

# Pacific Journal of Mathematics

**EXPONENTIAL RINGS, EXPONENTIAL POLYNOMIALS AND  
EXPONENTIAL FUNCTIONS**

LOU VAN DEN DRIES

# EXPONENTIAL RINGS, EXPONENTIAL POLYNOMIALS AND EXPONENTIAL FUNCTIONS

LOU VAN DEN DRIES

**In this paper we define the category of exponential rings and develop some of its basic properties.**

**Introduction.** An exponential ring, or  $E$ -ring for short, is a pair  $(R, E)$  with  $R$  a ring—in this paper always commutative with 1—and  $E$  a morphism of the additive group of  $R$  into the multiplicative group of units of  $R$ , that is,  $E(x + y) = E(x)E(y)$  for all  $x, y$  in  $R$ , and  $E(0) = 1$ . Examples are  $(\mathbf{R}, a^x)$ ,  $a$  any positive real, and  $(\mathbf{C}, e^x)$ . Of course, any ring  $R$  can be expanded to an  $E$ -ring  $(R, E)$  by putting  $E(x) = 1$  for all  $x$ ; such  $E$ -rings will be called trivial. Ken Manders observed that an  $E$ -ring whose underlying ring has no nilpotents  $\neq 0$  and has characteristic a prime  $p > 0$  is trivial: in such a ring each  $x$  satisfies  $1 = E(0) = E(px) = E(x)^p$ , so  $(E(x) - 1)^p = 0$ , which implies  $E(x) = 1$ .

Related notions of exponential ring have been considered by M. Beeson, by B. Dahn and Wolter, and by A. Wilkie, all in connection with the longstanding open problem of A. Tarski on the decidability of the field of reals with exponentiation. An effective positive solution to this problem seems unlikely without major advances in transcendental number theory: such a solution would give us a decision method to answer any question: is  $e^e = p/q?$ , where  $p, q$  are positive integers. Of course there is such a decision method, but, as we don't know yet whether  $e^e$  is rational, we don't know how it works.

Now in mathematical practice it is less the *effectiveness* of Tarski's decision method for the real field which matters—though this aspect is interesting—but rather the information the method provides on the algebraic-topological nature of the definable sets in  $\mathbf{R}^m$ , and on the asymptotic behavior of definable functions. For example in semi-algebraic and real algebraic geometry this use is formalized in the Tarski-Seidenberg theorem (in an inconstructive version) and in a result like the finiteness of the number of connected components of a semi-algebraic set.

Parts of this use of Tarski's work on the elementary theory of the reals offer more hope of being generalized to the  $E$ -ring  $(\mathbf{R}, e^x)$ . The following

conjecture seems to me justified:

*Each subset of  $\mathbf{R}^m$  definable (with parameters) in the language of  $E$ -rings has finitely many connected components.*

In fact, what I have in mind is a stronger conjecture, that definable sets have cylindrical decompositions, a little bit similar to those for semi-algebraic sets constructed by G. E. Collins [C]. This stronger conjecture has the advantage that one only needs to prove it for quantifier free definable sets. For  $m = 1$  this has been done long ago by Hardy [H], with effective versions more recently given by Richardson [R] and Macintyre [M]. (In the case  $m = 1$  the components are of course intervals.) The case  $m = 2$  will be treated in [D]. To prepare the ground for [D] we solve here two basic problems:

(1) *What is the structure of the free  $E$ -rings, respectively of the free  $E$ -algebras over a given  $E$ -ring?*

(2) *When is the map  $p \mapsto \hat{p}$  (assigning to an  $E$ -polynomial in  $X_1, \dots, X_m$  over  $(R, E)$  the corresponding  $R$ -valued function in  $m$  variables) injective?*

The answer to (1) is completely satisfactory, see §1 and §2, in particular (2.4). For (2) we have a sufficient condition in terms of the existence of derivations of certain type—see §3 and (4.1)—and we get positive answers in the cases  $(\mathbf{R}, e^x)$  and  $(\mathbf{C}, e^x)$ . The case  $(\mathbf{R}, e^x)$  generalizes in fact to  $E$ -rings  $(R, E)$  where  $R$  is an ordered field and  $E(x) \geq 1 + x$  for all  $x$ . If we add to this inequality the assumption that  $E$ -polynomial functions in one variable over  $R$  have a maximum on each segment  $[a, b]$ , then we can also give effective finite bounds on the number of roots such functions can have in  $R$ , see (4.11). (This is related to results for  $\mathbf{R}$  due to Richardson [R] and Macintyre [M].)

After a first draft of this paper was written we learned that the result in (4.6) for  $(\mathbf{C}, e^x)$  was also proved by W. Henson and L. Rubel by completely different methods, namely Nevanlinna theory, see *Notices Amer. Math. Soc.*, November 1981. (In contrast, we only use elementary algebra.)

Let us also mention here that the one variable case of (4.6) had been obtained before by A. Wilkie using differential algebra (unpublished).

### 1. Polynomial $E$ -rings.

(1.1) In the following let  $R$  be an  $E$ -ring with exponential map denoted by  $E$ , and  $m$  a positive integer.

We are going to define the ring of  $E$ -polynomials in the indeterminates  $X_1, \dots, X_m$  over  $R$ , denoted by  $R[X_1, \dots, X_m]^E$ . It will have the structure of a group ring over the ordinary polynomial ring  $R[X_1, \dots, X_m]$ . Its additive

group will be constructed as a direct sum

$$R \oplus A_0 \oplus A_1 \oplus A_2 \oplus \cdots = R \oplus \bigoplus_{k=0}^{\infty} A_k,$$

and for each  $k \geq -1$ , the additive group  $R \oplus A_0 \oplus \cdots \oplus A_k$  is equipped with a multiplication making it a ring  $R_k$ ; this is done in such a way that  $R_{-1} = R$  as a ring and  $R_k$  is a subring of  $R_{k+1}$ . Further, for each  $k \geq -1$  we define a morphism  $E_k$  of the additive group of  $R_k$  into the group of units of  $R_{k+1}$ ; again  $E_{k+1}$  will extend  $E_k$ . Then the underlying ring of  $R[X_1, \dots, X_m]^E$  will be taken as  $\lim_{\rightarrow} R_k = \bigcup R_k$ , and its exponential map will be given by  $E(x) = E_k(x)$  if  $x \in R_k$ .

The construction of the  $A_k$ ,  $R_k$ , and  $E_k$  is done by recursion: Put  $R_{-1} = R$ ,  $R_0 = R[X_1, \dots, X_m]$  and  $A_0 =$  the ideal  $(X_1, \dots, X_m)$   $R[X_1, \dots, X_m]$ ; this gives  $R_0 = R \oplus A_0$  (as additive groups); further  $E_{-1}$  is the composition  $R_{-1} = R \rightarrow R \Rightarrow R[X_1, \dots, X_m] = R_0$ .

Suppose  $k \geq 0$  and  $R_{k-1}$ ,  $R_k$ ,  $A_k$  and  $E_{k-1}$  have been defined in accordance with the description above:  $R_k = R_{k-1} \oplus A_k$ , and  $E_{k-1}$  is a morphism  $R_{k-1} \rightarrow$  group of units of  $R_k$ . Then we form a multiplicative copy  $\exp(A_k)$  of the additive group  $A_k$ , i.e.,  $\exp(A_k)$  is a multiplicative group and an isomorphism  $\exp: A_k \simeq \exp(A_k)$  is given. We put  $R_{k+1} = R_k[\exp(A_k)]$  (group ring of  $\exp(A_k)$  over  $R_k$ ), and  $A_{k+1} = R_k$ -submodule of  $R_{k+1}$  (freely) generated by the  $\exp(a)$  with  $a \in A_k$ ,  $a \neq 0$ . Obviously  $R_{k+1} = R_k \oplus A_{k+1}$  as additive groups. Write  $r \in R_k$  as  $r = r' + a$  with  $r' \in R_{k-1}$ ,  $a \in A_k$ , and define  $E_k: R_k \rightarrow R_{k+1}$  by  $E_k(r) = E_{k-1}(r') \exp(a)$ .

