Can. J. Math., Vol. XLII, No. 6, 1990, pp. 1041–1052

ON RINGS WITH A CERTAIN TYPE OF FACTORIZATION AND COMPACT RIEMANN SURFACES

PASCUAL CUTILLAS RIPOLL

ABSTRACT. Let $\mathcal{V}$ be a compact Riemann surface, $\mathcal{V}'$ be the complement of a nonvoid finite subset of $\mathcal{V}$ and $A(\mathcal{V}')$ be the ring of finite sums of meromorphic functions in $\mathcal{V}'$ with finite divisor. In this paper it is proved that every nonzero $f \in A(\mathcal{V}')$ can be decomposed as a product $\alpha\beta$, where α is either a unit or a product of powers of irreducible elements of $A(\mathcal{V}')$, uniquely determined by f up to multiplication by units, and β is a product of functions of the type $e^{\varphi} - 1$, with φ holomorphic and nonconstant in $\mathcal{V}'$. Furthermore, a similar result is obtained for a certain class of subrings of $A(\mathcal{V}')$.

1. Introduction and notations. Let $\mathcal{V}$ be a compact Riemann surface and $\mathcal{V}'$ be the complementary of a nonempty finite subset of $\mathcal{V}$. It is a clear consequence of Weierstrass theorem, on the existence of functions with prescribed divisor, that the only irreducible elements in the ring $O(\mathcal{V}')$ of holomorphic functions on $\mathcal{V}'$ are the functions which have a simple zero at a unique point of $\mathcal{V}'$ and no other zero in $\mathcal{V}'$. Therefore, it is evident that every function in $O(\mathcal{V}')$ which has an infinite divisor can not be expressed as a finite product of irreducible functions.

Our aim in this paper is to show that the behaviour of the ring $A(\mathcal{V}')$, generated by all meromorphic functions with finite divisor on $\mathcal{V}'$, with respect to the existence of irreducible functions and to the existence of factorizations, is very different from that of $O(\mathcal{V}')$. In fact, we shall prove that every non-identically-zero function f in $A(\mathcal{V}')$ is, roughly speaking, a product of irreducible functions uniquely determined by f up to multiplication by units, and of functions of the type $e^{\varphi} - 1$, with $\varphi \in O(\mathcal{V}') - \mathbb{C}$. As a consequence we shall deduce that there are nontrivial discrete valuations of the field of fractions $K(\mathcal{V}')$ of $A(\mathcal{V}')$ which assign the value zero to every function with finite divisor. Moreover, we shall extend these results to certain subrings of $A(\mathcal{V}')$, including, for instance, the ring generated over the field $\mathcal{M}(\mathcal{V})$ of meromorphic functions in $\mathcal{V}$ by the so-called Baker-Akhiezer functions in $\mathcal{V}'$, or also the ring generated over $\mathcal{M}(\mathcal{V})$ by the meromorphic functions with finite divisor in the complementary of a non-Weierstrass fixed point of $\mathcal{V}$, and whose logarithmic differential has at this point an order not less than $-g-1$, where g is the genus of $\mathcal{V}$; this last

Received January 11, 1990.

AMS (1980) subject classification: 30F10, 30D30.

ring being actually shown to be factorial, as well as every ring corresponding in the analogous way to a minimal W-field in $\mathcal{V}'$ (see Cutillas [2]).

In Section 2 we shall construct an associated sequence of factorial rings whose union is $A(\mathcal{V}')$. This sequence will be used in Section 3, after defining a class of rings, which we shall call 'semifactorial" because there exists in them a certain type of factorization which generalize that of factorial rings, in order to prove the existence of such a factorization for functions in $A(\mathcal{V}')$. Finally, in Section 4 we shall determine all functions which have no irreducible divisor in $A(\mathcal{V}')$ (here, of course, the word "divisor" means a function that divides a given one; and, there will be no risk of confusion on using also this other sense of it), whereupon we shall be able to obtain the final form of the factorization theorem.

The following notations will be utilized throughout this paper.

For every connected open subset U of $\mathcal{V}$, $\mathcal{M}(U)$ will be the field of meromorphic functions on U, $\mathcal{M}^*(U)$ the multiplicative group formed by the meromorphic functions on U which are not identically zero, $O(U)$ the ring of holomorphic functions on U and $E(U) = \{e^h : h \in O(U)\}$.

$\mathcal{V}'$, $A(\mathcal{V}')$ and $K(\mathcal{V}')$ will be as in the Introduction and $G(\mathcal{V}')$ will be the multiplicative group formed by the functions in $\mathcal{M}(\mathcal{V}')$ which have a finite divisor. For every subfield k of $\mathcal{M}(\mathcal{V}')$, we shall set $G(k) = k \cap G(\mathcal{V}')$, $E(k) = k \cap E(\mathcal{V}')$ and $A(K) = k \cap A(\mathcal{V}')$.

For every function $f \in G(\mathcal{V}')$, $\bar{f}$ will denote the class of f in the quotient group $G(\mathcal{V}')/\mathcal{M}^*(\mathcal{V})$ (i.e. the image of f by the quotient mapping).

We finish this introductory section with the statement of a theorem which will be useful later.

THEOREM 1.1. *If $f_1, \dots, f_n$ are functions in $G(\mathcal{V}')$ such that $f_1 + \cdots + f_n = 0$, every sum of all functions in the set $\{f_1, \dots, f_n\}$ having the same class in the quotient $G(\mathcal{V}')/\mathcal{M}^*(\mathcal{V})$ is also null.*

A proof of this theorem can be found in Cutillas [2].

2. An associated sequence of factorial rings. The fundamental idea of the proofs of our factorization theorems for functions in $A(\mathcal{V}')$ is to relate this ring with certain rings of polynomials. We shall do this after recalling a concept which was introduced in Cutillas [2].

