + z_n\omega_n$$

alakban, ahol $z_1, z_2, \ldots, z_n$ egész számok. Mivel az $\omega_1 = 1, \omega_2, \ldots, \omega_n$ lineárisan függetlenek $\mathbb{Z}$ fölött (és így $\mathbb{Q}$ fölött is), ezért $(1, \omega_2, \ldots, \omega_n)$ bázisa K-nak $\mathbb{Q}$-fölött. Így a β relatív konjugáltjai

$$\beta^{(i)} = z_1 + z_2\omega_2^{(i)} + \ldots + z_n\omega_n^{(i)}, \qquad (i = 1, \ldots, n)$$

alakban írhatók.

Legyen $(\alpha_1, \ldots, \alpha_n)$ egy bázisa K-nak $\mathbb{Q}$ felett, ekkor a *bázis diszkriminánsa* alatt a

$$D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \ldots & \alpha_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \ldots & \alpha_n^{(n)} \end{vmatrix}^2$$

mennyiséget értjük. Két különböző bázis diszkriminánsa között a bázistranszformációs mátrix teremt kapcsolatot. Legyenek $(\alpha_1, \ldots, \alpha_n)$ és $(\beta_1, \ldots, \beta_n)$ bázisai K-nak $\mathbb{Q}$ felett. Legyen $M = (m_{ij})_{n\times n}$ a köztük ható bázistranszformációs mátrix, $\beta_i = \sum_{j=1}^{n} m_{ij} \cdot \alpha_j$, azaz

$$M \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Ekkor a két bázis diszkriminánsa között az alábbi összefüggés áll fenn,

$$D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \det(M)^2 \cdot D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n).$$

Egy primitív $\alpha \in K$ *elem* $D_{K/\mathbb{Q}}(\alpha)$ *diszkriminánsa* alatt az általa generált $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ hatványbázis diszkriminánsát értjük, ami a Vandermonde-féle determináns kifejtése alapján az alábbi módon is számolható:

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

vagyis α diszkriminánsa pontosan a definiáló polinomjának a diszkriminánsa. A K *test diszkriminánsa* alatt egy tetszőleges $(\omega_1, \omega_2, \ldots, \omega_n)$ egész bázisának a diszkriminánsát értjük, és D_K-val jelöljük. Ez független az egész bázis megválasztásától.

Legyen most $(\alpha_1, \ldots, \alpha_n)$ egy algebrai egész elemekből álló bázisa K-nak $\mathbb{Q}$ felett. Ekkor

$$D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = J^2 \cdot D_K, \tag{2.1}$$

ahol J egy tetszőleges egész bázisból az $(\alpha_1, \ldots, \alpha_n)$ bázisba ható bázistranszformációs mátrix determinánsa. Megmutatható, hogy J éppen a $\left(\mathbb{Z}_K^+ : \mathcal{O}\right)$ modulus indexszel egyezik meg, ahol $\mathcal{O}$ az $\alpha_1, \ldots, \alpha_n$ elemek által generált modulus (ld. [53] Proposition 2.13).

Ha α egy primitív algebrai egész K-ban, akkor $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ algebrai egész elemekből álló bázisa K-nak $\mathbb{Q}$ felett. Ekkor K-ban az $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ elemek által generált modulus megegyezik a $\mathbb{Z}[\alpha]$ gyűrűbővítés additív csoportjával, mint $\mathbb{Z}$ feletti modulussal. A $(\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+)$ modulus indexet az α *indexének* nevezzük, és $I(\alpha)$-val jelöljük. A fentiek alapján tehát

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

2.1. Egész bázisok kiszámítása, hasznos eszközök és módszerek

Ebben a fejezetben egy adott algebrai számtest egy egész bázisának kiszámításához kapcsolódó módszereket gyűjtöttem össze a teljesség igénye nélkül. Az egész bázis kiszámítására jelenleg több hatékony algoritmus létezik, közülük a legelterjedtebb a *Round Four* algoritmus (ld. [57] Chapter 4.). Annak ellenére, hogy a legtöbb számelméleti programcsomagba ez az eljárás van beépítve, és meglehetősen jó futási idővel dolgozik konkrét számtestek esetén, a módszert nem fogom részletezni, mivel parametrikus esetben a használata kifejezetten nehézkes. Helyette egy lényegesen rosszabb futási idejű, de sokkal egyszerűbben alkalmazható eljárást idézek, amely az egyszerűségéből fakadóan parametrikus esetben is hatékony lesz. A módszer csupán az előző részben megemlített alapvető ismereteket használja ki (egy részletesebb és példákon keresztül bemutatott leírás található J. P. Cook [10] összefoglalójában).

2.1.1. Egész bázis kiszámítása: a favágó módszer

Legyen α egy n-edfokú algebrai egész, és $K = \mathbb{Q}(\alpha)$. Ekkor

$$(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$$

algebrai egészekből álló bázisa K-nak $\mathbb{Q}$ felett. A módszer ezt a bázist (vagy a K egy alkalmas algebrai egész elemekből álló bázisát) fogja több lépésben redukálni.

1. Tekintsük a K egy algebrai egész elemekből álló $(\alpha_1, \ldots, \alpha_n)$ bázisát, és számítsuk ki a diszkriminánsát.

2. Ha azt tapasztaljuk, hogy a diszkrimináns négyzetmentes, akkor kész is vagyunk, hiszen (2.1) alapján az $\alpha_1, \ldots, \alpha_n$ által generált modulus indexe $\mathbb{Z}_K^+$-ban csak 1 lehet, azaz $(\alpha_1, \ldots, \alpha_n)$ egész bázis. Ha nincs ilyen szerencsénk, akkor válasszunk egy p prímet, amelynek a négyzete osztja a bázis diszkriminánsát, és folytassuk a következő lépéssel.

3. Tekintsük az összes
$$\frac{\lambda_1\alpha_1 + \lambda_2\alpha_2 + \ldots + \lambda_n\alpha_n}{p}$$
alakú algebrai számot, ahol $0 \leq \lambda_i \leq p-1,\ \lambda_i \in \mathbb{Z},\ (i = 1, \ldots, n)$. Számítsuk ki a definiáló polinomjaikat, és vizsgáljuk meg, hogy közülük melyek algebrai egészek.

4. Ha a $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$ eseten kívül egyik sem algebrai egész, akkor válasszunk egy másik prímet, amelynek a négyzete osztja a bázis diszkriminánsát, és az előző lépéstől kezdve folytassuk az eljárást az új prímmel. Amennyiben már minden prímet megvizsgáltunk, és nincs az elemek között algebrai egész, akkor az eljárás véget ér, és a bemeneti bázis egész bázis lesz.

5. Ha találunk nem nulla algebrai egészeket, akkor p osztja az $\alpha_1, \ldots, \alpha_n$ által generált modulus indexét, így redukálnunk kell a bázist. Tegyük fel, hogy

$$\beta = \frac{\lambda_1\alpha_1 + \lambda_2\alpha_2 + \ldots + \lambda_n\alpha_n}{p}$$

egy olyan algebrai egész elem, amelyben nem minden λ_i együttható 0. Az általánosság megszorítása nélkül feltehetjük, hogy $\lambda_1 \neq 0$ (máskülönben átrendezzük a bázis elemeit). Legyen

$$r \equiv \lambda_1^{-1} \pmod{p},$$

és számítsuk ki az $r\cdot\beta$ elemet. Tegyük fel, hogy $r\cdot\lambda_i = p\cdot\mu_i + \lambda_i'$, $(i = 1, \ldots, n)$, ahol $0 \leq \lambda_i' \leq p-1$ és $\lambda_i', \mu_i \in \mathbb{Z}$. Ekkor $r \cdot \beta$ az alábbi módon írható:

$$r \cdot \beta = \frac{\lambda_1'\alpha_1 + \lambda_2'\alpha_2 + \ldots + \lambda_n'\alpha_n}{p} + \mu_1\alpha_1 + \mu_2\alpha_2 + \ldots + \mu_n\alpha_n,$$

ahonnan

$$\beta' = \frac{\lambda_1'\alpha_1 + \lambda_2'\alpha_2 + \ldots + \lambda_n'\alpha_n}{p} = r \cdot \beta - (\mu_1\alpha_1 + \mu_2\alpha_2 + \ldots + \mu_n\alpha_n)$$

szintén algebrai egész, hiszen két algebrai egész különbségeként írható. Továbbá $r \equiv \lambda_1^{-1} \pmod{p}$ miatt $\lambda_1' = 1$. Összefoglalva ez annyit jelent, hogy ha létezik olyan algebrai egész a fenti alakban, amelyben $\lambda_1 \neq 0$, akkor létezik olyan algebrai egész is, amelyben $\lambda_1 = 1$. Válasszunk β-nak egy ilyen elemet, és tekintsük a $(\beta, \alpha_2, \alpha_3, \ldots, \alpha_n)$ algebrai egész elemekből álló bázist. A β megválasztása alapján világos, hogy a $\beta, \alpha_2 \ldots, \alpha_n$ által generált modulus tartalmazza az $\alpha_1, \alpha_2 \ldots, \alpha_n$ által generált modulust. Továbbá az $M : (\alpha_1, \ldots, \alpha_n) \mapsto (\beta, \alpha_2, \ldots, \alpha_n)$ bázistranszformáció mátrixa:

$$M = \begin{pmatrix} \frac{1}{p} & \frac{\lambda_2}{p} & \frac{\lambda_3}{p} & \ldots & \frac{\lambda_n}{p} \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

tehát az új "redukált" bázis diszkriminánsa $\frac{1}{p^2}$-szerese az eredeti bázis diszkriminánsának.

6. Folytassuk az eljárást az 1. lépéstől a redukált bázisból kiindulva.

Mivel minden egyes lépésben vagy leáll az algoritmus, és megadja az egész bázist, vagy $\frac{1}{p^2}$-szeresére csökkenti a kiindulási diszkriminánst, ezért véges sok lépésben biztosan véget ér. Vegyük észre, hogy egy lépés során p^n darab elemnek a definiáló polinomját kell kiszámolni, ami eléggé számításigényes feladat, de ha valamilyen módon sikerül felülről becsülni a $(\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+)$ indexet, vagy korlátozni a vizsgálandó prímek halmazát, akkor a módszer könnyen alkalmazható parametrikus esetben is.

2.1.2. Hermite normál alakú egész bázis

Az előző fejezetben ismertetett algoritmus kimenetele függ az 5. pontban választott algebrai egésztől. Ez nem meglepő, hiszen egy számtestben végtelen sok egész bázist meg lehet adni. A testet generáló α elem rögzítése után van azonban ezek között egy bizonyos értelemben kitüntetett alakú bázis, amit az α-ra vonatkozó Hermite normál alakú egész bázisnak fogunk nevezni. Ennek a bázisnak a speciális tulajdonságai sok esetben megkönnyítik a bizonyításainkat.

A fejezet további részében H. Cohen [8] könyvének 2.4 és 4.7 fejezeteinek néhány idevágó eredményét foglalom össze. Tekintsünk egy teljes modulust $\mathbb{Z}^n$-ben. A modulus egy bázisa által meghatározott $n \times n$-es egész elemű A mátrix determinánsa nem nulla, továbbá tetszőleges U unimoduláris mátrix esetén az AU mátrix sorai szintén egy bázisát alkotják a modulusnak. Azt mondjuk, hogy egy nemnegatív egész elemű, nem nulla determinánsú $M = (m_{ij})_{n \times n}$ mátrix Hermite normál alakú, ha

- alsó háromszög alakú, ($m_{ij} = 0$, ha $j > i$),
- a főátlóban lévő elemek pozitívak, és az oszlopaikban dominánsak ($0 \leq m_{ij} < m_{jj}$, ha $i > j$).

Megmutatható, hogy tetszőleges $A \in \mathbb{Z}^{n \times n}$ mátrix esetén egyértelműen létezik olyan M mátrix, hogy M Hermite-féle normál alakú, és valamely U unimoduláris mátrixszal, $M = AU$. Továbbá, ez az M mátrix algoritmikusan meghatározható. Speciálisan, ha adva van $\mathbb{Z}^n$-ben n darab lineárisan független vektor, akkor az általuk generált $\mathbb{Z}$-modulusban egyértelműen meg tudunk adni egy olyan bázist, aminek a mátrixa Hermite-féle normál alakú.

Legyen K egy n-edfokú algebrai számtest, és legyen $(\alpha_1, \ldots, \alpha_n)$ egy bázisa K-nak $\mathbb{Q}$ felett. Ekkor a

$$K \mapsto \mathbb{Q}^n,$$

$$\alpha_i \mapsto e_i, \qquad (i = 1, \ldots, n),$$

megfeleltetés, ahol e_i az i. egységvektort jelöli $\mathbb{Q}^n$-ben, egy vektortér izomorfizmus. Ezen megfeleltetés szerint az $(\alpha_1, \ldots, \alpha_n)$ elemek által generált modulus képe $\mathbb{Z}^n$-nek felel meg.

Legyen R egy tetszőleges teljes modulus K-ban, és $(\psi_1, \psi_2, \ldots, \psi_n)$ az R egy $\mathbb{Z}$-bázisa. Mivel a ψ_i számok K-ban vannak, ezért létezik olyan d egész szám, hogy az $(\alpha_1, \ldots, \alpha_n)$ elemek által generált modulus minden $i = 1, \ldots, n$ esetén tartalmazza a $d\psi_i$ elemeket. A legkisebb ilyen d számot az R modulus $(\alpha_1, \ldots, \alpha_n)$-re vonatkozó nevezőjének mondjuk.

Alkalmas $d \in \mathbb{Z}$ számmal tehát a dR képe a fenti izomorfizmus mentén teljes modulus lesz $\mathbb{Z}^n$-ben, amelynek egyértelműen létezik Hermite normál alakú bázisa. Legyen M ehhez a Hermite normál alakú bázishoz tartozó mátrix, és $\beta_1, \ldots, \beta_n \in K$

a bázisvektorokhoz tartozó elemek a vektortér izomorfizmus mentén. Ekkor

$$M \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix},$$

ahol a $\beta_1, \ldots, \beta_n$ és $d\psi_1, \ldots, d\psi_n$ számok által generált K-beli modulusok megegyeznek. Ha tehát $\gamma_i = \frac{1}{d} \cdot \beta_i$, $(i = 1, \ldots, n)$, akkor

$$\frac{1}{d} \cdot M \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix},$$

ahol M továbbra is Hermite normál alakú, és a $\gamma_1, \ldots, \gamma_n$ és $\psi_1, \ldots, \psi_n$ által meghatározott modulusok megegyeznek. Ekkor $(\gamma_1, \ldots, \gamma_n)$ bázisa K-nak $\mathbb{Q}$ felett, melyet az R modulus $(\alpha_1, \ldots, \alpha_n)$*-hez tartozó Hermite normál alakú bázisának* nevezünk. A fenti számolásban kapott $(\gamma_1, \ldots, \gamma_n)$ bázishoz tartozó egyértelmű (d, M) párt pedig az R modulus $(\alpha_1, \ldots, \alpha_n)$*-hez tartozó Hermite normál alakjának* hívjuk.

Ha $R = \mathbb{Z}_K$, akkor az így kapott $(\gamma_1, \ldots, \gamma_n)$ bázist egyszerűen a K *test* $(\alpha_1, \ldots, \alpha_n)$*-hez tartozó Hermite normál alakú egész bázisának* nevezzük. Továbbá, ha $K = \mathbb{Q}(\alpha)$, akkor az $(\alpha_1, \ldots, \alpha_n) = (1, \alpha, \ldots, \alpha^{n-1})$ választás mellett röviden azt mondjuk, hogy a $(\gamma_1, \ldots, \gamma_n)$ bázis az R modulus α*-hoz tartozó Hermite normál alakú bázisa.*

A Hermite normál alak értelemszerűen kiterjeszthető nem négyzetes mátrixokra is (ld. [8], Definition 2.4.2.). Két $n \times n$-es egész elemű, invertálható mátrix konkatenációjaként kapott $2n \times n$-es mátrix Hermite normál alakjában az utolsó n sor csupa 0 lesz, így ezeket elhagyva a megmaradt $n \times n$-es mátrixot nevezzük a két mátrix közös Hermite normál alakjának. Erre úgy tekinthetünk, hogy a keletkezett mátrix sorai által generált modulus a legszűkebb, ami tartalmazza az eredeti mátrixok sorai által generált modulusokat.

Ennek segítségével, ha $(\psi_1, \psi_2, \ldots, \psi_n)$ és $(\omega_1, \omega_2, \ldots, \omega_n)$ két bázisa $K = \mathbb{Q}(\alpha)$-nak, valamint R_1 a $\psi_1, \psi_2, \ldots, \psi_n$, és R_2 az $\omega_1, \omega_2, \ldots, \omega_n$ elemek által generált $\mathbb{Z}$-modulusok, akkor könnyen kiszámítható az $R_1 + R_2$ modulus egy α-hoz tartozó Hermite normál alakú bázisa. Legyen ugyanis (d_1, M_1) és (d_2, M_2) az R_1 és R_2 modulusok Hermite normál alakja, és M a $d_2 M_1$ és $d_1 M_2$ mátrixok közös Hermite normál alakja. Ekkor az $R_1 + R_2$ modulus α-hoz tartozó Hermite normál alakja $(d_1 \cdot d_2, M)$ lesz.

A következő fejezetekben egy algebrai egész elem indexének becslésére illetve kiszámítására mutatok olyan módszereket, amelyek parametrikus esetben is jól használhatóak lesznek. Az első a duális bázis módszere, ami korlátozza egy β algebrai egész elem együtthatóinak nevezőjét egy $(\alpha_1, \ldots, \alpha_n)$ algebrai egészekből álló bázisra vonatkozóan. A másik a Newton-poligonok egy alkalmazása lesz, amely Ø.

Ore [56] nevéhez fűződik. Habár ez csak egy egyszerű alkalmazása Ore eredményeinek, a cikk ezeken messze túlmutat. J. Montes és E. Nart [52] Ore eredményeinek általánosításával olyan algoritmust dolgoztak ki, amely a korábbiaknál lényegesen hatékonyabban képes kiszámítani egy test egész bázisát, illetve egy $p \in \mathbb{Z}$ prím esetén a $p\mathbb{Z}_K$ prímideál faktorizációját.

2.1.3. Az index becslése I: Duális bázis

Legyen α egy n-edfokú algebrai egész, és $K = \mathbb{Q}(\alpha)$. A célunk felső becslést adni az α indexére. Mivel $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ bázisa K-nak $\mathbb{Q}$ felett, ezért minden $\beta \in \mathbb{Z}_K$ egyértelműen írható fel

$$\beta = \frac{z_0 + z_1\alpha + \ldots + z_{n-1}\alpha^{n-1}}{d} \tag{2.2}$$

alakban, ahol $z_0, \ldots, z_{n-1}, d \in \mathbb{Z}$, $\mathrm{lnko}(z_0, \ldots, z_{n-1}, d) = 1$.

Legyen most $(\alpha_1, \ldots, \alpha_n)$ egy tetszőleges algebrai egész elemekből álló bázisa K-nak. Ekkor a

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \cdot \alpha_j^*) = \begin{cases} 1, & \text{ha } i = j, \\ 0, & \text{ha } i \neq j, \end{cases}$$

által egyértelműen meghatározott $\alpha_1^*, \ldots, \alpha_n^*$ számok szintén bázist alkotnak K-ban, amit az $(\alpha_1, \ldots, \alpha_n)$ duális bázisának nevezünk. Egy algebrai egész elemekből álló bázis duális bázisának haszna abban rejlik, hogy segítségével tetszőleges $\beta \in \mathbb{Z}_K$ algebrai egész, racionális egész együtthatókkal írható fel. Valóban, tekintsünk egy

$$\beta = f_1\alpha_1^* + \ldots + f_n\alpha_n^*$$

algebrai egész elemet K-ban. A duális bázis definíciója és a nyom linearitása alapján

$$\mathrm{Tr}_{K/\mathbb{Q}}(\beta \cdot \alpha_i) = \sum_{j=1}^{n} f_j \cdot \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_j^* \cdot \alpha_i) = f_i$$

teljesül minden $i = 1, \ldots, n$ esetén. Mivel β és α_i algebrai egészek, a szorzatuk is algebrai egész, aminek a nyoma racionális egész szám így adódik, hogy f_i racionális egész minden $i = 1, \ldots, n$ esetén. Ennélfogva, az $\alpha_1^*, \ldots, \alpha_n^*$ elemek által generált modulus K-ban tartalmazza a $\mathbb{Z}_K$ algebrai egészek gyűrűjét.

Tegyük fel most, hogy $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ az $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ duális bázisa, és legyen

$$\gamma_i = \frac{z_{i,0} + z_{i,1}\alpha + \ldots + z_{i,n-1}\alpha^{n-1}}{d_i}, \qquad (i = 1, \ldots, n)$$

a γ_i elemek felírása az (2.2) alakban. Az előzőek alapján tetszőleges algebrai egész együtthatói racionális egész számok a $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ bázisra vonatkozóan, így (2.2)-ban lévő d nevezőre

$$d \mid \mathrm{lkkt}(d_1, d_2 \ldots, d_n)$$

teljesül. Ez a legkisebb közös többszörös sok esetben lényegesen kisebb, mint az eredetileg feltételezett lehető legnagyobb J modulus index, vagyis az a szám, melyre $D(\alpha)/J^2$ négyzetmentes, így ezzel jelentősen csökkenthetjük a vizsgálandó esetek számát.

További előnye még a duális bázisnak, hogy gyakran számolás nélkül is könnyű "kitalálni" az elemeit. Az ilyen esetekben ez szolgáltat egy azonnali képletet is a kiindulási bázis diszkriminánsára vonatkozóan, ugyanis a duális bázis definíciója alapján

$$D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \cdot D_{K/\mathbb{Q}}(\alpha_1^*, \ldots, \alpha_n^*) = 1,$$

így, ha

$$M \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \alpha_1^* \\ \alpha_2^* \\ \vdots \\ \alpha_n^* \end{pmatrix},$$

akkor

$$|D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)| = \frac{1}{|\det(M)|}.$$

2.1.4. Az index becslése II: Newton poligonok

Ebben a részben a Newton poligonok egy alkalmazását mutatom be Ø.Ore [56] cikke alapján, amely alkalmas arra, hogy tetszőleges p prím esetén pontosan megadja egy algebrai egész elem indexének p-adikus rendjét. Ehhez elsőként ki kell terjesztenünk a szokásos

$$v_p : \mathbb{Q} \mapsto \mathbb{Z}$$

p-adikus rendet a racionális együtthatós polinomokra a következő módon:

$$v_p : \mathbb{Q}(X) \mapsto \mathbb{Z},$$

$$v_p(a_0 + a_1X + a_2X^2 + \ldots + a_nX^n) := \min_{0 \le i \le n} \{v_p(a_i)\}.$$

Most legyen $f(X) \in \mathbb{Z}[X]$ tetszőleges 1 főegyüttható polinom, $\phi(X) \in \mathbb{Z}[X]$ pedig olyan 1 főegyüttható polinom, melynek $\overline{\phi(X)}$ redukciója modulo p irreducibilis, és $\overline{\phi(X)} \mid \overline{f(X)} \pmod p$. Ekkor $f(X)$ egyértelműen írható fel $\phi(X)$ polinomjaként a következő alakban:

$$f(X) = a_0(X) + a_1(X)\phi(X) + a_2(X)\phi(X)^2 + \ldots + a_r(X)\phi(X)^r,$$

ahol $a_i(X) \in \mathbb{Z}[X]$ és $\deg(a_i(X)) < \deg(\phi(X))$. Ezt nevezzük az $f(X)$ polinom ϕ-adikus kifejtésének.

Tekintsük az euklideszi síkon az alábbi ponthalmazt:

$$\{(i, v_p(a_i(X))) \in \mathbb{R}^2 : 0 \le i \le r\}.$$

Az $f(X)$ polinom *ϕ-Newton poligonja* ezen pontok alsó konvex burka, tehát szemléletesen az a törött vonal, amit a pontok konvex burkaként kapott sokszögből

"alulról látunk".

Példa: Legyen $p = 5$ és

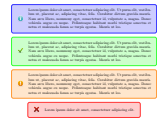
$$f(X) = X^{16} + 141X^{14} + 75X^{13} + 1787X^{12} + 905X^{11} + 10048X^{10} + 4675X^9 + 32120X^8 + \\ +14450X^7 + 63167X^6 + 28875X^5 + 76192X^4 + 34325X^3 + 50474X^2 + 18735X + 13181.$$

Ekkor

$$f(X) \equiv (X^2 + 2)^8 \pmod 5.$$

Válasszuk $\phi(X)$-et $X^2 + 2$-nek, így

$$a_0(x) = 625(X + 1),$$
$$a_1(x) = 625(X - 2),$$
$$a_2(x) = 25(-X + 6),$$
$$a_3(x) = 625(2X - 1),$$
$$a_4(x) = 125(X + 4),$$
$$a_5(x) = 5X,$$
$$a_6(x) = 25(3X - 3),$$
$$a_7(x) = 125,$$
$$a_8(x) = 1.$$



A piros pontok jelölik az $\{(i, v_p(a_i(X))) \in \mathbb{R}^2 : 0 \leq i \leq 8\}$ halmaz elemeit, és a kék törött vonal az $f(X)$ ϕ-Newton poligonja.

Az $f(X)$ polinom ϕ-adikus kifejtéséhez vegyük észre, hogy ha $q_i(X)$ jelöli az $f(X)/\phi(X)^i$ maradékos osztás hányadosát, akkor

$$q_i(X) = q_{i+1}(X) \cdot \phi(X) + a_i(X),$$

így a ϕ-adikus kifejtés valóban egyértelmű, és gyorsan kiszámítható.

A ϕ-Newton poligon negatív meredekségű szakaszai által meghatározott törött vonalat a poligon *fő részének* nevezzük és $N_\phi^-(f)$-el jelöljük. A $\phi(X)$ fokszámának és a sík azon pontjainak a számának szorzatát, amelyek mindkét koordinátája pozitív, és $N_\phi^-(f)$-en, vagy az alatt helyezkednek el, az $f(X)$ polinom *ϕ-indexének* nevezzük és $\mathrm{ind}_\phi(f)$-el jelöljük. Látható, hogy a fenti példában a ϕ-Newton poligon fő része megegyezik a teljes poligonnal (az alkalmazásaink jelentős részében is ugyanezt fogjuk tapasztalni), és könnyen összeszámolható, hogy az $f(X)$ polinom ϕ-indexe $2 \cdot 8 = 16$. Az index szó már utal arra, hogy ennek lesz valamilyen kapcsolata egy algebrai elem indexével, de mielőtt kimondanánk az Ore-féle indextételt, szükség van még egy definícióra.

Jelöljük $\overline{g(X)}$-el egy $g(X) \in \mathbb{Z}[X]$ polinom redukcióját modulo p, és legyen $c_i \in \mathbb{Z}[X]/(p, \phi(X))$, $(i = 0, \ldots, r)$, az alábbi módon definiálva,

$$c_i = \begin{cases} \overline{\left(\frac{a_i(X)}{p^{v_p(a_i(X))}}\right)}, & \text{ha } (i, v_p(a_i(X))) \in N_\phi^-(f), \\ 0, & \text{ha } (i, v_p(a_i(X))) \notin N_\phi^-(f). \end{cases}$$

Most tekintsük az $N_\phi^-(f)$ egy S oldalát. Legyen ennek az oldalnak a meredeksége $\lambda = \frac{-h}{e}$, ahol h és e pozitív relatív prím egészek. Legyen l az S oldal x tengelyre eső merőleges vetületének a hossza, és legyen $d := \frac{l}{e}$. Ekkor l-t az S hosszának, míg d-t a S fokának nevezzük. A fokszám lényegében azt mutatja meg, hogy az S oldalt hány részre bontják a rajta elhelyezkedő egész koordinátájú pontok. A fenti példában $N_\phi^-(f)$-nek 2 oldala van, az első oldal hossza 2, a másodiké 6, és mindkét oldal foka 2.

Legyen t az S oldal kezdőpontjának abszcisszája, ekkor az

$$R_\lambda(f)(Y) := c_t + c_{t+e}Y + \ldots + c_{t+de}Y^d \in (\mathbb{Z}[X]/(p, \phi(X)))[Y]$$

polinomot az S oldalhoz (vagy λ meredekséghez) tartozó *maradék polinomnak* nevezzük. A maradék polinomot úgy kell elképzelni, hogy tekintjük $N_\phi^-(f)$-nek egy oldalát, kiszámoljuk az oldal fokát (ami egyben a maradék polinom fokszáma is), végighaladunk az oldalra illeszkedő egész koordinátájú (i, j) pontokon, és ha $j = v_p(a_i(X))$, akkor a maradék polinomban az Y megfelelő fokszámú tagjának együtthatója $\overline{\left(\frac{a_i(X)}{p^{v_p(a_i(X))}}\right)}$ lesz, egyébként pedig 0.

A példánkban az első oldal meredeksége -1, a hozzá tartozó maradék polinom pedig

$$R_{-1}(f)(Y) = c_0 + c_1Y + c_2Y^2 = (X + 1) + (-X + 6)Y^2.$$

A másik oldal meredeksége $-\frac{1}{3}$, a hozzá tartozó maradék polinom pedig

$$R_{-\frac{1}{3}}(f)(Y) = c_2 + c_5Y + c_8Y^2 = (-X + 6) + XY + Y^2.$$

Azt mondjuk, hogy $f(X)$ *ϕ-reguláris*, ha az $N_\phi^-(f)$ összes oldalához tartozó maradék polinom szeparábilis. Mivel a

$$\mathbb{Z}[X]/(p, \phi(X)) \cong \mathbb{F}_{p^{\deg(\phi(X))}}$$

test tökéletes, a regularitási tulajdonság egyenértékű azzal, hogy a maradék polinomok négyzetmentesek, azaz $R_\lambda(f)(Y)$ és formális Y-szerinti deriváltja relatív prímek a $\mathbb{Z}[X]/(p, \phi(X))$ polinomgyűrűben, ami könnyen ellenőrizhető.
A következő tételre Ore-féle index-tételként hivatkozik a szakirodalom. Ez teremt kapcsolatot egy algebrai egész indexe, és a definiáló polinomjának ϕ indexei között.

2.1. Tétel. *Legyen p prím, $f \in \mathbb{Z}[X]$ egy 1 főegyütthatós polinom, és legyenek $\phi_1, \phi_2, \ldots, \phi_k \in \mathbb{Z}[X]$ olyan 1 főegyütthatós polinomok, melyek redukciói modulo p az $f(X)$ különböző irreducibilis faktorai. Legyen továbbá α az $f(X)$ egy gyöke, ekkor*

$$v_p(I(\alpha)) \geq \mathrm{ind}_{\phi_1}(f) + \ldots + \mathrm{ind}_{\phi_k}(f),$$

ahol pontosan akkor áll fenn egyenlőség, ha $f(X)$ ϕ_i-reguláris minden $i = 1, \ldots, k$ esetén.

Annak ellenére, hogy a regularitás korlátozza a tétel alkalmazhatóságát, a dolgozatban szereplő példák mindegyikében teljesülni fog ez a tulajdonság, így a fenti tételt minden esetben egyenlőséggel fogjuk tudni használni. Emellett Ore megmutatta, hogy tetszőleges számtestet lehet generálni olyan elemmel, amelynek a definiáló polinomja minden esetben reguláris.

Egy egyszerű és hatékonyan alkalmazható következménye a fenti tételnek a következő állítás.

2.2. Állítás. *Legyen p prím, $f \in \mathbb{Z}[X]$ egy 1 főegyütthatós n-edfokú polinom, amely p-Eisenstein. Legyen α az $f(X)$ egy gyöke. Ekkor*

$$v_p(I(\alpha)) = 0$$

Bizonyítás: Könnyű látni, hogy ha $f(X)$ p-Eisenstein, akkor $f(X) \equiv X^n \pmod{p}$, így csak egy irreducibilis faktora van modulo p, mégpedig a $\phi(X) = X$. Ekkor azonban az $f(X)$ ϕ-adikus kifejtése megegyezik $f(X)$-el, aminek a ϕ-Newton poligonja a $(0;1)$ és $(n;0)$ pontokat összekötő $-\frac{1}{n}$ meredekségű szakasz. Ennek a szakasznak a foka 1, így a hozzá tartozó maradék polinom fokszáma is 1, tehát nyilvánvalóan szeparábilis, és így az indextétel szerint

$$v_p(I(\alpha)) = \mathrm{ind}_\phi(f)$$

Azonban, $\mathrm{ind}_\phi(f) = 0$, hiszen egyetlen pozitív egész koordinátájú pont sincs a $(0;1)$ és $(n;0)$ pontokat összekötő szakasz alatt. □

Legtöbbször ez a következmény szolgáltatja majd a megfelelő feltételeket ahhoz, hogy végtelen parametrikus számtestcsaládok esetén véges sok prímre korlátozzuk a vizsgálatainkat.

2.1.5. Periodikus egész bázisok

Ebben a fejezetben parametrikus számtestek egész bázisának egy speciális, úgynevezett periodikus tulajdonságáról lesz szó. A definíciót konkrét számítási példák motiválták, melyek arra engedtek következtetni, hogy bizonyos feltételek mellett az egész bázisok "alakja" csak a paraméternek egy konkrét, a fokszámtól függő n_0 számmal való osztási maradékától függ. A legegyszerűbb példa a másodfokú számtestek jól ismert egész bázisából adódik. Legyen $f_m(X) = X^2 - m$, ahol m egy négyzetmentes egész szám. Legyen továbbá α_m az $f_m(X)$ egy gyöke és $K = \mathbb{Q}(\alpha_m)$. Ekkor $(1, \omega)$ egész bázisa K-nak, ahol

$$\omega = \begin{cases} \alpha_m, & \text{ha } m \equiv 2,3 \pmod 4, \\ \frac{1+\alpha_m}{2}, & \text{ha } m \equiv 1 \pmod 4. \end{cases}$$

Ezek alapján azt mondhatjuk, hogy az egész bázis alakja K-ban csupán a paraméter 4-es maradékától függ, vagyis ismétlődik modulo $n_0 = 4$. Ezt a jelenséget szeretnénk most precízebben leírni.

2.3. Definíció. Legyen $f_m(X) \in \mathbb{Z}[m][X]$ egy n-edfokú polinom, ahol $m \in \mathbb{Z}$ egy egész paraméter. Legyen α_m az $f_m(X)$ egy gyöke és $K = \mathbb{Q}(\alpha_m)$. Azt mondjuk, hogy a K *testek egész bázisa periodikusan ismétlődik modulo* n_0, ha minden $r = 0, \ldots, n_0 - 1$ esetén léteznek olyan $h_i^{(r)}(X) \in \mathbb{Q}[X]$ polinomok $(i = 0, \ldots, n-1)$, hogy ha $m \equiv r \pmod{n_0}$ és $f_m(X)$ irreducibilis, akkor

$$\left(h_0^{(r)}(\alpha_m), h_1^{(r)}(\alpha_m), \ldots, h_{n-1}^{(r)}(\alpha_m)\right)$$

egész bázist alkot K-ban.

A definícióban kiemelt szerepet játszik, hogy a K testeket egy parametrikus polinomcsalád különböző paramétereihez tartozó gyökeivel generáljuk. Enélkül nem is lenne igazán értelme periodikus egész bázisról beszélni. Azt is mondhatnánk, hogy ez a tulajdonság valójában nem is a számtesthez, hanem inkább a parametrikus polinomcsaládhoz köthető.

Láthatjuk, hogy a definíció értelmében az $f_m(X) = X^2 - m$ polinom gyöke által generált test egész bázisa tehát periodikusan ismétlődik modulo 4, amennyiben m négyzetmentes. Ha ilyen egyéb feltételek teljesülése esetén beszélhetünk csak periodikus egész bázisról, akkor a paramétereinket megszorítjuk, és csak a fennmaradó számtestcsaládokra mondjuk ki a periodikusságot. Előfordul ilyenkor, hogy bizonyos r maradékosztályokban egyáltalán nem is lesz megfelelő m paraméter, ezeket a maradékosztályokat azokban az esetekben értelemszerűen figyelmen kívül hagyjuk, azokhoz nem keresünk $h_i^{(r)}(X)$ polinomokat. (Ilyen például az $r = 4$ eset $f_m(X) = X^6 - m$ esetén, mivel itt a négyzetmentességi feltétel szerint egyik m paraméter sem adhat 36-al osztva 4 maradékot.)

A Hermite normál alakú bázisokon keresztül megközelítve a problémát, a definíciót a következő módon fogalmazhatjuk át. Legyen (d_m, M_m) a $K = \mathbb{Q}(\alpha_m)$ egész bázisának α_m-hez tartozó Hermite normál alakja. Azt mondjuk, hogy a K testek egész bázisa periodikusan ismétlődik modulo n_0, ha $s \equiv t \pmod{n_0}$ esetén

$$(d_s, M_s) = (d_t, M_t).$$

Értelemszerűen, ha ez csak bizonyos m-re vonatkozó feltételek mellett teljesül, akkor ebben az esetben is figyelmen kívül hagyjuk a nem megfelelő paramétereket.

Egy fontos észrevétel, hogy ha $I(\alpha_m)$-re a paramétertől független felső becslést tudunk adni, akkor ez már maga után vonja a periodikus egész bázis tulajdonságot.

2.4. Állítás. *Legyen $f_m(X) \in \mathbb{Z}[m][X]$ egy n-edfokú polinom, ahol $m \in \mathbb{Z}$ egy egész paraméter. Legyen α_m az $f_m(X)$ egy gyöke és $K_m = \mathbb{Q}(\alpha_m)$. Ha létezik olyan $C \in \mathbb{Z}$ szám, hogy*

$$C \cdot \mathbb{Z}_{K_m} \subset \mathbb{Z}[\alpha_m]$$

teljesül minden $m \in \mathbb{Z}$ esetén, akkor a K_m testek egész bázisa periodikusan ismétlődik modulo C^n.

Bizonyítás. Legyen $s, t \in \mathbb{Z}$ olyan számok, melyekre $C^n \mid (s-t)$. Meg fogjuk mutatni, hogy a $(d_s, M_s) = (d_t, M_t)$. Ehhez elegendő azt igazolni, hogy a $C \cdot \mathbb{Z}_{K_s}$ és a $C \cdot \mathbb{Z}_{K_t}$ modulusok képei a szokásos $\mathbb{Q}(\alpha_m) \mapsto \mathbb{Q}^n$ leképezés mentén, ugyanazt a $\mathbb{Z}^n$-beli modulust határozzák meg, más szóval tetszőleges $z_i \in \mathbb{Z}$, $(i = 0, \ldots, n-1)$ számok esetén

$$\beta_t = \frac{z_0 + z_1\alpha_t + \ldots + z_{n-1}\alpha_t^{n-1}}{C}$$

pontosan akkor algebrai egész, ha

$$\beta_s = \frac{z_0 + z_1\alpha_s + \ldots + z_{n-1}\alpha_s^{n-1}}{C}$$

algebrai egész. Ehhez tekintsük tetszőleges $m \in \mathbb{Z}$ paraméter esetén a

$$C \cdot \beta_m = z_0 + z_1\alpha_m + \ldots + z_{n-1}\alpha_m^{n-1}$$

definiáló polinomját

$$\prod_{i=1}^{n} \left(X - C\beta_m^{(i)} \right) = \prod_{i=1}^{n} \left(X - z_0 - z_1\alpha_m^{(i)} - \ldots - z_{n-1} \left(\alpha_m^{(i)} \right)^{n-1} \right).$$

Ha β_m nem primitív eleme a testnek, akkor ez valójában $C\beta_m$ definiáló polinomjának a $|\mathbb{Q}(\alpha_m) : \mathbb{Q}(\beta_m)|$-edik hatványa, de ez nem változtat a bizonyítás menetén. A fenti szorzat szimmetrikus polinomja $\alpha_m^{(1)}, \alpha_m^{(2)}, \ldots, \alpha_m^{(n)}$-nek, így az együtthatói a szimmetrikus polinomok alaptétele alapján $f_m(X)$ együtthatóinak egész együtthatós polinomjai, amik viszont m-nek egész együtthatós polinomjai. Vagyis léteznek olyan $P_0, P_1, \ldots, P_{n-1} \in \mathbb{Z}[X]$ polinomok, hogy

$$\prod_{i=1}^{n} \left(X - C\beta_m^{(i)} \right) = X^n + P_{n-1}(m) \cdot X^{n-1} + \ldots + P_1(m) \cdot X + P_0(m).$$

Ekkor β_m pontosan akkor algebrai egész, ha az

$$\frac{1}{C^n} \left((CX)^n + P_{n-1}(m) \cdot (CX)^{n-1} + \ldots + P_1(m) \cdot (CX) + P_0(m) \right)$$

polinom egész együtthatós, azaz ha $C^n \mid C^i \cdot P_i(m)$ teljesül minden $i = 0, \ldots, n-1$ esetén. Mivel $C^n \mid (s-t)$, ezért $C^n \mid P_i(s) - P_i(t)$ minden $i = 0, \ldots, n-1$ esetén, azaz a fenti feltétel pontosan akkor teljesül $m = s$ esetén, ha teljesül $m = t$ esetén. Ez pedig pontosan azt jelenti, hogy β_t pontosan akkor algebrai egész, ha β_s is az. Így tehát a $C \cdot \mathbb{Z}_{K_s}$-hez és a $C \cdot \mathbb{Z}_{K_t}$-hez tartozó modulusok $\mathbb{Z}^n$-ben megegyeznek, ennélfogva a Hermite normál alakú bázisaik által alkotott mátrixok is ugyanazok, amiből

$$(d_s, M_s) = (d_t, M_t)$$

következik, azaz a K_m testek egész bázisa periodikusan ismétlődik modulo C^n. $\square$

Ennek az állításnak egy további következménye, hogy a 2.1.1 algoritmust paraméteres számtestek estén is könnyen lehet alkalmazni. Ez a többi algoritmus esetén komoly nehézségeket okozna. Az eljárás sarkalatos pontja, hogy a

$$\beta = \frac{\lambda_1\alpha_1 + \lambda_2\alpha_2 + \ldots + \lambda_n\alpha_n}{p}$$

elemekről eldöntsük, hogy algebrai egészek-e. Mivel az eredetileg használt $\alpha_1, \ldots, \alpha_n$ elemek algebrai egészek, így az állítás bizonyításában használt elv alapján az, hogy β algebrai egész-e, csupán a λ_i együtthatóktól, és a paraméter p^n-el való osztási maradékától függ. Tehát az algoritmust csupán egy plusz lépéssel kell megtoldanunk, amelyben a β elemek definiáló polinomját minden $m = 0, 1, \ldots, p^n - 1$ esetén meg kell vizsgálni. Ez sajnos az eddigi p^n vizsgálat esetén újabb p^n esetet jelent, ami már erősen korlátozza az alkalmazhatóságot nagy fokszámok, és nagy prímek esetén.

