Doktori (Phd) értekezés tézisei

Algebrai számtestek egész bázisa és monogenitása

Remete László

Témavezető: Dr Gaál István

Debreceni Egyetem
Matematika- és számítástudományok doktori iskola

Debrecen, 2021

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 függően kétféle lehet. 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.

Ez a jelenség a másodfokú testeken kívül eddig csak nagyon kevés számtestben bukkant fel (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.

A periodikus egész bázis tulajdonság felhasználásával, végtelen parametrikus számtestcsaládok monogenitásával kapcsolatban is nyerhetünk eredményeket. Ezekhez az eredményekhez 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 ráadásul ez 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 gyűjtöttük össze. Az első részben az egész bázis meghatározásához, és a periodikus egész bázis igazolásához használt eljárásokat foglaljuk össze, majd precízen definiáljuk a periodikus egész bázis tulajdonságot. A fejezet második részében, az indexforma kiszámításához, és az egész együtthatós faktorizációjához kapcsolódó módszereket ismertetjük.

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

A 3. fejezetben megmutatjuk, hogy az egész bázis mindhárom család esetben periodikusan ismétlődik. A megfelelő paraméterekhez tartozó gyökbővítések esetén megadjuk a legkisebb periódushosszt, a legegyszerűbb testek kétféle általánosításai 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 a 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]). Az utolsó részben alacsonyabb fokú kompozit bővítések monogenitását vizsgáljuk az előző részben 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]).

A 2. fejezet definíciói közül az alábbiakban röviden részletezem a periodikus egész bázis, az index és az indexforma fogalmát, amelyek nélkülözhetetlenek az eredmények megfogalmazásához.

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.

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. Megmutatható, hogy

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

ahol $D_{K/\mathbb{Q}}(\alpha)$ az α, D_K pedig a K diszkriminánsa. Az index lényegében azt mutatja meg, hogy az α hatványai által generált bázis mennyire tér el a test egy egész bázisától.

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.

Lemma. *A fenti jelölések mellett,*

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

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

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

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

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

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

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 $(x_2,\dots,x_n) \in \mathbb{Z}^{n-1}$ megoldása az

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

ún. *indexforma egyenletnek*.

Végtelen parametrikus számtestek egész bázisai

A fejezetben három számtestcsaládot vizsgálunk, a gyökbővítéseket és a legegyszerűbb számtestek kétféle általánosításaként kapott számtesteket. Mindkét esetben sikerült a fokszámtól függő olyan n_0 konstanst találnunk, hogy a végtelen parametrikus számtest egész bázisa periodikusan ismétlődik modulo n_0. A három számtestcsaládban nyert eredmények összefűzésével, ezen számtestek kompozítumaiban is lehetőség nyílt az egész bázis periodikus tulajdonságának igazolására.

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.

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 megmutatjuk, hogy a tételben szereplő n_0 a legkisebb megfelelő periódushossz, amely szerint a $K = \mathbb{Q}(\sqrt[n]{m})$ gyökbővítések egész bázisa periodikusan ismétlődik.

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 $t \in \mathbb{N}$ 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.

A $\mathbb{Q}(\sqrt[n]{m})$ egész bázisát ezeknek a $\frac{h_t^{(r)}(\sqrt[n]{m})}{p^t}$ algebrai egészeknek segítségével fogjuk megkonstruálni.

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

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

ha pedig $k \le s$, akkor

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

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

Ennek következményeként kapjuk a periodikus egész bázis tulajdonságot.

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

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.

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*

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

Ezt a lemmát felhasználva most már össze tudjuk fűzni a két kisebb test egész bázisát a nagyobb test egy egész bázisává. 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 egész bázis csak a résztestek egész bázisainak alakjától függ, ezért prímtényezők szerinti teljes indukcióval adódik az általános tétel bizonyítása.

Ahhoz, hogy az így kapott periódushossz a legkisebb, azt kell észrevegyük, hogy ha az egész bázis periodiksan ismétlődik modulo n_0, akkor az $\sqrt[n]{m}$ indexe is periodikusan ismétlődik modulo n_0. Továbbá egyszerű példával igazolható, hogy $n = p^k$ prímhatványfokú gyökbővítések esetén az $\sqrt[n]{m}$ szám p-indexe periodikusan ismétlődik modulo p^{k+1}, de nem ismétlődik modulo p^k. Az előző lemmát felhasználva ebből már következik, hogy a tételben előírt n_0 valóban a legkisebb megfelelő periódushossz.

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.

Legegyszerűbb testek általánosításai és egész bázisai

A fejezethez kapcsolódó eredmények a [28] és [59] cikkben jelentek meg. Két esetet fogunk vizsgálni, az első a legegyszerűbb harmadfokú 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

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

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. Először megmutatjuk, hogy egy alkalmas Möbius transzformáció tranzitíven permutálja $f_t^{(n)}(X)$ gyökeit.

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.

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

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.

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

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

Ezután belátjuk az alábbi kulcsfontosságú tételt.

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 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

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

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 $n = 3$ 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 (ld. A. Hoshi [42]).

Az állításaink egyszerűbb megfogalmazása érdekében azt mondjuk, hogy $m \in \mathbb{Z}$ *megfelelő* paraméter, 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.

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

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

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

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

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 sokkal jobb korlátokat kaphatunk az egész bázisok periódusának hosszára. Ezek az új korlátok bizonyos kis fokszámok esetén már lehetőséget adtak arra, hogy minden megfelelő 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.

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 $f_m^{(n)}(X)$ polinom 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 [42]

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

Most következik a másik általánosítás, ami a legegyszerűbb negyedfokú polinomokat foglalja magába. A gondolatmenet teljesen hasonló lesz, mint az előző általánosítás esetén. Legyenek $g, h : \mathbb{N} \mapsto \mathbb{Q}$ az alábbi módon értelmezett függvények

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

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

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

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.

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.

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

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

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 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.

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

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

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*

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

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.

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.

Kompozitum testek egész bázisai

Ebben a fejezetben a korábban felmerülő nevezetes számtestcsaládok kompozíciójaként kapott számtestekben vizsgáljuk az egész bázisokat. Megmutatjuk, hogy megfelelő feltételek mellett a résztestek periodikus egész bázis tulajdonsága bizonyos értelemben öröklődik a kompozit testre is.

A következő táblázatban összefoglaljuk, hogy a vizsgált három polinomcsalád által definiált számtest családokból képzett kompozit testek paramétereire az eredeti feltételek mellett még mit követelünk meg, ahhoz, hogy az egész bázis periodikusan ismétlődjön. 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.*	$\mathrm{lnko}(m_1, m_2) \mid n_1 \cdot n_2$
I.	*II.*	$\mathrm{lnko}\,(m_1, s(m_2, n_2)) \mid n_1 \cdot n_2$
I.	*III.*	$\mathrm{lnko}\,(m_1, t(m_2, n_2)) \mid n_1 \cdot n_2$
II.	*II.*	$\mathrm{lnko}\,(s(m_1, n_1), s(m_2, n_2)) \mid n_1 \cdot n_2$
II.	*III.*	$\mathrm{lnko}\,(s(m_1, n_1), t(m_2, n_2)) \mid n_1 \cdot n_2$
III.	*III.*	$\mathrm{lnko}\,(t(m_1, n_1), t(m_2, n_2)) \mid n_1 \cdot n_2$

I.: Gyökbővítések
II.: Legyegyszerűbb számtestek első általánosításai
III.: Legyegyszerűbb számtestek második általánosításai

Következmény. *A fenti táblázat feltételei mellett a $K = LM$ kompozit testek egész bázisai periodikusan ismétlődnek.*

A különböző esetekben

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

értékének felső becsléseivel 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 redukció 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 túlzottan 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.

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.

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 megoldani. 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 kipróbálnunk, hiszen mindegyiknél adtunk felső korlátot a testet generáló elem indexére.

