TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 351, Number 8, Pages 2997–3071
S 0002-9947(99)02498-8
Article electronically published on April 8, 1999

MODEL THEORY OF DIFFERENCE FIELDS

ZOÉ CHATZIDAKIS AND EHUD HRUSHOVSKI

ABSTRACT. A difference field is a field with a distinguished automorphism σ. This paper studies the model theory of existentially closed difference fields. We introduce a dimension theory on formulas, and in particular on difference equations. We show that an arbitrary formula may be reduced into one-dimensional ones, and analyze the possible internal structures on the one-dimensional formulas when the characteristic is 0.

INTRODUCTION

A *difference field* is a field $(K, +, \cdot)$ together with a distinguished field automorphism σ. This is the algebraic structure appropriate for studying finite difference equations (on which abundant classical literature exists). The basic algebra of difference fields is described in [5]. Here we propose to describe their basic model theory. Our guides are Robinson's theory of model companions, Shelah's stability theory, and Zilber's "geometric stability theory". Using these tools we will give a description of the rough geometry of "varieties" defined by difference equations. We will find that certain equations matter more than others, describe them, and show how to reduce an arbitrary equation to the fundamental ones (a reduction sometimes involving a Galois theory).

Universal domains and quantifiers. Every difference field embeds in a *universal domain* $(\mathcal{U}, +, \cdot, \sigma)$. $\mathcal{U}$ is algebraically closed as a field, and has the following universality property:

Let $\mathcal{U}_0$ be the restriction of $\mathcal{U}$ to the algebraic closure of the prime field. For any "small" difference field L, algebraically closed as a field, and any map $h : \mathcal{U}_0 \to L$ of difference fields, there exists a map $f : L \to \mathcal{U}$ with $fh = Id_{\mathcal{U}_0}$. Further, f is unique up to conjugation by an element of $\mathrm{Aut}(\mathcal{U})$.

The model companion of difference fields, particularly in connection with Conjecture (1.14)(1), was discussed at MSRI by L. van den Dries, A. Macintyre and C. Wood in 1989-90. A report on this work and other issues can be found in Macintyre's paper [23]; here we give a more geometric description of the universal domains $\mathcal{U}$. These universal domains are the appropriate (initial) setting for the study of the geometry of sets defined by difference equations, playing the same role as algebraically closed fields in algebraic geometry. In particular, there is a bijective correspondence between prime difference ideals over $\mathcal{U}$ (consisting of difference equations in n variables) and irreducible difference varieties (their zero sets in $\mathcal{U}^n$).

Received by the editors August 14, 1996.
1991 *Mathematics Subject Classification.* Primary 03C60; Secondary 03C45, 08A35, 12H10.
Key words and phrases. Model theory applied to algebra, difference fields.
The second author was supported by NSF grants DMS 9106711 and 9400894.

So far the state of affairs is the same as in algebraic or differential-algebraic geometry. There is however a subtle difference. In algebraic geometry, every definable set is a Boolean combination of varieties (Tarski-Seidenberg); the same is true in differential algebra, for differential varieties (Robinson). The analog for difference varieties is false: one must consider the behavior of the automorphism not only on the function field of a given variety, but also on finite extensions. But it is not necessary to go too much further: a basic difference-definable subset of an algebraic variety X is the projection to X of a difference subvariety of V, where $V \to X$ is étale. This small difference gives the entire subject its particular flavor.

The above is explained in §1. We also take a look in this section at some of the basic model theoretic notions, in the case of difference fields. In particular, one can in general define the fundamental operations of *definable closure* and *algebraic closure* using the automorphism group of the universal domain $\mathcal{U}$:

An element is *definable* over a set B ($a \in dcl(B)$) if every automorphism of $\mathcal{U}$ fixing B also fixes a; it is *algebraic* over B ($a \in acl(B)$) if its orbit under $Aut(\mathcal{U}/B)$ is finite.

We show that a substructure of $\mathcal{U}$ is algebraically closed iff it is algebraically closed as a field. Definable closure is somewhat more delicate.

In addition, we show how to take quotients of definable sets by definable equivalence relations - "elimination of imaginaries" - and discuss some corollaries for pseudo-finite fields.

An intriguing conjectural connection with the Frobenius automorphisms is also discussed, though it is not directly relevant to the present paper.

(In)stability. In the beginning of stability theory, Shelah showed how to view a single formula $\phi(x, y)$ as a relation between two definable sets D_1, D_2. Let $B_a = \{b \in D_2 : \phi(a, b)\}$. Shelah identified three quite different kinds of behavior:

1) "Order property": Different sets B_a can be nested, or contained in each other; this happens when one has a definable ordering, such as in $(\mathbb{R}, +, \times)$, when $D_1 = D_2 = \mathbb{R}$ and the relation ϕ is $<$. This phenomenon does not occur in difference fields, and will not concern us in the present paper. (Though a similar case study for a rich theory with order should be of great value.)

2) "Independence property": For arbitrarily large finite sets $F \subset D_1$, for any distinct $a_1, \ldots, a_n, b_1, \ldots, b_m \in F$,

$$\bigcap_i B_{a_i} \cap \bigcap_j (D_2 \setminus B_{b_j}) \neq \emptyset.$$

3) Stability: neither of the above occurs. In this case (perhaps after a fixed finite partition of D_2), one shows that the sets B_a can be sharply divided into "small" and "large" ones; any finite collection of "large" sets has non-empty intersection, not contained in any finite union of "small" sets. In other words there is a single "generic" behavior for the points of D_2; a generic point is one that lies in each "large" set, but outside each "small" set, from a given collection.

For algebraically closed fields, every formula is equivalent to a quantifier-free one, and all quantifier-free formulas in the language of fields are stable: if D_2 above is an irreducible variety , then each set B_a is either contained in a proper subvariety ("small"), or contains a Zariski open subset (hence is "large"). On the other hand, let $(\mathcal{U}, +, \cdot, \sigma)$ be a universal domain for difference fields; let k be the fixed field for σ. Then k is a pseudo-finite field, and one has a well-known example of an

independent family ([8]):

$$D_1 = D_2 = k; \quad \phi(x, y) = (\exists t \in k)(t^2 = y - x).$$

Here $B_a = a + k^2$.

In particular, difference fields are unstable.

One of the surprises of the present paper is the discovery that such effects, occurring inside the fixed field, are the only sources of instability in difference fields of characteristic zero. (This will be an outcome of the full theory; it is false in positive characteristic.) In any event, we must initially work without the benefit of existing results in stability theory.

Simple unstable theories. Difference fields fall into a class of theories identified in [34], called "simple unstable theories" there. While a great body of technology was created in the 70's and 80's to analyze stable theories, simple unstable theories remained in the rudimentary state achieved in [34].

Such theories were encountered again (in the $\aleph_0$-categorical context) in [4] (see also [15], [19], [20]). It became clear that much of stability theory has analogs for at least some classes of unstable structures of this type. In particular, a theory of (finite) dimension and a theory of independence were developed (this is discussed further below). The "uniqueness of non-forking extensions" familiar from stability theory no longer holds, but an adequate replacement was found ("the independence theorem", see below.). Two contacts with stability were found, that deserve mention here; both are closer than a mere analogy.

1) The fundamental geometries of [4] all have an underlying stable structure, to which is added an unstable "coloring"; e.g. a vector space, with a quadratic form. The dependence structure comes entirely from the stable reduct; the unstable coloring is compatible with it, in each dimension, but does not itself contribute to the dimension theory. In particular, dependence is controlled by stable formulas. Somewhat later it was found that this is a general feature of finite rank ("S_1-rank") simple unstable theories. Quite recently, this was generalized to arbitrary simple unstable theories by [21] and [22]. In the difference field context, this is reflected in the fact that dependence can be understood in terms of the underlying field structure: two substructures are independent iff they are independent as fields.

2) Stability has a consequence for definable subsets of a structure, viewed as (relativized) structures in their own right. They are *stably embedded*; this means that every relation on the smaller structure, definable externally in the bigger one, is already definable using parameters in the smaller structure. It was realized that this notion has great significance outside the stable context; in particular it makes sense to consider substructures as coordinatizing geometries only if they are stably embedded. A review of this notion is included in an Appendix.

Motivated by this class of theories and by pseudo-finite fields, and more generally "PAC structures", a theory of definable groups was also worked out; part of it appears in [19].

The present paper uses these ideas, and indeed generalizations of much wider parts of stability and superstability. Given the state of the literature on simple unstable theories (the above survey was exhaustive), we must alternate between proving general results, and applying them in our context. While greatly aided by the conception of how things should be in such theories, we present the results for difference fields, and make no effort to achieve the highest possible generality;

sometimes we use as a crutch the presence of an ambient stable structure even when we could avoid it. Some results of a more general nature are collected in §7.

For most of the paper, no previous knowledge of stability is assumed, though we will continue to refer to it in general terms in the introduction.

Independence theorem. The first fundamental notion of stability is *independence* of two substructures, or of elements over a given substructure. (For fields, independence is algebraic independence; for differential fields, independence is the absence of a differential algebraic relation among elements.)

In the stable regime, a uniqueness theorem holds:

If two substructures A_1,A_2 are independent over an algebraically closed base B, and C is the substructure generated by A_1, A_2, then the isomorphism type of C (over A_1 and A_2) is uniquely determined.

(This is another aspect of the existence of a unique "generic" behavior, noted above at the level of a single formula.) This uniqueness is characteristic of stable theories. The replacement, which makes everything work for simple theories of finite rank, is the "independence theorem", stating that any coherent triple of possible isomorphism types of independent pairs (A_i, A_j) can be simultaneously realized.

Assume given substructures B,A_1,A_2,A_3,A_{12},A_{13},A_{23}, with B algebraically closed, and maps: $g_i : B \to A_i$ and $g_{ij} : B \to A_{ij}$, and $h_{ij} : A_i \to A_{ij}$, $h_{ji} : A_j \to A_{ij}$ $(i < j)$, with $g_{ij} = h_{ij}g_i$ for $i \neq j$.

If $h_{ij}(A_i), h_{ji}(A_j)$ are independent over $g_{ij}(B)$, there exist embeddings $f_{ij} : A_{ij} \to \mathcal{U}$ $(i < j)$ with

$$f_{ij}h_{ij} = f_{ik}h_{ik}.$$

Furthermore, the $f_{ij}h_{ij}(A_i)$ are independent over $f_{ij}g_{ij}(B)$.

Dimension theories. The appropriate dimension theories (traditionally gateways to stability) are developed in §2. A set is one-dimensional if it cannot be split into infinitely many definable subsets with pairwise finite intersections, and forming part of a single definable family of definable subsets. Even in superstable theories of finite rank, the intuitive notion of dimension splits technically into a number of somewhat distinct notions, due mostly to difficulties with "definability". Here too we use one notion of rank for definable sets (S_1-rank), and another more adapted to types (U-rank, called here SU-rank to avoid suggesting the theory is superstable). The dimension, or rank, of the set of solutions of $f(X, \sigma X, \dots, \sigma^m X) = 0$ (where f is a non-zero polynomial and X a single variable) is in any event bounded by m, but may be smaller. Sometimes we use the "degree" (m) itself; this is a straightforward invariant of a difference equation varying well in families, but less directly related to the geometry of the definable sets. In the rest of the introduction, we will not be precise about which dimension we use; sometimes a proof is given in terms of one, but works equally well for another.

Given the notion of dimension, one can define *independence*: Let $B_1 \subset B_2 \subset \mathcal{U}$ be substructures (i.e., subfields closed under σ and σ^{-1}). Let $rk(a/B)$ be the least integer d such that a lies in some B-definable set of dimension d. An element (or tuple) a is independent from B_2 over B_1 if $rk(a/B_2) = rk(a/B_1)$. Thus there is no substantially sharper description of a from the vantage point of B_2, over that of B_1. The independence theorem then follows from the type of dimension theory (S_1) used. We will however proceed in the opposite direction, first proving a generalized independence theorem (1.9), and then deducing the dimension theory in §2.

Also in §2, the nature of complete types (orbits of tuples under $Aut(\mathcal{U})$) is made explicit. Let B be an algebraically closed substructure of $\mathcal{U}$, a an element or tuple. Let $B(a)_\sigma$ be the substructure generated by $B \cup a$. The type of a over B is determined by the isomorphism type over B of $B(a)_\sigma^{alg}$ (this is equivalent to the quantifier elimination mentioned above). Moreover, it suffices to consider the isomorphism type over B of the union of all *finite* σ-invariant extensions of $B(a)_\sigma$ (2.8).

Traditionally in model theory, one considers either formulas or complete types. Here we find it necessary to use an intermediate object, "semi-types". With the above notation, this refers to the isomorphism type over B of a fixed finite σ-invariant extension of $B(a)_\sigma$.

This notion allows a curious version of the definability lemma of stability. Let $\phi(x, y)$ be a formula, $p(x)$ a type over B. Let $(d_p x)\phi(x, y)$ denote $\{b$: $\phi(a, b)$ holds for some a independent from b over B, and realizing $p\}$. In stable theories, $d_p\phi$ is itself equivalent to a formula. Here we show that if p is a complete type, $(d_p x)\phi(x, y)$ is given by a semi-type; while if p is a semi-type, $(d_p x)\phi(x, y)$ is a formula. This sometimes permits a two-stage argument, reducing from types to semi-types to definable sets. We don't know how to place this phenomenon within the general model theory of simple unstable theories.

Coordinatization by one-dimensional types. The key idea of Shelah's superstability theory is the existence of certain fundamental geometries within a given superstable structure; many properties have a "local-global" nature, holding true of the full structure iff they hold for each such fundamental geometry ("regular type"). Lascar showed that in finite dimensions, one can restrict attention to types of rank one. Difference fields (with a single difference operator) have "rank ω"; so excepting one ("generic") geometry, one expects the fundamental geometries to have dimension one. On each one-dimensional definable set, algebraic closure defines a combinatorial pregeometry (matroid, dependence relation).

In §3 it is shown that there are enough one-dimensional sets to control arbitrary types; see (3.4). In characteristic zero, using the trichotomy, the statement can be made in the following simpler form (cf. (4.12)):

Let B be a "sufficiently large" substructure of $\mathcal{U}$, $a \notin B$ with $rk(a/B)$ finite. Then there exists $b \in acl(B, a)$ with $rk(b/B) = 1$.

An elementary submodel is "sufficiently large". When the base B is arbitrary (a situation that must be considered if the construction is to be iterated), the situation is more complicated.

The conclusion remains the same if the geometry of the relevant one-dimensional type is simple enough ("modular"; see below). Later we will see that there is essentially only one exception to modularity: the fixed field k.

Stronger statements of this type will be proved in §5. Meanwhile we have sufficient motivation to embark on a classification of the one-dimensional sets. This will be done in §4; surprisingly, the coordinatization results of §3 will be needed there, for an inductive argument. Another result proved in §3 for this purpose (3.2) is that geometrically non-trivial types (see below) are essentially captured by a definable set. This generalizes a result from [11] in the superstable case, using the weak definability lemma mentioned above.

Zilber's Trichotomy. Zilber proposed a classification of the one-dimensional structures in the stable context, into three kinds. The idea is that after all possible reductions are made, the possible stable geometries (of finite dimension) are degenerate, or a form of linear algebra, or of classical algebraic geometry. This trichotomy is known to be very powerful; it does not hold for arbitrary structures of finite Morley rank, but when it does hold it settles essentially all fundamental issues concerning their model theory. On the other hand, it is expected to have validity in unstable domains. It has been shown to hold if the dimension theory is compatible with a Noetherian topology, and satisfies certain additional ("smoothness") axioms regarding intersections of closed sets. Our structures do not have finite Morley rank, nor do they satisfy the smoothness axioms, but we show the trichotomy holds nevertheless.

1. D is *geometrically trivial* if the associated matroid is trivial; equivalently, $acl(A \cup B) = acl(A) \cup acl(B)$ for subsets A, B of D. These turn out to be the sets we know least about; but at least we know there is no complicated geometry of definable sets on D^m. Many model theoretic questions, notably questions of coordinatizability, become simple for trivial types.

2. D is *module-like*, or *modular non-trivial*, if it is not geometrically trivial, and the lattice of algebraically closed sets of D (including imaginary elements) satisfies the modular law. The fundamental example is a vector space V over a division ring D, with structure on V consisting of the subsets of V^m defined by *linear* equations. One can show that such a set is equivalent to one with a definable group structure. If $(A, +, 0)$ is stable and modular, then ([18]) every definable subset of A^m is a finite Boolean combination of definable subgroups.

3. D is *field-like*; it interprets, and is interpreted in, an algebraically closed field.

The central result of §4, and of the paper, is the proof of this trichotomy for one-dimensional sets definable by difference formulas. We conjecture that the trichotomy is true in all characteristics, but can only prove it in characteristic 0.[1] Naturally, since we are not in the stable context, "algebraically closed" in (3) must be modified, and replaced with "pseudo-finite". In characteristic 0, the only definable pseudo-finite field is k (in characteristic $p > 0$, one has "twisted constant fields" also). Combined with the results of §3, the theorem can be stated as follows. By a surjective multi-valued map $f : E \to D$ we mean a pair of definable maps $j : E' \to E$, $f' : E' \to D$, with j finite-to-one and surjective, and f' surjective. (Think of "$f'j^{-1}$".)

Theorem. *Let $\mathcal{U}$ be a universal domain for difference fields of characteristic 0, B an algebraically closed substructure, E a set defined by a complete type (or semi-type) over B.*

There exist a definable set D over B, and a definable surjective multi-valued map $f : E \to D$. D is one-dimensional, and either geometrically trivial, or module-like, or equal to k.

(Cf. Theorems (3.4), (4.5) and (4.8).) By applying the theorem successively to E, to the fibers of f, etc., one obtains an "analysis" of E in finitely many steps in terms of one-dimensional sets; cf. (5.5).

[1]The conjecture is indeed true, and can be proved by the methods discussed below; see a forthcoming paper by Chatzidakis, Hrushovski and Peterzil

The map f need *not* be defined over B; this will be studied later (§5). In terms of equations, one can roughly rephrase this as follows: any non-trivial difference equation can be reduced by a change of variable to a difference equation of dimension one, of one of the three special types. In terms of field extensions: any algebraically closed difference field L properly extending $\mathcal{U}$ either has a point $a \in L \setminus \mathcal{U}$ with $\sigma(a) = a$, or else contains a new point of a one-dimensional module-like or geometrically trivial definable set.

We were surprised to find that all the one-dimensional sets of types (1) and (2) are actually stable (this appears to be an accident of characteristic 0). Thus the structure result for modular stable one-dimensional sets applies directly.

It is not difficult to classify the one-dimensional module-like definable sets; see (5.12). A rather typical example: let A be the multiplicative group, written additively, or a simple Abelian variety defined over k; and let $D = \{a \in A : \sigma(a) = 2a\}$. All one-dimensional module-like definable sets involve in a similar way Abelian varieties whose isogeny class is fixed by σ, or the multiplicative group $\mathbb{G}_m$.

We know less about the first type, geometrically trivial equations. In §6 we offer an example related to modular curves (showing they need not have Morley rank).

The proof of the trichotomy involves finding geometric dividing lines, which turn out to be equivalent to model theoretic properties of the difference equation. Observe that any difference equation $f(X, \sigma(X), \ldots, \sigma^m(X)) = 0$ implies difference equations involving σ^l, and not otherwise mentioning σ. For instance the equation $\sigma(X) = g(X)$ implies $\sigma^2(X) = g^\sigma(g(X))$. These "iterates" play an important role. (See the text for more precise definitions.)

For degree one equations, the first dichotomy is this:

Do the "iterates", the implied equations for σ^m, have unbounded degree?

If they do not, we show that the equation is equivalent to $\sigma(x) = x$, after a (difference-algebraic) change of variable. If they do, we show that the solution set E is a stable and stably embedded structure within $\mathcal{U}$.

For higher degree equations, the situation is a bit more complicated. We consider only irreducible equations (model theoretic dimension one, as explained above). Nonetheless the iterated equation, regarding the automorphism $\tau = \sigma^m$, may be reducible. In this case we move over to the reduct $\mathcal{U}[m] = (\mathcal{U}, +, \cdot, \tau)$, and apply the results of §3, and induction. (One cannot resist remarking on the following intriguing phenomenon: let E be the set defined by the original equation, and let $E[m]$ be the set defined by the "iterated" equation in the reduct $(\mathcal{U}, +, \cdot, \tau)$. Then $E[m]$ is better behaved because it has *more* structure than E. For instance if the equation is $\sigma(x) = f(x)$ as above, then there may be varieties inducing non-trivial relations on $E[2]$, but not on E; at the same time the relation σ on E is not lost - it coincides with f. Thus paradoxically, having started with a reduct, one faces an expansion, and the behavior of the induced structure improves with the expansion (i.e. with more divisible m). It is possible that a good understanding of this behavior will lead to a proof of the trichotomy in positive characteristic.)

Suppose finally that we have an equation of degree $m > 1$, all of whose iterates remain one-dimensional (in the appropriate reduct). We then show that the solution set E is stable and stably embedded. The idea is this: we would like to show that there are few definable subsets of E. E lies on some variety V, and we know that definable subsets of E come from projections of difference-subvarieties of finite covers $\tilde{V}$ of V. Now we look at the ramification locus R of $\tilde{V}$ over V. This locus is canonical, and we can expect σ to "respect" it (in an appropriate sense). This need

not happen, and $R \cap E$ may be finite; but one shows that for some m, $R \cap E[m]$ is Zariski dense in R. Since R is a smaller-dimensional variety than V, we obtain a contradiction. Thus we show roughly that the covers yielding definable subsets of E have controlled ramification; this implies that they are themselves under control (in characteristic 0).

Modularity is now obtained via a Galois-theoretic criterion, implicit in earlier work, that we now make explicit. The following criterion can easily be modified to become equivalent to modularity.

A stable, one-dimensional set is modular if "algebraic closure agrees with definable closure after projectivization": whenever $a \in acl(b_1, \ldots, b_n)$, there exist a' depending on a, and b'_i depending on b_i, such that $a' \in dcl(b'_1, \ldots, b'_n)$

This criterion is amenable to a geometric proof.

Analysis of finite dimensional types. We wish to have a version of the trichotomy theorem where all the maps are defined over the given base set. In this case one can consider the fibers of the "coordinatizing" maps, and apply the theorem to them, iteratively. The key notion is that of *internality*. We do not treat it systematically, since the only case of importance in characteristic 0 difference fields is that of definable sets *internal to* k. By definition, this means that there exists a definable bijection between the given definable set and a definable subset of k^n. This bijection may not be defined over a given base structure. However, there is a good Galois theory to explain this, analogous to the Lie-Kolchin Galois theory for differential equations (5.11). Here (unlike the case in stable theories) the Galois group need not quite act by automorphisms; it may not preserve some quantified formulas; however the superstructure associated with dependence will be preserved.

Using this notion, the trichotomy theorem can be stated over a fixed substructure. We state it this time for a complete type, though a version for definable sets exists as before. If D is a one-dimensional modular set, let $G_m(D)$ (the Grassmannian) be the set of m-element subsets of D. (k-internal types can be considered as complicated Grassmannians related to k).

Let E be the solution set of a complete type over an algebraically closed substructure B. Then there exist a B-definable set D, either a Grassmannian over a one-dimensional modular type, or else k-internal, and a B-definable non-constant map $f : E \to D$.

One can then analyze E in finitely many steps, by further breaking up the fibers of f using different Grassmannians. These and related results are contained in §5.

§6 contains a number of examples, demonstrating the general results and outlining their limits. We start with a detailed study of the equation $\sigma(x) = x^2 + b$ (which we were not able to deal with before developing the general methods of this paper!). We show that the model theoretic dimensions can "jump", by giving a family of equations whose generic element is one-dimensional, but such that a countable infinity of special values yield two-dimensional equations. A family of examples of difference Galois groups answers a question of Poizat's. A simple pair of coupled equations shows that instability need not "lie on the surface" of a type of dimension > 1, but that the analysis of §5 may be needed to uncover it. A geometrically trivial equation need not have Morley rank (though it is superstable); searching for the example led us to consider modular curves. Finally we exhibit an unstable type one-dimensional type orthogonal to all fields, in characteristic p;

we presume this type is modular. We hope that this will be the beginning of a structure theory in positive characteristic.

§7 gives some results on definable groups, and the Appendix gives a review of stable embeddability.

The authors wish to thank Anand Pillay for his careful reading of the manuscript and pointing out inaccuracies in the early version of the paper. They also thank the referee and the editor for their thorough and helpful comments.

0. Preliminaries on difference fields

The results given in this section are basic results on difference fields; all the references are to results in R. Cohn's book [5].

A difference ring is a ring A together with a ring isomorphism $\sigma : R \to R$ (not necessarily onto); if σ is onto, R is *inversive*. There is a unique (up to R-isomorphism) inversive closure of R, i.e., an extension (R^*, σ^*) of (R, σ) which is inversive and smallest such [2.5.2]. **All our difference fields will be inversive**.

For K a difference field and $X = (X_1, \dots, X_n)$, we define the difference polynomial ring over K, $K\langle X\rangle$, to be the difference ring whose underlying ring is the polynomial ring $K[X_1, \dots, X_n, \sigma(X_1), \dots, \sigma(X_n), \sigma^2(X_1), \dots]$ in the variables $\sigma^i(X_j)$, $i \in \mathbb{N}$, $j = 1, \dots, n$; σ is extended to $K\langle X\rangle$ in the manner suggested by the names of the variables. By abuse of language, we view $f(X, \dots, \sigma^k(X))$ both as a difference polynomial in the variable X and as an ordinary polynomial in the variables $X, \dots, \sigma^k(X)$.

There is a natural notion of σ-ideal of a difference ring R, i.e., an ideal closed under σ. If the ideal contains a whenever it contains $\sigma(a)$, it is called a *reflexive* σ-ideal; the quotient of an inversive difference ring by a reflexive σ-ideal is then an inversive difference ring.

Many of the results on polynomial rings have analogs in difference polynomial rings, sometimes with differences: $K\langle X\rangle$ is not noetherian (consider the σ-ideal generated by $X_1\sigma(X_1), X_1\sigma^2(X_1), \dots, X_1\sigma^k(X_1), \dots$); but it satisfies the ascending chain condition on prime σ-ideals and even on perfect σ-ideals [3.8.5] (I is perfect if whenever a product of transforms of a is in I, then $a \in I$); every perfect σ-ideal is an intersection of finitely many prime σ-ideals [3.5.4]. Under some mild assumptions on K, every prime σ-ideal of $K\langle X\rangle$ is generated (as a perfect σ-ideal) by $n + 1$ difference polynomials [8.20.13].

Let $K \subseteq L$ be two difference fields, and let a be a tuple from L; we denote by $K(a)_\sigma$ the field $K(\sigma^k(a))_{k\in\mathbb{Z}}$, and we say that it is generated by a; a subextension of a difference field finitely generated over K is itself finitely generated [5.23.18]. Assume that $L = K(a)_\sigma$; we define $deg_\sigma(L/K)$, or sometimes $deg_\sigma(a/K)$, to be the transcendence degree of L over K; if it is finite and a is a finite tuple, we define another invariant of L/K, called the limit degree of L over K, $ld(L/K)$, as follows: from some point on the integers $d_k = [K(a, \dots, \sigma^k(a)) : K(a, \dots, \sigma^{k-1}(a))]$ are finite and equal to each other [5.16]; we define $ld(L/K)$ to be this eventual value of the d_k's. It does not depend on the choice of the generators a. Similarly we define the inverse limit degree of L over K, $ild(L/K)$, to be the eventual value of $[K(a, \dots, \sigma^{-k}(a)) : K(a, \dots, \sigma^{-k+1}(a))]$. Moreover, these limit degrees are multiplicative in towers [5.17.2].

Another result of importance is a primitive element theorem for finitely generated extensions of finite degree: assume in addition that $K(a, \dots, \sigma^k(a))$ is a

(finite) separable extension of $K(a, \dots, \sigma^{k-1}(a))$ and $K(a, \dots, \sigma^{-k}(a))$ is a separable extension of $K(a, \dots, \sigma^{-k+1}(a))$ for k large enough; then $L = K(b)_\sigma$ for b a single element from L [7.5.3]. This will be used in the examples.

Conventions, notation, definitions. Unless otherwise specified, all the fields considered are inversive difference fields, and morphisms are σ-morphisms. We say that a subset E of a field K is a substructure if it is a subfield closed under σ and σ^{-1}; given $E \subseteq K$ we define $cl_\sigma(E)$ as the perfect closure of the smallest difference subfield of K containing E; E^s denotes the separable closure of E, and $G(E) = \mathcal{G}al(E^s/E)$ the absolute Galois group of E; E^{alg} denotes the (field-theoretic) algebraic closure of E, and $acl_\sigma(E)$ is $cl_\sigma(E)^{alg}$. We denote by $acl(E)$ and $dcl(E)$ the model-theoretic algebraic and definable closures.

We call a subfield algebraically closed if the underlying (pure) field is algebraically closed; an algebraically closed substructure is then an algebraically closed subfield which is stable under σ, σ^{-1}.

The letters x and a denote tuples (usually of finite length) of variables and elements; we explicitly mention when they have length 1.

Let $E \subseteq K$ be difference fields, and $a \in K$; we define $I(a/E)$ to be the σ-ideal $\{f \in E\langle X\rangle \mid f(a) = 0\}$. It is always a prime σ-ideal, and therefore finitely generated as a perfect σ-ideal; if it is trivial, we say that a is *transformally transcendental over* E if a is a single element, and *transformally independent over* E if it is a tuple. We also have a natural notion of transformal transcendence basis of K over E.

Fix a and E. We write $qftp(a/E)$ for the quantifier-free type of a over E. We say that the formula $\varphi(x)$ *determines* $qftp(a/E)$ if it is a quantifier-free formula from $qftp(a/E)$ such that $I(a'/E) \supseteq I(a/E)$ whenever $\varphi(a')$ holds. Determining formulas always exist, since $I(a/E)$ is finitely generated as a perfect σ-ideal. We say that $p(x)$ is a *semi-type* of a if $p(x)$ is of the form $\exists y\, q(x, y)$, where $q(x, y) = qftp(a, b/E)$ for some $b \in acl_\sigma(Ea)$. Note that it can be made first-order, using the quantifier-free formula determining $qftp(b/Ea)$.

Let p and q be (maybe incomplete) types over A; we denote by $p \times q$ the partial type $p(x) \cup q(y) \cup \{$formulas expressing that x and y are independent over $A\}$; observe that if p and q are semi-types, so is $p \times q$. Similarly, $p^{(n)}$ denotes the type $p(x_1) \times p(x_2) \times \cdots \times p(x_n)$.

1. The theory ACFA

In this section, we present the general model-theoretic results concerning existentially closed difference fields. We think (1.9)–(1.13) are new, while the other results of this section were known (though unpublished at the time of this writing); see [23]. **All varieties are absolutely irreducible**.

(1.1). Let $ACFA$ be the theory axiomatised by the scheme of axioms expressing the following properties of the $\mathcal{L}$-structure (K, σ):

(i) σ is an automorphism of K.
(ii) K is an algebraically closed field.
(iii) For every variety U, every variety $V \subseteq U \times \sigma(U)$ projecting generically onto U and $\sigma(U)$, and every algebraic set W properly contained in V, there is $a \in U(K)$ such that $(a, \sigma(a)) \in V \setminus W$ (by $U(K)$ we denote the K-rational points of U; $\sigma(U)$ denotes the conjugate by σ of the variety U, i.e., $\sigma(U) = \{\sigma(a) \mid a \in U\}$).

Theorem. *Every difference field embeds in a model of $ACFA$; $ACFA$ is model-complete.*

Proof. Let us first remark that (iii) is first-order. The only issue is to quantify over irreducible varieties, which follows from classical statements (see [7] for a discussion and model-theoretic proof).

Since every difference field embeds in a difference field satisfying (i) and (ii), it suffices to show that for every algebraically closed difference field K, and sets U, V and W as in (iii), there is a difference field L extending K and containing a point $(a, \sigma(a))$ of $V \setminus W$.

Let (a, b) be a generic point of V (in some overfield of K), and let L be the algebraic closure of $K(a, b)$; then a is a generic point of U, b is a generic point of $\sigma(U)$, and $(a, b) \notin W$.

By definition of $\sigma(U)$, σ extends to an isomorphism from $K(a)$ onto $K(b)$ which sends a to b; this σ in turn extends to an automorphism of L.

We have shown that every difference field embeds in a model of $ACFA$; it now remains to show that $ACFA$ is model complete. Let $K \models ACFA$, and let $\varphi(x)$ be a quantifier free formula with parameters in K in the variables $x = (x_1, \dots, x_n)$ which has a solution a in some difference field L extending K. By definition, for some $k \in \mathbb{N}$, $\varphi(x)$ is of the form

$$\begin{aligned} f_1(x, \sigma(x), \dots, \sigma^k(x)) &= f_2(x, \sigma(x), \dots, \sigma^k(x)) \\ &= \dots = f_m(x, \sigma(x), \dots, \sigma^k(x)) = 0 \\ &\wedge\ g(x, \sigma(x), \dots, \sigma^k(x)) \neq 0, \end{aligned}$$

where the f_i's and g are polynomials with coefficients in K.

Let V be the affine K-variety in $2kn$-space of which a generic point is

$$(a, \sigma(a), \dots, \sigma^{k-1}(a), \sigma(a), \sigma^2(a), \dots, \sigma^k(a)),$$

and U the closure of its projection onto the first kn coordinates; then $V \subseteq U \times \sigma(U)$; if $(b_1, \dots, b_{2k}) \in V$, then $f_1(b_1, \dots, b_k, b_{2k}) = \dots = f_m(b_1, \dots, b_k, b_{2k}) = 0$. Let W be the algebraic subset of V consisting of the points such that

$$g(x_1, x_2, \dots, x_k, x_{2k}) = 0;$$

then U, V, W satisfy the hypotheses of (iii), i.e., $\varphi(x)$ is satisfiable in K.

Remarks. (1) Observe that as a corollary of the proof of the consistency of $ACFA$ we see that if E is a substructure of a model K of $ACFA$ and K_0 is the set of elements of K transformally algebraic over E (i.e., of finite degree over E), then $K_0 \prec K$.

(2) An alternate axiomatisation of $ACFA$ can be given, replacing (iii) by a scheme of axioms expressing that every prime σ-ideal has a K-rational zero. We believe this axiomatisation to be closer to the one given in [23].

(1.2) Proposition. *Let $K \models ACFA$, and let F be the subfield of K fixed by σ. Then F is pseudo-finite.*

Proof. By the results of Ax [1], we need to verify that F is perfect, has exactly one extension of degree n for each $n \in \mathbb{N}$, and is pseudo-algebraically closed, i.e., that every (absolutely irreducible) variety defined over F has an F-rational point.

By definition F is perfect; if U is a variety defined over F, take V to be the diagonal of $U \times \sigma(U) = U \times U$ and apply (iii) to show that U has an F-rational

point. Clearly $\sigma(F^{alg}) = F^{alg}$, and the Galois group $G(F)$ of F^{alg} over F is generated by σ and therefore pro-cyclic, i.e. F has at most one extension of each degree. To finish the proof it suffices to show that F has an extension of degree n for each positive n. Consider the following system:

$$\sigma^n(x) = x,\ \sigma(x) \neq x,\ \sigma^2(x) \neq x, \dots,\ \sigma^{n-1}(x) \neq x.$$

It has a solution in an extension of K: let $t_1, \dots, t_n$ be algebraically independent over K, and extend σ to $K(t_1, \dots, t_n)$ by setting $\sigma(t_i) = t_{i+1}$ for $i < n$ and $\sigma(t_n) = t_1$. It therefore has a solution a in K, which is algebraic of degree n over F, since it has exactly n conjugates over F.

(1.3) Theorem. *Let (K_1, σ_1) and (K_2, σ_2) be two models of ACFA, and E a common algebraically closed subfield on which σ_1 and σ_2 agree and define an automorphism. Then*

$$(K_1, \sigma_1) \equiv_E (K_2, \sigma_2).$$

Proof. Moving K_2 if necessary, we may assume that K_1 and K_2 are linearly disjoint over E. Then σ_1 and σ_2 extend to a unique automorphism σ of the composite L of the fields K_1 and K_2: since K_1 and K_2 are linearly disjoint over E, L is the field of quotients of $K_1 \otimes_E K_2$. Define $\sigma(c \otimes d) = \sigma_1(c) \otimes \sigma_2(d)$ for $c \in K_1$, $d \in K_2$, and extend to L; then (L, σ) embeds into a model M of $ACFA$. By model completeness, $K_i \prec M$, which gives the result.

(1.4) Corollary. *Let (K_1, σ_1), (K_2, σ_2) be models of ACFA of the same characteristic, and E the algebraic closure of the prime field. Then*

$$(K_1, \sigma_1) \equiv (K_2, \sigma_2) \iff (E, \sigma_1|_E) \simeq (E, \sigma_2|_E).$$

Proof. The right to left implication follows from (1.3); for the converse, embed K_1 and K_2 in a common elementary extension.

Hence the completions of $ACFA$ are obtained by specifying the characteristic and the action of σ on the algebraic closure of the prime field. We will denote by $ACFA_0$, $ACFA_p$ the theories obtained by adding to $ACFA$ the requirements $\mathrm{char}(K) = 0$, $\mathrm{char}(K) = p$.

(1.5) Corollary (Description of the types)**.** *Let E be a substructure of a model K of ACFA, and a, b tuples from K. Then $tp(a/E) = tp(b/E)$ if and only if there is an E-isomorphism φ between $acl_\sigma(E(a))$ and $acl_\sigma(E(b))$ sending a to b.*

Proof. The sufficiency is clear by (1.3). The necessity follows by embedding K in a sufficiently saturated elementary extension.

