Model Theory, Algebra, and Geometry
MSRI Publications
Volume **39**, 2000

A Survey on the Model Theory of Difference Fields

ZOÉ CHATZIDAKIS

ABSTRACT. We survey the model theory of difference fields, that is, fields with a distinguished automorphism σ. After introducing the theory ACFA and stating elementary results, we discuss independence and the various concepts of rank, the dichotomy theorems, and, as an application, the Manin–Mumford conjecture over a number field. We conclude with some other applications.

Difference field are fields with a distinguished automorphism σ. They were first studied by Ritt in the 1930s. A good reference for the algebraic results is [Cohn 1965]. Interest in the model theory of difference fields started at the end of the eighties, particularly during the MSRI logic year, because of two questions.

The first question stemmed from the failure of Zil'ber's conjecture: there is a strongly minimal theory extending the theory of algebraically closed fields of any given characteristic. People were looking at the possibility of finding a non-definable automorphism σ of $\mathbb{F}_p^{\mathrm{alg}}$ (the algebraic closure of the field $\mathbb{F}_p$ with p elements), such that $\mathrm{Th}(\mathbb{F}_p^{\mathrm{alg}}, +, \cdot, \sigma)$ is strongly minimal. This question so far remains open.

The second problem had to do with the difference fields $\mathcal{F}_q = (\mathbb{F}_p^{\mathrm{alg}}, +, \cdot, \phi_q)$, where q is a power of p and $\phi_q : x \mapsto x^q$ is a power of the Frobenius automorphism $x \mapsto x^p$. The hope was to generalise the work of Ax on finite fields to these structures, and in particular to describe the theory of the non-principal ultraproducts of the difference fields $\mathcal{F}_q$.

These questions led Macintyre, van den Dries and Wood to look for a model companion of the theory of difference fields, and to prove various results (decidability, description of the completions, etc ...) for this theory, henceforth called ACFA. For details and attribution of results, see [Macintyre 1997]. I should also mention that the second problem was solved recently, by Hrushovski [1996b] and

Notes based on lectures given at MSRI, January 98.

Macintyre [$\geq$ 2000], showing that non-principal ultraproducts of $\mathcal{F}_q$'s are models of ACFA.

In 1994, Hrushovski and I started looking at stability-type properties of the theory ACFA. Our main result is a dichotomy result for types of rank 1 for models of characteristic 0, which was later partially extended to the case of positive characteristic with the help of Peterzil [Chatzidakis and Hrushovski 1999; Chatzidakis et al. 1999]. It has some applications to the description of types of finite rank, and to groups definable in models of ACFA. These results were used by Hrushovski [1995] to find explicit bounds in the Manin–Mumford conjecture.

The first four sections of the paper give a survey of the results obtained to-date for difference fields. In Section 5 we state the results used by Hrushovski in his proof of the Manin–Mumford conjecture over a number field, and show how he effectively derives from them the bounds. In the last section we conclude with the statements of some other applications due to Hrushovski and Scanlon.

Acknowledgements. I take this opportunity to thank MSRI for their support during the special semester on the Model Theory of Fields, and to show my appreciation for the congenial atmosphere. I would also like to thank D. Haskell and E. Hrushovski for many improvements to this paper.

1. Description and Elementary Results on the Theory ACFA

We work in the language $\mathcal{L} = \{+, -, \cdot, 0, 1, \sigma\}$, where $+, -, \cdot$ are the usual ring operations, 0 and 1 are constants, and σ is a unary function.

1.1. Some examples

(1) The shift operator. Consider the field $K = \mathbb{C}(t)$, and define σ by

$$\sigma|_{\mathbb{C}} = \mathrm{id}, \qquad \sigma(t) = t + 1.$$

The name "difference field" originated from this example: an equation of the form $P(f(t), f(t+1), \dots, f(t+n)) = 0$, where f is the unknown function to be found and P is a polynomial over K, is called an algebraic difference equation. One can replace K by other fields, e.g., the field of meromorphic functions on $\mathbb{C}$ or on $\mathbb{R}$.

(2) Let K be a field, K^s its separable closure and $\sigma \in \mathrm{Gal}(K^s/K)$. Then (K^s, σ) is a difference field. Note that because the algebraic closure K^{alg} of K is purely inseparable over K^s, σ extends uniquely to an automorphism of K^{alg}. One often identifies $\mathrm{Gal}(K^s/K)$ and $\mathrm{Aut}(K^{\mathrm{alg}}/K)$.

The structures $\mathcal{F}_q$ described above are a particular example. More generally, we have:

(3) Let K be a perfect field of characteristic $p > 0$, and q a power of p. Then (K, ϕ_q) is a difference field. If the field K is algebraically closed then

$(\mathbb{F}_p^{\mathrm{alg}}, \phi_q) \prec (K, \phi_q)$. This is because for fixed q the map $x \mapsto x^q$ is definable in the language of fields, and because the theory of algebraically closed fields is model complete.

1.2. Definitions, notation and some basic algebraic results. In the literature, a difference field is a field K with a distinguished monomorphism σ. If σ is onto, then (K, σ) is called an *inversive* difference field. However, a simple inductive limit argument shows that every difference field has a unique (up to isomorphism) inversive closure. We will assume in what follows, that *all our difference fields are inversive*. The references are to [Cohn 1965].

Let K be a difference field, and let $\bar{X} = (X_1, \ldots, X_n)$ be indeterminates. A difference polynomial over K in $X_1, \ldots, X_n$ is an ordinary polynomial with coefficients in K, in the variables $X_1, \ldots, X_n, \sigma(X_1), \ldots, \sigma^i(X_j), \ldots$. The ring of those difference polynomials is denoted $K[X_1, \ldots, X_n]_\sigma$, and σ extends naturally to $K[X_1, \ldots, X_n]_\sigma$, in the way suggested by the names of the variables.

NOTE. As defined, σ is not onto. It is sometimes convenient to consider the inversive closure of this ring, namely $K[\sigma^i(X_1), \ldots, \sigma^i(X_n)]_{i\in\mathbb{Z}}$, but we will not do this here.

There is a natural notion of *σ-ideal*, i.e., an ideal closed under σ, and of *reflexive* σ-ideal ($a \in I \iff \sigma(a) \in I$). The analog of a radical ideal is called a perfect σ-ideal: a σ-ideal I is *perfect* if $a \in I$ whenever $a^j\sigma^i(a) \in I$ for some $i, j \in \mathbb{N}$. A *prime σ-ideal* is a reflexive σ-ideal which is prime. Note that a prime σ-ideal is perfect. $K[X_1, \ldots, X_n]_\sigma$ does not satisfy the ascending chain condition on σ-ideals; however it satisfies it for perfect σ-ideals, and therefore for prime σ-ideals. This allows one to define σ-closed sets and σ-varieties (also called irreducible σ-closed sets) in affine n-spaces. They correspond dually to perfect σ-ideals and prime σ-ideals, and are the basic closed sets of a noetherian topology.

Let K be a difference field, a a tuple of elements (in some difference field extending K). We denote by $K(a)_\sigma$ the difference field generated by a over K, by $\mathrm{acl}_\sigma(Ka)$ its algebraic closure, and by $\deg_\sigma(a/K)$ the transcendence degree of $K(a)_\sigma$ over K. If a is a single element and $\deg_\sigma(a/K)$ is infinite, then a is called *transformally transcendental*. The elements $\sigma^j(a)$, $j \in \mathbb{Z}$, are then algebraically independent over K. If $\deg_\sigma(a/K)$ is finite, then a is called *transformally algebraic*. There are natural notions of transformal transcendence basis and transformal dimension.

1.3. An axiomatisation of the theory ACFA. Consider the theory ACFA, whose models are the $\mathcal{L}$-structures K satisfying these conditions:

(i) K is an algebraically closed field.
(ii) $\sigma \in \mathrm{Aut}(K)$.

(iii) If U and V are (affine) varieties defined over K, with $V \subseteq U \times \sigma(U)$ projecting generically onto U and $\sigma(U)$, then there is a tuple a in K such that $(a, \sigma(a)) \in V$.

Here, by a variety, we mean an absolutely irreducible Zariski closed set, i.e., a set defined by polynomial equations, and which is not the proper union of two smaller Zariski closed sets. The set $\sigma(U)$ is the variety obtained from U by applying σ to the coefficients of the defining polynomials of U. When we say that V projects generically onto U, we mean that the image of V under the natural projection $U \times \sigma(U) \to U$ is Zariski dense in U (i.e., not contained in any proper Zariski closed subset). Note that (iii) is indeed a conjunction of first-order sentences, since (by classical results on polynomial rings over fields) the fact that polynomials $f_1(\bar{X}), \ldots, f_n(\bar{X})$ generate a prime ideal of $K[\bar{X}]$ is an elementary condition on the coefficients of $f_1, \ldots, f_n$. Similarly for the inclusion of ideals in $K[\bar{X}]$.

THEOREM. ACFA *is the model companion of the theory of difference fields.*

SKETCH OF PROOF. We first need to show that every difference field embeds in a model of ACFA. Axioms (i) and (ii) pose no problem, as every automorphism of a field extends to its algebraic closure. Let U and V be as in (iii). Choose a generic point (a, b) of V over K (i.e., the ideal of polynomials over K vanishing at (a, b) is exactly the ideal of polynomials vanishing at all points of V), in some field containing K. Then a is a generic of U, and b is a generic of $\sigma(U)$. By elementary properties of algebraically closed fields, the isomorphism $\tau : K(a) \to K(b)$ that extends σ and sends a to b extends to an automorphism of the algebraic closure of $K(a, b)$.

This shows that every difference field embeds in a model of ACFA. It remains to show that the models of ACFA are existentially closed. Let $(K, \sigma) \models$ ACFA, let $\varphi(x)$, x a tuple of variables, be a quantifier-free formula with parameters in K, and assume that $\varphi(x)$ has a solution in some difference field (L, σ) extending K. The usual trick of replacing the inequality $y \neq 0$ by $\exists z \; yz - 1 = 0$, shows that one can assume that $\varphi(x)$ is a conjunction of σ-equations. Let $a \in L$ satisfy φ. For n large enough, the σ-ideal I generated by the set

$$\big\{ f(X, \sigma(X), \ldots, \sigma^n(X)) \mid \\ f(Y, Y_1, \ldots, Y_n) \in K[Y, Y_1, \ldots, Y_n], \; f(a, \sigma(a), \ldots, \sigma^n(a)) = 0 \big\}$$

is precisely the prime σ-ideal of difference polynomials over K annulled by a. Thus any point satisfying these equations will satisfy $\varphi(x)$.

Let U be the variety defined over K with generic $(a, \sigma(a), \ldots, \sigma^{n-1}(a))$, and V the variety defined over K with generic $(a, \sigma(a), \ldots, \sigma^{n-1}(a), \sigma(a), \ldots, \sigma^n(a))$. Then U and V satisfy the hypotheses of axiom (iii), and therefore there is a tuple b in K such that $(b, \sigma(b)) \in V$. Then $b = (c, \sigma(c), \ldots, \sigma^{n-1}(c))$ for some c, and $K \models \varphi(c)$. $\square$

1.4. The Frobenius automorphisms. Before continuing with the elementary properties of ACFA, we will state precisely the result of Hrushovski, from which follows that non-principal ultraproducts of $\mathcal{F}_q$'s are models of ACFA. It is then a consequence of Tchebotarev's theorem on the distribution of primes that ACFA is exactly the theory of all non-principal ultraproducts of $\mathcal{F}_q$'s, see [Macintyre 1997].

THEOREM [Hrushovski 1996b]. *Let U, V be varieties with $V \subseteq U \times \sigma(U)$, and assume that the projections are onto and have finite fibers. Let $d_1 = [K(V) : K(U)]$, $d_2 = [K(V) : K(\sigma(U))]_i$ (purely inseparable degree); let $c = d_1/d_2$ and $d = \dim(V)$. Then for some constant $C > 0$, depending on the two varieties U and V, and which remains bounded when U and V move inside an algebraic family of varieties,*

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

1.5. PROPOSITION. *If $(K, \sigma) \models$ ACFA, then the subfield $\mathrm{Fix}(\sigma)$ of K fixed by σ is a pseudo-finite field.*

PROOF. By [Ax 1968], one needs to show that: $\mathrm{Fix}(\sigma)$ is perfect; $\mathrm{Fix}(\sigma)$ has exactly one algebraic extension of each degree; every (absolutely irreducible) variety defined over $\mathrm{Fix}(\sigma)$ has an $\mathrm{Fix}(\sigma)$-rational point.

The first assertion is obvious, and the third one follows easily from axiom (iii). For the second assertion, it suffices to show that for each $n > 1$, the system

$$\sigma^n(x) = x, \qquad \sigma^j(x) \neq x \quad \text{for } j = 1, \ldots, n-1,$$

has a solution in K. Since K is existentially closed, it suffices to find a difference field extending K in which this system has a solution. Consider the field $K(X_1, \ldots, X_n)$ in n indeterminates, and extend σ by defining $\sigma(X_j) = X_{j+1}$ for $j < n$ and $\sigma(X_n) = X_1$. Then X_1 is a solution of the system. □

In characteristic $p > 0$ one shows similarly that if $m \neq 0$ and n are integers, then the set of elements of K satisfying $\sigma^m(x) = x^{p^n}$ is a pseudo-finite field.

1.6. It turns out that many of the proofs given in [Ax 1968] for pseudo-finite fields generalise to models of ACFA. Parts (1)–(5) of the following result appear in [Macintyre 1997].