A másik megközelítés az indexforma faktorai közötti kapcsolatra épül, és akkor bizonyul hatékonynak, amikor K-nak van valódi részteste. 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.

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 $K = \mathbb{Q}(\alpha)$. Az α-hoz tartozó Hermite normál alakú egész bázis alakja csak m-nek a 9-es maradékától függ, és 3 különböző esetet eredményez. Az első esetben, amikor $v_3(m^3 - m) = 1$, akkor α hatvány egész bázist generál, a többi esetben megadható végtelen sok oylan paraméter, amellyel monogén testet kapunk, de azt sejtjük, hogy végtelen sok olyan paraméter is létezik, amelyekkel nem kapunk monogén testet.

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.

Ebben az esetben ha $m = 16k + r$ 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 Arnóczki Tímea és Nyul Gábor [1] megmutatták, hogy ha igaz az ABC-sejtés, akkor létezik végtelen sok monogén és nem monogén test is.

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. Azokban az esetekben, amikor α nem generál hatvány egész bázist (azaz, ha $v_5(m^5 - m) > 1$), azt sejtjük, hogy létezik végtelen sok monogén és végtelen sok nem monogén testet szolgáltató paraméter is.

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 $K = \mathbb{Q}(\alpha)$. Az α-hoz tartozó Hermite normál alakú egész bázis alakja csak m-nek a 36-os maradékától függ, és 6 különböző esetet eredményez. Ebben az esetben ha $m = 36k + r$ négyzetmentes, akkor a $K = \mathbb{Q}(\sqrt[6]{m})$ test $r = 2, 3, 6, 7, 11, 14, 15, 22, 23, 30, 31, 34$ esetén 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 $v_7(m^7 - m) = 1$ 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.

Legyen $m \neq 0, 1$ négyzetmentes egész, α az $X^8 - m$ gyöke és $K = \mathbb{Q}(\alpha)$. Az α-hoz tartozó Hermite normál alakú egész bázis alakja csak m-nek a 16-os maradékától függ, és 4 különböző esetet eredményez. Ekkor, 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.

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. Legyen $m = 27k + r$ négyzetmentes, ekkor ha $r = 2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 16,\ 20, 21, 22, 23, 24, 25$, akkor K monogén, ha $r = 8, 10, 17, 19$, akkor nem monogén, a többi esetben pedig a azt sejtjük, hogy végtelen sok monogén és végtelen sok nem monogén test létezik.

Legegyszerűbb testek monogenitása

A legegyszerűbb testek általánosításai 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 $v_p(m^2+16)<2$, vagyis m^2+16 nem osztható semmilyen páratlan prím négyzetével.

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. 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. 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. 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 fel van sorolva Gaál István [20] cikkében.

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 megfelelő feltételek mellett 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.

Az általunk vizsgált összes esetben olyan összefüggés áll majd fenn az indexforma faktorai 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.

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. A két eset és a monogén testek paramétereihez kapcsolódó feltételek az alábbi táblázatban szerepelnek.

$m_1 \pmod 4$	1. feltétel	2. feltétel
$2, 3$	$4m_1 \mid m_2^2 + 3m_2 + 9 \pm 1$	$m_2^2 + 3m_2 + 9 \mid 64m_1^3 \pm 1$
1	$m_1 \mid m_2^2 + 3m_2 + 9 \pm 1$	$m_2^2 + 3m_2 + 9 \mid m_1^3 \pm 1$

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 $I(\alpha, \beta) \mid \mathrm{lnko}(D(\alpha)^3, D(\beta)^2)$, 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 $m_1 = -3$ lehetőség, amiből 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

$$X^4 - m_2X^3 - 6X^2 + m_2X + 1$$

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 $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2, \beta^3, \alpha\beta^3)$-höz tartozó Hermite normál alakú egész bázis periodikusan ismétlődik m_1-ben modulo 8 és m_2-ben modulo 16. 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. Most az $m_1 = -1$ eset a fejezetben kissé kilóg a sorból, ilyenkor ugyanis az általunk alkalmazott módszerekkel nem tudtuk igazolni, hogy a 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 $m_1 \neq 1$ 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. 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. Az indexforma ekkor még tovább bomlik, és az új faktorok között további hatékony összefüggéseket találhatunk. Összességében azt kapjuk, hogy a monogén testekhez tartozó lehetséges paraméterek: $m_2 = \pm 2, \pm 3, \pm 5$. Ezek közül ± 2, 3 és -5 esetekről a [27] cikkben megmutatjuk, hogy a kompozit test nem monogén, és ugyanezt sejtjük a kimaradt $m_2 = -3$ és $m_2 = 5$ esetén is 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 indexforma faktorai közötti összefüggéseket felhasználva, megmutattuk, hogy ha a test monogén, akkor m lehetséges értékei $-15, -6, -3, -2, 1, 2, 3, 5, 6$. Ezek közül az 1 és a -3 eleve ki volt zárva, így azt kaptuk, hogy $m \neq -15, -6, -2, 2, 3, 5, 6$ esetén a $K = \mathbb{Q}(i\sqrt{3}, \sqrt[6]{m})$ testek nem monogének.

Short thesis for the degree of doctor of philosophy (PhD)

Integral bases and monogenity of algebraic number fields

Remete László

Supervisor: Dr Gaál István

University of Debrecen
Doctoral School of Mathematical and Computational Sciences

Debrecen, 2021

Introduction

The main topic of the dissertation is the integral bases of algebraic number fields. The construction of an integral basis of a given number field is an easy task. The problem is more fascinating in the case of infinite parametric families of number fields.

In my thesis, we investigate infinite parametric families of number fields generated by roots of infinite parametric families of polynomials. The case of quadratic number fields provides an excellent example. These fields are generated by a root of $f_m(X) = X^2 - m$, where m is a square-free integer. The integral bases of such fields depend on the remainder of the parameter m modulo 4. If $m \equiv 2, 3 \pmod 4$, then $(1, \sqrt{m})$, and if $m \equiv 1 \pmod 4$, then $\left(1, \frac{1+\sqrt{m}}{2}\right)$ form an integral basis of $\mathbb{Q}(\sqrt{m})$.

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 to 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 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 fflα generates a power integral basis, then $\mathbb{Z}_K$, the 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.

The investigation of the monogenity of number fields is a classical topic of the algebraic number theory, which goes back to the work of R. Dedekind [12] and H. Hasse [40].

Using the periodic integral basis property, we obtained results in connection with the monogenity of infinite parametric families of number fields. We utilize the method of R. Dedekind [11], the theory of Newton polygons (see [33], Chapter 6.4), the theorem of the index by Ø. Ore [56] and the factorization of the index form to reach these result.

We do not intend to determine all of the generators of power integral bases, we just try to decide for which parameters can the field be monogenic. Our aim is to show that if the root of the polynomial does not generate a power integral basis for a given parameter, then the field is not monogenic. Recently, this approach became more popular, several articles deal with the monogenity of infinite parametric families of number fields (see [44], [43], [29], [32], [61], [46], [28], [45], [31], [27], [26], [39], [48], [62], [7], [55], [6])

This method is more general than the classical approach in the sense that it yields results for infinitely many number fields simultaneously. In most of the cases we investigated, this approach works efficiently. For example, in the case of pure sextic fields, we proved that if the root of the polynomial $X^6 - m$ does not generate power integral basis, then the field can not be monogenic (see [26]). This condition depends only on the remainder of the parameter m modulo 36, thus we described all of the monogenic pure sextic fields belonging to square-free parameters.

In the second chapter of the dissertation we collected the applied methods and statements. The first part consists of the methods and procedures used for the calculations of the integral basis and the proof of the periodicity of the integral basis. In the second part of the chapter we briefly introduce the methods in connection with the calculation of the index form and its factorization.

