Model theory of endomorphisms of separably closed fields

Zoé Chatzidakis – CNRS, Université Paris 7
Ehud Hrushovski [1,2] – Hebrew University

Introduction. The original motivation of this paper was to study the asymptotic theory of the difference fields $(\mathbb{F}_p(t)^s, x \mapsto x^p)$ as p goes to ∞, where $\mathbb{F}_p(t)^s$ denotes the separable closure of the field $\mathbb{F}_p(t)$. For each p, the field $\mathbb{F}_p(t)^s$ has a rich structure. For instance, the endomorphism $x \mapsto x^p$ is definable, as is the derivation D_p which satisfies $D_p(t) = 1$ (in the pure field language augmented by a constant symbol for t).

The asymptotic theory of the differential fields $(\mathbb{F}_p(t)^s, D_p)$ was shown in [5] to be undecidable. Moreover, the map $x \mapsto x^p$ is definable, uniformly in p, in the differential field $(\mathbb{F}_p(t)^s, D_p)$. In this paper we show that, a contrario, the asymptotic theory of the difference fields $(\mathbb{F}_p(t)^s, x \mapsto x^p)$ is decidable. It would be interesting to see where exactly the border between decidability and undecidability lies, among asymptotic theories of reducts of the differential fields $(\mathbb{F}_p(t)^s, D_p)$. Other canonical theories in characteristic p are the theory of algebraically closed valued fields with distinguished Frobenius, and the theory of differentially closed fields with distinguished Frobenius. The asymptotic theory is decidable in both these cases. The differential case depends on the results of this paper. These facts, mentioned for the sake of comparison, will be shown elsewhere.

The study of the asymptotic theory of these difference fields led naturally to the concept of generic endomorphisms of fields, subject to certain constraints (K is a regular extension of the perfect closure of $\sigma(K)$). The theory of these difference fields, denoted SCFE_e, is then model complete in a language extending the language of difference fields: if $K \subset L$ are models of SCFE_e, and K and $\sigma(L)$ are linearly disjoint over $\sigma(K)$, then $K \prec L$. Many of the results obtained for the theory ACFA of generic difference fields (see (1.13) for a definition) generalise easily to this context, and we obtain for instance the decidability of the theories SCFE_e, a description of their completions, of the types, of independence (including the independence theorem over algebraically closed sets, which shows that their completions are simple). Much of this study depends on results obtained for the reducts to the language of pairs (namely, the pair $(K, \sigma(K))$, for (K, σ) a field with generic endomorphism σ). In addition, given a model (K, σ) of SCFE_e, we investigate a few natural difference fields associated to K: its inversive closure, its perfect closure and the field $k = \bigcap_{n \in \mathbb{N}} \sigma^n(K)$. We show that they are models respectively of ACFA, SCFE_0 (provided K is ω-saturated), and ACFA. Furthermore, the only structure induced on k by K is the difference field structure, and k is stably embedded. Let us mention a result of independent interest involved in the proof of this last statement:

Theorem (5.3). Let L be a model of ACFA, and let $A \subset B$ be algebraically closed inversive difference subfields of L. Assume that if $b \in B$ is transformally algebraic over A, then $b \in A$. Then $tp(B/A)$ is stationary.

The machinery and results holding for models of ACFA also yield a characterisation of definable modular sets: they have finite SU-rank and are orthogonal to all fixed fields.

The paper is organised as follows. Section 1 contains a review of separably closed fields and difference fields, and sets up the notation. Section 2 studies pairs of separably

[1]Supported by the Israel Science Foundation
[2]Research carried out for the Clay Mathematics Institute as a Clay Prize research fellow

closed fields (the inclusion not being an elementary one: the larger field contains the algebraic closure of the smaller field). Section 3 gives the axiomatisation of the theory of separably closed fields with a generic endomorphism, and shows that it is model complete in a natural language. It also shows that non-principal ultraproducts of the difference fields $(\mathbb{F}_p(t)^s, x \mapsto x^q)$ are models of this theory. Section 4 studies the elementary invariants, algebraic closure and independence, and gives a proof of the independence theorem. Section 5 studies the induced structure on the various difference fields which "live" in our models. Section 6 gives results on modular sets. Appendix A discusses the notion of "stationarity almost over a predicate", and Appendix B gives a proof of Claim (5.3) not relying on the results of [13].

1 Preliminaries

In this section we review classical results on separably closed fields (and fields of characteristic $p > 0$), on difference fields and on models of ACFA. We assume familiarity with the basic notions of algebraic geometry: algebraic sets and varieties (or absolutely irreducible algebraic sets), generic points of varieties, dominant morphisms, linear disjointness, separable, primary and regular extensions, see e.g. Ch. I to III in [16]. For an introduction to classical model theory, one can consult [11].

(1.1). Setting and notation. We will always work inside a large algebraically closed field Ω, which will contain all fields considered. If K and L are subfields of Ω, we denote by KL the subfield of Ω composite of K and L, by K^s the separable closure of K inside Ω, i.e., the set of elements of Ω which are separably algebraic over K, and by K^{alg} the set of elements of Ω which are algebraic over K. Throughout the main body of the paper, $\mathcal{L}$ will denote the language of rings $\{+, -, \cdot, 0, 1\}$, $\mathcal{L}_C$ the language $\mathcal{L} \cup \{C\}$, where C is a unary relation symbol, and $\mathcal{L}_\sigma$ the language $\mathcal{L} \cup \{\sigma\}$, where σ is a unary function symbol.

Let p be the characteristic of Ω, and K a subfield of Ω, $n \in \mathbb{N}$. *Frob* will denote the identity map if $p = 0$, and the Frobenius automorphism $x \mapsto x^p$ if $p > 0$. For $n \in \mathbb{Z}$, K^{p^n} denote the subfield of Ω image of K by $Frob^n$, and $K^{p^\infty} = \bigcap_{n \in \mathbb{N}} K^{p^n}$, and $K^{p^{-\infty}} = \bigcup_{n \in \mathbb{N}} K^{p^{-n}}$ the *perfect closure* of K. Thus, if $p = 0$, all these fields are equal to K.

(1.2). p-bases. Up till (1.10), we assume $p > 0$. Details and proofs can be found in [1] §13. Let K be a subfield of Ω and k a subfield of K. Then kK^p is a subfield of K, and so K is a kK^p-vector space. We say that elements $b_1, \dots, b_n \in K$ are *p-independent over k* if the set of *p-monomials in* $b_1, \dots, b_n$, i.e., monomials of the form $b_1^{i(1)} \cdots b_n^{i(n)}$ with $0 \le i(1), \dots, i(n) \le p - 1$, is linearly independent in the kK^p-vector space K. Equivalently, if $b_i \notin kK^p(b_1, \dots, b_{i-1})$ for $i = 1, \dots, n$.

A subset B of K is *p-independent* over k if every finite subset of B is p-independent over k. If $B \subset K$ is not p-independent over k, then there is a finite subset B_0 of B and $b \in B \setminus B_0$ such that $b \in kK^p[B_0]$. A maximal p-independent over k subset of K is called a *p-basis of K over k*; if B is a p-basis of K over k, then $K = kK^{p^n}[B]$ for any $n \in \mathbb{N}$. Any two p-bases of K over k have the same cardinality. A *p-basis of K* is a p-basis of K over $\mathbb{F}_p$. We define the *degree of imperfection* of a field K as follows: if K has a finite p-basis B, then it is the size of B, and otherwise it is ∞. Observe that if B is a p-basis of K over k, then B is also a p-basis of K^s over k and over k^s, and the elements of B are algebraically independent over k.

(1.3). Recall that K is a *separable* extension of k if k and K^p are linearly disjoint over k^p. Equivalently, if any p-basis of k extends to a p-basis of K. If $B \subset K$ is a transcendence basis of K over k such that K is separably algebraic over $k(B)$, then B is called a *separating transcendence basis* of K over k. If K is finitely generated and separable over k then K has a separating transcendence basis over k. This result does not hold when K is infinitely generated over k: if t is transcendental over k, then the field $\bigcup_{n\in\mathbb{N}} k(t^{p^{-n}})$ is a separable extension of k, but does not have a separating transcendence basis over k. If $B \subset K$ is such that K is separably algebraic over $k(B)$, then B will contain a p-basis of K over k, and therefore a separating transcendence basis of K over k is always a p-basis of K over k. The converse however only holds if K is finitely generated over k as a field.

(1.4). The λ-functions.

For each n fix an enumeration $m_{i,n}(\bar{x})$ $(0 \leq i < p^n)$ of the p-monomials $x_1^{i(1)} \cdots x_n^{i(n)}$ with $0 \leq i(1), \dots, i(n) \leq p-1$, and define the $(n+1)$-ary functions $\lambda_{i,n} : K^n \times K \to K$ as follows: If the n-tuple $\bar{b}$ is not p-independent, or if the $(n+1)$-tuple $(\bar{b}, a)$ is p-independent, then $\lambda_{i,n}(\bar{b}; a) = 0$. Otherwise, the $\lambda_{i,n}(\bar{b}; a)$ satisfy

$$a = \sum_{i=0}^{p^n-1} \lambda_{i,n}(\bar{b}; a)^p m_{i,n}(\bar{b}).$$

Note that these functions depend on the field K, and that the above properties define them uniquely. These functions are definable in the pure ring K, and we call them the *λ-functions of* K. One checks easily that a subfield k of K is closed under the λ-functions of K if and only if K is a separable extension of k. Furthermore, if k is closed under the λ-functions of K and $a \in k^s$, then $k(a)$ is also closed under the λ-functions of K, since $k(a) = k(a^p)$.

(1.5). Separably closed fields. For each $e \in \mathbb{N} \cup \{\infty\}$, the theory expressing that K is a separably closed field of degree of imperfection e, is a complete theory (Ershov [10]), which we denote by SCF_e, and is stable (Wood [19]). If K is separably closed and $\{b_1, \dots, b_e\}$ is a p-basis of K, then $\mathrm{SCF}_{e,b} = Th(K, b_1, \dots, b_e)$ is model complete in the language $\mathcal{L}(b_1, \dots, b_e)$ and eliminates imaginaries. By a result of Delon [8], in the language $\mathcal{L}_\lambda = \{+, \cdot, 0, 1, \lambda_{i,n}, n \in \mathbb{N}, 0 \leq i < p^n\}$, the theory of separably closed fields, expanded by axioms expressing the defining properties of the λ-functions, eliminates quantifiers; its completions are obtained by specifying the degree of imperfection. We will fix a bijection between the set of pairs (i, n) with $n \in \mathbb{N}$ and $0 \leq i < p^n$ and a set I.

(1.6). Algebraic and definable closures in separably closed fields.

We fix a degree of imperfection $e \in \mathbb{N} \cup \{\infty\}$, a separably closed field K of degree of imperfection e and characteristic $p > 0$. The model theoretic results on separably closed fields which appear below can be found in [8].

Let B be a subfield of K. Then $dcl_K(B)$, the definable closure of B in the field K, is the field generated by closing B under the λ-functions of K. The algebraic closure of B, denoted by $acl_K(B)$, is the separable closure of $dcl_K(B)$.

(1.7). Generics in separably closed fields. Let K be as above, $B = acl_K(B) \subseteq K$, and let $n \in \mathbb{N}$. By stability of SCF_e, the generic n-type over B is unique. Let $a = (a_1, \dots, a_n) \in K^n$. The following are necessary and sufficient conditions for $tp(a_1, \dots, a_n/B)$ to be generic:

(1) If $e = 0$, $a_1, \dots, a_n$ are algebraically independent over B.

(2) If $e = \infty$, then $a_1, \dots, a_n$ are p-independent over B in K.

(3) Assume $e \in \mathbb{N}$ and B contains a p-basis $\{b_1, \dots, b_e\}$ of K, and define A_m by induction on m as follows: $A_0 = \{a_1, \dots, a_n\}$; $A_{m+1} = \{\lambda_{i,e}(b_1, \dots, b_e; b) \mid b \in A_m, 0 \leq i < p^e\}$. Then for each m the elements of A_m are algebraically independent over B. Note also that $dcl_K(B, a) = B(A_m \mid m \in \mathbb{N})$.

(4) Assume $e \in \mathbb{N}$, $\{b_1, \dots, b_f\}$ is a p-basis of B, and $f < e$. If $n \geq (e - f)$ and c is any $(e - f)$-sub-tuple of a, then c is p-independent over B, and $tp(a \setminus c/B(c)^s)$ is the generic $(n - e + f)$-type over $B(c)^s$. If $n \leq e - f$, then a is p-independent over B.

Observation. Assume that $tp(a/E)$ is generic and that B is a subfield of K^{p^∞}. Then $tp(a/EB)$ is also generic: this is because the generic type is orthogonal to all types realised in K^{p^∞}.

(1.8). Forking in separably closed fields. Let K be as above, and $A = acl_K(A)$, $B = acl_K(B)$ and $C = acl_K(C)$ be subsets of K, with $C \subseteq A \cap B$. We will describe necessary and sufficient conditions for $tp(A/B)$ not to fork over C (in that case we also say that A *and* B *are independent over* C). Fix p-bases $A_0 \subset A$ of A over C and $B_0 \subset B$ of B over C.

(a) If $e = \infty$, then A and B are independent over C if and only if $A_0 \cup B_0$ remain p-independent over C in K, and A and B are linearly disjoint over C.

(b) If $e \in \mathbb{N}$ and one of A_0, B_0 is empty, then A and B are independent over C if and only if they are linearly disjoint over C.

(c) Assume that $e \in \mathbb{N}$, and $A_0, B_0 \neq \emptyset$. Then $tp(A/B)$ does not fork over C if and only if $tp(A_0/B)$ does not fork over C, and $tp(A/B, A_0)$ does not fork over (C, A_0). Clearly, $tp(A_0/B)$ does not fork over C if and only if A_0 realises the generic $|A_0|$-type over B. Hence, $tp(A/B)$ does not fork over C if and only if A_0 realises the generic $|A_0|$-type over B, and A and $dcl_K(A_0, B)$ are linearly disjoint over $dcl_K(C, A_0) = C(A_0)$.

Assume that A and B are independent over C. In cases (a) and (b), the composite field AB is closed under the λ-functions of K, and therefore $dcl_K(A, B) = AB$, $acl_K(A, B) = (AB)^s$. In case (c), we get $dcl_K(A, B) = A dcl_K(A_0, B)$, and therefore $acl_K(A, B) = (A dcl_K(A_0, B))^s$. By (1.7)(3), $dcl_K(A_0, B)$ is the union of purely transcendental extensions of B, and we get $dcl_K(A, B) = \bigcup_m AB(A_m)$ (in the notation of (1.7)(3)).

(1.9). Remarks. Let $K \models \mathrm{SCF}_e$.

(1) Let $A = dcl_K(A) \subseteq K$, and let B be a countable subset of K. Then $dcl_K(A, B)$ is countably generated over A. If $B \subseteq A^{alg}$, then $dcl_K(A, B) = A(B)$.

(2) Let $A = dcl_K(A)$, $B = dcl_K(B)$ and $C = dcl_K(C)$ be subfields of K, with $C \subseteq A \cap B$, and $tp(A/B)$ not forking over C. The following conditions are equivalent:

   (i) $tp(A/C)$ has a unique non-forking extension to B.

   (ii) A and $B \cap C^s$ are linearly disjoint over C.

Proof. (1) The second assertion is obvious. For the first assertion, if $e \in \mathbb{N}$, this is clear. If $e \in \infty$, see [8].

(2) That (i) implies (ii) is clear. Assume (ii) holds, and note that it implies that $A \otimes_C B$ is an integral domain, with field of fractions the field AB. Hence, if AB is closed under the λ-functions of K, then $dcl_K(AB) = AB$, so that (i) is clear.

Let us therefore assume that AB is not closed under the λ-functions of K, and let A_0 be a p-basis of A over C. Our assumption implies that $tp(A_0/B)$ is the generic $|A_0|$-type over B, which is unique. To conclude, it will suffice to show that $tp(A/A_0C)$ has a unique non-forking extension to $dcl_K(B, A_0)$. Note that $dcl_K(C, A_0) = C(A_0)$. The description of $dcl_K(B, A_0)$ given in (1.7) shows that $dcl_K(B, A_0)$ is a primary extension of $B(A_0)$. Hence $dcl_K(B, A_0) \cap C(A_0)^s = B(A_0) \cap C(A_0)^s = (B \cap C^s)(A_0) = C(A_0)$. Then, $Adcl_K(B, A_0)$ is closed under the λ-functions of K, and using the previous case, $tp(A/C, A_0)$ has a unique non-forking extension to $dcl_K(B, A_0)$.

