Thue Equations associated with Ankeny-Brauer-Chowla Number Fields

F. Halter-Koch
Institut für Mathematik
Karl-Franzens-Universität Graz
Heinrichstraße 36
A-8010 Graz
Austria

G. Lettl
Institut für Mathematik
Karl-Franzens-Universität Graz
Heinrichstraße 36
A-8010 Graz
Austria

A. Pethö *
Laboratory of Informatics
University of Medicine
Nagyerdei Krt. 98
H-4032 Debrecen
Hungary

R.F. Tichy
Institut für Mathematik
Technische Universität Graz
Steyrergasse 30
A-8010 Graz
Austria

Abstract. For a wide class of one-parameter families of Thue equations of arbitrary degree $n \geq 3$ all solutions are determined if the parameter is sufficiently large. The result is based on the Lang-Waldschmidt conjecture, on the primitivity of the associated number fields and on an index bound, which does not depend on the coefficients. Applying the theory of Hilbertian fields and results on thin sets, primitivity is proved for almost all choices (in the sense of density) of the parameters.

*This paper was written in the academic year 1995/96 when the author was a visiting professor at the TU Graz

1 Introduction

For an algebraic number field $\mathbb{K}$, we denote by $N_{\mathbb{K}/\mathbb{Q}}$ the norm for $\mathbb{K}/\mathbb{Q}$. If $\mathbb{K} = \mathbb{Q}(\alpha)$, where α is an algebraic integer, then the polynomial $F(x, y) = N_{\mathbb{K}/\mathbb{Q}}(x - \alpha y)$ is an irreducible polynomial over $\mathbb{Z}$, and the binary diophantine equation

$$F(x, y) = 1$$

is called a *Thue equation* . Bombieri and Schmidt [BSch] proved that the number of solutions of a Thue equation of degree $n \geq 3$ is at most $O(n)$, and they observed that this result is best possible. Indeed, the Thue equation

$$\prod_{i=1}^{n}(x - a_i y) + y^n = 1$$

with distinct integers $a_i \in \mathbb{Z}$, has at least $n + 1$ solutions, namely

$$(x, y) = (1, 0), (a_1, 1), (a_2, 1), \ldots, (a_n, 1)\,.$$

In this paper, we shall be concerned with the Thue equation

$$\prod_{i=1}^{n}(x - a_i y) \pm y^n = \pm 1\ , \tag{1}$$

and we shall call any solution of (1) of the form $\pm(x, y) = (1, 0)$ or $\pm(x, y) = (a_i, 1)$ a *trivial solution*.

For $n = 3$, $a_1 = 0$, $a_2 = 1$, $a_3 = a \in \mathbb{Z}$, Mignotte and Tzanakis [MT] proved that if $|a| > 3.67{\cdot}10^{32}$, then (1) has only one non-trivial solution, namely $(x, y) = (-a{+}3, -a{+}2)$.

For $n = 4$, $a_1 = 0$, $a_2 = 1$, $a_3 = -1$, $a_4 = a \in \mathbb{Z}$, equation (1) was completely solved for $|a| \geq 2$ by Mignotte, Pethö and Roth [MPR] (for $|a| > 10^{28}$ already by Pethö [Pe]). In this case, there is again exactly one (parametrized) non-trivial solution, namely $(x, y) = (1, -a)$.

E. Thomas [Th] investigated equation (1) in the case, where the coefficients a_i are integer polynomials of distinct degrees in an integer variable a, $a_i = a_i(a) \in \mathbb{Z}[a]$. He conjectured that (1) has only the trivial solutions if a is large enough, and pointed out that the conjecture might also be true in specific cases of polynomials of equal degrees. In the case $n = 3$, $a_1 = 0$, $a_2 = a^k$, $a_3 = a^l$, where $a \in \mathbb{Z}$ and $0 < k < l$ are integers, Thomas proved in [Th] that for $a \geq \left(2 \cdot 10^6\,(k + 2l)\right)^{4.85/(l-k)}$, (1) has only the trivial solutions.

In section 4 we shall examine Thomas' conjecture in the case where $a_1, \ldots, a_{n-1}$ are distinct integers and $a_n = a$ is an integral parameter. We make the additional assumption that the algebraic number field $\mathbb{K} = \mathbb{Q}(\alpha)$, where α is a root of the polynomial

$$P(x) = \prod_{i=1}^{n}(x - a_i) \pm 1 \in \mathbb{Z}[x]\,,$$

is primitive. We investigate the unit group of the order $\mathcal{O} = \mathbb{Z}[\alpha]$ of $\mathbb{K}$ and derive, using the lower regulator bound of M. Pohst, an upper bound for certain linear forms in logarithms

of algebraic numbers. Unfortunately, this upper bound is not sharp enough to prove Thomas' conjecture by comparing it even with the best known lower bounds for linear forms in logarithms, see e.g. [BW]. However, assuming the *Lang-Waldschmidt conjecture* [La1], we are able to prove Thomas' conjecture in the cases described above (Theorem 4.1). On account of this result, the equations of degree 3 and 4 cited above, which possess a parametrized non-trivial solution, should be considered as singular phenomena.

Algebraic number fields $\mathbb{K} = \mathbb{Q}(\alpha)$, where α is a zero of a polynomial $P(x)$ as above, were first considered by Ankeny, Brauer and Chowla [ABC] as examples of number fields which usually have a large class number. Therefore we call these fields Ankeny-Brauer-Chowla number fields.

In section 2 we investigate the unit groups involved. We do this in a slightly more general setting, allowing also complex conjugates. In order to apply the lower regulator bounds of Pohst, we must assume that our number field is primitive. We have no explicit condition which guarantees primitivity for a large class of equations. However, we shall prove that in almost all cases (in the sense of density) the Galois group of the generating polynomial is the symmetric one, which in particular implies primitivity. Again, the investigations concerning the Galois group will be performed in a more general setting. This is done in section 3.

2 The Unit Group

We start by specifying notations and assumptions which remain valid throughout this chapter. Let $s, t \in \mathbb{N}_0$ be such that $n = s + 2t \geq 3$ and $r = s + t - 1 \geq 1$. Suppose that $d \in \mathbb{Z}\backslash\{0\}$, $a_1, \ldots, a_s \in \mathbb{Z}$, and let $a_{s+1}, \ldots, a_n \in \mathbb{C}$ be imaginary-quadratic integers such that $a_{j+t} = \overline{a_j}$ for $s+1 \leq j \leq s+t$. We make the following two assumptions **A.** and **B.** .

A. For all $1 \leq i < j \leq n$, $d|(a_i - a_j)$ and $|a_i - a_j| \geq 1$.

B. Either

B1. $s \geq 1$ and $a = a_s \geq 3$ is sufficiently large, compared with $a_1, \ldots, a_{s-1}, a_{s+1}, \ldots, a_n$.

or

B2. The following two inequalities hold:

$$|a_i - a_j| \geq \max\{2, |d|\} \quad \text{for } 1 \leq i < j \leq n \tag{2}$$

$$\prod_{\substack{j=1 \\ j \neq i}}^{n} \left(|a_i - a_j| - \frac{1}{3} \right) > \max\left\{ 3|d|, n^{\frac{5}{4}} \right\} \quad \text{for } 1 \leq i \leq n \ . \tag{3}$$

Note that condition (3) is not a very restrictive one. It follows from (2) whenever $n \geq 5$ or $|d| > 3$. Also in the remaining cases ($n = 3, 4$ and $|d| \leq 3$) there are only some special constellations of $a_1, \ldots, a_n$ in which (3) is violated.

Now we set

$$n^* = \begin{cases} 1 & \text{if } |d| = 1 \\ n & \text{if } |d| > 1 \end{cases} \ , \quad e_j = \begin{cases} 1 & \text{for } 1 \leq j \leq s \\ 2 & \text{for } s+1 \leq j \leq s+t \end{cases} \ , \quad \delta = \begin{cases} \frac{2}{a} & \text{in case } \underline{\textbf{B1.}} \\ \frac{1}{3} & \text{in case } \underline{\textbf{B2.}} \end{cases} \ .$$

For $1 \le i \le n$, we put $D_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} \Big(|a_i - a_j| - \delta \Big)$, and we obtain in both cases

$$D_i > \max\Big\{ \frac{|d|}{\delta}, n^{\frac{5}{4}} \Big\} .$$

Indeed, in case **B2.** this is just (3), and in case **B1.** the inequality is valid for sufficiently large a.

We consider the polynomial

$$P(x) = \prod_{j=1}^{n} (x - a_j) - d \in \mathbb{Z}[x],$$

and we formulate our preliminary results in a series of Lemmas.

Lemma 2.1 *The polynomial $P(x)$ has n distinct zeroes $\alpha_1, \ldots, \alpha_n$, which can be indexed in such a way that*

$$\alpha_1, \ldots, \alpha_s \in \mathbb{R} , \quad \alpha_{j+t} = \overline{\alpha_j} \quad \textit{for } s+1 \le j \le s+t$$

and

$$|\alpha_j - a_j| < \delta \quad \textit{for } 1 \le j \le n . \tag{4}$$

They satisfy the inequalities

$$(1-\delta)|a_i - a_j| \le |a_i - a_j| - \delta < |\alpha_i - a_j| < (1+\delta)|a_i - a_j|$$

for all $1 \le i, j \le n$ with $i \neq j$, and

$$\frac{|d|}{(1+\delta)^{n-1}} < |\alpha_j - a_j| \prod_{\substack{i=1 \\ i \neq j}}^{n} |a_i - a_j| < \frac{|d|}{(1-\delta)^{n-1}}$$

for all $1 \le j \le n$.

