SOME FOUNDATIONAL QUESTIONS CONCERNING DIFFERENTIAL ALGEBRAIC GROUPS

Anand Pillay

In this paper we solve some problems posed by Kolchin about differential algebraic groups. The main result (from which the others follow) is the embeddability of any differential algebraic group in an algebraic group. A crucial intermediate result, and one of independent interest, is a generalisation of Weil's theorem on recovering an algebraic group from birational data, to pro-algebraic groups.

1. Introduction.

Differential algebraic groups were introduced by Cassidy and Kolchin ([C1, 2] and [K2], and have been studied by them and several others, notably Buium (e.g. [B1]). In fact interest in the subject has been given a boost by Buium's recent work [B2] relating "finite- dimensional" differential algebraic groups to diophantine geometry. In any case, the preface to Kolchin's book [K2] ends with a few questions in the general theory which "suggest themselves with nagging persistence", specifically the question of embeddability into algebraic groups, the possibility of a "Chevalley-Barsotti" structure theorem, and some questions on fields of definition. We answer all the questions positively. Kolchin's set-up for "differential algebraic geometry" and the theory of differential algebraic groups, is, much like that in [K1], slightly unusual, although quite beautiful. A certain amount of what we do here is concerned with showing the equivalence between Kolchin's set-up and a more "natural" or "geometric" category of objects. This may give some of the work here a somewhat scholastic flavour. Actually we complicate matters by introducing a third category, the model theoretic one-namely the category of "groups definable in differentially closed fields", and we end up showing the equivalence of all three categories, even with respect to "differential fields of definition".

One will see quite quickly that from a differential algebraic group (in any of the senses) G defined over (the differential field) k, one obtains (and in fact generically embeds G in) a kind of *proalgebraic variety* V (also defined over k) equipped with a kind of generic group law. At this point one is in a purely algebraic-geometric context, and the main problem becomes to recover from

ANAND PILLAY

V, a proalgebraic group H (namely an inverse limit of algebraic groups H_{μ}), also defined over k. This we do. In fact our argument is motivated by (and could even be deduced from) a result of Hrushovski [**H**] about stable groups. Finally, a Noetherianity argument yields an embedding of G into some H_{μ} . In the remainder of this introduction we will recall the basic differential algebraic definitions, introduce the three versions of "differential algebraic group", and state formally Kolchin's questions.

We will be working with fields of characteristic 0 equipped with a single derivation δ . (However everything we say generalises to the case where we allow a fixed finite set Δ of commuting derivations.) We refer the reader also to [**B1**] and [**B4**] for a precise and concise background on differential algebra and "differential algebraic geometry", to [**Ho**] and [**P1**] for elementary model theory and stability theory, to [**M**] for more on the model theory of differential fields, and to [**Po**] for stable groups.

Let us first fix notation. By a differential field we will mean a field kof characteristic 0 equipped with an additive homomorphism $\delta : k \to k$ satisfying $\delta(x,y) = \delta(x) \cdot y + x \cdot \delta(y)$. Unless we say otherwise, by an embedding of such objects we mean a 1-1 map preserving both the field structure and the derivation. Similarly for isomorphism. If k < K are differential fields, and $A \subseteq K$ then $k\langle A \rangle$ denotes the differential subfield of K generated by $k \cup A$. Following Kolchin, it is convenient to work in a "universal" differential field. So **U** will denote a differential field of some cardinality $\kappa > \omega$, with the features (i) any differential field k of cardinality $< \kappa$ can be embedded in **U**, (ii) whenever k_1, k_2 are differential subfields of **U** of cardinality $< \kappa$, and $f: k_1 \cong k_2$, then f extends to an *automorphism* of **U**. For every $\kappa > \omega$ there is such **U**, which is moreover unique up to isomorphism. In model-theoretic language, **U** is simply a saturated differentially closed field of cardinality κ . Typically we will be interested in certain differential algebraic objects "defined over" a differential field k. The only requirement on κ will then be that $\kappa >$ cardinality of k.

From now on **U** will be fixed and k, k_1, \ldots , will denote differential subfields of **U** of cardinality $< \kappa$.

 $\mathbf{U}\{X_1,\ldots,X_n\}$ denotes the ring of differential polynomials over \mathbf{U} in differential indeterminates X_1, X_2, \ldots, X_n , namely ordinary polynomials over \mathbf{U} in indeterminates $\delta^j X_i$, $i = 1, \ldots, n, j < \omega$. Similarly for $k\{X_1, \ldots, X_n\}$. These are actually differential rings. Clearly if $f \in \mathbf{U}\{X_1, \ldots, X_n\}$, and $\mathbf{a} \in \mathbf{U}^n$, then f can be evaluated at \mathbf{a} . By an affine differential algebraic set, we mean a subset V of \mathbf{U}^n (for some n) which is the zero set of a (finite) set $f_1, \ldots, f_r \in \mathbf{U}\{X_1, \ldots, X_n\}$. We will say V is defined over k, if the f_i can be chosen in $k\{X_1, \ldots, X_n\}$. In any case we obtain a differential Zariski topology on \mathbf{U}^n by taking as closed sets the differential algebraic ones. We will say simply δ -closed for differential Zariski closed. This is a Noetherian topology. δ -k-closed will mean δ -closed and defined over k. We obtain the notion of δ -irreducible δ -closed sets, and also δ -k-irreducible δ -k-closed sets. By a δ -morphism from V to W (where V, W are δ -closed) we mean an everywhere defined map $f: V \to W$ such that V has a covering by finitely many open sets U_1, \ldots, U_s such that the restriction of f to each U_i is given by a tuple of differential rational maps (namely quotients of differential polynomials), everywhere defined on U_i . We also have natural notions of such a morphism being defined over k, (the U_i should be defined over k and restrictions of f to each U_i given by differential rational functions over k). We similarly obtain the notion of a δ - rational function between δ -closed sets. As in classical algebraic geometry, one can go on to define the notion of an (abstract) differential algebraic variety (or δ -algebraic variety) X, an object obtained by piecing together finitely many affine (or even quasi- affine) differential algebraic sets U_i , with differential rational transition maps f_{ij} . X comes then equipped with its own δ -Zariski topology. Such an object X say, is said to be defined over k, if the U_i and f_{ij} are all defined over k. So we are using here the analogue of the Weil definition of abstract algebraic varieties. By a δ -regular map from X to U we mean an everywhere defined map $f: X \to U$ such that when read in the charts U_i , f is locally differential rational. The referee has pointed out a difference with the algebraic-geometric category coming from the fact that there exists an affine differential algebraic variety V and a δ -regular map which is not given by a differential polynomial map. But this need not bother us. In any case one obtains the notions of δ -morphism and δ -rational map between abstract differential algebraic varieties. A differential algebraic group, or as we shall say a δ -algebraic group, is simply a δ -algebraic variety G with a group law given by a δ -morphism $G \times G \to G$. G is said to be defined over k, if both the underlying δ -algebraic variety, and the morphism giving the group law, are defined over k. We call such G δ -connected if G is irreducible, or equivalently if G has no δ -closed subgroups of finite index.

We now summarise Kolchin's notion of a δ -k-group. k is again a differential subfield of **U**, with $|k| < \kappa$.

Definition/Fact 1.1. (See pp. 29, 33 of [K2].)

(I) By a Kolchin δ -k-group we mean a group G, equipped with a preorder $x \to y$ (the specialisation relation), and for each $x \in G$, a differential field $k_x < \mathbf{U}$ finitely generated (as a differential field) over k, and for each pair $x, y \in G$ such that $x \leftrightarrow y$ (namely $x \to y$ and $y \to x$), a k-isomorphism $S(x, y) : k_x \to k_y$, such that certain axioms DAS 1 and 2, DAG 1, 2 and 3, are satisfied, where

DAS 1 says: There is a finite subset Φ of G such that for every $y \in G$, there

is $x \in \Phi$ such that $x \to y$.

DAS 2 says: (a) If $x \leftrightarrow y$ and $y \leftrightarrow z$ then S(x, z) is the composition of S(x, y) and S(y, z). (b) If $x \in G$ and f is a k-isomorphism of k_x with k' then there is a unique $y \in G$ such that $x \leftrightarrow y$, $k_y = k'$ and f = S(x, y).

DAG 1 says: For any $x, y \in G$, k_{xy} is contained in $k_x \langle k_y \rangle$, and also $k_{x^{-1}} = k_x$. DAG 2 says various things, but we wish to emphasise here: If $x, y, u, v \in G$, $x \leftrightarrow u, y \leftrightarrow v$ and there is an automorphism h of \mathbf{U} which extends both S(x, u) and S(y, v), then $xy \leftrightarrow uv$ and h extends S(xy, uv).

DAG 3 gives information about the "connected component" of G.

