Differential algebraic groups and the number of countable differentially closed fields

Anand Pillay
University of Notre Dame

Introduction.

We give an exposition of several results on definable groups in differentially closed fields, and applications thereof. Among other things we give a proof of the result [HS] that there are continuum many countable differentially closed fields of characteristic 0. The theory DCF_0 (of differentially closed fields of characteristic 0) is complete and ω-stable and thus by [SHM] has either $\leq \aleph_0$ or $2^{\aleph_0}$ countable models. But until recently it was not known which. Rather surprisingly it turns out that classical mathematical objects, specifically elliptic curves, lie behind the existence of continuum many countable models (or at least behind the present proof). One of the essential points is to find some strongly regular nonisolated type which is orthogonal to the empty set. The required type p is found inside a suitable definable (in DCF_0) subgroup G (of finite Morley rank) of an elliptic curve $E(a)$ with differentially transcendental j-invariant a. So it turns out that there are "exotic" groups of finite Morley rank definable in differentially closed fields. In any case in section 2 of this paper we prove the existence of $2^{\aleph_0}$ countable differentially closed fields. The argument we present was sketched for us by E. Hrushovski, although we have a few additional simplifications. In fact, given an example due to Manin [M], showing that for any elliptic curve E there is differential rational homomorphism from E onto G_a (the additive group), the existence of the required type p turns out to rather a direct matter, requiring neither the deep Zariski-geometry interpretation, nor the properties of "jet groups" of algebraic groups.

On the other hand, in so far as simple (noncommutative) groups of finite Morley rank are concerned, no exotic structures are to be found in differentially closed fields. Any such group G will be definably isomorphic to an algebraic group living in the constants. This is exactly the finite Morley rank case of Cassidy's Theorem [C2], of which I will give an easy proof in section 1. This implies that any infinite field F of finite Morley rank definable in a differentially closed field K is definably isomorphic to the field of constants of K. The remaining part (namely the infinite Morley rank case) of Cassidy's Theorem, states that a simple group of infinite Morley rank definable in a differentially closed field K is definably isomorphic to an algebraic group over K. We were unable to find

a "naive" proof of this (as in the finite Morley rank case), but in section 5 we outline a fast proof due to Buium. In sections 3 and 4 we present the machinery and properties of "jet" groups of algebraic groups. This is due to Buium [B1] and [B2], who worked scheme-theoretically. Following Buium, we recover Manin's results [M] concerning the existence of differential rational homomorphisms from arbitrary abelian varieties into vector groups. Following [HS] we point out how this, together with the "Zariski-geometry" interpretation, yields the classification, up to nonorthogonality, of nontrivial Morley rank 1 types in DCF_0.

For the remainder of this paper $\mathbf{U} = (U, +, \cdot, \delta)$ will denote a big saturated differentially closed field of characteristic 0. C denotes the field of constants of $\mathbf{U}$. All objects we talk about will be ones definable in $\mathbf{U}$. RU will denote Lascar's "U-rank". Morley rank (RM), RU etc., will always mean in the sense of $(U, +, \cdot, \delta)$, unless stated otherwise. We usually write x' in place of $\delta(x)$ The reader is referred to Marker's paper [Mr] in this volume for various basic facts about differentially closed fields. But I remark here that the field of constants C with all the definable structure induced from $\mathbf{U}$ is simply an algebraically closed field $(C, +, \cdot)$. For the purposes of this paper a differential algebraic group is simply a group definable in a differentially closed field. (The equivalence of the categories of differential algebraic groups and definable groups is pointed out in [P1]. However to obtain an equivalence which preserves "fields of definition" is rather more tricky, and appears in [P2].) By a minimal group we usually mean a definable commutative group without proper definable connected subgroups (where "definable" means in $\mathbf{U}$ or in the field structure of $\mathbf{U}$, depending on the context).

I will be using facts from stability theory and stable group theory quite freely. (See [Po].) Among other things, I may be using facts such as : an infinitely definable group in an ω-stable structure is definable; an infinite definable group in an ω-stable structure has an infinite definable commutative subgroup. I also use fairly freely the fact that any group definable in an algebraically closed field $(K, +, \cdot)$ is definably isomorphic to $G(K)$ for G some algebraic group defined over K, and also that an infinite field definable in $(K, +, \cdot)$ is definably isomorphic to K. We also make use in various places of the following theorems about abstract algebraic groups and abelian varieties (see for example [Sh] and [L]):

(a) If G is a connected algebraic group defined over a field k, then G has a unique maximal normal linear algebraic subgroup N, and G/N is an abelian variety.

(b) if A is an abelian variety then the torsion part of A is infinite, and for any n, the n-torsion of A is finite.

(c) if A is an abelian variety defined over k, then any algebraic subgroup (connected or not) of A is defined over $\mathrm{acl}(k)$.

At some points (as in (a), (b), (c) above for example) we will be interested in objects defined in $\mathbf{U}$ just in the field language. We will thus denote the structure $(U, +, \cdot)$ by $\mathbf{U}^-$., and we talk about "definable in $\mathbf{U}^-$". Similarly $tp^-(a/k)$ is the complete type of a over k in the structure $\mathbf{U}^-$, and $\mathrm{RM}^-(a/k)$ is the Morley

rank of $tp^-(a/k)$ in the structure $\mathbf{U}^-$. For notions from stability (including the "geometric" theory), I would recommend [P3]. Simply for basic stability I recommend [Las]. I thank E. Hrushovski for several communications, and also D. Marker for some helpful discussions.

§1 Simple groups of finite Morley-rank.

The key point in getting a handle on simple definable groups (of finite Morley dimension or not) is to embed them definably in some $GL(n, \mathbf{U})$. In fact any group definable in $\mathbf{U}$ can be embedded in an algebraic group over $\mathbf{U}$, namely into a a group definable in $\mathbf{U}^-$ (this is proved in [P2]). For groups of finite Morley rank the proof is a little easier and we give it now.

Lemma 1.1. Let G be a connected group of finite Morley rank definable in $\mathbf{U}$. Then G is definably embeddable into some definable group H where H is definable in $\mathbf{U}^-$ and connected (as a group definable in $\mathbf{U}^-$).

Proof.

Let k be a countable model (elementary substructure of $\mathbf{U}$, or equivalently differentially closed differential subfield of $\mathbf{U}$) over which G is defined. Let a be a generic point of G over k. As $\mathrm{RM}(a/k)$ is finite so is tr.degree $k\langle a\rangle/k$. Thus there is some tuple a from $k\langle a\rangle$ such that $k\langle a\rangle = k(a)$. Write $a = f(a)$ where $f(x)$ is some k-definable function defined at a. Choose $b \in G$ generic over $k\langle a\rangle$. So $k\langle b\rangle = k(f(b))$. Then $a \cdot b$ is generic in G over each of $k\langle a\rangle, k\langle b\rangle$. Moreover $a.b \in (k\langle a\rangle)\langle b\rangle = (k(f(a))(f(b))$. So $f(a.b) \in k(f(a), f(b))$. Let $p(x) = tp^-(a/k)$ $(= tp^-(f(b)/k) = tp^-(f(a.b)/k))$. Then easily $f(a)$ and $f(b)$ are independent realisations of p in $\mathbf{U}^-$. Similarly for $f(a)$ and $f(a \cdot b)$, $f(b)$ and $f(a \cdot b)$. Let $g(x, y)$ be a function k-definable in $\mathbf{U}^-$ such that $f(a.b) = g(f(a), f(b))$. Clearly then g is (in $\mathbf{U}^-$) a generically associative k-definable function from $p \times p$ to p. By a result of Hrushovski [Po, 5.23] (or even Weil's theorem) there is some connected group H definable over k in $\mathbf{U}^-$ such that $p(x)$ is the generic type of H. The map f which takes generic a of G to $f(a) \in H$ can be easily seen to extend to a definable embedding of G into H.

Corollary 1.2. Let G be a centreless connected group of finite Morley rank definable in $\mathbf{U}$. Then there is a definable embedding of G into $GL(n, \mathbf{U})$ for some n.

Proof.