PROPOSITION. (1) *Let (K_1, σ_1) and (K_2, σ_2) be models of* ACFA, *and let E be a common difference subfield. Then*

$$(K_1, \sigma_1) \equiv_E (K_2, \sigma_2) \iff (E^{\mathrm{alg}}, \sigma_1|_{E^{\mathrm{alg}}}) \simeq_E (E^{\mathrm{alg}}, \sigma_2|_{E^{\mathrm{alg}}}).$$

(2) *From this one deduces immediately that the completions of* ACFA *are obtained by describing the action of σ on the algebraic closure of the prime field ($\mathbb{Q}^{\mathrm{alg}}$ or $\mathbb{F}_p^{\mathrm{alg}}$). This then entails the decidability of the theory* ACFA, *as well as of its extensions* ACFA_0 *and* ACFA_p *obtained by specifying the characteristic of the field.*

(3) *It also gives a description of the types. Let E be a difference field, a and b two tuples from a model K of* ACFA *containing E. Then* $\mathrm{tp}(a/E) = \mathrm{tp}(b/E)$ *if and only if there is an isomorphism φ from the difference field* $\mathrm{acl}_\sigma(Ea) =_{\mathrm{def}} E(a)_\sigma^{\mathrm{alg}}$ *onto the difference field* $\mathrm{acl}_\sigma(Eb)$ *which is the identity on E and sends a to b.*

(4) *If E is an algebraically closed difference field, then*

$$\mathrm{ACFA} \cup \mathrm{qftp}(E) \vdash \mathrm{tp}(E),$$

where $\mathrm{qftp}(E)$ *denotes the quantifier-free type of E.*

(5) *The algebraic closure (in the model-theoretic sense) of a set A coincides with the algebraic closure (in the ordinary field sense) of the difference field generated by A (which we denote by* $\mathrm{acl}_\sigma(A)$*).*

(6) *Let $K \models$* ACFA, *let U be a variety, $l \geq 1$, and V a subvariety of $U \times \sigma(U) \times \cdots \times \sigma^l(U)$. Let $\pi_1 : U \times \sigma(U) \times \cdots \times \sigma^l(U) \to U \times \sigma(U) \times \cdots \times \sigma^{l-1}(U)$ and $\pi_2 : U \times \sigma(U) \times \cdots \times \sigma^l(U) \to \sigma(U) \times \cdots \times \sigma^l(U)$ be the two canonical projections, and assume that $\sigma\pi_1(V)$ and $\pi_2(V)$ have the same generics. Then the set of points $\tilde{V} = \{x \in U(K) \mid (x, \sigma(x), \ldots, \sigma^l(x)) \in V\}$ is Zariski dense in U.*

(7) *If $(K, \sigma) \models$* ACFA *and $m \geq 1$, then $(K, \sigma^m) \models$* ACFA.

Proof. (1) The left to right implication is almost immediate. For the other one, moving K_2 by some E-isomorphism, we may assume that $E = E^{\mathrm{alg}}$ and that K_1 and K_2 are linearly disjoint over E. This implies that the ring $K_1 \otimes_E K_2$ is a domain. Define $\sigma(a \otimes b) = \sigma_1(a) \otimes \sigma_2(b)$ for $a \in K_1$ and $b \in K_2$; then σ extends to an automorphism of the quotient field L of $K_1 \otimes_E K_2$, which agrees with σ_1 on K_1 and σ_2 on K_2. Now, (L, σ) embeds in a model (M, σ) of ACFA, and by model-completeness we have $(K_1, \sigma_1) \prec (M, \sigma)$ and $(K_2, \sigma_2) \prec (M, \sigma)$.

The first part of (2), (3) and (4) are immediate, applying compactness to (1). The decidability follows from the recursive axiomatisation of ACFA, together with the effective computability of Galois groups of the splitting fields over $\mathbb{Q}$ and $\mathbb{F}_p$ of polynomials of $\mathbb{Z}[T]$.

(5) Let $A = \mathrm{acl}_\sigma(A) \subseteq K \models \mathrm{ACFA}$ and $b \in K \setminus A$, $B = \mathrm{acl}_\sigma(Ab)$; let B_1 be an A-isomorphic copy of B, linearly disjoint over A. As in (1), there is a model of ACFA containing the difference fields B and B_1. By (3), $\mathrm{tp}(B_1/A) = \mathrm{tp}(B/A)$, which shows that $\mathrm{tp}(b/A)$ is not algebraic.

(6) We may assume that U and V are affine. Let

$$W \subseteq U \times \sigma(U) \times \cdots \times \sigma^{l-1}(U)$$

be the Zariski closure of $\pi_1(V)$. By assumption, $\pi_2(V)$ is Zariski dense in $\sigma(W)$, and we may therefore assume that $l = 1$. The proof that every difference field embeds in a model of ACFA shows that if K is sufficiently saturated, then K contains a point a such that $(a, \sigma(a))$ is a generic of V. This shows that $\tilde{V}$ is dense in U. $\square$

2. Independence and Rank

2.1. Definition of independence. Let A, B and C be subsets of a model K of ACFA. We say that A and B are *independent over* C, and write $A \perp_C B$, if $\mathrm{acl}_\sigma(CA)$ and $\mathrm{acl}_\sigma(CB)$ are linearly disjoint over $\mathrm{acl}_\sigma(C)$. This notion has all the usual properties of independence in algebraically closed fields. Recall that by Proposition 1.6(5), $\mathrm{acl}_\sigma(A)$ is the model-theoretic algebraic closure of the set A in the model K.

2.2. Definition of the SU-rank. We define a rank based on independence in the usual way, that is, for p a type over E, realised by a tuple a:

- $\mathrm{SU}(p) = \mathrm{SU}(a/E) \geq 0$,
- $\mathrm{SU}(p) \geq \alpha$ for α a limit ordinal, if and only if $\mathrm{SU}(p) \geq \beta$ for every $\beta < \alpha$,
- $\mathrm{SU}(p) \geq \alpha+1$ if and only if there is $F \supseteq E$ such that $a \not\perp_E F$ and $\mathrm{SU}(a/F) \geq \alpha$.

Then $\mathrm{SU}(p)$ is the least ordinal α such that $\mathrm{SU}(p) \not\geq \alpha + 1$. If $\varphi(x)$ is a formula with parameters in $E = \mathrm{acl}_\sigma(E)$, one also defines $\mathrm{SU}(\varphi) = \max\{\mathrm{SU}(a/E) \mid a \text{ satisfies } \varphi\}$.

2.3. The SU-rank shares the properties of the usual U-rank, and in particular, the Lascar rank inequality: if a, b are tuples and E a set, then $\mathrm{SU}(a/Eb) + \mathrm{SU}(b/E) \leq \mathrm{SU}(a,b/E) \leq \mathrm{SU}(a/Eb) \oplus \mathrm{SU}(b/E)$, where $\oplus$ denotes the natural sum on ordinal numbers. (Recall that $1 + \omega = \omega$, while $1 \oplus \omega = \omega + 1$.)

2.4. Some examples. Let E be a difference subfield of a model K of ACFA and a a tuple in K. From the definition of the SU-rank, it is clear that:

- $\mathrm{SU}(a/E) = 0 \iff a \in \mathrm{acl}_\sigma(E)$.
- $\mathrm{SU}(a/E) = 1 \iff a \notin \mathrm{acl}_\sigma(E)$, and for every $F \supseteq E$, either $a \perp_E F$ or $a \in \mathrm{acl}_\sigma(F)$.

Earlier we defined $\deg_\sigma(a/E)$, which is also an invariant of $\mathrm{tp}(a/E)$. It has some relation with SU-rank, since independence is defined in terms of non-forking in algebraically closed fields. For instance, one has, for $E \subseteq F$ difference fields and a a tuple with $\deg_\sigma(a/E) < \infty$,

$$a \not\perp_E F \iff \deg_\sigma(a/F) < \deg_\sigma(a/E),$$

and this implies

$$\mathrm{SU}(a/E) \leq \deg_\sigma(a/E).$$

Thus in particular, every non-algebraic type containing the equation $\sigma(x) = x^2+1$ has SU-rank 1. This inequality can be strict; see the example in 2.6 below.

2.5. One can also show that the SU-rank of an element transformally transcendental over the difference field E is ω: let a be such an element, and consider the sequence (b_i), $i \in \mathbb{N}$, defined by $b_0 = a$, $b_{i+1} = \sigma(b_i) - b_i$. Then the fields $L_i = E(b_i)_\sigma$ form a decreasing sequence of subfields of $E(a)_\sigma$, with tr $\deg(L_i/L_{i+1}) = 1$. By additivity of rank, we obtain $\mathrm{SU}(a/L_i) = i$, which implies that $\mathrm{SU}(a/E) \geq \omega$. On the other hand, $\mathrm{SU}(a/E) \not\geq \omega + 1$: if $a \not\perp_E F$ then $\deg_\sigma(a/F) < \infty$, which implies that $\mathrm{SU}(a/F) < \omega$. Hence $\mathrm{SU}(a/E) = \omega$.

Note that this gives an example of the left-hand equality in 2.3: $\mathrm{SU}(a/Eb_1) = 1$, $\mathrm{SU}(b_1/E) = \omega$, and $\mathrm{SU}(a/E) = \omega$. For a tuple b in K this also yields: $\mathrm{SU}(b/E) < \omega \iff \deg_\sigma(b/E) < \infty$.

2.6. Example. *Consider the formula* $\varphi(x) : \sigma^{-2}(x) = x^2 + 1$ *(in characteristic* $\neq 2$*). Then* $\mathrm{SU}(\varphi) = 1$.

Proof. By 2.4, we want to show that if E is any difference field and a is any solution of $\sigma^{-2}(x) = x^2+1$, then either $a \in \mathrm{acl}_\sigma(E)$, or $a \perp E$, i.e.: $\deg_\sigma(a/E) = 2$. Let $E = \mathrm{acl}_\sigma(E)$ be a field, and a a realisation of φ, $a \notin E$. We need to show that $\deg_\sigma(a/E) = 2$. Since E is an arbitrary algebraically closed difference field, this will imply: if $F = \mathrm{acl}_\sigma(F)$ contains E and $\mathrm{tp}(a/F)$ forks over E, then $a \in F$, and therefore that $\mathrm{SU}(\varphi) = 1$.

Suppose by way of contradiction that $\deg_\sigma(a/E) = 1$, and let $K = E(a, \sigma(a))$, $m = [K : E(a)]$ and $n = [K : E(\sigma(a))]$. Observe that K contains all $\sigma^{-j}(a)$ for $j \geq 0$ (because $\sigma^{-2j}(a) \in E(a)$). Since $E(\sigma^2(a))$ is a Galois extension of $E(a)$, we have that $[K(\sigma^2(a)) : K]$ divides $[E(\sigma^2(a)) : E(a)] = 2$.

Assume first that $[K(\sigma^2(a)) : K] = 1$. Then $\sigma(K) = K$, which implies that $K = E(a)_\sigma$. On the other hand, $E(a)_\sigma$ contains the infinite algebraic extension $E(\sigma^{2j}(a))_{j\in\mathbb{N}}$ of $E(a)$, which gives us a contradiction.

Thus $[K(\sigma^2(a)) : K] = 2$, and therefore $E(\sigma^2(a)) \cap K = E(a)$. So we have:

$$\begin{aligned}[E(\sigma(a), \sigma^2(a)) : E(a)] &= [E(\sigma(a), \sigma^2(a)) : K][K : E(a)] = 2m \\ &= [E(\sigma(a), \sigma^2(a)) : E(\sigma^2(a))][E(\sigma^2(a)) : E(a)] = 2n\end{aligned}$$

since $[E(\sigma(a), \sigma^2(a)) : E(\sigma^2(a))] = [K : E(\sigma(a))]$. This implies $m = n$. On the other hand,

$$\begin{aligned}[E(\sigma(a), \sigma^2(a)) : E(\sigma(a))] &= [K : E(a)] = m \\ &= [E(\sigma(a), \sigma^2(a)) : K][K : E(\sigma(a))] = 2n\end{aligned}$$

which gives $m = 2n$ and the desired contradiction. $\square$

2.7. The independence theorem. *Let* $E = \mathrm{acl}_\sigma(E) \subseteq K$, *let* a, b, c_1 *and* c_2 *be tuples from* K *such that* a, b, c_1 *and* c_2 *are independent over* E *and* $\mathrm{tp}(c_1/E) = \mathrm{tp}(c_2/E)$. *Then there is* c *(in some elementary extension of* K*) independent from* (a, b) *over* K, *and realising* $\mathrm{tp}(c_1/\mathrm{acl}_\sigma(Ea)) \cup \mathrm{tp}(c_2/\mathrm{acl}_\sigma(Eb))$.

A generalised version of this theorem holds: let $n \geq 3$, let $x_1, \ldots, x_n$ be tuples of variables, and let W be a set of proper subsets of $\{1, \ldots, n\}$ closed under intersection. Assume that for each $w \in W$ we are given a complete type $p_w(x_w)$ over $E = \mathrm{acl}_\sigma(E)$, in the variables $x_w = \{x_i \mid i \in w\}$, which can be realised by some $(a_i \mid i \in w)$ such that the elements $a_i, i \in w$, are independent over E (i.e., for each $j \in w$, the tuple a_j is independent from the set $\{a_i \mid i \in w,\ i \neq j\}$ over E). Assume moreover that if $v \subset w$ are in W then $p_v(x_v) \subset p_w(x_w)$. Then the type

$$\bigcup_{w \in W} p_w(x_w)$$

can be realised by some tuple $a_1, \ldots, a_n$, with $a_1, \ldots, a_n$ independent over E. The independence theorem corresponds to the case

$$n = 3, \quad W = \{\{1,2\},\{1,3\},\{2,3\}\}.$$

2.8. Independence and non-forking. Using the independence theorem, one proves that independence as defined above coincides with the usual notion of non-forking. Namely, assume that a and F are independent over $E = \mathrm{acl}_\sigma(E)$, and let $p(x) = \mathrm{tp}(a/F)$. Assume that $(F_i)_{i\in\mathbb{N}}$ is an E-indiscernible sequence of realisations of $\mathrm{tp}(F/E)$, and let $p_i(x)$ be the type over F_i which is the image of $p(x)$ by an E-automorphism mapping F to F_i. Then $\cup_i p_i(x)$ is consistent. Thus any completion of ACFA is simple in the sense of [Shelah 1980].

