Effective reduction theory of integral polynomials of given discriminant, and related topics

(survey with a brief historical overview)

K. Győry (Debrecen)

(partly joint work with J.-H. Evertse)

July, 2025

Leiden

We give a survey *on the* effective reduction theory of integral polynomials of given discriminant *and its* applications

$\mathbb{Z}$-equivalence and $GL_2(\mathbb{Z})$-equivalence of integral polynomials

$GL_2(\mathbb{Z})$: multiplicative group of 2×2 integral matrices with determinant ± 1

- *Two monic polynomials* $f, f^* \in \mathbb{Z}[X]$ *are called* $\mathbb{Z}$-**equivalent** *if* $f^*(X) = f(X + a)$ *for some* $a \in \mathbb{Z}$;
- *Two polynomials* $f, f^* \in \mathbb{Z}[X]$ *of degree* $n \geq 2$ *are called* $GL_2(\mathbb{Z})$ **-equivalent** *if there is* $\left(\begin{smallmatrix} b & a \\ d & c \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ *such that*

$$f^*(X) = \pm(dX + c)^n f\left(\frac{bX + a}{dX + c}\right)$$

$\Longrightarrow$ in both cases, f, f^* *have the* same discriminant

$\mathbb{Z}$*-equivalence* is much *stronger*, $\mathbb{Z}$-equivalent monic polynomials in $\mathbb{Z}[X]$ are clearly $GL_2(\mathbb{Z})$-equivalent with $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$

similar interpretation in terms of **binary forms**

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

The **effective reduction theory** we consider asks to find, for a given polynomial $f \in \mathbb{Z}[X]$, a $\mathbb{Z}$-*equivalent* or $GL_2(\mathbb{Z})$-*equivalent* integral polynomial whose *height* is *effectively bounded above* in terms of the degree and discriminant of f.

Classical results in case of degree ≤ 3

- Lagrange (1773), *quadratic* case, **effective**
- Hermite (1851), *cubic* case, **effective**
- Delone (1930), Nagell (1930), independently, *monic, cubic* case, **ineffective**

General results, for arbitrary degree

- Birch and Merriman (1972), **ineffective**
- Győry (1973), independently, *monic case*, **effective**
- Evertse and Győry (1991), **effective** version of B–M (1972)

$\longrightarrow$ a *great number* of **various consequences, applications** and **generalizations**

Later

- **significant progress** with several new applications and generalizations
- *very extensive literature* with numerous papers and some books by Evertse, Győry and others
- **the first monograph** on the subject:
  J.-H. Evertse and K. Győry, *Discriminant equations in Diophantine number theory*, Cambridge, 2017.

Since 2017

- many **new** results, **survey** of *older* and *recent* results and applications:
  J.-H. Evertse and K. Győry, *General effective reduction theory of integral polynomials of given non-zero discriminant and its applications*, arXiv: 2409.02627 math.NT 4 Sep 2024.
- a **considerably extended** version of the arXiv paper will be published soon.

I. Reduction of integral polynomials of degree ≤ 3 with given discriminant mod $GL_2(\mathbb{Z})$-equivalence, resp. $\mathbb{Z}$-equivalence

Reduction theory was initiated by Lagrange in terms of integral binary forms. He proved the following theorem in terms of binary forms. We present here an equivalent formulation for integral polynomials.

Lagrange (1773): *For* **quadratic** $f \in \mathbb{Z}[X]$ *with discriminant* $D \neq 0$, *there exists* $f^* \in \mathbb{Z}[X]$ $GL_2(\mathbb{Z})$*-equivalent to* f *such that* $H(f^*) \leq c(D)$ *with some effectively computable constant* $c(D)$.

