Publ. Math. Debrecen
79/3-4 (2011), 411–422
DOI: 10.5486/PMD.2011.5150

A survey on monogenic orders

By JAN-HENDRIK EVERTSE (Leiden)

To Kálmán Győry on his 70-th birthday,
with gratitude for a life-long cooperation

Abstract. Recall that an order $\mathcal{O}$ in an algebraic number field K is called *monogenic* if it is generated by one element, i.e., there is an α with $\mathbb{Z}[\alpha] = \mathcal{O}$. By work of Győry [11, 1976] there are, up to a suitable equivalence, only finitely many α such that $\mathbb{Z}[\alpha] = \mathcal{O}$. In this survey, we give an overview of recent results on estimates for the number of α up to equivalence.

1. Introduction

Let K be an algebraic number field of degree d and denote by $\mathcal{O}_K$ its ring of integers. Let $\mathcal{O}$ be an order in K, i.e., a subring of $\mathcal{O}_K$ with quotient field K. The order $\mathcal{O}$ is called *monogenic* if it can be expressed as $\mathbb{Z}[\alpha]$ with some $\alpha \in \mathcal{O}$. Equivalently, this means that $\mathcal{O}$ has a $\mathbb{Z}$-module basis of the shape $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$. Clearly, if $\mathcal{O} = \mathbb{Z}[\alpha]$ then also $\mathcal{O} = \mathbb{Z}[\beta]$ for any β of the shape $\pm\alpha + a$ with $a \in \mathbb{Z}$. Such β are said to be equivalent to α. It is well-known that orders in quadratic number fields are monogenic, but number fields of degree > 2 may have non-monogenic orders.

We consider the 'Diophantine equation'

$$\mathbb{Z}[\alpha] = \mathcal{O} \quad \text{in } \alpha \in \mathcal{O}. \tag{1.1}$$

Mathematics Subject Classification: Primary: 11R99; Secondary: 11D99, 11J99.
Key words and phrases: monogenic orders.

As explained above, the solutions of (1.1) can be divided into equivalence classes $\{\pm\alpha + a : a \in \mathbb{Z}\}$. We can rewrite (1.1) as a genuine Diophantine equation as follows. Fix a $\mathbb{Z}$-module basis $\{1, \omega_1, \ldots, \omega_{d-1}\}$ of $\mathcal{O}$. There exists a homogeneous polynomial $I \in \mathbb{Z}[X_1, \ldots, X_{d-1}]$ of degree $d(d-1)/2$ in $d-1$ variables, called the *index form* associated to this basis, such that $\alpha = x_0 + x_1\omega_1 + \cdots + x_{d-1}\omega_{d-1}$ with $x_i \in \mathbb{Z}$ is a solution of (1.1) if and only if $(x_1, \ldots, x_{d-1})$ is a solution of the *index form equation*

$$I(x_1, \ldots, x_{d-1}) = \pm 1 \quad \text{in } x_1, \ldots, x_{d-1} \in \mathbb{Z}. \tag{1.2}$$

Suppose that K has degree $d \geq 3$. In 1976, Győry [11] proved that the set of solutions of (1.1) is a union of at most finitely many equivalence classes and that a full system of representatives of those can be determined effectively. Equivalently, this means that (1.2) has only finitely many solutions which can be determined effectively. Today there are practical algorithms to solve (1.1) or (1.2) for arbitrary number fields of degree ≤ 6 and some special classes of higher degree number fields, see Gaál [8, 2002] and Bilu, Gaál and Győry [5, 2004].

In this survey, we do not go into the algorithmic resolution of (1.1), but rather focus on estimates for the number of solutions of (1.1) up to equivalence. We call an order $\mathcal{O}$ *k times monogenic* if (1.1) has at least k equivalence classes of solutions, i.e., if there are $\alpha_1, \ldots, \alpha_k$ such that

$$\mathcal{O} = \mathbb{Z}[\alpha_1] = \cdots = \mathbb{Z}[\alpha_k],\ \alpha_i \pm \alpha_j \notin \mathbb{Z} \quad \text{for } i, j = 1, \ldots, k \text{ with } i \neq j.$$

Analogously, we call $\mathcal{O}$ precisely/at most k times monogenic if (1.1) has precisely/at most k equivalence classes of solutions.

It is easy to see that every order in a quadratic number field is precisely one time monogenic. In case that K is a cubic number field, the index form equation (1.2) corresponding to (1.1) is a cubic Thue equation. Bennett [1, 2001] proved that such equations have up to sign not more than 10 solutions. Thus, any order in a cubic number field is at most 10 times monogenic. Gaál and Schulte [9, 1989] determined the solutions of (1.1) for several orders in cubic number fields. A consequence of their result is that $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ is precisely 9 times monogenic, where $\zeta_p := e^{2\pi i/p}$. It is believed that all other orders in a cubic number field are less than 9 times monogenic.

