Siegel's Lemma for Function Fields

JEFFREY LIN THUNDER

Introduction

Since the work of Thue early this century, an important tool in transcendental number theory and Diophantine approximation is the fact that a system of homogeneous linear equations over $\mathbb{Q}$ has a relatively small integer solution. This idea was formalized by Siegel in 1929 [7], and it has since been common to refer to results along this line of thought as "Siegel's lemma". Using the notion of a height, one can formulate the question of finding small solutions to systems of linear equations for arbitrary global fields—that is, fields for which one has a "product formula". It has proven useful to give versions of Siegel's lemma for such fields other than $\mathbb{Q}$. This was carried out for number fields by Bombieri and Vaaler in [3]. Here we formulate and prove a Siegel's lemma for function fields, where by "function field" we mean any finite algebraic extension of a field of rational functions in one indeterminate. We will give definitions for the heights used below in the next section.

Throughout this paper, $k = k_0(T)$ will denote the field of rational functions in one indeterminate over the field k_0 (we put no restrictions on the field k_0). We let K be any finite algebraic extension of k. As in [2], we denote by K_0 the *field of constants* of K (this is the algebraic closure of k_0 in K by [2, Chap. 12, Thm. 6]) and the *effective degree* by $\mathfrak{m}(K,k) = [K:k]/[K_0:k_0]$. More generally, if L is a finite algebraic extension of K with field of constants L_0, then the effective degree of this extension is $\mathfrak{m}(L,K) = [L:K]/[L_0:K_0]$.

THEOREM 1. *Let K be a function field and let h_A be a height on K^n (as defined below). There is a basis $\mathbf{a}_1, \ldots, \mathbf{a}_n$ of K^n satisfying*

$$\sum_{i=1}^{n} h_A(\mathbf{a}_i) \le h_A(K^n) + \frac{n}{\mathfrak{m}(K,k)}(g-1+\mathfrak{m}(K,k)),$$

where g is the genus of K.

As will be shown in Lemma 5, we always have the lower bound for a basis

$$\sum_{i=1}^{n} h_A(\mathbf{a}_i) \ge h_A(K^n),$$

Received April 25, 1994. Revision received August 29, 1994.
Michigan Math. J. 42 (1995).

so that the inequality in Theorem 1 is replaced by an equality whenever K is a field of rational functions, and this is best possible.

One can reformulate Minkowski's second convex-bodies theorem using the language of adeles (see e.g. [3]). Theorem 1 in the case where K is a field of rational functions is an analogue to this reformulation. In this case Theorem 1 follows from an upper bound on the first minima, that is, an analogue of Minkowski's first theorem. This upper bound is provided by a generalization of the Riemann–Roch theorem ([10, Chap. 6, Thm. 1] or Theorem 3 below) for the case of a field of rational functions.

Together, Theorem 1 and Lemma 5 imply the following.

COROLLARY 1. *Let K and h_A be as above. Then there is a nested sequence of subspaces $V_1 \subset V_2 \subset \cdots \subset K^n$ with $\dim_K(V_i) = i$ and*

$$\frac{n}{i} h_A(V_i) \leq h_A(K^n) + \frac{n}{\mathfrak{m}(K,k)}(g-1+\mathfrak{m}(K,k))$$

for $1 \leq i \leq n$.

We will see that Theorem 1 also implies the next corollary.

COROLLARY 2. *Let K be as above. Suppose m and n are positive integers with $m < n$, and let $M = (a_{ij})$ be an $m \times n$ matrix of rank m with entries $a_{ij} \in K$. Then there are linearly independent $\mathbf{b}_1, \ldots, \mathbf{b}_{n-m} \in K^n$ with $M\mathbf{b}^T = \mathbf{0}$ satisfying*

$$\sum_{i=1}^{n-m} h(\mathbf{b}_i) \leq h(M) + \frac{n-m}{\mathfrak{m}(K,k)}(g-1+\mathfrak{m}(K,k)).$$

Corollary 2 is an analogue of [3, Thm. 9]. The height h without the subscript denotes an analogue of the "usual" absolute height for number fields. Here we refer to the logarithmic, or additive, absolute height for number fields. In [3] the multiplicative height is used, so in order to make a direct comparison one should exponentiate both sides of the inequality in the statement of Corollary 2. The difference between Corollary 2 and Theorem 9 of [3] is that the quantity $g-1+\mathfrak{m}(K,k)$ plays the same role here that the discriminant plays in [3]. This is actually quite natural when one looks at the proofs. The discriminant appears in the results of Bombieri and Vaaler precisely as the covolume of a lattice (the lattice of integral points). This covolume is used in the adelic version of Minkowski's theorem which guarantees the existence of an integral point in a certain domain (i.e., a point of small height). Here we use an analogous argument to guarantee the existence of a point of small height, with the quantity above playing the role of the covolume. (See Theorem 3 below and its corollary.)

We can also prove results on relative extensions. Specifically, suppose K is as above and L is a finite algebraic extension of K with $[L:K] = r \geq 2$. Suppose F is a finite algebraic extension of L that is a galois extension of both K and L, with galois groups $G(F,K)$ and $G(F,L)$, respectively. Let $\sigma_1, \ldots, \sigma_r$ be

elements of $G(F, K)$ that are representatives of the distinct cosets of $G(F, L)$ in $G(F, K)$. We then have the following result analogous to Theorem 12 of [3].

COROLLARY 3. *Let M be an $m \times n$ matrix with entries in L, and let $\mathfrak{M}$ be the $mr \times n$ matrix*

$$\mathfrak{M} = \begin{pmatrix} \sigma_1(M) \\ \vdots \\ \sigma_r(M) \end{pmatrix}.$$

Suppose the rank of $\mathfrak{M}$ is mr and $mr < n$. Then there are linearly independent $\mathbf{b}_1, \ldots, \mathbf{b}_{n-mr} \in K^n$ with $M\mathbf{b}^T = \mathbf{0}$ that satisfy

$$\sum_{i=1}^{n-mr} h(\mathbf{b}_i) \leq h(\mathfrak{M}) + \frac{n-mr}{\mathfrak{m}(K,k)}(g-1+\mathfrak{m}(K,k)),$$

where g is the genus of K.

Corollary 3 follows from Corollary 2 just as Theorem 12 follows from Theorem 9 in [3].

As in the number-field case with the discriminant, one may well ask if the dependency on the genus is necessary. In [6] it is shown that some power of the discriminant is needed in the formulation of Siegel's lemma appearing in the work of Bombieri and Vaaler. Here we adapt the methods used in [6] to function fields and show the following theorem.