The third and fourth chapter of the dissertation contains the results about the three infinite parametric families of number fields. These results are published in papers [26], [27], [28], [29], [58] and [59].

In Chapter 3, we show that the integral bases of these fields are repeating periodically. In the case of pure number fields we give the smallest period length, in the case of the two different generalizations of the simplest number fields we give a general upper bound for the period length, and we calculate the smallest period length for some cases of small degrees. We prove that the splitting fields of these parametric polynomials are cyclic extensions of a certain algebraic number fields (this is trivially true for the pure number fields), because we conjecture that it is closely related to the periodic integral basis property and the connections between the factors of the index form, used in the investigation of the monogenity. Finally, 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.

In Chapter 4, by using the periodic integral bases, we investigated the monogenity of some infinite parametric families of number fields of small degrees from the previous chapter. These fields are the pure fields of degree at most 9, and the simplest cubic, quartic and sextic fields. Except for some residue classes, in most of the examples we could decide if the number fields belonging to the chosen parameter is monogenic or not (see [26], [27], [28]). In the last section, we investigated the monogenity of composite fields of small degrees, using the same tools as in the previous section, and we get similar general results (see [29]). 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.

The corresponding calculations were implemented in the Maple computer algebra software, which is very effective for these symbolic computations (see [3]).

We briefly recall some definitions from Chapter 2, which are necessary to formulate the results.

Definition. Let $f_m(X) \in \mathbb{Z}[m][X]$ be a polynomial of degree n, where $m \in \mathbb{Z}$ is an integer parameter. Let α_m be a root of $f_m(X)$ and $K = \mathbb{Q}(\alpha_m)$. We say that the integral bases of the fields K are repeating periodically modulo n_0, if for any residue class $r = 0, \ldots, n_0 - 1$ there are polynomials $h_i^{(r)}(X) \in \mathbb{Q}[X]$, $(i = 0, \ldots, n-1)$, such that if $m \equiv r \pmod{n_0}$ and $f_m(X)$ is irreducible, then the algebraic numbers

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

form an integral basis of K.

It is very important in the definition that the fields are generated by the roots of an infinite parametric family of polynomials. Without this construction, it makes no sense to speak about periodic integral bases. We can say that this property, in fact, belongs to a family of polynomials, not to a family of number fields.

If α is a primitive algebraic integer in K, then $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ is a basis of K over $\mathbb{Q}$ consisting of algebraic integers. Moreover, the $\mathbb{Z}$-module generated by the elements $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ coincides with the additive group of the ring extension $\mathbb{Z}[\alpha]$. The module index

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

is called the index of α, and is denoted by $I(\alpha)$. It can be shown that

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

where $D_{K/\mathbb{Q}}(\alpha)$ is the discriminant of α and D_K is the discriminant of K. In fact, the index tells us how far is the basis generated by the powers of α from an integral basis of the field.

Let $(\omega_1 = 1, \omega_2, \ldots, \omega_n)$ be an integral basis of K. Then

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

is called the linear form corresponding to the integral basis above. Let

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

be the relative conjugates of the linear form $L(\underline{X})$ and let

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

be the discriminant of $L(\underline{X})$.

Lemma. *Using the notation above*

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

where $I(X_2,\ldots,X_n)$ is a homogeneous linear from of degree $\frac{n(n-1)}{2}$ in $(n-1)$ variables with integer coefficients.

This $I(X_2,\ldots,X_n)$ form is called the index form corresponding to the integral basis $(1,\omega_2,\ldots,\omega_n)$. The most important property of the index form is that for an arbitrary n-touple

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

where $\alpha = x_1 + x_2\omega_2 + \ldots \omega_n \in \mathbb{Z}_K$ is a primitive element of K, the following holds,

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

This means that $\alpha = x_1 + x_2\omega_2 + \ldots \omega_n \in \mathbb{Z}_K$ generates power integral basis in K, if and only if $(x_2,\ldots,x_n) \in \mathbb{Z}^{n-1}$ is a solution of the so-called index form equation below,

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

Integral bases of infinite parametric families of number fields

In this section we investigate the integral bases of three infinite parametric families of number fields, these are the pure fields and the two different generalizations of the simplest number fields. In both cases, we found a constant n_0 depending on the degree n, for which the integral bases of the infinite parametric families of number fields repeating periodically. By combining the results of these sections, we proved the periodic integral basis property for composition of these fields.

Integral bases of pure fields

The related results appeared in the papers [26] és [58]. Let $n \geq 2$ and $m \neq 0, \pm 1$ be integers. Then the fields $K = \mathbb{Q}(\sqrt[n]{m})$ are called pure number fields.

Theorem. *Let $m \neq 0, \pm 1$ be a square-free integer, $n \geq 2$ be an integer, with prime factorization*

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

and let

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

Then the integral bases of $K = \mathbb{Q}(\sqrt[n]{m})$ are repeating periodically modulo n_0.

The proof consists of multiple steps. First we show that the statement is true for degrees $n = p^k$, where p is a prime. We give n linearly independent algebraic integers, such that the discriminant of the basis generated by them coincides with the discriminant of the field. After this, we show how to compose an integral basis of pure number fields of coprime degrees n_1 and n_2 to obtain an integral basis of the pure number field of degree $n_1 \cdot n_2$. Finally, we show that the period length n_0 given in the theorem is indeed the smallest appropriate period length.

Lemma. *Using the notation above, let r be the reaminder of m modulo p^{k+1} and let $s := v_p(m^p - m) - 1$. For $t \in \mathbb{N}$, let $h_t^{(r)}(X) \in \mathbb{Z}[X]$ given by the following formula*

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

Then

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

is an algebraic integer for any $0 \leq t \leq \min\{s, k\}$.

We will use these algebraic integers to construct an integral basis of $\mathbb{Q}(\sqrt[n]{m})$.

Lemma. *Using the notation above, let* $\alpha = \sqrt[n]{m}$. *If* $s < k$, *then*

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

else

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

is an integral basis of $\mathbb{Q}(\sqrt[n]{m})$.

This implies the periodic integral basis property for pure fields of prime power degree.

Corollary. *Using the notation above, the integral bases of* $\mathbb{Q}(\sqrt[n]{m})$ *are repeating periodically modulo* p^{k+1}.

The next step is to compose the integral bases of pure fields of coprime degrees. In order to do this, we proved the following theorem on the indices of the generators.

Lemma. *Let* $m \neq 0, \pm 1$ *be a square-free integer,* $2 \leq n_1, n_2$ *be coprime integers, and let* $n = n_1 \cdot n_2$. *Then*

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

Applying this lemma, we can compose the integral bases of two subfields of coprime degrees. Moreover, since the integral bases are repeating periodically modulo p^{k+1} for degree p^k, and in the construction above we use these integral bases, the main result arises by mathematical induction on prime factors.

Integral bases of generalizations of simplest number fields

The related results are published in [59] and [28]. We introduce two different generalizations. The first contains the simplest cubic and sextic fields, and the family of Hoshi of degree 12, and the second one involves the simplest quartic fields. From now on, let t be a rational parameter.

Let $g, h : \mathbb{N} \mapsto \mathbb{Q}$ be functions defined by

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

For $n \geq 0$, let

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

and let $r^{(n)}(X)$ be the derivative of $f_t^{(n)}(X)$ corresponding to the variable t, that is

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

These polynomials have many interesting properties. Among others, we show that an appropriate Möbius-transformation transitively permutes the roots of $f_t^{(n)}(X)$.

Theorem. *Let $n \geq 2$ be an integer, α be a root of $f_t^{(n)}(X)$ and β be a root of $r^{(n)}(X)$. Then*

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

is also a root of $f_t^{(n)}(X)$.

By this theorem, the following property on the splitting fields of the polynomials $f_t^{(n)}(X)$ holds, which is in connection with the periodic integral basis property by our conjecture.