This completes the definition of  $R[X_1, \dots, X_m]^E$ . Note that  $\exp: A_k \rightarrow \exp(A_k)$  is a restriction of the exponential map  $E$  of  $R[X_1, \dots, X_m]^E$ ; therefore we will write from now on  $E(A_k)$ ,  $E(p)$  instead of  $\exp(A_k)$ ,  $\exp(p)$ .  $R[X_1, \dots, X_m]^E$  is obviously an  $E$ -ring extension of  $R$ .

(1.2) PROPOSITION. *Given an  $E$ -ring  $S$  and  $s_1, \dots, s_m \in S$ , each  $E$ -ring morphism  $\phi: R \rightarrow S$  has a unique extension to an  $E$ -ring morphism  $\psi: R[X_1, \dots, X_m] \rightarrow S$  with  $\psi(X_i) = s_i$ ,  $i = 1, \dots, m$ .*

*Proof.* Use the corresponding universal property of  $R[X_1, \dots, X_m] = R_0$  and extend stepwise to each  $R_k$ ,  $k > 0$ . □

(1.3) We call the members of  $R[X_1, \dots, X_m]^E$  exponential polynomials, or  $E$ -polynomials for short, in the variables  $X_1, \dots, X_m$  over  $R$ .

Note that  $R[X_1, \dots, X_m]^E$  is generated as an  $E$ -ring by  $X_1, \dots, X_m$  over  $R$ . More generally if  $S$  is an  $E$ -ring extension of  $R$  and  $x_1, \dots, x_m \in S$ , then we write  $R[x_1, \dots, x_m]^E$  for the  $E$ -subring of  $S$  generated by  $x_1, \dots, x_m$  over  $R$ .

(1.4) If  $\phi: R \rightarrow S$  is an  $E$ -ring morphism, then, according to (1.2),  $\phi$  has a unique extension to an  $E$ -ring morphism  $R[X_1, \dots, X_m]^E \rightarrow S[X_1, \dots, X_m]^E$  sending  $X_i$  to  $X_i$ ; this morphism we will indicate by  $p \mapsto p^\phi$ . (For ordinary polynomials it replaces the coefficients of  $p$  by their  $\phi$ -images.)

If  $S$  is an  $E$ -ring extension of  $R$  and  $\phi$  is the inclusion  $R \rightarrow S$ , then  $p \mapsto p^\phi$  is 1-1, and we will identify  $p$  and  $p^\phi$ , as is common for ordinary polynomials. So  $R[X_1, \dots, X_m]^E \subset S[X_1, \dots, X_m]^E$ .

(1.5) A set  $I$  gives rise to the  $E$ -ring  $R^I$  of functions  $I \rightarrow R$  where the operations are defined pointwise. For  $I \neq \emptyset$  we identify the constant functions with their values in  $R$ , so  $R \subset R^I$ . If  $I = R^m$ , then the coordinate functions are denoted by  $x_1, \dots, x_m$  where  $x_i(r_1, \dots, r_m) = r_i$ . The  $E$ -ring morphism  $R[X_1, \dots, X_m]^E \rightarrow R^{(R^m)}$  fixing  $R$  and sending each  $X_i$  to  $x_i$  will be indicated by  $p \mapsto \hat{p}$ . The  $\hat{p}$ 's are called  $E$ -polynomial functions (in  $m$  variables).

In §4 we will give conditions under which  $p \mapsto \hat{p}$  is a 1-1 correspondence.

(1.6) PROPOSITION. *If  $R$  is an integral domain of characteristic 0 then  $R[X_1, \dots, X_m]^E$  is an integral domain whose units are of the form  $uE(p)$ ,  $u$  a unit of  $R$ ,  $p \in R[X_1, \dots, X_m]^E$ .*

*Proof.* By induction on  $k \geq 0$  we show that  $R_k$  is an integral domain whose units are of the form  $u \cdot E(p)$ ,  $u$  a unit of  $R$ ,  $p \in R_{k-1}$ . This is well known for  $k = 0$ . If we assume the result for  $k$ , then  $A_k$  is a torsion free abelian group, so the group  $\exp(A_k)$  has a linear order, from which it is routine to derive that the group ring  $R_k[\exp(A_k)] = R_{k+1}$  is an integral domain whose units are of the form  $\alpha \cdot E(\beta)$  with  $\alpha$  a unit of  $R_k$  and  $\beta \in A_k$ . Applying the induction hypothesis to  $\alpha$  gives the desired result.  $\square$

The following lemma is sometimes useful, but not needed in this paper.

(1.7) LEMMA. *Let  $R$  be an integral domain of characteristic 0.*

(a) If  $p_1, \dots, p_m \in A_k$ ,  $k \geq 0$ , then  $E(p_1), \dots, E(p_m)$  are algebraically independent over  $R_k$  if and only if  $p_1, \dots, p_m$  are  $\mathbf{Z}$ -linearly independent.

(b) Each finite subset of  $R_{k+1}$  ( $k \geq 0$ ) is included in a subring  $R_k[E(\pm p_1), \dots, E(\pm p_m)]$  of  $R_{k+1}$  where  $p_1, \dots, p_m$  are in  $A_k$  and  $\mathbf{Z}$ -linearly independent.

*Proof.* (a) is straightforward, and for (b) one uses the fact, implied by (1.6), that  $A_k$  is torsion free, and that therefore every finitely generated subgroup of  $A_k$  is free as an abelian group.  $\square$

(1.8) Suppose we have  $m + n$  indeterminates  $X_1, \dots, X_m, X_{m+1}, \dots, X_{m+n}$ . The universal property (1.2) implies that there is a unique  $R \cup \{X_1, \dots, X_{m+n}\}$ -fixing  $E$ -ring isomorphism

$$R[X_1, \dots, X_{m+n}]^E \simeq (R[X_1, \dots, X_m]^E)[X_{m+1}, \dots, X_{m+n}]^E.$$

As in the case of ordinary polynomials we usually identify the two  $E$ -rings via this isomorphism. In particular an  $E$ -polynomial in  $m + 1$  indeterminates  $X_1, \dots, X_{m+1}$  will be considered as an  $E$ -polynomial in  $X_{m+1}$ , over the  $E$ -ring  $R[X_1, \dots, X_m]^E$ .

(1.9) We call  $p(X) \in R[X]^E$

$$\begin{cases} \text{of height } k, & \text{if } p \in R_k \setminus R_{k-1}, k > 0 \\ \text{of height } 0, & \text{if } p \in R_0 = R[X]. \end{cases}$$

Intuitively the height is the maximum number of embedded exponentiations if we express  $p(X)$  in terms of the elements of  $R$ , the variable  $X$  and the symbols  $+$ ,  $\cdot$ , and  $E$ .

If  $p = p(X) \in A_k$ ,  $k > 0$ , we write  $p = \sum_{i=1}^h r_i E(a_i)$ , where  $a_1, \dots, a_h$  are distinct members of  $A_{k-1} \setminus \{0\}$ , and  $r_1, \dots, r_h$  are non-zero elements of  $R_{k-1}$ ; we put  $h = t(p)$ .