Definition 2.1. We shall say that a subfield k of $\mathcal{M}(\mathcal{V}')$ verifies the Weierstrass property (or, for short, that it is a W-field) in $\mathcal{V}'$, if k contains $\mathcal{M}(\mathcal{V})$ and if δ being an arbitrary finite divisor on $\mathcal{V}'$, there is a function in k whose divisor is δ.

It was also proved in Cutillas [2] the following:

THEOREM 2.2. *There exist minimal W-fields in $\mathcal{V}'$. If k is such a field, then $E(k) = \mathbb{C}^*$ and $G(k)/\mathcal{M}^*(\mathcal{V})$ is a divisible group.*

From now on, throughout this section, k_0 will be a fixed minimal W-field in $\mathcal{V}'$. It is, of course, a consequence of its minimality that k_0 is generated by functions with finite divisor.

The following theorem will permit us to select a useful system of generators of the group $G(\mathcal{V}')/\mathcal{M}^*(\mathcal{V})$.

THEOREM 2.3. *For every function $f \in G(\mathcal{V}')$ there exist $f_1 \in G(k_0)$ and $f_2 \in E(\mathcal{V}')$, uniquely determined up to multiplicative constants, such that $f = f_1 f_2$.*

Proof. Let f_1 be a function in $G(k_0)$ such that $\mathrm{Res}(d\log f_1, p) = \mathrm{Res}(d\log f, p)$ (we are using here the standard notation denoting residues) for every $p \in \mathcal{V}$, and such that the integrals of $d\log f_1$ and $d\log f$ along suitable closed curves defining a canonical system of generators of the first fundamental group of $\mathcal{V}$ coincide (see Theorem 8.4 in Cutillas [2]). Then, the integral of $d\log(ff_1^{-1})$ along any closed curve in $\mathcal{V}'$ is null, and so $ff_1^{-1} \in E(\mathcal{V}')$. The uniqueness of f_1 is a consequence of Theorem 2.2.

Let H be a (fixed from now on) vector subspace of $O(\mathcal{V}')$ such that $O(\mathcal{V}') = H \oplus \mathbb{C}$, and $e^H = \{e^h : h \in H\}$. Then, Theorem 2.3 implies that for every $f \in G(\mathcal{V}')$ there exist $f_1 \in G(k_0)$ and $f_2 \in e^H$, uniquely determined by f, such that $f = f_1 f_2$. Therefore, there is a set $\{f_i\}_{i\in I}$ of functions in $G(\mathcal{V}')$ such that $\{\bar{f}_i\}_{i\in I}$ is a basis of $G(\mathcal{V}')/\mathcal{M}^*(\mathcal{V})$, considered as a Q-vector space (bear in mind that $G(\mathcal{V}')/\mathcal{M}^*(\mathcal{V}')$ is a divisible group without torsion), and such that it is the union of subsets $\{f_i\}_{i\in I'}$, and $\{f_i\}_{i\in I''}$, verifying that $\{\bar{f}_i\}_{i\in I'}$, and $\{f_i\}_{i\in I''}$ are bases (in the same sense) of $G(k_0)/\mathcal{M}^*(\mathcal{V})$ and e^H respectively. Consider now for every $i \in I$ and $n \in \mathbb{N}$, functions $f_{i,n} \in G(\mathcal{V}')$ and $h_{i,n} \in M^*(\mathcal{V})$, such that $f_i = f_{i,n}^n h_{i,n}$, taking in particular $f_{i,1} = f_i$ for every $i \in I$ and $h_{i,n} = 1$ for every $i \in I''$, $n \in \mathbb{N}$; and let A_n be, for every $n \in \mathbb{N}$, the subring of $A(\mathcal{V}')$ generated by the functions $\{f_{i,n}\}_{i\in I}$, and their inverses, over the field $\mathcal{M}(\mathcal{V})$. Then, it is clear that $A_n \subset A_m$, if n divides m, and that $A(\mathcal{V}') = \bigcup_{n=1}^{\infty} A_n$.

Let now B be the localization of the ring of polynomials in the set of independent variables $\{t_i\}_{i\in I}$ (with subindices in the same above considered set I), with coefficients in $\mathcal{M}(\mathcal{V})$, with respect to the multiplicative system formed by the products of powers of the variables $\{t_i\}_{i\in I}$. Then, B is a factorial ring, since every ring of polynomials with coefficients in a field is factorial and localization preserves factoriality (see, for instance, Bourbaki [1], chapter 7). Moreover, we have:

THEOREM 2.4. *For every $n \in \mathbb{N}$, A_n and B are isomorphic rings.*

Proof. It will suffice to see that, for every $n \in \mathbb{N}$, $\{f_{i,n}\}_{i\in I}$ is a transcendence basis of the field of fractions K_n of A_n over $\mathcal{M}(\mathcal{V})$. Since every function in K_n

is a quotient of polynomials in the $\{f_{i,n}\}_{i\in I}$ with coefficients in $\mathcal{M}(\mathcal{V})$, it is also sufficient to show that $\{f_{i,n}\}_{i\in I}$ is an algebraically independent set; but this is a consequence of Theorem 1.1.

Thus, we have proved that $A(\mathcal{V}')$ coincides with the union of the factorial rings of the associated sequence (A_n). However, without more information, we can by no means deduce that $A(\mathcal{V}')$ is factorial (which is false) or that there exists any sort of factorization for the elements of $A(\mathcal{V}')$. In the remaining sections we shall obtain sufficient supplementary information for proving the existence of the desired factorizations. For the moment, we finish this section with two basic results. The first of them relates the irreducibility of a function in $A(\mathcal{V}')$ with the irreducibility of this function in the different rings A_n. We do not detail its proof which is quite easy.

THEOREM 2.5. *The following conditions on a function $f \in A(\mathcal{V}')$ are equivalent:*

1) f is irreducible in $A(\mathcal{V}')$.

2) f is irreducible in every ring A_n which contains it.

3) There exists $n \in \mathbb{N}$ such that $f \in A_n$ and such that for every multiple $m \in \mathbb{N}$ of n, f is irreducible in A_m.