(1.10). Difference rings and fields. Difference fields were first studied by Ritt in the 1930's; we recall briefly definitions and some results, which can be found in Cohn's book [7]. Unless otherwise indicated, the references are to [7].

A *difference ring* is a ring R with a distinguished injective endomorphism σ, and a *difference field* is a difference ring which is a field. A difference ring R is naturally an $\mathcal{L}_\sigma$-structure, where $\mathcal{L}_\sigma = \{+, \cdot, 0, 1, \sigma\}$. If $\sigma(R) = R$ then R is called an *inversive* difference ring. If S is an inversive difference ring containing R such for every $a \in S$ there is $n \in \mathbb{N}$ such that $\sigma^n(a) \in R$, then S is called an *inversive closure of* R. Any two inversive closures of R are R-isomorphic; if R is a domain, so is its inversive closure ([2.5.2]).

(1.11). Difference polynomial rings. Let k be a difference field contained in an inversive difference field Ω, and let $X_1, \dots, X_n$ be indeterminates. We define the *difference polynomial ring* $k[X_1, \dots, X_n]_\sigma$ by taking the ring $k[X_1, \dots, X_n]_\sigma$ to be the ordinary polynomial ring $k[\sigma^j(X_i) \mid i = 1, \dots, n, j \in \mathbb{N}]$, and extending σ to $k[X_1, \dots, X_n]_\sigma$ in the way suggested by the name of the generating elements. Note that σ is not onto. The order of a difference polynomial f is the largest m such that some indeterminate $\sigma^m(X_i)$ appears in f.

Ideals I of $k[X_1, \dots, X_n]_\sigma$ satisfying $\sigma(I) \subseteq I$ are called *σ-ideals.* A *perfect* σ-ideal of $k[X_1, \dots, X_n]_\sigma$ is a σ-ideal I satisfying moreover that $a\sigma(a^m) \in I$ implies $a \in I$ for all $m \in \mathbb{N}$. Thus a perfect σ-ideal is radical. A *prime σ-ideal* is a σ-ideal which is prime and perfect. Quotients of $k[X_1, \dots, X_n]_\sigma$ by prime σ-ideals are difference domains, on which σ defines an embedding. While $k[X_1, \dots, X_n]_\sigma$ has infinite ascending chains of σ-ideals, it satisfies the ascending chain condition on perfect σ-ideals and on prime σ-ideals ([3.8.5]); in particular, every perfect σ-ideal of $k[X_1, \dots, X_n]_\sigma$ is a finite intersection of prime σ-ideals.

Let a be a tuple of elements of Ω. We denote by $I_\sigma(a/k)$ the ideal of $k[X]_\sigma$ (X a tuple of indeterminates of the same length as a) of difference polynomials vanishing at a. Then $I_\sigma(a/k)$ is a prime σ-ideal.

The difference field generated by a over k is denoted by $k(a)_{\mathbb{N}}$, and if k is inversive, then $k(a)_{\mathbb{Z}}$ denotes the inversive closure of $k(a)_{\mathbb{N}}$, i.e., the difference field $k(\sigma^i(a) \mid i \in \mathbb{Z})$.

(1.12). Transformal transcendence bases. Let $k \subseteq \Omega$ be as above, and let a be a tuple of elements of Ω. If the transcendence degree $tr.deg(k(a)_{\mathbb{N}}/k)$ of $k(a)_{\mathbb{N}}$ over k is finite then we say that a is *transformally algebraic over* k. In that case, there is a non-negative integer m such that $k(a)_{\mathbb{N}} \subseteq k(a, \dots, \sigma^m(a))^{alg}$.

An element $b \in \Omega$ is *transformally transcendental over* k if the elements $\sigma^i(b)$, $i \in \mathbb{N}$, are algebraically independent over k. Observe that a tuple a is either transformally algebraic over k, or contains an element which is transformally transcendental over k. We call a set $B \subseteq \Omega$ *transformally independent* over k if the elements $\sigma^j(b)$, $b \in B$, $j \in \mathbb{N}$, are algebraically independent over k. If K is a difference subfield of Ω containing k, and $B \subset K$ is transformally independent over k and maximal such, then B is called a *transformal transcendence basis* of K over k. Observe that K is then transformally algebraic over $k(B)_{\mathbb{N}}$ ([5.5.1]). Any two transformal transcendence bases of K over k have the same cardinality, and this cardinality is called the transformal transcendence degree of K over k, and denoted by $\Delta(K/k)$ (see [5.5.2]). If a is a finite tuple, we also define $\Delta(a/k) = \Delta(k(a)_{\mathbb{N}}/k)$; observe that $\Delta(a/k) \leq tr.deg(k(a)/k)$ (the transcendence degree of $k(a)$ over k).

(1.13). The theory ACFA

Recall that the model companion ACFA of the theory of inversive difference fields in the language $\mathcal{L}_\sigma$ is axiomatised by the scheme of axioms expressing the following properties of (K, σ):

(i) K is an algebraically closed field and σ is an automorphism of K.

(ii) If U and V are varieties defined over K and of the same dimension, such that $V \subseteq U \times \sigma(U)$ and the projections $V \to U$ and $V \to \sigma(U)$ are dominant, then there is a tuple a such that $(a, \sigma(a)) \in V$ (here $\sigma(U)$ denotes the variety image by σ of the variety U).

Models of ACFA are called *generic difference fields*.

(1.14). Conventions. Unless otherwise stated, we will always view difference fields as $\mathcal{L}_\sigma$-structures. If K is a difference subfield of the difference field L, then $K \subseteq L$. Fix a sufficiently saturated model (Ω, σ) of ACFA. The uniqueness of the inversive closure of a difference field and the universal properties of Ω imply the following:

If $K \subset \Omega$ is a separably closed difference field, and L is a difference field containing K, with $|L| < |\Omega|$, then there is an $\mathcal{L}_\sigma(K)$-embedding of L in Ω.

From now on, all difference fields considered will be difference subfields of Ω, unless otherwise stated. Thus, if k is a difference subfield of Ω, then the inversive closure of k is simply $\bigcup_{n\in\mathbb{N}} \sigma^{-n}(k)$.

(1.15). Proposition ((2.11) in [4]). Let K be a difference subfield of Ω, and $n > 0$. If a and b are two n-tuples of transformally transcendental elements over K, then $tp_\Omega(a/K) = tp_\Omega(b/K)$, i.e., the $\mathcal{L}_\sigma(K)$-isomorphism which sends a to b extends to the algebraic closure of $K(a)_\mathbb{Z}$.

(1.16). Algebraic closure, independence and SU-rank in models of ACFA. We work in (Ω, σ). Recall from [4] that the model-theoretic algebraic closure of a subset A of Ω is the smallest algebraically closed inversive difference subfield of Ω containing A, and we denote it by $acl_\sigma(A)$. Hence, if k denotes the prime subfield of Ω, then $acl_\sigma(A) = k(A)_\mathbb{Z}^{alg}$.

If A, B, C are subsets of Ω, we say that A *and* B *are independent over* C if $acl_\sigma(AC)$ and $acl_\sigma(BC)$ are linearly disjoint over $acl_\sigma(C)$. This does correspond to non-forking in models of ACFA.

Let $A = acl_\sigma(A) \subset \Omega$, and assume that $|A| < |\Omega|$. Let a be a tuple of elements of Ω. The SU-rank of a over A, $SU(a/A)$, is a rank based on forking, defined in the same way the U-rank is. The reader may consult [4] for details. Here we only need the dichotomy finite/infinite, which is easy to describe:

The tuple a has *finite SU-rank over* A iff a is transformally algebraic over A, and otherwise a has *infinite SU-rank over* A. If $S \subseteq \Omega^n$ is the set of realisations of some set of types over A, then S has *finite SU-rank* iff all its elements have finite SU-rank over A, and *infinite SU-rank* otherwise.

(1.17). Definition of modularity. Let T be a complete simple theory, M a sufficiently saturated model of T. Recall that M^{eq} is the multi-sorted structure obtained by adding to M all the imaginary elements of M (i.e., all equivalence classes of 0-definable equivalence relations), and that if $A \subset M^{eq}$ then $acl^{eq}(A)$ denotes the algebraic closure of A in the structure M^{eq}. Assume that T eliminates hyperimaginaries (i.e., if $a \in M^\omega$ and R is a type-definable equivalence relation on M^ω, then the R-equivalence class of a is equidefinable with some subset of M^{eq}), let $D \subseteq M^n$ be invariant under $Aut(M/E)$, for some $E = acl(E) \subset M$. We say that D is *modular* (also called *one-based*) if whenever a and b are tuples of elements of D, then a and b are independent over $C = acl^{eq}(Ea) \cap acl^{eq}(Eb)$.

As ACFA eliminates imaginaries (and hyperimaginaries) we have that $acl^{eq}(E) = acl_\sigma(E)$. Hence, in models of ACFA, modularity translates as:
$D \subseteq \Omega^n$ is modular if and only if whenever a and b are tuples of elements of D, then a and b are independent over $C = acl_\sigma(Ea) \cap acl_\sigma(Eb)$.

In the above condition, one may also replace b by an arbitrary tuple of Ω. For other properties of modularity in models of ACFA, see [4].

(1.18). Orthogonality. Let T be a complete (simple) theory, M a sufficiently saturated model of T, and A, B, subsets of M.

(1) Two complete types p over A and q over B are *orthogonal* if, for any set C containing $A \cup B$, if a realises p and is independent from C over A, and b realises q and is independent from C over B, then a and b are independent over C.

(2) Let $E = acl_\sigma(E)$ be a subset of Ω, and let $S \subseteq \Omega^n$ be a set of realisations of a set of types over E. We say that S is *orthogonal to the fixed fields* if over any set E' containing E, every type realised in S is orthogonal to every type containing a formula of the form $\sigma^n(x) = Frob^m(x)$ for some $n \neq 0$ and $m \in \mathbb{Z}$. The negation of "orthogonal to the fixed fields" is *non-orthogonal to some fixed field.*

(1.19). The dichotomy theorem for ACFA ([4], [6]). Let $D \subseteq \Omega^n$ be definable over an algebraically closed inversive difference field E. If D has infinite SU-rank, then D is not modular. Assume that D has finite SU-rank. If D is not modular then D is non-orthogonal to a fixed field.

If the characteristic of Ω is 0 and D is modular, then every type realised in D is stable, and D is *stably embedded*, i.e., every subset S of D definable in Ω is definable with parameters from D.

(1.20). Theorem ([4], [6]). Let G be an algebraic group defined over Ω, and let B be a definable modular subgroup of $G(\Omega)$. If $X \subseteq G(\Omega)$ is quantifier-free definable, then $X \cap B$ is a Boolean combination of cosets of definable subgroups of B. If $char(\Omega) = 0$, then the same conclusion holds for arbitrary definable subsets X of $G(\Omega)$.

(1.21). Theorem. (Hrushovski [13], Macintyre [17]) Let Q be the set of prime powers, and for each $q = p^n$, let F_q be the difference field $(\mathbb{F}_p^{alg}, x \mapsto x^q)$. Let $\mathcal{U}$ be a non-principal ultrafilter on Q. Then $F = \prod_{q \in Q} F_q/\mathcal{U}$ is a model of ACFA.

2 Pairs of separably closed fields

We are interested in pairs of fields (K, C), where C and K are separably closed, and $C^{alg} \subseteq K$. Note that in particular C is usually not an elementary substructure of K. The examples we have in mind are:

(1) Take a separably closed field K of characteristic p, and consider a non-principal ultraproduct of the pairs (K, K^{p^n}), $n \in \mathbb{N}$.

(2) For each prime p, let K_p be a separably closed field of characteristic p, and q a power of p, and consider a non-principal ultraproduct of the pairs (K_p, K_p^q), p a prime.

(2.1). Setting, conventions and notations. We keep the notation and conventions of (1.1) and (1.14). Besides the characteristic p of Ω, we fix $e_1, e_2 \in \mathbb{N} \cup \{\infty\}$, with $e_1 = e_2 = 0$ if $p = 0$.

We consider the languages $\mathcal{L}_C = \mathcal{L} \cup \{C\}$, where C is a unary predicate, and $\mathcal{L}_0 = \mathcal{L}_C \cup \{R_n \mid n \in \mathbb{N}\} \cup \{\lambda_i^K, \lambda_i^C \mid i \in I\}$, where each R_n is an n-ary relation, and I is the index set defined in (1.5) if $p > 0$, and $I = \emptyset$ if $p = 0$. Let T_C be the $\mathcal{L}_C$-theory, whose models are structures K satisfying: K is a field of characteristic p and of degree of imperfection $\leq e_1$, C is a subfield of K of degree of imperfection $\leq e_2$ and $C^{p^{-\infty}} \subset K$, $C^s \cap K = C$.

Consider now the $\mathcal{L}_0$-theory T_0 obtained by adding to T_C axioms expressing the following properties of the $\mathcal{L}_0$-structure K:

– For each $n \in \mathbb{N}$, $R_n(x_1, \ldots, x_n) \iff$ the elements $x_1, \ldots, x_n$ are linearly independent in the C-vector space K.

– If $p > 0$, the λ_i^K are the λ-functions of K, and the λ_i^C are the λ-functions of C.

(2.2). Notation. We will use the notation of pairs, i.e., the notation (L, D) means that D is the interpretation of C in the model L of T_C. If (K, C) is a model of T_C, then (K, C) expands uniquely to an $\mathcal{L}_0$-structure model of T_0, since the axioms of T_0 uniquely define the interpretation of the symbols R_n and λ_i^K, λ_i^C.

Given a model (K, C) of T_0, we will often work in the $\mathcal{L}$-structure K and in the $\mathcal{L}$-structure C. We will refer to these structures as *the pure fields* K *and* C. Given $A \subset C$ and a tuple a in C, we will denote by $tp_C(a/A)$ the type of a over A in the pure field C, and by $dcl_C(A)$, $acl_C(A)$ the definable and algebraic closure of A in the field C. Similarly, if $A \subset K$ and a is a tuple from K, then $tp_K(a/A)$ will denote the type of a over A in the pure field K, and $dcl_K(A)$, $acl_K(A)$ the definable and algebraic closures of the set A in the field K.

(2.3). Remarks. (1) Note that if (K_1, C_1) is an $\mathcal{L}_0$-structure extending (K, C) and both are models of T_0, then:

– C_1 and K are linearly disjoint over C.

– C_1 is a separable extension of C and K_1 is a separable extension of K.

(2) Assume that (K, C) and (K_1, C_1) are models of T_0, with K a subfield of K_1. Then the inclusion is an inclusion of $\mathcal{L}_0$-structures if and only if the following conditions hold: K and C_1 are linearly disjoint over C; C_1 is a separable extension of C and K_1 is a separable extension of K.

(3) Let (K, C) be a model of T_0, and let a be a tuple in K. Consider the variety V which is the locus of a over C (or rather over C^{alg}) and let k be its field of definition. Then $k \subseteq dcl(a)$. Indeed, without loss of generality (replacing a by a^{p^n} for some integer n), we may assume that $C(a)$ is a separable extension of C, and hence a regular extension of C. Consider the set M of monomials in the elements of the tuple a, and let $M_0 \subset M$ be maximal C-independent. Then all elements of M are in $dcl(a)$, and if $b \in M \setminus M_0$, then b is a C-linear combination of elements of M_0, and the coefficients of this linear combination, being unique, are definable over a.

(4) Let $a \in K$. Then $tp_K(a/C)$ is stationary (as $C^{alg} = C^{p^{-\infty}}$), and we denote by $Cb(tp_K(a/C))$ the intersection of the canonical base $Cb(tp_K(a/C^{alg}))$ of $tp_K(a/C^{alg})$ with C. We know that $Cb(tp_K(a/C^{alg}))$ is the perfect closure of the field generated by the fields of definitions of all algebraic loci over C^{alg} of finite sub-tuples of $dcl_K(a)$. Hence, by (3), $Cb(tp_K(a/C))$ is contained in $dcl(a)$. $Cb(tp_K(a/C))$ can also be described as the smallest subfield A of C such that $A dcl_K(a)$ and C are linearly disjoint over A.

(2.4). Definition. Consider the theory $\mathrm{SCF}_C(e_1, e_2)$ in the language $\mathcal{L}_0$ axiomatised by adding to T_0 the following axioms:

– K and C are separably closed fields, of degree of imperfection e_1 and e_2 respectively.