Also, for  $p \in R_0 = R[X]$  we put  $t(p) = 0$  if  $p = 0$ , and  $t(p) = d + 1$  if  $\deg_x p = d \geq 0$ .

Now we can define an ordinal  $\text{ord}(p) < \omega^\omega$  for  $p \in R[X]^E$ . Note that  $R_k = R_0 \oplus A_1 \oplus \dots \oplus A_k$  ( $k \geq 0$ ). So any  $p(X)$  of height  $\leq k$  can be written uniquely as

$$p = p_0 + p_1 + \dots + p_k, \quad p_0 \in R_0, p_i \in A_i \text{ for } i > 0.$$

We put

$$\text{ord}(p) = \omega^k \cdot t(p_k) + \dots + \omega \cdot t(p_1) + t(p_0).$$

Note that  $\text{ord}(p) = 0 \Leftrightarrow p = 0$ .

We call  $p_0$  as above the polynomial part of  $p$ .

The ordinal  $\text{ord}(p)$  serves similar purposes as the degree for ordinary polynomials. It will enable us to give proofs by induction on  $\text{ord}(p)$ , see (4.1). But note that  $\text{ord}(p)$  does not put a bound on the “complexity” of  $p$  (as  $\text{deg}(p)$  does for ordinary polynomials), unless  $\text{ord}(p) < \omega$ .

(1.10) LEMMA. *If a nonzero  $p \in R[X]^E$  has zero polynomial part, then there is  $q \in R[X]^E$  such that  $\text{ord}(E(q) \cdot p) < \text{ord}(p)$ .*

*Proof.* Write  $p = p_0 + \cdots + p_k$  as above and assume that the minimal  $i$  such that  $p_i \neq 0$  is positive. Write

$$p_i = r_1 \cdot E(a_1) + \cdots + r_h \cdot E(a_h),$$

$$r_j \in R_{i-1}, a_j \in A_{i-1} \setminus \{0\}, h = t(p_i).$$

Then it is easy to check that  $\text{ord}(E(-a_1) \cdot p) < \text{ord}(p)$ . □

REMARK. A crucial but obvious point is that to any ordinary polynomial  $p$  over a ring  $R$  is associated a *finite* set  $C$ , its set of coefficients, which has the property that, for any ring morphism  $\phi: R \rightarrow S$ , one has  $p^\phi = 0$  if and only if  $\phi(C) \subset \{0\}$ .  $E$ -polynomials do not in general have a finite set of coefficients characterized by this property, but in the next section we will develop a suitable substitute.

## 2. Free $E$ -rings.

(2.1)  $E$ -rings form an equational class relative to the language  $\{0, 1, +, \cdot, -, E\}$ , so there are free  $E$ -rings.

Let  $X_1, \dots, X_m$  be (distinct) indeterminates as before, but we allow  $m = 0$ .

The free  $E$ -ring on  $X_1, \dots, X_m$ , denoted  $[X_1, \dots, X_m]^E$ , is an  $E$ -ring containing  $X_1, \dots, X_m$  as elements such that there is for each  $E$ -ring  $R$  and any  $r_1, \dots, r_m \in R$  exactly one  $E$ -ring morphism  $[X_1, \dots, X_m]^E \rightarrow R$  sending  $X_i$  to  $r_i$ ,  $i = 1, \dots, m$ .

This universal property obviously determines  $[X_1, \dots, X_m]^E$  up to (unique)  $\{X_1, \dots, X_m\}$ -fixing isomorphism. In view of §1 it will not surprise the reader how  $[X_1, \dots, X_m]^E$  looks like: its additive group is a direct sum

$$B_0 \oplus B_1 \oplus B_2 \oplus \cdots = \bigoplus_{k=0}^{\infty} B_k,$$

for each  $k \geq 0$  we equip  $B_0 \oplus \cdots \oplus B_k$  with a multiplication making it a ring, denoted  $[X_1, \dots, X_m]_k$ , in such a way that  $[X_1, \dots, X_m]_0 = Z[X_1, \dots, X_m]$  (the underlying additive group is called  $B_0$ ), and

$[X_1, \dots, X_m]_k$  is a subring of  $[X_1, \dots, X_m]_{k+1}$ ; moreover there is for each  $k \geq 0$  a morphism  $E_k$  from the additive group of  $[X_1, \dots, X_m]_k$  into the multiplicative group of  $[X_1, \dots, X_m]_{k+1}$ .

The precise construction of  $[X_1, \dots, X_m]_{k+1}$ ,  $B_{k+1}$ ,  $E_k$  from  $[X_1, \dots, X_m]_k = [X_1, \dots, X_m]_{k-1} \oplus B_k$  and  $E_{k-1}$  (where we put  $[X_1, \dots, X_m]_{-1} = \{0\}$  and  $E_{-1}(0) = 1$ ) ( $k \geq 0$ ) is as follows:

$$[X_1, \dots, X_m]_{k+1} = [X_1, \dots, X_m]_k [\exp(B_k)] \quad (\text{group ring construction}),$$

where  $\exp$  is an isomorphism from the additive group  $B_k$  onto the multiplicative group  $\exp(B_k)$ . Further,  $E_k(x) = E_{k-1}(r) \exp(b)$  if  $x = r + b$ ,  $r \in [X_1, \dots, X_m]_{k-1}$ ,  $b \in B_k$ .

Now  $[X_1, \dots, X_m]^E$  has underlying ring  $\varinjlim [X_1, \dots, X_m]_k = \bigcup_{k=0}^{\infty} [X_1, \dots, X_m]_k$ , and exponential map  $E$  given by  $E(x) = E_k(x)$  if  $x \in [X_1, \dots, X_m]_k$ .

(2.2) NOTATIONS.

We will write  $\bar{X}$  for  $(X_1, \dots, X_m)$ ,  $\bar{Y}$  for  $(Y_1, \dots, Y_n)$ , and the  $Y_1, \dots, Y_n$  will denote  $n$  distinct indeterminates (also distinct from the  $X$ 's).

Given  $p = p(\bar{X})$  in  $[\bar{X}]^E$ , an  $E$ -ring  $R$  and  $\bar{r} \in R^m$  we write  $p(\bar{r})$  for the image of  $p$  under the  $E$ -morphism  $[\bar{X}]^E \rightarrow R$  sending  $\bar{X}$  to  $\bar{r}$ .

A special case deals with the situation that  $R$  is an  $E$ -ring,  $\bar{r} \in R^m$  and one considers the  $E$ -ringmorphism  $[\bar{X}, \bar{Y}]^E \rightarrow R[\bar{Y}]^E$  sending  $\bar{X}$  to  $\bar{r}$  and fixing  $\bar{Y}$ . In accordance with the notational convention just established we write  $p(\bar{r}, \bar{Y})$  for the image of  $p(\bar{X}, \bar{Y}) \in [\bar{X}, \bar{Y}]^E$  in  $R[\bar{Y}]^E$ . The importance of these morphisms comes from the following lemma and subsequent theorem (2.4) with its corollary (2.5).

