A note on groups definable in difference fields.

Piotr Kowalski*
Dept. Mathematics
Univ. Wroclaw

A. Pillay†
Dept. Mathematics
University of Illinois at Urbana-Champaign

1 Introduction and preliminaries.

In this paper we record some observations around groups definable in difference fields. We were motivated by a question of Zoe Chatzidakis as to whether any group definable in a model of $ACFA$ is virtually definably embeddable in an algebraic group. We give a positive answer using routine methods. The only possibly "new" ingredient is the (stable) group configuration theorem in the $*$-definable category. The embeddability result for groups definable in $ACFA$ of finite SU-rank was already noted in [2], more or less by saying that the proof in [4] for groups definable in pseudofinite fields goes through.
We also take the opportunity to give an improved treatment of the analogous theorem for differentially closed fields (avoiding the category of $*$-definable groups).
Finally we adapt results from [5] and [1] about the unipotence of differential groups on affine spaces to the difference field context.
The results here have little to do with either automorphisms or derivations and could be presented in a suitable axiomatic framework.

*Supported by grant KBN 2 PO3A 020 18.
†Supported by NSF grant.

As usual we work in a saturated model $\bar{M}$ of a complete theory T. We work freely in $\bar{M}^{eq}$. We assume knowledge of stability theory, stable groups and the more general versions for simple theories. See [7], [9]. We will also use a result from [10]. We require also a few easy observations around stabilisers and generics which are not explicit in the literature, so we give them now.

Definition 1.1 *Assume T is simple, and G is a type-definable group over a model M.*
(i) Let H be a type-definable over M subgroup of G and X a right coset of H in G, also defined over M. Let $q(x)$ be a complete type over M of an element of X. We call $q(x)$ a generic type of X (over M) if for some realisation b of q and some element c of X independent from b over M, $tp(b.c^{-1}/M \cup \{c\})$ is a generic type of H. (Intuitively $q(x)$ is a translate of a generic type of H.) Analogously if X is a left coset of H in G.
(ii) Let $q(x), r(x)$ are complete types over M of elements if G. By $S(q,r)$ we mean the (type-definable over M) set consisting of those $a \in G$ such that for some realization b of q, independent with a over M, $a.b$ realises r and is independent with a over M.

Lemma 1.2 *(T simple and G type-definable over M.)*
(i) With the notation of (i) above, $q(x)$ is a generic type of X if and only if for any realization b of q and for any $a \in H$ independent of b over M, $a.b$ is independent from a over M.
(ii) With the notation of (i) above: let X be the right coset generated by $S(q,r)$. Then X is type-definable over M, X is a right coset of (left) $Stab(r)$ and $tp(a/M)$ is a generic type of X. Similarly, the left coset Y generated by $S(q,r)$ is type-definable over M, is a left coset of (left) $Stab(q)$ and $tp(a/M)$ is a generic type of Y.
(iii) Suppose a, b, c are elements of G pairwise independent over M such that $a.b = c$ and $tp(b/M) = tp(c/M) = q$. Let H = (left)$Stab(q)$. Then $H.b$ is type-definable over M and $tp(b/M)$ is a generic type of $H.b$.

Proof. (i) is routine.
(ii) Choose $d \in Stab(r)$, with d independent of a over M. Without loss of generality, d is independent of $\{a, b, c\}$ over M and moreover by the Independence Theorem we may assume that $d.c = c'$ realises r and is independent from d over M. So $d.a = c.b^{-1}$ is independent from d over M. By (i), $tp(a/M)$ is a generic of X.

(iii) Note that by (ii) $tp(a/M)$ is a generic type of H. Let $X = H.b$. Clearly also $X = H.c$. We first show that X is M-invariant, hence type-definable over M: Let c' realise q independently from c over M. By the Independence Theorem there is b' such that $tp(c, b'/M) = tp(c', b'/M) = tp(c, b/M)$. Hence $b' \in H.c \cap H.c'$, whereby $H.c = H.c'$ (as H is Minvariant). This is enough. Now by definition, q is a generic type of X.