Equivalently

There are only finitely many $GL_2(\mathbb{Z})$*-equivalence classes of* **quadratic** *polynomials in* $\mathbb{Z}[X]$ *with given non-zero discriminant* + **effective**

Similar assertions for monic quadratic polynomials in $\mathbb{Z}[X]$ with $\mathbb{Z}$*-equivalence*

Gauss (1801): *more precise result*

Hermite (1851): *There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of* **cubic** *polynomials in $\mathbb{Z}[X]$ with given non-zero discriminant*

Delone (1930), Nagell (1930), independently: *Up to $\mathbb{Z}$-equivalence, there are only finitely many irreducible* **cubic** *monic polynomials in $\mathbb{Z}[X]$ with given non-zero discriminant* + **ineffective**

Problem: *extend these results to the case of degree ≥ 3 resp. ≥ 4.*

II. Hermite's attempt (1857) for extending the previous reduction results to the general case

Hermite attempted to extend his theorem (1851) on cubic polynomials to the case of arbitrary degree $n \geq 4$, but *without success*. Instead, he proved a theorem with a *weaker equivalence*, see **Theorem A** below.

Hermite equivalence of polynomials and Hermite's finiteness theorem

Let $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n) \in \mathbb{Z}[X]$ with $c \in \mathbb{Z}\setminus\{0\}$, $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$. Then the discriminant of f : $D(f) = c^{2n-2}\prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$.

To f we associate the *decomposable form*

$$[f](\underline{X}) := c^{n-1}\prod_{i=1}^{n}(X_1 + \alpha_i X_2 + \cdots + \alpha_i^{n-1}X_n) \in \mathbb{Z}[X_1, \ldots, X_n].$$

We have $D(f) = D([f])$ (Vandermonde).

Hermite (1857): *Two polynomials* $f, f^* \in \mathbb{Z}[X]$ *of degree* n *are called by us* **Hermite equivalent** *if the associated decomposable forms* $[f]$ *and* $[f^*]$ *are* $GL_n(\mathbb{Z})$*-equivalent, i.e.,*

$$[f^*](\underline{X}) = \pm[f](U\underline{X}) \text{ for some } U \in GL_n(\mathbb{Z}).$$

$\Longrightarrow$ *Hermite equivalent polynomials in* $\mathbb{Z}[X]$ *have the same* discriminant.

Hermite proved the following *finiteness theorem on polynomials:*

Theorem A (Hermite, 1857)

Let $n \geq 2, D \neq 0$. *Then the polynomials* $f \in \mathbb{Z}[X]$ *of degree* n *and of discriminant* D *lie in finitely many Hermite equivalence classes.*

$+$ **ineffective**

Comparison of Hermite equivalence with $GL_2(\mathbb{Z})$-equivalence and $\mathbb{Z}$-equivalence

In Bhargava, Evertse, Győry, Remete, Swaminathan (BEGyRS, 2023), we have *integrated* Hermite's long-forgotten notion of equivalence and his **Theorem A**, corrected a faulty reference to Hermite's result in Narkiewicz excellent book "The story of algebraic numbers in the first half of the 20th century", Springer, 2018, and compared *Hermite equivalence* with $GL_2(\mathbb{Z})$-*equivalence* resp. $\mathbb{Z}$-*equivalence* of integral polynomials.

For integral polynomials of degree $n = 2$ *and* 3, *Hermite equivalence and* $GL_2(\mathbb{Z})$-*equivalence, resp.* $\mathbb{Z}$-*equivalence* **coincide**.

We proved in (BEGyRS, 2023) that *if* $f, f^* \in \mathbb{Z}[X]$ *are* $GL_2(\mathbb{Z})$-*equivalent, resp.* $\mathbb{Z}$-*equivalent, then they are Hermite equivalent.*

Further, for every $n \geq 4$, there are infinitely many pairs (f, f^*) of irreducible primitive polynomials in $\mathbb{Z}[X]$ with degree n such that f, f^* are Hermite equivalent but $GL_2(\mathbb{Z})$-inequivalent, resp. $\mathbb{Z}$-inequivalent in the monic case.

$\Longrightarrow$ *$GL_2(\mathbb{Z})$-equivalence*, resp. *$\mathbb{Z}$-equivalence* are **stronger** than *Hermite equivalence* $\Longrightarrow$ Hermite's **Theorem A** is **weaker** than **Theorems** of Győry (1973) and Evertse and Győry (1991) below.

