Complex Variables, 1989, Vol. 13, pp. 1–20
Reprints available directly from the publisher
Photocopying permitted by license only

Printed in the United States of America

Algebraic Properties of the Ring of General Exponential Polynomials

C. WARD HENSON and LEE A. RUBEL

Department of Mathematics, University of Illinois, 1409 West Green St., Urbana, IL 61801

and

MICHAEL F. SINGER

Department of Mathematics, North Carolina State University, P.O. Box 8205, Raleigh, NC 27695

AMS No. 30D99, 32A99
Communicated: K. F. Barth and R. P. Gilbert
(*Received September 15, 1987*)

INTRODUCTION

The motivation for the results given in this paper is our desire to study the entire functions of several variables which are defined by exponential terms. By an exponential term (in n variables) we mean a formal expression which can be built up from complex constants and the variables $z_1, \ldots, z_n$ using the symbols $+$ (for addition), $\cdot$ (for multiplication) and $\exp(\cdot)$ (for the exponential function with the constant base e). (These are the terms and the functions considered in Section 5 of [11]. There the set of exponential terms was denoted by Σ. Note that arbitrary combinations and iterations of the permitted functions can be formed; thus such expressions as

$$z_1 \cdot z_2 \cdot \exp(\exp(z_1 + z_2^2) + z_1^3) + \exp(2 \cdot z_1)$$

are included here.) Each exponential term in n variables evidently defines an analytic function on $\mathbb{C}^n$; we denote the ring of all such functions on $\mathbb{C}^n$ by A_n. This is in fact an *exponential ring*; that is, A_n is closed under application of the exponential function.

It is clear that each function in A_n can be written as a finite sum

$$\sum p_i \cdot \exp(g_i)$$

in which $p_1, \ldots, p_k$ are polynomials over $\mathbb{C}$ in the variables $z_1, \ldots, z_n$ and $g_1, \ldots, g_k$ are also in A_n. In [11, Section 5] Nevanlinna theory is used to show that this representation is unique, if we normalize by requiring that each of the functions g_i

This research was partially supported by grants from the National Science Foundation.

satisfies $g_i(0, \ldots, 0) = 0$. (This amounts to subtracting a constant from g_i and multiplying p_i by its exponential.) This argument, which is implicit in the proof of [11, Theorem 5.2], is given in Section 1 below.

From this normal form result for A_n it follows that A_n is isomorphic to a group ring in which the group is a vector space of dimension 2^ω over the field $\mathbb{Q}$ and the coefficient ring is the polynomial ring $\mathbb{C}[z_1, \ldots, z_n]$. We use this abstract representation of A_n and some purely algebraic arguments to prove several interesting facts about A_n. In particular we prove that it satisfies an interesting unique factorization theorem, and that it is a coherent ring. (See Sections 3 and 4.) We also use these ideas to give several examples which seem to have an analytic character, but which prove to be purely algebraic. (See Section 5.)

Our unique factorization theorem for A_n is of the same character as the unique factorization theorem proved by Ritt [15]–[17] for the ring S of all simple exponential sums

$$\sum \alpha_i \cdot e^{\beta_i z}$$

in which $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m$ are complex constants. This ring is evidently just a small subring of A_1. However, a simple version of our normal form result for this subring shows that it is isomorphic to a group ring in which the group is a 2^ω-dimensional vector space over $\mathbb{Q}$ (namely the vector space $(\mathbb{C}, +)$) and the coefficient ring is the field $\mathbb{C}$. From this point of view the only difference between A_n and the ring S is the "slightly" greater generality in the ring of coefficients. Our proof of the unique factorization theorem for A_n is closely patterned after Ritt's argument for S, and the key ideas are certainly to be found in [15]–[17]. We should also note that a similar unique factorization result is stated in [14] for the ring of exponential sums of the form

$$\sum p_i(z) \cdot e^{\alpha_i z}.$$

Nonetheless we wish to sketch this argument in some detail, especially because it seems surprising that the exponential rings A_n, in which the exponents can be extremely complicated, should satisfy a unique factorization result. (Certainly the analytic behavior of functions in A_n can be much more complicated than that of the sums studied by Ritt or by van der Poorten and Tijdeman.)

The normal form theorem proved in Section 1 is valid not only for the ring A_n but also for the apparently much larger ring, which we denote by B_n, of all entire functions of n variables $z_1, \ldots, z_n$ which can be written in the form

$$\sum p_i \cdot \exp(g_i)$$

in which each p_i is a polynomial and each g_i is an entire function. In fact, it follows immediately from the normal form theorem that A_n and B_n are isomorphic rings for each $n \geqslant 1$, that there is a retraction mapping from B_n onto A_n, that A_n is algebraically closed in B_n, etc.

In Section 5 we give several examples and raise some questions of an analytic character which seem interesting, and which indicate the kinds of problems about

exponential functions which motivated us to obtain the results which are presented here.

Throughout this paper we will make use of the group ring

$$R_V = \mathbb{C}[z_1, \ldots, z_n](V, +)$$

in which the coefficient ring is the ring $\mathbb{C}[z_1, \ldots, z_n]$ of polynomials over $\mathbb{C}$ in the variables $z_1, \ldots, z_n$, and the group $(V, +)$ is a divisible, torsion-free Abelian group. (That is, the group $(V, +)$ is simply a vector space over the field of rational numbers.) In this notation the number n is left as ambiguous and must be determined from the context. In this paper all vector space concepts, such as "linear independence" or "linear span" or "linear mapping" will be taken relative to the field $\mathbb{Q}$ of rational numbers.

It is convenient to write the elements of R_V as finite sums of the form

$$\sum p_i \cdot \exp(v_i)$$

in which each p_i is a non-zero polynomial in $\mathbb{C}[z_1, \ldots, z_n]$ and $v_1, \ldots, v_n$ are distinct elements of V. (We will refer to the vectors $v_1, \ldots, v_n$ as the *exponents* which occur in the given element of R_V.) This gives a unique representation of each element of R_V. The additive identity of R_V is thus represented as the empty sum and the multiplicative identity as $1 \cdot \exp(0)$. This point of view amounts to replacing the additive group $(V, +)$ by an isomorphic group which is written multiplicatively; the isomorphism takes each v to $\exp(v)$.

1. NORMAL FORMS

In Section 5 of [11] Nevanlinna theory was used to prove a normal form theorem for A_n (it is implicit in the proof of Theorem 5.2); essentially the same result was proved independently using algebraic techniques by van den Dries [7] and, for A_1, by A. Wilkie [unpublished]. Here we observe that essentially the same argument used in [11] yields a similar normal form result for the larger ring B_n.

THEOREM 1.1 *Each function in B_n can be written uniquely as a finite sum of the form:*

$$\sum_{i=1}^{m} p_i \cdot \exp(g_i)$$

where $p_1, \ldots, p_m$ are non-zero polynomials over $\mathbb{C}$ in the variables $z_1, \ldots, z_n$, $g_1, \ldots, g_m$ are distinct entire functions of $z_1, \ldots, z_n$, and we normalize by requiring that each $g_i(0, \ldots, 0) = 0$.

In addition, if the function being represented is in A_n, then the exponents $g_1, \ldots, g_n$ can be taken from A_n.

Proof The existence of such a representation is trivial, both for B_n and for A_n. To prove uniqueness, it suffices to show that if the constant function 0 is given by such a representation, then the sum is trivial. (That is, the sum has no terms.) (To treat the general case, take the difference between two representations of the same function and collect terms which have the same $\exp(g_i)$ part.)

