THE JOURNAL OF SYMBOLIC LOGIC
Volume 53, Number 2, June 1988

QUANTIFIER ELIMINATION IN SEPARABLY CLOSED FIELDS OF FINITE IMPERFECTNESS DEGREE

DAN HARAN

Introduction. The theory of separably closed fields of a fixed characteristic and a fixed imperfectness degree is clearly recursively axiomatizable. Ershov [1] showed that it is complete, and therefore decidable. Later it became clear that this theory also has the prime extension property in a suitable language (cf. [4, Proposition 1]); hence it admits quantifier elimination. The purpose of this work is to give an explicit, primitive recursive procedure for such quantifier elimination in the case of a finite imperfectness degree.

To be precise, the language Λ that we have in mind is the first order language of fields enriched with $(m+1)$-place function symbols λ_j^m, where $m = 0, 1, 2, \dots$ and $1 \leq j \leq p^m$. To interpret λ_j^m in a field M of characteristic p, consider the p-adic expansion $j_1 + j_2 p + \cdots + j_m p^{m-1}$ of $j - 1$, and for $x_1, \dots, x_m \in M$ let $\alpha_j(x_1, \dots, x_m) = x_1^{j_1} \cdots x_m^{j_m}$. If $x_1, \dots, x_m$ are p-independent and $y \in M$ is p-dependent on them, then $\alpha_1(x_1, \dots, x_m), \dots, \alpha_{p^m}(x_1, \dots, x_m)$ are linearly independent over M^p and y is linearly dependent on them. In this case there are unique $a_1, \dots, a_{p^m} \in M$ such that $y = \sum_j a_j^p \alpha_j(x_1, \dots, x_m)$; define $\lambda_j^m(x_1, \dots, x_m; y) = a_j$. Set $\lambda_j^m(x_1, \dots, x_m; y) = 0$ otherwise.

Denote by $\mathrm{SCF}(p, e)$ the theory of separably closed fields of characteristic p and finite imperfectness degree e, containing the above interpretation of the functions λ_j^m. We will prove:

MAIN THEOREM. *The theory* $\mathrm{SCF}(p,e)$ *allows primitive recursive quantifier elimination in* Λ *and is primitive recursively decidable.*

We intend to treat the case of infinite imperfectness degree in a subsequent paper; a unified treatment of both cases would involve many technical complications that can be avoided in the finite case.

The quantifier elimination procedure can be roughly described as follows: Given a well-formed formula in Λ, we first transform it into a form such that the variable to be eliminated represents roots of a separable polynomial over the field. Then we use the fact that our fields are separably closed, so we can eliminate one quantifier.

We do not attempt to find the "most effective" algorithm for the procedure in the Main Theorem; in fact, for the sake of clarity of the exposition we prefer to divide the

Received December 14, 1986; revised February 25, 1987.

0022-4812/88/5302-0012/$01.70

algorithm into smaller steps, even though this makes the procedure sometimes unnecessarily longer.

Acknowledgement. This note is based on research done in 1985/86 at Rutgers University, partly supported by the NSF. The author wishes to thank C. Wood and G. Cherlin for their interest and encouragement.

§1. Reduction of the problem. We fix a nonnegative integer e, write $N = p^e$, and introduce the following notation. Let L_0 denote the first order language of the theory of fields enriched with constants $t_1, \ldots, t_e$, and let L be L_0 enriched with N unary function symbols $\lambda_1, \ldots, \lambda_N$. Let $\alpha_1, \alpha_2, \ldots, \alpha_N$ be an enumeration of the monomials $t_1^{j_1} \cdots t_e^{j_e}$, where $0 \leq j_1, \ldots, j_e < p$, say, $\alpha_j = t_1^{j_1} \cdots t_e^{j_e}$, where $j_1 + j_2 p + \cdots + j_e p^{e-1}$ is the p-adic expansion of $j - 1$.

A field M of characteristic p and imperfectness degree e together with a p-basis is a structure in L_0 and L in the following way. The constants $t_1, \ldots, t_e$ are interpreted as elements of the given p-basis (so that $\alpha_1, \alpha_2, \ldots, \alpha_N$ correspond to a linear basis of M over M^p), and $\lambda_1, \ldots, \lambda_N \colon M \to M$ are implicitly defined by $a = (\lambda_1(a))^p \alpha_1 + \cdots + (\lambda_N(a))^p \alpha_N$, for every $a \in M$.