Proof. We set $d = |d|\varepsilon$ with $\varepsilon \in \{\pm 1\}$, and we may assume that $a_1 < a_2 < \ldots < a_s$. For $1 \le i \le s$, we have $\varepsilon P(a_i) = -|d| < 0$, and

$$\varepsilon P(a_i + (-1)^{s-i}\varepsilon\delta) \ge \delta \prod_{\substack{j=1 \\ j \neq i}}^{n} (|a_i - a_j| - \delta) - |d| = \delta D_i - |d| > 0.$$

Therefore P has a real zero α_i between a_i and $a_i + (-1)^{s-i}\varepsilon\delta$.

For $s+1 \le i \le s+t$ and $\xi \in \mathbb{C}$ with $|\xi| = \delta$, we have

$$|P(a_i + \xi) + d| = \prod_{j=1}^{n} |a_i - a_j + \xi| \ge \delta \prod_{\substack{j=1 \\ j \neq i}}^{n} (|a_i - a_j| - \delta) = \delta D_i > |d| .$$

Thus by Rouché's theorem, P has exactly one zero in the disc with radius δ around a_i. The other inequalities follow easily by using the triangle inequality and

$$\prod_{i=1}^{n} |\alpha_i - a_j| = |d|.$$

□

Using the zeroes $\alpha_1, \ldots, \alpha_n$ of $P(x)$ as specified in Lemma 2.1 we define, for $1 \le i \le n$ and $1 \le j \le s+t$, numbers $\eta_{ij} \in \mathbb{Z}[\alpha_i]$ as follows. For $|d| = 1$,

$$\eta_{ij} = \begin{cases} \alpha_i - a_j & \text{if } 1 \le j \le s \\ (\alpha_i - a_j)(\alpha_i - \overline{a_j}) & \text{if } s+1 \le j \le s+t \end{cases}.$$

For $|d| > 1$,

$$\eta_{ij} = \begin{cases} \dfrac{(\alpha_i - a_j)^n}{d} & \text{if } 1 \le j \le s \\ \dfrac{((\alpha_i - a_j)(\alpha_i - \overline{a_j}))^n}{d^2} & \text{if } s+1 \le j \le s+t \end{cases}.$$

As in [H-K1], we see that $\eta_{ij} \in \mathbb{Z}[\alpha_i]$ are units in $\mathbb{Z}[\alpha_i]$ satisfying $\prod_{j=1}^{s+t} \eta_{ij} = \pm 1$. Concerning their size, Lemma 2.1 implies, for $i \ne j$,

$$\left.\begin{array}{rcccll} (1-\delta)^{n^*} & \le & |\eta_{ij}| \dfrac{|d|}{|a_i - a_j|^{n^*}} & \le & (1+\delta)^{n^*} & \text{if } 1 \le j \le s \\ (1-\delta)^{2n^*} & \le & |\eta_{ij}| \dfrac{|d|^2}{(|a_i - a_j||a_i - \overline{a_j}|)^{n^*}} & \le & (1+\delta)^{2n^*} & \text{if } s+1 \le j \le s+t\ . \end{array}\right\} \quad (5)$$

Lemma 2.2

i) *$P(x)$ is irreducible.*

ii) *For $1 \le j \le s+t$, the numbers η_{ij} $(1 \le i \le s)$ are the real conjugates, and the numbers $\eta_{i,j},\ \eta_{i+t,j} = \overline{\eta_{i,j}}$ $(s+1 \le i \le s+t)$ are the pairs of complex conjugates of $\eta_{1,j}$.*

iii) *Every subsystem of size r of $\eta_{11}, \ldots, \eta_{1,s+t}$ is a system of independent units of $\mathbb{Z}[\alpha_1]$.*

Proof. In case **B2.** , (5) implies $|\eta_{ij}| > 1$ for $i \ne j$. Hence the assertions follow as in [H-K2], Lemma 3 and [H-K1], Satz 2.

Now suppose that **B1.** holds. We use the o- and O-notation for $a \to \infty$ (note that the constants depend on $d, a_1, \ldots, a_{s-1}, a_{s+1}, \ldots, a_{s+t}$). (5) implies for $i \ne j$

$$|\eta_{ij}| = \begin{cases} \left(\dfrac{a^{n^*}}{|d|}\right)^{e_j} (1 + o(1)) & \text{if } i = s \text{ or } j = s, \\ e^{O(1)} & \text{if } i \ne s \text{ and } j \ne s. \end{cases}$$

i) Assume on the contrary that P is reducible. Then P possesses a monic irreducible factor $Q \in \mathbb{Z}[x]$ such that $Q(\alpha_s) \ne 0$. If $\{\alpha_i \mid i \in I\}$ is the set of zeroes of Q, then the corresponding set $\{\eta_{is} \mid i \in I\}$ is a full system of conjugated algebraic units, each of modulus greater than 1, a contradiction.

ii) is an obvious consequence of **i)**.

iii) Since $\eta_{1,1}\cdot\ldots\cdot\eta_{1,s+t}=\pm1$ it is sufficient to prove that $\{\eta_{1j}\mid 1\le j\le s+t,\ j\ne s\}$ is a system of independent units. We calculate its regulator R_η. By definition,

$$R_\eta=\left|\det\Big[e_i\log|\eta_{ij}|\Big]_{\substack{1\le i,j\le s+t\\ i,j\ne s}}\right|=(\log a)^r\left|\det\Big[e_i\frac{\log|\eta_{ij}|}{\log a}\Big]_{\substack{1\le i,j\le s+t\\ i,j\ne s}}\right|\ .$$

For $s\ne i\ne j\ne s$ we have $e_i\frac{\log|\eta_{ij}|}{\log a}=o(1)$. For $i=j\ne s$, the estimate

$$|\eta_{jj}|<\begin{cases}\frac{2}{a} & \text{if } 1\le j\le s,\\ \frac{2}{a}\Big(|a_j-\overline{a_j}|+\frac{2}{a}\Big) & \text{if } s+1\le j\le t\end{cases}$$

implies $e_j\frac{\log|\eta_{jj}|}{\log a}<-1+o(1)$. If a is sufficiently large, we obain $R_\eta\ne0$, and the assertion follows.

□

Since P is irreducible, the algebraic number field $\mathbb{K}=\mathbb{Q}(\alpha_1)$ is of degree n with s real and t complex conjugates. We consider the order $\mathcal{O}=\mathbb{Z}[\alpha_1]$ of $\mathbb{K}$, we denote by $D_\mathcal{O}$ its discriminant, by $U_\mathcal{O}$ its group of units and by $R_\mathcal{O}$ its regulator. Let U_η be the subgroup of $U_\mathcal{O}$ generated by $\eta_{1,1},\ldots,\eta_{1,s+t}$ and R_η its regulator. It is well known that

$$(U_\mathcal{O}:U_\eta)=w\ \frac{R_\eta}{R_\mathcal{O}}\ ,$$

where w denotes the index of the torsion subgroups of $U_\mathcal{O}$ and U_η. We shall obtain an upper bound for the index $(U_\mathcal{O}:U_\eta)$ which only depends on s and t, provided that $\mathbb{K}$ is primitive (i.e. there are no intermediate fields between $\mathbb{Q}$ and $\mathbb{K}$). For w we have the trivial bound $w\le\psi(s,t)$, where $\psi(s,t)=2$ if $s\ge1$, and $\psi(0,t)=\max\{k\in\mathbb{N}\mid\varphi(k)|2t\}$.

Lemma 2.3 *We have*

$$R_\eta\le\left(\frac{2n^*}{r}\Big(n^2\log\frac{1+\delta}{1-\delta}+\log\prod_{j=1}^n D_j\Big)\right)^r\ .$$

Proof. By Hadamard's inequality,

$$\begin{aligned}R_\eta &= \left|\det\Big[e_i\log|\eta_{ij}|\Big]_{1\le i,j\le r}\right|\le\prod_{j=1}^r\left(\sum_{i=1}^r(e_i\log|\eta_{ij}|)^2\right)^{1/2}\\ &\le \prod_{j=1}^r\left(\sum_{i=1}^{s+t}e_i\Big|\log|\eta_{ij}|\Big|\right)=\prod_{j=1}^r\Bigg(\sum_{\substack{i=1\\|\eta_{ij}|>1}}^{s+t}e_i\log|\eta_{ij}|-\sum_{\substack{i=1\\|\eta_{ij}|<1}}^{s+t}e_i\log|\eta_{ij}|\Bigg)\\ &= 2^r\prod_{j=1}^r\Bigg(\sum_{\substack{i=1\\|\eta_{ij}|>1}}^{s+t}e_i\log|\eta_{ij}|\Bigg),\end{aligned}$$

since $\sum_{i=1}^{s+t} e_i \log|\eta_{ij}| = \log|N_{\mathbb{K}/\mathbb{Q}}(\eta_{1j})| = 0$.
Using the inequality between the arithmetic and the geometric mean, we obtain

$$|R_\eta| \le \left(\frac{2}{r}\log\prod_{j=1}^{r}\prod_{\substack{i=1\\|\eta_{ij}|>1}}^{s+t}|\eta_{ij}|^{e_i}\right)^r.$$

Now (5) implies, for $1 \le j \le r$,

$$\prod_{\substack{i=1\\|\eta_{ij}|>1}}^{s+t}|\eta_{ij}|^{e_i} \le \left[(1+\delta)^n\prod_{\substack{i=1\\i\neq j}}^{n}|a_i-a_j|\right]^{n^*e_j} \le \left(\left(\frac{1+\delta}{1-\delta}\right)^n D_j\right)^{n^*e_j},$$

and consequently

$$\prod_{j=1}^{r}\prod_{\substack{i=1\\|\eta_{ij}|>1}}^{s+t}|\eta_{ij}|^{e_i} \le \left(\left(\frac{1+\delta}{1-\delta}\right)^{n^2}\cdot\prod_{j=1}^{n}D_j\right)^{n^*},$$

which implies the assertion.

