ACTA ARITHMETICA
117.2 (2005)

Thue equations over algebraic function fields

by

Günter Lettl (Graz)

1. Introduction. It is well known that over a ring R, which is finitely generated over $\mathbb{Z}$, a Thue equation has only finitely many solutions in R (see e.g. [6, Chap. 8.4]). In principle, this can be shown by the original ideas of A. Thue. By an application of Baker's method, this result was made effective by K. Győry ([5, §2.3]).

On the other hand, these methods do not apply to rings whose unit group is not finitely generated, e.g. to polynomial rings over an infinite field. If R is a holomorphy ring of a function field K of characteristic 0 (i.e. the ring of S-integers for some finite set S of places), using methods developed by C. F. Osgood [11], W. M. Schmidt [13] established an effective bound for the height of the solutions of a Thue equation in R. Soon afterwards R. C. Mason [9], [10] strengthened this result and showed that all solutions of a Thue equation can be determined effectively. He analyzed the case of an infinite set of solutions, supposing that the binary form splits into linear factors over the function field under consideration and that the constant field is algebraically closed.

From the viewpoint of algebraic geometry, the results of Yu. I. Manin [8] and H. Grauert [4] on Mordell's conjecture over function fields imply that any Thue equation defining a curve of genus $g \geq 2$ (i.e. any Thue equation of degree $n \geq 4$) has only finitely many solutions in $K \times K$—as far as the curve cannot be defined over a constant field.

It is the aim of the present paper to investigate the set of solutions in just this exceptional case. On the one hand we impose an integrality condition (i.e. restrict to S-integral solutions), on the other hand most of our results hold for Thue equations of degree $n \geq 3$.

In principle, we follow Mason's ideas and adapt them to our more general situation. For a Thue equation $F(X,Y) = b$ we will define a set $\mathcal{L}$ of *special* solutions, and first show that there exist only finitely many solu-

2000 *Mathematics Subject Classification*: Primary 11R58; Secondary 11D59, 14G05, 14H05.

tions outside $\mathcal{L}$ (Proposition 3) and that a nonempty set $\mathcal{L}$ already implies that $F(X,Y)=b$ can be transformed into a Thue equation with constant coefficients (Proposition 4(b)). Using Faltings's theorem on Mordell's conjecture [3] we deduce that in case the constant field is a finite extension of $\mathbb{Q}$, any Thue equation of degree $n\geq 4$ has only finitely many solutions (Corollary 1(b)).

In what follows we obtain conditions for the finiteness of the solution set, which are independent of b and of constant field extensions (Corollary 2), or which are independent of K (Corollary 3). Over the splitting field of $F(X,Y)$ we give a complete description of the set $\mathcal{L}$ of special solutions (Corollary 4). In the last section we show how to construct cubic Thue equations with infinitely many solutions, supposing that the cubic form $F(X,Y)$ splits into linear factors, or is irreducible, resp., in $K[X,Y]$. So there are cubic Thue equations over $\mathbb{Q}(T)$ which have infinitely many solutions in $\mathbb{Q}[T]$, but (by the result mentioned at the beginning) only finitely many solutions in $\mathbb{Z}[T]$.

Finally, the author wants to thank E. Bombieri and K. Győry for very fruitful discussions about this topic, and A. Pethő for some quick and useful calculations concerning elliptic curves.

2. Notations and auxiliary results. We will use the notions and definitions as explained e.g. in the textbooks of H. Stichtenoth [16] or M. Rosen [12]. Throughout this paper let K be an algebraic function field in one variable over the field of constants K_0 of characteristic $\operatorname{char}(K_0)=0$, and let $g=g_K$ denote its genus.

A *place* P of K is the valuation ideal of a valuation ring $\mathcal{O}_P$ with $K_0\subset\mathcal{O}_P\subsetneqq K$; $v_P: K\to\mathbb{Z}\cup\{\infty\}$ denotes the normed, discrete valuation given by P, and $\deg P:=[\mathcal{O}_P/P:K_0]$ the degree of P. Let $\mathbb{P}_K$ denote the set of all places of K and $\operatorname{Div}(K)$ the group of divisors of K, i.e. the free abelian group generated by $\mathbb{P}_K$. For any divisor $D\in\operatorname{Div}(K)$, $\operatorname{supp}(D)\subset\mathbb{P}_K$ denotes the *support* of D, i.e. the set of all places occurring in D. For $u\in K^\times$ (1), let $(u)=(u)_0-(u)_\infty$ be the decomposition of the divisor of the function u into its divisor of zeroes and poles, resp. For a nonempty, finite set of places $S\subset\mathbb{P}_K$ put

$$\mathfrak{o}:=\mathfrak{o}_{K,S}=\{x\in K\mid v_P(x)\geq 0\text{ for all }P\notin S\}\subset K,$$

the ring of S-integers of K.

We recall two fundamental arithmetical results for function fields, the second of which we will apply to Thue equations in a well known way. Proposition 1 is the ABC-theorem for function fields, as proved e.g. in [12, Theorem 7.17], or under more special suppositions already in [10, Lemma 2

(1) For any ring R (commutative, with 1) we denote its group of units by $R^\times$.

on p. 14]. Proposition 2 is the theorem on S-unit equations for function fields—and indeed a direct consequence of Proposition 1, which again can be found in [12, Theorem 7.19] or [10, Corollary on p. 15]. Be aware that both results require a perfect constant field, and that Proposition 2 only holds for separable solutions (i.e. $K/K_0(u)$, $K/K_0(v)$ are both separable).

PROPOSITION 1. *Let $u, v \in K^\times$ with $u + v = 1$ and put $A = (u)_0$, $B = (v)_0$, $C = (u)_\infty = (v)_\infty$. Then*

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

The max in Proposition 1 is only needed to cover the case where u and v are constants and $g_K = 0$.

PROPOSITION 2. *For any nonempty, finite set of places $S' \subset \mathbb{P}_K$ of K there exist only finitely many $(u, v) \in (\mathfrak{o}_{K,S'}^\times \setminus K_0)^2$ with $u + v = 1$.*

For any extension field L/K let $L_0 = \{x \in L \mid x \text{ is algebraic over } K_0\}$ denote the constant field of L.

3. Thue equations over K. As above, $\mathfrak{o}$ denotes the ring of S-integers of the function field K with constant field K_0. We choose an algebraic closure $\overline{K}$ of K and denote the algebraic closure of K_0 inside $\overline{K}$ by $\overline{K}_0$. For $n \geq 3$ let

$$F = F(X, Y) = X^n + a_1 X^{n-1} Y + \cdots + a_{n-1} X Y^{n-1} + a_n Y^n \in \mathfrak{o}[X, Y]$$

be a normed, binary form of degree n (not necessarily irreducible) such that $F(X, 1)$ has no multiple roots in $\overline{K}$. We are interested in the solutions of the Thue equation

$$F(X, Y) = b \tag{1}$$

over $\mathfrak{o}$, where $0 \neq b \in \mathfrak{o}$. Obviously, if b and all coefficients of F are in K_0 and K_0 is algebraically closed, then (1) has infinitely many solutions in $K_0 \subset \mathfrak{o}$.

Let $L \subset \overline{K}$ be the splitting field of $F(X, 1)$ over K and $\mathfrak{O} \subset L$ be the integral closure of $\mathfrak{o}$ in L. Thus F splits over L into linear factors

$$F(X, Y) = \prod_{i=1}^{n} (X - \alpha_i Y)$$

with pairwise different $\alpha_i \in \mathfrak{O}$. Put

$$S' = \big\{P' \in \mathbb{P}_L \,\big|\, P' \mid P \text{ for some } P \in S \text{ or } P' \mid (b)_0 + (\operatorname{disc} F(X, 1))_0\big\},$$

the set of all places of L lying over S or occurring as zeroes of b or of the discriminant of $F(X, 1)$, and $\mathfrak{O}_{S'} := \mathfrak{o}_{L,S'}$.

