On subgroups of semi-abelian varieties defined by difference equations

Zoé Chatzidakis[*] – CNRS (UMR 8553) - Ecole Normale Supérieure
Ehud Hrushovski[†] – The Hebrew University of Jerusalem

Introduction

Consider the algebraic dynamics on an algebraic torus $T = \mathbb{G}_m^n$ given by a matrix $M \in \mathrm{GL}_n(\mathbb{Z})$. Assume no root of unity is an eigenvalue of M. We show that any finite, equivariant map from another algebraic dynamics into (T, M) arises from a group isogeny $\mathbb{G}_m^n \to \mathbb{G}_m^n$ (see 4.2 and more generally 4.8). In other words, the automorphism $x \mapsto x^M$ of $K(x) = K(x_1, \ldots, x_n)$ does not extend to any finite field extension, except those contained in $K(x_1^{1/m}, \ldots, x_n^{1/m})$ for some $m \geq 1$. A similar statement is shown for abelian varieties, and in fact for semi-abelian varieties.

More generally, we study irreducible difference equations of the form $n\sigma(x) = Mx$, with $M \in \mathrm{End}(A)$, $n \in \mathbb{N}$; for instance the equation $\sigma(x)^3 = x^2$ on $\mathbb{G}_m$. We obtain a similar statement for the function field of such equations.

Model-theoretically, this completes the description ([2], [3], [9]) of the induced structure on ACFA-definable subgroups of semi-abelian varieties. Such subgroups (up to finite index) are defined by difference equations of the form $n\sigma(x) = Mx$, with $M \in \mathrm{End}(A)$. The induced structure is stable, except when the equation involves the points $A(F)$ of the fixed field or a twisted fixed field $\sigma^r(x) = x^{p^m}$. Whereas the quantifier-free induced structure was understood previously – it corresponds to invariant subvarieties – the full induced structure involves also finite covers, and stability was known only in characteristic zero.

We proceed to describe the result in terms of difference algebra. By a difference field, we mean a field K with a distinguished automorphism σ. The theory ACFA of existentially closed difference fields was extensively studied in [2] and [3]. In these papers, a characterisation of modular types was given, and it was shown that, in characteristic 0, all modular types are stable and stably embedded. In characteristic $p > 0$, we however exhibited examples of modular subgroups of the additive group $\mathbb{G}_a$ which are not stable. The main result of this

[*]partially supported by PITN-2009-238381 and by ANR-06-BLAN-0183, ANR-09-BLAN-0047, ANR-13-BS01-0006.

[†]The research leading to these results has received funding from the European Research Council under the European Unions Seventh Framework Programme (FP7/2007- 2013)/ERC Grant Agreement No. 291111, as well as the Israel Science Foundation 1048/07.

paper, Theorem 4.4, is that all modular definable subgroups of a semi-abelian variety are stable and stably embedded. This implies that definable subsets of modular subgroups are Boolean combinations of cosets of definable subgroups.

Let F be the transformal function field of a definable subgroup B of a semi-abelian variety A. Stability of B is equivalent to the existence of few difference field extensions L of F, that are finite as field extensions. In fact we obtain a complete description of such extensions. In characteristic zero, the main geometric tool is the ramification divisor of L over appropriate varieties (A or powers of A.) With controlled exceptions, the ramification divisor of a potential extension L is invariant under the dynamics, leading to reduction of the dimension of B. For abelian varieties, the ramification divisor still carries enough information. If B lives on a torus $\mathbb{G}_m^n$ however, too many finite extensions have the same ramification divisor, and a finer invariant is needed. We consider a certain invariant subspace of the Berkovich space, consisting of valuations with center contained in the ramification divisor. We define an invariant, in the value group, associated with a wildly ramified extension L of F. Within this subspace, there may be no fixed points but there are always recurrent points of the dynamics. Such points lead again to an eigenvector of the dynamics (acting on the value group now) and to a reduction of the dimension of B. Such invariants of wildly ramified extensions are new to our knowledge, and may be of interest elsewhere. The use of recurrent points (rather than periodic points) also seems noteworthy.

The paper is organised as follows. In section 1 we set up the notation and recall some results on existentially closed difference fields from [4], [2] and [3]. Section 2 recalls the tools used to study definable subgroups of algebraic groups, and describes the criterion for modularity of a definable subgroup of a simple abelian variety or of $\mathbb{G}_m$.

Section 3 contains a host of technical lemmas, which will be used in the proofs of Propositions 4.1 and 4.3. Section 4 contains the proof of Theorem 4.4, and derives some consequences.

We would like to thank the referee for many useful comments.

1 Notation, preliminary definitions and results

1.1. Notation and conventions. We work in the language $\mathcal{L} = \{+, -, \cdot, 0, 1, \sigma\}$ of difference fields. **Unless explicitly stated otherwise, all difference fields are inversive**, i.e., the endomorphism σ is surjective. **Throughout the paper, we work inside a large saturated model** (Ω, σ) **of ACFA**. If K is a difference subfield of Ω, and $A \subset \Omega$, $K(A)_\sigma$ denotes the difference field generated by A over K, and $\mathrm{acl}_\sigma(A)$ the smallest algebraically closed field containing A and closed under σ and σ^{-1}. If A is a subfield of Ω, then A^{alg} denotes the (field-theoretic) algebraic closure of A and A^s its separable closure. We let Frob denote the identity of Ω if the characteristic of Ω is 0, and the automorphism $x \mapsto x^p$ if the characteristic is $p > 0$. If $char(\Omega) = p > 0$ and q is a power of p, we also denote by Frob_q the automorphism $x \mapsto x^q$ of Ω. If L is a finite algebraic extension of K, then $[L : K]$ denotes its degree, $[L : K]_s = [L \cap K^s : K]$ its *separable degree*, and $[L : K]_i = [L : K]/[L : K]_s$ its *inseparable degree*.

If n is a positive integer, we denote by $\mathcal{L}[n]$ the language $\{+, -, \cdot, 0, 1, \sigma^n\}$, viewed as a sublanguage of $\mathcal{L}$, and by $\Omega[n]$ the difference field (Ω, σ^n). Then $\Omega[n]$ is a model of ACFA ([2], Corollary (1.12)(1)), and is saturated. If E is a difference subfield of Ω, and a a tuple of Ω, then $tp(a/E)[n]$ denotes the type of a over E in the structure $\Omega[n]$.

Recall that the ring of difference polynomials over K in $\bar{X} = (X_1, \dots, X_n)$, denoted $K[\bar{X}]_\sigma$, is simply the polynomial ring $K[\sigma^j(X_i) \mid i = 1, \dots, n,\ j \in \mathbb{N}]$. The *$\sigma$-topology on K^n* is the topology with basic closed sets the *σ-closed sets* $\{\bar{a} \in K^n \mid f(\bar{a}) = 0\}$, where $f(\bar{X})$ is a tuple of difference polynomials over K. This topology is Noetherian (see [4], 3.V). When working inside $\Omega[n]$ we will speak of the σ^n-topology.

If V is an algebraic set, and τ an automorphism, we will denote by $\tau(V)$ or by V^τ the algebraic set whose defining equations are obtained by applying τ to the coefficients of the equations defining V. In particular, $V^\tau(\Omega) = \tau(V(\Omega))$.

1.2. Basic notions and results on ACFA. Model-theoretic algebraic closure coincides with acl_σ ((1.7) in [2]), and (model-theoretic) independence of algebraically closed sets A and B over a common algebraically closed subset C corresponds to linear independence of the fields A and B over C, and any completion of ACFA is supersimple (see (1.9) in [2] and use [14]). We also know that any completion of ACFA eliminates imaginaries ((1.12) in [2]).

Let E be a difference subfield of Ω, and a a tuple of elements of Ω. Then the quantifier-free type of a over E, denoted $qftp(a/E)$, is the set of quantifier-free $\mathcal{L}$-formulas with parameters in E which are satisfied by a. It therefore describes the isomorphism type of the difference field $E(a)_\sigma$ over E. Similarly, $qftp(a/E)[n]$ denotes the set of quantifier-free $\mathcal{L}[n]$-formulas with parameters in E which are satisfied by a.

The SU-rank is defined as usual. Let us mention that $\mathrm{SU}(a/A)$ is finite if and only if $\mathrm{tr.deg}(\mathrm{acl}_\sigma(A, a)/\mathrm{acl}_\sigma(A))$ is finite, if and only if all elements of the tuple a satisfy some non-trivial difference equation over $\mathrm{acl}_\sigma(A)$. We denote by $\mathrm{SU}(a/A)[n]$ the SU-rank in the reduct $\Omega[n]$ (thus it equals $\mathrm{SU}(a/acl_{\sigma^n}(A))[n]$).

Finally, assume that A is a difference subfield of $\Omega[n]$ for some n, and let $a \in \Omega$. We define the eventual SU-rank of a over A, denoted $\mathrm{evSU}(a/A)$, as $lim_{m\to\infty}\mathrm{SU}(a/A)[m!]$ (see (1.13) in [3]). It is well-defined, and only depends on $qftp(a/A)$. Note that if $A = \mathrm{acl}_\sigma(A)$ and $\sigma(a) \in A(a)^{alg}$, then $\mathrm{SU}(a/A)[m] \leq \mathrm{SU}(a/A)[mn]$ for all $m, n \neq 0$. This implies that there is some $m > 0$ such that for all $n > 0$, $\mathrm{evSU}(a/A) = \mathrm{SU}(a/A)[mn]$.

1.3. Completions of quantifier-free types. Let E be a difference subfield of Ω, and a a tuple of elements of Ω. Then $tp(a/E) = tp(b/E)$ if and only if there is an isomorphism $\mathrm{acl}_\sigma(E, a) \to \mathrm{acl}_\sigma(E, b)$, which leaves E fixed and sends a to b ((1.15) in [2]). In particular, if $E = \mathrm{acl}_\sigma(E)$, then ACFA $\cup qftp(E)$ is complete, and the completions of ACFA are obtained by describing the isomorphism type of the algebraic closure of the prime field.

A *finite σ-stable extension* of a difference subfield K of Ω is a finite (algebraic) extension L of K such that $\sigma(L) = L$. If L is a finite separable σ-stable extension of K, then so is its Galois closure M over K. Furthermore, whether or not $\sigma(M) = M$ does not depend on the extension of σ to M, but is completely determined by the isomorphism type of K: if M is finite separable over K, let $\alpha \in M$ be such that $M = K(\alpha)$, and let $P(T) \in K[T]$ be the minimal monic polynomial of α over K, and $P^\sigma(T)$ the polynomial obtained by applying σ to the coefficients of P. Then $\sigma(M) = M$ is equivalent to the following statement: the field $K[T]/(P(T))$ contains a root of $P^\sigma(T)$. Observe also that σ extends uniquely to the perfect hull of K.

Theorem 1.4. *(Babbitt, [4] Theorem 7.VIII). Let E be a difference subfield of Ω, and a, b tuples which have the same quantifier-free type over E. The following conditions are equivalent:*

(1) *$tp(a/E) = tp(b/E)$.*

(2) *Given any finite σ-stable Galois extension L of $E(a)_\sigma$, there is an E-embedding $L \to \Omega$ which sends a to b.*

In particular, if $E(a)_\sigma$ has no non-trivial finite separable σ-stable extension, then $qftp(a/E)$ is complete.

Let L be a finite separable σ-stable Galois extension of $E(a)_\sigma$. Then σ induces an automorphism of $G = \mathcal{G}al(L/E(a)_\sigma)$ given by $\rho \mapsto \sigma^{-1}\rho\sigma$; hence, for some ℓ we will have $\sigma^{-\ell}\rho\sigma^{\ell} = \rho$ for all $\rho \in G$. Difference fields between $E(a)_\sigma$ and L correspond to subgroups H of G which are stable under the action of σ.

While it may happen that $E(a)_\sigma$ has some non-trivial finite separable σ-stable extension, and yet $qftp(a/E)$ be complete, this does not hold if one wants to consider all the reducts $\Omega[n]$. Namely ((2.9)(5) in [2]):

Lemma 1.5. *Let F be a difference subfield of Ω. The following conditions are equivalent:*

(1) *$ACFA \cup qftp(F)[n]$ is complete, for all $n > 0$.*

(2) *F has no finite separable σ-stable extension.*

1.6. Modularity. Let $S \subset \Omega^n$ be stable under any $\mathrm{acl}_\sigma(E)$-automorphism of Ω. We say that S is *modular* if whenever a is a tuple of elements of S and $B \subset \Omega$, then a and B are independent over $\mathrm{acl}_\sigma(E,a) \cap \mathrm{acl}_\sigma(E,B)$. A type over E is *modular* if the set of its realisations is modular.

This notion of modularity is also called *one-basedness*. Here we use the fact that our theory is supersimple and eliminates imaginaries. The main result of [3] (see (7.5)) shows that S is modular if and only if, for every $F = \mathrm{acl}_\sigma(F)$ containing E and $a \in S$, $tp(a/F)$ is orthogonal to all fixed fields, i.e., to all formulas of the form $\sigma^n(x) = \mathrm{Frob}^m(x)$ where $n \geq 1$, $m \in \mathbb{Z}$. It follows that $tp(a/E)$ is modular if and only $tp(a/E)[\ell]$ is modular for every $\ell \geq 1$, and that a modular type has finite SU-rank.

Theorem 1.7. ([3] (7.6)). *Let G be an algebraic group and B a definable modular subgroup of $G(\Omega)$ of finite SU-rank. If D is a quantifier-free definable subset of B, then D is a finite Boolean combination of translates of quantifier-free definable subgroups of B. If B is defined over E, then every quantifier-free definable subgroup of B is definable over* $\mathrm{acl}_\sigma(E)$.

1.8. Stability and stable embeddability. A subset S of Ω^m stable under E-automorphisms of Ω is *stably embedded* if whenever $D \subset \Omega^{nm}$ is definable, then $D \cap S^n$ is definable with parameters from S (see the Appendix of [2] for properties). A type is *stably embedded* if the set of its realisations is stably embedded.

Let $E = \mathrm{acl}_\sigma(E)$ and a a tuple of elements of Ω. If $tp(a/E)$ is stationary (i.e., has a unique non-forking extension to any set $F \supset E$), then $tp(a/E)$ is definable (this is standard, using compactness). Hence, if all extensions of $tp(a/E)$ to algebraically closed sets are stationary, then $tp(a/E)$ is *stable and stably embedded* (see Lemma 2 and its Definition-Remark in the Appendix of [2]). A definable set D is *stable and stably embedded* if all types realised in D are stable and stably embedded. Equivalently, if D with the structure induced by Ω is stable and stably embedded.

Using the characterisation of modular types and Lemmas 2, 3 of the Appendix of [2], one easily deduces:

Proposition 1.9. *Let*

$$1 \longrightarrow B_1 \longrightarrow B_2 \longrightarrow B_3 \longrightarrow 1$$

be an exact sequence of groups definable in a model of ACFA. Then B_2 is modular [resp. stable and stably embedded] if and only if B_1 and B_3 are modular [resp. stable and stably embedded].

2 Definable subgroups of algebraic groups

In this chapter we introduce tools used to study definable groups, and give a brief sketch of the description of modular subgroups of abelian varieties. The proof in [9] was given in characteristic 0, and we indicate what changes need to be made in positive characteristic. Please see chapter 4 in [9] for more details.

2.1. Setting and notations. In what follows we will use p to denote $char(\Omega)$ if it is positive, and 1 if it is 0. Thus Frob will denote the map $x \mapsto x^p$ (see 1.1). Let G be a connected algebraic group, H a definable subgroup of $G(\Omega)$, everything defined over $E = \mathrm{acl}_\sigma(E) \subset \Omega$.

For $m \in \mathbb{N}$, define $G_{(m)} = G \times \sigma(G) \times \cdots \times \sigma^m(G)$ and $p_m : G \to G_{(m)}$ by $g \mapsto (g, \sigma(g), \dots, \sigma^m(g))$. Let $H_{(m)}$ be the Zariski closure of $p_m(H)$, and let $\tilde{H}_{(m)} = \{g \in G \mid p_m(g) \in H_{(m)}\}$. The intersection $\tilde{H}$ of the $\tilde{H}_{(m)}$ equals the σ-closure of H (in $G(\Omega)$), and equals some $\tilde{H}_{(m)}$, because every descending sequence of σ-closed sets stabilises. Then $[\tilde{H} : H] < \infty$: one easily shows that the generics of H (in the model-theoretic sense) are those $h \in H$ such that $p_m(h)$ is a generic of the algebraic group $H_{(m)}$ for every $m > 0$. Hence a generic of H is a generic of $\tilde{H}$.

Because the σ-topology is Noetherian, every σ-closed set S can be expressed as an irredundant union of σ-closed irreducible sets, which are called the irreducible components of S. Then the irreducible component of $\tilde{H}$ containing the identity of G is a subgroup of $\tilde{H}$; it is called the *connected component of* $\tilde{H}$ and is denoted by $\tilde{H}^0$. Then $[\tilde{H} : \tilde{H}^0] < \infty$. We let $H^0 = H \cap \tilde{H}^0$, and call it the *connected component* of H. Then also $[H : H^0] < \infty$.

2.2. c-minimal subgroups. Let B be a definable subgroup of some algebraic group. Then B is *c-minimal* iff every definable subgroup of B is either finite or of finite index in B. Note that c-minimality is preserved by definable homomorphisms with finite kernel; hence if B is c-minimal, then there is a definable homomorphism $g : B^0 \to G(\Omega)$, where $\mathrm{Ker}\,(g)$ is finite central, and G is an algebraic group which is simple and is the Zariski closure of $g(B^0)$. Indeed, one simply looks at the simple quotients of the Zariski closure of B^0, and at the images of B^0 in these quotients: one of these images must be isogenous to B^0.
Note also that if $SU(B) = 1$ then B is c-minimal. If B is modular, then the converse is true as well: c-minimality of B implies $SU(B) = 1$: this is because the stabilizer of any type realised in B has the same SU-rank as the type.

2.3. Definable endomorphisms and subgroups of abelian varieties. Let A be an abelian variety, defined over $E = \mathrm{acl}_\sigma(E)$. By standard results on abelian varieties, A is isogenous to a finite direct sum of simple abelian varieties defined over E, say to $\bigoplus_{i=1}^n A_i$. Renumbering, we may assume that for $i < j \le r$, for all $\ell \in \mathbb{Z}$, A_i is not isogenous to $\sigma^\ell(A_j)$, and that for any $j > r$ there are $i \le r$ and $\ell \in \mathbb{Z}$ such that A_i and $\sigma^\ell(A_j)$ are isogenous. For $i \le r$ let $m(i)$ be the number of indices j such that for some ℓ, A_i and $\sigma^\ell(A_j)$ are isogenous.

