Power integral bases in algebraic number fields

István Gaál (Debrecen)

Dubrovnik, Juni 22-28, 2025

in honour of Professors
Andrej Dujella, Ivica Gusić, and Borka Jadrijević

Notation

$K = \mathbb{Q}(\theta)$ algebraic number field, $[K : \mathbb{Q}] = n$,
$\mathbb{Z}_K$ ring of integers, D_K discriminant

$\mathbb{Z}_K$ is called **monogenic** (K is monogenic) if there exists $\alpha \in \mathbb{Z}_K$ such that $(1, \alpha, \ldots, \alpha^{n-1})$ is an integer basis:
power integral basis
In this case $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ (mono-generated)

index of $\alpha \in \mathbb{Z}_K$:

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

$\alpha \pm \beta \in \mathbb{Z} \Rightarrow I(\beta) = I(\alpha)$
equivalent algebraic integers in K
minimal index of K: $m_K = \min\{I(\alpha) | \alpha \in \mathbb{Z}_K, K = \mathbb{Q}(\alpha)\}$
field index of K: $m(K) = \gcd\{I(\alpha) | \alpha \in \mathbb{Z}_K, K = \mathbb{Q}(\alpha)\}$

$$\prod_{1 \le i < j \le n} D(\alpha) = \left|\alpha^{(i)} - \alpha^{(j)}\right|^2 = I(\alpha)^2 \cdot D_K$$

$$I(\alpha) = \frac{1}{\sqrt{|D_K|}} \prod_{1 \le i < j \le n} \left|\alpha^{(i)} - \alpha^{(j)}\right|$$

Index form equations

$(1, \omega_2, \ldots, \omega_n)$ integral basis, D_K discriminant of K

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

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

$$I(X_2, \ldots, X_n) = \frac{1}{\sqrt{|D_K|}} \prod_{1 \le i < j \le n} \left(L^{(i)}(\underline{X}) - L^{(j)}(\underline{X})\right)$$

$I(X_2, \ldots, X_n) \in \mathbb{Z}[X_2, \ldots, X_n]$ is a homogeneous form of degree $n(n-1)/2$ called the **index form**

For any primitive integer $\alpha = x_1 + \omega_2 x_2 + \ldots + \omega_n x_n \in \mathbb{Z}_K$
we have $I(\alpha) = |I(x_2, \ldots, x_n)|$
$I(\alpha) = 1 \Longleftrightarrow I(x_2, \ldots, x_n) = \pm 1$

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

index form equation

The index form equation has only finitely many solutions
$\Leftrightarrow$ up to equivalence there are only finitely many generators of power integral bases
(B.J.Birch and J.R.Merriman 1972; K.Győry 1973)

Monogenic polynomials

An irreducible **polynomial** $f(x) \in \mathbb{Z}[x]$ with a root ϑ is called **monogenic** if ϑ generates a power integral basis in $K = \mathbb{Q}(\vartheta)$

If $f(x)$ is monogenic, then K is also monogenic, but the converse is not true

History, importance

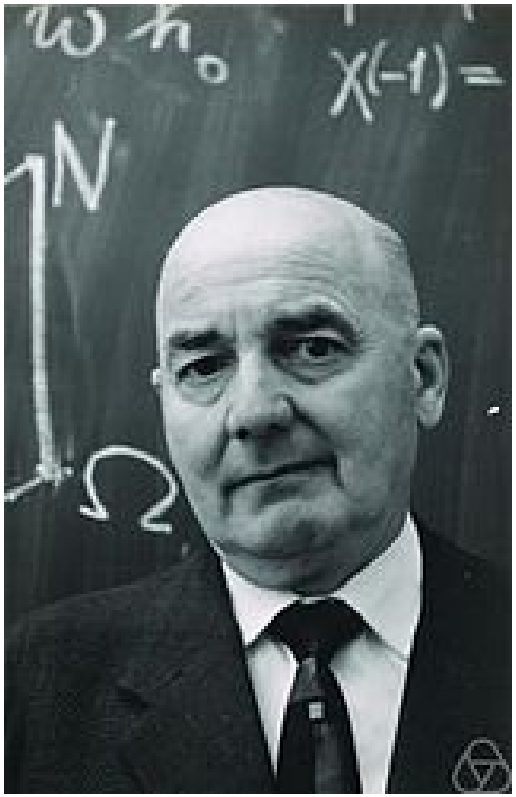
R.Dedekind, 1878: the first example for non-monogenic field
H.Hasse, 1960's: asked for an arithmetic characterization of monogenic fields.

Problems of **W.Narkiewicz** in his book:
–Find a necessary and sufficient condition for a field to have index 1
–Give an explicit formula for $\nu_p(m(K))$, the highest power of a given prime dividing the index of a field K.

The base numbers of **generalized number systems** of K are exactly the generators of power integral bases of K.



Julius Wilhelm Richard Dedekind
1831-1916



Helmut Hasse
1898-1979.



Marie-Nicole Gras
1942-2024



Blair Spearman
1951-2017



Wladislaw Narkiewicz
1936-

Some "classical" results obtained by algebraic methods

There are infinitely many totally real **cyclic cubic fields** that are monogenic, on the other hand the minimum index of such fields can be arbitrary large (D.S.Dummit and H.Kisilevsky, 1977)

Imaginary cyclic quartic fields can have power integral bases only in two trivial cases (M.N.Gras 1979)

The minimum index of **cyclic quartic fields** can be arbitrary large (T.Nakahara 1987)

There exists infinitely many **quartic fields** with Galois group **A4** and with power integral bases (B.K.Spearman, 2006)

If K is a **cyclic field of prime degree** ≥ 5 then K has no power integral bases except if K is the maximal real subfield of a cyclotomic field (M.N.Gras 1986)

If $n \geq 5$, relatively prime to 2 and 3, then there are only finitely many monogenic fields of degree n with **Abelian Galois group** (M.N.Gras, 1983)

There are several results on **cyclotomic fields**:

Let p be a prime and ζ a primitive p-th root of unity. Conjecture: up to equivalence ζ and $1/(1+\zeta)$ are all generators of power integral bases in $\mathbb{Q}(\zeta)$ (A.Bremner, 1988) Proof of the conjecture for $p \leq 23, p \neq 17$ (L.Robertson, 1998)

In the 2^m-th cyclotomic field only ζ^i generates power integral basis (L.Robertson, 2001)

If α generates a power integral basis in the p^m-th cyclotomic field $\mathbb{Q}(\zeta)$ (and ...), then α is either equivalent to ζ or $\alpha + \overline{\alpha}$ is an odd integer (I.Gaál and L.Robertson, 2006)

Monogenity and power integral bases

Online conferences

Our purpose is to bring together our colleagues working in this area. We are going to create an email list, circulate preprints and results, support collaboration.

For a long time it has not been possible to travel, but it was easy to meet online. Therefore we organized online meetings. I hope all participants enjoyed meeting at least online several colleagues who formerly was only known by their papers and results.

As long as there is enough interest I propose to continue these online meetings every couple of months in order to keep contact. Of course we hope to be able to meet also personally after the pandemy.

Please let me know if you have some new results in this area and these online meetings can be used to present them.

Started in January, 2021
After ten online meetings, the first in-person meeting:
July 8-10, 2025, Barcelona

Dedekind's criterion, 1878

Theorem

$f(x) \in \mathbb{Z}[x]$ monic, irreducible, $F(\alpha) = 0$, $K = \mathbb{Q}(\alpha)$, p prime $\overline{f(x)} = \prod_{i=1}^{r} \overline{\phi_i(x)}^{\ell_i} \pmod{p}$, $\overline{\phi_i(x)}$ are irred. pairwise coprime in $\mathbb{F}_p$.

$$M(x) = \frac{f(x) - \prod_{i=1}^{r} \phi_i^{\ell_i}(x)}{p}.$$

Then $M(x) \in \mathbb{Z}[x]$ and the following statements are equivalent:

1. p **does not divide the index** $I(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])$.
2. For every $i = 1, \ldots, r$, either $\ell_i = 1$ or $\ell_i \geq 2$ and $\overline{\phi_i(x)}$ does not divide $\overline{M(x)}$ in $\mathbb{F}_p[x]$.

Theorem (K. Hensel, 1908)

The prime factors of the field index are smaller than the degree of the field.

$\nu_p(k)$ the highest power of the prime p dividing k.

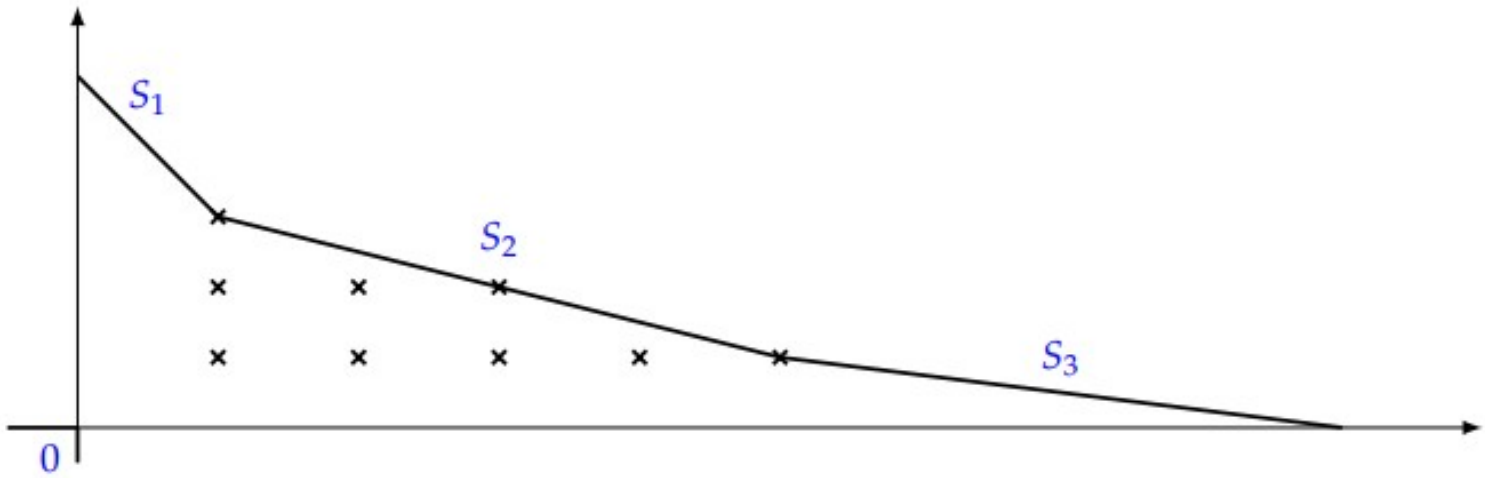
Theorem (H. T. Engström, 1930)

For number fields of degree $n \leq 7$, $\nu_p(m(K))$ is explicitly determined by the factorization of p into powers of prime ideals of $p\mathbb{Z}_K$.