We now consider orders in number fields K of degree $d \geq 4$. Győry and the author [6, 1985] proved that any order $\mathcal{O}$ in K is at most $(3 \times 7^{2g})^{d-2}$ times monogenic, where g is the degree of the normal closure of K. Note that $d \leq g \leq d!$. This was the first uniform bound of this type. In this survey, we deduce the following improvement.

Theorem 1.1. *Let K be a number field of degree $d \geq 4$. Then any order $\mathcal{O}$ in K is at most*

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

times monogenic.

This bound is probably far from best possible. The best lower bound we could find is due to Miller-Sims and Robertson [15, 2005]. They considered (1.1) for $\mathcal{O} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ where p is a prime, this is the ring of integers of the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$. They proved that if $p \geq 7$ then (1.1) is satisfied by $\zeta_p^k + \zeta_p^{-k}$, $(\zeta_p^k + \zeta_p^{-k} + b)^{-1}$ $(b = -1, 0, 1, 2,\ k = 1, \ldots, (p-1)/2)$. If $p = 7$ then among these numbers there are precisely nine pairwise inequivalent ones and by the result of Gaál and Schulte mentioned above these are up to equivalence the only solutions of (1.1). If $p \geq 11$ then all these numbers are pairwise inequivalent and thus, the ring $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ is $5(p-1)/2$ times monogenic.

We now fix a number field, and consider varying orders in that field. It can be shown that in a given number field, 'most' orders are only few times monogenic. The following result, which is a refinement of work of Bérczes [2, 2000], makes this more precise.

Theorem 1.2 (Bérczes, Evertse, Győry [3, to appear])**.** *Let K be a number field of degree $d \geq 3$. Then there are at most finitely many three times monogenic orders in K.*

It is not difficult to show that there are number fields with infinitely many two times monogenic orders. For instance, let K be a number field of degree $d \geq 3$ and suppose that K is not a CM-field, i.e., it is not a totally complex quadratic extension of a totally real field. Then the ring of integers $\mathcal{O}_K$ of K has infinitely many units ε such that $\mathbb{Q}(\varepsilon) = K$. If ε is one of these units, then from the minimal polynomial of ε one easily deduces that $\varepsilon^{-1} = g(\varepsilon)$, $\varepsilon = h(\varepsilon^{-1})$ for certain $g, h \in \mathbb{Z}[X]$, and thus $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon^{-1}]$. Moreover, ε^{-1} cannot be equivalent to ε since ε has degree ≥ 3. By varying ε we obtain infinitely many two times monogenic orders in K.

We believe that if K is a number field of degree $d \geq 3$, then the collection of two times monogenic orders in K consists of finitely many infinite classes of 'special' two times monogenic orders, and at most finitely many orders outside these classes. Bérczes, Győry and the author [3] managed to make this precise in some special cases. We recall their result.

Let again K be a number field of degree $d \geq 3$ and $\mathcal{O}$ an order in K. We call $\mathcal{O}$ an order of **type I** if there are $\alpha, \beta \in \mathcal{O}$, and a matrix $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z})$

with $a_3 \neq 0$ such that

$$\mathcal{O} = \mathbb{Z}[\alpha] = \mathbb{Z}[\beta], \quad \beta = \frac{a_1\alpha + a_2}{a_3\alpha + a_4}.$$

It is easily shown that such α, β are inequivalent. Hence type I orders are two times monogenic. If K is not a CM-field then it has infinitely many orders of type I. In [3] it is proved that every two times monogenic order in a cubic number field is of type I.

Type II orders exist only in quartic number fields. We call $\mathcal{O}$ an order of **type II** if there are $\alpha, \beta \in \mathcal{O}$, and $a_0, a_1, a_2, b_0, b_1, b_2 \in \mathbb{Z}$ with $a_2 b_2 \neq 0$ such that

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

Again, it is obvious that such α, β are inequivalent and thus, that orders of type II are two times monogenic. In [3], examples have been given of quartic number fields with infinitely many orders of type II. The construction of these orders uses cubic resolvents.

Recall that a number field K is called k times transitive (where $1 \leq k \leq [K : \mathbb{Q}]$) if, for any two ordered k-tuples of distinct embeddings $(\sigma_1, \ldots, \sigma_k)$, $(\tau_1, \ldots, \tau_k)$ of K in $\overline{\mathbb{Q}}$, there is $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\rho \circ \sigma_i = \tau_i$ for $i = 1, \ldots, k$.

