TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 359, Number 3, March 2007, Pages 1325–1337
S 0002-9947(06)04312-1
Article electronically published on October 17, 2006

ON ALGEBRAIC σ-GROUPS

PIOTR KOWALSKI AND ANAND PILLAY

Abstract. We introduce the categories of algebraic σ-varieties and σ-groups over a difference field (K, σ). Under a "linearly σ-closed" assumption on (K, σ) we prove an isotriviality theorem for σ-groups. This theorem immediately yields the key lemma in a proof of the Manin-Mumford conjecture. The present paper crucially uses ideas of Pilay and Ziegler (2003) but in a model theory free manner. The applications to Manin-Mumford are inspired by Hrushovski's work (2001) and are also closely related to papers of Pink and Roessler (2002 and 2004).

1. Introduction

The notion of an algebraic σ-variety over a difference field (K, σ) generalizes the notion of an algebraic variety equipped with a self-map. So, if K is an algebraically closed field, and σ an automorphism of K by an *algebraic σ-variety* (over (K, σ)), we mean an algebraic variety X over K together with a morphism ϕ from X to X^σ, sometimes assumed to be dominant. The category of algebraic σ-varieties over a difference field (K, σ) belongs entirely to algebraic geometry, but captures some of the geometry of difference equations. A *trivial* σ-variety is one of the form (X, id), where X is defined over the fixed field of σ. The main result of this paper (Theorem 3.7) is an "isotriviality" theorem for algebraic σ-groups over a "linearly σ-closed" difference field (K, σ): Assume (G, ϕ) to be a separable algebraic σ-group, and X a σ-subvariety of G which generates G (all defined over K). Then there is a normal algebraic σ-subgroup $N < Stab(X)$ of G such that $(G/N, \phi/N)$ is isomorphic to a trivial algebraic σ-group, again with N and the trivializing isomorphism defined over K. The result thus ties up with both issues of descent (to the fixed field of σ) and "periodicity" of ϕ.

The "linearly σ-closed" assumption on (K, σ) is that K is algebraically closed and that linear difference equations over (K, σ) have "enough solutions" in K. The proof of the isotriviality theorem (Theorem 3.7) is elementary, and makes use of a higher Gauss map. It is an adaptation of the more model-theoretic proofs in [10], but the construction also appears in [1].

In section 4 we point out how Theorem 3.7 yields an elementary proof of the Manin-Mumford conjecture concerning the intersection of a subvariety X of a semi-abelian variety A with the torsion subgroup of A. In that section we will go into

Received by the editors January 28, 2005.
2000 *Mathematics Subject Classification.* Primary 14K12.
The first author was supported by funds from NSF Focused Research Grant DMS 01-00979, and by the Polish KBN grant 2 P03A 018 24.
The second author was supported by NSF grants.

more detail regarding the connection with other work and the benefits or even superiority of our methods.

Both authors would like to thank the organizers of the Arizona Winter School in Logic and Number Theory (March 2003) where some of the work presented here was done. Thanks also to the referee for his/her helpful comments on the organization and emphasis of the paper.

2. Algebraic σ-varieties and their basic properties

Let K be an algebraically closed field, which we often assume to have an uncountable transcendence degree. Let Fr denote the Frobenius map $\mathrm{Fr}(x) = x^p$ on K in case K has characteristic $p > 0$.

We identify an algebraic variety X over K with its set of K-rational points.

Let us fix an automorphism σ of K (so (K, σ) is a *difference field*). Let C denote the fixed field $\{x \in K : \sigma(x) = x\}$ of σ. For X a variety over K, X^σ is the variety over K obtained from X by applying σ to the coefficients of the defining data of X. Likewise, if $f : X \to Y$ is a rational map defined over K, we obtain $f^\sigma : X^\sigma \to Y^\sigma$. Note that if X is a quasiprojective variety over K, then $X^\sigma = \sigma(X)$.

By an *algebraic σ-variety* we mean a pair (X, ϕ), where X is a variety over K and $\phi : X \to X^\sigma$ is a morphism defined over K.

We will be interested in several classes of σ-varieties (all maps mentioned below are assumed to be defined over K):

(X, ϕ) is said to be *dominant* if ϕ is dominant, namely $\phi(X)$ is Zariski-dense in X^σ.

(X, ϕ) is *separable* if ϕ is dominant and separable.

(X, ϕ) is *trivial* if X is defined over C and ϕ is the identity on X.

A *σ-morphism* between (X, ϕ) and (Y, ψ) is a morphism $f : X \to Y$ such that the following diagram is commutative:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ \sigma(X) & \xrightarrow[f^\sigma]{} & \sigma(Y) \end{array}$$

Note that the composition of σ-morphisms is also a σ-morphism, so that the family of σ-varieties becomes a category.

A σ-variety (X, ϕ) will be called *σ-isotrivial* if it is σ-isomorphic to a trivial σ-variety.

A *σ-rational map* from (X, ϕ) to (Y, ψ) is a rational map $f : X \to Y$ such that $f^\sigma \circ \phi = \psi \circ f$ holds on a Zariski-dense Zariski open subset of X. If (X, ϕ) is a σ-variety, by a (closed) *σ-subvariety* of (X, ϕ) we mean a (closed) subvariety Y of X such that $\phi(Y) \subseteq Y^\sigma$, namely, such that $(Y, \phi|Y)$ is a σ-variety itself. We will call a σ-subvariety Y of (X, ϕ) dominant (separable) if $(Y, \phi|Y)$ is dominant (separable).

We will say that (X, ϕ) is an irreducible σ-variety if X is irreducible as an algebraic variety.

The following summarizes some straightforward facts about the category of σ-varieties.