A periodikus egész bázis jelentősége akkor kerül előtérbe, amikor végtelen sok számtest egészeivel kapcsolatban szeretnénk állításokat megfogalmazni. Ilyen például, amikor egy parametrikus számtestcsaládban vizsgáljuk a monogenitási tulajdonságot. Mivel a monogenitáshoz előzetesen szükség van egy egész bázisra, ezért ha ez az egész bázis periodikusan ismétlődik, akkor a vizsgálatainkat véges sok esetre korlátozhatjuk, amelyekben parametrikusan végezhetjük a számításokat.

2.2. Monogenitás, hatvány egész bázis

Ebben a fejezetben összefoglalom a monogenitáshoz kapcsoló alapvető definíciókat, és állításokat, amelyeket a további fejezetekben fel szeretnék használni, természetesen itt is a teljesség igénye nélkül. Részletes és áttekintő képet kaphatunk a témakör eredményeiről Gaál István [21] és [22] könyveiből.

Legyen K egy n-edfokú algebrai számtest. Ekkor a K-beli $\mathbb{Z}_K$ algebrai egészek gyűrűjét *monogénnek* nevezzük, ha létezik olyan $\alpha \in K$, hogy $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, a $\mathbb{Z}$ egy egyszerű gyűrűbővítése. Ekkor $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ egész bázisa K-nak, amit *hatvány egész bázisnak* nevezünk. Világos, hogy ekkor $I(\alpha) = 1$, és az α diszkriminánsa megegyezik a test diszkriminánsával,

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

Legyen $(\omega_1 = 1, \omega_2, \ldots, \omega_n)$ egész bázis K-ban. Ekkor az

$$L(\underline{X}) = X_1 + \omega_2 X_2 + \ldots + \omega_n X_n$$

kifejezést az $(1, \omega_2, \ldots, \omega_n)$ *egész bázishoz tartozó lineáris formának* nevezzük. Legyenek

$$L^{(i)}(\underline{X}) = X_1 + \omega_2^{(i)} X_2 + \ldots + \omega_n^{(i)} X_n, \qquad (i = 1, \ldots, n)$$

az $L(\underline{X})$ relatív konjugáltjai, és

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

az $L(\underline{X})$ lineáris forma diszkriminánsa.

2.5. Lemma. *A fenti jelölések mellett,*

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

ahol D_K a K test diszkriminánsa, $I(X_2, \ldots, X_n)$ pedig egy $(n-1)$ változós egész együtthatós $\frac{n(n-1)}{2}$-fokú homogén forma.

Ezt az $I(X_2, \ldots, X_n)$ formát nevezzük az $(1, \omega_2, \ldots, \omega_n)$ egész bázishoz tartozó *indexformának*. Az indexforma legfontosabb tulajdonsága, hogy tetszőleges

$$(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$$

szám n-es esetén, amelyre az $\alpha = x_1 + x_2\omega_2 + \ldots + x_n\omega_n \in \mathbb{Z}_K$ elem primitív, teljesül, hogy

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

Ez azt is jelenti, hogy $\alpha = x_1 + x_2\omega_2 + \ldots + x_n\omega_n \in \mathbb{Z}_K$ pontosan akkor generál hatvány egész bázist K-ban, ha $(x_2, \ldots, x_n) \in \mathbb{Z}^{n-1}$ megoldása az

$$I(X_2, \ldots, X_n) = \pm 1$$

ún. *indexforma egyenletnek*. Világos, hogy ha $\beta = a \pm \alpha$ valamilyen $a \in \mathbb{Z}$ esetén, akkor $I(\alpha) = I(\beta)$, így érthető, hogy az indexforma független az X_1 változótól. Ilyenkor azt mondjuk, hogy α és β *ekvivalens* algebrai egészek. Ez alapján ekvivalencia erejéig az összes hatvány egész bázist generáló elem meghatározása ekvivalens a fenti indexforma egyenlet megoldásával.

A bevezetőben említettek szerint, adott fokszámú és adott diszkriminánsú binér formákról Birch és Merriman [5] fogalmazott meg ineffektív végességi tételeket, melyekből következik az indexforma egyenletek megoldásszámának végessége. Tőlük függetlenül Győry Kálmán [36] bizonyította a végességet effektív formában, majd a módszert finomítva [37]-ben effektív felső korlátokat adott az indexforma egyenlet megoldásaira. A Baker-módszer [2] felhasználásával nyert effektív korlátoknak számos élesítése és általánosítása született, ld Evertse, Győry Kálmán [17]. Ezek a korlátok azonban még a legegyszerűbb esetekben is a paraméterek duplán exponenciális függvényei, így gyakorlatban nem teszik lehetővé az egyenletek megoldásainak megkeresését. Az indexforma egyenletek megoldásaira vonatkozó konstruktív, algoritmikus eredményekre vonatkozóan ld. Gaál István [22] könyvét.

2.2.1. Az indexforma faktorai

Ahogy azt az előző részben láthattuk, egy n-edfokú számtestben egy egész bázishoz tartozó indexforma $(n-1)$ változós $\frac{n(n-1)}{2}$-fokú homogén forma. Ez már kis fokszámú számtestek esetén is kifejezettek sok tagból állhat, és nehezen kezelhetővé válik. Harmadfokú esetben az indexforma egyenlet egy harmadfokú Thue egyenlet, negyed-, ötöd-, és hatodfokú esetben pedig a megoldásuk visszavezethető alacsonyabb fokú egyenletek, illetve egységegyenletek megoldására (ld. [24],[23],[4]). Magasabb fokszámok esetén azonban nincs olyan hatékony számítógép, amely képes lenne elfogadható időn belül kiszámítani egy általános index forma egyenlet megoldásait. Csupán speciális esetekben vannak eredmények, melyek közül a legtöbb az index forma faktorizációjára, vagy relatív indexforma egyenletek megoldására épül.

Legyen α egy n-edfokú algebrai egész, $f(X) \in \mathbb{Z}[X]$ az α definiáló polinomja, $K = \mathbb{Q}(\alpha)$, és a szokásos módon jelölje $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ az α konjugáltjait. Legyen $(1, \omega_2, \ldots, \omega_n)$ egy egész bázis K-ban, és jelöljük az $(1, \alpha, \ldots, \alpha^{n-1}) \mapsto (1, \omega_2, \ldots, \omega_n)$ bázistranszformáció mátrixát M-el. Ekkor

$$X_1 + X_2\omega_2 + \ldots + X_n\omega_n = Y_1 + Y_2\alpha + \ldots + Y_n\alpha^{n-1},$$

ahol

$$\begin{pmatrix} X_1 & X_2 & \ldots & X_n \end{pmatrix} \cdot M = \begin{pmatrix} Y_1 & Y_2 & \ldots & Y_n \end{pmatrix}$$

Ezek alapján $1 \leq i \neq j \leq n$ esetén

$$\begin{aligned} L^{(i)}(\underline{X}) - L^{(j)}(\underline{X}) &= (X_1 + X_2\omega_2^{(i)} + \ldots + X_n\omega_n^{(i)}) - (X_1 + X_2\omega_2^{(j)} + \ldots + X_n\omega_n^{(j)}) = \\ &= (Y_2\alpha^{(i)} + \ldots + Y_n(\alpha^{(i)})^{n-1}) - (Y_2\alpha^{(j)} + \ldots + Y_n(\alpha^{(j)})^{n-1}) = \\ &= (\alpha^{(i)} - \alpha^{(j)}) \cdot \left(Y_2 + Y_3\beta_2^{(i,j)} + \ldots + Y_n\beta_{n-1}^{(i,j)}\right), \end{aligned}$$

ahol

$$\beta_k^{(i,j)} = \frac{(\alpha^{(i)})^k - (\alpha^{(j)})^k}{\alpha^{(i)} - \alpha^{(j)}} = (\alpha^{(i)})^{k-1} + (\alpha^{(i)})^{k-2}\alpha^{(j)} + \ldots + \alpha^{(i)}(\alpha^{(j)})^{k-2} + (\alpha^{(j)})^{k-1}.$$

Így az $(1, \omega_2, \ldots, \omega_n)$ bázishoz tartozó lineáris forma diszkriminánsa

$$\begin{aligned} D_{K/\mathbb{Q}}(L(\underline{X})) &= \prod_{1\le i<j\le n} (\alpha^{(i)} - \alpha^{(j)})^2 \cdot \left(Y_2 + Y_3\beta_2^{(i,j)} + \ldots + Y_n\beta_{n-1}^{(i,j)}\right)^2 = \\ &= D_{K/\mathbb{Q}}(\alpha) \cdot \prod_{1\le i<j\le n} \left(Y_2 + Y_3\beta_2^{(i,j)} + \ldots + Y_n\beta_{n-1}^{(i,j)}\right)^2, \end{aligned}$$

ahonnan $D_K = D_{K/\mathbb{Q}}(\alpha) \cdot \det(M)^2$ miatt az $(1, \omega_2, \ldots, \omega_n)$ bázishoz tartozó indexforma

$$I(X_2, \ldots, X_n) = \frac{1}{\det(M)} \prod_{1\le i<j\le n} \left(Y_2 + Y_3\beta_2^{(i,j)} + \ldots + Y_n\beta_{n-1}^{(i,j)}\right).$$

Ez a felírás több szempontból is hasznos. Egyrészt az esetek döntő többségében az így kifejezett indexformában jóval kevesebb tag van, mintha az eredeti változókat használnánk, és tapasztalataink szerint a számítógép sokkal gyorsabban is képes ezt meghatározni, majd elvégezni a változó helyettesítéseket, mint kiszámolni a megfelelő egész bázishoz tartozó lineáris forma diszkriminánsát. Másrészt pedig kézenfekvővé válik a kapcsolat az indexforma faktorai és az α definiáló polinomjának Galois csoportja között.

Legyen G az $f(X)$ Galois-csoportja, és tekintsük G hatását az

$$\{(\alpha^{(i)}, \alpha^{(j)}), 1 \le i \ne j \le n\}$$

halmazon. Ennek a hatásnak legyen egy orbitja S és tekintsük a

$$J_S = \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S} \left(Y_2 + Y_3\beta_2^{(i,j)} + \ldots + Y_n\beta_{n-1}^{(i,j)}\right)$$

szorzatot. Ez invariáns a Galois csoport összes elemével szemben, így racionális együtthatós. Tehát ha $S_1, S_2, \ldots, S_k$ a fenti hatás összes különböző orbitja, akkor

$$I(X_2, \ldots, X_n)^2 = \frac{1}{\det(M)^2} \cdot J_{S_1} \cdot J_{S_2} \cdot \ldots \cdot J_{S_k}$$

Mivel $\det(M^{-1}) = (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+)$, és $I(X_2, \ldots, X_n)$ egész együtthatós, ezért alkalmas $d_1, d_2 \ldots, d_k \in \mathbb{Q}$ számokkal, amelyekre

$$d_1 \cdot d_2 \cdot \ldots \cdot d_k = (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+)^2$$

teljesül, adódik az indexforma négyzetének

$$I(X_2, \ldots, X_n)^2 = I_{S_1} \cdot I_{S_2} \cdot \ldots \cdot I_{S_k}$$

egész együtthatós faktorizációja, ahol I_{S_i}-t a $d_i \cdot J_{S_i}$-ből kapjuk

$$\begin{pmatrix} Y_1 & Y_2 & \dots & Y_n \end{pmatrix} = \begin{pmatrix} X_1 & X_2 & \dots & X_n \end{pmatrix} \cdot M$$

helyettesítéssel. Ebből pedig már könnyű meghatározni az indexforma

$$I(X_2, \dots, X_n) = f_1(X_2, \dots, X_n) \cdot \dots \cdot f_m(X_2, \dots, X_n)$$

egész együtthatós faktorizációját.

A konkrét példáinkban ezen faktorok közötti összefüggéseket fogjuk felhasználni a monogenitás vizsgálatakor. Ha a $K = \mathbb{Q}(\alpha)$ testnek van valódi részteste, akkor a Galois csoport nem lehet 2-tranzitív, így az indexforma biztosan faktorizálódik. Ez az észrevétel motiválja a valódi résztesttel rendelkező, és a kompozit testek monogenitásának vizsgálatát. Ezekben az esetekben az index (és analóg módon az indexforma) faktorizációjának részletes leírását ld. Gaál István [22], 1.3 és 1.4 fejezet.

A következő fejezetekben speciális parametrikus számtestcsaládok egész bázisai és monogenitása kapcsán elért eredményeinket veszem sorba a [26], [58], [28], [59], [29], [27] cikkek alapján. A 3 fejezetben az egész bázis és annak periodikus tulajdonságával kapcsolatos eredmények, a 4. fejezetben pedig ezek felhasználásával a monogenitási vizsgálatok szerepelnek. Mivel ez utóbbi számításokhoz eleve szükség van a test egy egész bázisára, valamint magasabb fokszámok esetén számítástechnikai korlátok miatt már szinte reménytelenné válik az indexforma kiszámítása (az indexforma egyenlet megoldásáról már nem is beszélve), ezért a monogenitást csupán néhány alacsonyabb fokú esetben vizsgájuk részletesen.

3. fejezet

Végtelen parametrikus számtestek egész bázisai

A fejezetben három számtestcsaládot vizsgálunk, a gyökbővítéseket (3.1 fejezet) és az úgynevezett legegyszerűbb számtestek kétféle általánosításaként kapott számtesteket (3.2 fejezet). Mindkét esetben sikerült a fokszámtól függő olyan n_0 konstanst találnunk, hogy a végtelen parametrikus számtest egész bázisa periodikusan ismétlődik modulo n_0. A periodikussághoz szükséges feltételeink a paraméter első vagy másodfokú polinomjának négyzetmentességével függnek össze, így a tételeink minden esetben végtelen sok megfelelő számtestet fednek le. A három számtestcsaládban nyert eredmények összefűzésével, ezen számtestek kompozítumaiban is lehetőség nyílt az egész bázis periodikus tulajdonságának igazolására (3.3 fejezet).

3.1. Gyökbővítések egész bázisai

A fejezet eredményei a [26] és [58] cikkekben jelentek meg. Legyen $n \geq 2$ és $m \neq 0, \pm 1$ egészek. Ekkor a $K = \mathbb{Q}(\sqrt[n]{m})$ számtesteket *gyökbővítéseknek* nevezzük. Jól ismert tétel, hogy négyzetmentes m paraméter, és $n = 2$ esetén a $K = \mathbb{Q}(\sqrt{m})$ testben $(1, \omega)$ egész bázist alkot, ahol

$$\omega = \begin{cases} \sqrt{m}, & \text{ha } m \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{m}}{2}, & \text{ha } m \equiv 1 \pmod 4. \end{cases}$$

Harmadfokú esetben R. Dedekind [12] nyert hasonló eredményt. Legyen $m = ab^2$, ahol a és b négyzetmentes egészek. Ekkor a $K = \mathbb{Q}(\sqrt[3]{m})$ testben $(1, \omega_2, \omega_3)$ egész

bázist alkot, ahol $\omega_2 = \sqrt[3]{m}$ és

$$\omega_3 = \begin{cases} \frac{\sqrt[3]{m}^2}{b}, & \text{ha } m \equiv 0,2,3,4,5,6,7 \pmod 9, \\ \frac{b^2+b^2\sqrt[3]{m}+\sqrt[3]{m}^2}{3b}, & \text{ha } m \equiv 1 \pmod 9, \\ \frac{b^2-b^2\sqrt[3]{m}+\sqrt[3]{m}^2}{3b}, & \text{ha } m \equiv 8 \pmod 9. \end{cases}$$

A negyedfokú gyökbővítéseket T. Funakura [19] írta le analóg módon. Ezen kis fokszámú példákból jól látszik, hogy ha m négyzetmentes, akkor a $n = 2,3,4$ esetén a $K = \mathbb{Q}(\sqrt[n]{m})$ gyökbővítések egész bázisa periodikusan ismétlődik modulo $n_0 = 4, 9$ illetve 8.

Ebben a fejezetben belátjuk, hogy ez a periodikus tulajdonság tetszőleges fokszám esetén is igaz. Fontos megemlíteni, hogy négyzetmentes m paraméterek esetén az $X^n - m$ polinom m minden prímosztójára nézve Eisenstein, és így irreducibilis, tehát ezt a feltételt külön már nem kell vizsgálni.

3.1. Tétel. *Legyen $m \neq 0, \pm 1$ négyzetmentes egész, $n \geq 2$ egész, melynek prímtényezős felbontása*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_j^{k_j},$$

és legyen

$$n_0 = p_1^{k_1+1} \cdot p_2^{k_2+1} \cdot \ldots \cdot p_j^{k_j+1}.$$

Ekkor a $K = \mathbb{Q}(\sqrt[n]{m})$ gyökbővítések egész bázisa periodikusan ismétlődik modulo n_0.

A bizonyítás több lépésben történik. Először $n = p^k$ prímhatvány kitevőkre látjuk be az állítást. Megadunk n darab lineárisan független algebrai egész számot, úgy, hogy az általuk generált bázis diszkriminánsa megegyezzen a test diszkriminánsával. Ezek után megmutatjuk, hogy hogyan lehet összefűzni egy n_1 és egy n_2 fokú gyökbővítés egész bázisát, ahol n_1 és n_2 relatív prímek. Végül belátjuk, hogy a fenti n_0 periódushossz a legkisebb, ami szerint periodikusan ismétlődnek az egész bázisok.

Egy általános megállapítással kezdünk, amely korlátod ad egy algebrai egész együtthatóinak nevezőire a triviális bázisra vonatkozóan.

3.2. Állítás. *Legyen $n \geq 2$ egész, $m \neq 0, \pm 1$ négyzetmentes egész, és $K = \mathbb{Q}(\sqrt[n]{m})$. Jelölje $\mathbb{Z}_K$ a K test algebrai egészeinek a gyűrűjét, ekkor*

$$\frac{n}{\text{lnko}(n,m)} \cdot \mathbb{Z}_K \subset \mathbb{Z}[\sqrt[n]{m}].$$

Bizonyítás. Egyszerű számítással igazolható, hogy az $(1, \sqrt[n]{m}, \ldots, \sqrt[n]{m^{n-1}})$ algebrai egészekből álló bázis duális bázisa

$$\left(\frac{1}{n}, \frac{\sqrt[n]{m^{n-1}}}{n \cdot m}, \frac{\sqrt[n]{m^{n-2}}}{n \cdot m}, \ldots, \frac{\sqrt[n]{m}}{n \cdot m}\right).$$

A 2.1.3 fejezet alapján ez azt jelenti, hogy az $(1, \sqrt[n]{m}, \dots, \sqrt[n]{m^{n-1}})$ bázisban tetszőleges α algebrai egész felírható olyan racionális együtthatókkal, melyeknek a nevezője $n \cdot m$. Azonban m négyzetmentessége miatt, tetszőleges $p \mid m$ prím esetén az $X^n - m$ polinom p-Eisenstein, vagyis a 2.2 Állítás szerint $p \nmid I(\alpha)$, és így $\mathrm{lnko}(m, I(\alpha)) = 1$. Az előző megállapítással együtt ez azt jelenti, hogy az $(1, \sqrt[n]{m}, \dots, \sqrt[n]{m^{n-1}})$ bázisban tetszőleges algebrai egész felírható olyan racionális együtthatókkal, melyek nevezője

$$\frac{n}{\mathrm{lnko}(m,n)}.$$

Ebből következően tetszőleges $\alpha \in \mathbb{Z}_K$ esetén

$$\frac{n}{\mathrm{lnko}(m,n)} \cdot \alpha \in \mathbb{Z}[\sqrt[n]{m}],$$

amiből adódik az állítás. □

A 2.4 Állítás alapján ebből következik, hogy adott $n \geq 2$ esetén a $\mathbb{Q}(\sqrt[n]{m})$ testek egész bázisa periodikusan ismétlődik modulo

$$\left(\frac{n}{\mathrm{lnko}(m,n)}\right)^n.$$

Ez a periódushossz lényegesen rosszabb, mint a tételben szereplő n_0, így a továbbiakban arra törekszünk, hogy a periodikusságot az előírt n_0-al igazoljuk.

Megjegyezzük, hogy a könnyen meghatározható duális bázis egyik további haszna, hogy az

$$\left(1, \sqrt[n]{m}, \dots, \sqrt[n]{m^{n-1}}\right) \mapsto \left(\frac{1}{n}, \frac{\sqrt[n]{m^{n-1}}}{n \cdot m}, \frac{\sqrt[n]{m^{n-2}}}{n \cdot m}, \dots, \frac{\sqrt[n]{m}}{n \cdot m}\right)$$

bázistranszformáció M mátrixa is egyszerűen felírható:

$$M = \begin{pmatrix} \frac{1}{n} & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & \frac{1}{n \cdot m} \\ 0 & 0 & 0 & \dots & \frac{1}{n \cdot m} & 0 \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & 0 & \frac{1}{n \cdot m} & \dots & 0 & 0 \\ 0 & \frac{1}{n \cdot m} & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Ennek a determinánsa $\left(n^n \cdot m^{n-1}\right)^{-1}$, amiből pedig adódik, hogy

$$|D_{K/\mathbb{Q}}(\sqrt[n]{m})| = n^n \cdot m^{n-1}.$$

Ez természetesen pontosan is meghatározható a diszkrimináns eredeti definícióját használva,

$$D_{K/\mathbb{Q}}(\sqrt[n]{m}) = (-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot m^{n-1}.$$

Most térjünk rá a prímhatvány fokú esetre, és a megfelelő algebrai egészek meghatározására. Legyen $m \neq 0, \pm 1$ négyzetmentes egész, és $n = p^k$, ahol p prím. Az előző állítás szerint az

$$(1, \sqrt[n]{m}, \ldots, \sqrt[n]{m^{n-1}})$$

bázisban minden algebrai egész felírható olyan racionális együtthatókkal, melyeknek a nevezője osztja $\frac{n}{\text{lnko}(m,n)}$-t, azaz jelen esetben valamilyen p-hatvány. Továbbá, ha $p \mid m$, akkor az $X^n - m$ polinom p-Eisenstein, így a 2.2 Állítás alapján $v_p(I(\sqrt[n]{m})) = 0$, amiből pedig $\mathbb{Z}_K = \mathbb{Z}[\sqrt[n]{m}]$ következik.

3.3. Lemma. *A korábbi jelölések mellett, legyen r az m osztási maradéka p^{k+1}-el osztva, és legyen $s := v_p(m^p - m) - 1$. Legyen továbbá $t \in \mathbb{N}$ esetén a $h_t^{(r)}(X) \in \mathbb{Z}[X]$ polinom az alábbi módon adott,*

$$h_t^{(r)}(X) := \frac{X^{p^k} - r^{p^t}}{X^{p^{k-t}} - r} \in \mathbb{Z}[X].$$

Ekkor minden $0 \leq t \leq \min\{s, k\}$ esetén

$$\frac{h_t^{(r)}(\sqrt[n]{m})}{p^t} \in \mathbb{Q}(\sqrt[n]{m})$$

algebrai egész.

Bizonyítás. A bizonyítást $h_t^{(r)}(X)$ polinomok helyett a

$$H_t(X) := \frac{X^{p^k} - m^{p^t}}{X^{p^{k-t}} - m} \in \mathbb{Z}[X]$$

polinomokra fogjuk elvégezni. Mivel $H_t(X)$ és $h_t(X)$ egész együtthatós polinomok, ezért $p^{k+1} \mid m - r$ miatt $H_t(X) - h_t^{(r)}(X) \in p^{k+1} \cdot \mathbb{Z}[X]$, azaz

$$\frac{H_t(\sqrt[n]{m})}{p^t} - \frac{h_t^{(r)}(\sqrt[n]{m})}{p^t} \in p^{k+1-t} \cdot \mathbb{Z}[\sqrt[n]{m}].$$

Ez $t \leq k$ miatt azt jelenti, hogy a két szám eltérése algebrai egész, és így

$$\frac{H_t(\sqrt[n]{m})}{p^t} \in \mathbb{Z}_K$$

pontosan akkor teljesül, ha

$$\frac{h_t^{(r)}(\sqrt[n]{m})}{p^t} \in \mathbb{Z}_K.$$

Most belátjuk, hogy az

$$\frac{H_t(\sqrt[n]{m})}{p^t}$$

számok algebrai egész. A jelölések egyszerűsítése végett legyen $\ell = p^t$ és $\beta = H_t(\sqrt[n]{m})$. Behelyettesítéssel könnyű ellenőrizni, hogy β gyöke a

$$g(X) = \frac{mX^\ell - (m - m^\ell + mX)^\ell}{m - m^\ell}$$

polinomnak. Legyen a_i az X^i együtthatója a $g(X)$-ben. Ekkor a főegyüttható $a_\ell = 1$, a konstans tag

$$a_0 = -(m - m^\ell)^{(\ell-1)},$$

és $i = 1, \ldots, \ell - 1$ esetén

$$a_i = -\binom{\ell}{i} m^i (m - m^\ell)^{\ell-i-1}.$$

Szem előtt tartva, hogy $\ell = p^t$,

$$v_p\left(\binom{\ell}{i}\right) = v_p(\ell) - v_p(i) = t - v_p(i).$$

Továbbá, mivel

$$v_p(m - m^\ell) \geq v_p(m - m^p)$$

és

$$v_p(m - m^p) = s + 1 \geq t + 1,$$

ezért $i = 1, \ldots, \ell - 1$ esetén

$$\begin{aligned} v_p(a_i) &\geq v_p\left(\binom{\ell}{i}\right) + (\ell - i - 1) \cdot v_p(m - m^\ell) \geq \\ &\geq t - v_p(i) + (\ell - i - 1) \cdot (t + 1) = \\ &= t \cdot (\ell - i) + \ell - i - v_p(i) - 1 \geq \\ &\geq t \cdot (\ell - i). \end{aligned}$$

Emellett

$$v_p(a_0) \geq (\ell - 1)(t + 1) \geq \ell \cdot t,$$

így minden $i = 0, \ldots, \ell$ esetén teljesül, hogy $\ell^{(\ell-i)} \mid a_i$. Ebből következően az

$$\frac{1}{\ell^\ell} \cdot g(X \cdot \ell)$$

polinom egész együtthatós főpolinom, aminek $\frac{\beta}{\ell}$ gyöke, így $\frac{h_t(\sqrt[n]{m})}{p^t}$ valóban algebrai egész. □

A $\mathbb{Q}(\sqrt[n]{m})$ egész bázisát ezeknek a

$$\frac{h_t^{(r)}(\sqrt[n]{m})}{p^t}$$

algebrai egészeknek segítségével fogjuk megkonstruálni.

3.4. Lemma. *A korábbi jelölések mellett legyen még $\alpha = \sqrt[n]{m}$. Ekkor ha $s < k$, akkor*

$$\left(\begin{array}{llll} \frac{h_0^{(r)}(\alpha)}{p^0}, & \alpha\cdot\frac{h_0^{(r)}(\alpha)}{p^0}, & \alpha^2\cdot\frac{h_0^{(r)}(\alpha)}{p^0}, & \dots \quad , \alpha^{p^k-p^{k-1}-1}\cdot\frac{h_0^{(r)}(\alpha)}{p^0}, \\ \frac{h_1^{(r)}(\alpha)}{p^1}, & \alpha\cdot\frac{h_1^{(r)}(\alpha)}{p^1}, & \alpha^2\cdot\frac{h_1^{(r)}(\alpha)}{p^1}, & \dots \quad , \alpha^{p^{k-1}-p^{k-2}-1}\cdot\frac{h_1^{(r)}(\alpha)}{p^1}, \\ \frac{h_2^{(r)}(\alpha)}{p^2}, & \alpha\cdot\frac{h_2^{(r)}(\alpha)}{p^2}, & \alpha^2\cdot\frac{h_2^{(r)}(\alpha)}{p^2}, & \dots \quad , \alpha^{p^{k-2}-p^{k-3}-1}\cdot\frac{h_2^{(r)}(\alpha)}{p^2}, \\ & & \vdots & \\ \frac{h_{s-1}^{(r)}(\alpha)}{p^{s-1}}, & \alpha\cdot\frac{h_{s-1}^{(r)}(\alpha)}{p^{s-1}}, & \alpha^2\cdot\frac{h_{s-1}^{(r)}(\alpha)}{p^{s-1}}, & \dots \quad , \alpha^{p^{k-s+1}-p^{k-s}-1}\cdot\frac{h_{s-1}^{(r)}(\alpha)}{p^{s-1}}, \\ \frac{h_s^{(r)}(\alpha)}{p^s}, & \alpha\cdot\frac{h_s^{(r)}(\alpha)}{p^s}, & \alpha^2\cdot\frac{h_s^{(r)}(\alpha)}{p^s}, & \dots \quad , \alpha^{p^{k-s}-1}\cdot\frac{h_s^{(r)}(\alpha)}{p^s} \end{array} \right),$$

ha pedig $k \le s$, akkor

$$\left(\begin{array}{llll} \frac{h_0^{(r)}(\alpha)}{p^0}, & \alpha\cdot\frac{h_0^{(r)}(\alpha)}{p^0}, & \alpha^2\cdot\frac{h_0^{(r)}(\alpha)}{p^0}, & \dots \quad , \alpha^{p^k-p^{k-1}-1}\cdot\frac{h_0^{(r)}(\alpha)}{p^0}, \\ \frac{h_1^{(r)}(\alpha)}{p^1}, & \alpha\cdot\frac{h_1^{(r)}(\alpha)}{p^1}, & \alpha^2\cdot\frac{h_1^{(r)}(\alpha)}{p^1}, & \dots \quad , \alpha^{p^{k-1}-p^{k-2}-1}\cdot\frac{h_1^{(r)}(\alpha)}{p^1}, \\ \frac{h_2^{(r)}(\alpha)}{p^2}, & \alpha\cdot\frac{h_2^{(r)}(\alpha)}{p^2}, & \alpha^2\cdot\frac{h_2^{(r)}(\alpha)}{p^2}, & \dots \quad , \alpha^{p^{k-2}-p^{k-3}-1}\cdot\frac{h_2^{(r)}(\alpha)}{p^2}, \\ & & \vdots & \\ \frac{h_{k-1}^{(r)}(\alpha)}{p^{k-1}}, & \alpha\cdot\frac{h_{k-1}^{(r)}(\alpha)}{p^{k-1}}, & \alpha^2\cdot\frac{h_{k-1}^{(r)}(\alpha)}{p^{k-1}}, & \dots \quad , \alpha^{p^1-p^0-1}\cdot\frac{h_{k-1}^{(r)}(\alpha)}{p^{k-1}}, \\ & & \frac{h_k^{(r)}(\alpha)}{p^k} & \end{array} \right)$$

egész bázis $\mathbb{Q}(\sqrt[n]{m})$-ben.

Bizonyítás. Az, hogy a felírt elemek lineárisan függetlenek $\mathbb{Q}$-felett azonnal adódik abból az észrevételből, hogy a fokszámuk α-ban egyesével nő 0-tól $n-1$-ig. Az előző lemma miatt ezek valóban algebrai egészek is, így már csak azt kell megmutatnunk, hogy a belőlük képzett bázis diszkriminánsa megegyezik a test diszkriminánsával. Először kiszámítjuk a keletkezett bázisok diszkriminánsát. Mivel az elemek fokszáma α-ban egyesével nő, ezért az $(1, \alpha, \ldots, \alpha^{n-1})$ bázist ezekbe az új bázisokba transzformáló mátrixok alsó háromszög alakúak, melynek a főátlójában $\frac{1}{p^t}$ alakú számok szerepelnek. A mátrixok determinánsa így könnyen meghatározható.

Ha $s < k$, akkor

$$\det(M) = \left(\prod_{t=0}^{s-1} \left(\frac{1}{p^t}\right)^{p^{k-t}-p^{k-t-1}}\right) \cdot \left(\frac{1}{p^s}\right)^{p^{k-s}} = \left(\frac{1}{p}\right)^{\left(\frac{p^k-p^{k-s}}{p-1}\right)},$$

ha pedig $k \leq s$, akkor

$$\det(M) = \left(\prod_{t=0}^{k-1} \left(\frac{1}{p^t}\right)^{p^{k-t}-p^{k-t-1}}\right) \cdot \left(\frac{1}{p^k}\right) = \left(\frac{1}{p}\right)^{\left(\frac{p^k-1}{p-1}\right)}.$$

Az $(1, \alpha, \ldots, \alpha^{n-1})$ diszkriminánsának ismeretében így kiszámíthatjuk az új bázis diszkriminánsát is, amit most az egyszerűség kedvéért D_h-val jelölünk.

Ha $s < k$, akkor

$$D_h = \frac{D(\alpha)}{\left(p^{\left(\frac{p^k-p^{k-s}}{p-1}\right)}\right)^2},$$

ha pedig $k \leq s$, akkor

$$D_h = \frac{D(\alpha)}{\left(p^{\left(\frac{p^k-1}{p-1}\right)}\right)^2}.$$

Ahhoz, hogy belássuk, hogy ez éppen a test diszkriminánsa, meg kell mutatnunk, hogy az α indexe pontosan a nevezőben szereplő kifejezéssel egyezik meg. Mivel az α indexe p^k osztója, ezért szükségszerűen $I(\alpha) = p^{v_p(I(\alpha))}$. Tehát lényegében azt kell még igazolni, hogy ha $s < k$, akkor

$$v_p(I(\alpha)) = \frac{p^k - p^{k-s}}{p-1},$$

ha pedig $k \leq s$, akkor

$$v_p(I(\alpha)) = \frac{p^k - 1}{p-1}.$$

Ehhez a Newton poligonokat és az 2.1 Tételt fogjuk használni. Vegyük észre, hogy

$$\overline{X^{p^k} - m} \equiv \overline{(X-m)^{p^k}} \pmod{p}.$$

így $\phi(X) = X - m$ választással az $f(X) = X^{p^k} - m$ polinom ϕ-adikus kifejtése éppen az $f(X)$ Taylor sorba fejtése az m pont körül, azaz

$$f(X) = \sum_{i=0}^{p^k} \frac{f^{(i)}(m)}{i!} \cdot \phi(x)^i.$$

Így ha a_i jelöli az $f(X)$-nek a ϕ-adikus kifejtésben a $\phi(X)^i$ együtthatóját, akkor $a_0 = m^{p^k} - m$, és $i = 1, \ldots, p^k$ esetén

$$a_i = \frac{f^{(i)}(m)}{i!} = \binom{p^k}{i} m^{p^k - i}.$$

Mivel $p \mid m$ esetén $I(\alpha) = 1$, ezért feltehetjük, hogy $p \nmid m$. Ekkor

$$v_p(a_0) = v_p(m^{p^k} - m) = v_p(m^p - m) = s + 1,$$

és $i = 1, \ldots, p^k$ esetén

$$v_p(a_i) = v_p\left(\binom{p^k}{i}\right) = k - v_p(i).$$

Így tehát az $N_\phi(f)$ Newton poligon a

$$\{(0, s+1)\} \cup \left\{(i, k - v_p(i)) : i \in \{1, \ldots, p^k\}\right\}$$

pontok alsó konvex burka. Könnyű megmutatni, hogy ennek a csúcsai $s < k$ esetén

$$\{P_N, P_{k-s}, P_{k-s+1}, \ldots, P_k\}$$

és $k \leq s$ esetén

$$\{P_N, P_0, P_1, \ldots, P_k\},$$

ahol $P_N = (0, s+1)$, és $P_j = (p^j, k - j)$, $(j = 0, \ldots, k)$. Valójában, ha $p = 2$, $k \geq s$, akkor a fenti halmazok első 3 pontja egy egyenesre esik, így a középső nem valódi csúcsa a poligonnak de ez nem befolyásolja az eredményt. Látható az is, hogy minden oldal elsőfokú (illetve $p = 2$ és $k \geq s$ esetén az első oldal másodfokú, a hozzá tartozó maradék polinom pedig $Y^2 + Y + 1 \in \mathbb{Z}[X]/(p, \phi(X))))$, ezért az összes oldalhoz tartozó maradék polinom szeparábilis, vagyis az $f(X)$ polinom ϕ-reguláris, és így egyenlőséggel alkalmazható a 2.1 Tétel.

A megfelelő tartományba eső pozitív egész koordinátájú pontokat összeszámolva kapjuk, hogy ha $s < k$, akkor

$$v_p(I(\alpha)) = \mathrm{ind}_\phi(\alpha) = \sum_{j=1}^{s} p^{k-j} = \frac{p^k - p^{k-s}}{p-1},$$

ha pedig $k \leq s$, akkor

$$v_p(I(\alpha)) = \mathrm{ind}_\phi(\alpha) = \sum_{j=1}^{k} p^{k-j} = \frac{p^k - 1}{p-1}.$$

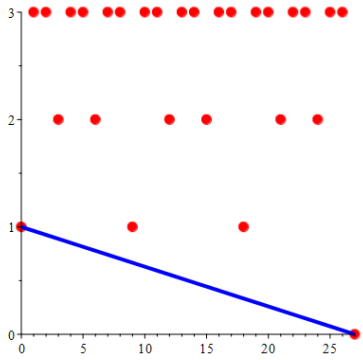
Ez pedig éppen azt jelenti, hogy a lemmában szereplő bázisok valóban egész bázist alkotnak $\mathbb{Q}(\sqrt[r]{m})$-ben. □

Ennek következményeként kapjuk a periodikus egész bázis tulajdonságot.

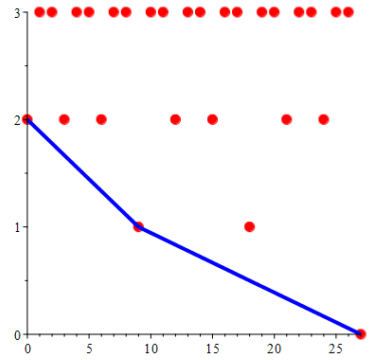
3.5. Következmény. *A korábbi jelölések mellett, a* $\mathbb{Q}(\sqrt[r]{m})$ *testek egész bázisa periodikusan ismétlődik modulo* p^{k+1}.