Suppose we have such a representation of the 0 function in which m is as small as possible, but with $m > 0$. It is clear that we must in fact have $m > 1$. Dividing by $\exp(g_1)$, and denoting $g_i - g_1$ by h_i for each $i = 2, \ldots, m$, we have:

$$-p_1 = \sum_{i=2}^{m} p_i \cdot \exp(h_i).$$

Note that $h_2, \ldots, h_m$ are distinct and non-constant, and satisfy $h_i(0, \ldots, 0) = 0$ for each i. As argued on pages 28-29 of [11], we may apply the H–O Lemma [11, Lemma 2.1 and the surrounding discussion]. It follows that there exist complex constants $c_2, \ldots, c_n$ (not all zero) such that

$$\sum_{i=2}^{m} c_i \cdot p_i \cdot \exp(h_i) = 0.$$

This sum must have at least one non-trivial term, and thus yields a non-trivial representation of the 0 function in which there are fewer than m terms. This contradicts the minimality of m and completes the proof. ■

Let V be the vector space of all entire functions g of the variables $z_1, \ldots, z_n$ which satisfy $g(0, \ldots, 0) = 0$. Let W be the subspace of V defined by

$$W = V \cap A_n.$$

We can rephrase Theorem 1.1 by saying that B_n is canonically isomorphic to the group ring $R_V = \mathbb{C}[z_1, \ldots, z_n](V, +)$ and that the isomorphism carries the subring $R_W = \mathbb{C}[z_1, \ldots, z_n](W, +)$ onto A_n. Note that both $(V, +)$ and $(W, +)$ are 2^ω-dimensional vector spaces over $\mathbb{Q}$. This statement and the number n of variables completely determine the structure of A_n and B_n and plays the key role in what we prove in later sections. Note that this shows in particular that A_n and B_n are isomorphic rings.

A result equivalent to Theorem 1.1 for the ring A_n was proved by van den Dries [7] using purely algebraic techniques. (His normalization of exponents is different from ours, but the two results can easily be seen to be equivalent.) Macintyre has extended this approach to prove a normal form theorem for the field F_n of *exponential rational functions* in the variables $z_1, \ldots, z_n$. Each element of F_n can be regarded as an analytic function defined on a connected, dense open subset of $\mathbb{C}^n$; it is the smallest field of such functions which contains the polynomial functions and is closed under application of the exponential function e^x. (The difference between F_n and A_n is that in F_n the operation of division is permitted; thus F_n contains functions such as $\exp\left(\frac{1}{z_i}\right)$ and $\frac{\exp(z_i) - 1}{z_i}$ which are not in A_n). The normal form theorem for F_n which Macintyre proved has the consequence that F_n is isomorphic, as an algebra over $\mathbb{C}[z_1, \ldots, z_n]$, to the field of fractions of R_V, where V is a vector space over $\mathbb{Q}$ of dimension 2^ω. (The vector space V can be explicitly identified from the development in [13, Chapter 7] but we will not give the details here.) Thus the results proved here about the rings

R_V can be used to obtain results concerning the fine structure of the field F_n, and its relation to A_n.

2. BASIC FACTS

Let $(V, +)$ be a vector space over $\mathbb{Q}$ and let W be a subspace of V. Evidently R_W is a subring of R_V. There is a linear mapping T of V onto W which is the identity on W. Each such mapping T can be used to define a ring homomorphism P from R_V onto R_W which is the identity on R_W. (P is a *retraction* of R_V onto R_W.) Namely, define P by

$$P(\sum p_i \cdot \exp(v_i)) = \sum p_i \cdot \exp(T(v_i)).$$

The existence of such retractions can be quite useful. For example, any element of R_W which is a unit in R_V will already be a unit in R_W; more generally, if f and g are in R_W and f divides g in R_V, then f must already divide g in the smaller ring R_W.

As is well known, all vector spaces over $\mathbb{Q}$ can be given a linear ordering which is compatible with the vector space structure. If V is finite dimensional, with basis $v_1, \ldots, v_n$ then we may give V the lexicographic ordering, under which $\sum q_i \cdot v_i$ is positive if its first non-zero coefficient q_i is positive. Or we may embed V into $\mathbb{R}$ over $\mathbb{Q}$ and pull back the usual linear ordering of $\mathbb{R}$ to get a linear ordering of V. The Hahn Embedding Theorem [8] states that every linear ordering on V can be obtained by a mixture of these two methods.

Linear orderings of V are very useful in obtaining results about R_V. For example, we can give an easy proof that R_V is an integral domain. Consider $f = \sum p_i \cdot \exp(v_i)$ and $g = \sum q_j \cdot \exp(w_j)$ both non-zero. We may suppose that the exponents of f and the exponents of g are listed in increasing order, with respect to a given linear ordering on V. The exponents of $f \cdot g$ will be among the sums $v_i + w_j$. Moreover, the term $p_1 \cdot q_1 \cdot \exp(v_1 + w_1)$ must actually occur in the product, since no cancellation wth other terms can take place. Hence the produce $f \cdot g$ cannot be 0.

Let $P(z, Y) = P(z_1, \ldots, z_n, Y_1, \ldots, Y_m)$ be a polynomial over $\mathbb{C}$ in the indicated $n + m$ variables. (For notational convenience we often write $z_1, \ldots, z_n$ simply as z and $Y_1, \ldots, Y_m$ as Y.) Given any m vectors in V, say $w_1, \ldots, w_m$, we may regard the expression

$$P(z_1, \ldots, z_n, \exp(w_1), \ldots, \exp(w_n))$$

as an element f of R_V in an obvious way. If P is a simple monomial

$$Y_1^{k_1} \ldots Y_m^{k_m}$$

then f is just

$$\exp(k_1 \cdot w_1 + \cdots + k_m \cdot w_m).$$

In general, f will consist of a finite combination of such terms with appropriate coefficients coming from $\mathbb{C}[z_1, \ldots, z_n]$.

Conversely, suppose $w_1, \ldots, w_m$ are linearly independent and f is an element of R_V whose exponents can all be written as linear combinations of $w_1, \ldots, w_m$ in which the coefficients are all non-negative integers. Then the process of the previous

paragraph can be reversed, yielding a polynomial $P(z, Y)$ which represents f, in the sense that

$$f = P(z_1, \ldots, z_n, \exp(w_1), \ldots, \exp(w_m)).$$

Finally, note that this representation of (certain) elements of R_V by multivariable polynomials is unique (as long as the same basis is being used.) That is, suppose $P(z, Y)$ and $Q(z, Y)$ are polynomials over $\mathbb{C}$, that $w_1, \ldots, w_m$ are linearly independent elements of V, and that

$$P(z_1, \ldots, z_n, \exp(w_1), \ldots, \exp(w_m)) = Q(z_1, \ldots, z_n, \exp(w_1), \ldots, \exp(w_m)).$$

Then $P(z, Y)$ and $Q(z, Y)$ must be equal as polynomials, as can be seen by comparing monomials in the variables $Y_1, \ldots, Y_m$.