Let H be a group definable in $\mathbf{U}^-$ such that G is definably embedded in H. H can be identified (definably) with an algebraic group over $\mathbf{U}$. H may be assumed to be connected. Choose H of least dimension (or equivalently least Morley rank in $\mathbf{U}^-$). Then $Z(H)$, the centre of H, has trivial intersection with G,

so G embeds definably in $H/Z(H)$ (another connected group definable in $\mathbf{U}^-$). Thus $Z(H)$ is finite (otherwise $\dim(H/Z(H)) < \dim(H)$). But then $H/Z(H)$ is centreless. Thus we have definably embedded G into a centreless algebraic group which we call H again. But it is well known [B] that any centreless algebraic group embeds (as an algebraic group, so definably in $\mathbf{U}^-$) in $GL(n, \mathbf{U})$ (some n). This completes the proof.

We need to know some elementary facts about definable subgroups of $\mathbf{U}^n$ and $(\mathbf{U}^*)^n$.

Fact 1.3. Let G be a definable (in $\mathbf{U}$) subgroup of $\mathbf{U}^n$. Then G is a vector space over C. If moreover G has finite Morley rank, then G is a finite-dimensional vector space over C.

Proof. The set $A = \{a \in C : aG \subseteq G\}$ is a definable (in $\mathbf{U}$) additive subgroup of C which is infinite (as it contains $\mathbf{Z}$). Thus (as C is strongly minimal in $\mathbf{U}$), $A = C$. The last remark is clear, for if the C-dimension of G is $> m$ then $\mathrm{RM}(G) > m$ (since C-dimension$(G) = \mathrm{RM}(G)$ if the latter is finite).

Fact 1.4. The map which sends $(x_1, \ldots, x_n)$ to $(\frac{x_1'}{x_1}, \ldots, \frac{(x_n)'}{x_n})$ defines a homomorphism from $(\mathbf{U}^*)^n$ onto $\mathbf{U}^n$ with kernel $(C^*)^n$.

Proof.

The fact that the map is a homomorphism with kernel as stated is checked immediately. Surjectivity follows for example by comparing RU-ranks (as $\mathbf{U}$ is differentially closed, so ω-stable).

Theorem 1.5. Let G be a simple group of finite Morley rank definable in $\mathbf{U}$. Then there is a group H definable in the structure $(C, +, \cdot)$ such that G is (in $\mathbf{U}$) definably isomorphic to H. Otherwise stated; there is an algebraic group H defined over C such that G is definably isomorphic to $H(C)$.

Proof.

By Corollary 1.2, we may assume G is a definable subgroup of $GL(n, \mathbf{U})$ for some n. Now G, as an ω-stable group, has an infinite commutative definable subgroup A. We use some elementary facts on linear algebraic groups, for which the reader is referred to [Bo]. By the Lie-Kolchin Theorem, we may assume that A is a group of upper triangular matrices. Let p be the homomorphism from A into the group D of diagonal $n \times n$ matrices (namely p is simply projection on the diagonal). p is clearly definable.

Case (i). $Ker(p)$ is nontrivial.

Let $B = Ker(p)$. B is then a commutative group of unipotent matrices, and is known to be isomorphic by the map

$$\log(X =)(X - I) - \frac{(X-I)^2}{2} + \ldots + (-1)^n \frac{(X-I)^{n-1}}{n-1}$$

to a subgroup, say B_1, of the additive group of $n \times n$ matrices over $\mathbf{U}$. Then B_1 is definable and of finite Morley rank. By Fact 1.3 $B1$ is a finite dimensional vector space over C. In particular B_1 and thus also B, are connected. As G is simple and of finite Morley rank, by Zilber's indecomposability theorem, there are $g(1), .., g(k)$ in G such that $G = B \cdot Bg(1) \cdots Bg(k)$. Thus G is definably isomorphic to a group $H \subseteq C^m/E$ (where E is some definable equivalence relation). But any definable (in $\mathbf{U}$) relation on C^m is definable in$(C, +, \cdot)$. Thus G can be identified with a group definable in $(C, +, \cdot)$, as required.

Case (ii). $Ker(p)$ is trivial.

Thus p yields an isomorphism of A with a subgroup D_1 of $(U^*)^n$. If $D_1 \cap (C^*)^n$ is infinite, then an application of Zilber's indecomposability theorem as in Case (i) again yields the desired conclusion. Otherwise let m be the cardinality of $D_1 \cap (C^*)^n$. Then clearly $mD_1 \cap (C^*)^n = 1$. Let $D_2 = mD_1$. So by Fact 1.4, D_2 is definably isomorphic to a (infinite) subgroup of $\mathbf{U}^n$, which must have finite Morley rank and is again a finite-dimensional vector space over C. Proceed as in Case (i). This completes the proof.

Corollary 1.6. If F is an infinite field definable in $\mathbf{U}$ and F has finite Morley rank, then F is definably isomorphic to the field C of constants of U.

Proof.

It is known that F must be algebraically closed. $PSL_2(F)$ is then a simple group of finite Morley rank definable in $\mathbf{U}$, so by 1.5, is definably isomorphic to a group H definable in C. Now F is definably isomorphic to a field definable in the pure group structure of $PSL_2(F)$ (by considering a Borel subgroup). Thus F is definably isomorphic to a field K living in C. Then K is definable in $(C, +, \cdot)$ so is (by [Po]) definably isomorphic to the field C. The result follows.

Remarks 1.7. (i) We were a little heavy handed in the proof of 1.5. From Facts 1.3, 1.4, simplicity of G and the facts used about commutative linear groups, one sees directly that G is nonorthogonal to C, thus internal to C.

(ii) Cassidy points out in [C1] that if G is any connected definable subgroup of $(U^*)^n$ and G_1 is the Zariski closure of G then $G_1 \cap (C^*)^n = G \cap (C^*)^n$. One can deduce from this that if such a group G has RU-rank ωm for some $m > 0$, then G is algebraic.

(iii) Proving that any definable simple group G of infinite Morley rank is definably isomorphic to an algebraic group over $\mathbf{U}$, is a rather more subtle issue. One can assume that G is Zariski dense in a simple algebraic group. But the kind of arguments used in the finite Morley rank case do not work, as U is not a "pure field". Cassidy's proof in [C2] involves detailed facts about root systems in Chevalley groups. Buium [B2] has a direct and conceptual proof using the "jet groups" which appear in the next sections, together with the fact that a simple algebraic group acts irreducibly on its Lie algebra. We sketch his proof in section 6. It would be nevertheless nice to find a more model-theoretic proof, for example by finding a "large" definable diagonalisable subgroup of G, and then

using (ii) and the indecomposability theorem. On the other hand it is not true that any simple differential algebraic subgroup of $GL(n, \mathbf{U})$ of infinite Morley rank is already algebraic (namely definable in $\mathbf{U}^-$).

For example let $G = \{(X, X\prime) : X \in SL(n, \mathbf{U})\}$ with multiplication $(X, X') \cdot (Y, Y') = (XY, (XY)')$. G can be represented as a definable subgroup of $GL(2n, \mathbf{U})$, with X in the top left hand corner and bottom right hand corner, and X' in the top right hand corner.

§2. Elliptic curves and many countable models

2. Elliptic curves and many countable models.

The aim here is to give as painless a proof as possible of the existence of continuum many countable differentially closed fields. We will give such a proof, modulo a result of Manin (Lemma 2.3 below). In fact Manin's result is essentially just an example in the introduction to [M]. There are several definitions of "elliptic curve". For example : a connected one-dimensional algebraic group which is complete as an algebraic variety, a nonsingular projective algebraic curve of genus one with a distinguished point, or even a nonsingular projective cubic curve with a distinguished point. Among the important things for us is that the family of such objects has an infinite moduli space. In any case an elliptic curve is a certain kind of algebraic group, and as such is an object defined in $\mathbf{U}^-$. (We view $\mathbf{U}^-$ as a universal domain for algebraic geometry. If you wish identify $\mathbf{U}^-$ with $\mathbf{C}$, the complex field.) More generally an abelian variety is a connected (infinite) algebraic group whose underlying variety is complete (see [Sh]). An abelian variety is said to be simple if it has no proper abelian subvarieties. An elliptic curve is then just a one-dimensional abelian variety. The following fundamental information can be found in any basic text on elliptic curves, e.g [Si].

