Nun gilt

$$\frac{1}{\sqrt{u}} x \circ g_k(1, x) \circ \sqrt{u}x = \sum_{t=0}^{[k/2]} \frac{k}{k-t} \binom{k-t}{t} (-1)^t u^{(k-1)/2-t} x^{k-2t}$$

$$\equiv u^{(k-1)/2} \sum_{t=0}^{[k/2]} \frac{k}{k-t} \binom{k-t}{t} (-v)^t x^{k-2t} \bmod p^e,$$

wenn v so gewählt wird, daß $uv \equiv 1 \bmod p^e$. Da aber das zuletzt erhaltene Polynom genau dann ein PP mod p ist, wenn $(k, p^2-1) = 1$, und genau dann ein PP mod p^e mit $e > 1$ ist, wenn $(k, p(p^2-1)) = 1$ (vgl. etwa [2]), gilt

SATZ 8. *Das mit* $\sqrt{u}(rx+s)$ *Transformierte von* $g_k(1, x)$ *mit* $k > 1$ *ist genau dann Permutationspolynom* mod p^e, *wenn* $(ur, p) = p$ *sowie* $(k, p) = 1$, *und wenn* $(ur, p) = 1$ *sowie* $(k, p^2-1) = 1$ *für* $e = 1$ *bzw.* $(k, p(p^2-1)) = 1$ *für* $e > 1$.

Die Berechnung der Fixpunktanzahl der Permutationen $x \to l^{-1} \circ g_k(1, x) \circ l \bmod p^e$ und die Ermittlung der Struktur der von diesen Permutationen bei festem l gebildeten Permutationsgruppe modulo p^e scheinen mühsam und nicht leicht zu sein.

Auf ähnliche Weise wie im Falle der Dickson-Polynome $g_k(1, x)$ lassen sich auch die ganzzahligen konjugierten Ketten der Kette der Dickson-Polynome $g_k(-1, x)$ bestimmen, was aber hier nicht mehr durchgeführt werden soll.

Literatur

[1] H. Lausch, W. Müller und W. Nöbauer, *Über die Struktur einer durch Dicksonpolynome dargestellten Permutationsgruppe des Restklassenringes modulo n*, J. Reine Angew. Math. 261 (1973), 88–99.

[2] H. Lausch and W. Nöbauer, *Algebra of Polynomials*, Amsterdam 1973.

[3] R. Lidl and W. Müller, *On Commutative Semigroups of Polynomials with Respect to Composition*, Mh. Math. 102 (1986), 139–153.

[4] W. Müller, *Über eine Klasse von durch Dickson-Polynome dargestellten Gruppen*, Coll. Math. Soc. Janós Bolyai 6, Keszthely 1971.

[5] W. Müller und W. Nöbauer, *Über die Fixpunkte der Potenzpermutationen*, Österr. Akad. Wiss., Sitzungsber. Math. Nat. Kl. 192 (1983), 93–97.

[6] R. Nöbauer, *Über die Fixpunkte einer Klasse von Dickson-Permutationen*, ibid. 193 (1984), 521–547.

[7] — *Über die Fixpunkte der Dickson-Permutationen*, ibid. 193 (1984), 115–133.

[8] — *Über eine Gruppe der Zahlentheorie*, Monatsh. Math. 58 (1954), 181–192.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT KLAGENFURT
A-9022 Klagenfurt
Austria

Eingegangen am 17. 9. 1986
und in revidierter Form am 8. 12. 1986 (1672)

ACTA ARITHMETICA
LI (1988)

Inhomogeneous norm form equations over function fields

by

I. GAÁL (Debrecen)

1. Introduction. In this paper, we give effective bounds for the solutions of inhomogeneous norm form equations in several dominating variables over function fields in all cases where the solutions can be bounded by usual parameters of the function field.

The first general effective finiteness result on norm form equations in two variables over $\mathbf{Z}$, i.e. on Thue equations was obtained by Baker [1]. This famous theorem was later generalized and extended by several authors. For further references on norm form equations in several variables over number fields see e.g. Győry [7], [9].

In 1974 Sprindžuk [21] gave an inhomogeneous generalization of Baker's result. He obtained effective bounds for all solutions of the equation

$$N_{K/\mathbf{Q}}(x+\alpha y+\lambda) = m \tag{1}$$

where $K = \mathbf{Q}(\alpha)$ is an algebraic number field of degree $\geqslant 3$, $0 \neq m \in \mathbf{Z}$ and the variables are $x, y \in \mathbf{Z}$ and [1] $\lambda \in \mathbf{Z}_K$. Here λ is a non-dominating variable such that [2] $\overline{|\lambda|} < (\max(|x|, |y|))^{1-\zeta}$ ($0 < \zeta < 1$ is a given constant). In the special case $\lambda = 0$ this theorem gives the above mentioned result of Baker.

Combining the method of Sprindžuk [21] with that of Győry and Papp [10], in [5], [6], we extended Sprindžuk's theorem to the case of certain inhomogeneous norm form equations in several dominating variables over number fields.

