DIFFERENTIAL GALOIS THEORY
BANACH CENTER PUBLICATIONS, VOLUME 58
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2002

COMPUTING THE GALOIS GROUP OF A LINEAR DIFFERENTIAL EQUATION

EHUD HRUSHOVSKI
Hebrew University, 91904 Jerusalem, Israel
E-mail: ehud@math.huji.ac.il

Introduction. We show how to determine effectively the (Picard-Vessiot-) Galois group of an ordinary linear differential equation over $\mathbb{Q}(t)$. Model-theoretically, let V be the solution set to the equation in a universal domain for differential fields, and let C denote the solution set to $x' = 0$. We show how to find $Aut(V/\mathbb{Q}(t), C)$.

Algorithms given by Picard can be used to show how to determine the invariants of the Galois group relative to a field L, acting on $V^{\otimes d}$ for bounded d, provided d and $[L : \mathbb{Q}(t)]$ are bounded. Let $G(d, L)$ be the subgroup of $GL(V)$ fixing these invariants. Then for some d, L one has $Aut(V/\mathbb{Q}(t)) = G(d, L)$. The problem is to find the right d, L.

Our approach is to first look for d_1 such that $Aut(V/\mathbb{Q}(t), C) \trianglelefteq G(d_1, \mathbb{Q}(t))$, and the quotient is a finite extension of a multiplicative torus T. Such a d_1, we show, can be found on the basis of $\dim(V)$ alone. It is essential at this point to work over $\mathbb{Q}(t)$ rather than the algebraic closure $\mathbb{Q}(t)^a$, in order to apply Picard; but with this done we pass to the connected components of the identity; $Aut(V/\mathbb{Q}(t)^a, C) \trianglelefteq G(d_1, \mathbb{Q}(t))^0$, and the quotient is a torus. This torus, viewed as a sub-torus of a canonical toric quotient of $G(d_1, \mathbb{Q}(t))^0$, can be determined by methods specific to inverse logarithmic derivatives; cf. [5], [22], [1]. That determines $Aut(V/\mathbb{Q}(t)^a)$. At this point it is an easy matter to retrieve $Aut(V/\mathbb{Q}(t))$, and the Picard-Vessiot group. It is an inevitable characteristic of this method that it deals with a (positive-dimensional) torus T even when $Aut(V/\mathbb{Q}(t), C))$ involves no such torus (or is even finite); connected tori are treated in preference to their large finite subgroups.

In §V, we exploit the same ideas in order to prove a characteristic 0 function-field analog of a conjecture of Grothendieck's regarding specializations of linear differential equations modulo primes of the ground field.

2000 *Mathematics Subject Classification*: Primary 34A30; Secondary 03C07, 12H05, 12L05, 14D05.

Work carried out in part as a Prize Research Fellow for Clay Mathematics Institute, and partly supported by the Israel Science Foundation. Thanks to both.

The paper is in final form and no version of it will be published elsewhere.

Appendix B explains the theory of definable automorphism groups used in this paper (the liaison group of two definable sets). The initial goal was purely expository; it was a pleasant surprise to realize that the theorem, originally conceived under a blanket stability assumption, can be proved for any first order theory. It is presented in this way. Ziv Shami, in part in collaboration with Bradd Hart, motivated by simple theories, independently made a similar discovery (with some additional restrictions, cf. his forthcoming preprint).

The appendix also discusses the equivalence of the Picard-Vessiot group with the model-theoretic formulation.

This paper was conceived in Będlewo, in the course of the Banach Center meeting on differential Galois theory. To prepare for the meeting, I read Vessiot's superb survey [23]. On p. 160, Vessiot states: "F. Marotte [15] a donné une méthode pour déterminer le groupe de rationalité d'une équation linéaire donnée: il ramène cette détermination à la recherche des intégrales d'une certaine équation linéaire auxiliaire qui ont une dérivée logarithmique rationnelle." To my 20th century ears, this meant that Marotte gave a proof of the universal validity of his method. However, Michael Singer assured me that Marotte's thesis contains no general algorithm. Indeed, Vessiot continues surprisingly: "F. Marotte a appliqué sa méthode aux équations d'ordre 2, 3, et 4" and nowhere claims that the method is known to work in general.

Some of the 20th century sequel was explained to me by Michael Singer, over many lunch and coffee breaks during the meeting. There is no chance at all that this article would have existed without the Będlewo meeting and this friendly instruction; may I express my warmest thanks and appreciation to Singer and to the organizers of this most useful and delightful meeting, Teresa Crespo and Zbigniew Hajto. Many thanks also to Julia Hartmann and Anand Pillay for other explanations that I was sometimes slow to understand, and to the referee for his or her excellent comments.

I wrote the paper in order to learn, and assumed that all ideas in it will be known to the experts. But only after seeing [22] did I realize how very closely this was the case. In particular, the group G^t (the minimal normal subgroup of G such that G/G^t is toric-by-finite) occurs in [22] (it is denoted $\mathrm{Ker}XG^0$ there), and its centrality is made fully clear. The paper [5] solves the decision problem in the completely reducible case. The reader is referred to [5] and [22] for correct references and often, undoubtedly, better proofs of many statements made here.

Characteristic 0 differential algebra was the paradigmatic example for Robinson's "model theoretic foundations for algebra", and that framework remains very convenient. We will thus use a universal domain K for differential fields of characteristic 0 (a saturated model of DCF0, the model completion of the theory of differential fields of characteristic 0). Consider for instance the set of sums $f_1 + f_2$, where f_1 is a solution of a linear differential equation L_1 and f_2 of another equation L_2. This set is itself the set of solutions of an equation L; this follows quickly from Robinson's quantifier-elimination, as L is by definition given by a first-order formula, $L(y) = (\exists x_1, x_2)(L_1(x_1)\ \&\ L_2(x_2)\ \&\ y = x_1 + x_2)$. It is convenient not to need special proofs of the various such facts of this type that come up.

A good deal of later model theory illuminated the same arena: ω-stability, orthogonality and regular types, geometric stability. We will require none of this.

Here is the essential information required regarding definable automorphism groups: Let

$$k = \{x \in K : x' = 0\}.$$

By the quantifier-elimination, k is a "pure" algebraically closed field, in the sense that any definable subset of k in the structure K is already definable in k. Working in K, let V be a $k(t)$-definable k-space, $\dim_k V = n$. Any automorphism σ of K fixing $k(t)$ induces an automorphism of V, denoted $\sigma|V$. Let

$$G = \{\sigma|V : \sigma \in Aut(K/k(t))\} \leq GL(V)\}.$$

Then G is definable. It follows from the purity of k (and the fact that Zariski-constructible subgroups are Zariski-closed) that G is an algebraic subgroup of $GL(V)$. G acts on the set of bases of V^{bases} of V, regularly on each orbit P. The opposite group $Aut_G(P) = \{h \in Sym(P) : (\forall g \in G)\ hg = gh\}$ also acts regularly on P; this group is definably isomorphic to a group $H(k)$, H an algebraic group over K. One has $G = Aut_H(P)$, i.e. G is the group of automorphisms of P as an H-torsor.

Some very elementary facts about linear algebraic groups are used, but all facts about linear differential equations are proved from scratch. We hope this will benefit of the model theoretic reader (and writer) and not disturb too much those from differential Galois theory. Readers from both fields are referred to Marker's article in [14] for explanations of the other.

In Appendix A, I take the occasion to respond to a question voiced elegantly in the Będlewo meeting: how is it possible, at the beginning of the 21st century, to continue to use universal domains?

NOTATION. The word "differential" will always refer to *ordinary* differential equations, i.e. to a single derivation. K denotes a universal domain for differential fields of characteristic 0 (cf. Appendix A, or ignore this point and view K as an arbitrary, enlargeable differential field). k is the field of constants of K. (We basically use the letters k and C interchangeably; we use k when we have the internal field structure in mind.) The derivative of an element $x \in K$ is denoted x', but when we need a letter for the operator $x \mapsto x'$, we use the letter D. $t \in K$ is a fixed element with $t' = 1$; so $(k(t)^a, d/dt)$ is embedded into K. The equations we will consider will have parameters in $k(t)^a$.

In §III, II-F and V-A, we will work purely algebraically, and no derivation will intervene. Elsewhere, the words "A-definable" used without further qualification will always mean: defined by (a finite Boolean combination of) differential equations with coefficients in A.

We will write $H \leq G$ when H is a subgroup (or if appropriate subspace, or subfield) of G. $H \trianglelefteq G$ means that H is a normal subgroup of G. H^0 denotes the connected component (of the unit element) in the algebraic group H, i.e. the smallest closed subgroup of finite index in H. H^t denotes the kernel of all multiplicative characters of H^0 (over any extension field), i.e. the smallest closed normal subgroup of H^0 such that H^0/H^t is a multiplicative torus. It is the subgroup of H generated by the unipotent elements.

U^* is the dual of a finite-dimensional vector space U. U^{bases} denotes the set of bases of U (a Zariski open subset of U^n).

$N_d(U)$ is the family of Zariski closed subsets of U defined by a set of polynomials each of degree at most d. (A polynomial of degree d is a linear combination of products of at most d linear functionals on U.)

V will always denote a finite-dimensional definable k-vector space. It is a DCF0-definable k-subspace of a vector space $\underline{V}$ defined in ACF0 (though in §II-F, III we will not need to remember this information). $GL(V)$ is the group of units of the endomorphism ring $End_k(V)$; it admits a basis-dependent isomorphism with the matrix ring $GL_n(k)$.

If $V \leq \underline{V}$, then V is defined within $\underline{V}$ by a linear differential equation $x^{(n)} = \sum_{i<n} M_i x^{(i)}$, with $M_i \in End(\underline{V})$; conversely such an equation defines a finite-dimensional V.

G_a, G_m denote the additive and multiplicative group (schemes), respectively, so that $G_a(K)$ is the additive group of K.

A *substructure* of an algebraic structure (ring, group, vector space, ...) is a subset closed under the (ring, group, vector space ...) operations.

Within a differential field $(K, +, \cdot, D)$, Dlog will denote the definable map: $x \mapsto x'/x$; for a set $C \subset K$, we denote: $\mathrm{Dlog}(C) = \{\mathrm{Dlog}(c) : c \in C\}$.

I. Picard's algorithm.[1] We begin with a reading of some pages of Picard's Traité d'analyse (pp. 553-562 of the 3rd edition, [17]). I felt the need to fill in a couple of points in Picard's treatment; perhaps these points (P1.1, P1.2 below) are evident if one reads the pages before 553. We also bring out the generality of the result (corollaries 1.5, 1.6; these may have to do with work of Darboux cited in [23]).

LEMMA 1.0. *Assume V is defined over $L \supset k(t)$. There exists an injective definable k-vector space homomorphism $V \to K$, defined over a finite extension field of L. The image of V is contained in a $k(t)$-definable finite-dimensional k-vector subspace of K.*

Proof. If V is any DCF0-definable k-vector space, defined over L, V embeds into some ACF0-definable vector space $\underline{V}$ defined over L, definably in DCF0. $\underline{V}$ has a basis defined over L', a finite Galois extension of $k(t)$ containing L. [2]

We proceed to prove two claims using differential dimension and order; model theorists who prefer can use the ω and constant coefficient of the U-rank, or the Morley rank.

CLAIM 1. *L is Kolchin dense in K.*

Proof. L contains $k[t, \ldots, t^n]$, hence contains k-spaces of arbitrarily large dimension, and hence cannot have finite differential order. As any proper Zariski closed subset of K has finite differential order, the Zariski closure of L must equal K.

CLAIM 2. *A generic element of $\underline{V}^*$ is injective on V.*

[1] The main steps of the procedure can already be gleaned in Riemann's "Two general theorems on linear differential equations with algebraic coefficients" (dated 20 Feb. 1857 in the collected works) though the question considered there was somewhat different.

[2] (With thanks to the referee.) By [20], Chapter X, Proposition 3 one may take $L' = L$. As a result, V is L-definably isomorphic to a k-vector subspace of K. We will not require this fact here.

Proof. Let $d = \dim(\underline{V})$. Let

$$G = \{(u, v) : 0 \neq u \in V, v \in \underline{V}^*, v(u) = 0\}.$$

The left projection $\pi_1 : G \to \underline{V}$ maps G into V, a Kolchin closed set of differential dimension 0; while each fiber is a proper subspace of $\underline{V}$, hence has differential dimension $d-1$. Thus G has differential dimension $\leq d-1$, and hence so does $\pi_2(G)$; so a generic element of $\underline{V}^*$ is not in $\pi_2(G)$.

Using the two claims, an element $f \in \underline{V}^*$ can be found with coordinates in L', whose kernel meets V trivially. This proves the first statement. Now let $f_1, \ldots, f_n$ be the conjugates of f under the action of $Gal(L'/k(t))$; then $V' = \sum_{i=1}^{n} f_i(V)$ is $k(t)$-definable and finite-dimensional. ∎

PROPOSITION 1. *Let V be a finite-k-dimensional $k(t)$-definable Kolchin closed subspace of K^n. Let $l < \dim(V)$. One can effectively find a quantifier-free formula $\phi(v, u, w)$ in the language of differential fields (v a variable ranging over V, $u = (u_1, \ldots, u_l)$ ranging over the constants, w a single variable) such that if U is a $k(t)$-definable Kolchin closed linear subspace of V of dimension l, then for some $b_1, \ldots, b_l \in k$, $b = (b_1, \ldots, b_l)$, we have*

$$U = \{v \in V : \phi(v, b, t)\}.$$

REMARKS 1.1. (a) We paraphrase this as: "the t-definable subspaces of V are uniformly definable." But note that the proposition asserts not only that these subspaces can be defined by a formula of a fixed form with parameters in $k(t)$, but also that these parameters themselves have "bounded height" in the sense of function fields (i.e. they are rational functions of bounded degree of denominator and numerator).

In terms of foliations (on the total space of a vector bundle over a curve), the uniformity means that all integral curves lie in a bounded algebraic family of curves.

(b) It comes to the same thing to say that there is a finite number of formulas ϕ, rather than just one, capturing all $k(t)$-definable subspaces; and perhaps this is a more natural way of putting it. (The transition from a finite number of formulas to one is trivial, but contrived.)

(c) Let k_0 be an algebraically closed subfield of k. If V is $k_0(t)$-definable, then in the Proposition, one can take $b_i \in k_0$. This follows from an elementary submodel argument.

(d) As in Lemma 1.0, we may assume $V \subset K$.

(e) On the other hand, taking a prolongation, we may instead assume that V is defined by first-order formulas, $v' = Mv$ with M a matrix with entries in $k(t)$. If $V \subset \underline{V}$, this may be achieved by replacing $\underline{V}$ by $\underline{V}^{\dim V}$ and V by the image of V under the map $v \mapsto (v, v', \ldots, v^{\dim V - 1})$.

(f) The assumption $V \subset K^n$ can be dispensed with; see corollary 1.6 below.

(g) An equivalent formulation: Let $Gr_l(V)$ be the set of l-dimensional subspaces of V. It can also be viewed as a Kolchin closed set. The set of elements of $Gr_l(V)$ defined over $k(t)$ is a-priori a countable union of Kolchin constructible sets. The Proposition asserts that it is in fact a constructible set.

EXAMPLE 1.2. It is not the case that ϕ varies uniformly with V; when V moves in a definable family, ϕ need not do the same. Thus for instance if $V = \{(x_1, x_2) : tx_1' = nx_1,$

$x_2' = 0\}$, then

$$U = \{(x_1, x_2) \in V : x_1 = t^n x_2\}$$

is a t-definable subspace, whose evident definition $\phi(x_1, x_2, w)$ depends non-uniformly on n.

LEMMA 1.3. *Proposition 1 reduces to the case $l = 1$.*

Proof. We may assume V is defined by a first-order equation, $v' = Mv$ (1.1e). Thus the natural map $V \otimes_k K \mapsto \underline{V}$ is *injective*. (In fact V is Zariski dense in $\underline{V}$, and V^n is Zariski dense in $\underline{V}^n$; thus there exist K-linearly independent $v_1, \ldots, v_n \in V$.) It follows that $\Lambda^l V \mapsto \Lambda^l \underline{V}$ is injective too. $\Lambda^l \underline{V}$ can be identified with $\underline{V}' = \mathbb{G}_a^{\frac{n_0!}{l!(n_0-l)!}}$. The image V' of $\Lambda^l V$ in $\Lambda^l \underline{V}$ is a Kolchin closed linear subspace of $\underline{V}'$, of finite-dimension over the constants. The l-dimensional K-subspaces of $\underline{V}$ are in 1-1-correspondence with a certain definable set of 1-dimensional K-subspaces of $\underline{V}'$; the correspondence takes the space generated by $\{v_1, \ldots, v_l\}$ to the one generated by $v_1 \wedge \ldots \wedge v_l$. The same correspondence carries l-dimensional subspaces of V to 1-dimensional subspaces of V', in a $k(t)$-definable manner. Thus if the 1-dimensional $k(t)$-definable subspaces of V' are uniformly definable, then so are the l-dimensional $k(t)$-definable subspaces of V. ∎

COROLLARY 1.4. *Let V be a finite-k-dimensional $k(t)$-definable Kolchin closed subspace of K^n. The $k(t)$-definable elements of $N_d(V)$ are uniformly definable, in the sense of Proposition 1. In particular they form a Kolchin constructible set whose definition can be found effectively in a definition of V.*

Proof. By 1.1 (d), we may assume $V \subset K$. Modifying as in 1.1 (e), we can take instead $V \subset \underline{V}$, $\underline{V} = K^n$, and $V = \{v \in \underline{V} : v' = Mv\}$ for some matrix M over $k(t)$. Then the map $V \otimes_k K \to \underline{V}$ is an isomorphism. Thus every k-linear map on V extends to a K-linear map on $\underline{V}$. Let $V^* = \{T \in \underline{V}^* : (\forall v \in V) T(v) \in k\}$. Then V^* is a finite-dimensional k-subspace of $\underline{V}^*$, and is definably isomorphic to the k-dual space of V. Note that $\underline{V}^*$ has a $k(t)$-definable basis, the dual basis to that of $\underline{V}$. Thus Proposition 1 applies to V^*. Similarly comparing k- and K-symmetric powers, we see that Proposition 1 holds also for the space

$$H_d = \sum_{i=0}^{d} Sym^i(V^*)$$

of polynomials of degree $\leq d$ on V. Now make an element S of $N_d(V)$ correspond to the subspace $H_d(S)$ of elements of H_d vanishing on S; apply Proposition 1 to H_d. ∎

REMARK 1.5. If in 1.5, V is defined over $k_0(t)$, then so is the Kolchin constructible set of the conclusion (it is invariant under automorphisms preserving $k_0(t)$).