Definition 2.1 An element f of R_V is *normalized* if it can be written in the form

$$f = P(z_1, \ldots, z_n, \exp(w_1), \ldots, \exp(w_m))$$

where $w_1, \ldots, w_m$ are linearly independent elements of V and $P(z, Y)$ is a polynomial over $\mathbb{C}$ which includes at least one monomial that does not contain any of the variables $Y_1, \ldots, Y_m$. When f is given in this way, we will refer to P as giving a *representation of f with respect to $w_1, \ldots, w_m$*.

Note that when f is normalized, then it has one term of the form $p \cdot \exp(0)$, with p non-zero. Moreover, the other exponents of f are given by linear combinations of the basis $w_1, \ldots, w_m$, in which all of the coefficients are *non-negative integers*.

LEMMA 2.2 *Each non-zero element g of R_V can be written in the form $g = \exp(v) \cdot f$.* where f is normalized.

Proof Fix g and let W be the linear span of the exponents which occur in g. By using a linear embedding, we may regard W as a linear subspace of $\mathbb{R}$. (Recall that we regard all vector spaces as over $\mathbb{Q}$.) Let v be the least exponent occurring in g (in the usual ordering on $\mathbb{R}$) and write the exponents in increasing order as $v < v + v_1 < \cdots < v + v_k$. It follows that if we set $g = \exp(-v) \cdot f$, then g has as its exponents the numbers $0 < v_1 < \cdots < v_k$. Let $r_1, \ldots, r_m$ be a basis over $\mathbb{Q}$ for the linear span of $v_1, \ldots, v_k$. For each $i = 1, \ldots, k$ let us write

$$v_i = \sum_{j=1}^{m} q_{ij} \cdot r_j$$

with all of the coefficients q_{ij} being rational. Now choose $T = (t_{ij})$ to be a non-singular $m \times m$ matrix of rational numbers, in which each t_{ij} is chosen to be very close to r_i. Using the non-singularity of T, there exist $s_1, \ldots, s_m$ in $\mathbb{R}$ which are linearly

independent over $\mathbb{Q}$ and such that

$$r_i = \sum_{j=1}^{m} t_{ij} \cdot s_j$$

for each $i = 1, \ldots, m$. Hence for each $i = 1, \ldots, k$ we have

$$v_i = \sum_{j=1}^{m} p_{ij} \cdot s_j$$

where the coefficients are given by

$$p_{ij} = \sum_{l=1}^{m} q_{il} \cdot t_{lj}.$$

Since each t_{lj} is very close to r_l it follows that p_{ij} is close to v_i itself. In particular, if this approximation is done carefully, all of the coefficients p_{ij} will be positive rational numbers. Let N be the least common denominator of these coefficients, and define $w_i = \frac{1}{N} \cdot s_i$ for each $i = 1, \ldots, m$. Then $w_1, \ldots, w_m$ is also a basis for the linear span of the exponents $v_1, \ldots, v_k$ and each v_i is a linear combination of these basis elements in which each coefficient is a *positive integer*. The discussion above makes it clear that g must be a normalized element of R_V. ■

Note The proof of Lemma 2.2 shows that if we are given finitely many elements $g_1, \ldots, g_k$ of R_V, then there exist $v_1, \ldots, v_k \in V$ and normalized elements $f_1, \ldots, f_k$ of R_V such that $g_i = \exp(v_i) \cdot f_i$ for each $i = 1, \ldots, k$ AND this can be done in such a way that there is a single set $w_1, \ldots, w_m$ of linearly independent elements of R_V such that $f_1, \ldots, f_k$ are represented by polynomials $P_1(z, Y), \ldots, P_k(z, Y)$ respectively with respect to the *same* basis $w_1, \ldots, w_m$.

The next result shows the usefulness of normalized elements of R_V in reducing factorization problems to questions about polynomials over $\mathbb{C}$.

LEMMA 2.3 *Suppose f is a normalized element of R_V, represented by the polynomial $P(z_1, \ldots, z_n, Y_1, \ldots, Y_k)$ with respect to the basis $w_1, \ldots, w_k$. Let g and h be elements of R_V satisfying $f = g \cdot h$. Then there exists $v \in V$ such that the ring elements $G = \exp(v) \cdot g$ and $H = \exp(-v) \cdot h$ are both normalized (and of course $f = G \cdot H$). Indeed there exist positive integers $N_1, \ldots, N_k$ and polynomials $Q(z_1, \ldots, z_n, Y_1, \ldots, Y_k)$ and $R(z_1, \ldots, z_n, Y_1, \ldots, Y_k)$ so that G is represented by $Q(z, Y)$ and H is represented by $R(z, Y)$, with respect to the basis $\frac{1}{N_1} \cdot w_1, \ldots, \frac{1}{N_k} \cdot w_k$. In this case it necessarily follows that*

$$P(z_1, \ldots, z_n, Y_1^{N_1}, \ldots, Y_k^{N_k}) = Q(z, Y) \cdot R(z, Y)$$

as polynomials over $\mathbb{C}$.

Note In this situation the element f is obviously represented by the polynomial $P(z_1, \ldots, z_n, Y_1^{N_1}, \ldots, Y_k^{N_k})$ with respect to the basis $\frac{1}{N_1} \cdot w_1, \ldots, \frac{1}{N_k} \cdot w_k$: thus the polynomial equation in Lemma 2.3 is equivalent to the equation $f = G \cdot H$.

Proof Let W be the linear span over $\mathbb{Q}$ of $\{w_1, \ldots, w_k\}$ and let $<$ be any vector space linear ordering on W with respect to which $w_1, \ldots, w_k$ are all > 0. It follows that every exponent which occurs in f must be $\geqslant 0$, since it can be written as a linear combination of the basis elements with non-negative integer coefficients. (Note that because f is normalized, 0 must occur as an exponent in f.) Extend this linear ordering in any way to the linear span of all exponents which occur in f, g or h. Let v be the least exponent in this ordering among those which occur in g. We set $G = \exp(-v) \cdot g$ and $H = \exp(v) \cdot h$; evidently $f = G \cdot H$, and we will show that they satisfy the other requirements in the Lemma.

The exponents which occur in G are all $\geqslant 0$, and 0 is an exponent in G. Suppose the exponents which occur in H are $v_1 < \cdots < v_p$. The exponents occurring in the product $G \cdot H$ will be included among the vectors $v + v_i$, where $1 \leqslant i \leqslant p$ and v occurs in G. Hence they are all $\geqslant v_1$. Moreover, v_1 must actually occur as an exponent in $G \cdot H$, since $v + v_i = v_1$ can only occur when $v = 0$ and $i = 1$. From this it follows that v_1 must be 0, and hence the exponents which occur in H are all $\geqslant 0$, and include 0.

Next we show that the exponents occurring in G are in W; by a similar argument the same must be true of H. If not, let $w_1, \ldots, w_k$ be expanded to a basis $w_0, w_1, \ldots, w_k, \ldots$ for the linear span of W together with all exponents which occur in G or in H. Do this in such a way that at least one exponent occurring in G has a negative w_0-coefficient when it is written in terms of this basis. On the linear span of this basis let $<$ be the lexicographic order; it extends the given ordering on W. Under this ordering, the exponents of f *are all* $\geqslant 0$, while at least one exponent of G is < 0. But 0 occurs as an exponent in H, so that the least exponent in H must be $\leqslant 0$. It follows that the least exponent which occurs in the product $G \cdot H$ would have to be negative, contradicting the fact that $G \cdot H = f$.