Bizonyítás. Mivel $p^{k+1} \mid m - r$, ezért $v_p(m^p - m) < k + 1$ esetén $v_p(m^p - m) = v_p(r^p - r)$, és $v_p(m^p - m) \geq k + 1$ esetén $v_p(r^p - r) \geq k + 1$. Ebből következik, hogy a 3.4 Lemmában szereplő egész bázisok alakja kizárólag r-től, azaz m-nek a p^{k+1}-el való osztási maradékától függ. Ez éppen azt jelenti, hogy a $\mathbb{Q}(\sqrt[r]{m})$ testek egész bázisa periodikusan ismétlődik modulo p^{k+1}. □

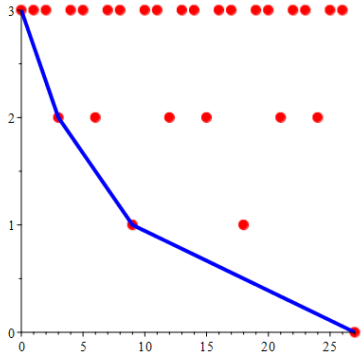
A következő ábrákon szemléltetésképp felvázoltuk az $X^{27} - m$ polinom ϕ-Newton poligonját $v_3(m^3 - m)$-től függően.



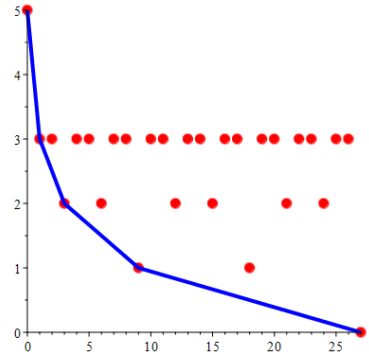
$v_3(m^3 - m) = 1$



$v_3(m^3 - m) = 2$



$v_3(m^3 - m) = 3$



$v_3(m^3 - m) > 3$

Minden oldal esetén vagy az x vagy az y koordináta mentén változik 1-et a kezdő és a végpont koordinátája, így egyértelmű, hogy nem tartalmazhatnak másik egész koordinátájú pontot, vagyis a fokuk minden esetben 1. A Newton poligonok alatt elhelyezkedő egész koordinátájú pontokat pedig az y-koordinátáik szerint csoportosítva könnyű összeszámolni.

A következő lépés két, egymáshoz relatív prím fokú gyökbővítés egész bázisának összefűzése. Ehhez először vizsgáljuk meg, hogyan viselkednek a megfelelő indexek a kompozit test képzésekor.

3.6. Lemma. *Legyen $m \neq 0, \pm 1$ négyzetmentes egész, $2 \leq n_1, n_2$ relatív prím egészek és $n = n_1 \cdot n_2$. Ekkor*

$$I(\sqrt[n]{m}) = I(\sqrt[n_1]{m})^{n_2} \cdot I(\sqrt[n_2]{m})^{n_1}.$$

Bizonyítás. Legyen

$$K = \mathbb{Q}(\sqrt[n]{m}), \qquad K_1 = \mathbb{Q}(\sqrt[n_1]{m}), \qquad K_2 = \mathbb{Q}(\sqrt[n_2]{m}),$$

és jelölje D_K, D_{K_1} és D_{K_2} a megfelelő testek diszkriminánsait. Az állítás igazolásához felhasználjuk a jól ismert összefüggést testbővítésláncok diszkriminánsára vonatkozóan (ld. [53] Chapter IV., Proposition 4.15). Tetszőleges $K/L/\mathbb{Q}$ testbővítéslánc esetén

$$D_K = N_{L/\mathbb{Q}}(D_{K/L}) \cdot D_L^{[K:L]},$$

ahol $D_{K/L}$ a K test relatív diszkriminánsa L fölött. Ebből a képletből számunkra az lesz a lényeges információ, hogy a K test diszkriminánsát osztja az L diszkriminánsának $[K:L]$-edik hatványa. Ezt fogjuk most alkalmazni a

$$K/K_1/\mathbb{Q} \qquad \text{és a} \qquad K/K_2/\mathbb{Q}$$

testbővítésláncokra. Az első esetben azt kapjuk, hogy $D_{K_1}^{n_2} \mid D_K$, a második esetben pedig $D_{K_2}^{n_1} \mid D_K$. Ezekből adódik, hogy

$$\operatorname{lkkt}\left((D_{K_1})^{n_2}, (D_{K_2})^{n_1}\right) \mid D_K. \tag{3.1}$$

Most használjuk a test diszkriminánsának kifejezését a generáló elem diszkriminánsának, és az indexének segítségével,

$$\begin{aligned}
D_K &= \frac{D(\sqrt[n]{m})}{I(\sqrt[n]{m})^2} = \frac{(-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot m^{n-1}}{I(\sqrt[n]{m})^2}, \\
D_{K_1} &= \frac{D(\sqrt[n_1]{m})}{I(\sqrt[n_1]{m})^2} = \frac{(-1)^{\frac{n_1(n_1-1)}{2}} \cdot n_1^{n_1} \cdot m^{n_1-1}}{I(\sqrt[n_1]{m})^2}, \\
D_{K_2} &= \frac{D(\sqrt[n_2]{m})}{I(\sqrt[n_2]{m})^2} = \frac{(-1)^{\frac{n_2(n_2-1)}{2}} \cdot n_2^{n_2} \cdot m^{n_2-1}}{I(\sqrt[n_2]{m})^2}.
\end{aligned}$$

A 3.2 Állítás alapján tudjuk, hogy ha $\text{lnko}(n_1, n_2) = 1$, akkor

$$\text{lnko}\left(I\left(\sqrt[n_1]{m}\right), I\left(\sqrt[n_2]{m}\right)\right) = 1,$$

valamint $I(\sqrt[n]{m})$, $I(\sqrt[n_1]{m})$ és $I(\sqrt[n_2]{m})$ mindegyike relatív prím m-hez. Mindezeket összevetve, (3.1)-ből kapjuk, hogy

$$\text{lkkt}\left(\left(\frac{n_1^{n_1}}{I\left(\sqrt[n_1]{m}\right)^2}\right)^{n_2}, \left(\frac{n_2^{n_2}}{I\left(\sqrt[n_2]{m}\right)^2}\right)^{n_1}\right) \;\Big|\; \frac{n^n}{I\left(\sqrt[n]{m}\right)^2},$$

amiből

$$\frac{n^n}{\left(I\left(\sqrt[n_1]{m}\right)^2\right)^{n_2} \cdot \left(I\left(\sqrt[n_2]{m}\right)^2\right)^{n_1}} \;\Big|\; \frac{n^n}{I\left(\sqrt[n]{m}\right)^2},$$

adódik, és így

$$I\left(\sqrt[n]{m}\right) \;\Big|\; I\left(\sqrt[n_1]{m}\right)^{n_2} \cdot I\left(\sqrt[n_2]{m}\right)^{n_1}. \tag{3.2}$$

A másik irányhoz elegendő megmutatni, hogy K-ban van olyan algebrai egész elemekből álló bázis, amelynek a diszkriminánsa osztja $D_{K_1}^{n_2} \cdot D_{K_2}^{n_1}$-et. Ehhez legyen $(\psi_1, \psi_2, \ldots, \psi_{n_1})$ a K_1 egy egész bázisa, $(\omega_1, \omega_2, \ldots, \omega_{n_2})$ a K_2 egy egész bázisa, és tekintsük az általuk generált

$$\begin{array}{cccc} (\psi_1\omega_1, & \psi_2\omega_1, & \ldots, & \psi_{n_1}\omega_1, \\ \psi_1\omega_2, & \psi_2\omega_2, & \ldots, & \psi_{n_1}\omega_2, \\ & & \vdots & \\ \psi_1\omega_{n_2}, & \psi_2\omega_{n_2}, & \ldots, & \psi_{n_1}\omega_{n_2}) \end{array}$$

kompozit bázist. Ez $\text{lnko}(n_1, n_2) = 1$ miatt valóban n darab lineárisan független elem $\mathbb{Q}$ fölött, így bázist alkotnak. Továbbá a bázis mindegyik eleme algebrai egész, és a diszkriminánsa pont $D_{K_1}^{n_2} \cdot D_{K_2}^{n_1}$. Ez azt jelenti, hogy

$$D_K \mid D_{K_1}^{n_2} \cdot D_{K_2}^{n_1},$$

így

$$\frac{n^n}{I\left(\sqrt[n]{m}\right)^2} \;\Big|\; \frac{n^n}{\left(I\left(\sqrt[n_1]{m}\right)^2\right)^{n_2} \cdot \left(I\left(\sqrt[n_2]{m}\right)^2\right)^{n_1}},$$

ahonnan pedig

$$I\left(\sqrt[n_1]{m}\right)^{n_2} \cdot I\left(\sqrt[n_2]{m}\right)^{n_1} \;\Big|\; I\left(\sqrt[n]{m}\right)$$

adódik. Ez (3.2)-vel együtt éppen a bizonyítandó állítást adja. □

Ezt a lemmát felhasználva most már össze tudjuk fűzni a két kisebb test egész bázisát a nagyobb test egy egész bázisává. Ha megvizsgáljuk az indexek közti összefüggést, akkor láthatjuk, hogy az előző bizonyításban szereplő bázis diszkriminánsa

csupán az m egy hatványával tér el a test diszkriminánsától. Egészen pontosan annak az $m^{(n_1-1)(n_2-1)}$-szerese, ezt szeretnénk most kijavítani. Az egyszerűsítés kedvéért a korábbiak mellé még bevezetjük az alábbi jelöléseket:

$$\alpha = \sqrt[n]{m}, \qquad \alpha_1 = \sqrt[n_1]{m}, \qquad \alpha_2 = \sqrt[n_2]{m}.$$

Legyen

$$(\psi_1, \psi_2, \ldots, \psi_{n_1})$$

a K_1 test,

$$(\omega_1, \omega_2, \ldots, \omega_{n_2})$$

pedig a K_2 test egy egész bázisa. Mivel $\text{lnko}(n_1, n_2) = 1$ miatt α foka K_1 fölött n_2, K_2 fölött pedig n_1, ezért $(1, \alpha, \ldots, \alpha^{n_2-1})$ bázisa K-nak K_1 fölött, és $(1, \alpha, \ldots, \alpha^{n_1-1})$ bázisa K-nak K_2 fölött. Most képezzük a K_1 egész bázisának és a K/K_1 relatív bázisának kompozícióját,

$$\begin{array}{cccc} (\psi_1, & \psi_1\alpha, & \ldots, & \psi_1\alpha^{n_2-1}, \\ \psi_2, & \psi_2\alpha, & \ldots, & \psi_2\alpha^{n_2-1}, \\ & & \vdots & \\ \psi_{n_1}, & \psi_{n_1}\alpha, & \ldots, & \psi_{n_1}\alpha^{n_2-1}). \end{array}$$

Ugyanígy, K_2-ből az alábbi bázist kapjuk,

$$\begin{array}{cccc} (\omega_1, & \omega_1\alpha, & \ldots, & \omega_1\alpha^{n_1-1}, \\ \omega_2, & \omega_2\alpha, & \ldots, & \omega_2\alpha^{n_1-1}, \\ & & \vdots & \\ \omega_{n_2}, & \omega_{n_2}\alpha, & \ldots, & \omega_{n_2}\alpha^{n_1-1}). \end{array}$$

Az egyszerűség kedvéért jelöljük az első bázis elemeit $(\Psi_1, \Psi_2, \ldots, \Psi_n)$-el, a második bázis elemeit pedig $(\Omega_1, \Omega_2, \ldots, \Omega_n)$-el. Mivel a $(\psi_1, \psi_2, \ldots, \psi_{n_1})$ bázis diszkriminánsa

$$\frac{D_{K_1/\mathbb{Q}}(\alpha_1)}{I(\alpha_1)^2},$$

az $(\omega_1, \omega_2, \ldots, \omega_{n_2})$ bázisé pedig

$$\frac{D_{K_2/\mathbb{Q}}(\alpha_2)}{I(\alpha_2)^2},$$

ezért a konstrukció alapján a $(\Psi_1, \Psi_2, \ldots, \Psi_n)$ bázis diszkriminánsa

$$\frac{D_{K/\mathbb{Q}}(\alpha)}{(I(\alpha_1)^2)^{n_2}},$$

az $(\Omega_1, \Omega_2, \ldots, \Omega_n)$ bázis diszkriminánsa pedig

$$\frac{D_{K/\mathbb{Q}}(\alpha)}{(I(\alpha_2)^2)^{n_1}}.$$

Látható, hogy ezekben az m kitevője pontosan annyi, amennyit szeretnénk, vagyis $n-1$. Érdemes tehát ezeket a bázisokat összeillesztenünk, úgy, hogy egy olyan bázist kapjunk, aminek a diszkriminánsa

$$\frac{D_{K/\mathbb{Q}}(\alpha)}{(I(\alpha_1)^2)^{n_2} \cdot (I(\alpha_2)^2)^{n_1}},$$

vagyis a 3.6 Lemma alapján éppen a K test diszkriminánsa.

Az összeillesztéshez legyen R_1 a $(\Psi_1, \Psi_2, \ldots, \Psi_n)$ által generált, R_2 pedig az $(\Omega_1, \Omega_2, \ldots, \Omega_n)$ által generált modulus K-ban, és legyen $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ az R_1+R_2 modulus egy bázisa. Erre a bázisra teljesül, hogy az általa generált modulus a legszűkebb, ami tartalmazza a $(\Psi_1, \Psi_2, \ldots, \Psi_n)$ és az $(\Omega_1, \Omega_2, \ldots, \Omega_n)$ által generált modulusokat, és így a diszkriminánsa osztja mindkét bázis diszkriminánsát. Továbbá, mivel algebrai egész elemekből álló modulusok összege szintén algebrai egészekből áll, ezért $\gamma_1, \gamma_2, \ldots, \gamma_n \in \mathbb{Z}_K$. Így tehát a $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ algebrai egész elemekből álló bázis D_γ diszkriminánsára teljesül, hogy

$$D_\gamma \;\Big|\; \operatorname{lnko}\left(\frac{D_{K/\mathbb{Q}}(\alpha)}{(I(\alpha_1)^2)^{n_2}}, \frac{D_{K/\mathbb{Q}}(\alpha)}{(I(\alpha_2)^2)^{n_1}}\right) = \frac{D_{K/\mathbb{Q}}(\alpha)}{(I(\alpha_1)^2)^{n_2} \cdot (I(\alpha_2)^2)^{n_1}} = D_K,$$

ennélfogva $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ egész bázist alkot K-ban.

Az $(\Psi_1, \Psi_2, \ldots, \Psi_n)$ és az $(\Omega_1, \Omega_2, \ldots, \Omega_n)$ bázisok ismeretében az $R_1 + R_2$ modulus α-hoz tartozó Hermite normál alakú bázisát könnyen meg tudjuk határozni.

Ezt most bemutatom egy egyszerű példán keresztül. Legyen $n_1 = 2$, $n_2 = 3$ valamint $m \neq 0, \pm 1$ olyan négyzetmentes egész, melyre $m \equiv 1 \pmod 4$ és $m \equiv 1 \pmod 9$ teljesül. Ekkor

$$\left(1, \frac{1+\alpha_1}{2}\right)$$

egész bázis K_1-ben, és

$$\left(1, \alpha_2, \frac{1+\alpha_2+\alpha_2^2}{3}\right)$$

egész bázis K_2-ben. Továbbá, a $(\Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5, \Psi_6)$ kompozit bázis

$$\left(1, \alpha, \alpha^2, \frac{1+\alpha_1}{2}, \frac{1+\alpha_1}{2} \cdot \alpha, \frac{1+\alpha_1}{2} \cdot \alpha^2\right),$$

az $(\Omega_1, \Omega_2, \Omega_3, \Omega_4, \Omega_5, \Omega_6)$ kompozit bázis pedig

$$\left(1, \alpha, \alpha_2, \alpha_2 \cdot \alpha, \frac{1+\alpha_2+\alpha_2^2}{3}, \frac{1+\alpha_2+\alpha_2^2}{3} \cdot \alpha\right).$$

Az R_1 modulus α-hoz tartozó Hermite normál alakja $(2, M_1)$, az R_2 modulus α-hoz tartozó Hermite normál alakja pedig $(3, M_2)$, ahol

$$M_1 = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A $(\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6)$ bázis meghatározásához ki kell számolni a $3M_1$ és a $2M_2$ mátrixok közös Hermite normál alakját:

$$\left(\begin{array}{cccccc} 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 & 0 \\ 0 & 3 & 0 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 & 0 & 3 \\ \hline 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 \\ 2 & 0 & 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 & 0 & 2 \end{array}\right) \Rightarrow \left(\begin{array}{cccccc} 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 & 0 \\ 4 & 3 & 2 & 0 & 1 & 0 \\ 0 & 4 & 3 & 2 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \Rightarrow \begin{pmatrix} 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 & 0 \\ 4 & 3 & 2 & 0 & 1 & 0 \\ 0 & 4 & 3 & 2 & 0 & 1 \end{pmatrix}.$$

Így az $R_1 + R_2$ modulus α-hoz tartozó Hermite normál alakja $(2 \cdot 3, M)$, ahol

$$M = \begin{pmatrix} 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 & 0 \\ 4 & 3 & 2 & 0 & 1 & 0 \\ 0 & 4 & 3 & 2 & 0 & 1 \end{pmatrix}.$$

Tehát a K test α-hoz tartozó Hermite normál alakú egész bázisa

$$\begin{pmatrix}\gamma_1\\ \gamma_2\\ \gamma_3\\ \gamma_4\\ \gamma_5\\ \gamma_6\end{pmatrix} = \frac{1}{6}\cdot M \cdot \begin{pmatrix}1\\ \alpha\\ \alpha^2\\ \alpha^3\\ \alpha^4\\ \alpha^5\end{pmatrix} = \begin{pmatrix}1\\ \alpha\\ \alpha^2\\ \frac{1+\alpha^3}{3}\\ \frac{4+3\alpha+2\alpha^2+\alpha^4}{6}\\ \frac{4\alpha+3\alpha^2+2\alpha^3+\alpha^5}{6}\end{pmatrix}.$$

Tekintettel arra, hogy p^k prímhatvány kitevő esetén a $\mathbb{Q}(\sqrt[p^k]{m})$ testek egész bázisa periodikusan ismétlődik modulo p^{k+1}, és a kompozit testek képzésekor a megkonstruált $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ egész bázis csak a résztestek egész bázisainak alakjától függ, ezért prímtényezők szerinti teljes indukcióval adódik a 3.1 Tétel bizonyítása.

Az utolsó lépésben megmutatjuk, hogy a tételben előírt n_0 a legkisebb megfelelő periódushossz. Legyen tehát

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_j^{k_j}$$

alakú, és tegyük fel, hogy valamely kisebb

$$n_0 \mid p_1^{k_1+1} \cdot p_2^{k_2+1} \cdot \ldots \cdot p_j^{k_j+1}$$

periódushossz is megfelelő. Ekkor n_0-ban valamely p_i prímnek a kitevője kisebb lenne, mint $k_i + 1$. Az általánosság megszorítása nélkül feltehetjük, hogy p_1 egy ilyen prímtényező, ekkor speciálisan

$$n_p = p_1^{k_1} \cdot p_2^{k_2+1} \cdot p_3^{k_3+1} \cdot \ldots \cdot p_j^{k_j+1}$$

szintén egy megfelelő periódushossz lenne. Világos, hogy ha a $K = \mathbb{Q}(\sqrt[n]{m})$ testek egész bázisa periodikusan ismétlődik modulo n_p, akkor az $\sqrt[n]{m}$ indexe is periodikusan ismétlődik modulo n_p. Ez azt jelenti, hogy ha m_1 és m_2 olyan négyzetmentes egészek, amelyekre $m_1 \equiv m_2 \pmod{n_p}$, akkor $I(\sqrt[n]{m_1}) = I(\sqrt[n]{m_2})$. A 3.4 Lemma bizonyításából adódóan a p^k fokú gyökbővítések esetén az $\sqrt[p^k]{m}$ elem p-indexe az alábbi alakban írható,

$$v_p\left(I(\sqrt[p^k]{m})\right) = \frac{p^k - p^t}{p-1},$$

ahol $t = \max\{k - v_p(m^p - m) + 1, 0\}$. Továbbá a 3.6 Lemma szerint, ha $n_1 = p_1^{k_1}$ és $n_2 = \frac{n}{n_1}$, akkor

$$I(\sqrt[n]{m}) = \left(I(\sqrt[n_1]{m})\right)^{n_2} \cdot \left(I(\sqrt[n_2]{m})\right)^{n_1},$$

ahonnan

$$v_{p_1}(I(\sqrt[n]{m})) = v_{p_1}\left(\left(I(\sqrt[n_1]{m})\right)^{n_2}\right) + v_{p_1}\left(\left(I(\sqrt[n_2]{m})\right)^{n_1}\right).$$

Mivel $p_1 \nmid n_2$, ezért a 3.2 Állítás alapján $v_{p_1}\left(\left(I(\sqrt[n_2]{m})\right)^{n_1}\right) = 0$, így

$$v_{p_1}(I(\sqrt[n]{m})) = v_{p_1}\left(\left(I(\sqrt[n_1]{m})\right)^{n_2}\right) = n_2 \cdot \frac{p_1^{k_1} - p_1^{t_1}}{p_1 - 1},$$

ahol $t_1 = \max\{k - v_{p_1}(m^{p_1} - m) + 1, 0\}$. Az előzőeket összevetve tehát, ha a $K = \mathbb{Q}(\sqrt[n]{m})$ testek egész bázisa periodikusan ismétlődik modulo n_0, akkor t_1 is periodikusan ismétlődik modulo n_0. A 3.4 Lemma alapján t_1 periodikusan ismétlődik modulo $p_1^{k_1+1}$, most megmutatjuk, hogy t_1 nem ismétlődik periodikusan modulo $p_1^{k_1}$. Ehhez tekintsünk olyan négyzetmentes m_1 és m_2 egészeket, amelyekre

$$m_1 \equiv 1 \pmod{p_1^{k_1+1}} \qquad \text{és} \qquad m_2 \equiv 1 + p_1^{k_1} \pmod{p_1^{k_1+1}}$$

teljesül. Ekkor értelemszerűen $m_1 \equiv m_2 \pmod{p_1^{k_1}}$, továbbá könnyen kiszámítható, hogy

$$v_{p_1}(m_1^{p_1} - m_1) \geq k + 1 \qquad \text{és} \qquad v_{p_1}(m_2^{p_1} - m_2) = k,$$

amiből

$$n_2 \cdot \frac{p_1^{k_1} - p_1^0}{p_1 - 1} = v_{p_1}(I(\sqrt[n]{m_1})) \neq v_{p_1}(I(\sqrt[n]{m_2})) = n_2 \cdot \frac{p_1^{k_1} - p_1^1}{p_1 - 1},$$

következik. Ez pontosan azt jelenti, hogy t_1 nem ismétlődhet periodikusan modulo $p_1^{k_1}$. Mivel t_1 periodikusan ismétlődik modulo $p_1^{k_1+1}$, és a feltevésünk szerint periodikusan ismétlődik modulo n_p, ezért a két periódushossz legnagyobb közös osztója szerint is periodikusan ismétlődik, ami pedig $p_1^{k_1}$. Ez ellentmond a korábbiaknak, így ezzel igazoltuk, hogy

$$n_0 = p_1^{k_1+1} \cdot p_2^{k_2+1} \cdot \ldots \cdot p_j^{k_j+1}$$

valóban a legkisebb megfelelő periódushossz.

Gyakorlatban ezt a következő módon fogjuk használni. Minden $r \in \{0, 1, 2 \ldots, n_0 - 1\}$ esetén, amelyre $\text{lnko}(r, n_0)$ négyzetmentes, legyen t_r olyan egész szám, amelyre $m_r = n_0 \cdot t_r + r$ négyzetmentes. Tetszőleges algoritmust használva kiszámítjuk a $\mathbb{Q}(\sqrt[n]{m_r})$ testekben a maximális rendek $\sqrt[n]{m_r}$-hez tartozó (d_r, M_r) Hermite normál alakjait. Ezután tetszőleges négyzetmentes m paraméter esetén, amelyre $m \equiv r \pmod{n_0}$, a $K = \mathbb{Q}(\sqrt[n]{m})$ test $\sqrt[n]{m}$-hez tartozó Hermite normál alakú egész bázisát az alábbi módon kapjuk

$$\begin{pmatrix} \gamma_1, \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = \frac{1}{d_r} \cdot M_r \begin{pmatrix} 1 \\ \sqrt[n]{m} \\ \vdots \\ \sqrt[n]{m^{n-1}} \end{pmatrix}.$$

Érdemes megjegyezni, hogy a (d_r, M_r) párok nem minden r esetén különböznek. Meg lehet mutatni, hogy p^k kitevő esetén $1+(p-1)\cdot k$ különböző ilyen pár adódik, és mivel ezekből a rakjuk össze n kitevő esetén a megfelelő párokat, ezért ilyenkor

$$\prod_{i=1}^{j}(1+(p_i-1)\cdot k_i)$$

darab pár keletkezik.

A periodikus egész bázis tulajdonság megjelenését eddig olyan n-edfokú polinomcsaládok esetében tapasztaltuk, amelyek felbontási teste n-edfokú ciklikus bővítése valamely másik számtestnek. Ez a gyökbővítések esetén természetesen teljesül, hiszen $X^n - m$ felbontási teste $\mathbb{Q}(\sqrt[n]{m}, \varepsilon_n)$, ami ciklikus n-edfokú bővítése $\mathbb{Q}(\varepsilon_n)$-nek, ahol ε_n egy n-edik primitív egységgyök. Hasonló tulajdonsággal rendelkeznek az úgynevezett legegyszerűbb polinomok egy bizonyos általánosításaként kapható polinomcsaládok is. Ezeket tárgyaljuk a következő fejezetben.

3.2. Legegyszerűbb testek általánosításai és egész bázisai

Ebben a fejezetben a legegyszerűbb polinomok, és az általuk generált legegyszerűbb számtestek egy bizonyos általánosításainak egész bázisairól lesz szó. A fejezethez kapcsolódó eredmények a [28] és [59] cikkben jelentek meg.

Legyen $a, b, c, d \in \mathbb{Q}$ és $\sigma : \mathbb{C} \mapsto \mathbb{C}$ a következő módon adott

$$\sigma(z) = \frac{az + b}{cz + d}.$$

Legyen $f(X) \in \mathbb{Z}[X]$ olyan polinom, melynek gyökei valósak, és azokat σ tranzitíven permutálja. Ekkor ha α az $f(X)$ egy gyöke, akkor a $\mathbb{Q}(\alpha)$ egy teljesen valós ciklikus számtest. Ahhoz, hogy ez teljesüljön, az

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL_2(\mathbb{Q})$$

mátrix rendje véges kell, hogy legyen. Ez a rend lesz az $f(X)$ polinom fokszáma. Könnyen megmutatható, hogy $PGL_2(\mathbb{Q})$ torziós csoportjában az elemek rendje $1, 2, 3, 4$ vagy 6 lehet.

D. Shanks [60], A. J. Lazarus [50], G. Lettl, A. Pethő és P. Voutier [51] és A. Hoshi [41] alapján a 3,4, illetve 6 rendekhez tartozó

$$f_m^{(3)}(X) = X^3 - mX^2 - (m+3)X - 1,$$

$$f_m^{(4)} = X^4 - mX^3 - 6X^2 + mX + 1,$$

$$f_m^{(6)}(X) = X^6 - 2mX^5 - 5(m+3)X^4 - 20X^3 + 5mX^2 + 2(m+3)X + 1$$

polinomokat 3,4 illetve 6-fokú legegyszerűbb polinomoknak nevezzük. Ezen polinomok gyöke által generált teljesen valós, ciklikus 3,4 és 6 fokú számtesteket legegyszerűbb számtesteknek hívjuk, melyeknek a speciális tulajdonságaikból adódóan kiterjedt irodalma van.

A harmadfokú esetet elsőként H. Cohn [9] és D. Shanks [60] vizsgálták. Ezeknek a számtesteknek viszonylag nagy, de relatíve könnyen kiszámolható ideálosztály számuk van, és legelőször emiatt kerültek az érdeklődés középpontjába.

Később M. N. Gras [34], [35], V. Ennola [13], [14] és A. J. Lazarus [50] a legegyszerűbb testek egységeinek csoportját vizsgálták, és K. Foster [18] megmutatta, hogy ezek a számtestek egyértelműen adódnak egy ciklikus bővítések egységeire felírt speciális azonosságból. Ez is mutatja, hogy ezek a számtestek több szempontból is egyedülállóak.

A. Hoshi [42] olyan általánosítását adta a legegyszerűbb számtesteknek, ami azok legtöbb tulajdonságát megőrzi. Úgy definiált egy 12-fokú polinomcsaládot, hogy azoknak a gyökeit szintén a fenti alakú σ Möbius transzformáció permutálja ciklikusan, azzal a kiterjesztéssel, hogy az a, b, c, d együtthatók már a $\mathbb{Q}(\sqrt{3})$ testből

kerülhetnek ki. Mivel a $PGL_2(\mathbb{Q}(\sqrt{3}))$ csoportban már van 12 rendű elem, ezért ezt felhasználva már lehet 12 fokú polinomcsaládokat is generálni. Ez az általánosítás motiválta a mi megközelítéseinket is.

Két esetet fogunk vizsgálni, az első a legegyszerűbb harmad-, illetve hatodfokú, és a Hoshi-féle 12 fokú családokat foglalja magába, a második pedig a legegyszerűbb negyedfokú polinomokat. A fejezet további részében t racionális paraméter.

Legyenek $g, h : \mathbb{N} \mapsto \mathbb{Q}$ az alábbi módon értelmezett függvények

$$g(i) := \begin{cases} 1, & \text{ha } i \equiv 0 \pmod 6, \\ -t, & \text{ha } i \equiv 1 \pmod 6, \\ -t-1, & \text{ha } i \equiv 2 \pmod 6, \\ -1, & \text{ha } i \equiv 3 \pmod 6, \\ t, & \text{ha } i \equiv 4 \pmod 6, \\ t+1, & \text{ha } i \equiv 5 \pmod 6, \end{cases} \quad \text{és } h(i) := \begin{cases} 0, & \text{ha } i \equiv 0 \pmod 6, \\ -1, & \text{ha } i \equiv 1 \pmod 6, \\ -1, & \text{ha } i \equiv 2 \pmod 6, \\ 0, & \text{ha } i \equiv 3 \pmod 6, \\ 1, & \text{ha } i \equiv 4 \pmod 6, \\ 1, & \text{ha } i \equiv 5 \pmod 6. \end{cases}$$

Legyen $n \geq 0$ esetén

$$f_t^{(n)}(X) := \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot g(n-i) \qquad \in \mathbb{Q}[t, X],$$

és legyen $r^{(n)}(X)$ ennek a t változó szerinti deriváltja, azaz

$$r^{(n)}(X) := \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot h(n-i) \qquad \in \mathbb{Z}[X].$$

Ezeknek a polinomoknak sok érdekes tulajdonsága van, ezek közül mutatok most be néhányat, amelyekre szükségünk lesz.

3.7. Lemma. *Minden $n \geq 0$ estén*

$$f_t^{(n+1)}(X) = (X-t) \cdot f_t^{(n)}(X) + (t^2+t+1) \cdot r^{(n)}(X), \tag{3.3}$$

és

$$r^{(n+1)}(X) = (X+t+1) \cdot r^{(n)}(X) - f_t^{(n)}(X). \tag{3.4}$$

Bizonyítás. Számítsuk ki X^k együtthatóját (3.3) bal illetve jobb oldalán. $f_t^{(n+1)}(X)$-ben X^k együtthatója definíció szerint

$$\binom{n+1}{k} \cdot g(n+1-k),$$

a jobb oldalon pedig

$$\binom{n}{k-1} \cdot g(n-k+1) - t \cdot \binom{n}{k} \cdot g(n-k) + (t^2+t+1) \cdot \binom{n}{k} \cdot h(n-k).$$

Könnyű ellenőrizni, hogy $n-k$ tetszőleges 6-os maradéka esetén a fenti két kifejezés megegyezik. Ugyanígy igazolható (3.4) is. □

Egyszerű összefüggést fedezhetünk fel a polinomok deriváltjainak kiszámolásakor is.

$$\begin{aligned}\left(f_t^{(n+1)}\right)'(X) &= \sum_{i=1}^{n+1}\binom{n+1}{i}\cdot i\cdot X^{i-1}\cdot g(n+1-i) = \\ &= (n+1)\sum_{i=1}^{n+1}\binom{n}{i-1}\cdot X^{i-1}\cdot g(n+1-i) = \\ &= (n+1)\cdot f_t^{(n)}(X)\end{aligned}$$

és hasonlóan

$$\left(r^{(n+1)}\right)'(X) = (n+1)\cdot r^{(n)}(X).$$

A következő tétel lesz a kulcs annak igazolásához, hogy az $f_t^{(n)}(X)$ polinomok gyökeit egy megfelelő Möbius transzformáció tranzitíven permutálja.

3.8. Tétel. *Tetszőleges $\beta\in\mathbb{C}$ és $n\geq 1$ esetén*

$$\begin{aligned}(X+\beta+1)^n\cdot f_t^{(n)}\left(\frac{\beta X-1}{X+\beta+1}\right) = \\ = f_t^{(n)}(\beta)\cdot f_t^{(n)}(X) - (t^2+t+1)\cdot r^{(n)}(\beta)\cdot r^{(n)}(X). \quad (3.5)\end{aligned}$$

Bizonyítás. A tételt n szerinti teljes indukcióval fogjuk igazolni. Az eljárás sok számolással jár, de semmilyen egyéb ötletet nem igényel.

Mivel $f_t^{(1)}(X) = X-t$ és $r^{(1)}(X)=-1$, ezért

$$(X+\beta+1)\cdot\left(\frac{\beta X-1}{X+\beta+1}-t\right) = (\beta-t)\cdot(X-t) - (t^2+t+1)\cdot(-1)\cdot(-1)$$

miatt az állítás igaz $n=1$ esetén. Most tegyük fel, hogy igaz valamely $n\in\mathbb{N}$ esetén, és legyen

$$F_t^{(n+1)}(X) := \frac{f_t^{(n+1)}(\beta)\cdot f_t^{(n+1)}(X) - (t^2+t+1)\cdot r^{(n+1)}(\beta)\cdot r^{(n+1)}(X)}{(X+\beta+1)^{n+1}}.$$

Meg fogjuk mutatni, hogy

$$F_t^{(n+1)}(X) = f_t^{(n+1)}\left(\frac{\beta X-1}{X+\beta+1}\right).$$

Ehhez először igazoljuk, hogy a deriváltjaik megegyeznek, majd pedig megmutatjuk, hogy a különbségük ekkor csak 0 lehet.

$$\begin{aligned}\left(F_t^{(n+1)}\right)'(X) &= \frac{(n+1)\left(f_t^{(n+1)}(\beta)\cdot f_t^{(n)}(X) - (t^2+t+1)\cdot r^{(n+1)}(\beta)\cdot r^{(n)}(X)\right)}{(X+\beta+1)^{n+1}} - \\ &- \frac{(n+1)\left(f_t^{(n+1)}(\beta)\cdot f_t^{(n+1)}(X) + (t^2+t+1)\cdot r^{(n+1)}(\beta)\cdot r^{(n+1)}(X)\right)}{(X+\beta+1)^{n+2}}.\end{aligned}$$

A 3.7 Lemma alapján végezzük el az alábbi helyettesítéseket

$$\begin{aligned} r^{(n+1)}(X) &= (X+t+1)\cdot r^{(n)}(X) - f_t^{(n)}(X), \\ f_t^{(n+1)}(X) &= (X-t)\cdot f_t^{(n)}(X) + (t^2+t+1)\cdot r^{(n)}(X), \\ r^{(n+1)}(\beta) &= (\beta+t+1)\cdot r^{(n)}(\beta) - f_t^{(n)}(\beta), \\ f_t^{(n+1)}(\beta) &= (\beta-t)\cdot f_t^{(n)}(\beta) + (t^2+t+1)\cdot r^{(n)}(\beta). \end{aligned}$$

Egyszerűsítés után a következő kifejezést kapjuk

$$\left(F_t^{(n+1)}\right)'(X) = \frac{(n+1)\cdot(\beta^2+\beta+1)\cdot\left(f_t^{(n)}(X)\cdot f_t^{(n)}(\beta) - (t^2+t+1)\cdot r^{(n)}(X)\cdot r^{(n)}(\beta)\right)}{(X+\beta+1)^{n+2}}.$$

Felhasználva, hogy az állítás igaz n esetén,

$$\begin{aligned} \left(F_t^{(n+1)}\right)'(X) &= \frac{(n+1)\cdot(\beta^2+\beta+1)\cdot(X+\beta+1)^n\cdot f_t^{(n)}\left(\frac{\beta X-1}{X+\beta+1}\right)}{(X+\beta+1)^{n+2}} = \\ &= \frac{(n+1)\cdot(\beta^2+\beta+1)\cdot f_t^{(n)}\left(\frac{\beta X-1}{X+\beta+1}\right)}{(X+\beta+1)^2}. \end{aligned}$$

Mivel $\left(f_t^{(n+1)}\right)'(X) = (n+1)\cdot f_t^{(n)}(X)$, ezért

$$\left(f_t^{(n+1)}\right)'\left(\frac{\beta X-1}{X+\beta+1}\right) = \frac{(n+1)\cdot(\beta^2+\beta+1)\cdot f_t^{(n)}\left(\frac{\beta X-1}{X+\beta+1}\right)}{(X+\beta+1)^2},$$

így tehát

$$\left(F_t^{(n+1)}\right)'(X) = \left(f_t^{(n+1)}\right)'\left(\frac{\beta X-1}{X+\beta+1}\right),$$

ahonnan

$$F_{n+1}(X) = f_t^{(n+1)}\left(\frac{\beta X-1}{X+\beta+1}\right) + c$$

adódik. Most megmutatjuk, hogy $c=0$. Ehhez szorozzuk be a fenti egyenlőség mindkét oldalát $(X+\beta+1)^{n+1}$-el. Így mindkét oldalon egy polinom fog szerepelni:

$$\begin{aligned} f_t^{(n+1)}(\beta)\cdot f_t^{(n+1)}(X) - (t^2+t+1)\cdot r^{(n+1)}(\beta)\cdot r^{(n+1)}(X) = \\ = (X+\beta+1)^{n+1}\cdot\left(f_t^{(n+1)}\left(\frac{\beta X-1}{X+\beta+1}\right)+c\right). \end{aligned}$$

Számítsuk ki a főegyütthatót az egyenlet két oldalán. A bal oldalon

$$f_t^{(n+1)}(\beta)\cdot g(0) - (t^2+t+1)\cdot r^{(n+1)}(\beta)\cdot h(0) = f_t^{(n+1)}(\beta),$$

a jobb oldalon pedig

$$f_t^{(n+1)}(\beta) + c.$$

Mivel ezeknek meg kell egyezni, ezért szükségképpen $c = 0$, tehát

$$F_{n+1}(X) = f_t^{(n+1)}\left(\frac{\beta X - 1}{X + \beta + 1}\right),$$

így az állítás igaz $n+1$-re is, és ennélfogva igaz minden $n \in \mathbb{N}$ esetén. □

Bevezetjük az $f_t^{(n)}(X)$ és $r^{(n)}(X)$ polinomok egy másik felírását, amikkel később sokkal könnyebb lesz dolgozni.

3.9. Lemma. *Minden $n \geq 1$ esetén*

$$f_t^{(n)}(X) = \frac{(X-\varepsilon_3)^n + \left(X-\varepsilon_3^2\right)^n}{2} + \left(t + \frac{1}{2}\right) \cdot r^{(n)}(X),$$

és

$$r^{(n)}(X) = \frac{i\sqrt{3}}{3}\left((X-\varepsilon_3)^n - \left(X-\varepsilon_3^2\right)^n\right),$$

ahol

$$\varepsilon_3 = \frac{-1 - i\sqrt{3}}{2}$$

primitív harmadik egységgyök.