For any solution $(x,y)\in\mathfrak{o}^2$ of (1) we put, for pairwise different indices $i,j,l\in\{1,\ldots,n\}$,

$$\begin{aligned}\beta_i(x,y)&=x-\alpha_i y,\\ \gamma_{i,j,l}(x,y)&=\beta_i(x,y)(\alpha_j-\alpha_l)=(x-\alpha_i y)(\alpha_j-\alpha_l),\\ \delta_{i,j,l}(x,y)&=\frac{\gamma_{i,j,l}(x,y)}{\gamma_{j,l,i}(x,y)}.\end{aligned}$$

From $0\neq b=\prod_{i=1}^n\beta_i(x,y)$ we obtain $0\neq\beta_i(x,y)\in\mathfrak{O}$, and furthermore $\beta_i(x,y)$, $\gamma_{i,j,l}(x,y)$ and $\delta_{i,j,l}(x,y)$ all belong to $\mathfrak{O}_{S'}^{\times}$. It is immediate to check that

$$\gamma_{i,j,l}(x,y)+\gamma_{j,l,i}(x,y)+\gamma_{l,i,j}(x,y)=0,$$

which usually is called *Siegel's identity* and from which we deduce

$$(2)\qquad -1=\delta_{i,j,l}(x,y)+\delta_{j,l,i}(x,y)^{-1}=\delta_{i,j,l}(x,y)+\delta_{l,j,i}(x,y).$$

The set of *special* solutions of (1), defined by

$$\begin{aligned}\mathcal{L}=\{(x,y)\in\mathfrak{o}^2\mid F(x,y)=b,\ &\text{and}\\ &\text{for all pairwise different } 1\le i,j,l\le n,\ \delta_{i,j,l}(x,y)\in L_0\},\end{aligned}$$

will play a central role in our investigations. It is well known and very easy to derive from Proposition 2 that there are only finitely many solutions of (1) outside $\mathcal{L}$.

PROPOSITION 3. *There are only finitely many $(x,y)\in\mathfrak{o}\times\mathfrak{o}$ with $F(x,y)=b$ and $(x,y)\notin\mathcal{L}$.*

Proof. Let (x,y) be any such solution, so $\delta_{i,j,l}(x,y)\in\mathfrak{O}_{S'}^{\times}\setminus L_0$ for some i,j,l and from (2) we have

$$1=-\delta_{i,j,l}(x,y)-\delta_{l,j,i}(x,y).$$

By Proposition 2, this equation has only finitely many solutions $\delta_{i,j,l}(x,y)\in\mathfrak{O}_{S'}^{\times}\setminus L_0$. On the other hand, $\delta_{i,j,l}(x,y)$ uniquely determines x/y by

$$\delta_{i,j,l}(x,y)\,\frac{\alpha_l-\alpha_i}{\alpha_j-\alpha_l}=\frac{x/y-\alpha_i}{x/y-\alpha_j}.$$

From $y^n=b\,F(x/y,1)^{-1}$ we see that for given x/y there exist at most n solutions of (1), thus for any triple of indices we get only finitely many solutions (x,y) with $\delta_{i,j,l}(x,y)\notin L_0$. ∎

From Proposition 3 we see that (1) has finitely many solutions if and only if $\mathcal{L}$ is finite. On the other hand, Proposition 4(b) below will show that whenever we have $\mathcal{L}\neq\emptyset$, (1) can be transformed into a Thue equation over the constant field L_0.

PROPOSITION 4. *Suppose that $\mathcal{L}\neq\emptyset$. Then:*

(a) *There exists a divisor* $A \in \mathrm{Div}(L)$ *of a function in* $\mathfrak{O}$ *such that for any choice of* $j_i \in \{2, \ldots, n\} \setminus \{i\}$, $2 \leq i \leq n$, *and for any solution* $(x, y) \in \mathcal{L}$ *one has*

(i) $n \cdot A = \left(b \, \frac{(\alpha_{j_2} - \alpha_1)(\alpha_{j_3} - \alpha_1) \cdots (\alpha_{j_n} - \alpha_1)}{(\alpha_2 - \alpha_{j_2})(\alpha_3 - \alpha_{j_3}) \cdots (\alpha_n - \alpha_{j_n})} \right)$,

(ii) $(\beta_1(x, y)) = A =: A_1$,
$(\beta_i(x, y)) = A + (\alpha_i - \alpha_{j_i}) - (\alpha_{j_i} - \alpha_1) =: A_i$,

(iii) *for any pairwise different* $1 \leq i, j, l \leq n$,

$$(\gamma_{i,j,l}(x, y)) = A_i + (\alpha_j - \alpha_l) = A_j + (\alpha_l - \alpha_i) = (\gamma_{j,l,i}(x, y)).$$

(b) *For any fixed solution* $(x, y) \in \mathcal{L}$, *the substitution*

$$\begin{aligned} X &= -C_1 \, \frac{\beta_1(x, y)\alpha_2}{\alpha_1 - \alpha_2} + C_2 \, \frac{\beta_2(x, y)\alpha_1}{\alpha_1 - \alpha_2}, \\ Y &= -C_1 \, \frac{\beta_1(x, y)}{\alpha_1 - \alpha_2} + C_2 \, \frac{\beta_2(x, y)}{\alpha_1 - \alpha_2}, \end{aligned} \tag{3}$$

transforms the Thue equation (1) *into the Thue equation in the variables* C_1, C_2,

$$G(C_1, C_2) := C_1 C_2 \prod_{j=3}^{n} (-1)(\delta_{1,j,2}(x, y) C_1 + \delta_{2,j,1}(x, y) C_2) = 1 \tag{4}$$

with coefficients in the constant field L_0.

Proof. (a) Fix $(x, y) \in \mathcal{L}$ and put $A_i = (\beta_i(x, y)) \in \mathrm{Div}(L)$. From

$$\delta_{i,j,l}(x, y) = \frac{\beta_i(x, y)(\alpha_j - \alpha_l)}{\beta_j(x, y)(\alpha_l - \alpha_i)} \in L_0^{\times}$$

we deduce $A_i + (\alpha_j - \alpha_l) = A_j + (\alpha_l - \alpha_i)$, and in particular for $j = 1$, $2 \leq i \leq n$ and $l = j_i \in \{2, \ldots, n\} \setminus \{i\}$,

$$A_i + (\alpha_1 - \alpha_{j_i}) = A_1 + (\alpha_{j_i} - \alpha_i) \quad \text{and} \quad (\beta_i(x, y)) = A_1 + (\alpha_i - \alpha_{j_i}) - (\alpha_{j_i} - \alpha_1).$$

Using $b = \prod_{i=1}^{n} \beta_i(x, y)$, for the divisor of b we obtain

$$(b) = \sum_{i=1}^{n} (\beta_i(x, y)) = A_1 + \sum_{i=2}^{n} (A_1 + (\alpha_i - \alpha_{j_i}) - (\alpha_{j_i} - \alpha_1)),$$

thus

$$n \cdot A_1 = \left(b \, \frac{(\alpha_{j_2} - \alpha_1)(\alpha_{j_3} - \alpha_1) \cdots (\alpha_{j_n} - \alpha_1)}{(\alpha_2 - \alpha_{j_2})(\alpha_3 - \alpha_{j_3}) \cdots (\alpha_n - \alpha_{j_n})} \right).$$

Since $A := A_1$ is independent of the choice of $(x, y) \in \mathcal{L}$, all assertions immediately follow from the above calculations.