THEOREM 2. *Let K be a separable algebraic extension of k of degree d with field of constants k_0. Let $1 \leq m < n-2$ and let $t = [(n-m-1)/2]$, where $[\cdot]$ denotes the greatest integer function. Then there is an $m \times n$ matrix M of rank m with entries in K such that any $n-m$ linearly independent $\mathbf{b}_1, \ldots, \mathbf{b}_{n-m} \in K^n$ with $M\mathbf{b}^T = \mathbf{0}$ satisfy*

$$\sum_{i=1}^{n-m} h(\mathbf{b}_i) \geq h(M) + \frac{t(g-1+d)}{d^2-d} - (n-m)(d-1).$$

If k_0 has at least d elements, then

$$\sum_{i=1}^{n-m} h(\mathbf{b}_i) \geq h(M) + \frac{t(g-1+d)}{d^2-d} - \frac{(n-m)(d-1)}{d}.$$

Theorem 2 shows that some dependency on the quantity $g-1+\mathfrak{m}(K,k)$ is necessary in the upper bound of Corollary 2, at least in certain instances. Note that the effective degree is generally bounded by the genus, except when the genus is 1. In [4] it is shown that there are function fields of genus 1 with arbitrarily large effective degree. Also, it is not clear whether separability should be an issue here. It only enters the picture due to our particular construction of a system where all solutions have relatively large height in terms of the height of the solution space. Finally, as in the case of number fields, there is the possibility of finding a basis defined over an algebraic extension of K which would have smaller height.

I. Heights and Divisors

Let K be a function field as above and let $M(K)$ denote the set of places of K over K_0. For $v \in M(K)$ we write K_v for the completion of K at the place v, and for $x \in K_v$ we write $\mathrm{ord}_v(x)$ for the order of x at v. Here ord_v is normalized so that its image is $\mathbb{Z}$ and, as usual, $\mathrm{ord}_v(0) = \infty$. Thus, K_0 is the subfield of all elements $x \in K$ with $\mathrm{ord}_v(x) = 0$ or ∞ for all places v. For n a positive integer and $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in K_v^n$ we set

$$\mathrm{ord}_v(\mathbf{x}) = \min_{1 \le i \le n} \mathrm{ord}_v(x_i).$$

We denote the ring of integers of K_v by R_v; that is,

$$R_v = \{x \in K_v : \mathrm{ord}_v(x) \ge 0\}.$$

An element

$$A = (A_v) \in \prod_{v \in M(K)} \mathrm{GL}_n(K_v)$$

will be called *admissible* if $R_v^n A_v = R_v^n$ for all but finitely many $v \in M(K)$, where $R_v^n \subset K_v^n$ denotes the R_v-module $\bigoplus_{i=1}^n R_v \mathbf{e}_i$; in other words, A is an idele in $\mathrm{GL}_n(K_{\mathbb{A}})$, where $K_{\mathbb{A}}$ is the adele ring of K. We denote the set of admissible elements by $\mathfrak{A}_{K^n}$, or simply $\mathfrak{A}$ if the field and dimension are understood.

Given an $A \in \mathfrak{A}_{K^n}$, we may define an additive height h_A on K^n for $n > 1$ as follows. Let $\mathbf{x} \in K^n$, $\mathbf{x} \neq \mathbf{0}$. We then get a divisor

$$\mathrm{div}_A(\mathbf{x}) = \textstyle\sum_v \mathrm{ord}_v(\mathbf{x} A_v) \cdot v,$$

and we define the *height* of $\mathbf{x}$ with respect to A to be

$$h_A(\mathbf{x}) = -\deg(\mathrm{div}_A(\mathbf{x}))/\mathfrak{m}(K, k).$$

This height is projective, as the degree of a principal divisor is 0. Moreover, it is "absolute" in the following sense. If L is a finite algebraic extension of K and $A \in \mathfrak{A}_{K^n}$, then A can also be viewed as in $\mathfrak{A}_{L^n}$ in the natural way. Suppose $\mathbf{x} \in K^n$ and let D be the divisor of K given by $D = \mathrm{div}_A(\mathbf{x})$. View $\mathbf{x}$ as in L^n and let D' be the divisor of L given by $D' = \mathrm{div}_A(\mathbf{x})$. by [2, Chap. 15, Thm. 9], we have $\deg(D') = \mathfrak{m}(L, K)\deg(D)$. By [2, Chap. 15, Thm. 2], $\mathfrak{m}(L, k) = \mathfrak{m}(L, K)\mathfrak{m}(K, k)$. Thus, $h_A(\mathbf{x})$ remains unchanged if one views $\mathbf{x}$ as in L^n.

We can extend this height to subspaces of K^n via Grassmann coordinates. Specifically, let $S \subset K^n$ be a subspace of dimension d over K where $0 < d < n$. (Throughout this section and the next two, d will denote a positive integer, *not* the degree of the extension in the statement of Theorem 2.) Pick a basis $\mathbf{s}_1, \ldots, \mathbf{s}_d$ of S and let (s_{ij}) be the $d \times n$ matrix with rows $\mathbf{s}_1, \ldots, \mathbf{s}_d$. Let $c(n, d)$ denote the set of ordered d-tuples of integers $(i_1, i_2, \ldots, i_d)$ satisfying $1 \le i_1 < i_2 < \cdots < i_d \le n$ and order the elements of $c(n, d)$ lexicographically. For $\alpha \in c(n, d)$, let

$$X_\alpha = \det_{\substack{1 \le i \le d \\ j \in \alpha}} (s_{ij}).$$

We then get a vector $\mathbf{X} = (X_\alpha) \in K^{\binom{n}{d}}$ which is the set of *Grassmann coordinates* of S with respect to the basis $\mathbf{s}_1, \ldots, \mathbf{s}_d$. We define

$$\mathrm{div}_A(S) = \sum_v \mathrm{ord}_v(\mathbf{X} \wedge^d A_v) \cdot v,$$

where $\wedge^d A_v$ is the dth compound of $A_v = (a_{ij}^v)$:

$$\wedge^d A_v = \left(\det_{\substack{i \in \beta \\ j \in \alpha}} (a_{ij}^v) \right).$$

Since the Grassmann coordinates are projective, $\mathrm{div}_A(S)$ is unique up to principal divisors, so we get a well-defined divisor class $\overline{\mathrm{div}_A(S)}$ which is independent of the choice of basis. We define the height of S with respect to A to be

$$h_A(S) = -\deg(\overline{\mathrm{div}_A(S)})/\mathfrak{m}(K, k).$$

We also define

$$\mathrm{div}(A) = \mathrm{div}_A(K^n) = \textstyle\sum_v \mathrm{ord}_v(\det(A_v)) \cdot v \quad \text{and} \quad \mathrm{div}_A(\{\mathbf{0}\}) = 0.$$

It can be shown (see [9, Part I, §2]) that

$$\mathrm{div}_A(S) = \textstyle\sum_v \mathrm{ord}_v(\mathbf{X}_v) \cdot v,$$

where $\mathbf{X}_v \in K_v^{\binom{n}{d}}$ is the set of Grassmann coordinates for the subspace of K_v^n spanned by SA_v with respect to the basis $\mathbf{s}_1 A_v, \ldots, \mathbf{s}_d A_v$. We also remark that if $S^* \subset K^n$ is the dual space of S (i.e., the set of $\mathbf{x} \in K^n$ such that $\mathbf{x} \cdot \mathbf{s} = 0$ for all $\mathbf{s} \in S$), then (see [9, Part I, §2])

$$h_B(S^*) = h_A(S) - h_A(K^n),$$

where $B \in \mathfrak{A}$ is given by $B_v = (A_v^T)^{-1}$, the inverse of the transpose of A_v.