Bizonyítás. A 3.7 Lemma szerint

$$\begin{pmatrix} f_t^{(n)}(X) \\ r^{(n)}(X) \end{pmatrix} = \begin{pmatrix} X-t & t^2+t+1 \\ -1 & X+t+1 \end{pmatrix} \cdot \begin{pmatrix} f_t^{(n-1)}(X) \\ r^{(n-1)}(X) \end{pmatrix}.$$

Legyenek a fenti mátrix sajátértékei $\lambda = X - \varepsilon_3$ és $\mu = X - \varepsilon_3^2$, ekkor a mátrix k-adik hatványa

$$\begin{pmatrix} X-t & t^2+t+1 \\ -1 & X+t+1 \end{pmatrix}^k =$$

$$= \begin{pmatrix} \dfrac{\lambda^k+\mu^k}{2} + \dfrac{i\sqrt{3}\left(t+\frac{1}{2}\right)(\lambda^k-\mu^k)}{3} & -\dfrac{i\sqrt{3}(t^2+t+1)(\lambda^k-\mu^k)}{3} \\ \dfrac{i\sqrt{3}(\lambda^k-\mu^k)}{3} & \dfrac{\lambda^k+\mu^k}{2} - \dfrac{i\sqrt{3}\left(m+\frac{1}{2}\right)(\lambda^k-\mu^k)}{3} \end{pmatrix}.$$

Így

$$\begin{pmatrix} f_t^{(n)}(X) \\ r^{(n)}(X) \end{pmatrix} = \begin{pmatrix} X-t & t^2+t+1 \\ -1 & X+t+1 \end{pmatrix}^n \cdot \begin{pmatrix} f_t^{(0)}(X) \\ r^{(0)}(X) \end{pmatrix}$$

alapján, ahol $f_t^{(0)}(X) = 1$ és $r^{(0)}(X) = 0$, azonnal adódik az állítás. □

Ezeknek az új felírásoknak két lényeges következménye van.

3.10. Következmény. *Minden $n \geq 2$ esetén az $r^{(n)}(X)$ összes gyöke*

$$\varepsilon_3 \cdot \frac{1-\varepsilon_3\varepsilon_n}{1-\varepsilon_n},$$

alakú, ahol $\varepsilon_n \neq 1$ egy n-edik egységgyök. Továbbá $f_t^{(n)}(X)$-nek és $r^{(n)}(X)$-nek nincs közös gyöke.

Bizonyítás. A 3.9 Lemmában szereplő képletbe helyettesítve könnyű ellenőrizni, hogy $\varepsilon_n \neq 1$ és $\varepsilon_n^n = 1$ esetén

$$\varepsilon_3 \cdot \frac{1-\varepsilon_3\varepsilon_n}{1-\varepsilon_n}$$

valóban gyöke $r^{(n)}(X)$-nek. Továbbá, ha ε_n és φ_n két különböző n-edik egységgyök, akkor az

$$\varepsilon_3 \cdot \frac{1-\varepsilon_3\varepsilon_n}{1-\varepsilon_n} = \varepsilon_3 \cdot \frac{1-\varepsilon_3\varphi_n}{1-\varphi_n}$$

egyenlőségből $\varepsilon_3 \neq 1$ miatt azt kapjuk, hogy $\varepsilon_n = \varphi_n$, vagyis az

$$\varepsilon_3 \cdot \frac{1-\varepsilon_3\varepsilon_n}{1-\varepsilon_n}, \qquad \varepsilon_n^n = 1, \varepsilon_n \neq 1$$

számok $n-1$ darab különböző gyökét adják az $n-1$-edfokú $r^{(n)}(X)$ polinomnak, azaz pontosan ezek a számok a gyökei.

Most tegyük fel, hogy β gyöke $f_t^{(n)}(X)$-nek és $r^{(n)}(X)$-nek is. Ez azt jelenti, hogy

$$r^{(n)}(\beta) = \frac{i\sqrt{3}}{3}\left((\beta-\varepsilon_3)^n - \left(\beta-\varepsilon_3^2\right)^n\right) = 0,$$

és

$$f_t^{(n)}(\beta) = \frac{(\beta-\varepsilon_3)^n + \left(\beta-\varepsilon_3^2\right)^n}{2} + \left(t+\frac{1}{2}\right)\cdot r^{(n)}(\beta) = 0.$$

Ezekből pedig azt kapjuk, hogy egy ilyen β számra teljesül, hogy

$$(\beta-\varepsilon_3)^n + \left(\beta-\varepsilon_3^2\right)^n = 0 \text{ és } (\beta-\varepsilon_3)^n - \left(\beta-\varepsilon_3^2\right)^n = 0,$$

amiből következően $\beta = \varepsilon_3$. Azonban ε_3 nem lehet gyöke $r^{(n)}(X)$-nek, hiszen nem létezik olyan n-edik egységgyök, amellyel

$$\varepsilon_3 = \varepsilon_3 \cdot \frac{1-\varepsilon_3\varepsilon_n}{1-\varepsilon_n},$$

így tehát $f_t^{(n)}(X)$-nek és $r^{(n)}(X)$-nek nincs közös gyöke. □

Most már minden készen áll ahhoz, hogy megadjuk azt a Möbius transzformációt, amely tranzitíven permutálja az $f_t^{(n)}(X)$ gyökeit.

3.11. Tétel. *Legyen $n \geq 2$ egész szám. Ekkor ha α az $f_t^{(n)}(X)$, β pedig az $r^{(n)}(X)$ polinom gyöke, akkor*

$$\frac{\beta\alpha - 1}{\alpha + \beta + 1}$$

szintén gyöke $f_t^{(n)}(X)$-nek.

Bizonyítás. A 3.8 Tétel alapján,

$$(\alpha+\beta+1)^n \cdot f_t^{(n)}\left(\frac{\beta\alpha-1}{\alpha+\beta+1}\right) = f_t^{(n)}(\beta)\cdot f_t^{(n)}(\alpha) - (t^2+t+1)\cdot r^{(n)}(\beta)\cdot r^{(n)}(\alpha).$$

Az egyenlet jobb oldala nullával egyenlő, hiszen $r^{(n)}(\beta) = f_t^{(n)}(\alpha) = 0$. Megmutatjuk, hogy $\alpha + \beta + 1$ nem lehet nulla, amiből

$$f_t^{(n)}\left(\frac{\beta\alpha-1}{\alpha+\beta+1}\right) = 0$$

következik, amit igazolni szeretnénk. Ehhez vegyük észre, hogy

$$-\varepsilon_3 - 1 = \varepsilon_3^2 \quad \text{és} \quad -\varepsilon_3^2 - 1 = \varepsilon_3$$

miatt a 3.9 Lemmából

$$r^{(n)}(-X-1) = \frac{i\sqrt{3}}{3}\left(\left(-X+\varepsilon_3^2\right)^n - (-X+\varepsilon_3)^n\right) = (-1)^{n-1}\cdot r^{(n)}(X)$$

adódik, azaz ha β gyöke $r^{(n)}(X)$-nek, akkor $-\beta - 1$ is gyöke. Így a 3.10 Következmény alapján ha α az $f_t^{(n)}(X)$ gyöke, és $-\beta - 1$ az $r^{(n)}(X)$ gyöke, akkor $\alpha \neq -\beta - 1$, amiből adódik az állítás. □

Adott $n \geq 2$ esetén vizsgáljuk meg a tételben szereplő

$$\sigma(z) = \frac{\beta z - 1}{z + \beta + 1}$$

Möbius transzformációt, ahol β az $r^{(n)}(X)$ gyöke. A transzformációhoz tartozó mátrix

$$M = \begin{pmatrix} \beta & -1 \\ 1 & \beta+1 \end{pmatrix}.$$

Jelöljünk továbbra is ε_3-al az első primitív harmadik egységgyököt, ekkor az M sajátértékei $\lambda = \beta - \varepsilon_3$ és $\mu = \beta - \varepsilon_3^2$, továbbá

$$M^k = \begin{pmatrix} \dfrac{\lambda^k+\mu^k}{2} + \dfrac{i\sqrt{3}(\lambda^k-\mu^k)}{6} & \dfrac{i\sqrt{3}(\lambda^k-\mu^k)}{3} \\ -\dfrac{i\sqrt{3}(\lambda^k-\mu^k)}{3} & \dfrac{\lambda^k+\mu^k}{2} - \dfrac{i\sqrt{3}(\lambda^k-\mu^k)}{6} \end{pmatrix}.$$

Ez alapján, ha $\sigma^k(\alpha) = \alpha$ teljesül valamilyen $\alpha \in \mathbb{C}$ és $k \in \mathbb{N}$ esetén, akkor

$$\frac{\left(\frac{\lambda^k+\mu^k}{2} + \frac{i\sqrt{3}(\lambda^k-\mu^k)}{6}\right) \cdot \alpha + \frac{i\sqrt{3}(\lambda^k-\mu^k)}{3}}{-\left(\frac{i\sqrt{3}(\lambda^k-\mu^k)}{3}\right) \cdot \alpha + \frac{\lambda^k+\mu^k}{2} - \frac{i\sqrt{3}(\lambda^k-\mu^k)}{6}} = \alpha,$$

azaz átrendezve

$$-\frac{i\sqrt{3}(\lambda^k - \mu^k)}{3} \cdot (\alpha^2 + \alpha + 1) = 0.$$

Tehát ha α nem harmadik egységgyök, akkor ez pontosan akkor teljesülhet, ha

$$\frac{i\sqrt{3}}{3}\left((\beta - \varepsilon_3)^k - \left(\beta - \varepsilon_3^2\right)^k\right) = 0,$$

ami a 3.9 Lemma alapján azt jelenti, hogy β gyöke $r^{(k)}(X)$-nek. Mivel $r^{(n)}(X)$ gyökei

$$\varepsilon_3 \cdot \frac{1 - \varepsilon_3\varepsilon_n}{1 - \varepsilon_n},$$

alakúak, ahol ε_n n-edik egységgyök, ezért ha φ_n egy primitív n-edik egységgyök, és

$$\beta = \varepsilon_3 \cdot \frac{1 - \varepsilon_3\varphi_n}{1 - \varphi_n},$$

akkor a legkisebb k természetes szám, amelyre β gyöke $r^{(k)}(X)$-nek, éppen n, és így a fenti σ Möbius transzformáció rendje pontosan n.

Ezekből következik az $f_t^{(n)}(X)$ polinomok felbontási testére vonatkozó alábbi tulajdonság, amely sejtéseink szerint összefügg az egész bázisok periodicitásával.

3.12. Tétel. *Legyen $n \geq 2$ természetes szám,*

$$\beta = \varepsilon_3 \cdot \frac{1 - \varepsilon_3\varepsilon_n}{1 - \varepsilon_n},$$

ahol ε_3 primitív harmadik egységgyök, ε_n pedig primitív n-edik egységgyök. Legyen α az $f_t^{(n)}(X)$ gyöke, ekkor az $f_t^{(n)}(X)$ polinom felbontási teste $\mathbb{Q}(\alpha, \beta)$, ami ciklikus bővítése $\mathbb{Q}(\beta)$-nak. Speciálisan, ha $t \in \mathbb{Q}$ olyan paraméter, hogy az $f_t^{(n)}(X)$ polinom irreducibilis, akkor $f_t^{(n)}(X)$ felbontási teste ciklikus n-edfokú bővítése $\mathbb{Q}(\beta)$-nak.

Bizonyítás. A feltételek alapján a

$$\sigma(z) = \frac{\beta z - 1}{z + \beta + 1}$$

Möbius transzformáció rendje $PGL_2(\mathbb{Q}(\beta))$-ban n, és a 3.11 Tétel szerint, ha α gyöke $f_t^{(n)}(X)$-nek, akkor $\sigma(\alpha)$ is gyöke, azaz, ha α nem harmadik egységgyök, akkor $f_t^{(n)}(X)$ összes különböző gyöke $\{\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\}$. A σ alakja miatt a

$\mathbb{Q}(\alpha,\beta)$ test tartalmazza az $f_t^{(n)}(X)$ összes gyökét. Másrészt az $f_t^{(n)}(X)$ felbontási teste tartalmazza α-t és $\sigma(\alpha)$-t, így tartalmazza az

$$\frac{\alpha^2+\alpha+1}{\alpha-\sigma(\alpha)}-\alpha-1$$

számot is, ami éppen β. Ez az előzővel együtt azt jelenti, hogy $f_t^{(n)}(X)$ felbontási teste $\mathbb{Q}(\alpha,\beta)$. Mivel a σ által generált hatás az $f_t^{(n)}(X)$ gyökein egy n hosszú ciklus, így ha $f_t^{(n)}(X)$ irreducibilis, akkor $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}(\beta)$ egy ciklikus n-edfokú bővítés. □

A következőkben megmutatjuk, hogy ha t olyan racionális paraméter, amellyel az $f_t^{(n)}(X)$ irreducibilis és egész együtthatós, valamint t^2+t+1 négyzetmentes, akkor a polinomcsalád gyökei által generált testek egész bázisa periodikusan ismétlődik modulo n_0, ahol n_0 alegnagyobb olyan egész, amelyre

$$n_0^2 \;\Big|\; \left(3^{\frac{n(n-1)}{2}}\cdot n^n\right)^n.$$

Ehhez először meg kell határoznunk az $f_t^{(n)}(X)$ diszkriminánsát. Legyen

$$A(X)=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0=a_n\cdot\prod_{i=1}^{n}(X-\gamma_i),$$

$$B(X)=b_mX^m+b_{m-1}X^{m-1}+\ldots+b_1X+b_0=b_m\cdot\prod_{i=1}^{m}(X-\delta_i).$$

Ekkor definíció szerint az $A(X)$ és $B(X)$ polinomok rezultánsa

$$\operatorname{res}(A,B)=a_n^m\cdot b_m^n\cdot\prod_{i=1}^{n}\prod_{j=1}^{m}(\gamma_i-\delta_j)=a_n^m\cdot\prod_{i=1}^{n}B(\gamma_i)=(-1)^{nm}\cdot b_m^n\cdot\prod_{i=1}^{m}A(\delta_i).$$

A számításokhoz két polinom rezultánsának alábbi tulajdonságait fogjuk használni (ld. [57], Chapter 2.3.3).

- Ha $n\geq m$ és Q,R olyan polinomok, hogy $A=QB+R$ teljesül, akkor
$$\operatorname{res}(A,B)=b_m^{n-r}\cdot\operatorname{res}(R,B), \tag{3.6}$$
ahol r az R polinom foka.
- Tetszőleges 1 főegyütthatós Q polinom esetén
$$\operatorname{res}(AQ,B)=\operatorname{res}(A,B)\cdot\operatorname{res}(Q,B). \tag{3.7}$$
- Tetszőleges $\lambda\in\mathbb{C}$ esetén
$$\operatorname{res}(\lambda A,B)=\lambda^m\cdot\operatorname{res}(A,B), \tag{3.8}$$
és
$$\operatorname{res}(A,\lambda B)=\lambda^n\cdot\operatorname{res}(A,B). \tag{3.9}$$

Ezeket és a 3.9 Lemmát használva már könnyen ki tudjuk számolni az $f_t^{(n)}(X)$ diszkriminánsát.

3.13. Állítás. *Ha $n \geq 2$, akkor $f_t^{(n)}(X)$ diszkriminánsa*

$$D_{f_t^{(n)}} = 3^{\frac{(n-1)(n-2)}{2}} \cdot n^n \cdot (t^2+t+1)^{n-1}.$$

Bizonyítás. Mivel

$$D_{f_t^{(n)}} = (-1)^{\frac{n(n-1)}{2}} \cdot \operatorname{res}\left(f_t^{(n)}(X), \left(f_t^{(n)}\right)'(X)\right)$$

és $\left(f_t^{(n)}\right)'(X) = n \cdot f_t^{(n-1)}(X)$, ezért (3.9) miatt

$$D_{f_t^{(n)}} = (-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot \operatorname{res}(f_t^{(n)}(X), f_t^{(n-1)}(X)).$$

Most használva a (3.3) összefüggést $f_t^{(n)}(X)$-re, $D_{f_t^{(n)}}$-re a következő kifejezést kapjuk:

$$(-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot \operatorname{res}\left((X-t) \cdot f_t^{(n-1)}(X) + (t^2+t+1) \cdot r^{(n-1)}(X), f_t^{(n-1)}(X)\right).$$

Ekkor $Q = X - t$, $B = f_t^{(n-1)}(X)$ és $R = (t^2+t+1) \cdot r^{(n-1)}(X)$ helyettesítéssel (3.6) alapján kapjuk, hogy

$$D_{f_t^{(n)}} = (-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot \operatorname{res}\left((t^2+t+1) \cdot r^{(n-1)}(X), f_t^{(n-1)}(X)\right),$$

amiből (3.8) miatt

$$D_{f_t^{(n)}} = (-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot (t^2+t+1)^{n-1} \cdot \operatorname{res}\left(r^{(n-1)}(X), f_t^{(n-1)}(X)\right)$$

adódik. Ez utóbbi rezultánst pedig meg is tudjuk határozni, mivel ismerjük $r^{(n-1)}(X)$ összes gyökét. A jelölések egyszerűsítése miatt inkább n kitevőre számoljuk ki ezt a rezultánst, majd a kapott képletbe n helyére $n-1$-et helyettesítünk. Mivel $r^{(n)}(X)$ főegyütthatója $\binom{n}{1} \cdot h(1) = -n$ és a gyökei

$$\varepsilon_3 \cdot \frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}, \qquad j = 1, \ldots, n-1,$$

ahol ε_n primitív n-edik egységgyök, ezért

$$\operatorname{res}\left(r^{(n)}(X), f_t^{(n)}(X)\right) = (-n)^n \cdot \prod_{j=1}^{n-1} f\left(\varepsilon_3 \cdot \frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}\right),$$

Az 3.9 Lemmából

$$f\left(\varepsilon_3\cdot\frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}\right)=\frac{\left(\varepsilon_3\cdot\frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}-\varepsilon_3\right)^n+\left(\varepsilon_3\cdot\frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}-\varepsilon_3^2\right)^n}{2}+$$
$$+\left(t+\frac{1}{2}\right)\cdot r^{(n)}\left(\varepsilon_3\cdot\frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}\right).$$

A második tag itt értelemszerűen eltűnik, hiszen $r^{(n)}(X)$-be pont egy gyökét helyettesítjük, így

$$f\left(\varepsilon_3\cdot\frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}\right)=\frac{\left(\varepsilon_3\cdot\frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}-\varepsilon_3\right)^n+\left(\varepsilon_3\cdot\frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}-\varepsilon_3^2\right)^n}{2}.$$

Ezt egyszerűbb alakra hozva,

$$f\left(\varepsilon_3\cdot\frac{1-\varepsilon_3\varepsilon_n^j}{1-\varepsilon_n^j}\right)=\frac{\left(\frac{\varepsilon_3-\varepsilon_3^2}{1-\varepsilon_n^j}\right)^n\cdot\left(\varepsilon_n^j\right)^n+\left(\frac{\varepsilon_3-\varepsilon_3^2}{1-\varepsilon_n^j}\right)^n}{2}=(i\sqrt{3})^n\cdot\frac{1}{(1-\varepsilon_n^j)^n}.$$

Így

$$\begin{aligned}\operatorname{res}\left(r^{(n)}(X),f_t^{(n)}(X)\right) &= (-n)^n\prod_{j=1}^{n-1}(i\sqrt{3})^n\cdot\frac{1}{(1-\varepsilon_n^j)^n}=\\ &= (-1)^{\frac{n(n-1)}{2}}\cdot 3^{\frac{n(n-1)}{2}}\cdot(-n)^n\cdot\prod_{j=1}^{n-1}\left(\frac{1}{1-\varepsilon_n^j}\right)^n.\end{aligned}$$

Vegyük észre, hogy a $\frac{1}{1-\varepsilon_n^j}$, $j=1,\dots,n-1$ számok pont az

$$(X-1)^n-X^n$$

polinom összes gyökei. Ennek a polinomnak a konstans tagja $(-1)^n$, a főegyütthatója $-n$, így a gyökeinek szorzata $\frac{(-1)^n}{-n}$. Ezek alapján

$$\operatorname{res}\left(r^{(n)}(X),f_t^{(n)}(X)\right)=(-1)^{\frac{n(n-1)}{2}}\cdot 3^{\frac{n(n-1)}{2}}\cdot(-n)^n\cdot\left(\frac{(-1)^n}{-n}\right)^n=(-1)^{\frac{3n^2-n}{2}}\cdot 3^{\frac{n(n-1)}{2}}.$$

Felhasználva, hogy $2n(n-1)$ osztható 4-el, azaz $3n^2-n\equiv n^2+n \pmod 4$, adódik, hogy

$$(-1)^{\frac{3n^2-n}{2}}=(-1)^{\frac{n(n+1)}{2}},$$

vagyis

$$\operatorname{res}\left(r^{(n)}(X),f_t^{(n)}(X)\right)=(-1)^{\frac{n(n+1)}{2}}\cdot 3^{\frac{n(n-1)}{2}}.$$

Ez alapján

$$\operatorname{res}\left(r^{(n-1)}(X),f_t^{(n-1)}(X)\right)=(-1)^{\frac{n(n-1)}{2}}\cdot 3^{\frac{(n-1)(n-2)}{2}},$$

amit visszahelyettesítve a diszkriminánsba, kapjuk, hogy

$$\begin{aligned} D_{f_t^{(n)}} &= (-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot (t^2+t+1)^{n-1} \cdot \operatorname{res}\left(r^{(n-1)}(X), f_t^{(n-1)}(X)\right) = \\ &= 3^{\frac{(n-1)(n-2)}{2}} \cdot n^n \cdot (t^2+t+1)^{n-1}. \end{aligned}$$

□

A következő lépésben megmutatjuk, hogy ha létezik olyan p prím, amelyre $v_p(t^2+t+1)=1$, akkor $f_t^{(n)}(X)$ irreducibilis.

3.14. Lemma. *Ha $p \neq 3$ olyan prím, amelyre $v_p(t^2+t+1)=1$, és $s \in \mathbb{Z}$ olyan, hogy $v_p(s-t)=1$, akkor $v_p\left(f_t^{(n)}(s)\right)=1$ teljesül minden $n \geq 1$ esetén.*

Bizonyítás. A 3.9 Lemma alapján könnyen ellenőrizhető, hogy $n \geq 2$ esetén

$$f_t^{(n)}(X) = (2X+1) \cdot f_t^{(n-1)}(X) - (X^2+X+1) \cdot f_t^{(n-2)}(X).$$

Ehhez legyen $A=(X-\varepsilon_3)$ és $B=(X-\varepsilon_3^2)$, ekkor

$$f_t^{(n)}(X) = \frac{A^n+B^n}{2} + \left(t+\frac{1}{2}\right) \cdot \frac{i\sqrt{3}}{3} \cdot (A^n-B^n).$$

Ebből

$$\frac{A^n+B^n}{2} = (A+B) \cdot \frac{A^{n-1}+B^{n-1}}{2} - A \cdot B \cdot \frac{A^{n-2}+B^{n-2}}{2}$$

és

$$A^n-B^n = (A+B) \cdot (A^{n-1}-B^{n-1}) - A \cdot B \cdot (A^{n-2}-B^{n-2}),$$

valamint $A+B=2X+1$ és $A \cdot B = X^2+X+1$ miatt adódik a fenti összefüggés.

Most legyen s olyan racionális egész, melyre teljesül, hogy $v_p(s-t)=1$. Ilyen s egész szám minden olyan $t \in \mathbb{Q}$ paraméter és p prím esetén létezik, melyre $v_p(t^2+t+1)=1$. Ilyenkor ugyanis $v_p(t)=0$, azaz $t=u/q$ alakban írható, ahol $u,q \in \mathbb{Z}$ és $v_p(u)=v_p(q)=0$. Így azok az s egész számok, melyekre $s \equiv u \cdot q^{-1} \pmod{p}$, és $s \not\equiv u \cdot q^{-1} \pmod{p^2}$ megfelelőek lesznek.

A fenti összefüggés szerint, ha $n \geq 2$, akkor

$$f_t^{(n)}(s) = (2s+1) \cdot f_t^{(n-1)}(s) - (s^2+s+1) \cdot f_t^{(n-2)}(s).$$

Ebből, a p-adikus rend tulajdonságai alapján, ha $n \geq 2$, akkor

$$v_p(f_t^{(n)}(s)) \geq \min\{v_p((2s+1) \cdot f_t^{(n-1)}(s)), v_p((s^2+s+1) \cdot f_t^{(n-2)}(s))\}, \quad (3.10)$$

következik, ahol egyenlőség áll fenn, ha a $(2s+1) \cdot f_t^{(n-1)}(s)$ és az $(s^2+s+1) \cdot f_s^{(n-2)}(s)$ kifejezések p-adikus rendje különbözik. A $v_p(t^2+t+1)=1$ és $v_p(s-t)=1$ összefüggésekből következően

$$v_p(s^2+s+1)=1, \text{ és } v_p((s-t)^2-(t^2+t+1))=1.$$

Továbbá, mivel $4(s^2+s+1)-(2s+1)^2=3$ és $p\neq 3$, ezért ha $v_p(s^2+s+1)=1$, akkor $v_p(2s+1)=0$, azaz (3.10) egyenlőséggel teljesül, ha

$$v_p(f_t^{(n-1)}(s)) \neq v_p(f_t^{(n-2)}(s))+1.$$

Mivel most

$$v_p(f_t^{(1)}(s)) = v_p(s-t) = 1,$$

és

$$v_p(f_t^{(2)}(s)) = v_p(s^2-2st-t-1) = 1,$$

ezért innentől $\min\{0+1, 1+1\}=1$ miatt n-szerinti teljes indukcióval adódik az állítás. □

3.15. Tétel. *Ha $p\neq 3$ olyan prím, amelyre $v_p(t^2+t+1)=1$, akkor $f_t^{(n)}(X)$ irreducibilis. Továbbá, ha α az $f_t^{(n)}(X)$ gyöke, ahol a t paraméterre a fentieken túl még az is teljesül, hogy az $f_t^{(n)}(X)$ polinom egész együtthatós, akkor a $\mathbb{Q}(\alpha)$ testben az α indexe nem osztható p-vel, vagyis $v_p(I(\alpha))=0$.*

Bizonyítás. Legyen $s\in\mathbb{Z}$ ismét olyan egész, melyre teljesül, hogy $v_p(s-t)=1$. Az állítás első feléhez tekintsük az $f_t^{(n)}(X)$ polinom s-körüli Taylor-sorát:

$$f_t^{(n)}(X) = \sum_{i=0}^{n} \frac{\left(f_t^{(n)}\right)^{(i)}(s)}{i!}\cdot(X-s)^i.$$

Mivel $\left(f_t^{(n)}\right)'(X) = n\cdot f_t^{(n-1)}(X)$, ezért

$$\left(f_t^{(n)}\right)^{(i)}(X) = \frac{n!}{(n-i)!}\cdot f_t^{(n-i)}(X),$$

és így

$$f_t^{(n)}(X) = \sum_{i=0}^{n}\binom{n}{i}\cdot f_t^{(n-i)}(s)\cdot(X-s)^i,$$

amiből $X=X+s$ helyettesítéssel,

$$f_t^{(n)}(X+s) = \sum_{i=0}^{n}\binom{n}{i}\cdot f_t^{(n-i)}(s)\cdot X^i.$$

Jelöljük a_i-vel az X^i együtthatóját az $f_t^{(n)}(X+s)$ polinomban. A 3.14 Lemma alapján $0\leq i\leq n-2$ esetén $v_p(a_i)=1$, továbbá $a_{n-1}=f_t^{(1)}(s)=0$ miatt $v_p(a_{n-1})=\infty$, végül $a_n=f_t^{(0)}(s)=1$ miatt $v_p(a_n)=0$. Tehát összességében teljesül az, hogy $v_p(a_n)=0$, $v_p(a_i)>0$, ha $0\leq i\leq n-1$ és $v_p(a_0)=1$, vagyis az $f_t^{(n)}(X+s)$ polinom p-Eisenstein és így irreducibilis, amiből következően $f_t^{(n)}(X)$ is irreducibilis.

Az állítás második részéhez vegyük észre, hogy a t-re vonatkozó feltételek miatt α algebrai egész, amely a $K = \mathbb{Q}(\alpha)$ testben nyilvánvalóan primitív, és így lehet értelmezni az indexét. Az index definíciója szerint

$$I(\alpha)^2 = \frac{D(\alpha)}{D_K},$$

ahol $D(\alpha)$ az α hatványai által generált bázis diszkriminánsa, D_K pedig a $\mathbb{Q}(\alpha)$ test diszkriminánsa. A $D(\alpha)$ megegyezik az $f_t^{(n)}(X)$ diszkriminánsával, ami pedig eltolás invariáns, azaz $D(\alpha) = D(\alpha - s)$. Az $\alpha - s$ szintén primitív algebrai egész a K testben, így annak is értelmezhető az indexe, amiből

$$I(\alpha)^2 = \frac{D(\alpha)}{D_K} = \frac{D(\alpha - s)}{D_K} = I(\alpha - s)^2,$$

azaz

$$v_p(I(\alpha)) = v_p(I(\alpha - s))$$

adódik. Az előzőek miatt $f_t^{(n)}(X + s)$, azaz az $\alpha - s$ definiáló főpolinomja p-Eisenstein, így a 2.2 Állítás miatt $v_p(I(\alpha - s)) = 0$, amiből következik, hogy

$$v_p(I(\alpha)) = 0.$$

□

Innentől kezdve legyen t olyan racionális paraméter, amellyel az $f_t^{(n)}(X)$ polinom egész együtthatós. Ez gyakorlatban azt jelenti, hogy

$$t = \frac{m}{3^{v_3(n)}},$$

ahol $m \in \mathbb{Z}$. A definíció alapján könnyű ellenőrizni, hogy $r^{(n)}(X)$ minden együtthatója osztható $3^{v_3(n)}$-el. Ez $v_3(n) = 0$ esetén triviális. Ha $v_3(n) \geq 1$, akkor a $h : \mathbb{N} \mapsto \mathbb{N}$ definíciója alapján az

$$r^{(n)}(X) = \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot h(n-i)$$

polinom együtthatói $3 \mid i$ esetén a 0-val egyenlőek, $3 \nmid i$ esetén pedig $\pm\binom{n}{i}$-vel. Kummer tétele szerint (ld. [47]), $v_3\left(\binom{n}{i}\right)$ megegyezik az $n - i$ és az i számok 3-as számrendszerbeli összeadásakor szükséges átvitelek számával. Mivel most $3 \nmid i$, így az i utolsó számjegye 3-as számrendszerben nem 0, viszont n utolsó $v_3(n)$ számjegye 0, így mikor összeadjuk $n-i$-t és i-t, legalább $v_3(n)$ darab átvitelt végzünk, vagyis ekkor

$$v_3\left(\binom{n}{i}\right) \geq v_3(n).$$

Végül, mivel $f_t^{(n)}(X) = f_0^{(n)}(X) + t \cdot r^{(n)}(X)$, ahol $f_0^{(n)}(X)$ definíció alapján egész együtthatós, a $t \cdot r^{(n)}(X)$ pedig az előzőek miatt lesz egész együtthatós, ezért a fenti helyettesítéssel $f_t^{(n)}(X)$ valóban egész együtthatós lesz.

A továbbiakban $f_t^{(n)}(X)$ helyett az $f_m^{(n)}(X)$ jelölést fogjuk használni, ami a fenti helyettesítésre utal. Itt megjegyezzük, hogy $n = 3$ és $n = 6$ esetén $f_m^{(n)}(X)$ megegyezik a legegyszerűbb harmad- és hatodfokú polinomokkal, így ez a megközelítés valóban azok általánosításának tekinthető. Továbbá $n = 12$ esetén a Hoshi-féle 12-edfokú polinomcsaládot kapjuk speciális esetként.

Az új paraméterezéssel, a polinom diszkriminánsára vonatkozó eredményünk a következőképpen módosul,

$$D_{f_m^{(n)}} = 3^{\frac{(n-1)(n-2)}{2}} \cdot n^n \cdot \left(\left(\frac{m}{3^{v_3(n)}} \right)^2 + \frac{m}{3^{v_3(n)}} + 1 \right)^{n-1}.$$

A 3.15 Tétel alapján, ha α az $f_m^{(n)}(X)$ gyöke, $p \neq 3$ prím, és $m \in \mathbb{Z}$ olyan egész szám, amelyre

$$v_p\left(\left(\frac{m}{3^{v_3(n)}} \right)^2 + \frac{m}{3^{v_3(n)}} + 1 \right) = 1.$$

teljesül, akkor $v_p(I(\alpha)) = 0$. Ennek segítségével adott n fokszám esetén felső becslést tudunk adni a α indexére.

Az állításaink egyszerűbb megfogalmazása érdekében azt mondjuk, hogy az $m \in \mathbb{Z}$ paraméter *megfelelő*, ha tetszőleges $p \neq 3$ prím esetén teljesül, hogy

$$v_p\left(\left(\frac{m}{3^{v_3(n)}} \right)^2 + \frac{m}{3^{v_3(n)}} + 1 \right) \leq 1,$$

azaz $t^2 + t + 1$-nek a 3-mentes része négyzetmentes. Megjegyezzük, hogy mivel $t^2 + t + 1$ irreducibilis polinom $\mathbb{Q}[t]$-ben, ezért T. Nagell [54] eredményei alapján végtelen sok megfelelő m paraméter létezik.

3.16. Tétel. *Legyen $m \in \mathbb{Z}$ megfelelő paraméter, és α az $f_m^{(n)}(X)$ gyöke. Ekkor*

$$I(\alpha)^2 \;\Big|\; 3^{\frac{n(n-1)}{2}} \cdot n^n.$$

Bizonyítás. Mivel $I(\alpha)^2 \mid D_{f_m^{(n)}}$, és $I(\alpha)$-nak $\left(\left(\frac{m}{3^{v_3(n)}} \right)^2 + \frac{m}{3^{v_3(n)}} + 1 \right)$-el csak a 3 lehet közös prímosztója, ezért

$$I(\alpha)^2 \;\Big|\; 3^{\frac{(n-1)(n-2)}{2} + (n-1)\cdot v_3\left(\left(\frac{m}{3^{v_3(n)}} \right)^2 + \frac{m}{3^{v_3(n)}} + 1 \right)} \cdot n^n$$

Most megmutatjuk, hogy tetszőleges $t \in \mathbb{Q}$ esetén $v_3(t^2 + t + 1) \leq 1$. Ha $v_3(t) \neq 0$, akkor $v_3(t^2), v_3(t)$ és $v_3(1)$ különböző számok, így

$$v_3(t^2 + t + 1) = \min\{v_3(t^2), v_3(t), v_3(1)\} \leq 0.$$

Ha pedig $v_3(t) = 0$, akkor $t = \frac{p}{q}$, ahol p és q hárommal nem osztható relatív prím egészek. Legyen r a q inverze modulo 9, és tegyük fel, hogy $v_3(t^2 + t + 1) \geq 2$. Ekkor a

$$(p \cdot r)^2 + (p \cdot r) + 1 \equiv 0 \pmod 9$$

kongruenciának lenne megoldása, azonban kézzel könnyen ellenőrizhető, hogy ez semmilyen $p \cdot r \in \{1, 2, 4, 5, 7, 8\}$ maradékosztály esetén sem teljesül, így ellentmondás kaptunk, amiből az következik, hogy $v_3(t^2 + t + 1) \leq 1$. A fenti képletben tehát

$$v_3\left(\left(\frac{m}{3^{v_3(n)}}\right)^2 + \frac{m}{3^{v_3(n)}} + 1\right) \leq 1$$

matt azt kapjuk, hogy

$$I(\alpha)^2 \;\Big|\; 3^{\frac{(n-1)(n-2)}{2}+(n-1)\cdot 1} \cdot n^n = 3^{\frac{n(n-1)}{2}} \cdot n^n.$$

□

Mivel $I(\alpha) \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha]$, ezért ebből a 2.4 Állítás alapján már következik a periodikus egész bázis tulajdonság, valamint felső korlátot is kapunk a periódus hosszára.

3.17. Következmény. *Legyen $m \in \mathbb{Z}$ megfelelő paraméter, és α az $f_m^{(n)}(X)$ gyöke. Ekkor a $K = \mathbb{Q}(\alpha)$ testek egész bázisa periodikusan ismétlődik modulo n_0, ahol n_0 a legnagyobb olyan egész szám, amelyre teljesül, hogy*

$$n_0^2 \;\Big|\; \left(3^{\frac{n(n-1)}{2}} \cdot n^n\right)^n.$$

Ez a periódushossz már kis fokszámok esetén is kifejezetten nagy, azonban a duális bázis módszerrel adott n fokszámok esetén javíthatunk a becsléseken. Például $n = 4$ esetén, ha α az $f_t^{(4)}(X)$ polinom gyöke, akkor az $(1, \alpha, \alpha^2, \alpha^3)$-höz tartozó duális bázis

$$\begin{aligned}
&\Bigg(\frac{8t^2+3t+12}{12(t^2+t+1)} + \frac{-4t^2+7t+18}{12(t^2+t+1)}\cdot\alpha + \frac{-8t^2+10t}{12(t^2+t+1)}\cdot\alpha^2 + \frac{2t-3}{12(t^2+t+1)}\cdot\alpha^3,\\
&\frac{-4t^2+7t+18}{12(t^2+t+1)} + \frac{40t^2+92t+62}{12(t^2+t+1)}\cdot\alpha + \frac{32t^2+46t+5}{12(t^2+t+1)}\cdot\alpha^2 + \frac{-8t-11}{12(t^2+t+1)}\cdot\alpha^3,\\
&\frac{-8t^2+10t}{12(t^2+t+1)} + \frac{32t^2+46t+5}{12(t^2+t+1)}\cdot\alpha + \frac{32t^2+8t+1}{12(t^2+t+1)}\cdot\alpha^2 + \frac{-8t-1}{12(t^2+t+1)}\cdot\alpha^3,\\
&\frac{2t-3}{12(t^2+t+1)} + \frac{-8t-11}{12(t^2+t+1)}\cdot\alpha + \frac{-8t-1}{12(t^2+t+1)}\cdot\alpha^2 + \frac{2}{12(t^2+t+1)}\cdot\alpha^3\Bigg).
\end{aligned}$$

Ebből azonnal adódik, hogy megfelelő m paraméterek esetén

$$12 \cdot \left(m^2 + m + 1\right) \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha],$$

ami azzal együtt, hogy

$$I(\alpha)^2 \;\Big|\; 3^{\frac{n(n-1)}{2}} \cdot n^n\,,$$

azt eredményezi, hogy $12 \cdot 3 \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha]$.

Ezeket a vizsgálatokat $n = 2, 3, \ldots, 12$ fokszámok esetén végeztük el, és az alábbi eredményeket kaptuk.

3.18. Állítás. *Legyen $m \in \mathbb{Z}$ megfelelő paraméter, és α az $f_m^{(n)}(X)$ gyöke. Ekkor az $(1, \alpha, \ldots, \alpha^{n-1})$ bázishoz tartozó duális bázis meghatározásával, majd alkalmazva a*

$$v_3\left(\left(\frac{m}{3^{v_3(n)}}\right)^2 + \frac{m}{3^{v_3(n)}} + 1\right) \leq 1$$

becslést, $n = 2, 3, \ldots, 12$ esetén azt kapjuk, hogy $C_n \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha]$, ahol

n	2	3	4	5	6	7	8	9	10	11	12
C_n	6	27	$3^2 \cdot 4$	$3^4 \cdot 5$	$3^5 \cdot 6$	$3^5 \cdot 7$	$3^6 \cdot 8$	$3^7 \cdot 9$	$3^6 \cdot 10$	$3^{10} \cdot 11$	$3^{10} \cdot 12$

.

Ezeket a C_n számokat felhasználva, a 2.4 Állítás segítségével sokkal jobb korlátokat kaptunk az egész bázisok periódusának hosszára. Ezek a kisebb n_0 korlátok bizonyos kis fokszámok esetén már lehetőséget adtak arra, hogy minden megfelelő n_0-maradékosztályba eső paraméterre egyenként meghatározzuk a α-hoz tartozó Hermite normál alakú egész bázist, majd ránézésre megállapítsuk a tényleges legkisebb periódushosszt. Ezt a vizsgálatot $n = 2, 3, 4, 5, 6, 8, 9$ és 12 esetén végeztük el, azzal a további megkötéssel, hogy most $v_3(m^2 + 3^{v_3(n)}m + 9^{v_3(n)}) \leq 1$ is teljesüljön, azaz $m^2 + 3^{v_3(n)}m + 9^{v_3(n)}$ legyen négyzetmentes. Ez a plusz feltétel egy 3 hatvánnyal csökkenti a periódushosszt, viszont így a későbbiekben könnyebb lesz használni az eredményt.