(II) By a δ -k-homomorphism between Kolchin δ -k-groups G and H, we mean an abstract group homomorphism $f : G \to H$ such that f preserves the specialisation relations \to , for all $x \in G$, k_x contains $k_{f(x)}$, and whenever $x, y \in G$ and $x \leftrightarrow y$ then S(x, y) extends S(f(x), f(y)). (In particular we have the notion of a δ -k-subgroup of G.)

(III) (More or less the content of DAG 3.) G is said to be *connected* if there is $x \in G$ such that k_x is a regular extension of k (in the field- theoretic sense) and for all $y \in G$, $x \to y$. Any such x is called a generic element of G over k.

Any Kolchin δ -k group has a smallest δ -k-closed subgroup of finite index, G^0 . Moreover G^0 is connected. (Here $X \subseteq G$ is called δ -k-closed if whenever $x \in X, y \in G$ and $x \to y$ then $y \in G$.)

Finally we present the model-theoretic category. Although the reader is advised to look at [Ho] we will begin with a few explanatory words, as well as give some comments on our treatment of algebraic geometry. By a language L we will mean a set of constant symbols, function symbols and relation symbols. The function symbols and relation symbols come with fixed "arities". A first order L-formula is something built up from these symbols together with a supply of variables x_i , and from the logical connectives $\&, \lor, \lor$ $\neg, \exists . \forall$, in the natural way. For example if R is a ternary relation symbol of L then $\forall x_1 \exists x_2(R(x_1, x_2, x_3))$ is such an L-formula. For such a formula φ we can speak of the *free*, (or unbound) variables in φ . (So in the above example the free variable is x_3 .) A formula without free variables is called an L-sentence. If **x** is the tuple of free variables in the formula φ , we may write $\varphi(\mathbf{x})$ for φ . We also let y_i, z_k etc. denote variables. By an L-structure M say, we mean a set X (the universe or underlying set of M), together with, for each constant symbol c of L, an element c^M of X, for each n-ary function symbol f of L, a function $f^M: X^n \to X$, and for each m-ary relation symbol R of L, a subset \mathbb{R}^M of X^m . Usually we notationally blur the distinction between X and M (so we also write M for the universe of M).

182

Now let $\varphi(\mathbf{x})$ be an L-formula with free variables $\mathbf{x} = (x_1, \ldots, x_n)$. Let $\mathbf{a} = (a_1, \ldots, a_n)$ be an *n*-tuple from M. It then makes sense to speak of " $\varphi(\mathbf{x})$ being true of \mathbf{a} in M", which we write as " $M \models \varphi(\mathbf{a})$ ". This notion is defined inductively in the obvious way. One of the base steps is: If R is a *n*-ary relation symbol, then $M \models R(a_1, \ldots, a_n)$ iff $(a_1, \ldots, a_n) \in R^M$. One of the inductive steps is: If $\varphi(\mathbf{x})$ is the formula $\exists y(\psi(\mathbf{x}, y))$, then $M \models \varphi(\mathbf{a})$ if for some $b \in M, M \models \psi(\mathbf{a}, b)$.

If τ is an L-sentence then we clearly have that $M \vDash \tau$ (τ is true in M or M is a model of τ) or $M \vDash \neg \tau$ (τ is false in M).

Th(M) (the theory of M) is the set of all L-sentences true in M. In general a complete theory is a set Σ of L-sentences such that Σ has a model, and for every L-sentence $\tau, \tau \in \Sigma$ or $\neg \tau \in \Sigma$. Any complete theory Σ is of the form Th(M) for some L-structure M. A structure M is said to have quantifierelimination if for any L- formula $\varphi(\mathbf{x})$ there is a quantifier-free L-formula $\psi(\mathbf{x})$ such that $M \vDash \forall \mathbf{x}(\varphi(\mathbf{x}) \leftrightarrow \psi(\mathbf{x}))$. Similarly for a (complete) theory to have quantifier-elimination.

Given an L-structure M it is convenient to add "names" or constants to the language L for elements of M, to obtain a language L(M). So a formula $\varphi(\mathbf{x})$ of L(M) may have additional "parameters" from M. If these parameters are from a subset A of M, we say φ is over A. When a model-theorist sudies a structure M he or she is studying the category of *definable sets* in M. So by a *definable set* in M, we mean a set $Y \subseteq M^n$ such that for some formula $\varphi(\mathbf{x})$ of L(M), $Y = \{\mathbf{a} \in M^n : M | = \varphi(\mathbf{a})\}$. Y is said to be A-definable (Asome subset of M) if φ can be chosen to be over A. By a *definable function* we mean a function (from some subset of M^n to some subset of M^m) whose graph is definable.

The structure M is said to be κ -saturated (κ some infinite cardinal) if whenever $n < \omega$, $A \subseteq M$ has cardinality $< \kappa$, and $\{X_i : i \in I\}$ is a family of A-definable subsets of M^n , every finite subset of which has nonempty intersection, then $\cap_i X_i \neq \emptyset$.

If **a** is a tuple from M and $A \subseteq M$, by $\operatorname{tp}(\mathbf{a}/A)$ (the type of **a** over A in M) we mean the set of formulas $\varphi(\mathbf{x})$ over A such that $M \models \varphi(\mathbf{a})$.

Let M be a substructure of N. We say that M is an *elementary* substructure of N (or N is an elementary extension of M) if whenever φ is an L(M)-sentence, then $M \vDash \tau$ iff $N \vDash \tau$. If $A \subseteq M$, and **a** is from M we say **a** \in acl(A) if there is some formula $\varphi(\mathbf{x})$ over A such that $M \vDash \varphi(\mathbf{a})$ and there are only finitely many points **b** from M such that $M \vDash \varphi(\mathbf{b})$. If $\varphi(\mathbf{x})$ can be chosen such that **a** is the *unique* solution of φ in M, then we say **a** \in dcl(A).

In this paper we shall be concerned exclusively with two languages: $L = \{+, -, ., 0, 1, \delta\}$ (the language for differential rings) and the sublanguage

 $L_0 = \{+, -, ., 0, 1\}$ (the language of rings). U as defined earlier is naturally an L-structure. The theory of U is precisely the theory of differentially closed fields of characteristic 0, often denoted DCF₀. U turns out to be a κ -saturated model of DCF₀. If we "forget" the distinguished derivation δ on U, we get an L₀- structure, U₀ say. The theory of U₀ (in L₀) is precisely the theory of algebraically closed fields of characteristic 0, ACF₀. Again U₀ is κ -saturated.

We will be using some model theory of algebraically closed fields, all of which is well-known to the model-theorist (but not necessarily to the algebraic geometer). The model-theoretic approach to algebraic geometry is essentially from the point of view of Weil's Foundations [W1]. As mentioned above ACF₀ is the theory of algebraically closed fields of characteristic 0. Let **K** be a κ -saturated model of ACF₀, which amounts to being simply an algebraically closed field of characteristic 0, of cardinality κ , which we consider as an L₀-structure, as well as a universal domain for algebraic geometry.

Fact 1.2. ACF_0 has quantifier-elimination as well as elimination of imaginaries.

Comment 1.3. Quantifier-elimination has been defined above, and amounts to saying that the definable subsets X of \mathbf{K}^n are precisely the constructible sets, namely finite Boolean combinations of Zariski closed sets. Moreover if $k < \mathbf{K}$ and X is k-definable, then the relevant Zariski closed sets can be chosen to be defined over k. Another consequence of quantifierelimination in ACF₀ is that if $A \subseteq \mathbf{K}$, then dcl (A) is precisely the subfield of **K** generated by A. Elimination of imaginaries is a rather more subtle notion, introduced by Poizat (which in the case of algebraically closed fields is intimately related to the existence of smallest fields of definitions for varieties). What it means is that if X is some k-definable subset of \mathbf{K}^n , and E some k-definable equivalence relation on X, then there is k-definable set $Y \subseteq \mathbf{K}^m$ (some m), and k-definable map f from X onto Y such that for $\mathbf{a}, \mathbf{b} \in X$, $E(\mathbf{a}, \mathbf{b})$ iff $f(\mathbf{a}) = f(\mathbf{b})$. A consequence of elimination of imaginaries is that any definable set has a smallest "field of definition", the Galois-theoretic interpretation of which is: If $X \subseteq \mathbf{K}^n$ is definable, then there is some tuple **c** from **K** such that for any automorphism σ of **K**, $\sigma(\mathbf{c}) = \mathbf{c}$ iff $\sigma(X) = X$.

Definition/Fact 1.4.

