ELSEVIER

Annals of Pure and Applied Logic 112 (2001) 43–115

ANNALS OF PURE AND APPLIED LOGIC

www.elsevier.com/locate/apal

The Manin–Mumford conjecture and the model theory of difference fields

Ehud Hrushovski [1]

Department of Mathematics, Hebrew University, Jerusalem, Israel

Received September 1995; accepted 17 April 2001

Communicated by A.J. Wilkie

Abstract

Using methods of geometric stability (sometimes generalized to finite S1 rank), we determine the structure of Abelian groups definable in ACFA, the model companion of fields with an automorphism. We also give general bounds on sets definable in ACFA. We show that these tools can be used to study torsion points on Abelian varieties; among other results, we deduce a fairly general case of a conjecture of Tate and Voloch on p-adic distances of torsion points from subvarieties.

MSC: 03C; 11G; 12H10

Keywords: Abelian varieties; Torsion points; Difference fields; Geometric stability; Model theory of difference equations

1. Introduction

This paper extends and specializes the general model theory of difference equations in characteristic 0, developed in [9]. We investigate the induced structure on definable Abelian groups of finite dimension. We also give general bounds on the number of solutions to a finite set of difference equations. As a corollary, we obtain a model-theoretic proof of the Manin–Mumford conjecture. The proof yields new number-theoretic information, particularly with respect to p-adic and algebraic uniformities of the bounds obtained.

1.1. The Manin–Mumford conjecture

The Manin–Mumford conjecture states that if C is a curve of genus two or more, embedded in its Jacobian J, then the set of torsion points on C is finite, see [18,

[1] The work was begun at MIT, with support from the NSF. The latter part was supported by the ISF.
E-mail address: ehud@math.huji.ac.il (E. Hrushovski).

0168-0072/01/$ - see front matter
PII: S0168-0072(01)00096-3

pp. 37–39; 27, p. 73]. This was proved by Raynaud. Indeed he proved (with K^a denoting the algebraic closure of a field K):

Theorem 1.1.1. *Let A be an Abelian variety, X a subvariety, over a number field K. Let $T(A)$ denote the group of torsion points of $A(K^a)$. Then there exist a finite number of suvarieties $c_i + A_i$ of X, all translates of group subvarieties A_i of A, such that $T(A) \cap X = \bigcup_i T(A_i) + c_i$.*

Subsequently, Hindry [11] found a version with an explicit bound on the finite number, and McQuillan generalized the theorem to semi-Abelian varieties (in a strong relative version, see Theorem 1.1.4 below). In the case of one-dimensional X (with some further restrictions) an effective proof was independently given by Buium [4]. Buium uses a new method, of p-jets, whose relation to ours is unclear and highly intriguing.

We will give another proof of these statements. All proofs deal first with the points of order relatively prime to a given prime p. The number theoretic proofs depend on the following idea: if K is a number field, p a fixed prime, then there exists a constant $c = c(K, A)$ such that for all prime-to-p torsion points t of A, ct and t are conjugate over K. Thus if X is defined over K, and $t \in X$ then also $ct \in X$ and this puts t into a smaller-dimensional variety, contained in $X \cap c^{-1}X$. From our point of view, this proof can be interpreted as intersecting X with solutions to the difference equation $\sigma(x) = cx$. Our proof will also use a difference equation, but a higher order one, of the form $\sum m_i \sigma^i(x) = 0$. We will obtain it from the characteristic equation of a Frobenius acting on the torsion points of A. To show that torsion points are solutions will be straightforward, and effective (by contrast to the deep study of the Galois representation required in the number theoretic approaches). To understand the intersection, however, both qualitatively and quantitatively, we will require the theory of difference equations.

Our proof does not use completeness, and applies directly to semi-Abelian varieties. With a little additional work (adding the model theoretic concept of orthogonality, to the local modularity used before), one obtains:

Theorem 1.1.2. *Theorem* 1.1.1 *is valid for arbitrary commutative algebraic groups.*

For example, let G be a nonsplit group extension of an elliptic curve E by the additive group G_a, and let X be any curve on the surface G. Then $X \cap T(G)$ is finite.

Effective bounds and uniformity: Fix a projective embedding of A, and hence of any subvariety X.

Theorem 1.1.3. *Let A be a commutative algebraic group, defined over some number field K. Let X be a subvariety, defined over K^a. Then there exist a finite number M of suvarieties $c_i + A_i$ of X, all translates of group subvarieties A_i of A, such that*

$$T(A) \cap X = \bigcup_i T(A_i) + c_i.$$

We have $M \leqslant c \deg(X)^e$, with c and e depending on A but not on X.

c and e can be (and are, in Section 5) written down explicitly; they are doubly exponential in some natural parameters associated with A.

Compare this to the bound in [11]. The bound there is given for X defined over a fixed number field K, and is not given uniformly in K. There is a constant, depending on K and A, whose existence follows from Serre's work on Galois representations, but was not known to be effective [18, p. 39; 29].

I learned from the referee report that the constant was later shown to be effective, as a corollary of "an alternative transcendence proof of the Tate and Shafarevich conjectures by Masser and Wüstholz [20], and subsequent work by Bost and David [1]."[2] At all events, the bounds given here are independent of this Galois theoretic data.

The bound we obtain can be written down more easily if one prime is excluded from the torsion. Let $ZCl(Y)$ denote the Zariski closure of Y.

Example 1.1.1. Let A be a connected, commutative algebraic group defined over a number field K. Let $\mathbf{p}$ be a prime of good reduction, with residue field $GF(q)$ of characteristic p. Let T_p' be the group of points of $A(K^a)$ of finite order prime to p. Let X be a subvariety of A. Then $ZCl(X \cap T_p')$ is a union of at most

$$(\deg(X)^{2d_r+1} d_+^{4d_r(2d_r+1)\log_2(1+q^{1/2})})^{2^{2d_r \dim(X)}}$$

cosets of group subvarieties of A, contained in X.

Here d_r is a certain dimension below $\dim(A)$, and d_+ is a degree associated to the graph of addition on A; they will be explained below. If $A = E^m$ for an elliptic curve E, then $d_r = 1$.

Remark 1.1.2. All the quantities in Example 1.1.1 are constant in algebraic families. Thus the bound remains uniform if A and X move in an algebraic family, so long as A remains defined and with good reduction over K_{p}. In particular, A may be moved in a p-adic neighborhood in moduli.

For the special case when X is a curve, or just contains no cosets of infinite group subvarieties, the bound obtained in the general case is similar to the restricted case (Example 1.1.1). In general, however, the bound and proof are more complicated (though still explicit, and of doubly exponential growth in the totality of parameters).

We also give a difference algebraic/model theoretic proof of McQuillan's theorem [21]:

Theorem 1.1.4. *Let A be a semi-Abelian variety over a number field K. Let X be a subvariety of A, and let $D = \{a \in A(K^a) : na \in A(K)$ for some $n\}$. There exists an integer m and group subvarieties A_i of A such that*

$$(D \cap X) = \bigcup_C (D \cap C).$$

[2] References and quote from the very useful referee report, for which I am grateful. The referee adds: "This might also be a good place to cite the important paper of Faltings [9], which underlay Serre's result."

The union is taken over a finite set of subvarieties $C \subseteq X$ of the form $A_i + c$, with $mc \in A(K)$. The integer m and the subvarieties A_i can be determined effectively.

Tate–Voloch conjecture. Tate and Voloch conjectured that the torsion points on an Abelian variety A over $\mathbb{C}_p$ that do not lie on a subvariety $V \subseteq A$, are bounded away from that variety. Certain special cases were proved by Tate–Voloch, and by Buium and Silverman. The proof of the Manin–Mumford conjecture given above lends itself immediately to a proof of the Tate–Voloch conjecture under much weaker restrictions: A must be assumed defined over a finite extension of $\mathbb{Q}_p$; must have good reduction; and the prime-to-p torsion points only are considered. We show this in Lemma 6.6.1.

Structure of the proof of Manin–Mumford: The proof moves from number theory through algebra to model theory; the main work is done there. The first step is to embed the group of torsion points into a group defined by difference equations. All the number theory used occurs here. Beyond this point we have a difference algebra setup, and we study it with model theoretic binoculars. Three levels of model theory are used.

(1) Quantifier elimination (to a certain level). Consider, for instance, the problem of showing that if two groups A and B satisfy the conclusion of Manin–Mumford, then so does $A \times B$. This involves considering projections to B of subvarieties $X \subseteq (A \times B)$, and their fibers. If A, B are taken to be groups of rational points, or torsion points, the projections are notoriously undecidable (Gödel). But if we take larger groups defined in a structure with quantifier elimination, then the projections are defined by similar formulas. This provides a reasonable context in which to carry out a proof.

(2) A dimension theory is developed to study the definable sets. We use S1-rank. This is much younger than Morley rank, and we need to develop the foundations to some extent (Section 3). The very existence of the dimension theory suffices for some purposes. For instance, by comparing dimensions, one sees that any definable group has finite index in one arising directly from an algebraic group (A finer argument can, in fact, completely give the structure of definable groups in terms of algebraic groups.) (cf. Remark 4.0.3).

(3) Model theory also permits second-order arguments; properties of the class of all definable sets are often more amenable to devissage, more functorial under interpretations, than of individual definable sets. A very simple example occurs in Proposition 3.4.1; see the remark following it. Another instance occurs in [5], and enters the present paper via the key Definition 4.1.2 (where a dichotomy is found between groups satisfying Manin–Mumford, and those embeddable into *the set of points of the fixed field* of an algebraic group). Within [5] one uses a relation, for arbitrary structures with a certain dimension theory, between Galois theory, amalgamation, and modularity (modularity is the abstract form of Manin–Mumford, or Mordell–Lang). This makes no sense for a single algebraic variety; it can be applied, roughly speaking, to an appropriate *class* of varieties, i.e. to a structure interpretable in (enriched) algebraic geometry.

The model theoretic part of the proof is very similar to that of the geometric Mordell–Lang conjecture in [14]; but the algebraic layer involves fields with automorphisms, rather than derivations, in order to be able to say something about number fields; as a consequence the relevant structures are not stable, leading to the use of a different dimension theory.

1.2. Difference algebra and model theory

A (k-fold) difference field is a field with distinguished automorphism $\sigma_1, \ldots, \sigma_k$. The deeper results of [5] are available only for $k = 1$. We will always assume $k = 1$ except where explicitly stated otherwise. We also restrict attention to characteristic zero throughout the paper. The (only) reason is that the deeper results of [5] are available only with this assumption. We expect entirely similar results concerning definable subgroups of semi-Abelian varieties in positive characteristic; for subgroups of vector groups new phenomena are encountered [5, Section 7].[3] The direct analogue of the Manin–Mumford conjecture is of course false for Abelian varieties defined over finite fields; once these are ruled out (in the appropriate sense), the result follows from [14].

The theory of difference fields of characteristic zero has a model companion; it plays the same role for difference fields as the algebraic closure does for a field. See [24] or [25] or [7] for this notion in general, and [5] for the case of difference fields (with a single autormorphism). We give a quick summary.

Definition 1.2.1. Let $(K, \sigma_1, \ldots, \sigma_k)$ be a difference field. K is *difference-closed* if K is algebraically closed, and the following condition holds:

Let X be an irreducible K-variety, X_i the variety obtained by conjugating by σ_i. Let Y be an irreducible subvariety of $X \times X_1 \times \cdots \times X_k$, projecting dominantly to each factor. Then there exists $a \in X(K)$ with $(a, \sigma_1(a), \ldots, \sigma_k(a)) \in Y$.

We will say that $(K, \sigma_1, \ldots, \sigma_k)$ is a *universal domain* if whenever K' is a relatively algebraically closed subfield, $\sigma(K') \subseteq K'$, K'' is a countable difference field, and $i : K' \to K''$ is an embedding of difference fields, then there exists an embedding $j : K'' \to K$ of difference fields, with $j \circ i = id_{K'}$. We will not use any nontrivial properties of universal domains; however it is easy to see that every (countable) difference field embeds into some universal domain. This amounts to saying that the class of algebraically closed difference fields has the amalgamation property; cf. [7].

Lemma 1.2.2. *Any universal domain is difference-closed.*

Proof. Let X, X_i be as in the definition of difference-closed. Let K' be a countable, σ_i-invariant, algebraically closed subfield of K, over which X is defined. Let $(a, a_1, \ldots, a_k)$ be a generic point of Y, over K'. Let K'' be an algebraically closed field extending $K'(a, a_1, \ldots, a_k)$, and of infinite transcendence degree over K'. It is easy to see that

[3] After these lines were written, major parts of [5] were generalized to positive characteristic in [6].

there exist automorphisms $\sigma_{i,K''}$ of K'' extending σ_i, and with $\sigma_{i,K''}(a) = a_i$. Let this determine a difference field structure on K''. Since K'' embeds into K over K', there exist also $(a, a_1, \ldots, a_k) \in Y(K)$ with $\sigma_i(a) = a_i$. □

In particular, every countable difference field embeds into a *difference-closed* difference field. In a difference-closed field, every set or relation definable by a first-order formula is definable by an existential formula, and moreover by one in which the quantifiers range only over a finite set, the set of roots of some polynomial; see [5] for a precise statement. This result follows from the form of the definition of a universal domain above, using standard model theory; see [7]. For the most part we will refer only to sets defined by *difference equations*. These are equations $f(X) = 0$, where $f(X)$ is a *difference polynomial*, i.e. a polynomial in the variables X^τ: $\tau \in \mathscr{F}_0$, with $\mathscr{F}_0$ the free semi-group generated by $\sigma_1, \ldots, \sigma_k$.

We observe that when $k > 1$ the automorphisms σ_i on a universal domain K do not commute. (One can obtain a universal domain for algebraically closed fields with k commuting automorphisms by taking within K the common fixed field L of the commutators $[\sigma_i, \sigma_j]$, and their conjugates. This infinitely definable pseudo-algebraically closed subfield of the universal domain for k noncommuting automorphisms is a substitute for a saturated model for the nonexistent model completion of the theory of k commuting automorphisms. It will play no role in our considerations.)

We now turn to the case $k = 1$. As in the case of fields, one has a correspondence between prime difference ideals in the difference ring of difference polynomials over K, in the variables $X = (X_1, \ldots, X_n)$, and between certain subsets of K^n, the zero sets of the ideals. But here, not every definable set is a Boolean combination of such "difference varieties". A basic definable set is rather the projection of such a difference variety; one can show that the projection can be taken to be finite-to-one.

Dimensions: It is possible to attach a finite dimension to certain definable sets. In model theory one considers more general ordinal-valued dimension theories, referring to them as the "rank". Thus we will speak of groups of finite rank. This is quite distinct from (in very special cases, dual to) the notion of an Abelian group of finite $\mathbb{Q}$-rank. Though sets of infinite rank occur in difference fields (as well as unranked sets, in the case of several automorphisms), we will largely be concerned with sets of finite rank. We refer to [5] for a detailed definition and discussion of the relevant dimension theories. Let us note here that there are three approaches to defining the dimension. Let K_0 be a difference field, D the zero set of a (finite) number of difference polynomials over K_0 (or more generally a quantifier-free definable set).

(i) The *transformal degree* of D is defined to be

$$\sup_{a \in D} tr.\deg_{K_0} K_0(\{\tau(a) : \tau \in \mathscr{F}_0\}).$$

For instance if $k = 1$, and f is a nonzero ordinary ($k = 1$) difference polynomial in one variable X, i.e. a polynomial in $X, X^\sigma, \ldots, X^{\sigma^m}$ for some m, and D is the 0-set of f, then (if X^{σ^m} occurs nontrivially in f), D has transformal degree m.

(ii) One can use the structure of quantifier-free definable subsets of D. The dimension of D is then the maximal m, such that there exist a chain $p_0 \subset \cdots \subset p_m$ of prime difference ideals, with the defining polynomials of D lying in p_0. This could be stated dually in terms of irreducible difference subvarieties of D.

(iii) One can use the structure of all definable subsets of D. See the discussion of S1-rank below. The ranks given in these three ways satisfy (iii)$\leqslant$(ii)$\leqslant$(i), despite the additional freedom permitted by (iii). It is this fact that will be used, later on, to show that all definable groups embed into algebraic groups, and are simply determined by certain algebraic-group data (up to finite index, in the version given here; a precise determination requires more work; this reflects the blindness of the rank to finite index).

Note that if G is an algebraic group, or generally an algebraic variety, then G has finite (Zariski) dimension as such, but infinite rank in the sense of σ.

(Classical model theory has developed a convention of denoting a model and its universe by the same symbol. This is gradually becoming cumbersome, as one works more and more with different structures on the same universe. For instance, here it would be much better to have different symbols for G as an algebraic group, and as a group defined in a difference field. However we will stick to this convention in the present paper, and trust to context.)

From now on, unless explicitly stated otherwise, we work in the ordinary case of a single automorphism, $k = 1$.

In our analysis of definable Abelian groups below, we will also require the general classification of difference formulas of finite rank, developed in [5]. With a little extra analysis, the central result there can be phrased as follows. Let $\phi(x)$ be any difference equation, or formula, of finite rank. One can try to simplify it by substitution, say the substitution of x' for x, where x' is a rational or algebraic function of $x, \sigma(x), \sigma^2(x), \ldots$. Using such transformations, ϕ can be reduced to an equation ϕ' of one of the following forms. Let $E = \{x' : \phi'(x')\}$.

- E is the fixed field k, i.e. ϕ' is the equation $\sigma(x') = x'$.
- E is a one-dimensional σ-definable subgroup of a simple Abelian variety A. Moreover, every σ-definable subset of E^n is a finite Boolean combination of σ-definable subgroups.
- ϕ' is "trivial" in the sense that there are no algebraic relations between pairwise independent solutions of ϕ.

Though this has been proved only in characteristic zero, we believe that an appropriate modification of the theorem holds in all characteristics. (In (i) one must allow more generally the equation for the fixed fields of $\sigma^l \mathrm{Frob}^k$, and in (ii) certain subgroups of vector groups must be taken into account.) Note the special role that this theorem accords to subgroups of Abelian varieties, among all difference equations. This by itself suggests a closer understanding of such groups could be useful.

Definable groups: In Section 4 we will develop the theory of Abelian groups definable in difference algebra. In principle, these groups may be defined by arbitrary first-order formulas in the language of commutative rings, with a symbol for the automorphism σ. However, one quickly sees that up to isogeny and finite index subgroups,

they can all be defined using "linear" equations $\sum e_i\sigma^i(x)=0$, where x ranges over a commutative algebraic group A (this will be explained in more detail in Section 4). We put "linear" in quotes, since if A is a semi-Abelian variety, and the equation is written out in coordinates, it is not linear at all. We are interested however in the inner structure of these groups, in the model-theoretic sense of "induced structure"; this includes polynomial relations among elements, intersections with subvarieties, behaviour of σ. We obtain essentially the full story here. As an example, we quote:

Definition 1.2.3. Let A be a semi-Abelian variety over K, defined over the fixed field k. An equation of the form

$$\sum_{i=0,\ldots,n} m_i\sigma^i(x)=0$$

(or in the inhomogeneous version, $\sum_{i=0,\ldots,n} m_i\sigma^i(x)=a$) is said to be of *restricted Abelian type* if the polynomial $\sum_{i=0}^{n} m_iT^i\in\mathbb{Z}[T]$ has no roots of unity among its zeroes.

Theorem 1.2.1. *Let (K,σ) be a difference-closed difference field, A be a semi-Abelian variety over K, and let $F(\sigma)=a$ be an equation of restricted Abelian type on A. Let B be the set of solutions to $F(\sigma)=a$ in K, and let X be a subvariety of A. Then $X\cap B$ is a finite union of cosets of (definable) subgroups of A.*

Note the analogy to Theorem 1.1.3.

At the other extreme, if $\sum m_iT^i$ is cyclotomic, the group in question is a possibly twisted algebraic group over the fixed field k, and as such carries a lot of structure. It is shown in Section 3.2 that any definable group of finite rank is built up from the two types of example, Abelian type groups and twisted algebraic groups. The two types are "orthogonal" in the model theoretic sense. This means that every definable subset of their product is a Boolean combination of "rectangles". In Sections 3.3, and 3.4, we describe the non-split ways these groups can be put together. Section 3.6 says something about the induced structure in this case.

Quantitative bounds: To obtain our quantitative bounds, we will need an estimate on the number of solutions to a difference equation. It is convenient to bound more generally the number of components of the Zariski closure of the set of solutions to a difference equation, working in the model completion. With an appropriate notion of ("total") degree of a subvariety of $\mathbb{P}_n^l$, we obtain:

Proposition 1.2.2. *Let X be a subvariety of $\mathbb{P}_n$, and let S be a subvariety of $\mathbb{P}_n^l$. Let (K,σ) be a difference-closed difference field, and let Z be the Zariski closure of*

$$\{x\in X(K):(x,\sigma(x),\ldots,\sigma^{l-1}(x))\in S\}.$$

Then

$$\deg(Z)\leqslant(\deg(X)^l\deg(S))^{2^d},\quad d=\min(\dim(S),l\dim(X)).$$

In particular, this bounds the number of irreducible components of Z.

These doubly exponential bounds will be proved in Section 2. The proof requires only Bezout's theorem and Proposition 2.2.1 (which can be taken as a definition of difference-closed difference fields). They apply a posteriori to any difference variety known to be finite, regardless of the effectivity of the initial proof of such finiteness. In particular they apply to the qualitative finiteness statement of Theorem 1.2.1, and yield the explicit bounds.

1.3. Postscript, November 2000

The proof of Manin–Mumford given in this paper was found in 1994 (cf. [13]), written and submitted in 1995. The present text is a great improvement over the 1995 preprint, thanks to the graceful help of Elisabeth Bouscaren, Zoé Chatzidakis, and Michael McQuillan, as well as Alex Wilkie and Boris Zilber. Asides from many local corrections, the following aspects are new.

Tate–Voloch: I heard about the Tate–Voloch conjecture a few weeks after the original preprint was submitted. It was immediately clear that the methods of this paper, with no further work other than a classical nonstandard analysis type argument, answer significant cases of that conjecture. The result (Proposition 6.6.1), circulated separately in early 1996, is now included in the text.

Uniformity in X: The proof of Manin–Mumford, unlike the number theoretic proofs, does not assume that X lies over the fixed field, and hence gives bounds uniform in X. In other words, if $\mathscr{X} \subseteq (A \times Y)$ is an algebraic variety, $X_b = \{a \in A : (a,b) \in \mathscr{X}\}$, then there exists m such that the Zariski closure of $X_b \cap Tor(A)$ is a union of at most m translates of group subvarieties. It seemed at the time of writing that this is a significant contribution of the present approach. But it turns out that this can be deduced directly from the statement! See automatic uniformity, below.

Uniformity in A: Uniformity in A (Theorem 1.1.2) does appear to be an important feature of this proof. In particular, going back to the original statement of Manin–Mumford, fix p and also $g \geqslant 2$; there exists an absolute bound $b(p,g)$ on the number of prime-to-p torsion points lying on a curve over $\mathbb{Q}_p$ of genus g and with good reduction at p.

Improvements in model-theoretic technology: The theory of "simple unstable" first-order theories has greatly matured in the intervening five years. The main advance was a generalization of the finite-dimensional theory (represented in part here) to the general simple context. But there were also advances within the finite-dimensional context, and in particular Frank Wagner found a much smoother and more general approach to internalizing groups. However I left the original treatment intact.

Automatic uniformity: Statements such as Manin–Mumford, or Mordell–Lang, at the level of all Abelian varieties (or at least all Cartesian powers of a given one), enjoy an automatic uniformity property. As soon as one knows that $ZCl(X \cap \Gamma^n)$ is a finite union of cosets of group subvarieties for any n and any subvariety X of A^n, one also obtains a bound on this finite number, that does not grow when X moves in an algebraic family. This uniformity (Corollary 3.5.9) seems to have gone unobserved

by number theorists and model theorists alike, but it is an immediate consequence of a lemma, Lemma 3.5.8, that was folklore in model theory since the mid-1980s, and whose proof is short and requires no technology beyond the compactness theorem. In particular, it has nothing to do with any of the aspects of the present paper, neither difference fields nor model theoretic dimension theories. In itself it seems to be of interest, for instance because of the following corollary:

Corollary 1.3.1. *Let A be a simple Abelian variety of dimension 2 over a number field K, and f a rational function on A. Let C_a be the curve $f^{-1}(a) \subseteq A$. Then for some integer M, $|C_a(K)| \leqslant M$ for all $a \in K$.*

Proof. By Faltings + automatic uniformity.

At the end of this section (Lemma 1.3.2) we include a complete and elementary proof, where even the use of compactness can be replaced by an algebraic argument.

Work of Scanlon: Later work of Scanlon amply demonstrated the potentiality of these model theoretic methods. Extending the ideas in Lemma 6.6.1 and in Theorem 1.1.4, he gave a proof of the full Tate–Voloch conjecture for semi-Abelian varieties over $\mathbb{Q}_p$. Transposing these ideas to Drinfeld modules, he proved Denis' conjecture. No other proofs are presently known.

New in this edition: Originally, the quantitative and qualitative arguments were separated inasfar as one automorphism goes, but were given together in the arguments using two automorphisms. They are now separated in all cases; a priori bounds are given first in Section 2.3.1, so that quantitative details need not confuse the actual proof of finiteness. The lemma on automatic uniformity is new here. Section 4.6 is also new (Problem 4.5.2 was previously proved ad hoc).

Lemma 1.3.2 (Automatic uniformity). *Let G be a commutative algebraic group over a field K. Let Y and $U \subseteq (G \times Y)$ be varieties; so that $\{U_y : y \in Y\}$ is a constructible family of subvarieties of G. Then there exists a finite number of subvarieties $C_i \subseteq G^{n_i}$ of Cartesian powers of G such that for any group $A \subseteq G(K)$, if*

$$C_i \cap A^{n_i} = F_i \cap A^{n_i}$$

for each i, with F_i the union of cosets of group subvarieties of G^{n_i}, then for some M, for any b, the Zariski closure of $U_b \cap A$ is the union of at most M cosets of group subvarieties of G.

Proof. For $g = (g_1, \ldots, g_n) \in G^n$, let

$$Y(g) = \left\{ y \in Y : \bigwedge_{i=1}^{n} (g_i, y) \in U \right\}.$$

Let

$$R_n = \{(g,h) \in G^n \times G : Y(g) \subseteq Y(h)\},$$

$$E_n = \left\{ (g_1,\ldots,g_n) \in G^n : \bigwedge_{i=1}^{n} Y(g_1,\ldots,g_{i-1}) \neq Y(g_1,\ldots,g_i) \right\}.$$

(For $i=1$, read: $Y \neq Y(g_1)$.) Then $R_n \subseteq G^n \times G$, $E_n \subseteq G^n$ are constructible sets. Take the C_i to be Zariski closed sets, so that each R_n is a Boolean combination of some of the C_i.

For large enough N, we have $E_N = \emptyset$. For otherwise, by compactness, we could find $g_1, g_2, \ldots \in G$ with $Y \neq Y(g_1) \neq Y((g_1,g_2)) \neq \ldots$, contradicting Noetherianity of Y in the Zariski topology.

Now let A be a subgroup of $G(K)$. Let $b \in Y$. Pick $g_1, g_2, \ldots, g_n \in A \cap U_b$ such that $g = (g_1,\ldots,g_n) \in E_n$, and n is as large as possible. (We have $n \leqslant N$.) So if $h \in A \cap U_b$, then $h \in R_n(g)$, i.e. $(g,h) \in R_n$. Conversely if $h \in R_n(g)$, then $b \in Y(g) \subseteq Y(h)$, so $h \in U_b$. Thus

$$A \cap U_b = A \cap R_n(g).$$

By assumption, $R_n \cap A^{n+1} = F_n \cap A^{n+1}$, where F_n is a Boolean combination of cosets. So $R_n(g) \cap A = F_n(g) \cap A$. But $F_n(g)$ is clearly a Boolean combination of boundedly many cosets. Hence so is $F_n(g) \cap A = A \cap U_b$, and thus also the Zariski closure of $A \cap U_b$. □

2. The number of solutions to difference equations

2.1. Bezout's theorem

In order to formulate our results, we embed our variety X in projective space $\mathbb{P}_n$. We wish to bound the number of elements of X satisfying some difference equations. This amounts to considering elements x of X such that $(x, \sigma x, \ldots, \sigma^l x)$ lies in a prescribed subvariety S of $\mathbb{P}_n^l$. We denote by $\deg(S)$ the sum of the multi-degrees of S; in particular if S is the set of zeroes of a multi-homogeneous polynomial, then $\deg(S)$ is the total degree of this polynomial.

There is however a more convenient description for our purposes, given in [10, p. 148, Example 8.4.4]. Viewing $\mathbb{P}_n$ as V'/G_m, where V' is an $(n+1)$-dimensional vector space with 0 removed, we obtain a representation of $\mathbb{P}_n^l$ as $(V')^l/(G_m)^l$. Let G_m be the diagonal subtorus of G_m^l. Then $(V')^l/(G_m)$ can be identified with an open subset U of $(V)^l/(G_m) = \mathbb{P}_{(n+1)l-1}$.