Let T denote the theory of separably closed fields of characteristic p and imperfectness degree e in L. (In particular, T includes the axioms defining the functions $\lambda_1, \ldots, \lambda_N$ in the above manner.)

The following lemma serves as a "flow chart" for our algorithms. It lists various "subroutines" and shows how the main algorithm is composed from them.

Let $\boldsymbol{X} = (X_1, \ldots, X_m)$ and $\boldsymbol{Y} = (Y_1, \ldots, Y_n)$ be blocks ($=$ finite sequences) of variables. In §2 we will define when a quantifier-free formula $\psi(\boldsymbol{X}, \boldsymbol{Y})$ in L_0 is *pre-separable in* $\boldsymbol{Y}$ and assign to such a formula an integer $l \geq -1$, the *level* of ψ. With the aid of this notion (the precise definition is immaterial at this stage) we can give the layout for our procedure.

(REDUCTION) LEMMA 1.1. *Given a quantifier-free formula $\psi(\boldsymbol{X}, \boldsymbol{Y})$ in L_0, assume that we can do the following procedures in a primitive recursive way*:

(a) *Find an integer $l \geq -1$ and a formula $\psi'(\boldsymbol{X}, \boldsymbol{Y})$ pre-separable in $\boldsymbol{Y}$ at level l such that*

$$(\exists Y_1, \ldots, \exists Y_n)\psi(\boldsymbol{X}, \boldsymbol{Y}) \equiv_T (\exists Y_1, \ldots, \exists Y_n)\psi'(\boldsymbol{X}, \boldsymbol{Y}).$$

(b) *If ψ is pre-separable in $\boldsymbol{Y}$ at level* 0 *or* -1, *find a quantifier-free formula $\psi'(\boldsymbol{X}, Y_1, \ldots, Y_{n-1})$ in L_0 such that*

$$(\exists Y_n)\psi(\boldsymbol{X}, \boldsymbol{Y}) \equiv_T \psi'(\boldsymbol{X}, Y_1, \ldots, Y_{n-1}).$$

(c) *If ψ is pre-separable in $\boldsymbol{Y}$ at level $l \geq 1$, let $\boldsymbol{Z}$ be a block of variables of length $m \times N$, and find a formula $\psi'(\boldsymbol{Z}, \boldsymbol{Y})$ in L_0 pre-separable in $\boldsymbol{Y}$ at level $l - 1$ such that*

$$\psi(\boldsymbol{X}, \boldsymbol{Y}) \equiv_T \psi'(\lambda_1(X_1), \ldots, \lambda_N(X_1), \ldots, \lambda_1(X_m), \ldots, \lambda_N(X_m), \boldsymbol{Y}).$$

Then we can find in a primitive recursive way a quantifier-free formula $\psi'(\boldsymbol{X})$ in L such that

$$(\exists Y_1, \ldots, \exists Y_n)\psi(\boldsymbol{X}, \boldsymbol{Y}) \equiv_T \psi'(\boldsymbol{X}).$$

PROOF. By (a) we may assume that ψ is pre-separable in $\boldsymbol{Y}$, say at level l. By induction, using (c), we may find for every $0 \leq k \leq l$ a formula $\psi_k(\boldsymbol{U}, \boldsymbol{Y})$ pre-separable in $\boldsymbol{Y}$ at level k such that $\psi(\boldsymbol{X}, \boldsymbol{Y}) \equiv_T \psi_k(\boldsymbol{u}, \boldsymbol{Y})$, where $\boldsymbol{U}$ is a block of variables and $\boldsymbol{u}$ is a block (of the same length) of terms in L constructed from the variables $X_1, \dots, X_m$ and the function symbols in L. Therefore we may assume that $l \leq 0$; by (b) we may eliminate Y_n.