It is clear that if f is a function in $G(\mathcal{V}')$, f is invertible in $A(\mathcal{V}')$. Furthermore, it is also easy to prove:

THEOREM 2.6. *A function f in $A(\mathcal{V}')$ is invertible if and only if it belongs to $G(\mathcal{V}')$.*

Proof. If f is invertible in $A(\mathcal{V}')$, it can not have infinitely many zeroes in $\mathcal{V}'$.

Remark. For every $n \in \mathbb{N}$ and every multiple $m \in \mathbb{N}$ of n, different from n, there exist elements of A_n which are irreducible in A_n and factorize nontrivially in A_m. In fact, if $P(t_1, \ldots, t_r)$ is an irreducible polynomial in r independent variables with coefficients in $\mathcal{M}(\mathcal{V})$, and $f_{i_1,m}, \ldots, f_{i_r,m} \in \{f_{i,m}\}_{i\in I}$ (notations as before Theorem 2.4), and if ϵ is a primitive $\frac{m}{n}$-th root of unity, the product of all functions of the type $P(\epsilon^{p_1} f_{i_1,m}, \ldots, \epsilon^{p_r} f_{i_r,m})$ (with $p_1, \ldots, p_r \in \mathbb{N}$) which are essentially different (i.e. no quotient of two of them is a root of unity), is of the type $Q(f_{i_1,n}, \ldots, f_{i_r,n})$, wherein $Q(t_1, \ldots, t_r)$ is also an irreducible polynomial, and so this product is an irreducible element of A_n.

3. Semifactorial rings. We shall prove in this section the existence of a first kind of factorization for functions in $A(\mathcal{V}')$, in which irreducible functions occur, as well as functions of another type which will be completely characterized later, in Section 4.

In order to simplify the exposition which follows, it will be useful to introduce the following terminology.

Definition 3.1. Let A be a commutative integral domain. We shall say that an element of A is infinitely decomposable, if it is not a unit and no irreducible element of A divides it.

The obvious justification of this terminology is that if $f \in A$ is infinitely decomposable, there exist, for every $n \in \mathbb{N}$, noninvertible elements $f_1, \dots, f_n$ of A such that $f = f_1 \dots f_n$.

Definition 3.2. Let A be a commutative integral domain. We shall say that A is semifactorial if every nonzero element f of A can be expressed as a product $\alpha\beta$, where α is either a unit or a product of irreducible elements of A, uniquely determined by f up to multiplication by units, and β is either 1 or an infinitely decomposable element of A.

It is evident that a semifactorial ring is factorial if and only if it contains no infinitely decomposable element.

Before stating the first factorization theorem, we prove an auxiliary result.

LEMMA 3.3. *Let f be a function in $A(\mathcal{V}')$ which is irreducible in some A_n and let $m \in \mathbb{N}$ be a multiple of n. Then, the irreducible divisors of f in A_m are all irreducible in $A(\mathcal{V}')$ or all factorizable in $A(\mathcal{V}')$.*

Proof. It will suffice to prove that if $P(t_1, \dots, t_r)$ is an irreducible polynomial in r independent variables with coefficients in $\mathcal{M}(\mathcal{V})$ and if $P(t_1^p, \dots, t_r^p)$ is not irreducible for some $p \in \mathbb{N}$, then between every two irreducible divisors $A(t_1, \dots, t_r)$, $B(t_1, \dots, t_r)$ of $P(t_1^p, \dots, t_r^p)$ there is a relation of the type $B(t_1, \dots, t_r) = hA(\epsilon_1 t_1, \dots, \epsilon_r t_r)$ for some $h \in \mathcal{M}(\mathcal{V})$ and some p-th roots of unity $\epsilon_1, \dots, \epsilon_r$. But, this is an easy consequence of the fact that if $\epsilon_1', \dots, \epsilon_r'$ are any p-th roots of unity, $A(\epsilon_1' t_1, \dots, \epsilon_r' t_r)$ is also a divisor of $P(t_1^p, \dots, t_r^p)$ and that the product of all the essentially different (in the same sense of the remark in Section 2) polynomials of the form $A(\epsilon_1' t_1, \dots, \epsilon_r' t_r)$ is also a polynomial in $t_1^p, \dots, t_r^p$.

The author discovered the following theorem while investigating the discrete valuations of $K(\mathcal{V}')$ (see Corollary 3.6).

THEOREM 3.4. *$A(\mathcal{V}')$ is a semifactorial ring.*

Proof. Let f be any non-identically-zero function in $A(\mathcal{V}')$ and let $n \in \mathbb{N}$ be such that $f \in A_n$. Let $f = f_1 \dots f_r$ be a decomposition of f as a product of irreducible elements of A_n. Then, it is clear that for any function f_i $(i = 1, \dots, r)$ one of the following two possibilities holds:

1. There exists a multiple $m_0 \in \mathbb{N}$ of n such that for every multiple $m \in \mathbb{N}$ of m_0, no irreducible divisor of f_i in A_{m_0} factorizes nontrivially in A_m.

2. For every multiple $n' \in \mathbb{N}$ of n, there exists a multiple $n'' \in \mathbb{N}$ of n', such that some irreducible divisor of f_i in $A_{n'}$ factorizes in $A_{n''}$.

Now, it is a consequence of Theorem 2.5 that if f_i verifies the first possibility, it is a product of irreducible elements of $A(\mathcal{V}')$, and it is a consequence of the same theorem and of Lemma 3.3 that if f_i verifies the second possibility, it is infinitely decomposable. Since the irreducible divisors of f in $A(\mathcal{V}')$ are also irreducible divisors of f in some ring A_m, we deduce from Definition 3.1 and from the above reasoning that these divisors are uniquely determined by f save for multiplication by invertible functions, whereupon the theorem is proved.

As we have remarked in the introduction to this paper, Weierstrass theorem clearly implies that $O(\mathcal{V}')$ is not semifactorial. However, it is easy now to prove the following:

COROLLARY 3.5. *$O(\mathcal{V}')\cap A(\mathcal{V}')$ is semifactorial.*

Proof. It is a consequence of Theorems 2.6 and 3.4.