Definition 2.1.1. We have a surjective rational map $\phi : \mathbb{P}_{(n+1)l-1} \to \mathbb{P}_n^l$ given by

$$\phi((x_0^1 : \ldots : x_n^1 : x_0^2 : \ldots : x_n^2 : \ldots : x_n^l) = ((x_0^1 : \ldots : x_n^1), \ldots, (x_0^1 : \ldots : x_n^l)))$$

ϕ is defined outside of the union L of l linear subvarieties. For a subvariety S of $\mathbb{P}_n^l$, we let S' be the Zariski closure of $\phi^{-1}S$. Let $\deg(S)=\deg(S')$, the latter taken in projective space. If S is a reducible variety, we define $\deg(S)$ to be the sum of the degrees of the components.

Our calculations will be based on:

Lemma 2.1.2 (Bezout's Theorem). (1) *Let $V_1,\dots,V_r$ be subvarieties of $(\mathbb{P}_n)^l$. Let $Z_1,\dots,Z_t$ be the irreducible components of $V_1\cap\cdots\cap V_r$. Then*

$$\sum_{i=1}^{t}\deg(Z_i)\leqslant\prod_{j=1}^{r}\deg(V_j)$$

(2) *Let V be a subvariety of $(\mathbb{P}_n)^l\times(\mathbb{P}_n)^k$, and let $\bar{V}$ be the (set-theoretic) projection to $(\mathbb{P}_n)^l$. Then $\deg(\bar{V})\leqslant\deg(V)$.*

(3) *Let X be a subvariety of $(\mathbb{P}_n)^l\times(\mathbb{P}_n)^k$ of degree d. Let pr_1 be the first projection, $X(a)=X\cap pr_1^{-1}(a)$. Suppose $\dim X(a)=r$ for generic $a\in pr_1X$. Then $\{a\in(\mathbb{P}_n)^l\colon\dim(X(a))>r\}$ is contained in a proper Zariski closed subset of pr_1X of degree at most d.*

(4) *Let V be a subvariety of $(\mathbb{P}_n)^l\times(\mathbb{P}_n)^l\times(\mathbb{P}_n)^k$, $\Delta=\{(a,b,c)\in(\mathbb{P}_n)^l\times(\mathbb{P}_n)^l\times(\mathbb{P}_n)^k\colon a=b\}$, and let $\bar{V}=pr(V\cap\Delta)$ be the (set-theoretic) projection of $V\cap\Delta$ to $(\mathbb{P}_n)^l\times(\mathbb{P}_n)^k$. Then $\deg(\bar{V})\leqslant\deg(V)$.*

Proof. (1) Note that $S=\phi(S'\cap U)$, and S' is irreducible if S is. For S' is invariant under the action of the torus G_m^l, acting by

$$\begin{aligned}&(\alpha_1,\dots,\alpha_l)\cdot((x_0^1:\dots:x_n^1:x_0^2:\dots:x_n^2:\dots:x_n^l)\\&\quad=((\alpha_1x_0^1:\dots:\alpha_1x_n^1:\alpha_2x_0^2:\dots:\alpha_2x_n^2:\dots:\alpha_lx_n^l).\end{aligned}$$

It follows that some component of S' of maximal rank must also be invariant; but then it has the form U' for some subvariety U, and necessarily $U=S$ and $U'=S'$. Thus the operation $S\to S'$ takes subvarieties of $\mathbb{P}_n^l$ to subvarieties of $\mathbb{P}_{(n+1)l-1}$, injectively and preserving the inclusion and irreducibility. Hence if Z is a component of $V_1\cap V_2$, then Z' is a component of $V_1'\cap V_2'$. The operation also preserves degree by our definition of degree. Thus we are reduced to the case $l=1$; this is [10, p. 148, Example 8.4.6].

(2) We may assume V, and hence $\bar{V}$, are irreducible. Let

$$\phi_1:\mathbb{P}_{(n+1)l-1}\to(\mathbb{P}_n)^l$$

and

$$\phi_2:\mathbb{P}_{(n+1)(l+k)-1}\to(\mathbb{P}_n)^k\times(\mathbb{P}_n)^l$$

be the maps from Definition 2.1.1 used to define degree on $(\mathbb{P}_n)^{l+k}$ and on $(\mathbb{P}_n)^l$. Let

$$\pi:(\mathbb{P}_n)^l\times(\mathbb{P}_n)^k\to(\mathbb{P}_n)^l$$

be the projection. Then clearly $\pi\phi_2 = \phi_1\theta$ where θ is a linear projection from $\mathbb{P}_{(n+1)(l+k)-1}$ to $\mathbb{P}_{(n+1)l-1}$. It remains to show:

Claim. *Let θ be a linear projection from $\mathbb{P}_N$ onto $\mathbb{P}_M$, with center C. Let V be a subvariety of $\mathbb{P}_N$, not contained in C. Let $\bar{V}$ be the Zariski closure of $\theta(V\backslash C)$. Then* $\deg(\bar{V}) \leqslant \deg(V)$.

Proof. Let $\bar{L}$ be a linear subspace of $\mathbb{P}_M$ of complementary dimension to $\bar{V}$. Let L be the pullback to $\mathbb{P}_N$, so $C \subseteq L$, L is a linear subspace of $\mathbb{P}_N$, and $\theta(V \cap L\backslash C) = \bar{L} \cap \bar{V}$. $V \cap L$ has at most $\deg(V)$ irreducible components. Hence the Zariski closure of $\theta(V \cap L)$ has at most $\deg(V)$ irreducible components. Since it is finite, it has size at most $\deg(V)$. So $\deg(\bar{V}) \leqslant \deg(V)$. □

(3) Let $\phi : \mathbb{P}_{k(n+1)-1} \to (\mathbb{P}_n)^k$ be the map from Definition 2.1.1, and let $\theta = Id_{(\mathbb{P}_n)^l} \times \phi$. Let Y be the Zariski closure of $\theta^{-1}X$. Let L be a generic linear subvariety of $\mathbb{P}_{k(n+1)-1}$ of codimension $r + k$. Let $X' = Y \cap ((\mathbb{P}_n)^l \times L)$. Note that $\deg(X') = \deg(Y) = \deg(X)$. For generic $a \in pr_1X$, $X'(a) = (Y(a) \cap L) = \emptyset$. On the other hand by the projective dimension theorem, if $\dim X(a) > r$ then $X'(a) \neq \emptyset$. Thus

$$\{a \in (\mathbb{P}_n)^k : \dim(X(a)) > r\} \subseteq pr_1X' \subseteq pr_1X$$

and we can apply (2).

(4) Δ is easily seen to have degree $l + 1$; so from (1) and (2) we get $\deg(\bar{V}) \leqslant (l + 1)\deg(V)$. To get the result with coefficient 1, recall the maps

$$\phi_0 : W_l^2 \times W_k \to (\mathbb{P}_l)^2 \times (\mathbb{P}_k),$$

$$\phi_0 : (x_0, \ldots, x_l, y_0, \ldots, y_l, z_0, \ldots, z_k) \mapsto ((x_0 : \ldots : x_l), (y_0, \ldots, y_l), (z_0, \ldots, z_k)),$$

where W_l is a standard $(l + 1)$-dimensional vector space with 0 removed; and also

$$\phi_0' : W_l \times W_k \to \mathbb{P}_l \times \mathbb{P}_k,$$

$$\phi_0' : (y_0, \ldots, y_l, z_0, \ldots, z_k) \mapsto ((y_0, \ldots, y_l), (z_0, \ldots, z_k)).$$

Now

$$\phi'^1(pr(V \cap \Delta)) = pr_0^*(\phi_0^{-1}(V) \cap \Delta_0^*),$$

where $pr_0^* : W_l^2 \times W_k \to W_l \times W_k$ is the projection, and $\Delta_0^* = \{(a, b, c) \in W_l^2 \times W_k : a = b\}$. The maps ϕ_0, ϕ_0', pr^* induce rational maps ϕ, ϕ', pr^* on and between appropriate subsets of the projectivizations $Proj(W_l \times W_l \times W_k)$, $Proj(W_l \times W_k)$. We have

$$\phi^1(pr(V \cap \Delta)) = pr^*(\phi^{-1}(V) \cap \Delta),$$

where Δ is the projectivization of Δ. Since Δ has degree 1, the result follows as in (1) and (2). □

2.2. Ordinary difference equations

We will also use the following characterization of difference-closed difference fields.

Lemma 2.2.1. *Let (K,σ) be a difference-closed difference field, and let X be an irreducible K-variety, X^σ the conjugate variety, and Y an irreducible K-subvariety of*

$$X \times X^\sigma \times \cdots \times X^{\sigma^l}.$$

Let π, π', π_0 be the projections to $X \times X^\sigma \times \cdots \times X^{\sigma^{l-1}}$, $X^\sigma \times \ldots \times X^{\sigma^l}$, X, respectively. Suppose $(\pi Y)^\sigma = \pi' Y$ (or just that these two sets have the same Zariski closure). Then

$$\{x \in X(K) : (x, \sigma(x), \ldots, \sigma^{l-1}(x)) \in Y\}$$

is Zariski dense in $\pi_0 Y$.

Proof. For $l=2$ this follows from Definition 1.2.1 of difference-closed difference fields: if H is a hypersurface in πY, by Definition 1.2.1 applied to $(\pi Y \backslash H), ((\pi Y)^\sigma \backslash H^\sigma), Y \cap (\pi Y \backslash H) \times ((\pi Y)^\sigma \backslash H^\sigma)$, there exists $a \in \pi Y \backslash H$ with $(a, \sigma(a)) \in Y$; since this holds for any H, $\{a : (a, \sigma(a)) \in Y\}$ is Zariski dense in πY. For higher l, let $X' = X \times \cdots \times X^{\sigma^{l-1}}$, $Y' = \{(\pi \bar{x}, \pi' \bar{x}) : \bar{x} \in Y\}$, and apply the case $l=2$. □

The following proposition yields estimates of finite numbers arising in difference algebra. We allow reducible varieties here.

Notation 2.2.2. $\mathbb{P} = \mathbb{P}_n = n$-dimensional projective space

$$\mathbb{P}^l = (\mathbb{P}_n)^l,$$

$$\pi(x_1, \ldots, x_l) = (x_1, \ldots, x_{l-1}),$$

$$\pi'(x_1, \ldots, x_l) = (x_2, \ldots, x_l),$$

$$\pi_1(x_1, \ldots, x_l) = x_1.$$

Proposition 2.2.1. *Let (K,σ) be a difference-closed difference field, and let S be a subvariety of $\mathbb{P}^l$, defined over K. Let*

$$Z = \text{Zariski closure of } \{x \in \mathbb{P}(K) : (x, \sigma(x), \ldots, \sigma^{l-1}(x)) \in S\}.$$

Then $\deg(Z) \leqslant \deg(S)^{2^{\dim(S)}}$. In particular, Z has at most $\deg(S)^{2^{\dim(S)}}$ irreducible components.

Say S is defined over $\mathbb{Q}(c)$. Then every irreducible component of Z is defined over $\mathbb{Q}(\sigma^i(c), \ldots, \sigma^{i-\dim(S)}(c))^a$ for some i, $0 \leqslant i \leqslant \dim(S)$.

Proof. We use Notation 2.2.2. Given a (nonempty) irreducible subvariety W of S, we define varieties W', W'' as follows.

Case 1: $(\pi W)^\sigma = \pi' W$.

In this case we let $W'' = W$, $W' = \emptyset$.

Case 2: $\pi' W \not\subseteq (\pi W)^\sigma$.

Then let $W' = (\mathbb{P} \times (\pi W)^\sigma) \cap W$, $W'' = \emptyset$.

Case 3: $(\pi W)^\sigma \not\subseteq \pi' W$, or equivalently $\pi W \not\subseteq (\pi' W)^{\sigma^{-1}}$.

Then let $W' = ((\pi' W)^{\sigma^{-1}} \times \mathbb{P}) \cap W$, $W'' = \emptyset$.

Claim. (1) $\deg(W'' \cup W') \leqslant \deg(W)^2$.

(2) $\pi_1 W'' \subseteq Z$.

(3) *If* $\bar{x} = (x, \sigma x, \ldots, \sigma^{l-1}(x)) \in W$, *then* $\bar{x} \in W'' \cup W'$.

(4) $\dim(W') < \dim(W)$.

(5) *If* W *is defined over* $\mathbb{Q}(c)$, *then* W' *and* W'' *are defined over* $\mathbb{Q}(\sigma^{-1}(c), c)$ *or over* $\mathbb{Q}(\sigma(c), c)$ (*depending on the case*).

Proof. (1) Follows from Lemma 2.1.2; projections, product with projective space $\mathbb{P}$, and application of σ do not increase degree, while the intersection (in cases (2) and (3)) squares it.

(2) Follows from Proposition 2.2.1

(3) Clear from the definition of W', W'' in each case.

(4) Clear since W is nonempty and irreducible, and W' is either empty or a proper subvariety, in each case.

(5) Evident. □

Now define $S(i), T(i)$ as follows:

$$S(0) = S; \quad T(0) = \emptyset,$$

$$S(i+1) = \bigcup \{W' : W \text{ a component of } S(i)\},$$

$$T(i+1) = \bigcup \{W'' : W \text{ a component of } S(i)\} \cup T(i).$$

Using Claim (4), it is clear that $S(k) = \emptyset$ for some $k \leqslant \dim(S) + 1$. By Claim (3), if $\bar{x} = (x, \sigma x \ldots, \sigma^{l-1}(x)) \in S$ then $\bar{x} \in S(i) \cup T(i)$ for each i, hence $\bar{x} \in T(k)$. Thus in this situation $x \in \pi_1 T(k)$. It follows that Z is contained in $\pi_1 T(k)$. Conversely, by Claim (2), every component of $\pi_1 T(k)$ is contained in Z. Hence $Z = \pi_1 T(k)$.

By Claim (1), $\deg(S(i) \cup T(i)) \leqslant \deg(S)^{2^i}$ and $\deg T(i+1) \leqslant \deg(S)^{2^i}$ for each i. The required bound on the degree follows using Lemma 2.1.2(2).

The rationality statement follows by induction from Claim (5). □

Corollary 2.2.3. *Let* X *be a subvariety of* $\mathbb{P}_n$, *and let* S *be an irreducible subvariety of* $\mathbb{P}_n^l$. *Let* (K, σ) *be a difference-closed difference field, and let*

$$Z = \text{Zariski closure of } \{x \in X(K) : (x, \sigma(x), \ldots, \sigma^{l-1}(x)) \in S\}.$$

Then

$$\deg(Z) \leqslant (\deg(X)^l \deg(S))^{2^d}, \quad d = \min(\dim(S), l\dim(X)).$$

In particular, this bounds the number of irreducible components of Z.

Proof. Let $S' = S \cap (X \times X^\sigma \times \cdots \times X^{\sigma^{l-1}})$. Then $\deg(S') \leqslant \deg(S)\deg(X)^l$, while the dimension is at most d. Thus Proposition 2.2.1 applies. □

Our original treatment required a uniform version of Proposition 2.2.1, when S is allowed to vary with a parameter. There may be embedded components that are hidden to Proposition 2.2.1, in a generic fiber, but appear upon specialization. The following somewhat technical lemma deals with this issue. Will not be used in present approach.

Notation 2.2.4. We keep Notation 2.2.2, except that we let $\mathbb{P} = \mathbb{P}_m \times \mathbb{P}_{m'}$, and $\rho : \mathbb{P} \to \mathbb{P}_m$ the projection. We also denote by ρ the map $\rho \times \cdots \times \rho : \mathbb{P}^l \to (\mathbb{P}_m)^l$. If Z is a subvariety of $\mathbb{P}^l$ and $a \in (\mathbb{P}_m)^l$,

$$Z(a) = \{b \in (\mathbb{P}^l_{m'}) : (a, b) \in Z\},$$

and if $r = \dim Z(a)$ for generic $a \in \rho Z$,

$$Z^* = \{a \in \rho Z : \dim Z(a) > r\}.$$

Lemma 2.2.5. *Let (K, σ) be a difference-closed difference field, and let S be a subvariety of $\mathbb{P}^l$, defined over K. There exist irreducible subvarieties Z_i of $\mathbb{P}$ such that:*
1. $\Sigma_i \deg(Z_i) \leqslant \sum_{i=0}^{\dim(S)} \deg(S)^{2^i}$.
2. $\{x \in Z_i(K) : (x, \sigma(x), \ldots, \sigma^{l-1}(x)) \in S\}$ *is Zariski dense in* Z_i.
3. *If* $a \in \{x \in \mathbb{P}(K) : (x, \sigma(x), \ldots, \sigma^{l-1}(x)) \in S\}$ *then for some* i, $a \in Z_i$ *and* $\rho(a) \in Z_i^*$.
4. (*Irredundancy*) *If* $i \neq j$ *and* $Z_i \subseteq Z_j$, *then* $\rho(Z_i) \subseteq Z_j^*$.

Proof. A straightforward variation on the proof of Proposition 2.2.1. $S(i), T(i)$ are treated as collections of irreducible varieties. In Case 1 we let $W'' = W$, $W' = (W^* \times \mathbb{P}_{m'}) \cap W$. By Lemma 2.1.2(3) and (1), we have $\deg(W') \leqslant \deg(W)^2$; so Claim 1 must be modified to:

$$\deg(W' \cup W'') \leqslant \deg(W)^2 + \deg(W).$$

As in Proposition 2.2.1, we begin with the variety S, and obtain a larger collection of irreducible varieties by closing under the operation: given W, add the irreducible components of W' and of W''. In addition, to achieve the fourth item, we close under the binary operation: given W_1 and W_2 such that $W_1 \subseteq W_2$, add $W_1 \cap (W_2^* \times \mathbb{P}_{m'})$. This allows to simply remove, at the end of the construction, any "redundant" Z_i as in (4). These operations always decrease dimension. One can show inductively that the sum of the degrees of the Z_i of codimension e in S is bounded by $(\deg S)^{2^e}$. □

2.3. Numerical bounds for partial difference equations

In this subsection, we work in a universal domain $\mathbb{U}$ for the theory of fields with r automorphisms, $\sigma_1,\ldots,\sigma_r$. $\mathscr{F}$ denotes the free group generated by $\sigma_1,\ldots,\sigma_r$.

$\mathscr{F}$ acts on itself by conjugation, and on the polynomial rings over $\mathbb{U}$ by acting on the coefficients. Putting these actions together we obtain an action of $\mathscr{F}$ on the difference polynomial ring. This action can be characterized by $F(a)^\tau = F^\tau(a^\tau)$.

Three considerations frame the effectivity picture for partial difference equations.

(1) For a finite number of difference equations, bounds entirely similar to the ordinary case hold. (Proposition 2.3.1).

(2) Unlike the ordinary case, prime difference ideals are not finitely generated, and one is typically interested in infinite sets of equations. In particular, if T is a set of points in the universal domain that is defined invariantly over $\mathbb{Q}$, such as the set of torsion points of an Abelian variety over $\mathbb{Q}$, then the set of equations satisfied by T will be invariant under $\mathscr{F}$-conjugation. If $\phi(X,\sigma(X))$ is an equation involving σ alone, the properties of ϕ as an ordinary difference equation correspond better to the properties of $\{\phi^\alpha\colon \alpha\in\mathscr{F}\}$, than to ϕ as a partial difference equation. (See for instance Problem 4.5.2 and Lemma 4.5.4.)

(3) The Zariski closure of the solution set of an infinite set of partial difference equations in the universal domain is already the Zariski closure of the set of solutions of a finite subsystem. Given (1), the problem becomes to find such a finite subsystem. One does not expect a general effective solution for conjugation-invariant difference ideals, even when finitely generated as such. The word problem for groups may be coded in such ideals, using equations in one variable of the form $x^w - x$.

In our application, we will directly estimate the number of equations needed in (3), and so (1) will apply.

A *path* in $\mathscr{F}$ is a sequence $\tau_1,\ldots,\tau_n$ such that for each $1\leqslant m<n$, for some generator σ_i of $\mathscr{F}$, $\tau_{m+1}=\sigma_i\tau_m$ or $\tau_{m+1}=\tau_m$ or $\tau_{m+1}=\sigma_i^{-1}\tau_m$. A subset $\Phi\subseteq\mathscr{F}$ is called *connected* if there exists a path connecting any two points of Φ.

Notation 2.3.1. Φ is a finite, connected subset of $\mathscr{F}$. $\mathbb{P}=(\mathbb{P}_n)$ is projective space, $\mathbb{P}^\Phi$ the Cartesian power of $\mathbb{P}$, with coordinates indexed by the elements of Φ. For each i, let

$$\Phi_{i,-} = \{a\in\Phi : \sigma_i a\in\Phi\},$$

$$\Phi_{i,+} = \{a\in\Phi : \sigma_i^{-1} a\in\Phi\}.$$

Let $\pi_{i,-},\pi_{i,+}$ be the projections

$$\pi_{i,-} : \mathbb{P}^\Phi \to \mathbb{P}^{\Phi_{i,-}}, \quad \pi_{i,+} : \mathbb{P}^\Phi \to \mathbb{P}^{\Phi_{i,+}}.$$

If $a\in\mathbb{P}$, let a^Φ denote the tuple $(\ldots,a^\phi,\ldots)\in\mathbb{P}^\Phi$ with a^ϕ in the ϕth-place.

Proposition 2.3.1. *Let Φ be a connected, finite subset of $\mathscr{F}$. Let S be a subvariety of $\mathbb{P}^\Phi$, defined over $\mathbb{U}$. Let*

$$Z = ZCl\{a \in \mathbb{P}(\mathbb{U}) : a^\Phi \in S\}.$$

Then

$$\deg(Z) \leqslant \deg(S)^{2^{\dim(S)}}.$$

In particular, Z has at most $\deg(S)^{2^{\dim(S)}}$ irreducible components.

If S is defined over $\mathbb{Q}(c)$, then every connected component is defined over $\mathbb{Q}(c, c^{\tau_1}, c^{\tau_2}, \ldots, c^{\tau_m})^a$ for some path $1, \tau_1, \ldots, \tau_m$ in $\mathscr{F}$ with $m \leqslant \dim(S)$.

Corollary 2.3.2. *Let X be a subvariety of $\mathbb{P}$, and let S be an irreducible subvariety of $\mathbb{P}^\Phi$. Let*

$$Z = ZCl\{a \in X(\mathbb{U}) : a^\Phi \in S\}.$$

Then

$$\deg(Z) \leqslant (\deg(X)^{|\Phi|}\deg(S))^{2^d}, \quad d = \min(\dim(S), |\Phi|\dim(X)).$$

In particular, this bounds the number of irreducible components of Z.

Proof. The proofs of Proposition 2.3.1, and of Corollary 2.3.2, are the same as to those of Proposition 2.2.1 and Corollary 2.2.3, replacing the use of Proposition 2.2.1 by that of Lemma 2.3.3 below. In the proof of Proposition 2.3.1, Case 1 is that for each i, $\pi_{i,-}W^{\sigma_i} = \pi_{i,+}W$. In this case, using Lemma 2.3.3, $Z \cap W$ will be Zariski dense in W. If Case 1 fails, there are $2r$ possible ways it can fail (two for each i), and one proceeds as in Proposition 2.2.1. □

Lemma 2.3.3. *Let X be an irreducible $\mathbb{U}$-variety, X^ϕ the conjugate variety ($\phi \in \mathscr{F}$), and Y an irreducible $\mathbb{U}$-subvariety of $\Pi_{\phi \in \Phi} hX^\phi$, projecting dominantly to each single factor. Let $\pi_{i,-}$, $\pi_{i,+}$ be as in Proposition 2.3.1. Suppose $(\pi_{i,-}Y)^{\sigma_i} = \pi_{i,+}Y$ for each $i = 1, \ldots, r$ (or just that these two sets have the same Zariski closure). Then $\{x \in X(\mathbb{U}) : x^\Phi \in Y\}$ is Zariski dense in X.*

Proof. Let $a = (a_\phi : \phi \in \Phi)$ be a generic element of Y over $\mathbb{U}$, $L = \mathbb{U}(a)^a$. Then for any subset $S \subseteq \Phi$, $(a_\phi : \phi \in S)$ is a generic element of the projection of Y to $\Pi_{\phi \in S} X^\phi$. In particular, for each i, $\pi_{i,-}(a)$ is a generic point of $\pi_{i,-}Y$, and $\pi_{i,+}(a)$ is a generic point of $\pi_{i,+}Y$. By assumption, the automorphism σ_i of $\mathbb{U}$ carries $ZCl\pi_{i,-}Y$ to $ZCl\pi_{i,+}Y$. Thus σ_i extends to an automorphism σ_i' of L with $\sigma_i'\pi_{i,-}(a) = \pi_{i,+}(a)$. We obtain an action of $\mathscr{F}$ on L. Since $\sigma_i(a_\phi) = a_{\sigma_i\phi}$ whenever $\phi, \sigma_i\phi \in \Phi$, we have $(\sigma_i\phi)^{-1}(a_{\sigma_i\phi}) = \phi^{-1}(a_\phi)$; as Φ is connected, $\phi^{-1}(a_\phi)$ is the same element a_0 for any $\phi \in \Phi$, and we have $\phi(a_0) = a_\phi$. Now a_0 is a generic element of X, and $a_0^\Phi \in Y$. As $\mathbb{U}$ is existentially closed, $\{x \in X(\mathbb{U}) : x^\Phi \in Y\}$ is Zariski dense in X. □

3. Abelian groups of finite S1-rank

We include here some of the general theory of groups of finite S1-rank. Some of this material appeared previously in an unpublished preprint PAC ("On PAC and related structures"), and some was introduced in [8]. We refer to Chap. 7 of [5].

In these lemmas, all structures are assumed to be of finite $S1$-rank; there are no other assumptions. To be precise, we assume that we work in a universal domain $\mathscr{U}$, with a map rk on nonempty definable sets, into the nonnegative integers, with the following properties. (set $rk(\emptyset) = -\infty$)

A point of a definable set D of rank d is said to be *generic* over a base set B if it does not lie in any B-definable set of rank $<d$:

1. Suppose $f : D \to E$ is a definable map. Let

$$E_i = \{e \in E : rk(f^{-1}(e)) = i\}.$$

Then E_i is definable, and $rk(D) = \max_{i\in\mathbb{N}} \{rk(E_i) + i\}$.

2. Suppose $R \subseteq (D \times E)$ is definable, and let $D_e = \{d \in D : (d, e) \in R\}$. Assume $e_i \in E$ for $i = 1, 2, \ldots, rk(D_e) = k$ for $e \in E$, and $rk(D_{e_i} \cap D_{e_j}) < k$ for $i \neq j$. Then $rk(D) > k$.

We will write $rk(Q)$ for $\inf\{rk(D) : Q \subseteq D\}$ if Q is an ∞-definable set. $rk(a/B)$ denotes the rank of the type of a over B. Note that $rk(Q)$ is the supremum of $rk(q)$ over all complete types q extending Q.

Remark 3.0.4. (1) These properties are satisfied by transformal degree in difference fields.

(2) If a rank function with the above properties exists, then one can find a smallest possible rank function satisfying the second property. However the first, "definability" property need no longer hold. (This indeed occurs in difference fields.)

(3) Define two elements a,b to be independent over a substructure C if $rk(a/bC) = rk(a/C)$. This is symmetric and transitive, by the properties of rank. One can show (cf. [5], Chap. 7) that the Independence Theorem holds:

Assume given substructures $B, A_1, A_2, A_3, A_{12}, A_{13}, A_{23}$, with B, A_1, A_2, A_3 algebraically closed, and maps:

$g_i : B \to A_i$ and $g_{ij} : B \to A_{ij}$, and

$h_{ij} : A_i \to A_{ij}$, $h_{ji} : A_j \to A_{ij}$ $(i < j,)$, with $g_{ij} = h_{ij} g_i$ for $i \neq j$.

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

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

Further, the $f_{ij} h_{ij}(A_i)$ are independent over the image of B.

(4) On the other hand, if a,b are not independent over C, $q(x, y) = tp(a, b/C)$, and $b_1, b_2, \ldots$ are independent realizations of $tp(b/C)$ over C, then one can show that $\bigcup_i q(x, b_i)$ is inconsistent. It follows from this and the independence theorem that independence in this sense coincides with independence in the sense of simple theories [17, 30].

3.1. Commensurable families of groups

Definition 3.1.1. Two definable subgroups A, B of a group G are *commensurable* if they share a common subgroup of finite index in both. Commensurability is an equivalence relation, denoted $A \sim B$. We also write $A \leqslant\sim B$ if $B \cap A$ has finite index in A. If H, H' are each the intersection of a bounded family of definable subgroups, we say H, H' are commensurable if one can write $H = \bigcap H_i$, $H' = \bigcap H_i'$, with all the H_i and H_i' commensurable; equivalently, $H \cap H'$ has bounded index in H and in H'.

An ∞-definable set (over C) is an intersection of C-definable sets. A generic (over C) element of a ∞-definable set Y (over C) is an element $b \in Y$ such that b is not in any C-definable set of smaller rank than Y.

