Illinois Journal of Mathematics
Volume 45, Number 3, Fall 2001, Pages 693–733
S 0019-2082

GENERIC AUTOMORPHISMS OF SEPARABLY CLOSED FIELDS

ZOÉ CHATZIDAKIS

ABSTRACT. We show that the class of separably closed fields with a generic automorphism is an elementary class, whose theory is model complete in a natural extension of the language of fields with an automorphism. We describe the completions of this theory and obtain some results on types, imaginaries, and modularity.

Introduction

Generic automorphisms of a saturated structure M appear in a paper by Lascar [L], where they are used towards the study of the automorphism group $\mathrm{Aut}(M)$. In many cases, if σ is a generic automorphism of M, then the structure (M, σ) is existentially closed in the class of models of $\mathrm{Th}(M)$ with a distinguished automorphism σ. A natural question arises: Given a model-complete theory T, does the theory of models of T with a distinguished automorphism σ have a model companion T_A? In [CP], Pillay and I showed that if this model-companion T_A exists, then it is well-behaved, and we obtained a description of the completions of T_A and of the types. In case T is also stable, we showed that T_A is simple (unstable in most cases), and obtained a description of the imaginaries in terms of the imaginaries of the models of T.

At the moment there is no general criterion for the existence of the theory T_A. We know that it exists when T is the theory of algebraically closed fields (see [M] and [CH]), or when T is the theory of differentially closed fields of characteristic 0 (unpublished result of Hrushovski). There are also some criteria of existence when T is ω-stable of finite rank; more details are given in [CP] (see also [KkP]). The theory T_A is known not to exist for various unstable theories T; see Kikyo's paper [K].

Consider the theory $T = \mathrm{SCF}_e$ of separably closed fields of degree of imperfection e, where $e \in \mathbb{N} \cup \{\infty\}$. Does T_A exist? Recall that a field with a distinguished automorphism σ is called a difference field, so our question

Received January 10, 2000; received in final form October 18, 2000.
2000 *Mathematics Subject Classification.* Primary 03C60. Secondary 03C45.

is equivalent to the following: Does the theory of separably closed difference fields of a fixed degree of imperfection have a model-companion?

As stated, the question has an immediate negative answer, since SCF_e is not model complete in the language $\mathcal{L}$ of rings. Hence we first need to enrich the language $\mathcal{L}$, and expand the theory SCF_e accordingly, so that in the new language, if $K \subseteq L$ are fields then L is a separable extension of K. This is done by adding to $\mathcal{L}$ new function symbols, called the λ-functions (see Section 1), getting a language $\mathcal{L}_\lambda$, and adding to T the axioms defining these functions to obtain the theory $\mathrm{SCF}_{e,\lambda}$. As these functions are definable within the field language, we are not adding any definable sets, but only strengthening the notion of substructure. If e is finite, one can instead add constant symbols $b_1, \ldots, b_e$ for the elements of a p-basis. Then $\mathrm{SCF}_{e,b} = \mathrm{SCF} \cup \{b_1, \ldots, b_e \text{ form a } p\text{-basis}\}$ is complete and model-complete in $\mathcal{L}(b_1, \ldots, b_e)$, but does not eliminate quantifiers.

Even with this first adjustment the problem is slightly delicate, because separably closed fields have a very rich and complicated structure. For instance, observe that if $\sigma \in \mathrm{Aut}(K)$ and $a \in K$ satisfies the equation $\sigma(x) = x^p$, then necessarily $a \in \bigcap_{n\in\mathbb{N}} K^{p^n}$. Thus the formula $\sigma(x) = x^p$ implies an infinite conjunction of $\mathcal{L}$-formulas (modulo $T \cup \{\sigma \text{ is an automorphism}\}$).

The main result of this paper is that if T is the appropriate extension of the theory of separably closed fields in $\mathcal{L}_\lambda$ (or possibly in $\mathcal{L}(b_1, \ldots, b_e)$ if we consider only fields of finite degree of imperfection), then T_A exists. We then derive some easy consequences along the lines of [CP] and [CH].

This paper is organised as follows. In Section 1, we set up the notation and conventions, and recall the basic facts on difference fields and separably closed fields needed in the paper. In Section 2 we show the existence and give axiomatisations of the model companion $\mathrm{SCFA}_{e,\lambda}$ of the theory of difference fields models of T_λ and of degree of imperfection $\leq e$ (see (2.6) and (2.12)); the cases of finite and infinite degree of imperfection need to be treated separately. We deduce the existence and an axiomatisation $\mathrm{SCFA}_{e,b}$ of the model companion $\mathrm{SCFA}_{e,b}$ of the theory (in the language $\mathcal{L}_\sigma(\bar{b})$) of difference fields with fixed p-basis $\bar{b} = \{b_1, \ldots, b_e\}$ (see (2.7)). In Section 3, we describe the completions of $\mathrm{SCFA}_{e,\lambda}$, its types, the formulas, and prove the independence theorem and elimination of imaginaries of the completions of $\mathrm{SCFA}_{e,b}$. These results are slightly stronger than those obtained by applying the results of [CP], but their proofs follow the same lines. In Section 4, we extend various results obtained in [CH] for the model companion ACFA of the theory of difference fields to $\mathrm{SCFA}_{e,\lambda}$: Let $(K, \sigma) \models \mathrm{SCFA}_{e,\lambda}$; then $\mathrm{Fix}(\sigma)$ is a PAC-field of degree of imperfection e, with absolute Galois group $\hat{\mathbb{Z}}$; if $n \geq 1$ then $(K, \sigma^n) \models \mathrm{SCFA}_{e,\lambda}$; if K is ω-saturated, then $\bigcap_n K^{p^n} \models \mathrm{ACFA}$. We also show that if K is a separable extension of the difference field k and is a model of $\mathrm{SCFA}_{e,\lambda}$, then the subfield of K consisting of elements which are

transformally algebraic over k is an elementary substructure of K. In Section 5 we study modular sets.

1. Preliminaries on difference fields and fields of positive characteristic

(1.1) Setting and notation. We will always work inside a large algebraically closed field Ω *of characteristic* $p > 0$, which will contain all fields considered. The language $\mathcal{L}_\sigma$ is obtained by adjoining to the language $\mathcal{L} = \{+, -, \cdot, 0, 1\}$ of rings a unary function symbol for σ. A difference field is a field K with a distinguished automorphism σ, and is naturally an $\mathcal{L}_\sigma$-structure. I should mention that our definition of difference fields slightly differs from the usual definition which only requires σ to be a field embedding, i.e., not necessarily onto. Our difference fields are called *inversive* by Cohn. All the basic algebraic results on difference fields can be found in the first few chapters of Cohn's book [C].

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. Since we are in characteristic p, the map Frob: $x \mapsto x^p$ defines a monomorphism on K, called the *Frobenius automorphism*, and the image K^p of K by this map is a subfield of K. Similarly, we denote by $K^{1/p}$ the image of K by the inverse of the Frobenius automorphism. We denote by K^{p^∞} the field $\bigcap_{n\in\mathbb{N}} K^{p^n}$, and by $K^{p^{-\infty}}$ the field $\bigcup_{n\in\mathbb{N}} K^{1/p^n}$. $\mathbb{A}^k$ denotes the k-dimensional affine space, and $\mathbb{A}^k(K)$ its K-rational points. We also view $\mathbb{A}^k(K)$ as a k-dimensional K-vector space.

We assume familiarity with the basic notions of algebraic geometry: algebraic sets and varieties (or absolutely irreducible algebraic sets), generic points, linear disjointness, separable and regular extensions; see, e.g., [L2, Chap. I–III].

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

- K is an algebraically closed field and σ is an automorphism of K.
- If U and V are varieties defined over K, such that $V \subseteq U \times \sigma(U)$ and the projections $V \to U$ and $V \to \sigma(U)$ are generically onto, then there is a tuple $\bar{a}$ such that $(\bar{a}, \sigma(\bar{a})) \in V$. (Here $\sigma(U)$ denotes the variety image by σ of the variety U.)

(1.3) Difference polynomial rings. Let $k \subseteq K$ be difference fields, with K a sufficiently saturated model of ACFA. We define the *difference polynomial ring* $k[X_1, \ldots, X_n]_\sigma$ by taking the ring $k[X_1, \ldots, X_n]_\sigma$ to be the ordinary polynomial ring $k[\sigma^j(X_i) \mid i = 1, \ldots, n; j \in \mathbb{N}]$, and extending σ to

$k[X_1, \ldots, X_n]_\sigma$ 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 $k[X_1, \ldots, X_n]_\sigma$ satisfying $\sigma(I) \subseteq I$ are called *σ-ideals*. A *perfect* σ-ideal of $k[X_1, \ldots, X_n]_\sigma$ 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 $k[X_1, \ldots, X_n]_\sigma$ by prime σ-ideals are domains on which σ defines an embedding. Thus they embed uniquely in a smallest difference field. If $\bar{a}$ is an n-tuple of K, we define $I_\sigma(\bar{a}/k) = \{f(\bar{X}) \in k[\bar{X}]_\sigma \mid f(\bar{a}) = 0\}$, where $\bar{X} = (X_1, \ldots, X_n)$. Then $I_\sigma(\bar{a}/k)$ is a prime σ-ideal of $k[X_1, \ldots, X_n]_\sigma$.

While $k[X_1, \ldots, X_n]_\sigma$ has infinite ascending chains of σ-ideals, it satisfies the ascending chain condition on perfect σ-ideals and on prime σ-ideals. A *σ-equation* (over k) is an equation of the form $f(x_1, \ldots, x_n) = 0$ where $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]_\sigma$. The set of solutions (in K^n) of a set of σ-equations is called a *σ-closed set*; it can be defined by a finite set of σ-equations. Thus the topology on K^n whose basic closed sets are the σ-closed sets is Noetherian. A σ-closed set is called *irreducible* if it is not the union of two proper σ-closed subsets. Every σ-closed set of K^n is the union of finitely many irreducible σ-closed sets, which are called its *irreducible components*. If the irreducible σ-closed set V is defined by σ-equations over k, then V is *defined over* k, and the set of difference polynomials over k vanishing on V is a prime σ-ideal of $k[X_1, \ldots, X_n]_\sigma$, denoted by $I(V)$. If $\bar{a} \in K^n$ and $I(V) = I_\sigma(\bar{a}/k)$, then a is called a *generic of V* over k.

(1.4) Transformal transcendence bases. Let $k \subseteq K$ be as above, and let $\bar{a}$ be a tuple of elements of K. We denote by $k(\bar{a})_\sigma$ the difference field generated by $\bar{a}$ over k, i.e., the difference subfield $k(\sigma^i(\bar{a}) \mid i \in \mathbb{Z})$ of K. If the transcendence degree $\mathrm{tr.deg}(k(\bar{a})_\sigma/k)$ of $k(\bar{a})_\sigma$ over k is finite then we say that $\bar{a}$ is *transformally algebraic over k*. In that case, there is a non-negative integer m such that $k(\bar{a})_\sigma \subseteq k(\bar{a}, \ldots, \sigma^m(\bar{a}))^{\mathrm{alg}}$. Observe that since σ and σ^{-1} are automorphisms of $k(\bar{a})_\sigma$, we then have $k(\bar{a})_\sigma \subseteq k(\sigma^j(\bar{a}), \ldots, \sigma^{j+m}(\bar{a}))^{\mathrm{alg}}$ for every $j \in \mathbb{Z}$.

An element $b \in K$ is *transformally transcendental over k*, if the elements $\sigma^i(b)$, $i \in \mathbb{Z}$, are algebraically independent over k. Observe that a tuple $\bar{a}$ is either transformally algebraic over k, or contains an element which is transformally transcendental over k. We call a set $B \subseteq K$ *transformally independent* over k if the elements $\sigma^j(b)$, $b \in B$, $j \in \mathbb{Z}$, are algebraically independent over k, or, equivalently, if the elements $\sigma^j(b)$, $b \in B$, $j \in \mathbb{N}$, are algebraically independent over k. If L is a difference subfield of K containing k, and $B \subset L$ is a maximal transformally independent set over k, then B is called a *transformal transcendence basis* of L over k. Observe that L is then transformally algebraic over $k(B)_\sigma$. Any two transformal transcendence

bases of L over k have the same cardinality, and this cardinality is called the transformal transcendence degree of L over k, and denoted by $\Delta(L/k)$. If $\bar{a}$ is a finite tuple, we also define $\Delta(\bar{a}/k) = \Delta(k(\bar{a})_\sigma/k)$; observe that $\Delta(\bar{a}/k) \leq \mathrm{tr.deg}(k(\bar{a})/k)$ (the transcendence degree of $k(\bar{a})$ over k).

(1.5) p-bases. Details and proofs can be found in [B, §13]. Let K be a field of characteristic $p > 0$ 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 $b_1, \ldots, b_n \in K$ are *p-independent over k* if the set of *p-monomials in $b_1, \ldots, b_n$*, i.e., monomials of the form $b_1^{i(1)} \cdots b_n^{i(n)}$ with $0 \leq i(1), \ldots, i(n) \leq p-1$, is linearly independent in the kK^p-vector space K, or, equivalently, if $b_i \notin kK^p(b_1, \ldots, b_{i-1})$ for $i = 1, \ldots, n$.

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. We define the *degree of imperfection* of a field K as the size of B if K has a finite p-basis B, and ∞ otherwise. Observe that a p-basis of K over k is also a p-basis of K^s over k and over k^s.

(1.6) Derivations. Let $R \subset S$ be commutative rings. Recall that an R-derivation on S is an additive map $\delta : S \to S$ which vanishes on R and satisfies $\delta(xy) = \delta(x)y + x\delta(y)$. Let $A \subseteq \Omega$ be a finite set, and assume that every k-derivation on $k(A)$ vanishes on $k(A)$. Then $k(A)$ is separably algebraic over k (see [L1, Prop. X.7.2]). We will use the following easy consequence of this fact:

LEMMA. *Let A, B be finite subsets of Ω.*

(1) *$A \subseteq k(A^p)$ if and only if A is separably algebraic over k.*
(2) *Assume that A is separably algebraic over $k(B^p)$ and that B is separably algebraic over $k(A)$. Then (A, B) is separably algebraic over k.*

Proof. (1) If a is separably algebraic over k then $a \in k(a^p)$, and this gives the right-to-left implication. Conversely, assume that $A \subset k(A^p)$ and let D be a k-derivation on $k(A)$. Then D vanishes on $k(A^p)$, and therefore vanishes on A. Hence A is separably algebraic over k.

(2) Let D be a k-derivation on $k(A, B)$. Then D vanishes on $k(B^p)$ and therefore vanishes on A since A is separably algebraic over $k(B^p)$. This implies that D vanishes on B, and therefore that (A, B) is separably algebraic over k.

(1.7). Recall that K is a *separable* extension of k if k and K^p are linearly disjoint over k^p, or, 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 $\bigcup_{n\in\mathbb{N}} k(t^{1/p^n})$ 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. Observe, however, that if B is a p-basis of K over k, then the elements of B are algebraically independent over k.

(1.8) Separably closed fields and the λ-functions. 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 [E]), which we denote by SCF_e, and is stable (Wood [W]). If K is separably closed and $\{b_1, \ldots, b_e\}$ is a p-basis of K, then $\mathrm{SCF}_{e,b} = \mathrm{Th}(K, b_1, \ldots, b_e)$ is model complete in the language $\mathcal{L}(b_1, \ldots, b_e)$.

For each n fix an enumeration $m_{i,n}(\bar{x})$ $(1 \leq i \leq p^n)$ of the p-monomials $x_1^{i(1)} \cdots x_n^{i(n)}$ with $0 \leq i(1), \ldots, i(n) \leq p-1$, 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

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

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 language, and we call them the *λ-functions of K*.

Consider the language $\mathcal{L}_\lambda = \mathcal{L} \cup \{\lambda_{i,n} \mid n \in \mathbb{N},\ 1 \leq i \leq p^n\}$, and let T_λ be the $\mathcal{L}_\lambda$-theory obtained by adjoining to the theory of fields axioms expressing the defining properties of the functions $\lambda_{i,n}$. Let $\mathrm{SCF}_{e,\lambda} = \mathrm{SCF}_e \cup T_\lambda$. Then $\mathrm{SCF}_{e,\lambda}$ is complete and eliminates quantifiers but does not eliminate imaginaries (Delon [D]).

Fix a separably closed field K. When the degree of imperfection of K is finite, one may fix a p-basis $\{b_1, \ldots, b_e\}$ of K, and only consider the unary functions $\lambda_{i,e}(b_1, \ldots, b_e; x)$. Then $\mathrm{Th}(K)$ eliminates quantifiers and imaginaries in the language $\mathcal{L}_\lambda(b_1, \ldots, b_e) = \mathcal{L} \cup \{b_1, \ldots, b_e, \lambda_{i,e}(b_1, \ldots, b_e; -) : 1 \leq i \leq p^e\}$ (Delon [D]).

(1.9) Lemma. *Let L be a subfield of K. Then K is a separable extension of L if and only if L is closed under the λ-functions of K.*

Proof. This follows easily from the definition of the λ-functions of K, but we will give the proof. Assume that K is not a separable extension of L. Choose a tuple $(a_1, \ldots, a_n) \in L^n$ which is p-independent in L but not in K, with n minimal. Then $a_1, \ldots, a_{n-1}$ are p-independent in K, and $a_n \in K^p[a_1, \ldots, a_{n-1}]$, $a_n \notin L^p[a_1, \ldots, a_{n-1}]$. Hence $\lambda_{i,n-1}(a_1, \ldots, a_{n-1}; a_n) \in K \setminus L$ for some i. This shows one direction. For the other direction assume that for some $a_1, \ldots, a_n \in L$ and some i the element $\lambda_{i,n-1}(a_1, \ldots, a_{n-1}; a_n)$ is not in L. Note that the $\lambda_j(a_1, \ldots, a_{n-1}; a_n)$ are (the unique) solutions of the equation $(*) : \sum_j X_j^p m_{j,n-1}(a_1, \ldots, a_{n-1}) = a_n$. From $\lambda_{i,n-1}(a_1, \ldots, a_{n-1}; a_n) \notin L$, we obtain first that $\{a_1, \ldots, a_{n-1}\}$ is p-independent in K, and then that $\{a_1, \ldots, a_n\}$ is p-independent in L, for otherwise there would be elements b_j in L satisfying $(*)$ in L, and we would have $b_j = \lambda_{j,n-1}(a_1, \ldots, a_{n-1}; a_n) \in K$ for all j. Thus $a_1, \ldots, a_n$ is p-independent in L but not in K.

(1.10) Basic λ-terms. We work in a large separably closed field K, with finite p-basis $B = \{b_1, \ldots, b_e\}$. We let $I = I(B) = \{1, \ldots, p^e\}$, $\lambda_i(B; -) = \lambda_{i,e}(b_1, \ldots, b_e; -)$ and $m_i(B) = m_{i,e}(b_1, \ldots, b_e)$. If $\mu \in I^n$, we define by induction on n the function $\lambda_\mu(B; -)$ and the p^n-monomial $m_\mu(B)$ as follows: if $n = 0$, then $\lambda_\mu(B; x) = x$, $m_\mu(B) = 1$; if $n \geq 1$, write $\mu = \nu^\frown i$, where $\nu \in I^{n-1}$, $i \in I$, and define

$$\lambda_\mu(B; x) = \lambda_i(B; \lambda_\nu(B; x)), \qquad m_\mu(B) = m_i(B)^{p^{n-1}} m_\nu(B).$$

Then we have, for any $a \in K$ and $n \in \mathbb{N}$,

$$a = \sum_{\mu \in I^n} \lambda_\mu(B; a)^{p^n} m_\mu(B).$$

If $\mu \in I^n$, we call λ_μ a *λ-term of level n*. Note that all basic λ-terms are terms of the language $\mathcal{L}_\lambda(b_1, \ldots, b_e)$. We let $I^{<\omega} = \bigcup_{n \in \mathbb{N}} I^n$.

If $B \subseteq K$ is infinite, then by abuse of notation, we will denote by $\{\lambda_\mu(B; x) \mid \mu \in I^n\}$ the set of all terms $\lambda_\mu(b_1, \ldots, b_e; x)$ where $e \in \mathbb{N}$, $b_1, \ldots, b_e \in B$, and $\mu \in I(\{b_1, \ldots, b_e\})^n$. Note that for a given element $c \in K$, the set $\{\lambda_\mu(B; c) \mid \mu \in I^n\}$ is finite, and that $c \in \mathbb{F}_p[\lambda_\mu(B; c) \mid \mu \in I^n]^{p^n}[B]$.