(b) From (3) we calculate

$$X - \alpha_i Y = \begin{cases} C_i \beta_i(x, y) & \text{for } i = 1, 2, \\ (-1)(\delta_{1,i,2}(x, y) C_1 + \delta_{2,i,1}(x, y) C_2) \beta_i(x, y) & \text{for } 3 \leq i \leq n \end{cases} \tag{5}$$

and obtain

$$\begin{aligned} b &= \prod_{i=1}^{n}(X-\alpha_i Y) \\ &= \prod_{i=1}^{n}\beta_i(x,y)\cdot C_1C_2\prod_{i=3}^{n}(-1)(\delta_{1,i,2}(x,y)C_1+\delta_{2,i,1}(x,y)C_2) \\ &= bG(C_1,C_2), \end{aligned}$$

which yields (4). ∎

Corollary 1. (a) *If $\mathcal{L}\neq\emptyset$, the inverse map of* (3) *defines an injection from $\mathcal{L}$ into*

$$\mathcal{L}_0=\{(c_1,c_2)\in L_0\times L_0 \mid G(c_1,c_2)=1\},$$

the set of solutions in $L_0\times L_0$ of the Thue equation (4).

(b) *If $[K_0:\mathbb{Q}]<\infty$ and $n\geq 4$ then* (1) *has only finitely many solutions in $\mathfrak{o}\times\mathfrak{o}$.*

Proof. (a) Fix any $(x,y)\in\mathcal{L}$ and note that (3) defines an automorphism of the vector space L^2 with determinant $\beta_1(x,y)\beta_2(x,y)\neq 0$. From Proposition 4(a)(ii) we see that for any solution $(\widetilde{x},\widetilde{y})\in\mathcal{L}$ we have $\beta_i(\widetilde{x},\widetilde{y})=c_i\beta_i(x,y)$ with some $c_i\in L_0^{\times}$. The calculations (5) show that (3) maps $(\widetilde{x},\widetilde{y})$ onto $(c_1,c_2)\in\mathcal{L}_0$.

(b) One checks easily that no linear factor of $G(C_1,C_2)$ is a constant multiple of another, thus (4) defines a smooth curve of genus $\binom{n-1}{2}\geq 2$ over the algebraic number field L_0. By Faltings's theorem on Mordell's conjecture (Satz 7 in [3]), $\mathcal{L}_0$ is finite, and by (a), $\mathcal{L}$ is finite as well. ∎

4. Further analysis of the solution set $\mathcal{L}$. In this section we will show that an infinite solution set $\mathcal{L}$ implies very restrictive conditions on (the right hand side b of) the Thue equation and on the splitting field L of $F(X,1)$ over K.

Proposition 5. *Suppose that* (1) *has infinitely many solutions in $\mathfrak{o}\times\mathfrak{o}$. Then for the splitting field L of $F(X,1)$ over K we have*

$$\begin{aligned} L &= KL_0 \\ &= K(\{\delta_{i,j,l}(x,y)\mid (x,y)\in\mathcal{L} \text{ and pairwise different } 1\leq i,j,l\leq n\}); \end{aligned}$$

i.e. L/K is a constant field extension.

As an immediate consequence of Proposition 5 we obtain

Corollary 2. *If $F(X,Y)$ has a nonlinear, irreducible factor in $\overline{K}_0K[X,Y]$ then the Thue equation* (1) *has only finitely many solutions in $\mathfrak{o}\times\mathfrak{o}$.*

Proof of Proposition 5. Put

$$K_\delta = K(\{\delta_{i,j,l}(x,y) \mid (x,y) \in \mathcal{L} \text{ and pairwise different } 1 \le i,j,l \le n\}),$$

so obviously $K \subset K_\delta \subset KL_0 \subset L$.

Assume that $K_\delta \subsetneq L$ and let $G_0 \le \mathrm{Gal}(L/K)$ denote the nontrivial Galois group of L/K_δ. We consider each element $\sigma \in \mathrm{Gal}(L/K)$ as a permutation of the indices of the roots of $F(X,1)$ via $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ for $1 \le i \le n$.

Now choose $\sigma \in G_0$ with $\sigma \ne \mathrm{id}$ and $i,j,l \in \{1,\ldots,n\}$ with $\sigma(i) \ne i$, $j \ne i, \sigma(i)$ and $l \ne i,j$. Since σ fixes each element of K_δ, we obtain, for all $(x,y) \in \mathcal{L}$,

$$\delta_{i,j,l}(x,y) = \sigma(\delta_{i,j,l}(x,y)) = \delta_{\sigma(i),\sigma(j),\sigma(l)}(x,y).$$

Abbreviating

$$0 \ne e_1 = \frac{\alpha_j - \alpha_l}{\alpha_l - \alpha_i} \quad \text{and} \quad 0 \ne e_2 = \frac{\alpha_{\sigma(j)} - \alpha_{\sigma(l)}}{\alpha_{\sigma(l)} - \alpha_{\sigma(i)}}$$

we get

$$\left(\frac{x}{y} - \alpha_i\right)\left(\frac{x}{y} - \alpha_{\sigma(j)}\right)e_1 = \left(\frac{x}{y} - \alpha_j\right)\left(\frac{x}{y} - \alpha_{\sigma(i)}\right)e_2.$$

Thus, for every $(x,y) \in \mathcal{L}$, x/y must be a zero of the polynomial

$$p = (X - \alpha_i)(X - \alpha_{\sigma(j)})e_1 - (X - \alpha_j)(X - \alpha_{\sigma(i)})e_2.$$

Since $p(\alpha_i) = -(\alpha_i - \alpha_j)(\alpha_i - \alpha_{\sigma(i)})e_2 \ne 0$, there are at most 2 possibilities for x/y, and arguing as in the proof of Proposition 3 we get $\#\mathcal{L} \le 2n$, contradicting our assumption. ∎

A second look at the above proof shows that one indeed obtains the following: If $\mathcal{L}$ is infinite then there exist infinitely many $(x',y') \in \mathcal{L}$ such that

$$L = K(\{\delta_{i,j,l}(x',y') \mid 1 \le i,j,l \le n \text{ pairwise different}\}).$$

LEMMA 1. *Let $I = \{1,\ldots,n\}$, fix any solution $(x,y) \in \mathcal{L}$ and put $\beta_i := \beta_i(x,y) = x - \alpha_i y \in \mathfrak{O}$ for all $i \in I$. Then the following assertions are equivalent*:

(i) *There exist $i,j \in I$ with $i \ne j$ such that $\beta_i/(\alpha_i - \alpha_j) \in \mathfrak{O}$.*

(ii) *For all $i,j \in I$ with $i \ne j$ we have $\beta_i/(\alpha_i - \alpha_j) \in \mathfrak{O}$.*

(iii) *There exists a $j \in I$ with $b/\big(\beta_j \frac{\partial F}{\partial X}(\alpha_j,1)\big) \in \mathfrak{O}$.*

(iv) *For all $j \in I$ we have $b/\big(\beta_j \frac{\partial F}{\partial X}(\alpha_j,1)\big) \in \mathfrak{O}$.*

Proof. Recall that for any pairwise different $i,j,l \in I$, $\delta_{i,l,j}(x,y) \in L_0^\times$ yields

$$\left(\frac{\beta_i}{\alpha_i - \alpha_j}\right) = \left(\frac{\beta_l}{\alpha_l - \alpha_j}\right) \in \mathrm{Div}(L). \tag{6}$$

(i)⇒(ii). Suppose that $\beta_i/(\alpha_i-\alpha_j)\in\mathfrak{O}$ and let $i'\neq j'\in I$.