– $\exists x \, \neg C(x)$.

(2.5). Theorem. Let $(K, C) \subseteq (K_1, C_1), (K_2, C_2)$, where (K_1, C_1) and (K_2, C_2) are models of $\mathrm{SCF}_C(e_1, e_2)$, and $(K, C) \models T_0$. Then $(K_1, C_1) \equiv_K (K_2, C_2)$. Hence, the theory $\mathrm{SCF}_C(e_1, e_2)$ is model-complete and complete. It is the model companion of the theory T_0.

Proof. Passing to elementary extensions, we may assume that (K_1, C_1) and (K_2, C_2) are sufficiently saturated. The proof is a standard back-and-forth argument. We consider the class $\mathcal{I}$ of partial $\mathcal{L}_0$-isomorphisms φ satisfying:

– $Dom(\varphi) = L_1$ contains K, is an $\mathcal{L}_0$-substructure of K_1 and a model of T_0.

– $Im(\varphi) = L_2$ contains K, is an $\mathcal{L}_0$-substructure of K_1 and a model of T_0.

It is enough to show that given $\varphi \in \mathcal{I}$ and $a \in K_1$, there is $\psi \in \mathcal{I}$ extending φ and with a in its domain, and that given $b \in K_2$, there is $\psi \in \mathcal{I}$ extending φ and with b in its image.

Let $a \in K_1$, $\varphi \in \mathcal{I}$ with domain (L_1, D_1) and image (L_2, D_2). We will show that φ extends to an isomorphism $\psi \in \mathcal{I}$, with domain (M_1, E_1) containing a and image (M_2, E_2). We know that L_i is closed under the λ-functions of K_i.

Consider $A = Cb(tp_{K_1}(L_1, a/C_1))$; then $D_1 \subseteq A \subseteq dcl(L_1, a)$ by Remark (2.3)(3), and $tp_{K_1}(L_1, a/A)$ has a unique non-forking extension to C_1. This implies that $tp_{K_1}(a/L_1A)$ has a unique non-forking extension to L_1C_1, i.e., that $(L_1A)^s \cap dcl_K(L_1A, a) = L_1A$.

Let $B \subseteq C_2$ realise $\varphi(tp_{C_1}(A/D_1))$. As C_i and L_i are linearly disjoint over D_i for $i = 1, 2$, φ extends to an isomorphism $\psi : L_1dcl_{C_1}(A) \to L_2dcl_{C_2}(B)$ sending A to B. Let $b \in K_2$ realise the unique non-forking extension of $\psi(tp_{K_1}(a/L_1A))$ to L_2C_2; then ψ extends to an isomorphism $\theta : dcl_{K_1}(L_1dcl_{C_1}(A), a) \to dcl_{K_2}(L_2dcl_{C_2}(B), b)$ sending a to b. By definition of A, we know that $dcl_{K_1}(L_1dcl_{C_1}(A), a)$ and C_1 are linearly disjoint over $dcl_{C_1}(A)$. Our choice of b implies that $dcl_{K_2}(L_2dcl_{C_2}(B), b)$ and C_2 are also linearly disjoint over $dcl_{C_2}(B)$. Hence $\theta \in \mathcal{I}$.

This shows one direction of the back-and-forth argument, and the other one follows by symmetry. Hence $K_1 \equiv_K K_2$. The model completeness of $\mathrm{SCF}_C(e_1, e_2)$ follows by taking $K = K_1$, and its completeness by taking K equal to the prime field. Clearly every model of T_0 embeds in a model of $\mathrm{SCF}_C(e_1, e_2)$ (this is where we use the axiom $C^s \cap K = C$).

(2.6). Corollary. $\mathrm{SCF}_C(e_1, e_2)$ is stable.

Proof. It suffices to count the types. Let (K, C) be a model of $\mathrm{SCF}_C(e_1, e_2)$, and $L \subseteq K$. We may assume that L is a model of T_0. Let $a \in K$. By the proof of Theorem (2.5), $tp(a/L)$ is described by the following data:

– The canonical base A of $tp_K(dcl_K(L, a)/C)$ (see Remarks (2.3)(3) and (4)). Note that $dcl_K(L, a)$ is countably generated over L. As L and C are linearly disjoint over $D = L \cap C$, we obtain that A is countably generated over D. Note also that the elements of A are definable over $L \cup a$. Then $tp(a/L)$ contains the formulas defining the elements of A from $L \cup a$, and also says that elements of $dcl_K(L, a)$ which are A-linearly independent remain C-linearly independent.

– $tp_C(A/D)$: by stability of the theory SCF_{e_2}, there are at most $(|L|)^{\aleph_0}$ possibilities (since A is countably generated over D).

– $tp_K(a/LA)$: again, there are at most $|L|^{\aleph_0}$ possibilities.

(2.7). Corollary. Let (K, C) be a model of $\mathrm{SCF}_C(e_1, e_2)$, and let L be a substructure of K, which is a model of T_0 and is relatively algebraically closed in K. Then L is algebraically closed (in the sense of (K, C)).

Proof. This is immediate from the description of the types given in Corollary (2.6).

(2.8). Corollary. Let $(K, C) \models \mathrm{SCF}_C(e_1, e_2)$. Then there is no induced structure on C, i.e., if $S \subseteq K^n$ is definable, then $S \cap C^n$ is definable in C in the pure field language.

Proof. By stability, $S \cap C^n$ is definable with parameters from C. The result follows from description of types given in Corollary (2.6).

(2.9). Proposition. Let (K, C) be a model of $\mathrm{SCF}_C(e_1, e_2)$, let $(L, D) \subseteq (M, E) \subseteq K$, with L and M algebraically closed in the pair (K, C), and let $a \in K$.

(1) Let A be the canonical base of $tp_K(dcl_K(L, a)/C)$. The following are equivalent:

(i) $tp(a/M)$ does not fork over L.

(ii) $tp_C(A/E)$ does not fork over D, and $tp_K(a/MC)$ does not fork over LA.

(2) $tp(a/L)$ is stationary.

Proof. The fact that $tp(a/L)$ has an extension to M satisfying the conditions of (1)(ii) is clear, and shows that (1)(i) implies (1)(ii). By stability, to prove (1) and (2) it therefore suffices to show that the conditions of (1)(ii) uniquely determine $tp(a/M)$.

Claim. MC is a primary extension of LA.

We know that M and C are linearly disjoint over E, and that each of the extensions $M/(LE)^s$, $(LE)^s/E$, and $C/(EA)^s$, $(EA)^s/E$ is primary. Hence MC is a primary extension of $(LE)^s(EA)^s$.

From the non-forking of $tp_C(A/E)$ over D and the linear disjointness of L and C over D, we deduce that the fields L, A and E are free over D (i.e., each field is free from the composite field of the other two over D). By Remark (1.9) in [4], this implies that $(LE)^{alg}(EA)^{alg} \cap (LA)^{alg} = L^{alg}A^{alg}$, and therefore that

$$MC \cap (LA)^s = (LE)^s(EA)^s \cap (LA)^s = L^{alg}A^{alg} \cap (LA)^s = LA.$$

By Remark (1.9)(2), $tp_K(a/LA)$ has a unique non-forking extension to MC. Since $tp_K(a/MC)$ describes in particular the isomorphism type over MC of the field $dcl_K(M, a)C$, this implies that $A' = Cb(dcl_K(M, a)/C)$ is contained in $dcl_K(MA) \cap C = EA$, so that $A' = EA$. The conditions of (1)(ii) uniquely determine $tp_C(EA/E)$ and $tp_K(a/MA)$, and by the discussion in (2.6) they uniquely determine $tp(a/M)$.

(2.10). More on independence. Let $L \subseteq M_1, M_2$ be algebraically closed subsets of $(K, C) \models \mathrm{SCF}_C(e_1, e_2)$.

(1) M_1 and M_2 are independent over L if and only if $tp_C(M_1 \cap C/M_2 \cap C)$ does not fork over $L \cap C$, and $tp_K(M_1/M_2C)$ does not fork over $L(M_1 \cap C)$.

(2) The non-forking of $tp(M_1/M_2)$ over L is equivalent to the following three conditions:

(a) $tp_K(M_1/M_2)$ does not fork over L.

(b) $tp_K(M_1M_2/C)$ does not fork over $(M_1 \cap C)(M_2 \cap C)$.

(c) $tp_C(M_1 \cap C/M_2 \cap C)$ does not fork over $L \cap C$.

Proof. (1) is clear by Proposition (2.9). For (2), observe that (c) implies that $tp_K(M_1 \cap C/M_2 \cap C)$ does not fork over $L \cap C$. The result follows using forking calculus.

(2.11). Description of the algebraic and definable closure.

Let $(K, C) \models T_0$, and let $A \subset K$. Let $B = Cb(tp_K(A/C))$. Then $B \subset dcl(A)$, and hence $dcl_C(B) \subseteq dcl(A)$. It follows that $dcl_K(Adcl_C(B)) \subseteq dcl(A)$. The description of the types shows that $dcl(A) = dcl_K(Adcl_C(B))$, and therefore that $acl(A) = dcl(A)^s = acl_K(Adcl_C(B))$.

(2.12). Quantifier-elimination. For $1 \leq n \in \mathbb{N}$, consider the functions $\mu_{i,n} : K^{n+1} \to C$, $i = 1, \ldots, n$, defined as follows: if the tuple $\bar{a} = (a_1, \ldots, a_n)$ is not linearly independent in the C-vector space K, or if b does not belong to the C-vector space generated by $\bar{a}$, then $\mu_{i,n}(\bar{a}; b) = 0$ for $i = 1, \ldots, n$. Otherwise the $\mu_{i,n}(\bar{a}; b)$ are uniquely defined by

$$b = \sum_{i=1}^{n} \mu_{i,n}(\bar{a}; b) a_i.$$

One sees easily that in the language $\mathcal{L}_0$ expanded by function symbols for the $\mu_{i,n}$, the theory $\mathrm{SCF}_C(e_1, e_2)$, together with the defining axioms for the functions $\mu_{i,n}$, eliminates quantifiers. This follows from that fact that if $A \subset (K, C) \models \mathrm{SCF}_C(e_1, e_2)$, then $dcl(A)$ is the smallest field containing A and closed under the functions $\lambda^K_{i,n}, \lambda^C_{i,n}$ and $\mu_{i,n}$. Furthermore, note that for any n, $R_n(x_1, \ldots, x_n)$ is equivalent to $x_1 \neq 0 \wedge \mu_{1,n}(x_1, \ldots, x_n; x_1) = x_1$ so that the predicates R_n can be omitted from the language.

3 Fields with an endomorphism

(3.1). Conventions and setting. We keep the notation and conventions of (1.1) and (1.14). Besides the characteristic p of Ω, we fix some $e \in \mathbb{N} \cup \{\infty\}$, with $e = 0$ if $p = 0$.

Let T_σ be the $\mathcal{L}_\sigma$-theory whose models are the $\mathcal{L}_\sigma$-structures K satisfying: K is a field of characteristic p, σ is an endomorphism of K, and $\sigma(K)^{p^{-\infty}} \subseteq K$, $\sigma(K)^s \cap K = \sigma(K)$.

Let $\mathcal{L}_1 = \mathcal{L}_\sigma \cup \{R_n \mid n \in \mathbb{N}\}$, and consider the $\mathcal{L}_1$-theory T_1 obtained by adding to T_σ the scheme of axioms expressing the following properties of the $\mathcal{L}_1$-structure K:

– For each $n \in \mathbb{N}$, $R_n(x_1, \ldots, x_n) \iff$ the elements $x_1, \ldots, x_n$ are linearly independent in the $\sigma(K)$-vector space K.

(3.2). Remarks. Let K be a difference field, and L a model of T_1.

(1) Any difference field which is a model of T_σ expands uniquely to an $\mathcal{L}_1$-structure which is a model of T_1. This is because the axioms added to T_σ define uniquely the predicates R_n.

(2) Assume that K is a model of T_σ and an $\mathcal{L}_1$-substructure of L. Then $K \models T_1$ if and only if K and $\sigma(L)$ are linearly disjoint over $\sigma(K)$.

(3) If $K \subseteq L$ are models of T_1, then, applying σ^i, we get that $\sigma^i(K)$ and $\sigma^{i+1}(L)$ are linearly disjoint over $\sigma^{i+1}(K)$ for every $i \in \mathbb{N}$. Hence, by induction we obtain that K and $\sigma^{i+1}(L)$ are linearly disjoint over $\sigma^{i+1}(K)$.

(4) The universal part of T_1 is much weaker than T_1, but is awkward to describe.

(3.3). Lemma. Let $K \subseteq L$ be difference fields, and assume that $\sigma(L)$ and K are linearly disjoint over $\sigma(K)$.

(1) If $a \in L$ is transformally algebraic over K, then $a \in K(\sigma(a))_{\mathbb{N}}^{alg}$.

(2) Assume that $L = K(a)_{\mathbb{N}}$ for some finite tuple a. Let b be a subset of a forming a transcendence basis of L over $K\sigma(L)$. Then b is a transformal transcendence basis of L over K, and $K(b)_{\mathbb{N}}$ and $\sigma(L)$ are linearly disjoint over $\sigma(K(b)_{\mathbb{N}})$.

(3) If $\sigma(L)^{p^{-\infty}} \subseteq L$, and the elements of the tuple b are p-independent over K in L, then they are algebraically independent over $K\sigma(L)$.

(4) If $\sigma(K)^{1/p} \subseteq K$, then L is a separable extension of K.

Proof. (1) Let m be minimal such that there is a non-zero polynomial $F(X_0, \dots, X_m) \in K[X_0, \dots, X_m]$ with $F(a, \sigma(a), \dots, \sigma^m(a)) = 0$. If the variable X_0 occurs in F, then $a \in K(\sigma(a), \dots, \sigma^m(a))^{alg}$. Assume that X_0 does not occur in F. The linear disjointness of $\sigma(L)$ and K over $\sigma(K)$ then implies that F has its coefficients in $\sigma(K)$. Hence, $\sigma^{-1}(F) \in K[X_1, \dots, X_m]$, and vanishes at $(a, \dots, \sigma^{m-1}(a))$, contradicting the minimality of m.

(2) By (1), the elements of b are transformally independent over K. Moreover, as $K\sigma(L)(b)$ is a purely transcendental extension of $K\sigma(L)$, we get that $K(b)_{\mathbb{N}}$ and $\sigma(L)$ are linearly disjoint over $\sigma(K(b)_{\mathbb{N}})$.

It remains to show that b is indeed a transformal transcendence basis of L over K. Adjoining b to K, we may assume that $b = \emptyset$, so that $a \in K(\sigma(a))_{\mathbb{N}}^{alg}$. Because a is finite, there is some integer m such that $a \in K(\sigma(a), \dots, \sigma^m(a))^{alg}$. If $i > 0$, then applying σ^i and using induction, one then shows that

$$K(a, \sigma(a), \dots, \sigma^{i+m}(a)) \subset K(\sigma^{i+1}(a), \dots, \sigma^{i+m}(a))^{alg}.$$

This shows that $tr.deg(K(a)_{\mathbb{N}}/K)$ is finite ($\leq m\, tr.deg(K(a)/K)$), i.e., that a is transformally algebraic over K.

(3) The assumption $\sigma(L)^{p^{-\infty}} \subseteq L$ implies that the elements of b are p-independent over $K\sigma(L)$ in L, and therefore they are algebraically independent over $K\sigma(L)$. Now apply (2).

(4) By hypothesis $\sigma(K)^{1/p}$ and $\sigma(L)$ are linearly disjoint over $\sigma(K)$, and therefore $\sigma(L)$ is a separable extension of $\sigma(K)$. As σ is an isomorphism, L is a separable extension of K.

(3.4). Definition. Let SCFE_e be the $\mathcal{L}_1$-theory axiomatised by the scheme of axioms expressing the following properties of the difference field (K, σ):

(i) T_1, $\exists x\, R_2(1, x)$, K is a separably closed field of degree of imperfection e.

(ii) Assume that U and V are varieties defined over K, of the same dimension, and that $V \subseteq U \times \sigma(U)$ projects dominantly onto U and onto $\sigma(U)$. If the characteristic is $p > 0$ and $e > 0$, assume moreover that if (a, b) is a generic of the variety V over K, then $a \in K(b^{1/q})^s$ for some $q = p^n$, $n \geq 0$. Then there is $a \in K$ such that $(a, \sigma(a)) \in V$.