(i) Let V be an irreducible (affine, say) variety, defined over k, with $\dim(V) = n$. A point $a \in V$ will be called a *generic point* of V over k, if tr.deg(k(a)/k) = n (where k(a) is as usual the field generated by k and a). In the same situation we call $\operatorname{tp}(a/A)$ a generic type of V over k. If a_1, a_2 are both generic points of V over k, then there is a k-automorphism of **K** which takes a_1 to a_2 , or equivalently $\operatorname{tp}(a_1/k) = \operatorname{tp}(a_2/A)$, and thus V has

a unique generic type over k.

(ii) $\operatorname{tp}(a/k)$ is said to be *stationary* if whenever k < L, k(a) is algebraically disjoint from L over k, and $\operatorname{tp}(b/k) = \operatorname{tp}(a/k)$ and k(b) is algebraically disjoint from L over k, then $\operatorname{tp}(a/L) = \operatorname{tp}(b/L)$. Now for any tuple a and subfield k of \mathbf{K} , let V(a/k) be the variety over k generated by a (namely the variety defined by all polynomials over k vanishing at a). Then the stationarity of $\operatorname{tp}(a/k)$ is equivalent to the (absolute) irreducibility of V(a/k), which is also equivalent to k(a) being a regular extension of k.

(iii) (With the notation of (i).) Suppose moreover that $\varphi(x, y)$ is an L₀formula (possibly with parameters from k). Let $Y = \{b : \text{for some (any)}$ generic point of V over k(b), $\mathbf{K} \models \varphi(a, b)\} = \{b : \varphi(x, b) \text{ defines a Zariski$ $dense subset of V}. Then Y is a k-definable set (so k-constructible). This is$ $not difficult: for example if <math>\varphi(x, y)$ defines a Zariski closed set, then $b \in Y$ iff $\mathbf{K} \models \forall x (x \in V \rightarrow \varphi(x, b))$. Now simply generalise to constructible sets. In any case this fact amounts to "definability of the generic type of V" in the sense of model theory.

Definition/Fact 1.5. By a group definable in **K** we mean a group (G, .)such that both G and the graph of multiplication are definable sets in **K** (so $G \subseteq \mathbf{K}^m$, graph (.) $\subseteq \mathbf{K}^{3m}$ for some m). By an algebraic group we as usual mean an (abstract) variety G (not necessarily irreducible) equipped with a group operation which is a morphism from $G \times G$ to G. A basic result in the model theory of algebraically closed fields states that there is an equivalence of categories between the category of definable groups (with definable homomorphisms) and algebraic groups. This result rests on Weil's theorem which recovers a (unique) algebraic group from birational data. The equivalence of categories moreover respects "fields of definition". The reader may at first sight think this equivalence of categories to be erroneous, as it suggests that all algebraic groups are (quasi-) affine. However, one should note that if $G \subset \mathbf{K}^n$ is a definable group, then the underlying subset of G need not be a quasi-affine variety, and also multiplication (being a constructible map) need not even be continuous for the Zariski topology. An important component in passing from an algebraic group to a definable group is the use of elimination of imaginaries. For one can view an abstract variety X as a finite disjoint union of Zariski closed subsets of certain affine spaces, quotiented out by a certain definable equivalence relation (given by the transition maps), and thus one can identify definably X with a certain constructible subset of some \mathbf{K}^m .

We now return to our universal differential field \mathbf{U} which as remarked above is a κ -saturated model of DCF₀, the theory of differentially closed fields of characteristic 0. Rather than having to refer back continually to the

ANAND PILLAY

underlying algebraically closed field \mathbf{U}_0 , we will rather distinguish betwen sets (with parameters) definable in \mathbf{U} in the language $\mathbf{L} = \{+, -, ., 0, 1, \delta\}$ which we will call δ -definable sets, and those definable in the language $\mathbf{L}_0 = \{+, -, ., 0, 1\}$ which we will call *f*-definable sets (unless there is no room for ambiguity). So the notions: δ -k-definable; *f*-k-definable, should be clear.

Fact 1.6. DCF_0 has quantifier-elimination, as well as elimination of imaginaries.

So the δ -definable sets are precisely the finite Boolean combinations of δ -closed sets. It also follows from quantifier-elimination that for any $A \subseteq \mathbf{U}$, dcl(A) is precisely the differential subfield of \mathbf{U} generated by A.

We can now introduce the third category of "differential algebraic groups".

Definition/Fact 1.7. By a group definable in **U** over k, we simply mean a group G such that both the universe of G and the graph of its group operation are definable sets (in \mathbf{U}^n , \mathbf{U}^{3n} , respectively, for some n). We will call such groups δ -definable groups. Again G will be said to be δ -definable over k, or δ -k-definable if both G and the graph of the group operation are δ -definable over k. Now the theory DCF₀ is ω -stable. Formally this means that the set of types over any countable differential subfield k of \mathbf{U} is countable. All we will use of this is a certain consequence for groups G defined in a models of ω -stable theories, namely any such G satisfies the descending chain condition on definable subgroups. In particular G has a smallest definable subgroup of finite index, its connected component. So this applies to δ -definable groups.

Definition/Fact 1.8. An important ingredient in all categories is the notion of δ -independence. If k is a differential subfield of **U**, and a, b are tuples from **U** we say that a is δ -independent from b over k, if $k\langle a \rangle$ and $k\langle b \rangle$ are algebraically disjoint over k. If G is a Kolchin δ -k-group we will say that $a, b \in G$ are δ -independent over k, if k_a and k_b are algebraically disjoint over k, if k_a and k_b are algebraically disjoint over k, if k_a and k_b are algebraically disjoint over k. We call tp(a/k) stationary if whenever L > k is a differential subfield of **U**, and tp(b/k) = tp(c/k) = tp(a/k) and each of b, c are independent from L over k, then tp(b/L) = tp(c/L). Stationarity of tp(a/k) is equivalent to $k\langle a \rangle$ being a regular extension of k, and also to V(a/k), the differential algebraic variety defined by the differential polynomials over k which vanish at a, being δ -irreducible.

We now consider the interaction between the various categories, beginning with some obvious statements.

Remark 1.9. Any δ -algebraic group defined over k, can be *canonically* given the structures of both a δ -k-definable group and a Kolchin δ -k group.

Proof. Let G be a δ -algebraic group defined over k. Fix an affine open covering (or even quasi-affine open covering) U_1, \ldots, U_n of G. Let H be the

disjoint union of the U_i quotiented by the (k-definable) equivalence relation E given by the identifications f_{ij} . Then (by elimination of imaginaries) H is a δ -k-definable group and we have a canonical isomorphism $f: G \cong H$.

Now to give G the structure of a Kolchin δ -k group: For $a \in G$, note f(a) is a point in some affine space \mathbf{U}^m . Put $k_a = k \langle f(a) \rangle$. Put $a \to b$ if b is a differential specialisation over k of a. It is then clear that $a \leftrightarrow b$ iff there is a k-automorphism of **U** which takes f(a) to f(b). This induces a k-isomorphism of k_a with k_b and we call this S(a, b). Everything follows.

In **[P3]**, it is shown that a δ -definable group G can be δ -definably equipped with the structure of a δ -algebraic group. This does not give information on fields of definition except in the case where G is K-definable for *differentially closed* K, in which case the δ -algebraic group can be chosen to be defined over K too. The results of this paper, among other things, generalise this to arbitrary k.

The notion of *generic* element is fundamental in all categories. For Kolchin groups the notion appears in Def. 1.1 III. It should also be mentioned that Kolchin defines the notion of a "pre δ -k homomorphism" f between (say connected) Kolchin δ -k-groups G, H as follows: f is a map from a subset of G containing the k-generic points of G, to H, such that if a, b are δ -kindependent, k-generic elements of G then $f(a,b) = f(a) \cdot f(b)$. Also the other conditions in Def. 1.1 II hold where relevant. If V is a δ -irreducible δ -variety defined over k, then an element $a \in V$ is said to be *generic* (or we may say δ -generic) over k, if $a \notin X$ for every proper δ -k-closed subset X of V. If a, b are δ -generic elements of V over k then (identifying a, b with points in the same δ -k-open affine subset of V) there is a k-isomorphism of U taking a to b. Moreover $k\langle a \rangle$ is a regular extension of k. If G is a δ -k-definable group, then we call $a \in G$ generic over k, if for all $b \in G$, a.b is δ -independent from b over k. (Equivalently, using model-theoretic notions, the Morley rank of tp (a/k) = Morley rank of G.) Again, if G is connected, then for any generic points a, b of G over k there is a k-automorphism of **U** taking a to b. Moreover again $k\langle a \rangle$ is a regular extension of k, which corresponds exactly to tp (a/k) being stationary. If the δ -connected δ -algebraic group G (defined over k) is identified as in Remark 1.8 with a δ -k-definable group, then the two notions of "generic point of G over k" coincide. Similarly if Gis considered as a Kolchin δ -k group. Moreover we have:

Fact 1.9. If G is a group in any of the three categories, which is defined over k, then for any $g \in G$ there are $g_1, g_2 \in G$, each generic over k, such that $g = g_1.g_2$.