Next we show that when the exponents occurring in G or in H are written as linear combinations of $w_1, \ldots, w_k$, then the coefficients will all be $\geqslant 0$. If not, then without loss of generality we may assume that some exponent in G has a negative w_1-coefficient. On W consider the lexicographic ordering given by the basis $w_1, \ldots, w_k$ (which might have been permuted). We get a contradiction as in the last paragraph: in this ordering, the exponents of f are still $\geqslant 0$, some exponent is G is < 0, and the least exponent of H is $\leqslant 0$. A similar argument treats the exponents which occur in H.

For each $i = 1, \ldots, k$ we now choose N_i to be a common denominator for all of the coefficients of the basis vector w_i, when the exponents of f, G or H are written as linear combinations of $w_1, \ldots, w_k$. These exponents can all be written in terms of the basis

$$\frac{1}{N_1} \cdot w_1, \ldots, \frac{1}{N_k} \cdot w_k$$

using only coefficients which are non-negative integers. One now obtains the polynomials Q and R from G and H and proves the last statement of the Lemma as is described just before Definition 2.1. ■

Remark Suppose we are given a normalized element of R_V, represented by $P(z, Y)$ with respect to a basis $w_1, \ldots, w_k$. We see that all factorizations of this element (up to multiplication by units of the form $\exp(v)$) can be obtained as follows: take positive integers $N_1, \ldots, N_k$ and factor the polynomial $P(z_1, \ldots, z_n, Y_1^{N_1}, \ldots, Y_k^{N_k})$, say as the product of polynomials $Q_i(z, Y)$ for $i = 1, \ldots, M$. For each i set

$$G_i = Q_i\left(z_1, \ldots, z_n, \exp\left(\frac{1}{N_1} \cdot w_1\right), \ldots, \exp\left(\frac{1}{N_k} \cdot w_k\right)\right).$$

Then the original element must be equal to the product $G_1 \cdot \ldots \cdot G_M$. Moreover, note that each of the factors G_i must be normalized. (Since P has at least one monomial not including any of the variables $Y_1, \ldots, Y_k$, the same must be true of each of the Q_i's.)

LEMMA 2.4 *Let f be a normalized element of R_V.*

(a) *If f is irreducible in R_V, and if f is represented by $P(z, Y)$ with respect to some basis, then $P(z, Y)$ is an irreducible polynomial. (Thus every polynomial of the form $P(z_1, \ldots, z_n, Y_1^{N_1}, \ldots, Y_k^{N_k})$ must also be irreducible, where $N_1, \ldots, N_k$ are positive integers.)*

(b) *Suppose $P(z, Y)$ is a polynomial over $\mathbb{C}$ with at least one monomial not containing any of the variables $Y_1, \ldots, Y_k$. If $P(z, Y)$ has the property that for every $N_1, \ldots, N_k$, the polynomial $P(z_1, \ldots, z_n, Y_1^{N_1}, \ldots, Y_k^{N_k})$ is irreducible, then any element of R_V which is represented by $P(z, Y)$ with respect to some basis must be an irreducible element of R_V.*

(c) *Every irreducible element of R_V generates a prime ideal in R_V.*

(d) *If W is a vector subspace of V, and if g is an irreducible element of R_W, then g remains irreducible in R_V. In particular, each irreducible polynomial in $\mathbb{C}[z_1, \ldots, z_n]$ is irreducible in R_V.*

Proof Parts (a) and (b) follow immediately from what is discussed above. Part (d) follows immediately from Lemma 2.2 and parts (a) and (b). In proving (c), it suffices to consider normalized elements, by Lemma 2.2. Let f be an irreducible, normalized element of R_V, and suppose $F \cdot G = f \cdot H$ is an element of the ideal generated by f in R_V. After multiplying F, G, H by units of the form $\exp(v)$, we may suppose that there exists a single basis $w_1, \ldots, w_k$, with respect to which all of f, F, G, H have polynomial representations. (Multiply H by such a unit to make the new product $f \cdot H$ normalized and then apply Lemma 2.3.) The polynomial by which f is represented must be irreducible, by part (a); hence it must divide one of the polynomials representing F or G. It follows that f must divide F or G in R_V, completing the proof. ■

It is not the case that every non-unit element of R_V has an irreducible factor. For example, consider $f = 1 + \exp(w)$; this is normalized, and is represented by the polynomial $1 + Y$ with respect to the basis w. By Lemma 2.3, any factor of f must

be (up to multiplication by a unit) of the form $g = q\left(\exp\left(\frac{1}{N}\cdot w\right)\right)$ for some integer $N > 0$ and some polynomial $q(Y)$ with non-zero constant term. If the complex number β is one of the roots of the polynomial $q(Y)$, then $-\beta + \exp\left(\frac{1}{N}\cdot w\right)$ divides g in R_V. If α is a complex number satisfying $\alpha^2 = \beta$ then g has factors $\left(\pm\alpha + \exp\left(\frac{1}{2N}\cdot w\right)\right)$. Hence no factor of f is irreducible in R_V. The proof of the unique factorization theorem (given in the next section) shows that in some sense this is a typical example of an element which fails to factor as a product of primes in R_V. (See especially Lemma 3.2.)

We close this section by noting that the units of R_V are exactly the elements of the form $c\cdot\exp(v)$ where c is a non-zero complex number. Evidently every such element is a unit. Lemma 2.2 shows that for the converse, it suffices to show that every normalized unit is a constant. This is easily proved using the representing polynomials as has been done several times above.

3. UNIQUE FACTORIZATION THEOREM

It is natural to call an element f of R_V *infinitely divisible* if f has no irreducible factor in R_V. The main result in this section (Theorem 3.1) is a unique factorization theorem which states that every non-zero, non-unit element of R_V is uniquely a product of an infinitely divisible element and a finite number of primes. Moreover, Theorem 3.1 and its proof give a detailed analysis of the infinitely divisible elements of R_V.

THEOREM 3.1 *Each (non-zero, non-unit) element of R_V can be written uniquely as a finite product of the form*:

$$\exp(u)\cdot p_1(\exp(v_1))\cdot\ldots\cdot p_k(\exp(v_k))\cdot b_1\cdot\ldots\cdot b_m$$

where $b_1, \ldots, b_m$ are primes in R_V, $p_1, \ldots, p_k$ are non-constant polynomials in one variable over $\mathbb{C}$ with $p_i(0) \neq 0$ for each i, and $u, v_1, \ldots, v_k$ are elements of V with the property that no v_i can be written as a rational multiple of any v_j with $i \neq j$. (Uniqueness of the factorization is up to order of the factors and up to multiplication of the factors by units.)

Note It is the elements $\{p_i(\exp(v_i)) \mid i = 1, \ldots, k\}$ which are asserted to be unique up to multiplication by units and order of listing. The complex polynomials $p_1(Y), \ldots, p_k(Y)$ are not uniquely determined by the elements which they represent.

Proof We will first prove the existence of such a factorization. By Lemma 2.2 it suffices to factor elements which are normalized. Let f be a normalized element, represented by the polynomial $P(z, Y)$ with respect to the basis $w_1, \ldots, w_m$. We first assume that $P(z, Y)$ is irreducible as a polynomial in $z_1, \ldots, z_n, Y_1, \ldots, Y_m$; we will treat the general case by factoring P and then treating the factors separately.

We will make use of the following theorem, which is a sharpening by Gourin [9] of a result originally proved by Ritt [15]–[17] in his analysis of factorization in the ring of simple exponential sums. An exposition of this theorem can also be found in [18, Chapter 15].