It is well known (see, for instance, Kra [5]) that every discrete valuation of $\mathcal{M}(\mathcal{V}')$ is equivalent to a valuation of the type v_p, with $v_p(f) = \text{ord}_p(f)$ for some $p \in \mathcal{V}'$ and every $f \in \mathcal{M}(\mathcal{V}')$ (standard notation), whereas it was proved in Cutillas [3] that there exist discrete valuations of $K(\mathcal{V}')$ which are not of the analogous type. This last assertion is also an evident consequence of the following:

COROLLARY 3.6. *For every irreducible $f \in A(\mathcal{V}')$ there exists a unique "f-adic" valuation of $K(\mathcal{V}')$; that is, a unique discrete valuation v_f of $K(\mathcal{V}')$ which assigns to every non-identically-zero $g \in A(\mathcal{V}')$ the multiplicity of f in any factorization of g as in Definition 3.2 (and so, it assigns in particular the value zero to every function with finite divisor).*

4. The infinitely decomposable elements of $A(\mathcal{V}')$. Throughout this section, we shall again consider the set of functions $\{f_i\}_{i\in I}$ introduced in Section 2 and use the allied notation also explained there. In particular, we shall fix, for every $i \in I$ and $n \in \mathbb{N}$, functions $f_{i,n} \in G(\mathcal{V}')$ and $h_{i,n} \in \mathcal{M}(\mathcal{V})$ such that $f_i = f_{i,n}^n h_{i,n}$. We shall also put $h_{i,n,m} = f_{i,n} f_{i,nm}^{-m} \in \mathcal{M}(\mathcal{V})$ so that $h_{i,n,m}$ corresponds to the function $f_{i,n}$ and to the number $m \in \mathbb{N}$ in the same way that $h_{i,m}$ to f_i and m. Note that $h_{i,n,m}$ is a n-th root of $h_{i,nm}h_{i,n}^{-1}$ for every $i \in I$, n, $m \in \mathbb{N}$.

From now on, unless otherwise stated, *all polynomials considered will have their coefficients in $\mathcal{M}(\mathcal{V})$; and we shall say that a polynomial is "nontrivial" if it does not reduce to its independent term and is not a monomial. $t_1, \ldots, t_r$ will be r independent variables over $\mathcal{M}(\mathcal{V})$; and we shall sometimes use the brief notation $P(t)$ or $P(t', t_r)$ for a polynomial $P(t_1, \ldots, t_r)$, where of course t' denotes the $r-1$ variables $t_1, \ldots, t_{r-1}$. Given a polynomial $P(t_1, \ldots, t_r)$ and*

$m \in \mathbb{N}$, $P(t_1^m, \ldots, t_r^m)$ will be represented in an abridged form by $P^m(t)$; and, if $\alpha = (i_1, \ldots, i_r) \in I^r$, $n \in \mathbb{N}$, $P(h_{i_1,m}t_1^m, \ldots, h_{i_r,m}t_r^m)$ will be represented as $P^{\alpha,m}(t)$, and $P(h_{i_1,m,n}t_1^n, \ldots, h_{i_r,m,n}t_r^n)$ as $P^{\alpha,m,n}(t)$. Finally, ϵ_n will be a primitive n-th root of unity for every $n \in \mathbb{N}$.

One of the fundamental ideas in what follows is to show that if the number of irreducible factors of $P(t_1^n, \ldots, t_r^n)$ increases with $n \in \mathbb{N}$, in a certain sense, for some nontrivial polynomial $P(t)$, then it must be essentially a binomial with coefficients in $\mathbb{C}$. Indeed, we shall prove a certain sort of generalization of this, by considering the powers $t_1^n, \ldots, t_r^n$ multiplied by the terms of sequences of the type of the $(h_{i,n})$ mentioned above.

LEMMA 4.1. *If $P(x)$ is an irreducible polynomial in one variable such that $P(x^n)$ factorizes for some $n > 1$, then there exists a divisor $d > 1$ of n such that $P(x^n) = h\prod_{j=1}^{d} Q(\epsilon_n^j x)$, where $h \in \mathcal{M}(\mathcal{V})$ and $Q(x)$ is an irreducible polynomial (which is also a polynomial in $(x^{x/d})$. Consequently, if β is a root of $P(x)$, the field $\mathcal{M}(\mathcal{V})(\beta)$ contains a d-th root of β.*

Proof. Consider a decomposition of $P(x)$ as a product of irreducible polynomials.

LEMMA 4.2. *If $n_1, \ldots, n_r \in \mathbb{N}$, $r \geqq 2$, and $\lambda \in \mathbb{C}^*$, then the polynomial $t_1^{n_1} \ldots t_r^{n_r} - \lambda$ is irreducible over $\mathcal{M}(\mathcal{V})$ if and only if $n_1, \ldots, n_r$ are relatively prime.*

Proof. If $A(t)$ is an irreducible divisor of $t_1^{n_1} \ldots t_r^{n_r} - \lambda$, then this last polynomial must coincide, up to multiplication by some element of $\mathcal{M}^*(\mathcal{V})$, with the product of all different polynomials of the type $A(\epsilon_{n_1}^{j_1} t_1, \ldots, \epsilon_{n_r}^{j_r} t_r)$, with $j_1, \ldots, j_r \in \mathbb{N}$. Therefore, the number of factors in this product is a common divisor of $n_1, \ldots, n_r$.

LEMMA 4.3. *Let $P(t_1, \ldots, t_r)$ be an irreducible polynomial, and $\alpha = (i_1, \ldots, i_r) \in I^r$. Then, the following conditions on $P(t)$ are equivalent:*

1) $P(f_{i_1}, \ldots, f_{i_r})$ is infinitely decomposable in $A(\mathcal{V}')$.