LEMMA. *Let $k \subseteq L \subseteq K$, assume that L is a separable extension of k, and that B is a p-basis of k and of K. Let C be a p-basis of L over k, and let $k\langle C\rangle = k(\lambda_\mu(B; c) \mid c \in C, \mu \in I^{<\omega})$, the λ-functions being those of K.*

1. *If $c \in L^{p^n}(B)$, then $\lambda_\mu(B; c) \in L$ for every $\mu \in I^n$.*
2. *$Lk\langle C\rangle$ is closed under the λ-functions of K. If $a \in L$ and $\nu \in I^n$, then $\lambda_\nu(B; a) \in L[\lambda_\mu(B; c) \mid c \in C, \mu \in I^n]$.*
3. *If D is another p-basis of K and $a \in L$, $\nu \in I^n$, then $\lambda_\nu(B; a) \in \mathbb{F}_p[\lambda_\mu(D; a), \lambda_\mu(B; d) \mid d \in D, \mu \in I^n]$. If $D \subset k$, then $\lambda_\nu(B; a) \in k[\lambda_\mu(D; a) \mid \mu \in I^n]$.*

Proof. (1) As $B \subset L$, we have $L^{p^n}(B) = L^{p^n}[B]$, and $c \in L^{p^n}[B_0]$ for some finite subset B_0 of B, so that we may assume that B is finite. Then $c = \sum_{j\in I} c_j^p m_j(B)$ for some $c_j \in L^{p^{n-1}}$. Thus $c_j = \lambda_j(B;c) \in L^{p^{n-1}}$. Since $\lambda_\mu = \lambda_\nu \circ \lambda_j$ for some $\nu \in I^{n-1}$ and $j \in I$, an induction on n gives us that $\lambda_\nu(B;c_j) = \lambda_\mu(B;c) \in L$.

(2) By assumption, $B \cup C$ is a p-basis of L; hence $L = L^{p^n}[B,C]$ for every $n \geq 0$. By the definition of the λ-functions, we also have that $c \in (\mathbb{F}_p[\lambda_\mu(B;c) \mid \mu \in I^n])^{p^n}[B]$ for any $c \in K$. Hence $L \subseteq (L[\lambda_\mu(B;c) \mid c \in C, \mu \in I^n])^{p^n}[B]$, and (1) gives that $\lambda_\nu(B;a) \in L[\lambda_\mu(B;c) \mid c \in C, \mu \in I^n]$. Hence $Lk\langle C\rangle$ is closed under the λ-functions of K.

(3) By assumption, $K = K^{p^n}[D] = K^{p^n}[B]$. If $a \in L$, then $a \in (\mathbb{F}_p[\lambda_\mu(D;a) \mid \mu \in I^n])^{p^n}[D]$, and if $d \in D$ then $d \in (\mathbb{F}_p[\lambda_\mu(B;d) \mid \mu \in I^n])^{p^n}[B]$. Thus $a \in \mathbb{F}_p[\lambda_\mu(D;a), \lambda_\mu(B;d) \mid \mu \in I^n, d \in D]^{p^n}[B]$, and (1) gives the first assertion. The second assertion follows from the fact that $D \subset k$ and that k is closed under the λ-functions of K.

(1.11) λ-polynomial rings over k when k has finite degree of imperfection. Let B be a p-basis of k of finite size e. Then the set I defined above has size p^e. We define $k\langle X\rangle_{\leq n,B}$ to be the quotient of the polynomial ring $k[X_\mu \mid \mu \in I^{\leq n}]$ by the ideal generated by the polynomials

$$X_\mu - \sum_{i\in I} X^p_{\mu^\frown i} m_i(B)$$

for $\mu \in I^{\leq n-1}$, and we let $k\langle X\rangle_B = \bigcup_n k\langle X\rangle_{\leq n,B}$. If we consider only one p-basis B, then we will omit B from the notation. We define $k\langle X_1,\ldots,X_n\rangle_{\leq n,B}$ and $k\langle X_1,\ldots,X_n\rangle_B$ analogously.

Then B is a p-basis of (the field of fractions of) $k\langle X_1,\ldots,X_n\rangle_B$. If B is a p-basis of an extension K of k and $a_1,\ldots,a_n \in K$, then there is a unique k-morphism $k\langle X_1,\ldots,X_n\rangle_B \to K$ which sends X_i to a_i. Note also that $k\langle X_1,\ldots,X_n\rangle_B$ is generated as a ring by the elements $\lambda_\mu(B;X_i), i = 1,\ldots,n, \mu \in I(B)^{<\omega}$.

If C is another p-basis of k, then there is a natural $k[X_1,\ldots,X_n]$-isomorphism : $k\langle X_1,\ldots,X_n\rangle_B \to k\langle X_1,\ldots,X_n\rangle_C$. This follows from the previous observation, and the fact that by Lemma 1.10(3), we have $k\langle X_1,\ldots,X_n\rangle_{\leq m,C} \subseteq k\langle X_1,\ldots,X_n\rangle_{\leq m,B}$ and $k\langle X_1,\ldots,X_n\rangle_{\leq m,B} \subseteq k\langle X_1,\ldots,X_n\rangle_{\leq m,C}$ for every $m \in \mathbb{N}$.

(1.12) Lemma. *Let K be a separable extension of k, with p-basis B over k, and let $C \subset k$ be p-independent. Consider the fields $k_1 = k(c^{1/p} \mid c \in C)$ and $k_2 = k(c^{1/p^n} \mid c \in C, n \in \mathbb{N})$. Then B is a p-basis of k_1K over k_1 and of k_2K over k_2.*

Proof. Clearly $k_1K = k_1K^p[B]$ and $k_2K = k_2K^p[B]$, so we only need to show that B is p-independent over k_1 in k_1K and over k_2 in k_2K. Since K

is a separable extension of k, the fields $k^{p^{-\infty}}$ and K are linearly disjoint over k. Hence K is linearly disjoint from k_1 and from k_2 over k. This implies that k_1K^p and K are linearly disjoint over kK^p. Hence linearly independent elements of the kK^p-vector space K stay linearly independent in the k_1K^p-vector space k_1K. This shows that B stays p-independent over k_1 in k_1K. The proof for k_2K is similar.

2. The main result

Let $e \in \mathbb{N} \cup \{\infty\}$, and $\mathcal{L}_{\lambda,\sigma} = \mathcal{L}_\lambda \cup \{\sigma\}$. In this section we prove that the $\mathcal{L}_{\lambda,\sigma}$-theory of difference fields models of T_λ and of degree of imperfection $\leq e$ has a model companion, and that the $\mathcal{L}_\sigma(b_1, \ldots, b_e)$-theory of difference fields with p-basis $\{b_1, \ldots, b_e\}$ has a model companion. Before embarking into preparatory lemmas, let me explain the strategy of the proof.

Clearly existentially closed difference fields (in $\mathcal{L}_{\lambda,\sigma}$ or in $\mathcal{L}_\sigma(b_1, \ldots, b_e)$) need to be separably closed, since any automorphism of a field extends to an automorphism of its separable closure. By a linearisation argument already used for the axiomatisation of the theory ACFA of existentially closed difference fields, one reduces the problem of solving systems of σ-equations to the problem of finding a point $\bar{a}$ in some variety U defined over K, such that $(\bar{a}, \sigma(\bar{a})) \in V$ for some variety V contained in $U \times \sigma(U)$ and projecting generically onto U and $\sigma(U)$. While in the theory of difference fields we know that such a problem always has a solution in some extension (cf. the axiomatisation of ACFA; see [CH] or [M], or (1.2)), here we need to find conditions on V, that are elementary in the parameters of K used to define V, and which ensure that there is a solution $\bar{a}$ in some $\mathcal{L}_{\lambda,\sigma}$-extension L of K. In particular, such an $\bar{a}$ must generate a difference field which is separable over K.

It turns out that the main difficulty is to find elementary conditions which ensure that $K(\bar{a})_\sigma$ is a separable extension of K: if we manage to do that, then Lemma (2.2) allows us to complete the proof. We then reduce the problem to the case where $\dim(U) = \dim(V)$; see Lemma (2.1). To show that $K(\bar{a})_\sigma$ is a separable extension of K, it is enough to show that $K(\bar{a}, \sigma(\bar{a}), \ldots, \sigma^m(\bar{a}))$ is a separable extension of K for every $m \in \mathbb{N}$. We solve this problem in (2.4) and (2.5).

Let me mention a case where the solution of the problem is easy. Let $K(V) = K(\bar{x}, \bar{y})$, and assume that $\bar{y}$ is separably algebraic over $K(\bar{x})$. This condition is certainly elementary in the parameters defining V. Let $(\bar{a}, \bar{a}_1)$ be a generic over K of the algebraic set V, and let σ be an extension of σ to Ω which sends $\bar{a}$ to $\bar{a}_1$. Then $\sigma(\bar{a}) \in K(\bar{a})^s$, and therefore $K(\bar{a}, \ldots, \sigma^m(\bar{a})) \subseteq K(\bar{a})^s$ for every $m \geq 0$, which implies that $K(\bar{a})_\sigma$ is a separable extension of K. A similar argument applies if $\bar{x}$ is separably algebraic over $K(\bar{y})$ in $K(V)$. However there are examples of equations solvable in a separable extension of K which are not of this form; e.g., the equation $\sigma^2(x)^p + b\sigma(x) + x^p = 0$ has

a solution in a separable extension of K. (Note also that if a is a solution of this equation which is generic over K, then the degree of transcendence of $K(a)_\sigma$ over K is 2, and $K(a)_\sigma$ has same p-basis as K.)

(2.1) LEMMA. *Let k be a difference field, and $k(\bar{a})_\sigma$ a separable extension of k. Then there is a transformal transcendence basis $\bar{b} \subseteq \bar{a}$ of $k(\bar{a})_\sigma$ over k, such that $k(\bar{a})_\sigma$ is a separable extension of $k(\bar{b})_\sigma$.*

Proof. The proof is by induction on the transformal transcendence degree $\Delta(\bar{a}/k)$ of $\bar{a}$ over k. If it equals 0, there is nothing to prove, so we will assume that it is positive. It suffices to find an element $b \in \bar{a}$ such that b is transformally transcendental over k and $k(\bar{a})_\sigma$ is a separable extension of $k(b)_\sigma$. We will then use induction applied to the extension $k(\bar{a})_\sigma$ of $k(b)_\sigma$ to obtain the result.

For $n \in \mathbb{N}$ consider the field $K_n = k(\bar{a}, \sigma(\bar{a}), \ldots, \sigma^n(\bar{a}))$. Replacing $\bar{a}$ by $\bar{a}^\frown \cdots ^\frown \sigma^m(\bar{a})$ for some m, we may assume that $\mathrm{tr.deg}(K_n/k) = d+ne$ where $d = \mathrm{tr.deg}(\bar{a}/k)$ and $e = \Delta(\bar{a}/k)$. Each K_n is a finitely generated separable extension of k, and therefore has a separating transcendence basis over k of size $d + ne$. In other words, we have

$$[K_n : k(K_n^p)] = p^{d+ne}. \tag{1}$$

CLAIM. *There is $b \in \bar{a}$ such that for any $n \geq 0$ the elements $b, \sigma(b), \ldots, \sigma^n(b)$ are p-independent over k in K_n.*

Otherwise, for each $b \in \bar{a}$, there is an $n = n(b)$ such that the elements $b, \sigma(b), \ldots, \sigma^n(b)$ are not p-independent over k in K_n. Take n minimal with this property; then for some $i \leq n$ we have $\sigma^i(b) \in k(K_n^p)(b, \sigma(b), \ldots, \sigma^{i-1}(b))$. As $\sigma(K_n) \subseteq K_{n+1}$, we get that $\sigma^{i+1}(b) \in k(K_{n+1}^p)(b, \ldots, \sigma^{i-1}(b))$, $\ldots$, $\sigma^{i+m}(b) \in k(K_{n+m}^p)(b, \ldots, \sigma^{i-1}(b))$ for $m \geq 0$, so that any subset of $\{b, \ldots, \sigma^{m+n}(b)\}$ which is p-independent in K_{m+n} has size $\leq n$.

Let $N = \sup\{n(b) \mid b \in \bar{a}\}$, and let $m \geq N$. By the above argument, any subset of $\{\bar{a}, \ldots, \sigma^m(\bar{a})\}$ which is p-independent in K_m has size at most $|\bar{a}|N$. Then $[K_m : k(K_m^p)] \leq p^{|\bar{a}|N}$, which contradicts the unboundedness of $[K_m : k(K_m^p)]$ given by equation (1) and proves the claim.

Take an element b satisfying the conclusion of the claim. Then the elements $\sigma^i(b), i \in \mathbb{N}$, are p-independent over k in the field $k(\sigma^i(\bar{a}) \mid i \in \mathbb{N})$. Using the fact that σ^{-1} is an automorphism, we deduce that the elements $\sigma^i(b), i \in \mathbb{Z}$, are p-independent over k in $k(\sigma^i(\bar{a}) \mid i \in \mathbb{Z}) = k(\bar{a})_\sigma$. Hence $k(\bar{a})_\sigma$ is a separable extension of $k(b)_\sigma$.

(2.2) LEMMA. *Let k be a difference field with finite p-basis B, and let $k(\bar{a})_\sigma$ be a finitely generated difference field extending k which is separable over k. Then $k(\bar{a})_\sigma$ embeds into a difference field M with p-basis B.*

Proof. By (2.1), it suffices to show the result in the following two cases:

(a) $\bar{a}$ is transformally independent over k.
(b) $\bar{a}$ is transformally algebraic over k.

The separable closure of k has also p-basis B, so we may assume that k is separably closed.

(a) Note that $k(\bar{a})_\sigma$ is a purely transcendental extension of k, with transcendence basis $\{\sigma^i(d) \mid d \in \bar{a}, i \in \mathbb{Z}\}$ over k. As σ induces a permutation of this transcendence basis, the automorphism σ of $k(\bar{a})_\sigma$ extends uniquely to an automorphism of $M = k(\sigma^i(d)^{1/p^n} \mid d \in \bar{a}, i \in \mathbb{Z}, n \in \mathbb{N})$. Then M is a separable extension of k, with p-basis B.

(b) Let C be a p-basis of $k(\bar{a})_\sigma$ over k. Then $k(\bar{a})_\sigma = k(\bar{a}^p)_\sigma(C)$. If $C = \emptyset$, then we are done: B is a p-basis of $k(\bar{a})_\sigma$. Assume therefore that $C \neq \emptyset$. Consider the quotient of the polynomial ring $k(C)\langle X_c \mid c \in C\rangle_B$ by the ideal generated by the polynomials $X_c - c$ for $c \in C$, and let M_0 be its field of fractions. Then M_0 is a separable extension of k, with p-basis B, and we may choose M_0 free from $k(\bar{a})_\sigma$ over $k(C)$, because the elements of C are p-independent over k in $k(\bar{a})_\sigma$. Hence $M = M_0 k(\bar{a})_\sigma$ is a separable extension of k, with p-basis B (by (1.10)(1) and because $k(\bar{a})_\sigma = k(\bar{a}^p)_\sigma(C)$). We consider the λ-functions of M indexed by $I = I(B)$, and define $\sigma(\lambda_\mu(B; c)) = \lambda_\mu(\sigma(B); \sigma(c))$ for $\mu \in I^{<\omega}$. We need to show that σ defines an automorphism of M. For $n \in \mathbb{N}$ let $M_n = k(\bar{a})_\sigma(\lambda_\mu(B; c) \mid c \in C, \mu \in I^n)$, let 0_n be the element of I^n corresponding to the p^n-monomial 1, and let $J_n = I^n \setminus \{0_n\}$. Then the elements $\lambda_\mu(B; c), c \in C, \mu \in J_n$, are algebraically independent over $k(\bar{a})_\sigma$ and generate M_n over $k(\bar{a})_\sigma$. As $\sigma(B)$ is also a p-basis of M, we know that for $c \in C$ we have $\sigma(c) = \sum_{\mu \in I^n} \lambda_\mu(\sigma(B); \sigma(c))^{p^n} m_\mu(\sigma(B))$, and by the definition of σ this coincides with $\sum_{\mu \in I^n} \sigma(\lambda_\mu(B; c)^{p^n}) \sigma(m_\mu(B))$. Hence σ extends uniquely to a ring homomorphism $M_n \to M_n$. We have:

$$\begin{aligned} k(\bar{a})_\sigma(\lambda_\mu(B; c) \mid c \in C, \mu \in I^n) &= k(\bar{a})_\sigma(\lambda_\mu(B, \sigma(c)) \mid c \in C, \mu \in I^n) \\ &\qquad \text{(by (1.10)(2))} \\ &= k(\bar{a})_\sigma(\lambda_\mu(\sigma(B), \sigma(c)) \mid c \in C, \mu \in I^n) \\ &\qquad \text{(by (1.10)(3)).} \end{aligned}$$

This shows that σ is onto, and therefore is also injective as the elements $\lambda_\mu(\sigma(B), \sigma(c)), c \in C, \mu \in J_n$, must be algebraically independent over $k(\bar{a})_\sigma$. Hence σ defines an automorphism of M_n for every n, and therefore defines an automorphism of M.

(2.3) An example. The following example shows that Lemma (2.2) does not generalise to the case where B is infinite.

Let b be an element transformally transcendental over $\mathbb{F}_p$, $k = \mathbb{F}_p(b)^s_\sigma$, and let a be a solution of $\sigma(x) = x + b$. If L is a difference field containing $k(a)_\sigma$ which is separable over k, then $\{\sigma^i(b) \mid i \in \mathbb{Z}\} \cup \{a\}$ is p-independent in L.

Let $B = \{\sigma^i(b) \mid i \in \mathbb{Z}\}$, let L be a difference field containing $k(a)_\sigma$, separable over k, and assume that $a \in L^p[B]$. Let $m < n \in \mathbb{Z}$ be such that $a \in L^p[\sigma^m(b), \ldots, \sigma^n(b)]$ and $n-m$ is minimal. Let $B_0 = \{\sigma^m(b), \ldots, \sigma^n(b)\}$, and write $a = \sum_i \lambda_i(B_0; a)^p m_i(B_0)$. By the minimality of $n-m$, we get that $\sigma^m(b) \in L^p[a, \sigma^{m+1}(b), \ldots, \sigma^n(b)]$ and $\sigma^n(b) \in L^p[\sigma^m(b), \ldots, \sigma^{n-1}(b), a]$. This implies that there are indices i and j such that $\lambda_i(B_0; a) \neq 0$, $\lambda_j(B; a) \neq 0$, and the exponents of $\sigma^m(b)$ in $m_i(B_0)$ and of $\sigma^n(b)$ in $m_j(B_0)$ are positive. Then $\sigma(a) - a = \sum_k \lambda_k(\sigma(B_0; \sigma(a))^p m_k(B_0) - \lambda_k(B_0; a)^p m_k(B_0)$, and the coefficients of the monomials $m_i(B_0)$ and $\sigma(m_j(B_0))$ in this expression are non-zero, because $\sigma^m(b) \notin \sigma(B_0)$, $\sigma^{n+1}(b) \notin B_0$. But this contradicts the p-independence of B and the fact that $\sigma(a) - a = b$.

(2.4) LEMMA. *Let $k(\bar{a})_\sigma$ be a separable extension of k, with $\sigma(\bar{a}) \in k(\bar{a})^{\mathrm{alg}}$, and let $d = \mathrm{tr.deg}(k(\bar{a})/k)$. Then there is a separating transcendence basis $\bar{c} \cup \bar{d}$ of $k(\bar{a}, \sigma(\bar{a}), \ldots, \sigma^d(\bar{a}))$ over k, such that $\bar{c} \cup \sigma^{-1}(\bar{d}) \subseteq \bar{a} \cup \sigma(\bar{a}) \cup \cdots \cup \sigma^{d-1}(\bar{a})$ and $\sigma^{-1}(\bar{d})$ is separably algebraic over $k(\bar{c}^p, \bar{d})$.*

Proof. Let $0 \leq i \leq d+1$, and consider the field

$$K_{d,i} = k(\bar{a}^p, \ldots, \sigma^{i-1}(\bar{a}^p), \sigma^i(\bar{a}), \ldots, \sigma^d(\bar{a})).$$

Then $K_{d,0} = k(\bar{a}, \ldots, \sigma^d(\bar{a}))$, $K_{d,d+1} = k(\bar{a}^p, \ldots, \sigma^d(\bar{a}^p)) = k(K^p_{d,0})$, and $K_{d,i}$ is a purely inseparable extension of $K_{d,i+1}$ for every $i \leq d$. As $K_{d,0}$ is a separable, finitely generated extension of k, of transcendence degree d over k, we have $[K_{d,0} : K_{d,d+1}] = p^d$. Hence there is $0 \leq i \leq d$ such that $K_{d,i} = K_{d,i+1}$, and we fix such an i. Choose $\bar{d} \subseteq \sigma^{i+1}(\bar{a}) \cup \cdots \cup \sigma^d(\bar{a})$ maximal p-independent over k in $K_{d,0}$. Then $K_{d,i} = K_{d,i+1} = k(K^p_{d,0})[\bar{d}]$, and $K_{d,0} = K_{d,i+1}(\bar{a}, \ldots, \sigma^{i-1}(\bar{a}))$. Choose $\bar{c} \subseteq \bar{a} \cup \cdots \cup \sigma^{i-1}(\bar{a})$ such that $\bar{c} \cup \bar{d}$ is a p-basis of $K_{d,0}$ over k. Then $\bar{c}, \bar{d}$ satisfy the conclusion: since $\sigma^{-1}(\bar{d}) \in K_{d,i}$, we have that $\sigma^{-1}(\bar{d}) \in k(K^p_{d,0})[\bar{d}] \subseteq k(\bar{c}^p, \bar{d}^p)^s[\bar{d}] \subseteq k(\bar{c}^p, \bar{d})^s$.