COROLLARY 1.6. *Let V be a finite-k-dimensional definable k-vector space, defined over a finite extension L_0 of $k(t)$. Let $l < \dim(V)$. There exists a quantifier-free formula $\phi(v, u)$ in the language of differential fields (v a variable ranging over V, $u = (u_1, \ldots, u_l)$) such that if U is an L_0-definable Kolchin closed linear subspace of V of dimension l, then for some $b_1, \ldots, b_l \in L_0$, $b = (b_1, \ldots, b_l)$, we have*

$$U = \{v \in V : \phi(v, b)\}.$$

Moreover the b_i can be taken to have bounded height, or equivalently to consist of a fixed generator of $L_0/k(t)$ together with t and elements of k.

Proof. By Lemma 1.0, over a finite Galois extension L of $k(t)$, there exist definable monomorphisms $f : V \to V'$, with V' a $k(t)$-definable finite-dimensional k-vector subspace of K. We first show that the L-definable l-dimensional subspaces of V' are uniformly definable. Let $d = [L : k(t)]$, $G = Aut(L/k(t))$. Pick $a \in L$ with $L = k(t, a)$. $a, a' \ldots, a^{(d)}$ are linearly dependent over $k(t)$, so there exists a nonzero linear differential operator with coefficients in $k(t)$ vanishing on a, hence a finite-dimensional $k(t)$-definable subspace E of K containing a (and thus also the conjugates Ga). Let $E_a \subset E^2$ be the subspace generated by $(1, a)$. If U is an l-dimensional subspace of V', defined over L, let $U_a = (U \times E_a) \subset K^3$, and let $\{U_i\}$ be the family of conjugates of U_a under G. Let $Z = Z(U) = \cup_i U_i$. Then $Z \in N_d(V' \times E)$. By 1.5, the $Z(U)$ are uniformly definable. From $Z(U)$ one can recover the family of d subspaces making it up as irreducible components. From this family and the element a, one finds the unique one of the form $U \times E_a$; and this gives the required U, in a uniform manner.

Thus there exists a fixed formula ϕ such that for any L-definable subspace U, for some $b = (b_1, \ldots, b_m) \in L$, U is defined by $\phi(v, b)$. Now consider an L_0-definable U. Let $G_1 = Aut(L/L_0)$. Then U is equally defined by $\phi(v, \sigma(b))$ for any $\sigma \in G_1$. Now the set Gb has size at most $[L : L_0]$, and is coded by a bounded tuple $e = (e_1, \ldots, e_m)$ of elements of L_0 (where m depends only on $[L : L_0]$). In other words for some formula $\rho(y, z)$ we have $y \in Gb$ iff $\rho(y, e)$. Thus U is defined by: $(\exists y)(\rho(y, e) \& \phi(v, y))$. This proves 1.6. ∎

Now for the proof of Proposition 1; by Lemma 1.3 we are reduced to the one-dimensional case. Now if U is a 1-dimensional k-space defined over $k(t)$, then u'/u has a fixed value b for nonzero $u \in U$; and $b \in k(t)$. So the 1-dimensional subspace is coded by b, and the problem becomes to show that b is a uniformly definable element of $k(t)$ (i.e. has bounded height).

This is the form in which Picard phrases the problem:

P Given a linear differential equation $L(x) = 0$ over $k(t)$, find all $h \in k(t)$ such that $L(x) = 0$ has a solution (in some differential extension field of $(k(t), d/dt)$ satisfying $x'/x = h$.

The diophantine sensitivity mentioned in 1.2 occurs already (and only) within a subalgorithm considered (justifiably) as evident by Picard:

LEMMA P1.1. *Given a linear differential equation $L(x) = 0$ over $k(t)$,*

$$\{f \in k[t] : \ L(f) = 0\}$$

is uniformly definable. In other words, the degree of a polynomial solution f is bounded. This bound is moreover computable from the coefficients of L.

Proof. Since L is homogeneous, we can take f to have the form $f = t^n + a_{n-1}t^{n-1} + \ldots$, and we need to bound n. Moreover we can take $L(x) = \sum c_i x^{(i)}$, with $c_i \in k[t]$. Separating the c_i into monomials and collecting terms differently, write $L(x) = \sum_{k=0}^{k_{max}} L_k(x)$, where

$$L_k(x) = \sum_{i+j=k} c_{ij} t^i x^{(j)}$$

and $c_{ij} \neq 0$ for some $i + j = k_{max}$. We obtain

$$L(f) = \left(\sum_{i+j=k_{max}} c_{ij} \frac{n!}{i!(n-i)!} t^{n+k_{max}} \right) + \text{lower terms in } t.$$

Thus

$$\sum_{i+j=k_{max}} c_{ij} \frac{n!}{i!(n-i)!} = 0.$$

With c_{ij} fixed, this can be viewed as a polynomial in n of degree $\leq k_{max}$. It has at most k_{max} solutions for n. ∎

One also needs:

LEMMA P1.2. *Let L be a given linear ODE over $k(t)$, defining a space V. Let $W = \{x'/x : x \in V, x \neq 0\}$. (So W is a $k(t)$-definable set of Morley rank (and differential order) $\dim(V) - 1$.) Let $\gamma \in k$, and fix a negative integer $-m$. Give $k((t-\gamma))$ the natural derivation; it is continuous on $k[[t-\gamma]]$ and extends d/dt. Let S be the set solutions of W in $k((t-\gamma))$ of the form*

$$s = c_{-m}(t-\gamma)^{-m} + c_{-(m-1)}(t-\gamma)^{-(m-1)} + \ldots + c_{-1}(t-\gamma)^{-1} + h$$

with $h \in k[[t-\gamma]]$. Then there exists an effectively computable finite set $F = F(L, m, \gamma)$ such that for any $s \in S$, we have $(c_{-m}, \ldots, c_{-1}) \in F$.

Proof. We may assume $\gamma = 0$. We use induction on m, thus supposing we have the algorithm for $m - 1$.

Claim: It suffices to prove this for c_{-m} alone.

For suppose this is done. Take any of the finitely many possible values c of c_{-m}; we need to determine the possible values of $c_{-(m-1)}, \ldots, c_{-1}$. Let $u \neq 0$ solve $u'/u = -ct^{-m}$. Replace V by $V' = Vu$. Then $W' = W - ct^{-m}$; and $S' = \{(s - ct^{-m}) : s \in S\}$. By the algorithm for $m - 1$, we know how to determine a finite set containing all possibilities for $c_{-(m-1)}, \ldots, c_{-1}$ where $c_{-(m-1)}t^{-(m-1)} + \ldots + c_{-1}t^{-1} + h \in S'$, some $h \in k[[t]]$; this solves our problem.

As for c_{-m}, we compute the equation of W. Let D denote the differentiation operator. V is defined by

$$D^n y + P_1 D^{n-1} y + \ldots + P_n y = 0$$

with $P_i \in k(t)$. We have $s = y'/y$ with $y \in V$. Writing S for the operator of multiplication by s, we have $Dy = Sy$, and inductively

$$D^{i+1} y = [(D + S)^i(s)]y.$$

Thus by the equation for $y \in V$, we have $[(D+S)^{n-1} + P_1(D+S)^{n-2} + \ldots + P_n](s)y = 0$ and so

$$[(D + S)^{n-1} + P_1(D + S)^{n-2} + \ldots + P_n](s) = 0.$$

The most negative exponent with nonzero coefficient of $(D + S)^{i-1}(s)$ is clearly that of t^{-im}. If $m \geq 2$, the coefficient is c_{-m}^i. If $-m = -1$, the coefficient is more complicated, but can be expressed as a polynomial in c_{-m} of the form ${c_{-m}}^i$+(lower terms in c_{-m}).

Let a_i, d_i be such that $P_i = d_i t^{a_i} + u_i$, with $u_i \in t^{a_i+1}k[[t]]$. Let ν be the least value taken by $a_i - im$, and let I be the set of indices i such that $a_i - im = \nu$. Let j be the maximal element of I. If $m \geq 2$, the coefficient of t^ν in the entire sum is

$$\sum_{i \in I} d_i {c_{-m}}^i.$$

If $m = 1$, it is more complicated, but still it is a polynomial in c_{-m} with leading term $d_j {c_{-m}}^j$. This gives a nonzero polynomial in c_{-m} of degree $j \leq n-1$; and the polynomial vanishes at c_{-m}. The set of roots of the polynomial is computable, and finite, and includes all possible values for c_{-m}.

With these in hand we can follow the argument in Traité d'analyse, proving Proposition 1 (with 1.1(d) assumed). Briefly, we consider solutions $y \in V$ with $y'/y \in \mathbb{Q}(t)$; we bound the poles of y'/y as in P1.2, and then find a finite set containing all possible polar parts of y'/y at poles of the equation itself; we write $y'/y = e + R$, where e is one of finitely many explicit possibilities, and R has distinct simple poles, with integer residues. We note that we can compute the equation for zV, where $z'/z = -e$; and that R is the logarithmic derivative of a polynomial solution of this auxiliary equation. See [17] for the full argument.

II-F. The finite part. Here, and in §III, we do not need to remember the differential structure. The underlying structure has the form $(k, V, \ldots)$, where k is an algebraically closed field and V is a vector space over k of fixed finite dimension. The ellipsis denotes possible additional sorts, that do not concern us; we do however assume that k is *fully embedded*, i.e. that in the full structure, every definable subset of k^n, possibly with parameters from $(k, V, \ldots)$, is a Zariski constructible set.

We let L be a substructure of $(k, V, \ldots)$. L is said to be *algebraically closed* (in the model-theoretic sense) if any *finite* subset of k,V or of another sort interpretable in this structure, defined over L, is contained in L.

A *torus* in $GL(V)$ is a subgroup T of $GL(V)$ that becomes isomorphic to ${\mathbb{G}_m}^n$, after fixing a basis of V and possibly extending the base field. A *character* of a definable subgroup H of $GL(V)$ is a definable homomorphism $f : T \to \mathbb{G}_m(k)$.

Remark 2F.1. In the application, k will be the field of constants of a differentially closed field K of characteristic 0, while V will be a definable k-space, solution set of a linear differential equation. In this case, elimination of imaginaries in K implies that it suffices to consider the home sort (elements of K); elimination of quantifiers implies that it suffices to consider sets defined by differential polynomials; and inspection shows that such definable sets are finite only when they are contained in the set of roots of an ordinary polynomial in $L[T]$. Thus a differential subfield L of a differentially closed field of characteristic 0 is algebraically closed model-theoretically iff $L = L^a$ field-theoretically.

Lemma 2F.2. *Let $H \leq GL_n$ be a linear algebraic group over an algebraically closed field, defined with parameters a. Given a definition H_a of H with parameters a, one can effectively find a definition F_a of $F = H^0$, the connected component of the identity in H.*

Moreover, one can effectively find a formula $\theta(x)$ such that $\theta(a)$, and such that whenever $\theta(b)$, $(H_b)^0 = F_b$.

Proof. This is in fact proved classically for any variety V: one can effectively and uniformly find a formula for the equivalence relation: "x, y lie in the same components of V" (cf. [7], [10] for model theoretic proofs and references). For our needs, one can also use the methods of (characteristic 0) linear groups. Sketch:

(1) Consider first the case that H is a commutative group consisting of semi-simple elements. Say $[H : H^0] = m$. The map $x \mapsto x^m$ maps H onto H^0; as $H^0 \simeq {\mathbb{G}_m}^l$, there exists a surjective homomorphism $g : H \to {\mathbb{G}_m}^l$. This last fact can be expressed by a first-order formula ϕ true of a; hence it holds for all a' with $\phi(a')$, and moreover the pair (m, ϕ) can be searched for, and found effectively (as it is guaranteed to exist). Now if $\phi(a')$ holds, then $H^0_{a'} = {H_{a'}}^m$ (the set of mth powers in $H_{a'}$).

(2) If $H = H_a$ is commutative, then $H^0 = H_u {H_t}^0$ where H_u, H_t are the unipotent and semi-simple parts, respectively.

(3) In general, $H^0 =< \cup_{g \in H} (C_H(C_H(g)))^0 >$, where $C_H(X) = \{h \in H : (\forall x \in X)\ hx = xh\}$. ∎

LEMMA 2F.3. *(a) Assume L is algebraically closed. Then $Aut(V/L, k)$ has no proper definable subgroups of finite index.*

(b) Let $H = \{g \in GL(V) : gR_i = R_i\}$, where $R_i \subset V^{m_i}$ is an L-definable relation. Then (given $L, V, R_1, \ldots, R_l$) one can effectively compute a finite extension L' of L, and $Q \subset V^{\dim(V)}$ defined over L', such that the subgroup of $GL(V)$ fixing Q is H^0.

Proof. (a) Follows from (b), since $Aut(V/L, k)$ must fix Q.

(b) Let P be an orbit of H on V^{bases}. If σ is an automorphism of the universal domain fixing L and k, then $\sigma(R_i) = R_i$, so $\sigma | V \in H$. Thus $\sigma(P) = P$. It follows that $P = P_c$ can be defined over L with parameters c from k. The set of c' such that $P_{c'}$ is a nonempty L-definable subset of k, being a constructible set, has a point c' rational over a finite extension L' of L. Let $P' = P_{c'}$.

Using 2F.2, identify H^0. The set of orbits of H^0 on P' is finite; each is therefore defined over a finite extension L''. Let Q be one of them. Then $H^0 = \{g \in GL(V) : gQ = Q\}$. ∎

LEMMA 2F.4. *Let $H = H^0$ be a definable subgroup of $GL(V)$, defined over a model-theoretically algebraically closed base set L. Then, though V may have no basis defined over L, every definable character of H is L-definable.*

Proof. The character group of V is countable; so the connected definable group $Aut(V/L, k)$ can only act on it trivially. (More explicitly: as H is L-definable, $Aut(V/L, k) \leq N_{GL(V)}(H)$. But the action of $N_{GL(V)}(H)$ on H/H^t factors through a finite group, by rigidity of this torus. So the connected group $Aut(V/L, k)$ acts trivially on H/H^t, hence on the characters.) ∎

II-T. The toric part. We return to the universal domain for differentially closed fields of characteristic 0. The main goal of this section is:

PROPOSITION 2. *Let V be a linear Kolchin closed set defined over $\mathbb{Q}(t)^a$. Let $H = H^0$ be a $\mathbb{Q}(t)^a$-definable subgroup of $GL(V)$, and assume $Aut(V/\mathbb{Q}(t)^a, C) \leq H$. Let $\bar{A}$ be the image of $Aut(V/\mathbb{Q}(t)^a, C)$ in H^0/H^t. Then $\bar{A}$ can be determined effectively.*

In a slightly different formulation, this is due to Singer [5], based on [16], [1]. See [22], Proposition 2.4. We repeat some of the proof here in order to set up the terminology.

LEMMA 2.1 (Kolchin). *Let $\underline{G}$ be an algebraic group defined over the differential field L_0. Assume $H^1(Gal(L_0^{alg}/L_0), \underline{G}(L_0{}^{alg})) = 0$ (e.g. this holds if $\underline{G} = \mathbb{G}_m$ or $\underline{G} = \mathbb{G}_a$ or $L_0 = L_0^a$).*

(i) Let there be given a (differentially) definable regular action of $G(K)$ on an affine Kolchin closed set P, defined over L_0. Then P is the trivial torsor, i.e. it has an L_0-rational point.

(ii) Let there be given a (differentially) definable regular action of $G(k)$ on an affine Kolchin closed set P, defined over L_0. Then P is L_0-isomorphic to an L_0-definable coset of $G(k)$ in $G(K)$.

(iii) In particular, if $G = \mathbb{G}_m$, P is L_0-definably isomorphic to $\{x : x'/x = e\}$, some $e \in L_0$.

Proof. (i) This is a famous theorem of Kolchin. (Sketch of proof: by taking prolongations, find Zariski-closed (G_1, P_1)—a group and a torsor—such that (G, P) are Kolchin closed, Zariski-dense in (G_1, P_1). P_1 is trivial, as can be seen by successively factoring from G_1 normal subgroups with trivial H^1. Factor out the unipotent "jet" part of G_1; this gives a map to (G_2, P_2), where G_2 is isomorphic to G, but also where P_2 is trivial, since P_1 is. But this quotient map is bijective on G, and thus on P.)

(ii) P induces an L_0-definable $G(K)$-torsor $P^* = P \times_H G(K)$. By (i) P^* is L_0-isomorphic to $G(K)$. Thus P is L_0-definably isomorphic to a $G(k)$-subtorsor of $G(K)$, i.e. to a coset.

(iii) This is the form of cosets of $\mathbb{G}_m(k)$ in $\mathbb{G}_m(K)$. ∎

LEMMA 2.2. *Let V, H be as in Proposition 2. Let $\chi : H \to \mathbb{G}_m(k)$ be an L-definable multiplicative character of H. Fix an H-orbit P of V^{bases}, defined over L. Then there exists an L-definable differential regular function γ on P such that* Dlog γ *takes a constant value e on P, $e \in L$, and*

$$\gamma \circ h = \chi(h)\gamma$$

for $h \in H$.

Proof. H acts regularly on P, and $\mathbb{G}_m(k)$ acts regularly on $P/Ker(\chi)$. By 2.1, $P/Ker(\chi)$ is differentially rationally isomorphic to $(\text{Dlog})^{-1}(e)$ for some $e \in L$. Let γ denote the composition

$$P \to (P/Ker(\chi)) \to (\text{Dlog})^{-1}(e).$$

The equation $\gamma \circ h = \chi(h)\gamma$ expresses the fact that we have morphisms of torsors. The fact that γ is everywhere defined on P (and not only a differentially rational function) follows from the transitivity of H on P, the regularity of χ and the functional equation. ∎

COROLLARY 2.2C. *Let V, H be as in Proposition 2. Let $\chi : H \to \mathbb{G}_m(k)^l$ be an L-definable surjective homomorphism. Fix an H-orbit P of V^{bases}, defined over L. Then there exist $e_1, \ldots, e_l \in L$, $Q_i = \{x : x'/x = e_i\}$, $Q = \prod_{i=1}^l Q_i$, and an L-definable morphism of differential algebraic varieties $\gamma : P \to Q$ such that*

$$\gamma \circ h = \chi(h)\gamma$$

for $h \in H$. Moreover, $\chi(Aut(V/L^a, C)) = Aut(Q/L^a, C)$.