3.19. Következmény. *Legyen $m \in \mathbb{Z}$ olyan paraméter, amelyre teljesül, hogy $m^2 + 3^{v_3(n)}m + 9^{v_3(n)}$ négyzetmentes, és legyen α az $f_m^{(n)}(X)$ gyöke. Ekkor $n = 2, 3, 4, 5, 6, 8, 9, 12$ esetén a $K = \mathbb{Q}(\alpha)$ testek egész bázisa periodikusan ismétlődik modulo n_0, ahol*

n	2	3	4	5	6	8	9	12
n_0	4	1	24	75	36	432	243	1944

.

Ezek az esetek tartalmazzák a három korábban vizsgált nevezetes polinomcsaládot.

- Legegyszerűbb harmadfokú polinomok

$$f_m^{(3)}(X) = X^3 - mX^2 - (m+3)X - 1.$$

- Legegyszerűbb hatodfokú polinomok

$$f_m^{(6)}(X) = X^6 - 2mX^5 - 5(m+3)X^4 - 20X^3 + 5mX^2 + 2(m+3)X + 1.$$

- Hoshi-féle 12-edfokú polinomok

$$\begin{aligned} f_m^{(12)}(X) &= X^{12} - 4mX^{11} - 22(m+3)X^{10} - 220X^9 + 165mX^8 + 264(m+3)X^7 + \\ &\quad + 924X^6 - 264mX^5 - 165(m+3)X^4 - 220X^3 + 22mX^2 + 4(m+3)X + 1. \end{aligned}$$

Most következik a másik általánosítás, ami a legegyszerűbb negyedfokú polinomokat foglalja magába. Mivel az állítások bizonyítása értelemszerű módosításokkal, pontosan ugyanúgy történik, mint az előző általánosítás esetében, ezért azokat nem fogom újra levezetni.

Legyenek $g, h : \mathbb{N} \mapsto \mathbb{Q}$ az alábbi módon értelmezett függvények

$$g(i) := \begin{cases} 1, & \text{ha } i \equiv 0 \pmod 4, \\ -t, & \text{ha } i \equiv 1 \pmod 4, \\ -1, & \text{ha } i \equiv 2 \pmod 4, \\ t, & \text{ha } i \equiv 3 \pmod 4. \end{cases} \quad \text{és } h(i) := \begin{cases} 0, & \text{ha } i \equiv 0 \pmod 4, \\ -1, & \text{ha } i \equiv 1 \pmod 4, \\ 0, & \text{ha } i \equiv 2 \pmod 4, \\ 1, & \text{ha } i \equiv 3 \pmod 4. \end{cases}$$

Legyen $n \geq 0$ esetén

$$f_t^{(n)}(X) := \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot g(n-i) \qquad \in \mathbb{Q}[t, X],$$

és legyen $r^{(n)}(X)$ ennek a t változó szerinti deriváltja, azaz

$$r^{(n)}(X) := \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot h(n-i) \qquad \in \mathbb{Z}[X].$$

3.20. Lemma. *Minden $n \geq 0$ estén*

$$f_t^{(n+1)}(X) = (X - t) \cdot f_t^{(n)}(X) + (t^2 + 1) \cdot r^{(n)}(X),$$

és

$$r^{(n+1)}(X) = (X + t) \cdot r^{(n)}(X) - f_t^{(n)}(X).$$

3.21. Tétel. *Tetszőleges $\beta \in \mathbb{C}$ és $n \geq 1$ esetén*

$$(X + \beta)^n \cdot f_t^{(n)}\left(\frac{\beta X - 1}{X + \beta}\right) = f_t^{(n)}(\beta) \cdot f_t^{(n)}(X) - (t^2 + 1) \cdot r^{(n)}(\beta) \cdot r^{(n)}(X).$$

3.22. Lemma. *Minden $n \geq 1$ esetén*

$$f_t^{(n)}(X) = \frac{(X + i)^n + (X - i)^n}{2} + t \cdot r^{(n)}(X),$$

és

$$r^{(n)}(X) = \frac{i}{2}\left((X + i)^n - (X - i)^n\right).$$

3.23. Következmény. *Minden $n \geq 2$ esetén az $r^{(n)}(X)$ összes gyöke*

$$\frac{i + i \cdot \varepsilon_n}{1 - \varepsilon_n},$$

alakú, ahol $\varepsilon_n \neq 1$ egy n-edik egységgyök. Továbbá $f_t^{(n)}(X)$-nek és $r^{(n)}(X)$-nek nincs közös gyöke.

3.24. Tétel. *Legyen $n \geq 2$ egész szám. Ekkor ha α az $f_t^{(n)}(X)$, β pedig az $r^{(n)}(X)$ polinom gyöke, akkor*

$$\frac{\beta\alpha - 1}{\alpha + \beta}$$

szintén gyöke $f_t^{(n)}(X)$-nek.

Adott $n \geq 2$ esetén vizsgáljuk meg a tételben szereplő

$$\sigma(z) = \frac{\beta z - 1}{z + \beta}$$

Möbius transzformációt, ahol β az $r^{(n)}(X)$ gyöke. A transzformációhoz tartozó mátrix

$$M = \begin{pmatrix} \beta & -1 \\ 1 & \beta \end{pmatrix}.$$

M sajátértékei $\lambda = \beta + i$ és $\mu = \beta - i$, továbbá

$$M^k = \begin{pmatrix} \dfrac{\lambda^k + \mu^k}{2} & \dfrac{i(\lambda^k - \mu^k)}{2} \\ -\dfrac{i(\lambda^k - \mu^k)}{2} & \dfrac{\lambda^k + \mu^k}{2} \end{pmatrix}.$$

Ennek alapján, ha $\sigma^k(\alpha) = \alpha$ teljesül valamilyen $\alpha \in \mathbb{C}$ és $k \in \mathbb{N}$ esetén, akkor

$$\frac{\left(\frac{\lambda^k+\mu^k}{2}\right) \cdot \alpha + \frac{i(\lambda^k-\mu^k)}{2}}{-\frac{i(\lambda^k-\mu^k)}{2} \cdot \alpha + \frac{\lambda^k+\mu^k}{2}} = \alpha,$$

azaz átrendezve

$$-\frac{i(\lambda^k - \mu^k)}{2} \cdot (\alpha^2 + 1) = 0.$$

Tehát ha α nem negyedik egységgyök, akkor ez pontosan akkor teljesülhet, ha

$$-\frac{i((X+i)^k - (X-i)^k)}{2} = 0,$$

ami azt jelenti, hogy β gyöke $r^{(k)}(X)$-nek. Így, mivel $r^{(n)}(X)$ gyökei

$$\frac{i + i \cdot \varepsilon_n}{1 - \varepsilon_n}$$

alakúak, ahol ε_n n-edik egységgyök, ezért ha φ_n primitív n-edik egységgyök, és

$$\beta = \frac{i + i \cdot \varphi_n}{1 - \varphi_n},$$

akkor a fenti σ Möbius transzformáció rendje pontosan n.

3.25. Tétel. *Legyen $n \geq 2$ természetes szám,*

$$\beta = \frac{i + i \cdot \varphi_n}{1 - \varphi_n},$$

ahol ε_n primitív n-edik egységgyök. Legyen α az $f_t^{(n)}(X)$ gyöke, ekkor az $f_t^{(n)}(X)$ polinom felbontási teste $\mathbb{Q}(\alpha, \beta)$, ami ciklikus bővítése $\mathbb{Q}(\beta)$-nak. Speciálisan, ha $t \in \mathbb{Q}$ olyan paraméter, hogy az $f_t^{(n)}(X)$ polinom irreducibilis, akkor $f_t^{(n)}(X)$ felbontási teste ciklikus n-edfokú bővítése $\mathbb{Q}(\beta)$-nak.

3.26. Állítás. *Ha $n \geq 2$, akkor $f_t^{(n)}(X)$ diszkriminánsa*

$$D_{f_t^{(n)}} = 2^{(n-1)(n-2)} \cdot n^n \cdot (t^2 + 1)^{n-1}.$$

3.27. Lemma. *Ha $p \neq 2$ olyan prím, amelyre $v_p(t^2+1) = 1$, és $s \in \mathbb{Z}$ olyan, hogy $v_p(s - t) = 1$, akkor $v_p\left(f_t^{(n)}(s)\right) = 1$ teljesül minden $n \geq 1$ esetén.*

3.28. Tétel. *Ha $p \neq 2$ olyan prím, amelyre $v_p(t^2 + 1) = 1$, akkor $f_t^{(n)}(X)$ irreducibilis. Továbbá, ha α az $f_t^{(n)}(X)$ gyöke, ahol a t paraméterre a fentieknek túl még az is teljesül, hogy az $f_t^{(n)}(X)$ polinom egész együtthatós, akkor a $\mathbb{Q}(\alpha)$ testben az α indexe nem osztható p-vel, vagyis $v_p(I(\alpha)) = 0$.*

Innentől kezdve legyen t olyan racionális paraméter, amellyel az $f_t^{(n)}(X)$ polinom egész együtthatós. Ez gyakorlatban azt jelenti, hogy

$$t = \frac{m}{2^{v_2(n)}},$$

ahol $m \in \mathbb{Z}$. A továbbiakban $f_t^{(n)}(X)$ helyett az $f_m^{(n)}(X)$ jelölést fogjuk használni, ami a fenti helyettesítésre utal. Itt megjegyezzük, hogy $n = 4$ esetén $f_m^{(n)}(X)$ megegyezik a legegyszerűbb negyedfokú polinomokkal, így ez a megközelítés valóban azok általánosításának tekinthető.

Az új paraméterezéssel, a polinom diszkriminánsára vonatkozó eredményünk a következőképpen módosul,

$$D_{f_m^{(n)}} = 2^{(n-1)(n-2)} \cdot n^n \cdot \left(\left(\frac{m}{2^{v_2(n)}}\right)^2 + 1\right)^{n-1}.$$

Ha α az $f_m^{(n)}(X)$ gyöke, $p \neq 2$ prím, és $m \in \mathbb{Z}$ olyan egész szám, amelyre

$$v_p\left(\left(\frac{m}{2^{v_2(n)}}\right)^2 + 1\right) = 1$$

teljesül, akkor $v_p(I(\alpha)) = 0$.

Az állításaink egyszerűbb megfogalmazása érdekében azt mondjuk, hogy $m \in \mathbb{Z}$ *megfelelő* paraméter, ha tetszőleges $p \neq 2$ esetén teljesül, hogy

$$v_p\left(\left(\frac{m}{2^{v_2(n)}}\right)^2 + 1\right) \leq 1.$$

Itt is megjegyezzük, hogy a $t^2+1 \in \mathbb{Q}[t]$ polinom irreducibilitása miatt T. Nagell [54] eredményeiből ebben az esetben is következik, hogy végtelen sok megfelelő m paraméter létezik.

3.29. Tétel. *Legyen $m \in \mathbb{Z}$ megfelelő paraméter, és α az $f_m^{(n)}(X)$ gyöke. Ekkor*

$$I(\alpha)^2 \;\Big|\; 2^{(n-1)^2} \cdot n^n.$$

3.30. Következmény. *Legyen $m \in \mathbb{Z}$ megfelelő paraméter, és α az $f_m^{(n)}(X)$ gyöke. Ekkor a $K = \mathbb{Q}(\alpha)$ testek egész bázisa periodikusan ismétlődik modulo n_0, ahol n_0 a legnagyobb olyan egész szám, amelyre teljesül, hogy*

$$n_0^2 \;\Big|\; \left(2^{(n-1)^2} \cdot n^n\right)^n.$$

3.31. Állítás. *Legyen $m \in \mathbb{Z}$ megfelelő paraméter, és α az $f_m^{(n)}(X)$ gyöke. Ekkor az $(1, \alpha, \ldots, \alpha^{n-1})$ bázishoz tartozó duális bázis meghatározásával és a*

$$v_2\left(\left(\frac{m}{2^{v_2(n)}}\right)^2 + 1\right) \leq 1.$$

becslés alkalmazásával, $n = 2, 3, \ldots, 12$ esetén azt kapjuk, hogy $C_n \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha]$, ahol

n	2	3	4	5	6	7	8	9	10	11	12
C_n	4	$2^2 \cdot 3$	$2^4 \cdot 4$	$2^5 \cdot 5$	$2^8 \cdot 6$	$2^9 \cdot 7$	$2^{11} \cdot 8$	$2^{12} \cdot 9$	$2^{16} \cdot 10$	$2^{17} \cdot 11$	$2^{19} \cdot 12$

.

Ezek közül $n = 2, 3, 4, 5, 6, 8, 9$ és 12 esetén határoztuk meg a legkisebb periódushosszt.

3.32. Következmény. *Legyen $m \in \mathbb{Z}$ megfelelő paraméter, és α az $f_m^{(n)}(X)$ gyöke. Ekkor $n = 2, 3, 4, 5, 6, 8, 9, 12$ esetén a $K = \mathbb{Q}(\alpha)$ testek egész bázisa periodikusan ismétlődik modulo n_0, ahol*

n	2	3	4	5	6	8	9	12
n_0	4	18	8	100	72	16	1728	4608

.

Speciálisan $n = 4$ esetén a legegyszerűbb negyedfokú polinomok

$$f_m^{(4)} = X^4 - mX^3 - 6X^2 + mX + 1$$

gyökei által generált testek egész bázisa periodikusan ismétlődik modulo 8, ami összhangban van J. H. Lee [49] eredményeivel.

3.3. Kompozitum testek egész bázisai

Ebben a fejezetben a korábban felmerülő nevezetes számtestcsaládok kompozíciójaként kapott számtestekben vizsgáljuk az egész bázisokat. Meg fogjuk mutatni, hogy megfelelő feltételek mellett a résztestek periodikus egész bázis tulajdonsága bizonyos értelemben öröklődik a kompozit testre is. A fejezet végén található konkrét példákhoz kapcsolódó eredmények a [29] cikkben jelentek meg.

Az elv ugyanaz lesz, mint amit a 3.6 Lemma bizonyításában használunk. Legyen $K = L \cdot M$ az $L = \mathbb{Q}(\alpha)$ és az $M = \mathbb{Q}(\beta)$ számtestek kompozituma, és tegyük fel, hogy $L \cap M = \mathbb{Q}$. Legyen továbbá $(\psi_1, \psi_2, \ldots, \psi_{n_1})$ az L, $(\omega_1, \omega_2, \ldots, \omega_{n_2})$ pedig az M egy egész bázisa. A már korábban is használt összefüggés alapján

$$D_L^{[K:L]} \mid D_K \qquad \text{és} \qquad D_M^{[K:M]} \mid D_K$$

teljesül, azaz

$$\operatorname{lkkt}\left(D_L^{[K:L]}, D_M^{[K:M]}\right) \mid D_K.$$

Másfelől, a $(\psi_1, \psi_2, \ldots, \psi_{n_1})$ és $(\omega_1, \omega_2, \ldots, \omega_{n_2})$ egész bázisok kompozíciójaként kapott

$$\begin{matrix} (\psi_1\omega_1, & \psi_2\omega_1, & \ldots, & \psi_{n_1}\omega_1, \\ \psi_1\omega_2, & \psi_2\omega_2, & \ldots, & \psi_{n_1}\omega_2, \\ & & \vdots & \\ \psi_1\omega_{n_2}, & \psi_2\omega_{n_2}, & \ldots, & \psi_{n_1}\omega_{n_2}) \end{matrix}$$

algebrai egész számok $L \cap M = \mathbb{Q}$ miatt bázist alkotnak K-ban $\mathbb{Q}$-felett, és ennek a bázisnak a diszkriminánsa $D_L^{[K:L]} \cdot D_M^{[K:M]}$. Mivel a test diszkriminánsa osztja a test tetszőleges algebrai egészekből álló bázisának a diszkriminánsát, ezért az előzővel együtt azt kapjuk, hogy

$$\operatorname{lkkt}\left(D_L^{[K:L]}, D_M^{[K:M]}\right) \mid D_K \mid D_L^{[K:L]} \cdot D_M^{[K:M]}.$$

Ha tehát sikerül olyan feltételeket találnunk, amelyek esetén a

$$\frac{D_L^{[K:L]} \cdot D_M^{[K:M]}}{\operatorname{lkkt}\left(D_L^{[K:L]}, D_M^{[K:M]}\right)} = \operatorname{lnko}\left(D_L^{[K:L]}, D_M^{[K:M]}\right)$$

hányados a paramétereinktől független szám, akkor K egy egész bázisát véges sok lépésben meg tudjuk határozni a fenti kompozit bázis 2.1.1 Fejezetben részletezett redukciójával és a 2.4 Állítás egy megfelelő általánosításának segítségével.

Tekintsünk egy egyszerű konkrét példát. Legyen α az $X^2 - m_1$, és β az $X^3 - m_2$ gyöke, ahol m_1 és m_2 négyzetmentes egészek, melyek legnagyobb közös osztója osztja a 6-ot. Legyen továbbá $L = \mathbb{Q}(\alpha)$, $M = \mathbb{Q}(\beta)$ és $K = L \cdot M$. Ekkor a 3.1 Tétel szerint L egész bázisa periodikusan ismétlődik modulo 4, M egész bázisa

pedig modulo 9. Nézzük először azt az esetet, amikor $m_1 \equiv 1 \pmod 4$ és $m_2 \equiv 1 \pmod 9$. Ekkor az L test α-hoz tartozó Hermite normál alakú egész bázisa

$$\left(1, \frac{1+\alpha}{2}\right),$$

az M test β-hoz tartozó Hermite normál alakú egész bázisa pedig

$$\left(1, \beta, \frac{1+\beta+\beta^2}{3}\right).$$

Ez alapján a $(\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6)$ kompozit bázis, amiből kiindulunk az alábbi,

$$\left(1, \frac{1+\alpha}{2}, \beta, \frac{(1+\alpha)\beta}{2}, \frac{1+\beta+\beta^2}{3}, \frac{(1+\alpha)(1+\beta+\beta^2)}{6}\right).$$

Mivel $D_L = m_1$, és $D_M = 3m_2^2$, ezért

$$\mathrm{lkkt}(m_1^3, 9 \cdot m_2^4) \mid D_K \mid 9 \cdot m_1^3 \cdot m_2^4.$$

Két lehetőséget különböztetünk meg, $3 \mid m_1$ vagy $3 \nmid m_1$. Az első esetben $\mathrm{lkkt}(m_1^3, 9 \cdot m_2^4) = m_1^3 \cdot m_2^4$, a másodikban pedig $\mathrm{lkkt}(m_1^3, 9 \cdot m_2^4) = 9 \cdot m_1^3 \cdot m_2^4$. Ez azt jelenti, hogy a második esetben a fenti bázis valójában egész bázis K-ban, az első esetben pedig az általuk generált modulus indexe a $\mathbb{Z}_K^+$ modulusban osztja 9-et. Ekkor a 2.1.1 Fejezetben leírt algoritmussal tudunk meghatározni egy egész bázist, és mivel a kiindulási bázis által generált modulus indexe a 9 osztója, ezért csak a 3 prímmel kell elvégezni a vizsgálatot, és azt is legfeljebb 1-szer, hiszen egy csere már 9-ed részére csökkenti a diszkrimináns. Legyen tehát $m_1 \equiv 1 \pmod 4$, $m_1 \equiv 0 \pmod 3$, azaz $m_1 = 12l_1 + 9$ valamilyen $l_1 \in \mathbb{Z}$-vel, és legyen $m_2 = 9l_2 + 1$, ahol $l_2 \in \mathbb{Z}$. Legyenek $0 \leq \lambda_i \leq 2$, $(i = 1, \ldots, 6)$ tetszőleges egészek, és tekintsük a

$$\delta = \frac{\lambda_1\gamma_1 + \lambda_2\gamma_2 + \lambda_3\gamma_3 + \lambda_4\gamma_4 + \lambda_5\gamma_5 + \lambda_6\gamma_6}{3}$$

algebrai számot. A 2.4 Állítás bizonyításával analóg módon látható, hogy a 3δ algebrai egész definiáló polinomja

$$X^6 + P_5(l_1, l_2) \cdot X^5 + \ldots + P_1(l_1, l_2) \cdot X + P_0(l_1, l_2)$$

alakú, ahol $P_i \in \mathbb{Z}[X, Y]$, $(i = 0, \ldots, 5)$. Most ahelyett, hogy minden $l_1 = 0, \ldots, 3^6 - 1$ és $l_2 = 0, \ldots, 3^6 - 1$ maradékosztályra végignéznék, hogy mikor lesz $3^i \cdot P_i(l_1, l_2)$ osztható 3^6-al, inkább szimultán megoldjuk a

$$\{3^5 \cdot P_5 \equiv 0;\ 3^4 \cdot P_4 \equiv 0;\ 3^3 \cdot P_3 \equiv 0;\ 3^2 \cdot P_2 \equiv 0;\ 3 \cdot P_1 \equiv 0;\ P_0 \equiv 0\}$$

kongruenciákat modulo 3^6. Ez látszólag ugyanaz a procedúra, de a matematikai programcsomagok az utóbbit lényegesen gyorsabban kiszámolják, mint a 3^{12} darab behelyettesítést. Ezeket a számításokat elvégezve minden lehetséges $\lambda_1, \ldots, \lambda_6$ értékek esetén, azt tapasztaljuk, hogy

$$(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6) = (2, 2, 1, 1, 0, 0),$$

illetve

$$(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6) = (1, 1, 2, 2, 0, 0),$$

és tetszőleges l_1, l_2 esetén δ algebrai egész lesz. Ez egy érdekes jelenség, hogy minden l_1, l_2 esetén ugyanazokkal a λ_i értékekkel kapunk algebrai egészt, de a legtöbb esetben ugyanez fordul elő. A $(2, 2, 1, 1, 0, 0)$ értékeket választva, a kiindulási bázisban kicseréljük a γ_4 elemet a

$$\delta = \frac{2\gamma_1 + 2\gamma_2 + \gamma_3 + \gamma_4}{3} = \frac{2 + (\alpha + 1) + \beta + \frac{(1+\alpha)\cdot\beta}{2}}{3} = \frac{6 + 2\alpha + 3\beta + \alpha\beta}{3}$$

elemmel, és így olyan algebrai egészekből álló bázist kapunk, aminek a diszkriminánsa 9-ed része a kiindulási bázis diszkriminánsának, és így az alsó becslés miatt ez szükségképpen egész bázis. Tehát $m_1 \equiv 9 \pmod{12}$ és $m_2 \equiv 1 \pmod{9}$ esetén

$$\left(1, \frac{1+\alpha}{2}, \beta, \frac{6 + 2\alpha + 3\beta + \alpha\beta}{3}, \frac{1 + \beta + \beta^2}{3}, \frac{(1+\alpha)(1+\beta+\beta^2)}{6}\right)$$

egész bázis K-ban.

Ugyanezt elvégezve minden $m_1 \equiv 1, 2, 3 \pmod{4}$ és $m_2 \equiv 1, 2 \ldots, 8 \pmod{9}$ maradékosztályok esetén, azt kapjuk, hogy az egész bázis alakja csak m_1-nek a 12-es és m_2-nek a 18-as maradékától függ. Precízebben fogalmazva, $\mathbb{Z}_K$-nak az $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2)$-hez tartozó Hermite normál alakja csak m_1-nek a 12-es és m_2-nek a 18-as maradékától függ, vagyis a $K = \mathbb{Q}(\alpha, \beta)$ testek egész bázisai periodikusan ismétlődnek m_1-ben modulo 12 és m_2-ben modulo 18.

Nagyjából ugyanazt az elvet látjuk kirajzolódni, amit az egyparaméteres számtestek esetén, ugyanis a fenti érvelésben a 9 nem más, mint a két résztest egész bázisainak kompozíciója által generált modulus indexének felső becslése a $\mathbb{Z}_K$ modulusban. Az, hogy ebből következik egy periodikus egész bázis tulajdonság, a 2.4 Állításhoz hasonló összefüggésre utal.

3.33. Állítás. *Legyen $f_{m_1}(X) \in \mathbb{Z}[m_1][X]$ egy n_1-edfokú és $f_{m_2}(X) \in \mathbb{Z}[m_2][X]$ egy n_2-edfokú 1 főegyütthatós polinom, ahol $m_1, m_2 \in \mathbb{Z}$ egész paraméterek. Legyen α az $f_{m_1}(X)$, β pedig az $f_{m_2}(X)$ egy gyöke és legyen $L = \mathbb{Q}(\alpha)$, $M = \mathbb{Q}(\beta)$. Tegyük fel, hogy $L \cap M = \mathbb{Q}$, és legyen $K = LM = \mathbb{Q}(\alpha, \beta)$. Ha létezik olyan $C \in \mathbb{Z}$ szám, hogy*

$$C \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha, \beta]$$

teljesül minden $m_1, m_2 \in \mathbb{Z}$ esetén, akkor a K testek egész bázisa periodikusan ismétlődik mindkét paraméterben modulo $C^{n_1 \cdot n_2}$.

Bizonyítás. Az ötlet ugyanaz lesz, mint a 2.4 Állítás esetében. Legyen $n = n_1 \cdot n_2$, és jelöljük $(\gamma_1, \gamma_2, \ldots, \gamma_n)$-el az α és a β hatványai által generált

$$\begin{matrix} (1, & \alpha, & \ldots, & \alpha^{n_1-1}, \\ \beta, & \alpha\cdot\beta, & \ldots, & \alpha^{n_1-1}\cdot\beta, \\ & & \vdots & \\ \beta^{n_2-1}, & \alpha\cdot\beta^{n_2-1}, & \ldots, & \alpha^{n_1-1}\cdot\beta^{n_2-1}) \end{matrix}$$

kompozit bázist. Legyen

$$\delta_{m_1,m_2} = \frac{z_1\gamma_1 + z_2\gamma_2 + \ldots + z_n\gamma_n}{C},$$

ekkor léteznek olyan $P_i \in \mathbb{Z}[X,Y]$, $(i = 0,\ldots,n-1)$ polinomok, hogy $C \cdot \delta_{m_1,m_2}$ definiáló polinomja

$$X^n + P_{n-1}(m_1,m_2)\cdot X^{n-1} + \ldots + P_1(m_1,m_2)\cdot X + P_0(m_1,m_2).$$

Legyenek s_1, s_2, t_1, t_2 olyan egészek, hogy $C^n \mid s_1 - t_1$ és $C^n \mid s_2 - t_2$. Ekkor $P_i \in \mathbb{Z}[X,Y]$, miatt $C^n \mid P_i(s_1,s_2) - P_i(t_1,t_2)$ teljesül minden $i = 0,\ldots,n-1$ esetén. Ez azt jelenti, hogy δ_{s_1,s_2} pontosan akkor algebrai egész, ha δ_{t_1,t_2} is az. Így $(d_{s_1,s_2}, M_{s_1,s_2}) = (d_{t_1,t_2}, M_{t_1,t_2})$, vagyis a K egész bázisa periodikusan ismétlődik mindkét paraméterben modulo C^n. □

Ezt az állítást megfelelő feltételek mellett, könnyen tudjuk alkalmazni olyan kompozit számtesteknél, amiknek a résztestei az előző fejezetben szereplő számtestcsaládok közül valók. Ha C_L, C_M olyan egészek, hogy

$$C_L \cdot \mathbb{Z}_L \subset \mathbb{Z}[\alpha], \qquad \text{és} \qquad C_M \cdot \mathbb{Z}_M \subset \mathbb{Z}[\beta],$$

akkor az L és az M egész bázisainak kompozíciója által generált $\mathbb{Z}_{L,M}$ K-beli modulusra teljesül, hogy

$$C_L \cdot C_M \cdot \mathbb{Z}_{L,M} \subset \mathbb{Z}[\alpha,\beta].$$

Ez egészen egyszerűen onnan látszik, hogy a kompozit bázis elemei olyan γ algebrai egészek, amelyek $\delta\cdot\epsilon$ alakban írhatóak, ahol $\delta \in \mathbb{Z}_L$ és $\epsilon \in \mathbb{Z}_M$. Így $C_L\cdot\delta \in \mathbb{Z}[\alpha]$ és $C_M\cdot\epsilon \in \mathbb{Z}[\beta]$ miatt $C_L\cdot C_M\cdot\delta\cdot\epsilon \in \mathbb{Z}[\alpha,\beta]$. Mivel a $\mathbb{Z}_{L,M}$ egy $\mathbb{Z}$-bázisának diszkriminánsa $D_L^{[K:L]}\cdot D_M^{[K:M]}$ és

$$D_K \mid D_L^{[K:L]}\cdot D_M^{[K:M]},$$

ezért ha sikerülne megmutatni, hogy megfelelő feltételek mellett a

$$C_K^2 := (\mathbb{Z}_K^+ : \mathbb{Z}[\alpha,\beta]^+)^2 = \frac{D_L^{[K:L]}\cdot D_M^{[K:M]}}{D_K}$$

szám a paraméterektől függetlenül felülről becsülhető, akkor a

$$C_K \cdot \mathbb{Z}_K \subset \mathbb{Z}_{L,M}$$

összefüggésből

$$C_L \cdot C_M \cdot C_K \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha,\beta]$$

következne, tehát a 3.33 Állítás értelmében a K testek egész bázisai periodikusan ismétlődnének.

Mindhárom vizsgált számtestcsalád esetén láthattuk, hogy megfelelő feltételek mellett léteznek ilyen C_L és C_M egészek, így a feladatunk most már csak a

$$\frac{D_L^{[K:L]} \cdot D_M^{[K:M]}}{D_K}$$

hányados paraméterektől független felső becslése. Mivel

$$\text{lkkt}\left(D_L^{[K:L]}, D_M^{[K:M]}\right) \mid D_K \mid D_L^{[K:L]} \cdot D_M^{[K:M]},$$

ezért

$$\frac{D_L^{[K:L]} \cdot D_M^{[K:M]}}{D_K} \;\Big|\; \text{lnko}\left(D_L^{[K:L]}, D_M^{[K:M]}\right).$$

Továbbá $D_L \mid D(\alpha)$ és $D_M \mid D(\beta)$ miatt

$$\text{lnko}\left(D_L^{[K:L]}, D_M^{[K:M]}\right) \;\Big|\; \text{lnko}\left(D(\alpha)^{[K:L]}, D(\beta)^{[K:M]}\right).$$

Innentől kezdve tehát azon fogunk dolgozni, hogy olyan feltételeket szabjunk a paramétereinkre, amelyekkel

$$\text{lnko}\left(D(\alpha)^{[K:L]}, D(\beta)^{[K:M]}\right)$$

a paraméterektől függetlenül felülről becsülhető, ami pedig azzal ekvivalens, hogy

$$\text{lnko}\left(D(\alpha), D(\beta)\right)$$

a paraméterektől függetlenül felülről becsülhető.

Összefoglalásképpen a három polinomcsalád, a paraméterekre kirótt feltételek és a diszkriminánsaik a következőek.

I. Gyökbővítések.

$$f_m^{(n)}(X) = X^n - m,$$

ahol $m \neq 0, \pm 1$ négyzetmentes egész.

$$D_{f_m^{(n)}} = (-1)^{\frac{n(n-1)}{2}} \cdot n^n \cdot m^{n-1}$$

II. Legegyszerűbb harmadfokú polinomok általánosításai.

$$f_m^{(n)}(X) = \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot g(n-i),$$

ahol

$$g(i) := \begin{cases} 1, & \text{ha } i \equiv 0 \pmod 6, \\ -\frac{m}{3^{v_3(n)}}, & \text{ha } i \equiv 1 \pmod 6, \\ -\frac{m}{3^{v_3(n)}} - 1, & \text{ha } i \equiv 2 \pmod 6, \\ -1, & \text{ha } i \equiv 3 \pmod 6, \\ \frac{m}{3^{v_3(n)}}, & \text{ha } i \equiv 4 \pmod 6, \\ \frac{m}{3^{v_3(n)}} + 1, & \text{ha } i \equiv 5 \pmod 6, \end{cases}$$

és tetszőleges $p \neq 3$ prím esetén $v_p\left(m^2 + 3^{v_3(n)}m + 9^{v_3(n)}\right) \leq 1$.

$$D_{f_m^{(n)}} = 3^{\frac{(n-1)(n-2)}{2}} \cdot n^n \cdot \left(\left(\frac{m}{3^{v_3(n)}}\right)^2 + \frac{m}{3^{v_3(n)}} + 1\right)^{n-1}.$$

III. Legegyszerűbb negyedfokú polinomok általánosításai.

$$f_m^{(n)}(X) = \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot g(n-i),$$

ahol

$$g(i) := \begin{cases} 1, & \text{ha } i \equiv 0 \pmod 4, \\ -\frac{m}{2^{v_2(n)}}, & \text{ha } i \equiv 1 \pmod 4, \\ -1, & \text{ha } i \equiv 2 \pmod 4, \\ \frac{m}{2^{v_2(n)}}, & \text{ha } i \equiv 3 \pmod 4, \end{cases}$$

és tetszőleges $p \neq 2$ prím esetén $v_p\left(m^2 + 4^{v_2(n)}\right) \leq 1$.

$$D_{f_m^{(n)}} = 2^{(n-1)(n-2)} \cdot n^n \cdot \left(\left(\frac{m}{2^{v_2(n)}}\right)^2 + 1\right)^{n-1}.$$

A következő táblázatban összefoglalom, hogy a fenti három polinomcsalád által definiált számtestcsaládokból képzett kompozit testek paramétereire a korábbi feltételek mellett még mit követelünk meg, ahhoz, hogy

$$\text{lnko}\left(D(\alpha), D(\beta)\right)$$

a paraméterektől függetlenül felülről becsülhető legyen. Legyen az L test foka n_1, a paramétere m_1, az M test foka n_2, a paramétere pedig m_2, és legyenek

$$s(m,n) = m^2 + 3^{v_3(n)} \cdot m + 9^{v_3(n)},$$

$$t(m,n) = m^2 + 4^{v_2(n)}.$$

Ekkor a paraméterekre vonatkozó feltételek a következők.

L	M	Feltétel
$I.$	$I.$	$\text{lnko}(m_1, m_2) \mid n_1 \cdot n_2$
$I.$	$II.$	$\text{lnko}\,(m_1, s(m_2, n_2)) \mid n_1 \cdot n_2$
$I.$	$III.$	$\text{lnko}\,(m_1, t(m_2, n_2)) \mid n_1 \cdot n_2$
$II.$	$II.$	$\text{lnko}\,(s(m_1, n_1), s(m_2, n_2)) \mid n_1 \cdot n_2$
$II.$	$III.$	$\text{lnko}\,(s(m_1, n_1), t(m_2, n_2)) \mid n_1 \cdot n_2$
$III.$	$III.$	$\text{lnko}\,(t(m_1, n_1), t(m_2, n_2)) \mid n_1 \cdot n_2$

Ezen megkötések esetén egyszerű számolással adódik a paraméterektől független felső becslés $\text{lnko}\,(D(\alpha), D(\beta))$-ra.

Tekintsük például a harmadik esetet, ahol $L = \mathbb{Q}(\alpha)$ gyökbővítés, $M = \mathbb{Q}(\beta)$ pedig egy legegyszerűbb negyedfokú testek általánosításával kapott számtest. Ekkor

$$D(\alpha) = (-1)^{\frac{n_1(n_1-1)}{2}} \cdot n_1^{n_1} \cdot m_1^{n_1-1},$$

$$D(\beta) = 2^{(n_2-1)(n_2-2)} \cdot n_2^{n_2} \cdot \left(\left(\frac{m_2}{2^{v_2(n_2)}} \right)^2 + 1 \right)^{n_2-1}.$$

Tudjuk, hogy m_1 négyzetmentes és $m_2^2 + 4^{v_2(n_2)}$ a 2 prímtényezőtől eltekintve négyzetmentes. Így ha k_1 az n_1, k_2 pedig az n_2 prímtényezőinek szorzata, valamint $k_3 = \text{lnko}(m_1, t(m_2, n_2))$, akkor azok a prímek, amik osztják m_1-et és $D(\beta)$-t is, osztják $k_2 \cdot k_3$-at. Hasonlóan, a 2-től eltekintve, azok a prímek, melyek osztják $m_2^2 + 4^{v_2(n)}$-t és $D(\alpha)$-t is, osztják $k_1 \cdot k_3$-at. Továbbá

$$v_2(m_2^2 + 4^{v_2(n)}) = 2 \cdot v_2(n) + v_2\left(\frac{m_2^2}{4^{v_2(n)}} + 1 \right) \leq 2 \cdot v_2(n) + 1,$$

így $\text{lnko}\,(D(\alpha), D(\beta))$ osztja a

$$\text{lnko}\left(n_1^{n_1} \cdot (k_2 \cdot k_3)^{n_1-1}, 2^{(n_2-1)(n_2-2)} \cdot n_2^{n_2} \cdot \left(2^{2v_2(n)+1} \cdot k_1 \cdot k_3 \right)^{n_2-1} \right)$$

kifejezést. Ez pedig $k_3 \mid 2 \cdot k_1 \cdot k_2$ miatt osztja a

$$\text{lnko}\left(n_1^{n_1} \cdot (k_2 \cdot k_1)^{n_1-1}, 2^{(n_2-1)(n_2-2)} \cdot n_2^{n_2} \cdot \left(2^{2v_2(n)+2} \cdot k_1 \cdot k_2 \right)^{n_2-1} \right)$$

legnagyobb közös osztót, ami már független m_1, m_2-től.

Ugyanígy lehet a többi esetet is becsülni, amiből az alábbi következményt kapjuk.

3.34. Következmény. *A fenti táblázat feltételei mellett a $K = LM$ kompozit testek egész bázisai periodikusan ismétlődnek.*

A különböző esetekben

$$\operatorname{lnko}\left(D(\alpha)^{[K:L]}, D(\beta)^{[K:M]}\right)$$

értékének felső becsléseivel, és a 3.33 Állítás segítségével explicite megadható egy felső becslés a periódus hosszára is, de ezek a becslések messze nem optimálisak. Néhány kis fokszámú esetben azonban meg tudtuk határozni a legkisebb periódushosszt. A következőkben ezeket az eseteket foglalom össze.

A táblázat első oszlopában az $L = \mathbb{Q}(\alpha)$ testet, a második oszlopában pedig az $M = \mathbb{Q}(\beta)$ testet generáló elem definiáló polinomja található. A harmadik illetve negyedik oszlopban pedig a paraméterekhez tartozó periódushosszak, amelyek szerint a $K = \mathbb{Q}(\alpha, \beta)$ egész bázisai ismétlődni fognak.

L	M	m_1	m_2
$X^2 - m_1$	$X^3 - m_2X^2 - (m_2+3)X - 1$	4	1
$X^2 - m_1$	$X^3 - m_2$	12	18
$X^2 - m_1$	$X^4 - m_2X^3 - 6X^2 + m_2X + 1$	8	16
$X^2 - m_1$	$X^4 - m_2$	8	8
$X^2 + 3$	$X^6 - m_2$	$--$	36

Látható, hogy a másodfokú és a hatodfokú gyökbővítések kompozíciója esetén a másodfokú résztest fixen a hatodik egységgyököket tartalmazó test. Ennek az az oka, hogy mivel a kompozit test 12 fokú, így a bázis redukciója során minden lépésben 2^{12} vagy 3^{12} darab algebrai számról kell parametrikusan eldönteni, hogy algebrai egész-e, ami egy paraméter esetén még kivitelezhető, de két paraméter esetén már túl időigényes a számítás. Így csak egy konkrét esetet volt kapacitásunk vizsgálni, amihez az $m_1 = -3$ választás azért célszerű, mert ebben az esetben a kompozit bővítés $\mathbb{Q}$-nak normális bővítése, ami a monogenitás szempontjából majd különösen jól kezelhető lesz. A szintén normális $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{m_2})$ testek monogenitását M.-L. Chang [6] vizsgálta, a $\mathbb{Q}(i, \sqrt[4]{m_2})$ testekkel kapcsolatos eredményeink pedig a [27] cikkben jelentek meg, melyeket a [29] cikkben egészítettünk ki.

A legegyszerűbb és a kompozit számtestekben a megfelelő n_0 periódushosszak igazolásához n-edfokú számtest esetén, minden vizsgálandó p prímre $n_0 \cdot p^n$ darab számtest egy egész bázisát kellett meghatároznunk. 24 óra alatt átlagosan 10^6 ilyen számítást képes elvégezni a számítógép. Ez az oka annak, hogy a vizsgálatok során bizonyos eseteket kihagyunk. Például 12-ed fokú esetben a legegyszerűbb polinomok esetén, és a fenti normális kompozit bővítésnél is a nagyságrendileg 3^{12} számítást még elvégeztük, de például 7-ed fokú esetben a $p = 7$ prímmel a közel kétszer annyi, 7^7 darab vizsgálatot már nem. Ugyanezen ok miatt maradt ki a kompozit testeknél a másodfokú és ötödfokú testek kompozítuma is, hiszen ott már az 5 prímmel is $\sim 5^{10}$ darab számítást kellene elvégezni.