Fact 1.10. If G, H are (say connected) groups over k in any of the three categories, and if f_0 is a "generically defined" δ -map from G to H

ANAND PILLAY

satisfying: If a, b are δ -generic, δ -independent elements of G over k, then $f_0(a.b) = f_0(a).f_0(b)$. Then f_0 extends to a unique δ -k homomorphism f from G to H. Moreover if f_0 is 1-1 on k-generics of G, then f is 1-1. Here by "generically" defined δ -map, we mean the obvious thing in each of the categories.

In fact, at the "generic" level it is easy to see that the three notions of δ -k-group are *identical*.

Definition 1.11. By a *pre-\delta-k group* we mean an irreducible δ -variety V defined over k, and a δ -rational map $f: V \times V \to V$, defined over k, such that

(I) if a, b are δ -independent δ -generic points of V over k, and c = f(a, b)then $k\langle a, b \rangle = k\langle b, c \rangle = k\langle a, c \rangle$, and

(II) if a, b, c are δ -independent δ -generic points of V over k, then f(f(a, b), c) = f(a, f(b, c)).

Such a map f is said to be a normal law of composition.

Note that if V is a pre- δ -k group, and U is an open affine subset of V defined over k, then U is also a pre- δ -k group (in fact essentially the same one as V). Clearly a δ -connected, δ -algebraic group G, defined over k, is a pre- δ -k-group (where f is simply multiplication in G). Also if G is a connected δ -definable group defined over k, then G gives rise to a pre δ -k group as follows. Let $p(\mathbf{x})$ be the generic type of G over k (in the model-theoretic sense). p is stationary, which implies that p is the generic type of some affine δ -irreducible δ -k-algebraic set V. For **a**, **b** independent realisations of p, $\mathbf{a}.\mathbf{b} \in \operatorname{dcl}(k, \mathbf{a}, \mathbf{b}) = k \langle \mathbf{a}, \mathbf{b} \rangle$. So $\mathbf{a}.\mathbf{b} = f(\mathbf{a}, \mathbf{b})$ for some δ -k-rational function f. (V, f) is then easily seen to be a pre- δ -k group. Finally if G is a connected Kolchin δ -k group then G also gives rise to a pre- δ -k group: Fix a some generic point of G (over k). Fix some tuple $\alpha(a)$ such that $k_a = k \langle \alpha(a) \rangle$. Now k_a is a regular extension of k. So if we let V be the δ -k-locus of $\alpha(\alpha)$, then V is δ -irreducible. For any generic $b \in G$, define $\alpha(b)$ to be $S(a, b)\alpha(a)$. So $\alpha(b)$ is a k-generic point of V. On the other hand any k-generic point of V will be of the form $\alpha(c)$ for some generic c in G (by Axiom DAS 2 (b)). Choose a, b such that $\alpha(a)$, $\alpha(b)$ are δ -independent over k (namely k_a is algebraically disjoint from k_b over k). Let c = a.b. Then c is generic in G. Let $\alpha(c) = f(\alpha(a), \alpha(b))$ for some δ -k-rational function f. From the Kolchin axioms written above it is easy to conclude that (V, f) is a pre- δ -k group.

Kolchin asks in [K2] the following questions about Kolchin δ -k-groups G: (1) Is G embeddable (by a Kolchin δ -k₁-homomorphism for some $k_1 \supseteq k$) in an algebraic group?

(2) Is G covered by affine δ -k-open sets? (Here a δ -k-open set is affine if it is δ -k isomorphic to a δ -k-closed subset of \mathbf{U}^m , for some m. In fact Kolchin

states this with "quasi-affine" in place of affine.)

(3) Is there a structure theorem for G analogous to the Chevalley-Barsotti theorem for algebraic groups? (Recall the latter says that any connected algebraic group has a (unique) maximal connected normal linear group and the quotient group is an abelian variety.)

We will answer all these questions positively. In fact we prove (1) with $k_1 = k$, and the algebraic group defined over k. (2) and (3) follow, although some additional work is required to get the uniqueness part of (3). Of course the main problem in trying to prove (1) is to see how to transform the differential rational group law on G into some kind of rational group law.

I would like to thank Phyllis Cassidy for her comments and questions on an earlier draft of this paper. I would like also to thank Ehud Hrushovski for sharing with me his understanding and interpretation of Buium's work. Finally I would finally like to thank Zeljko Sokolovic for various discussions at the time this work was done.

2. Pro-algebraic varieties.

In this section we point out the rather obvious fact that if (V, f) is a δ -pregroup, then one obtains a canonical "pro algebraic variety" W defined over k, a k-rational "generic" group law h on W and a δ -k-rational generically surjective mapping φ of V to W such that for δ -generic and δ -independent points a, b of V over $k, \varphi(f(a.b)) = h(\varphi(a), \varphi(b))$. Possibly with some ambiguity, we will call a proalgebraic variety with a generically defined group law, a pre pro-group. This is a priori not the same as a projective limit of pre-groups, but in fact one of the main points (proved in 3) is that these notions do coincide.

There appears to be no *systematic* account of pro-algebraic varieties in the literature, although there has been some work on the subject ([Se], [Ko]). In any case we will give definitions suitable for our purposes. In Definition 2.1 K will be a universal domain for algebraic geometry, which we take to be an algebraically closed field (of characteristic 0 say) which has cardinality κ for some given $\kappa > \omega$. If V is a variety over K then we as usual identify V with its set of K-rational points.

Definition 2.1.

(i) Let **I** be a directed set of cardinality $< \kappa$. So we have a partial ordering \leq on **I**, and for all μ , $v \in \mathbf{I}$ there is $\lambda \in \mathbf{I}$ such that $\lambda \geq \mu$ and $\lambda \geq v$. Let, for each $\mu \in \mathbf{I}$, V_{μ} be a variety over **K**, and for $v \geq \mu$, $\pi_{v\mu}$ an everywhere defined generically surjective morphism from V_v to V_{μ} , with the usual compatibility requirements. By a *pro algebraic variety*, we mean the inverse limit V of such a directed system $(V_{\mu}, \pi_{v\mu})$.

(ii) We will call V irreducible if each V_{μ} is irreducible. We will say that V is *defined over* k ($k < \mathbf{K}$) if each V_{μ} and each $\pi_{v\mu}$ is defined over k. (Note that the cardinality conditions on I implies that there is $k < \mathbf{K}$ with $|k| < \kappa$ such that V is defined over k.)

(iii) By a point of V (in **K**) we mean simply an **I**-tuple ($\alpha_{\mu} : \mu \in \mathbf{I}$) such that for each μ in $\mathbf{I}, \alpha_{\mu} \in V_{\mu}$, and if $v \geq \mu$ then $\pi_{v\mu}(a_v) = a_{\mu}$. Assuming V to be defined over $k < \mathbf{K}$, such a point is said to be a generic point of V over k, if each a_{μ} is a generic point of V_{μ} over k. If **a**, **b** are points of V, we will say that **a** is independent from **b** over k, if $k(\mathbf{a})$ is algebraically disjoint from $k(\mathbf{b})$ over k. Note that assuming $|k| < \kappa$, then there will be generic points of V over k. In fact for any $\mu \in \mathbf{I}$ and generic point c of V_{μ} over k, there will be a generic point (a_v)_{$v \in \mathbf{I}$} of V such that $a_{\mu} = c$. (This is simply because $|\mathbf{K}| = \kappa$ and thus \mathbf{K} is " κ -saturated" in the model-theoretic sense.) Note also that because the $\pi_{v\mu}$ are not necessarily surjective, such a pro algebraic variety is in a sense only a "birationally defined" kind of object, and has no natural structure of a scheme. Assume now V to be irreducible and defined over k with $|k| < \kappa$.

(iv) By a rational function on V, defined over k, we mean simply a rational function on some V_v , defined over k (namely an element of $k(V_v)$). If f is such then f is defined at any point $\mathbf{a} = (a_{\mu})_{\mu \in \mathbf{I}}$ which is generic over k, by $f(\mathbf{a}) = f(a_v)$. Such a rational function will be often written as $f(X_{\mu} : \mu \in \mathbf{I})$ with the understanding that its value depends only on a_v , or equivalently on a finite number of a_{μ} 's.

(v) Suppose $W = \text{inv. limit}(W_{\lambda} : \lambda \in \mathbf{J})$ is another pro-algebraic variety defined over k. By a rational map from V to W defined over k, we mean a sequence $\mathbf{f} = (f_{\lambda} : \lambda \in \mathbf{J})$ of rational functions on V, each defined over k, such that for $\mathbf{a} \in V$ generic over k, $(f_{\lambda}(\mathbf{a}))_{\lambda \in \mathbf{J}} \in W$. We can view such \mathbf{f} as being defined on a "Zariski open" subset of V. Note that such a rational map is an inverse system of rational maps $f_{\lambda} : V_{\nu(\lambda)} \to W_{\lambda}$, where $\nu(\lambda)$ is an order preserving map on the index sets.