Theorem. *Let $n \geq 2$ be an integer,*

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

where ε_3 is a primitive third and ε_n is a primitive n-th root of unity. Then the splitting field of $f_t^{(n)}(X)$ is a cyclic extension of $\mathbb{Q}(\beta)$. Moreover, if $f_t^{(n)}(X)$ is irreducible, and α is one of its roots, then the splitting field of $f_t^{(n)}(X)$ is $\mathbb{Q}(\alpha,\beta)$, which is a cyclic extension of $\mathbb{Q}(\beta)$ of degree n.

Proposition. *If $n \geq 2$, then the discriminant of $f_t^{(n)}(X)$ is*

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

After this, we prove the following significant theorem.

Theorem. *If $p \neq 3$ is a prime, such that $v_p(t^2+t+1) = 1$, then $f_t^{(n)}(X)$ is irreducible. Furthermore, if t is a rational parameter, such that $f_t^{(n)}(X)$ has integer coefficients, and α is a root of $f_t^{(n)}(X)$, then p does not divide the index of α in the field $\mathbb{Q}(\alpha)$.*

From now on, let t be a rational parameter, such that $f_t^{(n)}(X)$ has integer coordinates. In fact, it means that

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

where $m \in \mathbb{Z}$. Hence, we write $f_m^{(n)}(X)$ instead of $f_t^{(n)}(X)$ to refer to the substitution above. With this notation, $f_m^{(n)}(X)$ has integer coordinates, if and only if $m \in \mathbb{Z}$. We remark, that for $n = 3$ and $n = 6$, $f_m^{(n)}(X)$ is the family of simplest cubic and sextic polynomials, thus we indeed obtained a generalization of these fields. Moreover, for $n = 12$, we get the family of polynomials defined by A. Hoshi [42].

To simplify our statements, we say that $m \in \mathbb{Z}$ is an appropriate parameter, if for any prime $p \neq 3$,

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

That is, the 3-free part of t^2+t+1 is square-free. We remark, that since t^2+t+1 is an irreducible polynomial in $\mathbb{Q}[t]$, then by the results of T. Nagell [54], there exist infinitely many appropriate parameters m.

Theorem. *Let $m \in \mathbb{Z}$ be an appropriate parameter and α be a root of $f_m^{(n)}(X)$. Then*

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

Since $I(\alpha) \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha]$, then this theorem implies the periodic integral basis property, and we can give an upper bound for the period length.

Corollary. *Let $m \in \mathbb{Z}$ be an appropriate parameter and α be a root of $f_m^{(n)}(X)$. Then the integral bases of the fields $K = \mathbb{Q}(\alpha)$ are repeating periodically modulo n_0, where n_0 is the greatest integer such that*

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

This period length can be huge even for small degrees, but using the dual basis method, we can improve our estimates for some given degrees. We performed these calculations for degrees $n = 2, 3, \ldots, 12$.

Proposition. *Let $m \in \mathbb{Z}$ be an appropriate parameter, α is a root of $f_m^{(n)}(X)$ and $K = \mathbb{Q}(\alpha)$. Then, by calculating the dual basis of $(1, \alpha, \ldots, \alpha^{n-1})$ and by applying the estimate*

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

we get that $C_n \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha]$, where

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

.

From these better C_n constants we can derive much better estimates for the period length. In some cases, these better bounds allow us to calculate the Hermite normal form integral basis belonging to α in each residue class, and to determine the smallest period length. We did this task for degrees $n = 2, 3, 4, 5, 6, 8, 9$ and 12, under the additional condition $v_3(m^2 + 3^{v_3(n)}m + 9^{v_3(n)}) \leq 1$. This restriction makes the result less general, but it decreases the period length with a power of 3, and after it, there would be easier to use the result.

Corollary. *Let $m \in \mathbb{Z}$ be an integer, such that $m^2 + 3^{v_3(n)}m + 9^{v_3(n)}$ is square-free and let α be a root of $f_m^{(n)}(X)$. Then the integral bases of the fields $K = \mathbb{Q}(\alpha)$ are repeating periodically modulo n_0 for $n = 2, 3, 4, 5, 6, 8, 9, 12$, where*

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

.

These cases contain the three infinite parametric families investigated formerly.

- Simplest cubic polynomials

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

- Simplest sextic polynomials

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

- Infinite family of A. Hoshi [42]

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

The next is the other generalization of simplest number fields, which contains the simplest quartic fields. The method is the same as in the previous generalization. Let $g, h : \mathbb{N} \mapsto \mathbb{Q}$ be functions defined by

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

For $n \geq 0$, let

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

and let $r^{(n)}(X)$ be the derivative of $f_t^{(n)}(X)$ corresponding to the variable t, that is

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

Theorem. *Let $n \geq 2$ be an integer, α be a root of $f_t^{(n)}(X)$ and β be a root of $r^{(n)}(X)$. Then*

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

is also a root of $f_t^{(n)}(X)$.

Theorem. *Let $n \geq 2$ be an integer,*

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

where ε_n is a primitive n-th root of unity. Then the splitting field of $f_t^{(n)}(X)$ is a cyclic extension of $\mathbb{Q}(\beta)$. Moreover, if $f_t^{(n)}(X)$ is irreducible, and α is one of its roots, then the splitting field of $f_t^{(n)}(X)$ is $\mathbb{Q}(\alpha, \beta)$, which is a cyclic extension of $\mathbb{Q}(\beta)$ of degree n.

Proposition. *If $n \geq 2$, then the discriminant of $f_t^{(n)}(X)$ is*

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

Theorem. *If $p \neq 2$ is a prime, such that $v_p(t^2+1) = 1$, then $f_t^{(n)}(X)$ is irreducible. Furthermore, if t is a rational parameter, such that $f_t^{(n)}(X)$ has integer coefficients, and α is a root of $f_t^{(n)}(X)$, then p does not divide the index of α in the field $\mathbb{Q}(\alpha)$.*

From now on, let t be a rational parameter, such that $f_t^{(n)}(X)$ has integer coordinates. In fact, it means that

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

where $m \in \mathbb{Z}$. Henceforth, we write $f_m^{(n)}(X)$ instead of $f_t^{(n)}(X)$ to refer to the substitution above. With this notation, $f_m^{(n)}(X)$ has integer coordinates, if and only if $m \in \mathbb{Z}$. We remark, that for $n = 4$, $f_m^{(n)}(X)$ is the family of simplest quartic polynomials, thus we indeed obtained a generalization of these fields.

To simplify our statements, we say that $m \in \mathbb{Z}$ is an appropriate parameter, if for any prime $p \neq 2$,

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

That is, the 2-free part of t^2+1 is square-free. We remark, that since t^2+1 is an irreducible polynomial in $\mathbb{Q}[t]$, then by the results of T. Nagell [54], there exist infinitely many appropriate parameters m.

Theorem. *Let $m \in \mathbb{Z}$ be an appropriate parameter and α be a root of $f_m^{(n)}(X)$. Then*

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

Corollary. *Let $m \in \mathbb{Z}$ be an appropriate parameter and α be a root of $f_m^{(n)}(X)$. Then the integral bases of the fields $K = \mathbb{Q}(\alpha)$ are repeating periodically modulo n_0, where n_0 is the greatest integer such that*

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

Proposition. *Let $m \in \mathbb{Z}$ be an appropriate parameter, α is a root of $f_m^{(n)}(X)$ and $K = \mathbb{Q}(\alpha)$. Then by calculating the dual basis of $(1, \alpha, \ldots, \alpha^{n-1})$, and by applying the estimate*

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

we get that $C_n \cdot \mathbb{Z}_K \subset \mathbb{Z}[\alpha]$, *where*

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

.