(2.5) LEMMA. *Let U and V be varieties of dimension d defined over the difference field k, and assume that $V \subseteq U \times \sigma(U)$, and that V projects generically onto U and onto $\sigma(U)$. Write $k(V) = k(x_1, \ldots, x_n, y_1, \ldots, y_n)$ and assume that there is $1 \leq r \leq d$ such that $(x_1, \ldots, x_r, y_{r+1}, \ldots, y_d)$ is a separating transcendence basis of $k(V)$ over k, and that $x_{r+1}, \ldots, x_d$ are separably algebraic over $k(x_1^p, \ldots, x_r^p, y_{r+1}, \ldots, y_d)$. Then there is a tuple $\bar{a}$ such that $k(\bar{a})_\sigma$ is a separable extension of k, and $(\bar{a}, \sigma(\bar{a}))$ is a generic of V over k.*

Proof. Choose in some difference field (K, σ) containing k (e.g., in a model of ACFA) a tuple $\bar{a} = (a_1, \ldots, a_n)$ such that $(\bar{a}, \sigma(\bar{a}))$ is a generic of the algebraic set V. Our assumption on the dimensions of U and V implies that

$\sigma(\bar{a})$ is algebraic over $k(\bar{a})$, so that $k(\bar{a})_\sigma \subseteq k(\bar{a})^{\mathrm{alg}}$. Let $\bar{c} = (a_1, \ldots, a_r)$, and $\bar{d} = (\sigma(a_{r+1}), \ldots, \sigma(a_d))$. Then $\bar{c} \cup \bar{d}$ is a separating transcendence basis of $k(\bar{a}, \sigma(\bar{a}))$ over k, and $\sigma^{-1}(\bar{d})$ is separably algebraic over $k(\bar{c}^p, \bar{d})$. We will show by induction on $m \geq 1$ that

(i) $\sigma^{-1}(\bar{d}), \ldots, \sigma^{m-2}(\bar{d})$ are separably algebraic over $k(\bar{c}^p, \sigma^{m-1}(\bar{d}))$;
(ii) $\bar{c} \cup \sigma^{m-1}(\bar{d})$ is a separating transcendence basis of $k(\bar{a}, \ldots, \sigma^m(\bar{a}))$ over k.

For $m = 1$, this is our assumption. Assume the result proved for m. Then $\sigma(\bar{c}) \in k(\bar{c}, \bar{d})^s$ and by applying σ to (i) we get that $\bar{d}, \ldots, \sigma^{m-1}(\bar{d}) \in k(\sigma(\bar{c})^p, \sigma^m(\bar{d}))^s$. By Lemma (1.6)(2) applied to $k(\bar{c}, \sigma^m(\bar{d}))$, $\bar{d}$ and $\sigma(\bar{c})$, we obtain that $\sigma(\bar{c}), \bar{d} \in k(\bar{c}, \sigma^m(\bar{d}))^s$, and therefore that $\bar{d}, \ldots, \sigma^{m-1}(\bar{d}) \in k(\bar{c}^p, \sigma^m(\bar{d}))^s$ (as $\sigma(\bar{c})^p \in k(\bar{c}^p, \sigma^m(\bar{d}^p))^s$). From $\sigma^{-1}(\bar{d}) \in k(\bar{c}^p, \bar{d})^s$ we deduce (i).

We know that $\bar{a} \in k(\bar{c}, \bar{d})^s \subseteq k(\bar{c}, \sigma^m(\bar{d}))^s$, and by the induction hypothesis we have $\sigma(\bar{a}), \ldots, \sigma^{m+1}(\bar{a}) \in k(\sigma(\bar{c}), \sigma^m(\bar{d}))^s$. As $\sigma(\bar{c}) \in k(\bar{c}, \bar{d})^s$, we get (ii).

Hence $k(\bar{a}, \ldots, \sigma^m(\bar{a}))$ is a separable extension of k for every $m \geq 1$. This implies that $k(\bar{a})_\sigma$ is separable over k.

(2.6) THEOREM. *Let $e \in \mathbb{N}$. The theory of difference fields of degree of imperfection $\leq e$ which are models of T_λ, has a model companion $SCFA_{e,\lambda}$. The theory $SCFA_{e,\lambda}$ is axiomatised by formulas expressing the following properties of the $\mathcal{L}_{\lambda,\sigma}$-structure (K, σ):*

(i) *$SCF_{e,\lambda}$.*
(ii) *σ is an automorphism of K.*
(iii) *If U and V are varieties defined over K and satisfy the hypotheses of (2.5), then there is a tuple $\bar{a}$ such that $(\bar{a}, \sigma(\bar{a})) \in V$.*

Proof. We will first show that (iii) is expressible by an infinite collection of first-order statements. Let U and V be varieties defined over K. Then there is a finite tuple $\bar{c}$ of elements of K, and finite tuples $F(\bar{X}, \bar{T})$ and $G(\bar{X}, \bar{Y}, \bar{T})$ of polynomials over $\mathbb{F}_p$, such that the ideal of $K[\bar{X}]$ of polynomials vanishing on U is generated by the tuple $F(\bar{X}, \bar{c})$, and the ideal of $K[\bar{X}, \bar{Y}]$ of polynomials vanishing on V is generated by $G(\bar{X}, \bar{Y}, \bar{c})$. Write $K[V] = K[\bar{x}, \bar{y}]$, $\bar{x} = (x_1, \ldots, x_n)$, $\bar{y} = (y_1, \ldots, y_n)$, and let $r \leq d$ be such that $K(x_1, \ldots, x_r, y_{r+1}, \ldots, y_d)$ is a separating transcendence basis of $K(V)$ over K, and $x_{r+1}, \ldots, x_d$ are separably algebraic over $K(x_1^p, \ldots, x_r^p, y_{r+1}, \ldots, y_d)$. Since the algebraic varieties U and V are defined over $\mathbb{F}_p(\bar{c})$, this implies that $\mathbb{F}_p(\bar{c})(V)$ is separably algebraic over $\mathbb{F}_p(\bar{c})(x_1, \ldots, x_r, y_{r+1}, \ldots, y_d)$, and $x_{r+1}, \ldots, x_d$ are separably algebraic over $\mathbb{F}_p(\bar{c})(x_1^p, \ldots, x_r^p, y_{r+1}, \ldots, y_d)$.

If $\bar{d}$ is a finite tuple of K of the same length as $\bar{c}$, define $U(\bar{d})$ to be the algebraic set defined by the equations $F(\bar{X}, \bar{d}) = 0$, and $V(\bar{d})$ to be the algebraic set defined by $G(\bar{X}, \bar{Y}, \bar{d}) = 0$. We claim that there is a quantifier-free formula φ of the language $\mathcal{L}$ of rings satisfied by $(\bar{c}, \sigma(\bar{c}))$, and such that if

$(\bar{d}, \sigma(\bar{d}))$ satisfies φ, then the algebraic sets $U(\bar{d})$ and $V(\bar{d})$ have the following properties:

- $U(\bar{d})$ and $V(\bar{d})$ are (absolutely irreducible) varieties of dimension d.
- $V(\bar{d}) \subseteq U(\bar{d}) \times U(\sigma(\bar{d}))$, and the projections $V(\bar{d}) \to U(\bar{d})$ and $V(\bar{d}) \to U(\sigma(\bar{d}))$ are generically onto.
- $\mathbb{F}_p(\bar{d})(V(\bar{d}))$ is separably algebraic over $\mathbb{F}_p(\bar{d})(x_1, \ldots, x_r, y_{r+1}, \ldots, y_d)$, and the elements $x_{r+1}, \ldots, x_d$ of $\mathbb{F}_p(\bar{d})(V(\bar{d}))$ are separably algebraic over $\mathbb{F}_p(\bar{d})(x_1^p, \ldots, x_r^p, y_{r+1}, \ldots, y_d)$.

Since the theory of algebraically closed fields is strongly minimal and eliminates the quantifier $\exists^\infty$, the property of the Zariski closure of a definable set of being of a given dimension is elementary in the parameters defining this set. Then standard results on polynomial rings over fields (see, e.g., [DS]) and elimination of quantifiers of the theory of algebraically closed fields give that the first two items are elementary properties of $\bar{d}$.

The conditions of separability given in the third item are easily expressible using the polynomials $G(\bar{x}, \bar{y}, \bar{d})$, since they correspond to some subdeterminants of the Jacobian of $G(\bar{x}, \bar{y}, \bar{d})$ being non-zero; see [L1], Proposition X.7.3. Note that as $d = \dim(V(\bar{d}))$, the elements $x_1, \ldots, x_r, y_{r+1}, \ldots, y_d$ of $\mathbb{F}_p(\bar{d})(V(\bar{d}))$ are necessarily algebraically independent over $\mathbb{F}_p(\bar{d})$.

Using compactness, we deduce that there is a scheme of axioms expressing the properties (i), (ii) and (iii). It now remains to prove that $\mathrm{SCFA}_{e,\lambda}$ is indeed the model-companion of the theory of difference fields of degree of imperfection $\leq e$ which are models of T_λ. We will first show that every difference field (K, σ) of degree of imperfection $\leq e$ which is a model of T_λ embeds in a model of $\mathrm{SCFA}_{e,\lambda}$.

First note that if K is a model of T_λ, then any field automorphism σ of K is an $\mathcal{L}_\lambda$-automorphism, since the λ-functions of K are first-order definable in K. Also, any difference field of degree of imperfection $f < e$ embeds in one of degree of imperfection e: Let $\bar{t}$ be an $(e-f)$-tuple of elements algebraically independent over K, and extend σ to $K(\bar{t})$ so that it fixes the elements of $\bar{t}$. Then the degree of imperfection of $K(\bar{t})$ is e. Also, any automorphism of a field K extends to an automorphism of the separable closure K^s of K, and we may therefore assume that K satisfies (i) and (ii).

Let U and V be varieties defined over K and satisfying the hypotheses of (iii). By (2.5), there is a separable extension $K(\bar{a})_\sigma$ of K such that $(\bar{a}, \sigma(\bar{a}))$ is a generic of V. By Lemma (2.2) there is a difference field M containing $K(\bar{a})_\sigma$, separable over K and with the same p-basis as K. Thus we have shown that every occurrence of axiom (iii) can be satisfied in some separable extension M of K with the same p-basis as K. A standard limit argument then shows that K embeds in a model of $\mathrm{SCFA}_{e,\lambda}$. It remains to show that $\mathrm{SCFA}_{e,\lambda}$ is model-complete, i.e., that if $K \subseteq L$ are models of $\mathrm{SCFA}_{e,\lambda}$ then K is existentially closed in L.

Let $(K,\sigma) \subseteq (L,\sigma)$ be models of $\mathrm{SCFA}_{e,\lambda}$. As e is finite, if B is a p-basis of K, then B is also a p-basis of L, and therefore L is an elementary $\mathcal{L}$-extension of K. Any quantifier-free formula of $\mathcal{L}_\lambda$ is equivalent, modulo the $\mathcal{L}_\lambda(B)$-theory of (K,B), to an existential $\mathcal{L}(B)$-formula. Hence it is enough to show that any quantifier-free $\mathcal{L}_\sigma$-formula $\varphi(\bar{x})$ with parameters in K which is satisfied in L is already satisfied in K. Using the usual trick of replacing the formula $(x \neq 0)$ by $(\exists y\ xy = 1)$, we may furthermore assume that $\varphi(\bar{x})$ is positive, i.e., that $\varphi(\bar{x})$ is a finite conjunction of difference equations with coefficients in K. Let $\bar{a}$ be a tuple of L satisfying $\varphi(\bar{x})$. Because φ is a finite conjunction of difference equations, any tuple $\bar{d}$ with $I_\sigma(\bar{d}/K) \supseteq I_\sigma(\bar{a}/K)$ will satisfy φ. We will show that such a tuple exists in an elementary extension K^* of K, and therefore also in K.

By Lemma (2.1), there is a subtuple $\bar{b}$ of $\bar{a}$ such that $\bar{b}$ is transformally independent over K and $K(\bar{a})_\sigma$ is a separable transformally algebraic extension of $k = K(\bar{b})_\sigma$. Choose m large enough such that $k(\bar{a})_\sigma \subseteq k(\bar{a},\ldots,\sigma^m(\bar{a}))^{\mathrm{alg}}$, and such that if $\bar{a}'$ is a tuple (in some model of ACFA containing K) such that there is a k-isomorphism sending $(\bar{a}',\ldots,\sigma^m(\bar{a}'))$ to $(\bar{a},\ldots,\sigma^m(\bar{a}))$, then this k-isomorphism extends to a k-isomorphism of difference fields $k(\bar{a}')_\sigma \to k(\bar{a})_\sigma$ (see [C, 8.20.13] for the existence of such an m). By (2.4) applied to $k = K(\bar{b})_\sigma$, there is an integer $n > m$ and a separating transcendence basis $\bar{c} \cup \bar{d}$ of $k(\bar{a},\ldots,\sigma^n(\bar{a}))$ over k with $\bar{c} \cup \sigma^{-1}(\bar{d}) \subseteq \bar{a} \cup \cdots \cup \sigma^{n-1}(\bar{a})$, and such that $\sigma^{-1}(\bar{d})$ is separably algebraic over $k(\bar{c}^p,\bar{d})$.

Let U be the algebraic locus of $(\bar{a},\ldots,\sigma^{n-1}(\bar{a}))$ over k^s (i.e., the smallest algebraic set defined over k^s and containing $(\bar{a},\ldots,\sigma^{n-1}(\bar{a}))$, and V the algebraic locus of $(\bar{a},\ldots,\sigma^{n-1}(\bar{a}),\sigma(\bar{a}),\ldots,\sigma^n(\bar{a}))$ over k^s. As $K(\bar{a})_\sigma$ is a separable extension of $k = K(\bar{b})_\sigma$, the algebraic sets U and V are varieties defined over k^s, of the same dimension (because $k(\bar{a})_\sigma \subseteq k(\bar{a},\ldots,\sigma^{n-1}(\bar{a}))^{\mathrm{alg}}$), and they satisfy the hypotheses of (2.5) over k^s after some renaming of the variables.

Let K^* be a sufficiently saturated elementary extension of K. It then suffices to show that $\varphi(\bar{x})$ is satisfied in K^*. We first claim that K^* contains arbitrarily large finite tuples of elements which are transformally transcendental over K. First observe that any instance of (iii) with the varieties U and V defined over K has a realisation $\bar{e}$ in K^* with $(\bar{e},\sigma(\bar{e}))$ a generic of the algebraic variety V over K. This follows from the saturation of K^* and the fact that, by (iii), any formula $(\bar{x},\sigma(\bar{x})) \in V \wedge zg(\bar{x},\sigma(\bar{x})) = 1$, where $g \in K[V] \setminus \{0\}$, has a solution in K. Thus, for any n,m, there is an m-tuple $\bar{e}$ of elements of K^* satisfying $\sigma^n(x) = x$ and $\mathrm{tr.deg}(k(\bar{e})_\sigma/k) = nm$. By saturation, there is $\bar{e} \in (K^*)^m$ such that the elements $\sigma^i(g), g \in \bar{e}, i \in \mathbb{N}$, are algebraically independent over K.

Choose a tuple $\bar{c}$ of K^*, of the same length as $\bar{b}$, and which is transformally independent over K. Then the difference fields $k = K(\bar{b})_\sigma$ and $K(\bar{c})_\sigma$ are K-isomorphic, by an isomorphism f sending $\bar{b}$ to $\bar{c}$. By Proposition 2.10 of [CH],

if τ is an automorphism of $K(\bar{c})^s_\sigma$ which agrees with σ on $K(\bar{c})_\sigma$, then τ is conjugate to σ by an element of $\mathrm{Gal}(K(\bar{c})^s_\sigma/K(\bar{c})_\sigma)$. Hence the isomorphism f extends to a difference field embedding $f : k^s \to K^*$. By axiom (iii) and saturation of K^*, there is a tuple $\bar{e}$ in K^*, such that $(\bar{e}, \sigma(\bar{e}))$ is a generic of $f(V)$ over $K(\bar{c})^s_\sigma$. Then $\bar{e} = (\bar{d}, \ldots, \sigma^{n-1}(\bar{d}))$ for some tuple $\bar{d}$ of the same length as $\bar{a}$, and $I_\sigma(\bar{a}/K) = I_\sigma(\bar{d}/K)$ because $n > m$, so that $\bar{d}$ satisfies φ.

(2.7). We added only the λ-functions symbols to the language to ensure that if (L, σ) is an extension of (K, σ) then L is separable over K. In case the degree of imperfection e is finite, this could have been achieved as well by adding constant symbols for the elements of a p-basis, together with the axioms expressing that these elements form a p-basis.

THEOREM. *Consider the language $\mathcal{L}_\sigma(b_1, \ldots, b_e)$, and the class of difference fields (K, σ) with p-basis $\{b_1, \ldots, b_e\}$. The existentially closed members of this class form an elementary class, axiomatised by* (ii) *and* (iii) *above, together with* (i')*: $SCF_{e,b}$.*

Proof. This follows easily from (2.6) and the following observations: a field expands uniquely to a model of T_λ; if $K \subseteq L$ are two difference fields with the same p-basis, then K is an $\mathcal{L}_{\lambda,\sigma}$-substructure of L.

(2.8). Let us denote this theory by $\mathrm{SCFA}_{e,b}$. Note that this gives a slightly less general result than (2.6), as the p-basis is fixed by σ. However, the advantage is that the theory $\mathrm{SCF}_{e,b}$ of separably closed fields with p-basis $\{b_1, \ldots, b_e\}$ eliminates imaginaries. It is also model-complete but doesn't eliminate quantifiers as the λ-functions are only existentially definable. We will see that it implies that any completion of $\mathrm{SCFA}_{e,b}$ eliminates imaginaries (in the language $\mathcal{L}_\sigma(\bar{b})$).

(2.9). The case $e = \infty$ necessitates a few more lemmas. The problem comes from the fact that quantifier-free $\mathcal{L}_\lambda$-formulas are *not* equivalent modulo $\mathrm{SCF}_{\infty,\lambda}$ to existential $\mathcal{L}$-formulas, because the λ-functions allow us to say that elements are p-independent. Indeed, the formula $\bigwedge_i(\lambda_{i,n}(x_1, \ldots, x_n; y) = 0) \wedge y \neq 0$ says that either $(x_1, \ldots, x_n)$ are p-dependent, or that $(x_1, \ldots, x_n, y)$ are p-independent. We have a first reduction:

LEMMA. *Let $\varphi(\bar{x})$ be a quantifier-free $\mathcal{L}_\lambda$-formula. Then, modulo $SCF_{\infty,\lambda}$, $\varphi(\bar{x})$ is equivalent to a finite disjunction of $\mathcal{L}$-formulas of the form*

$$\exists \bar{y}\ \psi(\bar{x}, \bar{y}) \wedge \theta(\bar{x}, \bar{y}),$$

where $\psi(\bar{x}, \bar{y})$ is quantifier-free, and $\theta(\bar{x}, \bar{y})$ is a conjunction of universal formulas expressing that some subtuples of $\bar{x}^\frown\bar{y}$ are p-independent.