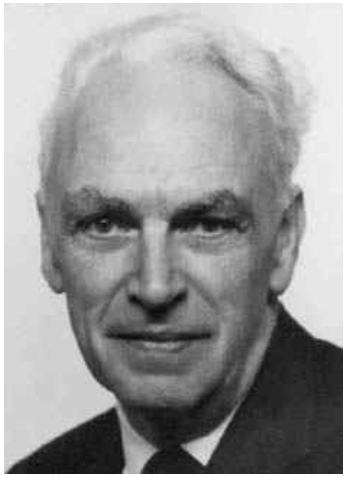
Newton polygon method

$$f(x) = \sum_{i=0}^{\ell} a_i(x)\phi(x)^i.$$

The ϕ-*Newton polygon* of $f(x)$ with respect to p is the lower boundary convex envelope of the set of points $\{(i, \nu_p(a_i(x))),\ a_i(x) \neq 0\}$



Theorem of Oystein Ore (1928)
– $\nu_p(\mathrm{ind}(f))$
– factorization of p into prime ideals



(1899-1968)

J.Montes, E.Nart (1992)
L. El Fadil, J.Montes, E.Nart (2012): p integral bases of K
J.Guardia, J.Montes, E.Nart (2012): higher order Newton polygons
J.Guardia and E.Nart (2015)

Pure fields, $x^n - m$, m squarefree, 2021-2024

- Z. S. Aygin and K. D. Nguyen: $n = 3$;
- L. El Fadil $n = 12, 18, 20, 24, 36$;
- L. El Fadil, H. Ben Yakkou and J. Didi $n = 42$;
- L. El Fadil, H. Choulli and O. Kchit $n = 60$;
- L. El Fadil and M. Faris $n = 84$;
- H. Ben Yakkou and O. Kchit $n = 3^k$;
- L. El Fadil $n = 2 \cdot 3^k$, $2^k \cdot 3^\ell$
- H. Ben Yakkou, A. Chillali and L. El Fadil: $n = 2^k \cdot 5^\ell$;
- L. El Fadil $n = 3^k \cdot 7^\ell$, $n = 2^k \cdot 3^\ell \cdot 5^t$
- L. El Fadil and A. Najim $n = 2^k \cdot 3^\ell$;
- L. El Fadil and O. Kchit $n = 2^k \cdot 7^\ell$;
- H. Ben Yakkou and L. El Fadil $n = p^k$;
- L. El Fadil $n = 6$, m composite;
- L. El Fadil and I. Gaál $n = 8$, m composite.

Theorem

(L. El Fadil and A. Najim, 2022)
Let α be a root of the irreducible polynomial $x^{2^k \cdot 3^\ell} - m$ with a squarefree m.
If $m \not\equiv 1 \pmod 4$ and $m \not\equiv \pm 1 \pmod 9$ then α generates a **power integral basis** in $K = \mathbb{Q}(\alpha)$.
If $m \equiv 1 \pmod 4$, or
$m \equiv 1 \pmod 9$, or
$k = 2$ and $m \equiv -1 \pmod 9$, then K is **not monogenic**.

Integral bases and monogenity of pure fields, $x^n - m, n \leq 9$, m squarefree, (I.Gaál and L. Remete, 2016)

The structure of the integral bases of $K = \mathbb{Q}(\sqrt[n]{m})$ is **periodic** in m. For $3 \leq n \leq 9$ the period length is n^2.

Example:
$K = \mathbb{Q}(\sqrt[4]{m})$
$m \equiv 2, 3, 6, 7, 10, 11, 14, 15 \pmod{16}$, $B = \{1, x, x^2, x^3\}$
$m \equiv 1, 9 \pmod{8}$, $B = \left\{1, x, \frac{1+x^2}{2}, \frac{1+x+x^2+x^3}{4}\right\}$
$m \equiv 5, 13 \pmod{8}$, $B = \left\{1, x, \frac{1+x^2}{2}, \frac{x+x^3}{2}\right\}$

Monogenity of pure quartic fields:

Theorem

Let m be a square-free integer. The field $K = \mathbb{Q}(\sqrt[4]{m})$ is **monogenic** if $m \equiv 2, 3, 6, 7, 10, 11, 14, 15 \pmod{16}$ and is **not monogenic** if $m \equiv 1, 5, 13 \pmod{16}$ with the exception of $\mathbb{Q}(\sqrt[4]{-3})$ which is monogenic.

Integral bases and monogenity of pure fields, $x^n - m, n \leq 9$, m arbitrary, (L. El Fadil and I.Gaál 2023)

$K = \mathbb{Q}(\sqrt[4]{m})$, $m = a_1 a_2^2 a_3^3$, a_1, a_2, a_3 pairwise coprime sq-free

Theorem

$\mathbb{Z}[\alpha]$ is the ring of integers of K is and only if $m \neq \pm 1$ is squarefree and $m \not\equiv 1 \pmod 4$.

Necessary conditions for monogenity of K:
If $\nu_2(m)$ odd or $\nu_2(m-1) = 1$, then $4a_1a_3$ divides $(a_2^2 \pm 1)$
If $m \equiv 4 \mod 16$, then a_1a_3 divides $(4a_2^2 \pm 1)$.
If $m \equiv 12 \mod 32$, then $4a_1a_3$ divides $(a_2^2 \pm 16)$.
If $m \equiv 28 \mod 32$, then a_1a_3 divides $(a_2^2 \pm 64)$.
If $m \equiv 5 \mod 8$, then a_1a_3 divides $(4a_2^2 \pm 1)$.

Pure sextic fields, L. El Fadil and I.Gaál, 2023

$m \neq \pm 1$, $m = a_1 a_2^2 a_3^3 a_4^4 a_5^5$, where a_1, a_2, a_3, a_4, a_5 are pairwise coprime square free, $\alpha = \sqrt[6]{m}, K = \mathbb{Q}(\alpha)$

Theorem

$\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if m is square-free, $m \not\equiv 1 \pmod 4$ and $m \not\equiv \pm 1 \pmod 9$

Theorem

Assume $\nu_2(m)$ is odd and $\nu_3(m) \neq 3$.
If K is monogenic, then $a_1 a_5$ divides $(a_3^2 \pm a_2^2 a_4^2)$
etc.

Monogenity of several types of trinomials

$x^n + ax^m + b$

C.T.Davis and B.K.Spearman: deg=3,4
S.Alaca and K.S.Williams: deg=4
L.El Fadil and I.Gaál: deg=4
L.El Fadil: deg=5,6

L.El Fadil, O.Kchit, H.Ben Yakkou
B.Jhorar
A.Jakhar, S.K.Khanduja, N.Sangwan
R.Ibarra, H.Lembeck, M.Ozaslan, H.Smith, and K.E.Stange
L.Jones , L.Jones and D.White

Theorem

(L. Jones and D. White 2021)
Let $n \geq 2$ be an integer, with $m \geq 1$ a proper divisor of n. Let $t = n/m$ and let κ denote the squarefree kernel of m. Let A and B be positive integers with $\gcd(A, B) > 1$, and define

$$D := \frac{t^t B^{t-1} + (1-t)^{t-1} A^t}{\gcd(A, B)^{t-1}}.$$

If B and D are squarefree, and $\gcd(A, B) = 0 \pmod{\kappa}$, then $f(x) = x^n + Ax^m + B$ is **monogenic**. Moreover, $D(f)$ is not squarefree if $m \geq 2$.

Quartic trinomials, L. El Fadil and I.Gaál, 2023

$F(x) = x^4 + ax^2 + b \in \mathbb{Z}[x]$ irreducible, $\nu_p(a) < 2$ or $\nu_p(b) < 4$ (for every prime p), $F(\alpha) = 0$, $K = \mathbb{Q}(\alpha)$

Theorem

$\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if one of the following conditions is satisfied:

1. there is a prime p such that $\nu_p(a) \geq 1$ and $\nu_p(b) = 1$
2. $b \equiv 2 \pmod 4$ and $a \equiv 3 \pmod 4$
3. 2 does not divide b and $a \equiv 1 - b \pmod 4$
4. 2 does not divide ab and $a \equiv 3 \pmod 4$
5. 2 does not divide ab and $b \not\equiv a \pmod 4$

Theorem

Describing explicitly the exact values of $\nu_2(i(K))$, $\nu_3(i(K))$ in terms of the parameters a, b.

Theorem

Assume $a > 1, b > 1$ and $f(x) = x^4 + ax^2 + b$ is irreducible and **monogenic**. If a, b are **not** of type

$$a = \frac{u \pm 1}{v}, \quad b = \frac{u^2 - 1}{4v^2} \tag{1}$$

for some $u, v \in \mathbb{Z}, v \neq 0, u \neq \pm 1$ then up to equivalence the root ξ of $f(x)$ is the **only generator of power integral bases** in $K = \mathbb{Q}(\xi)$.