Here we have defined a height on K^n (actually on L^n for any finite algebraic extension L of K) via the local changes of coordinates given by A. Typically, one defines the height on K^n via the canonical basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ (using the identity matrix for every place v), and we denote this height simply by h. From the duality described above, the height of the null space of the matrix M in Corollary 2 is equal to the height of the row space of M. We define $h(M)$ to be this height. If V is any n-dimensional vector space over K and $A \in \mathfrak{A}_{K^n}$, we get a height on V by choosing a basis for V and identifying it with K^n. As we shall see in the following section, the height induced on a subspace of K^n can be realized in this manner, so that Corollary 2 follows from Theorem 1.

II. An Extended Riemann–Roch Theorem

We continue with the notation of the previous section. For each place v let $P_v \subset R_v$ be the unique maximal ideal:

$$P_v = \{a \in R_v : \mathrm{ord}_v(a) > 0\}.$$

For $d \leq n$ we write $K_v^d = \bigoplus_{i=1}^d K_v \mathbf{e}_i$, and similarly for R_v^d and P_v^d.

LEMMA 1. *Let v be any place and d be a positive integer less than or equal to n. If $A_v \in \mathrm{GL}_n(K_v)$ then*

$$R_v^n A_v^{-1} \cap K_v^d = R_v^d B_v'$$

for an $n \times n$ matrix B_v', where B_v' consists of a $B_v \in \mathrm{GL}_d(K_v)$ in the upper left-hand corner and zeros elsewhere. Moreover,

$$\mathrm{ord}_v(\det(B_v)) = -\mathrm{ord}_v(\mathbf{X}_v),$$

where $\mathbf{X}_v \in K_v^{\binom{n}{d}}$ is the set of Grassmann coordinates for the subspace $S_v = K_v^d A_v$ with respect to the basis $\mathbf{e}_1 A_v, \ldots, \mathbf{e}_d A_v$.

Proof. The first statement is true since R_v is a principal ideal domain, so that every R_v-module is free. We have

$$R_v^n \cap S_v = R_v^d B_v' A_v.$$

Let $C_v = B_v' A_v$ and denote the nonzero rows of C_v by $\mathbf{s}_1, \ldots, \mathbf{s}_d$. Then the $\mathbf{s}_i$s are a basis for S_v, and the equality above may be expressed as

$$R_v^n \cap S_v = \bigoplus_{i=1}^d R_v \mathbf{s}_i. \tag{1}$$

Moreover, if $\mathbf{Y}_v \in K_v^{\binom{n}{d}}$ is the set of Grassmann coordinates of S_v with respect to the basis $\mathbf{s}_1, \ldots, \mathbf{s}_d$, then

$$\mathbf{Y}_v = \det(B_v)\mathbf{X}_v \in R_v^{\binom{n}{d}}.$$

Thus, it suffices to show that $\mathrm{ord}_v(\mathbf{Y}_v) = 0$.

Suppose this is not the case and write $P_v = \pi_v R_v$. Then C_v has rank less than d modulo π_v; that is, there are $c_1, \ldots, c_d \in R_v$, not all in P_v, satisfying

$$\sum_{i=1}^d c_i \mathbf{s}_i \in P_v^n.$$

We then have

$$\sum_{i=1}^d c_i \pi_v^{-1} \mathbf{s}_i \in R_v^n,$$

which contradicts (1). This proves the lemma. □

Let $S \subseteq K^n$ be a subspace of dimension $d > 0$. For $A = (A_v) \in \mathfrak{A}_{K^n}$ we define

$$L_S(A) = \{\mathbf{x} \in S : \mathbf{x} \in R_v^n A_v \text{ for all } v\}.$$

Then $L_S(A)$ is a vector space over K_0 and we denote its dimension by $l_S(A)$. In the case $n = 1$, $A \in \mathfrak{A}_K$ corresponds to the divisor $\mathrm{div}(A) = \sum \mathrm{ord}_v(A_v) \cdot v$ and $L_K(A)$ consists of all $x \in K$ such that $\mathrm{ord}_v(x) \geq \mathrm{ord}_v(A_v)$. If $D = \sum D_v \cdot v$ is any divisor of K we let $L_K(D)$ be the set of $x \in K$ such that $\mathrm{ord}_v(x) \geq D_v$ for all places v.

The *repartitions* (*adeles*) *over* S, which we denote by $\mathfrak{R}_S$, are elements

$$\mathbf{r} = (\mathbf{r}_v) \in \prod_{v \in M(K)} S_v$$

satisfying $\operatorname{ord}_v(\mathbf{r}_v) \geq 0$ for all but finitely many v, where $S_v \subseteq K_v^n$ is the subspace spanned by S. We view $S \subset \mathfrak{R}_S$ by setting $\mathbf{x}_v = \mathbf{x}$ for $\mathbf{x} \in S$. For A as above we define the *parallelotope* $\Lambda_S(A)$ to be

$$\Lambda_S(A) = \{\mathbf{r} \in \mathfrak{R}_S : \mathbf{r}_v \in R_v^n A_v \text{ for all } v\}.$$

Thus, $L_S(A) = \Lambda_S(A) \cap S$. Similar to the case $n = 1$ above, if $D = \sum D_v \cdot v$ is a divisor of K we define $\Lambda_K(D)$ to be the set of $(r_v) \in \mathfrak{R}_K$ that satisfy $\operatorname{ord}_v(r_v) \geq D_v$ for all $v \in M(K)$.

Under componentwise addition, $\mathfrak{R}_S$ forms a vector space over K_0, with subspaces $\Lambda_S(A)$ and S. The following theorem in the case $n = 1$ is equivalent to the Riemann–Roch theorem.

THEOREM 3. *Let K be a function field with field of constants K_0. For $S \subseteq K^n$ a subspace of dimension $d > 0$ and $A \in \mathfrak{A}_{K^n}$,*

$$\dim_{K_0}\left(\frac{\mathfrak{R}_S}{\Lambda_S(A^{-1}) + S}\right) - l_S(A^{-1}) = -\deg(\overline{\operatorname{div}_A(S)}) + d(g-1);$$

that is,

$$\dim_{K_0}\left(\frac{\mathfrak{R}_S}{\Lambda_S(A^{-1}) + S}\right) - l_S(A^{-1}) = h_A(S)\,\mathfrak{m}(K, k) + d(g-1),$$

where g is the genus of K and $A^{-1} = (A_v^{-1}) \in \mathfrak{A}$.

