TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 344, Number 1, July 1994

GROUPS AND FIELDS INTERPRETABLE IN SEPARABLY CLOSED FIELDS

MARGIT MESSMER

ABSTRACT. We prove that any infinite group interpretable in a separably closed field F of finite Eršov-invariant is definably isomorphic to an F-algebraic group. Using this result we show that any infinite field K interpretable in a separably closed field F is itself separably closed; in particular, in the finite invariant case K is definably isomorphic to a finite extension of F.

This paper answers a question raised by D. Marker, whose help and guidance made this work possible. I would like to thank A. Pillay for helpful discussions, and E. Hrushovski for pointing out mistakes in the first version of this paper.

1. INTRODUCTION

It is well known in model theory that any infinite superstable field is algebraically closed, by results of A. Macintyre [10], G. Cherlin and S. Shelah [4]. Separably closed fields are the only other known stable fields. Furthermore, by results of A. Weil, E. Hrushovski, and L. van den Dries (see [17, 15, 16, 2]), we know that any infinite group interpretable in an algebraically closed field is definably isomorphic to an algebraic group, and any infinite field interpretable in an algebraically closed field K is definably isomorphic to K. So the main two theorems of this paper (2.6 and 3.6) are analogues of these results in the setting of separably closed fields. Moreover, since all structures interpretable in a stable theory are also stable, result 3.6 supports the open conjecture that all stable fields are separably closed.

We assume some knowledge about the model theory of separably closed fields as developed in [18, 7, 14 and 5], and familiarity with some basic concepts of linear algebraic groups, see [8 and 1].

A field F is said to be *separably closed* if it has no proper separable algebraic extension. We fix the characteristic to be $p \neq 0$ for all fields under discussion. (Note: A field of characteristic 0 is separably closed iff it is algebraically closed.) For the subfield F^p of all pth powers the index $[F : F^p]$ is either infinite or p^e for some $e < \omega$; we say that *Eršov-invariant* (or degree of imperfection) of F is infinite or e, accordingly, and call SCF_e the theory of separably closed fields (of characteristic p) of invariant e $(e \in \omega \cup \{\infty\})$. (Note: $\mathrm{SCF}_0 =$ the theory of algebraically closed fields.) SCF_e is complete, (see [7]), and stable (see [18]).

Received by the editors January 14, 1992 and, in revised form, August 7, 1993.
1991 *Mathematics Subject Classification.* Primary 03C60; Secondary 12L12.
This work has appeared in the author's Ph.D. thesis at the University of Illinois at Chicago.

0002-9947/94 $1.00 + $.25 per page

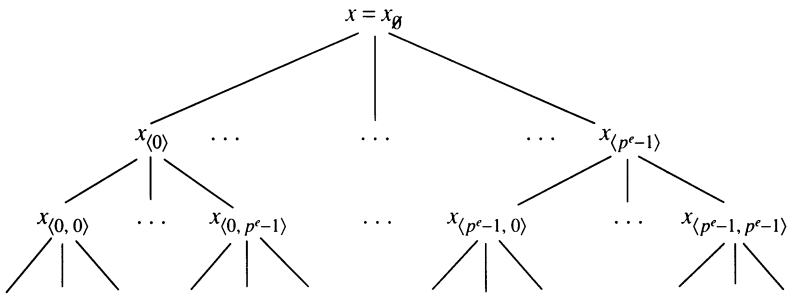

FIGURE 1

Up to §4 we fix $1 \leq e < \omega$, a monster model $\mathscr{M}$ of SCF_e and $F \prec \mathscr{M}$. We expand the language of fields as follows:

A set $\{a_1, \ldots, a_e\} \subset F$ is called a *p-basis* of F if the set of p-monomials $\{\prod_{i=1}^e a_i^{n_i} : 0 \leq n_i < p\} = \{m_0 = 1, m_1, \ldots, m_{p^e-1}\}$ forms a vector space basis for F over F^p. We work in the first-order language $\mathscr{L} = \{+, -, \cdot, ^{-1}, 0, 1\} \cup \{a_1, \ldots, a_e\} \cup \{\lambda_\sigma : \sigma \in (p^e)^{<\omega}\}$, where $a_1, \ldots, a_e$ are names for a fixed p-basis and λ_σ are unary function symbols interpreted as follows:

$$\lambda_{\langle j\rangle}(x) = x_{\langle j\rangle} \quad \text{for } j \in \{0, \ldots, p^e - 1\} \text{ iff } x = \sum_{j=0}^{p^e-1} x_{\langle j\rangle}^p m_j.$$

For $\sigma \in (p^e)^{<\omega}$: $\lambda_{\sigma^\frown\langle j\rangle}(x) = \lambda_{\langle j\rangle}(\lambda_\sigma(x)) = x_{\sigma^\frown\langle j\rangle}$ $[\lambda_\emptyset(x) = x_\emptyset = x]$, i.e., to $x \in F$ there is associated a tree as in Figure 1.

Note:

- All λ_σ are definable in the field language together with $a_1, \ldots, a_e$.
- $x_\sigma = \sum_{j=0}^{p^e-1} x_{\sigma^\frown\langle j\rangle}^p m_j$; in particular x is interdefinable with the elements of any one level of its tree.
- For $F \models \mathrm{SCF}_e$ and $X \subset \mathscr{M}$ define $F\langle X\rangle = F(x_\sigma : x \in X, \sigma \in (p^e)^{<\omega})$. It is easy to see that $F\langle X\rangle$ is closed under the λ_σ-functions. Therefore, by [14, Proposition 1] or [5, pp. 23–24], the separable closure of $F\langle X\rangle$ is a model of SCF_e, in fact the prime model over $F \cup X$. This shows that $F\langle X\rangle = \mathrm{dcl}(F \cup X)$, the definable closure of $F \cup X$.

In the language $\mathscr{L}$, SCF_e *eliminates quantifiers* (see [5, Proposition 35]). In fact there is a 1-1 correspondence between complete 1-types over F and certain prime ideals in $F[X_\sigma : \sigma \in (p^e)^{<\omega}]$ given by

$$I_F(\mathrm{tp}(x)/F) = \{f(X_{\sigma_1}, \ldots, X_{\sigma_m}) \in F[X_\sigma : \sigma \in (p^e)^{<\omega}] : f(\overline{x_\sigma}) = 0\}$$

(for details see [5]). Moreover, SCF_e has *elimination of imaginaries* (only for $e < \omega$), since we added names for a p-basis to the language (see [5, Proposition 43]). This means that any structure interpretable in F is definably isomorphic to a definable structure, where by an interpretable structure we mean a structure given as a definable set modulo some definable equivalence relation (e.g. a definable group modulo some definable normal subgroup).

Variety structures. We introduce two different topologies on $F^{\times n}$, the set of n-tuples over F (we also write F^n for $F^{\times n}$ if clear from the context).

F-Zariski topology. A subset $A \subseteq F^{\times n}$ is called *F-closed* if there are polynomials $f_1, \ldots, f_m \in F[X_1, \ldots, X_n]$, $m \in \omega$, such that

$$A = \{\overline{x} \in F^{\times n} : f_i(\overline{x}) = 0 \text{ for } i = 1, \ldots, m\}.$$

$V = V_1 \cup \cdots \cup V_k$ is called a *variety in F* if there are F-closed 'charts' $U_i \subseteq F^{\times n}$ and bijections $f_i : V_i \to U_i$ such that $U_{ij} = f_i(V_i \cap V_j)$ are F-open subsets of U_i and such that the $f_{ij} = f_j \circ f_{i-1} : U_{ij} \to U_{ji}$ are rational functions over F, for $1 \leq i, j \leq k$.

Note. Any F-open set $B \subseteq F^{\times n}$ is a variety in F as follows: If B is defined by $\bigvee_{i=1}^{m} f_i(\overline{x}) \neq 0$ then let $V_i = \{\overline{x} \in B : f_i(\overline{x}) \neq 0\}$ and set $U_i = \{(\overline{x}, y) : f_i(\overline{x}) \cdot y - 1 = 0\} \subseteq F^{n+1}$, $U_{ij} = \{(\overline{x}, y) \in U_i : f_j(\overline{x}) \neq 0\}$, and $f_{ij} : (\overline{x}, y) \mapsto (\overline{x}, f_j(\overline{x})^{-1})$.