4. fejezet

Végtelen parametrikus számtestek monogenitása

Ebben a fejezetben a korábban vizsgált parametrikus számtestek, illetve azok kompozíciójával nyert testek monogenitását vizsgáljuk. A fejezet eredményei a [26], [27], [28] és [29] cikkekben jelentek meg.

Egy K n-edfokú algebrai számtestet monogénnek nevezünk, ha egészeinek a $\mathbb{Z}_K$ gyűrűje előáll a $\mathbb{Z}$ egyszerű gyűrűbővítéseként,

$$\mathbb{Z}_K = \mathbb{Z}[\alpha].$$

Értelemszerűen ekkor $I(\alpha) = 1$, és $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ egész bázis K-ban. Ha $(\omega_1 = 1, \omega_2, \ldots, \omega_n)$ egész bázis K-ban, és $\alpha = x_1 + x_2\omega_2 + \ldots \omega_n$ egy primitív algebrai egész K-ban, akkor

$$I(\alpha) = |I(x_2, x_3, \ldots, x_n)|,$$

ahol $I(X_2, \ldots, X_n) \in \mathbb{Z}[X_2, \ldots, X_n]$ az $(\omega_1, \omega_2, \ldots, \omega_n)$ egész bázishoz tartozó indexforma. Az 1 indexű elemek keresését tehát visszavezethetjük az

$$I(X_2, \ldots, X_n) = \pm 1$$

indexforma egyenlet megoldására.

A periodikus egész bázis tulajdonságnak köszönhetően, az indexformát fel tudjuk írni paraméteresen, és ez a felírás csak az egész bázis Hermite normál alakjától függ. Ebből adódóan, a periodikus esetben csak véges sok különböző paraméteres indexforma egyenletet kell vizsgálni. A paraméterezés miatt, kerülni fogjuk az indexforma egyenlet explicit megoldását. Ehelyett inkább arra törekszünk, hogy ha a testet generáló elem nem generál hatvány egész bázist, akkor belássuk, hogy az indexforma egyenletnek nincs megoldása.

Ehhez két módszert fogunk használni. Az első, hogy ha lehetséges, megmutatjuk, hogy valamilyen p prím estén az indexforma egyenletnek nincs megoldása

modulo p. Ez leginkább akkor fordul elő, ha a testindex nem 1, vagyis létezik olyan p prím, hogy tetszőleges algebrai egész indexe osztható p-vel, azaz az indexforma tetszőleges helyettesítés esetén p-vel osztható értéket ad, speciálisan nem lehet ± 1. Ebben az esetben mindhárom számtestcsaládnál csak véges sok prímet kell kipróbálnunk, hiszen mindegyiknél adtunk felső korlátot a testet generáló elem indexére.

Ez a megközelítés ekvivalens azzal, mint amit Dedekind [11] alkalmazott, amikor elsőként adott példát egy nem monogén testre. Az ő példája az

$$f(X) = X^3 - X^2 - 2X - 8$$

polinom egy gyöke által generált K számtest volt, a módszere pedig az, hogy meghatározta a $2 \cdot \mathbb{Z}_K$ prímideál faktorizációját

$$2\mathbb{Z}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3,$$

ahol a $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ különböző prímideálok maradékosztály-foka egyaránt 1. Ebből következően, ha lenne olyan $\alpha \in \mathbb{Z}_K$ algebrai egész, amelynek az indexe nem osztható 2-vel, akkor α definiáló polinomja modulo 2 nézve, három különböző elsőfokú polinom szorzata lenne. Azonban nincs 3 különböző elsőfokú polinom $\mathbb{F}_2[X]$-ben, így ellentmondást kapunk, azaz minden algebrai egész indexe osztható 2-vel.

Az indexforma felől megközelítve ez a következőképpen nézne ki. Legyen α az $X^3 - X^2 - 2X - 8$ egy gyöke, ekkor a $K = \mathbb{Q}(\alpha)$ egy egész bázisa

$$\left(1, \alpha, \frac{\alpha + \alpha^2}{2}\right),$$

az ehhez tartozó indexforma pedig

$$I(X_2, X_3) = 2X_2^3 + 5X_2^2X_3 + 3X_2X_3^2 - 2X_3^3.$$

Tekintve az indexformát modulo 2, az az alábbi alakban írható

$$I(X_2, X_3) \equiv X_2X_3(X_2 + X_3) \pmod 2.$$

Ez pedig tetszőleges $X_2 = 0, 1$, $X_3 = 0, 1$ helyettesítés esetén 0 maradékot ad 2-vel osztva, tehát az $I(X_2, X_3) = \pm 1$ indexforma egyenletnek nincs megoldása modulo 2, és így az egész számok körében sincs.

Dedekind általános eredménye azt mondja ki, hogy egy K algebrai számtestben a testindex pontosan akkor osztható egy p prímmel, ha létezik olyan f egész szám, hogy a $p \cdot \mathbb{Z}_K$ prímideál faktorizációjában az olyan prímideálok száma, melyeknek a maradékosztály-foka f, nagyobb, mint a különböző f-edfokú irreducibilis polinomok száma az $\mathbb{F}_p[X]$ polinomgyűrűben. A fenti érvelés alapján ez pontosan akkor teljesül, ha az indexforma tetszőleges helyettesítés esetén p-vel osztható értéket vesz fel, ami speciális esete annak, hogy az indexforma egyenletnek nincs megoldása modulo p.

A másik megközelítés az indexforma faktorai közötti kapcsolatra épül, és azokban az esetekben látszik hatékonynak, amikor K-nak van valódi részteste. A valódi résztest létezése maga után vonja, hogy az indexforma szorzattá alakítható $\mathbb{Z}[X_2,\dots,X_n]$-ben (ld. Gaál István [22], Chapter 7.3 és 7.5), de ez visszafelé nem feltétlenül igaz. Azokban az esetekben, amikor az indexforma reducibilis, de nincs valódi résztest, eddig még nem sikerült ténylegesen hatékony összefüggéseket találnunk a faktorok között.

A következőkben egy egyszerű példán bemutatom, hogy hogyan működik ez a módszer. Legyen α az X^4-m egy gyöke, ahol $m\neq 0,1$ négyzetmentes egész. Legyen $K=\mathbb{Q}(\alpha)$, és tekintsük az $(1,\alpha,\alpha^2,\alpha^3)$ bázishoz tartozó $L(\underline{X})$ lineáris forma diszkriminánsát,

$$D_{K/\mathbb{Q}}(L(\underline{X}))=\prod_{1\le i<j\le 4}\left(L^{(i)}(\underline{X})-L^{(i)}(\underline{X})\right)^2.$$

Ekkor

$$\beta_k^{(i,j)}=\frac{(\alpha^{(i)})^k-(\alpha^{(j)})^k}{\alpha^{(i)}-\alpha^{(j)}}$$

jelöléssel, az $(1,\alpha,\alpha^2,\alpha^3)$ bázishoz tartozó indexforma

$$I(X_2,X_3,X_4)=\prod_{1\le i<j\le 4}\left(X_2+X_3\beta_2^{(i,j)}+X_4\beta_3^{(i,j)}\right)=$$

$$=m^3X_4^6+m^2X_2^2X_4^4-8m^2X_2X_3^2X_4^3+4m^2X_3^4X_4^2-mX_2^4X_4^2+8mX_2^3X_3^2X_4-4mX_2^2X_3^4-X_2^6.$$

Mivel $\mathbb{Q}(\alpha^2)$ a K valódi részteste, ezért a fenti indexforma szorzattá alakítható $\mathbb{Z}[X_2,X_3,X_4]$-ben. Valóban, ha G az X^4-m Galois csoportja, akkor G hatása szerint az

$$\{(\alpha^{(i)},\alpha^{(j)}),1\le i\neq j\le 4\}$$

halmaz 2 orbitra esik szét. Legyen σ a G egy 4-edrendű eleme, és legyenek

$$\alpha^{(1)}=\alpha,\ \ \alpha^{(2)}=\sigma(\alpha),\ \ \alpha^{(3)}=\sigma^2(\alpha),\ \ \alpha^{(4)}=\sigma^3(\alpha).$$

Ekkor a 2 orbit

$$\begin{aligned}S_1 &= \{(\alpha^{(1)},\alpha^{(3)}),(\alpha^{(2)},\alpha^{(4)}),(\alpha^{(3)},\alpha^{(1)}),(\alpha^{(4)},\alpha^{(2)})\},\\ S_2 &= \{(\alpha^{(1)},\alpha^{(2)}),(\alpha^{(2)},\alpha^{(3)}),(\alpha^{(3)},\alpha^{(4)}),(\alpha^{(4)},\alpha^{(1)}),\\ &\quad (\alpha^{(2)},\alpha^{(1)}),(\alpha^{(3)},\alpha^{(2)}),(\alpha^{(4)},\alpha^{(3)}),(\alpha^{(1)},\alpha^{(4)})\}.\end{aligned}$$

Ezek alapján

$$\begin{aligned}J_1 &= \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_1}\left(X_2+X_3\beta_2^{(i,j)}+X_4\beta_3^{(i,j)}\right)=\left(mX_4^2-X_2^2\right)^2,\\ J_2 &= \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_2}\left(X_2+X_3\beta_2^{(i,j)}+X_4\beta_3^{(i,j)}\right)=\\ &= \left(m^2X_4^4+2mX_2^2X_4^2-8mX_2X_3^2X_4+4mX_3^4+X_2^4\right)^2\end{aligned}$$

az $I(X_2, X_3, X_4)^2$ két faktora. Valóban, könnyen ellenőrizhetjük, hogy

$$F_1 = mX_4^2 - X_2^2$$

és

$$F_2 = m^2X_4^4 + 2mX_2^2X_4^2 - 8mX_2X_3^2X_4 + 4mX_3^4 + X_2^4$$

választással

$$I(X_2, X_3, X_4) = F_1 \cdot F_2.$$

Ezek után könnyen észrevehetjük, hogy $F_2 - F_1^2$-ből kiemelhető m, azaz egészen pontosan

$$F_2 - F_1^2 = 4m(X_2X_4 - X_3^2)^2.$$

Ez azt jelenti, hogy ha $\gamma = x_1 + x_2\alpha + x_3\alpha^2 + x_4\alpha^3$ hatványai bázisát alkotják az $(1, \alpha, \alpha^2, \alpha^3)$ által generált modulusnak, akkor $I(x_2, x_3, x_4) = \pm 1$, amiből $F_1 = \pm 1$ és $F_2 = \pm 1$. Így a fenti oszthatóságból az következik, hogy $4m$ osztja $(\pm 1) - (\pm 1)^2$-t. Ez első ránézésre nem egy túl nagy megszorítás m-re, hiszen $F_2 = 1$ esetén a fenti kifejezés értéke 0. Ebben az esetben nem is várhatnánk mást, mivel $x_2 = 1, x_3 = 0, x_4 = 0$ választással a $\gamma = \alpha$ hatványai m-től függetlenül bázist alkotnak a fenti modulusban. Ha viszont m olyan paraméter, hogy $(1, \alpha, \alpha^2, \alpha^3)$ nem egész bázis K-ban, akkor F_1 és F_2 értéke már nem feltétlenül ± 1 lesz, és így már valódi megszorítást kaphatunk m értékére nézve. Legyen például $m \equiv 5 \pmod 8$, azaz $m = 8k + 5$ valamilyen $k \in \mathbb{Z}$-vel. Ekkor K egész bázisa

$$\left(1, \alpha, \frac{1+\alpha^2}{2}, \frac{\alpha+\alpha^2}{2}\right)$$

alakú, azaz, ha

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix},$$

akkor a fenti egész bázishoz tartózó indexforma

$$I(X_2, X_3, X_4) = \frac{1}{\det(M)} \prod_{1 \le i < j \le 4} \left(Y_2 + Y_3\beta_2^{(i,j)} + Y_4\beta_3^{(i,j)}\right),$$

ahol

$$\begin{pmatrix} X_1 & X_2 & X_3 & X_4 \end{pmatrix} \cdot M = \begin{pmatrix} Y_1 & Y_2 & Y_3 & Y_4 \end{pmatrix}.$$

Ezzel, és az $m = 8k + 5$ helyettesítéssel,

$$\begin{aligned} F_1 &= mY_4^2 - Y_2^2 = 2kX_4^2 - X_2^2 - X_2X_4 + X_4^2 \\ F_2 &= m^2Y_4^4 + 2mY_2^2Y_4^2 - 8mY_2Y_3^2Y_4 + 4mY_3^4 + Y_2^4 = \\ &= 4k^2X_4^4 + 6kX_4^4 + \frac{9}{4}X_4^4 + 4kX_4^2X_2^2 + 4kX_4^3X_2 + 4X_4^2X_2^2 + 3X_4^3X_2 + X_2^4 - \\ &\quad -8kX_3^2X_4X_2 - 4kX_3^2X_4^2 - 5X_3^2X_4X_2 - \frac{5}{2}X_3^2X_4^2 + 2kX_3^4 + \frac{5}{4}X_3^4 + 2X_2^3X_4. \end{aligned}$$

Ez alapján ebben az esetben, az indexforma egész együtthatós faktorizációja $f_1 = F_1$ és $f_2 = 4F_2$ választással.

$$I(X_2, X_3, X_4) = f_1 \cdot f_2.$$

Így ha most egy

$$\gamma = x_2 \cdot \alpha + x_3 \cdot \frac{1+\alpha^2}{2} + x_4 \cdot \frac{\alpha+\alpha^2}{2}$$

elem hatvány egész bázist generál $\mathbb{Z}_K$-ban, akkor $X_2 = x_2, X_3 = x_3$ és $X_4 = x_4$ helyettesítés esetén $f_1 = \pm 1$ és $f_2 = \pm 1$. Továbbá

$$F_2 - F_1^2 = 4m(Y_2Y_4 - Y_3^2)^2$$

miatt

$$f_2 - 4f_1^2 = 4F_2 - 4F_1^2 = 16m(Y_2Y_4 - Y_3^2)^2 = (8k+5)(2X_2X_4 - X_3^2 + X_4^2)^2.$$

Mivel $f_2 - 4f_1^2$ értéke -3 vagy -5, ezért ebből adódik, hogy $m = 8k+5$ osztja -3-at vagy -5-öt. Továbbá, mivel a fenti kifejezésben az $m = 8k+5$ mellett a másik tényező teljes négyzet, és ez szintén osztja -3-at vagy -5-öt, ezért annak az értéke csak 1 lehet. Így adódik, hogy a fenti egyenlőség csak $m = -3$ esetén teljesülhet. Ez azt jelenti, hogy $m \equiv 5 \pmod 8$ esetén $K = \mathbb{Q}(\sqrt[4]{m})$ csak akkor lehet monogén, ha $m = -3$. Végül pedig $K = \mathbb{Q}(\sqrt[4]{-3})$ esetén könnyű megtalálni egy megoldását az indexforma egyenletnek, pl $(x_2, x_3, x_4) = (1, 1, 0)$ választással

$$\gamma = \frac{1+2\alpha+\alpha^2}{2}$$

hatvány egész bázist generál K-ban.

Hasonló összefüggéseket kapunk a legtöbb esetben, amit ebben a fejezetben vizsgálunk. Láthatjuk, hogy ez a megközelítés akkor ad tényleges megszorítást a paraméterre nézve, ha F_1-be és F_2-be az új változókat helyettesítve, azoknak különböző lesz a nevezője. Ezeket a nevezőket az $\frac{1}{\det(M)}$ tényezővel pótoljuk, hogy egész együtthatós faktorizációt kapjunk, viszont az F_1 és F_2 között fennálló összefüggés az új f_1 és f_2 faktorokra már olyan együtthatókkal teljesül, amelyekkel a kifejezés értéke már nem lehet 0, és így az korlátozza m lehetséges értékeit. Mivel az új faktorok lényegében csak az M mátrixtól függnek, azaz az egész bázis α-hoz tartozó Hermite normál alakjától, ezért periodikus esetben könnyedén végig lehet vizsgálni az összes lehetőséget.

Azokban az esetekben, amelyekben egyik módszer sem vezet eredményre, csupán sejtéseket tudunk megfogalmazni. A következőben sorra veszem a részletesen vizsgált testeket, és a hozzájuk tartozó eredményeket.

4.1. Gyökbővítések monogenitása

Ebben az fejezetben az $n = 2, 3, 4, 5, 6, 7, 8$ és 9 fokú gyökbővítések monogenitásával kapcsolatos eredményeket részletezem, melyek részben a [26] cikkben jelentek meg.

Harmadfokú gyökbővítések

Legyen $m \neq 0, \pm 1$ négyzetmentes egész, α az $X^3 - m$ gyöke és $K = \mathbb{Q}(\alpha)$. Ekkor az indexforma egyenlet egy harmadfokú Thue egyenlet, amelynek bizonyos esetekben van megoldása, máskor pedig nincs. Az α-hoz tartozó Hermite normál alakú egész bázis alakja csak m-nek a 9-es maradékától függ, és 3 különböző esetet eredményez.

1. Ha $r = 2, 3, 4, 5, 6$ vagy 7 és $m = r + 9k$ négyzetmentes, akkor

   $$(1, \alpha, \alpha^2)$$

   egész bázis K-ban és a hozzá tartozó indexforma

   $$I(X_2, X_3) = X_2^3 - mX_3^3.$$

   Ekkor K természetesen monogén, hiszen α hatvány egész bázist generál, vagyis $(1, 0)$ megoldása az indexforma egyenletnek.

2. Ha $m = 1 + 9k$ négyzetmentes, akkor

   $$\left(1, \alpha, \frac{1 + \alpha + \alpha^2}{3}\right)$$

   egész bázis K-ban, a hozzá tartozó indexforma

   $$I(X_2, X_3) = 3 \cdot (Y_2^3 - mY_3^3),$$

   ahol

   $$\begin{pmatrix} Y_1 & Y_2 & Y_3 \end{pmatrix} = \begin{pmatrix} X_1 & X_2 & X_3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix},$$

   azaz

   $$I(X_2, X_3) = 3X_2^3 + 3X_2^2X_3 + X_2X_3^2 - kX_3^3 = \frac{(3X_2 + X_3)^3 - mX_3^3}{9}.$$

   Az indexforma egyenletnek végtelen sok négyzetmentes $m = 1+9k$ paraméter esetén van megoldása. Tekintsük például azokat a m számokat, amelyek előállnak a $P(X) = 27X^3+27X^2+9X+10$ polinom egész helyeken vett helyettesítési értékeként. Ilyen négyzetmentes m számokból Erdős Pál [15] eredménye alapján végtelen sok van, továbbá ezek nyilvánvalóan $1 + 9k$ alakúak, és ha $m = P(x)$, akkor $(x, 1)$ megoldása az indexforma egyenletnek. Mindemellett

azonban azt sejtjük, hogy végtelen sok olyan négyzetmentes $m = 1+9k$ alakú paraméter is létezik, amellyel a K test nem monogén. Elhagyva a négyzetmentességre vonatkozó feltételt, M. Hall [38] például megmutatta, hogy a harmadfokú gyökbővítésekben a minimális index tetszőlegesen nagy lehet.

3. Ha $m = 8 + 9k$ négyzetmentes, akkor

$$\left(1, \alpha, \frac{1+\alpha+\alpha^2}{3}\right)$$

egész bázis K-ban, a hozzá tartozó indexforma (az előzőhöz hasonlóan könnyedén megkaphatjuk az első esetből változó helyettesítéssel)

$$I(X_2, X_3) = 3X_2^3 + 6X_2^2X_3 + 4X_2X_3^2 - kX_3^3 = \frac{(3X_2 + 2X_3)^3 - mX_3^3}{9}.$$

Az előző esethez hasonlóan, most is lehet konstruálni végtelen sok paramétert, amellyel a kompozit test monogén. Ezek például a $P(X) = 27X^3 + 54X^2 + 36X + 17$ polinom egész helyeken felvett négyzetmentes értékei. Továbbá ismét csak sejtjük, hogy végtelen sok olyan paraméter van, amellyel a kompozit test nem monogén.

Az eset egyszerűsége egyben a nehézsége is. Nincs résztest, az indexforma nem faktorizálódik, és a fokszám is túl alacsony ahhoz, hogy a $3\mathbb{Z}_K$ faktorizációjával ellentmondást kapjunk, azaz, ahogy azt konkrétan láthatjuk is, az indexformák mindig megoldhatóak modulo 3.

Negyedfokú gyökbővítések

Legyen $m \neq 0, 1$ négyzetmentes egész, α az $X^4 - m$ gyöke és $K = \mathbb{Q}(\alpha)$. Az α-hoz tartozó Hermite normál alakú egész bázis alakja csak m-nek a 8-as maradékától függ, és 3 különböző esetet eredményez.

1. Ha $r = 2, 3, 6, 7$ és $m = r + 8k$ négyzetmentes, akkor

$$(1, \alpha, \alpha^2, \alpha^3)$$

egész bázis K-ban, a hozzá tartozó indexforma

$$I(X_2, X_3, X_4) = \left(mX_4^2 - X_2^2\right) \cdot \left(m^2X_4^4 + 2mX_2^2X_4^2 - 8mX_2X_3^2X_4 + 4mX_3^4 + X_2^4\right).$$

Ekkor K természetesen monogén, hiszen α hatvány egész bázist generál, vagyis $(1, 0, 0)$ megoldása az indexforma egyenletnek.

2. Ha $m = 5 + 8k$ négyzetmentes, akkor

$$\left(1, \alpha, \frac{1+\alpha^2}{2}, \frac{\alpha+\alpha^3}{2}\right)$$

egész bázis K-ban, a hozzá tartozó indexformát a korábbi érvelésben már részleteztem. Az indexforma két faktorra bomlik,

$$I(X_2, X_3, X_4) = f_1 \cdot f_2,$$

amelyekre teljesül, hogy $f_2 - 4f_1^2$-ből kiemelhető m. Így ha K monogén, akkor $m \mid -3$ vagy $m \mid -5$. Ez $m = 5 + 8k$ miatt csak $m = -3$ vagy $m = 5$ esetén teljesülhet, melyek közül az utóbbi esetet a faktorok közötti összefüggésekből előjelvizsgálattal ki lehet zárni. Végül a $K = \mathbb{Q}(\sqrt[4]{-3})$ test valóban monogén, például $(1, 1, 0)$ megoldása az indexforma egyenletnek.

3. Ha $m = 1 + 8k$ négyzetmentes, akkor

$$\left(1, \alpha, \frac{1+\alpha^2}{2}, \frac{1+\alpha+\alpha^2+\alpha^3}{4}\right)$$

egész bázis K-ban, a hozzá tartozó indexforma pedig az előzőből értelemszerű helyettesítéssel könnyedén meghatározható. Érdekessége ennek az esetnek, hogy a vizsgálataink során tovább bontható két lényegesen különböző eredményeket mutató osztályra. Ha $m = 1 + 16k$, akkor az indexforma egyenletnek nincs megoldása modulo 2, vagyis a testindex osztható 2-vel. Ha pedig $m = 9 + 16k$, akkor Arnóczki Tímea és Nyul Gábor [1] megmutatták, hogy ha igaz az ABC-sejtés, akkor végtelen sok olyan négyzetmentes paraméter létezik, amellyel a K test monogén. Ebből következően nem is kaphattunk volna az indexforma faktorai között fennálló összefüggésekből az előző esthez hasonló megszorítást a paraméterekre vonatkozóan.

Összefoglalva, ha $m = r + 16k$ négyzetmentes, akkor a $K = \mathbb{Q}(\sqrt[4]{m})$ test $r = 2, 3, 6, 7, 10, 11, 14, 15$ esetén monogén, $r = 1, 5, 13$ esetén csak akkor monogén, ha $m = -3$, és végül $r = 9$ esetén, ha igaz az ABC-sejtés, akkor Arnóczki Tímea és Nyul Gábor [1] eredményei alapján, ilyen paraméterekkel végtelen sok monogén és végtelen sok nem monogén testet is kaphatunk.

Ötödfokú gyökbővítések

Az ötödfokú eset sokban hasonlít a harmadfokúra. Az indexforma irreducibilis, és a testindex semelyik esetben sem osztható 5-el, így ha a testet generáló elem indexe nem 1, akkor nem tudunk általános eredményt megfogalmazni a monogenitással kapcsolatban.

Legyen $m \neq 0, \pm 1$ négyzetmentes egész, α az $X^5 - m$ gyöke és $K = \mathbb{Q}(\alpha)$. Az α-hoz tartozó Hermite normál alakú egész bázis alakja csak m-nek a 25-ös maradékától függ, és 5 különböző esetet eredményez.

1. Ha $r = 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22, 23$ valamint $m = r + 25k$ négyzetmentes, azaz röviden $v_5(m^5 - m) < 2$ és m négyzetmentes, akkor

$$(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$$

egész bázis K-ban. Ezekben az esetekben tehát K monogén. Az indexforma már túlságosan sok tagból áll, ahhoz, hogy megérje feltüntetni, de a megszokott módon kiszámítható, és ebből az esetből a megfelelő helyettesítésekkel adódik a többi egész bázishoz tartozó indexforma is.

2. Ha $m = 1 + 25k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4}{5}\right)$$

egész bázis K-ban.

3. Ha $m = 7 + 25k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1 + 3\alpha + 4\alpha^2 + 2\alpha^3 + \alpha^4}{5}\right)$$

egész bázis K-ban.

4. Ha $m = 18 + 25k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1 + 2\alpha + 4\alpha^2 + 3\alpha^3 + \alpha^4}{5}\right)$$

egész bázis K-ban.

5. Ha $m = 24 + 25k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1 + 4\alpha + \alpha^2 + 4\alpha^3 + \alpha^4}{5}\right)$$

egész bázis K-ban.

A 2., 3., 4. és 5. esetekben azt sejtjük, hogy a megadott maradékosztályokba eső paraméterekkel végtelen sok monogén és végtelen sok nem monogén testet is kaphatunk.

Hatodfokú gyökbővítések

Mind közül ez a legjobban kezelhető eset. Most két valódi résztest is van, így az indexformának már 3 faktora lesz, melyek között több megfelelő összefüggést is találhatunk.

Legyen $m \neq 0, \pm 1$ négyzetmentes egész, α az $X^6 - m$ gyöke és $K = \mathbb{Q}(\alpha)$. Ha σ az $X^6 - m$ Galois csoportjának 6-odrendű eleme, és

$$\alpha^{(1)} = \alpha, \qquad \alpha^{(2)} = \sigma(\alpha), \qquad \alpha^{(3)} = \sigma^2(\alpha),$$
$$\alpha^{(4)} = \sigma^3(\alpha), \qquad \alpha^{(5)} = \sigma^4(\alpha), \qquad \alpha^{(6)} = \sigma^5(\alpha),$$

akkor a Galois csoport hatása szerint az

$$\{(\alpha^{(i)},\alpha^{(j)}), 1 \le i \ne j \le 6\}$$

halmaz 3 orbitja:

$$\begin{aligned}
S_1 &= \{(\alpha^{(1)},\alpha^{(4)}),(\alpha^{(2)},\alpha^{(5)}),(\alpha^{(3)},\alpha^{(6)}),(\alpha^{(4)},\alpha^{(1)}),(\alpha^{(5)},\alpha^{(2)}),(\alpha^{(6)},\alpha^{(3)})\},\\
S_2 &= \{(\alpha^{(1)},\alpha^{(3)}),(\alpha^{(2)},\alpha^{(4)}),(\alpha^{(3)},\alpha^{(5)}),(\alpha^{(4)},\alpha^{(6)}),(\alpha^{(5)},\alpha^{(1)}),(\alpha^{(6)},\alpha^{(2)}),\\
&\quad (\alpha^{(3)},\alpha^{(1)}),(\alpha^{(4)},\alpha^{(2)}),(\alpha^{(5)},\alpha^{(3)}),(\alpha^{(6)},\alpha^{(4)}),(\alpha^{(1)},\alpha^{(5)}),(\alpha^{(2)},\alpha^{(6)})\},\\
S_3 &= \{(\alpha^{(1)},\alpha^{(2)}),(\alpha^{(2)},\alpha^{(3)}),(\alpha^{(3)},\alpha^{(4)}),(\alpha^{(4)},\alpha^{(5)}),(\alpha^{(5)},\alpha^{(6)}),(\alpha^{(6)},\alpha^{(1)}),\\
&\quad (\alpha^{(2)},\alpha^{(1)}),(\alpha^{(3)},\alpha^{(2)}),(\alpha^{(4)},\alpha^{(3)}),(\alpha^{(5)},\alpha^{(4)}),(\alpha^{(6)},\alpha^{(5)}),(\alpha^{(1)},\alpha^{(6)})\}.
\end{aligned}$$

Ez alapján az $(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5)$ bázishoz tartozó indexforma az alábbi módon faktorizálható

$$I(X_2,X_3,X_4,X_5,X_6,) = F_1\cdot F_2\cdot F_3,$$

ahol

$$\begin{aligned}
F_1^2 &= \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_1} \left(X_2+X_3\beta_2^{(i,j)}+X_4\beta_3^{(i,j)}+X_5\beta_4^{(i,j)}+X_6\beta_5^{(i,j)}\right),\\
F_2^2 &= \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_2} \left(X_2+X_3\beta_2^{(i,j)}+X_4\beta_3^{(i,j)}+X_5\beta_4^{(i,j)}+X_6\beta_5^{(i,j)}\right),\\
F_3^2 &= \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_3} \left(X_2+X_3\beta_2^{(i,j)}+X_4\beta_3^{(i,j)}+X_5\beta_4^{(i,j)}+X_6\beta_5^{(i,j)}\right),
\end{aligned}$$

$$\beta_k^{(i,j)} = \frac{(\alpha^{(i)})^k-(\alpha^{(j)})^k}{\alpha^{(i)}-\alpha^{(j)}}.$$

Könnyen ellenőrizhetjük, hogy $F_3-F_1^2$-ből kiemelhető $9m$, és F_3-F_2-ből kiemelhető $4m$. Ezeket fogjuk majd felhasználni a monogenitási vizsgálatokhoz. Emellett több esetben is előfordul majd, hogy a testindex nagyobb, mint 1, és így az indexforma egyenletnek nem lesz megoldása modulo p, valamilyen alkalmas p prímmel.

Az α-hoz tartozó Hermite normál alakú egész bázis alakja csak m-nek a 36-os maradékától függ, és 6 különböző esetet eredményez.

1. Ha $r = 2,3,6,7,11,14,15,22,23,30,31,34$ és $m = r+36k$ négyzetmentes, akkor
$$\left(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5\right)$$
egész bázis K-ban, tehát ezekben az esetekben K monogén.

2. Ha $r = 5,13,21,25,29,33$ és $m = r+36k$ négyzetmentes, akkor
$$\left(1,\alpha,\alpha^2,\frac{1+\alpha^3}{2},\frac{\alpha+\alpha^4}{2},\frac{\alpha^2+\alpha^5}{2}\right)$$

egész bázis K-ban. Ez az eset egyszerre két irányból is támadható. Egyfelől az indexforma egyenletnek nincs megoldása modulo 2, azaz tetszőleges algebrai egész indexe osztható 2-vel. Másrészt pedig a megfelelő helyettesítések elvégzése után az indexforma faktorainak különböző lesz a nevezője. Ezeket a nevezőket az $I(\alpha)$-val pótoljuk, hogy egész együtthatós faktorizációt kapjunk. Legyen f_1 az F_1-hez, f_2 az F_2-höz, és f_3 az F_3-hoz tartozó faktor, ekkor $64f_3 - f_1^2$-ből kiemelhető $9m$. Ez azt jelenti, hogy ha K monogén, akkor $9m$ osztja 63-at vagy 65-öt, amiből nyilvánvalóan csak az első teljesülhet, és így m osztja 7-et. Az m-re való megszorításunkat is figyelembe véve, ez azt jelenti, hogy csak a $K = \mathbb{Q}(\sqrt[6]{-7})$ lehetne monogén, ami viszont természetesen nem monogén, hiszen a testindexe a korábbiak alapján osztható 2-vel.

3. Ha $r = 10, 19$ és $m = r + 36k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1 + \alpha^2 + \alpha^4}{3}, \frac{\alpha + \alpha^3 + \alpha^5}{3}\right)$$

egész bázis K-ban. A testindex ebben az esetben 3-mal lesz osztható, mivel az indexforma egyenletnek nincs megoldása modulo 3. Továbbá $9f_3 - f_2$-ből kiemelhető $4m$. Ez azt eredményezi, hogy monogén esetben m osztja 2-t, ami a feltételek alapján nem lehetséges. Tehát ebben az esetben sem lehet semmilyen paraméter mellet monogén a $K = \mathbb{Q}(\sqrt[6]{m})$.

4. Ha $r = 26, 35$ és $m = r + 36k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1 + 2\alpha^2 + \alpha^4}{3}, \frac{\alpha + 2\alpha^3 + \alpha^5}{3}\right)$$

egész bázis K-ban. Most a testindex ugyan nem osztható 3-mal, de továbbra is fennáll az az összefüggés, hogy $4m$ kiemelhető $9f_3 - f_2$-ből, tehát monogén esetben az m ismét a 2 osztója kell legyen. Ez a feltételek alapján csak $m = -1$ esetén teljesülhetne, amit viszont az elején kizártunk, hiszen ekkor az $X^6 - m$ nem lenne irreducibilis. Így ekkor sem lehet monogén a K.

5. Ha $r = 17$ és $m = r + 36k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \frac{1 + \alpha^3}{2}, \frac{4 + 3\alpha + 2\alpha^2 + \alpha^4}{6}, \frac{4\alpha + 3\alpha^2 + 2\alpha^3 + \alpha^5}{6}\right)$$

egész bázis K-ban. Ebben az esetben az indexforma egyenletnek nincs megoldása modulo 2, vagyis nem lehetnek monogének a testek. A másik módszerrel pedig azt láthatjuk, hogy $64f_3 - f_1^2$-ből és $9f_3 - f_2$-ből egyaránt kiemelhető m. Azaz ha a K monogén lenne, akkor m osztja 65-öt vagy 63-at és m osztja 8-at vagy 10-et. Ezek egyszerre csak $m = 5$ esetén teljesülnének, ami nem 17-et ad maradékul 36-al osztva, tehát innen is láthatjuk, hogy ezek a testek nem monogének.

6. Ha $r = 1$ és $m = r + 36k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \frac{1+\alpha^3}{2}, \frac{4+3\alpha+4\alpha^2+\alpha^4}{6}, \frac{3+4\alpha+3\alpha^2+\alpha^3+\alpha^5}{6}\right)$$

egész bázis K-ban. Ekkor a testindex osztható 6-al, tehát az indexforma egyenletnek sem modulo 2, sem pedig modulo 3 nincs megoldása. Továbbra is teljesül, hogy $64f_3 - f_1^2$-ből és $9f_3 - f_2$-ből egyaránt kiemelhető m, ami monogén esetben csak $m = 5$-el teljesülhet, ami ugyanúgy nem felel meg a feltételeinknek, mint az előző esetben.

Összefoglalva tehát ha $r = 2, 3, 6, 7, 11, 14, 15, 22, 23, 30, 31, 34$ és $m = r + 36k$ négyzetmentes, akkor $\mathbb{Q}(\sqrt[6]{m})$ monogén, a többi esetben pedig nem monogén. Ez azt jelenti, hogy a négyzetmentes paraméterekhez tartozó hatodfokú gyökbővítések monogenitása csupán a paraméter 36-os maradékától függ.

A hetedfokú eset teljesen hasonló a harmadfokú és ötödfokú esethez. A Hermite normál alakú egész bázis alakja m-nek a 49-es maradékától függ, és 7 különböző esetet eredményez. Az esetek többségében (amikor $v_7(m^7 - m) < 2$ teljesül), $\sqrt[7]{m}$ hatvány egész bázist generál, a többi esetben viszont nincs általános eredményünk, ezért ezt az esetet nem részletezem.

Nyolcadfokú gyökbővítések

Ez az eset is majdnem olyan jól megfogható, mint a hatodfokú. Most is két valódi résztest van, azonban ezek közül most az egyik a másik részteste. Ettől függetlenül az indexformának 3 faktora van, amelyek között most is fennállnak a megfelelő összefüggések.

Legyen $m \neq 0, 1$ négyzetmentes egész, α az $X^8 - m$ gyöke és $K = \mathbb{Q}(\alpha)$. Legyen σ az az $X^8 - m$ polinom Galois csoportjának 8-adrendű eleme, és legyenek

$$\begin{aligned} &\alpha^{(1)} = \alpha, && \alpha^{(2)} = \sigma(\alpha), && \alpha^{(3)} = \sigma^2(\alpha), && \alpha^{(4)} = \sigma^3(\alpha), \\ &\alpha^{(5)} = \sigma^4(\alpha), && \alpha^{(6)} = \sigma^5(\alpha), && \alpha^{(7)} = \sigma^6(\alpha), && \alpha^{(8)} = \sigma^7(\alpha). \end{aligned}$$

Ekkor a Galois csoport hatása szerint az

$$\{(\alpha^{(i)}, \alpha^{(j)}), 1 \leq i \neq j \leq 8\}$$

halmaz orbitjai:

$$\begin{aligned} S_1 &= \left\{(\alpha^{(i)}, \alpha^{(j)}) \mid (i-j) \in \{-4, 4\}\right\}, \\ S_2 &= \left\{(\alpha^{(i)}, \alpha^{(j)}) \mid (i-j) \in \{-6, -2, 2, 6\}\right\}, \\ S_3 &= \left\{(\alpha^{(i)}, \alpha^{(j)}) \mid (i-j) \in \{-7, -5, -3, -1, 1, 3, 5, 7\}\right\}. \end{aligned}$$

Így az $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7)$ bázishoz tartozó indexforma egész együtthatós faktorizációja

$$I(X_2, \ldots, X_8) = F_1 \cdot F_2 \cdot F_3,$$

ahol

$$\begin{aligned} F_1^2 &= \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_1} \left(X_2 + X_3\beta_2^{(i,j)} + \ldots + X_8\beta_7^{(i,j)}\right), \\ F_2^2 &= \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_2} \left(X_2 + X_3\beta_2^{(i,j)} + \ldots + X_8\beta_7^{(i,j)}\right), \\ F_3^2 &= \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_3} \left(X_2 + X_3\beta_2^{(i,j)} + \ldots + X_8\beta_7^{(i,j)}\right), \end{aligned}$$

$$\beta_k^{(i,j)} = \frac{(\alpha^{(i)})^k - (\alpha^{(j)})^k}{\alpha^{(i)} - \alpha^{(j)}}.$$

A 3 különböző résztest tartalmazás miatt 3 összefüggést is kapunk a faktorok között. Az $F_3 - F_1^4$-ből és $F_3 - F_2^2$-ből kiemelhető $8m$, valamint $F_2 - F_1^2$-ből kiemelhető $16m$. Ezek mellett, több esetben is előfordul majd, hogy a testindex osztható 2-vel.

Az α-hoz tartozó Hermite normál alakú egész bázis alakja csak m-nek a 16-os maradékától függ, és 4 különböző esetet eredményez.

1. Ha $r = 2, 3, 6, 7, 10, 11, 14, 15$ és $m = r + 16k$ négyzetmentes, akkor

   $$\left(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\right)$$

   egész bázis K-ban, tehát ezekben az esetekben K monogén.

2. Ha $m = 1 + 16k$ négyzetmentes, akkor

   $$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1+\alpha^4}{2}, \frac{\alpha+\alpha^5}{2}, \frac{1+\alpha^2+\alpha^4+\alpha^6}{4}, \frac{1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5+\alpha^6+\alpha^7}{8}\right)$$

   egész bázis K-ban. Ebben az esetben sem az indexforma faktorai segítségével sem pedig modulo 2 nem jutunk ellentmondásra. Ha azonban feltesszük, hogy $m \equiv 1 \pmod{32}$, akkor az indexforma egyeneletnek már nem lesz megoldása modulo 2. Ezt pontosan ugyanaz a jelenség okozza, ami a negyedfokú esetben az $m = 1+16k$ paraméter esetén azt eredményezte, hogy a testindex osztható 2-vel. A $2 \cdot \mathbb{Z}_K$ faktorizációjakor azt kapjuk, hogy

   $$2 \cdot \mathbb{Z}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4^4,$$

   ahol mindegyik prímideál maradékosztály foka 1. Mivel nincs 4 darab különböző elsőfokú polinom $\mathbb{F}_2[X]$-ben, ezért nincs olyan elem, aminek az indexe nem osztható 2-vel.