Proof. Unraveling the λ-functions appearing in φ, it is easy to see that there are an integer m, a tuple $\bar{y} = (y_1, \ldots, y_m)$, a quantifier-free $\mathcal{L}$-formula

$\psi_0(\bar{x},\bar{y})$, and a formula $\theta_0(\bar{x},\bar{y})$, which is a conjunction of formulas of the form $y_i = \lambda_{j,k}(\bar{z};t)$ with $(\bar{z},t)$ some $(k+1)$-subtuple of $(\bar{x},y_1,\dots,y_{i-1})$, such that $\varphi(\bar{x})$ is equivalent to the formula

$$\exists \bar{y}\ \psi_0(\bar{x},\bar{y}) \wedge \theta_0(\bar{x},\bar{y}).$$

Modulo $\mathrm{SCF}_{\infty,\lambda}$, the formula $y = \lambda_{j,k}(\bar{z};t)$ is equivalent to a formula

$$(\exists \bar{u}\ \psi_j(\bar{z},t,y,\bar{u})) \vee (y = 0 \wedge \theta_j(\bar{z},t)),$$

where $\psi_j(\bar{z},t,y,\bar{u})$ is the quantifier-free $\mathcal{L}$-formula

$$(t = \sum_{i=1}^{p^k} u_i^p m_{i,k}(\bar{z}) \wedge u_j = y) \vee (y = 0 \wedge 0 = \sum_{i=1}^{p^k} u_i^p m_{i,k}(\bar{z}) \wedge \bigvee_{i=1}^{p^k} u_i \neq 0),$$

and $\theta_j(\bar{z},t)$ is the universal $\mathcal{L}$-formula expressing that $(\bar{z},t)$ is p-independent. The result follows.

(2.10) Lemma. *Let $\bar{a}$ be transformally algebraic over the difference field k. Assume that $\sigma(\bar{a}) \in k(\bar{a})^{\mathrm{alg}}$, and that $k(\bar{a})_\sigma$ is separable over k. For some m, there are tuples $\bar{b} \subset \{\bar{a},\dots,\sigma^{m-1}(\bar{a})\}$, $\bar{c} \subseteq \{\sigma(\bar{a}),\dots,\sigma^{m-1}(\bar{a})\}$ and $\bar{d} \subset \{\sigma(\bar{a}),\dots,\sigma^{m}(\bar{a})\}$, such that*

(a) *$\bar{b},\bar{c},\bar{d}$ is a separating transcendence basis of $k(\bar{a},\dots,\sigma^m(\bar{a}))$.*
(b) *$\bar{c} \in k(\bar{b}^p,\bar{d}^p,\sigma(\bar{c}))^s$, and $\sigma(\bar{c}) \in k(\bar{b}^p,\bar{d}^p,\bar{c})^s$.*
(c) *$\sigma^{-1}(\bar{d}) \in k(\bar{b}^p,\bar{c},\bar{d})^s$.*

Proof. Let $\bar{c} \subseteq \{\sigma^i(\bar{a}) \mid i \in \mathbb{Z}\}$ be a p-basis of $k(\bar{a})_\sigma$ over k. Replacing $\bar{c}$ by $\sigma^i(\bar{c})$ for some $i \in \mathbb{N}$ and $\bar{a}$ by $\bar{a}^\frown \cdots ^\frown \sigma^j(\bar{a})$ for some $j \in \mathbb{N}$, we may assume that $\bar{a}$ contains $\bar{c} \cup \sigma^{-1}(\bar{c})$, and that $\bar{c} \in k(\bar{a})^p(\sigma^{-1}(\bar{c}))$, $\sigma^{-1}(\bar{c}) \in k(\bar{a})^p(\bar{c})$. Let $d = \mathrm{tr.deg}(k(\bar{a})_\sigma/k)$, and consider the fields $K_{d,i}$, $i = 0,\dots,d+1$, defined in (2.4). Let i be such that $K_{d,i+1} = K_{d,i}$; then $K_{d,i+1}$ contains the tuple $\sigma^d(\bar{c})$, which is p-independent over k. Let $\bar{d} \subset \{\sigma^{i+1}(\bar{a}),\dots,\sigma^d(\bar{a})\}$ be such that $(\sigma^d(\bar{c}),\bar{d})$ is maximal p-independent over k in $K_{d,0}$. Let $\bar{b} \subseteq \{\bar{a},\dots,\sigma^{i-1}(\bar{a})\}$ be such that $\bar{b},\bar{c},\bar{d}$ is a p-basis of $K_{d,0}$ over k. Then $\sigma^{-1}(\bar{d}) \in k(\bar{b}^p,\bar{c},\bar{d})^s$ (see (2.4)), and so $(\bar{b},\bar{c},\bar{d})$ is our desired tuple.

(2.11) Lemma. *Let U and V be varieties of dimension d, defined over a difference field k. We assume that $V \subseteq U \times \sigma(U)$, and that V projects generically onto U and $\sigma(U)$. Let us write $k(V) = k(x_1,\dots,x_n,y_1,\dots,y_n)$. We also assume that there are integers $1 \leq r \leq s \leq d$ such that*

- *$(x_1,\dots,x_r,y_{r+1},\dots,y_d)$ is a separating transcendence basis of $k(V)$ over k.*
- *$x_{r+1},\dots,x_s$ are separably algebraic over $k(x_1^p,\dots,x_r^p,y_{r+1},\dots,y_s,y_{s+1}^p,\dots,y_d^p)$ and $y_{r+1},\dots,y_s$ are separably algebraic over $k(x_1^p,\dots,x_r^p,x_{r+1},\dots,x_s,y_{s+1}^p,\dots,y_d^p)$.*
- *$x_{s+1},\dots,x_d$ are separably algebraic over $k(x_1^p,\dots,x_r^p,y_{r+1},\dots,y_d)$.*

Then in some difference field extending k, there is a tuple $\bar{a}$ such that $k(\bar{a})_\sigma$ is separable over k, $(\bar{a}, \sigma(\bar{a})) \in V$ and $(a_{r+1}, \ldots, a_s)$ is p-independent over k in $k(\bar{a})_\sigma$.

Proof. Choose in some difference field (K, σ) containing k (e.g., in a model of ACFA), a tuple $\bar{a} = (a_1, \ldots, a_n)$ such that $(\bar{a}, \sigma(\bar{a}))$ is a generic of the algebraic set V. Our assumption on the dimensions of U and V implies that $\sigma(\bar{a})$ is algebraic over $k(\bar{a})$, so that $k(\bar{a})_\sigma \subseteq k(\bar{a})^{\mathrm{alg}}$. Let $\bar{b} = (a_1, \ldots, a_r)$, $\bar{c} = (\sigma(a_{r+1}), \ldots, \sigma(a_s))$, and $\bar{d} = (\sigma(a_{s+1}), \ldots, \sigma(a_d))$. Then $\bar{b} \cup \bar{c} \cup \bar{d}$ is a separating transcendence basis of $k(\bar{a}, \sigma(\bar{a}))$ over k, and $\sigma^{-1}(\bar{d})$ is separably algebraic over $k(\bar{b}^p, \bar{c}, \bar{d})$. Moreover, $\bar{c}$ is separably algebraic over $k(\bar{b}^p, \sigma^{-1}(\bar{c}), \bar{d}^p)$ and $\sigma^{-1}(\bar{c})$ is separably algebraic over $k(\bar{b}^p, \bar{c}, \bar{d}^p)$, and therefore, for every $M \geq 0$, we have

$$(*) \qquad k(\bar{a}^p, \ldots, \sigma^{M+m}(\bar{a})^p)(\bar{c}) = k(\bar{a}^p, \ldots, \sigma^{M+m}(\bar{a})^p)(\sigma^{M-1}(\bar{c})).$$

As in (2.5), one shows that for all M:

(a) $\sigma^{-1}(\bar{d}), \ldots, \sigma^{M-2}(\bar{d}) \in k(\bar{b}^p, \sigma^{M-1}(\bar{c}), \sigma^{M-1}(\bar{d}))^s$.
(b) $\bar{b} \cup \sigma^{M-1}(\bar{c}, \bar{d})$ is a separating transcendence basis of $k(\bar{a}, \ldots, \sigma^{m+M}(\bar{a}))$ over k.

By $(*)$, if $-1 \leq j \leq M$, then $\bar{b}, \sigma^j(\bar{c}), \sigma^{M-1}(\bar{d})$ is also a separating transcendence basis of $k(\bar{a}, \ldots, \sigma^{m+M}(\bar{a}))$ over k. This implies that $\bar{c}$ is p-independent over k in all the fields $k(\sigma^i(\bar{a}) \mid -n \leq i \leq n)$, and therefore is p-independent over k in $k(\bar{a})_\sigma$.

(2.12) THEOREM. *The theory of difference fields models of T_λ has a model companion $SCFA_{\infty,\lambda}$, which is axiomatised by expressing the following properties of the $\mathcal{L}_{\lambda,\sigma}$-structure (K, σ):*

(i) *$SCF_{\infty,\lambda}$.*
(ii) *σ is an automorphism of K.*
(iv) *For all m, if U and V are varieties defined over K satisfying the hypotheses of* (2.11) *(over K), then K satisfies:*

$$\forall z_1, \ldots, z_m, \exists x_1, \ldots, x_n, (\bar{x}, \sigma(\bar{x})) \in V$$
$$\wedge (\{z_1, \ldots, z_m\} \text{ } p\text{-independent}$$
$$\rightarrow \{z_1, \ldots, z_m, x_{r+1}, \ldots, x_s\} \text{ } p\text{-independent}).$$

Proof. As in Theorem (2.6), one shows that these axioms are indeed first-order. We will first show that every difference field model of T_λ embeds in a model of $\mathrm{SCFA}_{\infty,\lambda}$. Let K be a difference field, and let U, V be varieties satisfying the hypothesis of (2.11), let $\bar{b}$ be a tuple of elements of K, which we may assume p-independent in K. Consider the separable extension $L = K(\bar{a})_\sigma$ of K given by Lemma (2.11). Then $a_{r+1}, \ldots, a_s$ are p-independent over K, and therefore also over $\mathbb{F}_p(\bar{b})$. We conclude as in (2.6) that every difference field embeds in a model of $\mathrm{SCFA}_{\infty,\lambda}$.

It remains to show that $\mathrm{SCFA}_{\infty,\lambda}$ is model complete. Let K be a model of $\mathrm{SCFA}_{\infty,\lambda}$, and L a difference field containing K and separable over K. Let $\varphi(\bar{x})$ be a quantifier-free $\mathcal{L}_{\lambda,\sigma}$-formula with parameters in K, and assume that it is satisfied in L by a tuple $\bar{a}$. By (2.9), enlarging $\bar{a}$ if necessary, we may replace $\varphi(\bar{x})$ by a formula $\psi(\bar{x}) \wedge \theta(\bar{x})$, where $\psi(\bar{x})$ is a quantifier-free positive $\mathcal{L}_\sigma(K)$-formula, and $\theta(\bar{x})$ is an $\mathcal{L}(K)$-formula expressing that certain subtuples of $(\bar{x}, \bar{e})$ are p-independent, for some $\bar{e}$ in K.

We will show that there is $\bar{d}$ in some elementary extension K^* of K, such that K^* is a separable extension of $K(\bar{d})_\sigma$, and such that the difference fields $K(\bar{a})_\sigma$ and $K(\bar{d})_\sigma$ are isomorphic by a K-isomorphism f sending $\bar{a}$ to $\bar{d}$. Let $\bar{e} \in K$; if a subtuple of $\bar{a}$ is p-independent over $\mathbb{F}_p(\bar{e})$ in L, then it is also p-independent over $\mathbb{F}_p(\bar{e})$ in $K(\bar{a})_\sigma$, and therefore its image by f is p-independent over $\mathbb{F}_p(\bar{e})$ in $K(\bar{d})_\sigma$, and also in K^* as K^* is separable over $K(\bar{d})_\sigma$. Finding such a $\bar{d}$ will then finish the proof.

By (2.1), there is a tuple $\bar{b} \subseteq \bar{a}$ such that $\bar{b}$ is transformally transcendental over K, $K(\bar{a})_\sigma$ is separable and transformally algebraic over $K(\bar{b})_\sigma$. The saturation of K^* implies that K^* contains a tuple $\bar{c}$ of the same length as $\bar{b}$, of elements transformally transcendental over K, and such that K^* is a separable extension of $K(\bar{c})_\sigma$. Indeed, let $n = |\bar{b}|$; then for any m, the partial type saying that the elements $\sigma^i(x_j)$, $i = 0, \ldots, m-1, j = 1, \ldots, n$, are distinct and p-independent over K (in K^*), is finitely consistent, and therefore realised in K^*. Choose a tuple $\bar{c} = (c_1, \ldots, c_n)$ such that the elements $\sigma^i(c_i)$, $i \in \mathbb{Z}, 1 \leq j \leq n$, are p-independent over K. Then the tuple $\bar{c}$ is transformally transcendental over K, and K^* is a separable extension of $K(\bar{c})_\sigma$.

As in the proof of (2.6), we show that there is a K-isomorphism of difference fields $f : K(\bar{b})^s_\sigma \to K(\bar{c})^s_\sigma \subseteq K^*$. We use the saturation of K^*, (2.10) and (2.11), axiom (iv), and reason as in the proof of (2.6) to get a tuple $\bar{d}$ in K^* and a difference field isomorphism extending $f : K(\bar{b}, \bar{a})_\sigma \to K^*$ and sending $\bar{a}$ to $\bar{d}$. By axiom (iv) and (2.11), we may assume that the p-basis of $K(\bar{d})_\sigma$ over $K(\bar{c})_\sigma$ stays p-independent in K^*, and this implies that K^* is a separable extension of $K(\bar{d})_\sigma$. This finishes the proof.

(2.13). At first sight, the axiomatisations of $\mathrm{SCFA}_{e,\lambda}$ are quite different for $e \in \mathbb{N}$ and for $e = \infty$. We will show that $\mathrm{SCFA}_{\infty,\lambda}$ is nevertheless the limit of the theories $\mathrm{SCFA}_{e,\lambda}$, $e \in \mathbb{N}$.

PROPOSITION. *Let θ be an $\mathcal{L}_{\lambda,\sigma}$-sentence, and assume that $SCFA_{\infty,\lambda} \models \theta$. There is e_0 such that for all $e \geq e_0$, $SCFA_{e,\lambda} \models \theta$.*

Proof. By compactness, it suffices to show the assertion for all sentences occurring in the scheme of axioms given in (2.12). This is clear for axioms of type (i) or (ii). Let $K \models \mathrm{SCFA}_{e,\lambda}$, let $\bar{b}$ be an m-tuple of p-independent elements of K, and U, V varieties defined over K and satisfying the hypotheses of (2.11). Assume moreover that $m + (s - r) \leq e$ (in the notation of

(2.11)). We will show that there is a tuple $\bar{a}$ in K such that $(\bar{a}, \sigma(\bar{a})) \in V$ and $\{\bar{b}, a_{r+1}, \ldots, a_s\}$ is p-independent.

Let $\theta(\bar{x}, \bar{y})$ be the $\mathcal{L}_{\lambda,\sigma}(K)$-formula expressing this property of the tuple $(\bar{a}, \bar{b})$, and let $K(\bar{a})_\sigma$ be the extension of K constructed in Lemma (2.11). Then $\{a_{r+1}, \ldots, a_s\}$ is contained in a p-basis C of $K(\bar{a})_\sigma$ over K. Fix a p-basis B of K containing the m-tuple $\bar{b}$, and consider the extension M of $K(\bar{a})_\sigma$ constructed in Lemma 2.2(b). Then M is a separably algebraic extension of a field M_0 which is isomorphic to the field of fractions of $K\langle X_c \mid c \in C\rangle_B$. Hence it is enough to show that the elements of $\{\bar{b}, X_{a_i} \mid i = r+1, \ldots, s\}$ are p-independent in the field of fractions of $K\langle X_c \mid c \in C\rangle_B$. This will immediately follow from the following claim:

Claim. *Let $c_1, \ldots, c_n$ be distinct elements of B. Then $B \setminus \{c_1, \ldots, c_n\} \cup \{X_1, \ldots, X_n\}$ is a p-basis of the field of fractions K_n of $K\langle X_1, \ldots, X_n\rangle_B$.*

Proof. This is proved by induction on n. Assume first that $n = 1$. We identify $I(B)$ with $I(B \setminus \{c_1\}) \times \{0, \ldots, p-1\}$, by viewing a p-monomial in B as the product of a p-monomial in $B \setminus \{c_1\}$ with a p-monomial in c_1. This allows us to write

$$X = \sum_{i=0}^{p-1} \Big(\sum_{j \in I(B\setminus\{c_1\})} X_{i,j}^p m_j(B \setminus \{c_1\}) \Big) c_1^i.$$

Hence c_1 satisfies an equation of degree $p-1$ over $K_1^p[B \setminus \{c_1\}, X]$; c_1 is also purely inseparable over this field, and hence is an element of this field. As B is a p-basis of K_1, so is $B \setminus \{c_1\} \cup \{X\}$, which proves the claim when $n = 1$.

Assume the result proved for n and view K_{n+1} as the field of fractions of $K_n\langle X_{n+1}\rangle_B$. By induction, $B_n = B \setminus \{c_1, \ldots, c_n\} \cup \{X_1, \ldots, X_n\}$ is a p-basis of K_n, and by (1.11), $K_n\langle X_{n+1}\rangle_B$ is naturally isomorphic to $K_n\langle X_{n+1}\rangle_{B_n}$ by a $K_n[X_{n+1}]$-isomorphism. Hence the case $n = 1$ gives us that $B_n \setminus \{c_{n+1}\} \cup \{X_{n+1}\} = B \setminus \{c_1, \ldots, c_{n+1}\} \cup \{X_1, \ldots, X_{n+1}\}$ is a p-basis of K_{n+1}.

By the claim, M is a separable extension of K, of the same degree of imperfection as K, and which satisfies $\exists \bar{x}\, \theta(\bar{x}, \bar{b})$. By model completeness of $\mathrm{SCFA}_{e,\lambda}$, K also satisfies this formula. Note that the integer e_0 does not depend on the parameters defining U and V but only on $m + s - r$. This proves the proposition.

3. Elementary invariants and types

Recall that if K is separably closed and $A \subseteq K$, then the model-theoretic algebraic closure of A inside the $\mathcal{L}$-structure K is obtained by taking the separable closure of the $\mathcal{L}_\lambda$-substructure of K generated by A (see [D]). Let K be a model of $\mathrm{SCFA}_{e,\lambda}$ for some e. If $A \subseteq K$, we define $\mathrm{acl}_\sigma(A)$ (or

$\mathrm{acl}_{\sigma,K}(A)$ if we need to specify in which field we take the λ-closure) to be the smallest separably closed subfield of K that is closed under σ, σ^{-1} and the λ-functions of K and which contains A. We know by results in [CP] that any completion of $\mathrm{SCFA}_{e,\lambda}$ is simple. We also know that if $K \models \mathrm{SCFA}_{e,\lambda}$, then the theory of K is completely determined by the isomorphism type of any difference separably closed subfield K_0 of K of degree of imperfection e. Thus, a priori, the theory of K might depend on the action of σ on a given p-basis. We will show that this is not the case, and that $\mathrm{Th}(K)$ is completely determined by the isomorphism type of its difference subfield $\mathbb{F}_p^s$. We will also obtain a slight generalisation of the independence theorem, and show that types over algebraically closed sets coincide with Lascar strong types. We start with a description of p-bases when $e \in \mathbb{N}$.