Lemma 2.1. *Let (X, ϕ) and (X', ϕ') be σ-varieties and $f : X \to X'$ a σ-morphism.*

(i) *If (X, ϕ) is σ-trivial, and Y is a subvariety of X, then Y is a σ-subvariety if and only if Y is defined over C. In particular a σ-subvariety of a trivial σ-variety is itself trivial.*

(ii) *The Zariski-closure of $f(X)$ is a σ-subvariety of (X', ϕ').*

(iii) *If Y' is a σ-subvariety of (Y', ϕ'), then $f^{-1}(Y')$ is a σ-subvariety of (X, ϕ).*

(iv) *$\{(x, y) \in X \times X : f(x) = f(y)\}$ is a σ-subvariety of $(X \times X, \phi \times \phi)$.*

(v) *If Y_1, Y_2 are σ-subvarieties of (X, ϕ), then so are $Y_1 \cup Y_2$ and $Y_1 \cap Y_2$.*

(vi) *Suppose f is dominant, (X'', ϕ'') is a σ-variety, $g : X' \to X''$ is a morphism (of varieties), and $g \circ f$ is a σ-morphism between (X, ϕ) and (X'', ϕ''). Then g is also a σ-morphism from (X', ϕ') to (X'', ϕ'').*

(vii) *The "σ-rational map" analogues of* (ii), (iii), (iv) *and* (vi) *hold.*

Proof. (i) So our assumption is that X is defined over C and $\phi = \mathrm{id}$. Right to left is clear.

Left to right: Assume Y is a σ-subvariety of (X, id). So $Y^\sigma = Y$. Let c be a finite tuple from K generating the field of definition of Y. So $\sigma(c) = c$, whereby the tuple c is from C and Y is defined over C.

(ii) Let Z be the Zariski-closure of $f(X)$. Then Z^σ is the Zariski-closure of $f^\sigma(X^\sigma)$. For $x \in X$,

$$\phi'(f(x)) = f^\sigma(\phi(x)) \in f^\sigma(X^\sigma) \subseteq Z^\sigma.$$

So $\phi'(z) \in Z^\sigma$ for all $z \in Z$, as $f(X)$ is Zariski-dense in Z.

(iii) If $x \in f^{-1}(Y)$, then

$$f^\sigma(\phi(x)) = \phi'(f(x)) \in Y^\sigma.$$

Hence

$$\phi(x) \in (f^\sigma)^{-1}(Y^\sigma) = (f^{-1}(Y))^\sigma.$$

(iv) follows from (iii), since the diagonal is a σ-subvariety of $(X' \times X', \phi' \times \phi')$.

(v) This is immediate.

(vi) Let $x \in X$ and $x' = f(x)$. Then $\phi'(x') = f^\sigma(\phi(x))$. Hence

$$g^\sigma(\phi'(x')) = g^\sigma \circ f^\sigma(\phi(x)) = (g \circ f)^\sigma(\phi(x)) = \phi''(g(f(x)) = \phi''(g(x')).$$

As $f(X)$ is Zariski-dense in X', we see that for all $x' \in X'$, $g^\sigma(\phi'(x')) = \phi''(g(x'))$, and g is a σ-morphism.

(vii) The same proofs work.

By an *algebraic σ-group*, we mean an algebraic group G (over K) together with a homomorphism of algebraic groups, $\phi : G \to G^\sigma$ (also defined over K). Equivalently, an algebraic σ-group is a group object in the category of algebraic σ-varieties, namely an algebraic σ-variety (G, ϕ) such that G is an algebraic group, and the group operation is a σ-morphism from $(G \times G, \phi \times \phi)$ to (G, ϕ).

By a σ-homomorphism of algebraic σ-groups we mean the obvious thing, a homomorphism of algebraic groups which is also a σ-morphism. Likewise for a σ-subgroup of an algebraic σ-group.

For an algebraic group G, and subvariety X, $\mathrm{Stab}(X)$ denotes as usual $\{g \in G : gX = X\}$, an algebraic subgroup of G.

We begin by compiling some easy facts about σ-groups.

Lemma 2.2. *Let (G, ϕ) be an algebraic σ-group, H a σ-subgroup of (G, ϕ), and X an irreducible dominant σ-subvariety of (G, ϕ). Then:*

(i) $\mathrm{Stab}(X)$ *is a σ-subgroup of (G, ϕ).*

(ii) *The principal homogeneous space G/H has the structure of a σ-variety such that the action of G on G/H is a σ-morphism. If moreover H is normal, then G/H with its σ-variety structure is an algebraic σ-group.*

(iii) *If ϕ is dominant (so surjective), then $Z(G)$, the center of G is a σ-subgroup.*

(iv) *The connected component H^0 of H is a σ-subgroup of (G, ϕ).*

Proof. (i) Let $g \in \mathrm{Stab}(X)$ and $x \in X$. Then $\phi(g)\phi(x) = \phi(gx) \in X^\sigma$. As $\phi(X)$ is Zariski-dense in X^σ, $\phi(g) \in \mathrm{Stab}(X^\sigma) = (\mathrm{Stab}(X))^\sigma$.

(ii) Note that $(G/H)^\sigma = G^\sigma/H^\sigma$. Define

$$\phi/H : G/H \to (G/H)^\sigma, \quad \phi/H(gH) := \phi(g)H^\sigma.$$

Then it is easily checked that $(G/H, \phi/H)$ is a PHS for (G, ϕ) in the category of algebraic σ-varieties.

(iii) As $\phi : G \to G^\sigma$ is surjective, $\phi(Z(G)) \subseteq Z(G^\sigma) = (Z(G))^\sigma$.

(iv) Clearly $\phi(H^0)$ is a connected algebraic subgroup of H^σ, hence contained in $(H^\sigma)^0 = (H^0)^\sigma$.

The next lemma requires a little more work.