2) For every $n \in \mathbb{N}$ and every irreducible divisor $Q(t)$ of $P^{\alpha,n}(t)$, there exists $l \in \mathbb{N}$ such that $Q^{\alpha,n,l}(t)$ is not irreducible.

3) For every $n \in \mathbb{N}$ there exists a multiple $m \in \mathbb{N}$ of n such that the number of irreducible factors of $P^{\alpha,m}(t)$ is larger than that of $P^{\alpha,n}(t)$.

Proof. It is a consequence of the algebraic independence of $f_{i_1}, \ldots, f_{i_r}$ over $\mathcal{M}(\mathcal{V})$, and of Theorem 2.5, that 1) and 2) are equivalent. To prove that 2) $\Rightarrow$ 3), note that if $m \in \mathbb{N}$ is a multiple of n, $Q(t)$ is an irreducible divisor of $P^{\alpha,n}(t)$, and $l = mn^{-1}$, then the equality $P^{\alpha,m}(t) = P^{\alpha,n}(h_{i_1,n,l}t_1^l, \ldots, h_{i_r,n,l}t_r^l)$ implies that every divisor of $Q^{\alpha,n,l}(t)$ is also a divisor of $P^{\alpha,m}(t)$. Finally, 3) $\Rightarrow$ 2) is a consequence of the fact that between every two irreducible divisors $Q_1(t)$,

$Q_2(t)$ of $P^{\alpha,n}(t)$ there must be a relation of the type $Q_2(t) = hQ_1(\epsilon_n^{p_1}t_1, \ldots, \epsilon_n^{p_r}t_r)$ for some $h \in \mathcal{M}(\mathcal{V})$ and $p_1, \ldots, p_r \in \mathbb{N}$.

The following definitions will be convenient for stating and proving some other auxiliary results.

Definition 4.4. Given a polynomial $P(t_1, \ldots, t_r)$, and $m \in \mathbb{N}$, a factorization of $P^m(t)$ will be called simple if it is of the form $g \prod_{j=1}^{m} A(t', \epsilon_m^j t_r)$, for some $g \in \mathcal{M}^*(\mathcal{V})$ and some irreducible polynomial $A(t)$.

Note that if $P^m(t)$ has a simple factorization (with $P(t)$ and m as in Definition 4.4), $P(t)$ is irreducible.

Definition 4.5. We shall say that a polynomial $P(t_1, \ldots, t_r)$ is projectively irreducible with respect to $t_1, \ldots, t_{r-1}$ if $P(t_1^n, \ldots, t_{r-1}^n, t_r)$ is irreducible for every $n \in \mathbb{N}$.

We now summarize some useful (for this paper) properties of polynomials.

LEMMA 4.6. *Let $P(t_1, \ldots, t_r)$ be a polynomial with degree $\geqq 1$ with respect to t_r. Then*

1) If $P(t)$ is irreducible, there exists $q \in \mathbb{N}$ such that every irreducible divisor of $P(t_1^q, \ldots, t_{r-1}^q, t_r)$ is projectively irreducible with respect to $t_1, \ldots, t_{r-1}$.

2) If $P(t)$ is projectively irreducible with respect to $t_1, \ldots, t_{r-1}$ and $m \in \mathbb{N}$ is minimal such that $P^m(t)$ factorizes, this factorization is simple.

3) If $P(t)$ is as in 2) and $P^m(t)$ has a simple factorization for some $m \in \mathbb{N}$, every irreducible divisor of $P^m(t)$ is projectively irreducible with respect to $t_1, \ldots, t_{r-1}$.

4) If for some $m, n \in \mathbb{N}$ and some irreducible divisor $Q(t)$ of $P^m(t)$, the factorizations of $P^m(t)$ and $Q^n(t)$ are simple, the same is true for $P^{mn}(t)$.

Proof. 1) If the conclusion were false, the number of irreducible factors of $P(t_1^q, \ldots, t_{r-1}^q, t_r)$ should be larger than the degree of $P(t)$ with respect to t_r for an adequate election of $q \in \mathbb{N}$, which is impossible.

2) Let $A(t)$ be an irreducible factor of $P^m(t)$, and $l \in \mathbb{N}$ be minimal verifying that $A(t) = A(t', \epsilon_m^l t_r)$. Then, it follows from the hypothesis that $P^m(t) = h \prod_{j=1}^{l} A(t', \epsilon_m^j t_r)$ for some $h \in \mathcal{M}(\mathcal{V})$. Since this implies that $A(t)$ remains invariant if we replace in it $\epsilon_m^l t_s$ by t_s for $s = 1, \ldots, r$ (and so, $A(t)$ is a polynomial in $t_1^{m/l}, \ldots, t_r^{m/l}$), one easily deduces that $m = l$.

3) Consider an arbitrary $n \in \mathbb{N}$ and a simple factorization $h \prod_{j=1}^{m} B(t', \epsilon_m^j t_r)$ of $P^m(t)$. Then, $P^m(t_1^n, \ldots, t_{r-1}^n, t_r) = h \prod_{j=1}^{m} B(t_1^n, \ldots, t_{r-1}^n, \epsilon_m^j t_r)$; and since $P(t_1^{nm}, \ldots, t_{r-1}^{nm}, t_r)$ is irreducible, one deduces that so is $B(t_1^n, \ldots, t_{r-1}^n, t_r)$.

4) Easy.

Let $P(t_1, \ldots, t_r)$ be a nontrivial polynomial, and let $f_1, \ldots, f_r \in E(\mathcal{V}')$ be independent over $\mathbb{C}^*$ (i.e. such that no product $f_1^{n_1} \ldots f_r^{n_r}$ belongs to $\mathbb{C}^*$, with

https://doi.org/10.4153/CJM-1990-055-7 Published online by Cambridge University Press

$n_1, \dots, n_r \in \mathbb{Z}$ not all zero). Then, since the set $\{f_i\}_{i \in I}$ could have been supposed to contain these functions, one deduces from Lemma 4.3 that $P(f_1, \dots, f_r)$ is infinitely decomposable in $A(\mathcal{V}')$ if and only if $P(t)$ fulfils the condition (independent of the considered set $\{f_1, \dots, f_r\}$), which appears in the following:

Definition 4.7. A polynomial $P(t_1, \dots, t_r)$ will be said to be p.i.d. (abbreviation of "projectively infinitely decomposable") if for every $n \in \mathbb{N}$ and every irreducible divisor $Q(t)$ of $P^n(t)$ there exists $m \in \mathbb{N}$ such that $Q^m(t)$ factorizes.

