Monogenity, multiple monogenity and power integral bases in number fields

K. Győry
(University of Debrecen)

Online Research Seminar "Diophantine Number Theory"

Debrecen, March 5, 2021

Slides have been posted on
https://math.unideb.hu/en/talks-kalman-gyory

Table of contents

1. Notations, introduction

- K *number field*, $[K:\mathbb{Q}]=d$, D_K *discriminant*, O_K *ring of integers* (maximal order), $D_{K/\mathbb{Q}}(\alpha)$ *discriminant of* $\alpha \in O_K$
- $O(\subseteq O_K)$ *order* in K, D_O its *discriminant*, $I_O(X_2,\ldots,X_d)$ *index form* associated with an integral basis $\{1,\omega_2,\ldots,\omega_d\}$ of O. For $\alpha \in O$ with $\mathbb{Q}(\alpha)=K \Longrightarrow$

$$I_O(\alpha) := [O:\mathbb{Z}[\alpha]] = |I_O(x_2,\ldots,x_d)| \tag{1}$$

the *index* of α in O, where $\alpha = x_1 + x_2\omega_2 + \ldots + x_d\omega_d$, $x_i \in \mathbb{Z}$ for $1 \le i \le d$.
- If $f_\alpha(X) \in \mathbb{Z}[X]$ *minimal* (monic) polynomial of $\alpha \in O \Longrightarrow$

$$D(f_\alpha) = D_{K/\mathbb{Q}}(\alpha) = I_O^2(\alpha) D_O. \tag{2}$$

- If *in particular* $O = O_K$, we write $D_K, I(\alpha), I(X_2,\ldots,X_d)$ instead of $D_O, I_O(\alpha), I_O(X_2,\ldots,X_d)$.

Definitions of equivalence and monogenity

Def: $\alpha, \alpha' \in O$ *equivalent* if $\alpha' = \pm\alpha + a$ with some $a \in \mathbb{Z}$. Then their discriminants and indices coincide.

Def: O resp. K *monogenic if*

O resp. $O_K = \mathbb{Z}[\alpha]$ for some α in O, resp. in O_K, and *n-times monogenic* if

$$O \text{ resp. } O_K = \mathbb{Z}[\alpha_1] = \ldots = \mathbb{Z}[\alpha_n]$$

for some pairwise inequivalent $\alpha_1, \ldots, \alpha_n$ in O, resp. in O_K.

Equivalent statements

Proposition. *For O, and in particular for $O = O_K$, the following statements are equivalent:*

(i) $O = \mathbb{Z}[\alpha]$ *for some* $\alpha \in O$;

(ii) $\{1, \alpha, \ldots, \alpha^{d-1}\}$ *is a power integral basis in* O;

(iii) $D(f_\alpha) = D_{K/\mathbb{Q}}(\alpha) = D_O$;

(iv) $I_O(\alpha) = 1$;

(v) $I_O(x_2, \ldots, x_d) = \pm 1$ *solvable in* $x_2, \ldots, x_d \in \mathbb{Z}$.

$\Longrightarrow$ *O resp. K n-times monogenic* $\Leftrightarrow$ *there are n inequivalent generators for power integral bases in O, resp. in K* $\Leftrightarrow$ *(v) has n solutions.*

2. General effective finiteness results

(motivation for further effective and algorithmic investigations)

First general **effective** finiteness results on *power integral bases* and *monogenity*: in the series of papers of Győry (1973,74,76,78a,78b).

Def: monic polynomials $f, f' \in \mathbb{Z}[X]$ *equivalent* if $f'(X) = f(X + a)$ for some $a \in \mathbb{Z} \Rightarrow D(f') = D(f)$.

$H(f)$ *height* of $f \in \mathbb{Z}[X]$, i.e. the maximum of the absolute values of the coefficients of f.

