Nun gilt
\[
\frac{1}{\sqrt{\mu}} x \circ \psi_k(1, x) \circ \psi_k^{-1} = \sum_{j=0}^{\left\lfloor \frac{2}{k} \right\rfloor} \frac{k}{j} \binom{k-1}{j} (-1)^j u^{k-1} v^{2-1} x^{k-2j} \mod p^r,
\]

wenn \( v \) so gewählt wird, daß \( uv \equiv 1 \mod p^r \). Da aber das zuletzt erhaltene Polynom genau dann ein \( \text{PP} \mod p \) ist, wenn \( (k, \ p^r - 1) = 1 \), und genau dann ein \( \text{PP} \mod p^r \) mit \( e > 1 \) ist, wenn \( (k, \ p(2^e - 1)) = 1 \) (vgl. etwa [2]), gilt
\[
\text{Satz 8. \ Das mit } \sqrt{\mu}(ru + s) \text{ Transformierte von } g_k(1, x) \text{ mit } k > 1 \text{ ist genau dann Permutationspolynom } \mod p^\theta, \text{ wenn } (ur, p) = p \text{ sowie } (k, \ p) = 1, \text{ und wenn } (ur, p) = 1 \text{ sowie } (k, \ p^2 - 1) = 1 \text{ für } e = 1 \text{ bzw. } (k, \ p(p^2 - 1)) = 1 \text{ für } e > 1.
\]

Die Berechnung der Fixpunktzahl der Permutationen \( x \rightarrow i^{-1} \circ \psi_k(1, x) \circ \psi_k^{-1} \mod p^\theta \) und die Ermittlung der Struktur der von diesen Permutationen bei festem \( \ell \) gebildeten Permutationsgruppe modulo \( p^\ell \) 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


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

Inhomogeneous norm form equations over function fields

by

I. GAAL (Debrecen)

I. 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. Györy [7], [9].

In 1974 Sprindz̆uk [21] gave an inhomogeneous generalization of Baker’s result. He obtained effective bounds for all solutions of the equation
\[
N_{K/Q}(x + ay + \lambda) = m
\]
where \( K = Q(a) \) is an algebraic number field of degree \( \geq 3 \), \( 0 \neq m \in \mathbf{Z} \) and the variables are \( x, y \in \mathbf{Z} \) and \( (1) \lambda \in K. \) Here \( \lambda \) is a non-dominating variable such that \( (2) \mid \lambda \mid < (\max\{|x|, |y|\})^{1-\varepsilon} \) (\( 0 < \varepsilon < 1 \) is a given constant). In the special case \( \lambda = 0 \) this theorem gives the above mentioned result of Baker.

Combining the method of Sprindz̆uk [21] with that of Györy and Papp [10], in [5], [6], we extended Sprindz̆uk’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], Györy [8] and Brindza [2] gave effective bounds for the solutions of Thue equations. Györy [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

\(\ell \in K \) denotes the ring of integers of an algebraic number field \( K. \)

\( |\lambda| \) is the size of an algebraic number \( \lambda, \) 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 $k(x)$ be the field of rational functions over $k$. If $K$ is any finite extension field of $k(x)$, denote by $\Omega_k$ the set of all (additive) valuations on $K$ with value group $\mathbb{Z}$. The valuation $v \in \Omega_k$ is called finite if $v(x) > 0$, otherwise $v$ is called infinite.

For any non-zero $\alpha \in K$ the additive height of $\alpha$ 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

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

$$H_K(\alpha + \beta) \leq H_K(\alpha) + H_K(\beta),$$

$$H_K(\alpha\beta) \leq H_K(\alpha) + H_K(\beta)$$

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

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

If $1 \in \mathcal{S}$ and $0 \notin \mathcal{S} \subseteq K$ then we have

$$H_K(\mathcal{S}) \leq H_K(\mu, \mathcal{S})$$

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

$$w(N_{L/K}(\alpha)) = \sum_{v \in \Omega_k} v(\alpha)$$

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 $k(x)$ with $L \subseteq K$. Denote by $\mathcal{O}$ the ring of elements of $L$ integral over $k(x)$. Let $M$ be a finitely generated $\mathcal{O}$-module in $K$. For any field $F$ lying between $L$ and $K$ let

$$M^F = \{m \in M \mid \forall v \in \mathfrak{F} : 0 \leq 3 \in L \text{ with } |m|_v \}. $$