(1.6). (1.5) implies that every formula $\varphi(x)$ in the variables $x = (x_1, \dots, x_n)$ is equivalent modulo $ACFA$ to a disjunction of formulas of the form $\exists y\, \theta(x, y)$, where y is a single variable, θ is quantifier-free, and for every a, $\theta(a, b)$ implies that b is algebraic (in the pure field sense) over $a^\frown\sigma(a)^\frown \cdots ^\frown \sigma^m(a)$ for some $m \in \mathbb{N}$.

Moreover, (1.4) implies the decidability of the theories $ACFA$, $ACFA_0$ and $ACFA_p$. Indeed, for each finite Galois extension E of $\mathbb{Q}$, and each conjugacy class c of elements of $\mathcal{G}al(E/\mathbb{Q})$, let $\varphi_{E,c}$ be the sentence expressing that $\sigma|_E \in c$; for n and i relatively prime integers with $i < n$, let $\varphi_{n,i}$ be the sentence expressing that

σ sends a primitive n-th root ζ of 1 to ζ^i. Let θ be a sentence. By (1.4) we know that

$$ACFA_0 \vdash \ \theta \leftrightarrow \bigvee_i \varphi_{E,c_i}$$

for some finite Galois extension E of $\mathbb{Q}$ and conjugacy classes c_i of $\mathcal{G}al(E/\mathbb{Q})$. Moreover, a proof of this equivalence only requires finitely many statements about the characteristic, which implies that for some N, for every prime $p > N$, we have

$$ACFA_p \vdash \ \theta \leftrightarrow \bigvee_i \varphi_{E,c_i}.$$

Moreover, for each prime p, there are an integer $n(p)$ and a set $I(p)$ such that

$$ACFA_p \vdash \ \theta \leftrightarrow \bigvee_{i \in I(p)} \varphi_{n(p),i}.$$

Thus

$$ACFA \vdash \ \theta \leftrightarrow \Big(\bigwedge_{p>N} (p \neq 0) \wedge (\bigvee_i \varphi_{E,c_i}) \Big) \vee \Big(\bigvee_{p \leq N} (p = 0) \wedge \bigvee_{i \in I(p)} \varphi_{n(p),i} \Big).$$

Hence, $ACFA_0 \vdash \theta$ if and only if all the conjugacy classes of $\mathcal{G}al(E/\mathbb{Q})$ occur among the c_i's; $ACFA_p \vdash \theta$ if and only if $I(p)$ contains all $i < n(p)$ relatively prime to $n(p)$; and $ACFA \vdash \theta$ if and only if $ACFA_0 \vdash \theta$ and $ACFA_p \vdash \theta$ for every $p \leq N$.

(1.7) Proposition. *The model-theoretic and algebraic notions of algebraic closure over a substructure coincide.*

Proof. Let E be an algebraically closed substructure of $K \models ACFA$, and let $a \in K \setminus E$. Let (K', σ') be an E-isomorphic copy of (K, σ) which is linearly disjoint from K over E. As in the proof of (1.2), σ and σ' have a common extension to the composite L of K and K'; if M is a model of $ACFA$ containing L, then M is an elementary extension of K and K', and $M \setminus K$ contains a realisation of $tp(a/E)$. This shows that $tp(a/E)$ has infinitely many realisations in a sufficiently saturated extension of K.

(1.8). It follows from this result and the preceding one that for a formula $\varphi(x, y)$ there is an integer n such that for every $a \in K \models ACFA$, if $\varphi(a, K)$ is finite, then it has $\leq n$ elements. Thus we have some kind of algebraic boundedness in the sense of van den Dries [6]. We need however to modify the definition of algebraic boundedness by allowing difference polynomials. More precisely, given a formula $\varphi(x, y)$ with x a tuple of variables and y a single variable, there are difference polynomials $f_1(X, Y), \ldots, f_m(X, Y)$ which are ordinary polynomials in Y (i.e. elements of $\mathbb{Z}\langle X \rangle[Y]$) such that, for every model K of $ACFA$ and tuple a from K, if $\varphi(a, K)$ is finite, then it is included in the set of zeroes of $f_i(a, Y)$, for some i such that $f_i(a, Y)$ is a non-trivial polynomial in Y.

(1.9) Definition. Let A, B and C be subsets of a model K of $ACFA$. We say that A and B are independent over C if the (pure) fields $acl_\sigma(C, A)$ and $acl_\sigma(C, B)$ are algebraically independent (or, equivalently, linearly disjoint) over $acl_\sigma(C)$.

Generalised independence theorem. *Let $K \models ACFA$, and let E be an algebraically closed substructure of K. Let n be an integer, W a collection of subsets of $\{1, \ldots, n\}$ closed under subsets;; assume that for each $w \in W$ we are given a complete type $p_w(x_w)$ over E, in the (infinitely many) variables x_w, which satisfy:*

(i) *if* $w \subseteq w'$, *then* $p_w \subseteq p_{w'}$ *and* $x_w \subseteq x_{w'}$; *we denote* $p_{\{i\}}$ *by* p_i.

If (a_w) *realises* p_w *then*

(ii) $\{a_i \mid i \in w\}$ *is independent over* E, *and*

(iii) $a_w \subseteq acl_\sigma(E, a_i \mid i \in w)$.

Then there is $p_{\{1,\dots,n\}}$ *such that* (i) – (iii) *hold for* $W \cup \{1, \dots, n\}$.

Proof. We reduce to the case where W is the set of all proper subsets of $\{1, \dots, n\}$, and whenever a_w realises p_w then a_w enumerates $acl_\sigma(E, a_i \mid i \in w)$. We use induction on n, the case $n = 2$ being trivial. We assume that K is sufficiently saturated, and $n \geq 3$.

We need to realise simultaneously the types p_w in a way which is consistent; that is, in such a way that the interpretations of σ on each a_w have a common extension to (the field) $L = acl_\sigma(a_1, \dots, a_n)$.

Let a_n realise p_n, and let $W_1 = \{w \in W \mid n \in w\}$. Adding to each p_w, $w \in W_1$, a system of equations expressing $x_n = a_n$, we obtain a system of types q_w over the algebraically closed substructure a_n, but in effect indexed by the proper subsets of $\{1, \dots, n-1\}$. By the induction hypothesis, the partial type $\bigcup_{w \in W_1} q_w$ is consistent with the set of formulas expressing that $x_1, \dots, x_{n-1}$ are independent over a_n and has a completion q. Let a_w, $w \in W_1$, realise q; since independence is defined in the context of pure algebraically closed fields, $a_1, \dots, a_n$ are independent over E.

Let F_1 be the composite of the fields a_w, $w \in W_1$, and let σ_1 be the automorphism of F_1 as given by q; let F_0 be the composite of the fields a_w, where w ranges over all proper subsets of $\{1, \dots, n-1\}$, and let $F_2 = acl_\sigma(a_1 \dots, a_{n-1})$. By the definition of $p_{\{1,\dots,n-1\}}$, $\sigma_1|_{F_0}$ extends to an automorphism σ_2 of F_2 such that (F_2, σ_2) realises $p_{\{1,\dots,n-1\}}$.

It suffices to show that σ_1 and σ_2 have a common extension to L, i.e. that they are compatible on the composite F of F_1 and F_2. It is enough to show that F_1 and F_2 are linearly disjoint over F_0, which, because $F_2 = F_0^{alg}$ and F_1 is perfect (it is the composite of algebraically closed fields), reduces to showing that $F_1 \cap F_2 = F_0$.

Let $b \in F_1 \cap F_2$ and write

$$b = \sum_{i=1}^{m} \prod_{w \in W_1} b_{i,w},$$

where each $b_{i,w}$ is in $a_w = acl_\sigma(a_n, a_{w \setminus \{n\}})$; for i,w, let $q_{i,w}(x, x_n) \in a_{w \setminus \{n\}}[x, x_n]$ be such that $q_{i,w}(x, a_n)$ is the minimal polynomial of $b_{i,w}$ over the composite of a_n and $a_{w \setminus \{n\}}$. Then

$$L \models \exists (y_{i,w})_{i=1,\dots,m, w \in W_1} \left(b = \sum_{i=1}^{m} \prod_{w \in W_1} y_{i,w} \right) \wedge \bigwedge_{i,w} q_{i,w}(y_{i,w}, a_n) = 0.$$

Since a_n and F_2 are independent over E, it follows that for some a in E the polynomials $q_{i,w}(y_{i,w}, a)$ are non-trivial, and

$$L \models \exists (y_{i,w})_{i=1,\dots,m, w \in W_1} \left(b = \sum_{i=1}^{m} \prod_{w \in W_1} y_{i,w} \right) \wedge \bigwedge_{i,w} q_{i,w}(y_{i,w}, a) = 0,$$

i.e., $b \in F_0$.

Remarks. (1) Note that the proof of $F_1 \cap F_2 = F_0$ only used the minimality of algebraically closed fields; hence similar results hold in strongly minimal theories.

(2) Taking $n = 3$ and σ the identity automorphism, the proof that $F_1 \cap F_2 = F_0$ can be translated as follows:

If A, B and C are algebraically closed fields containing an algebraically closed subfield E, and if C is independent from AB over E, then $(AC)^{alg}(BC)^{alg} \cap (AB)^{alg} = AB$.

From this one deduces that

$$(AC)^{alg}(BC)^{alg} \cap (AB)^{alg}C = ABC,$$

and

$$(AC)^{alg}(BC)^{alg} \cap (AB)^{alg}(BC)^{alg} = A(BC)^{alg}.$$

Indeed, assume that $\alpha \in (AB)^{alg}C$ is in $(AC)^{alg}(BC)^{alg}$, but not in ABC. Take $\beta \in (AB)^{alg}$ such that $ABC(\alpha) = ABC(\beta)$. Then

$$\beta \in (AB)^{alg} \cap (AC)^{alg}(BC)^{alg} = AB,$$

so that $\alpha \in ABC$ after all. The proof of the second assertion is similar.

(3) By results of Kim and Pillay, the independence theorem also shows that our notion of independence coincides with non-forking, and any completion of $ACFA$ is simple, see [22].

(1.10) Elimination of imaginaries. Let $K \models ACFA$; then $\mathrm{Th}(K)$ eliminates imaginaries.

Proof. We may assume that K is somewhat saturated. Throughout the proof we work in K^{eq}; in particular acl and dcl are in K^{eq}. Let e be an imaginary element; we must show that for some tuple $c \in K$ we have $dcl(c) = dcl(e)$. Let $E = acl(e) \cap K$; we will first show that $e \in dcl(E)$. Choose a definable function f and a tuple a in K such that $f(a) = e$. Let P be the set of realisations of $tp(a/E)$.

Claim 1. There is $c \in P$ such that $f(c) = e$ and a and c are independent over E.

Proof. Since E is algebraically closed, there is a conjugate b of a over $E \cup \{e\}$ satisfying

$$acl(Ea) \cap acl(Eb) \cap K = acl(Ee) \cap K = E,$$

see [9], Lemma 1.4. Choose such a b with maximal transformal transcendence degree m over Ea, and then such that for some transformal transcendence basis $b_1 \subseteq b$, $deg_\sigma(b/Eab_1) = n$ is as large as possible (by compactness and maximality of m, this n is finite). Now take c such that $tp(c/Ea) = tp(b/Ea)$, and c is independent from b over Ea. Then $f(c) = e$, and $acl(Ec) \cap acl(Eb) \subseteq acl(Ec) \cap acl(Ea) = E$, so that the transformal transcendence degree of c over Eb is less than or equal to m; thus it equals m because the transformal transcendence degree of c over Eab equals m. Similarly, for $c_1 \subseteq c$ corresponding to $b_1 \subseteq b$, $deg_\sigma(c/Ebc_1) \leq n$, and therefore equals n. Hence c is independent from a over Eb, and from b over Ea (by choice). This implies that c is independent from ab over $acl(Ea) \cap acl(Eb) = E$, and in particular proves our claim.

Claim 2. f is constant on P.

Proof. Otherwise there is an element d in P such that $f(a) \neq f(d)$ and a and d are independent over E. Using the independence theorem with $p_{12} = p_{13} = tp(a, c/E)$ and $p_{23} = tp(a, d/E)$ we reach a contradiction.

Hence $e \in dcl(E)$. Let $b \in E$ be such that $e \in dcl(b)$; as algebraically closed fields eliminate imaginaries, there is a tuple c in K coding the set of conjugates of b over e (which is finite). Then $dcl(c) = dcl(e)$.

Remark. The proofs of (1.9) and (1.10) are simple translations to our context of proofs given by the second author in [14] to prove analogous results for pseudo-finite fields and related structures. Because of σ, the results obtained in our case are actually stronger: we do not need the presence of additional constant symbols.

(1.11) Proposition. *The fixed field F is stably embedded; that is, every definable (with parameters) subset of F^m is definable with parameters from F. Moreover, it is definable in F in the pure field language.*

Proof. The first part is an immediate consequence of elimination of imaginaries: if c is a code for a definable subset of F^m, and $\varphi(x, c)$ the defining formula, then every automorphism of the model K leaves $\varphi(x, c)$ invariant if and only if it leaves every element of c fixed. Since σ is such an automorphism, c is in F.

By (1.6), $\varphi(x)$ is equivalent to a disjunction of formulas of the form $\exists y\, \psi(x, y)$, where

$$\psi(x, y) = [f(x, y) = 0 \ \wedge\ \sigma(y) = g(x, y) \ \wedge\ h(x, y) \neq 0]$$

for some tuples of polynomials f, g and h with coefficients in F and satisfying the following condition: whenever $f(a, b) = 0 \wedge h(a, b) \neq 0$ holds, then the field generated by (a, b) is an algebraic extension of degree $\leq d$ of the field generated by a. Let $m = d!$ and choose $\alpha \in F^{alg}$ of degree m over F. Take any tuple (a, b) satisfying $f(a, b) = 0 \wedge h(a, b) \neq 0$, with a in F. Then $b \in F(\alpha)$.

Let u be the m-tuple of coefficients of the minimal polynomial of α over F, and let $v = (v_1, \ldots, v_m) \in F^m$ be such that $\sigma(\alpha) = v_1 + v_2\alpha + \cdots + v_m\alpha^{m-1}$. Identifying $F(\alpha)$ with $F + F\alpha + \cdots + F\alpha^{m-1}$, one sees that the difference field $(F(\alpha), \sigma)$ is interpretable in F, with parameters (u, v). Thus, there is a formula $\theta(x, z)$ of the language of fields such that:

For any tuples a in F and b in $F(\alpha)$, if $b = c_1 + c_2\alpha + \cdots + c_m\alpha^{m-1}$ with the c_i in F, then

$$(F(\alpha), \sigma) \models \psi(a, b) \iff F \models \theta(a, c).$$

Thus, for $a \in F^m$, $(K, \sigma) \models \exists y\, \psi(a, y)$ if and only if $F \models \exists z\, \theta(a, z)$. This finishes the proof.

(1.12) Lemma. *Let $E = acl_\sigma(E)$, let $k > 1$, and assume that (E_0, τ) is a difference field extending (E, σ^k). Then there is a difference field (E', σ') containing (E, σ), and such that ${\sigma'}^k$ extends τ.*

Proof. We work in the pure field context. For each $0 < i < k$ choose a field E_i realising $\sigma^i(tp(E_0/E))$, and such that $E_0, E_1, \ldots, E_{k-1}$ are linearly disjoint over E; then E_{i+1} realises $\sigma(tp(E_i/E))$. For each $0 < i < k$ choose an isomorphism $\sigma_i : E_{i-1} \to E_i$ extending σ on E, and define $\sigma_k : E_{k-1} \to E_0$ by $\sigma_k = \tau \circ \sigma_1^{-1} \circ \cdots \circ \sigma_{k-1}^{-1}$; then σ_k extends σ. Let E' be the composite of $E_0, \ldots, E_{k-1}$; since the E_i's are linearly disjoint over E, E' is isomorphic to the quotient field of $E_0 \otimes_E E_1 \otimes_E \cdots \otimes_E E_{k-1}$, and there is a unique automorphism σ' of E' which extends σ_i for each $0 < i \leq k$. By the definition of σ_k, ${\sigma'}^k$ extends τ.

Corollaries. *Let (K,σ) be a model of $ACFA$, and $k>1$, $m\in\mathbb{Z}$. Let $Frob$ denote the identity morphism if $char(K)=0$, and the automorphism $x\mapsto x^p$ if $char(K)=p>0$.*

1. *The reduct $(K, Frob^m\circ\sigma^k)$ is also a model of $ACFA$.*
2. *If (K,σ) is κ-saturated, so is $(K, Frob^m\circ\sigma^k)$.*
3. *If $(K,\sigma)\models ACFA$ is saturated, and there is an automorphism τ of the algebraic closure of the prime field such that σ and τ^k agree on the algebraic closure of the prime field, then there is an automorphism τ of K such that $\tau^k=\sigma$ and (K,τ) is a saturated model of $ACFA$.*

(1.13). Let F be the fixed field of a model (K,σ) of $ACFA$. In view of (1.10) and (1.11) one can wonder whether the theory of F in the pure field language admits elimination of imaginaries. This is however not the case, as the following example shows. Assume that F contains the algebraic closure of the prime field; then the cosets of the subgroup of n-th powers of the multiplicative group $F^\times$ are imaginary elements that belong to $acl(\emptyset)$ (in F^{eq}) but are not definable over $acl(\emptyset)\cap F$. One should also note that some of these cosets are definable over $acl(\emptyset)$ in the full language (with σ), whereas they are not in the pure field language: for F containing the algebraic closure of the prime field, n a prime and ζ a primitive n-th root of unity, the equation $\sigma(x)=\zeta x$ defines a unique coset of $F^{\times n}$; however in the pure field language, all the cosets of $F^{\times n}$ not containing 1 are conjugate over $acl(\emptyset)\cap F$. The problem comes from the fact that the definable closure is sometimes much smaller in the pure field language, as is shown by the following remark.

Lemma. *Let F_0 be a subfield of F. Let $G=\mathcal{G}al(F_0^{alg}/F_0)$ be its absolute Galois group.*

1. *In the pure field language (that is, inside the pseudo-finite field F), the definable closure of F_0 is the fixed field of $N_G(\langle\sigma\rangle)$, the normaliser in G of the closed subgroup generated by σ.*
2. *In $ACFA$, the definable closure of F_0 is the fixed field of $C_G(\sigma)$, the centraliser in G of σ.*

Proof. (2) is obvious, since every automorphism τ of (K,σ) commutes with σ; (1) comes from looking at elements of G which send $F\cap F_0^{alg}$ to itself.

We will now study in more detail the structure induced on F by (K,σ), and show, as can be expected in view of (1.11), that to obtain elimination of imaginaries it is enough to add constants to F.

For each integer $n>1$, there is a unique extension L of F of degree n over F, and this extension is interpretable in F, using parameters from F: let $X^n+a_1X^{n-1}+\cdots+a_n$ be the minimal polynomial over F of an element α generating L over F; then, identifying elements of L with their n-tuple of coordinates with respect to the basis $\{1,\alpha,\dots,\alpha^{n-1}\}$, one observes that multiplication by α in L gives rise to a linear map $F^n\to F^n$, the matrix of which has entries among $\{0,1,-a_1,\dots,-a_n\}$. Note that the algebraic extension L is the imaginary element corresponding to the 0-definable set $A_n=\{(a_1,\dots,a_n)\mid X^n+a_1X^{n-1}+\cdots+a_n \text{ is irreducible}\}$.

Let S_n be the imaginary sort with elements the isomorphism types (over F) of structures (L,τ) consisting of a field extension L of F of degree n together with a distinguished element τ of $\mathcal{G}al(L/F)$. Each such structure is then interpretable in F: let $\alpha\in L$ be such that $L=F(\alpha)$, and let $X^n+a_1X^{n-1}+\cdots+a_n$ be its

minimal polynomial over F; if $\tau(\alpha) = b_1 + b_2\alpha + \cdots + b_n\alpha^{n-1}$ (where $b_1, \ldots, b_n \in F$) then the structure (L, τ) is interpretable in F using the a_i's and b_i's. Each $e \in S_n$ corresponds to the definable set C of $2n$-tuples from F coding the corresponding structure (L, τ) (and C is definable over any $2n$-tuple in it).

Because $\mathcal{G}al(L/F)$ is abelian, the definition of $(b_1, \ldots, b_n)$ does not depend on the choice of the particular root α, which implies that S_n has precisely n elements.

Claim. Each element of S_n is 0-definable in K.

Proof. This is clear: if $Fix(\sigma^n)$ is the subfield of K fixed by σ^n, then τ is the restriction to $Fix(\sigma^n)$ of σ^j, for some $j < n$.

Proposition A. *The induced structure on F is precisely the field structure together with the distinguished constants $e_{j,n} \in S_n$ for $n > 1$, $0 \leq j < n$, where $e_{j,n}$ codes the isomorphism type over F of $(Fix(\sigma^n), \sigma^j|_{Fix(\sigma^n)})$.*

Proof. $\sigma|_{F^{alg}}$ is the unique element of $\mathcal{G}al(F^{alg}/F)$ such that $e_{j,n}$ is the structure $(Fix(\sigma^n), \sigma^j|_{Fix(\sigma^n)})$ for all $0 \leq j < n$. The result follows by (1.3).

In particular, we will later use

Corollary. *For elements of F^{eq}, definable closure in $(F, e_{j,n})_{0 \leq j < n}$ and in K are the same.*

Proposition B. (1) *$(F, e_{j,n})$ has elimination of imaginaries.*

(2) *For each $n > 1$, select a $2n$-tuple c_n allowing one to define the extension $(Fix(\sigma^n), \sigma|_{Fix(\sigma^n)})$. Then $(F, c_n)_{n \in \mathbb{N}}$ has elimination of imaginaries.*

(3) *For each $n > 1$ select an n-tuple $a_n \in A_n$. Then the pure field $(F, a_n)_{n \in \mathbb{N}}$ has elimination of imaginaries.*

Proof. (1) Clear by the above corollary and (1.10), (1.11).

(2) Clear, since $e_{1,n}$ is definable over c_n, and each $e_{j,n}$ is definable over $e_{1,n}$.

(3) Except when explicitly stated we work in the pure field language, with added constants a_n, $n \in \mathbb{N}$ (in particular, *acl* and *dcl* are in the sense of the theory ACF of algebraically closed fields). For each n, choose a $2n$-tuple c_n as in (2); since there are only finitely many possibilities for σ on $Fix(\sigma^n)$, we may choose $c_n \in acl(a_n)$. Let e be an imaginary element of F. By (2), there are a tuple $b \in F$ and an integer n such that e and b are equi-definable in the structure $(K, \sigma, c_1, \ldots, c_n)$. Since $c_j \in acl(a_j)$, we have

$$e \in acl(b, a_1, \ldots, a_n) \quad \text{and} \quad b, c_1, \ldots, c_n \in acl(e, a_1, \ldots, a_n).$$

Let $d \in F$ code the set of conjugates of $(b, c_1, \ldots, c_n)$ over $(e, a_1, \ldots, a_n)$; then $d \in dcl(e, a_1, \ldots, a_n)$, $b, c_1, \ldots, c_n \in acl(d)$ and

$$tp(b, c_1, \ldots, c_n/d) \vdash tp(b, c_1, \ldots, c_n/e, a_1, \ldots, a_n).$$

By symmetry,

$$tp(e, a_1, \ldots, a_n/d) \vdash tp(e, a_1, \ldots, a_n/b, c_1, \ldots, c_n),$$

which implies that $e \in dcl(d)$.

A more algebraic description of the imaginaries. We saw, at the beginning of the section, that in certain cases there was a natural correspondence between the imaginary elements of S_n and cosets of certain definable subgroups, namely $F^\times/(F^\times)^n$. By duality, this gives a correspondence between S_n and $\hom(F^\times, \langle\zeta_n\rangle)$, where ζ_n denotes a primitive n-th root of unity. We will generalise this correspondence to give an interpretation of the sorts S_n for n a prime power, in the case when $e_{1,n}$ is not already 0-definable in the pseudo-finite field F.

Theorem. *Let F be the fixed field of a model (K, σ) of ACFA of characteristic greater than 3. Let P be the set of primes such that the maximal p-extension of F is not obtained by composing F with some abelian extension of the prime field. Add to the language of fields constant symbols for elements of a new sort T_q, for each prime power $q = p^r$, $p \in P$, where T_q is defined as follows:*

(a) *If $\mathrm{char}(F) \neq p$, we let $F' = F(\zeta_p)$ if $p \neq 2$, $F' = F(i)$ if $p = 2$ ($i^2 = -1$). Then*

$$T_q = \hom(F'^\times, \langle\zeta_q\rangle).$$

(b) *If $\mathrm{char}(F) = p > 0$, let J be any elliptic curve of Hasse invariant 1 defined over F_p, let ν_q denote the subgroup of J of elements of order q, and let $F' = F(\nu_p)$; then*

$$T_q = \hom(J(F'), \nu_q).$$

Then $(F, T_q)_q$ eliminates imaginaries.

Proof. By construction, the imaginary constant $e_{j,n}$ codes the isomorphism type of the structure $(Fix(\sigma^n), \sigma|^j_{Fix(\sigma^n)})$. We already observed that $e_{j,n} \in dcl(e_{1,n})$; also, if m and n are relatively prime, then $e_{1,mn} \in dcl(e_{1,m}, e_{1,n})$. Hence it is enough to show that, for $q = p^f$: if $p \notin P$, then $e_{1,q} \in dcl(0)$; if $p \in P$, then $e_{1,q} \in dcl(\bigcup_r T_{p^r})$ and $T_q \subseteq dcl(e_{1,q})$.

Fix a prime p and let $F(p)$ denote the maximal Galois p-extension of F; then $\mathcal{G}al(F(p)/F) \simeq \mathbb{Z}_p$.

Claim. Assume that the extension L of F is obtained by composing F with an abelian extension L_0 of the prime field k. Then $S_n \subseteq dcl(0)$, where $n = [L : F]$.

Proof. The restriction map gives an isomorphism between $\mathcal{G}al(L/F)$ and $\mathcal{G}al(L_0/L_0 \cap F)$. Consider now the structure (L_0, τ), where $\tau \in \mathcal{G}al(L_0/L_0 \cap F)$. As above, the isomorphism type of this structure over the prime field k is k-definable, hence 0-definable. Since $\mathcal{G}al(L_0/k)$ is abelian, it follows that the isomorphism type of (L_0, τ) over $(L_0 \cap F)$ is 0-definable. This implies that the isomorphism type of (L, τ') over F, where τ' is the extension of τ which is the identity on F, is 0-definable, and $S_n \subseteq dcl(0)$.

This gives the result for $p \notin P$: if $F(p)$ is obtained by composing F with an abelian extension of the prime field k, then $S_q \subseteq dcl(0)$ for every p-th power q. We will now assume that $p \in P$; let q range over all powers of p, and let F_q denote the extension of F of degree q. The proof splits in two cases:

Case 1. $\mathrm{char}(F) \neq p$.

Let μ_p denote the group of all p^m-th roots of 1, $m \in \mathbb{N}$. Then $\mathcal{G}al(F(\mu_p)/F)$ is isomorphic to a closed subgroup of $\mathbb{Z}_p \times (\mathbb{Z}/(p-1)\mathbb{Z})$ [$\mathbb{Z}_2 \times (\mathbb{Z}/2\mathbb{Z})$ if $p = 2$];

since $p \in P$ and $k(\mu_p)$ is an abelian extension of k, it follows that $\mathcal{G}al(F(\mu_p)/F)$ has no quotient isomorphic to $\mathbb{Z}_p$, and therefore is isomorphic to a subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$ [resp. $\mathbb{Z}/2\mathbb{Z}$]. This implies that $\mu_p \subseteq F(\zeta_p)$ [$\mu_2 \subseteq F(i)$]. Set $F' = F(\zeta_p)$ [$F' = F(i)$].

We will first assume that $i \in F$ if $p = 2$. Let F'_q denote the algebraic extension of F' of degree q. Since $[F' : F]$ divides $p-1$, $F'_q = F'F_q$, and there is a canonical isomorphism between $\mathcal{G}al(F_q/F)$ and $\mathcal{G}al(F'_q/F')$. By Kummer theory, $F'_q = F'(\alpha)$, for some α satisfying $\alpha^q \in F'$; if $\tau \in \mathcal{G}al(F'_q/F')$ then $\tau(\alpha)/\alpha \in \langle\zeta_q\rangle \subseteq F'$, and only depends on α^q, not on the choice of the individual root α. Thus the correspondence is as follows: to the imaginary element $(F_q, \tau) \in S_q$, we associate the homomorphism $f_\tau : {F'}^\times \to \langle\zeta_q\rangle$ defined by $f_\tau(a) = \tau'(\alpha)/\alpha$, where α is any q-th root of a and τ' is the extension of τ to F'_q which is the identity on F'.

Observe that $f_\tau(\sigma(a)) = \sigma(f_\tau(a))$, and that F' is 0-interpretable in F. Thus the homomorphism f_τ and the corresponding $e_{j,q}$ are bi-interpretable in F, and $dcl(S_q) = dcl(T_q)$.

Assume now that $p = 2$, and $i \notin F$. Then $[F' : F] = 2$, and F' is 0-interpretable in F, and so are the two elements of S_2. The construction given above applies to F' and establishes a correspondence between the elements $e_{2j,2q}$ and $\hom({F'}^\times, \langle\zeta_q\rangle)$. Now observe that $e_{1,q} \in dcl(e_{1,2}, e_{2,2q})$ to conclude.

This shows that the elements of $\bigcup_{q=p^f} S_q$ are equi-definable with the imaginary elements $\bigcup_{q=p^f} \hom({F'}^\times, \langle\zeta_q\rangle)$.

Case 2. $\mathrm{char}(F) = p$.

(The references are to Hartshorne [10, Chapter IV] for the results on elliptic curves.) Let J be an elliptic curve with Hasse invariant 1, defined over $\mathbb{F}_p$ (Cor. 4.23). Let ν_q be the subgroup of points of J of order dividing q; then ν_q is cyclic of order q (see exercise 4.15), and contained in $J(\mathbb{F}_p^{alg})$. Set $F' = F(\nu_p)$; then $[F' : F]$ is prime to p, and therefore there is a canonical isomorphism between $\mathcal{G}al(F'F(p)/F')$ and $\mathcal{G}al(F(p)/F)$. Since $\mathcal{G}al(\mathbb{F}_p(\bigcup_{q=p^f} \nu_q)/\mathbb{F}_p(\nu_p)) \simeq \mathbb{Z}_p$, our assumption on p implies that $\bigcup_{q=p^f} \nu_q$ is contained in F'. This in turn implies that $J(F')/([q]J(F'))$ is cyclic of order q, because F' is pseudo-finite and the homomorphism $a \mapsto [q]a$ has a kernel of size q.

Choose b in $J(F')$ not divisible by p, and let $a \in J(F^{alg})$ be such that $[q]a = b$. Then the solutions of $[q]x = b$ are the elements $a + c$ for $c \in \nu_q$. Since ν_q is cyclic of order q and b is not divisible by p, this implies that $[F'(a) : F'] = q$. Let $\tau \in \mathcal{G}al(F'(a)/F')$; then $\tau(a) - a \in \nu_q$, and only depends on b, not on the choice of the particular root a (since they are all translates by elements of $J(F')$). Thus we define the correspondence as follows: to the imaginary element $(F_q, \tau) \in S_q$ we associate the homomorphism $f_\tau : J(F') \to \nu_q$ defined by $f_\tau(b) = \tau'(a) - a$, where a is any solution of $[q]a = b$ and τ' is the extension of τ to $F'F_q$ which is the identity on F'.

Reasoning as in the previous case, we deduce that the homomorphism f_τ and the corresponding $e_{j,q}$ are bi-interpretable in F, and that $dcl(S_q) = dcl(T_q)$.

Remark. The elements of T_q are 0-definable in (K, σ); we could thus obtain elimination of imaginaries by naming them. We wish however to obtain elimination of imaginaries without changing the automorphism group. The theorem thus describes precisely the sorts of F^{eq} that must be added to obtain elimination of imaginaries.

The restriction on the characteristic of F is only used in the last case, to find an elliptic curve with Hasse invariant 1 defined over $\mathbb{F}_p$; there are analogous but more complicated descriptions of the imaginary elements in characteristic 2 and 3.

(1.14) Two conjectures. One motivation behind the study of $ACFA$ is the hope that it is an axiomatisation of the theory of almost all structures $(\mathbb{F}_p^{alg}, \sigma_q)$, where σ_q is the map $x \mapsto x^q$ for some p-power q. More precisely,

Conjecture 1. *Assume that $ACFA \models \theta$. Then, for some $C > 0$, θ holds in all the $\mathcal{L}$-structures $(\mathbb{F}_p^{alg}, \sigma_q)$ provided that $q > C$.*

A consequence of a positive solution to this conjecture would be a generalisation of Ax's results [1] to the structures $(\mathbb{F}_p^{alg}, \sigma_q)$. Indeed, let us assume that Conjecture 1 is true, and let θ be a sentence; by (1.4) we have a finite Galois extension E of $\mathbb{Q}$ and conjugacy classes c_i in $\mathcal{G}al(E/\mathbb{Q})$ such that a model K of $ACFA_0$ satisfies θ if and only if $\sigma|_E \in c_i$ for some i. By the Čebotarev density theorem, the set of primes p such that the Artin symbol $(\frac{E/\mathbb{Q}}{p}) = c$, for c a conjugacy class in $\mathcal{G}al(E/\mathbb{Q})$, has density $|c|/[E : \mathbb{Q}]$, and in particular is infinite. If p is sufficiently large and $(\frac{E/\mathbb{Q}}{p}) = c$, then $(\mathbb{F}_p^{alg}, \sigma_p) \models \varphi_{E,c}$, where $\varphi_{E,c}$ is defined as in (1.6), and is positive. From this it now follows easily that, letting Φ be a collection of sentences expressing that the fixed field is infinite,

$$\begin{aligned} ACFA &= \mathrm{Th}(\mathbb{F}_p^{alg}, \sigma_p) \cup \{\Phi\} \\ &= \mathrm{Th}(\mathbb{F}_p^{alg}, \sigma_q) \cup \{\Phi\}, \end{aligned}$$

where p ranges over all prime numbers, and q over all powers of p. One also has

$$ACFA_p = \mathrm{Th}(\mathbb{F}_p^{alg}, \sigma_q) \cup \{\Phi\},$$

where q ranges over all p-th powers.

In order to state the second conjecture, we first need a remark: clearly the scheme of axioms (iii) is the only one posing any problem. It turns out that we may replace (iii) by an apparently weaker scheme of axioms:

(iii') For every variety U, and every variety $V \subseteq U \times \sigma(U)$ such that the projections $V \to U$ and $V \to \sigma(U)$ are onto and have finite fibers, there is $a \in U(K)$ such that $(a, \sigma(a)) \in V$.

Claim. (i), (ii), (iii') axiomatise $ACFA$.

Proof. Let K be a model of these axioms, and let $L \supseteq K$ be a model of $ACFA$; it is enough to show that every finite system of equations with coefficients in K which has a solution in L has a solution in K. By remark (1.1)(1), we may assume that all elements of L have finite degree over K. Let

$$\begin{aligned} f_1(x, \sigma(x), \dots, \sigma^k(x)) &= f_2(x, \sigma(x), \dots, \sigma^k(x)) \\ &= \dots = f_m(x, \sigma(x), \dots, \sigma^k(x)) = 0 \end{aligned}$$

be a system of equations with coefficients in K and in the variables $x = (x_1, \dots, x_n)$, and let $a \in L^n$ be a solution of this system. Then $f_1, \dots, f_m \in I(a/K)$; as a prime σ-ideal, $I(a/K)$ is finitely generated, say by polynomials involving the variables $x, \sigma(x), \dots, \sigma^\ell(x)$. In particular, since $deg_\sigma(a/K)$ is finite,

$$\sigma^\ell(a) \in K(a, \sigma(a), \dots, \sigma^{\ell-1}(a))^{alg}.$$

Let U and V be the K-varieties of which

$$(a, \sigma(a), \dots, \sigma^{\ell-1}(a)) \quad \text{and} \quad (a, \sigma(a), \dots, \sigma^{\ell-1}(a), \sigma(a), \dots, \sigma^{\ell}(a))$$

are generic points; then some open subsets U_0 of U and V_0 of V satisfy the hypotheses of (iii'); adding an extra variable if necessary, we may assume that $U_0 = U$ and $V_0 = V$. Let $c \in K$ be such that $(c, \sigma(c)) \in V$, and write c as $b^\frown\sigma(b)^\frown\sigma^{\ell-1}(b)$; then

$$\begin{aligned} f_1(b, \sigma(b), \dots, \sigma^k(b)) &= f_2(b, \sigma(b), \dots, \sigma^k(b)) \\ &= \dots = f_m(b, \sigma(b), \dots, \sigma^k(b)) = 0. \end{aligned}$$

Conjecture 2. *Let U, V be varieties with $V \subseteq U \times \sigma(U)$, and assume that the projections are onto and have finite fibers. Let*

$$d_1 = [K(V) : K(U)], \quad d_2 = [K(V) : K(\sigma(U))]_i$$

(purely inseparable degree); let $c = d_1/d_2$ and $d = dim(V)$. Then for some constant $C > 0$, depending on the two varieties U and V, and which remains bounded when U and V move inside an algebraic family of varieties,

$$\left| |\{a \in \mathbb{F}_p^{alg^n} \mid (a, a^q) \in V\}| - cq^d \right| \leq Cq^{d-1/2}.$$

These two conjectures have been solved positively by the second author [17]. Independently, Macintyre announced a proof of Conjecture 1; see [24].

2. The ranks S_1 and SU

Throughout this section, we place ourselves in a saturated model K of $ACFA$.

(2.1) The rank S_1. For $\varphi(x)$ a formula defined over a set A, we define, by induction on $n \in \mathbb{N}$,

– $S_1(\varphi) > 0$ iff $\varphi(x)$ has infinitely many solutions, and

– $S_1(\varphi(x)) > n+1$ iff there exist a sequence $(b_i)_{i\in\omega}$ of indiscernibles over A and a formula $\psi(x, y)$ such that

(i) $S_1(\psi(x, b_i) \wedge \psi(x, b_j)) \leq n$ for $i \neq j$, and

(ii) $S_1(\varphi(x) \wedge \psi(x, b_i)) > n$ for each i.