(3.1) LEMMA. *Let $K \models SCFA_{e,\lambda}$, and assume that B is a finite p-independent subset of K such that $\sigma(B) \subset K^p[B]$. Then there is a finite set D of elements fixed by σ, such that $K^p[D] = K^p[B]$.*

Proof. Let $e = |B|$, fix an enumeration of the p-monomials $m_i(B)$ in B, $i = 1, \ldots, p^e$, and let $m_i(\sigma(B)) = \sigma(m_i(B))$. As $\sigma(B)$ is also p-independent in K, we have that $K^p[\sigma(B)] = K^p[B]$. Let $A = (a_{j,i})$ be the $(p^e \times p^e)$-matrix with entries in K defined by $m_i(\sigma(B)) = \sum_j a_{j,i}^p m_j(B)$. Then A is an invertible matrix. Consider the following system of equations, in the unknown $\bar{X} = (X_1, \ldots, X_{p^e})$:

$$\begin{pmatrix} X_1 \\ \vdots \\ X_{p^e} \end{pmatrix} = A \begin{pmatrix} \sigma(X_1) \\ \vdots \\ \sigma(X_{p^e}) \end{pmatrix}. \tag{1}$$

If $(c_1, \ldots, c_{p^e})$ is a solution of (1) in $\mathbb{A}^{p^e}(K)$, then

$$\begin{aligned} \sigma\left(\sum_{i=1}^{p^e} c_i^p m_i(B)\right) &= \sum_{i=1}^{p^e} \sigma(c_i)^p m_i(\sigma(B)) = \sum_{i=1}^{p^e} \sigma(c_i)^p \sum_{j=1}^{p^e} a_{j,i}^p m_j(B) \\ &= \sum_{j=1}^{p^e} \sum_{i=1}^{p^e} \big(\sigma(c_i) a_{j,i}\big)^p m_j(B) = \sum_{j=1}^{p^e} c_j^p m_j(B), \end{aligned}$$

so that $\sum_{i=1}^{p^e} c_i^p m_i(B)$ is fixed by σ and belongs to $K^p[B]$. Let $F = \mathrm{Fix}(\sigma)$. The set of solutions of (1) in $\mathbb{A}^{p^e}(K)$ forms an F-vector space, and we will first show that it generates a K-vector space of dimension p^e. We prove by induction on $i \leq p^e$ that there are p^e-tuples $\bar{c}_1, \ldots, \bar{c}_i$ which are solutions of (1) and are (K-)linearly independent. Assume that we have already found the elements $\bar{c}_1, \ldots, \bar{c}_i$, and that $i < p^e$. Consider the $(p^e \times (i+1))$-matrix with columns $\bar{X}, \bar{c}_1, \ldots, \bar{c}_i$. Since the vectors $\bar{c}_1, \ldots, \bar{c}_i$ are independent in $\mathbb{A}^{p^e}(K)$, this matrix has a submatrix of size $(i+1) \times (i+1)$ with non-zero determinant

$g(\bar{X}) \in K[\bar{X}]$. Let $U \subseteq \mathbb{A}^{p^e+1}$ be the variety defined by $g(\bar{X})X' = 1$, and let $V \subseteq U \times \sigma(U)$ be defined by $\bar{X} = A\bar{Y}$. Then U and V satisfy the hypotheses of axiom (iii) of $\mathrm{SCFA}_{e,\lambda}$ (note that $k(U) = k(V)$), and therefore there is $(\bar{c}, c')$ in K such that $\bar{c} = A\sigma(\bar{c})$ and $g(\bar{c})c' = 1$. Then $\bar{c}_1, \ldots, \bar{c}_i, \bar{c}$ are linearly independent solutions of (1).

Fix linearly independent solutions $\bar{c}_1 = (c_{1,j}), \ldots, \bar{c}_{p^e} = (c_{p^e,j})$ of (1), and let $d_i = \sum_{j=1}^{p^e} c_{i,j}^p m_j(B)$ for $i = 1, \ldots, p^e$. Then the elements $d_1, \ldots, d_{p^e}$ are linearly independent in the K^p-vector space K. We claim that $\{d_1, \ldots, d_{p^e}\}$ contains a p-independent subset of size e. This is again proved by induction on $i \leq p^e$. Assume that $j(1), \ldots, j(i)$ are such that $d_{j(1)}, \ldots, d_{j(i)}$ are p-independent in K. Then $K^p[d_{j(1)}, \ldots, d_{j(i)}]$ is a K^p-vector space of dimension p^i. If $i < e$ then there is an n such that $d_n \notin K^p[d_{j(1)}, \ldots, d_{j(i)}]$, i.e., such that $d_{j(1)}, \ldots, d_{j(i)}, d_n$ are p-independent in K, and we let $j(i+1) = n$. Hence $K^p[B] \cap F$ contains a p-independent set D of size e. This implies that $K^p[B] = K^p[D]$.

(3.2) Corollary. *Let $e \in \mathbb{N}$ and let K be a model of $SCFA_{e,\lambda}$. Then K has a p-basis consisting of elements fixed by σ.*

(3.3) Corollary. *Let $K \models SCFA_{\infty,\lambda}$, and assume that K is transformally algebraic (over $\emptyset$). Then K has a p-basis contained in* $\mathrm{Fix}(\sigma)$.

Proof. If $\bar{a}$ is a tuple of elements of K, then the field $\mathbb{F}_p(\bar{a})_\sigma$ has finite transcendence degree, and therefore $K^p(\bar{a})_\sigma$ is a finite extension of K^p. By (3.1), there is a finite tuple $\bar{b}$ of elements of $\mathrm{Fix}(\sigma)$ such that $K^p(\bar{a})_\sigma = K^p(\bar{b})$. Hence we get that $K \subseteq K^p(\mathrm{Fix}(\sigma))$, and therefore $\mathrm{Fix}(\sigma)$ contains a p-basis of K.

(3.4) Lemma. *Let k be a separably closed difference field, let K_1 and K_2 be difference fields containing k, which are linearly disjoint and separable over k. Let B_1 be a p-basis of K_1 over k and B_2 a p-basis of K_2 over k, and assume that there is an injection $f : B_1 \to B_2$, and that the elements of $B_1 \cup f(B_1)$ are fixed by σ. Then K_1 and K_2 are contained in a common difference field L, which is separable over K_1 and over K_2, and in which B_2 is a p-basis of L over k. If f is onto, then B_1 is also a p-basis of L over k.*

Proof. As K_1 and K_2 are linearly disjoint over k, the field K_1K_2 has a unique structure of a difference field extending those of K_1 and K_2; this result is well-known but we will repeat the proof. To avoid confusion, let us denote by σ_i the automorphism of K_i, for $i = 1, 2$. By assumption σ_1 and σ_2 agree on k. Since K_1 and K_2 are linearly disjoint over k, their composite K_1K_2 is separable over K_1 and over K_2, and is isomorphic to the field of fractions of $K_1 \otimes_k K_2$. Define σ on K_1K_2 by setting $\sigma(a \otimes b) = \sigma_1(a) \otimes \sigma_2(b)$ for $a \in K_1$ and $b \in K_2$, and extending to K_1K_2. This is well-defined as K_1 and K_2 are linearly disjoint over k and σ_1 and σ_2 agree on k.

Let $C = \{b - f(b) \mid b \in B_1\}$ and $L = K_1K_2[c^{1/p^n} \mid c \in C, n \in \mathbb{N}]$. By assumption, the elements of C are fixed by σ, which implies that the automorphism σ of K_1K_2 extends uniquely to an automorphism of L, with $\sigma(c^{1/p^n}) = c^{1/p^n}$ for $c \in C$, $n \in \mathbb{N}$. Clearly we have $L = kL^p[B_2]$, so it is enough to show that B_1 and B_2 stay p-independent in L. This will ensure that L is separable over K_1 and over K_2.

As K_1 and K_2 are linearly disjoint over k, we know that $B_1 \cup B_2$ is a p-basis of K_1K_2 over k. Then $B_1 \cup C \cup (B_2 \setminus f(B_1))$ is also a p-basis of K_1K_2 over k. Thus K_1K_2 is a separable extension of $k(C)$, with p-basis $B_1 \cup (B_2 \setminus f(B_1))$ over $k(C)$. Lemma (1.12) tells us that $B_1 \cup (B_2 \setminus f(B_1))$ remains p-independent over $k(c^{1/p^n} \mid c \in C, n \in \mathbb{N})$ in L. This proves the result for B_1; the proof for B_2 is similar, using the fact that $B_2 \cup C$ is a p-basis of K_1K_2 over k.

(3.5) THEOREM. *Let (K_1, σ_1) and (K_2, σ_2) be models of SCFA$_{e,\lambda}$, with a common difference subfield (A, σ), and let $A_i =_{\text{def}} \operatorname{acl}_{\sigma_i, K_i}(A)$ for $i = 1, 2$. Then*

$$(K_1, \sigma_1) \equiv_A (K_2, \sigma_2) \iff (A_1, \sigma_1) \simeq_A (A_2, \sigma_2).$$

Proof. The left-to-right implication is clear. For the reverse implication, let $f : (A_1, \sigma_1) \to (A_2, \sigma_2)$ be an A-isomorphism of difference fields. Let g be an A-automorphism of the field Ω which extends f^{-1}. Because A_1 is separably closed and K_1, $g(K_2)$ are separable over A_1, we may choose g such that the field $g(K_2)$ is linearly disjoint from K_1 over A_1; then $g(A_2) = A_1$ is a substructure of the difference field $(g(K_2), g\sigma_2 g^{-1})$, and it is enough to show that $(g(K_2), g\sigma_2 g^{-1}) \equiv_{A_1} (K_1, \sigma_1)$. Hence we may assume that $A = A_1 = A_2$, and that K_1 and K_2 are linearly disjoint over the separably closed field A. Then there is a unique automorphism σ of K_1K_2 which extends σ_1 and σ_2 (see the proof of (3.4)).

Our assumption then implies that K_1 and K_2 are separable extensions of A, and that they have the same degree of imperfection $e \in \mathbb{N} \cup \{\infty\}$. If $e = \infty$, then by (2.12) the $\mathcal{L}_{\lambda,\sigma}$-structure (K_1K_2, σ) embeds in a model L of SCFA$_{\infty,\lambda}$, separable over K_1 and over K_2.

If $e \in \mathbb{N}$, then by (3.1) K_1 and K_2 have p-bases which are fixed by σ_1 and σ_2, respectively. Let $C_i \subset K_i \cap \operatorname{Fix}(\sigma_i)$ be a p-basis of K_i over A for $i = 1, 2$. If B is a p-basis of A, then $|B| + |C_i| = e$, and therefore $|C_1| = |C_2|$. By (3.4), there is a difference field L_0 containing K_1K_2, which is separable over A, and in which C_1 and C_2 are p-bases over A. Thus L_0 is a separable extension of K_1 and of K_2, of degree of imperfection e. By (2.6), L_0 embeds in a model L of SCFA$_{e,\lambda}$, separable over K_1 and over K_2.

In both cases, the model completeness of SCFA$_{e,\lambda}$ gives us that $(K_i, \sigma_i) \prec (L, \sigma)$ for $i = 1, 2$, and therefore that $(K_1, \sigma_1) \equiv_A (K_2, \sigma_2)$.

(3.6). This result has numerous consequences, which we now list. Most of them already appear in [CP].

COROLLARIES. *Let K be a model of $SCFA_{e,\lambda}$.*

(1) *Let $A = \mathrm{acl}_\sigma(A)$ and $B = \mathrm{acl}_\sigma(B)$ be subfields of K. Any difference field isomorphism f between A and B is elementary.*
(2) *Let $K \models SCFA_{e,\lambda}$, let $A \subseteq K$, and let $\bar{a}$ and $\bar{b}$ be tuples from K. Then $\mathrm{tp}(\bar{a}/A) = \mathrm{tp}(\bar{b}/A)$ if and only if there is a difference field isomorphism $f : \mathrm{acl}_\sigma(A, \bar{a}) \to \mathrm{acl}_\sigma(A, \bar{b})$ which fixes A and sends $\bar{a}$ to $\bar{b}$.*
(3) *The completions of $SCFA_{e,\lambda}$ are obtained by describing the isomorphism type of the difference field $\mathbb{F}_p^s$.*
(4) *Let $e \in \mathbb{N}$, $\bar{b} = \{b_1, \ldots, b_e\}$. The completions of $SCFA_{e,b}$ are obtained by describing the isomorphism type of the $\mathcal{L}_\sigma(\bar{b})$-structure $(\mathbb{F}_p(b_1, \ldots, b_e)^s, b_1, \ldots, b_e)$.*
(5) *Let $A \subseteq K$. Then $\mathrm{acl}_\sigma(A)$ is the model theoretic algebraic closure of A in K.*
(6) *Let $\varphi(\bar{x})$ be a formula of $\mathcal{L}_\sigma$. Then $\varphi(\bar{x})$ is equivalent modulo $SCFA_{e,\lambda}$ to a disjunction of formulas of the form*

$$(*) \qquad \exists \bar{y}\ \psi(\bar{x}, \bar{y}),$$

where $\psi(\bar{x}, \bar{y})$ is a positive quantifier-free $\mathcal{L}_{\lambda,\sigma}$-formula. Moreover there is a finite tuple $F(\bar{x})$ of terms of the language $\mathcal{L}_{\lambda,\sigma}$ such that in any difference field K, if $(\bar{a}, \bar{b})$ is a tuple of K satisfying ψ, then $\bar{b}$ is separably algebraic over $\mathbb{F}_p(F(\bar{a}))$.
(7) *If $\bar{b} = \{b_1, \ldots, b_e\}$, then any completion of $SCFA_{e,b}$ eliminates imaginaries.*

Proof. (1) Extend f to an automorphism of Ω, and consider the difference field $(L, \tau) = (f(K), f\sigma f^{-1})$. Then $\mathrm{acl}_{\tau,L}(B) = B$; by (3.5) this implies that $(L, \tau) \equiv_B (K, \sigma)$. As f defines an isomorphism between the difference fields (K, σ) and (L, τ), this implies that f is elementary.

(2)–(4) are clear by (3.5).

(5) As $\mathrm{acl}_\sigma(A)$ is separably closed, and K is a separable extension of $\mathrm{acl}_\sigma(A)$, there is an $\mathrm{acl}_\sigma(A)$-automorphism g of Ω such that the field $g(K)$ is linearly disjoint from K over $\mathrm{acl}_\sigma(A)$. As in the proof of (3.5), there is a model M of $\mathrm{SCFA}_{e,\lambda}$, containing the difference fields (K, σ) and $(g(K), g\sigma g^{-1})$, and separable over K and $g(K)$. Then $K \prec M$, $g(K) \prec M$, and every type over A realised in $K \setminus \mathrm{acl}_\sigma(A)$ is realised anew in $g(K)$, and is therefore non-algebraic.

(6) Let Σ be the set of formulas of the form given by $(*)$. Then Σ is closed under finite conjunctions.

Let K be a model of $\mathrm{SCFA}_{e,\lambda}$, and let $\bar{a}$ be a tuple of elements of K. By (3.5), the type of $\bar{a}$ (over $\emptyset$) is obtained by describing the isomorphism

type of the difference field $\mathrm{acl}_\sigma(\bar{a})$ with distinguished constants the elements of $\bar{a}$. Hence it is axiomatised by an infinite conjunction of formulas of Σ (note that for any formula $\theta(\bar{y})$ we always have $\theta(\bar{y}) \iff \theta(\sigma(\bar{y}))$; this allows us to describe the isomorphism type of $\mathrm{acl}_\sigma(\bar{a})$ without using σ^{-1}). Use compactness to deduce that each formula is equivalent modulo $\mathrm{SCFA}_{e,\lambda}$ to a disjunction of formulas of Σ.

(7) Let $K \models \mathrm{SCFA}_{e,b}$. Then any algebraically closed substructure of K is a separably closed field of degree of imperfection e, because the language contains symbols for elements of a p-basis. Thus Theorem (3.7) of [CP] (the independence theorem) holds over any algebraically closed subset of $(K, \bar{b})$. The proof of (2.9) in [CP] then gives us the result.

(3.7) Definition of independence, and the independence theorem. Let $K \models \mathrm{SCFA}_{e,\lambda}$, let $A, B, C \subseteq K$. We say that A and B are *independent over* C iff the fields $\mathrm{acl}_\sigma(C, A)$ and $\mathrm{acl}_\sigma(C, B)$ are linearly disjoint over $\mathrm{acl}_\sigma(C)$, and if, moreover, K is a separable extension of $\mathrm{acl}_\sigma(C, A)\,\mathrm{acl}_\sigma(C, B)$ when $e = \infty$.

The following result is a simple generalisation of (3.7) in [CP], and implies that any completion of $\mathrm{SCFA}_{e,\lambda}$ is simple, and that independence as defined above is non-forking, provided $\mathrm{acl}_\sigma(C)$ contains a p-basis of K if e is finite (see [KP]). It also gives a description of the Lascar strong types: $\mathrm{Lstp}(\bar{a}/A) \simeq \mathrm{tp}(\bar{a}/\,\mathrm{acl}_\sigma(A))$, provided $\mathrm{acl}_\sigma(A)$ contains a p-basis of K when $e \in \mathbb{N}$.

THEOREM. *Let $K \models SCFA_{e,\lambda}$, let $E = \mathrm{acl}_\sigma(E) \subseteq K$. Let $\bar{a}, \bar{b}, \bar{c}_1$ and $\bar{c}_2$ be tuples from K which satisfy:*

(i) *$\bar{a}$ and $\bar{b}$ are independent over E, $\bar{a}$ and $\bar{c}_1$ are independent over E, $\bar{b}$ and $\bar{c}_2$ are independent over E.*
(ii) *$\mathrm{tp}(\bar{c}_1/E) = \mathrm{tp}(\bar{c}_2/E)$.*
(iii) *If $e \in \mathbb{N}$, then E contains a p-basis of K.*

Then in some elementary extension of K there is $\bar{c}$ realising $\mathrm{tp}(\bar{c}_1/E \cup \bar{a}) \cup \mathrm{tp}(\bar{c}_2/E \cup \bar{b})$, which is independent from $(\bar{a}, \bar{b})$ over E.

Proof. The proof is absolutely standard, and follows the lines of (3.7) in [CP]. Below we will indicate some changes or remarks, which will allow the reader to modify suitably (3.7) of [CP]. Let $A = \mathrm{acl}_\sigma(E, \bar{a})$, $B = \mathrm{acl}_\sigma(E, \bar{b})$, $C = \mathrm{acl}_\sigma(E, \bar{c}_1)$, $C_2 = \mathrm{acl}_\sigma(E, \bar{c}_2)$, and $T = \mathrm{SCF}_e$.

(1) Note that our independence assumptions on A, B, C and C_2 simply mean that $\mathrm{tp}_T(A/B)$, $\mathrm{tp}_T(A/C)$ and $\mathrm{tp}_T(B/C_2)$ do not fork over E; see [D].

(2) Moving $\bar{c}_1$ by an A-automorphism, we may assume that C is independent (in the sense of T) from (A, B) over E: if $e = \infty$, this is immediate; if e is finite, this is because E contains a p-basis of K.

(3) $\mathrm{dcl}_T(-)$ will denote the λ-closure, and $\mathrm{acl}_T(-)$ the separable closure of $\mathrm{dcl}_T(-)$ (i.e., we are not working in T^{eq} as in [CP]). In our case, the independence assumptions give $\mathrm{dcl}_T(A, B) = AB$, $\mathrm{acl}_T(A, B) = (AB)^s$, etc.

(4) The claim is replaced by the following:

CLAIM. *$(AB)^s(AC)^s$ and $(BC)^s$ are linearly disjoint over BC.*

By Remark (1.9) in [CH], we know that $(AB)^s(AC)^s \cap (BC)^s \subseteq B^{\mathrm{alg}}C^{\mathrm{alg}}$. As $B^{\mathrm{alg}}C^{\mathrm{alg}}$ is purely inseparable over BC, this implies that $(AB)^s(AC)^s \cap (BC)^s = BC$, which gives the claim because $(BC)^s$ is a Galois extension of BC.

(5) From this new claim, we deduce that $\sigma \cup \sigma_2$ defines an automorphism of $L = (AB)^s(AC)^s(BC)^s$. Since the degree of imperfection of L is $\leq e$, we can embed L into a model K^* of $\mathrm{SCFA}_{e,\lambda}$. The result then follows from (3.6)(2).

(3.8) COROLLARY. *Independence as defined in* (3.7) *coincides with non-forking.*

(3.9) COROLLARY. *Let $A = \mathrm{acl}_\sigma(A) \subseteq K \models SCFA_{e,\lambda}$, and assume that A contains a p-basis of K if e is finite. Then the Lascar strong type over A of a tuple $\bar{a}$ in K is implied by* $\mathrm{tp}(\bar{a}/A)$.

Proof. We first recall the definition of the Lascar strong type. Let K^* be a large saturated elementary extension of K, and consider the group H of automorphisms of K^* generated by all groups $\mathrm{Aut}(K^*/M)$ where $A \subseteq M \prec K^*$. Then two elements of K^* have the same Lascar strong type over A if they are conjugate by some element of H.

It is enough to show that if $\bar{b}$ realises $\mathrm{tp}(\bar{a}/A)$ and is independent from $\bar{a}$ over A, then there is a difference field M containing A, such that $M \equiv_A K$ and $\mathrm{tp}(\bar{a}/M) = \mathrm{tp}(\bar{b}/M)$. Since A is separably closed, there is an A-automorphism f of Ω such that $f(K)$ is free from $\mathrm{acl}_\sigma(A, \bar{a}, \bar{b})$ over A. Then $(K, f\sigma f^{-1}) \equiv_A (K, \sigma)$. Since $\bar{a}$ and $\bar{b}$ realise the same type over A, there is an A-isomorphism $g : \mathrm{acl}_\sigma(A, \bar{a}) \to \mathrm{acl}_\sigma(A, \bar{b})$ which sends $\bar{a}$ to $\bar{b}$. By the independence theorem (3.7), there is M realising $\mathrm{tp}(f(K)/\mathrm{acl}_\sigma(A, \bar{a})) \cup g(\mathrm{tp}(f(K)/\mathrm{acl}_\sigma(A, \bar{a}))$, and independent from $\mathrm{acl}_\sigma(A, \bar{a}, \bar{b})$ over A. Then we have $M \equiv_A K$, and $\mathrm{tp}(\bar{a}/M) = \mathrm{tp}(\bar{b}/M)$.