Lemma 3.1.2. *Let Q be the solution set of a complete type over an algebraically closed set C. Let G be a C-∞-definable group. Let $H \subseteq Q \times G$ be ∞-definable, such that $H(a)$ is a subgroup of G, for $a \in Q$. Suppose all the $H(a)$ are commensurable. Then there exists a C-∞-definable subgroup H^* of G, commensurable with each $H(a)$. Moreover,*

(i) *For independent $a, b \in Q$, $H(a) \cap H(b) \subseteq H^*$.*

(ii) *If $h \in H^*$ is generic, then there exists an element a generic over h, with $h \in H(a)$.*

Proof. Let $B = \{g \in G : \text{for some } a \in Q, g, a \text{ independent}, g \in H(a)\}$. This is an ∞-definable subset of G. An easy application of the independence theorem shows that if b_1, b_2 are independent elements of B, then $b_1 b_2^{-1} \in B$. Thus $H^* = BB$ is a subgroup of G, and a generic element of BB is in B. It follows that $rk(H^*) \leqslant rk(B) \leqslant rk(H(a))$. Now let a, b be independent elements of Q (over C). We have $rk(H(a)) = rk(H(b)) = rk(H(a) \cap H(b))$. Pick $c \in H(a) \cap H(b)$ with $rk(c/C \cup \{a, b\}) = rk(H(b))$. Then $rk(c/Cab) \geqslant rk(H(b)) \geqslant rk(c/Cb)$ so c is independent from a over bC. Since also a,b are independent, over C, c and a are independent over C. Thus by definition $c \in BB$. This shows that a generic element of $H(a) \cap H(b)$ is in BB; hence $H(a) \cap H(b) \subseteq BB$. Since $H(a)$,$H(b)$ are commensurable, and $rk(H^*) \leqslant rk(H(a) \cap H(b))$, it follows that all these groups are commensurable. □

Remark. The existence of H^*, and (i), are valid for partial types too.

If one assumes in that G and H are definable, one obtains a definable H^* commensurable with each $H(a)$, and satisfying (i).

(Any ∞-definable group in a finite S1-rank theory is an intersection of definable groups (over the same set); see [5, Chap. 7].)

Lemma 3.1.3. *Let Q be a possibly incomplete type over a set C. Let G be a C-definable group. Let $H \subseteq Q \times G$ be ∞-definable, such that $H(a)$ is a subgroup of G, for $a \in Q$. Suppose all the $H(a)$ are commensurable, and further that all the conjugates of the $H(a)$ are commensurable among themselves. Then there exists a*

C-∞-definable normal subgroup H^* of G, commensurable with each $H(a)$. If $h \in H^*$ is generic, then there exists an element a generic over h, with $h \in H(a)$. If H is definable, we can take H^* to be definable.

Proof. Assume $C = 0$ for convenience. We may assume here that Q is complete. Let Q_0 be a 0-definable set containing Q. Let G_0 be a copy of G. Let G act on itself by conjugation, on G_0 by translation, and on Q_0 trivially; call this action on $R = G \cup G_0 \cup Q_0$, as well as the induced action on the powers of R, ρ. Let R' be the reduct with universe R, and language L' consisting of the L-0-definable relations, that are also ρ-equivariant. Observe that $H' \subseteq G \times G_0 \times Q$ defined by: $(a, e, c) \in H'$ iff $e^{-1}ae \in H(c)$ is in L'. Also the group structure on G is in L'. Similarly, any L-definable subset of R is L'-definable with parameters, so R' has the same $S1$-rank as L, and it is L'-definable. By Lemma 3.1.2 applied to (R', L'), there exists in this reduct a 0-∞-definable group H^* commensurable with each $H(a)$. Being 0-definable in L', it must be respected by the action ρ on G, so it is normal. By the remark following Lemma 3.1.2, we can take H^* to be definable if each $H(a)$ is definable. □

Remark. Q could be a partial $*$-type, i.e. a type in infinitely many variables.

3.2. Indecomposability lemma

Lemma 3.2.1. *Let $\mathcal{U}$ be the universal domain of a theory of finite $S1$-rank, C a countable elementary submodel. Let G be a C-definable group, P the set of realizations in $\mathcal{U}$ of a generic type of G over C. Let X_2 be the set of products gh^{-1}, with g, h independent elements of P. Then the set of products $\{ef : e, f \in X_2\}$ is an ∞-definable subgroup of G of bounded index (intersection of boundedly many definable subgroups of finite index). Hence there exists a bounded set R such that $RPPPP = G$.*

The notation $G(C)$ means the set of elements of G definable over C. The last sentence of the lemma states that any element of G is the product of an element of R, and four elements of P. The lemma can easily but tediously be proved directly, but follows more pleasantly from the theory of stabilizers, and we refer to [5] in lieu of a proof.

The following lemma, originating in the theory of algebraic groups as the "indecompasability theorem", was lifted by Zilber to the finite Morley rank context. The key is the development of a theory of stabilizers valid there. The existence of a (different) theory of stabilizers makes the lemma valid also in the finite $S1$-rank context, cf. [5, Chap. 7].

Lemma 3.2.2. *Let G be a group definable in a structure of finite $S1$ rank. Let Y be the set of solutions of a complete type over an algebraically closed set. Then for some n, $(YY^{-1})^n$ is a subgroup of G.*

Lemma 3.2.3. *Let G be a group definable in a structure of finite $S1$ rank. For any definable $Y \subseteq G$ there exist definable groups H_i of G and finitely many cosets C_i of H_i such that*:
1. $Y \subseteq \bigcup_i C_i$.
2. *For some n, every element of H_i has the form*

$$\prod_{1 \leqslant i \leqslant 2n} a_i^{(-1)^i}$$

with $a_i \in (Y \cap C_i)$.

3.3. Internal groups

Definition 3.3.1. A definable set D is *stably embedded* if every definable subset of D, with parameters possibly outside D, is definable also with parameters from D.

This notion seems to have arisen first in [8]. See [5] for its basic properties. Note here that in a saturated model $\mathbb{U}$, a 0-definable set D, endowed with the induced structure, is stably embedded iff the restriction map $Aut(\mathbb{U}) \mapsto Aut(D)$ is surjective. (Given stable embeddedness, surjectivity can be shown by a back-and-forth construction using domains of the form $D \cup X$, X small. Conversely, if the map is surjective, every $\mathbb{U}$-definable subset of D has at most $|\mathbb{U}|$ conjugates under $Aut(D)$; it follows using a standard criterion of Joyal and Shelah that it is D-definable with parameters.)

Definition 3.3.2. A definable set E is *internal* to a definable set D if there exists a definable (with parameters) surjective map $h : D_1 \to E$, where $D_1 \subseteq D^k$ is definable

We will use this when D is stably embedded; in this case it is equivalent to: $\equiv_D C$ is trivial, for some finite (or countable) C; where:

Definition 3.3.3. Let D be a C-definable set. Write $a \equiv_{CD} a'$ if $tp(a/C \cup D) = tp(a'/C \cup D)$.

In the difference field context, D will usually be the fixed field. When E is a $*$-definable set, we will say that E is D-internal if every definable quotient of E is D-internal; in particular, if K is an intersection of a descending sequence of definable subgroups K_i of a definable group G, we will say that G/K is D-internal to mean: G/K_i is D-internal, for each i.

The finite case:

Lemma 3.3.4. *Let G be a 0-definable group, D a stably embedded 0-definable set, C a finite or countable set, p a generic type of G over C, P the set of realizations of*

p in the universal domain. If $a \in P$, *let*

$$E(a) = \{a' : tp(a/C \cup D) = tp(a'/C \cup D)\}$$

and suppose $E(a)$ *is finite for* $a \in P$. *Then there exists a finite normal subgroup* N *of* G *with* G/N *D-internal. Moreover, for any* $a \in P$ *and* $n \in N$, $na \in P$ *and*

$$tp(na/C \cup D) = tp(a/C \cup D).$$

Proof. Enlarging C, and replacing p by a complete type over the new base, preserves the hypothesis. Hence we may assume that C is algebraically closed, and that any subgroup of G of finite index, definable over C, has a set of coset representatives in $G(C) = \{a \in G : a \in dcl(C)\}$. Then by assumption, $E(a)$ is finite, of size k say. Replace C and p by another set and type, in such a way that k is least possible.

Let

$$K = \{a \in G(C) : \text{for some } b \in P, ab \in P, \text{ and } tp(b/C \cup D) = tp(ab/C \cup D)\}.$$

Since P is the solution set of a complete type, one can equally well say "for all $b \in P$" in the definition of K. It follows that K forms a subgroup of G. By assumption, for $b \in P$, only finitely many $b' \in P$ have the same type over $C \cup D$ as b; hence Kb is finite, so K is finite.

Note that if $a \in G$, and for some $b \in P$ with a, b independent over C, $tp(b/C \cup D) = tp(ab/C \cup D)$, then $a \in K$. This is because $ab \in E(b) \subseteq acl(C \cup \{b\})$, so $a \in acl(C \cup \{b, ab\}) = acl(C \cup \{b\})$; as a, b are C-independent, $a \in acl(C) = C$; and hence $a \in K$.

Claim. *For* $a \in P$, $E(a) = Ka$.

Proof. $Ka \subseteq E(a)$ by definition. Let a, d be independent elements of P over C, $a = db^{-1}$. Let $a' \in E(a)$; let $c = a'a^{-1}$; we will show that $c \in K$. Note that $a' \in acl(C \cup \{a, a'\}) = acl(C \cup \{a\})$; and that a, b are C-independent, by genericity of P. We have

$$tp(a/C \cup \{b\} \cup D) = tp(a'/C \cup \{b\} \cup D)$$

for otherwise, replacing C by a bigger set C' containing b, and replacing p by $tp(a/C')$, we will decrease k, contradicting the minimal choice of k. Thus the two types are equal, and

$$tp(ab/(C \cup D)) = tp(a'b/(C \cup D)).$$

Thus $a'b \in acl(C \cup \{ab\})$, and so $c = a'a^{-1} = (a'b)(ab)^{-1} \in acl(C \cup \{ab\})$. We also have $c \in acl(C \cup \{a\})$, and ab, a are independent over C. Thus $c \in acl(C) = C$. Now by the definition of K it follows that $c \in K$. □

Similarly, we may show that K has a normalizer of finite index. Let a, a' be independent generic elements of P, and let $b = a'a^{-1}$. We will show that b normalizes K. Let $c \in K$. Then

$$tp(a/(C \cup \{b\} \cup D) = tp(ca/(C \cup \{b\} \cup D)$$

as in the previous claim. Thus,

$$tp(ba/(C \cup D)) = tp(bca/(C \cup D)),$$

So

$$tp(a'/(C \cup D)) = tp((bcb^{-1}a'/(C \cup D))$$

and hence $bcb^{-1} \in K$. Now by Lemma 3.2.1, it follows that the normalizer $N(K)$ contains a subgroup of G of finite index.

Now P is divided into finitely many cosets of $N(K)$; so there exists a translate gP of P such that $gP \cap N(K)$ has rank equal to G. $N(K)$ has a set of coset representatives in $G(C)$, so we may take $g \in G(C)$. Let $P' = gP \cap N(K)$. If $a \in P'$, in particular $a \in gP$, so every conjugate of a over $C \cup D$ is in Ka; hence the image $\bar{a}$ of a in $\bar{G} = (N(K)/K)$ has no proper conjugates over $C \cup D$. Since D is stably embedded, $\bar{a} \in dcl(C \cup D)$. Let $\bar{P}$ be the set of elements of $\bar{G}$ with the same type over C as $\bar{a}$. Then $\bar{P} \subseteq dcl(C \cup D)$. By Lemma 3.2.1, there exists a finite subset $\bar{R}$ of $\bar{G}(C)$ such that $\bar{R}(\bar{P})^4 = \bar{G}$. Thus every element of $\bar{G}$ is in $dcl(C \cup D)$.

However, we wanted this conclusion for a quotient of G itself. Let G_1 be the intersection of all conjugates of $N(K)$ in G; since $N(K)$ has finite index in G, so does G_1. Let N be the intersection of all conjugates of K; since K is finite, it is a finite intersection. By the assumption on C, we have

$$N = \bigcap_{i=1,\ldots,m} g_i^{-1} K g_i, \quad g_1, \ldots, g_m \in G(C).$$

We have $(g_i^{-1}(N(K))g_i)/(g_i^{-1}Kg_i) \subseteq dcl(C \cup D)$, so $G_1/(g_i^{-1}Kg_i) \subseteq dcl(C \cup D)$ for each i, and it follows that $G_1/N \subseteq dcl(C \cup D)$. But N is normal in G, and there exists in $(G/N)(C)$ a set of coset representatives for G_1/N; thus $G/N \subseteq dcl(C \cup D)$. □

Remark 3.3.5. In Lemma 3.3.4, one can find a 0-definable finite N^* normal in G, with G/N^* D-internal.

Proof. Let $N^* = \bigcap \{\sigma(N) : \sigma \in Aut(\mathcal{U})\}$, where $\mathcal{U}$ is the universal domain. Then $N^* \subseteq N$ so N^* is finite. It is $Aut(\mathcal{U})$-invariant, hence is 0-definable. By finiteness, $N^* = \bigcap_{i=1,\ldots,m} \sigma_i(N)$ for some $\sigma_1, \ldots, \sigma_m \in Aut(\mathcal{U})$. Then $G/(\sigma_i(N))$ is D-internal, and G/N^* embeds definably into the product of these groups.

Internalizing groups (*General case*): Recall that $a \equiv_{CD} b$ iff a, b have the same type over $C \cup D$. Observe that $\equiv_{CD}$ is ∞-definable: $a \equiv_{CD} a'$ iff for every formula

$\theta(x, y_1, \ldots, y_r)$ over C, E^θ:

$$(\forall y_1)\ldots(\forall y_r)\wedge_i D(y_i) \;\Rightarrow\; (\theta(a, y_1,\ldots, y_r) \leftrightarrow \theta(a', y_1,\ldots, y_r).$$

Indeed this shows that $\equiv_{CD}$ is an intersection of $\aleph_0+|C|$ definable equivalence relations, E^θ written above. We define $a/\equiv_{CD}$ to be $((a/E^\theta)\colon \theta\in L(C))$. Note that $a\equiv_{CD} b$ iff $a/E^\theta = b/E^\theta$ for each such θ.

Proposition 3.3.1. *Let G be a 0-definable group. Let D be a stably embedded, 0-definable set. Then there exists an ∞-definable (over $\emptyset$) normal subgroup K^* of G, such that: G/K^* is D-internal, and such that if $a\in K^*$ is generic, then for some generic $b\in G$, $b\equiv_{\emptyset D} ab$.*

Corollary 3.3.6. *Let G be a 0-definable group. Let D be a stably embedded, 0-definable set. Suppose every element of G is algebraic over D. Then G/K is D-internal for some finite normal subgroup K.*

Proof. This is a special case of Lemma 3.3.4.

Remark 3.3.7. More generally, if D is any 0-definable set, there exists an ∞-definable normal subgroup K of G, such that: for some C, $\equiv_{CD}$ is trivial on G/K; and for any C, for generic $a\in K$, for some generic $b\in G$, $b\equiv_{CD} ab$.

Remark 3.3.8. Still more generally, one can prove an analog for any definable equivalence relation E on G; the lemma will give a normal subgroup K, such that the kernel of $G\to(G/K)$ is the "generic intersection" of all the translates of E.

Proof of Proposition 3.3.1. Consider pairs (p, C) with C the algebraic closure of a finite set (or a set of bounded size), and p a complete generic type of G over C. P will denote the set of realizations of p. Let $k(p, C) = k$ be the maximal integer such that for some $a, a'\in P$, $a\equiv_{CD} a'$ and $rk(a'/C\cup\{a\}) = k$. (Then for any $a\in P$, for some a', $a\equiv_{CD} a'$ and $rk(a'/C\cup\{a\}) = k$.) Let k_0 be the least possible integer of this form; we will consider only pairs (p, C) with $k(p, C) = k = k_0$.

Let $K(p, C)$ be the set of elements $a\in G$ such that for some generic realization c of p over $C\cup\{a\}$, $ac\equiv_{CD} c$. Then $K(p, C)$ is ∞-definable over C. Let $\bar{K}(p, C) = K(p, C)K(p, C)$.

Claim 1. *$K = K(p, C)K(p, C)$ is a subgroup of G. $rk(K\backslash K(p, C)) < rk(K)$.*

Proof. It suffices to show that if a, b are independent elements of K, then $ab^{-1}\in K$. Let $e\in P$ be such that $ae\equiv_{CD} e$ and $be\equiv_{CD} e$; this is possible simultaneously by the independence theorem. Then $e' = ae\in P$, e' is generic over $C\cup\{a, b\}$, and $ba^{-1}e' = be\equiv_{CD} e\equiv_{CD} e'$; so $ba^{-1}\in K$. □

Claim 2. *$rk(K) = k_0$.*

Proof. Let (a,d) be mutually generic realizations of p, $b=a^{-1}d$. Let $C'=C\cup b$, and let $p'=tp(a/C')$. Pick a' with $a\equiv_{C'D}a'$, and $rk(a'/C'\cup\{a\})=k(p',C')\geqslant k_0$. So $k(a,a'/C')\geqslant k_0+rk(p)$. Now clearly $a\equiv_{CD}a'$, so $rk(a,a'/C)\leqslant rk(p)+k_0$. Thus (a,a') is independent from b over C; hence also b is generic over $C\cup\{a,a'\}$. Let $c=a'a^{-1}$. Then c is independent from ab over C.

Since $tp(a'/C'\cup D)=tp(a/C'\cup D)$ and $b\in C'$, we also have $tp(a'b/C'\cup D)=tp(ab/C'\cup D)$, and in particular $ab\equiv_{CD}a'b$. But $a'b=cab$. Thus $c\in K$.

It follows that $rk(K)\geqslant rk(c/C)\geqslant rk(a'/C\cup\{a\})=k_0$. Conversely, if $c'\in K(p,C)$ then for some generic a, $c'a\equiv_{CD}a$, so $rk(c'/a)=rk(c'a/a)\leqslant k_0$. □

Claim 3. *All $\bar{K}(p,C)$ are commensurable.*

Proof. Recall that we are referring only to $K(p,C)$ with $k(p,C)=k_0$. If we extend C to C' and p to a generic type p' over C', it's clear that $\bar{K}(p',C')\subseteq\bar{K}(p,C)$; by the minimality of k_0, they must be commensurable. If p,q are two generic types over C, let b,c be independent elements over C realizing p,q. Let $d=b^{-1}c$, and let $C'=C\cup d$, and $p'=tp(b/C')$. Now $K(p',C')\subseteq K(q,C)$: to see this let $a\in K(p',C')$. Then $tp(ab'/C'\cup D)=tp(b'/C'\cup D)$ for some $b'\in P'$; we may assume $b'=b$. Since $d\in C'$, $abd\equiv_{CD}bd$; i.e. $ac\equiv_{CD}c$; showing that $a\in K(q,C)$. □

Claim 4. *If $K=K(p,C)$ and $K'=e^{-1}Ke$ is a conjugate of K, then K, K' are commensurable.*

Proof. After increasing C (using the previous claim), we may assume $e\in C$. Let $b\in P$, $c=e^{-1}b$, $q=tp(c/C)$. We show $K(q,C)\subseteq K'$, so that commensurability follows from the equality of ranks. Let $a\in K(q,C)$. Then we may assume $ac\equiv_{CD}c$. Since $e\in C$, it follows that $eac\equiv_{CD}ec$. In other words, $(eae^{-1})b\equiv_{CD}b$. Thus $eae^{-1}\in K$, so $a\in K'$.

□

Let C continue to range over sets of the type considered above. By Lemma 3.1.3, there exists a (0-)∞-definable normal subgroup K^* of G, commensurable with all the $\bar{K}(p,C)$, and such that a generic element of K^* lies in some generic $\bar{K}(p,C)$ (a,C are independent). Moreover, (using also the proof of the previous claim), if $a\in\bar{K}(p,C)$ for any p and any generic C, then $a\in K^*$. It remains only to show that G/K^* is D-internal. Write $K^*=\bigcap_j K_j$, where K_j are definable groups, commensurable with each other. Let $G_j=G/K_j$, and let $\pi_j: G\to G_j$ be the quotient map. Let P_j be the image of P under π_j.

Claim 5. *Let $\equiv_{CD}(a)$ be the $\equiv_{CD}$-class of a. Then $\equiv_{CD}(a)$ is contained in finitely many cosets of each K_j.*

Proof. Some generic $c\in K(p,C)$ satisfies $ca\in\equiv_{CD}(a)$, so $K(p,C)a\cap\equiv_{CD}(a)$ has rank k_0. Since $\bar{K}(p,C)$ is ∞-definable over C, and all elements of $\equiv_{CD}(a)$ realize the same type over C, all cosets of $\bar{K}(p,C)$ intersecting $\equiv_{CD}(a)$ must intersect it in a

set of the same rank k_0. Since also $rk(\equiv_{CD}(a)) = k_0$, $\equiv_{CD}(a)$ is contained in finitely many cosets of $\bar{K}(p, C)$. Since $\bar{K}(p, C)$ and K^* are commensurable, the same is true for K^*. □

Claim 6. *If $a^*, b^* \in P_j$ and $a^* \equiv_{CD} b^*$, then there exist $a, b \in P$, $a \equiv_{CD} b$, with $\pi_j(a) = a^*$, $\pi_j(b) = b^*$. (And a may be chosen arbitrarily, with $\pi_j(a) = a^*$.)*

Proof. Since D is stably embedded, there exists an automorphism σ of $\mathscr{U}$ fixing $C \cup D$ with $\sigma(a^*) = b^*$. Pick any $a \in P$ with $\pi_j(a) = a^*$, and let $b = \sigma(a)$.

It follows from the last two claims that $\equiv_{CD}$ has finite classes on G_j. By Lemma 3.3.4, there exists a finite normal subgroup N^* of G_j such that G_j/N^* is D-internal, and

$$\text{for any } a \in P^* \text{ and } n \in N^*,\ tp(na/C \cup D) = tp(a/C \cup D).$$

I claim that $N^* = 1$. Let $n^* \in N^*$, and lift it to $n \in G$. We must show that $n \in K^*$. For this it suffices to show that $n \in K(p, C)$ for generic C. This follows from Claim 6. Thus $N^* = 1$ so G_j is D-internal. □

3.4. Stability and modularity

We introduce here one of our central notions, of a locally modular group. In ordinary difference fields of characteristic 0, these groups will be stable and stably embedded. It is misleadingly easy to define modularity in group-theoretic terms, but the more abstract point of view of stability is better suited to analyze the relation of such a group to its environment (or of two such groups), a relation that need not a priori be group-theoretic. We start with a property of independence in stable theories.

Lemma 3.4.1. *If a, b are independent over $acl(C \cup \{a\}) \cap acl(C \cup \{b\})$, and (a, b) is independent from C over $E \subseteq C$, then a, b are independent over $acl(E \cup \{a\}) \cap acl(E \cup \{b\})$.*

Proof. Let $E' = acl(E \cup \{a\}) \cap acl(E \cup \{b\})$, $C' = acl(C \cup \{a\}) \cap acl(C \cup \{b\})$. It suffices to show that a, b are independent from C' over E'. Note that a is independent from $C' \cup \{b\}$ over $E \cup \{b\}$, since $acl(C' \cup \{b\}) = acl(C \cup \{b\})$. Thus (a, b) is independent from C' over $E \cup \{b\}$. Similarly (a, b) is independent from C' over $E \cup \{a\}$. It follows that the canonical base of $tp(ab/C')$ is contained in $acl(E \cup \{a\})$ and in $acl(E \cup \{b\})$, hence in their intersection E'.

Definition 3.4.2. A theory is called 1-based if it is stable, and in any model M of T, any two algebraically closed substructures of M^{eq} are independent over their intersection. A structure is 1-based if the theory of that structure is that.

An equivalent condition: A saturated stable structure M is 1-*based* iff the lattice of algebraically closed substructures of M^{eq} (including imaginary elements) satisfies

the modular law: if $X \subseteq Z$, then $acl(X \cup Y) \cap Z = acl(X \cup (Y \cap Z))$. Such structures are also called "locally modular". It would be better to call them "modular", but for historical reasons, this word is reserved for locally modular structures satisfying an additional condition of a weak elimination of imaginaries.

Corollary 3.4.3. *Suppose M is a saturated stable structure, and the result M' of naming constants in M for elements of the countable set C, is* 1*-based. Then M is* 1*-based.*

Proof. Let A, B be algebraically closed subsets of M. We may assume $A \cup B$ is independent from C, by moving them by an appropriate automorphism. But then the result follows from Lemma 3.4.1.

Definition 3.4.4. We will say that a definable group B is LMS (stable, stably embedded, locally modular) if every definable subset of B^n (with parameters possibly outside B) is a finite Boolean combination of cosets of definable subgroups of B^n.

Remark 3.4.5. By Hrushovski and Pillay [15], the condition LMS for a stable group B is equivalent to 1-basedness of the induced structure. By quantifier elimination for Abelian structures (Baur, Ziegler), an Abelian group G with extra structure generated by subgroups of G^n, for various n, is always 1-based.

It is also shown in [15] that there are no infinite definable families of distinct definable subgroups of a 1-based group.

Proposition 3.4.1. (1) *Let $0 \to A \to B \to C \to 0$ be an exact sequence of definable Abelian groups and homomorphisms, in a structure W. Then B is LMS iff A and C are LMS.*

(2) *More generally, let $g : B \to C$ be a surjective definable map in a saturated structure W. Then B is stable, stably embedded, and* 1*-based iff these three properties hold for C and for every fiber of g.*

(3) *In particular, the union of two* 1*-based, stably embedded sets again enjoys this property.*

Remark 3.4.6. If A is stable, stably embedded and 1-based, then it remains so after a parameter is added; hence every coset of A in B is also stable, stably embedded and 1-based. Thus the first statement is indeed a special case of the second one.

Remark 3.4.7. The proof is an instance of the use of second-order characterizations in model theory. The number of types is a global property of the family of all definable sets; perhaps the simplest one. It is much more amenable to devissage (i.e. reductions as in Proposition 3.4.1) than the geometric description of the structure of each individual definable set. Similarly for the modularity property. We did not find a good direct proof; the difficulty occurs already in case A is finite. We offer a direct proof of a similar statement in Proposition 3.6.1 (Section 3.2); see also Lemma 3.5.11.

Proof of Proposition 3.4.1. We will use the following characterization (cf. [5], lemmas on stable embeddability).

$(*)$ B is stable and stably embedded iff for any subset X of the universal domain, of size $\lambda = \lambda^{\aleph_0}$, there are at most λ types of elements of B over X.

If $(*)$ holds for B, then it certainly holds for C and for every fiber of g, as they are interpretable in the structure B (with a named parameter). Conversely, assume $(*)$ holds for C and for every fiber of g. Then there are $\leqslant\lambda$ possibilities for $tp(c/X)$, with $c \in C$. For any given $c \in C$, there are $\leqslant\lambda$ possibilities for $tp(a/cX)$, with $a \in g^{-1}(c)$. Thus there are also at most $\lambda^2 = \lambda$ possibilities for $tp(bc/X)$, $b \in B$, $c = g(b)$; equivalently, $\leqslant\lambda$ possibilities for $tp(b/X)$.

Now for 1-basedness.

Note first (#): *if a definable set D is stably embedded in B and* 1*-based, and $X \subseteq D$, $Y \subseteq B$, then X, Y are independent over $acl(X) \cap acl(Y)$.*

Indeed with $Y' = acl(Y) \cap D^{\mathrm{eq}}$, we have X, Y' independent over $(acl(X) \cap D^{\mathrm{eq}}) \cap Y'$, while by stable embeddability we have Y independent from $X \cup Y'$ over Y', and transitivity applies.

More generally, in (#) we may take $X \subseteq acl(D)$ instead of $X \subseteq D$; since then with $X' = X \cap D^{\mathrm{eq}}$, we have $acl(X) = acl(X')$.

In fact, (##): *Suppose that for some set F independent from X and some F-definable set D that D is stably embedded and $X \subseteq acl(D \cup F)$. Then for any Y,*

$$X \underset{(acl(X) \cap acl(Y))}{\downarrow} Y.$$

For we may assume (X, Y) is independent from F; so (#) is valid over F; and by Proposition 3.4.1 it holds over $\emptyset$.

Moreover in the conclusion of (#) or (##), we may say X, Y are independent over $acl(acl(X) \cap acl(Y) \cap D^{\mathrm{eq}})$. For if $W = acl(W) \subseteq acl(D)$ then $W = acl(W \cap D^{\mathrm{eq}})$.

It follows that if B is stable and 1-based, then so is every interpretable set D. Indeed if X, Y are relatively algebraically closed subsets of D^{eq}, then they are independent over $acl(X) \cap acl(Y) \cap D^{\mathrm{eq}}$.

Let us now prove (3): Let $X, Y \subseteq D_1 \cup D_2$ be relatively algebraically closed where D_1, D_2 are 1-based, stably embedded. By naming parameters, we may assume $X \cap Y \subseteq dcl(\emptyset)$. We wish to show that X, Y are independent. Let $X_i = dcl(X) \cap dcl(D_i)$,

$$Y_i = \{b \in Y^{\mathrm{eq}} : tp(b) \text{ is } D_i\text{-internal}\}.$$

Then $dcl(X) = dcl(X_1 \cup X_2)$ and similarly for Y. Moreover $D_1 \underset{Y_1}{\downarrow} Y$ so $X_1 \underset{Y_1}{\downarrow} Y$; but by 1-basedness of D_1, $X_1 \underset{\emptyset}{\downarrow} Y_1$; so $X_1 \underset{\emptyset}{\downarrow} Y$. Dually, $Y_2 \underset{\emptyset}{\downarrow} X$, so also $Y_2 \underset{X_1}{\downarrow} X$.