2 Groups in stable theories and simple theories

By a $*$-tuple we mean simply a possibly infinite tuple $(a_i)_{i \in I}$ of elements of $\bar{M}^{eq}$ (where the index set I has cardinality less than that of $\bar{M}$). By a $*$-definable (over A) set we mean a collection of $*$-tuples (each tuple being indexed by some fixed I), which is the set of realizations of a partial type $\Sigma(x_i)_{i \in I}$ over a set A of parameters. By a $*$-definable (over A) group we mean a group G such that both G and the graph of multiplication are $*$-definable (over A) sets. We have similarly the notion of a $*$-definable homogeneous space (G, S). If the underlying set of G consists of finite tuples, we will say that G is finitary. A finitary $*$-definable group is what is usually called a type-definable group. If T is stable the theory of generic types etc., passes over to $*$-definable groups. Moreover Hrushovski proves in [3] that (for T stable) any $*$-definable group (homogeneous space) is $*$-definably isomorphic to a projective limit of finitary $*$-definable groups (homogeneous spaces). In the totally transcendental case, this becomes a projective limit of definable groups (homogeneous spaces). Our first general result is the group configuration theorem (as stated in Theorem 4.5 of [7]) generalized to $*$-definability. This must be well-known to anybody who has thought about it. There is only one delicate point that has to be take care of which we will point out below. As a matter of notation when we say, for example, that a $*$-tuple $c = (c_i)_{i \in I}$ is contained in $acl(A)$, we mean that each $c_i \in acl(A)$.

Proposition 2.1 *Let M be a saturated model of the stable theory T. Let a, b, c, x, y, z be $*$-tuples of length strictly less than the cardinality of M. Suppose that the following are true:*
(i) $acl(M, a, b) = acl(M, a, c) = acl(M, b, c)$,
(ii) $acl(M, a, x) = acl(M, a, y)$ and $Cb(stp(x, y/M, a))$ is interalgebraic with

a over M.
(iii) As in (ii) with b, z, y in place of a, x, y.
(iv) As in (ii) with c, z, x in place of a, x, y.
(v) Other than $\{a, b, c\}$, $\{a, x, y\}$, $\{b, z, y\}$ and $\{c, z, x\}$, any 3-element subset of $\{a, b, c, x, y, z\}$ is M-independent.
Then there is a $*$-definable (over M) homogeneous space (G, S) and generic (over M) elements a', b', c' of G and x', y', z' of S such that $a' \cdot x' = y'$, $b' \cdot y' = z'$, and $c' \cdot x' = z'$ (so $a' \cdot b' = c'$) such that each nonprimed element is interalgebraic over M with the corresponding primed element.

Proof. The proof goes exactly as in the proof of the Theorem referred to above in [7]. The only possibly problematic step is the first one:

Lemma 2.2 *There are $*$-tuples $a_1, b_1, c_1, x_1, y_1, z_1$ such that a_1 interalgebraic over M with a etc., and such that moreover $y_1 \in dcl(M, b_1, z_1)$ and $z_1 \in dcl(M, b_1, y_1)$.*

Proof of Lemma. b is first replaced by b_1 and y by y_1 in such a way that b is interalgebraic with b_1 over M, y is interalgebraic with y_1 over M, and moreover whenever $tp(z'/M, b_1, y_1) = tp(z/M, b_1, y_1)$ then z and z_1 are interalgebraic over M. In the finitary case, z is then replaced by the finite *set* z_1 of its M, b_1, y_1-conjugates, another imaginary element, interalgebraic with a over M and in $dcl(M, b_1, y_1)$. In the $*$-situation, the (in general infinite) set X of (M, b_1, y_1)-conjugates of z is not on the face of it another $*$-tuple. However, as pointed out in [6], X *can be* identified with a $*$-tuple: let $z = (z_i)_{i \in I}$ say. For each finite $J \subset I$, let z'_J be the (finite) set of M, b_1, y_1-conjugates of the J-tuple $(z_j)_{j \in J}$, a single imaginary. Let z_1 be the $*$-tuple $(z'_J)_J$. Then z_1 is interdefinable with X (an automorphism fixes the $*$-tuple z_1 iff it fixes setwise the set X of $*$-tuples). In particular z_1 is as required. The rest of the proof of the lemma proceeds in this way.

