APPROXIMATION IN ALGEBRAIC FUNCTION FIELDS OF ONE VARIABLE

JOHN COATES

(Received 10 January 1966)

In his paper (4), Mahler established several strong quantitative results on approximation in algebraic number fields using the geometry of numbers. In the present paper I derive analogous results for algebraic function fields of one variable using an analogue of the geometry of numbers.

The main result of this paper states that every fractional ideal of certain Dedekind subrings of the function field has a basis such that all the valuations of all the basis elements lie between certain limits which are given in terms of field constants and arbitrary parameters. This result is then applied to study the approximation of adeles by field elements, the approximation of field elements by other field elements, and the properties of certain classes of divisors. Most of the results obtained are well known, but it seems worthwhile to derive them from the point of view of the geometry of numbers.

I wish to thank Professor Mahler for his advice on this work, and also the referee for his suggestions.

1

In his paper [5], Mahler established various number-geometrical properties of fields of formal power series. Since I shall be applying some of these properties here, I begin by stating those needed without proof.

In a notation different from Mahler's, let k_0 be a field of arbitrary characteristic, t an element transcendental over k_0, $i_t = k_0[t]$ the ring of polynomials in t with coefficients in k_0, k the quotient field of i_t, and v_q the valuation of k defined by $v_q(0) = \infty$, and $v_q(\xi) = f$ if $\xi \neq 0$ is of order $f =$ degree denominator-degree numerator. Let further k_q be the completion of k relative to v_q and thus the field of all formal power series

$$\xi = \gamma_f \left(\frac{1}{t}\right)^f + \gamma_{f+1} \left(\frac{1}{t}\right)^{f+1} + \cdots, \text{ with } \gamma_i \in k_0.$$

The valuation v_q is extended to k_q by continuity, so that $v_q(\xi) = f$ if $\gamma_f \neq 0$.

Next, denote by P^n the Cartesian product of k_q n times, and thus the space of all points $\xi = (\xi_1, \cdots, \xi_n)$ with components $\xi_i \in k_{\mathfrak{q}}$. Denote by Λ^n the set of all lattice points in P^n, i.e. the set of all points with components in i_t.

The following result was proven. Let $A = (v_{ij})$ be a non-singular matrix with elements in $k_{\mathfrak{q}}$ and determinant D, and let for $\xi \in P^n$

$$F(\xi) = \min_{i=1,\cdots,n} v_{\mathfrak{q}}\Big(\sum_{j=1}^{n} a_{ij}\xi_j\Big).$$

Then there exist n lattice points

$$\xi_h = (\xi_{h1}, \cdots, \xi_{hn}) \in \Lambda^n \qquad (k = 1, \cdots, n)$$

with the following properties:

(1) $F(\xi_1) \geqq F(\xi_2) \geqq \cdots \geqq F(\xi_n)$;

(2) $F(\xi_1)$ is the maximum of $F(\xi)$ for all $\xi \neq 0$ in Λ^n; and for each suffix $h = 2, \cdots, n$, $F(\xi_h)$ is the maximum of $F(\xi)$ for all ξ in Λ^n that are linearly independent of $\xi_1, \cdots, \xi_{h-1}$;

(3) $F(\xi_1) + \cdots + F(\xi_n) = v_{\mathfrak{q}}(D)$;

(4) the determinant of the components ξ_{hj} of the lattice points $\xi_1, \cdots, \xi_n$ is equal to 1.

2

Let K be a finitely generated extension of k_0 of transcendence degree equal to one. Assume that K is a separable extension of k_0. Further, assume k_0 is algebraically closed in K.

Choose any separating transcendence basis $\{t\}$ of K over k_0, and, as in § 1, let k be the field of rational functions in t with coefficients in k_0. Then K is a separable algebraic extension of k of finite degree n, say.

In the following, elements of k (resp. K) will be denoted by small (resp. capital) Greek letters, and divisors of k (resp. K) by small (resp. capital) German letters. The letters $\mathfrak{p}$ and $\mathfrak{P}$ will be reserved for prime divisors of k and K, respectively. k^* (resp. K^*) will denote the multiplicative group of non-zero elements of k (resp. K). As usual, Z will denote the rational integers.

All results stated without proof in the following are well known, and can be found in [1], [2] or [6].

3

The function fields k and K have infinitely many prime divisors $\mathfrak{p}$ and $\mathfrak{P}$ with the corresponding order valuations

$$v_{\mathfrak{p}} \text{ with } v_{\mathfrak{p}}(0) = \infty, \text{ and } v_{\mathfrak{P}} \text{ with } v_{\mathfrak{P}}(0) = \infty,$$

respectively. We denote the degree of $\mathfrak{p}$ (resp. $\mathfrak{P}$) by $d_{\mathfrak{p}}$ (resp. $d_{\mathfrak{P}}$).

Let $k_{\mathfrak{p}}$ (resp. $K_{\mathfrak{P}}$) denote the completion of k (resp. K) at $\mathfrak{p}$ (resp. $\mathfrak{P}$), $i_{\mathfrak{p}}$ (resp. $I_{\mathfrak{P}}$) the ring of integers of $k_{\mathfrak{p}}$ (resp. $K_{\mathfrak{P}}$), and $\bar{k}_{\mathfrak{p}}$ (resp. $\bar{K}_{\mathfrak{P}}$) the residue field of $i_{\mathfrak{p}}$ (resp. $I_{\mathfrak{P}}$).

Let $\pi \in k_{\mathfrak{p}}$ and $\Pi \in K_{\mathfrak{P}}$ satisfy $v_{\mathfrak{p}}(\pi) = 1$ and $v_{\mathfrak{P}}(\Pi) = 1$, respectively. Then the elements α of $k_{\mathfrak{p}}$ and A of $K_{\mathfrak{P}}$ can be written as series

$$\alpha = \sum_{i=u}^{\infty} \gamma_i \pi^i \text{ and } A = \sum_{i=v}^{\infty} \Gamma_i \Pi^i,$$

where $\gamma_u, \gamma_{u+1}, \cdots$ are representatives of $\bar{k}_{\mathfrak{p}}$ in $k_{\mathfrak{p}}$, and $\Gamma_v, \Gamma_{v+1}, \cdots$ are representatives of $\bar{K}_{\mathfrak{P}}$ in $K_{\mathfrak{P}}$.