$\langle G, \cdot \rangle$ is an *F-algebraic group* if G is a variety in F such that the maps $(x, y) \mapsto x \cdot y$ and $x \mapsto x^{-1}$ are morphisms with respect to the F-Zariski topology, i.e., are locally F-rational functions. Note: This notion of an F-algebraic group differs from the one of an F- (or k-) group commonly used in algebraic group theory, as for example in [1, 1.1], in the sense that here the universal domain is a separably, not algebraically, closed field.

To describe all definable sets we need a finer topology.

λ-topology. A subset $A \subseteq F^{\times n}$ is called *basic λ-closed* if there are finitely many polynomials $f_i \in F[X_{1_\sigma}, \ldots, X_{n_\sigma} : \sigma \in (p^e)^{<\omega}]$ such that

$$A = \left\{ \overline{x} \in F^{\times n} : \bigwedge_i f_i(x_{1_{\sigma_1}}, \ldots, x_{1_{\sigma_l}}, \ldots, x_{n_{\sigma_1}}, \ldots, x_{n_{\sigma_l}}) = 0 \right\}.$$

Basic λ-open sets are complements of basic λ-closed sets. Note that this topology is not noetherian; λ-closed sets are countable intersections of basic λ-closed sets.

λ-varieties are defined in analogy to varieties in F, where the charts U_i are basic λ-closed, the U_{ij}'s are basic λ-open, the f_{ij}'s are rational functions over F as before in the $\overline{x} \in U_{ij}$ (not in the expanded tuples). A *λ-algebraic group* is a λ-variety such that multiplication and inversion are F-rational functions on each chart. Note:

1. A λ-variety is irreducible iff it is irreducible with respect to *basic* λ-closed sets.
2. The λ-topology can be considered as a refinement of countably many *λ_m-topologies* defined as follows: λ_m-closed sets are of the form $\{\overline{x} \in F^{\times n} : \bigwedge_{i=1}^{k} f_i(x_{1_{\sigma_1}}, \ldots, x_{1_{\sigma_M}}, \ldots, x_{n_{\sigma_1}}, \ldots, x_{n_{\sigma_M}}) = 0\}$, where $f_i \in F[X_{1_\sigma}, \ldots, X_{n_\sigma} : |\sigma| \leq m]$. Define *$\lambda_m$-varieties* and *$\lambda_m$-algebraic groups* accordingly. Notice that the λ_0- topology is the F-Zariski topology, and all λ_m-topologies are noetherian. Furthermore, G is a λ-algebraic group iff there is $m < \omega$ such that G is a λ_m-algebraic group.

Quantifier elimination implies (see [5, Proposition 35]) that every formula $\Phi(\overline{x})$ over F defines a set of the form $\bigcup_{i=1}^{k}(O_i \cap C_i)$ where the O_i are basic λ-open, the C_i basic λ-closed. Without loss of generality we can assume that there is $l < \omega$ such that all O_i and C_i are defined by polynomials in $F[X_{1_\sigma}, \ldots, X_{n_\sigma} : \text{length}(\sigma) = |\sigma| = l]$, by replacing any x_{i_τ} by the corresponding term in the x_{i_σ}'s, where l is the maximal length of all occurring τ's.

There is an obvious but somewhat crucial connection between these two topologies:

Lemma 1.1. *Given finitely many basic λ-closed sets $A_1, \ldots, A_k \subseteq F^{\times n}$, there exists $m < \omega$ and a definable bijection $\Phi: F^{\times n} \to F^{\times m}$ such that $\Phi(A_1), \ldots, \Phi(A_k)$ are F-closed.*

Proof. Using the remark above we can assume that all A_i are defined by polynomials in X_{i_σ}, $1 \leq i \leq n$, $|\sigma| = l$. Set $m = n \cdot p^{e \cdot l} = n \cdot q$ and define $\Phi: F^{\times n} \to F^{\times m}$ by $\Phi(\ldots, x_i, \ldots) = (\ldots, x_{i_{\sigma_1}}, \ldots, x_{i_{\sigma_q}}, \ldots)$ where $\{\sigma_1, \ldots, \sigma_q\} = \{0, \ldots, p^e - 1\}^l$. So the image of a set defined by polynomials $f_i \in F[\overline{X_\sigma}: |\sigma| = l]$ is defined by the same polynomials viewed as elements of $F[Y_1, \ldots, Y_m]$. □

2. The groups

Let G be an infinite group interpretable, hence definable, in SCF_e. To prove that G can be definably equipped with the structure of an F-algebraic group, we follow the lines of the proof for the corresponding theorem for algebraically closed fields (see [2, 15, 16, 12, 17]). We first find a λ-algebraic group structure on G, and then turn G into an F-algebraic group using Lemma 1.1. G is a stable group as it is definable in the stable theory SCF_e. So we can apply the concept of generic types to G, introduced by Poizat.

Let G be a stable group.

(A) A type p over G is called *generic* (for G) iff for every formula $\varphi(x) \in p$ finitely many translates of φ cover G; i.e., there are $a_1, \ldots, a_m \in G$ such that $G \models \forall x(\bigvee_{i=1}^m \varphi(a_i^{-1} \cdot x))$; see [12, Chapter 5]. Note that if y is a realization of a generic type over G, then so is y^{-1} and $y \cdot x$ for every $x \in G$.

(B) G^0 denotes the intersection of all definable subgroups of G of finite index. We call G^0 the *connected component of* G. G is said to be connected iff $G^0 = G$; see [12, p. 25].

(C) The generic types of G are in one-to-one correspondence with the cosets of G modulo G^0; see [12, Proposition 5.9].

We need a few preliminary lemmas.

Lemma 2.1. *A definable subgroup H of a λ-algebraic group G is basic λ-closed in G, hence itself a λ-algebraic group.*

Proof. We find $m < \omega$ such that G is a λ_m-algebraic group and H is of the form $\bigcup_i (O_i \cap C_i)$, where O_i, C_i are λ_m-open, λ_m-closed, respectively. So H is a constructible subgroup of G with respect to the λ_m-topology in the sense of [1, AG.1.3]. As in [1, Proposition 1.3(c)], it follows that H is λ_m-closed in G. Hence H itself is a λ_m-algebraic group, and therefore a λ-algebraic group. □

Note. The same proof as in [12, 4.e.6] shows that if G is a λ-variety such that multiplication is locally an F-rational function then G is definably isomorphic to a λ-algebraic group.

Lemma 2.2. *Any infinite group G definable in $F \models \mathrm{SCF}_e$ is connected-by-finite; i.e., $[G : G^0] < \omega$.*

Proof. Suppose G is a definable subset of $F^{\times n}$. There is a definable injection Ψ from $F^{\times n}$ to F (and from the set of n-types to the set of 1-types) given by

$$\Psi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^{p^l} \tilde{m}_i$$

where l is such that $p^{l \cdot e} \geq n$ and $\{\tilde{m}_1, \ldots, \tilde{m}_{p^{l \cdot e}}\}$ is the set of p^l-monomials over $\{a_1, \ldots, a_e\}$, hence a basis of F over F^{p^l}. So $\Psi(x)$ is an element, the lth level of whose tree is $(x_1, \ldots, x_n, 0, \ldots, 0)$. Therefore, without loss of generality, we can assume that G is a definable subset of F. By [5, Proposition 44] there are a finite number of 'maximal types' (or minimal ideals) containing a given formula, which are the only candidates for being generic types of G. So by remark (C), G is connected-by-finite. □

Now, since G is covered by finitely many cosets of G^0, the same argument as in [12, 4.e.9], together with Lemma 2.1, gives

Corollary 2.3. *If G is an infinite group definable in $F \models \mathrm{SCF}_e$ such that the connected component G^0 of G is definably isomorphic to a λ-algebraic group, then so is G.*

To prove the following proposition, we use the same idea as for algebraically closed fields of characteristic p; here the λ_σ-functions play the role of the p^nth root functions. (Notice: If x is a p^nth power, then $x_{\langle 0, \ldots, 0\rangle} = \sqrt[p^n]{x}$ for $|\langle 0, \ldots, 0\rangle| = n$.)