(vi) If $V = \text{inv.lim}(V_{\upsilon} : \upsilon \in \mathbf{I})$, $W = \text{inv.lim}(W_{\lambda} : \lambda \in \mathbf{J})$ are pro algebraic varieties defined over k, then $V \times W = \text{inv.lim}(V_{\mu} \times W_{\lambda} : (\mu, \lambda) \in \mathbf{I} \times \mathbf{J})$ is also a pro algebraic variety defined over k: We put $(\mu, \lambda) \ge (\mu', \lambda')$ iff $\mu \ge \mu'$ and $\lambda \ge \lambda'$, and $\pi_{(\mu', \lambda')(\mu, \lambda)} = \pi_{\mu'\mu} \times \pi_{\lambda'\lambda}$.

(vii) By a pre pro group, defined over k, we mean a pro-algebraic variety $V = \text{inv. } \lim (V_{\mu} : \mu \in \mathbf{I})$ defined over k, equipped with a rational function $\mathbf{f} : V \times V \to V$ with the features

a) if **a**, **b** are independent generic points of V over k, and $f(\mathbf{a}, \mathbf{b}) = \mathbf{c}$, then **a**, **c** are independent generic points of V over k, similarly for **b**, **c**, and also $k(\mathbf{a}, \mathbf{b}) = k(\mathbf{b}, \mathbf{c}) = k(\mathbf{a}, \mathbf{c})$,

b) if **a**, **b**, **c** are independent generic points of V over k then $f(f(\mathbf{a}, \mathbf{b}), \mathbf{c}) =$

 $f(\mathbf{a}, f(\mathbf{b}, \mathbf{c}))$. Again **f** is called a normal law of composition on V.

(viii) By a pro algebraic group G defined over k, we mean the inverse limit of a directed system $(G_{\mu}, \pi_{\nu\mu})_{\mu \in \mathbf{I}}$, where each G_{μ} is an algebraic group defined over k, and where $\pi_{\nu\mu} : G_{\nu} \to G_{\mu}$ is a surjective homomorphism, defined over k. Note that a proalgebraic group is now a global object, in particular a group (and also a scheme). Group multiplication is an everywhere defined rational map (defined over k), and trivially gives G also the structure of a pre pro group.

Remark. Any pro algebraic variety V defined over k is in birational correspondence with a pro affine algebraic variety defined over k. For if V =inv.lim $(V_{\lambda})_{\lambda}$, then let W_{λ} be an open affine subset of V_{λ} defined over k, and the identity map from inv.lim (W_{λ}) to V is the required correspondence.

We now return to the differential field context. The universal differentially closed field **U** is as mentioned in the introduction, also a universal domain for algebraic geometry, so Definition 2.1 makes sense with **U** in place of **K**. k will be a differential subfield of **U** with $|k| < \kappa$.

Definition 2.2. Let X be some δ -algebraic variety defined over k, and $V = \operatorname{inv.lim} (V_{\mu})_{\mu \in \mathbf{I}}$ a pro algebraic variety defined over k. By a δ -k-rational map from X into V one simply means a sequence $\mathbf{f} = (f_{\mu})_{\mu \in \mathbf{I}}$ where each f_{μ} is a δ -k-rational map from X into V_{μ} , and such that for $a \in X \delta$ -generic over k, and for $v \geq \mu$ in \mathbf{I} , $\pi_{v\mu}(f_v(a)) = f_{\mu}(a)$.

Lemma 2.3. Let X be a δ -irreducible pre δ -k group, with $f: X \times X \to X$ the normal law of composition. Then there is an irreducible pro affine pre pro group $V = \text{inv.} \lim(V_{\mu})_{\mu \in \mathbf{I}}$ (some I), defined over k, with normal law of composition $\mathbf{g}: V \times V \to V$, and there is a δ -k-rational map \mathbf{h} from X into V such that

- (i) if a, b are distinct δ -generic points of X over k, then $\mathbf{h}(a)$, $\mathbf{h}(b)$ are distinct generic points of V over k,
- (ii) if a, b are δ -generic δ -independent points of X over k, then $\mathbf{h}(f(a, b)) = \mathbf{g}(\mathbf{h}(a), \mathbf{h}(b)).$

Proof. This is simply a matter of seeing what the words mean. We may assume that X is affine. We first point out that if (i) holds then at least (ii) makes sense. If a, b are δ -generic δ -independent points of X over k, then $k\langle a \rangle$ is algebraically disjoint from $k\langle b \rangle$ over k. But $\mathbf{h}(a) \subseteq k\langle a \rangle$, and $\mathbf{h}(b) \subseteq k\langle b \rangle$, thus $\mathbf{h}(a)$ is independent from $\mathbf{h}(b)$ over k, so if (i) is true, $\mathbf{h}(a), \mathbf{h}(b)$ will be generic independent points of V over k, whereby $\mathbf{g}(\mathbf{h}(a), \mathbf{h}(b))$ is defined. Note that the δ -irreducibility of X means that if a is a δ -generic point of X over k, then $k\langle a \rangle$ is a regular extension of k. Let a be a δ -generic point of X over k. So $a \in \mathbf{U}^m$ some m, say $a = (e_1, \ldots, e_m)$. Then there is a countable sequence **a** such that $k\langle a \rangle = k(\mathbf{a})$. For example we could take **a** as a sequence whose elements are of the form $\delta^n(e_i)$ where $n < \omega$, and $1 \le i \le m$. Write $\mathbf{a} = (\mathbf{a}_i : i < \omega)$. Let **J** be the set of finite subsets of ω . Then **J** is a directed set, where we put $j \leq j'$ iff $j \subseteq j'$. For $j \in \mathbf{J}$, let $\mathbf{a}(j) = (\mathbf{a}_i : i \in j)$. Let V_j be the locus of $\mathbf{a}(j)$ over k. Then V_j is an affine variety defined over k which is irreducible (as by the remark above, $k(\mathbf{a}(j))$ is a regular extension of k), and $\mathbf{a}(j)$ is a generic point of V_j over k. For $j' \geq j$ in **J**, let $\pi_{j'j}$ be the restriction map: So $\pi_{j'j}(\mathbf{a}(j')) = \mathbf{a}(j)$. Let V be inv.lim $(V_j, \pi_{j'j})_{j \in \mathbf{J}}$. Now we can write $\mathbf{a}(j) = h_j(a)$, where h_j is a suitable δ -k-rational map from X into V_j . By construction $\mathbf{h} = (h_j)_{j \in \mathbf{J}}$ is then a δ -k-rational map of X into V satisfying (i) of the lemma. Now let b be a δ -generic point of X over $k\langle a \rangle$ (i.e. b is δ -generic over k, and δ -independent from a over k). So we can write $k\langle b \rangle$ as $k(\mathbf{b})$ where $\mathbf{b} = (\mathbf{b}_i : i < \omega)$ and $\mathbf{b}(j) = (\mathbf{b}_i : i \in j) = h_i(\mathbf{b})$ for $j \in \mathbf{J}$. Let c = f(a, b). By the pre- δ -k group hypothesis, $k\langle c \rangle \subseteq k\langle a \rangle \langle k\langle b \rangle \rangle$. But the latter is the same thing as $k(\mathbf{a})(\mathbf{b})$. Thus $k(\mathbf{c}) \subseteq k(\mathbf{b}, \mathbf{c})$. So for each $j \in \mathbf{J}$ we can find $j' \in \mathbf{J}$ such that $\mathbf{c}(j) \subseteq k(\mathbf{a}(j'), \mathbf{b}(j'))$, and we can thus write $\mathbf{c}(j)$ as $g_i(\mathbf{a}(j'), \mathbf{b}(j'))$ for some k-rational function $g_i(X_{j'}, Y_{j'})$. It is then clear that $\mathbf{g} = (g_j : j \in \mathbf{J})$ is a rational map from $V \times V$ to V, defined over k. By construction $\mathbf{g}(\mathbf{h}(a),\mathbf{h}(b)) = \mathbf{h}(f(a,b))$. Also clearly \mathbf{g} satisfies the conditions (in Definition 2.1 (vii)) for being a normal law of composition.

3. A Weil theorem for pro-algebraic groups.

Here we show how from a pre pro group (V, f) defined over k, we can recover an (essentially unique) pro algebraic group G defined over k. This result is simply a geometric adaptation of a result by Hrushovski on so-called *groups in stable theories [**H**]. This section takes place completely in the algebraic (and pro- algebraic) geometrical category. Namely we are working in a universal domain **K** as at the beginning of Section 2. k is again a subfield of **K** with $|k| < \kappa$.