Now let us turn to norm form equations considered over function fields. In the special case of two variables, Osgood [16], [17], Schmidt [18]–[20] Stepanov [22], Mason [11], Győry [8] and Brindza [2] gave effective bounds for the solutions of Thue equations. Győry [8] derived effective results also for the solutions of certain norm form equations in several variables.

A general effective theorem on norm form equations over function fields

---

[1] Z_K denotes the ring of integers of an algebraic number field K.

[2] $\overline{|\lambda|}$ is the size of an algebraic number λ, that is the maximum absolute value of its conjugates.

was obtained by Mason [13]. He proved that if the module generated by the coefficients of the norm form is "non-degenerate" (for the exact concept see Section 3), then there are only finitely many solutions and he derived a bound for all solutions. He showed that if the assumption of non-degeneracy does not hold, then the solutions cannot always be bounded by usual parameters.

In [11] and [13], Mason constructed also algorithms to determine all solutions of Thue equations and general norm form equations (with non-degenerate modules), respectively. For further results on norm form equations over function fields see Mason [14], [15].

Recently, Brindza and the author [3] obtained an effective result on inhomogeneous Thue equations over function fields and proved an analogue of Sprindžuk's theorem [21] on equation (1).

Our purpose in this paper is to derive effective bounds for the solutions of general inhomogeneous norm form equations (with non-degenerate modules) over function fields, that is, to give a common generalization of Theorem 2 of Mason [13] and of the Theorem of our paper [3].

In our proof we combined the arguments of Mason [13] and Brindza and Gaál [3] with some new ideas.

2. Preliminaries concerning function fields. First we introduce our notation and recall some basic facts concerning function fields.

Let k denote an algebraically closed field of characteristic 0 and let $k(z)$ be the field of rational functions over k. If K is any finite extension field of $k(z)$, denote by Ω_K the set of all (additive) valuations on K with value group $\mathbf{Z}$. The valuation $v \in \Omega_K$ is called *finite* if $v(z) \geqslant 0$, otherwise v is called *infinite*. For any non-zero $\alpha \in K$ the *additive height* of α is defined by

$$H_K(\alpha) = -\sum_{v \in \Omega_K} \min\{0, v(\alpha)\}.$$

Obviously, $H_K(\alpha) = 0$ if and only if $\alpha \in k$. (For $\alpha = 0$ put $H_K(\alpha) = 0$.) It follows from the additive form

$$\sum_{v \in \Omega_K} v(\alpha) = 0$$

of the well-known product formula that

$$H_K(\alpha^m) = |m| H_K(\alpha),$$

$$H_K(\alpha+\beta) \leqslant H_K(\alpha)+H_K(\beta), \quad H_K(\alpha\beta) \leqslant H_K(\alpha)+H_K(\beta)$$

for any non-zero $\alpha, \beta \in K$ and $m \in \mathbf{Z}$. For any finite set $\mathscr{S}$ of elements of K the *height* is defined by

$$H_K(\mathscr{S}) = -\sum_{v \in \Omega_K} \min(0, v(s); s \in \mathscr{S}).$$

If $1 \in \mathscr{S}$ and $0 \neq \mu \in K$ then we have

$$H_K(\mathscr{S}) \leqslant H_K(\mu\mathscr{S})$$

where $\mu\mathscr{S} = \{\mu s \mid s \in \mathscr{S}\}$. Finally, we remark that if L is a field lying between $k(z)$ and K and $w \in \Omega_L$, then

$$w(N_{K/L}(\alpha)) = \sum_{v|w} v(\alpha) \tag{2}$$

for any non-zero $\alpha \in K$, where on the right-hand side v runs over all valuations $v \in \Omega_K$ which extends the valuation w to K.

For these and further properties of the valuations of function fields and the height function see e.g. Mason [12].

3. Results. Now let us turn to the formulation of our theorem. Following the notation of Mason [13], let L and K be finite extensions of $k(z)$ with $L \subset K$. Denote by $\mathcal{O}$ the ring of elements of L integral over $k[z]$. Let M be a finitely generated $\mathcal{O}$-module in K. For any field F lying between L and K let

$$M^F = \{m \in M \mid \forall j \in F \ \exists l \in L \text{ with } ljm \in M\}.$$

M^F is a submodule of M, it is either $\{0\}$ or the rank of M^F is $\geqslant [F:L]$. M is called *non-degenerate* (see [13]) if for each F $r_F > r_L$ implies $M^F = \{0\}$, where r_F and r_L denote the number of infinite valuations of F and L, respectively. Mason [13] considered equations of the form

$$N_{K/L}(x) = c \quad \text{in } x \in M \tag{3}$$

where $c \in L$ is fixed. He proved that if M is non-degenerate then (3) has only finitely many solutions $x \in M$ for each $c \in L$. Moreover, he gave an effective algorithm to determine all solutions of (3) and derived a bound for the heights of the solutions.

As an inhomogeneous generalization of (3) let us consider the equation

$$N_{K/L}(x+\lambda) = c \tag{4}$$

in $x \in M$ and $\lambda \in K$. Under the condition that the height of λ is "small" compared with the height of x (and M is non-degenerate), in our theorem we give an effective bound for the heights of all solutions of equation (4).