□

Lemma 2.4 *If $\mathbb{K}$ is primitive, then*

$$R_{\mathcal{O}} \ge \left(\frac{3}{n(n^2-1)-6t}\right)^{\frac{r}{2}}\left(\frac{2^t}{n\gamma_r^r}\right)^{\frac{1}{2}}\left(\log\prod_{j=1}^{n}D_j - n\log n\right)^r.$$

Proof. By [PZ], ch. 5.6, (6.22), we have

$$R_{\mathcal{O}} \ge \left(\frac{3}{n(n^2-1)-6t}\right)^{\frac{r}{2}}\left(\frac{2^t}{n\gamma_r^r}\right)^{\frac{1}{2}}\left(\log|D_{\mathcal{O}}| - n\log n\right)^r,$$

provided that $\mathbb{K}$ is primitive and $|D_{\mathcal{O}}| > n^n$. Since

$$|D_{\mathcal{O}}| = \prod_{j=1}^{n}|P'(\alpha_j)| = \prod_{j=1}^{n}\prod_{\substack{i=1\\i\neq j}}^{n}|\alpha_j-a_i| \ge \prod_{j=1}^{n}\prod_{\substack{i=1\\i\neq j}}^{n}(|a_i-a_j|-\delta) = \prod_{j=1}^{n}D_j > n^{\frac{5}{4}n},$$

the assertion follows.

□

Theorem 2.1 *If $\mathbb{K}$ is primitive and conditions* **A.** *and* **B.** *hold, then*

$$(U_{\mathcal{O}} : U_\eta) \le \psi(s,t)\left(\frac{16nn^*}{r}\right)^r\left(\frac{n(n^2-1)-6t}{3}\right)^{\frac{r}{2}}\left(\frac{n\gamma_r^r}{2^t}\right)^{\frac{1}{2}}.$$

Proof. By Lemmata 2.3 and 2.4,

$$\begin{aligned}(U_{\mathcal{O}} : U_\eta) &\leq \psi(s,t)\,\frac{R_\eta}{R_{\mathcal{O}}} \\ &\leq \psi(s,t)\left(\frac{2n^*}{r}\right)^r \left(\frac{n(n^2-1)-6t}{3}\right)^{\frac{r}{2}} \left(\frac{n\gamma_r^r}{2^t}\right)^{\frac{1}{2}} \left(\frac{n^2\log\frac{1+\delta}{1-\delta}+\log\prod_{j=1}^n D_j}{\log\prod_{j=1}^n D_j - n\log n}\right)^r .\end{aligned}$$

Since $D_1\cdot\ldots\cdot D_n > n^{\frac{5}{4}n}$, we obtain $\log\prod_{j=1}^n D_j - n\log n > \frac{1}{4}n\log n$, and consequently

$$\frac{n^2\log\frac{1+\delta}{1-\delta}+\log\prod_{j=1}^n D_j}{\log\prod_{j=1}^n D_j - n\log n} < \frac{4n^2\log 5}{n\log n} + 5 < 8n,$$

which implies the Theorem.

□

3 The Galois Group

Definition 3.1 *Let $m \geq 2$, $d \neq 0$, $s \geq 0$, $t \geq 0$ be integers such that $n = s + 2t \geq 2$.*

a) *A vector $(a_1,\ldots,a_s,b_1,\ldots,b_t,c_1,\ldots,c_t) \in \mathbb{Z}^n$ is called* admissible *if the following conditions are fulfilled:*

(A1) $a_i - a_j \equiv a_i - b_l \equiv b_k - b_l \equiv 0 \mod md$ *for all $i,j \in \{1,\ldots,s\}$ and $k,l \in \{1,\ldots,t\}$.*

(A2) $b_j^2 - c_j < 0$ *and* $b_j^2 - c_j \equiv 0 \mod d^2$ *for all $j \in \{1,\ldots,t\}$.*

(A3) *The polynomial*

$$P(x) = \prod_{i=1}^s (x-a_i)\prod_{j=1}^t (x^2 - 2b_jx + c_j) - d \in \mathbb{Z}[x]$$

is irreducible and has the symmetric group $\mathfrak{S}_n$ as its Galois group over $\mathbb{Q}$.

b) *Suppose that $s \geq 1$. We say that a vector $\vec{a} = (a_2,\ldots,a_s,b_1,\ldots,b_t,c_1,\ldots,c_t) \in \mathbb{Z}^{n-1}$* has an admissible completion *if for $X > 0$*

$$\#\{a_1 \in \mathbb{N} \mid a_1 < X\,,\ (a_1,\mathbf{a}) \in \mathbb{Z}^n \text{ is not admissible}\} \ll \sqrt{X}\ \log X\ .$$

Theorem 3.1 *Let the notations be as in the definition.*

i) *For $X > 0$, we have*

$$\#\{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{x} \text{ is admissible, } |\mathbf{x}| \leq X\} \gg X^n\ .$$

ii) *Suppose that $s \geq 1$. Then we have for $X > 0$*

$$\#\{\mathbf{x} \in \mathbb{Z}^{n-1} \mid \mathbf{x} \text{ has an admissible completion, } |\mathbf{x}| \leq X\} \gg X^{n-1}\ .$$

For the proof of Theorem 3.1 we need several preparations from Galois theory and from the theory of Hilbertian fields and thin subsets. We start with Galois theory.

Proposition 3.1 *Let k be a field, $n \in \mathbb{N}$, $n \geq 2$ and $\mathrm{char}(k) \nmid n(n-1)$. Let $T_1, \ldots, T_n$ be (algebraically independent) indeterminates over k, $d \in k^\times$ and*

$$P(x) = \prod_{i=1}^{n}(x - T_i) - d \in k(T_1, \ldots, T_n)[x]\,.$$

Then P has the symmetric group $\mathfrak{S}_n$ as its Galois group over $k(T_1, \ldots, T_n)$.

Proof. Let $s_i \in k[T_1, \ldots, T_n]$ be the i-th elementary symmetric polynomial in $T_1, \ldots, T_n$; then

$$P(x) = x^n + \sum_{i=1}^{n-1}(-1)^i s_i x^{n-i} + (-1)^n s_n - d\,.$$

Let M be a fixed algebraic closure of $k(T_1, \ldots, T_n)$, let K be the splitting field of P over $k(s_1, \ldots, s_n)$ inside M, and consider the field $L = k(T_1, \ldots, T_n) \cap K$. Then $K(T_1, \ldots, T_n)$ is the splitting field of P over $k(T_1, \ldots, T_n)$, and

$$\mathrm{Gal}\,(K(T_1, \ldots, T_n)/k(T_1, \ldots, T_n)) = \mathrm{Gal}\,(K/L)\,.$$

Therefore it is sufficient to prove that $\mathrm{Gal}\,(K/L) = \mathfrak{S}_n$.

Since the coefficients of $P(x)$ are algebraically independent over k and generate $k(s_1, \ldots, s_n)$, the Galois group of $K/k(s_1, \ldots, s_n)$ is the symmetric group $\mathfrak{S}_n$, and hence $\mathrm{Gal}\,(K/L) < \mathfrak{S}_n$. Since $k(T_1, \ldots, T_n)/k(s_1, \ldots, s_n)$ and $K/k(s_1, \ldots, s_n)$ are normal, the same is true for $L/k(s_1, \ldots, s_n)$, and therefore $\mathrm{Gal}\,(K/L) \lhd \mathfrak{S}_n$.

Suppose now that $\mathrm{Gal}\,(K/L) \neq \mathfrak{S}_n$. Then we have $\mathrm{Gal}\,(K/L) \subset \mathfrak{A}_n$, and therefore L contains the fixed field L_0 of $\mathfrak{A}_n$, which is given by $L_0 = k(s_1, \ldots, s_n)(\sqrt{D})$, where D is the discriminant of $P(x)$. Therefore the theorem will be proved if we can show that D is not a square in $k(T_1, \ldots T_n)$.

We consider the specialization $T_1 = \ldots = T_{n-1} = 0$ and $T_n = T$, where T is an indeterminate over k. Then $P(x)$ specializes to $P_0(x) = x^n - Tx^{n-1} - d$, and it is sufficient to prove that the discriminant of P_0 is not a square in $k(T)$. By [Sw], theorem 2, the discriminant of P_0 is given by

$$\Delta(T) = (-1)^{\frac{(n-1)(n-2)}{2}} d^{n-2}\left(n^n d + (n-1)^{n-1} T^n\right) = AT^n + B\,,$$

where A, $B \in k^\times$. Since $\Delta(T)$ is coprime with $\Delta'(T) = nAT^{n-1}$ in $k[T]$, it cannot be a square in $k[T]$ (and hence in $k(T)$).