Theorem 1.3 (Bérczes, Evertse, Győry [3, to appear])**.** (i) *Let K be a number field of degree 4 such that the normal closure of K has Galois group S_4. Then there are at most finitely many two times monogenic orders in K that are not of type I or II.*

(ii) *Let K be a four times transitive number field of degree ≥ 5. Then there are at most finitely many two times monogenic orders in K that are not of type I.*

We mention that in [3], more general versions of Theorems 1.2 and 1.3 are proved about orders that are monogenic over an arbitrary domain which is integrally closed and finitely generated over $\mathbb{Z}$. We do not know if Theorem 1.3 remains valid if we drop the conditions on K.

In Section 2 we prove Theorem 1.1. In Sections 3, 4, respectively we give brief sketches of the proofs of Theorems 1.2 and 1.3. For the full (and lengthy) proofs of these theorems we refer to [3].

2. Proof of Theorem 1.1

Given a field G, we denote by $(G^*)^m$ the group of m-tuples $(x_1, \ldots, x_m)$ with $x_1, \ldots, x_m \in G^*$, endowed with coordinatewise multiplication

$$(x_1, \ldots, x_m)(y_1, \ldots, y_m) = (x_1 y_1, \ldots, x_m y_m).$$

Our main tool is the following result.

Proposition 2.1. *Let G be a field of characteristic 0, and Γ a finitely generated subgroup of $(G^*)^2$ of rank r. Then the equation*

$$x + y = 1 \quad \text{in } (x, y) \in \Gamma$$

has at most $2^{8(r+1)}$ solutions.

PROOF. BEUKERS, SCHLICKEWEI [4, 1996]. □

We deduce the following consequence.

Lemma 2.2. *Let G be a field of characteristic 0, $n \geq 1$, and Γ a finitely generated subgroup of $(G^*)^{2n}$ of rank r. Then the system of equations*

$$x_i + y_i = 1 \ (i = 1, \ldots, n) \quad \text{in } (x_1, y_1, \ldots, x_n, y_n) \in \Gamma \tag{2.1}$$

has at most $2^{8(r+2n-1)}$ solutions.

PROOF. We proceed by induction on n. For $n = 1$, Lemma 2.2 is precisely Proposition 2.1. Assume that $n \geq 2$, and that the lemma is true for systems of fewer than n equations. Write $\mathbf{x} := (x_1, y_1, \ldots, x_n, y_n)$, $\mathbf{x}' := (x_1, y_1, \ldots, x_{n-1}, y_{n-1})$ and define the homomorphism $\varphi : \mathbf{x} \mapsto \mathbf{x}'$. Let $\Gamma' := \varphi(\Gamma)$ and $\Gamma_0 := \ker(\varphi : \Gamma \to \Gamma')$. Notice that if $\mathbf{x}$ is a solution of (2.1), then $\varphi(\mathbf{x})$ is a solution of the system consisting of the first $n-1$ equations of (2.1). By the induction hypothesis, if $\mathbf{x}$ runs through the solutions of (2.1), then $\mathbf{x}'$ runs through a set of cardinality at most $2^{8(r'+2n-3)}$, where $r' := \operatorname{rank} \Gamma'$. Pick an element from Γ' and then an element from its inverse image under φ, say $\mathbf{x}^* := (x_1^*, y_1^*, \ldots, x_n^*, y_n^*) \in \Gamma$. To finish the induction step we have to prove that (2.1) has at most $2^{8(r-r'+2)}$ solutions $\mathbf{x} = (x_1, \ldots, y_n)$ with $\varphi(\mathbf{x}) = \varphi(\mathbf{x}^*)$, i.e., with $\mathbf{x} \cdot (\mathbf{x}^*)^{-1} \in \Gamma_0$.

Let Γ_1 be the image of the group generated by Γ_0 and $\mathbf{x}^*$ under the projection $(x_1, y_1, \ldots, x_n, y_n) \mapsto (x_n, y_n)$. Then Γ_1 is a group of rank at most $\operatorname{rank} \Gamma_0 + 1 = r - r' + 1$. Notice that if $\mathbf{x} = (x_1, \ldots, y_n)$ is a solution of (2.1) with $\varphi(\mathbf{x}) = \varphi(\mathbf{x}^*)$, then $x_i = x_i^*, y_i = y_i^*$ for $i = 1, \ldots, n-1$, $x_n + y_n = 1$ and $(x_n, y_n) \in \Gamma_1$. From Proposition 2.1 it follows that for (x_n, y_n), hence $\mathbf{x}$, we have at most $2^{8(r-r'+2)}$ possibilities. This completes our induction step. □