Proposition 2.3 *Let $\bar{M}$ be a saturated model of a simple theory T. Suppose that G, H are groups type-definable over a small model M and that there are elements a, b, c of G and a', b', c' of H such that*
(i) a, b are generic independent over M.
(ii) $a.b = c$ and $a'.b' = c'$,
(iii) a is interalgebraic with a' over M, and similarly for b, b' and c, c'.
Then there is a type-definable over M subgroup G_1 of bounded index in G

and a type-definable over M subgroup H_1 of H, and a type-definable over M isomorphism f between G_1/K_1 and H_1/L_1 where K_1 is a finite normal subgroup of G_1, and L_1 is a finite normal subgroup of H_1.

Proof. Let $p = tp(a, a'/M)$, $q = tp(b, b'/M)$ and $r = tp(c, c'/M)$. Then $(a, a') \in S(q, r)$. By Lemma 1.2 $S(q, r)$ generates a type-definable over M right coset X say of $Stab(r)$. The projection of $Stab(r)$ on G is G^0_M. By 1.2 (a, a') is a generic point of X over M. By definition, there is $(e, e') \in G \times H$, independent with (a, a') over M such that $(d, d') = (a, a')(c, c')^{-1}$ is a generic point of $Stab(r)$ over $M \cup \{e, e')\}$. As a and a' are interalgebraic over M it follows that d and d' are interalgebraic over M. Thus both $Ker(Stab(q))$ $= \{g \in G : (g, 1) \in Stab(q)\}$ and $Coker(Stab(q)) = \{h \in H : (1, h) \in Stab(q))\}$ are finite normal subgroups of G^0 and $\pi_2(Stab(q))$. This yields the proposition.

Remark 2.4 *Suppose in the above that T is supersimple and that G, H are definable. Then by [10] G_1 can be chosen to be a definable subgroup of G of finite index and f can be chosen to be definable.*

3 Groups in difference fields

We will prove:

Theorem 3.1 *Let $\bar{M} = (K, +, ., \sigma)$ be a model of $ACFA$. Let G be a group definable in $\bar{M}$. Then there is a group H definable in $(K, +, .)$ (i.e. an algebraic group) a definable subgroup G_1 of G of finite index, a definable finite normal subgroup N_1 of G_1 and a definable isomorphism of G/N_1 with H_1/N_2 where H_1 is a definable (in $\bar{M}$) subgroup of G and N_2 a finite normal subgroup of H_1.*

Proof. We assume that $\bar{M}$ is saturated and work over a model M over which G is defined. Let a, b, y be M-generic M-independent elements of G. Let $x = a.y$, $z = b^{-1}.y$ and $c = a.b$. Then $c.z = x$. Let $\bar{a}$ be the $*$-tuple $(\sigma^i(a) : i \in \mathbf{Z})$ and similarly for $\bar{b}$, $\bar{c}$, $\bar{x}$, $\bar{y}$ and $\bar{z}$. Then working in the field reduct $(K, +, .)$, $(\bar{a}, \bar{b}, \bar{c}, \bar{x}, \bar{y}, \bar{z})$ satisfy conditions (i) to (v) of Proposition 2.1. By that proposition there is in $(K, +, .)$ a $*$-definable group over M, say H with generic independent (over M) elements a^*, b^*, with $c^* = a^* \cdot b^*$ and such that, in $(K,+,.)$, a^* is interalgebraic with $\bar{a}$ over M, etc. By [3], H is an inverse limit of groups H_i ($i \in \omega$), each which is *definable* (in $(K,+,.)$), over M. Let π_i be the canonical surjective homomorphism from H to H_i. Let $a_i = \pi_i(a^*)$ and similarly for b_i, c_i. So in $(K,+,.)$, a^* is interdefinable with $(a_i : i \in \omega)$ over M, and likewise for b^* and c^*. In particular, in the structure $\bar{M}$, a is interalgebraic with $(a_i : i \in \omega)$, and similarly for b, c. As a, b, c are each finite tuples (and for $j < i$, $a_j \in dcl(M, a_i)$), there is some $i \in \omega$ such that a is interalgebraic with a_i, b with b_i and c with c_i (all over M). Now apply Proposition 2.3 and Remark 2.4.

