LINEAR FORMS IN FUNCTION FIELDS[1]

LEONARD TORNHEIM

We shall prove algebraically an analogue for function fields[2] of a well known theorem of Minkowski on linear forms.[3]

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

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

be n linear expressions with coefficients a_{ij} in $F(z)$ and with the determinant $|a_{ij}|$ of degree[4] *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 $L_i z^{c-c_i}$. 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 by 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_{1j}; then $b_1 = \sum_{j=1}^{n} a_{1j}c_{j1}$ for appropriate c_{j1} in $F[z]$. Necessarily the c_{j1} 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.[5] Thus the transfor-

---

[1] Presented to the Society, April 13, 1940.

[2] See M. Deuring, *Zur Theorie der Idealklassen in algebraischen Funktionenkörpern*, Mathematische Annalen, vol. 106 (1932), pp. 103–106, for a related result. I believe the results I prove are new.

[3] A bibliography of both analytic and algebraic proofs of the theorem of Minkowski on linear forms is given by E. Jacobsthal, *Der Minkowskische Linearformensatz*, Sitzungsberichte Berliner mathematischen Gesellschaft, vol. 33 (1934), pp. 62–64. See also L. J. Mordell, *Minkowski's theorem on homogeneous linear forms*, Journal of the London Mathematical Society, vol. 8 (1933), pp. 179–192.

[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 $x_j=\sum_{k=1}^{n} c_{jk}x_k'$ 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 $a_{1k}'=\sum_{j=1}^{n} a_{1j}c_{jk}$, and, being a linear combination of a_{1j}, it is divisible by their g.c.d. b_1; $a_{1k}'=b_1a_k$. The transformation

$$x_1' = x_1'' - \sum_{k=2}^{n} a_k x_k'', \qquad x_r' = x_r'', \qquad r = 2, \cdots, n,$$

of determinant unity transforms the L_i' into L_i'' with $L_1''=b_1x_1''$.

The procedure is repeated for the $n-1$ linear forms $M_i=\sum_{j=2}^{n} a_{ij}''x_j''$ $(i=2, \cdots, n)$. 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_{ii} 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 $(s_1, \cdots, s_n)=s$ 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 $L_1, \cdots, L_{r-1}$ 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 $G_r/G_{r+1}\simeq P_r/Q_r$, a fact which follows from the mapping of G_r on P_r and G_{r+1} on Q_r. Hence $[G_1:G_{n+1}]\leqq\sum_{i=1}^{n} d_i=d$. 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 $u_{n+1}\geqq 1$, that is, $nc=\sum c\geqq d+1-n$.

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.

UNIVERSITY OF CHICAGO

g.c.d. of any finite number of elements exists and is linearly expressible in terms of those elements, that is, that every ideal with a finite basis is principal.