In what follows, let K be a number field of degree $d \geq 4$, say $K = \mathbb{Q}(\theta)$ and denote by G its normal closure, i.e., $G = \mathbb{Q}(\theta^{(1)}, \ldots, \theta^{(d)})$, where $\theta^{(1)} = \theta, \ldots, \theta^{(d)}$ are the conjugates of θ. Denote by $x \mapsto x^{(i)}$ the embedding of K in G defined by $\theta^{(i)}$. Further, define the fields $L_{ij} := \mathbb{Q}(\theta^{(i)} + \theta^{(j)}, \theta^{(i)}\theta^{(j)})$ $(1 \leq i, j \leq d,\ i \neq j)$. Denote by U_{ij} the unit group of the ring of integers of L_{ij}.

Let $\mathcal{O}$ be an order in K and define

$$S(\mathcal{O}) := \{\alpha \in \mathcal{O} : \mathbb{Z}[\alpha] = \mathcal{O}\}.$$

Lemma 2.3. *Let $\alpha, \beta \in S(\mathcal{O})$. Then*

$$u_{ij}(\alpha,\beta) := \frac{\alpha^{(i)} - \alpha^{(j)}}{\beta^{(i)} - \beta^{(j)}} \in U_{ij} \quad \text{for } 1 \le i,\ j \le d,\ i \ne j. \tag{2.2}$$

Proof. Let $i, j \in \{1, \dots, d\}$, $i \ne j$. The quantity $u_{ij}(\alpha,\beta)$ is a symmetric function in $\theta^{(i)}, \theta^{(j)}$, hence it belongs to L_{ij}. There are $f, g \in \mathbb{Z}[X]$ such that $\beta = f(\alpha)$ and $\alpha = g(\beta)$. This shows that both $u_{ij}(\alpha,\beta)$ and its multiplicative inverse are algebraic integers, hence it is an algebraic unit. □

Lemma 2.4. *The multiplicative subgroup of $(G^*)^{d(d-1)/2}$ generated by the tuples*

$$\rho(\alpha) := \left(\alpha^{(i)} - \alpha^{(j)} : 1 \le i < j \le d\right) \quad (\alpha \in S(\mathcal{O})) \tag{2.3}$$

has rank at most $\frac{1}{2}d(d-1)$.

Proof. Denote by U the group under consideration. We fix $\beta \in S(\mathcal{O})$ (if no such β exists we are done) and let $\alpha \in S(\mathcal{O})$ vary. Then for $\alpha \in S(\mathcal{O})$ we have

$$\rho(\alpha) = \rho(\beta) \cdot \mathbf{u}(\alpha) \quad \text{with } \mathbf{u}(\alpha) := (u_{ij}(\alpha,\beta) : 1 \le i < j < d). \tag{2.4}$$

We partition the collection of 2-element subsets of $\{1, \dots, d\}$ into classes such that $\{i, j\}$ and $\{i', j'\}$ belong to the same class if and only if there exists $\sigma \in \mathrm{Gal}(G/\mathbb{Q})$ such that $\sigma(\theta^{(i)} + \theta^{(j)}) = \theta^{(i')} + \theta^{(j')}$, $\sigma(\theta^{(i)}\theta^{(j)}) = \theta^{(i')}\theta^{(j')}$. Then by Lemma 2.3 and since $u_{ij}(\alpha,\beta)$ is a symmetric function in $\theta^{(i)}, \theta^{(j)}$ we have

$$u_{i',j'}(\alpha,\beta) = \sigma(u_{ij}(\alpha,\beta)) \quad \text{for } \alpha \in S(\mathcal{O}). \tag{2.5}$$

Clearly, the cardinality of the class represented by $\{i, j\}$ is $[L_{ij} : \mathbb{Q}]$.