Claim. $dcl(D_2) \cap dcl(X_1 \cup Y) \subseteq dcl(X_1 \cup Y_2)$.

We prove the claim using the theory of germs of definable functions in a stable theory; cf. [12]. In a stable theory, germs of definable functions into a definable set

D always have a canonical base e of definition with $tp(e)$ D-internal; and there exists a representative of the germ, defined over e. So if $t \in dcl(X_1 \cup Y) \cap dcl(D_2)$, write $t = f(a_1, b)$, $a_1 \in X_1$, $b \in Y$, $r = tp(a_1)$; then the r-germ g of $f(\ , b)$ is in $dcl(b)$ and has a D_2-internal type; hence $g \in Y_2$. Let F be a g-definable function agreeing with $f(\ , b)$ on generic realizations of r; then $F(a_1) = f(a_1, b) = t$, so $t \in dcl(a_1, g) \subseteq dcl(X_1 \cup Y_2)$.

Remark. A parallel but more formal proof of the same Claim, using algebraic closure throughout, may be given along the lines of Proposition 3.4.1; see the proof of (2) below.

Note that any formula $\phi(u)$ implying $D_2(u)$ is defined over D_2 (by stable embeddedness of D_2); so if we accept the claim, and if ϕ is also defined over $X_1 Y$, then it is defined over $X_1 Y_2$. Thus $tp(Y/X_1 Y_2)$ implies $tp(Y/X_1 D_2)$, so

$$Y \underset{X_1 \cup Y_2}{\downarrow} D_2.$$

Resuming, we have in particular:

$$Y \underset{X_1 Y_2}{\downarrow} X_2$$

hence as $X \subseteq dcl(X_1 X_2)$,

$$Y \underset{X_1 Y_2}{\downarrow} X$$

but $Y_2 \underset{X_1}{\downarrow} X$ so

$$Y \underset{X_1}{\downarrow} X$$

and recalling $Y \underset{\emptyset}{\downarrow} X_1$ we have $X \underset{\emptyset}{\downarrow} Y$. This finishes the proof of (3).

Now to prove (2), assume C and every fiber of g are stable, stably embedded, and 1-based. Then every finite union of fibers of g is also stably embedded, and 1-based. We also already know that B is stable. Let X, Y be algebraically closed subsets of B^{eq}. We must show that X, Y are independent over $X \cap Y$. By naming parameters, we may assume $X \cap Y \subseteq dcl(\emptyset)$. We may assume $X = acl(b)$, where $b = (b_1, \ldots, b_n)$; denote $gb = (gb_1, \ldots, gb_n)$. Then $gb \in X_0 = X \cap C^{eq}$. By (#), X_0, Y are independent. Let Y' be the canonical base of $tp(b/Y)$. Then $b \underset{Y'}{\downarrow} Y$, so we may assume $Y = acl(Y')$. Now if $b, b', b'', \ldots$ is a sequence of independent realizations of $tp(b/Y)$, then $Y' \subseteq acl(b, b', \ldots)$ by a basic result of stability (Shelah). So $Y \subseteq acl(b, b', \ldots)$. But $(gb, gb', \ldots) \underset{\emptyset}{\downarrow} Y$. And $(b, b', \ldots)$ lies in a $(gb, gb', \ldots)$-definable 1-based stably embedded set (namely the union of the fibers of g above the elements $gb_i, gb_i', \ldots$). Thus the hypothesis and hence the conclusion of (##) apply to Y. □

Lemma 3.4.8. *Suppose X is LMS*:
1. *If $f : Y \to X$ a* 1-1 *definable map, then Y is LMS.*

2. *If* $g: X^m \to Z$ *is surjective, then* Z *is LMS.*
3. *If a definable subset* X *of a definable group* G *is LMS and* X *generates* G*, then* G *is LMS.*

Proof. The first two items are immediate from the definition of 1-basedness. The third follows from the second, since by saturation, for some n, the map $X^{2n} \to G$ given by

$$(x_1, \ldots, x_{2n}) \mapsto \Pi_i x_i^{(-1)^i}$$

is surjective. □

Recall that two definable sets p, q are *orthogonal* if for any base set B over which p, q are defined, and any a realizing p and b realizing q, a, b are independent over B. The term *hereditarily orthogonal* is sometimes used, but the distinction this reflects will not be important for us. Orthogonality is inherited by powers. In a language to be introduced later, the following lemma says that orthogonality of finite rank groups implies complete orthogonality.

Lemma 3.4.9. *Let* G_1, G_2 *be definable groups of finite rank. Suppose* G_1, G_2 *are orthogonal, and at least one of them is stably embedded. Then every definable* $R \subseteq G_1 \times G_2$ *is a finite union of rectangles* $X_1 \times X_2$.

Proof. Say G_2 is stably embedded, and work over an algebraically closed base set B. Let $R \subseteq G_1 \times G_2$ be B-definable. Let $(a_1, a_2) \in R$. Since G_2 is stably embedded, $R(a_1) = \{y \in G_2 : (a_1, y) \in R\}$ is definable with a parameter from G_2. Taking a canonical parameter c, we have $c \in acl(B, a_1)$, hence by the hypothesis of the lemma, $c \in acl(B) = B$. Thus $R(a_1) = X_2$ is B-definable. Let $X_1 = \{a \in G_1 : R(a) = X_2\}$. Then X_1 is a B-definable subset of G_1, $(a_1, a_2) \in X_1 \times X_2 \subseteq R$. So R is a union of B-definable rectangles. By compactness, it is a union of finitely many. □

Remark 3.4.10. By the structure theory we are about to prove, for definable groups of finite rank in ordinary difference fields of characteristic 0, the assumption that at least one of G_1, G_2 is stably embedded is unnecessary. For if G_i is not LMS, we will see that G_i has a definable subquotient of the form $H_i(k)$, H_i an algebraic group over the constants. But then H_1, H_2 are not orthogonal, and hence neither are G_1, G_2.

3.5. Algebraic modularity

In generalizations to two automorphisms or to positive characteristic, stability is lost, and different proofs and definitions must be given. Initial steps in this direction were taken in [8]. Here we will refer to such modularity only in passing, essentially as a convenient summary of facts about the one-automorphism case. Thus we will not develop here the theory of modularity in simple theories.

At the level of definitions, we will use the ambient Zariski topology. (We will use little more about the ambient field, than that every definable set is a Boolean combination of closed ones.)

Let ZCl denote Zariski closure, and ZCl_k closure for the k-Zariski-topology. $ZCl_0 = ZCl_\emptyset$.

Definition 3.5.1. Let A be a set of points of an algebraic variety V', over an algebraically closed field L. Assume A is Zariski dense in a subvariety V of V', defined over $k \subseteq L$.

Let A_{Zar} be the structure whose universe is V, and whose basic relations are the closed sets $ZCl(X)$, $X \subseteq A^n$; i.e. those Zariski-closed sets $W \subseteq V^n$ such that $W \cap A^n$ is Zariski dense in W.

Let A_{Zar_k} denote the structure whose universe is V, and whose basic relations are the sets $ZCl_k(X)$, $X \subseteq A^n$.

Definition 3.5.2. Let A_{zar} denote the structure whose universe is A, and whose basic relations are the sets $U \cap A^n$, where U is a subvariety of V^m, defined over the prime field.

Lemma 3.5.3. *Let $X \subseteq A^m$ be arbitrary. Then $ZCl(X)$ is definable in A_{Zar_k}, using parameters from A. Conversely, there exists a countable $k_0 \subseteq L$ such that if $k_0 \subseteq k$, then every basic relation of A_{Zar_k} is also definable in A_{Zar}. Thus A_{Zar} has an essentially (i.e. up to constants) countable language.*

Thus A_{Zar} has an essentially (i.e. up to constants) countable language. Note as a corollary that for any two sufficiently large fields k', k'', $A_{Zar_{k'}}, A_{Zar_{k''}}$ differ only by constants.

Proof of Lemma 3.5.3. Let $Y \subseteq V^m$, $X = Y \cap A^m$, $Y = ZCl(X)$. Then as a variety Y is defined over $k(A)$, hence over $k(a_1, \ldots, a_l)$ for some $a_1, \ldots, a_l \in A$. Let $a = (a_1, \ldots, a_l)$, and let $W = ZCl_k(\{a\} \times X)$. Then W is a subvariety of V^{l+m}, and $W(a) = Y$. By definition of A_{Zar_k}, W is one of its basic relations; thus Y is definable in A_{Zar_k}, with parameters from A.

If $k_0 \subseteq k$, the same proof shows that an A_{Zar_k}-definable set is $A_{Zar_{k_0}}$-definable, with parameters. Thus it suffices to prove the converse for one countable k. Take k to be the universe of an elementary submodel of $(L, +, \cdot, A)$. If $U \subseteq V^m$ is a basic relation of A_{Zar_k}, let $X = U \cap A^m$, $Y = ZCl(X)$, and let W be as above, so that $Y = W(a)$ for some a. But for any $a' \in k^l$, if $U(k) \cap A^m \subseteq W(a') \subseteq U$ then $U = W(a')$ (here $U(k)$ is the set of k-points of U). By elementarity, for any $a' \in L^l$, if $U(L) \cap A^m \subseteq W(a') \subseteq U$ then $U = W(a')$. So $U = W(a) = Y$. Thus every relation of A_{Zar_k} is also one of A_{Zar}; we have already seen the other direction. □

Lemma 3.5.4. *Let U be any subvariety of V^m. Then $U \cap A^m$ is definable in A_{zar} (with parameters).*

Proof. Let $U' = ZCl(U \cap A^m)$. Then $U \cap A^m = U' \cap A^m$, so we may assume $U = U'$. Now U is a relation of A_{Zar}, so by Lemma 3.5.3, $U = W(a)$ for some $W \in A_{Zar_k}$ and some $a \in A^l$, where we take k to be the prime field. Now $W' = W \cap A^{l+m}$ is a relation of A_{zar}, and $W'(a) = U \cap A^n$. $\square$

Consider an expansion $\mathbb{U} = (\mathbb{U}, +, \cdot, \ldots)$ of a field.

Definition 3.5.5. Assume $\mathbb{U}$ is a field, with additional structure, V an algebraic variety over $\mathbb{U}$, and denote $V = V(\mathbb{U})$. Let A be a subset of V. Say that A is *algebraically modular* (ALM) if for every $X \subseteq A^m$, $(m = 1, 2, \ldots)$, there exists a 1-based structure whose universe is V and one of whose m-ary relations is the Zariski closure of X.

Remark 3.5.6.

- If $X, X' \subseteq A^m$, then $ZCl(X \times X') = ZCl(X) \times ZCl(X')$. Thus in the above definition, one may take finitely many X at once. It is thus equivalent to say that A_{Zar} is 1-based.
- If V is an algebraic group and A is a subgroup, the definition agrees with Definition 3.5.7 below. Also, it agrees with: $Th(A_{zar})$ is 1-based.
- If A is ALM, then so is every subset of A. (Trivially from Definition 3.5.5).
- If $U = ZCl(X)$, then $X \subseteq A \cap U \subseteq U$, so $U = ZCl(A \cap U)$. So the definition would not change if it referred only to subsets of the form $X = A \cap V$ with V a subvariety of G^m.

Definition 3.5.7. Assume $\mathbb{U}$ is a field, with additional structure. Let A be a subgroup of an algebraic group G. Say that A is *algebraically modular* (ALM) if for ever $m = 1, 2, \ldots, A$ is m-ALM: for every $X \subseteq A^m$, the Zariski closure of X is a finite union of cosets of algebraic subgroups of G^m.

If A is an LMS definable group, it is ALM. For if V is a subvariety of G^m, then $V \cap A$ is a finite Boolean combination of cosets. It can be written as a finite union $\bigcup_i (C_i \backslash F_i)$, where the sets C_i are pairwise disjoint cosets of groups H_i, and F_i is contained in a finite union of cosets of subgroups of H_i of infinite index. It follows that the Zariski closure of $V \cap A$ equals the union of the Zariski closures of the C_i.

Conversely, as the following lemma shows, A is ALM iff it is LMS in $(K, +, \cdot, A)$.

Lemma 3.5.8. *Let $A \subseteq K^n$, K an algebraically closed field. Then A_{zar} is stably embedded in $(K, +, \cdot, A)$.*

Proof. Let (K', A') be a saturated model of $Th((K, A))$. It suffices to show (cf. [5]) that any automorphism $f : A' \to A'$ (preserving the relations of A'_{zar}) extends to an automorphism of K'. We may first extend f to an automorphism f_L of the field L generated by the coordinates of the points in A'. This is possible since any relations $f(X_1, \ldots, X_n) = 0$, $f \in \mathbb{Z}[X_1, \ldots, X_n]$, restricted to A', form part of A'_{zar} so are respected by f. Let I be a transcendence basis for K' over L; extend $f_L \cup Id_I$ to an automorphism

of $L(I)$. Extending further to the algebraic closure, we obtain an automorphism of K (preserving A'). □

Corollary 3.5.9 (Automatic uniformity). *Let G be an algebraic group over an algebraically closed field K, and let $A \subseteq G(K)$ be ALM. Then it is uniformly ALM: if $U_c \subseteq G$ is an algebraic family of subvarieties of G, then there exist finitely many algebraic subgroups H_i of G, and an integer n, such that for any c, $ZCl(U_c \cap A)$ is a union of at most n cosets of the H_i.*

Proof. If not, then by compactness there exists an elementary extension (A^*, K^*) of (A, K), and $c \in K^*$, such that $ZCl(U_c \cap A^*)$ is not a finite union of cosets of K-definable subgroups of G. But any basic relation of $(A^*)_{zar}$, i.e. $U \cap (A^*)_{zar}$ with U defined over the prime field, is a Boolean combination of cosets of subgroups. Hence by quantifier elimination for Abelian structures, every definable relation of $(A^*)_{zar}$ is a Boolean combination of cosets of subgroups. Now by stable embeddedness, $U_c \cap A^*$ is definable in $(A^*)_{zar}$ (with parameters), so it is a Boolean combination of cosets of subgroups. By Hrushovski and Pillay [15], these subgroups are A-definable (indeed $acl(\emptyset)$-definable in $(A^*)_{zar}$, so their Zariski closures are K-definable. So $ZCl(U_c \cap A^*)$ is a finite union of cosets of K-definable subgroups of G after all. □

Products with ALM groups: Algebraic modularity is not in general inherited by products. For instance, let $(a_i : i = 1, 2, \ldots)$ be algebraically independent over $\mathbb{Q}$. Let Γ_1 be the multiplicative group generated by the a_i. Then Γ_1 is easily seen to be ALM (directly, or using the results of the next section, embedding it in a group of the form $\sigma(x) = x^2$). Let $b_i = a_i + 1$. Then $(b_i : i = 1, 2, \ldots)$ are also algebraically independent over $\mathbb{Q}$, so the group Γ_2 generated by them is ALM. However, $\Gamma_1 \times \Gamma_2$ is not ALM; the graph of addition by 1 is not a group subvariety of G_m^2, yet it meets $\Gamma_1 \times \Gamma_2$ in a Zariski dense subset.

In the above example, $(\Gamma_1 \times \Gamma_2)_{zar}$ is superstable, with locally modular regular types. But this is not always the case, and even when it is, without finite rank it will not serve our purposes. We thus proceed to make a stronger statement in the context of difference fields. It is an application of the material of this section, but requires a preliminary remark on transformal degree.

Lemma 3.5.10. *Let B be a variety, $E \subseteq B \times \cdots \times B^{\sigma^k}$ a subvariety with $\dim(E) \leqslant k$. Then $H = \{b \in B : (b, \sigma(b), \ldots, \sigma^k(b)) \in E\}$ has transformal degree $\leqslant k$. Conversely, if Y is a definable set of transformal degree $\leqslant k$, then $ZCl(\{(y, \sigma(y), \ldots, \sigma^k(y)) : y \in Y\})$ has dimension $\leqslant k$.*

Proof. Say E, B are K-definable, K a difference field, and let $b \in H$. Then

$$tr.\deg._K K(b, \sigma(b), \ldots, \sigma^k(b)) \leqslant \dim(E) \leqslant k.$$

So $tr.\deg_K K(b,\sigma(b),\ldots,\sigma^{i-1}(b)) = tr.\deg_K K(b,\sigma(b),\ldots,\sigma^{i}(b))$ for some $i \leqslant k$, and

$$\sigma^i(b) \in K(b,\sigma(b),\ldots,\sigma^{i-1}(b))^a.$$

Applying σ, transitivity of algebraic closure, and induction, we have

$$\sigma^j(b) \in K(b,\sigma(b),\ldots,\sigma^{i-1}(b))^a \quad \text{for all } j \geqslant i.$$

Thus $tr.\deg_K K(b,\sigma(b),\ldots) \leqslant k$. □

Lemma 3.5.11. *Let $\mathbb{U} = (\mathbb{U},\sigma)$ be a universal domain for difference fields. H, G be commutative algebraic groups over $\mathbb{U}$. Let B be an LMS definable subgroup of G, of finite transformal degree d. Assume V is a definable subset of $H \times G$, whose projection to G is finite-to-one. Let E be a subgroup of H, not necessarily definable, such that $E \times \sigma(E) \times \cdots \times \sigma^d(E)$ is 1-ALM. Let $X \subseteq ((E \times B) \cap V)$. Then $ZCl(X)$ is a finite union of cosets of group subvarieties.*

Proof. We will show that X is a union of finitely many pieces, each contained in an LMS group. Since LMS groups are ALM, the lemma will follow. First:

Claim. *$V \cap (E \times B)$ is contained in a finite union of cosets of definable groups of finite $S1$-rank.*

Proof. Let $Z = ZCl(\{(b,\sigma(b),\ldots,\sigma^d(b)) : b \in B\})$. Then $\dim(Z) \leqslant d$. Write V^* for

$$\left\{((a_0,\ldots,a_d),(b_0,\ldots,b_d)) : \bigwedge_{0 \leqslant i \leqslant d} (a_i,b_i) \in V^{\sigma^i}\right\}.$$

Also write H^* for $H \times H^\sigma \times \cdots \times H^{\sigma^d}$, G^* for $G \times G^\sigma \times \cdots \times G^{\sigma^d}$, E^* for $E \times \sigma(E) \times \cdots \times \sigma^d(E)$. Let $\tilde{Z} = (H^* \times Z) \cap V^*$. As $V^* \to G^*$ is finite-to-one (by the assumption on V), $\tilde{Z} \to Z$ is finite-to-one, so $\dim(\tilde{Z}) \leqslant \dim(Z) = d$. Let $V(Z)$ be the projection to H^* of $\tilde{Z}$. So $V(Z)$ is a constructible set, and $\dim V(Z) \leqslant \dim Z = d$. Since E^* is 1-ALM, $ZCl(V(Z) \cap E^*)$ is a finite union of cosets F_i of group subvarieties. As $F_i \subseteq V(Z)$, $\dim(F_i) \leqslant d$. By Lemma 3.5.10, $\bar{F}_i = \{x : (x,\sigma(x),\ldots,\sigma^d(x)) \in F_i\}$ is a finite $S1$-rank coset. It remains only to show that if $(a,b) \in V \cap (E \times B)$, then $a \in \bar{F}_i$ for some i. (So that $V \cap (E \times B) \subseteq \bigcup_i (\bar{F}_i \times B)$).) Let $(a,b) \in V \cap (E \times B)$. Then

$$(a,\sigma(a),\ldots,\sigma^d(a)),(b,\sigma(b),\ldots,\sigma^d(b)) \in (H^* \times Z) \cap V^*.$$

So $(a,\sigma(a),\ldots,\sigma^d(a)) \in V(Z)$. But $a \in E$, so $(a,\sigma(a),\ldots,\sigma^d(a)) \in D^*$. Thus $(a,\sigma(a),\ldots,\sigma^d(a)) \in F_i$ for some i. So $a \in \bar{F}_i$, proving the claim.

By Lemma 3.2.3, there exist a finite number of definable sets P_i and definable groups H_i, with cosets $(H_i + c_i)$, such that $Z = \bigcup_{i=1}^{l} P_i$, $P_i \subseteq (H_i + c_i)$, and $(P_i P_i^{-1})^{l_i} = H_i$. It suffices to consider separately each piece $P_i \subseteq (H_i + c_i)$. We have $P_i \subseteq V \cap (E \times B) \subseteq acl(B)$, so $H_i \subseteq acl(B)$. Now B is a definable LMS group of finite rank. By Proposition 4.0.4, H_i is also LMS. Hence so are $(H_i + c_i)$ and $(H_i + c_i) \times B$. Since the union of these last covers $V \cap (E \times B)$, and hence X, the lemma is proved. □

3.6. Orthogonality and domination

The following result generalizes Proposition 4.4 of [14]. We will make no stability assumptions here of any kind. We take the structures to be saturated. We consider Abelian groups, and write them additively.

Let P, Q be two definable sets within the same structure. The strongest orthogonality assumption on P, Q in the definable category is that for any n, any 0-definable subset of $P^n \times Q^n$ is a finite union of rectangles $D \times D'$, with $D \subseteq P^n$ and $D' \subseteq Q^n$ 0-definable. (It follows that P, Q are stably embedded.) It is easily seen that this condition is inherited by subsets and quotients under definable equivalence relations. Let us call this complete orthogonality.

Given two completely orthogonal definable Abelian groups A, B, the induced structure on the product $A \times B$ is known; we wish to understand the possible definable relations on nonsplit definable extensions of B by A. Let $0 \to A \to G \to_\pi B \to 0$ be an exact sequence of definable groups and homomorphisms.

One possibility is a homomorphic section $f : B \to G$ of $\pi : G \to B$ (so that G is definably split). One may also have a partial section $f : Y \to G$, with $Y \subseteq B$. In this case let us say that f is (*affine*) *homomorphic* if f extends to an affine homomorphism on the coset $\langle Y \rangle$ generated by Y; equivalently, if there exists a subgroup H of B and a homomorphic section $h : H \to G$, such that $f(y) - h(y)$ is constant on Y.

Equivalently, for $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n$, with $\sum_i m_i = 0$, let $Y(m) = \{(y_1, \ldots, y_n) \in Y^n : \sum m_i y_i = 0\}$. Define

$$f_{*m} : Y(m) \to A$$

by

$$f_{*m}(y_1, \ldots, y_n) = \sum m_i f(y_i).$$

(By applying π, one sees that f indeed goes into A.) Then f is affine-homomorphic iff $f_{*m} = 0$, for all m.

Say that f is *almost homomorphic* if f_{*m} has finite image, for all m as above. Equivalently (in a universal domain), there exists a countable subgroup Δ of G, such that the composition $Y \to G \to (G/\Delta)$ extends to an affine homomorphism $\langle Y \rangle \to (G/\Delta)$.

If f is an almost homomorphic section, we will also say that the image S of f is an *approximately homomorphic section*. Note that S determines f.

If Δ can be taken to be a *finite* subgroup of G, we will call S a *virtually homomorphic section*. Any definable subset of A, or of a coset of A, is also a definable subset of G.

One can take sums of subsets of A, and approximately homomorphic sections of the previous types. One can also do this modulo a subgroup of A. We thus arrive at the following definition: If N is a definable subgroup of A, we have an induced definable exact sequence, $0 \to (A/N) \to (G/N) \to B \to 0$. If T a definable subset of A/N, $S \subseteq (G/N)$ an approximately (virtually) homomorphic section, then the pullback to G of $S + T$ is called an *approximate* (*virtual*) *rectangle*.

Proposition 3.6.1. *Let* $0 \to A \to G \to_\pi B \to 0$ *be an exact sequence of* 0*-definable Abelian groups and maps in a given saturated structure. Assume* A *is stably embedded in* G*, and* A, B *are completely orthogonal. Then every definable subset of* G *is a finite union of approximate rectangles.*

If moreover the conclusion of Lemma 3.2.3 *holds for* G*, then every definable subset of* G *is a finite union of virtual rectangles.*

Proof. Let X be a definable subset of G. For $b \in B$, let $A(b) = \pi^{-1}(b)$, a coset of A.

Claim. *There exists a finite partition of* B *into definable sets* B_i*, and definable sets* $S_i \subseteq A$*, such that for* $b \in B_i$,

$(*)$ *For some* $g \in A(b)$, $A(b) \cap X = S_i + g$.

Proof. For each type q of elements of B, pick $b = b_q$ realizing q, and also pick $g \in A(b)$. Let $S_q = \{c \in A : g + c \in X\}$. Then

$(*_q)$ For some $g \in A(b_q)$, $A(b_q) \cap X = S_q + g$.

As S_q is a subset of A and A is stably embedded, it is definable over some $C_q \subseteq A$. By complete orthogonality, q implies a complete type over C_q. Thus $(*)$ remains true if b_q is replaced by any realization of q. So

$(**)$ For any $b \in B$, for some q, for some $g \in A(b_q)$, $A(b) \cap X = S_q + g$.

By compactness, finitely many of the S_q suffice. This proves the claim. □

Partitioning X according to $\pi^{-1}(B_i)$, it suffices to show the conclusion for each piece; thus we may assume $X \subseteq \pi^{-1}(B_1)$; and even, shrinking B_1 now, that $\pi(X) = B_1$. Let $S = S_1$. So $X \cap A(b) = S + g$, some g. Let $K = \{c \in A : c + S = S\}$. K is a definable subgroup of A. We have also $c + X = X$ for $c \in K$. So X is the pullback of a definable subset of G/K; and by passing to the quotient, we may assume $K = 0$.

Now if $S + g = S + g'$, then $g - g' \in A$ (otherwise, $S + g$ and $S + g'$ will be in different cosets of A) so $g - g' \in K = 1$. Thus we have a definable map

$$f : B_1 \to G,$$

$f(b) = g$ iff $A(b) \cap X = S + g$.

f is a section of the natural projection $(G/K) \to (G/A) = B$; we denote this projection too by π.

Now let f_{*m} be as in the definition of an approximate homomorphism. It is a map from B_1^n into A/K. By complete orthogonality, the graph of f_{*m} is a finite union of rectangles. But functions contain only 1×1 rectangles. So the image of f_{*m} must be finite. Thus f is an approximate homomorphism. If Y is the image of f, then $S + Y = X$. This proves the lemma in the general case.

Assuming the conclusion of the Indecomposability Theorem 3.2.3, apply it to $Y = f(B_1) \subseteq G$. This gives a partition of Y; by partitioning X further, we may assume $B_1 = \pi(Y)$ is contained in a single coset of $J = \pi(H)$, H a definable subgroup of G; and generated by sums of elements from Y.

All the required properties of X hold, except that we must still show that K is a subgroup of finite index of $H \cap A$ (i.e. with our assumption $K = 0$, that $H \cap A$ is finite).

Note that each element of J is an alternating sum of $2n$ elements of B_1. Let $R \subseteq J \times G$ be the relation:

$$R(c,b) \text{ iff there are } a_1,\ldots,a_{2n} \in B_1 \text{ with } c = \sum_{0 \leqslant i \leqslant 2n-1} (-1)^i a_i$$

$$\text{and } b = \sum 0 \leqslant i \leqslant 2n-1 (-1)^i f(a_i).$$

Then for each $c \in J$ there are finitely many $b \in G$ with $R(c,b)$.

Let W be the subgroup of A generated by $\bigcup_m f_{*m}(C_m)$. Then W is a countable group. f extends to a well defined map $\bar{f}: J \to G/W$, namely

$$\bar{f}\left(\sum (-1)^i a_i\right) = \sum (-1)^i f(a_i).$$

Moreover, $\bar{f}$ is a group homomorphism.

Let $E = (\bar{f})^{-1}(((H \cap A) + W)/W)$. $\bar{f}$ induces an isomorphism between $E/\ker(\bar{f})$ and $((H \cap A) + W)/W$. The graph of this isomorphism is the image of the definable relation R, after factoring out the possibly nondefinable subgroup W. The orthogonality condition (ii) applied to R shows immediately that $E/\ker(\bar{f})$ and $((H \cap A) + W)/W$ must be finite. Hence $(H \cap A)/K$ is at most countable, so being definable it is finite, as required. □

We include also the analog of the socle lemma, Proposition 4.3 of [14]. Here we use stabilizers in the sense of theories of finite $S1$-rank [5]. This lemma will not be used in our application.

Proposition 3.6.2. *Let G be a definable Abelian group of finite $S1$-rank, in some structure. Let A be definable subgroup, X a definable subset of G. Assume*:

(i) *Every $acl(G/A)$-definable subgroup of A is commensurable to an $acl(0)$-definable subgroup.*

(ii) *G has no definable subgroup A' containing A with A'/A infinite and $A' \subseteq acl(Y, A, C)$ for some rank-one Y and finite C.*

(iii) *For any complete type $X' \subseteq X$ over an algebraically closed set, $Stab(X') \cap A$ is finite.*

Then X is contained in finitely many cosets of A, up to a set of smaller rank.

Proof. Using compactness, we may replace X by a complete type over an algebraically closed base set C; we must show that X is contained in a single coset of A. Let $X/A = \{x + A: x \in X\}$. For $b \in (X/A)$, let $A(b)$ be b viewed as a coset of A. Let b be an element of X/A. Then $X(b) = X \cap A(b) \neq \emptyset$. As X is the solution set of $tp(a/C)$ for $a \in X(b)$, and $b \in dcl(Ca)$, $X(b)$ is the solution set of a complete type over $C \cup \{b\}$. Let X_1 be the solution set of some type over $acl(Cb)$, extending this type.

