LINEAR FORMS IN FUNCTION FIELDS

LEONARD TORNHEIM

We shall prove algebraically an analogue for function fields of a well known theorem of Minkowski on linear forms.

THEOREM 1. Let $F$ be a field and $z$ an indeterminate over $F$. Let

(1) $L_i = \sum_{j=1}^{n} a_{ij}x_j,$ $i = 1, \cdots, n,$

be $n$ linear expressions with coefficients $a_{ij}$ in $F(z)$ and with the determinant $|a_{ij}|$ of degree $d$. Then for any set of $n$ integers $c_1, \cdots, c_n$ which satisfy the condition $\sum_{i=1}^{n} c_i > d - n$ there exists a set of values for $x_1, \cdots, x_n$ in $F[z]$ and not all zero such that each $L_i$ has degree at most $c_i$.

First, we may assume that all of the $c_i$ are equal. For, suppose that $c$ is the maximum of the $c_i$. Write $L_i'$ for $L_i - c - c_i$. The determinant of the coefficients of the $L_i'$ has degree $d' = d + \sum (c - c_i) < \sum c + n$. If there is a set of values for $x_1, \cdots, x_n$ with the property that the degree of each $L_i'$ is at most $c$, then these same values will make the degree of $L_i$ at most $c_i$.

Next, we may assume, after multiplying each $L_i$ by a suitable polynomial and using an argument similar to that above, that all the $a_{ij}$ are in $F[z]$.

We shall now convert our system of $L_i$ by means of a transformation of determinant unity with elements in $F[z]$ into an equivalent system having $a_{ij} = 0$ for $i < j$. Let $b_1$ be the g.c.d. of the $a_{ij}$; then $b_1 = \sum_{j=1}^{n} a_{1j}c_{1j}$ for appropriate $c_{1j}$ in $F[z]$. Necessarily the $c_{1j}$ are relatively prime. It is possible to find other quantities $c_{jk}$ ($k = 2, \cdots, n$) such that the determinant $|c_{jk}|$ has value unity. Thus the transfor-

---

1 Presented to the Society, April 13, 1940.
4 The degree of a rational function is the degree of the numerator less that of the denominator. Zero is assigned the degree minus infinity.
5 A. A. Albert, Normalized integral bases of algebraic number fields I, Annals of Mathematics, (2), vol. 38 (1937), p. 926 ff. The statement is proved for rational integral $c_{jk}$ but the proof applies to any integral domain having the property that a
mation $x_i = \sum_{k=1}^{n} c_{jk} x_k'$ has determinant unity and hence it has a reciprocal transformation with elements in $F[z]$. The forms $L_i$ are transformed into $L'_i = \sum_{k=1}^{n} a_{ik} x_k'$. Here $a_{ik} = \sum_{j=1}^{n} d_{ij} c_{jk}$, and, being a linear combination of $a_{ij}$, it is divisible by their g.c.d. $b_i$; $a_{ik} = b_i d_{ik}$.

The transformation

$$x'_i = x'_i - \sum_{k=2}^{n} a_{ik} x'_k, \quad x'_r = x''_r, \quad r = 2, \ldots, n,$$

of determinant unity transforms the $L'_i$ into $L''_i$ with $L''_i = b_i x'_i$.

The procedure is repeated for the $n-1$ linear forms $M_i = \sum_{j=2}^{n} a_{ij} x'_j$ ($i = 2, \ldots, n$). Finally, if this process is continued, the resultant transformation converts the original system (1) into one with $a_{ij} = 0$ for $i < j$. As a consequence, if the degree of $a_{ij}$ is $d_i$, then $\sum d_i = d$. By using another transformation of determinant unity we may assume that the degree of each $a_{ij}$ is at most $d_i$.

Let $G_1$ be the set of all $n$-tuples $(s_1, \ldots, s_n) = s$ where the $s_i$ are in $F[z]$ and have degree not greater than $c$; hence $G_1$ is a linear set over $F$ whose order $u_1 = n(c+1)$. Write $L_i(s)$ for $\sum_{j=1}^{n} a_{ij} s_j$. Let $G_r$ of order $u_r$ over $F$ be the linear subset of $G_1$ composed of all quantities $s$ for which $L_1, \ldots, L_{r-1}$ all take values of degree not greater than $c$. Designate by $P_r$ the set of all $L_r(s)$ with $s$ in $G_r$, and by $Q_r$ the set of all polynomials in $P_r$ of degree not exceeding $c$. Since the maximum degree possible for a polynomial in $P_r$ is $c + d_r$, the number of linearly independent polynomials of $P_r$ which are not in $Q_r$, that is, the order of $P_r/Q_r$, is less than or equal to $d_r$. Now $G_r/Q_{r+1} \simeq P_r/Q_r$, a fact which follows from the mapping of $G_r$ on $P_r$ and $G_{r+1}$ on $Q_r$. Hence $[G_r:G_{r+1}] \leq \sum_{i=m+1}^{n} d_i = d$. Therefore the order $u_{n+1}$ of $G_{n+1}$ is not less than $n(c+1) - d$. To be sure that $G_{n+1}$ has elements other than zero, we must have $u_{n+1} \geq 1$, that is, $nc = \sum c \geq d + 1 - n$.

The following theorem applies if some of the $L_i$ must be made equal to zero.

**Theorem 2.** If in Theorem 1 the first $m$ of the $L_i$ are to be made equal to zero and if their coefficients are in $F[z]$, then the conclusion will hold if $\sum_{i=m+1}^{n} c_i > d - (n - m)$.

For, the first $m$ polynomials $s_i$ must be zero if we have the transformed system used in the proof of Theorem 1. Application of Theorem 1 for the remaining $L_i$ yields Theorem 2.