(2.3) LEMMA. *Let  $R$  be an  $E$ -ring and  $q(\bar{Y}) \in R[\bar{Y}]^E$ . Then there is  $m \geq 0$  and  $\bar{X} = (X_1, \dots, X_m)$ , such that  $q(\bar{Y}) = p(\bar{r}, \bar{Y})$  for some  $p(\bar{X}, \bar{Y}) \in [\bar{X}, \bar{Y}]^E$  and  $\bar{r} \in R^m$ .*

*Proof.* If  $q(\bar{Y}) \in R[\bar{Y}] = R_0$ , then this is obvious:  $\bar{r}$  can be taken as the vector of non-zero coefficients of  $q$ , in any order. If  $q(\bar{Y}) = p(\bar{r}, \bar{Y})$ , then  $E(q(\bar{Y})) = P(\bar{r}, \bar{Y})$  where  $P = E(p(\bar{X}, \bar{Y}))$ . If  $q_1(\bar{Y}) = p_1(\bar{r}, \bar{Y})$ ,  $q_2(\bar{Y}) = p_2(\bar{s}, \bar{Y})$  where  $\bar{r} = (r_1, \dots, r_m)$ ,  $\bar{s} = (s_1, \dots, s_t)$ , then  $q_1(\bar{Y}) + q_2(\bar{Y}) = P(\bar{r}, \bar{s}, \bar{Y})$  with  $P = p_1(X_1, \dots, X_m, \bar{Y}) + p_2(X_{m+1}, \dots, X_{m+t}, \bar{Y})$ . Similarly for products. □

(2.4) THEOREM. *Let  $p(\bar{X}, \bar{Y}) \in [\bar{X}, \bar{Y}]^E$ . There is a positive quantifier free formula  $Z_p(\bar{X})$  in the language  $\{+, \cdot, -, 0, 1, E\}$  such that for each  $E$ -ring  $R$  and  $\bar{r} \in R^m$  we have:  $p(\bar{r}, \bar{Y}) = 0$  in  $R[\bar{Y}]$  if and only if  $R \models Z_p(\bar{r})$ .*



Before we prove this, let us note the following useful consequence:

(2.5) COROLLARY. *Given an  $E$ -ring  $R$  and  $q \in R[\bar{Y}]^E$  there is a finite set  $\{c_1, \dots, c_t\} \subset R$  such that for each  $E$ -morphism  $\phi$  from  $R$  into an  $E$ -domain  $D$  we have:  $q^\phi = 0$  in  $D[\bar{Y}]$  if and only if  $\phi(c_1) = \dots = \phi(c_t) = 0$ .*

*Proof.* Use (2.3) to write  $q = p(\bar{r}, \bar{Y})$ ,  $p \in [\bar{X}, \bar{Y}]^E$ ,  $\bar{r} \in R^m$ . Take a positive quantifier free formula  $Z_p(\bar{X})$  with the property stated in (2.4). Relative to the theory of  $E$ -domains (that is:  $E$ -rings with  $0 \neq 1$  and without zero divisors) this formula is equivalent to a formula  $p_1(\bar{X}) = \dots = p_t(\bar{X}) = 0$ , where  $p_i(\bar{X}) \in [\bar{X}]^E$ ,  $i = 1, \dots, t$ . Take  $c_1 = p_1(\bar{r}), \dots, c_t = p_t(\bar{r})$ . As  $q^\phi = p(\phi(\bar{r}), \bar{Y})$ , we have:

$$\begin{aligned} q^\phi = 0 \text{ in } D[\bar{Y}]^E &\Leftrightarrow D \models Z_p(\phi(\bar{r})) \quad (\text{by (2.4)}) \\ &\Leftrightarrow p_1(\phi\bar{r}) = \dots = p_t(\phi\bar{r}) = 0 \\ &\Leftrightarrow \phi(c_1) = \dots = \phi(c_t) = 0. \quad \square \end{aligned}$$

(2.6) *Proof of (2.4).* Let  $R$  denote an  $E$ -ring and  $\bar{r}$  an  $m$ -tuple in  $R^m$ .

We identify the free  $E$ -ring  $[\bar{X}, \bar{Y}]^E$  with the  $E$ -polynomial ring  $([\bar{X}]^E)[\bar{Y}]^E$  over  $[\bar{X}]^E$ . Let us write  $A_k(\bar{X}, \bar{Y})$ ,  $R_k(\bar{X}, \bar{Y})$  for the  $A_k$  and  $R_k$  arising in the construction of  $([\bar{X}]^E)[\bar{Y}]^E$  from  $[\bar{X}]^E$  and  $\bar{Y}$ . (See (1.1).) Similarly we let  $A_k(\bar{Y})$ ,  $R_k(\bar{Y})$  stand for the  $A_k$ ,  $R_k$  arising in the construction of  $R[\bar{Y}]^E$  from  $R$ . A trivial induction gives that for all  $k$ :

$$p(\bar{X}, \bar{Y}) \in R_k(\bar{X}, \bar{Y}) \Rightarrow p(\bar{r}, \bar{Y}) \in R_k(\bar{Y}).$$

Unfortunately we cannot replace  $R_k$  by  $A_k$  in this implication.

Let  $E$ -rings be the theory of  $E$ -rings. We shall prove by induction on  $k \geq 0$ :

(\*) Let  $p \in R_k(\bar{X}, \bar{Y})$ . There is a positive open formula  $Z_p(\bar{X})$  with the property stated in the theorem. Moreover, there are formulas  $\phi_1 = \phi_1(\bar{X}), \dots, \phi_t = \phi_t(\bar{X})$ , and for each  $j = 1, \dots, t$  there are  $p_{j0}, p_{j1} \in R_k(\bar{X}, \bar{Y})$  such that  $p = p_{j0} + p_{j1}$ , and  $E$ -rings  $\vdash \bigvee_{j=1}^t \phi_j$ ; and, whenever  $R \models \phi_j(\bar{r})$ ,  $1 \leq j \leq t$ ,  $R$  any  $E$ -ring,  $\bar{r} \in R^m$ , then  $p_{j0}(\bar{r}, \bar{Y}) \in R_{k-1}(\bar{Y})$ ,  $p_{j1}(\bar{r}, \bar{Y}) \in A_k(\bar{Y})$ .

$k = 0$ : write  $p = q_0(\bar{X}) + q_1(\bar{X})\bar{Y}^{\alpha_1} + \dots + q_s(\bar{X})\bar{Y}^{\alpha_d}$ , where  $q_i(\bar{X}) \in [\bar{X}]^E$  and the  $\bar{Y}^{\alpha_i}$  are monomials in  $\bar{Y}$  different from 1. Then we can take for  $Z_p(\bar{X})$  the formula  $q_0(\bar{X}) = q_1(\bar{X}) = \dots = q_s(\bar{X}) = 0$ . Moreover, one can take  $t = 1$  and for  $\phi_1(\bar{X})$  the formula  $0 = 0$ , and  $p_{10} = q_0$ ,  $p_{11} = q_1 \cdot \bar{Y}^{\alpha_1} + \dots + q_s \cdot \bar{Y}^{\alpha_d}$ . This proves (\*) for  $k = 0$ .

Suppose (\*) holds for  $k$ . (Induction hypothesis.) Let  $p \in R_{k+1}(\bar{X}, \bar{Y})$ , so  $p = q_1 \cdot E(p_1) + \cdots + q_s E(p_s)$  where the  $q$ 's are in  $R_k(\bar{X}, \bar{Y})$  and the  $p_i$ 's in  $A_k(\bar{X}, \bar{Y})$ . We apply the induction hypothesis to each  $p_i$  and obtain open formulas  $\phi_{i1}, \dots, \phi_{it(i)}$ , and  $p_{ij0}, p_{ij1}$ , in  $R_k(\bar{X}, \bar{Y})$  for  $j = 1, \dots, t(i)$  with the implied property. Take any  $E$ -ring  $R$  and  $\bar{r} \in R^m$ . For each  $i = 1, \dots, s$  there is  $j$ ,  $1 \leq j \leq t(i)$  such that  $R \models \phi_{ij}(\bar{r})$ ; whence also  $p_{ij0}(\bar{r}, \bar{Y}) \in R_{k-1}(\bar{Y})$ ,  $p_{ij1}(\bar{r}, \bar{Y}) \in A_k(\bar{Y})$ . For simplicity let us write  $\phi_i$  for this  $\phi_{ij}$  and  $p_{i0}, p_{i1}$ , for the corresponding  $p_{ij0}, p_{ij1}$ . So we have  $R \models \phi_1(\bar{r}) \wedge \cdots \wedge \phi_s(\bar{r})$ . (But note that this is only one of  $t_1 \cdot t_2 \cdots t_s$  alternative conjunctions.)