Let us denote by $\mathrm{End}(A)$ the ring of (algebraic) endomorphisms of A, by $\mathrm{Hom}(A, A_i)$ the group of algebraic homomorphisms $A \to A_i$, and by $\mathrm{End}_\sigma(A)$ the ring of definable endomorphisms of $A(\Omega)$, $\mathrm{Hom}_\sigma(A, A_i)$ the group of definable homomorphisms $A \to A_i$. Hrushovski gives a good description of $\mathbb{Q}\otimes\mathrm{End}_\sigma(A)$ in [9], and we refer to this paper for the results quoted below. First, note that $\mathbb{Q}\otimes\mathrm{End}_\sigma(A) \simeq \prod_{i=1}^r M_{m(i)}(\mathbb{Q}\otimes\mathrm{End}_\sigma(A_i))$, so that it suffices to describe the rings $\mathrm{End}_\sigma(A_i)$. We will therefore restrict our attention to simple abelian varieties.

Recall that two definable subgroups B and C of a group are *commensurable* if $B \cap C$ has finite index in both B and C. Hrushovski shows that a definable subgroup of $A(\Omega)$ is commensurable to a definable subgroup $\bigcap_{j=1}^n \mathrm{Ker}\,(F_j)$, where $F_j \in \mathrm{Hom}_\sigma(A, A_j)$.

The study in [9] is made for difference fields of characteristic 0. However, the proofs generalise to positive characteristic without any trouble. Note that in positive characteristic, the Frobenius map may define an endomorphism of the variety.

Theorem 2.4. *Let A be a simple abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, let B be an infinite definable subgroup of $A(\Omega)$.*

(1) *If there is no integer $n > 0$ such that A and $\sigma^n(A)$ are isogenous, then $\mathrm{End}_\sigma(A) = \mathrm{End}(A)$, and $B = A(\Omega)$.*

(2) *Assume that there is an integer $n > 0$ such that A and $\sigma^n(A)$ are isogenous. We fix such an n, smallest possible, and choose an isogeny $h : A \to \sigma^n(A)$ of minimal degree m. If $\sigma^n(A) = A$, then we choose h to be the identity. Let $h' : \sigma^n(A) \to A$ be such that $h'h = [m]$ (multiplication by m in A; such an h' exists by standard results on abelian varieties); then $hh' = [m]$. Define $\tau = \sigma^{-1}h$ and $\tau' = h'\sigma$.*

Then $\mathbb{Q} \otimes \mathrm{End}_\sigma(A) \simeq \mathbb{Q} \otimes \mathrm{End}(A)[\tau, \tau']$, and B is commensurable to $\mathrm{Ker}\,(f)$ for some $f \in \mathrm{End}(A)[\tau, \tau']$. Furthermore, $\mathbb{Q} \otimes \mathrm{End}_\sigma(A)$ is an Ore domain and if $C \subseteq B$ is *definable, then C is commensurable to some* $\mathrm{Ker}\,(g)$ *with g dividing f (i.e, $hg = f$ for some $h \in \mathbb{Q} \otimes \mathrm{End}_\sigma(A)$). It follows that B is c-minimal if and only if f is left-irreducible.*

Proof. In characteristic 0, this is given by Proposition 4.1.1 of [9]. The proof goes through verbatim.

Theorem 2.5. *Let A be a simple abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, and let $B = \mathrm{Ker}\,(f)$ be a* **proper** *definable subgroup of $A(\Omega)$, which is c-minimal and connected. Assume that B is not modular.*

(1) *Then A is isomorphic to an abelian variety A' defined over $\mathrm{Fix}(\rho)$, where $\rho = \mathrm{Frob}^m\sigma^n$ for some $m \in \mathbb{Z}$, $n > 0$.*

(2) *Assume that A is defined over $\mathrm{Fix}(\theta)$, where $\theta = \mathrm{Frob}^s\sigma^t$ for some $s \in \mathbb{Z}$, $t > 0$. If A is not isomorphic to any variety defined over the algebraic closure of the prime field, then f divides $\theta^\ell - 1$ for some ℓ. If A is isomorphic to a variety A' defined over the algebraic closure of the prime field, by an isomorphism F, then for some $m \in \mathbb{Z}$, $n > 0$ and $\rho = \mathrm{Frob}^m\sigma^n$, $F(B) \subset A'(\mathrm{Fix}(\rho))$.*

Proof. First observe that the c-minimality of B implies that if q is any non-algebraic type realised in B, then the realisations of q generate a subgroup of finite index in B.

(1) In characteristic 0, this result is Proposition 4.1.2 of [9]. The proof generalises easily to the positive characteristic case, using the results of [3]. Here is a sketch of the main steps: if B is not modular, then by c-minimality, the type of a generic of B is non-orthogonal to one of the fixed fields, say $k = \mathrm{Fix}(\rho_0)$, where $\rho_0 = \sigma^n\mathrm{Frob}^m$, $n \geq 1$, and $(n, m) = 1$ if $m \neq 0$. Thus, modulo a finite kernel, it is qf-internal to k, i.e., there is a finite subgroup C of B, and a definable map g_0 from some definable set $S \subset k^\ell$ onto B/C (in fact g_0 is given piecewise by difference rational functions).

Elimination of imaginaries in ACFA tells us that B/C is then definably isomorphic (via some g_1) with a group H_0 living in some cartesian power of k. On the other hand, every subset of a cartesian power of k which is definable in Ω, is already definable in the difference field k, using maybe extra parameters from k (see (7.1)(5) in [3]). Note that k has SU-rank 1 ((7.1)(1) in [3]). An argument similar to the one given in [13] or in [15] then gives us a definable (in k) map $g_2 : H_0' \to H_1(k)$, where $\mathrm{Ker}\,(g_2)$ is finite, H_0' is a subgroup of finite index of H_0, and H_1 is an algebraic group defined over k. Then $H_0' \supseteq [N]H_0$ for some N, and so $g_1([N]B/C) \subseteq H_0'$. Hence, replacing g_1 by $g_1 \circ [N]$, we may assume that $H_0' = H_0$. (Recall that the N-torsion of all these groups is finite).

Composing these maps, we therefore obtain a definable group homomorphism $h : B \to H_1(k)$, with $\mathrm{Ker}\,(h)$ finite. We may assume that the Zariski closure of $h(B)$ is all of H_1.

Since B is *c*-minimal, so is $h(B)$, and this implies that if $\pi : H_1 \to A'$ is a projection of H_1 onto a simple quotient A' of H_1, then $\pi h(B)$ is Zariski dense in A', and therefore $\mathrm{Ker}\,(\pi) \cap h(B)$ is finite. Replacing ρ_0 by some power $\rho = \rho_0^r$ (and k by its algebraic extension of degree r), we may assume that A' and π are defined over k. Hence we get a definable map $B \to A'(k)$, with finite kernel. This implies that $\mathrm{Hom}(A, \sigma^\ell(A')) \neq (0)$ for some ℓ, and applying some power of σ to A', we may assume that $\mathrm{Hom}(A, A') \neq 0$. Thus A' is a simple abelian variety, defined over k, and isogenous to A. This implies that A is isomorphic to an abelian variety A'' defined over some finite extension of k. Replacing ρ by its appropriate power, we have shown (1).

(2) By the proof of (1), we have a definable map $\varphi : B \to A'(k)$, with finite kernel D, where $\rho = \mathrm{Frob}^m\sigma^n$ and $k = \mathrm{Fix}(\rho)$. Moreover A' is isogenous to A. If $mt = sn$, then we may assume that $\theta = \rho$ and $A' = A$. If $mt \neq sn$, then A is isomorphic to a variety A'' defined over $\mathrm{Fix}(\theta)^{alg} \cap \mathrm{Fix}(\rho)^{alg} = \mathbb{F}_p^{alg}$, and we are in the second case. The result will follow from the following claim:

Claim. Let A be an abelian variety defined over $k = \mathrm{Fix}(\rho)$, let B be a definable subgroup of $A(\Omega)$ and $\varphi : B \to A(k)$ a definable homomorphism with finite kernel D. Then $B \subseteq A(\mathrm{Fix}(\rho^\ell))$ for some ℓ.

Proof. The graph of φ is a definable subgroup of A^2; as there are only countably many of those (see 4.1.10 in [9]), it must be defined over k^{alg}. Hence, φ is definable over k^{alg}, and, replacing ρ by an appropriate power we may assume that φ is defined over $\mathrm{Fix}(\rho)$. Let $k_0 \prec k$ be such that everything is defined over k_0. Since D is finite, if $b \in B$ then $b \in \mathrm{acl}_\sigma(k_0(\varphi(b))) = k_0(\varphi(b))_\sigma^{alg}$. By compactness, there is ℓ such that $[k_0(\varphi(b))_\sigma(b) : k_0(\varphi(b))_\sigma] \leq \ell$ for every $b \in B$ and this implies that $b \in \mathrm{Fix}(\rho^{\ell!})$.

2.6. Definable subgroups of tori. Similar results hold for tori, i.e., algebraic groups isomorphic to $\mathbb{G}_m^n$ for some n. Recall that algebraic subgroups of $\mathbb{G}_m^n$ are defined by equations of the form $\prod_{i=1}^n x_i^{m_i} = 1$ for some integers $m_1, \ldots, m_n$. These subgroups are connected if the m_i's have no common divisor. Using the description of definable subgroups of algebraic groups given in 2.1, one shows easily that a definable subgroup B of $\mathbb{G}_m$ is commensurable to $\mathrm{Ker}\,(f(\sigma))$ for some $f(T) \in \mathbb{Z}[T]$, and that B is c-minimal if and only if f is irreducible. Here, if $f = \sum m_i T^i$ and $a \in \mathbb{G}_m$, we define $f(\sigma)(a) = \prod \sigma^i(a)^{m_i}$.

The proof of Theorem 2.5 generalises to this setting to show that modular subgroups of $\mathbb{G}_m$ are those which are commensurable to some $\mathrm{Ker}\,(f(\sigma))$, where $f(T)$ is relatively prime (in $\mathbb{Q}[T]$) to all elements of the form $T^n - p^m$, with $n > 0$ and $m \in \mathbb{Z}$. Indeed, let $B = \mathrm{Ker}\,(f(\sigma))$, where $f \in \mathbb{Z}[T]$ and assume that B is not modular. Then for some $k = \mathrm{Fix}(\sigma^n\mathrm{Frob}^m)$, there is a definable homomorphism $h : B \to \mathbb{G}_m(k)$ with infinite image. Hence $\mathrm{Ker}\,(h)$ is commensurable with some $\mathrm{Ker}\,(g(\sigma))$ with $g(T) \in \mathbb{Z}[T]$, so that g divides f in $\mathbb{Q}[T]$. The homomorphism h then induces a homorphism $\pi : B/B \cap \mathrm{Ker}\,(g(\sigma)) \to \mathbb{G}_m(k)$ with finite kernel. The proof of the claim in 2.5 generalises to show that $B/B \cap \mathrm{Ker}\,(g(\sigma)) \subseteq \mathbb{G}_m(\mathrm{Fix}(\sigma^{n\ell}\mathrm{Frob}^{m\ell}))$ for some ℓ, so that B is commensurable to $\mathrm{Ker}\,((\sigma^{n\ell} - p^{m\ell})g(\sigma))$.

Lemma 2.7. *Let $f \in \mathbb{Z}[T]$, $f(T) = \sum_{i=0}^n b_i T^i$, with $b_0 b_n \neq 0$, and assume that the b_i's are relatively prime. Let a be a generic of* $\mathrm{Ker}\,(f(\sigma))$ *over some field $E = \mathrm{acl}_\sigma(E)$*[1]*, let $m \geq n$, and let $g \in \mathbb{Z}[T]$ be such that $g(\sigma)(a) = 1$.*

(1) *Then g belongs to the ideal generated by f in $\mathbb{Z}[T]$.*

[1] I.e., a satisfies $\prod_{i=0}^n \sigma^i(a^{b_i}) = 1$, and $\mathrm{tr.deg}(E(a)_\sigma/E) = n$.

(2) *Write* $g = \sum_{i=0}^{m} c_i T^i$*. Then* b_n *divides* c_m*.*

(3) *Let* $r > 1$*, and let* $h(T) \in \mathbb{Q}[T]$ *be monic and of least degree such that, writing* N *for the least positive integer such that* $Nh(T) \in \mathbb{Z}[T]$*, then* $Nh(\sigma^r)(a) = 1$*. Then every prime divisor of* N *divides* b_n*.*

(4) *(char*$(\Omega) = p > 0$*) Let* $m > 0$ *and consider* $\tau = \sigma \mathrm{Frob}^m$*. Then* a *is in* $\mathrm{Ker}\, s(\tau)$*, where* $s(T) = p^\ell \sum_{i=0}^{n} p^{-mi} b_i T^i$*, with* $\ell = -\inf_i\{v_p(b_i) - mi\}$*,* v_p *being the* p*-adic valuation on* $\mathbb{Q}$*. Moreover,* s *is irreducible.*

Proof. (1) The set of $h \in \mathbb{Q}[T]$ such that $h(\sigma)(a) = 1$ is an ideal. Since $\mathbb{Q}[T]$ is a Euclidian domain, there are $q, r \in \mathbb{Q}[T]$ such that $g = fq + r$ and $\deg(r) < \deg(f) = n$. If $r \neq 0$, then $g(\sigma)(a) = 1$ implies $r(\sigma)(a) = 1$, which implies $\mathrm{tr.deg}(E(a)_\sigma/E) \leq \deg(r) < \deg(f)$, a contradiction since we assume a to be a generic of $\mathrm{Ker}\,(f(\sigma))$. Hence $r = 0$. Let ℓ be a prime number, and define a valuation v on $\mathbb{Q}[T]$ extending the ℓ-adic valuation v_ℓ by setting $v(\sum a_i T^i) = \min_i\{v_\ell(a_i)\}$. Our assumption on f implies that $v_\ell(f) = 0$, and our assumption on g that $v(g) \geq 0$. It follows that $v(q) \geq 0$. This being true for any prime ℓ implies that $q \in \mathbb{Z}[T]$.

(2) Follows from (1).

(3) We now work in $\mathbb{Q}[T]$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(T)$ in $\mathbb{Q}^{alg}$. Then the roots of $h(T)$ in $\mathbb{Q}^{alg}$ are among $\alpha_1^r, \ldots, \alpha_n^r$. Let ℓ be a prime number not dividing b_n. This means that all α_i's are integral algebraic over $\mathbb{Z}_\ell$; hence so are all α_i^r, and this implies that the coefficients of h are in $\mathbb{Z}_\ell$, in other words, that ℓ does not divide N.

(4) A simple calculation shows that $s(T) \in \mathbb{Z}[T]$ and has relatively prime coefficients, and that $a \in \mathrm{Ker}\, s(\tau)$. The roots of $s(T)$ are $p^m\alpha_1, \ldots, p^m\alpha_n$, from which one deduces the irreducibility of $s(T)$.

3 Technical lemmas

In this chapter we collect some technical lemmas which will be used in the proof of the main results.

3.1. Valuations - basic results and notation. We refer to the book of Engler and Prestel [7] for all notions and results. First a definition: if E is a subring of the field K, then we say that a valuation v on K is an *E-valuation* if v is trivial on E. Given a valuation v on a field K, we denote by $\mathcal{O}_v$ or $\mathcal{O}_K$ its valuation ring, by $\mathcal{M}_v$ or $\mathcal{M}_K$ its maximal ideal, by k_K its residue field $\mathcal{O}_K/\mathcal{M}_K$, and by $\Gamma(K)$ its value group. If $a \in \mathcal{O}_v$, then we denote by $\bar{a}$ its residue, i.e., the image of a in $\mathcal{O}_v/\mathcal{M}_v$. The number p will denote the *residual characteristic* of v (i.e., the characteristic of k_K) if it is positive, and 1 if it is 0. Let L be a finite algebraic extension of K, and w an extension of v to L, $\Gamma(L)$ and k_L the corresponding value group and residue field. We define $e(w/v) = e(L/K) = [\Gamma(L) : \Gamma(K)]$ (the *reduced ramification index* of w in L), $r(w/v) = r(L/K) = e(L/K)[k_L : k_K]_i$ (the *ramification index*) and $f(w/v) = f(L/K) = [k_L : k_K]$ (the *residual degree* or *inertia degree* of w in L). We say that w *ramifies over* K if $r(L/K) > 1$, and that v *ramifies in* L if some extension of v to L ramifies over K.

If L is a finite normal extension of K, then all extensions of v to L are conjugate, so that the numbers $e(L/K)$, $r(L/K)$ and $f(L/K)$ will not depend on the choice of w. We denote by $g(L/K)$ the number of extensions of v to L. The numbers $e(L/K), f(L/K)$, $r(L/K)$ and $g(L/K)$ are multiplicative in towers.

The *defect* of a finite algebraic extension L of K is the number $d = d(L/K)$ such that $[L : K] = d \sum_w e(w/v)f(w/v)$ where w ranges over all extensions of v to L. This number is a power of p (Theorem 3.3.3 in [7]). We say that the valued field K is *defectless* if for every finite extension L of K, we have $d(L/K) = 1$. This property is preserved under finite algebraic extensions, see e.g. (18.1) in [6]. Note that a Henselian valued field which is defectless has no proper finite immediate extension. We will use the following results:

Fact 3.2. *Let (K, v) be a valued field. Then (K, v) is defectless in the following cases:*

(1) *k_K has characteristic* 0 *(Obvious since then $p = 1$).*

(2) $\Gamma(K) \simeq \mathbb{Z}$ *(Theorem 3.3.5 in [7]).*

(3) *K is finitely generated over a subfield E on which E is trivial, and* $\mathrm{tr.deg}(K/E) = \mathrm{tr.deg}(k_K/E) + \dim_{\mathbb{Q}}\Gamma(K) \otimes \mathbb{Q}$ *(Theorem 1.1. in [16]).*

Lemma 3.3. *Let (K, v) be a valued field, L a finite Galois extension of K, and M an algebraic extension of K. We assume that K is defectless.*

(1) *Assume that char$(K) = p > 0$, and that L is an Artin-Schreier extension of K, generated by a root α of $X^p - X - a = 0$. If $r(L/K) = p$, then for any $d \in K$, $v(d^p - d - a) < 0$.*

(2) *Assume that M is purely inseparable and finite over K. Then $r(L/K) = r(LM/M)$, where M is endowed with the unique extension of v to M.*

(3) *Assume that M is Galois over K, and that $\mathrm{e}(M/K) = 1$. Then $\mathrm{e}(L/K)$ divides $\mathrm{e}(LM/M)$, and equality holds if the residue fields k_L and k_M are linearly disjoint over k_K.*

(4) *Assume that M is finite Galois over K, and that $\mathrm{e}(M/K)$ and $\mathrm{e}(L/K)$ are relatively prime. Then $\mathrm{e}(L/K)$ divides $\mathrm{e}(LM/M)$, and equality holds if the residue fields k_L and k_M are linearly disjoint over k_K.*

(5) *Assume that M is Galois over K, that $k_M \subseteq k_K^s$, and that $m\Gamma(L), m\Gamma(M) \subseteq \Gamma(K)$ for some integer m relatively prime to p. Then also $m\Gamma(LM) \subseteq \Gamma(K)$. In particular, if $m\Gamma(M) = \Gamma(K)$, then $e(LM/M) = 1$.*

(6) *Assume that M is Galois over K, that $k_M \subseteq k_K^s$, and that $m\Gamma(M) = \Gamma(K)$ for some integer m prime to p and divisible by the exponent of the prime-to-p part of $\Gamma(L)/\Gamma(K)$. Then $e(LM/M)$ is a power of p.*

Proof. (1) Assume that there is $d \in K$ such that $v(d^p - d + a) > 0$. As $\alpha + d$ is a root of $X^p - X - (d^p - d + a)$, we may assume that $v(a) > 0$. Then $\bar{a} = 0$, the equation $X^p - X = 0$ has p distinct roots in the residue field, and therefore α lies in the henselization of K. This implies $e(L/K) = f(L/K) = 1$, which contradicts $r(L/K) = p$. Hence, for every $d \in K$, $v(d^p - d - a) \leq 0$.
Assume now that there is $d \in K$ such that $v(d^p - d + a) = 0$. As above, we may assume $v(a) = 0$. Our assumption then implies that the polynomial $X^p - X - \bar{a}$ has no root in k_K (since if $d \in \mathcal{O}_K$ lifts a root, then $v(d^p - d - a) > 0$) and therefore $\bar{\alpha}$ generates an extension of degree p of k_K. I.e., k_L is separable of degree p over k_K, $r(L/K) = 1$, and again we reach a contradiction. This gives us the desired result.