Monogenity of several types of quadrinomials, quintinomials, 2021–

- Lenny Jones;
- T. A. Gassert, H. Smith and K. E. Stange;
- J. Harrington and L. Jones;
- A. Jakhar and R. Kalwaniya;
- A.Jakhar, S.Kaur and S.Kumar;

- L. Jones constructed infinite families of reciprocal monogenic polynomials with prescribed Galois group;
- L. Jones showed that if $4 \leq n \geq m \geq 0$ and $\gcd(n, m) = \gcd(n, k) = 1$ then $x^{n-m}(x + k)^m + p$ is monogenic for infinitely many primes p;
- L. Jones $x^n + A(Bx + 1)^m$;
- L. Jones $x^n + t \cdot g(x)$ with $n > \deg(g)$, when $g(x)$ is monic and $\deg(g) \in \{2, 3, 4\}$
- L. Jones constructed reciprocal monogenic quintinomials of type $x^{2^n} + Ax^{3 \cdot 2^{n-2}} + Bx^{2^{n-1}} + Ax^{2^{n-2}} + 1$;
- L. Jones considered infinite families of monogenic quadrinomials, quintinomials and sextinomials.

Monogenity of composite polynomials

- J. Harrington and L. Jones: composition of $x^n - a$ and $x^m - b$;
- Jakhar, A. R. Kalwaniya and P. Yadav: composition of $x^n - a$ and $x^m - b$
- J. Harrington and L. Jones: $\Phi_{p^a}(\Phi_{2^b}(x))$, where $\Phi_N(x)$ is the cyclotomic polynomial of index N;
- L. Jones considered monotonically stable polynomials of type $g(f^n(x))$;
- L. Jones considered monogenity of $f(x^p)$, where $f(x)$ is the char pol of an Nth order lin recurrence;
- J. Harrington and L. Jones gave conditions for the monogenity of $f(x^{p^n})$, where $f(x) = x^m + ax^{m-1} + b$;
- S. Kaur, S. Kumar and L. Remete considered monogenity of $f(x^k)$, where $f(x) = x^d + A \cdot h(x), \deg h < d$.

Theorem (J. Harrington and L. Jones, 2021)

Let a and b be positive integers, and let p be a prime. Then the polynomial $\Phi_{p^a}(\Phi_{2^b}(x))$ is monogenic, where $\Phi_N(x)$ is the cyclotomic polynomial of index N.

$$\Phi_n(x) = \prod_{1 \leq k \leq n, \gcd(k,n)=1} \left(x - e^{2\pi i \frac{k}{n}} \right)$$

Connected results in the relative case

- M. E. Charkani and A. Deajim, A. Deajim and L. El Fadil: $x^p - m$ over number fields
- M. Sahmoudi and M. E. Charkani: relative pure cyclic ext.
- A. Soullami, M. Sahmoudi and O. Boughaleb: $x^{3^n} + ax^{3^s} - b$ over number fields;
- O. Boughaleb, A. Soullami and M. Sahmoudi: $x^{p^n} + ax^{p^s} - b$ over number fields;
- H. Smith studied relative radical extensions;
- S. K. Khanduja and B. Jhorar gave equivalent versions of Dedekind's criterion in general rings;
- S. Arpin, S. Bozlee, L. Herr and H. Smith: monogenity of number rings from a modul-theoretic perspective;
- R. Sekigawa constructed an infinite number of cyclic relative extensions of prime degree that are relative

Connection of monogenity with WSS primes

$a, b > 0$, $u_0 = 0, u_1 = 1, u_n = au_{n-1} + bu_{n-2}$ Lucas sequence
$u_m (\mathrm{mod}\, m)$ is periodic, if $m \geq 2, (b, m) = 1$
denote by $\pi(m) = \pi_{(a,b)}(m)$ the period length

Definition, Wall-Sun-Sun primes, WSS primes

(D.D.Wall 1960, Zhi Hong Sun-Zhi Wei Sun 1992)
A prime p is an (a, b)-**WSS prime** if $(b, p) = 1$ and $\pi(p^2) = \pi(p)$
For $a = k, b = 1$ a prime p is a k-**WSS prime** if $\pi(p^2) = \pi(p)$
For $a = 1, b = 1$ a prime p is a **WSS prime**, if $\pi(p^2) = \pi(p)$

$a, b > 0$ integers, $a \not\equiv 0 (\mathrm{mod}\ 4)$, b square-free
$D = a^2 + 4b$ if k is odd, $D = (a/2)^2 + b$ if k is even
D square-free
$s \geq 1$ integer, $\gcd(b, s) = 1$
$\left(\frac{D}{p}\right) \neq 1$ for any prime divisors $p \geq 3$ of s, $\left(\frac{D}{p}\right) = -1$ if $3|s$
$f(x) = x^2 - ax - b, \quad x \leftarrow x^{s^n}$

Theorem, Lenny Jones, 2023

$f(x^{s^n}) = x^{2s^n} - ax^{s^n} - b$ is monogenic for all $n \geq 1 \iff$
no prime divisor of s is an (a, b)-WSS prime.

Number of generators of power integral bases

- S. Akhtari showed that a **positive proportion of cubic number fields**, when ordered by their discriminant, are **not monogenic**;
- L. Alpöge, M. Bhargava, A. Shnidman showed that, if isomorphism classes of cubic fields are ordered by absolute discriminant, then a **positive proportion are not monogenic** and yet have no local obstruction to being monogenic
- M. Bhargava proved that an order O in a **quartic** number field can have at most 2760 inequivalent generators of power integral bases (and at most 182 if $|D(O)|$ is sufficiently large).
- S. Akhtari gave another proof of Bhargava's result

Miscellaneous

- H. H. Kim:the **number of monogenic dihedral quartic** ext with abs disc $\leq X$ is of size $O(X^{3/4}(\log X)^3)$;
- N. Khan, S. Katayama, T. Nakahara and T. Uehara: the **composite of a tot real field with a cyclotomic field** of odd conductor ≥ 3 or even ≥ 8 has no power integral basis;
- N. Khan, T. Nakahara and H. Sekiguchi proved that there are exactly **three monogenic cyclic sextic fields of prime-power conductor**, namely $\mathbb{Q}(\zeta_7), \mathbb{Q}(\zeta_9)$ and the maximal real subfield of $\mathbb{Q}(\zeta_{13})$;
- D. Gil-Muñoz and M. Tinková considered the indices of non-monogenic simplest cubic polynomials;
- M. Castillo showed, e.g., that $\mathbb{Q}(\alpha_n), n \geq 1$ is monogenic, where $\alpha_0 = 1$ and $\alpha_n = \sqrt{2 + \alpha_{n-1}}$ for $n \geq 1$;

Explicit calculations:

frequency of monogenic fields

the behaviour minimal indices of number fields

Frequency of monogenic pure cubic fields $\mathbb{Q}(\sqrt[3]{n})$

D_K	# fields	frequency
$0 \leq \lvert D_K \rvert < 12 \cdot 10^5$	376	0.37
$12 \cdot 10^5 \leq \lvert D_K \rvert < 2 \cdot 12 \cdot 10^5$	178	0.27
$2 \cdot 12 \cdot 10^5 \leq \lvert D_K \rvert < 3 \cdot 12 \cdot 10^5$	137	0.27
$3 \cdot 12 \cdot 10^5 \leq \lvert D_K \rvert < 4 \cdot 12 \cdot 10^5$	122	0.27
$4 \cdot 12 \cdot 10^5 \leq \lvert D_K \rvert < 5 \cdot 12 \cdot 10^5$	116	0.25
$5 \cdot 12 \cdot 10^5 \leq \lvert D_K \rvert < 6 \cdot 12 \cdot 10^5$	97	0.26
$6 \cdot 12 \cdot 10^5 \leq \lvert D_K \rvert < 7 \cdot 12 \cdot 10^5$	86	0.24
$7 \cdot 12 \cdot 10^5 \leq \lvert D_K \rvert < 8 \cdot 12 \cdot 10^5$	80	0.26
$8 \cdot 12 \cdot 10^5 \leq \lvert D_K \rvert < 9 \cdot 12 \cdot 10^5$	80	0.20
$9 \cdot 12 \cdot 10^5 \leq \lvert D_K \rvert < 12 \cdot 10^6$	81	0.21

Averages of min ind of $S_4(c)$ quartic fields (44122)

D_K	$S_4(c)$
$0 < D_K < 100000$	2.2
$100000 \leq D_K < 200000$	3.3
$200000 \leq D_K < 300000$	3.8
$300000 \leq D_K < 400000$	4.4
$400000 \leq D_K < 500000$	4.8
$500000 \leq D_K < 600000$	5.2
$600000 \leq D_K < 700000$	5.5
$700000 \leq D_K < 800000$	5.7
$800000 \leq D_K < 900000$	5.9
$900000 \leq D_K < 1000000$	6.0
Total average	4.8

A diophantine approach:
calculate generators of power integral bases

If we can not exclude the existence of generators of power integral bases (e.g. congruences, Newton Polygon method), then the only way to decide about monogenity is to **solve the index form equation** (a much harder problem)

1. Calculate all generators of power integral bases

1.a. Calculate generators of power integral bases with "small" ($< 10^{500}$) coefficients in the integral basis

2. Consider infinite parametric families of number fields

Cubic fields: the index form equation is a cubic Thue equation

$K = \mathbb{Q}(\xi)$,
$\xi : f(x) = x^3 + a_1 x^2 + a_2 x + a_3$

$$\alpha = \frac{a + x\xi + y\xi^2}{d}$$

Theorem

We have $I(\alpha) = m$ if and only if

$$x^3 - 2a_1 x^2 y + (a_1^2 + a_2)xy^2 - (a_1 a_2 - a_3)y^3 = \pm\frac{d^3 m}{I(\xi)}$$

I. Gaál and N. Schulte (1989)

Example: Simplest cubic fields

$K = \mathbb{Q}(\xi)$, ξ: $P_a(x) = x^3 - ax^2 - (a+3)x - 1$
Integral basis: $(1, \xi, \xi^2)$ if $a^2 + 3a + 9$ is square free

$$\alpha = x_1 + x_2\xi + x_3\xi^2 \quad (u, x, y \in \mathbb{Z})$$

Index form:

$$x_2^3 + 2ax_2^2x_3 + (a^2 - a - 3)x_2x_3^2 + (-a^2 - 3a - 1)x_3^3 = \pm 1 \ \text{ in } \ x, y \in \mathbb{Z}$$