Each prime divisor $\mathfrak{P}$ of K divides exactly one prime divisor $\mathfrak{p}$ of k, which is denoted symbolically by

$$\mathfrak{P} \mid \mathfrak{p}, \text{ or conversely } \mathfrak{p} = \mathfrak{p}(\mathfrak{P}).$$

For the corresponding valuations this means that

$$v_{\mathfrak{P}}(\alpha) = e_{\mathfrak{P}} v_{\mathfrak{p}}(\alpha) \text{ for all } \alpha \in k_{\mathfrak{p}}, \tag{1}$$

where $e_{\mathfrak{P}}$ is the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, and for the corresponding residue fields that $\bar{K}_{\mathfrak{P}}$ is a finite extension of $\bar{k}_{\mathfrak{p}}$ of degree $f_{\mathfrak{P}}$, so that

$$d_{\mathfrak{P}} = f_{\mathfrak{P}} d_{\mathfrak{p}}. \tag{2}$$

Further, $K_{\mathfrak{P}}$ is then a finite extension of $k_{\mathfrak{p}}$ of degree $n_{\mathfrak{P}} = e_{\mathfrak{P}} f_{\mathfrak{P}}$.

Conversely

$$\sum_{\mathfrak{P} \mid \mathfrak{p}} n_{\mathfrak{P}} = n, \tag{3}$$

and thus at most n prime divisors of K divide a given prime divisor of k.

Assume that $\mathfrak{P} \mid \mathfrak{p}$. Then there exists an integral basis

$$\Omega_1, \cdots, \Omega_{n_{\mathfrak{p}}}$$

of $K_{\mathfrak{P}}$ over $k_{\mathfrak{p}}$. This means that every $A \in K_{\mathfrak{P}}$ can be written uniquely in the form

$$A = \sum_{i=1}^{n_{\mathfrak{P}}} \alpha_i \Omega_i, \text{ with } \alpha_i \in k_{\mathfrak{p}},$$

and that further $A \in I_{\mathfrak{P}}$ if and only if all $\alpha_i \in i_{\mathfrak{p}}$. It follows that

$$v_{\mathfrak{P}}(A) \geqq e_{\mathfrak{P}} \min_i v_{\mathfrak{p}}(\alpha_i). \tag{4}$$

This estimate is the basis of our subsequent investigations.

The discriminant

$$\delta_{\mathfrak{P}} = \begin{vmatrix} \Omega_1^{(1)}, \cdots, \Omega_1^{(n_{\mathfrak{P}})} \\ \Omega_{n_{\mathfrak{p}}}^{(1)}, \cdots, \Omega_{n_{\mathfrak{p}}}^{(n_{\mathfrak{P}})} \end{vmatrix}^2$$

of the basis $\Omega_1, \cdots, \Omega_{n_{\mathfrak{p}}}$ is an element of $k_{\mathfrak{p}}$. The value $v_{\mathfrak{p}}(\delta_{\mathfrak{P}})$ does not depend on the particular integral basis of $K_{\mathfrak{P}}$ over $k_{\mathfrak{p}}$.

4

We next consider global properties of the function fields k and K.

For each $\alpha \in k^*$ and $A \in K^*$ at most finitely many of the values $v_{\mathfrak{p}}(\alpha)$ and $v_{\mathfrak{P}}(A)$ are distinct from zero. These values are linked by the fundamental equations

$$(1) \qquad \sum_{\mathfrak{p}} d_{\mathfrak{p}} v_{\mathfrak{p}}(\alpha) = 0 \text{ if } \alpha \in k^*, \text{ and } \sum_{\mathfrak{P}} d_{\mathfrak{P}} v_{\mathfrak{P}}(A) = 0 \text{ if } A \in K^*.$$

An element of the free abelian group generated by the prime divisors of k (resp. K) is called a *divisor* of k (resp. K). A divisor $\mathfrak{A}$ of k can therefore be written in the form ("almost all" means "except for finitely many")

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{l_{\mathfrak{p}}}, \text{ with } l_{\mathfrak{p}} \in Z, \text{ and } l_{\mathfrak{p}} = 0 \text{ for almost all } \mathfrak{p},$$

and a divisor $\mathfrak{A}$ of K in the form

$$\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{l_{\mathfrak{P}}}, \text{ with } l_{\mathfrak{P}} \in Z, \text{ and } l_{\mathfrak{P}} = 0 \text{ for almost all } \mathfrak{P}.$$

The exponents $l_{\mathfrak{p}}$ and $l_{\mathfrak{P}}$ are denoted by $v_{\mathfrak{p}}(\mathfrak{a})$ and $v_{\mathfrak{P}}(\mathfrak{A})$, respectively, and the degrees of $\mathfrak{a}$ and $\mathfrak{A}$ are defined to be

$$d(\mathfrak{a}) = \sum_{\mathfrak{p}} d_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{a}) \text{ and } d(\mathfrak{A}) = \sum_{\mathfrak{P}} d_{\mathfrak{P}} v_{\mathfrak{P}}(\mathfrak{A}),$$

respectively. The group of divisors of k (resp. K) is denoted by D_k (resp. D_K).

A divisor $\mathfrak{A} \in D_K$ is said to be *integral* if

$$v_{\mathfrak{P}}(A) \geqq 0 \qquad \text{for all } \mathfrak{P},$$

and we say that $\mathfrak{A}$ divides $\mathfrak{B}$ (written $\mathfrak{A} | \mathfrak{B}$) if the divisor $\mathfrak{B}\mathfrak{A}^{-1}$ is integral.

With each $\alpha \in k^*$ and $A \in K^*$ we associate the divisors

$$[\alpha] = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)} \text{ and } [A] = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(A)},$$

respectively. Such divisors are called *principal*. By the fundamental equation (1), the degree of a principal divisor is equal to zero. The set of all

https://doi.org/10.1017/S1446788700004183 Published online by Cambridge University Press

principal divisors of k (resp. K) is a subgroup of D_k (resp. D_K), which is denoted by P_k (resp. P_K).