If $j'=j$, then (6) with $l=i'$ yields $\beta_{i'}/(\alpha_{i'}-\alpha_{j'})\in\mathfrak{O}$.

If $j'\neq j$, then (6) with $l=j'$ yields $\beta_{j'}/(\alpha_{j'}-\alpha_j)\in\mathfrak{O}$, thus also $-\beta_{j'}/(\alpha_{j'}-\alpha_j)-y=\beta_j/(\alpha_j-\alpha_{j'})\in\mathfrak{O}$, and again using (6) we end up with $\beta_{i'}/(\alpha_{i'}-\alpha_{j'})\in\mathfrak{O}$.

(ii)⇒(iv)⇒(iii)⇒(i). From

$$(-1)^{n-1}\prod_{i,\,i\neq j}\frac{\beta_i}{\alpha_i-\alpha_j}=\frac{b}{\beta_j\,\frac{\partial F}{\partial X}(\alpha_j,1)}$$

we immediately obtain the first implication. The second one is trivial, and the third one also follows from the last formula, since all factors of the product have the same divisor by (6). ∎

Proposition 6. *If there exists a solution* $(x,y)\in\mathcal{L}$ *and indices* $1\le i\neq j\le n$ *such that*

$$\frac{\beta_i(x,y)}{\alpha_i-\alpha_j}\notin\mathfrak{O}$$

then $\#\mathcal{L}\le n$. *More precisely*, $\mathcal{L}\subset\{(\zeta^m x,\zeta^m y)\mid 1\le m\le n\}$, *where* $\zeta\in\overline{K}_0$ *denotes a root of unity of order* n.

Proof. Suppose that $\lambda:=\beta_i(x,y)/(\alpha_i-\alpha_j)\notin\mathfrak{O}$. Since

$$\frac{\beta_j(x,y)}{\alpha_i-\alpha_j}-\frac{\beta_i(x,y)}{\alpha_i-\alpha_j}=y\in\mathfrak{o},\tag{7}$$

also $\lambda':=\beta_j(x,y)/(\alpha_i-\alpha_j)\notin\mathfrak{O}$. Thus we can find a place $P\in\mathbb{P}_L$, not lying over a place of S, such that λ and λ' have a pole of the same order at P. Furthermore we see from (7) that the local expansions (with respect to some local parameter for P) of λ and λ' at P have the same leading coefficient.

For any further solution $(\widetilde{x},\widetilde{y})\in\mathcal{L}$, we have $\widetilde{x}-\alpha_i\widetilde{y}=c_i\beta_i(x,y)$ and $\widetilde{x}-\alpha_j\widetilde{y}=c_j\beta_j(x,y)$ with $c_i,c_j\in L_0^\times$, which yields $\widetilde{y}=c_j\lambda'-c_i\lambda\in\mathfrak{o}$. Considering again the leading coefficients of the local expansions at P we deduce that $c_i=c_j$, i.e.

$$1=\frac{c_i}{c_j}=\frac{\widetilde{x}/\widetilde{y}-\alpha_i}{\widetilde{x}/\widetilde{y}-\alpha_j}\cdot\frac{\beta_j(x,y)}{\beta_i(x,y)}.$$

So for any $(\widetilde{x},\widetilde{y})\in\mathcal{L}$ we obtain $\widetilde{x}/\widetilde{y}=x/y$, and from $\widetilde{y}^n=y^n=b/F(x/y,1)$ all assertions of Proposition 6 follow. ∎

Using

$$\prod_{j=1}^{n}\frac{b}{\beta_j(x,y)\,\frac{\partial F}{\partial X}(\alpha_j,1)}=\frac{b^{n-1}}{\operatorname{disc}F(X,1)}$$

and Lemma 1, we immediately obtain from Proposition 6:

COROLLARY 3. *If* $b^{n-1}/\operatorname{disc} F(X,1) \notin \mathfrak{o}$ *or* $b/\frac{\partial F}{\partial X}(\alpha_j,1) \notin \mathfrak{O}$ *for some* $1 \le j \le n$ *then* $\#\mathcal{L} \le n$.

REMARK. For example, the first condition of Corollary 3 is satisfied if $b \in \mathfrak{o}^\times$ (e.g. if b is a constant) and $\operatorname{disc} F(X,1)$ is not a unit in $\mathfrak{o}$.

As a partial converse to Proposition 6 we can deduce from Proposition 4 the following result for Thue equations which already split in the function field under consideration.

COROLLARY 4. *Suppose that* F *splits in* $K[X,Y]$ *into linear factors* (*i.e.* $L = K$) *and that there exist* $(x,y) \in \mathcal{L}$ *with* $\beta_1(x,y)/(\alpha_1-\alpha_2) \in \mathfrak{o}$. *Then*

$$\mathcal{L} = \left\{ \left(\widetilde{x} = -c_1 \frac{\beta_1(x,y)\alpha_2}{\alpha_1-\alpha_2} + c_2 \frac{\beta_2(x,y)\alpha_1}{\alpha_1-\alpha_2}, \right.\right.$$
$$\left.\left. \widetilde{y} = -c_1 \frac{\beta_1(x,y)}{\alpha_1-\alpha_2} + c_2 \frac{\beta_2(x,y)}{\alpha_1-\alpha_2} \right) \,\middle|\, (c_1,c_2) \in \mathcal{L}_0 \right\},$$

where

$$\mathcal{L}_0 = \left\{ (c_1,c_2) \in K_0^2 \,\middle|\, \right.$$
$$\left. G(c_1,c_2) = c_1c_2 \prod_{j=3}^{n} (-1)(\delta_{1,j,2}(x,y)c_1 + \delta_{2,j,1}(x,y)c_2) = 1 \right\}.$$

In particular, $\#\mathcal{L} = \#\mathcal{L}_0$.

Proof. Having fixed $(x,y) \in \mathcal{L}$, the substitution (3) is defined over K, because all $\alpha_i \in \mathfrak{o}$, and maps $\mathcal{L}$ injectively into $\mathcal{L}_0$ by Corollary 1(a).

On the other hand, any $(c_1,c_2) \in \mathcal{L}_0$ corresponds under (3) to a solution $(\widetilde{x},\widetilde{y})$ of (1), which indeed lies in $\mathfrak{o} \times \mathfrak{o}$, since $\beta_1(x,y)/(\alpha_1-\alpha_2) \in \mathfrak{o}$ and, by Lemma 1, also $\beta_2(x,y)/(\alpha_1-\alpha_2) \in \mathfrak{o}$. ∎