For convenience of presentation, we formulated in (BEGyRS, 2023) the former and new results **uniformly**, *in terms of integral polynomials*, instead of monic polynomials and binary forms.

These and some new results in the effective reduction theory inspired us with Evertse to write a long joint survey paper and give this talk on the subject, including several older and recent results, applications and generaliztaions.

III. Reduction theory of integral polynomials with given discriminant: the general effective case

Significant breakthroughs in the 1970's and 1990's

Hermite's *original objective – proving that there are only finitely many* $GL_2(\mathbb{Z})$*-equivalence, resp.* $\mathbb{Z}$*-equivalence classes of integral polynomials of given degree and given non-zero discriminant – was finally achieved more than a* century *later by* Birch *and* Merriman (1972) *and independently,for monic polynomials, in a* more precise *and* **effective** *form by* Gy (1973). *The result of* Birch *and* Merriman *was subsequently made* **effective** *by* Evertse *and* Gy (1991).

In other words, Gy (1973) *and* Evertse *and* Gy (1991) *together* solved the main problem *of the effective reduction theory in* **full generality** *and in an* **effective** *way, which resulted in many* **significant consequences** *and* **applications**.

Birch and Merriman proved the following.

Theorem B (Birch and Merriman, 1972)

Let $n \geq 2, D \neq 0$. There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of polynomials in $\mathbb{Z}[X]$ with degree n and discriminant D.

Proof, partly based on the finiteness of the number of solutions of unit equations + some *ineffective* arguments $\Longrightarrow$ **ineffective**

For monic polynomials, the corresponding result with $\mathbb{Z}$-equivalence was proved *independently* by Győry (1973) in an **effective** form.

Theorem C (Győry, 1973)

Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 3$ with discriminant $D \neq 0$. There is an $f^* \in \mathbb{Z}[X]$, $\mathbb{Z}$-equivalent to f, such that $H(f^*) \leq c_1(n, D)$ and $n \leq c_2(D)$, where c_1, c_2 are **effectively** *computable positive numbers depending only on n, D, resp. on D.*

Apart from the **ineffectivity** of Theorem B, Theorems B and C are **generalizations** for $n \geq 3$ of the theorems of Lagrange (1773), case $n = 2$, and Hermite (1851), case $n = 3$.

The **proof** is based on a combination of an effective result of Győry (1973), proved by Baker's method, on unit equations and a so-called graph method of Győry.

Corollary (Gy, 1973)

Let $D \neq 0$. There are only finitely many $\mathbb{Z}$-equivalence classes of monic polynomials in $\mathbb{Z}[X]$ with discriminant D, and a full set of representatives of these classes can be **effectively** *determined.*

Note that here the degree of the monic polynomials under consideration is not fixed.

Theorem C confirmed a conjecture of Nagell (1967,68) in an effective form. Further, it made effective and significantly *generalized* the theorems of Delone (1930) and Nagell (1930) obtained in the cubic case.

Effective/explicit version of Theorem B and explicit version of Theorem C

First **effective** version of Theorem B (Birch and Merriman): Evertse and Gy (1991) in a quantitative form. In 2017, improved and completely **explicit** version:

Theorem D (Evertse and Gy (2017))

Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ and discriminant $D \neq 0$. Then f is $GL_2(\mathbb{Z})$-equivalent to a polynomial $f^* \in \mathbb{Z}[X]$ for which

$$H(f^*) \leq \exp\{(4^2 n^3)^{25n^2} \cdot |D|^{5n-3}\}. \tag{3.1}$$

Further (Gy, 1974):

$$n \leq 3 + 2\log|D|/\log 3.$$

First explicit version of Theorem C: Gy (1974). In the **proof**, this was the first explicit application of Baker's method to unit equations.

Improved version:

Theorem E (Evertse and Gy, 2017)

Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 2$ and discriminant $D \neq 0$. Then f is $\mathbb{Z}$-equivalent to a polynomial $f^* \in \mathbb{Z}[X]$ for which

$$H(f^*) \leq \exp\{n^{20} 8^{n^2+19} (|D|(\log|D|)^n)^{n-1}\}. \tag{3.2}$$

Further (Gy, 1974):

$$n \leq 2 + 2\log|D|/\log 3.$$

Clearly, Theorems B, D, and in the monic case Theorems C, E are *much more precise* and *deeper* than Theorem A of Hermite.