If not$(S_1(\varphi) > n)$ and n is least such, then we set $S_1(\varphi) = n$; if no such n exists, we set $S_1(\varphi) = \infty$. For p a (partial) type we define $S_1(p) = \min\{S_1(\varphi) \mid p \models \varphi\}$. We also set $S_1(a/A) = S_1(tp(a/A))$.

(2.2) The rank SU. Recall that we say that a and b are independent over C if the fields $acl_\sigma(Ca)$ and $acl_\sigma(Cb)$ are independent over $acl_\sigma(C)$, where acl_σ denotes taking the (field-theoretic) algebraic closure of the closure by σ and σ^{-1}.

Let $A \subseteq B$, $a \in K$, $p = tp(a/A)$, $q = tp(a/B)$. If a and B are not independent over A we say that q *forks* over A, or that q is a *forking extension* of p; if a and B are independent over A, we say that q is a non-forking extension of p. Note that a non-algebraic type p may have many non-forking extensions to B.

Let p be a complete type defined over A. We define by induction $SU(p) \geq \alpha$ by:

– $SU(p) \geq 0$ iff p is consistent.

– For α a limit ordinal, $SU(p) \geq \alpha$ iff $SU(p) \geq \beta$ for all $\beta < \alpha$.

– $SU(p) \geq \alpha + 1$ iff p has a forking extension q with $SU(q) \geq \alpha$.

For φ a formula we define $SU(\varphi) = \max\{SU(p) \mid p \models \varphi\}$. We set $SU(a/A) = SU(tp(a/A))$.

Remarks. (1) By (1.7), $SU(p) = 0$ if and only if p has only finitely many realisations (i.e. p is algebraic).

(2) For $A \subseteq B$ and a an element, the type of a over B forks over A if and only if $deg_\sigma(a/acl_\sigma(B)) < deg_\sigma(a/acl_\sigma(A))$.

(3) Hence $SU(a/A) \leq deg_\sigma(a/acl_\sigma(A))$ if the latter is finite.

(2.3) Lemma. *If a and E' are independent over E, then $SU(a/E) = SU(a/EE')$.*

Proof. We may assume that $E = acl_\sigma(E) \subseteq E' = acl_\sigma(E')$. We will show, by induction on α, that $SU(a/E) \geq \alpha$ implies $SU(a/E') \geq \alpha$ (the other inequality being always true). For $\alpha = 0$ there is nothing to prove, and for α a limit ordinal, the result is clear by induction. Assume therefore that $\alpha = \beta + 1$, and let $F \supseteq E$ be such that $SU(a/F) \geq \beta$ and F and a are dependent over E; moving F by an $E(a)_\sigma$-isomorphism if necessary, we may assume that F is independent from E' over $E(a)_\sigma$. Then a is independent from FE' over F. By the induction hypothesis we have $SU(a/FE') \geq SU(a/F) \geq \beta$; since a and FE' are not independent over E', this implies that $SU(a/E') \geq \alpha$.

(2.4) Lemma. *$SU(a/Eb) + SU(b/E) \leq SU(ab/E) \leq SU(a/Eb) \oplus SU(b/E)$ (the natural sum on ordinals), and equality holds if either side is finite.*

Proof. The proof is the same as in the superstable case. For the first inequality, we will show by induction on α that $SU(b/E) \geq \alpha$ implies $SU(a/Eb)+\alpha \leq SU(ab/E)$. For $\alpha = 0$, it is clear, and for α a limit ordinal it follows by induction. Assume therefore that $\alpha = \beta + 1$, and let $F \supseteq E$ be such that $SU(b/F) \geq \beta$ and $tp(b/F)$ forks over E; as in (2.3), we may choose F so that F is independent from a over Eb. By (2.3) we have $SU(a/Fb) = SU(a/Eb)$ and $SU(ab/F) < SU(ab/E)$, which gives the result using induction.

For the second inequality, we will show by induction on α that $SU(ab/E) \geq \alpha$ implies $SU(a/Eb) \oplus SU(b/E) \geq \alpha$. If $\alpha = 0$ or is a limit ordinal, this is clear. Assume that $\alpha = \beta + 1$, and choose $F \supseteq E$ such that $SU(ab/F) \geq \beta$ and $tp(ab/F)$ forks over E. By the induction hypothesis, $SU(a/Fb) \oplus SU(b/F) \geq \beta$. Our hypothesis on F implies that $tp(a/Fb)$ forks over Eb or that $tp(b/F)$ forks over E (by transitivity of algebraic independence for fields). Thus $SU(a/Eb) \oplus SU(b/E) > SU(a/Fb) \oplus SU(b/F)$, which gives the result.

Finally, $+$ and $\oplus$ define the same operation on finite ordinals, which gives the last assertion.

(2.5) The type of SU-rank ω. Let E be an algebraically closed substructure, and let a be an element which is transformally transcendental over E.

By induction on n, define $b_0 = a$, $b_n = \sigma(b_{n-1}) - b_{n-1}$. Let $L_n = E(b_n)_\sigma$; then $L_n \subseteq L_{n-1} \subseteq \ldots \subseteq L_0 = E(a)_\sigma$. From $deg_\sigma(b_{n-1}/L_n) = 1$ we deduce that $SU(b_{n-1}/Eb_n) = 1$, and therefore, by additivity of the rank, $SU(a/L_n) = n$. Thus, $SU(a/E) \geq \omega$; on the other hand, if $tp(a/F)$ forks over E, then a must satisfy a transformal equation over F, i.e., $deg_\sigma(a/F) = n$ for some integer n, which by (2.2) implies $SU(a/F) < \omega$. Hence $SU(a/E) = \omega$.

We will show in (2.10) that $tp(a/E)$ is implied by the collection of formulas expressing that a is transformally transcendental over E. This result, as well as the preparatory lemmas, can be found in [5], Chapter 7, Theorems 6, 8 and 9. For the sake of completeness, we will give the proofs.

We will denote by $p_\omega(E)$, or p_ω, this unique 1-type of SU-rank ω.

(2.6) Lemma. *Let E be a substructure, and fix σ on E^{alg}. Then the following are equivalent:*

(1) *Every extension of $\sigma|_E$ to E^{alg} is isomorphic over E to σ.*
(2) *The map $G(E) \to G(E)$, $\tau \mapsto [\sigma, \tau]$, is onto.*
(3) *For every finite Galois extension L of E, if $M = L\sigma(L)$ and $\varphi : \mathcal{G}al(M/E) \to \mathcal{G}al(L/E)$ is the map $\tau \mapsto [\sigma, \tau]|_L$, then $|\varphi^{-1}(1)| = [M : L]$ (and therefore φ is onto).*

Proof. (1) $\iff$ (2): (1) is clearly equivalent to the assertion that if σ_1 is an extension of $\sigma|_E$ to E^{alg}, then there is an E-isomorphism τ sending (E^{alg}, σ_1) to (E^{alg}, σ). This τ is therefore an element of $G(E)$, and satisfies $\tau\sigma_1 = \sigma\tau$, i.e., $\sigma^{-1}\sigma_1 = [\sigma, \tau]$. If we set $\sigma^{-1}\sigma_1 = \tau_0 \in G(E)$, this is equivalent to the assertion that for any $\tau_0 \in G(E)$, there is $\tau \in G(E)$ such that $[\sigma, \tau] = \tau_0$.

(2) $\iff$ (3): (2) is equivalent to the assertion that the map $\tau \mapsto [\sigma, \tau]|_L$ is onto for every finite Galois extension L of E. Clearly the value of $[\sigma, \tau]|_L$ depends only on $\tau|_L$ and $\tau^{-1}|_{\sigma(L)}$. Hence, (2) is equivalent to the assertion that for every L, M and φ as in (3), the map φ is onto. Observe that $\varphi(\tau_1) = \varphi(\tau_2) \iff \tau_1\tau_2^{-1} \in \varphi^{-1}(1)$, and therefore the size of the image of φ equals $[M : E]/|\varphi^{-1}(1)|$. Thus φ is onto if and only if $|\varphi^{-1}(1)| = [M : L]$.

(2.7) Lemma. *Let E be a substructure, L a finite Galois extension of E, and $M = L\sigma(L)$. Let $L_1 = L \cap \sigma(L)$ and $M_1 = L_1\sigma(L_1)$. Assume that the map $\varphi_1 : \mathcal{G}al(M_1/E) \to \mathcal{G}al(L_1/E)$ defined by $\tau \mapsto [\sigma, \tau]|_{L_1}$ is onto. Then $\varphi : \mathcal{G}al(M/E) \to \mathcal{G}al(L/E)$, $\tau \mapsto [\sigma, \tau]|_L$, is onto, and every element of $\varphi_1^{-1}(1)$ lifts to an element of $\varphi^{-1}(1)$.*

Proof. Observe first that $\varphi^{-1}(1)$ is a subgroup of $\mathcal{G}al(M/E)$, and that the restriction of any of its elements is in $\varphi_1^{-1}(1)$. From $[M : L] = [\sigma(L) : L \cap \sigma(L)] = [\sigma(L) : M_1][M_1 : L_1]$ and the hypothesis on φ_1, it follows that it is enough to show that $|\varphi^{-1}(1) \cap \mathcal{G}al(M/M_1)| = [\sigma(L) : M_1]$. This will follow from the equality $\varphi^{-1}(1) \cap \mathcal{G}al(M/\sigma(L)) = 1$. Write $L = E(\alpha)$ and let $\tau \in \mathcal{G}al(M/\sigma(L))$. Then

$$\begin{aligned} \tau \in \varphi^{-1}(1) &\iff \sigma\tau(\alpha) = \tau\sigma(\alpha) \\ &\iff \sigma\tau(\alpha) = \sigma(\alpha) \\ &\iff \tau = 1. \end{aligned}$$

The last assertion is clear from the proof.

(2.8) Lemma. *Let E be a substructure, and assume that E has no proper finite Galois extension L such that $\sigma(L) = L$. Then all extensions of $\sigma|_E$ to E^{alg} are E-isomorphic.*

Proof. By Lemma 2.6, it suffices to show that for every finite Galois extension L of E and $M = L\sigma(L)$, the map $\varphi_L : \tau \mapsto [\sigma, \tau]|_L$ is onto. This is shown by induction on $[L : E]$: assume that the result holds for Galois extensions of E of smaller degree than $[L : E]$; since $\sigma(L) \neq (L)$, $[L \cap \sigma(L) : E] < [L : E]$, which by Lemma 2.7 gives the result.

(2.9). In the following lemma, we clarify the relation between two properties: E has no proper finite σ-stable extensions; all extensions of $\sigma|_E$ to E^{alg} are isomorphic.

Note in particular the following consequence of (3) below: whether E has a proper finite σ-stable extension or not depends only on $\sigma|_E$, and not on a particular extension of $\sigma|_E$ to E^{alg}.

Lemma. *Let E be a field, and let $\sigma \in Aut(E^{alg})$ be such that $\sigma(E) = E$. Assume that $\tau \in Aut(E^{alg})$ extends $\sigma|_E$.*

1. *All extensions of $\sigma|_E$ to the perfect hull of E are isomorphic.*
2. *If K is a normal extension of E and $\sigma(K) = K$, then $\tau(K) = K$.*
3. *Let K be a difference field containing E, Galois over E. Assume that L is a finite separable extension of E such that $\sigma(KL) = KL$. If M is the normal closure of L over E, then $\sigma(KM) = KM = \tau(KM)$.*
4. *E has no proper finite σ-invariant Galois extension if and only if E has no proper finite σ^m-invariant extension for all $m \geq 1$ if and only if E has no proper finite τ-invariant Galois extension.*
5. *E has no proper finite σ-invariant extension if and only if for all $m \geq 1$, $\sigma^m|_E$ has a unique extension to E^{alg}, up to conjugation by an element of $\mathcal{G}al(E^{alg}/E)$.*
6. *Suppose that E is the directed union of the difference fields E_i, $i \in I$, where each E_i is algebraic over the difference field F, and such that each E_i has no proper finite σ-invariant extension. Then E has no proper finite σ-invariant extension.*

Proof. (1) If $a^{p^n} = b$, then $\sigma(a)$ is uniquely defined by the equation $X^{p^n} = \sigma(b)$.

(2) Let $\alpha \in K$, and let $p(X) \in E[X]$ be its minimal polynomial over E. Then K contains the roots of all the polynomials $p^{\sigma^n}(X) \in E[X]$, $n \in \mathbb{Z}$. From $\tau|_E = \sigma|_E$ we deduce that $E(\alpha)_\tau \subseteq K$.

(3) Write $L = E(\alpha)$, and let $p(X)$ be the minimal polynomial of α over E. Then $\sigma(\alpha)$ is a root of $p^\sigma(X)$ and $K(\alpha)$ contains a root of $p^\sigma(X)$. Because K is Galois over E, the same is true of every conjugate of α over E. Hence KM contains all the roots of $p^\sigma(X)$. Since KM is generated over K by all the conjugates of α over E, and contains all the conjugates of $\sigma(\alpha)$, we have $\sigma(KM) = KM$. The second equality follows by (2).

(4) One direction of the first equivalence is clear. For the other, assume that L is a proper finite extension of E which is stable under σ^m, and let M be the composite of the fields $\sigma^j\tau(L)$ for $1 \leq j < m$, and τ an E-embedding of L in E^{alg}. Then M is Galois over E and stable under σ. The second equivalence is clear by (2).

(5) One direction is clear by (2.8); for the other one, assume that L is a proper finite Galois extension of E, σ-invariant and fix σ on L. Conjugation by σ induces an automorphism of $G = \mathcal{G}al(L/E)$; hence, if m is the order of $Aut(G)$, σ^m commutes with every element of G, which implies that the non-isomorphic extensions of $\sigma^m|_E$ to L correspond to the conjugacy classes of G.

(6) We need to show that for every m, $\sigma^m|_E$ has a unique extension (up to conjugation) to E^{alg}. Fix m, and let σ_1, σ_2 be two extensions of $\sigma^m|_E$ to E^{alg}. For every $i \in I$ there is $\tau_i \in \mathcal{G}al(E^{alg}/E_i)$ such that $\sigma_1 = \tau_i^{-1}\sigma_2\tau_i$; since $\mathcal{G}al(E^{alg}/E)$

is the inverse limit of the $\mathcal{G}al(E_i^{alg}/E_i)$, there is some $\tau \in \mathcal{G}al(E^{alg}/E)$ such that $\sigma_1 = \tau^{-1}\sigma_2\tau$.

(2.10) Proposition. *Let E be an algebraically closed substructure, and a an element transformally transcendental over E. Then:*

(1) *$E(a)_\sigma$ has no proper finite Galois extension left invariant under σ. Thus, there is a unique 1-type of a transformally transcendental element over E.*

(2) *Let $K = acl_\sigma(K)$ be linearly disjoint from $E(a)_\sigma$ over E. Then $Kacl_\sigma(Ea)$ has no proper finite Galois extension left invariant under σ.*

Proof. Let $L = E(a)_\sigma(\alpha)$ be finite Galois over $E(a)_\sigma$; let $i \leq j$ be such that α is algebraic over $E(\sigma^i(a), \dots, \sigma^j(a))$, with $j - i$ minimal such. Since the elements $\sigma^n(a)$, $n \in \mathbb{Z}$, are algebraically independent over E, we have $\sigma^{j-i+1}(L) \cap L = E(a)_\sigma$, which implies that $\sigma(L) \neq L$.

The second assertion is immediate, by (2.8).

(2) Let L be a finite Galois extension of $Kacl_\sigma(Ea)$ left invariant under σ; we may write L as $L_0 Kacl_\sigma(Ea)$, where L_0 is finite over $KE(a, \sigma(a), \dots, \sigma^n(a))$ for some n. Let $F_1 = E(a, \sigma(a), \dots, \sigma^n(a))^{alg}$, $F_2 = E(\sigma^m(a))_{m<0, m>n}$; then F_1, F_2 and K are independent over E. Furthermore we have $L_0 \subseteq (KF_1)^{alg}$ and $\sigma^{n+1}(L_0) \subseteq (KF_2)^{alg}$; from

$$L = \sigma^{n+1}(L) = L_0(F_1F_2)^{alg} = \sigma^{n+1}(L_0)(F_1F_2)^{alg}$$

we deduce that

$$L \subseteq \big((KF_1)^{alg}(F_1F_2)^{alg}\big) \cap \big((KF_2)^{alg}(F_1F_2)^{alg}\big) = K(F_1F_2)^{alg} = Kacl_\sigma(Ea)$$

(by Remark 1.9), which proves our assertion.

(2.11) Corollaries. *Let E be an algebraically closed substructure.*

(1) *Let $a = (a_1, \dots, a_n)$, and assume that $a_1, \dots, a_d$ are transformally independent over E, and that $deg_\sigma(a/Ea_1, \dots, a_d) < \infty$. Then $\omega d \leq SU(a/E) \leq \omega d + deg_\sigma(a/Ea_1, \dots, a_d)$.*

(2) *Let V be a variety in affine n-space, defined over E and of dimension d. Then V has a unique type over E of SU-rank ωd, which we will call the generic type of V over E: this type expresses that $x_1, \dots, x_n$ is in V, and that the tuples $\sigma^n(\bar{x})$, $n \in \mathbb{Z}$, are algebraically independent over E.*

While the finite rank types only have weak definability (as we will see in (2.16)), the generic ones actually have full definability:

(3) *Let V be an irreducible (affine) variety defined over the difference field E. Then the generic type p_V of V over E is definable.*

Proof. (1) Use induction on d and $deg_\sigma(a/Ea_1, \dots, a_d)$.

(2) Let $(a_1, \dots, a_n)$ be a generic point of V; we may assume that $a_1, \dots, a_d$ are algebraically independent over E. By Proposition (2.10), $tp(a_1, \dots, a_d/E)$ is completely axiomatised by saying that $a_1, \dots, a_d$ are transformally transcendental over E. In particular, this implies that $qftp(a_1, \dots, a_n/E)$ is axiomatised by the formulas expressing that $((x_1, \dots, x_n)$ is a generic point of V, and the tuples $\sigma^i(\bar{x})$, $i \in \mathbb{Z}$, are algebraically independent over $E)$.

As in the proof of Proposition (2.10), one then shows that $E(a_1, \dots, a_n)_\sigma$ has no proper finite Galois extension left invariant by σ, which by Lemma 2.8 shows that the above axiomatisation is complete.

(3) Let X be the set of formulas $\theta(x, \sigma(x), \dots, \sigma^k(x), y)$ which are positive and quantifier-free in the pure language of fields. For such a θ, let $d\theta(y)$ be the quantifier-free formula of the pure language of fields (with parameters from E), equivalent modulo the theory of algebraically closed fields to the formula

$$\forall (x_0, x_1, \dots, x_k) \in V \times \sigma(V) \times \cdots \times \sigma^k(V),\ \theta(x_0, x_1, \dots, x_k, y).$$

Then, by (2), over any difference field F containing E, p_V is axiomatised as follows: $x \in V$ and the set

$$\Phi(F) = \{ \big(\theta(x, \sigma(x), \dots, \sigma^k(x), b) \leftrightarrow d\theta(b)\big) \mid \theta \in X,\ b \in F \}.$$

By construction, each formula $\theta(x, \sigma(x), \dots, \sigma^k(x), y) \in X$ has a definition over E; it follows then that p_V is definable over E.

(2.12) Proposition. *Let $\varphi(x)$ be a formula of finite SU-rank. Then $S_1(\varphi) = SU(\varphi)$.*

Proof. We will show by induction on n that $SU(\varphi) > n \ \Rightarrow\ S_1(\varphi) > n$ and $S_1(\varphi) > n \ \Rightarrow\ SU(\varphi) > n$. For $n = 0$, both implications follow from (1.7). Assume they hold for $n-1$, and let E be an algebraically closed substructure over which φ is defined.

$SU(\varphi) > n \ \Rightarrow\ S_1(\varphi) > n$:

Take a satisfying φ such that $SU(a/E) > n$ and choose an algebraically closed structure F containing E such that $SU(a/F) = n$. Let $\psi(x, b)$ be a formula in $tp(a/F)$ of finite SU-rank and such that whenever $\psi(a', b)$ holds, then $tp(b/Ea')$ forks over E. Then $SU(\psi(x, b)) \geq n$.

Choose a sequence $(b_i)_{i \in \mathbb{N}}$ of E-independent realisations of $tp(b/E)$ which are indiscernible over E. Suppose that $\psi(a', b_1) \wedge \ldots \wedge \psi(a', b_k)$ holds; using the fact that $tp(b_k/Ea')$ forks over E, an easy computation (and symmetry of forking) gives that $SU(a'/Eb_1, \dots, b_k) < SU(a'/Eb_1, \dots, b_{k-1})$. Therefore, for k sufficiently large we have $SU(\psi(x, b_1) \wedge \ldots \wedge \psi(x, b_k)) < n$.

Choose k minimal such, and let

$$\theta(x, y) = \bigwedge_{i=1}^{k-1} \psi(x, y_i), \qquad c_i = (b_{(k-1)i}, \dots, b_{(k-1)(i+1)-1}).$$

Then $SU(\theta(x, c_i)) \geq n$ and $SU(\theta(x, c_i) \wedge \theta(x, c_j)) < n$ for $i \neq j$. By the induction hypothesis, this implies $S_1(\theta(x, c_i)) \geq n$ and $S_1(\theta(x, c_i) \wedge \theta(x, c_j)) < n$ for $i \neq j$, i.e., $S_1(\varphi) > n$.

$S_1(\varphi) > n \ \Rightarrow\ SU(\varphi) > n$:

Take an E-formula $\psi(x, y)$ and a sequence $(b_i)_{i \in \mathbb{N}}$ of indiscernibles over E such that $\psi(x, y) \to \varphi(x)$, $S_1(\psi(x, b_i)) \geq n$ and $S_1(\psi(x, b_i) \wedge \psi(x, b_j)) < n$ for $i \neq j$. By enlarging E, we may assume that the sequence (b_i) is independent over E.

Using the induction hypothesis, choose a satisfying $\psi(x, b_1)$ with $SU(a/Eb_1) \geq n$. We claim that a and b_1 are not independent over E: else, using the independence theorem, we may assume that $tp(a/Eb_1) = tp(a/Eb_2)$ and a is independent from b_1, b_2 over E. But this implies $SU(a/Eb_1b_2) = SU(a/Eb_1) \geq n$; by induction we obtain $S_1(\psi(x, b_1) \wedge \psi(x, b_2)) \geq n$, which contradicts our assumption.

Hence $tp(a/Eb_1)$ forks over E, and therefore $SU(a/E) > n$, which implies $SU(\varphi) > n$.

Corollary. (1) *If $S_1(\varphi) = n$, then for some a satisfying φ, $S_1(a/E) = n$.*

(2) *$S_1(p) \geq SU(p)$.*

(3) *Let $\varphi(x)$ be a formula over E. Then there is an a satisfying φ such that $SU(a/E) = SU(\varphi)$.*

(4) *(The S_1-property for formulas of arbitrary rank) Let $\varphi(x)$, $\psi(x, y)$ be formulas over E, with $\psi(x, y) \to \varphi(x)$, α an ordinal, and assume that there is a sequence $(b_i)_{i\in\mathbb{N}}$ of indiscernibles over E satisfying, for all integers $i \neq j$,*

$$SU(\psi(x, b_i)) = \alpha > SU(\psi(x, b_i) \wedge \psi(x, b_j)).$$

Then $SU(\varphi) > \alpha$.

Proof. (1) Take a satisfying φ such that $SU(a/E) = n$; then every formula ψ satisfied by a has rank at least n, and therefore $S_1(a/E) = n$.

(2) is clear. For (3), let a be any tuple and $b \subseteq a$ a transformal transcendence basis of a over E. Then $SU(a/E) = SU(a, b/E)$, and $SU(b/E) = \omega|b|$. From the SU-rank inequality, we deduce that $\omega|b| \leq SU(a/E) \leq \omega|b| + deg_\sigma(a/Eb)$.

Let $m \in \mathbb{N}$ be the maximal transformal transcendence degree over E of a realisation of φ. By compactness, there is an integer n such that if a realises φ and is of transformal transcendence degree m over E, and $b \subseteq a$ is a transformal transcendence basis of a over E, then $deg_\sigma(a/Eb) \leq n$. By the above we deduce that $\omega m \leq SU(\varphi) \leq \omega m + n$. This implies that $SU(\varphi) = SU(a/E)$ for some realisation a of φ of transformal transcendence degree m over E.

(4) Enlarging E if necessary, and passing to a subsequence of b_i's, we may assume that the b_i's are independent over E. By (3), there is a realisation a of $\psi(x, b_1)$ with $SU(a/Eb_1) \geq \alpha$. Reason as in the step $S_1(\varphi) > n \Rightarrow SU(\varphi) > n$ of the proof of the proposition to conclude that a and b_1 are not independent over E. Thus $SU(\varphi) \geq SU(a/E) > SU(a/Eb_1) \geq \alpha$.

(2.13) Canonical bases. Let E be a difference field, and a a tuple. We define the canonical base of $tp(a/E)$, $Cb(a/E)$, as the smallest perfect difference field over which $I(a/E)$ is defined; since it is a priori infinite, we will extend this notation and write $c = Cb(a/E)$ whenever c is a tuple such that $cl_\sigma(c) = Cb(a/E)$; thus $Cb(a/E)$ is only defined up to definability. Observe that, working in the pure field language, $Cb(a/E)$ is simply the canonical base of $tp((a)_\sigma/E)$ (which may be non-stationary).

Lemma. *Let a, E be as above.*

1. *$tp(a/E)$ does not fork over $Cb(a/E)$.*
2. *For some n, $Cb(a/E)$ is contained in the algebraic closure of the difference field generated by n independent realisations of $tp(a/E)$.*
3. *For some n, $Cb(a/E)$ is contained in the perfect closure of the difference field generated by n independent realisations of $qftp(a/E)$.*
4. *If $dcl(E) \cap E(a)_\sigma$ is purely inseparable over E, then for some n, $Cb(a/E)$ is contained in the (perfect closure of the) difference field generated by n independent realisations of $tp(a/E)$. This happens in particular if E is relatively separably closed in $E(a)_\sigma$*
5. *Assume that $SU(a/E) = n < \omega$. Then $SU(a/Eb) = n - 1$ for some b with $SU(b/E) < \omega$.*

Proof. (1) – (3) follow from the definition of Cb and from analogous facts in algebraically closed fields (note for (3) that $I(a/E)$ depends only on $qftp(a/E)$).

(4) If E is relatively separably closed in $E(a)_\sigma$, this follows from the analogous result in algebraically closed fields. Let a be separably algebraic over E, and consider the tuple b encoding the set of conjugates of a over E; then $b \in dcl(E)$. From this one deduces the result.

(5) Let $F \supseteq E$ be such that $F = acl_\sigma(F)$ and $SU(a/F) = n-1$. Then $Cb(a/F)$ is contained in the algebraic closure of finitely many realisations of $tp((a)_\sigma/F)$ and therefore has finite transcendence degree over E; since it is stable under σ, its SU-rank over E is finite.

(2.14). Recall that if K is a field and a a finite tuple in some overfield of K, then $K(a)$ is a *primary extension* of K iff $K(a) \cap K^s = K$. Then the K-irreducible algebraic set V having a for generic is a variety (i.e., is absolutely irreducible). Note that the field of definition of V (in the sense of algebraic geometry) can be a purely inseparable extension of K.

Lemma (see 7.23.11 in [5])**.** *We work over a difference field E. Let $\varphi(x,y)$ be a quantifier-free formula satisfied by the tuple (a,b), and assume that $E(a,b)_\sigma$ is a primary extension of $E(a)_\sigma$. Let $c \subseteq b$ be a transformal transcendence basis for $E(a,b)_\sigma$ over $E(a)_\sigma$, let ℓ be its size and $n = deg_\sigma(b/E(a,c)_\sigma)$.*

Then for some quantifier-free formula $\delta(x)$ satisfied by a, whenever $\delta(a')$ holds, then there is b' such that $\varphi(a',b')$ holds, and if $c' \subseteq b'$ corresponds to $c \subseteq b$, then c' is a transformal transcendence basis for $E(a',b')_\sigma$ over $E(a')_\sigma$, and $n = deg_\sigma(b'/E(a',c')_\sigma)$.

Proof. Replacing a by $a^\frown\sigma(a)^\frown\cdots^\frown\sigma^k(a)$ and similarly for b, replacing elements of c by their images under appropriate powers of σ^{-1}, and strengthening $\varphi(x,y)$ if necessary, we will assume the following:

- The tuple c is transcendental over $E(a)_\sigma(\sigma(b))$.
- Let $d = \{\sigma^k(c) \mid k \in \mathbb{Z}\} \cap \{b, \sigma(b)\}$; then $\sigma(b) \in E(a,\sigma(a),d,b)^{alg}$ and $n = tr.deg(b/E(a,\sigma(a),d))$.
- $E(a,\sigma(a),b,\sigma(b))$ is a primary extension of $E(a,\sigma(a))$.
- The formula $\varphi(x,y)$ is of the form $(x,y,\sigma(x),\sigma(y)) \in W \wedge p(x,y) \neq 0$, for some polynomial $p(x,y) \in E[x,y]$ and variety $W \subseteq V \times \sigma(V)$ projecting generically onto V and $\sigma(V)$; the formula $(x,y,\sigma(x),\sigma(y)) \in W$ determines $qftp(a,b/E)$.

We work in the context of pure algebraically closed fields, and view W as a variety in the (x,y,x_1,y_1)-plane. Observe that since $E(a,\sigma(a),b,\sigma(b))$ is a primary extension of $E(a,\sigma(a))$, the set $W(a,\sigma(a))) =_{\text{def}} \{(y,y_1) \mid (a,y,\sigma(a),y_1) \in W\}$ is a variety, projecting generically onto the varieties $V(a)$ and $\sigma(V)(\sigma(a))$. There is a quantifier-free formula of the language of fields $\varepsilon(x,x_1)$ satisfied by $(a,\sigma(a))$ and such that whenever $\varepsilon(a',a'_1)$ holds then:

(1) $W(a',a'_1)$ is a variety of dimension $dim(W(a,\sigma(a))$, and projects generically onto $V(a')$ and $\sigma(V)(a'_1)$, which have dimension $dim(V(a))$;
(2) a generic point of $W(a',a'_1)$ satisfies $p(a',y) \neq 0$;
(3) for generic $(b',b'_1) \in W(a',a'_1)$, if $c' \subseteq d' \subseteq b'^\frown b'_1$ correspond to $c \subseteq d \subseteq b^\frown\sigma(b)$, then $tr.deg(c'/E(a',a'_1,b'_1)) = \ell$, $tr.deg(b'/E(a',a'_1,d')) = n$ and $b'_1 \in E(a',a'_1,d',b')^{alg}$.

Let $\delta(x)$ be the formula $\varepsilon(x, \sigma(x))$. Take a' satisfying $\delta(x)$, and let (b', b'_1) be a point of $W(a', \sigma(a'))$, generic over $E(a')_\sigma$; then $p(a', b') \neq 0$, $tr.deg(b'/E(a')_\sigma(b'_1)) = \ell$, and c' is a transcendence basis for b' over $E(a')_\sigma(b'_1)$.

We now need to extend σ (defined on $acl_\sigma(Ea')$) to b'. We define by induction on $i \in \mathbb{N}$ a sequence b'_i, and field isomorphisms $\tau_i : acl_\sigma(Ea')(b'_0, \ldots, b'_i) \to acl_\sigma(Ea')(b'_1, \ldots, b'_{i+1})$ extending σ. At stage 0 let $b'_0 = b'$, and observe that b'_0 and b'_1 are generic points of the varieties $V(a')$ and $\sigma(V)(\sigma(a')) = \sigma(V(a'))$; hence σ extends to an isomorphism $\tau_0 : acl_\sigma(Ea')(b'_0) \to acl_\sigma(Ea')(b'_1)$ sending b'_0 to b'_1. Assume that b'_i and τ_{i-1} are already defined. Let b'_{i+1} be a realisation of a non-forking extension to $acl_\sigma(Ea')(b'_0, \ldots, b'_i)$ of the type image by τ_{i-1} of the type in the pure field language of b'_i over $acl_\sigma(Ea')(b'_0, \ldots, b'_{i-1})$, and define τ_i extending τ_{i-1} by setting $\tau_i(b'_i) = b'_{i+1}$. Then $tr.deg(b'_{i+1}/acl_\sigma(Ea')(b'_0, \ldots, b'_i)) = tr.deg(b'_i/acl_\sigma(Ea')(b'_0, \ldots, b'_{i-1})) = \ell$.

We now take the unique difference field containing $acl_\sigma(Ea')(b'_i)_{i\in\mathbb{N}}$ with automorphism σ extending the τ_i's.

Our choice of the b'_i ensures that the elements of c' form a transformal transcendence basis for $E(a', b')_\sigma$ over $E(a')_\sigma$. Furthermore, since $d' \subseteq b'^\frown\sigma(b')$, and the other transforms of c' are algebraically independent from (b', b'_1) over $E(a')_\sigma$, we have $deg_\sigma(b'/E(a', c')_\sigma) = tr.deg(b'/E(a')_\sigma(d')) = n$, as desired.

(2.15) Lemma. *Let $\varphi(x, y)$ be a formula, $n \in \mathbb{N}$. The set $\{b \mid SU(\varphi(x, b)) \geq n\}$ is open, i.e., a union of 0-definable sets.*

Proof. We will show by induction on n that for every b such that $SU(\varphi(x, b)) \geq n$ there is a formula $\delta(y)$ satisfied by b and such that $\models \delta(b')$ implies $SU(\varphi(x, b')) \geq n$. Assume the result true for $n-1$, and take a satisfying $\varphi(x, b)$ and such that $SU(a/b) \geq n$; choose c with $SU(a/bc) \geq n-1$ such that $tp(a/bc)$ forks over b.

Let $\psi(x, y, z)$ be a quantifier-free formula satisfied by (a, b, c) which witnesses the fact that $tp(c/ab)$ forks over b. That is, we know that either some transformal transcendence basis d of c over b satisfies a non-trivial equation over a, b, or that $deg_\sigma(c/abd) < deg_\sigma(c/bd)$; either of these phenomena can be described by a quantifier-free formula.

Using the induction hypothesis, let $\varepsilon(y, z)$ be a formula satisfied by (b, c) and such that $SU(\psi(x, b', c') \wedge \varphi(x, b')) \geq n-1$ whenever (b', c') satisfy ε.

By (1.6) there are finite tuples $\tilde{b} \in acl_\sigma(b)$, $\tilde{c} \in acl_\sigma(c)$, containing b, c respectively, and a quantifier-free formula $\eta(\tilde{y}, \tilde{z})$ satisfied by $(\tilde{b}, \tilde{c})$, and such that $\eta(\tilde{y}, \tilde{z}) \to \varepsilon(y, z)$. Let k be the prime field, and consider the field $k(\tilde{b}, \tilde{c})_\sigma \cap k(b)^s_\sigma$. It is a difference subfield of a finitely generated difference field, and therefore is finitely generated as a difference field. Enlarging $\tilde{b}$, we may therefore assume that $k(\tilde{b}, \tilde{c})_\sigma$ is a primary extension of $k(\tilde{b})_\sigma$

Let $\theta(\tilde{y})$ be the quantifier-free formula given by (2.14) applied to $(\tilde{b}, \tilde{c})$ and $\eta(\tilde{y}, \tilde{z})$. Write $\tilde{y} = y^\frown y_1$, and let $\delta(y) = \exists y_1\ \theta(\tilde{y})$. Assume that $\delta(b')$ holds, take b'_1 such that $\theta(\tilde{b}')$ holds (for $\tilde{b}' = b'^\frown b'_1$), and take $\tilde{c}'$ generic (in the sense of having maximal transformal and transcendence degrees as in 2.14) satisfying $\eta(\tilde{b}', \tilde{z})$. Then

$$SU(\psi(x, b', c') \wedge \varphi(x, b')) \geq n-1$$

by hypothesis; take a' satisfying $\psi(x, b', c') \wedge \varphi(x, b')$, with $SU(a'/b'c') \geq n-1$. Since a' satisfies $\psi(x, b', c')$ and c' is generic, $tp(c'/a'b')$ forks over b'; by symmetry $SU(a'/b') > SU(a'/b'c') \geq n-1$.

(2.16) Lemma (Weak definability principle)**.** *Let a, b be independent over the difference field E, and let $\varphi(x,y)$ be a formula satisfied by (a,b).*

(1) *Let q be a semi-type of b over E. Then there is a formula $\delta(x)$ satisfied by a and such that, whenever a' satisfies δ, then there is a realisation b' of q which is independent from a' over E and satisfies $\varphi(a',y)$.*

(2) *There are semi-types $p_1 \subseteq tp(a/E)$ and $q_1 \subseteq tp(b/E)$ such that whenever p', q' are complete types over E extending p_1, q_1 respectively, then $p' \times q' \cup \{\varphi(x,y)\}$ is consistent.*

(3) *Let p_1, q_1 be as in (2), and let p', q' be non-forking extensions of p_1 and q_1 respectively to some E' containing E; then $p' \times q' \cup \{\varphi(x,y)\}$ is consistent.*

(4) *Let r be a semi-type over E satisfied by (a,b). There are semi-types $p_1 \subseteq tp(a/E)$ and $q_1 \subseteq tp(b/E)$ such that whenever p', q' are non-forking extensions of p_1, q_1 relative to some E' containing E, then $p' \times q' \cup r$ is consistent.*

Proof. We will assume that $\varphi(x,y)$ is of the form $\exists z \psi(x,y,z)$, where $\psi(x,y,z)$ is a quantifier-free formula (with parameters from E) such that $c' \in acl_\sigma(Ea'b')$ whenever $\psi(a',b',c')$ holds. Let c be such that $\psi(a,b,c)$ holds; let $F = acl_\sigma(Ea)acl_\sigma(Eb)$. Replacing c by $c^\frown\sigma(c)^\frown\cdots^\frown\sigma^k(c)$, we may assume that $[F(c,\sigma(c)) : F(c)] = [F(c,\dots,\sigma^\ell(c)) : F(c,\dots,\sigma^{\ell-1}(c))]$ for all positive ℓ. Choose $\tilde{a} \supseteq a$ in $acl_\sigma(Ea)$ and $\tilde{b} \supseteq b$ in $acl_\sigma(Eb)$ such that $E(\tilde{a},\tilde{b},c)_\sigma$ is a primary extension of $E(\tilde{a})_\sigma$, and F and $E(\tilde{a},\tilde{b})_\sigma(c,\sigma(c))$ are linearly disjoint over $E(\tilde{a},\tilde{b})_\sigma$. Then, because of the degree assumption on $\sigma(c)$, F and $E(\tilde{a},\tilde{b},c)_\sigma$ are linearly disjoint over $E(\tilde{a},\tilde{b})_\sigma$.