Note that if $P(t_1, \dots, t_r)$ is p.i.d., then so is $P(t_1^{m_1}, \dots, t_r^{m_r})$ for every $m_1, \dots, m_r \in \mathbb{N}$.

LEMMA 4.8. *Let $P(t_1, \dots, t_r)$ be a p.i.d. polynomial with degree $\geqq 1$ with respect to t_r and projectively irreducible with respect to $t_1, \dots, t_{r-1}$. Then, there are arbitrarily large numbers $n \in \mathbb{N}$ such that $P^n(t)$ has a simple factorization.*

Proof. It is a consequence of parts (2), (3) and (4) of Lemma 4.6.

Our next lemma shows, in particular, that the p.i.d. polynomials are of a very special type as was remarked in the observation prior to the lemmas.

LEMMA 4.9. *A nontrivial irreducible polynomial $P(t_1, \dots, t_r)$ is p.i.d. if and only if it is of the form $h(t_{\sigma(1)}^{n_1} \dots t_{\sigma(s)}^{n_s} - \lambda t_{\sigma(s+1)}^{n_{s+1}} \dots t_{\sigma(r)}^{n_r})$, where $h \in \mathcal{M}^*(\mathcal{V})$, $\lambda \in \mathbb{C}^*$, σ is a permutation of the set $\{1, \dots, r\}$, and $n_1, \dots, n_r$ are relatively prime. Consequently, every p.i.d. polynomial has, after multiplying it if necessary by some element of $\mathcal{M}^*(\mathcal{V})$, its coefficients in $\mathbb{C}$.*

Proof. The latter assertion is a clear consequence of the former. In this, the sufficiency part is easy, and we shall prove the necessity one by induction on r.

For $r = 1$, if β is any root of the polynomial $P(t_1)$, Lemma 4.1 implies that the field $\mathcal{M}(\mathcal{V})(\beta)$ must contain infinitely many roots of β of different orders, which is impossible unless $\beta \in \mathbb{C}$ (take into account, for instance, that $\mathcal{M}(\mathcal{V})(\beta)$ is isomorphic to the field of meromorphic functions on some compact Riemann surface), whereupon one obtains the desired conclusion.

Assume now that the condition of the statement is necessary for polynomials in $r-1$ variables, and suppose that $P(t)$ is independent of none of the variables $t_1, \dots, t_r$. By replacing, if necessary, $P(t)$ by an irreducible divisor of $P(t_1^q, \dots, t_{r-1}^q, t_r)$, with q as in Lemma 4.6, we can also suppose that $P(t)$ is projectively irreducible with respect to $t_1, \dots, t_{r-1}$. Let now l_i be the degree of $P(t)$ with respect to t_i, for $i = 1, \dots, r$. Then, by Lemma 4.8 there exists $n > l_1 l_r + \max\{l_1, \dots, l_r\}$ such that $P(t_1^n, \dots, t_r^n) = h \prod_{j=0}^{n-1} R(t', \epsilon_n^j t_r)$ for some $h \in \mathcal{M}^*(\mathcal{V})$ and some irreducible polynomial $R(t)$, whence one deduces that $R(t_1, \dots, t_{i-1}, \epsilon_n t_i, t_{i+1}, \dots, t_r) = \epsilon_n^{p_i} R(t', \epsilon^{q_i} t_r)$ for some p_i, $q_i \in \{0, 1, \dots, n-1\}$ and so, if we call $a_{s_1, \dots, s_r}$ the coefficient of $t_1^{s_1} \dots t_r^{s_r}$ in $R(t)$, then $a_{s_1, \dots, s_r} \neq 0$ implies that $s_i - p_i - q_i s_r$ must be a multiple of n for every $i = 1, \ldots, r-1$. Hence, as is not difficult to see, $R(t)$ must be of the form $\sum_{j=0}^{k} \sum_{s=0}^{m_j} b_{js} t_1^{p_1 - jn} \ldots t_{r-1}^{p_{r-1}-jn} (t_1^{q_1} \ldots t_{r-1}^{q_{r-1}} t_r)^s$ for some nonnegative integers $k, m_0, \ldots, m_k$ and some $b_{js} \in \mathcal{M}(\mathcal{V})$; but then the assumption on n and the fact that l_i is also the degree of $R(t)$ with respect to t_i, imply that $R(t) = M_0(t') + M_1(t')t_r + \cdots + M_{l_r}(t')t_r^{l_r}$ where $M_j(t')$ is a monomial for every $j = 0, \ldots, l_r$. Let us now write l instead of l_r and let d_j be the exponent of t_1 in $M_j(t')$. Then, one obtains easily from $R(\epsilon_n t_1, t_2, \ldots, t_r) = \epsilon_n^{p_1} R(t', \epsilon_n^{q_1} t_r)$ that $p_1 = d_0$ and that $d_j - d_0 = q_1 j - k_j n$ for some $k_j \in \mathbb{Z}$, and $j = 1, \ldots, l$; from which we deduce that $q_1 = \dfrac{d_l - d_0 + k_l n}{l}$, and substituting, that $d_j - d_0 = \dfrac{d_l - d_0 + k_l n}{l} j - k_j n$ for every $j = 1, \ldots, l$. Finally, from the hypothesis on n, it follows that $d_j - d_0 = \dfrac{d_l - d_0}{l} j$; and so, that $\dfrac{d_j - d_0}{j} = \dfrac{d_l - d_0}{l} = \dfrac{a}{b}$ for every $j = 1, \ldots, l$ and some relatively prime $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Thus there exists a polynomial in $r-1$ variables $A(x_1, \ldots, x_{r-1})$ such that $R(t) = t_1^{d_0} A(t_2, \ldots, t_{r-1}, t_1^a t_r^b)$, and we can apply the induction hypothesis in order to conclude (see the observation prior to Definition 4.7).