The main result of Part I:

Theorem A (Gy, 1973). *Let $D \geq 1$ and $f \in \mathbb{Z}[X]$ a monic polynomial with*

$$0 < |D(f)| \leq D. \tag{3}$$

Cont., remarks

There are effectively computable constants $c_1(D), c_2(D)$ *depending only on* D *such that*

$$\deg f \leq c_1(D),\ H(f') \leq c_2(D) \tag{4}$$

for some $f' \in \mathbb{Z}[X]$ *equivalent to* f.

Corollary (Gy, 1973). *Up to equivalence, there are only finitely many monic polynomials* $f \in \mathbb{Z}[X]$ *with a given non-zero discriminant, and all of them can be, at least in principle, effectively determined.*

Remark 1. Hermite (1854,1857) introduced a *much more complicated and weaker equivalence* for polynomials of given degree and given non-zero discriminants, and proved a finiteness theorem on such polynomials. For monic polynomials, our Corollary implies a much more precise and **effective** generalization of Hermite's *forgotten* theorem; see also Evertse, Gy and Remete (202?).

Remark 2. For *irreducible cubic* polynomials, the finiteness assertion of the Corollary in **ineffective** form: Delone (1930) and independently Nagell (1930). Nagell (1967, 1968) conjectured that this is true for all irreducible polynomials in $\mathbb{Z}[X]$ of given degree $d \geq 3$ and given discriminant. Our Corollary$\Longrightarrow$*proof of Nagell conjecture* in more general and **effective** form.

Remark 3. Theorem A was obtained *independently* of Birch and Merriman (1972). They proved an **ineffective** *finiteness theorem* on *binary forms* of **fixed** *degree* and *discriminant* from which, for monic polynomials of **fixed** *degree*, an **ineffective** version of our Corollary can be deduced. For **effective** version and **generalizations** of result of Birch and Merriman, see Evertse and Gy (1991, 1992).

Basic idea of the proof of Theorem A (see also Part II)

The **method** is important for algorithmic/computational applications too; see below.

Reduction to a *'connected'* system of *unit equations, effective bound* for the *unknown exponents* in the unit equations *by Baker's method.*

More precisely, let $f \in \mathbb{Z}[X]$ monic with (3). After having proved *degf* $\leq c_1(D)$, let $\alpha_1, \ldots, \alpha_d$ zeros, L the splitting field of f. Then (3)$\Longrightarrow \alpha_i - \alpha_j$ have bounded norms. Further,

$$(\alpha_i - \alpha_j) + (\alpha_j - \alpha_k) + (\alpha_k - \alpha_i) = 0 \text{ for every } i, j, k. \qquad (5)$$

Hence (5)$\Longrightarrow$*'connected'* system of *unit equations*

$$\delta_{ijk}\varepsilon_{ijk} + \tau_{ijk}\nu_{ijk} = 1, \tag{6}$$

δ_{ijk}, τ_{ijk} finitely many and effectively determinable values, $\varepsilon_{ijk}, \nu_{ijk}$ unknown units. *Represent* $\varepsilon_{ijk} = \zeta_{ijk}\rho_1^{a_{ijk_1}} \cdots \rho_r^{a_{ijk_r}}$ and similarly ν_{ijk}, ζ_{ijk} root of unity, $\rho_1, \ldots, \rho_r$ fundamental system of units in L with $r \leq d! - 1$. Applying *Baker's method* to (6)$\Longrightarrow$*effective bound* for the *exponents*$\Longrightarrow$*effective bound* for the *height* of $\alpha_i - \alpha_j$ for every $i, j$$\Longrightarrow$(4).