For (2) – (6), we replace K by its Henselisation, and therefore assume that v has a unique extension to K^{alg}, which we will also denote v. This does not affect the ramification indices, nor the possible linear disjointness of the residue fields, nor the defectlessness.

(2) References are to [7], chapter 5, and particularly sections 5.2 and 5.3. Reasoning by induction, we may assume that $[M : K] = p$. If L_v denotes the subfield of L fixed by $H = \{\rho \in \mathcal{G}al(L/K) \mid \forall a \in L\, v(\rho(a) - a) > v(a)\}$, then the residue field of L_v equals $k_L \cap k_K^s$, $e(L_v/K)$ is prime to p, and H is a p-group, $r(L/K) = e(L_v/K)[L : L_v]$. Since e is multiplicative in towers, and $[M : K] = p$, one clearly has that $e(L_vM/M) = e(L_v/K)$, and furthermore, the residue field of L_v is a separable extension of k_K, so does not contribute to $r(L/K)$. We may therefore assume that $K = L_v$, and the proof is by induction on $[L : K]$. As $\mathcal{G}al(L/K)$ is a p-group, L contains an Artin-Schreier extension, generated over K by a root α of $X^p - X = a$, for some $a \in K$. Because K and M are Henselian and defectless, we know that $K(\alpha)$ and $M(\alpha)$ are not immediate. Using the multiplicativity in towers of r, we will therefore assume that $L = K(\alpha)$. Then $[LM : M] = p$, so that either $e(LM/M) = p$ or $f(LM/M) = p$. It therefore suffices to show that if $e(LM/M) = 1$, then the residue field k_{LM} of LM is purely inseparable over k_K.

By (1), we know that for all $c \in K$, $v(c^p - c + a) < 0$. Assume by way of contradiction that $e(LM/M) = 1$, and that k_{LM}/k_K is separable. Then k_{LM} is an Artin-Schreier extension of k_M, i.e., is generated over k_M by a root of a polynomial $X^p - X - \bar{b}$, for some $b \in M$. Since LM is Henselian, LM contains therefore a root of $X^p - X - b$, and this root generates LM over M. By the theory of Artin-Schreier extensions[2], there is some positive integer $i < p$ and element $d \in M$ such that $a + d^p - d = bi$, and in particular, $v(d^p - d + a) = 0$. Since $[M : K] = p$, $d^p = c \in K$. But as L is separable over K, we have $K(\alpha) = K(\alpha^p)$ and α^p is a root of $X^p - X - a^p = 0$. Hence, $v(c^p - c + a^p) = 0$, and L is generated over K by a root of $X^p - X - (c^p - c + a^p)$. This contradicts (1).

(4) The residue field of LM contains the residue fields of L and of M. Hence $f(LM/K)$ divides $f(L/K)f(M/K)$ and equality holds if k_L and k_M are linearly disjoint over k_K. Each of $e(L/K)$, $e(M/K)$ divides $e(LM/K)$, and therefore so does their product since they are relatively prime. This proves the first assertion, and the second follows from $f(LM/K) = f(L/K)f(M/K)$ and

[2]See e.g. Theorem VIII.8.15 in S. Lang, *Algebra*, Addison-Wesley 1971.

the defectlessness and Henselianity of K (which gives $[LM : K] = e(LM/K)f(LM/K)$). This shows (4), from which also (3) follows.

(5) This is implicit in the description of the second exact sequence in [7] (section 5.3, see in particular p. 129, and 5.3.3, 5.3.8), but we will give the proof. Recall that we assume K Henselian, so that v has a unique extension to K^{alg}, also denoted by v, and that p denotes the characteristic of k_K if it is positive, and 1 otherwise. We let $G = \mathcal{G}al(K^s/K)$, $G^t = \{\rho \in G \mid v(\rho(x) - x) > 0 \,\forall x \in \mathcal{O}_{K^s}\}$ (the inertia group), $G^v = \{\rho \in G \mid v(\rho(x) - x) > v(x) \,\forall x \in (K^s)^\times\}$ (the ramification group), and K^t, K^v, the subfields of K^s fixed by G^t and G^v. Then G^t and G^v are normal subgroups of G, G_v is a pro-p-group, and G^t/G^v is abelian, all of its finite quotients having order relatively prime to p. The profinite group G^t/G^v has the following description: Let Ω denote the subgroup of $\mathbb{Q}/\mathbb{Z}$ consisting of elements of order prime to p. Then

$$G^t/G^v \simeq \mathrm{Hom}(\Gamma(K^s)/\Gamma(K), \Omega).$$

Note that our assumption on M implies that $M \subseteq K^v$, so that $LM \cap K^v = (L \cap K^v)M$, and $[LM : LM \cap K^v] = [L : L \cap K^v]$. If $L \not\subseteq K^v$, then $p > 1$, and our assumption that $e(L/K)$ is prime to p implies that

$$e(L/L \cap K^v) = 1, \quad [L : L \cap K^v] = [LK^v : K^v] = r(L/K)/e(L/K) = [k_L : k_K]_i = [k_{K^vL} : k_{K^v}].$$

Hence $[LM : LM \cap K^v] = [L : L \cap K^v] = [k_L : k_K]_i$, and $e(LM/LM \cap K^v) = 1$. From this we deduce that $\Gamma(LM) = \Gamma(LM \cap K^v)$.

Let $G(m)$ denote the subgroup of G^t/G^v corresponding to those $f \in \mathrm{Hom}(\Gamma(K^s)/\Gamma(K), \Omega)$ such that $\mathrm{Ker}\,(f)$ contains all elements of order m of $\Gamma(K^s)/\Gamma(K)$, and let $K(m)$ be the subfield of K^v fixed by $G(m)$. Note that $G^t/G(m)$ has exponent m, and is the largest quotient of G^t with this property. In other words, if N is a Galois extension of K, then $\Gamma(N)/\Gamma(K)$ has exponent dividing m if and only if $N \subseteq K(m)$. Our hypothesis on L and M then implies that $M \subseteq K(m)$ and $L \cap K^v \subseteq K(m)$. Hence, $LM \cap K^v \subseteq K(m)$, which implies that $m\Gamma(LM) \subseteq \Gamma(K)$. This shows the first assertion, and the second follows immediately: $\Gamma(LM) = \Gamma(M) = 1/m\Gamma(K)$, whence $e(LM/M) = 1$.

(6) Let $L_0 \subseteq L$ contain K and be such that $[L : L_0] = r(L/L_0)$ equals the highest power of p dividing $r(L/K)$. Then L_0 is Galois over K, and $\Gamma(L_0)/\Gamma(K)$ has exponent dividing m, i.e., $m\Gamma(L_0) \subseteq \Gamma(K)$. By (5), we get $e(L_0M/M) = 1$. As $[LM : L_0M]$ is a power of p, so is $e(LM/M) = e(LM/L_0M)$.

3.4. Generalised power series. Recall that if Γ is an ordered abelian group and E a field, then the field of generalised power series $E((t^\Gamma))$ is defined as the set of all formal sums $f = \sum_{\gamma\in\Gamma} a_\gamma t^\gamma$ with $a_\gamma \in E$ and such that the support of f, $\mathrm{Supp}(f) = \{\gamma \in \Gamma \mid a_\gamma \neq 0\}$, is well-ordered.

We define a valuation v on $E((t^\Gamma))$ by $v(f) = \inf \mathrm{Supp}(f)$. If $a \in E((t^\Gamma))$ and $\gamma \in \Gamma$, we denote by $a_{|\gamma}$ the unique element b of $E((t^\Gamma))$ with support contained in $(-\infty, \gamma)$ and such that $v(a - b) \geq \gamma$.

We denote by $E[t^\Gamma]$, [resp. $E(t^\Gamma)$] the subring [resp. subfield] of $E((t^\Gamma))$ generated by E and all elements t^γ, $\gamma \in \Gamma$.

Lemma 3.5. *Let E be an algebraically closed field of positive characteristic p, and let Γ be a torsion free abelian group. Let $f = \sum a_\gamma t^\gamma \in E[t^\Gamma]$, and let Δ be the subgroup of Γ generated by* $\mathrm{Supp}(f)$.

(1) *There is $h \in E(t^\Gamma)$ such that $h^p - h = f$ if and only if there is a partition of $\mathrm{Supp}(f) \setminus \{0\}$ into subsets S_i satisfying the following condition for each i: there is $\gamma_i \in S_i$ such that for all $\gamma \in S_i$, there exists $m(\gamma) \in \mathbb{N}$ such that*

$$\gamma = p^{m(\gamma)}\gamma_i, \text{ and } \sum_{\gamma\in S_i} a_\gamma^{1/p^{m(\gamma)}} = 0.$$

Furthermore, if $f = h^p - h$ then $h \in E[t^\Delta]$.

(2) *Assume that no element of $\mathrm{Supp}(f)$ is divisible by p in the subgroup Δ, and that for some $g \in E[t^\Delta]$, with $|\mathrm{Supp}(g)| = |\mathrm{Supp}(f)|$, there is some $h \in E[t^\Gamma]$ such that $h^p - h = f - g$. Then there is a (unique) bijection $\pi : \mathrm{Supp}(f) \to \mathrm{Supp}(g)$ such that for each $\gamma \in \mathrm{Supp}(f)$, there is some $m(\gamma)$ such that $\pi(\gamma) = p^{m(\gamma)}\gamma$, and the coefficient of $t^{\pi(\gamma)}$ in g equals $-a_\gamma^{p^{m(\gamma)}}$.*

Proof. (1) The right to left implication is clear, since for any integer $m > 0$, $x^{p^m} - x = h^p - h$, where $h = \sum_{i=0}^{m-1} x^{p^i}$. Note that this h belongs to the ring generated by x.
Assume now that $f = h^p - h$. The ring $E[t^\Gamma]$ is integrally closed, and therefore $h \in E[t^\Gamma]$. Write $h = \sum_\gamma c_\gamma t^\gamma \in E[t^\Gamma]$, and assume that the right hand side of the equivalence does not hold. We will show that this leads to a contradiction. Observe that the sets S_i are uniquely determined by the support of f. Using the remark made in the proof of the right to left implication and the fact that E is perfect, we may assume that no non-zero element of the support of f is divisible by p in Δ. Hence, each S_i consists of a singleton, and at least one of them is non-empty. But on the other hand, we have

$$a_\gamma = (c_{\gamma/p})^p - c_\gamma \tag{$*$}$$

for each $\gamma \in \Gamma$. If $\gamma = 0$, this simply says that $a_0 = c_0^p - c_0$. If $\gamma \neq 0$, our condition on the S_i's implies that $a_{p^i\gamma} = 0$ for all $0 \neq i \in \mathbb{Z}$. Hence,

$$c_{p^{i-1}\gamma}^p = c_{p^i\gamma} \text{ for all } 0 \neq i \in \mathbb{Z}.$$

But h has finite support, so this implies that all $c_{p^i\gamma}, i \in \mathbb{Z}$, are 0, and therefore that $a_\gamma = 0$, the desired contradiction.
Using $(*)$, the same reasoning shows that if $h^p - h = f$, then $h \in E[t^\Delta]$.
(2) This is essentially clear from (1). Note that $0 \notin \mathrm{Supp}(f)$. Let $S = \mathrm{Supp}(f) \cup \mathrm{Supp}(g)$, and $\{S_i\}$ the partition of S given by (1). Then each S_i contains at most one element of $\mathrm{Supp}(f)$, has at least two elements (by (1)), and therefore contains precisely one element of $\mathrm{Supp}(f)$ and one element of $\mathrm{Supp}(g)$. This gives the bijection π, and the rest follows from (1).

The following result is probably well-known, but for lack of a reference we will give its proof.

Proposition 3.6. *Let E be a field, and Γ a subgroup of $\mathbb{R}$ such that $\bigcap_{n\in\mathbb{N}} p^n\Gamma = (0)$ if $char(E) = p > 0$. The elements of $E((t^\Gamma))$ which are separably algebraic over $E(t^\Gamma)$ have the following property: their support is either finite or of order type ω and cofinal in $\mathbb{R}$. Moreover, the subring $E[t^\Gamma]$ is dense in $E(t^\Gamma)^s \cap E((t^\Gamma))$.*

Proof. We consider the completion $E(t^\Gamma)^c$ of $E(t^\Gamma)$ with respect to the valuation. This is the smallest field containing limits of all sequences $(a_n)_{n\in\mathbb{N}}$ of elements of $E(t^\Gamma)$, with $v(a_{n+1} - a_n)$ increasing and cofinal in $\mathbb{R}$. Then $E(t^\Gamma)^c$ is henselian (see Chapter 2 of [23]).

Claim. $E(t^\Gamma)^c$ coincides with the set K of elements of $E((t^\Gamma))$ whose support is either finite or of order type ω and cofinal in Γ.

Note that $a \in K$ if and only if for every $\gamma \in \mathbb{R}$, $\mathrm{Supp}(a) \cap (-\infty, \gamma)$ is finite. Clearly K contains $E[t^\Gamma]$ and is closed under addition. For multiplication, let $a, b \in K$, $\gamma \in \mathbb{R}$; then $\mathrm{Supp}(ab) \cap (-\infty, \gamma) \subset \mathrm{Supp}(a_{|\gamma - v(b)} \cdot b_{|\gamma - v(a)})$. Similarly, if $a \in K$ with $v(a) > 0$, $\gamma > 0$, and k is the smallest integer such that $kv(a) > \gamma$, then $\mathrm{Supp}((1 + a)^{-1}) \cap (-\infty, \gamma) \subset \mathrm{Supp}(1 + a_{|\gamma} + \cdots + a^{k-1}{}_{|\gamma})$. This implies that K is a subfield of $E((t^\Gamma))$. It follows that every element of $E(t^\Gamma)^c$ is the limit of a sequence of elements of $E[t^\Gamma]$, and therefore coincides with K. This finishes the proof of the claim.

Thus the ring $E[t^\Gamma]$ is dense in $E(t^\Gamma)^c$: for every $a \in E(t^\Gamma)^c$ and $\gamma \in \mathbb{R}$, there is $b \in E[t^\Gamma]$ such that $v(a-b) > \gamma$. The field $E(t^\Gamma)^c$ is henselian, and if $char(E) = 0$, it has no proper immediate algebraic extension (see 3.2), so that the result holds.

Assume now that $char(E) = p > 0$, and that L is a finite Galois extension of $E(t^\Gamma)^c$, with Galois group G. We need to show that $L_0 := L \cap E((t^\Gamma)) = E(t^\Gamma)^c$. We assume this is not the case, and take such an L_0 of minimal degree over K, and L its normal closure over K. We denote also by v the unique extension of v to L. If $G_v = \{\rho \in G \mid \forall x \in L\, v(\rho(x) - x) > v(x)\}$, then the subfield L_1 of L fixed by G_v is contained in $L_2 := E'(t^{\Gamma'})^c$, for some separable extension E' of E and overgroup Γ' of Γ such that $[\Gamma' : \Gamma]$ is prime to p. Indeed, $L_1 = K(\alpha, \beta)$, where the residue field of $K(\alpha)$ is separable over E, and the extension $K(\alpha, \beta)/K(\alpha)$ is totally ramified of degree prime to p, see Corollary 5.3.8 in [7]. Moreover L_2 and L_0 are linearly disjoint over K, and $\mathcal{G}al(L/L_1) = G_v$ is a p-group, which is normal in G. The minimality of L_0 then implies that L_0L_1 contains a Galois extension of degree p of L_1, i.e., contains some Artin-Schreier extension of L_1 which is immediate over L_1. As L_2 and L_0 are linearly disjoint over K, it is enough to show: no Artin-Schreier extension of L_2 is immediate.

Assume by way of contradiction that $L_2(a)$ is an immediate Artin-Schreier extension of L_2, where $b = a^p - a \in L_2$. Because L_2 is Henselian, every element of positive valuation is of the form $x^p - x$ for some $x \in L_2$, so that $v(b) \le 0$, and without loss of generality, $b \in E'[t^{\Gamma'^{\le 0}}]$ has finite support (use the claim, and the fact that every element of positive valuation is of the form $x^p - x$ in a Henselian field). Write $b = \sum_\gamma c_\gamma t^\gamma$, $c_\gamma \in E'$, $\gamma \in \Gamma'$. We may then assume that each $c_\gamma t^\gamma$ with $\gamma < 0$ is not a p-th power in L_2: otherwise, let s be maximal such that $c_\gamma t^\gamma \in L_2^{p^s}$ (recall that no element of Γ is infinitely p-divisible, hence the same holds for Γ'), and add to b the element $c_\gamma^{p^{-s}} t^{p^{-s}\gamma} - c_\gamma t^\gamma$ (which is of the form $d^p - d$ for some $d \in L_2$, see 3.5, proof of (1)). Let γ_0 be the least element of the support of b. Now, $v(a) = v(b)/p$, and because

$e(L_2(a)/L_2) = 1$, it follows that $\gamma_0 \in p\Gamma'$; if $\gamma_0 < 0$, it then implies that c_{γ_0} is not a p-th power in E', but as $v(a - c_{\gamma_0} t^{\gamma_0/p}) > v(a)$, we get a contradiction with $f(L_2(a)/L_2) = 1$. Finally, we cannot have $\gamma_0 = 0$, since then $L_2(a)$ would be a purely residual extension of L_2.
Comment. Actually, this proof can be easily modified to show that $K = E(t^\Gamma)^c$ is defectless, the point being to reduce to the case of immediate Artin-Schreier extensions.