The *exponential feature* of the *bounds* in (3.1) and (3.2) is a consequence of the use of *Baker's method*. It is likely that the bounds in (3.1) and (3.2) can be replaced by some polynomial expressions in terms of $|D|$; cf. Conjecture 15.1 and Theorem 15.1.1 in Evertse and Győry (2017).

IV. Consequences of Theorem C of Győry (1973) in algebraic number theory, and in particular for monogenic number fields and monogenic orders

Important breakthrough; *general effective finiteness theorems* for **monogenity** and **power integral bases** of number fields.

K number field, $n = [K : \mathbb{Q}]$, *discriminant* D_K, *ring of integers* $\mathcal{O}_K$; for $\alpha \in \mathcal{O}_K$, $f_\alpha(X) \in \mathbb{Z}[X]$ *minimal* (monic) *polynomial of* $\alpha \Longrightarrow$

$$\begin{cases} D_{K/\mathbb{Q}}(\alpha) & := D(f_\alpha) \text{ discriminant of } \alpha, \\ I(\alpha) & := [\mathcal{O}_K : \mathbb{Z}[\alpha]] \text{ index of } \alpha; \text{ we have} \end{cases} \tag{4.1}$$

$$D_{K/\mathbb{Q}}(\alpha) = I^2(\alpha) \cdot D_K \tag{4.2}$$

Definition

- $\alpha, \alpha^* \in \mathcal{O}_K$ **equivalent** *if* $\alpha^* = \pm\alpha + a$, $a \in \mathbb{Z} \Rightarrow D_{K/\mathbb{Q}}(\alpha) = D_{K/\mathbb{Q}}(\alpha^*)$, $I(\alpha) = I(\alpha^*)$
- *K* **monogenic** *if* $\mathcal{O}_K = \mathbb{Z}[\alpha]$ *for some* $\alpha \in \mathcal{O}_K \Leftrightarrow \{1, \alpha, \ldots, \alpha^{n-1}\}$ **power integral basis** *in K, and* $k \geq 1$ **times monogenic** *if* $\mathcal{O}_K = \mathbb{Z}[\alpha_1] = \cdots = \mathbb{Z}[\alpha_k]$ *for some pairwise inequivalent* $\alpha_1, \ldots, \alpha_k \in \mathcal{O}_K$*;* k **multiplicity** *of monogenity*

Most important consequences of Theorem C (Gy, 1973): **effective finiteness theorems in** Gy (1973, 74, 76, 78a, 78b), i.e. in Part I-V of Gy (1973)

for algebraic integer α, $D(\alpha) := D_{K/\mathbb{Q}}(\alpha)$, where $K = \mathbb{Q}(\alpha)$

Corollary 1 of Theorem C

Up to equivalence, there are only finitely many algebraic integers with given non-zero discriminant + **effective**. (This is Corollary 3 in Győry (1973); for the finiteness part see also the **ineffective** Corollary of Theorem 2 in Birch and Merriman (1972).)

In **given number field** K:

Corollary 2 of Theorem C

Up to equivalence, there are only finitely many $\alpha \in \mathcal{O}_K$ *with given index* I + **effective** and **quantitative**

The **most significant consequence** of Theorem C

Corollary 3 of Theorem C (Gy, 1973)

Up to equivalence, there only finitely many $\alpha \in \mathcal{O}_K$ *with* $\mathcal{O}_K = \mathbb{Z}[\alpha] \Leftrightarrow \{1, \alpha, \ldots, \alpha^{n-1}\}$ *power integral basis* + **effective** and **quantitative** (apply Corollary 2 with $I = 1$.)

breakthrough $\Longrightarrow$ the **first general effective algorithm** for **deciding** the **monogenity** resp. **multiplicity of monogenity** of a **number field** and, up to equivalence, **determining all power integral bases** in K + **generalizations** for **orders** (Part III) and for the **relative case** (Part IV)