Denote the different classes by $C_1, \dots, C_t$, and suppose that $\{i_k, j_k\} \in C_k$ for $k = 1, \dots, t$. Property (2.5) and Lemma 2.3 imply that

$$(x_{ij} : 1 \le i < j \le d) \mapsto (x_{i_1,j_1}, \dots, x_{i_t,j_t})$$

defines an injective homomorphism from the group generated by the tuples $\mathbf{u}(\alpha)$ ($\alpha \in S(\mathcal{O})$) into $U_{i_1,j_1} \times \cdots \times U_{i_t,j_t}$. By Dirichlet's Unit Theorem, $\operatorname{rank} U_{i_k,j_k} \le [L_{i_k,j_k} : \mathbb{Q}] - 1 = \#C_k - 1$ for $k = 1, \dots, t$. Together with (2.4), this implies that U has rank at most

$$1 + \sum_{k=1}^{t} (\#C_k - 1) \le \tfrac{1}{2}d(d-1). \qquad \square$$

PROOF OF THEOREM 1.1. Let $\mathcal{O}$ be an order in K. Notice that we have the relations

$$\frac{\alpha^{(i)}-\alpha^{(1)}}{\alpha^{(2)}-\alpha^{(1)}}+\frac{\alpha^{(2)}-\alpha^{(i)}}{\alpha^{(2)}-\alpha^{(1)}}=1 \quad (i=3,\dots,d). \tag{2.6}$$

The group homomorphism from $(G^*)^{d(d-1)/2} \to (G^*)^{2d-4}$,

$$(x_{ij} : 1 \le i < j \le d) \mapsto (x_{31}/x_{21}, x_{23}/x_{21}, \dots, x_{d1}/x_{21}, x_{2d}/x_{21})$$

maps, for every $\alpha \in S(\mathcal{O})$, the tuple $\rho(\alpha)$ as defined in Lemma 2.4 to

$$\tau(\alpha) := \left(\frac{\alpha^{(3)}-\alpha^{(1)}}{\alpha^{(2)}-\alpha^{(1)}}, \frac{\alpha^{(2)}-\alpha^{(3)}}{\alpha^{(2)}-\alpha^{(1)}}, \dots, \frac{\alpha^{(d)}-\alpha^{(1)}}{\alpha^{(2)}-\alpha^{(1)}}, \frac{\alpha^{(2)}-\alpha^{(d)}}{\alpha^{(2)}-\alpha^{(1)}}\right).$$

Together with Lemma 2.4, this implies that the rank of the multiplicative group generated by the tuples $\tau(\alpha)$ ($\alpha \in S(\mathcal{O})$) is at most $\frac{1}{2}d(d-1)$. By applying Lemma 2.2 to (2.6), it follows that among the tuples $\tau(\alpha)$ ($\alpha \in \mathcal{O}$) there are at most $2^{8(d(d-1)/2+2d-5)} = 2^{4(d+5)(d-2)}$ distinct ones.

Theorem 1.1 follows once we have proved that if $\alpha_1, \alpha_2 \in S(\mathcal{O})$ and $\tau(\alpha_1) = \tau(\alpha_2)$, then α_1, α_2 are equivalent. Take such α_1, α_2. By simple linear algebra, there exist unique $\lambda \in G^*$, $\mu \in G$ such that $\alpha_2^{(i)} = \lambda\alpha_1^{(i)} + \mu$ for $i = 1, \dots, d$. Thus,

$$\lambda = \frac{\alpha_2^{(i)}-\alpha_2^{(j)}}{\alpha_1^{(i)}-\alpha_1^{(j)}} \quad \text{for } 1 \le i < j \le d.$$

By Galois symmetry we have $\lambda \in \mathbb{Q}^*$, and by Lemma 2.3, λ is an algebraic unit. Hence $\lambda = \pm 1$. But then, $\mu = \alpha_2^{(i)} \pm \alpha_1^{(i)}$ for $i = 1, \dots, d$. This shows that $\mu \in \mathbb{Q}$ and μ is an algebraic integer, hence $\mu \in \mathbb{Z}$. So α_1, α_2 are indeed equivalent. This concludes the proof of Theorem 1.1. □

3. Sketch of the proof of Theorem 1.2

The next proposition is our main tool. Let G be a field of characteristic 0, and Γ a finitely generated subgroup of $(G^*)^2$. We consider equations

$$ax + by = 1 \quad \text{in } (x, y) \in \Gamma \tag{3.1}$$

where $a, b \in G^*$. By LANG [13, 1960] or Proposition 2.1 above, each such equation has only finitely many solutions. We call the pair (a, b) *normalized* if $(1, 1)$ is a solution of (3.1), i.e., if $a + b = 1$. In general, if (x_0, y_0) is a solution of (3.1) then the pair (ax_0, by_0) is normalized, and the equation $(ax_0)x + (by_0)y = 1$ in $(x, y) \in \Gamma$ has the same number of solutions as (3.1).