Put

$$Q_1 = q_1 E(p_{10}), \dots, Q_s = q_s E(p_{s0}),$$

$$P_1 = p_{11}, \dots, P_s = p_{s1}.$$

Then, as  $p_i = p_{i0} + p_{i1}$ , we have

$$p = Q_1 E(P_1) + \cdots + Q_s E(P_s), \quad (\text{in } [\bar{X}, \bar{Y}]^E),$$

$$Q_i(\bar{r}, \bar{Y}) \in R_k(\bar{Y}),$$

$$P_i(\bar{r}, \bar{Y}) \in A_k(\bar{Y}) \quad \text{for } i = 1, \dots, s.$$

It follows that  $p(\bar{r}, \bar{Y}) = 0$  in  $R[\bar{Y}]^E$  if and only if there is a partition of  $\{1, \dots, s\}$  into subsets  $I_1, \dots, I_\mu$  such that for each  $\lambda = 1, \dots, \mu$ :  $P_{i_1}(\bar{r}, \bar{Y}) = P_{i_2}(\bar{r}, \bar{Y})$  for all  $i_1, i_2 \in I_\lambda$  and  $\sum_{i \in I_\lambda} Q_i(\bar{r}, \bar{Y}) = 0$ .

By the induction hypothesis this equivalence can be reformulated as:

$$p(\bar{r}, \bar{Y}) = 0 \quad \text{in } R[\bar{Y}]^E \Leftrightarrow R \models Z_{p, \phi_1, \dots, \phi_s}(\bar{r}),$$

where  $Z_{p, \phi_1, \dots, \phi_s}$  is a positive open formula depending only on  $p$  and the alternative  $\phi_1 \wedge \phi_2 \wedge \cdots \wedge \phi_s$  satisfied by  $(R, \bar{r})$ . A subtle but crucial point is that the  $\Leftarrow$  direction holds also for those  $(R, \bar{r})$  which do not satisfy the conjunction  $\phi_1 \wedge \cdots \wedge \phi_s$ .

Notice that we obtain in this way  $t_1 \cdots t_s$  formulas  $Z_{p, \phi_1, \dots, \phi_s}$ . Now we let  $Z_p$  be the disjunction of these  $t_1 \cdots t_s$  formulas  $Z_{p, \phi_1, \dots, \phi_s}$ , and it is easy to see that

$$p(\bar{r}, \bar{Y}) = 0 \Leftrightarrow R \models Z_p(\bar{r}),$$

for any  $E$ -ring  $R$  and  $\bar{r} \in R^m$ .

To prove the second part of (\*) for  $k := k + 1$ , we let  $R, \bar{r}$  be as before, in particular  $R \models \phi_1(\bar{r}) \wedge \cdots \wedge \phi_s(\bar{r})$ . Given any subset  $I$  of

$\{1, \dots, s\}$  there are, by the induction hypothesis, formulas  $\phi_I(\bar{X})$  and  $\psi_I(\bar{X})$  such that

$$\begin{aligned} R \models \phi_I(\bar{r}) &\Leftrightarrow P_i(\bar{r}, \bar{Y}) = 0 \quad \text{for all } i \in I, \\ R \models \psi_I(\bar{r}) &\Leftrightarrow P_i(\bar{r}, \bar{Y}) \neq 0 \quad \text{for all } i \notin I. \end{aligned}$$

Now it is clear that the disjunction of the  $t_1 \cdots t_s \cdot 2^s$  formulas  $\phi_1 \wedge \cdots \wedge \phi_s \wedge \phi_I \wedge \psi_I$  is true in all  $E$ -rings, that

$$p = P_{I,0} + P_{I,1},$$

where

$$P_{I,0} = \sum_{i \in I} Q_i \cdot E(P_i), \quad P_{I,1} = \sum_{i \notin I} Q_i \cdot E(P_i),$$

and that, if  $(R, \bar{r}) \models \phi_1 \wedge \cdots \wedge \phi_s \wedge \phi_I \wedge \psi_I$ , then  $P_{I,0}(\bar{r}, \bar{Y}) \in R_k(\bar{Y})$ ,  $P_{I,1}(\bar{r}, \bar{Y}) \in A_{k+1}(\bar{Y})$ .  $\square$

*Note.* The formulas  $\phi_i$  are not necessarily positive open, though they can be taken to be open, and therefore should not be part of the  $Z_p$ 's. This causes some of the complications in the proof.

### 3. Derivations on $E$ -polynomial rings.

(3.1) Let  $R$  again be an  $E$ -ring,  $X$  an indeterminate.

We know that the polynomial ring  $R[X]$  has a standard derivation:  $(\sum_0^n r_i X^i)' = \sum_1^n i r_i X^{i-1}$ . We can extend this derivation uniquely to one on  $R[X]^E$  in such a way that  $E(q)' = q'E(q)$  (for all  $q$ ), a reasonable formula if one thinks of  $E(q)$  as  $e^q$ . In fact, the following lemma is more general, and takes also into account an interpretation of  $E(q)$  as  $a^q$  with derivative  $(\log a) \cdot q' \cdot a^q$ .

(3.2) LEMMA. *Given  $r \in R$  there is exactly one derivation on  $R[X]^E$  which is trivial on  $R$  and satisfies  $X' = 1$ ,  $E(q)' = r \cdot q' \cdot E(q)$  for all  $q \in R[X]^E$ . This derivation maps  $R_k$  into itself,  $k \geq 1$ .*

*Proof.* Suppose we have a derivation  $'$  on  $R_k$  satisfying the above, with  $q$  restricted to  $R_{k-1}$ ,  $k \geq 0$ . (Induction hypothesis, obviously holding for  $k = 0$ .) To extend to a derivation  $'$  on  $R_{k+1}$  satisfying the above for  $q$  in  $R_k$ , we have to put

$$\left( \sum_{i=1}^h p_i \cdot E(q_i) \right)' = \sum_{i=1}^h (p_i' + r p_i q_i') E(q_i),$$

where  $p_i \in R_k$ ,  $q_i \in A_k$ ,  $q_i \neq q_j$  for  $i \neq j$ . Now it is straightforward to check that this formula does indeed define a derivation on  $R_{k+1}$ .

As  $R[X]^E = \bigcup R_k$ , we obtain in this way a derivation on  $R[X]^E$ , with the required properties. The uniqueness of  $'$  is clear by a very similar argument.  $\square$

Now we can extend (1.10) as follows.

(3.3) LEMMA. *Let  $r \in R$  and let  $'$  be the derivation on  $R[X]^E$  defined in the previous lemma. If  $p \in R[X]^E$  is nonzero, then either  $\text{ord}(E(q) \cdot p) < \text{ord}(p)$  for some  $q \in R[X]^E$ , or  $\text{ord}(p') < \text{ord}(p)$ .*

*Proof.* Let  $p_0$  be the polynomial part of  $p$ . The case  $p_0 = 0$  leads to the first alternative, by (1.10), so suppose  $p_0 \neq 0$ . Then  $t(p'_0) < t(p_0)$ . Moreover, it is clear from the proof of (3.2) that  $'$  maps  $A_i$  into  $A_i$  for  $i > 0$  and that  $t(q') \leq t(q)$  for  $q \in A_i$ . So it follows from the definition of  $\text{ord}$  that  $\text{ord}(p') < \text{ord}(p)$ .  $\square$

The following result is crucial in §4. Its proof is based on a suggestion by Ken Manders and replaces an earlier more complicated proof based on differential algebra.