THEOREM (Gourin) *Let $P(z_1, \ldots, z_n, Y_1, \ldots, Y_m)$ be an irreducible polynomial over $\mathbb{C}$ which has at least three monomials (as a polynomial in its $n+m$ variables). Let d be the maximum degree of P in its individual variables. For each m-tuple $k_1, \ldots, k_m$ of positive integers, there are positive integers $\tau_1, \ldots, \tau_m$, all $\leqslant d^2$, and integers $l_1, \ldots, l_m$ with $k_j = \tau_j \cdot l_j$ for each $j = 1, \ldots, m$, such that if*

$$P(z_1, \ldots, z_n, Y_1^{\tau_1}, \ldots, Y_m^{\tau_m}) = \prod_{i=1}^{r} Q_i(z, Y)$$

is a factorization into irreducible polynomials, then $Q_1, \ldots, Q_r$ are distinct, and

$$P(z_1, \ldots, z_n, Y_1^{k_1}, \ldots, Y_m^{k_m}) = \prod_{i=1}^{r} Q_i(z_1, \ldots, z_n, Y_1^{l_1}, \ldots, Y_m^{l_m})$$

is a factorization into irreducible polynomials.

We continue with the proof of Theorem 3.1, in the case where the irreducible polynomial $P(z, Y)$ has at least three monomials. By the theorem above, there exists an integer D such that each of the polynomials $P(z_1, \ldots, z_n, Y_1^{k_1}, \ldots, Y_m^{k_m})$ is the product of at most D irreducible polynomials. Let D be the smallest such bound, and choose $k_1, \ldots, k_m$ so that it is achieved. Let

$$P(z_1, \ldots, z_n, Y_1^{k_1}, \ldots, Y_m^{k_m}) = \prod_{i=1}^{D} Q_i(z, Y)$$

be a factorization into irreducible polynomials. For each $i = 1, \ldots, m$ let

$$b_i = Q_i\left(z_1, \ldots, z_n, \exp\left(\frac{1}{k_1} \cdot w_1\right), \ldots, \exp\left(\frac{1}{k_m} \cdot w_m\right)\right)$$

so that our original normalized element f is equal to the product $b_1 \cdot \ldots \cdot b_m$.

We claim that each b_i is irreducible in R_V. If not, then by Lemma 2.4(b) there must exist $l_1, \ldots, l_m$ so that $Q_i(z_1, \ldots, z_n, Y_1^{l_1}, \ldots, Y_m^{l_m})$ splits into at least two irreducible factors. But it would follow from this that $P(z_1, \ldots, z_n, Y_1^{k_1 l_1}, \ldots, Y_m^{k_m l_m})$ would have at least $D+1$ irreducible factors, which is impossible by the minimality of D.

Note that this shows that if f is any normalized element of R_V which is represented by an irreducible polynomial having at least three terms, then f is a product of primes in R_V. Moreover, the argument gives a procedure by which these primes can (in principle) be found.

We must still deal with the case where the polynomial representing f has two or fewer terms. The case where it has just one term, meaning that f is simply an element of $\mathbb{C}[z_1, \ldots, z_n]$, is trivial, since irreducible polynomials in this ring remain irreducible in R_V. Thus we are left with the case where

$$P(z, Y) = M_1(z) + M_2(z) \cdot Y_1^{n_1} \cdot \ldots \cdot Y_m^{n_m}$$

where M_1 and M_2 are monomials in the variables $z_1, \ldots, z_n$.

Suppose that M_1 and M_2 are not both constants. We may suppose that z_1 occurs in one of them. Then the polynomial $P(z_1 + 1, z_2, \ldots, z_n, Y_1, \ldots, Y_m)$ has at least three monomials, so that (by the argument above) the element g of R_V which is defined by

$$g = P(z_1 + 1, \ldots, z_n, \exp(w_1), \ldots, \exp(w_m))$$

is a product of primes in R_V. But there is an automorphism of R_V which corresponds to the replacement of z_1 by $z_1 + 1$, and this automorphism takes f to g. Hence f must also be a product of primes in R_V.

The remaining case is where $P(z, Y)$ is of the form $\alpha + \beta \cdot Y_1^{n_1} \cdot \ldots \cdot Y_m^{n_m}$ with α, β non-zero complex numbers and $n_1, \ldots, n_m$ not all zero. But then $f = \alpha + \beta \cdot \exp(v)$, where $v = n_1 \cdot w_1 + \cdots + n_m \cdot w_m \neq 0$. Hence our treatment of the case where f is represented by an irreducible polynomial is complete. Note that we have shown in this case that either f is of the form $\alpha + \beta \cdot \exp(v)$ for some non-zero complex numbers α, β and some non-zero v from V, or f is a product of irreducible elements of R_V.

At this point we know that an arbitrary non-zero, non-unit element of R_V is equal to the product of a finite number of irreducible elements of R_V and a finite number of elements of the form $\alpha + \beta \cdot \exp(v)$. We now discuss how to group these latter factors into the form required by the statement of Theorem 3.1. Suppose $u_1, \ldots, u_p$ are non-zero elements of V and that each u_i, u_j can be written as a rational multiple of the other. Choose N so that each u_i is an integer multiple of $u = \frac{1}{N} \cdot u_1$. For each $i = 1, \ldots, p$, consider an element of R_V of the form $g_i = \alpha_i + \beta_i \cdot \exp(u_i)$, in which α_i and β_i are non-zero complex numbers, and let $g = g_1 \cdot \ldots \cdot g_p$. Multiplying g by appropriate units (of the form $\exp(-u_i)$) if necessary, we may suppose that each u_i in this representation is a *positive* integer multiple of u, say $u_i = k_i \cdot u$. Then $g = p(\exp(u))$, where p is the polynomial

$$p(Y) = \prod_{i=1}^{p} (\alpha_i + \beta_i \cdot Y^{k_i}).$$

This completes the proof that there exists a factorization of the required type for each non-zero, non-unit element of R_V.

For the uniqueness of this factorization, we need to analyze the factors of the form $f = p(\exp(v))$ somewhat more. In particular, we will show that such an f has no irreducible factors, and no factors of the form $q(\exp(u))$ unless u is a rational multiple of v.

LEMMA 3.2 *Let v be a non-zero element of V and let $p(Y)$ be a polynomial in one variable over $\mathbb{C}$ which has at least two terms. Up to multiplication by units, every factor of $p(\exp(v))$ in R_V is of the form $q\left(\exp\left(\frac{1}{N}\cdot v\right)\right)$ for some integer $N>0$ and some polynomial $q(Y)$. (In particular, $p(\exp(v))$ has no irreducible factors in R_V.)*

Proof We may suppose that $p(0)\neq 0$; otherwise factor out a power of Y and use the fact that $(\exp(v))^k=\exp(k\cdot v)$ is a unit in R_V. Then $p(\exp(v))$ is a normalized element of R_V, represented by $p(Y)$ with respect to the basis v. By the remark after Lemma 2.3, every factor of $p(\exp(v))$ must have the required form. Moreover, any such factor $q\left(\exp\left(\frac{1}{N}\cdot v\right)\right)$ of $p(\exp(v))$ has a factor of the form $-\alpha+\exp\left(\frac{1}{N}\cdot v\right)$ (take $\alpha\in\mathbb{C}$ with $q(\alpha)=0$) and hence further factors, for example $\pm\beta+\exp\left(\frac{1}{2N}\cdot v\right)$ if $\beta^2=\alpha$. ■

We now complete the proof of Theorem 3.1, by showing that the terms in the factorization are uniquely determined (up to multiplication by units) by their product. Using Lemmas 2.4 and 3.2 it follows that no two factors which appear in this product have any divisors in common, if the restrictions in the statement of Theorem 3.1 are satisfied. The uniqueness proof therefore goes along the usual lines, once we have proved the following Lemma.