$x_2 = x_0 - ay_0, x_3 = y_0$

$$x_0^3 - ax_0^2y_0 - (a+3)x_0y_0^2 - y_0^3 = \pm 1$$

parametric family of Thue equations, c.f. E.Thomas and others

Quartic fields

$K = \mathbb{Q}(\xi)$ quartic number field
ξ min pol $f(x) = x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 \in \mathbb{Z}[x]$

$$\alpha \in \mathbb{Z}_K : \quad \alpha = \frac{a_\alpha + x\xi + y\xi^2 + z\xi^3}{d}$$

$$F(u,v) = u^3 - a_2 u^2 v + (a_1 a_3 - 4a_4)uv^2 + (4a_2 a_4 - a_3^2 - a_1^2 a_4)v^3$$

$$Q_1(x,y,z) = x^2 - xya_1 + y^2 a_2 + xz(a_1^2 - 2a_2) + yz(a_3 - a_1 a_2)$$
$$+z^2(-a_1 a_3 + a_2^2 + a_4) + yz(a_3 - a_1 a_2) + z^2(-a_1 a_3 + a_2^2 + a_4)$$

$$Q_2(x,y,z) = y^2 - xz - a_1 yz + z^2 a_2$$

Theorem(I.Gaál, A.Pethő and M.Pohst 1996)

Let $i_m = d^6 m/n$ where $n = I(\xi)$.
$I(\alpha) = m$ if and only if there is a solution $(u, v) \in \mathbb{Z}^2$ of

$$F(u, v) = \pm i_m$$

such that (x, y, z) satisfies

$$Q_1(x, y, z) = u, \quad Q_2(x, y, z) = v.$$

Mordell:
$Q_0(x,y,z) = uQ_2(x,y,z) - vQ_1(x,y,z) = 0 \implies$
$kx = f_x(p,q), ky = f_y(p,q), kz = f_z(p,q)$

Theorem (I.Gaál, A.Pethő and M.Pohst 1996)

At least one of the equations

$$F_1(p,q) = Q_1(f_x(p,q), f_y(p,q), f_z(p,q)) = k^2 u$$

$$F_2(p,q) = Q_2(f_x(p,q), f_y(p,q), f_z(p,q)) = k^2 v$$

is a Thue equation over K.

(k divides a small integer)

An example

$D_K = 15188, f(x) = x^4 - x^3 - 7x^2 + x + 2$, Galois group S_4,
integral basis $(1, \xi, \xi^2, (\xi + \xi^3)/2), n = 2, m(K) = 1,$
$m = 1, F(u, v) = u^3 + 7u^2v - 9uv^2 - 59v^3 = \pm 32$

$F_2(p, q) = p^4 + 14p^3q + 52p^2q^2 + 22pq^3 - q^4 = \pm 2, \pm 8, \pm 32$
$F_2(p, q) = 2(p^4 + 11p^3q + 33p^2q^2 + 19pq^3 - 26q^4) = \pm 2, \pm 8$
$F_2(p, q) = 2(11p^4 + 119p^3q + 447p^2q^2 + 649pq^3 + 248q^4) = \pm 2, \pm 8$

Minimal index: $\mu(K) = 1,$
Solutions: (1,–2,1),(2,1,–1),(4,1,–1),(12,1,–3)

An infinite family of totally real bicyclic biquadratic number fields
(I.Gaál and B.Jadrijevic, 2018)

$K = \mathbb{Q}(\sqrt{2c}, \sqrt{2(c+4)})$, $c \neq 2$, $c, c+4$ squarefree
ξ a root of $f(x) = x^4 - (2c+4)x^2 + 4$
An integral basis of K is given by
$\left(1, \xi, \frac{\xi^2}{2}, \frac{\xi^3}{2}\right)$, if c is odd
$\left(1, \xi, \frac{\xi^2+2\xi+2}{4}, \frac{\xi^3+2\xi+4}{8}\right)$, if $c \equiv 2 \pmod 8$
$\left(1, \xi, \frac{\xi^2+2\xi+2}{4}, \frac{\xi^3+6\xi+4}{8}\right)$, if $c \equiv 6 \pmod 8$.
There are no power integral bases of K
Elements of minimal index are determined: 4,23,31,32

Calculating relativ power integral bases in a family of quartic extensions of imaginary quadratic fields (Z.Franusic and B.Jadrijevic, 2018)

$M = \mathbb{Q}(\sqrt{-D})$
$f(x) = x^4 - 2cx^3 + 2x^2 + 2cx + 1,\ f(\xi) = 0$
$K = M(\xi)$
describe generators of relative power integral bases
of $\mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$

An attempt to use a general direct method

Applying the genaral approach using unit equations for
—$n = 5$: I.Gaál, K.Győry (1999)
—$n = 6$: Y.Bilu, I.Gaál, K.Győry (2004)
for $n = 5$: $r \leq 9$,
for $n = 6$: $r \leq 14$
CPU time:
—$n = 5$: 8 hours!!!!
—$n = 6$: 4.5 months!!!!
The direct method is not applicable in practice!
(Baker's method, LLL reduction, enumeration method, sieving)

How to construct faster algorithms?

The algorithms are much more efficient if we consider the special structure of number fields

—consider **special types** of higher degree number fields
—consider composites of number fields
—reduce index form equations to **Thue and relative Thue equations** if possible
—factor the index form (subfields, subgroups of the Galois group) —find relations between the factors

Sextic fields with a quadratic subfield

M: quadratic field with integral basis $(1, \omega)$
$K = \mathbb{Q}(\vartheta)$ sextic field, ϑ rel min pol:
$f(t) = t^3 + \gamma_2 t^2 + \gamma_1 t + \gamma_0 \in \mathbb{Z}_M[t]$
Let $\vartheta^{(1)}$ and $\vartheta^{(2)}$ be distinct roots of $f(t)$ and put
$\rho = -\vartheta^{(1)} - \vartheta^{(2)}$.
Integral basis of K (99%): $(1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2)$

$$\alpha = x_1 + x_2\vartheta + x_3\vartheta^2 + y_1\omega + +y_2\omega\vartheta + y_3\omega\vartheta^2$$

Theorem(I.Gaál, 1995,...)

If α has index 1, then $(X, Y) = (x_2 + \omega y_2, x_3 + \omega y_3)$ is a solution of the relative Thue equation

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

where ν is a unit in M, and

$$F(x_2, x_3, y_1, y_2, y_3) = \pm 1,$$

with a homogeneous polynomial F of degree 9 with integer coefficients.

Relative extensions (I.Gaál, L.Remete and T.Szabó, 2016)

$$Q \subset M \subset K,\ \alpha \in \mathbb{Z}_K$$

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

$$I(\alpha) = I_{K/M}(\alpha) \cdot J(\alpha)$$

Definition

relative index: $I_{K/M}(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}_M[\alpha]^+)$.

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

Statement

Let $\mathbb{Q} \subset M \subset K$. If $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ then $I(\alpha) = 1$, therefore $I_{K/M}(\alpha) = 1$. Hence α is $\mathbb{Z}_M$-**equivalent** to a generator of a relative power integral basis:

$$\alpha = a + \varepsilon\beta$$

where $I_{K/M}(\beta) = 1$, $a \in \mathbb{Z}_M$, $\varepsilon \in U_M$.

Calculate generators of power integral bases into two consecutive steps:

Calculate generators of power integral bases from generators of relative power integral bases:

1. Determine β from $I_{K/M}(\beta) = 1$ and then
2. Determine $a \in \mathbb{Z}_M$, $\varepsilon \in U_M$ from $J(\alpha) = 1$.

Simplest D_4 octics (I.Gaál, L.Remete and T.Szabó (2016)

B.K.Spearman and K.S.Williams (2008)
$t < 0, t^2 + 4$ square free, ϑ a root of

$$x^8 + (t^2 + 2)x^4 + 1 = (x^4 + itx^2 + 1)(x^4 - itx^2 + 1)$$

$K = \mathbb{Q}(\vartheta) \supset M = \mathbb{Q}(i)$ relative quartic extension
Galois group D_4, integral basis given :

$$(1, \vartheta, \vartheta^2, \vartheta^3, i, i\vartheta, i\vartheta^2, i\vartheta^3)$$

apply the method for quartic fields in the relative case
(I.Gaál and M.Pohst, (2000)) and a result of V.Ziegler (2006):

Theorem

For $t > 11$ up to equivalence the only generators of **relative power integral bases** of $\mathbb{Z}_K$ over $\mathbb{Z}_M$ are given by

$$\alpha =$$

$$\vartheta, \quad -2it^2\vartheta + \vartheta^3,$$
$$(1 + 4t^4)\vartheta \pm (1 + i)t\vartheta^2 + 2it^2\vartheta^3,$$
$$\pm(1 + i)t\vartheta^2 + \vartheta^3$$

Theorem

For $t > 11$ $\mathbb{Z}_K$ is **not monogenic**.