Fact 2.1. To each elliptic curve E can be associated an element $j(E) \in U$, with the following properties.

(i) $j(E)$ is in any field of definition of E (in the algebraic sense).

(ii) E is isomorphic to E_1 iff $j(E) = j(E_1)$ (Here isomorphic means as algebraic groups).

(iii) for any j, there is an elliptic curve E such that $j(E) = j$ and E is defined over j.

Example 2.2. Let $a, b \in \mathbf{U}$ satisfy $4a^3 + 27b^2 \neq 0$. Then the solutions of the equation $y^2 = x^3 + a^x + b$ together with the point at infinity form an elliptic curve (whose 0 is the point at infinity, and with the "chord-tangent" group law). The j-invariant of this curve is traditionally given as $(12^3)(4a^3/4a^3 + 27b^2)$.

Any elliptic curve is isomorphic to one of the above form. Given $j \neq 0, 12^3$, the following cubic defines an elliptic curve with invariant j: $y^2 = 4x^3 - 27(j/j - 12^3)x - 27(j/j - 123)$.

The following appears essentially in the introduction to [M].

Lemma 2.3. Let E be an elliptic curve. Then there is a definable (in $\mathbf{U}$) nontrivial homomorphism from E into $(\mathbf{U}, +)$.

Let us quickly remark that if X is a set definable in $\mathbf{U}^-$, then the Morley rank (or U-rank) of X in $\mathbf{U}$, is simply ωd, where $d = \mathrm{RM}^-(X)$. In particular, an elliptic curve has RU-rank ω, as an object definable in $\mathbf{U}$.

Corollary 2.4. Let E be an elliptic curve defined (in $\mathbf{U}^-$) over k. Then there is a subgroup G of E, definable in $\mathbf{U}$ such that

(i) G has finite Morley rank,

(ii) G is infinite, connected and k-definable, and has no proper infinite k-definable subgroup.

Proof.

Let $f : E \to \mathbf{U}$ be the homomorphism given by lemma 2.3. Now in $\mathbf{U}$, E has U-rank ω (and is still connected). Thus $ker(f)$ is a proper definable subgroup of E, hence has finite RU-rank (equivalently finite Morley rank). As $(\mathbf{U}, +)$ is torsion-free it follows that $ker(f)$ contains $\mathrm{Tor}(E)$ (the torsion part of E). Note that $\mathrm{Tor}(E)$ is infinite. Let B be the intersection of all definable subgroups of E which contain $\mathrm{Tor}(E)$. Then B is k-definable, infinite, connected, and of finite Morley rank. Now choose G to be a k-definable infinite connected subgroup of B which has no proper infinite k-definable infinite subgroup.

The main point is to show that for suitable elliptic curves E, any group G as given by 2.4 has generic type orthogonal to $\emptyset$.

Theorem 2.5. Suppose $a \in \mathbf{U}$ is differentially transcendental. Let $E(a)$ be an elliptic curve defined over a (in $\mathbf{U}^-$) and with $j(E(a)) = a$. Let G be a subgroup of $E(a)$ of finite Morley rank, which is connected, infinite, defined over a (in $\mathbf{U}$), and has no proper infinite definable subgroup also defined over a. Let $p(x)$ be the generic type of G. Then $p(x)$ is orthogonal to $\emptyset$.

Proof.

Let us write $p(x)$ as $p(x, a)$. Basic facts about orthogonality mean that we have to prove:

Restatement: if $b \in \mathbf{U}$, $tp(b/d) = tp(a/\emptyset)$ and b is independent from a over $\emptyset$, then $p(x, a)$ is orthogonal to $p(x, b)$.

Aiming for a contradiction, we assume this fails. Thus we have b as in the hypothesis of the restatement, but with $p(x, a)$ nonorthogonal to $p(x, b)$.

Step I. We find a connected group H defined over some parameter c with c independent from a over $\emptyset$, and a definable isomorphism h between H and G.

Note $p(x,a)$ is the generic type of G. By assumption $p(x,a)$ is nonorthogonal to $p(x,b)$. Let $G(b)$ denote the "copy" of G over b. Let $\{b_0, b_1, \ldots\}$ be a set of realisations of $tp(a/d)$ such that $\{a, b_0, b_1, ...\}$ is $\emptyset$-independent.

Claim Ia. There is a "small set" A of parameters, there is a proper a-definable subgroup N of G, and there is $n < \omega$ such that $G/N \subseteq \mathrm{dcl}(A \cup G(b_0) \cup \ldots \cup G(b_n))$.

Proof.

This is really a basic stable-group-theoretic result due essentially to Hrushovski. However, I do not know a reference for the specific form in which the claim is stated, so I sketch the proof. The nonorthogonality assumption means that there is a model M containing $\{a,b\}$, and there are elements c realising $p(x,a)|M$ and d realising $p(x,b)|M$ such that c forks with d over M. Let e be the canonical base of $tp(d, M/c, a)$. Then $e \in \mathrm{dcl}(c,a) \cap \mathrm{dcl}(d, M, d_1, M_1, .., d_n, M_n)$ (for some n) where $(d_0, M_0) = (d, M)$ and (d_i, M_i) is an $\{a,c\}$-independent sequence of realisations of $tp(d, M/c, a)$. Let $b_i \in M_i$ be the copy of b. Then clearly $\{a, b_0, \ldots, b_n\}$ is an independent set of realisations of $tp(a/d)$ so we may assume that the b_i are the same as the ones mentioned before the claim. Also note that c (as well as e) is independent from $M_0 \cup \ldots \cup M_n$ over a. Let $G_i = G(b_i)$. Note that $d_i \in G(b_i)$. Write $e = f(c)$ for some a-definable function f. Let N be $\{g \in G :$ for c_1 realising $p(x,a)|\{a,g\}$, $f(g \cdot c_1) = f(c_1)\}$. Then (as $e \in \mathrm{acl}(a)$) one can show that N is a proper a-definable subgroup of G. Let X be a big Morley sequence in$p(x,a)|(M_0 \cup \ldots \cup M_n)$. Then one can show that for c_1 realising $p(x,a)|(M_0 \cup \ldots \cup M_n \cup X)$, $c_1/N \in \mathrm{dcl}(\{a\} \cup X \cup \{f(c_1 \cdot c_2) : c_2 \in X\})$. But (for such c_1) for all $c_2 \in X$, by automorphism, $f(c_1 \cdot c_2) \in \mathrm{dcl}(M_0 \cup \ldots \cup M_n \cup \{h_0, ..., h_n\})$ for some $h_i \in G(b_i)$. Thus, choosing A to be $X \cup M_0 \cup \ldots \cup M_n \cup \{a\}$, we see that $c_1/N \in \mathrm{dcl}(A \cup G(b_0) \cup \ldots \cup G(b_n))$. As every element of G/N is a product of such generic elements c_1/N, it follows that $G/N \in \mathrm{dcl}(A \cup G(b_0) \cup \ldots \cup G(b_n))$, so proving the claim.

Let Y denote the $\{b_0, .., b_n\}$-definable set $G(b_0) \cup \ldots \cup G(b_n)$. By the claim (and compactness), there is some A-definable set of tuples from Y, and some A-definable equivalence relation E on X, such that G/N is in A-definable bijection with X/E. By stability, there is some tuple c of parameters from $Y \cup \{b_0, .., b_n\}$ such that X, E and also the induced group operation on X/E are all definable with parameter c. Let H be the resulting c-definable group, and let h be the A-definable isomorphism between H and G/N.

Claim Ib. c is independent from a over $\emptyset$.

Proof. By choice, $\{b_0, \ldots, b_n\}$ is independent from a over $\emptyset$, and as c is contained in $Y = G(b_0) \cup \ldots \cup G(b_n)$, $tp(c/b_0, .., b_n)$ has finite RU-rank. As $tp(a/b_0, .., b_n)$ has RU-rank ω, c must be independfent from a over $\{b_0, .., b_n\}$. Thus c is independent from a over $\emptyset$.