The connections between the independence theorem and simplicity were first observed by Hrushovski in the context of pseudofinite fields (and more generally bounded PAC fields); see [Hrushovski 1991; Hrushovski and Pillay 1994]. The case $n > 3$ of the generalised independence theorem goes beyond simplicity, and its model theoretic meaning remains to be clarified.

Recall that any PAC field which is not separably closed is unstable by a result of Duret [Duret 1980]. Hrushovski recognised the usefulness of the independence theorem for studying definable groups and generalising the techniques of stability theory to the context of pseudofinite fields, and more generally, to models of S_1-theories (an S_1-theory has finite SU-rank and some definability property of the SU-rank).

The independence theorem is indeed a good substitute for "uniqueness of non-forking extension" which is true in stable theories, and allows one to generalise the concepts of generic type of a group and of stabilisers of types to groups definable in finite fields, and later, to groups definable in models of ACFA.

The independence theorem was later generalised by B. Kim and A. Pillay [Kim and Pillay 1997] to Lascar types in simple theories. Moreover their result gives a nice characterisation of non-forking. The results on definable groups were also generalised to the context of simple theories; see [Pillay 1998; Wagner 1997].

2.9. The independence theorem is also used in the proof of these two statements:

PROPOSITION. *Let K be a model of* ACFA.

(1) $\mathrm{Th}(K)$ *has elimination of imaginaries.*
(2) *Let $S \subseteq \mathrm{Fix}(\sigma)^n$ be definable in K. Then S is definable in the pure field* $\mathrm{Fix}(\sigma)$ (*maybe with additional parameters from* $\mathrm{Fix}(\sigma)$).

2.10. Groups of finite SU-rank. Using the techniques developed in [Hrushovski and Pillay 1994; 1995], one obtains for instance a generalisation of a well-known result of algebraic geometry:

PROPOSITION. *Let G be a group of finite* SU*-rank defined over a model K of* ACFA, *and let $\{X(i) \mid i \in I\}$ be a family of definable subsets of G. There is a definable group H contained in the subgroup of G generated by the $X(i)$, $i \in I$, such that $X(i)H/H$ is finite for every $i \in I$.*

Note that no uniformity is assumed in the family $X(i)$, just that each of them is definable by some formula. The proof gives more information. Without loss of generality we will assume that for every $i \in I$ there is $j \in I$ such that $X(j) = X(i)^{-1}$.

(1) There are elements $i_1, \dots, i_n \in I$ such that $H \subseteq X(i_1) \cdots X(i_n)$ and $n \leq 2\,\mathrm{SU}(G)$.

(2) Assume that G is a subgroup of an algebraic group defined over K, that G and the sets $X(i)$ are irreducible σ-closed sets, and that the identity element of the group belongs to all $X(i)$'s. Then H is the subgroup generated by all the $X(i)$'s, and the number n in (1) is $\leq \mathrm{SU}(G)$.

2.11. Finite simple groups. One can then use Hrushovski's result on the Frobenius automorphisms ϕ_q of Section 1.4 to get information about certain classes of finite simple groups. With the exception of the sporadic groups and the alternating groups, finite simple groups are defined in terms of algebraic groups, and form families (e.g., $\mathrm{PSL}_n(\mathbb{F}_q)$ for fixed n and q ranging over prime powers). All but the Suzuki and Ree families are already definable over finite fields in the language of fields $\{+, -, \cdot, 0, 1\}$. The Suzuki and Ree families become uniformly definable in the structures $\mathcal{F}_{p^{m+1}}$, for $p = 2$ or 3, as m varies over the positive integers. Indeed, these groups are defined as follows: we have some algebraic group G (in the family B_2, G_2 or F_4), and an algebraic automorphism φ of G whose square induces the Frobenius map ϕ_p on $G(\mathbb{F}_p^{\mathrm{alg}})$. Then the subgroup ${}^2G(p^{2m+1})$ is the subgroup of $G(\mathbb{F}_{p^{2m+1}})$ left fixed by $\varphi\phi_{p^{m+1}}^{-1}$ (see [Suzuki 1982, p. 388]). This implies that ${}^2G(p^{2m+1})$ is the subgroup of $G(\mathbb{F}_p^{\mathrm{alg}})$ defined by the equation $\sigma(g) = \varphi(g)$ in the structure $\mathcal{F}_{p^{m+1}}$.

The results in the previous subsection apply and give for instance: if m is large enough, then any non-trivial conjugacy class of ${}^2G(p^{2m})$ generates the whole group in at most $\dim(G)+1$ steps ($\dim(B_2) = 10$, $\dim(G_2) = 14$, $\dim(F_4) = 52$).

2.12. PROPOSITION. *Let G be a group of finite* SU*-rank defined over a model K of* ACFA. *There is an algebraic group H defined over K, and a definable group homomorphism f from some definable subgroup G_0 of G of finite index in G into $H(K)$, with* $\mathrm{Ker}(f)$ *finite central.*

Note that $f(G_0)$ has infinite index in $H(K)$, since $H(K)$ has SU-rank $\omega \dim(H)$. However, if H_0 is the smallest quantifier-free definable subgroup of H containing $f(G_0)$, then $f(G_0)$ has finite index in H_0, and $\mathrm{SU}(G) = \mathrm{SU}(H_0)$.

3. Study of Types of Finite Rank

In this section we will study types of finite SU-rank. First a reduction to types of SU-rank 1:

3.1. PROPOSITION. *Let $E = \mathrm{acl}_\sigma(E)$ and a a tuple with $0 < \mathrm{SU}(a/E) < \omega$. Then there is a tuple b independent from a over E, and an element*

$$c \in \mathrm{acl}_\sigma(Eab) \setminus \mathrm{acl}_\sigma(Eb)$$

such that $\mathrm{SU}(c/Eb) = 1$.

3.2. Orthogonality. Recall that two types p and q are *orthogonal* (denoted by $\perp$), if for every set E containing the sets over which p and q are defined, if a and b realise non-forking extensions of p and q respectively to E, then $a \mathop{\smile\!\!\!\!\!\!\mid}_E b$. A type is *orthogonal to a formula* if it is orthogonal to any type containing this formula. Two formulas $\varphi(x)$ and $\psi(y)$ are *orthogonal* if and only if, for every $F = \mathrm{acl}_\sigma(F)$ containing the parameters needed to define φ and ψ, and any tuples a and b satisfying φ and ψ respectively, a and b are independent over F.

Rephrased in terms of orthogonality, Proposition 3.1 says that every type of finite SU-rank is non-orthogonal to a type of SU-rank 1.

3.3. Modularity. Let $E = \mathrm{acl}_\sigma(E)$ be a subset of the model K of ACFA, and let $R \subseteq K^n$ be the set of realisations of a set of types over E (so, for instance, a subset of K^n which is definable over E). We say that R is *modular* (*over* E) if and only if any two subsets A and B of R are independent over $\mathrm{acl}_\sigma(EA) \cap \mathrm{acl}_\sigma(EB)$. We say that a (possibly incomplete) type over E, or a formula, is *modular* (*over* E) if its set of realisations is modular over E.

REMARKS. (1) The definition of modularity first appears in an unstable context in [Cherlin and Hrushovski 1998], where it is given in terms of $\mathrm{acl}^{\mathrm{eq}}$. This agrees with our definition because ACFA eliminates imaginaries. This notion of modularity generalises several notions introduced in the eighties: locally modular, one-based, module-like. All three were defined in a stable context, and some required the underlying set to be a set of realisations of rank 1 types, or of regular types.

(2) It suffices to check modularity for finite sets A and B.

(3) A modular set satisfies the stronger property: if $A \subseteq R$ and $B \subseteq K$, then A and B are independent over $\mathrm{acl}_\sigma(EA) \cap \mathrm{acl}_\sigma(EB)$.

(4) The set of realisations of (a set of) modular types of SU-rank 1 is modular. A subset of a modular set is modular. Any trivial type of SU-rank 1 is modular (a

type p over E is *trivial* if $\mathrm{acl}_\sigma(EA) = \bigcup_{a\in A} \mathrm{acl}_\sigma(Ea)$ for any set A of realisations of p).

(5) Assume that the elements of R have SU-rank 1 over E. Then the modularity of R can be rephrased as follows: there is no rank-2 family of definable curves on R^2.

(6) If p and q are non-orthogonal types of SU-rank 1, and if p is modular then so is q.

(7) Assume that R is the set of realisations of a type of SU-rank 1 over E, and that R is modular and stable, stably embedded. Then R satisfies the stronger property: any two subsets A and B of R are independent over $\mathrm{acl}_\sigma(EA) \cap \mathrm{acl}_\sigma(EB) \cap R$, provided this intersection is non-empty. This coincides with the classical notion of local modularity known to model theorists.

3.4. Additional remarks on modularity

(1) Modularity is a very strong property. In particular it implies that no field is interpretable. As we will see below, if a stable group G is modular, then there is essentially only one possible group law on G (see Proposition 4.2 below). Modular stable groups are abelian by finite.

Let me show by an example that an algebraically closed field k cannot be modular (we work in the language of rings $\{+, -, \cdot, 0, 1\}$). Indeed, consider three (algebraically) independent elements a, b, c in some algebraically closed field containing k, and let $d = ac + b$. Then the algebraic closures of the fields $k(a, b)$ and $k(c, d)$ intersect in k; but clearly (a, b) and (c, d) are not independent over k since e.g., $\mathrm{tr}\ \deg(k(a, b, c, d)/k) = 3 < \mathrm{tr}\ \deg(k(a, b)/k) + \mathrm{tr}\ \deg(k(c, d)/k) = 4$. The failure of modularity is of course due to the existence of the two-dimensional family $C_{a,b}$ of curves $y = ax + b$ in the plane.

(2) Let $K \models$ ACFA, let $R \subseteq K^n$ be definable over $E = \mathrm{acl}_\sigma(E)$, and assume that R is modular. This gives us information about the field of definition of the σ-closure $\bar{R}$ of R: if $a \in R$ is a generic of an irreducible component Z of $\bar{R}$, then Z is defined over $\mathrm{acl}_\sigma(Ea)$. When R is quantifier-free definable, then $\bar{R}$ is what we could call a "good approximation" of R, because $\deg_\sigma(\bar{R} \setminus R) < \deg_\sigma(R)$. When R is not quantifier-free definable, then usually $\deg_\sigma(\bar{R} \setminus R) = \deg_\sigma(R)$, and in an unstable context it may happen that any set S containing R and satisfying $\deg_\sigma(S \setminus R) < \deg_\sigma(R)$ "needs" parameters from outside the algebraic closure of the field of definition of $\bar{R}$.

3.5. Proposition. *Let $K \models$ ACFA, let $E = \mathrm{acl}_\sigma(E) \subseteq K$ and let p be a non-trivial modular type over E, of* SU*-rank* 1*. Then p is non-orthogonal to the generic of a definable subgroup of some (simple) commutative algebraic group, i.e., a simple abelian variety, or the multiplicative group $\mathbb{G}_m$, or the additive group $\mathbb{G}_a$; the latter case can only occur in positive characteristic.*

3.6. Zil'ber's conjecture and the dichotomy. Zil'ber's conjecture states: Let T be a strongly minimal theory. Then either all types of T are modular, or T interprets a (pure) algebraically closed field.

This conjecture was disproved by Hrushovski. However, the philosophy behind Zil'ber's conjecture remains true: in most natural situations, the conjecture should be valid. An axiomatic system of such "natural situations" is given in [Hrushovski and Zilber 1996] (Zariski geometries).

The dichotomy "modular/field" was proved for strongly minimal types in differentially closed fields (see [Hrushovski and Ž. Sokolović 1994]) and for minimal types in separably closed fields (see [Hrushovski 1996c; Delon 1998]). Its interest lies in the fact that there is a complete characterisation of the fields of rank 1 interpretable in the theory of differentially closed fields or in the theory of separably closed fields of positive degree of imperfection: they are definably isomorphic to, respectively, the field of constants and the field of elements which are q-th powers for all power q of the characteristic. This is an important tool in Hrushovski's proof of the Geometric Mordell–Lang conjecture.

4. The Dichotomy Theorems

As explained in the previous section, our goal was to prove the following dichotomy: a type of SU-rank 1 is either non-orthogonal to one of the fixed fields, or it is modular. We first proved the characteristic 0 case, in a stronger form. The proof in that case is very algebraic and uses ramification theory. We were then able to establish the dichotomy in positive characteristic by completely different methods, see 4.4 for some details.

The dichotomy result allows us to get a good description of certain definable sets in the modular case (see Sections 4.2 and 4.7 below) and a semi-minimal analysis of types of finite rank 4.6.