Proposition 3.1. Let $V = \text{inv.} \lim(V_{\mu}, \pi_{\lambda\mu} : \mu \in I)$ be a pro affine irreducible pro algebraic variety defined over k, with a normal law of composition \mathbf{f} , defined over k. Then there is a connected proalgebraic group $G = \text{inv.} \lim(G_{\lambda} : \lambda \in \mathbf{J})$ defined over k, and a birational map $\mathbf{h} : V \to G$ defined over k, such that for generic, independent $\mathbf{a}, \mathbf{b} \in V$ over k, $\mathbf{h}(\mathbf{f}(\mathbf{a}, \mathbf{b})) = \mathbf{h}(\mathbf{a}).\mathbf{h}(\mathbf{b}).$

Proof. By assumption each V_{μ} is affine. We write $\mathbf{a} \in V$ as $(\mathbf{a}_{\lambda} : \lambda \in \mathbf{I})$, and we write $\mathbf{x} * \mathbf{y}$ in place of $\mathbf{f}(\mathbf{x}, \mathbf{y})$. For each $\lambda \in \mathbf{I}$, we define a relation E_{λ} on the set of generic points of V over k as follows: $E_{\lambda}(\mathbf{a}^1, \mathbf{a}^2)$ iff there exist

independent generic points \mathbf{b}, \mathbf{c} of V over $k(\mathbf{a}^1, \mathbf{a}^2)$ such that $(\mathbf{b} * \mathbf{a}^1 * \mathbf{c})_{\lambda} = (\mathbf{b} * \mathbf{a}^2 * \mathbf{c})_{\lambda}$. Note that

(*) this does not depend on the choice of **b**, **c**.

For if $\mathbf{b}_1, \mathbf{c}_1$ are also independent generic points of V over $k(\mathbf{a}^1, \mathbf{a}^2)$, then by irreducibility of V, there is a $k(\mathbf{a}^1, \mathbf{a}^2)$ -automorphism of \mathbf{K} taking (\mathbf{b}, \mathbf{c}) to $(\mathbf{b}_1, \mathbf{c}_1)$. In particular E_{λ} is an equivalence relation. Let us fix λ .

Claim I. For \mathbf{a}, \mathbf{b} independent generic points of V over k, the E_{λ} -class of $\mathbf{a} * \mathbf{b}$ depends only on the E_{λ} -classes of \mathbf{a} and \mathbf{b} , the E_{λ} -class of \mathbf{a} depends only on the E_{λ} -classes of \mathbf{b} and $\mathbf{a} * \mathbf{b}$, and the E_{λ} -class of \mathbf{b} depends only on the E_{λ} -classes of \mathbf{a} and $\mathbf{a} * \mathbf{b}$.

Proof. Suppose $E_{\lambda}(\mathbf{a}', \mathbf{a})$ and $E_{\lambda}(\mathbf{b}', \mathbf{b})$. Let \mathbf{c}, \mathbf{d} be generic independent points of V over $k(\mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}')$. Then (as * is a normal law of composition on V), we see that $\mathbf{c} * \mathbf{a}', \mathbf{d}$ are generic independent points of V over $k(\mathbf{b}, \mathbf{b}')$ whereby by (*)

(i) $((\mathbf{c} \ast \mathbf{a}') \ast \mathbf{b} \ast \mathbf{d})_{\lambda} = ((\mathbf{c} \ast \mathbf{a}') \ast \mathbf{b}' \ast \mathbf{d})_{\lambda}$. Similarly

(ii) $(\mathbf{c} * \mathbf{a}' * (\mathbf{b} * \mathbf{d}))_{\lambda} = (\mathbf{c} * \mathbf{a} * (\mathbf{b} * \mathbf{d}))_{\lambda}$. From (i) and (ii), and the generic associativity of * we conclude

(iii) $(\mathbf{c} * (\mathbf{a}' * \mathbf{b}') * \mathbf{d})_{\lambda} = (\mathbf{c} * (\mathbf{a} * \mathbf{b}) * \mathbf{d})_{\lambda}$, showing that $E_{\lambda}(\mathbf{a}' * \mathbf{b}', \mathbf{a} * \mathbf{b})$. The argument shows that $\mathbf{a} * \mathbf{b}/E_{\lambda}$ is a function only of \mathbf{a}/E_{λ} and \mathbf{b}/E_{λ} . The rest of the claim is proved in a similar fashion. For example to show that \mathbf{b}/E_{λ} depends only on \mathbf{a}/E_{λ} and $\mathbf{a} * \mathbf{b}/E_{\lambda}$, suppose that $E_{\lambda}(\mathbf{a}, \mathbf{a}')$, \mathbf{a}' is independent from \mathbf{b}' over k, and $E_{\lambda}(\mathbf{a} * \mathbf{b}, \mathbf{a}' * \mathbf{b}')$. Choose \mathbf{c}, \mathbf{d} as before. Then our assumptions imply that (ii) and (iii) above hold. But then we deduce (i) which shows that $E_{\lambda}(\mathbf{b}, \mathbf{b}')$.

Now it follows from the definition of a rational map that the map $g(x, y, z) = (x * y * z)_{\lambda}$ from $V \times V \times V$ to V_{λ} is given by a k-rational map, also called g, from $V_{\nu} \times V_{\nu} \times V_{\nu}$ to V_{λ} . We then clearly obtain:

Claim II. If $\mathbf{a}^1, \mathbf{a}^2$ are generic points of V over k, then $E_{\lambda}(\mathbf{a}^1, \mathbf{a}^2)$ if and only if for some (any) generic independent points b, c of V_v over $k(\mathbf{a}_v^1, \mathbf{a}_v^2)$, $g(b, \mathbf{a}_v^1, c) = g(b, \mathbf{a}_v^2, c)$.

Now, by 1.4 (iii) there is a k-constructible equivalence relation ε such that for any x, y in V_v , $\varepsilon(x, y)$ holds iff for generic independent points b, c of V_v over k(x, y), g(b, x, c) and g(b, y, c) are both defined and g(b, x, c) = g(b, y, c). Note that by Claim II, for generic points \mathbf{a}^1 , \mathbf{a}^2 of V, $E_\lambda(\mathbf{a}^1, \mathbf{a}^2)$ if and only if $\varepsilon(\mathbf{a}^1_v, \mathbf{a}^2_v)$. Let a be a generic point of V_v over k. Then the ε -equivalence class of a is a constructible set, so by Comment 1.3, there is a tuple σ (in some \mathbf{K}^m) such that any automorphism of \mathbf{K} fixes σ iff it fixes a/ε . This holds in particular of k-automorphisms of \mathbf{K} . Now any k(a)-automorphism of \mathbf{K} fixes a/ε and thus fixes σ . Thus (as we are in characteristic 0), $\sigma \in k(a)$, so $\sigma = h(a)$ for some k-rational function h. Note that if a_1 is another generic point of V_v over k, and $\sigma_1 = h(a_1)$ then again any k-automorphism of \mathbf{K} fixes σ_1 iff it fixes a_1/ε . Let W be the irreducible affine variety over k whose generic point over k is σ . So h yields a generically surjective rational map from V_v to W defined over k. h thus induces a generic point of V over k, $h(\mathbf{a}) = h(\mathbf{a}_v)$. Claim I can now be restated as:

Claim III . Let **a**, **b** be generic independent points of V over k. Then $h(\mathbf{a} * \mathbf{b}) \in k(h(\mathbf{a}), h(\mathbf{b})), h(\mathbf{a}) \in k(h(\mathbf{b}), h(\mathbf{a} * \mathbf{b}))$ and $h(\mathbf{b}) \in k(h(\mathbf{a}), h(\mathbf{a} * \mathbf{b}))$.

Proof. We again use an argument by automorphism. Let f be any $k(h(\mathbf{a}), h(\mathbf{b}))$ automorphism of \mathbf{K} . Then by the above remarks f fixes the ε -classes of \mathbf{a}_v and \mathbf{b}_v and thus fixes the E_{λ} -classes of \mathbf{a} and \mathbf{b} . By Claim I, f fixes the E_{λ} class of $\mathbf{a} * \mathbf{b}$. By above remarks, f fixes the ε -class of $(\mathbf{a} * \mathbf{b})_v$, and thus f fixes $h(\mathbf{a} * \mathbf{b})$. This shows that $h(\mathbf{a} * \mathbf{b})$ is rational over $k(h(\mathbf{a}), h(\mathbf{b}))$. The rest is similar.