Composite fields

$[L : \mathbb{Q}] = \ell$, $[M : \mathbb{Q}] = m$, $K = LM$, $[K : \mathbb{Q}] = \ell \cdot m$

$\alpha \in \mathbb{Z}_K$:

$$I(\alpha) = I_{K/L}(\alpha) J_L(\alpha)$$

$$I(\alpha) = I_{K/M}(\alpha) J_M(\alpha)$$

$$I(\alpha) = I_{K/M}(\alpha) \cdot I_{K/L}(\alpha) \cdot J_{L,M}(\alpha)$$

$L,\ D_L,\ (l_1 = 1, l_2, \ldots, l_r),\ I_L(x_2, \ldots, x_r)$
$M,\ D_M,\ (m_1 = 1, m_2, \ldots, m_s),\ I_M(x_2, \ldots, x_s)$
Assume $(D_L, D_M) = 1$. Then any $\alpha \in \mathbb{Z}_K$:

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

Theorem(I.Gaál, 1998)

If α generates a power integral basis in $K = LM$ then

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

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

Remarks:

—In case of a cubic extension the equation is a relative Thue equation

—The above equations are equivalent to

$$I_{K/M}(\alpha) = 1 \quad \text{and} \quad I_{K/L}(\alpha) = 1.$$

The third factor of the index is

$$J_{L,M}(\alpha) = 1.$$

Composites of totally real fields and imaginary quadratic fields

$f(x) \in \mathbb{Z}[x]$ irred. $\xi = \xi^{(1)}, \ldots, \xi^{(n)} \in \mathbb{R}$,
$L = \mathbb{Q}(\xi)$ integral basis $(\ell_1 = 1, \ell_2, \ldots, \ell_n)$, discriminant D_L
index form $I_L(x_2, \ldots, x_n)$
$0 < d \in \mathbb{Z}$ square-free integer,
Let $M = \mathbb{Q}(i\sqrt{d})$, integral basis $(1, \omega)$, discriminant D_M

Set $K = L \cdot M$, assume $(D_L, D_M) = 1$

$\alpha \in \mathbb{Z}_K$:
$\alpha = x_1 + x_2\ell_2 + \ldots x_n\ell_n + y_1\omega + y_2\omega\ell_2 + \ldots + y_n\omega\ell_n =$
$X_1 + X_2\ell_2 + \ldots + X_n\ell_n$
with $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{Z}$ and $X_j = x_j + \omega y_j \in \mathbb{Z}_M$

Lemma (I.Gaál, 2020)

If α generates a power integral basis in K then

$$N_{M/Q}(I_L(X_2, \ldots, X_n)) = \pm 1, \tag{2}$$

$$N_{L/Q}(y_1 + y_2\ell_2 + \ldots + y_n\ell_n) = \pm 1,$$

and

$$F(x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) = \pm 1.$$

(2) implies:

Theorem (I.Gaál, 2020)

Assume α generates a power integral basis in K.
If $-d \equiv 2, 3 \pmod 4$, then

$$|I_L(x_2, \ldots, x_n)| \leq 1,$$

$$|I_L(y_2, \ldots, y_n)| \leq \frac{1}{(\sqrt{d})^{n(n-1)/2}}.$$

If $-d \equiv 1 \pmod 4$, then

$$|I_L(2x_2 + y_2, \ldots, 2x_n + y_n)| \leq 2^{n(n-1)/2},$$

$$|I_L(y_2, \ldots, y_n)| \leq \left(\frac{2}{\sqrt{d}}\right)^{n(n-1)/2}.$$

$\alpha = x_1 + x_2\ell_2 + \ldots x_n\ell_n + y_1\omega + y_2\omega\ell_2 + \ldots + y_n\omega\ell_n$
If $d \neq 1, 3$ then $\mathbb{Z}_K = \mathbb{Z}[\alpha] \Longrightarrow$
$y_2 = \ldots y_n = 0, \quad y_1 = \pm 1, \quad I_L(x_2, \ldots, x_n) = \pm 1$

As a consequence of the above arguments we have

Theorem (I.Gaál, 2020)

If $d \neq 1, 3$ then all generators of power integral bases of K are of the form

$$\alpha = x + \beta \pm \omega$$

where β generates a power integral basis in L and $x \in \mathbb{Z}$ is arbitrary.

Proof

$\alpha = x_1 + x_2\ell_2 + \ldots x_n\ell_n + y_1\omega + y_2\omega\ell_2 + \ldots + y_n\omega\ell_n$
conjugates corresponding to $\omega^{(k)}, \xi^{(j)}: \quad \ell_h^{(j)}, \alpha^{(j,k)}$
$X_j = x_j + \omega y_j \in \mathbb{Z}_M$

$$|N_{M/Q}(I_L(X_2, \ldots, X_n))| = \prod_{k=1}^{2} \left(\frac{1}{|\sqrt{D_L}|} \prod_{1 \le j_1 < j_2 \le n} \left| \alpha^{(j_1,k)} - \alpha^{(j_2,k)} \right| \right)$$

If $-d \equiv 2, 3 \pmod 4$, then

$$\mathrm{Re}(\alpha^{(j_1,k)} - \alpha^{(j_2,k)}) = x_2(\ell_2^{(j_1)} - \ell_2^{(j_2)}) + \ldots + x_n(\ell_n^{(j_1)} - \ell_n^{(j_2)})$$

and

$$\mathrm{Im}(\alpha^{(j_1,k)} - \alpha^{(j_2,k)}) = \sqrt{d} \cdot \left(y_2(\ell_2^{(j_1)} - \ell_2^{(j_2)}) + \ldots + y_n(\ell_n^{(j_1)} - \ell_n^{(j_2)}) \right).$$

$$|I_L(x_2,\ldots,x_n)|^2 = |N_{M/Q}(I_L(x_2,\ldots,x_n))|$$

$$= \prod_{k=1}^{2}\left(\frac{1}{|\sqrt{D_L}|}\prod_{1\le j_1<j_2\le n}\left|x_2(\ell_2^{(j_1)}-\ell_2^{(j_2)})+\ldots+x_n(\ell_n^{(j_1)}-\ell_n^{(j_2)})\right|\right)$$

$$= \prod_{k=1}^{2}\left(\frac{1}{|\sqrt{D_L}|}\prod_{1\le j_1<j_2\le n}\left|\mathrm{Re}(\alpha^{(j_1,k)}-\alpha^{(j_2,k)})\right|\right)$$

$$\le \prod_{k=1}^{2}\left(\frac{1}{|\sqrt{D_L}|}\prod_{1\le j_1<j_2\le n}\left|\alpha^{(j_1,k)}-\alpha^{(j_2,k)}\right|\right)$$

$$= |N_{M/Q}(I_L(X_2,\ldots,X_n))| \le 1$$

$$\left(\sqrt{d}\right)^{n(n-1)} |I_L(y_2,\ldots,y_n)|^2 = \left(\sqrt{d}\right)^{n(n-1)} |N_{M/Q}(I_L(y_2,\ldots,y_n))|$$

$$= \prod_{k=1}^{2} \left(\frac{1}{|\sqrt{D_L}|} \prod_{1\le j_1<j_2\le n} \sqrt{d} \left| y_2(\ell_2^{(j_1)} - \ell_2^{(j_2)}) + \ldots + y_n(\ell_n^{(j_1)} - \ell_n^{(j_2)}) \right| \right)$$

$$= \prod_{k=1}^{2} \left(\frac{1}{|\sqrt{D_L}|} \prod_{1\le j_1<j_2\le n} \left| \mathrm{Im}(\alpha^{(j_1,k)} - \alpha^{(j_2,k)}) \right| \right)$$

$$\le \prod_{k=1}^{2} \left(\frac{1}{|\sqrt{D_L}|} \prod_{1\le j_1<j_2\le n} \left| \alpha^{(j_1,k)} - \alpha^{(j_2,k)} \right| \right)$$

$$= |N_{M/Q}(I_L(X_2,\ldots,X_n))| \le 1$$

Example: Composites of simplest quartic fields with imaginary quadratic fields

$a > 0$, $a \neq 3$, ξ a root of $f(x) = x^4 - ax^3 - 6x^2 + ax + 1$
$L = \mathbb{Q}(\xi)$ simplest quartic fields (M.N.Gras)
P.Olajos (2005): power integral basis exists only for $a = 2, 4$
I.Gaál and G.Petrányi (2014):
minimal indices and elements of minimal index

$M = \mathbb{Q}(i\sqrt{d})$, $(D_M, D_L) = 1$, $K = L \cdot M$

Theorem (I.Gaál, 2020)

For $d \neq 3$ the field K is not monogenic.

Monogenity in a family of cyclic sextic fields (I.Gaál, 2025)

$$f(x) = x^6 + (n^2+5)x^4 + (n^2+2n+6)x^2 + 1$$

Theorem

(L. Jones, 2025) $f(x)$ is irreducible for all $n \in \mathbb{Z}$, and is monogenic exactly for $n = -2, -1, 0, 1$.

$f(\xi) = 0$, $K = \mathbb{Q}(\xi)$ cyclic sextic field

Subfields: $M = \mathbb{Q}(i)$, $L = \mathbb{Q}(\alpha)$ totally real cubic

$g(\alpha) = 0$, $g(x) = x^3 + (n^2+5)x^2 + (n^2+2n+6)x + 1$,

$K = L \cdot M$, $(D_L, D_M) = 1$

If $(1, \beta_2, \beta_3)$ is an integral basis of L, then $(1, \beta_2, \beta_3, i, i\beta_2, i\beta_3)$ is integral basis in K

$$\gamma = x_1 + x_2\beta_2 + x_3\beta_3 + iy_1 + iy_2\beta_2 + iy_3\beta_3 \in \mathbb{Z}_K$$

Theorem

$n = -56, -14, -7, -5, -2, -1, 0, 1, 4, 6, 13$ are the only values of n with $-100 \leq n \leq 100$, such that K admits generators of power integral bases with coefficients $\leq 10^{100}$ in the integral basis.