$M^F$ is a submodule of $M$, it is either $\{0\}$ or the rank of $M^F$ is $\geq [F:L]$. $M$ 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

$$N_{L/K}(x) = c$$

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

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

in $x \in M$ and $\lambda \in K$. Under the condition that the height of $\lambda$ 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 $H_K(x_1, \ldots, x_n) \leq H$. 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

$$H_K(x) < 2^{2n+3} [(d^2(n+1)^3)]^n (H + r + g + H_K(c) + 1).$$
The condition of non-degeneracy of \( M \) is necessary since otherwise even equation (3) (which is a special case of (4) restricting the variable \( \lambda \) 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 \( \mathcal{K} \)-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 \( \geq 3 \) over \( L \). If \( x, y \in \mathcal{O} \) and \( \lambda \in K \) is a solution of

\[
N_{K/L}(x + ay + \lambda) = c
\]

with \( H_k(\lambda) < \epsilon_0 \max \{H_k(x), H_k(y)\} \), where \( \epsilon_0 = (2^{25} d^4 H_k(\alpha)^{-1}) \), then we have

\[
\max \{H_k(x), H_k(y)\} < 2^{27} d^6 (H_k(\alpha) + r + g + H_k(c) + 1).
\]

The result of Corollary 2 may be compared with that special case of the Theorem of [3] when \( \mathcal{K} \) 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 \( \lambda \) (cf. [13]).

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

**Lemma.** Let \( \mathcal{K} \) be a finite subset of \( \Omega_k \) and let \( u_1, \ldots, u_n \) be \( \mathcal{K} \)-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

\[
H_k\left(\frac{u_2}{u_1}, \ldots, \frac{u_n}{u_1}\right) \leq \frac{1}{2}(n-1)(n-2)[|\mathcal{K}| + 2g - 2]
\]

where \( |\mathcal{K}| \) denotes the cardinality of \( \mathcal{K} \).

Our lemma is Corollary I of Brownwell 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, \( x = x_1 x_1 \) with \( x_1 \in \mathcal{O} \). Put \( \lambda_0 = \lambda/x_1 \); then equation (4) can be written in the form

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

It means that \( x_1 \) is a root of the polynomial

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

We recall that the height \( H_k(f) \) of a polynomial \( f \) in \( K[x] \) is defined by \( H_k(f) \) where \( f \) is the set of its coefficients. Since \( f(\lambda_0) = \prod_{\sigma \in \mathcal{K}\{\lambda_0\}} (\lambda_0 \sigma) \) is a power of the minimal defining polynomial of \( \lambda_0 \) over \( L \), hence by Lemma 4 of Mason [12] we can see that \( H_k(f) \leq dH_k(\lambda_0) \). Obviously,

\[
H_k(f) \leq H_k(f_1) + H_k\left(\frac{c}{N_{K/L}(x_1)}\right).
\]

It follows from the Corollary to Lemma 4 of Mason [12] that \( H_k(x_1) \leq H_k(f) \). Combining our results, we obtain

\[
H_k(x_1) = H_k(x_1 x_1) \leq (2d + 1) H + dH_k(\lambda) + H_k(c).
\]

II. Now let us suppose that \( n > 1 \). Denote by \( F \) the field generated by \( x_1/x_1, x_2/x_1, \ldots, x_n/x_1 \) over \( L \). Since \( x_1, x_2, \ldots, x_n \) are linearly independent over \( L \), hence 1, \( x_1/x_1, x_2/x_1, \ldots, x_n/x_1 \) are also linearly independent over \( L \), that is \( [F:L] \geq n \). 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 \( \{1, x_1/x_1, \ldots, x_n/x_1\} \) is a basis of \( F \) over \( L \). Any \( j \in F \) can be written as

\[
j = \sum_{i=1}^{n} a_i \frac{x_i}{x_1} \quad \text{with} \quad a_1, \ldots, a_n \in L.
\]

Denote by \( l \) an element of \( L \) such that \( a_1, \ldots, a_n \in \mathcal{O} \); then \( \{x_1, \ldots, x_n\} \) is in \( M^F \), that is, \( x_i \in M^F \). By our assumption \( M \) is non-degenerate; hence \( M^F \neq \{0\} \) implies \( r_F = r_1 \).

