EFFECTIVE REDUCTION THEORY OF INTEGRAL POLYNOMIALS OF GIVEN DISCRIMINANT, AND RELATED TOPICS

(survey with a brief historical overview)

JAN-HENDRIK EVERTSE AND KÁLMÁN GYŐRY

Dedicated to Charles Hermite (1822-1901) and Alan Baker (1939-2018), for their fundamental contributions to the field

ABSTRACT. For polynomials in $\mathbb{Z}[X]$, the classical $\mathbb{Z}$-equivalence (monic case) and $GL_2(\mathbb{Z})$-equivalence preserve the discriminant as an invariant. The effective reduction theory for integral polynomials of given degree and discriminant consists of results that give, for a given polynomial $f \in \mathbb{Z}[X]$, a $\mathbb{Z}$-equivalent (in the monic case) or $GL_2(\mathbb{Z})$-equivalent polynomial g whose coefficients are effectively bounded above in terms of only the degree and discriminant of f. We discuss the effective results of this type on quadratic and cubic polynomials, implied by work of Lagrange (1773) and Hermite (1851), the general ineffective theorem of Birch and Merriman (1972), the general effective theorem of Győry (1973) for monic polynomials, obtained independently, and that of Evertse and Győry (1991) for arbitrary polynomials. The proofs of these two effective theorems use Győry's effective results on unit equations, which were proved by means of Baker's effective theory of logarithmic forms. Later Evertse, Győry and others obtained several applications and generalizations; see the book Evertse and Győry (2017). In his long-forgotten paper Hermite (1857), Hermite attempted to extend the above results of Lagrange and Hermite to polynomials of arbitrary degree. However, as was pointed out in our joint work with Bhargava, Remete and Swaminathan (2023), Hermite (1857) proved an important result but with a weaker equivalence only. Thus, it was only by the above mentioned theorems of Győry (1973) and Evertse and Győry (1991) that Hermite's problem from 1857 was settled in full generality. This and many other recent results inspired us to write this survey paper on the subject. We present here several older and recent generalizations and applications of the effective reduction theory, e.g., to monogenic number fields and monogenic and rationally monogenic orders. We also give an overview of bounds on the number of times a given order is monogenic or rationally monogenic. In the Appendix we discuss further related topics not strictly belonging to the reduction theory of integral polynomials.

2020 Mathematics Subject Classification: 11C08, 11D72, 11J86.

Keywords and Phrases: polynomials, discriminants, $\mathbb{Z}$-equivalence, $GL_2(\mathbb{Z})$-equivalence, Hermite equivalence, power integral bases, monogenic number fields, monogenic and rationally monogenic orders.

Contents

1. Introduction

We give an overview of older and recent results on the reduction theory of integral polynomials of given discriminant, and its many consequences and applications. We first recall some definitions and notation.

1.1. **Preliminaries.**

Two monic polynomials $f, g \in \mathbb{Z}[X]$ of degree $n \geq 2$ are called $\mathbb{Z}$-*equivalent* if

$$g(X) = f(X + a) \text{ or } g(X) = (-1)^n f(-X + a) \text{ for some } a \in \mathbb{Z},$$

and two not necessarily monic polynomials $f, g \in \mathbb{Z}[X]$ of degree $n \geq 2$ are called $GL_2(\mathbb{Z})$-*equivalent* if

$$g(X) = \pm(cX + d)^n f\big(\tfrac{aX+b}{cX+d}\big) \text{ for some matrix } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z}),$$

i.e., $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$. Clearly, for monic polynomials $\mathbb{Z}$-equivalence implies $GL_2(\mathbb{Z})$-equivalence.

The *discriminant* of a polynomial

$$f = a_0 X^n + \cdots + a_n = a_0 \prod_{i=1}^{n} (X - \alpha_i), \quad \text{with } a_0 \neq 0$$

is defined by

$$D(f) := a_0^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

This is a homogeneous polynomial of degree $2n - 2$ in $\mathbb{Z}[a_0, \ldots, a_n]$; thus, if $f \in \mathbb{Z}[X]$ then $D(f) \in \mathbb{Z}$. As one may easily verify, polynomials that are $\mathbb{Z}$-equivalent or $GL_2(\mathbb{Z})$-equivalent have the same discriminant.

We define the *height* $H(f)$ of a polynomial $f = a_0 X^n + \cdots + a_n \in \mathbb{Z}[X]$ by

$$H(f) := \max(|a_0|, \ldots, |a_n|).$$

An *invariant* is a function $\mathbb{Z}[X] \to \mathbb{R}$ that assumes the same value at $GL_2(\mathbb{Z})$-equivalent polynomials. In general, *reduction theory of polynomials* is about results of the following type: given a set of invariants, $I_1, \ldots, I_t$, say, there exists for any $f \in \mathbb{Z}[X]$ a polynomial $g \in \mathbb{Z}[X]$ that is $GL_2(\mathbb{Z})$-equivalent (or $\mathbb{Z}$-equivalent in the monic case) to f and whose coefficients are bounded in terms of $I_1(f), \ldots, I_t(f)$. In this paper, we focus on results in which the height $H(g)$ of g is bounded above in terms of $\deg f$ and $|D(f)|$, i.e., on *reduction theory for polynomials of given degree and given discriminant*. Such results imply that up to $GL_2(\mathbb{Z})$-equivalence (resp. $\mathbb{Z}$-equivalence if

we restrict ourselves to monic polynomials) there are only finitely many polynomials $f \in \mathbb{Z}[X]$ of degree n and given discriminant $D \neq 0$.

In fact, most of the literature deals with reduction theory of *binary forms* of given discriminant. Recall that any binary form $F(X,Y) \in \mathbb{Z}[X,Y]$ can be factored as $\prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$ with algebraic α_i, β_i, and that its discriminant is $D(F) := \prod_{1\leq i<j\leq n}(\alpha_i\beta_j - \alpha_j\beta_i)^2$, which is a rational integer. Two binary forms $F, G \in \mathbb{Z}[X,Y]$ are called $GL_2(\mathbb{Z})$-equivalent if $G(X,Y) = \pm F(aX+bY, cX+dY)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$, and clearly, $GL_2(\mathbb{Z})$-equivalent binary forms have the same discriminant. The results on reduction theory for binary forms F can be translated immediately into results for univariate polynomials f and vice-versa, using the correspondence $f(X) = F(X,1)$, $F(X,Y) = Y^{\deg f} f(X/Y)$, i.e., F is the homogenization of f. Indeed, f and F have the same height and discriminant. Further, two polynomials $f, g \in \mathbb{Z}[X]$ are $GL_2(\mathbb{Z})$-equivalent if and only if their homogenizations are $GL_2(\mathbb{Z})$-equivalent. As in our joint paper BEGyRS (2023) with Bhargava, Remete and Swaminathan, we have chosen to formulate all our results in terms of univariate polynomials, to unify the separate reduction theories of monic polynomials and binary forms.

For definitions of *effectively given* concepts, structures and *effective determination, computation*, one can consult e.g. the corresponding sections of our books Evertse and Győry (2015, 2017, 2022).

1.2. **Summary and organization.**

Lagrange (1773) developed a reduction theory of integral binary quadratic forms of given discriminant, which can be translated immediately into a reduction theory for integral quadratic polynomials of given discriminant. His results imply that up to the classical $GL_2(\mathbb{Z})$-equivalence, resp. $\mathbb{Z}$-equivalence (monic case) there are only finitely many quadratic polynomials in $\mathbb{Z}[X]$ of given discriminant. Lagrange's result is *effective* in the sense that one can effectively determine the reduced polynomials. This was later made more precise by Gauss (1801).

Hermite (1848, 1851) introduced a reduction theory for binary forms, or equivalently univariate polynomials of arbitrary degree but using another invariant instead of the discriminant. In the case of cubic polynomials, Hermite's invariant is up to a constant a power of the absolute value of the discriminant. Thus, Hermite's reduction theory implies that up to $GL_2(\mathbb{Z})$-equivalence there are only finitely many *cubic* polynomials in $\mathbb{Z}[X]$ of given

discriminant. Hermite was apparently interested to extend this to polynomials of arbitrary degree $n \geq 4$. In Hermite (1857) he introduced a new equivalence relation (called by us '*Hermite equivalence*', see Section 3) and proved in an ineffective way a finiteness result on the corresponding equivalence classes of integral polynomials of degree n and discriminant D. But he did not compare his equivalence relation to the classical equivalence relations, i.e., to $GL_2(\mathbb{Z})$-equivalence and $\mathbb{Z}$-equivalence. The result of Hermite (1857) does not appear to have been studied in the literature until the excellent book of Narkiewicz (2018), where Hermite equivalence was confused with the classical equivalence relations.

Hermite's apparent goal, i.e., the finiteness result with $GL_2(\mathbb{Z})$-equivalence instead of Hermite equivalence, was finally achieved more than a century later by Birch and Merriman (1972) for arbitrary polynomials in an ineffective form and independently, for monic polynomials and in a more precise and effective form by Győry (1973). The general result of Birch and Merriman was subsequently made effective by Evertse and Győry (1991a). More precisely, Győry (1973) and Evertse and Győry (1991a) proved that there exists an effectively computable number $c(n, D)$ depending only on n and D such that every $f \in \mathbb{Z}[X]$ of degree n and discriminant $D \neq 0$ is $GL_2(\mathbb{Z})$-equivalent (and even $\mathbb{Z}$-equivalent in the monic case) to a polynomial g with height

$$H(g) \leq c(n, D). \tag{1.1}$$

These results heavily depend on effective finiteness results for unit equations $ax + by = 1$ with solutions x, y from the unit group of the ring of integers of a number field, which were derived in turn using Baker's theory of logarithmic forms. This solved the old problem of Hermite (1857) mentioned above in an effective way, and further resulted in many significant consequences and applications. For example, in the 1970's, Győry deduced from his paper from 1973 the first general effective algorithm that decides monogenicity [1] and existence of power integral bases of number fields, and in fact finds all power integral bases. For later applications and generalizations we refer to the monograph Evertse and Győry (2017) and Sections 4–9 of the present paper.

In our recent paper BEGyRS (2023) with Bhargava, Remete and Swaminathan we provided a thorough treatment of the notion of Hermite equivalence, and proved that $\mathbb{Z}$-equivalence and $GL_2(\mathbb{Z})$-equivalence are much more

[1] In the literature, the terms 'monogeneity' and 'monogenity' are also used.

precise than Hermite equivalence. This confirmed that Hermite's result from 1857 was weaker than those of Birch and Merriman, Győry, and that of Evertse and Győry mentioned above. It should of course be mentioned that unlike the last authors, Hermite didn't have the powerful Baker's theory of logarithmic forms and its application to unit equations at his disposal.

In Section 2 we briefly recall the reduction theory of quadratic and cubic polynomials of given non-zero discriminant. In Section 3, following BEGyRS (2023), we deal with Hermite equivalence and compare it with $\mathbb{Z}$-equivalence and $GL_2(\mathbb{Z})$-equivalence. In Section 4 we discuss in more detail the general results of Birch and Merriman (1972), Győry (1973), Evertse and Győry (1991a), and those from the paper BEGyRS (2023). We present the best known effective height estimates for the solutions of unit equations and S-unit equations. We sketch how to deduce results of the type (1.1). An important part of Section 4 is Subsection 4.7, which gives much stronger conjectural upper bounds for the height of g. These bounds follow from the abc-conjecture over number fields and related conjectures. This is partly joint work with Rafael von Känel. In Section 5 we present some consequences in algebraic number theory. In particular, we give an overview of effective finiteness results concerning algebraic numbers/integers of given discriminant, resp. given index, and index form equations. Further, we deduce applications to monogenic number fields and orders, and also generalizations to so-called rationally monogenic orders. In Section 6 we discuss practical algorithms for solving concrete index form equations, i.e., determining all power integral bases in concrete number fields of degree ≤ 6. In Section 7 we give applications to canonical number systems in number fields and orders, and in Section 8 to some classical Diophantine equations. Section 9 gives a brief overview of generalizations, among others to the number field and $\mathfrak{p}$-adic case, and to results where the ground ring is of characteristic 0 and finitely generated as a $\mathbb{Z}$-algebra. In Section 10 we give an overview of results concerning multiply monogenic and rationally monogenic orders, where we present uniform upper bounds for the multiplicity of (rational) monogenicity of orders, depending only on the degree of the underlying number field. In the Appendix we briefly discuss related topics not strictly belonging to reduction theory of integral polynomials, in particular statistical results for monogenic and rationally monogenic number fields, and Hasse's problem to give an arithmetic characterization of the monogenic number fields.

Remark. Since the 1970's, the reduction theory of integral polynomials of given discriminant has been constantly developing, with a growing number of results and applications. Except for Section 2, the other sections contain results from this period. We propose some problems, whose solutions would yield considerable progress in the reduction theory.

Acknowledgments. We thank Professors Yann Bugeaud, David Masser and Robert Tijdeman for their helpful and inspiring remarks. We are very much indebted to Professor Rafael von Känel for his important contributions to Subsection 4.7, and Professor Attila Pethő for his useful comments on Section 7. We are very grateful to Dr. Csanád Bertók for typing a substantial part of the manuscript. The second named author was supported in part from the Austrian-Hungarian joint project ANN130909 (FWF-NKFIH) and from NKFIH 150284.

2. Reduction theory of integral quadratic and cubic polynomials of given non-zero discriminant

As we mentioned, Lagrange (1773) was the first to develop a reduction theory for binary quadratic forms with integral coefficients. His theory was made more precise by Gauss (1801). For integral polynomials, their theories imply the following. Recall that the *height* $H(g)$ of a polynomial with integral coefficients is the maximum of the absolute values of its coefficients.

Theorem 2.1 (Lagrange, 1773; Gauss, 1801)**.** *For any quadratic polynomial $f \in \mathbb{Z}[X]$ of discriminant $D \neq 0$, there exists $g \in \mathbb{Z}[X]$, $GL_2(\mathbb{Z})$-equivalent to f, such that $H(g) \leq c(D)$ with some effectively computable constant $c(D)$ depending only on D.*

For monic polynomials, the following more precise variant is known.

Theorem 2.2. *For any monic quadratic polynomial $f \in \mathbb{Z}[X]$ of discriminant $D \neq 0$, there exists $g \in \mathbb{Z}[X]$, $\mathbb{Z}$-equivalent to f, such that $H(g) \leq c'(D)$ with some effectively computable constant $c'(D)$ depending only on D.*

The above results have the following effective equivalent variants.

Theorem 2.3. *There are only finitely many $GL_2(\mathbb{Z})$-equivalence (resp. $\mathbb{Z}$-equivalence) classes of quadratic (resp. monic quadratic) polynomials in $\mathbb{Z}[X]$ of given discriminant $D \neq 0$. Further, each equivalence class has a representative of height at most $c(D)$ (resp. $c'(D)$).*

Later, mostly these equivalent versions were investigated, used and generalized.

Hermite (1848, 1851) studied integral binary forms of degree larger than 2. He developed an effective reduction theory for such forms which implies, among other things, the following:

Theorem 2.4 (Hermite, 1848, 1851)**.** *There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of cubic polynomials in $\mathbb{Z}[X]$ of given non-zero discriminant, and a full set of representatives of these classes can be effectively determined (in the sense that the proof provides an algorithm to determine, at least in principle, a full system of representatives).*

In fact, Hermite (1848, 1851) introduced another invariant for polynomials $f \in \mathbb{Z}[X]$ of arbitrary degree, which is in fact the discriminant Δ_f of a positive definite binary quadratic form $\Phi_f(X,Y) = AX^2 + BXY + CY^2 \in \mathbb{R}[X]$ associated with f. He called f reduced if Φ_f is reduced in Gauss' sense, i.e., if $|B| \leq A \leq C$. He showed that f is $GL_2(\mathbb{Z})$-equivalent to a reduced polynomial g, and that the coefficients of g are bounded effectively in terms of Δ_f. Hermite showed further that for cubic f, $|\Delta_f| = |27D(f)|^{1/4}$, implying Theorem 2.4. Hermite's theory was made more precise by Julia (1917).

For more details about reduction theories of integral binary forms and polynomials of low degree we refer to Dickson, Vol. 3 (1919, reprinted 1971), Cremona (1999), Evertse and Győry (2017), Bhargava and Yang (2022), and for more general results and applications, also to Section 4 of the present paper and the references given there.

For the number of $\mathbb{Z}$-equivalence classes of *cubic monic* integral polynomials with given non-zero discriminant, no finiteness results were known before 1930. Then Delone and Nagell proved independently the following.

Theorem 2.5 (Delone, 1930; Nagell, 1930)**.** *Up to $\mathbb{Z}$-equivalence, there are only finitely many irreducible cubic monic polynomials in $\mathbb{Z}[X]$ of given non-zero discriminant.*

The proofs of Delone and Nagell of Theorem 2.5 were both *ineffective*, in that they did not provide a method to determine the polynomials. In fact, these proofs were based on a classical ineffective finiteness theorem of Thue (1909) on *Thue equations*, i.e. on equations of the form $F(x,y) = m$, $x, y \in \mathbb{Z}$, where $F \in \mathbb{Z}[X,Y]$ is an irreducible binary form of degree ≥ 3 and m is an integer. In some concrete cases Delone and Faddeev (1940) made effective

Theorem 2.5, and posed the problem to make it effective for any irreducible cubic monic polynomial. An effective version of Theorem 2.5 follows from the famous effective result of Baker (1968b) on Thue equations.

3. Hermite's attempt (1857) to extend the reduction results of polynomials of degree ≤ 3 to polynomials of arbitrary degree

3.1. $\mathbf{GL_n}(\mathbb{Z})$-equivalence of decomposable forms.

Hermite tried to extend his theorem (1851) on cubic integral binary forms resp. polynomials to the case of any degree $n \geq 4$, but without success. Instead, he proved a finiteness theorem with a *weaker equivalence*, see Theorem 3.2 below. Hermite's notion of equivalence (called by us 'Hermite equivalence') is based on an equivalence relation for certain *decomposable forms*.

Consider decomposable forms of degree $n \geq 2$ in the same number n of variables

$$F(\mathbf{X}) = a_0 \prod_{i=1}^{n} (\alpha_{i,1}X_1 + \cdots + \alpha_{i,n}X_n) \in \mathbb{Z}[X_1, \ldots, X_n],$$

where a_0 is a non-zero rational number and $\alpha_{i,j}$ are algebraic numbers, not all zero, for $i, j = 1, \ldots, n$. The *discriminant* of F is defined as

$$D(F) := a_0^2(\det(\alpha_{i,j}))^2.$$

It is important to note that $D(F)$ is a rational integer.

Let $GL_n(\mathbb{Z})$ denote the multiplicative group of $n \times n$ integer matrices of determinant ± 1. Two decomposable forms F, G as above are called $GL_n(\mathbb{Z})$-equivalent if

$$G(\mathbf{X}) = \pm F(U\mathbf{X}) \quad \text{for some } U \in GL_n(\mathbb{Z}),$$

where $\mathbf{X}$ denotes the column vector of variables $(X_1, \ldots, X_n)^T$.

It is easy to see that two $GL_n(\mathbb{Z})$-equivalent decomposable forms in n variables have the same discriminant.

Hermite proved the following.

Theorem 3.1 (Hermite, 1851)**.** *Let n and D be integers with $n \geq 2$, $D \neq 0$. Then the decomposable forms in $\mathbb{Z}[X_1, \ldots, X_n]$ of degree n and discriminant D lie in finitely many $GL_n(\mathbb{Z})$-equivalence classes.*

3.2. **Hermite equivalence of polynomials and Hermite's finiteness theorem.**
Let

$$f(X) = a_0(X - \alpha_1) \cdots (X - \alpha_n) \in \mathbb{Z}[X]$$

be an integral polynomial with $a_0 \in \mathbb{Z} \setminus \{0\}$, and $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$. Then the *discriminant* of f is

$$D(f) = a_0^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \in \mathbb{Z}.$$

To f we associate the *decomposable form*

$$[f](\mathbf{X}) := a_0^{n-1} \prod_{i=1}^{n} (X_1 + \alpha_i X_2 + \cdots + \alpha_i^{n-1} X_n) \in \mathbb{Z}[X_1, \ldots, X_n].$$

Using the properties of Vandermonde determinants, one can prove that

$$D([f]) = D(f). \tag{3.1}$$

The following equivalence relation was introduced by Hermite (1857):

- *Two polynomials $f, g \in \mathbb{Z}[X]$ of degree n are said to be* Hermite equivalent *if the associated decomposable forms $[f]$ and $[g]$ are $GL_n(\mathbb{Z})$-equivalent, i.e.,*

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

From (3.1) it follows directly that Hermite equivalent polynomials in $\mathbb{Z}[X]$ have the same discriminant.

Hermite's Theorem 3.1 on decomposable forms and identity (3.1) imply the following finiteness theorem on polynomials.

Theorem 3.2 (Hermite, 1854, 1857)**.** *Let $n \ge 2$ and $D \ne 0$ be integers. Then the polynomials $f \in \mathbb{Z}[X]$ of degree n and of discriminant D lie in finitely many Hermite equivalence classes.*

Hermite's proof is *ineffective*.

3.3. **Comparison between Hermite equivalence and $GL_2(\mathbb{Z})$-equivalence and $\mathbb{Z}$-equivalence.**
In our five authors paper with Bhargava, Remete and Swaminathan (BEGyRS, 2023) we integrated Hermite's long-forgotten notion of equivalence and his finiteness theorem into the reduction theory, corrected a faulty reference to Hermite's result in Narkiewicz' excellent book (2018) and compared

Hermite's theorem with the most significant results of this area; see the next Section 4.

In BEGyRS (2023) we proved that $GL_2(\mathbb{Z})$-equivalence and, in the monic case, $\mathbb{Z}$-equivalence imply Hermite equivalence.

Theorem 3.3 (BEGyRS, 2023)**.** *Let $f, g \in \mathbb{Z}[X]$ be two $\mathbb{Z}$-equivalent, resp. $GL_2(\mathbb{Z})$-equivalent integral polynomials. Then they are Hermite equivalent.*

Since $\mathbb{Z}$-equivalence implies $GL_2(\mathbb{Z})$-equivalence, it suffices to prove Theorem 3.3 for $GL_2(\mathbb{Z})$-equivalence. We recall the proof from BEGyRS (2023).

Proof. Let f, g in $\mathbb{Z}[X]$ be any two $GL_2(\mathbb{Z})$-equivalent polynomials of degree n. Then they can be written in the form $f(X) = a_0 \prod_{i=1}^{n}(X - \alpha_i)$ and $g(X) = \pm(cX + d)^n f\left(\frac{aX+b}{cX+d}\right)$, where $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$. Thus, we have

$$g(X) = \pm a_0 \prod_{i=1}^{n}(\beta_i X - \gamma_i), \text{ where } \beta_i = c - a\alpha_i,\ \gamma_i = -d + b\alpha_i$$

for $i = 1, \ldots, n$. Define the inner product of two column vectors

$$\mathbf{x} = (x_1, \ldots, x_n)^T,\ \mathbf{y} = (y_1, \ldots, y_n)^T \text{ by } \langle \mathbf{x}, \mathbf{y} \rangle := x_1 y_1 + \cdots + x_n y_n.$$

Let as before $\mathbf{X} = (X_1, \ldots, X_n)^T$. Thus,

$$[f](\mathbf{X}) = a_0^{n-1} \prod_{i=1}^{n} \langle \mathbf{a}_i, \mathbf{X} \rangle, \text{ where } \mathbf{a}_i = (1, \alpha_i, \ldots, \alpha_i^{n-1})^T,$$

$$[g](\mathbf{X}) = \pm a_0^{n-1} \prod_{i=1}^{n} \langle \mathbf{b}_i, \mathbf{X} \rangle, \text{ where } \mathbf{b}_i = (\beta_i^{n-1}, \beta_i^{n-2}\gamma_i, \ldots, \gamma_i^{n-1})^T.$$

Then $\mathbf{b}_i = t(A)\mathbf{a}_i$ with some $t(A) \in GL_n(\mathbb{Z})$ for $i = 1, \ldots, n$. So

$$\begin{aligned} [g](\mathbf{X}) &= \pm\, c^{n-1} \prod_{i=1}^{n} \langle t(A)\mathbf{a}_i, \mathbf{X} \rangle = \\ &= \pm c^{n-1} \prod_{i=1}^{n} \langle \mathbf{a}_i, t(A)^T \mathbf{X} \rangle = \pm [f](t(A)^T \mathbf{X}), \end{aligned}$$

i.e. f and g are indeed Hermite equivalent. □

For integral polynomials of degree 2 and 3, Hermite equivalence and $GL_2(\mathbb{Z})$-equivalence coincide. For quadratic polynomials this is trivial, while for cubic polynomials this follows from a result of Delone and Faddeev (1940).

In BEGyRS (2023) we gave, for every $n \geq 4$ and both for the non-monic and for the monic case, infinite collections of polynomials in $\mathbb{Z}[X]$ with degree

n that are Hermite equivalent but not $GL_2(\mathbb{Z})$-equivalent. More precisely we proved the following.

Theorem 3.4 (BEGyRS, 2023)**.** *Let n be an integer ≥ 4.*

(i) There exist infinitely many Hermite equivalence classes of properly non-monic[2] *primitive*[3]*, irreducible polynomials of degree n that split into more than one $GL_2(\mathbb{Z})$-equivalence class.*

(ii) There exist infinitely many Hermite equivalence classes of monic irreducible polynomials of degree n that split into more than one $GL_2(\mathbb{Z})$-equivalence class.

In the monic case every $GL_2(\mathbb{Z})$-class contains a $\mathbb{Z}$-equivalence class, hence in (ii) $GL_2(\mathbb{Z})$-equivalence can be replaced by $\mathbb{Z}$-equivalence.

We proved Theorem 3.4 simultaneously for the cases (i) and (ii). We constructed, for every integer $n \geq 4$, an infinite parametric family of pairs $(f_{t,c}^{(n)}, g_{t,c}^{(n)})$ of primitive, irreducible polynomials $f_{t,c}^{(n)}$, $g_{t,c}^{(n)}$ of degree n, where c runs through 1 and an infinite set of primes, and t runs through an infinite set of primes with $t \neq c$ with the following properties:

(3.2) for each n, $f_{t,c}^{(n)}$, $g_{t,c}^{(n)}$ have leading coefficient c and are properly non-monic if $c > 1$;

(3.3) for each n, $f_{t,c}^{(n)}$, $g_{t,c}^{(n)}$ are Hermite equivalent;

(3.4) for each n, $f_{t,c}^{(n)}$, $g_{t,c}^{(n)}$ are not $GL_2(\mathbb{Z})$-equivalent;

(3.5) the pairs $(f_{t,c}^{(n)}, g_{t,c}^{(n)})$ $(n = 1, 2, \ldots)$ lie in different Hermite equivalence classes.

In fact, the construction is as follows. We start with a formal power series in X,

$$C(X) := \frac{1 - \sqrt{1 - 4X}}{2X} = (2X)^{-1}\left(1 - \sum_{i=0}^{\infty} \binom{1/2}{i}(-4X)^i\right) = \sum_{i=0}^{\infty} C_i X^i \tag{3.6}$$

[2]That is, not $GL_2(\mathbb{Z})$-equivalent to any monic polynomial

[3]An integral polynomial is called *primitive* if its coefficients have greatest common divisor 1

where $C_i = \frac{1}{i+1} \cdot \binom{2i}{i}$ is the i-th *Catalan number*. It is known that the C_i are integers, see, e.g., Stanley (2015). Next, let $n \geq 4$ be an integer, and let

$$a^{(n)}(X) := \sum_{i=0}^{n-2} C_i \cdot X^i \in \mathbb{Z}[X]$$

be the $(n-2)$-th partial sum of $C(X)$. Since

$$X \cdot C(X)^2 - C(X) + 1 = 0,$$

the coefficients of X^k $(k = 0, \ldots, n-2)$ in $X \cdot (a^{(n)}(X))^2$ and in $a^{(n)}(X) - 1$ are the same. Thus, as polynomials in $\mathbb{Z}[X]$, we have that

$$X^{n-1} \mid X \cdot (a^{(n)}(X))^2 - a^{(n)}(X) + 1. \tag{3.7}$$

Let

$$b^{(n)}(X) := \frac{X \cdot (a^{(n)}(X))^2 - a^{(n)}(X) + 1}{X^{n-1}}.$$

By (3.7), we have that $b^{(n)}(X)$ is a polynomial in $\mathbb{Z}[X]$ of degree $n-2$. Then, substituting $X - X^2$ for X in (3.6) we obtain

$$C(X - X^2) = \frac{1 - \sqrt{(1-2X)^2}}{2(X - X^2)} = \frac{1}{1-X}.$$

Using again that the coefficients of X^k $(k = 0, \ldots, n-2)$ in $(1-X) \cdot a^{(n)}(X - X^2)$ and in $(1-X) \cdot C(X - X^2) = 1$ are the same, we find that

$$X^{n-1} \mid (1-X) \cdot a^{(n)}(X - X^2) - 1. \tag{3.8}$$

Let

$$h^{(n)}(X) := \frac{(1-X) \cdot a^{(n)}(X - X^2) - 1}{X^{n-1}},$$
$$k^{(n)}(X) := -h^{(n)}(1-X) = \frac{1 - X \cdot a^{(n)}(X - X^2)}{(1-X)^{n-1}}.$$

By (3.8) $h^{(n)}(X)$ and $k^{(n)}(X)$ are polynomials in $\mathbb{Z}[X]$ of degree $n-2$. Now, let c be either 1 or a prime, and let t be a prime different from c. Define the polynomials

$$\widetilde{f_{t,c}^{(n)}}(X) := X^n + c^{n-1} t \cdot k^{(n)}(X),$$
$$\widetilde{g_{t,c}^{(n)}}(X) := X^n + c^{n-1} t (1 - 2X a^{(n)}(X)) + (c^{n-1} t)^2 \cdot b^{(n)}(X).$$

Then $f_{t,c}^{(n)}$, $g_{t,c}^{(n)}$ are given by

$$f_{t,c}^{(n)}(X) := c^{1-n}\widetilde{f_{t,c}^{(n)}}(cX) = cX^n + t \cdot k^{(n)}(cX),$$
$$g_{t,c}^{(n)}(X) := c^{1-n}\widetilde{g_{t,c}^{(n)}}(cX) = cX^n + t(1 - 2cXa^{(n)}(cX)) + c^{n-1}t^2 \cdot b^{(n)}(cX).$$

We briefly outline the main steps of the proofs of (3.2)–(3.5). Properties (3.2) and (3.3) are derived from the definitions of $f_{t,c}^{(n)}$ and $g_{t,c}^{(n)}$ by an elementary argument. The proof of (3.4) is more complicated. It requires the use of an irreducibility theorem of Dumas (1906), Chebotarev's density theorem, and Dirichlet's theorem on primes in arithmetic progressions. Finally, if we fix n, c and let $t \to \infty$, then the absolute value of the discriminant of $f_{t,c}^{(n)}$ tends to ∞. By making a selection, we may assume that the discriminants of the polynomials $f_{t,c}^{(n)}$ are pairwise different. Since Hermite equivalent polynomials have the same discriminant, we obtain (3.5).

Remark. We note that in our paper BEGyRS (2023) it turned out that the Hermite equivalence class of a polynomial has a very natural interpretation in terms of the so-called invariant order and invariant ideal associated with the polynomial, see Theorem 5.11 in Subsection 5.6 for more details. This fact turned out to be important in the above proofs.

Theorems 3.3 and 3.4 imply that $GL_2(\mathbb{Z})$-equivalence, resp. $\mathbb{Z}$-equivalence are *stronger* than Hermite equivalence, and hence that Hermite's Theorem 3.2 is weaker than the most significant results of this area presented in Section 4 below.

4. Reduction theory of integral polynomials of given non-zero discriminant and of arbitrary degree

As was mentioned in the Introduction, the breakthroughs in the reduction theory due to Birch and Merriman (1972), Győry (1973), and Evertse and Győry (1991a) settled the old problem of Hermite (1857), to prove that for every given $n \geq 2$ and $D \neq 0$ there are up to $GL_2(\mathbb{Z})$-equivalence only finitely many polynomials $f \in \mathbb{Z}[X]$ of degree n and discriminant D, and to determine these effectively. We state the results in more detail.