3.7. Conventions and some basic results and definitions in algebraic geometry. Recall that we work in a large saturated model (Ω, σ) of ACFA. Our varieties will always be quasi-projective and absolutely irreducible. If a variety V is defined over the field K, then $K(V)$ denotes its function field, and if V is affine, $K[V]$ denotes the affine ring of V (over K). We view the elements of $K(V)$ as (partially defined) functions on V. If $x \in V(K)$, then $\mathcal{O}_{x,V}$ will denote the ring of elements of $K(V)$ which are defined at x, and $\mathcal{M}_{x,V}$ its maximal ideal, which consists of functions vanishing at x. We use the same notation if U is an affine open subset of V, and x a prime ideal of $K[U]$, to denote the localization of $K[U]$ at the ideal x and its maximal ideal.

Recall that the variety V is *normal* if whenever U is an affine open subset of V (defined over K), then $K[U]$ is integrally closed in its fraction field. If V is normal and affine, and L is a finite algebraic extension of $K(V)$, then the *normalisation of* V *in* L is the variety W whose affine ring is the integral closure R of $K[V]$ in L; it is therefore affine, and comes with a dominant finite map $f : W \to V$, dual to the inclusion $K[V] \subset R$. If V is normal and projective, and $V = \bigcup U_i$ where the U_i's are affine open, then the *normalisation* W *of* V *in* L is $W = \bigcup W_i$, where each W_i is the normalisation of U_i in L. The map $f : W \to V$ is obtained by glueing the maps $f_i : W_i \to U_i$. See Theorem 4 of III.8 in [21], or Theorem 4 of V.4 in [18].

3.8. Finite morphisms, ramification. A dominant morphism $f : V \to W$ between two affine varieties is *finite* if $K[V]$ is integral over $f^*(K[W])$. If V and W are quasi-projective, then it is *finite* if W can be covered by affine subsets W_i with $f^{-1}(W_i)$ affine, and the restriction of f to $f^{-1}(W_i)$ finite.
Assume that W is **normal**, and f finite. If $y \in W(\Omega)$, the dominant finite morphism f is *unramified over* y if $f^{-1}(y)$ contains $\deg(f)$ distinct points, where $\deg(f) = [K(V) : f^*K(W)]$; if $|f^{-1}(y)| < \deg(f)$, then we say that f *ramifies over* y. The set of points of W over which f is ramified is called the *locus of ramification* (or *ramification locus*) of f. This is a Zariski closed subset of W, which is defined over K (see Thm 4 of II. 6.3 of [24]). If f is inseparable, it is all of W. We say that f is *unramified over* W, if it is unramified over every point of W.

There is an alternate, equivalent definition involving local rings, see [20] I.3 (p. 21): without loss of generality assume that V and W are affine, let x be a prime ideal of $K[V]$, $y = f(x)$, and $\mathcal{O}_x, \mathcal{O}_y$ the corresponding localisations of $K[V]$ and $K[W]$; we identify $\mathcal{O}_y$ with a subring of $\mathcal{O}_x$ via f^*. Then f is unramified at x if and only if $\mathcal{O}_x/\mathcal{M}_y\mathcal{O}_x$ is a separable field extension of $\mathcal{O}_y/\mathcal{M}_y$. Note that this statement has two implications: that $\mathcal{M}_y$ generates the maximal ideal of $\mathcal{O}_x$, and that the residue field $\mathcal{O}_x/\mathcal{M}_x$ is separably algebraic over $\mathcal{O}_y/\mathcal{M}_y$. We say that f is unramified over y if it is unramified at every point $x \in f^{-1}(y)$, and that it is unramified over W if it is unramified over every point of W (or equivalently, of $W(K^{alg})$).

3.9. Ramification divisor. Let $f : V \to W$ be as above, and $S \subset W$ a subvariety of codimension 1. As W is normal, the function which to an element $g \in K(W)$ associates its order of vanishing on S, defines a discrete valuation v_S on $K(W)$, which we call a *divisorial valuation*. This valuation v_S extends to $K(V)$, and may or may not ramify. Note that by 3.2, v_S is defectless.
The *ramification divisor* is the union of all subvarieties S of V of codimension 1 such that the associated valuation v_S ramifies in $K(W)$. Note that we are not interested in multiplicities here; thus the ramification divisor in our sense is the support of the ramification divisor in the sense, e.g., of Hartshorne [8], p. 301 (for curves).

We will use the following result of Zariski, see [17], Proposition 4, or [1], Thm 1:

Theorem 3.10. *If W is non-singular, then the ramification divisor of f and the ramification locus of f coincide.*

Lemma 3.11. *Let $E = \mathrm{acl}_\sigma(E)$, let B be a definable subgroup of some algebraic group G defined over E, and let a be a generic of B. Assume that $\sigma(a) \in E(a)^{alg}$, let $\ell > 0$ and let $B_{(0)}$ and $V_{0,\ell}$ be the algebraic loci of a and of $(a, \sigma^\ell(a))$ over E. Assume that the variety $V_{0,\ell}$ contains a proper infinite subvariety W such that $\pi_0(W)^{\sigma^\ell} = \pi_\ell(W)$ have the same dimension as W, where $\pi_0 : V_{0,\ell} \to B_{(0)}$ and $\pi_\ell : V_{0,\ell} \to B_{(0)}^{\sigma^\ell}$ are the natural projections given by the inclusion $V_{0,\ell} \subset B_{(0)} \times B_{(0)}^{\sigma^\ell}$. Then $\mathrm{evSU}(a/E) > 1$.*

Proof. The assumption $\sigma(a) \in E(a)^{alg}$ implies that $\dim(V_{0,\ell}) = \dim(B_{(0)})$, and that $\dim(W) < \dim(B_{(0)})$. Moreover, $\sigma(a) \in E(a)^{alg}$ implies that a is also a generic of $B(\ell)$, and therefore B, $B(\ell)$ and $tp(a/E)$ have the same evSU-rank.

We now work in $\Omega[\ell]$. Let $F = \mathrm{acl}_\sigma(F)$ contain E and such that W is defined over F. By properties of the theory ACFA and the fact that $\Omega[\ell]$ is a model of ACFA, there is some $b \in B(\ell)$ such that $(b, \sigma^\ell(b)) \in W$, and $\mathrm{tr.deg}(F(b)_\sigma/F) = \dim(W)$. Then $0 < \mathrm{tr.deg}(F(b)_\sigma < \mathrm{tr.deg}(E(a)_\sigma/E)$, so b is not a generic of $B(\ell)$, and is not algebraic over F. Hence $\mathrm{SU}(a/E)[\ell] > 1$.

Proposition 3.12. *Let $E = \mathrm{acl}_\sigma(E)$, G a connected commutative algebraic group, and B a definable modular subgroup of $G(\Omega)$, of eventual SU-rank 1 and Zariski dense in G, everything being defined over E. Let a be a generic of B over E (so that $E(a) \simeq E(G)$), and assume that $\sigma(a) \in E(a)^{alg}$. Let L be a finite Galois extension of $E(a)$, and assume that L is linearly disjoint from $E(a)_\sigma$ over $E(a)$, and is such that $L(\sigma(a)) = \sigma(L)(a)$. If W is the normalisation of G in L, then the map $f : W \to G$ is unramified.*

Proof. Assume by way of contradiction that the map $f : W \to G$ is ramified, let $\mathcal{S}$ be the ramification divisor of f, S an irreducible component of $\mathcal{S}$, and $v = v_S$ the associated valuation (see 3.9). Let V_1 be the algebraic locus of $(a, \sigma(a))$ over E. Then V_1 is an algebraic subgroup of $G \times G^\sigma$, and is therefore non-singular.

Each of the projections $\pi_0 : V_1 \to G$ and $\pi_1 : V_1 \to G^\sigma$, being a group homomorphism, is the composition of a purely inseparable morphism with an unramified morphism. Moreover, as

E is algebraically closed, so that $G(E)$ contains the torsion subgroup of G, the field $E(a, \sigma(a))$ is a normal extension of $E(a)$ and of $E(\sigma(a))$. Then, Lemma 3.3 (2) and (3) imply that if w is any extension of v to $E(a, \sigma(a))$, then $r(L/E(a)) = r(L(\sigma(a))/E(a, \sigma(a))) = r(\sigma(L)/E(\sigma(a)))$ (here we use the fact that $\sigma(L)(a) = L(\sigma(a))$). Then the restriction of w to $E(\sigma(a))$ is a divisorial valuation v_T, with T an irreducible component of $\pi_1\pi_0^{-1}(S)$ (this uses the fact that the ramification divisor coincides with the ramification locus – see 3.10 – and that the maps π_0 and π_1 are finite, everywhere defined).

On the other hand, we know that $\mathcal{S}^\sigma$ is the ramification divisor of $f^\sigma : W^\sigma \to G^\sigma$. Hence T is an irreducible component of $\mathcal{S}^\sigma$. This reasoning can be repeated: we fix an extension w of v to $E(a, \sigma(a), \dots, \sigma^\ell(a))$, with $\ell = |\mathcal{S}|$. We then get a sequence $S = S_0, S_1, \dots, S_\ell$ of elements of $\mathcal{S}$ such that the restriction of w to $E(\sigma^i(a))$ coincides with the valuation v_i associated to $S_i^{\sigma^i}$. Then necessarily there are $0 \le i < j \le \ell$ such that $S_i = S_j$, and looking at the algebraic locus $V_{i,j}$ of $(\sigma^i(a), \sigma^j(a))$ over E, we obtain a subvariety U of $V_{i,j}$, such that $v_U = w|E(\sigma^i(a), \sigma^j(a))$ ramifies in $\sigma^i(L)(\sigma^j(a))$, and the projections of U on G^{σ^i} equals $S_i^{\sigma^i}$, the projection of U on G^{σ^j} equals $S_i^{\sigma^j}$. Lemma 3.11 gives us the desired contradiction when $\dim(G) > 1$.

Assume now that $\dim(G) = 1$. Because $tp(a/E)$ is modular and $\text{tr.deg}(a/E) = 1$, we know that the set $\{[E(a, \sigma^k(a)) : E(a)]_s \mid k \in \mathbb{Z}\}$ is unbounded (see (4.5) in [2]). Choose $k \in \mathbb{Z}$ such that $[E(a, \sigma^k(a)) : E(a)]_s = N > |\mathcal{S}|$. As E is algebraically closed, if $P \in \mathcal{S}$ then the valuation v_P has N distinct extensions $w_1, \dots, w_N$ to $E(a, \sigma^k(a))$, which correspond to the N distinct points $Q_1, \dots, Q_N \in G^{\sigma^k}(E)$ such that each (P, Q_i) belongs to the algebraic locus $V_{0,k}$ of $(a, \sigma^k(a))$ over E; the restrictions of the valuations w_i to $E(\sigma^k(a))$ are therefore distinct (they equal the v_{Q_i}), and the points $Q_1, \dots, Q_N$ are in $\mathcal{S}^{\sigma^k}$. This gives the desired contradiction.

Lemma 3.13. *Let G be a semi-abelian variety defined over $E = \text{acl}_\sigma(E)$, and let B be a definable subgroup of $G(\Omega)$ of finite SU-rank. Let $n \in \mathbb{N}^{>0}$, and let a be a generic of B over E, and b such that $[n]b = a$. Then $E(b)_\sigma$ is a finite σ-stable normal extension of $E(a)_\sigma$.*

Proof. We use the notation introduced at the beginning of section 2. The truth of this statement only depends on $qftp(a/E)$ (see (2.9)(2) in [2]), and we may therefore assume that $b \in B$, and that $B = \tilde{B}$. Since $[B : B^0]$ is finite and E is algebraically closed, we may also assume that $B = B^0$. The normality of $E(b)_\sigma$ over $E(a)_\sigma$ follows from the fact that E contains the torsion subgroup of G and of the G^{σ^i}. Let m be such that $B = \tilde{B}_{(m)}$, and let $N \ge m$. Then $B_{(N)}$ is a semi-abelian variety which projects onto $B_{(m)}$ with finite fibers, so that $\dim(B_{(N)}) = \dim(B_{(m)}) =: g$. Moreover, if r is the dimension of the maximal abelian quotient of $B_{(m)}$, then it is also the dimension of the maximal abelian quotient of $B_{(N)}$. Therefore, the map $[n] : B_{(N)} \to B_{(N)}$ has degree $n^{2r+g-r} = n^{g+r}$.

The tuple $(b, \sigma(b), \dots, \sigma^N(b))$ is a generic of $B_{(N)}$ for every N, whence

$$[E(b, \sigma(b), \dots, \sigma^N(b)) : E(a, \dots, \sigma^N(a))] = n^{g+r}, \qquad \text{and } [E(b)_\sigma : E(a)_\sigma] = n^{g+r}.$$

Lemma 3.14. *Let $E = \text{acl}_\sigma(E) \subseteq F = \text{acl}_\sigma(F)$, and let a be independent from F over E. Assume that L is a proper finite separable σ-stable extension of $\text{acl}_\sigma(Ea)F$. Then there is F_1, independent from (a, F) over E, and a finite σ-stable Galois extension M of $FF_1(a)_\sigma$ such that $L \subseteq \text{acl}_\sigma(F_1 a)M$.*

Proof. Write $A = E(a)^s_\sigma$, and $L_0 = L \cap (AF)^s$. Note that since L is separable over $\mathrm{acl}_\sigma(Ea)F$, and $\mathrm{acl}_\sigma(Ea)$ is purely inseparable over A, we have $L = L_0\mathrm{acl}_\sigma(Ea)$. It therefore suffices to find such an M with $L_0 \subseteq \mathrm{acl}_\sigma(F_1a)M$.
AF is a normal extension of $F(a)_\sigma$, and the normal closure of L_0 over $F(a)_\sigma$ is therefore a finite σ-stable Galois extension of AF (see (2.9)(3) in [2]). We may therefore assume that L_0 is Galois over $F(a)_\sigma$.
Recall that we work inside the large difference field Ω. Let φ be an A-automorphism of Ω such that $\varphi(F) = F_1$ is independent from (F, a) over E, and let $L_1 = \varphi(L_0)$. Then L_0L_1 is a Galois extension of $FF_1(a)_\sigma$, which contains AF, and we will identify

$$\mathcal{G}al(L_0L_1/FF_1(a)_\sigma) \simeq \mathcal{G}al(L_0/F(a)_\sigma) \times_{\mathcal{G}al(A/E(a)_\sigma)} \mathcal{G}al(L_1/F_1(a)_\sigma).$$

Consider the subgroup H of $\mathcal{G}al(L_0L_1/FF_1(a)_\sigma)$ defined by

$$H = \{(\tau, \varphi\tau\varphi^{-1}) \mid \tau \in \mathcal{G}al(L_0/F(a)_\sigma)\}.$$

As φ is an A-isomorphism of difference fields, H is a closed subgroup of $\mathcal{G}al(L_0L_1/FF_1(a)_\sigma)$, which projects onto $\mathcal{G}al(A/E(a)_\sigma)$ and $\sigma^{-1}H\sigma = H$. Observe that $[\mathcal{G}al(L_0L_1/FF_1(a)_\sigma) : H] = [L_0 : AF]$ is finite. Hence, the subfield M of L_0L_1 which is fixed by H is a finite σ-stable extension of $FF_1(a)_\sigma$, and intersects AFF_1 in $FF_1(a)_\sigma$.

We have $\mathcal{G}al(L_0L_1/L_1) \cap H = \{1\}$, whence $L_1M = L_0L_1$. From $L_1 \subset F_1(a)^s_\sigma$, we obtain the result.

Lemma 3.15. *Let $E = \mathrm{acl}_\sigma(E)$, a a finite tuple, and assume that M is a finite σ-stable extension of $E(a)_\sigma$. Then there are $r \in \mathbb{N}$ and a finite extension L of $E(a, \dots, \sigma^r(a))$ such that $M = LE(a)_\sigma$, L is linearly disjoint from $E(a)_\sigma$ over $E(a, \dots, \sigma^r(a))$, $[L : E(a, \dots, \sigma^r(a))] = [M : E(a)_\sigma]$ and $\sigma(L)(a) = L(\sigma^{r+1}(a))$.*
Moreover, if L is as above and $E(a, \dots, \sigma^r(a)) \subseteq L_0 \subseteq L$ is such that $L_0E(a)_\sigma$ is σ-stable, then we also have $\sigma(L_0)(a) = L_0(\sigma^{r+1}(a))$, and $L\sigma(L) = L_0\sigma(L_0) = \sigma(L_0)L$.

Proof. Fix a finite tuple α generating M over $E(a)_\sigma$. Then there are integers $i \leq j$ such that the extension $M' = E(\sigma^i(a), \dots, \sigma^j(a), \alpha)$ of $E(\sigma^i(a), \dots, \sigma^j(a))$ has degree $[M : E(a)_\sigma]$. By assumption, $\sigma(M') \subseteq M'E(a)_\sigma$ and $M' \subseteq \sigma(M')E(a)_\sigma$. Hence there are integers $\ell \leq i$ and $k \geq j$ such that $\sigma(M') \subseteq M'E(\sigma^\ell(a), \dots, \sigma^k(a))$ and $M' \subseteq \sigma(M')E(\sigma^\ell(a), \dots, \sigma^k(a))$. Define $L = \sigma^{-\ell}(M')E(a, \dots, \sigma^{-\ell+k}(a))$. Then $[L : E(a, \dots, \sigma^{-\ell+k}(a))] = [M : E(a)_\sigma]$. An easy computation shows that $\sigma(L) \subseteq L(\sigma^{-\ell+k+1}(a))$ and $L \subseteq \sigma(L)(a)$.
Write $b = (a, \dots, \sigma^{-\ell+k}(a))$, and let now $E(b) \subset L_0 \subset L$ be such that $L_0E(b)_\sigma$ is σ-stable. The linear disjointness of L and $E(a)_\sigma = E(b)_\sigma$ over $E(b)$ implies that L is linearly disjoint from $M_0 = L_0E(b)_\sigma$ over $L_0E(b) = L_0$. In particular, $[L : L_0] = [L\sigma(L_0) : L_0\sigma(L_0)] = [L\sigma(L) : L_0\sigma(L_0)]$ (because $\sigma(b) \in \sigma(L_0)$), and therefore we obtain $[L_0\sigma(L_0) : E(b, \sigma(b))] = [L_0 : E(b)]$, which implies $L_0(\sigma(b)) = L_0\sigma(L_0) = \sigma(L_0)(b)$. The second set of equalities is also clear from the above.