5. The cubic case.

First we will apply Corollary 4 to study Thue equations of degree $n = 3$ with infinite solution set, where the form F splits in $K[X,Y]$ into linear factors. So let $\alpha_1,\alpha_2,\alpha_3 \in \mathfrak{o}$ be pairwise different, and (using a linear transformation of the variables) we may suppose $\alpha_3 = 0$, thus

$$F(X,Y) = X^3 - (\alpha_1+\alpha_2)X^2Y + \alpha_1\alpha_2XY^2.$$

Next we look for a suitable right hand side b. Supposing that we have any $(x,y) \in \mathcal{L}$ we solve

$$\delta_{1,3,2}(x,y) = \frac{(x-\alpha_1y)(-\alpha_2)}{x(\alpha_2-\alpha_1)} = -d$$

for x/y to obtain

$$\frac{x}{y} = \frac{\alpha_1\alpha_2}{d\alpha_1 + (1-d)\alpha_2}$$

with some not yet determined $d \in K_0 \setminus \{0,1\}$. Putting $x = \alpha_1\alpha_2$ and $y = d\alpha_1 + (1-d)\alpha_2$, we obtain a suitable right hand side

$$b = F(x,y) = -d(1-d)(\alpha_1\alpha_2(\alpha_1-\alpha_2))^2 = d(1-d)\operatorname{disc} F(X,1).$$

Applying Corollary 4 we get

Lemma 2. *Let $\alpha_1, \alpha_2 \in \mathfrak{o} \setminus \{0\}$ with $\alpha_1 \neq \alpha_2$ and $d \in K_0 \setminus \{0,1\}$. Then for the Thue equation*

$$(X-\alpha_1 Y)(X-\alpha_2 Y)X = -d(1-d)(\alpha_1\alpha_2(\alpha_1-\alpha_2))^2$$

we have

$$\mathcal{L} = \{((c_1 d + c_2(1-d))\alpha_1\alpha_2, c_1 d\alpha_1 + c_2(1-d)\alpha_2) \mid \\ (c_1,c_2) \in K_0^2 \text{ with } c_1c_2(dc_1+(1-d)c_2) = 1\}.$$

To obtain an infinite $\mathcal{L}$ one has to look for $d \in K_0 \setminus \{0,1\}$ such that the elliptic curve $C_1C_2(dC_1 + (1-d)C_2) = 1$ has infinitely many K_0-rational points. Dividing by C_2^3 and substituting $U = d/C_2$ and $V = d^2C_1/C_2 + d(1-d)/2$, transforms this curve into

$$E_d: \ V^2 = U^3 + \left(\frac{d(1-d)}{2}\right)^2,$$

containing the point $P = (d, d(1+d)/2)$.

For $d \in \mathbb{Z}\setminus\{0,1\}$, P has integral coordinates and infinite order by the result of Lutz–Nagell (see e.g. [15, VIII, Cor. 7.2]) for $d \neq -7,-4,-3,-2,-1, 2, 5$. Since $E_d = E_{1-d}$, only the cases $d \in \{2,5\}$ remain. From the tables of J. E. Cremona we find that $E_2(\mathbb{Q})$ is finite and $E_5(\mathbb{Q})$ is infinite (see curve "A1" with conductor $N = 36$ on p. 92 and curve "C1" with conductor $N = 900$ on p. 216 in [2]). Thus for any $d \in \mathbb{Z}\setminus\{-1,0,1,2\}$ the solution set $\mathcal{L}$ in Lemma 2 is infinite.

Explicit Example. Taking $\mathfrak{o} = \mathbb{Q}[T]$, the ring of polynomials in T over the rationals, $\alpha_1 = T, \alpha_2 = 1, \alpha_3 = 0$ and $d = 3$, we find that the Thue equation

$$X^3 - (T+1)X^2Y + TXY^2 = 6T^2(T-1)^2 \tag{8}$$

has infinitely many solutions in $\mathbb{Q}[T]$, namely

$$(x,y) = ((3c_1 - 2c_2)T, 3c_1T - 2c_2),$$

where (c_1, c_2) run through the $\mathbb{Q}$-rational points of the elliptic curve

$$C_1C_2(3C_1 - 2C_2) = 1,$$

which is isomorphic to $E_3 : V^2 = U^3 + 9$. On the other hand, the results of [5] show that equation (8) has only finitely many solutions in $\mathbb{Z}[T]$.

Now we turn to Thue equations of degree $n = 3$, where the form F is irreducible in $K[X,Y]$. So L/K is either cyclic cubic or has the full symmetric group on 3 elements as Galois group. We keep the notations of Section 3 and start with a more precise form of Proposition 5.

LEMMA 3. *Let the Thue equation* (1) *be given with an irreducible*, *cubic form* $F \in K[X,Y]$, *and* $\sigma \in \mathrm{Gal}(L/K)$ *with* $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$ *and* $\sigma(\alpha_3) = \alpha_1$. *If* $[L:K] = 6$ *let* $\tau \in \mathrm{Gal}(L/K)$ *with* $\tau(\alpha_1) = \alpha_3$ *and* $\tau(\alpha_3) = \alpha_1$. *Then*:

(a) *For every* $(x,y) \in \mathcal{L}$,

$$\sigma(\delta_{1,3,2}(x,y)) = -1 - \delta_{1,3,2}(x,y)^{-1}, \tag{9}$$

and furthermore if $[L:K] = 6$ *then*

$$\tau(\delta_{1,3,2}(x,y)) = \delta_{1,3,2}(x,y)^{-1}. \tag{10}$$

(b) *If* $(x,y) \in \mathcal{L}$ *such that* $\delta_{1,3,2}(x,y)$ *is not a root of unity of order* 3 *then* $L = K(\delta_{1,3,2}(x,y))$ (*in particular*, L/K *is a constant field extension*).

(c) *If* $\#\mathcal{L} \geq 7$ *then there exist* $(x,y) \in \mathcal{L}$ *such that* $\delta_{1,3,2}(x,y)$ *is not a root of unity of order* 3.

Proof. (a) Since $x, y \in \mathfrak{o}$ are fixed by σ (and τ, resp.), the Galois action on the roots α_i and (2) yield

$$\sigma(\delta_{1,3,2}(x,y)) = \delta_{2,1,3}(x,y) = -1 - \delta_{1,3,2}(x,y)^{-1},$$

and even more easily one gets (10).

(b) If $\delta_{1,3,2}(x,y)$ were fixed by σ, (9) shows that it would be a root of $X^2 + X + 1$, a contradiction. If $\delta_{1,3,2}(x,y)$ were fixed by τ, $\sigma\tau$ or $\tau\sigma$, (9) and (10) give that it would equal ± 1, 0, -2 or $-1/2$, thus belong to K_0, but this contradicts the action of σ on $\delta_{1,3,2}(x,y)$.

(c) As in the proof of Proposition 3 one can see that for any $d \in L_0$ there exist at most 3 solutions $(\widetilde{x}, \widetilde{y}) \in \mathcal{L}$ with $\delta_{1,3,2}(\widetilde{x}, \widetilde{y}) = d$. Thus for $\#\mathcal{L} \geq 7$ there always exists an $(x,y) \in \mathcal{L}$ for which $\delta_{1,3,2}(x,y)$ is not a root of unity of order 3. ∎

PROPOSITION 7. *Let the notations be as in Lemma* 3. *Assume that* $[L:K] = 3$, *that there exists* $(x,y) \in \mathcal{L}$ *such that* $d := \delta_{1,3,2}(x,y)$ *is not a root of unity of order* 3 *and* $\beta_1(x,y)/(\alpha_1 - \alpha_2) \in \mathfrak{O}$. *Let*

$$X^3 + mX^2 + (m-3)X - 1 \in K_0[X]$$

be the minimal polynomial of d *over* K_0. *Then*

$$\mathcal{L} = \biggl\{\biggl(\widetilde{x} = -c_1 \frac{\beta_1(x,y)\alpha_2}{\alpha_1 - \alpha_2} + c_2 \frac{\beta_2(x,y)\alpha_1}{\alpha_1 - \alpha_2}, \\ \widetilde{y} = -c_1 \frac{\beta_1(x,y)}{\alpha_1 - \alpha_2} + c_2 \frac{\beta_2(x,y)}{\alpha_1 - \alpha_2}\biggr) \biggm| (c_1, c_2) \in \mathcal{E}\biggr\},$$

where

$$\mathcal{E} = \{(c_1 = (s-\sigma(d))t, c_2 = (s-\sigma^2(d))t) \in L_0^2 \mid (s,t) \in K_0^2 \text{ with } s^3+ms^2+(m-3)s-1 = 1/t^3\} \cup \{(c,c) \in K_0^2 \mid c^3 = 1\}.$$

Remark. If $\#\mathcal{L} \geq 7$ there exists $(x,y) \in \mathcal{L}$ such that d is not a root of unity of order 3 by Lemma 3(c), and if $\#\mathcal{L} \geq 4$ then $\beta_1(x,y)/(\alpha_1-\alpha_2) \in \mathfrak{O}$ for all $(x,y) \in \mathcal{L}$ by Proposition 6.