Proof. The first part is merely 2.2, applied separately to each $\chi_i = pr_i \circ \chi$, pr_i the ith projection, and put together again. For the "moreover", we identified $Aut(Q/L^a, C)$ with a subgroup of $\mathbb{G}_m(k)^l$ in the obvious way. Let ϕ be an automorphism of the universal domain, over L. Then ϕ fixes γ, and so, being an automorphism,

$$\gamma \circ (\phi|P) = (\phi|Q) \circ \gamma.$$

Comparing this to the equation $\gamma \circ h = \chi(h)\gamma$, we see that if $h = \phi|V$ then $\phi|Q$ acts by multiplication by $\chi(h)$. This shows both that χ carries $Aut(V/L^a, C)$ to $Aut(Q/L^a, C)$, and that it does so surjectively. ∎

Note $\mathrm{Dlog}(L)$ is a $\mathbb{Q}$-subspace of $(L, +)$, if L is closed under roots. At all events we write: $rk\ \mathrm{Dlog}(L) = dim_{\mathbb{Q}} \mathbb{Q} \otimes \mathrm{Dlog}(L)$.

LEMMA 2.3. *Let $\mathbb{Q}^a(t) \leq L \leq \mathbb{Q}(t)^a$. Let $e_i \in L$, and*

$$P = \{(x_1, \ldots, x_n) : x_i'/x_i = e_i\}.$$

Let Δ be the group of characters χ of ${\mathbb{G}_m}^l$, $\chi(x_1, \ldots, x_n) = \prod x_i^{d_i}$, such that $\sum d_i e_i \in \mathrm{Dlog}(L)$. Then

$$Aut(P/L, C) = \Delta^* = \{a \in {\mathbb{G}_m}^l : \forall \chi \in \Delta.\ \chi(a) = 1\}.$$

Proof. It suffices to show the dual statement, that $\chi \in \Delta$ iff $\chi(Aut(P/L, C)) = 1$. Write $x = (x_1, \ldots, x_l)$, $\chi(x) = \prod {x_i}^{d_i}$. If $\chi \in \Delta$, $\mathrm{Dlog}\, \chi(x) = \sum d_i e_i = \mathrm{Dlog}\, f$ for some $f \in L$. So $\mathrm{Dlog}\, f^{-1}\chi(x) = 0$, hence $\chi(x) = cf^{-1}$ for some $c \in C$. So if if $\sigma \in Aut(P/L, C)$, $\sigma(x_i) = c_i x_i$, then $\chi(x) = \sigma(\chi(x)) = \chi(\sigma(x)) = \chi(c_1, \ldots, c_l)\chi(x)$. Thus $\chi(c_1, \ldots, c_l) = 1$.

Conversely, if $\chi(Aut(P/L, C)) = 1$, then by reversing the calculation we see that $\sigma(\chi(x)) = \chi(x)$ for each $\sigma \in Aut(P/L, C)$; so $\chi(x) \in L$. It follows that $\mathrm{Dlog}\, \chi(x) = \sum d_i e_i$, so $\sum d_i e_i \in \mathrm{Dlog}(L)$. Thus $\chi \in \Delta$. ∎

In the application of Lemma 2.3, we will not need to know $Aut(P/L, C)$, but only the connected component of the unit element of this group. (Finite quotients being dealt with separately.)

LEMMA 2.3^0. *In the situation of Lemma 2.3, let $\Delta^0 = \{a \in \mathbb{Z}^n : ma \in \Delta,\ some\ 0 \neq m \in \mathbb{N}\}$ be the relatively divisible hull of Δ in $\mathbb{Z}^n$. Then $Aut(P/L, C)^0 = (\Delta^0)^*$.*

Proof. Δ^0/Δ is a finitely generated torsion group, hence finite. Thus $\Delta^*/(\Delta^0)^*$ is finite, and we have to show that $(\Delta^0)^*$ is connected. If H is a closed subgroup of $(\Delta^0)^*$ of finite index, let χ be a character of ${\mathbb{G}_m}^l$ such that $\chi(H) = 1$. Then $\chi(\Delta^0)^*$ is finite, so some multiple of χ is trivial on $(\Delta^0)^*$, hence is in Δ^0; as Δ^0 is divisible, $\chi \in \Delta^0$. Thus

$$(\Delta^0)^* = \cap_{\chi \in \Delta^0} Ker(\chi) \subset \cap_{\chi(H)=1} Ker(\chi) = H.$$ ∎

We are thus led to the problem of determining $\mathrm{Dlog}(L)$, and more generally, given $e_1, \dots, e_l \in L$, of finding $\{(d_1, \dots, d_l) : \sum d_i e_i \in \mathrm{Dlog}(L)\}$. To state this geometrically, we view L as the function field of a (smooth, complete) curve X, and recall some standard notions regarding X.

Let F be the free Abelian group on generators X, $F_0 = \{\sum m_p p \in F : \sum m_p = 0\}$. Given $D \in F$, $D = \sum_{p \in X} m_p p$ (with $m_p = 0$ for all but finitely many $p \in X$), let $\Omega(D)$ be the space of all 1-forms on X with a pole of order at most m_p at each p. Then $\Omega(D)$ is a finite-dimensional k-space. Let Ω_{log} be the $\mathbb{Q}$-space of forms of the form df/f, $f \in k(C)^a$, and let $\Omega_{log}(D) = \Omega_{log} \cap \Omega(D)$. Define

$$res : \Omega(D) \to k \otimes_{\mathbb{Z}} F_0, \quad \omega \mapsto \sum_p res_p(\omega) p.$$

Given $f \in k(X)$, let $div(f)$ be the divisor of f. Let $div(k(X))$ be the group of all divisors of functions in $k(X)$. The Jacobian J of X can be identified with $Pic_0(X) = F_0/div(k(X))$; let $ab : F_0 \to J$ be the natural map, and extend it to $ab : (\mathbb{Q} \otimes_{\mathbb{Z}} F_0) \to \mathbb{Q} \otimes_{\mathbb{Z}} J$.

LEMMA 2.4. *Given 1-forms $\omega_1, \dots, \omega_l$ on a curve X over k, the group*

$$\left\{ d = (d_1, \dots, d_l) \in \mathbb{Q}^l : (\exists f \in k(X)^a) \sum d_i \omega_i = df/f \right\}$$

can be effectively determined.

Proof. We refer the reader to the proof of Proposition 2.4 of [22] (but I think one should read "no nonzero residues" in place of "holomorphic" there). An outline of that proof follows. An alternative, without explicit use of residues, is possible along the lines of 5A.12.

Fix D such that each $\omega_i \in \Omega(D)$. Define an additive map $v : \mathbb{Z}^l \to \Omega(D)$ by $v(n) = n \cdot \omega = \sum n_i \omega_i$. The problem is to determine $v^{-1}(\Omega_{log}(D))$.

1. Every element of Ω_{log} has rational residues. Determine $A_1 = v^{-1} res^{-1}(\mathbb{Q} \otimes_{\mathbb{Z}} F_0)$. So $v^{-1}(\Omega_{log}(D)) \subset A_1$.

2. Let A_2 be the kernel of $(ab \circ res \circ v)|A_1$. As $res(df/f) = div(f)$, $ab \circ res$ vanishes on Ω_{log}. Thus $v^{-1}(\Omega_{log}(D)) \subset A_2$.

To determine A_2 is to find a basis for the linear relations among the images of the generators of A_1, holding in J. Here [16] or [1] are called upon to show that this is effective.

Here one could also use methods analogous to those of 5A.8(3), presumably less efficient, but softer in that they avoid use of transcendence methods.

3. For each $g \in A_2$, $res(v(g)) = (f_g)$ for some rational function g; $g \mapsto dlog(f_g)$ is a well-defined homomorphism $v' : \mathbb{Z}^l \to \Omega(D)$. Let $v'' = v - v'$. Then $v(g) \in \Omega_{log}(D)$ iff $v''(g) \in \Omega_{log}(D)$ iff $v''(g) = 0$ (the latter, because $v''(g)$ has no nonzero residues, while $dlog(f)$ always has nonzero residues unless it is zero). So it remains to find $ker(v'')$; this can be done by determining v' on a set of generators.

Proof of Proposition 2. Find a finite extension L of $\mathbb{Q}(t)$ with V, H defined over L, and also with some H-orbit $P \subset V^{bases}$ defined over L. The latter is possible by (b) of the proof of Lemma 2F.3. Enlarge L a bit further so as to find an L-definable isomorphism $\chi : H/H^t \to \mathbb{G}_m(k)^l$ for some l (cf. 2F.4). Find $\gamma : P \to Q$ as in Corollary 2.2C. Since

P, χ, γ, Q etc. are known to exist and can be recognized effectively, they can be found effectively. (The proof provides a better algorithm than this general reasoning.) As χ is an isomorphism, it suffices to find the image of $Aut(V/\mathbb{Q}(t)^a, C)$ under χ. By 2.2C, this is $Aut(Q/\mathbb{Q}(t)^a, C)$. Lemmas 2.3^0 and 2.4 conclude the argument. ∎

III. Uniformly definable subgroups of linear algebraic groups. The framework is that of II-F; a structure $(k, V, \ldots)$, k an algebraically closed field, V is a k-vector space of fixed finite dimension. After adding parameters for a basis of V, this becomes (bi-interpretable with) the theory of k. While the collection of 0-definable sets changes if one adds parameters for a basis, the collection of definable families of definable sets does not really change (each is cofinal in the other), so where only the question of uniformity of a family is concerned, we will feel free to work with GL_n rather than $GL(V)$. However this freedom in the proofs does not extend to the statements; we may require 3.8 below in cases that V does not have a rational basis.

Most of what we do uses only finite Morley rank, and undoubtedly with more information the description can be improved. (The reference to Morley rank here extends the generality of some of the statements, but is mostly due to habit; restricting to algebraic groups, one can equally well read "dimension".)

DEFINITION. Let $\phi(x, y)$ be a formula such that for any b, $\phi(x, b)$ defines a subgroup of $GL(V)$. The family$\mathcal{F}$ of subgroups defined in this way is called a *uniformly definable family of subgroups* (via the formula ϕ).

LEMMA 3.1. *Let $\mathcal{F}$ be a uniformly definable family of subgroups of $GL(V)$. Then so is:*

(a) The family $\mathcal{F}_\cap$ of all intersections of (finitely many) elements of $\mathcal{F}$.

(b) The family $\mathcal{F}^0$ of connected components of the unit element of groups in $\mathcal{F}$.

In fact, the family of pairs of groups

$$\{(M, M^0) : M \in \mathcal{F}\}$$

is also uniformly definable.

(c) The family of subgroups generated by a (finite) set of elements of $\mathcal{F}^0$.

In each of these cases, the passage from a definition of $\mathcal{F}$ to that of the new family is effective.

Proof. (a) is valid for stable groups; it is called the Baldwin-Saxl lemma. The point is that for some integer M, any intersection of elements of $\mathcal{F}$ is an intersection of at most M of them. To give an algebraic proof, and to explain how to compute M, let $V \subset \mathbb{A}^n$ be any algebraic subset of N-dimensional affine space, and let $\{W_c : c\}$ be any uniformly definable family of Zariski closed subsets of V. Then each W_c is the zero set of an ideal I_c of the polynomial ring in N variables; and by uniformity, it is generated by a set S_c of polynomials of bounded total degree d (this degree can be read off of a quantifier-free definition of W). Now the space $P(d, N)$ of polynomials of degree at most d in N variables has some finite dimension M. Clearly the union of any set of sets S_c generates the same

subspace as a subset of M of them; hence also the same ideal. Thus the intersection of any collection of the sets W_c is also the intersection of M of them.

(b) This is Lemma 2F.2.

(c) is a case of the indecomposability theorem; cf. e.g. [18] for Zilber's proof for groups of finite Morley rank, or [12] for a proof for algebraic groups. The group generated by any number of elements of $\mathcal{F}^0$ is already generated by at most n^2 of them, and in fact has the form AA^{-1}, $A = A_1A_2 \dots A_m$ where $m \leq n^2$ and each $A_i \in \mathcal{F}^0$. ∎

NOTATION. Let $\mathcal{F}$ be a uniformly definable family of subgroups of $GL(V)$. If H is any Zariski closed subset of $GL(V)$, let $H_{\mathcal{F}}$ be the intersection of all $G \in \mathcal{F}$ with $H \subset G$.

EXAMPLE 3.2. (a) Let $G = GL(V)$ (or any stable group). Let $C_G(A)$ be the centralizer in G of a set A. Then $\mathcal{F}_z = \{C_G(A) : A\}$ is a uniformly definable family of subgroups of G. More generally, if $\mathcal{F}$ is a uniformly definable family of subgroups, then so is

$$\{C_F(Y) : F \in \mathcal{F}, Y \text{ an arbitrary subset of } G\}.$$

(b) Let G be an algebraic group over k, $char(k) = 0$. There exists a uniformly definable family $\mathcal{F}_{ad}$ such that for any connected subgroup A of G, $N_G(A) \in \mathcal{F}_{ad}$.

Proof of (b). Consider the adjoint action of G on the Lie algebra. $N_G(A)$ is the subgroup stabilizing the Lie algebra of A. In particular it is the stabilizer of a subspace; this is a uniformly definable family.

(c-1) The family of maximal connected Abelian subgroups (and of maximal Abelian subgroups) of a given group G is uniformly definable.

Proof. If A is a maximal Abelian subgroup, then $A = C_G(C_G(A))$, so A is an intersection of centralizers of single elements. Thus A lies inside the uniformly definable family $\mathcal{F}_z$ of 3.2(a). Moreover A is maximal Abelian iff it is a maximal Abelian element of $\mathcal{F}_z$. The latter is a definable condition, so it cuts out a uniformly definable subfamily of $\mathcal{F}_z$. The connected case follows by 3.1(c).

(c-2) If A varies uniformly among connected Abelian subgroups of G, then so does the semi-simple part of A, $T(A)$.

Proof. $T(A)$ is the set of semi-simple elements of A.

The family of all tori (or even, all copies of $\mathbb{G}_m$ within ${\mathbb{G}_m}^2$) is not uniformly definable. However:

(c-3) The family $\mathcal{F}_{mt}(G)$ of maximal tori of G is uniformly definable. So is the family $\mathcal{F}_{imt}(G)$ of intersections of maximal tori of G. If G itself moves in a uniformly definable family, then these families are definable uniformly in a parameter for G.

Proof. If $H \in \mathcal{F}_{mt}(G)$, then $H = T(A)$ where A is a maximal connected Abelian subgroup of G; so (c-1,c-2) give a formula for $\mathcal{F}_{mt}(G)$. By 3.1(a), $\mathcal{F}_{imt}(G)$ is also uniformly definable.

(c-4) More generally, if $\mathcal{F}_1, \mathcal{F}_2$ are uniformly definable, then so is $\mathcal{F}_{mt:\mathcal{F}_1/\mathcal{F}_2}$ defined as:

$$\{H : (\exists H_1 \in \mathcal{F}_1, H_2 \in \mathcal{F}_2)(H_1 \trianglelefteq H_2, H_1 \leq H \leq H_2, H/H_1 \in \mathcal{F}_{mt}(H_2/H_1)\}.$$

Proof. Write the formula for $\mathcal{F}_{mt}(H_1/H_2)$, pull back to H_1, to get a formula for

$$\{H : H_1 \trianglelefteq H_2, H_1 \leq H \leq H_2, H/H_1 \in \mathcal{F}_{mt}(H_2/H_1)\}.$$

Quantify existentially over $H_1 \in \mathcal{F}_1$, $H_2 \in \mathcal{F}_2$ to get the required formula.

(d) The family of copies of the additive group $\mathbb{G}_a$ within $GL(V)$ is uniformly definable. (Any such subgroup is the image of a homomorphism $\mathbb{G}_a \to GL(V)$ of the form $t \mapsto exp(tM) = 1 + tM + \ldots + \frac{1}{(n-1)!}t^{n-1}M^{n-1}$: for $t \in \mathbb{G}_a$, with $M \in End(V)$ nilpotent, $M^n = 0$ where $n = \dim(V)$.)

Remark. By 3.1(b) and (d), the family $\mathcal{F}_{up}$ of all subgroups generated by unipotents is uniformly definable. This family is large in the sense that for any connected definable subgroup H of $GL(V)$, there exists H' in the family with $H' \subset H$ and H/H' a torus. A toric "error" is unavoidable in view of the negative part of (b). We would like to approximate H from above in this sense, too. Here is proof valid in any connected group G of finite Morley rank (and perhaps also giving a better algorithm). In the application, take $\mathcal{F}_{ad}$ as given by 3.2(b), so that H can be any connected subgroup.

Lemma 3.5. *Let $\mathcal{F}_2$ be a uniformly definable family of subgroups of G. There exists a uniformly definable family $\mathcal{F}$ of subgroups of G, such that for any definable $H \leq G$, if $H \trianglelefteq K$ for some connected $K \in \mathcal{F}_2$, then there exist $F, F' \in \mathcal{F}$, $F, F' \trianglelefteq K$, with $F \leq H \leq F'$, and F'/F Abelian.*

Proof. Let $H \trianglelefteq K$, $K \in \mathcal{F}_2$ connected. Let F be a subgroup of H of maximal Morley rank, generated by classes of the form $[a, K]$, $a \in H$. By Zilber's indecomposability theorem (or the indecomposability theorem for algebraic groups), F is generated in $\leq 2\dim(G)$ steps by the elements of $\leq \dim(G)$ such classes. So it is a member of a uniformly definable family $\mathcal{F}_1$ (independent of H).