Proposition 3.1. *There are at most finitely many normalized pairs $(a,b) \in (G^*)^2$ such that (1.1) has more than two solutions, the pair $(1,1)$ included.*

PROOF. EVERTSE, GYŐRY, STEWART, TIJDEMAN [7, 1988]. □

We keep the notation from the previous section; thus, K is an algebraic number field of degree $d \geq 3$ and G is its normal closure. The next lemma, which we state without proof, is used in both the proofs of Theorems 1.2 and 1.3. For x with $\mathbb{Q}(x) = K$ and distinct $i,j,k \in \{1,\ldots,d\}$ we put

$$x^{(ijk)} := \frac{x^{(i)} - x^{(j)}}{x^{(i)} - x^{(k)}}.$$

Lemma 3.2. *Let $c_{ijk} \in G^*$ $(1 \leq i < j < k \leq d)$ be given. Then the set of $\beta \in \mathcal{O}_K$ such that*

$$\beta^{(ijk)} = c_{ijk} \text{ for } 1 \leq i < j < k \leq d, \quad \mathbb{Z}[\beta] \text{ is two times monogenic}$$

is contained in finitely many equivalence classes.

PROOF. [3], Lemmas 5.3, 6.2. □

To give a flavour, we prove Theorem 1.2 under the assumption that K is three times transitive. This condition can be dropped, but then the proof becomes more complicated. Our assumption on K implies the following:

Lemma 3.3. *Let $\mathcal{O}$ be an order in K and suppose that $\mathbb{Z}[\alpha_1] = \mathbb{Z}[\alpha_2] = \mathcal{O}$ and $\alpha_1^{(123)} = \alpha_2^{(123)}$. Then α_1, α_2 are equivalent.*

PROOF. By taking conjugates, using that K is three times transitive, it follows that also $\alpha_1^{(ijk)} = \alpha_2^{(ijk)}$ for $1 \leq i < j < k \leq d$. Then, similarly to the last part of the proof of Theorem 1.1 one shows that α_1, α_2 are equivalent. □

Let $\mathcal{O}$ be a three times monogenic order in K. Fix β with $\mathbb{Z}[\beta] = \mathcal{O}$. We claim that the equation

$$\beta^{(123)}x + \beta^{(321)}y = 1 \quad \text{in } x, y \in \mathcal{O}_G^* \tag{3.2}$$

has at least three distinct solutions, including $(1,1)$. Indeed, let $\alpha \in S(\mathcal{O})$. Then by Lemma 2.3, we have $x_\alpha := \alpha^{(123)}/\beta^{(123)} = u_{12}(\alpha,\beta)/u_{13}(\alpha,\beta) \in \mathcal{O}_G^*$ and likewise, $y_\alpha := \alpha^{(321)}/\beta^{(321)} \in \mathcal{O}_G^*$. Since $\alpha^{(123)} + \alpha^{(321)} = 1$ this shows that (x_α, y_α) is a solution of (3.2). By our assumption that $\mathcal{O}$ is three times monogenic, and by Lemma 3.3, there are at least three different values among the numbers $\alpha^{(123)}$, hence among the numbers x_α, for $\alpha \in S(\mathcal{O})$. So indeed, (3.2) has at least three distinct solutions, and taking $\alpha = \beta$ we get the solution $(1,1)$. Now by Proposition 3.1, if β runs through the numbers in $\mathcal{O}_K$ such that $\mathbb{Z}[\beta]$ is three times monogenic, then $\beta^{(123)}$ runs through a finite set. By taking

conjugates, using that K is three times transitive, it follows that also $\beta^{(ijk)}$ runs through a finite set, for all distinct $i, j, k \in \{1, \dots, d\}$. But then by Lemma 3.2, the β under consideration lie in only finitely many equivalence classes, and so there are only finitely many possibilities for the order $\mathbb{Z}[\beta]$. This completes our proof. □

4. Sketch of the proof of Theorem 1.3

Let for the moment G be any field of characteristic 0 and m an integer ≥ 2. An algebraic subset of $(G^*)^m$ is the set of common zeros in $(G^*)^m$ of a set of polynomials in $G[X_1, \dots, X_m]$. An algebraic subgroup of $(G^*)^m$ is an algebraic subset which is also a subgroup of $(G^*)^m$ under coordinatewise multiplication. An algebraic coset in $(G^*)^m$ is a coset $\mathbf{a}H = \{\mathbf{a} \cdot \mathbf{x} : \mathbf{x} \in H\}$, where $\mathbf{a} \in (G^*)^m$ and H is an algebraic subgroup of $(G^*)^m$. The proof of Theorem 1.3 uses the following result.