Proof of Proposition 7. Throughout this proof we will fix $(x,y) \in \mathcal{L}$ as given in the proposition. By (9), $\sigma(d) = -1-1/d$, and by Lemma 3(b) and Proposition 9(b) of the appendix, the minimal polynomial of d over K_0 indeed has the shape as indicated above.

Since $\beta_1(x,y)/(\alpha_1-\alpha_2) \in \mathfrak{O}$, the set of special solutions of (1) in $\mathfrak{O}\times\mathfrak{O}$ (i.e. inside the splitting field L of $F(X,1)$ over K) is given by Corollary 4. So we only have to find out which of these solutions are invariant under σ. Let

$$(11)\quad \widetilde{x} = -c_1\frac{\beta_1(x,y)\alpha_2}{\alpha_1-\alpha_2} + c_2\frac{\beta_2(x,y)\alpha_1}{\alpha_1-\alpha_2}, \qquad \widetilde{y} = -c_1\frac{\beta_1(x,y)}{\alpha_1-\alpha_2} + c_2\frac{\beta_2(x,y)}{\alpha_1-\alpha_2}$$

with $(c_1,c_2) \in L_0^2$ satisfying $c_1c_2(-dc_1+(1+d)c_2) = 1$. From (5) we obtain

$$(12)\quad \text{for } 1 \leq i \leq 3: \quad \widetilde{x}-\alpha_i\widetilde{y} = c_i(x-\alpha_i y) \quad \text{with } c_3 = -dc_1+(1+d)c_2$$

and

$$\delta_{1,3,2}(\widetilde{x},\widetilde{y}) = \frac{c_1}{c_3}\,\delta_{1,3,2}(x,y) = \frac{dc_1}{-dc_1+(1+d)c_2} =: \widetilde{d}.$$

Assuming that $\widetilde{x},\widetilde{y} \in \mathfrak{o}$, (9) yields $\sigma(\widetilde{d}) = -(1+\widetilde{d})/\widetilde{d}$, and Proposition 9(c) of the appendix gives $\widetilde{d} = d$ or $\widetilde{d} = ((1+s)d+1)/(s-d)$ with some $s \in K_0$. The first case yields $c_1 = c_2 = c_3 = c$ with $c^3 = 1$ and $(\widetilde{x},\widetilde{y}) = (cx,cy)$. In the second case we insert the expression for $\widetilde{d}$ and obtain

$$c_1 d(1+s(1+d)) = c_2(1+d)(1+d(1+s)), \qquad \frac{c_1}{s-\sigma(d)} = \frac{c_2}{s-\sigma^2(d)}.$$

Since $\widetilde{x},\widetilde{y} \in \mathfrak{o}$, (12) shows that the c_i are conjugates of each other, so $t := c_1/(s-\sigma(d))$ is invariant under σ and we obtain

$$c_1 = (s-\sigma(d))t, \quad c_2 = (s-\sigma^2(d))t, \quad c_3 = (s-d)t, \quad s,t \in K_0.$$

From $1 = c_1c_2c_3 = t^3(s^3+ms^2+(m-3)s-1)$ we find that $(s,t) \in K_0^2$ must be a solution of the equation defining the set $\mathcal{E}$.

To prove the other inclusion, let $(s,t) \in K_0^2$ satisfy $s^3+ms^2+(m-3)s-1 = 1/t^3$, i.e. $1 = t^3(s-d)(s-\sigma(d))(s-\sigma^2(d))$. Putting $c_1 = (s-\sigma(d))t$ and $c_2 = (s-\sigma^2(d))t$, we get $c_3 = -dc_1+(1+d)c_2 = t(s-d)$, thus $(c_1,c_2) \in L_0^2$ is a solution of $C_1C_2(-dC_1+(1+d)C_2) = 1$, and $(\widetilde{x},\widetilde{y}) \in \mathfrak{O}\times\mathfrak{O}$ as given by (11) is a solution of the Thue equation (1). Since the c_i's are conjugates of each other, we get

$$\widetilde{x}-\alpha_2\widetilde{y}=c_2(x-\alpha_2 y)=\sigma(c_1(x-\alpha_1 y))=\sigma(\widetilde{x}-\alpha_1\widetilde{y})=\sigma(\widetilde{x})-\alpha_2\sigma(\widetilde{y}),$$

and similarly $\widetilde{x}-\alpha_3\widetilde{y}=\sigma(\widetilde{x})-\alpha_3\sigma(\widetilde{y})$, which implies that $\widetilde{x},\widetilde{y}$ are fixed by σ, and thus indeed $(\widetilde{x},\widetilde{y})\in\mathcal{L}$. ■

In the situation of Proposition 7 we obtain an infinite set $\mathcal{L}$ of special solutions if and only if the elliptic curve

$$S^3+mS^2+(m-3)S-1=\left(\frac{1}{T}\right)^3$$

has infinitely many K_0-rational points. This curve can be birationally transformed into

$$E'_m:\ V^2=U^3+16(m^2-3m+9)^2,$$

containing the point $P=\left(\frac{4}{9}(m+3)(m-6),\ \frac{4}{27}(2m-3)(m^2-3m+63)\right)$.

If for $m\in\mathbb{Z}$, m^2-3m+9 is a 3rd-power free integer, the only torsion points of $E'_m(\mathbb{Q})$ are $Q^{\pm}=(0,\pm4(m^2-3m+9))$, which have order 3 (see e.g. [1, §12, Ex. 3]). Since for $m\neq-3,6$ we have $P\neq Q^{\pm}$, under these conditions $\#E'_m(\mathbb{Q})=\infty$.

On the other hand, if $3\,|\,m$ for some $m\in\mathbb{Z}$, the point P has integral coordinates, and one can again use the result of Lutz–Nagell as above to show that $\#E'_m(\mathbb{Q})=\infty$ for $m\in3\mathbb{Z}\setminus\{-3,3,6\}$.