Proof. Let $M \in \mathrm{GL}_n(K)$ taking K^d to S, and let $\mathbf{s}_i = \mathbf{e}_i M$ for $1 \leq i \leq d$. Then

$$L_S(A^{-1}) \cong \{\mathbf{x} \in K^d : \mathbf{x} \in R_v^n (MA_v)^{-1} \text{ for all } v\}$$

and similarly for $\Lambda_S(A^{-1})$. Let $\mathbf{X}_v \in K_v^{\binom{n}{d}}$ be the set of Grassmann coordinates of $S_v A_v$ with respect to the basis $\mathbf{s}_1 A_v, \ldots, \mathbf{s}_d A_v$. Then $\mathbf{X}_v$ is also the set of Grassmann coordinates of $K_v^d M A_v$ with respect to the basis $\mathbf{e}_1 M A_v, \ldots, \mathbf{e}_d M A_v$. We let $B \in \mathfrak{A}$ be defined by $B_v = MA_v$. We then have $\overline{\operatorname{div}_A(S)} = \overline{\operatorname{div}_B(K^d)}$, $l_S(A^{-1}) = l_{K^d}(B^{-1})$, and

$$\frac{\mathfrak{R}_S}{\Lambda_S(A^{-1}) + S} \cong \frac{\mathfrak{R}_{K^d}}{\Lambda_{K^d}(B^{-1}) + K^d},$$

so we may assume that $S = K^d$. Now by Lemma 1 we may assume $d = n$. The theorem in the case where K_0 is finite follows from [10, Chap. 6, Thm. 1]. Here we basically follow the first proof of the Riemann–Roch theorem given in [2].

We first show that $l_{K^n}(A)$ is finite for all admissible A. Toward this end, write $A_v = (a_{ij}^v)$ and consider the R_v module $R_v a_{11}^v + R_v a_{21}^v + \cdots + R_v a_{n1}^v$. Since R_v is a principal ideal domain, this module is equal to $R_v A_{v1}$ for some $A_{v1} \in K_v \backslash \{0\}$. We then have $A_1 = (A_{v1}) \in \mathfrak{A}_K$, where $\mathbf{x} \in L_{K^n}(A)$ implies that $x_1 \in L_K(A_1)$. We repeat this for each column of A, getting $A_i \in \mathfrak{A}_K$ such that

$\mathbf{x} \in L_{K^n}(A)$ implies that $x_i \in L_K(A_i)$ for each i between 1 and n. Now each $l_K(A_i)$ is finite by [2, Chap. 14, §2], so $l_{K^n}(A)$ must be finite as well.

Next, for $A, B \in \mathfrak{A}_{K^n}$ we say $A \mid B$ if $R_v^n A_v \supseteq R_v^n B_v$ for all $v \in M(K)$; that is, $\Lambda_{K^n}(A) \supseteq \Lambda_{K^n}(B)$. If $A \mid B$, we claim that

$$\dim_{K_0}\left(\frac{\Lambda_{K^n}(A)}{\Lambda_{K^n}(B)}\right) = \deg\left(\sum_{v \in M(K)} [R_v^n A_v : R_v^n B_v] \cdot v\right)$$
$$= \deg(\operatorname{div}(B)) - \deg(\operatorname{div}(A)).$$

Indeed, it suffices to consider the case where $R_v^n A_v = R_v^n B_v$ for all but one place v, and further that $n = 1$. This case follows from the definition of degree (see [2, Chap. 14, §1, Lemma 1]). From standard isomorphism theorems, we now have (dropping the subscripts)

$$\frac{\Lambda(A)/\Lambda(B)}{(\Lambda(B)+\Lambda(A)\cap K^n)/\Lambda(B)} \cong \frac{\Lambda(A)}{\Lambda(B)+\Lambda(A)\cap K^n} \cong \frac{\Lambda(A)+K^n}{\Lambda(B)+K^n}$$

and

$$\frac{\Lambda(B)+\Lambda(A)\cap K^n}{\Lambda(B)} \cong \frac{\Lambda(A)\cap K^n}{\Lambda(B)\cap\Lambda(A)\cap K^n} = \frac{\Lambda(A)\cap K^n}{\Lambda(B)\cap K^n} = \frac{L(A)}{L(B)}.$$

Thus

$$\deg(\operatorname{div}(B)) - \deg(\operatorname{div}(A)) = \dim_{K_0}\left(\frac{L(A)}{L(B)}\right) + \dim_{K_0}\left(\frac{\Lambda(A)+K^n}{\Lambda(B)+K^n}\right) \quad (2)$$

for $A \mid B$.

By [2, Chap. 13, §2, Lemma 2], there is an $a_0 \in \mathfrak{A}_K$ such that $\Lambda(a_0)+K = \mathfrak{R}_K$. Define $A_0 \in \mathfrak{A}_{K^n}$ by $A_0 = a_0 I$, where $I \in \mathfrak{A}_{K^n}$ is the admissible element given by the identity matrix at all places. Then $\Lambda_{K^n}(A_0)+K^n = \mathfrak{R}_{K^n}$. Let $B \in \mathfrak{A}_{K^n}$ be arbitrary and let $A \in \mathfrak{A}_{K^n}$ be given by $\Lambda(A) = \Lambda(A_0)+\Lambda(B)$. Then $A \mid B$ and, by (2),

$$\deg(\operatorname{div}(B)) - \deg(\operatorname{div}(A)) = \dim_{K_0}\left(\frac{L(A)}{L(B)}\right) + \dim_{K_0}\left(\frac{\mathfrak{R}_{K^n}}{\Lambda(B)+K^n}\right).$$

This shows that the last summand above is finite, and we may rewrite (2) as

$$\deg(\operatorname{div}(B)) - \deg(\operatorname{div}(A))$$
$$= l(A) - l(B) + \dim_{K_0}\left(\frac{\mathfrak{R}_{K^n}}{\Lambda(B)+K^n}\right) - \dim_{K_0}\left(\frac{\mathfrak{R}_{K^n}}{\Lambda(A)+K^n}\right) \quad (2')$$

for $A \mid B$.