The stabilizer S of X_1 with respect to the action of A on $A(b)$ is an $acl(Cb)$-definable subgroup of A. By (i), S is commensurable to a C-definable group $S_0 \subseteq A$. Now a generic element of $S \cap S_0$ is independent from b over C, and hence is in the stabilizer of X_1. But by (iii), this stabilizer is finite. Thus S is finite. In particular S does not have finite index in A (A is infinite, using (ii), letting $A' \subseteq G$ be generated by a rank-one Y). It follows that some finite intersection of A-translates of X_1 is nonempty and finite. A little combinatorics will show that some finite intersection U of A-translates of $X(b)$ is nonempty and finite.

Since U is defined over $\{b\} \cup A$, we have $U \subseteq acl(b, A)$. Every element of $A(b)$ has the form $a + x$ for some $a \in A$, $x \in U$, so $A(b) \subseteq acl(b, A)$. If $rk(b) = 0$, then X/A is finite, and being complete, it consists of a single element; in other words X is contained in a single coset. Otherwise, we will get a contradiction. Find $F = acl(F)$ so that $rk(b/F) = 1$, and let Y be the locus of b over F, and $X' = \{x \in X : x + A \in Y\}$. Then $A(b) \subseteq acl(b, A)$ for $b \in Y$, so $X' \subseteq acl(Y \cup A)$. By the lemma on finite generation, Lemma 3.2.1, for some finite m, $\{\sum n_i y_i : (y_1, \ldots, y_m) \in Y^m, (n_1, \ldots, n_m) \in Z^m, \sum_i n_i = 0\}$ is a subgroup of G/A. So $\{a + \sum n_i b_i : a \in A, (b_1, \ldots, b_m) \in X'^m, (n_1, \ldots, n_m) \in Z^m, \sum_i n_i = 0\}$ is a subgroup of G, and evidently it contains A and is contained in $dcl(A \cup X') \subseteq acl(Y \cup A)$. This contradicts assumption (ii).

4. Groups in difference fields

The Abelian groups definable in difference fields can be described in detail. We will concentrate on finite rank subgroups of Abelian varieties; this is where the new minimal sets come in. It is also the only case that will play a role in our number theoretic application. We will however point out the new phenomena among definable groups of finite index of other kinds; enough so, we hope, to make an exhaustive classification straightforward.

From now on (and for the rest of the paper), definable groups are definable in a universal domain for difference fields. Note that [5] one has elimination of imaginaries; so there is no difference between the category of definable groups, and the apparently more general one of intepretable groups (taken with full induced structure). In particular, the quotient of a definable group by a definable subgroup is definably isomorphic to a definable group.

Proposition 4.0.3. *Let A be an algebraic group, not necessarily commutative. Every definable subgroup of A is contained as a subgroup of finite index in a group of the form*:

$$\{a \in A : (a, \sigma a, \ldots, \sigma^n a) \in S\},$$

where S is a Zariski closed subgroup of $A \times \cdots \times A^{\sigma^n}$.

Proof. Let $A_n = A \times A^{\sigma} \times \cdots \times A^{\sigma^{n-1}}$. Let H be a definable subgroup of A. Let S_n be the Zariski closure in A_n of $\{(a, \sigma(a), \ldots, \sigma^{n-1}(a)) : a \in H\}$. Let $H_n = \{a \in A : (a, \sigma(a), \ldots, \sigma^{n-1}(a)) \in S_n\}$, $H' = \bigcap_n H_n$. Then H' is an ∞-definable subgroup of A, and $H \subseteq H'$. Let p' be a generic type of H' over some substructure C', and let p be an extension of p' to a bigger set C, with p generic over C in a coset of H. Suppose the index $[H' : H]$ is infinite; then $SU(p) < SU(p')$; p is a forking extension of p'. It follows by Chatzidakis and Hrushovski [5] that if a realizes p over C, then $(a, \sigma(a), \sigma^2(a), \ldots)$ forks with C over C', in the sense of fields. However $(a, \sigma(a), \ldots, \sigma^{n-1}(a))$ is a generic point over C' of S_n; and S_n is defined over C'; a contradiction. Thus $[H' : H]$ is finite. By compactness, for some n, $[H_n : H]$ is finite. □

Proposition 4.0.4. *Let E be a definable group. Then there exists a definable map of E into an algebraic group A, with finite kernel.*

We mention the proposition here as background, but will not require it; we give the ideas of the proof in passing. Here is a somewhat more general statement.

Proposition. *Let $\mathbb{U}$ be a saturated structure of finite $S1$-rank with stable reduct $\mathbb{U}'$. Assume that for algebraically closed $A, B \subseteq \mathbb{U}$, $C = A \cap B$,*
(1) $acl_{\mathbb{U}}(A \cup B) = acl_{\mathbb{U}'}(A \cup B)$.
(2) *A, B are independent over C in $\mathbb{U}$ iff they are independent in $\mathbb{U}'$.*
Then every $\mathbb{U}$-definable group admits a $\mathbb{U}$-definable homomorphism on an ∞-definable subgroup of bounded index, into a $\mathbb{U}'$-definable group, with finite kernel.

The proof below (as opposed to the statement) was known in the late 1980s, as an application of the then-new technology of $*$-definable groups. (The compactness argument at the end may be due to Pillay; at all events it was discussed in a phone conversation with him around 1988.) A $*$-type is a type in infinitely many variables; in the stable framework, essentially all techniques with types go through verbatim for $*$-types, and in particular this is true of the algebraic group configuration (cf. [2]).The second salient fact is that a $*$-definable group is pro-definable, (cf. [12]).

Proof. Let G be a $\mathbb{U}$-definable group. For a type $p = tp(c)$ of an element $c \in G$, let c^* enumerate $acl(c)$, and let $p^* = tp(c^*)$. If a, b are independent generics of G, let $c = ab$. Then a^*, b^*, c^* are algebraically dependent in pairs, but independent in pairs, as sequences in $\mathbb{U}'$. By the group configuration, there exists a $*$-definable group H^* in $\mathbb{U}$, with elements α, β, γ equi-algebraic with a, b, c (in eponymous pairs). Let $P = tp(b, \beta)$. So $P \subseteq G \times H$. Let S be the stabilizer. Left multiplication by (a, α) stabilizes P into $tp(c, \gamma)$; composing with the inverse of a generic conjugate of (a, α), one concludes that the stabilizer S of P contains a generic element (d, δ), with $d \in G$ generic; and $acl(d) = acl(\delta)$. It follows that S projects to G and to H^* with bounded kernel; and the projection $f : S \to G$ has image $K = f(S)$ of bounded index.

We may factor out the bounded, infinitely definable (=pro-finite) group of S, the kernel of the projection to G. Then we get a well-defined map $s: K \to H^*$, with graph S; it has bounded kernel.

Now recall that H^* is a projective limit of a definable projective system (H_i, h_{ij}) of definable groups and maps in $\mathbb{U}'$; we have $h_i: H^* \to H_i$. Then by compactness, for some i, $h_i \circ s$ has bounded, i.e. finite kernel. □

Remark. (1) The assumption of finite $S1$-rank is used only to make use of the theory of group generics and stabilizers. The proof is thus valid in any context in which these are available.

(2) In a finite $S1$-rank theory, an ∞-definable group is an intersection of definable groups (unpublished preprint "On PAC and related structures"). Using this and some cosmetics, the conclusion of the proposition can be improved to: *every $\mathbb{U}'$-definable group admits a $\mathbb{U}'$-definable homomorphism into a $\mathbb{U}$-definable group, with finite kernel.*

Lemma 4.0.1. *Let G be a definable group, defined over a finite or countable set C, and suppose any two elements of B have distinct types over $C \cup k$, $k = \mathrm{Fix}(\sigma)$. Then there exists a definable homomorphism $\gamma: G \to H(k)$, H a k-algebraic group, γ injective, with γG of finite index in $H(k)$.*

Proof. By Chatzidakis and Hrushovski [5], every type over k is definable (k is stably embedded). Hence any element of G is in $dcl(C \cup k)$. By compactness, there is a finite definable partition of G into subsets G_i, and definable surjective maps $f_i: R_i \to G_i$, with R_i a definable subset of k^{n_i}. Now the relations induced on the R_i by pulling back the graph of multiplication are definable over k; this uses again the stable embeddedness of k. Putting the pieces back together, and it follows that G is definably isomorphic to a definable group G' over k. Now every definable group over k has the stated form, by Hrushovski and Pillay [15]. □

Lemma 4.0.2. *Let G be a definable group, defined over a set C_0. Suppose $C_0 \subseteq C$, C a finite or countable set, and every element of G is algebraic over $C \cup k$. Then there exists a definable homomorphism $\gamma: G \to H(k)$, H a k-algebraic group, $\ker\gamma$ finite, with γG of finite index in $H(k)$.*

Proof. By Corollary 3.3.6 G has a finite normal subgroup K with G/K internal to k. By Lemma 4.0.1, G/K is of the required form. □

Remark 4.0.3. In Lemma 4.0.2, one can take $\ker\gamma$ to be C_0-definable (but not necessarily γ itself).

Proof. Let $\gamma: G \to H(k)$ be as in the conclusion of Lemma 4.0.2. Let $K = \ker(\gamma)$. Let $K^* = \bigcap \{\tau(K): \tau \in Aut(U/C_0)\}$, where U is the universal domain. Then $K^* \subseteq K$ so K^* is finite. It is $Aut(U/C_0)$-invariant, hence is C_0-definable. By finiteness, $K^* = \bigcap_{i=1,\ldots,m} \tau_i(K)$ for some $\tau_1, \ldots, \tau_m \in Aut(U/C)$. Let $h_i: G \to H_i(k)$ be the conjugate of $h: G \to$

$H(k)$ by τ_i. Let $h^* = (h_1, \ldots, h_m)$. Then clearly h^* has kernel K^*. The image of h^* need not of course be of finite index in the product of the H_i, but is isomorphic to a subgroup of finite index of some $H^*(k)$, using again the result in [16]. □

Lemma 4.0.4. *Let G be a definable group, defined over a set C_0. Suppose $C_0 \subseteq C$, C a finite or countable set, and every element of G is algebraic over $C \cup D$, where D is a stable, stably embedded, 1-based definable set of finite rank (e.g. an LMS group). Then G is LMS.*

Proof. By Corollary 3.3.6, G a finite normal subgroup K with G/K internal to D. So G/K and, certainly, K are LMS. Thus by Proposition 3.4.1, G is LMS. □

4.1. Abelian varieties

We seek to classify the definable subgroups of finite rank of an Abelian variety A. We refer here to definability in the language of difference fields; in particular, equations may use σ as a primitive operation. For more details we refer the reader to [5]. We will also use the notion of the ($S1$-)rank of a definable set from [5]; it is a kind of dimension theory. It is convenient to work in the universal domain.

We begin with a classification up to commensurability.

Notation 4.1.1. Let A be a semi-Abelian variety. We let $End(A)$ be the group of endomorphisms of A given by rational maps. We let $E(A) = \mathbb{Q} \otimes End(A)$.

$E(A)$ is a semisimple Artin ring; if A is a simple Abelian variety, then $E(A)$ is a division ring.

Definition 4.1.2. A definable group B will be called *c-minimal* if B is infinite, and every infinite definable subgroup of B has finite index in B.

Definition 4.1.3. If E is a ring, and σ is an automorphism of E, we let E_σ be the ring of formal finite sums $\sum_i e_i t^i$, where the index i ranges over $\mathbf{Z}$, and $e_i = 0$ for almost all i. Multiplication is defined using the commutation rule: $ta = \sigma(a)t$ for $a \in E$.

Lemma 4.1.4. *Let E be a division ring, σ an automorphism of E, $E' = E_\sigma$. Then every left ideal of E' is principal.*

Proof. E' is the direct sum of Et^n. Let E^+ be the sum of Et^n for $n \geqslant 0$. Then E^+ is a subring of E'; if I is an ideal of E^+, then $I^+ = I \cap E^+$ is an ideal of E^+, and I is generated by I^+. Thus it suffices to prove the result for E^+. We define $\deg(\sum_{i \leqslant n} a_i t^i) = n$ where $a_n \neq 0$. The standard proof of the (left) Euclidean algorithm goes through. If I is a left ideal and f is an element of least degree in I, and $g \in I$, then $g = rf + s$ with $s = 0$ or $\deg(s) < \deg(f)$ by the Euclidean algorithm, so $s \in I$ and hence $\deg(s) \geqslant \deg(f)$, so $s = 0$. Thus $I = E^+ f$. □

Lemma 4.1.5. *Suppose A is a simple Abelian variety, and for all n, A and A^{σ^n} are not isogenous Abelian varieties. Then every σ-definable subgroup of A is commensurable to a Zariski closed subgroup.*

Proof. Immediate from Lemma 4.0.3; since every Zariski closed subgroup S of $A \times \cdots \times \sigma^n A$ is commensurable to a product of Zariski closed subgroups of the $\sigma^i A$. □

Lemma 4.1.6. *Suppose A_i is a simple Abelian variety, with no A_i isogenous to $\sigma^k A_j$ unless $i = j$. Then every σ-definable subgroup of $\Pi_i A_i$ is commensurable to a product of σ-definable subgroups of A_i.*

Proof. Similar to the previous Lemma 4.1.5. □

Lemma 4.1.7. *Let A, E be Abelian varieties, A simple, E isogenous to A^n, and let B be a definable subgroup of E. Then there exist definable homomorphisms $F_j : E \to \sigma^{m(j)} A$ such that B is a subgroup of finite index of $\bigcap_{i=1,\ldots,l} Ker(F_i)$. For each j, F_j has the following form. There exist L_{ring}-definable homomorphisms $h_{jk} : E^{\sigma^k} \to A^{\sigma^{m(j)}}$ such that $F_j(e) = \sum_k (h_{jk}\sigma^k(e)))$.*

Proof. By Remark 4.0.3 B is a finite index subgroup of $\{a \in E\colon (a, \sigma a, \ldots, \sigma^m a) \in S\}$ where S is a Zariski closed subgroup of $E \times \cdots \times \sigma^m E$. By Poincaré complete reducibility, S is a finite index subgroup of the kernel of some homomorphism, or of the joint kernel of some homomorphisms on $E \times \cdots \times \sigma^m E$ into simple Abelian varieties. Thus there exist algebraically definable homomorphisms F_j into $\sigma^{m(j)} A$ such that B is a subgroup of finite index of $\{a \in E\colon F_j(a, \sigma a, \ldots, \sigma^m a) = 0$ for each $j\}$. The lemma follows upon decomposing F_j into a sum of components. □

Notation 4.1.8. Let A be a definable, divisible Abelian group. We let $End^*(A)$ denote the ring of definable endomorphisms of A, and $E^*(A) = \mathbb{Q} \otimes End^*(A)$.

Lemma 4.1.9. *Let A be an Abelian variety. Let*

$$A \simeq \prod_{i=1,\ldots,m} \prod_{j=1,\ldots,n_i} B_{ij},$$

where $\simeq$ denotes isogeny, each B_{ij} is isogenous to some $\sigma^{j'}$-conjugate of A_i, and where for $i \neq i'$ and $j, j' \geqslant 0$, $(A_i)^{\sigma^j} \not\simeq (A_{i'})^{\sigma^{j'}}$. (Thus the A_i are representatives for the equivalence relation generated by isogeny and σ-conjugacy, and the n_i is the multiplicity of A_i in A for this notion.) Then

$$E^*(A) \simeq \prod_{1 \leqslant i \leqslant m} M_{n_i} E^*(A_i).$$

Proof. This follows easily from Lemma 4.1.6; it will not be used, except as motivation for considering the case of A simple. □

Proposition 4.1.1 (Structure of $E^*(A)$). *Let A be a simple Abelian variety. Then*:
(1) *$E(A)$ is a division ring.*
(2) *If A is simple, and A and $\sigma^n A$ are non-isogenous for all n, then $E^*(A) = E(A)$. Suppose now that A is simple, and A and $\sigma^n A$ are isogenous for some n. Then*
(3) *$E^*(A)$ admits a $\mathbf{Z}$-grading. $E(A)$ is the homogeneous component of degree 0. If τ is any homogeneous element of degree 1, then τ is invertible, and the homogeneous component of degree n is $\tau^n E(A) = E(A)\tau^n$. In particular $E(A)$ is stabilized by conjugation by τ, and $E^*(A)$ is generated as a ring by $(E(A), \tau, \tau^{-1})$. The powers of τ are linearly independent over $E(A)$. Thus $E^*(A)$ is isomorphic to $E(A)_\tau$ defined in Definition* 4.1.3, *where τ acts on $E(A)$ by conjugation.*
(4) *Every definable subgroup of A is commensurable to the kernel of a definable endomorphism of A.*
(5) *B is a C-minimal subgroup (up to commensurability) iff B is commensurable to $Ker(h)$ with h a left-irreducible element of $E^*(A)$*
(6) *Any nonzero definable endomorphism of A is surjective.*

Proof. Conditions (1) and (2) have already been noted. For the rest, let n be least such that A and $\sigma^n A$ are isogenous, and fix an isogeny h from A to $\sigma^n A$, and an isogeny h' from $\sigma^n A$ to A, such that $h'h = [m]$ (where $[m]$ is multiplication by an integer m). We have $hh'(hx) = h(mx) = mh(x)$ so as h is onto, $hh' = [m]$. Mapping g to $(1/m)hgh'$ gives an isomorphism γ between $E(A)$ and $E(\sigma^n A)$; the choice of h, h' affects γ only up to conjugation. (If $A = A^{\sigma^n}$, it is natural to choose $h = h' = Id$.)

Let $\tau = h'\sigma^n$; it is a definable endomorphism of A. Let $\tau' = \sigma^{-n}h$. We have $\tau\tau' = \tau'\tau = [m]$.

We will show that $E^*(A)$ is generated by $E(A)$ and τ, τ'. For now let $E'(A)$ be the ring generated by $End(A)$ and τ, τ', and let $E''(A)$ be the ring of endomorphisms e of A such that $Me \in E'(A)$ for some M. So $E'(A) \subseteq E''(A) \subseteq \mathbb{Q} \otimes E'(A) \subseteq E^*(A)$.

Claim 1. *Let $r : \sigma^k A \to \sigma^l A$ be an algebraic homomorphism. Then $\sigma^{-l} r \sigma^k \in E''(A)$. It is a homogeneous element, i.e. a product of a power of τ or τ' with an element of $E(A)$.*

Proof. If $r = 0$ the statement is trivial. Otherwise $\sigma^k A$, $\sigma^l A$ are isogenous, so $k = l \bmod n$. We use induction on $|k - l|$. If $k = l$, then $\sigma^{-l} r \sigma^k = \sigma^{-l}(r) \in E(A)$. Say $k < l$ (otherwise use τ instead of τ'). We have $\sigma^k(h') : \sigma^{k+n} A \to \sigma^k A$. Let $r' : \sigma^{k+n} A \to \sigma^l A$, $r' = r\sigma^k(h')$. By induction,

(i) $\sigma^{-l} r' \sigma^{k+n} = \sigma^{-l} r \sigma^k(h') \sigma^{k+n}$ is a homogeneous element of $E''(A)$. On the other hand, consider σ as an automorphism of the structure including itself, and allow applying it to definable functions in this structure. Then $\sigma^{-n}\sigma^k(h) = \sigma^k(\sigma^{-n}h) = \sigma^k(\tau')$ so

(ii) $\sigma^{-k-n}\sigma^k(h)\sigma^k = \sigma^{-k}\sigma^k(\tau')\sigma^k = \tau'$.

Multiplying (i) and (ii), the claim follows.

Now if $F_j : A^p \to \sigma^{m(j)} A$ is an endomorphism as in Lemma 4.1.7, then each of the summands of $\sigma^{-m(j)} F_j : A^p \to A$ mentioned in Lemma 4.1.7 is of the form appearing in

the Claim, hence can be viewed as an element of $E''(A)$; thus $\sigma^{-m(j)}F_j = s_j$ for some $s_j \in E''(A)$, and $Ker(F_j) = Ker(s_j)$. We conclude. □

Claim 2. *Every definable subgroup of A^p is commensurable with one defined by a finite number of $E''(A)$-linear equations.*

Claim 3. *An element of $E''(A)$ is a unit in $\mathbb{Q} \otimes E''(A)$ iff it has finite kernel.*

Proof. Suppose $g \in E''(A)$ is not invertible in $\mathbb{Q} \otimes E''(A)$. Then it is not a homogeneous element. So after multiplying by a power of τ, it can be written as $\sum_{i=0}^{p} a_i \tau^i$, with $a_0 \neq 0$ and $a_p \neq 0$, $p > 0$. Opening up the definition of τ and multiplying out, we can also write $g = \sum_{i=0}^{p} b_i \sigma^i$, where b_i is a definable homomorphism from $\sigma^i A$ to A, and $b_0 \neq 0$, $b_p \neq 0$. Let C be the principal component of the subgroup of $A \times \cdots \times A^{\sigma^p}$ defined by $\sum b_i x_i = 0$, and let $S = \{((x_0, \ldots, x_p), (y_0, \ldots, y_p)) \in C \times \sigma C : x_1 = y_0,\ x_2 = y_1, \ldots, x_p = y_{p-1}\}$. Then S projects onto C and onto σC, using the surjectiveness of b_0 and b_p. Thus by the axioms of model completeness, Lemma 2.2.1, there are infinitely many $x \in C$ with $(x, \sigma x) \in S$. This implies that $Ker(g)$ is infinite. The other direction is trivial, since ker[n] is finite for all n.

The same argument shows that the map from $E(A)_\tau$ of Definition 4.1.3 to $\mathbb{Q} \otimes E'(A)$ is injective, hence an isomorphism. By Claim 2 with $p = 1$, every definable subgroup B of A is commensurable with one of the form $\{a \in A : s_i a = 0,\ i = 1, \ldots, q\}$. However, by Lemma 4.1.4, the left ideal of $\mathbb{Q} \otimes E''(A)$ generated by $\{s_1, \ldots, s_q\}$ is generated by a single element s. We may replace s by Ms with $Ms \in E''(A)$; then $B \sim Ker(Ms)$. This proves (4).

Claim 4. *Every definable endomorphism of A is in $E''(A)$.*

Proof. Let e be a definable endomorphism of A, and let E be the graph of e, a subgroup of A^2. Consider

$$I_2 = \{(f, g) \in E''(A)^2 : f(x) + g(y) = 0 \text{ for any } (x, y) \in E\}.$$

This is a submodule of $E''(A)^2$. By Claim 2, $E \sim \bigcap_j \{(x, y) : f_j(x) + g_j(y) = 0\}$ for certain $(f_j, g_j) \in I_2$. Let I be the second projection of I_2, an ideal of $E''(A)$. We claim that $\mathbb{Q} \otimes I$ is the unit ideal of $\mathbb{Q} \otimes E''(A)$. Otherwise, $\mathbb{Q} \otimes I$ is generated by some g which is not a unit, hence by Claim 3 has infinite kernel K. Each g_j is a multiple of g in $\mathbb{Q} \otimes E''(A)$. If $a \in K$, then $g_j(a) = 0$ for each j, so a subgroup of finite index of $(0) \times K$ is contained in E. This contradicts the fact that E is the graph of a homomorphism. Thus $1 \in \mathbb{Q} \otimes I$, so $M \in I$ for some integer M. Thus for some $f \in E''(A)$, $f(x) + My = 0$ for all $(x, y) \in E$. So $Me(x) = f(x)$, hence $Me \in E''(A)$, and so $e \in E''(A)$.

Condition (3) follows from Claim 4.

Claim 5. *Let $f, g \in E''(A)$. Then $Ker(f) \leqslant \sim Ker(g)$ iff for some $h \in \mathbb{Q} \otimes E''(A)$, $g = hf$.*

Proof. One direction is evident. For the other, we may assume upon multiplying by an integer that $Ker(f) \subseteq Ker(g)$. Thusone may define an endomorphism h of A by $g(x) = h(f(x))$. By Claim 4, $h \in E''(A)$.

Proof of (5) and (6). The inclusion ordering on definable subgroups of A, up to commensurability, is now known to be isomorphic to the divisibility ordering on elements of $\mathbb{Q} \otimes E''(A)$. Thus (5) is immediate. For (6), suppose f is a definable endomorphism. Then $Im(f) \sim Ker(g)$ for some g. So $ngf = 0$ for some $n \neq 0$. But the ring $E^*(A)$ has no zero-divisors, so $f = 0$ or $g = 0$. In the latter case, f is surjective. □

Remark 4.1.10. A semi-Abelian variety S has only countably many definable subgroups.

Proof. By Proposition 4.0.3, any subgroup of S is commensurable to one determined by an algebraic subgroup of $S \times \cdots \times S^{\sigma^n}$ for some n. It is well known that there are at most countably many algebraic subgroups of a semi-Abelian variety (any such subgroup is the Zariski closure of the torsion points within it). Thus there are countably many definable subgroups up to commensurability. If H is a definable subgroup of S, for any n, the map $x \mapsto nx$ has finite kernel on H; so nH has the same rank as H; so $[H : nH]$ is finite; thus H has finitely many subgroups of index n. Similarly, S/H has only finitely many torsion points of order N, so H has only finitely many supergroups of index n. Thus there countably many definable subgroups altogether. □

Lemma 4.1.11. *Let A be a simple Abelian variety.*

(a) *Let $D^*(A)$ be the ring of definable homomorphisms $A \to A/T$, where T is a definable subgroup of A of finite rank. One identifies h with πh if $h : A \to A/T$, $T \subseteq T'$, and $\pi : A/T \to A/T'$ is the natural projection. Then with the natural addition and multiplication, $D^*(A)$ is a division ring. $E^*(A)$ embeds into $D^*(A)$. Every element of $D^*(A)$ can be written as fg^{-1} with $f, g \in E^*(A)$ (or alternatively as $f^{-1}g$).*

(b) *$E^*(A)$ is an Ore ring: for any $f, g \in E^*(A) - (0)$, for some $u, v \in E^*(A) - (0)$, $gu = fv$.*

Proof. The fact that $D^*(A)$ is a division ring is immediate, by defining inverses. The fact that every element of $D^*(A)$ is a quotient of elements of $E^*(A)$ can be shown as in Claim 4 of Definition 4.1.2. Condition (b) follows formally. □

Lemma 4.1.12. *Let A be an Abelian variety, B a definable subgroup of finite rank. Then B is LMS iff every c-minimal definable subgroup of gB is LMS, for any $g \in E^*(A)$. If $B = Ker(f), f = f_1 \cdot \ldots \cdot f_r f_i \in E^*(A)$ irreducible, then B is LMS iff $Ker(f_i)$ is LMS for each i.*

Proof. This reduces easily to the case of simple A. Let $E^*(A)$ be the ring of definable endomorphisms of A, tensor $\mathbb{Q}$. By Proposition 4.1.1 we have $B \sim Ker(f)$ for some $f \in E^*(A)$. If f is a unit there is nothing to prove. Otherwise we use induction (say

Noetherian induction on the left ideal generated by f, or on the rank of B). If $f = gh$, with h not a unit, then $Ker(h) \subseteq Ker(f)$. If $hB \subseteq B$, we are done using the exact sequence

$$0 \to Ker(h) \to B \to hB \to 0.$$

Otherwise we have the definable exact sequence

$$0 \to Ker(h) \to B \cap h^{-1}B \to B \to gB \to 0.$$

In this sequence, the map $Ker(h) \to B \cap h^{-1}B$ is the inclusion. The next map is given by h. The next is given by g. One has $gh = 0$ on B. One must also verify that if $x \in B$, $g(x) = 0$, then $x = h(y)$ for some $y \in B$. By Proposition 4.1.1(6), we have $x = h(y)$ for some y; and $f(y) = gh(y) = g(x) = 0$, so $y \in B$. Thus the sequence is indeed exact. Now g annihilates $Ker\, h$, so gB has smaller dimension than B. On the other hand hB has smaller dimension than B since $0 \neq Ker\, h \subseteq B$, and we assumed that $hB \not\subseteq B$, so $\dim(B \cap h^{-1}B) < \dim(B)$. In either case we are done by Propostion 3.4.1 and induction. □

Proposition 4.1.2 (Structure of c-minimal subgroups). *Let A be a simple Abelian variety, B a c-minimal definable subgroup of A (up to commensurability).*

(a) *Precisely one of the following cases occurs*:
  (i) $B = A$.
  (ii) *B is definably isomorphic to a subgroup of finite index of $H(k)$, $k = \mathrm{Fix}(\sigma)$, H a k-algebraic group.*
  (iii) *B is LMS, of U-rank one.*

(b) *Case* (i) *occurs iff A is not isogenous to A^{σ^n} for any $n > 0$. Case* (iii) *occurs if A is isogenous to A^{σ^n} for some $n > 0$, but not isomorphic to an Abelian variety A' defined over* $\mathrm{Fix}(\sigma^n)$ *for some $n > 0$.*
Thus we may assume A is defined over $\mathrm{Fix}(\sigma^n)$.