Claim III enables us to endow W with a normal law of composition w defined over k, by: For independent generic points σ , τ of W over k, $w(\sigma, \tau) = \rho$ if there are independent generic points \mathbf{a} , \mathbf{b} of V over k, such that $h(\mathbf{a}) = \sigma$, $h(\mathbf{b}) = \tau$ and $h(\mathbf{a} * \mathbf{b}) = \rho$. (It is easily verified that this is a normal law of composition, and hence W becomes a pre group in the sense of Weil.) Now by Weil's theorem [W2], there is a connected algebraic group G defined over k, and a birational isomorphism ϕ of W with G, defined over k, such that for generic independent points σ , τ of W over k, $\phi(w(\sigma, \tau)) = \phi(\sigma).\phi(\tau)$.

Let us rename G as G_{λ} to reflect its dependence on λ . Composing ϕ with h, gives a a rational generically surjective map h_{λ} from V to G_{λ} , defined over k, such that for \mathbf{a} , \mathbf{b} generic independent points of V over k, $h_{\lambda}(\mathbf{a} * \mathbf{b}) = h_{\lambda}(\mathbf{a}).h_{\lambda}(\mathbf{b})$. It is clear from the construction that if $\mu \geq \lambda$ then $h_{\mu} = h_{\lambda}.\pi_{\mu\lambda}$, and thus induces a generically surjective rational map $g_{\mu\lambda}$ from G_{μ} to G_{λ} , defined over k, which preserves generic multiplication. A basic theorem from algebraic groups says that $g_{\mu\lambda}$ is (or extends to) a surjective k-rational homomorphism from G_{μ} to G_{λ} . Let G be the pro-algebraic group inv.lim $(G_{\lambda}, g_{\mu\lambda})_{\lambda \in \mathbf{I}}$. Now clearly if $\mathbf{a} \neq \mathbf{b}$ are generic points of V over k, then for some λ , $h_{\lambda}(\mathbf{a}) \neq h_{\lambda}(\mathbf{b})$. Thus $\mathbf{h} = (h_{\lambda})_{\lambda \in \mathbf{I}}$ yields a birational isomorphism of V over k, such that for \mathbf{a} , \mathbf{b} generic independent points of V over k, then for some λ , $h_{\lambda}(\mathbf{a} * \mathbf{b}) = \mathbf{h}(\mathbf{a}).\mathbf{h}(\mathbf{b})$. The proof is complete.

4. Conclusions for differential algebraic groups.

Finally we return to the category of differential algebraic groups. The result from which everything follows is the following version of Weil's theorem for pre- δ -k groups. Again **U** is a universal domain for differential algebraic geometry, and k is a differential subfield of **U** of cardinality $< \kappa$.

Proposition 4.1. Let X be a δ -irreducible pre- δ -k group with normal law of composition *. Then there is a connected algebraic group H defined over k, a δ -connected δ -algebraic subgroup H_1 of H defined over k, and a δ -birational isomorphism h of X with H_1 also defined over k, such that for δ -independent δ -generic a, $b \in X$ over k, h(a * b) = h(a).h(b).

Proof. It is convenient to make use of the model-theoretic category. By [H] (together with ω -stability) there is a connected δ -definable group A, defined over k, such that the generic points of A over k are precisely the δ -generic points of X over k, and that * agrees with multiplication in A on such points which are δ -independent over k. Combining Lemma 2.3 and Proposition 3.1 we obtain a proalgebraic group $G = \text{inv.} \lim(G_{\lambda}, g_{\mu\lambda} : \lambda \in \mathbf{I})$ defined over k, and a δ -rational map (not everywhere defined) $\mathbf{h} = (h_{\lambda})_{\lambda \in \mathbf{J}}$ of X into G, such that for each $\lambda \in \mathbf{J}$, and for δ -generic δ -independent points a, b of X over k, $h_{\lambda}(a * b) = h_{\lambda}(a) \cdot h_{\lambda}(b)$ (where the latter multiplication is in G_{λ}), and for any $a \neq b$ generic points of X over k, for some λ , $h_{\lambda}(a) \neq h_{\lambda}(b)$. By Fact 1.4 (for the δ -definable category) each h_{λ} extends to a δ -definable homomorphism of A into G_{λ} , definable over k, which we call h'_{λ} . The h'_{λ} commute naturally with the $g_{\mu\lambda}$'s. Let $N_{\lambda} = \ker(h'_{\lambda})$. Then N_{λ} is a definable subgroup of A, and note that if $\mu \geq \lambda$ then $N_{\mu} \leq N_{\lambda}$. By Fact 1.7 (the DCC for δ -definable groups), there is a *finite* subset Λ of **I** such that $\cap \{N_{\lambda} : \lambda \in \mathbf{I}\} = \cap \{N_{\lambda} : \lambda \in \Lambda\}$. So choosing $v \in \mathbf{I}$ such that $v \geq \lambda$ for all $\lambda \in \Lambda$, we see that

$$(*) \qquad \qquad \cap \{N_{\lambda} : \lambda \in \mathbf{I}\} = N_{v}.$$

Claim. $N_v = \{1\}.$

If not, let $c \in N_v$, with $c \neq 1$. Let $a \in A$ be generic over $k\langle c \rangle$, and let b = c.a. Then a, b are distinct generic points of X over k. But then for some $\lambda \in \mathbf{I}$ which we may suppose is $\geq v$, we have $h_{\lambda}(a) \neq h_{\lambda}(b)$. Then clearly $c \notin \operatorname{Ker}(h'_{\lambda}) = N_{\lambda}$, contradicting (*). This proves the claim.

By the Claim, h_v is an *embedding* of A in G_v . Put $H = G_v$, and B = the image of A under h_v . Then B is a connected δ -definable subgroup of H, defined over k. It is a routine fact that B has to be *closed* in the δ -Zariski topology on H. Now H, as an algebraic group defined over k, has a covering by finitely many affine open sets defined over k. The intersection of each of

these with B is an affine open subset of B in the δ -Zariski topology, which is moreover defined over k. Thus B has the structure of a δ -algebraic group, defined over k, and h_v is the required δ -birational isomorphism of X with B.

Corollary 4.2.

- (i) The three categories of δ-connected δ-algebraic groups defined over k, connected Kolchin δ-k groups, and connected δ-definable groups defined over k, are equivalent.
- (ii) Any group in one of the above categories embeds by a homomorphism (in the suitable category) defined over k in a connected algebraic group defined over k.

Proof. Let G be a group in any of the three categories. By 4.1, the corresponding pre- δ -k group is in δ -birational correspondence with a δ -connected δ -algebraic subgroup B (defined over k) of a connected algebraic group H defined over k. By 1.4 this birational correspondence extends to an isomorphism defined over k (in the relevant category) of G with B. This proves (i) and (ii).

Remark 4.3. Corollary 4.2 solves (1) and (2) of Kolchin's problems. First, by (ii) any Kolchin δ -k group embeds in an algebraic group. Second, by (i), if G is a connected Kolchin δ -k group, then G is isomorphic by a Kolchin δ -k isomorphism to a δ -connected δ -algebraic group defined over k. In particular this equips G with a covering by δ -k affine δ -k-open subsets of G.

Finally we aim towards a Chevalley-Barsotti theorem for δ -algebraic groups, answering the third of Kolchin's "nagging" questions. The issue of existence and uniqueness of a maximal δ -connected normal subgroup is somewhat subtle and requires additional information. In particular we will need to point out the connection with Buium's "prolongations" of algebraic groups. Remark 4.4. (i) Suppose H is a δ -connected δ -algebraic group defined over k. As in the proof of 4.2, we obtain from 2.3 and 3.1 a canonical proalgebraic group $G = \text{inv.} \lim(G_{\lambda}, \pi_{\mu\lambda} : \lambda \in \mathbf{I})$ and a family of δ -homomorphisms $h_{\lambda}: H \to G_{\lambda}$ commuting with the $\pi_{\mu\lambda}$. So we have a canonical embedding $\mathbf{h}: H \to G$. We call this data the canonical proalgebraic group associated to H. It should be clear that G is essentially *unique*. The specific nature of such proalgebraic groups G will be studied in a future paper. (They should be "proalgebraic D- groups", to borrow language of Buium [B1], and moreover the category of proalgebraic D-groups which satisfy a certain finiteness condition should be equivalent to the category of differential algebraic groups.) For now we only wish to point out that the association of G (and the as-

196

sociated maps) to H is functorial, in the sense that if $f: H_1 \to H_2$ is a δ -homomorphism defined over k, then there is a homomorphism $g: G_1 \to G_2$ of proalgebraic groups (defined over k) such that all relevant maps commute. This is not difficult: Let c_1 be a δ -generic point of H_1 over k. Then $f(c_1) \in k\langle c_1 \rangle$. Let $k(\mathbf{c}) = k\langle c \rangle$, and $k(\mathbf{d}) = k\langle f(c) \rangle$. Then $\mathbf{d} \subseteq k(\mathbf{c})$, \mathbf{c} is a generic point of G_1 over k, and \mathbf{d} can be considered as a point of G_2 . The "k-rational" map taking \mathbf{c} to \mathbf{d} can be extended to a homomorphism $G_1 \to G_2$ of prolagebraic groups, defined over k. We will call this functor F.