Now by choice of G and the fact that N is a-definable, N must be finite. At this point we could replace G by G/N and E by E/N. Alternatively, let h_1

be the map from H into G defined by $h_1(y) = \sum h^{-1}(y)$. Using the fact that both G and H are divisible, with finite n-torsion for all n, it is clear that h_1 is a surjective definable homomorphism with finite kernel N_1. Now N_1 must be acl(c)-definable (by the torsion condition on H). Thus h_1 induces a definable isomorphism between H/N_1 and G, where H/N_1 is definable over $c_1 \in \text{acl}(c)$. By the claim c_1 is independent with a over $\emptyset$. Thus Step I is complete.

Step II. From H, c and h as given by Step I, we construct a commutative group H_n defined over $\mathbf{Q}\langle c\rangle$ in $\mathbf{U}^-$, and a surjective homomorphism h_1, definable in Um, from H_n to E.

Let $r \in S(\mathbf{Q}\langle a\rangle)$ be the generic type of G, and r^- the reduct of r to $\mathbf{U}^-$. So r^- is precisely the generic type of E (over a). Note that RM H is finite. By Lemma 1.1 (and its proof), we may assume that H is a subgroup of a group defined over $k_0 = \mathbf{Q}\langle c\rangle$ in $\mathbf{U}^-$. In particular the group operation on H is definable in $\mathbf{U}^-$ over k_0. Let k be some differential field containing a, c such that the isomorphism h is defined over k (in $\mathbf{U}$). Let b be a generic point of H over k. Then $h(b)$ is a generic point of G over k. Moreover, by quantifier elimination, there is some n, such that $h(b) \in k(b, b', .., b^{(n)})$ (the field generated by k together with $\{b, b', .., b^{(n)}\}$). Thus $h(b) = h_1(b, b', .., b^{(n)})$ where $h(y)$ is k-rational. Let $q^- = tp^-(b, b', .., b^{(n)}/\mathbf{Q}\langle c\rangle)$. As in the proof of Lemma 1.1, mulitiplication on H induces a k_0-rational generically associative map * from $q^- \times q-$ to $q-$, yielding as there a (commutative) group H_n say, definable over k_0 in $\mathbf{U}^-$, and with generic type q^-, and with group operation agreeing with * generically. It is clear that for b realising $q^-|k$, $h_1(b)$ realises $r^-|k$. It should also be clear that for generic k-independent (in the sense of $\mathbf{U}^-$) realisations b, c of $q^-|k$, $h_1(b \cdot c) = h_1(b) \cdot h_1(c)$. Thus h_1 defines a k-rational isomorphism from H_n onto E.

Step III. We find a quotient group B of H_n, definable over acl($\mathbf{Q}\langle c\rangle$) in $\mathbf{U}^-$, which is definably (in $\mathbf{U}^-$) isomorphic to G.

This part of the proof just involves facts about algebraic groups. We now use the fact that H_n (obtained in Step II) has the structure of a (commutative) algebraic group defined over $k_0 = \mathbf{Q}\langle c\rangle$, and that h_1 is a rational homomorphism from H_n onto the elliptic curve E. Now H_n has a unique maximal connected linear algebraic subgroup L, and H_n/L is an abelian variety. As there is no nonzero rational homomorphism from a linear algebraic group into an abelian variety, it follows that $L < ker(h_1)$. Note that (by uniqueness) L is defined over k_0 (in $\mathbf{U}^-$), thus H_n/L is also defined over k_0. Now if A is an abelian variety defined over k_0 then any algebraic subgroup of A is defined over acl(k_0). Thus in particular, we see that $ker(h_1)$ is defined over acl(k_0). Let $B = H_n/ker(h_1)$. Thus B is an algebraic group defined over acl(k_0) and h_1 induces a rational isomorphism h_2 say between B and E. Thus B is also an elliptic curve, whereby $j(B) = j(E)$ (by 2.1 (ii)). By 2.1 $j(E) \in \mathbf{Q}\langle a\rangle \cap$ acl($\mathbf{Q}\langle c\rangle$). But $\mathbf{Q}\langle a\rangle$ is independent from acl($\mathbf{Q}\langle c\rangle$) over $\emptyset$ in $\mathbf{U}$, so the same is true in $\mathbf{U}^-$, thus $a = j(E) \in \text{acl}(\mathbf{Q})$, which is a contradiction to the choice of a. This contradiction proves Theorem 2.5.

Corollary 2.6. DCF_0 has $2^{\aleph_0}$ countable models.

Proof.

Let $E(a)$ be an elliptic curve defined over a (in $\mathbf{U}^-$) and with j-invariant a, where $a \in \mathbf{U}$ is differentially transcendental over $\emptyset$. Let $G = G(a)$ be a subgroup of $E(a)$ given by Corollary 2.4. Let $p(x) \in S(a)$ be the generic type of G. By Theorem 2.5, $p(x)$ is orthogonal to $\emptyset$. We will show that DCF_0 has "ENI-DOP". Formally T having "ENI-DOP means that there are models M_0, M_1, M_2, M such that $M_0 \subset M_1$, $M_0 \subset M_1$, M_1 is independent from M_2 over M_0, M is prime over $M1 \cup M_2$, and there is a strongly regular stationary "eventually nonisolated" type $p_1 \in S(M)$ such that p is orthogonal to M_1 and orthogonal to M_2. (A stationary type q is said to be eventually nonisolated if there is a finite set A and a stationarisation of q over A which is nonisolated.). To obtain this, let M_0 be some model independent with a over $\emptyset$. Let b, c be independent generics of $\mathbf{U}$ over M_0 such that $b+c = a$. Then $\{a, b, c\}$ is pairwise independent over $\emptyset$, and also pairwise independent over M_0. Let M_1 be prime over $M_0 \cup \{b\}$, and M_2 prime over $M_0 \cup \{c\}$. In particular a is independent from each of M_1, M_2 over $\emptyset$. Thus $p(x)$ is orthogonal to each of M_1, M_2. Let M be prime over $M_1 \cup M_2$. Then $a \in M$. We can find types $p_1, .., p_m$ over M each of Morley rank 1 such that $p(x)$ is domination equivalent to $p1 \otimes \cdots \otimes p_m$ (this uses the fact that $p(x)$ is the generic type of a group of finite Morley rank.) Thus each p_i is orthogonal to each of M_1, M_2. Now G is divisible. So as a structure in its own right (namely with all a-definable structure induced from $\mathbf{U}$) G is not $\aleph_0$-categorical. It easily follows that some p_i is eventually nonisolated. (In fact the fact that G has no proper infinite connected a-definable subgroups implies that G is almost rank 1, namely that after adding finitely many parameters, there is a Morley rank 1 (not necessarily degree 1) subset X of G such that $G \in \mathrm{dcl}(X)$. As G is not $\aleph_0$-categorical, some strongly minimal subset of X is not $\aleph_0$-categorical, yielding the required ENI-type.) So p_i witnesses ENI-DOP. By [SHM], DCF_0 has continuum many countable models.

Remark 2.7. As we shall see below, if E is an elliptic curve, then any infinite definable (in $\mathbf{U}$) subgroup of E contains $\mathrm{Tor}(E)$, and thus E has a unique minimal infinite definable subgroup (of finite Morley rank). This is also true if E is a simple abelian variety, namely an abelian variety without proper connected nontrivial algebraic subgroups. Thus the group G in 2.4 can be taken to be minimal (namely without proper connected definable subgroups). In fact making use of the Zariski interpretation, one can show (as we do later) that G must be actually strongly minimal.

In the remainder of this paper we develop tighter connections between groups definable in $\mathbf{U}$ and those definable in $\mathbf{U}^-$. In particular we obtain (following Buium [B2]) a generalisation of Lemma 2.3 to arbitrary abelian varieties. This is connected with Manin's "Theorem of the kernel" from [M].

§3 Jet Groups.

In this section we develop the theory and some properties of the "twisted jet groups" of Buium [B2], but working in the definable category. We work as before in the big differentially closed field $\mathbf{U}$.

As motivation let us first consider the general linear group $G = GL(n, \mathbf{U})$. If the matrix $X = (x_{i,j}) \in G$, let X' denote the matrix whose i, j^{th} coordinate is $x'_{i,j}$. The set $\{(X, X') : X \in G\}$ has a natural group structure: $(X, X') \cdot (Y, Y') = (XY, (XY)')$. It is rather clear that this group is precisely the subgroup of $GL(n, \mathbf{U})$ consisting of matrices

$$\begin{pmatrix} X & X' \\ 0 & X \end{pmatrix}$$

where $X \in G$.