4.1. **The theorems of Birch and Merriman (1972), Győry (1973) and Evertse and Győry (1991a).**

Theorem 4.1 (Birch and Merriman, 1972). *Let $n \geq 2$ and $D \neq 0$. There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of polynomials in $\mathbb{Z}[X]$ of degree n and discriminant D.*

Birch and Merriman established this theorem in an equivalent form, in terms of integral binary forms. Their proof uses the finiteness of the number of solutions of *unit equations* $ax + by = 1$ in units x, y of the ring of integers of a number field, for which at the time effective proofs were available, but it combines this with some ineffective arguments. Consequently, Birch's and Merriman's proof of Theorem 4.1 is ineffective.

For monic polynomials, the corresponding result with $\mathbb{Z}$-equivalence was proved *independently* by Győry (1973) but in an *effective* form. This turned out to be of crucial importance in many applications; see e.g. Sections 5 to 9 below and Evertse and Győry (2017).

Theorem 4.2 (Győry, 1973). *Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 2$ with discriminant $D \neq 0$. Then*

(i) $n \leq c_1(|D|)$, and

(ii) there is a monic $g \in \mathbb{Z}[X]$, $\mathbb{Z}$-equivalent to f, such that

$$H(g) \leq c_2(n, |D|),$$

where c_1 and c_2 are effectively computable positive numbers depending on $|D|$, resp. on n and $|D|$.

This theorem was first proved and published in Győry's PhD dissertation Győry (1972a) and was utilized in Győry (1972b) as well.

Corollary 4.3 (Győry, 1973). *There are only finitely many $\mathbb{Z}$-equivalence classes of monic polynomials in $\mathbb{Z}[X]$ of given non-zero discriminant, and a full set of representatives of these classes can be at least in principle determined.*

In Győry (1974), an explicit version was given; see below.

In his proof of Theorem 4.2, Győry combined his own effective result on unit equations obtained by Baker's method, with his so-called 'graph method'. We sketch below the proof of Theorem 4.2.

Theorem 4.1, resp. Theorem 4.2 and its Corollary 4.3 are generalizations of the corresponding results presented in Section 2 for polynomials of degree $n \leq 3$; Theorem 4.1 gives an ineffective generalization of Theorem 2.4 for degree $n \geq 4$ and Theorem 4.2 is an effective generalization of Theorem

2.3 in the monic case for degree $n \geq 3$, and of Theorem 2.5 for any monic polynomial of degree $n \geq 3$.

In 1991, Evertse and Győry gave a new, effective proof for Birch's and Merriman's theorem, proving the following.

Theorem 4.4 (Evertse and Győry, 1991a)**.** *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ and discriminant $D \neq 0$. There is $g \in \mathbb{Z}[X]$, $GL_2(\mathbb{Z})$-equivalent to f, such that*

$$H(g) \leq c_3(n, |D|),$$

where $c_3(n, |D|)$ is an effectively computable number, given explicitly in terms of n and $|D|$.

This theorem was stated and proved in Evertse and Győry (1991a) in an equivalent form, in terms of integral binary forms.

As was mentioned above, Theorems 4.2 and 4.4 led to a general effective reduction theory of integral polynomials of given non-zero discriminant.

The main tool in our proof of Theorem 4.4 is an effective result of Győry (1974) *on homogeneous unit equations* in *three unknowns*, whose proof is also based on Baker's theory of logarithmic forms.

We note that Theorems 4.1 and 4.4 were established directly in a more general form, in the number field and $\mathfrak{p}$-adic case. In the proof of this more general version of Theorem 4.4 we used in Evertse and Győry (1991a) an effective result on homogeneous S-unit equations from Győry (1979). For such and other generalizations of Theorem 4.2, (ii), see Győry (1978b, 1984) and Section 9 below.

Theorems 4.2 and 4.4, their *explicit* versions below and their various generalizations have a great number of consequences and applications; see our book Evertse and Győry (2017) and Sections 5 to 9 below.

4.2. **Explicit versions of theorems of Győry (1973) and Evertse and Győry (1991a).**

First we present explicit versions of Theorem 2.1, Theorem 2.2 and Theorem 2.4 in the quadratic and cubic cases. An explicit version of Theorem 2.1 is the following.

Theorem 2.1*. *Let $f \in \mathbb{Z}[X]$ be a quadratic polynomial of discriminant $D \neq 0$. Then f is $GL_2(\mathbb{Z})$-equivalent to a quadratic polynomial $g \in \mathbb{Z}[X]$ such that*

(i) $H(g) \leq |D|/3$ if $D < 0$;

(ii) $H(g) \le |D|/4$ *if* $D > 0$ *and* f *is irreducible;*
(iii) $H(g) \le D^{1/2}$ *if* $D > 0$ *and* f *is reducible.*

The proof of this result is elementary. In the cubic case, we have the following.

Theorem 2.4*. *Let* $f \in \mathbb{Z}[X]$ *be a cubic polynomial of discriminant* $D \neq 0$. *Then* f *is* $GL_2(\mathbb{Z})$*-equivalent to a cubic polynomial* $g \in \mathbb{Z}[X]$ *such that*

(i) $H(g) \le \frac{64}{27}|D|^{1/2}$ *if* f *is irreducible;*
(ii) $H(g) \le \frac{64}{3\sqrt{3}}|D|$ *if* f *is reducible.*

This is Theorem 13.1.3 of Evertse and Győry (2017). In fact, Theorem 2.4* follows from Proposition 4.13 below and the remark following it.

In the monic case, it is relatively simple to prove the following explicit version of Theorem 2.2.

Theorem 2.2*. *For any monic quadratic polynomial* $f \in \mathbb{Z}[X]$ *with discriminant* $D \neq 0$, *there exist* $g \in \mathbb{Z}[X]$, $\mathbb{Z}$*-equivalent to* f, *such that*

$$H(g) \le |D|/4 + 1.$$

As was mentioned above, the first explicit version of Theorem 4.2 was given in Győry (1974). The height estimate was improved in 2017 by the authors.

We use the notation $\log^* x := \max(1, \log x)$ for $x > 0$.

Theorem 4.2* (Evertse and Győry, 2017)**.** *Let* $f \in \mathbb{Z}[X]$ *be a monic polynomial of degree* $n \ge 2$ *and discriminant* $D \neq 0$. *Then* f *is* $\mathbb{Z}$*-equivalent to a polynomial* $g \in \mathbb{Z}[X]$ *for which*

$$H(g) \le \exp\{n^{20} 8^{n^2+19} (|D|(\log^* |D|)^n)^{n-1}\}. \tag{4.1}$$

This is in fact Theorem 6.6.2 from Evertse and Győry (2017) with a slightly larger, simplified constant in terms of n.

A completely explicit, improved version of Theorem 4.4 was also established by the authors.

Theorem 4.4* (Evertse and Győry, 2017, Theorem 14.1.1)**.** *Let* $f \in \mathbb{Z}[X]$ *be a polynomial of degree* $n \ge 2$ *and discriminant* $D \neq 0$. *Then* f *is* $GL_2(\mathbb{Z})$*-equivalent to a polynomial* $g \in \mathbb{Z}[X]$ *for which*

$$H(g) \le \exp\{(4^2 n^3)^{25n^2} \cdot |D|^{5n-3}\}. \tag{4.2}$$

In both Theorems 4.2* and 4.4*, the degree n of f can also be explicitly estimated from above in terms of $|D|$.

Theorem 4.5 (Győry, 1974)**.** *Every polynomial $f \in \mathbb{Z}[X]$ with discriminant $D \neq 0$ has degree at most*

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

For monic polynomials $f \in \mathbb{Z}[X]$, the upper bound can be improved slightly to $2 + 2\log|D|/\log 3$.

Theorem 4.4 together with Theorem 4.5 implies the following analogue of Corollary 4.3.

Corollary 4.6 (Evertse and Győry, 1991a)**.** *There are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of polynomials in $\mathbb{Z}[X]$ of given non-zero discriminant, and a full set of representatives of these classes can be at least in principle effectively determined.*

4.3. **Consequences of Theorems 4.4*, 4.2* and Theorem 3.3 for Hermite equivalence classes.**

As was pointed out in BEGyRS (2023),an important consequence of the above Theorem 3.3 is that the effective finiteness theorems 4.4, 4.4* and 4.2, 4.2* for $GL_2(\mathbb{Z})$-equivalence classes resp. $\mathbb{Z}$-equivalence classes apply just as well to Hermite equivalence classes.

We present here the following, more precise, explicit variant of Hermite's result in Theorem 3.2.

Corollary 4.7 (of Theorems 4.4* and 4.2*; cf. BEGyRS, 2023)**.**

(i) Every Hermite equivalence class of polynomials in $\mathbb{Z}[X]$ of degree $n \geq 2$ and of discriminant $D \neq 0$ has a representative with coefficients not exceeding

$$\exp\{(4^2n^3)^{25n^2}|D|^{5n-3}\}$$

in absolute value.

(ii) Every Hermite equivalence class of monic polynomials in $\mathbb{Z}[X]$ with degree $n \geq 2$ and discriminant $D \neq 0$ has a representative with coefficients not exceeding

$$\exp\{n^{20}8^{n^2+19}(|D|(\log^*|D|)^n)^{n-1}\}$$

in absolute value.

It is an immediate consequence of Theorem 4.5 that in (i) above $n \leq 3 + 2\log|D|/\log 3$. Further, in (ii), the slightly better inequality $n \leq 2 + 2\log|D|/\log 3$ holds.

The above result implies an effective version of Theorem 3.2, i.e., for given n and a non-zero integer D, one can effectively determine a full system of representatives for the Hermite equivalence classes of polynomials $f \in \mathbb{Z}[X]$ of degree n and discriminant D. Indeed, one can make a finite list of all polynomials $f \in \mathbb{Z}[X]$ of height below one of the bounds in Corollary 4.7. For each polynomial in the list one can check whether it has discriminant D. Further, for each pair of polynomials in the list one can check whether they are Hermite equivalent, by computing the corresponding decomposable forms $[f], [g]$, and checking whether they are $GL_n(\mathbb{Z})$-equivalent, using, e.g., Lemma 18 of Evertse and Győry (1992a).

The similarity of Theorems 4.4* , 4.2* and Corollary 4.7 is only apparent. As was seen in Section 3, the $GL_2(\mathbb{Z})$-equivalence and $\mathbb{Z}$-equivalence are in fact much stronger than the Hermite equivalence.

Remark. Every improvement of the bounds in (4.1) or (4.2) would yield the same improvement in the bounds of Corollary 4.7.

4.4. **Unit equations and S-unit equations.**

The unit equations and more general S-unit equations play a fundamental role in Diophantine number theory, and in particular in the effective reduction theory of integral polynomials of given discriminant.

First we recall unit equations and S-unit equations, and then briefly outline how to apply Baker's theory of logarithmic forms to obtain effective bonds for the solutions of these equations. Then we recall the best known height bounds for the solutions of unit equations and S-unit equations over number fields.

For a detailed treatment of unit equations, S-unit equations and their further generalizations and applications we refer to our books Evertse and Győry (2015, 2017, 2022).

Let K be an algebraic number field, $\mathcal{O}_K$ its ring of integers, $\mathcal{O}_K^*$ the unit group of $\mathcal{O}_K$, and M_K its set of places, consisting of the finite set of infinite places S_∞ of K (corresponding to the real embeddings and the pairs of conjugate complex embeddings of K in $\mathbb{C}$) and the finite places, which we may identify with the prime ideals of $\mathcal{O}_K$. To the places in M_K we can associate a set of absolute values $\{|\cdot|_v : v \in M_K\}$, normalized such that if v

lies above the place $p \in M_{\mathbb{Q}} := \{\infty\} \cup \{\text{primes}\}$, then for $a \in \mathbb{Q}$ one has $|a|_v = |a|_p^{[K_v:\mathbb{Q}_p]}$. These absolute values satisfy the product formula $\prod_{v \in M_K} |\alpha|_v = 1$ for $\alpha \in K^*$.

Let a, b be given non-zero elements of K. Equations of the form

$$ax + by = 1 \text{ in unknowns } x, y \in \mathcal{O}_K^* \tag{4.3}$$

are called *unit equations* (*in two unknowns*). More generally, let S be a finite subset of M_K with $S \supseteq S_\infty$. Denote by $\mathcal{O}_S$ the ring of S-integers, i.e., $\{x \in K : |x|_v \leq 1 \text{ for } v \notin S\}$ and by $\mathcal{O}_S^*$ denote the unit group of $\mathcal{O}_S$, i.e., group of S-units. Thus, $\mathcal{O}_S^* = \{x \in K : |x|_v = 1 \text{ for } v \notin S\}$. For $S = S_\infty$ we have $\mathcal{O}_S^* = \mathcal{O}_K^*$. Equations of the form

$$ax + by = 1 \text{ in unknowns } x, y \in \mathcal{O}_S^* \tag{4.4}$$

are called *S-unit equations* (*in two unknowns*). In many cases it is more convenient to consider the unit equations and S-unit equations in homogeneous form

$$ax + by + cz = 0 \text{ in unknowns } x, y, z \in \mathcal{O}_K^*, \text{ resp. } \mathcal{O}_S^*, \tag{4.4a}$$

where a, b, c denote fixed elements of $K \setminus \{0\}$.

For a long time these equations were utilized merely in special cases and in an implicit way. It was implicitly proved by Siegel (1921) for $S = S_\infty$ and by Parry (1950) for any S that equation (4.4) has only finitely many solutions. This implies the finiteness of the number of solutions of equation (4.4a) up to a common proportional factor. Lang (1960) gave a direct proof for a more general version of these finiteness theorems. Their proofs were ineffective.

Generalizing Gelfond's (1935) famous result obtained in the case $m = 2$, in the 1960's Baker made a major breakthrough in number theory by giving non-trivial explicit lower bounds for the absolute value of linear forms in logarithms of the form

$$b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m \neq 0, \ m \geq 2$$

where $b_1, \ldots, b_m$ are rational integers, resp. algebraic numbers, $\alpha_1, \ldots, \alpha_m$ are algebraic numbers different from 0 and 1, and $\log \alpha_1, \ldots, \log \alpha_m$ denote fixed determination of the logarithms. In case of rational integers $b_1, \ldots, b_m$, this is equivalent to bounding $|\prod \alpha_i^{b_i} - 1|$ non-trivially from below. Baker's general effective estimates led to significant applications, and opened a new effective epoch in the theory of Diophantine equations. Baker's quantitative results were later improved, generalized, extended to the $\mathfrak{p}$-adic case and

so on by himself and many other authors; for comprehensive overviews we refer to Baker (1990), Wüstholz, ed. (2002), Baker and Wüstholz (2007), and Bugeaud (2018), and for a shorter overview see Evertse and Győry (2015), Section 3.2. The last five decades saw the development of an *effective theory* of Diophantine equations.

General effective upper bounds for the solutions of (4.3) and (4.4a) in the case $S = S_\infty$ were deduced by Győry (1972a,b, 1973) using an effective result of Baker and Coates (1970), p. 601, on relative Thue equations over number fields. The first *explicit* upper bounds for the solutions of (4.3) and (4.4a) in case $S = S_\infty$ were deduced by Győry (1974) from an explicit inequality of Baker (1968a, Part IV) for linear forms in logarithms of algebraic numbers. For general S, Győry (1979) derived the first explicit bound for the solutions of (4.4), using also the $\mathfrak{p}$-adic version of Baker's theory. Independently, a slightly weaker effective bound was given by Kotov and Trelina (1979).

Let K be an algebraic number field. Given $\alpha_1, \ldots, \alpha_n \in K$, not all 0, we define the height of $(\alpha_1, \ldots, \alpha_n)$ relative to K by

$$H_K(\alpha_1, \ldots, \alpha_n) := \prod_{v \in K} \max(|\alpha_1|_v, \ldots, |\alpha_n|_v).$$

Recall that the naive height $H(\alpha)$ of an algebraic number α is given by the maximum of the absolute values of its minimal polynomial, with coefficients having gcd 1. Then we have

$$H(\alpha) \leq 2^{\deg \alpha} H_{\mathbb{Q}(\alpha)}(1, \alpha).$$

Following Section 1.3 from the paper "Solving Diophantine equations by Baker's theory" by Győry (2002), we briefly *sketch* a proof of the following theorem, by means of Baker's theory.

Theorem 4.8. *Let K be a number field, S a finite set of places of K containing S_∞, and a, b non-zero elements of K. Let $x, y \in \mathcal{O}_S^*$ satisfy* (4.4). *Then*

$$\max(H(x), H(y)) \leq c_4(K, S, a, b),$$

where c_4 is an effectively computable number, depending only on K, S, a, b.

Sketch. Let s denote the cardinality of S. There is a system of fundamental S-units $\{\varrho_1, \ldots, \varrho_{s-1}\}$ in $\mathcal{O}_S^*$ with heights bounded in terms of K and S. Let x, y be a solution of (4.4) in S-units. Then one can write

$$x = \xi_1 \varrho_1^{a_{11}} \cdots \varrho_{s-1}^{a_{1,s-1}}, \ y = \xi_2 \varrho_1^{a_{21}} \cdots \varrho_{s-1}^{a_{2,s-1}},$$

where ξ_1, ξ_2 are roots of unity in K and a_{ij} are unknown rational integer exponents. Assume without loss of generality that $A := \max_j |a_{1j}| \geq \max_j |a_{2j}|$. By elementary means one can show that

$$A \leq c_5 \log \max_{v \in S} |x|_v,$$

and combining this with $\prod_{v \in S} |x|_v = 1$, one concludes that there is a $v \in S$ such that

$$|x|_v \leq c_6 \exp\{-c_7 A\},$$

where c_5, c_6, c_7 can be given explicitly and depend only on K and S. This implies

$$0 < |\varrho_1^{a_{21}} \cdots \varrho_{s-1}^{a_{2,s-1}} - \alpha|_v \leq c_8 \exp\{-c_9 A\} \tag{4.5}$$

with an appropriate $\alpha \in K$ of bounded height. The constants c_8, c_9 and c_{10} below depend at most on K, S and a, b and can be given explicitly.

One can now apply the complex or $\mathfrak{p}$-adic version of Baker's theory according as $v \in S_\infty$ or $v \in S \setminus S_\infty$ and this yields

$$\exp\{-c_{10} \log A\} \leq |\varrho_1^{a_{21}} \cdots \varrho_{s-1}^{a_{2,s-1}} - \alpha|_v.$$

Comparing this with (4.5) we get

$$A \leq A_0 \tag{4.6}$$

where A_0 can be given explicitly. Finally, we obtain an upper bound for $H(x)$ and $H(y)$ which can also be given explicitly. □

Later, several improvements, effective generalizations, applications and algorithmic results have been obtained for unit and S-unit equations by means of Baker's theory; see among others Győry (1980b, 2002, 2019, 2022), Shorey and Tijdeman (1986), Sprindžuk (1993), Bugeaud and Győry (1996), Smart (1998), Gaál and Győry (1999), Hindry and Silverman (2000), Wüstholz, ed. (2002), Bilu (2002), Bilu, Gaál and Győry (2004), Győry and Yu (2006), Baker and Wüstholz (2007), Zannier (2009), Hajdu (2009), Bérczes, Evertse and Győry (2009), Evertse and Győry (2013, 2015 2017, 2022), Bérczes (2015a, 2015b), Bertók and Hajdu (2015, 2018), Bugeaud (2018), Gaál (2019), Le Fourn (2020), Alvarado et al. (2021), Győry and Le Fourn (2024), and the references given there.

The best known height bound for the solutions of (4.3) is due to Győry and Yu (2006). We formulate it in simplified form. As above, let K be a number

field of degree d and r the rank of $\mathcal{O}_K^*$. Denote by h_K, R_K the class number and regulator of K, respectively, and write again $\log^* x := \max(1, \log x)$.

Then Győry and Yu (2006) proved the following.

Theorem 4.9. *Let a, b be non-zero elements of K. Then for all $x, y \in \mathcal{O}_K^*$ satisfying (4.3) we have*

$$H_K(1, x, y) \leq (3H_K(1, a, b))^A,$$

where

$$A = d^5(2r+2)^{4r+40} R_K \log^* R_K.$$

Remark. The following inequality implies that A can be bounded abouve in terms of d and D_K only:

$$h_K R_K \leq |D_K|^{1/2} (\log^* |D_K|)^{d-1}.$$

The first inequality of this type was proved by Landau (1918). For the above version, see, e.g., Evertse and Győry (2015, formula (1.5.2)).

In this section we shall use only Theorem 4.9. Below we formulate a generalization to S-unit equations, Theorem 4.10, which is not used in this section, but will be needed in Section 9.

Consider the general case where S is an arbitrary finite set of places containing S_∞. In terms of S, the best known bounds can be found in Győry (2019), Le Fourn (2020) and Győry and Le Fourn (2024). We mention here the bound from Győry (2019) in simplified form. We introduce the necessary notation. Let as above K be a number field of degree d and r the rank of $\mathcal{O}_K^*$. Denote by h_K, R_K the class number and regulator of K, respectively. Further, let $S = S_\infty \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ with $t \geq 0$ are the prime ideals in S. Let $s := \#S$, and denote by R_S the S-regulator. It is known that

$$R_S = R_K \text{ if } t = 0, \quad R_S = i_S R_K \prod_{i=1}^{t} \log N_K \mathfrak{p}_i \text{ otherwise},$$

where i_S is a divisor of h_K and $N_K\mathfrak{a}$ denotes the norm of a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, i.e., $\#\mathcal{O}_K/\mathfrak{a}$. Let $P_S := 1$ if $t = 0$ and $P_S := \max_{1 \leq i \leq t} N_K \mathfrak{p}_i$ if $t \geq 1$. Further, put $P_S' := 1$ if $t \leq 2$ and P_S' the third largest among the quantities $N_K\mathfrak{p}_i$, $i = 1, \ldots, t$ if $t \geq 3$. Finally, put $\mathcal{T}_K := \max(h_K, 160r! \cdot (r+1)^2 R_K)$.

Theorem 4.10. *Let a, b be non-zero elements of K. Then for all $x, y \in \mathcal{O}_S^*$ with (4.4) we have*

$$H_K(1, x, y) \le (3H_K(1, a, b))^{A_S},$$

where

$$A_S := 2s^5(16ed)^{4s+3}\mathcal{T}_K^{t+4} \cdot \frac{P_S'}{\log^* P_S'}\Big(1 + \frac{\log^* \log P_S}{\log^* P_S'}\Big)R_S.$$

Observe that for $S = S_\infty$, A is much smaller than A_S. Further, A_S can be bounded above in terms of d, $|D_K|$, t, and P_S.

We compare Theorem 4.10 with the abc-conjecture over number fields. We first recall the abc-conjecture over $\mathbb{Q}$, as proposed by Masser in 1985, refining an earlier conjecture of Oesterlé, see Masser (2017) for a historical account. Define the *radical* of a non-zero integer a by $\mathcal{R}(a) := \prod_{p|a} p$.

Conjecture 4.11 (Masser-Oesterlé abc-conjecture, 1985)**.** *There is a constant $C(\epsilon) > 0$ depending on ϵ such that for all $\epsilon > 0$ and all non-zero integers a, b, c with $a + b = c$ and $\gcd(a, b, c) = 1$ we have $\max(|a|, |b|, |c|) \le C(\epsilon)\mathcal{R}(abc)^{1+\epsilon}$.*

There are various proposals to extend this to number fields. We recall a version of Masser (2002). Let K be a number field and D_K its discriminant. Take a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$. Masser defined the modified radical of $\mathfrak{a}$ by $\mathcal{R}_K(\mathfrak{a}) := \prod_{\mathfrak{p}|\mathfrak{a}} N_K\mathfrak{p}^{e_\mathfrak{p}}$, where the product is taken over all prime ideals dividing $\mathfrak{a}$ and $e_\mathfrak{p}$ is the ramification index of $\mathfrak{p}$. Masser considered this modified radical since it has a good behaviour under field extensions, e.g., if L is an extension of K of degree m, then $\mathcal{R}_L(\mathfrak{a}\mathcal{O}_L) = \mathcal{R}_K(\mathfrak{a})^m$.

Recall that the different of K can be expressed as $\mathfrak{D}_K = \prod_\mathfrak{p} \mathfrak{p}^{w_\mathfrak{p}}$, where the product is taken over all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ with $e_\mathfrak{p} > 1$, and where $w_\mathfrak{p} \ge e_\mathfrak{p} - 1$. Further, $|D_K| = N_K\mathfrak{D}_K$. This implies that for any ideal $\mathfrak{a}$ of $\mathcal{O}_K$,

$$\mathcal{R}_K'(\mathfrak{a}) \,|\, \mathcal{R}_K(\mathfrak{a}) \,|\, D_K \cdot \mathcal{R}_K'(\mathfrak{a}), \quad \text{where } \mathcal{R}_K'(\mathfrak{a}) := \prod_{\mathfrak{p}|\mathfrak{a}} N_K\mathfrak{p}. \tag{4.7}$$

Conjecture 4.12 (Masser's uniform abc conjecture over number fields, 2002)**.** *There is a constant $C(\epsilon) > 0$ depending on ϵ, such that for every $\epsilon > 0$ the following holds. For every number field K of discriminant D_K and every non-zero $\alpha, \beta, \gamma \in K$ with $\alpha + \beta = \gamma$, we have*

$$H_K(\alpha, \beta, \gamma) \le C(\epsilon)^{[K:\mathbb{Q}]}\big(|D_K| \cdot \mathcal{R}_K(\mathfrak{a}^{-3}\alpha\beta\gamma)\big)^{1+\epsilon},$$

where $\mathfrak{a}$ *is the fractional ideal generated by* α, β, γ.

This implies the following bound for the solutions of the S-unit equation (4.4) $ax + by = 1$ in $x, y \in \mathcal{O}_S^*$, where again S is a finite set of places of K, containing the infinite places and $a, b \in K^*$: let $\mathcal{R}_S := 1$ if $S = S_\infty$ and $\mathcal{R}_S := \prod_{i=1}^t N_K \mathfrak{p}_i^{e_{\mathfrak{p}_i}}$, and put $\mathcal{R}_K(a,b) := \prod_{\mathfrak{p}} N\mathfrak{p}^{e_{\mathfrak{p}}}$, where the product is taken over all $\mathfrak{p} \in M_K \setminus S$ such that $|a|_{\mathfrak{p}}$ and $|b|_{\mathfrak{p}}$ are not both equal to 1. Then for every solution $x, y \in \mathcal{O}_S^*$ of $ax + by = 1$ we have

$$H_K(1,x,y) \le C(\epsilon)^d \big(|D_K| \cdot \mathcal{R}_S \cdot \mathcal{R}_K(a,b)\big)^{1+\epsilon} H_K(1,a,b)^2.$$

See also Győry (2022), Theorem 3.

Some alternative effective methods were also developed to obtain effective bounds for the solutions of S-unit equations. Bombieri (1993, 2002) and Bombieri and Cohen (1997, 2003) worked out such an effective method in Diophantine approximation, based on an extended version of the Thue–Siegel principle, Dyson's Lemma and some geometry of numbers. Bugeaud (1998), following their approach and combining it with estimates for linear forms in logarithms, proved results which are in certain parameters sharper than those of Bombieri and Cohen.

During 1983–95 Frey initiated and developed in several papers the modular approach for S-unit equations over $\mathbb{Q}$; see e.g. Frey (1997) where he gives height bounds for such equations which became unconditional around 2000 when the Shimura-Taniyama conjecture was proved. As is surveyed by von Känel (2024), these height bounds for S-unit equations over $\mathbb{Q}$ were made explicit independently and simultaneously by von Känel (2013, 2014b) and by Murty and Pasten (2013), Pasten (2014).

However, it should be remarked that for most applications of S-unit equations, including the reduction theory of integral polynomials treated in our paper, more general results concerning S-unit equations of the form (4.4) over arbitrary number fields are needed. At present, these cannot be obtained by the modular method.

4.5. **A brief sketch of the proof of a less precise version of Theorem 4.2.**

Consider a monic polynomial $f \in \mathbb{Z}[X]$ of degree n and discriminant $D \neq 0$. In view of Theorem 2.3 we may assume that $n \ge 3$.

First we sketch the proof of assertion (i). Assume that f is irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$ for a zero α of f, and denote by D_K the discriminant of

K. Then combining the Minkowski inequality with the fact that D_K divides $D(f)$, i.e. D, (i) follows with an appropriate c_1. If now f is reducible and $f = f_1 \cdots f_t$ with monic irreducible $f_1, \ldots, f_t$, then using $D(f_j) \mid D(f)$ in $\mathbb{Z}$ and applying the just proved (i) for $j = 1, \ldots, t$, we obtain (i) in the general case as well.

We now sketch the proof of (ii) in Theorem 4.2. Its main steps are as follows.

1. Denote by $\alpha_1, \ldots, \alpha_n$ the zeros of f, and by G the splitting field of f over $\mathbb{Q}$. Then $[G : \mathbb{Q}] \leq n!$ and the absolute value $|D_G|$ of the discriminant of G can be estimated from above by a constant $c_{11}(n, |D|)$. Here and below $c_{11}, \ldots$ are effectively computable numbers depending only on n and $|D|$.

2. Putting $\Delta_{ij} := \alpha_i - \alpha_j$ we have

$$\prod_{1 \leq i < j \leq n} \Delta_{ij}^2 = D,$$

which implies $|N_{G/\mathbb{Q}} \Delta_{ij}| \leq c_{12}(n, |D|)$. It follows that

$$\Delta_{ij} = \delta_{ij} \varepsilon_{ij}, \text{ where } H(\delta_{ij}) \leq c_{13}(n, |D|) \tag{4.8}$$

and ε_{ij} is a unit in the ring of integers of G.

3. The following identity plays a basic role in the proof:

$$\Delta_{ij} + \Delta_{jk} = \Delta_{ik} \text{ for every } i, j, k. \tag{4.9}$$

Consider the *graph*, whose vertices are Δ_{ij} $(1 \leq i \neq j \leq n)$ and whose edges are $[\Delta_{ij}, \Delta_{ik}]$, $[\Delta_{ij}, \Delta_{jk}]$ $(1 \leq i \neq j \leq n,\ k \neq i, j)$. This graph is obviously connected.

4. Equations (4.8) and (4.9) give rise to a 'connected' system of *unit equations*

$$\delta_{ijk} \varepsilon_{ijk} + \tau_{ijk} \nu_{ijk} = 1, \tag{4.10}$$

where $\delta_{ijk} := \delta_{ij}/\delta_{ik}$, $\tau_{ijk} := \delta_{jk}/\delta_{ik}$ are non-zero elements of G with heights effectively bounded above in terms of n and $|D|$ only, and $\varepsilon_{ijk} := \varepsilon_{ij}/\varepsilon_{ik}$, $\nu_{ijk} := \varepsilon_{jk}/\varepsilon_{ik}$ are *unknown* units in the ring of integers of G.

5. Applying Theorem 4.9, together with the Remark following it, we get upper bounds for the heights of the quotients $\Delta_{ij}/\Delta_{ik} = \delta_{ijk}\varepsilon_{ijk}$ for each triple $\{i, j, k\} \subset \{1, \ldots, n\}$, depending on G, n and $|D|$, and so eventually only on n and $|D|$, and likewise for Δ_{jk}/Δ_{ik}.

6. Using the connectedness of the unit equations involved, this yields effective

upper bounds for the height of Δ_{ij} for every i, j, depending only on n and $|D|$. Indeed, one first obtains an upper bound for the height of any quotient Δ_{ij}/Δ_{kl} via

$$\frac{\Delta_{ij}}{\Delta_{kl}} = \frac{\Delta_{ij}}{\Delta_{ik}} \cdot \frac{\Delta_{ik}}{\Delta_{kl}}$$

(using the path $\Delta_{ij} \to \Delta_{ik} \to \Delta_{kl}$ in the graph) and subsequently for the height of each Δ_{ij} individually via

$$\Delta_{ij}^{n(n-1)} = \pm D \cdot \prod_{1 \le k \ne l \le n} \frac{\Delta_{ij}}{\Delta_{kl}}.$$

7. Adding the differences $\Delta_{ij} = \alpha_i - \alpha_j$ for fixed i and for $j = 1, \ldots, n$, using the fact that $\alpha_1 + \cdots + \alpha_n \in \mathbb{Z}$, putting $\alpha_1 + \cdots + \alpha_n = na + a'$ with $a, a' \in \mathbb{Z}$, $0 \le a' < n$, and writing

$$\beta_i := \alpha_i - a \text{ for } i = 1, \ldots, n,$$
$$g(X) = \prod_{i=1}^{n} (X - \beta_i),$$

we have that $g(X) = f(X + a) \in \mathbb{Z}[X]$ and that the height of g has an effective upper bound depending only on n and $|D|$. □

Remark. We note that for cubic and quartic monic polynomials $f \in \mathbb{Z}[X]$ of given non-zero discriminant, Klaska (2021, 2022) devised another approach for proving Corollary 4.3 via the theory of integral points on elliptic curves.