It is no loss of generality to assume further that K is a normal extension of L and M is a free $\mathcal{O}$-module in K (cf. [13]). Denote by d, g and r the degree of K over L, the genus of K/k and the number of infinite valuations of K, respectively, and let $x_1, \ldots, x_n$ be an $\mathcal{O}$-basis of M with height $H_K(x_1, \ldots, x_n) \leqslant H$. Our main result is the following:

THEOREM. *If M is non-degenerate and $x \in M$, $\lambda \in K$ is a solution of equation (4) with $H_K(\lambda) < c_0 H_K(x)$, where $c_0 = [20d^2(n+1)^3]^{-n}$ then*

$$H_K(x) < 2^{5n+3}[d^2(n+1)^3]^n(H+r+g+H_K(c)+1). \tag{5}$$

The condition of non-degeneracy of M is necessary since otherwise even equation (3) (which is a special case of (4) restricting the variable λ to zero) can have solutions which cannot be bounded by usual parameters (cf. Mason [13]). We remark that although the height of the solutions of equation (4) is bounded, it may obviously have infinitely many solutions.

In the special case $\lambda = 0$ our theorem gives the following corollary:

COROLLARY 1. *If M is non-degenerate then for all solutions $x \in M$ of equation* (3) *we have* (5).

The assertion of Corollary 1 coincides with Theorem 2 of Mason [13], just our constant is somewhat different.

In [3] we considered $\mathcal{S}$-integral solutions of inhomogeneous Thue equations over function fields. For equations of this type our theorem gives

COROLLARY 2. *Let $\alpha \in K$ be of degree $\geqslant 3$ over L. If $x, y \in \mathcal{O}$ and $\lambda \in K$ is a solution of*

$$N_{K/L}(x+\alpha y+\lambda) = c$$

with $H_K(\lambda) < \bar{c}_0 \max(H_K(x), H_K(y))$, where $\bar{c}_0 = (2^{25} d^4 H_K(\alpha))^{-1}$, then we have

$$\max(H_K(x), H_K(y)) < 2^{27} d^4 (H_K(\alpha) + r + g + H_K(c) + 1). \tag{6}$$

The result of Corollary 2 may be compared with that special case of the Theorem of [3] when $\mathcal{S}$ consists only of the infinite valuations of K (the constant in [3] is much better than (6)).

4. Proofs. In our proof we follow the arguments of Mason [13]. The basic steps of the proof of [13] were modified and considerably extended in our paper, in order to be able to deal with the inhomogeneous variable λ (cf. [13]).

The proof is based on an effective theorem on $\mathcal{S}$-unit equations in several variables. The theorem was first proved by Mason [13] and later improved by Brownawell and Masser [4]. In order to get a better bound in our theorem we shall apply this later result. We recall that if $\mathcal{S}$ is a finite subset of Ω_K then $\alpha \in K$ is called *$\mathcal{S}$-unit* if $v(\alpha) = 0$ for all $v \in \Omega_K \setminus \mathcal{S}$.

LEMMA. *Let $\mathcal{S}$ be a finite subset of Ω_K and let $u_1, \ldots, u_n$ be $\mathcal{S}$-units of K such that*

$$u_1 + \ldots + u_n = 0,$$

but no non-empty proper subset of $\{u_1, \ldots, u_n\}$ is linearly dependent over k. Then we have

$$H_K\left(\frac{u_2}{u_1}, \ldots, \frac{u_n}{u_1}\right) \leqslant \tfrac{1}{2}(n-1)(n-2)[|\mathcal{S}| + 2g - 2]$$

where $|\mathcal{S}|$ denotes the cardinality of $\mathcal{S}$.

Our lemma is Corollary I of Brownawell and Masser [4].

Proof of the Theorem. We shall denote by $G(K/L)$ and $G(K/F)$ the Galois groups of the extensions K/L and K/F, respectively.

I. First let us consider the case where $n = 1$. In this case, $x = \alpha_1 x_1$ with $\alpha_1 \in \mathcal{O}$. Put $\lambda_0 = \lambda/x_1$; then equation (4) can be written in the form

$$\prod_{\sigma \in G(K/L)} (\alpha_1 + \lambda_0 \sigma) = \frac{c}{N_{K/L}(x_1)}.$$

It means that α_1 is a root of the polynomial

$$f(x) = \prod_{\sigma \in G(K/L)} (x + \lambda_0 \sigma) - \frac{c}{N_{K/L}(x_1)} \in K[x].$$

We recall that the height $H_K(f_1)$ of a polynomial f_1 in $K[x]$ is defined by $H_K(\mathcal{S})$ where $\mathcal{S}$ is the set of its coefficients. Since $f_1(x) = \prod_{\sigma \in G(K/L)} (x + \lambda_0 \sigma)$ is a power of the minimal defining polynomial of $-\lambda_0$ over L, hence by Lemma 4 of Mason [12] we can see that $H_K(f_1) \leqslant d H_K(\lambda_0)$. Obviously,

$$H_K(f) \leqslant H_K(f_1) + H_K\left(\frac{c}{N_{K/L}(x_1)}\right).$$

It follows from the Corollary to Lemma 4 of Mason [12] that $H_K(\alpha_1) \leqslant H_K(f)$. Combining our results, we obtain

$$H_K(x) = H_K(\alpha_1 x_1) \leqslant (2d+1) H + d H_K(\lambda) + H_K(c). \tag{7}$$

