JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Volker ZIEGLER

Thomas' conjecture over function fields

Tome 19, n° 1 (2007), p. 289-309.

<http://jtnb.cedram.org/item?id=JTNB_2007__19_1_289_0>

Journal de Théorie des Nombres de Bordeaux **19** (2007), 289-309

Thomas' conjecture over function fields

par Volker ZIEGLER

Résumé. La conjecture de Thomas affirme que, pour des polynômes unitaires $p_1, \dots, p_d \in \mathbb{Z}[a]$ tels que $0 < \deg p_1 < \cdots < \deg p_d$, l'équation de Thue

$$(X - p_1(a)Y) \cdots (X - p_d(a)Y) + Y^d = 1$$

n'admet pas de solution non triviale (dans les entiers relatifs) pourvu que $a \geq a_0$, avec une borne effective a_0. Nous nous intéressons à un analogue de la conjecture de Thomas sur les corps de fonctions pour le degré $d = 3$ et en donnons un contrexemple.

Abstract. Thomas' conjecture is, given monic polynomials $p_1, \dots, p_d \in \mathbb{Z}[a]$ with $0 < \deg p_1 < \cdots < \deg p_d$, then the Thue equation (over the rational integers)

$$(X - p_1(a)Y) \cdots (X - p_d(a)Y) + Y^d = 1$$

has only trivial solutions, provided $a \geq a_0$ with effective computable a_0. We consider a function field analogue of Thomas' conjecture in case of degree $d = 3$. Moreover we find a counterexample to Thomas' conjecture for $d = 3$.

1. Introduction

In 1909 Thue [20] proved his famous theorem on the approximation of algebraic numbers by rational numbers. As a corollary he proved that the Diophantine equation

$$F(X, Y) = m,$$

where $F \in \mathbb{Z}[X, Y]$ is a binary irreducible form of degree at least 3 and m some non-zero integer, has only finitely many solutions. Since then such Diophantine equations are called Thue equations. There were several extensions of Thue's approximation theorem, e.g. to number fields by Wirsing [21] and also to function fields by Gill [7]. However Thue's theorem is not effective and so it is not possible to solve Thue equations effectively with this theorem. However, Baker [2] showed how to solve Thue equations effectively using his theorem on linear forms of logarithms [1, 3]. Since then

Manuscrit reçu le 16 novembre 2005.

The author was supported by the Austrian Science Foundation, project P18079-N12.

Mots clefs. Thue equation, function fields.

several Thue equations and families of Thue equations were solved. In 1993 Thomas [19] proved that the family

$$X(X-p_1(a)Y)(X-p_2(a)Y)+Y^3=1,$$

where $p_1,p_2\in\mathbb{Z}[a]$ are monic polynomials, such that $0<\deg p_1<\deg p_2$ and p_1,p_2 fulfill some growth conditions, has only trivial solutions, i.e. $(X,Y)=(1,0),(0,1),(p_1(a),1)$ and $(p_2(a),1)$, provided a is larger than some effective computable constant a_0. This led Thomas to his conjecture that

$$X(X-p_1(a)Y)\cdots(X-p_{d-1}(a)Y)+Y^d=1,$$

where $p_1,\dots,p_{d-1}\in\mathbb{Z}[a]$ are monic polynomials and $\deg p_1<\cdots<\deg p_{d-1}$, has only the trivial solutions $(X,Y)=(\pm1,0),(0,\pm1)$, $(\pm p_1(a),\pm1)$, $\dots,(\pm p_{d-1}(a),\pm1)$, provided a is sufficiently large and the minus sign only appears if d is even. This conjecture has been proved by Heuberger [8] under the assumption of some complicated degree conditions. However, if we allow $\deg p_1=0$, then some counterexamples are known, e.g. if $d=3$ and $p_1=\pm1$. In this case there exist the non-trivial solutions $(1,-(1+p_2(a)))$ respectively $(3+p_2(a),-2-p_2(a))$ found by Lee [10] respectively Mignotte and Tzanakis [15]. To the authors knowledge these are the only exceptions known yet in the case of rational integers and $d=3$. In this paper we find a counterexample with $\deg p_1>0$ and disprove Thomas conjecture for degree 3.

Halter-Koch, Lettl, Pethő and Tichy considered the following equation

$$X(X-a_1Y)\cdots(X-a_{d-2}Y)(X-aY)\pm Y^d=\pm1, \tag{1}$$

where $a_1,\dots,a_{d-2}\in\mathbb{Z}$ are fixed integers and a is some parameter. This equation has been solved under the assumption of the Lang-Waldschmidt conjecture [9]. In this paper we want to solve the function field analogue of equation (1).

Gill's result [7] applied to Thue equations, yields that the height of the solutions are bounded. About 50 years later Schmidt [18] and Mason (cf. [12], resp. [14]) considered the problem to determine effectively all solutions of a given Thue equation over some function field. In contrast to the number field case Thue equations over function fields may have infinitely many solutions. Recently, Lettl [11] proved criteria for which a given Thue equation has only finitely many solutions. Also families of Thue equations over the function field $\mathbb{C}(T)$ have been solved (cf. [5, 6]). We propose to prove following variant of Thomas' conjecture.

Theorem 1. *Let $\kappa, \lambda \in \mathbb{C}[T]$ be polynomials such that $0 < \deg \kappa < \deg \lambda$. Let κ be fixed and let $(X, Y) \in \mathbb{C}[T] \times \mathbb{C}[T]$ be a solution to the Diophantine equation*

$$X(X - \kappa Y)(X - \lambda Y) + Y^3 = \xi \tag{2}$$

with $\xi \in \mathbb{C}^*$. Then either the triple (λ, X, Y) is trivial, i.e.

$$(X, Y) \in \{(\zeta, 0), (0, \zeta), (\zeta\kappa, \zeta), (\zeta\lambda, \zeta) \,:\, \zeta^3 = \xi\}$$

or $(\lambda, X, Y) \in \mathcal{L}$ with $|\mathcal{L}| \le 16452$. In particular, if $34 \deg \kappa < \deg \lambda$, then there exist only trivial solutions.

If $\kappa \in \mathbb{C}^*$ then a non-trivial solution $(X, Y) \in \mathbb{C}[T] \times \mathbb{C}[T]$ to (2) exists, if and only if $\kappa^6 = 1$. All non-trivial solutions are listed in table 1.

Table 1. The non-trivial solutions to (2) in the case of $\kappa \in \mathbb{C}^*$ (ω_3 is a primitive third root of unity).

κ	X	Y	κ	X	Y
1	ζ	$-\zeta(1+\lambda)$	-1	$\zeta(3+\lambda)$	$-\zeta(2+\lambda)$
ω_3	$\zeta\omega_3^2$	$-\zeta(\omega_3+\lambda)$	$-\omega_3$	$\zeta(3\omega_3^2+\omega_3\lambda)$	$-\zeta(2\omega_3+\lambda)$
ω_3^2	$\zeta\omega_3$	$-\zeta(\omega_3^2-\lambda)$	$-\omega_3^2$	$\zeta(3\omega_3+\omega_3^2\lambda)$	$-\zeta(2\omega_3^2-\lambda)$

We see that in the case of $\kappa \in \mathbb{C}^*$ there are essentially no further solutions than those known before (except the cases $\kappa = -\omega_3, -\omega_3^2$ were not stated explicitly). These non-trivial solutions have been found by Lee [10], Mignotte and Tzanakis [15] in the rational case and by Ziegler [22] in the imaginary quadratic case ($\kappa = \omega_3, \omega_3^2$).

One might conjecture, as Thomas [19] did, that there are only trivial solutions, if $\deg \kappa > 0$ but this is not true. Indeed if $\lambda = \kappa^4 + 3\kappa$ or $\lambda = \kappa^4 - 2\kappa$, then there exist non-trivial solutions. The author conjectures that these are the only non-trivial solutions.

Conjecture 1. *The Diophantine equation* (2) *has only trivial solutions, except the solutions*

$$\begin{aligned} \zeta(-\lambda\kappa^5 - 4\kappa^3 - 1, \lambda\kappa - 6\kappa^2 - \lambda\kappa^4 - \kappa^5) \quad &\text{if } \lambda = \kappa^4 + 3\kappa, \\ \zeta(\kappa^3 - 1, \lambda\kappa - \lambda\kappa^4 - \kappa^2) \quad &\text{if } \lambda = \kappa^4 - 2\kappa, \end{aligned}$$

with $\zeta^3 = -\xi$.

To the authors knowledge the non-trivial solutions stated in Conjecture 1 have not be known before. Therefore we have disproved Thomas' conjecture in the case of $d = 3$.

The restriction $\kappa \neq 0$ is essential, because in this case we can find fundamental units. If $\kappa = 0$ and the valuation at infinity is ramified we are still able to determine the unit group. Theorem 2 characterizes for which λ's ramification at infinity occurs.