4.1. THEOREM (THE DICHOTOMY IN CHARACTERISTIC 0). *Let p be a type of SU-rank 1 over $E = \mathrm{acl}_\sigma(E)$. Then either $p \not\perp (\sigma(x) = x)$, or p is modular, stable, stably embedded, and has a unique non-forking extension to any set containing E. Also, $p \not\perp (\sigma(x) = x)$ if and only if $\deg_\sigma(p) = 1$ and there is an integer N such that $[E(a, \sigma^k(a)) : E(a)] \leq N$ for every $k \in \mathbb{Z}$.*

Stably embedded means (n the arity of p, P the set of realisations of p): if $S \subseteq K^{nm}$ is definable, then $S \cap P^m = S' \cap P^m$ for some S' definable with parameters from P.

Note that a type can be stably embedded even if it is unstable. Indeed, one can show that if P is the set of realisations of a type p containing the formula $\sigma(x) = x$, then the field generated by P is all of $\mathrm{Fix}(\sigma)$. Thus, by 2.9(2), p is stably embedded.

4.2. The result of 4.1 extends to formulas: if $\varphi(x) \perp (\sigma(x) = x)$, then the set of elements satisfying φ, with the structure inherited from K, is stable and modular. In the case of groups, this has the following striking consequence, by a theorem of Hrushovski and Pillay [1987]:

PROPOSITION. *Assume characteristic* 0. *Let G be a group of finite* SU*-rank definable in a model K of* ACFA, *and assume that the formula defining G is orthogonal to $(\sigma(x) = x)$, and has its parameters in $E = \mathrm{acl}_\sigma(E)$. Let $S \subseteq G^m$ be definable. Then S is a Boolean combination of cosets of E-definable subgroups of G^m.*

4.3. THEOREM (THE DICHOTOMY IN CHARACTERISTIC $p > 0$). *Let q be a type of* SU*-rank* 1. *Then either q is modular, or q is non-orthogonal to the formula $\sigma^m(x) = x^{p^n}$ for some $m > 0$ and $n \in \mathbb{Z}$.*

REMARKS. (1) The Frobenius automorphism $x \mapsto x^p$ is definable. Hence, for $m > 0$ and $n \in \mathbb{Z}$, the formula $\sigma^m(x) = x^{p^n}$ defines a pseudofinite subfield of K. We will refer to these fields as *fixed fields*.

(2) The result obtained in characteristic 0 does not generalise to characteristic $p > 0$. For instance, one can show that the set of realisations of $\sigma(x) = x^p - x$ is unstable, and not stably embedded either. However, any complete type containing this formula is modular. We will see below that this is enough for some applications.

(3) There is a criterion analogous to the one given in characteristic 0 for types non-orthogonal to $(\sigma(x) = x^{p^n})$: one replaces algebraic degree by separable degree. If the field is defined by the equation $\sigma^m(x) = x^{p^n}$ with $m > 1$, then the criterion has to be suitably modified.

4.4. The proof of the dichotomy in characteristic $p > 0$ is quite different from the one in zero characteristic. An essential ingredient of the proof is the central role played by certain reducts of the structure. If $\mathcal{M} = (K, \sigma)$ is a model of ACFA, we let $\mathcal{M}[n]$ be the structure (K, σ^n), which is also a model of ACFA by Proposition 1.6(7). While $\mathcal{M}[n]$ is a reduct of $\mathcal{M}$, certain definable sets appear to attain more structure. It turns out that $\mathcal{M}[n]$ behaves more and more smoothly as n approaches infinity (a phenomenon which already showed up in the proof of the characteristic 0 case). In the characteristic $p > 0$, the proof begins by defining a certain limit structure $\mathcal{M}[\infty]$ of the sequence $\mathcal{M}[n]$ (the "virtual structure"). This limit structure is shown to be very well-behaved, and some of its properties are translated back to the reducts $\mathcal{M}[n]$ and to $\mathcal{M}$. This role for reducts and the type of limit taken, appear to be new in model theory.

We put a topology on some definable subsets of $\mathcal{M}[\infty]$, and show that it satisfies an adapted version of the axioms of Zariski geometries. Then, given a non-modular definable subset X of $\mathcal{M}[\infty]$, we reproduce the proof of [Hrushovski and Zilber 1996] to obtain a field F of rank 1 interpretable in $\mathcal{M}[\infty]$ and non-orthogonal to X, and show that this field F is algebraically closed. The proof that this gives the theorem uses the following result, of independent interest:

4.5. PROPOSITION. *Let H be a simple algebraic group, and let G be a Zariski dense subgroup of $H(K)$ definable in $K \models$ ACFA. If $\mathrm{SU}(G)$ is infinite, then $G = H(K)$. If $\mathrm{SU}(G)$ is finite, then the generics of G are non-orthogonal to some fixed field F. Moreover, some subgroup of finite index of G is conjugate to a subgroup of $H(F)$.*

4.6. Semi-minimal analysis. Let $E = \mathrm{acl}_\sigma(E)$, and a a tuple with $\mathrm{SU}(a/E) < \omega$. There are $a_1, \dots, a_n \in \mathrm{acl}_\sigma(Ea)$, such that $a \in \mathrm{acl}_\sigma(Ea_1, \dots, a_n)$, and for every i, either $\mathrm{tp}(a_{i+1}/E(a_i)_\sigma)$ is modular of SU-rank 1, or there is some finite set B, such that the set of realisations of $\mathrm{tp}(a_{i+1}/E(a_i)_\sigma)$ is contained in the perfect closure of the difference field generated by $E(a_i) \cup B \cup F$, where F is some fixed field.

4.7. One can show easily that if a formula $\varphi(x)$ is orthogonal to all fixed fields then $\varphi(x)$ is modular. While the full theory of the set of realisations of $\varphi(x)$ may be unstable, we have what is called quantifier-free ω-stability. Thus, in the case of groups, we get the analogue of 4.2 but only for subsets of G^m defined by quantifier-free formulas (within G^m).

I thought it worthwhile to give a proof of this result, for two reasons. The first is the reaction of the audience during my talk at MSRI: they weren't surprised by the dichotomy results but by their corollaries. The second is that in the particular context of a quantifier-free definable set X of an algebraic group H, the classical proof of [Hrushovski and Pillay 1987] becomes very short, and still retains many of the ingredients which demonstrate the strength of modularity.

PROPOSITION. *Let $K \models$ ACFA, H an algebraic group defined over K, and let G be a definable subgroup of finite SU-rank of $H(K)$. Assume that the formula defining G is orthogonal to all fixed fields, and has its parameters in $E = \mathrm{acl}_\sigma(E)$. Let $X \subseteq H(K)^m$ be a quantifier-free definable set. Then $X \cap G^m$ is a Boolean combination of cosets of subgroups of G^m which are defined in G^m by a quantifier-free formula with parameters in E.*

PROOF. The group G has finite index in the smallest quantifier-free definable group $\bar{G}$ containing it. By 4.3, the group G is modular, which implies that $\bar{G}$ is also modular. We may therefore assume that G is quantifier-free definable. By an easy reduction, we may also assume that $m = 1$ (work in G^m), and that X is an irreducible σ-closed set contained in G. We then want to show that X is the coset of a σ-closed subgroup S of G, and that S is defined over E.

We will assume that the difference field (K, σ) has sufficiently many automorphisms. If Z is a σ-closed set defined over some difference field F, we define $\deg_\sigma(Z) = \max\{\deg_\sigma(a/F) \mid a \in Z\}$. Note that $\deg_\sigma$ is invariant under translation, that is, $\deg_\sigma(Z) = \deg_\sigma(aZ)$ for any $a \in G$. In analogy with algebraic varieties, if Z is an irreducible σ-closed set defined over some field F, we will say that *a is a generic of Z over F* if $a \in Z$ and every difference polynomial over F which vanishes at a, vanishes on Z. Equivalently, if $a \in Z$ and $\deg_\sigma(a/F) = \deg_\sigma(Z)$. One can show that the generics of the group G in the stability theoretic sense (i.e., of maximal SU-rank) are precisely the generics of G in this sense.

Let F be the smallest algebraically closed difference field containing E and over which X is defined. Let $S = \{h \in G \mid hX = X\}$, fix a generic a of X over F, and a generic g of G over $F(a)_\sigma$. Then S is a σ-closed subgroup of G defined over F, and $b = ga$ is a generic of G over $\mathrm{acl}_\sigma(Fa)$. Consider the set $Y = gX$; then b is a generic of Y over $\mathrm{acl}_\sigma(Fg)$.

Claim 1. *Let τ be an automorphism of the difference field (K, σ), which is the identity on F. Then $\tau(Y) = Y \iff \tau(gS) = gS$.*

Proof. Indeed, using the fact that X and S are defined over F, we get: $\tau(Y) = Y \iff \tau(gX) = gX \iff \tau(g)X = gX \iff g^{-1}\tau(g) \in S \iff \tau(gS) = gS$, which gives the result. □

Claim 2. *The fields of definition of Y and of gS are equi-algebraic over F.*

Proof. This follows from Claim 1 and the following two observations: (1) If τ does not fix the field of definition of an irreducible σ-closed set Z, then $\tau(Z) \neq Z$. (2) Let $k_0 \subseteq k_1 \subseteq K$ be fields, with $k_1 \not\subseteq \mathrm{acl}_\sigma(k_0)$. Then there is some automorphism τ of (K, σ) which fixes $\mathrm{acl}_\sigma(k_0)$ and does not fix k_1. □

By modularity and because b is a generic of Y over $\mathrm{acl}_\sigma(Fg)$, the field of definition of Y is contained in $\mathrm{acl}_\sigma(Fb) \cap \mathrm{acl}_\sigma(Fg)$. Choose a $c \in \mathrm{acl}_\sigma(Fb) \cap \mathrm{acl}_\sigma(Fg)$ that generates the field of definition of Y (and the one of gS by Claim 2). Using $b = ga$ and the fact that g and b are independent from a over F, and hence over $F(c)_\sigma$, we obtain that $\deg_\sigma(Y) = \deg_\sigma(b/F(c,a)_\sigma) = \deg_\sigma(g/F(c,a)_\sigma) = \deg_\sigma(gS)$. Hence $\deg_\sigma(S) = \deg_\sigma(X)$, and from $Sa \subseteq X$ and the irreducibility of the σ-closed set X, we deduce that $S = Xa$.

Because g is a generic of the coset gS and by modularity, gS is defined over $\mathrm{acl}_\sigma(Eg)$, which implies that $S = g^{-1}(gS)$ is also defined over $\mathrm{acl}_\sigma(Eg)$. So, S is defined over $\mathrm{acl}_\sigma(Eg) \cap F = E$. □

5. Application: the Manin–Mumford Conjecture over a Number Field

The result of Raynaud [1983] (which implies the Manin–Mumford conjecture) states that if A is an abelian variety and X a subvariety of A, then $\mathrm{Tor}(A) \cap X$ is a finite union of sets of the form $a_i + \mathrm{Tor}(A_i)$, with A_i a group subvariety of A. (Here, $\mathrm{Tor}(A)$ denotes the set of torsion points of A.) This result was later extended by Hindry and McQuillan. It is a particular case of a conjecture of Lang; for details see [Lang 1991, p. 37].

Hrushovski saw that the results on difference fields could be used to obtain a new proof of this theorem, for A a commutative algebraic group defined over a number field K. His proof gives an explicit bound on the number of cosets, of the form $M = c\deg(X)^e$, where c and e depend on A but not on X, and $\deg(X)$ is the degree of the variety X with respect to a fixed embedding of A into projective space. His result appears in [Hrushovski 1995]; see also [Pillay 1997]. His bound is explicit modulo the choice of two primes of good reduction for A; see Section 5.10 for the definition of good reduction. (If A is semi-abelian, let $h(A)$ denote the height of A in the sense of Faltings; according to one specialist, the order of magnitude of a bound for a prime of good reduction is likely to be $h(A)$.)

The strategy is very simple. Suppose we are given a commutative algebraic group A, a subvariety X of A, and some subgroup Γ of A. Then we would like to find an automorphism σ of some large model L of ACFA containing Γ, and a modular definable subgroup G of $A(L)$ containing Γ. The result then would follow by 4.2. This is however too simple to work. There are two problems:

- In characteristic 0, every proper definable subgroup of $\mathbb{G}_a(L)$ is non-orthogonal to the fixed field (see Section 5.9), and is therefore never modular. One gets around this difficulty by reducing to the case of a semi-abelian variety, using model theory.
- In order to get explicit bounds, one needs an explicit description of G (and not only its mere existence). When Γ is the subgroup $\mathrm{Tor}_{p'}(A)$ of prime-to-p-torsion, for p a prime with good properties, then Weil's result on abelian varieties defined over finite fields gives an equation of bounded complexity for σ a lifting of the Frobenius. However, this doesn't say anything on the points of order a power of p. A further trick is needed, involving some model theory and ugly computations.

We indicate below some of the ingredients involved in the proof of Hrushovski. This section is organised as follows. We first introduce some tools and definitions from algebraic geometry, and state the main results used in Hrushovski's proof. Of particular interest in my opinion is his description of definable subgroups of abelian varieties and of their definable endomorphisms. And of course, his criterion for modularity is absolutely fundamental in the proof; see Theorem 5.6. We then show in Section 5.13 how to obtain the qualitative result, and reduce the problem of finding an explicit bound for the number of cosets to the case where the group variety A is a semi-abelian variety.

We give a fairly detailed exposition on how to get the explicit bound. This part is essentially self-contained if one accepts the results stated earlier together with those of Section 5.12. We start with the "easy case" of the p'-torsion subgroup in Theorem 5.14. We then proceed slowly towards a proof of the full result, given in Theorem 5.17.