4.6. **A brief sketch of the proof of a less precise version of Theorem 4.4.**

Take an integral polynomial $f \in \mathbb{Z}[X]$ of degree n and discriminant $D \ne 0$. In view of Theorems 2.1, 2.2 and 2.4 we may assume that $n \ge 4$. The absolute value of the discriminant of the splitting field of f can be estimated from above in terms of $|D|$, and by the Hermite-Minkowski Theorem, this leaves only a finite, effectively determinable collection of possible splitting fields for f. So we may restrict ourselves to polynomials f with given splitting field G and ring of integers $\mathcal{O}_G$.

Take such f and pick a factorization of f,

$$f = \prod_{i=1}^{n} (\alpha_i X - \beta_i) \text{ over } \overline{\mathbb{Q}}, \tag{4.11}$$

such that the number of linear factors with real coefficients is maximal, and the factors with complex coefficients fall apart into complex conjugate pairs. After multiplying f by a small positive rational integer, which can be effectively bounded in terms of G, hence in terms of n and $|D|$ and which is negligible compared with the other estimates arising from the application of Baker's method, we may assume that f has such a factorization with $\alpha_i, \beta_i \in \mathcal{O}_G$ for $i = 1, \ldots, n$. Put

$$\Delta_{ij} := \alpha_i\beta_j - \alpha_j\beta_i \quad \text{for } 1 \le i, j \le n.$$

We now follow the approach of Evertse and Győry (2017), chapters 13 and 14. We outline the main steps of the proof.

1. We start with a small variation on the reduction theories of Hermite (1848, 1851) and Julia (1917). Let $\mathbf{t} = (t_1, \ldots, t_n)$ be a tuple of positive reals such that $t_i = t_j$ for each pair (i, j) such that α_i, β_i are the complex conjugates of α_j, β_j. Consider the positive definite quadratic form

$$\Phi_{f,\mathbf{t}}(X, Y) := \sum_{i=1}^{n} t_i^{-2}(\alpha_i X - \beta_i Y)(\overline{\alpha_i} X - \overline{\beta_i} Y).$$

By Gauss' reduction theory for positive definite binary quadratic forms, there is $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ such that $\Phi_{f,\mathbf{t}}(aX + bY, cX + dY)$ is reduced, i.e., equal to $AX^2 + BXY + CY^2$ with $|B| \le A \le C$. Define the polynomial

$$g(X) = (cX + d)^n f\left(\frac{aX + b}{cX + d}\right),$$

which is $GL_2(\mathbb{Z})$-equivalent to f. We denote by $H(g)$ the height of g. We recall Theorem 13.1.3 of Evertse and Győry (2017), and refer for the elementary proof to section 13.1 of that book.

Proposition 4.13. *Let $n \ge 3$, and*

$$M := t_1 \cdots t_n, \quad R := \left(\sum_{1 \le i < j \le n} \frac{|\Delta_{ij}|^2}{t_i^2 t_j^2}\right)^{1/2}.$$

Then

$$H(g) \le \left(\frac{4}{n\sqrt{3}}\right)^n M^2 R^n$$

if f has no root in $\mathbb{Q}$, and

$$H(g) \leq \left(\frac{2}{\sqrt{n}}\right)^n \cdot \left(\frac{2}{\sqrt{3(n-1)}}\right)^{n(n-1)/(n-2)} (M^2R^n)^{(n-1)/(n-2)}$$

if f does have a root in $\mathbb{Q}$.

Remark. Theorem 2.4* stated above follows by applying Proposition 4.13 with $n = 3$, $t_1 = |\Delta_{23}|^{-1}$, $t_2 = |\Delta_{13}|^{-1}$, $t_3 = |\Delta_{12}|^{-1}$.

2. Assume henceforth that $n \geq 4$. For any quadruple i, j, k, l of distinct indices we have the identity

$$\Delta_{ij}\Delta_{kl} + \Delta_{jk}\Delta_{il} = \Delta_{ik}\Delta_{jl}. \tag{4.12}$$

Notice that all terms Δ_{ij} are in $\mathcal{O}_G$ and divide D. Hence $|N_{G/\mathbb{Q}}(\Delta_{ij})| \leq |D|^{[G:\mathbb{Q}]}$ for all i, j where $[G : \mathbb{Q}] \leq n!$. As above in Section 4.4, we can express each term Δ_{ij} as a product of an element of height effectively bounded in terms of n, D and a unit from $\mathcal{O}_G$. By substituting this into the identities (4.12) we obtain homogeneous unit equations in three terms. Dividing (4.12) by $\Delta_{ik}\Delta_{jl}$ we get unit equations like in (4.10) above, and using Theorem 4.9 we obtain effective upper bounds for the heights of the quotients $\Delta_{ij}\Delta_{kl}/\Delta_{ik}\Delta_{jl}$.

3. To obtain an effective upper bound for the height of g in terms of n and $|D|$, it suffices to effectively estimate the quantities M and R from Proposition 4.13 from above in terms of n and $|D|$, for a suitable choice of the t_i. For the t_i we choose

$$t_i := \left(\prod_{k=1, k\neq i}^{n} |\Delta_{ik}|\right)^{1/(n-2)} \quad \text{for } i = 1, \ldots, n.$$

With this choice,

$$M = |D|^{1/(n-2)}$$

and

$$\frac{|\Delta_{ij}|}{t_i t_j} = \left(|D|^{-1} \cdot \prod_{k,l} \left|\frac{\Delta_{ij}\Delta_{kl}}{\Delta_{ik}\Delta_{jl}}\right|\right)^{1/(n-1)(n-2)},$$

where the product is taken over all pairs of indices k, l such that $1 \leq k, l \leq n$, $k \neq i, j$, $l \neq i, j$ and $k \neq l$. By inserting the upper bounds for the heights of the quantities $\Delta_{ij}\Delta_{kl}/\Delta_{ik}\Delta_{jl}$ obtained in the previous step, we can estimate

from above M and R, and subsequently $H(g)$, effectively in terms of n and $|D|$ only. □

4.7. **Conjectural improvements (partly joint work with von Känel).**

This subsection contains important contributions by Rafael von Känel.

As was mentioned above, for $n \geq 4$ resp. $n \geq 3$ the proofs of Theorems 4.2, 4.4, 4.2* and 4.4* are based on effective results of Győry on unit equations whose proofs depend on Baker's theory of logarithmic forms. The exponential feature of the bounds in (4.1) and (4.2) is a consequence of the use of Baker's method. It is likely that the bounds in (4.1) and (4.2) can be replaced by some bounds polynomial in terms of $|D|$. This can be achieved if we restrict ourselves to polynomials $f \in \mathbb{Z}[X]$ having a *fixed splitting field* G over $\mathbb{Q}$. In this case the bounds in (4.1) and (4.2) can be replaced by bounds of the form

$$c_{14}(n, G)|D|^{c_{15}(n,G)},$$

where $c_{14}(n, G), c_{15}(n, G)$ are effectively computable numbers which depend only on n and the discriminant of G; see Győry (1984, 1998) resp. Evertse and Győry (1991a). The following conjectures seem plausible.

Conjecture 4.14. *Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 3$ and discriminant $D \neq 0$. Then f is $\mathbb{Z}$-equivalent to a monic polynomial g in $\mathbb{Z}[X]$ such that*

$$H(g) \leq c_{16}(n)|D|^{c_{17}(n)}$$

where $c_{16}(n), c_{17}(n)$ depend only on n.

Conjecture 4.15. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 4$ and of discriminant $D \neq 0$. Then f is $GL_2(\mathbb{Z})$-equivalent to a polynomial g in $\mathbb{Z}[X]$ such that*

$$H(g) \leq c_{18}(n)|D|^{c_{19}(n)}$$

where $c_{18}(n), c_{19}(n)$ depend only on n.

Conjecture 4.15 has been formulated in Chapter 15 of Evertse and Győry (2017). In fact, Conjecture 4.15 implies Conjecture 4.14.

Conjecture 4.15 $\Longrightarrow$ Conjecture 4.14. Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 3$ and discriminant $D \neq 0$. Consider the polynomial $g(X) := (2X+1)^{n+1} f(\frac{X}{2X+1})$. Using that f is monic, one shows by means of a

straightforward computation that g has degree $n+1$ and $D(g) = D$. By Conjecture 4.15 there is $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ such that $g^*(X) := (cX+d)^{n+1} g(\frac{aX+b}{cX+d})$ has height at most $c_{18}(n+1)|D|^{c_{19}(n+1)}$. A straightforward computation shows that

$$g^*(X) = (c'X + d')f^*(X),$$

$$\text{with } c' = 2a + c,\ d' = 2b + c, \quad f^*(X) = (c'X + d')^n f(\tfrac{aX+b}{c'X+d'}).$$

Note that $|c'|, |d'|, H(f^*) \le c_{20}(n)H(g^*)$. Let r be an integer such that $a' := a + rc'$ satisfies $|a'| \le \frac{1}{2}|c'|$. Then from $ad' - bc' = \pm 1$ it follows that $b' := b' + rd'$ satisfies $|b'| \le \frac{1}{2}|d'| + 1$. Now define $f^{**}(X) := (-c'X + a')^n f^*(\frac{d'X-b'}{-c'X+a'})$. One verifies that $f^{**}(X) = f(\pm X \pm r)$ and $H(f^{**}) \le c_{16}(n)|D|^{c_{17}(n)}$. □

We give some evidence for the conjectures mentioned above. Evertse proved the following what one may call semi-effective result.

Theorem 4.16 (Evertse, 1993)**.** *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \ge 4$ and of discriminant $D \ne 0$, having splitting field G over $\mathbb{Q}$. Then f is $GL_2(\mathbb{Z})$-equivalent to a polynomial g of height*

$$H(g) \le c_{21}(n, G)|D|^{21/n}.$$

Here $c_{21}(n, G)$ is a number depending only on n and G, which is not effectively computable by the method of proof. For a proof, see also Evertse and Győry (2017, Chap. 15).

The main tool in Evertse's proof is the following theorem. The constant in this theorem is ineffective. Let K be a number field. Given $\alpha, \beta, \gamma \in K$, we define the height $H_K(\alpha, \beta, \gamma) := \prod_{v \in M_K} \max(|\alpha|_v, |\beta|_v, |\gamma|_v)$.

Theorem 4.17. *Let α, β, γ be non-zero elements of $\mathcal{O}_K$ with $\alpha + \beta = \gamma$. Then for all $\epsilon > 0$ we have*

$$H_K(\alpha, \beta, \gamma) \le c_{22}(K, \epsilon)|N_{K/\mathbb{Q}}(\alpha\beta\gamma)|^{1+\epsilon},$$

where $c_{22}(K, \epsilon)$ depends only on K and ϵ.

In fact, this is a special case of a general multivariable result of Evertse (1984b, Theorem 1), see also Evertse and Győry (2015, Theorem 6.1.1). The proof of this general result is based on Schmidt's Subspace Theorem over number fields. For Theorem 4.17 one needs the two-dimensional case, which is Roth's Theorem over number fields. Theorem 4.16 was deduced from Theorem 4.17 essentially by following the arguments in Subsection 4.6,

but with various refinements to obtain a bound with an exponent $O(1/n)$ on $|D|$.

In order to prove Conjecture 4.15, the following variation on Theorem 4.17 would suffice:

Conjecture 4.18. *For all number fields K of degree $d \geq 2$ and discriminant D_K and all non-zero $\alpha, \beta, \gamma \in \mathcal{O}_K$ with $\alpha + \beta = \gamma$ we have*

$$H_K(\alpha, \beta, \gamma) \leq c_{23}(d)|D_K \cdot N_{K/\mathbb{Q}}(\alpha\beta\gamma)|^{c_{24}(d)},$$

where $c_{23}(d)$, $c_{24}(d)$ depend only on d.

This obviously follows from Masser's uniform abc-conjecture over number fields, i.e. Conjecture 4.12, but is of course much weaker.

Conjecture 4.18 $\Longrightarrow$ Conjecture 4.15 (sketch). We follow the argument in Subsection 4.6, and use the same notation. Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 4$ and discriminant $D \neq 0$. Denote by G the splitting field of f. By e.g., Evertse and Győry (2017, Corollary 13.3.4), there is $a \in \mathbb{Q}$ with $1 \leq |a| \leq c_{25}(n)|D_G|^{c_{26}(n)}$ such that $f_1 := af = \prod_{i=1}^{n}(\alpha_i X - \beta_i)$ with $\alpha_i, \beta_i \in \mathcal{O}_G$ for $i = 1, \ldots, n$, and such that the non-real factors among the $\alpha_i X - \beta_i Y$ can be divided into complex conjugate pairs. Let $D_1 := D(f_1)$. Now define $\Delta_{ij} := \alpha_i\beta_j - \alpha_j\beta_i$ $(1 \leq i < j \leq n)$ and apply Conjecture 4.18 to the identities

$$\Delta_{ij}\Delta_{kl} + \Delta_{jk}\Delta_{il} = \Delta_{ik}\Delta_{jl}.$$

Noting that $|N_{G/\mathbb{Q}}(\Delta_{ij})| \leq |D_1|^{n!}$, it follows that for all quadruples i, j, k, l,

$$H_G(\Delta_{ij}\Delta_{kl}, \Delta_{jk}\Delta_{il}, \Delta_{ik}\Delta_{jl}) \leq c_{27}(n)|D_G \cdot D_1|^{c_{28}(n)}.$$

This leads to upper bounds for the quantities $|\Delta_{ij}\Delta_{kl}/\Delta_{ik}\Delta_{jl}|$. Following the arguments in part 3 of Subsection 4.6, applying Proposition 4.13, one obtains that f_1 is $GL_2(\mathbb{Z})$-equivalent to a polynomial g_1 with

$$H(g_1) \leq c_{29}(n)|D_G \cdot D_1|^{c_{30}(n)}.$$

One can show that D_G divides $D_1^{c_{31}(n)}$. Taking $g := a^{-1}g_1$ one obtains that g is $GL_2(\mathbb{Z})$-equivalent to f and that $H(g) \leq c_{18}(n)|D|^{c_{19}(n)}$. □

We are interested in upper bounds for $H(g)$ that depend as much as possible on D_G and the radical of $D = D(f)$, and as little as possible on D itself. Under assumption of Conjecture 4.12 (Masser's version of the abc-conjecture over number fields), we deduce the following result for monic polynomials. In fact, it is a modification of some ideas of Rafael von Känel, which he kindly

shared with us. Recall that the radical of a non-zero rational integer a is defined by $\mathcal{R}(a) := \prod_{p|a} p$.

Theorem 4.19. *Under assumption of Conjecture 4.12, the following holds. Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 3$ and of discriminant $D \neq 0$. Let G be the splitting field of f and D_G its discriminant. Then f is $\mathbb{Z}$-equivalent to a monic polynomial $g \in \mathbb{Z}[X]$ such that*

$$H(g) \leq c_{32}(n)\big(|D_G \cdot \mathcal{R}(D)|\big)^{c_{33}(n)} \cdot |D|^{1/(n-1)},$$

where $c_{32}(n)$, $c_{33}(n)$ depend only on n.

Remark. With a more elaborate computation, $c_{33}(n)$ can be computed explicitly.

Proof. We use the following notation: we write $A \ll^* B$ if there are positive numbers $c'(n)$, $c''(n)$, depending only on n, such that $A \leq c'(n)|D_G \cdot \mathcal{R}(D)|^{c''(n)} B$. At each occurrence of $\ll^*$, the constants $c'(n), c''(n)$ may be different.

Write $f(X) = (X-\alpha_1)\cdots(X-\alpha_n)$. Choose a rational integer a such that $|a - (\alpha_1 + \cdots + \alpha_n)/n| \leq \frac{1}{2}$, and take $g(X) := f(X+a)$. This g is clearly $\mathbb{Z}$-equivalent to a. Then

$$H(g) \leq 2^n \prod_{i=1}^{n} \max(1, |\alpha_i - a|) \leq 2^n \prod_{i=1}^{n} \max(1, \tfrac{1}{2} + |\alpha_i - (\alpha_1 + \cdots + \alpha_n)/n|),$$

hence

$$H(g) \leq 2^n \prod_{i=1}^{n} \big(1 + n^{-1} \sum_{j=1}^{n} |\alpha_i - \alpha_j|\big). \tag{4.13}$$

We prove Theorem 4.17 by estimating the right-hand side from above, and to this end we apply Conjecture 4.12 to the identities

$$(\alpha_i - \alpha_j) + (\alpha_j - \alpha_k) = (\alpha_i - \alpha_k) \quad (i,j,k \in \{1,\ldots,n\} \text{ pairwise distinct}).$$

Note that all terms in this sum are algebraic integers in G, composed of prime ideals in $\mathcal{O}_G$ dividing D. So by Conjecture 4.12,

$$H_G\Big(1, \frac{\alpha_i - \alpha_j}{\alpha_i - \alpha_k}\Big) \leq H_G(\alpha_i - \alpha_j, \alpha_j - \alpha_k, \alpha_i - \alpha_k) \ll^* 1.$$

This implies

$$\Big|\frac{\alpha_i - \alpha_j}{\alpha_i - \alpha_k}\Big| \ll^* 1 \text{ for all pairwise distinct } i,j,k$$

and subsequently, using $\frac{\alpha_i-\alpha_j}{\alpha_k-\alpha_l} = -\frac{\alpha_i-\alpha_j}{\alpha_i-\alpha_k} \cdot \frac{\alpha_k-\alpha_i}{\alpha_k-\alpha_l}$,

$$\left|\frac{\alpha_i-\alpha_j}{\alpha_k-\alpha_l}\right| \ll^* 1 \quad \text{for all pairwise distinct } i,j,k,l.$$

This leads us to

$$|\alpha_i-\alpha_j| \ll^* \Big(\prod_{1\le k\ne l\le n} |\alpha_k-\alpha_l|\Big)^{1/(n(n-1))} = |D|^{1/n(n-1)} \quad \text{for all } i\ne j.$$

By inserting this into (4.13), we arrive at $H(g) \ll^* |D|^{1/(n-1)}$. This completes our proof. □

Rafael von Känel kindly communicated to us a conjecture on monic cubic polynomials of given discriminant that is equivalent to the Masser-Oesterlé abc-conjecture over $\mathbb{Q}$, i.e., Conjecture 4.11. To formulate von Känel's conjecture, we introduce the weighted height of $f = X^3+a_1X^2+a_2X+a_3 \in \mathbb{Z}[X]$ by

$$\mathrm{Ht}(f) := \max(|a_1|, |a_2|^{1/2}, |a_3|^{1/3}).$$

Further, we introduce the quantity

$$\delta_f := \max\{d\in\mathbb{Z}:\ d^2|P \text{ and } d^3|U\}, \quad \text{where } P := a_1^2-3a_2,\ U := 2a_1^3+27a_3-9a_1a_2. \tag{4.14}$$

Here P and U are the usual two seminvariants of f, which satisfy $4P^3-U^2 = 27D$, where $D = D(f)$. Note that δ_f^6 divides $27D$.

Conjecture 4.20 (von Känel)**.** *There is a constant $c_{34}(\epsilon) > 0$ depending on ϵ, such that for every real $\epsilon > 0$ the following holds:*
For every monic cubic polynomial $f \in \mathbb{Z}[X]$ of discriminant $D \ne 0$, there is a polynomial $g \in \mathbb{Z}[X]$ that is $\mathbb{Z}$-equivalent to f and for which

$$\mathrm{Ht}(g) \le c_{34}(\epsilon)\cdot\delta_f\cdot\mathcal{R}(27D/\delta_f^6)^{1+\epsilon}.$$

Theorem 4.21 (von Känel)**.** *The Masser-Oesterlé abc-conjecture over $\mathbb{Q}$ is equivalent to Conjecture 4.20.*

Remark. It might be possible to extend the proof to prove a version for any number field K without introducing substantial new ideas. However it will be clear that the proof does not work for polynomials of degree ≥ 4.

Observing that $\delta_f\cdot\mathcal{R}(27D/\delta_f^6)$ divides $27D$, this implies at once the following:

Corollary 4.22. *Assume the Masser-Oesterlé abc-conjecture over $\mathbb{Q}$ holds. Then there is a constant $c_{35}(\epsilon) > 0$ depending on ϵ, such that for every real $\epsilon > 0$ the following holds:*
For every monic cubic polynomial $f \in \mathbb{Z}[X]$ of discriminant $D \neq 0$, there is a polynomial $g \in \mathbb{Z}[X]$ that is $\mathbb{Z}$-equivalent to f and for which

$$\mathrm{Ht}(g) \leq c_{35}(\epsilon) \cdot |D|^{1+\epsilon}.$$

Noting that $H(g) \leq \mathrm{Ht}(g)^3$, Corollary 4.22 immediately implies a version of Conjecture 4.14.

Proof of Theorem 4.21. We follow von Känel's argument.

It is known (see Bombieri-Gubler (2005, 12.5.12)) that the Masser-Oesterlé abc-conjecture over $\mathbb{Q}$ is equivalent to the following

Conjecture 4.23. *For every real $\epsilon > 0$ there is a constant $c_{36}(\epsilon)$ such that all $u, v \in \mathbb{Z}$ with $w := u^3 - v^2 \neq 0$ and $\gcd(u^3, v^2)$ sixth power-free satisfy*

$$|u| \leq c_{36}(\epsilon) \cdot \mathcal{R}(w)^{2+\epsilon}, \quad |v| \leq c_{36}(\epsilon) \cdot \mathcal{R}(w)^{3+\epsilon}.$$

Therefore it suffices to show that Conjecture 4.20 is equivalent to Conjecture 4.23. This equivalence is a consequence of Lemmas 4.24 and 4.25 that are proved below. □

In what follows we write $A \ll_\epsilon B$ if there is a constant $c(\epsilon) > 0$ depending only on ϵ such that $A \leq c(\epsilon)B$.

Lemma 4.24. *Conjecture 4.23 implies Conjecture 4.20.*

Proof. We assume that Conjecture 4.23 holds and we let $\epsilon > 0$ be a real number.

Let $f \in \mathbb{Z}[X]$ be a cubic monic polynomial of discriminant $D \neq 0$. Write $f = X^3 + a_1X^2 + a_2X + a_3$ with $a_i \in \mathbb{Z}$, and let $\delta = \delta_f$, P, U be as in (4.14). We compute

$$f(X - \tfrac{a_1}{3}) = X^3 + b_2X + b_3, \quad b_2 = -\tfrac{P}{3}, \quad b_3 = \tfrac{U}{27}, \quad 4P^3 - U^2 = 27D. \tag{4.15}$$

The definition of δ assures that $P_0 = P/\delta^2$ and $U_0 = U/\delta^3$ lie in $\mathbb{Z}$ with $\gcd(P_0^3, U_0^2)$ sixth power-free. Moreover, it follows from (4.15) that P_0 and U_0 satisfy

$$(4P_0)^3 - (4U_0)^2 = 16 \cdot 27(D/\delta^6).$$

Next we define $\rho := \max\{d \in \mathbb{Z} : \ d^2 \mid 4P_0 \text{ and } d^3 \mid 4U_0\}$. Then we observe that $u = 4P_0/\rho^2$ and $v = 4U_0/\rho^3$ lie in $\mathbb{Z}$ with $\gcd(u^3, v^2)$ sixth power-free, and we obtain

$$u^3 - v^2 = w, \quad w = \tfrac{16\cdot 27}{\rho^6}(D/\delta^6) \neq 0.$$

Here we used our assumption that $D \neq 0$. It holds that $\mathcal{R}(w) \leq 6\cdot\mathcal{R}(27D/\delta^6)$ since $\rho \in \mathbb{Z}$ and then an application of Conjecture 4.23 with u, v leads to

$$\max(|u|^3, |v|^2) \ll_\epsilon \mathcal{R}(w)^{6+\epsilon} \ll_\epsilon \mathcal{R}(27D/\delta^6)^{6+\epsilon}. \tag{4.16}$$

As $\gcd(P_0^3, U_0^2)$ is sixth power-free, the definition of ρ implies $\rho \mid 2$. Then, on combining (4.16) with the definitions of b_2, b_3 and u, v, we deduce

$$\max(|b_2|^{1/2}, |b_3|^{1/3}) \leq \delta \cdot \max(|u|^{1/2}, |v|^{1/3}) \ll_\epsilon \delta \cdot \mathcal{R}(27D/\delta^6)^{1+\epsilon}. \tag{4.17}$$

In the case when $-a_1/3 \in \mathbb{Z}$, we can take $g = f(X + \tau) \in \mathbb{Z}[X]$ for $\tau = -a_1/3 \in \mathbb{Z}$. Indeed $\mathrm{Ht}(g) = \max(|b_2|^{1/2}, |b_3|^{1/3})$ by (4.15) and thus (4.17) gives $\mathrm{Ht}(g) \ll_\epsilon \delta \cdot \mathcal{R}(27D/\delta^6)^{1+\epsilon}$.

Suppose from now on that $-a_1/3 \notin \mathbb{Z}$. Then we may and do choose $\sigma \in \{\frac{1}{3}, \frac{2}{3}\}$ such that $\tau' = -\frac{a_1}{3} + \sigma \in \mathbb{Z}$. Define $g = f(X + \tau')$ and write $g = X^3 + c_1X^2 + c_2X + c_3$ with $c_i \in \mathbb{Z}$. On using that $g = f((X + \sigma) - \frac{a_1}{3}) = (X + \sigma)^3 + b_2(X + \sigma) + b_3$, we obtain the identities

$$c_1 = 3\sigma, \quad c_2 = 3\sigma^2 + b_2, \quad c_3 = \sigma^3 + b_2\sigma + b_3.$$

The definition of σ gives $|\sigma| \leq 2/3$, and our assumption $D \neq 0$ assures that not both b_2, b_3 are zero. Hence we deduce $\mathrm{Ht}(g) \ll_\epsilon \max(|b_2|^{1/2}, |b_3|^{1/3})$ which together with (4.17) implies $\mathrm{Ht}(g) \ll_\epsilon \delta \cdot \mathcal{R}(27D/\delta^6)^{1+\epsilon}$ as desired. This completes the proof of Lemma 4.24. □

Lemma 4.25. *Conjecture 4.20 implies Conjecture 4.23.*

Proof. We assume that Conjecture 4.20 holds and we let $\epsilon > 0$ be a real number.

Let $u, v \in \mathbb{Z}$ with $\gcd(u^3, v^2)$ sixth power-free and $w = u^3 - v^2 \neq 0$. We consider the monic cubic $f = X^3 + a_2X + a_3$ in $\mathbb{Z}[X]$ where $a_2 = -3u$ and $a_3 = 2v$. A direct computation shows that the discriminant D of f and the seminvariants P, U of f are given by

$$D = 4 \cdot 27w, \quad P = 9u, \quad U = 2 \cdot 27v.$$

It follows that $D \neq 0$, since $w \neq 0$ by assumption. Moreover our assumption that $\gcd(u^3, v^2)$ is sixth power-free implies that the quantity δ in (4.14)

satisfies $\delta \mid 6$. Then an application of Conjecture 4.20 with f gives that there is $\tau \in \mathbb{Z}$ such that $g = f(X+\tau)$ satisfies

$$\mathrm{Ht}(g) = \max_i |c_i|^{1/i} \ll_\epsilon \mathcal{R}(D)^{1+\epsilon} \tag{4.18}$$

where $g = X^3 + c_1X^2 + c_2X + c_3$ and $c_i \in \mathbb{Z}$. As $f = X^3 + 0 \cdot X^2 - 3uX + 2v$ we obtain that $c_1 = 3\tau$ and thus $g(X - \frac{c_1}{3}) = f$. This leads to the following identities

$$-3u = a_2 = -\tfrac{c_1^2}{3} + c_2, \quad 2v = a_3 = \tfrac{2}{27}c_1^3 - \tfrac{c_1c_2}{3} + c_3.$$

Thus (4.18) combined with $D = 4 \cdot 27w$ implies $|u| \ll_\epsilon \mathcal{R}(w)^{2+\epsilon}$ and $|v| \ll_\epsilon \mathcal{R}(w)^{3+\epsilon}$ as desired. This completes the proof of Lemma 4.25. □

We finish this subsection by recalling a function field analogue of Conjecture 4.15 that has been proved unconditionally. Let $\Bbbk$ be an algebraically closed field of characteristic 0. Define the polynomial ring $A := \Bbbk[t]$ and its quotient field $L := \Bbbk(t)$.

Define an absolute value $|\cdot|_\infty$ on L as follows: if $a, b \in A$ are two non-zero polynomials, then put $|a/b|_\infty := \exp(\deg a - \deg b)$. Further, define the height of $f(X) := a_0X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$ by $H(f) := \max(|a_0|_\infty, \ldots, |a_n|_\infty)$. Call two polynomials $f, g \in A[X]$ of degree n $GL_2(A)$-equivalent, if $g(X) = u(cX+d)^n f(\frac{aX+b}{cX+d})$ for some $u \in \Bbbk^*$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(A)$.

In his PhD-thesis, Zhuang (2015, Chap. 5, Theorem 5.3.2) proved the following result (in fact, Zhuang formulated this in terms of binary forms $F \in A[X,Y]$; using the correspondence $f(X) = F(X,1)$ one obtains the theorems below).

Theorem 4.26. *Let $f \in A[X]$ be a polynomial of degree $n \geq 3$ and discriminant $D \neq 0$. Assume that f has splitting field G over L, and denote by g_G the genus of G. Then f is $GL_2(A)$-equivalent to a polynomial g for which*

$$H(g) \leq \exp\left(n^2 + 6n - 7 + \frac{(5n-5)(2g_G-1)}{24[G:K]}\right) \cdot |D|_\infty^{21/n}.$$

By estimating g_G from above in terms of n and $|D(f)|_\infty$, Zhuang (2015, Chap. 5, Main Theorem) obtained the following, unconditional, function field analogue of Conjecture 4.15:

Theorem 4.27. *Let $f \in A[X]$ be a polynomial of degree $n \geq 3$ and discriminant $D \neq 0$. Then f is $GL_2(A)$-equivalent to a polynomial g for which*

$$H(g) \leq \exp\big((n-1)(n+6)\big) \cdot |D|_\infty^{20+(1/n)}.$$

The proof of Theorem 4.26 is similar to that of Theorem 4.16, except that instead of Theorem 4.17 Zhuang used the Stothers-Mason abc-Theorem for function fields.

We recall this theorem. Let K be a function field of transcendence degree 1 over an algebraically closed field $\Bbbk$ of characteristic 0. Let M_K be the set of normalized discrete valuations on K, i.e., with value group $\mathbb{Z}$. These valuations satisfy the sum formula $\sum_{v \in M_K} v(x) = 0$ for $x \in K^*$. Denote by g_K the genus of K. Define the height of a tuple $(\gamma_1, \ldots, \gamma_n) \in K^n$ by $h_K(\gamma_1, \ldots, \gamma_n) := -\sum_{v \in M_K} \min(v(\gamma_1), \ldots, v(\gamma_n))$.

Theorem 4.28. *Let α, β, γ be elements of $K \setminus \Bbbk$ such that $\alpha + \beta = \gamma$. Let s denote the number of valuations v of K such that $v(\alpha)$, $v(\beta)$, $v(\gamma)$ are not all equal. Then*

$$h_K(\alpha, \beta, \gamma) \leq s + 2g_K - 2.$$

For a proof, see Mason (1984).

5. Consequences in algebraic number theory, in particular for monogenicity and rational monogenicity

We give some consequences of Theorems 4.1, 4.2 and 4.4 in algebraic number theory. Of particular interest are applications to monogenicity of number fields and (rational) monogenicity of orders.

Theorem 4.1 due to Birch and Merriman from 1972 has an important ineffective finiteness consequence for algebraic integers of given discriminant; see Theorem 5.1 below.