Applying this argument, we may inductively find for every $0 \leq j \leq n$ a quantifier-free formula $\varphi_j(\boldsymbol{V}_j, Y_1, \dots, Y_j)$ in L_0 such that

$$(\exists Y_1, \dots, \exists Y_n)\psi(\boldsymbol{X}, \boldsymbol{Y}) \equiv_T (\exists Y_1, \dots, \exists Y_j)\varphi_j(\boldsymbol{v}, \boldsymbol{Y}),$$

where $\boldsymbol{V}_j$ is a block of variables, and $\boldsymbol{v}_j$ is a block (of the same length) of terms in L constructed from the variables $X_1, \dots, X_m$ and the function symbols in L. If $j = 0$, this gives the desired formula. //

Note that the formula $\lambda_j(V) = U$ is equivalent modulo T to

$$(\exists V_1, \dots, \exists V_N)(V_1^p \alpha_1 + \cdots + V_N^p \alpha_N = V \wedge V_j = U),$$

and $\lambda_j(V) \neq U$ is equivalent to

$$(\exists V_1, \dots, \exists V_N)(V_1^p \alpha_1 + \cdots + V_N^p \alpha_N = V \wedge V_j \neq U).$$

Therefore, if $\psi(\boldsymbol{X}, \boldsymbol{Y})$ is a quantifier-free formula in L we can find a block $\boldsymbol{Y}' = (Y_1', \dots, Y_k')$ and a quantifier-free formula $\psi'(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Y}')$ in L_0 such that

$$(\exists Y_1, \dots, \exists Y_n)\psi(\boldsymbol{X}, \boldsymbol{Y}) \equiv_T (\exists Y_1, \dots, \exists Y_n, \exists Y_1', \dots, \exists Y_k')\psi'(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Y}').$$

Thus if conditions (a)–(c) of the lemma are satisfied (as we show in §§2 and 3), we obtain:

THEOREM 1.2. *The theory T of separably closed fields of characteristic p and finite imperfectness degree e in L allows primitive recursive quantifier elimination and is primitive recursively decidable.*

The second assertion of Theorem 1.2 is an easy consequence of the following observation:

REMARK 1.3. If $t_1, \dots, t_e$ are p-independent elements in a field of characteristic p, then they are algebraically independent over $\mathbf{F}_p$.

The Main Theorem immediately follows from Theorem 1.2. To see this, consider the set of axioms $S = T \cup \mathrm{SCF}(p, e)$ in the language $\Lambda \cup L$. Interpreting the functions λ_j^m according to their definition in $\mathrm{SCF}(p, e)$, we can find for every formula φ_1 in Λ a formula φ_2 in the language of fields, equivalent to φ_1 modulo $\mathrm{SCF}(p, e)$, and hence also modulo S. By Theorem 1.2 we can find a quantifier-free formula $\varphi_3(\boldsymbol{X})$ in L equivalent to φ_2 modulo T, and hence also modulo S. Now $\varphi_3(\boldsymbol{X})$ is equivalent modulo S to

$$\varphi = [\lambda_1^e(T_1, \dots, T_e, 1) = 1] \wedge \varphi_3'(\boldsymbol{X}),$$

where $\varphi_3'(\boldsymbol{X})$ is obtained from $\varphi_3(\boldsymbol{X})$ by replacing $t_1, \dots, t_e$ by the variables $T_1, \dots, T_e$, and all terms of the form $\lambda_j(u)$ by $\lambda_j^e(T_1, \dots, T_e, u)$, for $1 \leq j \leq p^e$. (Note that $t_1, \dots, t_e$ are p-independent elements in a field M if and only if $M \models \lambda_1^e(t_1, \dots, t_e, 1) = 1$.) Thus $\varphi_1 \equiv \varphi$ modulo $\mathrm{SCF}(p, e)$.

§2. Elimination. Let $R = \mathbf{F}_p[t_1, \ldots, t_e]$ be the ring of polynomials and $E = \mathbf{F}_p(t_1, \ldots, t_e)$ the field of rational functions in $t_1, \ldots, t_e$ over the prime field $\mathbf{F}_p$. Since $t_1, \ldots, t_e$ are assumed to be p-independent elements in a field of characteristic p, they are algebraically independent over $\mathbf{F}_p$.

Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be tuples of variables, $\boldsymbol{Y} = (Y_1, \ldots, Y_n)$, and let q be an integer. For $h(\boldsymbol{X}, \boldsymbol{Y}) \in E[\boldsymbol{X}, \boldsymbol{Y}]$ we shall abbreviate $h(\boldsymbol{X}, Y_1^q, \ldots, Y_n^q)$ by $h(\boldsymbol{X}, \boldsymbol{Y}^q)$.