II. Now let us suppose that $n > 1$. Denote by F the field generated by $x_2/x_1, \ldots, x_n/x_1$ over L. Since $x_1, x_2, \ldots, x_n$ are linearly independent over L, hence $1, x_2/x_1, \ldots, x_n/x_1$ are also linearly independent over L, that is, $[F:L] \geqslant n$. We shall examine separately the cases $[F:L] = n$ and $[F:L] > n$. In the following let $x \in M$ and $\lambda \in K$ be a fixed solution of equation (4).

II.A. First assume that $[F:L] = n$, that is $\{1, x_2/x_1, \ldots, x_n/x_1\}$ is a basis of F over L. Any $j \in F$ can be written as

$$j = \sum_{i=1}^{n} \alpha_i \frac{x_i}{x_1} \quad \text{with } \alpha_1, \ldots, \alpha_n \in L.$$

Denote by l an element of L such that $l\alpha_1, \ldots, l\alpha_n \in \mathcal{O}$; then $l j x_1 \in M$, that is, $x_1 \in M^F$. By our assumption M is non-degenerate; hence $M^F \neq \{0\}$ implies $r_F = r_L$.

If $x = \alpha_1 x_1 + \ldots + \alpha_n x_n$ $(\alpha_1, \ldots, \alpha_n \in \mathcal{O})$ is in M then $y = \frac{x}{x_1} = \alpha_1 + \alpha_2 \frac{x_2}{x_1} + \ldots + \alpha_n \frac{x_n}{x_1}$ is in F. Further, put $\lambda_0 = \lambda/x_1$. Then equation (4) can be written in the form

$$N_{K/L}(y + \lambda_0) = \frac{c}{N_{K/L}(x_1)}. \tag{8}$$

We are interested in the values of $N_{K/F}(y+\lambda_0)$ at different valuations $v \in \Omega_K$.

Let v be an arbitrary finite valuation in Ω_K. Then we have

$$(9) \qquad v(N_{K/F}(y+\lambda_0)) = \sum_{\sigma \in G(K/F)} v(y+\lambda_0\sigma) \geqslant \sum_{\sigma \in G(K/F)} \min\left\{v\left(\frac{x_2}{x_1}\right), \ldots, v\left(\frac{x_n}{x_1}\right), v(\lambda_0\sigma)\right\}.$$

Now let v be any infinite valuation in Ω_K. Denote by v_F a valuation in Ω_F which is the restriction of v to F. By $r_F = r_L$ there is only one valuation v_L in Ω_L, which is the restriction of v_F to L. Further, let e and e_1 be the ramification indices of v over L and of v over F, respectively. Using the property (2) from [8] we get

$$(10) \qquad v\left(\frac{c}{N_{K/L}(x_1)}\right) = v(N_{K/L}(y+\lambda_0)) = e\, v_L(N_{K/L}(y+\lambda_0))$$
$$= e\, v_L(N_{F/L}(N_{K/F}(y+\lambda_0))) = e \sum_{v_F|v_L} v_F(N_{K/F}(y+\lambda_0))$$
$$= e\, v_F(N_{K/F}(y+\lambda_0)) = \frac{e}{e_1} v(N_{K/F}(y+\lambda_0)).$$

Put $\mu = N_{K/F}(y+\lambda_0)$. Combining (9) and (10) we obtain

$$(11) \qquad H_K(\mu) \leqslant dH_K\left(\frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}\right) + dH_K(\lambda_0) + dH_K\left(\frac{c}{N_{K/L}(x_1)}\right)$$
$$\leqslant d(d+2)H + dH_K(\lambda) + dH_K(c).$$

In view of $y \in F$ the equation $N_{K/F}(y+\lambda_0) = \mu$ means that y is a root of the polynomial $f(x) = \prod_{\sigma \in G(K/F)} (y+\lambda_0\sigma) - \mu$. Similarly, as in point I we obtain that

$$H_K(y) \leqslant H_K(f) \leqslant dH_K(\lambda_0) + H_K(\mu).$$

Combining it with (11) we get

$$(12) \qquad H_K(x) = H_K(x_1 y) \leqslant (d^2+3d+1)H + 2dH_K(\lambda) + dH_K(c).$$