(c) *Suppose A is defined over* $\mathrm{Fix}(\sigma^n)$. *Then B is not LMS if and only if $B \subseteq Ker(\sigma^N - 1)$ for some N (with $n|N$).*

(d) *Suppose B is a c-minimal definable subgroup of the multiplicative group G_m. Then* (c) *holds*: *B is not LMS if and only if $B \subseteq Ker(\sigma^n - 1)$ for some n.*

Proof. If A is not isogenous to A^{σ^n} for any n, we have already shown that A has no proper definable subgroups. Conversely, if A is isogenous to A^{σ^n}, say via an isogeny f, then one cannot have $B = A$ since for example $\{a: \sigma^n(a) = f(a)\}$ is a smaller subgroup; and it is clear that any B must have finite rank. Suppose from now on that indeed B has finite rank. If B is LMS, then it has U-rank one since every infinite LMS group has a rank one definable subgroup, and B is c-minimal. Suppose B is not LMS; we must show that A is isomorphic to an Abelian variety A' defined over $\mathrm{Fix}(\sigma^n)$ for some n, and that (c) holds. Choose a base C such that A,B are defined over C, and there is a minimal type $X \subseteq B$, also over C. By Lemma 3.2.2, X generates (in boundedly many steps) a coset of an infinitely-definable subgroup B' of B, and B' is the intersection

of countably many definable subgroups of B (each, by c-minimality, of finite index in B). Further every type of B is a translate of some type of B'. Now if X were locally modular, then so would be B', and hence B. Thus X is not, and so by the trichotomy theorem for minimal types, there exists a definable finite-to-one map $h: X \to \mathrm{Fix}(\sigma)$ (defined over some finite C). Since every element of B' is a finite sum of elements of X, every element of B' is algebraic over $C \cup k$. Enlarging C so as to include coset representatives for B/B' (at most continuum), $B \subseteq acl(C \cup k)$. By Lemma 4.0.2, there exists an isogeny between B and a definable subgroup of finite index of $H'(k)$, with H' an algebraic group over k.

Choose H' a k_1-algebraic group of least possible dimension, such that k_1 is a finite extension of k, and with B definably isogenous to a subgroup of $H'(k_1)$. Then it is clear that H' is a definably simple commutative algebraic group (if it has proper subgroups, enter them or factor them out). The existence of the isogeny between B and a subgroup of H', together with Lemma 4.1.6, shows that some conjugate of H' by a power of σ is isogenous to A as an Abelian variety. Thus A is isomorphic to H''/F for some H'' defined over a finite extension of k, and some finite subgroup F of H''; so A is isomorphic to an Abelian variety defined over a finite extension of k.

Finally, to prove (c) and (d), suppose A is defined over $k_1 = \mathrm{Fix}(\sigma^n)$. If $B \subseteq Ker(\sigma^N - 1)$ for some N (with $n|N$), then $B \subseteq A(\mathrm{Fix}(\sigma^N))$, and it is clear that there exists a finite-to-one map of B into k, and B is not LMS. Conversely, if B is not LMS, then we saw that there exists a definable isogeny $h: B \to H(k_1)$ (perhaps after enlarging k_1). The isogeny h can be viewed as a definable subgroup of $A \times H$, and by Remark 4.1.10 there are only countably many such subgroups; hence h is defined over some finite extension k_2 of k_1. If $[k_2 : k]$ divides N, then clearly every point of $B/Ker(h)$ is fixed by σ^N. Say $Ker(h)$ has order m; then

$$\sigma^N(x) = x(\mathrm{mod}\, Ker(h))$$

for every $x \in B$, so mx is fixed by σ^N, and since mB has finite index in B, every point of B is fixed by some power of σ^N; thus enlarging N if necessary, B is fixed pointwise by σ^N. □

Corollary 4.1.13. *Let A be a semi-Abelian variety, defined over* $\mathrm{Fix}(\sigma)$. *Let $p(T)$ be a polynomial with integer coefficients. Then $Ker(p(\sigma))$ is LMS iff p has no cyclotomic factors, i.e. iff $p(\omega) \neq 0$ for ω a root of unity.*

Proof. Suppose first that p has a cyclotomic factor q. Then $Ker(q(\sigma)) \subseteq Ker(p(\sigma))$. But $Ker(q(\sigma))$ is contained in some finite extension of the fixed field, i.e. in $Ker(\sigma^n - 1)$ for some n. So $Ker(q(\sigma))$ is not LMS, hence $Ker(p)$ is not either.

For the other direction, we may assume A is a simple Abelian variety, or G_m. Suppose $Ker(p)$ is not LMS. Write $f = p(\sigma) = f_1 \cdot \ldots \cdot f_r$, $f_i \in E^*(A)$ irreducible. Then by Lemma 4.1.12, $Ker(f_i)$ is not LMS for some i. By Proposition 4.1.2, $Ker(f_i) \subseteq Ker(\sigma^N - 1)$ for some N. We may choose N large enough so that all endomorphisms of A as a semi-Abelian variety are defined over $\mathrm{Fix}(\sigma^N)$. By Proposition 4.1.1(3),

$C = Ker(\sigma^N - 1)$ is a submodule of A with respect to the action of $E^*(A)$. Let R be the ring $E^*(A)$ modulo the kernel of this action. Since $p(T)$ has no cyclotomic factors, $p, T^N - 1$ are relatively prime in $\mathbb{Q}[T]$, so p is invertible in $\mathbb{Q}[T]/(T^N - 1)$, and hence $f = p(\sigma)$ is invertible in R. However, $Ker(f_i)$ has nonzero rank, and is contained in C. Thus $rank(f_i(C)) < rank(C)$, and so $rank(f_1 \cdot \ldots \cdot f_r(C)) < rank(C)$, contradicting the invertibility. □

Corollary 4.1.14. *Let $M \in M_n(\mathbb{Z}) \cap GL_n(\mathbb{Q})$. Let A be a semi-Abelian variety defined over $Fix(\sigma)$, with group law written additively. Let M act on A^n by matrix multiplication. Let $A_M = \{a \in A^n : \sigma(a) = Ma\}$. Then A_M is LMS if the characteristic polynomial of M has no roots of unity among its zeroes.*

Proof. Let $\pi_i : A^n \to A$ be the ith projection, $E_i = \pi_i A_M$. Then A_M is LMS iff each such E_i is LMS. Now σ acts on A_M and on E_i, and the projection is σ-invariant. Let p be the characteristic polynomial of M. Then $p(\sigma) = 0$ on A_M, hence also on E_i. Thus the minimal polynomial p_i satisfied by σ on E_i divides p. So if p has no root of unity roots, neither does p_i, and each E_i is LMS. Conversely, if p does have a root of unity root, then so does the minimal polynomial satisfied by σ, and since this polynomial divides $\Pi_i p_i$, so does some p_i. This reduces the situation to Corollary 4.1.13. □

4.2. Extensions of Abelian varieties by vector groups

We begin by observing that the finite $S1$-rank definable subgroups of vector groups are all finite-dimensional vector spaces over the fixed field k, hence are not locally modular. (This is the only point that we believe to be really different in positive characteristic; there some of the definable groups appear to be locally modular, though unstable.) We then note new phenomena occurring inside extensions of Abelian varieties by vector groups. We will find there, in particular, definable groups containing a k-space as a subgroup, with LMS quotient. We will describe the definable subgroups of $\tilde{A}$, the maximal extension of A by a vector group. Arbitrary extensions of A by a vector group can be viewed as a direct sum of vector groups, and of quotients of $\tilde{A}$ by vector subgroups; so the entire situation is determined by what happens within $\tilde{A}$.

Definition 4.2.1. We say that an algebraic group G is a vector group if it also admits an algebraic vector space structure; equivalently G is isomorphic to G_a^n for some n.

A definable group E of finite rank is a vector group if it admits a definable vector space structure over the fixed field k.

Lemma 4.2.2. *Every finite rank definable subgroup of a vector group G_a^m is non-orthogonal to the fixed field k, and indeed is a finite-dimensional k-space. A finite rank definable group is a vector group iff it embeds into an algebraic vector group.*

Proof. If B is a definable subgroup of G_a^m, then $\{a: aB \subseteq B\}$ is a definable subring containing the integers, hence containing k. Conversely, if B admits a definable vector space structure over k, let S be the semi-direct product of k and B. By Lemma 4.0.4 there exists a definable group homomorphism $\rho: S \to H$, H an algebraic group, with finite kernel. However there are no finite normal subgroups of B, so ρ is injective on B, and one sees that the Zariski closure of $\rho(B)$ is an algebraic vector group. □

Let A be an Abelian variety. We are interested in exact sequences

$$0 \to L \to G \to A \to 0$$

with L a vector group; sometimes we will write G when we have the whole exact sequence in mind.

Definition 4.2.3. Let $0 \to L \to G \to A \to 0$ be exact, and let $h: L \to L'$ be a homomorphism. We define $h(G)$ and an exact sequence

$$0 \to L' \to h(G) \to A \to 0$$

as follows. Let $H = \{(h(x), -x): x \in L\} \subseteq L' \times G$. Let $h(G) = (L' \times G)/H$. Define a map $L' \to h(G)$ by sending $x \in L'$ to $(x, 0)/H$. Define a map $h(G) \to A$ by $(x, y)/H \mapsto \pi(y)$. We also have a natural morphism $G \to h(G)$, given by $x \mapsto (0, x)/H$.

Lemma 4.2.4. *There exists an exact sequence*

$$0 \to L \to \tilde{A} \to_{\pi_A} A \to 0$$

With L a vector group, with the following universal property: For any extension

$$0 \to L' \to G' \to A \to 0$$

there exists a unique homomorphism h from the $\tilde{A}$ exact sequence to the G' exact sequence, above the identity on A. We have $h = (h_L, h, Id_A)$; and $G' = h_L(G)$ in the sense of Definition 4.2.3.

Proof (Serre [28])**.** We take $L = H^1(A, \mathcal{O}_A)^*$. Given any $e \in L'^*$, we form $e(G')$, and obtain an element of $H^1(A, \mathcal{O}_A)$. This describes a map $L'^* \to H^1(A, \mathcal{O}_A)$, whose dual is h_L. One shows that $h_L(G) \simeq G'$. Uniqueness of h can be seen by applying Lemma 4.2.5 below: the graph of h is the unique minimal subgroup of $\{(x, y) \in G \times G': \pi(x) = \pi(y)\}$ projecting onto the diagonal of A. □

The map $A \to \tilde{A}$ can be made into a functor; given a homomorphism of Abelian varieties

$$e: A \to B,$$

one can canonically define

$$\tilde{e}: \tilde{A} \to \tilde{B}.$$

Let

$$G' = \{(g, g') \in \tilde{A} \times \tilde{B} : e(\pi_A(g)) = \pi_B(g')\}.$$

Let $L' = (Ker(\pi_A) \times Ker(\pi_B)) \subseteq G'$. Then $0 \to L' \to G' \to_{\pi_A pr_1} A \to 0$ is exact. The universal property of G_a gives a map $h : \tilde{A} \to G'$. We let $\tilde{e} = pr_2 h$.

We can also describe $\tilde{e}$ using the following lemma.

Lemma 4.2.5. *Let $0 \to L \to G \to_\pi A \to 0$ be an exact sequence of algebraic groups, with L linear, and A an Abelian variety. Then there exists a unique minimal $H \subseteq G$ with $\pi(H) = A$.*

Proof. $\pi(H) = A$ iff G/H is a linear group. If H_1, H_2 have this property, so does their intersection $H_1 \cap H_2$. □

Then the graph of $\tilde{e}$ is the unique minimal subgroup of $\tilde{A} \times \tilde{B}$ projecting onto the graph of e. In particular, for any algebraic homomorphism $A \to A^{\sigma^k}$, we get $\tilde{e} : \tilde{A} \to \tilde{A}^{\sigma^k}$.

Using Proposition 4.1.1, we obtain a homomorphism from the definable endomorphisms of A to the definable endomorphisms of $\tilde{A}$: we map $h = \sum e_i \sigma^i$ to $\tilde{h} = \sum \tilde{e}_i \sigma^i$. Finally, if $N = Ker(h)$, we let $\tilde{N} = Ker(\tilde{h})$. It is easy to see that this is well defined; and that $\pi(\tilde{N}) = N$.

The following proposition shows that every definable subgroup of $\tilde{A}$ is the pullback of a subgroup of the vector group $\ker(\pi : \tilde{A} \to A)$, under a certain homomorphism, whose kernel is one of the canonical groups $\tilde{N}$, N a subgroup of A.

Proposition 4.2.1. *Let A be an Abelian variety, $\pi : \tilde{A} \to A$ the maximal vector extension A. Let $N = Ker(h)$ be a definable subgroup of A of finite rank, and let $\tilde{N}$, $\tilde{h}$ be the corresponding subgroup and endomorphism of $\tilde{A}$. Then*:

(1) *$\tilde{N}$ has finite rank. There is an exact sequence*

$$0 \to (L \cap \tilde{N}) \to \tilde{N} \to N \to 0$$

whose kernel $L \cap \tilde{N}$ is a definable vector group.

(2) *There exists a definable exact sequence*

$$0 \to \tilde{N} \to \pi^{-1}(N) \to \ker(\pi) \to 0$$

(3) *$\pi(\tilde{N})$ projects onto N, and is minimal in the following sense*: *Let M be any definable subgroup of G, projecting onto a finite index subgroup of N. Then M contains a subgroup of $\tilde{N}$ of finite index.*

Proof. (1) Is clear.

(2) The map $\tilde{h}$ takes $\pi^{-1}(N)$ to $\pi^{-1}(h(N)) = \pi^{-1}(0) = \ker(\pi)$. The kernel of this map, by definition, is $\tilde{N}$.

(3) Left to the reader; uses Lemma 4.2.5.

4.3. Semi-Abelian varieties

Let A be an Abelian variety. We are interested in extensions

$$0 \to T \to G \to A \to 0$$

with T a multiplicative torus. Let $X(T)$ be the group of rational homomorphisms of T into G_m, defined over an algebraic closure. For $\chi \in X(T)$, we obtain an extension of A by G_m; we pass from G to $\chi(G)$, with the structure of extension of A by G_m defined in Definition 4.2.3. Forgetting the group structure, this can be viewed as a line bundle over A, with the 0-section removed; by [27], the line bundle is algebraically equivalent to 0. We thus obtain an element of $A^*(\mathbb{U})$, where A^* is the dual Abelian variety, and $\mathbb{U}$ is the universal domain. Let $\gamma(G)$ be the set of all elements of $A^*(\mathbb{U})$ obtained in this way, using different χ. This is a finitely generated subgroup of $A^*(\mathbb{U})$, with (at most) $rank(T)$ generators.

Fix a finitely generated torsion free subgroup Γ of $A^*(\mathbb{U})$, and let $\mathcal{G}(\Gamma)$ be the class of extensions G as above with $\gamma(G) \subseteq \Gamma$. This class admits a universal object A_Γ, in the same sense as in the vector case treated above:

Lemma 4.3.1. *There exists an exact sequence in $\mathcal{G}(\Gamma)$,*

$$0 \to T_\Gamma \to A_\Gamma \to_\pi A \to 0$$

with $T_\Gamma = Hom(\Gamma, G_m)$. Given an extension

$$0 \to T' \to G' \to_{\pi'} A \to 0$$

in $\mathcal{G}(\Gamma)$, there exists a unique homomorphism $h : A_\Gamma \to G'$ with $\pi' h = \pi$.

Proof. Let $\{\gamma_i\}$ be a $\mathbb{Z}$-basis for Γ. By Serre [28], there exists a (unique) extension

$$0 \to G_m \to H_i \to_{\pi_i} A \to 0$$

with corresponding line bundle γ_i. Let $A_\Gamma = \Pi_{A,\pi_i} H_i$ be the fiber product. The kernel $T = \Pi_i G_m$ of A should be identified with $Hom(\Gamma, G_m)$. Given $\gamma \in \Gamma$, evaluation at γ gives a homomorphism $e_\gamma : T \to G_m$. We form $e_\gamma(A_\Gamma)$ as in Definition 4.2.3.

Claim. *Let $\gamma \in \Gamma$. Then $e_\gamma(A_\Gamma)$ is the extension of A by G_m corresponding to the element γ of A^*.*

Proof. Let s_i be a rational section of π_i. Let D_i be the corresponding divisor (zero divisor minus polar divisor). Then $(\sigma_1, \ldots, s_k)$ is a section of $\pi : A_\Gamma \to A$. Composing with the projection $A_\Gamma \to e_\gamma(A_\Gamma)$ we obtain a rational section of $e_\gamma(A_\Gamma)$. If $e_\gamma(t_1, \ldots, t_k) = \Pi_i t_i^{m_i}$, then the divisor of s is given by $\sum_i m_i D_i$. Since $\gamma = \sum_i m_i \gamma_i$ within Γ, s corresponds to γ as required.

Now let G' be as in the lemma. Given $\chi \in Hom(T', G_m)$, we obtain as above an extension $\chi(G')$ by G_m, corresponding to an element $\gamma(\chi)$ of Γ. By the claim, we

obtain a surjective map $h_\chi : A_\Gamma \to \chi(G')$, with kernel $Ker(e_\gamma)$. Now if $\chi_1, \ldots, \chi_r$ form a $\mathbb{Z}$-basis of $Hom(T', G_m)$, then the maps $\chi_{i*} : G' \to G'/Ker(\chi)$ induce an isomorphism of G' with the fiber product over A of the groups $G'/Ker(\chi)$. Thus the h_{χ_i} glue together to give a map $h : A_\Gamma \to G'$, with $\pi' h = \pi$.

Uniqueness can be proved as in the vector extension case, using Lemma 4.2.5: the graph of h is the unique minimal subgroup of the pullback to $G_A \times G'$ projecting via (π, π') onto the diagonal of A. □

Remark 4.3.2. (1) In the situation of the lemma, the restriction of h to T_Γ is given as follows: Given $\chi \in Hom(T', G_m)$, we obtain as above $\chi(G')$, an element of Γ. This gives a map $X(T') \to \Gamma = X(T)$. Dualizing we get a map $T_\Gamma \to T'$; this agrees with h.

(2) Torsion points in $A^*(\mathbb{U})$ correspond to extensions by G_m that become trivial upon a base change to an isogenous Abelian variety. Thus by considering only the case of torsion free Γ, we will not miss out any groups.

(3) More generally, let $\Gamma \subseteq \Delta$ be torsion free subgroups of $A^*(\mathbb{U})$. We have a surjective restriction map $i^* : Hom(\Delta, G_m) \to Hom(\Gamma, G_m)$. The following lemma will describe how to extend i^* to a map $A_\Delta \to A_\Gamma$, with the same kernel. If Γ has finite index in Δ, i^* has finite kernel.

(4) The group A_Γ is defined abstractly, but not as a group variety over k; if we choose a $\mathbb{Z}$-basis $b = (b_1, \ldots, b_r)$ for Γ, then A_Γ can be realized as a group variety over $k(b)$; the torus T_Γ can then be identified with G_m^r.

Lemma 4.3.3. *Let $h : A \to A'$ be a homomorphism of algebraic groups. h induces a map $h^* : A'^* \to A^*$, by pulling back line bundles. Let Δ be a finitely generated, torsion free group contained in $h^{*-1}(\Gamma)$. There exists a unique homomorphism of extensions of A: $h_\Gamma : A_\Gamma \to A'_\Delta$. Conversely, if Δ is a finitely generated torsion free subgroup of A'^*, and $g : A_\Gamma \to A'_\Delta$ is a homomorphism of algebraic group extensions of A, then $\Delta \subseteq h^{*-1}(\Gamma)$.*

Proof. First let Δ be a finitely generated torsion free subgroup of A'^*, and $g : A_\Gamma \to A'_\Delta$ a homomorphism compatible with h. Let $\delta \in \Delta$. We wish to show that $h^*(\delta) \in \Gamma$. Let Δ' be the subgroup generated by δ. Composing g with the natural surjection from A'_Δ to $A'_{\Delta'}$ we obtain another homomorphism compatible with h. Thus we may assume Δ is generated by δ. In this case A'_Δ is an extension of A' by G_m, corresponding precisely to $\delta \in A'^*$. Let χ be the restriction of g to the torus T of A_Γ. Then $\chi(A_\Gamma) = A'_\Delta \times_{A',h} A$. As line bundles, $A'_\Delta \times_{A',h} = h^*(A'_\Delta)$. Thus $h^*(\delta) \in \gamma(A_\Gamma) = \Gamma$.

Now assume $\Delta \subseteq h^{*-1}(\Gamma)$. Let $G = A'_\Delta \times_{A',h} A$. G fits into an exact sequence $0 \to T_\Delta \to G \to A \to 0$. We have $G \in \mathscr{G}(\Gamma)$, since $h^*(\delta) \in \Gamma$ for $\delta \in \Delta$. By the universal property, there exists a unique homomorphism $f : A_\Gamma \to G$ compatible with the identity on A, and the map $h^* : \Delta \to \Gamma$. Composing f with the natural map of G in A'_Δ, we obtain the desired homomorphism h_Γ.

For the uniqueness, note first that if $h' : A_\Gamma \to A'_\Delta$ is any homomorphism compatible with h, and $\pi : A_\Gamma \to A$ is the structure map, then $h''(x) = (h'(x), \pi(x))$ defines a

homomorphism of extensions of A $h'' : A_\Gamma \to G$. Thus the uniqueness follows from the corresponding statement for h'' in the universal property. □

The definable subgroups of A_Γ can now be determined in a manner analogous to the case of a vector group extension. We first extend the contravariant duality functor $A \mapsto A^*$ to the category of Abelian variety and definable homomorphisms (rather than just algebraic homomorphisms). To do so, using Claim 4 of Proposition 4.1.1, it suffices to set: $(\sigma^n)^* : A^{\sigma^n} \to A$, $(\sigma^n)^*(x) = \sigma^{-n}(x)$.

Next, if $f : A \to A'$ is a definable homomorphism of Abelian varieties, Γ is a finitely generated torsion free subgroup of A^*, and Δ of A'^*, and $\Delta \subseteq f^{*-1}(\Gamma)$, we construct a definable map $\hat{f}_\Gamma : A_\Gamma \to A'_\Delta$, as follows. We can write $f = e \circ (Id_A, \sigma, \ldots, \sigma^m)$. Let $B = A \times \cdots \times A^{\sigma^m}$, and let $G = A_\Gamma \times \cdots \times A_\Gamma^{\sigma^m}$. Then $G = B_{pr_0^*\Gamma + \cdots + pr_n^*\Gamma^{\sigma^m}}$. By Lemma 4.3.3, the map $e : B \to A'$ lifts to a map $\hat{e} : G \to A'_\Delta$. Let $\hat{f}(x) = \hat{e}((x, \sigma(x), \ldots, \sigma^m(x)))$. The kernels of the maps $\hat{f}$ are (up to commensurability) the definable subgroups of the groups A_Γ. We leave the remaining details to the reader. □

4.4. Mixed structures

If A is a finite rank subgroup of the fixed field, or is LMS, then the structure on A is clear. A bit more remains to be said in the mixed case; in the case of subgroups of vector extensions of Abelian varieties, we saw that a group may have a k-space as a subgroup, with LMS quotient, yet be indecomposable. Similarly, there are subgroups of semi-Abelian varieties with an LMS subgroup, whose quotient is an orthogonal LMS group. In this section we include two lemmas that can be used to determine the structure in such cases. In the case of finite Morley rank, similar results were proved in [14]. Curiously, the "almost-orthogonality" case was important there, and the "full-orthogonality" case was included but not used; here just the opposite situation prevails.

Definition 4.4.1. Let A be a commutative algebraic group. Let V be the maximal vector subgroup of A. By a *special* subvariety of A we will mean one of the form $C + Y$, with C a coset of a connected group subvariety of A, and Y a subvariety of V.

If more generally A is a definable group, B the maximal vector subgroup, a definable subset of A will be called special if it has the form $C + Y$, C a coset of a definable subgroup of A, Y a definable subset of V.

Corollary 4.4.2. *Let A be a commutative algebraic group, assumed for simplicity to be defined over the fixed field* $\mathrm{Fix}(\sigma)$ *in a difference-closed difference field K. Let $F \in \mathbb{Z}[T]$ be an integral polynomial with no cyclotomic factors, and let $G = \{a \in A(K) : F(\sigma)(a) = 0\}$. Then every definable subset of G is a finite Boolean combination of special subsets. If X is a subvariety of A, then the Zariski closure of $G \cap X$ is a finite union of special subvarieties of A.*

Proof. Let $0 \to V \to A \to_\pi B \to 0$ be exact, V the maximal vector subgroup of A, B a semi-Abelian variety. Let $0 \to (V \cap G) \to G \to \bar{B} \to 0$ be the restriction to G. By Corollary 4.1.13, $\bar{B}$ is LMS; on the other hand $V \cap G$ is a definable vector group. Hence, using Lemmas 3.4.8 and 3.4.9, the hypotheses of Proposition 3.6.1 hold for this latter sequence. Moreover, since $\bar{B}$ is stable, the approximate affine homomorphism in the conclusion is an affine homomorphism, and further since B is LMS, the set B_1 in the conclusion is a finite Boolean combination of cosets of group subvarieties of $\bar{B}$. Thus by Proposition 3.6.1, every definable subset of G is a finite Boolean combination of special definable subsets of G. Applying this to $G \cap X$, and taking Zariski closure, we get the desired conclusion. □

We observe that there is little difference between special subvarieties and group subvarieties, as far as the torsion points are concerned.

Lemma 4.4.3. *Let A be a commutative algebraic group over $\mathbb{Q}^a$, T the group of torsion points (or, prime-to-p torsion points) of $A(\mathbb{Q}^a)$, X a subvariety of A. Suppose $X \cap T \subseteq \bigcup_{i=1}^{M} D_i$, where $D_i \subsetneq X$ is a special subvariety of A. Then the Zariski closure of $X \cap T$ is the union of at most M cosets of connected group subvarieties of A.*

Proof. Let D be a special subvariety of A, with $D \cap T \neq \emptyset$. We will show that the Zariski closure Z of $T \cap D$ is a coset of a connected group subvariety of A. Since the Zariski closure of $T \cap X$ equals the union of the Zariski closures of the sets $T \cap D_i$, this will prove the lemma.

Write $D = C + Y$, C a coset of a connected group subvariety E of A, and Y a subvariety of a vector subgroup V of A. Since V is a vector group, there exists a definable endomorphism $\pi : V \to V$ with kernel $V \cap E$, $\pi^2 = \pi$. We have $D = C + Y = C + E + Y = C + E + \pi(Y) = C + \pi(Y)$. Thus replacing Y by $\pi(Y)$ and V by $\pi(V)$, we may assume $E \cap V = (0)$. Pick $d_0 \in (D \cap T)$. For any $d \in (D \cap T)$, let $d' = d - d_0$, $Y' = Y - d_0$. Then $d' \in (E + Y') \cap T$. Write $d' = e + y$, $e \in E$, $y \in Y$. Then $me + my = 0$ for some $m > 0$. So $me = -my \in (E \cap V) = (0)$. Hence $my = 0$ so $y = 0$. Thus $d' = e \in E$, so $d \in E + d_0$. We have shown that $(D \cap T) = (E + d_0) \cap T = (E \cap T) + d_0$, the last equality because d_0 is torsion. Let E' be the Zariski closure of $(E \cap T)$, E_1 the connected component. Since E_1 is divisible, the sequence $0 \to T(E_1) \to T(E) \to T(E/E_1) \to 0$ is exact, so E/E_1 has a finite torsion group, hence is a vector group and actually has no torsion. Thus $E' = E_1$ is connected. The Zariski closure of $(D \cap T)$ is a coset of E_1. □

4.5. Several automorphisms

It is illuminating to trace the local modularity demarcation line in the case of several automorphisms. The results will be obtained in a weak form; algebraic modularity in place of LMS. The stronger form (including stability of the full induced structure) does not hold in the more general context. The present results will be deduced from the ordinary ($r = 1$) case without reopening [5].

In this subsection, we work in a universal domain $\mathbb{U}$ for the theory of fields with r automorphisms, $\sigma_1,\ldots,\sigma_r$. $\mathscr{F}$ denotes the free group generated by $\sigma_1,\ldots,\sigma_r$. If $\tau\in F$, we denote by $(\mathbb{U},\tau)$ the structure consisting of the underlying field of $\mathbb{U}$, and the automorphism τ. It is a universal domain for ordinary difference fields. Write $\mathbb{U}_i=(\mathbb{U},\sigma_i)$.

Recall the action of $\mathscr{F}$ on difference equations. We obtain an induced action on the class of all definable sets, that we denote: $B\mapsto B^\tau$. Also write $B^{\mathscr{F}}=\bigcap_{\tau\in\mathscr{F}}B^\tau$.

In the ordinary case one could indifferently study definable subgroups, or infinitely definable ones; the latter were connected components of definable subgroups. For $r>1$ the situation is different; one must allow infinite intersections of definable subgroups in order to obtain a group of finite rank. It remains true (with the same proof) that every definable group maps into an algebraic one, with finite kernel. Finite rank subgroups of the additive group are vector spaces over the common fixed field k of all the automorphisms. Minimal definable groups thus live (up to isogeny) in simple Abelian varieties, or in G_m, as before.

Finite transformal degree: Consider a simple Abelian variety (or torus) G defined over k. Let $E=\mathbb{Q}\otimes End(G)$. The "twisted" group ring $E[\mathscr{F}]$ is defined in the obvious way, taking into account the action of the σ_i on $End(G)$. (Of course this ring is no longer Euclidean.) Let A be an ∞-definable subgroup of G, of finite transformal degree. Associate to A a left ideal and a two-sided ideal of $E[\mathscr{F}]$:

$I_0(A)=\{r: rA \text{ is finite}\}$,

$I(A)=\{r: rsA \text{ is finite for all } s\in E[\mathscr{F}]\}$,

$R(A)=E[\mathscr{F}]/I(A)$.