(ii) Suppose now that H is a connected *algebraic* group defined over k. In particular H is a δ -connected δ -algebraic group defined over k. (δ -connectedness is due to Kolchin.) Then the proalgebraic group G associated to H is identical to the inverse limit of Buium's prolongations: $\dots \to H_n \to H_{n-1} \to$ $\dots \to H_1 \to H$, from [**B3**] or [**B4**]. This is not difficult to see and depends on the fact that if a is a δ -generic point of H over k, then $(a, \delta(a), \dots, \delta^n(a))$ is a generic point of H_n over k.

Lemma 4.5. Let H_1 be a δ -connected δ -algebraic group defined over k. Suppose $f : H_1 \to H_2$ to be a δ -homomorphism from H_1 into a connected algebraic group H_2 , where both f and H_2 are defined over k. Suppose moreover $f(H_1)$ to be Zariski-dense in H_2 . Let G_1 be the canonical proalgebraic group associated to H_1 and $\mathbf{h} : H_1 \to G_1$ the canonical embedding. Then

- (i) there is a surjective homomorphism $\pi : G_1 \to H_2$ (of proalgebraic groups), defined over k, such that $f = \pi \cdot \mathbf{h}$.
- (ii) Suppose moreover that f is an embedding. Then Ker(π) is commutative and prounipotent.

Proof. We will be brief.

(i) Let c be a δ -generic point of H_1 over k. Then $f(c) \in k\langle c \rangle$, and f(c) is a k-generic point of H_2 (by Zariski-denseness of $f(H_1)$ in H_2). Let \mathbf{c} be a possibly infinite tuple such that $k(\mathbf{c}) = k\langle c \rangle$. Then \mathbf{c} is a generic point of G_1 over k. All that has to be checked is that the (k-rational) map π taking \mathbf{c} to f(c) extends to a surjective homomorphism $\pi : G_1 \to H_2$ of proalgebraic groups, which satisfies the requirements. This is left to the reader.

(ii) Let $G_2 = f(H_2)$. There is a canonical surjective homomorphism of proalgebraic groups $g: G_2 \to H_2$ (such that $g.\mathbf{h}_2 = \mathrm{id}$ on H_2). By [**B3**], Ker (g)is commutative and prounipotent. By functoriality F(f) is an embedding of proalgebraic groups $G_1 \to G_2$. Let π be as in (i). We leave the reader to check that $g.F(f) = \pi$. Thus ker (π) is commutative and prounipotent. \Box

Definition 4.6. Let G be a δ -algebraic group. We call G linear if there is a δ -embedding of G in some $GL_n(\mathbf{U})$. We call G of Abelian-type if there is a δ -embedding of G in some abelian variety A.

Lemma 4.7. Let H be a linear δ -connected δ -algebraic group. Suppose that f_1 is a δ -homomorphism from H into a connected algebraic group H_1 , and $f_1(H)$ is Zariski-dense in H_1 . Then H_1 is also linear.

Proof. By definition of H being linear, there is a δ -embedding f_2 of H in a linear algebraic group H_2 , and we may assume $f_2(H)$ is Zariski-dense in H_2 , and thus H_2 is connected. Let k be a differential field such that all the above data are defined over k. Let G be the canonical proalgebraic group associate to H. By Lemma 4.5 we have surjective homomorphisms $\pi_1 : G \to H_1$ and $\pi_2 : G \to H_2$ of proalgebraic groups, where moreover ker (π_2) is commutative and prounipotent. Thus (as H_2 is linear), G is prolinear. Thus H_1 is linear.

Corollary 4.8. Let G be a δ -connected δ -algebraic group, defined over k. Then G has a unique maximal linear δ -connected δ -closed subgroup N. N is normal, defined over k, and the quotient G/N is of Abelian-type.

Proof. By 4.2 we may assume G to be a subgroup of a connected algebraic group H defined over k, and we may also assume G to be Zariski-dense in H. By the Chevalley-Barsotti Theorem, H has a (unique) maximal connected linear algebraic subgroup H_1 defined over k, H_1 is normal in H and H/H_1 is an abelian variety B say. Then $G \cap H_1$ is δ -closed in G and defined over k. Let N be the δ -connected component of $G \cap H_1$. N is normal in G, δ -connected δ -algebraic, defined over k, and linear. We must show

(i) G/N is of Abelian type, and

(ii) N contains every other normal linear δ -connected δ -algebraic subgroup of G.

First, let G_1 be $G/G \cap H_1$. Then G_1 embeds canonically in $B = H/H_1$, as a δ -connected δ -closed subgroup, and in particular is commutative. On the other hand N has finite index in $G \cap H_1$, whereby we have a canonical surjective homomorphism $\pi: G/N \to G_1$ with finite kernel $G \cap H_1/N$. As G/N is δ -connected, it easily follows that G/N is also commutative. Clearly G_1 is divisible with only finitely many elements of any given order. The same is then true of G/N. Thus we can form the "dual isogeny" $\pi^*: G_1 \to G/N$ defined by $\pi^*(c) = \Sigma \pi^{-1}(c)$, which will be a surjective δ -homomorphism with finite kernel K. We thus obtain a δ -isomorphism $\pi^{**}: G/N \to G_1/K$, inducing a δ -embedding of G/N in B/K. But the latter is also an abelian variety. This yields (i). Suppose N_1 is some other δ -connected δ -closed linear subgroup of G. Let H_2 be the Zariski-closure of N_1 in H. Then H_2 is connected, and by Lemma 4.7, linear. By the properties of H_1, H_2 is contained in H_1 , and thus N_1 is contained in $H_1 \cap G = N$. This yields (ii). The proof is complete. Note that Lemma 4.7 shows that the class of linear δ -connected δ -algebraic groups is closed under homomorphic images. Methods like those above show that this class is also closed under extensions. The class of δ -connected δ -algebraic groups of Abelian-type is closed under extensions, but *not* under homomorphic images.

References

- [B1] A. Buium, Differential algebraic groups of finite dimension, Springer Lecture Notes in Math., 1506 (1992).
- [B2] _____, Intersections in jet spaces and a conjecture of S. Lang, Annals of Math., 139 (1992), 557-567.
- [B3] _____, Geometry of differential polynomial functions I: Algebraic groups, American J. of Math., 1994.
- [B4] _____, Differential algebra and diophantine geometry, Hermann, Paris, 1994.
- [C1] Ph.J. Cassidy, Differential algebraic groups, American J. of Math., 94 (1971), 247-273.
- [C2] _____, The classification of semisimple differential algebraic groups, J. of Algebra, 121 (1989), 169-238.
- [Ho] W.A. Hodges, Model Theory, Encyclopedia of Mathematics and its applications, 42, Cambridge University Press, Cambridge, 1993.
- [H] E. Hrushovski, Unidimensional theories are superstable, Annals of Pure and Applied Logic, 50 (1990), 117-138.
- [K1] E. Kolchin, Differential algebra and algebraic groups, Academic Press, New York, 1973.
- [K2] _____, Differential algebraic groups, Academic Press, New York, 1985.
- [Ko] J. Kovacic, Pro-algebraic groups and the Galois theory of differential fields, American J. of Math., XCV (1973), 507-536.
- [M] D. Marker, Model theory of differential fields, in "Model Theory of Fields", (by D. Marker, M. Messmer and A. Pillay), Lecture Notes in Logic, 5, Springer-Verlag, 1996.
- [P1] A. Pillay, Model theory, stability and stable groups, in "The Model Theory of Groups", edited by A. Nesin and A. Pillay, Notre Dame Press, 1989.
- [P2] _____, Differential algebraic groups and the number of countable differentially closed fields, Model theory of Fields, Lecture Notes in Logic, 5, Springer-Verlag, 1996.
- [P3] _____, Differential algebraic group chunks, J. of Symbolic Logic, 55 (1990), 1138-1142.
- [Po] B. Poizat, Groupes Stables, Nur al-mantiq walma'rifah, Villeurbanne, 1987.
- [Se] J.P. Serre, *Groupes pro-algebriques*, I.H.E.S. Publications Math., 7 (1960).
- [W1] A. Weil, Foundations of Algebraic Geometry, Am. Math. Soc. Colloq. Publication, New York, 1946.

ANAND PILLAY

[W2] _____, On algebraic groups of transformations, American J. of Math., 77 (1955), 355-391.

Received July 28, 1993 and revised September 11, 1996. This author was partially supported by NSF grants DMS 9203399 and 9504788.

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, 1409 W. GREEN ST URBANA, IL 61801 *E-mail address*: pillay@math.uiuc.edu

200