We define the two homomorphisms of injection and norm

$$i : D_k \to D_K,$$
$$N : D_K \to D_k$$

as follows. Since D_k and D_K are free abelian groups generated by the prime divisors of k and K, respectively, it suffices to define $i(\mathfrak{p})$ and $N(\mathfrak{P})$. Put

$$i(\mathfrak{p}) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}},$$
$$N(\mathfrak{P}) = \mathfrak{p}(\mathfrak{P})^{f_{\mathfrak{P}}}.$$

From this definition and § 3(2), we see that $d(\mathfrak{A}) = d(N(\mathfrak{A}))$. Henceforth we shall identify $\mathfrak{p}$ and $i(\mathfrak{p})$. With this convention, it follows from § 2(1) that the same divisor $[\alpha]$ is obtained whether α is considered an element of k^* or K^*.

If $\mathfrak{P}|\mathfrak{p}$, let the discriminant $\delta_{\mathfrak{P}}$ of the integral basis $\Omega_1, \cdots, \Omega_{n_{\mathfrak{P}}}$ be defined as in § 3. The non-negative rational integer

$$\nu_{\mathfrak{p}} = \sum_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{p}}(\delta_{\mathfrak{P}})$$

depends only on $\mathfrak{p}$, K and k. We define the local *discriminant* from K to k to be the divisor $\mathfrak{d}_{\mathfrak{p}} = \mathfrak{p}^{\nu_{\mathfrak{p}}}$ of k. Further, as $\mathfrak{p}$ ranges over all prime divisors of k, at most finitely many of the $\nu_{\mathfrak{p}}$ are non-zero. We can therefore define the *discriminant* from K to k to be the divisor

(2) $$\mathfrak{d}_{K|k} = \prod_{\mathfrak{p}} \mathfrak{d}_{\mathfrak{p}}, \text{ and put } \mu_t = \tfrac{1}{2}d(\mathfrak{d}_{K|k}).$$

5

In what follows, we single out the prime divisor $\mathfrak{q}$ of k to play a special role. The valuation $v_{\mathfrak{q}}$ defined in § 1 corresponds to $\mathfrak{q}$. Obviously $d_{\mathfrak{q}} = 1$.

When considered as an element of D_K, $\mathfrak{q}$ will split into factors

(1) $$\mathfrak{q} = \prod_{l=1}^{r} \mathfrak{Q}_l^{e_{\mathfrak{Q}_l}}, \qquad (1 \leqq r \leqq n).$$

Here $d_{\mathfrak{Q}_l} = f_{\mathfrak{Q}_l}$ and the integers $n_l = l_{\mathfrak{Q}_l} f_{\mathfrak{Q}_l}$ satisfy $\sum_{l=1}^{r} n_l = n$.

Henceforth the letter $\mathfrak{r}$ will denote any prime divisor of k not equal to $\mathfrak{q}$, and the letter $\mathfrak{R}$ any prime divisor of K apart from $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_r$; the letter $\mathfrak{Q}$ will denote any of $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_r$. As before, $\mathfrak{p}$ (resp. $\mathfrak{P}$) will denote any prime divisor of k (resp. K). Further, for any divisor $\mathfrak{a} \in D_k$, put

$$\mathfrak{a}_0 = \prod_{\mathfrak{r}} \mathfrak{r}^{v_{\mathfrak{r}}(\mathfrak{a})} \quad \text{and} \quad \mathfrak{a}_\infty = \mathfrak{q}^{v_{\mathfrak{q}}(\mathfrak{a})},$$

and similarly for any divisor $\mathfrak{A} \in D_K$

$$\mathfrak{A}_0 = \prod_{\mathfrak{R}} \mathfrak{R}^{v_{\mathfrak{R}}(\mathfrak{A})} \quad \text{and} \quad \mathfrak{A}_\infty = \prod_{\mathfrak{Q}} \mathfrak{Q}^{v_{\mathfrak{Q}}(\mathfrak{A})}.$$

The results of § 3 may now be applied to each of the prime divisors, separately. Hence for each suffix $l = 1, \cdots, r$, there exists an integral basis

$$\Omega_{l1}, \cdots, \Omega_{ln_l}$$

of $K_{\mathfrak{Q}_l}$ over $k_{\mathfrak{q}}$. Every element A of $K_{\mathfrak{Q}_l}$, and so in particular every element of K, can be written uniquely in the form

$$A = \sum_{i=1}^{n_l} \alpha_{li}\Omega_{li}, \text{ with } \alpha_{li} \in k_{\mathfrak{q}}.$$

Moreover

$$v_{\mathfrak{Q}_l}(A) \geqq e_{\mathfrak{Q}_l} \min_i v_{\mathfrak{q}}(\alpha_{li}) \qquad (l = 1, \cdots, r). \tag{2}$$

We shall apply these estimates shortly.

To overcome a technical point in the proof of our main theorem, it is necessary to consider a certain subgroup of the group D_K. More presicely, we define a *ceiling* of K (this terminology is due to Mahler [4]) to be a divisor $\mathfrak{C}$ of K satisfying the following conditions:

(3) $v_{\mathfrak{Q}}(\mathfrak{C})$ *is an integral multiple of* $e_{\mathfrak{Q}}$ *for all* $\mathfrak{Q}$;

(4) $v_{\mathfrak{R}}(\mathfrak{C})$ *may assume arbitrary integral values for all* $\mathfrak{R}$.

The set of all ceilings of K form a very "large" subgroup of D_K, which we shall denote by C_t. This subgroup clearly depends on the particular transcendental element t of K chosen initially.

6

Let

$$I_t = \bigcap_{\mathfrak{R}} I_{\mathfrak{R}} \text{ and } i_t = \bigcap_{\mathfrak{r}} i_{\mathfrak{r}}.$$

Then I_t is a Dedekind ring whose quotient field is K, and, as before, i_t is the polynomial ring $k_0[t]$, whose quotient field is k. Hence the group of fractional I_t-ideals of K is a free group generated by the prime ideals of I_t, and i_t is a unique factorization domain. In particular, the well known approximation theorem for finitely many $\mathfrak{R}$-adic valuations ([1], [6]) is valid in K.

