ON UNIQUE FACTORIZATION IN ALGEBRAIC FUNCTION FIELDS

BY

J. V. Armitage

1. Introduction

Let K be a field of algebraic functions of one variable over an algebraically closed field k and let R be an integrally closed sub-domain of K, properly containing k, which is contained in all but a finite number of valuation rings of K/k. Cunnea [3, Corollary 4.2] has proved that R is a unique factorization domain if and only if K has genus 0. The present writer [1][1] has discussed the question of the existence of a euclidean algorithm in a ring which is essentially like R and, in particular, has proved that R is euclidean if K has genus 0. As usual, the existence of a euclidean algorithm in R implies that factorization is unique. In the light of this and of Cunnea's results the following is perhaps of interest.

Theorem. *Let K be a field of algebraic functions of one variable over an infinite field k and let R be an integrally closed sub-domain of K, properly containing k, which has no poles outside a finite set $S = \{\mathfrak{P}_1, \cdots, \mathfrak{P}_s\}$ of places of K/k. Then R is euclidean if and only if*

$$g + d_S = 1, \tag{1}$$

where g is the genus of K and d_S is the greatest common divisor of the degrees of the places in S.

We recall the essential results of [1] and deduce the sufficiency part of the theorem in §2. In §3 we prove a lemma on linear spaces and the proof of the theorem is concluded in §4. The case of finite k is mentioned in §5.

2. Euclid's algorithm in function fields

Let $\mathfrak{b}$ be a divisor of K based on the set S and let $\mathfrak{L}(\mathfrak{b}, S)$ denote the set

$$\mathfrak{L}(\mathfrak{b}, S) = \{\beta \in K : \nu_{\mathfrak{P}_i}(\beta) \geq \nu_{\mathfrak{P}_i}(\mathfrak{b}), \mathfrak{P}_i \in S\}, \tag{2}$$

where $\nu_{\mathfrak{P}_i}$ denotes the order function at $\mathfrak{P}_i$. By a straightforward adaptation of the argument in [1], it follows that R is a euclidean domain if and only if

$$K = \bigcup (\mathfrak{L}(\mathfrak{b}, S) + R), \tag{3}$$

where the union is taken over all divisors $\mathfrak{b}$ based on S such that $\deg(\mathfrak{b}) \geq 1$. Moreover

Received March 18, 1966.

[1] In [1], k was a finite field; the extension to an infinite field presents no difficulty. Section 7 of [1] is fallacious, but is not relevant to the present paper; see Corrigendum and Addendum to appear in J. London Math. Soc.

(4)
$$\dim_k K \,/\, (\mathfrak{L}(\mathfrak{b}, S) + R) = \deg(\mathfrak{b}) + l(\mathfrak{b}) - 1 + g$$
$$= \delta(\mathfrak{b}^{-1}),$$

where $\delta(\mathfrak{b}^{-1})$ denotes the dimension of the space of differentials which are $\equiv 0 \pmod{\mathfrak{b}^{-1}}$. It is an immediate consequence of (3) and (4) that R is euclidean if $g = 0$ and $\deg(\mathfrak{b}) = 1$. This proves the sufficiency part of the theorem.

3. A lemma on linear spaces

To prove necessity, we must examine the implications of (3) and for this we require the following lemma.

LEMMA. *Let $L_1, \cdots, L_N$ be sub-spaces of K over k and suppose that*

$$K = L_1 \cup \cdots \cup L_N .$$

Then $K = L_i$ for some i with $1 \leq i \leq N$.

Proof. (Induction on N.) If $N = 1$, there is nothing to prove. Suppose that the lemma has been proved for fewer than N linear spaces, that

$$K = L_1 \cup \cdots \cup L_N$$

and that $K \neq L_i$ for each i. Then

$$K \neq L_2 \cup \cdots \cup L_N$$

by the induction hypothesis. Hence there exists $\alpha_1 \in L_1$ but $\alpha_1 \notin L_i$ $(2 \leq i \leq N)$. Similarly, there exists $\alpha_2 \in L_2$ but $\alpha_2 \notin L_i$ $(i = 1, 3, \cdots, N)$. Now the elements $\alpha_1 + \lambda_1\alpha_2, \cdots, \alpha_1 + \lambda_N \alpha_2$ of K, where $\lambda_1, \cdots, \lambda_N$ are distinct elements of k (k is infinite), are all different. Also, none of these vectors is in L_2, for $\alpha_1 + \lambda_i \alpha_2 \in L_2$ implies $\alpha_1 + \lambda_i \alpha_2 - \lambda_i \alpha_2 \in L_2$ implies $\alpha_1 \in L_2$—a contradiction.

Thus two distinct vectors belong to the same sub-space; say

$$\alpha_1 + \lambda_i \alpha_2 \in L_t, \quad \alpha_1 + \lambda_j \alpha_2 \in L_t, \qquad t \neq 2, i \neq j.$$

Hence

$$(\alpha_1 + \lambda_i \alpha_2) - (\alpha_1 + \lambda_j \alpha_2) \in L_t .$$

That is,

$$(\lambda_i - \lambda_j)\alpha_2 \in L_t .$$

But $\lambda_i \neq \lambda_j$; so $\alpha_2 \in L_t$, $t \neq 2$—a contradiction. This proves the lemma.