The Zariski closure of this group in $GL(2n, \mathbf{U})$ is the set of matrices

$$\begin{pmatrix} X & Y \\ 0 & X \end{pmatrix}$$

with $X \in G$ and Y arbitrary. Let us call this group G_1.

We have a natural projection map $p : G_1 \to G$ whose kernel is the group of matrices

$$\begin{pmatrix} I & Y \\ 0 & I \end{pmatrix}$$

where Y is an arbitrary $n \times n$ matrix. Let us call this kernel L_1. Note that L_1 is isomorphic to the vector space $\mathbf{U}^{n^2}$. In fact L_1 is precisely $gl(n, \mathbf{U})$, the "Lie algebra" of G, and G_1 splits as a semidirect product of the group of matrices

$$\begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}$$

with L_1. Let us call the first group $G_{1,1}$ (a copy of G). The action of $G_{1,1}$ on L_1 by conjugation in G_1 is exactly the action of G on $gl(n, \mathbf{U})$ by conjugation, inducing the "adjoint" representation. We also have a map $f : G \to L_1$ defined in DCF_0, obtained by taking X to $(X, X') \in G_1$ and then projecting onto L_1. (f will not be a homomorphism, but a crossed homomorphism.) It can be checked that f is precisely the map $X \mapsto X^{-1}X'$. Thus $Ker(f)$ is $G(C) = GL(n, C)$, the group of C-rational points of G. By comparing with [Bo. AG 16 and I.3], we see that G_1 is precisely the tangent bundle of G. Note that the process can be iterated, to obtain linear algebraic groups $G_2, G_3, \ldots$ where for example G_2 is the group consisting of matrices

$$\begin{pmatrix} X & Y & Z \\ 0 & X & Y \\ 0 & 0 & X \end{pmatrix}$$

with $X \in G, Y, Z$ arbitrary. These groups are the natural jet space groups attached to G (higher versions of the tangent bundle).

We proceed to develop these objects in greater generality. As mentioned above, we work in the definable category (namely we do not concern ourselves with the geometric structure of objects). The constructions below generalise arguments in the proof of 2.5.

Definition 3.1. Let G be a connected group definable in $\mathbf{U}$, defined over $k \subset \mathbf{U}$. So a point of G is some n-tuple from $\mathbf{U}$. If $a = (a_1, .., a_n) \in G$then by a' we mean the tuple $(a'_1, \ldots, a'_n)$.

(i) for $m > 0$, $e_m(G)$ denotes the group $(\{(a, a', .., a^{(m)}) : a \in G\}, *_{(m)})$ where the group operation $*_{(m)}$ is defined by :

$$(a, a', \ldots, a^{(m)}) *_{(m)} (b, b', \ldots, b(m)) = ((a \cdot b), ..., (a \cdot b)^{(m)}).$$

(So $e_0(G)$ is precisely G). We also let e_m denote the map from G to $e_m(G)$: $a \mapsto (a, a', \ldots, a^(m))$.

Remark 3.2. (i) For any $m > 0$, $e_m(G)$ is also a connected group definable in $\mathbf{U}$ over k, and e_m is a k-definable group isomorphism.

(ii) Suppose that the group operation on G is definable over k in $\mathbf{U}^-$, namely there is a partial function $f(\ ,\ )$ defined over k in the field language, such that for $a, b \in G$, $f(a, b) = a \cdot b$. Then for any m, the group operation $*_{(m)}$ is also defined over k in $\mathbf{U}^-$. For example this is the case if G itself is definable in $\mathbf{U}^-$, or if G is a subgroup of such a group.

As mentioned earlier RM^- denotes Morley rank computed in the structure $\mathbf{U}^-$. For the remainder of this section we assume that G is a group definable over k in $\mathbf{U}^-$, which is connected in $\mathbf{U}^-$, and thus also connected in $\mathbf{U}$. (The latter fact is not obvious. It is due to Kolchin (see appendix C of Marker's paper [Mr] in this volume. The special case we use here is also proved in [HS].)

Construction 3.3.

We construct, for each m, a group G_m also definable over k in $\mathbf{U}^-$, and surjective homomorphisms $\pi_m : G_m \to G_{m-1}$.

For $m = 0, G_m = G$.

Let $m > 1$. Let a be a generic point of $e_m(G)$ over k (generic in the sense of $\mathbf{U}$). (Note that a is then of the form $(a, a', \ldots, a^{(m)}) = e_m(a)$, where a is some generic point of G over k, in the sense of $\mathbf{U}$.) Let $p_m(x) = tp(a/k)$, and $p_m^-(x) = tp^-(a/k)$. So p^- is uniquely determined and is moreover a stationary type. Let us write simply . for multiplication in $e_m(G)$. Let a, b, c be an independent (in $\mathbf{U}$) set of realisations of p_m. Then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, and $(a \cdot b)$ is independent from c over k etc. Now working in $\mathbf{U}^-$, a, b, c are also independent realisations of p_m^- over k, and the above independence facts remain true. Also by 3.2 (ii), the group operation $\cdot$ is definable over k in $\mathbf{U}^-$. So a result of Hrushovski [Po, 5.23] (or equivalently Weil's theorem) yields a connected group Gm definable over k in $\mathbf{U}^-$, whose generic type is p^-, and whose group operation agrees with . on independent realisations of p^-. So we have defined the groups G_m. To obtain the homomorphisms π_m, note that, for all $a \in G$ and in particular for generic

such a, $e_{m-1}(a)$ is a subtuple of $e_m(a)$. Define $\pi_m(e_m(a)) = e_{m-1}(a)$. Then clearly p_{m-1} is a map, defined over k in $\mathbf{U}^-$, from the realisations of p_m^- onto the realisations of p_{m-1}^-, which is "generically" a group homomorphism from G_m to G_{m-1}. Namely for independent realisations a, b of p_m^-, $\pi_m(a \cdot b) = \pi_m(a) \cdot \pi_m(b)$. Thus π_m extends to a surjective homomorphism from G_m to G_{m-1}, defined over k in $\mathbf{U}^-$.

The above construction yields an identification of the generic points of $e_m(G)$ with certain generic (in $\mathbf{U}^-$) points of G_m (via the identity map). We would like however to identify in a $\mathbf{U}^-$-definable manner all of $e_m(G)$ with a subgroup of G_m. This is actually quite straigtforward, and can be obtained (as we show now) through the Hrushovski construction of Gm as the group of "germs" of $\mathbf{U}^-$-definable generically defined maps from p_m^- to p_m- generated by the maps $f_a : b \to a*b$ for generic independent realisations a, b of p_m^-. (Here we let $*$ denote the group operation on $e_m(G)$.) In particular G "is" the group of such germs of the form $f_{a_1} \cdot f_{a_2}$. Let now O be the set of $\{(a,b) : a, b$ both realise p^-, $a * b$ is defined, and for generic c realising p^-, $(a*b)*(c) = a*(b*c)\}$. Then Oincludes $\{(a,b) : a, b$ are generic points of $e_m(G)\}$. Define an equivalence relation $\sim$ on O, by $(a,b) \sim (a_1,b_1)$ if for generic c realising p^-, $a*(b*c) = a_1*(b_1*c)$ (if and only if (a,b) and (a_1,b_1) define the same germ, namely the same element of G_m). So we see that $O/\sim$ "is" a subset of G_m. Let $X = \{c :$ for some $(a,b) \in O$, $a*b$ is defined and equals c, and for generic d realising p^-, $(c*d)*d^{-1}$ is defined and equals $c\}$. Then clearly $e_m(G) \in X$ and X is ∞-definable over k in $\mathbf{U}^-$. Define a map f from X into G_m, by: if $c = a*b$ for $(a,b) \in O$, then $f(c) = (a,b)/\sim$. Clearly f is well-defined (for if $c = a_1 * b_1$ for $(a_1,b_1) \in O$ then for generic d realising p^-, $(a*b)*d = c*d = (a1*b1)*d)$. On the other hand f is 1-1, for if $f(c) = f(c_1)$, then for generic d realising p^-, we must have $c*d = c_1*d$. By the second clause in the definition of X, we conclude (after "multiplying" by d^{-1}) that $c = c_1$.