(1) Enlarging $\tilde{b}$ if necessary, we will assume that $q = qftp(\tilde{b}/E)$. Let $\psi'(\tilde{x},\tilde{y},z)$ be a quantifier-free formula satisfied by $(\tilde{a},\tilde{b},c)$, which implies $\psi(x,y,z)$ as well as a formula $\theta(\tilde{y})$ determining q.

Let $\varepsilon(\tilde{x})$ be as given by Lemma 2.14 applied to $\tilde{a}$, $(\tilde{b},c)$ and the formula $\psi'(\tilde{x},\tilde{y},z)$; for $\tilde{x} = x^\frown x_1$, define $\delta(x) = \exists x_1 \varepsilon(\tilde{x})$. Let $\tilde{a'}$ satisfy $\varepsilon(\tilde{x})$, and take $(\tilde{b'},c')$ satisfying the conclusion of 2.14 (for $\psi'(\tilde{x},\tilde{y},z)$); given that $\theta(\tilde{b'})$ holds and that the various transcendence degrees (transformal, and ordinary over a transformal transcendence basis) do not change, we deduce that $qftp(\tilde{b'}/E) = qftp(\tilde{b}/E)$, and that $\tilde{a'}$ and $\tilde{b'}$ are independent over E.

(2) Let $p_1'(\tilde{x}) = qftp(\tilde{a}/E)$, $q_1'(\tilde{y}) = qftp(\tilde{b}/E)$, and set $p_1(x) = \exists x_1\, p_1'(x,x_1)$, $q_1(y) = \exists y_1\, q_1'(y,y_1)$. Given that ψ is quantifier-free, it is enough to show the following: if τ is an automorphism of F which agrees with σ on $E(\tilde{a},\tilde{b})_\sigma$, then τ extends to an automorphism of F^{alg} which agrees with σ on $E(\tilde{a},\tilde{b},c)_\sigma$. But this is obvious, since F and $E(\tilde{a},\tilde{b},c)_\sigma$ are linearly disjoint over $E(\tilde{a},\tilde{b})_\sigma$.

(3) Observe first that (2) proves the result for $E' = acl_\sigma(E)$. Apply the independence theorem to p', q', $\varphi(x,y)$ (over $acl_\sigma(E)$).

(4) The semitype $r(x,y)$ is of the form

$$\exists z\, s(x,y,z),$$

where $s(x,y,z) = qftp(a,b,c/E)$ for some $c \in acl_\sigma(E,a,b)$. Since c is field-algebraic over $E(a,b)_\sigma$, $qftp(c/Eab)$ is isolated; thus there is a quantifier-free formula $\psi(x,y,z)$ such that

$$s(x,y,z) = qftp(a,b/E) \cup \{\psi(x,y,z)\}.$$

Apply (3) to the formula $\exists z\, \psi(x,y,z)$.

Remark. Note that if $\varphi(x,y)$ is quantifier-free and E is relatively separably closed in $E(a)_\sigma$ or in $E(b)_\sigma$, one obtains a much stronger result. Indeed, since a and b are independent over E, and the type over E in the pure field language of either a or b is stationary, the formula $\varphi(x,y)$ is implied by a formula satisfied by (a,b), which is of the form $\varphi_1(x) \wedge \varphi_2(y) \wedge h(x,y) \neq 0$ for some formulas φ_1, φ_2, and difference polynomial $h(x,y) \in E\langle x,y\rangle$. Strengthening φ_1, we may assume that $h(a',y)$ is not the zero polynomial whenever $\varphi_1(a')$ holds, and similarly for φ_2. Then we have:

For any types $p'(x)$, $q'(y)$ containing $\varphi_1(x)$ and $\varphi_2(y)$ respectively, $p' \times q' \cup \{\varphi(x,y)\}$ is consistent.

3. Local geometry of forking

(3.1) Definitions. The concepts of orthogonality and triviality have a straightforward generalisation to our (unstable) case. Let p, q be (maybe incomplete) types over A and B respectively, $\varphi(x)$ a formula.

(1) If $A = B$, p is almost orthogonal to q ($p \perp^a q$), if any realisations of p and q are independent over A.
(2) Let $A \subseteq C$. A type p' over C extending p is a non-forking extension of p if some realisation of p' is independent from C over A.
(3) p and q are orthogonal ($p \perp q$) if for every $C \supseteq A \cup B$, if p', q' are extensions of p, q to C which do not fork over A and B respectively, then $p' \perp^a q'$.
(4) p is orthogonal to $\varphi(x)$ ($p \perp \varphi(x)$) if p is orthogonal to any type containing the formula $\varphi(x)$.
(5) The type p of SU-rank 1 is trivial if for any $C \supseteq A$ and realisations $a_1, \ldots, a_n$ of non-forking extensions of p to C, $a_1, \ldots, a_n$ are independent over C if and only if they are pairwise independent.
(6) The complete type p has weight 1 if for some a realising p the following assertion is true: for any tuples b and c, if $tp(a/Eb)$ and $tp(a/Ec)$ fork over E then b and c are not independent over E.

Remarks. (1) Since our notion of independence comes from pure algebraic independence, inspection of the classical proof yields $p \perp q \iff p^{(n)} \perp^a q^{(n)}$ for every $n \in \mathbb{N}$, where $p^{(n)}$ denotes the (maybe incomplete) type $p(x_1) \cup \cdots \cup p(x_n) \cup$ {formulas expressing that $x_1, \ldots, x_n$ are independent over A}.

(2) Note that $\not\perp^a$ is an equivalence relation on types of SU-rank 1. However, $\not\perp$ is a priori not transitive on types of SU-rank 1: this is because of the possibility of many distinct non-forking extensions of the same type. We will see later that it actually is transitive in characteristic 0, because the unstable types of SU-rank 1 are pairwise non-orthogonal. In any case, one easily checks the following: let $p \in S(A)$, $q \in S(B)$ and $r \in S(C)$ be types of SU-rank 1, and assume that $p \not\perp q$, $q \not\perp r$, $B = acl_\sigma(B)$, and A, C are independent over B; then $p \not\perp r$.

(3) Any type of finite SU-rank is orthogonal to the type p_ω. Indeed, assume that $SU(a/E) < \omega$ and b realises $p_\omega(E)$; by (2.4), $SU(b/Ea)$ cannot be finite. Hence it equals ω, i.e., a and b are independent over E.

(4) Using a regular type decomposition or (3.4)(2) in the finite SU-rank case, one can show that the property of having weight 1 as defined above, is preserved under taking non-forking extensions, and therefore coincides with the usual notion of weight 1 used in stability theory.

(3.2) Proposition. *Let p be a non-trivial type of SU-rank 1 (over an algebraically closed substructure E). There exists a formula $\delta(x)$ in p such that $SU(\delta) = 1$.*

Moreover, any two non-algebraic types (over any set E' containing E) in δ are non-orthogonal.

Proof. We work over E. It clearly suffices to prove the following two facts:

(i) Let p be a non-trivial type of SU-rank 1; then there exists a semi-type $q(x)$ contained in p such that $SU(q) = 1$. Moreover any two non-algebraic types over some $E' \supset E$ extending q are non-orthogonal.

(ii) Let q be the above semi-type. Then there exists a formula $\delta(x)$ in q such that $SU(\delta) = 1$. Moreover, any non-algebraic type over E containing δ contains q.

By assumption there are c, a_1, a_2, a_3 such that each a_i realises p and is independent from c; the a_i's are pairwise independent over c, but not independent over c.

Let $\varphi(x_1, x_2, x_3, y)$ be a formula satisfied by a_1, a_2, a_3, c and such that whenever $\varphi(b_1, b_2, b_3, d)$ holds then

(a) $b_2 \in acl_\sigma(d, b_1, b_3)$;
(b) $b_1 \in acl_\sigma(d, b_2, b_3)$;
(c) $deg_\sigma(b_3) \leq deg_\sigma(a_1)$ $(= deg_\sigma(p))$.

Sublemma. *Let $E' \supseteq E$, and assume that $\varphi(b_1, b_2, b_3, d)$ holds for some b_1, b_2, b_3, d such that b_1 is non algebraic over E', $SU(b_2/E') = 1$, $deg_\sigma(b_2/E') = deg_\sigma(p)$ and b_1, b_2 and d are independent over E'.*

Then $SU(b_1/E') = 1$, b_1, b_3, d are independent over E', $b_1 \in acl_\sigma(E', b_2, b_3, d)$, and $deg_\sigma(b_1/E') = deg_\sigma(p)$.

Proof. Using (a) and (c),

$$deg_\sigma(p) = deg_\sigma(b_2/E', b_1, d) \leq deg_\sigma(b_3/E', b_1, d) \leq deg_\sigma(b_3) \leq deg_\sigma(p),$$

so that equality holds everywhere and b_3, and (b_1, d) are independent over E'. Hence, using (b),

$$\begin{aligned} 1 \leq SU(b_1/E') &= SU(b_1/E', d) = SU(b_1/E', b_3, d) \\ &\leq SU(b_2/E', b_3, d) \leq SU(b_2/E') = 1. \end{aligned}$$

Thus, $SU(b_1/E') = 1$, and b_1, b_3 and d are independent over E'; since b_1 and b_2 are not independent over $\{E', b_3, d\}$, they are equi-algebraic over it, and therefore $deg_\sigma(b_1/E') = deg_\sigma(b_1/E', b_3, d) = deg_\sigma(b_2/E', b_3, d) = deg_\sigma(p)$.

We now start with the proof of (i).

Let $\psi(x_1, x_2, y) = \exists x_3\, \varphi(x_1, x_2, x_3, y)$. By (2.16)(3) there are semi-types $q_1(x_1) \subseteq tp(a_1/E)$ and $r(x_2, y) \subseteq tp(a_2, c/E)$ such that whenever p_1 and r' are non-forking extensions of q_1 and r to some $E' \supseteq E$, then $p_1(x_1) \times r'(x_2, y) \cup \{\psi(x_1, x_2, y)\}$ is consistent. By (2.16)(4), there are semi-types $q_2(x_2) \subseteq tp(a_2/E)$ and $s(y) \subseteq tp(c/E)$ such that whenever p_2 and s' are non-forking extensions of q_2 and s to some $E' \supseteq E$, then $p_2(x_2) \times s'(y) \cup r(x_2, y)$ is consistent.

Thus, putting everything together and taking $q(x) = q_1(x) \wedge q_2(x)$, we obtain:

Whenever $E' \supseteq E$ and p_1, p_2 are non-forking extensions of q to E', then $p_1(x_1) \times p_2(x_2) \times s(y) \cup \{\psi(x_1, x_2, y)\}$ is consistent.

Choose (b_1, b_2, d) realising $q(x_1) \times p(x_2) \times s(y) \cup \{\psi(x_1, x_2, y)\}$, and let b_3 be such that $\varphi(b_1, b_2, b_3, d)$ holds; then b_1, b_2, b_3 and d satisfy the hypotheses of the sublemma, and therefore $SU(q) = 1$.

Let p_1, p_2 be non-forking extensions of q to some E' containing E. Choose (b_1, b_2, d) realising $p_1(x_1) \times p_2(x_2) \times s(y) \cup \{\psi(x_1, x_2, y)\}$, and let b_3 be such that

$\varphi(b_1, b_2, b_3, d)$ holds; then b_1, b_2, b_3, d satisfy the hypotheses of the sublemma, and therefore b_1 and b_3, d are independent over E', and $b_1 \in acl_\sigma(E', b_2, b_3, d)$, which shows precisely that $p_1 \not\perp p_2$. This finishes the proof of (i).

By (2.16)(1), there is a formula $\delta(x_1)$ satisfied by a_1 and such that, whenever $\delta(b_1)$ holds, there are (b_2, d) realising $q(x_2) \times s(y)$, independent from b_1 over E, and satisfying $\psi(b_1, x_2, y)$; strengthening $\delta(x_1)$ if necessary, we will assume that $qftp(a_1/E) \cup \{\delta(x_1)\} \vdash q(x_1)$, and that $\delta(x_1)$ determines $qftp(a_1/E)$.

Let b_1 be any realisation of δ non-algebraic over E; choose (b_2, d) realising $q(x_2) \times s(y)$, independent from b_1 over E, and satisfying $\psi(b_1, x_2, y)$, and let b_3 be such that $\varphi(b_1, b_2, b_3, d)$ holds; then b_1, b_2, b_3, d satisfy the hypotheses of the sublemma, and therefore $SU(b_1/E) = 1$ and $deg_\sigma(b_1/E) = deg_\sigma(p)$. Since $\delta(x_1)$ determines $qftp(a_1/E)$, and $deg_\sigma(b_1/E) = deg_\sigma(a_1/E)$, b_1 realises $qftp(a_1/E)$; thus, it satisfies q. This proves (ii).

Remark. All non-algebraic types containing the formula $\sigma(x) = x$ are pairwise non-orthogonal. This comes from the fact that every definable subset of $Fix(\sigma)^n$ is already definable in the field language and using parameters from $Fix(\sigma)$ (see (1.11)), and since every infinite definable subset of $Fix(\sigma)$ generates it (as a ring), see [3].

(3.3) Modularity.

Definitions. Let T be a complete theory, $\mathcal{U}$ a sufficiently saturated model of T, and $E \subseteq \mathcal{U}$ a small set. Let R be a subset of $\mathcal{U}^m$ which is invariant under E-automorphism.

(1) R is modular (over E) if for every $A, B \subseteq R$, A and B are independent over $acl^{eq}(EA) \cap acl^{eq}(EB)$.
(2) Let p be a type over E, and P the set of realisations of p. We say that p is modular if P is modular.

Comments on the terminology. Note that we do not assume that the theory T is stable. Modularity as defined above belongs to a family of closely related notions developed in the seventies and eighties for various classes of stable theories, initially by Lachlan and Zilber in categorical contexts. Our form is closest to the "one-based" variant, but with a more symmetric emphasis. Outside the stable domain it was first used in [4] for certain $\aleph_0$-categorical theories, possessing a rudimentary notion of rank.

Remarks. Let $E = acl_\sigma(E) \subseteq K \models ACFA$.

(1) By elimination of imaginaries, we may replace acl^{eq} by acl_σ in the definition of modular.
(2) It suffices to show modularity for finite subsets A and B.
(3) A trivial type of SU-rank 1 over E is always modular.
(4) We will see below that modularity for types of SU-rank 1 is preserved under non-orthogonality. Thus, if p is modular, then for any $E' = acl_\sigma(E')$ containing E, the set $\{a \mid SU(a/E') = 1,\ tp(a/E') \not\perp p\}$ has a modular geometry.

Lemma. *Let $E = acl_\sigma(E)$.*

(1) *Let A, B be sets, $E_1 = acl_\sigma(EA) \cap acl_\sigma(EB)$, $E_2 \supseteq E_1$, and assume that $A \cup B$ is independent from E_2 over E_1. Then $acl_\sigma(A, E_2) \cap acl_\sigma(B, E_2) = E_2$.*
(2) *Assume that R is modular, let $a \subseteq R$, and B a set. Then a and B are independent over $acl_\sigma(Ea) \cap acl_\sigma(EB)$.*

(3) *Suppose that R is modular (over E) and let $E' \supseteq E$. Then R is modular over E'. Thus a non-forking extension of a modular type is modular.*
(4) *Suppose that R is a union of realisations of modular types of SU-rank 1 over E. Then R is modular.*
(5) *Let $E' = acl_\sigma(E')$, and let p be a type over E and q a type over E', both of SU-rank 1. If p is modular and q is non-orthogonal to p, then q is modular.*
(6) *If R is modular and consists of elements of SU-rank 1 over E and $A, B \subseteq R$, then A and B are independent over $\{c \in acl_\sigma(EA) \cap acl_\sigma(EB) \mid SU(c/E) \leq 1\}$.*
(7) *Suppose $p = tp(d/E)$ is modular of SU-rank 1. If c and b are independent over E, then dc and b are independent over $acl_\sigma(Edc) \cap acl_\sigma(Eb)$.*
(8) *Suppose c and b are independent over E, e is independent from cd over E, $tp(d'/Ee)$ is modular of SU-rank 1, and $d \in acl_\sigma(E, c, e, d')$. Then dc and b are independent over $acl_\sigma(Edc) \cap acl_\sigma(Eb)$.*
(9) *Assume that $\{c_i \mid i < \omega\}$ is independent over E, $\{c_i d_i \mid i < \omega\}$ is indiscernible over E, and $tp(d_i/Ec_i)$ is modular of SU-rank 1. If the $c_i d_i$ are independent in pairs over E, then they are independent over E.*

Proof. (1) This reduces immediately to the case of pure fields.

(2) By (2.13) there is $d \subseteq R$ independent from a over EB and such that $Cb(a/EB) \subseteq acl_\sigma(Ed)$; then $acl_\sigma(Ea) \cap acl_\sigma(Ed) \subseteq acl_\sigma(Ea) \cap acl_\sigma(EB)$, and therefore a and d are independent over $acl_\sigma(Ea) \cap acl_\sigma(EB)$. This gives the result.

(3) Let $a, b \subseteq R$, let $C = acl_\sigma(E'a) \cap acl_\sigma(E'b)$, and choose a set d of realisations of $tp(a, b/C)$ independent from ab over C and such that $Cb(a, b/C) \subseteq acl_\sigma(d)$; by (1), $acl_\sigma(E'da) \cap acl_\sigma(E'db) = acl_\sigma(Cd)$, and therefore $acl_\sigma(E'da) \cap acl_\sigma(E'b) = acl_\sigma(Cd) \cap acl_\sigma(E'b) = acl_\sigma(C)$ and $acl_\sigma(Eda) \cap acl_\sigma(Eb) = C_0 \subseteq C$. Since R is modular, this implies that da and b are independent over C_0. From $C_0 \subseteq C \subseteq acl_\sigma(d)$, we deduce that a and b are independent over C.

(4) Use (1) to reduce to orthogonal types.

(5) Using (1), the assertion is clear if $E = E'$. Take $E'' = acl_\sigma(E'')$ containing E and E', and assume that p is modular, but q is not. By (1) and the fact that $E' = acl_\sigma(E')$, the set of realisations of q independent from E'' over E' is not modular, and therefore, by (3) q has a non-forking extension q' to E'' which is not modular. Taking a non-forking extension p' of p to E'' which is non-orthogonal to q' gives us the result, by (3) and the first case.

(6) This is proved by induction on the size of A. If A contains only one element, then there is nothing to prove. Assume the result proved for $A = \{a_1, \ldots, a_n\}$, and let $a \in R$ be independent from A over E. Without loss of generality we may also assume that $a_1, \ldots, a_n$ are independent over E. Let $C = acl_\sigma(EA) \cap acl_\sigma(EB)$. If Aa and B are independent over C, then there is nothing to prove. If $a \in acl_\sigma(EB)$, then Aa and B are independent over $Ca \subseteq acl_\sigma(EAa) \cap acl_\sigma(EB)$, and we are done. Assume therefore that $a \in acl_\sigma(CAB)$, $a \notin acl_\sigma(EB)$. Since the elements of R have SU-rank 1 over E, there is some index i such that a and a_i are equi-algebraic over $acl_\sigma(CB, A \setminus \{a_i\})$, and $a_i \notin acl_\sigma(CB, A \setminus \{a_i\})$. Let $A_0 = A \setminus \{a_i\}$. Then $C \subseteq acl_\sigma(EA_0)$, because $a_i \notin acl_\sigma(A_0 C)$.

Then there is $c \in acl_\sigma(Eaa_i) \cap acl_\sigma(CBA_0)$ such that (a, a_i) and CBA_0 are independent over $acl_\sigma(Cc)$. Since $a_i \notin acl_\sigma(CBA_0)$ and (a, a_i) and CBA_0 are not independent over E, we get $SU(c/E) = 1$. Then $acl_\sigma(Eac) = acl_\sigma(Ea_i c)$.

Now consider A_0c and B. Since a is independent from A over E, $c \notin acl_\sigma(EA)$. Since $c \in acl_\sigma(CBA_0)$, this implies that (A_0, c) and B are not independent over C. By (5) and by induction hypothesis, (A_0, c) and B are independent over $\{d \in acl_\sigma(EA_0c) \cap acl_\sigma(EB) \mid SU(d/E) = 1\}$. This gives us the result.

(7) The assertion is obvious if $d \in acl_\sigma(Eb) \cup acl_\sigma(Ec)$, or if $d \notin acl_\sigma(Ebc)$; we will therefore assume that $d \in acl_\sigma(Ebc)$, $d \notin acl_\sigma(Eb) \cup acl_\sigma(Ec)$. Let P be the set of realisations of p. By (1) we may enlarge E to any bigger E' independent from $Ebcd$ over E. We choose such an E' with $SU(c/E', (acl_\sigma(E'c) \cap P))$ least possible (in the sense that no bigger E' makes this rank smaller). Let $C = acl_\sigma(E'c) \cap P$.

Claim. $d \in acl_\sigma(E'Cb)$.

First note that c and b are independent over $E'C$. Suppose that $d \notin acl_\sigma(E'Cb)$ and let (b_1, d_1) be a realisation of $tp(b, d/acl_\sigma(E'c))$, independent from (b, d) over $acl_\sigma(E'c)$. Then b_1 and (b, c) are independent over E', and $d_1 \in acl_\sigma(E'b_1c) \cap P$, $d_1 \notin acl_\sigma(E'b_1C)$. Thus $SU(c/E'(b_1), (acl_\sigma(E'b_1c) \cap P)) < SU(c/E'b_1C)$, which contradicts the choice of E'.

We may therefore assume that $c \subseteq P$, and (2) gives us the result.

(8) As in (7), we may assume that $d \in acl_\sigma(Ebc)$, $d \notin acl_\sigma(Eb) \cup acl_\sigma(Ec)$. We will also assume that e is independent from b over Ecd, and hence that bcd and e are independent over E. By (1), it suffices to show that dc and b are independent over $acl_\sigma(Eedc) \cap acl_\sigma(Eeb)$. Let $E' = acl_\sigma(Ee)$. Then $acl_\sigma(Eedc) = acl_\sigma(E'd'c) = acl_\sigma(E'dc)$ and b, c are independent over E'. By (7), $d'c$ and b are independent over $acl_\sigma(E'd'c) \cap acl_\sigma(E'b)$, which gives the result.

(9) It suffices to show that they are independent in triples. Suppose for contradiction they are not. Then $d_i \in acl_\sigma(Ec_ic_jc_kd_jd_k)$ for distinct i, j, k.

Note that:

$$(*) \qquad acl_\sigma(Ec_1d_1) \cap acl_\sigma(Ec_2d_2c_3d_3) = E.$$

Indeed, let

$$u \in acl_\sigma(Ec_2d_2c_3d_3) \cap acl_\sigma(Ec_1d_1);$$

then, by indiscernibility, $u \in acl_\sigma(Ec_id_i)$ for all $i > 3$, which implies that $u \in E$ by the independence in pairs.

Also, for each i there exist e_i independent from c_id_i over E, and d_i' with $tp(d_i'/Ee_i)$ modular of SU-rank 1, and $acl_\sigma(Ee_ic_id_i) = acl_\sigma(Ee_ic_id_i')$, namely: $e_i = (c_jc_kd_j)$ and $d_i' = d_k$.

Thus the hypothesis of (8) holds for c_i, d_i, E. Let $b = c_jc_kd_jd_k$. Then c_i is independent from b over E. By (7) and $(*)$, c_1d_1 is independent from $c_2d_2c_3d_3$ over E. This shows independence in triples after all.

(3.4) Proposition. *Let $E = acl_\sigma(E)$. Suppose that $tp(a/E)$ has finite rank $n > 0$. Then*

1. *There exists c, independent from a, and $d \in acl_\sigma(E, a, c)$ such that $SU(d/E, c) = 1$ and $SU(c/E) < \omega$.*
2. *If $tp(a/E)$ has weight 1, then c can be dispensed with.*
3. *If d and c are as in (1), and $tp(d/E, c)$ is modular, then there exists $e \in acl_\sigma(E, a)$ such that $SU(e/E) = 1$, and $tp(e/E) \not\perp tp(d/E, c)$.*

Proof. We work over E.

(2) Choose b of finite SU-rank (see (2.13)) such that $SU(a/b) = n-1$. Let b' be a realisation of $tp(b/a)$, independent from b over a. Since $tp(a/b)$ and $tp(a/b')$ fork over $\emptyset$, and $tp(a)$ has weight 1, b and b' are dependent. From

$$SU(b/a, b') = SU(b/a) = SU(b) - 1 \geq SU(b/b')$$

we deduce that b and a are independent over b'. We also have b and b' independent over a; hence b is independent from $acl_\sigma(a)acl_\sigma(b')$ over $acl_\sigma(a) \cap acl_\sigma(b')$ (using elimination of imaginaries and the fact that $Cb(b/ab') \subseteq acl(Cb(b/a)) \cap acl(Cb(b/b')) \subseteq acl_\sigma(a) \cap acl_\sigma(b')$). Since a and b are not independent, $acl_\sigma(a) \cap acl_\sigma(b')$ contains an element $d \notin acl_\sigma(\emptyset)$; thus $d \in acl_\sigma(a)$ and $SU(a/d) \geq SU(a/b) = n-1$, so that $SU(d) = 1$.

(1) Let c, b be such that a and c are independent, $SU(a/b, c) = n-1$, $SU(b, c) < \omega$, and $SU(b/c)$ is least possible. Let a' realise $tp(a/b, c)$, independent from a over b, c.

Assume that a and a' are independent over c, and let $c' = (c, a')$; then a is independent from c', $SU(a/b, c') = n-1$, but since a' and b are not independent over c, we must have $SU(b/c') < SU(b/c)$, which contradicts our minimality assumption.

Therefore $SU(a'/c, a) < n$, which implies that $SU(a'/c, a) = n-1$ (because $SU(a'/c, a) \geq SU(a'/b, c, a) = n-1$); so we have that a' is independent from a over (b, c) and from b over (a, c). Reasoning as in (2) gives an element

$$d \in acl_\sigma(a, c) \cap acl_\sigma(b, c) \setminus acl_\sigma(c)$$

such that $SU(a/d) = n-1$; then $SU(d/c) = 1$.

(3) Let c, d satisfy the conclusion of (1), and let $e_i = (c_i, d_i)$, $0 \leq i \leq n$, be indiscernible independent realisations of $tp(c, d/a)$. Since c and a are independent, $c_0, \ldots, c_n, a$ are independent; we also have $SU(a/e_0, \ldots, e_i) \leq SU(a/e_0, \ldots, e_{i-1})$, so equality must hold somewhere, say at $k \leq n$. Then a is independent from e_k over $e_0, \ldots e_{k-1}$.

Since a is not independent from e_k, $\{e_0, \ldots, e_k\}$ cannot be independent. By Lemma 3.3(9), e_i and e_j are not independent for some $i \neq j$ (and hence for all $i \neq j$ by indiscernibility); from $SU(d_i/c_0, \ldots, c_k) = 1$ we deduce that

$$SU(d_0, \ldots, d_k/c_0, \ldots, c_k) = 1.$$

Also, by construction, e_k is independent from $\{e_0, \ldots, e_{k-1}\}$ over a; hence e_k is independent from $acl_\sigma(a)acl_\sigma(e_0, \ldots, e_{k-1})$ over $B = acl_\sigma(a) \cap acl_\sigma(e_0, \ldots, e_{k-1})$ (because $Cb(e_k/a, e_0, \cdots, e_{k-1}) \subseteq acl_\sigma(a) \cap acl_\sigma(e_0, \cdots, e_{k-1})$). Since a and e_k are not independent, $SU(B) > 0$; since $B \subseteq acl_\sigma(a)$, B and $c_0, \ldots, c_k$ are independent, i.e., $SU(B) = SU(B/c_0, \ldots, c_k)$. Then $B \subseteq acl_\sigma(e_0, \ldots, e_k)$ implies $SU(B/c_0, \ldots, c_k) \leq 1$, i.e. $SU(B) = 1$.

(3.5) Lemma. *Let p be a type over $E = acl_\sigma(E)$ of finite SU-rank, and let $q = tp(b/Ec)$ be a non-trivial type of SU-rank 1. If $p \not\perp q$, there is a formula (with parameters in E) $\delta(x, y)$ satisfied by (b, c), and such that whenever (b', c') satisfies δ and $b' \notin acl_\sigma(Ec')$, then $SU(b'/Ec') = 1$ and $tp(b'/Ec')$ is non-orthogonal to p and q.*

If $E \models ACFA$, there is a formula φ over E of SU-rank 1, and such that every non-algebraic type in φ is non-orthogonal to p and to q.

Proof. We work over E. Enlarging c if necessary, we may assume that p is not almost orthogonal to q over c. Let a realise p, independent from c.

Let c' realise $tp(c)$, independent from c over a, and let q' be the corresponding conjugate of q (over E).

Claim. $q \not\perp q'$.

By the independence theorem (1.9) there is a sequence $(c_i)_{i\in\mathbb{N}}$ of realisations of $tp(c/a)$, independent over a, such that $tp(c_i, c_j/a) = tp(c, c'/a)$ for $i < j$. Let q_i be the corresponding conjugate of q. Since $p \not\perp^a q$, for each i there is a realisation b_i of q_i in $acl_\sigma(c_i, a)$. If q and q' are orthogonal, then so are q_i and q_j for $i \neq j$, and the elements b_i are independent over $\{c_0, c_1, \dots\}$, yet a is not independent from any b_i over $\{c_0, c_1, \dots\}$, a contradiction.

The proof now follows very closely the lines of the proof of (3.2). Enlarging c if necessary, we may assume that the types q and q' above are not almost orthogonal over c, c', and that the non-triviality of q is witnessed over c by some triple of realisations of q. Choose independent realisations c_1 and c_2 of $tp(c)$, and b_1, b_2, b_3 pairwise independent over c_1, c_2 but not independent, and such that $tp(b_1, c_1) = tp(b_2, c_2) = tp(b_3, c_2) = tp(b, c)$.

Let $\varphi(x_1, x_2, x_3, y_1, , y_2)$ be a formula satisfied by b_1, b_2, b_3, c_1, c_2 and such that whenever $\varphi(b'_1, b'_2, b'_3, c'_1, c'_2)$ holds then

(a) $b'_2 \in acl_\sigma(c'_1, c'_2, b'_1, b'_3)$;
(b) $b'_1 \in acl_\sigma(c'_1, c'_2, b'_2, b'_3)$;
(c) $deg_\sigma(b'_3/c'_2) \leq deg_\sigma(b/c)$.

As in (3.2), one argues as follows. Let $E' \supseteq E$ and assume $\varphi(b'_1, b'_2, b'_3, c'_1, c'_2)$ holds for some $b'_1, b'_2, b'_3, c'_1, c'_2$ such that: $b'_1 \notin acl_\sigma(E', c'_1)$; $SU(b'_2/E', c'_2) = 1$ and $deg_\sigma(b'_2/E', c_2) = deg_\sigma(b/E, c)$; b'_1 and b'_2 are independent over E', c'_1, c'_2. Then $SU(b'_1/E', c'_1) = 1$, b'_1 and b'_3 are independent over E', c'_1, c'_2, and

$$b'_1 \in acl_\sigma(E', c'_1, c'_2, b'_2, b'_3).$$

Let $\psi(x_1, x_2, y_1, y_2) = \exists x_3\, \varphi(x_1, x_2, x_3, y_1, y_2)$ and choose a semi-type $r(x, y) \subseteq tp(b, c)$ such that whenever $r_1(x_1, y_1)$, $r_2(x_2, y_2)$ are non-forking extensions of r to some E' containing E, then $r_1 \times r_2 \cup \{\psi(x_1, x_2, y_1, y_2)\}$ is consistent. If (b'_i, c'_i) satisfies r_i for $i = 1, 2$, then $SU(b'_i/E', c'_i) = 1$, and moreover, if c'_1 and c'_2 are independent over E', then $tp(b'_1/E', c'_1)$ and $tp(b'_2/E', c'_2)$ are non-orthogonal.

Using (2.16)(1), let $\delta(x, y)$ be a formula satisfied by (b, c) and such that, whenever $\delta(b'_1, c'_1)$ holds, then there are (b'_2, c'_2) realisations of $r(x, y)$, independent from (b'_1, c'_1) and such that $\psi(b'_1, b'_2, c'_1, c'_2)$ holds. Assume that $\delta(b'_1, c'_1)$ holds, that $b'_1 \notin acl_\sigma(c'_1)$, and let (b'_2, c'_2) be as above; then $SU(b'_1/c'_1) = 1$, and $tp(b'_1/c'_1)$ and $tp(b'_2/c'_2)$ are non-orthogonal.

Let (b'_1, c'_1) satisfy δ, with $b'_1 \notin acl_\sigma(c'_1)$. Choose (b'_2, c'_2) independent from c, b'_1, c'_1, realising r, and such that $tp(b'_2/c'_2) \not\perp tp(b'_1/c'_1)$; we also know that any two non-forking extensions of $tp(b/c)$ and $tp(b'_2/c'_2)$ are non-orthogonal (from the definition of r). This implies that $tp(b'_1/c'_1)$ is non-orthogonal to any non-forking extension of $tp(b/c)$, and therefore also to p. Note also that, if $\theta(x, c)$ is the formula given by (3.2) for $tp(b/c)$, then any non-algebraic type in $\theta(x, c)$ is non-orthogonal to any non-algebraic type in $\delta(x, c'_1)$.

If $E \models ACFA$, choose $c_1 \in E$ such that $\delta(x, c_1)$ is infinite, and let $\varphi(x) = \delta(x, c_1)$; if $b_1 \notin E$ satisfies φ, then $tp(b_1) \not\perp q$ and $tp(b_1) \not\perp p$.

(3.6) Lemma. *We work over an algebraically closed substructure E. Let $\varphi(x)$ be a formula of SU-rank 1, let p be a type (over E) of finite SU-rank, non-orthogonal*

to $\varphi(x)$. Then there exists a semi-type $r(y)$ such that, over any element satisfying r, p is not almost orthogonal to φ.

Proof. Let a realise p, let c be independent from a and such that some $b \in acl_\sigma(a,c) \setminus acl_\sigma(c)$ satisfies $\varphi(x)$, and let $\theta(a,c,x)$ isolate $tp(b/a,c)$. We may assume that $c = Cb(a,b/c)$. Using (2.16), let $r(y)$ be a semi-type satisfied by c and such that whenever $r(c')$ holds, there exists a' realising p, independent from c' and such that $\exists x\, \theta(a',c',x) \wedge \varphi(x)$.

Let c' satisfy r, let a' realise p, independent from c', and let b' be such that $\models \theta(a',c',b') \wedge \varphi(b')$. By our choice of θ, $deg_\sigma(a'/b',c') < deg_\sigma(a') = deg_\sigma(a'/c')$; hence $SU(b'/c') = 1$, which implies that $tp(a'/c') \not\perp^a tp(b'/c')$.

(3.7). We conclude this section with some comments on non-orthogonality to the fixed field F, i.e., to the formula $\sigma(x) = x$.

Proposition. *Let A be a difference field, a a tuple with $SU(a/A) < \omega$.*

1. *$acl_\sigma(A) \cap F = (A \cap F)^{alg} \cap F$.*
2. *Assume that $tp(a/A) \not\perp (\sigma(x) = x)$. Then there are quantifier-free formulas $\varphi(x)$ and $\psi(y)$, with parameters in A, and a difference polynomial $h(x,y)$ over A, such that $\models \exists y\ \varphi(a) \wedge \psi(y) \wedge h(a,y) \neq 0$, and for every a',c' satisfying $\varphi(a') \wedge \psi(c') \wedge h(a',c') \neq 0$, there is some $b' \in A(a',c')_\sigma \cap F$ such that $SU(a'/A,b',c') < SU(a/A)$.*

In particular, if a' realises $qftp(a/A)$, then $tp(a'/A)$ is not almost orthogonal to $(\sigma(x) = x)$ over any element satisfying ψ.

3. *Let a be a tuple of elements of the fixed field. Then $Cb(a/A)$ is contained in (the perfect hull of) $A \cap F$.*
4. *Let p be a type over A. If $p \perp^a (\sigma(x) = x)$, then $p \perp^a \left(\bigwedge_{i=1}^n \sigma(x_i) = x_i\right)$.*

Proof. (1) If a is fixed by σ and is algebraic over A, then the coefficients of the minimal (monic) polynomial of a over A are also fixed by σ.

(2) Take c independent from a over A and b fixed by σ, such that

$$b \in acl_\sigma(A,a,c) \setminus acl_\sigma(A,c);$$

by (1), we may assume that $b \in A(a,c)_\sigma$. Write b as $f(a,c)/g(a,c)$ for some difference polynomials $f(x,y)$, $g(x,y)$ over A. Thus we have a difference polynomial $h(x,y)$ with $h(a,c) \neq 0$, and quantifier-free formulas $\varphi(x)$ and $\psi(y)$ satisfied by a and c respectively, such that, if $\models \varphi(a') \wedge \psi(c') \wedge h(a',c') \neq 0$, then the element $b' = f(a',c')/g(a',c')$ is defined, is fixed by σ, and $SU(a'/A,b',c') < SU(a/A)$.