4. Proof of the theorem

We must prove that if $g + d_S > 1$ then R is not euclidean.

Let $\mathfrak{a}$ be a fixed divisor of K, based on S, of degree $<2 - 2g$. Let

(5)
$$K_0 = \mathfrak{L}(\mathfrak{a}, S)$$

Then $\deg(\mathfrak{a}^{-1}) > 2g - 2$ and so

(6) $$\dim_k K/(K_0 + R) = \delta(\mathfrak{a}^{-1}) = 0.$$

Hence, $K = K_0 + R$, or, in other words, the neighbourhood K_0 when translated along the lattice R covers K. Evidently (1) holds if and only if

(7) $$K_0 \subset K_0 \cap [\bigcup (\mathfrak{L}(\mathfrak{b}, S) + R)].$$

We regard K as being embedded in the locally linearly compact space

$$\hat{E} = \hat{K}_{\mathfrak{P}_i} \times \cdots \times \hat{K}_{\mathfrak{P}_s}$$

where $\hat{K}_{\mathfrak{P}_i}$ denotes the completion of K, considered as for $\mathfrak{P}_i$, at $\mathfrak{P}_i$ with respect to the valuation

$$\| \alpha \|_{\mathfrak{P}_i} = c^{v_{\mathfrak{P}_i}(\alpha)}, \qquad \alpha \in K, 0 < c < 1.$$

(See [4] and [5].)

The idea of the proof is to show that either (7) does not hold (in which case R is not euclidean) or that it holds with a *finite* union; say

(8) $$K_0 \subset K_0 \cap [L_1 \cup \cdots \cup L_N],$$

where $L_i = \mathfrak{L}(\mathfrak{b}_i, S) + R$ for some $\mathfrak{b}_i$, $1 \leq i \leq N$. In the latter case, we use the lemma to show that R is not euclidean.

We suppose that the linear spaces $L = \mathfrak{L}(\mathfrak{b}, S) + R$ have been ordered in some way (this is clearly possible) and for each n we consider all cosets

(9) $$L_1 + \lambda_1, \cdots, L_n + \lambda_n$$

of $L_1, \cdots, L_n$ with $\lambda_i \notin L_i$, $\lambda_i \in K$. Denote by $\mathfrak{F}_n$ the set of all intersections

$$F_n = \bigcap_{i=1}^{n} (L_i + \lambda_i)$$

formed from these cosets. Then either

(10) $$K_0 \cap F_n = \emptyset$$

for every $F_n \in \mathfrak{F}_n$, or there exist $\lambda_1, \cdots, \lambda_n$ in K such that for the corresponding F_n

(11) $$K_0 \cap F_n \neq \emptyset.$$

In case (10) we know that

$$K_0 = \bigcup_{i=1}^{n} L_i,$$

and so we are in the situation (8).

If (11) holds for every n, then there exists a sequence $(\lambda_i)_{i \in \mathbf{N}}$ such that for every *finite* sub-family the corresponding F_n satisfies

(12) $$K_0 \cap F_n \neq \emptyset.$$

But K_0 is linearly compact and so

(13) $$K_0 \cap F \neq \emptyset,$$

where

$$F = \bigcap_{i=1}^{\infty} (L_i + \lambda_i).$$

Hence, there exists $\alpha \in K$ which is not in any of the L_i and so

$$K \neq \bigcup L_i .$$

This means (cf. (3)) that R cannot be euclidean.

Thus, either R is not euclidean (in which case there is nothing to prove) or it follows from (8) that

$$K = L_1 \cup \cdots \cup L_N .$$

By the lemma, $K = L_i$ for some i. But this is impossible if $g + d_S > 1$, from (4). Hence R is not euclidean, and the proof of the theorem is complete.

5. The case of finite k

The proof breaks down in the case when k is finite, which is the case most closely related to classical number theory. The theorem still holds if S contains exactly two places, but I have not been able to extend the argument to the general case.

BIBLIOGRAPHY

1. J. V. ARMITAGE, *Euclid's algorithm in algebraic function fields*, J. London Math. Soc., vol. 38 (1963), pp. 55–59.
2. C. CHEVALLEY, *Algebraic functions of one variable*, Amer. Math. Soc. Surveys, no. 6, 1951.
3. W. M. CUNNEA, *On the rings of valuation vectors*, Illinois J. Math., vol. 8 (1964), pp. 425–438.
4. K. IWASAWA, Ann. of Math., vol. 57 (1953), pp. 331–356.
5. S. LEFSCHETZ, *Algebraic topology*, Amer. Math. Soc. Colloquium Publications, vol. 27, 1942.

UNIVERSITY OF DURHAM
DURHAM CITY, ENGLAND