5.1. Degrees of varieties. We embed our algebraic group A in some projective space $\mathbb{P}_n$. By the degree of a subset of $\mathbb{P}_n$ we mean the degree of its Zariski closure. It is convenient to define a degree on algebraic subsets of cartesian powers of $\mathbb{P}_n$, in such a way that it satisfies the following conditions:

(1) Let $V_1, \ldots, V_r$ be algebraic subsets of $(\mathbb{P}_n)^l$, and let $Z_1, \ldots, Z_s$ be the irreducible components of $V_1 \cap \cdots \cap V_r$. Then
$$\sum_{i=1}^{s} \deg(Z_i) \leq \prod_{j=1}^{r} \deg(V_j).$$
(2) Let V be an algebraic subset of $(\mathbb{P}_n)^l \times (\mathbb{P}_n)^k$, and consider the projection $\rho : (\mathbb{P}_n)^l \times (\mathbb{P}_n)^k \to (\mathbb{P}_n)^l$. Then $\deg(\rho(V)) \leq \deg(V)$.
(3) Let V be an algebraic subset of $(\mathbb{P}_n)^l \times (\mathbb{P}_n)^k$, and let ρ be defined as above. For $a \in (\mathbb{P}_n)^l$ define $V(a) = V \cap \rho^{-1}(a)$. Suppose that $\dim(V(a)) = r$ for generic $a \in \rho(V)$. Then the Zariski closure V^* of the set $\{a \in (\mathbb{P}_n)^l \mid \dim(V(a)) > r\}$ has degree $\leq \deg(V)$.

For the definition of this degree and further properties, see [Fulton 1984, Example 8.4.4] or [Hrushovski 1995].

5.2. Let A be an algebraic group. Then A has a unique maximal connected linear subgroup H, and A/H is an *abelian variety*, i.e., a commutative projective group variety. If H is commutative then the simple factors of H are isomorphic to either the multiplicative group $\mathbb{G}_m$ or the additive group $\mathbb{G}_a$.

A *semi-abelian variety* is a commutative algebraic group A with no simple factor isomorphic to $\mathbb{G}_a$. If A is an abelian variety, then there is an *isogeny* (epimorphism with finite central kernel) from some product $A_1 \times \cdots \times A_n$ onto A, with the A_i's simple abelian subvarieties of A. A good reference for facts on abelian varieties is [Lang 1959].

5.3. We first show how to get from an effective description of G to an effective bound M. The group G will be described as $\{g \in A(K) \mid (g, \sigma(g), \ldots, \sigma^l(g)) \in S\}$ for some algebraic subgroup S of $A \times \sigma(A) \times \cdots \times \sigma^l(A)$. We view A as embedded in $\mathbb{P}_n$, and define $\deg(S)$ and $\deg(X)$ with respect to this embedding. Let $V = S \cap (X \times \sigma(X) \times \cdots \times \sigma^l(X))$. Then $\dim(V) \leq e = \min\{\dim(S), (l{+}1)\dim(X)\}$ and $\deg(V) \leq \deg(X)^{l+1}\deg(S)$. Thus an effective bound for the number of components of the Zariski closure of $G \cap X$ is given by the following result:

LEMMA. *Let $V \subseteq A^{l+1}$ be an algebraic set, and set*
$$\tilde{V} = \{g \in A(K) \mid (g, \sigma(g), \ldots, \sigma^l(g)) \in V\}.$$
Then the Zariski closure of $\tilde{V}$ has degree at most $\deg(V)^{2^{\dim(V)}}$. If V is defined over $L(c)$, where $\sigma(L) = L$, then Z is defined over
$$L\big(\sigma^{-\dim(V)}(c),\ \ldots,\ c,\ \sigma(c),\ \ldots,\ \sigma^{\dim(V)}(c)\big).$$

The proof of this result uses the properties of degrees of varieties stated in Section 5.1. We'll make a simple observation on how the irreducible components of Z are obtained. Let π_0 denote the projection on the first copy of $\mathbb{P}_n$, π_1 the projection on the first l copies of $\mathbb{P}_n$, and π_2 the projection on the last l. The irreducible components of Z are images by π_0 of algebraic subsets W of $\mathbb{P}_n^{l+1}$ satisfying $\sigma\pi_1(W) = \pi_2(W)$. Thus the procedure for getting the irreducible components of Z is as follows: start with some irreducible component W of V. If $\sigma\pi_1(W) = \pi_2(W)$, $\pi_0(W)$ will be an irreducible component of Z. If not, then consider $W \cap \pi_2^{-1}\sigma\pi_1(W)$, look at its irreducible components and repeat the procedure. This procedure stops after $\dim(V) + 1$ steps.

This result needs to be refined to give more information when X varies in a family of varieties (we are now thinking of $X + a$ for various a's in the p-torsion subgroup).

5.4. Notation. Let $\mathbb{P} = (\mathbb{P}_n)^k \times (\mathbb{P}_n)^m$, and $\rho : \mathbb{P} \to (\mathbb{P}_n)^k$ the projection. If Z is a subvariety of $\mathbb{P}$ and $a \in (\mathbb{P}_n)^k$ we define $Z(a) = \{b \in (\mathbb{P}_n)^m \mid (a, b) \in Z\}$, and if $r = \dim(Z(a))$ for generic $a \in \rho(Z)$, we set $Z^* = \{a \in \rho(Z) \mid \dim(Z(a)) > r\}$.

Proposition. *Let $(K, \sigma) \models$ ACFA, and let V be a closed subset of $\mathbb{P}^l$ defined over K. There exist irreducible subvarieties Z_i of $\mathbb{P}$ satisfying these properties*:

(1) *If $a \in \tilde{V} =_{\rm def} \{x \in \mathbb{P}(K) \mid (x, \sigma(x), \dots, \sigma^{l-1}(x)) \in V\}$, then there is an i such that $a \in Z_i$, $a \notin \rho^{-1}(Z_i^*)$.*
(2) *$Z_i(K) \cap \tilde{V}$ is dense in Z_i for every i.*
(3) $\sum_i \deg(Z_i) \leq \sum_{j=0}^{\dim(V)} \deg(V)^{2^j} \leq 2\deg(V)^{2^{\dim(V)}}$.
(4) *If $i \neq j$ and Z_i is a proper closed subset of Z_j, then $\rho(Z_i) \subseteq Z_j^*$.*

5.5. Definable endomorphisms and definable subgroups of an abelian variety. Let A be an abelian variety defined over a model (K, σ) of ACFA, and let $\mathrm{End}(A)$ denote the ring of algebraic endomorphisms of A, $\mathrm{End}_\sigma(A)$ the ring of definable endomorphisms of A. Denote by $E(A)$ and $E_\sigma(A)$ the rings $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(A)$ and $\mathbb{Q} \otimes_{\mathbb{Z}} E_\sigma(A)$ respectively. Then $E(A)$ and $E_\sigma(A)$ have a description in terms of matrix rings over $E(A_i)$ and $E_\sigma(A_i)$ for some simple abelian subvarieties of A. The result is well-known for $E(A)$ because of Poincaré's reducibility theorem, and we will describe what happens for $E_\sigma(A)$:

Proposition. *Let A be an abelian variety defined over K.*

(1) *Let $A_1, \dots, A_n$ be abelian subvarieties of A such that A and $A_1 \times \cdots \times A_n$ are isogenous. Let $I \subseteq \{1, \dots, n\}$ be maximal such that if $i \neq j$ are in I and $k \in \mathbb{N}$, then A_i and $\sigma^k(A_j)$ are not isogenous. For each $i \in I$ let $m(i)$ be the number of indices $j \leq n$ such that A_j and $\sigma^k(A_i)$ are isogenous for some $k \in \mathbb{N}$. Then $E_\sigma(A) \simeq \prod_{i\in I} M_{m(i)}(E_\sigma(A_i))$.*
(2) *Let $k \geq 1$ and let B be a definable subgroup of $A^k(K)$. Then B is commensurable with a finite intersection H of kernels of definable homomorphisms*

$A^k(K) \to A(K)$ (*commensurable* means that $B \cap H$ has finite index in both B and H). *If* $k = 1$, *a single homomorphism suffices.*

Thus the study of definable subgroups of $A(K)$ reduces to the study of the rings $E_\sigma(A_i)$, $i \in I$. Of particular interest are the *c-minimal subgroups* of $A(K)$, i.e., definable subgroups which are minimal up to commensurability, because of the following result:

LEMMA. *Let B be a definable subgroup of $A(K)$ A. Then B is modular if and only if, for every $f \in \mathrm{End}_\sigma(A)$, every c-minimal subgroup of $f(B)$ is modular. If $B = \mathrm{Ker}(fg)$ for $f, g \in \mathrm{End}_\sigma(A)$ with infinite kernels, then B is modular if and only if $\mathrm{Ker}(f)$ and $\mathrm{Ker}(g)$ are modular.*

The next result gives a complete description.

5.6. THEOREM. *Let A be a simple abelian variety defined over $K \models$ ACFA.*

(1) *Assume that for every $n \in \mathbb{N}$, A and $\sigma^n(A)$ are not isogenous. Then $E_\sigma(A) = E(A)$, and every definable proper subgroup of $A(K)$ is finite.*
(2) *Assume that $n \geq 0$ is minimal such that there is an isogeny $h : A \to \sigma^n(A)$, and let $h' : \sigma^n(A) \to A$ and $m \in \mathbb{N}^{>0}$ be such that $h'h = [m]$. Define $\psi = \sigma^{-n}h$ and $\psi' = h'\sigma^n$. Then $E_\sigma(A)$ is isomorphic to the twisted Laurent polynomial ring $E(A)[\psi, \psi']$. Note that $\psi'\psi = [m]$.*

From now on we assume that the hypotheses in (2) hold.

(3) *Let $f \neq 0$ be an element of $\mathrm{End}_\sigma(A)$. Then f is onto and $\mathrm{Ker}(f)$ has finite rank.*
(4) *A definable subgroup B of $A(K)$ is c-minimal if and only if it is commensurable with $\mathrm{Ker}(f)$, for some $f \in \mathrm{End}_\sigma(A)$ which is irreducible in $E_\sigma(A)$. Thus, if $f \in \mathrm{End}_\sigma(A)$ is non-zero, then $\mathrm{Ker}(f)$ is modular if and only if $\mathrm{Ker}(g)$ is modular for every irreducible divisor g of f.*
(5) *Let B be a c-minimal subgroup of $A(K)$. If B is not modular, then there is an abelian variety A' defined over $\mathrm{Fix}(\tau)$ for some $\tau = \sigma^m\phi_p^{-n}$, and an algebraic isomorphism $\varphi : A \to A'$ such that $\varphi(B) \subseteq A'(\mathrm{Fix}(\tau^l))$ for some l.*

Similar results hold for the multiplicative group $\mathbb{G}_m$ (with $E_\sigma(\mathbb{G}_m) \simeq \mathbb{Q}[\sigma, \sigma^{-1}]$), and putting everything together, one obtains:

THEOREM. *Let A be a semi-abelian variety defined over $\mathrm{Fix}(\sigma)$, and let $f(T) \in \mathbb{Z}[T]$. Assume that $f(T)$ is relatively prime to all cyclotomic polynomials. Then $\mathrm{Ker}(f(\sigma))$ is orthogonal to the formula $\sigma(x) = x$, and therefore modular if the characteristic is 0.*

5.7. REMARK. In characteristic p, one obtains a similar criterion for semi-abelian varieties defined over $\mathrm{Fix}(\sigma)$ or over $\mathrm{Fix}(\tau)$ for some $\tau = \sigma^{-m}\phi_p^n$.

Also, observe that if A is a simple abelian variety defined over $\mathrm{Fix}(\sigma)$ and if $A(K)$ has a definable subgroup B of finite rank non-orthogonal to the formula

$\sigma^m(x) = x^{p^n}$ for some $m > 0$, $n \in \mathbb{Z}$ with $n \neq 0$, then A must be isomorphic to a variety A' defined over $\mathrm{Fix}(\tau)$, where $\tau = \sigma^{-m}\phi_p^n$. This implies that the field of definition of A is contained in a finite algebraic extension of $\mathrm{Fix}(\tau)$, and therefore is finite, since $\mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\tau^l) = \mathrm{Fix}(\sigma, \phi_p^{nl}) \subseteq \mathbb{F}_{p^{nl}}$.

Assume that A is defined over the finite field $\mathbb{F}_q$ fixed by σ. Let $f(T) \in \mathbb{Z}[T]$, and consider the subgroup B of $A(K)$ defined by the equation $f(\sigma)(x) = 0$. Let $\alpha_1, \ldots, \alpha_r$ be the roots of $f(T) = 0$ (in $\mathbb{C}$). Going to some power of τ, we may assume that σ^m and ϕ_p^n commute with all elements of $\mathrm{End}(A)$ (and fix the field of definition of A). To finish the discussion we need the following result of Weil (see [Weil 1971] or [Mumford 1974, pp. 203 and 205]), which will also be used in the proof:

Theorem. *Let A be an abelian variety defined over a finite field $\mathbb{F}_q$, and consider the endomorphism $\phi_q : x \mapsto x^q$ of A. If $\omega_1, \ldots, \omega_{2d}$ are the roots in $\mathbb{C}$ of the characteristic polynomial of ϕ_q on $A(\mathbb{F}_q^{\mathrm{alg}})$, then $d = \dim(A)$, the ω_i's are algebraic integers of modulus $|\omega_i| = q^{1/2}$, and q/ω_i is among the ω_j's.*

Hence, the endomorphism τ satisfies a functional equation $g(T) = 0$ on B, where the roots of $g(T)$ are of the form $\alpha_i^{-m}\omega_j^l$, where l is such that $q^l = p^n$. Thus, B is orthogonal to $\mathrm{Fix}(\tau)$ if and only if no $\alpha_i^{-m}\omega_j^l$ is a root of unity.

Thus we obtain: B is modular if and only if $\alpha_i^{-m}\omega_j^l \neq 1$ for every i and j, $m \neq 0$ and l.