Consider the formula

$$(1) \qquad f_1(\boldsymbol{X}, \boldsymbol{Y}) = 0 \wedge \cdots \wedge f_r(\boldsymbol{X}, \boldsymbol{Y}) = 0 \wedge g_1(\boldsymbol{X}, \boldsymbol{Y}) \neq 0 \wedge \cdots \wedge g_s(\boldsymbol{X}, \boldsymbol{Y}) \neq 0,$$

where $f_1, \ldots f_r, g_1, \ldots, g_s \in R[\boldsymbol{X}, \boldsymbol{Y}]$, and $r, s \geq 1$.

DEFINITION 2.1. Let l be a nonnegative integer. Formula (1) is *pre-separable* in $\boldsymbol{Y}$ (*at level* l) if there is a polynomial $h(\boldsymbol{X}, \boldsymbol{Y}) \in R[\boldsymbol{X}, \boldsymbol{Y}]$ separable in Y_n such that $f_1(\boldsymbol{X}, \boldsymbol{Y}) = h(\boldsymbol{X}, \boldsymbol{Y}^{p^l})$ and $(\partial h / \partial Y_n)(\boldsymbol{X}, \boldsymbol{Y}^{p^l}) = g_1(\boldsymbol{X}, \boldsymbol{Y})$.

Furthermore, (1) is *pre-separable* in $\boldsymbol{Y}$ *at level* -1 if Y_n does not appear in $f_1, \ldots, f_r$.

A quantifier-free formula $\varphi(\boldsymbol{X}, \boldsymbol{Y})$ is *pre-separable* (*at level* l) in $\boldsymbol{Y}$ if it is a disjunction of pre-separable formulas $\varphi_1, \ldots, \varphi_k$ in $\boldsymbol{Y}$ of the form (1) at levels $l_1, \ldots, l_k$, respectively, and $l = \max(l_1, \ldots, l_k)$.

We call a quantifier-free formula *separable* in $\boldsymbol{Y}$ if it is pre-separable in $\boldsymbol{Y}$ at level ≤ 0.

(ELIMINATION) LEMMA 2.2. *Let $\psi(\boldsymbol{X}, \boldsymbol{Y})$ be a formula separable in $\boldsymbol{Y}$ and let $\psi'(\boldsymbol{X}, Y_1, \ldots, Y_{n-1})$ be a quantifier-free formula in L_0 such that*

$$(2) \qquad (\exists Y_n)\psi(\boldsymbol{X}, \boldsymbol{Y}) \equiv \psi'(\boldsymbol{X}, Y_1, \ldots, Y_{n-1})$$

modulo the theory of algebraically closed fields containing E. Then (2) *is true also modulo T.*

PROOF. Without loss of generality ψ is of the form (1). Let M be a separably closed field containing E and let $\boldsymbol{x}$ and $(y_1, \ldots, y_{n-1})$ be tuples of elements of M such that $\tilde{M} = \psi'(\boldsymbol{x}, y_1, \ldots, y_{n-1})$.

If Y_n does not appear in $f_1, \ldots, f_r$, then $f_i(\boldsymbol{x}, y_1, \ldots, y_{n-1}) = 0$, for $i = 1, \ldots, r$ and $g_j(\boldsymbol{x}, y_1, \ldots, y_{n-1}, Y_n) \neq 0$, for $j = 1, \ldots, s$. As M is infinite, there is $y_n \in M$ such that $g_j(\boldsymbol{x}, y_1, \ldots, y_{n-1}, y_n) \neq 0$, for $j = 1, \ldots, s$. Thus $M \models \psi(\boldsymbol{x}, \boldsymbol{y})$.

If (1) is pre-separable in $\boldsymbol{Y}$ at level 0 then by the definition of ψ' there is y_n in the algebraic closure $\tilde{M}$ of M such that $\tilde{M} \models \psi(\boldsymbol{x}, \boldsymbol{y})$, where $\boldsymbol{y} = (y_1, \ldots, y_{n-1}, y_n)$. But $f_1(\boldsymbol{x}, \boldsymbol{y}) = 0$ and $(\partial f_1 / \partial Y_n)(\boldsymbol{x}, \boldsymbol{y}) = g_1(\boldsymbol{x}, \boldsymbol{y}) \neq 0$, so y_n is separable over M, whence $y_n \in M$. Thus $M \models \psi(\boldsymbol{x}, \boldsymbol{y})$. //

It is well known that the theory of algebraically closed fields containing E allows a primitive recursive quantifier elimination in L_0 [3, 8.3]; thus we can find for a given ψ the formula ψ' in Lemma 2.2 in a primitive recursive way. This gives condition (b) of Lemma 1.1.