An important reformulation of Corollaries 2 and 3 of Theorem C in terms of index form equations

Hensel (1894): *To every integral basis* $\{1, \omega_2, \ldots, \omega_n\}$ *of* K *there corresponds a form* $I(X_2, \ldots, X_n)$ *of degree* $n(n-1)/2$ *in* $n-1$ *variables with coefficients in* $\mathbb{Z}$ *such that for* $\alpha \in \mathcal{O}_K$,

$$I(\alpha) = |I(x_2, \ldots, x_n)| \text{ if } \alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n \text{ with } x_1, \ldots, x_n \in \mathbb{Z} \quad (4.3)$$

$I(X_2, \ldots, X_n)$ *is called an* **index form**, *and for given non-zero* $I \in \mathbb{Z}$

$$I(x_2, \ldots, x_n) = \pm I \text{ in } x_2, \ldots, x_n \in \mathbb{Z} \quad (4.4)$$

an **index form equation**.

In view of (4.3), Corollary 2 is **equivalent** to

Corollary 4 of Theorem C

For given $I \in \mathbb{Z} \setminus \{0\}$ the index form equation (4.4) *has only finitely many solutions, and they can be, at least in principle, effectively determined* (Part III of Gy; 1973).

In particular, **for** $I = 1$ we get the following *equivalent reformulation* of *Corollary 3*

Corollary 5 of Theorem C

The index form equation

$$I(x_2, \dots, x_n) = \pm 1 \text{ in } x_2, \dots, x_n \in \mathbb{Z} \tag{4.5}$$

has only finitely many solutions + **effective** and **quantitative** (Part III).

The best known bound for the solutions of (4.5):

$$\max_{2 \le i \le n} |x_i| < \exp\{10^{n^2}(|D_K|(\log |D_K|)^n)^{n-1}\}, \tag{4.6}$$

see Evertse and Gy (2017).

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

K number field of *degree* $n \geq 3$, $\mathcal{O}_K$ ring of integers, $I(X_2, \ldots, X_n)$ an *index form* over K

$$I(x_2, \ldots, x_n) = \pm 1 \text{ in } x_2, \ldots, x_n \in \mathbb{Z} \tag{4.5}$$

(4.6) **exponential** bound for $\max_i |x_i|$ *too large* for *practical* use

If $|D_K|$ is not too large, there are *methods* for *solving* (4.5) in *concrete* cases $\Leftrightarrow$ for *computing* all *generators* of *power integral bases* in K, *up to degree* $\mathbf{n \leq 6}$ **in general**, and for many special *higher degree fields up to about degree* 15 $\Rightarrow$ for *deciding how many times K is monogenic*. **Breakthrough in the 1990's, practical algorithms, computational results** and **tables**.

For $\mathbf{n = 3, 4}$, (4.5) $\Longrightarrow$ *Thue equations of degree* ≤ 4, *efficient algorithm;*

$\mathbf{n = 3}$, (4.5) $\Longrightarrow$ *cubic Thue quation* (Gaál, Schulte 1989);

$\mathbf{n = 4}$, (4.5) $\Longrightarrow$ *one cubic and some quartic Thue equations* (Gaál, Pethő, Pohst, 1991–96), many very interesting results

Refined version of the general approach combined with reduction and enumeration algorithms

In general, for $\mathbf{n \geq 5}$, a **refined version** of the **general approach** involving **unit equations** is needed. Since

$$(4.5) \Longleftrightarrow D_{K/\mathbb{Q}}(\alpha) = D_K \Longleftrightarrow D(f_\alpha) = D_K \text{ in } \alpha \in \mathcal{O}_K$$

with minimal polynomial $f_\alpha \in \mathbb{Z}[X]$, in case of *concrete equations* (4.5), the **basic idea** of the **proof** of **Theorem C** must be *combined* with some reduction and enumeration algorithms.

Refined version of the general method: *reduction* to *unit equations* but in considerably smaller subfields in the normal closure L of K, and use of Baker's method; cf. Gy (1998, 2000), see also Evertse and Gy (2017).