We shall use the notion of thin subsets of $\mathbb{Q}^n$ as in [Se1], 9.1 and the notion of Hilbertian subsets of $\mathbb{Q}^n$ as in [La2], Ch.9. Instead of repeating the rather involved definitions, we collate the results which will become relevant in the sequel.

1) Subsets and finite unions of thin sets are thin. Zariski-closed proper subsets are thin. Complements of Hilbert sets are thin.

2) If $\Delta \subset \mathbb{Q}^n$ is thin, then

$$\#\{\mathbf{x} \in \mathbb{Z}^n \cap \Delta \mid \ |\mathbf{x}| \leq X\} \ll X^{n-\frac{1}{2}} \ \log X$$

holds as $X \to \infty$; see [Se2], Theorem 3.4.4.

3) Let $\mathbf{T} = (T_1, \ldots, T_n)$ be algebraically independent over $\mathbb{Q}$, and let $f_{\mathbf{T}}(x) \in \mathbb{Q}(\mathbf{T})[x]$ be a monic and irreducible polynomial with Galois group $G < \mathfrak{S}_n$ over $\mathbb{Q}(\mathbf{T})$. Then there is a thin subset $\Delta \subset \mathbb{Q}^n$ such that for all $\mathbf{a} \in \mathbb{Q}^n \setminus \Delta$:

i) $\mathbf{a}$ is not a pole of any of the coefficients of $f_{\mathbf{T}}(x)$.

ii) If $f_{\mathbf{a}}(x) \in \mathbb{Q}[x]$ arises from $f_{\mathbf{T}}(x)$ by the specialization $\mathbf{T} \mapsto \mathbf{a}$, then $f_{\mathbf{a}}(x)$ is irreducible and has G as its Galois group over $\mathbb{Q}$. See [Se2], Prop. 3.3.5.

Proposition 3.2 *Let $s \geq 0$, $t \geq 0$ be integers such that $n = s + 2t \geq 2$, and $d \in \mathbb{Q}^\times$. Then there exists a thin subset $\Delta \subset \mathbb{Q}^n$ such that for all*

$$(a_1, \ldots, a_s, b_1, \ldots, b_t, c_1, \ldots, c_t) \in \mathbb{Q}^n \setminus \Delta\,,$$

the polynomial

$$P(x) = \prod_{i=1}^{s}(x - a_i) \prod_{j=1}^{t}(x^2 - 2b_j x + c_j) - d \in \mathbb{Q}[x]$$

is irreducible and has the symmetric group $\mathfrak{S}_n$ as its Galois group over $\mathbb{Q}$.

Proof. Let $\mathbf{A} = (A_1, \ldots, A_s)$, $\mathbf{B} = (B_1, \ldots, B_t)$, $\mathbf{C} = (C_1, \ldots, C_t)$ be algebraically independent over $\mathbb{Q}$, and set $K = \mathbb{Q}(\mathbf{A}, \mathbf{B}, \mathbf{C})$. By **3)**, it is sufficient to prove that the polynomial

$$P(x) = \prod_{i=1}^{s}(x - A_i) \prod_{j=1}^{t}(x^2 - 2B_j x + C_j) - d \in K[x]$$

is irreducible and has the symmetric group $\mathfrak{S}_n$ as its Galois group over K. Fix an algebraic closure $\overline{K}$ of K, and let $Y_j, Y_j' \in \overline{K}$ be such that

$$x^2 - 2B_j x + C_j = (x - Y_j)(x - Y_j')\,.$$

If $\mathbf{Y} = (Y_1, \ldots, Y_t)$, $\mathbf{Y}' = (Y_1', \ldots, Y_t')$ then $\mathbf{A}, \mathbf{Y}, \mathbf{Y}'$ are algebraically independent over $\mathbb{Q}$, and $\Big[\mathbb{Q}(\mathbf{A}, \mathbf{Y}, \mathbf{Y}') : \mathbb{Q}(\mathbf{A}, \mathbf{B}, \mathbf{C})\Big] = 2^t$. By Proposition 3.1, $P(x)$ is irreducible and has $\mathfrak{S}_n$ as its Galois group over $\mathbb{Q}(\mathbf{A}, \mathbf{Y}, \mathbf{Y}')$. Hence the same is true over $\mathbb{Q}(\mathbf{A}, \mathbf{B}, \mathbf{C})$. □

Proof of Theorem 3.1. Let Ω be the set of all $\mathbf{x} \in \mathbb{Z}^n$ satisfying **(A1)** and **(A2)**. Then Ω contains a set of the form $C \cap (\mathbf{u} + \Gamma)$, where $\mathbf{u} \in \mathbb{Z}^n$, $\Gamma < \mathbb{Z}^n$ is a complete lattice and C is an open cone in $\mathbb{R}^n$. Therefore we have for $X > 0$

$$\#\{\mathbf{x} \in \Omega \mid \ |\mathbf{x}| \leq X\} \gg X^n\,.$$

If $\Sigma \subset \mathbb{Z}^n$ is the set of all $\mathbf{a} \in \mathbb{Z}^n$ for which **(A3)** is not satisfied, then Σ is contained in a thin subset of $\mathbb{Q}^n$ by Proposition 3.2, and consequently

$$\#\{\mathbf{x} \in \Sigma \mid \ |\mathbf{x}| \leq X\} \ll X^{n-\frac{1}{2}} \ \log X$$

by **2)**. Thus **i)** follows.

The proof of **ii)** runs along the same lines, using the following Lemma on thin sets. □

Lemma 3.1 *For $\mathbf{b} \in \mathbb{Q}^n$, define $j_{\mathbf{b}} : \mathbb{Q}^m \to \mathbb{Q}^{m+n} = \mathbb{Q}^m \times \mathbb{Q}^n$ by $j_{\mathbf{b}}(\mathbf{a}) = (\mathbf{a}, \mathbf{b})$. Let $\Delta \subset \mathbb{Q}^{m+n}$ be a thin subset. Then there exists a thin subset $\Delta_2 \subset \mathbb{Q}^n$ such that for all $\mathbf{b} \in \mathbb{Q}^n \setminus \Delta_2$ the set $j_{\mathbf{b}}^{-1}(\Delta) \subset \mathbb{Q}^m$ is thin.*

Proof. Use the polynomial description of thin sets as given in [Se1], 9.1. Observe that the rational function field $\mathbb{Q}(X_1, \ldots, X_n)$ is Hilbertian and that complements of Hilbertian subsets of $\mathbb{Q}^n$ are thin. □

4 Connections between the Lang-Waldschmidt conjecture and a conjecture of E. Thomas

We now turn to apply the results of sections 2 and 3 to establish a connection between the conjectures of Lang-Waldschmidt [La1] and E. Thomas [Th]. To formulate the result we need a definition.

Let $\gamma \neq 0$ be an algebraic number, $l_m x^m + \ldots + l_0 \in \mathbb{Z}[x]$ its minimal polynomial and $\gamma_1, \ldots, \gamma_m$ its conjugates. Then the *absolute logarithmic height* of γ is defined by

$$h(\gamma) = \frac{1}{m} \log \left| l_m \prod_{i=1}^{m} \max\{1, |\gamma_i|\} \right| \ .$$

Conjecture 4.1 (Lang-Waldschmidt [La1]) *Let $\mathbb{K}$ be an algebraic number field of degree m, $\beta_1, \ldots, \beta_k \in \mathbb{K}$ and $b_1, \ldots, b_k \in \mathbb{Z}$. Let $B_1, \ldots, B_k, B$ be real numbers such that*

$$\log B_i \geq h(\beta_i) \ , \ i = 1, \ldots, k, \quad \text{and} \quad B \geq \max\{|b_1|, \ldots, |b_k|, e\} \ .$$

Then there exists a constant $c(k, m) > 0$ such that

$$|b_1 \log \beta_1 + \ldots + b_k \log \beta_k| > \exp\{-c(k, m)(\log B_1 + \ldots + \log B_k) \log B\},$$

provided that $b_1 \log \beta_1 + \ldots + b_k \log \beta_k \neq 0$.

We remark that this conjecture is stated in [La1] explicitly only for $\beta_1, \ldots, \beta_k \in \mathbb{Z}$, but in a sharper form. It is a possible refinement of A. Baker's theory of linear forms in logarithms of algebraic numbers, where presently the best lower bounds are depending on $\log B_1 \cdots \log B_k$ (see for example [BW]), instead of the conjectured $\log B_1 + \ldots + \log B_k$.

We shall prove that a special case of the conjecture of E. Thomas [Th] is a consequence of the Lang-Waldschmidt conjecture. More precisely, we prove the following theorem.

Theorem 4.1 *Let $n \geq 3$, $a_1 = 0, a_2, \ldots, a_{n-1}$ be distinct integers and $a_n = a$ an integral parameter. Let $\alpha = \alpha(a)$ be a zero of $P(x) = \prod_{i=1}^{n}(x - a_i) - d$ with $d = \pm 1$ and suppose that the index I of $\langle \alpha - a_1, \ldots, \alpha - a_{n-1} \rangle$ in $U_{\mathcal{O}}$, the group of units of $\mathcal{O}$, is bounded by a constant $J = J(a_1, \ldots, a_{n-1}, n)$ for every a from some subset $\Omega \subset \mathbb{Z}$. Assume further that the Lang-Waldschmidt conjecture is true. Then for all but finitely many values $a \in \Omega$ the diophantine equation*

$$\prod_{i=1}^{n}(x - a_i y) - dy^n = \pm 1 \tag{6}$$

only has trivial solutions, except when $n = 3$ and $|a_2| = 1$, or when $n = 4$ and $(a_2, a_3) \in \{(1, -1), (\pm 1, \pm 2)\}$, in which cases (6) has exactly one more general solution, as described in the Introduction.