We calculated the smallest period length for degrees $n = 2, 3, 4, 5, 6, 8, 9$ and 12.

Corollary. *Let $m \in \mathbb{Z}$ be an appropriate parameter and let α be a root of $f_m^{(n)}(X)$. Then the integral bases of the fields $K = \mathbb{Q}(\alpha)$ are repeating periodically modulo n_0 for $n = 2, 3, 4, 5, 6, 8, 9, 12$, where*

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

.

As a special case, the integral bases of the simplest quartic number fields, generated by a root of

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

are repeating periodically modulo 8, which agrees with the results of J. H. Lee [49].

Integral bases of composite fields

In this section 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. The results appeared in the paper [29].

In the following table we summarize the additional conditions which are necessary for the periodic integral basis property. Let n_1, n_2 and m_1, m_2 be the degrees and the parameters belonging to the fields L and M respectively. Further, let

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

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

Then the additional conditions are listed in the following table based on the subfields.

L	M	Condition
I.	*I.*	$\gcd(m_1, m_2) \mid n_1 \cdot n_2$
I.	*II.*	$\gcd(m_1, s(m_2, n_2)) \mid n_1 \cdot n_2$
I.	*III.*	$\gcd(m_1, t(m_2, n_2)) \mid n_1 \cdot n_2$
II.	*II.*	$\gcd(s(m_1, n_1), s(m_2, n_2)) \mid n_1 \cdot n_2$
II.	*III.*	$\gcd(s(m_1, n_1), t(m_2, n_2)) \mid n_1 \cdot n_2$
III.	*III.*	$\gcd(t(m_1, n_1), t(m_2, n_2)) \mid n_1 \cdot n_2$

I.: Pure number fields
II.: First generalization of simplest fields
III.: Second generalization of simplest fields.

Corollary. *In the table above, the integral bases of the composite fields $K = LM$ are repeating periodically.*

In each case, using an estimate for $\gcd\left(D(\alpha)^{[K:L]}, D(\beta)^{[K:M]}\right)$, we can give an upper bound for the period length, but these bounds are far from the best. However, in some cases of small degrees, we can compute the smallest period length. These cases are contained in the following table.

The defining polynomials of the generators of the subfields are in the first and the second columns. The period length of the integral bases for the corresponding parameters are in the third and fourth columns.

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

We can see, that in the last case the quadratic subfield is fixed. The calculations in the general case would take too much time, so we have to choose a single example. Then $\mathbb{Q}(i\sqrt{3})$ is a reasonable choice, because then the composite field is a Galois extension.

Monogenity of infinite parametric families of number fields

In this section, we investigate the monogenity of some infinite parametric families of number fields of small degrees from the previous chapter. The related results are published in the papers [26], [27], [28] and [29].

By using the periodical integral basis property, we can compute the index form with one parameter. We just need the Hermite normal form integral bases, which have only finitely many different forms, thus we have to solve finitely many parametric index form equations. Because of the parametrization, we avoid solving the index form equation explicitly. Instead, we try to show that if the primitive element we use does not generate a power integral basis, then there is no solution of the index form equation.

We use 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 efficient if and only if the field index is not equal to 1, i.e. 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 compute the index form, then we determine 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 solve 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 obtain some non-trivial restrictions on the parameters belonging to monogenic fields. We found these coherences by investigating the factorization of certain linear combinations of the factors of the index form.

Monogenity of pure number fields

In this section we investigate the monogenity of pure fields of degrees $n = 2, 3, 4, 5, 6, 7, 8, 9$. The related results appeared in [26].

Pure cubic fields

Let $m \neq 0, \pm 1$ be a square-free integer, α be a root of $X^3 - m$ and $K = \mathbb{Q}(\alpha)$. The Hermite normal form of the integral basis belonging to α depends on the remainder of m modulo 9, and there are 3 different cases. In the first case, when $v_3(m^3 - m) = 1$, α generates a power integral basis. In other cases we can give infinitely many parameters belonging to monogenic fields, but we conjecture that there exist also infinitely many parameters belonging to non-monogenic fields.

Pure quartic fields

Let $m \neq 0, 1$ be a square-free integer, α be a root of $X^4 - m$ and $K = \mathbb{Q}(\alpha)$. The Hermite normal form of the integral basis belonging to α depends on the remainder of m modulo 8, and there are 3 different cases. If $m = 16k + r$ is square-free, then $K = \mathbb{Q}(\sqrt[4]{m})$ is monogenic if $r = 2, 3, 6, 7, 10, 11, 14,\ 15$, non-monogenic if $r = 1, 5, 13$ (except $m = -3$), and for $r = 9$, T. Arnóczki and G. Nyul [1] showed that by assuming the ABC-conjecture, there exists infinitely many monogenic and infinitely many non monogenic fields with such parameters.

Pure quintic fields

This case is very similar to the cubic case. The index form is irreducible, 5 does not divide the index of α, thus we can not get a general result other than the case when α generates a power integral basis.

Let $m \neq 0, \pm 1$ be a square-free integer, α be a root of $X^5 - m$ and $K = \mathbb{Q}(\alpha)$. The Hermite normal form of the integral basis belonging to α depends on the remainder of m modulo 25, and there are 5 different cases. In the first case, when $v_5(m^5 - m) = 1$, α generates a power integral basis. In other cases we conjecture that there exist infinitely many monogenic and infinitely many non-monogenic fields.

Pure sextic fields

This is the best case. Now we have two proper subfields, thus the index form has 3 factors, which provide us efficient conditions on the parameters belonging to monogenic fields.

Let $m \neq 0, \pm 1$ be a square-free integer, α be a root of $X^6 - m$ and $K = \mathbb{Q}(\alpha)$. The Hermite normal form of the integral basis belonging to α depends on the remainder of m modulo 36, and there are 6 different cases. If $m = 36k + r$ is square-free, then $K = \mathbb{Q}(\sqrt[6]{m})$ is monogenic if and only if $r = 2, 3, 6, 7, 11, 14, 15, 22, 23, 30, 31, 34$. This means that the monogenity of the pure sextic fields belonging to square-free parameters depends on the remainder of the parameter modulo 36.

The septic case is similar to the cubic and quintic case. The Hermite normal form of the integral basis belonging to α depends on the remainder of m modulo 49, and there are 7 different cases. In most of the cases, when $v_7(m^7 - m) = 1$, $\sqrt[7]{m}$ generates a power integral basis, in other cases we do not have any general result.

Pure octic fields

This case is almost as treatable as the sextic case. We have two proper subfields again, but now either of them is a subfield of the other one.

Let $m \neq 0, 1$ be a square-free integer, α be a root of $X^8 - m$ and $K = \mathbb{Q}(\alpha)$. The Hermite normal form of the integral basis belonging to α depends on the remainder of m modulo 16, and there are 4 different cases. If $m = 32k + r$ is square-free, then $K = \mathbb{Q}(\sqrt[8]{m})$ is monogenic if $r = 2, 3, 6, 7, 10, 11, 14, 15, 18, 19, 22, 23, 26, 27, 30, 31$ and $m = -3$, and not monogenic if $m \neq -3, 5$ and $r = 1, 5, 9, 13, 21, 25, 29$. The lacking residue class is $m \equiv 17 \pmod{32}$, in which case we conjecture that there are infinitely many monogenic and infinitely many non-monogenic fields.

Pure nonic fields

This case is similar to the quartic case, since the degree is a square of a prime. Let $m \neq 0, \pm 1$ be a square-free integer, α be a root of $X^9 - m$ and $K = \mathbb{Q}(\alpha)$. The Hermite normal form of the integral basis belonging to α depends on the remainder of m modulo 27, and there are 5 different cases. If $m = 27k + r$ is square-free, then $K = \mathbb{Q}(\sqrt[9]{m})$ is monogenic if $v_3(m^3 - m) = 1$, non-monogenic, if $r = 8, 10, 17, 19$ and in the remaining cases, for $r = 1, 26$, we conjecture that there are infinitely many monogenic and infinitely many non-monogenic fields.