If $\mathfrak{C}$ is any ceiling, we associate with $\mathfrak{C}$ the set $(\mathfrak{C})_t$ of all elements $A \in K$ satisfying

$$v_{\mathfrak{R}}(A) \geqq v_{\mathfrak{R}}(\mathfrak{C}) \qquad \text{for all } \mathfrak{R}.$$

$(\mathfrak{C})_t$ is then a fractional I_t-ideal. Conversely, to any fractional I_t-ideal there corresponds in this manner infinitely many ceilings. In particular, I_t corresponds to the unit ceiling $\mathfrak{I} = \prod_{\mathfrak{P}} \mathfrak{P}^0$.

The ideal $(\mathfrak{C})_t$ has a basis $B_1, \cdots, B_n$ over i_t as follows. Firstly, every element $A \in (\mathfrak{C})_t$ can be written uniquely in the form

$$A = \sum_{j=1}^{n} \xi_j B_j,$$

where $\xi_1, \cdots, \xi_n$ are polynomials in i_t. Secondly, the discriminant

$$d(B_1, \cdots, B_n) = \begin{vmatrix} B_1^{(1)}, & \cdots, & B_1^{(n)} \\ B_n^{(1)}, & \cdots, & B_n^{(n)} \end{vmatrix}^2$$

on this basis is an element of k^*. Its divisor $\mathfrak{d}_t(\mathfrak{C}) = [d(B_1, \cdots, B_n)]$ does not depend on the particular basis $B_1, \cdots, B_n$.

In the special case when $\mathfrak{C} = \mathfrak{I}$, then it can be shown that $\mathfrak{d}_t(\mathfrak{I})_0 = (\mathfrak{d}_{K|k})_0$. For arbitrary ceilings $\mathfrak{C}$, the divisor $\mathfrak{d}_t(\mathfrak{C})$ is related to the divisor $\mathfrak{d}_t(\mathfrak{I})$ by the equation

$$\mathfrak{d}_t(\mathfrak{C})_0 = (N\mathfrak{C}_0)^2 \mathfrak{d}_t(\mathfrak{I})_0 = (N\mathfrak{C}_0)^2 (\mathfrak{d}_{K|k})_0.$$

Since the divisors $\mathfrak{d}_t(\mathfrak{C})$ and $d_t(\mathfrak{I})$ are both principal, and $d(\mathfrak{C}_0) = d(N(\mathfrak{C}_0))$, it follows that

$$\text{(1)} \qquad \mathfrak{d}_t(\mathfrak{C})_\infty = \mathfrak{p}^{-2d(\mathfrak{C}_0) - d(\mathfrak{d}_{K|k_0})}.$$

7

All elements A of $(\mathfrak{C})_t$ can be written uniquely in the form

$$A = \sum_{j=1}^{n} \xi_j B_j,$$

where $\xi_1, \cdots, \xi_n$ are in i_t. Further, A satisfies the inequalities

$$\text{(1)} \qquad v_{\mathfrak{R}}(A) \geqq v_{\mathfrak{R}}(\mathfrak{C}) \qquad \text{for all } \mathfrak{R}.$$

These inequalities say nothing about the remaining values

$$v_{\mathfrak{Q}}(A) \qquad \text{for all } \mathfrak{Q},$$

and we shall now investigate how large these can be made if $\xi_1, \cdots, \xi_n$ are chosen suitably in i_t. This investigation will depend upon the results from the geometry of numbers collected in § 1.

https://doi.org/10.1017/S1446788700004183 Published online by Cambridge University Press

Let the bases

$$\Omega_{l1}, \cdots, \Omega_{ln_l} \qquad (l = 1, \cdots, r)$$

be defined as in § 5. For each suffix $l = 1, \cdots, r$, each of the basis elements B_j of $(\mathfrak{C})_t$ can be written in the form

$$B_j = \sum_{i=1}^{n_l} \beta_{lij} \Omega_{li}, \text{ with } \beta_{lij} \in k_{\mathfrak{q}} \qquad (j = 1, \cdots, n).$$

Let $\sigma_1, \cdots, \sigma_r$ be elements of $k_{\mathfrak{q}}$ satisfying

$$v_{\mathfrak{q}}(\sigma_l) = v_{\mathfrak{Q}_l}(\mathfrak{C})/e_{\mathfrak{Q}_l} \qquad (l = 1, \cdots, r).$$

Hence, if we put

$$\sigma = \prod_{l=1}^{r} \sigma_l^{n_l}, \text{ then } v_{\mathfrak{q}}(\sigma) = d(\mathfrak{C}_\infty).$$

Now

$$A = \sum_{j=1}^{n} \sum_{i=1}^{n_l} \beta_{lij} \xi_j \Omega_{li} = \sum_{i=1}^{n_l} \sigma_l \mathscr{L}_{li}(\xi) \Omega_{li} \qquad (l = 1, \cdots, r), \tag{2}$$

where, for brevity, we have put

$$\mathscr{L}_{li}(\xi) = \sum_{j=1}^{n} \sigma_l^{-1} \beta_{lij} \xi_j. \tag{3}$$

Since $\sum_{l=1}^{r} n_l = n$, this construction therefore produces n linear forms

$$\mathscr{L}_{li}(\xi) \qquad (l = 1, \cdots, r;\ i = 1, \cdots, n_l)$$

in $\xi_1, \cdots, \xi_n$ with coefficients in $k_{\mathfrak{q}}$. We arrange this system of linear forms lexicographically, and denote its determinant by β.