Further consequences of Theorem A in Parts I-V

Using (1), (2) and equivalence of (i)-(v),

Consequences: *up to equivalence, effective finiteness results:*

- *for algebraic integers α with a given non-zero discriminant* (Part I, quantitative version in Part II); apply $D(\alpha) = D(f_\alpha)$, f_α minimal polynomial of α;

in given number field K,

- *for α in O, resp. in O_K with a given index I* (Part III, quantitative version); apply $D_{K/\mathbb{Q}}(\alpha) = I^2 D_K$ for $\alpha \in O_K$;
- *for the solutions of index form equation*

$$I_O(x_2, \dots, x_d) = \pm I \text{ in } x_2, \dots, x_d \in \mathbb{Z}$$

  (Part III, quantitative version);
- *for $\alpha \in O$ resp O_K with $\mathbb{Z}[\alpha] = O$ resp. $O_K \Leftrightarrow \{1, \alpha, \dots, \alpha^{d-1}\}$ power integral basis* (Part III, quantitative form);
- *to decide effectively whether O resp. K is monogenic, resp. n-times monogenic* (Part III, quantitative).

Quantitative versions, generalizations

Quantitative versions: in Part II, Theorem A with

$$c_1(D) = 2(1 + \log D / \log 3), \ \textit{sharp}$$

$c_2(D)$ *explicit* but *large* (Baker's method).

In general, the **final** explicit *bounds* are *too large* for *practical use*. Then *refined versions* of the *general method* (Gy,1998,2000) must be combined with *reduction* and *enumeration* algorithms; see below.

Generalizations

- D resp. I replaced by $p_1^{z_1} \cdots p_s^{z_s}$, p_i prime, $z_i \geq 0$ also *unknown* (Gy Part V, Trelina)
- relative case, S-integers (Gy Part IV, Papp);
- more general decomposable form equations (Gy, Papp);
- étale algebras over finitely generated domains (Evertse, Gy);
- "inhomogeneous" case (Gaál);
- analogue results over function fields (Gaál, Gy, Shlapentokh).

⋮

Applications

- *Diophantine equations; Thue, Mordell, elliptic, superelliptic, discriminant form, of discriminant type* (Bérczes, Brindza, Evertse, Gy, Haristoy, Papp, Pink, Pintér, Trelina);
- *Irreducible polynomials* (Gy);
- *Canonical number systems* (Evertse, Gy, Kovács, Pethő, Thuswaldner)
- *Arithmetic properties of discriminants and indices of elements of* O_K (Gy).

$\vdots$

Uniform upper bounds for the number of solutions (Bérczes, Evertse, Gy).

Books

For further **consequences**, **generalizations**, **applications** and **quantitative versions**, see the **books** with a *great number* of *references*:

- *K. Győry*, Résultats effectifs sur la représentation des entiers par des formes décomposables, Kingston, Canada, 1980.
- *W. Narkiewicz*, Elementary and Analytic Theory of Algebraic Numbers, 2nd ed., Springer 1990.
- *J.-H. Evertse* and *K. Győry*, Unit Equations in Diophantine Number Theory, Cambridge University Press, 2015.
- *J.-H. Evertse* and *K. Győry*, Discriminant Equations in Diophantine Number Theory, Cambridge University Press, 2017.
- *I. Gaál*, Diophantine Equations and Power Integral Bases, 2nd ed., Birkhäuser, 2019.

3. Algorithmic resolution of index form equations, application to (multiply) monogenic orders/number fields

K number field of *degree $d \geq 3$*, $O \subseteq O_K$ *order*, $I(X_2, \ldots, X_d)$ *index form* associated with a given integral basis of K resp. O.

$$I(x_2, \ldots, x_d) = \pm 1 \text{ in } x_2, \ldots, x_d \in \mathbb{Z}. \tag{7}$$

There are *efficient methods* for *solving* (7) in *concrete* cases$\Leftrightarrow$for *computing* all *generators* of *power integral bases* in K resp. in O, *up to degree $d \leq 6$* in *general*, and for certain classes of *higher degree fields up to about degree* 15.$\Longrightarrow$ for *deciding how many times* K resp. O is *monogenic*.