Theorem 2. *The function field* $\mathbb{C}(T,\alpha)$*, where* α *is a root of*

$$X^2(X-\lambda)+1,$$

is unramified over the prime corresponding to $\mathcal{O}_\infty := \{f(T)/g(T) : f,g \in \mathbb{C}[T], \deg(f) \leq \deg(g)\}$ *of* $\mathbb{C}[T]$*, if and only if* $2|\deg\lambda$*. In the case of ramification the ramification index of the ramified prime is* 2*.*

The methods used in the proof of Theorem 1 together with Theorem 2 yield:

Theorem 3. *The only solutions* $(X,Y) \in \mathbb{C}[T]\times\mathbb{C}[T]$ *to the Diophantine equation*

$$X^2(X-\lambda Y)+Y^3=\xi, \tag{3}$$

where $\lambda \in \mathbb{C}[T]\setminus\mathbb{C}$ *and* $\deg\lambda \equiv 1 \pmod 2$*, are trivial, i.e.* $(X,Y) = (\zeta,0),(0,\zeta)$ *or* $(\zeta\lambda,\zeta)$*, with* $\zeta^3=\xi$*.*

It is dissatisfactory to know nothing about the case of $\kappa = 0$ and $2|\deg\lambda$ except the finiteness of solutions, which we know from a result of Lettl [11, Corollary 2]. Although we do not know the structure of the unit group we are able to estimate the number of solutions to (3):

Theorem 4. *The Diophantine equation* (3) *has at most* 17691 *non-trivial solutions* $(X,Y) \in \mathbb{C}[T]\times\mathbb{C}[T]$ *for fixed* λ*.*

For the rest of the paper we will use following notation:

$$F(\kappa,\lambda) = X(X-\kappa)(X-\lambda)+1. \tag{4}$$

We remark that all theorems hold if we replace $\mathbb{C}$ by any algebraic closed field k of characteristic 0. In particular, the theorems are valid in $\bar{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$.

The paper is organized as follows. In section 2 we remind some well known facts on function fields and fix notations for the rest of the paper. After this we will prove Theorem 2 by using Puiseux's theorem in section 3. By a careful analysis of the valuations at infinity we are able to find fundamental units of the fields related to (2) and to (3) in the case of $2 \nmid \deg\lambda$. In the case of (3) and $2|\deg\lambda$ we can estimate by methods originating from the geometry of numbers the number of possible solutions. All these results give a lower bound for the height of solutions to (2) and (3) and are subject of section 4. The upper bound for the height of the solutions is computed in section 5. Knowing upper and lower bounds we can effectively determine the number of solutions. In the cases for which we know fundamental solutions we can determine all solutions. This is done in section 6. In section 7 we use a theorem of Minkowski in order to prove Theorem 4.

2. Auxiliary results

Let us remind first the ABC-Theorem for function fields (see e.g. [17, Theorem 7.17]).

Proposition 1 (ABC-Theorem)**.** *Let K be a function field of characteristic 0, genus g_K and with constant field k. Let $\alpha, \beta \in K^*$ satisfying $\alpha+\beta=1$ and put $A=(\alpha)_0$, $B=(\beta)_0$ and $C=(\alpha)_\infty=(\beta)_\infty$, where $(\cdot)_0$ denotes the zero divisor and $(\cdot)_\infty$ denotes the polar divisor. Then*

$$\deg A = \deg B = \deg C \leq \max\left(0, 2g_K - 2 + \sum_{P\in \operatorname{Supp}(A+B+C)} \deg_K P\right).$$

If the constant field k is algebraically closed and of characteristic 0, Mason [14, chapter 1, Lemma 2] proved following special case.

Corollary 1. *Let $H(\alpha) := -\sum_{\nu\in M_K} \min(0,\nu(\alpha))$ denote the height of $\alpha \in K$ and let $\gamma_1,\gamma_2,\gamma_3 \in K$ with $\gamma_1+\gamma_2+\gamma_3=0$. Let $\mathcal{V}$ be a finite set of valuations such that for all $\nu \notin \mathcal{V}$ we have $\nu(\gamma_1)=\nu(\gamma_2)=\nu(\gamma_3)$, then*

$$H(\gamma_1/\gamma_2) \leq \max(0, 2g_K - 2 + |\mathcal{V}|).$$

Here we denote the set of all valuations in K by M_K. It is rather easy to deduce Corollary 1 from Proposition 1 (cf. [5]). Use the fact that the residue class degree is 1, provided the constant field is algebraic closed and of characteristic 0.

Another well known fact is the following: Let A be a Dedekind ring, K its quotient field and let B be the integral closure of some finite algebraic extension L/K. Further, let d be the exact power of a prime $\mathfrak{P}$ dividing the different $\mathcal{D}_{B/A}$. Then $d = e_{\mathfrak{P}} - 1$ provided the characteristic of $B/\mathfrak{P}$ does not divide the ramification index $e_{\mathfrak{P}}$. Our main interest is in function fields with constant field of characteristic 0. In this case $B/\mathfrak{P}$ has always characteristic 0 and we have $\mathcal{D}_{B/A} = \prod \mathfrak{P}^{e_{\mathfrak{P}}-1}$. We will use this fact in the case of $A = \mathcal{O}_a := \{f(T)/g(T) : f,g \in \mathbb{C}[T], g(a)\neq 0\}$ with $a \in \mathbb{C}$. Assume L/K is a Galois extension, A a discrete valuation ring and B its integral closure in L. Let $\mathfrak{p}$ be the maximal prime of A, then $\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$. We have $\mathcal{D}_{B/A} = (\mathfrak{P}_1\cdots\mathfrak{P}_g)^{e-1}$ and

$$\mathrm{N}_{L/K}(\mathcal{D}_{B/A}) = \mathfrak{p}^{f(e-1)g} = \mathfrak{p}^{(e-1)g} = \delta_{B/A}, \tag{5}$$

where $\delta_{B/A}$ denotes the discriminant. This will allow us to determine, where ramification occurs and compute the ramification index.

We have already introduced for every $a \in \mathbb{C}$ the discrete valuation ring $\mathcal{O}_a$, the corresponding valuations ν_a to these rings are called finite. There is also another valuation ring $\mathcal{O}_\infty := \{f(T)/g(T) : f,g \in \mathbb{C}[T], \deg(f) \leq \deg(g)\}$, which has already been introduced in Theorem 2. The corresponding valuation ν_∞ will be called the infinite valuation. It is well known (see e.g. [4, chapter 1, Proposition 4.4]) that the finite and infinite valuations are in fact all $\mathbb{C}$-valuations of $\mathbb{C}(T)$.

The following result is useful to determine ramifications and valuations:

Proposition 2 (Puiseux). *Let k be an algebraic closed field of characteristic 0. And let K be a function field defined by the polynomial*

$$P(X,T) = X^d + P_{d-1}(T)X^{d-1} + \cdots + P_0(T)$$

with coefficients $P_0, \ldots, P_{d-1} \in k(T)$, then for each $a \in k$ there exist formal Puiseux series

$$y_{i,j} = \sum_{h=m_i}^{\infty} c_{h,i}\zeta_i^{hj}(T-a)^{h/e_{a,i}} \qquad (1 \leq j \leq e_{a,i}, 1 \leq i \leq r_a),$$

where $c_{h,i} \in k$ and $\zeta_i \in k$ is an $e_{a,i}$-th root of unity such that

$$P(X,T) = \prod_{i=1}^{r_a}\prod_{j=1}^{e_{a,i}}(X - y_{i,j}).$$

Moreover let $\mathfrak{P}_1, \ldots, \mathfrak{P}_{r_a}$ be the primes of K lying above the prime $(T-a)$ then $e_{a,i} = e(\mathfrak{P}_i|(T-a))$ for $i = 1, \ldots, r_a$ for some appropriate order of the indices.

Note that a similar statement is true for infinite valuations. Furthermore the m_i are the valuations of α with respect to the primes above $(T-a)$, where α is a root of $P(X,T)$.

Let $F(X,Y) = m$ be a Thue equation over the integral closure $\mathcal{O}_L$ of $k[T]$ in some finite extension $L/k(T)$. Mason [12] proved an effective bound for the height of solutions (X,Y) to $F(X,Y) = m$ by using his fundamental inequality presented in Corollary 1. For an application of Mason's fundamental lemma (Corollary 1), we need a tool to compute the genus of a function field. The Riemann-Hurwitz formula (see e.g. [17, Theorem 7.16]) yields such a tool.

Proposition 3 (Riemann-Hurwitz). *Let L/K be a geometric extension of function fields of characteristic 0, with constant field k and let g_K and g_L be the genera of K and L, respectively, then*

$$2g_L - 2 = [L:K](2g_K - 2) + \sum_{w \in M_L}(e_w - 1), \tag{6}$$

where M_L is the set of valuations of L and e_w denotes the ramification index of w in the extension L/K.

By a geometric extension L/K we denote a finite algebraic extension of function fields such that $L \cap \bar{k} = k$ holds for the constant field k. Note that if k is algebraic closed, every finite algebraic extension is geometric.

We end this section by investigating some properties of the polynomials of interest. First we prove that they are irreducible.

Lemma 1. *The polynomials*

$$X^2(X-\lambda)+1 \quad \textit{and} \quad X(X-\kappa)(X-\lambda)+1$$

are irreducible under the same restrictions as made in Theorems 1 and 2. We also allow κ to be a constant.