Let us explain why (ii) is indeed first order. Let c be a tuple of elements of K, and $F(T,X)$, $G(T,X,Y)$ tuples of polynomials with integer coefficients. It is then well-known that the following properties of the tuple c are elementary (see e.g. [9]):

$F(c,X)=0$ defines an absolutely irreducible variety U, $G(c,X,Y)=0$ defines an absolutely irreducible variety V contained in $U\times\sigma(U)$ and of the same dimension as U; the projections $V\to U$ and $V\to\sigma(U)$ are dominant.

If $p>0$, $e>0$, and V satisfies the last condition given in (ii), then there is a $|Y|$-tuple $H(T',X',Y)$ of polynomials with integer coefficients such that $H(c^q,X^q,Y)$ belongs to the ideal J generated by $G(c,X,Y)$ in $K[X,Y]$, and the matrix $J(c,X,Y)=\frac{\partial H}{\partial X'}(c^q,X^q,Y)$ is non-singular (modulo the ideal J). This condition is also elementary in c, given F,G,H. Here we are using the well-known fact that an n-tuple a is separably algebraic over a field L if and only if there exists an n-tuple $F(x)$ of polynomials over L which vanishes at a and is such that the determinant of the Jacobian matrix $J_F(x)$ of F does not vanish at a.

(3.5). Theorem. The theory SCFE_e is the model companion of the theory obtained by adding to T_1 an axiom saying that the degree of imperfection is $\leq e$.

Proof. We will first show that every model of T_1 of degree of imperfection $\leq e$ embeds in a model of SCFE_e. Axiom (i) is no problem: σ extends to an endomorphism of K^s, and K is linearly disjoint from $\sigma(K^s)=\sigma(K)^s$ over $\sigma(K)$ because $\sigma(K)^s\cap K=\sigma(K)$. If (K,σ) is a model of T_1 of characteristic p and degree of imperfection $f<e$, choose elements $a_1,\dots,a_{e-f}\in\Omega$ which are transformally independent over the inversive closure of K. Then the difference field generated over K by $\{a_i,\sigma(a_i^{1/p^n})\mid n\in\mathbb{N}, i=1,\dots,e-f\}$ is a model of T_1 of degree of imperfection e, and is an $\mathcal{L}_1$-extension of K. If $e\neq 0$, then $\sigma(K)\neq K$. If $e=0$ and $\sigma(K)=K$, let $a\in\Omega$ be transformally transcendental over K. Then the difference field $K(a)_{\mathbb{N}}^{alg}$ is a model of T_1 extending K, which is perfect, and on which the map σ is not onto.

We may therefore assume that K is separably closed and satisfies (i). Let U,V and q be as in (ii). Choose $a\in\Omega$ such that $(a,\sigma(a))$ is a generic of the variety V over the inversive closure of K. Since $\sigma(a)$ is a generic of the variety $\sigma(U)$ which is defined over $\sigma(K)$,

$$\text{the fields } \sigma(K)(\sigma(a)) \text{ and } \sigma^{-1}(K) \text{ are linearly disjoint over } \sigma(K). \tag{1}$$

Observe that our conditions on U and V imply that for every $m\geq 0$,

$$\sigma^{m+1}(a)\in\sigma^m(K(a))^{alg} \text{ and } \sigma^m(a)\in\sigma^m(K(\sigma(a^{1/q}))^s. \tag{2}$$

Let $M=\sigma(K(a))^{alg}$; then $\sigma(K(a)_{\mathbb{N}})\subseteq M$ and $a\in(KM)^s$ by (2). Also, M and $\sigma^{-1}(K)$ are linearly disjoint over $\sigma(K)^{alg}$, by (1). Hence $N=(KM)^s$ is a separable extension of K, is a separably closed difference field containing a and is a model of T_σ, and therefore expands uniquely to a model of T_1. In order to show that (K,σ) is an $\mathcal{L}_1$-substructure of (N,σ), it suffices to show that $\sigma(N)$ and K are linearly disjoint over $\sigma(K)$, or equivalently, that N is linearly disjoint from $\sigma^{-1}(K)$ over K.

The linear disjointness of M and $\sigma^{-1}(K)$ over $\sigma(K)^{alg}$ implies the linear disjointness of KM and $\sigma^{-1}(K)$ over K; because K is separably closed, this implies the linear disjointness of $N=(KM)^s$ and $\sigma^{-1}(K)$ over K.

We now need to show that the models of SCFE_e are existentially closed. Let $(K,\sigma) \models \mathrm{SCFE}_e$, and let (L,σ) be a model of T_1 containing (K,σ) and of degree of imperfection $\leq e$. It is enough to show that there is an $\mathcal{L}_1(K)$-embedding of L in some saturated elementary extension K^* of K. Let us fix this K^*. We may assume that L is separably closed, since $\sigma(L)^s$ and K are linearly disjoint over $\sigma(K)$.

It is enough to show the following:

(∗) There is an $\mathcal{L}_\sigma(K)$-embedding φ of L into K^* such that K^* is a separable extension of $\varphi(L)$, and $\sigma(K^*)$ is free from $\varphi(L)$ over $\sigma(\varphi(L))$.

Indeed, the freeness condition will imply that $\sigma(K^*)^{alg} = \sigma(K^*)^{p^{-\infty}}$ and $\varphi(L)$ are linearly disjoint over $\sigma(\varphi(L))^{alg} = \sigma(\varphi(L))^{p^{-\infty}}$. The separability of K^* over $\varphi(L)$ will then imply the linear disjointness of $\sigma(K^*)$ and $\varphi(L)$ over $\sigma\varphi(L)$. Thus the map φ will be an $\mathcal{L}_1(K)$-morphism, and because $L \models T_1$, will be an $\mathcal{L}_1$-isomorphism.

Note that in order to show that K^* is a separable extension of $\varphi(L)$, it is enough to show that if a_1 is a tuple of L which is p-independent over K (in L), then $\varphi(a_1)$ is p-independent over K in K^*. Similarly, to show that $\sigma(K^*)$ is free from $\varphi(L)$ over $\sigma\varphi(L)$, it is enough to show that a tuple of elements of L which are algebraically independent over $K\sigma(L)$ is sent by φ to a tuple of elements which are algebraically independent over $K\sigma(K^*)$. By compactness, it is therefore enough to show that given a finite tuple a in L and a sub-tuple a_1 of a which is p-independent over K in L, there is an $\mathcal{L}_\sigma(K)$-embedding φ of $K(a)_{\mathbb{N}}$ in K^* such that:

(a) $\varphi(a_1)$ is p-independent over K in K^*.

(b) If $b \subseteq a$ is a transcendence basis of $K(a)_{\mathbb{N}}$ over $K(\sigma(a))_{\mathbb{N}}$, then the elements of $\varphi(b)$ are algebraically independent over $K\sigma(K^*)$.

Consider $M = \sigma(K(a)_{\mathbb{N}})^{alg})$. Then $KM(a) \subseteq L$, and $KM(a)$ is a finitely generated extension of KM, which contains $K(a)_{\mathbb{N}}$. We know that $KM(a)$ is a separable extension of K, hence linearly disjoint from $K^{p^{-\infty}}$ over K; hence $KM(a)$ is linearly disjoint from $K^{p^{-\infty}}M$ over KM; as M is perfect, this says that $KM(a)$ is a separable extension of KM.

Let $a_1 \subset a$ be a tuple which is p-independent over K in L ($a_1 = \emptyset$ if $e \in \mathbb{N}$), and let $b \subset a$ be a separating transcendence basis of $KM(a)$ over KM containing a_1 (such a basis exists by the previous paragraph). Then the elements of b are transformally independent over K, form a transformal transcendence basis of $K(a)_{\mathbb{N}}$ over K (because $\Delta(a/K) = tr.deg(K(a)_{\mathbb{N}}/K(\sigma(a))_{\mathbb{N}})$, see lemma (3.3)), and $K(a)_{\mathbb{N}} \subseteq KM(b)^s$. Hence, for some $q = p^n$, we have that

$$a \subset (K(\sigma(a^{1/q}))_{\mathbb{N}}(b))^s. \tag{3}$$

From $K \models \exists x\, R_2(1,x)$, we deduce that $\sigma(K) \neq K$. The saturation of K^* then implies that the transcendence degree of K^* over $\sigma(K^*)$ is infinite. If $e = \infty$, it also implies that any p-basis of K^* over K is infinite. If $e \in \mathbb{N}$, choose $c \in K^*$ of the same length as b, whose elements are algebraically independent over $K\sigma(K^*)$. If $e = \infty$, choose $c \in K^*$ of the same length as b, whose elements are p-independent over K (in K^*, and hence algebraically independent over $K\sigma(K^*)$).

By Proposition (1.15), there is a K-isomorphism of difference fields $\psi : K(b)_{\mathbb{N}}^{alg} \to K(c)_{\mathbb{N}}^{alg}$ which sends b to c. Letting $M_0 = \sigma(K(b)_{\mathbb{N}}^{alg})$, this isomorphism restricts to a K-embedding ψ of the difference field $k = (KM_0(b))^s$ into K^*. Note that by our choice of b, we have that k is free from M over $\sigma(k)$. Also, $(kM)^s$ is a difference field and contains $k(a)_{\mathbb{N}}$ (by (3)).

Consider $I_\sigma(a/k)$. It is a prime σ-ideal; the ascending chain condition on perfect σ-ideals and the fact that a is transformally algebraic over k imply that there is an integer m such that if $d \in \Omega$ is such that there is a field isomorphism $k(d, \dots, \sigma^m(d)) \to k(a, \dots, \sigma^m(a))$ which sends $\sigma^i(a)$ to $\sigma^i(d)$ for $i = 0, \dots, m$, and fixes k, then the difference fields $k(a)_{\mathbb{N}}$ and $k(d)_{\mathbb{N}}$ are k-isomorphic by an isomorphism sending a to d. Fix such an m, and let U be the algebraic locus of $u = (a, \dots, \sigma^{m-1}(a))$ over k, V the algebraic locus of $(u, \sigma(u))$ over k. Because a is transformally algebraic over k and by our choice of m, we know that $\sigma(u) \in k(u)^{alg}$ and $u \in k(\sigma(u))^{alg}$. By equation (3), $u \in k(\sigma(u^{1/q}))^s$.

Claim. $\sigma(u)$ is a generic of the variety $\sigma(U)$ over k.

From $k(a)_{\mathbb{N}} \subset (kM)^s$, we obtain $\sigma(k(a)_{\mathbb{N}}) \subseteq \sigma(kM)^s \subseteq M$. As k is free from M over $\sigma(k)$, this implies that $tr.deg(\sigma(u)/k) = tr.deg(\sigma(u)/\sigma(k)) = tr.deg(u/k) = dim(\sigma(U))$, and this proves the claim.

Thus U, V, q satisfy the assumptions of axiom (ii) over the field k. Hence, if U' and V' are the images of U and V under the isomorphism ψ, axiom (ii) says that there is $g \in K^*$ such that $(g, \sigma(g)) \in V'$. The saturation of K^* implies that we may assume that $(g, \sigma(g))$ is a generic of the variety V' over $\psi(k)$. Our choice of m implies that ψ extends to an isomorphism of difference fields $\varphi : k(u)_{\mathbb{N}} \to \psi(k)(g)_{\mathbb{N}}$ sending u to g. By our choice of b and c, the map φ satisfies conditions (a) and (b), and its domain contains $K(a)_{\mathbb{N}}$.

(3.6). Remark. Let K be a model of SCFE$_e$. Our proof shows that if L is a model of T_1 containing K and of degree of imperfection e, then there is an elementary extension of K in which L K-embeds. This implies that in (ii) the dimension hypothesis on U, V can be dropped, i.e., that K satisfies the following scheme of axioms:

(ii') Assume that U and V are varieties defined over K and that $V \subseteq U \times \sigma(U)$ projects dominantly onto U and onto $\sigma(U)$. If the characteristic is $p > 0$ and $e > 0$, assume moreover that if b is a generic of the variety $\sigma(U)$, then the field of definition of the irreducible components of the algebraic set $V(b) = \{a \mid (a, b) \in V\}$ is contained in $K(b^{1/q})^s$ for some $q = p^n$, $n \geq 0$. Then there is $a \in K$ such that $(a, \sigma(a)) \in V$.

(3.7). Ultraproducts of powers of Frobenius automorphisms. Consider the set Q of all prime powers, and for each $q = p^n \in Q$, choose a separably closed field K_q of characteristic p, which is not algebraically closed, and consider the difference field (K_q, σ_q), where $\sigma_q : x \mapsto x^q$. Let $\mathcal{U}$ be a non-principal ultrafilter on Q, and consider $K^* = \prod_q K_q/\mathcal{U}$, with the distinguished endomorphism $\sigma = (\sigma_q)_{\mathcal{U}}$. Then K^* is a model of T_σ, and therefore expands uniquely to an $\mathcal{L}_1$-structure model of T_1.

Theorem. $K^* \models$ SCFE$_e$ for some $e \in \mathbb{N} \cup \{\infty\}$.

Proof. Clearly K^* is a separably closed field, of a certain degree of imperfection e, and σ is an endomorphism of K^*, which is not onto as the fields K_q are not perfect. Note however that $e > 0$ if $char(K^*) = p > 0$.

Let us consider an instance (U, V, q) of axiom (ii) (with $q = 1$ if the characteristic of K^* is 0), and let $c = (c_r)_\mathcal{U} \in K^*$ and $F(T, X)$, $G(T, X, Y)$ be polynomials with integral coefficients such that the equations $F(c, X) = 0$ and $G(c, X, Y) = 0$ define the varieties U and V. If the characteristic of K^* is 0, let $J(T, X, Y)$ be the matrix $\frac{\partial G}{\partial X}(T, X, Y)$, and if the characteristic is $p > 0$, let $J(T^q, X^q, Y)$ be the matrix defined in (3.4).

For each $r \in Q$ consider the difference field $L_r = K_r^{alg}$, with the automorphism $\sigma_r : x \mapsto x^r$, and let $L^* = \prod_r L_r/\mathcal{U}$, and $\sigma = (\sigma_r)_\mathcal{U}$. Then (K^*, σ) is a difference subfield of (L^*, σ). There is $A \in \mathcal{U}$ such that if $r \in A$ then $r > q$ and the algebraic sets U_r and V_r defined by $F(c_r, X) = 0$ and $G(c_r, X, Y) = 0$ satisfy the following: U_r and V_r are varieties of the same dimension, $V_r \subseteq U_r \times \sigma_r(U_r)$, the projection maps $V_r \to U_r$ and $V_r \to \sigma_r(U_r)$ are dominant, and if (a_r, b_r) is a generic of the variety V_r, then $J(c_r^q, a_r^q, b_r)$ has rank $|Y|$.

By Theorem (1.21), there is a set $B \in \mathcal{U}$ contained in A and such that for every $r \in B$, there is a tuple $a_r \in L_r$ such that $(a_r, \sigma_r(a_r)) \in V_r$ and $J(c_r^q, a_r^q, \sigma_r(a_r))$ has rank $|Y|$. If $r \in B$ then $a_r^q \in \mathbb{F}_p(c_r^q, a_r^r)^s$; since $q < r$, $a_r \in \mathbb{F}_p(c_r)^s$, i.e., $a_r \in K_r$. This shows that $a = (a_r)_\mathcal{U} \in K^*$ and finishes the proof.

4 Elementary invariants, algebraic closure, independence, etc.

In this section we show how the proofs for models of ACFA generalise easily to our context.

(4.1). Theorem. Let $e \in \mathbb{N} \cup \{\infty\}$, let (K_1, σ) and (K_2, σ) be models of SCFE_e, and assume that E is a separably closed model of T_1 and is contained in K_1 and in K_2. Then $K_1 \equiv_E K_2$.

Proof. By (1.14), there is some E-embedding φ of K_2 into Ω such that $\varphi(K_2)$ is linearly disjoint from K_1 over E. Then $\varphi(K_2) \equiv_E K_2$, and we may therefore assume that K_2 is linearly disjoint from K_1 over E.

Let $L = (K_1K_2)^s$. Then L is a difference subfield of Ω, as $\sigma(K_1K_2) \subseteq K_1K_2$. Moreover, as L contains the perfect closure of $\sigma(K_1K_2)$, it is a model of T_σ. Expand L to an $\mathcal{L}_1$-structure so that it is a model of T_1. Then K_1 and K_2 are difference subfields of L, and we want to show that they are $\mathcal{L}_1$-substructures of L. Hence we need to show for $i = 1, 2$, that L is a separable extension of K_i and that $\sigma(L)$ and K_i are linearly disjoint over $\sigma(K_i)$.