Remark 3.2 *The proof of Theorem 3.1 can be modified to show that the group configuration theorem (Proposition 2.1) holds for the theory ACFA (namely for any completion of ACFA). We prove a special case (Lemma 3.3) below. It is still unkown whether the group configuration theorem holds in arbitrary simple theories.*

Lemma 3.3 *Work in a saturated model $\bar{M}$ of $ACFA$, and let M be a reasonably saturated submodel. Let a, b, c, x, y, z be finite tuples from $\bar{M}$ such that (i), (iv), (v) from 2.1 hold, as well as*
(ii)' $acl(M, a, x) = acl(M, a, y) = acl(M, x, y)$, and
(iii)' $acl(M, b, z) = acl(M, b, y) = acl(M, z, y)$.
Then there is an M-definable group G and M-generic M-independent elements a', b' of G, such that a is interalgebraic with a' over M, b is interalgebraic with b' over M and c is interalgebraic with $a'.b'$ over M.

Proof. The proof of Theorem 3.1 yields an M-definable group H, and elements a', b', c' of H such that $a'.b' = c'$, a is interalgebraic with a' over M, b is interalgebraic with b' over M and c is interalgebraic with c' over M. All we have do it is show that we can rechoose a', b' so as to be generic independent elements of some M-definable subgroup G of H. Let $p = tp(a'/M)$, $q = tp(b'/M)$ and $r = tp(c'/M)$. Then $a' \in St(q, r)$. By Lemma 1.2 (ii) p is a generic type of a left coset X of $Stab(q)$. Choose a_1 realizing p, independent from $\{a', b', c'\}$ over M such that $tp(a_1, c/M) = tp(a, c/M)$. Let $d = a_1^{-1}.a$, and $b_1 = a_1^{-1}.c'$. Then $d.b' = b_1$, b_1 realises q and $\{d, b', b_1\}$ is pairwise independent over M. By Lemma 1.2 (iii), q is a generic type of a right coset Y of $Stab(q)$. By [10], $Stab(q)$ is the intersection of M-definable subgroups G_i. Choose $G = G_i$ with $SU(G_i) = SU(G)$. Let X' be the unique left translate of G containing X, and Y' the unique right translate of G containing Y. Note that X', Y' are M-definable sets, p is a generic type of X' and q a generic type of Y'. Let $a'' \in M \cap X'$ and $b'' \in M \cap Y'$. Then $a_1 = (a'')^{-1}.a'$ and $b_1 = b'.(b'')^{-1}$ are M-generic elements of G, interdefinable with a', b' respectively over M. Moreover $c_1 = a_1.b_1$ is interdefinable with c' over M. So G and a_1, b_1 work.

Remark 3.4 *Hrushovski (unpublished) has classified the Zariski-dense definable subgroups of simple algebraic groups definable in models of $ACFA$. So with Theorem 3.1 this yields a classification of simple groups definable in models of $ACFA$.*

4 The differential case revisited

The following was proved in [8].

Theorem 4.1 *Let $M = (K, +, ., D)$ be a differentially closed field of characteristic 0. Let G be a connected group definable in M. Then there is a connected group H definable in $(K, +, .)$ and a definable (in M) embedding of G in H.*

The proof (on which the proof of Theorem 3.1 is modelled) involved embedding G in a group G^∞ which is $*$-definable in ACF, then appealing to the fact that G^∞ is an inverse limit of groups definable in ACF (algebraic groups) as well as to the DCC for differential algebraic groups, so as to embed G in an algebraic group. The use of the DCC was unnecessary. In fact the construction of G^∞ also turns out to be unnecessary, and we will here sketch a rather more direct proof of Theorem 4.1. (However the new proof involves the same machinery used to prove that a $*$-definable group is an inverse limit of type-definable groups, but applied only once.)