4. Properties of models of $\mathrm{SCFA}_{e,\lambda}$

In this section, we show how some of the results of [CH] generalise to the theory $\mathrm{SCFA}_{e,\lambda}$. If $K \models \mathrm{SCFA}_{e,\lambda}$, we study $\mathrm{Fix}(\sigma)$, the difference fields (K, σ^n), and the difference field K^{p^∞} when K is ω-saturated.

(4.1) PROPOSITION. *Let (K, σ) be a model of $SCFA_{e,\lambda}$, and let $n > 0$. Then $(K, \sigma^n) \models SCFA_{e,\lambda}$. If (K, σ) is κ-saturated, so is (K, σ^n).*

Proof. The result will follow from the following claim:

CLAIM. *Let (k,σ) be a separably closed difference field, let (K,σ^n) be a separably closed difference field extending (k,σ^n), separable over k, and of the same degree of imperfection as k if $e \in \mathbb{N}$. Then there is a difference field (L,σ) containing (k,σ) and such that (L,σ^n) extends (K,σ^n) and is a separable extension of K.*

The proof of this claim is identical to the proof of (1.12) of [CH], but we will repeat it. For $i = 1,\dots,n-1$, choose a field extension K_i of k, which is isomorphic to K by an isomorphism $f_i : K \to K_i$ which agrees with σ^i on k, and let $K_0 = K$, $f_0 = id$. Since k is separably closed and the K_i's are separable extensions of k, we may assume that the K_i's are linearly disjoint over k, so that the composite L of $K_0 \cdots K_{n-1}$ is the field of fractions of the domain $K_0 \otimes_k K_1 \otimes_k \cdots \otimes_k K_{n-1}$. Note that L is a separable extension of K_0. For $i = 0,\dots,n-2$, let $\sigma_i = f_{i+1} f_i^{-1} : K_i \to K_{i+1}$; then σ_i is an isomorphism which agrees with σ on k. Let $\sigma_{n-1} = \sigma^n f_{n-1}^{-1} : K_{n-1} \to K$; then σ_{n-1} is an isomorphism which agrees with σ on k. Thus the isomorphisms σ_i, $i = 0,\dots,n-1$, extend to a unique automorphism σ' of L, which agrees with σ on k. It remains to show that σ'^n agrees with σ^n on K. Let $a \in K$; then $\sigma'^n(a) = \sigma_{n-1}\cdots\sigma_1\sigma_0(a) = (\sigma^n f_{n-1}^{-1})(f_{n-1}\cdots f_1^{-1})(f_1 f_0^{-1})(a) = \sigma^n(a)$.

Thus any instance of axiom (iii) or (iv) for (K,σ^n) has a solution in a difference field (L,σ) containing (K,σ), separable over K and of the same degree of imperfection. This shows that (K,σ^n) is a model of the scheme of axioms (iii) and (iv) if $e = \infty$. It is also clearly a separably closed σ^n-difference field of degree of imperfection e, and is therefore a model of $\mathrm{SCFA}_{e,\lambda}$. The statement about saturation is proved similarly.

(4.2) PROPOSITION. *Let (K,σ) be a model of $SCFA_{e,\lambda}$, let $\tau = \sigma^n \mathrm{Frob}^m$ for some $n \geq 1$ and $m \in \mathbb{Z}$, and let $F = \mathrm{Fix}(\tau)$, the subfield of K fixed by τ. Then F is a PAC field (i.e., every absolutely irreducible variety defined over F has an F-rational point), and $\mathrm{Gal}(F^s/F) \simeq \hat{\mathbb{Z}}$. Furthermore, K is a separable extension of F, and the degree of imperfection of F is e if $m = 0$, and 0 otherwise.*

Proof. Let us first do the case $m \neq 0$. Then $F \subseteq k = K^{p^\infty}$, so that F is perfect. Let V be a variety defined over F. Let (L,σ) be a model of ACFA containing k, linearly disjoint from K over k and let F' be the subfield of L fixed by $\sigma^n \mathrm{Frob}^m$. The composite field KL is then a difference field, separable over K and of the same degree of imperfection, so that it embeds in some elementary extension K^* of K. Since V is defined over $F \subset k$, and L is a model of ACFA the variety V has an F'-rational point, and $\mathrm{Gal}(F'^s/F') \simeq \hat{\mathbb{Z}}$. Hence, in K^*, if $F^* = \mathrm{Fix}(\sigma^n \mathrm{Frob}^m)$, then the same statements are true of F^*.

If $m = 0$, then by (4.1) we may assume that $\tau = \sigma$. Let $V \subseteq \Omega^n$ be an absolutely irreducible variety defined over F, and consider the subvariety W of $V \times V$, intersection of $V \times V$ with the diagonal of $\Omega^n \times \Omega^n$. Then W satisfies the assumptions of axiom (iii) or (iv), and so (K, σ) contains a tuple $\bar{a}$ with $(\bar{a}, \sigma(\bar{a})) \in W$. Then $\bar{a} \in V(F)$ by definition of W.

Fix $n > 1$, let $t_1, \ldots, t_n$ be algebraically independent over K, and extend σ to $K(t_1, \ldots, t_n)$ by setting $\sigma(t_i) = t_{i+1}$ for $i < n$, and $\sigma(t_n) = t_1$. Then the difference field $K(t_1, \ldots, t_n)$ is a separable extension of K, and satisfies the sentence $\exists x\ \sigma^n(x) = x \wedge \bigwedge_{i=1}^{n-1} \sigma^i(x) \neq x$. As K is existentially closed, K also satisfies that sentence, and therefore F has at least one extension of degree n for every $n > 1$. On the other hand, we know that $\mathrm{Gal}(F^s/F)$ is generated by the restriction of σ to F^s, which implies that F has at most one extension of degree n for each n. Hence $\mathrm{Gal}(F^s/F) \simeq \hat{\mathbb{Z}}$.

As the λ-functions of K are definable, F is closed under the λ-functions of K, and therefore K is a separable extension of F.

If $e \in \mathbb{N}$, then (3.2) shows that F contains a p-basis of K. If $e = \infty$, then axiom (iv) ensures that F contains infinitely many elements which are p-independent in K.

Remark. The conclusion that $\mathrm{Fix}(\sigma)$ is PAC with absolute Galois group isomorphic to $\hat{\mathbb{Z}}$ was also proved by Kudaibergenov; see [Ku].

(4.3) Proposition. *Let (K, σ) be a model of $SCFA_{e,\lambda}$ for some $e \in \mathbb{N}$, let $\tau = \sigma^n \mathrm{Frob}^m$ for some $n \geq 1$ and $m \in \mathbb{Z}$, and let $F = \mathrm{Fix}(\tau)$. Then every definable subset D of F^ℓ is definable using only parameters from F. If $n = 1$, then D is definable in the pure field F.*

Proof. Let $D \subseteq F^\ell$ be definable in K. The automorphism σ fixes D, and therefore, by elimination of imaginaries of $\mathrm{SCFA}_{e,b}$ ((3.6)(7)), the set D is definable by a formula of $\mathcal{L}_{\lambda,\sigma}$ with parameters in F.

If $n = 1$, then any field automorphism of F is an $\mathcal{L}_{\lambda,\sigma}$-automorphism (because $\sigma|_F = x^{p^{-m}}$ is definable in the pure field language, and because K is a separable extension of F). Fix a finite set of parameters $\bar{c}$ in F over which D is defined, and let F_0 be a countable elementary substructure of F containing $\bar{c}$. By compactness, it suffices to show that $\mathrm{SCFA}_{e,b} \cup \mathrm{tp}_F(\bar{a}/F_0) \vdash \mathrm{tp}_K(\bar{a}/F_0)$ for any $\bar{a} \in D$. (Here, $\mathrm{tp}_F(\bar{a}/F_0)$ denotes the type of the tuple $\bar{a}$ over F_0 in the pure field F, and $\mathrm{tp}_K(\bar{a}/F_0)$ the type of $\bar{a}$ over F_0 in the difference field K.) Without loss of generality, we may assume that F is sufficiently saturated.

Let $\bar{d} \in F$ realise $\mathrm{tp}_F(\bar{a}/F_0)$. Then there is a field automorphism f of F which leaves F_0 fixed and sends $\bar{a}$ to $\bar{d}$. Since F_0 is an elementary substructure of F, F and F_0^s are linearly disjoint over F_0, and $F_0^s F = F^s$. Hence f extends to an automorphism of F^s which is the identity on F_0^s. This implies that f commutes with σ because $\mathrm{Gal}(F^s/F) \simeq \mathrm{Gal}(F_0^s/F_0)$. By (3.6)(1),

f is an elementary partial map of the difference field K, and this gives the conclusion.

(4.4) LEMMA. *Let $k \subseteq K$ be difference fields, and assume that K is separable over k. Let L be the subfield of K consisting of elements transformally algebraic over k. Then K is a separable extension of L.*

Proof. Let $\bar{a}$ be a finite tuple of elements of L. By the definition of L, the transcendence degree of $k(\bar{a})_\sigma$ over k is finite. Hence there is a finite tuple $\bar{b} \subseteq \{\sigma^i(\bar{a}) \mid i \in \mathbb{N}\}$, that is maximal p-independent over k in K. Then $k(\bar{a})_\sigma \subseteq kK^p[\bar{b}]$. As σ is an automorphism of K, we also have $k(\bar{a})_\sigma \subseteq kK^p[\sigma^n(\bar{b})]$ for any n. Also, there is a positive integer m such that $k(\bar{a})_\sigma = k(\bar{a}^p)_\sigma[\bar{a}, \ldots, \sigma^m(\bar{a})]$.

We will show that there is a finite tuple $\bar{u}$ of elements of K, such that $\sigma^n(\bar{a}) \subseteq k(\bar{a}^p)_\sigma(\bar{b}, \bar{u}^p)$ for every $n \in \mathbb{Z}$. Indeed, choose $\bar{u}$ such that $\bar{a}, \ldots, \sigma^m(\bar{a}) \in k(\bar{b}, \bar{u}^p)$; then $k(\bar{a})_\sigma \subseteq k(\bar{a}^p)_\sigma[\bar{a}, \ldots, \sigma^m(\bar{a})] \subseteq k(\bar{a}^p)_\sigma(\bar{b}, \bar{u}^p)$. As σ is an automorphism of K, each $\sigma^n(\bar{b})$ is also p-independent in K. Consider the $k(\bar{a}^p)_\sigma(\bar{u}^p)$-vector space V generated by the p-monomials in $\bar{b}$. It has dimension $p^{|\bar{b}|}$. The p-monomials in $\sigma^n(\bar{b})$ are also linearly independent in V because the elements of $\sigma^n(\bar{b})$ are p-independent in K, and this implies that $k(\bar{a}^p)_\sigma(\bar{b}, \bar{u}^p) = k(\bar{a}^p)_\sigma(\sigma^n(\bar{b}), \bar{u}^p)$ for every $n \in \mathbb{Z}$. Fix a p-basis B of k. Then $\sigma^n(B)$ is also a p-basis of k and $k = k^p[B] = k^p[\sigma^n(B)]$. Hence for every $n \in \mathbb{Z}$ we have

$$k(\bar{a})_\sigma \subseteq (k(\bar{a})_\sigma(\bar{u}))^p[B, \bar{b}] = (k(\bar{a})_\sigma(\bar{u}))^p[\sigma^n(B), \sigma^n(\bar{b})]. \tag{1}$$

Fix $c \in k(\bar{a})_\sigma$ and a finite subset B_0 of B such that $c \in K^p[B_0, \bar{b}]$. From equation (1), we get that $\lambda_i(B_0 \cup \{\bar{b}\}; c)$ and $\lambda_i(\sigma^n(B_0) \cup \{\sigma^n(\bar{b})\}; \sigma^n(c)) \in k(\bar{a})_\sigma(\bar{u})$ for every $n \in \mathbb{Z}$ (the λ-functions are those of K). As the latter is the image of the former by σ^n, we obtain that the difference field generated by the elements $\lambda_i(B_0 \cup \{\bar{b}\}; c)$, where $c \in k(\bar{a})_\sigma$ and B_0 is a finite subset of B, has finite transcendence degree over $k(\bar{a})_\sigma$, and therefore is contained in L.

This shows that L is closed under the λ-functions of K, and therefore that K is a separable extension of L.

(4.5) PROPOSITION. *Let $e \in \mathbb{N} \cup \{\infty\}$, and let k be a difference field of degree of imperfection $\leq e$. Let (K, σ) be a model of $SCFA_{e,\lambda}$, separable over k. Let L be the set of elements of K which are transformally algebraic over k. Then $L \prec K$.*

Proof. The difference field L is certainly separably closed; hence L satisfies (i) and (ii). Any instance of axiom (iii) or (iv) is satisfied in a transformally algebraic extension of L contained in K, and hence in L, by the definition of L. If $e \in \mathbb{N}$, then K has a p-basis consisting of elements fixed by σ (by (3.1)), and these elements are therefore in L. If $e = \infty$, then $\mathrm{Fix}(\sigma) \subseteq L$ has infinite

degree of imperfection by (4.2). By Lemma (4.4), K is a separable extension of L. The model-completeness of $\mathrm{SCFA}_{e,\lambda}$ gives the result.

(4.6) PROPOSITION. *Let K be an ω-saturated model of $SCFA_{e,\lambda}$, and let $k = K^{p^\infty}$. Then $k \models ACFA$.*

Proof. Clearly k is a difference subfield of K and is algebraically closed. We need to show that if U and V are varieties defined over k, with $V \subseteq U \times \sigma(U)$, and such that V projects generically onto U and onto $\sigma(U)$, then there is a tuple $\bar{a}$ in k such that $(\bar{a}, \sigma(\bar{a})) \in V$. Let k_0 be a countable algebraically closed difference subfield of k over which U and V are defined. Choose, in some saturated model of ACFA containing k_0, an element $\bar{a}$ satisfying $(\bar{a}, \sigma(\bar{a})) \in V$, and such that $k_0(\bar{a})_\sigma$ and K are linearly disjoint over k_0. Consider $k_1 = k_0(\bar{a})_\sigma^{\mathrm{alg}}$. As k_0 is algebraically closed, k_1 is a separable extension of k_0, and therefore k_1K is a separable extension of K, of the same degree of imperfection. Hence there is an elementary extension L of K containing k_1K, and $\bar{a} \in L^{p^\infty}$. By ω-saturation of K, $\mathrm{tp}(k_1/k_0)$ is realised in K.

(4.7) PROPOSITION. *Let k and K be as above. If D is a quantifier-free definable subset of K^n, then $D \cap k^n$ is quantifier-free definable in the difference field (k, σ).*

Proof. We will first show that we may assume that D is quantifier-free definable by an $\mathcal{L}_\sigma$-formula, and then that we can assume that its defining parameters are in k. The first assertion follows from the fact that the value of the λ-term $\lambda_{i,m}(x_1, \ldots, x_m; x_{m+1})$ at any tuple $(a_1, \ldots, a_{m+1})$ with $a_j \in K^p$ is $a_j^{1/p}$ if $j = m+1$, $a_1, \ldots, a_m$ are p-independent, and the p-monomial corresponding to $\lambda_{i,m}$ is the p-monomial 1, and is 0 otherwise. Hence there is an integer ℓ such that a tuple $(a_1, \ldots, a_n)$ is in $D \cap k^n$ if and only if $(a_1^{1/p^\ell}, \ldots, a_n^{1/p^\ell})$ satisfies some $\mathcal{L}_\sigma(K)$-quantifier-free formula, if and only if $(a_1, \ldots, a_n)$ satisfies an $\mathcal{L}_\sigma(K)$-quantifier-free formula. Hence we may assume that D is a Boolean combination of σ-closed subsets of K^n.

For the second assertion we may therefore assume that D is a σ-closed subset of K^n. Then $D' = D \cap k^n$ is a σ-closed subset of k^n. If $\bar{a}_i, i \in \mathbb{N}$, is an infinite indiscernible sequence of tuples in D', then D' is defined over $\mathrm{acl}_\sigma(\bar{a}_i, i \in \mathbb{N})$; see [CH, (2.13)]. As $\mathrm{acl}_\sigma(\bar{a}_i, i \in \mathbb{N}) \subseteq k$, we get the result.

REMARK. There are, however, definable subsets of k^n which need parameters from K. E.g., if the characteristic is $\neq 2$, let $b \in K \setminus k$ be such that $\sigma(b) = b$, and consider the set D defined by

$$\sigma(x) = x \wedge \exists y\ \sigma(y) = y \wedge y^2 = x - b.$$

Then $D \cap k$ is not definable in the difference field (k, σ).

5. Modularity

In this section we investigate modularity of definable subsets of models of $\mathrm{SCFA}_{e,b}$ (for a fixed $e \in \mathbb{N}$). A word of warning on the terminology: our notion of modularity does not coincide with the notion of modularity defined on minimal sets; in the case of a stable theory, our notion agrees with one-basedness. Recall that in models of ACFA we have the following results (see [CHP]):

Let S be the set of realisations in a model of ACFA of a set of types over some set E. If S is modular, then all elements of S are transformally algebraic over E. Assume that all elements of S are transformally algebraic over E. Then S is modular if and only if S is orthogonal to all formulas $\sigma^n(x) = x^{p^m}$, with $n \geq 1$, $m \in \mathbb{Z}$.

We investigate how these results extend to models of $\mathrm{SCFA}_{e,b}$. We are not able to show the first assertion in our case. Assume now that S is such that any tuple of S is transformally algebraic over E. We are then able to show that non-modularity of S implies that S is non-orthogonal to some formula $\sigma^n(x) = x^{p^m}$ as above; the converse only holds if S is definable, and we give examples of modular ∞-definable subsets of $\mathrm{Fix}(\sigma^n \mathrm{Frob}^{-m})$. It is also likely that there are ∞-definable modular sets which contain elements not transformally algebraic over E. We derive some consequences of modularity for quantifier-free definable subsets of modular subgroups of an algebraic group. We end the chapter with some questions and an example.

(5.1) Definition of modularity. Let T be a simple theory, M a large saturated model of T and $E = \mathrm{acl}(E)$ a small subset of M. Let $S \subseteq M^n$ be a set which is invariant under $\mathrm{Aut}(M/E)$. Thus, S is either a definable set, or is the union of realisations of a set of types over E.

We say that S is *modular* if whenever $\bar{a}$ and $\bar{b}$ are finite tuples of members of S and $C = \mathrm{acl}^{\mathrm{eq}}_\sigma(E, \bar{a}) \cap \mathrm{acl}^{\mathrm{eq}}_\sigma(E, \bar{b})$, then $\mathrm{tp}(\bar{a}/C, \bar{b})$ does not fork over C.

(5.2). We will consider the theories $T = \mathrm{ACFA}$ and $T = \mathrm{SCFA}_{e,b}$. Note that any completion of either theory is simple and eliminates imaginaries. Recall that in case $T = \mathrm{ACFA}$, the algebraic closure of a subset of a model of ACFA is simply the smallest algebraically closed difference field containing that set (see [CH, (1.7)]). In case $T = \mathrm{SCFA}_{e,b}$, algebraic closure coincides with acl_σ; see (3.6)(5).

In both theories, independence of sets A, B over C is defined as linear disjointness of $\mathrm{acl}(C, A)$ and $\mathrm{acl}(C, B)$ over $\mathrm{acl}(C)$, and the independence theorem holds, thus showing that our notion of independence coincides with non-forking. It follows that the modularity of S can be expressed as follows: If $\bar{a}$ and $\bar{b}$ are finite tuples of members of S, then the fields $\mathrm{acl}(E, \bar{a})$ and $\mathrm{acl}(E, \bar{b})$ are linearly disjoint over $\mathrm{acl}(E, \bar{a}) \cap \mathrm{acl}_\sigma(E, \bar{b})$.

The following lemma is routine. Note that we are using here that if $A = \mathrm{acl}(A)$ and $\bar{a}$, $\bar{b}$ are independent over A, then $\mathrm{acl}(A, \bar{a}) \cap \mathrm{acl}(A, \bar{b}) = A$. The corresponding statement with $\mathrm{acl}^{\mathrm{eq}}$ may be false in an arbitrary simple theory.