Lemma 2.3. *Suppose that (G, ϕ) is a σ-group, (Y, id) is a trivial σ-variety and $h : Y \to G$ is a dominant σ-rational map. Then (G, ϕ) is σ-isotrivial.*

Proof. Note that the connected component of G is a σ-subgroup of (G, ϕ). Likewise every irreducible component of Y is (trivially) a σ-subvariety of (Y, id). Hence we may and will assume that Y and G are irreducible. Let W be the Zariski-closure of $\{(x, y) \in Y \times Y : h(x) = h(y)\}$. By Lemma 2.1(iv), W is a σ-subvariety of $(Y \times Y, \mathrm{id})$, so by Lemma 2.1(i) is defined over C. Let k_0 be a countable subfield of C over which Y and W are defined. Let K_0 be a countable field containing k_0 over which (G, ϕ) and h are defined. Note that for x, y generic points of Y over K_0, $(x, y) \in W$ if and only if $h(x) = h(y)$. It follows that the restriction of W to generic points of Y over k_0 is an equivalence relation. Hence there is an irreducible variety Z defined over k_0 and a dominant rational map $h' : Y \to Z$ defined over k_0 such that for $x, y \in Y$, each generic over K_0, $h'(x) = h'(y)$ if and only if $h(x) = h(y)$. Note that h is a σ-rational dominant map between the trivial σ-varieties (Y, id) and (Z, id). Clearly we obtain a σ-birational isomorphism h'' between (Z, id) and (G, ϕ). The pullback of the group operation on G to Z then gives a generically associative and invertible σ-rational map $* : Z \times Z \to Z$. Again by Lemma 2.1, $*$ is defined over C. A classical theorem of Weil [15] then yields a connected algebraic group H defined over C and a birational isomorphism (defined over C) between Z and H which takes $*$ to the group operation of H. Putting everything together we obtain a σ-birational isomomorphism between (G, ϕ) and (H, id) which takes the group operation of G to that of H. This clearly extends to a σ-isomorphism of σ-groups between (G, ϕ) and (H, id), which completes the proof.

We will need one more σ-isotriviality result, for which the following well-known fact about algebraic groups is needed.

Lemma 2.4. *Let G be a connected algebraic group, and U the unipotent radical of the maximal normal linear subgroup L of G. Let $n > 0$, and let G_n be the connected algebraic subgroup of G generated by $\{x^n : x \in G\}$. Then $G_n \cup U$ generates G.*

Proof. In the characteristic zero case G_n already equals G, but we give a proof valid in all characteristics.

Note that G_n projects onto the abelian variety G/L. Hence we may assume that $G = L$ is linear. Now G/U is reductive, and hence by [6], Exercise 12, is generated by its semisimple elements. For any semisimple $s \in G/U$ there is semisimple $s' \in G$ such that $s'/U = s$. By [6], 15.3, s' is contained in a maximal algebraic torus T of G. But $T^n = T$. Hence G^n projects onto G/U, and we are finished.

The next lemma is obvious.

Lemma 2.5. *Let τ be an automomorphism of K which commutes with σ. Then for any σ-variety (X, ϕ), (X^τ, ϕ^τ) is also a σ-variety. Moreover (X, ϕ) is σ-isotrivial if and only if (X^τ, ϕ^τ) is σ-isotrivial.*

Proposition 2.6. *Let (G, ϕ) be a connected σ-group, and $f : (G, \phi) \to (H, \mathrm{id})$ a surjective σ-homomorphism with finite kernel. Then (G, ϕ) is σ-isotrivial.*

Proof. To begin with, let us note that as f is an n-to 1 homomorphism (some n) and $f^\sigma : G^\sigma \to H$ is likewise, and $f^\sigma = f \circ \phi$, it follows that ϕ is a bijective homomorphism $G \to G^\sigma$. (In fact as the referee noted, a degree counting argument shows that ϕ is an isomorphism of algebraic groups.)

We first prove:

Claim 1. The proposition is true if G is unipotent.

Proof. So assume G to be unipotent and connected and (G, ϕ) to be a σ-group. We show by induction on $dim(G)$ that (G, ϕ) is σ-isotrivial. By Lemma 2.2(iii) and (iv) $Z(G)^0$ is a normal σ-subgroup of (G, ϕ), and as G is unipotent, $dim(Z(G)^0) > 0$. Now let L be the subgroup of $Z(G)^0$ consisting of elements of order p. Then L is an infinite connected normal σ-subgroup of (G, ϕ). We will first show that $(L, \phi|L)$ is σ-isotrivial. By Proposition 11, Chapter VII of [14], L is a vector group, namely isomorphic (over K) to K^d for some d. Hence replacing L by K^d we may assume that $L^\sigma = L$, hence $\phi|L$ is an (abstract) automorphism of the group L. Our assumptions give us a finite-to-one homomorphism f' from $(L, \phi|L)$ onto a trivial σ-group. So ϕ fixes $ker(f')$ setwise and induces the identity on $L/Ker(f')$. It follows easily that $Fix(\phi|L) = \{x \in L : \phi(x) = x\}$ is a subgroup of L of finite index. As L is connected, ϕ is the identity on L. We have shown that L is σ-isotrivial.

By induction hypothesis $(G/L, \phi/L)$ is σ-isotrivial. By Lemma 2, Chapter VII of [14], the projection $\pi : G \to G/L$ has a rational section s. As π is a σ-homomorphism, s is a σ-rational map. As G is generated by L and the image of s, it follows that (G, ϕ) is σ-isotrivial. We have proved Claim 1.

We now return to the general case. Let $N = \ker(f)$. Then N is central (as G is connected). Let $n = |N|$. Thus the n-th power map $g \mapsto g^n$ induces a function $s : H \to G$ (such that $f(s(g)) = g^n$), which is clearly constructible.

Claim 2. $s^\sigma = \phi \circ s$.