Explicit Example. Let us take $\mathfrak{o}=\mathbb{Q}[T]$, $K=\mathbb{Q}(T)$ and θ a root of $X^3-3X-1=0$, so $\mathbb{Q}(\theta)$ is a cyclic cubic number field with Galois operation $\sigma(\theta)=-(1+\theta)/\theta$. The cubic form

$$F(X,Y)=X^3-3(T^2-T+1)XY^2-(T^3+3T^2-6T+1)Y^3\in\mathbb{Q}(T)[X,Y]$$

has roots $\alpha_1=\theta T+\sigma^2(\theta)$ and its conjugates, thus $L=\mathbb{Q}(\theta)(T)$ is its splitting field. Choosing $\delta_{1,3,2}(x,y)=\sigma(\theta)$ we calculate that a possible solution $(x,y)\in\mathcal{L}$ should satisfy $x/y=(1-T^2)/T$, which yields an appropriate right hand side $b=F(1-T^2,T)=(T^3-3T^2+1)^2$. From Proposition 7 we conclude that

$$X^3-3(T^2-T+1)XY^2-(T^3+3T^2-6T+1)Y^3=(T^3-3T^2+1)^2$$

has an infinite set of special solutions, namely

$$\mathcal{L}=\{(-(s+1)tT^2+2tT+st,\ stT+t)\mid(s,t)\in\mathbb{Q}^2\text{ with }s^3-3s-1=1/t^3\}.$$

Finally, let us study the case where $[L:K]=6$, and let $K'\subset L$ denote the quadratic extension of K inside L.

Proposition 8. *Let the notations be as in Lemma* 3. *Assume that* $[L\!:\!K]=6$, *there exists* $(x,y)\in\mathcal{L}$ *such that* $d:=\delta_{1,3,2}(x,y)$ *is not a root of unity of order* 3 *and* $\beta_1(x,y)/(\alpha_1-\alpha_2)\in\mathfrak{O}$. *Let* $K'_0\subset L_0$ *denote the quadratic* *extension of K_0 inside L_0 and let*

$$p = X^3 + \mu X^2 + (\mu - 3)X - 1 \in K_0'[X]$$

be the minimal polynomial of d over K_0'. Then the minimal polynomial of d over K_0 is

$$X^6 + 3X^5 - \bigl(m + \tfrac{3}{4}\bigr)X^4 - \bigl(2m + \tfrac{13}{2}\bigr)X^3 - \bigl(m + \tfrac{3}{4}\bigr)X^2 + 3X + 1 \in K_0[X]$$

with $m = \bigl(\mu - \frac{3}{2}\bigr)^2 = \mu^2 - 3\mu + \frac{9}{4} \in K_0$, *and*

$$\mathcal{L} = \biggl\{ \biggl(\widetilde{x} = -c_1 \frac{\beta_1(x,y)\alpha_2}{\alpha_1 - \alpha_2} + c_2 \frac{\beta_2(x,y)\alpha_1}{\alpha_1 - \alpha_2}, \\ \widetilde{y} = -c_1 \frac{\beta_1(x,y)}{\alpha_1 - \alpha_2} + c_2 \frac{\beta_2(x,y)}{\alpha_1 - \alpha_2} \biggr) \biggm| (c_1, c_2) \in \mathcal{E}' \biggr\},$$

where

$$\mathcal{E}' = \bigl\{ \bigl(c_1 = \bigl(sm - \bigl(\tfrac{1}{2} + \sigma(d)\bigr)\bigl(\mu - \tfrac{3}{2}\bigr)\bigr)t, \\ c_2 = \bigl(sm - \bigl(\tfrac{1}{2} + \sigma^2(d)\bigr)\bigl(\mu - \tfrac{3}{2}\bigr)\bigr)t\bigr) \in L_0^2 \bigm| (s,t) \in K_0^2 \text{ with} \\ m^2\bigl(ms^3 + ms^2 - \tfrac{9}{4}s - \tfrac{1}{4}\bigr) = 1/t^3 \bigr\} \cup \{(c,c) \in K_0^2 \mid c^3 = 1\}.$$

Proof (sketch). Fix $(x,y) \in \mathcal{L}$ as in the statement. By Lemma 3(b), d generates L over K, and by (10) the reciprocals of the roots of $p(X)$ are also conjugates of d over K, so its minimal polynomial over K_0 can be calculated as $-p(X)\,X^3 p(1/X)$. Furthermore, $K_0' = K_0(\sqrt{m})$.

Applying Proposition 7 to the cyclic cubic extension L/K' we find that all special solutions of (1) inside $K' \times K'$ are given by (11) with

$$c_1 = (s' - \sigma(d))t', \qquad c_2 = (s' - \sigma^2(d))t', \tag{13}$$

where $(s', t') \in K_0' \times K_0'$ with

$$s'^3 + \mu s'^2 + (\mu - 3)s' - 1 = 1/t'^3. \tag{14}$$

First suppose that $(\widetilde{x}, \widetilde{y}) \in \mathfrak{o} \times \mathfrak{o}$. Applying (10) to

$$\widetilde{d} = \delta_{1,3,2}(\widetilde{x}, \widetilde{y}) = \frac{(1 + s')d + 1}{s' - d}$$

we deduce from $\tau(\widetilde{d}) = 1/\widetilde{d}$ that $0 = (d^2 + d + 1)(\tau(s') + s' + 1)$ and consequently $\tau(s') = -1 - s'$ and $s' = -\frac{1}{2} + s\bigl(\mu - \frac{3}{2}\bigr)$ with some $s \in K_0$. Since $c_1 = (\widetilde{x} - \alpha_1\widetilde{y})/(x - \alpha_1 y)$ is fixed by $\sigma\tau$, we obtain

$$\bigl(s' + 1 + \tfrac{1}{d}\bigr)t' = (s' - \sigma(d))t' = c_1 = \sigma\tau(c_1) \\ = (\tau(s') - \tau(d))\tau(t') = \bigl(-1 - s' - \tfrac{1}{d}\bigr)\tau(t')$$

and thus $\tau(t') = -t'$ and $t' = t\bigl(\mu - \frac{3}{2}\bigr)$ with some $t \in K_0$. Inserting these expressions for s' and t' into (13) and (14) yields the description of $\mathcal{L}$ as given in the proposition.

To prove the other inclusion, note that we know already that $\widetilde{x}, \widetilde{y} \in K'$. Checking that c_1 (c_2, resp.) as given in the definition of $\mathcal{E}'$ is invariant under $\sigma\tau$ (τ, resp.), we obtain $\widetilde{x} - \alpha_i \widetilde{y} = \tau(\widetilde{x}) - \alpha_i \tau(\widetilde{y})$ for $i = 1, 2$ and therefore $\widetilde{x} = \tau(\widetilde{x}) \in \mathfrak{o}$ and $\widetilde{y} = \tau(\widetilde{y}) \in \mathfrak{o}$. ■

In the situation of Proposition 8 we obtain an infinite set $\mathcal{L}$ of special solutions if and only if the elliptic curve

$$m^3S^3 + m^3S^2 - \frac{9}{4}m^2S - \frac{1}{4}m^2 = \left(\frac{1}{T}\right)^3$$

has infinitely many K_0-rational points. This curve can be birationally transformed into

$$E''_m : \ V^2 = U^3 + m^3(27 + 4m)^2,$$

containing the point $P = \left(\frac{4}{9}m^2 - 9m, \frac{8}{27}m^3 + 18m^2\right)$.

If $m^3(27+4m)^2$ is a 6th-power free integer for some $m \in \mathbb{Z} \setminus \{0\}$, then P is not a torsion point (see e.g. [1, §12, Ex. 3]), so in this case $\#E''_m(\mathbb{Q}) = \infty$.

On the other hand, if $3 \mid m$ for $m \in \mathbb{Z} \setminus \{0\}$, then the point P has integral coordinates, and one can again use the result of Lutz–Nagell as above to show that for $m \in 3\mathbb{Z} \setminus \{-60, -54, 0, 2 \cdot 3^5, 20 \cdot 3^5, 182 \cdot 3^5, 1640 \cdot 3^5, 14762 \cdot 3^5\}$ we have $\#E''_m(\mathbb{Q}) = \infty$.