Proof. Suppose one of the polynomials is reducible, then this polynomial splits into a linear factor $X-a$ and a quadratic factor X^2+bX+c with $a,b,c \in \mathbb{C}(T)$. Since the coefficients of the polynomial are elements of $\mathbb{C}[T]$ also $a,b,c \in \mathbb{C}[T]$, hence a is a constant. Moreover, a is a root of the polynomial and therefore $a^2(a-\lambda)+1=0$ respectively $a(a-\kappa)(a-\lambda)+1=0$. If $a \neq 0$, $a \neq \lambda$ respectively $a \neq 0$ $a \neq \kappa$ and $a \neq \lambda$ the left hand side has degree at least $\deg \lambda > 0$ therefore $a=0$, $a=\lambda$ respectively $a=0, a=\kappa$ or $a=\lambda$. In any case this would yield $1=0$. Therefore the polynomial is irreducible. $\square$

For the rest of the paper we will denote by α a root of $F(\kappa,\lambda)$ respectively $F(0,\lambda)$ and by $\alpha_1 := \alpha, \alpha_2$ and α_3 its conjugates over $\mathbb{C}(T)$.

Let us denote by $\delta := (\alpha_1-\alpha_2)^2(\alpha_2-\alpha_3)^2(\alpha_3-\alpha_1)^2$ the discriminant of the polynomial $F=F(\kappa,\lambda)$ resp. $F=F(0,\lambda)$. If δ is a square in $\mathbb{C}(T)$ we know that the field $K=\mathbb{C}(T,\alpha)$ is Galois over $\mathbb{C}(T)$. We compute

$$\delta = \begin{cases} 4(\lambda+\kappa)^3+\lambda^2\kappa^2(\lambda+\kappa)^2 & \\ -18\lambda\kappa(\lambda+\kappa)-4\lambda^3\kappa^3-27, & \text{if } F=F(\kappa,\lambda), \\ 4\lambda^3-27, & \text{if } F=F(0,\lambda). \end{cases} \tag{7}$$

Lemma 2. *Let α be a root of $F=F(0,\lambda)$, then $K=\mathbb{C}(T,\alpha)$ is not Galois over $\mathbb{C}(T)$.*

Proof. The lemma is equivalent to the statement that the equation $4X^3-27=Y^2$ has only constant solutions. We apply a theorem of Mason (see [14, Theorem 6] or [13]) to this equation:

Lemma 3 (Mason)**.** *For a fixed function field $L/\mathbb{C}$ let $\alpha_1,\dots,\alpha_n \in L$ and $\mathcal{O}_L$ the integral closure of $\mathbb{C}[T]$ in L. Assume $(X,Y) \in \mathcal{O}_L \times \mathcal{O}_L$ is a solution of the equation*

$$(X-\alpha_1)\cdots(X-\alpha_n)=Y^2,$$

then $H_L(X) \leq 26H+8g_L+4(r-1)$, where H is the height of the polynomial on the left side of the equation, g_L is the genus of L and r is the number of valuations of L above ∞.

We apply Lemma 3 for $L=\mathbb{C}(T)$. Then we have $r=1$, $g_L=0$ and $H=0$. Therefore $H(X)\leq 0$, which means X is a constant, hence both X and Y are constants. $\square$

Note that instead of Mason's theorem (Lemma 3) we could also use a theorem of Ribenboim [16] on Diophantine equations in polynomials.

The author conjectures that the Galois group of the polynomial $F(\kappa,\lambda)$, with $-\infty<\deg\kappa<\deg\lambda$ is always the symmetric group S_3. Unfortunately the author could only prove Lemma 2.

3. Proof of Theorem 2

The proof will essentially depend on Puiseux's theorem (Proposition 2). In particular, we use the fact that the m_i (in the notation of Puiseux's theorem) are the different valuations of the root α of $P(X,T)$ in K. In view of Theorem 2 we denote by α a root of $X^2(X-\lambda)+1$. The Puiseux series at infinity can be interpreted as the "asymptotic" expansion of α. We compute the Puiseux series of $X^2(X-T)+1$ and obtain

$$\begin{aligned}\alpha_1&=T-\frac{1}{T^2}-\frac{2}{T^5}+\cdots,\\ \alpha_2&=\frac{1}{T^{1/2}}+\frac{1}{2T^2}+\frac{5}{8T^{7/2}}+\cdots,\\ \alpha_3&=-\frac{1}{T^{1/2}}+\frac{1}{2T^2}-\frac{5}{8T^{7/2}}+\cdots.\end{aligned}\tag{8}$$

Therefore we have proved Theorem 2 in the special case $\lambda=T$. Since Puiseux series are formal power series we may replace T by $\lambda(T)$ and replace $\sqrt{\lambda(T)}$ by one of the Puiseux series of $X^2-\lambda(T)$ at ∞. Let $l=\deg\lambda>0$ and a_l the leading coefficient of λ. We obtain after replacing and rearranging the power series (8) the series

$$\begin{aligned}\alpha_1&=a_lT^l+\cdots\\ \alpha_2&=\frac{1}{\sqrt{a_l}}T^{-l/2}+\cdots\\ \alpha_3&=-\frac{1}{\sqrt{a_l}}T^{-l/2}+\cdots\end{aligned}$$

Obviously K is ramified at infinity if l is odd. So it remains to show that K is unramified at infinity if l is even. A close look on Puiseux's theorem shows that if the series of α_2 and α_3 correspond to the same ramified valuation then, the coefficients coincide for every integral exponent. Therefore ramification at infinity can only occur if $\sqrt{a_l}=-\sqrt{a_l}$, hence $a_l=0$, but this is a contradiction to the assumption that a_lT^l is the leading term of λ. Therefore the valuation at infinity is unramified in this case, which proves Theorem 2.

4. Fundamental Units

In order to solve Diophantine equations (2) and (3) we have to investigate the structure of $\mathbb{C}[T,\alpha]^*$. In particular we prove:

Proposition 4. *Let α be a root of $F(\kappa,\lambda)$ with $\kappa \neq 0$ then, $\mathbb{C}[T,\alpha]^* = \langle \alpha, \alpha-\kappa\rangle \times \mathbb{C}^*$. If α is a root of $F(0,\lambda;X)$ and $\deg\lambda = l$ is odd, then $\mathbb{C}[T,\alpha]^* = \langle\alpha\rangle \times \mathbb{C}^*$.*

Let $\varepsilon \in \mathbb{C}[T,\alpha]^*$ and $\varepsilon_1 := \varepsilon, \varepsilon_2$ and ε_3 its conjugates, then we have

$$\varepsilon_i = h_0 + h_1\alpha_i + h_2\alpha_i^2 \quad (1 \le i \le 3), \tag{9}$$

with $h_0, h_1, h_2 \in \mathbb{C}[T]$. Solving this linear system by Cramer's rule one obtains

(10)

$$h_0 = \frac{\varepsilon_1\alpha_2\alpha_3(\alpha_3-\alpha_2)+\varepsilon_2\alpha_3\alpha_1(\alpha_1-\alpha_3)+\varepsilon_3\alpha_1\alpha_2(\alpha_2-\alpha_1)}{\delta},$$
$$h_1 = \frac{\varepsilon_1(\alpha_2+\alpha_3)(\alpha_2-\alpha_3)+\varepsilon_2(\alpha_3+\alpha_1)(\alpha_3-\alpha_1)+\varepsilon_3(\alpha_1+\alpha_2)(\alpha_1-\alpha_2)}{\delta},$$
$$h_2 = \frac{\varepsilon_1(\alpha_3-\alpha_2)+\varepsilon_2(\alpha_1-\alpha_3)+\varepsilon_3(\alpha_2-\alpha_1)}{\delta},$$

where

$$\delta = \det(\alpha_j^{i-1})_{1\le i,j\le 3} = (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)$$

is the square root of the discriminant of $F(\kappa,\lambda)$ resp. $F(0,\lambda)$.

We know that h_0, h_1 and $h_2 \in \mathbb{C}[T]$, that is their valuations at infinity are ≤ 0 or $= +\infty$. The following lemma is essential for proving Proposition 4.

Lemma 4. *Let $\varepsilon \in \mathbb{C}[T,\alpha]^* \setminus \mathbb{C}^*$ then $H(\varepsilon) \ge \deg\lambda + \deg\kappa$ if α is a root of $F(\kappa,\lambda)$ with $\kappa \neq 0$, and $H(\varepsilon) \ge \deg\lambda$ if α is a root of $F(0,\lambda)$ and $2 \nmid \deg\lambda$.*

Proof. We have to distinguish two cases: $\kappa \neq 0$, $\kappa = 0$ and $2 \nmid l$. For the rest of the proof and also for the rest of the paper we define $l := \deg\lambda$ and $k := \deg\kappa$.