Clearly $F \trianglelefteq K$. Moreover, H/F is commutative (for any $a \in H$, $[a, H] \subset F$, so the conjugacy class a^H has a single element modulo F). Within K/F, let F'/F be the double centralizer of H/F. Then F'/F is commutative, and uniformly definable by 3.2(a). ∎

Lemma 3.5b. *Let $\mathcal{F}$ be a uniformly definable family of subgroups of GL_n, and let*

$$I_0(n, \mathcal{F}) = \max\{[M : M^0] : M = T \cap G, G \in \mathcal{F}, T \in \mathcal{F}_{imt}(GL_n)\}.$$

Then $I_0(n, \mathcal{F})$ is finite, and can be bounded effectively given a definition of $\mathcal{F}$. In particular, one can explicitly bound

$$I_0(n) = \max\{[M : M^0] : M \in \mathcal{F}_{imt}(GL_n)\}.$$

Proof. The family of intersections of G with maximal tori is uniformly definable; by 3.1(b) the family of pairs (M, M^0) is uniformly definable; hence the family of numbers $[M : M^0]$ is uniformly definable, so it must be bounded, with a computable bound. ∎

Lemma 3.5c. *Actually $I_0(n) = 1$.*

Proof. View $G = GL_n$ as a Zariski open subset of M_n, the linear space of $n \times n$ matrices. The standard maximal torus D is the group of diagonal matrices; it has the form $G \cap H$ for a certain linear subspace H of M_n. Hence any conjugate of D has the same description. As the intersection of linear subspaces is a linear space, any intersection

of maximal tori is a linear space intersected with GL_n. Being a Zariski open subset of a linear space, it is irreducible. ∎

Let $J(n)$ be a Jordan bound (cf. [21]), so that every finite subgroup of GL_n contains a normal Abelian group of index at most $J(n)$.

LEMMA 3.6a. *There exists a computable integer $I_1(n)$ with the following property. Let H be a finite subgroup of GL_n. Then there exists $M \in \mathcal{F}_{imt}(GL_n)$ normalized by H, and with*

$$[H : H \cap M^0] \leq I_1(n, \mathcal{F}).$$

(Actually $I_1(n) = J(n)$.)

Proof. Let H be a finite subgroup of GL_n. By definition of $J(n)$, there exists $A \trianglelefteq H$, A Abelian, $[H : A] \leq J(n)$.

A finite Abelian subgroup of GL_n is diagonalizable; so there exists a maximal torus T of GL_n containing A. Let M be the intersection of all such maximal tori of GL_n. Note that H normalizes M, hence also M^0. Also $A \leq M$. Now $[M : M^0] \leq I_0(n)$. So $[A : A \cap M^0] \leq I_0(n)$, and thus $[H : H \cap M^0] \leq J(n)I_0(n)$. ∎

LEMMA 3.6d. *There exists a computable integer $I_2(n)$, and a computable, uniformly definable family $\mathcal{F}$ of subgroups of GL_n, with the following property.*

Let H be any Zariski closed subgroup of GL_n. Then there exists $F \in \mathcal{F}$ such that

(i) $H^0 \leq F$.
(ii) H normalizes F; so $F \trianglelefteq HF \leq GL_n$.
(iii) $[H : H \cap F] = [HF : F] \leq I_2(n)$.
(iv) Every unipotent element of F lies in H^0.

REMARK 3.6e. We may insist in 3.6d that the groups in $\mathcal{F}$ be connected; this may be achieved by replacing $\mathcal{F}$ by $\mathcal{F}^0$, and I_2 by $I_2 \cdot \max\{[F : F^0] : F \in \mathcal{F}\}$ (3.1(b)).

Proof of 3.6d. Lemma 3.6a proves this for finite groups H (with $\mathcal{F} = (\mathcal{F}_{imt})^0$, $I_2 = I_1$).

Consider next the case of subgroups $H \leq GL_n$ such that H^0 is a torus. Let $M = (H^0)_{\mathcal{F}_{imt}}$, the intersection of all maximal tori of GL_n containing H^0. M is clearly normalized by H.

Let $G = G_{M^0} = N_{GL_n}(M^0)$, and let

$$\tau = \tau_{M^0} : G \to GL_{n^*}$$

be a homomorphism of algebraic groups with kernel M^0 (cf. 3.9). As $H^0 \leq M^0$, $\tau(H)$ is a finite subgroup of GL_{n^*}. By the finite case just considered, we have $\tau(H) \leq F^*$ for some $F^* \in \mathcal{F}^0_{imt}(GL_{n^*})$, and (i)-(iii) hold for $\tau(H), F^*$ (with $I_2(n) = I_1(n^*)$). Let $F = \tau^{-1}(F^*)$. Then (i)-(iii) follow by the homomorphism theorems for groups. Moreover, if $c \in F$ is unipotent, then so is $\tau(c) \in F^*$; but F^* is contained in a torus, so $\tau(c) = 1$; thus $c \in ker(\tau) = M^0 \subset M$. Now M too is contained in a torus, so $c = 1$.

Thus the lemma holds in case H^0 is toric, with $I_2 = I_1(n^*)$ and

$$\mathcal{F} = \{{\tau_{M^0}}^{-1}(F^*) : M \in \mathcal{F}_{imt}(GL_n), F^* \in (\mathcal{F}_{imt})^0(GL_{n^*})\}.$$

For the general case, let $U = H^t$ be the subgroup of H^0 generated by the unipotent elements of H^0. Let $G = N_{GL_n}(U)$. Clearly $H \leq G$. U, G are restricted to move in the uniformly definable families, $\mathcal{F}_{up}$, $\mathcal{F}_{ad}$. So G/U moves in a uniformly definable family $\mathcal{F}'$ of subgroups of $GL_{n'}$ for some fixed, computable n' (cf. 3.9); n' and $\mathcal{F}'$ are defined independently of H. Let

$$\mu = \mu_U : G \to GL_{n'}$$

be a homomorphism of algebraic groups with kernel U. Then $\mu(H)^0$ is a torus. Proceed as above to pull back a solution for $\mu(H)$ to a solution for H. ∎

COROLLARY 3.7. *There exists a computable, uniformly definable family $\mathcal{F}$ of subgroups of GL_n, with the following property. Let H be any Zariski closed subgroup of GL_n. Then there exists $M \in \mathcal{F}$ such that $H \leq M$, and every unipotent element of M lies in H^0.*

Proof. Let $\mathcal{F}_0$ be the family of 3.6d, and

$$\mathcal{F} = \{M : (\exists F \in \mathcal{F}_0)\, F \trianglelefteq M,\ [M : F] \leq I_2(n)\}.$$

Any element of $\mathcal{F}$ is the union of at most $I_2(n)$ cosets of an element of $\mathcal{F}_0$; so $\mathcal{F}$ is uniformly definable by the obvious explicit formula. If H is a Zariski closed subgroup of GL_n, let $F \in \mathcal{F}_0$ be as in 3.6(d); let $M = FH$; then $H \leq M$. Every unipotent element of M lies in $M^0 = F^0$, hence in H^0. ∎

Invariants of uniformly definable groups

NOTATION. Given $n = \dim(V), k, d$, let $\mathcal{F}_{V,k,d}$ be the family of subgroups $H \leq GL(V)$ of the form

$$H(u) = \{g \in GL(V) : gu = u\}$$

with $u \in N_d(V^k)$ (and $GL(V)$ acting naturally on this space).

LEMMA 3.8. *(i) $\mathcal{F}_{V,k,d}$ is a uniformly definable family of subgroups of $GL(V)$.*

(ii) If $\mathcal{F}$ is any uniformly definable family of subgroups of $GL(V)$, then $\mathcal{F} \subset \mathcal{F}_{V,n,d}$ for some d.

(iii) Given a formula ϕ defining $\mathcal{F}$, the integer d in (ii) can be computed effectively (and an explicit ending time can be given for the algorithm).

Proof. (i) is clear as $\mathcal{F}_{V,k,d}$ is by definition given by a single formula, with parameter varying in $N_d(V^k)$.

ii,iii) Let $V^{bases} \subset V^n$ be the set of bases of V. Let H_v be a typical element of $\mathcal{F}$, and let $H_v z$ be a typical orbit of an element of V^{bases}. Find d such that (for any such H_v) the Zariski closure $\overline{H_v z}$ of $H_v z$ is cut out by polynomials of degree $\leq d$. If $g \in GL(V)$ fixes $\overline{H_v z}$, then $gH_v z \cap H_v z \neq \emptyset$; say $ghz = h'z = h'h^{-1}(hz)$, $h, h' \in H_v$. As hz is a basis for V, $g = h'h^{-1}$, so $g \in H_v$. Thus H_v is the subgroup fixing $\overline{H_v z}$, an element of $N_d V^n$. ∎

LEMMA 3.9. *Let $\mathcal{F}$, $\mathcal{F}'$ be uniformly definable families of subgroups of GL_n. One can compute n^* such that if $G \in \mathcal{F}$, $N \in \mathcal{F}'$, and $N \trianglelefteq G$, then there exists an (equally uniform, and computable) embedding of G/N in GL_N.*

Proof. By compactness and Chevalley's theorem. Theoretical computability is automatic from the existence of n^* and the embedding (search for them). An explicit algorithm

is provided by the standard proof of Chevalley's theorem. (As in 3.8, find d such that $N \in \mathcal{F}_{V,n,d}$ (where $GL_n = GL(V)$). G acts on a Grassmannian P, in such a way that N is the stabilizer of a point p. Thus G/N acts on T_pP and more generally on the higher jet spaces J_p^m. Take m larger than the maximal order of tangency between the graph of the action of two elements of G/N on P^2 at p; then the action of G/N on J_p^m is a faithful linear action.) ∎

IV. Computing Galois groups. First, a lemma to show the equivalence of two formulations of the problem. Actually we will directly solve the harder of the two, so the lemma will not be used, but it seems good to know that the equivalence is true on "soft" grounds.

LEMMA 4.0. *Assume we are given an algorithm (A) that given a linear differential equation E over L, and given a group G, decides whether or not G is the Galois group of E. Then one can find an algorithm (A') that inputs E and outputs the equations for the correct Galois group of E.*

Proof. The algorithm (A') proceeds as follows: Assume E defines X, a k-space of dimension n.

(1) Let $l = 1$; let $G_1 = GL(V)$.

(2) Ask (A): is G_l the Galois group? If the answer is YES, output G.

(3) Otherwise, search for a $\mathbb{Q}(t)$-definable subset S of E^n, that is not G-invariant. As G inductively contains the Galois group, but is not the Galois group, there must be such an invariant; eventually it will be found. Let G_{l+1} be the subgroup of G_l leaving S invariant; return to (2) with $l \mapsto l + 1$.

(4) Steps (2-3) cannot repeat forever, since otherwise the G_l would contradict the Noetherianity of the algebraic variety $GL(n)$.

ALGORITHM B. Given a linear Kolchin closed V defined over $\mathbb{Q}(t)$, $n = \dim(V)$:

(a) Using 3.8, determine $d = d(n)$ such that $\mathcal{F} = \mathcal{F}_{V,n,d}$ enjoys the property of Corollary 3.7.

(b) Find the subgroup H of $GL(V)$ fixing all $k(t)$-definable elements of $N_d(V^n)$. (By corollary 1.5, these elements come in finitely many uniformly definable families, with constant parameters; given these definable families, we immediately obtain a first-order definition of H, as the group fixing all elements of these families.)

(c) Using Lemma 2F.3, compute a finite extension L of $\mathbb{Q}(t)$, and finitely many relations S_j on V defined over L, such that the subgroup of $GL(V)$ fixing the S_j is H^0.

(d) Applying Proposition 2 to H^0, compute the image $\bar{A}$ of $Aut(V/\mathbb{Q}(t)^a, C)$ in H^0/H^t.

(e) Declare that $Aut(V/\mathbb{Q}(t)^a, C)$ is the pullback A' of $\bar{A}$ to H^0 (i.e. the group A' with $H^t \leq A'$ and $A'/H^t = \bar{A}$).

PROPOSITION 4.1. *Algorithm B works correctly.*

Proof. Let $A = Aut(V/C, \mathbb{Q}(t))$. By 2F.3(a), $A^0 = Aut(V/C, \mathbb{Q}(t)^a)$. By (a),(b) we have $H = A_{\mathcal{F}}$; by 3.7, every unipotent element of H lies in A^0. Thus $H^t \leq A^0$. By Proposition 2, $A^0/H^t = \bar{A}$. Thus $A^0 = A'$. ∎

REMARK 4.2. The algorithm provides invariants for $Aut(V/C, \mathbb{Q}(t)^a)$, i.e. a finite extension L of $\mathbb{Q}(t)$; some elements of $H_{V,n,d}(V)$; and in addition finitely many rational functions of the form $\prod_{i=1}^{l} {g_i}^{d_i}$; such that $Aut(V/C, \mathbb{Q}(t)^a)$ is precisely the group fixing all these.

ALGORITHM C. To determine $Aut(V/k(t))$.

Find a Galois extension L of $k(t)$ as in Algorithm B, and n-ary relations $R_1, \ldots, R_\nu$ on V defined over L, such that $Aut(V/k(t)^a) = Fix(R_1, \ldots, R_\nu)$. Take the set $\{R_i : i \leq \nu\}$ to be $Aut(L/k(t))$-invariant; for $\sigma \in Aut(L/k(t))$, let ${R_i}^\sigma$ denote the σ-conjugate of R_i. This finite group action is computable.

Let

$$G = \{g \in GL(V) : (\exists \sigma \in Aut(L/k(t))) \bigwedge_i ({R_i}^\sigma(gv_1, \ldots, gv_\nu)) \equiv R_i(v_1, \ldots, v_\nu)\}.$$

Then $G = Aut(V/k(t)$.

Proof. Clearly $Aut(V/k(t)) \leq G$, and $Fix(R_1, \ldots, R_\nu) = Aut(V/k(t)^a) \trianglelefteq G$. If $g \in G$, then for some $\sigma \in Aut(L/k(t))$, $R_i(v) \equiv {R_i}^\sigma(gv)$. As σ fixes $k^a = k = C(k(t))$, it extends to an automorphism over C, in particular it is compatible with some $s \in Aut(V/C, k(t))$. Now for each i, ${R_i}^\sigma(sv) \equiv R_i(v) \equiv {R_i}^\sigma(gv)$ so $R_j(g^{-1}su) \equiv R_j(u)$. Thus $g^{-1}s \in Fix(R_\nu)$, so $g^{-1}s \in Aut(V/k(t)^a)$. Thus $g \in Aut(V/C, k(t))$. ∎

REMARK 4.3. In the notation of Theorem B.1 (appendix B), Algorithm C identifies the differential Galois group G. There is no difficulty then to effectively find P and hence the opposite group H. It is H that is usually referred to as the Picard-Vessiot group.

REMARK 4.4. Our presentation focused on obtaining a general recursive algorithm. But at each step, the existence of a primitive recursive algorithm was also pointed out (or in the toric case, referred to). We made no attempt to compute the implied time bounds, but would guess that none require more than doubly exponential time.

REMARK 4.5. For simplicity of notation, we assumed the equation defined over $\mathbb{Q}(t)$. The same proofs would work for $k_0(t)$, k_0 any effectively presented field of constants.

V. A function field analog of Grothendieck's conjecture. Grothendieck's conjecture concerns the reduction to $\mathbb{F}_p$ of certain foliations over $\mathbb{Q}$ (corresponding to linear differential equations over $\mathbb{Q}(t)$). We prove here the natural analog in equal characteristic 0. We do not know whether it has been considered before.

We show that if V is a linear differential equation over $(\mathbb{Q}^a(s,t), d/dt)$, and for almost places p of $\mathbb{Q}^a(s)$, the reduced equation V_p has a basis of algebraic solutions, then so does V. Moreover, the Galois group of V specializes precisely to the Galois group of V_p, for many p. The proof follows closely that of Lemma 4.1. In effect, we use the algorithm of Lemma 4.1 for both V and V_p. Most of the calculations involved are first-order in the theory of algebraically closed fields; these go the same way for almost all p. Only two

procedures involve rationality questions on the coefficients: the toric case, and the case of polynomial solutions. We show that these too go the same way for many (though not almost all) p.

V-A. Preliminaries. For the moment, no derivations intervene.

Notions of largeness. Let F be a field of characteristic 0, $F \subset D \subset L$. Assume D is a finitely generated F -algebra. For any F-algebra L', let $Hom_F(D, L')$ be the set of L'-valued points of Spec D, i.e. of F-algebra homomorphisms $D \to L'$.

We consider four notions of basic open subsets of Spec D. The first is Zariski: a basic Zariski open has the form $\{p : a \notin p\}$, where $a \in D, a \neq 0$. Next, A *basic ad-open subset* of Spec D has the form $\{p : p \cap H = (0)\}$, where H is a finitely generated subgroup of $(D, +)$. More generally, let G be a commutative algebraic group scheme over $D[a^{-1}]$ (some $a \in D, a \neq 0$). Let Γ be a finitely generated subgroup of $G(D)$. Let $W(G, \Gamma)$ be the set of primes p of D such that the induced map $G(D) \to G_p(D_p)$ is injective on Γ. A set of the form $W(G, \Gamma)$ will be called a *basic gr-open subset* of Spec D. If G is restricted to be semi-Abelian, $W(G, \Gamma)$ will be called a *basic sa-open subset* of Spec D.

The intersection of two basic open sets of the same type clearly contains another basic open set. We will see below (5A.10) that no basic open set of any type is empty. A set containing a basic open set of one of the types above will be called *(Zar,ad,sa,gr)-large.* The complement of a large set will be called small.

A set Y of F-algebra homomorphisms on D will be called (Zar,ad,sa,gr)-large if $\{Ker(h) : h \in Y\}$ is large in the same sense. If $tr.deg_F(L') = 1$, a set Y of places of L over F will be called large if for some finitely generated F-algebra D and large subset Y' of homomorphisms on D, Y contains every place whose restriction to D is in Y'.

We will say that a property holds "for (Zar,ad,sa,gr)-almost every ..." if it holds for a large set in the corresponding sense. Without qualification, the phrase "almost every" will refer to Zar.

When the fraction field of D has transcendence degree 1 over F, one sees immediately that any set of primes of D whose residue fields have bounded degree over F must be ad-small. Conversely, 5A.3 will show that (in transcendence degree 1) these are precisely the ad-small sets.

The notions of largeness ad, sa are incomparable; the inclusions among the notions (Zar,ad,sa,gr) look like a diamond.

This appearance of "ad-almost" may seem discouraging in connection with the mixed-characteristic case. For many purposes however 5A.2 will suffice.