Lemma 3.16. *Let $E = \mathrm{acl}_\sigma(E)$, B a E-quantifier-free definable subgroup of a semi-abelian variety G, and assume that if $a \in B$, then $\sigma(a) \in E(a)^{alg}$. Let $n \geq 1$ be an integer, let $B(n)$*

be the σ^n-closure of B (for the σ^n-topology), let B^0 be the connected component of B, and let $m \in \mathbb{Z}$, $\tau = \mathrm{Frob}^m \sigma^n$. We use the additive notation for the group law. The following properties are equivalent:

(a) For all (some) generic a of B^0 (over E), and field $F = \mathrm{acl}_\sigma(F)$ containing E, if L is a finite separable σ-stable extension of $F(a)_\sigma$, then for some integer N and $b \in G(\Omega)$ such that $[N]b = a$, we have $L \subset F(b)_\sigma$.

(b) For all $a \in B$ and field $F = \mathrm{acl}_\sigma(F)$ containing E, if L is a finite separable σ-stable extension of $F(a)_\sigma$, then for some integer N and $b \in G(\Omega)$ such that $[N]b = a$, we have $L \subset F(b)_\sigma$.

(c) For all $a \in B(n)$ and field $F = \mathrm{acl}_{\sigma^n}(F)$ containing E, if L is a finite separable σ^n-stable extension of $F(a)_{\sigma^n}$, then for some integer N and $b \in G(\Omega)$ such that $[N]b = a$, we have $L \subset F(b)_{\sigma^n}$.

(d) For all $a \in B(n)$ and field $F = \mathrm{acl}_\tau(F)$ containing E, if L is a finite separable τ-stable extension of $F(a)_\tau$, then for some integer N and $b \in G(\Omega)$ such that $[N]b = a$, we have $L \subset F(b)_\tau$.

Proof. First some comments about (a): recall that the finite σ-stable Galois extensions of a difference field are determined by its isomorphism type and do not depend on the extension of the automorphism to the algebraic closure (1.3). Hence, the truth of (a) only depends on the generic quantifier-free type of B^0, not on a particular realisation. (b) clearly implies (a), and we will now show that (a) implies (b). Let $a \in B$, $F = \mathrm{acl}_\sigma(F)$ containing E and L a finite separable σ-stable extension of $F(a)_\sigma$. Let a_2 be a generic of B^0 over $\mathrm{acl}_\sigma(Fa)$, let $a_1 = a - a_2$, and $F_1 = \mathrm{acl}_\sigma(Fa_1)$. By (a), there are an integer N and a tuple b_2 such that $[N]b_2 = a_2$ and $F_1L \subset F_1(b_2)_\sigma$. If $b_1 \in F_1$ is such that $[N]b_1 = a_1$, setting $b = b_1 + b_2$, we obtain $L \subset F_1(b)_\sigma \cap \mathrm{acl}_\sigma(Fa) = F(b)_\sigma$. This proves (b) and finishes the proof of the first equivalence.

Observe that if $a \in B$ realises a generic of B, then $qftp(a/E)[m]$ is a generic type of $B(m)$. Together with the first equivalence (applied to σ^n and to τ), this allows us to restrict our attention to tuples a which are generics of B^0. We let a denote a generic of B over E.

Assume (c), and let L be a finite separable σ-stable extension of $F(a)_\sigma$, for some $F = \mathrm{acl}_\sigma(F)$ containing E. Because $\sigma(a) \in E(a)^{alg}$, it follows that for some $N > 0$, we have $[N]\sigma^j(a) \in E(a)_{\sigma^n}$ for all $j = 1, \dots, n-1$, and that $F(a)_\sigma$ is a finite σ^n-stable extension of $F(a)_{\sigma^n}$ (Lemma 3.13). Hence so is L, which easily gives the result: if $L_0 = L \cap F(a)^s_{\sigma^n}$, then L_0 is a finite separable σ^n-stable extension of $F(a)_{\sigma^n}$ and $L = L_0F(a)_\sigma$, so that (c) implies (b).

Assume now (b). Let $F = \mathrm{acl}_{\sigma^n}(F)$ contain E, and L a finite separable σ^n-stable extension of $F(a)_{\sigma^n}$. We may assume that F is closed under σ as well (by (1.12) in [2] applied to the extension $FE(a)_\sigma$ of $E(a)_\sigma$). But then $L\sigma(L)\cdots\sigma^{n-1}(L)$ is a finite separable σ-stable extension of $F(a)_\sigma$, and therefore contained in $F(b_1)_\sigma$ for some b_1 with $[N]b_1 = a$ some N. As $\sigma(a), \dots, \sigma^{n-1}(a) \in E(a)^{alg}$, there is M such that $E(a)_\sigma \subset E(b_2)_{\sigma^n}$ for some b_2 with $[M]b_2 = a$. If b is such that $[MN]b = a$, then $L \subset E(b)_{\sigma^n}$.

To show the last equivalence, we may assume that $n=1$. Observe that τ is definable in (Ω,σ), that σ is definable in (Ω,τ), and that $E(a)_\sigma E(a)_\tau$ is purely inseparable over $E(a)_\sigma$ and over $E(a)_\tau$.

Assume first that it holds for τ, and that $m<0$; let $F=\mathrm{acl}_\sigma(F)$ $(=\mathrm{acl}_\tau(F))$ contain E, and L a finite separable σ-stable extension of $F(a)_\sigma$. Apply Lemma 3.15 to get a generator α of L over $F(a)_\sigma$, and an integer r such that the minimal polynomial of α over $F(a)_\sigma$ has its coefficients in $F(a,\sigma(a),\dots,\sigma^r(a))$ and $F(a,\sigma(a),\dots,\sigma^r(a),\sigma^{r+1}(a),\alpha) = F(a,\sigma(a),\dots,\sigma^{r+1}(a),\sigma(\alpha))$. Note that $\tau(\alpha)=\sigma(\alpha)^{p^m}$ generates $\sigma(L)$ over $E(\sigma(a),\dots,\sigma^{r+1}(a))$ (because $\sigma(L)$ is separable over $E(\sigma(a),\dots,\sigma^{r+1}(a))$). Then $\sigma=\tau\mathrm{Frob}^{-m}$, so that $F(a,\sigma(a),\dots,\sigma^r(a),\sigma^{r+1}(a))\subset F(a,\tau(a),\dots,\tau^{r+1}(a))$. As the extension $F(a,\tau(a),\dots,\tau^{r+1}(a))$ of $F(a,\sigma(a),\dots,\sigma^r(a),\sigma^{r+1}(a))$ is purely inseparable, it follows that

$$F(a,\tau(a),\dots,\tau^{r+1}(a),\alpha)=F(a,\tau(a),\dots,\tau^{r+1}(a),\tau(\alpha)),$$

so that $F(a)_\tau(\alpha)$ is a finite separable τ-stable extension of $F(a)_\tau$. By assumption, there is some N and b such that $[N]b=a$ and $\alpha\in F(b)_\tau$. Our assumptions on α then imply $\alpha\in F(b)_\sigma$.
If $m=0$, there is nothing to prove, and if $m\geq 1$, replacing τ and σ by τ^{-1} and σ^{-1} gives the result. The other direction is symmetric, interverting the roles of σ and τ.

Remark 3.17. Let $E=\mathrm{acl}_\sigma(E)$, a a tuple in $\mathcal{U}$ and assume that $\mathrm{evSU}(a/E)=1$, and $\mathrm{tr.deg}(E(a)_{\sigma^\ell}/E)$ does not depend on $\ell>0$. Let $\tau=\mathrm{Frob}^m\sigma^n$, and consider a in the reduct (Ω,τ). Then also $\mathrm{evSU}_\tau(a/E)=1$.

Proof. Our assumption on the transcendence degrees implies that $E(a)_\sigma\subset E(a)_{\sigma^n}^{alg}$. By definition of the evSU-rank, we know that the evSU-ranks of a over E in (Ω,σ) and in (Ω,σ^n) are the same, and so both equal 1. Assume that there is some $F=\mathrm{acl}_\tau(F)$ containing E and such that a is not independent from F over E (in (Ω,τ), equivalently in $\Omega[n]$). Noting that $F=\mathrm{acl}_{\sigma^n}(F)$, implies $a\in F$ and gives the desired conclusion.

3.18. Algebraically closed valued fields. Consider the theory of algebraically closed valued fields in the 2-sorted language $\mathcal{L}_{\mathrm{val}}$, with sorts for the valued field and the value group, v the valuation map : $K\to\Gamma\cup\{\infty\}$, and K and Γ are structures in the languages $\{+,-,\cdot,0,1\}$ and $\{+,-,0,\leq\}$ respectively. V. Weispfenning [25] showed that this theory eliminates quantifiers. (Other quantifier elimination results for algebraically closed valued fields were obtained by A. Robinson [22] and F. Delon [5].)

Let (K,v) be an algebraically closed valued field, E an algebraically closed subfield on which v is trivial, and assume that $\bar a=(a_1,\dots,a_n)\in K$ is such that $v(a_1),\dots,v(a_n)$ are $\mathbb{Q}$-linearly independent. Then, if $f(X_1,\dots,X_n)=\sum_\nu b_\nu X^\nu\in E[X_1,\dots,X_n]$ $(\nu=(\nu_1,\dots,\nu_n)\in\mathbb{N}^n$, $X^\nu=X_1^{\nu_1}\cdots X_n^{\nu^n})$, we have

$$v(f(\bar a))=\min_\nu\{v(b_\nu)+v(\bar a^\nu)\}.$$

In particular, $a_1,\dots,a_n$ are algebraically independent over E. Quantifier elimination then implies that $tp(\bar a/E)$ is completely determined by $tp(v(a_1),\dots,v(a_n))$ (in Γ), i.e., by the set of formulas $\sum_{i=1}^n m_i\xi_i > 0$ (where $m_i \in \mathbb{Z}$) satisfied by $v(\bar{a}) = (v(a_1), \ldots, v(a_n))$.

Let $\alpha \in E(\bar{a})^s$. Then $v(\alpha)$ belongs to the $\mathbb{Q}$-vector space generated by $v(a_1), \ldots, v(a_n)$; thus there are $\mathbb{Q}$-linear combinations $t_1(\bar{\xi}), \ldots, t_k(\bar{\xi})$ such that the values of the conjugates of α over $E(\bar{a})$ are in the set $\{t_1(v(\bar{a})), \ldots, t_k(v(\bar{a}))\}$. Let $P(\bar{a}, X)$ be the minimal polynomial of α over $E(\bar{a})$. Since $tp(v(\bar{a})) \vdash tp(\bar{a}/E)$, there is a finite conjunction $\psi(\bar{\xi})$ of formulas of the form $\sum_{i=1}^n m_i\xi_i > 0$ such that if $\bar{b} \in K$ is such that $v(\bar{b})$ satisfies ψ, and if β is a root of $P(\bar{b}, X)$, then $v(\beta) \in \{t_1(v(\bar{b})), \ldots, t_k(v(\bar{b}))\}$.

3.19. Algebraically closed valued fields with value group $\mathbb{R}$. Let E be an algebraically closed field of characteristic $p > 0$, and consider the (algebraically closed) valued field $(E((t^{\mathbb{R}})), v)$ with its natural valuation (see 3.4). We fix a positive integer n and define $\mathcal{R}$ to be the set of n-tuples of $\mathbb{R}^n$ which are $\mathbb{Q}$-linearly independent.

Let $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathcal{R}$, and let $\Gamma = \langle\gamma\rangle$ be the subgroup of $\mathbb{R}$ generated by the elements of γ. Let $\bar{a} = (t^{\gamma_1}, \ldots, t^{\gamma_n})$, let $\alpha \in E(\bar{a})^s$, $P(\bar{a}, X)$ its minimal polynomial over $E(\bar{a})$. An *open ball containing* γ is a set $B(\gamma; \varepsilon) = \{\delta \in \mathbb{R}^n \mid \|\delta - \gamma\| < \varepsilon\}$ for some $\varepsilon > 0$ (here $\| \ \|$ denotes the usual norm in Euclidean space). We will show the following:

Lemma 3.20. *Assumptions and notation as above. If $\alpha \in E((t^\Gamma))$, then there is an open ball B containing γ such that if $\bar{b}$ is an n-tuple in $E((t^{\mathbb{R}}))$ with $v(\bar{b}) \in B$, then the polynomial $P(\bar{b}, X)$ has a root β which generates an immediate extension of $E(\bar{b})$.*
Furthermore, if $Q(\bar{X}, \bar{Y}) \in E[\bar{X}, \bar{Y}]$ is such that $\alpha_{|0} = Q(\bar{a}, \bar{a}^{-1})$, then B can be chosen so that in addition the above root β satisfies $\beta_{|0} = Q(\bar{b}, \bar{b}^{-1})$.

Proof. The main difficulty is to say in a first order way that the extension is immediate. We will use repeatedly Proposition 3.6. Every element of Γ is a $\mathbb{Z}$-linear combination of elements of $v(\bar{a})$. Hence, there is $R[\bar{X}, \bar{Y}] \in E[\bar{X}, \bar{Y}]$ such that if $c = R(\bar{a}, \bar{a}^{-1})$, then $v(c) \geq 0$, and the minimal (monic) polynomial $F(\bar{a}, T)$ of $\alpha' = c\alpha$ over $E(\bar{a})$ has its coefficients in $E[t^{\Gamma_{\geq 0}}]$. By Proposition 3.6, we know that

$$\alpha' = \lim_{m\to\infty} \alpha'_{|m},$$

and therefore

$$\lim_{m\to\infty} v(F(\bar{a}, \alpha'_{|m})) = +\infty.$$

As $F'(\bar{a}, \alpha') \neq 0$ and $v(F'(\bar{a}, \alpha')) \geq 0$, for all sufficiently large $m \in \mathbb{N}$ we will have

$$v(F'(\bar{a}, \alpha'_{|m})) = v(F'(\bar{a}, \alpha')) \geq 0 \text{ and } v(F(\bar{a}, \alpha'_{|m})) > 2v(F'(\bar{a}, \alpha'_{|m})) + v(c).$$

We choose such an $m \geq v(c)$, so that $v(\alpha - \alpha'_{|m}c^{-1}) \geq m - v(c) \geq 0$. Let $Q_m[\bar{X}, \bar{Y}]$ be such that $\alpha'_{|m} = Q_m(\bar{a}, \bar{a}^{-1})$, and consider the $\mathcal{L}_{\mathrm{val}}(E)$-formula $\theta_{\mathrm{imm}}(\bar{x})$ which expresses the following:
(i) $v(F(\bar{x}, Q_m(\bar{x}, \bar{x}^{-1}))) > 2v(F'(\bar{x}, Q_m(\bar{x}, \bar{x}^{-1}))) + v(R(\bar{x}, \bar{x}^{-1}))$.
(ii) $v(Q_m(\bar{x}, \bar{x}^{-1})R(\bar{x}, \bar{x}^{-1})^{-1} - Q(\bar{x}, \bar{x}^{-1})) \geq 0$.
(iii) All monomials occuring in $Q(\bar{x}, \bar{x}^{-1})$ have valuation < 0, and $v(F'(\bar{x}, Q_m(\bar{x}, \bar{x}^{-1}))) \geq 0$, $v(R(\bar{x}, \bar{x}^{-1})) \geq 0$.

Then $\bar{a}$ satisfies this formula. Recall that because $\gamma \in \mathcal{R}$, $tp(\bar{a}/E)$ is axiomatised by formulas of the form $\sum_i m_i v(x_i) > 0$, where the m_i's are in $\mathbb{Z}$. Hence, there is a definable open subset X of $\mathbb{R}^n$ containing γ, and such that if $v(\bar{b}) \in X$, then $\bar{b}$ satisfies $\theta_{\rm imm}$. Because $\gamma \in \mathcal{R}$, there is an open ball B containing γ and contained in this set X.

Let $\bar{b}$ satisfy $\theta_{\rm imm}$. Then, by Hensel's Lemma, there is a root β' of $F(\bar{b}, T) = 0$ in the Henselization of $E(\bar{b})$, and which furthermore satisfies

$$v(\beta' - Q_m(\bar{b}, \bar{b}^{-1})) = v(F(\bar{b}, Q_m(\bar{b}, \bar{b}^{-1}))) - v(F'(\bar{b}, Q_m(\bar{b}, \bar{b}^{-1}))) \geq v(R(\bar{b}, \bar{b}^{-1})) \geq 0$$

and

$$v(\beta' R(\bar{b}, \bar{b}^{-1})^{-1} - Q(\bar{b}, \bar{b}^{-1})) \geq 0.$$

So, if $\beta = R(\bar{b}, \bar{b}^{-1})^{-1}\beta'$, then $P(\bar{b}, \beta) = 0$, $E(\bar{b}, \beta)$ is an immediate extension of $E(\bar{b})$, and $v(\beta - Q(\bar{b}, \bar{b}^{-1})) \geq 0$ (i.e.: $\beta_{|0} = Q(\bar{b}, \bar{b}^{-1})$).

Lemma 3.21. *Let $A \in \mathrm{GL}_n(\mathbb{Q})$, with $n \geq 1$. Suppose that for every $m \geq 1$, the characteristic polynomial of A^m is irreducible over $\mathbb{Q}$. Let $S \subset \mathcal{R}$ with the following properties:*

— *$A(S) \subseteq S \neq \emptyset$,*
— *if $r \in \mathbb{R}^{>0}$, then $rS = S$.*
— *S is closed in $\mathcal{R}$.*

Then there is $\gamma \in S$ such that for every $\varepsilon > 0$, there are infinitely many integers m such that

$$\left\| \frac{A^m(\gamma)}{\|A^m(\gamma)\|} - \frac{\gamma}{\|\gamma\|} \right\| < \varepsilon.$$

Proof. Our assumption on A implies that for every $m \geq 1$, all eigenvalues of A^m (in $\mathbb{Q}^{alg}$) are distinct, and that $\mathbb{R}^n$ has no A^m-stable subspace defined over $\mathbb{Q}$ (other than (0), $\mathbb{R}^n$). Hence, if V is a proper subspace of $\mathbb{R}^n$ defined over $\mathbb{Q}$, then V cannot contain a (non-empty) subset D other than $\{0\}$ which is A^m-stable for some $m \geq 1$: otherwise $\bigcap_n A^{mn}(V)$ would be a proper A^m-stable subspace of $\mathbb{R}^n$ containing D and defined over $\mathbb{Q}$.