Since K_1 and K_2 are linearly disjoint over E, L is a separable extension of K_1 and of K_2. Since $\sigma(K_2)$ is linearly disjoint from E over $\sigma(E)$, and K_2 is linearly disjoint from K_1 over E, we deduce that $\sigma(K_2)$ is linearly disjoint from K_1 over $\sigma(E)$. Hence $\sigma(K_1K_2)$ and K_1 are linearly disjoint over $\sigma(K_1)$. Now $\sigma(L)$ is the separable closure of the separable extension $\sigma(K_1K_2)$ of the separably closed field $\sigma(K_1)$, and $\sigma(K_1K_2)$ is linearly disjoint from K_1 over $\sigma(K_1)$: this implies that $\sigma(L)$ is linearly disjoint from K_1 over $\sigma(K_1)$ and shows that (K_1, σ) is an $\mathcal{L}_1$-substructure of (L, σ). Similarly, (K_2, σ) is an $\mathcal{L}_1$-substructure of (L, σ).

If $e = \infty$, or if E has degree of imperfection e, then L has degree of imperfection e, and therefore embeds in a model (M, σ) of SCFE_e. We then have $(K_i, \sigma) \prec (M, \sigma)$ by model-completeness of SCFE_e, and we get the result.

Assume now that $p > 0$, $e \in \mathbb{N}$, and let b_1 be a p-basis of K_1 over E, b_2 a p-basis of K_2 over E. Then b_1 and b_2 have the same size, and we fix a bijection $f : b_1 \to b_2$. Note that the elements of b_1 and of b_2 are transformally independent over E. Consider the field $L_1 = L((b - f(b))^{1/p^n} \mid b \in b_1, n \in \mathbb{N})$. This is a purely inseparable extension of L, and $\sigma(b - f(b))^{1/p^n} = \sigma(b)^{1/p^n} - \sigma(f(b))^{1/p^n} \in L$ for $n \in \mathbb{N}$. Moreover b_1 and b_2 are p-bases of L_1 over E, and so L_1 is a separable extension of K_1 and of K_2, of degree of imperfection e. We now need to show that $\sigma(L_1)$ and K_i are linearly disjoint over $\sigma(K_i)$ for $i = 1, 2$, so that K_1 and K_2 will be $\mathcal{L}_1$-substructures of L_1. Since $\sigma(L_1) \subseteq \sigma(L)^{alg}$, and $\sigma(L)^{alg}$ is linearly disjoint from K_1 over $\sigma(K_1)^{alg}$, we obtain that $\sigma(L_1)\sigma(K_1)^{alg}$ is linearly disjoint from K_1 over $\sigma(K_1)^{alg}$. Because L_1 is a separable extension of K_1, the fields $\sigma(L_1)$ and $\sigma(K_1)^{alg}$ are linearly disjoint over $\sigma(K_1)$, and this implies that $\sigma(L_1)$ and K_1 are linearly disjoint over $\sigma(K_1)$.

Similarly, $\sigma(L_1)$ and K_2 are linearly disjoint over $\sigma(K_2)$. Hence L_1 embeds in a model M of SCFE_e, and we conclude as in the previous case.

(4.2). Corollary. The completions of SCFE_e are obtained by describing the action of σ on the algebraic closure of the prime field. For each e, the theory SCFE_e is decidable, as well as the theory $\text{SCFE} = \bigcap_{e \in \mathbb{N} \cup \{\infty\}} \text{SCFE}_e$.

Proof. The first statement is immediate from Theorem (4.1). The others follow by standard arguments.

(4.3). Lemma. Let $E = acl(E) \subseteq K \models \text{SCFE}_e$. Then $E \models T_1$, and E is separably closed.

Proof. Clearly E is a difference subfield of K, which is closed under the λ-functions of K, and is relatively algebraically closed in K, which implies that it is separably closed. Hence it is enough to show that E and $\sigma(K)$ are linearly disjoint over $\sigma(E)$. But this is clear by Remark (2.3)(3).

(4.4). If $E = acl(E) \subseteq K \models \text{SCFE}_e$, then $\text{SCFE}_e \cup qftp(E) \vdash tp(E)$. (Here, $qftp(E)$ denotes the *quantifier-free type* of E).

Proof. Immediate from Lemma (4.3) and Theorem (4.1).

(4.5). Let $E \subseteq K \models \text{SCFE}_e$, and let a, b be tuples in K. Then $tp(a/E) = tp(b/E)$ if and only if there is an E-isomorphism $acl(Ea) \to acl(Eb)$ which sends a to b.

Proof. Clear by Theorem (4.1) and Corollary (4.4).

(4.6). Notation. We will work in the (pure) separably closed field K, and we need to introduce some notation: $acl_K(-)$ and $dcl_K(-)$ will denote the algebraic and definable closures in the field reduct K, and $tp_K(-/-)$ will denote a type in the sense of K.

Corollary. Let E be a difference subfield of the model K of SCFE_e, and assume that $acl_K(E) = E$, and that E and $\sigma(K)$ are linearly disjoint over $\sigma(E)$. Then $acl(E) = E$.

Proof. Our assumption implies that E is separably closed, contains $\sigma(E)^{alg}$, and that K is a separable extension of E. Hence, if K_1 is a difference field linearly disjoint from K over E and E-isomorphic to K, then K, K_1 and E satisfy the hypotheses of Theorem (4.1). Hence any type realised in $K \setminus E$ is realised anew in K_1, and this shows that $E = acl(E)$ (by Corollary (4.5)).

(4.7). Description of the algebraic closure. Let $K \models \mathrm{SCFE}_e$, and let $A \subset K$. We build by induction on $i \in \mathbb{N}$ a sequence of subsets of K which are contained in the definable closure of A as follows: Let $B_0 = dcl_K(A)$, and assume that we have defined a subset B_i of $dcl(A)$. Let C_i be the canonical basis of $tp_K(B_i/\sigma(K))$, and let $B_{i+1} = dcl_K(B_i, \sigma^{-1}(C_i), \sigma(B_i), C_i)$. Then $B_{i+1} \subset dcl(B_i)$.

Proposition. Let K, A, and the B_n, $n \in \mathbb{N}$, be defined as above. Then $acl(A) = (\bigcup_{n\in\mathbb{N}} B_n)^s$.

Proof. Let $B = (\bigcup_{n\in\mathbb{N}} B_n)^s$. Then B is a separably closed difference subfield of K. Each B_n is closed under the λ-functions of K, and therefore K is a separable extension of B. Moreover, as B_n contains the perfect closure of $\sigma(B_{n-1})$, the field B contains $\sigma(B)^{alg}$. By definition, each B_n is linearly disjoint from $\sigma(K)$ over $C_n \subset \sigma(B_{n+1})$, and therefore B is free from $\sigma(K)$ over $\sigma(B)$. As $\sigma(K)$ is a regular extension of $\sigma(B)$, this implies that B is linearly disjoint from $\sigma(K)$ over $\sigma(B)$. Hence B satisfies the hypotheses of Corollary (4.6), and $B = acl(B)$.

(4.8). Corollary. Let K be a model of SCFE_e, and let $D \subseteq K^n$ be 0-definable, defined by the formula $\varphi(x)$.

(1) There is m and a set $W \subseteq K^{n+m}$ defined by a positive quantifier-free formula such that if $\pi : K^{n+m} \to K^n$ is the natural projection, then $\pi(W) = D$.

(2) There is a partition $D_1, \dots, D_r$ of D into definable sets, and for each i there is a subset W_i of K^{n+m_i} (for some m_i) such that the natural projection $\pi_i : K^{n+m_i} \to K^n$ restricts to a finite-to-one map from W_i onto D_i. Each W_i is defined by a formula $\psi_i(x, y) \wedge \rho_i(x, y)$, where $\psi_i(x, y)$ is a quantifier-free positive $\mathcal{L}_1$-formula, and $\rho_i(x, y)$ expresses that certain subtuples of $x^\frown y$ are p-independent.

Proof. (1) By model-completeness, $\varphi(x)$ is equivalent modulo SCFE_e to an existential formula. To conclude, note that modulo SCFE_e the formulas $y \neq 0$ and $\neg R_m(y_1, \dots, y_m)$ are equivalent to $\exists z\, yz = 1$ and $\exists z_1, \dots, z_m \sum_{i=1}^m y_i\sigma(z_i) = 0$ respectively.

(2) Let a be an n-tuple, and let $A = a$, and B and the B_n's be defined as in (4.7). We know that modulo SCFE_e, $qftp(B) \vdash tp(a)$. As the field B is linearly disjoint from $\sigma(K)$ over $\sigma(B)$, the observation made in (1) shows that any formula of $qftp(B)$ is implied by some positive quantifier-free formula of $qftp(B)$ (modulo the theory SCFE_e).

Hence there is a tuple b in B, and a positive $\mathcal{L}_1$-formula $\psi_a(x, y) \in qftp(a, b)$ such that

$$\mathrm{SCFE}_e \cup \psi_a(x, y) \vdash \varphi(x) \text{ or } \mathrm{SCFE}_e \cup \psi_a(x, y) \vdash \neg\varphi(x).$$

We will then show the following statement $(*)$: maybe enlarging b, there is a positive $\mathcal{L}_1$-formula $\theta_a(x, y) \in qftp(a, b)$ and a formula $\rho_a(x, y) \in tp(a, b)$ which expresses that certain subtuples of $x^\frown y$ are p-independent, such that whenever a tuple (a', b') satisfies $\rho_a(x, y) \wedge \theta_a(x, y)$, then the set defined by $\theta_a(a', y) \wedge \rho_a(a', y)$ is finite or empty. This will show the result, since by compactness, finitely many of the formulas $\exists y\, \psi_a(x, y) \wedge \theta_a(x, y) \wedge \rho_a(x, y)$ cover $\varphi(x)$.

The proof is done in two steps. We first show how to reduce to the case $b \in B_n$ for some n, then show how the inductive definition of the B_n's gives the result. Let k denote the prime field ($\mathbb{F}_p$ or $\mathbb{Q}$).

Choose a tuple $c \in \bigcup_n B_n$ such that b is integral algebraic over $k[a,c]$. Thus there is a quantifier-free positive $\mathcal{L}$-formula $\theta(x,y,z)$ satisfied by (a,c,b), and such that for any (a',c') the set $\theta(a',c',z)$ is finite. Hence it suffices to show $(*)$ for tuples (a,b) where $b \in \bigcup_n B_n$.

Observe that $\bigcup_n B_n$ is the smallest field containing a, which is closed under the functions σ, $\sigma^{-1}|_{\sigma(K)}$, the λ-functions of K and the functions $\mu_{i,n}$ of the pair $(K,\sigma(K))$ (see (2.12)). If $n > 0$, then there is a positive quantifier-free $\mathcal{L}$-definable set $W \subset K^{n+1+p^n}$ such that for any $c \in K^n$ which is p-independent, and $d \in K$, $W(c,d) = \{y \in K^{p^n} \mid (c,d,y) \in W\}$ defines the tuple $(\lambda_{i,n}(c;d))_{i<p^n}$ if $d \in K^p(c)$, and is empty otherwise. Similarly, if $n > 0$, there is a positive quantifier-free $\mathcal{L}_\sigma$-definable set $W \subset K^{n+1+n}$ such that for any $c \in K^n$ which is $\sigma(K)$-linearly independent, and $d \in K$, the set $W(c,d)$ defines the tuple $(\sigma^{-1}(\mu_{i,n}(a,b)))_{1\leq i\leq n}$ if d belongs to the $\sigma(K)$-vector space generated by c, and is empty otherwise. This shows, using induction, that if $b \in \bigcup_n B_n$, then (a,b) satisfies $(*)$, and finishes the proof of (2).

Remark. The sets W_i are almost quantifier-free definable. In fact, they are positively quantifier-free definable in the language $\mathcal{L}_1$ to which one has added symbols for the λ-functions of K. Similarly if $e \in \mathbb{N}$ and one adds to $\mathcal{L}_1$ constant symbols for a p-basis of K.

(4.9). Independence.

Definition. Let $K \models \mathrm{SCFE}_e$, and let A, B, E be subsets of K. We say that A and B are *independent over* E iff $tp_K(acl(E,A)/acl(E,B))$ does not fork over $acl(E)$, and $tp_K(acl(E,A)/acl(E,B)\sigma(K))$ does not fork over $acl(E)\sigma(acl(E,A))$.

(4.10). Remarks and discussion. (1) The pair $(K,\sigma(K))$ is a reduct of K, and is a model of $\mathrm{SCF}_C(e,e)$. By (2.10), the independence of A and B over E is equivalent to the non-forking of $tp_{(K,\sigma(K))}(acl(E,A)/acl(E,B))$ over $acl(E)$. Here $tp_{(K,\sigma(K))}(-/-)$ denotes the type in the $\mathcal{L}_0$-structure $(K,\sigma(K))$ (but acl is in the sense of the $\mathcal{L}_1$-structure K).

(2) Hence independence is symmetric and transitive. We will show below that it corresponds to non-forking.

(4.11). Lemma. Let $K \models \mathrm{SCFE}_e$, $E = acl(E) \subseteq B = acl(B) \subseteq K$, and let a be a tuple of elements of K which are transformally algebraic over E.

(1) Then the elements of $acl(Ea)$ are transformally algebraic over E, and $acl(Ea) = E(a)_{\mathbb{N}}^{alg} \cap K$, and E and $acl(Ea)$ have the same p-basis.

(2) a and B are independent over E if and only if $acl(Ea)$ and B are linearly disjoint over E, if and only if $E(a)_{\mathbb{N}}$ is free from B over E.

Proof. (1) Replacing a by $a^\frown\sigma(a)^\frown\cdots^\frown\sigma^m(a)$ if necessary, we may assume that $E(a)^{alg} = E(\sigma(a))^{alg}$ (by Lemma (3.3)).

Claim. $acl(Ea) = E(a)^{alg} \cap K$.

Because a is algebraic over $E(\sigma(a))$, E is closed under the λ-functions of K, and $\sigma(a)^{1/p^n} \in K$ for every n, we get that $A = E(a)^{alg} \cap K$ is closed under the λ-functions of K, and has the same p-basis as E. Hence K is a regular extension of A. To finish the proof, we need to show that A and $\sigma(K)$ are linearly disjoint over $\sigma(A)$. The linear disjointness of E and $\sigma(K)$ over $\sigma(E) \subset \sigma(A)$ has two consequences:

– it is enough to show that A and $E\sigma(K)$ are linearly disjoint over $E\sigma(A)$,

– $E\sigma(K)$ is a regular extension of $E\sigma(A)$ (because $\sigma(K)$ is a regular extension of $\sigma(A)$).

All elements of A being algebraic over $E\sigma(A)$, we obtain that A and $E\sigma(K)$ are linearly disjoint over $E\sigma(A)$.

(2) Clearly the independence of a and B over E implies the linear disjointness of $acl(Ea)$ and B over E. Conversely, assume that $A = acl(Ea)$ and B are linearly independent over E. We proved in (1) that a p-basis of E is also a p-basis of A, and this implies that $tp_K(A/B)$ does not fork over E. It remains to show (see Proposition (2.9)) that $tp_K(A/B\sigma(K))$ does not fork over $E\sigma(A)$: but this is clear, since $A \subset (E\sigma(A))^{alg}$.

(4.12). Definition. Let $K \models \mathrm{SCFE}_e$, and let $E = acl(E) \subset K$. Let a be an n-tuple from K. We say that a is *generic over* E if $tp_K(a/E)$ is the generic n-type over E of SCF_e. Note that then $tp_K(a/E\sigma(K))$ is also generic, since $\sigma(K) \subseteq K^{p^\infty}$.

(4.13). Proposition. Let K and E be as above, with K sufficiently saturated, and let $n \in \mathbb{N}$. Then K contains generic n-tuples. Moreover any two generic n-tuples realise the same type over E.

Proof. By saturation of K, there is $a \in K$ realising the generic n-type of SCF_e over E (or over $(E\sigma(K)^{alg})^s$), and this shows the existence. If a is a generic n-tuple over E, then $dcl_K(E\sigma(K), a)$ is a union of purely transcendental extensions of $E\sigma(K)^{alg}$, generated over $E\sigma(K)^{alg}$ by $dcl_K(E, a)$. Let M_1 be the difference subfield of K generated by $\sigma(dcl_K(E, a))$, and consider $M = (M_1^{alg} dcl_K(E, a))^s$. Then M is separably closed, M and $\sigma(K)$ are linearly disjoint over $\sigma(M) = M_1 \cap \sigma(K)$, M is closed under the λ-functions of K, and therefore $M = acl(Ea)$.