Now let $A, B \in \mathfrak{A}_{K^n}$ be arbitrary. Let $C \in \mathfrak{A}_{K^n}$ be such that $C \mid A$ and $C \mid B$ (the existence of such a C is clear). Then, by (2') (again dropping subscripts),

$$\deg(\operatorname{div}(A)) - \dim_{K_0}\left(\frac{\mathfrak{R}_{K^n}}{\Lambda(A)+K^n}\right) + l(A)$$
$$= \deg(\operatorname{div}(C)) - \dim_{K_0}\left(\frac{\mathfrak{R}_{K^n}}{\Lambda(C)+K^n}\right) + l(C)$$
$$= \deg(\operatorname{div}(B)) - \dim_{K_0}\left(\frac{\mathfrak{R}_{K^n}}{\Lambda(B)+K^n}\right) + l(B).$$

Thus, for any $A \in \mathfrak{A}_{K^n}$, the quantity $\deg(\mathrm{div}(A)) - \dim_{K_0}(\mathfrak{R}_{K^n}/(\Lambda(A)+K^n)) + l(A)$ is the same. By considering $I \in \mathfrak{A}_{K^n}$, we get

$$\begin{aligned}
&\deg(\mathrm{div}(A)) - \dim_{K_0}\left(\frac{\mathfrak{R}_{K^n}}{\Lambda_{K^n}(A)+K^n}\right) + l_{K^n}(A) \\
&\quad = \deg(\mathrm{div}(I)) - \dim_{K_0}\left(\frac{\mathfrak{R}_{K^n}}{\Lambda_{K^n}(I)+K^n}\right) + l_{K^n}(I) \\
&\quad = n\left(l_K(0) - \dim_{K_0}\left(\frac{\mathfrak{R}_K}{\Lambda_K(0)+K}\right)\right) \\
&\quad = n(1-g),
\end{aligned}$$

where 0 denotes the zero divisor. Note that $\deg(\mathrm{div}(A^{-1})) = -\deg(\mathrm{div}(A))$ for any $A \in \mathfrak{A}_{K^n}$. Theorem 3 follows. □

As remarked in the introduction, Theorem 3 in the case where K is a field of rational functions yields an analogue to Minkowski's first convex-bodies theorem. More generally, it yields the adelic analogue of Minkowski's first theorem for function fields. Specifically, we have the following.

COROLLARY. *Let K be as above and let $A \in \mathfrak{A}_{K^n}$. If $\deg(\mathrm{div}(A)) > n(g-1)$, then there is a nonzero $\mathbf{x} \in L_{K^n}(A^{-1})$. In particular, if K is a field of rational functions and $h_A(K^n) < n$, then there is a nonzero $\mathbf{x} \in K^n$ with $h_A(\mathbf{x}) \leq 0$.*

III. Proof of Theorem 1

Let $A \in \mathfrak{A}_{K^n}$, giving a height h_A on K^n as defined above. We define minima $\mu_1, \ldots, \mu_n$ as follows:

$$\mu_i = \inf\{\mu : K^n \text{ has } i \text{ linearly independent elements of height} \leq \mu\}.$$

Certainly $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$. Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be a basis for K^n with $h_A(\mathbf{v}_i) = \mu_i$ for $1 \leq i \leq n$. We then define

$$V_i = \bigoplus_{j=1}^{i} K\mathbf{v}_j \quad \text{for } 0 < i \leq n$$

and $V_0 = \{\mathbf{0}\}$.

LEMMA 2. *Let $1 \leq i \leq n$. If $h_A(\mathbf{x}) < \mu_i$ then $\mathbf{x} \in V_{i-1}$; that is, $h_A(\mathbf{x}) \geq \mu_i$ for all $\mathbf{x} \notin V_{i-1}$.*

Proof. The case $i = 1$ is true by the definition of μ_1. We proceed by induction on i. If $\mathbf{x} \notin V_{i-1}$, then

$$\mu_i \leq \max\{h_A(\mathbf{x}), \mu_{i-1}\},$$

whence $\mu_i = \mu_{i-1}$. We get a contradiction by the induction hypothesis since $V_{i-2} \subset V_{i-1}$. □

The subspaces V_i are thus "minimal" in the sense that they contain all vectors of minimal height. These will turn out to be the subspaces in Corollary 1.

We first prove Theorem 1 in the case where $K = k$, so assume until stated otherwise that this is the case.

Let $w \in M(K)$ be the place with $\mathrm{ord}_w(T) = -1$ and let $M \in \mathrm{GL}_n(K_w)$ satisfy $R_w^n M = R_w^n$ and $V_i{}^w M = K_w^i$ for each $i = 1, \ldots, n$, where $V_i{}^w \subseteq K_w^n$ is the subspace spanned by $V_i A_w$. Let $D = \sum D_v \cdot v$ be a divisor of degree -1 and let $b_1, \ldots, b_n \in K_w$ satisfy $\mathrm{ord}_w(b_i) = \mu_i$. Define

$$B_w = \pi_w^{D_w} A_w M \begin{pmatrix} b_1 & & \\ & \ddots & \\ & & b_n \end{pmatrix}$$

and define $B_v = \pi_v^{D_v} A_v$ for all places $v \neq w$. (Recall that $P_v = \pi_v R_v$.) Then $B \in \mathfrak{A}_{K^n}$ and we get a new height h_B satisfying

$$h_B(K^n) = h_A(K^n) + n - \sum_{i=1}^{n} \mu_i, \tag{3}$$

since $\mathrm{ord}_w(\det(M)) = 0$.

LEMMA 3. *For any* $\mathbf{x} \in V_i \backslash V_{i-1}$, $h_B(\mathbf{x}) \geq 1$. *In particular,* $h_B > 0$ *on* K^n.

Proof. Let $\mathbf{x} \in V_i \backslash V_{i-1}$. Then $\mathbf{x} A_w M \in K_w^i$. Using this and $\mathrm{ord}_w(\pi_w) = 1$ gives

$$\begin{aligned} \mathrm{ord}_w(\mathbf{x} B_w) &= \mathrm{ord}_w(\pi_w^{D_w}) + \mathrm{ord}_w\left(\mathbf{x} A_w M \begin{pmatrix} b_1 & & \\ & \ddots & \\ & & b_n \end{pmatrix}\right) \\ &\leq \mathrm{ord}_w(\mathbf{x} A_w M) + \mathrm{ord}_w(b_i) + D_w \\ &= \mathrm{ord}_w(\mathbf{x} A_w M) + \mu_i + D_w. \end{aligned}$$

Now since $R_w^n M = R_w^n$, we have $\mathrm{ord}_w(\mathbf{x} A_w M) = \mathrm{ord}_w(\mathbf{x} A_w)$. Thus

$$\mathrm{ord}_w(\mathbf{x} B_w) \leq \mathrm{ord}_w(\mathbf{x} A_w) + \mu_i + D_w.$$

Also,

$$\mathrm{ord}_v(\mathbf{x} B_v) = \mathrm{ord}_v(\mathbf{x} A_v) + D_v$$

for all $v \neq w$. This shows that $h_B(\mathbf{x}) \geq h_A(\mathbf{x}) + 1 - \mu_i$. Since $\mathbf{x} \notin V_{i-1}$, we have $h_A(\mathbf{x}) \geq \mu_i$ by Lemma 2. This proves Lemma 3. □

Lemma 3 and the corollary to Theorem 3 imply that $h_B(K^n) \geq n$. This together with (3) gives Theorem 1 in the case where K is a field of rational functions.