In a first step we compute the infinite valuations of α. To obtain the valuations of α we have to factor $F(\kappa,\lambda)$ over $\mathbb{C}((1/T))$. Let

$$\begin{aligned} F(\kappa,\lambda) =& X^3 - (\lambda+\kappa)X^2 + \lambda\kappa X + 1 \\ =& (X - (a_{v_1}^{(1)}T^{v_1} + \cdots))(X - (a_{v_2}^{(2)}T^{v_2} + \cdots))(X - (a_{v_3}^{(3)}T^{v_3} + \cdots)), \end{aligned}$$

then $-v_i$ are the infinite valuations of α. Let us assume $v_1 \geq v_2 \geq v_3$. By comparing coefficients we obtain for $\kappa \neq 0$

$$\begin{aligned}\lambda+\kappa =&(a_{v_1}^{(1)}T^{v_1}+\cdots)+(a_{v_2}^{(2)}T^{v_2}+\cdots)+(a_{v_3}^{(3)}T^{v_3}+\cdots),\\ \lambda\kappa =&(a_{v_1}^{(1)}T^{v_1}+\cdots)(a_{v_2}^{(2)}T^{v_2}+\cdots)+(a_{v_2}^{(2)}T^{v_2}+\cdots)(a_{v_3}^{(3)}T^{v_3}+\cdots)\\ &+(a_{v_3}^{(3)}T^{v_3}+\cdots)(a_{v_1}^{(1)}T^{v_1}+\cdots),\\ -1 =&(a_{v_1}^{(1)}T^{v_1}+\cdots)(a_{v_2}^{(2)}T^{v_2}+\cdots)(a_{v_3}^{(3)}T^{v_3}+\cdots),\end{aligned}$$

hence

$$\max\{v_1,v_2,v_3\}\geq l,\ \max\{v_1+v_2,v_2+v_3,v_3+v_1\}\geq l+k,\ v_1+v_2+v_3=0.$$

In the case of $v_1=v_2=v_3$ we have $v_1=v_2=v_3=0$, hence $l\leq 0$ which is a contradiction. If $v_1=v_2>v_3$, then $2v_1=l+k$, but $\max(v_1,v_2,v_3)=l/2+k/2<l$, again a contradiction. Let $v_1>v_2=v_3$. Then $v_1=l$, hence $v_2\geq k$ and $v_1+v_2+v_3\geq l+2k>0$. Now assume $v_1>v_2>v_3$, then we have $v_1=l$, $v_1+v_2=l+k$ and $v_1+v_2+v_3=0$, hence $v_1=l, v_2=k$ and $v_3=-l-k$.

In the case of $\kappa=0$ we similarly obtain $v_1=l$ and $v_2=v_3=-l/2$. Moreover it is easy to compute the a's. We find that $a_l^{(1)}=a_l$ and $a_{l/2}^{(2)}=-a_{l/2}^{(3)}=\frac{1}{\sqrt{a_l}}$ where a_l is the leading coefficient of λ. Note that we have already proved this in section 3.

First we study the case $\kappa\neq 0$. Let ∞_1,∞_2 and ∞_3 be the infinite valuations of $K=\mathbb{C}(T,\alpha)$ such that $(\alpha)=-l\infty_1-k\infty_2+(l+k)\infty_3$ is the principal divisor of α. Moreover, let $\varepsilon\in\mathbb{C}[T,\alpha]^*$ with $(\varepsilon)=e_1\infty_1+e_2\infty_2+e_3\infty_3$ and $\varepsilon=h_0+h_1\alpha+h_2\alpha^2$. We denote by d_i the degree of h_i with $i=0,1,2$. In the case of $h_i=0$ we set $d_i=-\infty$. We note that if two of the h's are zero it is easy to see that Lemma 4 holds.

Let $m=\min\{-d_0,-d_1-l,-d_2-2l\}$. First we suppose $-d_0=m$. Since $l>k$ we get $-d_0<\min\{-d_1-k,-d_2-2k\}$ and $-d_0<\min\{-d_1+l+k,-d_2+2l+2k\}$ and therefore $e_2=e_3=-d_0\leq -d_2-2l\leq 2l$ if $h_2\neq 0$ and $e_2=e_3=-d_0\leq -d_1-l\leq -l$ if $h_1\neq 0$, hence $|e_1|=|e_2+e_3|\geq 2l$ and $H_K(\varepsilon)\geq 2l\geq l+k$. Now we assume $-d_1-l=m<-d_2-2l$ or $-d_2-2l=m$ is the sole minimum. Then $e_1=m\leq -2l$ and again $H_K(\varepsilon)\geq 2l\geq l+k$. At last we assume $-d_1-l=-d_2-2l=m\neq -d_0$ note that in this case d_1 or d_2 cannot be $-\infty$. Then $d_1=d_2+l$ and the minimum of $\{-d_0,-d_1-k,-d_2-2k\}$ is either $-d_0$ or $-d_1-k=-d_2-l-k$. If $d_0\neq d_1+k$ then e_2 is equal to the minimum which is $\leq -d_2-l-k$. If $d_0=d_1+k$ we have $(-d_0,-d_1+l+k,-d_2+2l+2k)=(-d_1-k,-d_1+l+k,-d_1+l+2k)$. The sole minimum of this set is $e_3=-d_1-k=-d_2-l-k\leq -l-k$.

Now let us consider the case $\kappa=0$ and $2\nmid l$. In this case $(\alpha)=-l\infty_1+l\infty_2$, where ∞_2 denotes the ramified valuation. Moreover we let $(\varepsilon)=$

$e_1\infty_1 + e_2\infty_2$. Note that $e_1 = -e_2$, because ε is a unit of $\mathbb{C}[T,\alpha]$. This time we put $m = \min\{-d_0, -d_1 - l, -d_2 - 2l\}$.

Suppose $m = -d_0$ then $-2d_0 < \min\{-2d_1 + l, -2d_2 + 2l\}$, i.e. $e_2 = -2d_0 = 2m \leq -2d_2 - 4l \leq -4l$ if $h_2 \neq 0$ and $e_2 \leq -2d_1 - 2l \leq -2l$ if $h_1 \neq 0$. If $m = -d_1 - l$ or $m = -d_2 - 2l$ is the sole minimum, then $e_1 = -d_1 - l$ or $e_1 = -d_2 - 2l$. In any case $H_K(\varepsilon) = |e_1| \geq l$. Now let us assume $-d_1 - l = -d_2 - 2l = m$ respectively $d_1 = d_2 + l$. We find $(-2d_0, -2d_1 + l, -2d_2 + 2l) = (-2d_0, -2d_1 + l, -2d_1 + 4l)$. Either $-2d_0$ or $-2d_1 + l = -2d_2 - l$ is the sole minimum or $2d_0 = 2d_1 + l$. The first two cases yield that e_2 is equal to the sole minimum which is at most $-2d_2 - l \leq -l$, hence $H_K(\varepsilon) \geq l$. The last case is impossible since l is odd. $\square$

Now we prove $\mathbb{C}[T,\alpha]^* = \langle \alpha, \alpha - \kappa\rangle \times \mathbb{C}^*$. Let us write $\eta_1 = \alpha$ and $\eta_2 = \alpha - \kappa$. Moreover, we define the map

$$\log:\ \mathbb{C}[T,\alpha]^* \to \mathbb{R}^2 \qquad \log(\varepsilon) \mapsto (e_1, e_2),$$

where $(\varepsilon) = e_1\infty_1 + e_2\infty_2 + e_3\infty_3$. Obviously $\log(\mathbb{C}[T,\alpha]^*)$ is a lattice $\Lambda \subset \mathbb{Z}^2$ and we have $\ker\log = \mathbb{C}^*$. Therefore we have to prove $\log(\eta_1)$ and $\log(\eta_2)$ generate Λ or equivalently $\log(\eta_1) = (-l, -k) = \omega_1$ and $\log(\eta_1/\eta_2) = (0, l + 2k) = \omega_2$ generate Λ. Now let ε be any unit with $\log(\varepsilon) = (e_1, e_2)$. It is clear that subtracting from (e_1, e_2) suitable (integral) multiples of ω_1 and ω_2 we obtain a new vector (e_1', e_2') with $-l/2 \leq e_1' < l/2$ and $-(l + 2k)/2 \leq e_2' < (l + 2k)/2$. By Lemma 4 we know $\max\{|e_1|, |e_2|, |e_1 + e_2|\} \geq l + k$ or $\varepsilon \in \mathbb{C}^*$. Therefore $(e_1', e_2') = (0, 0)$, i.e. ω_1 and ω_2 generate Λ.

In the case of $F(0,\lambda)$ and $2 \nmid l$ the proof is easier. This time we define our log-map as follows:

$$\log:\ \mathbb{C}[T,\alpha]^* \to \mathbb{R} \qquad \log(\varepsilon) \mapsto e_1,$$

where $(\varepsilon) = e_1\infty_1 + e_2\infty_2$. Again $\log(\mathbb{C}[T,\alpha]^*)$ is a lattice $\Lambda \subset \mathbb{Z}$ and we have $\ker\log = \mathbb{C}^*$. Therefore we have to prove that $\log(\alpha) = -l$ generates Λ. Because of Lemma 4 we know that for any $\varepsilon \in \mathbb{C}[T,\alpha]^* \setminus \mathbb{C}^*$ we have $|\log(\varepsilon)| \geq l$ and therefore $\log(\varepsilon)$ must be a multiple of $\log(\alpha)$. Otherwise there would exist an integer k such that

$$-l/2 \leq \log(\varepsilon') = \log(\varepsilon\alpha^{-k}) = \log(\varepsilon) - k\log(\alpha) < l/2$$

and $\log(\varepsilon') \neq 0$, a contradiction.