(3) Working in the pure field language, let V be the irreducible algebraic set defined over A of which a is a generic point. Then $\sigma(V) = V$ since $a \in V \cap \sigma(V)$ (and if $V \neq \sigma(V)$, then $dim(V \cap \sigma(V)) < dim(V)$). The field B of definition of V is fixed by every automorphism leaving V invariant, in particular by σ. Thus B is contained in the perfect hull of $A \cap F$.

(4) Let b realise p, and let a be a tuple of elements of F such that a and b are not independent over A. Then $Cb(a/A,b)$ is not contained in $acl_\sigma(A)$ and by (3) is contained in the perfect hull of $A(b)_\sigma \cap F$; hence some element of $Cb(a/A,b)$ witnesses $p \not\perp^a (\sigma(x) = x)$.

The point in (4) is that if a realization of p can fork with a tuple from the fixed field, it can fork over the same base with a single element of the fixed field.

4. Study of rank-one types - The dichotomy

The main result of this section is a dichotomy theorem for types of rank 1 in characteristic 0. We start with some definitions: bounded, unbounded and superficially stable types. The dichotomy is then: a rank-1 type is either bounded of σ-degree 1 and non-orthogonal to the fixed field, or it is superficially stable, modular. In the latter case, the type will be stable and stably embedded, and a minimal type in the sense of stability (see the Appendix).

The proof that a bounded type is non-orthogonal to the fixed field works in all characteristics, and is given in (4.5). To show the second part of the dichotomy, we need preliminary results: a description of the consequences of superficial stability, given in (4.2) and (4.3), and some results on ramification of discrete valuations (4.6) and (4.7). The proof of the main result is then given in (4.10), and we conclude the section with some easy applications.

(4.1) Definitions and notation. (1) Let p be a type defined over an algebraically closed structure E. We say that p is *superficially stable* if for every realisation a of p, and algebraically closed structure F containing E and independent from a over E, the field $F(acl_\sigma(Ea))$ has no proper finite σ-stable Galois extension.

(2) Let p and q be types over an algebraically closed structure E; we say that p and q are *superficially co-stable* iff for all independent over E realisations a and b of p and q respectively, the field $acl_\sigma(Ea)acl_\sigma(Eb)$ has no proper finite σ-stable extension. Note that this relation is symmetric.

(3) Let E be an algebraically closed structure. For k a positive integer and $a \in M$ realising a complete type p, we denote by $p[k]$ or $tp_k(a/E)$ the type of the element a over E in the model M_k, reduct of M to the language $\{+, \cdot, 0, 1, \sigma^k\}$. We denote by $qftp_k(a/E)$ the quantifier-free part of $tp_k(a/E)$.

(4) For E a field and a a tuple algebraic over E, we define $\mathrm{Mult}(a/E)$ to be the (separable) degree $[E(a) : E]_s$ (i.e., the multiplicity of a over E in the pure field language).

(5) Let p be a complete type over an algebraically closed substructure E. Let a realise p and assume that $\sigma(a) \in E(a)^{alg}$. We say that p is *bounded* if there is a natural number N such that for every integer k (positive or negative) $\mathrm{Mult}(\sigma^k(a)/E(a)) \leq N$; if no such N exists, we say that p is *unbounded*.

(4.2) Theorem. *Let p be an n-type over an algebraically closed structure E, realised by some tuple a.*

1. *Assume p has a unique non-forking extension to any difference field F containing E. Let $\alpha \in acl_\sigma(E, a)$. Then $tp(a, \alpha/E)$ has the same property.*
2. *p is superficially stable if and only if for each m, $tp_m(a, \sigma(a), \ldots, \sigma^{m-1}(a)/E)$ has a unique non-forking extension to any difference field F containing E.*

Assume now that p is superficially stable. Then

3. *If F contains E, then p has a unique non-forking extension q to F, and q is superficially stable.*
4. *If p does not fork over the algebraically closed substructure E' of E, then $p|_{E'}$ is superficially stable.*
5. *$p \perp (\sigma(x) = x)$.*
6. *If M is a model of $ACFA$ containing E, then the non-forking extension of p to M is definable over E.*

Assume now in addition that $SU(p) = 1$, and let P be the set of realisations of p.

(7) *If $D \subseteq K^n$ is definable, then $D \cap P$ is either finite or cofinite. If $F \supseteq E$, then p has at most $|F| + \aleph_0$ extensions to F.*
(8) *For every tuple a in P and every algebraically closed substructure F_1 containing E, $tp(a/F_1)$ is superficially stable.*
(9) *p is stably embedded, i.e., if $D \subseteq M^{nm}$ is definable with parameters, then $D \cap P^m$ is definable with parameters from P.*

Proof. (1) Assume by way of contradiction that $tp(a, \alpha/E)$ has two distinct non-forking extensions to some difference field F_1 containing E. Let $F_2, \ldots, F_n$ realise $tp(F_1/E)$, with $F_1, \ldots, F_n$ independent over E. Applying the independence theorem, we get that $tp(a, \alpha/E)$ has at least 2^n distinct non-forking extensions $p_i(x, y)$ to $F_1 \cdots F_n$. The restrictions of $p_i(x, y)$ to the tuple of variables x (corresponding to a) are non-forking extensions of p, hence are all equal. Thus there exist α_i with (a, α_i) realizing p_i. The α_i must be 2^n distinct elements, a contradiction if $2^n > [E(a)_\sigma(\alpha) : E(a)_\sigma]$.

(2) Assume that p is superficially stable. Let $F = acl_\sigma(F)$ contain E and be independent from a over E. By superficial stability, the field $K = Facl_\sigma(Ea)$ has no proper finite σ-stable Galois extension. Hence, by (2.8), all extensions of $\sigma|_K$ to $acl_\sigma(Fa)$ are K-isomorphic, which gives the uniqueness of the non-forking extension of p to F.

By (2.9), $Facl_\sigma(Ea)$ has no proper finite σ^m-stable Galois extension. Observing that $acl_\sigma(Ea) = acl_{\sigma^m}(E, a, \sigma(a), \ldots, \sigma^{m-1}(a))$, the first part gives the uniqueness of the non-forking extension of $tp_m(a, \sigma(a), \ldots, \sigma^{m-1}(a)/E)$ to F.

For the converse, assume by way of contradiction that for some $F = acl_\sigma(F)$ containing E and independent from a over E, the field $K = Facl_\sigma(Ea)$ has a proper finite σ-stable Galois extension L. Choose $\alpha \in acl_\sigma(Ea)$ such that L is the composite of K with some finite Galois extension L_1 of $F(a, \alpha)_\sigma$. Enlarging α, we may assume that $\sigma(L_1) = L_1$. By (2.9), for some m there is $\sigma_1 \in Aut(L_1)$ which agrees with σ^m on $F(a, \alpha)_\sigma$ but is not conjugate to σ^m under any element of $\mathcal{G}al(L_1/F(a, \alpha)_\sigma)$. This implies that $tp_m(a, \sigma(a), \ldots, \sigma^{m-1}(a), \alpha, \sigma(\alpha), \ldots, \sigma^{m-1}(\alpha)/E)$ has two distinct non-forking extensions to F, and contradicts (1).

(3) Immediate from (2).

(4) Suppose that $tp(a/E')$ is not superficially stable. Then there is $F = acl_\sigma(F)$ containing E' and such that $acl_\sigma(E'a)F$ has a proper finite σ-invariant Galois extension L. By the independence theorem, we may assume that F, E and a are independent over E', which implies that E and F are independent over $acl_\sigma(E'a)$. This implies (see e.g. Remark 1.9) that $(acl_\sigma(E'a)F)^{alg} \cap acl_\sigma(Ea)F = acl_\sigma(E'a)F$, and therefore that $Lacl_\sigma(Ea)F$ is a proper extension of $acl_\sigma(Ea)F$. This contradicts the superficial stability of $tp(a/E)$.

(5) Assume that $p \not\perp (\sigma(x) = x)$, and let $F = acl_\sigma(F)$ containing E be independent from a over E and such that $acl_\sigma(F, a) \setminus F$ contains an element α fixed by σ. Choose β fixed by σ, independent from Fa over E, let $F' = acl_\sigma(F, \beta) = F(\beta)^{alg}$, and fix a prime number $\ell \neq char(F)$.

We claim that the equation $X^\ell = \alpha + \beta$ does not have a solution in $F'acl_\sigma(Fa)$. Indeed, $(\alpha + \beta)$ is not an ℓ-th power in $acl_\sigma(Fa)(\beta)$, because it has degree 1 in β. Assume by way of contradiction that there is c in $F'acl_\sigma(Fa)$ such that $c^\ell = \alpha + \beta$. Then $acl_\sigma(Fa)(\beta, c)$ is a Galois extension of degree ℓ of $acl_\sigma(Fa)(\beta)$, contained in

$F'acl_\sigma(Fa)$. Since β is transcendental over $acl_\sigma(Fa)$, we have $F' \cap acl_\sigma(Fa)(\beta) = F(\beta)$, and therefore $acl_\sigma(Fa)(\beta, c) = acl_\sigma(Fa)L$ for some Galois extension L of $F(\beta)$ of degree ℓ. By Kummer theory, there is $d \in L$ such that $d^p \in F(\beta)$ and $cd^{-1} \in acl_\sigma(Fa)(\beta)$. Let $h_1, h_2 \in acl_\sigma(Fa)[\beta]$ and $d_1, d_2 \in F[\beta]$ be such that $cd^{-1} = h_1/h_2$ and $d^\ell = d_1/d_2$. We may assume that d_1 and d_2, and h_1 and h_2, are relatively prime in $acl_\sigma(Fa)[\beta]$. We then have

$$(\alpha + \beta)h_2^\ell d_2 = h_1^\ell d_1.$$

Let $\beta - u$ be an irreducible factor of d_1. In $acl_\sigma(Fa)[\beta]$ it is relatively prime to $\alpha + \beta$, since $u \in F$. Hence the above equation implies that $(\beta - u)$ divides h_2, and therefore that $(\beta - u)^\ell$ divides $h_1^\ell d_1$, and hence divides d_1 (since $(h_1, h_2) = 1$). Thus d_1 is an ℓ-th power in $acl_\sigma(Fa)[\beta]$. Reasoning in the same way with d_2, we reach a contradiction.

Hence, the roots of the equation $X^\ell - \alpha - \beta$ generate a finite proper Galois extension of $acl_\sigma(Ea)F'$, stable under σ. Thus p is not superficially stable.

Note that $tp(a/F)$ has (at least) two distinct non-forking extensions to F': let $\psi(x, y)$ be the formula such that $\psi(a, y)$ isolates $tp(\alpha/Fa)$ and consider the formula $\varphi(x, \beta) = \exists y, z\ \psi(x, y) \wedge (z^\ell = y + \beta) \wedge \sigma(z) = z)$. Then both $tp(a/F) \cup \{\varphi(x, \beta)\}$ and $tp(a/F) \cup \{\neg\varphi(x, \beta)\}$ extend to non-forking extensions of $tp(a/F)$ over F'. This implies in particular (using the independence theorem) that no non-forking extension of $tp(a/F)$ is definable.

(6) This is in fact a direct consequence of (3) (and does not need E to be algebraically closed). Let $M \supseteq E$ be a model of $ACFA$, and p' the non-forking extension of p to M. Let $A \supseteq M$. By Lemma 1.15 of [25], there is a type q over A, heir of p'. We claim that q is a non-forking extension of p: let a realise q; then for every $c \in cl_\sigma(Ma)$, $tp(c/A)$ is an heir of $tp(c/M)$, which implies that the fields $cl_\sigma(Ma)$ and $cl_\sigma(A)$ are linearly disjoint over M, and therefore that $tp(a/A)$ does not fork over M.

Hence, for every $A \supseteq M$, p' has exactly one heir on A. By Proposition 1.17 of [25], p' is definable. Since p' is left invariant by any E-automorphism of M (because it is the unique non-forking extension of p to M), we see that it is definable over E.

(7) Obvious, since all forking extensions of p are algebraic.

(8) This is shown by induction on the length of the tuple a. Let $a \in P^m$, $b \in P$, and assume that the result holds for all m-tuples, but does not hold for (a, b) over some algebraically closed substructure F_1 containing E. Without loss of generality, $F_1 = E$; then $b \notin acl_\sigma(Ea)$. Let $F = acl_\sigma(F)$ be independent from (a, b) over E, such that the field $K = Facl_\sigma(Eab)$ has a proper finite Galois extension L which is stable under σ.

$Lacl_\sigma(Fa)$ is a finite Galois extension of $acl_\sigma(Fa)acl_\sigma(Eab)$, stable under σ, and therefore must equal $acl_\sigma(Fa)acl_\sigma(Eab)$, because $tp(b/acl_\sigma(Ea))$ is superficially stable by (2). Hence, $L \subseteq acl_\sigma(Fa)acl_\sigma(Eab)$. Since L is a proper finite Galois extension of $K = Facl_\sigma(Eab)$, there is $\alpha \in acl_\sigma(Fa)$ such that $L = K(\alpha)$. Note that $\alpha \notin Facl_\sigma(Ea)$, and that $\sigma(\alpha) \in acl_\sigma(Fa) \cap K(\alpha)$. Since b is independent from Fa over E, this implies that $\sigma(\alpha) \in Facl_\sigma(Ea)(\alpha)$ (use Remark (1.9)(2)), and therefore that $Facl_\sigma(Ea)(\alpha)$ is stable under σ. This contradicts our induction hypothesis.

(9) For an alternate and more direct proof, use (7) and Lemma 2 of the Appendix. Let D be defined by the formula $\varphi(x, b)$, for some tuple b in M. We will

first assume that $E = acl_\sigma(Cb(p))$; thus E is contained in the algebraic closure of a finite subset of P by (2.13). Let $P_0 \subseteq P$ be such that b and P are independent over P_0, and $acl_\sigma(P_0) \supseteq E$. Let $c \in P^m \cap D$; our choice of P_0 ensures that all extensions of $tp(c/P_0)$ to $P_0 b$ are non-forking extensions. By (8) and (2), $tp(c/acl_\sigma(P_0)) \vdash tp(c/acl_\sigma(P_0), b)$. Thus, using compactness, D is definable over $acl_\sigma(P_0)$, and has therefore only a finite number of distinct conjugates over P_0, say $D = D_1, D_2, \ldots, D_n$; changing the indices, we may assume that $D_i \cap P^m = D \cap P^m$ if and only if $i \leq \ell$. For each $i > \ell$, choose $d_i \in (D_i \cap P^m) \triangle (D \cap P^m)$. Then $\bigcup_{i \leq \ell} D_i$ is definable over $P_1 = P_0 \cup \{d_i \mid \ell < i \leq k\}$, and has the same intersection with P^m as D.

In the general case, let P' be the set of realisations of $p|_C$, where $C = acl_\sigma(Cb(p))$, and let D' be the set of elements of P'^m satisfying $\varphi(x, b)$; then $D' \cap P^m = D$, and by the first case we may assume that $b \in P'$. Choose $P_0 \subseteq P$ such that b and P_0 are independent over P_0, and $acl_\sigma(P_0) \supseteq C$. By choice of P_0, all the extensions of $tp(b/P_0)$ to P are non-forking. Since $p|_C$ is superficially stable, $tp(b/acl_\sigma(P_0)) \vdash tp(b/acl_\sigma(P_0)P)$; by compactness, this implies that D is definable over $acl_\sigma(P_0)$. As above, one deduces that it is definable over P.

(4.3) Theorem. *Let p be a type over $E = acl_\sigma(E)$, of SU-rank 1 and superficially stable. Then p is modular.*

Proof. We work over the parameter set E. Observe that by (4.2), p is stable and stably embedded, and also minimal. By Lemma 4 of the Appendix, it therefore suffices to establish the following fact.

Claim. If $c_1, c_2 \in P^m$ are independent, and $c_0 \in acl_\sigma(c_1, c_2) \cap P$, then there are elements d_i with $acl_\sigma(d_i) = acl_\sigma(c_i)$ for $i = 0, 1, 2$, and with $d_0 \in cl_\sigma(d_1, d_2)$.

We will assume that $tr.deg(c_i) = deg_\sigma(c_i)$, so that acl_σ is the field-theoretic algebraic closure, which we denote by acl. We work in the pure field language. Let $A_1 = acl(c_1)$, $A_2 = acl(c_2)$, and $B = A_1 A_2$ (the composite). Let d code the set of (field-) conjugates of c_0 over B which are equi-algebraic with c_0; then $acl(d) = acl(c_0)$. We claim that $d \in B(\sigma(d))$: otherwise, since B is perfect (because it is the composite of algebraically closed fields), there is $d_1 \neq d$, conjugate of d over $B(\sigma(d))$. Since $acl(d) = acl(\sigma(d))$, this implies that $acl(d_1) = acl(d)$. On the other hand, since d and d_1 are conjugate over B and distinct, we have $acl(d_1) \neq acl(d)$, which gives us a contradiction. Hence $d \in B(\sigma(d))$, which implies that $B(\sigma(d))$ is stable under σ^{-1} and therefore under σ (since $[B(d) : B] = [B(\sigma(d)) : B]$). But B has no finite proper σ-stable extension (by (8)), which implies that $\sigma(d) \in B$. Take $d_0 = d$, $d_1 = A_1$, $d_2 = A_2$.

(4.4) Lemma. *Let E be an algebraically closed structure, let a be a tuple, and assume that $deg_\sigma(a/E) = 1$ and that $[E(a, \sigma^k(a)) : E(a)]$ is bounded by some integer N for every $k \in \mathbb{N}$. Then there is $b \in acl_\sigma(Ea)$ such that $\sigma(b) \in E(b)$ and $acl_\sigma(Eb) = acl_\sigma(Ea)$.*

Proof. Replacing a by $a^\frown \sigma(a)^\frown \cdots^\frown \sigma^\ell(a)$, if necessary, we may assume that

$$[E(a, \sigma(a)) : E(\sigma(a))] = [E(\sigma^i(a))_{i \geq 0} : E(\sigma^i(a))_{i \geq 1}].$$

Claim. $E(\sigma^i(a))_{i \leq 0}$ and $E(\sigma^i(a))_{i \geq 0}$ are linearly disjoint over $E(a)$.

Proof. Let $n < 0$; then

$$\begin{aligned}[E(\sigma^i(a))_{i\geq n} : E(\sigma^i(a))_{i\geq 0}] &= \prod_{j=n}^{-1} [E(\sigma^i(a))_{i\geq j} : E(\sigma^i(a))_{i\geq j+1}] \\ &= \prod_{j=n}^{-1} [E(\sigma^i(a))_{j\leq i\leq 0} : E(\sigma^i(a))_{j+1\leq i\leq 0}] \\ &= [E(\sigma^i(a))_{n\leq i\leq 0} : E(a)].\end{aligned}$$

Let $k < 0$ be such that $N = [E(a, \sigma^k(a)) : E(\sigma^k(a))]$ is maximal. Then, for $i < k$, since $E(a, \sigma^k(a))$ and $E(\sigma^k(a), \sigma^i(a))$ are linearly disjoint over $E(\sigma^k(a))$, we have

$$\begin{aligned}N &\geq [E(a, \sigma^i(a)) : E(\sigma^i(a))] \geq [E(a, \sigma^i(a), \sigma^k(a)) : E(\sigma^i(a), \sigma^k(a))] \\ &= [E(a, \sigma^k(a)) : E(\sigma^k(a))],\end{aligned}$$

so that all these numbers are equal. Let a_1 be any element from the tuple a not in E; by the above, a_1 has the same monic minimal polynomial over $E(\sigma^k(a))$, $E(\sigma^i(a), \sigma^k(a))$ and $E(\sigma^i(a))$ for any $i < k$. Hence the tuple b of coefficients of the minimal monic polynomial of a_1 over $E(\sigma^k(a))$ is in $F = \bigcap_{i\leq k} E(\sigma^i(a))$. Since $a_1 \notin E$, b is not in E, which implies that $acl_\sigma(E(a)) = acl_\sigma(E(b))$. The field F is a subfield of a finitely generated extension of E, and is therefore equal to $E(c)$ for some tuple c; from $b \in F$ we obtain $E(a)^{alg} = E(c)^{alg}$. We have

$$\sigma(F) = \bigcap_{i\leq k} E(\sigma^{i+1}(a)) = \bigcap_{i\leq k+1} E(\sigma^i(a)),$$

i.e., $\sigma(F) \subseteq F$.

(4.5) Theorem (The degree 1, bounded case)**.** *Let E be a model of $ACFA$. Assume that $deg_\sigma(a/E) = 1$, and that $[E(a, \sigma^k(a)) : E(a)] \leq N$ for every $k \in \mathbb{Z}$. Then there is a b such that $\sigma(b) = b$ and $E(a)^{alg} = E(b)^{alg}$.*

Proof. By the lemma there is a tuple b equi-algebraic with a over E and such that $\sigma(b) \in E(b)$. For $k \in \mathbb{Z}$ we have

$$\begin{aligned}[E(b, \sigma^k(b)) : E(b)] &\leq [E(b, \sigma^k(b), a, \sigma^k(a)) : E(b)] \\ &= [E(b, \sigma^k(b), a, \sigma^k(a)) : E(b, a, \sigma^k(a))] \times [E(b, a, \sigma^k(a)) : E(b, a)] \\ &\qquad \times [E(a, b) : E(b)] \\ &\leq [E(\sigma^k(a), \sigma^k(b)) : E(\sigma^k(a))] \times [E(\sigma^k(a)) : E(a)] \times [E(a, b) : E(b)] \\ &= [E(a, b) : E(a)] \times [E(a, b) : E(b)] \times [E(a, \sigma^k(a)) : E(a)].\end{aligned}$$

Hence $[E(b, \sigma^k(b)) : E(b)] \leq [E(a, b) : E(a)] \times [E(a, b) : E(b)] \times N$ for all $k \in \mathbb{Z}$. From $\sigma(b) \in E(b)$ we deduce that the fields $E(\sigma^k(b))$, $k \geq 0$, form a decreasing chain, and therefore $[E(b, \sigma^k(b)) : E(\sigma^k(b))] = [E(b, \sigma(b)) : E(\sigma(b))]^k$ for $k \in \mathbb{N}$; this degree must therefore equal 1, i.e., $E(b) = E(b)_\sigma$.

Changing b, we may assume that b is the generic point of a non-singular complete curve $\mathcal{C}$ defined over E. Let $g(x)$ be the tuple of functions on $\mathcal{C}$ such that $\sigma(b) = g(b)$. Since σ is an automorphism of $E(b)$ and $\mathcal{C}$ is complete, the map $g : \mathcal{C} \to \sigma\mathcal{C}$ is an isomorphism.

Let $\alpha \in \mathcal{C}(E)$ be such that $\sigma(\alpha) = g(\alpha)$ (this is possible since $E \models ACFA$), choose $m \in \mathbb{N}$ so that the divisor $m\alpha$ is very ample, and let $\varphi : \mathcal{C} \to \mathbb{P}^n$ be an embedding given by the divisor $m\alpha$ (see [10] or [32] for the relationship between divisors and embeddings into projective space; note that φ is a closed immersion). Then $\sigma\varphi : \sigma\mathcal{C} \to \mathbb{P}^n$, obtained by applying σ to the coefficients appearing in the coordinate functions of φ, is an embedding determined by the divisor $\sigma(m\alpha) = mg(\alpha)$; thus the embeddings φ and $\sigma\varphi_\circ g$ correspond to the same divisor $m\alpha$ because g is an isomorphism. This implies that for some $A \in PGL_n(E)$ we have

$$A_\circ\varphi = \sigma\varphi_\circ g.$$

Using again the fact that E is a model, let $B \in PGL_n(E)$ be such that $B = \sigma(B)A$, and let $\psi = B_\circ\varphi : \mathcal{C} \to \mathbb{P}^n$. Then

$$\psi = \sigma(B)_\circ A_\circ\varphi = \sigma(B)_\circ\sigma\varphi_\circ g = \sigma\psi_\circ g.$$

Let $c = \psi(b)$. Then

$$\sigma(c) = \sigma\big(\psi(b)\big) = \sigma\psi\big(\sigma(b)\big) = \sigma\psi\big(g(b)\big) = \psi(b) = c,$$

i.e., c is left fixed by σ. Since ψ is a closed immersion, $E(b)^{alg} = E(c)^{alg}$.

Remark. In characteristic $p > 0$, the result can be strengthened as follows (when $deg_\sigma(a/E) = 1$ and $E \models ACFA$). Assume that for some N, $\mathrm{Mult}(\sigma^k(a)/E(a)) \leq N$ for every integer k. Then there is b, equi-algebraic with a over E and such that $\sigma(b) = b^{p^n}$ for some n.

Proof. Let a_1 be any element from a not in E; since $\sigma(a_1) \in E(a_1)^{alg}$, there is $n \in \mathbb{Z}$ such that a_1 and $\sigma(a_1)^{p^n}$ are separably equi-algebraic over E. Let $\tau = Frob^n \circ \sigma$; then τ sends the separable closure of $E(a_1)$ to itself. This implies that for every b in $E(a_1)^{alg}$, b and $\tau(b)$ are separably equi-algebraic over E, and therefore that $\mathrm{Mult}(\tau^k(b)/Eb) = [E(b, \tau^k(b)) : E(b)]$. Apply the theorem to τ.

(4.6) Ramification locus. Let E be an algebraically closed field, K a function field over E and L a separable algebraic extension of K of degree n. Choose $a \in K$ such that $E(a) = K$ and $E[a]$ is integrally closed; let $\alpha \in L$ be such that $E[a, \alpha]$ is the integral closure of $E[a]$ in L. Let V, W be the varieties (over E) of which a and (a, α) are generic points, and $\pi : W \to V$ the obvious projection. Then V and W are normal, and π is a finite morphism. Let $f(a, Y)$ be the minimal (monic) polynomial of α over $E(a)$, and consider $D(a)$, the discriminant of $f(a, Y)$; then $D(a) \neq 0$ because L is separable over K.

Let $b \in V$; then $D(b) \neq 0$ if and only if $\pi^{-1}(b)$ has n elements. Thus, the set of points of V over which π is ramified is the algebraic subset S of V of codimension 1 defined by the equation $D(x) = 0$.

Theorem. *Assume that the characteristic is* 0. *Let E_0 be an algebraically closed subfield of E over which the variety V and the algebraic set S are defined. Then $L \subseteq K(E_0(a)^{alg})$.*

Proof. Our assumption implies that the restriction of π to $W \setminus \pi^{-1}(S)$ is étale. Since our result deals with the function fields, we may replace V by a variety birationally equivalent to V, and which is in bijection with $V \setminus S$ by a birational map (everything being defined over E_0). We may therefore assume that S is empty, and therefore that π is an étale cover of V. This implies that W is isomorphic (over V) to a cover

$\pi' : W' \to V$ defined over E_0. For a proof, see [31], Thm. 6.3.3. Dualising this, we obtain that $E(W) = E(E_0(W'))$, which proves our assertion.

(4.7) Valuations and their ramification. Let E be an algebraically closed field, a a tuple such that $E[a]$ is integrally closed, $K = E(a)$, and V the variety defined over E of which a is a generic point. Then V is normal.

Let U be a subvariety of V of codimension 1, and $\mathcal{P} \subseteq E[V]$ the associated prime ideal. Since V is normal, it is non-singular in codimension 1, and the localisation of $E[V]$ at $\mathcal{P}$ is a valuation ring, $\mathcal{O}_v$; let v be the corresponding valuation on $E(V)$. The maximal ideal $\mathcal{M}_v$ of $\mathcal{O}_v$ is $\mathcal{P}\mathcal{O}_v$, and the valuation group of v is infinite cyclic. Thus v is a discrete rank-1 valuation. We denote by $\mathcal{V}(E[a]/E)$ the set of valuations on $K = E(a)$ arising in this fashion.

Let L be a finite separable extension of K, generated by an element α integral over $E[a]$; let $f(a, Y)$ be the minimal (monic) polynomial of α over $E[a]$. Then $E[a, \alpha]$ is integrally closed.

Fix a valuation $v \in \mathcal{V}(E[a]/E)$, and let $\mathcal{O}_L = \mathcal{O}_v(\alpha)$; then $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_v$ in L. One has

$$\mathcal{O}_L/\mathcal{P}\mathcal{O}_L \simeq \prod_w \mathcal{O}_L/(\mathcal{Q}_w)^{e_w},$$

where w runs over all valuations extending v, $\mathcal{Q}_w$ is the prime ideal of $\mathcal{O}_L$ associated to w, and e_w is a positive integer, called the ramification index of w over K (see [30], Prop. I.4.10). If $e_w > 1$, we say that v ramifies in L, or that w ramifies over K.

Let $\bar{f}(\bar{a}, Y)$ be the polynomial obtained from $f(a, Y)$ by modding out by $\mathcal{M}_v$, and $D(a)$ the discriminant of $f(a, Y)$; then v ramifies in L if and only if $\bar{f}(\bar{a}, Y)$ has multiple roots (in the algebraic closure of $\mathcal{O}_v/\mathcal{M}_v$), if and only if $D(a) \in \mathcal{M}_v$. Thus valuations of $\mathcal{V}(E[a]/E)$ which ramify in L correspond to the irreducible components of the algebraic subset S of V defined by $D(x) = 0$.

Lemma. *Keeping the same notation, let M be a finite extension of K, and w a valuation on M extending v.*

(1) *If L is Galois over K, then all extensions of v to L are conjugate by an element of $\mathcal{G}al(L/K)$. Hence all ramification indices are equal and all residue fields $\mathcal{O}_L/\mathcal{Q}_w$ are isomorphic. Thus, v ramifies in L if and only if all its extensions to L ramify over K.*

(2) *If v does not ramify in L, then w does not ramify in LM.*

(3) *If $M \subseteq L$, then v does not ramify in L if and only if v does not ramify in M and w does not ramify in L.*

(4) *Assume that v does not ramify in L, and that its residue field is algebraically closed; then v has $[L : K]$ distinct extensions to L. This happens if K has transcendence degree 1 over E.*

(5) *Let E_0 be an algebraically closed subfield of E, over which V is defined. Then v is defined over E_0 if and only if $\mathcal{M}_v \cap E_0[a] \neq (0)$.*

(6) *Let R be a subring of K, and assume that v is identically 0 on $R \setminus \{0\}$. Then v is identically 0 on all elements of $K \setminus \{0\}$ which are algebraic over R.*

Proof. (1), (3), (4), (6) are immediate.

(2) The minimal polynomial of α over M divides $f(a, Y)$, and $\bar{f}(\bar{a}, Y)$ has no multiple root.

(5) Indeed, $\mathcal{M}_v \cap E_0[a]$ defines a subvariety of V, which is of codimension at most 1; if it is of codimension 1, then $\mathcal{M}_v \cap E_0[a]$ generates $\mathcal{M}_v$.

(4.8) Theorem (The degree 1 unbounded case) (char. 0)**.** *Let $E = acl_\sigma(E)$, let a be a tuple, and assume that $deg_\sigma(a/E) = 1$ and that $tp(a/E)$ is unbounded. Then $tp(a/E)$ is superficially stable.*

Proof. Let $F \supseteq E$ be an algebraically closed structure not containing a. Let $K = Facl_\sigma(Ea)$.

Assume that L is a proper finite Galois extension of K, and that $\sigma(L) = L$. Changing a if necessary, we will assume that $L = L_1K$, where L_1 is a finite Galois extension of $F(a)$, that $E[a]$ is integrally closed, and that the variety V with generic a is non-singular. Choose α integral over $F[a]$ and such that $L_1 = F(a, \alpha)$. Keeping the notation of (4.7), let $\mathcal{S}$ be the set of valuations in $\mathcal{V}(F[a]/F)$ which ramify in L_1 and are not defined over E.

Claim. $\mathcal{S}$ is finite and non-empty.

Let W be the variety (over F) with generic (a, α), and let $\pi : W \to V$ be the finite morphism dual to $F[a] \subseteq F[a, \alpha]$. By assumption $L_1 \not\subset F(E(a)^{alg})$, which, by Theorem 4.6, implies that the algebraic subset S over which π ramifies is not defined over E. Since V is non-singular, all components of S have codimension 1, and the components of S not defined over E correspond to the elements of $\mathcal{S}$, which is therefore finite. Since S is not defined over E, $\mathcal{S}$ is not empty.

For $k \in \mathbb{Z}$ and $v \in \mathcal{V}(F[a]/F)$, we define a valuation $\sigma^k(v) \in \mathcal{V}(F[\sigma^k(a)]/F)$ by $\sigma^k(v)(x) \geq 0 \iff v(\sigma^{-k}(x)) \geq 0$. Then $\sigma^k(\mathcal{S})$ is the set of elements of $\mathcal{V}(F[\sigma^k(a)]/F)$ which ramify in $\sigma^k(L_1)$ and are not defined over E. Fix $v \in \mathcal{S}$ and choose $k \in \mathbb{Z}$ such that $\mathrm{Mult}(\sigma^k(a)/F(a)) > |\mathcal{S}|$.

Then v ramifies in $L_1\sigma^k(L_1)$, and because L_1 is Galois over $F(a)$, all extensions of v to $L_1\sigma^k(L_1)$ ramify over $F(a)$. Since v is not defined over E, it does not ramify in $F(a, \sigma^k(a))$. Hence, if w is any extension of v to $F(a, \sigma^k(a))$, then w ramifies in $L_1\sigma^k(L_1)$, and so does the restriction w' of w to $F(\sigma^k(a))$. Since $L_1\sigma^k(L_1) \subseteq K\sigma^k(L_1)$, the valuations of $\sigma^k(L_1)$ which ramify in $L_1\sigma^k(L_1)$ are defined over E. From $F(\sigma^k(a)) \subseteq \sigma^k(L_1) \subseteq L_1\sigma^k(L_1)$, we then deduce that w' ramifies in $\sigma^k(L_1)$. By (4.7)(5) and (6), the valuation ring of w' contains F and $E(\sigma^k(a))$, and therefore $w' \in \sigma^k(\mathcal{S})$.

It now suffices to count the number of such w' to reach a contradiction: since the residue field of $F(a)$ at v is algebraically closed, v has $\mathrm{Mult}(\sigma^k(a)/F(a))$ extensions to $F(a, \sigma^k(a))$, and their restrictions to $F(\sigma^k(a))$ are all distinct. By the choice of k, there are more than $|\mathcal{S}|$ of them.

(4.9) Proposition (char 0)**.** *Let p be a type over an algebraically closed substructure E, and assume that p and $tp(b/E)$ are not superficially co-stable. Then $p[k] \not\perp^a qftp(b/E)[k]$ for some $k \geq 1$, and $SU(p[k]) > 1$ if $deg_\sigma(p) > 1$.*

Proof. Let a realise p and let b be a tuple of elements independent from a over E. Let $F = acl_\sigma(Eb)$ and $K = F(acl_\sigma(Ea))$. Assume that L is a finite proper Galois extension of K such that $\sigma(L) = L$. Enlarge b so that $L = L_1K$, with L_1 a finite Galois extension of $acl_\sigma(Ea)(b)$.

Claim 1. We may assume that $deg_\sigma(b/E)$ is finite.

Proof. Indeed, if c is an element from b with $deg_\sigma(c/E)$ infinite, then c realises p_ω. By (2.10)(2), the field $acl_\sigma(Ea)acl_\sigma(Ec)$ has no proper finite σ-stable algebraic extension. Thus L is not contained in $acl_\sigma(Eac)$. Replace E by $acl_\sigma(Ec)$ and p by its (unique) non-forking extension to $acl_\sigma(Ec)$ (note: $tp(a/acl_\sigma(Ec))[k] \not\perp^a qftp(b/acl_\sigma(Ec))[k]$ implies $tp(a/E)[k] \not\perp^a qftp(b/E)[k]$). Proceed in this way to get the desired E.

Let $E' = acl_\sigma(Ea)$. Increase b if necessary so that

$$\mathrm{Mult}(\sigma^k(b)/Eb\sigma(b)\cdots\sigma^{k-1}(b)) = \mathrm{Mult}(\sigma(b)/Eb)$$

and

$$\mathrm{Mult}(b/E\sigma(b)\cdots\sigma^k(b)) = \mathrm{Mult}(b/E\sigma(b))$$

for every positive integer k, $E[b]$ is integrally closed in $E(b)$ and the variety V of which b is a generic point is non-singular; let α be such that $L_1 = E'(b,\alpha)$ and $E'[b,\alpha]$ is the integral closure of $E'[b]$ in L_1. With the notation of (4.7), let $\mathcal{S}$ be the set of valuations in $\mathcal{V}(E'[b]/E')$ which ramify in L_1 and are not defined over E.

Claim 2. $\mathcal{S}$ is finite and non-empty.

Proof. Similar to the proof of the claim in (4.8).

For $v \in \mathcal{V}(E'[b]/E')$ and $k \in \mathbb{Z}$, we define the valuation $\sigma^k(v) \in \mathcal{V}(E'[\sigma^k(b)]/E')$ by $\sigma^k(v)(x) \geq 0 \iff v(\sigma^{-k}(x)) \geq 0$. We define a binary relation I on $\mathcal{S}$ by vIw iff v and $\sigma(w)$ are compatible, i.e., have a common extension to $E'(b)^{alg}$.

Claim 3. Given $v \in \mathcal{S}$, there is a $w \in \mathcal{S}$ such that vIw.

Proof. Proceed as in (4.8) to show that if w' is **any** valuation on $E'(\sigma(b))$ compatible with v, then $w' \in \sigma(\mathcal{S})$. Take $w = \sigma^{-1}(w')$.

The finite oriented graph $(\mathcal{S}, I)$ therefore contains a cycle, say $v = v_0, v_1, \ldots, v_k = v$.