Now f is k-definable in $\mathbf{U}^-$. By compactness we can find sets $X_0 \supseteq X$ and $Y_0 \subseteq G_m$, both definable over k in $\mathbf{U}^-$, and a bijection g between X_0 and Y_0, also defined over k in $\mathbf{U}^-$, such that the restriction of g to $X$is precisely f. So the restriction of the map g to $e_m(G)$ defines a group embedding into G_m extending the identity map on p^-. By means of this embedding we can and will assume that $e_m(G)$ is actually a subgroup of G_m, and thus that e_m is an embedding of G into G_m. If the reader is unhappy with this, he or she can work with elements of $g(e_m(G))$ (g as above) in place of $e_m(G)$. (Note that it is trivial to find an embedding of $e_m(G)$ in G_m definable in $\mathbf{U}$, but the question here was to find one "definable in $\mathbf{U}^-$".)

Lemma 3.4. (i) $\mathrm{RM}^-(G_m) = (m+1)\mathrm{RM}^-(G)$, for all m.

(ii) If X is a subset of G which is definable in $\mathbf{U}$, then for some m there is a subset Y of G_m definable in $\mathbf{U}^-$ such that $e_m(X) = Y \subseteq e_m(G)$.

(iii) If H is a (connected) subgroup of G which is definable in $\mathbf{U}$, then for some m there is a (connected) subgroup H_m of G_m, definable in $\mathbf{U}^-$ and such that $e_m(H)$

Proof.

(i) Suppose $\mathrm{RM}^-(G) = n$. Let a be a generic point of G over k in the sense of U. Then clearly n = differential transcendence degree of $k(a)$ over k. In fact n of the coordinates of a are differentially transcendental over k, and the rest are algebraic over these together with k. So clearly the transcendence degree of $k(a, a', ..., a^{(m)})/k) = (m+1)n$. Thus $\mathrm{RM}^-(tp^-(e_m(a)/k) = (m+1)n$. As $tp^-(e_m(a)/k)$ is a generic type of G_m it follows that $\mathrm{RM}^-(G_m) = (m+1)n$.

(ii). By quantifier elimination in DCF_0, there is some $m < \omega$ and some formula $\psi(x_0, x1, ..., x_m)$ (with parameters) in the language of fields such that $X = \{a \in G : \mathbf{U} \models \psi(a, a', ..., a^{(m)}\}$. So simply let Y be the subset of G_m defined by $\psi(x)$.

(iii). This does not appear to follow directly from (ii). We may assume H is defined over k. Let again $m < \omega$ and $\psi(x_0, .., x_m)$ be a formula (over k) in the language of fields such that $\psi(x, x', ..., x^{(m)})$ defines H in $\mathbf{U}$. Then again $e_m(H) = \{(x_0, x_1, .., x_m) \in G_m : (x_0, .., x_m) \in e_m(G)$ and $\psi(x_0, .., x_m)\}$. Let b be a generic point of H over k. Then $e_m(b)$ is a generic point of $e_m(H)$ over k. Let $q^-(x) = tp^-(e_m(b)/k)$. As in Construction 3.3, the realisations of q^- in G_m are closed under generic (in $\mathbf{U}^-$) multiplication. Thus basic stable group theory yields a connected subgroup H_m of G_m, definable in $\mathbf{U}^-$ over k, and with generic type q^-.

Claim. $H_m \cap e_m(G) = e_m(H)$.

Proof of claim. Clearly $e_m(H) \subseteq H_m$ (as any element of $e_m(H)$ is a product of generics of $e_m(H)$, and all generics are in H_m. For the other inclusion it is enough to show that if $\mathbf{c} = (c, c', ..., c^{(m)})$ is a generic point of $H_m \cap e_m(G)$ over k (in the sense of $\mathbf{U}$) then $\mathbf{c} \in e_m(H)$. Let $\mathbf{c}$ be such. It is then easy to see that tr.degree($\mathbf{c}/k$) $\geq$ tr.degree($e_m(b)/k$) (where remember $e_m(b)$ was a generic point of $e_m(H)$ over k). On the other hand, as $\mathbf{c} \in H_m$ and q^- is (the unique) generic (in $\mathbf{U}^-$) type of H_m, it follows that $\mathrm{RM}^-(\mathbf{c}/k) =$ tr.degree($\mathbf{c}/k$) = tr.degree(q^-) (=RM(q^-)). Thus $\mathrm{tp}^-(\mathbf{c}/k) = q^-$. In particular $\mathbf{U} \models \psi(\mathbf{c})$, namely $\mathbf{U} \models \psi(c, c', ..., c(m))$. So $\mathbf{c} \in e_m(H)$.

§4 Vector groups, the Buium-Manin homomorphism and rank 1 types.

We begin to make more use of notions from algebraic geometry. The reader is referred to [Sh]. Recall the notation from section 3 : given a connected group definable in $\mathbf{U}^-$, we have groups G_1, $G_2 \ldots$ definable in $\mathbf{U}^-$ and rational homomorphisms $\pi_m : G_m \times G_{m-1}$. Let τ_m be the induced homomorphism from G_m onto $G = G_0$.

Lemma 4.1. Suppose $G$is an algebraic group defined over k, of dimension n (namely $\mathrm{RM}^-(G) = n$. Then for all r, $ker(\tau_r)$ is a vector group of dimension $r.n$.

Proof.

We just sketch the proof. We first do it for the case $r = 1$. Let V be an affine open neighbourhood of the identity in G, $V \subset \mathbf{U}^m$, some m, such that the identity element e of G is the origin $(0, ..., 0)$. Assume G is defined over k. Let O_e denote the local ring of G at e, and m_e its maximal ideal. We also assume that the first n coordinates of $x = (x_1, .., x_m) \in V$ form local coordinates (or parameters) for G at e. Namely the coordinate functions $x_1, ..., x_n$ form a basis of the k-vector space m_e/m_e^2. One also knows that $x_1, .., x_n$ generate m_e (in O_e). Thus there are $a_{i,j} \in k$ such that $x \in V$ has the form

$$(x_1, .., x_n, \sum_{i=1}^{n} \alpha_{i,n+1} x^i)(m_e^2), \ldots, \sum_{i=1}^{n} \alpha_{i,m} x^i)(m_e^2)).$$

Namely for $j = n + 1, .., m$,

$$x_j = \sum_{i=1}^{n} \alpha_{i,j} x^i mod(m_e^2).$$

As any element of m_e^2 is of the form $\sum f_i x_i$ for $f_i \in m_e$, this means that for $j = n + 1, ..., m$, $x_j = \sum \alpha_{i,j} x_i + \sum f_{i,j} x_i$ (where $f_{i,j}$ is in m_e). $(*)$

We now want to bring in the group G_1. Let x denote a point of $\mathbf{U}^m$. With a little work we can consider V_1 = Zariski closure in U^{2m} of $\{(x, x') : x \in V\}$, as an affine open subset of G_1, with (0,0) the identity of $G1$. Let $O \subset V \times V = \{(x, y) \in V \times V : x \cdot y \in V\}$, where $x \cdot y$ refers to multiplication in G. Then the group operation on O is given by a rational function f(-,-) (defined over k). The function which takes $((a, a'), (b, b'))$ to $(a \cdot b), (a \cdot b)')$ for $(a, b) \in O$, is also a rational function f_1 say defined over k. Then we can assume that whenever $(a, a_1) \in V_1$, $(b, b_1) \in V_1$ and the product (in G_1), $(a, a_1) \cdot (b, b_1) \in V_1$, then this product is $f_1((a, a_1), (b, b_1))$. Now $x_1, .., x_n$ are also differentially independent parameters over k, so generically $\{x_1, .., x_n, x_1', ..., x_n'\}$ is algebraically independent over k. Thus we can choose an affine open neighbourhood of the identity in G_1, a point of which has the form $(x_1, .., x_n, x_{n+1}, .., x_m, t_1, .., t_n, t_{n+1}, .., t_m)$,

where the x_i satisfy $(*)$, $x_1,..,x_n,t_1,..,t_n$ are local parameters at the identity (0,.....,0) of G_1, and for $j = n+1,..,m$, t_j is of the form:

$$\sum_{i=1}^{n}(\alpha'_{i,j}x_i + \alpha_{i,j}t_i) + \sum_{i=1}^{n} g_{i,j}x_i + \sum_{i=1}^{n} f_i t_i. \qquad (**)$$

where $f_{i,j} = f_{i,j}(x_1,...,x_n) \in m_e$, and $g_{i,j}$ is some rational function of $(x_1,...,x_n,t_1,...,t_n)$. Now such points (x,t) with $x = (0,..,0)$, clearly form an open neighbourhood of the identity in the algebraic group $ker(\pi_1) \subseteq G_1$. By $(**)$ any such point has the form:

$$(0,...,0,t_1,..,t_n), \sum_{i=1}^{n} \alpha_{i,n+1}t_i, ..., \sum_{i=1}^{n} \alpha_{i,m}t_i). \qquad (***)$$