LEMMA. *Let $K \models SCFA_{e,b}$ be sufficiently saturated, and let S be a set of realisations of a set of types over some $E = \mathrm{acl}_\sigma(E) \subseteq K$. Assume that S is modular. Let $\varphi(\bar{x}, \bar{y})$ be a formula over E, and assume that for every $\bar{a} \in S$ the set defined by $\varphi(\bar{a}, \bar{y})$ is finite. Then the set U of tuples $\bar{b}$ such that there is $\bar{a} \in S$ satisfying $\varphi(\bar{x}, \bar{b})$ is modular.*

Proof. Assume that U is not modular, and let $\bar{c} = (\bar{c}_1, \ldots, \bar{c}_n)$ and $\bar{d} = (\bar{d}_1, \ldots, \bar{d}_m)$ be tuples of elements of U such that $\bar{c}$ and $\bar{d}$ are not independent over $C = \mathrm{acl}_\sigma(E, \bar{c}) \cap \mathrm{acl}_\sigma(E, \bar{d})$. Choose tuples $\bar{a} = (\bar{a}_1, \ldots, \bar{a}_n), \bar{b} = (\bar{b}_1, \ldots, \bar{b}_m)$ in S such that $\varphi(\bar{a}_i, \bar{c}_i)$ and $\varphi(\bar{b}_j, \bar{d}_j)$ hold for all i, j, and such that $\bar{a}$ and $\bar{d}$ are independent over $E \cup \bar{c}$, and $\bar{b}$ and $\bar{a}$ are independent over $E \cup \bar{d}$. Then $\mathrm{acl}_\sigma(E, \bar{a}) \cap \mathrm{acl}_\sigma(E, \bar{b}) = C$, since our independence assumptions imply that $\mathrm{acl}_\sigma(E, \bar{a}) \cap \mathrm{acl}_\sigma(E, \bar{b}) \subseteq \mathrm{acl}_\sigma(E, \bar{d})$, and $\mathrm{acl}_\sigma(E, \bar{a}) \cap \mathrm{acl}_\sigma(E, \bar{c}, \bar{d}) \subseteq \mathrm{acl}_\sigma(E, \bar{c})$. This contradicts the modularity assumption on S.

(5.3) LEMMA. *Let $K \models SCFA_{e,b}$, and let $S \subseteq K^n$ be a set of realisations of a set of types over $E = \mathrm{acl}_\sigma(E) \subseteq K$. If S is modular, then for any tuple $\bar{a}$ of elements of S and any tuple $\bar{b}$ of elements of K, $\bar{a}$ and $\bar{b}$ are independent over* $\mathrm{acl}_\sigma(E, \bar{a}) \cap \mathrm{acl}_\sigma(E, \bar{b})$.

Proof. Let $\bar{a}$ be a tuple of elements of S and $\bar{b}$ a tuple of elements of K and assume that $\bar{a}$ and $\bar{b}$ are not independent over $C = \mathrm{acl}_\sigma(E, \bar{a}) \cap \mathrm{acl}_\sigma(E, \bar{b})$. Choose $\bar{c}$ in $\mathrm{acl}_\sigma(E, \bar{a})$ and $\bar{d}$ in $\mathrm{acl}_\sigma(E, \bar{b})$ such that the fields $C(\bar{c})_\sigma$ and $C(\bar{d})_\sigma$ are not linearly disjoint over C. Thus there is some algebraic set V defined over $C(\bar{d})_\sigma$ and not over C, such that $(\bar{c}, \ldots, \sigma^m(\bar{c}))$ is a generic of the variety V over $C(\bar{d})_\sigma$. Let $(\bar{a}_n, \bar{c}_n), n \in \mathbb{N}$, be an infinite sequence of realisations of $\mathrm{tp}(\bar{a}, \bar{c}/\mathrm{acl}_\sigma(E, \bar{b}))$ that is independent over $\mathrm{acl}_\sigma(E, \bar{b})$, with $(\bar{a}_1, \bar{c}_1) = (\bar{a}, \bar{c})$. Then $\mathrm{acl}_\sigma(E, \bar{a}_1) \cap \mathrm{acl}_\sigma(E, \bar{a}_i \mid i > 1) = C$, and the tuples $(\bar{c}_i, \ldots, \sigma^m(\bar{c}_i))$, $i > 1$, are generics of V and algebraically independent over $\mathrm{acl}_\sigma(E, \bar{b})$. By a classical result in algebraic geometry, a variety is defined over the algebraic closure of a finite set of independent generic solutions, and this implies that V is defined over the algebraic closure of $\mathbb{F}_p(\bar{c}_2, \ldots, \bar{c}_n)_\sigma$ for some n. This shows that $\bar{a}_1$ and $(\bar{a}_2, \ldots, \bar{a}_n)$ are not independent over C, and therefore shows that S is not modular.

(5.4) Definitions of orthogonality. We work in a model K of the theory T, where $T = \mathrm{ACFA}$ or $T = \mathrm{SCFA}_{e,b}$.

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

(2) Let p be a complete type over A and S a set of realisations of a set of types over $E = \mathrm{acl}(E)$. Then p is *orthogonal* to S if for any $F = \mathrm{acl}(F)$ containing E and $\bar{a} \in S$, $\mathrm{tp}(\bar{a}/F)$ is orthogonal to p.

(3) If S and T are two sets of realisations of sets of types over some $E = \mathrm{acl}(E)$, then S and T are *orthogonal* if for any $F = \mathrm{acl}(F)$ containing E and $\bar{a} \in S$, $\bar{b} \in T$, the tuples $\bar{a}$ and $\bar{b}$ are independent over F.

(4) Let $E = \mathrm{acl}(E)$ be a subset of K, and let $S \subseteq K^n$ be a set of realisations of a set of types over E. We say that S is *orthogonal to the fixed fields* if S is orthogonal to all formulas $\sigma^n(x) = x^{p^m}$ where $n \geq 1$, $m \in \mathbb{Z}$. Similarly, we say that a type p over E is *orthogonal to the fixed fields* if it is orthogonal to all formulas $\sigma^n(x) = x^{p^m}$ where $n \geq 1$, $m \in \mathbb{Z}$.

Remark. If $\mathrm{tp}(\bar{a}/E)$ is orthogonal to the fixed fields, and $b \in \mathrm{acl}(E, \bar{a})$, then $\mathrm{tp}(b/E)$ is orthogonal to the fixed fields.

(5.5). The following result should have been proved in [CHP], but was somehow overlooked:

Proposition. *Let L be a model of ACFA, let $E = \mathrm{acl}(E) \subseteq B = \mathrm{acl}(B) \subseteq L$, let $\bar{a} \in L$ be transformally algebraic over E, and assume that $\mathrm{acl}(E, \bar{a}) \cap B = E$. If $\bar{a}$ and B are not independent over E, then $\mathrm{tp}(\bar{a}/E)$ is non-orthogonal to a fixed field.*

Proof. Assume that B and $\bar{a}$ are not independent over E, but that $\mathrm{tp}(\bar{a}/E)$ is orthogonal to all fixed fields. Then $E(\bar{a})_\sigma$ and B are not linearly disjoint over E. By [CH] (2.13)(1), $Cb(\bar{a}/B)$ is contained in the algebraic closure of the difference field generated by finitely many realisations of $\mathrm{tp}(\bar{a}/E)$, and therefore is transformally algebraic over E. Hence there is $\bar{b} \in B$, with $\mathrm{tr.deg}(E(\bar{b})_\sigma/E) < \infty$, such that $E(\bar{a})_\sigma$ and $E(\bar{b})_\sigma$ are not linearly disjoint over E. We may therefore assume that $B = \mathrm{acl}(E, \bar{b})$. The proof is by induction on $SU(\bar{b}/F)$, for all F and all $\bar{a}'$ such that $\mathrm{tp}(\bar{a}'/F)$ is orthogonal to all fixed fields, and $\mathrm{acl}(F, \bar{a}') \cap \mathrm{acl}(F, \bar{b}) = F$.

Since $\bar{b}$ has finite SU-rank over E, by (3.4)(1) of [CH], there is $F = \mathrm{acl}(F)$ containing E and independent from $\bar{b}$ over E, and $c \in \mathrm{acl}(F, \bar{b})$ such that $SU(c/F) = 1$. We may choose this F independent from $(\bar{a}, \bar{b})$ over E, and this implies that $\mathrm{acl}(F, \bar{a}) \cap \mathrm{acl}(F, \bar{b}) = F$. Note that c is independent from $\bar{a}$ over F because $SU(c/F) = 1$ and $c \notin \mathrm{acl}_\sigma(F, \bar{a})$. Hence $\mathrm{tp}(\bar{a}/F, c)$ is orthogonal to all fixed fields and $SU(\bar{b}/F, c) < SU(\bar{b}/E)$. To use the induction hypothesis and prove the result, it is therefore enough to show that $\mathrm{acl}(F, \bar{a}, c) \cap \mathrm{acl}(F, \bar{b}) = \mathrm{acl}(F, c)$.

Assume that this is not the case and let $d \in \mathrm{acl}(F, \bar{a}, c) \cap \mathrm{acl}(F, \bar{b})$, $d \notin \mathrm{acl}(F, c)$. Using the semi-minimal analysis of $\mathrm{tp}(\bar{b}/\mathrm{acl}(F, c))$ (see [CHP] (7.3) and [CH] (5.4)), we may assume that either $\mathrm{tp}(d/F, c)$ is modular of rank 1, or that $\mathrm{tp}(d/F, c)$ is qf-internal to some fixed field defined by an equation

$\sigma^n(x) = x^{p^m}$ for some $n \geq 1$ and $m \in \mathbb{Z}$. Since $\mathrm{tp}(\bar{a}/F, c)$ is orthogonal to all fixed fields, it will be orthogonal to anything which is qf-internal to a fixed field. It follows that $\mathrm{tp}(d/F, c)$ is modular and of rank 1.

If $\mathrm{tp}(c/F)$ is modular, then so is $\mathrm{tp}(c, d/F)$ (see [CHP, (7.4)]), which gives us a contradiction, as $\mathrm{acl}(F, c, d) \cap \mathrm{acl}(F, \bar{a}) = F$ and $d \in \mathrm{acl}(F, \bar{a}, c)$. If $SU(d/F) = 1$ and $\mathrm{tp}(c/F)$ is non-modular, we also reach a contradiction, since $d \in \mathrm{acl}(F, \bar{a}, c)$ implies $d \in \mathrm{acl}(F, \bar{a})$. Hence we are left with the case where $SU(d/F) = 2$ and $\mathrm{tp}(c/F)$ is non-modular. Note that $c \in \mathrm{acl}(F, d)$. Let $(c, d) = (c_1, d_1), \ldots, (c_n, d_n), \ldots$, be an infinite sequence of independent realisations of $\mathrm{tp}(c, d/\mathrm{acl}(F, \bar{a}))$; because $\bar{a}$ and (c, d) are not independent over F, the sequence (c_n, d_n) is not independent over F, and there is a largest i such that $SU(c_1, d_1, \ldots, c_i, d_i/F) = 2i$. Then $d_1, \ldots, d_i$ are independent over F, and $SU(d_{i+1}/F, d_1, \ldots, d_i) \leq 1$. By the choice of our sequence, $c_{i+1} \notin \mathrm{acl}(F, d_1, \ldots, d_i)$, and $d_{i+1} \in \mathrm{acl}(F, d_1, \ldots, d_i, c_{i+1})$. Hence $\mathrm{tp}(d_1/\mathrm{acl}(F, d_2, \ldots, d_i, c_{i+1}))$ does not fork over F, and is not almost orthogonal to the modular rank-1-type $\mathrm{tp}(d_{i+1}/\mathrm{acl}(F, c_{i+1}))$. This means that $\mathrm{tp}(d/F)$ is non-orthogonal to a modular type of rank 1. Hence there is $F' = \mathrm{acl}(F')$, independent from $(\bar{a}, \bar{b})$ over F, such that $\mathrm{acl}(F', d)$ contains an element e realising a modular type of SU-rank 1 over F'. By the first case, we have that $\mathrm{acl}(F', \bar{a}, e) \cap \mathrm{acl}(F', \bar{b}) = \mathrm{acl}(F', e)$. By the induction hypothesis on $SU(\bar{b}/F', e) < SU(\bar{b}/F')$, we get that $(\bar{a}, e)$ and $\bar{b}$ are independent over $\mathrm{acl}(F', e)$, and therefore that $\bar{a}$ and $\bar{b}$ are independent over F', which gives us the desired contradiction. Hence this case cannot happen, which means that $\mathrm{acl}(F, \bar{a}, c) \cap \mathrm{acl}(F, \bar{b}) = \mathrm{acl}(F, c)$, and we are done.

(5.6) Proposition. *Let $K \models SCFA_{e,b}$, $E = \mathrm{acl}_\sigma(E) \subseteq K$, and let $S \subseteq K^n$ be the set of realisations of a set of types over E, and assume that all elements of S are transformally algebraic over E. If S is non-modular, then S is non-orthogonal to a fixed field.*

Proof. Let L be a model of ACFA containing K, and assume that S is not modular. Then there are $\bar{a}_1, \ldots, \bar{a}_m \in S$, and $B = \mathrm{acl}_\sigma(B) \supseteq E$ such that $(\bar{a}_1, \ldots, \bar{a}_m)$ and B are not independent over $C = \mathrm{acl}_\sigma(E, \bar{a}_1, \ldots, \bar{a}_m) \cap B$. Let $\bar{d} \in A = \mathrm{acl}_\sigma(E, \bar{a}_1, \ldots, \bar{a}_m)$ be such that the fields $C(\bar{d})_\sigma$ and B are not linearly disjoint over C. We may assume that $\bar{d}$ contains $\bar{a}_1^\frown \cdots^\frown \bar{a}_m$. By Lemma 4.4, $\bar{d}$ is transformally algebraic over E, and therefore also over C.

We will denote by $\mathrm{acl}_L(-)$ the algebraic closure in the sense of L, and by tp_L types in the sense of $\mathrm{Th}(L)$. Recall that $A = \mathrm{acl}_L(A)$ if and only if A is an algebraically closed difference field. Hence, if $A = \mathrm{acl}_\sigma(A)$, then $\mathrm{acl}_L(A) = A^{\mathrm{alg}} = A^{p^{-\infty}}$.

Our assumption on A, B, C implies that $\mathrm{acl}_L(A) \cap \mathrm{acl}_L(B) = \mathrm{acl}_L(C)$, and that $\bar{d}$ is not independent from B over C (in the sense of L). By (5.5), this implies that $\mathrm{tp}_L(\bar{d}/C)$ is non-orthogonal to a formula $\sigma^n(x) = x^{p^m}$ for some

$n \geq 1$ and $m \in \mathbb{Z}$, and we may assume that $(n, m) = 1$. Let $\mathrm{Fix}(\tau)$ be the subfield of L fixed by $\tau = \sigma^n \operatorname{Frob}^{-m}$.

Claim. *There are independent realisations $\bar{d}_1, \ldots, \bar{d}_k$ of $\mathrm{tp}(\bar{d}/C)$ in K such that $C(\bar{d}_1, \ldots, \bar{d}_k)_\sigma \cap \mathrm{Fix}(\tau)$ contains an element not in C.*

Indeed, since $\mathrm{tp}_L(\bar{d}/C)$ is non-orthogonal to $\sigma^n(x) = x^{p^m}$, there are integers k, ℓ, and independent realisations $\bar{d}_1, \ldots, \bar{d}_k$ of $\mathrm{tp}_L(\bar{d}/C^{\mathrm{alg}})$ in L, elements $b_1, \ldots, b_\ell$ of $\mathrm{Fix}(\tau)$ that are independent over C and such that the fields $\mathrm{acl}_L(C, \bar{d}_1, \ldots, \bar{d}_k)$ and $\mathrm{acl}_L(C, b_1, \ldots, b_\ell)$ are not linearly disjoint over C^{alg} (see Remark (3.1)(1) in [CH]). Now $\mathrm{acl}_L(C, b_1, \ldots, b_\ell)$ is algebraic over $C(b_1, \ldots, b_\ell, \ldots, \sigma^{n-1}(b_\ell))$, and hence we obtain that $(b_1, \ldots, \sigma^{n-1}(b_\ell))$ are not algebraically independent over $C(\bar{d}_1, \ldots, \bar{d}_k)_\sigma$. Let V be the algebraic locus of $(b_1, \ldots, \sigma^{n-1}(b_\ell))$ over $C(\bar{d}_1, \ldots, \bar{d}_k)_\sigma$; then $(b_1, \ldots, \sigma^{n-1}(b_\ell))$ is a generic of V, is fixed by τ, and therefore is also a generic of $\tau(V)$. Hence $\tau(V) = V$, the field of definition of V is fixed by τ, contained in the perfect hull of $C(\bar{d}_1, \ldots, \bar{d}_k)_\sigma$, and not contained in C^{alg}. This implies that $C(\bar{d}_1, \ldots, \bar{d}_k)_\sigma$ contains an element of $\mathrm{Fix}(\tau)$ not in C.

The above result depends only on the isomorphism type of the difference field $C(\bar{d}_1, \ldots, \bar{d}_k)_\sigma$, and so one may furthermore impose that the tuples $\bar{d}_1, \ldots, \bar{d}_k$ realise independent realisations of $\mathrm{tp}(\bar{d}/C)$ in K. This proves the claim.

Hence we have $\bar{a}_1, \ldots, \bar{a}_{mk}$ in S, such that $\mathrm{acl}_\sigma(E, \bar{a}_1, \ldots, \bar{a}_{mk}) \cap \mathrm{Fix}(\tau)$ contains an element b not in C, and hence not in E. Thus there is i such that $b \in \mathrm{acl}_\sigma(E, \bar{a}_1, \ldots, \bar{a}_i)$, $b \notin \mathrm{acl}_\sigma(E, \bar{a}_1, \ldots, \bar{a}_{i-1})$, and we have shown that S is non-orthogonal to a fixed field.

(5.7) Proposition. *Let $K \models SCFA_{e,b}$, let S be a definable modular subset of K^n, defined over $E = \mathrm{acl}_\sigma(E)$. Then S is orthogonal to the fixed fields.*

Proof. By (5.2) it suffices to show that any infinite definable subset S of a fixed field $k = \{x \mid \sigma^n(x) = x^{p^m}\}$, $n \geq 1$, $m \in \mathbb{Z}$, $(n, m) = 1$ if $m \neq 0$, is non-modular.

We first assume that $m = 0$. By (4.3), we know that S is definable in the pure field language within k. Let B be the p-basis of k (which is also a p-basis of K). By Theorem 3.5 and Proposition 4.1, the type of a tuple $\bar{a}$ of k is determined by the isomorphism type of its algebraic closure, which is the relative separable closure in k of the closure of $\mathbb{F}_p(B, \bar{a})$ under the λ-functions $\lambda_i(B; -)$, $i \in I(B)$. Hence, using compactness, it follows that $S = \pi(W(k))$ for some algebraic set W and algebraic morphism π, which is finite-to-one on $W(k)$. By (5.2), we may therefore replace S by $W(k)$, where W is a (absolutely irreducible) variety defined over k. Then the function field $k(W)$ is a regular extension of k. Let $x \in k(W)$ be an element of a separating transcendence

basis of $k(W)$ over k, and let $y \in k(W)$ be such that $k(W) \cap k(x)^s = k(x,y)$. Then $k(W)$ is a regular extension of $k(x,y)$. If $f(x,Y) \in k(x)[Y]$ is the minimal polynomial of y over $k(x)$, then the equation $f(X,Y) = 0$ defines an absolutely irreducible curve C, and we have a rational map $g : W \to C$, defined over k; then, for all but finitely many $(a,b) \in C(k^{\mathrm{alg}})$, $g^{-1}(a,b)$ is absolutely irreducible. Hence, since k is PAC, $g(W(k))$ is a cofinite subset of the infinite set $C(k)$. Thus we have reduced the problem to showing that $C(k)$ is not modular.

The proof now uses a trick already used for pseudo-finite fields. Observe first that $k(x^{1/p^n}, y \mid n \in \mathbb{N})$ is a separable extension of k, because $k(x,y)$ is separably algebraic over $k(x)$. Let k_1 be a saturated extension of k, and let $(a_1,a_2),(b_1,b_2) \in C(k_1)$, with $a_1, b_1 \in k_1^{p^\infty}$, transcendental and algebraically independent over k. Consider $(k_1)^{\mathrm{alg}}(x,y)$. By 11.7 and 12.9 of [FJ], there is a Zariski open subset U of $\mathbb{A}^2$ such that if $a,b \in U$, then the polynomial $f(a+bx,Y)$ is irreducible over $(k_1)^{\mathrm{alg}}(x,y)$; since f has its coefficients in k, the Zariski open set U is defined over k, and therefore contains a_1 and b_1.