II.B. Let us consider now the case where $[F:L] > n$. In this case there exists a set X consisting of $n+1$ elements of $G(K/L)$ which act pairwise differently on F (that is, $n+1$ elements from distinct right cosets of $G(K/F)$ in $G(K/L)$). The $n+1$ linear forms

$$x\sigma = \sum_{i=1}^{n} \alpha_i(x_i\sigma) \qquad (\sigma \in X)$$

in the n variables $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$ are linearly dependent over K, hence there

exist non-zero elements A_σ, $\sigma \in X$ in K such that

$$(13) \qquad \sum_{\sigma \in X} A_\sigma(x\sigma) = 0$$

holds for all x in M. The coefficients A_σ, $\sigma \in X$ can be obtained as maximal non-vanishing minors of the matrix with elements $x_i\sigma$, $\sigma \in X$, $1 \leqslant i \leqslant n$, whence

$$(14) \qquad H_K(A_\sigma, \sigma \in X) \leqslant |X| \cdot H = (n+1)H.$$

(13) implies

$$(15) \qquad \sum_{\sigma \in X} A_\sigma(x\sigma+\lambda\sigma) + \Lambda = 0$$

where $\Lambda = -\sum_{\sigma \in X} A_\sigma(\lambda\sigma)$ and using (14)

$$(16) \qquad H_K(\Lambda) \leqslant (n+1)(H + H_K(\lambda)).$$

Let us consider the summands $A_\sigma(x\sigma+\lambda\sigma)$, $\sigma \in X$ and Λ in (15). Among these summands Λ may be zero but others are non-zero.

Equation (15) may yield the following subcases (a1, a2, b).

a. First suppose that there are two non-zero elements of $A_\sigma(x\sigma+\lambda\sigma)$, $\sigma \in X$ and Λ which are linearly dependent over k.

a1. If $\Lambda \neq 0$ and for some $\sigma \in X$, $A_\sigma(x\sigma+\lambda\sigma)$ and Λ are linearly dependent over k then by (14) and (16) we get

$$(17) \qquad H_K(x) < 2(n+1)H + (n+2)H_K(\lambda).$$

a2. If for some $\sigma, \sigma^* \in X$, $A_\sigma(x\sigma+\lambda\sigma)$ and $A_{\sigma^*}(x\sigma^*+\lambda\sigma^*)$ are linearly dependent over k then we immediately get (22) and we may continue our arguments after (22).

b. Suppose now that any two non-zero elements of $A_\sigma(x\sigma+\lambda\sigma)$, $\sigma \in X$ and Λ are linearly independent over k. In this case by (15) there exists a minimal subset of non-zero summands of (15) consisting of at least three elements, which are linearly dependent over k, but no proper subset of which is linearly dependent over k. Hence there is a subset Y of X and there are non-zero coefficients k_σ, $\sigma \in Y$ and k_Λ in k such that either we have an equation of the form

$$(18) \qquad \sum_{\sigma \in Y} k_\sigma A_\sigma(x\sigma+\lambda\sigma) + k_\Lambda \Lambda = 0$$

if $\Lambda \neq 0$ and Λ is an element of the above minimal subset; or we have an equation of the form

$$(19) \qquad \sum_{\sigma \in Y} k_\sigma A_\sigma(x\sigma+\lambda\sigma) = 0$$

if Λ is not an element of this minimal subset. Further, in equations (18), (19) any proper subset of the summands is linearly independent over k. In order to apply our lemma to the above equations let $\mathscr{S}$ be the set of those valuations in Ω_K at which one or more of the following occur:

$v(A_\sigma) \neq 0$ $(\sigma \in X)$; $v(x_i\sigma) < 0$ $(\sigma \in G(K/L),\ 1 \leqslant i \leqslant n)$;
$v(\lambda\sigma) < 0$ $(\sigma \in G(K/L))$; $v(\Lambda) \neq 0$; $v(c) > 0$;
v is infinite valuation.

Then the summands in equations (18), (19) are all $\mathscr{S}$-units and for the cardinality of $\mathscr{S}$ we have

$$|\mathscr{S}| \leqslant (n+2)\,H_K(A_\sigma,\ \sigma \in X) + dH + dH_K(\lambda) + 2H_K(\Lambda) + H_K(c) + r. \tag{20}$$

If we have an equation of the form (18) then applying our lemma to (18) we obtain

$$H_K\left(\frac{A_\sigma(x\sigma+\lambda\sigma)}{\Lambda}\right) < \frac{n(n+1)}{2}(|\mathscr{S}|+2g-2) \quad \text{for some } \sigma \in Y.$$

Using (14), (16) and (20), from this we get

$$H_K(x) \leqslant \tfrac{1}{2}n(n+1)\left[(n^2+7n+6+d)\,H + (3n+4+d)\,H_K(\lambda) + H_K(c) + r + 2g - 2\right]. \tag{21}$$

Otherwise, if we have an equation of the form (19) then by our lemma we have

$$H_K\left(\frac{A_\sigma(x\sigma+\lambda\sigma)}{A_{\sigma^*}(x\sigma^*+\lambda\sigma^*)}\right) < \frac{n(n+1)}{2}(|\mathscr{S}|+2g-2) \tag{22}$$

for some distinct $\sigma, \sigma^* \in Y$. Put $\tau = \sigma^{-1}\sigma^*$ and $t = (x+\lambda)/(x\tau+\lambda\tau)$. Using (14), from the above inequality we get

$$H_K(t) \leqslant \tfrac{1}{2}n(n+1)(|\mathscr{S}|+2g-2) + 2(n+1)H. \tag{23}$$

By an argument of Mason [13] we may extend $x_1, \ldots, x_n$ to a basis $x_1, \ldots, x_d$ of K over L such that

$$H^* = H_K(x_1, \ldots, x_d) \leqslant H + 2g + d. \tag{24}$$

There exist elements γ_{ij}, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant d$ in L such that

$$t(x_i\tau) = \sum_{j=1}^{d} \gamma_{ij}x_j \quad (1 \leqslant i \leqslant n). \tag{25}$$