If \( x = x_1 x_4 + \ldots + x_n x_n \) \((\alpha_1, \ldots, \alpha_n \in \mathcal{O}) \) is in \( M \) then \( y = x/x_1 = x_1 x_2/x_1 + \ldots + x_n x_n/x_1 \) is in \( F \). Further, put \( \lambda_0 = \lambda/x_1 \). Then equation (4) can be written in the form

\[
N_{K/L}(y + \lambda_0) = \frac{c}{N_{K/L}(x_1)}.
\]

5 - Acta Arithmetica 51,1
We are interested in the values of $N_{K/L}(y + \lambda_0)$ at different valuations $v \in \Omega_K$.

Let $v$ be an arbitrary finite valuation in $\Omega_K$. Then we have

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

Now let $v$ be any infinite valuation in $\Omega_K$. Denote by $v_F$ a valuation in $\Omega_F$ which is the restriction of $v$ to $F$. By $r_F = r_L$, there is only one valuation $v_L$ in $\Omega_L$ 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

$$v\left(\frac{c}{N_{K(L)(x_1)}}\right) = v(N_{K/L}(y + \lambda_0)) = e v_L(N_{K/L}(y + \lambda_0)) = e \sum_{v_F \not\subseteq L} v_F(N_{K/F}(y + \lambda_0)) = e \sum_{v_F \not\subseteq L} v_F(N_{K/F}(y + \lambda_0)).$$

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

$$H_K(\mu) \leq d H_K\left(\frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}\right) + d H_{K}(\lambda_0) + d H_K\left(\frac{c}{N_{K(L)(x_1)}}\right) \leq d(d+2)H + d H_K(\lambda) + d H_K(c).$$

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

$$H_K(y) \leq H_K(f) \leq d H_K(\lambda_0) + H_K(\mu).$$

Combining it with (11) we get

$$H_K(x) = H_K(x_1, y) \leq (d^2 + 3d + 1)H + 2d H_K(\lambda) + d H_K(c).$$

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 tight cosets of $G(K/F)$ in $G(K/L)$). The $n + 1$ linear forms

$$x_\sigma = \sum_{i=1}^n a_i(x_i \sigma) \quad (\sigma \in X)$$

in the $n$ variables $x_1, \ldots, x_n \in \mathcal{O}$ are linearly dependent over $K$, hence there exist non-zero elements $A_\sigma, \sigma \in X$ in $K$ such that

$$\sum_{\sigma \in X} A_\sigma(x_\sigma) = 0$$

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

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

(13) implies

$$\sum_{\sigma \in X} A_\sigma(x_\sigma + \lambda \sigma) + A = 0$$

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

$$H_K(A) \leq (n + 1)(H + H_K(\lambda)).$$

Let us consider the summands $A_\sigma(x_\sigma + \lambda \sigma), \sigma \in X$ and $A$ in (15). Among these summands $A$ 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 $A$ which are linearly dependent over $k$.

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

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

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 $A$ 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 $k_\sigma, \sigma \in Y$ and $k_A$ in $K$ such that either we have an equation of the form

$$\sum_{\sigma \in Y} k_\sigma A_\sigma(x_\sigma + \lambda \sigma) + k_A A = 0$$

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

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

(18)
if $A$ 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 $S$ be the set of those valuations in $\Omega_K$ at which one or more of the following occur:

- $v(A) \neq 0$ (if $\sigma \in X$);
- $v(x, \sigma) < 0$ (if $\sigma \in G(K/L)$, $1 \leq i \leq n$);
- $v(\lambda \sigma) < 0$ (if $\sigma \in G(K/L)$);
- $v(A) \neq 0$;
- $v(c) > 0$;

$v$ is infinite valuation.

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

- $|S| \leq (n+2) H_K(A, \sigma \in X) + d H + d H_K(\lambda) + 2 H_K(A) + H_K(c) + r$.