(3.4) PROPOSITION. *Let  $R$  be a domain of characteristic 0,  $r \in R \setminus \{0\}$ , and let  $'$  denote the derivation on  $R[X]^E$  introduced in (3.2). Then the ring of constants of  $R[X]^E$  is  $R$ , that is:*

$$p' = 0 \Leftrightarrow p \in R.$$

*Proof.* We first show by induction on  $k \geq 0$ : if  $p \in R_k \setminus \{0\}$  and  $q \in R_k \setminus R_{k-1}$ , then  $p' + rpq' \neq 0$ . For  $k = 0$  one just notices that, as  $rq' \neq 0$ ,  $rpq'$  has higher degree in  $X$  than  $p'$ , so  $p' + rpq' \neq 0$ . Suppose the statement holds for some  $k$  and let  $p \in R_{k+1} \setminus \{0\}$ ,  $q \in R_{k+1} \setminus R_k$ . We fix a linear order on the abelian (torsion free) group  $A_k$  and write  $p = \sum_{i=1}^m a_i E(b_i)$ ,  $q = \sum_{j=1}^n c_j E(d_j)$  with all  $a_i, c_j \in R_k \setminus \{0\}$  and  $b_i, d_j \in A_k$  with  $b_1 < \dots < b_m, d_1 < \dots < d_n$ . There are two cases:

- (1)  $d_n > 0$ .
- (2)  $d_1 < 0$ .

Consider first case (1). Now  $q' = \sum_{j=1}^n (c'_j + rc_j d'_j) \cdot E(d_j)$  and  $c'_n + rc_n d'_n \neq 0$  by induction assumption. So  $rpq'$  contains a 'highest' term  $ra_m \cdot (c'_n + rc_n d'_n)E(b_m + d_n) \neq 0$  and  $p'$  contains only 'lower' terms  $(a'_i + ra_i b'_i)E(b_i)$ . Hence  $p' + rpq' \neq 0$ . Case (2) is treated in the same way, looking instead at the lowest term in  $rpq'$ . This proves our assertion.

Now let  $p \in R[X]^E \setminus R$ . So  $p \in R_{k+1} \setminus R_k$ , some  $k \geq -1$ . We have to show that  $p' \neq 0$ . For  $k = -1$  this is obvious, and for  $k \geq 0$ , write  $p = \sum_{i=1}^m a_i \cdot E(b_i)$  as before. So either  $b_1 \neq 0$  or  $b_m \neq 0$ . Again, if  $b_1 \neq 0$ , then  $a'_1 + ra_1 b'_1 \neq 0$  by the assertion proved above, so  $p' = \sum (a'_i + ra_i b'_i) E(b_i)$  contains a lowest non-zero term  $(a'_1 + ra_1 b'_1) \cdot E(b_1)$ , hence  $p' \neq 0$ . The case  $b_m \neq 0$  is treated similarly.  $\square$

**4. Exponential functions.** Recall from (1.5) that  $R[x_1, \dots, x_m]^E$  consists of the  $E$ -polynomial functions  $R^m \rightarrow R$ , and that  $p = p(X_1, \dots, X_m) \mapsto \hat{p} = p(x_1, \dots, x_m)$  assigns to each  $E$ -polynomial its corresponding function.

(4.1) PROPOSITION. *Suppose the  $E$ -ring  $R$  is an integral domain of characteristic 0, that there is a nonzero  $r$  in  $R$ , and that there are derivations  $d_1, \dots, d_m$  on a ring extension of  $R[x_1, \dots, x_m]^E$  which are trivial on  $R$  and satisfy  $d_i(x_j) = \delta_{ij}$ ,  $1 \leq i, j \leq m$ , and  $d_i(E(f)) = r \cdot d_i(f) \cdot E(f)$  for all  $f$  in  $R[x_1, \dots, x_m]^E$  and  $i = 1, \dots, m$ .*

*Then the map  $p \mapsto \hat{p}: R[X_1, \dots, X_m]^E \rightarrow R[x_1, \dots, x_m]^E$  is an isomorphism.*

*Proof.* By induction on  $m$ . The case  $m = 0$  is trivial. Suppose  $m > 0$  and the statement is true upon replacing  $m$  by  $m - 1$ . Note that then the morphism  $\hat{\phantom{p}}$  above maps the  $E$ -subring  $R[X_1, \dots, X_{m-1}]^E$  of  $R[X_1, \dots, X_m]^E$  isomorphically onto the  $E$ -subring  $R[x_1, \dots, x_{m-1}]^E$  of  $R[x_1, \dots, x_m]^E$ .

Now use (1.6) and (3.2) to equip  $R[X_1, \dots, X_m]^E$  with the derivation  $D$  which is trivial on  $R[X_1, \dots, X_{m-1}]^E$  and satisfies  $D(X_m) = 1$  and  $D(E(p)) = r \cdot D(p) \cdot E(p)$  for all  $p \in R[X_1, \dots, X_m]^E$ .

A trivial induction on height ( $p$ ) gives:

$$(*) \widehat{D(p)} = d_m(\hat{p}).$$

Now we prove by induction on  $\text{ord}(p)$ , defined relative to  $R[X_1, \dots, X_{m-1}]^E$  as ground  $E$ -ring (see (1.9)), that  $p \neq 0 \Rightarrow \hat{p} \neq 0$ .

Suppose  $p \neq 0$  but  $\hat{p} = 0$ . According to (3.3) either  $\text{ord}(E(q) \cdot p) < \text{ord}(p)$ , some  $q$ , or  $\text{ord}(\widehat{D(p)}) < \text{ord}(p)$ .

In the first case  $\widehat{E(q) \cdot p} = \widehat{E(q)} \cdot \hat{p} = 0$  implies by the inductive assumption that  $E(q) \cdot p = 0$ , so  $p = 0$ , contradiction.

In the case that  $\text{ord} D(p) < \text{ord}(p)$  we use (\*) and get  $\widehat{D(p)} = d_m(\hat{p}) = d_m(0) = 0$ , and again the inductive assumption implies that  $D(p) = 0$ . Now (3.4) implies that this can only happen if  $p$  is in the ground ring, i.e.  $p \in R[X_1, \dots, X_{m-1}]^E$ . But then  $\hat{p} = 0$ ,  $p \neq 0$  contradicts the induction assumption on  $m$ .  $\square$

(4.2) COROLLARY. *The maps  $p \mapsto \hat{p}$  from  $\mathbf{R}[X_1, \dots, X_m]^E$  into  $\mathbf{R}[x_1, \dots, x_m]^E$  and from  $\mathbf{C}[X_1, \dots, X_m]^E$  into  $\mathbf{C}[x_1, \dots, x_m]^E$  are isomorphisms. Here exponentiation on  $\mathbf{R}$  can be taken as  $a^x$ , where  $a$  is a fixed positive real  $\neq 1$ , and exponentiation on  $\mathbf{C}$  as  $e^{rx}$ ,  $r$  a fixed complex number  $\neq 0$ .*

*Proof.* The hypothesis of the proposition is obviously satisfied by taking  $d_1, \dots, d_m$  as the partial derivatives  $\partial/\partial x_1, \dots, \partial/\partial x_m$  (and  $r = \log a$  for  $\mathbf{R}$ ).