For **d=3,4**, (7)$\Longrightarrow$*Thue equations* of *degree* ≤ 4, efficient algorithm;

d=3, (7)$\Longrightarrow$*cubic Thue equation*, Gaál, Schulte (1989);

d=4, (7)$\Longrightarrow$*one cubic and some quartic Thue equations*, Gaál, Pethő, Pohst (1991–1996);

General approach combined with reduction and enumeration algorithms

In general, for $\boldsymbol{d} \geq \mathbf{5}$ the *general approach* involving *unit equations* is needed. Since

$$(7) \Leftrightarrow D_{K/\mathbb{Q}}(\alpha) = D_K \Leftrightarrow D(f_\alpha) = D_K \text{ in } \alpha \in O_K$$

with minimal polynomial $f_\alpha \in \mathbb{Z}[X]$, in case of *concrete* equations (7), the *basic idea* of the *proof* of *Theorem A* can be *combined* with *further fundamental algorithms* and *refinements:*

Refined version of the general method: *reduction* to *unit equations* but in considerably <u>smaller subfields</u> in the normal closure L of K. Then the number of unknown exponents a_{ijk} <u>much smaller</u>, $\leq d(d-1)/2-1$; cf. Gy (1998), Gy (2000), pp. 197, 206–207, Gaál, Gy (1999), Evertse, Gy (2017), pp. 90, 119–120. Then *bound* the exponents by *Baker's method*.

Reduction algorithm: *reducing* the *Baker's bound* by *refined versions* of the L^3-*algorithm*; cf. de Weger; Wildanger; Gaál and Pohst.

Enumeration algorithm: determining the **small** solutions *under the reduced bound*; cf. Wildanger; Gaál and Pohst; Bilu, Gaál and Gy.

$\Longrightarrow$ *determining* all *power integral bases* $\Longrightarrow$ *checking* the *monogenity* and the *multiplicity of the monogenity* of K.

Examples

Examples: in the most difficult case when $K = \mathbb{Q}(\alpha)$, degree d, *totally real*, with Galois group (of the normal closure) of K S_d, $f \in \mathbb{Z}[X]$ *minimal polynomial* of α.

d=3, $f(X) = X^3 - X^2 - 2X + 1$, K 9 *times* monogenic, Gaál, Schulte (1989);

d=4, $f(X) = X^4 - 4X^2 - X + 1$, K 17 *times* monogenic, Gaál,Pethő, Pohst (1990's);

d=5, $f(X) = X^5 - 5X^3 + X^2 + 3X - 1$, K 39 *times* monogenic, Gaál, Gy (1999);

d=6, $f(X) = X^6 - 5X^5 + 2X^4 + 18X^3 - 11X^2 - 19X + 1$, K 45 *times* monogenic, Bilu, Gaál, Gy (2004);

Books, research papers

Results, methods, references

Books

- *B. M. M. de Weger*, Algorithms for Diophantine Equations, CW, Trad 65, Amsterdam, 1989.
- *N. P. Smart*, the Algorithmic Resolution of Diophantine Equations, Cambridge University Press, 1998.
- *J.-H. Evertse and K. Győry*, Discriminant Equations in Diophantine Number Theory, Cambridge University Press, 2017.
- *I. Gaál*, Diophantine Equations and Power Integral Bases, 2nd ed., Birkhäuser, 2019.

Research papers, a great number of authors, including: Ahmed, Arnóczki, Bilu, El Fadil, Gaál, Gassert, Guardia, Győry, Hamed, Husnine, Jadrijevič, Járási, Kashio, Kim, Lavallee, Montes, Motoda, Nakahara, Nart, Nyul, Olajos, Pethő, Pohst, Remete, Robertson, Schertz, Schulte, Shah, Smart, Smith, Spearman, Stange, Szabó, Tanoé, de Weger, Wildanger, Williams, Ziegler,...