If X is an algebraic geometry object defined over the field of fractions of D, (for instance a curve C or a pair consisting of a curve C together with a 1-form ω on C), then for almost all primes p of D one can define the reduced object X over D/p, denoted X_p. More generally, if $h : D \to L'$ is a homomorphism, X_h denotes the corresponding object over L', obtained by applying h to the coefficients of the defining equations of X.

Lemma 5A.1. *Let $D \subset D' \subset L$, with D' finitely generated over D. Let $Y \subset$ Spec D', $Z \subset$ Spec D.*

(a) Assume ad-almost all $p \in \operatorname{Spec} D$ are in Z. Then for ad-almost all $p' \in \operatorname{Spec} D'$, $p' \cap D \in Z$.

(b) Assume ad-almost all $p \in \operatorname{Spec} D'$ are in Y. Then ad-almost all $p \in \operatorname{Spec} D$ extend to an element of Y.

Proof. (a) is immediate from the definition. For (b), let $H' \subset D'$ be a finitely generated subgroup. We are to find a finitely generated $H \subset D$ such that any prime p of D with $p \cap H = (0)$ extends to a prime p' of D' with $p' \cap H = (0)$.

If $D' \subset D[{c_1}^{-1}, \ldots, {c_l}^{-1}]$ then one can take H to be generated by $H' \cap D$ together with $c_1, \ldots, c_l$.

If $D' = D[t]$ is a polynomial ring over D we can take H to be generated by the coefficients of the elements of H' (they have bounded degree). (And extend p to $pD[t]$.)

If D' is integral algebraic over D, let $W = \{w_1, \ldots, w_m\}$ be a finite generating set for H'. Let G be the Galois group of a finite Galois extension of the field of fractions of D, containing W. Let $g_1, \ldots, g_e$ be the distinct elements of G. Let H be generated by all products

$$\sum_{\nu \in Sym(e)} \prod_{i=1}^{e} g_i(a_\nu(i))$$

where $a_1, \ldots, a_e$ are elements of W. If $w = \sum n_i w_i \in H'$, the $N_{K'/K}(w) = \prod_{g \in G} g(w)$ is easily seen to be in the $\mathbb{Q}$-span of H. Now if $p = p' \cap D$, $p' \in Spec(D')$ and $w \in p'$, then $N(w) \in (p' \cap D) = p$; so if $(p \cap H) = 0$ then $p' \cap H' = 0$.

Composing these three cases (polynomial ring, localization, integral algebraic), we can arrive at some D'' with $D' \subset D''$; then go back to D' using (a). ∎

Lemma 5A.2. *Let $K_0 \leq K \leq L$ be fields, with K, L algebraically closed, $K_0 \neq K$, and $\alpha_1, \ldots, \alpha_n \in L \setminus K_0$. There exists a K-algebra homomorphism $h : K[\alpha_1, \ldots, \alpha_n] \to K$ with $h(\alpha_i) \notin K_0$.*

Proof. We use induction on $tr.deg._K(L)$ (it may clearly be supposed finite). If $K \subset K' \subset L$, we have by induction

$$h' : K'[\alpha_1, \ldots, \alpha_n] \to K'$$

with $h'(\alpha_i) \notin K_0$, and then

$$h'' : K[h(\alpha_1), \ldots, h(\alpha_n)] \to K$$

with $h''(h(\alpha_i)) \notin K_0$. Let $h = h'' \circ (h' | K[\alpha_1, \ldots, \alpha_n])$. This reduces the problem to the case $L = K(t)^a$. If some $\alpha_i \in K$, then $h(\alpha_i) = \alpha_i \notin K_0$ for any K-algebra homomorphism h; so this α_i can be ignored, and we may suppose each $\alpha_i \notin K$.

Note that we may increase K_0 as long as it stays a proper subfield of K. In particular we may if necessary add to K_0 a transcendence basis for K/K_0; so we may assume ${K_0}^a = K$. If -1 is not a sum of squares in K_0, we may assume it is real closed. In this case let C be the locus of $(\alpha_1, \ldots, \alpha_n)$, and let f_i be the ith projection, restricted to C. Then f_i is finite-to-one, so ${f_i}^{-1}(K_0)$ is one-dimensional in the sense of real closed fields (or o-minimal structures), yet the curve $C(K)$ is two-dimensional (in the same sense), so it has a point a with $f_i(a) \notin K_0$.

Suppose now that K_0 is not a real field. Then by Artin-Schreier, $K = {K_0}^a$ is not finitely generated over K_0. Now $K(t, \alpha_i)$ is a finite extension of $K(\alpha_i)$; say $[K(t, \alpha_i) : K(\alpha_i)] = m_i$. So $\sum_{j \le m_i} f_{ij}(\alpha_i) t^j = 0$, with $f_{ij} \in K[X]$. Increasing K_0 within K, we may assume $f_{ij} \in K_0[X]$.

Pick $0 \neq d(t) \in K_0[T]$ such that each α_i and each $f_{i,m_o}^{-1}(\alpha_i)$ are integral over $K_0[T, d(t)^{-1}]$. Pick $b \in {K_0}^a$ with $[K_0(b) : K_0] > \max\{m_1, \ldots, m_n, \deg(d)\}$. Then $d(b) \neq 0$. Let $h : K[t, d(t)^{-1}] \to K$ be the homomorphism of K-algebras with $h_0(t) = b$. Extend h to the integral extension

$$K[t, \alpha_1, \ldots, \alpha_n, f_{1,m_1}^{-1}(\alpha_1), \ldots, f_{n,m_n}^{-1}(\alpha_n)]$$

of $K[t, d(t)^{-1}]$. Let $\beta_i = h(\alpha_i)$. Then

$$\sum_{j \le m_i} f_{ij}(\beta_i) b^j = 0$$

while $f_{i,m_0}(\beta_i) \neq 0$; so

$$[K_0[b, \beta_i] : K_0[\beta_i]] \le m_i.$$

As $[K_0[b] : K_0] > m_i$, it follows that $\beta_i \notin K_0$. ∎

LEMMA 5A.3. *Let $K \subset L$ be fields, $tr.deg._K(L) = 1$; let $D \subset L$ be a finitely generated K-algebra, and let $V \subset D$ be a finite-dimensional K-space. Then there exists an (effective) integer M such that for any K-algebra homomorphism $h : D \to K^a$, either $h(D) \subseteq K'$ for some finite extension K' of K with $[K' : K] \le M$, or else $h|V$ is injective.*

Proof. Let t be a tuple of generators of D as a K-algebra, I the ideal of polynomials over K^a vanishing on t, I_0 a finite set of generators for I. Then $I_0 \subset K_0[T]$ for some finite extension K_0 of K. Let C be the variety corresponding to I; it is irreducible and defined over K_0, and is either a curve or a point, as $tr.deg._K(L) = 1$. Let $d_1, \ldots, d_m \in D$ form a K-basis for V. Given any $s_1, \ldots, s_m \in K^{alg}$ (or in any algebraically closed extension field L), the equations

$$\sum s_i d_i = 0$$

viewed as polynomials in T, cut out a proper algebraic subset of C (over L). They therefore have only finitely many solutions. By quantifier-elimination, or by a direct devissage procedure, one finds M_0 such that for any $s = (s_1, \ldots, s_m)$, all these solutions are roots of a common polynomial over $K_0(s)$ of degree $\le M_0$. In particular this holds for s from K. Now for any $h : D \to K^a$, if the $h(d_i)$ are linearly dependent over K, then $\sum s_i h(d_i) = 0$ for some $s_1, \ldots, s_m \in K$, and thus the $h(d_i)$ are all roots of one polynomial over K_0 of degree $\le M_0$. It follows that $[K(h(D)) : K] \le M_0[K_0 : K] =_{def} M$. ∎

REMARK 5A.3R. There are variants of 5A.3 for higher transcendence degrees. For instance if t_1, t_2 form a transcendence basis for L/K, and $K[t_1, t_2] \subset D \subset L$, let $V \subset D$ be a finite-dimensional K-space. Then there exists M_1 and an effectively computable function $M_2 : \mathbb{N} \to \mathbb{N}$ such that for any K-algebra homomorphism $h : D \to K^a$, if $[K(h(t_1)) : K] = d_1 > M_1$, and $[K(h(t_2)) : K(h(t_1))] > M_2(d_1)$, then h is injective on V.

LEMMA 5A.4. *Let $K_0 \le K \le L$ be fields, with K algebraically closed, but K_0 neither real closed nor algebraically closed. Let $D \subset L$ be a finitely generated K_0-algebra, and*

$V \subset D^m$ be a finite-dimensional K_0-space. There exists a K_0-algebra homomorphism $h : D \to K$ such that h is injective on V. (If $\mathbb{Q} = K_0$, ad-almost all h have this property.)

Proof. The case $m = 1$ follows from 5A.3 and Artin-Schreier. To treat the general case, embed $V \to D$ by a D-linear map $D^m \to D$, as in Lemma 1.0. Alternatively, one can proceed as in 5.8A(5).

Remark 5A.5. Let D be a finitely generated sub-domain of $L = L^a$, $K = K^a$, let $\phi(u_1, \ldots, u_n)$ be a formula in the language of fields, $\alpha_i \in D$, and assume $L \models \phi(\alpha_1, \ldots, \alpha_n)$. Then for almost all $h \in Hom_F(D, K)$, $K \models \phi(h(\alpha_1), \ldots, h(\alpha_n))$.

Proof. By Tarski's theorem, we can take ϕ to be a conjunction of polynomials equalities and inequalities. The equalities are automatically preserved by homomorphisms, so the additional condition reduces to: $h(e) \neq 0$ for a certain nonzero $e \in K[\alpha_1, \ldots, \alpha_n]$.

Example 5A.6. Let A be an Abelian variety (resp. commutative unipotent group) defined over $K(\alpha_1, \ldots, \alpha_n)$. Then for almost all h, A_h is also an Abelian variety (unipotent).

Proof. A admits a projective embedding, and an algebraic group structure; these two things can be witnessed by a first-order formula in the parameters; so 5.A5 applies. Similarly for the unipotent case, there exists an L-definable isomorphism $A \to \mathbb{G}_a{}^l$ for some l.

Remark 5A.7. Let D be a finitely generated sub-domain of $L = L^a$, $K = K^a$. Let $Q(u) \in D[u]$. Then for ad-almost all $h \in Hom_F(D, K)$, Q_h has no rational solutions except for the rational solutions of Q.

Proof. Localizing D, we may assume Q is monic. Let $\alpha_1, \ldots, \alpha_m$ be the irrational solutions of Q in L, and $\beta_1, \ldots, \beta_l$ the rational ones. For ad-almost all $h \in D[\alpha_1, \ldots, \alpha_m](K)$, each $h(\alpha_i)$ is irrational, so Q_h has no rational solutions other than the β_i. By 5A.1, ad-almost all $h \in Hom_F(D, K)$ have the same property. ∎

Discussion 5A.8. Let F be a number field.

(1) If $f_i(X, T)$ are polynomials with no roots in $F(T)$, then

$$H = \{a \in F : \wedge_{i=1}^m \neg \exists x \in F.\, f_i(X, a) = 0\}$$

is a typical *Hilbert set*. This is one of the central subjects of [8]; see the proofs there that Hilbert sets are non-empty. In particular, by Theorem 12.7 of that book, H contains a translate of a nonzero ideal I of the ring of integers $\mathcal{O}_F$ of F. As no coset of I can be contained in a proper subfield F' of F, or a finite union of such subfields, this gives one way of seeing that the Hilbert set has infinitely many elements that are not in any proper subfield of F.

(2) Let $L = F(t)$ be a finite extension of $F(t)$. Consider places $p : L \to F^a$ over F; i.e. we have a valuation ring $F \subset \mathcal{O}_p \subset L$, and a surjective F-algebra homomorphism $res_p : \mathcal{O}_p \to k_p$, the residue field k_p being a finite extension of F. There exists a Hilbert set $H \subset F$ such that if ($t \in \mathcal{O}_p$ and) $res_p(t) \in H$, then $[k_p : F] = [L : F(t)]$. (The standard (Robinson?) nonstandard proof of this standard (Hilbert?) fact: if U is any ultrafilter containing the Hilbert sets, and p_a is a place with $resp_a(t) = a$, then one

obtains an embedding of $F(t)$ into $F^* = Ult_U F$ ($t \mapsto (res_{p_a}(t))_U$) such that $F(t)$ is relatively algebraically closed in F^*. Then $F(t)^a$ is linearly disjoint over $F(t)$ from F^*. So $[L : F(t)] = [LF^* : F^*] = [k_p : F]$ (the last equality holding for almost all p).)

(2a) Let L be a finitely generated field over F, of transcendence degree 1. Given a finite extension L' of L, let $H(L, L')$ be the set of valuations p of L sdover F extending to a valuation p' of L' with $[k_{p'} : k_p] = [L' : L]$. A set of the form $H(L, L')$ (or cofinite in such a set) will be called a Hilbert set of valuations. It follows from (2) that Hilbert sets are nonempty. (Let $t \in L \setminus F^a$. If $p|F(t) \in H(F(t), L')$ then $p \in H(L, L')$.)

(2b) If X is a finite subset of $L' \setminus L$, then a cofinite subset of $p \in H(L, L')$ extend to p' such that satisfy $[k_{p'} : k_p] = [L' : L]$, $X \subset \mathcal{O}_{p'}$, and $p'(X) \cap k_p = \emptyset$. (Write $L' = L[c]$. Let $d \in L' \setminus L$. For almost all p, c, d are integral over $\mathcal{O}_p$. Moreover for p as in (2a), if $m = [L' : L]$, $p'(1), p'(c), \ldots, p'(c^{m-1})$ are linearly independent over k_p. Write $d = \sum_{0 \le i < m} a_i c^i$. Then $a_i \neq 0$ for some $1 \le i < m$; for almost all p, $p(a_i) \neq 0$; so $p'(d) \notin k_p$.)

(3) Let L be a function field over F, and let A be an Abelian variety over L. Then for almost all places p of L, the reduction of A at p is an Abelian variety over the residue field k_p (a finite extension of F), and one has a reduction homomorphism $r_p : A(L) \to A(k_p)$. Neron showed the existence of a Hilbert set H such that for $p \in H$, r_p is *injective*. (Pick a rational prime l such that $A = A(L)$ has no l-torsion, and let $b_1, ..., b_m$ represent the classes of A/lA; then find H such that for $p \in H$, S_p has no k_p-rational l-torsion points, and $r_p(b_i)$ has no F-rational lth roots; thus r_p induces an injection on A/lA into $A(k_p)/lA(k_p)$; one concludes algebraically that f_a is injective. See [14].)

(4) An entirely similar argument works for finitely generated subgroups Γ of the multiplicative group G_m.

(5) Let $A \xrightarrow{j} B \xrightarrow{f} C$ be an exact sequence of Abelian groups. Let

$$A' \xrightarrow{j'} B' \xrightarrow{f'} C'$$

be another sequence, with $f'j' = 0$, and j' injective. Let $h_A : A \to A'$, $h_B : B \to B'$, $h_C : C \to C'$ be homomorphisms with $h_B j = j' h_A, f' h_B = h_C f$. Finally let Γ be a finitely generated subgroup of B. Assume h_A is injective on $j^{-1}(\Gamma)$ and h_C is injective on $f(\Gamma)$. Then h_B is injective on Γ.

LEMMA 5A.9. *Let F be a number field, L a finitely generated extension field of transcendence degree* 1. *If H is a Hilbert set of places of L over F, and Y is an ad-large set of places of L, then $H \cap Y$ is infinite.*

Proof. By Lemma 5A.3, there exists a finitely generated F-subalgebra D of L, and an integer M such that $p \in Y$ whenever $p(D)$ is finite and is not contained in an extension of F of degree $\le M$. Say H is cofinite in $H(L, L')$. Let F' be an extension of F of degree $> M$. Let $t \in D \setminus F^a$.

For some $0 \neq c \in F[t]$, $D[c^{-1}]$ is integral over $F[t, c^{-1}]$. Let Z be the zero set of the polynomial c. If $a \in F^a \setminus Z$, then the homomorphism $h_a : F[t] \to F^a$, $t \mapsto a$, extends to a homomorphism $h : D \to F^a$.

By 5A.8 (1,2a), there exists a Hilbert set $H' \subset F'$ such that if $t \in \mathcal{O}_p$ and $res_p(t) \in H'$ then $p \in H$. By 5A.8 (1), there exists $a \in H$, with a not in any proper subfield of F',

and also $a \notin Z$. For any such a, any place p with $res_p(t) = a$ satisfies both conditions, and so lies in $H \cap Y$. ∎

LEMMA 5A.10. *Let F be a number field, L a finitely generated extension field of transcendence degree 1. Then every gr-large set of places of L contains the intersection of a Hilbert set with an ad-large set (and hence is infinite.) Explicitly, let G be a commutative algebraic group over L, and let Γ be a finitely generated subgroup of $G(L)$. For almost all places p of L over F, p induces a well-defined homomorphism $r_p : \Gamma \to G(k_p)$. There exists a Hilbert set H and an ad-large set Y such that for all $p \in H \cap Y$, r_p is injective on Γ.*

Proof. Enlarging L if necessary, we can find an exact sequence $0 \to V \to G \to S \to 0$ of algebraic groups over L, with $V \simeq {G_a}_L{}^l$ and S semi-abelian. By 5.8(5), and because the target sets (Hilbert meet ad-large) are closed under finite intersections, it suffices to prove the lemma separately for V and for S. Similarly, splittting S and then the vector and toric parts, we may assume G is an Abelian variety, or G_m or G_a. In the former two cases, 5A.8 (3,4) give the appropriate set (a Hilbert set). The case of G_a follows from the definition of an ad-large set. ∎

LEMMA 5.11. *Let F be a number field, L a finitely generated extension field of transcendence degree 1, H a commutative group scheme over D. Let $\chi_1, \ldots, \chi_r$ be homomorphisms $H \to G_m$ of algebraic groups, defined over L, and forming a $\mathbb{Q}$-basis for $Hom(H, G_m)$; i.e. for every (L^a-definable) algebraic group homomorphism $\chi : H \to G_m$, for some $m > 0$, there exist unique $m_1, \ldots, m_r \in \mathbb{Z}$ with $\chi^m = \prod {\chi_i}^{m_i}$. Then for sa-almost all places p of L, $\chi_1, \ldots, \chi_r$ form a $\mathbb{Q}$-basis for $Hom(H_p, G_m)$.*

Proof. First one needs to show that reduction mod p leaves the χ_i $\mathbb{Q}$-linearly independent (for almost all p.) Note that $h = (\chi_1, \ldots, \chi_r) : H \to {G_m}^r$ induces a bijection $\bar{H} \to {G_m}^r$; so it is also a bijection on L-rational points of these groups. Find $a \in {G_m}^r(\mathbb{Q})$ that is not in any proper algebraic subgroup of ${G_m}^r(L)$ (e.g. $a = (l_1, \ldots, l_r)$ with the l_i distinct rational primes.) Let $h(b) = a$, $b \in \bar{H}$. Then for almost all places p, $h(red_p(b)) = a$, and it follows that the χ_i remain $\mathbb{Q}$-linearly independent.