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

- $H_K(A \sigma + x \lambda \sigma) \leq \frac{n(n+1)}{2} (|S| + 2g - 2)$ for some $\sigma \in Y$.

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

- $H_K(x) \leq \frac{1}{2} n(n+1)(n^2 + 7n + 6 + d) H + (3n + 4 + d) H_K(\lambda) + H_K(c) + r + 2g - 2$.

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

- $H_K\left(\frac{A \sigma + x \lambda \sigma}{A \sigma + x \lambda \sigma}\right) < \frac{n(n+1)}{2} (|S| + 2g - 2)$

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

- $H_K(t) \leq \frac{1}{2} n(n+1)(|S| + 2g - 2) + 2(n+1) H$.

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

- $H^* = H_K(x_1, \ldots, x_d) \leq H + 2g + d$.

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

- $t(x_i \tau) = \sum_{j=1}^{d} y_{ij} x_j$ (1 $\leq i \leq n$).

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

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

by Cramer's rule and we get

- $H_K(y_{ij}, 1 \leq i \leq n, 1 \leq j \leq d) \leq 2d H^* + d H_K(\lambda) + d H$.

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

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

whence by (25) we get

- $\sum_{j=1}^{d} x_j x_j = x = \sum_{i=1}^{n} a_i t(x_i \tau) + [t(\lambda \tau) - \lambda]$

where $A_{ij}$ (1 $\leq i \leq j \leq d$) denote the components of $A_0 = t(\lambda \tau) - \lambda$ in the base $x_1, \ldots, x_d$ ($A_{ij} \in L, 1 \leq i \leq j \leq d$). These components can be obtained from the linear system

- $A_0 \sigma = \sum_{j=1}^{d} A_{ij} (x_j \sigma) \quad (\sigma \in G(K/L))$

and we have

- $H_K(A_{ij}, \ldots, A_{ij}) \leq 2d H^* + d H_K(\lambda) + 2d H^* + 2d H_K(\lambda) + d H_k(t)$.

Since $x_1, \ldots, x_d$ is a basis of $K$ over $L$ and $x_i, y_{ij}, A_{ij}$ (1 $\leq i \leq n, 1 \leq j \leq d$) are in $L$, hence (27) implies

- $a_j = \sum_{i=1}^{n} a_i y_{ij} + A_{ij}$ (1 $\leq j \leq d$)

that is, we have an equation system of the form

- $\Gamma \left[ \begin{array}{c} a_1 \\ \vdots \\ a_n \end{array} \right] = \left[ \begin{array}{c} -A_{1j} \\ \vdots \\ -A_{nj} \end{array} \right]$

in $a_1, \ldots, a_n$ where

- $\Gamma = \left[ \begin{array}{cccc} (y_{11} - 1) & y_{12} & \cdots & y_{1n} \\ y_{12} & (y_{22} - 1) & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{1n} & y_{2n} & \cdots & (y_{nn} - 1) \end{array} \right]$
If any element of $\Gamma$ is zero then (25) is of the form $t(x; \tau) = x_i \quad (1 \leq i \leq n)$, that is

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

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

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

$$\gamma x_1 = -A_{j0},$$

that is

$$a_1 x_1 = -A_{j0} x_1 / \gamma.$$

In this case let

$$\bar{x} = x_2 x_2 + \ldots + a_n x_n \quad \text{and} \quad \bar{\lambda} = \lambda - \frac{A_{j0} x_1}{\gamma}.$$ 

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

$$\bar{H} = H_K(x_2, \ldots, x_n) \leq H$$

and

$$H_K(\bar{\lambda}) \leq H_K(\lambda) + H_K(A_{j0}; 1 \leq j \leq d) + H$$

+ $H_K(\gamma_{j0}; 1 \leq i \leq n, 1 \leq j \leq d).$

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 $j$ $(1 \leq j \leq d)$ such that the $j$th row of $\Gamma$ (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

$$\gamma_1 a_1 + \ldots + \gamma_n a_n + A_{j0} = 0,$$

whence

$$a_1 = -\frac{\gamma_2}{\gamma_1} a_2 - \ldots - \frac{\gamma_n}{\gamma_1} a_n - \frac{A_{j0}}{\gamma_1}.$$ 