Now suppose more generally that K is any function field. Let $x_1, \ldots, x_m$ be a basis for K over k. View $\mathfrak{R}_{k^{nm}}$ as the Cartesian product of m copies of $\mathfrak{R}_{k^n}$. Define $\phi: \mathfrak{R}_{k^{nm}} \to \mathfrak{R}_{K^n}$ by

$$\phi(\mathbf{r}_1, \ldots, \mathbf{r}_m) = \sum_{i=1}^{m} x_i \mathbf{r}_i.$$

Then ϕ is one-to-one, onto, and bicontinuous with respect to the restricted direct product topologies [2, Chap. 13, §2]. Let $A' \in \mathfrak{A}_{k^{nm}}$ be given by

$$\phi^{-1}(\Lambda_{K^n}(A^{-1})) = \Lambda_{k^{nm}}((A')^{-1}).$$

(It is clear that the inverse image of a parallelotope is a parallelotope.) Since ϕ maps k^{nm} to K^n and the genus of k is 0, Theorem 3 gives

$$\mathfrak{m}(K,k)h_A(K^n)+n(g-1) = (\mathfrak{m}(K,k)/m)(h_{A'}(k^{nm})-nm). \tag{4}$$

LEMMA 4. *For $\mathbf{v}\in k^{nm}$ with $\mathbf{v}\neq\mathbf{0}$, we have $h_{A'}(\mathbf{v}) \geq h_A(\phi(\mathbf{v}))$.*

Proof. Let $\mathbf{v}\in k^{nm}$, $\mathbf{v}\neq\mathbf{0}$, and let $D' = -\mathrm{div}_{A'}(\mathbf{v})$, so that $h_{A'}(\mathbf{v}) = \deg(D')$. Now by construction we have $\mathrm{ord}_w(D'_w\mathbf{v}A'_w) = 0$ for all $w\in M(k)$, so that $D'\mathbf{v}\in\Lambda_{k^{nm}}((A')^{-1})$. This implies that $\phi(D'\mathbf{v})\in\Lambda_{K^n}(A^{-1})$; that is,

$$\mathrm{ord}_v(D'_w\phi(\mathbf{v})A_v)\geq 0 \quad \text{for all } v\,|\,w,\ w\in M(k).$$

Thus

$$h_A(\phi(\mathbf{v})) \leq \frac{\deg(D)}{\mathfrak{m}(K,k)},$$

where D is the divisor

$$D = \sum_{w\in M(k)}\ \sum_{v\,|\,w} D'_w\cdot v.$$

Since $\deg(D) = \mathfrak{m}(K,k)\deg(D')$ [2, Chap. 15, Thm. 9], the lemma follows. □

We now apply what we have proven already to k^{nm} and A' to get $\mathbf{v}_1,\ldots,\mathbf{v}_{nm}\in k^{nm}$, linearly independent over k, with

$$\sum_{l=1}^{nm} h_{A'}(\mathbf{v}_l) \leq h_{A'}(k^{nm}).$$

Assume that $h_{A'}(\mathbf{v}_1)\leq\cdots\leq h_{A'}(\mathbf{v}_{nm})$. Define $\mathbf{a}_1 = \phi(\mathbf{v}_1)$, and recursively $\mathbf{a}_{i+1} = \phi(\mathbf{v}_l)$, where l is least such that $\mathbf{a}_1,\ldots,\mathbf{a}_i$, $\phi(\mathbf{v}_l)$ are linearly independent over K. Note that $l\leq mi+1$ since $[K:k]=m$ and the $\mathbf{v}_i$s are linearly independent over k. Thus

$$\sum_{i=1}^{n} h_{A'}(\phi^{-1}(\mathbf{a}_i)) \leq \frac{h_{A'}(k^{nm})}{m}.$$

Theorem 1 follows from this, Lemma 4, and (4). □

LEMMA 5. *Let K and A be as above and let $\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_m$ be linearly independent elements of K^n. Let p and q be two positive integers with $p+q\leq m$. Let S and T be the subspaces of K^n spanned by $\mathbf{x}_1,\ldots,\mathbf{x}_p$ and $\mathbf{x}_{p+1},\ldots,\mathbf{x}_{p+q}$, respectively, and let W be the subspace spanned by $\mathbf{x}_1,\ldots,\mathbf{x}_{p+q}$. Then*

$$h_A(W)\leq h_A(S)+h_A(T).$$

Proof. Let $v\in M(K)$ and write $\mathbf{x}_i^v = \mathbf{x}_iA_v$ for all i. By definition

$$\mathrm{ord}_v\left(\bigwedge_{i=1}^{p+q}\mathbf{x}_i^v\right) = \min_{\alpha\in c(n,p+q)}\left\{\mathrm{ord}_v\left(\det_{\substack{1\leq i\leq p+q\\ j\in\alpha}}(x_{ij}^v)\right)\right\}.$$

But, by Laplace's expansion of the determinant,

$$\det_{\substack{1\le i\le p+q\\ j\in\alpha}}(x_{ij}^v)=\sum_{\substack{\sigma\in c(n,p)\\ \sigma\subseteq\alpha}}\det_{\substack{1\le i\le p\\ j\in\sigma}}(x_{ij}^v)\det_{\substack{p+1\le i\le p+q\\ j\in\sigma'}}(x_{ij}^v),$$

where $\sigma'=\alpha\backslash\sigma$. Therefore

$$-\mathrm{ord}_v\left(\bigwedge_{i=1}^{p+q}\mathbf{x}_i^v\right)\le-\mathrm{ord}_v\left(\bigwedge_{i=1}^{p}\mathbf{x}_i^v\right)-\mathrm{ord}_v\left(\bigwedge_{i=p+1}^{p+q}\mathbf{x}_i^v\right),$$

which proves the lemma. □

Lemma 5 shows that if $\mathbf{x}_1, \ldots, \mathbf{x}_n$ is any basis for K^n, then

$$\sum_{i=1}^{n}h_A(\mathbf{x}_i)\ge h_A(K^n).$$

Thus, in the case where K is a field of rational functions, the inequality of Theorem 1 becomes an equality and this is best possible. This also shows that $h_A(V_i)\le\mu_1+\cdots+\mu_i$ for each $1\le i\le n$, so that Corollary 1 follows from Theorem 1.