The *bounds* in concrete cases are still *too large*. Hence **reduction algorithm** is needed, *reducing* the *Baker's bound* in several steps if necessary by *refined versions* of the L^3*-algorithm*; cf. de Weger; Wildanger.

The *last step* is to apply **enumeration algorithm**, determining the **small** solutions *under the reduced bound*; cf. Wildanger; Gaál and Pohst; Bilu, Gaál and Gy.

Combining the *refined version* with *reduction* and *enumeration algorithms*, for $\mathbf{n = 5, 6}$ Gaál and Győry (1999), resp. Bilu, Gaál and Győry (2004) $\Longrightarrow$ *algorithms for determining all power integral bases* $\Longrightarrow$ checking the *monogenity* and the *multiplicity of the monogenity* of K.

Examples: Resolution of *index form equations* (4.5), in the most difficult cases when $K = \mathbb{Q}(\alpha)$, degree n, *totally real*, with Galois group S_n, $f_\alpha \in \mathbb{Z}[X]$ *primitive minimal polynomial of* $\alpha \Longrightarrow$ *all power integral bases* $\Longrightarrow$ *multiplicity of the monogenity of* K:

n = 3, $f_\alpha(X) = X^3 - X^2 - 2X + 1$, K 9 *times* monogenic (Gaál, Schulte, 1989);

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

n = 5, $f_\alpha(X) = X^5 - 5X^3 + X^2 + 3X - 1$, K 39 *times* monogenic (Gaál, Gy, 1999); $\approx$ 8h

n = 6, $f_\alpha(X) = X^6 - 5X^5 + 2X^4 + 18X^3 - 11X^2 - 19X + 1$, K, 45 *times* monogenic (Bilu, Gaál, Gy, 2004); hard computation

For **n** $\geq$ **7**, the above algorithms **do not work** in general. Hence, for $n \geq 7$, further improvements would be needed.

Theorem D can be applied to algebraic numbers that are not necessarily algebraic integers. Given an algebraic number α, we denote by f_α its *primitive minimal polynomial*, i.e.,

$$f_\alpha = a_0X^n + a_1X^{n-1} + \cdots + a_n = a_0(X - \alpha^{(1)}) \cdots (X - \alpha^{(n)}) \in \mathbb{Z}[X], \quad (6.1)$$

where $a_0 > 0$, $\gcd(a_0, \ldots, a_n) = 1$ and $\alpha^{(1)} = \alpha, \ldots, \alpha^{(n)}$ are the conjugates of α. We recall that the *height* and *discriminant* of α are defined by those of f_α, i.e.,

$$H(\alpha) := H(f_\alpha), \ D(\alpha) := D(f_\alpha).$$

Two algebraic numbers α, β are called $GL_2(\mathbb{Z})$-*equivalent* if

$$\beta = \frac{a\alpha + b}{c\alpha + d} \text{ with } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}).$$

If α, β are $GL_2(\mathbb{Z})$-equivalent then so are f_α, f_β while conversely, if f_α, f_β are $GL_2(\mathbb{Z})$-equivalent then α is $GL_2(\mathbb{Z})$-equivalent to a conjugate of β.

Now **Theorem D** implies at once

Theorem 6.1 (Evertse and Gy, 1991)

Every algebraic number α of degree $n \geq 2$ and discriminant $D \neq 0$ is $GL_2(\mathbb{Z})$-equivalent to an algebraic number β with

$$H(\beta) \leq c(n, |D|),$$

where c is an effectively computable positive number.

Further, by Theorem 1 of Gy (1974), we have

$$n \leq 2 \log |D| / \log 3$$

Rationally monogenic orders

Monogenic orders $\mathbb{Z}[\alpha]$, where α is an algebraic integer, can be generalized to so-called *rationally monogenic orders* $\mathbb{Z}_\alpha$, where α is not necessarily integral.

Let α be a non-zero, not necessarily integral algebraic number of degree $n \geq 3$, and f_α its primitive minimal polynomial given by (6.1).