The main point however is that (on a large set) no new characters show up after reduction. For simplicity, take $r = 0$ (one can reduce to that case, by going to $\cap_{i=1}^r Ker(\chi_i)$). One can factor out the maximal vector subgroup of H without changing the terms of the lemma. So:

(A) H is a semi-Abelian variety, with no multiplicative characters.

We have however (after taking a finite extension of L, as the conditions and conclusions of the lemma permit) an exact sequence $0 \to T \to H \to A$, with A an Abelian variety, and $T \simeq {G_m}^l$. For almost all p, A_p remains an Abelian variety, and the sequence remains exact. For each character $\rho : T \to G_m$, factoring out by $ker(\rho)$ we obtain an exact sequence $0 \to G_m \to H \to A$, i.e an extension of A by G_m, corresponding to an element of the dual Abelian variety $A^* = Pic_0(A)$ (cf. [19]). Let $\rho_1, \ldots, \rho_l$ generate the characters of T, and let $b_1, \ldots, b_l$ be their images $\in A^*$. Then

(B) $b_1, \ldots, b_l \in A^*$ are $\mathbb{Q}$-linearly independent in $\mathbb{Q} \otimes_{\mathbb{Z}} A^*$.

Indeed (B) is precisely equivalent to (A); and the equivalence is preserved for almost all specializations.

Now (B) is preserved under an sa-large set of specializations, by definition of sa-largeness. ∎

NOTATION. We will say that a 1-form on a curve C is rationally logarithmic if it has the form df/f for some rational function on C, or is a rational multiple of such a form. We will say that forms $\omega_1, \ldots, \omega_n$ are rationally logarithmically independent if whenever $\gamma_1, \ldots, \gamma_n \in \mathbb{Q}$ and $\sum \gamma_i \omega_i$ is logarithmic, we have $\gamma_i = 0$ for each i.

LEMMA 5A.12. *Let K be a number field, L a finitely generated extension of transcendence degree* 1. *Let C be a curve defined over L, and let $\omega_1, \ldots, \omega_l$ be l rationally logarithmically independent 1-forms on C. Then for gr-almost all places p of L over K, the forms $(\omega_i)_p$ are rationally logarithmically independent 1-forms on C_p.*

Proof. Let $j : C \to J$ be a generalized Jacobian of C, such that $\omega_i = j^*\psi_i$ for some invariant 1-form ψ_i on J ([19], V.10, Prop.5). If $\sum \gamma_i \omega_i = df/f$, let B be the multiplicative group written additively, and define

$$h : C \to (J \times B)\ , \qquad h(c) = (j(c), f(c)).$$

Let π_J, π_B be the projections on $J \times B$, and let $\theta = \sum \gamma_i (\pi_J)^* \psi_i - \pi_B^*(dt/t)$. This 1-form on $J \times B$ is nonzero (even on $(0) \times B$) but vanishes on the image $h(C)$ of C. We may assume that $0 \in h(C)$; so $h(C)$ generates an algebraic group $A \leq J \times B$, and θ vanishes on A. As $\theta \neq 0$, $A \neq J \times B$. Now A maps surjectively to J, with finite kernel $((1) \times B) \cap A$; for some m, $m(((1) \times B) \cap A) = 0$; so

$$\{(a, mb) : (a, b) \in A\}$$

is the graph of a homomorphism $\chi : J \to B$. We have moreover $\sum \gamma_i \psi_i = m\chi^*(dt/t)$, or $\sum (1/m)\gamma_i \psi_i = \chi^*(dt/t)$.

Thus the rational logarithmic independence condition on the forms ω_i follows from a condition on the ψ_i:

(*) there should be no nonzero rational γ_i and homomorphism $\chi : J \to B$ with

$$\chi^*(dt/t) = \sum \gamma_i \psi_i.$$

Conversely, if $j : C \to J'$ is any map of C into a commutative algebraic group, and $\omega_i = j^*\psi_i$ for an invariant 1-form ψ_i on J', and $j(C)$ generates J', and (*) fails, then it is clear that the ω_i are rationally linearly dependent over forms df/f.

Thus we can forget about C, and just consider J and the forms ψ_i. Let $\chi_1, \ldots, \chi_r$ be a $\mathbb{Q}$-basis for the multiplicative characters of J, and $\theta_i = {\chi_i}^*(dt/t)$. By 5A.11, the reductions of the χ_i form a $\mathbb{Q}$-basis for the reduction of J, on an sa-large set of valuations. Once the χ_i are known to be a $\mathbb{Q}$-basis, (*) becomes

(**) $\theta_1, \ldots, \theta_r, \psi_1, \ldots, \psi_m$ are $\mathbb{Q}$-linearly independent.

This condition (**) is preserved by reduction on an ad-large set of places (5A.4). ∎

REMARK 5A.12R. An alternative treatment analogous to 2.4 is also possible, avoiding the generalized Jacobian. There one uses residues, and ends up requiring injectivity on a finitely generated subgroup of the Jacobian rather than the dual.

V.1. Specializations of Kolchin closed sets. We now take a derivation into consideration. Let k be the constant field of the derivation. Let F be a field of characteristic 0, $F \subset D \subset L \subset k$. Assume D is a finitely generated F-algebra. Let V be a linear Kolchin closed set defined over $(D(t), d/dt)$.

Let V be a linear Kolchin closed set defined over L. Then V is defined over a finitely generated F-algebra D. Given $p \in Hom_F(D, L')$, we can define a Kolchin closed set V_p by applying p to the coefficients of the defining equations of V. This makes sense also for $G = Aut(V/L(t), C)$ (since $G \leq GL(V)$ is also a Kolchin closed set).

PROPOSITION 5.1. *Let $G = Aut(V/L(t), C)$. Then for gr-almost all $p \in \operatorname{Spec} D$, $G_p = Aut(V_p/k(t), C)$.*

COROLLARY. *If for almost all $p \in Hom_F(D, k)$, V_p has a basis of solutions in $k(t)^a$, then V has a basis of solutions in $L(t)^a$. (Analog of Grothendieck's conjecture.)*

Proof. V has a basis of solutions in $L(t)^a$ iff G is finite. ∎

REMARK 5.2. The hypothesis of 5.1 can be weakened to "for g-almost all p", but not to: "for infinitely many p", for the same reason as in Example 1.2. Moreover the set of exceptional p may contain any given sa-small or ad-small set.

COROLLARY 5.3. *The Proposition implies that $Aut(V/k(t)^a)_p = Aut(V_p/k(t)^a)$ for gr-almost all p.*

An interesting case occurs when for infinitely many p, G_p is finite, but of unbounded size. In this case a limit group $lim_p G$ is in effect considered, and shown to be a finite extension of a torus. The proof thus essentially works with G_p and not with ${G_p}^0$.

LEMMA 5.4. *Let the linear Kolchin closed set V be defined by*

$$P_n x^{(n)} + \ldots + P_1 x' + P_0 x = 0$$

with $P_i \in D[t]$. There exists a bound N (valid for almost all $h \in Hom_F(D, k)$) on the order of vanishing of a nonzero power series solution of D_h at 0. In other words if $\sum_{i=N+1}^{\infty} \gamma_i t^i \in V(k[[t]])$ then each $\gamma_i = 0$.

Proof. The equation for V can be written

$$\sum_{i,j} c_{ij} t^i D^j x = 0$$

(where $c_{ij} \in D$ for $i, j \in \mathbb{N}$, and only finitely many c_{ij} are nonzero). Let

$$k = \min\{i - j : c_{ij} \neq 0\}$$

if $\sum_{i=m}^{\infty} \gamma_i t^i \in V(k[[t]])$ with $\gamma_m \neq 0$, looking at the coefficient of t^{m+k} we obtain:

$$\sum_j c_{k+j,j} \frac{m!}{j!(m-j)!} = 0.$$

Let $Q(u) = \sum_j c_{k+j,j} \frac{u!}{j!(u-j)!} \in D[u]$. By 5A.7, for ad-almost all h, Q_h has no rational solutions other than those of Q, and in particular no integral solutions larger than the maximal integer solution of Q. ∎

LEMMA 5.5. *Let V be as in 5.4. If, for ad-almost all $p \in Hom_F(D,k)$, V_p has a solution in $k[t]$, then V has a solution in $k[t]$. In fact if $V(k[t])$ denotes the space of $k[t]$-valued elements of V, and $d = \dim V(k[t])$, then $\dim(V_p(k[t])) = d$ for almost all $p \in Hom_F(D,k)$.*

Proof. First let $H_N(k)$ be the space of polynomials of degree $\leq N$ (over the constant field k). This is a finite-dimensional vector space with a distinguished basis $1, t, \ldots, t^N$. The operator d/dt acts on it via a known (diagonal) matrix, and hence any linear differential operator $\sum P_i D^i$ acts on H_N in a definable way, uniformly in the coefficients P_i. The kernel of the operator is therefore uniformly definable in field theory. Thus if d_N is the dimension of the subspace of H_N consisting of solutions to V, then for almost all $p \in Hom_F(D,k)$, the dimension of the solution space to V_p also equals d_N.

Thus it suffices to find N such that for ad-almost all p, any polynomial solution of any V_p must have degree $\leq N$. But such an N is given by a bound for the pole at ∞ of the possible polynomial solutions; i.e. by a bound for the pole at 0 of a solution given as a power series in t^{-1} (Lemma 5.4). ∎

LEMMA 5.6. *There exists a Kolchin closed linear subspace V' of V, defined over $D[t]$, such that for ad-almost all $p \in Hom_F(D,k)$, $(V')_p = V_p(k[t])$.*

Proof. Let V' be the k-span of $V(k[t])$. The lemma follows from 5.5. ∎

NOTATION. Let W be a Kolchin closed or a Kolchin constructible set defined over $k(t)$. Denote by IW the set of elements of W defined over $k(t)$. IW is a (finite or) countable union of Kolchin constructible sets; if k_0 is an algebraically closed subset of k and W is defined over $k_0(t)$, these Kolchin closed sets can also be taken to be so definable.

Recall that $N_d(V)$ is the set of Zariski closed subsets of V defined by polynomials of degree $\leq d$; and that by Corollary 1.5, $IN_d(V)$ is Kolchin constructible. In particular $N_1(V)$ is the set of affine subspaces of V of various dimensions; let $L_k(V)$ be the set of k-dimensional linear subspaces of V, $L(V) = \cup_{k \leq \dim(V)} L_k(V)$. $L_1(V)$ is in definable bijection with $\{v'/v : v \in V\}$.

LEMMA 5.7. *Assumptions as in 5.4. For ad-almost all $h \in Hom_F(D,k)$, $IL_1(V_h) = (IL_1(V))_h$.*

Proof. We repeat the proof of P1.1, noting that it is uniform as V varies in a uniformly definable family of Kolchin closed sets. Let $W = \{v'/v : v \in V\}$. It suffices to show that $I(W_h) = I(W)_h$. This follows Picard. A rational solution to W can have poles at the zeroes of P_n, and other poles; but the other poles have order at most 1, and positive integral residue (bounded by the order of V). The poles at the zeros of P_n have bounded order ($\leq n$), and finitely many possible polar parts. We split W according to these possible polar parts, at each zero of P_n. We find a (not necessarily rational, nor in V, but with a'/a rational) having the same polar information. Replacing V by aV (hence W by $a'/a + W$), we reach a similar situation but where we can restrict attention to rational

$w \in W$ with finite poles of order at most 1, and integral residues. Pulling back to V, the solutions of interest are polynomial, and 5.6 applies. ∎

LEMMA 5.8. *For ad-almost all $h \in Hom_F(D,k)$, $IN_d(V_h) = (IN_d(V))_h$.*

Proof. The proof of Proposition 1 gives constructible bijections, compatible with the functor I: from $N_d(V)$ to a finite union of subsets of some $L_k(V')$; from there to some $L_1(V'')$. These bijections are all constructible, and commute with almost every h. This reduces the problem to 5.7. ∎

We need to consider finite extensions of $k(t)$. These have the forms $k(C)$, C a curve defined over k. The embedding $k(t) \subset k(C)$ corresponds to a rational map t on C, that we fix.

LEMMA 5.9 (finite case). *Assume $k(C)$ is a finite Galois extension of $k(t)$, with Galois group G. Then the same is true of $k(C_p)$ for almost all p.*

Proof. G^{op} acts on C over $t : C \to \mathbb{P}^1$; regularly on almost all fibers; being an elementary statement, this remains true for C_p, for almost all p. Moreover, C_p irreducible for almost all p (cf. e.g. [7], [8], [10]). This suffices for $Aut(C_p/\mathbb{P}^1)$ to be transitive on almost all fibers. It follows that $Aut(C_p/\mathbb{P}^1) = (G^{op})^{op} \simeq G$. ∎

LEMMA 5.10 (toric case). *Let V have the equation: $x_i' = e_i x_i$, $e_i \in L(C)$, C a curve defined over D. Let $G = Aut(V/k(t)^a) \leq {\mathbb{G}_m}^n$. Then for ad-almost all p, $G = Aut(V_p/k(t)^a)$.*

Proof. Let $\Delta, \Delta(p)$ be defined as in Lemma 2.3 for V, V_p respectively. By 2.3^0, it suffices to show that $\mathbb{Q}\otimes\Delta = \mathbb{Q}\otimes\Delta(p)$ for ad-almost all p. This is just Lemma 5A.12. ∎

Proof of Proposition 5.1. The proof is now identical to that of Proposition 4.1 (any troublesome ingredients having been dealt with). One first considers the uniform cover $H(V) = Aut(V/k(t))_{\mathcal{F}}$ of the Galois group of V, and shows that $H(V)_p = H(V_p)$ for ad-almost all p. This is in fact immediate from 5.8. Thus also $(H(V)^t)_p = H(V_p)^t$ for ad-almost all p. Next, aiming first to prove Corollary 5.3, let $G_t(V)$ be the image of $Aut(V/k(t))^0$ in $H(V)/H(V)^t$. It will suffice to show that $G_t(V)_p = G_t(V_p)$ for gr-almost all p. But $G_t(V)$ is the Galois group over $\mathbb{Q}(t)^a$ of an auxiliary equation of toric type, and Lemma 5.10 does the job. The deduction of Proposition 5.1 from Corollary 5.3, as in that of Algorithm C from Algorithm B, uses Lemma 5.9. ∎

Appendix A: Did schemes supplant the universal domain? We are interested in an algebraic theory T_0, given as a set of universal sentences (such as

$$(\forall x)(\forall y)((xy)' = x'y + y'x), \quad \text{or } (\forall x)(\forall y)(xy = 0 \Rightarrow (x = 0 \vee y = 0))).$$

For simplicity assume the language has a finite or countable number of relation and function symbols.

Let C_0 be the class of "all" models of T_0; well, say all countable ones.

Examples: integral domains; differential integral domains. (Can we always take some kind of *rings*? No, not even for geometric purposes. For instance in the fundamental

theorem of projective geometry, we start with a point-line incidence system, and *end* with a ring. If we had to start with a ringed object, we would lose the theorem. There are other such situations, some arising within differential equations. Even when we do start with a ring, elimination of imaginaries can take us elsewhere.)

Let us distinguish four approaches to the algebra in question.

(1) Proof theoretic: the objects are formulas: e.g. in algebra or differential algebra, systems of polynomial equations, or differential polynomial equations (or coordinate-free versions of the above). One has a more or less strong idea that the formulas have some meaning; leading in particular to identifying formulas differing only by certain transformations. But one does not explicitly work with solutions, and does not need to specify where they live.

(2) At the opposite extreme, one takes seriously abstract algebraic structures (fields, differential fields, models), almost to the point of ignoring formulas.

(3) "Representable functors": the emphasis is again on formulas; but a formula ϕ is viewed not syntactically, but as a *functor* that takes a structure $A \in C_0$ to the set of solutions of ϕ in A.

(4) Universal domains: the functor in (3) is replaced by its value at a single structure; this can work only when a single structure can be viewed as the amalgam of "all structures".

Approach (4) is possible only when the class of structures in question admits amalgamation. When it does, (4) is entirely equivalent to (3); any structure admits an embedding in the universal domain, unique up to an automorphism of the universal domain; permitting recovery of the value of the functor there.

The history of algebra passed through (1) (complex numbers in the 16th century), (4) (complex numbers in the 19th), (2) ("modern algebra"), (4) (Weil's universal domains, in any characteristic), (1) + (3) (Grothendieck).

In model theory, (1) was followed by (2) and (3); Shelah introduced (4) as a convention in his book on classification theory, and this became generally accepted in the 80's, more so within stability theory than in other parts of model theory.

With sufficient hindsight in a particular context, (1) can be also treated so as to become equivalent to (3). This is done in some presentations of schemes (but usually the functors come in straightaway after).

Thus a "Kolchin closed set" corresponding to some differential equations can be interpreted as (3) a functor mapping a differential field to the solution set of these equations, (1) the radical ideal generated by the equations, (4) the set of all solutions of the equations (in a universal domain).

It should be clear that these are surface transformations; they do not effect the deep grammar. It is useful to be aware of all three; there is as little reason to commit to one interpretation as to deciding whether real numbers are Dedekind cuts, or equivalence classes of Cauchy sequences.

(2) on the other hand really treats more algebraic and less geometric material. The isomorphism types of particular models becomes involved.

Connection to schemes. These distinctions relate to the revolution of schemes only at its surface. Grothendieck's real contribution, in this respect, was not the change of language, but the incorporation of infinitesimals, and of homological algebra, as intrinsic parts of the geometry. These go beyond Weil's original universal domain, not because it is a universal domain, but because it is a universal domain for the wrong class of structures (rings, and without nilpotents). When one speaks about nontrivial groups without nonzero points, etc., it is Weil's universal domain that lacks the points, but are there others?