4. Monogenic and multiply monogenic number fields

selected results and problems

K number field of degree d with ring of integers O_K

Distribution of monogenic number fields

for $\mathbf{d=1,2}$, K monogenic;

for $\mathbf{d=3}$, first example for *non-monogenic* number field: Dedekind (1878);

for *fixed* $\mathbf{d\geq 3}$, inifnitely many *monogenic* and infinitely many *non-monogenic* number fields of degree d;

for $\mathbf{d=3,4,6}$, tables of Gaál (2019): *frequency of monogenic number fields of degree d is decreasing in tendency as $|D_K|$ increases.*

Theorem B (Bhargava, Shankar and Wang, 2016, 202?). *For given $d \geq 3$, the number of isomorphism classes of monogenic number fields K of degree d with $|D_K| \leq X$ and with associated Galois group S_d is $\gg X^{1/2+1/(d-1)}$.*

A weaker equivalence

Def: $\alpha, \beta \in O_K$ *equivalent* if $\beta = \pm\alpha + a$ for some $a \in \mathbb{Z} \Rightarrow \mathbb{Z}[\beta] = \mathbb{Z}[\alpha]$

Theorem A $\Longrightarrow$ Up to equivalence, there are only finitely many $\alpha \in O_K$ with $O_K = \mathbb{Z}[\alpha]$, and they can be effectively determined$\Longrightarrow$*effectively decidable whether K is monogenic, and the multiplicity of the monogenity can also be effectively determined.*

Def: $\alpha, \beta \in O_K$ weakly equivalent *if $\beta = \pm\alpha' + a$ for some $a \in \mathbb{Z}$ and some conjugate α' of α (over $\mathbb{Q}$)*

equivalence $\Longrightarrow$ weak equivalence

Def: *K n times monogenic in weak sense if*

$$O_K = \mathbb{Z}[\alpha_1] = \ldots = \mathbb{Z}[\alpha_n]$$

for some pairwise weakly inequivalent $\alpha_1, \ldots, \alpha_n$ in O_K.

Theorem A $\Longrightarrow$ *effectively decidable whether K is n times monogenic in weak sense*

If the *Galois group of* (the normal closure of) K *is S_d* $\Longrightarrow$ *the two equivalences coincide*

$\Longrightarrow$ in the above **examples** of degree $\boldsymbol{d = 3, 4, 5, 6}$ resp., the corresponding fields K are $9, 17, 39, 45$ *times monogenic in weak sense*

Cyclotomic fields

Cyclotomic fields and *their maximal real subfields* are **monogenic**.

$p \geq 3$ *prime*, ξ primitive pth root of unity, $K = \mathbb{Q}(\xi)$ pth *cyclotomic field*

$$\xi, \dots, \xi^{p-1}, 1/(1+\xi), \dots, 1/(1+\xi^{p-1})$$

generate power integral bases in O_K; K $2(p-1)$ times monogenic, but only $\xi, 1/(1+\xi)$ generate distinct power integral bases. These are *inequivalent* in weak sense.

Bremner's **conjecture** (1988): *no further power integral basis in K in weak sense*

> *proved* for $p \leq 41$: Robertson, Wildanger, Russel

If the *conjecture* is *true* $\Longrightarrow$ K *precisely* 2 *times monogenic in weak sense.*

Bounds for the multiplicity of monogenity

In the above *examples* for $\boldsymbol{d = 3, 4, 5, 6}$, K is *at least* d^2 *times monogenic* in weak sense. On the contrary, the first upper bound in terms of d: Evertse and Gy (1985). The *best known upper bound:*

Theorem C (Evertse, 2011). *Let K be an algebraic number field of degree $d \geq 4$. Then any order in K (including O_K)* is at most

$$2^{4(d+5)(d-2)} \tag{8}$$

times monogenic.

In particular, this provides an *upper bound* for *the multiplicity of the monogenity of K.* Clearly, the bound (8) is valid in case of *weak equivalence* as well.