For fixed i, the elements γ_{ij}, $1 \leqslant j \leqslant d$ can be determined from the linear equation system

$$(t\sigma)(x_i\tau\sigma) = \sum_{j=1}^{d} \gamma_{ij}(x_j\sigma) \quad (\sigma \in G(K/L))$$

by Cramer's rule and we get

$$H_K(\gamma_{ij};\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant d) \leqslant 2dH^* + dH_K(t) + dH. \tag{26}$$

Put $\alpha_j = 0$ for $j = n+1, \ldots, d$. Then from the definition of t we obtain

$$(x+\lambda)/t = x\tau + \lambda\tau = \sum_{i=1}^{n} \alpha_i(x_i\tau) + \lambda\tau$$

whence by (25) we get

$$\sum_{j=1}^{d} \alpha_j x_j = x = \sum_{i=1}^{n} \alpha_i\, t(x_i\tau) + [t(\lambda\tau) - \lambda] = \sum_{i=1}^{n} \alpha_i \sum_{j=1}^{d} \gamma_{ij}x_j + \Lambda_0 = \sum_{j=1}^{d} x_j\Big(\sum_{i=1}^{n} \alpha_i\gamma_{ij} + \Lambda_{0j}\Big) \tag{27}$$

where Λ_{0j} $(1 \leqslant j \leqslant d)$ denote the components of $\Lambda_0 = t(\lambda\tau) - \lambda$ in the base $x_1, \ldots, x_d$ $(\Lambda_{0j} \in L,\ 1 \leqslant j \leqslant d)$. These components can be obtained from the linear equation system

$$\Lambda_0\sigma = \sum_{j=1}^{d} \Lambda_{0j}(x_j\sigma) \quad (\sigma \in G(K/L))$$

and we have

$$H_K(\Lambda_{01}, \ldots, \Lambda_{0d}) \leqslant 2dH^* + dH_K(\Lambda_0) \leqslant 2dH^* + 2dH_K(\lambda) + dH_K(t). \tag{28}$$

Since $x_1, \ldots, x_d$ is a base of K over L and α_j, γ_{ij}, Λ_{0j} $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant d)$ are in L, hence (27) implies

$$\alpha_j = \sum_{i=1}^{n} \alpha_i\gamma_{ij} + \Lambda_{0j} \quad (1 \leqslant j \leqslant d)$$

that is, we have an equation system of the form

$$\Gamma\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{bmatrix} = \begin{bmatrix}-\Lambda_{01}\\ \vdots\\ -\Lambda_{0d}\end{bmatrix} \tag{29}$$

in $\alpha_1, \ldots, \alpha_n$ where

$$\Gamma = \begin{bmatrix} (\gamma_{11}-1) & \gamma_{21} & \ldots & \gamma_{n1} \\ \gamma_{12} & (\gamma_{22}-1) & \ldots & \gamma_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ \gamma_{1n} & \gamma_{2n} & \ldots & (\gamma_{nn}-1) \\ \gamma_{1,n+1} & \gamma_{2,n+1} & \ldots & \gamma_{n,n+1} \\ \ldots & \ldots & \ldots & \ldots \\ \gamma_{1d} & \gamma_{2d} & \ldots & \gamma_{nd} \end{bmatrix}$$

is a matrix of type $d \times n$.

If any element of Γ is zero then (25) is of the form $t(x_i\tau)=x_i$ $(1\leqslant i\leqslant n)$, that is

$$\left(\frac{x_i}{x_1}\right)\tau=\frac{x_i}{x_1}\qquad(1\leqslant i\leqslant n),$$

so τ is the identity map on F in contradiction with our construction. Thus there must be non-zero elements of Γ. We may have two possible cases (1,2):

1. First suppose that any row of Γ contains at most one non-zero element. Suppose that the jth row contains $\gamma\neq 0$ and for simplicity we may assume that γ is in the first column. Then we have

$$\gamma\alpha_1=-\Lambda_{0j},$$

that is

$$\alpha_1 x_1=-\Lambda_{0j}x_1/\gamma.$$

In this case let

$$\bar{x}=\alpha_2 x_2+\ldots+\alpha_n x_n\quad\text{and}\quad\bar{\lambda}=\lambda-\frac{\Lambda_{0j}x_1}{\gamma}.$$

Hence $x+\lambda$ can be written in the form $\bar{x}+\bar{\lambda}$, where $\bar{x}$ is an element of the free $\mathcal{O}$-module $\bar{M}$ of rank $n-1$ generated by $x_2,\ldots,x_n$ and $\bar{\lambda}\in K$. We have

$$\bar{H}=H_K(x_2,\ldots,x_n)\leqslant H \tag{30}$$

and

$$H_K(\bar{\lambda})\leqslant H_K(\lambda)+H_K(\Lambda_{0j};\ 1\leqslant j\leqslant d)+H \tag{31}$$
$$+H_K(\gamma_{ij};\ 1\leqslant i\leqslant n,\ 1\leqslant j\leqslant d).$$

Further, $\bar{M}$ is obviously non-degenerate, since M is non-degenerate and $\bar{M}$ is a submodule of M.