Proof. The graph of s is $\{(f(g), g^n) : g \in G\}$. As f is a σ-morphism and H is σ-trivial, we have that $f(g) = f^\sigma(\phi(g))$ for all $g \in G$. Hence for $g \in G$, $(f(g), \phi(g)^n)$ is in the graph of s^σ, which suffices.

As s is constructible there is some $k \geq 0$ and a rational map $s' : H \to \mathrm{Fr}^k(G)$ such that (generically) s coincides with the composition of s' with $\mathrm{Fr}^{-k} : \mathrm{Fr}^k(G) \to G$. By Lemma 2.4, $(\mathrm{Fr}^k(G), \mathrm{Fr}^k(\phi))$ is a σ-group. It follows from Claim 2 that s' is a σ-rational map (from (H, id) to $(\mathrm{Fr}^k(G), \mathrm{Fr}^k(\phi))$). By Lemma 2.3, the algebraic subgroup of $\mathrm{Fr}^k(G)$ generated by $\mathrm{im}(s')$ is a σ-isotrivial σ-subgroup. As $\mathrm{im}(s') = \mathrm{Fr}^k(\mathrm{im}(s))$ we conclude by 2.4 that:

Claim 3. The algebraic subgroup of G generated by $\mathrm{im}(s)$ is a σ-isotrivial σ-subgroup.

Now let U be the unipotent radical of the linear part of G.

Claim 4. U is a σ-isotrivial σ-subgroup of (G, ϕ).

Proof. Clearly U^σ is the unipotent radical of the linear part of G^σ. Moreover the bijective homomorphism ϕ takes U to the unipotent radical of G^σ. This shows that U is a σ-subgroup of G. By Claim 1, $(U, \phi|U)$ is σ-isotrivial.

As $\mathrm{im}(s) = \{g^n : g \in g\}$, it follows from Claims 3 and 4 together with Lemma 2.4 that (G, ϕ) is σ-isotrivial.

3. Linearly closed difference fields and an isotriviality theorem

In this section we will we define a genericity property (for (K, σ)) which allows us to prove an important isotriviality theorem for algebraic σ-groups. This isotriviality theorem has its origin in Proposition 4.3 of Hrushovski's [4] which has come to be known as the "socle theorem".

Definition 3.1. Let (K, σ) be a difference field.

(i) By a σ-module over (K, σ) we mean a finite-dimensional vector space V over K together with an additive automorphism $\Phi : V \to V$ such that

$$\Phi(cv) = \sigma(c)\Phi(v) \quad \text{for all } v \in V \text{ and } c \in K.$$

(Equivalently, a σ-module over (K, σ) is a left module for for the noncommutative ring $K[\sigma]$.)

(ii) We say that (K, σ) is linearly closed if (K is algebraically closed and) for any σ-module (V, Φ) over (K, σ), we can find a basis for V over K consisting of vectors $v \in V$ such that $\Phi(v) = v$.

Remark 3.2. A σ-module over (K, σ) can be thought of as yielding the linear difference equation $\Phi(v) = v$ over (K, σ), and linear closedness of (K, σ) means that we can always find over K a "fundamental system of solutions" of such an equation.

Definition 3.3. A difference field (K, σ) is said to be *existentially closed* if any finite system of difference equations and inequations over K with a solution in some difference field extension of (K, σ) already has a solution in K.

Fact 3.4. *The difference field (K, σ) will be linearly closed in either of the following cases:*

(i) *(K, σ) is existentially closed,*

(ii) *K is an algebraically closed field of characteristic $p > 0$, and σ is some integer power of the Frobenius.*

Proof. Let (V, Φ) be a σ-module over (K, σ), where $dim_K(V) = n$, say. After choosing a basis $v_1, ..., v_n$ for V over K, this σ-module becomes $(K^n, A\sigma)$, where A is the (invertible) $n \times n$ matrix over K such that $\Phi((v_1, ..., v_n)^t) = A(v_1, ..., v_n)^t$. So to prove that V has a basis consisting of solutions of $\Phi(v) = v$, it suffices to find a nonsingular $n \times n$ matrix B over K such that $A\sigma(B) = B$. Equivalently,

(*) find $B \in \mathrm{GL}(n, K)$ such that $A = B^{-1}\sigma(B)$.

Case (i). We can easily solve $A = X^{-1}\sigma(X)$, $X \in \mathrm{GL}(n, -)$ in some difference field extension of (K, σ). Namely, simply extend σ to an automorphism of the function field of $\mathrm{GL}(n, -)$ over K by putting $\sigma(X) = AX$. So assuming (K, σ) to be existentially closed, we find a solution in $\mathrm{GL}(n, K)$.

Case (ii). Suppose first that σ is a positive power of the Frobenius, say $\sigma(x) = x^q$. Then we can find B as in (*) by for example Proposition 3 of [14] which says that for a connected algebraic group G defined over $\mathbf{F}_q$ the map taking $g \in G$ to $g^{-1}\sigma(g)$ is surjective. Equivalently, use that fact that $H^1(k, \mathrm{GL}(n))$ is trivial for k perfect.

The general case (where σ is a possibly negative power of the Frobenius) follows because any power of the Frobenius yields a bijection $\mathrm{GL}(n, K) \to \mathrm{GL}(n, K)$.