The most serious objection to universal domains is that they apply only when the structures in question admit amalgamation; and preferably a certain finiteness property allowing a model companion. Do these properties hold for an appropriate presentation of schemes with infinitesimals, or for varieties with coherent sheaves over them? There has been little work on these questions; perhaps because of the view, widely held and published by model-theorists, that ACF remains the first-order theory underlying algebraic geometry; that Grothendieck somehow changed the logical way of looking at it, rather than the theory itself. The answer to the second question appears to be positive. For the first, Cherlin showed that commutative rings with infinitesimals do *not* have a model companion in the language of rings; essentially because the order of infinitesimals must be taken seriously. But once this is done, a positive answer may exist. (Truncated valuation rings have a good model theory, and give a partial response.)

The above speculation is quite irrelevant to differential algebra at the level of the present paper, neither infinitesimals nor sheaves or cohomology occur; both fields and differential fields of characteristic 0 admit universal domains, and model completions.

The approach (4) often brings out the geometry, with minimal intervention of particular algebras. Thus for instance, Picard's original treatment (using (4)) assigned a group to an equation. In the modern-algebra treatment (2) of differential Galois theory, one takes two algebras A, B and obtains an abstract group $Aut(A/B)$. The fact that the group really belongs to a geometric object must be seen later and separately, via base change properties for B/A; similarly the fact that the abstract group is related to an algebraic group. By contrast using (4), one takes as input two definable sets (say, a Kolchin closed linear space V and the equation C of constants) and yields a definable group $(Aut(V/C))$; all three are directly geometric. This is explained in Appendix (B).

The construction of (4) uses some quite harmless set-theory to explain the meaning of "all" structures. This can be done via cardinality differences, or recursiveness considerations, or taking a proper class universal domain; in other words the set theory is not really relevant. To avoid it completely, take $\kappa = \aleph_0$ below, so that we obtain a countable universal domain for finitely generated structures. The assumption α below is met when T_0 is the theory of differential integral domains of characteristic 0, and the universal domain thus obtained is adequate for our purposes. It is more convenient, and more general, to permit other choices of regular cardinals κ; using some easy set theory, one can *always* arrange that assumption α holds; so the amalgamation requirement β is the only serious assumption. (To shorten the discussion, we included a joint embedding property in β.)

THEOREM A1. *Let*

$$C_0 = \{M \models T_0 : M \text{ is generated by } < \kappa \text{ elements}\}.$$

Assume (α) that for $M \in C_0$, there are $\leq \kappa$ isomorphism types over M of finitely generated extensions of M in C_0. Assume (β) that any two structures in C_0 embed into a common one; and moreover that if $f_i : A \to B_i$ are embeddings, $A, B_1, B_2 \in C_0$, then there exists $B \in C_0$ and embeddings $g_i : B_i \to B$ with $g_1 \circ f_1 = g_2 \circ f_2$. (Amalgamation.) Then there exists a $\mathbb{U} \models T_0$, generated by κ elements, such that any $A \in C_0$ embeds uniquely into $\mathbb{U}$; uniqueness means that $Aut(\mathbb{U})$ acts transitively on the set of embeddings. This $\mathbb{U}$ is unique up to isomorphism. It is called the universal domain for C_0.

Call a subset of $\mathbb{U}^n$ *constructible over* A if it is the solution set to a basic formula in the language, possibly using parameters from A, or a finite Boolean combination of such. A countable intersection (union) of constructible sets will be called *ω-constructible over A* (Σ-constructible). If A is not mentioned, it is taken to be $\mathbb{U}$ (i.e. unrestricted parameters); if $A = \emptyset$, we say: "0-constructible", etc.

(A1) already shows that $Aut(\mathbb{U})$ is large, and forms the beginning of a Galois theory; the construction of $\mathbb{U}$ once and for all allows later to avoid many base changes, while $Aut(\mathbb{U})$ still permits to keep track of the base when one wishes, via a kind of Galois descent:

Let $A_0 \subset \mathbb{U}$, $|A_0|$ countable or finite. Then a constructible set D is constructible over A_0 iff $Aut(\mathbb{U}/A_0)$ leaves D invariant. A similar statement hold for ω- or Σ-constructible sets.

In particular, the union of all one-element A_0-constructible sets coincides with $Fix(Aut(\mathbb{U}/A_0))$; it is called the definable closure of A_0, or $dcl(A_0)$.

$\mathbb{U}$ also has a *countable compactness* property; any countable collection of constructible sets with the finite intersection property, has nonempty intersection. It follows for example that a set that is both ω-constructible and Σ-constructible is constructible. (If $P = \cap_n P_n$ while $\neg P = \cap_n Q_n$, then $\cap_n (P_n \cap Q_n) = \emptyset$, so for some N, $\cap_{n \leq N} (P_n \cap Q_n) = \emptyset$, and it follows that $P = \cap_{n \leq N} P_n$.)

Appendix B: Definable automorphism groups. We present the main definability results on relative automorphism groups ([9], Theorem 3), and show that they can be obtained without stability assumptions. This carries no logical advantage in the present context—all applications envisaged here are stable—but it does greatly free the exposition.

In the case of ∞-definable sets, stability assumptions are lightened but not eliminated (B.5).

We also discuss the connection to Picard-Vessiot and related theories, including Matzat's characteristic p theory.

The reader interested only in the applications of this paper, or wishing to read with an example in mind, can set parameters as follows. T_0 is the theory of differential fields of characteristic 0. T is the model completion, theory of differential closed fields. It is ω-stable; this will be used only incidentally, via B.1.4. It has elimination of imaginaries. It

is stable so that every definable set (indeed *every* set) is stably embedded. $C = \tilde{C}$ is the equation $Dx = 0$. Q is the solution set to a linear differential equation. The torsor P in that case can be taken to be orbit of $Aut(\mathbb{U}/F, C)$ on the set of bases, an open subset of Q^n; the opposite group is the subgroup of elements $M_n(C)$ preserving P and the action of $Aut(\mathbb{U}/F, C)$ on P, where $M_n(C)$ is the group of $n \times n$ matrices with coefficients from C, acting on V^n by matrix-vector multiplication.

For Matzat's theory, T_0 is the theory of differential fields of characteristic $p > 0$, endowed with a stack of Hasse derivations D_n. C is the ω-constructible sets $D_1 x = 0, D_2 x = 0, \cdots$. Q is the solution set to a system of linear differential equations. T_0 has again a model completion; over $F_p(t)$ it is equivalent to the theory of separably closed fields. It is stable, with EI; cf. [6].

B.1. Background. Let T be a complete first-order theory. We make two assumptions on T of a notational rather than substantial nature; they can be achieved in general by a canonical redefinition of the language, without changing the category of models or the automorphism group. Quantifier elimination is achieved by viewing every definable set as constructible; elimination of imaginaries, by viewing every equivalence class as a kind of point. Both assumptions are true at the outset for differentially closed fields (in char. 0, or using Hasse derivations in positive characteristic).

Elimination of quantifiers (QE): Every formula is equivalent, in a model of T, to a quantifier-free one. If T_0 is the set of universal sentences of T, then T_0 automatically has a universal domain $\mathbb{U}$; it is a model of T. T is then called *the model completion of* T_0. In this context, the words "constructible" and "definable" mean the same thing.

Elimination of imaginaries (EI): Every definable set can be defined using a *canonical parameter*. This means that the definable set has the form $D_c = \{x : (x, c) \in D\}$, with $c \in P$, D, P 0-definable, and such that if $c_1 \neq c_2 \in P$ then $D_{c_1} \neq D_{c_2}$.

A third notion will need to be considered, though not assumed:

Stable embeddedness

(SE1) A constructible set $X \subset \mathbb{U}$ is called *stably embedded* if any constructible subset $Y \subset X$ is constructible over some $X_0 \subset X$.

In the presence of (QE) and (EI), (SE1) is equivalent to:

(SE2) for any tuples a, b from $\mathbb{U}$, if $dcl(a) \cap dcl(X) = dcl(b) \cap dcl(X) =_{def} e$ and a, b are $Aut(\mathbb{U}/e)$-conjugate, then a, b are $Aut(\mathbb{U}/X)$-conjugate.

(The proof is a straightforward modification of A1; cf. appendix to [3].)

Grace to the following lemma, we will avoid any assumption of stable embeddedness in the general first-order framework.

LEMMA B.1.1. *Let $\mathbb{U}$ be a saturated model of a first-order theory. Let D be a Σ-definable set over F. Then there exists a stably embedded Σ-definable set $\tilde{D}$ over F (the stably embedded hull of D) with $Aut(\mathbb{U}/D) = Aut(\mathbb{U}/\tilde{D})$.*

Proof. For simplicity (and without loss of generality, as one may add constants for F to the language) we assume $F = \emptyset$. Let $\tilde{D}$ be the union of all 0-definable sets D_0 such that $Aut(\mathbb{U}/D)$ fixes D_0. By definition $Aut(\mathbb{U}/D) \leq Aut(\mathbb{U}/\tilde{D})$, but $D \subset \tilde{D}$ so

$Aut(\mathbb{U}/D) \leq Aut(\mathbb{U}/D)$, i.e. they are equal. If $S \subset (\tilde{D})^l$ is definable, then $S = R_a$ is definable with a canonical parameter a. There exists a 0-definable D_0 with $a \in D_0$ and such that if $b \neq c \in D_0$ then $R_b \neq R_c$, and $R_b \subset (\tilde{D})^l$. If $\sigma \in Aut(\mathbb{U}/D)$ and $\sigma(b) = c$, then (as σ fixes $\tilde{D}$) , $R_c = \sigma(R_b) = R_b$; so $c = b$. Thus $Aut(\mathbb{U}/D)$ fixes D_0, so $a \in D_0 \subset \tilde{D}$. This shows that any definable relation on $(\tilde{D})^l$ is definable with parameters from $\tilde{D}$, i.e. $\tilde{D}$ is stably embedded. ∎

COROLLARY B.1.2. *Let $D \subset \mathbb{U}$ be Σ-constructible. Then $Aut(\mathbb{U}/D)$-conjugacy is an ω-constructible equivalence relation.*

Proof. By Lemma B.1.1, we may assume D is stably embedded. In this case, two elements a, b are $Aut(\mathbb{U}/D)$-conjugate iff for any constructible R and any tuple c of elements of D, one has $R(a, c) \equiv R(b, c)$. This shows immediately that $Aut(\mathbb{U}/D)$-conjugacy is ω-constructible. ∎

ω-constructible groups. Finally, we will mention without proof some background facts regarding definability of groups. By an ω-constructible group we mean a group whose universe is an ω-constructible set, and whose operations are constructible maps (maps whose graphs are constructible). A special case, call it a $\cap$-constructible group, is obtained as follows: G_1 is a constructible group, $\ldots G_n \leq \ldots \leq G_2 \leq G_1$ is a sequence of constructible subgroups, and $G = \cap_{n=1}^{\infty} G_n$.

B.1.3. If T is stable, every ω-constructible group is $\cap$-constructible. (There is a similar statement for homogeneous spaces.)

B.1.4. If T is ω-stable, every ω-constructible group is constructible.

B.1.5. If T is the theory of algebraically closed fields, every ω-constructible group is an algebraic group.

See Poizat's book [18] for these. B.1.3 is proved in [9], Theorem 2, and the Remark following it; B.1.4 is an immediate corollary. By an insight of van den Dries, B.1.5 is a corollary of Weil's group chunk theorem (and an auxiliary result of Serre in positive characteristic). See also [9], §4.

The applications to Picard-Vessiot theory require an easier special case, where the ω-constructible group is known in advance to be a subgroup of a certain algebraic group. In this case B.1.4 is due to Poizat (cf. [18]), while B.1.5 is immediate from Tarski's quantifier-elimination and the fact that constructible subgroups are closed.

B.2. Definition of internality

DEFINITION. D is *C-internal* if there exists a definable $V \subset C^k$ and a definable *surjective* map $V \to D$. The surjective map in question may require parameters. To emphasize this, let us say that D is *C-interpreted over F* if C, D are F-definable, and there exist F-definable V, f with $V \subset C^k$ and $f : V \to D$ surjective.

The reason for the terminology is that f allows to interpret D inside the induced structure on C, with universe $V/Ker(f)$.

The relation between a C-internal set and a C-interpreted set is like the relation between an abstract algebraic variety and an embedded affine or projective variety.

EXAMPLE. The affine line over an algebraically closed field. As an abstract algebraic variety, it has automorphisms over k. The appropriate model-theoretic presentation (with the same automorphism group) is a two-sorted one (k, V), where V has the structure of a (one-dimensional) k-affine space, but no distinguished basis. In this structure, V is k-internal, but not k-interpreted.

EXAMPLE. In a universal domain for differential fields, Robinson's quantifier elimination shows that the constants C have the structure of an algebraically closed field, and no additional structure (the derivation is of no use on C). Any linear Kolchin closed set V, being a finite-dimensional vector space over C, is C-internal; it suffices to fix a basis to obtain a surjective definable map $C^n \to V$. V is C-interpreted over F iff V has a basis of F-rational points.

LEMMA B.2.1. *Let C be an ω-constructible set in $\mathbb{U}$. Assume C has the structure of an algebraically closed field, and no additional structure: every constructible relation is constructible in the Zariski sense. Let G be a C-internal ω-constructible group. Then G can be given the structure of an algebraic group $\underline{G}$ over k. Moreover every constructible subset of G^n is constructible in the sense of $\underline{G}$.*

Proof. When G is *C-interpreted*, this is B.1.5. When it is only C-internal, there exist a family of constructible group isomorphisms $f_a : G \to H$, where H is C-interpreted. By the above, H has the structure of an algebraic group over C. The maps $f_a f_b^{-1}$ are isomorphisms of this algebraic group over C. Thus the algebraic groups structure $G(a)$ on G obtained by pulling back that of H, via f_a , does not actually depend on a. Let $\underline{G}$ be their common value. Any constructible relation on G is mapped via f_a to a constructible relation on H, hence is Zariski constructible in $\underline{G}$. ∎

B.3. Internality and Galois groups of constructible sets

THEOREM B.1. *Let $\mathbb{U}$ be a universal domain for a theory T with elimination of quantifiers and elimination of imaginaries.*

Let Q be a definable set, internal to the Σ-definable set C. (Assume both are defined over a substructure F of $\mathbb{U}$.)

(1) There exists an ω-constructible group G, and a constructible action of G on Q (both defined over F), such that G is isomorphic to $Aut(Q/C, F)$ as a permutation group on Q.

(2) G is C-internal.

(3) There exists an ω-constructible G-torsor P, an ω-constructible group H (defined over $F \cup C$), such that $Aut(\mathbb{U}/P, C, F) = Aut(\mathbb{U}/Q, C, F)$, and $H = Aut_G(P)$.

(4) $Aut(\mathbb{U}/F, C) \subset Aut(\mathbb{U}/F, H)$. (So that H is interpreted over F in the stably embedded hull $\tilde{C}$ of C.)

(5) G is F-constructible; it is unique up to a unique F-constructible isomorphism. P is $F, \tilde{C}$-constructible, and is unique up to an $F, \tilde{C}$-constructible isomorphism of G-torsors.

EXPLANATIONS.

(1) $Aut(\mathbb{U}/A) = \{\sigma \in Aut(\mathbb{U}) : (\forall a \in A)\sigma(a) = a\}$.

$Aut(Q/C) = Aut(\mathbb{U}/F, C)/Aut(\mathbb{U}/Q, C)$; it acts faithfully on Q.

(2) A G-torsor is a set P together with a regular action of G on P (a faithful transitive action without fixed points of nonidentity elements).

(3) $H = Aut_G(P)$ is the group of isomorphisms of P as a G-torsor; i.e. the permutations of P commuting with the elements of G. It is called the opposite group (relative to P). Any element $p \in P$ gives an isomorphism $G \to H$, mapping $g \to h^{-1}$ when $g(p) = h(p)$.

Proof of Theorem B.1. By definition of internality, there exists a definable $V \subset C^k$ and a definable surjective map $g_e : V \to Q$. We may take e to be a canonical parameter for (V and for) g_e. Let $P = Aut(\mathbb{U}/F, C)\, e$ be the orbit of e under $Aut(\mathbb{U}/F, C)$. Denote by $\equiv_C$ the relation of $Aut(\mathbb{U}/F, C)$-conjugacy. By B.1.2, $\equiv_C$ is ω-constructible. P is a class of $\equiv_C$, hence is also ω-constructible.

If $\sigma \in Aut(\mathbb{U}/F, C)$ fixes e, then (as g_e is surjective) it must fix Q pointwise. But then for any $e' \in P$, the graph of $g_{e'}$, a subset of $Q \times C^k$, is also fixed by σ (pointwise, hence as a relation). Since e' is a canonical parameter, $\sigma(e') = e'$. Thus the stabilizer of e in $Aut(\mathbb{U}/F, C)$ fixes all of P. By definition of P, $Aut(\mathbb{U}/F, C)$ is transitive on P. Thus:

(1) $Aut(\mathbb{U}/F, C)$ acts transitively on P; and if $\sigma \in Aut(\mathbb{U}/F, C)$ fixes one point of P, it fixes them all.

Consider the quaternary relation R on P:

$$R(x, y, u, w) \text{ iff } (x, u) \equiv_C (y, w).$$

R is ω-constructible by B.1.2; but I claim it is actually constructible (relative to P), i.e. it coincides on P^4 with a constructible relation. Indeed for any $x, y \in P$, there exists (according to (1)) a unique σ with $\sigma(x) = y$. Thus $(x, u) \equiv_C (y, w)$ iff one has, for this σ, $\sigma(u) = w$. So

$$(x, y, u, w) \notin R \text{ iff } (\exists w' \in P) R(x, y, u, w') \,\&\, w' \neq w).$$

The projection of an ω-constructible relation in a universal domain is ω-constructible (appendix A); so $\neg R$ is ω-constructible, as well as R; thus they are both relatively constructible.

Let $H = Aut_{Aut(\mathbb{U}/F,C)}(P) = \{h \in Sym(P) : (\forall \sigma \in Aut(\mathbb{U}/F, C))\, \sigma h = h\sigma\}$. By (i), the action of $Aut(P/C) = Aut(\mathbb{U}/F, C)/Aut(\mathbb{U}/F, P, C)$ on P is isomorphic to the action of $Aut(P/C)$ on itself by left-translation; so H is isomorphic to $Aut(P/C)$ acting on itself by right translation. Thus

(2) H acts transitively on P, without fixed points of nontrivial elements.