We will work in the sphere $\mathbb{S}^{n-1} = (\mathbb{R}^n \setminus \{0\})/\mathbb{R}^{>0}$, which we identify with a compact subset of $\mathbb{R}^n$. We denote by $\tilde{S}$, $\tilde{\mathcal{R}}$, the images of S and $\mathcal{R}$ in $\mathbb{S}^{n-1}$, i.e. with the above identification, $\tilde{S} = S \cap \mathbb{S}^{n-1}$, $\tilde{\mathcal{R}} = \mathcal{R} \cap \mathbb{S}^{n-1}$. Let T be the closure of $\tilde{S}$ in $\mathbb{S}^{n-1}$; then T is compact and A-invariant. We call a point c of $\mathbb{S}^{n-1}$ *recurrent* if for every open set U containing c the set $\{m \in \mathbb{N} \mid A^m(c) \in U\}$ is infinite. So we want to find a recurrent point which is in $\tilde{S}$.

Since S is closed in $\mathcal{R}$, also $\tilde{S}$ is closed in $\tilde{\mathcal{R}}$, and it suffices to show that T contains a recurrent point which is in $\tilde{\mathcal{R}}$, since this point will necessarily be in $\tilde{S}$.

We recall the usual proof from topological dynamics: Take a maximal chain of non-empty closed A-invariant subsets of T; then the intersection C of this chain is non-empty (by compactness of T) and is minimal closed A-invariant. Thus if $c \in C$ and $k \geq 1$, then c belongs to the closure of $\{A^m(c) \mid m \geq k\}$, so that c is recurrent. Note also that $A(C) = C$.

Assume that $C \cap \tilde{\mathcal{R}}$ is empty. Thus C is covered by a union of hyperplanes of $\mathbb{R}^n$ which are defined over $\mathbb{Q}$. There are countably many such hyperplanes, and by Baire's lemma, there is a hyperplane H defined over $\mathbb{Q}$ such that $C \cap H$ has non-empty interior in C for the induced topology. I.e., there is an open subset O of $\mathbb{S}^{n-1}$ such that $\emptyset \neq O \cap C \subseteq H$. Note that $\bigcup_{m\in\mathbb{Z}} A^m(O)$ is an open set which is A-invariant and intersects C; by minimality of C, it contains C, and by compactness of C, there is a finite subset I of $\mathbb{Z}$ such that $C = \bigcup_{m\in I} A^m(C \cap O)$. Hence $C \subset \bigcup_{m\in I} A^m(H)$. From $A(C) = C$, we deduce that $\bigcap_{n\in\mathbb{N}} A^n(\bigcup_{m\in I} A^m(H))$ is non-empty and A-invariant. I.e, there are subspaces $V_1, \dots, V_r$ of $\mathbb{R}^n$ which are defined over $\mathbb{Q}$ and are such that $C \subset V_1 \cup \cdots \cup V_r = A(V_1 \cup \cdots \cup V_r)$. Thus A permutes the spaces V_i, and $A^{r!}(V_i) = V_i$ for any i. This contradicts our assumption.

4 The main result.

Notation and conventions are as before. In particular, p denotes $char(\Omega)$ if it is positive, and 1 if it is 0.

Proposition 4.1. *Let A be an abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, let B be a definable modular subgroup of $A(\Omega)$, with* $\mathrm{evSU}(B) = 1$*, let a be a generic of B over E, and let M be a finite σ-stable Galois extension of $E(a)_\sigma$. Assume that for every $\ell > 1$,* $\mathrm{tr.deg}(E(a)_\sigma/E) = \mathrm{tr.deg}(E(a)_{\sigma^\ell}/E)$*. Then for some N and $b \in A(\Omega)$ satisfying $[N]b = a$, $M \subset E(b)_\sigma$.*

Proof. B^0 has finite index in B, so at the cost of replacing a by some multiple $[m]a$ (see Lemma 3.13), we may assume that $a \in B^0$. Replacing a by $p_n(a) = (a, \dots, \sigma^n(a))$ for some n (and A by $B_{(n)}$, B by $p_n(B)$, see 2.1 for the notation), we may assume that $\sigma(a) \in E(a)^{alg}$, and that $M = LE(a)_\sigma$, where L is finite Galois over $E(a)$, linearly disjoint from $E(a)_\sigma$ over $E(a)$, and such that $L(\sigma(a)) = \sigma(L)(a)$ (see Lemma 3.15). Indeed, our assumption on the difference fields $E(a)_\sigma$ and $E(a)_{\sigma^\ell}$ implies that $\mathrm{evSU}(p_n(B)) = 1$ for all $n \geq 1$ (see Remark 3.17). Note that B is Zariski dense in A (by definition of $B_{(n)}$).
Let $f : W \to A$ be the normalisation of A in L.

By Proposition 3.12, f is unramified. By a result of Lang-Serre (Theorem 2 in [19]), this implies that W is isomorphic over E to an abelian variety A', and that f is a translate of an isogeny $A' \to A$. As E is algebraically closed, this implies that $L \subset E(b)$ where $[N]b = a$ for some $N > 0$.

4.2. The toric analogue, Proposition 4.3, is more involved, especially in characteristic $p > 0$; before plunging into the proof, we sketch it in a simplified setting. Using additive notation, up to finite index, the subgroups in question can be written:

$$B = \{x \in \mathbb{G}_m^n \mid \sigma(x) = Mx\},$$

where $M \in \mathrm{GL}_n(\mathbb{Q})$, and denominators are cleared in the obvious way. We treat here the case $M \in \mathrm{GL}_n(\mathbb{Z})$; a slight extension will work for $M \in \mathrm{GL}_n(\mathbb{Z}_p) \cap \mathrm{GL}_n(\mathbb{Q})$, but the general case is harder. We also consider, for simplicity, only Galois extensions of order p, where p is the characteristic.

We work over an algebraically closed difference field E, and define $E(B)$, the function field of B, to be $E(a)$ with the given action of σ: $a \mapsto Ma$, where $a = (a_1, \dots, a_n)$ is an n-tuple of independent elements. Let L be a difference field extension of $E(B)$, which is also a Galois extension of order p. We will show that if any such L exists, then B is non-orthogonal to the fixed field; indeed for some $k \geq 1$, B has a subgroup isogenous to a subgroup of $\mathbb{G}_m(\mathrm{Fix}(\sigma^k))$.

Any group embedding $\rho : \mathbb{Z}^n \to \mathbb{R}$ induces a Berkovich point, i.e. an $\mathbb{R}$-valued valuation on $E(B)$ over E; namely, the valuation satisfying

$$v(\sum_{\nu \in \mathbb{Z}^n} e_\nu a^\nu) = \min_{e_\nu \neq 0} \rho(\nu).$$

Let X be the space of all such valuations; so $X \subset \mathrm{Hom}(\mathbb{Z}^n, \mathbb{R}) = \mathbb{R}^n$, and X can be identified with $\mathcal{R}$ (see 3.19). The automorphism σ of $E(B)$ induces an automorphism σ of X. We let S be the set of valuations in X which ramify in L.

For any valuation v in S, if $L = E(B)(\alpha)$ with $\alpha^p - \alpha = c \in E(B)$ such that $v(c) < 0$ and $v(c)$ is not divisible by p in the value group of v, then it is easy to see that $v(c)$ is uniquely determined in terms of L, v: any c' with the same conditions will have $v(c') = v(c)$. (In fact, $c(1 + \mathcal{O}_v)$ is similarly determined.) See 3.3 and 3.5. Thus we may define $\theta(L, v) = v(c)$. Moreover, any Artin-Schreier extension of $E(B)$ in which v ramifies can be described in this fashion.

Furthermore, the variety $(\mathbb{P}^1)^n$ has no unramified covers, and using Lemma 3.12 and the inclusion $\mathbb{G}_m^n \subset (\mathbb{P}^1)^n$, it follows that S is non-empty. It also satisfies the hypotheses of Lemma 3.21.

We now work in the positive projectivization $\tilde{S} = (S/\mathbb{R}^{>0})$ of S and find a point $\bar{v}$ such that $\sigma^k(\bar{v})$ comes arbitrarily close to $\bar{v}$ (in $\tilde{S} \subset \mathbb{S}^{n-1}$). Say $\bar{v}$ is represented by $v \in S$.

Let Γ be the value group of v, a subgroup of $\mathbb{R}$ isomorphic to $\mathbb{Z}^n$. Then $\sigma^m(v) = v \circ \sigma^{-m}$ is a valuation with value group Γ; we have a group automorphism of Γ, still denoted σ, satisfying $v(\sigma(x)) = \sigma(v(x))$ (and with associated matrix M with respect to the basis $\{v(a_1), v(a_2), \ldots, v(a_n)\}$ of the $\mathbb{Z}$-module Γ).

Of course, σ does not preserve the ordering on Γ. But it does preserve (non)divisibility by p. Moreover since v was chosen recurrent, for any given element b of $E(B)$, if $v(b) < 0$ then for infinitely many k, taking $\sigma^k(v)(b)$ close enough to $v(b)$, we have also $\sigma^k(v)(b) < 0$. It follows that $\theta(L, v) = \theta(L, \sigma^k(v))$ for infinitely many k.

However, this means that σ^k has a fixed point in its action on Γ, namely $\theta(L, v)$. Thus the characteristic polynomial of M has a root ω with $\omega^k = 1$. It follows that B is (up to isogeny) a direct sum of subgroups, one of which has the form $\sigma(x) = M'x$ with M' having a cyclotomic characteristic polynomial. This finishes the sketch of proof in this easy case.

Proposition 4.3. *Let B be a definable modular subgroup of $\mathbb{G}_m(\Omega)$ of* evSU*-rank* 1*, defined over $E = \mathrm{acl}_\sigma(E)$, and let a be a generic of B over E. Assume that for every $\ell \geq 1$,* $\mathrm{tr.deg}(E(a)_{\sigma^\ell}/E) = n$*. If M is a finite σ-stable Galois extension of $E(a)_\sigma$, then $M \subseteq E(a^{1/N})_\sigma$ for some N.*

Proof. Our assumption on the transcendence degrees implies that $\mathrm{SU}(a/E)[\ell] = 1$ for every $\ell \geq 1$. By Lemma 3.16, we may replace B by its σ^ℓ-closure if necessary, and assume that B (or $B(\ell)$) is connected. Then a satisfies an equation $\prod_{i=0}^n \sigma^i(x^{d_i}) = 1$, where the d_i's are integers. We take such an equation of minimal complexity, i.e., n is minimal, and the d_i's have no common divisor (this latter condition is possible since B is connected; it will only be used in step 1, not in the rest of the proof). The minimality of n implies that $p_n(B)$ is Zariski dense in $\mathbb{G}_m^n$. Moreover, the polynomial $f(T) = \sum d_i T^i$ is irreducible (in $\mathbb{Q}[T]$, see 2.6).

Since the existence of such an M only depends on $qftp(a/E)$, we will also assume that for every $m > 1$, a has an m-th root in B.

Step 1. We may assume that $\sigma^n(a) \in E(a, \dots, \sigma^{n-1}(a))^s$, and if $n = 1$, that $a \in E(\sigma(a))^s$.
If $n = 1$, then p may divide one of d_0, d_1 but not both. Let $m = v_p(d_1/d_0)$ (v_p the p-adic valuation on $\mathbb{Q}$), and consider $\tau = \mathrm{Frob}^m\sigma$. If $m > 0$, then a satisfies $a^{d_0}\tau(a)^{p^{-m}d_1} = 1$, and if $m < 0$, a satisfies $a^{d_0p^m}\tau(a)^{d_1} = 1$. If $m = 0$, then both d_0 and d_1 are prime to p and we do nothing.
Assume now that $n > 1$, that p divides d_n, and let m be minimal such that $\ell := v_p(d_n) - nm = \inf\{v_p(d_i) - im \mid i = 0, \dots, n\}$. If $\tau = \mathrm{Frob}^m\sigma$, then $\tau(a)$ is in $\mathrm{Ker}\, s(\tau)$, where $s(T) = p^{-\ell}\sum_{i=0}^n p^{-im} d_i T^i \in \mathbb{Z}[T]$, is irreducible (see Lemma 2.7, and Remark 3.17), and has leading coefficient not divisible by p.
By Lemma 3.16 (see the proof), M gives rise to a finite τ-stable Galois extension of $E(a)_\tau$, so we may replace σ by τ.

Step 2. We may assume that for any $N > 1$, the extensions M and $E(a^{1/N})_\sigma$ are linearly disjoint over $E(a)_\sigma$.
It suffices to take m sufficiently large, and replace a by $a^{1/m}$.

We want to show that M is not proper, i.e., that $M = E(a)_\sigma$. We assume this is not the case, and define an action of σ on $\mathbb{Q}^n$ and on $\mathbb{R}^n$ by $\sigma(\gamma) = A\gamma$ where

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -d_0/d_n & -d_1/d_n & -d_2/d_n & \dots & -d_{n-1}/d_n \end{pmatrix}$$

Then $f(T) = \sum_{i=0}^n d_i T^i$ is the characteristic polynomial of A. Since $\mathrm{evSU}(B) = 1$, $f(T)$ is irreducible over $\mathbb{Q}$ (see 2.6). Also, the characteristic polynomial of A^m for any $m \geq 1$ is irreducible over $\mathbb{Q}$: otherwise, the σ^m-closure $B(m)$ of B would contain some definable infinite subgroup of infinite index, and therefore we would have $\mathrm{SU}(B(m)) > 1$. Then $\mathrm{evSU}(B) = \mathrm{evSU}(a/E) = 1$ would imply that $\mathrm{tr.deg}(E(a)_{\sigma^m}/E) < n$, which contradicts our assumption. Hence $\mathbb{Q}^n$ has no proper σ^m-stable subspace for any $m \geq 1$. Moreover, by modularity of B, $f(T)$ is relatively prime to all polynomials of the form $T^m - p^\ell$ where $m \geq 1$, $\ell \in \mathbb{Z}$ (2.6).

Observe also that if v is a valuation on $E(a)_\sigma$ which is trivial on E and such that $\gamma = (v(a), \dots, v(\sigma^{n-1}(a)))^T \in \mathbb{R}^n$, and if $\ell \in \mathbb{Z}$, then $A^\ell\gamma = (v(\sigma^\ell(a)), \dots, v(\sigma^{\ell+n-1}(a)))^T$.

Step 3. We may assume that conjugation by σ induces the identity on $\mathcal{G}al(M/E(a)_\sigma)$.
There is some ℓ such that σ^ℓ commutes with the elements of $\mathcal{G}al(M/E(a)_\sigma)$. The divisible hull (in $\mathbb{G}_m(\Omega)$) of the multiplicative subgroup generated by the elements $\sigma^i(a)$, $i \in \mathbb{Z}$, is isomorphic to $\mathbb{Q}^n$, and σ acts on it in the obvious manner, sending $\sigma^i(a)$ to $\sigma^{i+1}(a)$. Since $\mathbb{Q}^n$ has no

proper σ^ℓ-stable $\mathbb{Q}$-subspace, this implies that $\sigma(a), \dots, \sigma^{n-1}(a)$ belong to the divisible hull of the subgroup of $G(\Omega)$ generated by $a, \sigma^\ell(a), \dots, \sigma^{\ell(n-1)}(a)$; hence, for some $N \geq 1$ they belong to the group generated by $a^{1/N}, \sigma^\ell(a^{1/N}), \dots, \sigma^{\ell(n-1)}(a^{1/N})$. We replace a by $a^{1/N}$, and σ by σ^ℓ. If $char(\Omega) = p > 0$, we need to check that the separability assumptions made in Step 1 are still verified: it is obvious when $n = 1$, and follows from Lemma 2.7(3) when $n > 1$.

Step 4. We may assume that $M = LE(a)_\sigma$, where L is finite Galois over $E(a, \dots, \sigma^{n-1}(a))$, linearly disjoint from $E(a)_\sigma$ over $E(a, \dots, \sigma^{n-1}(a))$, and satisfies $L(\sigma^n(a)) = \sigma(L)(a)$.
By Lemma 3.15, there is some $m \geq n$ such that the desired conclusion holds with m replacing n. Note that $\sigma^n(a) \in E(a^{1/d_n}, \dots, \sigma^{n-1}(a)^{1/d_n})$. Let $N = d_n^{m-n}$: the assumption that $M \cap E(a^{1/N})_\sigma = E(a)_\sigma$ implies that by replacing a by $a^{1/N}$ and L by $L(a^{1/N}, \dots, \sigma^{n-1}(a^{1/N}))$, we obtain the desired conclusion.

Step 5. If e is the prime-to-p divisor of $[L : E(a, \dots, \sigma^{n-1}(a))]$, then we may assume that L is defined over $E(a^e, \dots, \sigma^{n-1}(a^e))$, i.e., that $L = L'(a, \dots, \sigma^{n-1}(a))$ for some finite Galois extension L' of $E(a^e, \dots, \sigma^{n-1}(a^e))$, with $L'E(a^e)_\sigma$ finite σ-stable over $E(a^e)_\sigma$, and L' linearly disjoint from $E(a)_\sigma$ over $E(a^e)$.
We just replace a by $a^{1/e}$, and L by $L(a^{1/e}, \dots, \sigma^{n-1}(a^{1/e}))$.

Step 6. Consider the set $\mathcal{V}$ of E-valuations v on $E(a, \dots, \sigma^{n-1}(a))$ such that $v(a) = \gamma_0, \dots, v(\sigma^{n-1}(a)) = \gamma_{n-1}$ are $\mathbb{Q}$-linearly independent, and v ramifies in L. Then $\mathcal{V}$ is non-empty.
We identify the tuple $(a, \dots, \sigma^{n-1}(a))$ with a generic point $(x_0, \dots, x_{n-1})$ of $(\mathbb{P}^1)^n$. It is known that $\mathbb{P}^1$ has no *unramified cover*, i.e, that if $f : V \to \mathbb{P}^1$ is finite, then f is ramified. Hence, if W is the normalisation of $(\mathbb{P}^1)^n$ in L, then the associated map $f : W \to (\mathbb{P}^1)^n$ is ramified. Let $\mathcal{S}$ be its ramification locus, S an irreducible component of $\mathcal{S}$. Then by 3.12 and 3.10, S does not intersect $\mathbb{G}_m^n$ and is of codimension 1. It follows that S is of the form $x_i = 0$ or $x_i = \infty$ for some i. Fix such S and i, let v_S be the associated valuation. Let Δ be an ordered abelian group generated by elements $\gamma_0, \dots, \gamma_{n-1}$ which are $\mathbb{Q}$-linearly independent, and consider $\mathbb{Z} \oplus \Delta$ with the lexicographical ordering. Define a valuation v on $E(a, \sigma(a), \dots, \sigma^{n-1}(a))$ by setting $v(\sigma^j(a)) = (0, \gamma_j)$ if $j \neq i$, and $v(\sigma^i(a)) = (v_S(\sigma^i(a)), 0)$. Because the values of $a, \sigma(a), \dots, \sigma^{n-1}(a)$ are $\mathbb{Q}$-linearly independent, this defines v uniquely, and v ramifies in L.