If b is another generic n-tuple over E, then similarly $acl(Eb) = (N_1^{alg} dcl_K(E, b))^s = N$, where N_1 is the difference subfield of K generated by $\sigma(dcl_K(E, b))$; moreover there is an E-isomorphism $\varphi : dcl_K(E, a) \to dcl_K(E, b)$ which sends a to b; because elements of $dcl_K(E, a)$ which are algebraically independent over E are transformally independent over E, and similarly for elements of $dcl_K(E, b)$, φ extends to a difference field isomorphism $M \to N$. This shows the uniqueness.

Remark. Let K and E be as above, and B an algebraically closed subset of K containing E. If a is generic over B, then a is also generic over E, and $A = acl(Ea)$ and B are independent over E.

(4.14). Lemma. Let K and E be as above, with K sufficiently saturated, and let A, B be algebraically closed subsets of K. Then there is A' realising $tp(A/E)$ and independent from B over E.

Proof. We will first assume that E contains a p-basis of A if $e \in \mathbb{N}$. Choose A' realising the non-forking extension of $tp_{(K,\sigma(K))}(A/E)$ to B, and let $\varphi : A \to A'$ be an $\mathcal{L}_0(E)$-isomorphism. Let $\tau = \varphi\sigma|_A\varphi^{-1}$. Then $\tau \in End(A')$, and τ and σ agree on E. Our hypotheses imply that A' and B are linearly disjoint over E, and that $(A'B)$ has degree of imperfection $\leq e$. Hence there is a unique $\rho \in End(A'B)$ which extends σ on B and τ on

A': define $\rho(a \otimes b) = \tau(a) \otimes \sigma(b)$ for $a \in A'$ and $b \in B$, extend by linearity to $A' \otimes_E B$, and then to its field of fractions $A'B$. As in Theorem (4.1), on shows that $(A'B, \rho)$ expands to a model of T_1 extending A' and B. Let θ be an extension of ρ to $(A'B)^s$. Then, by the model completeness of $Th(K)$, we may assume that $(A'B)^s \subseteq K$. This implies that $(A'B)^s$ is algebraically closed in K, and proves the result.

Assume now that $e \in \mathbb{N}$, and that $A_0 \neq \emptyset$ is a p-basis of A over E. By Proposition (4.13), there is A_0' realising the $|A_0|$-generic over B, and A_0' and B are independent over E. Moving A by an E-automorphism, we may assume that $A_0 = A_0'$. Then, by the first case, there is A' realising $tp(A/EA_0)$, independent from $acl(BA_0)$ over $acl(EA_0)$. Then A realises $tp(A/E)$, and A is independent from B over E.

(4.15). Theorem. Let $K \models \text{SCFE}_e$ be sufficiently saturated, let $E = acl(E) \subseteq K$. Let a, b, c_1, c_2 be tuples of elements in K satisfying:

(i) $tp(c_1/E) = tp(c_2/E)$.

(ii) a and b are independent over E, a and c_1 are independent over E, and b and c_2 are independent over E.

Then there is $c \in K$ realising $tp(c_1/E, a) \cup tp(c_2/E, b)$, such that c and (a, b) are independent over E.

Proof. If $e \in \mathbb{N}$, we will first treat the case where E contains a p-basis of K. Let $A = acl(E, a)$, $B = acl(E, b)$, $C = acl(E, c_1)$ and $C_2 = acl(E, c_2)$. Moving C by an A-automorphism, we may assume that C and $acl(AB)$ are independent over E. Fix an $\mathcal{L}_1(E)$-isomorphism $f : C_2 \to C$ which sends c_2 to c_1, and extend it to an $\mathcal{L}(B)$-isomorphism $g : (BC_2)^s \to (BC)^s$. Consider the field $L = (AB)^s(AC)^s(BC)^s$. By Remark (1.9) in [4], we have $(AB)^s(AC)^s \cap (BC)^s \subseteq B^{alg}C^{alg}$. As $B^{alg}C^{alg}$ is a purely inseparable extension of BC, this implies that $(BC)^s$ and $(AB)^s(AC)^s$ are linearly disjoint over BC. By assumption, the endomorphism $\tau = g\sigma g^{-1}$ of $(BC)^s$ agrees with σ on B and on C; hence there is an automorphism ρ of L which agrees with σ on $(AB)^s(AC)^s$ and with τ on $(BC)^s$, and we may extend ρ to L^s. Note that $\rho(L^s) = \rho(ABC)^s = \sigma(L^s)$. Clearly also, L^s is a separable extension of $(AB)^s$ and of C^s, and hence $(AB)^s$ and C^s are $\mathcal{L}_1$-substructures of (L^s, ρ). Hence, moving L by an $(AB)^s$-automorphism of K, we may assume that $\rho = \sigma$. Since $acl(AC) = (AC)^s$ and $acl(BC) = (BC)^s$, c realises $tp(c/A) \cup tp(c_2/B)$. It remains to show that c is independent from AB over E. Clearly $acl(AB)$ and $acl(C)$ are linearly disjoint over E, by our choice of C and because $acl(AB) = (AB)^s$. Since L is an $\mathcal{L}_1$-substructure of K and is model of T_1, we have that L and $\sigma(K)$ are linearly disjoint over $\sigma(L)$. This implies that $Cacl(AB)$ and $\sigma(K)$ are linearly disjoint over $\sigma(Cacl(AB))$, and therefore that C is independent from (AB) over E.

If $e \in \mathbb{N}$, we will show how to reduce to the case where E contains a p-basis of K. Let f be the degree of imperfection of E and assume that $f < e$. Choose an $(e - f)$-tuple d which is generic over $acl(Eabc_1c_2)$, and let $F = acl(Ed)$. By definition, (ii) holds over F. Moreover, the uniqueness of the generic type implies $tp(c_1/F) = tp(c_2/F)$. Hence the assumptions of the theorem hold over F. Let c realise $tp(c_1/F, a) \cup tp(c_2/F, b)$, and independent from $acl(F, a, b)$ over F. As c and F are independent over E, the transitivity of independence implies that c and (a, b) are independent over E.

(4.16). Corollary. Independence is non-forking, and all completions of SCFE_e are simple.

Proof. Follows from [14].

(4.17). Remarks. (1) One cannot deduce, as in [3], that any of the completions of the theories SCFE eliminate imaginaries. One can however show, using techniques similar to those of [3], that the imaginaries of a model K of SCFE_e are inter-definable with the imaginaries of the pair $(K, \sigma(K))$.

(2) We will present an alternate proof of the independence theorem at the end of section 5.

(3) One can however deduce that any of the completions of SCFE eliminates hyper-imaginaries. This follows immediately from the independence theorem: if (K, σ) is a model of some SCFE_e, $E = acl(E) \subset K$, and $tp(a/E) = tp(b/E)$, then the Lascar strong types $Lstp(a/E)$ and $Lstp(b/E)$ are equal; this implies that $Cb(Lstp(a/E)) \subseteq E$ and yields the result (see e.g. section 3.6 of [18]).

(4) If K is a model of SCFE_e, and $a \in K$ is transformally algebraic over a difference subfield E of K, then $tp(a/E)$ has finite SU-rank. This follows immediately from Corollary (4.16) and Lemma (4.11).

5 Various results

Notation and conventions are the same as in the previous sections.

(5.1). Theorem. Let $K \models \mathrm{SCFE}_e$, let $n \geq 1$, and $m \in \mathbb{N}$ if $e > 0$, $m \in \mathbb{Z}$ if $e = 0$. Let $\tau = \sigma^n Frob^m$. Then $(K, \tau) \models \mathrm{SCFE}_e$.

Proof. The scheme of axioms (i) is clear: if $e > 0$, then $m \geq 0$ and τ is an endomorphism of K; if $e = 0$, then K is perfect, and τ is an endomorphism of K.

Case 1. $n = 1$ and $m \neq 0$.

Then $p > 0$. Let U, V be varieties defined over K, with $V \subset U \times \tau(U)$ projecting dominantly onto each of the factors, and such that if (a, b) is a generic of the variety V, then $a \in K(b^{1/q})^s$ for some power q of p. We want to show that there is $c \in K$ such that $(c, \sigma(c^{p^m})) \in V$. Consider the variety W with generic $(a, b^{1/p^m})$. Then b^{1/p^m} is a generic of the variety $Frob^{-m}\tau(U)$, i.e., of $\sigma(U)$. Moreover, $a \in K(b^{1/p^m q})^s$. Hence, by axiom (ii), there is $c \in K$ such that $(c, \sigma(c)) \in W$, i.e., $(c, \tau(c)) \in V$.

Case 2. $n > 1$, $m = 0$.

By model-completeness of SCFE_e, it suffices to show that if (L, τ) is a model of T_1 extending (K, σ^n), there is a model (M, ρ) of T_1 containing (K, σ) such that (L, τ) is an $\mathcal{L}_1$-substructure of (M, ρ^n).

Without loss of generality, L is separably closed. For $i = 0, \dots, n-1$, choose by induction on i isomorphisms $f_i : L \to L_i$ extending σ^i on K, such that: $f_0 = id_L$, and $L_i = f_i(L)$ is linearly disjoint from $L_0 \cdots L_{i-1}$ over $\sigma^i(K)$ for $i > 0$. Then $L_0 \cdots L_{i-1}$ and $L_i \cdots L_{n-1}$ are linearly disjoint over $\sigma^i(K)$ if $i > 0$, and $M = L_0(L_1 \cdots L_{n-1})^{p^{-\infty}}$ is a separable extension of L. Define $\sigma_i : L_{i-1} \to L_i$ for $i = 1, \dots, n-1$ and $\sigma_n : L_{n-1} \to \tau(L)$ by

$$\sigma_i = f_i f_{i-1}^{-1} \text{ for } i = 1, \dots, n-1, \quad \text{and } \sigma_n = \tau f_{n-1}^{-1}.$$

For $1 < i \leq n$ extend σ_i to $L_{i-1}^{p^{-\infty}}$. Then $\sigma_n\sigma_{n-1}\cdots\sigma_1$ and τ agree on $L_0 = L$. Moreover, each σ_i agrees with σ on $\sigma^{i-1}(K)$; this, together with the linear disjointness assumptions on the L_i's, shows that $\sigma_1 \cup \cdots \cup \sigma_n = \rho$ extends uniquely to an endomorphism of M extending σ. Clearly (M, ρ) is a model of T_σ, and therefore expands to a model of T_1.

We need to show that $\rho(M)$ and K are linearly disjoint over $\sigma(K)$, and that $\rho^n(M)$ and L are linearly disjoint over $\tau(L)$. Because M is a separable extension of L, letting $M_0 = L_0 \cdots L_{n-1}$, it is enough to show that $\rho(M_0)$ and K are linearly disjoint over $\sigma(K)$, and that $\rho^n(M_0)$ and L are linearly disjoint over $\tau(L)$.

By construction, L and $L_1 \cdots L_{n-1} = \rho(L_0 \cdots L_{n-2})$ are linearly disjoint over $\sigma(K)$, and hence L and $\rho(M_0)$ are linearly disjoint over $\sigma(K)\tau(L)$. We also know that $\tau(L)$ and K are linearly disjoint over $\sigma^n(K)$, and hence $\sigma(K)\tau(L)$ and K are linearly disjoint over $\sigma(K)$. As $L \supset K\tau(L)$, this implies that $\rho(M_0)$ and K are linearly disjoint over $\sigma(K)$.

Since K and $\rho(M_0)$ are linearly disjoint over $\sigma(K)$, also K and $\rho^n(M_0)$ are linearly disjoint over $\sigma^n(K)$ (see Remark (3.2)(3)), and therefore K and $\rho^n(KL_1 \cdots L_{n-1})$ are linearly disjoint over $\sigma^n(K)$. The linear disjointness of L and $L_1 \cdots L_{n-1}$ over $\sigma(K)$ implies the linear disjointness of L and $\rho^n(KL_1 \cdots L_{n-1})$ over $\sigma^n(K)$. As $\tau(L) = \rho^n(L) \subseteq L$, this gives that L and $\rho^n(M_0)$ are linearly disjoint over $\tau(L)$.

Case 3. $n > 1$, $m \neq 0$.

Use Case 2 and Case 1.

(5.2). Proposition. Let $K \models \mathrm{SCFE}_e$, and consider $L = \bigcup_n \sigma^{-n}(K)$, the inversive closure of K. Then $K^{alg} \models \mathrm{SCFE}_0$ and $L \models \mathrm{ACFA}$.

Proof. If $p = 0$, then $K = K^{alg}$. Assume therefore that $p > 0$. Clearly K^{alg} is an algebraically closed field, and σ is an endomorphism of K which is not onto.

Let U and V be varieties of the same dimension, defined over K^{alg}, such that $V \subseteq U \times \sigma(U)$ and V projects dominantly onto U and onto $\sigma(U)$. Let (a, b) be a generic of the variety V over K^{alg}. Our assumption on the dimensions of U and V implies that $a \in K(b)^{alg}$ and $b \in K(a)^{alg}$. Choose powers q and r of p such that U and V are defined over $K^{1/q}$, and $a \in K^{1/q}(b^{1/r})^s$. The difference fields K and $K^{1/q}$ are isomorphic, and therefore $K^{1/q}$ is a model of SCFE_e. Hence $K^{1/q}$ contains a tuple c such that $(c, \sigma(c)) \in V$, and this shows that $K^{alg} \models \mathrm{SCFE}_0$.

The second assertion follows immediately: observe that $L = \bigcup_n \sigma^{-n}(K^{alg})$, where each $\sigma^{-n}(K^{alg})$ is a model of SCFE_0. As axiom (ii) for ACFA coincides with axiom (ii) for SCFE_0, and σ is an automorphism of the difference field L, it follows that L is a model of ACFA.

(5.3). Theorem. Let L be a model of ACFA, and let $A = acl_\sigma(A) \subseteq B = acl_\sigma(B) \subseteq L$. Assume that A contains all elements of B which are transformally algebraic over A. Then $tp(B/A)$ is stationary (here tp is the type in the sense of the generic difference field L).

Proof. We may assume that L is sufficiently saturated. Let $C = acl_\sigma(C)$ containing A and independent from B over A. We want to show that $tp(B/A)$ has a unique non-forking extension to C. We will first show that we may assume that C is transformally algebraic over A.

Step 1. $tp(B/A)$ is orthogonal to all types of finite SU-rank over A, i.e.: if $F = acl_\sigma(F) \supset A$ is linearly disjoint from B over A, and $c \in acl_\sigma(F, B)$ is transformally algebraic over F, then $c \in F$ (see (1.16)).

Indeed, let F, c be as above. By (2.13) in [4], the canonical base D of $tp(F, c/B)$ is contained in $acl_\sigma(A, F_1, c_1, \ldots, F_n, c_n)$ for some n and independent realisations $(F_1, c_1), \ldots, (F_n, c_n)$ of $tp(F, c/B)$. Hence D is transformally algebraic over $acl_\sigma(F_1, \ldots, F_n)$. As $D \subseteq B$, and B and $acl_\sigma(F_1, \ldots, F_n)$ are linearly disjoint over A, D must be transformally algebraic over A, whence $D = A$ and $c \in F$.

Step 2. We may assume that $C = A(d)_{\mathbb{Z}}$ where d is transformally algebraic over A.

First of all, we certainly may assume that $C = A(d)_{\mathbb{Z}}$ for some finite tuple d. Let $c \subset d$ be a transformal transcendence basis of C over A, and let $A' = acl_\sigma(A, c)$. By (1.15), $tp(A'/A)$ has a unique non-forking extension to B, or equivalently, $tp(B/A)$ has a unique non-forking extension to A'. To show the result, it is therefore enough to show that $tp(acl_\sigma(B, c)/A')$ has a unique non-forking extension to $A'(d)_{\mathbb{Z}}$. By step 1, A' and $acl_\sigma(B, c)$ satisfy the hypotheses satisfied by A and B.

Step 3.

Let S be an A-definable set of finite SU-rank containing d, defined by the formula $\theta(a, x)$. If $tp(B/A)$ has several non-forking extensions to $A(d)_{\mathbb{Z}}$, then there is a B-definable subset X of S, such that $d \in X$ and some realisation of a non-forking extension of $tp(d/A)$ to B is in $S \setminus X$. By elimination of imaginaries, X has a code $b \in B$. Thus if an A-automorphism of some elementary extension of L fixes all elements satisfying $\theta(a, x)$ then necessarily it also fixes b. We will assume by way of contradiction that b contains an element $b_1 \notin A$.