A simple calculation with determinants shows that

$$d(B_1, \cdots, B_n) = \delta_{\mathfrak{Q}_1} \cdots \delta_{\mathfrak{Q}_r} \beta^2 \sigma^2,$$

whence, in particular, β is non-zero. Further

$$v_{\mathfrak{q}}(\mathfrak{d}_t(\mathfrak{C})) = v_{\mathfrak{q}}(\delta_{\mathfrak{Q}_1} \cdots \delta_{\mathfrak{Q}_r} \beta^2 \delta^2).$$

But, by definition, $v_{\mathfrak{q}}(\delta_{\mathfrak{Q}_1} \cdots \delta_{\mathfrak{Q}_r}) = d(\mathfrak{d}_{K|k_\infty})$ and $v_{\mathfrak{q}}(\sigma) = d(\mathfrak{C}_\infty)$. Hence, combining this result with § 6 (1), it is clear that

$$v_{\mathfrak{q}}(\beta) = -\mu_t - d(\mathfrak{C}), \tag{4}$$

where the constant μ_t is defined by § 4 (2).

Hence, putting

$$F(\xi) = \min_{l,i} v_{\mathfrak{q}}(\mathscr{L}_{li}(\xi)) \text{ for } \xi \in P^n,$$

the results of § 1 imply that there exist n lattice points

$$\xi_h = (\xi_{h1}, \cdots, \xi_{hn}) \in \Lambda^n \qquad (h = 1, \cdots, n),$$

with determinant equal to 1, such that

$$F(\xi_1) \geqq F(\xi_2) \geqq \cdots \geqq F(\xi_n); \tag{5}$$

$$F(\xi_1) + \cdots + F(\xi_n) = v_{\mathfrak{q}}(\beta) = -\mu_t - d(\mathfrak{C}). \tag{6}$$

Therefore, if we define

$$A_h = \sum_{j=1}^{n} \xi_{hj} B_j. \qquad (h = 1, \cdots, n),$$

then $A_1, \cdots, A_n$ is a basis for the ideal $(\mathfrak{C})_t$. From (2) we see that, for each suffix $l = 1, \cdots, r$.

$$A_h = \sum_{i=1}^{n_l} \sigma_l \mathscr{L}_{li}(\xi_h) \Omega_{li} \qquad (h = 1, \cdots, n). \tag{7}$$

and thus by § 5 (2)

$$v_{\mathfrak{Q}_l}(A_h) \geqq v_{\mathfrak{Q}_l}(\mathfrak{C}) + e_{\mathfrak{Q}_l} F(\xi_h) \qquad (h = 1, \cdots, n). \tag{8}$$

Substitute the inequalities (1) and (8) into the fundamental equations

$$\sum_{\mathfrak{P}} d_{\mathfrak{P}} v_{\mathfrak{P}}(A_h) = 0 \qquad (h = 1, \cdots, n), \tag{9}$$

whence we obtain the upper estimate

$$F(\xi_h) \leqq \frac{1}{n} d(\mathfrak{C}) \qquad (h = 1, \cdots, n). \tag{10}$$

Next, substitute all but one of the inequalities (10) into (6). This then gives the lower estimate

$$F(\xi_h) \geqq -\mu_t - \frac{1}{n} d(\mathfrak{C}) \qquad (h = 1, \cdots, n). \tag{11}$$

Combining (8) and (11), we see immediately that, for $h = 1, \cdots, n$,

$$v_{\mathfrak{Q}}(A_h) \geqq v_{\mathfrak{Q}}(\mathfrak{C}) - \frac{e_{\mathfrak{Q}}}{n} d(\mathfrak{C}) - e_{\mathfrak{Q}}\mu_t \qquad \text{for all } \mathfrak{Q}. \tag{12}$$

Finally, substituting all but one of the lower estimates (1) and (12) into (9), it follows that, for $h = 1, \cdots, n$,

$$\begin{aligned} v_{\mathfrak{R}}(A_h) &\leqq v_{\mathfrak{R}}(\mathfrak{C}) + n\mu_t && \text{for all } \mathfrak{R}, \\ v_{\mathfrak{Q}}(A_h) &\leqq v_{\mathfrak{Q}}(\mathfrak{C}) + (n - e_{\mathfrak{Q}})\mu_t - \frac{e_{\mathfrak{Q}}}{n} d(\mathfrak{C}) && \text{for all } \mathfrak{Q}. \end{aligned} \tag{13}$$

Combining these results we arrive at the following theorem.

https://doi.org/10.1017/S1446788700004183 Published online by Cambridge University Press

THEOREM 1. *If $\mathfrak{C}$ is any ceiling of K, and $(\mathfrak{C})_t$ the corresponding ideal, then there exists a basis $A_1, \cdots, A_n$ of $(\mathfrak{C})_t$ such that, for $h = 1, \cdots, n$,*

$$v_{\mathfrak{R}}(\mathfrak{C}) \leqq v_{\mathfrak{R}}(A_h) \leqq v_{\mathfrak{R}}(\mathfrak{C})+n\mu_t \qquad \text{for all } \mathfrak{R},$$

$$v_{\mathfrak{Q}}(\mathfrak{C}) - \frac{e_{\mathfrak{Q}}}{n} d(\mathfrak{C}) - e_{\mathfrak{Q}}\mu_t \leqq v_{\mathfrak{Q}}(A_h) \leqq v_{\mathfrak{Q}}(\mathfrak{C}) - \frac{e_{\mathfrak{Q}}}{n} d(\mathfrak{C}) + (n-e_{\mathfrak{Q}})\mu_t \qquad \textit{for all } \mathfrak{Q}.$$

The basis $A_1, \cdots, A_n$ given by Theorem 1 will henceforth be called a $\mathfrak{C}$-*basis*. The estimates given for the valuations of the basis elements are convenient, but not best possible. We shall return to this question after first giving several applications of Theorem 1.

8

We first apply Theorem 1 to study the approximation of adeles of K by field elements. We recall that an adele $a = \{a_{\mathfrak{P}}\}$ of K is an infinite family, where to each prime divisor $\mathfrak{P}$ of K there corresponds a component $a_{\mathfrak{P}} \in K_{\mathfrak{P}}$, subject to the condition that

$$v_{\mathfrak{P}}(a_{\mathfrak{P}}) \geqq 0 \qquad \text{for almost all } \mathfrak{P}.$$

The set of all adeles of K is an abelian group under componentwise addition, which we denote by $\mathscr{A}_K$. By identifying $A \in K$ with adele $\{A\}$, we see that K can be embedded in $\mathscr{A}_K$. Finally, the degree of an adele $a = \{a_{\mathfrak{P}}\}$ is defined to be

$$d(a) = \sum_{\mathfrak{P}} d_{\mathfrak{P}} v_{\mathfrak{P}}(a_{\mathfrak{P}})$$

and hence is either a rational integer or ∞.