Claim 4. The valuation v extends to a valuation w on $E'(b)_\sigma$ satisfying $\sigma^k(w) = w$.

For $i \in \mathbb{Z}$, define a valuation $w_i \in \mathcal{V}(E'[\sigma^i(b)]/E')$ by

$$w_i = \sigma^i(v_j), \qquad \text{where } i = j + kn,\ 0 \leq j < k.$$

It then suffices to show that the w_i's are compatible: any w extending the w_i's will satisfy the requirement. Note that by definition, w_i and w_{i+1} are compatible.

By compactness (and translation by σ), it suffices to show that $w_0, \ldots, w_i$ are compatible for $i > 0$, which we do by induction on i. For $i = 1$ there is nothing to prove. Assume the result true for i; let w be a valuation on $E'(b, \sigma(b), \ldots, \sigma^i(b))$ extending $w_0, \ldots, w_i$, and let w' be a valuation on $E'(\sigma^i(b), \sigma^{i+1}(b))$ extending w_i, w_{i+1}.

By our choice of b we have $[E(b,\sigma(b)) : E(\sigma(b))] = [E(\sigma^i(b))_{i\geq 0} : E(\sigma^i(b))_{i\geq 1}]$; hence the hypotheses of the claim of (4.4) are satisfied, and $E'(b, \sigma(b), \ldots, \sigma^i(b))$ and $E'(\sigma^i(b), \sigma^{i+1}(b))$ are linearly disjoint over $E'(\sigma^i(b))$. Since w and w' agree on $E'(\sigma^i(b))$, they have a common extension to $E'(b, \sigma(b), \ldots, \sigma^i(b), \sigma^{i+1}(b))$, which proves the compatibility for $i + 1$.

We fix such an extension w of v; since v is not defined over E, $w(\sigma^i(b)) = 0$ for every integer i, and therefore w is non-negative on the ring $E'[\sigma^i(b)]_{i\in\mathbb{Z}}$; let

$R = \{r \in E'(b)_\sigma \mid w(r) \geq 0\}$, $\mathcal{M} = \{r \in R \mid w(r) > 0\}$. Then $\mathcal{M}$ is a prime ideal of R, stable under σ^k.

Consider now the σ^k-ring $R/\mathcal{M}$; it is a domain, and contains isomorphic copies of $E' = acl_\sigma(Ea)$ and $E(b)_\sigma$, viewed as σ^k-difference fields. Let a', b' be the images of a, b in $R/\mathcal{M}$; from the definition of w, it follows that a' realises $p[k]$ and b' realises $qftp(b/E)[k]$. They are not independent over E, which shows the first assertion.

Assume that $deg_\sigma(p) > 1$. From $deg_{\sigma^k}(a'/E(\sigma^{ki}(b'))_{i\in\mathbb{Z}}) = deg_{\sigma^k}(a/E) - 1 = deg_\sigma(a/E) - 1$, we deduce that $a' \notin acl_{\sigma^k}(Eb')$, and therefore

$$SU(p[k]) = SU(tp_k(a'/E)) > SU(tp_k(a'/Eb')) \geq 1.$$

This finishes the proof of the proposition.

(4.10) Theorem (char. 0)**.** *Let p be a type of SU-rank 1 over an algebraically closed substructure E. Then either p is superficially stable, or $p \not\perp (\sigma(x) = x)$, in which case $deg_\sigma(p) = 1$.*

Proof. If $deg_\sigma(p) = 1$, then (4.5) and (4.8) give us the result; assume therefore that $deg_\sigma(p) > 1$, and that the theorem is true for types of smaller degree. Assume that $p = tp(a/E)$ is not superficially stable; we want to reach a contradiction.

Replacing a by $a^\frown\sigma(a)^\frown\cdots^\frown\sigma^\ell(a)$, we may assume that $\sigma(a) \in E(a)^{alg}$. By (4.9), for some integer $k > 1$, $SU(p[k]) > 1$; by (3.4) and (1.12), there are $E_1 \supseteq E$, independent from a over E, and $c \in acl_\sigma(E_1 a)$ such that $SU(tp_k(c/E_1)) = 1$. By the induction hypothesis, either $tp_k(c/E_1)$ is superficially stable, or for some $E_2 \supseteq E_1$, independent from a over E_1, $acl_\sigma(E_2, c)$ contains a realisation d of $\sigma^k(x) = x$ not in E_2; the second case cannot happen, since the code of the set $\{d, \sigma(d), \ldots, \sigma^{k-1}(d)\}$ is then in $acl_\sigma(E_2, c) = acl_\sigma(E_2, a)$ but not in E_2, contrary to our assumption that $1 = SU(a/E) < deg_\sigma(p)$.

Since $SU(tp_k(c/E_1)) = 1 < SU(tp_k(a/E_1))$, we have

$$deg_{\sigma^k}(c/E_1) < tr.deg_{\sigma^k}(a/E_1) = deg_\sigma(p).$$

Hence $tp_k(c/E_1)$ is superficially stable. Let $i \leq k-1$ be smallest such that $\sigma^{i+1}(c)$ is algebraic over $E_1(c, \sigma(c), \ldots, \sigma^i(c))$. Observe that $tp_k(\sigma^j(c)/E_1)$ has SU-rank 1 and is superficially stable; by (4.2)(2), any non-forking extension of $tp_k(\sigma^j(c)/E_1)$ is also superficially stable, and so is $tp_k(c, \sigma(c), \ldots, \sigma^i(c)/E_1)$ (see e.g. the proof of (4.2)(8)); since $a \in E(c, \sigma(c), \ldots, \sigma^i(c))^{alg}$, it follows that $tp(a/E_1)$ is superficially stable, a contradiction.

(4.11) Theorem (char. 0)**.** *Let p be a type of finite rank, orthogonal to $(\sigma(x) = x)$. Then p is superficially stable.*

Proof. We may assume that the set E over which p is defined equals $acl_\sigma(E)$. Let a realise p, and assume that p is not superficially stable; by (4.3), if $E' \supseteq E$, then any non-forking extension of p to E' is not superficially stable. Enlarging E if necessary, we will therefore assume that E and b satisfy:

(i) p and $tp(b/E)$ are not superficially co-stable.
(ii) $SU(b/E)$ is minimal, i.e, if E' and b' satisfy (i), then $SU(b'/E') \geq SU(b/E)$.
(iii) There is $c \in acl_\sigma(Eb)$ such that $SU(c/E) = 1$.

By Claim 1 of Proposition 4.9, $SU(b/E) < \omega$. Let L be a proper finite Galois extension of $acl_\sigma(Ea)acl_\sigma(Eb)$ stable under σ; then $SU(b/Ec) < SU(b/E)$, and therefore $tp(a/Ec)$ and $tp(b/Ec)$ are superficially co-stable. This implies that $L \subseteq acl_\sigma(Eac)acl_\sigma(Eb)$. Let $M = L \cap acl_\sigma(Eac)$; then $L = Macl_\sigma(Eb)$, so that $\sigma(M) \subseteq$

$L \cap acl_\sigma(Eac) = M$. Thus $tp(a/E)$ and $tp(c/E)$ are not superficially co-stable, which implies that $SU(b/E) = SU(c/E) = 1$. The result now follows by (4.9) and (4.10).

(4.12) Corollaries (char. 0). (1) *Assume that* $E \models ACFA$, $1 < SU(a/E) < \omega$. *Then there is* $b \in acl_\sigma(Ea)$ *such that* $SU(b/E) = 1$.

(2) *If* p *and* q *are superficially stable, so is* $p \times q$.

(3) *Note that* p_ω *is superficially stable, but unstable.*

Proof. (1) By (3.4), $tp(a/E)$ is non-orthogonal to a type q over E of SU-rank 1. If q is modular, then (3.4)(3) gives us the result. If q is not modular, then $tp(a/E) \not\perp (\sigma(x) = x)$. By (3.7)(2) there is a consistent formula $\psi(y)$ (over E) such that $tp(a/E)$ is not almost orthogonal to $(\sigma(x) = x)$ over any realisation of $\psi(y)$. Since $E \models ACFA$, it contains elements satisfying ψ, and therefore $acl_\sigma(Ea) \setminus E$ contains some element b with $\sigma(b) = b$.

The other assertions are obvious.

5. Semi-minimal analysis of types

The main result in this section is that, given a of finite rank over E, there is a sequence $a_1, \ldots, a_n$ of elements in $acl_\sigma(E, a)$ satisfying $a \in acl_\sigma(E, a_1, \ldots a_n)$, and $tp(a_i/E, a_1, \ldots, a_{i-1})$ is either stable and modular of rank 1, or is F-internal, where F is the field fixed by σ. We also study internality, stable embeddability, and derive results on Galois theory and the structure of modular non-trivial sets of rank 1. While the main results use the dichotomy theorem of Chapter 4 and therefore require the characteristic to be 0, many of the auxiliary ones hold in any characteristic. Throughout the section, unless explicitly stated to the contrary, the results are valid in any characteristic; F **denotes the fixed field**.

(5.1) Two notions of internality. Let p and q be types (possibly incomplete) over A.

We say that p is *internal* to q over A iff there is a small set B containing A such that whenever a realises p, there is a tuple b of realisations of q such that $a \in dcl(B, b)$. If b can be chosen so that $a \in cl_\sigma(B, b)$, we say that p is *qf-internal* to q over A.

The second notion clearly implies the first one; it is mainly used when the type q is unstable. We start by showing that the criteria for internality (in the stable case) and qf-internality are as can be expected, namely that it is enough to show internality with some independent a and B.

(5.2) Lemma (qf-internality to the fixed field). *Let A be a difference field, F the fixed field, and D a quantifier-free definable set of SU-rank 1, $SU(a/A) < \omega$.*

(1) *Assume that a and c are independent over A, and that $a \in cl_\sigma(A, c, b)$ for some tuple b of elements of F. Then b and c can be chosen so that in addition $b \in cl_\sigma(A, c, a)$ and $c = Cb(a, b/acl_\sigma(A, c))$.*

Assume now that a and c are independent over A, and that $a \in cl_\sigma(A, c, b)$ and $b \in cl_\sigma(A, c, a)$ for some tuple b in D. Then

(2) *There are formulas $\psi(y)$ and $\varphi(x) \in tp(a/A)$ such that ψ is consistent and, for any C satisfying ψ, $\varphi(x) \subseteq cl_\sigma(A, C, D)$.*

(3) *There is a set C of (finitely many) independent realisations of $tp(c/A)$, and a semi-type q satisfied by a, such that $q \subseteq cl_\sigma(A, C, D)$. In particular, q and*

$tp(a/A)$ are qf-internal to D. If A is relatively separably closed in $A(a)_\sigma$, then we may take $q = qftp(a/A)$.

(4) *Let C be given by (3). There is a semi-type r satisfied by C such that, for any C' realising r, $q \subseteq cl_\sigma(A, C', D)$. Furthermore r is qf-internal to D.*

Proof. (1) Enlarging c if necessary, we may assume that $b \in acl_\sigma(A, c, a)$. Let $e = Cb(b/A, c, a)$. Then $e \in cl_\sigma(A, c, a)$, and furthermore, $a \in cl_\sigma(A, c, e)$. By (3.7)(4), $e \in F$. Let $d = Cb(a, e/A, c)$; then $a \in cl_\sigma(A, d, e)$ and $e \in cl_\sigma(A, d, a)$.

(2) Enlarging c, we may assume that b is independent from c over A, and that $c = Cb(a, b/acl_\sigma(A, c))$. Let $u(y, x)$ and $v(y, z)$ be difference rational functions over A (i.e., quotients of difference polynomials with coefficients in A) such that $b = u(c, a)$ and $a = v(c, b)$. Let $\theta(x, y)$ be a quantifier-free formula expressing that $u(y, x)$ is defined and in D, and $v(y, u(y, x))$ is defined and equals x.

We will first assume that A is relatively separably closed in $A(a)_\sigma$. By Remark (2.16), there are quantifier-free formulas $\varphi_0(x), \psi_0(y_1)$ and a difference polynomial $h(x, y_1)$ such that for any (a', c') satisfying $\varphi_0(x) \wedge \psi_0(y_1) \wedge h(x, y_1) \neq 0$, $\theta(a', c')$ holds. Let $S = \{a' \mid \models \forall y_1\, (\psi_0(y_1) \rightarrow h(a', y_1) = 0)\}$; then S is defined over A, by a formula $\varphi_1(x)$, and equals $\{a' \mid \models \bigwedge_{i=1}^{k} h(a', c_i) = 0\}$ for some k and tuples $c_1, \ldots c_k$ satisfying ψ_0. Let

$$\varphi(x) :\ \varphi_0(x) \wedge \neg\varphi_1(x),$$

$$\psi(y_1, \ldots, y_k) :\ \bigwedge_{i=1}^{k} \psi_0(y_i)\ \wedge\ \forall x\ \left(\bigwedge_{i=1}^{k} h(x, y_i) = 0\ \rightarrow\ \varphi_1(x) \right).$$

Assume that $\models \varphi(a') \wedge \psi(c'_1, \ldots, c'_k)$; then $a' \notin S$, so that $h(a', c'_i) \neq 0$ for some i; thus $\models \theta(a', c'_i)$ and therefore $a' \in cl_\sigma(c'_i, D)$. Thus $\varphi \subseteq cl_\sigma(A, c'_1, \ldots, c'_k, D)$.

For the general case, let $\alpha \in acl_\sigma(A)$ be such that $A(\alpha)_\sigma$ is relatively separably closed in $A(a)_\sigma$. By the previous case (and its proof), there are formulas $\varphi'(x, \alpha)$ and $\psi'(y, \alpha)$ such that, if $\Phi(\alpha)$ denotes the set of realisations of $\varphi'(x, \alpha)$, and c' satisfies $\psi'(y, \alpha)$, then $\Phi(\alpha) \subseteq cl_\sigma(A, c', D)$. Let $\eta(t)$ be the formula isolating $tp(\alpha/A)$, and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_\ell$ denote the conjugates of α over A. We then define

$$\varphi(x) :\ \exists t\ \eta(t) \wedge \varphi'(x, t),$$

$$\psi(y_1, \ldots, y_\ell) :\ \exists t_1, \ldots, t_\ell\ \bigwedge_{i \neq j} (t_i \neq t_j) \wedge \bigwedge_{i} (\eta(t_i) \wedge \psi'(y_i, t_i)).$$

Assume that $\varphi(a')$ and $\psi(c'_1, \ldots, c'_\ell)$ hold; then $a' \in \Phi(\alpha_i)$ for some i. This α_i appears as one of the t_j's of ψ, which gives the result.

(3) By construction, the formula ψ obtained in (2) is satisfied by a set C of independent realisations of $tp(c/A)$. Let $\eta(t)$ be as in (2), and consider the semi-type $q(x) = \exists t\ \eta(t) \wedge q'(x, t)$, where $q'(x, t) = qftp(a, \alpha/A)$.

(4) Since $c = Cb(a, b/acl_\sigma(A, c))$, there are independent realisations $(a_1, b_1), \ldots, (a_n, b_n)$ of $tp(a, b/A, c)$ such that $c \in cl_\sigma(a_1, b_1, \ldots, a_n, b_n)$; then c and $a_1, \ldots, a_n$ are independent over A, so that $tp(c/A)$ is qf-internal to D by (1) or (2), and therefore so is $tp(C/A)$. The existence of r now follows by (2).

(5.3) *Remark.* We can therefore apply Lemma (5.2) to the fixed field F. Recall also from [3] that if S is a definable infinite subset of F, then every element of F can be written as $ab + c + d$ for some $a, b, c, d \in S$; thus qf-internality to F is equivalent to qf-internality to S.

(5.4) Lemma (qf-internality and internality to a fully stable type)**.** *Assume that $SU(a/A) < \omega$, and let q be a fully stable (maybe incomplete) type of SU-rank 1 over the difference field A (see the Appendix for the definition and properties of fully stable).*

(1) *Assume that for some c independent from a over A there is a tuple b of realisations of q such that $a \in cl_\sigma(A, b, c)$. Then $tp(a/A)$ is qf-internal to q. If $A = acl_\sigma(A)$ and $b \in acl_\sigma(A, c, a)$, then $tp(a/A) \subseteq cl_\sigma(A, C, q)$ for some set C consisting of finitely many realisations of $tp(c/A)$.*

(2) *Assume that for some c independent from a over A there is a tuple b of realisations of q such that $a \in dcl(A, b, c)$. Then $tp(a/A)$ is internal to q. If $A = acl_\sigma(A)$ and $b \in acl_\sigma(A, c, a)$, then $tp(a/A) \subseteq dcl(A, C, q)$ for some set C consisting of finitely many realisations of $tp(c/A)$.*

Proof. We will prove both results at the same time. First, observe that to prove the qf-internality or internality of $tp(a/A)$ to q, it is enough to show it when $A = acl_\sigma(A)$: if $tp(a'/A) = tp(a/A)$, then there is an A-automorphism τ such that $tp(a'/acl_\sigma(A)) = \tau(tp(a/acl_\sigma(A)))$; hence $tp(a/acl_\sigma(A)) \subseteq cl_\sigma(B, q)$ implies $tp(a'/acl_\sigma(A)) \subseteq cl_\sigma(\tau(B), q)$, and similar statements hold with dcl; $tp(a/A)$ has a bounded number of extensions to $acl_\sigma(A)$. We therefore assume that $A = acl_\sigma(A)$.

Let b, c be as given by the hypothesis. Since q has rank 1, enlarging c if necessary, we may assume that $b \in acl_\sigma(A, a, c)$.

Since $a \in cl_\sigma(A, b, c)$ and $tp(b/A)$ has a unique non-forking extension to any set containing A, $tp(a/A, c)$ has a unique non-forking extension to any set containing A, c.

Claim. $tp(a/A)$ has a unique non-forking extension to any set containing A ($= acl_\sigma(A)$).

Assume, by way of contradiction, that $tp(a/A)$ has two distinct non-forking extensions to Ac. By the independence theorem (1.9), there are realisations c_1, c_2 of $tp(c/A)$, realising the same type over Ac, independent from a and c over A, satisfying $tp(c_1/Aa) = tp(c/Aa) \neq tp(c_2/Aa)$; then $tp(a/Acc_1) \neq tp(a/Acc_2)$, which contradicts the fact that $tp(a/Ac)$ has a unique non-forking extension to any set containing Ac.

Let $B = A \cup \{c_1, \ldots, c_k\}$, where $c_1, \ldots, c_k$ are independent realisations of $tp(c/A)$ for some $k > SU(a/A)$. Then for some i, a and c_i are independent over A. Since $tp(a/A)$ has a unique non-forking extension to any set containing A, $tp(a, c_i/A) = tp(a, c/A)$, and therefore $a \in cl_\sigma(A, c_i, b')$, or $a \in dcl(A, c_i, b')$, for some tuple b' of realisations of q.

(5.5) Theorem. (Semi-minimal analysis of types of finite rank in char. 0) *Suppose that $SU(a/E) < \omega$, where E is a difference field. Then there is a sequence $a_1, \ldots, a_n$ of elements in $acl_\sigma(E, a)$ such that $a \in acl_\sigma(E, a_1, \ldots, a_n)$ and, for every $i < n$, $tp(a_{i+1}/E, a_1, \ldots, a_i)$ is either fully stable modular of SU-rank 1, or is qf-internal to the fixed field F.*

Proof. Assume that we already have $a_1, \ldots, a_i$; if $a \in acl_\sigma(E, a_1, \ldots, a_i)$, we are done. Otherwise, $SU(a/E, a_1, \ldots, a_i) \geq 1$. By Proposition 3.4, $tp(a/E, a_1, \ldots, a_i)$ is non-orthogonal to a type q of SU-rank 1. Let $E_0 = cl_\sigma(E, a_1, \ldots, a_i)$ and $E_1 = acl_\sigma(E, a_1, \ldots, a_i)$.

If q is fully stable, then it is also modular by (4.3) and (4.10), in which case, by (3.4), there is $a_{i+1} \in acl_\sigma(E, a)$ such that $tp(a_{i+1}/E_1)$ is fully stable modular of rank 1. Since $E_1 = acl_\sigma(E_0)$, the same is true of $tp(a_{i+1}/E_0)$ (use (3.3)(2)).

If q is not fully stable, then q is non-orthogonal to the formula $(\sigma(x) = x)$ by Theorem (4.11), and therefore $tp(a/E_1) \not\perp (\sigma(x) = x)$. Choose c independent from a over E_0, and $b \in F \cap acl_\sigma(E_0, c, a)$, $b \notin acl_\sigma(E_0, c)$; by (3.7), we may assume that $b \in cl_\sigma(E_0, c, a)$. Let $a_{i+1} = Cb(b, c/acl_\sigma(E_0, a))$. Then $a_{i+1} \in acl_\sigma(E_0, a)$, and $a_{i+1} \notin acl_\sigma(E_0)$; moreover, $a_{i+1} \in cl_\sigma(b_1, c_1, \ldots, b_m, c_m)$ for some independent realisations of $tp(b, c/E_0(a))$. Then a_{i+1} and $c_1, \ldots, c_m$ are independent over E_0, so that, by (5.2), $tp(a_{i+1}/E_0)$ is qf-internal to the fixed field F.

(5.6) Theorem (Description of fully stable types in char. 0)**.** *Let p be a type of finite SU-rank. Then p is fully stable if and only if every extension of p is orthogonal to the fixed field.*

Proof. Necessity is essentially immediate: assume that some extension p' of p is non-orthogonal to $(\sigma(x) = x)$. By (the proof of) Lemma (4.2)(5), p' is not definable. By Lemma 2 of the Appendix, this implies that p' and p are not fully stable.

For the sufficiency, we use induction on $SU(a/A)$ for $A = acl_\sigma(A)$ containing the set over which p is defined, and a a realisation of p. Our hypothesis on p implies that any type of SU-rank 1 non-orthogonal to $tp(a/A)$ is orthogonal to the formula $(\sigma(x) = x)$. Hence, by (5.5) there is $b \in acl_\sigma(A, a)$ such that $SU(b/A) = 1$ and $tp(b/A)$ is fully stable. Then $SU(a/A, b) = n - 1$, and by the induction hypothesis $tp(a/A, b)$ is fully stable; by Lemma 3 of the Appendix, $tp(ab/A)$ is fully stable, and hence so is $tp(a/A)$.

(5.7) Proposition. *Let p and q be (possibly incomplete) types. If p is qf-internal to q and q is stably embedded, then so is the set $P \cup Q$ of realisations of p and q.*

Proof. The usual canonical basis argument shows that we may assume that $P \subseteq cl_\sigma(B, Q)$ for some small set B of realisations of p. Fix a, and let $Q_0 \subseteq Q$ be small and such that $tp(a, B/Q_0) \vdash tp(a, B/Q)$; then $tp(a/B, Q_0) \vdash tp(a/B, Q)$, and therefore $tp(a/B, Q_0) \vdash tp(a/P, Q)$.

(5.8) Proposition (char. 0)**.** *Let E be a difference field and assume that $tp(a/E) \perp^a (\sigma(x) = x)$, and that $dcl(E)$ is relatively algebraically closed in $dcl(EF)$.*

1. *Then $tp(a/E) \vdash tp(a/EF)$ and $tp(a/acl_\sigma(E)) \vdash tp(a/acl_\sigma(EF))$.*
2. *Assume that S is definable over E, and that $h : S \to F^k$ is a finite-to-one (algebraic, E-definable) map. Then $tp(a/acl_\sigma(E)) \vdash tp(a/ES)$.*
3. *Assume that $tp(a/E) \perp (\sigma(x) = x)$; let S be defined over E, and $h : S \to F^k$ a finite-to-one definable map (not necessarily over E). Then $tp(a/acl_\sigma(E)) \vdash tp(a/ES)$.*

In both (2) and (3), Lemma 1 of the Appendix applies and gives that $tp(a/ES)$ is definable over $acl_\sigma(E)$, and S is stably embedded (over $acl_\sigma(E)$).

Proof. (1) Assume that a' realises $tp(a/E)$; then there is an isomorphism between $K = acl_\sigma(Ea)acl_\sigma(EF)$ and $acl_\sigma(Ea')acl_\sigma(EF)$ which sends a to a' and is the identity on EF. To prove both assertions it therefore suffices to show that all extensions of $\sigma|_K$ to K^{alg} are isomorphic. By (2.8), it is enough to show that K has no proper finite Galois extension L such that $\sigma(L) = L$. Suppose by way of contradiction that L is such a Galois extension. By (4.9), this implies that

$tp(a/E)[k] \not\perp^a (\sigma^k(x) = x)$ for some integer k; but this is absurd since every new realisation of $\sigma^k(x) = x$ gives a new realisation of $\sigma(x) = x$.

(2) We have $S \subseteq acl_\sigma(EF)$; the result follows by (1)

(3) Assume that the formula $\varphi(x, y, c)$ defines the map h; then there is an E-definable set T consisting of elements d such that $\varphi(x, y, d)$ defines a finite-to-one map from S to F^k. It is enough to show that $tp(a/acl_\sigma(E)) \vdash tp(a/acl_\sigma(Es))$ for $s \in S$. Choose d in T independent from a, s over E, and let $E' = acl_\sigma(Ed)$; by (2)

$$(*) \qquad tp(a/E') \vdash tp(a/acl_\sigma(Es)).$$

Let $t \in F^k$ be such that $\varphi(s, t, d)$ holds; by the orthogonality of $tp(a/E)$ to the fixed field, a and t are independent over E', and therefore a and s are independent over E'. Hence a, E', s form an independent triple over $acl_\sigma(E)$. By the independence theorem and $(*)$, it follows that $tp(a/acl_\sigma(E)) \vdash tp(a/acl_\sigma(Es))$.

(5.9) Proposition (char. 0)**.** *Let φ be a formula orthogonal to the fixed field; then φ is fully stable.*

Proof. Clear by (5.6) and Lemma 2 of the Appendix.

(5.10) Theorem (char. 0)**.** *Let φ be a formula orthogonal to the fixed field. Consider the set S of realisations of φ inside a model M of $ACFA$, together with the structure induced by M, and let $T = \mathrm{Th}(S)$. Then T is modular (one-based).*

Proof. By (5.9), T is superstable of finite U-rank; by (4.3) and (4.10) (and elimination of imaginaries in $ACFA$), all types of U-rank 1 in T^{eq} are modular. Hence Buechler's result [2] applies and gives the result.

(5.11) Galois theory for types qf-internal to the fixed field. Let $q = tp(a/A)$ be a type qf-internal to the fixed field F. At one extreme, $a \in cl_\sigma(A, F)$, which implies that every automorphism fixing $A \cup F$ fixes every realisation of q. However, if $a \notin cl_\sigma(A, F)$, then the action of an automorphism fixing $A \cup F$ on the realisations of q may be non-trivial. One reduces this study to the case where q is almost orthogonal to the fixed field.

Theorem. *Assume that $q = tp(a/A)$ is qf-internal to F, and $q \perp^a (\sigma(x) = x)$. Let Q be the set of realisations of q in a universal domain M. There are an ∞-definable group G, defined over A, qf-internal to F, and an A-definable action of G on Q. Moreover G acts transitively on the elements of Q and fixes F.*

Proof. Let $G_1 = \mathrm{Aut}(M/A, F)$. By (5.2), there is a semi-type r over A such that $Q \subseteq cl_\sigma(A, c, F)$ whenever c realises r; moreover, inspection of the proof of (5.2) shows that for some finite set d of realisations of q, the set R of realisations of r is contained in $cl_\sigma(A, d, F)$.

Let $N = \mathrm{Aut}(M/A, F, Q)$ $(= \mathrm{Aut}(M/A, F, R))$; then $N \lhd G_1$. Let $G_2 = G_1/N$; then G_2 acts faithfully on Q and on R (by definition of N). Since $Q \subseteq cl_\sigma(A, c, F)$ for any $c \in R$, G_2 acts freely on R: if $g \in G_2$ fixes an element from R, then g fixes Q and therefore equals 1.

For $c \in R$, let $A_c = A \cup (acl_\sigma(A, c) \cap F)$, and let R_c be the set of realisations of $tp(c/A_c)$. Then G_1 acts transitively on R_c: since $tp(c/A_c) \perp^a (\sigma(x) = x)$, by (5.8) $tp(c/A_c) \vdash tp(c/A, F)$. Thus the map $g \mapsto g(c)$ gives a bijection between G_2 and R_c.

Since $Q \subseteq cl_\sigma(A, c, F)$, there are an ∞-definable subset D_c of F^m, and a definable bijection $f_c : Q \to D_c$ (by (1.10) and (1.11)); thus an element $d \in R_c$ induces

$g_d = f_d^{-1} \circ f_c : Q \to Q$. Let $G = \{f_d^{-1} \circ f_c \mid d \in R_c\}$, the group law being composition. Note that G is ∞-definable over A and c, and its group law and its action on Q are definable over A, c.

Claim. If $d = g(c)$ for $g \in G_2$, then $f_d^{-1} \circ f_c$ and g have the same action on Q.

Proof. Applying g to $f_c(x) = y$, we obtain $f_d(g(x)) = y$ (because $y \in F$), which precisely says that $f_d^{-1} \circ f_c(x) = g(x)$.

We therefore have a canonical isomorphism: $(G_2, \cdot) \simeq (G, \circ)$.

Suppose that d realises $tp(c/A)$, and let G_d be the associated group; then the isomorphism between $(G, \circ)$ and $(G_d, \circ)$ (induced by the isomorphisms with G_2) is definable over A, c, d. Hence in fact $(G, \circ)$ and its action on Q are (∞-)definable over A.

Remark. Since G is qf-internal to F, there is a definable bijection between G and some ∞-definable subset H of F^m, which is therefore also endowed with a definable group structure. By (1.11), the group H is ∞-definable in the pseudo-finite field F (see [19] for the theory of groups of finite (S_1-)rank defined over F). In particular, it is shown there that every infinitely definable group is contained in a definable group, and is the intersection of subgroups of finite index thereof. Also, definable groups are definably isomorphic to subgroups of finite index of groups of the form $H(F)$, where H is some algebraic group over F. Simple groups can be classified and have to do with the classical groups (unitary, orthogonal, etc.).

(5.12). In the modular case, a similar result holds. However here it is somehow less significant, and the main statement is this:

Theorem. *Let p be a non-trivial modular type defined over $E = acl_\sigma(E)$, with $SU(p) = 1$. Then there exist a simple abelian variety A defined over E, or $A = \mathbb{G}_m$, or $A = \mathbb{G}_a$, and a definable subgroup H of A, of SU-rank 1, with generic type non-orthogonal to p. The case $A = \mathbb{G}_a$ can only occur when the characteristic is positive.*

Proof. Changing p if necessary, we may assume that if a realises p then $\sigma(a) \in E(a)^{alg}$. We work over E. By non-triviality, there are a_1, a_2, a_3, a_4 realising p such that any triple is independent, but a_1, a_2, a_3, a_4 is not independent; by modularity and elimination of imaginaries, this implies that $acl_\sigma(a_4, a_1) \cap acl_\sigma(a_2, a_3) = acl_\sigma(a_1')$, $acl_\sigma(a_4, a_2) \cap acl_\sigma(a_1, a_3) = acl_\sigma(a_2')$ and $acl_\sigma(a_4, a_3) \cap acl_\sigma(a_1, a_2) = acl(a_3')$, for some a_1', a_2', a_3' of SU-rank 1. Enlarging a_i' we may assume that $\sigma(a_i') \in E(a_i')^{alg}$; then the algebraic closures are in fact in ACF (over E), so that we have the abelian group configuration in ACF. By standard results, see Chapter 5, Theorem 4.5 of [26], there are an abelian algebraic group A defined over E, and elements b_i, $i = 1, 2, 3, 4$, realising the generic of A (in ACF) such that a_i and b_i are equi-algebraic (over E), and $b_1 + b_4 = b_2 + b_3$. Going back to $ACFA$, we let $q = qftp(b_1)$, and for a independent from b_1 and realising q, we let $r = qftp(b_1 - a)$. Observe that any type extending q is non-orthogonal to any type extending r, which implies that for Q the set of realisations of q and R the set of realisations of r, Q and R are modular, of SU-rank 1.

Define $H = \{a \in A \mid \text{ for generic } b \in Q,\ a + b \in Q\}$; by (2.14), H is definable by a quantifier-free formula.

Claim. H is a group of SU-rank 1, $H = R \cup acl_\sigma(\emptyset)$, every element of H can be written as the sum of two elements in R, and the types extending r are the generics of H.

Proof. Clearly H is a group, of SU-rank 1. Let $a \in H$, $a \notin acl_\sigma(\emptyset)$; choose $b \in Q$ independent from a; since $a+b$ is independent from b and realises q, and everything is quantifier-free, $(a+b)-b$ realises r. Now let $c \in acl_\sigma(\emptyset)$; then $a-c \in H$ and $a-c \notin acl_\sigma(\emptyset)$, so that $(a-c) \in R$, which proves the next assertion. Finally, the last statement is by definition of generic.

It now remains to show the assertions on A. For that, observe that A is simple (as an algebraic group). Indeed, let B be an infinite algebraic subgroup of A. Then, either $H \cap B$ is infinite, which implies that $dim(B) = dim(H)$ since $SU(H) = 1$, and therefore $B = A$. Or $H \cap B$ is finite; but $dim(A/B) < dim(A) = dim(H)$, which gives a contradiction. Hence A is either a simple abelian variety, or $\mathbb{G}_m$, or $\mathbb{G}_a$. In characteristic 0 it cannot be $\mathbb{G}_a$, since the only algebraic automorphisms of $\mathbb{G}_a$ are linear. One then shows that H must be of deg_σ 1, commensurable to a group defined by a linear equation $\sigma(x) = ax$ for some $a \in K$; but the formula $\sigma(x) = ax$ is non-orthogonal to the fixed field, which contradicts our modularity hypothesis.

Remark (char. 0). Let H be as above, C a subset of A and $b \in H$ non-algebraic; let $H^* = \bigcap_{n\in\mathbb{N}} nH$. Then since H has rank 1, every definable infinite subgroup of H contains H^*; since H is modular, $tp(b/C)$ is therefore determined by the coset of b modulo H^*.

6. Examples

In this section we will give various examples, which show that many of our results are in some sense best possible.

(6.1). The equation $\sigma(x) = x^2 + b$ (char. 0).

Let $E = acl_\sigma(E)$, and consider a solution a of $\sigma(x) = x^2 + b$, where $b \in E$. By (4.8) and (4.2), $tp(a/E)$ has a unique non-forking extension to any F containing E. We will show that the formula $\sigma(x) = x^2 + b$ is strongly minimal if $b \neq 0$; for $b = 0$, there are several possibilities, depending on the action of σ on the primitive roots of 1. We also study the non-orthogonality relation between such types, and show that its equivalence classes are least possible.

To determine whether or not $tp(a/E)$ is strongly minimal, we need to study the finite σ-stable extensions of the field $K =_{\text{def}} E(a)_\sigma$.

Suppose that L is a finite Galois extension of K which is stable under σ; write L as KL_1 for some finite Galois extension L_1 of $E(a)$ satisfying $[L : K] = [L_1 : E(a)]$. Then $\sigma(L_1) \subseteq L_1$, $E(\sigma^{-1}(a))$ and L_1 are linearly disjoint over $E(a)$, and $\sigma^{-1}(L_1) = E(\sigma^{-1}(a))L_1$.

Let $\mathcal{S}$ be the set of finite E-valuations on $E(a)$ which ramify in L_1; we know that $\mathcal{S}$ is non-empty. For $\alpha \in E$, we write $(a \to \alpha)$ for the valuation on $E(a)$ positive on $(a - \alpha)$. Observe that $(a \to \sigma^{-1}(b))$ is the only (finite) valuation ramifying in $E(\sigma^{-1}(a))$.

Assume that $(a \to \alpha)$ ramifies in L_1, for some $\alpha \neq \sigma^{-1}(b)$; since it does not ramify in $E(\sigma^{-1}(a))$, it has exactly two extensions to $E(\sigma^{-1}(a))$ and they both ramify in $\sigma^{-1}(L_1)$. These extensions can be described as $(\sigma^{-1}(a) \to \pm\sqrt{\alpha - \sigma^{-1}(b)})$. Taking images by σ, the two valuations $(a \to \pm\sqrt{\sigma(\alpha) - b})$ ramify in L_1.

Assume now that $(a \to \sigma^{-1}(b))$ ramifies in L_1, with ramification index $e \neq 2$; then the extension $\sigma^{-1}(L_1)$ of $E(\sigma^{-1}(a))$ is ramified at the unique extension of

$(a \to \sigma^{-1}(b))$, i.e. at $(\sigma^{-1}(a) \to 0)$, with ramification index e or $e/2$. Thus $(a \to 0)$ ramifies in L_1.

We define an oriented graph relation I on $\mathcal{T} =_{\text{def}} \{\alpha \mid (a \to \alpha) \in \mathcal{S}\}$ as follows: $\alpha I \beta \iff \sigma(\alpha) = \beta^2 + b$. We have therefore shown that if $\alpha \in \mathcal{T}$ and $\alpha \neq \sigma^{-1}(b)$, then for some β we have

$$\beta \in \mathcal{T}, -\beta \in \mathcal{T}, \alpha I \beta, \alpha I(-\beta).$$

Assume that $\mathcal{T}$ contains an element α with $\alpha \neq \sigma^{-1}(b)$; since $\mathcal{T}$ is finite, any path through α must be a loop. If n is the length of such a loop, one checks that α is then a solution of the equation $\sigma^n(X) = p^{(n)}(X)$, where $p^{(n)}(X) \in E[x]$ is defined by $\sigma^n(a) = p^{(n)}(a)$. Thus there is an N which will work for all α's in $\mathcal{T} \setminus \{\sigma^{-1}(b)\}$. But $\sigma^N(\alpha) = p^{(N)}(\alpha)$ implies $\sigma^N(-\alpha) = -p^{(N)}(\alpha)$, and therefore $\mathcal{T} \subseteq \{0, \sigma^{-1}(b)\}$. There are now two cases to consider.