Remark: The integers $d, a_1, \ldots, a_n = a$ of Theorem 4.1 satisfy assumptions **A.** and **B1.** of section 2 with $s = n$; thus the results of section 2 apply. By Theorem 2.1, the index $(U_{\mathcal{O}} : U_\eta)$ is bounded by a constant J depending only on n, provided that $\mathbb{K} = \mathbb{Q}(\alpha)$ is primitive over $\mathbb{Q}$. Therefore, if n is a prime we can choose $\Omega = \mathbb{Z}$ in Theorem 4.1. For composite n the results of section 3 show that for most $a_1, \ldots, a_{n-1} \in \mathbb{Z}$ we can choose Ω to be a dense subset of $\mathbb{Z}$ (e.g. the set of all a for which Gal $(\mathbb{K}/\mathbb{Q}) = \mathfrak{S}_n$).

In the exceptional cases Theorem 4.1 is unconditionally true by the results of Mignotte and Tzanakis [MT] as well as by Pethő [Pe] and Mignotte, Pethő and Roth [MPR]. Motivated by these results and by the proof of Theorem 4.1 (especially by Lemmata 4.3 and 4.4) we formulate the following conjecture.

Conjecture 4.2 *Let $n \geq 3$, $a_1 = 0, a_2, \ldots, a_{n-1}$ be distinct integers and $a_n = a$ an integral parameter. If a is large enough then the diophantine equation (6) has only the trivial solutions $\pm(x, y) = (1, 0), (a_i, 1)$, $i = 1, \ldots, n$ except when $n = 3$ and $|a_2| = 1$, and when $n = 4$ and $(a_2, a_3) = (1, -1), (\pm 1, \pm 2)$, in which cases it has exactly one more parametrized solution.*

After these remarks we start to prepare the proof of Theorem 4.1. We may assume without loss of generality that $0 < |a_2| \leq \ldots \leq |a_{n-1}| < a$ and put $A = \log(a)$. Assume further that the zeros α_i of $P(x)$ are ordered according to Lemma 2.1, thus

$$|\alpha_i - a_i| < \delta = \frac{2}{a} \leq \frac{1}{3} \quad \text{for } 1 \leq i \leq n \text{ and } 6 \leq a \ .$$

For $y = 0$ equation (6) only has trivial solutions with $|x| = 1$.

Thus let us assume that $(x, y) \in \mathbb{Z}^2$ with $y \neq 0$ is a solution of (6). Then

$$\left| y^n P\left(\frac{x}{y}\right) \right| = \left| \prod_{i=1}^{n}(x - a_i y) - dy^n \right| = \left| \prod_{i=1}^{n}(x - \alpha_i y) \right| = 1.$$

Define $j \in \{1, \ldots, n\}$ to be that index such that

$$|x - \alpha_j y| = \min_{1 \leq i \leq n} |x - \alpha_i y|. \tag{7}$$

Obviously, $|x - \alpha_j y| < 1$. Let us put $Y = \log |y|$.

Lemma 4.1 *Let the notations be as above and j be given by (7). Then*

$$\log|x-\alpha_i y| = \begin{cases} -(n-1)Y - A + O(1) & \text{if } i=j<n, \\ -(n-1)(Y+A)+O(1) & \text{if } i=j=n, \\ Y + O(1) & \text{if } i\neq j, i, j<n, \\ Y + A + O(1) & \text{if } i\neq j, i \text{ or } j=n. \end{cases}$$

Here and in the sequel the O-constants depend only on n and $a_2,\dots,a_{n-1}$.

Proof. For $i\neq j$, we obtain

$$|x-\alpha_i y| \geq \frac{|x-\alpha_i y|+|x-\alpha_j y|}{2} \geq \frac{|y||\alpha_i-\alpha_j|}{2} > |y|\frac{|a_i-a_j|}{6},$$

and so

$$|x-\alpha_i y| > \begin{cases} \dfrac{|y|}{6} & \text{if } \ i,j\neq n, \\ \dfrac{|ya|}{12} & \text{if } \ i \text{ or } j=n, \text{ and } a\geq 2|a_{n-1}|\ . \end{cases} \tag{8}$$

On the other hand, (6) and (8) imply

$$|x-\alpha_j y| = \frac{1}{\prod\limits_{\substack{i=1\\ i\neq j}}^{n}|x-\alpha_i y|} < \begin{cases} \dfrac{6^n}{a|y|^{n-1}} & \text{if } \ j\neq n, \\ \dfrac{12^{n-1}}{|ay|^{n-1}} & \text{if } \ j=n. \end{cases} \tag{9}$$

Since $|x-\alpha_j y|<1$, we obtain for $i\neq j$ the upper bound

$$|x-\alpha_i y| \leq |x-\alpha_j y| + |y||\alpha_i-\alpha_j| < |y|(|a_i-a_j|+2), \tag{10}$$

which easily yields the stated asymptotic relations for the case $i\neq j$.

Finally, the lower bound in the case $i=j$ follows from (6) and (10) immediately. □

As in section 2, we put $\eta_{ij}=\alpha_i-a_j$ for $1\leq i,j\leq n$. Then η_{ij} are units in $\mathbb{Q}(\alpha_i)$. Let us agree to choose $\alpha=\alpha_1$ and let I denote the index of $U_\eta=\langle\eta_{11},\dots,\eta_{1n}\rangle$ in the group of units $U_{\mathcal{O}}$ of the order $\mathcal{O}=\mathbb{Z}[\alpha]$. By Lemma 2.2 the regulator R_η of U_η is non-zero if a is large enough, hence I is a positive integer, and any subset of size $n-1$ of the set $\{\eta_{11},\dots,\eta_{1n}\}$ generates U_η, possibly up to $\{\pm1\}$.

We have $x-\alpha y\in U_{\mathcal{O}}$, hence there exist integers $u_i,\ i\in\{1,\dots,n\}\backslash\{j\}$ such that

$$(x-\alpha y)^I = \pm\prod_{\substack{i=1\\ i\neq j}}^{n}\eta_{1i}^{u_i}\ . \tag{11}$$

Lemma 4.2 *Let the index j be defined by (7) and let $u_i,\ i\in\{1,\dots,n\}\backslash\{j\}$ be the integers given by (11). Then*

$$\frac{u_i}{I} = \begin{cases} -\frac{nY}{A}-1 & +O\left(\frac{Y+A}{A^2}\right) & \text{if } \ j\neq n,\ 1\leq i<n, \\ -\frac{(n-1)Y}{A}-1 & +O\left(\frac{Y+A}{A^2}\right) & \text{if } \ j\neq n,\ i=n, \\ -\frac{Y}{A}-1 & +O\left(\frac{Y+A}{A^2}\right) & \text{if } \ j=n,\ 1\leq i<n\,. \end{cases}$$

Proof. ¿From Lemma 2.1 we immediately obtain

$$\log|\eta_{ki}| = \begin{cases} O(1) & \text{if } \ i \neq k \text{ and } i < n \text{ and } k < n, \\ -A + O(1) & \text{if } \ i = k < n, \\ A + O(1) & \text{if } \ i < k = n \text{ or } k < i = n, \\ -(n-1)A + O(1) & \text{if } \ i = k = n. \end{cases} \tag{12}$$

Taking absolute values and logarithms of all equations conjugated to (11), we obtain n linear equations

$$\log|x - \alpha_k y| = \sum_{\substack{i=1 \\ i \neq j}}^{n} \frac{u_i}{I} \log|\eta_{ki}| \ , \quad 1 \leq k \leq n \ ,$$

for the $n-1$ rational numbers $\dfrac{u_i}{I}, i \in \{1, \ldots, n\} \backslash \{j\}$. Any $n-1$ of these n equations have determinant $\pm R_\eta$, so we may omit any one of the equations. We omit the equation with $k = j$ and obtain a regular system of linear equations

$$\log|x - \alpha_k y| = \sum_{\substack{i=1 \\ i \neq j}}^{n} \frac{u_i}{I} \log|\eta_{ki}| \ , \quad k \in \{1, \ldots, n\} \setminus \{j\}, \tag{13}$$

with determinant

$$R = \det\left(\log|\eta_{ki}|\right)_{\substack{1 \leq i,k \leq n \\ i,k \neq j}} = (-A)^{n-1} + O(A^{n-2}) \ , \tag{14}$$

where here and in the following we continuously use (12).

To simplify notations, for $1 \leq \ell \leq n-2$ let $\vec{v}_\ell$ denote any vector of $\mathbb{R}^{n-1}$ of the shape

$$\vec{v}_\ell = (O(1), \ldots, O(1), -A + O(1), O(1), \ldots, O(1), A + O(1)) \ ,$$

where $-A + O(1)$ stands at the ℓ-th position. Similarly we put

$$\begin{aligned} \vec{v}_0 &= (O(1), \ldots, O(1), -A + O(1)), \\ \vec{v}_{n-1} &= (A + O(1), \ldots, A + O(1), -(n-1)A + O(1)), \\ \vec{w} &= (Y + O(1), \ldots, Y + O(1), Y + A + O(1)), \\ \vec{z} &= (Y + A + O(1), \ldots, Y + A + O(1)). \end{aligned}$$

Now we distinguish the two cases $j \neq n$ and $j = n$.