   Ez az észrevétel könnyen általánosítható, ugyanis Ore módszerével paraméteresen is ki lehet számolni a fenti prímideál faktorizációt. Általánosságban azt mondhatjuk, hogy ha $l \geq 2$, akkor $K = \mathbb{Q}(\sqrt[2^l]{m})$-ben a $2 \cdot \mathbb{Z}_K$ prímideál faktorizációjában, $v_2(m^2 - m) \leq l + 1$ esetén pontosan $v_2(m^2 - m) - 2$ darab, és $v_2(m^2 - m) > l + 1$ esetén pontosan $l + 1$ darab különböző prímideál

van, amelynek a maradékosztály foka 1. Páratlan prímek esetén még egyszerűbb az állítás. Ha p páratlan prím, $l \geq p$, akkor $K = \mathbb{Q}(\sqrt[p^l]{m})$-ben a $p \cdot \mathbb{Z}_K$ prímideál faktorizációjában pontosan $\min\{v_p(m^p - m), l+1\}$ darab prímideál van, amelynek a maradékosztály foka 1. Ezek a megfelelő Newton poligonok oldalaival állnak kapcsolatban.

3. Ha $r = 5, 13$ és $m = r + 16k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1+\alpha^4}{2}, \frac{\alpha+\alpha^5}{2}, \frac{\alpha^2+\alpha^6}{2}, \frac{\alpha^3+\alpha^7}{2}\right)$$

egész bázis K-ban. Ebben az esetben az indexforma f_1, f_2 és f_3 faktoraira teljesül hogy m kiemelhető $f_3 - 16f_1^4$-ből. Ha tehát K monogén, akkor m osztja 15-öt vagy 17-et, ami a fenti feltételek mellett csak $m = 5$ vagy $m = -3$ esetén teljesülhet. Ezek közül $K = \mathbb{Q}(\sqrt[8]{-3})$ monogén, például $\frac{\alpha+\alpha^5}{2}$ hatvány egész bázist generál, a $K = \mathbb{Q}(\sqrt[8]{5})$ esetében viszont azt sejtjük, hogy nem monogén.

4. Ha $m = 9 + 16k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \frac{1+\alpha^4}{2}, \frac{\alpha+\alpha^5}{2}, \frac{1+\alpha^2+\alpha^4+\alpha^6}{4}, \frac{\alpha+\alpha^3+\alpha^5+\alpha^7}{4}\right)$$

egész bázis K-ban. Ebben az esetben az indexforma faktorai f_1, f_2 és f_3, melyekre teljesül, hogy m kiemelhető $f_3 - 16f_1^4$-ből és $f_2 - 4f_1^2$-ből is. Így ha K monogén, akkor m osztja a 3-at vagy az 5-öt, ami a fenti feltételek mellett semmilyen m egészre sem teljesül, vagyis ilyenkor K nem lehet monogén.

Összefoglalva, ha $m = r + 32k$ négyzetmentes, akkor a $K = \mathbb{Q}(\sqrt[8]{m})$ test $r = 2, 3, 6, 7, 10, 11, 14, 15, 18, 19, 22, 23, 26, 27, 30, 31$, illetve $m = -3$ esetén monogén, $m \neq -3, 5$ és $r = 1, 5, 9, 13, 21, 25, 29$ esetén nem monogén. A kimaradt maradékosztály az $m \equiv 17 \pmod{32}$, mely esetben azt sejtjük, hogy végtelen sok olyan paraméter létezik, amellyel a test monogén, és végtelen sok olyan is, amellyel nem monogén.

Kilencedfokú gyökbővítések

Ez az eset sokban hasonlít a negyedfokú esethez, mivel itt is egy prímnek a négyzete a fokszám. Egy résztest van, az indexformának két faktora van, egy 9-ed fokú F_1, és egy 27-ed fokú F_2 faktora, amelyekre teljesül, hogy $F_2 - F_1^3$-ből kiemelhető m. Az indexforma kiszámítása ebben az esetben már kifejezetten számításigényes feladat.

Legyen $m \neq 0, \pm 1$ négyzetmentes egész, α az $X^9 - m$ gyöke és $K = \mathbb{Q}(\alpha)$. Az α-hoz tartozó Hermite normál alakú egész bázis alakja csak m-nek a 27-es maradékától függ, és 5 különböző esetet eredményez.

1. Ha $r = 2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 16, 20, 21, 22, 23, 24, 25$ és $m = r + 27k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8\right)$$

egész bázis K-ban, tehát a szokásos módon, ezekben az esetekben K monogén.

2. Ha $m = 1 + 27k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \frac{1 + \alpha^3 + \alpha^6}{3}, \frac{\alpha + \alpha^4 + \alpha^7}{3}, \frac{1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^8}{9}\right)$$

egész bázis K-ban.

3. Ha $r = 8, 17$ és $m = r + 27k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \frac{1 + 2\alpha^3 + \alpha^6}{3}, \frac{\alpha + 2\alpha^4 + \alpha^7}{3}, \frac{\alpha^2 + 2\alpha^5 + \alpha^8}{3}\right)$$

egész bázis K-ban. Ezekben az esetekben az indexforma f_1 és f_2 faktorára teljesül, hogy m kiemelhető $27f_2 - f_1^3$-ből. Így monogén esetben m osztja 26-ot vagy 28-at, ami a fenti feltételekkel semmilyen m-re nem teljesülhet, vagyis ezek a testek nem monogének.

4. Ha $r = 10, 19$ és $m = r + 27k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \frac{1 + \alpha^3 + \alpha^6}{3}, \frac{\alpha + \alpha^4 + \alpha^7}{3}, \frac{\alpha^2 + \alpha^5 + \alpha^8}{3}\right)$$

egész bázis K-ban. Hasonlóan az előző esethez, itt is kiemelhető m a $27f_2 - f_1^3$-ből. Így a fenti feltételek mellett látható, hogy K ebben az esetben sem lehet monogén.

5. Ha $m = 26 + 27k$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \frac{1 + 2\alpha^3 + \alpha^6}{3}, \frac{\alpha + 2\alpha^4 + \alpha^7}{3}, \frac{1 + 2\alpha + \alpha^2 + 8\alpha^3 + 7\alpha^4 + 8\alpha^5 + \alpha^6 + 2\alpha^7 + \alpha^8}{9}\right)$$

egész bázis K-ban.

Összefoglalva, az első esetben K monogén, a harmadik és negyedik esetben nem monogén, a második és ötödik esetben pedig a szokásos módon azt sejtjük, hogy végtelen sok monogén és végtelen sok nem monogén test létezik.

Nagyjából itt látszik a határ, ameddig gyökbővítések esetén a jelenlegi számítástechnikai eszközökkel érdemes elmenni. Több résztesttel rendelkező testek esetén (pl. $K = \mathbb{Q}(\sqrt[12]{m})$) még van esély az indexforma explicit kiszámítására, de a fokszám és a változók száma miatt innentől kezdve ez az irány nem látszik hatékonynak. A felsorolt esetekben az indexforma kiszámítása átlagos számítógépen (4

mag, 3,4GHz, 16Gb RAM) csupán néhány percet vagy másodpercet vesz igénybe. A legtöbb idő a kilencedfokú gyökbővítések esetén a 27-ed fokú faktor kiszámításához kellett, kb 5 perc. Érdekességképpen, a 11-ed fokú gyökbővítések esetén az indexforma kiszámításakor a program kb 4 óra futás után memóriahiány miatt áll le, ami érthető is, hiszen a 10 változós, 55-öd fokú, és nagyjából 200 000 tagból álló polinom meghatározásához egy 10^{55} tagú algebrai egész együtthatós polinomot kell egyszerűsíteni.

4.2. Legegyszerűbb testek monogenitása

A legegyszerűbb testek általánosításai a monogenitási vizsgálatok szempontjából teljesen hasonlóan viselkednek, mint a gyökbővítések. Csak a nevezetes legegyszerűbb 3, 4 és 6-od fokú testeket fogom részletezni. A legegyszerűbb harmadfokú testek monogenitását már D. Shanks [60] is leírta, hiszen az m^2+3m+9 négyzetmentessége esetén a polinom gyöke hatvány egész bázist generál. Ezt úgy is szokták mondani, hogy a polinom monogén. A legegyszerűbb negyedfokú testek esetén Gaál István és Petrányi Gábor [25] a monogenitás mellett még a minimális indexű elemeket is vizsgálták. A legegyszerűbb hatodfokú számtestek monogenitásával kapcsolatos eredményeink a [28] cikkben jelentek meg.

Legegyszerűbb harmadfokú testek

Ahogy azt már megelőlegeztem, ez a legegyszerűbb eset mind közül. Ezek a testek az

$$f(X)=X^3-mX^2-(m+3)X-1$$

ciklikus polinom egy tetszőleges α gyöke által generált teljesen valós testek. Ha m olyan paraméter, hogy m^2+3m+9 négyzetmentes, akkor α hatvány egész bázist generál a $K=\mathbb{Q}(\alpha)$ legegyszerűbb harmadfokú testben, tehát ezek a testek monogének.

Legegyszerűbb negyedfokú testek

Legyen α az

$$f(X)=X^4-mX^3-6X^2+mX+1$$

polinom egy tetszőleges gyöke, ahol $m\neq 0,\pm 3$. Ekkor a $K=\mathbb{Q}(\alpha)$ testeket legegyszerűbb negyedfokú testeknek nevezzük. Most tegyük fel, hogy m megfelelő paraméter, azaz tetszőleges $p\neq 2$ prím esetén $v_p(m^2+16)<2$, azaz m^2+16 nem osztható semmilyen páratlan prím négyzetével. Az ilyen paraméterkehez tartozó testeknek a monogenitását, és minimális indexű elemeit Gaál István és Petrányi Gábor [25]-ben már vizsgálták a Gaál István, Pethő Attila és M. Pohst [24] cikkében kidolgozott módszer segítségével, amivel egy negyedfokú számtestben az indexforma egyenletet vissza lehet vezetni harmad- és negyedfokú Thue egyenletek megoldására. Most megvizsgáljuk, hogy a mi módszereinkkel a korábbiakhoz képest meddig lehet elmenni.

Legyen $\sigma:\mathbb{C}\mapsto\mathbb{C}$ az alábbi módon értelmezett Möbius transzformáció

$$\sigma(z)=\frac{z-1}{z+1}.$$

Ekkor σ tranzitíven permutálja $f(X)$ gyökeit. Így

$$\alpha^{(1)}=\alpha,\quad \alpha^{(2)}=\sigma(\alpha),\quad \alpha^{(3)}=\sigma^2(\alpha),\quad \alpha^{(4)}=\sigma^3(\alpha)$$

az α konjugáltjai. A Galois csoport hatása szerint az $\{(\alpha^{(i)}, \alpha^{(j)}), 1 \leq i \neq j \leq 4\}$ halmaz orbitjai:

$$\begin{aligned} S_1 &= \left\{(\alpha^{(i)}, \alpha^{(j)}) \mid (i-j) \in \{-2, 2\}\right\}, \\ S_2 &= \left\{(\alpha^{(i)}, \alpha^{(j)}) \mid (i-j) \in \{-3, -1, 1, 3\}\right\}. \end{aligned}$$

Az $(1, \alpha, \alpha^2, \alpha^3)$ bázishoz tartozó indexforma egész együtthatós faktorizációja

$$I(X_2, X_3, X_4) = F_1 \cdot F_2,$$

ahol

$$F_1^2 = \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_1} \left(X_2 + X_3\beta_2^{(i,j)} + X_4\beta_3^{(i,j)}\right),$$

$$F_2^2 = \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_2} \left(X_2 + X_3\beta_2^{(i,j)} + X_4\beta_3^{(i,j)}\right).$$

A faktorok között most több érdekes és hasznos összefüggés is fennáll. Az $m^2 + 16$ kiemelhető az alábbiakból

$$F_2 - F_1^2,$$

$$16F_2 + m^2F_1^2,$$

$$(m^2 + 25)^2F_2 - (m^2 + 7)^2F_1^2.$$

A 3.32 következmény alapján ezeknek a testeknek az α-hoz tartozó Hermite normál alakú egész bázisa csak m-nek a 8-as maradékától függ. Ez alapján 4 különböző esetet kapunk.

1. Ha $r = 1, 3, 5, 7$, $m = r + 8k$ és $m^2 + 16$ négyzetmentes, akkor

$$\left(1, \alpha, \alpha^2, \frac{1 + \alpha^3}{2}\right)$$

egész bázis K-ban. Ekkor az indexforma egyenletnek nincs megoldása modulo 2, vagyis a testindex osztható 2-vel. A $2\mathbb{Z}_K$ prímideál faktorizációjában most két különböző prímideál van, melyeknek a maradékosztály foka 2, de az egyetlen másodfokú irreducibilis polinom $\mathbb{F}_2[X]$-ben az X^2+X+1, így adódik az eredmény. A másik oldalról megközelítve a problémát, láthatjuk, hogy az indexforma f_1 és f_2 faktoraira teljesül, hogy m^2+16 kiemelhető $4f_2 - f_1^2$-ből, és így monogén esetben $m^2 + 16$ osztja a 3-at vagy az 5-öt. Ez semmilyen m paraméter esetén nem teljesülhet, így ezek a testek nem monogének.

2. Ha $r = 2, 6$, $m = r + 8k$ és $(m^2 + 16)/4$ négyzetmentes, akkor

$$\left(1, \alpha, \frac{1 + \alpha^2}{2}, \frac{\alpha + \alpha^3}{2}\right)$$

egész bázis K-ban. Az indexforma f_1 és f_2 faktoraira teljesül, hogy $\frac{m^2+16}{4}$ kiemelhető $4f_2 - f_1^2$-ből, és így monogén esetben m^2+16 osztja a 12-t vagy az 20-at. Ez csupán $m = \pm 2$ esetén teljesülhet, és ezekben az esetben $K = \mathbb{Q}(\alpha)$ monogén is, például $\frac{1+\alpha^2}{2}$ hatvány egész bázist generál. Valójában m és $-m$ paraméterek esetén ugyanazt a legegyszerűbb negyedfokú testet kapjuk, hiszen ha m esetén a polinomnak α gyöke, akkor $-m$ esetén $-\alpha$ lesz gyöke, így elegendő lenne csak a pozitív paraméterekre elvégezni a vizsgálatainkat, de ez az eredményen nem változtat.

3. Ha $m = 4 + 8k$ és $(m^2 + 16)/32$ négyzetmentes, akkor

$$\left(1, \alpha, \frac{1+\alpha^2}{2}, \frac{1+\alpha+\alpha^2+\alpha^3}{2}\right)$$

egész bázis K-ban. Ebben az esetben az indexforma faktorai között az az összefüggés lesz számunkra hasznos, hogy $4(m^2+16)$ kiemelhető $16f_2+m^2f_1^2$-ből. Ez monogén esetben azt jelentené, hogy $4(m^2 + 16)$ osztja $m^2 + 16$-ot vagy $m^2 - 16$-ot. Mivel $4(m^2 + 16)$ tetszőleges m esetén nagyobb, mint $m^2 \pm 16$, ezért ez az oszthatóság csak akkor teljesülhet, ha $m = \pm 4$, és így $m^2 - 16 = 0$. Ezekben az esetekben pedig a K valóban monogén, például $(2, 2, -1)$ megoldása az indexforma egyenletnek.

4. Ha $m = 8k$ és $(m^2 + 16)/16$ négyzetmentes, akkor

$$\left(1, \alpha, \frac{3+2\alpha+\alpha^2}{4}, \frac{2+3\alpha+\alpha^3}{4}\right)$$

egész bázis K-ban. Ekkor $\frac{m^2+16}{16}$ kiemelhető $f_2 - 16f_1^2$-ből, ami monogén esetben azt jelenti, hogy m^2+16 osztja 240-et vagy 272-t. Ez a fenti feltételek mellett csak $m = \pm 8$ és $m = \pm 16$ esetén teljesülhet, mivel $m = 0$ esetén a polinom nem irreducibilis, és így ezt az elején kizártuk. Tehát ebben az esetben csak $m = \pm 8$ és $m = \pm 16$ paraméterek mellett lehet monogén a K. Ezekben az esetekben a mi módszereink nem vezetnek ellentmondásra, azonban [25] Lemma 2. alapján ezek a testek nem monogének.

Összefoglalva tehát az általunk alkalmazott módszerek segítségével megállapíthatjuk, hogy a legegyszerűbb negyedfokú testek csak $m = \pm 2, \pm 4, \pm 8, \pm 16$ paraméterek esetén lehetnek monogének.

Legegyszerűbb hatodfokú testek

Ugyanúgy, mint a gyökbővítéseknél, itt is a hatodfokú eset lesz a legjobban kezelhető. Az egész bázissal és a monogenitással kapcsolatos eredményeink a [28] cikkben jelentek meg.

Legyen $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$ és α az

$$f(X) = X^6 - 2mX^5 - 5(m+3)X^4 - 20X^3 + 5mX^2 + 2(m+3)X + 1$$

polinom egy tetszőleges gyöke. Ekkor a $K = \mathbb{Q}(\alpha)$ testeket legegyszerűbb hatodfokú testeknek nevezzük. Most tegyük fel, hogy m megfelelő paraméter, azaz $m^2 + 3m + 9$ négyzetmentes. Legyen $\sigma : \mathbb{C} \mapsto \mathbb{C}$ az alábbi módon értelmezett Möbius transzformáció

$$\sigma(z) = \frac{z-1}{z+2}.$$

Ekkor σ tranzitíven permutálja $f(X)$ gyökeit. Így

$$\begin{aligned} &\alpha^{(1)} = \alpha, && \alpha^{(2)} = \sigma(\alpha), && \alpha^{(3)} = \sigma^2(\alpha), \\ &\alpha^{(4)} = \sigma^3(\alpha), && \alpha^{(5)} = \sigma^4(\alpha), && \alpha^{(6)} = \sigma^5(\alpha), \end{aligned}$$

az α konjugáltjai. A Galois csoport hatása szerint az $\{(\alpha^{(i)}, \alpha^{(j)}), 1 \le i \ne j \le 6\}$ orbitjai:

$$\begin{aligned} S_1 &= \left\{(\alpha^{(i)}, \alpha^{(j)}) \mid (i-j) \in \{-3, 3\}\right\}, \\ S_2 &= \left\{(\alpha^{(i)}, \alpha^{(j)}) \mid (i-j) \in \{-4, -2, 2, 4\}\right\}, \\ S_3 &= \left\{(\alpha^{(i)}, \alpha^{(j)}) \mid (i-j) \in \{-5, -1, 1, 5\}\right\}. \end{aligned}$$

Így, az $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ bázishoz tartozó indexforma egész együtthatós faktorizációja

$$I(X_2, X_3, X_4, X_5, X_6) = F_1 \cdot F_2 \cdot F_3,$$

ahol

$$F_1^2 = \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_1} \left(X_2 + X_3\beta_2^{(i,j)} + X_4\beta_3^{(i,j)} + X_5\beta_4^{(i,j)} + X_6\beta_5^{(i,j)}\right),$$

$$F_2^2 = \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_2} \left(X_2 + X_3\beta_2^{(i,j)} + X_4\beta_3^{(i,j)} + X_5\beta_4^{(i,j)} + X_6\beta_5^{(i,j)}\right),$$

$$F_3^2 = \prod_{(i,j):(\alpha^{(i)},\alpha^{(j)})\in S_3} \left(X_2 + X_3\beta_2^{(i,j)} + X_4\beta_3^{(i,j)} + X_5\beta_4^{(i,j)} + X_6\beta_5^{(i,j)}\right).$$

A faktorok között most is több érdekes összefüggés is fennáll, azonban ezek közül csak arra lesz szükségünk, hogy $m^2 + 3m + 9$ kiemelhető $F_3 - F_2$-ből. A 3.19 következmény alapján ezeknek a testeknek az α-hoz tartozó Hermite normál alakú egész bázisa csak m-nek a 36-os maradékától függ. Ez alapján 19 különböző esetet kapunk. Az egyes eseteket most nem sorolom fel (könnyen meghatározhatóak minden maradékosztályból egy megfelelő paraméterre kiszámítva a Hermite normál alakú egész bázist), mivel mindegyiknél pontosan ugyanaz az összefüggés szolgáltatja az ellentmondást. Ha a megfelelő egész bázisokhoz tartozó indexforma faktorai f_1, f_2, és f_3, akkor $m^2 + 3m + 9$ minden esetben kiemelhető $27f_3 - f_2$-ből. Ebből pedig az következik, hogy monogén esetben $m^2 + 3m + 9$ osztja 26-ot vagy 28-at, ami csak $m = -4, -2, -1, 1$ esetén teljesülhet. Ezekhez a paraméterekhez tartozó testek pedig valóban monogének, az összes hatvány egész bázist generáló elem pedig fel van sorolva Gaál István [20] cikkében.

4.3. Kompozitum számtestek monogenitása

Ebben a fejezetben az előző fejezetek eredményeit összedolgozva, kompozit számtestek monogenitását fogom vizsgálni. A kompozit számtest $K = LM$ alakú lesz, ahol az $L = \mathbb{Q}(\alpha)$ és $M = \mathbb{Q}(\beta)$ testeket generáló elemek definiáló polinomjai az alábbi táblázatból kerülnek ki

L	M
$X^2 - m_1$	$X^3 - m_2X^2 - (m_2 + 3)X - 1$
$X^2 - m_1$	$X^3 - m_2$
$X^2 - m_1$	$X^4 - m_2X^3 - 6X^2 + m_2X + 1$
$X^2 - m_1$	$X^4 - m_2$
$X^2 + 3$	$X^6 - m_2$

A 3.3 fejezet eredményei alapján ezeknek a testeknek az egész bázisa mindkét paraméterben periodikusan ismétlődik. A Hermite normál alakú egész bázist az α és a β hatványai által generált bázisra vonatkozóan fogjuk megadni. A fejezet eredményei a [29] cikkben jelentek meg.

Mivel most a K testnek elve van két valódi részteste, ezért az indexformának minden esetben lesz legalább 3 faktora. Azt is látni fogjuk, hogy a korábbiakhoz hasonlóan ezek között is fennállnak majd bizonyos összefüggések, amik segítik a monogenitás vizsgálatát.

Legyenek $|L : \mathbb{Q}| = n_1$, $|M : \mathbb{Q}| = n_2$, az α konjugáltjai

$$\alpha^{(1)} = \alpha, \alpha^{(2)}, \ldots, \alpha^{(n_1)},$$

a β konjugáltjai pedig

$$\beta^{(1)} = \alpha, \beta^{(2)}, \ldots, \beta^{(n_2)}.$$

Legyen $L(\underline{X})$ az α és a β hatványai által generált kompozit bázishoz tartozó lineáris forma, azaz

$$L(\underline{X}) = \sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot \alpha^{k-1} \cdot \beta^{l-1}.$$

Jelöljük $L^{(i,j)}(\underline{X})$-el az $L(\underline{X})$ relatív konjugáltjait, ahol i az α, j pedig a β megfelelő konjugáltjára utal, vagyis

$$L^{(i,j)}(\underline{X}) = \sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot \left(\beta^{(j)}\right)^{l-1}.$$

Mivel

$$\begin{aligned} L^{(i,j_1)}(\underline{X}) - L^{(i,j_2)}(\underline{X}) &= \sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot \left(\left(\beta^{(j_1)}\right)^{l-1} - \left(\beta^{(j_2)}\right)^{l-1}\right) = \\ &= \left(\beta^{(j_1)} - \beta^{(j_2)}\right) \cdot \sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot B_{l-1}^{(j_1,j_2)}, \end{aligned}$$

ahol

$$B_{l-1}^{(j_1,j_2)} = \frac{\left(\beta^{(j_1)}\right)^{l-1} - \left(\beta^{(j_2)}\right)^{l-1}}{\beta^{(j_1)} - \beta^{(j_2)}},$$

és hasonlóan

$$L^{(i_1,j)}(\underline{X}) - L^{(i_2,j)}(\underline{X}) = \left(\alpha^{(i_1)} - \alpha^{(i_2)}\right) \cdot \sum_{k=1}^{n_1}\sum_{l=1}^{n_2} X_{k,l} \cdot A_{k-1}^{(i_1,i_2)} \cdot \left(\beta^{(j)}\right)^{l-1}$$

ahol

$$A_{k-1}^{(i_1,i_2)} = \frac{\left(\alpha^{(i_1)}\right)^{k-1} - \left(\alpha^{(i_2)}\right)^{k-1}}{\alpha^{(i_1)} - \alpha^{(i_2)}},$$

ezért a

$$\prod_{i=1}^{n_1} \prod_{1\le j_1<j_2\le n_2} \left(L^{(i,j_1)}(\underline{X}) - L^{(i,j_2)}(\underline{X})\right)^2 =$$

$$= D(\beta)^{n_1} \cdot \prod_{i=1}^{n_1} \prod_{1\le j_1<j_2\le n_2} \left(\sum_{k=1}^{n_1}\sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot B_{l-1}^{(j_1,j_2)}\right)^2$$

és a

$$\prod_{1\le i_1<i_2\le n_1} \prod_{j=1}^{n_2} \left(L^{(i_1,j)}(\underline{X}) - L^{(i_2,j)}(\underline{X})\right)^2 =$$

$$= D(\alpha)^{n_2} \cdot \prod_{1\le i_1<i_2\le n_1} \prod_{j=1}^{n_2} \left(\sum_{k=1}^{n_1}\sum_{l=1}^{n_2} X_{k,l} \cdot A_{k-1}^{(i_1,i_2)} \cdot \left(\beta^{(j)}\right)^{l-1}\right)^2$$

kifejezések a szimmetrikus polinomok alaptétele miatt az $L(\underline{X})$ diszkriminánsának egész együtthatós faktorai. Továbbá mivel az α és a β által generált kompozit bázis diszkriminánsa $D(\alpha)^{n_2} \cdot D(\beta)^{n_1}$, ezért a hozzá tartozó $I(\underline{X})$ indexformának F_1, F_2 és F_3 egész együtthatós faktorai, ahol

$$F_1 = \prod_{i=1}^{n_1} \prod_{1\le j_1<j_2\le n_2} \left(\sum_{k=1}^{n_1}\sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot B_{l-1}^{(j_1,j_2)}\right),$$

$$F_2 = \prod_{1\le i_1<i_2\le n_1} \prod_{j=1}^{n_2} \left(\sum_{k=1}^{n_1}\sum_{l=1}^{n_2} X_{k,l} \cdot A_{k-1}^{(i_1,i_2)} \cdot \left(\beta^{(j)}\right)^{l-1}\right),$$

$$F_3 = \prod_{1\le i_1\ne i_2\le n_1} \prod_{1\le j_1<j_2\le n_2} \left(L^{(i_1,j_1)}(\underline{X}) - L^{(i_2,j_2)}(\underline{X})\right).$$

Ha az α és a β hatványai által generált kompozit bázis helyett a résztestek egy-egy algebrai egészekből álló bázisának kompozíciójaként kapott bázishoz tartozó indexforma faktorizációjára vagyunk kíváncsiak, akkor azt a fentiből a megfelelő

változó transzformációval kaphatjuk. Ez a felírás pontosan megfelel a Gaál István [22] könyvének 1.10 Lemmájában szereplő felbontással.

Az általunk vizsgált összes esetben olyan összefüggés áll majd fenn ezen faktorok között, ami monogén esetben az egyik paramétert korlátozza a másikkal. Ez azt fogja jelenteni, hogy ha az egyik paramétert rögzítjük, akkor a másiknak csak véges sok olyan értéke lehet, amellyel a kompozit test monogén. Ezek a faktorok a legtöbb esetben még tovább bomlanak majd, és az új faktorok további feltételeket szabnak a monogén testek paramétereire. A vizsgált esetekben azt tapasztaltuk, hogy a testindex 1, így az indexforma vizsgálata modulo egy prímszám most nem jelent segítséget.

Másodfokú és a legegyszerűbb harmadfokú testek kompozítuma

Legyen α az $X^2 - m_1$ egy gyöke, ahol $m_1 \neq 1$ négyzetmentes, és legyen β az $X^3 - m_2X^2 - (m_2+3)X - 1$ egy gyöke, ahol $m_2^2+3m_2+9$ négyzetmentes, valamint $\text{lnko}(m_1, m_2^2 + 3m_2 + 9) = 1$. Legyen $K = \mathbb{Q}(\alpha, \beta)$, ekkor az $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2)$-hez tartozó Hermite normál alakú egész bázis csak m_1-nek a 4-es maradékától függ, és 2 esetet eredményez.

1. Ha $r = 2, 3$ és $m_1 = r + 4k$ négyzetmentes, akkor

$$\left(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2\right)$$

egész bázis K-ban. Mivel ez pont az α és a β által generált kompozit bázis, ezért az ehhez tartozó indexformának a faktorai pontosan a korábbi F_1, F_2, F_3 kifejezések. Ezekre teljesül, hogy $4m_1$ kiemelhető $F_3 - (m_2^2+3m_2+9)^2F_1$-ből, és $m_2^2+3m_2+9$ kiemelhető $F_3 - 64m_1^2F_2^2$-ből. Ez monogén esetben azt jelenti, hogy $4m_1$ osztja $m_2^2+3m_2+10$-et vagy $m_2^2+3m_2+8$-at, valamint $m_2^2+3m_2+9$ osztja $64m_1^3 + 1$-et vagy $64m_1^3 - 1$-et. Így valamelyik paramétert rögzítve, a másik paraméter csak véges sok értéket vehet fel úgy, hogy a kompozit test monogén legyen.

2. Ha $m_1 = 1 + 4k$ négyzetmentes, akkor

$$\left(1, \frac{1+\alpha}{2}, \beta, \frac{\beta+\alpha\beta}{2}, \beta^2, \frac{\beta^2+\alpha\beta^2}{2}\right)$$

egész bázis K-ban. A megfelelő helyettesítéseket elvégezve, F_1, F_2, F_3-ból megkapjuk a fenti egész bázishoz tartozó indexforma f_1, f_2, f_3 faktorait. Ezekre most az teljesül, hogy m_1 kiemelhető $F_3 - (m_2^2 + 3m_2 + 9)^2F_1$-ből, és $m_2^2 + 3m_2 + 9$ kiemelhető $F_3 - m_1^2F_2^2$-ből, ami monogén esetben azt jelenti, hogy m_1 osztja $m_2^2+3m_2+10$-et vagy $m_2^2+3m_2+8$-at, valamint $m_2^2+3m_2+9$ osztja $m_1^3 + 1$-et vagy $m_1^3 - 1$-et. Így tehát ismét teljesül az, hogy valamelyik paramétert rögzítve, a másik paraméter csak véges sok értéket vehet fel úgy, hogy a kompozit test monogén legyen.

Másodfokú és harmadfokú gyökbővítések kompozítuma

Legyen α az $X^2 - m_1$ és β az $X^3 - m_2$ gyöke, ahol $m_1 \neq 0, 1$ és $m_2 \neq 0, \pm 1$ olyan négyzetmentes paraméterek, hogy $\mathrm{lnko}(m_1, m_2) \mid 6$. Legyen $K = \mathbb{Q}(\alpha, \beta)$, ekkor az $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2)$-hez tartozó Hermite normál alakú egész bázis periodikusan ismétlődik m_1-ben modulo 12 és m_2-ben modulo 18.

Az $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2)$-hez tartozó indexforma faktorai között most az az összefüggés áll fenn, hogy $4m_1$ kiemelhető $F_3 - 27m_2^2F_1$-ből, illetve $9m_2$ kiemelhető $F_3 - 64m_1^3F_2^2$-ből. Mivel $I(\alpha, \beta)$ osztja $\mathrm{lnko}(D(\alpha)^3, D(\beta)^2)$-t, ami pedig a feltételek alapján m_1-től és m_2-től függetlenül korlátos, ezért a megfelelő egész bázisokhoz tartozó indexforma f_1, f_2 és f_3 faktoraira fennálló összefüggések csak konstans szorzóban térnek el az F_1, F_2 és F_3-ra vonatkozó összefüggésektől. Monognén esetben az indexforma egyenlet egy megoldását helyettesítve f_1, f_2, f_3-ba, azok értéke ± 1 kell legyen, így oszthatósági összefüggéseket nyerünk a paraméterek között. Ezeket a paraméterek megfelelő maradékai szerint az alábbi táblázat tartalmazza. Az oszthatóságoknál a $\pm$ jel azt jelenti, hogy az vagy $+$ vagy $-$ előjellel kell teljesüljön.

$m_1 \pmod{12}$	$m_2 \pmod{18}$	$4m_1 \mid F_3 - 27m_2^2F_1$	$9m_2 \mid F_3 - 64m_1^3F_2^2$
$1, 5$	$1, 8, 10, 17$	$m_1 \mid 3m_2^2 \pm 1$	$m_2 \mid m_1^3 \pm 1$
$1, 5$	$2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 16$	$m_1 \mid 27m_2^2 \pm 1$	$9m_2 \mid m_1^3 \pm 1$
$2, 7, 10, 11$	$1, 17$	$4m_1 \mid 3m_2^2 \pm 1$	$m_2 \mid 64m_1^3 \pm 1$
$2, 7, 10, 11$	$3, 5, 7, 11, 13, 15$	$4m_1 \mid 27m_2^2 \pm 1$	$9m_2 \mid 64m_1^3 \pm 1$
$2, 7, 10, 11$	$2, 4, 6, 12, 14, 16$	$4m_1 \mid \frac{27}{2}m_2^2 \pm 2$	$9m_2 \mid 16m_1^3 \pm 2$
$2, 7, 10, 11$	$8, 10$	$4m_1 \mid \frac{3}{2}m_2^2 \pm 2$	$9m_2 \mid 16m_1^3 \pm 2$
$3, 6$	$1, 17$	$\frac{4}{3}m_1 \mid m_2^2 \pm 3$	$3m_2 \mid \frac{64}{9}m_1^3 \pm 3$
$3, 6$	$3, 5, 7, 11, 13, 15$	$4m_1 \mid 9m_2^2 \pm 3$	$9m_2 \mid \frac{64}{9}m_1^3 \pm 3$
$3, 6$	$8, 10$	$\frac{4}{3}m_1 \mid \frac{1}{2}m_2^2 \pm 6$	$3m_2 \mid \frac{16}{9}m_1^3 \pm 6$
$3, 6$	$2, 4, 6, 12, 14, 16$	$4m_1 \mid \frac{9}{2}m_2^2 \pm 6$	$9m_2 \mid \frac{16}{9}m_1^3 \pm 6$
9	$1, 10$	$\frac{1}{3}m_1 \mid m_2^2 \pm 3$	$3m_2 \mid \frac{1}{9}m_1^3 \pm 3$
9	$8, 17$	$\frac{1}{3}m_1 \mid m_2^2 \pm 3$	$m_2 \mid \frac{1}{9}m_1^3 \pm 3$
9	$2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 16$	$m_1 \mid 9m_2^2 \pm 3$	$9m_2 \mid \frac{1}{9}m_1^3 \pm 3$

A táblázat alapján világos, hogy ha $m_1 \neq \pm 1$ és $m_1 \neq \pm 3$, akkor a táblázat harmadik és negyedik oszlopában az osztandók nem lehetnek egyenlőek 0-val, így az egyik paraméter rögzítése után, a másik paraméternek csak véges sok olyan értéke lehet, amellyel a kompozit test monogén. A feltételeket is figyelembe véve, láthatjuk hogy az $m_1 = \pm 1$ csak $m_1 \equiv 1, 5 \pmod{12}$ mellett okoz fennakadást, azaz csak az $m_1 = 1$ marad, mint problémás érték, amit viszont az elején kizártunk, mert az $X^2 - 1$ nem irreducibilis. Tehát marad az $m_1 = \pm 3$ lehetőség, amivel a $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{m_2})$ normális testeket kapjuk. Ezekről M.-L. Chang [6] megmutatta, hogy csak $m_2 = 2$ esetén lehetnek monogének. Ezzel tehát az összes paraméter párra teljesül, hogy az egyiket rögzítve, csak véges sok monogén testet kaphatunk.

Másodfokú és legegyszerűbb negyedfokú testek kompozítuma

Legyen α az $X^2 - m_1$ egy gyöke, ahol $m_1 \neq 1$ négyzetmentes, és legyen β az $X^4 - m_2X^3 - 6X^2 + m_2X + 1$ polinom egy gyöke, ahol $m_2 \neq 0, \pm 3$ és $m_2^2 + 16$ négyzetmentes, valamint $\text{lnko}(m_1, m_2^2 + 16) \mid 2$. Legyen $K = \mathbb{Q}(\alpha, \beta)$, ekkor az $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2, \beta^3, \alpha\beta^3)$ bázishoz tartozó Hermite normál alakú egész bázis periodikusan ismétlődik m_1-ben modulo 8 és m_2-ben modulo 16.

Legyen $\sigma : \mathbb{C} \mapsto \mathbb{C}$ a $\sigma(z) = \frac{z-1}{z+1}$ módon adott Möbius transzformáció. Ekkor az α konjugáltjai $\alpha^{(1)} = \alpha, \quad \alpha^{(2)} = -\alpha$, és β konjugáltjai

$$\beta^{(1)} = \beta, \quad \beta^{(2)} = \sigma(\beta), \quad \beta^{(3)} = \sigma^2(\beta), \quad \beta^{(4)} = \sigma^3(\beta).$$

A legegyszerűbb negyedfokú testnek van másodfokú részteste, ezért a fenti kompozit bázishoz tartozó indexformának 5 faktora lesz, mivel a kompozit testeknél általánosan megjelenő F_1 és F_3 faktorok tovább bomlanak még 2-2 tényezőre. Ha tehát S_1 és S_2 a legegyszerűbb negyedfokú testeknél definiált két halmaz (értelemszerűen α helyett β-t írva, hiszen most β-val jelöltem a legegyszerűbb negyedfokú polinom gyökét), akkor a kompozit bázishoz tartozó indexforma faktorai $F_{11}, F_{12}, F_2, F_{31}, F_{32}$, ahol

$$\begin{aligned}
F_{11}^2 &= \prod_{i=1}^{2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_1} \left(\sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot B_{l-1}^{(j_1,j_2)} \right) \\
F_{12}^2 &= \prod_{i=1}^{2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_2} \left(\sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot B_{l-1}^{(j_1,j_2)} \right) \\
F_2 &= \prod_{1\le i_1<i_2\le 2} \prod_{j=1}^{4} \left(\sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot A_{k-1}^{(i_1,i_2)} \cdot \left(\beta^{(j)}\right)^{l-1} \right) \\
F_{31}^2 &= \prod_{1\le i_1\neq i_2\le 2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_1} \left(L^{(i_1,j_1)}(\underline{X}) - L^{(i_2,j_2)}(\underline{X}) \right). \\
F_{32}^2 &= \prod_{1\le i_1\neq i_2\le 2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_2} \left(L^{(i_1,j_1)}(\underline{X}) - L^{(i_2,j_2)}(\underline{X}) \right).
\end{aligned}$$

Érdekesség, hogy az F_{31} faktorból kiemelhető a 4, azaz a bázis által generált modulusban tetszőleges elem indexe osztható 4-el, bár ez az algebrai egészek indexére nincs különösebb hatással. A faktorok között 6 lényegesen különböző összefüggést találtunk. Először is m_1 kiemelhető az $F_{31}-(m_2^2+16)F_{11}$-ből és $F_{32}-(m_2^2+16)F_{12}$-ből, valamint m_2^2+16 kiemelhető az alábbi 4 kifejezésből:

$$F_{12}-F_{11}^2, \quad F_{32}-F_{31}^2, \quad F_{31}-16m_1^2F_2, \quad F_{32}-256m_1^4F_2^2.$$

Ezek segítségével monogén esetben a legtöbb paramétert ki lehet zárni. A fentiek közül, a faktoroknak azok a lineáris kombinációi, amelyekben az együtthatók nem függnek a paraméterektől, globálisan korlátozzák a monogén testekhez kapcsolódó paramétereket. Megmutattuk, hogy monogén testek esetén az $m_1 \equiv 1,3,5,7 \pmod 8$ és $m_2 \equiv 4,12 \pmod{16}$ paraméterektől eltekintve,

$$|m_2| \leq 64, \text{ és } |m_1| \leq 4m_2^2+192$$

teljesül. A fennmaradó $m_1 \equiv 1,3,5,7 \pmod 8$ és $m_2 \equiv 4,12 \pmod{16}$ esetekben pedig ha $m_1 \neq -1$, akkor a szokásos módon, az egyik paramétert rögzítve, a másik csak véges sok értéket vehet fel, úgy, hogy a kompozit test monogén legyen. Az $m_1=-1$ eset a fejezetben kissé kilóg a sorból, ilyenkor ugyanis az általunk alkalmazott módszerekkel nem tudtuk igazolni, hogy csak véges sok olyan m_2 paraméter létezik, amellyel a kompozit test monogén.