IV. Proof of Theorem 2

Throughout this section K will be a separable algebraic extension of k of degree d, genus g, and field of constants k_0 (so that $\mathfrak{m}(K,k)=d$). To prove Theorem 2 we will explicitly construct a system of m equations in n unknowns which satisfy the statement. In order to do this we require some auxiliary results. Our first goal is a general result that is an analogue of [6, Lemma 4]. A similar result (but not explicitly involving the genus) was proven by Silverman in [8].

LEMMA 6. *Let F be a finite algebraic extension of k and let G be a finite algebraic extension of F (separable or not) of degree e. Let $x_1, x_2, \ldots, x_e$ be a basis for G over F. Then*

$$\mathfrak{m}(G,k)h(x_1,\ldots,x_e)\ge g_G-1-\mathfrak{m}(G,F)(g_F-1),$$

where g_G and g_F denote the genera of G and F, respectively. If $G=F(\alpha)$ then

$$(e-1)\mathfrak{m}(G,k)h(1,\alpha)\ge g_G-1-\mathfrak{m}(G,F)(g_F-1).$$

In particular, if $F=k$ then

$$h(x_1,\ldots,x_e)\ge\frac{g_G-1+\mathfrak{m}(G,k)}{\mathfrak{m}(G,k)},\qquad h(1,\alpha)\ge\frac{g_G-1+\mathfrak{m}(G,k)}{(e-1)\mathfrak{m}(G,k)}.$$

Proof. Write $\mathbf{x}=(x_1,\ldots,x_e)$ and $D=\mathrm{div}(\mathbf{x})$, so that $\mathfrak{m}(G,k)h(\mathbf{x})=-\deg(D)$. Denote the constant fields of G and F by G_0 and F_0, respectively. By Theorem 3,

$$\mathfrak{m}(G,k)h(\mathbf{x}) = g_G - 1 + l_G(D) - \dim_{G_0}\left(\frac{\mathfrak{R}_G}{\Lambda_G(D)+G}\right). \tag{5}$$

Note that $x_1, \ldots, x_e \in L_G(D)$ are all linearly independent over F_0 (since they are over F). Thus, at least $\mathfrak{m}(G,F)$ of them are linearly independent over G_0 and we have

$$l_G(D) \geq \mathfrak{m}(G,F). \tag{6}$$

Define $\phi: \mathfrak{R}_{F^e} \to \mathfrak{R}_G$ as in the proof of Theorem 1:

$$\phi(\mathbf{r}) = \phi(r_1, \ldots, r_e) = \sum_{i=1}^{e} x_i r_i.$$

Let $I \in \mathfrak{A}_{F^e}$ be the admissible element given by the identity matrix at all places. We claim that $\phi(\Lambda_{F^e}(I)) \subseteq \Lambda_G(D)$. Indeed, if $\mathbf{r} \in \Lambda_{F^e}(I)$ and $w \in M(G)$, then

$$\begin{aligned}
\operatorname{ord}_w(\mathbf{r}\cdot\mathbf{x}) &\geq \min_{1\leq i\leq e}\{\operatorname{ord}_w(r_i x_i)\} \\
&= \min_{1\leq i\leq e}\{\operatorname{ord}_w(r_i) + \operatorname{ord}_w(x_i)\} \\
&\geq \min_{1\leq i\leq e}\{\operatorname{ord}_w(x_i)\} \\
&= \operatorname{ord}_w(D),
\end{aligned}$$

by the definition of D and since $\operatorname{ord}_v(r_i) \geq 0$ for all $v \in M(F)$. This shows that

$$\dim_{F_0}\left(\frac{\mathfrak{R}_G}{\Lambda_G(D)+G}\right) \leq \dim_{F_0}\left(\frac{\mathfrak{R}_{F^e}}{\Lambda_{F^e}(I)+F^e}\right). \tag{7}$$

Now, by Theorem 3,

$$\begin{aligned}
\dim_{F_0}\left(\frac{\mathfrak{R}_{F^e}}{\Lambda_{F^e}(I)+F^e}\right) &= l_{F^e}(I) - \deg(\operatorname{div}(I)) + e(g_F - 1) \\
&= e - 0 + e(g_F - 1) \\
&= eg_F.
\end{aligned} \tag{8}$$

The first part of the lemma follows from (5)–(8) and the definition of the effective degree.

Finally, suppose that $G = F(\alpha)$. Then $1, \alpha, \alpha^2, \ldots, \alpha^{e-1}$ is a basis for G over F. By the definition of h,

$$(e-1)h(1,\alpha) = h(1, \alpha, \ldots, \alpha^{e-1}).$$

This finishes the proof of Lemma 6. □

We now make the following definitions. A *primitive* element $\alpha \in K$ is an element that satisfies $k(\alpha) = K$. We define $\delta(K)$ to be the smallest number such that there exists a primitive element $\alpha \in K$ with $h(1,\alpha) = \delta(K)$; this makes sense because we are assuming that K is a separable extension of k. By Lemma 6 we have

$$\delta(K) \geq \frac{g-1+d}{d^2-d}. \tag{9}$$

The *field of definition* of a nonzero point $(x_1, x_2, \ldots, x_n) \in K^n$ viewed as a projective point is the subfield of K generated over k by the quotients x_i/x_j with $x_j \neq 0$.

LEMMA 7. *Let* $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in K^n$ *with* $\mathbf{x} \neq \mathbf{0}$. *If* K *is the field of definition of* $\mathbf{x}$ *viewed as a projective point, then*

$$h(\mathbf{x}) \geq \delta(K) - (d-1).$$

If the cardinality of k_0 *is at least* d, *then* $h(\mathbf{x}) \geq \delta(K)$.

Proof. This is clear if $d = 1$, so assume $d \geq 2$. After possibly reordering the coordinates, we have proper inclusions

$$k \subset k(x_1) \subset \cdots \subset k(x_1, \ldots, x_t) = K.$$

Let F be a separable closure of k and consider the polynomial

$$P(X_1, \ldots, X_t) = \prod_{i=2}^{d} \left(\sum_{j=1}^{t} (x_j - \sigma_i(x_j)) X_j \right),$$

where $\sigma_1, \ldots, \sigma_d$ are the embeddings of K into F with σ_1 the identity map. Since $K = k(x_1, \ldots, x_t)$, this is a nonzero homogeneous polynomial of degree $d-1$. Suppose first that k_0 has at least d elements. Then there exist $a_1, \ldots, a_t \in k_0$ such that $P(a_1, \ldots, a_t) \neq 0$. We then have that $\alpha = \sum_{j=1}^{t} a_j x_j$ is a primitive element of K. Moreover, we have $\mathrm{ord}_v(\alpha) \geq \mathrm{ord}_v(x_1, \ldots, x_t)$. We may assume without loss of generality that $x_n = 1$, and thus $h(1, \alpha) \leq h(\mathbf{x})$. If k_0 has less than d elements we choose $a_1, \ldots, a_t \in k_0[T]$ of degree less that d such that $P(a_1, \ldots, a_t) \neq 0$. Let α be as above. Then α is again a primitive element and we have

$$h(1, \alpha) \leq h(x_1, \ldots, x_t) + (d-1)h(1, T) \leq h(\mathbf{x}) + (d-1). \qquad \square$$

LEMMA 8. *Let* $a \in K$ *with* $a \neq 0$, *and let* $\mathbf{x} = (x_1, \ldots, x_n) \in K^n$ *be a nonzero solution of*

$$x_1 + ax_2 + \cdots + a^{n-1}x_n = 0.$$

Then $h(\mathbf{x}) \geq h(1, a)$.