This shows that the algebraic set defined by $f(x,y) = 0 = f(a_1 + b_1 x, y')$ is absolutely irreducible, and defined over k_1. Hence it has a solution (c_1,c_2,d_2) in k_1, and we may assume that c_1 belongs to $k_1^{p^\infty}$ and is transcendental over $k(a_1,b_1)$. Let $d_1 = a_1 + b_1 c_1$. Then $(c_1,c_2),(d_1,d_2) \in C(k_1)$. Since $a_1,b_1,c_1,d_1 \in k_1^{p^\infty}$, we have $\mathrm{acl}_\sigma(k,a_1,b_1) \subseteq k(a_1,b_1)^{\mathrm{alg}}$ and $\mathrm{acl}_\sigma(k,c_1,d_1) \subseteq k(c_1,d_1)^{\mathrm{alg}}$, and therefore $\mathrm{acl}_\sigma(k,a_1,b_1) \cap \mathrm{acl}_\sigma(k,c_1,d_1) \subseteq k^{\mathrm{alg}} \cap k_1 = k$. However, (a_1,b_1) and (c_1,d_1) are not independent over k, and this shows that $C(k)$ is not modular.

If $m \neq 0$, then $k \subseteq K^{p^\infty}$. Proposition (7.1)(1) of [CHP] gives that if E is a difference field, and $a \in k$, $a \notin E$, then $\mathrm{tr.deg}(a/E) = n$. This implies that in K, any element of k is either in E or independent from E, so that $SU(k) = 1$. Hence $SU(S) = SU(k) = 1$, and the non-modularity of the field k implies the non-modularity of S. Observe that this also proves the result for an ∞-definable S.

(5.8) Proposition. *Let $K \models SCFA_{e,b}$, let S be a definable modular subset of K^n, defined over $E = \mathrm{acl}_\sigma(E)$. Then every tuple $\bar{a} \in S$ is transformally algebraic over E.*

Proof. By (5.2) and (3.6)(6), we may assume that S is defined by a quantifier-free $\mathcal{L}_\sigma$-formula. Assume by way of contradiction that there is $\bar{a} = (a_1,\ldots,a_n) \in S$ which is not transformally algebraic over E. By Lemma 2.1, $\bar{a}$ contains an element, say a_1, which is transformally transcendental over E and such that $E(\bar{a})_\sigma$ is a separable extension of $E(a_1)_\sigma$. If S_1 is the projection of S on the first coordinate, then S_1 is also modular by (5.2), and because S is defined by a quantifier-free formula of $\mathcal{L}_\sigma$, S_1 contains all elements of

K which are transformally transcendental over E. Then $E(\bar{a}, a_1^{p^n} \mid n \in \mathbb{N})_\sigma$ is a separable extension of E, and we may therefore assume that $a_1 \in K^{p^\infty}$. Let $b = \sigma(a_1) - a_1$; then $a_1 \notin \mathrm{acl}_\sigma(E, b)$, and $\mathrm{acl}_\sigma(E, b) \subseteq E(b)_\sigma^{\mathrm{alg}}$ because $b \in K^{p^\infty}$. Hence the set S_2 defined by $x \in S_1 \wedge \sigma(x) - x = b$ contains a_1, and is infinite, and hence is modular and orthogonal to the fixed fields by (5.2) and (5.7). But the set of solutions of $\sigma(x) - x = b$ equals $a_1 + \mathrm{Fix}(\sigma)$, and we get a contradiction.

(5.9) Remark. Proposition 5.7 does not generalise to ∞-definable subsets of K^n if $e > 0$. Indeed, let $k = \mathrm{Fix}(\sigma)$. Hrushovski has shown the following result (see 2.15, 2.16 and 5.6 in [H]):

Let L be a separably closed field, let G be a simple abelian variety defined over L but not isomorphic to one defined over L^{p^∞}. Then $\Gamma = \bigcap_n [p^n]G(L)$ is modular.

Assume that $L = k^s$, and that G is defined over k. Observe that if $A \subseteq k$, then $\mathrm{acl}_L(A)$ (the model-theoretic algebraic closure of A in the sense of the separably closed field L) equals $\mathrm{acl}_\sigma(A)$. Indeed, $\mathrm{acl}_L(A)$ is obtained by taking first the λ-closure of the field generated by A under the λ-functions of L, and then its separable closure. On k, the λ-functions of K, k and L agree (as they have a common p-basis B), and this shows the assertion.

This implies that if $A, B \subseteq k$, then A and B are independent over $C = \mathrm{acl}_\sigma(A) \cap \mathrm{acl}_\sigma(B)$ if and only if they are independent over C in the separably closed field L. Hence $\Gamma \cap G(k)$ is a modular subgroup of $G(K)$.

(5.10) Two questions.

(1) Let S be an ∞-definable subset of K^n, and assume that S is modular. Does this imply that every element of S is transformally algebraic over the set over which S is defined?

(2) Is there a criterion analogous to (5.6) for modular subsets of models of $\mathrm{SCFA}_{\infty,\lambda}$? Recall that by (3.7), forking may arise at the level of p-independence and so we may have $\mathrm{acl}_\sigma(E, \bar{a})$ and $\mathrm{acl}_\sigma(E, \bar{b})$ linearly disjoint over $E = \mathrm{acl}_\sigma(E)$, but $\bar{a}$ and $\bar{b}$ not independent over E. We also do not have a good description of imaginaries in $\mathrm{SCF}_{\infty,\lambda}$.

(5.11). Modularity is an important tool in the study of definable sets, and in our context, modular subgroups of algebraic groups have good properties.

Theorem. *Let $K \models SCFA_{e,\lambda}$, let G be an algebraic group definable over K and let S be a subgroup of $G(K)$ which is ∞-definable by quantifier-free $\mathcal{L}_{\lambda,\sigma}$-formulas and which is modular. Let $U \subseteq G(K)$ be quantifier-free definable. Then $U \cap S$ is a Boolean combination of cosets of definable subgroups of S. If S is defined over $E = \mathrm{acl}_\sigma(E)$, then so are these subgroups.*

Proof. We assume K sufficiently saturated, and let B be the p-basis of K (which is fixed by σ and contained in E because the elements of B are in the

language). Consider the set Δ of quantifier-free $\mathcal{L}_{\lambda,\sigma}$-formulas. Then over any subset $E = \mathrm{acl}_\sigma(E)$ of K, there are at most $|E|^{\aleph_0}$ Δ-types. Indeed, the Δ-type of a tuple $\bar{a}$ over E is determined by the $\mathcal{L}_\lambda$-type of the countable tuple $(\sigma^i(\bar{a}))_{i\in\mathbb{Z}}$ over E. Since the theory $\mathrm{SCF}_{e,b}$ is stable, there are at most $|E|^{\aleph_0}$ $\mathcal{L}_\lambda$-types of countable tuples over E, and hence at most $|E|^{\aleph_0}$ Δ-types over E. The result now follows by a result of Pillay [P], because the formulas of Δ are stable and witness forking. Since Pillay's result is unpublished, we will give an alternate proof of the result in our particular case, using the underlying topology on Cartesian powers of K. Since we will be dealing with integers which are powers of p, we will use the notation $\mathbb{A}^m(K)$ to denote the Cartesian product of m copies of K.

We put two topologies on $\mathbb{A}^m(K)$: the σ-topology and the $\lambda\sigma$-topology. The σ-topology is the topology whose basic closed sets are defined by positive quantifier-free $\mathcal{L}_\sigma$-formulas, and we call these sets σ-closed. This topology is Noetherian (see [C]), and therefore any σ-closed set X is the union of finitely many irreducible σ-closed sets, called the irreducible components of X. Note that $\mathbb{A}^m(K)$ is compact and Hausdorff.

The $\lambda\sigma$-topology on $\mathbb{A}^m(K)$ is generated by the closed sets $X \subseteq \mathbb{A}^m(K)$ defined by positive Δ-formulas; we call these sets basic $\lambda\sigma$-closed. The $\lambda\sigma$-tology is not Noetherian, but every $\lambda\sigma$-closed set is the intersection of countably many basic $\lambda\sigma$-closed sets. Again, each $\mathbb{A}^m(K)$ is compact and Hausdorff.

For each $n \in \mathbb{N}$, we identify K with $\mathbb{A}^{p^{en}}(K)$ via the map $\psi_n : x \mapsto (\lambda_\mu(B;x))_{\mu\in I(B)^n}$. Then the algebraic group G gives rise to an algebraic group $G_n = \psi_n(G)$ defined over K, of dimension $p^{en}\dim(G)$.

If X is a basic $\lambda\sigma$-closed subset of $\mathbb{A}^m(K)$, there is an integer n such that $X_n = \psi_n(X)$ is σ-closed in $\mathbb{A}^{mp^{ne}}(K)$, and then $X = \psi_n^{-1}(X_n)$. Thus the $\lambda\sigma$-topology on $\mathbb{A}^m(K)$ is the smallest topology such that all maps $\psi_n : \mathbb{A}^m(K) \to \mathbb{A}^{mp^{en}}(K)$ are continuous, where $\mathbb{A}^{mp^{en}}(K)$ is equipped with the σ-topology.

We call a $\lambda\sigma$-closed set X irreducible if it is not the proper union of two closed subsets. We say that a $\lambda\sigma$-closed set X is defined over C if it is defined by positive Δ-formulas with parameters in C. If X is defined over $C = \mathrm{acl}_\sigma(C)$, and $a \in X$, we say that a is a generic of X over C if X is the smallest $\lambda\sigma$-closed set defined over C and containing a. By the saturation of K, any (non-empty) irreducible $\lambda\sigma$-closed set has a generic.

If H is an ∞-Δ-definable subgroup of $G(K)$, then H is $\lambda\sigma$-closed, and H is the intersection of definable $\lambda\sigma$-closed subgroups of $G(K)$. Indeed, $H = \bigcap_n \psi_n^{-1}(\tilde{H}_n)$, where $\tilde{H}_n$ is the σ-closure of $\psi_n(H)$ in $G_n(K)$. We define the connected component H^0 of H as the intersection of all $\lambda\sigma$-closed subgroups of H of finite index in H. Then H^0 is irreducible. Indeed, if H^0 is not irreducible, then for some n the σ-closure $\tilde{H}_n^0$ of $\psi_n(H^0)$ is not irreducible in the σ-topology. Since the σ-topology is Noetherian, $\tilde{H}_n^0$ has a σ-closed proper

subgroup of finite index H', and $\psi_n^{-1}(H') \cap H^0$ is then a proper $\lambda\sigma$-closed subgroup of H^0 of finite index in H^0.

Note that if H is defined over $A = \mathrm{acl}_\sigma(A) \supseteq E$, then so are the groups $\tilde{H}_n$ and $\tilde{H}_n^0$, and therefore so is H^0. Moreover, $[\tilde{H}_n : \tilde{H}_n^0] < \infty$, and by elimination of imaginaries, this implies that all cosets of $\tilde{H}_n^0$ in $\tilde{H}_n$ are defined over A. Hence all cosets of H^0 in H are defined over A.

The proof of the theorem follows the line of the classical proof, using the $\lambda\sigma$-topology. Let a be a tuple in S^0, let $E \subseteq A = \mathrm{acl}_\sigma(A) \subseteq K$, and let X be the $\lambda\sigma$-closure of the set of realisations of the quantifier-free type of a over A. We will show that $X = Ha$, where H is an ∞-definable subgroup of S, and that H is defined over E.

By definition, X is $\lambda\sigma$-closed, defined over A, and is an irreducible $\lambda\sigma$-closed set, since $A = \mathrm{acl}_\sigma(A)$. Let $H = \{g \in S \mid gX = X\}$. Then H is a $\lambda\sigma$-closed subgroup of S, and $Ha \subseteq X$, by the definition of H.

Let $g \in S$ be a generic of S^0 over $A \cup a$. Then $b = ga$ is independent from a over A. [Proof: If V is a basic $\lambda\sigma$-closed set defined over $\mathrm{acl}_\sigma(A, a)$ and containing b, then Va^{-1} contains g, and therefore also S^0, and is defined over A. Hence V contains S^0a, and this shows that b is a generic of S^0a over $A \cup a$; as S^0a is defined over $A = \mathrm{acl}_\sigma(A)$, this implies that b is independent from a over A.] Consider the $\lambda\sigma$-closed set $Y = gX$. Then b is a generic of Y over $A \cup g$.

Claim. *The fields of definition of Y and of gH have the same algebraic closure over A.*

Let τ be an automorphism of (K, σ) which fixes A. Then $\tau(X) = X$ and $\tau(H) = H$, as X is defined over A; hence $\tau(Y) = Y$ if and only if $\tau(gX) = gX$ if and only if $\tau(g)X = gX$ if and only if $g^{-1}\tau(g) \in H$ if and only if $\tau(gH) = gH$. Let $C_1 = \mathrm{acl}_\sigma(C_1)$, resp. $C_2 = \mathrm{acl}_\sigma(C_2)$, be the smallest algebraically closed subsets of K containing A over which Y, resp. gH, is defined. Assume $C_1 \not\subseteq C_2$. By (3.6)(5), there is some A-automorphism τ of (K, σ) which fixes C_2 and moves C_1; then $\tau(Y) \neq Y$ and $\tau(gH) = gH$, which gives us a contradiction. Similarly, we cannot have $C_2 \not\subseteq C_1$, and therefore $C_1 = C_2 = C$.

Note that b is a generic of Y over $A \cup g$, and Y is defined over C and over $A \cup g$. This implies that b and g are independent over C, and that $C \subseteq \mathrm{acl}_\sigma(A, b) \cap \mathrm{acl}_\sigma(A, g)$. (Here we are using the fact that modularity is preserved under addition of constants.)

From the independence of a and b over A, we deduce that a is independent from b over C, and therefore the set of realisations of $\mathrm{qftp}(a/C, b)$ is dense in X. Note that if a' realises $\mathrm{qftp}(a/C, b)$, then ba'^{-1} realises $\mathrm{qftp}(g/C, b)$, and is therefore an element of gH. Since gH is $\lambda\sigma$-closed, this implies that $bX^{-1} \subseteq gH$. From $Ha \subseteq X$ we deduce that

$$b(a^{-1}H) \subseteq bX^{-1} \subseteq gH,$$

and therefore that $bX^{-1} = gH$, and $X = Ha$.

The proof of the theorem now follows by compactness. We may assume that U is defined by positive quantifier-free formulas. If $a \in U$, then $Ha \subseteq U$, and this implies that $H'a \subseteq U$ for some quantifier-free definable subgroup H' of $G(K)$ containing H. Thus $U \cap S$ is a finite union of translates of quantifier-free definable subgroups of S.

REMARK. In the particular case that the subgroup S is contained in $G(K^{p^\infty})$, there is a direct proof of this result. By (4.7), $S = G(K^{p^\infty}) \cap S'$, where S' is ∞-definable in the language $\mathcal{L}_\sigma$. As any descending sequence of σ-closed subsets of a difference field stabilises, this implies that S is a quantifier-free definable subgroup of the difference field (K^{p^∞}, σ). Hence, by (4.6) the results of [CHP] apply and give us the desired conclusion.

(5.12) An example and some questions. The criterion for modularity given in (5.6) is very impractical. Even in simple cases, it is quite difficult to determine whether a set is modular or not. We will illustrate this with an example. Assume $p \neq 2$, and consider the subgroup S of $\mathbb{G}_m(K)$ defined by $\sigma(x) = x^2$. We do not know whether this group is modular (but we conjecture that it is).

The "generic" of S is the type specifying that $\sigma(x) = x^2$ and that for each $n \in \mathbb{N}$, the elements $\lambda_\mu(B; x)$, $\mu \in I(B)^n$, are algebraically independent. At the other extreme, we have the type $\sigma(x) = x^2 \wedge x \in K^{p^\infty}$. The set of its realisations is the group $\mathbb{G}_m(K^{p^\infty}) \cap S$, which is modular by (7.4) in [CHP] (since the multiplicity of x over $\sigma^n(x)$ is 2^n, and hence unbounded).

In order to prove that S is modular, one needs to solve the following problem: Let $a \in S$, let $E = \mathrm{acl}_\sigma(E)$ contain a p-basis, and show that there is no element $b \in \mathrm{acl}_\sigma(E, a) \setminus E$ satisfying $\sigma^n(x) = x^{p^m}$ for some $n \geq 1$. In fact (see [CHP] (7.1)(2)), it suffices to show that there is no such b in the λ-closure of the field $E(a)$. From the equation $\sigma(a) = a^2$, we deduce equations relating the elements $\lambda_i(B; a)$, $i \in I(B)$, and the elements $\sigma(\lambda_i(B; a)) = \lambda_i(\sigma(B); a^2)$, $i \in I(B)$. However, determining which additional algebraic relations are allowed is quite complicated.

Of independent interest would be to describe the quantifier-free definable subgroups of S. The first difficulty here is to determine the quantifier-free $\mathcal{L}_\lambda$-definable subgroups of $\mathbb{G}_m(K)$. Note that these are λ-closed (i.e., defined by $\mathcal{L}_\lambda$-equations). Examples of such groups are the following: Let n be an integer, and $c_1, \ldots, c_m \in K$; then $K^{p^n}[c_1, \ldots, c_m]$ is a subfield of K definable in K, and all definable subfields of K are of this form (Messmer [Me]). Then $\mathbb{G}_m(K^{p^n}[c_1, \ldots, c_m])$ is a λ-closed definable subgroup of $\mathbb{G}_m(K)$. The first question we need to answer is the following: Is every λ-closed subgroup of $\mathbb{G}_m(K)$ of this form? Then one needs to investigate the λ-closed subgroups of $\mathbb{G}_m(K)^n$ for $n \in \mathbb{N}$ in order to describe the quantifier-free definable subgroups of S. Such a subgroup is defined by $(g, \sigma(g), \ldots, \sigma^{n-1}(g)) \in U$ for some n and λ-closed subgroup U of $\mathbb{G}_m(K)^n$.

References

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

[CH] Z. Chatzidakis and E. Hrushovski, *Model theory of difference fields*, Trans. Amer. Math. Soc. **351** (1999), 2997–3071.

[CHP] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, *Model theory of difference fields, II: Periodic ideals and the trichotomy in all characteristics*, preprint, 1999.

[CP] Z. Chatzidakis and A. Pillay, *Generic structures and simple theories*, Ann. Pure Appl. Logic **95** (1998), 71–92.

[C] R. M. Cohn, *Difference algebra*, Interscience Publishers, John Wiley & Sons, New York-London-Sydeny, 1965.

[D] F. Delon, *Idéaux et types sur les corps séparablement clos*, Mém. Soc. Math. France (N.S.) **33** (1988), 76 pp.

[DS] L. van den Dries and K. Schmidt, *Bounds in the theory of polynomial rings over fields. A nonstandard approach*, Invent. Math. **76** (1984), 77–91.

[E] Yu. Ershov, *Fields with a solvable theory (English translation)*, Sov. Math. Doklady **8** (1967), 575 – 576.

[FJ] M. D. Fried and M. Jarden, *Field arithmetic*, Springer-Verlag, Berlin, 1986.

[H] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, J. Amer. Math. Soc. **9** (1996), 667–690.

[K] H. Kikyo, *Model companions of theories with an automorphism*, J. Symbolic Logic **65** (2000), 1215–1222.

[KkP] H. Kikyo and A. Pillay, *The definable multiplicity property and generic automorphisms*, Ann. Pure Appl. Logic **106** (2000), 263–273.

[KP] B. Kim and A. Pillay, *Simple theories*, Joint AILA-KGS Model Theory Meeting (Florence, 1995), Ann. Pure Appl. Logic **88** (1997), 149–164,

[Ku] K. Zh. Kudaibergenov, *On the fixed field of a generic automorphism*, Siberian Adv. Math. **11** (2001), 25–34.

[L1] S. Lang, *Algebra*, second ed., Addison-Wesley, Reading, MA, 1984.

[L2] ———, *Introduction to algebraic geometry*, third printing, Addison-Wesley, Reading, Mass., 1972.

[L] D. Lascar, *Les beaux automorphismes*, Arch. Math. Logic **31** (1991), 55–68.

[M] A. Macintyre, *Generic automorphisms of fields*, Joint AILA-KGS Model Theory Meeting (Florence, 1995). Ann. Pure Appl. Logic **88** (1997), 165–180,

[Me] M. Messmer, *Groups and fields interpretable in separably closed fields*, Trans. Amer. Math. Soc. **344** (1994), 361–377.

[P] A. Pillay, talk given at MSRI, Spring 1998.

[W] C. Wood, *Notes on the stability of separably closed fields*, J. Symbolic Logic **44** (1979), 412–416.

UFR de Mathématiques, Université Paris 7, Case 7012, 2, place Jussieu, 75251 Paris Cedex 05, FRANCE

E-mail address: zoe@logique.jussieu.fr