Our attempt to write quantifier-free formulas as separable formulas leads us first to condition (a) of Lemma 1.1:

(STRATIFICATION) LEMMA 2.3. *Let $\varphi(\boldsymbol{X}, \boldsymbol{Y})$ be a quantifier-free formula in L_0. Then we can find an integer $l \geq -1$ and a formula $\varphi'(\boldsymbol{X}, \boldsymbol{Y})$ pre-separable in $\boldsymbol{Y}$ at level l such that*

$$(\exists Y_1, \ldots, \exists Y_n)\varphi(\boldsymbol{X}, \boldsymbol{Y}) \equiv_T (\exists Y_1, \ldots, \exists Y_n)\varphi'(\boldsymbol{X}, \boldsymbol{Y}).$$

PROOF. By [2, Lemma 2.14], φ can be effectively written as a disjunction of formulas describing *basic* sets, i.e., conjunctions of the form (1) with $s = 1$ such that the affine variety V defined over E by $f_1, \dots, f_r$ is irreducible over E and g_1 does not vanish on V. Considering each disjunct separately, we may assume that φ represents such a basic set.

Let $(\mathbf{x}, y_1, \dots, y_n)$ be a generic point of V over E, and denote $F = E(\mathbf{x})$. We may assume that $y_1, \dots, y_n$ are algebraically dependent over F (otherwise φ is pre-separable in $\mathbf{Y}$ at level -1).

It suffices to find a polynomial $f(\mathbf{X}, \mathbf{Y}) \in R[\mathbf{X}, \mathbf{Y}]$ that vanishes on V, but $f(\mathbf{X}, \mathbf{Y}) = h(\mathbf{X}, \mathbf{Y}^{p^l})$, where $h(\mathbf{X}, \mathbf{Y}) \in R[\mathbf{X}, \mathbf{Y}]$ and $(\partial h/\partial Y_k)(\mathbf{X}, \mathbf{Y}^{p^l})$ does not vanish on V, for some $1 \le k \le n$ (so, in particular, $h(\mathbf{X}, \mathbf{Y})$ is separable in Y_k). Indeed, φ is then equivalent modulo the theory of fields to $\varphi_1 \vee \varphi_2$, where φ_1 is

$$f(\mathbf{X}, \mathbf{Y}) = 0 \wedge f_1(\mathbf{X}, \mathbf{Y}) = 0 \wedge \cdots \wedge f_r(\mathbf{X}, \mathbf{Y}) = 0$$
$$\wedge \frac{\partial h}{\partial Y_k}(\mathbf{X}, \mathbf{Y}^{p^l}) \neq 0 \wedge g_1(\mathbf{X}, \mathbf{Y}) \neq 0$$

and φ_2 is

$$\frac{\partial h}{\partial Y_k}(\mathbf{X}, \mathbf{Y}^{p^l}) = 0 \wedge f_1(\mathbf{X}, \mathbf{Y}) = 0 \wedge \cdots \wedge f_r(\mathbf{X}, \mathbf{Y}) = 0 \wedge g_1(\mathbf{X}, \mathbf{Y}) \neq 0.$$

Thus, abbreviating $(\exists Y_1, \dots, \exists Y_n)$ by $(\exists \mathbf{Y})$,

$$(\exists \mathbf{Y})\varphi(\mathbf{X}, \mathbf{Y}) \equiv_T (\exists \mathbf{Y})\varphi_1(\mathbf{X}, \mathbf{Y}) \vee (\exists \mathbf{Y})\varphi_2(\mathbf{X}, \mathbf{Y}) \equiv_T (\exists \mathbf{Y})\varphi'_1(\mathbf{X}, \mathbf{Y}) \vee (\exists \mathbf{Y})\varphi_2(\mathbf{X}, \mathbf{Y}),$$

where φ'_1 is the formula obtained from φ_1 by transposing Y_k and Y_n. Clearly φ'_1 is pre-separable in $\mathbf{Y}$ at level l, and φ_2 can be effectively written as a disjunction of formulas representing basic sets of dimension strictly smaller than dim V. Thus the lemma will follow by induction on the dimension on V.