For *given* $d \geq 3$, denote by $M(d)$ the maximal number for which there exists $M(d)$ times monogenic number field K of degree d.

Problem 1 (Gy, 2000). *Is $M(d)$ polynomial or exponential in terms of d?*

Arithmetic characterization of monogenic and multiply monogenic number fields

Hasse's problem (1960's): *give an arithmetic characterization of monogenic number fields*

A very great number of *important results* for *deciding the monogenity* of certain classes of number fields, including

- cyclotomic fields, abelian number fields;
- various types of quartic and sextic fields;
- multiquadratic fields;
- pure fields;
- composite fields;

$\vdots$

Various approaches

- infinite parametric families of fields, use of the index form approach;
- ideal theoretic approach, Dedekind's criterion;
- Montes algorithm, Newton polygons;
- Gröbner bases approach;
- irreducible monic polynomials with square-free discriminant;
- non-squarefree discriminant approach;

$\vdots$

Books, research papers

Books: Hensel (1908), Hasse (1963), Narkiewicz (1990), Evertse and Győry (2017), Gaál (2019) with many references.

Research papers, a great number of *authors*, including:

Ahmad, Archinard, Arnóczki, Bell, Bérczes, Bilu, Bozlee, Brenner, Brunotte, Cougnard, Delone, Dummit, Evertse, El Fadil, Faddeev, Gaál, Gassert, Gras, Guardia, Győry, Hameed, Hasse, Huard, Husnine, Jadrijevic, Jakhar, Járási, Jones, Katayama, Khan, Khanduja, Kim, Kisilevsky, Kovács, Lavallee, Liang, Merriman, Montes, Motoda, Nakahara, Nart, Nguyen, Nyul, Park, Pethő, Pohst, Ranieri, Remete, Robertson, Russel, Sangwan, Sekigawa, Shah, Simon, Smart, Smith, Spearman, Stange, Sultan, Tanoé, Thérond, Uehara, Wildanger, Williams, Ziegler,...

Problem 2: *give an arithmetic characterization of* **multiply monogenic** *number fields*

New arithmetic properties of monogenic number fields and orders

Recently, it has been proved in a *precise* and *quantitative form* that the monogenity has an increasing effect on the class group of number fields and orders; see Bhargava and Varma (2016), Ho, Shankar and Varma (2018), Bhargava, Hanke and Shankar (2020), Siad, Parts I, II (2020), Swaminathan (2020).

The above **examples** of degree **d=3,4,5,6** show that the multiplicity of monogenity can be relatively large if the Galois group is S_d, i.e. large.

Problem 3: Has the *size* or *structure* of the *Galois group* any futher **effect on the class group of multiply monogenic number fields and orders?**

5. Multiply monogenic orders in number fields

Fix *number field* K with degree $d \geq 3$, and consider **varying orders** O in K. **Theorem C** $\Longrightarrow$ *every order* in $K \leq 2^{4(d+5)(d-2)}$ *times monogenic.* It can be shown that 'most' orders in K are only few times monogenic. More precisely,

Theorem D (Bérczes, Evertse, Gy, 2013). *There are at most finitely many three times monogenic orders in* K.

The bound **three** is *best possible* in the sense that there are number fields having infinitely many two times monogenic orders, see below.

Def. *The order* O *in* K *is called of* **type I** *if there are* $\alpha, \beta \in O$ *and* $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \boldsymbol{GL}(2, \mathbb{Z})$ *such that*

$$O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta], \ \beta = \frac{a_1\alpha + a_2}{a_3\alpha + a_4}, \ a_3 \neq 0 \tag{9}$$

Then α, β **not** *equivalent*, i.e. O *two times monogenic.*

Two times monogenic orders of types I and II

One can prove that *every two times* monogenic order in a *cubic field* is of **type I**. Further, if K is not a CM-field (i.e., not a totally complex quadratic extension of a totally real field), then K has *infinitely many two times* monogenic orders of **type I**.