5.8. Before going on with Hrushovski's proof, we mention an easy corollary of his characterisation of modular subgroups.

Proposition. *Let A be a semi-abelian variety, and X a subvariety of A. Assume that m is an integer > 1 and prime to the characteristic of the field of definition of A, such that $[m]X = X$. Then $X = a + C$ for some group subvariety C of A and element $a \in A[m-1]$.*

Proof. Let k be an algebraically closed field over which X and A are defined, and embed k in a model (L, σ) of ACFA, with σ being the identity on k. By assumption, if u is a generic of X, then so is $[m]u$, and they have the same type (in the language of fields) over k. Hence, in L there is a generic u of X such that $\sigma(u) = [m]u$. Consider the subgroup B of A defined by the equation $\sigma(x) = [m]x$. Since $m > 1$ is prime to the characteristic of k, B is modular. Hence, $B \cap X$ is a finite union of cosets of definable subgroups of B. On the other hand, $B \cap X$ contains a generic point of X, which implies that one of these cosets is Zariski dense in X. This shows that $X = a + C$ for some algebraic subgroup C of A. We also have: $[m]X = [m]a + C = X = a + C$, which implies that $[m-1]a \in C$. Since C is divisible, we may choose $a \in A[m-1]$. $\square$

5.9. Definable subgroups of $\mathbb{G}_a(K)$. The ring of endomorphisms of $\mathbb{G}_a$ definable in the model (K, σ) of ACFA contains the twisted ring $\mathrm{End}_K(\mathbb{G}_a)[\sigma, \sigma^{-1}]$, with the appropriate action of σ on $\mathrm{End}_K(\mathbb{G}_a)$. If the characteristic is 0, then

$\mathrm{End}_K(\mathbb{G}_a)$ is canonically isomorphic to K. If the characteristic is $p>0$, then $\mathrm{End}_K(\mathbb{G}_a)$ is generated over K by the Frobenius $\phi_p : x \mapsto x^p$.

In characteristic 0, a definable subgroup of $\mathbb{G}_a(K)$ will be commensurable to a subgroup defined by an equation $\sum_{i=0}^n a_i\sigma^i(x)=0$ for some n and $a_0,\dots,a_n\in K$. One checks easily that a polynomial $\sum_{i=0}^n a_i\sigma^i$ with $a_n=1$ can be written as a product of linear terms of the form $\sigma-a$. Furthermore, if $a\neq 0$ then the solution set of $\sigma(x)=ax$ is non-orthogonal to the fixed field: if b_1 and b_2 are two solutions then $\sigma(b_1/b_2)=b_1/b_2$.

5.10. Hypotheses and some notations. Let A be a commutative algebraic group defined over a number field K. Choose a sequence $(0)=D_0\subset D_1\subset\cdots\subset D_s=A$ of algebraic subgroups of A such that each factor D_{i+1}/D_i is a K-irreducible abelian variety or torus for $i\geq 1$. Let $\{E_j\}$ be a set of representatives of the K-isogeny classes of the factors D_{i+1}/D_i and define $d=\sum\dim(E_j)$. Note that this number d does not change when we take powers of A.

We fix a prime p of good reduction, by which we mean: if $\mathbb{F}_q$ is the residue field of K modulo p and $\bar{D}_i$ denotes the algebraic set obtained by reducing modulo p, then each $\bar{D}_i$ is a reduced connected algebraic group. Moreover, for each $i\geq 1$, $\bar{D}_{i+1}/\bar{D}_i$ and D_{i+1}/D_i have the same dimension and are of the same type (i.e., an abelian variety or a torus). We also request that $\bar{D}_1$ be a vector group.

We denote by $\mathrm{Tor}_{p'}(A)$ the subgroup of torsion elements of A of order prime to p, and by $\mathrm{Tor}_p(A)$ the subgroup of torsion elements of A of order a power of p. Then $\mathrm{Tor}(A)=\mathrm{Tor}_{p'}(A)\oplus\mathrm{Tor}_p(A)$.

5.11. Proposition. *With notation as above, there is $\sigma\in\mathrm{Aut}(\mathbb{Q}^{\mathrm{alg}})$ and an integral polynomial $F(T)$ with no roots of unity among its roots, such that $F(\sigma)$ vanishes on $\mathrm{Tor}_{p'}(A)$. Furthermore, the degree of F is at most $2d$ and the sum of the absolute values of its coefficients is bounded by $(1+q^{1/2})^{2d}$.*

Proof. Consider the Frobenius map $\phi_q : x\mapsto x^q$ defined on $\mathbb{F}_p^{\mathrm{alg}}$, and let $\sigma\in\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/K)$ be a lifting of ϕ_q. Note first that our assumptions on p imply that reduction modulo p induces an isomorphism $\mathrm{Tor}_{p'}(A)\to\mathrm{Tor}_{p'}(\bar{A})$. Thus, for $F(T)\in\mathbb{Z}[T]$, if $F(\phi_q)$ vanishes on $\mathrm{Tor}_{p'}(\bar{A})$, then $F(\sigma)$ will automatically vanish on $\mathrm{Tor}_{p'}(A)$.

Note also that if $f(T),g(T)\in\mathbb{C}[T]$, then the sum of the absolute values of the coefficients of $fg(T)$ is no greater than the product of the sums of the absolute values of the coefficients of $f(T)$ and of $g(T)$. It therefore suffices to show the assertion for each of the factors $\bar{D}_{i+1}/\bar{D}_i$ and for $\bar{D}_1$. Since $\bar{D}_1$ has no points of order prime to p, we may take the constant polynomial 1. If $\bar{D}_{i+1}/\bar{D}_i$ is a K-simple abelian variety, then Weil's result 5.7 gives us a monic polynomial of degree $2\dim(\bar{D}_{i+1}/\bar{D}_i)$, with roots of modulus $q^{1/2}$. Hence the sum of the absolute values of the coefficients of this polynomial is $\leq(1+q^{1/2})^{2\dim(D_{i+1}/D_i)}$. Assume that $\bar{D}_{i+1}/\bar{D}_i$ is a torus, isomorphic to $\mathbb{G}_m^n$ via an algebraic map φ defined over the finite field $\mathbb{F}_{q^l}$. The Frobenius map on $\bar{D}_{i+1}/\bar{D}_i$ induces an automorphism ψ of $\mathbb{G}_m^n$, which is the composition of $\theta = \varphi \circ \phi_q(\varphi)^{-1}$ with raising to the q-th power in $\mathbb{G}_m^n$. Since $\theta \in \mathrm{End}(\mathbb{G}_m^n) \simeq \mathrm{GL}_n(\mathbb{Z})$, it is left fixed by ϕ_p. Hence,

$$\theta^l = \theta \circ \phi_q(\theta) \circ \cdots \circ \phi_q^{l-1}(\theta) = \mathrm{id},$$

which implies that the roots of the characteristic polynomial of θ in $\mathrm{GL}_n(\mathbb{Z})$ are roots of unity. Thus, the characteristic polynomial of ψ has degree n and its roots have absolute value q. Going back to $\bar{D}_{i+1}/\bar{D}_i$ we get the result.

Since we may choose the same polynomial within a K-isogeny class, we get the correct bounds. □

5.12. Now comes the time to take care of the vector subgroup of G (a *vector group* is an algebraic group isomorphic to a product of copies of the additive group $\mathbb{G}_a$). For that, we need two results, which we state below. The proof of the Proposition uses model theory and the full strength of Theorem 4.1. In positive characteristic the proof seems to work for quantifier-free definable subsets of G. The proof of the lemma is purely algebraic.

DEFINITION. Let A be a commutative algebraic group, and let V be the maximal vector subgroup of A. A definable set $X \subseteq A(K)$ is *special* if it is of the form $Y + C$ where Y is a definable subset of $V(K)$ and C is a coset of a definable subgroup of $A(K)$. Similarly, an algebraic subset of A is *special* if it is of the form $Y + C$ where Y is an algebraic subset of V and C is a coset of an algebraic subgroup of A.

PROPOSITION. *Assume characteristic* 0. *let* $(K,\sigma) \models \mathrm{ACFA}$ *and let A be a commutative algebraic group defined over* $\mathrm{Fix}(\sigma)$. *Let $F(T) \in \mathbb{Z}[T]$ be a polynomial with no root of unity among its roots, and let $G = \{g \in A(K) \mid F(\sigma)(g) = 0\}$. Then every definable subset of G is a finite Boolean combination of special subsets of G. If X is a subvariety of A, then $X \cap G$ is a finite union of special subvarieties of A.*

LEMMA. *Let A be a commutative algebraic group defined over $\mathbb{Q}^{\mathrm{alg}}$, and T the group of torsion points of A (or of prime-to-p torsion points of A). Let X be a subvariety of A and assume that $X \cap T \subseteq \bigcup_{i=1}^M D_i$, where each D_i is a special subvariety of X. Then the Zariski closure of $X \cap T$ is the union of at most M cosets of group subvarieties of A. More precisely, for every i, $D_i \cap T$ is either empty or its Zariski closure is the coset of a group subvariety of A.*

5.13. The qualitative result and reduction to the semi-abelian case. Let A be a commutative algebraic group defined over the number field K, let V be the maximal vector subgroup of A and $B = A/V$. We want to find $\sigma' \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/K)$ and $G(T) \in \mathbb{Z}[T]$ such that $G(\sigma')$ vanishes on $\mathrm{Tor}(A)$. Since the reduction map $A \to B$ is injective on $\mathrm{Tor}(A)$, it suffices to find σ' and $G(T)$ such that $G(\sigma')$ vanishes on $\mathrm{Tor}(B)$.

By Proposition 5.11 applied to two primes p and l of good reduction for B, there are $\sigma \in \mathrm{Gal}(K(\mathrm{Tor}_{p'}(B))/K)$ and $\tau \in \mathrm{Gal}(K(\mathrm{Tor}_p(B))/K)$, and polynomials $F_p(T), F_l(T) \in \mathbb{Z}[T]$, with no roots of unity among their roots, and such that $F_p(\sigma)$ vanishes on $\mathrm{Tor}_{p'}(B)$ and $F_l(\tau)$ vanishes on $\mathrm{Tor}_p(B)$.

Using a result of Serre [1985/86], one can show that the field

$$L = K(\mathrm{Tor}_{p'}(B)) \cap K(\mathrm{Tor}_p(B))$$

is a finite Galois extension of K, over which $K(\mathrm{Tor}_{p'}(B))$ and $K(\mathrm{Tor}_p(B))$ are linearly disjoint. Hence, for $m = [L : K]$, there is $\sigma' \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/L)$ that extends σ^m on $K(\mathrm{Tor}_{p'}(B))$ and τ^m on $K(\mathrm{Tor}_p(B))$. Let $\alpha_1, \ldots, \alpha_{2d}$ and $\beta_1, \ldots, \beta_{2d}$ be the roots of $F_p(T)$ and $F_l(T)$ respectively, and define

$$G(T) = \prod_{i=1}^{2d} (T - \alpha_i^m)(T - \beta_i^m).$$

Then $G(\sigma')$ vanishes on $\mathrm{Tor}(B)$, and $\mathrm{Ker}(G(\sigma'))$ defines a modular subgroup of B in any model of ACFA extending $(\mathbb{Q}^{\mathrm{alg}}, \sigma')$.

This shows immediately, by the two results in Section 5.12, that the Zariski closure of $X \cap \mathrm{Tor}(A)$ is the union of finitely many cosets of group subvarieties of A. However, since we don't know $[L : K]$, we cannot expect to get an explicit bound on the number of cosets. To get the explicit bound we reduce to the semi-abelian case via the following observation:

Let Y be the image of X in B. Then the map $A \to B$, which is injective on $\mathrm{Tor}(A)$, establishes a bijection between the irreducible components of the Zariski closure of $X \cap \mathrm{Tor}(A)$ and the irreducible components of the Zariski closure Z of $Y \cap \mathrm{Tor}(B)$. Thus the Zariski closure of $X \cap \mathrm{Tor}(A)$ is the union of at most $\deg(Z)$ cosets of algebraic subgroups of A. So, we have

THEOREM. *Let A be a commutative algebraic group defined over the number field K, let X be a subvariety of A. Then $X \cap \mathrm{Tor}(A) = \bigcup_{i=1}^{M} a_i + \mathrm{Tor}(A_i)$ where each A_i is an algebraic subgroup of A. Let V be the maximal vector subgroup of A, and Y the image of X in $B = A/V$. The number M is bounded by the number of irreducible components of the Zariski closure of $Y \cap \mathrm{Tor}(B)$.*

5.14. THEOREM (THE BOUND ON M IN THE CASE OF THE p'-TORSION SUBGROUP). *Let A be a commutative algebraic group over a number field K, let X be a subvariety of A, and fix a prime p such that A has good reduction at p. Let q be the size of the residue field of K at p. Then*

$$X \cap \mathrm{Tor}_{p'}(A) = \bigcup_{i=1}^{M} a_i + \mathrm{Tor}_{p'}(A_i),$$

where each A_i is an algebraic subgroup of A. If $d \leq \dim(A)$ is defined as in Section 5.10, and if d_+ is the degree of the graph of addition in A^3, then

$$M \leq \left(\deg(X)^{2d+1} d_+^{2d^2(2d+1)(\log_2(1+q^{1/2})+1)^2}\right)^{2^{d \dim(X)}}.$$