Proposition 2.4. *Let $\langle G, \circ\rangle$ be a connected group definable in $\mathcal{M}$. Then G is definably isomorphic to a group $\langle G', *\rangle$ such that for independent generic elements a, $b \in G'$, the map $(a, b) \mapsto a * b$ is a rational function.*

Proof. As in Lemma 2.2 we can assume that $G \subset \mathcal{M}$, with G and its group operation defined over some countable $F \prec \mathcal{M}$. Let $\Phi(x)$ define G over F. Let K be ω_1-saturated with $F \prec K \prec \mathcal{M}$, and let $G(K) = G \cap K$, the group Φ defines in K. For x, $y \in G$, $x \circ y \in \mathrm{dcl}(F \cup \{x, y\}) = F\langle x, y\rangle$. Recall $F\langle x, y\rangle = F(x_\sigma, y_\sigma : \sigma \in (p^e)^{<\omega})$. By compactness and the usual replacing process we find finitely many rational functions $R_i \in F(X_\sigma, Y_\sigma : |\sigma| = l)$ such that for all x, $y \in G$, $x \circ y \in \{R_i(x_{\sigma_1}, \ldots, x_{\sigma_N}, y_{\sigma_1}, \ldots, y_{\sigma_N}) : 1 \leq i \leq n\}$; i.e.,

$$\mathcal{M} \models \forall x, y \left(\Phi(x) \wedge \Phi(y) \rightarrow \bigvee_{i=1}^{n} x \circ y = R_i(\overline{x_\sigma}, \overline{y_\sigma}) \right)$$

where '$\circ$' is given by a formula over F. Now let $g \in G$ be generic over K and define $K((g)) \stackrel{\mathrm{def}}{=} K(a \circ g \circ b : a, b \in G(K))$. By the above $K((g)) \subseteq K(g_\tau : |\tau| = 2l)$. So $K((g))$ is a subfield of a finitely generated field over K, hence itself finitely generated. Hence there are finitely many rational functions $Q_i \in K(X_\tau : |\tau| = 2l)$ such that $K((g)) = K(c_1, \ldots, c_m)$ and $c_i = Q_i(g_{\tau_1}, \ldots, g_{\tau_L}) = Q_i(\overline{g_\tau})$, with $|\tau| = 2l$. Now define the function $f : G \to \mathcal{M}^{m+1}$ by $f(x) = (x, Q_1(\overline{x_\tau}), \ldots, Q_m(\overline{x_\tau}))$. [If $Q_i(\overline{x_\tau})$ is not defined set it equal to zero.] Clearly the image of $\langle G, \circ\rangle$, say $\langle G', *\rangle$, is definably isomorphic to G, if we define '$*$' appropriately. G' will turn out to have the desired property.

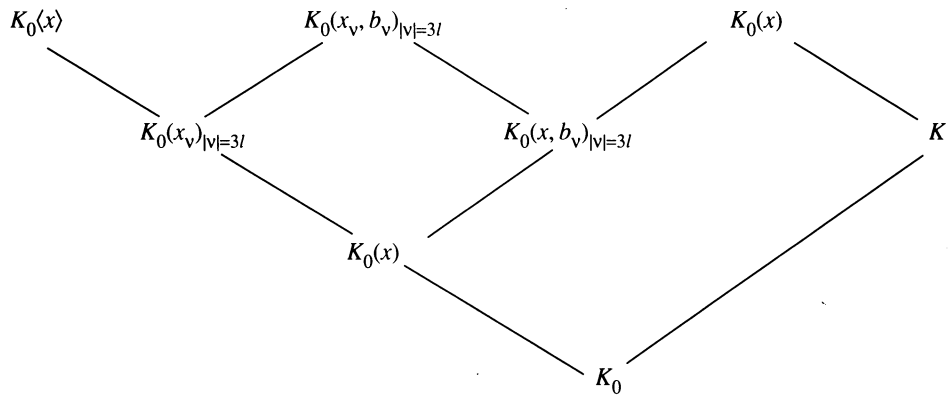

FIGURE 2

Since G, and hence G', has a unique generic type, it is easy to see that for *every* generic element x' of G' over K, $K(x') = K(a * x' * b)$ for all $a, b \in G'(K) = G' \cap K^{m+1}$. Now let K_0 be countable with $F \preceq K_0 \prec K$, containing all the parameters needed to define $Q_1, \ldots, Q_m$. By ω_1-saturation of K we find $b \in G'(K)$ generic over K_0, $x \in G'$ generic over K; i.e., x and b are two independent realizations of the generic type of G' over K_0. We have

- $x * b \in K_0(x_\nu, b_\nu : |\nu| = 3l)$, since if $x = (x_1, \ldots, x_{m+1})$ and $b = (b_1, \ldots, b_{m+1})$ then

$$x * b = (R_j(\overline{x_{1_\sigma}}, \overline{b_{1_\sigma}}), Q_1(\overline{R_j(\overline{x_{1_\sigma}}, \overline{b_{1_\sigma}})_\tau}), \ldots, Q_m(\overline{R_j(\overline{x_{1_\sigma}}, \overline{b_{1_\sigma}})_\tau})),$$

  for some $1 \leq j \leq n$. So $x * b \in K_0(x_\nu, y_\nu : |\nu| = 3l)$, since $|\sigma| = l$ and $|\tau| = 2l$. Furthermore
- $x * b \in K(x)$ since $x * b \in K(x * b)$ and $K(a * x * b) = K(x)$ for all a, $b \in G'(K)$, in particular when $a = 1$.

By the choice of x, x is independent from K over K_0 which is equivalent to $K_0\langle x\rangle$ and K being linearly disjoint over K_0, see [5, Proposition 36]. So $K_0(x_\nu : |\nu| = 3l)$ and K are linearly disjoint over K_0, hence $K_0(x_\nu : |\nu| = 3l)$ and $K(x)$ are linearly disjoint over $K_0(x)$. Then also $K_0(x_\nu, b_\nu : |\nu| = 3l)$ and $K(x)$ are linearly disjoint over $K_0(x, b_\nu : |\nu| = 3l)$. Here we used the following fact from algebra [9, p. 162], noting also that $x \in K_0(x_\nu : |\nu| = 3l)$ and that $b_\nu \in K$ (see Figure 2):

> If the two fields L and K are linearly disjoint over F then for any $x \in L$, L and $K(x)$ are linearly disjoint over $F(x)$.

Therefore $x * b \in K_0(x_\nu, b_\nu : |\nu| = 3l) \cap K(x) = K_0(x, b_\nu : |\nu| = 3l)$. For x, y independent generic elements of G' over K_0 we have that $\mathrm{tp}(x, y/K_0) = \mathrm{tp}(y, x/K_0)$. This ensures that $x * y \in K_0(x, y_\nu : |\nu| = 3l) \cap K_0(x_\nu, y : |\nu| = 3l)$. But x and y being independent over K_0 implies that $K_0(x_\nu : |\nu| = 3l)$ and $K_0(y_\nu : |\nu| = 3l)$ are linearly disjoint over K_0. So $K_0(x_\nu : |\nu| = 3l)$ and $K_0(x, y_\nu : |\nu| = 3l)$ are linearly disjoint over $K_0(x)$. Then $K_0(x_\nu, y : |\nu| = 3l)$ and $K_0(x, y_\nu : |\nu| = 3l)$ are also linearly disjoint over $K_0(x, y)$. This finally gives $x * y \in K_0(x, y_\nu : |\nu| = 3l) \cap K_0(x_\nu, y : |\nu| = 3l) = K_0(x, y)$ (see Figure 3). Hence in G', multiplication is rational for independent generic elements. □

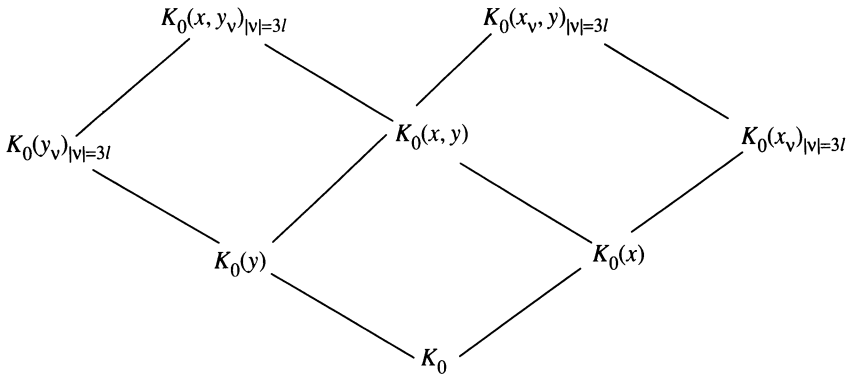

FIGURE 3

The next proposition allows us to equip G with the structure of a λ-algebraic group.