The next lemma tells us something about the valuations of units in the case of $\kappa = 0$ and $2|l$.

Lemma 5. *Let $\varepsilon \in \mathbb{C}[T,\alpha]^* \setminus \mathbb{C}^*$. Then $H(\varepsilon) \geq \deg\lambda/2$, if α is a root of $F(0,\lambda)$ and $2|\deg\lambda$. Let $(\varepsilon) = e_1\infty_1 + e_2\infty_2 + e_3\infty_3$, where we choose $\infty_1, \infty_2, \infty_3$ such that $(\alpha) = -l\infty_1 + l/2\infty_2 + l/2\infty_3$. We have*

$$
\begin{aligned}
&|e_1| \geq l, && \text{if } |e_1| = \max_i |e_i|,\\
&|e_2| \geq l/2, && \text{if } |e_2| = \max_i |e_i|, \qquad (11)\\
&|e_3| \geq l/2, && \text{if } |e_3| = \max_i |e_i|.
\end{aligned}
$$

Proof. In order to prove this lemma we have to consider the normal closure $L = \mathbb{C}(T, \alpha_1 - \alpha_2)$ of $K = \mathbb{C}(T,\alpha)$. We have to compute the valuations in the closure, since we want to compute the degree of h_2 in terms of e_1, e_2 and e_3 using (10). For the valuations of the relevant quantities see table 2.

TABLE 2. Valuations of the relevant quantities.

	$\sigma_1: \alpha_1-\alpha_2 \mapsto \alpha_1-\alpha_2$	$\sigma_2: \alpha_1-\alpha_2 \mapsto \alpha_1-\alpha_3$	$\sigma_3: \alpha_1-\alpha_2 \mapsto \alpha_2-\alpha_3$	$\sigma_4: \alpha_1-\alpha_2 \mapsto \alpha_2-\alpha_1$	$\sigma_5: \alpha_1-\alpha_2 \mapsto \alpha_3-\alpha_1$	$\sigma_6: \alpha_1-\alpha_2 \mapsto \alpha_3-\alpha_2$
$\alpha_1-\alpha_2$	$-l$	$-l$	$l/2$	$-l$	$-l$	$l/2$
$\alpha_2-\alpha_3$	$l/2$	$l/2$	$-l$	$-l$	$-l$	$-l$
$\alpha_3-\alpha_1$	$-l$	$-l$	$-l$	$l/2$	$l/2$	$-l$
α_1	$-l$	$-l$	$l/2$	$l/2$	$l/2$	$l/2$
α_2	$l/2$	$l/2$	$l/2$	$-l$	$-l$	$l/2$
α_3	$l/2$	$l/2$	$-l$	$l/2$	$l/2$	$-l$

At first, note that L is unramified above ∞, since with $K_1 = \mathbb{C}(T,\alpha_1)$ and $K_2 = \mathbb{C}(T,\alpha_2)$ also $L = K_1K_2$ is unramified. We obtain

$$
\begin{aligned}
\left(\frac{\varepsilon_1(\alpha_3-\alpha_2)}{\delta}\right)_\infty =&(e_1+2l)\infty_1 + (e_1+2l)\infty_2 + (e_2+l/2)\infty_3\\
&+ (e_2+l/2)\infty_4 + (e_3+l/2)\infty_5 + (e_3+l/2)\infty_6,\\
\left(\frac{\varepsilon_2(\alpha_1-\alpha_3)}{\delta}\right)_\infty =&(e_2+l/2)\infty_1 + (e_3+l/2)\infty_2 + (e_3+l/2)\infty_3\\
&+ (e_1+2l)\infty_4 + (e_1+2l)\infty_5 + (e_2+l/2)\infty_6,\\
\left(\frac{\varepsilon_3(\alpha_2-\alpha_1)}{\delta}\right)_\infty =&(e_3+l/2)\infty_1 + (e_2+l/2)\infty_2 + (e_1+2l)\infty_3\\
&+ (e_3+l/2)\infty_4 + (e_2+l/2)\infty_5 + (e_1+2l)\infty_6,
\end{aligned}
$$

where $(\cdot)_\infty$ denotes the polar divisor, ∞_i is the valuation corresponding to σ_i and

$$(\varepsilon)_\infty = e_1\infty_1 + e_1\infty_2 + e_2\infty_3 + e_2\infty_4 + e_3\infty_5 + e_3\infty_6.$$

Now let $m = \min\{e_1 + 2l, e_2 + l/2, e_3 + l/2\}$. We know $0 \geq -\deg h_2 \geq m$ if $h_2 \neq 0$. This can only happen if either $e_1 \leq -2l$ or $e_2 \leq -l/2$ or $e_3 \leq -l/2$. Therefore (11) is satisfied in this case.

Now we want to prove that $H_K(\varepsilon) \geq l$ if $h_2 = 0$. We use the same method as used in the proof of Lemma 4. Remind that $d_i = \deg h_i$ for $i = 0, 1$. Let $m = \min\{-d_0, -d_1 - l\}$. Assume $m = -d_0$, then $-d_0 < -d_1 + l/2$ and $e_2 = -d_0 \leq -d_1 - l \leq -l$. On the other hand if $-d_1 - l$ is the sole minimum of $\{-d_0, -d_1 - l\}$ then $e_1 = -d_1 - l \leq -l$. □

5. Bounding the height of the solutions

The aim of this section is to prove an upper bound for the solutions to (2) resp. (3). We start with some notations usually used in the case of number fields. Let (X, Y) be a solution to (2) resp. (3) and let α_i, with $i = 1, 2, 3$ be the roots of $F(\kappa, \lambda)$ resp. $F(0, \lambda)$. Then we define

$$\alpha_{i,j} := \alpha_i - \alpha_j, \qquad \beta_i := X - \alpha_i Y, \qquad \gamma_{i,j,k} := \beta_i \alpha_{j,k},$$

and we write $\beta := \beta_1 = X - \alpha Y$. Equation (2) resp. (3) may be expressed as $\mathrm{N}_{K/\mathbb{C}(T)}(X - \alpha Y) = \xi$, where $\mathrm{N}_{K/\mathbb{C}(T)}$ denotes the norm from $K = \mathbb{C}(T, \alpha)$ to $\mathbb{C}(T)$. From this norm notation we deduce $\beta_i \in \mathbb{C}[T, \alpha]^*$. We denote by $L := K(\alpha_2, \alpha_3) = \mathbb{C}(T, \alpha_1 - \alpha_2)$ the splitting field of $F(\kappa, \lambda)$. If K is Galois then $K = L$. By δ_K respectively δ_L we denote the discriminant of the Dedekind ring extension $\mathcal{O}_K/\mathbb{C}[T]$ respectively $\mathcal{O}_L/\mathbb{C}[T]$. By $\hat{\delta}_K$ respectively $\hat{\delta}_L$ we denote the discriminant of the element α_1 respectively $\alpha_1 - \alpha_2$.

In order to get sharp estimates for the height of β we investigate Mason's approach to Thue equations (see [12, 14]). In particular we use Siegel's identity

$$\gamma_{1,2,3} + \gamma_{2,3,1} + \gamma_{3,1,2} = 0$$

and combine it with the ABC-Theorem (Proposition 1), respectively with Mason's fundamental lemma (Corollary 1).

In the following we distinguish whether $K = \mathbb{C}(T, \alpha)$ is Galois or not. We start by factoring the discriminant. Let $\mathcal{O}_L$ denote the algebraic closure of $\mathbb{C}[T]$ in $L = \mathbb{C}(T, \alpha_1, \alpha_2, \alpha_3) = \mathbb{C}(T, \alpha_1 - \alpha_2)$. Since $\mathbb{C}[T, \alpha_1 - \alpha_2] \subset \mathcal{O}_L$ we compute the discriminant $\tilde{\delta} = \delta(\alpha_1 - \alpha_2)$. If K is Galois, then

$$\hat{\delta}_K = \tilde{\delta} = (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_3 - \alpha_1)^2.$$

If K is not Galois, we find

$$\begin{aligned}\hat{\delta}_L = \tilde{\delta} = &64(\alpha_1 - \alpha_2)^6 (\alpha_2 - \alpha_3)^6 (\alpha_3 - \alpha_1)^6 \\ &\times (2\alpha_1 - \alpha_2 - \alpha_3)^4 (2\alpha_2 - \alpha_1 - \alpha_3)^4 (2\alpha_3 - \alpha_1 - \alpha_2)^4.\end{aligned}$$

Note that $\tilde{\delta}$ is a symmetric polynomial in α_1, α_2 and α_3. Therefore we can write $\tilde{\delta}$ as a polynomial in $s_1 = \alpha_1 + \alpha_2 + \alpha_3 = \lambda\kappa$, $s_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 =$

$\lambda+\kappa$ and $s_3 = \alpha_1\alpha_2\alpha_3 = -1$. A symbolic computation e.g. in Mathematica shows

$$\begin{aligned}\hat{\delta}_L &= 64(27 - 2\kappa^3 + 3\kappa^2\lambda + 3\kappa\lambda^2 - 2\lambda^3)^4 \\ &\quad \times (-27 - 6\kappa\lambda^2 + \kappa^4\lambda^2 + 4\lambda^3 + \kappa^2\lambda(-6+\lambda^3) - 2\kappa^3(-2+\lambda^3))^3,\end{aligned}$$

respectively

$$\hat{\delta}_K = -27 - 4\kappa^3\lambda^3 - 18\kappa\lambda(\kappa+\lambda) + \kappa^2\lambda^2(\kappa+\lambda)^2 + 4(\kappa+\lambda)^3.$$

Now it is easy to deduce $\deg \hat{\delta}_K = 4l + 2k$, if K is Galois and $\deg \hat{\delta}_L = 24l + 6k$ if K is not Galois and $\kappa \neq 0$, respectively $\deg \hat{\delta}_L = 21l$ if $\kappa = 0$.