$n = -56$, integral basis of L: $\left(1, \frac{x+4}{7}, \frac{x^2+9353x+18531}{150871}\right)$

$(x_2, x_3, y_1, y_2, y_3) = (0,0,9,-49,170), (0,0,10,-49,170), (0,0,-4,17,-59),$
$(0,0,-3,17,-59), (0,0,-5,32,-111), (0,0,-4,32,-111)$

$n = -14$, integral basis of L: $\left(1, \frac{x+1}{3}, \frac{x^2+32x+1282}{1629}\right)$

$(x_2, x_3, y_1, y_2, y_3) = (0,0,12,-5,-16), (0,0,13,-5,-16), (0,0,11,-4,-13),$
$(0,0,12,-4,-13), (0,0,-25,9,29), (0,0,-24,9,29)$

$n = -7$, integral basis of L: $\left(1, x, \frac{x^2+141x+254}{287}\right)$

$(x_2, x_3, y_1, y_2, y_3) = (0,0,-19,-7,23), (0,0,-18,-7,23), (0,0,7,3,-10),$
$(0,0,8,3,-10), (0,0,11,4,-13), (0,0,12,4,-13)$

$n = -5$, integral basis of L: $\left(1, x, \frac{x^2+14x+25}{57}\right)$

$(x_2, x_3, y_1, y_2, y_3) = (0,0,0,-2,-7), (0,0,1,-2,-7), (0,0,1,-1,-4),$
$(0,0,2,-1,-4), (0,0,-4,3,11), (0,0,-3,3,11)$

$n = -2$, integral basis of L: $(1, x, x^2)$

$(x_2, x_3, y_1, y_2, y_3) = (0,0,-5,-17,-2), (0,0,-4,-17,-2), (0,0,-4,-9,-1),$

$(0,0,-3,-9,-1), (0,0,9,26,3), (0,0,10,26,3)$

$n = -1$, integral basis of L: $(1, x, x^2)$
$(x_2, x_3, y_1, y_2, y_3) = (0, 0, -4, -6, -1), (0, 0, -3, -6, -1), (0, 0, -2, -5, -1),$
$(0, 0, -1, -5, -1), (0, 0, 4, 11, 2), (0, 0, 5, 11, 2)$

$n = 0$, integral basis of L: $(1, x, x^2)$
$(x_2, x_3, y_1, y_2, y_3) = (0, 0, -1, -3, -1), (0, 0, 0, -3, -1), (0, 0, -2, -1, 0),$
$(0, 0, -1, -1, 0), (0, 0, 2, 4, 1), (0, 0, 3, 4, 1)$

$n = 1$, integral basis of L: $(1, x, x^2)$
$(x_2, x_3, y_1, y_2, y_3) = (0, 0, -1, -3, -1), (0, 0, 0, -3, -1), (0, 0, -3, -1, 0),$
$(0, 0, -2, -1, 0), (0, 0, 1, 4, 1), (0, 0, 2, 4, 1)$

$n = 4$, integral basis of L: $\left(1, x, \frac{x^2 + 53x + 16}{57}\right)$
$(x_2, x_3, y_1, y_2, y_3) = (0, 0, 0, -4, 7), (0, 0, 1, -4, 7), (0, 0, -1, 1, -2),$
$(0, 0, 0, 1, -2), (0, 0, 1, 3, -5), (0, 0, 2, 3, -5)$

$n = 6$, integral basis of L: $\left(1, x, \frac{x^2 + 74x + 200}{287}\right)$
$(x_2, x_3, y_1, y_2, y_3) = (0, 0, -11, -2, 17), (0, 0, -10, -2, 17), (0, 0, 4, 1, -9),$
$(0, 0, 5, 1, -9), (0, 0, 5, 1, -8), (0, 0, 6, 1, -8)$

$n = 13$, integral basis of L: $\left(1, x, \frac{x^2 + 521x + 169}{1629}\right)$
$(x_2, x_3, y_1, y_2, y_3) = (0, 0, 4, -16, 25), (0, 0, 5, -16, 25), (0, 0, -3, 7, -11),$

$(0, 0, -2, 7, -11), (0, 0, -2, 9, -14), (0, 0, -1, 9, -14)$

$$S = \{n \ : \ n \in [-1000, -100) \cup (100, 1000], \quad n^2+n+7 \text{ square free}\}.$$

The set S contains 1110 parameters n.
Integral basis of L in all cases: $(1, \alpha, \beta)$,

$$\beta = \frac{\alpha^2 + (n^2 - n + 3)\alpha + n^2}{n^2 + n - 1}.$$

$$\gamma = x_1 + x_2\alpha + x_3\beta + iy_1 + iy_2\alpha + iy_3\beta \in \mathbb{Z}_K$$

Theorem

For $n \in S$ there are no generators γ of power integral bases of K with coefficients $x_2, x_3, y_1, y_2, y_3 \in \mathbb{Z}$ having absolute values $< 10^{100}$.

Computational aspects:

Maple: solving cubic Thue equations

$-100 \leq n \leq +100$: 30 minutes, out of which
$-50 \leq n \leq +50$: 1.5 minutes

$n \in S$: 39 minutes

Generators of power integral bases in totally complex pure sextic fields (I.Gaál, 2023)

$0 \neq m \in \mathbb{Z}$ sixth power-free, $\alpha = \sqrt[6]{m}$,
$K = \mathbb{Q}(\alpha)$, with ring of integers $\mathbb{Z}_K$.

Theorem (Lhoussain El Fadil)

α generates a power integral basis in K, if and only if

(*) m is square-free, $m \not\equiv 1 \pmod 4$ and $m \not\equiv \pm 1 \pmod 9$.

Theorem

In the 1521 fields with $0 > m > -5000$ with property (*) up to equivalence α is the only generator of power integral basis with coefficients $< 10^{100}$ in the integral basis $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ of K

Conjecture

Up to equivalence α is the only generator of power integral basis in K

Remarks on CPU times

- complete resolution, general method for sextic fields (unit equations): **4.5 months**
- complete resolution, sextic fields with a quadratic subfield: **3 hours**
- pure sextic fields:
  complete resolution: **14 minutes**
  "small" solutions: **12 seconds**

Generators of power integral bases in totally complex pure octic fields, I.Gaál, 2023

$0 \neq m \in \mathbb{Z}$, $\alpha = \sqrt[8]{m}$, $K = \mathbb{Q}(\alpha)$ with ring of integers $\mathbb{Z}_K$.

Theorem, L. El Fadil and I. Gaál, 2023

α generates a power integral basis in K, if and only if
(*) $m \neq 1$ is square-free, $m \not\equiv 1 \pmod 4$.

$(1, \alpha, \alpha^2, \alpha^3, \sqrt{m}, \alpha\sqrt{m}, \alpha^2\sqrt{m}, \alpha^3\sqrt{m})$ is also an integral basis

$$\gamma = x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3 + y_0\sqrt{m} + y_1\alpha\sqrt{m} + y_2\alpha^2\sqrt{m} + y_3\alpha^3\sqrt{m}$$

$$\max(|y_0|, |x_1|, |y_1|, |x_2|, |y_2|, |x_3|, |y_3|) < 10^{200}.$$

Theorem

In the 2024 fields $K = \mathbb{Q}(\sqrt[8]{m})$ with $0 > m > -5000$ satisfying (*), up to equivalence $\sqrt[8]{m}$ is the only generator of power integral bases with the above properties, except for $m = -1$, when we additionally have $i\sqrt[8]{m}, (\sqrt[8]{m})^3, i(\sqrt[8]{m})^3$.

Conjecture

If $m < 0$ satisfies (*) then up to equivalence $\sqrt[8]{m}$ is the only generator of power integral bases in $K = \mathbb{Q}(\sqrt[8]{m})$, except for $m = -1$, when we additionally have $i\sqrt[8]{m}, (\sqrt[8]{m})^3, i(\sqrt[8]{m})^3$.

A family of even octic reciprocal polynomials (I.Gaál, 2025)

$f(x) = x^8 + ax^6 + bx^4 + ax^2 + 1$ with $a, b \in \mathbb{Z}$.
Set $W_1 = b + 2 - 2a$, $W_2 = b + 2 + 2a$, $W_3 = a^2 - 4b + 8$

Theorem (L. Jones, 2024-2025)

If $W_1 W_2 W_3$ is square free and

$$(a \bmod 4,\ b \bmod 4) \in \{(1,3),(3,1),(3,3)\}$$

then the polynomial $f(x)$ is monogenic.

$f(x) = x^8 + ax^6 + bx^4 + ax^2 + 1$
$f(\alpha) = 0$, $K = \mathbb{Q}(\alpha)$
consider parameters a, b such that $f(x)$ is **monogenic**
(not necessarily satisfying the above condition)

Are there any further generators of power integral bases of K in addition to α?

$f(x) = x^8 + ax^6 + bx^4 + ax^2 + 1$, $f(\alpha) = 0$
$g(x) = x^4 + ax^3 + bx^2 + ax + 1$, $\beta = \alpha^2$ is a root of $g(x)$

$$\mathbb{Q} \overset{4}{\subset} L = \mathbb{Q}(\beta) \overset{2}{\subset} K = \mathbb{Q}(\alpha).$$

But

$$\beta^4 + a\beta^3 + b\beta^2 + a\beta + 1 = 0,$$

$$\left(\beta + \frac{1}{\beta}\right)^2 + a\left(\beta + \frac{1}{\beta}\right) + b - 2 = 0.$$

Hence $\delta = \beta + \frac{1}{\beta}$, and satisfies $\delta^2 + a\delta + (b-2) = 0$

$$\mathbb{Q} \overset{2}{\subset} M = \mathbb{Q}(\delta) \overset{4}{\subset} K = \mathbb{Q}(\alpha)$$

$h(x) = x^4 - \delta x^2 + 1$ is the relative def polynomial of α over M

$$\delta = \frac{-a + \sqrt{a^2 - 4b + 8}}{2},$$

$m = W_3 = a^2 - 4b + 8 < 0$ square-free

$m \equiv 1 \pmod 4$, integral basis of M: $(1, \omega)$,$\omega = \frac{1+\sqrt{m}}{2}$

If K is monogenic, then it is also relative monogenic over M:

$$\mathbb{Z}_K \ni \gamma = C + X\alpha + Y\alpha^2 + Z\alpha^3$$

$$C = c_1 + \omega c_2, X = x_1 + \omega x_2, Y = y_1 + \omega y_2, Z = z_1 + \omega z_2 \in \mathbb{Z}_M$$

with $c_1, c_2, x_1, x_2, y_1, y_2, z_1, z_2 \in \mathbb{Z}$.