Proposition 4.1. *Let X be an algebraic subset of $(G^*)^m$ and Γ a finitely generated subgroup of $(G^*)^m$. Then $X \cap \Gamma$ is contained in a finite union of algebraic cosets $\mathbf{a}_1 H_1 \cup \cdots \cup \mathbf{a}_t H_t$ with $\mathbf{a}_i H_i \subseteq X$ for $i = 1, \dots, t$.*

Proof. Laurent [14, 1984]. □

Like in the statement of Theorem 1.3, let K be number field of degree $d \geq 4$, and assume that either $d = 4$ and the normal closure of K has Galois group S_4, or $d \geq 5$ and K is four times transitive. Denote by G the normal closure of K. We consider pairs (α, β) such that

$$\alpha, \beta \in \mathcal{O}_K,\ \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = K,\ \mathbb{Z}[\alpha] = \mathbb{Z}[\beta], \quad \alpha, \beta \text{ are inequivalent.} \tag{4.1}$$

We have to show that there is a finite collection of orders in K, such that for every pair (α, β) with (4.1), the order $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ either belongs to this collection or is of type I or (if $d = 4$) of type II.

Let Γ be the multiplicative group generated by the tuples

$$\left(\frac{\alpha^{(i)} - \alpha^{(j)}}{\beta^{(i)} - \beta^{(j)}} : 1 \leq i < j \leq d \right),$$

for all α, β with (4.1). By Lemma 2.3, Γ is a subgroup of $(\mathcal{O}_G^*)^{d(d-1)/2}$. Hence Γ is finitely generated.

Take α, β with (4.1). Put

$$u_{ij} := \frac{\alpha^{(i)} - \alpha^{(j)}}{\beta^{(i)} - \beta^{(j)}} \quad (1 \le i, j \le d,\ i \ne j).$$

Write again $x^{(ijk)} := (x^{(i)} - x^{(j)})/(x^{(i)} - x^{(k)})$ for x with $\mathbb{Q}(x) = K$ and distinct indices i, j, k. Then from

$$\beta^{(jik)} + \beta^{(kij)} = 1,$$

$$\beta^{(jik)} \cdot \frac{u_{ij}}{u_{jk}} + \beta^{(kij)} \cdot \frac{u_{ik}}{u_{jk}} = \alpha^{(jik)} + \alpha^{(kij)} = 1,$$

it follows that

$$\beta^{(ijk)} \cdot \Big(1 - \frac{u_{ij}}{u_{jk}}\Big) = 1 - \frac{u_{ik}}{u_{jk}} \quad \text{for any distinct } i, j, k \in \{1, \dots, d\}. \tag{4.2}$$

We can eliminate the terms depending on β by applying the above identities with the triples (i, j, k), (i, k, l) and (i, l, j), and using $\beta^{(ijk)}\beta^{(ikl)}\beta^{(ilj)} = 1$. This leads to

$$\Big(1 - \frac{u_{ij}}{u_{jk}}\Big)\Big(1 - \frac{u_{ik}}{u_{kl}}\Big)\Big(1 - \frac{u_{il}}{u_{jl}}\Big) = \Big(1 - \frac{u_{ik}}{u_{jk}}\Big)\Big(1 - \frac{u_{il}}{u_{kl}}\Big)\Big(1 - \frac{u_{ij}}{u_{jl}}\Big)$$
$$\text{for any distinct } i, j, k, l \in \{1, \dots, d\}. \tag{4.3}$$

It follows that the tuple $\mathbf{u} = (u_{ij} : 1 \le i < j \le d)$ lies in $X \cap \Gamma$, where X is the algebraic subset of $(G^*)^{d(d-1)/2}$ defined by (4.3).

We apply Proposition 4.1 to $X \cap \Gamma$. By a precise analysis of the algebraic set X and the group Γ (see [3]) it can be shown that there is a finite set $\mathcal{S}$ such that for each $\mathbf{u} \in X \cap \Gamma$, at least one of the following three alternatives holds:

(**i**) $u_{ij}/u_{ik} \in \mathcal{S}$ for all distinct $i, j, k \in \{1, \dots, d\}$;

(**ii**) $u_{ij}u_{kl} = u_{ik}u_{jl}$ for all distinct $i, j, k, l \in \{1, \dots, d\}$;

(**iii**) $d = 4$ and $u_{12} = -u_{34},\ u_{13} = -u_{24},\ u_{14} = -u_{23}$.

In the deduction of this, Bérczes et.al. heavily used the conditions imposed on K in Theorem 1.3; probably without these conditions there are more alternatives.

If (α, β) run through the set of pairs with (4.1) for which the corresponding tuple $\mathbf{u}$ satisfies (i), then by (4.2), the quantities $\beta^{(ijk)}$ $(1 \le i < j < k \le d)$ run through a finite set. Now Lemma 3.2 implies that the β lie in at most finitely

many equivalence classes, and thus, that there are only finitely many possibilities for the order $\mathbb{Z}[\beta]$.