An effective version of Theorem 5.1 was obtained independently in Győry (1973), as a consequence of his effective Theorem 4.2 presented above; see Theorem 5.2 below.

Theorem 5.2 as well as its various effective consequences, applications, quantitative variants and generalizations in Győry (1973, 1974, 1976, 1978a,b, 1980a,b, 1981) led to breakthroughs in the effective theory of number fields. These furnished among others general effective finiteness results for integral elements of given discriminant resp. of given index in number fields and, more generally, in their orders; see Corollaries 5.3 and 5.4. In particular, as

an immediate consequence of his Theorem 5.2, Győry provided the *first general effective algorithm* for deciding the *monogenicity* and for determining, at least in principle, *all power integral bases* in number fields and in their orders; see Theorems 5.5 and 5.6 below.

As a consequence of Theorem 4.4 we present from Evertse and Győry (1991a) a general effective finiteness theorem on algebraic numbers of given discriminant; see Theorem 5.10. Finally, we introduce rationally monogenic orders, which are generalizations of monogenic orders, and give an algorithm to determine in principle whether a given order is rationally monogenic, see Theorems 5.14 and 5.15 below.

For convenience, we formulate the above-mentioned effective finiteness results in their simplest form. For generalizations, further applications and comprehensive treatment of this extensive area, we refer to Győry (1983, 1984, 1998, 2000, 2006), Evertse and Győry (1991a, 2017, 2022), BEGyRS (2023), the references given there, and to Sections 6–9 of the present paper.

5.1. **Preliminaries.**

Throughout this section, K will denote a number field of degree $n \geq 2$ with ring of integers $\mathcal{O}_K$ and discriminant D_K. Recall that K has precisely n distinct embeddings in its normal closure over $\mathbb{Q}$, which we denote by $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$. Here $x^{(1)} = x$.

Let $\mathcal{M}$ be a free $\mathbb{Z}$-module in K of rank n, and pick a $\mathbb{Z}$-module basis $\{\omega_1, \ldots, \omega_n\}$ of $\mathcal{M}$. Then the discriminant of $\mathcal{M}$ is defined by

$$D(\mathcal{M}) := \left(\det \left(\omega_i^{(j)} \right)_{i,j=1}^{n} \right)^2.$$

This is a non-zero rational number, and it does not depend on the choice of the basis. If $\mathcal{M} \subseteq \mathcal{O}_K$, then $D(\mathcal{M})$ is a non-zero integer. In particular, $D(\mathcal{O}_K) = D_K$ is the discriminant of K.

Given two free $\mathbb{Z}$-modules $\mathcal{M}_1, \mathcal{M}_2$ in K of rank n with $\mathcal{M}_1 \supseteq \mathcal{M}_2$, denote by $[\mathcal{M}_1 : \mathcal{M}_2]$ the *index* of $\mathcal{M}_2$ in $\mathcal{M}_1$, i.e., the cardinality of $\mathcal{M}_1/\mathcal{M}_2$. Then for any two $\mathbb{Z}$-module bases $\{\omega_1, \ldots, \omega_n\}$ of $\mathcal{M}_1$ and $\{\theta_1, \ldots, \theta_n\}$ of $\mathcal{M}_2$ we have

$$[\mathcal{M}_1 : \mathcal{M}_2] = \left| \det \left(a_{ij} \right)_{i,j=1,\ldots,n} \right|, \tag{5.1}$$

$$\text{with } a_{ij} \in \mathbb{Z} \text{ given by } \theta_i = \sum_{j=1}^{n} a_{ij} \omega_j \text{ for } i = 1, \ldots, n.$$

By taking conjugates, and applying the product rule for determinants, it follows that

$$D(\mathcal{M}_2) = [\mathcal{M}_1 : \mathcal{M}_2]^2 D(\mathcal{M}_1). \tag{5.2}$$

Let α be a non-zero algebraic integer. Then we denote by $f_\alpha(X)$ the minimal (monic) polynomial of α in $\mathbb{Z}[X]$. Thus, $f_\alpha(X) = \prod_{i=1}^n (X - \alpha^{(i)})$. We now define the *discriminant* of α by

$$D(\alpha) := D(f_\alpha) = \prod_{1 \le i < j \le n} (\alpha^{(i)} - \alpha^{(j)})^2. \tag{5.3}$$

We recall that an *order* of K is a subring of K which as a $\mathbb{Z}$-module is free of rank n. The maximal order of K, containing all other orders, is its ring of integers $\mathcal{O}_K$.

Let $\alpha \in \mathcal{O}_K$ be a primitive element of K. The ring $\mathbb{Z}[\alpha]$ is clearly an order of K, with $\mathbb{Z}$-module basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$, and by Vandermonde's identity,

$$D(\alpha) = D(\mathbb{Z}[\alpha]). \tag{5.4}$$

Let now $\mathcal{O}$ be an order of K, and $D(\mathcal{O})$ its discriminant. For a primitive element α of K with $\alpha \in \mathcal{O}_K$ resp. $\alpha \in \mathcal{O}$, we define

$$I(\alpha) := [\mathcal{O}_K : \mathbb{Z}[\alpha]], \quad I_{\mathcal{O}}(\alpha) := [\mathcal{O} : \mathbb{Z}[\alpha]] \tag{5.5}$$

to be the *index* of α in $\mathcal{O}_K$ resp. in $\mathcal{O}$. Then, by (5.2), (5.4),

$$D(\alpha) = I(\alpha)^2 D_K \text{ for } \alpha \in \mathcal{O}_K, \quad D(\alpha) = I_{\mathcal{O}}(\alpha)^2 D(\mathcal{O}) \text{ for } \alpha \in \mathcal{O}. \tag{5.6}$$

Two algebraic integers α, β are called $\mathbb{Z}$-*equivalent* if $\beta = \pm\alpha + a$ for some $a \in \mathbb{Z}$. If α and β are $\mathbb{Z}$-equivalent then so are f_α and f_β. Conversely, if f_α and f_β are $\mathbb{Z}$-equivalent then α is $\mathbb{Z}$-equivalent to a conjugate of β.

Clearly, $\mathbb{Z}$-equivalent elements in $\mathcal{O}_K$ resp. in $\mathcal{O}$ have the same discriminant and hence the same index in $\mathcal{O}_K$ resp. in $\mathcal{O}$.

A number field K is called *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. This is equivalent to the fact that $I(\alpha) = 1$ and that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a *power integral basis* in K, i.e., a $\mathbb{Z}$-module basis of $\mathcal{O}_K$. Similarly, an order $\mathcal{O}$ of K is said to be *monogenic* if $\mathcal{O} = \mathbb{Z}[\alpha]$, i.e. if $I_{\mathcal{O}}(\alpha) = 1$ for some $\alpha \in \mathcal{O}$. Clearly, if $\mathcal{O} = \mathbb{Z}[\alpha]$ then also $\mathcal{O} = \mathbb{Z}[\beta]$ for every β that is $\mathbb{Z}$-equivalent to α.

Further, K resp. $\mathcal{O}$ is called $k\,(\ge 1)$ *times monogenic* if $\mathcal{O}_K$ resp. $\mathcal{O}$ equals $\mathbb{Z}[\alpha_1] = \cdots = \mathbb{Z}[\alpha_k]$ for some pairwise $\mathbb{Z}$-inequivalent $\alpha_1, \ldots, \alpha_k$ in $\mathcal{O}_K$ resp. in $\mathcal{O}$. In case that in the above definition k is maximal, it is called the *multiplicity* of the monogenicity of K, resp. of $\mathcal{O}$.

5.2. **Consequences of Theorems 4.1 and 4.2 for algebraic integers of given discriminant.**
From their Theorem 4.1, Birch and Merriman in 1972 deduced the following ineffective finiteness theorem.

Theorem 5.1 (Birch and Merriman, 1972)**.** *Up to $\mathbb{Z}$-equivalence, there are only finitely many algebraic integers with given non-zero discriminant.*

Independently, as a consequence of his Theorem 4.2, Győry (1973) proved the following effective version of Theorem 5.1.

By the *height* $H(\alpha)$ of an algebraic integer α we mean the height $H(f_\alpha)$.

Theorem 5.2 (Győry, 1973)**.** *Let α be an algebraic integer of degree $n \geq 2$ and discriminant $D \neq 0$. Then*

(i) $n \leq c_1(|D|)$, and
(ii) There is an algebraic integer β, $\mathbb{Z}$-equivalent to α such that

$$H(\beta) \leq c_2(n, |D|),$$

where c_1, c_2 denote the same effectively computable positive numbers as in Theorem 4.2.

This theorem was stated and proved in Győry (1973) as 'Corollaire 3' of the 'Théorème', cf. Theorem 4.2 above.

As was mentioned in Section 2, the cubic case was settled independently by Delone (1930) and Nagell (1930), and the quartic case by Nagell (1967) in an ineffective way.

Theorems 5.1 resp. 5.2 confirmed in full generality, and in fact Theorem 5.2 in an effective form, a conjecture of Nagell (1967). Further both Theorem 5.1 and Theorem 5.2 imply, Theorem 5.2 in an effective form, that there are only finitely many algebraic units in $\overline{\mathbb{Q}}$ of given discriminant. This gave the effective solution to Problem 19 in the book Narkiewicz (1974).

Finally, we note that Theorem 5.2 easily follows from Theorem 4.2. Indeed, if α is an algebraic integer with the properties specified in Theorem 5.2, then by (5.3), $D(f_\alpha) = D$ and $\deg f_\alpha = n$. Further, by Theorem 4.2 f_α is $\mathbb{Z}$-equivalent to some monic $g \in \mathbb{Z}[X]$ of degree n and discriminant D such that $n \leq c_1(|D|)$ and $H(g) \leq c_2(n, |D|)$, where c_1, c_2 denote the effectively computable numbers occurring in Theorem 4.2. But then α is $\mathbb{Z}$-equivalent to a zero of g, say β, whence $\deg \beta \leq c_1(|D|)$ and $H(\beta) \leq c_2(n, |D|)$ follow. $\square$

The first explicit version of (ii) in Theorem 5.2 was established by Győry (1974) by means of Baker's method. For $c_1(|D|)$ one can take $2\log|D|/\log 3$. For $c_2(n,|D|)$ we can obtain an explicit bound, using Theorem 4.2* instead of Theorem 4.2. An even better explicit estimate can be obtained in (ii), observing that in fact we apply Theorem 4.2 (or its explicit version Theorem 4.2*) only to irreducible polynomials f_α. The best known bound in (ii) comes from Theorem 6.4.1 of Evertse and Győry (2017).

5.3. **Consequences for monogenic number fields and orders.** Let again K be a number field of degree $n \geq 2$ with ring of integers $\mathcal{O}_K$ and discriminant D_K.

The following effective corollaries are immediate consequences of Theorem 5.2 (i.e. the 'Corollaire 3') of Győry (1973). Although this was not mentioned by Birch and Merriman in their 1972 paper, it should be remarked that from their Theorem 5.1 one can also deduce in ineffective form the finiteness consequences of the results below.

Corollary 5.3 (of Theorem 5.2)**.** *Let $\mathcal{O}$ be an order of K and D a non-zero integer. Every $\alpha \in \mathcal{O}$ of discriminant $D_{K/\mathbb{Q}}(\alpha) = D$ is $\mathbb{Z}$-equivalent to some $\beta \in \mathcal{O}$ such that*

$$H(\beta) \leq c_2(n,|D|),$$

where $c_2 = c_2(n,|D|)$ denotes the same effectively computable positive number as in Theorem 5.2.

This is a special case of Theorem 5.2, restricted to the elements of $\mathcal{O}$. It follows from Corollary 5.3 that up to $\mathbb{Z}$-equivalence, there are only finitely many elements of $\mathcal{O}$ of given non-zero discriminant, and all of them can be, at least in principle, effectively determined.

As was mentioned above, the first quantitative versions of Theorem 5.2 and Corollary 5.3 were established in Győry (1974).

Corollary 5.4 (of Theorem 5.2)**.** *Let $\mathcal{O}$ be an order in K of discriminant $D(\mathcal{O})$, and $I_\mathcal{O}$ a positive integer. Every α in $\mathcal{O}$ with index $I_\mathcal{O}(\alpha) = I_\mathcal{O}$ is $\mathbb{Z}$-equivalent to some $\beta \in \mathcal{O}$ such that*

$$H(\beta) \leq c_2(n, I_\mathcal{O}^2 \cdot |D(\mathcal{O})|),$$

where c_2 denotes the same effectively computable positive number as in Theorem 5.2 with $|D|$ replaced by $I_\mathcal{O}^2 \cdot |D(\mathcal{O})|$.

This follows immediately from Corollary 5.3 and the second identity in (5.6). Corollary 5.4 implies that up to $\mathbb{Z}$-equivalence there are only finitely many elements in $\mathcal{O}$ with given index and all of them can be, at least in principle, effectively determined.

The next Theorem 5.5 and its more general version Theorem 5.6 are the most influential consequences of Theorem 5.2. They provided the first general effective algorithm for deciding the monogenicity, the multiplicity of monogenicity, and for determining, at least in principle, all power integral bases in K and in its orders.

Of particular importance are the cases when in Corollaries 5.3, and 5.4 $\mathcal{O}$ is just $\mathcal{O}_K$, the ring of integers of K. Then Corollary 5.4 implies

Theorem 5.5 (Győry, 1976). *Every $\alpha \in \mathcal{O}_K$ with $\mathcal{O}_K = \mathbb{Z}[\alpha]$ is $\mathbb{Z}$-equivalent to some $\beta \in \mathcal{O}_K$ such that*

$$H(\beta) \leq c_2(n, |D_K|),$$

where c_2 denotes the same effectively computable positive number as in Corollary 5.4 with $I_{\mathcal{O}} = 1$, $D(\mathcal{O}) = D_K$. Consequently, there are only finitely many $\mathbb{Z}$-equivalence classes of α in $\mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, and a full set of representatives of these classes can be, at least in principle, effectively found.

More generally, Corollary 5.4 immediately gives the following:

Theorem 5.6 (Győry, 1976). *Let $\mathcal{O}$ be an order of K of discriminant $D(\mathcal{O})$. Every $\alpha \in \mathcal{O}$ with $\mathcal{O} = \mathbb{Z}[\alpha]$ is $\mathbb{Z}$-equivalent to some $\beta \in \mathcal{O}$ such that*

$$H(\beta) \leq c_2(n, |D(\mathcal{O})|),$$

where c_2 denotes the same effectively computable positive number as in Corollary 5.4 with $I_{\mathcal{O}} = 1$.

The first explicit, quantitative versions of Corollary 5.4 and Theorems 5.5 and 5.6 were given in Győry (1976).

Remark. With the above formulation of Corollaries 5.3, 5.4 and Theorem 5.6 it was easier to point out that these are indeed consequences of Theorems 4.2 and 5.2. Further, we note that their explicit versions can be easily derived from the explicit variant Theorem 4.2* of Theorem 4.2. Finally, the corollaries can be deduced with better bounds from less general versions of Theorem 4.2, where the polynomials f involved are irreducible; for such versions we refer to Győry (1976, 1998, 2000), Evertse and Győry (2017) and in fact Corollary 5.3 above.

5.4. **Reformulation of Corollaries 5.3, 5.4 and Theorem 5.6 in terms of polynomial Diophantine equations over $\mathbb{Z}$.**
Let K be an algebraic number field of degree $n \geq 2$ with ring of integers $\mathcal{O}_K$ and discriminant D_K. Denote by $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings of K in $\mathbb{C}$. Consider Corollaries 5.3, 5.4 and Theorem 5.6. Let $\mathcal{O}$ be an order of K, and $\{1, \omega_2, \ldots, \omega_n\}$ a $\mathbb{Z}$-module basis of $\mathcal{O}$. For $\alpha \in \mathcal{O}$ with

$$\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n, \quad x_1, x_2, \ldots, x_n \in \mathbb{Z},$$

its discriminant

$$D(\alpha) = D(x_2\omega_2 + \cdots + x_n\omega_n) = \prod_{1 \leq i < j \leq n} \Big(\sum_{k=2}^{n} x_k(\omega_k^{(i)} - \omega_k^{(j)}) \Big)^2$$

can be regarded as a decomposable form of degree $n(n-1)$ in $x_2, \ldots, x_n$ with coefficients in $\mathbb{Z}$, i.e., it is a product of $n(n-1)$ linear forms in $x_2, \ldots, x_n$ with algebraic coefficients. The form $D(x_2\omega_2 + \cdots + x_n\omega_n)$, which was introduced by Kronecker (1882), is called *discriminant form*, while, for $D \neq 0$, the equation

$$D(x_2\omega_2 + \cdots + x_n\omega_n) = D \text{ in } x_2, \ldots, x_n \in \mathbb{Z} \tag{5.7}$$

is called a *discriminant form equation.*

Clearly, Corollary 5.3 implies the following.

Corollary 5.7 (of Theorem 5.2)**.** *For given $D \neq 0$, the discriminant form equation* (5.7) *has only finitely many solutions and they can be effectively determined.*

We recall some facts about *index forms*, which were introduced by Hensel (1908). Let $\mathcal{O}$ be an order of K. Pick an *ordered* $\mathbb{Z}$-module basis $(1, \omega_2, \ldots, \omega_n)$ of $\mathcal{O}$. Set $\omega_1 := 1$. There are polynomials $f_{ij} \in \mathbb{Z}[X_2, \ldots, X_n]$ such that if $\alpha = x_2\omega_2 + \cdots + x_n\omega_n$ with $x_2, \ldots, x_n \in \mathbb{Z}$, then

$$\alpha^{i-1} = \sum_{j=1}^{n} f_{ij}(x_2, \ldots, x_n)\omega_j \quad \text{for } i = 1, \ldots, n.$$

Define the polynomial

$$I := \det\big(f_{ij}\big)_{i,j=1,\ldots,n} \in \mathbb{Z}[X_2, \ldots, X_n]. \tag{5.8}$$

Note that $I_{\mathcal{O}}(\alpha) = [\mathcal{O} : \mathbb{Z}[\alpha]]$ is invariant under $\mathbb{Z}$-equivalence. Thus, from (5.1) it follows that for $\alpha \in \mathcal{O}$,

$$I_{\mathcal{O}}(\alpha) = |I(x_2, \ldots, x_n)| \tag{5.9}$$

where $x_1, x_2, \ldots, x_n$ are the integers with $\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n$. In particular, if $(1, \omega_2, \ldots, \omega_n)$ is an ordered integral basis of K, i.e., an ordered $\mathbb{Z}$-module basis of $\mathcal{O}_K$, we have

$$I(\alpha) = |I(x_2, \ldots, x_n)|. \tag{5.10}$$

From (5.6) it follows that

$$D(x_2\omega_2 + \cdots + x_n\omega_n) = I(x_2, \ldots, x_n)^2 D(\mathcal{O}). \tag{5.11}$$

Since the left-hand side is a decomposable form of degree $n(n-1)$, the polynomial I is a decomposable form of degree $n(n-1)/2$. We call I the *index form associated with the ordered basis* $(1, \omega_2, \ldots, \omega_n)$ *of* $\mathcal{O}$ and, for given non-zero $I \in \mathbb{Z}$,

$$I(x_2, \ldots, x_n) = \pm I \quad \textit{in } x_2, \ldots, x_n \in \mathbb{Z} \tag{5.12}$$

an *index form equation.*

Identity (5.11) shows that if D, I are non-zero integers related by $D = I^2 D(\mathcal{O})$, then the equations (5.7) and (5.12) are equivalent. Consequently, the finiteness assertion of Corollary 5.4 is equivalent to the following.

Corollary 5.8 (of Theorem 5.2)**.** *For given $I \in \mathbb{Z} \setminus \{0\}$, the index form equation* (5.12) *has only finitely many solutions, and they can be effectively determined.*

In particular, for $I = 1$, we get the following consequence of Corollary 5.8, which we have included for reference purposes.

Corollary 5.9 (of Theorem 5.2)**.** *The index form equation*

$$I(x_2, \ldots, x_n) = \pm 1 \ \textit{in } x_2, \ldots, x_n \in \mathbb{Z} \tag{5.13}$$

has only finitely many solutions, and they can be effectively determined.

Corollaries 5.7, 5.8 and 5.9 were proved in Győry (1976) with explicit upper bounds for the solutions, see also Győry (2000) and Evertse and Győry (2017).

The best known upper bound for the solutions of (5.13) is

$$\max_{2 \le i \le n} |x_i| < \exp\{10^{n^2}(|D_K|(\log |D_K|)^n)^{n-1}\} \tag{5.14}$$

which is due to Evertse and Győry (2017). We note that a conjectural improvement of the upper bound, with a polynomial dependence on $|D_K|$, follows immediately from Conjecture 4.14.

5.5. **A consequence of Theorem 4.4 for algebraic numbers of given discriminant.**
Theorem 4.4 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.,

$$f_\alpha = a_0X^n + \cdots + a_n = a_0(X - \alpha^{(1)}) \cdots (X - \alpha^{(n)}) \in \mathbb{Z}[X] \tag{5.15}$$

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

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

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

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

One easily verifies that 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.

Consequently, if α, β are $GL_2(\mathbb{Z})$-equivalent, then $D(\alpha) = D(\beta)$. Now Theorem 4.4 implies at once:

Theorem 5.10 (Evertse and Győry, 1991a)**.** *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*

$$H(\beta) \leq c_3(n, |D|),$$

where c_3 denotes the same effectively computable positive number as in Theorem 4.4.

Further, by Théorème 1 of Győry (1974) we have

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

5.6. **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. We will formulate an analogue of Corollary 5.3 for rationally monogenic orders. While in the results for monogenic orders, $\mathbb{Z}$-equivalence of algebraic integers plays an important role, for rationally monogenic orders we have to

deal with $GL_2(\mathbb{Z})$-equivalence of algebraic numbers. Before we define rationally monogenic orders, we briefly go into some history and introduce the necessary terminology.

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 (5.15). 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), who observed that it is contained in the ring of integers of $\mathbb{Q}(\alpha)$, and that for its discriminant we have

$$D(\mathbb{Z}_\alpha) = D(f_\alpha) = D(\alpha). \tag{5.16}$$

Nakagawa (1989) showed that $\mathbb{Z}_\alpha$ is in fact an *order* of the field $\mathbb{Q}(\alpha)$, i.e., closed under multiplication. More precisely, he showed that

$$\omega_i\omega_j = -\sum_{\max(i+j-n,1)\leq k\leq i} a_{i+j-k}\omega_k + \sum_{j<k\leq\min(i+j,n)} a_{i+j-k}\omega_k \tag{5.17}$$
$$\text{for } i,j = 1,\ldots,n-1, \text{ where } \omega_n := -a_n.$$

This order was further studied by Simon (2001, 2003) and Del Corso, Dvornicich and Simon (2005). They showed that

$$\mathbb{Z}_\alpha = \mathbb{Z}[\alpha] \cap \mathbb{Z}[\alpha^{-1}]. \tag{5.18}$$

As was very likely known at the time, another description of $\mathbb{Z}_\alpha$ is as follows. Let $\mathcal{M}_\alpha$ be the $\mathbb{Z}$-module generated by $1, \alpha, \ldots, \alpha^{n-1}$. Then $\mathbb{Z}_\alpha$ is the *ring of coefficients* of $\mathcal{M}_\alpha$ (see Borevich and Shafarevich (1967), Section 2.2), i.e.,

$$\mathbb{Z}_\alpha = \{\xi \in \mathbb{Q}(\alpha) :\ \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}. \tag{5.19}$$

We have

$$\mathbb{Z}_\alpha = \mathbb{Z}[\alpha] \ \text{ if } \alpha \text{ is an algebraic integer.} \tag{5.20}$$

Indeed, if α is an algebraic integer of degree n, the powers α^i $(i \geq n)$ belong to $\mathcal{M}_\alpha$, and thus, $\mathbb{Z}_\alpha = \mathcal{M}_\alpha = \mathbb{Z}[\alpha]$. Further, for any two non-zero algebraic numbers α, β we have

$$\alpha,\ \beta\ GL_2(\mathbb{Z})\text{-equivalent} \implies \mathbb{Z}_\alpha = \mathbb{Z}_\beta. \tag{5.21}$$

Indeed, let $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$. Then $\mathcal{M}_\beta = (c\alpha + d)^{1-n}\mathcal{M}_\alpha$ where $n = \deg\alpha$, and thus, $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$.

We call an order $\mathcal{O}$ of a number field K *rationally monogenic* if there is α such that $\mathcal{O} = \mathbb{Z}_\alpha$. From (5.20) it follows that monogenic orders are rationally monogenic. Below we explain that rationally monogenic orders are in fact special cases of invariant orders of polynomials. In particular, $\mathbb{Z}_\alpha$ is the invariant order of f_α.

Recall that the index of an algebraic integer was defined in (5.5). Following Simon (2001), we generalize this to not necessarily integral algebraic numbers as follows. Given a non-zero algebraic number α, we define the index of α by

$$I(\alpha) := [\mathcal{O}_K : \mathbb{Z}_\alpha],$$

where $K = \mathbb{Q}(\alpha)$. In fact, this is the index of f_α as it was introduced by Simon. From (5.2) and (5.16) we deduce, analogously to the first identity of (5.6),

$$D(\alpha) = I(\alpha)^2 D_K. \tag{5.22}$$

For more results and properties of this index, we refer to Simon (2001).

There is a connection between rationally monogenic orders and Hermite equivalence classes of polynomials, which we explain here without proof. For a non-zero algebraic number α, let $\mathcal{I}_\alpha$ be the fractional ideal of $\mathbb{Z}_\alpha$ generated by 1 and α. This is known to be invertible, see Simon (2003). It is called also the *invariant ideal* of f_α.

Theorem 5.11 (BEGyRS, 2023)**.** *Let $f, g \in \mathbb{Z}[X]$ be two primitive, irreducible polynomials. Then the following three assertions are equivalent:*

(i) f and g are Hermite equivalent;

(ii) f has a root α and g a root β such that $\mathcal{M}_\beta = \lambda \mathcal{M}_\alpha$ for some non-zero $\lambda \in \mathbb{Q}(\alpha)$;

(iii) f has a root α and g a root β such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and $\mathcal{I}_\alpha$ and $\mathcal{I}_\beta$ lie in the same ideal class of $\mathbb{Z}_\alpha$.

In the particular case that f and g are monic, we have $\alpha \in \mathbb{Z}[\alpha] = \mathbb{Z}_\alpha$ and $\mathcal{I}_\alpha = \mathbb{Z}_\alpha$ and likewise for g and β. This leads to the following corollary.

Corollary 5.12 (BEGyRS, 2023)**.** *Let $f, g \in \mathbb{Z}[X]$ be two monic, irreducible polynomials. Then f and g are Hermite equivalent if and only if f has a root α and g a root β such that $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$.*

In BEGyRS (2023) an example of a quartic algebraic number field K was given such that $\mathcal{O}_K = \mathbb{Z}_\alpha = \mathbb{Z}_\beta$ for certain $\alpha, \beta \in K$, but f_α, f_β lie in

different Hermite equivalence classes. So far, we haven't been able to find similar examples for algebraic number fields of degree ≥ 5.

An order $\mathcal{O}$ of a number field K is called *primitive* if there are no integer $a > 1$ and order $\mathcal{O}'$ such that $\mathcal{O} = \mathbb{Z} + a\mathcal{O}'$. It is not difficult to show that a rationally monogenic order is primitive. It follows from work of Delone and Faddeev (1940) that every primitive order of a cubic number field is rationally monogenic. Simon (2001) gave various examples of number fields of degree ≥ 4 that are not rationally monogenic, i.e., whose rings of integers are not rationally monogenic.

In Evertse (2023) the following was shown:

Theorem 5.13. *Every number field K of degree ≥ 3 has infinitely many orders that are rationally monogenic but not monogenic.*

We finally arrive at the main result of this subsection, which follows directly from Theorem 5.10 and (5.16):

Theorem 5.14. *Let $\mathcal{O}$ be an order of 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 $H(\beta) \leq c_3(n, |D(\mathcal{O})|)$, where c_3 denotes the same effectively computable positive number as in Theorem 5.10.*

This implies

Theorem 5.15. *Let $\mathcal{O}$ be an order of a number field K. Then 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.

Idea of proof. Suppose K is effectively given in the form $\mathbb{Q}(\gamma)$, with an algebraic number γ of degree n. Thus, each element of K has a represention as a $\mathbb{Q}$-linear combinations of $1, \gamma, \ldots, \gamma^{n-1}$, and we can express all computations on K in terms of such representations.

Let the order $\mathcal{O}$ be given by a $\mathbb{Z}$-module basis $1, \theta_2, \ldots, \theta_n$ (with represention as described above). Using Theorem 5.10, one can effectively determine a full system of representatives for the $GL_2(\mathbb{Z})$-equivalence classes of those $\alpha \in K$ with $D(\alpha) = D(\mathcal{O})$. To check whether such a representative α satisfies $\mathbb{Z}_\alpha = \mathcal{O}$, one can proceed as follows. Verify that $\mathcal{O} \subseteq \mathbb{Z}_\alpha$ by checking $\theta_i \mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha$ for $i = 2, \ldots, n$. If so, we have in fact $\mathcal{O} = \mathbb{Z}_\alpha$ by (5.16). $\square$

The rationally monogenic orders introduced above are in fact special cases of *invariant orders* or *invariant rings* of binary forms, for which there is now a vast general theory. Although outside the scope of this paper, we give some background on these rings.

Let A be a commutative ring (with 1), and $a_0, \ldots, a_n \in A$. Then the *invariant ring* (order if $A = \mathbb{Z}$) associated with $(a_0, \ldots, a_n)$, or rather with the binary form $F(X, Y) = a_0X^n + \cdots + a_nY^n$ (but we allow here that $a_0 = 0$ or even $a_0 = \cdots = a_n = 0$) is given by the A-algebra A_F with A-module basis $1, \omega_2, \ldots, \omega_n$ satisfying the multiplication table (5.17). This is in fact a commutative, associative A-algebra. The name 'invariant ring' (invariant order if $A = \mathbb{Z}$) comes from the following invariance property: if F, G are two $GL_2(A)$-equivalent binary forms, i.e., $G(X, Y) = uF(aX + bY, cX + dY)$ for some $u \in A^*$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(A)$, then $A_G \cong A_F$ as A-algebras. Any ring that is the invariant ring of a binary form is called a binary ring (or binary order if $A = \mathbb{Z}$).

Thus, $\mathbb{Z}_\alpha$ is the invariant order of $F_\alpha(X, Y) := Y^n f_\alpha(X/Y)$. In other words, a rationally monogenic order is the invariant order of a primitive, irreducible binary form.

From work of Delone and Faddeev (1940), later extended by Gan, Gross, and Savin (2002) and Deligne (unpublished) (see also section 16.3 of Evertse and Győry (2017)) it follows that for every commutative ring A, the map $F \mapsto A_F$ gives a one-to-one correspondence between $GL_2(A)$-equivalence classes of binary cubic forms in $A[X, Y]$ and isomorphism classes of free cubic A-algebras, i.e., commutative, associative, unital A-algebras that as an A-module are free of rank 3. Wood (2011) gave a geometric interpretation of invariant rings of binary forms.

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

As above, K will denote a number field of degree $n \geq 3$ with ring of integers $\mathcal{O}_K$ and discriminant D_K.

We consider the above index form equation (5.13), but for an index form $I(X_2, \ldots, X_n)$ associated with an ordered integral basis $(1, \omega_2, \ldots, \omega_n)$ of K, i.e., we restrict ourselves to the case $\mathcal{O} = \mathcal{O}_K$.

The exponential bound (5.14) for the solutions of (5.13) is too large for practical use. In the 1990's, there were new breakthroughs, leading to the

complete resolution of certain index form equations. In fact, practical methods were elaborated for solving equation (5.13) when $|D_K|$ is not too large, and the degree n of K is ≤ 6. Further, (5.13) was solved for some special higher degree number fields K up to about degree 15 and for some relative extensions of degree ≤ 4.