Proposition 2.5. *Let $\langle G, \cdot \rangle \subseteq F^n$ be an infinite, connected, definable group, $F \models \mathrm{SCF}_e$, such that for independent generic elements $a, b \in G$ multiplication is a rational function (i.e. $a \cdot b = R(a, b)$ with $R(X, Y) = (R_1(\overline{X}, \overline{Y}), \ldots, R_n(\overline{X}, \overline{Y}))$: $R_i(\overline{X}, \overline{Y}) \in F(\overline{X}, \overline{Y})$). Then G can be definably equipped with the structure of a λ-algebraic group.*

Proof. We have to put a λ-variety structure on G such that '$\cdot$' is a morphism $G \times G \to G$.

Claim 1. Let $V \subseteq G$ (or $G^{\times n}$) be an irreducible λ-variety and $X \subseteq V$ a definable set containing the generic of G (or G^n). Then X contains a basic λ-open subset of V containing the generic.

X is of the form $\bigcup_i (O_i \cap C_i)$, O_i basic λ-open, C_i basic λ-closed in V. Let $O \cap C$ contain the generic. So C contains the generic, but also $V - C$ does, if it is nonempty, since it is open in V. (Recall: the generic is among the types with minimal ideal.) Since G has a unique generic, $C = V$. So $O \subseteq V$. This proves the claim.

Now, again by quantifier elimination, G is of the form $\bigcup_i (O_i \cap C_i)$, O_i, C_i as before. Let $V_1 = O_i \cap C_i$ contain the generic of G. The set $\{(x, y) \in V_1 \times V_1 : x \cdot y = R(x, y)\}$ is definable and contains the generic of $G \times G$. So by the claim there is a basic λ-open set W_1 containing the generic such that for all $x, y \in W_1$, $x \cdot y = R(x, y)$. Define $V_2 = \{x \in V_1 :$ for any generic element y of G independent from x, $(y, x) \in W_1$ and $(y^{-1}, y \cdot x) \in W_1\}$.

Claim 2. V_2 is definable.

Let $\Psi(y, x)$ be the formula saying '$(y, x) \in W_1$ and $(y^{-1}, y \cdot x) \in W_1$' and let $q(y)$ be the nonforking extension of the generic type of G to V_1. By stability, $q(y)$ is definable (for details see [11]), i.e., there is a formula $d\Psi(x)$ over V_1 such that $\Psi(y, a) \in q(y)$ iff $G \models d\Psi(a)$, which says that $d\Psi$ defines V_2.

Clearly V_2 contains the generic since y being generic over x implies y^{-1} and $y \cdot x$ being generics (see remark (A)). Again there is $V_3 \subseteq V_2$ basic λ-open in V_2 containing the generic. Finally let $V = V_3 \cap V_3^{-1}$ and $W = \{(x, y) \in W_1 : x, y, x \cdot y \in V\} \cap V \times V$.

Then '$\cdot$': $W \to V$ is a morphism as it is given by $R(X, Y)$.

For $a \in V$ and $x \in G$ generic over a, $(x, a) \in W$ and $(x^{-1}, x \cdot a) \in W$. As in [12, p. 143] it follows now that for a, $b \in G$, $U_{a,b} = \{(x, y) \in V \times V: a \cdot x \cdot b \cdot y \in V\}$ is basic λ-open in $V \times V$ and the map $(x, y) \mapsto a \cdot x \cdot b \cdot y$ is a morphism from $U_{a,b}$ to V.

For $c \in G$ put $a = c \cdot x_0^{-1}$ and $b = 1$. Then the section of $x = x_0$ gives $V_c = V \cap c^{-1}V = \{y \in V: c \cdot y \in V\}$ is basic λ-open in V and the map $y \mapsto c \cdot y$ is a morphism from V_c to V.

Since V is a definable set containing the generic of G, finitely many translates aV of V cover G (see remark (A) above). This gives a definable λ-variety structure on G. By the above, for a, $b \in G$, $U_{c^{-1} \cdot a,b} = \{(x, y) \in V \times V: a \cdot x \cdot b \cdot y \in cV\}$ is λ-open in $V \times V$ and $(x, y) \mapsto c^{-1} \cdot a \cdot x \cdot b \cdot y$ is a rational function from $U_{c^{-1} \cdot a,b}$ to V which makes '$\cdot$' a morphism on G. □

Main Theorem 2.6. *Any infinite group $\langle G, \cdot \rangle$ interpretable in a separably closed field F of finite Eršov-invariant is definably isomorphic to an F-algebraic group.*

Proof. By 2.3, 2.4, and 2.5 it suffices to show that any λ-algebraic group is definably isomorphic to an F-algebraic group. The data of a λ-algebraic group involve only finitely many basic λ-closed subsets of F^n for some n (the charts U_i and the $U_i \setminus U_{ij}$). So by Lemma 1.1 there is a definable bijection $\Phi: F^n \to F^m$ for some $m < \omega$ such that $\Phi(U_i)$ and $\Phi(U_{ij})$ are F-closed. One can check that the bijection Φ turns F-rational functions into F-rational functions; this says, given an F rational map $R: F^n \to F^n$ (or $R: F^n \times F^n \to F^n$) then the map $S = \Phi \circ R \circ \Phi^{-1}: F^m \to F^m$ (or $S: F^m \times F^m \to F^m$ with $S(x, y) = \Phi(R(\Phi^{-1}(x), \Phi^{-1}(y)))$) is an F-rational function as well. (Note: This fact is implicitly contained in Delon's quantifier elimination result, see [5, Proposition 35].) Hence the image of the λ-algebraic group G under the definable bijection Φ is an F-algebraic group. □

In order to prove an analogue of Rosenlicht's theorem (see [13 and 12, 4.7]) we need a preliminary lemma.

Lemma 2.7. *Let G be a definable subgroup of $GL_n(F)$ for some $n < \omega$, the (definable) group of invertible $n \times n$-matrices over F. Then G is definably isomorphic to an F-closed subgroup H of $GL_m(F)$ for some $m < \omega$.*

Note. We consider $GL_n(F)$ as the F-closed subset

$$\{(x_{ij}, y)_{1 \le i,j \le n}: \det((x_{ij})) \cdot y = 1\} \subset F^{n^2+1}.$$

Proof. Throughout the first part of this proof we make the following minor change in notation. We will use indices $\tau \in \{0, \dots, p-1\}^e = p^e$, tuples of length e over the set $\{0, \dots, p-1\}$ to index the basis $B = \{m_0 = 1, m_1, \dots, m_{p^e-1}\}$ of F over F^p. So now, $B = \{m_\tau: \tau \in p^e\}$, where $m_\tau = a_1^{\tau_1} \cdots a_e^{\tau_e}$ for $\tau = \langle \tau_1, \dots, \tau_e \rangle$. (Remember: $\{a_1, \dots, a_e\}$ is the fixed p-basis.) Furthermore, we can add (and subtract) elements in p^e coordinatewise modulo p. So, as before, $x = \sum_{\tau \in p^e} x_\tau^p m_\tau$. The following map α is definable in F:

$$\alpha: F \to M_{p^e}(F), \qquad x \mapsto (x_{\tau\nu})_{\tau \in p^e, \nu \in p^e},$$

where $M_{p^e}(F)$ is the ring of $p^e \times p^e$-matrices over F, where we think of the rows and columns being indexed by elements of $\{0, \dots, p-1\}^e$, and where

$$x_{\tau\nu} = x_{\nu - \tau} a_1^{\varepsilon_1} \cdots a_e^{\varepsilon_e},$$

with

$$\varepsilon = \begin{cases} 0 & \text{if } \tau_i \leq \nu_i, \\ 1 & \text{if } \tau_i > \nu_i. \end{cases}$$

Note that the first row of $\alpha(x)$ consists of the elements x_τ, $\tau \in p^e$. For example, for $p = 2$, $e = 1$, $x = x_0^2 + x_1^2 m$, and

$$\alpha(x) = \begin{pmatrix} x_0 & x_1 \\ x_0 m & x_0 \end{pmatrix}.$$

One can check that α is a ring embedding. Therefore the following map β is a group embedding:

$$\beta: GL_n(F) \to GL_{n \cdot p^e}(F), \qquad (x_{ij}) \mapsto (\alpha(x_{ij}));$$

here every entry x_{ij} is replaced by the matrix $\alpha(x_{ij})$. Notice that the elements x_{ij_τ} for $1 \leq i$, $j \leq n$, $\tau \in p^e$ occur as certain entries in the matrix $\beta((x_{ij}))$. All other entries of $\beta((x_{ij}))$ are given by definable linear combinations of the x_{ij_τ} over F.