Monogenity of simplest fields

The generalizations of the simplest number fields works very similar to the pure fields. We just deal with the simplest cubic, quartic and sextic fields. The monogenity of the simplest cubic fields has already been investigated by D. Shanks [60]. If $m^2 + 3m + 9$ is square-free, then the root of the simplest cubic polynomial generates a power integral basis, in other words the polynomials are monogenic. In the case of the simplest quartic fields, István Gaál and Gábor Petrányi [25] investigated the elements with minimal indices, which is a more general problem than the monogenity. The results in connection with the monogenity of simplest sextic fields are published in the paper [28].

Simplest cubic fields

As we mentioned before, this is the simplest case. These fields are generated by a root of the polynomial

$$f(X) = X^3 - mX^2 - (m + 3)X - 1.$$

If m is an integer parameter, such that $m^2 + 3m + 9$ is square-free, then α generates a power integral basis in the simplest cubic number fields $K = \mathbb{Q}(\alpha)$, thus these are monogenic.

Simplest quartic fields

Let α be a root of the polynomial

$$f(X) = X^4 - mX^3 - 6X^2 + mX + 1,$$

where $m \neq 0, \pm 3$. Then the fields $K = \mathbb{Q}(\alpha)$ are called simplest quartic fields. Assume that m is an appropriate parameter, i.e. for any prime $p \neq 2$, $v_p(m^2+16) < 2$, in other words $m^2 + 16$ has no odd square factor.

The Hermite normal form of the integral basis belonging to α depends on the remainder of m modulo 8, and there are 4 different cases. Our methods provides that these fields can be monogenic only if $m = \pm 2$, ± 4, ± 8, ± 16.

Simplest sextic fields

Similarly to the pure fields, the sextic case is the most treatable case again. Let $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$ and α be a root of

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

Then the fields $K = \mathbb{Q}(\alpha)$ are called simplest sextic fields. Assume that m is an appropriate parameter, which means that $m^2 + 3m + 9$ is square-free.

The Hermite normal form of the integral basis belonging to α depends on the remainder of m modulo 36, and there are 19 different cases. If f_1, f_2 and f_3 denote the factors of the index form, then in all of the cases we can pull out $m^2 + 3m + 9$ from $27f_3 - f_2$. This implies, that in the monogenic case, $m^2 + 3m + 9$ divides 26 or 28, thus these fields can be monogenic only if $m = -4, -2, -1, 1$. Moreover, the simplest sextic fields belonging to these parameters are indeed monogenic, and the generators of the power integral bases are listed by István Gaál [20].

Monogenity of composite fields

In this section, we investigated the monogenity of some composite fields $K = LM$, where $L = \mathbb{Q}(\alpha)$ and $M = \mathbb{Q}(\beta)$, and the defining polynomials of α and β are listed in the table below.

L	M
$X^2 - m_1$	$X^3 - m_2X^2 - (m_2 + 3)X - 1$
$X^2 - m_1$	$X^3 - m_2$
$X^2 - m_1$	$X^4 - m_2X^3 - 6X^2 + m_2X + 1$
$X^2 - m_1$	$X^4 - m_2$
$X^2 + 3$	$X^6 - m_2$

Under the appropriate conditions, the integral bases of these fields are repeating periodically in both variables. We give the Hermite normal form of the integral basis corresponding to the composite basis generated by the powers of α and β. The related results appeared in the paper [29].

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 is monogenic. Moreover, for some residue classes, we got a universal upper bound for the parameters belonging to monogenic fields.

Composition of quadratic and simplest cubic fields

Let α be a root of $X^2 - m_1$, where $m_1 \neq 1$ is square-free and let β be a root of $X^3 - m_2X^2 - (m_2 + 3)X - 1$, where $m_2^2 + 3m_2 + 9$ is square-free. Moreover, assume that $\gcd(m_1, m_2^2 + 3m_2 + 9) = 1$. Let $K = \mathbb{Q}(\alpha, \beta)$, then the Hermite normal form of the integral basis of K corresponding to the basis $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2)$, depends on the remainder of m_1 modulo 4. The cases and the conditions on the parameters of the possibly monogenic fields are listed in the table below.

$m_1 \pmod 4$	Condition 1	Condition 2
$2, 3$	$4m_1 \mid m_2^2 + 3m_2 + 9 \pm 1$	$m_2^2 + 3m_2 + 9 \mid 64m_1^3 \pm 1$
1	$m_1 \mid m_2^2 + 3m_2 + 9 \pm 1$	$m_2^2 + 3m_2 + 9 \mid m_1^3 \pm 1$

Composition of quadratic and pure cubic fields

Let α be a root of $X^2 - m_1$ and β be a root of $X^3 - m_2$, where $m_1 \neq 0, 1$ and $m_2 \neq 0, \pm 1$ are square-free integers such that, $\gcd(m_1, m_2) \mid 6$. Let $K = \mathbb{Q}(\alpha, \beta)$,

then the Hermite normal form of the integral basis of K corresponding to the basis $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2)$, depends on the remainders of m_1 modulo 12 and m_2 modulo 18. By investigating the factors of the index form belonging to the basis $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2)$, we found that we can pull out $4m_1$ from $F_3 - 27m_2^2F_1$ and $9m_2$ from $F_3 - 64m_1^3F_2^2$. Since $I(\alpha, \beta) \mid \gcd(D(\alpha)^3, D(\beta)^2)$, which is bounded independently from m_1 and m_2, then the coherences between the factors of the index forms corresponding to the integral bases in each cases, differ from the above by a constant multiple. In the monogenic case, by substituting a solution of the index from equation into the factors, their value should be ± 1, thus we obtain some divisibility relations for the parameters. These are listed in the table below based on the remainders of the parameters. The $\pm$ sign in the conditions means that it must hold either with $+$ or $-$.

$m_1 \pmod{12}$	$m_2 \pmod{18}$	$4m_1 \mid F_3 - 27m_2^2F_1$	$9m_2 \mid F_3 - 64m_1^3F_2^2$
$1, 5$	$1, 8, 10, 17$	$m_1 \mid 3m_2^2 \pm 1$	$m_2 \mid m_1^3 \pm 1$
$1, 5$	$2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 16$	$m_1 \mid 27m_2^2 \pm 1$	$9m_2 \mid m_1^3 \pm 1$
$2, 7, 10, 11$	$1, 17$	$4m_1 \mid 3m_2^2 \pm 1$	$m_2 \mid 64m_1^3 \pm 1$
$2, 7, 10, 11$	$3, 5, 7, 11, 13, 15$	$4m_1 \mid 27m_2^2 \pm 1$	$9m_2 \mid 64m_1^3 \pm 1$
$2, 7, 10, 11$	$2, 4, 6, 12, 14, 16$	$4m_1 \mid \frac{27}{2}m_2^2 \pm 2$	$9m_2 \mid 16m_1^3 \pm 2$
$2, 7, 10, 11$	$8, 10$	$4m_1 \mid \frac{3}{2}m_2^2 \pm 2$	$9m_2 \mid 16m_1^3 \pm 2$
$3, 6$	$1, 17$	$\frac{4}{3}m_1 \mid m_2^2 \pm 3$	$3m_2 \mid \frac{64}{9}m_1^3 \pm 3$
$3, 6$	$3, 5, 7, 11, 13, 15$	$4m_1 \mid 9m_2^2 \pm 3$	$9m_2 \mid \frac{64}{9}m_1^3 \pm 3$
$3, 6$	$8, 10$	$\frac{4}{3}m_1 \mid \frac{1}{2}m_2^2 \pm 6$	$3m_2 \mid \frac{16}{9}m_1^3 \pm 6$
$3, 6$	$2, 4, 6, 12, 14, 16$	$4m_1 \mid \frac{9}{2}m_2^2 \pm 6$	$9m_2 \mid \frac{16}{9}m_1^3 \pm 6$
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	$2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 16$	$m_1 \mid 9m_2^2 \pm 3$	$9m_2 \mid \frac{1}{9}m_1^3 \pm 3$

We can see that if $m_1 \neq \pm 1$ and $m_1 \neq \pm 3$, then in the third and fourth columns of the table, the right hand sides of the relations can not be equal to 0, thus by fixing one of the parameters, the other can have only finitely many values for which the composite field is monogenic. Considering the first two columns of the table, we

can see that there remains only one case which does not satisfy the property above, $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{m_2})$. However, these normal extensions are investigated by M.-L. Chang [6], who showed that they are monogenic if and only if $m_2 = 2$. Therefore, for any pairs of parameters, if either of them is fixed, then the other can have only finitely many values for which the composite field is monogenic.