On the other hand, it is well-known (see [L]) that (working back in the original affine open neighbourhood V of G) for (generic) $x, y \in V$, and $i = 1,..,n$, $(x \cdot y)_i = (x_i + y_i) \bmod M^2$, where M is the maximal ideal of the local ring at the identity of $G \times G$. It follows from this together with $(***)$ that for generic $(0,t),(0,s)$ in $ker(\pi_1)$, $(0,t)\cdot(0,s) = (0,t+s)$. Thus generically $ker(\pi_1)$ is isomorphic to the group $\mathbf{U}^n$. So $ker(\pi_1)$ is isomorphic to $\mathbf{U}^n$, as required.

Suppose the lemma is proved for r. The kernel of the projection $(G_r)_1 \to G_r$ is a vector group, by what we have just shown. On the other hand this clearly factors through $p_{r+1} : G_{r+1} \to G_r$. So $ker(\pi_r)$ is a vector group (of dimension $= \dim(G)$). Composing with τ_r completes the proof.

The dimension assertions are contained in 3.4 (i).

Lemma 4.2. Let A be a connected commutative algebraic group. Let B be a connected definable (in $\mathbf{U}$) Zariski-dense subgroup of A. Then A/B is definably isomorphic to a subgroup of $\mathbf{U}^n$ (for some n). In particular B contains the torsion part of A. Proof. Let $A_0 = A, A_1, ...$ be as in section 3. By Lemma 3.4 there is some m such that $e_m(B) = B_m \cap e_m(A)$. As B is Zariski-dense in A, clearly $\tau_m|B_m$ is onto A. Let $L_m = ker(\tau_m)$. Then $A_m = B_m L_m$. As (by 4.1) L_m is a vector group, $B_m \cap L_m$ has a complement L in L_m and A_m is the direct product of B_m and L. Let π be the corresponding projection map from A_m onto L. Let f be the homomorphism $A \to L$ defined by: $f(a) = \pi(a, a', ..., a^{(m)})$. Then $a \in$ ker(f) iff $(a, a', .., a^{(m)}) \in B_m$ iff $(a, a', .., a^{(m)}) \in e_m(B)$ iff $a \in B$.

Note that this lemma recovers Remark 1.7 (ii).

Corollary 4.3. Let A be a simple abelian variety. Then A has a unique minimal infinite connected definable subgroup.

Proof. As A has no proper connected nontrivial algebraic subgroups, every infinite definable subgroup of A is Zariski-dense. In particular, by 4.2, any infinite connected definable subgroup of A contains the torsion part of A (which is

known to be infinite). Thus the intersection of all connected definable subgroups of A is infinite, and is definable (by ω-stability).

Nothing we have said so far shows that proper definable subgroups exist. We proceed to show that one can always find definable subgroups of finite Morley rank (of abelian varieties).

As in Buium's treatment we require the following result of Rosenlicht [R. Lemma 3]:

Fact 4.4. Let A be an abelian variety, B a vector group, and G an extension of A by B. (Namely we have an exact sequence of algebraic groups:

$$0 \to B \to G \to A \to 0.)$$

Then there is a connected algebraic subgroup G_1 of G such G_1 projects onto A and $\dim(G_1) \leq 2\dim(A)$.

Proposition 4.5. Let A be an abelian variety. Then A contains an infinite definable subgroup B of finite Morley rank.

Proof. Let A_m be as in section 3. Let τ_m be the projection $A_m \to A$ (composition of the π_i). For each m there is a unique minimal algebraic subgroup B_m such that B_m projects onto A under π_m. (Uniqueness is by the fact that if B_1, B_2 both project onto A then each of A_m/B_1, A_m/B_2 embeds in the vector group $L_m = ker(\tau_m)$, whereby $A_m/(B_1 \cap B_2)$ embeds in a vector group, so $B_1 \cap B_2$ projects onto A. The last implication is due to the fact that there is no nontrivial homomorphism from a vector group into an abelian variety.) By uniqueness we conclude that π_m maps B_m onto B_{m-1}. On the other hand Fact 4.4 says that $\dim(B_m)$ is bounded by $2\dim(A)$. Let $D = \{a \in A : (a, a', ..., a^{(m)}) \in B_m$ for all $m\}$. Then D is a definable subgroup of A.

Claim. D has finite Morley rank.

Proof.

Assume everything is defined over $k \subset \mathbf{U}$. The bound on the dimensions of the $B_m$means that $\mathrm{tr.deg}(k(a, a', ...a(m), ...)/k)$ is finite, for any $a \in D$, and thus $\mathrm{RM}(tp(a/k))$ is finite for any $a \in D$. Thus $\mathrm{RM}(D)$ is finite.

Putting together 4.3 and 4.5 we have:

Corollary 4.6. Let A be a simple abelian variety. Then A contains a unique smallest definable nontrivial connected subgroup of finite Morley rank.

Lemma 4.7. Suppose A, B are simple abelian varieties, and G, H are definable subgroups of A, B respectively. If G is definably isogenous to H, then A is rationally isogenous to B (namely isogenous by a map definable in $\mathbf{U}^-$).

Proof.

Without loss of generality, H is definably isomorphic to G via the isomorphism $f : H \to G$. Assume everything is defined over k. We use the notation of section 3. Let b be a generic point of H over k. Then for some n and for some k-rational function f_1, $f(b) = f_1(b, b', ..., b^{(n)})$. b is a generic point of B over k (in the sense of $\mathbf{U}^-$) and $f(b)$ is a generic point of A over k (in the sense of $\mathbf{U}^-$) (as G is Zariski-dense in A and H is Zariski-dense in B). Also $(b, b', .., b^{(n)})$ is a generic point of the group H_n over k (in the se nse of $\mathbf{U}^-$). Thus clearly f_1 gives rise to a surjective k-rational homomorphism from H_n onto A. Let τ_n denote the canonical k-rational surjection $B_n \to B$. Then $\tau_n | H_n : H_n \to B$ is surjective. Let $L = ker(\tau_n | Hn)$. So $L \subset ker(\tau_n)$ and the latter is, by 4.1 a vector group. As there is no nontrivial rational homomorphism from a vector group into an abelian variety, it follows that $L \subset ker(f_1)$. Thus f_1 induces a rational map from H_n/L onto A. As H_n/L is rationally isomorphic to B, we obtain a rational homomorphism h from B onto A. As B is a simple abelian variety, h is an isogeny (namely has finite kernel). This completes the proof of 4.7.

We now bring in some rather heavier model-theoretic facts.

Fact 4.8. [HS, HZ]. Let X be a strongly minimal set definable in $\mathbf{U}$. If X is not locally modular then a strongly minimal field is definable in X^{eq}.

Let p_C denote the generic type of the constants $C_{\mathbf{U}}$ of $\mathbf{U}$. p_C has Morley rank 1.

Corollary 4.9. Let q be a non locally modular type of RU-rank 1 (in $\mathbf{U}$). Then q is nonorthogonal to p_C.

Proof. Let X be a strongly minimal set in q. By 4.8 some infinite field (of finite Morley rank) F, is definable in X^{eq}. By Corollary 1.6, F is definably isomorphic to $C_{\mathbf{U}}$. This clearly suffices.