Proof. Without loss of generality, $x_1 = a$. If $\mathrm{ord}_v(a) \leq 0$ then $\mathrm{ord}_v(\mathbf{x}) \leq \mathrm{ord}_v(a) = \mathrm{ord}_v(1, a)$. If $\mathrm{ord}_v(a) \geq 0$ then

$$\mathrm{ord}_v(a) = \mathrm{ord}_v(x_1) \geq \min\{\mathrm{ord}_v(ax_2), \ldots, \mathrm{ord}_v(a^{n-1}x_n)\},$$

so that $\mathrm{ord}_v(\mathbf{x}) \leq 0 = \mathrm{ord}_v(1, a)$ again. This proves the lemma. $\square$

We are now in a position to prove Theorem 2. Let $\alpha \in K$ be a primitive element with $h(1, \alpha) = \delta(K)$ and let $a \in k_0[T]$ be of degree e, where $e = [\delta(K)]$. Put $r = n - m - t$ and $s = t + 1$, and consider the system of equations

$$x_1+ax_2+\cdots+a^{r-1}x_r+\alpha x_{r+1}+a\alpha x_{r+2}+\cdots+a^{s-1}\alpha x_{r+s}=0$$
$$x_{r+s+1}=0$$
$$\vdots$$
$$x_n=0.$$

This is a system of m linearly independent equations in n variables, and since $r \geq s$, the solution space $V \subset K^n$ satisfies

$$\begin{aligned} h(V) &= h(1, a, \ldots, a^{r-1}, \alpha, a\alpha, \ldots, a^{s-1}\alpha) \\ &\leq e(r-1)+h(1,\alpha) \\ &\leq r\delta(K). \end{aligned}$$

Now suppose $\mathbf{x} \in K^n$ is a nonzero element of V and set $u = x_1+ax_2+\cdots+a^{r-1}x_r$ and $v = x_{r+1}+ax_{r+2}+\cdots+a^{s-1}x_{r+s}$. If $v=0$ then $h(\mathbf{x}) \geq h(1,a) = e \geq \delta(K)-(d-1)/d$ by Lemma 8. On the other hand, if $v \neq 0$ then K is the field of definition of $\mathbf{x}$ viewed as a projective point and Lemma 7 gives $h(\mathbf{x}) \geq \delta(K)-(d-1)$, or $h(\mathbf{x}) \geq \delta(K)$ if k_0 has at least d elements. Thus, if $\mathbf{x}_1, \ldots, \mathbf{x}_{n-m}$ is any basis for V, then

$$\begin{aligned} \sum_{i=1}^{n-m} h(\mathbf{x}_i) &\geq (n-m)(\delta(K)-(d-1)) \\ &= r\delta(K)+t\delta(K)-(n-m)(d-1) \\ &\geq h(V)+t\delta(K)-(n-m)(d-1). \end{aligned}$$

Similarly, if k_0 has at least d elements then we obtain

$$\sum_{i=1}^{n-m} h(\mathbf{x}_i) \geq h(V)+t\delta(K)-\frac{(n-m)(d-1)}{d}.$$

Theorem 2 now follows from (9). □

V. Concluding Remarks

Others have studied geometry of numbers over function fields. In particular, Mahler in [5] proves what amounts to our Theorem 1 in the case where K is a field of rational functions. However, he did not prove it the same way we do here. In particular, he did not use a result like Theorem 3 to derive an upper bound for the first minima. Our proof here is much shorter. It is interesting to note that Armitage [1] was able to prove the Riemann–Roch theorem for function fields using Mahler's result.

Note that our proof of Theorem 3 is almost entirely self-contained; we need only the following two facts:

(i) The dimension $l_K(D)$ is finite for any divisor D.
(ii) There is a divisor D such that $\Lambda_K(D)+K = \mathfrak{R}_K$.

Both these facts are easily verified when K is a field of rational functions (for the second, use the zero divisor). Thus, one can give a short, self-contained proof of Theorem 3 in the case where K is a field of rational functions.

Now suppose K is any function field and let $R = K_0(X)$ be a rational subfield of K, where K_0 is the field of constants of K and $X \in K \setminus K_0$. Using the fact that $\phi(\mathfrak{R}_{R^{m(K/R)}})$ is dense in $\mathfrak{R}_K$ and that Theorem 3 holds for R, one immediately verifies (i) and (ii) for K (for (ii), use $D = \mathrm{div}(\mathbf{x})$ with $\mathbf{x}$ a basis for K over R, as in the proof of Lemma 6). The fact that the image of ϕ is dense follows from the approximation theorem (see [2, Chap. 13, §2, Lemma 2]). Thus, a rather short proof of the Riemann–Roch theorem can be given using only standard facts from the theory of valuations.

References

[1] J. V. Armitage, *Algebraic functions and an analogue of the geometry of numbers: The Riemann–Roch theorem,* Arch. Math. (Basel) 18 (1967), 383–393.
[2] E. Artin, *Algebraic numbers and algebraic functions,* Gordon and Breach, New York, 1967.
[3] E. Bombieri and J. Vaaler, *On Siegel's Lemma,* Invent. Math. 73 (1983), 11–32.
[4] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties,* Amer. J. Math 80 (1958), 659–684.
[5] K. Mahler, *An analogue to Minkowski's geometry of numbers in a field of series,* Ann. of Math. (2) 42 (1941), 488–522.
[6] D. Roy and J. Thunder, *A note on Siegel's Lemma over number fields,* Monatsh. Math. (to appear).
[7] C. L. Siegel, *Über einige Anwendungen diophantischer Aproximationen,* Abh. Preuß. Akad. d. Wiss., Math. Phys. Kl., Nr.1 (= Ges. Abh., I) (1929), 209–266.
[8] J. Silverman, *Lower bounds for height functions,* Duke Math. J. 51 (1984), 395–403.
[9] J. Thunder, *Asymptotic estimates for rational points of bounded height on flag varieties,* Compositio Math. 88 (1993), 155–188.
[10] A. Weil, *Basic number theory,* Springer, New York, 1967.

Department of Mathematics
Northern Illinois University
DeKalb, IL 60115