We now point out that a σ-module over (K, σ) is really the same thing as a "σ-vector group". Recall that a vector group G over an algebraically closed field K is simply an algebraic group over K which is isomorphic (as an algebraic group) to some power of the additive group. As such G has the structure of a vector space over K. By a σ-vector group over (K, σ) we mean a vector group G over K together with an isomorphism (of vector groups, so K-linear), $\phi : G \to G^\sigma$. Note that if V is a vector group, then $\mathrm{Gr}(V)$, the set of linear subspaces of V has the structure of an algebraic variety, and $\mathrm{GL}(V)$ the group of linear transformations of V has the structure of an algebraic group. If (V, ϕ) is a σ-vector group, then $\mathrm{Gr}(V)$ is equipped with the structure of a σ-variety $(\mathrm{Gr}(V), \mathrm{Gr}(\phi))$, where if W is a linear subspace of V, $(\mathrm{Gr}(\phi))(W) = \phi(W)$ a linear subspace of V^σ. Likewise, $\mathrm{GL}(V)$ acquires an algebraic σ-group structure $(\mathrm{GL}(V), \mathrm{GL}(\phi))$, where for $\alpha \in \mathrm{GL}(V))$, and $v \in V^\sigma$, $((\mathrm{GL}(\phi))(\alpha))(v) = \phi\alpha\phi^{-1}(v)$.

Fact 3.5. *Suppose (K, σ) is linearly closed, and (V, ϕ) is a σ-vector group. Then*

(i) *(V, ϕ) is isotrivial, in fact is linearly isomorphic to a trivial σ-vector group.*

(ii) *Both $(\mathrm{Gr}(V), \mathrm{Gr}(\phi))$ and $(\mathrm{GL}(V), \mathrm{GL}(\phi))$ are also isotrivial.*

Proof. (i) Note that $(V, \phi^{-1}\sigma)$ is a σ-module over (K, σ). By Fact 3.4, let $v_1, .., v_n$ be a basis of V consisting of solutions of $\phi^{-1}\sigma(v) = v$, namely of $\phi(v) = \sigma(v)$. This basis gives rise to an isomorphism $f : V \to K^n$, which is a σ-isomorphism between (V, ϕ) and (K^n, id).

(ii) follows directly. □

Lemma 3.6. *Let (G, ϕ) be a separable σ-group. Then $(G/Z(G), \phi/Z(G))$ is σ-isotrivial.*

Proof. By Lemma 2.2(ii) and (iii), $(G/Z(G), \phi/Z(G))$ is a σ-group and the quotient map from G to $G/Z(G)$ is a σ-homomorphism.

Let V denote the Lie algebra (tangent space to identity) of G, and let $\mathrm{Ad}_G : G \to \mathrm{GL}(V)$ be the adjoint representation. Note that V^σ is the Lie algebra of G^σ. As $\phi : G \to G^\sigma$ is separable, its differential $\phi' : V \to V^\sigma$ is an isomorphism (of K-vector spaces), whence (V, ϕ') is a σ-vector group. By Fact 3.5, $(\mathrm{GL}(V), \mathrm{GL}(\phi'))$ is an isotrivial algebraic σ-group. It is rather easy to see that Ad_G is actually a σ-homomorphism from (G, ϕ) to $(\mathrm{GL}(V), \mathrm{GL}(\phi'))$. As $\ker(\mathrm{Ad}_G) = Z(G)$, we obtain a σ-embedding

$$\psi : (G/Z(G), \phi/Z(G)) \to (\mathrm{GL}(V), \mathrm{GL}(\phi')).$$

By Lemma 2.1 and Fact 3.5(ii), the image of $(G/Z(G), \phi/Z(G))$ under ψ is σ-isotrivial.

Here is our "isotriviality theorem" for σ-groups.

Theorem 3.7. *Let (G, ϕ) be a separable algebraic σ-group, and X an irreducible σ-subvariety of G which contains the identity and generates G. Then there is a normal connected σ-subgroup N of (G, ϕ) such that $N < \mathrm{Stab}(X)$ and $(G/N, \phi/N)$ is isotrivial.*

Proof. First we recall the generalized Gauss map (see [12] and [10]). Suppose H is an algebraic group, and W an irreducible subvariety of H. Let V be the r-jet of H at the identity, for some $r \geq 1$. (If $r = 1$, V is the tangent space.) Let $F_W : W \to \mathrm{Gr}(V)$ be defined by: $F_W(x)$ is the image of the r-jet at the identity of the variety $x^{-1}W$ in V, a linear subspace of V. F_W is a rational map, and for r sufficiently large, after quotienting by $\mathrm{Stab}(W)$, F_W becomes a birational embedding. Note also that $W/\mathrm{Stab}(W)$ is Zariski-closed in $G/\mathrm{Stab}(W)$.

We now return to the context of the theorem. As ϕ is finite and separable, it induces a linear isomorphism ϕ' from V to V^σ, where V is the r-jet of G at the identity for sufficiently large r. So $(\mathrm{Gr}(V), \mathrm{Gr}(\phi'))$ is a σ-variety. It is easy to check that $\mathrm{Gr}(\phi') \circ F_X = F_{X^\sigma} \circ (\phi|X)$. Thus F_X is a σ-rational map from $(X, \phi|X)$ to $(\mathrm{Gr}(V), \mathrm{Gr}(\phi'))$. By Lemma 2.2(i) and (ii), $(G/\mathrm{Stab}(X), \phi/\mathrm{Stab}(X))$ is a σ-variety and the quotient map $G \to G/\mathrm{Stab}(X)$ is a σ-morphism. By Lemma 2.1(vii), the birational embedding $X/\mathrm{Stab}(X) \to \mathrm{Gr}(V)$ is σ-rational. By Fact 3.5 $(\mathrm{Gr}(V), \mathrm{Gr}(\phi'))$ is isotrivial. By Lemma 2.1(i) and (ii) we conclude that $X/\mathrm{Stab}(X)$ is σ-birational with a trivial σ-variety.