LEMMA 3.3 *Let f, g, F, G be non-zero, non-unit elements of R_V. Suppose $f\cdot g=F\cdot G$ in R_V and that f and F have no non-trivial factors in common. Then f divides G in R_V.*

Proof Applying Lemma 2.3 twice we may suppose that the elements f, g, F, G are all normalized, represented say by polynomials P, Q, R, S with respect to the same basis $w_1,\ldots,w_m$. Hence we have $P\cdot Q=R\cdot S$. The hypothesis implies that P and R must be relatively prime as polynomials in $z_1,\ldots,z_n, Y_1,\ldots,Y_m$. Therefore P must divide S in $\mathbb{C}[z, Y]$, implying that f divides H in R_V. ■

Note that a similar argument to that used in proving Lemma 3.3 can be used to show that if $f, g\in R_V$, then f divides g in R_V if and only if the factors of f (according to the factorization given in Theorem 3.1) occur among the factors of g, counting multiplicities, up to multiplication of factors by units. It follows that in R_V each finite set of elements has a greatest common divisor and a least common multiple; indeed, these can be obtained in the usual way directly from the factorization of the elements as given in Theorem 3.1.

We close this section by noting that if W is a vector subspace of V and if f is an element of R_W, then the unique factorization of f is the same in R_V as in R_W. By Lemma 2.4(d) the irreducible factors of f in R_W remain irreducible in R_V, and the infinitely divisible factors of f also remain unchanged on passing from R_W to R_V.

4. COHERENCE

In this section we show that the integral domains R_V considered here are coherent in the sense of Bourbaki [3, Chapters 1–2]. A commutative ring is said to be *coherent* if every finitely generated ideal is finitely presented. For integral domains, this is equivalent to the statement that the intersection of two finitely generated ideals is finitely generated. (See [6].) Note that R_V is not Noetherian, unless $V = \{0\}$. Indeed, if $w \neq 0$ and we let I_n be the ideal of R_V generated by the element $1 - \exp\left(\frac{1}{n!} \cdot w\right)$, then it can easily be shown that $\{I_n \mid n = 1, 2, \ldots\}$ provides a strictly increasing sequence of ideals in R_V.

We will use the fact that R_V is the localization of the direct limit of a family $\{B_I\}$ of rings, where each ring B_I is a purely transcendental extension of $\mathbb{C}$ (and is therefore Noetherian) and where B_J is a free B_I-module whenever B_J is an extension of B_I in the family. Before describing this representation of R_V, we explain why it shows that R_V is coherent. First we make use of the criterion in [3, Ex. 12c, p. 63]; it states that the direct limit of the system $\{B_I\}$ is coherent, providing that: (i) each B_I is coherent, and (ii) B_J is a flat B_I-module whenever B_J extends B_I. These conditions follow from the fact that each B_I is Noetherian and that free modules are flat. Hence R_V is the localization of a coherent subring; it follows using [10] that R_V is coherent.

To obtain the desired representation of R_V we proceed as follows. Let $\sum$ be a basis over $\mathbb{Q}$ for the vector space V. An index I consists of a positive integer $i = i(I)$ and a finite subset $b(I)$ of $\sum$. The ring B_I is the subring of R_V which is generated by $\mathbb{C}[z_1, \ldots, z_n]$ and the elements $\exp\left(\frac{1}{i} \cdot w\right)$, where $i = i(I)$ and $w \in b(I)$. We regard B_J as an extension of B_I when $i(I)$ divides $i(J)$ and $b(I) \subseteq b(J)$; when these conditions are satisfied then evidently $B_J \supseteq B_I$, so that we have a directed system of subrings with the natural inclusion mappings.

Evidently each B_I is a finitely generated, purely transcendental extension of $\mathbb{C}$. Indeed, we may write

$$B_I = \mathbb{C}[z_1, \ldots, z_n, X_1, \ldots, X_p]$$

where $X_1, \ldots, X_p$ is a list of the elements $\exp\left(\frac{1}{i} \cdot w\right)$ with $i = i(I)$ and $w \in b(I)$. If B_J is an extension in this family of B_I, then

$$B_J = \mathbb{C}[z_1, \ldots, z_n, X_1^{1/k}, \ldots, X_p^{1/k}, X_{p+1}, \ldots, X_{p+m}]$$

where k is the integer such that $i(J) = k \cdot i(I)$ and $X_{p+1}, \ldots, X_{p+m}$ is a list of all the elements $\exp\left(\frac{1}{j} \cdot w\right)$ with $j = i(J)$ and $w \in b(J) \setminus b(I)$. The elements $z_1, \ldots, z_n$, $X_1, \ldots, X_{p+m}$ are algebraically independent; it follows that B_J is freely generated as a B_I-module by the products

$$\prod_{i=1}^{p} (X_i^{1/k})^{n_i} \cdot \prod_{i=1}^{m} X_{p+i}^{n_{p+i}}$$

in which $n_1, \ldots, n_{p+m}$ are non-negative integers and $n_1, \ldots, n_p$ are all $< k$. Hence the directed system $\{B_I\}$ has the required properties and, as discussed above, its direct limit is coherent. Let this direct limit be R. It is easily seen that R is the subring of R_V which is generated by $\mathbb{C}[z_1, \ldots, z_n]$ and the elements $\exp(q \cdot w)$ where $w \in \Sigma$ and q is a *positive* rational number. Let S be the set of all products of these latter elements; that is, S consists of all elements $\exp(v)$, where v can be written as a finite linear combination of basis elements from Σ in which the coefficients are all non-negative. It is evident that R_V is precisely the localization of the direct limit R at the multiplicatively closed set S. This completes the proof that R_V is a coherent ring.

5. MISCELLANY

In this section we discuss several consequences of the results in the earlier sections and discuss the relation between the algebraic and the analytic behavior of exponential functions. We raise here a number of problems for further investigation.

First of all we note that A_n is algebraically closed in B_n for each n. More generally:

THEOREM 5.1 *If V is a vector space and W is a subspace of V, then R_W is algebraically closed in R_V.*

Proof Suppose $f_0, \ldots, f_k$ are elements of R_W $(k > 0)$, g is in R_V, and

$$\sum f_j \cdot g^j = 0.$$

Without loss of generality we may assume $f_0 \neq 0$ and $f_k \neq 0$; evidently g divides f_0 in R_V. As noted at the end of Section 3, the unique factorization of f_0 is the same in R_W as in R_V. From the Unique Factorization Theorem (Theorem 3.1) it follows that there exists $v \in V$ such that $\exp(v) \cdot g$ is in R_W. (The irreducible factors of g must be among the irreducible factors of f_0, and hence must be in R_W up to multiplication by a unit. The infinitely divisible factors of g must divide the infinitely divisible factors of f_0; Lemma 3.2 implies that these factors of g must also be in R_W up to multiplication by a unit.)