Case 1. $b \neq 0$.

Then $0 \in \mathcal{T}$ implies that $\pm\sqrt{-b} \in \mathcal{T}$, which is impossible. Hence the only (finite) valuation which ramifies in L_1 is the valuation $(a \to \sigma^{-1}(b))$, and its ramification index is 2. This implies that $L_1 = E(a, \sqrt{a - \sigma^{-1}(b)}) = E(\sigma^{-1}(a))$, which contradicts our choice of L_1, since we assumed it is linearly disjoint from K over $E(a)$.

By (2.8), the formula $\sigma(x) = x^2 + b$ is therefore strongly minimal.

Case 2. $b = 0$.

Then $\mathcal{T} = \{0\}$, and $L_1 = E(\sqrt[e]{a})$ for some e (which is odd by linear disjointness from K over $E(a)$). Fix such an e, let ζ be a primitive e-th root of 1, and fix $b = \sqrt[e]{a}$. Let σ be defined on $K(b)$ by $\sigma(b) = b^2$, let $\tau \in \mathcal{G}al(K(b)/K)$ be defined by $\tau(b) = \zeta^j b$ and let k be such that $\sigma(\zeta) = \zeta^k$ and $1 \leq k < e$; then $[\sigma, \tau](b) = \sigma^{-1}(\zeta)^{j(k-2)} b$. Thus, if $k \neq 2$, then all extensions of σ to $K(b)$ are conjugate by elements of $\mathcal{G}al(K(b)/K)$; if $k = 2$, then there are e non-isomorphic extensions of σ to L_1, and the formula $\sigma(a) = a^2$ is not strongly minimal.

We now are concerned with the triviality of such types when $b \neq 0$. This will follow from our next lemma.

Lemma. *Let E be a difference field, and let $a \notin acl_\sigma(E)$ be such that $\sigma(a) = a^2 + b$ for some $b \in E$, $b \neq 0$. Assume that $c \in acl_\sigma(Ea) \setminus acl_\sigma(E)$ is such that $\sigma(c) = c^2 + d$ for some $d \in E$. Then $c = \sigma^k(a)$ for some $k \in \mathbb{Z}$.*

Step 1. $c \in E(a)_\sigma$.

Replacing c by an appropriate transform, we may assume that $[E(a, c) : E(a)] = [E(a)_\sigma(c) : E(a)_\sigma]$. Then $[E(a, \sigma(c)) : E(a)] = [E(\sigma(a), \sigma(c)) : E(\sigma(a))] = [E(a, c) : E(a)]$, which implies that $E(a, c) = E(a, \sigma(c))$; from this we deduce that $E(a, c)_\sigma = E(a)_\sigma(c)$, which is only possible if $c \in E(a)_\sigma$, since $E(a)_\sigma$ has no finite proper algebraic extension stable under σ.

Step 2. $E(c) = E(\sigma^k(a))$ for some $k \in \mathbb{Z}$.

Let j be minimal such that $E(c) \supseteq E(\sigma^j(a))$; replacing c by a transform, we may assume that $j = 0$. Let k be minimal such that $E(\sigma^{-k}(a)) \supseteq E(c)$, and assume that $k > 0$. Then $E(c, \sigma^{-1}(a)) \subseteq E(\sigma^{-k}(a))$, and therefore $E(\sigma(c), a) \subseteq E(\sigma^{-k+1}(a))$; also $[E(c) : E(\sigma(c))] = 2 = [E(a) : E(\sigma(a))]$ and $E(\sigma(c)) \cap E(a) = E(\sigma(a))$, which

implies that $E(c) = E(a, \sigma(c))$. Hence $E(c) \subseteq E(\sigma^{-k+1}(a))$, a contradiction. This implies that $k = 0$.

Replacing c by an appropriate transform, we may therefore assume that $E(a) = E(c)$; thus for some $\alpha, \beta, \gamma, \delta \in E$ such that $\alpha\delta - \beta\gamma \neq 0$, we have $c = \frac{\alpha a+\beta}{\gamma a+\delta}$. Applying σ, we then obtain

$$\left(\frac{\alpha a + \beta}{\gamma a + \delta}\right)^2 + d = \frac{\alpha(a^2 + b) + \beta}{\gamma(a^2 + b) + \delta};$$

looking at poles, given that $b \neq 0$, we obtain that $\gamma = 0$, and hence we may assume that $c = \alpha a + \beta$, with $\alpha \neq 0$. Thus

$$\alpha^2 a^2 + 2\alpha\beta a + \beta^2 + d = \alpha a^2 + \alpha b + \beta,$$

which implies $\beta = 0$ and $\alpha = 1$.

From the lemma, we deduce two things:

(1) If $b \neq 0$, then the type $\sigma(x) = x^2 + b$ is trivial.
(2) $(\sigma(x) = x^2 + b) \not\perp (\sigma(x) = x^2 + d)$ implies that $d = \sigma^k(b)$ for some $k \in \mathbb{Z}$.

(6.2). An unstable type of SU-rank 2 orthogonal to the fixed field (and therefore superficially stable) (char. 0).

Let $E = acl_\sigma(E)$, and consider a generic solution (a, b) of the equations

$$\sigma(x) = x + y, \quad \sigma(y) = y^2 + 1.$$

Then a lies in an additive coset of the fixed field F, and therefore $tp(a/Eb)$ is unstable, which implies that $tp(a/E)$ is also unstable. We claim that $tp(a/E)$ however is superficially stable, and therefore has a unique non-forking extension to any set containing E, and is definable. This claim is equivalent to the claim that $tp(a/E)$ is orthogonal to the fixed field.

Let $E' = acl_\sigma(E')$ contain E and be independent from a over E. In (6.1), we showed that the field $E'(b)_\sigma$ has no proper finite Galois extension stable under σ, and therefore no proper finite algebraic extension stable under σ. Assume that $a' \in E'(b)^{alg}$ satisfies $\sigma(a') = a' + b$; then $\sigma(E'(b)_\sigma(a')) = E'(b)_\sigma(a')$, which implies that $a' \in E'(b)_\sigma$. We want to reach a contradiction.

Let $k \in \mathbb{Z}$ be least such that $\sigma^k(a') \in E'(b)$. Then $k \geq 0$: $\sigma^k(a') - \sigma^{k+1}(a')$ is also in $E'(b)$, and equals $\sigma^k(b)$. Write $\sigma^k(a')$ as $p(b)/q(b)$, where p, q are relatively prime polynomials with coefficients in E'; then

$$\sigma^{k+1}(a') = \frac{p(b)}{q(b)} + \sigma^k(b) = \frac{p^\sigma(b^2 + 1)}{q^\sigma(b^2 + 1)},$$

and degree considerations imply that $q(b) = 1$, that is, $\sigma^k(a') = p(b)$, $\sigma^{k+1}(a') = p(b) + \sigma^k(b) = p^\sigma(b^2 + 1)$. The minimality of k implies that $\sigma^k(a') \notin E'(b^2 + 1)$, and therefore $p(b) \notin E'(b^2 + 1)$; then $\sigma^{k+1}(a') = p(b) + \sigma^k(b) \in E'(b^2 + 1)$ implies that $\sigma^k(b) \notin E'(b^2 + 1)$ and therefore that $k = 0$. Thus $\sigma(a') = p(b) + b = p^\sigma(b^2 + 1)$, and degree considerations give the desired contradiction.

This implies that $tp(a/E)$ is orthogonal to the fixed field: if $c \in acl_\sigma(E'a) \setminus E'$ satisfies $\sigma(c) = c$, then $a \in acl_\sigma(E'(b, c))$, which contradicts our statement, with E' replaced by $E'(c)^{alg}$.

(6.3) (char. 0)**.** Undefinability of the rank.

(All results on elliptic curves can be found in [10], Ch. IV.4.) Consider the family of elliptic curves $C(\lambda)$, $\lambda \neq 0, 1$, where $C(\lambda)$ is defined by the equation

$$x_2^2 = x_1(x_1 - 1)(x_1 - \lambda).$$

The j-invariant of $C(\lambda)$ is then $j(\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$, and depends only on the isomorphism type of the variety $C(\lambda)$ (thus λ, $1/\lambda$, $1-\lambda$, $1/(1-\lambda)$, $\lambda/(1-\lambda)$ and $(\lambda-1)/\lambda$ all give the same curve).

We assume that σ is the identity on $\mathbb{Q}^{alg}$. We work over an algebraically closed difference field E. Let d be an integer, and consider the formula

$$\varphi(x, y) : x_2^2 = x_1(x_1 - 1)(x_1 - y) \wedge \sigma(y) = y \wedge \sigma^2(x) + [d]x = 0,$$

where $x = (x_1, x_2)$, "+" is taken in the sense of the elliptic curve, and $[d]$ is multiplication by d on the elliptic curve.

If $d = 1$, then $\varphi(x, \lambda)$ is non-orthogonal to the fixed field; one checks easily that $SU(\varphi(x, \lambda)) = 2$. Assume now that $d > 1$.

The ring R_λ of endomorphisms of $C(\lambda)$ is in general isomorphic to $\mathbb{Z}$, except for countably many values of λ, which are algebraic over $\mathbb{Q}$, in which case one says that $C(\lambda)$ has complex multiplication, and the ring R_λ is isomorphic to a subring of the ring of integers of $\mathbb{Q}(\sqrt{-n})$ for some positive integer n. Moreover, given a positive integer d, there are infinitely many values of λ for which $R_\lambda \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{-d})$.

Claim ($d > 1$). $SU(\varphi(x, \lambda)) = 2 \iff R_\lambda \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{-d})$.

Proof. Assume that $R_\lambda \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{-d})$; then $m\sqrt{-d} \in R_\lambda$ for some integer m. If e is the corresponding endomorphism then the equation $\sigma^2(x) + [d]x = 0$ implies $([m]\sigma - e)([m]\sigma + e)(x) = 0$, which has SU-rank 2. Indeed, let a be a generic solution of $\varphi(x, \lambda)$. Then $deg_\sigma(a/\mathbb{Q}^{alg}) = 2$. If $b = [m]a + e(a)$, then $[m]\sigma(b) - e(b) = 0$, which implies that $deg_\sigma(b/\mathbb{Q}^{alg}) = 1$. Hence $tp(a/\mathbb{Q}(b)^{alg})$ forks over $\mathbb{Q}^{alg}$ and is not algebraic, i.e., $SU(a/\mathbb{Q}^{alg}) = 2$.

For the converse, assume that $SU(\varphi(x, \lambda)) = 2$, and let $E' = acl_\sigma(E')$ and a satisfying $\varphi(x, \lambda)$ be such that $tp(a/E')$ forks over E, but is non-algebraic. Then $deg_\sigma(a/E') = 1$. Since $\mathrm{Mult}(a/E(\sigma^2(a))) = d^2$, it follows that $tp_2(a/E)$ is unbounded of deg 1; hence it is stable by (4.8) and (4.2), and so is $tp(a/E)$ (by a reasoning similar to that given in (4.10)).

Consider the group G of realisations of $\varphi(x, \lambda)$ in $K \models ACFA$ with the structure induced from K. By (5.10), G is modular. By [18], this implies that the formula determining $qftp(a/E')$ is equivalent to a Boolean combination of cosets of definable subgroups of G. One of them, say H, will have SU-rank 1. Thus without loss of generality we will assume that $a \in H$.

Let $S \subseteq C(\lambda) \times C(\lambda)$ be the Zariski closure of the subgroup $H' =_{\mathrm{def}} \{(b, \sigma(b)) \mid b \in H\}$; then S is a subgroup of $C(\lambda) \times C(\lambda)$, which projects generically onto each factor $C(\lambda)$ and is of dimension 1 since $(a, \sigma(a))$ is a generic point of S. Let $m = |S \cap (0) \times C(\lambda)|$. Then the set $T = \{(x, [m]y) \mid (x, y) \in S\}$ is the graph of a morphism $\psi : C(\lambda) \to C(\lambda)$, and $\psi(a) = [m]\sigma(a)$. Thus $\psi \circ \psi(a) = [m^2]\sigma^2(a) = [-dm^2]a$. Since $(a, \psi(a))$ is a generic point of T, R_λ must contain an element whose square behaves like $[-dm^2]$, i.e., $R_\lambda \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{-d})$.

Hence the set of λ for which $SU(\varphi(x, \lambda)) = 2$ is countably infinite; this set is therefore not definable.

(6.4) (char. 0)**.** Examples of difference-field Galois groups.

Let A be a simple abelian variety of dimension d, defined over the field F fixed by σ. For b in A, let $A(b) = \{x \in A \mid \sigma(x) = x + b\}$. Then $A(0)$ is simply the set of F-rational points of A, and any other $A(b)$ is a coset of $A(0)$ in A. Thus $SU(A(0)) = SU(A(b)) = d$. By a generic b of A, we mean a tuple $b \in A$ such that $F(b)_\sigma$ has transformal transcendence degree d, or equivalently $SU(b/F) = \omega d$. Note that there is a unique generic of A, by (2.11)(2).

For $b \in A$, let $G(b) = Aut(A(b)/F(b))$ be the group of bijections of $A(b)$ which fix $F(b)$ and lift to automorphisms of the universal domain. Then $G(b)$ embeds naturally in $A(0)$, via $g \mapsto (g(x) - x)$, where x is any element of $A(b)$. We will now describe G in two cases: when b is a non-torsion point of $A(F)$; when b is generic.

We first recall some results on definable subgroups of $A(F)$. By (1.11), every definable subgroup of $A(F)$ is in fact definable in the pure field F. By [19], every definable subgroup H of $A(F)$ has finite index in $B(F)$, where B is the Zariski closure of H in $A(F^{alg})$, and therefore an algebraic subgroup of A. Since A is simple, every definable subgroup of $A(F)$ is therefore either infinite and of finite index, or finite. Furthermore, if (H_i) is a family of uniformly definable subgroups of $A(F)$, then there is an integer N such that for every i, either the size or the index of H_i is at most N.

We also know that $[n]A(F)$ has finite index in $A(F)$. Thus there are only finitely many definable subgroups of $A(F)$ of a given index. We define A^* to be the intersection of all subgroups of $A(F)$ of finite index; then A^* is divisible.

Claim 1. If b is a non-torsion point in $A(F)$, then $G(b)$ contains A^*.

Proof. For $\varphi(x, y)$ a formula, define

$$G_\varphi = \{g \in A(F) \mid \forall x \in A(b), \forall y \in F^{\ell(y)}\ (\varphi(x, y) \iff \varphi(x + g, y))\}.$$

Then each G_φ either is finite or contains A^*; thus, either $G(b)$ contains A^*, or $G(b)$ is finite. The latter is impossible, since then we would have $A(b) \subseteq F^{alg}$, and any tuple from F^{alg} has finite orbit, contradicting our assumption that $[n]b \neq 0$ for every n.

Claim 2. If b is generic, then $G(b) = A(F)$.

Proof. It suffices to show that any two elements a and a' of $A(b)$ have the same type over $F(b)$. Any two such elements satisfy $\sigma(x) - x$ generic, and thus are themselves generic. Thus a and a' are conjugated over F by some automorphism τ, which clearly fixes b.

Note that in either case, since $G(b)$ has SU-rank d, every element of $A(b)$ has SU-rank d over $F(b)_\sigma$.

Claim 3. If $SU(c/Fb) < d$, then any two elements of $A(b)$ which have the same type over $F(b)_\sigma$ have the same type over $F(b, c)_\sigma$.

Proof. As in Claim 1, $Aut(A(b)/F(b, c))$ is infinitely definable (over b, c), and is therefore either finite or contains A^*. If it is finite, then $A(b) \subseteq acl_\sigma(F, b, c)$, which implies $SU(a/Fb) \leq SU(c/Fb) < d$ for any $a \in A(b)$ and contradicts our previous observation.

Thus $tp(a/Fb)$ is almost orthogonal to any type of SU-rank $< d$, even though it is internal to q, for any type q of a non-algebraic element of $A(F)$.

Moreover, we know by [5], 7.5.3, that $F(b,a)_\sigma$ can be written as $F(b,c)_\sigma$, where c is a singleton. Thus there is a difference equation (over $F(b)_\sigma$) whose Galois group is precisely $A(F)$: take b generic in A.

(6.5). An example in characteristic $p > 0$.

We show that in char. $p > 0$ there are types orthogonal to every fixed field, yet unstable. Let us first remark that we have many definable subfields of a model of $ACFA_p$: for any integers m and $n \geq 1$, the set of points fixed by the automorphism $x \mapsto \sigma^n(x)x^{p^m}$ is a definable subfield that is pseudo-finite. Automatically, the type of an element of such a subfield is unstable. There are however examples of unstable types of SU-rank 1 which are orthogonal to all such types. We are in characteristic $p > 0$, and work over an algebraically closed substructure E.

Let $S = \{a \mid \sigma(a) = a^p - a\}$. Then, if $a \notin E$, $\mathrm{Mult}(a/E(\sigma(a))) = p$. Since the fields $E(\sigma^n(a))$, $n \in \mathbb{N}$, form a decreasing chain, it follows that $\mathrm{Mult}(a/E(\sigma^n(a))) = p^n$ and is therefore unbounded. This implies that $tp(a/E)$ is orthogonal to all formulas of the form $\sigma^n(x)x^{p^m} = x$ (see the argument in the proof of Theorem 4.5 which shows that boundedness is preserved by equi-algebraicity).

Now consider the set $T = \{b \mid \sigma(b)^p - \sigma(b) + b^p = 0\}$; a similar argument shows that the type over E of any element of T not in E is orthogonal to all formulas of the form $\sigma^n(x)x^{p^m} = x$.

Let $a \in S \setminus E$, $b \in T \setminus E$ be independent over E. Consider the extension L of $K = acl_\sigma(Ea)acl_\sigma(Eb)$ obtained by adding a root α of the equation $X^p - X = ab$; then $[L : K] = p$. Moreover, $\sigma(ab) - ab = a^p\sigma(b) - (b + \sigma(b))a$. By assumption, $\sigma(b) = (b + \sigma(b))^p$, and therefore $\beta = \alpha + a(b + \sigma(b))$ is a root of the equation $X^p - X = \sigma(ab)$. Hence $\sigma(L) = L$; moreover, there are p choices for $\sigma(\alpha)$, namely all the conjugates of β over K.

We define a bilinear form $q : S \times T \to \mathbb{F}_p$ by $q(x,y) = \sigma(\xi) - \xi - x(y + \sigma(y))$, for ξ a (any) root of $X^p - X = xy$. It is easy to see that this bilinear form is non-degenerate. Thus the two types are unstable.

It would be interesting to determine the induced structure on such definable groups. We feel it is likely that the induced structure on the two groups consists only of the group structure, endomorphisms, constants, and this bilinear map, and that (up to non-orthogonality) groups of this type and fixed fields are the only unstable SU-rank one types in characteristic p.

(6.6). A stable type of SU-rank 1 which is bounded (char. 0).

A natural question arises from (4.5): Does the result generalise to types of $deg_\sigma > 2$, or, equivalently, if $tp(a/E)$ is bounded and $SU(a/E) = 1$, does it follow that $deg_\sigma(a/E) = 1$? We show here that this is not the case, and that there exist stable types which are bounded.

Let A be a simple abelian variety, with endomorphism ring R, containing an invertible element u which is not a root of unity. There are such varieties, and they have dimension greater than 1. For instance let R be the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Then $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$ is of CM type, and there is an abelian variety A with $End(A) \simeq R$ (see [29], p.85). The element $(3 + 2\sqrt{2})$ is invertible in R and is not a root of 1.

Let E be an algebraically closed field containing the parameters used to define A and u, and choose a model (K, σ) of $ACFA$ which contains E and is such that σ is the identity on E. Consider the formula $\varphi(x)$: $x \in A \wedge \sigma(x) = u(x)$; since u is

invertible, if a satisfies φ then $E(a)_\sigma = E(a)$, so that $tp(a/E)$ is bounded, but in $(\mathbb{Q} \otimes R)[t]$ the polynomials $t^n - 1$ and $t - u$ are relatively prime for every $n \in \mathbb{N}$. By a result in [16], this implies that the formula $\varphi(x)$ is orthogonal to the formula $\sigma(x) = x$, and therefore every type containing $\varphi(x)$ is stable.

(6.7). A non-strongly minimal trivial type of degree 1.

We first recall some results on elliptic curves. Let $k = \mathbb{Q}^{alg}$, let J be an elliptic curve with transcendental j-invariant a, defined over $k(a)$, for instance, by the equation

$$y^2 + xy = x^3 - \frac{36}{a - 1728}x - \frac{1}{a - 1728}.$$

Then the following assertions are true.

(1) For $n \in \mathbb{N}$, the subgroup $J[n]$ of elements of J of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
(2) For $n \in \mathbb{N}$, let L be the field obtained by adjoining to $k(a)$ all elements of $J[n]$. Then $\mathcal{G}al(L/k(a)) \simeq SL_2(\mathbb{Z}/n\mathbb{Z})$.
(3) For p a prime, let L_p be the extension of $k(a)$ obtained by adjoining to $k(a)$ all points of $T_p(J)$, the p-torsion subgroup of J. Then $\mathcal{G}al(L_p/k(a)) \simeq SL_2(\mathbb{Z}_p)$, and the extensions L_p, where p varies over all primes, are linearly disjoint over k.
(4) $End(J) \simeq \mathbb{Z}$.
(5) Let A and B be subgroups of J of order p^m, and assume that there is an isomorphism $\theta : J/A \to J/B$. Then $A = B$ and $\theta = \pm 1$.

Proof. (1) See [35], III.6.4.
(2) See [31], Section 5.1.
(3) Immediate from (2).
(4) See C.11.1 in [35].
(5) Let $\varphi : J \to J/A$ and $\psi : J \to J/B$ be isogenies (with kernels A and B respectively); they have degree p^m. Consider the morphism $\eta : J \to J$ defined by $\eta = \hat{\psi} \circ \theta \circ \varphi$ ($\hat{\psi}$ is the isogeny dual to ψ; see [35, III.6] for its properties). Since $\hat{\psi}$ has degree p^m, it follows that η has degree p^{2m}. From $End(J) \simeq \mathbb{Z}$, it follows that $\eta = \pm[p^m]$. From $\hat{\psi} \circ \psi = [p^m]$, we then deduce that $\psi = \pm\theta \circ \varphi$. This implies that $A = B$, and that $\theta = \pm 1$, since J/A has transcendental j-invariant, and therefore $End(J/A) \simeq \mathbb{Z}$.

We fix an element a transcendental over $k = \mathbb{Q}^{alg}$, and consider an elliptic curve J_a with j-invariant a, defined over $k(a)$. For p a prime, define $T_p(a)$ to be the set of elements of J_a of order a power of p, let $S_p(a)$ be the set of (unordered) pairs $\{b, -b\}$ for $b \in T_p(a)$, and define $L_p = k(a, T_p(a))$, $K_p = k(a, S_p(a))$. Then L_p is a Galois extension of $k(a)$, with $\mathcal{G}al(L_p/k(a)) \simeq SL_2(\mathbb{Z}_p)$, K_p is the subfield of L_p fixed by $\{1, -1\}$, and $\mathcal{G}al(K_p/k(a)) \simeq PSL_2(\mathbb{Z}_p)$.

Fix a prime p, and a subgroup A of $T_p(a)$ such that $A_m = A \cap J_a[p^m]$ is cyclic of order p^m for every m. For $m \in \mathbb{N}$, define a_m as the j-invariant of the elliptic curve J_a/A_m. Since all cyclic subgroups of order p^m of J_a are conjugate by an automorphism of L_p over $k(a)$, it follows that, in the pure field language, the type of $(a, a_1, \dots, a_m)$ over k is completely determined by the fact that a is transcendental over k, and for some cyclic subgroup B of order p^m of J_a, a_i is the j-invariant of $J_a/[p^{m-i}]B$. In particular, $(a, a_1, \dots, a_m)$ and $(a_1, \dots, a_{m+1})$ have the same type over k. Define σ by $\sigma(a) = a_1$, $\sigma(a_m) = a_{m+1}$ for $m > 0$, and extend it to an

automorphism σ, which defines the difference field $k(a)_\sigma$. Denote $\sigma^n(a)$ by a_n for $n \in \mathbb{Z}$. Fix an isogeny $h : J_a \to J_a/A_1$.

Claim 1.

$$[k(a, a_m) : k(a)] = (p+1)p^{m-1}, \qquad k(a)_\sigma \subseteq K_p,$$
$$\mathcal{G}al(L_p/k(a)_\sigma) \simeq \{\begin{pmatrix} k & 0 \\ 0 & 1/k \end{pmatrix} \mid k \in \mathbb{Z}_p^*\}.$$

First observe that $\sigma^m(a) \in K_p$ for $m \geq 0$. Indeed, by (5), a_m is uniquely determined by the cyclic subgroup A_m of $T_p(a)$. Hence a_m and the code of the subgroup A_m are equi-definable over $k(a)$; since $\mathcal{G}al(L_p/K_p)$ does not move A_m, this implies that $a_m \in K_p$. But $J_a[p^m] \simeq \mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$ has $(p+1)p^{m-1}$ distinct cyclic subgroups of order p^m, and they are permuted by $\mathcal{G}al(L_p/k(a))$. Hence a_m has multiplicity $(p+1)p^{m-1}$ over $k(a)$.

Now consider $\hat{h} : J_{a_1} \to J_a$; it has a kernel B_1 of order p, and $h(A_2) \cap B_1 = (0)$, since $\hat{h} \circ h = [p]$. As above, we therefore have that a and the code of the subgroup B_1 are equi-definable over $k(a_1)$; hence $a \in k(a_1, S_p(a_1))$, and applying σ^{-1} we deduce the first two assertions for all $m \in \mathbb{Z}$.

Hence, the automorphisms of L_p which leave $k(a)_\sigma$ fixed are those which leave invariant the two subgroups A and B of $T_p(a)$, where B is defined as the union of the kernels of the morphisms $J_a \to J_{a_m}$ for $m < 0$; we have $T_p(a) = A \oplus B$. This gives the third assertion.

Claim 2. The code $\bar{h}$ of the set $\{h, -h\}$ is defined over $k(a)_\sigma$.

This also follows by (5), since up to a change of sign, h is determined by the j-invariants a and a_1.

Claim 3. The fields K_q for $q \neq p$ and $k(a)_\sigma$ are linearly disjoint over $k(a)$.

This is true because $k(a)_\sigma \subseteq K_p$, and the fields K_q, q a prime, are linearly disjoint over $k(a)$.

Now let q be an odd prime, $q \neq p$. For $m \in \mathbb{N}$, define $K_{q,m}$ to be the Galois extension of $k(a)_\sigma$ obtained by adjoining to $k(a)_\sigma$ the codes of the pairs $\{b, -b\}$ for $b \in J_a[q^m]$.

Claim 4. $k(a)_\sigma(S_q(a)) = k(a)_\sigma(S_q(a_1))$; also, $k(a)_\sigma K_q$ and $K_{q,m}$ are σ-invariant.

Indeed, h defines a group isomorphism: $T_q(a) \to T_q(a_1)$, and therefore $\bar{h}$ defines a bijection between $S_q(a)$ and $S_q(a_1)$; thus for $b \in T_q$, $\{b, -b\}$ and $\bar{h}(\{b, -b\})$ generate the same extension of $k(a)_\sigma$. This proves the assertions.

Claim 5. σ has at least two non-conjugate extensions to $K_{q,m}$, provided $q > 3$.

To show that there is more than one way of defining σ on $K_{q,m}$ (up to isomorphism), it suffices, by (2.6), to show that some extension of σ has non-trivial centraliser in $\mathcal{G}al(K_{q,m}/k(a)_\sigma)$. Let us first produce such an extension.

Choose b_1, b_2 of order q^m and generating $J_a[q^m]$. Let $c_1, c_2 \in J_{a_1}[q^m]$ be such that $tp(a, b_1, b_2/k) = tp(a_1, c_1, c_2/k)$ (types are here in the pure field language); then c_1, c_2 generate $J_{a_1}[q^m]$, and so do $h(b_1)$, $h(b_2)$. Thus there is an element $\tau \in \mathcal{G}al(\mathbb{Q}(a_1, c_1, c_2)/\mathbb{Q}(a_1)) \simeq GL_2(\mathbb{Z}/q^m\mathbb{Z})$, such that $\tau(c_i) = h(b_i)$ for $i = 1, 2$. Thus for some $\ell \in (\mathbb{Z}/q^m\mathbb{Z})^*$, (c_1, c_2) and $(h(b_1), [\ell]h(b_2))$ realise the same type over

$k(a_1)$. Since $k(a)_\sigma$ and $k(a_1, c_1, c_2)$, are linearly disjoint over $k(a_1)$, they realise the same type over $k(a)_\sigma$.

Thus we may extend σ to $K_{q,m}$ by setting

$$\sigma(\{b_1, -b_1\}) = \{h(b_1), -h(b_1)\}, \qquad \sigma(\{b_2, -b_2\}) = \{[\ell]h(b_2), -[\ell]h(b_2)\}.$$

Let c be an invertible element of $\mathbb{Z}/q^m\mathbb{Z}$, $c \neq 1, -1$. Then the element $\tau \in \mathcal{G}al(K_{q,m}/k(a)_\sigma)$ defined by

$$\tau(\{b_1, -b_1\}) = \{[c]b_1, -[c]b_1\}, \tau(\{b_2, -b_2\}) = \{[1/c]b_2, -[1/c]b_2\}$$

commutes with σ: observe first that $\bar{h}$ and τ commute, since $\bar{h}$ is defined over $k(a)_\sigma$. Hence

$$\begin{aligned}
\tau\sigma(\{b_1, -b_1\}) &= \tau h(\{b_1, -b_1\}) = h\tau(\{b_1, -b_1\}) \\
&= h(\{[c]b_1, -[c]b_1\}) = \sigma\tau(\{b_1, -b_1\}), \\
\tau\sigma(\{b_2, -b_2\}) &= \tau h(\{b_2, -b_2\}) = h\tau(\{b_2, -b_2\}) \\
&= h(\{[1/c]b_2, -[1/c]b_2\}) = \sigma\tau(\{b_2, -b_2\}).
\end{aligned}$$

There are $\big((q-1)q^{m-1}/2\big) - 1$ such elements τ.

We have therefore shown that no extension of $r = qftp(a/k)$ is strongly minimal.

Claim 6. Assume that a realises r and $p = tp(a/k)$ is non-trivial. Then there is a finite Galois extension L of $k(a)_\sigma$ such that $qftp(L^{ab}/K) \vdash tp(a/K)$.

By Claim 1 and (4.8), $tp(a/k)$ is stable and therefore modular. By (5.12) there exist a k-definable abelian group A of SU-rank 1, and a generic b of A equi-algebraic with a over k. Replacing k if necessary by some larger algebraically closed structure independent from a over k, we may assume that b is inside the connected component $A^* = \bigcap_n nA$ of A. Now define $b_1 = b$, $nb_{n+1} = b_n$. Then $qftp(b_1, \dots, b_n, \dots /k) \vdash tp(b_1, \dots, b_n, \dots /k)$. Since a is algebraic over $E(b)$, $qftp(a, b_1, \dots, b_n, \dots /k)$ determines $tp(a, b_1, \dots, b_n, \dots /k)$ up to finitely many possibilities. Adding some finite c from $k(a)^{alg}$, we have $qftp(a, c, b_1, \dots, b_n, \dots /k) \vdash tp(a/k)$.

Observe that $k(a, c, b_1, \dots, b_n, \dots)$ is an abelian extension of $k(a, c, b_1)$. We will show that no such thing is true of $tp(a/k)$.

Claim 7. All extensions of r are trivial.

Assume that $tp(a/k)$ is non-trivial, and let $c, b_1, b_2, \dots$ be as in Claim 6, and $L = k(a, c, b_1)_\sigma$. As a difference field, L is finitely generated over $k(a)_\sigma$; hence, there is a finite set I_0 of prime numbers q containing p and such that L and the fields $K_q(a)_\sigma$, q a prime not in I_0, are linearly disjoint over $k(a)_\sigma$. Since the groups $PSL_2(\mathbb{Z}_q)$ have no abelian quotient, L^{ab} and the fields $K_q(a)_\sigma$, q a prime not in I_0, are linearly disjoint over $k(a)_\sigma$. Hence the restriction of σ to L^{ab} has infinitely many extensions to K_q, which contradicts Claim 6.

Remarks. (1) Let q be a prime, $q \neq p$, and assume that b_1, b_2 generate $J_a[q^m]$. Then $h(b_1), h(b_2)$ generate $J_{a_1}[q^m]$, which implies that (a, b_1, b_2) and $(a_1, h(b_1), h(b_2))$ realise the same type over $\mathbb{Q}$. Thus, whether they realise the same type over k will depend on the action of σ on $\mathbb{Q}(\mu_q)$ (μ_q the group of all roots of unity of order a power of q).

Assume that there is an extension of σ to K_q such that σ and $\bar{h}$ agree on $S_q(J_a)$; since $\bar{h} \in k(a)_\sigma$, it commutes with all elements of $\mathcal{G}al(K_q k(a)_\sigma / k(a)_\sigma)$, and therefore the isomorphism types over $k(a)_\sigma$ of the extensions of σ to K_q are in one-to-one correspondence with the conjugacy classes of $PSL_2(\mathbb{Z}_q)$.

(2) One shows easily that K_p is σ-stable. However L_p is probably not: indeed h is defined over $k(a, J_a[p], J_{a_1}[p])$, while it is not defined over $K_p(J_a[p])$.

(3) Similarly, one shows that $L_q k(a,h)_\sigma$ is σ-invariant.

(4) One can show that any extension of σ to K_p commutes with the elements of $\mathcal{G}al(K_p/k(a)_\sigma)$. Hence the isomorphism types of extensions of σ to K_p are in one-to-one correspondence with the elements of $\mathcal{G}al(K_p/k(a)_\sigma)$.

(6.8). An example showing that qf-internality is stronger than internality.

We find two types p and q with p internal to q, but not qf-internal to q. Assume that σ is the identity on $E_0 = \mathbb{Q}^{alg}$, and let $q(x)$ be the (non-algebraic) type over E_0 given by the equation $\sigma(x) = x^2 + 1$. By (6.1) we know that this type is strongly minimal and trivial. Let a realise q, let α be a cubic root of a, and consider the element $\beta = \alpha\sigma(\alpha)^2$. Then $\beta \notin E_0(a)_\sigma$, and we claim that $\beta \in dcl(E_0, a)$.

Indeed, let $K = E_0(a)_\sigma$ and $L = K(\alpha)_\sigma$. By (6.1), K has no proper finite σ-stable extension. Hence the fields $K(\sigma^i(\alpha))$, $i \in \mathbb{Z}$, are linearly disjoint over K, and therefore $G = \mathcal{G}al(L/K)$ is isomorphic to a product of copies of $\mathbb{Z}/3\mathbb{Z}$ indexed by the integers.

Let τ be a generator of $\mathcal{G}al(K(\alpha)/K)$; then $C_G(\sigma)$ is the subgroup of $\mathcal{G}al(L/K)$ generated by the element $(\sigma^i\tau\sigma^{-i})_{i\in\mathbb{Z}}$ of G. One verifies that $C_G(\sigma)$ leaves β fixed, which shows that $\beta \in dcl(E_0, a)$. Hence, $p = tp(\beta/E_0)$ is internal to q.

Assume now by way of contradiction that p is qf-internal to q. Then there are a field $E = acl_\sigma(E)$ containing E_0 and independent from a, and realisations $a_1, \ldots, a_n$ of q such that $\beta \in E(a_1, \ldots, a_n)_\sigma$. Enlarging E, we may assume that $a_1, \ldots, a_n$ are equi-algebraic with a over E. By Lemma 6.1, this implies that $a_1, \ldots, a_n \in E(a)_\sigma$. Since $\beta \notin E(a)_\sigma$, we obtain the desired contradiction.

7. Groups of finite rank

In [14] and [20] the new concepts of S_1-theory and of geometric structures were introduced, in an attempt to isolate the stability theoretic properties of pseudo-finite fields and related structures. Both these concepts require the definability of the S_1-rank for formulas (which in our case equals the SU-rank), i.e., given a formula $\varphi(x, y)$, the set of elements b such that $S_1(\varphi(x, b)) \geq n$ is definable. While this property does not hold in our case (see 6.3), a similar one for deg_σ holds. Let us write $deg_\sigma(\varphi(x)) \leq n$ to express that if A is a set containing the parameters for φ and a is any realisation of φ, then $deg_\sigma(a/A) \leq n$. Since this property is purely field-theoretic, it follows that if $\varphi(x, y)$ is a formula and n a positive integer, then the set of elements b such that $deg_\sigma(\varphi(x, b)) \geq n$ is definable. This allow one to retrieve the main results of [19] and [20], with minor modifications in the proofs.

In this section we will give an overview of these results; for the proofs we refer to the original papers, but indicate the changes that have to be made.

Throughout this section, K denotes a model of $ACFA$. Let us start with an easy observation:

(7.1) Lemma. (1) *Let G be a group definable in K and of finite SU-rank. Then the elements of G of maximal SU-rank are exactly those of maximal deg_σ.*

(2) *Assume that H is an algebraic group defined over K, and that G is a definable subgroup of H of finite SU-rank. Consider the σ-ideal J of difference equations vanishing on all elements of G, and let G' be the set of elements g of H such that $I(g/K)$ contains J. Then G' is a quantifier-free definable subgroup of H, and $[G' : G]$ is finite. We call G' the* σ-closure of G in H.

Proof. (1) We work over $E = acl_\sigma(E)$, over which everything is defined. Choose $a, b \in G$ independent, such that $SU(a)$ and $deg_\sigma(b)$ are maximal, and consider the element $ab \in G$. Using the fact that a and ab are equi-definable over b, we deduce that $SU(ab/b) = SU(a/b) = SU(a)$ and $deg_\sigma(ab/b) = deg_\sigma(a)$; by the maximality of $SU(a)$, this implies that ab and b are independent, and therefore $deg_\sigma(ab/b) = deg_\sigma(ab)$.