By Lemmas 2.1(v) and 2.2(iii), $\mathrm{Stab}(X) \cap Z(G)$ is a σ-subgroup of G which is clearly normal. Let N' denote this subgroup. By Lemma 2.1(v) the natural embedding of G/N' in $G/\mathrm{Stab}(X) \times G/Z(G)$ is a σ-embedding. By the previous paragraph $X/\mathrm{Stab}(X)$ is σ-birational with some trivial (Y, id). So $X/\mathrm{Stab}(X) \times G/Z(G)$ is σ-birational with $Y \times (G/Z(G))$, which is σ-isotrivial. We clearly obtain a σ-birational isomorphism of X/N' with a σ-subvariety of $Y \times (G/Z(G))$, and so by Lemma 2.1, we see that X/N' is σ-birational with a trivial σ-variety. But X/N' generates G/N', so we easily find some trivial σ-variety and a dominant σ-rational map from it to G/N'. We conclude by Lemma 2.3 that $(G/N', \phi/N')$ is σ-isotrivial. Let N be the connected component of N'. Then by Proposition 2.6, G/N is also σ-isotrivial.

4. On ϕ-invariant subvarieties of semiabelian varieties and the Manin-Mumford conjecture

In this section we give some applications of the general formalism of algebraic σ-groups and in particular of Theorem 3.7. Our main result here is Proposition

4.1(i) and (ii), which concerns algebraic groups G equipped with an isogeny ϕ, and ϕ-invariant subvarieties X of G. This corresponds to Propositions 7.1 and 7.3 in [12]. However their 7.3 deals only with semiabelian varieties, but part (ii) of our Proposition 4.1 below deals with arbitrary algebraic groups.

The importance of Proposition 4.1(i) is that it yields, by standard techniques, the Manin-Mumford conjecture. This was the route in Theorem 3.6 of [12]. So as to make the current paper self-contained and complete, we take the liberty of stating and proving the Manin-Mumford conjecture this way (Theorem 4.3 below). We also discuss a positive characteristic version of Manin-Mumford, and the role of Proposition 4.1(i) and (ii).

Hrushovski's proof [5] of the Manin-Mumford conjecture over number fields has a strong model-theoretic character, depending on a detailed study of definable sets in existentially closed difference fields and a crucial dichotomy theorem [2]. In [10] we gave another proof of the dichotomy theorem using higher Gauss maps (in characteristic zero). We wanted to apply our methods to obtain a direct proof of Manin-Mumford without the model-theoretic detour (as was done for Mordell-Lang in [9]). After seeing [11] and [12] the second author saw how to accomplish this, and this is more or less the approach in the current paper. But [12] also contains a version of Manin-Mumford in positive characteristic, which essentially says that any counterexample is defined over a finite field. Answering a question of the second author, the first author saw how to prove a key lemma in [12] by simply applying the isotriviality theorem in the case where σ is a power of the Frobenius. In fact we generalize the key lemma from [12] from semi-abelian varieties to arbitrary algebraic groups. This is Proposition 4.1(ii) of the current paper. Another proof of the positive characteristic version of Manin-Mumford was given by Scanlon [13], using the "dichotomy theorem" in positive characteristic [3]. Our methods have so far been unable to yield this positive-characteristic dichotomy theorem in full generality.

In any case our treatment of the Manin-Mumford issues here is very closely related in mathematical content to [12], although we believe that our account of the key lemmas (our Proposition 4.1(i) and (ii)) is more elementary and direct. The paper [11] (see also [8]) dealing just with the abelian variety case uses relatively simple arguments, but requiring more sophisticated background theories, such as a result of Ueno on stabilizer-free subvarieties of abelian varieties being of general type, as well as Matsumura's theorem on the automorphism groups of varieties of general type.

Proposition 4.1. (i) *Let K be an algebraically closed field. Let A be a semiabelian variety over K, $\phi : A \to A$ a separable isogeny of A, and X an irreducible subvariety of A containing 0 which generates A and is ϕ-invariant ($\phi(X) \subseteq X$). Assume also that $\mathrm{Stab}_A(X)$ is finite. Then ϕ is an automorphism of A of finite order.*

(ii) *Let K be an algebraically closed field of characteristic $p > 0$, and let G be a connected algebraic group over K. Suppose $\phi : G \to G$ is a surjective homomorphism (of algebraic groups). Let X be an irreducible subvariety of G which contains the identity, generates G, is ϕ-invariant, and has finite stabilizer. Assume that for some $r, s > 0$, $\phi^s \circ \mathrm{Fr}^{-r} : \mathrm{Fr}^r(G) \to G$ is separable. Then there is an algebraic group H defined over $\mathbb{F}_{p^r}$ and an isomorphism f of G with H such that f takes ϕ^s to Fr^r (so (G, ϕ^s) and (H, Fr^r) are isomorphic as algebraic* id*-groups).*

Proof. (i) Without loss of generality there is an automorphism σ of K such that (K, σ) is existentially closed and A, ϕ, X are defined over the fixed field C of σ. By Fact 3.4 (K, σ) is weakly generic and Theorem 3.7 applies. So as $\mathrm{Stab}(X)$ is finite, (A, ϕ) is σ-isotrivial. Thus there is a σ-isomorphism f of (A, ϕ) with (B, id) for some semiabelian variety B defined over C. Now f is defined over a finite extension of C, so for some $s > 0$, $\sigma^s(f) = f$. But clearly $\sigma^s(f)\phi^s = f : A \to B$. It follows that ϕ^s is the identity.

(ii) Let $\psi = \phi^s \circ \mathrm{Fr}^r$. So $(\mathrm{Fr}^r(G), \psi)$ is a separable Fr^{-r} group. By Fact 3.4(ii) and Theorem 3.7, $(\mathrm{Fr}^r(G), \psi)$ is Fr^{-r}-isotrivial, hence there is an algebraic group H defined over $\mathbb{F}_{p^r}$ and an isomomorphism $f : \mathrm{Fr}^r(G) \to H$ such that

$$\mathrm{Fr}^{-r}(f) \circ \phi^s \circ \mathrm{Fr}^{-r} = f : \mathrm{Fr}^r(G) \to H.$$

But also clearly

$$f \circ \mathrm{Fr}^r = \mathrm{Fr}^r \circ \mathrm{Fr}^{-r}(f) : G \to H.$$

So putting these together we see that

$$\mathrm{Fr}^{-r} \circ \phi^s = \mathrm{Fr}^r \circ \mathrm{Fr}^{-r}(f) : G \to H.$$

So $\mathrm{Fr}^{-r}(f)$ is an isomorphism between G and H which takes ϕ^s to Fr^r.