Finally we describe a relationship between nontrivial types of Morley rank 1 which are orthogonal to p_C and simple abelian varieties which are not rationally isomorphic to algebraic groups defined over C_U. We are interested in such types up to nonorthogonality, and some groups up to rational isogeny.

First let q be such a type. By 4.8, q is locally modular and hence by [H], there is a strongly minimal group G whose generic type is nonorthogonal to q, so is without loss q itself. By 1.1, let A be an algebraic group in which G is definably embedded. As G is commutative and strongly minimal, we may assume that A is commutative, connected with no proper connected algebraic subgroups. A is then either a linear group, or a simple abelian variety. If A is linear, then the proof of Theorem 1.5 shows that G is definably isomorphic to a group living in $C_{\mathbf{U}}$, contradicting the nonorthogonality of q to p_C. Thus A is a

simple abelian variety. Note that G must be the unique minimal finite Morley rank definable subgroup of A.

On the other hand, let A be a simple abelian variety not rationally isomorphic to an algebraic group defined over $C_{\mathbf{U}}$. Let G be the definable subgroup of A given by 4.6. Then G is connected, infinite, and has no proper infinite definable subgroups. Thus G is almost strongly minimal. Let X be a strongly minimal subset of G. If X is not locally modular, then by 4.8 the generic type of X is nonorthogonal to p_C. In particular the generic type of G is nonorthogonal to p_C. As in the proof of 2.5 (Step I), G is definably isomorphic to a group H living in $C_{\mathbf{U}}^{\mathrm{eq}}$. As in Step II of the proof of 2.5, A is rationally isomorphic to an algebraic group defined over $C_{\mathbf{U}}$, contradicting our hypotheses on A.

It follows that X must be locally modular. As G is almost strongly minimal, G is a 1-based group. By [HP], and the "minimality" of G, G is already strongly minimal. Let q be the generic type of G.

Proposition 4.10. The above relationship establishes a bijection between the nonorthogonality classes of nontrivial Morley rank 1 types which are orthogonal to p_C, and the isogeny classes of simple abelian varieties which do not "descend" to $C_{\mathbf{U}}$.

Proof.

Let A, B be simple abelian varieties, G, H strongly minimal locally modular definable subgroups of A, B respectively. Let q, r be the generic types of G, H respectively.

From the above discussion it is clearly enough to prove that A is isogenous to B iff q is nonorthogonal to r. First suppose that f is a rational isogeny of A with B. Thus $f(G)$ is a strongly minimal subgroup of B. By 4.6, $f(G) = H$. Thus (as f is finite-to-one), f witnesses the nonorthogonality of q and r. Conversely suppose q is nonorthogonal to r. As G and H are both locally modular strongly minimal groups it follows that G and H are definably isogenous. (After naming enough parameters, we have generics $a \in G, b \in H$ such that a and b are interalgebraic. Now $G \times H$ is a "1-based group". Thus by [HP] $tp(a, b)$ is the generic type of a strongly minimal subgroup of $G \times H$, which yields the required isogeny. By 4.7 A and B are rationally isogenous.

§5 Zariski-dense definable subgroups of simple algebraic groups.

Finally we give a sketch proof (due essentially to Buium [B2]) of the infinite Morley rank case of Cassidy's theorem. We start with a simple (noncommutative) group G, definable in $\mathbf{U}$ and of infinite Morley rank. The aim is to show that G is definably isomorphic to an algebraic matrix group $H \subseteq GL(n, \mathbf{U})$ for some n.

First, a proof like that of Corollary 1.2, but using so-called $*$-groups, shows that G is definably embeddable in $GL(n, \mathbf{U})$ for some n. (This appears in [P2].) Let H be the Zariski-closure of G. Using the simplicity of G, we may assume that H is simple (i.e. has no normal algebraic subgroups). So we are finished if we prove:

Proposition 5.1. Let H be a simple algebraic group over $\mathbf{U}$, and G a Zariski-dense definable (in $\mathbf{U}$) subgroup of H with infinite Morley rank (in $\mathbf{U}$). Then $G = H$.

Proof.

It is known that any simple algebraic group over an algebraically closed field is rationally isomorphic to a matrix group defined over the prime field (namely $\mathbf{Q}$). So we may assume H is such. We make use of the following:

Fact. The action of H on its Lie algebra by the adjoint representation is irreducible.

Let us go back to the "jet groups" H_1, H_2, etc. As in the beginning example in section 3, the action of H on $ker(\pi_1)$, defined by : for $a \in H$, $b \in ker(\pi_1)$, let $a_1 \in H_1$ be such that $\pi_1(a1) = a$, and define $b^a = a_1^{-1} \cdot b \cdot a$, is exactly the adjoint action of H on $Lie(H)$. It follows similarly that for any m, the action of H_m on $ker(\pi_{m+1})$, defined in a similar fashion, is isomorphic to the action of H on $Lie(H)$. Thus all this actions are irreducible.

Now suppose that $G \neq H$. By Lemma 3.4, for some m, G_m is a proper algebraic subgroup of H_m. Choose least such m. (Note $m > 0$, as $G_0 = H_0 = H$). It follows that $\pi_m | Gm : G_m \to H_{m-1}$ is surjective. Let $Lm \subseteq H_m$ be the kernel of π_m. Thus $L_m \cap G_m$ is a proper subgroup of L_m which is invariant under the above-mentioned action of H_{m-1}. By irreducibility, $L_m \cap G_m = \{0\}$. This says that $\pi_m | G_m$ is finite-to one. In particular for generic $a \in G, a^{(m)} \in \text{acl}(a, a', ..., a^{(m-1)}, k)$ (where k is some field over which G is defined). It follows easily that $\text{RM}(tp(a/k))$ is finite, thus $\text{RM}(G) < \omega$, contradiction.

References

[Bo] A. Borel, Linear Algebraic Groups, Springer 1991.

[B1] A Buium, Differential Algebraic Groups of Finite Dimension, Springer Lecture Notes 1506, 1992.

[B2] A Buium, Differential polynomial functions on algebraic varieties I: Differential algebraic groups, American Journal of Mathematics, 1993.

[C1] Ph. Cassidy, Differential algebraic groups, American Journal of Mathematics, 94 (1972), 891-954.

[C2] Ph. Cassidy, The classification of semisimple differential algebraic groups, J. Algebra, 121 (1990), 169-238.

[H] E. Hrushovski, Locally modular regular types, in Classification Theory, ed. J. Baldwin, Lecture Notes in Math. 1292, 1987.

[HP] E. Hrushovski and A. Pillay, Weakly normal groups, Logic Colloquium '85, North-Holland, 1987.

[HS] E. Hrushovski and Z. Sokolovic, Minimal subsets of differentially closed fields, preprint 1994.

[HZ] E. Hrushovski and B. Zilber, Zariski geometries, to appear in Journal of A.M.S..

[L] S. Lang, Introduction to Algebraic Geometry, Interscience, New York, 1959.

[Las] D. Lascar, Stability in Model Theory, Longman, 1987.

[M] Yu. Manin, Rational points of algebraic curves over function fields, AMS Translations, Ser. II 50 (1966), 189-234.

[Mr] D. Marker, Model theory of differential fields, this volume.

[P1] A. Pillay, Differential algebraic group chunks, Journal of Symbolic Logic, 55 (1990), 1138-1142.

[P2] A. Pillay, Some foundational questions concerning differential algebraic groups, preprint 1994.

[P3] A. Pillay, Geometrical stability theory, to appear, Oxford University Press.

[Po] B. Poizat, Groupes Stables, Nur al-Mantiq wal-Ma'rifah, Paris 1987.

[R] M. Rosenlicht, Extensions of vector groups by abelian varieties, American Journal of Mathematics, 80 (1958), 685-714.

[Sh] I. R. Shafarevich, Basic Algebraic Geometry, Springer, 1977.

[SHM] S. Shelah, L. Harrington and M. Makkai, A proof of Vaught's conjecture for ω-stable theories, Israel Journal of Mathematics, 49 (1984), 259-278.

[Si] J. Silverman, Arithmetic of Elliptic Curves, Springer, 1987