THEOREM 4.10. *Let $P(t_1, \ldots, t_r)$ be an irreducible polynomial independent of none of the variables $t_1, \ldots, t_r$. If for some $\alpha = (i_1, \ldots, i_r) \in I^r$, $P(f_{i_1}, \ldots, f_{i_r})$ is infinitely decomposable in $A(\mathcal{V}')$, then $f_{i_1}, \ldots, f_{i_r} \in E(\mathcal{V}')$ and $P(t)$ is p.i.d.*

Proof. By induction on r. For $r = 1$, one proves as in Lemma 4.9 that $P(t_1) = h(t_1 - \beta)$ for some $h \in \mathcal{M}^*(\mathcal{V})$ and $\beta \in \mathbb{C}$; and this together with the infinite decomposability of $P(f_{i_1})$ implies that $f_{i_1} \in E(\mathcal{V}')$.

Suppose now that the theorem is proved for polynomials in $r-1$ variables, and let $P(t) = P_0(t') + \cdots + P_l(t')t_r^l$ be the expression of $P(t)$ as a polynomial in t_r with coefficients in $\mathcal{M}(\mathcal{V})[t']$. By Lemma 4.3 there are infinitely many numbers $n \in \mathbb{N}$ such that $P^{\alpha,n}(t)$ has a factorization of the type $h_n \prod Q_n(\epsilon_n^{j_1} t_1, \ldots, \epsilon_n^{j_r} t_r)$, with $h_n \in \mathcal{M}^*(\mathcal{V})$, $Q_n(t)$ irreducible, $(j_1, \ldots, j_r)$ varying in a certain finite subset of $\mathbb{N}^r$ (of course, the product having one factor for each element of this set), and with a number p_n of factors which increases with n. Let $Q_n(t) = Q_{n,0}(t') + \cdots + Q_{n,k_n}(t')t_r^{k_n}$ be the expression of $Q(t)$ analogous to that of above for $P(t)$. Then, one deduces:

1) $P_0(h_{i_1,n} t_1^n, \ldots, h_{i_{r-1},n} t_{r-1}^n) = h_n \prod Q_{n,0}(\epsilon_n^{j_1} t_1, \ldots, \epsilon_n^{j_{r-1}} t_{r-1})$.
2) $h_{i_r,n}^l P_l(h_{i_1,n} t_1^n, \ldots, h_{i_{r-1},n} t_{r-1}^n) = h_n \epsilon_n^{s_n} \prod Q_{n,k_n}(\epsilon_n^{j_1} t_1, \ldots, \epsilon_n^{j_{r-1}} t_{r-1})$

where $s_n \in \mathbb{N}$ and the number of factors is the same as above. Hence, as is not difficult to see (for instance, by Theorem 3.4) $P_0(f_{i_1}, \ldots, f_{i_{r-1}})$ and $P_l(f_{i_1}, \ldots, f_{i_{r-1}})$ must be infinitely decomposable in $A(\mathcal{V}')$ and so, by the induction hypothesis, those functions in the set $\{f_{i_1}, \ldots, f_{i_{r-1}}\}$ with degree $\geqq 1$ in them, belong to $E(\mathcal{V}')$, and $P_0(t')$, $P_l(t')$ are p.i.d. (as well as $Q_{n,0}(t')$ and

https://doi.org/10.4153/CJM-1990-055-7 Published online by Cambridge University Press

$Q_{n,k_n}(t')$ for every n as above). Therefore, Lemma 4.9 implies that there exist $g_1, g_2 \in \mathcal{M}^*(\mathcal{V})$ such that $g_1P_0(t')$ and $g_2P_l(t')$ have their coefficients in $\mathbb{C}$ (and that the similar assertion is true for $Q_{n,0}(t')$ and $Q_{n,k_n}(t')$). But then, equality (1) shows that h_ng_1 has a p_n-th root in $\mathcal{M}(\mathcal{V})$, and it results from (2) that the same is true for $h^l_{i_r,n}g_1^{-1}g_2^{-1}$. Thus, $f^l_{i_r}g_1^{-1}g_2^{-1}$ has a p_n-th root in $G(\mathcal{V}')$; and being this true for every n of the said type, one concludes that $f_{i_r} \in E(\mathcal{V}')$. Finally, it is clear that the same reasoning is valid for $f_{i_1}, \ldots, f_{i_{r-1}}$ and so, that $P(t)$ must be p.i.d.

The foregoing results already allows us to state and prove easily the following characterization of infinitely decomposable functions.

THEOREM 4.11. *A function $f \in A(\mathcal{V}')$ is infinitely decomposable if and only if there exist $g \in G(\mathcal{V}')$ and $\varphi_1, \ldots, \varphi_n \in O(\mathcal{V}') - \mathbb{C}$ such that $f = g(e^{\varphi_1} - 1)\ldots(e^{\varphi_n} - 1)$.*

Proof. First, we show that $e^{\varphi} - 1$ is infinitely decomposable for every $\varphi \in O(\mathcal{V}') - \mathbb{C}$. With the notation of Section 2, there exist $i_1, \ldots, i_k \in I''$ such that $e^{\varphi} = f^{m_1}_{i_1,l}\ldots f^{m_k}_{i_k,l}$ for some $l \in \mathbb{N}$, and some $m_1, \ldots, m_k$ which, replacing if necessary some of the functions $f_{i_1}, \ldots, f_{i_k}$ by their inverses, can be supposed to belong to $\mathbb{N}$; and, since $q \in \mathbb{N}$ divides $m_1, \ldots, m_k$ if and only if $e^{\varphi/q} \in A_l$, one deduces from Lemma 4.2 that a decomposition of $e^{\varphi} - 1$ as a product of irreducible elements of A_l is $e^{\varphi} - 1 = (e^{\varphi/p} - 1)(e^{\varphi/p} - \epsilon_p)\ldots(e^{\varphi/p} - \epsilon_p^{p-1})$ where p is the greatest common divisor of $m_1, \ldots, m_k$. Hence, as this is valid for every $l \in \mathbb{N}$ such that $e^{\varphi} \in A_l$, we obtain the desired conclusion.