To find f as above, choose a minimal nonempty subset of $\{y_1, \dots, y_n\}$ algebraically dependent over F, say (to simplify the notation) $\{y_1, \dots, y_d\}$. Find $f \in R[\mathbf{X}, Y_1, \dots, Y_d]$ such that $f(\mathbf{x}, y_1, \dots, y_d) = 0$ (e.g., let $f(\mathbf{x}, y_1, \dots, y_{d-1}, Y_d)$ be an irreducible polynomial (not necessarily monic) of y_d over $F(y_1, \dots, y_{d-1})$). Without loss of generality $f(\mathbf{x}, \mathbf{Y})$ is irreducible in $F[\mathbf{Y}]$—otherwise replace it by an appropriate factor. Let $1 \le k \le d$; by Gauss' lemma (cf. [5, p. 128]) $f(\mathbf{x}, \mathbf{Y})$ is irreducible within $F(Y_1, \dots, Y_{k-1}, Y_{k+1}, \dots, Y_d)[Y_k]$, and therefore $f(\mathbf{x}, y_1, \dots, y_{k-1}, Y_k, y_{k+1}, \dots, y_d)$ is an irreducible polynomial of y_k over $F(y_1, \dots, y_{k-1}, y_{k+1}, \dots, y_d)$.

Now find the largest power q of p such that $f \in R[\mathbf{X}, \mathbf{Y}^q]$, and write $f(\mathbf{X}, \mathbf{Y}) = h(\mathbf{X}, \mathbf{Y}^q)$ with $h \in R[\mathbf{X}, \mathbf{Y}]$. Then there is $1 \le k \le d$ and a monomial P of $h(\mathbf{X}, \mathbf{Y})$ such that $p \nmid \deg_{Y_k} P$. Thus $(\partial h/\partial Y_k)(\mathbf{X}, \mathbf{Y}) \neq 0$. But $(\partial h/\partial Y_k)(\mathbf{X}, \mathbf{Y}^q)$ is of smaller degree in Y_k than $f(\mathbf{X}, \mathbf{Y}) = h(\mathbf{X}, \mathbf{Y}^q)$, and hence $(\partial h/\partial Y_k)(\mathbf{x}, \mathbf{y}^q) \neq 0$. //

§3. Substitution. We need some notation.

Let $\mathbf{V}$ be a block of variables over the field $E = \mathbf{F}_p(t_1, \dots, t_e)$. Then the basis $\alpha_1, \alpha_2, \dots, \alpha_N$ of R over R^p (see §1) is also a basis of the module $R[\mathbf{V}^p]$ over the ring $R^p[\mathbf{V}^p] = (R[\mathbf{V}])^p$. Let $\Lambda_1, \dots, \Lambda_N$: $R[\mathbf{V}^p] \to R[\mathbf{V}]$ be the maps defined by

$$h = (\Lambda_1(h))^p \alpha_1 + \cdots + (\Lambda_N(h))^p \alpha_N, \quad \text{where } h \in R[\mathbf{V}^p].$$

(It will be clear from the context which block of variables $\Lambda_1, \ldots, \Lambda_N$ are associated with.) If $M \models T$ and $a_1, a_2, \ldots \in M$ then $(\Lambda_j(h))(a) = \lambda_j(h(a))$; thus $h(a) = 0$ if and only if $(\Lambda_j(h))(a) = \lambda_j(h(a)) = 0$, $j = 1, \ldots, N$. In other words,

$$(3) \qquad h(V) = 0 \equiv_T \Lambda_1(h(V)) = 0 \wedge \cdots \wedge \Lambda_N(h(V)) = 0 \equiv_T \bigwedge_{j \in J} \Lambda_j(h(V)) = 0,$$

We consider the R-homomorphism $\rho: R[X, Y] \to R[Z^p, Y]$, where $X = (X_1, \ldots, X_m)$, $Y = (Y_1, \ldots, Y_n)$, $Z = (Z_{ij} \mid i = 1, \ldots, m, j = 1, \ldots, N)$, given by the substitutions $X_i = \sum_{j=1}^N Z_{ij}^p \alpha_j$, $i = 1, \ldots, m$, i.e. by

$$\rho(h(X, Y)) = h\left(\sum_{j=1}^N Z_{1j}^p \alpha_j, \ldots, \sum_{j=1}^N Z_{mj}^p \alpha_j, Y_1, \ldots, Y_n \right).$$