Similarly, from the equi-definability of b and ab over a, and the maximality of $deg_\sigma(b)$, we deduce that $deg_\sigma(ab/a) = deg_\sigma(b/a) = deg_\sigma(b)$, $SU(ab/a) = SU(b)$, and ab and a are independent. Putting everything together, we obtain $SU(a) = SU(ab) = SU(b)$ and $deg_\sigma(a) = deg_\sigma(ab) = deg_\sigma(b)$.

(2) Since the group operation is defined without quantifiers, G' is a subgroup of H, which has the same deg_σ as G; by (1), G and G' have therefore the same SU-rank, which implies that G is of finite index in G'.

(7.2) Proposition (3.1 in [19]). *Let G be a group of finite SU-rank, definable in K. There are a definable subset A over which G is defined, an algebraic group H definable over A, and points a, b, c of G, and a', b', c' of H such that*:

(i) *$ab = c$ (in G) and $a'b' = c'$ (in H).*
(ii) *$acl_\sigma(A, a) = acl_\sigma(A, a')$, $acl_\sigma(A, b) = acl_\sigma(A, b')$ and $acl_\sigma(A, c) = acl_\sigma(A, c')$.*
(iii) *a and b are generic points of G and are independent over A; a' and b' are generic points of H and are independent over A.*

Proof. The proof follows exactly the one given in [19], Proposition 3.1, replacing everywhere *dim* by deg_σ, and *acl* by acl_σ. Expand a to $a^\frown\sigma(a)\cdots^\frown\sigma^\ell(a)$ for large enough ℓ and similarly for b, to work in the pure field language.

(7.3) Lemma (5.21 in [19]). *Let $\varphi(x, y)$, $\psi(x, z)$ be formulas such that for all a, b in K, $deg_\sigma(\varphi(x, a)) \leq n$ and $deg_\sigma(\psi(x, b)) \leq n$. Let $\delta(y, z)$ be the formula such that for all a, b in K, $\models \delta(a, b)$ if and only if $deg_\sigma(\varphi(x, a) \wedge \psi(x, b)) \geq n$. Then $\delta(y, z)$ is stable.*

Proof. Same as in [19].

(7.4) Lemma (6.1 in [19]). *Let G be a group of finite rank definable in K, and let H be an ∞-definable subgroup of G. Then H is the intersection of definable subgroups of G.*

Proof. Same as in [19].

(7.5) Proposition (6.2 in [19]). *Let G be a group of finite SU-rank definable in K. Then there are an algebraic group H defined over K, a definable (in the difference field K) subgroup G_0 of finite index in G, and a definable homomorphism $f : G_0 \to H(K)$ with finite central kernel.*

Proof. Same as in [19]. Note that here we cannot deduce that $f(G_0)$ has finite index in $H(K)$. As in [19], one can then enlarge H and get a homomorphism defined on G.

Corollary. *Let G be a group of finite SU-rank definable on in K. Then G satisfies the descending chain condition on centralisers.*

Proof. By the theorem, there is a definable group homomorphism $f : G \to H(K)$, with $\ker(f)$ finite. Since algebraic groups have the d.c.c on centralisers, so does $G/\ker(f)$. The result follows from the finiteness of $\ker(f)$.

(7.6) Theorem (7.2 in [14]). *Let G be a group of finite SU-rank definable in K. Let X_i be definable subsets of G, $i \in I$. Then there exists a definable subgroup H of $\langle X_i \mid i \in I\rangle$ such that X_i/H is finite for every $i \in I$. The definability of H in particular implies that $H \subseteq X_{i_1}^{\pm 1} \cdot \cdots \cdot X_{i_m}^{\pm 1}$ for some $i_1, \ldots, i_m \in I$.*

Proof. We work over an algebraically closed set over which everything is defined. Choose $a \in \langle X_i \mid i \in I\rangle$ of maximal deg_σ, say n, and let Q be the set of realisations of $tp(a)$ (in some saturated model). Let S be defined by

$$S = \{h \in G \mid \text{there is } a' \in Q, \text{ independent from } h \text{ and such that } ha' \in Q\},$$

and let $H = S \cdot S$. Then S is an ∞-definable subset of G: S is the intersection of the sets $S_\varphi = \{g \in G \mid deg_\sigma(\varphi(x) \wedge \varphi(gx)) \geq n\}$ over all $\varphi \in tp(a)$. Clearly $S \subseteq \langle X_i \mid i \in I\rangle$. Using the maximality of $deg_\sigma(a)$, one obtains that $deg_\sigma(S) \leq deg_\sigma(a)$; on the other hand, choosing $a, a' \in Q$ independent, $a'a^{-1} \in S$ and $deg_\sigma a'a^{-1} = deg_\sigma(a)$. Hence $deg_\sigma(S) = deg_\sigma(a)$.

By the independence theorem, if h_1, h_2 are independent elements of S, then h_1^{-1}, $h_1h_2 \in S$.

Let $h_1, h_2, h_3 \in S$; we want to show that their product is in H. For that, choose $h_4 \in S$ independent from h_1, h_2, h_3, and write $h_1h_2h_3$ as $(h_1h_4^{-1})(h_4h_2h_3)$. Then $h_1h_4^{-1} \in S$, $h_4h_2 \in S$ and is independent from h_3; hence $h_4h_2h_3 \in S$, which proves our assertion.

We then have $deg_\sigma(H) = deg_\sigma(S) = deg_\sigma(a)$. By (7.4), H is the intersection of definable subgroups H_m of G. By compactness, there is an n such that H_m is contained in $\langle X_i \mid i \in I\rangle$ and has the same deg_σ as H. Then $SU(H_m) = SU(H) = SU(a) \geq SU(X_i)$. This implies that X_i/H_m is finite.

(7.7) Proposition (7.5 in [14]). *Assume that moreover the collection X_i, $i \in I$, is invariant under conjugation. Then H can be chosen normal in G.*

Proof. We will first show that we can find such an H with $N(H)$ of finite index in G. We apply (7.6) to the group $G_1 = G \rtimes G$, where the second copy of G acts on the first by conjugation, and to the family $\{(X_i \times 1) \mid i \in I\} \cup \{1 \times G\}$. We obtain a subgroup T of $\langle X_i \times 1, 1 \times G \mid i \in I\rangle$ such that $(X_i \times 1)/T$ and $(1 \times G)/T$ are finite for each $i \in I$. Setting $H = T \cap (G \times 1)$, the normaliser of H in G contains $(1 \times G) \cap T$, whence it has finite index in G.

Consider the family $\mathcal{H}$ of definable subgroups H' of $\langle X_i \mid i \in I\rangle$ such that $N(H')$ is of finite index in G and X_i/H' is finite for every $i \in I$. Let $H_1 \in \mathcal{H}$ be of maximal SU-rank, and let H_2 be a conjugate of H_1. We will show that $H_1 \cap H_2$ is of finite index in H_1 and H_2.

The group $N = N(H_1) \cap N(H_2)$ normalises H_1 and H_2. Hence, the group H_3 generated by $(N \cap H_1)$ and $(N \cap H_2)$ equals their product, and is therefore definable, and normalised by N. Hence $H_3 \in \mathcal{H}$, and

$$SU(H_1) \geq SU(H_3) \geq SU(H_1 \cap N) = SU(H_1),$$

which shows that $N \cap H_1$ has finite index in H_3. Similarly, $N \cap H_2$ has finite index in H_3, which implies that $N \cap H_1 \cap H_2$ has finite index in H_3. From this we obtain that $SU(H_1 \cap H_2) = SU(H_1) = SU(H_2)$, which shows that $H_1 \cap H_2$ has finite index in H_1 and H_2.

Thus any two conjugates of H_1 are commensurable. Hence the intersection H of the finitely many conjugates of H_1 has finite index in H_1 and therefore is in $\mathcal{H}$.

(7.8) Corollary (7.6 in [14]). *Let G be a definable group of finite rank. Then $[G,G]$ is definable.*

Proof. By (7.6) and (7.7) applied to the set X of commutators, there is a definable normal subgroup H of G, contained in $[G,G]$ and such that XH/H is finite. Hence, G/H has finitely many commutators, which implies that the commutator subgroup of G/H is finite (see 14.5.11 in [28]) and therefore that $[G,G]$ is definable.

(7.9) Corollary (7.8 in [14]). *Let G be a definable group of finite rank. Then G is simple if and only if it is definably simple and non-abelian.*

Proof. Assume that G is definably simple; then it has no center and no definable subgroup of finite index. Therefore all conjugacy classes of non-identity elements are infinite. Let N be a normal subgroup of G, and let $a \in N$, $a \neq 1$, and consider the infinite set X_a consisting of all conjugates of a. By (7.6), there is a definable normal subgroup H of N such that X_a/H is finite, and this implies that H is infinite.

(7.10) Proposition (3.3 in [20]). *Let G be a connected algebraic group, and G_1 a definable subgroup of G of finite SU-rank. Assume that G_1 is Zariski dense in G, and that its σ-degree equals* $\dim(G)$. *Then there are an algebraic group H, a quantifier-free definable subgroup H_1 of H, and an isogeny $f : H \to G$ such that $f(H_1)$ is a subgroup of finite index of G_1.*

Proof. Let G_0 be the σ-closure of G_1 in G (see (7.1)(2)); then $SU(G_0) = SU(G_1)$ by (7.1), and G_1 has finite index in G_0, since G_0 is quantifier-free definable, and therefore $a \in G_0$ is equivalent to $(a, \sigma(a), \cdots, , \sigma^m(a)) \in V_m$ for some m and algebraic subgroup V_m of $G \times \sigma(G) \times \cdots \times \sigma^m(G)$. Going to the connected component of V_m, we may assume that V_m is a variety for every m, and that G_0 has no quantifier-free definable subgroup of finite index. The natural projections $V_m \to G$ are epimorphisms, with finite central kernels. Making the appropriate changes, we will assume that $(x, \sigma(x)) \in V_1$ determines G_0. It will be enough to find an isogeny $f : H \to V_1$ and a quantifier-free definable subgroup H_1 of H such that $f(H_1)$ is a subgroup of finite index of $V_1 \cap (G_1 \times \sigma(G))$.

If $G_0 = G_1$ there is nothing to prove; we will therefore assume that G_1 is a proper subgroup of G_0. Let b be a generic point of G_1; since G_0 contains G_1 properly, by (2.8) there is a finite Galois extension $E(b, \hat{b})_\sigma$ of $E(b)_\sigma$ such that if $(c, \hat{c})$ realises $qftp(b, \hat{b}/E)$ then $c \in G_1$. Take such a c independent from b over E, let $a = cb^{-1}$, and let a_1 be such that $acl_\sigma(Ea) \cap E(b, \hat{b}, c, \hat{c})_\sigma = E(a, a_1)_\sigma$. Then $E(a, a_1)_\sigma$ is a finite Galois extension of $E(a)_\sigma$. Define b_1, c_1 as follows:

$$E(b, b_1)_\sigma = E(b, \hat{b})_\sigma \cap E(a, a_1, c, \hat{c})_\sigma, \quad E(c, c_1)_\sigma = E(c, \hat{c})_\sigma \cap E(a, a_1, b, b_1)_\sigma.$$

Then $E(a, a_1, b, b_1)_\sigma = E(a, a_1, c, c_1)_\sigma = E(b, b_1, c, c_1)_\sigma$. Summarising the situation, we have:

(i) (a, a_1), (b, b_1), (c, c_1) are pairwise independent over E, and each of them is in the difference field generated by the other two.
(ii) $E(a, a_1)_\sigma$ is finite Galois over $E(a)_\sigma$, $E(b, b_1)_\sigma$ is finite Galois over $E(b)_\sigma$, and $E(c, c_1)_\sigma$ is finite Galois over $E(c)_\sigma$.

We now work in the pure field language. From this data, one reasons as in [20]. From (ii), deduce a generic action of the set P of realisations of $qftp(a, a_1)$ on the set Q of realisations of $qftp(b, b_1)$. Thus the elements of P are in a natural way

germs of functions on Q, and there is a generically associative group law on P. Find an algebraic group H whose generic α is equi-definable with (a, a_1). Then compare the group law on H to the one on G_1, and conclude that the inclusion map $k(a) \subseteq k(a, a_1)$ yields a group homomorphism from a quantifier-free definable subgroup H_1 of H to G_1, with finite kernel. Observe that by construction $deg_\sigma(H_1) = deg_\sigma(G_1) = dim(G) = dim(H)$.

(7.11) Internal quotients. Assume that G is a definable group of finite SU-rank, with generic non-orthogonal to a type q of SU-rank 1. Under certain additional assumptions the techniques used in [11], Lemma 3.3.6, gereralise easily to our context, and show that G has a definable normal subgroup N such that G/N is (qf)-internal to q. Below, we will give two such results, and some details of the proof.

Theorem. *Let G be a definable group of SU-rank m, and assume that for some generic $a \in G$ (i.e., of maximal SU-rank), $tp(a)$ is not orthogonal to $\sigma(x) = x$. Then there is a definable normal subgroup N of G such that G/N is internal to the fixed field F. If G is a definable subgroup of an algebraic group, then N can be chosen so that G/N is qf-internal to F.*

Proof. By (7.5), we may assume that G is a subgroup of some algebraic group H. Since G is of finite index in its quantifier-free closure, we may assume that G is quantifier-free definable, and contains no quantifier-free definable subgroup of finite index. Indeed if G_0 is a normal subgroup of finite index of G, and if N_0 is a normal subgroup of G_0 such that G_0/N_0 is qf-internal to F, then $N = \bigcap_{g \in G_0 \backslash G} N_0^g$ is definable. Since G_0/N embeds in $\prod_{g \in G_0 \backslash G} G/N_0^g$, it is qf-internal to F. Now use the fact that G is the union of finitely many cosets of G_0 to conclude. The non-orthogonality of a generic of G to F is preserved.

Let a be a generic of G; then $tp(a) \not\perp (\sigma(x) = x)$. Choose c independent of a and such that some $b \in F$ is algebraic over a, c, but not over just c. By (3.7), we may assume that $b \in cl_\sigma(a, c)$. Let $d = Cb(b, c/a)$. Since c and a are independent, a is relatively algebraically closed in $cl_\sigma(a, b, c) = cl_\sigma(a, c)$, and therefore $d \in cl_\sigma(b_1, c_1, \ldots, b_r, c_r)$ for some independent realisations of $tp(b, c/a)$. By (5.2), this implies that $tp(d)$ is qf-internal to F. Let h be the rational difference function such that $h(a) = d$ (we know that $d \in cl_\sigma(a)$), and let P_0 be the set of realisations of $qftp(d)$, P the set of realisations of $qftp(a)$. From our assumptions on G, we know that P is precisely the set of generics of G.

Define a relation $\sim$ on P by putting $a \sim b$ if for some generic $(g_1, g_2) \in G^2$ we have $h(g_1 a g_2) = h(g_1 b g_2)$. Since we are dealing with quantifier-free types, and the group, its group law and the function h are quantifier-free definable, we can replace "for some generic" by "for all generic" in the definition of $\sim$.

Claim 1. $\sim$ is a quantifier-free definable equivalence relation on P.

Proof. As above, the relevant ingredients are quantifier-free definable. Hence the definability results (2.16) apply to give the result.

Claim 2. Assume that $a \sim b$, and let $g \in G$ be independent from a and b. Then $ga \sim gb$ and $ag \sim bg$.

Proof. Let $(g_1, g_2) \in G^2$ be generic over g, a, b. Then $(g_1 g, g_2)$ is generic, independent from a, b, and therefore $h(g_1 g a g_2) = h(g_1 g b g_2)$. We also have that (g_1, g_2) is

independent from $ga, gb \in P$. This shows that $ga \sim gb$; the proof that $ag \sim bg$ is similar.

Define $N = \{n \in G \mid \text{ for all generic } g,\ g \sim gn\}$.

Claim 3. N is a definable normal subgroup of G.

Proof. The fact that N is closed under multiplication and inverse is clear: if g is generic independent from n_1, n_2, then gn_1 and gn_1n_2 are in P, and $\sim$ is an equivalence relation on P. It is definable, since $n \in N$ if and only if $g \sim gn$ for some generic g, which is a definable relation.

Let $g \in G$, and let $g_1 \in G$ be generic, independent from n, g. Then g_1g^{-1} is independent from n, which implies that $g_1g^{-1} \sim g_1g^{-1}n$. Also, g is independent from g_1g^{-1} and from $g_1g^{-1}n$, and therefore $g_1 \sim g_1g^{-1}ng$, which shows that N is normal.

Claim 4. G/N is qf-internal to F.

Proof. Every element of G is the product of two elements of P. Also, for every $a \in P$, the $\sim$-equivalence class of a, $[a]_\sim$, is contained in the coset $a + N$: if $a \sim b$, choose $g \in G$ generic and independent from a, b; then $ga \sim gb$, and $g \sim gba^{-1}$, i.e. $ba^{-1} \in N$. It therefore suffices to show that, for each $a \in P$, the equivalence class $[a]_\sim$ is qf-internal to F. By this we mean that there is an element c, whose type is qf-internal to F, and such that $[a]_\sim$ is quantifier-free definable over c.

Fix $a \in P$, and let B be a set of $m + 1$ independent realisations (g_i, g_i') $(0 \leq i \leq m = SU(G))$ of the generic of G^2. We will show that $[a]_\sim$ is quantifier-free definable over $cl_\sigma(B, d_0, \ldots, d_m)$, where $d_i = h(g_iag_i')$. Indeed, for $b \in P$, there is an i such that (g_i, g_i') is independent from (a, b), and we have

$$h(g_ibg_i') = d_i \iff b \in [a]_\sim.$$

By compactness there is a quantifier-free formula $\psi(x, y, y', z)$ that is satisfied by (a, g_i, g_i', d_i) for all i, and such that for any $b \in P$,

$$\models \psi(b, g_i, g_i', d_i) \to (h(g_ibg_i') = d_i \leftrightarrow a \sim b).$$

Then $x \in [a]_\sim$ is equivalent to the formula $\bigwedge_{i=0}^{m}(\psi(x, g_i, g_i', d_i) \to h(g_ixg_i') = d_i)$. This finishes the proof.

Note. A more general result is proved in Chapter 3 of [16].

(7.12) Theorem (char. 0)**.** *Let G be a definable group of finite SU-rank m. Assume that G has a generic type p which is superficially stable, and let q be a type of SU-rank 1, not orthogonal to p. Then G has a definable normal subgroup N such that G/N is internal to q.*

Proof. Observe that our hypothesis implies that all generics of G are superficially stable, and therefore definable. Also, q must be stable and stably embedded.

The proof is basically the same as the proof of (7.11), replacing the quantifier-free types by types, and using the fact that "for some generic" is equivalent to "for all generic".

(7.13) Concluding remarks. Some of the results in this section can be obtained in a greater generality. The proofs actually do not use SU-rank or S_1-rank per se, but rather certain properties of deg_σ. We will state these properties explicitly below ((1)– (4)); they can be viewed as a proposed revised definition of "finite S_1-dimension". We will show that certain other basic properties ((5), (6)) follow from them axiomatically, and hence also the results (7.4), (7.6), (7.7), (7.8) and (7.9).

Suppose that we have a function d from definable sets to $\mathbb{N} \cup \{\infty\}$ satisfying the following properties:

(1) $d(\varphi(x,a)) = 0$ if and only if $\varphi(x,a)$ has finitely many realisations.

(2) d is definable, i.e., given n and a formula $\varphi(x,y)$, the set $\{a \mid d(\varphi(x,a)) \geq n\}$ is definable.

(3) Additivity. Let $\varphi(x,y)$ and $\psi(y)$ be formulas (maybe with additional parameters). Assume that $d(\psi(y)) = m$, and for all a satisfying ψ, $d(\varphi(x,a)) = n$. Then $d(\varphi(x,y) \wedge \psi(y)) = m + n$.

(4) The S_1-property. Assume that $d(\varphi(x)) = n$. For any formula $\psi(x,y)$, there is no infinite sequence $(a_i)_{i \in I}$ such that for all $i \neq j \in I$

$$d(\varphi(x) \wedge \psi(x,a_i)) = n > d(\varphi(x) \wedge \psi(x,a_i) \wedge \psi(x,a_j)).$$

Remark. The difference from the usual definition of S_1-rank lies in condition (4): we cannot compute the d-rank from (4), we only know its lower bound. Thus our rank can "jump". This is why we must add the additivity condition, so that d is preserved under definable bijections. Note also that if $d(\varphi)$ is finite then $S_1(\varphi) \leq d(\varphi)$.

Clearly deg_σ satisfies all these conditions.

One can then define d for types (we call it d-rank): $d(p) = \inf\{d(\varphi) \mid \varphi \in p\}$. Note that it is additive for types of finite d-rank: $d(ab/A) = d(a/Ab) + d(b/A)$. Also, if p is defined on A and $A \subseteq B$, then p has an extension q to B such that $d(p) = d(q)$. We call such a type a non-forking extension of p, and if a realises q we say that a and B are independent over A. Additivity of the rank implies symmetry of forking. From the S_1-property, we obtain, as in 5.21 of [19],

(5) Existence of stable formulas. Assume that for some integer n, for every b and every c we have $d(\varphi(x,b)) \leq n$ and $d(\psi(x,c)) \leq n$. Then the formula $\delta(y,z)$ that defines the set of tuples (b,c) such that $d(\varphi(x,b) \wedge \psi(x,c)) = n$ is stable.

From this, one deduces, exactly as in 5.22 of [19],

(6) The independence theorem for types of finite d-rank (we work in T^{eq}). Let $A = acl(A)$, and let a, b, c_1, c_2 be such that: (i) a, b, c_1 and c_2 are independent over A; (ii) c_1, c_2 realise the same type over A; (iii) a, b, c_1 have finite d-rank over A.

Then there is c independent from (a,b) over A, and realising $tp(c_1/acl(A,a)) \cup tp(c_2/acl(A,b))$.

Appendix. Study of stable embeddability

We present some of the results on stable embeddability and stability which we needed in our proofs. See also [4] for a discussion of stable embeddability.

Setting. Let $T = T^{eq}$ be a complete theory in a countable language, and M an uncountable saturated model of T. Let p be a (partial) m-type over the empty set and let P be the set of realisations of p in M, together with the structure induced from M, i.e., the 0-definable subsets of P^n are the traces on P^n of 0-definable subsets of M^{mn}.

Recall first that P is *stably embedded* if for every n, if $D \subseteq M^{mn}$ is definable, then $D \cap P^m$ is definable with parameters from P.

Lemma 1. *The following conditions are equivalent:*

(1) *For every a, $tp(a/dcl(a) \cap dcl(P)) \vdash tp(a/P)$.*
(2) *For every a, there is a small (e.g., of size $\leq 2^{\aleph_0}$) $P_0 \subseteq P$ such that $tp(a/P_0) \vdash tp(a/P)$.*
(3) *For every a, there is a small $P_1 \subseteq P$ such that $tp(a/acl(P_1)) \vdash tp(a/P)$.*
(4) *For every a, $tp(a/P)$ is definable over some (countable) $P_0 \subseteq P$.*
(5) *P is stably embedded.*
(6) *Every automorphism of P lifts to an automorphism of M.*

Proof. (1) $\rightarrow$ (2) and (2) $\rightarrow$ (3) are clear.

(3) $\rightarrow$ (4). Let $\varphi(x, y)$ be a formula, and let P_1 be as given by (3). We will first show that $\varphi(x, y)$ has a definition over $acl(P_1)$. If not, then for every formula $\psi(y)$ with parameters from $acl(P_1)$, there are b_1, b_2 in P satisfying $\psi(y)$ and $\varphi(a, b_1) \leftrightarrow \neg\varphi(a, b_2)$. Thus, by compactness, there are b_1 and b_2 in P realising the same type over $acl(P_1)$, and satisfying $\varphi(a, b_1) \leftrightarrow \neg\varphi(a, b_2)$, which is a contradiction.

Thus $\varphi(x, y)$ has a definition $\psi(y)$ with parameters in $acl(P_1)$. Let $D \subseteq P$ be the set of tuples of P satisfying $\psi(y)$. Since D is definable over the algebraic closure of P_1, it has finitely many distinct conjugates over P_1. For each such conjugate D', pick an element in $D \triangle D'$, and enlarge P_1 to a set P_2 by adding these elements. Then D is definable over P_2.

Since the language is countable, $tp(a/P)$ is defined over some countable set P_0.

(4) $\rightarrow$ (5). Let $D \subseteq P^n$ be defined by the formula $\varphi(x, b)$, and let $d_\varphi(y)$ be a definition for $\varphi(x, y)$ in $tp(b/P)$. Then, for $a \in P^n$, $a \in D \leftrightarrow \models d_\varphi(a)$.

(5) $\rightarrow$ (4). Let $\varphi(x, y)$ be a formula. Then the set $\{a \in P^n \mid \models \varphi(a, b)\}$ is of the form $\{a \in P^n \mid \models \psi(a)\}$ for some formula $\psi(y)$ with parameters in P. This formula ψ gives us the definition for $\varphi(x, y)$. Since there are countably many formulas, the set P_0 can be chosen countable.

(2) $\rightarrow$ (6). Let $\kappa = |M|$, let A and B be subsets of M of size $< \kappa$, and assume that $\tau : P \cup A \rightarrow P \cup B$ is an elementary map with $\tau(P) = P$. If $a \in M$, then there is a $b \in M$ realising $\tau(tp(a/P, A))$.

Indeed, by (1) applied to finite subsets of Aa, there is a subset P_0 of P, of size smaller than κ, such that $tp(A, a/P_0) \vdash tp(A, a/P)$. By saturation of M, there is $b \in M$ realising $\tau(tp(a/P_0, A))$; then $tp(b/\tau(P_0), B) \vdash tp(b/B, P)$ and therefore $tp(b/P, B) = \tau(tp(a/P, A))$.

Now a standard back and forth argument gives the result.

(6) $\rightarrow$ (5). Assume that P is not stably embedded, and let $S \subseteq P^n$ be definable in M, but not definable over P. Let G be the group of automorphisms of M sending P to itself. Our assumption and the saturation of M imply that if $P_0 \subseteq P$ has size less than $\kappa = |M|$, then there is $g \in G$ fixing P_0 and such that $g(S) \neq S$. Let S_α, $\alpha < \kappa$, be an enumeration of the orbit of S under G, and fix an enumeration of P. We will construct an automorphism τ of P such that $\tau(S) \neq S_\alpha$, for every α. Then τ does not lift to an automorphism of M. Assume that an elementary onto map $\tau_\alpha : P_\alpha \rightarrow P'_\alpha$ has already been constructed, where P_α and P'_α are subsets of P of size less than κ, and assume that $\tau_\alpha(S \cap P_\alpha) \not\subset S_\beta$ for every $\beta < \alpha$. We will do the forth direction, the reverse direction being similar. There are two steps in each direction.

Step 1. If there is no element $g \in G$ extending τ_α such that $g(S) = S_\alpha$, let $a = a' = \emptyset$ and go to step 2. Assume therefore that there is such an element g.

Our assumption on P and S implies that there is an element $a \in S$ such that both $tp(a/P_\alpha) \cup \{x \in S\}$ and $tp(a/P_\alpha) \cup \{x \notin S\}$ are consistent; this implies that $\tau_\alpha(tp(a/P_\alpha)) \cup \{x \notin S_\alpha\}$ is also consistent. Choose $a' \notin S_\alpha$ realising $\tau_\alpha(tp(a/P_\alpha))$.

Step 2. take the first element b of the enumeration of P not in $dom(\tau_\alpha)$ and choose $b' \in P$ such that (a', b') realises $\tau_\alpha(tp(a, b/P_\alpha))$.

Then define $P_{\alpha+1} = P_\alpha \cup \{a, b\}$, $P'_{\alpha+1} = P'_\alpha \cup \{a', b'\}$, and $\tau_{\alpha+1}$ as the extension of τ_α sending (a, b) to (a', b').

(5) $\rightarrow$ (1). Let $\varphi(x, y)$ be a formula. By stable embeddability, the set $\{b \in P^n \mid \varphi(a, b)\}$ is definable by a formula $\psi(y, c)$ for some $c \in P^\ell$. By compactness, there is a 0-definable set D containing P^n and such that $\{b \in D \mid \varphi(a, b)\} = \{b \in D \mid \psi(b, c)\}$. Consider the equivalence relation $E(z_1, z_2)$ on P^ℓ defined by $\forall y \in D\,(\psi(y, z_1) \iff \psi(y, z_2))$. Then the class of c modulo E belongs to $dcl(a) \cap dcl(c)$.

Thus $tp(a/P)$ is definable over $P_0 = dcl(a) \cap dcl(P)$. Let $b_1, b_2 \in P^n$, with the same type over P_0. By assumption, each formula $\varphi(x, y)$ has a definition with parameters in P_0. This implies that b_1 and b_2 have the same type over $P_0 \cup a$, and proves (1).

Lemma 2. *Let T be a complete theory in a countable language, M an uncountable saturated model of T, and p a (partial) m-type, P its set of realisations in M. The following conditions are equivalent:*

1. *For every countable $A \subseteq M$, and formula $\varphi(x, y)$, the set $\{tp_\varphi(c/A) \mid c \in P\}$ is countable.*
2. *For every A, the set of m-types over A realised in P has size at most $|A|^{\aleph_0}$.*
3. *For every A, the type over A of an element of P is definable.*
4. *For every formula $\varphi(x, y)$, $\varphi(x, y) \wedge p(x)$ is stable, i.e., there is no infinite sequence (a_n, b_n), $n \in \mathbb{N}$, such that $a_n \in P$ for every n and*

$$M \models \varphi(a_n, b_m) \qquad \iff \qquad n < m.$$

Proof. The proof is standard. See e.g [33], (I.2.10 and II.2.2), or [27], section 15d.

Definition-Remark. Under the equivalent conditions of Lemma 2, we will say that P (or p) is *stable and stably embedded*, or *fully stable*. When the type p is complete, this is what Shelah calls a stable type.

By (2), if P is fully stable then so is P^n for $n \in \mathbb{N}$, and so is also any subset of P. One also shows that a fully stable type is stably embedded; see e.g. Lemma 15.13 in [27].

If P is a 0-definable set, it can be shown that P is fully stable if and only if P is stably embedded and the induced structure on P is stable.

Lemma 3. *If $tp(b/Aa)$ and $tp(a/A)$ are fully stable, then so is $tp(ab/A)$.*

Proof. Let $B \supseteq A$. (We may assume that A and the language are countable.) We want to count the number of extensions of $tp(ab/A)$ to B, and show it is at most $|B|^{\aleph_0}$. Equivalently, if we enumerate B, we must show that $tp(B/A)$ has at most $|B|^{\aleph_0}$ extensions to Aab. Now $tp(B/A)$ has at most $|B|^{\aleph_0}$ extensions to Aa (by full stability of $tp(a/A)$), and $tp(B/Aa)$ has at most $|B|^{\aleph_0}$ extensions to Aab (by full stability of $tp(b/Aa)$). The conclusion follows.

Lemma 4. *Let p be a minimal type, fully stable, and P the set of realisations of p. Assume that if $c_1, c_2 \in P^m$ are independent and $c_0 \in acl(c_1, c_2) \cap P$, then there are elements d_i with $acl(d_i) = acl(c_i)$ for $i = 0, 1, 2$, and with $d_0 \in dcl(d_1, d_2)$.*

Then p is modular.

Proof. Assume that p is not modular. By [12], §5, non-modularity implies:

There is a minimal subset $C(b)$ of P^2, defined over parameters b with $SU(b) = 3$, such that if U equals $C(b)$ up to a finite set, then U cannot be defined over a set of SU-rank < 3.

The proof of Proposition 3.1 of [13] goes through, and we obtain the following statement:

Let b_1, b_2 be independent realisations of $tp(b)$, and let $I(b_1, b_2) =_{\text{def}} C(b_1) \cap C(b_2)$. There are $e_1, e_2 \in I(b_1, b_2)$, independent, and such that some automorphism τ leaves b_1, b_2 fixed but exchanges e_1 and e_2.

By stable embeddability, we may assume that $b_i = acl(c_i)$ for $i = 1, 2$, where the $c_i \in P^m$ are independent. Find $d_i \in dcl(acl(c_1), acl(c_2))$ such that $acl(d_i) = acl(e_i)$ for $i = 1, 2$; then $\tau(acl(e_i)) = acl(e_i)$, which is a contradiction.

References

1. J. Ax, The elementary theory of finite fields, Annals of Math. 88 (1968), 239 – 271. MR **37:**5187
2. S. Buechler, Locally modular theories of finite rank, Ann. Pure Appl. Logic 30 (1986), 83 – 94. MR **87j:**03035
3. Z. Chatzidakis, L. van den Dries and A. Macintyre, Definable sets over finite fields, J. Reine Angew. Math. 427 (1992), 107 – 135. MR **94c:**03049
4. G. Cherlin, E. Hrushovski, Large finite structures with few 4-types, preprint 1998 (earlier version: Smoothly approximable structures, 1994).
5. R.M. Cohn, Difference algebra, Tracts in Mathematics 17, Interscience, New York, 1965. MR **34:**5812
6. L. van den Dries, Dimension of definable sets, algebraic boundedness and henselian fields, Ann. Pure Appl. Logic 45 (1989), 189 – 209. MR **91k:**03082
7. L. van den Dries, K. Schmidt, Bounds in the theory of polynomials rings over fields. A non-standard approach. Invent. Math. 76 (1984), 77 – 91. MR **85i:**12016
8. J.-L. Duret, Les corps pseudo-algébriquement clos non séparablement clos ont la propriété d'indépendance, in: Model theory of algebra and arithmetic, Proc. Karpacz 1979, Springer Lecture Notes in Math. 834 (1980), 136 – 161. MR **83i:**12024
9. D.M. Evans, E. Hrushovski, On the automorphism groups of finite covers, Ann. Pure Appl. Logic 62 (1993), 83 – 112. MR **94e:**03035
10. R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics 52, Springer-Verlag, 1977. MR **57:**3116
11. E. Hrushovski, Contributions to stable model theory, Ph. D. Thesis, Berkeley 1985.
12. E. Hrushovski, Unimodular minimal structures, J. London Math. Soc. (2) 46 (1992), 385 – 396. MR **94b:**03062
13. E. Hrushovski, Finitely axiomatisable $\aleph_1$-categorical theories, J. Symbolic Logic 59 (1994), 838 – 844. MR **95k:**03061
14. E. Hrushovski, Pseudo-finite fields and related structures, preprint (1991).
15. E. Hrushovski, Finite structures with few types, in: Finite and Infinite Combinatorics in Sets and Logic, NATO ASI Series C 411, Kluwer, Dordrecht, 1993, 175 – 187. MR **95h:**03084
16. E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, preprint (1995).
17. E. Hrushovski, The first-order theory of the Frobenius, preprint (1996).
18. E. Hrushovski, A. Pillay, Weakly normal groups, in: Logic Colloquium 85, North-Holland 1987, 233 – 244. MR **88e:**03051
19. E. Hrushovski, A. Pillay, Groups definable in local fields and pseudo-finite fields, Israel J. Math. 85 (1994), 203 – 262. MR **95f:**12015

20. E. Hrushovski, A. Pillay, Definable subgroups of algebraic groups over finite fields, J. Reine Angew. Math. 462 (1995), 69 – 91. MR **97f:**20059
21. B. Kim, Forking in simple unstable theories, J. London Math. Soc. (2) 57 (1998), 257–267. CMP 99:01
22. B. Kim, A. Pillay, Simple theories, in: Proc. AILA-KGS conference (Florence, 1995), A. Lachlan, D. Mundici editors, Ann. Pure Appl. Logic 88 (1997), 149 – 164. MR **99b:**03049
23. A. Macintyre, Generic automorphisms of fields, in: Proc. AILA-KGS conference (Florence, 1995), A. Lachlan, D. Mundici editors, Ann. Pure Appl. Logic 88 (1997), 165 – 180. CMP 98:07
24. A. Macintyre, Nonstandard Frobenius, in preparation.
25. A. Pillay, An introduction to stability theory, Oxford Logic Guide 8, Clarendon Press, Oxford, 1983. MR **85i:**03104
26. A. Pillay, Geometric Stability, Clarendon Press, Oxford 1996. MR **98a:**03049
27. B. Poizat, Cours de Théorie des Modèles, Nur Al-Mantiq Wal-Ma'rifah, Paris 1985. MR **87f:**03084
28. D.J.S. Robinson, A course in the theory of groups, 2nd ed., Graduate Texts in Mathematics 80, Springer-Verlag, New York 1996. MR **96f:**20001
29. M. Rosen, Abelian varieties over $\mathbb{C}$, in: Arithmetic Geometry, G. Cornell and J. H. Silverman ed., Springer-Verlag 1986. MR **89b:**14029
30. J. -P. Serre, Local fields, Springer-Verlag 1979. MR **82e:**12016
31. J. -P. Serre, Topics in Galois Theory, Research Notes in Mathematics, Vol. 1, Jones and Bartlett Pub., Boston 1992. MR **94d:**12006
32. I.R. Shafarevich, Basic Algebraic Geometry 1 and 2, 2nd ed., Springer-Verlag 1994. MR **95m:**14001; MR **95m:**14002
33. S. Shelah, Classification theory and the number of nonisomorphic models, Studies in Logic 92, North-Holland 1978. MR **81a:**03030
34. S. Shelah, Simple unstable theories, Ann. Math. Logic 19 (1980), 177 – 203. MR **82g:**03055
35. J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics 106, Springer-Verlag, 1986. MR **87g:**11070

Université Paris 7, Case 7012, 2, place Jussieu, 75251 Paris Cedex 05, France
E-mail address: zoe@logique.jussieu.fr

Institute of Mathematics, The Hebrew University, Givat Ram, Jerusalem 91904, Israel
E-mail address: ehud@sunset.ma.huji.ac.il