Sketch of proof of 4.1. We may assume M is saturated. Let k be a small model over which G is defined. Let $p(x) \in S(k)$ be the generic type of G. Let a realise $p(x)$ and let $p^*(x^*)$ be the complete type of $a^* = (a, D(a), D^2(a), ...)$ over k in the algebraically closed field $(K, +, .)$. As definable functions in DCF_0 are differential rational, for independent realizations a, b of $p(x)$, $(a.b)^*$ is contained in $k(a^*, b^*)$, and so is of the form $f(a^*, b^*)$ for some $*$-definable

function over k in ACF. Note that $(a.b)^*$ realises p^* and that $a^*, b^*, (a,b)^*$ are pairwise independent over k in ACF. Now suppose c, d are independent over k realizations of p^* (in ACF). So in ACF $tp(c,d/k) = tp(a^*, b^*/k)$ whereby $f(c,d)$ is defined and also realises p^*, independently from each of c, d. We write $f(c,d)$ as $c.d$, hopefully without ambiguity. Note that for independent c, d, e realising p^* (in ACF) we have $(c.d).e = c.(d.e)$ realises p^*. We write $c.d.e$ for this. We also write a realization c of p^* as $(c_0, c_1, ..)$ (corresponding to the enumeration $a^* = (a, D(a), ...))$.
We now work in ACF. Define the following equivalence relation E on realizations of p^*: $E(c,c')$ if for some (any) realisations d, e of p^* such that d and e are generic, independent over $k \cup \{c, c'\}$, $(d.c.e)_0 = (d.c'.e)_0$. By definability of types in ACF, E is $*$-definable over k.
Claim 1. For c, d k-independent realizations of p^*, each of c/E, d/E, $c.d/E$ depends only on the other two.
Proof. We show that if $E(c,c')$ where c' realizes p^* and is independent from d over k then $c.d/E = c'.d/E$. Choose e, f realizing p^* independent over everything, then e and $d.f$ are realizations of p^* independent of c, c' over k. Hence $(e.c.(d.f))_0 = (e.c'.(d.f))_0$. So $(e.(c.d).f)_0 = (e.(c'.d).f)_0$ and $c.d/E = c'.d/E$. This proves that $c.d/E$ depends on c/E and d/E. The rest of the claim follows similarly.

Claim 2. Let c, c' realize p^*, then $E(c,c')$ implies $c_0 = c'_0$.
Proof. Choose d, e generic independent over c, c' realizations of p^*. Clearly $c = d.b.e$ for some realization b of p^* independent with d, e over k, and likewise $c' = d.b'.e$ for suitable b' realising p^*. As $E(c,c')$, by Claim 1 we get $E(b.e, b'.e)$ and again by Claim 1, $b/E = b'/E$. As d, e are generic independent realizations of p^* over b, b' it follows that $c_0 = c'_0$ as required.

Claim 3. Let c realise p^*, then for some $n < \omega$, c/E depends only on $(c_0, .., c_n)$.
Proof. Let d, e be independent realizations of p^* over k, c. Then the finite tuple $(d.c.e)_0$ is in $k(d,c,e)$ so in $k(d_0, .., d_n, c_0, .., c_n, e_0, .., e_n)$ for some n. So clearly $c/E \in k(c_0, .., c_n)$.

By Claim 3 let c' be a finite tuple such that c' is interdefinable with c/E over k (in ACF). Let $p'(x) = tp(c'/k)$ in ACF. By Claim 1, the operation . on realisations of p^* induces an operation $f(-,-)$ on independent realisations of p'. f is definable over k in ACF and generically associative. By Weil's theorem (or the more general version due to Hrushovski [3]), p' is the generic type of a k-definable connected group (in ACF), H say, and f agrees with multiplication in H. The map taking a realization a of p to $(a^*)'$ (definable in DCF over k) is 1-1 by Claim 2, so extends to a definable (in DCF) embedding of G into H.