Define $\mathbb{Z}_\alpha$ to be the $\mathbb{Z}$-*module with basis*

$1, \omega_2 := a_0\alpha, \omega_3 := a_0\alpha^2 + a_1\alpha, \ldots, \omega_n := a_0\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-2}\alpha.$

This $\mathbb{Z}$-module was introduced by Birch and Merriman (1972), $\mathbb{Z}_\alpha \subset$ ring of integers of $\mathbb{Q}(\alpha)$, and

$$D(\mathbb{Z}_\alpha) = D(f_\alpha) = D(\alpha). \tag{6.2}$$

Nakagawa (1989): $\mathbb{Z}_\alpha$ *order* in $\mathbb{Q}(\alpha)$.

Del Corso, Dvornicich, Simon (2005): $\mathbb{Z}_\alpha = \mathbb{Z}[\alpha] \cap \mathbb{Z}[\alpha^{-1}]$

If α algebraic integer $\Longrightarrow \mathbb{Z}_\alpha = \mathbb{Z}[\alpha]$

If α, β algebraic and $GL_2(\mathbb{Z})$-equivalent $\Longrightarrow \mathbb{Z}_\alpha = \mathbb{Z}_\beta$

Definition

An *order* $\mathcal{O}$ in a number field K *rationally monogenic if there is* α *s.t.* $\mathcal{O} = \mathbb{Z}_\alpha \Longrightarrow$ monogenic orders are rationally monogenic

Evertse (2023): *Every number field* K *of degree* ≥ 3 *has infinitely many orders that are rationally monogenic but not monogenic.*

The following theorem follows directly from **Theorem 6.1** (Evertse and Gy, 1991) and (6.2).

Theorem 6.2 (Evertse and Gy, 202?)

Let $\mathcal{O}$ be an order in a number field K, and denote by $D(\mathcal{O})$ its discriminant. Then every α such that $\mathbb{Z}_\alpha = \mathcal{O}$ is $GL_2(\mathbb{Z})$-equivalent to some $\beta \in K$ of height $H(\beta) \leq c(n, |D(\mathcal{O}|)$, where c denotes the same effectively computable positive number as in Theorem 6.1.

This is an analogue of **Corollary 3** of **Theorem C** (Gy, 1973) and its generalization for orders, see also Remark 2 in Section 4.

Theorem 6.2 implies that for given order $\mathcal{O}$ in K, it can be effectively decided whether there is α such that $\mathcal{O} = \mathbb{Z}_\alpha$. Moreover, there are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of $\alpha \in K$ such that $\mathbb{Z}_\alpha = \mathcal{O}$, and a full system of representatives of those can be effectively determined.

VII. Further generalizations, consequences and applications of the effective reduction theory

Generalizations for

- algebraic number field case, $\mathfrak{p}$-adic case, finite étale algebras, finitely generated case
- analogous results over function fields

Consequences, applications to

- classical Diophantine equations (Thue equations, Thue–Mahler equations, Mordell equation, elliptic equations, superelliptic equations,
- discriminant form equations, more general decomposable form equations)
- arithmetic properties of discriminants and indices of algebraic integers,
- effective version of Shafarevich' conjecture/Faltings' theorem for hyperelliptic curves,
- root separation of integral polynomials
- effective version of Hermite's **Theorem A**
- canonical number systems in number fields and orders
- irreducible polynomials
- and many others

Related topics, not *strictly belonging* to the effective reduction theory

- *multiply monogenic and rationally monogenic orders*; uniform upper bounds for the multiplicity of (rational) monogenicity *of orders*
- *distribution of monogenic and non-monogenic number fields*;
- *arithmetic characterization of monogenic* and *multiply monogenic number fileds*. **Hasse problem**, great number of interesting special results, *the problem has not yet been solved in full generality*

Thank you for your attention!

Dear Jan-Hendrik,

Many thanks for our long and very fruitful collaboration which resulted in 35 joint papers and the books

- J.-H. Evertse and K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge, 2015
- J.-H. Evertse and K. Győry, *Discriminant Equations in Diophantine Number Theory*, Cambridge, 2017
- J.-H. Evertse and K. Győry, *Effective Results and Methods for Diophantine Equations over Finitely Generated Domains*, Cambridge, 2022

Best wishes,

Kálmán