Lemma 4.5.1.

- $\dim_E E[\mathscr{F}]/I_0(A)\leqslant\dim(A)$.
- $\dim_{\mathbb{Q}} E[\mathscr{F}]/I(A)\leqslant(\dim(A)\dim_{\mathbb{Q}} E)^2<\infty$.
- *There exists an ∞-definable subgroup B of G, of finite transformal degree, containing A, such that $I_0(B)=I(B)=I(A)$ and $R(A)=E[\mathscr{F}]/I(B)$.*

Proof. Let $d=\dim(A)$. Note first that

$$\dim_{\mathbb{Q}\otimes E} E[\mathscr{F}]/I_0(A)]\leqslant\dim(A).$$

To prove this it suffices to find an E-dependence relation among any $d+1$ elements $h_0,\ldots,h_d\in E[\mathscr{F}]$. Let $h(x)=(h_0(x),\ldots,h_d(x))$ and consider the subgroup $h(A)$ of G^{d+1}. This is a definable subgroup of transformal degree at most d. Thus the Zariski closure has dimension at most d. Using the simplicity of G one obtains an E-linear dependence relation, as in the case $r=1$.

Thus $\dim_{\mathbb{Q}} E[\mathscr{F}]/I_0(A)\leqslant\dim_{\mathbb{Q}}(E)\cdot\dim(A)$.

Let $r_1,\ldots,r_n$ be a $\mathbb{Q}$-basis for $E[\mathscr{F}]/I_0(A)$. Let $B=\sum_{i=1}^n r_i(A)$. If $r\in E[\mathscr{F}]$, then $mr=\sum a_i r_i+s$ with $s(A)$ finite, $m>0$ and $m,a_1,\ldots,a_n\in\mathbb{Z}$. So $mr(A)\subseteq B+s(A)$, i.e. $r(A)\cap B$ has finite index. Thus $r(B)\cap B$ has finite index for any $r\in E[\mathscr{F}]$. Now clearly $I_0(B)=I(B)=I(A)$.

Applying the first item to B, the second follows. □

Proposition 4.5.1. *Let G be a simple Abelian variety defined over k. Let A be a definable subgroup of finite transformal degree*:

1. *If the image of $\mathscr{F}$ in $E[\mathscr{F}]/I(A)^*$ is a finite group, then A is definably isomorphic to an ∞-definable subgroup of $H(k)$, H a k-algebraic group.*
2. *Otherwise, A is algebraically modular. Moreover, every quantifier-free definable subset of A is a Boolean combination of definable cosets.*

Proof. Let $\mathscr{K}$ be the kernel of the homomorphism $\mathscr{F} \to E[\mathscr{F}]/I(A)^*$. If the image of this homomorphism is finite, of order n, then $\mathscr{K}$ is finitely generated, say by $g_1, \ldots, g_m$. By definition, $(1 - g_i)(A)$ is finite; so there exists a subgroup A' of A of finite index in A, such that each g_i fixes A'. Thus $A' \subseteq G(k_n)$ where $k_n = \mathrm{Fix}(\mathscr{K})$, a Galois field extension of k of order n, $k = K^{\mathscr{F}}$ being the total fixed field. By reduction of scalars we obtain the desired statement.

Assume the image $\mathscr{F}$ is infinite. A finitely generated periodic linear group over $\mathbb{Q}$ is finite; hence if the image of $\mathscr{F}$ is infinite, it must contain an element $\bar{\sigma}$ of infinite order. $\bar{\sigma}$ is the image of some σ in $\mathscr{F}$. Now $F(\bar{\sigma}) = 0$ for some $F \in \mathbb{Z}[X]$, and we may take F irreducible in $\mathbb{Q}[X]$. Then F has no cyclotomic factors. The solution set in $\mathbb{U}_1$ of $F(\sigma) = 0$ is ALM, and contains A. Thus A is also ALM.

For the "moreover", as I is a two-sided ideal, $F(\overline{\tau\sigma\tau^{-1}}) = 0$ for any τ. So $A \subseteq Ker\, F(\sigma\tau^{-1})$, and $\tau(A) \subseteq Ker(F(\sigma))$. Thus any finite product of the sets $\tau(A)$ is contained in some power of $Ker(F(\sigma))$, so it is ALM. Consider the many-sorted structure V whose universes are the groups $\tau(A)$, and whose relations are the intersections of subvarieties of G^m with products on m of these. Then V is a many-sorted Abelian structure. Let V' be the result of adding the isomorphisms $\sigma : \tau(A) \to \rho(A)$, for any pair σ, τ and $\rho = \sigma\tau$. These isomorphisms are additive, so V' is still an Abelian structure. Every quantifier-free definable subset of A (in $\mathbb{U}$) is also definable in V', and the conclusion follows. □

It seems likely that if no $\bar{\sigma}$ is a root of unity, $\sigma \neq 1 \in \mathscr{F}$, then A is LMS. In case the image of $\mathscr{F}$ is infinite, but the image of some $\sigma \neq 1$ is a root of unity, A is ALM by Proposition 4.5.1, but one does not have stability.

Problem 4.5.2. Is there an analog of the proposition, for infinitely-definable sets of finite rank, not assumed to carry a group structure?

Products of ALM groups: In the case of one automorphism, arbitrary definable groups could be decomposed into finite rank groups, and algebraic groups; the finite rank theory is thus decisive. Here the situation is more complex; even where the automorphisms commute, one has groups of intermediate orders of magnitude; and beyond that, the theory is not even supersimple. In particular, the finite rank results of the previous paragraph do not yield a classification of all ALM infinitely definable subgroups.

We restrict ourselves to pointing out one class of ALM groups. It consists of groups $A^{\mathscr{F}}$, where A is a definable LMS group in some ordinary reduct $\mathbb{U}_i$, and of their products. The proof that $A^{\mathscr{F}}$ is ALM is the same as that given in the previous paragraph; but the proof that the property holds for products is different, and may be of use in other situations.

Proposition 4.5.2. *Let G_i be a commutative algebraic group over $\mathbb{U}$. Let $k = \mathrm{Fix}(\mathscr{F})$. Let A_i be a $\mathbb{U}_i$-definable subgroup, LMS of finite dimension as such, defined over k. Then $(A_1)^{\mathscr{F}} \times \cdots \times (A_r)^{\mathscr{F}}$ is algebraically modular.*

For notational simplicity, we prove Proposition 4.5.2 in case $r = 2$. But in this case we formulate a sharper statement, paying attention to the number of conjugates used. Assume $r = 2$, and write $\sigma = \sigma_1$, $\tau = \sigma_2$. Then Proposition 4.5.2 follows from Lemma 4.5.3 (keeping in mind the proof of 3.5.6(3)).

Lemma 4.5.3. *Let G_i be a commutative algebraic group over $\mathbb{U}$ $(i = 1, 2)$, G_i defined over $\mathrm{Fix}(\tau_j)$ $(\{i, j\} = \{1, 2\})$, and V a constructible subset of $G_1 \times G_2$. Let A_i be a $\mathbb{U}_i$-definable subgroup of G_i, LMS of finite transformal degree d_i as such.*

Let $E_2 = \bigcap_{n=-d_1}^{d_1} A_2^{\sigma^n}$, $E_1 = \bigcap_{n=0}^{(2d_1+1)d_2} A_1^{\tau^n}$.

Then the Zariski closure of $(E_1 \times E_2) \cap V$ is a finite union of cosets of group subvarieties.

Proof. Assume the data are defined over an algebraically closed difference field K. For $b \in G_2$, let $V(b) = \{a \in G_1 : (a, b) \in V\}$. Let $Z(b) = ZCl(V(b) \cap A_1)$. As A_1 is ALM, $A_1 \cap V(b)$ is a finite union of cosets of $\mathbb{U}_1$-definable subgroups. By Hrushovski and Pillay [15], in a 1-based group, there are no infinite definable families of definable subgroups, so as b varies only finitely many distinct subgroups arise. Thus also upon taking Zariski closure, there exist K-algebraic subgroups $H_1, \ldots, H_l \subseteq G_1$, such that for any $b \in G_2$, $Z(b)$ is a finite union of cosets of the H_i. By Proposition 2.2.1, each such coset is definable over $K(b^{\sigma^{-d_1}}, \ldots, b^{\sigma^{d_1}})^a$. Let $G = G_2^{2d_1+1}$. For $b \in G_2$, let $b^* = (b^{\sigma^{-d_1}}, \ldots, b^{\sigma^{d_1}}) \in G$. Let $\pi((y_{-d_1}, \ldots, y_{d_1})) = y_0$, $\pi : G \to G_2$. By compactness, there exists constructible sets $W_i \subseteq G_1 \times G$ such that for any $b \in G_2$, $Z(b) = \bigcup_i W_i(b^*)$, and for any $y = (y_{-d_1}, \ldots, y_{d_1}) \in G$, $W_i(y)$ is a finite union of cosets of H_i, and $W_i(y) \subseteq V(y_0)$.

So far, we have not used τ at all.

Let $X_i = \{(a, b) \in E_1 \times E_2 : (a, b^*) \in W_i\}$. Then $(E_1 \times E_2) \cap V = \bigcup_i X_i$. So it suffices to prove that $ZCl(X_i)$ is a finite union of cosets of group subvarieties, for each i. Fix one value of i. Let $H = G_1/H_i$, $E =$ the image of E_1 in H, $B = A_2^{2d_1+1} \subseteq G$, $V' =$ image of W_i in $H \times G$, $X = \{(a, b^*) : (a, b) \in X_i\}$. Note that if $b \in E_2$ then $b^* \in B$. Applying Lemma 3.5.11 to this data, and to the automorphism τ (viewing E as a possibly undefinable group of points), we find that $ZCl(X) = \bigcup_j C_j$, with C_j cosets of group subvarieties. Write π also for the map $(Id, \pi) : (G_1 \times G) \to (G_1 \times G_2)$. Then πC_j is a constructible coset of $G_1 \times G_2$ (hence a coset of a group subvariety). We have $X_i = \pi X \subseteq \bigcup_j \pi C_j$. As $X \cap C_j$ is Zariski dense in C_j, $\pi(X \cap C_j)$ is Zariski dense

in πC_j; but $\pi(X \cap C_j) \subseteq (\pi X \cap \pi C_j) = (X_i \cap \pi C_j)$. Thus $ZCl(X_i) = \bigcup \pi C_j$, proving the lemma. □

Let G be an algebraic group defined over $\mathbb{U}$. Say that a subgroup H of $G(\mathbb{U})$ is *difference-algebraically modular* if for any difference-algebraic variety $V \subseteq G^m$, $H \cap V$ is a finite union of cosets. The following remark applies, in particular, to the group obtained in the conclusion of Proposition 4.5.2, and can be used to strengthen that conclusion.

Lemma 4.5.4. *Let G be an algebraic group defined over k. Let H be an $\mathscr{F}$-invariant group, $\sigma_i H \subseteq H$, and suppose H is algebraically modular. Then H is difference-algebraically modular.*

Proof. $V \subseteq G$ be a difference-algebraic variety (it suffices to consider this case, applying it to powers of G and of H). Then for some finite $F \subseteq \mathscr{F}$, and some variety $V' \subseteq G^F$, $V = \{a \in G : a^F \in V'\}$. Now $V' \cap H^F$ is a finite union of cosets, since H is ALM. Thus so is $V \cap H = \{a : a^F \in (V' \cap H^F)\}$. □

4.6. Locally modular subgroups (complements added in proof)

While our main results concern individual locally modular subgroups, we add two remarks on the family of all such subgroups taken together. They are stated for LMS definable subgroups of an Abelian variety, in a universal domain for ordinary difference fields; but should go through in positive characteristic, or with several automorphisms, for ALM groups. This section is not used in the rest of the paper.

Definition 4.6.1. Let A be a semi-Abelian variety defined over a difference field K. Let A_{LM} be the union of all LMS definable subgroups of A.

Remark 4.6.2. By Remark 4.1.10, every definable subgroups of A is commensurable with one defined over K^a, and indeed is a subgroup of finite index of a group defined over K^a. The sum of two LMS groups is LMS (Lemma 3.4.1). Thus if B is LMS and defined over K^a, the sum of conjugates of B is also LMS, and defined over K. So A_{LMS} is a union of k-definable groups. It is moreover a subgroup of A.

If C is an Abelian group, we write $rk_{\mathbb{Q}}(C)$ for the $\mathbb{Q}$-dimension of $C \otimes_{\mathbb{Z}} \mathbb{Q}$.

Lemma 4.6.3. *Let A be a semi-Abelian variety defined over a difference field $K = K^a$. Let L be a difference field extension of K and suppose $tr.\deg_K L = n < \infty$. Then*

$$rk_{\mathbb{Q}}(A_{\mathrm{LM}}(L)/A_{\mathrm{LM}}(K)) \leqslant n \dim_{\mathbb{Q}}(End(A)).$$

Proof. For simplicity of notation, we prove the lemma when A is defined over the fixed field of σ, then comment on the generalization.

Pick $a_1,\dots,a_r \in A_{\mathrm{LM}}(L)$ with $t = tr.\deg_K(a_1,\dots,a_r)$ as large as possible; so $t \leqslant n$. In particular, $\sigma(a_i) \in k(a_1,\dots,a_r)^a$. Each a_i satisfies an equation of the form $m_k\sigma^k(a_i) = \sum_{i<k} e_i\sigma^i(a_i)$, where the e_i are endomorphisms of A, and m_k is an integer. (Reduces to simple case, and there follows from Proposition 4.1.1, and from the fact that $\mathbb{Q}\otimes End(A)$ is a division ring there.)

$U = A_{\mathrm{LM}}(L)/A_{\mathrm{LM}}(K)$ is a divisible Abelian group. Let V be the $\mathbb{Q}\otimes \mathrm{End}(A)$-subspace of U generated by $\{\sigma^k(a_i) : k = 1,2,\dots,\ i = 1,\dots,r\}$. By the above remark, V is finite dimensional (as an $\mathbb{Q}\otimes End(A)$-space, hence as a $\mathbb{Q}$-space).

Let $b \in A_{\mathrm{LM}}(L)$. We will show that $b \in V$; i.e. that $mb = h(a) + e$ for some $h \in Hom(A^r, A)$, $e \in A_{\mathrm{LM}}(K)$, and some integer $m > 0$.

a, b are both part of the same LM group B, of finite rank, and we have $b \in acl_k(a_1,\dots,a_r)$. Thus by LM there exists a definable subgroup $S_0 \subseteq B \times B^r$, and $e \in B(k^a)$, with $S_0 \cap (B \times 0)$ finite, and with $(e + b, a) \in S_0$. So there exists a definable homomorphism $h_0 : B^r \to B$, and an integer $m \neq 0$, with $m(e + b) = h_0(a)$.

This proves the lemma when A is defined over the fixed field. For the general case, one may reduce to $A = G_m$ or A a simple Abelian variety. If A has a finite rank subgroup at all, then A is isogenous to A^τ for some $\tau = \sigma^n$ (take $n > 0$ least possible). An entirely analogous proof then shows that $rk_{\mathbb{Q}}(A_{\mathrm{LM}}(L)/A_{\mathrm{LM}}(K)) \leqslant n \dim_{\mathbb{Q}}(Hom(A, A^\tau))$. But $\mathbb{Q}\otimes Hom(A, A^\tau)$ is a one-dimensional vector space over $\mathbb{Q}\otimes End(A)$, so $\dim_{\mathbb{Q}} \mathbb{Q}\otimes Hom(A, A^\tau) \leqslant \dim_{\mathbb{Q}} \mathbb{Q}\otimes End(A)$. □

Problem 4.6.4. *Suppose A is defined over a difference field K, $tr.\deg_{\mathbb{Q}}(K) < \infty$. Is $rk_{\mathbb{Q}}(A_{\mathrm{LM}}(K))$ finite?*

This problem is analogous to the Manin–Chai theorem of the kernel, for differential fields. We prove the case: A defined over k^a:

Lemma 4.6.5. *Let (L,σ) be a difference field, A a semi-Abelian variety defined over $k = \mathrm{Fix}(\sigma^l)$ for some l. Suppose $tr.\deg_k L = n < \infty$. Then $rk_{\mathbb{Q}}(A_{\mathrm{LM}}(L)) \leqslant n rk_{\mathbb{Q}}(End(A))$. In particular, if $L \subseteq k^a$ then $A_{\mathrm{LM}}(L)$ is torsion.*

Proof. By the relative case, Lemma 4.6.3, it suffices to show that every element of $e \in A_{\mathrm{LM}}(k^a)$ is torsion. This reduces to the case that A is a simple Abelian variety, or G_m. We have $\sigma^l(e) = e$ for some l. So $(\sigma^l - 1)(e) = 0$. e lies in an LMS group B. $F \in End(A)[T]$, $Ker(F(\sigma))$ is commensurable with B; we may assume (replacing F by some nF if necessary) that $B \subseteq Ker(F(\sigma))$. Now $F, T^l - 1$ generate a left ideal I bigger than $E(A)[T]F$, say generated by G. Then $Ker(G(\sigma)) \subseteq Ker(\sigma^l - 1) \cap Ker(F)$; as $Ker(F)$ is LMS, the intersection is finite. So $Ker(G(\sigma))$ is finite, hence $G \in E(A)$; as also $G \in End(A)[T]$, $G \in End(A)$; and $G \neq 0$. Every element g of the ideal I satisfies $g(\sigma)e = 0$. So $Ge = 0$. Now $G \neq 0$, so there exists $G' \in End(A)$, $G'G = m \in \mathbb{Z}\setminus 0$. Thus $me = 0$, hence e is torsion. □

Lemma 4.6.6. *Let A be a commutative algebraic group defined over a difference field $K = K^a$. Let V be a constructible subset of A containing no translates of positive-*

dimensional group subvarieties of A. Then there exists a difference field L of finite transcendence degree over K, such that every point of $V \cap A_{\mathrm{LM}}$, in any difference field extension, lies in $A(L)$.

For simplicity, we stated the lemma in the case when V contains no translates of positive-dimensional group subvarieties of A; in general, $ZCl(V \cap A_{\mathrm{LM}})$ is a finite union of $A(L)$-definable cosets.

Proof. Let L_1 be a finitely generated difference field over K, with V defined over L_1. Note that there is no properly increasing chain $K \subseteq L(1) \subseteq L(2) \ldots$ of relatively algebraically closed difference subfields of $(L_1)^a$. For in such a chain, let $I(n)$ be the ideal of difference polynomials over $L(n)$ vanishing on a given tuple of generators of L_1 over K. If $I(n)$ is generated by $I(n-1)$, it is easy to see that $L(n) = L(n+1)$. Thus we have an increasing chain of prime difference ideals, contradiction. Hence, there exists a maximal algebraically closed difference subfield L of $(L_1)^a$ satisfying $K \subseteq L$ and $tr.\deg._K(L) < \infty$. Now if $c \in A_{\mathrm{LM}} \cap V$, then $c \in B$ for some LM group $B \subseteq A$, and by LM and the assumption on V, $B \cap V$ is finite. So $c \in (L_1)^a$. But $c \in B$, so the difference subfield generated by c over K has finite transcendence degree over K. Thus $c \in L$. □

Putting together Lemmas 4.6.6, 4.6.5, and the theorem of Faltings–McQuillan, we see that if A is a semi-Abelian variety defined over $\mathrm{Fix}(\sigma^n)$, then A_{LM} is Mordellic, i.e. the Zariski closure of any subset of A_{LM} is a finite union of cosets of subgroups. It would be very good to prove this without quoting Faltings' theorem, and to remove the assumption that A is defined over $\mathrm{Fix}(\sigma^n)$.

5. Finding the difference equations

This section contains all the number theory that we will need for the main results. We show there that the torsion points are contained in a group defined by an appropriate difference equation. This equation arises from characteristic equations of Frobenius maps, lifted to characteristic zero.

We begin by fixing a prime p and restricting attention to the group of points of finite order prime to p. We will be able to get bounds on the full group T of torsion points by using two different primes; however our bounds for T'_p are better.

Definition 5.0.7. Let A be a commutative algebraic group.

1. $\dim_m(A)$ is the dimension of the maximal algebraic torus embedded as a subgroup of A.
2. $\dim_{ab}(A)$ is the maximal dimension of an Abelian variety quotient of A.
3. $\dim_r(A) \leqslant \dim(A)$ is defined as follows: let $0 = A_0 \subseteq \cdots \subseteq A_m = A$, with A_i a group subvariety of A over K, and A_{i+1}/A_i a K-simple Abelian variety or torus. Let $\{B_j\}$ be the quotients A_{i+1}/A_i, but choose only one B_j for each K-isogeny type. Let $\dim_r(A) = \sum_j \dim(B_j)$.

Now suppose A is defined over the ring of integers R of a number field K. A prime p of K is a prime of good reduction for A if the following holds. The reduced variety A_k over the residue field $k = R_p/p$ becomes also a commutative, connected algebraic group. Moreover, $\dim_{ab}(A_k) = \dim_{ab}(A)$, and $\dim_m(A_k) = \dim_m(A)$.

Definition 5.0.8. Let p be a rational prime. $T'_p(A)$ denotes the group of points of $A(L)$ of finite order prime to p; where L is some algebraically closed field over which A is defined. If p is a prime of a number field, we will sometimes write $T'_p(A)$ with reference to the residue characteristic of p.

We begin with a well-known result of Weil's concerning Abelian varieties; it generalizes without effort to arbitrary commutative algebraic groups. Fix a prime p, let $k = GF(q)$ be a finite field of characteristic p, and let k^a be an algebraic closure. Let ϕ_q be the q-Frobenius automorphism of k^a.

Lemma 5.0.9. *Let A be a commutative algebraic group over $k = GF(q)$. Then there exists a polynomial $F(T) \in \mathbb{Z}[T]$ with no cyclotomic factors such that $F(\phi_q)$ vanishes on $T'_p(A)$. We have* $\deg(F) \leqslant 2\dim_r(A)$. *The sum of the absolute values of the coefficients of F is at most* $(1 + q^{1/2})^{2\dim_r(A)}$.

Proof. Observe that if f, g are two complex polynomials, and $s(f)$ denotes the sum of the absolute values of the coefficients of f, then $(*)$: $s(fg) \leqslant s(f)s(g)$. This will be used twice. First $(*)$ permits a decomposition of A. Note that there exists over k an exact sequence $0 \to L \to A \to \bar{A} \to 0$, with L a linear algebraic group and $\bar{A}$ an Abelian variety. This gives rise to an exact sequence $0 \to T(L) \to T(A) \to T(\bar{A})$. Thus if $F_1(\phi_q)$ vanishes on $T(L)$ and $F_2(\phi_q)$ vanishes on $T(\bar{A})$, then $F_1F_2(\phi_q)$ vanishes on $T(A)$. This reduces the problem to the three cases of linear tori, commutative unipotent groups, and Abelian varieties. When A is an Abelian variety, the result comes from [31]. Weil actually shows the existence of a monic F of degree $2\dim_r(A)$ whose eigenvalues are all of absolute value $q^{1/2}$, and then we can use the observation $(*)$ above.

When A is an algebraic torus, there exists an isomorphism $g : A \to G_m^n$, defined over a finite field $GF(q^l)$. The Frobenius conjugate $\phi_q(g)$ is another such isomorphism, so $\psi = g \circ \phi_q(g)^{-1}$ is an algebraic automorphism of G_m^n, i.e. $\psi \in GL_n(\mathbb{Z})$. So ψ is fixed by ϕ_q, and

$$\psi^l = \psi \circ \phi_q(\psi) \circ \cdots \circ \phi_q^{l-1}(\psi) = Id$$

using also that g is fixed by ϕ_q^l. Now (A, ψ_q) is isomorphic (via g) to $(G_m^n, g\phi_q g^{-1})$, and $g\phi_q g^{-1}) = \psi \circ \phi_q$. Now $(\psi \circ \phi_q)^l = (\phi_q)^l = \phi_{q^l}$, so the polynomial $T^l - q^l$ works.

When A is a unipotent group, it has no points of finite order prime to p, so the constant polynomial 1 will do. □

To lift this to characteristic zero, suppose now that A is a connected commutative algebraic group over a number field K, and p is a prime of good reduction. Then

$T'_p(A) \subseteq A(L)$, where L is the maximal unramified extension of the completion K_p of K at p. The Frobenius automorphism ϕ_0 of k^a lifts to an automorphism ϕ of L.[4] The reduction map from L to k^a induces an injective map on $T'_p(A)$.[5] It follows that ϕ satisfies the same functional equation on $T'_p(A)$ as ϕ_q does on $T'_p(A_k)$. Thus:

Lemma 5.0.10. *With the above assumptions, there exists an automorphism σ_0 of K^a and an integral polynomial F with no cyclotomic factors, of degree $\dim_r(A)$, absolute coefficient sum bounded by $(1+q^{1/2})^{2\dim_r(A)}$, such that $F(\sigma_0)$ vanishes on the prime-to-p torsion points of A.*

If (L,σ) is any difference field extending (K^a,σ_0), then $F(\sigma)$ vanishes on the prime-to-p torsion points of A, since they all lie in K^a. We may thus embed (K^a,σ_0) in a universal domain (L,σ) for difference fields, and work there.

6. The theorems on torsion points

In this section we prove the number theoretic applications. For the group T'_p of torsion points of order prime to a given prime p (characteristic of a prime of good reduction), we show: (1) T'_p is algebraically modular, i.e. the Manin–Mumford conjecture holds for it; (1^+) The same is true for vector extensions of semi-Abelian varieties; (2) relative version, reducing the Mordell–Lang conjecture for groups of finite $\mathbb{Q}$-rank to Falting's theorem regarding finitely generated groups; (3) For groups over $\mathbb{Q}_p$ with good reduction, the distance of a subvariety to points of T'_p not on it is bounded away from 0. This partially confirms a conjecture of Silverman, Tate, Voloch.

We then show (4) that the bounds in (1)–(3) are effective; in the case of (1) and (2) we write them effectively. They are also uniform when the subvariety varies in an algebraic family, and when the Abelian variety is perturbed p-adically.

Conditions (1), (2) and (4) also follow from results of Faltings, Serre, Raynaud, Hindry, McQuillan, Bost, David, Masser-Wüstholz, as explained in the introduction.

These results will be easy applications of our theory of definable groups in the universal domain for ordinary difference fields. Condition (1) will be an immediate consequence of embedding T'_p in an LMS definable group. For (1^+) and (2), orthogonality is also used. For the effectivity, the general numerical bounds of Section 2 apply. With the intervention of a Robinson-style compactness argument, (3) becomes as easy as (1),

If we wish to extend the results to the group of all torsion points, two routes are available. One is to find an automorphism satisfying an appropriate functional equation

[4] For model theorists, this can be viewed as a consequence of quantifier-elimination for algebraically closed valued fields, in a language with a sort for the residue field; it follows that the residue field is stably embedded, with no additional induced structure.

[5] The tangent bundle of A can be trivialized, using the differentials of the translations. Then at any point a, map $x \mapsto p'x$ induces the map $(x \mapsto p'x)$ on the tangent spaces. It follows that the roots of $p'x = 0$ are simple modulo p).

on all torsion points. This requires more than the elementary number theory we have used so far. If one is willing to quote Serre to show the existence of such an automorphism, results (1), (2) and (4) become equally easy for all torsion points, still using the ordinary theory. (Condition (3) would require a p-adically continuous automorphism of this nature.)

The second route keeps the number theory of this paper at its present primitive level, but uses two automorphisms instead of one. Using this method we prove Manin–Mumford for semi-Abelian varieties (5), and find the explicit bounds (6). Since we have not developed orthogonality beyond the finite rank context, this method does not immediately yield the analogs of (1^+) or (2). We expect these can be done either by an ad hoc extension of the proof, or by developing orthogonality theory, but will be content with (5) and (6).

6.1. Qualitative results

Proposition 6.1.1. *Let A be a semi-Abelian variety defined over a number field K. Let $T = T(A)$ be the group of torsion points of A. For any subvariety $X \subseteq A$, the Zariski closure of $X \cap T$ is a finite union of cosets of group subvarieties of A.*

Proof. Pick two primes of good reduction of A, of distinct residual characteristics p, l. We will treat the group T of all torsion points as a sum $T = T_p' + T_l'$. Choose σ and τ and polynomials F_p, F_l as in Lemma 5.0.9, independently for the two primes p, l; so that $F_p(\sigma)$ vanishes on T_p', and $F_l(\tau)$ vanishes on T_l'. Let $A_p = Ker(F_p(\sigma))$, $A_l = Ker(F_l(\tau))$. Let $\mathscr{F}$ the free group generated by σ, τ. With notation as in Proposition 4.5.2, by Corollary 4.1.13 and Proposition 4.5.2, $A_p^{\mathscr{F}} \times A_l^{\mathscr{F}}$ is algebraically modular. Hence (see Proposition 6.1.1 below) so is $A_p^{\mathscr{F}} + A_l^{\mathscr{F}}$. Since $T_p' \subseteq A_p$ and T_p' is $\mathscr{F}$-invariant, $T_p' \subseteq A_p^{\mathscr{F}}$; and $T_l' \subseteq A_l$, we have $T \subseteq A$. So T is algebraically modular. □

To clarify the relation between $A_p \times A_l$ and $A_p + A_l$, note:

Lemma 6.1.1. *Let X be a subvariety of A,*

$$Y = \{(a, b) \in A^2 : a + b \in X\},$$

$$Z = ZCl(Y \cap (T_p' \times T_l')),$$

$$f : A^2 \to A, \quad f(x, y) = x + y.$$

Then $f(Z) = ZCl(X \cap T)$.