5 Difference algebraic groups on affine spaces

In this final section we briefly point out that results from [5] and [1] pass over to the difference context.
Let $(K, +, ., \sigma)$ be a model of $ACFA$ and let $K\{X_1, .., X_n\}$ be the difference ring of difference polynomials over K in difference indeterminates $X_1, .., X_n$.

Definition 5.1 *(i) By an affine difference variety we mean a subset X of K^n which is the zero set of a finite number of difference polynomials.*
(ii) By a morphism between affine difference varieties $X \subseteq K^n$ and $Y \subseteq K^m$ we mean a map $(f_1, .., f_m)$ from X to Y where each f_i is the restriction to X of a differential polynomial in $K\{X_1, .., X_n\}$.
(iii) By an affine difference algebraic group we mean a group G such that the underlying set of G is an affine difference variety and both multiplication and inversion are morphisms.

Remark 5.2 *It would be more appropriate to define a morphism to be something which is locally given by a difference rational function. However we will be interested here in the case where the underlying set of G is K^n and in this case the notions coincide.*

Theorem 5.3 *Suppose G is a difference algebraic group whose underlying set is K^n. Then G is embeddable, by a morphism of difference algebraic groups, in a linear unipotent algebraic group H over K.*

Proof sketch. For $a \in G$ (namely in K^n) let $a^* = (a, \sigma(a), \sigma^2(a), ...)$. Let X_i, Y_i denote n-tuples of indeterminates. Then as in [5] there are polynomial functions $f_i(X_0, X_1, ..., Y_0, Y_1, ..)$ and $g_i(X_0, X_1, ...)$ over K $(i < \omega)$ such that
(i) there is a group G^∞ on infinite dimensional affine space A^∞ over K, whose multiplication is defined by $(f_i)_i$ and inversion by $(g_i)_i$.
(ii) for $a, b \in K^n$, $(a.b, \sigma(a.b), ...) = (f_0(a^*, b^*), f_1(a^*, b^*), ...)$, and similarly

for inversion.
By Theorem 2 of [1], G^∞ is isomorphic, as a group scheme over K to an inverse limit $(G_i)_{i<\omega}$ of linear unipotent connected algebraic groups over K. Let μ_i be the canonical surjective homomorphism from G^∞ to G_i.
The map h taking a to a^* is an embedding of G into G^∞, quantifier-free definable in $(K,+,.,\sigma)$. Composing with the μ_i gives quantifier-free definable homomorphisms $h_i : G \to G_i$. The intersection of all the $Ker(h_i)$ is the identity of G. On the other hand, each $Ker(h_i)$ is quantifier-free definable in $(K,+,.\sigma)$, so by the DCC on quantifier-free definable subgroups, some h_i is an embedding, as required.

Remark 5.4 *(i) Clearly $(K,+,.,\sigma)$ can be an arbitrary difference field (not necessarily a model of $ACFA$) above.*
(ii) What can be said about groups definable in a model $(K,+,.,\sigma)$ whose underlying set is some K^n? (Namely the group operation is definable, but not necessarily by a difference polynomial function.)

References

[1] M. Chalupnik and P. Kowalski, Lazard's theorem for differential algebraic groups and pro-algebraic groups on affine spaces, preprint 1999.

[2] Z. Chatzidakis and E. Hrushovski, Model theory of difference fields, Transactions of AMS, 351 (1999), 2997-3071.

[3] E. Hrushovski, Unidimensional theories are superstable, Annals of Pure and Applied Logic, 50 (1990), 117-138.

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

[5] P. Kowalski and A. Pillay, Pro-algebraic and differential algebraic group structures on affine spaces, American Journal of Mathematics, 1222 (2000), 213-221.

[6] D. Lascar and A. Pillay, Hyperimaginaries and automorphism groups, to appear in Journal of Symbolic Logic.

[7] A. Pillay, *Geometric Stability Theory*, Oxford University Press, 1996.

[8] A. Pillay, Some foundational questions on differential algebraic groups, Pacific Journal of Math., 179 (1997), 179-20.

[9] A. Pillay, Definability and definable groups in simple theories, Journal of Symbolic Logic, 63 (1998), 788-796.

[10] F. O. Wagner, Groups in simple theories, preprint 1999.