(4.3) Dahn and Wolter drew my attention to the fact that it is a formal consequence of the axioms for ordered fields and the inequality  $e^x \geq 1 + x$  that the exponential map  $e^x$  on  $R$  satisfies the differential equation  $y' = y$ . Elaborating this a bit we get a real-algebraic version of the first part of (4.2):

(4.4) PROPOSITION. *Suppose  $R$  is an ordered  $E$ -field and its exponential map  $E$  satisfies  $E(x) \geq 1 + rx$  for a fixed nonzero  $r \in R$  and all  $x \in R$ . Then the map  $p \mapsto \hat{p}$  from  $R[X_1, \dots, X_m]^E$  into  $R[x_1, \dots, x_m]^E$  is an isomorphism.*

(4.5) Before proving this, let us state some general facts on functions defined on ordered fields. Given an ordered field  $F$  and a function  $f: F \rightarrow F$  we call  $f$  differentiable at  $a \in F$  with derivative  $b \in F$  if

$$\forall \varepsilon > 0 \exists \delta > 0 \forall h \left( 0 < |h| < \delta \Rightarrow \left| \frac{f(a+h) - f(a)}{h} - b \right| < \varepsilon \right)$$

holds in  $F$ . In that case  $b$  is unique and we write  $f'(a) = b$ . We have the usual rules: if  $f, g$  are differentiable at  $a$ , so are  $f + g$ ,  $cf$  ( $c \in F$ ), and  $fg$ , with  $(f + g)'(a) = f'(a) + g'(a)$ ,  $(cf)'(a) = c \cdot f'(a)$ ,  $(fg)'(a) = f'(a) \cdot g(a) + f(a) \cdot g'(a)$ . If  $f$  is differentiable at  $a$  and  $g$  is differentiable at  $f(a)$ , then  $g \circ f$  is differentiable at  $a$  and

$$(g \circ f)'(a) = g'(f(a)) \cdot f'(a).$$

Of course we can now also define partial differentiability w.r.t.  $x_i$  at a point  $a \in F^m$  for functions  $f: F^m \rightarrow F$ , and we write  $\partial f(a)/\partial x_i$  for this partial derivative.

Suppose now that  $E$  is an exponential operation on  $F$  satisfying  $E(x) \geq 1 + rx$  for a fixed  $r \in F$  and all  $x \in F$ . Then it is easy to derive that  $E$  is differentiable at 0 and  $E'(0) = r$ . (Use  $E(-h) = E(h)^{-1} \geq 1 - rh$  to get  $1 + rh \leq E(h) \leq (1 - rh)^{-1}$  for small  $|h|$ .) The morphism

property of  $E$  then gives that  $E$  is differentiable everywhere and  $E' = rE$ . It follows that  $F[x_1, \dots, x_m]^E$  is closed under  $\partial/\partial x_1, \dots, \partial/\partial x_m$  and that the hypothesis of (4.1) holds for  $R = (F, E)$  and  $d_i = \partial/\partial x_i, i = 1, \dots, m$ . (4.4) follows.

(4.6) REMARK. From a logician's point of view the theorems above have the following interpretation (for  $R$  satisfying the hypothesis of (4.1)): *each identity in the language of  $E$ -rings augmented by constants from  $R$  which holds in  $R$  is derivable from the theory of  $E$ -rings augmented by  $\text{Diagram}^+(R)$ .*

(4.7) *In the remainder of this section  $F$  is an ordered  $E$ -field whose exponential map satisfies*

$$E(x) \geq 1 + x, \quad \text{all } x \in F \text{ (e.g. } (\mathbf{R}, e^x)).$$

We are interested in the roots of  $E$ -polynomials  $p(X)$  in *one* variable  $X$  over  $F$ . By (4.4) it is harmless to identify such a  $p(X)$  with the function  $\hat{p}$  it defines, and we shall do so. Let us call  $a$  in  $F$  a root of multiplicity  $n$  ( $n > 0$ ) of  $p(X)$  if

$$p(a) = \dots = p^{(n-1)}(a) = 0, \quad p^{(n)}(a) \neq 0.$$

We shall prove that each root of a *nonzero*  $E$ -polynomial  $p(X)$  has a multiplicity. This may seem somewhat surprising as the usual proof for  $(\mathbf{R}, e^x)$  does not work for general  $F$ : for the reals one notes that  $p^{(i)}(a) = 0$  for all  $i$  means that the Taylor series for  $p$  at  $a$  has all coefficients 0, whence, by analytic continuation,  $p$  vanishes on  $\mathbf{R}$ , i.e.  $p = 0$ .

The following lemma leads to another proof.

(4.8) LEMMA. *Given a nonzero  $p(X)$  in  $F[X]^E$  there is a finite sequence  $p = p_0, p_1, \dots, p_M$  in  $F[X]^E$  such that:*

(a)  $p_M = cE(q)$  for some nonzero  $c \in F$  and some  $q$  in  $F[X]^E$ ,

(b) for each  $i < M$  we have  $p_{i+1} = (E(q_i) \cdot p_i)'$  for some  $q_i$  in  $F[X]^E$ , and  $\text{ord}(p_{i+1}) < \text{ord}(p_i)$ . Moreover, given such a sequence we have for each  $i \leq M$ :

(c)  $p_i = \alpha_{i,0}p + \alpha_{i,1}p^{(1)} + \dots + \alpha_{i,i}p^{(i)}$  for certain  $\alpha_{i,j}$  in  $F[X]^E$  and  $\alpha_{i,i} = E(\beta_{i,i})$  for some  $\beta_{i,i}$  in  $F[X]^E$ .

*Proof.* There certainly is a sequence  $p = p_0, p_1, \dots, p_N$  with  $p_N = 0$  and property (b) for  $i < N$ : just apply (3.3) and the fact that  $\omega^\omega$  is well ordered. Now  $0 = p_N = (E(\bar{q}) \cdot p_{N-1})'$  for some  $\bar{q}$ , so  $E(\bar{q}) \cdot p_{N-1}$  is a nonzero constant  $c \in F$ . (It can't be 0, as  $\text{ord}(p_{N-1}) > \text{ord}(p_N) = 0$ .) Hence  $p_{N-1} = c \cdot E(-\bar{q})$ . Now take  $M = N - 1$  to realize (a).

(c) is proved by induction on  $i$ . The case  $i = 0$  being trivial we assume that  $i < M$  and (c) holds. Then  $p_{i+1}$  is the derivative of  $E(q_i) \cdot (\alpha_{i,0}p + \alpha_{i,1}p^{(1)} + \dots + \alpha_{i,i}p^{(i)})$  which is a linear combination  $\alpha_{i+1,0}p + \alpha_{i+1,1}p^{(1)} + \dots + \alpha_{i+1,i+1}p^{(i+1)}$  where  $\alpha_{i+1,i+1} = E(q_i) \cdot \alpha_{i,i} = E(q_i + \beta_{i,i})$ .  $\square$

(4.9) COROLLARY. *Each root in  $F$  of a nonzero  $E$ -polynomial  $p(X)$  over  $F$  has a multiplicity  $\leq M$ , where  $M$  is as in (4.8).*

*Proof.* (4.8) part (c) applied to  $i = M$  gives: if  $p(a) = p^{(1)}(a) = \dots = p^{(M)}(a) = 0$ , then  $p_M(a) = 0$ ; but  $p_M$  has no zeros, by (a).  $\square$

(4.10) REMARK. A similar argument, involving also part (c) of (4.8), gives in fact that a root  $a$  of  $p(X)$  has multiplicity  $n \leq M$  if and only if  $p_i(a) = 0$  for  $i < n$ ,  $p_n(a) \neq 0$ . (Here  $p(X)$  and the sequence  $p_0, \dots, p_M$  are as described in (4.8).) So the  $p_i$ 's serve as a kind of derivatives of  $p$ .