Let $h = \exp(v) \cdot g$ and $F_j = f_j \cdot h^j$ for each $j = 0, \ldots, k$; we have then

$$\sum F_j \cdot \exp(-jv) = 0.$$

If $v \in W$, then we are done. Otherwise we may construct an automorphism of V which fixes every element of W, and which maps v to any other element of $V \setminus W$. Each such mapping gives rise to an automorphism of R_V which leaves the elements of R_W fixed; it follows that the polynomial equation

$$\sum F_j \cdot Y^j = 0$$

has infinitely many roots in R_V, which is impossible. (Indeed, this equation would be satisfied by every $Y = \exp(-u)$, where u is an element of $V \setminus W$.) ■

Note For the logician we remark that if V and W are as in Theorem 5.1, and if W has infinite dimension over $\mathbb{Q}$, then R_W must actually be an elementary subring of R_V. In particular, A_n is an elementary subring of B_n for each n. This can be proved using the Tarski test for elementary submodels (see [5]) and the easy fact that (when

W is infinite dimensional) for any given elements $f_1, \ldots, f_k$ of R_W and g of R_V, there is an automorphism of R_V which leaves each f_j fixed and which moves g into R_W. This automorphism comes from a linear automorphism of V which fixes each exponent of $f_1, \ldots, f_k$ and which moves all the exponents of g into W.

In contrast to these results, the nature of the algebraic relation of A_n or B_n to the ring of all entire functions of n variables is very unclear. For example, we do not know how to answer the following natural question.

QUESTION 1 *If f is an entire function of n variables and f^2 is an element of B_n, then must f also be in B_n? (A positive answer would give the same result with B_n replaced by A_n, using Theorem 5.1.)*

If f and g are elements of B_1 with no common zero, then we can find entire functions F and G which solve the Bezout equation

$$f \cdot F + g \cdot G = 1.$$

However, we need not be able to find F and G in B_1. For example, suppose $f = 1 + \exp(z)$ and $g = 1 + \exp(z^2)$. Writing $B_1 = R_V$ for an appropriate vector space V, we see that $f = 1 + \exp(v)$ and $g = 1 + \exp(w)$ for exponents v, w which are linearly independent over $\mathbb{Q}$. From Lemma 3.2 it follows that f and g have no non-trivial common factor in B_1. However, there cannot exist F, G in B_1 which solve the Bezout equation for f, g. If otherwise, we may assume without loss of generality that all exponents of F, G lie in the linear span of $\{v, w\}$. (Apply a retraction of V onto the linear span of $\{v, w\}$ as discussed at the beginning of Section 2.) Choose an integer k large enough so that all exponents of F and of G are $\geqslant -k(v + w)$ in the lexicographic ordering on the span of $\{v, w\}$. As discussed in Section 2, we may therefore obtain polynomials $P(Y_1, Y_2)$ and $Q(Y_1, Y_2)$ over $\mathbb{C}$ such that

$$\exp(-k(v+w)) \cdot F = P\left(\exp\left(\frac{1}{r} \cdot v\right), \exp\left(\frac{1}{s} \cdot w\right)\right)$$

and

$$\exp(-k(v+w)) \cdot G = Q\left(\exp\left(\frac{1}{r} \cdot v\right), \exp\left(\frac{1}{s} \cdot w\right)\right)$$

for appropriate integers r and s. After multiplying through by $\exp(-k(v + w))$ and using the uniqueness of the representation of elements of R_V by polynomials, we obtain the polynomial equation

$$(1 + Y_1^r) \cdot P(Y_1, Y_2) + (1 + Y_2^s) \cdot Q(Y_1, Y_2) = Y_1^{kr} \cdot Y_2^{ks}.$$

This is impossible, as can be seen by taking Y_1 and Y_2 to be appropriate roots of unity in $\mathbb{C}$.

A similar argument (shown to us by A. Macintyre and L. van den Dries) shows that the identity 1 is not even in the E-ideal generated by $1 + \exp(z)$ and $1 + \exp(z^2)$ in A_1. (An ideal I is an E-ideal if $f \in I$ always implies $\exp(f) - 1 \in I$. See [7].) If

otherwise, then there would be an exponential term τ in two variables such that $\tau(0, 0) = 0$ and

$$1 = \tau(1 + \exp(z), 1 + \exp(z^2)).$$

From the results proved in [7] it follows that this equation must hold as an identity in all E-rings. However, one can use the methods of [7] to construct an E-ring with an element α satisfying $E(\alpha) = E(\alpha^2) = -1$, thus obtaining a contradiction.

QUESTION 2 *Given f and g in A_n or in B_n, is there any "algebraic" way to recognize that f and g have no common zero?*

Ritt [17] showed that if f and g are simple exponential sums (of the form $\sum \alpha_i \cdot e^{\beta_i z}$ for some complex numbers $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k$) and if $\frac{f}{g}$ is an entire function, then $\frac{f}{g}$ must itself be a simple exponential sum. (That is, if g divides f in the ring of entire functions, then g divides f in the ring of simple exponential sums.) Berenstein and Dostal [2] extended this result to functions of several variables. The entire functions $\frac{1 - e^z}{z}$ and (more subtly) $\frac{\sin(\pi \cdot z^2)}{\sin(\pi \cdot z)}$ are quotients of functions in A_1, but are not themselves elements of A_1. (This can be shown by a fairly simple argument based on the Normal Form Theorem, Theorem 1.1.) It is an open question whether there is any generalization of the Ritt result to A_n or B_n. For example:

QUESTION 3 *If $f, g \in A_n$ and $\frac{f}{g}$ is an entire function, then must there exist an exponential term which defines g and which is syntactically simpler than any exponential term which defines f?*

In this question we may reasonably assume that f and g have no non-trivial common factor in the ring A_n. The example $f = \sin(\pi \cdot z^2), g = \sin(\pi \cdot z)$ seems especially suggestive here.

One may ask several related questions concerning the possible zero sets of functions in A_n or B_n, and rather little seems known here, even for $n = 1$. While $\sin(\pi \cdot z)$ has $\mathbb{Z}$ as its zero set, it is not hard to show that no function defined by an exponential term, indeed no function in B_1, can have $\mathbb{N}$ as its zero set. (If f were such a function, then we could write

$$f(-z) = \frac{1}{\Gamma(z)} \cdot e^{h(z)}$$

where h is an entire function and $\Gamma(z)$ is the usual Gamma function. From this it would follow that $\frac{\sin(\pi \cdot z)}{\pi \cdot z} = \frac{1}{\Gamma(1 + z) \cdot \Gamma(1 - z)}$ would be in B_1; this is false, as noted above.)

QUESTION 4 *We conjecture: If $f \in A_1$ and if $f(k) = 0$ for $k = 1, 2, 3, \ldots$, then also $f(0) = 0$. (Applying this repeatedly to $f(z - k)$ would yield the further conclusion that $f(r) = 0$ for all $r \in \mathbb{Z}$.)*

To provide a little support for this conjecture, we prove that it holds when f is a simple exponential polynomial,

$$f(z) = \sum q_i(z) \cdot e^{\lambda_i z}$$

for complex polynomials $q_1, \ldots, q_k$ and complex numbers $\lambda_1, \ldots, \lambda_k$. To do this we make use of some p-adic analysis as in the proof of the Skolem–Mahler–Lech Theorem. In particular, we invoke the following result of Cassels [4]. (See also [12] for other applications of this result to obtain several generalizations of the Skolem–Mahler–Lech Theorem.)