Now let $G \leq GL_n(F)$ be defined by a boolean combination of formulas of the form $f(x_{ij_{\sigma_1}}, \ldots, x_{ij_{\sigma_k}}, 1 \leq i, j \leq n) = 0$ (in the old notation), where f is a polynomial over F, and the σ_i are of fixed length l. Iterate the map β l times and get a definable map $\beta^l: GL_n(F) \to GL_{n \cdot p^{l \cdot e}}(F)$. For $(x_{ij}) \in GL_n(F)$, $\beta^l((x_{ij}))$ is a matrix with certain entries equal to x_{ij_σ} for all $1 \leq i, j \leq n$, $\sigma \in (p^e)^{<\omega}$ with $|\sigma| = l$, and all other entries are given by polynomials over F in these x_{ij_σ}'s.

Now $\beta^l(G) = H$ is definably isomorphic to G and, as a subgroup of $GL_{n \cdot p^{l \cdot e}}(F)$, H is quantifier-free definable in the pure language of fields. This says that H is a constructable subgroup of $GL_{np^{le}}$ with respect to the F-Zariski-topology. Now it follows, as in [1, Proposition 1.3(c)], that H is F-closed in $GL_{np^{l \cdot e}}(F)$. □

We now prove Rosenlicht's theorem for infinite groups interpretable in SCF_e. For details see [12, 4.f]:

Corollary 2.8. *Let G be a connected infinite group interpretable in a separably closed field F of finite Eršov-invariant. Then $G/Z(G)$ is definably isomorphic to a linear F-algebraic group.*

Note. By a linear F-algebraic group we mean an F-closed subgroup of $GL_N(F)$ for some $N < \omega$. Here $Z(G)$ denotes the center of G.

Proof. By Theorem 2.6 we can assume that G is an F-algebraic group. Show that G acts on the local ring A or rational functions defined in a neighborhood of the identity e by $f^g(x) = f(gxg^{-1})$. Furthermore G preserves M^n, where $M = \langle \{f \in F[G]: f(e) = 0\} \rangle$, the maximal ideal of A. A/M^n is a finite-dimensional vector space over F. The action of G on A/M^n is definable, given by rational functions, and linear. So for all $n \in \omega$, $G_n = \{g \in G : f^g = f, \forall f \in A/M^n\}$ is an F-closed subset of G with $G_{n+1} \subseteq G_n$. Since all G_n are closed there is $m \in \omega$ such that $G_n = G_m$ $\forall n \geq m$. This shows that $G_m = Z(G)$ and so $G/Z(G)$ is definably embedded in $GL_d(F)$, where $d = \dim(A/M^m)$ as a vector space over F. Now by Lemma 2.7, $G/Z(G)$ is definably isomorphic to an F-closed subgroup of $GL_N(F)$ for some N. □

The following remark will be needed in the next section. Throughout $\tilde{F}$ denotes the algebraic (field-)closure of F.

Remark 2.9. Let G be a connected linear F-algebraic group (i.e., an irreducible F-closed subgroup of $GL_n(F)$). Then the Zariski-closure $\mathcal{G}$ of G in $GL_n(\tilde{F})$ is a connected, linear algebraic group which is defined over F. Moreover, G consists of the F-rational points of $\mathcal{G}$, i.e., $G = \mathcal{G} \cap GL_n(F)$, and clearly G is dense in $\mathcal{G}$.

Note. We say that a connected linear algebraic group $\mathcal{G} \leq GL_n(\tilde{F})$ is defined over F if its (prime) ideal $I_{\tilde{F}}(\mathcal{G}) = \{f \in \tilde{F}[X_1, \ldots, X_{n^2+1}]: f(\overline{x}) = 0 \text{ for all } \overline{x} \in \mathcal{G}\}$ is generated by elements of $F[\overline{X}]$.

Proof of Remark 2.9. [1, Proposition 1.3(b)] shows that $\mathcal{G}$ is a (closed) subgroup of $GL_n(F)$ which is defined over F. By [1, Proposition 1.2], $\mathcal{G}^0$ is also defined over F. Therefore, since G is irreducible (as an F-closed group), $\mathcal{G}^0 \cap G = G$. Hence $\mathcal{G}^0 = \mathcal{G}$, so $\mathcal{G}$ is connected. Since G is F-closed, it follows that $G = \mathcal{G} \cap GL_n(F)$. This completes the proof.

Observe that, given the prime ideal $I = I_F(G) = \{f \in F[\overline{X}]: f(\overline{x}) = 0 \text{ for all } \overline{x} \in G\}$ of G over F, the ideal of $\mathcal{G}$ over $\tilde{F}$ is $J = I \cdot \tilde{F}[\overline{X}]$. It is easy to show that J is prime, and obviously generated by elements of $F[\overline{X}]$. □

3. The fields

Throughout let $F \models \mathrm{SCF}_e$ with $e < \omega$, K an infinite field interpretable, hence definable in F. We want to show that K is definably isomorphic to a finite extension of F.

Lemma 3.1. *Any infinite, definable, multiplicative subgroup* $M \leq F^*$ $(= F - \{0\})$ *contains* $(F^*)^{p^l}$ *for some* $l < \omega$.

Proof. M is of the form $\bigcup_i (O_i \cap C_i)$ where O_i is basic λ-open defined by $P_i(\overline{x_\sigma}) \neq 0$, C_i basic λ-closed defined by $\bigwedge_j Q_{ij}(\overline{x_\sigma}) = 0$, P_i, Q_{ij} polynomials over F, all σ of fixed length l. We show $(F^*)^{p^l} \subseteq M$:

$M \cap (F^*)^{p^l}$ is defined by

$$\bigvee_i \left[P_i(x_{\langle 0,0,\ldots,0\rangle}, 0, \ldots, 0) \neq 0 \wedge \bigwedge_j Q_{ij}(x_{\langle 0,\ldots,0\rangle}, 0, \ldots, 0) = 0 \right] \wedge \bigwedge_{\sigma \neq \langle 0,\ldots,0\rangle} x_\sigma = 0$$

which is equivalent to

$$\exists y \left(x = y^{p^l} \wedge \bigvee_i \left[P_i'(y) \neq 0 \wedge \bigwedge_j Q_{ij}'(y) = 0 \right] \right)$$

where $P_i'(y) = P_i(y, 0, \ldots, 0)$ and $Q_{ij}'(y) = Q_{ij}(y, 0, \ldots, 0)$.

Hence $M \cap (F^*)^{p^l}$ is finite or cofinite in $(F^*)^{p^l}$. But $M \cap (F^*)^{p^l}$ is an infinite subgroup of M, since it contains M^{p^l} which is isomorphic to M. Therefore $M \cap (F^*)^{p^l} = (F^*)^{p^l}$. □

Corollary 3.2. *An infinite, definable subfield K of F is a finite extension of some F^{p^l} (and definably isomorphic to a finite extension of F).*

Proof. By Lemma 3.1 K contains F^{p^l} for some $l < \omega$. $[F : F^{p^l}] = p^{e \cdot l} < \omega$ and so K is a finite extension of F^{p^l}. $\Phi: F \to F^{p^l}$ with $\Phi(x) = x^{p^l}$ is an isomorphism. So $\Phi^{-1}(K)$ is a finite extension of F (viewed as a vector space over F). □

Remark 3.3. Let L be a finite (hence purely inseparable) extension of F. F is definable in L, since F is a finite extension of L^{p^l} for some $l < \omega$. We may view the field L as a finite-dimensional vector space over F, hence as an $\langle F, +, -, \cdot, ^{-1}, 0, 1\rangle$-structure, with the same definable sets as the L-structure L. Likewise we may view F as an L-structure, with the same definable sets as the F-structure F.

Since K is definable in the stable theory SCF_e it is itself stable. So by [12, Theorem 5.10] K has a unique generic type which is generic for multiplication and addition. From now on we work with the definable group $K^+ \rtimes K^*$ (K^* acts on K^+ by multiplication) which is therefore connected. It is centerless, so by 2.8 we can assume it to be a linear F-algebraic group.