Def. *The order O in K is called of* **type II** *if there are $\alpha, \beta \in O$ and $a_0, a_1, a_2, b_0, b_1, b_2 \in \mathbb{Z}$ with $a_2 b_2 \neq 0$ such that*

$$O = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta], \ \beta = a_0 + a_1\alpha + a_2\alpha^2, \ \alpha = b_0 + b_1\beta + b_2\beta^2. \quad (10)$$

Then α, β **not** *equivalent*, so O *two times monogenic.*

Type II *orders* exist only in *quartic number fields*. Further, there exist *quartic number fields* with *infinitely many orders of* **type II**.

Theorem E (Bérczes, Evertse, Gy, 2013). *Let K be a number field of degree $d \geq 4$, whose normal closure has Galois group S_d. Then*

(i) *If $d = 4$, then apart from finitely many exceptions every multiply monogenic order in K is two times monogenic of* **type I** or **II**.

(ii) *If $d \geq 5$, then apart from finitely many exceptions every multiply monogenic order in K is two times monogenic of* **type I**.

Problem 4. *Is Theorem E valid without the assumption on the Galois group?*

Method of proof *of Theorems D and E: reduction to unit equations* in *more than two unknowns*, and *use* of *ineffective finiteness theorems* on these equations. **Problem 5.** *Make effective Theorems D and E*

This seems to be very hard. At present, it is not known how to make the results on unit equations in more than two unknowns effective.

Theorem F. (Evertse, Gy, Remete, 202?). *For every $d \geq 5$ there exists number field K of degree d having a two times monogenic order which is not of* **type I**.

Explicit examples

Explicit examples for **Theorem F** (Evertse, Gy, Remete, 202?): Let $d \geq 5$ and

$$g^{(d)}(X) := \begin{cases} X^d + X^{d-1} - 1 \text{ if } d \text{ odd,} \\ X^d + X^{d-1} + X^{d-2} + 1 \text{ if } d \text{ even.} \end{cases}$$

By results of Selmer (1965) resp. Ljunggren (1960), $g^{(d)}(X)$ is irreducible over $\mathbb{Q}$. Let

$$f^{(d)}(X) := \begin{cases} X^{\frac{d+1}{2}} - X^{\frac{d-1}{2}} + 1 \text{ if } d \text{ odd,} \\ X^{\frac{d+2}{2}} + X^{\frac{d}{2}} + X^{\frac{d-2}{2}} + X + 1 \; if\ d\ even. \end{cases}$$

It is easy to check that

$$f^{(d)}(X^2) - X = \begin{cases} g^{(d)}(X)(X-1) \text{ if } d \text{ odd,} \\ g^{(d)}(X)(X^2 - X + 1) \text{ if } d \text{ even.} \end{cases} \tag{11}$$

Then, if α is a zero of $g^{(d)}(X)$, (11) implies that $\alpha = f^{(d)}(\alpha^2)$, whence $\alpha \in \mathbb{Z}[\alpha^2]$ and $\mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\alpha^2]$. But $\mathbb{Z}[\alpha^2] \subseteq \mathbb{Z}[\alpha]$, so $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha^2]$.

Since $d \geq 5$, there are no $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ with $a_3 \neq 0$ and

$$\alpha^2 = \frac{a_1\alpha + a_2}{a_3\alpha + a_4}.$$

Consequently, $O := \mathbb{Z}[\alpha] = \mathbb{Z}[\alpha^2]$ is a two times monogenic order in the number field $K := \mathbb{Q}(\alpha)$ of degree d which is not of **type I**.

Remark. It seems to be an extremely hard **problem** *to describe completely the multiply monogenic orders in a number field.*

Application to canonical number systems

K number field of degree ≥ 3, O and *order* in K.