Proof. By the algebraic modularity of $A_p \times A_l$, Z is a finite union of cosets of group subvarieties. For each such coset C, $f(C)$ is a constructible coset, hence is Zariski closed. So $f(Z)$ is Zariski closed. Clearly $(X \cap T) \subseteq f(Z)$; so $ZCl(T \cap X) \subseteq f(Z)$. On the other hand $Y \cap (T_p' \times T_l') \subseteq f^{-1}(X \cap T)$, so $Z \subseteq f^{-1}(ZCl(X \cap T))$, and $f(Z) \subseteq ZCl(X \cap T)$. So they are equal. □

Similarly, one can show:

Proposition 6.1.2. *Let K be a difference field. Let A be a semi-Abelian variety over K. Let T be the group of torsion points of A. Then T is difference-algebraically modular.*

Proof. This can be deduced just as in the proof of Proposition 6.1.1, adding two automorphisms in order to define the torsion points, and quoting Proposition 4.5.2 and Lemma 4.5.4. □

6.2. A second route

In this subsection we assume $(*)$ that S is a semi-Abelian variety over a number field K, that p, l are two primes of good reduction, *and that the fields $K(T_p), K(T_p')$ are linearly disjoint over K*. It follows from Serre's results that this last hypothesis can always be achieved after a finite field extension of K. (And presumably, using [1, 20], the extension can be found effectively if not explicitly.) With the hypothesis in place, we obtain the results of the previous section using one automorphism only. Choose σ and τ and polynomials F_p, F_l in the previous section, so that $F_p(\sigma)$ vanishes on T_p', and $F_l(\tau)$ vanishes on T_l'. Now $T_p \subseteq T_l'$, so $F_l(\tau)$ vanishes on T_p. Using $(*)$, we find a single automorphism ρ of K^a agreeing with σ on T_p', and with τ on T_p. Then $F_p(\rho)$ vanishes on T_p and $F_l(\rho)$ vanishes on T_p'. Let $F = F_p F_l$. Then F vanishes on $T_p + T_p' = T$. And F has no cyclotomic factors.

We obtain:

Proposition 6.2.1. *Assume $(*)$, and let $0 \mapsto U \to A \to S \to 0$ be an extension of S by a vector group. Let V be a subvariety of A. Then the torsion points on V lie on a finite union of torsion translates of group subvarieties of V.*

Proof. Immediate from Corollary 4.4.2 and Lemma 4.4.3. □

Observe that the proposition is equally valid without $(*)$ if one restricts to prime-to-p torsion points.

6.3. Explicit bounds: p'-torsion points

Here is a variant applicable to p'-torsion points on arbitrary commutative algebraic groups (without the assumption $(*)$).

Notation 6.3.1. A is a commutative algebraic group over a number field K. $\mathfrak{p}$ is a prime of K, with residue field $GF(q)$ of characteristic p. $F_q = \sum_i m_i T^i$ is the equation in Lemma 5.0.9. We fix a projective embedding of A; we then obtain an embedding of any subvariety of A^r, in multi-projective space; degrees will refer to this embedding,

as in Section 2. In particular, we have the graph of addition contained in A^3; we refer to the degree of this variety as d_+. Let $d_r = \dim_r(A)$, $D_r = 2d_r + 1$, and

$$S_q = \{(a_0, \ldots, a_{2d_r}) : \Sigma m_i a_i = 0\} \subseteq A^{2d_r+1},$$

$$\tilde{S}_q = \{a \in A) : (a, \sigma(a), \ldots, \sigma^{2d_r}(a)) \in S_q\}.$$

$\tilde{S}_q$ is to be viewed as a difference equation; the points are from a universal domain for difference fields.

Lemma 6.3.2.

- *S_q is a group subvariety of A^{2d_r+1} of dimension $2d_r(\dim A)$.*
- $\deg(S_q) \leqslant d_+^{4d_r(2d_r+1)\log_2(1+q^{1/2})} < d_+^{2D_r^2 \log_2(1+q^{1/2})}$.
- *There exists an automorphism σ of K^a such that $F(\sigma)$ vanishes on T_p', the prime-to-p torsion points of A.*
- *If A is a semi-Abelian variety, $\{a \in A : (a, \ldots, \sigma^{2d_r}(a)) \in S\}$ is LMS.*

Proof. Everything but the bound on degree has been demonstrated. Multiplication by an integer $M \geqslant 2$, in an Abelian group, can be achieved by $\leqslant 2\log_2(M) - 1$ operations of addition or of multiplication by 2 (express M in base 2). Hence a linear polynomial $\sum_{i=0}^{g} m_i x_i = 0$ can be expressed (using additional variables) by means of at most $g + \sum_i (2\log_2(|m_i|) - 1) \leqslant (g+1)^2(\log_2(M))$ additions or subtractions, where $M = \max\{|m_i|, 2\}$.

In our case by Lemma 5.0.9, $M \leqslant (1 + q^{1/2})^{2d_r}$, $g \leqslant 2d_r$, so we can express S_q as a projection of the intersection of

$$(2d_r + 1)2\log_2((1 + q^{1/2})^{2d_r}) = 4d_r(2d_r + 1)\log_2((1 + q^{1/2})$$

varieties of the form $a_j + a_j' = a_j''$. By Lemma 2.1.2(1) and (2), this has degree at most

$$d_+^{4d_r(2d_r+1)\log_2((1+q^{1/2})}. \qquad \square$$

Proposition 6.3.1. *Let A be a connected, commutative algebraic group defined over a number field K. Let* **p** *be a prime of good reduction, with residue field GF(q) of characteristic p. Let T_p' be the group of points of $A(K^a)$ of finite order prime to p. Let X be a subvariety of A. Then the Zariski closure of $X \cap T_p'$ is a union of at most*

$$(\deg(X)^{2d_r+1} d_+^{4d_r(2d_r+1)\log_2(1+q^{1/2})})^{2^{2d_r \dim(X)}}$$

cosets of group subvarieties of A.

Proof. By Corollary 4.4.2, the Zariski closure $X \cap \tilde{S}_q$ is a finite union of a finite number M of special subvarieties of A. By Lemma 4.4.3, the Zariski closure of $X \cap T_p'$ is a union of at most M cosets of group subvarieties of A (necessarily contained in X). It remains only to bound M; i.e. to bound the number of components of the Zariski closure Z of $X \cap \tilde{S}_q$. Let $S = (X \times \cdots \times X^{\sigma^{2d_r}}) \cap S_q$. Then Z is

the Zariski closure of $\{x\colon (x,\sigma(x),\dots,\sigma^{2dr}(x))\in S\}$. By Corollary 2.2.3, Z has a projective embedding of degree at most $\deg(S)^{2^{\dim(S)}}$. We have $\dim(S)\leqslant 2d_r\dim(X)$, $\deg(S)\leqslant \deg(X)^{2d_r+1}\deg(S_q)$. The result follows using Lemma 6.3.2. □

Remark 6.3.3. Assuming $(*)$ of Section 6.2, we obtain a similar bound for all torsion points, using two primes of good reduction but a single automorphism, as in Proposition 6.2.1.

6.4. Explicit bounds: all torsion points

Fix a number field K and a semi-Abelian variety A over K, and a subvariety $X\subseteq A$; X need not be defined over K. We compute the bound arising from Proposition 6.1.1. It is a question of mechanically putting together Lemma 4.5.3, Proposition 2.3.1, and Lemma 5.0.9.

Fix $\mathbf{q}$ and p as in Proposition 6.3.1, and another prime of good reduction $\mathbf{l}$, with residue field $GF(l)$; assume $l\leqslant q$. We let F_q, F_l be the equations as in Lemma 5.0.9, and fix automorphisms σ and τ such that $F_q(\sigma)=0$ on T_p' and $F_l(\tau)=0$ on T_l'. Let Y be as in Proposition 6.1.1. By Proposition 6.1.1, the number of components of $X\cap T$ is at most that of $Y\cap(T_p'\times T_l')$. Let notation be as in Proposition 6.3.1. Let $d_1,d_2\leqslant 2d_r$ be the degrees of F_q,F_l, respectively; and let

$$\Phi=\{\tau^j\sigma^i : -d_1\leqslant i\leqslant d_1, 0\leqslant j\leqslant d_2\}\cup\{\sigma^j\tau^i : 0\leqslant i\leqslant (2d_1+1)d_2, 0\leqslant j\leqslant d_1\}.$$

So Φ is a connected subset of $\mathscr{F}$ of size

$$|\Phi|\leqslant 16(d_r+1)^3.$$

Note that Y is the projection to $A\times A$ of the intersection of the graph of addition on A, with $(\mathbb{P}\times\mathbb{P}\times X)$. Thus

$$\deg(Y)\leqslant \deg(X)d_+.$$

We have as before

$$\deg(S_q)\leqslant {d_+}^{4d_r(2d_r+1)\log_2(1+q^{1/2})}$$

so

$$\deg\left(\prod_{i=0}^{(2d_1+1)d_2} S_q\right)\leqslant {d_+}^{4(2d_1+1)d_2d_r(2d_r+1)\log_2(1+q^{1/2})}\leqslant {d_+}^{16(d_r+1)^4\log_2(1+q^{1/2})}.$$

The last estimate refers to the equations for $E_1=\bigcap_{i=0}^{(2d_1+1)d_2} A_l{}^{\tau^i}$; these amount to the equations for A_l, applied to $\tau^i(x)$ for each i, $0\leqslant i\leqslant(2d_1+1)d_2$.

Similarly, if $E_2=\bigcap_{j=-d_1}^{d_1} A_q^{\sigma^j}$, the corresponding equations have degree

$$\deg\left(\prod_{j=-d_1}^{d_1} S_l\right)\leqslant \deg(S_l)^{2d_1+1}\leqslant 32(d_r+1)^3.$$

Let $S' = \prod_{i=0}^{(2d_1+1)d_2} S_q \times \prod_{j=-d_1}^{d_1} S_l$;

$$\deg(S') \leqslant d_+^{2^9(d_r+1)^7(\log_2(1+q^{1/2}))^2}.$$

Using the estimate $\dim(S') \leqslant |\Phi| \dim(A)$, we get

$$\deg ZCl((E_1 \times E_2) \cap Y) \leqslant \deg(S') \deg(Y)^{2^{|\Phi| \dim(A)}}$$

where each of the terms $\deg(S')$, $\deg(Y)$, $|\Phi|$ is estimated above. By Proposition 4.5.2 and Lemma 4.4.3, this also bounds the number of components of $ZCl((T_p' \times T_l') \cap Y)$, and hence of $ZCl(T \cap X)$. To summarize:

Proposition 6.4.1. *The number of components of $ZCl(T \cap X)$ is at most*

$$d_+^{2^9(d_r+1)^7(\log_2^2(1+q^{1/2}))} \deg(X)^{2^{16(d_r+1)^3 \dim(A)}}.$$

6.5. The relative case; McQuillan's theorem

Let A be a semi-Abelian variety over a number field K, Let

$$\tilde{\Gamma} = \{a \in A(K^a) : ma \in A(K) \text{ for some integer } m\}.$$

The Mordell–Lang conjecture stated that $\tilde{\Gamma}$ is ALM. Raynaud, Hindry and McQuillan reduced it to showing that $A(K)$ is ALM (Faltings' theorem). We wish to show here how to do the same with our methods. If $F(\sigma)(x) = 0$ is an equation capturing the torsion points, $(\sigma - 1)F(\sigma)(x) = 0$ will capture $\tilde{\Gamma}$; and the orthogonality theory applies to $\ker(\sigma - 1), \ker F(\sigma)$.

Pick a prime of K, of good reduction, with residue field k of characteristic p, and let

$$\tilde{\Gamma}_p = \{a \in A(K^a) : ma \in A(K) \text{ for some integer } m \text{ prime to } p\}.$$

For variety, we write the statements for varieties containing no translates of infinite group subvarieties. We first give the statement for the prime-to-p torsion points.

Proposition 6.5.1. *Let A be a semi-Abelian variety over K, $X \subseteq A$ a subvariety of A containing no translates of infinite group subvarieties of A. One can effectively find an integer μ such that $\tilde{\Gamma}_p \cap X(K^a) \subseteq \mu^{-1}A(K)$. Moreover one can effectively find coset representatives r_i of $A(K)/\mu A(K)$, such that $\tilde{\Gamma}_p \cap X(K^a) \subseteq \bigcup_i \mu^{-1}(r_i + \mu A(K))$.*

Pick a prime of K, of good reduction, with residue field k of characteristic p. Let $F = F_p$ be the Weil polynomial; and let σ be a lifting and extension of Frobenius to K^a, so that $F(\sigma)$ vanishes on the group T_p' of prime-to-p torsion points of A. Let

$$\tilde{\Gamma}_p = \{a \in A(K^a) : ma \in A(K) \text{ for some integer } m \text{ prime to } p\}.$$

Lemma 6.5.1. $(\sigma - 1)F(\sigma)$ *vanishes on* $\tilde{\Gamma}_p$.

Proof. $F(\sigma)\tilde{\Gamma}_p$ has no p'-torsion. For let $c = F(\sigma)(b)$, $b \in \Gamma$; $n_1 c = 0$, $(p, n_1) = 1$. We have $n_2 b \in A(K)$ for some n_2 prime to p. σ fixes $n_2 b$, hence

$$0 = n_2 n_1 F(\sigma)(b) = n_1 F(\sigma)(n_2 b) = n_1 F(1) n_2 b$$

so b is torsion. Let r be the maximal power of p dividing $F(1)$. We can write $b = b_1 + b_2$ with $b_1, b_2 \in \tilde{\Gamma}_p$, $b_1 \in T_p'$, and $r b_2 = 0$. Then $F(\sigma)(b_1) = 0$, and $F(1) b_2 = 0$. But also $b_2 \in A(K)$; so $F(\sigma)(b_2) = F(1) b_2 = 0$. Thus $c = F(\sigma)(b) = 0$.

It follows that σ fixes $F(\sigma)\tilde{\Gamma}_p$. For if $c \in F(\sigma)\tilde{\Gamma}_p$, then $nc \in A(K)$ for some n prime to p; so $n(c - \sigma(c)) = nc - \sigma(nc) = 0$, and thus $c - \sigma(c) = 0$. So $(\sigma - 1)$ annihiliates $F(\sigma)\tilde{\Gamma}_p$. □

Lemma 6.5.2. *The* σ*-definable groups* $\ker(\sigma^n - 1)$, $\ker(F(\sigma))$ *are orthogonal. Their intersection consists of finitely many torsion points.*

Proof. $\ker(\sigma^n - 1)$ is internal to the fixed field k, while $\ker(F(\sigma))$ is LMS. Hence they are orthogonal, and in particular have finite intersection; the intersection is a finite subgroup, consisting of torsion points. The last statement is also easy to see directly; both $\sigma^n - 1$ and $F(\sigma)$ vanish on the intersection, hence so does $G(\sigma)$ whenever G is a polynomial of $\mathbb{Z}[T]$ in the ideal generated by F and $T^n - 1$. But some constant polynomial is in this ideal. □

Lemma 6.5.3. $X \cap \ker((\sigma - 1)F(\sigma))$ *is contained in finitely many cosets of* $\ker(\sigma - 1)$.

Proof. Let $h : \ker((\sigma - 1) \times \ker(F(\sigma)) \to \ker((\sigma - 1)F(\sigma))$ be the map $h(x, y) = x + y$. h has finite kernel. $h^{-1}(X)$ is a finite union of rectangles, $U \times V$, by Lemma 3.4.9. Since $\ker(F(\sigma))$ is LMS, V is a Boolean combination of definable cosets; their Zariski closure is a Zariski closed coset contained in X, so by the assumption on X, $h(V)$ is finite. The lemma follows. □

The cosets of $\ker(\sigma - 1)$ have the form $\{a \in A : (\sigma - 1)(a) = \alpha\}$; finitely many α occur in the conclusion of the lemma. Let n_1 be such that $n_1 \alpha = 0$ for each of these α that is torsion. (Actually, we only need that $n_1 p^m \alpha = 0$ for some m; for this, if one is interested in the explicit version, one can take n_1 to be the order of the group $A(k')$, where k' is the field extension of k of degree $[K(\alpha) : K]$.)

Note that if $a \in Ker((\sigma - 1)F(\sigma)) \cap A(K^a)$, and $(\sigma - 1)(a) = \alpha$, then $\alpha \in A(K^a)$, and $F(\sigma)(\alpha) = 0$; it follows by Lemma 6.5.2 that α is torsion. Thus $n_1 \alpha = 0$, so $n_1 a \in \mathrm{Fix}(\sigma)$. We have

$$X \cap \ker((\sigma - 1)F(\sigma)) \cap A(K^a) \subseteq \{x : n_1 x \in \mathrm{Fix}(\sigma)\}.$$

Hence by Proposition 6.5.1

$$n_1(X \cap \tilde{\Gamma}_p) \subseteq \mathrm{Fix}(\sigma).$$

The same proof applies to any automorphism σ' with the same properties as σ; and since we chose a priori difference-field bounds on the finite numbers involved, the same number n applies to all such σ'. Thus

$$n_1(X \cap \tilde{\Gamma}) \subseteq \cap\{\mathrm{Fix}(\tau) : \tau \text{ a conjugate of } \sigma\} = B.$$

Now the group B on the right is invariant under $Aut(K^a/K)$. If $a \in B \cap T_p'$, then the reduction map takes a into $A(k)$ (the fixed field of Frobenius). Let m_p be the order of $A(k)$; then $m_p a$ reduces to 0; since the reduction map is injective on T_p', $m_p a = 0$. So $H = m_p B \cap K^a$ is p'-torsion free, and $Aut(K^a/K)$-invariant. It follows that if $b \in H$, and $mb \in A(K)$, $(m, p) = 1$, then $b \in A(K)$; for b is the unique mth root of mb in H, hence is invariant under $Aut(K^a/K)$. Since every element of $\tilde{\Gamma}_p$ has a p'-multiple in $A(K)$, we obtain:

$$nm_p(X \cap \tilde{\Gamma}_p) \subseteq A(K).$$

This finishes the proof of Proposition 6.5.1. □

Remark 6.5.4. Assuming $(*)$, Proposition 6.5.1 holds also for $\tilde{\Gamma}$.

Proof. Identical, using a single σ-equation capturing all torsion points as in Section 6.2. □

(No doubt a proof can also be given without $(*)$, using two automorphisms.)

6.6. Tate–Voloch conjecture

Tate and Voloch conjectured that the torsion points on an Abelian variety A over $\mathbb{C}_p$ that do not lie on a subvariety $V \subseteq A$, are bounded away from that variety. Certain special cases were proved by Tate–Voloch, and by Buium and Silverman. The proof of the Manin–Mumford conjecture given above lends itself immediately to a proof of the Tate–Voloch conjecture under some restrictions: A must be assumed defined over a finite extension of $\mathbb{Q}_p$; must have good reduction; and the prime-to-p torsion points only are considered. We show this easy deduction here. In later work, using much more p-adic Galois theory, Scanlon removed the last two constraints. See his papers [26] for this and for references to the history of the problem.

Assumptions, Notation. $\mathbb{C}_p$ is the completion of the algebraic closure of $\mathbb{Q}_p$; the ring of integers of L is denoted $\mathcal{O}_{\mathcal{L}}$, the residue field k. $|x|$ is the p-adic absolute value.

L is a finite extension of $\mathbb{Q}_p$. $\mathcal{O}_L$ is the ring of integers of L. k_L the residue field. $K = L^a$ is the field of algebraic numbers.

$\mathcal{S}$ is a group scheme over $\mathcal{O}_L$, with generic and special fibers S and S_p respectively. S is a semi-Abelian variety, and has good reduction in the sense of Lemma 5.0.10.

$$T_p'(S) = \{a \in S(K) : ma = 0 \text{ for some } m, (p, m) = 1\},$$

$$\bar{T} = \{a \in S_p(k) : ma = 0 \text{ for some } m, (p,m) = 1\}.$$

Because of the good reduction assumption, there is a bijective reduction map $r_S : T'_p(S) \to \bar{T}$.

We assume a notion of a distance from a point of A to a subvariety X, such that if $d(a_i, X) \to 0$, then for any affine open U of A, and any f in the affine polynomial ring of U vanishing on X, $|f(a_i)| \to 0$.

Proposition 6.6.1. *Let X be a closed subvariety of S. There exists a bound $b > 0$ such that for $a \in T'_p(S)$, either $a \in X(K)$ or the distance from a to X is $\geqslant b$.*

Proof. By Lemma 5.0.10, there exists an automorphism σ of $K = L^a$ and an integral polynomial F with no cyclotomic factors, such that $F(\sigma_0)$ vanishes on the prime-to-p torsion points of S_p. As the reduction map is injective, $F(\sigma)$ vanishes on S. (#)

By Corollary 4.1.13, $F(\sigma) = 0$ is LMS, and therefore ALM:

Lemma 6.6.1. *Let K be an algebraically closed field of characteristic 0, with an automorphism σ. Let A be a semi-Abelian variety over the fixed field of σ. Let $F \in \mathbb{Z}[T]$ be a polynomial with no cyclotomic factors. Let B be the set of solutions to $F(\sigma) = 0$ in K, and let X be a subvariety of A. Then there are finitely many group subvarieties A_i of A, and cosets Y_i of A_i, defined over K, with $Y_i \subseteq X$, and such that with $Y = \bigcup_i Y_i$,*

$$X \cap B = Y \cap B.$$

Moreover, this remains true if B is replaced by the set of solutions in any difference field (K', σ') extending (K, σ).

Proof. In a universal domain extending (K, σ), the equation $F(\sigma) = 0$ is LMS (Corollary 4.1.13), so the solution set is a finite union of definable subgroups. Let the Y_i be the components of the Zariski closure of these definable subgroups. They are defined over K in the sense of difference fields. Since K is algebraically closed and an inversive difference field, it is also algebraically closed as a difference field [5], so the Y_i are defined over K algebraically. □

Returning to the proof of the proposition, let $a_i \in T'_p(S)$, with $d(a_i, X) \to 0$. We will show that $a_i \in X$ for almost all i. Suppose otherwise, and let U be an ultrafilter, concentrating on the indices i with $a_i \notin X$. Let $R = l^\infty(K)$ be the ring of bounded sequences $(b_0, b_1, \ldots)$ from K. Let

$$I_n = \{r \in R : r = (b_0, b_1, \ldots), \{i : |b_i| \leqslant p^{-n}\} \in U\}, \quad I = \bigcap_n I_n.$$

Then I is an ideal of R. Evidently, σ lifts to R and respects I; so it induces an automorphism of the domain $D = R/I$. It is also easy to see that R/I is a field. (If $r = (b_0, b_1, \ldots) \notin I$, then $r \notin I_n$ for some n, so $|b_i| > p^{-n}$ for $i \in X$, $X \in U$. Letting

$c_i = b_i^{-1}$ for $i \in X$, $c_i = 0$ for $i \notin X$, $s = (c_0, c_1, \ldots)$, we see that $rs - 1 \in I$.) Every diagonal sequence is in R, and we obtain an embedding $j : K \to D$. Since $\mathcal{O}$ is bounded, $\Pi_i \mathcal{O} \subseteq R$, and we obtain a map $\Pi_i \mathcal{O} \to D$, yielding a natural map $\theta : \Pi_i \mathcal{S}(\mathcal{O}) \to \mathcal{S}(D)$. Let $a_* \in S(D)$ denote the image of $(a_0, a_1, \ldots)$ there. The assumption $d(a_i, X) \to 0$ implies that for any rational f regular near a_* and vanishing on X, $|f(a_i)| \to 0$, hence the sequence $(f(a_i))_i$ lies in I. It follows that $f(a_*) = 0$, hence $a_* \in X$.

Note that since each $a_i \in T_p'(S)$, by (#) above, $F(\sigma)a_i = 0$; and so $F(\sigma)a_* = 0$. By Lemma 6.6.1, $a_* \in Y$ for some K-defined coset Y of a connected subgroup W of S. Let $\pi : A \to S/W$ be the projection, $c = \pi(Y)$. So $\pi(a_*) = c \in (S/W)(K)$. But $\pi(a_*) = \theta((\pi(a_0), \pi(a_1), \ldots))$. It follows that the sequence $\pi(a_i)$ comes arbitrarily close to c, and in particular, for large i, $r_{S/W}(\pi a_i) = r_{S/W}(c)$. Now $r_{S/W}$ is injective on the prime-to-p torsion points of S/W, so $\pi(a_i) = c$ for large i. Thus for large i, $a_i \in Y$, and in particular, $a_i \in X$. □

References

[1] J.-B. Bost, Périodes et isogenies des variétés abéliennes sur les corps de nombres, d'apres D. Masser et G. Wüstholz. Séminarie Bourbaki Exp. No. 795.
[2] E. Bouscaren, E. Hrushovski, On one-based theories, J. Symbolic Logic 59 (2) (1994) 579–595.
[3] S. Buechler, Locally modular theories of finite rank, Ann. Pure Appl. Logic 30(1) (1986) 83–94.
[4] A. Buium, Geometry of p-adic jets, Duke J. Math 82 (2) (1996) 349–367.
[5] Z. Chatzidakis, E. Hrushovski, Model theory of difference fields, AMS Trans. 351 (8) (2000) 2997–3071.
[6] Z. Chatzidakis, E. Hrushovski, Y. Peterzil, Model Theory of difference fields II: periodic ideals and the trichotomy in all characteristics, Trans. AMS, to appear.
[7] C.C. Chang, J. Keisler, Model Theory, 3rd ed., North-Holland, Amsterdam, Tokyo, 1990.
[8] G. Cherlin, E. Hrushovski, Quasi-finite structures (preprint available in www.math.rutgers.edu//cherlin).
[9] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (3) (1983) 349–366.
[10] W. Fulton, Intersection Theory, Springer, Berlin, Tokyo, 1984.
[11] M. Hindry, Autour d'une conjecture de Serge Lang, Invent. Math. 94 (3) (1988) 575–603.
[12] E. Hrushovski, Unidimensional theories are superstable, Ann. Pure Appl. Logic 50 (1990) 117–138.
[13] E. Hrushovski, The Manin–Mumford conjecture and the model theory of difference fields, extended abstract (5pp), in: M. Jarden (Ed.), Proc. Field Arithmetic conf., Institute for Advanced Study, Jerusalem, 1995.
[14] E. Hrushovski, The Mordell–Lang conjecture for function fields, J. AMS 9 (3) (1996) 667–690.
[15] E. Hrushovski, A. Pillay, Weakly normal groups, in: Logic Colloquium 85, North-Holland, Amsterdam, 1986.
[16] E. Hrushovski, A. Pillay, Definable subgroups of algebraic groups over finite fields, J. Reine Angew. Math. 462 (1995) 69–91.
[17] B. Kim, A. Pillay, Simple theories, Ann. Pure Appl. Logic 88 (1997) 149–164.
[18] S. Lang, in: Number Theory III: Diophantine Geometry, Encyclopaedia of Mathematical Sciences, Vol. 60, Springer, Berlin, Heidelberg, 1991.
[19] S. Lang, J. Tate, Principal homogeneous spaces over abelian varieties, Amer. J. Math. 80 (1958) 659–684.
[20] D. Masser, G. Wüstholz, Factorisation estimates for abelian varieties, Pub. Math. IHES 81 (1995) 5–24.
[21] M. McQuillan, Division points on semi-abelian varieties, Invent. Math. 120 (1995) 143–149.
[22] A. Pillay, Model theory, stability theory, and stable groups, in: A. Nesin, A. Pillay (Eds.), The Model Theory of Groups, Notre Dame Mathematical Lectures 11, University of Notre Dame Press, Notre Dame, Indiana, 1989.

[23] M. Raynaud, Around the Mordell conjecture for function fields and a conjecture of Serge Lang, in: Proc. Algebraic Geometry of Tokyo, Lecture Notes, vol. 1016, Springer, Berlin, 1982.
[24] A. Robinson, Introduction to Model Theory and the Metamathematics of Algebra, North-Holland, Amsterdam, 1963.
[25] G. Sacks, Saturated Model Theory, W.A. Benjamin, Reading, MA, 1972.
[26] T. Scanlon, Conjecture of Tate and Voloch on p-adic proximity to torsion, International Math. Research Notices 1999 no 17, 909–914; p-adic distance from torsion points of semi-Abelian varieties, J. Reine Angew. Math. 499 (1998) 225–236.
[27] J.-P. Serre, Lectures on the Mordell–Weil Theorem, Vieweg, Braunschweig/Wiesbaden, 1997.
[28] J.-P. Serre, in: Groupes algébriques et corps de classes, Actualités scientifiques et industrielles, Vol. 1264, Hermann, Paris, 1959.
[29] J.-P. Serre, Oeuvres, Vol. IV, 1985–1998, Springer, Berlin, 2000.
[30] S. Shelah, Simple unstable theories, Ann. Math. Logic 19 (1980) 177–203.
[31] A. Weil, Variétés abeliennes et courbes algébriques, Hermann, Paris, 1948.