First, let us consider the non-Galois case. Since the discriminant (cf. section 2)

$$\delta_L = (\mathfrak{p}_{1,2}\cdots\mathfrak{p}_{r_2,2})^3(\mathfrak{p}_{1,3}\cdots\mathfrak{p}_{r_3,3})^4(\mathfrak{p}_{1,6}\cdots\mathfrak{p}_{r_6,6})^5 = (d_L),$$

we have

$$d_L = \prod_{g=1}^{r_2}(T - a_{g,2})^3 \prod_{g=1}^{r_3}(T - a_{g,3})^4 \prod_{g=1}^{r_6}(T - a_{g,6})^5$$

and $\hat{\delta}_L = d_L R^2$ with $d_L, R \in \mathbb{C}[T]$: Note that the $\mathfrak{p}_{i,j}$ are the primes generated by $T - a_{i,j}$.Therefore we have

$$\deg \hat{\delta}_L = 3r_2 + 4r_3 + 5r_6 + 2r, \tag{12}$$

where r_i is the number of finite primes ramified with ramification index $e = i$ and where $r = \deg R$. In the Galois case we obtain similarly

$$\deg \hat{\delta}_L = 2r_3 + 2r. \tag{13}$$

Note that in the case of $\kappa = 0$ and $l \equiv 1 \pmod 2$ also the infinite prime is ramified with ramification index 2.

We have to consider four different cases: the case of K is Galois (case I), this implies $\kappa \neq 0$ (see Lemma 2), the case of K is not Galois and $\kappa \neq 0$ (case II), the case of $\kappa = 0$ and l is odd (case III) and at last the case of $\kappa = 0$ and l is even (case IV).

First we compute the genus g_L of L. By the Hurwitz-formula (Proposition 3) we obtain

$$\begin{aligned} 2g_L - 2 &= -6 + 2r_3 && \text{(case I)},\\ 2g_L - 2 &= -12 + 5r_6 + 4r_3 + 3r_2 && \text{(case II)},\\ 2g_L - 2 &= -9 + 5r_6 + 4r_3 + 3r_2 && \text{(case III)},\\ 2g_L - 2 &= -12 + 5r_6 + 4r_3 + 3r_2 && \text{(case IV)}.\end{aligned}$$

In view of Corollary 1 we have to compute the quantity $|\mathcal{V}|$, where $\mathcal{V}$ is the set of valuations such that $\gamma_{1,2,3}, \gamma_{2,3,1}$ and $\gamma_{3,1,2}$ do not have the same valuation. Obviously

$$\begin{aligned}\mathcal{V} \subset \mathcal{V}' &:= \{\nu \,:\, \nu(\gamma_{1,2,3}\gamma_{2,3,1}\gamma_{3,1,2}) \neq 0\} \cup \{\nu \,:\, \nu|\infty\}\\ &= \{\nu \,:\, \nu(\hat{\delta}) \neq 0\} \cup \{\nu \,:\, \nu|\infty\}.\end{aligned}$$

Let us consider case I. Since the finite part of $\mathcal{V}'$ are those primes (valuations) that divide $\hat{\delta}_K = d_K R^2$ we have $|\mathcal{V}'| = r_3 + 2r + 3$, where

$$d_K = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 = \prod_{g=1}^{r_3}(T - a_{g,3})^2.$$

Now we investigate the other three cases. The finite parts of the $\mathcal{V}'$'s are the same, so we have essentially only one case. We obtain in any case $|\mathcal{V}'_0| \leq r_6 + 2r_3 + 3r_2 + 6r$, where $\mathcal{V}'_0$ denotes the finite part of $\mathcal{V}'$. In order to obtain $|\mathcal{V}'|$, we have to add 6 or 3 or 6 according to the different cases.

Now we apply Mason's fundamental lemma (Corollary 1) and obtain:

$$\begin{aligned} H_L\left(\frac{\gamma_{1,2,3}}{\gamma_{2,3,1}}\right) &\leq 3(r_3 + r - 1) && \text{(case I)},\\ H_L\left(\frac{\gamma_{1,2,3}}{\gamma_{2,3,1}}\right) &\leq 6(r_6 + r_3 + r_2 + r - 1) && \text{(case II, III, IV)},\end{aligned}$$

where H_L denotes the height of elements in L.

Next we want to obtain an upper bound for $H_L\left(\frac{\beta_1}{\beta_2}\right)$. Let us denote by

$$H_a(\alpha) := -\sum_{\omega|\nu_a} \min(0, \omega(\alpha)), \quad a \in \mathbb{C} \cup \{\infty\}$$

the local height. Obviously, we have

$$H_L(\alpha) = \sum_{a \in \mathbb{C}\cup\{\infty\}} H_a(\alpha). \tag{14}$$

Using notation (14) we obtain

$$\begin{aligned} H_L\left(\frac{\gamma_{1,2,3}}{\gamma_{2,3,1}}\right) &= \sum_{\nu_a \in \mathcal{V}_0} H_a\left(\frac{\alpha_{2,3}}{\alpha_{3,1}}\right) + H_\infty\left(\frac{\gamma_{1,2,3}}{\gamma_{2,3,1}}\right)\\ &\geq H_\infty\left(\frac{\beta_1}{\beta_2} \cdot \frac{\alpha_{2,3}}{\alpha_{3,1}}\right)\\ &\geq H_\infty\left(\frac{\beta_1}{\beta_2}\right) - H_\infty\left(\frac{\alpha_{2,3}}{\alpha_{3,1}}\right).\end{aligned} \tag{15}$$

Now we have to estimate the quantity $H_L(\alpha_{2,3}/\alpha_{3,1})$. In order to get good estimates we have to consider the normal closure and compute some valuations. Since we know the valuation of α, it is easy to compute table 3. Note that if K is Galois σ_2, σ_4 and σ_6 are not elements of the Galois group of K and should not be considered in that case.

TABLE 3. Valuations of the relevant quantities.

	$\sigma_1:$ $\alpha_1-\alpha_2 \mapsto \alpha_1-\alpha_2$	$\sigma_2:$ $\alpha_1-\alpha_2 \mapsto \alpha_1-\alpha_3$	$\sigma_3:$ $\alpha_1-\alpha_2 \mapsto \alpha_2-\alpha_3$	$\sigma_4:$ $\alpha_1-\alpha_2 \mapsto \alpha_2-\alpha_1$	$\sigma_5:$ $\alpha_1-\alpha_2 \mapsto \alpha_3-\alpha_1$	$\sigma_6:$ $\alpha_1-\alpha_2 \mapsto \alpha_3-\alpha_2$
α_1	$-l$	$-l$	$-k$	$-k$	$l+k$	$l+k$
α_2	$-k$	$l+k$	$l+k$	$-l$	$-l$	$-k$
α_3	$l+k$	$-k$	$-l$	$l+k$	$-k$	$-l$
$\alpha_1-\alpha_2$	$-l$	$-l$	$-k$	$-l$	$-l$	$-k$
$\alpha_2-\alpha_3$	$-k$	$-k$	$-l$	$-l$	$-l$	$-l$
$\alpha_3-\alpha_1$	$-l$	$-l$	$-l$	$-k$	$-k$	$-l$

Now we find from tables 2 and 3

$$H_L\left(\frac{\alpha_{2,3}}{\alpha_{3,1}}\right) \le l-k \qquad \text{(case I)},$$

$$H_L\left(\frac{\alpha_{2,3}}{\alpha_{3,1}}\right) \le 2l-2k \qquad \text{(case II)},$$

$$H_L\left(\frac{\alpha_{2,3}}{\alpha_{3,1}}\right) \le 3l \qquad \text{(case III, IV)}.$$