Proof. Choose σ and $F(T) = \sum_{i=0}^{2d} m_i T^i$ as in 5.11, and work in a model of ACFA extending $(\tilde{\mathbb{Q}}, \sigma)$. Let $\tilde{S} = \operatorname{Ker} F(\sigma)$ and consider the subgroup S of A^{2d+1} defined by $\{(a_0, \ldots, a_{2d}) \in A^{2d+1} \mid \sum_{i=0}^{2d} [m_i] a_i = 0\}$. Using the fact that $\sum_i |m_i| \leq (1 + q^{1/2})^{2d}$, and that multiplication by a number $M \geq 2$ can be achieved with $\log_2(M)(\log_2(M) + 1)/2$ additions, one obtains $\deg(S) \leq d_+^{2d^2(2d+1)(\log_2(1+q^{1/2})+1)^2}$. Let Z be the Zariski closure of $\tilde{S} \cap X$. Then 5.3 gives

$$\deg(Z) \leq (\deg(X)^{2d+1} \deg(S))^{2^{2d \dim(X)}}.$$

Furthermore, by modularity of $\tilde{S}$, Z consists of cosets of algebraic subgroups of A. Each of these cosets intersects $\operatorname{Tor}_{p'}(A)$ in either the empty set or a Zariski dense set. This gives the result. $\square$

5.15. The whole torsion subgroup. Finding the bound on M in the case of all torsion is rather involved. By the qualitative result in Section 5.13 we may assume that A is semi-abelian. Fix two primes p and l of good reduction for A, and let $F_p(T), F_l(T) \in \mathbb{Z}[T]$ and $\sigma, \tau \in \operatorname{Aut}(\mathbb{Q}^{\mathrm{alg}})$ be as in 5.13. Choose also some (K_p, σ) and (K_l, τ) models of ACFA and extending $(\mathbb{Q}^{\mathrm{alg}}, \sigma)$ and $(\mathbb{Q}^{\mathrm{alg}}, \tau)$ respectively. We may, and will, identify the fields K_p and K_l. That is, we are working in a large algebraically closed field $K_p = K_l$, with two distinguished automorphisms σ and τ. Write $F_p(T) = \sum_{i=0}^{2d} m_i T^i$ and $F_l(T) = \sum_{i=0}^{2d} n_i T^i$. Put

$$S_q = \left\{ (a_0, \ldots, a_{2d}) \;\middle|\; \sum_i [m_i] a_i = 0 \right\}$$

and

$$\tilde{S}_q = \{ a \in A(K_p) \mid (a, \sigma(a), \ldots, \sigma^{2d}(a)) \in S_q \},$$

and define the sets S_l and $\tilde{S}_l$ similarly. The groups $\tilde{S}_q$ and $\tilde{S}_l$ are modular in the structures (K_p, σ) and (K_l, τ) respectively.

Set also

$$\omega_1 = 2d \dim(X) \quad (\leq 2d \dim(A)), \quad \omega_2 = 2\omega_1 + 1, \quad \omega_3 = 2d\omega_2 \dim(A).$$

We know that if b is any element of A, then $(X - b) \cap \tilde{S}_q$ is of the form $C_b(K_p) \cap \tilde{S}_q$, with $C_b(K_p) \cap \tilde{S}_q$ Zariski dense in C_b, and where C_b is a finite union of cosets of algebraic subgroups of A; moreover we know that C_b is defined over $L(\sigma^{-\omega_1}(b), \ldots, \sigma^{\omega_1}(b))$, where $L = \sigma(L)$ is a finite Galois extension of K over which X is defined.

We first define the various components of C_b uniformly in b. For that we need to look at the Zariski closure of the set $(\sigma^{-\omega_1}(b), \ldots, \sigma^{\omega_1}(b), a)$ when b ranges over $A(K_p)$, $a \in \tilde{S}_q$ and $a + b \in X$, and more precisely at the algebraic set which defines it, i.e., at the algebraic subset S of $(A^{\omega_2} \times A)^{2d+1}$ defined by:

(1) $(x_0, \ldots, x_{2d}) \in S_q$;

(2) $(x_i + y_{0,i}) \in \sigma^i(X)$ for $0 \leq i \leq 2d$;

(3) $\quad y_{j,i+1} = y_{j+1,i} \quad$ for $0 \leq i \leq 2d-1, \ -\omega_1 \leq j \leq \omega_1$.

A word about the indices: x_i corresponds to $\sigma^i(a)$, and $y_{j,i}$ to $\sigma^i(\sigma^j(b))$. One verifies that

$$\dim(S) = 2d\dim(A) + (2d+1)\dim(X) + 2\omega_1\dim(A) \leq (4d+\omega_2)\dim(A),$$
$$\deg(S) \leq \deg(A)^{2\omega_1}\deg(S_q)(\deg(X)d_+)^{2d+1}.$$

We now apply Lemma 5.4 to S and obtain a set of irreducible subvarieties W_i of $A^{\omega_2} \times A$, such that, if $\rho : A^{\omega_2} \times A \to A^{\omega_2}$ is the projection, the following conditions hold:

(i) If $(b,a) \in \tilde{S} =_{\text{def}} \{(b,a) \mid ((b,a),\ldots,\sigma^{2d}(b,a)) \in S\}$, then for some i we have $(b,a) \in W_i$ and $b \notin W_i^*$.
(ii) The set $\tilde{W}_i = W_i(K_p) \cap \tilde{S}$ is Zariski dense in W_i.
(iii) $\sum_i \deg(W_i) \leq \sum_{i=0}^{\dim(S)} \deg(S)^{2^i} \leq 2\deg(S)^{2^{\dim(S)}}$.

By (ii) we may choose $(b,a) \in \tilde{S}$ which is a generic of W_i (in the sense of the Zariski topology). Since W_i is irreducible, we know that the irreducible components of $\rho^{-1}(b) \cap W_i$ are conjugate over $L(b)$. Since $\tilde{S}_q$ is modular we also know that these components are cosets of some algebraic subgroups of A. Let A_i be the algebraic subgroup of A such that the component of $\rho^{-1}(b) \cap W_i$ containing (b,a) is a coset of A_i. If c is a generic of A_i, then $(b,a+c)$ is a generic of $\rho^{-1}(b) \cap W_i$ and therefore $(b,a+c)$ is a generic of W_i. Since W_i is closed this shows that $W_i = W_i + ((0) \times A_i)$, and therefore that for every $y \in \rho(W_i)$, $\rho^{-1}(y) \cap W_i$ is a union of cosets of A_i. Furthermore these cosets are finite in number if $y \notin W_i^*$.

5.16. Working on W_i. Fix i, let $W_i^0 = W_i \setminus \rho^{-1}(W_i^*)$, $B_i = A/A_i$ and let $\theta_i : A \to B_i$ be the natural projection. For $j \in \mathbb{Z}$ let $\tau^j(B_i) = A/\tau^j(A_i)$ and $\tau^j(\theta_i) = \tau^j\theta_i\tau^{-j} : A \to \tau^j(B_i)$. Define also $B_i' = \prod_{j=0}^{\omega_3} \tau_j(B_i)$, $C = A^{\omega_2}$.

We are interested in the set $\Theta_i = \{(b,\theta_i(a)) \mid (b,a) \in \tilde{W}_i, \ b \notin W_i^*, b \in \tilde{S}_l^{\omega_2}\}$. Note that if $(b,c) \in \Theta_i$ then $c \in L(b)^{\text{alg}}$. From $\deg_\tau(b) \leq 2d\omega_2\dim(A) = \omega_3$ we deduce that $\deg_\tau(c) \leq \omega_3$.

Let $R \subseteq C^{\omega_3+1}$ be defined by

$$R = \left\{ (y_0,\ldots,y_{\omega_3}) \in C^{\omega_3+1} \;\middle|\; \sum_{j=0}^{2d} [n_j] y_{i+j} = 0 \text{ for } 0 \leq i \leq \omega_3 - 2d \right\}.$$

Then $\dim(R) = \omega_3$ and $\deg(R) \leq \deg(S_l)^{\omega_2(\omega_3-2d+1)}$. Consider now the closed set $U_i \subseteq (C \times B_i) \times (C \times \tau(B_i)) \times \cdots \times (C \times \tau^{\omega_3}(B_i))$ which is the Zariski closure of the set of tuples $((y_0,z_0),\ldots,(y_{\omega_3},z_{\omega_3}))$ satisfying:

- $(y_0,\ldots,y_{\omega_3}) \in R$.
- For every $0 \leq j \leq \omega_3$, and x_j such that $\tau^j(\theta)(x_j) = z_j$, $(y_j,x_j) \in \tau^j(W_i^0)$.

We also let V_i be the image of U_i in B_i' under the natural projection

$$(C \times A)^{\omega_3+1} \to A^{\omega_3+1} \to \prod_{j=0}^{\omega_3} \tau^j(B_i).$$

Then $\deg(V_i) \leq \deg(U_i) \leq \deg(R)\deg(W_i)^{\omega_3+1}$, and $\dim(U_i) = \dim(V_i) \leq \dim(R) \leq \omega_3$.

By Theorem 5.14 the Zariski closure Z_i of $V_i \cap T_{p'}(B_i')$ is a finite union of cosets of definable subgroups of B_i', and $\dim(Z_i) \leq \omega_3$. Moreover,

$$\deg(Z_i) \leq (\deg(V_i)^{2d+1}\deg(S_q)^{\omega_3+1})^{2^{2d\dim(R)}}.$$

Claim. $\tilde{Z}_{i,\tau} = \{a \in B_i \mid (a, \tau(a), \ldots, \tau^{\omega_3}(a)) \in Z_i\}$ is a finite union of cosets of τ-definable subgroups of B_i of finite SU-rank.

Proof. Being a coset of a subgroup is a property preserved under homomorphisms and intersections. The first assertion follows since $\tilde{Z}_{i,\tau}$ is obtained from Z_i using projections, intersections, and the maps τ, τ^{-1}.

Let a be a generic of $\tilde{Z}_{i,\tau}$. Since $\dim(Z_i) \leq \omega_3$, we have

$$\operatorname{tr}\deg(a, \tau(a), \ldots, \tau^{\omega_3}(a)) \leq \omega_3,$$

which implies that $\deg_\tau(a) < \infty$ and that the SU-rank of $\tilde{Z}_{i,\tau}$ in (K_l, τ) is finite. $\square$

Now consider the set

$$\tilde{U}_{i,\tau} = \{(b,a) \in \tilde{S}_l^{\omega_2} \times B_i \mid ((b,a), \ldots, \tau^{\omega_3}(b,a)) \in U_i,\ (a, \ldots, \tau^{\omega_3}(a)) \in Z_i\}.$$

Since $Z_i \subseteq B_i'$ and $((b,a), \ldots, \tau^{\omega_3}(b,a)) \in U_i$ implies $b \in \tilde{S}_l^{\omega_2}$, Lemma 5.3 implies that the Zariski closure of $\tilde{U}_{i,\tau}$ has degree $\leq (\deg(U_i)\deg(Z_i))^{2^{\dim(R)}}$, and $\tilde{U}_{i,\tau} \subseteq \tilde{S}_l^{\omega_2} \times \tilde{Z}_{i,\tau}$. By the claim, $\tilde{Z}_{i,\tau}$ is a union of cosets of definable subgroups of B_i of finite SU-rank. We also know that $\tilde{Z}_{i,\tau}$ is modular (since every element in it is algebraic over a tuple from $\tilde{S}_l$). Hence, every definable subset of $\tilde{S}_l^{\omega_2} \times \tilde{Z}_{i,\tau}$ is a Boolean combination of cosets of definable subgroups of $A^{\omega_2} \times B_i$.

This implies that $\{(\theta_i^{-1}(a) + b_0) \mid (b_{-\omega_1}, \ldots, b_{\omega_1}, a) \in \tilde{U}_{i,\tau}\}$ is the union of at most $(\deg(U_i)\deg(Z_i))^{2^{\dim(R)}}$ cosets of definable subgroups of A.

5.17. Theorem. *Let A be a commutative algebraic group defined over a number field K and X a subvariety of A. Then the Zariski closure of $X \cap \mathrm{Tor}(A)$ consists of finitely many cosets of algebraic subgroups of A, and a bound on the number M of these cosets can be effectively computed (modulo the choice of the primes p and l).*

Proof. The first assertion is proved in Section 5.13. It remains to show that the results of the previous paragraph give us the bound. For that we need to show:

Claim. If $c \in \mathrm{Tor}(A) \cap X$, if $c = a + b$ with $a \in \mathrm{Tor}_{p'}(A)$ and $b \in \mathrm{Tor}_p(A)$ and $b^* = (\sigma^{-\omega_1}(b), \dots, \sigma^{\omega_1}(b))$, then $(b^*, \theta_i(a)) \in \tilde{U}_{i,\tau}$ for some i.

By definition, $a \in \tilde{S}_q$ and $a+b \in X$ so that $(b^*, a) \in \tilde{S}$ (see Section 5.15). Choose i such that $(b^*, a) \in W_i^0$. Then $\tau^j(b^*, a) \in \tau^j(W_i^0)$ and $\tau^j(b^*) \in \tilde{S}_l^{\omega_2}$ for every j. Hence, $((b^*, \theta_i(a)), \dots, \tau^{\omega_3}(b^*, \theta_i(a)) \in U_i$, so that $(b^*, \theta_i(a)) \in \tilde{U}_{i,\tau}$. □

Note also that if $(c_{-\omega_1}, \dots, c_{\omega_1}, d) \in \tilde{U}_{i,\tau}$, then $(c_0 + d) \in X$, so that the Zariski closure of the coset containing $a + b$ is contained in X.