Claim. There is an elementary extension K of L, and an automorphism of K which is the identity on all elements of K which are transformally algebraic over A, and which moves b_1.

Proof. By Theorem (1.21), there is an ultrafilter $\mathcal{U}$ on the set Q of prime powers, and a sequence of algebraically closed fields $F_q, q \in Q$, such that the difference field A embeds in $\prod_{q \in Q}(F_q, Frob_q)/\mathcal{U}$, where $Frob_q : x \mapsto x^q$. Let K_q be an algebraically closed field properly containing F_q, and fix $c_q \in K_q \setminus F_q$, and $h_q \in Aut(K_q/F_q)$ such that $h_q(c_q) \neq c_q$. Consider the structure $M_q = (K_q, F_q, Frob_q, h_q, c_q)$, and let $M = (K, F, \sigma, h, c)$ be a highly saturated elementary extension of $\prod_{q \in Q} M_q/\mathcal{U}$. Then there is an embedding φ of the difference field A in F, and $h \in Aut(K/F)$, $h(c) \neq c$. All elements of K_q are transformally transcendental over F_q (because σ_q is algebraic), and therefore all elements of K are transformally transcendental over F.

Since $b_1 \notin A$, b_1 is transformally transcendental over A. Then $tp(c/\varphi(A)) = \varphi(tp(b_1/A))$ (by Proposition (1.15)). Using the saturation of M, there is a difference field embedding ψ of L in K which extends φ and such that $\psi(b_1) = c$. Then $\psi(L) \prec K$.

The claim allows us to conclude that $b \in A$: the elements of K satisfying $\theta(\varphi(a), x)$ are transformally algebraic over A, and therefore are in F. Hence they are fixed by h and this implies that h fixes $\psi(b)$; but this contradicts the claim.

Remark. Another way of stating Theorem (5.3) is to say, that over an algebraically closed set, all types of SU-rank ωn for some n, are stationary. In Appendix B, we give an alternate proof of the claim, which does not rely on the results of [13].

(5.4). Corollary. Let K be a model of SCFE_e, and $E = acl(E) \subset A = acl(A)$ subfields of K. Assume that all elements of $A \setminus E$ are transformally transcendental over E. Then $tp(A/E)$ is stationary.

Proof. We will first assume that E contains a p-basis of K if $e \in \mathbb{N}$. Let $B = acl(B) \subset K$ containing E, and let A_1, A_2 realise non-forking extensions of $tp(A/E)$ to B. Let L, E', A_1', A_2' and B' denote the inversive closures of K, E, A_1, A_2, B respectively. Then all elements of A_1' are transformally transcendental over E', and therefore $tp_L(A_1'/B') = tp_L(A_2'/B')$ by Theorem (5.3) and Proposition (5.2) (tp_L denotes the type in the generic difference field L). Hence there is an $\mathcal{L}_\sigma(B')$-isomorphism $\varphi : acl_\sigma(B', A_1') \to acl_\sigma(B', A_2')$ which sends A_1 to A_2. Since E contains a p-basis of K if $e \in \mathbb{N}$, we get that $acl(B, A_1) = (BA_1)^s$, $acl(B, A_2) = (BA_2)^s$, so that φ restricts to an $\mathcal{L}_1(B)$-isomorphism $acl(B, A_1) \to acl(B, A_2)$. This shows that $tp(A_1/B) = tp(A_2/B)$.

Assume now that $e \in \mathbb{N}$, and that $[E : E^p] = p^f$, with $f < e$. Let $B = acl(B)$ contain E, independent from A over E, and let B_0 realise the generic $(e - f)$-type over (A, B). Then $tp(A/E)$ has a unique non-forking extension to $acl(E, B_0)$ by Proposition (4.13), and it suffices to show that $tp(acl(A, B_0)/acl(E, B_0))$ has a unique non-forking extension to $acl(B, B_0)$. The discussion in (1.8) gives that $dcl_K(A, B_0)$ is contained in $A(B_0, C)^{alg}$, for some set C of elements which are algebraically independent over $AK^{p^\infty}(B_0)$, and therefore over $A\sigma(K)(B_0)$. We then have $acl(A, B_0) \subset A(B_0, C)^{alg}_{\mathbb{N}} \cap K$, and the elements of C are transformally independent over $A(B_0)$. By step 1 of the proof of Theorem (5.3), the elements of $acl(A, B_0)$ which are transformally algebraic over $acl(E, B_0)$ are already in $acl(E, B_0)$. The previous case gives the result.

(5.5). Proposition. Let K be a model of SCFE_e, and let $k = \bigcap_n \sigma^n(K)$. Then $k \models$ ACFA, and if $D \subset K^n$ is definable, then $D \cap k^n$ is definable in the difference field (k, σ). Thus there is no induced structure on the $\mathcal{L}_\sigma$-structure k, and k is stably embedded.

Proof. Let L be the inversive closure of K. Then $L \models$ ACFA by Proposition (5.2). Note that $\sigma(k) = k$ and $k = \bigcap_n \sigma^{n+1}(K)^{alg}$ is algebraically closed.

If $a \in K$ is transformally algebraic over k, then $k(a)_{\mathbb{Z}} \subset k(\sigma(a), \ldots, \sigma^m(a))^{alg}$ for some m, so that $a \in k$. By Remark (1.1)(1) in [4], k is a model of ACFA.

Let $B = acl(B) \subset K$, and let $A = B \cap k$. Then B and k are linearly disjoint over $A = acl(A)$, and all elements of $B \setminus A$ are transformally transcendental over A. By Corollary (5.4), $tp(B/A)$ is stationary, and in particular has a unique non-forking extension to k.

This implies (see Lemma 1 in the Appendix of [4]) that k is stably embedded, and that any elementary automorphism of k lifts to an automorphism of K. But, as $k = acl(k)$ is perfect, any $\mathcal{L}_\sigma$-automorphism of k is elementary in K, and this gives the result.

(5.6). Theorem. Let K be a model of SCFE_e, let $n \geq 1$ and $m \in \mathbb{Z}$, and let F be the subfield of K consisting of the elements satisfying $\sigma^n(x) = Frob^m(x)$. Then F is a pseudo-finite field, and every subset D of F^ℓ definable in K is definable using parameters from F. If $n = 1$, then D is definable in the pure field F.

Proof. All elements of F are transformally algebraic, and therefore $F \subseteq \bigcap_{n\in\mathbb{N}} \sigma^n(K) = k$. Let $D \subseteq K^\ell$ be definable. By Proposition (5.5), $D \cap k^\ell$ is definable in the difference field (k, σ), and k is a model of ACFA. The result follows by (7.1)(5) in [6].

(5.7). Proposition. Let K be an ω-saturated model of SCFE_e. Then $K^{p^\infty} \models \mathrm{SCFE}_0$.

Proof. Clearly K^{p^∞} is algebraically closed, and σ restricts to an endomorphism of K^{p^∞}. Because K is ω-saturated, there is $a \in K^{p^\infty}$, $a \notin \sigma(K)$, and therefore σ is not onto.

Let U and V be varieties defined over K^{p^∞}, of the same dimension, and such that $V \subset U \times \sigma(U)$, and V projects dominantly onto U and onto $\sigma(U)$. Fix a generic (a, b) of the variety V over K^{p^∞}, and for each $n \geq 1$, let U_n, V_n be the varieties defined over K of which $(a, a^{1/p^n})$ and $(a, a^{1/p^n}, b, b^{1/p^n})$ are generics. Then each pair (U_n, V_n) satisfies the assumptions of (3.4)(ii). By ω-saturation of K, there are c, c_n, $n \in \mathbb{N}$ in K, such that $(c, c_n, \sigma(c), \sigma(c_n)) \in V_n$ for all n. Then $(c, \sigma(c)) \in V$, and $c \in K^{p^\infty}$.

(5.8). Sketch of an alternate proof of the independence theorem. Let K, E, a, b, c_1 and c_2 be as in Theorem (4.15), $A = acl(Ea)$, $B = acl(Eb)$, $C_1 = acl(Ec_1)$ and $C_2 = acl(Ec_2)$. Let A^0 be the difference subfield of A consisting of the elements of A which are transformally algebraic over E, and define similarly B^0, C_1^0 and C_2^0. By Lemma (4.11), we know that $A^0 \subseteq (E\sigma(A^0))^{alg}$, and similarly for B^0 and the C_i^0. Proceed as in the first part of the proof of Theorem (4.15) to show that there is C^0, independent from (A, B) over E, and realising $tp(C_1^0/A^0) \cup tp(C_2^0/B^0)$. Then consider isomorphisms $\psi_1 : acl(A^0, C_1^0) \to acl(A^0, C^0)$ and $\psi_2 : acl(B^0, C_2^0) \to acl(B^0, C^0)$, fixing A^0 and B^0 respectively, and which witness the fact that C^0 realises $tp(C_1^0/A^0) \cup tp(C_2^0/B^0)$. Let C realise a non-forking extension of $\psi_1(tp(C_1/C_1^0))$ to (A, B). Then C is independent from (A, B) over E, because C^0 is independent from (A, B) over E. By Corollary (5.4), $tp(C_1/C_1^0)$ is stationary. Hence, C realises $\psi_1(tp(C_1/A^0, C_1^0))$ and $\psi_2(tp(C_2/B^0, C_2^0))$. This implies that C realises $tp(C_1/A) \cup tp(C_2/B)$.

6 Study of modularity

(6.1). Proposition. Let $E = acl(E) \subset K \models \mathrm{SCFE}_0$, and assume that $acl(Ea)$ contains an element b which is transformally transcendental over E. Then the set S of realisations of $tp(a/E)$ is not modular.

Proof. Since $acl(Ea) = dcl(Ea)^s$, we may assume that $b \in dcl(Ea)$. Choose $c \in Fix(\sigma)$ independent from a over E, and let $d = b \cdot c$. Then $tp(d/E) = tp(b/E)$, and the set of realisations of $tp(d/Eb)$ is in definable bijection with $Fix(\sigma)$. Hence there is a definable subset S' of S which projects onto $Fix(\sigma)$. By Theorem (5.6), $Fix(\sigma)$ has no induced structure, and every infinite ∞-definable subset of $Fix(\sigma)$ is non-modular.

(6.2). Remarks. If $e \neq 0$ and we do not assume that $b \in K^{p^\infty}$, then the result does not necessarily hold. Let $a \in K$ and assume that (the pure field type) $tp_K(a/E)$ is minimal and orthogonal to the generic type of K^{p^∞}. Using Lemmas (3.3) and (4.11) one can then show that $tp(a/E)$ is minimal. By (1.15), one also obtains that $tp_K(a/E)$ uniquely determines $tp(a/E)$. Furthermore, if $tp_K(a/E)$ is modular [resp. non-trivial], so is $tp(a/E)$. These observations show that there are many non-trivial minimal modular types which are realised by non-transformally algebraic elements, using e.g. any of the types described in [12] or in [2].

In the case of a definable set S however, the result extends to the non-perfect case.

(6.3). Proposition. Let K be a model of SCFE$_e$, and let $S \subset K^n$ be definable over $E = acl(E)$. If S contains elements which are not transformally algebraic over E, then S is non-modular.

Proof. Enlarging E, we will assume that it contains a p-basis of K if $e \in \mathbb{N}$. We also assume that K is sufficiently saturated. By Corollary (4.8), using the fact that modularity and non-modularity are preserved under finite covers, we may assume that S is defined by a formula $\varphi(x) \wedge \theta(x) \wedge \rho(x)$, where $\varphi(x)$ is a quantifier-free $\mathcal{L}_\sigma(E)$-formula, $\theta(x)$ is a conjunction of formulas of the form $R_n(x_1, e)$, where e is a tuple of elements of E and $x_1 \subseteq x$, and $\rho(x)$ is an $\mathcal{L}(E)$-formula expressing that certain tuples in $x \cup E$ are p-independent in K.

First of all, assume that there is some $a \in S$ such that some sub-tuple of a is p-independent over E in K. This means that a contains a realisation a_1 of the generic 1-type over E, and implies that $tp(a/E)$ is non-modular: if $c \in Fix(\sigma)$ is independent from a_1 over E, then $tp(a_1c/E)$ also realises the generic 1-type over E. As in (6.1), this implies that S is non-modular.

Hence we may assume that S is defined by $\varphi(x) \wedge \theta(x)$. Let $a \in S$, not transformally algebraic over E. We will show that there is b in S such that the difference fields $E(a)_\mathbb{N}$ and $E(b)_\mathbb{N}$ are isomorphic, some element b_1 of b realises the generic type over E. Reasoning as in the previous paragraph will then show that non-modularity of S.

We know that $E(a)_\mathbb{N}$ is a separable extension of E. We proceed exactly as in the proof in Theorem (3.5) that the models of SCFE$_e$ are existentially closed: we let $M = \sigma(E(a)_\mathbb{N})^{alg}$, and select $a_1 \subset a$, a separating transcendence basis of $EM(a)$ over EM. As a is not transformally algebraic over E, we know that a_1 is non-empty. We then choose b_1 realising the generic $|a_1|$-type, and, as in Theorem (3.5), find b extending b_1, such that the difference fields $E(a)_\mathbb{N}$ and $E(b)_\mathbb{N}$ are E-isomorphic, by an isomorphism f sending a to b. By construction, the elements of b_1 are algebraically independent over $E\sigma(K)$. This implies that any formula of the form $R_n(y, e)$ satisfied by a sub-tuple of a will also be satisfied by the corresponding sub-tuple of b. Hence, $b \in S$.

(6.4). Theorem. Let $K \models$ SCFE$_e$ be sufficiently saturated, and let $E = acl(E) \subset K$. Let $S \subset K^n$ be a subset which is invariant under $Aut(K/E)$, and such that the elements of S are transformally algebraic over E. The following conditions are equivalent:

(1) S is non-modular.

(2) S is non-orthogonal to some fixed field, i.e., there is a tuple $a \in S$, and a set $F = acl(F)$ containing E, such that $acl(Fa) \setminus F$ contains an element b satisfying $\sigma^n(b) = Frob^m(b)$ for some $n \geq 1$ and $m \in \mathbb{Z}$.

Proof. We will work in the inversive closure L of K, and will denote by tp_L the types in the generic difference field L. Without loss of generality, if $e \in \mathbb{N}$, then E contains a p-basis of K.

If S is not modular, there are tuples a and b, with a a tuple of elements of S, such that a and b are not independent over $acl^{eq}(Ea) \cap acl^{eq}(Eb)$. Let $A = acl(Ea)$, $B = acl(Eb)$ and $C = A \cap B$. Then $C = acl(C)$, and therefore $acl_\sigma(A) \cap acl_\sigma(B) = acl_\sigma(C)$. As $C \subset acl^{eq}(Ea) \cap acl^{eq}(Eb)$, we certainly have that A and B are not independent over C.

Our assumption on the elements of S and Lemma (4.11)(2) imply that A and B are not linearly disjoint over C. Let $d \in A$ be such that the field $C(d)_{\mathbb{N}}$ and B are not linearly disjoint over C. Then $acl_\sigma(C)(d)_{\mathbb{Z}}$ and $acl_\sigma(B)$ are not linearly disjoint over $acl_\sigma(C)$. By Proposition (1.19), $tp_L(d/acl_\sigma(C))$ is non-orthogonal to the formula $\sigma^n = x^{p^m}$ for some $n \geq 1$ and $m \in \mathbb{Z}$ (where p is the characteristic of K if it is positive, and 1 if it is 0). Let $Fix(\tau)$ be the subfield of L defined by $\sigma^n = x^{p^m}$. Then $Fix(\tau) \subseteq K$.

Claim. There are independent realisations $d_1, \dots, d_k$ of $tp(d/C)$ in K, such that $Fix(\tau) \cap C(d_1, \dots, d_k)_{\mathbb{N}}$ contains an element b not in C.

Proof. Indeed, since $tp_L(d/acl_\sigma(C))$ is non-orthogonal to $\sigma^n(x) = x^{p^m}$, there is an integer k and independent realisations $d_1, \dots, d_k$ of $tp_L(d/acl_\sigma(C))$, and an element $b \in Fix(\tau) \cap acl_\sigma(C)(d_1, \dots, d_k)_{\mathbb{Z}}$, $b \notin acl_\sigma(C)$. Note that $\sigma(Fix(\tau)) = Fix(\tau)$. Hence, replacing b by $\sigma^\ell(b)$ for a suitable ℓ, we may assume that $b \in C(d_1, \dots, d_k)_{\mathbb{N}}$.