(4.11) COROLLARY. *Suppose  $F$  has the extra property that each  $E$ -polynomial over  $F$  has a maximum value on each segment  $[a, b]$ . Then each nonzero  $E$ -polynomial  $p(X)$  over  $F$  has at most  $M$  roots in  $F$ , counted with their multiplicity, where  $M$  is as in (4.8).*

*Proof.* The hypothesis implies that Rolle's theorem holds for  $E$ -polynomials over  $F$ . That is, whenever  $p(a) = p(b) = 0$ ,  $a < b$ , there is  $c$  with  $a < c < b$  and  $p'(c) = 0$ : just take  $c$  where  $p$  is maximal or minimal on  $(a, b)$ .

Now let  $p(X)$  be nonzero and take a sequence  $p_0, p_1, \dots, p_M$  as in (4.8). We assume as an inductive hypothesis that the result is true for all  $q(X)$  with  $\text{ord}(q) < \text{ord}(p)$ . This means that  $p_1 = (E(q_0) \cdot p)'$  has at most  $M - 1$  zeros (assuming  $M > 0$ ; the case  $M = 0$  is trivial). Hence by Rolle's theorem and a simple counting argument the  $E$ -polynomial  $E(q_0) \cdot p$ , and therefore  $p$  itself, has at most  $M$  zeros.  $\square$

(4.12) Let us mention another result in this area which can be proved by the same induction method.

(\*) *For each nonzero  $E$ -polynomial  $p(X)$  over  $(\mathbf{R}, e^x)$ , all  $a, b \in \mathbf{R}$  with  $a < b$  and each ordered  $E$ -extension field  $F$  of  $(\mathbf{R}, e^x)$  we have: all roots of  $p(X)$  in  $F$  between  $a$  and  $b$  are in  $\mathbf{R}$ .*

Another version of this is:

(\*\*) *Let  $\text{Exp}_{\mathbf{R}}$  be the theory  $\text{Diag}(\mathbf{R}, e^x) \cup$  theory of ordered  $E$ -fields  $\cup \{\forall x E(x) \geq 1 + x\}$ . Then  $\text{Exp}_{\mathbf{R}}$  proves every true statement of the form: " $p(X)$  has exactly  $k$  roots in  $[a, b]$ " ( $p(X) \in \mathbf{R}[X]^E$ ,  $a, b \in \mathbf{R}$ ).*



(\*) follows easily by induction on  $\text{ord}(p)$ . An analysis of the proof shows that (\*), and therefore (\*\*), remain true if the ordered  $E$ -field  $(\mathbf{R}, e^x)$  is replaced by any ordered  $E$ -field with  $E(x) \geq 1 + x$  for all  $x$ , and satisfying Rolle's theorem and the intermediate value theorem for  $E$ -polynomials.

(4.13) An important problem seems to me whether in statement (\*) above the restriction to roots between given reals  $a, b$  can be omitted, while at the same time restricting the extensions  $F$  to those which satisfy a decent set of 1st order axioms.

This problem is related to, what Macintyre calls, the 'last root' problem for real  $E$ -polynomials: *consider non-zero real  $E$ -polynomials of "bounded complexity" (so in particular the number of real roots is bounded, by (4.11)). Is there an intelligible function of the (finitely many) real parameters on which the  $E$ -polynomial depends, which bounds the absolute value of its real roots?*

A positive answer to this question should remove one of the main obstacles in obtaining a satisfactory analysis of the elementary theory of  $(\mathbf{R}, e^x)$ .

**Acknowledgement.** I would like to thank Angus Macintyre, Ken Manders, and Alex Wilkie for many stimulating discussions on this subject at Yale University.

#### REFERENCES

- [C] G. E. Collins, *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition*, Automata Theory and Formal Language, 2nd G. I. Conference, Kaiserslautern, pp. 134–183, Berlin, Springer-Verlag, 1975.
- [D] L. van den Dries, *Analytic Hardy fields and exponential curves in the real plane*, Amer. J. Math., **106** (1984).
- [H] G. H. Hardy, *Orders of Infinity*, Cambridge, 1910.
- [M] A. Macintyre, *The Laws of Exponentiation*, Springer LNM 890, 185–197, 1981.
- [R] D. Richardson, *Solution of the identity problem for integral exponential functions*, Zeitschr. für Math. Logik und Grundl. der Math., **15** (1969), 333–340.

Received December 11, 1981. The author was partially supported by an NSF grant #MCS80-02717.

STANFORD UNIVERSITY  
STANFORD, CA 94305

# PACIFIC JOURNAL OF MATHEMATICS

## EDITORS

DONALD BABBITT (Managing Editor)  
University of California  
Los Angeles, CA 90024

HUGO ROSSI  
University of Utah  
Salt Lake City, UT 84112

C. C. MOORE and ARTHUR OGUS  
University of California  
Berkeley, CA 94720

J. DUGUNDJI  
Department of Mathematics  
University of Southern California  
Los Angeles, CA 90089-1113

R. FINN and H. SAMELSON  
Stanford University  
Stanford, CA 94305

## ASSOCIATE EDITORS

R. ARENS

E. F. BECKENBACH  
(1906–1982)

B. H. NEUMANN

F. WOLF

K. YOSHIDA

## SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA  
UNIVERSITY OF BRITISH COLUMBIA  
CALIFORNIA INSTITUTE OF TECHNOLOGY  
UNIVERSITY OF CALIFORNIA  
MONTANA STATE UNIVERSITY  
UNIVERSITY OF NEVADA, RENO  
NEW MEXICO STATE UNIVERSITY  
OREGON STATE UNIVERSITY

UNIVERSITY OF OREGON  
UNIVERSITY OF SOUTHERN CALIFORNIA  
STANFORD UNIVERSITY  
UNIVERSITY OF HAWAII  
UNIVERSITY OF TOKYO  
UNIVERSITY OF UTAH  
WASHINGTON STATE UNIVERSITY  
UNIVERSITY OF WASHINGTON

Flavio E. A. da Silveira, Rational homotopy theory of fibrations .....	1
Donald M. Davis, Desuspensions of stunted projective spaces .....	35
Lou van den Dries, Exponential rings, exponential polynomials and exponential functions .....	51
Fred Galvin and Samuel David Shore, Completeness in semimetric spaces .....	67
Fereidoun Ghahramani, Compact elements of weighted group algebras .....	77
Munehiko Itō, The closed image of a hereditary $M_1$ -space is $M_1$ .....	85
Elvira Laura Livorni, Classification of algebraic surfaces with sectional genus less than or equal to six. I. Rational surfaces .....	93
H. Alan MacLean, Riesz sets and a theorem of Bochner .....	115
E. Neher, Jordan triple systems with completely reducible derivation or structure algebras .....	137
Joe Repka, Shalika's germs for $p$ -adic $GL(n)$ . I. The leading term .....	165
Joe Repka, Shalika's germs for $p$ -adic $GL(n)$ . II. The subregular term .....	173
Rae Michael Andrew Shortt, Borel density, the marginal problem and isomorphism types of analytic sets .....	183
Baruch Solel, The multiplicity functions of invariant subspaces for nonselfadjoint crossed products .....	201
Su-wın Yang, Self-intersection number of immersions and enumeration of nonstable vector bundles .....	215
W. M. Zajączkowski, Local solvability of nonstationary leakage problem for ideal incompressible fluid. II .....	229