Let $a = \{a_{\mathfrak{P}}\}$ be an adele and $\mathfrak{C}$ any ceiling of K. We first study the approximation of a by field elements at the prime divisors $\mathfrak{R}$.

LEMMA 1. *There exists $B \in K$ such that*

$$v_{\mathfrak{R}}(a_{\mathfrak{R}} - B) \geqq v_{\mathfrak{R}}(\mathfrak{C}) \qquad \textit{for all } \mathfrak{R}.$$

PROOF. The proof is due to Mahler [4]. Let X^* be the set of all $\mathfrak{R}$ for which either $v_{\mathfrak{R}}(a_{\mathfrak{R}})$ is negative or $v_{\mathfrak{R}}(\mathfrak{C})$ is non-zero, so that X^* has only a finite number of elements. Let M be the set of all prime elements of k whose corresponding prime divisors are divisible by at least one prime divisor in X^*. Denote by X and $\bar{X}$ the sets of all prime divisors R which divide, and do not divide, a prime of k corresponding to an element of M, respectively. Denote by $\mathfrak{M}$ the product of all elements of M.

From these definitions

$$v_{\mathfrak{R}}(a_{\mathfrak{R}}) \geqq 0 = v_{\mathfrak{R}}(\mathfrak{C}) = v_{\mathfrak{R}}(\mathfrak{M}) \qquad \text{for all } \mathfrak{R} \in \bar{X}. \tag{1}$$

https://doi.org/10.1017/S1446788700004183 Published online by Cambridge University Press

Choose m to be so large a positive integer that

$$v_{\mathfrak{R}}(\mathfrak{M}^m a_{\mathfrak{R}}) \geqq 0 \qquad \text{for all } \mathfrak{R} \in X.$$

The finitely many elements $\mathfrak{M}^m a_{\mathfrak{R}}$, for $\mathfrak{R} \in X$, are thus $\mathfrak{R}$-adic integers. By the approximation theorem for finitely many $\mathfrak{R}$-adic valuations of K, there exists $C \in I_t$ such that

$$(2) \qquad v_{\mathfrak{R}}(M^m a_{\mathfrak{R}} - C) \geqq v_{\mathfrak{R}}(\mathfrak{C}) + v_{\mathfrak{R}}(\mathfrak{M}^m) \qquad \text{for all } \mathfrak{R} \in X.$$

Choose $B = \mathfrak{M}^{-m}C$. It follows from (2) that

$$v_{\mathfrak{R}}(a_{\mathfrak{R}} - B) \geqq v_{\mathfrak{R}}(\mathfrak{C}) \qquad \text{for all } \mathfrak{R} \in X.$$

Further, the inequalities (1) imply that

$$v_{\mathfrak{R}}(a_{\mathfrak{R}} - B) \geqq \min \{v_{\mathfrak{R}}(a_{\mathfrak{R}}), v_{\mathfrak{R}}(B)\} \geqq 0 = v_{\mathfrak{R}}(\mathfrak{C}) \qquad \text{for all } R \in \bar{X}.$$

Hence B satisfies the assertions of the lemma.

The system of inequalities

$$v_{\mathfrak{R}}(a_{\mathfrak{R}} - A) \geqq v_{\mathfrak{R}}(\mathfrak{C}) \qquad \text{for all } \mathfrak{R},$$

has not only the solution $A = B$ constructed in the last paragraph, but it is more generally satisfied by all elements of the form

$$(3) \qquad A = B + x_1 A_1 + \cdots + x_n A_n$$

where $A_1, \cdots, A_n$ is any $\mathfrak{C}$-basis, and $x_1, \cdots, x_n$ are arbitrary polynomials in i_t.

We now choose the polynomials $x_1, \cdots, x_n$ in such a way that also

$$v_{\mathfrak{Q}}(a_{\mathfrak{Q}} - A) \qquad \text{for all } \mathfrak{Q},$$

allow simple lower estimates. To this end, we note that, by § 7(7), for each suffix $l = 1, \cdots, r$,

$$A_h = \sum_{i=1}^{n_l} \sigma_l \mathscr{L}_{li}(\xi_h) \Omega_{li} \qquad (h = 1, \cdots, n),$$

where the matrix formed from the $\sigma_l \mathscr{L}_{li}(\xi_h)$ has non-zero determinant. Further, there exist n elements $\alpha_{li} \in k_{\mathfrak{q}}$ such that

$$a_{\mathfrak{Q}_l} - B = \sum_{i=1}^{n_l} \alpha_{li} \Omega_{li} \qquad (l = 1, \cdots, r).$$

There exist then $y_1, \cdots, y_n$ in $k_{\mathfrak{q}}$ such that

$$\alpha_{li} = \sum_{h=1}^{n} \sigma_l \mathscr{L}_{li}(\xi_h) y_h \qquad (i = 1, \cdots, n_l; \ \ l = 1, \cdots, r).$$

We now choose the polynomials $x_1, \cdots, x_n$ to satisfy the inequalities

$$v_{\mathfrak{q}}(y_h - x_h) \geqq 1 \qquad (h = 1, \cdots, n).$$

Obviously

$$a_{\mathfrak{Q}_l} - B = (y_1 - x_1)A_1 + \cdots + (y_n - x_n)A_n \qquad (l = 1, \cdots, r),$$

so that by Theorem 1

$$v_{\mathfrak{Q}}(a_{\mathfrak{Q}_l} - B) \geqq v_{\mathfrak{Q}_l}(\mathfrak{C}) - \frac{e_{\mathfrak{Q}_l}}{n} d(\mathfrak{C}) - e_{\mathfrak{Q}_l}(\mu_t - 1) \qquad (l = 1, \cdots, r).$$

We have therefore proven the following theorem.