Consider first $j \neq n$. By Lemma 4.1, the left hand side of the system (13) equals

$$\left(\log|x - \alpha_k y|\right)_{\substack{1 \leq k \leq n \\ k \neq j}} = \vec{w} \ ,$$

thus solving (13) by Cramer's rule we get

$$\Delta_\ell := \det(\vec{v}_1, \ldots, \vec{v}_{\ell-1}, \vec{y}, \vec{v}_{\ell+1}, \ldots, \vec{v}_{n-1}) = \begin{cases} \frac{u_\ell}{I} R & \text{if } \ 1 \leq \ell < j \ , \\ \frac{u_{\ell+1}}{I} R & \text{if } \ j \leq \ell \leq n-1 \ . \end{cases}$$

To compute Δ_ℓ we use the relation $\vec{v}_{n-1}+\sum_{\substack{k=1\\k\neq\ell}}^{n-2}\vec{v}_k=-\vec{v}_\ell+\vec{v}_0$. Thus we get for $1\le\ell\le n-2$

$$\begin{aligned}\Delta_\ell &= \det(\vec{v}_1,\dots,\vec{v}_{\ell-1},\vec{w},\vec{v}_{\ell+1},\dots,\vec{v}_{n-1}) = -\det(\vec{v}_1,\dots,\vec{v}_{\ell-1},\vec{v}_{n-1},\vec{v}_{\ell+1},\dots,\vec{v}_{n-2},\vec{w})\\ &= -\det(\vec{v}_1,\dots,\vec{v}_{\ell-1},\vec{v}_{n-1}+\sum_{\substack{h=1\\h\neq\ell}}^{n-2}\vec{v}_h,\vec{v}_{\ell+1},\dots,\vec{v}_{n-2},\vec{w})\\ &= \det(\vec{v}_1,\dots,\vec{v}_{n-2},\vec{w})-\det(\vec{v}_1,\dots,\vec{v}_{\ell-1},\vec{v}_0,\vec{v}_{\ell+1},\dots,\vec{v}_{n-2},\vec{w})=\Delta_{n-1}-\Delta'_\ell.\end{aligned}$$

Adding all rows but the last to the last row of Δ_{n-1}, we obtain

$$\Delta_{n-1}=\begin{vmatrix} -A+O(1) & O(1) & \dots & O(1) & Y+O(1)\\ \vdots & \vdots & & \vdots & \vdots\\ O(1) & O(1) & \dots & -A+O(1) & Y+O(1)\\ O(1) & O(1) & \dots & O(1) & (n-1)Y+A+O(1)\end{vmatrix}$$

and $\Delta_{n-1}=(-A)^{n-2}((n-1)Y+A)+O(A^{n-3}(Y+A))$. Therefore,

$$\frac{u_n}{I}=\frac{\Delta_{n-1}}{R}=-\frac{(n-1)Y}{A}-1+O\left(\frac{Y+A}{A^2}\right).$$

Computing Δ'_ℓ, we obtain

$$\begin{aligned}\Delta'_\ell &= \det(\vec{v}_1,\dots,\vec{v}_{\ell-1},\vec{v}_0,\vec{v}_{\ell+1},\dots,\vec{v}_{n-2},\vec{w})\\ &= \det(\vec{v}_1+\vec{v}_0,\vec{v}_2+\vec{v}_0,\dots,\vec{v}_{\ell-1}+\vec{v}_0,\vec{v}_0,\vec{v}_{\ell+1}+\vec{v}_0,\dots,\vec{v}_{n-2}+\vec{v}_0,\vec{w}).\end{aligned}$$

Interchanging now the last and the ℓ-th row we get

$$\Delta'_\ell=-\begin{vmatrix} -A+O(1) & O(1) & \dots & O(1) & Y+O(1)\\ O(1) & -A+O(1) & \dots & O(1) & Y+O(1)\\ \vdots & \vdots & & \vdots & \vdots\\ O(1) & O(1) & \dots & -A+O(1) & Y+O(1)\\ O(1) & O(1) & \dots & O(1) & Y+O(1)\end{vmatrix},$$

where the ℓ-th coordinate of the last column is $Y+A+O(1)$, hence

$$\Delta'_\ell=-(-A)^{n-2}Y+O(A^{n-3}(Y+A)).$$

Thus

$$\begin{aligned}\Delta_\ell &= \Delta_{n-1}-\Delta'_\ell=(-A)^{n-2}((n-1)Y+A)+(-A)^{n-2}Y+O(A^{n-3}(Y+A))\\ &= (-A)^{n-2}(nY+A)+O(A^{n-3}(Y+A))\ ,\end{aligned}$$

and together with (14) this yields

$$\frac{u_\ell}{I}=-\frac{nY}{A}-1+O\left(\frac{Y+A}{A^2}\right)\quad\text{for }\ 1\le\ell\le n-1,\ \ell\neq j\ .$$

We now turn to the case $j = n$. For the system (13) we now have

$$(\log|\eta_{ki}|)_{k=1,\dots,n-1} = \begin{cases} \vec{v}_i + \vec{v}_0 & \text{for} \quad 1 \le i \le n-2 \ , \\ \vec{v}_0 & \text{for} \quad i = n-1 \ , \end{cases}$$

and as left hand side

$$(\log|x - \alpha_k y|)_{k=1,\dots,n-1} = \vec{z}.$$

Applying again Cramer's rule to (13) we obtain

$$\begin{aligned} R\frac{u_i}{I} &= \det(\vec{v}_1 + \vec{v}_0, \dots, \vec{v}_{i-1} + \vec{v}_0, \vec{z}, \vec{v}_{i+1} + \vec{v}_0, \dots, \vec{v}_{n-2} + \vec{v}_0, \vec{v}_0) \\ &= (Y + A)(-A)^{n-2} + O((Y + A)A^{n-3}). \end{aligned}$$

Using (14), we get for $i = 1, \dots, n-1$

$$\frac{u_i}{I} = -\frac{Y}{A} - 1 + O\left(\frac{Y + A}{A^2}\right) \ .$$

□

The next lemma shows that equation (6) can have only finitely many solutions which are of special kind.

Lemma 4.3 *Let $I, j, u, v \in \mathbb{Z}$ be integers with $0 < I$ and $1 \le j < n$. If $n \in \{3, 4\}$ assume furthermore that $nv - (n-1)u + I = 0$. If*

$$(u, v) \neq \begin{cases} (0,0), (-1,-1)I, (-4,-3)I & \text{if } n = 3 \text{ and } |a_2| = 1, \\ (0,0), (-1,-1)I, (-5,-4)I & \text{if } n = 4 \text{ and } (a_2, a_3) = (1,-1), (\pm 1, \pm 2), \\ (0,0), (-I,-I) & \text{otherwise,} \end{cases}$$

then there exist only finitely many $a \in \mathbb{Z}$ for which

$$\left(\prod_{\substack{i=1 \\ i \neq j}}^{n-1} \eta_{1i}\right)^u \eta_{1n}^v = (x - \alpha y)^I \tag{15}$$

has a solution $(x, y) = (x(a), y(a)) \in \mathbb{Z}^2$.

Proof. Let $(x, y) \in \mathbb{Z}$ be a solution of (15) and let $1 \le h, p, q \le n$ be pairwise distinct integers. Then

$$(\alpha_h - \alpha_p)(x - \alpha_q y) + (\alpha_p - \alpha_q)(x - \alpha_h y) = (\alpha_h - \alpha_q)(x - \alpha_p y) \tag{16}$$

holds. Using $\prod_{i=1}^{n} \eta_{ki} = d$ we obtain

$$x - \alpha_k y = \eta_{kn}^w \left(d\eta_{kj}\right)^U \ , \quad 1 \le k \le n, \tag{17}$$

with $U = -\dfrac{u}{I}$ and $w = \dfrac{v - u}{I}$.