Next we are going to prove that $\frac{2}{3}H_L\left(\frac{\beta_1}{\beta_2}\right) \ge H_L(\beta_1)$. We consider only the cases II, III and IV, for which the proofs are the same. The proof of case I is similar. Since $\beta_1 \in K$ we may assume

$$(\beta_1) = b_1\infty_1 + b_1\infty_2 + b_2\infty_3 + b_2\infty_4 + b_3\infty_5 + b_3\infty_6,$$

where the valuations ∞_i are indicated by the σ_i given by table 3. Then

$$(\beta_2) = b_2\infty_1 + b_3\infty_2 + b_3\infty_3 + b_1\infty_4 + b_1\infty_5 + b_2\infty_6,$$

and furthermore

$$\begin{aligned}(\beta_1/\beta_2) =&(b_1-b_2)\infty_1 + (b_1-b_3)\infty_2 + (b_2-b_3)\infty_3 + (b_2-b_1)\infty_4\\ &+ (b_3-b_1)\infty_5 + (b_3-b_2)\infty_6.\end{aligned}$$

Let us assume $b_1 > 0 \ge b_2 \ge b_3$ (all other cases run the same way, since we have $H_L(\beta_1) = 2\max_i |b_i|$). We have $b_1 = -b_2 - b_3$ and $-b_3 \ge \frac{1}{2}b_1$, since β_1 is a unit in $\mathcal{O}_K$. We also know that $H_L(\beta_1) = 2b_1$ and $H_L\left(\frac{\beta_1}{\beta_2}\right) = 2b_1 - 2b_3 \ge 3b_1 = \frac{3}{2}H_L(\beta_1)$.

The cases II, III and IV yield $H_L(\beta_1) = 2H_K(\beta_1)$. Therefore we obtain

$$\begin{aligned}H_K(\beta_1) \le&2(r_3+r-1) + \tfrac{2}{3}l - \tfrac{2}{3}k &&\text{(case I)},\\ H_K(\beta_1) \le&2(r_6+r_3+r_2+r-1) + \tfrac{2}{3}l - \tfrac{2}{3}k &&\text{(case II)},\\ H_K(\beta_1) \le&2(r_6+r_3+r_2+r-1) + l &&\text{(case III, IV)}.\end{aligned} \tag{16}$$

From (12), (13) and (16) we find:

Lemma 6. *If K is Galois we have $H_K(\beta_1) < 7l$ and $H_K(\beta_1) < 31l$ if K is not Galois. In the case of $\kappa = 0$ we have $H_K(\beta_1) < 22l$. If we assume $34 \deg \kappa < \deg \lambda$, then we obtain the following improvements: If K is Galois, then $H_K(\beta_1) < 5l$. In the non-Galois case we obtain $H_K(\beta_1) < 25l$.*

Proof. The lemma follows from the following inequalities:

$$\begin{aligned} H_K(\beta_1) \leq& 2(r_3 + r - 1) + \frac{2}{3}l - \frac{2}{3}k = 2r_3 + 2r - 2 + \frac{2}{3}l - \frac{2}{3}k \\ =& \deg \tilde{\delta}_L - 2 + \frac{2}{3}l - \frac{2}{3}k = 4l + 2k + \frac{2}{3}l - \frac{2}{3}k \qquad \text{(case I)}, \\ H_K(\beta_1) \leq& 2(r_6 + r_3 + r_2 + r - 1) + \frac{2}{3}l - \frac{2}{3}k \\ \leq& \deg \tilde{\delta}_L - 2 + \frac{2}{3}l - \frac{2}{3}k = 24l + 6k + \frac{2}{3}l - \frac{2}{3}k \qquad \text{(case II)}, \\ H_K(\beta_1) \leq& 2(r_6 + r_3 + r_2 + r - 1) + l \\ \leq& \deg \tilde{\delta}_L - 2 + l = 22l - 2 < 22l \qquad \text{(case III, IV)}. \end{aligned}$$

□

6. Proof of theorem 1 and theorem 3

We start with the proof of Theorem 1. First let us assume that κ is not a constant. From Lemma 6 we know $H_K(\beta_1) < 31l$. We also know that $\beta_1 = \varepsilon \eta_1^{a_1} \eta_2^{a_2}$, with $a_1, a_2 \in \mathbb{Z}$, $\eta_1 = \alpha_1$, $\eta_2 = \alpha_1 - \kappa$ and $\varepsilon \in \mathbb{C}^*$. This yields

$$(\beta_1) = -(a_1 + a_2)l\infty_1 + ((a_2 - a_1)k + a_2 l)\infty_2 + ((a_1 - a_2)k + a_1 l)\infty_3.$$

Therefore $31l > H_K(\beta_1) \geq l \max\{|a_1 + a_2|, |a_1|, |a_2|\}$, hence $30 \geq \max\{|a_1 + a_2|, |a_1|, |a_2|\}$. This yields 2791 possibilities for (a_1, a_2). We compute for every possibility the quantity β_1 in the form of $X_0 + X_1\alpha_1 + X_2\alpha_1^2$. It is clear that β_1 yields a solution, namely $(X_0, -X_1)$, to (2), if and only if $X_2 = 0$.

Unconditionally $X_2 = 0$, if and only if $(a_1, a_2) \in \mathcal{E}$, with

$$\mathcal{E} := \{(-1, -1), (0, 0), (1, 0), (0, 1)\}.$$

From these β's we obtain the trivial solutions. The strategy to prove that there are essentially only trivial solutions is to prove for every possible β that X_2 does not vanish (with only some possible exceptions). Let us consider X_2 as a polynomial in λ and κ. We use following simple criterion to exclude some X_2's. Let us consider the following degree function $\widehat{\deg} P := \deg_\lambda P + \deg_\kappa P$, where $\deg_\kappa P$ resp. $\deg_\lambda P$ denotes the degree of P considered as a polynomial in κ and λ. Let M_1 and M_2 be two monomials of P we write $M_1 \overset{*}{>} M_2$ if $\widehat{\deg} M_1 > \widehat{\deg} M_2$ or

$\widehat{\deg} M_1 = \widehat{\deg} M_2$ and $\deg_\lambda M_1 > \deg_\lambda M_2$. If the largest monomial M with respect to $\overset{*}{>}$ has maximal λ-exponent, then P cannot be zero. Indeed M is the unique monomial which has maximal degree in T, since we assume $\deg \lambda > \deg \kappa > 0$. Using this criterion for $P = X_2$ there remain only 392 exponents (a_1, a_2). Let us pick out the exponents $(4, -1)$ and $(-1, 4)$, for which we find $X_2 = \lambda + 2\kappa - \kappa^4$ respectively $X_2 = \lambda - 3\kappa - \kappa^4$. These values yield the "sporadic" solutions stated in Conjecture 1. Furthermore, we pick out the exponents $(5, -1)$ and $(-1, 5)$, for which $X_2 = \lambda^2 + 2\lambda\kappa + 3\kappa^2 - \kappa^5$ respectively $X_2 = \lambda^2 - 4\lambda\kappa + 6\kappa^2 + \kappa^5$. We want to prove that in these two cases $X_2 = 0$ is not possible.

Lemma 7. *The equations*

$$X^2 + 2XY + 3Y^2 - Y^5 = 0$$

and

$$X^2 - 4XY + 6Y^2 + Y^5 = 0$$

do not have a solution $(X, Y) \in \mathbb{C}[T]^2$, such that X is not a constant.

Proof. Put $X + Y = Z$ respectively $X - 2Y = Z$, then we have to show that $Z^2 = Y^5 - Y^2$ respectively $Z^2 = -Y^5 - 2Y^2$ has only constant solutions. Because of a theorem of Mason [13] (see Lemma 3) we can easily show that $H(Z) \leq 0$ in both cases. Therefore Z is a constant, hence also Y is a constant. Since $X = Z - Y$ resp. $X = Z + 2Y$ also X is a constant, which yields the lemma. Not that instead of Mason's theorem we could also apply a theorem of Ribenboim [16]. $\square$

In order to proof Conjecture 1 we have to show that the 388 remaining equations arising from $X_2 = 0$ have only constant solutions. The author could only solve the 4 cases stated above.

Let us prove the second statement of Theorem 1. Note that each exponent (a_1, a_2) yields for fixed κ and λ at most three solutions. Indeed one receives from one solution all other solutions by multiplying this solution by the third roots of ξ. So we are reduced to determine how many λ's exist that yield solutions, if κ is fixed. We want to count the number of solutions of the 388 remaining equations. Since one equation has at most $\deg_\lambda X_2$ solutions, provided κ is fixed we add the degrees of all 388 possibilities and obtain that there are at most 5482 different λ's. Adding the two possibilities that we gain from the exponents $(4, -1)$ and $(-1, 4)$ we have at most 5484 different λ's and therefore at most 16452 non-trivial solutions.

Now let us prove that there are only trivial solutions if $\deg \lambda > 34 \deg \kappa$. Lemma 6 and a similar argument as above yields that only exponents (a_1, a_2) with $\max\{|a_1|, |a_2|, |a_1 + a_2|\} \leq 24$ yield solutions to (2). Let us modify the degree argument given above, by using the weighted degree function $\widehat{\deg} P := 34 \deg_\lambda P + \deg_\kappa P$ instead. Now the criterion that the largest monomial has maximal λ exponent together with the assumption $\deg \lambda > 34 \deg \kappa$ yields that this monomial has unique maximal degree, with respect to T and therefore X_2 cannot be zero. A short computation on a computer shows that this criterion is always fulfilled for all 1801 possibilities and therefore we have proved the first part of Theorem 1.