6.1. **The case $\mathbf{n = 3}$ and 4. Approach via Thue equations of degree 3 and 4.**

It is known that in the case $n = 3$ equation (5.13) can be reduced to a cubic Thue equation while, in the case $n = 4$, to a cubic and some quartic Thue equations, that is to equations of the form

$$F(x, y) = m \text{ in } x, y \in \mathbb{Z}, \tag{6.1}$$

where m is a non-zero integer and $F \in \mathbb{Z}[X, Y]$ is a binary form of degree 3 or 4 with pairwise non-proportional linear factors over $\overline{\mathbb{Q}}$. By a general theorem of Thue (1909), every equation of the type (6.1) with F of degree ≥ 3 has only finitely many solutions, and Baker (1968b) gave an explicit upper bound for their solutions in terms of $|m|$ and the height and degree of F. The best known bound is due to Bugeaud and Győry (1996b). However, in concrete cases this bound is too large for practical use. For solving concrete Thue equations, general practical methods were developed in Pethő and Schulenberg (1987) for $m = 1$, and in Tzanakis and de Weger (1989) for arbitrary m. Later, these methods were made even more efficient in Bilu and Hanrot (1996, 1999) and Hanrot (1997). Their algorithms are based on Baker's method and certain reduction and enumeration techniques. Hence we possess efficient algorithms for solving equation (5.13) for $n = 3$ and 4. However, this approach cannot be applied in general to index form equations in number fields K of degree $n > 4$, except for $n = 6, 8, 9$ when K has a quadratic or cubic subfield; then equation (5.13) leads to relative cubic or quartic Thue equations.

For $\mathbf{n = 3}$, Gaál and Schulte (1989) reduced equation (5.13) to a cubic Thue equation with $m = 1$. Then, using the algorithm elaborated for solving cubic Thue equations, they determined all power integral bases of cubic fields K with discriminant $-300 \leq D_K \leq 3137$. Their computations were later extended in Schulte (1989, 1991).

For $\mathbf{n = 4}$, Gaál, Pethő and Pohst (1993, 1996) first reduced the equation (5.13) to a cubic Thue equation and a pair of ternary quadratic equations.

Then the quadratic equations were themselves reduced to quartic Thue equations. Finally, by means of efficient algorithms for solving such Thue equations, they computed the solutions of equation (5.13) for quartic number fields with not too large discriminant. They obtained several interesting tables among others on the distribution of minimal indices and about the average behaviour of minimal indices.

6.2. **The cases $\mathbf{n = 5}$ and 6. Refined version of the general approach via unit equations, combined with reduction and enumeration algorithms.**
For $\mathbf{n \geq 5}$, the approach via Thue equations does not work in general. For $\mathbf{n = 5}$ and **6** a refined version of the general approach involving unit equations is needed. Since by (5.10), (5.6) and (5.3) we have for $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$

$$(5.13) \Leftrightarrow D(\alpha) = D_K \Leftrightarrow D(f_\alpha) = D_K \text{ in } \alpha \in \mathcal{O}_K,$$

where $f_\alpha \in \mathbb{Z}[X]$ is the minimal polynomial of α, in case of concrete equations (5.13) a refinement of the proof of Theorem 4.2 for irreducible f_α's must be combined with some reduction and enumeration algorithms.

The refined version of the general method for solving index form equations (5.13) consists of the following steps:

1. Reduction to unit equations but in considerably smaller subfields of the normal closure G of K, of which the unit rank is much smaller than that of G, i.e., at most $n(n-1)/2 - 1$ (note that the unit rank of G may be as large as $n! - 1$); cf. Győry (1998, 2000). Then in the unit equation corresponding to (4.10), one can write $\varepsilon_{ijk} = \zeta_{ijk}\rho_1^{a_{ijk,1}} \cdots \rho_r^{a_{ijk,r}}$, with a root of unity ζ_{ijk} and a fundamental system of units $\rho_1, \ldots, \rho_r$ of bounded height, and in concrete cases one can bound the exponents $|a_{ijk,l}|$ by Baker's method. Here the estimate of Baker and Wüstholz (1993) for linear forms in logarithms of algebraic numbers is very practical to apply in calculations.

2. The bounds in concrete cases are still too large. Hence a *reduction algorithm* is needed, reducing the Baker's bound for $|a_{ijk,l}|$ in several steps if necessary by a refined version of the *L^3-algorithm*; cf. de Weger (1989), Tzanakis and de Weger (1989), Wildanger (1997) and Gaál and Pohst (1996).

3. The last step is to apply an *enumeration algorithm*, determining the small solutions under the reduced bound; cf. Wildanger (1997, 2000), Gaál and Győry (1999) and Bilu, Gaál and Győry (2004).

Combining the refined version of the general approach with reduction and enumeration algorithms, for $n = 5, 6$ and for not too large $|D_K|$, Gaál and Győry (1999), resp. Bilu, Gaál and Győry (2004) gave algorithms for determining all power integral bases and hence checking the monogenicity and determining the multiplicity of the monogenicity of K.

We note that the use of the refined version of the general approach is particularly important in the application of the enumeration algorithm.

To perform computations, algebraic number theory packages, a computer algebra system and in some cases a supercomputer were needed.

6.3. **Examples: resolutions of index form equations of the form** (5.13) **for $\mathbf{n = 3, 4, 5, 6}$ in the most difficult case.**
In the examples below, the authors resolved concrete index form equations of the form (5.13) for $n = 3, 4, 5, 6$. Each number field K of degree n is given by an irreducible monic polynomial $f(X) \in \mathbb{Z}[X]$, a zero of which generates K over $\mathbb{Q}$. In each case all power integral bases in K, and therefore the *multiplicity of the monogenicity of* K, denoted by $mm(K)$, are computed by the method outlined above. For the lists of the power integral bases, we refer to the original papers and to Evertse and Győry (2017) and Gaál (2019).

$\mathbf{n = 3}$, $f(X) = X^3 - X^2 - 2X + 1$, $mm(K) = 9$ (Gaál and Schulte, 1989);

$\mathbf{n = 4}$, $f(X) = X^4 - 4X^2 - X + 1$, $mm(K) = 17$ (Gaál, Pethő and Pohst, 1990's);

$\mathbf{n = 5}$, $f(X) = X^5 - 5X^3 + X^2 + 3X - 1$, $mm(K) = 39$ (Gaál and Győry, 1999);

$\mathbf{n = 6}$, $f(X) = X^6 - 5X^5 + 2X^4 + 18X^3 - 11X^2 - 19X + 1$, $mm(K) = 45$ (Bilu, Gaál, and Győry, 2004).

We note that from the point of view of computation, the above examples belong to the most difficult cases for $n = 3, 4, 5$, and 6, K being in each case totally real with Galois group S_n. In these cases the number of exponents in the unit equations involved is the largest possible.

Remark. The general procedure outlined above to solve any concrete equation (5.13) for $n = 6$ requires considerable CPU-time. In certain special cases (e.g., if $n = 6$ and K has a quadratic subfield), there are faster algorithms, see Gaál (2024, 2025). However, some of these algorithms determine only the "small" solutions, and do not exclude the existence of "large" solutions.

For $n \geq 7$, the above mentioned algorithms do not work in general. Then the number of fundamental units, $\rho_1, \ldots, \rho_r$ involved can be $\geq \frac{7 \cdot 6}{2} - 1 = 20$ which is too large to use the enumeration algorithm.

Problem 1. *For given* $\mathbf{n \geq 7}$*, establish a practical algorithm for solving equation* (5.13) *in case of* ***any*** *number field* K *of degree* $\mathbf{n}$ *with not too large discriminant.*

7. Power integral bases and canonical number systems in number fields

Number systems and their generalizations have been intensively studied for a long time. Here we present an important generalization for the number field case, point out its close connection with power integral bases and formulate an application of the above Theorem 5.5 to this generalization.

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$, and let $\alpha \in \mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(\alpha)| \geq 2$. Then $\{\alpha, \mathcal{N}(\alpha)\}$ with

$$\mathcal{N}(\alpha) = \{0, 1, \ldots, |N_{K/\mathbb{Q}}(\alpha)| - 1\}$$

is called a *canonical number system*, in short CNS, in $\mathcal{O}_K$, if every non-zero element of $\mathcal{O}_K$ has a unique representation of the form

$$a_0 + a_1\alpha + \cdots + a_k\alpha^k \text{ with } a_i \in \mathcal{N}(\alpha) \text{ for } i = 0, \ldots, k,\ a_k \neq 0.$$

Then α is called the *base* and $\mathcal{N}(\alpha)$ the *set of digits* of the number system. This concept is a generalization of the radix representation considered in $\mathbb{Z}$.

B. Kovács (1981) proved the following fundamental theorem.

Theorem 7.1 (B. Kovács, 1981)**.** *In* $\mathcal{O}_K$ *there exists a canonical number system if and only if* $\mathcal{O}_K$ *has a power integral basis.*

Together with the above Theorem 5.5 of Győry (1976) this implies that it is effectively decidable whether there exists a CNS in $\mathcal{O}_K$. Theorem 5.5 provides even a general algorithm to determine all power integral bases in $\mathcal{O}_K$. Using this, B. Kovács and Pethő (1991) proved as follows.

Theorem 7.2 (B. Kovács and Pethő, 1991). *Up to $\mathbb{Z}$-equivalence, there are only finitely many CNS's in $\mathcal{O}_K$, and all of them can be effectively determined.*

In fact, using Theorem 5.6, they extended their result to any order $\mathcal{O}$ of K as well. In an order $\mathcal{O}$, a canonical number system $\{\alpha, \mathcal{N}(\alpha)\}$ is defined in a similar way as in $\mathcal{O}_K$.

We note that Brunotte (2001) considerably improved the procedure of B. Kovács and Pethő (1991) and gave an efficient algorithm for finding all such CNS's, provided that one has an efficient algorithm for determining all power integral bases in $\mathcal{O}_K$, resp. in $\mathcal{O}$. As was seen in Section 6, such an algorithm is known for number fields K of degree at most 4 if their discriminants are not too large in absolute value.

B. Kovács and Pethő (1991) gave also a complete, effective characterization of CNS's in number fields and in their orders.

Theorem 7.3 (B. Kovács and Pethő, 1991). *Let $\mathcal{O}$ be an order in a number field K. There exist $\alpha_1, \ldots, \alpha_t \in \mathcal{O}$, $n_1, \ldots, n_t \in \mathbb{Z}$, $N_1, \ldots, N_t$ finite subsets of $\mathbb{Z}$, which are all effectively computable, such that $\{\alpha, \mathcal{N}(\alpha)\}$ is a CNS in $\mathcal{O}$, if and only if $\alpha = \alpha_i - h$ for some integers i, h with $1 \le i \le t$ and $h \ge n_i$ or $h \in N_i$.*

Several generalizations and applications have been obtained. Pethő and Varga (2017) generalized the result of B. Kovács to CNS's over imaginary quadratic Euclidean domains. Pethő and Thuswaldner (2018) study CNS's in relative extensions. Most of the results of B. Kovács and Pethő (1991) are generalized to this situation. Further generalizations are in Evertse, Győry, Pethő and Thuswaldner (2019) over general orders.

Pethő (1991) introduced the notion of CNS polynomials. The monic polynomial $P(X) \in \mathbb{Z}[X]$ is called *CNS polynomial* if $|P(0)| \ge 2$ and for every $0 \ne Q(X) \in \mathbb{Z}[X]$ there exist unique integers $\ell \ge 0$, $q_1, \ldots, q_\ell \in \{0, 1, \ldots, |P(0)| - 1\}$ such that

$$Q(X) \equiv \sum_{j=0}^{\ell} q_j x^j \pmod{P(X)}.$$

He proved that *if $P(X)$ is irreducible and monic and α is one of the zeros of $P(X)$, then $P(X)$ is a CNS polynomial if and only if $\{\alpha, 0, 1, \ldots, |P(0)|-1\}$ is a* CNS *in $\mathbb{Z}[\alpha]$.*

A. Kovács (2001) computed all CNS polynomials with $P(0) = 2$ up to degree 8. This computation was extended up to degree 14 in Burcsi and A. Kovács (2008).

Akiyama, Borbély, Brunotte, Pethő and Thuswaldner (2005) defined the *shift* radix system (SRS). It is a discrete dynamical system, which is a common generalization of CNS polynomials and some kind of β representations of real numbers. Many properties of SRS were also described.

For surveys, we refer to Brunotte (2001), Pethő (2004), Brunotte, Huszti and Pethő (2006), Komornik (2011), Evertse, Győry, Pethő and Thuswaldner (2019) and the references given there.

8. Further consequences and applications of the reduction theory

The main results from the effective reduction theory for polynomials discussed before, i.e., Theorems 4.2 and 4.4, as well as their various versions led to many applications. Some of them were treated in Sections 4 to 7. Below we briefly present some others in their simplest form. For further applications, we refer to the survey paper Győry (2006), the books Győry (1980b), Smart (1998), Evertse and Győry (2017) and the references given there.

8.1. **Applications to classical Diophantine equations.**

Theorem 4.2 can be applied to superelliptic equations and the Schinzel–Tijdeman equation.

- Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n \geq 3$ with discriminant $D(f) \neq 0$, and $m \geq 2$ an integer. Consider the solutions $x, y \in \mathbb{Z}$ of the equation

$$f(x) = y^m. \tag{8.1}$$

  Applying various variants of Theorem 4.2 to the polynomial f and then using Baker's method for the reduced equation, Trelina (1985) and, for $n = 3, m = 2$, Pintér (1995) gave effective upper bounds for $|y|$ that depend on m, n and $|D(f)|$, but *not on the height* of f. We recall that the height of f can be arbitrarily large with respect to $|D(f)|$. Furthermore, Győry and Pintér (2008) showed that for each solution x, y of (8.1) with $\gcd(y, D(f)) = 1$, $|y|^m$ can be effectively bounded in terms of the radical of $D(f)$, i.e. the product of the distinct prime factors of $D(f)$. It should be noted that $|D(f)|$ can be arbitrarily large with respect to its radical.

Brindza, Evertse and Győry (1991), Haristoy (2003) and Győry and Pintér (2008) gave upper bounds even for m that depend only on n and $|D(f)|$.

- Consider now an application of Theorem 4.2 to *equations of discriminant type*

$$D(x_1, \dots, x_n) = D \text{ in } x_1, \dots, x_n \in \mathbb{Z}, \tag{8.2}$$

where $D(x_1, \dots, x_n) := D(f(X))$ is the discriminant of the polynomial $f(X) = X^n + x_1 X^{n-1} + \cdots + x_n$ in X, and $D \neq 0$ is a given rational integer. If $(x_1, \dots, x_n)$ is a solution of (8.2) then so is

$$(x_1^*, \dots, x_n^*) = \left(\frac{f^{(n-1)}(a)}{(n-1)!}, \dots, f(a) \right) \text{ for any } a \in \mathbb{Z},$$

where $X^n + x_1^* X^{n-1} + \cdots + x_n^* =: f^*(X) = f(X+a)$. Such a set of solutions of (8.2) is called a *family of solutions*. Using a quantitative version of his Theorem 4.2, Győry (1976) proved that (8.2) has only finitely many families of solutions and a representative of every family can be effectively determined. Theorem 4.2* above gives a considerable improvement of this result of Győry (1976).

The binary form variant of Theorem 4.4 can be applied to Thue equations, Thue inequalities and Thue–Mahler equations.

- Let $F \in \mathbb{Z}[X, Y]$ be an irreducible binary form of degree $n \geq 3$ and discriminant D, let $p_1, \dots, p_s$ $(s \geq 0)$ be distinct primes not exceeding P, and let m be a positive integer coprime with $p_1, \dots, p_s$. There are several upper bounds for the *number* of solutions x, y of the Thue equation

$$F(x, y) = m, \tag{8.3}$$

the Thue inequality

$$0 < |F(x, y)| \leq m \tag{8.4}$$

and the Thue–Mahler equation

$$F(x, y) = m p_1^{z_1} \cdots p_s^{z_s}, \text{ with } (x, y) = 1, \tag{8.5}$$

where $z_1, \dots, z_s$ are also unknown non-negative integers.

Using a quantitative binary form version of Theorem 4.4, e.g. the general effective Theorem 1 of Evertse and Győry (1991a) on binary forms of given degree and given discriminant over $\mathbb{Z}$, the previously obtained upper bounds for the *number* of solutions of these equations were substantially

improved under the assumptions that n, D, m, s and P satisfy some additional conditions. Such improved upper bounds were derived in Stewart (1991) for equation (8.5) with $\gcd(x, y) = 1$ when $m > C_1$, in Brindza (1996) for (8.3) with $\gcd(x, y) = 1$ when $m > C_2$, and in Thunder (1995) for (8.4) when $m > C_3$, where C_1, C_2, C_3 are effectively computable numbers such that C_1 depends on $n, |D|, P, s$ and C_2, C_3 on n and $|D|$. Further, Evertse and Győry (1991b) showed that if $|D| > C_4$, then the number of coprime solutions of (8.4) is at most $6n$ if $n > 400$, and by Győry (2001) it is at most $28n + 6$ if $|D| > C_5$ and $3 \leq n \leq 400$. For $m = 1$ and $|D| > C_6$, this was later improved by Akhtari (2012) to $11n - 2$. Here C_4, C_5, C_6 are effectively computable numbers such that C_4, C_5 depend on m and n, and C_6 on n. Together with the above mentioned quantitative version of Theorem 4.4, these imply that for given $n \geq 3$ and $m \geq 1$, there are only finitely many $GL_2(\mathbb{Z})$-equivalence classes of irreducible binary forms $F \in \mathbb{Z}[X, Y]$ of degree n for which the number of coprime solutions of (8.4) exceeds $28n + 6$, resp. $11n - 2$ if $m = 1$.

- The quantitative version of Theorem 4.4, proved in Evertse and Győry (1991a) was also applied in Evertse (1993) to bound the number of solutions of some resultant inequalities, and in Ribenboim (2006) to binary forms with given discriminant, having additional conditions on the coefficients.

  We remark that using the improved and completely explicit version Theorem 4.4* of Evertse and Győry (2017), the above quoted applications can be made more precise.

8.2. **Some other applications of Theorems 4.2 and 4.4.**

- In Evertse and Győry (2017), as a consequence of Theorem 4.4*, we derived for any separable polynomial $f \in \mathbb{Z}[X]$ of degree $n \geq 4$ an improvement of the previous bounds for the minimal root distance of f.
- Some applications of Theorem 4.2 were given to the reducibility of a general class of polynomials of the form $g(f(X))$ where f, g are monic polynomials, $g(X)$ is irreducible with CM splitting field. For given prime p and $g \in \mathbb{Z}[X]$, there are up to $\mathbb{Z}$-equivalence only finitely many $f \in \mathbb{Z}[X]$ of degree p with distinct real zeros for which $g(f(X))$ is reducible; see Győry (1976, 1982).

- In Evertse and Győry (1991a), a quantitative binary form variant of Theorem 4.4 was utilized to give effective upper bounds for the minimal non-zero absolute value of binary forms at integral points.
- For an application of an earlier version of Theorem 5.2 (ii) to integral valued polynomials, see Peruginelli (2014).
- For an application of Theorem 5.2 to so-called binomially equivalent numbers, see Yingst (2006).

As will be seen in the next section, the various generalizations presented there of Theorems 4.2 and 4.4 have also several applications.

9. Generalizations and their consequences, applications

In Sections 4 to 8 we presented the most significant results and consequences/applications of the effective reduction theory of integral polynomials over $\mathbb{Z}$. In the last decades this effective theory has been generalized by the authors among others for the number field case, more precisely for the case of integral, resp. S-integral polynomials over number fields. In the monic case, they have obtained even more general effective results for polynomials over finitely generated domains of characteristic 0 which may contain transcendental elements, too. These provided many important consequences and applications, and yielded a further advancement in the theory.

In this section we formulate some typical general effective theorems on integral polynomials over number fields and finitely generated domains, including various generalizations of Theorems 4.2, 4.4 and their consequences.

For simplicity, we present them in qualitative forms. For explicit versions and further results and applications, we refer to our original works or our books Evertse and Győry (2017, 2022). The proofs depend explicitly or implicitly on an effective finiteness theorem of Győry (1979) or its improvements by Bugeaud and Győry (1996a), Győry and Yu (2006), Evertse and Győry (2015) or Győry (2019), see Theorem 4.10 above on S-unit equations, resp. of Evertse and Győry (2013) on unit equations over finitely generated domains.

For convenience, the monic and non-monic cases are treated separately in the Subsections 9.1 and 9.2 below.

9.1. **Generalizations: the monic case.**

9.1.1. *Results over number fields.*
Let L be a number field with ring of integers $\mathcal{O}_L$, and S a finite set of places on L containing all infinite places S_∞. The ring of S-integers of L, denoted by

$\mathcal{O}_S$, consists of those elements of L which are integral at every finite placee outside S. A fractional ideal of $\mathcal{O}_S$ is a subset $\mathfrak{a}$ of L such that there is non-zero $\delta \in L$ such that $\delta\mathfrak{a}$ is an ideal of $\mathcal{O}_S$. Given a subset $\mathcal{V} \neq \{0\}$ of L such that $\delta\mathcal{V} \subset \mathcal{O}_S$ for some non-zero $\delta \in \mathcal{O}_S$, we denote by $(\mathcal{V})_S$ the fractional ideal of $\mathcal{O}_S$ generated by $\mathcal{V}$. Lastly, we denote by $\mathcal{O}_S^*$ the unit group of $\mathcal{O}_S$.

Two *monic* polynomials $f, g \in \mathcal{O}_S[X]$ of degree n are called $\mathcal{O}_S$-*equivalent* if

$$g(X) = \varepsilon^n f(\varepsilon^{-1}X + a) \text{ for some } \varepsilon \in \mathcal{O}_S^* \text{ and } a \in \mathcal{O}_S,$$

and *strongly* $\mathcal{O}_S$-*equivalent* if

$$g(X) = f(X + a) \text{ for some } a \in \mathcal{O}_S.$$

In this case $D(g) = \varepsilon^{n(n-1)}D(f)$, resp. $D(g) = D(f)$.

For a polynomial $g \in \overline{\mathbb{Q}}[X]$, we denote by $H(g)$ the absolute height of the vector whose coordinates are the coefficients of g.

Theorem 9.1 (Győry, 1978b, 1984)**.** *Let $\delta \in \mathcal{O}_S \setminus \{0\}$, and let $f \in \mathcal{O}_S[X]$ be a monic polynomial of degree $n \geq 2$ with discriminant $D(f) \in \delta\mathcal{O}_S^*$. Then f is $\mathcal{O}_S$-equivalent to a monic polynomial $g \in \mathcal{O}_S[X]$ for which*

$$H(g) < C_1(L, S, (\delta)_S, n)$$

where C_1 is an effectively computable number depending only on L, S, δ and n.

For $L = \mathbb{Q}$, $S = S_\infty$, this is just Theorem 4.2, (ii), where the bound given for $H(g)$ is in fact independent of n. We note that this is not the case in general, see Evertse and Győry (2017), p. 155.

For the best known, completely explicit bound C_1 see also Evertse and Győry (2017), Theorem 8.2.3.

Theorem 9.1 implies the following effective finiteness results.

Corollary 9.2. *For given integer $n \geq 2$ and $\delta \in \mathcal{O}_S \setminus \{0\}$, there are only finitely many $\mathcal{O}_S$-equivalence classes of monic polynomials f in $\mathcal{O}_S[X]$ of degree n and with $D(f) \in \delta\mathcal{O}_S^*$. Further, there exists an algorithm that for any $n \geq 2$ and any effectively given L, S and δ computes a full set of representatives of these classes.*

Theorem 9.1 gives also in an effective form that there are only finitely many strong $\mathcal{O}_S$-equivalence classes of monic polynomials $f \in \mathcal{O}_S[X]$ of given degree $n \geq 2$ and with given discriminant $D(f) = \delta \neq 0$. For a quantitative and explicit version, see Corollary 8.2.6 in Evertse and Győry (2017).

We recall that for definitions of *effectively given* concepts, structures, etc. we referred in Subsection 1.1 to the corresponding sections of our books Evertse and Győry (2015, 2017, 2022).

We now present another version of Theorem 9.1 which is more convenient to apply.

With the above notation, let $\mathcal{L} = \mathcal{O}_S^* \cap \mathcal{O}_L$. If $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ denote the prime ideals of $\mathcal{O}_L$ corresponding to the finite places of S, then $\mathcal{L}$ is just the multiplicative semigroup of non-zero elements of $\mathcal{O}_L$ which are not divisible by any prime ideal different from $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. The set $\mathcal{L}$ contains obviously the unit group $\mathcal{O}_L^*$ of $\mathcal{O}_L$, and, for $t = 0$, $\mathcal{L} = \mathcal{O}_L^*$.

We say that the monic polynomials $f, g \in \mathcal{O}_L[X]$ are *strongly $\mathcal{O}_L$-equivalent* if

$$g(X) = f(X + a) \text{ for some } a \in \mathcal{O}_L.$$

The next theorem was proved in Győry (1978b) in a quantitative form.

Theorem 9.3 (Győry, 1978b)**.** *Let $L, \mathcal{L}$ be as above and let δ be a non-zero element of $\mathcal{O}_L$. If $f \in \mathcal{O}_L[X]$ is a monic polynomial of degree $n \geq 2$ with discriminant $D(f) \in \delta\mathcal{L}$, then it is strongly $\mathcal{O}_L$-equivalent to a polynomial of the form $\eta^n g(\eta^{-1}X)$, where $\eta \in \mathcal{L}$, $g \in \mathcal{O}_L[X]$ and*

$$H(g) \leq C_2(L, \mathcal{L}, (\delta)_S, n),$$

where C_2 is an effectively computable number depending only on $L, \mathcal{L}, (\delta)_S$ and n.

If $L = \mathbb{Q}$ and $t = 0$, then $\mathcal{L} = \{\pm 1\}$, and Theorem 9.3 gives again Theorem 4.2 (ii). For a more general version of Theorem 9.3 with not necessarily non-zero δ, see also Theorem 2 in Győry (1981).

We present now some applications of Theorem 9.3 to algebraic integers whose *discriminants* resp. *indices* over L belong to $\delta\mathcal{L}$.

For an algebraic integer α of degree $n \geq 2$ over L, $f_{\alpha,L}$ will denote the monic minimal polynomial of α over L, i.e., the monic polynomial in $\mathcal{O}_L[X]$ of minimal degree of which α is a zero. We define the discriminant of α relative to L by

$$D_L(\alpha) := D(f_{\alpha,L}) = \prod_{1 \leq i < j \leq n} (\alpha^{(i)} - \alpha^{(j)})^2,$$

where $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are the conjugates of α over L. The algebraic integers α and β are said to be *strongly $\mathcal{O}_L$-equivalent* over L when $\alpha - \beta \in \mathcal{O}_L$. In this case their minimal polynomials over L are also strongly $\mathcal{O}_L$-equivalent.

We denote by $H(\beta)$ the absolute height of an algebraic number β.

Corollary 9.4 is an immediate consequence of Theorem 9.3. It was proved in Győry (1978b) in quantitative form.

Corollary 9.4 (Győry, 1978b)**.** *Let $L, \mathcal{L}$ and δ be as in Theorem 9.3, and let α be an algebraic integer with degree $n \geq 2$ and discriminant $D_L(\alpha) \in \delta\mathcal{L}$ over L. Then α is strongly $\mathcal{O}_L$-equivalent to an algebraic integer of the form $\eta\beta$, where $\eta \in \mathcal{L}$ and β is an algebraic integer satisfying*

$$H(\beta) < C_3(L, \mathcal{L}, \delta, n)$$

with an effectively computable number C_3 depending only on $L, \mathcal{L}, \delta$ and n.

This is a considerable effective generalization of Theorem 5.2 in two different directions, for the number field case and for the $\mathfrak{p}$-adic case. We note that in the special case $L = \mathbb{Q}$, Corollary 9.4 was proved independently by Trelina (1977a).

A simple consequence of Corollary 9.4 is that up to the obvious multiplications by elements of $\mathcal{L}$ and translations by integers of L, there are only finitely many algebraic integers α with given degree n and discriminant $D_L(\alpha) \in \delta\mathcal{L}$ over L and they can be effectively determined. As is remarked in Győry (1978b), the first, finiteness part can be deduced, in an *ineffective* form, from the *ineffective* Theorem 4.1 of Birch and Merriman (1972) over number fields and from the finiteness of the number of solutions of the generalized Thue–Mahler equation; cf. Parry (1950).

As is pointed out in Győry (1978b), p. 177, if in Corollary 9.4 we restrict ourselves to integers α of a fixed algebraic number field K of degree $n \geq 3$ over L, then the proof of Corollary 9.4 in Győry (1978b) gives the following in quantitative form.

Corollary 9.5 (Győry, 1978b, 1981)**.** *Let $L, \mathcal{L}, \delta$ and K be as above, and let α be a primitive integral element of K with discriminant $D_{K/L}(\alpha) \in \delta\mathcal{L}$ over L. Then α is strongly $\mathcal{O}_L$-equivalent to an algebraic integer of the form $\eta\beta$, where $\eta \in \mathcal{L}$, and β is an algebraic integer in K such that*

$$H(\beta) < C_4(L, K, \mathcal{L}, \delta, n)$$

with an effectively computable number C_4 which depend only on $L, K, \mathcal{L}$ and δ.

Keeping the above notations, we present some consequences of Corollary 9.5. Consider an order $\mathcal{O}$ of the field extension K/L (i.e. let $\mathcal{O}$ be a subring

of $\mathcal{O}_K$, the ring of integers of K, that has the full dimension n as an $\mathcal{O}_L$-module). Denote by $\mathfrak{D}_{K/L}(\mathcal{O})$ the *discriminant ideal* of $\mathcal{O}$. Then we have (cf. Fröhlich, 1967)

$$(D_L(\alpha)) = \mathfrak{I}^2_{\mathcal{O}}(\alpha) \cdot \mathfrak{D}_{K/L}(\mathcal{O})$$

for any $\alpha \in \mathcal{O}$ such that $L(\alpha) = K$. Here $\mathfrak{I}_{\mathcal{O}}(\alpha)$ is an integral ideal which is called the *index* of α in $\mathcal{O}$. It is clear that if $\alpha, \beta \in \mathcal{O}$ are strongly $\mathcal{O}_L$-equivalent then $\mathfrak{I}_{\mathcal{O}}(\alpha) = \mathfrak{I}_{\mathcal{O}}(\beta)$.

Corollary 9.6 (Győry, 1981)**.** *If $\alpha \in \mathcal{O}$ has index $\mathfrak{I}_{\mathcal{O}}(\alpha)$ not divisible by any prime ideal different from $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, then α is strongly $\mathcal{O}_L$-equivalent to an algebraic integer of the form $\eta\beta$, where $\eta \in \mathcal{L}, \beta \in \mathcal{O}$, and*

$$H(\beta) < C_5(L, K, \mathcal{O}, \mathfrak{p}_1, \ldots, \mathfrak{p}_t),$$

where C_5 is an effectively computable number depending only on $L, K, \mathcal{O}, \mathfrak{p}_1, \ldots, \mathfrak{p}_t$.

In the case $\mathcal{O} = \mathcal{O}_K$, a prime ideal $\mathfrak{p}$ in L is called a *common index divisor* of K/L if $\mathfrak{p}$ divides $\mathfrak{I}_{\mathcal{O}_K}(\alpha)$ for every primitive integral element α of K/L. The number of common index divisors is finite and a well-known theorem of Hasse (1980) gives an elegant characterization of these divisors. It is interesting to apply Corollary 9.6 to the case when $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are just the common index divisors of K/L. There are relative extensions of arbitrary high degree in which there exists no element α with index not divisible by prime ideals different from the common index divisors; cf. Pleasants (1974). Corollary 9.6 provides and effective algorithm for deciding whether such an element α exists and for determining all α having this property.

Corollaries 9.5 and 9.6 allowed Győry (1981) to get some information about the arithmetical structure of those non-zero algebraic integers resp. non-zero integral ideals in L which are discriminants resp. indices of elements of $\mathcal{O}_K$ over L.

We now present generalizations of Theorems 5.5 and 5.6 for the relative case.

Let again L be a number field, K an extension of degree $n \geq 2$ of L, and $\mathcal{O}$ an order of K over L. Then $\mathcal{O} = \mathcal{O}_L[\alpha]$ for some $\alpha \in \mathcal{O}$ if and only if $\mathfrak{I}_{\mathcal{O}}(\alpha) = \mathcal{O}_L$. In this case $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a $\mathcal{O}_L$-module basis for $\mathcal{O}$. There exists an extensive literature of such power bases of orders of number fields and related topics; we refer the reader to the works of Hensel (1908), Hasse

(1980), Narkiewicz (1974), Győry (1978a, 1978/79), and Evertse and Győry (2017), and thence to the literature mentioned there.