Lemma 3.4. *Let K be as above. Then* $\mathrm{char}(K) = \mathrm{char}(F) = p$.

Proof. Since K^+ is abelian it is definably isomorphic to a subgroup of the upper triangular matrices over a finite extension L of F (see [8, 15.4]). Let $\varphi_i: K^+ \to L^*$ be the group homomorphism which maps an element of K^+ to the ith elements of its diagonal (where K^+ is in upper triangular form over L). φ_i is definable and $K^+/\mathrm{Ker}(\varphi_i) \simeq \mathrm{Im}(\varphi_i) \leq L^*$.

Case 1. $\mathrm{char}(K) = 0$. Then K^+, hence $K^+/\mathrm{Ker}(\varphi_i)$ and $\mathrm{Im}(\varphi_i)$ are divisible. But, by 3.1 and 3.3, L^* has no nontrivial divisible definable subgroup. So $\mathrm{Im}(\varphi_i) = \{1\}$.

Case 2. $\mathrm{char}(K) = q > 0$. Then $\mathrm{Im}(\varphi_i)$ is a subgroup of L^* of exponent q. But L^* contains only finitely many elements of order q. K^+ is connected, so $\mathrm{Im}(\varphi_i) = \{1\}$.

So K^+ is given by unipotent matrices. Since $\mathrm{char}(L) = p$, the order of any unipotent matrix over L is a power of p. Hence $\mathrm{char}(K) = p$. □

Proposition 3.5. *K (as above) is definably isomorphic to a subfield of a finite extension of F.*

Proof. As before K^+ can be identified with a connected, unipotent, linear F-algebraic group which, by Remark 2.9 consists of the F-rational points of some connected, commutative, linear algebraic group V^+ (in $\tilde{F}$) of exponent p. (Note: Since K^+ is dense in V^+, V^+ satisfies the same polynomial identities over F as K^+ does.) V^+ is definably isomorphic to a closed subgroup of a vector group $\tilde{F}^+ \times \cdots \times \tilde{F}^+$ and hence to a vector group W itself, see [8, pp. 127, 130, 131].

In the same way K^* can be identified with the F-rational points of some connected, commutative, linear algebraic group V^* (in $\tilde{F}$). We know K^* acts on K^+ by multiplication.

Claim 1. V^* acts on V^+ (and therefore on the vector group W).

Note:

V^* and V^+ are connected, closed subgroups of $GL_n(\tilde{F})$ for some n.

V^* and V^+ are defined over F (see Remark 2.9); and for $I_F(K^*)$, the ideal of K^* over F, and $I_{\tilde{F}}(V^*)$, the ideal of V^* over $\tilde{F}$, we have

$$I_{\tilde{F}}(V^*) = I_F(K^*) \cdot \tilde{F}[\overline{X}] \quad \text{and} \quad I_F(K^*) = I_{\tilde{F}}(V^*) \cap F[\overline{X}] = I_F(V^*).$$

And the same for K^+ and V^+:

$$I_{\tilde{F}}(V^+) = I_F(K^+) \cdot \tilde{F}[\tilde{X}] \quad \text{and} \quad I_F(K^+) = I_{\tilde{F}}(V^+) \cap F[\overline{X}] = I_F(V^+).$$

We first show that K^* acts on V^+. For all $x \in K^+$ and $g \in K^*$ we have $x^g \in K^+$. This says $P(\overline{X}) \in I_F(K^+)$ implies $P^g(\overline{X}) \in I_F(K^+)$ where $P^g(\overline{X})$ is such that $P^g(x^g) = P(x)$. (Note: The action is given by conjugation in $GL_n(\tilde{F})$.) But $I_F(K^+) = I_F(V^+)$. Hence $x^g \in V^+$ for all $x \in V^+$, $g \in K^*$.

Now show that V^* acts on V^+. For all $y \in K^*$ and $a \in V^+$ we have $a^y \in V^+$. This says $P(\overline{Y}) \in I_F(K^*)$ implies $P_a(\overline{Y}) \in I_{\tilde{F}}(V^+)$ for all $a \in V^+$, where $P_a(\overline{Y})$ is such that $P_a(a^y) = P(y)$. But $I_F(K^*) = I_F(V^*)$. Hence $a^y \in V^+$ for all $y \in V^*$, $a \in V^+$. So V^* acts on V^+.

Our goal is to find an algebraically closed field definable in $\tilde{F}$ (as an algebraically closed field) in which K is embedded.

V^* is $\tilde{F}$-definably isomorphic to $V_s \times V_u$, where V_s, V_u are the semisimple, unipotent parts of V^*, respectively. A unipotent matrix over $\tilde{F}$ has order p^l for some l. So there is $L < \omega$ such that $x^{p^L} \in V_s$ for all $x \in V^*$. (Note: V^* is commutative.) V_s is a torus and $x \mapsto x^{p^l}$ is a bijection from V_s to V_s (see [1, Proposition 8.9]). Consider $\pi: V^* \to V_s$ the projection onto the semisimple part. $\pi|_{K^*}$ is injective since K^* contains no nontrivial elements of order p, hence no nontrivial unipotent elements. Thus $x \mapsto x^{p^l}$ is injective from K^* to $K^* \cap V_s$.

Claim 2. V_s is a one-dimensional torus, i.e., definably isomorphic to $\tilde{F}^*$.

V^* is a connected, commutative linear algebraic group which is defined over F. So V_s is a closed subgroup defined over F (see [1, Theorem 10.6]). V_s is diagonalisable and split over a finite separable extension of F, hence over F itself; i.e., V_s is isomorphic (over F) to $D_m(\tilde{F})$ for some m, a diagonal group over $\tilde{F}$.

To prove that $m = 1$ it suffices to show that for some prime q with $(p, q) = 1$ all the qth roots of unity in V_s lie inside K^*. (Then there are at most q many and so $m = 1$.) But for $\alpha_q: V_s \to V_s$ with $\alpha_q(x) = x^q$, $\mathrm{Ker}(\alpha_q) \subseteq V_s \cap F \subseteq K^*$ (see [1, Proposition 8.9]), which proves that there is an isomorphism $\alpha: \tilde{F}^* \to V_s$.

We summarize the situation: K^* is embedded (via $x \mapsto x^{p^L}$) in a one-dimensional torus which is definably isomorphic (over F) to $\tilde{F}^*$ and which is acting on a vector group W in which W^+ is definably embedded.

The field structure of K is given on the set $K^* \cup \{0\}$ as follows: multiplication correspondes to multiplication in K^*, addition is given by the action on an element $a \in W$ which corresponds to a nonzero element from K^+; i.e., for $x, y, z \in K^*$: $x \oplus y = z$ iff $a^x + a^y = a^z$, where $\oplus$ is addition on $K^* \cup \{0\}$, '+' is addition in W. [Notice: This action might be defined over some finite extension L of F since $V^+ \to W$ is defined over some $L \supseteq F$.] Moreover $a = (a_1, \ldots, a_n)$ can be chosen such that $a_i \neq 0 \ \forall i$, since $\{\overline{x}: x_i \neq 0$ for $i = 1, \ldots, n\}$ is open in W and K^+ is dense in $V^+ \simeq W$. This field structure

on $K^* \cup \{0\}$ is definably isomorphic to the field structure on $\mathrm{Im}(K^*)$ under $x \mapsto x^{p^L}$ given in the same manner, since for $x, y, z \in K$: $x + y = z$ iff $x^{p^L} + y^{p^L} = z^{p^L}$ (char $= p$).

Claim 3. The action of V_s on W is linear, in particular given by diagonal matrices.

The action of an element s of V_s on W is an $\tilde{F}$-definable automorphism of W. (Here we mean an isomorphism as algebraic groups; the inverse is also an isomorphism since it is given by conjugation of matrices.) So s and s^{-1} act as a sequence of p-polynomials (see [12, p. 77]) and it follows that this action is linear; i.e., $V_s \xrightarrow{\simeq} H \leq GL(W)$. By [1, 8.4] the action of V_s on W is diagonalisable; i.e., there is a suitable basis for W such that H is a diagonal group $\mathscr{D} \subseteq D_n(\tilde{F})$; i.e., there is an isomorphism $\beta: V_s \to \mathscr{D}$.