$$N_{M/\mathbb{Q}}(F(U,V)) = \pm 1.$$

$$F(U,V) = (U-2V)(U+2V)(U+\delta V),\ U=\varepsilon, V=0$$

$$Q_1(X,Y,Z) = \varepsilon,\ Q_2(X,Y,Z) = 0$$

$$Q_0(X,Y,Z) = UQ_2 - VQ_1 = 0, \quad X_0 = 1, Y_0 = 0, Z_0 = 0$$

$$Q_2(X,Y,Z) = Y^2 - XZ - \delta Z^2 = 0.$$

$$X = RX_0, Y = RY_0 + P, Z = RZ_0 + Q, \quad RQ = P^2 - \delta Q^2$$

$$kX = P^2 - \delta Q^2, kY = PQ, kZ = Q^2$$

$$F(P,Q) = P^4 - \delta P^2 Q^2 + Q^4 = \varepsilon,$$

Solving

$$F(P,Q) = P^4 - \delta P^2 Q^2 + Q^4 = \varepsilon,$$

calculating "small" solutions $P = p_1 + \omega p_2, Q = q_1 + \omega q_2$ with coeff $|p_i|, |q_i| \leq 10^{200} \Rightarrow$ determining all generators γ_0 of relative power integral bases of K over M

$$\gamma = c_1 + \omega c_2 + \varepsilon \gamma_0,$$

few possible units $\varepsilon \in M$,
$J(\gamma) = 1$ a polynomial equation of degree 16 in c_2

Numerical calculations

51 examples (526 sec): $-25 \le a \le 25, 2 \le b \le 25$,

$m < 0$ squarefree, $f(x)$ irred, monogenic

$$\gamma = (c_1 + \omega c_2) + (x_1 + \omega x_2)\alpha + (y_1 + \omega y_2)\alpha^2 + (z_1 + \omega z_2)\alpha^3.$$

$(a, b, m), (c_2, x_1, x_2, y_1, y_2, z_1, z_2) = (0, 1, 0, 0, 0, 0, 0)$ and

$(-9, 23, -3)$,	$[0, 4, 1, 0, 0, -1, 0]$		
$(-7, 15, -3)$,	$[0, 3, 1, 0, 0, -1, 0]$		
$(-7, 19, -19)$,	$[0, 3, 1, 0, 0, -1, 0]$		
$(-7, 23, -35)$,	$[0, 3, 1, 0, 0, -1, 0]$		
$(-5, 9, -3)$,	$[0, 2, 1, 0, 0, -1, 0]$,	$[1, -2, 1, 1, -1, 1, -1]$,	$[1, 2, -1, 1, -1, -1, 1]$
$(-5, 10, -7)$,	$[0, 2, 1, 0, 0, -1, 0]$		
$(-5, 11, -11)$,	$[0, 2, 1, 0, 0, -1, 0]$		
$(-5, 14, -23)$,	$[0, 2, 1, 0, 0, -1, 0]$		
$(-5, 18, -39)$,	$[0, 2, 1, 0, 0, -1, 0]$		
$(-5, 19, -43)$,	$[0, 2, 1, 0, 0, -1, 0]$		
$(-5, 21, -51)$,	$[0, 2, 1, 0, 0, -1, 0]$		
$(-5, 22, -55)$,	$[0, 2, 1, 0, 0, -1, 0]$		
$(-5, 23, -59)$,	$[0, 2, 1, 0, 0, -1, 0]$		
$(-5, 25, -67)$,	$[0, 2, 1, 0, 0, -1, 0]$		
$(-3, 7, -11)$,	$[0, 1, 1, 0, 0, -1, 0]$		
$(-3, 15, -43)$,	$[0, 1, 1, 0, 0, -1, 0]$		
$(-1, 3, -3)$,	$[0, 0, 1, 0, 0, -1, 0]$,	$[0, 1, -1, 0, 0, 0, 1]$,	$[0, 1, 0, 0, 0, -1, 1]$,
		$[0, 1, -1, 0, 0, 0, 0]$,	$[0, 0, 1, 0, 0, 0, 0]$

$(-1, 6, -15)$, $[0, 0, 1, 0, 0, -1, 0]$
$(-1, 7, -19)$, $[0, 0, 1, 0, 0, -1, 0]$
$(-1, 10, -31)$, $[0, 0, 1, 0, 0, -1, 0]$
$(-1, 11, -35)$, $[0, 0, 1, 0, 0, -1, 0]$
$(-1, 13, -43)$, $[0, 0, 1, 0, 0, -1, 0]$
$(-1, 15, -51)$, $[0, 0, 1, 0, 0, -1, 0]$
$(-1, 17, -59)$, $[0, 0, 1, 0, 0, -1, 0]$
$(-1, 19, -67)$, $[0, 0, 1, 0, 0, -1, 0]$
$(-1, 22, -79)$, $[0, 0, 1, 0, 0, -1, 0]$
$(1, 3, -3)$, $[0, -1, 1, 0, 0, -1, 0]$, $[0, 0, 0, 1, -1, 0, 1]$, $[0, 0, 1, 0, 0, -1, 1]$,
$[0, 1, 0, 0, 0, 0, 1]$, $[0, 0, 0, 1, -1, 0, -1]$,
$[1, -1, 2, -1, 1, -1, 0]$, $[1, 1, -2, -1, 1, 1, 0]$,
$[0, 1, -1, 0, 0, 0, 0]$, $[0, 0, 1, 0, 0, 0, 0]$

$(1, 7, -19)$, $[0, -1, 1, 0, 0, -1, 0]$
$(1, 11, -35)$, $[0, -1, 1, 0, 0, -1, 0]$
$(1, 15, -51)$, $[0, -1, 1, 0, 0, -1, 0]$
$(1, 19, -67)$, $[0, -1, 1, 0, 0, -1, 0]$
$(3, 5, -3)$, $[0, -2, 1, 0, 0, -1, 0]$, $[0, 1, -2, 0, 0, 1, -1]$, $[0, -1, -1, 0, 0, 0, -1]$,
$[-1, 1, 0, 0, -1, 1, 0]$, $[1, 1, 0, 0, 1, 1, 0]$,
$[0, 0, -2, 0, -1, 1, -1]$, $[0, 0, -2, 0, 1, 1, -1]$,
$[0, 1, -1, 0, 0, 0, 0]$, $[0, 0, 1, 0, 0, 0, 0]$

$(3, 6, -7)$, $[0, -2, 1, 0, 0, -1, 0]$
$(3, 7, -11)$, $[0, -2, 1, 0, 0, -1, 0]$
$(3, 9, -19)$, $[0, -2, 1, 0, 0, -1, 0]$
$(3, 14, -39)$, $[0, -2, 1, 0, 0, -1, 0]$
$(3, 15, -43)$, $[0, -2, 1, 0, 0, -1, 0]$
$(3, 18, -55)$, $[0, -2, 1, 0, 0, -1, 0]$
$(3, 21, -67)$, $[0, -2, 1, 0, 0, -1, 0]$
$(3, 25, -83)$, $[0, -2, 1, 0, 0, -1, 0]$
$(5, 11, -11)$, $[0, -3, 1, 0, 0, -1, 0]$

In addition to (0,1,0,0,0,0,0), there is another solution with (0,k,1,0,0,-1,0) where k seems to be related to a.

$$k = -\frac{a+1}{2}.$$

Theorem

If $f(x)$ is monogenic and m is square free, then

$$\gamma = \left(-\frac{a+1}{2} + \omega\right)\alpha - \alpha^3$$

also generates a power integral basis in K.

Sextic fields with a real quadratic subfield, I.Gaál, 2025

$M = \mathbb{Q}(\sqrt{m})$ ($m > 1$ square free), $(1, \omega)$
$K = M(\alpha)$, α rel def pol: $f(x) = x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Z}_M$

Integral basis: $(1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2)$
$\gamma = A + X\alpha + Y\alpha^2 \in \mathbb{Z}_M$
$A = a_1 + \omega a_2, X = x_1 + \omega x_2, Y = y_1 + \omega y_2$
with $a_1, a_2, x_1, x_2, y_1, y_2 \in \mathbb{Z}$
$\max(|a_2|, |x_1|, |x_2|, |y_1|, |y_2|) < C, \qquad C = 10^{50}$

$$I(\gamma) = I_{K/M}(\gamma) \cdot J(\gamma)$$

$$N_{M/\mathbb{Q}}(N_{K/M}(X - \vartheta Y)), \quad \vartheta = f_2 + \alpha$$

The fast method for finding "small" solutions of relative Thue equations does not work in this case.
Is there another efficient method?

$$X - \vartheta Y = \eta^k \varepsilon_1^{k_1} \cdots \varepsilon_h^{k_h}$$

η unit in M, $\varepsilon_1, \ldots, \varepsilon_h$ relative units of K over M

$$\max(|k|, |k_1|, \ldots, |k_h|) \leq \log C$$

$$X' - \vartheta Y' = \eta^{-k}(X - \vartheta Y) = \varepsilon_1^{k_1} \cdots \varepsilon_h^{k_h}$$

using sieve method diminish the number of possible $(k_1, \ldots, k_h)$ considerably

Siegel's identity:

$$(\vartheta^{(1,1)} - \vartheta^{(1,2)})(X' - \vartheta^{(1,3)}Y')$$

$$+(\vartheta^{(1,2)}-\vartheta^{(1,3)})(X'-\vartheta^{(1,1)}Y')+(\vartheta^{(1,3)}-\vartheta^{(1,1)})(X'-\vartheta^{(1,2)}Y') = 0.$$

$$f_{\mathbb{Q}}(x) = (x-r_1)(x-r_2)(x-r_3)(x-r_4)(x-r_5)(x-r_6) \pmod{p}.$$

the mod $\mathfrak{p}$ congruence implies a mod p congruence:

$$(t_{(1,1)} - t_{(1,2)})e_{1,(1,3)}^{k_1} \cdots e_{h,(1,3)}^{k_h} + (t_{(1,2)} - t_{(1,3)})e_{1,(1,1)}^{k_1} \cdots e_{h,(1,1)}^{k_h}$$

$$+(t_{(1,3)} - t_{(1,1)})e_{1,(1,2)}^{k_1} \cdots e_{h,(1,2)}^{k_h} \equiv 0 \pmod{p}.$$

out of 93025 possible $(k_1, \ldots, k_h)$ only 122 survived

Having all generators γ_0 of relative power integral bases of K over M:

$$\gamma = a_1 + a_2\omega \pm \eta^k \gamma_0$$

$k \leq \log C$, for all k calculate a_2 from $J(\gamma) = 1$
(find integer roots of polynomials with integer coefficients)

Example
$f(x) = x^3 + (2+\sqrt{2})x + (1+\sqrt{2})$
$(x_{10}, x_{20}, y_{10}, y_{20}) = (1,0,0,0)$, $k = 0, a_2 = 0$, $\gamma = \alpha$,
$(x_{10}, x_{20}, y_{10}, y_{20}) = (-2,2,-3,1)$, no solutions for a_2,
$(x_{10}, x_{20}, y_{10}, y_{20}) = (0,0,-1,1)$, $k = 0, a_2 = 0$, $\gamma = \alpha^2(-1+\sqrt{2})$,
$(x_{10}, x_{20}, y_{10}, y_{20}) = (3,-2,-6,4)$, $k = 2, a_2 = -4$,
$\gamma = -4\sqrt{2} + \alpha - 2\alpha^2$.