Now we consider the case of $\kappa \in \mathbb{C}^*$. The quantity X_2 considered as polynomial in κ and λ may only vanish if there is either no monomial or at least two monomials for each power of λ. Checking all possibilities we are left to 48 cases. Next we check whether the constant term, the coefficients of λ and λ^2 can vanish simultaneously. This yields that $(a_1, a_2) \in \mathcal{E}$, where

$$\mathcal{E} := \{(-1,-1), (-1,3), (0,0), (0,1), (1,0), (3,-1)\}.$$

These exponents only yield the trivial solutions and the 6 exceptions listed in table 1.

Now we prove Theorem 3. The argument is the same but easier, because we have only one exponent to keep track of. We know β_1 is a unit and therefore $\beta_1 = \varepsilon \alpha_1^{a_1}$ (see Proposition 4), with $\varepsilon \in \mathbb{C}^*$. If we combine this result with Lemma 6 we obtain

$$22l > H_K(\beta_1) = |a_1| l,$$

and therefore $|a_1| \leq 21$. We compute each possible $\beta_1 = X_0 + X_1\alpha_1 + X_2\alpha_1^2$. Of course β_1 yields a solution if and only if $X_2 = 0$. Unconditionally $X_2 = 0$ if $a_1 \in \{-2, 0, 1\}$. These values for a_1 yield the trivial solutions. We have to prove that there are no further possibilities for X_2 to vanish. A close look on the other X_2 shows that they are polynomials only in λ and so $X_2 = 0$ is impossible, since λ is not a constant.

7. Proof of theorem 4

Since there is no analog of Dirichlet's unit theorem for function fields we only know that the unit group of $\mathcal{O}_K$ has rank at most 2. Since we have found one non-constant unit we know that the rank is at least 1. In the case of rank 1 the proof of Theorem 4 is the same as the proof of Theorem 3, and we obtain only 9 different solutions. Indeed α generates the unit group since the log-function defined in section maps $\mathbb{C}[T,\alpha]^*$ on a line through $\log(\alpha) = (-l, l/2)$ and $(0,0)$. But $\log(\alpha)$ would be the smallest element on that line that lies inside (11).

Now let us assume the rank of the unit group is 2. As stated in the paragraph above $\alpha_1 \neq \eta^k$ for any unit $\eta \in \mathbb{C}[T,\alpha_1]^*$ and $|k| > 1$. Therefore we can write $\beta_1 = \varepsilon \alpha_1^{a_1} \eta^{a_2}$, where $\varepsilon \in \mathbb{C}^*$, α_1 and η are a system of fundamental units and $a_1, a_2 \in \mathbb{Z}$. We reduce this counting problem to a problem of counting lattice points in a domain. Since β_1 is a unit we map β_1 to the plane $\mathbb{R}^2$ using the log function, defined in section 4. We know that the units form a lattice $\Lambda \subset \mathbb{Z}^2$. Furthermore we know that no lattice point lies in the open domain $\mathcal{A}$ given by (11). Since $\mathcal{A}$ is not convex we consider the convex domain $\mathcal{D} := \{(e_1, e_2) : \max\{|e_1|, |e_2|\} < l/2\} \subset \mathcal{A}$. By Minkowski's famous theorem we know that the lattice constant of Λ is at least $l^2/4$, since $|\mathcal{D}| = l^2$, where $|\mathcal{D}|$ denotes the area of $\mathcal{D}$. In order to proof Theorem 4 we have to estimate the number of lattice points of Λ lying in the domain

$$\mathcal{S} := \begin{cases} |e_1 + e_2| < 22l & \text{if } \operatorname{sign} e_1 = \operatorname{sign} e_2, \\ \max\{|e_1|, |e_2|\} < 22l & \text{if } \operatorname{sign} e_1 \neq \operatorname{sign} e_2. \end{cases}$$

Let us consider the domain

$$\mathcal{S}' := \begin{cases} |e_1 + e_2| < (22 + 1/4)l & \text{if } \operatorname{sign} e_1 = \operatorname{sign} e_2, \\ \max\{|e_1|, |e_2|\} < (22 + 1/4)l & \text{if } \operatorname{sign} e_1 \neq \operatorname{sign} e_2. \end{cases}$$

Then every domain $\frac{1}{2}\mathcal{D} + \omega$ such that $\omega \in \Lambda \cap \mathcal{S}$ is contained in $\mathcal{S}'$. Since all $\frac{1}{2}\mathcal{D} + \omega$ are disjoint, we have

$$\sharp\{\omega : \omega \in \Lambda \cap \mathcal{S}\} \left| \frac{1}{2}\mathcal{D} \right| \leq |\mathcal{S}'|,$$

hence

$$\sharp\{\omega : \omega \in \Lambda \cap \mathcal{S}\} \leq \frac{3(22 + 1/4)^2 l^2}{(l/2)^2} = 5940.75.$$

Therefore we have only 5940 possibilities for the exponents (a_1, a_2) of β_1. Obviously exponents of the form $(a_1, 0)$ yield only solutions that appear in the case of $l \equiv 1 \pmod 2$. Since in this case we only have trivial solutions, we may exclude the 43 possibilities given by $(a_1, 0)$. So we are left to 5897 possibilities. Since every pair of exponents yields at most three solutions we have proved Theorem 4.

Acknowledgment

The author wants to thank Clemens Heuberger and Günther Lettl for many helpful suggestions. The author also wants to thank the referee for many helpful suggestions, in particular on the proof of Lemma 4 and Proposition 4. The author also wants to thank Guy Barat for his help with the French abstract.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers. I, II, III.* Mathematika **13** (1966), 204–216; ibid. **14** (1967), 102–107; ibid. **14** (1967), 220–228.

[2] A. Baker, *Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms.* Philos. Trans. Roy. Soc. London Ser. A **263** (1967/1968), 173–191,

[3] A. Baker, *Linear forms in the logarithms of algebraic numbers. IV.* Mathematika **15** (1968), 204–216.

[4] P. M. Cohn, *Algebraic numbers and algebraic functions.* Chapman and Hall Mathematics Series. Chapman & Hall, London, 1991.

[5] C. Fuchs, V. Ziegler, *On a family of Thue equations over function fields.* Monatsh. Math. **147** (2006), 11–23.
[6] C. Fuchs, V. Ziegler, *Thomas' family of Thue equations over function fields.* Quart. J. Math. **57** (2006), 81–91.
[7] B. P. Gill, *An analogue for algebraic functions of the Thue-Siegel theorem.* Ann. of Math. (2) **31(2)** (1930), 207–218.
[8] C. Heuberger, *On a conjecture of E. Thomas concerning parametrized Thue equations.* Acta. Arith. **98** (2001), 375–394.
[9] S. Lang, *Elliptic curves: Diophantine analysis.* Volume **231** of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1978.
[10] E. Lee, *Studies on Diophantine Equations.* PhD thesis, Cambridge University, 1992.
[11] G. Lettl, *Thue equations over algebraic function fields.* Acta Arith. **117(2)** (2005), 107–123.
[12] R. C. Mason, *On Thue's equation over function fields.* J. London Math. Soc. (2) **24(3)** (1981), 414–426.
[13] R. C. Mason, *The hyperelliptic equation over function fields.* Math. Proc. Camb. Philos. Soc. **93** (1983), 219–230.
[14] R. C. Mason, *Diophantine equations over function fields.* Volume **96** of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1984.
[15] M. Mignotte, N. Tzanakis, *On a family of cubics.* J. Number Theory **39(1)** (1991), 41–49.
[16] P. Ribenboim, *Remarks on existentially closed fields and diophantine equations.* Rend. Sem. Mat. Univ. Padova **71** (1984), 229–237.
[17] M. Rosen, *Number theory in function fields.* Volume **210** of Graduate Texts in Mathematics. Springer-Verlag, New York, 2002.
[18] W. M. Schmidt, *Thue's equation over function fields.* J. Austral. Math. Soc. Ser. A **25(4)** (1978), 385–422.
[19] E. Thomas, *Solutions to certain families of Thue equations.* J. Number Theory **43(3)** (1993), 319–369.
[20] A. Thue, *Über Annäherungswerte algebraischer Zahlen.* J. Reine und Angew. Math. **135** (1909), 284–305.
[21] E. Wirsing, *Approximation mit algebraischen Zahlen beschränkten Grades.* J. Reine Angew. Math. **206** (1960), 67–77.
[22] V. Ziegler, *On a family of Cubics over Imaginary Quadratic Fields.* Period. Math. Hungar. **51(2)** (2005), 109–130.

Volker Ziegler
Institute of Analysis and Computational Number Theory
Technische Universität Graz
Steyrergasse 30, A-8010 Graz, Austria
E-mail: ziegler@finanz.math.tugraz.at