Assume first that $n \geq 5$. Choose $p, q \in \{1, \ldots, n\} \backslash \{j, n\}$ distinct, and such that $|a_j - a_p| \neq |a_j - a_q|$, which is always possible. Put $h = j$ and insert (17) into (16). Then

$$(\alpha_j - \alpha_p)\eta^w_{qn}(d\eta_{qj})^U + (\alpha_p - \alpha_q)\eta^w_{jn}(d\eta_{jj})^U = (\alpha_j - \alpha_q)\eta^w_{pn}(d\eta_{pj})^U.$$

Dividing this equation by $\eta^w_{jn}(\alpha_p - \alpha_q)d^U$ we derive

$$\eta^U_{jj} = \frac{\alpha_j - \alpha_q}{\alpha_p - \alpha_q}\left(\frac{\eta_{pn}}{\eta_{jn}}\right)^w \eta^U_{pj} - \frac{\alpha_j - \alpha_p}{\alpha_p - \alpha_q}\left(\frac{\eta_{qn}}{\eta_{jn}}\right)^w \eta^U_{qj} \ .$$

Assume that (15) has solutions for infinitely many $a \in \mathbb{Z}$. Then for some $j \in \{1, \ldots, n\}$, the algebraic function

$$\eta^U_{jj} - \frac{\alpha_j - \alpha_q}{\alpha_p - \alpha_q}\left(\frac{\eta_{pn}}{\eta_{jn}}\right)^w \eta^U_{pj} + \frac{\alpha_j - \alpha_p}{\alpha_p - \alpha_q}\left(\frac{\eta_{qn}}{\eta_{jn}}\right)^w \eta^U_{qj}$$

has infinitely many zeros, so it is identically zero. By Lemma 2.1 we have for any $i, k \in \{1, \ldots, n-1\}$ with $i \neq k$

$$\lim_{a\to\infty} \frac{\eta_{in}}{\eta_{kn}} = \lim_{a\to\infty} \frac{\alpha_i - a}{\alpha_k - a} = 1 \quad \text{and} \quad \lim_{a\to\infty}(\alpha_i - \alpha_k) = a_i - a_k = \lim_{a\to\infty} \eta_{ik} \ .$$

This yields

$$\lim_{a\to\infty} \eta^U_{jj} = \frac{(a_j - a_q)(a_p - a_j)}{a_p - a_q}\left((a_p - a_j)^{U-1} - (a_q - a_j)^{U-1}\right).$$

The right hand side is a constant, and since $\lim\limits_{a\to\infty} \eta_{jj} = 0$, U must be positive and the constant must be zero. As a_j, a_p and a_q are pairwise different, this means

$$(a_p - a_j)^{U-1} = (a_q - a_j)^{U-1}.$$

Since $|a_p - a_j| \neq |a_q - a_j|$, this implies $U = 1$, i.e. $u = -I$.

Consider again (16), but now put $h = j, p = n$ and $q \in \{1, \ldots, n\} \backslash \{j, n\}$, so

$$(\alpha_j - \alpha_n)\eta^w_{qn}\,\eta_{qj} + (\alpha_n - \alpha_q)\eta^w_{jn}\,\eta_{jj} = (\alpha_j - \alpha_q)\eta^w_{nn}\,\eta_{nj}.$$

Dividing by $\eta_{nj}\eta^w_{jn}$ we get

$$\frac{\alpha_j - \alpha_n}{\eta_{nj}}\left(\frac{\eta_{qn}}{\eta_{jn}}\right)^w \eta_{qj} + \frac{\alpha_n - \alpha_q}{\eta_{nj}}\eta_{jj} = (\alpha_j - \alpha_q)\left(\frac{\eta_{nn}}{\eta_{jn}}\right)^w.$$

As above, one can see that for a tending to infinity the left hand side tends to $a_j - a_q \neq 0$. Since $\lim\limits_{a\to\infty}\left|\frac{\eta_{nn}}{\eta_{jn}}\right| = 0$, this implies $w = 0$. Thus we proved the lemma for $n \geq 5$ and also for $n = 4$, provided we can find suitable a_p, a_q with $|a_j - a_p| \neq |a_j - a_q|$.

For $n \in \{3, 4\}$ we choose $h = j$ and $p = n$. If $n = 3$, put q the remaining element of

the set $\{1,2,3\}$, while in the case $n=4$ we choose q either such that $|a_j-a_q|>1$ or, if this is not possible, one of the elements of the set $\{1,2,3\}\backslash\{j\}$. Equation (16) implies

$$(\alpha_j-\alpha_n)\eta_{qn}^w\,\eta_{qj}^U+(\alpha_n-\alpha_q)\eta_{jn}^w\,\eta_{jj}^U=(\alpha_j-\alpha_q)\eta_{nn}^w\,\eta_{nj}^U,$$

which can be reformulated as

$$\eta_{jj}^U=\frac{\alpha_n-\alpha_j}{\alpha_n-\alpha_q}\left(\frac{\eta_{qn}}{\eta_{jn}}\right)^w\eta_{qj}^U+\frac{\alpha_j-\alpha_q}{\alpha_n-\alpha_q}\eta_{nj}^U\left(\frac{\eta_{nn}}{\eta_{jn}}\right)^w. \tag{18}$$

If a tends to inifinity then the first term of the right hand side tends to $(a_q-a_j)^U\neq 0$. The second term of the right hand side can be transformed to

$$\frac{\alpha_j-\alpha_q}{\alpha_n-\alpha_q}\,\eta_{nj}^U\left(\frac{\eta_{nn}}{\eta_{jn}}\right)^w=(\alpha_j-\alpha_q)\,\frac{\eta_{nj}}{\alpha_n-\alpha_q}\left(\frac{\eta_{nj}}{\eta_{jn}}\right)^{U-1}\frac{\eta_{nn}^w}{\eta_{jn}^{w-U+1}}\,.$$

Using the definition of w and U and the assumption $nv-(n-1)u+I=0$ we find $w-U+1=-(n-1)w$. Thus

$$\frac{\eta_{nn}^w}{\eta_{jn}^{w-U+1}}=(\eta_{nn}\,\eta_{jn}^{n-1})^w=\left(\frac{d\eta_{jn}^{n-1}}{\prod_{k=1}^{n-1}\eta_{kn}}\right)^w$$

because $\prod_{k=1}^n\eta_{kn}=d$. Summing up, the second term of the right hand side of (18) is

$$(\alpha_j-\alpha_q)\,\frac{\alpha_n-\alpha_j}{\alpha_n-\alpha_q}\left(\frac{\eta_{nj}}{\eta_{jn}}\right)^{U-1}\left(\frac{d\eta_{jn}^{n-1}}{\prod_{k=1}^{n-1}\eta_{kn}}\right)^w,$$

which tends to a_j-a_q if a tends to infinity. Hence $\lim_{a\to\infty}\eta_{jj}^U=(a_q-a_j)^U+(a_j-a_q)d^w$. As $\lim_{a\to\infty}\eta_{jj}=0$, U must be positive, and $(a_q-a_j)\left((a_q-a_j)^{U-1}-d^w\right)=0$, which implies $U=1$, i.e. $u=v=-I$ provided $|a_q-a_j|>1$. Thus the lemma is proved also in this case.

If $n=3$ then $|a_q-a_j|=1$ is only possible if $|a_2|=1$, while if $n=4$ then $|a_q-a_j|=1$ for $q\in\{1,2,3\}\backslash\{j\}$ is only possible if $(a_2,a_3)=(\pm1,\mp1),(\pm1,\pm2)$. In these cases the assertion of the lemma follows from the theorems of [MT] as well as from [Pe], [MPR].

□

Lemma 4.4 *Let I be a positive integer and $u\in\mathbb{Z}$. If $u\neq 0,I$ then there exist only finitely many $a\in\mathbb{Z}$ for which*

$$\eta_{1n}^u=(\alpha_1-a)^u=(x-\alpha y)^I \tag{19}$$

has a solution $(x,y)=(x(a),y(a))\in\mathbb{Z}^2$.

Proof. Assume that $u\neq 0$ and (19) holds for infinitely many a.
If $u<0$ then $\lim_{a\to\infty}|\alpha_i-a|^{u/I}=0$ for $1\leq i<n$, which together with (19) contradicts

$$\frac{1}{3}<|(\alpha_2-\alpha_1)y|\leq|x-\alpha_1y|+|x-\alpha_2y|.$$

Hence we have $u > 0$. Now we apply (16) with $p = n$ and $1 \le h < q < n$ to those a's for which (19) holds. Thus we obtain

$$(\alpha_h - \alpha_n)\eta_{qn}^{u/I} + (\alpha_n - \alpha_q)\eta_{hn}^{u/I} = (\alpha_h - \alpha_q)\eta_{nn}^{u/I}.$$

Dividing by $(\alpha_n - \alpha_h)\eta_{qn}^{u/I}$ and using (12) we get

$$\frac{\alpha_n - \alpha_q}{\alpha_n - \alpha_h}\left(\frac{\eta_{hn}}{\eta_{qn}}\right)^{\frac{u}{I}} - 1 = \frac{\alpha_h - \alpha_q}{\alpha_n - \alpha_h}\left(\frac{\eta_{nn}}{\eta_{qn}}\right)^{\frac{u}{I}} = O\left(\frac{1}{a^{1+\frac{nu}{I}}}\right).$$

If a is large enough, the right hand side is less then $1/2$. Using that $|\log(x+1)| < 2|x|$ for $|x| < 1/2$, we conclude

$$\left|\log\frac{\alpha_n - \alpha_q}{\alpha_n - \alpha_h} + \frac{u}{I}\log\frac{a_n - \alpha_h}{a_n - \alpha_q}\right| < O\left(a^{-(1+\frac{nu}{I})}\right). \tag{20}$$

On the other hand,

$$\frac{\alpha_n - \alpha_q}{\alpha_n - \alpha_h} = 1 + \frac{\alpha_h - \alpha_q}{\alpha_n - \alpha_h} = 1 + \frac{\alpha_h - \alpha_q}{a_n - a_h} + O\left(\frac{1}{a^3}\right)$$

gives us

$$\log\frac{\alpha_n - \alpha_q}{\alpha_n - \alpha_h} + \frac{u}{I}\log\frac{a_n - \alpha_h}{a_n - \alpha_q} = \left(\frac{u}{I} - 1\right)\frac{a_h - a_q}{a} + O\left(\frac{1}{a^2}\right).$$

Thus (20) is only possible if $u = I$, and the lemma is proved.