Step 7. If $char(E) = 0$, then $M = E(a)_\sigma$.
Because the characteristic is 0, all valuations are defectless. We use the notation of step 5, and fix some $v \in \mathcal{V}$. Then L' is defined over $E(a^e, \dots, \sigma^{n-1}(a^e))$, is linearly disjoint from $E(a, \dots, \sigma^{n-1}(a))$ over K, and $L'E(a, \dots, \sigma^{n-1}(a)) = L$. The number e of Step 5 equals $[L : E(a, \dots, \sigma^{n-1}(a))]$, and L' is defined over $E(a^e, \dots, \sigma^{n-1}(a^e))$. So $e(L'/E(a^e, \dots, \sigma^{n-1}(a^e)))$ divides e; moreover, $e\Gamma(E(a, \dots, \sigma^{n-1}(a))) = \Gamma(E(a^e, \dots, \sigma^{n-1}(a^e)))$. So if $v \in \mathcal{V}$, then v does not ramify in L by Lemma 3.3(6) (applied to $(K, L, M) = (E(a^e, \dots, \sigma^{n-1}(a^e)), L', E(a, \dots, \sigma^{n-1}(a)))$), and this contradicts step 5, unless $L = E(a, \sigma(a), \dots, \sigma^{n-1}(a))$ and $M = E(a)_\sigma$.

For the rest of the proof, we assume that the characteristic is $p > 0$.

Step 8. The set of valuations $v \in \mathcal{V}$ with value group contained in $\mathbb{R}$ is non-empty.
Let us write $\bar{a} = (a, \dots, \sigma^{n-1}(a))$. Extend the valuation v of Step 6 to a valuation on some algebraically closed field K containing $E(\bar{a})$, and let $u \in L$ be such that $v(u) = \sum_{j=0}^{n-1} m_j v(\sigma^j(a)) \notin$

$\Gamma(E(\bar{a}))$ (the m_j's are in $\mathbb{Q}$); let $P(\bar{a}, T) \in E[\bar{a}, T]$ the minimal polynomial of u over $E(\bar{a})$. Then, in the valued field (K, v), $tp(\bar{a}/E) \vdash \exists y\, P(\bar{x}, y) = 0 \wedge v(y) = \sum_j m_j v(x_j)$.

By elimination of quantifiers of the theory of algebraically closed fields, and because the elements of $v(\bar{a})$ are $\mathbb{Q}$-linearly independent (see the discussion in 3.18), there is a formula $\psi(\bar{\xi})$ satisfied by the n-tuple $v(\bar{a})$, which is a conjunction of formulas of the form $\sum_{j=0}^{n-1} \ell_j \xi_j > 0$ ($\ell_j \in \mathbb{Z}$), and such that whenever $\bar{b} = (b_1, \dots, b_n)$ is any n-tuple in (K, v), such that $v(\bar{b})$ satisfies ψ and belongs to $\mathcal{R}$ (the set of n-tuples of real numbers which are $\mathbb{Q}$-linearly independent), then some root β of $P(\bar{b}, T) = 0$ has valuation $\sum_j m_j v(b_j)$, so that $v(\beta) \notin \langle v(\bar{b}) \rangle$. Choose some n-tuple $\delta = (\delta_1, \dots, \delta_n) \in \mathcal{R}$ satisfying ψ, and define the E-valuation v_δ on $E(\bar{a})$ by setting $v_\delta(\sigma^j(a)) = \delta_{j+1}$. Then some conjugate u' of u satisfies $v(u') = \sum_j m_j \delta_{j+1} \notin \langle \delta \rangle = v_\delta(E(\bar{a}))$. So, v_δ belongs to $\mathcal{V}$ and has value group contained in $\mathbb{R}$.

Step 9. Definition of $S \subset \mathcal{R}$.
Let $\gamma \in \mathcal{R}$, and define v_γ on $E(\bar{a})$ as in the previous step. We let S be the set of $\gamma \in \mathcal{R}$ such that the valuation v_γ on $E(\bar{a})$ ramifies in L.

Step 10. If $\gamma \in \mathcal{R}$, then there is an open ball B' containing γ and such that $B' \cap \mathcal{R} \subset S$ if $\gamma \in S$, and $B' \cap S = \emptyset$ if $\gamma \notin S$.
Observe that because the residue field of $(E(\bar{a}), v_\gamma)$ is algebraically closed, if the valuation v_γ does not ramify in L, then the extension $L/E(\bar{a})$ is immediate.
If $\gamma \in S$, then the reasoning made in Step 8 gives us a ball B' containing γ and such that if $\delta = (\delta_1, \dots, \delta_n) \in B' \cap \mathcal{R}$ and $\bar{b} = (b_1, \dots, b_n)$ with $v(b_i) = \delta_i$ for $i = 1, \dots, n$, then some root β of $P(\bar{b}, T) = 0$ satisfies $v(\beta) \notin \langle \delta \rangle$, so that $E(\bar{b}, \beta)$ is a ramified extension of $E(\bar{b})$ since $\Gamma(E(\bar{b})) = \langle \delta \rangle$.
If $\gamma \notin S$, then $L \subset E((t^\Gamma))$ and Lemma 3.20 gives us the result.

Step 11. $\sigma(S) \subseteq S$.
Let $\gamma \in S$, and fix an extension v of v_γ to $L(\sigma(\bar{a}))$. Then the isomorphism σ^{-1} sends $(E(\sigma(\bar{a})), v)$ to $(E(\bar{a}), v_{\sigma(\gamma)})$, and therefore it suffices to show that the restriction of v to $\sigma(L)$ ramifies over $E(\sigma(\bar{a}))$.
Observe that by step 5, and because e is the prime to p divisor of $[L : E(\bar{a})]$, the index of ramification of v_γ in L is a power of p (see Lemma 3.3(6) and the discussion in Step 7). Moreover, since the residue field of v_γ is algebraically closed, we have $r(L/E(\bar{a})) = e(L/E(\bar{a}))$.
We also know that $L\sigma(\bar{a}) = \sigma(L)(\bar{a})$, and that L and $E(\bar{a}, \sigma(\bar{a}))$ are linearly disjoint over $E(\bar{a})$, $\sigma(L)$ and $E(\bar{a}, \sigma(\bar{a}))$ are linearly disjoint over $E(\sigma(\bar{a}))$. If $\Gamma = \langle \gamma \rangle \otimes \mathbb{Z}[1/d_n]$ (viewed as a subgroup of $\mathbb{R}$), then $v(E(\bar{a}, \sigma(\bar{a}))) \subset \Gamma$, but $v(L) \not\subset \Gamma$ because p does not divide d_n. If $\sigma(L)/E(\sigma(\bar{a}))$ is not ramified for the valuation v, then it is immediate, with value group contained in Γ. As $E(\bar{a}, \sigma(\bar{a}))$ is a totally ramified extension of $E(\sigma(\bar{a}))$, it follows that the value group of $\sigma(L)(\bar{a})$ is contained in Γ (see Lemma 3.3). This contradicts $\sigma(L)(\bar{a}) = L(\sigma(\bar{a}))$.

Step 12. Choosing an E-embedding of $L(\sigma^i(a) \mid i \geq 0)$ into $E((t^{\mathbb{R}}))$ endowed with its natural valuation (see 3.19).
Observe that if $\gamma \in S$, and $r \in \mathbb{R}^{>0}$, then $r\gamma \in S$, because the valuations v_γ and $v_{r\gamma}$ are equivalent. If $n > 1$, by steps 10 and 11, the conclusion of Lemma 3.21 holds. Hence there is some $\gamma \in S$ such that if B' is any open ball containing γ, then there are infinitely many $k \in \mathbb{N}$

such that $\frac{\|\gamma\|}{\|\sigma^k(\gamma)\|}\sigma^k(\gamma) \in B'$.

Fix such a $\gamma = (\gamma_0, \dots, \gamma_{n-1})$. For $i = 0, \dots, n-1$, we identify $\sigma^i(a)$ with t^{γ_i}. By induction, using the fact that for $m > 0$, the equation $\prod_{i=0}^n \sigma^{i+m}(a_i^{d_i}) = 1$ determines $\sigma^{n+m}(a)$ up to possibly multiplication by a d_n-th root of 1, and using the fact that a is a generic of the connected group B, it follows that we may identify $\sigma^i(a)$ with t^{γ_i} for all $i \geq 0$, with $\gamma_i = v(\sigma^i(a))$. This defines an E-embedding of $E(\sigma^i(a) \mid i \geq 0)$ into $E((t^{\mathbb{R}}))$, which extends to L. We therefore view $L(\sigma^i(a) \mid i \geq 0)$ as a valued subfield of $E((t^{\mathbb{R}}))$, the value group of $E(\sigma^i(a) \mid i \geq 0)$ being contained in $\Gamma = \langle\gamma\rangle \otimes \mathbb{Z}[1/d_n]$.

Step 13. The final contradiction.

Recall that by step 5, the index of ramification of $v_{|E(\bar{a})} = v_\gamma$ in L is a power of p. Moreover, because E is algebraically closed and $(E(\bar{a}), v_\gamma)$ is defectless (by 3.2(3)), it follows that (L, v) is obtained by taking first an immediate extension of $E(\bar{a})$ (namely, $L \cap E((t^\Gamma))$ by 3.6), followed by a tower of Artin-Schreier extensions. Hence there is $c \in L$ such that $c^p - c = \alpha \in E((t^\Gamma))$, and the restriction of v to $E(\bar{a}, c)$ ramifies over $E(\bar{a})$ (but its restriction to $E(\bar{a}, \alpha)$ does not).

By Proposition 3.6 applied to Γ, $\alpha_{|0}$ is a polynomial in $\bar{a}, \bar{a}^{-1}$, and we may assume (by 3.5) that $\alpha_{|0} = \sum_{\nu\in J} c_\nu \bar{a}^\nu$, where ν ranges over a finite subset J of $(\mathbb{Z} \setminus p\mathbb{Z})^n$, and the c_ν are in E. Let $P(\bar{a}, T)$ be the minimal polynomial of α over $E(\bar{a})$. We now use Lemma 3.20: there is an open ball B' containing γ such that whenever $\delta \in B'$ and $\bar{b} = (t^{\delta_1}, \dots, t^{\delta_n})$, then $P(\bar{b}, T)$ has a root β generating an immediate extension of $E(\bar{b})$ and such that $\beta_{|0} = \sum_J c_\nu \bar{b}^\nu$, with $v(\bar{b}^\nu) < 0$ for each $\nu \in J$. Moreover, by Lemma 3.20, these properties of $\bar{b}$ are implied by some $\mathcal{L}_{\rm val}(E)$-formula θ satisfied by $\bar{a}$, namely, $v(\bar{x}) \in B'$.

Let $k \in \mathbb{N}$ be such that $\frac{\|\gamma\|}{\|\sigma^k(\gamma)\|}\sigma^k(\gamma) \in B'$. Then $(E(\bar{a}), v_{\sigma^k(\gamma)}) \models \theta(\bar{a})$: here we use the fact that v_γ and $v_{r\gamma}$ are equivalent, for any $r \in \mathbb{R}^{>0}$. We saw that σ^k defines an isomorphism of valued fields between $(E(\bar{a}), v_{\sigma^k(\gamma)})$ and $(E(\sigma^k(\bar{a})), v)$. Hence $(E(\sigma^k(\bar{a})), v) \models \theta^k(\sigma^k(\bar{a}))$, where θ^k is obtained from θ by applying σ^k to the parameters from E. We let α_k be a root of $P^{\sigma^k}(\sigma^k(\bar{a}), T)$ satisfying $v(b_k - \sum_{\nu\in J} \sigma^k(c_\nu \bar{a}^\nu)) > 0$, and c_k a solution of $T^p - T = \alpha_k$.

We let I be the set of positive integers k such that $\frac{\|\gamma\|}{\|\sigma^k(\gamma)\|}\sigma^k(\gamma) \in B'$, an infinite set by our choice of γ in Step 12. We will shrink I successively using Ramsey's theorem.

Each α_k is a field conjugate of $\sigma^k(\alpha)$, and it therefore follows (by Ramsey's theorem) that there is an infinite subset I_1 of I such that if $k < \ell$ are in I_1 then $\sigma^{\ell-k}(\alpha_k) = \alpha_\ell$. By Step 3, every field between $E(a)_\sigma$ and M is a difference subfield. By Step 4 and Lemma 3.15 (the moreover part), we obtain that $E(\sigma^k(\bar{a}), \dots, \sigma^\ell(\bar{a}))(\alpha_k) = E(\sigma^k(\bar{a}), \dots, \sigma^\ell(\bar{a}))(\alpha_\ell)$. Hence $E(\sigma^k(\bar{a}), \dots, \sigma^\ell(\bar{a}))(c_k)$ contains $\sigma^{\ell-k}(c_k)$, which is a root of $T^p - T = \alpha_\ell$, and therefore $E(\sigma^k(\bar{a}), \dots, \sigma^\ell(\bar{a}))(c_k) = E(\sigma^k(\bar{a}), \dots, \sigma^\ell(\bar{a}))(c_\ell)$. The theory of Artin-Schreier extensions tells us that there is a non-zero $c(k, \ell) \in \mathbb{F}_p$ and $g \in E(\sigma^k(\bar{a}), \dots, \sigma^\ell(\bar{a}))(\alpha_k)$ such that $\alpha_k - c(k, \ell)\alpha_\ell = g^p - g$. We will now use Lemma 3.5.

Let $D = \{\nu \cdot \gamma \mid \nu \in J\}$ (= $\mathrm{Supp}(\alpha) \cap (-\infty, 0)$; we use the inner product notation $\nu \cdot \gamma$ for $\sum_{i=0}^{n-1} \nu_i\gamma_i$). Then $\mathrm{Supp}(\alpha_k) \cap (-\infty, 0) = \sigma^k(D)$, no element of $\sigma^k(D)$ is divisible by p in $\sigma^k(\Gamma)$, and similarly for $\mathrm{Supp}(\alpha_\ell) \subset \sigma^\ell(\Gamma) \subseteq \sigma^k(\Gamma)$. Recall that the elements of γ form a basis of the free $\mathbb{Z}[1/d_n]$-module Γ, so that each element of D corresponds to a unique tuple $\nu \in J$. By Lemma 3.5(2), there is a (unique) permutation $f_{k,\ell}$ of J such that for all $\nu \in J$, $f_{k,\ell}(\nu) \cdot \sigma^\ell(\gamma)/\nu \cdot \sigma^k(\gamma)$ is a power of p. By Ramsey's theorem, there is an infinite subset I_2 of I_1 such that if $k < \ell$ are in I_2, then $f_{k,\ell} = id$. Fix $\nu = (\nu_0, \dots, \nu_{n-1}) \in J$, $k < \ell$ in I_2. As above, using the freeness of Γ, the existence of $m \in \mathbb{Z}$ such that $\nu \cdot \sigma^k(\gamma) = p^m \nu \cdot \sigma^\ell(\gamma)$ translates into the following: if $u = (\nu_0, \dots, \nu_{n-1})$, then $uA^k = p^m uA^\ell$. So, $A^{k-\ell}$ has an eigenvalue which is a power of p. This contradicts our assumption on B' (see 2.6), and finishes the proof.

Theorem 4.4. *Let Ω be a model of ACFA, let G be a semi-abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, and let B be a definable modular subgroup of $G(\Omega)$ defined over E. Then the following statements hold.*

(1) *B is stable and stably embedded.*

(2) *Every definable subset of B^n is a Boolean combination of translates of definable subgroups of B^n. The definable subgroups of B^n are defined over E.*

(3) *If $a \in B$ and $F = \mathrm{acl}_\sigma(F)$ contains E, and L is a finite separable σ-stable extension of $F(a)_\sigma$, then L is contained in $F(b)_\sigma$ for some $b \in G(\Omega)$ and N with $[N]b = a$.*

Proof. Replacing B by $p_r(B)$ if necessary (see 2.1 for the definition), we will assume that if $a \in B$, then $\sigma(a) \in E(a)^{alg}$. Hence, for every $m \geq 1$, $\mathrm{tr.deg}(E(a)_\sigma/E) = \mathrm{tr.deg}(E(a)_{\sigma^m}/E)$. For $m \geq 1$, we let $B(m)$ be the σ^m-closure of B. Then $B(m)$ is also modular (see 1.6). Note also that by lemma 3.16, if a satisfies (3) in some reduct $(\mathcal{U}, \sigma^m)$, then it will satisfy it in every reduct $(\mathcal{U}, \sigma^m)$. By 2.1, the connected component B^0 of B (for the σ-topology) has finite index in B, say m, and therefore $[m]B \subseteq B^0$. By Lemma 3.13, if $a \in B$, then $[E(a)_\sigma : E([m]a)]_\sigma$ is finite, and therefore proving the equivalence of (1) – (3) for $[m]a$ will give the result. We may therefore always assume that our definable subgroups B and $B(\ell)$ are quantifier-free definable and connected. Let us start with some easy remarks.

Step 1: (1) implies (2).
B with the induced structure is stable and modular, whence weakly normal by [12]. In particular every definable subset of B^n is a Boolean combination of translates of definable subgroups of B^n.

Step 2: (3) implies (1).
Let $a \in B$, and $E \subset F = \mathrm{acl}_\sigma(F) \subset K = \mathrm{acl}_\sigma(K)$, and assume that $F(a)_\sigma$ and K are independent over F. By (3), we know that all finite separable σ-stable extensions of $K(a)_\sigma$ are contained in $\mathrm{acl}_\sigma(Ea)K \subseteq \mathrm{acl}_\sigma(Fa)K$. Assume that L is a finite separable σ-stable extension of $\mathrm{acl}_\sigma(Fa)K$. By Lemma 3.14, there is some K_1 independent from $K(a)_\sigma$ over F and such that $L \subset \mathrm{acl}_\sigma(K_1 a)M$ for some finite separable σ-stable extension M of $KK_1(a)_\sigma$. By (3), we get $M \subset \mathrm{acl}_\sigma(Fa)\mathrm{acl}_\sigma(KK_1)$, therefore $L \subset \mathrm{acl}_\sigma(Fa)\mathrm{acl}_\sigma(KK_1) \cap \mathrm{acl}_\sigma(Ka) = \mathrm{acl}_\sigma(Fa)K$ (Because K_1 is independent from $\mathrm{acl}_\sigma(Ka)$ over F; see e.g. Remark 1.9(2) in [2] applied to $A = \mathrm{acl}_\sigma(Fa)$, $B = K$ and $C = K_1$). By Lemma 1.5 (applied to $K\mathrm{acl}_\sigma(Fa)$), $tp(a/F) \cup qftp(a/K)$ is complete, which shows that $tp(a/F)$ is stationary. Hence every type over an algebraically closed set which

is realised in B is stationary. The result follows by 1.8. Moreover, by Lemma 3.16, we obtain that all $B(m)$ are stable and stably embedded.