THEOREM C (Cassels) *Let K be a finitely generated field extension of $\mathbb{Q}$, and let C be a finite set of non-zero elements of K. Then there exist infinitely many rational primes p such that there is an embedding $\varphi: K \to \mathbb{Q}_p$ of K into $\mathbb{Q}_p$ for which $|\varphi(c)|_p = 1$ for all $c \in C$.*

Suppose that $f(z)$ is a simple exponential polynomial as above and that $f(k) = 0$ for every positive integer k. Let C be the collection of all the coefficients of $q_1, \ldots, q_k$ and all of $\lambda_1, \ldots, \lambda_k$, and let K be $\mathbb{Q}(C)$. Let $\varphi: K \to \mathbb{Q}_p$ be one of the embeddings given by Theorem C. Let Q_j be the polynomial over $\mathbb{Q}_p$ which is the image of q_j under φ (for each $j = 1, \ldots, k$) and let F be the function on $\mathbb{Q}_p$ which is defined by

$$F(z) = \sum Q_j(z) \cdot e^{\varphi(\lambda_j)z}.$$

It is easy to see that F is given by a power series in the p-adic variable z $\left(\text{using } e^w = \sum \frac{w^n}{n!}\right)$ and that this series converges in a suitable p-adic disc about $z = 0$.

By hypothesis, F vanishes at infinitely many p-adic integers. Hence the zeros of F have a p-adic limit point, so that F must be identically 0 on $\mathbb{Q}_p$. In particular $F(0) = 0$ and consequently also $f(0) = 0$, which was to be proved.

Note that the above conjecture becomes false if one replaces A_1 by B_1. This is because the function

$$1 - \exp\left(\frac{1}{\Gamma(1 - z)}\right)$$

is an element of B_1.

There are several decision problems for exponential terms which are connected with the results given here. These make sense only when we restrict the constants which are allowed to occur; let us consider here just the case where we allow only Gaussian integers ($a + b \cdot i$, $a, b \in \mathbb{Z}$) as constants. We will call an exponential term (and the function it defines) *restricted* if it is built up from constants for the Gaussian integers (but not for any other complex numbers) and from the variables, using addition, multiplication and exponentiation. If the term contains no variable, then we will refer to the complex number which it represents as an *exponential constant*. (There are natural sets of complex numbers other than the Gaussian integers to use

as a starting set of constants here, and we only mean to illustrate here the results and questions which are possible.) For example $e^{e^2} + e^i$ is an exponential constant.

It is an open problem whether there is an algorithm for the equality problem between exponential constants. Let us denote this decision problem by EQ. Most decision problems about restricted exponential terms contain EQ, and thus it is natural to consider these problems relative to an oracle for EQ. For example, there is an algorithm relative to EQ which produces, for each restricted exponential term, the term which is its normal form (as in Theorem 1.1). This permits us to decide, relative to EQ, whether two terms represent the same function. (This is true iff they have the same normal form.) In the same way we can decide, relative to EQ, whether the function defined by a given restricted exponential term has a root. (It has no root exactly when its normal form equals a non-zero constant multiplied by an exponential.)

QUESTION 5 *Do there exist algorithms, relative to EQ, which* (a) *decide whether the function defined by a given restricted exponential term is irreducible*, (b) *decide whether a given such function is infinitely divisible*, (c) *produce the factorization of a given such function*, (d) *determine whether a given finite sequence of such functions are linearly independent over* $\mathbb{Q}$, (e) *determine whether or not a given finite sequence of such functions have a common factor in the appropriate ring* A_n?

Adler [1] has shown that there is no *absolute* algorithm for deciding whether a given finite set of restricted exponential terms (in several variables) define functions which have a common zero. (This is equivalent to saying that the existential theory of the exponential field $(\mathbb{C}, +, \cdot, \exp)$ is undecidable. Adler's proof shows that this undecidability result remains true even if $\exp(z)$ is replaced by 2^z, a modification which would seem to lead to a smaller collection of exponential constants and to a perhaps "simpler" class of decision problems.) It seems unlikely that the introduction of an oracle for the equality problem EQ (which is itself likely to be decidable) would change this state of affairs. However, it seems interesting to consider such decision problems in restricted settings, such as when functions of just one variable are concerned.

QUESTION 6 *Is there an algorithm (possibly relative to an oracle for the equality problem EQ) which will determine whether the finite sequence of functions, defined by a given sequence of restricted exponential terms involving only the single variable* z, *have a common zero? Indeed, is there an algorithm (possibly relative to an oracle for some portion of EQ) which decides whether two simple exponential polynomials* $f = \sum p_i \cdot e^{\alpha_i z}$ *and* $g = \sum q_j \cdot e^{\beta_j z}$ *have a common zero in* $\mathbb{C}$? *(Here the* p_i*'s and* q_j*'s are polynomials in* z *with Gaussian integer coefficients and the* α_i*'s and* β_j*'s are Gaussian integers.)*

References

[1] A. Adler, Some recursively unsolvable problems in analysis, *Proc. Amer. Math. Soc.* **22** (1969), 523–526.

[2] C. A. Berenstein and M. A. Dostal, The Ritt theorem in several variables, *Ark. Mat.* **12** (1974), 267–280.

[3] N. Bourbaki, *Algèbre Commutative*, Chapters 1 and 2, Hermann, Paris, 1961.
[4] J. W. S. Cassels, An embedding theorem for fields, *Bull. Australian Math. Soc.* **14** (1976), 193–198.
[5] C. C. Chang and H. J. Keisler, *Model Theory*, North-Holland, Amsterdam, 1973.
[6] S. U. Chase, Direct products of modules, *Trans. Amer. Math. Soc.* **97** (1960), 457–473.
[7] L. van den Dries, Exponential rings, exponential polynomials and exponential functions, *Pacific J. Math.* **113** (1984), 51–66.
[8] L. Fuchs, *Partially Ordered Algebraic Systems*, Pergamon, London, 1963.
[9] E. Gourin, On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves, *Trans. Amer. Math. Soc.* **32** (1930), 485–501.
[10] M. E. Harris, Some results on coherent rings, *Proc. Amer. Math. Soc.* **17** (1966), 474–479.
[11] C. W. Henson and L. A. Rubel, Some applications of Nevanlinna theory to mathematical logic: identities of exponential functions, *Trans. Amer. Math. Soc.* **282** (1984), 1–32; correction, **294** (1986), 381.
[12] V. Laohakosol, Some extensions of the Skolem–Mahler–Lech Theorem, *PhD Thesis*, University of Illinois at Urbana-Champaign, 1983.
[13] A. Macintyre, Notes on real exponentiation, *Unpublished Lecture Notes*, University of Illinois, 1984
[14] A. J. van der Poorten and R. Tijdeman, On common zeros of exponential polynomials, *L'Enseignement Mathématique* **21** (1975), 57–67
[15] J. F. Ritt, A factorization theory for functions, *Trans. Amer. Math. Soc.* **29** (1927), 584–596.
[16] J. F. Ritt, Algebraic combinations of exponentials, *Trans. Amer. Math. Soc.* **31** (1929), 654–679.
[17] J. F. Ritt, On the zeros of exponential polynomials, *Trans. Amer. Math. Soc.* **31** (1929), 680–686.
[18] A. Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor, 1982.