Thus $(x, h(x)) \mapsto h$ gives a well-defined, surjective map $P^2 \to H$; the kernel of this map is the equivalence relation $\equiv_C$ on P^2. Since we have shown that this relation is constructible, by elimination of imaginaries EI, $P^2/\equiv_C$ is constructibly isomorphic to an ω-constructible set; and we may identify it with H.

Similarly, let $G = Aut_H(P)$. Using (2) in place of (1), $(x, gx) \mapsto g$ is well-defined and surjective; and G coincides with the image of $Aut(\mathbb{U}/F, C)$ in $Sym(P)$. (x, y),(u, w) have the same image in G iff for some $g \in G$, $y = gx, w = gu$, iff $(x, u) \equiv_C (y, w)$ iff

$R(x,y,u,w)$. So G can be identified with the ω-constructible set $(P^2)/R$. The actions of G, H on P are also seen to be ω-constructible (their graph is R, read in different ways).

As for the action of G on Q, for $g \in G$, $c, d \in Q$,

$$g(c) = d \text{ iff } (\exists a, b \in P)(g(a) = b,\ (a,c) \equiv_C (b,d))$$

and also

$$g(c) \neq d \text{ iff } (\exists a, b \in P, d' \in Q)(g(a) = b,\ (a,c) \equiv_C (b,d')\, d \neq d')$$

so the action is constructible.

We have shown (1-3); (4) follows from the fact that $H, Aut(\mathbb{U}/F, C)$ commute.

G was defined using P; P is c-constructible, where c is not necessarily in F. To clarify this write $G = G_c$. We also found an isomorphism $i_c : G_c \to Aut(Q/C)$. Now if the choice of c is changed to c', we have $i_{c'} : G_{c'} \to Aut(Q/C)$, and composing, we get $i_{c,c'} = i_{c'}^{-1} \circ i_c : G_c \to G_{c'}$. This isomorphism $G_c \to G_{c'}$ is constructible: $i_{c,c'}(g) = g'$ iff $(\forall y \in Q)(g(y) = g'(y))$. On $\cup_c \{c\} \times G_c$ we have an equivalence relation, identifying (c, g) with $(c', i_{c,c'}(g))$; the quotient is an F-definable group, isomorphic to any of the G_c. Thus G could be taken F-definable. The uniqueness is clear, using again the action on Q.

P was the orbit of e under $Aut(\mathbb{U}/F, C) = Aut(\mathbb{U}/F, \tilde{C})$. Let P_0 be the orbit of e under $Aut(\mathbb{U}/F)$. As $\tilde{C}$ is stably embedded, for $e, e' \in P_0$ we have $e \equiv_C e'$ iff $dcl(Fe) \cap dcl(F, \tilde{C}) = dcl(Fe') \cap dcl(F, \tilde{C})$. Thus P is the orbit of e under $Aut(\mathbb{U}/C_0)$ with $C_0 = dcl(Fe) \cap dcl(F, \tilde{C})$, so it is $F, \tilde{C}$-definable. If P, P' are two torsors with the same properties, we have (3) $Aut(\mathbb{U}/P, C, F) = Aut(\mathbb{U}/Q, C, F) = Aut(\mathbb{U}/P', C, F)$. If $e \in P$, then $Aut(\mathbb{U}/C, F, e)$ fixes P and hence P'; so an element e' of P' can be written $e' = h(e, \tilde{c})$ with h an F-definable function and $\tilde{c} \in \tilde{C}$. Applying $Aut(P \cup P'/C)$, we see that $x \mapsto h(x, \tilde{c})$ carries P bijectively to P', commuting with G. ∎

B.3.1. A supplementary lemma. The geometric theory above translates to results about automorphism groups of particular structures only after one knows that the torsors P of Theorem B.1 are defined over the base structure. The need for this additional point, and its model theoretic proof, were first seen by Poizat in the original Picard-Vessiot context, and extended by Pillay to a more general context of definable automorphism groups in differentially closed fields.

Here we will assume the conclusion of B.1.4 (at least for G itself).

LEMMA B.3.1. *In Theorem B.1, assume in addition that every ω-constructible group is constructible. Also assume $\tilde{C}(F)$ is existentially closed in $\tilde{C}(\mathbb{U})$. Then the torsor P can be taken to be (ω-) constructible over F. If so chosen, it is unique up to a F-definable isomorphism.*

Proof. We may assume $C = \tilde{C}$. Say $P = P_c$ of Theorem B.1 is defined over $F(c)$, $c \in \tilde{C}$. The fact that P_c is a G-torsor and $P_c \subset dcl(F, C)$ can be stated by a first-order formula $\phi(c)$; as $C(F)$ is existentially closed, one can find a witness in F. Similarly if P, P' are two such torsors over F, we know by B.3.1 that they are isomorphic over $F \cup C$, hence again the parameter can be taken in $F \cup C(F)$. ∎

This lemma permits one, given F, Q, C, to define an associated extension E of F, the Picard-Vessiot extension; it is the extension $F(e)$ for $e \in P$. The uniqueness and homogeneity of P show that the extension does not depend on the choice of P or of $e \in P$.

While in the model theoretic presentation these last lines appear as an afterthought, in the Kolchin-style approach to Picard-Vessiot they are essential to the very definition of the Galois group. For difference fields, the existential closure hypothesis of B.3.1 can fail even when $C(F)$ is an algebraically closed field; but it holds asymptotically when σ is replaced by $\sigma^{n!}$, $n \to \infty$. This is related to the appearance, in the theory of Singer and Van der Put, of a product of n domains permuted cyclically by σ as the "Picard-Vessiot *ring*".

B.4. Connection to Picard-Vessiot. The group G defined above is a definable object, i.e. a geometric object. How does it relate to the automorphism group of particular structures? (A substructure is a subset E of $\mathbb{U}$ closed under constructible functions.)

Proposition B.4.1. *Assume C, P, Q of Theorem B.1 are defined over F, and $E = F(e)$ for some $e \in P$. Then $\tilde{C}(E) = \tilde{C}(F)$, and $Aut(E/F) = G(E)$, the set of E-rational points of G. $Aut(E/F)$ is also isomorphic to $H(F)^{op}$. (There is no difference between $H(F)$ and $H(F)^{op}$ as abstract groups; we use the notation to emphasize that $H(F)$, $G(E)$ can give different subgroups of $Sym(E)$.)*

Proof. If $a \in \tilde{C}(E)$, then by definition of E, $a = f(e)$ for some constructible function f, defined over F. Applying $Aut(\mathbb{U}/F, C)$ we see that $a = f(e')$ for any $e' \in P$, so a is F-definable, hence $a \in F$.

Let $\theta \in Aut(E/F)$; say $\theta(e) = e'$. Then $e, e' \in P$ so $e \equiv_{F,C} e'$; so there exists $\sigma \in Aut(\mathbb{U}/F, C)$, $\sigma(e) = e'$. As $E = F(e)$, $\theta = \sigma|E$. If $\sigma \in Aut(\mathbb{U}/F, C, P)$ then $\sigma(e) = e$ and hence $\sigma|E = Id_E$; so we may view σ as an element of the quotient group $Aut(P/F, C)$. Conversely, if $\sigma|E = Id_E$, then σ fixes a point of P and hence fixes P (by (1) of Theorem B.1). This identifies $Aut(E/F)$ with a subgroup of $Aut(P/F, C)$, equivalently of G, consisting of elements carrying e to an element of $Q(E)$. If $g(e) = e' \in E$, then g is the unique element of G solving this equation, so $g \in F(e, e') = E$. Conversely if $g \in G(E)$, then $g(e) \in F(e, g) = E$.

Similarly, the action of H on P induces a regular action of $H(E)$ on $P(E)$. Thus $G(E) = H(E)^{op}$. However, $H \subset dcl(\tilde{C}, F)$; so $H(E) = H(F)$. ∎

Remark B.4.2. ω-constructible subgroups of H, defined over F, correspond naturally to F-definable equivalence relations on P, or equivalently to isomorphism classes of F-definable surjective maps $f : P \to P'$. Given $H_1 \leq H$, the equivalence relation is H_1-conjugacy. Conversely given E, as G acts transitively on P and leaves invariant E and the action of H, $H_1 = \{h \in H : h(e)Ee\}$ does not depend on the choice of $e \in P$; and clearly E coincides with H_1-conjugacy.

Remark B.4.3. Fix $e \in E$. Then the standard algebra-geometry duality maps subextensions E_1 of E with $F \leq E_1 \leq E$ bijectively to isomorphism classes of F-definable quotients of P. ($f : P \to P'$ corresponds to the intermediate extension $F(f(e))$.)

Composing the correspondences of B.4.2 and B.4.3, we obtain a a 1-1 correspondence between F-Zariski closed subgroups of $H(F)$, and subextensions of E/F. *But this correspondence is not canonical.* Vessiot, p. 157: "Ce groupe (our H) s'appelle le *groupe de transformations* ou *groupe de rationalité* de l'équation ... comme, du reste, rien ne précise à priori le système fondamental (our e) ... (H) n'est défini qu'à une transformation linéaire homogène près (...) ."

On the other hand if one is willing to use the isomorphic group $G(E)$ in place of $H(F)$, the correspondence between subextensions and a certain class of constructible subgroups becomes canonical:

Remark B.4.4. G, H are E-isomorphic, so $G(E)$ is isomorphic to $H(E) = H(F)$ (cf. Explanation 3 of B.1). Two E-definable isomorphisms $\psi : G \to H$ differ by conjugation by an element of $H(E) = H(F)$. Moreover, any such ψ takes the family of E-definable subgroups of G to the family of F-definable subgroups of H. Indeed if K is an E-definable subgroup of G, then $\psi(E)$ is an E-definable subgroup of H; but then if d is a canonical parameter for $\psi(E)$ (cf. EI), then $d \in \tilde{H} \subset \tilde{C}$ by Theorem B.1(4) (suppressing F from notation). By B.4.1, $\tilde{C}(E) = \tilde{C}(F)$ so $d \in F$. Thus $\psi(E)$ is F-definable.

Thus if $Sb_F(H)$ (resp. $Sb_E(G)$) denote the families of ω-constructible subgroups of H (resp. G) defined over F (resp. E), any of these isomorphisms ψ carries $Sb_F(H)$ to $Sb_E(G)$.

Proposition B.4.5. *There is a canonical 1-1 correspondence between elements of $Sb_E(G)$ and substructures E_1 of E containing F:*

$$E_1 \mapsto Aut(P/C, E_1),$$
$$G_1 \mapsto \{e_1 \in E : (\forall g \in G_1) g(e_1) = e_1\}.$$

Proof. The canonicity of the correspondence is evident. To prove that it is 1-1 one is allowed to fix $e \in E$; then use B.4.2, B.4.3 and verify the match. ∎

B.5. Complement: Galois theory of ω-constructible sets. The definability theorem B1 presented above is somewhat weaker than the original presentation, as only constructible sets are allowed. We present here another version that permits also ω-constructible sets. We require stable embeddedness, but still very far from a global stability assumption. The construction includes Matzat's positive characteristic Galois group; but not his analog of B.3.1!

Moreover, it is natural to work in an arbitrary universal domain for a universal theory T_0, not necessarily having a comprehensible completion. So we no longer assume QE (cf. [11]).

If D is an ω-constructible set, D is C-internal if there exists an ω-constructible $V \subset C^k$ and a constructible *surjective* map $V \to D$.

A weak form of elimination of imaginaries can be achieved here: (EI0) the quotient of a constructible set by a constructible equivalence relation is constructibly isomorphic to a constructible set. (Adding such a quotient as a new sort preserves the properties of a universal domain. We could even, but will not, do this for an ω-constructible equivalence relation E; in this case equality on S/E may not be a constructible relation.)

REMARK B.5.1. Lemma B1.1 holds in the general context too, if sufficiently strong assumptions of elimination of imaginaries are made. The strong version needed is this: Let S, T be ω-constructible subsets of $\mathbb{U}^k, \mathbb{U}^l$, and let $R \subset S \times T$ be constructible. For $a \in S$, let

$$R_a = \{y \in T : (a, y) \in R\}.$$

Then there exist S' and a constructible $R' \subset S' \times T$, such that for each $a \in S$, there exists a unique $a' \in S'$ with $R'_{a'} = R_a$.

(This is valid in stable theories with EI.)

THEOREM B.1'. *Let $\mathbb{U}$ be a universal domain for T_0. Assume $\mathbb{U}$ has (EI0). Let Q be an ω-constructible set, internal to the $Aut(\mathbb{U})$-invariant set C. Assume C and $Q \cup C$ are stably embedded in the sense (SE2). Say all are defined over F, and write dcl for dcl_F etc.*

(1) There exists an ω-constructible group G, and a constructible action of G on Q (both defined over F), such that G is isomorphic to $Aut(Q/C)$ as a permutation group on Q.

(2) G is C-internal.

(3) There exists an ω-constructible G-torsor P, an ω-constructible group H (defined over $F \cup C$), such that $dcl(P, C) = dcl(Q, C)$, and $H = Aut_G(P)$.

(4) $H \subset dcl(C)$.

(5) G is F-constructible; it is unique up to a unique F-constructible isomorphism. P is F, C-constructible, and is unique up to an F, C-constructible isomorphism of G-torsors.

NOTE. In stable theories, SE2 is valid for any ω-constructible set (using canonical bases; cf. proof of this theorem in [9]).

Proof. Let g be a definable map, such that $Q \subset g(C^k)$. We may find an ∞-definable $C' \subset C^k$ such that $g(C') = Q$. If e_0 is a parameter for g, let $E = dcl(e_0) \cap dcl(Q \cup C)$. Then by (SE2) for $C \cup Q$, $r = tp(e_0/E)$ implies $tp(e_0/Q \cup C')$; so for $a \in C'$,

$$g(a) = b \text{ iff } b \in Q \,\&\, (\exists w)(r(w) \,\&\, g_w(a) = b).$$

Thus g (or rather some function agreeing with g on C') can be defined over E; write from now $g = g_e$, $e \in E \subset dcl(C \cup Q)$. Let $C_0 = dcl(e) \cap dcl(C)$, and

$$P = \{e' : tp(e'/C_0) = tp(e/C_0)\}.$$

Using (SE2) for C, $Aut(\mathbb{U}/C)$ is transitive on P. On the other hand if $\sigma \in Aut(\mathbb{U}/C)$ fixes $e \in P$, then σ fixes Q, and hence P. We thus obtain (1) of B.1.

If $e, e' \in P$ and $b, b' \in Q$, let $\sigma \in Aut(\mathbb{U}/C)$, $\sigma(e) = e'$. Then

$$\sigma(b) = b' \text{ iff } (\exists y \in C')(b = g_e(y) \,\&\, b' = g_{e'}(y)).$$

Thus $Aut(\mathbb{U}/C)$-conjugacy is an ω-constructible equivalence relation on $P \times Q$ (and as $P \subset dcl(C \cup Q)$, also on P^2). The rest of the proof is identical to that of B.1.

REMARK B.5.2. In Theorem B.1, the hypothesis of internality may obviously be weakened to: Q is $\tilde{C}$-internal. In this form it is optimal; if Q is not $\tilde{C}$-internal, then there

exist models $\mathbb{U}$ such that $Aut(Q/C)$ has larger cardinality than $\mathbb{U}$, so that it cannot be interpretable.

References

[1] D. Bertrand, *Minimal heights and polarizations on group varieties*, Duke Math. J. 80 (1995), 223–250.

[2] A. Buium, *Uniform bounds for generic points of curves in tori*, J. Reine Angew. Math. 469 (1995), 211–219.

[3] Z. Chatzidakis and E. Hrushovski, *Model theory of difference fields*, Trans. AMS 351, 2997–3071.

[4] G. Cherlin, *Algebraically closed commutative rings*, J. Symbolic Logic 38 (1973), 493–499.

[5] E. Compoint and M. Singer, *Computing Galois groups of completely reducible differential equations*, J. Symbolic Comput. 28 (1999), 473–494.

[6] F. Delon, *Idéaux et types sur les corps séparablement clos*, Supplément au Bull. SMF, Mémoire 33, Tome 116 (1988).

[7] L. van den Dries and K. Schmidt, *Bounds in the theory of polynomial rings over fields. A nonstandard approach*, Invent. Math. 76 (1984), 1, 77–91.

[8] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, 1986.

[9] E. Hrushovski, *Unidimensional theories are superstable*, Ann. Pure Appl. Logic 50 (1990), 117–138.

[10] E. Hrushovski, *Strongly minimal expansions of algebraically closed fields*, Israel J. Math. 79 (1992), 129-151.

[11] E. Hrushovski, *Simple theories and the Lascar group*, preprint.

[12] J. E. Humphreys, *Linear Algebraic Groups*, Grad. Texts in Math., Springer-Verlag, 1987.

[13] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[14] D. Marker, M. Messmer and A. Pillay, *Model Theory of Fields*, Lecture Notes in Logic 5, Springer, 1996.

[15] F. Marotte, thèse, Paris 1898.

[16] D. Masser, *Linear relations on algebraic groups*, in: New Advances in Transcendence Theory, A. Baker (ed.), Cambridge University Press, Cambridge, 1988, 248–262.

[17] E. Picard, *Traité d'analyse*, troisième édition, Tome III, Gauthier-Villars, 1928.

[18] B. Poizat, *Groupes Stables*, Nur Al-Mantiq Wal-Ma'rifah, Lyon, 1987.

[19] J.-P. Serre, *Algebraic Groups and Class Fields*, Springer-Verlag, New York, 1975.

[20] J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[21] M. F. Singer, *Liouvillian solutions of nth order homogeneous linear differential equations*, Amer. J. Math. 103 (1981), 661–682.

[22] M. F. Singer, *Moduli of linear differential equations on the Riemann sphere with fixed Galois groups*, Pacific J. Math. 106 (1993), 343–395.

[23] E. Vessiot, *Méthodes d'intégration élémentaires*, in: Encyclopédie des Sciences Mathématiques Pures et Appliquées, Jules Molk (ed.), Tome II (3ème vol.), Gauthier-Villars, Paris, and B.G. Teubner, Leipzig, 1910; reprinted by Éditions Jacques Gabay, 1992.