Composition of quadratic and simplest quartic fields

Let α be a root of $X^2 - m_1$, where $m_1 \neq 1$ is square-free and let β be a root of $X^4 - m_2X^3 - 6X^2 + m_2X + 1$, where $m_2 \neq 0, \pm 3$ and $m_2^2 + 16$ is square-free. Moreover, assume that $\gcd(m_1, m_2^2 + 16) \mid 2$.

Let $K = \mathbb{Q}(\alpha, \beta)$, then the Hermite normal form of the integral basis of K corresponding to the basis $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2, \beta^3, \alpha\beta^3)$, depends on the remainders of m_1 modulo 8 and m_2 modulo 16. We showed that aside from the cases $m_1 \equiv 1, 3, 5, 7 \pmod 8$ and $m_2 \equiv 4, 12 \pmod{16}$, the parameters of the monogenic fields satisfy

$$|m_2| \leq 64, \text{ and } |m_1| \leq 4m_2^2 + 192.$$

In the remaining cases, if $m_1 \neq -1$, then as usual, by fixing one of the parameters, the other can have only finitely many values for which the composite field is monogenic. The case of $m_1 = -1$ is unlike to other cases, because we can not prove that there are only finitely many values of m_2, such that the composite field is monogenic.

Composition of quadratic and pure quartic fields

Let α be a root of $X^2 - m_1$ and β be a root of $X^4 - m_2$, where $m_1 \neq 0, 1$ and $m_2 \neq 0, 1$ are square-free integers such that, $\gcd(m_1, m_2) \mid 2$. Let $K = \mathbb{Q}(\alpha, \beta)$, then the Hermite normal form of the integral basis of K corresponding to the basis $(1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2, \beta^3, \alpha\beta^3)$, depends on the remainders of m_1 and m_2 modulo 8.

We proved that if

- $m_1 \equiv 1 \pmod 4$ and $m_2 \equiv 5 \pmod 8$ or
- $m_1 \equiv 2 \pmod 4$ or
- $m_1 \equiv 3 \pmod 4$ and $m_2 \equiv 1 \pmod 2$,

then the parameters belonging to monogenic fields satisfy $|m_2| \leq 130$ and $|m_1| \leq 32|m_2| + 32$. In the other cases, if $m_1 \neq -1$, then by fixing one of the parameters, the other can have only finitely many values for which the composite field is monogenic.

Finally, if $m_1 = -1$, then the composite field $K = \mathbb{Q}(i, \sqrt[4]{m_2})$ is a normal extension of $\mathbb{Q}$. The index form in this case has more factors than in the general

case, and we can find some very useful connections among them. We can derive from these coherences, that if K is monogenic, then the only possible values for m_2 are ± 2, ± 3 and ± 5. In the paper [27] we showed that if $m_2 = \pm 2, 3$ or -5, then K is not monogenic, so there remains only 2 possibilities, $m_2 = -3$ and $m_2 = 5$. We conjecture that in these cases K is also not monogenic.

As we saw in the previous sections, the normal extensions $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{m})$ and $\mathbb{Q}(i, \sqrt[4]{m})$ were under more detailed examinations. To make this process complete, we investigated the monogenity of $\mathbb{Q}(i\sqrt{3}, \sqrt[6]{m})$. Thus, all of the monogenic normal pure extensions of quadratic fields are given, except some special parameters.

Monogenity of the fields $\mathbb{Q}(i\sqrt{3}, \sqrt[6]{m})$

Let ω be a third root of unity, β be a root of $X^6 - m$, where $m \neq \pm 1, -3$ square-free. Let $K = \mathbb{Q}(\omega, \beta)$, then the Hermite normal form of the integral basis of K corresponding to the basis

$$(1, \omega, \beta, \omega\beta, \beta^2, \omega\beta^2, \beta^3, \omega\beta^3, \beta^4, \omega\beta^4, \beta^5, \omega\beta^5)$$

depends on the remainder of m modulo 36. By using the coherences between the factors of the index form, we proved, that these fields can be monogenic only if $m = -15, -6, -2, 2, 3, 5, 6$.

References

[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.

DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR
H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

Nyilvántartási szám: DEENK/186/2021.PL
Tárgy: PhD Publikációs Lista

Jelölt: Remete László
Doktori Iskola: Matematika- és Számítástudományok Doktori Iskola
MTMT azonosító: 10073338

A PhD értekezés alapjául szolgáló közlemények

Idegen nyelvű tudományos közlemények hazai folyóiratban (2)

1. **Remete, L.**: A generalization of simplest number fields and their integral basis.
   Acta Math. Hung. 163 (2), 437-461, 2021. ISSN: 0236-5294.
   DOI: http://dx.doi.org/10.1007/s10474-020-01093-8
   IF: 0.588 (2019)

2. **Remete, L.**: Integral bases of pure fields with square-free parameter.
   Stud. Sci. Math. Hung. 57 (1), 91-115, 2020. ISSN: 0081-6906.
   DOI: http://dx.doi.org/10.1556/012.2020.57.1.1450
   IF: 0.468 (2019)

Idegen nyelvű tudományos közlemények külföldi folyóiratban (4)

3. Gaál, I., **Remete, L.**: Integral Bases and Monogenity of Composite Fields.
   Exp. Math. 28 (2), 209-222, 2019. ISSN: 1058-6458.
   DOI: http://dx.doi.org/10.1080/10586458.2017.1382404
   IF: 0.659

4. Gaál, I., **Remete, L.**: Integral bases and monogenity of the simplest sextic fields.
   Acta Arith. 183 (2), 173-183, 2018. ISSN: 0065-1036.
   DOI: http://dx.doi.org/10.4064/aa170502-23-10
   IF: 0.416

5. Gaál, I., **Remete, L.**: Integral bases and monogenity of pure fields.
   J. Number Theory. 173, 129-146, 2017. ISSN: 0022-314X.
   DOI: http://dx.doi.org/10.1016/j.jnt.2016.09.009
   IF: 0.774

6. Gaál, I., **Remete, L.**: Non-monogenity in a family of octic fields.
   Rocky Mt. J. Math. 47 (3), 817-824, 2017. ISSN: 0035-7596.
   DOI: http://dx.doi.org/10.1216/RMJ-2017-47-3-817
   IF: 0.33

DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR
H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

További közlemények

Idegen nyelvű tudományos közlemények hazai folyóiratban (1)

7. Gaál, I., **Remete, L.**: Power integral bases in cubic and quartic extensions of real quadratic fields.
   Acta Sci. Math. 85 (3-4), 413-429, 2019. ISSN: 0001-6969.
   DOI: http://dx.doi.org/10.14232/actasm-018-080-z

Idegen nyelvű tudományos közlemények külföldi folyóiratban (8)