Def. $\alpha \in O$, $\alpha \neq 0$ *is called a* **basis** *of* a **canonical number system** (*or* CNS **basis**) *for O if every nonzero element of O can be represented in the form*

$$a_0 + a_1\alpha + \ldots + a_m\alpha^m$$

with $m \geq 0$, $a_i \in \{0, 1, \ldots, |N_{K/\mathbb{Q}}(\alpha)| - 1\}$ *for* $i = 0, \ldots, m$ *and* $a_m \neq 0$.

CNS is a *natural generalization* of *radix representations* of rational integers to algebraic integers.

Def. *When there exists a CNS in O, then O is called a CNS* **order**.

Such orders have been intensively investigated, see e.g. the survey paper Brunotte, Huszti, Pethő (2006).

Kovács (1981) proved that *O is a CNS order $\Leftrightarrow$ O is monogenic*. If α is a *CNS basis* in $O \Longrightarrow O = \mathbb{Z}[\alpha]$. *Conversely, if $O = \mathbb{Z}[\alpha]$ then there are infinitely many α' equivalent to α such that α' is a CNS basis for O.* For a *characterization* of CNS bases in O, see Kovács and Pethő (1991).

Consequence of *the* **Corollary** *to* **Theorem A** (Gy, 1973) $\Longrightarrow$ *up to equivalence, there are only finitely many canonical number systems in O, and all them can be effectively determined*.

Def. O is said to be *n times CNS order if there are at least n pairwise inequivalent CNS bases in O.*

Theorem D (Bérczes, Evertse, Gy, 2013) $\Longrightarrow$

Corollary. *There are at most finitely many three times CNS orders in K*

6. Some new effective generalizations

(motivation for further investigations)

K number field, $D \neq 0$ integer

Corollary of **Theorem A** from Gy (1973) $\Longrightarrow$ *Up to equivalence, the equation*

$$D_{K/\mathbb{Q}}(\alpha) = D \textit{ in } \alpha \in O_K \tag{12}$$

has only finitely many solutions + effective

In the **books** Evertse, Gy (2017) and Gaál (2019) many results mentioned in Sections 2 and 3 above are *generalized* for the *relative case*, *over the rings of (S−) integers of number fields*. Further generalizations are given for the finitely generated case in the **books** Evertse, Gy (2017) and

Evertse and Győry, *Effective results and methods for Diophantine equations over finitely generated domains*, Cambridge University press, to appear.

A new effective generalization

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be a *finitely generated domain* with *algebraic* or *transcendental* generators $z_1, \ldots, z_r$, M *quotient field* of A, Ω a *finite étale M-algebra* (i.e. a direct product of finite extensions $K_1, \ldots, K_t$ of M). Let O be an *A-order* of Ω (i.e. an A-subalgebra of the integral closure of A in Ω, which spans Ω as an M-vector space).

Def. $\alpha, \alpha' \in O$ *A-equivalent if* $\alpha' - \alpha \in A \Longrightarrow D_{\Omega/M}(\alpha') = D_{\Omega/M}(\alpha)$

B^+ *additive group* of a ring B, D a *non-zero element* of A

As a *generalization* of (12), consider the *discriminant equation*

$$D_{\Omega/M}(\alpha) = D \text{ in } \alpha \in O. \tag{13}$$

Theorem G (Evertse and Gy, 202?). *If*

$$(O \cap M)^+/A^+ \text{ finite}, \tag{14}$$

then the set of $\alpha \in O$ with (13) *is a union of finitely many A-equivalence classes. Moreover, if A, Ω, O and D are given effectively in a well-defined way, one can determine a set consisting of precisely one element from each of these classes.*

For $A = \mathbb{Z}$, $M = \mathbb{Q}$, $\Omega =$number field K, $O = O_K$, Theorem G $\Longrightarrow$ the above theorem concerning equation (12).

The *condition* (14) *necessary* and *decidable*.

Thank you for your attention!