We say that $\alpha, \beta \in \mathcal{O}$ are $\mathcal{O}_L$-*equivalent* if $\beta = a + \varepsilon\alpha$ for some $a \in \mathcal{O}_L$ and unit ε in $\mathcal{O}_L$. If α is a generator of $\mathcal{O}$ over $\mathcal{O}_L$, i.e. $\mathcal{O} = \mathcal{O}_L[\alpha]$ then so is every β which is $\mathcal{O}_L$-equivalent to α.

The following fundamental theorem is a consequence of Corollary 9.6.

Theorem 9.7 (Győry, 1981)**.** *Let $\mathcal{O}$ be an order of K/L, and suppose that $\mathcal{O} = \mathcal{O}_L[\alpha]$ for some $\alpha \in \mathcal{O}$. Then there is $\beta \in \mathcal{O}$ that is $\mathcal{O}_L$-equivalent to α and for which*

$$H(\beta) < C_6(L, K, \mathcal{O}),$$

where C_6 is an effectively computable number depending only on L, K and $\mathcal{O}$.

For $L = \mathbb{Q}$, this gives Theorems 5.5 and 5.6 above. In the case $\mathcal{O} = \mathcal{O}_K$, Theorem 9.7 was proved in Győry (1978a) with a completely explicit bound corresponding to C_6. For the best known explicit bound in Theorem 9.7, see Corollary 8.4.13 in Evertse and Győry (2017).

Theorem 9.7 provides a general effective algorithm for deciding whether a relative extension K/L resp. an order $\mathcal{O}$ of K over L is monogenic or not, and for determining all $\alpha \in \mathcal{O}_K$ resp. all $\alpha \in \mathcal{O}$ for which $\mathcal{O}_K = \mathcal{O}_L[\alpha]$ resp. $\mathcal{O} = \mathcal{O}_L[\alpha]$.

We now present a very important consequence of Theorem 9.7. Let again L be a number field, K an extension of degree $n \geq 2$, and $\mathcal{O}_K, \mathcal{O}_L$ the rings of integers of K resp. L. Pleasants (1974) gave an explicit formula which enables one to compute a positive integer $m(\mathcal{O}_K, \mathcal{O}_L)$ such that if $r(\mathcal{O}_K, \mathcal{O}_L)$ denotes the minimal number of generators of $\mathcal{O}_K$ as $\mathcal{O}_L$-algebra then

$$m(\mathcal{O}_K, \mathcal{O}_L) \leq r(\mathcal{O}_K, \mathcal{O}_L) \leq \max\{m(\mathcal{O}_K, \mathcal{O}_L), 2\}.$$

Pleasants proved that if $L = \mathbb{Q}$, there are number fields K of arbitrarily large degree over $\mathbb{Q}$ such that $m(\mathcal{O}_K, \mathbb{Z}) = 1$ and $\mathcal{O}_K$ is not monogenic. Consequently, his theorem does not make it possible to decide whether the ring of integers of a number field is monogenic. Together with Pleasants' result, our Theorem 9.7 above gives the following

Corollary of Theorem 9.7 (and of Pleasants (1974))**.** *There is an algorithm for determining the least number of elements of $\mathcal{O}_K$ that generate $\mathcal{O}_K$ as an $\mathcal{O}_L$-algebra.*

Chapter 11 of Evertse and Győry (2017) considers more generally $\mathcal{O}_S$-orders of finite étale L-algebras, and gives a method to determine a system of $\mathcal{O}_S$-algebra generators of minimal cardinality of such an order. This was basically work of Kravchenko, Mazur and Petrenko (2012), worked out in more detail in a special case.

We give an overview of generalizations of some of the results from the previous sections.

- In Section 5, several results have reformulations in terms of polynomial Diophantine equations; see equations (5.7) and (5.12). In the present section the above extensions of the results from Section 5 have also reformulation in terms of discriminant form equations and index form equations over number fields and in the $\mathfrak{p}$-adic case.
- Corollaries 5.7, 5.8 were first extended to the case when D resp. I is replaced by $p_1^{u_1} \cdots p_s^{u_s}$, where $p_1, \ldots, p_s$ are fixed primes and $u_1, \ldots, u_s$ are unknown non-negative integers; see Győry (1978b, 1981), Trelina (1977a, 1977b), Győry and Papp (1977). These results yielded e.g. explicit lower bounds for the greatest prime factor of the discriminant and index of an integer of a number field. For generalizations for the number field case, see Győry (1980a, 1981).
- Corollary 5.7 on discriminant form equations was generalized for more general decomposable form equations of the form

$$F(x_1, \ldots, x_m) = F \text{ in } x_1, \ldots, x_m \in \mathbb{Z}, \tag{9.1}$$

  where $F \in \mathbb{Z} \setminus \{0\}$ and $F(X_1, \ldots, X_m)$ is a decomposable form with coefficients in $\mathbb{Z}$ which factorizes into linear factors over $\overline{\mathbb{Q}}$ such that these factors form a so-called triangularly connected system (i.e. (9.1) can be reduced to a connected system of three terms unit equations); see Győry and Papp (1978) and, more generally, Győry (1998).

  For discriminant form equations and more general decomposable form equations, see also Evertse and Győry (2017), Chapters 6, 8 and 10, and Evertse and Győry (2022), Chapters 2 and 4.
- Corollary 5.7 was generalized for the 'inhomogeneous' case by Gaál (1986).
- Analogous results were established over function fields by Győry (1984, 2000), Gaál (1988), Mason (1988), Shlapentokh (1996).

9.1.2. *Results over finitely generated domains.*

We now present two general finiteness theorems where the ground ring is an integrally closed integral domain A of characteristic 0 that is finitely generated over $\mathbb{Z}$ as a $\mathbb{Z}$-algebra, i.e., $A = \mathbb{Z}[z_1, \ldots, z_r]$, where we allow some of the z_i to be transcendental.

We say that the monic polynomials $f, g \in A[X]$ are *strongly A-equivalent* if $g(X) = f(X+a)$ with some $a \in A$. Then f and g have the same discriminant.

Theorem 9.8 (Győry, 1982)**.** *Let G be a finite extension of the quotient field of A. Up to strong A-equivalence, there are only finitely many monic $f(X)$ in $A[X]$ with given non-zero discriminant δ having all their zeros in G.*

This was made effective by Győry (1984) in a special case, and in full generality by Evertse and Győry (2017), provided that A, G and δ are given effectively in the sense defined in Evertse and Győry (2017, 2022).

Theorem 9.9 (Evertse and Győry, 2017, 2022)**.** *Let A, G, δ be as above. Up to strong A-equivalence, there are only finitely many monic $f(X)$ in $A[X]$ with $D(f) = \delta$, and if A, G, δ are effectively given, all these f can be effectively determined.*

Problem 2. *Are Theorems 9.8 and 9.9 true without fixing the splitting field G?*

Several results of the theory have been extended to the case of étale algebras in Evertse and Győry (2017, 2022).

- Let K be a number field with ring of integers $\mathcal{O}_K$, and $D \neq 0$ an integer. As was seen above, up to strong $\mathbb{Z}$-equivalence, the equation

$$D(\alpha) = D \text{ in } \alpha \in \mathcal{O}_K \tag{9.2}$$

has only finitely many solutions, and all of them can be effectively determined.

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be an integral domain of characteristic 0 with algebraic or transcendental generators $z_1, \ldots, z_r$, L its quotient field, and Ω a *finite étale L-algebra* (i.e., a direct product of finite extensions $K_1, \ldots, K_t$ of L). Denote by A_Ω the integral closure of A in Ω. The *discriminant* of $\alpha \in A_\Omega$ over L with $\Omega = L[\alpha]$ is given by $D_L(\alpha) := D(f_{\alpha,L})$, where $f_{\alpha,L}$ is the monic minimal polynomial of α over L.

Let $\mathcal{O}$ be an *A-order* of Ω, i.e. an A-subalgebra of A_Ω which spans Ω as an L-vector space. We say that $\alpha, \beta \in \mathcal{O}$ are *strongly A-equivalent* if

$\beta - \alpha \in A$. One verifies that if $\alpha, \beta \in \mathcal{O}$ are strongly A-equivalent then $f_{\alpha,L}$, $f_{\beta,L}$ are also strongly A-equivalent, and thus, $D_L(\beta) = D_L(\alpha)$.

Let δ be a non-zero element of L. Consider the following generalization of equation (9.2):

$$D_L(\alpha) = \delta \text{ in } \alpha \in \mathcal{O}. \tag{9.3}$$

For an integral domain B, denote by B^+ the additive group of B.

Theorem 9.10 (Evertse and Győry, 2022)**.** *If*

$$(\mathcal{O} \cap L)^+/A^+ \text{ is finite,} \tag{9.4}$$

then the set of $\alpha \in \mathcal{O}$ with (9.3) *is a union of finitely many strong A-equivalence classes. Moreover, if $A, \Omega, \mathcal{O}$ and δ are given effectively in a well-defined way, one can determine a set consisting of precisely one element from each of these classes.*

The condition (9.4) is necessary and decidable.

For $A = \mathbb{Z}$, $L = \mathbb{Q}$, $\Omega =$ number field K, $\mathcal{O} = \mathcal{O}_K$, Theorem 9.10 gives the above theorem concerning equation (9.2).

9.2. **Generalizations: the non-monic case.**
As was seen above, Theorem 4.2 (ii) and its consequences in Sections 4 and 5 were later extended to the number field case and $\mathfrak{p}$-adic case. Theorem 4.4 was already generalized for the same generality by the authors in the first paper on the subject, in Evertse and Győry (1991a).

We present now this general theorem from the non-monic case which corresponds to Theorem 9.1 above.

Keeping the above notations, let again L be a number field, and S a finite set of places on L containing all infinite places. We denote by $\mathcal{O}_S$ the ring of S-integers and by $\mathcal{O}_S^*$ the group of S-units. Two polynomials $f, g \in \mathcal{O}_S[X]$ of degree n are said to be $GL_2(\mathcal{O}_S)$-*equivalent* if

$$g(X) = \varepsilon(cX+d)^n f\left(\frac{aX+b}{cX+d}\right) \text{ with some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}_S) \text{ and } \varepsilon \in \mathcal{O}_S^*.$$

As above, for a polynomial $g(X) \in \overline{\mathbb{Q}}[X]$ we denote by $H(g)$ the absolute height of the vector whose coordinates are the coefficients of g.

Theorem 9.11 (Evertse and Győry, 1991a)**.** *Let $\delta \in \mathcal{O}_S \setminus \{0\}$, and let $f \in \mathcal{O}_S[X]$ be a polynomial of degree $n \geq 2$ and of discriminant $D(f) \in \delta\mathcal{O}_S^*$.*

Then f is $GL_2(\mathcal{O}_S)$-equivalent to a polynomial $g \in \mathcal{O}_S[X]$ such that

$$H(g) < C_7(L, S, (\delta)_S, n),$$

where C_7 is an effectively computable number, given explicitly in terms of $L, S, (\delta)_S$ and n.

For $L = \mathbb{Q}, \mathcal{O}_S = \mathbb{Z}$, when $\mathcal{O}_S^* = \{\pm 1\}$, Theorem 9.11 gives Theorem 4.4. For the best known, completely explicit bound C_7, see Theorem 14.2.2 in Evertse and Győry (2017).

The binary form variant of Theorem 4.4 was later generalized for decomposable forms in more than two variables in Evertse and Győry (1992) and Győry (1994).

Let K be an extension of L of degree $n \geq 3$. Let α be a primitive element of K/L, i.e., $K = L(\alpha)$. We would have liked to define the discriminant of α over $\mathcal{O}_S$ to be the discriminant of f, where f is a minimal polynomial of α in $\mathcal{O}_S[X]$ whose coefficients generate the unit ideal. But in case that $\mathcal{O}_S$ is not a principal ideal domain, such a minimal polynomial need not exist. Instead, we give a more subtle definition. Denote by $\mathcal{P}_S(\alpha)$ the set of polynomials $f \in \mathcal{O}_S[X]$ such that f is irreducible in $L[X]$ and $f(\alpha) = 0$, and define the discriminant ideal of α with respect to $\mathcal{O}_S$ by

$$\mathfrak{d}_S(\alpha) := (D(f) : \ f \in \mathcal{P}_S(\alpha))_S.$$

Given $f(X) = a_0X^n + \cdots + a_n \in \mathcal{P}_S(\alpha)$, let $\mathfrak{c}_S(f) := (a_0, \ldots, a_n)_S$ denote its content. Then

$$\mathfrak{d}_S(\alpha) = D(f) \cdot \mathfrak{c}_S^{2-2n}. \tag{9.5}$$

Two elements α, β of K are called $GL_2(\mathcal{O}_S)$-equivalent if $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathcal{O}_S)$; such elements satisfy $\mathfrak{d}_S(\alpha) = \mathfrak{d}_S(\beta)$.

Theorem 9.11 has the following consequence.

Theorem 9.12. *Let α with $K = L(\alpha)$. Then α is $GL_2(\mathcal{O}_S)$-equivalent to an element $\beta \in K$ with*

$$H(\beta) \leq C_8(L, S, \mathfrak{d}_S(\alpha), n),$$

where C_8 is an effectively computable number, which can be given explicitly in terms of $L, S, \mathfrak{d}_S(\alpha)$ and n.

Idea of proof. Choose a finite set of ideals of $\mathcal{O}_S$ that form a full system of representatives for the ideal classes of $\mathcal{O}_S$. This depends only on L and S. There is $f \in \mathcal{P}_S(\alpha)$ such that $\mathfrak{c}_S(f) = \mathfrak{a}$, where $\mathfrak{a}$ belongs to this finite set of

ideals. By Theorem 9.11, there is $g \in \mathcal{O}_S[X]$, $GL_2(\mathcal{O}_S)$-equivalent to f, such that

$$H(g) < C_7(L, S, (D(f))_S, n) = C_7(L, S, \mathfrak{a}^{2n-2}\mathfrak{d}_S(\alpha), n).$$

Now g has a zero β that is $GL_2(\mathcal{O}_S)$-equivalent to α, and for this β we have $H(\beta) < C_8(L, S, \mathfrak{d}_S(\alpha), n)$. □

10. Multiply monogenic and rationally monogenic orders

In this section we consider 'Diophantine equations'

$$\mathbb{Z}[\alpha] = \mathcal{O} \text{ in algebraic integers } \alpha, \tag{10.1}$$

$$\mathbb{Z}_\alpha = \mathcal{O} \text{ in algebraic numbers } \alpha, \tag{10.2}$$

where $\mathcal{O}$ is a given order of a number field K. As observed before, from the effective reduction theory for polynomials one can deduce effective finiteness results for the collection of $\mathbb{Z}$-equivalence classes of algebraic integers α with (10.1), respectively the collection of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of algebraic numbers α with (10.2). Although this does not strictly belong to the effective reduction theory for polynomials, in this section, we give an overview of results with upper bounds for the *number* of these classes, i.e., for the multiplicity of (rational) monogenicity for the order $\mathcal{O}$ under consideration. An important feature of these bounds is their uniformity, i.e., they depend at most on the degree of K. We have included outlines of the proofs of the main results. The main tools are upper bounds for the number of solutions of equations $ax + by = 1$ in algebraic units x, y.

10.1. **Monogenic orders.**

In this subsection, we consider (10.1). Let K be a number field with ring of integers $\mathcal{O}_K$, and $\mathcal{O}$ an arbitrary order of K, i.e., a subring of $\mathcal{O}_K$ with quotient field K. It follows from Theorem 5.6 above (in an effective form) that up to $\mathbb{Z}$-equivalence, there are only finitely many $\alpha \in \mathcal{O}$ with $\mathcal{O} = \mathbb{Z}[\alpha]$. The order $\mathcal{O}$ is said to be *k-times monogenic/precisely k times monogenic/at most k times monogenic* if there are at least/precisely/at most k pairwise $\mathbb{Z}$-inequivalent such generators α of $\mathcal{O}$ over $\mathbb{Z}$.

It is easy to see that every order of a quadratic number field is precisely one time monogenic.

For fixed $n \geq 3$, we denote by $M(n)$ the smallest integer k such that for every number field K of degree n and every order $\mathcal{O}$ of K, the order $\mathcal{O}$ is at most k times monogenic. We start with recalling an old result of ours.

Theorem 10.1 (Evertse and Győry, 1985). *Let K be a number field of degree $n \geq 3$, and suppose that its normal closure has degree g. Then every order of K is at most $(3 \times 7^{2g})^{n-2}$ times monogenic.*

In particular, $M(n)$ is finite, and $M(n) \leq (3 \times 7^{2n!})^{n-2}$.

This was deduced from an upper bound for the number of solutions of S-unit equations, obtained shortly before by the first author, see Evertse (1984a).

There are now much better upper bounds for $M(n)$. The problem of estimating $M(3)$ can be reduced via index form equations to estimating the number of integer solutions of a Thue equation $|F(x,y)| = 1$ with F an integral cubic binary form. Bennett (2001) proved that such an equation has up to sign at most 10 solutions. This gives the following.

Theorem 10.2 (Bennett, 2001). *We have $M(3) \leq 10$.*

For $n \geq 4$, the first author improved the bound of Theorem 10.1 as follows.

Theorem 10.3 (Evertse, 2011). *For $n \geq 4$, $M(n) \leq 2^{4(n+5)(n-2)}$ holds.*

The main tool in the proof is an important improvement and generalization of the first author's result from 1984, due to Beukers and Schlickewei (1996), see Theorem 10.6 in Section 10.2.

In the case of quartic number fields, Bhargava (2022) substantially improved Evertse's bound by proving the following theorem.

Theorem 10.4 (Bhargava, 2022). *We have $M(4) \leq 2760$ (and $M(4) \leq 182$ if $|D(\mathcal{O})|$ is sufficiently large).*

Bhargava proved his theorem via a parametrization of quartic rings and their cubic resolvent rings, and utilized Akhtari's recent upper bound (see the Appendix of Bhargava (2022)) for the number of solutions of quartic Thue equations.

Akhtari (2022) gave another, more direct proof for Theorem 10.4, following the approach of Gaál, Pethő and Pohst (1996) (which in fact is going into the same direction as Bhargava's approach but is less general), and combining this with her own upper bound for the number of solutions of quartic Thue equations.

Theorem 10.3 is probably far from best possible in terms of n. We pose the following problem:

Problem 3 (Győry, 2000). *Do there exist absolute constants c_1, c_2 such that $M(n) < c_1 n^{c_2}$ for all $n \geq 4$?*

The best lower bound we could find is due to Miller-Sims and Robertson (2005). Let p be a prime number, ζ_p a primitive p-th root of unity, and K_p the associated real cyclotomic field, i.e., $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Then K_p has degree $(p-1)/2$, and its ring of integers is $\mathcal{O}_p := \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. They proved that if $p \geq 7$ then $\mathbb{Z}[\alpha] = \mathcal{O}_p$ is satisfied by $\alpha = \zeta_p^k + \zeta_p^{-k}$, $(\zeta_p^k + \zeta_p^{-k} + b)^{-1}$ $(b = -1, 0, 1, 2,\ k = 1, \ldots, (p-1)/2)$. If $p = 7$ then among these numbers there are precisely nine pairwise $\mathbb{Z}$-inequivalent ones and by a result of Gaál and Schulte (1989) these are up to $\mathbb{Z}$-equivalence the only numbers α with $\mathbb{Z}[\alpha] = \mathcal{O}_7$. If $p \geq 11$ then all these numbers are pairwise $\mathbb{Z}$-inequivalent and thus, the order $\mathcal{O}_p$ is $5(p-1)/2 = 5[K_p : \mathbb{Q}]$ times monogenic.

We now fix a number field K of degree ≥ 3, and consider only orders of K. As it turned out, most orders of K have only small multiplicity of monogenicity, bounded above independently even of the degree of K. In 2013, we proved the following result with Bérczes:

Theorem 10.5 (Bérczes, Evertse and Győry, 2013). *Let K be an algebraic number field of degree ≥ 3. Then K has only finitely many orders that are three times monogenic.*

To see that this is optimal, let K be a non-CM number field of degree ≥ 3. Then the ring of integers of K has infinitely many units ε with $K = \mathbb{Q}(\varepsilon)$. For every of these ε we obtain a two times monogenic order $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$ of K.

Theorem 10.5 is proved by means of a reduction to unit equations in more than two unknowns, and a use of ineffective finiteness theorems for these equations. So Theorem 10.5 is ineffective, in the sense that its proof does not allow to determine the exceptional orders.

Problem 4. *Make Theorem 10.5 effective.*

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

10.2. Outlines of the proofs of Theorems 10.3 and 10.5.

We start with recalling some auxiliary results from the literature.

Theorem 10.6 (Beukers and Schlickewei, 1996). *Let F be a field of characteristic 0, and Γ a multiplicative subgroup of $F^* \times F^*$ of rank r. Then the equation $x + y = 1$ has at most 2^{8r+8} solutions $(x, y) \in \Gamma$.*

Corollary 10.7. *Let F be a field of characteristic 0, let $m \geq 1$, and let Γ be a multiplicative subgroup of $(F^*)^{2m}$ of rank r. Then there are at most $2^{8(r+2m-1)}$ tuples $(x_1, y_1, \ldots, x_m, y_m) \in \Gamma$ satisfying*

$$x_i + y_i = 1 \quad \text{for } i = 1, \ldots, m. \tag{10.3}$$

This result is easily deduced from Theorem 10.6 using induction on m, see Evertse (2011), or Evertse and Győry (2017), Corollary 4.3.5.

Theorem 10.8. *Let F be a field of characteristic 0, let $m \geq 1$, and let Γ be a multiplicative subgroup of $(F^*)^m$. Then there are at most finitely many tuples $(x_1, \ldots, x_m) \in \Gamma$ satisfying*

(10.4)

$$\begin{cases} x_1 + \cdots + x_m = 1, \\ x_{i_1} + \cdots + x_{i_t} \neq 0 \text{ for each non-empty subset } \{i_1, \ldots, i_t\} \text{ of } \{1, \ldots, m\}. \end{cases}$$

This was proved by Evertse (1984b) and van der Poorten and Schlickewei (1982, 1991), combining Schmidt's and Schlickewei's Subspace Theorem from Diophantine approximation with a specialization argument. We note that Theorem 10.8 is ineffective, hence so are its consequences. Although we will not need these here, we mention that there are explicit upper bounds for the number of solutions of (10.4) depending only on m and on $r := \operatorname{rank} \Gamma$, see Evertse, Schlickewei and Schmidt (2002) or Amoroso and Viada (2009), who obtained the up to now best upper bound $(8m)^{4m^4(m+r+1)}$.

Theorem 10.9. *Let F be a field of characteristic 0, and Γ a multiplicative subgroup of $F^* \times F^*$. Then there are only finitely many pairs $(a, b) \in F^* \times F^*$ such that $a + b = 1$, and such that $ax + by = 1$ has three solutions $(x, y) \in \Gamma$, the pair $(1, 1)$ included.*

Idea of proof. This is basically a result of Evertse, Győry, Stewart, and Tijdeman (1988), see also Evertse and Győry (2015), Theorem 6.1.6. The idea is as follows. Suppose that there are $(x_1, y_1), (x_2, y_2) \in \Gamma$, distinct from each other and distinct from $(1, 1)$, such that $ax_i + by_i = 1$ for $i = 1, 2$. Then

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \end{vmatrix} = 0.$$

Expand the determinant, divide by a term to obtain a five term sum equal to 1, consider all possible partitions into minimal vanishing subsums, and apply Theorem 10.8 to each of them. □

Let K be a number field of degree $n \geq 3$. Denote by $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings of K in G, where G is the normal closure of K. For α with $\mathbb{Q}(\alpha) = K$ and $i = 3, \ldots, n$, define

$$x_i(\alpha) = \frac{\alpha^{(i)} - \alpha^{(1)}}{\alpha^{(2)} - \alpha^{(1)}}, \quad y_i(\alpha) = \frac{\alpha^{(2)} - \alpha^{(i)}}{\alpha^{(2)} - \alpha^{(1)}}$$

and the tuple

$$\kappa(\alpha) := (x_3(\alpha), y_3(\alpha), \ldots, x_n(\alpha), y_n(\alpha)).$$

In addition, we need a few simple lemmas. We call α, β $\mathbb{Q}$-equivalent if $\beta = \lambda\alpha + a$ for some $\lambda \in \mathbb{Q}^*$, $a \in \mathbb{Q}$.

Lemma 10.10. *Let α, β with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$.*

(i) $\kappa(\alpha) = \kappa(\beta) \iff \alpha, \beta$ are $\mathbb{Q}$-equivalent.

(ii) Assume in addition that $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ and that α, β are $\mathbb{Q}$-equivalent. Then α, β are $\mathbb{Z}$-equivalent.

Proof. (i) Clearly, $\kappa(\alpha) = \kappa(\beta)$ if and only if $(\alpha^{(i)}, \beta^{(i)})$ $(i = 1, \ldots, n)$ are collinear, i.e., $\beta^{(i)} = \lambda\alpha^{(i)} + a$ $(i = 1, \ldots, n)$ for some $\lambda \in G^*$, $a \in G$. One easily shows that this is posible only if λ, a are invariant under Galois action, i.e., lie in $\mathbb{Q}$.

(ii) Our assumption $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ implies that $\beta = f(\alpha)$ for some unique polynomial $f \in \mathbb{Q}[X]$ of degree $< n$, and then $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ implies $f \in \mathbb{Z}[X]$. So if α, β are $\mathbb{Q}$-equivalent, then $\beta = \lambda\alpha + a$ with $\lambda, a \in \mathbb{Z}$. By interchanging the role of α, β we see that $\lambda^{-1} \in \mathbb{Z}$, hence $\lambda = \pm 1$. □

Lemma 10.11. *Let α, β be such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ and $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$. Then*

$$\frac{\beta^{(i)} - \beta^{(j)}}{\alpha^{(i)} - \alpha^{(j)}} \in \mathcal{O}_G^* \text{ for } i, j = 1, \ldots, n,\ i \neq j.$$

Proof. Use $\beta = f(\alpha)$, $\alpha = g(\beta)$ for some $f, g \in \mathbb{Z}[X]$. □

Sketch of the proof of Theorem 10.3. Let $\mathcal{O}$ be an order of K. Note that for $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$ we have relations

$$x_i(\alpha) + y_i(\alpha) = 1 \quad (i = 3, \ldots, n)$$

where

$$x_i(\alpha) = \frac{\alpha^{(i)} - \alpha^{(1)}}{\alpha^{(2)} - \alpha^{(1)}}, \quad y_i(\alpha) = \frac{\alpha^{(2)} - \alpha^{(i)}}{\alpha^{(2)} - \alpha^{(1)}}.$$

It was proved in Evertse (2011), see also Evertse and Győry (2017), pages 206–208, that if one restricts to α with $\mathbb{Z}[\alpha] = \mathcal{O}$, then the set of tuples

$$\{\kappa(\alpha) : \mathbb{Z}[\alpha] = \mathcal{O}\}$$

generates a multiplicative subgroup of $(G^*)^{2n-4}$ of rank at most $n(n-1)/2$. In the deduction of this we used a refinement of Lemma 10.11. Now an application of Corollary 10.7 and Lemma 10.10 implies Theorem 10.3. □

In the proof of Theorem 10.5 we need the following lemma. Call α_1 k-special if $\alpha_1 \in O_K$, $K = \mathbb{Q}(\alpha_1)$ and there are $\alpha_2, \ldots, \alpha_k$ such that $\alpha_1, \ldots, \alpha_k$ are pairwise $\mathbb{Z}$-inequivalent and $\mathbb{Z}[\alpha_1] = \mathbb{Z}[\alpha_2] = \cdots = \mathbb{Z}[\alpha_k]$.

Lemma 10.12. *Let $\mathcal{C}$ be a $\mathbb{Q}$-equivalence class of 2-special numbers. Then $\mathcal{C}$ is the union of finitely many $\mathbb{Z}$-equivalence classes.*

Proof. For the somewhat involved argument we refer to Bérczes, Evertse and Győry (2013) or Evertse and Győry (2017), Lemma 9.5.6. □

Sketch of the proof of Theorem 10.5. We have to prove that there are only finitely many orders $\mathbb{Z}[\alpha]$ such that α is 3-special. It suffices to show that the 3-special α lie in finitely many $\mathbb{Z}$-equivalence classes. We sketch the argument.

Let $\alpha \in O_K$ be 3-special. Pick β, γ such that α, β, γ are pairwise $\mathbb{Z}$-inequivalent, and $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta] = \mathbb{Z}[\gamma]$. For any three distinct indices i, j, k from $\{1, \ldots, n\}$, define

$$\varepsilon_{ijk} = \frac{(\beta^{(i)} - \beta^{(j)})/(\beta^{(i)} - \beta^{(k)})}{(\alpha^{(i)} - \alpha^{(j)})/(\alpha^{(i)} - \alpha^{(k)})}, \quad \eta_{ijk} = \frac{(\gamma^{(i)} - \gamma^{(j)})/(\gamma^{(i)} - \gamma^{(k)})}{(\alpha^{(i)} - \alpha^{(j)})/(\alpha^{(i)} - \alpha^{(k)})}.$$

Then by Lemma 10.11, the equation

$$\frac{\alpha^{(i)} - \alpha^{(j)}}{\alpha^{(i)} - \alpha^{(k)}} x + \frac{\alpha^{(j)} - \alpha^{(k)}}{\alpha^{(i)} - \alpha^{(k)}} y = 1 \quad \text{in } x, y \in \mathcal{O}_G^*$$

has three solutions

$$(1, 1), \ (\varepsilon_{ijk}, \varepsilon_{kji}), \ (\eta_{ijk}, \eta_{kji}).$$

If for all i, j, k and all α, β, γ as above these three solutions were distinct, we could conclude from Theorem 10.9 that there is a finite set $\mathcal{S}$ such that $\alpha^{(i,j,k)} \in \mathcal{S}$ for all i, j, k and all 3-special α. It need not be true, however, that in all cases these three solutions are distinct. However, by means of a combinatorial argument, worked out in Bérczes, Evertse and Győry (2013) or Evertse and Győry (2017), pp. 211–216 we deduce that the existence of

a finite set $\mathcal{S}$ as above still holds. Now Lemma 10.10 (i) implies that the 3-special numbers α lie in only finitely many $\mathbb{Q}$-equivalence classes. Finally, Lemma 10.12 implies that the 3-special numbers lie in only finitely many $\mathbb{Z}$-equivalence classes. □

10.3. **Generalizations for rationally monogenic orders.**
The theorems stated in Subsection 10.1 have analogues for rationally monogenic orders. For the necessary terminology and properties we refer to Subsection 5.6.

For a not necessarily integral algebraic number α of degree $n \geq 3$ we define

$$\mathcal{M}_\alpha := \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} : x_0, \ldots, x_{n-1} \in \mathbb{Z}\},$$
$$\mathbb{Z}_\alpha := \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}.$$

Recall that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ if α and β are $GL_2(\mathbb{Z})$-equivalent.

An order $\mathcal{O}$ of a number field K is called *rationally monogenic* if $\mathcal{O} = \mathbb{Z}_\alpha$ for some algebraic number α. As observed in Subsection 5.6, if α is an algebraic integer, then $\mathbb{Z}_\alpha = \mathbb{Z}[\alpha]$. Thus, monogenic orders are rationally monogenic. We further recall that rationally monogenic orders are primitive, i.e., they cannot be expressed as $\mathbb{Z} + a\mathcal{O}'$ for some integer $a > 1$ and order $\mathcal{O}'$.

We say that an order $\mathcal{O}$ of a number field K is *k times/precisely k times/at most k-times rationally monogenic* if up to $GL_2(\mathbb{Z})$-equivalence there are at least/precisely/at most k numbers α such that $\mathcal{O} = \mathbb{Z}_\alpha$. Denote by $RM(n)$ the least number k such that for every number field K of degree n and every order $\mathcal{O}$ of K, the order $\mathcal{O}$ is at most k times rationally monogenic.