8. Gaál, I., Jadrijević, B., **Remete, L.**: Totally real Thue inequalities over imaginary quadratic fields: an improvement.
   Glas. Mat. 55 (2), 191-194, 2020. ISSN: 0017-095X.
   DOI: http://dx.doi.org/10.3336/gm.55.2.02
   IF: 0.564 (2019)

9. Gaál, I., Jadrijević, B., **Remete, L.**: Simplest quartic and simplest sextic Thue equations over imaginary quadratic fields.
   Int. J. Number Theory. 15 (1), 11-27, 2019. ISSN: 1793-0421.
   DOI: http://dx.doi.org/10.1142/S1793042118501695
   IF: 0.606

10. Gaál, I., Jadrijević, B., **Remete, L.**: Totally real Thue inequalities over imaginary quadratic fields.
    Glas. Mat. 53 (2), 229-238, 2018. ISSN: 0017-095X.
    DOI: http://dx.doi.org/10.3336/gm.53.2.02
    IF: 0.554

11. Gaál, I., **Remete, L.**, Szabó, T.: Calculating power integral bases by using relative power integral bases.
    Funct. Approx. Comment. Math. 54 (2), 141-149, 2016. ISSN: 0208-6573.
    DOI: http://dx.doi.org/10.7169/facm/2016.54.2.1

12. Gaál, I., **Remete, L.**: Power integral bases in a family of sextic fields with quadratic subfields.
    Tatra Mt. Math. Publ. 64 (1), 59-66, 2015. ISSN: 1210-3195.
    DOI: http://dx.doi.org/10.1515/tmmp-2015-0041

13. Gaál, I., **Remete, L.**: Solving binomial Thue equations.
    J. Algebra, Number Theory & Appl. 36 (1), 29-42, 2015. ISSN: 0972-5555.

14. Gaál, I., **Remete, L.**: Binomial Thue equations and power integral bases in pure quartic fields.
    J. Algebra, Number Theory & Appl. 32 (1), 49-61, 2014. ISSN: 0972-5555.

DEBRECENI EGYETEM
EGYETEMI ÉS NEMZETI KÖNYVTÁR
H-4002 Debrecen, Egyetem tér 1, Pf.: 400
Tel.: 52/410-443, e-mail: publikaciok@lib.unideb.hu

15. Gaál, I., **Remete, L.**, Szabó, T.: Calculating power integral bases by solving relative Thue equations.
Tatra Mt. Math. Publ. 59 (1), 79-92, 2014. ISSN: 1210-3195.
DOI: http://dx.doi.org/10.2478/tmmp-2014-0020

A közlő folyóiratok összesített impakt faktora: 4,959
A közlő folyóiratok összesített impakt faktora (az értekezés alapjául szolgáló közleményekre): 3,235

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

Debrecen, 2021.04.12.

DEBRECENI EGYETEM * Egyetemi és Nemzeti Könyvtár *

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

Registry number: DEENK/186/2021.PL
Subject: PhD Publication List

Candidate: László Remete
Doctoral School: Doctoral School of Mathematical and Computational Sciences
MTMT ID: 10073338

List of publications related to the dissertation

Foreign language scientific articles in Hungarian journals (2)

1. **Remete, L.**: A generalization of simplest number fields and their integral basis.
   Acta Math. Hung. 163 (2), 437-461, 2021. ISSN: 0236-5294.
   DOI: http://dx.doi.org/10.1007/s10474-020-01093-8
   IF: 0.588 (2019)

2. **Remete, L.**: Integral bases of pure fields with square-free parameter.
   Stud. Sci. Math. Hung. 57 (1), 91-115, 2020. ISSN: 0081-6906.
   DOI: http://dx.doi.org/10.1556/012.2020.57.1.1450
   IF: 0.468 (2019)

Foreign language scientific articles in international journals (4)

3. Gaál, I., **Remete, L.**: Integral Bases and Monogenity of Composite Fields.
   Exp. Math. 28 (2), 209-222, 2019. ISSN: 1058-6458.
   DOI: http://dx.doi.org/10.1080/10586458.2017.1382404
   IF: 0.659

4. Gaál, I., **Remete, L.**: Integral bases and monogenity of the simplest sextic fields.
   Acta Arith. 183 (2), 173-183, 2018. ISSN: 0065-1036.
   DOI: http://dx.doi.org/10.4064/aa170502-23-10
   IF: 0.416

5. Gaál, I., **Remete, L.**: Integral bases and monogenity of pure fields.
   J. Number Theory. 173, 129-146, 2017. ISSN: 0022-314X.
   DOI: http://dx.doi.org/10.1016/j.jnt.2016.09.009
   IF: 0.774

6. Gaál, I., **Remete, L.**: Non-monogenity in a family of octic fields.
   Rocky Mt. J. Math. 47 (3), 817-824, 2017. ISSN: 0035-7596.
   DOI: http://dx.doi.org/10.1216/RMJ-2017-47-3-817
   IF: 0.33

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

List of other publications

Foreign language scientific articles in Hungarian journals (1)

7. Gaál, I., **Remete, L.**: Power integral bases in cubic and quartic extensions of real quadratic fields.
   Acta Sci. Math. 85 (3-4), 413-429, 2019. ISSN: 0001-6969.
   DOI: http://dx.doi.org/10.14232/actasm-018-080-z

Foreign language scientific articles in international journals (8)

8. Gaál, I., Jadrijević, B., **Remete, L.**: Totally real Thue inequalities over imaginary quadratic fields: an improvement.
   Glas. Mat. 55 (2), 191-194, 2020. ISSN: 0017-095X.
   DOI: http://dx.doi.org/10.3336/gm.55.2.02
   IF: 0.564 (2019)

9. Gaál, I., Jadrijević, B., **Remete, L.**: Simplest quartic and simplest sextic Thue equations over imaginary quadratic fields.
   Int. J. Number Theory. 15 (1), 11-27, 2019. ISSN: 1793-0421.
   DOI: http://dx.doi.org/10.1142/S1793042118501695
   IF: 0.606

10. Gaál, I., Jadrijević, B., **Remete, L.**: Totally real Thue inequalities over imaginary quadratic fields.
    Glas. Mat. 53 (2), 229-238, 2018. ISSN: 0017-095X.
    DOI: http://dx.doi.org/10.3336/gm.53.2.02
    IF: 0.554

11. Gaál, I., **Remete, L.**, Szabó, T.: Calculating power integral bases by using relative power integral bases.
    Funct. Approx. Comment. Math. 54 (2), 141-149, 2016. ISSN: 0208-6573.
    DOI: http://dx.doi.org/10.7169/facm/2016.54.2.1

12. Gaál, I., **Remete, L.**: Power integral bases in a family of sextic fields with quadratic subfields.
    Tatra Mt. Math. Publ. 64 (1), 59-66, 2015. ISSN: 1210-3195.
    DOI: http://dx.doi.org/10.1515/tmmp-2015-0041

13. Gaál, I., **Remete, L.**: Solving binomial Thue equations.
    J. Algebra, Number Theory & Appl. 36 (1), 29-42, 2015. ISSN: 0972-5555.

14. Gaál, I., **Remete, L.**: Binomial Thue equations and power integral bases in pure quartic fields.
    J. Algebra, Number Theory & Appl. 32 (1), 49-61, 2014. ISSN: 0972-5555.

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

15. Gaál, I., **Remete, L.**, Szabó, T.: Calculating power integral bases by solving relative Thue equations.
Tatra Mt. Math. Publ. 59 (1), 79-92, 2014. ISSN: 1210-3195.
DOI: http://dx.doi.org/10.2478/tmmp-2014-0020

Total IF of journals (all publications): 4,959
Total IF of journals (publications related to the dissertation): 3,235

The Candidate's publication data submitted to the iDEa Tudóstér have been validated by DEENK on the basis of the Journal Citation Report (Impact Factor) database.

12 April, 2021

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.