2. Let us assume now that there is a j $(1\leqslant j\leqslant d)$ such that the jth row of Γ (denote the elements of it by $\gamma_1,\ldots,\gamma_n$) contains at least two non-zero elements. For simplicity let us suppose that $\gamma_1\neq 0$ and $\gamma_2\neq 0$. Then we have an equation of the form

$$\gamma_1\alpha_1+\ldots+\gamma_n\alpha_n+\Lambda_{0j}=0,$$

whence

$$\alpha_1=-\frac{\gamma_2}{\gamma_1}\alpha_2-\ldots-\frac{\gamma_n}{\gamma_1}\alpha_n-\frac{\Lambda_{0j}}{\gamma_1}.$$

Then we get

$$x+\lambda=\alpha_1 x_1+\ldots+\alpha_n x_n+\lambda=\alpha_2 y_2+\ldots+\alpha_n y_n+\bar{\lambda}$$

where

$$y_i=x_i-x_1\frac{\gamma_i}{\gamma_1}\quad(2\leqslant i\leqslant n)\quad\text{and}\quad\bar{\lambda}=\lambda-x_1\frac{\Lambda_{0j}}{\gamma_1}.$$

Thus we obtain again that $x+\lambda$ can be written in the form $\bar{x}+\bar{\lambda}$, where $\bar{x}$ is an element of the free $\mathcal{O}$-module $\bar{M}$ generated by $y_2,\ldots,y_n$ and $\bar{\lambda}\in K$ for which we have (31) as before. Further,

$$\bar{H}=H_K(y_2,\ldots,y_n)\leqslant H_K(\gamma_{ij};\ 1\leqslant i\leqslant n,\ 1\leqslant j\leqslant d)+H \tag{32}$$

and $\bar{M}$ is again a non-degenerate $\mathcal{O}$-module, since $\bar{M}$ is a submodule of M.

Put $M_n=M$, $M_{n-1}=\bar{M}$, $x_n=x$, $x_{n-1}=\bar{x}$, $\lambda_n=\lambda$, $\lambda_{n-1}=\bar{\lambda}$, $H_n=H$, $H_{n-1}=\bar{H}$ and let us summarize our results in the proof of the theorem. If $x_n\in M_n$ and $\lambda_n\in K$ is a solution of equation (4) then there are two possibilities.

Firstly, if we get to (7), (12), (17) or (21) then we obtain a bound for $H_K(x_n)$. Combining the above estimates we have

$$H_K(x_n)\leqslant C\big(H_n+H_K(\lambda_n)\big)+D \tag{33}$$

where

$$C=\tfrac{1}{2}n(n+1)(d^2+8d+6)\quad\text{and}\quad D=\tfrac{1}{2}n(n+1)\big(r+2g-2+dH_K(c)\big).$$

Secondly, if we cannot immediately give a bound for $H_K(x_n)$ then there exists x_{n-1}, λ_{n-1} such that $x_n+\lambda_n=x_{n-1}+\lambda_{n-1}$ where x_{n-1} is an element of a free non-degenerate $\mathcal{O}$-module M_{n-1} of rank $n-1$ and $\lambda_{n-1}\in K$. Combining (16), (20), (23), (24), (26) and (28), by (30) and (32) for the height of the generators of M_{n-1} we have

$$H_{n-1}\leqslant A\big(H_n+H_K(\lambda_n)\big)+B \tag{34}$$

and by (31)

$$H_K(\lambda_{n-1})\leqslant A\big(H_n+H_K(\lambda_n)\big)+B, \tag{35}$$

where

$$A=dn(n+1)(n^2+7n+10+d),$$
$$B=dn(n+1)\big(r+6g+2d+H_K(c)\big).$$

Further, from (35) and the equation $x_n=x_{n-1}+\lambda_{n-1}-\lambda_n$ we obtain

$$H_K(x_n)\leqslant H_K(x_{n-1})+A\big(H_n+H_K(\lambda_n)\big)+B. \tag{36}$$

(We remark that in (35) $A-1$ is also sufficient instead of A.)

If we repeat our arguments then we obtain a sequence M_n, M_{n-1}, $M_{n-2},\ldots$ of free non-degenerate $\mathcal{O}$-modules and two sequences x_n, x_{n-1}, $x_{n-2},\ldots$ and λ_n, λ_{n-1}, $\lambda_{n-2},\ldots$ of elements with the following properties:

M_i is of rank i, $x_i\in M_i$, $\lambda_i\in K$ such that

$$x_i+\lambda_i=x_{i+1}+\lambda_{i+1}$$

and for the height H_i of the generators of M_i (cf. (34))

$$H_i\leqslant A\big(H_{i+1}+H_K(\lambda_{i+1})\big)+B. \tag{37}$$

Further (cf. (35))

$$H_K(\lambda_i) \leqslant A\left(H_{i+1}+H_K(\lambda_{i+1})\right)+B \tag{38}$$

and (cf. (36))

$$H_K(x_{i+1}) \leqslant H_K(x_i)+A\left(H_{i+1}+H_K(\lambda_{i+1})\right)+B. \tag{39}$$

In each step either we obtain

$$H_K(x_i) \leqslant C\left(H_i+H_K(\lambda_i)\right)+D \tag{40}$$

(see (33)) and stop the procedure, or we continue with M_{i-1}, x_{i-1}, λ_{i-1}.