From work of Delone and Faddeev (1940) it follows that $RM(3) \leq 1$, that is, every order of a cubic number field is at most one time rationally monogenic (and in fact precisely one time if the order is primitive). From a result of Bérczes, Evertse and Győry (2004) the following analogue of Theorem 10.3 can be deduced:

Theorem 10.13. *For every $n \geq 4$, $RM(n)$ is finite and in fact, $RM(n) \leq n \times 2^{24n^3}$.*

Similarly to Theorem 10.3 the proof uses Theorem 10.6 of Beukers and Schlickewei (1996) mentioned above.

This bound has been improved. The best bounds to date are as follows:

Theorem 10.14. *We have*

(i) $RM(4) \leq 40$ *(Bhargava (2022));*
(ii) $RM(n) \leq 2^{5n^2}$ *for* $n \geq 5$ *(Evertse and Győry (2017)).*

The proof of part (ii) is similar to that of Theorem 10.13 but with a combinatorial improvement in the argument. The proof of part (i) also uses a parametrization of quartic rings and their cubic resolvent rings.

Recently, the following analogue of Theorem 10.5 for rationally monogenic orders was proved:

Theorem 10.15 (Evertse, 2023)**.**

(i) Let K be a number field of degree 4. Then K has only finitely many three times rationally monogenic orders.
(ii) Let K be a number field of degree ≥ 5 such that the normal closure of K is 5-transitive. Then K has only finitely many two times rationally monogenic orders.

Part (i) is best possible in the sense that there are quartic number fields having infinitely many two times rationally monogenic orders. In fact, Bérczes, Evertse and Győry (2013, end of Section 1) give the following construction:

Let r, s be integers such that $f(X) = (X^2 - r)^2 - X - s$ is irreducible, and let $K = \mathbb{Q}(\alpha)$, where α is a root of f. Then K has infinitely many orders $\mathcal{O}_m$ $(m = 1, 2, \ldots)$ with the following property: $\mathcal{O}_m = \mathbb{Z}[\alpha_m] = \mathbb{Z}[\beta_m]$, where $\beta_m = \alpha_m^2 - r_m$, $\alpha_m = \beta_m^2 - s_m$ for some integers r_m, s_m.

It is clear that α_m, β_m in the above theorem are not $\mathrm{GL}_2(\mathbb{Z})$-equivalent. We would like to pose the following problem:

Problem 5. *Does every quartic number field have infinitely many orders that are two times rationally monogenic? If not, can we characterize those quartic number fields that do? Do the two times rationally monogenic orders have a particular structure?*

Similary to Theorem 10.5, Theorem 10.15 has been proved by means of a reduction to unit equations in more than two unknowns, and a use of ineffective finiteness theorems for such equations. So likewise, Theorem 10.15 is ineffective.

It is not clear whether the 5-transitivity condition on the Galois closure of K in part (ii) is necessary; this was just a technical condition needed for the proof. We are interested in the following problem:

Problem 6. *Is it true that every number field of degree $n \geq 5$ has only finitely many orders that are two times rationally monogenic? If not, can we characterize those number fields that do?*

Combining Theorems 5.11 and 10.15 one can deduce the following counterpart of Theorem 3.4. For a number field K, let $\mathcal{PI}(K)$ denote the set of primitive, irreducible polynomials in $\mathbb{Z}[X]$ having a root α such that $K = \mathbb{Q}(\alpha)$.

Corollary 10.16 (Evertse, 2023)**.**

(i) Let K be a quartic number field. Then $\mathcal{PI}(K)$ has only finitely many Hermite equivalence classes that split into more than two $GL_2(\mathbb{Z})$-equivalence classes.

(ii) Let K be a number field of degree ≥ 5 whose normal closure is 5-transitive. Then $\mathcal{PI}(K)$ has only finitely many Hermite equivalence classes that split into more than one $GL_2(\mathbb{Z})$-equivalence class.

Part (ii) was conjectured in BEGyRS (2023), without the 5-transitivity condition.

10.4. **Outlines of the proofs of Theorems 10.14 (ii) and 10.15.** The main new tool is the following result.

Theorem 10.17. *Let F be a field of characteristic 0, and Γ a finitely generated subgroup of F^*. Then there is a finite subset $\mathcal{S}$ of F^* with $1 \in \mathcal{S}$, such that for the set of solutions $(x_1, x_2, x_3, y_1, y_2, y_3) \in \Gamma^6$ of*

$$(x_1 - 1)(x_2 - 1)(x_3 - 1) = (y_1 - 1)(y_2 - 1)(y_3 - 1) \tag{10.5}$$

at least one of the following holds:

(i) *at least one of $x_1, \ldots, y_3$ belongs to $\mathcal{S}$;*
(ii) *there are $\eta_1, \eta_2, \eta_3 \in \{\pm 1\}$ such that (y_1, y_2, y_3) is a permutation of $(x_1^{\eta_1}, x_2^{\eta_2}, x_3^{\eta_3})$;*
(iii) *one of the numbers in $\{x_i x_j,\ x_i/x_j,\ y_i y_j,\ y_i/y_j : 1 \leq i < j \leq 3\}$ is equal to either -1, or to a primitive cube root of unity.*

Proof. This is Proposition 8.1 of Bérczes, Evertse and Győry (2013). The proof is basically to expand (10.5), divide by one term to get an equation of type (10.4) in 16 terms equal to 1, consider all possible partitions into minimal vanishing subsums, and apply Theorem 10.8 to each of them (by using symmetric properties we can substantially reduce the number of cases). □

We need some other lemmas. Let K be a number field of degree $n \geq 4$. Denote by G the normal closure of K and by $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$ the embeddings of K in G. For α with $\mathbb{Q}(\alpha) = K$ we define the *cross ratios*

$$\mathrm{cr}_{ijkl}(\alpha) := \frac{(\alpha^{(i)} - \alpha^{(j)})(\alpha^{(k)} - \alpha^{(l)})}{(\alpha^{(i)} - \alpha^{(k)})(\alpha^{(j)} - \alpha^{(l)})}$$

for any four distinct indices $i, j, k, l \in \{1, \ldots, n\}$ and we define the tuple

$$\lambda(\alpha) := (\mathrm{cr}_{123i}(\alpha), \mathrm{cr}_{1i32}(\alpha) : i = 4, \ldots, n).$$

We call $\alpha, \beta \in K$ $GL_2(\mathbb{Q})$-equivalent if $\beta = \frac{a\alpha+b}{c\alpha+d}$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$.

Lemma 10.18. *Let α, β with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$.*
(i) $\lambda(\alpha) = \lambda(\beta) \iff \alpha, \beta$ are $GL_2(\mathbb{Q})$-equivalent.
(ii) If $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$ and α, β are $GL_2(\mathbb{Q})$-equivalent, then α, β are $GL_2(\mathbb{Z})$-equivalent.

Proof. (i). $\Longleftarrow$ is straighforward. As for $\Longrightarrow$, from elementary projective geometry it follows that if $\lambda(\alpha) = \lambda(\beta)$ then there is a projective transformation of $\mathbb{P}^1$ defined over G that maps $\alpha^{(i)}$ to $\beta^{(i)}$, for $i = 1, \ldots, n$. It is easy to verify that this projective transformation is invariant under Galois action, hence defined over $\mathbb{Q}$.

(ii). See for instance Lemma 2.6 of Evertse (2023). □

Lemma 10.19. *Let α, β with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ and $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$. Then for all distinct $i, j, k, l \in \{1, \ldots, n\}$ we have $\mathrm{cr}_{ijkl}(\beta)/\mathrm{cr}_{ijkl}(\alpha) \in \mathcal{O}_G^*$.*

Proof. This is Lemma 2.4 of Evertse (2023). □

Sketch of the proof of Theorem 10.14 (ii). Let $\mathcal{O}$ be an order of K. Note that for $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$ we have relations

$$\mathrm{cr}_{123i}(\alpha) + \mathrm{cr}_{1i32}(\alpha) = 1 \quad (i = 4, \ldots, n).$$

By Lemma 17.7.3 of Evertse and Győry (2017), the set of tuples

$$\{\lambda(\alpha) : \mathbb{Z}_\alpha = \mathcal{O}\}$$

generates a multiplicative subgroup of $(G^*)^{2n-6}$ of rank at most $n(n-1)/2$. In the deduction of this we used a refinement of Lemma 10.19. Now an application of Corollary 10.7 and Lemma 10.18 implies Theorem 10.14 (ii). □

Call α_1 with $\mathbb{Q}(\alpha_1) = K$ *k-special* if there are $\alpha_2, \dots, \alpha_k \in K$ such that $\alpha_1, \dots, \alpha_k$ are pairwise $GL_2(\mathbb{Z})$-inequivalent and $\mathbb{Z}_{\alpha_1} = \cdots = \mathbb{Z}_{\alpha_k}$. We should mention here that if K has degree 3 then there are no 2-special numbers in K.

In the proof of Theorem 10.15, we need the following lemma.

Lemma 10.20. *Assume $n \geq 4$. Let $\mathcal{C}$ be a $GL_2(\mathbb{Q})$-equivalence class of 2-special numbers. Then $\mathcal{C}$ is the union of finitely many $GL_2(\mathbb{Z})$-equivalence classes.*

Idea of proof. This is Proposition 5.1 of Evertse (2023). Its proof is fairly complicated. We give a brief outline.

We define $\mathrm{cr}_{ijkl}(\mathcal{C}) := \mathrm{cr}_{ijkl}(\alpha)$ for any $\alpha \in \mathcal{C}$. This is well-defined since $GL_2(\mathbb{Q})$-equivalent algebraic numbers have the same cross ratios. Let $\alpha \in \mathcal{C}$, let $\beta \in K$ be such that $\mathbb{Z}_\beta = \mathbb{Z}_\alpha$ and β is not $GL_2(\mathbb{Z})$-equivalent to α, and let $\mathcal{D}$ be the $GL_2(\mathbb{Q})$-equivalence class of β. Then $\mathcal{D} \neq \mathcal{C}$ by Lemma 10.18 (ii). Clearly, $\mathrm{cr}_{ijkl}(\beta) =: \mathrm{cr}_{ijkl}(\mathcal{D})$ depends only on $\mathcal{D}$. By Lemma 10.19 we have $\mathrm{cr}_{ijkl}(\mathcal{D})/\mathrm{cr}_{ijkl}(\mathcal{C}) \in \mathcal{O}_G^*$ for all i, j, k, l. Further,

$$1 = \mathrm{cr}_{ijkl}(\beta) + \mathrm{cr}_{ilkj}(\beta) = \mathrm{cr}_{ijkl}(\mathcal{C}) \cdot \frac{\mathrm{cr}_{ijkl}(\mathcal{D})}{\mathrm{cr}_{ijkl}(\mathcal{C})} + \mathrm{cr}_{ilkj}(\mathcal{C}) \cdot \frac{\mathrm{cr}_{ilkj}(\mathcal{D})}{\mathrm{cr}_{ilkj}(\mathcal{C})}$$

for all i, j, k, l. Now by Theorem 10.6, for given $\mathcal{C}$ there are only finitely many possible values for each $\mathrm{cr}_{ijkl}(\mathcal{D})$ and thus, by Lemma 10.18, at most finitely many possibilities for $\mathcal{D}$. It follows that $\mathcal{C}$ is the union of finitely many sets

$$\mathcal{C}(\mathcal{D}) := \{\alpha \in \mathcal{C} : \text{ there is } \beta \in \mathcal{D} \text{ with } \mathbb{Z}_\alpha = \mathbb{Z}_\beta\}$$

where $\mathcal{D} \neq \mathcal{C}$ is a $GL_2(\mathbb{Q})$-equivalence class of 2-special numbers. So it suffices to prove that each set $\mathcal{C}(\mathcal{D})$ is the union of finitely many $GL_2(\mathbb{Z})$-equivalence classes.

Now fix $\mathcal{D}$, $\alpha \in \mathcal{C}(\mathcal{D})$, and $\beta \in \mathcal{D}$ such that $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$. Let α' be any other element of $\mathcal{C}(\mathcal{D})$. Then we can write

$$\alpha' = \frac{a\alpha + b}{c\alpha + d} \text{ with } a, b, c, d \in \mathbb{Z},\ \gcd(a, b, c, d) = 1,\ ad - bc =: \Delta \neq 0.$$

We have to prove that the numbers $\alpha' \in \mathcal{C}(\mathcal{D})$ lie in only finitely many $GL_2(\mathbb{Z})$-equivalence classes. Recall that there are $U \in GL_2(\mathbb{Z})$ and $a', b', d' \in \mathbb{Z}$ with $a'd' = \Delta$, $|b'| \leq |d'|/2$ such that $U\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right)$. Hence α' is $GL_2(\mathbb{Z})$-equivalent to $\alpha^* := (a'\alpha + b')/d'$. It suffices to prove that there are only finitely many possibilities for α^*. It is in fact sufficient to prove that Δ is bounded, since for given Δ there are only finitely many possibilities

for (a', b', d'). The boundedness of Δ is provided by the following elementary lemma, which is Proposition 4.1 of Evertse (2023). We refer to that paper for the rather lengthy proof.

Lemma 10.21. *Let D be the discriminant of $\mathbb{Z}_\alpha$, and let $\mathfrak{a}(\alpha,\beta)$ be the ideal of $\mathcal{O}_G$ generated by the numbers $\mathrm{cr}_{ijkl}(\beta)/\mathrm{cr}_{ijkl}(\alpha) - 1$ $(1 \le i < j < k < l \le n)$. Then Δ divides $D^5 \cdot \mathfrak{a}(\alpha,\beta)^2$.*

□

Sketch of the proof of Theorem 10.15. For α, β with $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K$ and distinct $i, j, k, l \in \{1, \dots, n\}$ we put

$$\varepsilon_{ijkl}(\alpha,\beta) := \frac{\mathrm{cr}_{ijkl}(\beta)}{\mathrm{cr}_{ijkl}(\alpha)}.$$

Lemma 10.19 implies that if $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$, then $\varepsilon_{ijkl}(\alpha,\beta) \in \mathcal{O}_G^*$.

The case $n = 4$. We have to show that there are only finitely many orders $\mathcal{O}$ of K such that $\mathcal{O} = \mathbb{Z}_\alpha$ for some 3-special α. It clearly suffices to show that the 3-special numbers α lie in only finitely many $GL_2(\mathbb{Z})$-equivalence classes.

Let $\alpha \in K$ be 3-special, and choose $\beta, \gamma \in K$ such that α, β, γ are pairwise $GL_2(\mathbb{Z})$-inequivalent, and $\mathbb{Z}_\alpha = \mathbb{Z}_\beta = \mathbb{Z}_\gamma$. Let (i, j, k, l) be a permutation of $(1, 2, 3, 4)$. Then the equation

$$\mathrm{cr}_{ijkl}(\alpha)x + \mathrm{cr}_{ilkj}(\alpha)y = 1$$

has three distinct solutions $(x, y) \in \mathcal{O}_G^* \times \mathcal{O}_G^*$, i.e., $(1, 1)$, $(\varepsilon_{ijkl}(\alpha,\beta), \varepsilon_{ilkj}(\alpha,\beta))$, $(\varepsilon_{ijkl}(\alpha,\gamma), \varepsilon_{ilkj}(\alpha,\gamma))$. Now Theorem 10.9 implies that $\mathrm{cr}_{ijkl}(\alpha)$ can assume only finitely many values. From Lemma 10.19 it now follows that the 3-special $\alpha \in K$ lie in only finitely $GL_2(\mathbb{Q})$-equivalence classes. Finally, from Lemma 10.20 it follows that they lie in finitely many $GL_2(\mathbb{Z})$-equivalence classes.

The case $n \ge 5$. We have to show that there are only finitely many orders $\mathcal{O}$ of K such that $\mathcal{O} = \mathbb{Z}_\alpha$ for some 2-special α. It clearly suffices to show that the 2-special numbers α lie in only finitely many $GL_2(\mathbb{Z})$-equivalence classes.

Let $\alpha \in K$ be 2-special, and choose β such that α, β are $GL_2(\mathbb{Z})$-inequivalent and $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$. Henceforth, we write ε_{ijkl} for $\varepsilon_{ijkl}(\alpha,\beta)$. Let i, j, k, l be distinct

indices from $\{1,\dots,n\}$. Then

$$\mathrm{cr}_{ijkl}(\alpha)+\mathrm{cr}_{ilkj}(\alpha)=1,\quad \mathrm{cr}_{ijkl}(\alpha)\varepsilon_{ijkl}+\mathrm{cr}_{ilkj}(\alpha)\varepsilon_{ilkj}=1,$$

$\varepsilon_{ilkj}/\varepsilon_{ijkl}=\varepsilon_{iljk}$, which imply

$$\mathrm{cr}_{ijkl}(\alpha)=\frac{\varepsilon_{ilkj}-1}{\varepsilon_{ilkj}-\varepsilon_{ijkl}},\quad \mathrm{cr}_{ijkl}(\beta)=\varepsilon_{ijkl}\mathrm{cr}_{ijkl}(\alpha)=\frac{\varepsilon_{ilkj}-1}{\varepsilon_{iljk}-1}. \tag{10.6}$$

Now picking a fifth index m, and using $\frac{\mathrm{cr}_{jmlk}(\beta)\mathrm{cr}_{ijkm}(\beta)}{\mathrm{cr}_{ijkl}(\beta)}=1$, we obtain

$$\frac{\varepsilon_{jklm}-1}{\varepsilon_{jkml}-1}\cdot\frac{\varepsilon_{imkj}-1}{\varepsilon_{imjk}-1}\cdot\frac{\varepsilon_{iljk}-1}{\varepsilon_{ilkj}-1}=1. \tag{10.7}$$

We apply Theorem 10.17 to (10.7) for all i,j,k,l,m. Our assumption that the Galois group of G is 5-transitive implies various conjugacy relations between the ε_{ijkl}. Using all of these, we infer that for each quadruple i,j,k,l there are only finitely many possible values for ε_{ijkl} (we should mention here that without the 5-transitivity assumption, we do not know how to prove this). Now (10.6) implies that there are only finitely many possible values for $\mathrm{cr}_{ijkl}(\alpha)$, if α runs through the 2-special numbers of α, and thus, by Lemma 10.18, that the 2-special $\alpha\in K$ lie in only finitely many $GL_2(\mathbb{Q})$-equivalence classes. Finally, from Lemma 10.20 it follows that they lie in only finitely many $GL_2(\mathbb{Z})$-equivalence classes. □

Appendix: Related topics

We briefly discuss some further topics related to monogenic number fields and monogenic orders and generalizations thereof that do not strictly belong to the reduction theory of integral polynomials.

A. Monogenicity, class group and Galois group

Recently, surprising results have been obtained in precise and quantitative form that imply that on average, the monogenicity of a number field has an altering effect on the structure of its 2-class group, see Bhargava, Hanke and Shankar (2020), Siad (2021), Swaminathan (2023), Shankar, Siad and Swaminathan (2025), and Bhargava, Shankar and Swaminathan (2025). The 2-class group $Cl_2(K)$ of a number field K is the group of ideal classes of K whose order divides 2.

To illustrate this, we recall some results from the literature. A *monogenized number field* is a pair (K,α) consisting of a number field K and $\alpha\in\mathcal{O}_K$

such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Two monogenized number fields (K_1, α_1), (K_2, α_2) are called isomorphic if there are a field isomorphism $\varphi : K_1 \to K_2$ and a rational integer a such that $\alpha_2 = \pm\varphi(\alpha_1) + a$.

We now restrict ourselves to monogenized cubic fields. We define the height of a monogenized cubic field (K, α) as follows. Let $f = X^3 + aX^2 + bX + c \in \mathbb{Z}[X]$ be the minimal polynomial of α. Then the height of (K, α) is

$$H(K, \alpha) := \max(|P(f)|^3, U(f)^2/4),$$
$$\text{where } P(f) := a^2 - 3b, \quad U(f) := 2a^3 - 9ab + 27c.$$

One can show that isomorphic monogenized cubic fields have the same height. Further, the pair $(P(f), U(f)^2)$ uniquely determines an isomorphism class. Lastly, the discriminant of f is $D(f) = \frac{1}{27}\big(4P(f)^3 - U(f)^2\big)$.

Theorem A.1 (Bhargava, 2005)**.** *Let K run through the cubic number fields, ordered by discriminant.*
(i) The average size of $Cl_2(K)$ over the totally real cubic fields is $5/4$.
(ii) The average size of $Cl_2(K)$ over the complex cubic fields is $3/2$.

Theorem A.2 (Bhargava, Hanke and Shankar, 2020)**.** *Let (K, α) run through the monogenized cubic number fields whose Galois closure has Galois group isomorphic to S_3, ordered by height.*
(i) The average size of $Cl_2(K)$ over the totally real monogenized cubic fields is $3/2$.
(ii) The average size of $Cl_2(K)$ over the complex monogenized cubic fields is 2.

Siad (2021) proved a generalization of the last theorem for number fields of odd degree ≥ 5.

We briefly discuss some other topics. Recently, Arpin, Bozlee, Herr and Smith (2023a,b) introduced and studied twisted monogenic relative extensions K/L. They proved that L has trivial class group (this is the case if e.g. $L = \mathbb{Q}$) if and only if every twisted monogenic extension of L is monogenic.

Another topic worth of study is the connection between (multiplicity of) monogenicity of the ring of integers of a number field K and the size of the Galois group of its Galois closure. The examples of number fields K of degree $n = 3, 4, 5, 6$ in Section 6 show that the multiplicity of monogenicity of $\mathcal{O}_K$ can be relatively large if the Galois group of the Galois closure of K is S_n, i.e. if its size is large relative to n.

B. Distribution of monogenic and non-monogenic number fields

As is well-known, all quadratic number fields and cyclotomic fields are monogenic. For degree $n = 3$, the first example of a non-monogenic number field was given by Dedekind (1878). For every $n \geq 3$, there are infinitely many isomorphism classes of *monogenic*, cf. Kedlaya (2012), and infinitely many isomorphism classes of *non-monogenic* number fields of degree n.

Let K be a number field, and $(1, \omega_2, \ldots, \omega_n)$ an ordered $\mathbb{Z}$-module basis of $\mathcal{O}_K$. Denote by $I(X_2, \ldots, X_n)$ the associated index form, defined by (5.8). Thus, if $\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n$ with $x_1, \ldots, x_n \in \mathbb{Z}$, then $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = |I(x_2, \ldots, x_n)|$. Consequently, K is monogenic if and only if $I(x_2, \ldots, x_n) = \pm 1$ is solvable in $x_2, \ldots, x_n \in \mathbb{Z}$. We say that K has *no local obstruction to being monogenic* if either for every prime number p, the equation $I(x_2, \ldots, x_n) = 1$ has a solution $x_2, \ldots, x_n$ in the p-adic integers, or for every prime number p, the equation $I(x_2, \ldots, x_n) = -1$ has a solution $x_2, \ldots, x_n$ in the p-adic integers. This notion does not depend on the choice of $\omega_2, \ldots, \omega_n$. We recall some recent results.

Theorem B.1 (Alpöge, Bhargava and Shnidman, 2025 , Thm. 1)**.** *Let K run through the isomorphism classes of cubic fields, ordered by their absolute discriminant. Then a positive proportion of them are not monogenic, and yet have no local obstruction to being monogenic.*

Subsequently, but published earlier, the same authors proved the following result for quartic fields. Recall that a number field is called rationally monogenic if its ring of integers is rationally monogenic.

Theorem B.2 (Alpöge, Bhargava and Shnidman, 2024)**.** *For each $r \in \{0, 2, 4\}$, the following holds. Let K run through the isomorphism classes of quartic fields with precisely r real embeddings, ordered by their absolute discriminant. Then a positive proportion of them are not* rationally *monogenic, and yet have no local obstruction to being monogenic.*

This statement differs from Theorem 1 of the paper mentioned. But see sections 4–6 of that paper, where collections of fields are constructed, satisfying the assertion of Theorem B.2.

We recall some recent results concerning *pure* number fields, i.e., number fields of the shape $K_{m,n} := \mathbb{Q}(\alpha)$ with $\alpha^n = m$ for some positive integer n and non-zero integer m. Let $\mathcal{O}_{m,n}$ denote the ring of integers of $K_{m,n}$. We

call $K_{m,n}$ *α-monogenic* if $\mathcal{O}_{m,n} = \mathbb{Z}[\alpha]$ for some α with $\alpha^n = m$. This is a priori stronger than $K_{m,n}$ being monogenic. Recall that the two-sided natural density of an infinite subset A of $\mathbb{Z}$ is defined by

$$\delta(A) := \lim_{X\to\infty} \frac{1}{2X} \cdot \#\big(\{x \in A : |x| \le X\}\big)$$

provided the limit exists. Denote by S_n the set of $m \in \mathbb{Z}$ such that m is square-free and $X^n - m$ is irreducible.

Theorem B.3 (Nguyen-Dang and Hung, 2026)**.** *For every integer $n \ge 4$, the set of m such that $m \in S_n$ and $K_{m,n}$ is α-monogenic has positive two-sided natural density, i.e., $\frac{6}{\pi^2}\prod_{p|n}\frac{p}{p+1}$.*

In a recent preprint, Nguyen-Dang showed that for the fields $K_{m,n}$, in almost all cases, having no local obstruction to being monogenic, monogenicity and α-monogenicity are the same, which is in contrast to Theorems B.1 and B.2.

Theorem B.4 (Nguyen-Dang, 2026)**.** *Let $n \ge 4$ be an integer.*

(i) The set of m such that $m \in S_n$ and $K_{m,n}$ is not α-monogenic but has no local obstruction to being monogenic has two-sided natural density 0*.*

(ii) The set of m such that $m \in S_n$ and $K_{m,n}$ is monogenic but not α-monogenic has two-sided natural density 0*. Consequently, the set of m such that $m \in S_n$ and $K_{m,n}$ is monogenic has two-sided natural density $\frac{6}{\pi^2}\prod_{p|n}\frac{p}{p+1}$.*

For $n = 3, 4, 6$, tables of Gaál (2019) suggest that the density of monogenic number fields K of degree n decreases with the absolute value of the discriminant $|D_K|$.

Bhargava, Shankar and Wang established the following pioneering results.

Theorem B.5 (Bhargava, Shankar and Wang, 2022)**.** *Denote by $M_n(X)$ the number of isomorphism classes of monogenic number fields K of degree n with $|D_K| \le X$ and with associated Galois group S_n. Then for every $n \ge 2$ we have*

$$M_n(X) \gg X^{1/2+1/n} \quad \text{as } X \to \infty.$$

The authors conjecture that the exponent on X is optimal.

In Part II of their paper, the authors proved a corresponding result for rationally monogenic number fields:

Theorem B.6 (Bhargava, Shankar and Wang, 2025). *Denote by $RM_n(X)$ the number of isomorphism classes of rationally monogenic number fields K of degree n with $|D_K| \leq X$ and with associated Galois group S_n. Then for every $n \geq 3$ we have*

$$RM_n(X) \gg X^{1/2+1/(n-1)} \quad \text{as } X \to \infty.$$

Let $N_n(X)$ denote the number of isomorphism classes of number fields X of degree n with $|D_K| \leq X$. It is conjectured that $N_n(X) \asymp X$ as $X \to \infty$. This is easy for $n = 2$. Davenport and Heilbronn (1971) proved this conjecture for $n = 3$ and Bhargava (2005, 2010) for $n = 4, 5$.

C. Arithmetic characterization of monogenic and multiply monogenic number fields

The following problem continues to attract considerable attention:

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

In this direction there are many important results for deciding the *monogenicity* or *non-monogenicity* of number fields from certain special infinite classes, including quadratic, cyclotomic, abelian, cyclic, pure, composite number fields, certain quartic, sextic, multiquadratic number fields and relative extensions, and parametric families of number fields defined by binomial, trinomial,... irreducible polynomials.

In their proofs various types of tools are used, among others Dedekind's criterion; Newton polygons; Montes' algorithm; Ore's theorem; Engström's theorem; Gröbner basis approach; reduction to binomial Thue equations; elliptic curve approaches, irreducible monic polynomials with square-free discriminant; non-squarefree discriminant approach; infinite parametric families of number fields; use of the index form equation approach with "small" solutions.

For details, we refer to Dedekind (1878) and to the books Hensel (1908), Hasse (1963), Narkiewicz (1974), Evertse and Győry (2017), Gaál (2019) and the references given there. For some recent developments, see also the survey article Gaál (2024) with many interesting special results, and the recent interesting papers Kaur, Kumar and Remete (2025), Sharma and Sarma (2025), Guàrdia and Perdet (2025), Gaál (2025), Harrington and Jones (2025), Yakkou, Aghzer and Boua (2025), König (2025), and Barman,

Jakhar, Kalwaniya and Yadav (2026). We note that Hasse's problem has not yet been solved in full generality.

It would be interesting to prove analogues for rationally monogenic orders of all that has been mentioned above for monogenic orders. Some work in this direction has been done by Del Corso, Dvornicich and Simon (2005), who generalized Dedekind's necessary condition for monogenicity of a number field to a condition for rational monogenicity. Perhaps this provides a tool to construct more examples of number fields that are not rationally monogenic.

Clearly, one may pose an analogue of Hasse's problem for rationally monogenic number fields, i.e., to give an arithmetic characterization of such fields. A more precise version of Hasse's problem and this analogue is as follows.

Problem 7. *For $m \geq 1$, give an arithmetic characterization of those number fields whose ring of integers is m times (rationally) monogenic.*

Clearly, Hasse's problem and Problem 7 do not properly belong to the reduction theory of integral polynomials.

References

[1] S. Akhtari (2012), *Representation of unity by binary forms*, Trans. Amer. Math. Soc. **364**, 2129–2155.

[2] S. Akhtari (2022), *Quartic index form equations and monogenizations of quartic orders*, Essent. Number Theory **1**, no, 1, 57–72.

[3] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. Thuswaldner (2005), *Generalized radix representations and dynamical systems I*, Acta. Math. Hungar. **108**, 207–238.

[4] L. Alpöge, M. Bhargava, A. Shnidman (2024), *A positive proportion of quartic fields are not monogenic yet have no local obstruction to being so*, Math. Ann. **388** (4), 4037–4052.

[5] L. Alpöge, M. Bhargava, A. Shnidman (2025), *A positive proportion of cubic fields are not monogenic yet have no local obstruction to being so*, Math. Ann. **391** (4), 5535–5551.

[6] A. Alvarado, A. Koutsianas, B. Malmskog, C. Rasmussen, C. Vincent and M. West (2021), *A robust implementation for solving the S-unit equation and several applications*, In: Arithmetic Geometry, Number Theory and Computation, Springer Verlag, 1–41.

[7] F. Amoroso and E. Viada (2009), *Small points on subvarieties of a torus*, Duke Math. J. **150**, 407–442.

[8] S. Arpin, S. Bozlee, L. Herr and H. Smith (2023a), *The scheme of monogenic generators I: Representability*, Res. Number Theory **9**, Paper No. 14.