Appendix. Auxiliary results on cubic field extensions. Throughout this appendix let L/K denote an arbitrary field extension of degree 3 and let $\mathrm{PGL}_2(K) = \mathrm{GL}_2(K)/K^\times$ operate on the projective line $L \cup \{\infty\}$ via Möbius transformations, i.e. if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ represents $\Lambda \in \mathrm{PGL}_2(K)$ then $\Lambda\alpha = \frac{a\alpha+b}{c\alpha+d}$ for all $\alpha \in L$.

Proposition 9. *Let L/K be a field extension of degree* 3 *and $\theta \in L$ with $L = K(\theta)$. Then*:

(a) *For every $\alpha \in L \backslash K$ there exists a unique $\Lambda \in \mathrm{PGL}_2(K)$ with $\alpha = \Lambda\theta$.*

Suppose further that L/K is Galois, *$\sigma \in \mathrm{Gal}(L/K)$ generates the Galois group and*

$$\sigma(\theta) = -\frac{1+\theta}{\theta} = T\theta \quad \textit{with } T = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then:

(b) *The minimal polynomial of θ over K is*

$$X^3 + mX^2 + (m-3)X - 1 \in K[X],$$

where $-m = \mathrm{tr}_{L/K}(\theta) \in K$ is the trace of θ from L to K.

(c) *For $\alpha \in L$ we have $\sigma(\alpha) = -(1+\alpha)/\alpha = T\alpha$ if and only if $\alpha = \theta$ or*

$$\alpha = \frac{(1+s)\theta + 1}{-\theta + s} = \Sigma\theta \quad \textit{with } \Sigma = \begin{pmatrix} 1+s & 1 \\ -1 & s \end{pmatrix} \textit{ for some } s \in K.$$

Proof. (a) Choose any $\alpha \in L \setminus K$, thus $\alpha = r_0 + r_1\theta + r_2\theta^2$ with $r_i \in K$ and $(r_1, r_2) \neq (0,0)$. Equating

$$r_0 + r_1\theta + r_2\theta^2 = \frac{a\theta + b}{c\theta + d},$$

using the minimal polynomial of θ over K and comparing coefficients with respect to the K-basis $(1, \theta, \theta^2)$, one obtains a system of linear equations for (a, b, c, d) of rank 3, and the solutions yield a unique element $\Lambda = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) K^\times \in \mathrm{PGL}_2(K)$.

(b) Since the conjugates of θ are $-(1+\theta)/\theta$ and $-1/(1+\theta)$, this follows from a direct calculation.

(c) First suppose that $\alpha \in K$. Since $\alpha = \sigma(\alpha) = -1 - 1/\alpha$, α must be a root of unity of order 3 in K, and the assertion holds with $s = \alpha^2$ (the only values of s for which $\Sigma = \left(\begin{smallmatrix} 1+s & 1 \\ -1 & s \end{smallmatrix}\right)$ is singular).

Now let $\alpha \in L \setminus K$. Using part (a) we may put $\alpha = \Lambda\theta$ for some $\Lambda \in \mathrm{PGL}_2(K)$. Therefore $\sigma(\alpha) = T\alpha$ if and only if $\Lambda T\theta = \Lambda\sigma(\theta) = \sigma(\Lambda\theta) = T\Lambda\theta$, i.e. Λ commutes with T in $\mathrm{PGL}_2(K)$. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$ represent Λ, so we have to find all $(a, b, c, d) \in K^4$ such that $\left(\begin{smallmatrix} a-b & a \\ c-d & c \end{smallmatrix}\right)$ equals $\left(\begin{smallmatrix} a+c & b+d \\ -a & -b \end{smallmatrix}\right)$ up to a nonzero constant.

First observe that $b = 0$ if and only if $c = 0$, and if this holds we get $a = d$, $\Lambda = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\alpha = \theta$. (From the projective point of view, this corresponds to Σ with $s = \infty$.)

Now we may suppose $bc \neq 0$ and get the system of equations

$$\begin{aligned} &\text{(I)} & b(b-a) &= c(a+c), \\ &\text{(II)} & -ab &= c(b+d), \\ &\text{(III)} & -ac &= b(d-c). \end{aligned}$$

Adding (II) and (III) gives $(a+d)(b+c) = 0$, so we will consider 2 cases:

Case 1: $c = -b$ $(\neq 0)$. Now (III) yields $a = b + d$ and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} b+d & b \\ -b & d \end{pmatrix} = b\begin{pmatrix} 1+s & 1 \\ -1 & s \end{pmatrix} \qquad \text{with } s = d/b \in K,$$

representing an element of $\mathrm{PGL}_2(K)$, provided s is not a root of unity of order 3.

Case 2: $d = -a$. Since $b + c = 0$ was already considered in Case 1, we infer from (I) that $a = b - c$ and therefore $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ b-a & -a \end{smallmatrix}\right)$. But this matrix has determinant $-a^2 + ab - b^2$, which equals 0 by (III), and we get no further solutions in this case. ∎

Remark. If the special Galois operation as considered in Proposition 9 occurs for $K = \mathbb{Q}$ and integral θ, then L is called a "simplest cubic number field", a notion going back to D. Shanks [14].

If σ generates the Galois group of a cubic extension $K(\theta)/K$, Proposition 9(a) gives $\sigma(\theta) = \Lambda\theta$, where $\Lambda \in \mathrm{PGL}_2(K)$ is a torsion element of order 3. For $K = \mathbb{Q}$, Lemma 1(a) in [7] shows that Λ must be conjugate to T or T^2, thus any cyclic cubic extension of $\mathbb{Q}$ can be generated by a (not necessarily integral) element with Galois operation given by T as in Proposition 9.

References

[1] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Stud. Texts 24, Cambridge Univ. Press, 1991.

[2] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1992.

[3] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[4] H. Grauert, *Mordells Vermutung über rationale Punkte auf algebraischen Kurven und Funktionenkörper*, Inst. Hautes Études Sci. Publ. Math. 25 (1965), 131–149.

[5] K. Győry, *Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains*, Acta Math. Hungar. 42 (1983), 45–80.

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

[7] G. Lettl, A. Pethő and P. Voutier, *Simple families of Thue inequalities*, Trans. Amer. Math. Soc. 351 (1999), 1871–1894.

[8] Yu. I. Manin, *A proof of the analog of the Mordell conjecture for algebraic curves over function fields*, Dokl. Akad. Nauk SSSR 152 (1963), 1061–1063 (in Russian); English transl.: Soviet Math. Dokl. 4 (1963), 1505–1507.

[9] R. C. Mason, *On Thue's equation over function fields*, J. London Math. Soc. 24 (1981), 414–426.

[10] —, *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Ser. 96, Cambridge Univ. Press, 1984.

[11] C. F. Osgood, *Effective bounds on the "Diophantine approximation" of algebraic functions over fields of arbitrary characteristic and applications to differential equations*, Indag. Math. 37 (1975), 105–119; *Errata*, ibid. 37 (1975), 401.

[12] M. Rosen, *Number Theory in Function Fields*, Grad. Texts in Math. 210, Springer, 2002.

[13] W. M. Schmidt, *Thue's equation over function fields*, J. Austral. Math. Soc. 25 (1978), 385–422.

[14] D. Shanks, *The simplest cubic fields*, Math. Comp. 28 (1974), 1137–1152.

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[16] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993.

Institut für Mathematik und wissenschaftliches Rechnen
Karl-Franzens-Universität
Heinrichstraße 36, A-8010 Graz, Austria
E-mail: guenter.lettl@uni-graz.at

Received on 8.3.2004 (4732)