THEOREM 2. *If $a = \{a_{\mathfrak{P}}\}$ is any adele and $\mathfrak{C}$ any ceiling of K, then there exists $A \in K$ such that*

$$v_{\mathfrak{R}}(a_{\mathfrak{R}} - A) \geqq v_{\mathfrak{R}}(\mathfrak{C}) \qquad \textit{for all } \mathfrak{R},$$

$$v_{\mathfrak{Q}}(a_{\mathfrak{Q}} - A) \geqq v_{\mathfrak{Q}}(\mathfrak{C}) - \frac{e_{\mathfrak{Q}}}{n} d(\mathfrak{C}) - e_{\mathfrak{Q}}(\mu_t - 1) \qquad \textit{for all } \mathfrak{Q}.$$

COROLLARY. *To every adele a there exists $A \in K$ such that the degree of the adele $a - A$ is at least $n(1 - \mu_t)$.*

This theorem is essentially equivalent to the Riemann-Roch Theorem (see [1] or [3]). In the next section we shall indicate how to derive the Riemann-Roch Theorem from it, and conversely, we can deduce a slightly improved version of it from the Riemann-Roch Theorem, although we do not give the details here.

9

We next give one application of Theorem 2. If $\mathfrak{A}$ is any divisor of K, we define $\Lambda(\mathfrak{A})$ to be the set of all adeles $a = \{a_{\mathfrak{P}}\}$ of K satisfying

$$v_{\mathfrak{P}}(a_{\mathfrak{P}}) \geqq v_{\mathfrak{P}}(\mathfrak{A}) \qquad \text{for all } \mathfrak{P}.$$

Both $\mathscr{A}_K$ and $\Lambda(\mathfrak{A})$ are vector spaces over k_0, and we now investigate the k_0-dimension of the quotient space $\mathscr{A}_K/\Lambda(\mathfrak{A}) + K$.

THEOREM 3. *If $\mathfrak{A}$ is any divisor of K, then the k_0-dimension of the quotient space $\mathscr{A}_K/\Lambda(\mathfrak{A}) + K$ is at most* $\max\{0, d(\mathfrak{A}) + n(\mu_t - 1)\}$.

PROOF. For this paragraph only, let us choose the transcendence basis $\{t\}$ of K over k_0 so that $\mathfrak{q}$ is unramified in K, i.e. $e_{\mathfrak{Q}_1} = \cdots = e_{\mathfrak{Q}_r} = 1$. This is always possible since only a finite number of prime divisors of a given rational subfield of K ramify in K. With this choice of transcendence basis, the ceiling group C_t is equal to D_K.

If x is a real number, $[x]$ denotes, as usual, the integral part of x.

If $\mathfrak{A}$ is any divisor of K, put $s = \max\{0, [(1/n)d(\mathfrak{A}) + \mu_t - 1]\}$. By Theorem 2, for every adele $a = \{a_{\mathfrak{P}}\}$ of K, there exists $A \in K$ satisfying

$$v_{\mathfrak{R}}(a_{\mathfrak{R}}-A) \geqq v_{\mathfrak{R}}(\mathfrak{A}) \qquad \text{for all } \mathfrak{R}$$
$$v_{\mathfrak{Q}}(a_{\mathfrak{Q}}-A) \geqq v_{\mathfrak{Q}}(\mathfrak{A})-s \qquad \text{for all } \mathfrak{Q}$$

Hence, if $\pi \in k_{\mathfrak{q}}$ satisfies $v_{\mathfrak{q}}(\pi) = 1$, and if, for each suffix $l = 1, \cdots, r$, $w_{l1} \cdots, w_{ln_l}$ are representatives in $K_{\mathfrak{Q}_l}$ of a basis of $\bar{K}_{\mathfrak{Q}_l}$ over k_0, then there exist $\alpha_{jij} \in k_0$ such that

$$v_{\mathfrak{Q}_l}\Big(a_{\mathfrak{Q}_l}-A-\sum_{i=0}^{s-1}\sum_{j=1}^{f_{\mathfrak{Q}_l}} \alpha_{lij} w_{lj} \pi^{v_{\mathfrak{Q}_l}(A)-s+i}\Big) \geqq v_{\mathfrak{Q}_l}(\mathfrak{A}) \qquad (l = 1, \cdots, r).$$

Thus the images of the adeles

$$b_{lij} = \{b_{lij\mathfrak{P}}\}, \text{ where } b_{lij\mathfrak{P}} = \begin{cases} w_{lj}\pi^{v_{\mathfrak{Q}_l}(\mathfrak{A})-s+i} & \text{if } \quad P = \mathfrak{Q}_l \\ 0 & \text{if } \quad P \neq \mathfrak{Q}_l \end{cases}$$
$$(l = 1, \cdots, r;\ i = 0, \cdots, s-1;\ j = 1, \cdots, f_{\mathfrak{Q}_l})$$

under the canonical homomorphism $\mathscr{A}_K \to \mathscr{A}_K/\Lambda(\mathfrak{A})+K$ generate $\mathscr{A}_K/(\mathfrak{A})+K$ over k_0. Since the number of these adeles is at most $\max\{o, d(\mathfrak{A})+n(\mu_t-1)\}$, this completes the proof.

It is a routine matter to deduce the indefinite form of the Riemann-Roch Theorem from Theorem 3 (see (1), (3)). We omit the details. The definite form of the Riemann-Roch Theorem implies that the constant $n(\mu_t-1)$ appearing in Theorem 3 can be improved to the best possible value $2g-1$, i.e. $2(\mu_t-n)+1$, using the classical formula $g = \mu_t-n+1$ for the genus of K. The above estimate is therefore quite good, despite the bad estimates of § 7.

10

As a second application of Theorem 1, we study the approximation of elements of K by elements of K. The Thue-Siegel-Mahler-Roth Theorem shows that this approximation cannot be very good. The following theorem is in the opposite direction.