Claim 4. The orbit $a^{\mathscr{D}}$ of $a \in W$ under $\mathscr{D}$ together with 0 form a subgroup of W.

We have $\tilde{F}^* \xrightarrow{\alpha} V_s \xrightarrow{\beta} \mathscr{D} \xrightarrow{\pi_i} \tilde{F}^*$ where π_i is the projection on the ith diagonal element. So $\pi_i \circ \beta \circ \alpha$ for $i = 1, \ldots, n$ are characters of $\tilde{F}^*$ which are all of the form $x \mapsto x^m$ ($m \in \mathscr{Z}$ an integer). Hence

$$\mathscr{D} = \left\{ \begin{pmatrix} x^{m_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & x^{m_n} \end{pmatrix} : x \in \tilde{F}^* \right\} \quad \text{for some } m_i \in \mathscr{Z}.$$

Via β, K^* is embedded in $\mathscr{D}$. So $\mathscr{D}$ contains an *infinite* subgroup U (isomorphic to K^*) such that $a^U \cup \{0\}$ ($\hat{=} K^+$) is a subgroup of W (since the action of U corresponds to the field multiplication).

Subclaim (a). $m_i \neq 0$ for all $i = 1, \ldots, n$.

Suppose without loss of generality $m_1 = 0$, i.e.,

$$\mathscr{D} = \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & x^{m_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & x^{m_n} \end{pmatrix} : x \in \tilde{F}^* \right\}.$$

But then, since $a_1 \neq 0$, for $x, y \in U$:

$$a^x + a^y = \begin{pmatrix} a_1 \\ a_2 x^{m_2} \\ \vdots \\ a_n x^{m_n} \end{pmatrix} + \begin{pmatrix} a_1 \\ a_2 y^{m_2} \\ \vdots \\ a_n y^{m_n} \end{pmatrix} \neq a^z \qquad \forall z \in \tilde{F}^*$$

which gives a contradiction.

Subclaim (b). $\{0\}$ is the only finite orbit of W under the action of $\mathscr{D}$.

Since $m_i \neq 0$ $\forall i$ there are no single-element orbits except $\{0\}$. Furthermore there cannot be any orbits O of length $2 \leq n < \omega$ since $\alpha: V_s \to \mathrm{Sym}(O)$ gives $V_s / \mathrm{Ker}(\alpha) \simeq \mathrm{Im}(\alpha)$ which is finite, but V_s is connected.

We know that $a^U \cup \{0\}$ is a subgroup of W. Hence $\overline{a^U \cup \{0\}}$, the (Zariski-) closure of $a^U \cup \{0\}$, is a subgroup of W as well (see [1, Proposition 1.3(b)]).

Subclaim (c). $\overline{a^U \cup \{0\}} = a^{\mathscr{D}} \cup \{0\}$.

First show $a^{\mathscr{D}} \cup \{0\}$ is closed in W: By [8, p. 60] each orbit in W is a locally closed subset of W whose boundary is a union of orbits of strictly lower dimension. So by Subclaim (b) the boundary of $a^{\mathscr{D}}$ is empty or $\{0\}$. [Since $\mathscr{D}$ is one-dimensional, any orbit is at most one-dimensional.] Hence $a^{\mathscr{D}} \cup \{0\}$ is closed.

So $\overline{a^U \cup \{0\}}$ is an infinite closed subset of $a^{\mathscr{D}} \cup \{0\}$ which is closed, irreducible and one-dimensional. Thus $\overline{a^U \cup \{0\}} = a^{\mathscr{D}} \cup \{0\}$ is a subgroup of W.

Now we are in the situation to apply Zil'ber's field theorem, see [12, Theorem 3.7], in the theory of the algebraically closed field $\tilde{F}$:

V_s is an infinite, definable, abelian group acting (definably) faithfully on the infinite abelian group $a^{\mathscr{D}} \cup \{0\}$ which is V_s-minimal (since it is an orbit). So there is a definable field $\mathscr{K}$ with $\mathscr{K}^+ \simeq a^{\mathscr{D}} \cup \{0\}$ and the action of V_s on $a^{\mathscr{D}} \cup \{0\}$ corresponds to multiplication in $\mathscr{K}$; or in our case $\mathscr{K}^* \simeq V_s$. We have K definably (over L) embedded in $\mathscr{K}$.

Now $\mathscr{K}$ is $\tilde{F}$-definably isomorphic to $\tilde{F}$, by [12, Theorem 4.15], via a map χ which is defined over some extension L' of F. χ carries K into a subfield of some finite extension of F. (Notice: Since algebraically closed fields have quantifier elimination, the defining formula of χ can be interpreted in F for elements of K, i.e., χ restricted to K is definable in F.) □

Main Theorem 3.6. *Any infinite field K which is interpretable in a separably closed field F of a finite Eršov-invariant is definably isomorphic to a finite (hence purely inseparable) extension of F.*

Proof. By 3.5 K is definably isomorphic to a subfield E of a finite extension L of F. So by 3.2 and 3.3 E contains F^{p^l} for some $l < \omega$. But F^{p^l} is definably isomorphic to F via $x \mapsto \sqrt[p^l]{x}$ which carries E to a finite extension of F. □

Note. The proof also shows that K is definably isomorphic to a subfield k of F such that k is a finite extension of F^{p^l} for some $l < \omega$.

Remark 3.7. Any finite extension L of a separably closed field F of finite Eršov-invariant is itself separably closed and of the same Eršov-invariant.

Proof. A field K is separably closed iff the minimal polynomial over K of any algebraic element over K is of the form $x^{p^m} - c$, $c \in K$. So let a be an element algebraic over L. Then the minimal polynomial $\min_L(a)$ of a over L divides the minimal polynomial $\min_F(a)$ of a over F. But $\min_F(a)$ is of the form $x^{p^m} - c$, $c \in F$, which has only one root (in $\tilde{F}$). Hence $\min_L(a)$ cannot be separable (i.e., cannot have distinct roots).

To see that L has the same invariant as F let $e(K)$ denote the Eršov-invariant of a field K of characteristic p. Clearly $e(L) \leq e(F)$ (to increase e we have to adjoin transcendentals). On the other hand $[L : F] < \omega$, so there is $n < \omega$ such that $L^{p^n} \leq F$ and $[F : L^{p^n}]$ is finite. $e(L) = e(L^{p^n})$ since for $\{a_1, \ldots, a_e\}$ a p-basis of L, $\{a_1^{p^n}, \ldots, a_n^{p^n}\}$ is a p-basis of L^{p^n}. Therefore, as above, $e(F) \leq e(L^{p^n}) = e(L)$ which gives $e(F) = e(L)$. □

Now we want to discuss the question whether finite extensions of $F (\models \mathrm{SCF}_e)$ are (definably) isomorphic to F. Note: If F is a saturated model of SCF_e,

then any finite extension L of F is also saturated, since L is definable in F. Hence L is isomorphic (but not necessarily definably so) to F with respect to the pure field language.

Proposition 3.8. *Any definable field endomorphism* $\Phi\colon F \to E$ *onto a subfield* $E \leq F$ *is of the form* $x \mapsto x^{p^n}$ *for some* $n \geq 0$.

Proof. By compactness (as in the proof of 2.4) there are rational functions $R_1, \ldots, R_m$ over F such that $\forall x \in F$, $\Phi(x) \in \{R_1(\overline{x_\sigma}), \ldots, R_m(\overline{x_\sigma})\}$ where, as usual, $\overline{x_\sigma} = (x_{\sigma_1}, \ldots, x_{\sigma_{p^e \cdot l}})$, $|\sigma_i| = l$. So for $x \in F^{p^l}$,

$$x \in \{R_1(x_{\overline{0}}, 0, \ldots, 0), \ldots, R_m(x_{\overline{0}}, 0, \ldots, 0)\}$$

where $\overline{0} = \langle 0, \ldots, 0\rangle$. Note: $x_{\overline{0}} = \sqrt[l]{x}$. Let $R_i'(y) = R_i(y, 0, \ldots, 0)$.

Let $F^{p^\infty} = \bigcap_{n\in\omega} F^{p^n}$ an algebraically closed field.

Claim. $\Phi|_{F^{p^\infty}}$, Φ restricted to F^{p^∞}, is a field endomorphism of F^{p^∞} which definable in F^{p^∞} as an algebraically closed field.