This only depends on the isomorphism type of the difference field $C(d_1, \dots, d_k)_{\mathbb{N}}$, and therefore we may assume that $d_1, \dots, d_k$ are independent realisations of $tp(d/C)$.

Since $d_1, \dots, d_k$ are independent realisations of $tp(d/C)$, we may choose $a_1, \dots, a_k$ in K such that $tp(a_i, d_i/C) = tp(a, d/C)$. Then $b \in C(a_1, \dots, a_k)_{\mathbb{N}}$.

The other direction is easy: $Fix(\tau) \subseteq k = \bigcap_{\ell \in \mathbb{N}} \sigma^\ell(K)$, and the only induced structure on k is that of an $\mathcal{L}_\sigma$-structure model of ACFA (by (5.5)). By the main result of [6], every non-algebraic type which is non-orthogonal to a fixed field is non-modular.

(6.5). Concluding remarks.

Let K be a model of SCFE$_e$, $E = acl(E) \subset K$. If $D \subset K^n$ is definable and consists of elements transformally algebraic over E, then we know by Remark (4.17) that D has finite SU-rank. Moreover forking in K coincides with forking in the sense of the $\mathcal{L}_\sigma$-structure L which is the inversive closure of K. Hence, if D is modular and the characteristic of K is 0, then we know that all types realised in D are stable, and that D is stably embedded over E, see (1.19).

Let G be a modular group definable over E in K. We know by Proposition (6.3) that if $a \in G$ then a is tranformally algebraic over E, so that by Lemma (4.11), $acl(Ea)$ is contained in $E(a)_{\mathbb{N}}^{alg}$. By the results of [15] and this description of algebraic closure, there is a definable map $f : G_1 \to H(K)$, where H is an algebraic group, G_1 is a definable subgroup of G of finite index, and $Ker(f)$ is finite. Theorem (1.23) then yields a nice description of quantifier-free definable subsets of $f(G_1)$.

Appendix A - Stationarity almost over a predicate

In this appendix, we mention a general result that (using Theorem (5.3)) gives another proof of the validity of the independence theorem in SCFE over bases contained in k.

A.1 Setting. Let T be a complete theory in a language $\mathcal{L}$. We assume that we have a notion of independence in $\mathcal{U}^{eq}$ which is well-behaved, i.e., it is $Aut(\mathcal{U})$-invariant and, for all $A \subseteq B \subseteq C \subseteq \mathcal{U}$, and tuple a in $\mathcal{U}$ we have:

(i) (Extension property) There is a' realising $tp(a/A)$ and which is independent from B over A.

(ii) (Transitivity) a is independent from C over A if and only if it is independent from B over A and from C over B.

(iii) (Finite character) For any $D \subseteq \mathcal{U}$, D is independent from B over A if and only if every finite tuple of elements of D is independent from B over A.

(iv) (Symmetry) a is independent from B over A if and only if B is independent from a over A.

(v) (Local character) There is $A_0 \subset A$, with $|A_0| \leq |\mathcal{L}| + \aleph_0$, such that a is independent from A over A_0.

A.2 Definition. Let $\mathcal{U}$ be a sufficiently saturated model of a theory T in a language $\mathcal{L}$. Let $S \subset \mathcal{U}^{eq}$ be preserved under all automorphisms of $\mathcal{U}$. We say that $\mathcal{U}$ is *stationary almost over* S if for all subsets $A \subset B$ of $\mathcal{U}$, $tp(acl^{eq}(B)/acl^{eq}(B) \cap acl^{eq}(S, A))$ is stationary.

Here stationarity is meant with respect to our independence notion: if C contains $acl^{eq}(B) \cap acl^{eq}(S, A)$, then there is a unique type over C extending $tp(acl^{eq}(B)/acl^{eq}(B) \cap acl^{eq}(S, A))$ and whose realisations are independent from C over $acl^{eq}(B) \cap acl^{eq}(S, A)$.

A.3 Remark. If $\mathcal{U}$ is stationary almost over S, then S is stably embedded.

Proof. See Lemma 1 in the Appendix of [4].

A.4 Proposition. Assume that $\mathcal{U}$ is stationary almost over S. Let A, B, C_1, C_2, E, be algebraically closed subsets of $\mathcal{U}^{eq}$ satisfying the following conditions:

(1) A is independent from B over E, C_1 is independent from A over E and C_2 is independent from B over E.

(2) $tp(C_1/E) = tp(C_2/E)$.

(3) There is $\tilde{C} \subset acl^{eq}(S)$ realising $tp(C_1 \cap acl^{eq}(S)/A \cap acl^{eq}(S)) \cup tp(C_2 \cap acl^{eq}(S)/B \cap acl^{eq}(S))$, which is independent from $(A \cap acl^{eq}(S), B \cap acl^{eq}(S))$ over $\tilde{E} = E \cap acl^{eq}(S)$.

Then there is $C \subseteq \mathcal{U}^{eq}$ realising $tp(C_1/A) \cup tp(C_2/B)$ and which is independent from (A, B) over E.

Proof. Let $\tilde{C}$ be as given by (3), and independent from (A, B) over $\tilde{E}$.

Let $A' = acl^{eq}(E, A \cap acl^{eq}(S))$, $B' = acl^{eq}(E, B \cap acl^{eq}(S))$. By stationarity almost over S, $tp(A'/A \cap acl^{eq}(S))$ has a unique non-forking extension to $(A \cap acl^{eq}(S), \tilde{C})$, and therefore $tp(\tilde{C}/A') = tp(C_1 \cap acl^{eq}(S)/A')$. Hence $C' = acl^{eq}(E, \tilde{C})$ and $C_1' = acl^{eq}(E, C_1 \cap acl^{eq}(S))$ have the same type over A'. Similarly, C' and $C_2' = acl^{eq}(E, C_2 \cap acl^{eq}(S))$ have the same type over B'.

Choose C independent from (A, B), and such that $tp(C, C'/E) = tp(C_1, C_1'/E)$. We know that $tp(C_1/C_1')$ is stationary, and therefore $tp(C/A) = tp(C_1/A)$ because C and C_1 are independent from A over C', C_1', respectively. Similarly, $tp(C/B) = tp(C_2/B)$.

A.5 Corollary. Let $E = acl^{eq}(E) \subseteq \mathcal{U}^{eq}$, and assume that in $acl^{eq}(S)$, the independence theorem holds over $\tilde{E} = E \cap acl^{eq}(S)$. Then it holds in $\mathcal{U}$ over E.

A.6 Corollary. If $Th(acl^{eq}(S))$ is simple, and the restriction of the independence notion to $acl^{eq}(S)$ coincides with non-forking, then T is also simple, and our notion of independence coincides with non-forking.

Proof. By results of Kim-Pillay [14], the independence theorem holds in $acl^{eq}(S)$ over submodels, and our results imply that it holds in $\mathcal{U}$ over submodels. Moreover, the properties satisfied by our independence notion imply that it coincides with non-forking.

Appendix B

In this appendix we provide a proof of Claim (5.3) not relying on the results of [13].

B.1 Proposition. Let T be a first-order theory, with saturated model $\mathcal{U}$. Assume given a function rk defined on consistent formulas over $\mathcal{U}$, into $\mathbb{N}\cup\{\infty\}$. Assume $rk(\varphi) \leq rk(\psi)$ if φ implies ψ. Define $rk(a/B) = \inf\{rk(\varphi) \mid \varphi \in tp(a/B)\}$.

Assume

(i) Definability: if $rk(\varphi(x,a)) = m \in \mathbb{N}$, then there exists $\psi \in tp(a)$ such that $\psi(a')$ implies $rk(\varphi(x,a')) = m$.

(ii) Density: over any set A, any consistent formula over A is implied by some consistent formula of finite rank over A.

(iii) Additivity: $rk(ab/C) = rk(b/C) + rk(a/Cb)$.

(iv) Zero: $rk(\varphi) = 0$ iff φ has finitely many solutions.

(v) For any set A, there exists $c \notin A$ such that if $rk(d/A) < \infty$ then $tp(d/A)$ implies $tp(d/Ac)$.

Then there exists an automorphism of $\mathcal{U}$ fixing the finite rank part (i.e. fixing pointwise every 0-definable set of finite rank), and which is not the identity.

B.2 Definition. $tp(a/B)$ is j-isolated if for some $\varphi(x) \in tp(a/B)$, whenever $\varphi(a')$ holds, then $rk(a'/B) = rk(a/B)$.

B.3 Remark. In the definition of j-isolated, $rk(a/B)$ is necessarily finite (using density.)

B.4 Lemma. $tp(b_1b_2/C)$ is j-isolated iff both $tp(b_1/C)$ and $tp(b_2/Cb_1)$ are.

Proof. First suppose $tp(b_1b_2/C)$ is j-isolated, say by $\varphi(x_1,x_2)$. Then $\varphi(b_1,x_2)$ j-isolates $tp(b_2/Cb_1)$, by additivity of rk. Find $\psi(x_1) \in tp(b_1/C)$ such that $\psi(b_1')$ implies $rk(\varphi(b_1',x_2)) = rk(\varphi(b_1,x_2))$. Then $\psi(x_1) \wedge (\exists x_2)\,\varphi(x_1,x_2)$ j-isolates $tp(b_1/C)$. The converse is similar.

B.5 Definition. (B/C) is j-atomic if for any finite tuple b from B, $tp(b/C)$ is j-isolated.

B.6 Lemma. Assume (B/C) is j-atomic, and (a/BC) is j-isolated. Then (aB/C) is j-atomic.

Proof. Similar to the above.

B.7 Lemma. Let $A \subset \mathcal{U}$. Then there exists a model M, $A \subset M$, with (M/A) j-atomic.

Proof. Let $B \subset \mathcal{U}$ be maximal j-atomic over A, and assume by way of contradiction that B is not an elementary substructure of $\mathcal{U}$. Then there is a formula $\varphi(x) \in \mathcal{L}(B)$ which is realised in $\mathcal{U}$ and not in B. Take such a formula of minimal rank m, which by density is in $\mathbb{N}$. If $m = 0$, then any realisation of φ is in $acl(B)$ and its type over B is isolated. Assume $m > 0$, and take $b \in \mathcal{U}$ satisfying φ. Then $rk(b/B) = m$ (by the minimality of $rk(\varphi)$), and so $tp(b/B)$ is j-isolated. By (B.6), (Bb/A) is j-atomic, and this gives us the required contradiction.

B.8 *Proof of Proposition B.1.* Now let M_0 be a small model (size of language.) Using (v), construct a large set I such that $rk(d/M_0) < \infty$ implies $tp(d/M_0) \vdash tp(d/M_0 I)$.

Let M be a j-atomic model over $M_0 I$. If $a \in M$ with $rk(a/M_0) < \infty$, then $tp(a/M_0 I)$ is j-isolated; since $tp(a/M_0) \vdash tp(a/M_0 I)$, $tp(a/M_0)$ is also j-isolated. But this implies that $a \in M_0$. Thus the finite rank part of M is contained in M_0. By Morley's two cardinal theorem (since I is large compared to M_0), if we choose a Skolemization L', T' of the language, there exists a model M' of T' with an indiscernible sequence over M_0 and which does not realise any finite rank non-algebraic type over M_0. This model clearly has automorphisms fixing the finite rank part (which is contained in M_0). Hence so does $\mathcal{U}$.

B.9 Remarks. (1) Note that Proposition B.1 also holds if (v) is weakened to: For any set A, there exists $c \notin A$ such that if $rk(d/A) < \infty$ and $tp(d/Ac)$ is j-isolated then so is $tp(d/A)$, and they have the same rank.

Indeed, one constructs a large set I such that if $rk(d/M_0) < \infty$ and $tp(d/M_0 I)$ is j-isolated, then so is $tp(d/M_0)$ and they have the same rank. Thus all elements of M not in M_0 have infinite rank over M_0.

(2) If T satisfies (i) – (v), and $A \subset \mathcal{U}$, so does $T(A)$ $(= Th(\mathcal{U}, a)_{a \in A}))$.

B.10 Proposition. The hypotheses hold for ACFA: take rk to be transformal order, i.e., $rk(\varphi(x, a)) = \sup\{tr.deg(A(b)_{\mathbb{Z}}/A) | \models \varphi(b, a)\}$, where A is the difference field generated by a; in (v), take c transformally transcendental over A (see (1.15)).

B.11 Corollary (Claim (5.3)). Let $A \subset B$ be algebraically closed difference subfields of a model L of ACFA, and assume that all elements of B which are transformally algebraic over A are already in A. Let $b \in B \setminus A$. Then in some elementary extension $\mathcal{U}$ of L, there is an automorphism h of $\mathcal{U}$ which is the identity on the set of elements of $\mathcal{U}$ which are transformally algebraic over A, and which moves b.

Proof. By Propositions B.1, B.10 and Remark B.9 (2), there is a saturated model $\mathcal{U}$ of ACFA containing A, and with an automorphism h which is the identity on the set of elements transformally algebraic over A, and moves some element c. Then c is transformally transcendental over A, as is b. By (1.15), $tp(b/A) = tp(c/A)$, so that there is an A-automorphism φ of $\mathcal{U}$ which sends b to c. Then $h\varphi(b) \neq \varphi(b)$, so that $\psi = \varphi^{-1}h\varphi$ is the identity on the set of elements transformally algebraic over A and moves b.

References

[1] N. Bourbaki, XI, *Algèbre Chapître 5*, Corps commutatifs, Hermann, Paris 1959.

[2] E. Bouscaren, F. Delon, Minimal groups in separably closed fields, J. Symbolic Logic 67 (2002), no. 1, 239–259.

[3] Z. Chatzidakis, Generic automorphisms of separably closed fields, Illinois J. Math. 45 (2001), no. 3, 693–733.

[4] Z. Chatzidakis, E. Hrushovski, Model theory of difference fields, Trans. A.M.S. 351 (1999), 2997 – 3071.

[5] Z. Chatzidakis, E. Hrushovski, Asymptotic theories of differential fields, Illinois J. of Mathematics 47 Nr 3 (2003), 593 – 618.

[6] Z. Chatzidakis, E. Hrushovski, Y. Peterzil, Model theory of difference fields, II: Periodic ideals and the trichotomy in all characteristics, Proceedings of the London Math. Society (3) 85 (2002), 257 – 311.

[7] R.M. Cohn, *Difference algebra*, Tracts in Mathematics 17, Interscience Pub. 1965.

[8] F. Delon, *Idéaux et types sur les corps séparablement clos*, Supplément au Bull. de la S.M.F, Mémoire 33, Tome 116, 1988.

[9] L. van den Dries, K. Schmidt, Bounds in the theory of polynomials rings over fields. A non-standard approach. Invent. Math. 76 (1984), 77 – 91.

[10] Yu. Ershov, Fields with a solvable theory (eng. transl.), Sov. Math. Doklady 8 (1967), 575 – 576.

[11] W. Hodges, *Model theory*, Encyclopedia of Mathematics and its Applications, 42, Cambridge University Press, Cambridge, 1993.

[12] E. Hrushovski, The Mordell-Lang conjecture for function fields, J. of the AMS Vol 9 Nr 3 (1996), 667 – 690.

[13] E. Hrushovski, The first-order theory of the Frobenius, preprint (1996).

[14] B. Kim, A. Pillay, Simple theories, APAL 88 Nr 2-3 (1997), 149 – 164.

[15] P. Kowalski, A. Pillay, A note on groups definable in difference fields, Proceedings of the AMS, 130 (2001), 205 – 212.

[16] S. Lang, *Introduction to algebraic geometry*, Addison-Wesley Pub. Co., Menlo Park 1973.

[17] A. Macintyre, Nonstandard Frobenius, in preparation.

[18] F. Wagner, *Simple theories*, Kluwer Academic Pub., Dordrecht 2000.

[19] C. Wood, Notes on the stability of separably closed fields, JSL 44 (1979), 412 – 416.

Current addresses:

UFR de Mathématiques
Université Paris 7, Case 7012
2, place Jussieu

75251 Paris Cedex 05
France
e-mail: zoe@logique.jussieu.fr

Institute of Mathematics
The Hebrew University
Givat Ram
91904 Jerusalem
Israel
e-mail: ehud@math.huji.ac.il