Másodfokú és negyedfokú gyökbővítések kompozítuma

Legyen α az X^2-m_1 egy gyöke, ahol $m_1 \neq 0,1$ négyzetmentes, és legyen β az X^4-m_2 egy gyöke, ahol $m_2 \neq 0,1$ négyzetmentes, valamint $m_1 \neq m_2$ és $\text{lnko}(m_1,m_2) \mid 2$. Legyen $K=\mathbb{Q}(\alpha,\beta)$, ekkor az $(1,\alpha,\beta,\alpha\beta,\beta^2,\alpha\beta^2,\beta^3,\alpha\beta^3)$-höz tartozó Hermite normál alakú egész bázis periodikusan ismétlődik m_1-ben és m_2-ben modulo 8. Legyenek $\alpha^{(1)}=\alpha, \alpha^{(2)}=-\alpha$ az α, és

$$\beta^{(1)}=\beta, \qquad \beta^{(2)}=i\cdot\beta, \qquad \beta^{(3)}=-\beta, \qquad \beta^{(4)}=-i\cdot\beta$$

a β konjugáltjai. Az előző példához hasonlóan, most is van másodfokú részteste a negyedfokú gyökbővítéseknek, így megint 5 faktora van a fenti kompozit bázishoz tartozó indexformának. Ezeket pontosan ugyanazok a szorzatok szolgáltatják, mint az előző esetben, és lényegében ugyanazok az összefüggések teljesülnek rájuk értelemszerű módosításokkal. Az m_1 kiemelhető $F_{31}-16m_2F_{11}$-ből és $F_{32}-16m_2^2F_{12}$-ből, valamint m_2 kiemelhető az alábbi 4 kifejezésből:

$$F_{12}-F_{11}^2, \qquad F_{32}-F_{31}^2, \qquad F_{31}-16m_1^2F_2, \qquad F_{32}-256m_1^4F_2^2.$$

Végigvizsgálva az egyes maradékosztályokhoz tartozó indexformák faktorai közötti kapcsolatokat, azt találtuk, hogy ha

- $m_1 \equiv 1 \pmod 4$ és $m_2 \equiv 5 \pmod 8$ vagy
- $m_1 \equiv 2 \pmod 4$ vagy

- $m_1 \equiv 3 \pmod 4$ és $m_2 \equiv 1 \pmod 2$,

akkor a K csak olyan paraméterekkel lehet monogén, amelyekre teljesül, hogy $|m_2| \leq 130$ és $|m_1| \leq 32|m_2| + 32$. Az összes többi esetben, ha $m_1 \neq -1$, akkor az egyik paraméter rögzítése után, a másik paraméternek csak véges sok értéke lehet, úgy, hogy a K monogén legyen.

Maradt az $m_1 = -1$ eset. Ez azért különösen érdekes, mert ekkor a kompozit test $K = \mathbb{Q}(i, \sqrt[4]{m_2})$ normális bővítése $\mathbb{Q}$-nak. Ez azt eredményezi, hogy a nyolcadfokú F_{32} tovább bomlik két negyedfokú tényezőre, $F_{32} = F_4 \cdot F_5$. Az újabb faktorok megjelenése további összefüggéseket is szolgáltat, amelyek lényegesen hatékonyabbak a korábbiaknál. Az m_2 paraméter 4-es maradékától függően az alábbi összefüggéseket nyerjük.

- Ha $m_2 \equiv 1 \pmod 4$, akkor m_2 kiemelhető $4f_2 + f_4$-ből
- Ha $m_2 \equiv 3 \pmod 4$, akkor m_2 kiemelhető $f_2 + 4f_4$-ből
- Ha $m_2 \equiv 2 \pmod 4$, akkor m_2 kiemelhető $f_2 - f_4$-ből és 4 osztja $f_2 + f_4$ összes együtthatóját.

Monogén testek esetén az első és második esetből kapjuk az $m_2 = \pm 3, \pm 5$ lehetőségeket, a harmadikból pedig az $m_2 = \pm 2$ értékeket. A harmadik eset a korábbiakhoz képest kissé különleges, hiszen használunk egy paramétertől független oszthatóságot. Ezt a következőképpen lehet jól kihasználni. Mivel 4 osztja $f_2 + f_4$ összes együtthatóját, ezért monogén esetben az 1 indexű elem együtthatóit helyettesítve $f_2 + f_4$-be, a kapott szám 4-el osztható lesz. Továbbá f_2 és f_4 értéke ± 1 kell legyen, így szükségképpen $f_2 + f_4 = 0$. Ebből viszont $f_2 - f_4 = \pm 2$ következik, amit oszt az m_2, és így adódik az $m_2 = \pm 2$ megszorításunk a paraméterre. Világos, hogy $m_2 = \pm 1$ esetén nem kapnánk nyolcadfokú kompozit testet, ezt a lehetőséget az $m_2 \neq 1$ és $m_1 \neq m_2$ feltételekkel eleve ki is zártuk. Az $m_2 = \pm 2$, $m_2 = 3$ és $m_2 = -5$ esetekről a [27] cikkben megmutattuk, hogy nem monogének, és a kimaradt két esetről is ugyanezt sejtjük kb. 10^6 darab kis együtthatójú elem indexének kiszámítása alapján.

Ahogy azt láttuk az előző fejezetekben, a $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{m})$ és a $\mathbb{Q}(i, \sqrt[4]{m})$ normális bővítések külön részletesebb vizsgálatok tárgyát képezték, így teljessé téve ezt az irányt, a következőkben a $\mathbb{Q}(i\sqrt{3}, \sqrt[6]{m})$ testek monogenitását fogjuk vizsgálni. Ezzel véges sok paramétertől eltekintve, az összes másodfokú test feletti normális gyökbővítés monogenitása le lesz írva.

A $\mathbb{Q}(i\sqrt{3}, \sqrt[6]{m})$ testek monogenitása

Legyen ω harmadik primitív egységgyök, β pedig az $X^6 - m$ polinom gyöke, ahol $m \neq \pm 1, -3$ négyzetmentes egész. Legyen $K = \mathbb{Q}(\omega, \beta)$, ekkor az

$$(1, \omega, \beta, \omega\beta, \beta^2, \omega\beta^2, \beta^3, \omega\beta^3, \beta^4, \omega\beta^4, \beta^5, \omega\beta^5)$$

kompozit bázishoz tartozó Hermite normál alakú egész bázis periodikusan ismétlődik m-ben modulo 36. Az indexformának ezúttal 9 faktora van, az F_1 további 3, az F_3 pedig 5 tényezőre esik szét. Ha S_1, S_2 és S_3 a 4.1 fejezetben definiált orbitok értelemszerűen α helyett β-t írva, akkor az indexformának $F_{11}, F_{12}, F_{13}, F_2, F_{31}, F_{32}, F_{33}$ egész együtthatós faktorai, ahol

$$
\begin{aligned}
F_{11}^2 &= \prod_{i=1}^{2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_1} \left(\sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot B_{l-1}^{(j_1,j_2)} \right) \\
F_{12}^2 &= \prod_{i=1}^{2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_2} \left(\sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot B_{l-1}^{(j_1,j_2)} \right) \\
F_{13}^2 &= \prod_{i=1}^{2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_3} \left(\sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot \left(\alpha^{(i)}\right)^{k-1} \cdot B_{l-1}^{(j_1,j_2)} \right) \\
F_2 &= \prod_{1\le i_1<i_2\le 2} \prod_{j=1}^{6} \left(\sum_{k=1}^{n_1} \sum_{l=1}^{n_2} X_{k,l} \cdot A_{k-1}^{(i_1,i_2)} \cdot \left(\beta^{(j)}\right)^{l-1} \right) \\
F_{31}^2 &= \prod_{1\le i_1\ne i_2\le 2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_1} \left(L^{(i_1,j_1)}(\underline{X}) - L^{(i_2,j_2)}(\underline{X}) \right) \\
F_{32}^2 &= \prod_{1\le i_1\ne i_2\le 2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_2} \left(L^{(i_1,j_1)}(\underline{X}) - L^{(i_2,j_2)}(\underline{X}) \right) \\
F_{33}^2 &= \prod_{1\le i_1\ne i_2\le 2} \prod_{(j_1,j_2):(\beta^{(j_1)},\beta^{(j_2)})\in S_3} \left(L^{(i_1,j_1)}(\underline{X}) - L^{(i_2,j_2)}(\underline{X}) \right).
\end{aligned}
$$

Ezek közül pedig F_{32} és F_{33} esik még szét két faktorra. Egy igazán hatékony összefüggést találtunk, a faktorok között, mégpedig, hogy m kiemelhető $F_{31} - F_{32}$-ből. Amikor áttérünk a megfelelő egész bázishoz tartozó indexformára, akkor annak f_{31} és f_{32} faktoraira az alábbiak teljesülnek

- ha $m \equiv 1, 5 \pmod{12}$, akkor $m \mid f_{31} - 9f_{32}$,
- ha $m \equiv 2, 7, 10, 11 \pmod{12}$, akkor $4m \mid f_{31} - 9f_{32}$,
- ha $m \equiv 3, 6 \pmod{12}$, akkor $\frac{4m}{3} \mid f_{31} - 9f_{32}$,
- ha $m \equiv 9 \pmod{12}$, akkor $\frac{m}{3} \mid f_{31} - 9f_{32}$.

Ha a test monogén, akkor $f_{31} = \pm 1$ és $f_{32} = \pm 1$, így a fentiekkel együtt a lehetséges paraméterek $m = -15, -6, -3, -2, 1, 2, 3, 5, 6$. Ezek közül az 1 és a -3 eleve ki volt zárva, így azt kaptuk, hogy $m \ne -15, -6, -2, 2, 3, 5, 6$ esetén a $K = \mathbb{Q}(i\sqrt{3}, \sqrt[6]{m})$ testek nem monogének. A kimaradó esetekről a korábbiakhoz hasonlóan úgy sejtjük, hogy nem monogének.

Összefoglaló

Az értekezés központi témája az algebrai számtestek egész bázisai. Adott számtest esetén az egész bázis meghatározására hatékony algoritmusok léteznek. A legtöbb ilyen algoritmus esetén bemeneti adatként az algebrai számtestet egy primitív α elemének definiáló polinomját szokás megadni. A kimenetként kapott egész bázis elemei általában ennek az α elemnek a polinomjaiként vannak megadva. Egészen pontosan, egy n-edfokú algebrai számtest esetén olyan legfeljebb $n-1$-edfokú $h_0, h_1, \ldots, h_{n-1} \in \mathbb{Q}[X]$ polinomokat határoznak meg az eljárások, amelyekre teljesül, hogy

$$(h_0(\alpha), h_1(\alpha), \ldots, h_{n-1}(\alpha))$$

egész bázist alkot $\mathbb{Q}(\alpha)$-ban.

Bizonyos végtelen parametrikus polinomcsaládok gyökei által generált számtestcsaládok egész bázisainak vizsgálata során kiderült, hogy a paraméterek egy alkalmas megszorítása esetén a fenti $h_i(X)$ polinomok csak a paraméternek egy alkalmas n_0 periódushossz szerint vett osztási maradékától függnek. Ilyenkor azt mondjuk, hogy a végtelen parametrikus számtestcsalád egész bázisai periodikusan ismétlődnek modulo n_0.

A legegyszerűbb példa az $f_m(X) = X^2 - m$ végtelen parametrikus polinomcsalád gyöke által generált másodfokú számtestek, ahol $m \neq 1$ négyzetmentes egész. Ezen testek esetén jól ismert tény, hogy ha $m \equiv 2, 3 \pmod 4$, akkor $(1, \sqrt{m})$, ha pedig $m \equiv 1 \pmod 4$, akkor $\left(1, \frac{1+\sqrt{m}}{2}\right)$ egész bázist alkot $\mathbb{Q}(\sqrt{m})$-ben. A fenti megközelítést tekintve ezt úgy is mondhatjuk, hogy $(h_0(\sqrt{m}), h_1(\sqrt{m}))$ egész bázist alkot $\mathbb{Q}(\sqrt{m})$-ben, ahol a $h_0, h_1 \in \mathbb{Q}[X]$ polinomok csak m-nek a 4-el való osztási maradékától függnek,

$$\begin{aligned} &h_0(X) = 1, \qquad &&h_1(X) = X, \qquad &&\text{ha } m \equiv 2, 3 \pmod 4, \\ &h_0(X) = 1, \qquad &&h_1(X) = \frac{1}{2} + \frac{1}{2} \cdot X, \qquad &&\text{ha } m \equiv 1 \pmod 4. \end{aligned}$$

Ez a jelenség a másodfokú testeken kívül eddig csak kevés számtestben volt ismert (pl. harmadfokú [12] és negyedfokú gyökbővítések [19], legegyszerűbb negyedfokú testek [49]).

A 3. fejezetben három végtelen parametrikus polinomcsalád gyökei által generált számtestcsalád esetén igazoljuk ezt a periodikus egész bázis tulajdonságot. A polinomcsaládokat értelemszerű módon kiterjesztjük tetszőleges fokszámokra, és

meghatározunk olyan, kizárólag a fokszámtól függő konstansokat, amelyek szerint a végtelen parametrikus számtestek egész bázisa periodikusan ismétlődni fog. A kapcsolódó eredmények a [26], [28], [58] és [59] cikkekben jelentek meg.

A vizsgált polinomcsaládok a következőek:

I. Gyökbővítések.

$$f_m^{(n)}(X) = X^n - m,$$

ahol $m \neq \pm 1$ négyzetmentes egész.

II. Legegyszerűbb harmadfokú polinomok általánosításai.

$$f_m^{(n)}(X) = \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot g(n-i),$$

ahol

$$g(i) := \begin{cases} 1, & \text{ha } i \equiv 0 \pmod 6, \\ -\frac{m}{3^{v_3(n)}}, & \text{ha } i \equiv 1 \pmod 6, \\ -\frac{m}{3^{v_3(n)}} - 1, & \text{ha } i \equiv 2 \pmod 6, \\ -1, & \text{ha } i \equiv 3 \pmod 6, \\ \frac{m}{3^{v_3(n)}}, & \text{ha } i \equiv 4 \pmod 6, \\ \frac{m}{3^{v_3(n)}} + 1, & \text{ha } i \equiv 5 \pmod 6, \end{cases}$$

és tetszőleges $p \neq 3$ prím esetén $v_p\left(m^2 + 3^{v_3(n)}m + 9^{v_3(n)}\right) \leq 1$.

III. Legegyszerűbb negyedfokú polinomok általánosításai.

$$f_m^{(n)}(X) = \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot g(n-i),$$

ahol

$$g(i) := \begin{cases} 1, & \text{ha } i \equiv 0 \pmod 4, \\ -\frac{m}{2^{v_2(n)}}, & \text{ha } i \equiv 1 \pmod 4, \\ -1, & \text{ha } i \equiv 2 \pmod 4, \\ \frac{m}{2^{v_2(n)}}, & \text{ha } i \equiv 3 \pmod 4, \end{cases}$$

és tetszőleges $p \neq 2$ prím esetén $v_p\left(m^2 + 4^{v_2(n)}\right) \leq 1$.

A 3.1 fejezetben foglalkozunk a gyökbővítésekkel. Megmutatjuk, hogy ha

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_j^{k_j},$$

és

$$n_0 = p_1^{k_1+1} \cdot p_2^{k_2+1} \cdot \ldots \cdot p_j^{k_j+1},$$

akkor a $K = \mathbb{Q}(\sqrt[n]{m})$ testek egész bázisa periodikusan ismétlődik modulo n_0. A Newton poligonok, és Ø. Ore [56] módszerét felhasználva először igazoljuk, hogy a fenti állítás teljesül $n = p^k$ prímhatvány kitevők esetén, majd megmutatjuk, hogy hogyan lehet két relatív prím fokú gyökbővítés egész bázisából meghatározni a két test kompozítumának egy egész bázisát. Végül ebből a módszerből adódik a periódushossz általános kitevők esetén is.

A 3.2 fejezetben tárgyaljuk a legegyszerűbb polinomok általánosításait. Ezek esetében először igazoljuk, hogy az n-edfokú esetben a felbontási testük ciklikus n-edfokú bővítése egy résztestének. Ez a tulajdonság gyökbővítések esetén nyilvánvalóan teljesül, és sejtéseink szerint szoros kapcsolatban áll a periodikus egész bázis tulajdonsággal, valamint a monogenitás vizsgálata során használt indexforma faktorai között fennálló összefüggésekkel. Ezután meghatározzuk a polinomok diszkriminánsát a kitevő és a paraméter függvényében, és megmutatjuk, hogy a megfelelő megszorításoknak eleget tevő paraméterek esetén a polinomok irreducibilisek. Ezek a megszorítások a paraméter másodfokú polinomjának négyzetmentes értékeivel állnak kapcsolatban, így T. Nagell [54] eredményei alapján ténylegesen végtelen sok paraméter marad, amelyekre az eredményeink vonatkoznak. A megfelelő paraméterek esetén igazoljuk a periodikus egész bázis tulajdonságot, a kitevő függvényében felső korlátot adunk periódushosszra, valamint $n = 2, 3, 4, 5, 6, 8, 9, 12$ esetén meghatározzuk a legkisebb periódushosszt. Vizsgálatainkat először a legegyszerűbb harmadfokú testek, majd ugyanazon séma szerint a legegyszerűbb negyedfokú testek általánosításai esetén végeztük el. Mivel a bizonyítások a két esetben teljesen analóg módon végezhetőek el, ezért az utóbbi esetben azokat nem részletezzük.

A 3.3 fejezetben általánosítjuk a periodikus egész bázis tulajdonságot kompozit testekre, majd megmutatjuk, hogy a megfelelő feltételek mellett az előző két részben tárgyalt számtestcsaládok kompozíciójaként kapott testek egész bázisai is periodikusan ismétlődnek. Néhány alacsonyabb fokú kompozít bővítés esetén meghatároztuk a paraméterekhez tartozó legkisebb periódushosszt, amely szerint az egész bázisok ismétlődnek. Ezeket az eseteket az alábbi táblázat tartalmazza.

L	M	m_1	m_2
$X^2 - m_1$	$X^3 - m_2X^2 - (m_2 + 3)X - 1$	4	1
$X^2 - m_1$	$X^3 - m_2$	12	18
$X^2 - m_1$	$X^4 - m_2X^3 - 6X^2 + m_2X + 1$	8	16
$X^2 - m_1$	$X^4 - m_2$	8	8
$X^2 + 3$	$X^6 - m_2$	$--$	36

Algebrai számtestek egész bázisai között kitüntetett szerepet töltenek be az $(1, \alpha, \ldots, \alpha^{n-1})$ alakú hatvány egész bázisok. Ha az n-edfokú K algebrai számtestben létezik ilyen α algebrai egész, amelynek a hatványai egész bázist generálnak, akkor a egészek gyűrűjét $\mathbb{Z}$ felett egyetlen elem generálja, $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, azaz Z_K mono-generált, más néven *monogén* gyűrű. Egy testben a hatvány egész bázis

generátorok meghatározása ekvivalens egy Diofantikus egyenlet, az úgynevezett indexforma egyenlet megoldásával.

A disszertáció 4. fejezetében az korábbi eredményeket felhasználva néhány alacsonyabb fokú nevezetes számtestcsalád esetében vizsgáljuk a monogenitást. Ezek a legfeljebb kilencedfokú gyökbővítések, a legegyszerűbb harmad-, negyed-, illetve hatodfokú számtestek. Számításaink során nem célunk meghatározni az összes hatvány egész bázis generátort, csupán azt igyekszünk eldönteni, hogy mely paraméterek esetén lehet monogén a test. Arra törekszünk, hogy ha egy adott paraméter esetén a parametrikus polinomcsalád gyöke nem generál hatvány egész bázist, akkor megmutassuk, hogy a test nem monogén, vagyis az indexforma egyenletnek nincs megoldása.

Ehhez két különböző megközelítést használunk. Az első szorosan kapcsolódik R. Dedekind [12] módszeréhez, amely racionális prímek prímideál faktorizációját használja fel a nem-monogenitás igazolásához. Ez akkor működik, ha a testindex nem 1, vagyis létezik olyan p prím, amely tetszőleges algebrai egész indexét osztja. Ekkor az indexforma egyenletnek értelemszerűen nem lesz megoldása modulo p, és így az egészek körében sem. Az indexforma kiszámítása után meghatározzuk a lehetséges p prímeket, melyekből a fenti polinomcsaládok esetén csak véges sok van, hiszen felső becsléseket adtunk az indexekre, és ezen prímekre megvizsgáljuk, hogy az indexforma egyenletnek van-e megoldása modulo p.

A második megközelítés az indexforma faktorai közötti összefüggéseket használja fel. Ehhez persze szükséges, hogy az indexformának legyen egynél több egész együtthatós faktora, de amennyiben ez teljesül, szinte mindegyik esetben találunk olyan összefüggéseket, amelyekből nemtriviális feltételeket nyerünk a monogén testek paramétereire. Ezek az összefüggések sejtéseink szerint kapcsolatban állnak a vizsgált polinomok felbontási testének egy speciális tulajdonságával, nevezetesen, hogy a felbontási test ciklikus n-edfokú bővítése egy résztestének. Az összefüggéseket minden esetben a faktorok megfelelő hatványaiból képzett lineáris kombinációk együtthatóinak oszthatósági vizsgálatával sikerült megtalálnunk.

A fejezeteben szereplő legtöbb számtestcsaládban néhány maradékosztálytól eltekintve, minden paraméterre el tudjuk dönteni, hogy az ahhoz tartozó számtest monogén vagy sem. A legáltalánosabb eredményeket a hatodfokú gyökbővítések és a legegyszerűbb hatodfokú számtestek esetén nyertük. Az előbbi esetben megmutattuk, hogy ha m négyzetmentes, akkor a $\mathbb{Q}(\sqrt[6]{m})$ test monogenitása, csak m-nek a 36-os maradékától függ, az utóbbiban pedig azt igazoltuk, hogy ha m^2+3m+9 négyzetmentes, akkor csak $m=-4,-2,-1,1$ paraméterek esetén lesz monogén a legegyszerűbb hatodfokú számtest.

Végül a 4.3 fejezetben, a korábbi táblázatban szereplő kompozit bővítések esetén vizsgáljuk a monogenitást. Minden esetben olyan feltételeket kapunk a kompozit testek paramétereire, hogy az egyik rögzítése után a másik paraméternek csak véges sok olyan értéke lehet, amellyel a kompozit test monogén. Sőt, néhány maradékosztály esetén univerzális felső korlátot is kapunk a monogén testekhez kapcsolódó paraméterekre. Speciális esetként kapjuk, hogy az M.-L. Chang [6] által vizsgált X^3-m polinomhoz hasonlóan, néhány meghatározott paramétertől eltekintve az X^4-m és az X^6-m polinomok felbontási testei sem lehetnek monogének.

Summary

The main topic of the dissertation is the integral bases of the algebraic number fields. Efficient algorithms exsist for calculating an integral basis of a given number field. The input of most of these algorithms is the defining polynomial $f(X)$ of a primitive element α of the field. Let n be the degree of the algebraic number field over $\mathbb{Q}$, that is the degree of $f(X)$, then the integral bases calculated by the algorithms are usually of the form

$$(h_0(\alpha), h_1(\alpha), \ldots, h_{n-1}(\alpha)),$$

where $h_0, h_1, \ldots, h_{n-1} \in \mathbb{Q}[X]$ are polynomials of degree $n-1$ at most.

During the investigation of certain infinite parametric families of number fields generated by a root of an infinite parametric family of polynomials we found that with some appropriate restrictions on the parameters, the $h_i(X)$ polynomials above depend only on the remainder of the parameter modulo a suitable integer n_0. In such cases we say that the integral bases of the fields are repeating periodically modulo n_0.

The simplest example having this property is the infinite parametric family of the quadratic number fields generated by a root of $f(X) = X^2 - m$, where $m \neq 1$ is a square-free integer. It is well known that if $m \equiv 2, 3 \pmod 4$, then $(1, \sqrt{m})$, otherwise $\left(1, \frac{1+\sqrt{m}}{2}\right)$ is an integral basis of $\mathbb{Q}(\sqrt{m})$. In other words, $(h_0(\sqrt{m}), h_1(\sqrt{m}))$ form an integral basis of $\mathbb{Q}(\sqrt{m})$, where the polynomials $h_0, h_1 \in \mathbb{Q}[X]$ depend only on the remainder of m modulo 4,

$$\begin{aligned} &h_0(X) = 1, && h_1(X) = X, && \text{if } m \equiv 2, 3 \pmod 4, \\ &h_0(X) = 1, && h_1(X) = \frac{1}{2} + \frac{1}{2} \cdot X, && \text{if } m \equiv 1 \pmod 4. \end{aligned}$$

Similar phenomena occurs in some other parametric families of number fields (e.g. pure cubic [12] and pure quartic fields [19], simplest quartic fields [49]).

In the dissertation we proved this so-called periodic integral basis property for three infinite parametric families of number fields. We implicitly expanded our results for arbitrary degrees, and determined integers n_0 depending only on the degree of the field, such that the integral bases of the fields are repeating periodically modulo n_0. The related results appeared in the papers [26], [28], [58] and [59].

The investigated number fields are the following:

I. Pure number fields.
$$f_m^{(n)}(X) = X^n - m,$$
where $m \neq \pm 1$ is a square free integer.

II. Generalization of simplest cubic fields.
$$f_m^{(n)}(X) = \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot g(n-i),$$
where
$$g(i) := \begin{cases} 1, & \text{if } i \equiv 0 \pmod 6, \\ -\frac{m}{3^{v_3(n)}}, & \text{if } i \equiv 1 \pmod 6, \\ -\frac{m}{3^{v_3(n)}} - 1, & \text{if } i \equiv 2 \pmod 6, \\ -1, & \text{if } i \equiv 3 \pmod 6, \\ \frac{m}{3^{v_3(n)}}, & \text{if } i \equiv 4 \pmod 6, \\ \frac{m}{3^{v_3(n)}} + 1, & \text{if } i \equiv 5 \pmod 6, \end{cases}$$
and $v_p\left(m^2 + 3^{v_3(n)}m + 9^{v_3(n)}\right) \leq 1$ for any prime $p \neq 3$.

III. Generalization of simplest quartic fields.
$$f_m^{(n)}(X) = \sum_{i=0}^{n} \binom{n}{i} \cdot X^i \cdot g(n-i),$$
where
$$g(i) := \begin{cases} 1, & \text{if } i \equiv 0 \pmod 4, \\ -\frac{m}{2^{v_2(n)}}, & \text{if } i \equiv 1 \pmod 4, \\ -1, & \text{if } i \equiv 2 \pmod 4, \\ \frac{m}{2^{v_2(n)}}, & \text{if } i \equiv 3 \pmod 4, \end{cases}$$
and $v_p\left(m^2 + 4^{v_2(n)}\right) \leq 1$ for any prime $p \neq 2$.

In the case of pure number fields, we show in section 3.1, that if
$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_j^{k_j},$$
and
$$n_0 = p_1^{k_1+1} \cdot p_2^{k_2+1} \cdot \ldots \cdot p_j^{k_j+1},$$
then the integral bases of the fields $K = \mathbb{Q}(\sqrt[n]{m})$ are repeating periodically modulo n_0. By using the theory of Newton polygons and the method developed by

Ø. Ore [56], we first prove, that the statement above is true for prime power degrees $n = p^k$, and then we describe a method to construct an integral basis of a composite field of two pure fields of coprime degrees by combining their integral bases. This method implies that the statement is true for any degree n.

The generalizations of the simplest polynomials are investigated in section 3.2. We first prove that the splitting fields of these polynomials are cyclic extensions of degree n of an appropriate algebraic number field. This property is obviously true for the pure number fields and we conjecture that this is in connection with the periodic integral basis property, and with the coherence of the factors of the index form. Furthermore, we determined the discriminants of these polynomials as functions of their degrees and parameters, and we showed that under some assumptions, these polynomials are irreducible. These assumptions are in connection with the square-free values of irreducible quadratic polynomials of the parameters, so by the results of T. Nagell [54], there exist infinitely many appropriate parameters. With these appropriate parameters, we prove the periodic integral basis property, and we give an upper bound for the period length as a function of the degree. Moreover, for degrees $n = 2, 3, 4, 5, 6, 8, 9, 12$, we determine the shortest period length. We first investigated the generalizations of the simplest cubic fields, and then, in the same scheme, the generalizations of the simplest quartic fields. Since the proofs are the same in the two cases, we did not gone into details in the second case.

In section 3.3 we generalize the periodic integral basis property to composite fields, and we show that under certain assumptions, the composition of two families of number fields investigated in the previous sections inherits the periodic integral basis property from its subfields. We determined the smallest period length in some composite fields of smaller degrees. These fields are contained in the following table.

L	M	m_1	m_2
$X^2 - m_1$	$X^3 - m_2X^2 - (m_2 + 3)X - 1$	4	1
$X^2 - m_1$	$X^3 - m_2$	12	18
$X^2 - m_1$	$X^4 - m_2X^3 - 6X^2 + m_2X + 1$	8	16
$X^2 - m_1$	$X^4 - m_2$	8	8
$X^2 + 3$	$X^6 - m_2$	$--$	36

The integral bases of the form $(1, \alpha, \ldots, \alpha^{n-1})$, called power integral bases, have an important role among the integral bases. If there exists an algebraic intger $\alpha \in \mathbb{Z}_K$, such that α generates power integral basis, then the $\mathbb{Z}_K$ ring of integers of K, is generated by a single element over $\mathbb{Z}$, $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, i.e. $\mathbb{Z}_K$ is mono-generated, in other words, it is a monogenic ring. In order to find all of the generators of power integral bases, one has to solve a Diophantine equation, the so-called index form equation.

In Chapter 4, by using the periodic integral bases, we investigated the monogenity of some infinite parametric families of number fields of small degree from

the previous chapter. These fields are the pure fields of degrees at most 9, and the simplest cubic, quartic and sextic fields. Our aim was just to decide whether these fields are monogenic or not for certain parameters, we did not want to calculate all of the generators of power integral bases. In fact, we intended to show that if a root of a polynomial does not generate a power integral basis for a given parameter, then the field is not monogenic, i.e. there is no solution of the index form equation.

We used two different approaches for these investigations. The first is strongly related to the method of R. Dedekind [12], which uses the ramification of rational primes to prove the non-monogenity. This method is effective if and only if the field index is not equal to 1, that is there exists a prime number p such that p divides the index of any algebraic integer. In this case there is no solution of the index from equation modulo p, thus there is no integer solution. We first computed the index form, then we determined all of the possible prime divisors of the index of an algebraic integer (there are only finitely many such primes, since we gave an upper bound for the indices in these fields), and we solved the index form equations modulo these primes.

The second approach uses the coherence between the factors of the index forms. This requires reducible index forms, but if there are at least two factors, then in almost all cases we obtained some non-trivial restrictions on the parameters belonging to monogenic fields. We conjecture that these coherences between the factors are in connection with the fact that the splitting field of the polynomial is a cyclic extension of degree n of an appropriate algebraic number field. We found these coherences by investigating the factorization of certain linear combinations of the appropriate powers of the factors of the index form.

Excepting some residue classes, in most of the examples we could decide that the number belonging to the chosen parameter is monogenic or not. We obtained the most general results in the case of the pure sextic and the simplest sextic fields. In the foregoing case we proved that if m is square-free, then the monogenity of the fields $\mathbb{Q}(\sqrt[6]{m})$ depends only on the remainder of m modulo 36. In the latter case we proved that if $m^2 + 3m + 9$ is square-free, then these fields can be monogenic only if $m = -4, -2, -1, 1$.

Finally, in section 4.3, we investigated the monogenity of the composite fields contained in the table above. In all of the cases, we obtained that by fixing one of the parameters, the other can have only finitely many values for which the composite field can be monogenic. Moreover, for some residue classes we got a universal upper bound for the parameters belonging to monogenic fields. As a special case, we proved that similarly to the splitting field of $X^3 - m$ investigated by M.-L. Chang [6], the splitting field of $X^4 - m$ and $X^6 - m$ can not be monogenic, except for some specific parameters.

Irodalomjegyzék

[1] T. Arnóczki, G. Nyul, *On a conjecture concerning the minimal index of pure quartic fields*, (submitted)

[2] A. Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge 1990.

[3] L. Bernardin, P. Chin, P. DeMarco, K. O. Geddes, D. E. G. Hare, K. M. Heal, G. Labahn, J. P. May, J. McCarron, M. B. Monagan, D. Ohashi and S. M. Vorkoetter, *Maple Programming Guide.* Maplesoft, a division of Waterloo Maple Inc., 1996–2020.

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

[5] B. J. Birch and J. R. Merriman, *Finiteness theorems for binary forms with given discriminant*, Proc. Lond. Math. Soc. **24** (1972) 385–394.

[6] M.-L. Chang, *Non-monogenity in family of sextic fields*, J. Number Theory **97** (2002) 252–268.

[7] M.-L. Chang, *Monogeneity in biquadratic fields.* Int. J. Pure Appl. Math. **31 (4)** (2006) 481–490.

[8] H. Cohen, *A course in computational algebraic number theory*, Springer, 2013.

[9] H. Cohn, *A device for generating fields of even class number*, Proc. Amer. Math. Soc. **7** (1956) 595–598.

[10] J.P.Cook, *Computing Integral Bases*, `https://12c5f6ec-39bc-67f0-3029-0905a40b98eb.filesusr.com/ugd/18f425_58e29a3ba780690f4b00fd9f66a5c529.pdf`

[11] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie höhere Congruenzen*, Abh. König. Ges. der Wissen. zu Göttingen, **23** (1878) 3–38.

[12] R. Dedekind, *Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. **121** (1900) 40–123.

[13] V. Ennola, *Cubic number fields with exceptional units*, Computational number theory, Proc. Colloq., Debrecen/Hung., **1989** (1991) 103–128.

[14] V. Ennola, *Fundamental units in a family of cubic fields*, Journal de théorie des nombres de Bordeaux, **16.3** (2004) 569–575.

[15] P. Erdős, *Arithmetical properties of polynomials*, Journal of the London Mathematical Society, **Vol. s1-28 (4)** (1953) 416–425.

[16] J. H. Evertse and K. Győry, *Unit equations in Diophantine number thoery*, Cambridge University Press, 2015.

[17] J. H. Evertse and K. Győry, *Discriminant equations in Diophantine number theory*, Cambridge University Press, 2017.

[18] K. Foster, *HT90 and "simplest" number fields*, Illinois J. Math., **55(4)** (2011) 1621–1655.

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

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

[21] I. Gaál, *Diophantine equations and power integral bases*, Birkhäuser, 2002.

[22] I. Gaál, *Diophantine equations and power integral bases. Theory and algorithms. 2nd edition.*, Birkhäuser, 2019.

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

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

[25] I. Gaál and G. Petrányi, *Calculating all elements of minimal index in the infinite parametric family of simplest quartic fields*, Czech Math J **64** (2014) 465-–475.

[26] I. Gaál and L. Remete, *Integral bases and monogenity of pure fields*, J. Number Theory **173** (2017) 129–146.

[27] I. Gaál and L. Remete, *Non-monogenity in family of octic fields*, Rocky Mt. J. Math. **47**(3) (2017) 817–824.

[28] I. Gaál and L. Remete, *Integral bases and monogenity of the simplest sextic fields*, Acta. Arith. **183**(2) (2018) 173–183.

[29] I. Gaál and L. Remete, *Integral bases and monogenity of composite fields*, Exp. Math. **28**(2) (2019) 209-222.

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

[31] T. A. Gassert, *A note on the monogeneity of power maps.* Albanian J. Math. **11** (2017) 3–12.

[32] T. A. Gassert, H. Smith and K. E. Stange, *A family of monogenic S_4 quartic fields arising from elliptic curves.* J. Number Theory **197** (2019) 361–382.

[33] F. Q. Gouvêa, *p- adic numbers: An introduction.* Springer Verlag, 1993.

[34] M. N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de* $\mathbb{Q}$, Publ. Math. Fac. Sci. Besançon, Théor. Nombres, **2** (1977-1978), 1–79.

[35] M. N. Gras, *Families of units in real cyclic extensions of* $\mathbb{Q}$ *of degree 6*, Publ. Math. Fac. Sci. Besançon, Théor. Nombres **1984/85-1985/86** (1986), Exp. No. 2, 27 p.

[36] K. Győry, *Sur les polynômes à coeffiecients entiers et de discriminant donne*, Acta Arith. **23** (1973), 419–426.

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

[38] M. Hall, *Indices in cubic fields*, Bull. Amer. Math. Soc. **43(2)** (1937) 104–108.

[39] A. Hameed and T. Nakahara, *Integral bases and relative monogenity of pure octic fields.* Bull. Math. Soc. Sci. Math. Roum., Nouv. Sér. **58 (106)**, No. 4 (2015) 419–433.

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

[41] A. Hoshi, On the simplest sextic fields and related Thue equations, *Funct. Approximatio, Comment. Math.,* **47** (2012), no. 1, 35–49.

[42] A. Hoshi, *Complete solutions to a family of Thue equations of degree 12*, J. Théor. Nombres Bordx., **29 (2)** (2017), 549–568.

[43] L. Jones, *A brief note on some infinite families of monogenic polynomials.* Bull. Aust. Math. Soc. **100 (2)** (2019) 239–244.

[44] L. Jones, *Monogenic polynomials with non-squarefree discriminant.* Proc. Am. Math. Soc. **148 (4)** (2020) 1527–1533.

[45] L. Jones and T. Phillips, *Infinite families of monogenic trinomials and their Galois groups.* Int. J. Math. **29 (5)** (2018) 11 p.

[46] J. König, *A note on families of monogenic number fields.* Kodai Math. J. **41 (2)** (2018) 456–464.

[47] E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, Journal für die reine und angewandte Mathematik. **44** (1852) 93—146.

[48] M. J. Lavallee, B. K. Spearman and K. S. Williams, *Lifting monogenic cubic fields to monogenic sextic fields.* Kodai Math. J. **34 (3)** (2011) 410–425.

[49] J. H. Lee, *Evaluation of the Dedekind zeta function at s=-1 of the simplest quartic fields*, Journal of Number Theory, **143** (2014) 24–45.

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

[51] G. Lettl, A. Pethő and P. Voutier, *On the arithmetic of simplest sextic fields and related Thue equations*, Number Theory: Diophantine, Computational and Algebraic Aspects (K. Győry, A. Pethő and V.T. Sós, eds.), Walter de Gruyter Publ. Co. (1998), 331–348.

[52] J. Montes and E. Nart, *On a Theorem of Ore*, Journal of Algebra, **146** (1992) 318–334.

[53] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers. 3rd ed.*, Springer Monogr. Math. (2004).

[54] T. Nagell, *Zur Arithmetik der Polynome*, Abhandl. Math. Sem. Hamburg **1** (1922) 179–194.

[55] G. Nyul, *Non-monogenity of multiquadratic number fields.* Acta Math. Inform. Univ. Ostrav. **10 (1)** (2002) 85–93.

[56] Ø. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper,* Math. Ann. **99** (1928) 84–117.

[57] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, (1989).

[58] L. Remete, *Integral bases and monogenity of pure fields with square-free parameter*, Stud. Sci. Math. Hung. **57**(1) (2020) 91-115

[59] L. Remete, *A generalization of simplest number fields and their integral basis*, Acta Math. Hungar. **163 (2)** (2021) 437–461.

[60] D. Shanks, *The simplest cubic fields*, Math. Comput. **28** (1974) 1137–1152.

[61] H. Smith, *Two families of monogenic S4 quartic number fields.* Acta Arith. **186 (3)** (2018) 257–271.

[62] B. K. Spearman, *Monogenic A4 quartic fields.* Int. Math. Forum **1** (2006) 1969–1974.

NEMZETI KUTATÁSI, FEJLESZTÉSI
ÉS INNOVÁCIÓS HIVATAL

AZ INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTÉRIUM
ÚNKP-20-3-II KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG
PROGRAMJÁNAK A NEMZETI KUTATÁSI,
FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL
FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL
KÉSZÜLT.