THEOREM 4. *If A is any element of K^*, then there exists an infinite sequence $B_1, B_2, \cdots$ of distinct elements of K^* such that*

$$\lim_{h\to\infty} d([A-B_h]_\infty) = \infty,$$

and

$$d([A-B_h]_\infty) \geqq d([B_h]_\infty)+n(1-\mu_t) \qquad (h = 1, 2, \cdots).$$

PROOF. Let $\mathfrak{C}_1$ be an ceiling of K such that

(1) $$-d(\mathfrak{C}_{10})+n(1-\mu_t) < d([A]_\infty),$$

and let $A_1, \cdots, A_n$ be a $\mathfrak{C}_1$-basis. A can be written in the form

https://doi.org/10.1017/S1446788700004183 Published online by Cambridge University Press

$A = y_1A_1 + \cdots + y_nA_n$, where $y_1, \cdots, y_n$ are in k. Thus, if we choose polynomials $x_1, \cdots, x_n$ to satisfy

$$v_{\mathfrak{Q}}(y_i - x_i) \geqq 1 \qquad (i = 1, \cdots, n),$$

then, by Theorem 1, the element $B_1 = x_1A_1 + \cdots x_nA_n$ of $(\mathfrak{C}_1)_t$ satisfies

$$d([A-B_1)_\infty] \geqq -d(\mathfrak{C}_{10}) + n(1-\mu_t).$$

But by the choice (1) of $\mathfrak{C}_1$, we see that B_1 is non-zero, and therefore, by the fundamental equation $\sum_{\mathfrak{P}} d_{\mathfrak{P}} v_{\mathfrak{P}}(B_1) = 0$, it follows that

$$(2) \qquad d([A-B_1]_\infty) \geqq d([B_1)_\infty) + n(1-\mu_t).$$

Now choose any ceiling $\mathfrak{C}_2$ satisfying

$$(3) \qquad -d(\mathfrak{C}_{20}) + n(1-\mu_t) > d([A-B_1]_\infty),$$

and construct the approximating element B_2 just as B_1 was constructed for the ceiling $\mathfrak{C}_1$. By (3) it is immediate that

$$d([A-B_2]_\infty) > d([A-B_1]_\infty).$$

Continuing in this manner, it is clear that we can construct the required sequence $B_1, B_2, \cdots$. This completes the proof.

11

As a final application of the results of § 7, we derive an analogue of a theorem of Minkowski. Let D_{K0} be the set of all divisors of K of the form $\mathfrak{A}_0$ for some divisor $\mathfrak{A} \in D_K$, and let P_{K0} be the subgroup of D_{K0} consisting of all divisors of the form $[A]_0$ for some $A \in K^*$. The elements of the quotient group D_{K0}/P_{K0} are called *divisor classes*.

THEOREM 5. *In every divisor class of the group D_{K0}/P_{K0} there is an integral divisor $\mathfrak{A}_0$ satisfying $0 \leqq d(\mathfrak{A}_0) \leqq \mu_t$.*

PROOF. As mentioned before, the estimates given in Theorem 1 are not best possible. In particular, taking § 7(5) and § 7(6) together, we can immediately give the better estimate $F(\xi_1) \geqq -\mu_t/n - 1/n\, d(\mathfrak{C})$, whence the basis element A_1 defined in § 7 satisfies.

$$v_{\mathfrak{Q}}(A_1) \geqq v_{\mathfrak{Q}}(\mathfrak{C}) - \frac{e_{\mathfrak{Q}}\mu_t}{n} - \frac{e_{\mathfrak{Q}}}{n} d(\mathfrak{C}) \qquad \text{for all } \mathfrak{Q}$$

Hence we have shown that, for every ceiling $\mathfrak{C}$, there exists a non-zero element A of $(\mathfrak{C})_t$ satisfying $d([A]_\infty) \geqq -d(\mathfrak{C}_0) - \mu_t$.

Now let $\mathfrak{B}_0$ be any divisor in D_{K0}. Then, by the remark just made, there exists a non-zero element $A \in (\mathfrak{B}_0^{-1})_t$ satisfying $d([A]_\infty) \geqq -d(\mathfrak{B}_0^1) - \mu_t$.

The fundamental equation $\sum_{\mathfrak{P}} d_{\mathfrak{P}} v_{\mathfrak{P}}(A) = 0$ therefore implies that $d([A]_0) \leqq d(\mathfrak{B}_0^{-1})+\mu_t$. Hence the divisor $\mathfrak{A}_0 = [A]_0\mathfrak{B}_0$ is an integral divisor in the same class as $\mathfrak{B}_0$ satisfying $0 \leqq d(\mathfrak{A}_0) \leqq \mu_t$. This completes the proof.

In the case when the constant field k_0 is finite, there are only finitely many integral divisors having degree at most μ_t. Thus Theorem 5 implies the classical result that the group D_{K0}/P_{K0} is finite and, in addition, gives quite a good estimate for the order of this group.

One can make further application of Theorem 1 when the constant field k_0 is finite (e.g. many of Mahler's results for algebraic number fields carry over verbatim to function fields over k_0). We omit the details.

Finally, I note that Eichler has also used an analogue of the geometry of numbers for fields of formal power series to obtain the Riemann-Roch Theorem for function fields of one variable. However, he uses an analogue of Minkowski's theorem on linear forms, rather than an analogue of Minkowski's theorem on the successive minima of a distance function, as we have done. Naturally, both methods give substantially the same result when applicable. Eichler's results can be found in his book. "Einführung in die Theorie der algebraischen Zahlen und Funktionen".

References

[1] E. Artin, *Algebraic numbers and algebraic functions* (Princeton University, 1951).
[2] H. Hasse, *Zahlentheorie* (Akademie-Verlag, Berlin, 1963).
[3] S. Lang, '*Introduction to algebraic geometry*' (Interscience, New York, 1958).
[4] K. Mahler, 'Inequalities for ideal bases in algebraic number fields', *J. Aust. Math. Soc.* 4 (1964), 425–448.
[5] K. Mahler, 'Analogue of Minkowski's geometry of numbers in fields of series', *Ann. of Math.*, 42 (1941), 488–522.
[6] O. O'Meara, *Introduction to quadratic forms* (Springer-Verlag, Berlin, 1963).

Australian National University
Canberra, A.C.T.