□

Proof of the Theorem 4.1 In the sequel $c_1, c_2, \ldots$ will denote constants depending only on $a_2, \ldots, a_{n-1}$ and n. Let $(a, x(a), y(a)) = (a, x, y) \in \mathbb{Z}^3$ be a solution of (6) with $a > |a_{n-1}|$ and $|y| > 1$ (the solutions of (6) with $|y| = 1$ are only the trivial ones). Let the index j be defined by (7) and let the integers $u_i,\ i \in \{1, \ldots, n\}\backslash\{j\}$, be given by (11).

Put $p = j$ and choose $h, q \in \{1, \ldots, n\}\backslash\{j\}$ to be distinct numbers. Applying (16) with these indices we get

$$\frac{\alpha_h - \alpha_j}{\alpha_q - \alpha_j}\ \prod_{\substack{i=1\\ i\neq j}}^{n}\left(\frac{\eta_{qi}}{\eta_{hi}}\right)^{\frac{u_i}{I}} - 1 = \frac{\alpha_h - \alpha_q}{\alpha_q - \alpha_j}\ \frac{x - \alpha_j y}{x - \alpha_h y}\ .$$

The right hand side is bounded by $\exp\{-nY - A + c_1\}$ by Lemma 4.1, which is less then $1/4$ if a is large enough.
Thus we have

$$0 < |\Lambda| := \left| I\ \log\left|\frac{\alpha_h - \alpha_j}{\alpha_q - \alpha_j}\right| + \sum_{\substack{i=1\\ i\neq j}}^{n} u_i \log\left|\frac{\eta_{qi}}{\eta_{hi}}\right| \right| < e^{-nY - A + c_2}\ .$$

Put $U = \max\{J, e, |u_i|\ \mid 1 \le i \le n,\ i \neq j\}$, where J is the upper bound for I as assumed in the statement of the Theorem. Moreover, by Lemma 4.2

$$\frac{U}{J} \le \frac{U}{I} < \left(\frac{nY}{A} + 1 + c_3\frac{Y + A}{A^2}\right) < \frac{(n+1)Y}{A}\ ,$$

if a is large enough. Thus $Y > \dfrac{A}{(n+1)J}\,U$. Hence we get the upper bound

$$\log|\Lambda| < -\frac{nA}{(n+1)J}U - A + c_2\ .$$

To apply the Lang-Waldschmidt conjecture we have to estimate the absolute logarithmic height of the algebraic numbers appearing in Λ. We start with the units. Using (12) we obtain

$$\begin{aligned} h(\eta_{qi}) &= h(\eta_{qi}^{-1}) = \frac{1}{n}\log\prod_{k=1}^{n}\max\{1,|\eta_{ki}^{-1}|\} \\ &\le -\frac{1}{n}\Big(\log|\eta_{ii}| + \log(1-\frac{1}{a})\Big) < \frac{n-1}{n}A + O(1) < A \end{aligned}$$

for $q,i \in \{1,\dots,n\}$. Hence $h\Big(\dfrac{\eta_{qi}}{\eta_{hi}}\Big) < 2A$ for any $1 \le i \le n$.
Further

$$h(\alpha_h - \alpha_j) \le \binom{n}{2}^{-1}\log\prod_{1\le k<\ell\le n}\max\{|\alpha_k-\alpha_\ell|,1\} = \frac{2}{n}A + O(1) < A\ .$$

The leading coefficient of the minimal polynomial of $(\alpha_q-\alpha_j)^{-1}$ is a divisor of the integer

$$\prod_{1\le k<\ell\le n}|\alpha_k-\alpha_\ell| < c_4 a^{n-1}.$$

Since the conjugates of $(\alpha_q-\alpha_j)^{-1}$ are less than 1 up to at most one, which is less than 3 by Lemma 2.1, we have

$$h\left(\frac{1}{\alpha_q-\alpha_j}\right) < \frac{2}{n}A + O(1) < A\ ,$$

and consequently

$$h\left(\frac{\alpha_h-\alpha_j}{\alpha_q-\alpha_j}\right) < 2A$$

for $1 \le j \le n$. Finally the degree of $\mathbb{Q}(\alpha_1,\dots,\alpha_n)$ is at most $n!$.

After these preparations we apply the Lang-Waldschmidt conjecture to Λ with the parameters $m = n!\,,\ k = n,\ \log B_1 = \ldots = \log B_n = 2A$ and $B = U$ and obtain

$$\log|\Lambda| > -c(n,n!)\,2nA\,\log U.$$

A comparison of this estimate with the lower bound yields

$$c_5(n)A\log U > \frac{nA}{(n+1)J}\,U + A - c_2$$

with $c_5 = 2n\,c(n,n!)$. The last inequality implies

$$U \le c_6 = c_6(a_1, \dots, a_{n-1}, n) \tag{21}$$

for all solutions of equation (6).

Assume now that (6) has infinitely many solutions $(a, x(a), y(a)) \in \mathbb{Z}^3$ with $|y(a)| > 1$. To any such triplet corresponds a vector

$$\vec{u} = (u_1, \dots, u_n, I) = \Big(u_1(a, x, y), \dots, u_n(a, x, y), (U_{\mathcal{O}} : U_\eta)\Big) \in \mathbb{Z}^{n+1}$$

via (11). (We put $u_j = 0$ for simplicity.) The absolute value of the coordinates of $\vec{u}$ is bounded by (21). As for any given $a \in \mathbb{Z}$ (6) has only finitely many solutions, $|y(a)| > 1$ holds for infinitely many a. Therefore there exists an $\vec{u} = (u_1, \dots, u_n, I)$ with $|u_i| < c_6$, which corresponds to solutions $(a, x(a), y(a))$ of (6) with $|y(a)| > 1$ for infinitely many $a \in \mathbb{Z}$. Let $\mathcal{A}$ denote the set of these infinitely many a's. In the remaining part of the proof we have to distinguish the cases $j < n$ and $j = n$.

Consider first the case $j < n$. Without restriction of generality, let us assume that $j \neq 1$. If there exists an $1 < i < n$ with $i \neq j$ such that $u_i \neq u_1$, then by Lemma 4.2 we have

$$0 \neq \frac{u_i - u_1}{I} = O\left(\frac{Y + A}{A^2}\right)$$

and therefore $Y \ge O(A^2)$. Consequently, $|u_1| \ge c_7 A$ by Lemma 4.2, which contradicts (21) if a is large enough. Hence $u_1 = u_i$ (for $1 \le i \le n-1,\ i \neq j$) for all but finitely many $a \in \mathcal{A}$. Similarly we derive $nu_n - (n-1)u_1 + I = 0$ for all but finitely many $a \in \mathcal{A}$. Let

$$\mathcal{A}_1 = \{a \in \mathcal{A} \mid u_i = u_1,\ 1 \le i \le n-1,\ i \neq j;\ nu_n - (n-1)u_1 + I = 0\}.$$

Then $\mathcal{A}_1$ is an infinite set and by (11) we get

$$(x(a) - \alpha_1 y(a))^I = \left(\prod_{\substack{i=1 \\ i \neq j}}^{n-1} \eta_{1i}\right)^{u_1} \eta_{1n}^{u_n}$$

for all $a \in \mathcal{A}_1$. By Lemma 4.3 this is only possible if $u_1 = u_n = -I$, i.e. if

$$x(a) - \alpha_1 y(a) = \pm\eta_{1j} = \pm(\alpha_1 - a_j).$$

But now $y(a) = \pm 1$ yields a contradiction.

The case $j = n$ is similar. Using Lemma 4.2 one proves first that $u_i = u_1$ $(1 \le i \le n-1)$ holds for all but finitely many $a \in \mathcal{A}$. Then one derives a contradiction by means of Lemma 4.4. This completes the proof of Theorem 4.1.

References

[ABC] N.C. Ankeny, R. Brauer and S. Chowla, *A note on the class numbers of algebraic number fields,* Amer. J. Math. **78** (1956), 51–61.

[BW] A. Baker and G. Wüstholz, *Linear forms and group varieties,* J. reine und angew. Math. **442** (1993), 19–63.

[BSch] E. Bombieri and W.M. Schmidt, *On Thue's equation,* Invent. Math. **109** (1992), 445–472.

[H-K1] F. Halter-Koch, *Unabhängige Einheitensysteme für eine allgemeine Klasse algebraischer Zahlkörper,* Abh. Math. Sem. Univ. Hamburg **43** (1975), 85–91.

[H-K2] F. Halter-Koch, *Große Faktoren in der Klassengruppe algebraischer Zahlkörper,* Acta Arith. **39** (1981), 33–47.

[La1] S. Lang, *Elliptic Curves: Diophantine Analysis*, Springer Verlag, 1978.

[La2] S. Lang, *Fundamentals of Diophantine Geometry*, Springer Verlag, 1983.

[MPR] M. Mignotte, A. Pethő and R. Roth, *Complete solutions of quartic Thue and index form equations*, Math. Comp., **65** (1996), 341–354.

[MT] M. Mignotte and N. Tzanakis, *On a family of cubics*, J. Number Theory **39** (1991), 41–49.

[Pe] A. Pethő, *Complete solutions to a family of quartic diophantine equations,* Math. Comp. **57** (1991), 777–798.

[PZ] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory,* Cambridge Univ. Press 1989.

[Se1] J.-P. Serre, *Lectures on the Modell-Weil Theorem*, Vieweg, 1989.

[Se2] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, 1992.

[Sw] R.G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.

[Th] E. Thomas, *Solutions to Certain Families of Thue Equations*, J. Number Theory **43** (1993), 319–369.