To conclude, we obtain the following bound on the number of cosets: M is bounded by the sum over i of the degrees of the Zariski closures of $\tilde{U}_{i,\tau}$. Unwinding, we get

$$M \leq \sum_i \deg \tilde{U}_{i,\tau} \leq \sum_i (\deg(U_i) \deg(Z_i))^{2^{\omega_3}},$$

$$\sum_i \deg(U_i) \deg(Z_i) \leq \deg(S_q)^{(\omega_3+1)2^{2d\omega_3}} \sum_i \deg(V_i)^{(2d+1)2^{2d\omega_3}+1},$$

$$\sum_i \deg(V_i) \leq \deg(S_l)^{\omega_2(\omega_3-2d+1)} \sum_i \deg(W_i)^{\omega_3+1},$$

$$\begin{aligned}\sum_i \deg(W_i) &\leq 2\deg(S)^{2^{\dim(S)}} \\ &\leq 2(\deg(A)^{2\omega_1} \deg(S_q) \deg(X)^{2d+1} d_+^{2d+1})^{2^{(4d+\omega_2)\dim(A)}},\end{aligned}$$

so that

$$M \leq 2^{M_1} \deg(S_q)^{M_2} \deg(S_l)^{M_3} \deg(A)^{M_4} (d_+ \deg(X))^{M_5},$$

where

$$\begin{aligned}
M_1 &= (\omega_3 + 1)((2d+1)2^{2d\omega_3} + 1)2^{\omega_3}, \\
M_2 &= 2^{(4d+\omega_2)\dim(A)} M_1 + (\omega_3 + 1)2^{(2d+1)\omega_3}, \\
M_3 &= \omega_2(\omega_3 - 2d + 1)((2d+1)2^{2d\omega_3} + 1)2^{\omega_3} \\
M_4 &= 2\omega_1 2^{(4d+\omega_2)\dim(A)} M_1, \\
M_5 &= (2d+1)2^{(4d+\omega_2)\dim(A)} M_1.
\end{aligned}$$

The order of magnitude of ω_3 is $8d^2 \dim(A)\dim(X) \leq 8d^2 \dim(A)^2$.

6. Some Other Applications

In this section we state without proofs some other applications of the results on difference fields. We start with a result of Hrushovski, and conclude with two results by T. Scanlon.

6.1. Reduction of a conjecture of Lang. Let A be a commutative algebraic group defined over a number field K, let Γ be the division group of $A(K)$, i.e., the set of elements $a \in A(K^{\mathrm{alg}})$ such that $[m]a \in A(K)$ for some non-zero integer m. A conjecture of Lang states that if X is a subvariety of A containing no cosets of infinite algebraic subgroups of A, then $X \cap \Gamma$ is finite.

The techniques used in the previous paragraph give the following reduction of the conjecture (also proved by Raynaud, Hindry, McQuillan), with effective bounds:

THEOREM [Hrushovski 1995]. *Let A be a commutative algebraic group defined over a number field, and let Γ be the division group of $A(K)$. Suppose that X is a subvariety of A, containing no cosets of infinite algebraic subgroups of A. One can effectively find an integer M such that $\Gamma \cap X(K^{\mathrm{alg}}) \subseteq \frac{1}{M}A(K)$. Moreover one can effectively find coset representatives r_i of $A(K)/MA(K)$ such that $\Gamma \cap X(K^{\mathrm{alg}}) \subseteq \bigcup_i \frac{r_i}{M} + A(K)$.*

IDEA OF THE PROOF. Fix a prime p of good reduction for A and let $\Gamma_{p'}$ denote the p'-division subgroup of $A(K)$, i.e. we require that the integer m in the definition of division group be prime to p. Let $\mathbb{F}_q$ be the residue field of K at p, σ a lifting of the Frobenius $\phi_q : x \mapsto x^q$ to K, and $F_p(T) \in \mathbb{Z}[T]$ the Weil polynomial.

One first shows that $(\sigma - 1)F_p(\sigma)$ vanishes on $\Gamma_{p'}$. Using the fact that $\mathrm{Ker}(F_p(\sigma))$ is orthogonal to the fixed field and the assumption on X, one then shows that that $X(K^{\mathrm{alg}}) \cap \mathrm{Ker}((\sigma-1)F_p(\sigma))$ is contained in finitely many cosets of $\mathrm{Ker}(\sigma - 1) = A(\mathrm{Fix}(\sigma))$. From this one deduces a number M_p such that $M_p(X(K^{\mathrm{alg}}) \cap \Gamma_{p'}) \subseteq A(K)$.

Choosing another prime l of good reduction for A one obtains a number M_l such that $M_l(X(K^{\mathrm{alg}}) \cap \Gamma_{l'}) \subseteq A(K)$. Then $M_p M_l(X(K^{\mathrm{alg}}) \cap \Gamma) \subseteq A(K)$. The bound $M_p M_l$ is effective, modulo the choice of the two primes p and l. $\square$

6.2. CONJECTURE (TATE AND VOLOCH). *Let G be a semi-abelian variety defined over $\mathbb{C}_p$, and let X be a subvariety of G. There is a constant N such that for any $P \in \mathrm{Tor}(G)$, either $P \in X$ or $d(P, X) > N$.*

Here $\mathbb{C}_p$ is the completion of the algebraic closure of $\mathbb{Q}_p$ (with respect to the p-adic valuation on $\mathbb{Q}_p^{\mathrm{alg}}$), and $d(P,X)$ is a p-adic distance associated to the valuation. If X is a subvariety of an affine space, one defines $d(P,X) = \max\{p^{-v(f(P))} \mid f \in I\}$, where I is the ideal of polynomials defining X. In the general case, one extends the definition by using a cover by affine sets.

When G is a torus, this conjecture is a theorem [Tate and Voloch 1996]. Hrushovski [1996a] proved the conjecture when G is over $\mathbb{Q}_p^{\mathrm{alg}}$, has good reduction, and for prime-to-p torsion points. Scanlon [1998; 1999a] proved the conjecture when G is defined over $\mathbb{Q}_p^{\mathrm{alg}}$. He considers liftings σ of the Frobenius, a Weil polynomial $F_q(T)$, and uses the fact that $\mathrm{Tor}(G) \subseteq \mathrm{Ker}((\sigma - 1)F_q(\sigma))$.

6.3. Drinfeld modules. Let K be an algebraically closed field of positive characteristic p and of positive transcendence degree. Consider the ring $\mathrm{End}_K(\mathbb{G}_a)$ of endomorphisms of $\mathbb{G}_a$ defined over K. Then $\mathrm{End}_K(\mathbb{G}_a)$ is isomorphic to the twisted polynomial ring $K[\phi_p]$. Let $A = \mathbb{F}_p[T]$ and view it as a subring of K, by identifying T with some transcendental $t \in K$.

A *Drinfeld module* (*over* A) is given by a ring homomorphism $\varphi : A \to \mathrm{End}_K(A)$ so that if $\varphi(T) = \sum_{i=0}^n a_i \phi_p^i$, then $a_0 = t$ and $a_n = 1$.

THEOREM [Scanlon 1999b]. *Let φ be a Drinfeld module. Consider K^N as an A-module via φ. If X is a subvariety of K^N then the intersection of X, the A-torsion subgroup of K^N (that is, $\{x \in K^N \mid \varphi(a)(x) = 0$ for some nonzero $a \in A\}$) is a finite union of translates of A-torsion subgroups of algebraic subgroups of K^N.*

References

[Ax 1968] J. Ax, "The elementary theory of finite fields", *Ann. of Math.* (2) **88** (1968), 239–271.

[Chatzidakis and Hrushovski 1999] Z. Chatzidakis and E. Hrushovski, "Model theory of difference fields", *Trans. Amer. Math. Soc.* **351**:8 (1999), 2997–3071.

[Chatzidakis et al. 1999] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, "The model theory of difference fields II: periodic ideals and the trichotomy in all characteristics", preprint, 1999. Available at http://www.logique.jussieu.fr/www.zoe/.

[Cherlin and Hrushovski 1998] G. Cherlin and E. Hrushovski, "Large finite structures", preprint, 1998. Available at http://www.math.rutgers.edu/~cherlin/Paper. Earlier version: "Smoothly approximable structures", 1994.

[Cohn 1965] R. M. Cohn, *Difference algebra*, Tracts in Math. **17**, Interscience, New York, 1965.

[Delon 1998] F. Delon, "Separably closed fields", pp. 143–176 in *Model theory and algebraic geometry*, edited by E. Bouscaren, Lecture Notes in Math. **1696**, Springer, Berlin, 1998.

[Duret 1980] J.-L. Duret, "Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendence", pp. 136–162 in *Model theory of algebra and arithmetic* (Karpacz, 1979), edited by L. Pacholski et al., Lecture Notes in Math. **834**, Springer, Berlin, 1980.

[Fulton 1984] W. Fulton, *Intersection theory*, Ergebnisse der Mathematik (3) **2**, Springer, Berlin, 1984. Second edition, 1998.

[Hrushovski 1991] E. Hrushovski, "Pseudo-finite fields and related structures", manuscript, 1991.

[Hrushovski 1995] E. Hrushovski, "The Manin–Mumford conjecture and the model theory of difference fields", preprint, 1995.

[Hrushovski 1996a] E. Hrushovski, 1996. E-mail to José Felipe Voloch.

[Hrushovski 1996b] E. Hrushovski, "The first-order theory of the Frobenius", preprint, 1996.

[Hrushovski 1996c] E. Hrushovski, "The Mordell–Lang conjecture for function fields", *J. Amer. Math. Soc.* **9**:3 (1996), 667–690.

[Hrushovski and Pillay 1987] U. Hrushovski and A. Pillay, "Weakly normal groups", pp. 233–244 in *Logic colloquium* '85 (Orsay, 1985), edited by the Paris Logic Group, Stud. Logic Found. Math. **122**, North-Holland, Amsterdam, 1987.

[Hrushovski and Pillay 1994] E. Hrushovski and A. Pillay, "Groups definable in local fields and pseudo-finite fields", *Israel J. Math.* **85**:1-3 (1994), 203–262.

[Hrushovski and Pillay 1995] E. Hrushovski and A. Pillay, "Definable subgroups of algebraic groups over finite fields", *J. Reine Angew. Math.* **462** (1995), 69–91.

[Hrushovski and Ž. Sokolović 1994] E. Hrushovski and Ž. Sokolović, "Minimal subsets of differentially closed fields", 1994. To appear in *Trans. Amer. Math. Soc.*

[Hrushovski and Zilber 1996] E. Hrushovski and B. Zilber, "Zariski geometries", *J. Amer. Math. Soc.* **9**:1 (1996), 1–56.

[Kim and Pillay 1997] B. Kim and A. Pillay, "Simple theories", *Ann. Pure Appl. Logic* **88**:2-3 (1997), 149–164.

[Lang 1959] S. Lang, *Abelian varieties*, Interscience, New York, 1959. Reprinted by Springer, New York, 1983.

[Lang 1991] S. Lang, *Number theory III: Diophantine geometry*, Encyclopaedia of Math. Sciences **60**, Springer, Berlin, 1991.

[Macintyre 1997] A. Macintyre, "Generic automorphisms of fields", *Ann. Pure Appl. Logic* **88**:2-3 (1997), 165–180.

[Macintyre $\geq$ 2000] A. Macintyre, "Nonstandard Frobenius". In preparation.

[Mumford 1974] D. Mumford, *Abelian varieties*, 2nd ed., Tata Institute Studies in Mathematics **5**, Oxford U. Press, London, 1974.

[Pillay 1997] A. Pillay, "ACFA and the Manin–Mumford conjecture", pp. 195–205 in *Algebraic model theory* (Toronto, 1996), edited by B. Hart et al., NATO Adv. Studies Inst. Series, C **496**, Kluwer, Dordrecht, 1997.

[Pillay 1998] A. Pillay, "Definability and definable groups in simple theories", *J. Symbolic Logic* **63**:3 (1998), 788–796.

[Raynaud 1983] M. Raynaud, "Around the Mordell conjecture for function fields and a conjecture of Serge Lang", pp. 1–19 in *Algebraic geometry* (Tokyo/Kyoto, 1982), Lecture Notes in Math. **1016**, Springer, Berlin, 1983.

[Scanlon 1998] T. Scanlon, "p-adic distance from torsion points of semi-abelian varieties", *J. Reine Angew. Math.* **499** (1998), 225–236.

[Scanlon 1999a] T. Scanlon, "The conjecture of Tate and Voloch on p-adic proximity to torsion", *Internat. Math. Res. Notices* **1999**:17 (1999), 909–914.

[Scanlon 1999b] T. Scanlon, "Diophantine geometry of the torsion of a Drinfeld module", Preprint, 1999.

[Serre 1985/86] J.-P. Serre, "Résumés des cours au Collège de France", *Annuaire du Collège de France* (1985/86), 95–99.

[Shelah 1980] S. Shelah, "Simple unstable theories", *Ann. Math. Logic* **19**:3 (1980), 177–203.

[Suzuki 1982] M. Suzuki, *Group theory, I*, Grundlehren der mat. Wiss. **247**, Springer, Berlin, 1982.

[Tate and Voloch 1996] J. Tate and J. F. Voloch, "Linear forms in p-adic roots of unity", *Internat. Math. Res. Notices* **1996**:12 (1996), 589–601.

[Wagner 1997] F. Wagner, "Groups in simple theories", preprint, 1997. Available at http://www.desargues.univ-lyon1.fr/home/wagner/publ.html.

[Weil 1971] A. Weil, *Courbes algébriques et variétés abéliennes*, Hermann, Paris, 1971.

Zoé Chatzidakis
Équipe de Logique Mathématique (CNRS - UPRESA 7056)
UFR de Mathématiques, Case 7012
Université Paris 7
2, place Jussieu
75251 Paris Cédex 05
France
zoe@logique.jussieu.fr