Then we get

$$x + \lambda = a_1 x_1 + \ldots + a_n x_n + \lambda = a_2 y_2 + \ldots + a_n y_n + \bar{\lambda},$$

where

$$y_i = x_i - x_1 \frac{\gamma_i}{\gamma_1} \quad (2 \leq i \leq n) \quad \text{and} \quad \bar{\lambda} = \lambda - x_1 \frac{A_{j0}}{\gamma_1}.$$ 

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 $\mathfrak{c}$-module $\bar{M}$ generated by $y_2, \ldots, y_n$ and $\bar{\lambda} \in K$ for which we have (31) as before. Further,

$$(32) \quad \bar{H} = H_K(y_2, \ldots, y_n) \leq H_K(\gamma_j; 1 \leq i \leq n, 1 \leq j \leq d) + H$$

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

Put $M_n = M$, $M_{n-1} = \bar{M}$, $y_2 = x_{n-1}$, $y_{n-1} = \lambda$, $\lambda_{n-1} = \lambda$, $H_{n-1} = H$, $H_{n-1} = H$ and let us summarize our results in the proof of the theorem. If $x_n \in M_n$ and $\lambda \in K$ 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

$$(33) \quad H_K(x_n) \leq C(H_n + H_K(\lambda_n)) + D$$

where

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

Secondly, if we cannot immediately give a bound for $H_K(x_n)$ then there exists $x_{n-1}, \lambda_{n-1}$ such that $x_n + \lambda_n = x_{n-1} + \lambda_{n-1}$ where $x_{n-1}$ is an element of a free non-degenerate $\mathfrak{c}$-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

$$(34) \quad H_{n-1} \leq A(H_n + H_K(\lambda_n)) + B$$

and by (31)

$$H_K(\lambda_{n-1}) \leq A(H_n + H_K(\lambda_n)) + B,$$

where

$$A = d n(n+1)(n^2 + 7n + 10 + d),$$

$$B = d n(n+1)(r + 6g + 2d + H_K(c)).$$

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

$$(36) \quad H_K(x_n) \leq H_K(x_{n-1}) + A(H_n + H_K(\lambda_n)) + B.$$

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

If we repeat our arguments then we obtain a sequence $M_n, M_{n-1}, \ldots$ of free non-degenerate $\mathfrak{c}$-modules and two sequences $x_n, x_{n-1}, x_{n-2}, \ldots$ and $\lambda_n, \lambda_{n-1}, \lambda_{n-2}, \ldots$ 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))

$$(37) \quad H_i \leq A(H_{i-1} + H_K(\lambda_{i+1}))) + B.$$
Further (cf. (35))

\[ H_k(\lambda_i) \leq A(H_{i+1} + H_k(\lambda_{i+1})) + B \]

and (cf. (36))

\[ H_k(x_{i-1}) \leq H_k(x_i) + A(H_{i+1} + H_k(\lambda_{i-1})) + B. \]

In each step either we obtain

\[ H_k(x_i) \leq C(H_i + H_k(\lambda_i)) + D \]

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

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 \( i_0 \geq 1 \)). By (40) we have

\[ H_k(x_{i_0}) \leq CS_{i_0} + D. \]

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

\[ S_i \leq (2A)^{i-1} \left( S_i + \frac{2B}{A} \right) \]

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

\[ H_k(x_i) \leq A(S_{i_0+1} + \ldots + S_i) + (n-1)B + H_k(x_{i_0}). \]

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

\[ H_k(x_{i_0}) \leq A(2A)^{i_0} \left( H_i + \frac{B}{2A} \right) + A(2A)^{i_0} - 1 H_k(\lambda_{i_0}) + nB. \]

By our condition on \( H_k(\lambda_i) \) we have \( A(2A)^{i_0} - 1 H_k(\lambda_{i_0}) < \frac{1}{2} H_k(x_{i_0}) \), whence the assertion (5) of our theorem follows.

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

\[ \max(H_k(\alpha), H_k(\beta)) \leq 4H_k(\alpha) + 2H_k(\alpha + \beta). \]

**References**


KOSZUTH LAJOS UNIVERSITY
MATHEMATICAL INSTITUTE
4010 Debrecen, P. 13, Hungary

Received on 22. 9. 1986 (1673)