We will now show how the Manin-Mumford conjecture (for semiabelian varieties) follows from Proposition 4.1(i). The proof is an elementary consequence of Proposition 4.1(i) together with the following nontrivial number-theoretic fact.

Fact 4.2. *Let A be a semiabelian variety defined over a number field k. Then there is an automorphism σ of $\bar{k}$ over k, and a monic integral polynomial $P(T) \in \mathbb{Z}[T]$ such that $P(\sigma)$ annihilates $T(A)$, the torsion subgroup of A, and neither* 0 *nor any roots of unity are among the zeroes of $P(T)$.*

Explanation and remarks. Write A additively. If $P(T) = T^n + a_{n-1}T^{n-1} + ... + a_1T + a_0$ and $\sigma \in \mathrm{Gal}(\bar{k}/k)$, then $P(\sigma)$ is the (abstract) endomorphism of $A(\bar{k})$ given by $P(\sigma)(x) = \sigma^n(x) + a_{n-1}\sigma^{n-1}(x) + ... + a_0x$. Details about Fact 4.2 are given in Sections 5 and 6.2 of [5]. Although the condition that $P(0) \neq 0$ is not explicitly mentioned, it is clearly true from the construction there. The abelian variety case is dealt with in Section 3 of [11]. It should be said that a nontrivial result of Serre concerning the intersection of the fields generated over k by the p-torsion and prime-to-p torsion subgroups of $A(\bar{k})$ is involved here. One can avoid recourse to Serre's result at the expense of weakening the conclusion of Fact 4.2 to: for arbitrarily large primes there is suitable $P_p(T)$ and σ such that $P_p(\sigma)$ annihilates the prime-to-p torsion of A. All that is involved here is lifting the characteristic polynomial of the Frobenius acting on the Tate module of the reduction of A mod p. In any case, using two primes as in [5], the methods of the present paper still yield an elementary proof of Manin-Mumford.

Theorem 4.3. *Let k be a number field, A a semiabelian variety defined over k, and X an irreducible subvariety of A, also over k. Assume that $T(A) \cap X$ is Zariski-dense in X, where $T(A)$ is the torsion subgroup of A. Then X is the translate of a semiabelian subvariety of A.*

Proof. After translating by an element of $T(A) \cap X$, we may assume that X contains 0. Let $\sigma \in \mathrm{Gal}(\bar{k}/k)$ and $P(T) = T^n + a_{n-1}T^{n-1} + ... + a_1T + a_0$ be as given by Fact 4.2. Let $A^n = A \times ... \times A$ (n times), also a semiabelian variety. Let ϕ be the

endomorphism of A^n defined as $\phi(x_0, ..., x_{n-1}) = (x_1, x_2, ..., x_{n-1}, -a_0x_0 - a_1x_1 - ... - a_{n-1}x_{n-1})$.

Claim. ϕ is an isogeny of A^n, and for each r, $\phi^r - \mathrm{id}$ is an isogeny of A^n.

Proof. Note that $P(\phi) = 0$. If ϕ were not an isogeny of A^n with itself, then there would be a positive-dimensional semiabelian subvariety B of A^n such that $\phi|B = 0$. Evaluating $P(\phi)$ at an element $x \in B$ of infinite order yields that $P(0) = 0$, a contradiction. So ϕ is an isogeny of A^n.

For each $r \geq 1$ there is an integral polynomial $P_r(T)$ without complex roots of unity among its zeroes such that $P_r(\phi^r) = 0$. It follows as above, using the assumptions on $P(T)$, that $\phi^r - \mathrm{id}$ is an isogeny of A^n with itself.

Let $\pi : A^n \to A$ be projection on the first coordinate. Let $\nabla : A(\bar{k}) \to A^n(\bar{k})$ be given by $\nabla(x) = (x, \sigma(x), ..., \sigma^{n-1}(x))$. Let Y be the Zariski-closure of $\nabla(X \cap T(A))$. As $P(\sigma)$ vanishes on $T(A)$ it follows that $\phi(\nabla(x)) = \nabla(\sigma(a)) \in \nabla(X \cap T(A))$ for $x \in X \cap T(A)$. Hence $\phi(Y) \subseteq Y$. Also X is the Zariski-closure of $\pi(Y)$. Let Y' be an irreducible component of Y such that X is the Zariski-closure of $\pi(Y')$. Then as ϕ "permutes" the components of Y, $\phi^m(Y') \subseteq Y'$ for some $m \geq 1$. Let X' be the translate of Y' by y^{-1} for some $y \in Y' \cap \nabla(X \cap T(A))$. Then X' contains the identity of A^n, is still ϕ^m-invariant, and some translate of X is the Zariski closure of $\pi(X')$.

Case 1. X' is a semiabelian subvariety of A^n.

Then, as $0 \in X$, $\pi(X') = X$ and X is a semiabelian subvariety of A, proving the theorem.

Case 2. Otherwise.

Let B be the semiabelian subvariety of A^n generated by X'. Then ϕ^m is an isogeny of B with itself. Let $S = \mathrm{Stab}_B(X')$. Then S is ϕ^m-invariant, and X'/S is a positive-dimensional irreducible subvariety of the semiabelian variety B/S with trivial stabilizer. Moreover ϕ^m induces an isogeny ϕ^m/S of B/S with itself; X'/S is ϕ^m/S-invariant and generates B/S. By Proposition 4.1(i), some positive power of ϕ^m/S is the identity on B/S. This contradicts the Claim above and so proves Theorem 4.3.