Furthermore, let $\partial: R[X, Y] \to R[X, Y]$ and $\partial: R[Z, Y] \to R[Z, Y]$ denote the differentiation with respect to Y_n, and $\pi: R[X, Y] \to R[X, Y^p]$ and $\pi: R[Z, Y] \to R[Z, Y^p]$ the substitution of $(Y_1^p, \ldots, Y_n^p)$ for $(Y_1, \ldots, Y_n)$.

LEMMA 3.1. (a) *The maps $\Lambda_1, \ldots, \Lambda_n$, ∂, ρ and π are additive; moreover, ρ and π are ring-homomorphisms.*

(b) *$\rho \circ \partial = \partial \circ \rho$ and $\rho \circ \pi = \pi \circ \rho$.*

(c) *$\pi \circ \Lambda_j = \Lambda_j \circ \pi$ on $R[Z^p, Y^p]$.*

(d) *$\partial \circ \Lambda_j \circ \pi = \Lambda_j \circ \pi \circ \partial$ (either as maps from $R[X^p, Y]$ to $R[X, Y]$ or as maps from $R[Z^p, Y]$ to $R[Z, Y]$).*

(e) *If $l \geq 1$ then $\Lambda_j \circ \rho \circ \pi^l = \pi^{l-1} \circ \Lambda_j \circ \rho \circ \pi$.*

(f) *If $l \geq 1$ then $\pi^{l-1} \circ \partial \circ \Lambda_j \circ \rho \circ \pi = \Lambda_j \circ \rho \circ \pi^l \circ \partial$.*

PROOF. (a) is trivial; the equalities of (b), (c) and (d) are easily checked on monomials with coefficients in R, which suffices by (a).

(e) Note that $\rho \circ \pi(R[X, Y]) \subseteq R[Z^p, Y^p]$. Therefore by (c) and (b)

$$\pi^{l-1} \circ \Lambda_j \circ \rho \circ \pi = \Lambda_j \circ \pi^{l-1} \circ \rho \circ \pi = \Lambda_j \circ \rho \circ \pi^{l-1} \circ \pi = \Lambda_j \circ \rho \circ \pi^l.$$

(f) Note that $\pi \circ \partial \circ \rho(R[X, Y]) \subseteq R[Z^p, Y^p]$. Thus

$$\begin{aligned} \pi^{l-1} \circ \partial \circ \Lambda_j \circ \rho \circ \pi &= \pi^{l-1} \circ (\partial \circ \Lambda_j \circ \pi) \circ \rho && \text{(by 3.1(b))} \\ &= \pi^{l-1} \circ \Lambda_j \circ \pi \circ \partial \circ \rho && \text{(by 3.1(d))} \\ &= \Lambda_j \circ \pi^{l-1} \circ \pi \circ \partial \circ \rho && \text{(by 3.1(c))} \\ &= \Lambda_j \circ \rho \circ \pi^l \circ \partial && \text{(by 3.1(b)).} \quad // \end{aligned}$$

Extend the map ρ to quantifier-free formulas: if φ is a quantifier-free formula in the blocks of variables X, Y, let $\rho(\varphi)$ be the formula in the blocks of variables Z, Y obtained from φ by the substitution of $\sum_{j=1}^N Z_{ij}^p \alpha_j$ for X_i, $i = 1, \ldots, m$, i.e., by replacing each atomic subformula $h(X, Y) = 0$ by $\rho(h)(Z, Y) = 0$.

PROPOSITION 3.2. *Let $\varphi(X, Y)$ be a formula pre-separable in Y at level l.*

(a) *If $\varphi(X, Y)$ is separable in Y then so is $\rho(\varphi)(Z, Y)$.*

(b) *If $l \geq 1$ then we can effectively find a formula $\psi(Z, Y)$ pre-separable in Y at level $< l$ such that $\rho(\varphi)(Z, Y) \equiv_T \psi(Z, Y)$. In particular,*

$$\varphi(X_1, \ldots, X_m, Y) \equiv_T \psi(\lambda_1(X_1), \ldots, \lambda_N(X_1), \ldots, \lambda_1(X_m), \ldots, \lambda_N(X_m), Y).$$

PROOF. Without loss of generality φ is of the form (1).