If (α, β) is a pair with (4.1) such that the corresponding tuple $\mathbf{u}$ satisfies (ii), then

$$\frac{(\alpha^{(i)} - \alpha^{(j)})(\alpha^{(k)} - \alpha^{(l)})}{(\alpha^{(i)} - \alpha^{(k)})(\alpha^{(j)} - \alpha^{(l)})} = \frac{(\beta^{(i)} - \beta^{(j)})(\beta^{(k)} - \beta^{(l)})}{(\beta^{(i)} - \beta^{(k)})(\beta^{(j)} - \beta^{(l)})}$$

for all distinct $i, j, k, l \in \{1, \ldots, d\}$, i.e., the cross ratio of any four of the $\alpha^{(i)}$ is equal to that of the corresponding four $\beta^{(i)}$. By elementary projective geometry on $\mathbb{P}^1(G)$, there is a matrix $A = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2, G)$ such that $\beta^{(i)} = (a_1\alpha^{(i)} + a_2)/(a_3\alpha^{(i)} + a_4)$ for $i = 1, \ldots, d$. By Galois symmetry, we can choose A from $\mathrm{GL}(2, \mathbb{Q})$, and in [3] it is shown that A can be chosen from $\mathrm{GL}(2, \mathbb{Z})$. Hence $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ is an order of type I.

If (α, β) is a pair with (4.1) such that the corresponding $\mathbf{u}$ satisfies (iii) then by elementary algebra it can be shown that $\beta = a_0 + a_1\alpha + a_2\alpha^2$ and $\alpha = b_0 + b_1\beta + b_2\beta^2$ for certain $a_i, b_i \in \mathbb{Q}$ with $a_2 b_2 \neq 0$. But since $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ it then follows that $a_i, b_i \in \mathbb{Z}$ for $i = 1, 2, 3$. Hence $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ is an order of type II. This completes our sketch of the proof of Theorem 1.3. □

References

[1] M. A. Bennett, On the representation of unity by binary cubic forms, *Trans. Amer. Math. Soc.* **353** (2001), 1507–1534.

[2] A. Bérczes, On the number of solutions of index form equations, *Publ. Math. Debrecen* **56** (2000), 251–262.

[3] A. Bérczes, J.-H. Evertse and K. Győry, Multiply monogenic orders, preprint, arXiv:1103.4740v1 [math.NT].

[4] F. Beukers and H. P. Schlickewei, The equation $x + y = 1$ in finitely generated groups, *Acta Arith.* **78** (1996), 189–199.

[5] Yu. Bilu, I. Gaál and K. Győry, Index form equations in sextic fields: a hard computation, *Acta Arith.* **115** (2004), 85–96.

[6] J.-H. Evertse and K. Győry, On unit equations and decomposable form equations, *J. reine angew. Math.* **358** (1985), 6–19.

[7] J.-H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, On S-unit equations in two unknowns, *Invent. Math.* **92** (1988), 461–477.

[8] I. Gaál, Diophantine equations and power integral bases, New Computational Methods, *Birkhäuser, Boston*, 2002.

[9] I. Gaál and N. Schulte, Computing all power integral bases of cubic fields, *Math. Comp.* **53** (1989), 689–696.

[10] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné, *Acta Arith.* **23** (1973), 419–426.

[11] K. Győry, Sur les polynômes à coefficients entiers et de dicriminant donné III, *Publ. Math. Debrecen* **23** (1976), 141–165.

[12] K. Győry, Corps de nombres algébriques d'anneau d'entiers monogène, in: Séminaire Delange-Pisot-Poitou, 20e année: 1978/1979, Théorie des nombres, Fasc. 2 (French), *Secrétariat Math., Paris*, 1980, pp. Exp. No. 26, 7.

[13] S. Lang, Integral points on curves, *Inst. Hautes Études Sci. Publ. Math.* **6** (1960), 27–43.

[14] M. Laurent, Équations diophantiennes exponentielles, *Invent. Math.* **78** (1984), 299–327.

[15] L. Miller-Sims and L. Robertson, Power integral bases for real cyclotomic fields, *Bull. Austral. Math. Soc.* **71** (2005), 167–173.

J.-H. EVERTSE
UNIVERSITEIT LEIDEN
MATHEMATISCH INSTITUUT
POSTBUS 9512, 2300 RA LEIDEN
THE NETHERLANDS

E-mail: evertse@math.leidenuniv.nl

(Received February 14, 2011; revised April 12, 2011)