Clearly Φ induces a field endomorphism of F^{p^∞}. Since $F^{p^\infty} \subseteq F^{p^l}$, $\Phi(x) \in \{R_i'(\sqrt[l]{x})\colon i = 1, \ldots, m\}$ for $x \in F^{p^\infty}$. For any definable set $A \subseteq F$ there is $N < \omega$ such that for all $n \geq N$, $A \cap F^{p^n}$ is finite or cofinite in F^{p^n} (same proof as in 3.1). So for any F-definable subset A of F, $A \cap F^{p^\infty}$ is finite or cofinite in F^{p^∞} and therefore $\widetilde{F}$-definable (as an algebraically closed field). Furthermore there is $j \in \{1, \ldots, m\}$ such that $\Phi(x) = R_j'(\sqrt[l]{x})$ for all but finitely many $b_1, \ldots, b_k \in F^{p^\infty}$.

Now let X be the graph of the function $\Theta\colon \widetilde{F} \to \widetilde{F}$ given by

$$\Theta(x) = \begin{cases} R_j'(\sqrt[l]{x}) & \text{if defined and } x \notin \{b_1, \ldots, b_k\}, \\ 0 & \text{if } R_j'(\sqrt[l]{x}) \text{ is not defined and } x \notin \{b_1, \ldots, b_k\}, \\ \Phi(b_i) & \text{if } x = b_i. \end{cases}$$

X is definable in $\widetilde{F}$. $F^{p^\infty} \prec \widetilde{F}$ as algebraically closed fields. So by definability of types for stable theories (see [11]), $X \cap (F^{p^\infty} \times F^{p^\infty})$ is definable in F^{p^∞}. But $X \cap (F^{p^\infty} \times F^{p^\infty})$ is the graph of $\Phi|_{F^{p^\infty}}$. This proves the claim.

So $\Phi|_{F^{p^\infty}}$ is of the form $x \mapsto x^{p^n}$ for some $n \in \mathscr{Z}$, since any definable field endomorphism of an algebraically closed field of characteristic p is such, see [12, p. 77].

Now consider $L = \{x \in F\colon \Phi(x) = x^{p^n}\}$. L is an infinite, definable subfield of F, hence contains F^{p^l} for some $l \geq 0$. But if $\Phi(x) = x^{p^n}$ for all $x \in F^{p^l}$ then for an arbitrary $x \in F$, $\Phi(x) = y$ implies $\Phi(x^{p^l}) = y^{p^l} = (x^{p^n})^{p^l}$. So $y = x^{p^n}$ for $\Phi(x) = x^{p^n}$ for all $x \in F$. Furthermore $n \geq 0$ otherwise Φ would not be defined on all of F. □

Corollary 3.9. *Let* $F \models \mathrm{SCF}_e$ *with* $e < \omega$.

(a) *If* $e = 1$ *then any finite extension* L *of* F *is definably isomorphic to* F *(with respect to the pure language of fields).*

(b) *For* $2 \leq e < \omega$ *there are finite extensions* L *of* F *which are not definably isomorphic to* F.

Note. Since L is definable in F and F is definable in L, it is irrelevant whether we work in L or in F.

Proof. (a) If $e = 1$, any finite extension L of F is of the form $F(\sqrt[p^m]{a})$ for some $m < \omega$, where $\{a\}$ is the p-basis of F. Then it is easy to see that $F = L^{p^m}$.

(b) For $\{a_1, \ldots, a_e\}$ a p-basis of F, let $L = F(\sqrt[q]{a_1})$. By Proposition 3.8, any definable field endomorphism of L is of the form $x \mapsto x^{p^n}$. Hence it is either the identity on L or it is not surjective onto F. □

4. The infinite invariant

The following result about separably closed fields of infinite Eršov-invariant emerged from a conversation with A. Macintyre.

Theorem 4.1. *Let K be an infinite field definable in $F \models \mathrm{SCF}_\infty$. Then K is separably closed of infinite Eršov-invariant with* $\mathrm{char}(K) = \mathrm{char}(F) = p$.

Proof. We work in the language of pure fields and view SCF_∞ as $\Pi_{e<\omega}\mathrm{SCF}_e$. This means, if $F_e \models \mathrm{SCF}_e$ for all $e < \omega$ then for any nonprincipal ultrafilter $\mathscr{F}$ on ω the ultraproduct $\prod_{e<\omega} F_e/\mathscr{F} \equiv F$ is a model of SCF_∞.

Now let Φ be the definition of the field K. So there is a filter set $A \in \mathscr{F}$ such that Φ defines a field L_e in F_e. For any filter set $B \in \mathscr{F}$ we have $D = A \cap B \in \mathscr{F}$ and $K \equiv \prod_{e\in D} L_e/\mathscr{F}_D$ where $\mathscr{F}_D = \{X \cap D\colon X \in \mathscr{F}\}$.

Claim. $D = \{e \in A\colon L_e \text{ is infinite}\} \in \mathscr{F}$.

Suppose $D \notin \mathscr{F}$. Then $S = \{e \in A\colon L_e \text{ is a finite field}\} = (\omega\backslash D) \cap A \in \mathscr{F}$. So, by the above, $K \equiv \prod_{e\in S} L_e/\mathscr{F}_S$, which is a pseudofinite field. But this contradicts the stability of K, since pseudofinite fields are unstable, see [6]. This proves the claim.

Hence $D \in \mathscr{F}$ and $K \equiv \prod_{e\in D} L_e/\mathscr{F}_D$. By 3.6 and 3.7, L_e is a separably closed field of characteristic p of Eršov-invariant e for all $e \in D$. It follows that K is separably closed of characteristic p. K has infinite Eršov invariant since $\{e \in D\colon e > e_0\} \in \mathscr{F}_D$ for all $e_0 \in \omega$. □

References

1. A. Borel, *Linear algebraic groups*, 2nd ed., Springer-Verlag, Berlin and New York, 1991.
2. E. Bouscaren, *Model-theoretic version of Weil's theorem on pregroups*, The Model Theory of Groups (A. Nesin and A. Pillay, eds.), Univ. of Notre Dame Press, 1989, pp. 177–185.
3. Z. Chatzidakis, G. Cherlin, S. Shelah, G. Srour, and C. Wood, *Orthogonality in separably closed fields*, Classification Theory (J. Baldwin, ed.), Springer, New York and Berlin, 1985, pp. 72–88.
4. G. Cherlin and S. Shelah, *Superstable fields and groups*, Ann. Math. Logic **18** (1980), 227–270.
5. F. Delon, *Ideaux et types sur les corps séparablement clos*, Suppl. Bull. Soc. Math. France, Mém. 33, Tome **116** (1988).
6. J.-L. Duret, *Les corps pseudo-finis ont la propriété d'indépendance*, C. R. Acad. Sci. Paris Sér. I Math. **290** (1980), 981–983.
7. Ju. L. Eršov, *Fields with a solvable theory*, Dokl. Akad. Nauk SSSR **174** (1967), 19–20; English transl., Soviet Math. Dokl. **8** (1967), 575–576.
8. J. E. Humphreys, *Linear algebraic groups*, Springer-Verlag, Berlin and New York, 1975.
9. N. Jacobson, *Lectures in abstract algebra.* III, Van Nostrand, Princeton, NJ, 1964.
10. A. Macintyre, *On ω_1-categorical theories of fields*, Fund. Math. **71** (1971), 1–25.
11. A. Pillay, *An introduction to stability theory*, Clarendon Press, Oxford, 1983.

12. B. Poizat, *Groupes stables*, Nur alMantiq walMa'arifah, Villeurbanne, 1987.
13. M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math. **78** (1956), 401–443.
14. G. Srour, *The independence relation in separably closed fields*, J. Symbolic Logic **51** (1986), 715–725.
15. L. P. D. van den Dries, *Definable groups in characteristic* 0 *are algebraic groups*, Abstracts Amer. Math. Soc. **3** (1982), 142.
16. ———, *Weil's group chunk theorem: a topological setting*, Illinois J. Math. **34** (1990), 127–139.
17. A. Weil, *On algebraic groups of transformations*, Amer. J. Math. **77** (1955), 203–271.
18. C. Wood, *Notes on the stability of separably closed fields*, J. Symbolic Logic **44** (1979), 412–416.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, INDIANA UNIVERSITY, SOUTH BEND, INDIANA 46634-7111

E-mail address: mmessmer%mathcs%iusb@vines.iusb.indiana.edu