(a) If Y_n does not appear in $f_1, \dots, f_r$ then it does not appear in $\rho(f_1), \dots, \rho(f_r)$. If $\partial(f_1) = g_1 \neq 0$ (i.e., φ is pre-separable in $\boldsymbol{Y}$ at level 0) then $\partial \circ \rho(f_1) = \rho(g_1) \neq 0$, by Lemma 3.1(b). Thus $\rho(\varphi)$ is separable in Y in both cases.

(b) By (3) we have $\rho(\varphi)(\boldsymbol{Z}, \boldsymbol{Y}) \equiv_T \bigvee_{j \in J} \psi_j(\boldsymbol{Z}, \boldsymbol{Y})$, where $\psi_j(\boldsymbol{Z}, \boldsymbol{Y})$ is

$$\Lambda_j \circ \rho(f_1) = 0 \wedge \rho(f_1) = 0 \wedge \cdots \wedge \rho(f_r) = 0$$
$$\wedge\ \Lambda_j \circ \rho(g_1) \neq 0 \wedge \rho(g_1) \neq 0 \wedge \cdots \wedge \rho(g_s) \neq 0$$

and $J = \{1 \leq j \leq N \mid \Lambda_j \circ \rho(g_1) \neq 0\}$. We claim that ψ_j is pre-separable in $\boldsymbol{Y}$ at level $l - 1$ for every $j \in J$.

By assumption there is $h \in E[\boldsymbol{X}, \boldsymbol{Y}]$ separable in Y_n such that

$$f_1(\boldsymbol{X}, \boldsymbol{Y}) = h(\boldsymbol{X}, \boldsymbol{Y}^{p^l}) \quad \text{and} \quad (\partial h/\partial Y_n)(\boldsymbol{X}, \boldsymbol{Y}^{p^l}) = g_1(\boldsymbol{X}, \boldsymbol{Y}).$$

In our notation this can be written as

$$f_1 = \pi^l(h) \quad \text{and} \quad \pi^l \circ \partial(h) = g_1. \tag{4}$$

Denote $H(\boldsymbol{Z}, \boldsymbol{Y}) = \Lambda_j \circ \rho \circ \pi(h)$. By Lemma 3.1(e) and (f),

$$\Lambda_j \circ \rho(f_1) = \pi^{l-1}(\Lambda_j \circ \rho \circ \pi(h)) = \pi^{l-1}(H)$$

and

$$\pi^{l-1} \circ \partial(H) = \pi^{l-1} \circ \partial \circ \Lambda_j \circ \rho \circ \pi(h) = \Lambda_j \circ \rho(g_1).$$

In particular $\partial(H) \neq 0$, since $\Lambda_j \circ \rho(g_1) \neq 0$, i.e., H is separable in Y_n. Thus ψ_j is separable in $\boldsymbol{Y}$ at level $l - 1$.

The last assertion of (b) immediately follows from the definitions of ρ and $\lambda_1, \dots, \lambda_N$. //

Thus condition (d) of Lemma 1.1 has been verified, which completes the proof of Theorem 1.2.

REFERENCES

[1] Yu. L. Ershov, *Fields with solvable theory*, ***Soviet Mathematics Doklady***, 8 (1967), pp. 575–576.

[2] M. Fried, D. Haran and M. Jarden, *Galois stratification over Frobenius fields*, ***Advances in Mathematics***, vol. 51 (1984), pp. 1–35.

[3] M. Fried and M. Jarden, ***Field arithmetics***, Springer-Verlag, Berlin, 1986.

[4] G. Srour, *The independence relation in separably closed fields*, this Journal, vol. 51 (1986), pp. 715–725.

[5] S. Lang, ***Algebra***, 2nd ed., Addison-Wesley, Reading, Massachusetts, 1984.

SCHOOL OF MATHEMATICAL SCIENCES
RAYMOND AND BEVERLY SACKLER FACULTY OF EXACT SCIENCES
TEL-AVIV UNIVERSITY
RAMAT-AVIV, TEL-AVIV, ISRAEL