We complete this section with remarks on the positive characteristic analogue of Manin-Mumford. This is Theorem 4.4 below. It was proved in [12] (Theorem 3.6(b)). A proof was also given by Scanlon [13], using the "dichotomy theorem" for rank 1 types in existentially closed difference fields of positive characteristic from [3]. The Pink-Roessler proof has two ingredients. The first is a result stating that if A is a semiabelian variety and $\phi : A \to A$ an isogeny, then there are semiabelian varieties $A_1, ..., A_n$, and for each i an isogeny ϕ_i of A_i such that for each i, there is $s > 0$ and $r \geq 0$ such that ϕ^s is a composition of Fr^r with a separable isogeny, and such that (A, ϕ) is isogenous to $(\sum A_i, \sum \phi_i)$. The proof uses formal groups and Dieudonné modules. The second ingredient is Proposition 4.1 above for which we have given a somewhat elementary proof. The statement below follows relatively easily (as in the proof of Theorem 4.3 above) from these ingredients.

Theorem 4.4. *Let A be a semiabelian variety over an algebraically closed field K of characteristic $p > 0$, and X an irreducible subvariety of A such that $T(A) \cap X$ is Zariski-dense in X. Let B be the identity component of* $\mathrm{Stab}_A(X)$. *Then there is a semiabelian variety A' and an irreducible subvariety X' of A', both defined over a*

finite field, and a homomorphism $h : A' \to A/B$ with finite kernel, such that X/B is a translate of $h(X')$.

5. Additional remarks

In [7], the authors studied algebraic D-varieties and D-groups and proved a "Chevalley-type theorem": the image of a D-constructible subset of an algebraic D-group under a D-homomorphism is also D-constructible. Here D-constructible means Boolean combination of D-closed. This result is precisely "quantifier-elimination" for the many-sorted structure of algebraic D-groups with predicates for algebraic D-subvarieties of Cartesian powers.

Our original aim was to do something similar for the category of separable algebraic σ-groups equipped with predicates for dominant subvarieties. However, among the problems is that the intersection of two dominant subvarieties may no longer be dominant as the following example shows.

Let the algebraic σ-group be $(\mathbb{G}_m^2, \phi)$, where $\phi(x_1, x_2) = (x_1^2, x_2^2)$. We have two dominant subvarieties: X given by $x_1 = x_2^2$ and Y given by $x_1 = x_2^4$. $X \cap Y = \{(1,1), (1,-1)\}$, which is not dominant.

However, we can prove the following weak version of quantifier-elimination.

Theorem 5.1. *Suppose that G and G_0 are separable σ-groups and $f : G \to G_0$ is a σ-homomorphism. Let X be an irreducible dominant σ-subvariety of G. Then $f(X)$ is a Boolean combination of dominant σ-varieties.*

Proof. The proof proceeds as in the proof of the analogous Theorem 3.2 of [7]. The relevant lemmas were proved in Section 2. One should only note that the result holds for trivial σ-varieties because of Lemma 2.1 and the Chevalley's theorem (quantifier-elimination) for algebraically closed fields.

References

[1] D. Abramovich, Subvarieties of semiabelian varieties, Compositio Math, 90 (1994), 37-52. MR1266493 (95c:14054)

[2] Z. Chatzidakis and E. Hrushovski, The model theory of difference fields, Transactions AMS 351 (1999), 2997-3071. MR1652269 (2000f:03109)

[3] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, Model theory of difference fields II, Proceedings London Math. Soc. (3) 85 (2002), 257-311. MR1912052 (2004c:03047)

[4] E. Hrushovski, Mordell-Lang conjecture for function fields, Journal AMS 9 (1996), 667-690. MR1333294 (97h:11154)

[5] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, Annals of Pure and Applied Logic 112 (2001), 43-115. MR1854232 (2003d:03061)

[6] J. E. Humphreys, *Linear Algebraic Groups*, Springer, 1975. MR0396773 (53:633)

[7] P. Kowalski and A. Pillay, Quantifier-elimination for algebraic D-groups, Transactions AMS 358 (2006), 167-181. MR2171228

[8] J. Oesterlé, La conjecture de Manin-Mumford (d'apres Pink et Roessler), electronic letter to D. Roessler, 20 Dec. 2002. (See preprints at http://www.math.ethz.ch/ roessler/.)

[9] A. Pillay, Mordell-Lang conjecture for function fields in characteristic zero, revisited, Compositio Math. 140 (2004), 64-68. MR2004123 (2005b:14079)

[10] A. Pillay and M. Ziegler, Jet spaces of varieties over differential and difference fields, Selecta Math. New Ser. 9 (2003), 579-599. MR2031753 (2004m:12011)

[11] R. Pink and D. Roessler, On Hrushovski's proof of the Manin-Mumford conjecture, Proceedings ICM 2002, Vol. I, Higher Education Press, 2002. MR1989204 (2004f:14062)

[12] R. Pink and D. Roessler, On ψ-invariant subvarieties of semiabelian varieties and the Manin-Mumford conjecture, Journal of Algebraic Geometry 13 (2004), 771-798. MR2073195 (2005d:14061)

[13] T. Scanlon, Positive characteristic Manin-Mumford, Compositio Math. 141 (2005), 1351-1364. MR2185637

[14] J.-P. Serre, *Groupes algebriques et corps de classes*, Hermann, 1956. MR0103191 (21:1973)

[15] Andre Weil, On algebraic groups of transformations, American J. Math. 77 (1955). MR0074083 (17:533e)

Department of Mathematics, University of Wroclaw, pl Grunwaldzki 2/4, 50-384 Wroclaw, Poland – and – Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801-2975

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801-2975 – and – School of Mathematics, University of Leeds, Leeds, England LS2 9JT