Consider now an infinitely decomposable function $f \in A(\mathcal{V}')$. For the sake of simplicity we can also suppose without loss of generality that $f \in A_1$. Hence, there exist $g_0 \in G(\mathcal{V}')$, $i_1, \ldots, i_r \in I$, and a polynomial $A(t_1, \ldots, t_r)$ such that $f = g_0A(f_{i_1}, \ldots, f_{i_r})$; and applying to each irreducible factor of $A(t)$, Lemma 4.9 and Theorem 4.10, one easily deduces that f must be as in the statement.

As an immediate consequence of Theorems 3.4 and 4.11 we obtain now the final form of the factorization theorem for functions in $A(\mathcal{V}')$.

THEOREM 4.12. *Every non-identically-zero $f \in A(\mathcal{V}')$ can be decomposed as a product f_1f_2, where f_1 is either a function in $G(\mathcal{V}')$ or a product of irreducible functions uniquely determined by f up to multiplication by functions in $G(\mathcal{V}')$, and f_2 is either 1 or a product of the type $(e^{\varphi_1} - 1)\ldots(e^{\varphi_n} - 1)$, with $\varphi_1, \ldots, \varphi_n \in O(\mathcal{V}') - \mathbb{C}$.*

The terminology introduced in the following definition will be useful in order to extend this theorem to a special class of subrings of $\mathcal{M}(\mathcal{V}')$.

Definition 4.13. We shall say that a subring A of $\mathcal{M}(\mathcal{V}')$ is regular if it contains $\mathcal{M}(\mathcal{V})$, is generated over this field by functions with finite divisor, and if the quotient group $G(\mathcal{V}') \cap A/\mathcal{M}^*(\mathcal{V})$ is divisible.

It is obvious that every regular subring of $\mathcal{M}(\mathcal{V}')$ is contained in $A(\mathcal{V}')$. A first nontrivial example of regular subring of $\mathcal{M}(\mathcal{V}')$ is $A(\mathcal{V}')$ itself; and, other remarkable examples are, $A(k)$ for every minimal $\mathcal{W}$-field k in $\mathcal{V}'$ (by Theorem 2.2), and the ring $B(\mathcal{V}')$ generated over $\mathcal{M}(\mathcal{V})$ by the so-called Baker-Akhiezer functions in $\mathcal{V}'$, of frequent appearance in modern mathematical literature, principally in relation with the theory of certain partial differential equations (see Dubrovin [4]). This last ring coincides with the ring of sums of functions in $\mathcal{M}(\mathcal{V}')$ with exponential singularities of finite degree at the points of $\mathcal{V} - \mathcal{V}'$ in the sense of Cutillas [2].

Regular subrings of $\mathcal{M}(\mathcal{V}')$ have many similar properties to those of $A(\mathcal{V}')$. For instance, Theorem 4.12 can be generalized for them.

THEOREM 4.14. *Every regular subring A of $\mathcal{M}(\mathcal{V}')$ is semifactorial. The infinitely decomposable elements of A are the products of the type $g(f_1-1)\dots(f_n-1)$, where $g \in G(\mathcal{V}')\cap A$ and $f_1,\dots,f_n$ are nonconstant functions in $E(\mathcal{V}')\cap A$.*

Proof. Consider functions in $G(\mathcal{V}')\cap A$ whose classes in $G(\mathcal{V}')\cap A/M^*(\mathcal{V})$ form a suitable basis of this quotient group, considered as a Q-vector space, and repeat the arguments used in the proof of the analogous theorem for $A(\mathcal{V}')$ (or extend the considered basis to a suitable basis of $G(\mathcal{V}')/M^*(\mathcal{V})$ and use what we have already proved).

The first assertion of the following corollary is a consequence of Theorem 2.2 and Theorem 4.14.

COROLLARY 4.15. *1) For every minimal W-field k in $\mathcal{V}'$, the ring $A(k)$ is factorial. In particular, if ∞ is a non-Weierstrass point of $\mathcal{V}$, the ring of sums of functions in $\mathcal{M}(\mathcal{V} - \{\infty\})$ with exponential singularity at ∞ of degree less than or equal to the genus of $\mathcal{V}$, is factorial.*

2) The ring $B(\mathcal{V}')$ (above defined) is semifactorial, and its infinitely decomposable elements are the products of the type $g(f_1 - 1)\dots(f_n - 1)$, where $g \in G(\mathcal{V}')\cap B(\mathcal{V}')$ and $f_1,\dots,f_n$ are exponentials of nonconstant functions in $\mathcal{M}(\mathcal{V})\cap O(\mathcal{V}')$.

REFERENCES

1. N. Bourbaki, *Commutative algebra*, Hermann, Paris, 1965.
2. P. Cutillas Ripoll, *Construction of certain function fields associated with a compact Riemann surface*, Amer. J. of Math. *106*, (1984), 1423–1450.
3. ——— *On the isomorphisms between certain function fields over compact Riemann surfaces*, Math. Ann. *275* (1986), 81–85.
4. B. A. Dubrovin, *Theta functions and nonlinear equations*, Russian Math. Surveys, *36* (1981) 11–92.
5. H. R. Farkas and I. Kra, *Riemann Surfaces*, Springer. 1980.
6. I. Kra, *Automorphic functions and kleinian groups*, New York, Benjamin, 1972.

Dpto. de Matemáticas,
Universidad de Salamanca,
Spain