For simplicity let $S_i = H_i+H_K(\lambda_i)$ for any i and denote by i_0 the index where the procedure stops (obviously $i_0 \geqslant 1$). By (40) we have

$$H_K(x_{i_0}) \leqslant CS_{i_0}+D. \tag{41}$$

Further, it follows from (37) and (38) that

$$S_i \leqslant (2A)^{n-i}\left(S_n+2\frac{B}{A}\right) \tag{42}$$

for any i. Finally, by (39) we get

$$H_K(x_n) \leqslant A(S_{i_0+1}+\ldots+S_n)+(n-1)B+H_K(x_{i_0}). \tag{43}$$

Combining (41), (42) and (43) we obtain

$$H_K(x_n) \leqslant A(2A)^{n-1}\left(H+2\frac{B}{A}\right)+A(2A)^{n-1}H_K(\lambda_n)+nB.$$

By our condition on $H_K(\lambda_n)$ we have $A(2A)^{n-1}H_K(\lambda_n) < \frac{1}{2}H_K(x_n)$, whence the assertion (5) of our theorem follows.

Proof of Corollary 2. We remark only that the $\mathcal{O}$-module $M = \{1, \alpha\}$ is non-degenerate. The assertion follows from the theorem in view of

$$\max\left(H_K(x), H_K(y)\right) \leqslant 4H_K(\alpha)+2H_K(x+\alpha y).$$

References

[1] A. Baker, *Contributions to the theory of Diophantine equations*, Phil. Trans. Roy. Soc. London, A 263 (1968), 173–208.

[2] B. Brindza, *On the equation $F(x, y) = z^n$ over function fields*, Acta Math. Hungar. 49 (1987), 267–275.

[3] B. Brindza and I. Gaál, *Inhomogeneous norm form equations in two dominating variables over function fields*, Acta Math. Hungar. 50 (1987), 147–153.

[4] W. D. Brownawell and D. W. Masser, *Vanishing sums in function fields*, to appear.

[5] I. Gaál, *Norm form equations with several dominating variables and explicit lower bounds for inhomogeneous linear forms with algebraic coefficients*, Studia Sci. Math. Hungar. 19 (1984), 399–411.

[6] — *Norm form equations with several dominating variables and explicit lower bounds for inhomogeneous linear forms with algebraic coefficients, II*, ibid. 20 (1985), 333–344.

[7] K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Applied Math., No. 56, Kingston, Canada, 1980.

[8] — *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.

[9] — *On norm form, discriminant form and index form equations*, Coll. Math. Soc. János Bolyai 34., Budapest, 1981. *Topics in Classical Number Theory*, North-Holland Publ. Comp., Amsterdam 1984, pp. 617–676.

[10] K. Győry and Z. Z. Papp, *Norm form equations and explicit lower bounds for linear forms with algebraic coefficients*, Studies in Pure Mathematics (To the Memory of Paul Turán), Akadémiai Kiadó, Budapest 1983, pp. 245–267.

[11] R. C. Mason, *On Thue's equation over function fields*, J. London Math. Soc., Ser. 2, 24 (1981), 414–426.

[12] — *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Series, No. 96, Cambridge 1984.

[13] — *Norm form equations I*, J. Number Theory 22 (1986), 190–207.

[14] — *Norm form equations IV: Rational functions*, Mathematika 33 (1986), 204–211.

[15] — *Norm form equations V: Degenerate modules*, J. Number Theory 25 (1987), 239–248.

[16] C. F. Osgood, *An effective lower bound on the diophantine approximation of algebraic functions by rational functions*, Mathematika 20 (1973), 4–15.

[17] — *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.

[18] W. M. Schmidt, *On Osgood's effective Thue theorem for algebraic functions*, Commun. on Pure and Applied Math. 29 (1976), 759–773.

[19] — *Thue's equation over function fields*, J. Austral. Math. Soc., Ser. A, 25 (1978), 385–422.

[20] — *Polynomial solutions of $F(x, y) = z^n$*, Proc. Queen's Number Theory Conf., 1979, Queen's Papers in Pure and Applied Math., No. 54, Kingston, Canada, 1980, pp. 33–65.

[21] V. G. Sprindžuk, *Representation of numbers by norm forms with two dominating variables*, J. Number Theory 6 (1974), 481–486.

[22] S. A. Stepanov, *Diophantine equations over function fields* (in Russian), Mat. Sbornik 112 (1980), 86–93.

KOSSUTH LAJOS UNIVERSITY
MATHEMATICAL INSTITUTE
4010 Debrecen Pf. 12, Hungary

Received on 22. 9. 1986 (1673)