Step 3: (1) for all $B(\ell)$ implies (3).
Let $F = \mathrm{acl}_\sigma(F)$ contain E, and let $a \in B$. Let C be the σ-closed connected subgroup of B such that a is a generic of the coset $a + C$ over F. Let a_1 be a generic of $a + C$ which is independent from a over F. Then $tp(a/Fa_1)$ is completely determined by the class of $(a - a_1)$ in C/C^*, where $C^* = \bigcap_{m\geq 1}[m]C$. This comes from the fact that $tp(a/Fa_1)$ is uniquely determined by the set of cosets of definable subgroups D of C which are defined over $F(a_1)_\sigma$ and which contain $(a - a_1)$; as $(a - a_1)$ is a generic of C over $F(a_1)_\sigma$, these subgroups D must have finite index in C, and therefore contain $[m]C$ for some positive integer m. For each $m > 1$ choose $b_m \in G$ such that $[m]b_m = a - a_1$, and let $F_1 = \mathrm{acl}_\sigma(Fa_1)$. Then $tp(a/F_1)$ is completely determined by $qftp(a, b_2, \dots, b_m, \dots /F_1)$. Similarly, for every $\ell \geq 1$, $tp(a/F_1)[\ell]$ is completely determined by $qftp(a, b_2, \dots, b_m, \dots /F_1)[\ell]$. That is (see 1.5), the field $F_1(a, b_2, \dots)_\sigma$ has no finite proper separable σ-stable extension.

Let L be a finite separable σ-stable extension of $F(a)_\sigma$. Then $LF_1(a, b_2, \dots)_\sigma$ is a finite σ-stable extension of $F_1(a, b_2, \dots)_\sigma$, so that $L \subset F_1(b_m)_\sigma$ for some m.

Note that F_1 contains a root of $[m]x = a_1$. Hence $F_1(b_m)_\sigma = F_1(c_m)_\sigma$ where $[m]c_m = a$, and $L \subset F_1(c_m)_\sigma$. As a_1 was independent from a over F, we have $F_1(c_m)_\sigma \cap \mathrm{acl}_\sigma(Fa) = F(c_m)_\sigma$, so that $L \subset F(c_m)_\sigma$.

It therefore suffices to show (3) or to show (1) for all ℓ.

Step 4. Case where B has evSU-rank 1.
Assume that B has evSU-rank 1.
If G is an abelian variety, then Proposition 4.1 gives (3).

Assume now that G is not abelian, but has an abelian quotient A (via a morphism π) such that $\pi(B)$ is infinite; then the restriction of π to B has finite kernel, and by the previous case, we obtain that $\pi(B)(\ell)$ is stable and stably embedded for every $\ell > 0$. As $\mathrm{Ker}\,(\pi) \cap B$ is finite, Proposition 1.9 gives that $B(\ell)$ is stable and stably embedded for every $\ell > 0$, and therefore gives also (3) and (2). This show (1) and (3) in the "abelian case".
Assume now that the Zariski closure of B is contained in some toric subvariety of G. Recall that $\sigma(a) \in E(a)^{alg}$. Without loss of generality, $G = \mathbb{G}_m^r$ for some r. Let $a_1 \in \mathbb{G}_m$ be an element of the tuple a which does not belong to E. Then $\mathrm{tr.deg}(E(a_1)_\sigma/E) = \mathrm{tr.deg}(E(a)_\sigma/E)$ (because $\mathrm{evSU}(a/E) = 1$), and as above, the projection π of $\mathbb{G}_m^r$ on the corresponding copy of $\mathbb{G}_m$ restricts to a morphism on B with finite kernel. Applying Proposition 4.3 to a_1 shows that if L is a finite σ-stable extension of $F(a_1)_\sigma$, then $L \subset F(a_1^{1/N})_\sigma$ for some integer N. Hence, $\pi(B)(\ell)$ is stable and stably embedded for every $\ell > 0$, and so is $B(\ell)$. This finishes the proof when $\mathrm{evSU}(B) = 1$.

Step 5. The general case.
Let a be a generic of B over E, and $n = \mathrm{tr.deg}(E(a)_\sigma/E)$. Recall that if $a \in B$, then $\sigma(a) \in E(a)^{alg}$. Let m be large enough so that $\mathrm{SU}(a/E)[m] = \mathrm{evSU}(a/E) = k$, and replace B by

$B(m)$ (or by its connected component, but we will keep the notation $B(m)$). We now work in (Ω, σ^m). Using the modularity of $B(m)$, there is a sequence $(0) = B_0 \subset B_1 \subset \cdots \subset B_k = B(m)$ of subgroups of $B(m)$, with $[B_i : B_{i-1}] = \infty$ for $i = 1, \ldots, k$: take a sequence $F_{k-1} \subset \cdots \subset F_1$ of difference subfields of $\Omega[m]$ such that $SU(a/F_i)[m] = i$. Then for each i, a is the generic of a coset of a σ^m-closed subgroup B_i of G of $SU[m]$-rank i, by Theorem 1.7. If $C_i = B_i/B_{i-1}$, then $\mathrm{evSU}(C_i) = 1$ for $i = 1, \ldots, k$. We will now show that each C_i "lives" in a semi-abelian variety, so that it satisfies (3) by the previous steps. Let π be a morphism (of algebraic groups) from the Zariski closure of B_i (inside $G(\Omega)$) onto some simple semi-abelian variety H, such that $[\pi(B_i) : \pi(B_{i-1})]$ is infinite. Let $f(\sigma) \in \mathrm{End}_\sigma(H)$ be such that $\pi(B_{i-1})$ is commensurable to $\mathrm{Ker}\,(f(\sigma))$; multiplying f by an integer, we may assume $\pi(B_{i-1})$ is contained in $\mathrm{Ker}\,(f(\sigma))$; then $f(\sigma) \circ \pi(B_i)$ is an infinite subgroup of $H(\Omega)$, because $\mathrm{Ker}\,(f(\sigma))$ has infinite index in $\pi(B_i)$, and the induced map $C_i \to H(\Omega)$ has finite kernel. Hence, by Step 4 and 1.9, each C_i is stable and stably embedded, and by 1.9, this implies that $B(m)$ is stable and stably embedded. The same reasoning shows that all $B(m\ell)$ are stable and stably embedded; using Step 3 and Lemma 3.16, $B(m)$ and B satisfy (3), and therefore also (1) and (2). This finishes the proof.

4.5. Some remarks about $B/[n]B$. Let A be a semi-abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, and let $B \subset A(\Omega)$ be a definable modular subgroup of $A(\Omega)$, n an integer bigger than 1. The induced structure of the definable group B is largely determined by the finite index subgroups $[n]B$. For instance if $[n]B = B$ for all $n > 0$, then B is strongly minimal and the induced structure reduces to a module structure (cf. [11]). However this only occurs in the rare event that B is torsion-free; it will usually have infinite torsion. One thus wants to understand the finite imaginary sort $B/[n]B$ in terms of a similar quotient for the ambient algebraic group A. In what follows, we will assume that B is a quantifier-free definable subgroup of $A(\Omega)$, of finite SU-rank.
Since Ω is elementarily equivalent to an ultraproduct of difference fields $(\mathbb{F}_p^{alg}, \mathrm{Frob}_q)$ (see [10]), we know that $[B : [n]B] = |B \cap A[n]|$: the group B is elementarily equivalent to an ultraproduct of finite groups, and one considers the endomorphism $x \mapsto [n]x$. We will be able to give a precise description of $B/[n]B$ in two cases: when $B = \mathrm{Ker}\,(f)$ for some $f \in \mathrm{End}_\sigma(A)$; and when B is connected (for the σ-topology). Any definable group of finite SU-rank B is isomorphic (via a map p_N) to a finite index subgroup of some B' of the first type, and contains a finite index subgroup B'' of the second type, so our description is rather complete.

Proposition 4.6. *Let A be a semi-abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, and let $B \subset A(\Omega)$ be a quantifier-free definable subgroup of $A(\Omega)$ of finite SU-rank, $n > 1$ an integer.*

(1) *Assume that $B = \mathrm{Ker}\,(f)$ for some $f \in \mathrm{End}_\sigma(A)$. Then*
$$B/[n]B \simeq A[n]/f(A[n]).$$

(2) *Assume that $B = \tilde{B}^0$, let N be such that $B = \tilde{B}_{(N)}$, and consider the semi-abelian variety $D = B_{(N)}$. Take a definable homomorphism $F : D \to D'$, where D' is the quotient of the semi-abelian variety D^σ by some finite subgroup C_2, and the map F is*

of the form $f(p_N(x)) - g(\sigma(p_N(x))$ for some algebraic homomorphisms f, g, such that $B = \{b \in A(\Omega) \mid F(p_N(b)) = 0\}$. Then

$$B/[n]B \simeq D'[n]/F(D[n]).$$

Proof. (1) Let us first suppose that $B = \mathrm{Ker}\,(f)$. Consider $A[n]/f(A[n])$. Then $[A[n] : f(A[n])] = |\mathrm{Ker}\,(f) \cap A[n]| = |B \cap A[n]|$. Define

$$\varphi : B \to A[n]/f(A[n])$$

as follows: if $a \in B$ take $b \in A$ such that $[n]b = a$, and define $\varphi(a) = f(b) + f(A[n])$. Since distinct choices of b differ by an element of $A[n]$, this map is well-defined. One checks easily that it is a group homomorphism, and that its kernel is precisely $[n]B$, so that it defines an isomorphism between $B/[n]B$ and $A[n]/f(A[n])$.

(2) We will use the general description of quantifier-free definable subgroups given in 2.1, and follow its notation. Replacing $B = \tilde{B}^0$ by $p_N(B)$ for some N and A by $B_{(N)} = D$, we may assume that $B = \tilde{B}_{(1)}$, and that B is Zariski dense in the semi-abelian variety A (this is where we use that B has no quantifier-free definable subgroup of finite index: $B_{(N)}$ is connected). If we define C_1, C_2 by

$$C_1 \times \{0\} = B_{(1)} \cap (A \times \{0\}), \qquad \{0\} \times C_2 = B_{(1)} \cap (\{0\} \times A^\sigma),$$

the group $B_{(1)}/C_1 \times C_2$ is the graph of a (definable in ACF) group isomorphism

$$f : A/C_1 \to A^\sigma/C_2.$$

If $h_1 : A \to A/C_1$ and $h_2 : A^\sigma \to A^\sigma/C_2$ are the natural isogenies, $a \in B$ if and only if $fh_1(a) = h_2(\sigma(a))$.
Let $A' = A^\sigma/C_2$, let $F : A \to A'$ be defined by $F(x) = fh_1(x) - h_2(\sigma(x))$. Then $B = \mathrm{Ker}\,(F)$. Define $\varphi : B \to A'[n]/F(A[n])$ as follows: if $a \in B$, let $b \in A$ be such that $[n]b = a$, and set $\varphi(a) = F(b) + F(A[n])$. As A and A' are isogenous semi-abelian varieties, we know that $|A[n]| = |A'[n]|$, whence $[A'[n] : F(A[n])] = |\mathrm{Ker}\,(F) \cap A[n]| = |B \cap A[n]|$, and we get an isomorphism between $A'[n]/F(A[n])$ and $B/[n]B$.

4.7. Algebraic dynamics. We call *algebraic dynamic* a pair (V, ϕ) consisting of a (quasi-projective, irreducible) variety V, together with a dominant rational map $\phi : V \to V$. A map between algebraic dynamics (V, ϕ) and (W, ψ) is a dominant rational map $f : V \to W$ such that $f \circ \phi = \psi \circ f$. For $n > 0$, $\phi^{(n)}$ denotes $\phi \circ \phi \cdots \circ \phi$ (n times).

If (V, ϕ) is defined over the field E, then we put the structure of a (non-inversive) difference field on $E(V)$ by setting $\sigma(a) = \phi^*(a) = a \circ \phi$. Note that σ is the identity on E. A dominant rational map $f : (V, \phi) \to (W, \psi)$ (defined over E) then corresponds to an embedding of difference fields $f^* : E(W) \subset E(V)$.

Proposition 4.8. *Let G be a semi-abelian variety, defined over an algebraically closed field E. Let $\phi : G \to G$ be a dominant endomorphism, and assume that the set $\{x \in G(\Omega) \mid \sigma(x) = \phi(x)\}$ is one-based (in some existentially closed difference field Ω containing (E, id)). Let (W, ψ) be an algebraic dynamic, and $f : (W, \psi) \to (G, \phi)$ a finite separable map, everything being defined over E. Then there is a birational map $g : (W, \psi) \to (H, \rho)$, and an isogeny $h : (H, \rho) \to (G, \phi)$ such that $h \circ g = f$, where H is a semi-abelian variety, and ρ a dominant endomorphism of H.*

Proof. We work in the difference field Ω, a model of ACFA. We take $b \in W$, generic over E and satisfying $\sigma(b) = \psi(b)$, and let $a = f(b)$. Then $a \in G$, is generic over E and satisfies $\sigma(a) = \phi(a)$. Then $E(a) \subset E(b)$ are closed under σ, but not under σ^{-1}, unless ϕ and ψ are isomorphisms. Moreover, $E(b)$ is a finite separable extension of $E(a)$. Results on the limit degrees (equal to 1 in both cases), and the fact that b is algebraic over $E(a)$ imply that $E(b)_\sigma$ is a finite (separable) σ-stable extension of $E(a)_\sigma$ (see [4], Theorem 5.22.XVI).
Let $B \subset G(\Omega)$ be the subgroup defined by the difference equation $\sigma(x) = \phi(x)$. By Theorem 4.4, $E(b)_\sigma \subset E(a^{1/N})_\sigma$ for some integer $N > 0$. This implies that for some $n \geq 0$, $N > 0$, $E(b) \subset E(\sigma^{-n}(a^{1/N}))$. Note that $[N]\phi^n : G \to G$ is an isogeny, which sends $\sigma^{-n}(a^{1/N})$ to a. It factors as $h_1 \circ h_2$, where h_1 and h_2 are isogenies such that h_1 is separable, and (setting $c = h_2(\sigma^{-n}(a^{1/N})))$ $E(b) = E(c)$. Let $H = h_2(G)$, ρ the endomorphism of H such that $\sigma(c) \in E(c)$, and $h = h_1$.

Remarks 4.9. The hypotheses of Proposition 4.8 are not very friendly to non-logicians.
In the notation of the proof of 4.8, assume that B is not one-based. Then, there is a semi-abelian (simple) variety H, and an algebraic map $h : G \to H$, such that $h(B) = C \subseteq H(\tau)$, with $\tau = \sigma^m \mathrm{Frob}^n$ for some $m \geq 1$ and $n \in \mathbb{Z}$, and $h(C)$ infinite. If $\tau = \sigma^m$, then H and h can be taken defined over E; if $\tau = \sigma^m \mathrm{Frob}^n$ with $n \neq 0$, then H can be taken to be defined over some finite field, and h over E as before.

In the first case, as for m sufficiently large, σ^m commutes with all elements of $\mathrm{End}(G)$, it will follow that for some m, the map $\phi^{(m)} - id$ is not onto.

The second case is not as easy to describe. If G is simple and equals $\mathbb{G}_m$, then $\phi^{(m)} - \mathrm{Frob}^{-n}$ is not onto (and we get that $-n > 0$). Assume now that G is abelian simple, and let $h : G \to H$ be the isogeny given above, $h^* : H \to G$ its dual, and M the integer such that $hh^* = [M]$. Then for some m and n, we have that $M\phi^{(m)} - h^* \mathrm{Frob}^n h$ is not dominant.

The general case is harder to describe.

4.10. Problem. In positive characteristic, do there exist any stable definable subgroups of $\mathbb{G}_a$?

It is easy to show that in characteristic 0 there are none since any quantifier-free definable subgroup of $\mathbb{G}_a$ is defined by linear difference equations. See e.g. Theorem 5.12 in [2].

References

[1] S. Abhyankar, On the ramification of algebraic functions, Amer. J. of Math. Vol. 77 (1955), 575 – 592.

[2] Z. Chatzidakis, E. Hrushovski, Model theory of difference fields, Trans. Amer. Math. Soc. 351 (1999), pp. 2997-3071.

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

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

[5] F. Delon, Hensel fields in equal characteristic $p > 0$, in: *Model Theory of Algebra and Arithmetic, Proc. Karpacz 1979*, Lecture Notes in Mathematics Nr 834, Springer-Verlag Berlin Heidelberg 1980.

[6] Otto Endler, *Valuation Theory*, Springer-Verlag Berlin Heidelberg New York 1972.

[7] Antonio J. Engler, Alexander Prestel, *Valued fields*, Springer monographs in Mathematics, Berlin (2005).

[8] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics 52, Springer Verlag 1977.

[9] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, Ann. Pure Appl. Logic 112 (2001), no. 1, 43 – 115.

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

[11] E. Hrushovski, J. Loveys, Strongly and co-strongly minimal abelian structures, JSL, 75, 2, pp. 442 – 458.

[12] E. Hrushovski, A. Pillay, Weakly normal groups, in: *Logic Colloquium 85*, North Holland 1987, 233 – 244.

[13] E. Hrushovski, A. Pillay, Groups definable in local fields and pseudo-finite fields, Israel J. of Math. 85 (1994), 203 –262.

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

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

[16] Franz-Viktor Kuhlmann, Elimination of ramification I: The generalized stability theorem, Trans. AMS 362 (2011), Nr 11, 5697 – 5727.

[17] S. Lang, Unramified class field theory over function fields in several variables, Annals of Math., 2nd series, Vol. 64 No 2 (1956), 285 – 325.

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

[19] S. Lang, J.-P. Serre, Sur les revêtements non ramifiés des variétés algébriques (French), Amer. J. Math. 79 (1957), 319 – 330. Erratum in: Amer. J. Math. 81 (1959) 279 – 280.

[20] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series Nr 31, Princeton University Press, Princeton 1980.

[21] David Mumford, *The Red Book of Varieties and Schemes*, Springer Lect. Notes 1358, 2nd expanded ed., Springer-Verlag Berlin Heidelberg, 1999.

[22] A. Robinson, *Complete theories*, North-Holland, Amsterdam 1956.

[23] O.F.G. Schilling, *The theory of valuations*, AMS Mathematical Survey 4, New York 1950.

[24] I.R. Shafarevich, *Basic Algebraic Geometry 1*, 2nd ed., Springer Verlag 1994.

[25] V. Weispfenning, Quantifier elimination and decision procedures for valued fields. Models and sets (Aachen, 1983), Lecture Notes in Math., 1103, Springer, Berlin, 1984, 419 — 472.

Current addresses:

Département de Mathématiques et Applications (UMR 8553)
Ecole Normale Supérieure
45 rue d'Ulm
75230 Paris Cedex 05
France
e-mail: `zchatzid@dma.ens.fr`

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