Statement

If a unit α generates a power integral basis in the number field $K = \mathbb{Q}(\alpha)$, then $1/\alpha$ also generates a power integral basis in K.

$$D\left(\frac{1}{\alpha}\right) = \prod_{1 \le i < j \le n} \left(\frac{1}{\alpha^{(i)}} - \frac{1}{\alpha^{(j)}}\right)^2$$

$$= \prod_{1 \le i < j \le n} \frac{(\alpha^{(i)} - \alpha^{(j)})^2}{(\alpha^{(i)}\alpha^{(j)})^2} = \frac{D(\alpha)}{N(\alpha)^{2(n-1)}} = D(\alpha),$$

since $N(\alpha) = \pm 1$.

Statement

Assume the number field K is generated by a root α of an irreducible monogenic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x \pm 1 \in \mathbb{Z}[x],$$

of degree > 2 with constant term ± 1. Then, in addition to α, the inequivalent element

$$a_2\alpha + a_3\alpha^2 + \ldots + a_{n-1}\alpha^{n-2} + \alpha^{n-1}$$

also generates a power integral basis in K.

α is a unit, by $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_2\alpha^2 + a_1\alpha \pm 1 = 0$, we obtain

$$\pm\frac{1}{\alpha} = -a_1 - a_2\alpha - \ldots - a_{n-1}\alpha^{n-2} - \alpha^{n-1}$$

Recent results

Jordi Guardia and Francesc Pedret (2025):
Determining monogenity of pure cubic number fields using elliptic curves

A. Jakhar, K. Srinivas and P. Yadav (2025):
Monogenic polynomials having squarefull discriminant

Produce infinitely many new families of monogenic polynomials

$$f(x) = x^{n-km}(x^k + A)^m + B \in \mathbb{Z}[x]$$

having a powerful and k-full discriminant. **Provide asymptotics for number of such monogenic polynomials** for fixed A and with $B \leq X$.

A. Jakhar, S. Kotyada, S. Laishram, and P. Yadav (2025): Behaviour of Newton polygon over polynomial composition

Give sufficient conditions under which the successive vertices of the **Newton polygon of the composition** $g(f^n(x))$ with respect to a prime p can be explicitly described in terms of the Newton polygon of the polynomial $g(x)$.

L. Jones and J. Harrington (2024 Nov)
Monogenic trinomials of the form $x^4 + ax^3 + d$ and their Galois groups

Assuming that $f(x)$ is monogenic, we give necessary and sufficient conditions involving only a and d to determine the Galois group G of $f(x)$ over $\mathbb{Q}$

L. Jones (2024 Nov)
Monogenic cyclic trinomials of the form $x^4 + cx + d$

We show that there do not exist any monogenic cyclic trinomials of the form $f(x) = x^4 + cx + d$. This result, combined with previous work, proves that **the only monogenic cyclic quartic trinomials** are $x^4 - 4x^2 + 2, x^4 + 4x^2 + 2$ and $x^4 - 5x^2 + 5$.

L. Jones (2024 Dec)
Monogenic cyclic cubic trinomials

(after describing all monogenic cyclic quartic trinomials)
Two irreducible cyclic cubic trinomials are said to be equivalent if their splitting fields are equal. We show that there exist two infinite families of non-equivalent monogenic cyclic cubic trinomials of the form $x^3 + Ax + B$. We also show that **there exist exactly four monogenic cyclic cubic trinomials of the form** $x^3 + Ax^2 + B$, all of which are equivalent to $x^3 - 3x + 1$.

L. Jones (2024 Nov)
The monogenicity and Galois groups of certain reciprocal quintinomials

$$F(x) = x^{2^n} + Ax^{3\cdot 2^{n-2}} + Bx^{2^{n-1}} + Ax^{2^{n-2}} + 1$$
$$W_1 = B + 2 - 2A, W_2 = B + 2 + 2A, W3 = A^2 - 4B + 8,$$

If $W_1 W_2 W_3$ is squarefree and
$(A \mod 4, B \mod 4) \in \{(1,3),(3,1),(3,3)\}$,
then $F(x)$ is **monogenic** for all $n \geq 2$.

describing Galois groups of $F(x)$

L. Jones (2025)
Monogenic reciprocal quartic polynomials and their Galois groups

$f(x) = x^4 + Ax^3 + Bx^2 + Ax + 1 \in \mathbb{Z}[x]$
$W_1 = B + 2 - 2A$, $W_2 = B + 2 + 2A$, $W_3 = A^2 - 4B + 8$,
$W = W_1 W_2 W_3$
If $A \neq 0, \pm 1$, $B = 0$, then $f(x)$ is monogenic if and only if $2|A$ and $A - 1, A + 1$ and $(A/2)^2 + 2$ are all squarefree.

describe **monogenity and Galois groups** of $f(x)$

L. Jones (2025)
Monogenic even cyclic sextic polynomials

$f(x) = x^6 + ax^4 + bx^2 + c$

If $f(x)$ is irreducible over $\mathbb{Q}$ with $ab = 0$, then $\mathrm{Gal}(f) \neq C_6$. Consequently, there exist no monogenic even cyclic sextic binomials or trinomials.

describes **infinite families of monogenic $f(x)$ with cyclic Galois groups**

J. König (2025):
A note on monogenic even polynomials

extend works of L. Jones on even sextic monogenic polynomials

Theorem

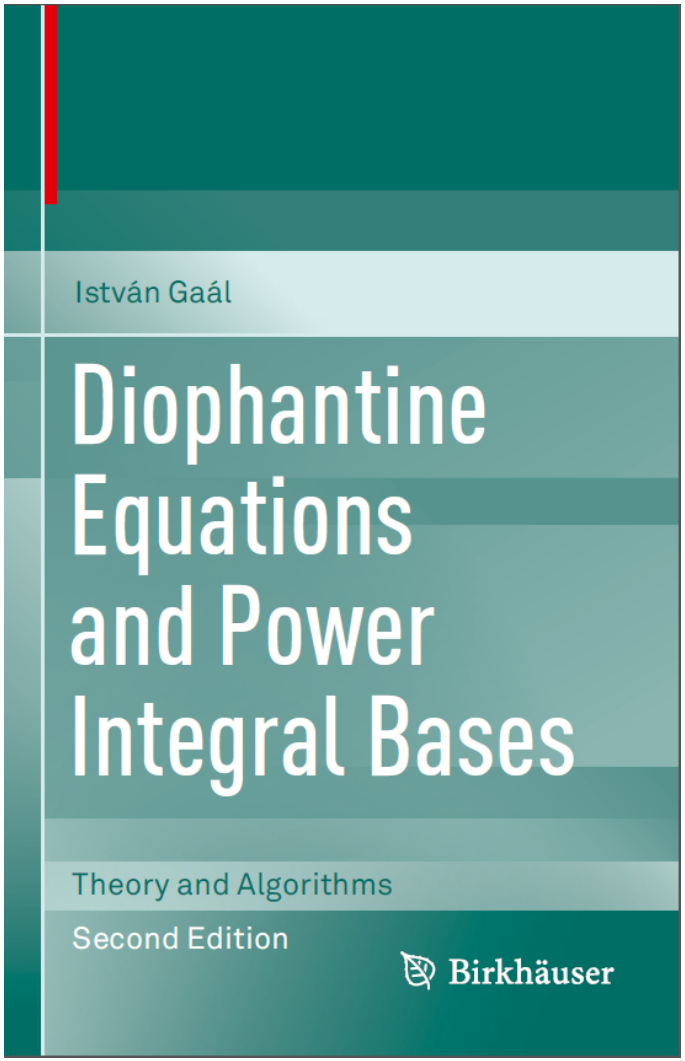
Let $f(X) = X^6 + aX^4 + bX^2 + c$ with $a, b, c \in \mathbb{Z}$ such that f is irreducible and $\mathrm{Gal}(f/\mathbb{Q}) \equiv C_6$. Then f is monogenic if and only if
$(a, b, c) \in$
$\{(-7, 14, -7), (-6, 9, -3), (5, 6, 1), (6, 5, 1), (6, 9, 1), (9, 6, 1)\}$.

J. König, H. Smith and Z. Wolske (2024 Dec)
Critical Point Criteria and Dynamically Monogenic Polynomials

Establish necessary and sufficient conditions in terms of the critical points of $f(x)$ for the **iterates of $f(x)$ to be monogenic** polynomials.

S.Kumar (2025)
Monogenity of composition of polynomials

Let $f(x)$ and $g(x)$ belonging to $\mathbb{Z}[x]$ be two monic polynomials and α be a root of $f \circ g(x)$. Then $f \circ g(x)$ is **monogenic** if and only if
(1) $f(x)$ is monogenic, and
(2) $\mathbb{Z}_L = \mathbb{Z}_K[\alpha]$, where $L = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}(g(\alpha))$.


István Gaál
Diophantine Equations and Power Integral Bases
Theory and Algorithms
Second Edition
Birkhäuser

Thank you for your attention!