[9] S. Arpin, S. Bozlee, L. Herr and H. Smith (2023b), *The scheme of monogenic generators II: Local monogenicity and twists*, Res. Number Theory **9**, Paper No. 43.
[10] A. Baker (1968a), *Linear forms in logarithms of algebraic numbers, IV*, Mathematika **15**, 204–216.
[11] A. Baker (1968b), *Contributions to the theory of Diophantine equations*, Philos. Trans. Roy. Soc. London Ser. A **263**, 173-208.
[12] A. Baker (1968c), *The Diophantine equation* $y^2 = ax^3 + bx^2 + cx + d$, J. London Math. Soc. **43**, 1–9.
[13] A. Baker (1990), *Transcendental Number Theory*, 3rd ed., Cambridge University Press, Cambridge.
[14] A. Baker and J. Coates (1970), *Integer points of curves of genus* 1, Proc. Camb. Phil. Soc. **67**, 595–602.
[15] A. Baker and G. Wüstholz (1993), *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442**, 19–62.
[16] A. Baker and G. Wüstholz (2007), *Logarithmic Forms and Diophantine Geometry*, Cambridge University Press.
[17] R. Barman, A. Jakhar, R. Kalwaniya and P. Yadav (2026), *Arithmetic aspects of number fields generated by polynomial families*, arXiv:2602.19726 [math.NT].
[18] M. A. Bennett (2001), *On the representation of unity by binary cubic forms,* Trans. Amer. Math. Soc. **353**, 1507–1534.
[19] A. Bérczes (2015a), *Effective results for unit points on curves over finitely generated domains*, Math. Proc. Cambridge Philos. Soc. **158**, 331–353.
[20] A. Bérczes (2015b), *Effective results for division points on curves in* $\mathbb{G}_m^2$, J. de Th. des Nombres de Bordeaux **27**, 405–437.
[21] A. Bérczes, J.-H. Evertse and K. Győry (2004), *On the number of equivalence classes of binary forms of given degree and given discriminant*, Acta Arith. **113**, 363–399.
[22] A. Bérczes, J.-H. Evertse and K. Győry (2009), *Effective results for linear equations in two unknowns from a multiplicative division group*, Acta Arith. **136**, 331–349.
[23] A. Bérczes, J.-H. Evertse and K. Győry (2013), *Multiply monogenic orders*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **12** 467–497.
[24] Cs. Bertók and L. Hajdu (2015), *A Hasse-type principle for exponential diophantine equations and its applications*, Math. Comp. **85**, 849–860.
[25] Cs. Bertók and L. Hajdu (2018), *A Hasse-type principle for exponential diophantine equations over number fields and its applications*, Monatsh. Math. **184**, 425–436.
[26] F. Beukers and H. P. Schlickewei (1996), *The equation* $x+y=1$ *in finitely generated groups*, Acta. Arith. **78**, 189–199.
[27] M. Bhargava (2005), *The density of discriminants of quartic rings and fields*, Ann. of Math. **162** (2), 1031–1063.
[28] M. Bhargava (2010), *The density of discriminants of quintic rings and fields*, Ann. of Math. **172** (2), 1559–1593.
[29] M. Bhargava (2022), *On the number of monogenizations of a quartic order*, with an appendix by S. Akhtari. Publ. Math. Debrecen **100**, no. 3-4, 513–531.

[30] M. Bhargava, J.-H. Evertse, K. Győry, L. Remete and A.A. Swaminathan (BEGyRS), (2023), *Hermite equivalence of polynomials,* Acta Arith. **209**, 17–58.

[31] M. Bhargava, J. Hanke and A. Shankar (2020), *The mean number of 2-torsion elements in the class groups of n-monogenized cubic fields*, preprint, arXiv:2010.15744 [math.NT]

[32] M. Bhargava, A. Shankar and A.A. Swaminathan (2025), *The second moment of the size of the 2-class group of monogenized cubic fields*, preprint, arXiv:2506.05539v1 [math.NT]

[33] M. Bhargava, A. Shankar and X. Wang (2022), *Squarefree values of polynomial discriminants I*, Invent. math. **228** (3), 1037–1073.

[34] M. Bhargava, A. Shankar and X. Wang (2025), *Squarefree values of polynomial discriminants II*, Forum of Math. Pi, **13**:e17, 1–57.

[35] M. Bhargava and I. Varma (2016), *The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders*, Proc. London Math. Soc. **112** (2), 235–266.

[36] M. Bhargava and A. Yang (2022), *On the number of integral binary n-ic forms having bounded Julia invariant*, Bull. London Math. Soc. **54** (4), 1234–1248.

[37] Y. Bilu (2002), *Baker's method and modular curves*, in: A Panorama of Number Theory or The View from Baker's Garden, G. Wüstholz, ed., Cambridge, pp. 79–88.

[38] Y. Bilu, I. Gaál and K. Győry (2004), *Index form equations in sextic fields: a hard computation*, Acta Arith. **115**, No. 1, 85–96.

[39] Y. Bilu and G. Hanrot (1996), *Solving Thue equations of high degree*, J. Number Theory **60**, 373–392.

[40] Y. Bilu and G. Hanrot (1999), *Thue equations with composite fields*, Acta Arith. **88**, 311–326.

[41] B. J. Birch and J.R. Merriman (1972), *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. **24**, 385–394.

[42] E. Bombieri (1993), *Effective diophantine approximation on* $\mathbb{G}_m$, Ann. Scuola Norm. Sup. Pisa (IV), **20**, 61–89.

[43] E. Bombieri (2002), *Forty Years of Effective Results in Diophantine Theory*, in: G. Wüstholz, ed. A Panorama of Number Theory or The View from Baker's Garden, Cambridge University Press, 2002, pp. 194–213.

[44] E. Bombieri and P. B. Cohen (1997), *Effective Diophantine approximation on* $\mathbb{G}_m$, *II*, Ann. Scuola Norm. Sup. Pisa (IV) **24**, 205–225.

[45] E. Bombieri and P. B. Cohen (2003), *An elementary approach to effective Diophantine approximation on* $\mathbb{G}_m$, in Number Theory and Algebraic Geometry, London Math. Soc., Lecture Note Series **303**, Cambridge University Press, pp. 41–62.

[46] E. Bombieri and W. Gubler (2006), *Heights in Diophantine Geometry*, Cambridge University Press.

[47] Z.I. Borevich and I.R. Shafarevich (1967), *Number Theory*, 2nd ed., Academic Press.

[48] B. Brindza (1996), *On large values of binary forms*, Rocky Mountain J. Math. **26**, 839–845.

[49] B. Brindza, J.-H. Evertse and K. Győry (1991), *Bounds for the solutions of some diophantine equations in terms of discriminants*, J. Austral. Math. Soc. Ser. A **51**, 8–26.

[50] H. Brunotte (2001), *On trinomial bases of radix representations of algebraic integers*, Acta Sci. Math. **67**, 521–527.

[51] H. Brunotte, A. Huszti and A. Pethő (2006), *Bases of canonical number systems in quartic algebraic number fields*, Journal de Théorie de Nombres de Bordeaux **18**, 537–557.

[52] Y. Bugeaud (1998), *Bornes effectives pour les solutions des équations en S-unités et des équations de Thue–Mahler*, J. Number Theory **71**, 227–244.

[53] Y. Bugeaud (2018), *Linear Forms in Logarithms and Applications*, European Math. Soc.

[54] Y. Bugeaud and K. Győry (1996a), *Bounds for the solutions of unit equations*, Acta Arith. **74**, 67–80.

[55] Y. Bugeaud and K. Győry (1996b), *Bounds for the solutions of Thue–Mahler equations and norm form equations*, Acta Arith. **74**, 273–292.

[56] P. Burcsi and A. Kovács (2008), *Exhaustive search methods for CNS polynomials*, Monatsh. Math. **155**, 421–430.

[57] J. Cremona (1999), *Reduction of binary cubic and quartic forms*, J. London Math. Soc. ISSN, 1461–1570.

[58] H. Davenport and H. Heilbronn (1971), *On the density of cubic fields II*, Proc. Roy. Soc. London Ser. A **322**, 405–420.

[59] R. Dedekind (1878), *Über die Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Abh. König. Ges. Wissen. Göttingen **23**, 1–23.

[60] I. Del Corso, R. Dvornicich and D. Simon (2005), *Decomposition of primes in non-maximal orders*, Acta Arith. **120**, 231–244.

[61] B. N. Delone (Delaunay) (1930), *Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante*, Math. Z, **31**, 1–26.

[62] B. N. Delone and D. K. Faddeev (1940), *The theory of irrationalities of the third degree (Russian)*, Inst. Math. Steklov **11**, Acad. Sci. USSR, Moscow-Leningrad, 1940. English translation, Amer. Math. Soc., Providence, 1964.

[63] L. E. Dickson (1919), *History of the Theory of Numbers, Vol.III, Quadratic and Higher Forms*, Washington Carnegie Inst., reprinted Dover, 1971.

[64] G. Dumas (1906), *Sur quelques cas irreductibilité des polynomes à coefficients rationnels*, J. Math. pures et appl., 6-ième sér. **2**, 191–258

[65] J.-H. Evertse (1984a), *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75**, 561–584.

[66] J.-H. Evertse (1984b), *On sums of S-units and linear recurrences*, Compos. Math. **53**, 225–244.

[67] J.-H. Evertse (1993), *Estimates for reduced binary forms*, J. Reine Angew. Math. **434**, 159–190.

[68] J.-H. Evertse (2011), *A survey on monogenic orders*, Publ. Math. **79**, No. 3–4, 411–422.

[69] J.-H. Evertse (2023), *Orders with few rational monogenizations*, Acta Arith. **210**, 307–335.

[70] J.-H. Evertse and K. Győry (1985), *On unit equations and decomposable form equations*, J. Reine Angew. Math. **358**, 6–19.

[71] J.-H. Evertse and K. Győry (1991a) *Effective finiteness results for binary forms with given discriminant*, Compos. Math. **79**, 169–204.

[72] J.-H. Evertse and K. Győry (1991b), *Thue inequalities with a small number of solutions*, in: The Mathematical Heritage of C. F. Gauss, World Scientific Publ. Comp., pp. 204–224.

[73] J.-H. Evertse and K. Győry (1992), *Effective finiteness theorems for decomposable forms of given discriminant*, Acta. Arith. **60**, 233–277.

[74] J.-H. Evertse and K. Győry (2013), *Effective results for unit equations over finitely generated domains*, Math. Proc. Cambridge Phil. Soc. **154**, 351–380.

[75] J.-H. Evertse and K. Győry (2015), *Unit equations in Diophantine number theory*, Camb. Stud. Adv. Math. **146**, Cambridge University Press.

[76] J.-H. Evertse and K. Győry (2017), *Discriminant equations in Diophantine number theory*, Camb. New Math. Monogr. **32**, Cambridge University Press.

[77] J.-H. Evertse and K. Győry (2022), *Effective Results and Methods for Diophantine Equations over Finitely Generated Domains*, Loondon Math. Soc. Lecture Notes Ser. **475**, Cambridge University Press.

[78] J.-H. Evertse, K. Győry, A. Pethö and J.M. Thuswaldner (2019), *Number systems over general orders*, Acta Math. Hung. **159** (1), 187–205.

[79] J.-H. Evertse, K. Győry, C.L. Stewart and R. Tijdeman (1988), *On S-unit equations in two unknowns*, Invent. Math. **92**, 461–477.

[80] J.-H. Evertse, H.P. Schlickewei and W.M. Schmidt (2002), *Linear equations in variables which lie in a multiplicative group*, Ann. Math. **155**, 807–836.

[81] G. Frey (1997), *On Ternary Equations of Fermat Type and relations with Elliptic Curves*, in: Modular Forms and Fermat's Last Theorem, G. Cornell, J.H. Silverman, G. Stevens, eds., Springer, pp. 527–548.

[82] A. Fröhlich (1967), *Local fields, in Algebraic number theory*, ed. by J. W. S. Cassels and A. Fröhlich, London and New York.

[83] I. Gaál (1986), *Inhomogeneous discriminant form and index form equations and their applications*, Publ. Math. Debrecen **33**, 1–12.

[84] I. Gaál (1988), *Integral elements with given discriminant over function fields*, Acta. Math. Hung. **52**, 133–146.

[85] I. Gaál and N. Schulte (1989), *Computing all power integral bases of cubic fields*, Math. Comp. **53**, 689–696.

[86] I. Gaál (2019), *Diophantine equations and power integral bases. Theory and algorithms* 2nd edition, Birkhäuser.

[87] I. Gaál (2024), *Monogenity and Power Integral Bases: Recent Developments*, Axioms **13** (7), 429.

[88] I. Gaál (2025). *Calculating generators of power integral bases in sextic fields with real quadratic subfields*, JP J. Algebra, Number Theory and Applications **64**, 289–306.

[89] I. Gaál and K. Győry (1999), *Index form equations in quintic fields*, Acta Arith. **89**, No. 4, 379–396.

[90] I. Gaál, A. Pethő and M. Pohst (1993), *On the resolution of index form equations in quartic number fields*, J. Symbolic Comp. **16**, 563–584.

[91] I. Gaál, A. Pethő and M. Pohst (1996), *Simultaneous representation of integers by a pair of ternary quadratic forms - with an application to index form equations in quartic number fields*, J. Number Theory **57**, 90–104.

[92] I. Gaál and M. Pohst (1996), *On the resolution of index form equations in sextic fields with an imaginary quadratic subfield*, J. Symbolic Comp. **22** (4), 425–434.

[93] I. Gaál and N. Schulte (1989), *Computing all power integral bases of cubic number fields*, Math. Comput., **53**, 689–696.

[94] W.T. Gan, B. Gross and G. Savin (2002), *Fourier coefficients of modular forms on G_2,* Duke Math. J. **115**, 105–169.

[95] C. F. Gauss (1801), *Disquisitiones Arithmeticae*, (German translation, 2nd ed, reprinted, Chelsea Publ. New York, 1981).

[96] A. O. Gelfond (1935), *On approximating transcendental nunmbers by algebraic numbers*, Dokl. Akad. Nauk SSSR **2**, 177–182.

[97] J. Guàrdia and F. Perdet (2025), *Determining monogenity of pure cubic number fields using elliptic curves*, arXiv:2505.06213v1 [math.NT]

[98] K. Győry (1972a), *Diophantine investigations in the theory of irreducible polynomials* (in Hungarian), PhD dissertation, Debrecen, pp. 173.

[99] K. Győry (1972b), *Sur l'irréductibilité d'une classe des polynômes II*, Publ. Math. Debrecen **19**, 293–326.

[100] K. Győry (1973), *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. **23**, 419–426.

[101] K. Győry (1974), *Sur les polynômes à coefficients entiers et de discriminant donné II*, Publ. Math. Debrecen 21, 125–144.

[102] K. Győry (1976), *Sur les polynômes à coefficients entiers et de discriminant donné, III*, Pub. Math. Debrecen. **23**, 141–165.

[103] K. Győry (1978a), *On polynomials with integer coefficients and given discriminant, IV* Publ. Math. Debrecen **25**, (1978a) 155–167.

[104] K. Győry (1978b), *On polynomials with integer coefficients and given discriminant V: p-adic generalizations*, Acta Math. Acad. Sci. Hung. **32**, 175–190.

[105] K. Győry (1978/79), *On the greatest prime factors of decomposable forms at integer points*, Ann. Acad. Sci. Fenn., Ser. A I Math **4**, 341-355.

[106] K. Győry (1979), *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. **54**, 583–600.

[107] K. Győry (1980a), *Corps de nombres algébriques d'anneau d'entiers monogène*, Semin. Delange-Pisot-Poitou, 20e Annee 1978/79, Théorie des nombres, Fasc. 2, No. **26**, 1–7.

[108] K. Győry (1980b), *Résultats effectifs sur la représentation des entiers par des formes désomposables*, Queen's Papers in Pure and Applied Math., No.**56**, Kingston, Canada

[109] K. Győry (1981), *On discriminants and indices of integers of an algebraic number field*, J. Reine Angew. Math. **324**, 114–126.

[110] K. Győry (1982), *On certain graphs associated with an integral domain and their applications to Diophantine problems,* Publ. Math. Debrecen **29**, 79–94.

[111] K. Győry (1983), *Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains,* Acta Math. Hung. **42**, 45–80.

[112] K. Győry (1984), *Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains*, J. Reine Angew. Math. **346**, 54–100.

[113] K. Győry (1994), *Upper bounds for the degrees of decomposable forms of given discriminant*, Acta. Arith. **66**, 261–268.

[114] K. Győry (1998), *Bounds for the solutions of decomposable form equations*, Publ. Math. Debrecen, **52**, 1–31.

[115] K. Győry (2000), *Discriminant form and index form equations*, in: Algebraic Number Theory and Diophantine Analysis, de Gruyter, pp. 191-214.

[116] K. Győry (2001), *Thue inequalities with a small number of primitive solutions*, Periodica Math. Hungar. **42**, 199–209.

[117] K. Győry (2002), *Solving Diophantine Equations by Baker's Theory*, in: G. Wüstholz, ed. A Panorama of Number Theory or The View from Baker's Garden, Cambridge University Press, 2002, pp. 38–72.

[118] K. Győry (2006), *Polynomials and binary forms with given discriminant*, Publ. Math. Debrecen **69**, 473–499.

[119] K. Győry (2019), *Bounds for the solutions of S-unit equations and decomposable form equations II*, Publ. Math. Debrecen **94**, 507–526.

[120] K. Győry (2022), *S-unit equations and Masser's ABC conjecture in algebraic number fields*, Publ. Math. Debrecen **100**, 499–511.

[121] K. Győry and S. Le Fourn (2024), *Improved bounds for some S-unit equations*, Acta Arith. **214**, 311–326.

[122] K. Győry and Z. Z. Papp (1977), *On discriminant form and index form equations*, Studia Sci. Math. Hungar. **12**, 47–60.

[123] K. Győry and Z. Z. Papp (1978), *Effective estimates for the integer solutions of norm form and discriminant form equations*, Publ. Math. Debrecen **25**, 311–325.

[124] K. Győry and Á. Pintér (2008), *Polynomial powers and a common generalization of binomial Thue-Mahler equations and S-unit equations*, in: Diophantine Equations (ed. by N. Saradha), Narosa Publ. House, New Delhi, India, pp. 103–119.

[125] K. Győry and K. Yu (2006), *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith. **123**, 9–41.

[126] L. Hajdu (2009), *Optimal systems of fundamental S-units for LLL-reduction*, Periodica Math. Hung. **59**, 79–105.

[127] G. Hanrot (1997), *Solving Thues equations without the full unit group*, Math. Comp. **69**, 395–405.
[128] J. Haristoy (2003), *Équations diophantiennes exponentielles*, Thèse de docteur, Strasbourg.
[129] J. Harrington and L. Jones (2025), *Monogenic cyclic polynomials in recurrence sequences*, arXiv:2505.09481v1 [math.NT]
[130] H. Hasse (1963), *Zahlentheorie*, Akademie-Verlag (Berlin).
[131] H. Hasse (1980), *Number Theory* (English translation), Berlin–Heidelberg–New York.
[132] K. Hensel (1908), *Theorie der algebraischen Zahlen*, Teubner Verlag, Leipzig-Berlin, 1908.
[133] C. Hermite (1848), *Note sur la réduction des fonctions homogènes à coefficients entiers et à deux indeterminées*, J. Reine Angew. Math. **36**, 357–364.
[134] C. Hermite (1851), *Sur l'introduction des variables continues dans la théorie des nombres*, J. Reine Angew. Math. **41**, 191–216.
[135] C. Hermite (1854), *Sur la théorie des formes quadratiques, I*, J. Reine Angew. Math. **47**, 313–342.
[136] C. Hermite (1857), *Extrait d'une lettre de M. C. Hermite à M. Borchardt sur le nombre limité d'irrationalités auxquelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés*, J. Reine Angew. Math. **53**, 182–192.
[137] M. Hindry and J. H. Silverman (2000), *Diophantine Geometry, An Introduction*, Springer Verlag.
[138] W. Ho, A. Shankar and I. Varma (2018), *Odd degree number fields with odd class number*, Duke Math. J. **167** (5), 995–1047.
[139] G. Julia (1917), *Étude sur les formes binaires non-quadratiques à indéterminées réelles ou complexes*, Acad. Sci. l'Inst. France, **55**, 1–296.
[140] R. von Känel (2011), *An effective proof of the hyperelliptic Shafarevich conjecture and applications*, PhD dissertation, ETH Zürich, 54 pp.
[141] R. von Känel (2014a), *An effective proof of the hyperelliptic Shafarevich conjecture*, J. Théor. Nombres Bordeaux **26**, 507–530
[142] R. von Känel (2014b), *Modularity and integral points on moduli schemes*, arXiv:1310.7263v2 [math.NT]
[143] R. von Känel (2024), *Integral points on moduli schemes*, J. Number Theory (2024), https://doi.org/10.1016/j.jnt.2024.07.005
[144] R. von Känel and B. Matschke (2023), *Solving S-unit, Mordell, Thue, Thue–Mahler and generalized Ramanujan–Nagell equations via the Shimura–Taniyama conjecture*, Mem. Amer. Math. Soc. **286** (1419), vi+142.
[145] S. Kaur, S. Kumar and L. Remete (2025), *On the index of power compositional polynomials*, Finite Fields and Their Applications **107**, 102642
[146] K. S. Kedlaya (2012), *A constuction of polynomials with squarefree discriminants*, Proc. Amer. Math. Soc. **140**, 3025–3033.

[147] J. Klaska (2021), *On cubic polynomials with a given discriminant*, Math. Appl. **10**, 103–113.

[148] J. Klaska (2022), *Quartic polynomials with a given discriminant*, Math. Slovaca **72**, 35–50.

[149] V. Komornik (2011), *Expansions in noninteger bases*, Integers, 11B

[150] J. König (2025), *A note on monogenic even polynomials*, arXiv:2505.10119v1 [math. NT]

[151] S. V. Kotov and L. Trelina (1979), *S-ganze Punkte auf elliptischen Kurven*, J. Reine Angew. Math. **306**, 28–41.

[152] A. Kovács (2001), *Generalized binary number systems*, Ann. Univ. Sci. Eötvös, Sect. Comput., **20**, 195–206.

[153] B. Kovács (1981), *Canonical number systems in algebraic number fields*, Acta Math. Acad. Sci. Hungar. **37**, 405–407.

[154] B. Kovács and A. Pethő (1991), *Number systems in integral domains, especially in orders of algebraic number fields*, Acta Sci. Math. **55**, 287–299.

[155] R. V. Kravchenko, M. Mazur, B. V. Petrenko (2012), *On the smallest number of generators and the probability of generating an algebra*, Algebra and Number Theory **6**, 243–291.

[156] L. Kronecker (1882), *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. Reine Angew. Math. **92**, 1–122.

[157] J. L. Lagrange (1773), *Recherches d'arithmétique*, Nouv. Mém. Acad. Berlin, 265–312, Oeuvres, III, 693–758.

[158] E. Landau (1918), *Verallgemeinerung eines Polyaschen Satzes auf algebraische Zahlkörper*, Nachr. Ges. Wiss. Göttingen, 475–488.

[159] S. Lang (1960), *Integral points on curves,* Inst. Hautes Études Sci. Publ. Math. **6**, 27–43.

[160] S. Le Fourn (2020), *Tubular approaches to Baker's method for curves and varieties*, Algebra & Number Theory **14**, 785–807.

[161] G. Malle (2008), *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory **128** (10), 2823–2835.

[162] G. Malle (2010), *On the distribution of class groups of number fields*, Experiment. Math. **19** (4), 465–474.

[163] R.C. Mason (1984), *Diophantine equations over function fields*, Cambridge University Press.

[164] R. C. Mason (1988), *The study of Diophantine equations over function fields*, in: New Advances in Transcendence Theory, Proc. Conf. Durham 1986, ed. by A. Baker.

[165] D. W. Masser (2002), *On abc and discriminants*, Proc. Amer. Math. Soc. **130**, 3141–3150.

[166] D.W. Masser (2017), *Abcological anecdotes*, Mathematika **63**, 713–714.

[167] E. M. Matveev (2000), *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers II*, Izv. Math. **64**, 1217–1269.

[168] J. R. Merriman, N. P. Smart (1993a), *The calculation of all algebraic integers of degree* 3 *with discriminant a product of powers of* 2 *and* 3 *only*, Publ. Math. Debrecen **43**, 105–111.

[169] J. R. Merriman, N. P. Smart (1993b), *Curves of genus* 2 *with good reduction away from* 2 *with a rational Weierstrass point*, Math. Proc. Cambridge Philos. Soc. **114**, 203–214. Correginda: ibid. 118 (1995), 189.

[170] L. Miller-Sims and L. Robertson (2005), *Power integral bases for real cyclotomic fields,* Bull. Austral. Math. Soc. **71**, 167–173.

[171] M. R. Murty and H. Pasten (2013), *Modular forms and effective Diophantine approximation*, J. Number Theory **133**, 3739–3754.

[172] T. Nagell (1930), *Zur Theorie der kubischen Irrationalitäten*, Acta Math. **55**, 33–65.

[173] T. Nagell (1967), *Sur les discriminants des nombres algébriques*, Arkiv för Mat. **7**, 265–282.

[174] J. Nakagawa (1989), *Binary forms and orders of algebraic number fields*, Invent. Math. **97**, 219–235.

[175] W. Narkiewicz (1974), *Elementary and analytic theory of algebraic numbers*, Springer Verlag/PWN-Polish Scientific Publishers; 2nd ed. (1990), Springer Verlag.

[176] W. Narkiewicz (2018), *The story of algebraic numbers in the first half of the 20th century. From Hilbert to Tate*, Springer.

[177] K.-H. Nguyen-Dang (2026), *Eisenstein-prime obstruction sieve for monogenicity*, preprint, arXiv:2602.10488 [math.NT].

[178] K.-H. Nguyen-Dang and N.T. Hung (2026), *α-monogeneity of pure number fields: criterion and density*, preprint, arXiv:2510.20232v2 [math.NT].

[179] C. J. Parry (1950), *The $\mathfrak{p}$-adic generalization of the Thue–Siegel theorem*, Acta Math. **83**, 1–100.

[180] H. Pasten (2014), *Arithmetic problems around the abc-conjecture and connection with logic*, PhD thesis, Queen's University, Canada.

[181] G. Peruginelli (2014), *Integral-valued polynomials over the set of algebraic integers of bounded degree*, J. Number Theory **137**, 241–255.

[182] A. Pethő (1991), *On a polynomial transformation and its application to the construction of a public key cryptosystem*, in: Computational Number Theory, de Gruyter, pp. 31–44.

[183] A. Pethő (2004), *Connections between power integral bases and radix representations in algebraic number fields*, in: Yokoi-Chowla Conjecture and related problems, Furukawa Total Printing Co. LTD, Saga, Japan. pp. 115–125.

[184] A. Pethő and R. Schulenberg (1987), *Effektives Lösen von Thue Gleichungen*, Publ. Math. Debrecen **34**, 189–196.

[185] A. Pethő and J. Thuswaldner (2018), *Number systems over orders*, Monatsh. Math. **187**, 681–704.

[186] A. Pethő and P. Varga (2017), *Canonical number systems over imaginary quadratic Euclidean domains*, Colloq. Math. **146**, 165–186.

[187] C. Petsche (2012), *Critically separable rational maps in families*, Compositio Math. **148**, 1880–1896.

[188] Á. Pintér (1995), *On the magnitude of integer points on elliptic curves*, Bull. Austral. Math. Soc. **52**, 195–199.

[189] P. A. B. Pleasants (1974), *The number of generators of the integers of a number field*, Mathematika **21**, 160–167.

[190] A.J. van der Poorten and H.P. Schlickewei (1982), *The growth condition for recurrence sequences*, Macquarie Universsity Math. Rep. 82-0041.

[191] A.J. van der Poorten and H.P. Schlickewei (1991), *Additive relations in fields*, J. Austral. Math. Soc. (Ser A) **51**, 154–170.

[192] P. Ribenboim (2006), *Finite sets of binary forms*, Publ. Math. Debrecen, **68**, 261–282.

[193] N. Schulte (1989), *Indexgleichungen in kubischen Zahlkörpern*, Diplomarbeit, Heinrich-Heine Universität, Düsseldorf.

[194] N. Schulte (1991), *Index form equations in cubic number fields,* in "Computational Number Theory", de Gruyter, Berlin-New York, 281–287.

[195] I. R. Shafarevich (1963), *Algebraic number fields*, In: Proc. Intern. Congr. Math. (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, pp. 163–176; English transl. in Amer. Math. Soc. Transl **31** (1963), 25–39.

[196] A. Shankar, A Siad and A.A. Swaminathan (2023), *Counting integral points on symmetric varieties with applications to arithmetic statistics*, Proc. London Math. Soc. **130**; https://doi.org/10.1112/plms.70039.

[197] H. Sharma and R. Sarma (2025), *Monogenity of composition of polynomials*, Ramanujan J. (2025) 67:45.

[198] A. Shlapentokh (1996), *Polynomials with a given discriminant over fields of algebraic functions of positive characteristic*, Pacific J. Math. **173**, 533–555.

[199] T. N. Shorey and R. Tijdeman (1986), *Exponential Diophantine Equations*, Cambridge University Press.

[200] A. J. Siad (2021), *Monogenic Fields with Odd Class Number*, PhD-thesis, Toronto.

[201] C.L. Siegel (1921), *Approximation algebraischer Zahlen*, Math. Z. **10**, 173–213.

[202] C. L. Siegel (1929), *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss., 1–41.

[203] D. Simon (2001), *The index of nonmonic polynomials*, Indag. Math. (N.S) **12**, 505–517.

[204] D. Simon (2003), *La classe invariante d'une forme binaire*, C.R. Math. Acad. Sci. Paris **336**, 7–10.

[205] N. P. Smart (1993), *Solving a quartic discriminant form equation*, Publ. Math. Debrecen **43**, 29–39.

[206] N. P. Smart (1995), *The solution of triangularly connected decomposable form equations*, Math. Comp. **64**, 819–840.

[207] N. P. Smart (1996), *Solving discriminant form equations via unit equations*, J. Symbolic Comp. **21** (3), 367-374.

[208] N. P. Smart (1997), *S-unit equations, binary forms and curves of genus 2*, Proc. London Math. Soc. **75** (2), 271–307.

[209] N. P. Smart (1998), *The Algorithmic Resolution of Diophantine Equations*, Cambridge.

[210] V. G. Sprindžuk (1993), *Classical Diophantine Equations*, Lecture Notes Math. 1559, Springer Verlag.

[211] H.P. Stanley (2015), *Catalan numbers*, Cambridge University Press.

[212] C. L. Stewart (1991), *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc. **4**, 793–835.

[213] B. J. Stout (2014), *A dynamical Shafarevich theorem for twists of rational morphisms*, Acta Arith. **166**, 69–80.

[214] A. A. Swaminathan (2023), *A new parametrization for ideal classes in rings defined by binary forms, and applications*, J. Reine Angew. Math. **798**, 143–191.

[215] L. Szpiro and T. J. Tucker (2008), *A Shafarevich-Faltings theorem for rational functions*, Pure and Appl. Math. Quartely **4**, 1–14.

[216] A. Thue (1909), *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. **135**, 284–305.

[217] J. L. Thunder (1995), *On Thue inequalities and a conjecture of Schmidt*, J. Number Theory **52**, 319–328.

[218] L. A. Trelina (1977a), *On algebraic integers with discriminants having fixed prime divisors*, Mat. Zametki **21**, 289–296 (Russian).

[219] L. A. Trelina (1977b), *On the greatest prime factor of an index form*, Dokl. Akad. Nauk BSSR **21**, 975–976 (Russian).

[220] L. A. Trelina (1985), *Representation of powers by polynomials in algebraic number fields*, Dokl. Akad. Nauk BSSR **29**, 5–8 (Russian).

[221] N. Tzanakis and B. M. M. de Weger (1989), *On the practical solution of the Thue equation*, J. Number Theory **31**, 99–102.

[222] B. M. M. de Weger (1989), *Algorithms for Diophantine Equations*, CWI Tract **65**, Amsterdam.

[223] K. Wildanger (1997), *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve*, Dissertation, Technical University, Berlin.

[224] K. Wildanger (2000), *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern*, J. Number Theory **82**, 188–224.

[225] M.M. Wood (2011), *Rings and ideals parameterized by binary n-ic forms*, J. London Math. Soc. **83** (2011) 208–231.

[226] G. Wüstholz, ed. (2002), *A Panorama of Number Theory or the View from Baker's Garden*, Cambridge Univers ity Press.

[227] B. Yakkou, I. Aghzer and A. Boua (2025), *On index divisors of certain sextic number fields defined by quadrinomials*, Georgian Math. J., https://doi.org/10.1515/gmj-2025-2078.

[228] A. Q. Yingst (2006), *A characterization of homeomorphic Bernoulli trial measures*, PhD dissertation, Univ. North Texas.

[229] K. Yu (2007), *P-adic logarithmic forms and group varieties III*, Forum Mathematicum **19**, 187–280.

[230] U. Zannier (2009), *Lecture Notes on Diophantine Analysis*, Scuola Normale Superiore di Pisa (New Series).

[231] W. Zhuang (2015), *Symmetric Diophantine approximation over function fields*, PhD dissertation, Universiteit Leiden.

J.-H. Evertse
Universiteit Leiden, Mathematisch Instituut,
Postbus 9512, 2300 RA Leiden, The Netherlands
URL: https://pub.math.leidenuniv.nl/∼evertsejh
Email address: evertse@math.leidenuniv.nl

K. Győry
University of Debrecen, Institute of Mathematics,
P.O. Box 400, 4002 Debrecen, Hungary
URL: https://math.unideb.hu/en/dr-kalman-gyory
Email address: gyory@science.unideb.hu