ILLINOIS JOURNAL OF MATHEMATICS
Volume 42, Number 4, Winter 1998

DIFFERENTIAL GALOIS THEORY I

ANAND PILLAY

1. Introduction

This paper is devoted to an extension of Kolchin's Galois theory of differential fields [8], [9], [10], [11]. When we say an "extension" of Kolchin's theory, we mean that a *larger* class of differential field extensions $F < K$ is subsumed by our theory. Kolchin's theory was itself an extension, in the context of differential algebra, of the classical Picard-Vessiot theory. Kolchin called his differential field extensions *strongly normal*. In the Picard-Vessiot theory, the Galois groups have a natural structure as *algebraic* matrix groups over the constants (namely algebraic subgroups of $GL(n, C)$), where C denotes the constants of the differential field F). In Kolchin's theory, the Galois groups correspond to (not necessarily linear) algebraic groups in the constants, and moreover any algebraic group can arise. Our approach is quite simple-minded, and consists of replacing the role of the constants in Kolchin's definition, by an arbitrary differential algebraic set X, to obtain the notion of an X-strongly normal extension K of F. The Galois groups that arise have naturally the structure of *finite-dimensional differential algebraic groups* (of which algebraic groups in the constants are a special case). If G is such a Galois group, then the Galois correspondence is between differential fields L between F and K, and differential algebraic subgroups of G. This is carried out in Section 2, where we also give an analogue of Bialynicki-Birula's approach ([1]). In Section 3 we present an analogue of Kolchin's "G-primitive extensions" characterization of strongly normal extensions, where we make use of the embeddability of differential algebraic groups in algebraic groups, as well as of "constrained Galois cohomology". In Section 4 we show that any finite-dimensional differential algebraic group arises as the Galois group of some "generalised" strongly normal extension $F < K$ (for some F, K). In Section 5, we point out that we *do* obtain a larger class of extensions in our theory, essentially due to the fact that there are finite-dimensional differential algebraic groups which are *not* isomorphic (as differential algebraic groups) to algebraic groups in the constants. In a sense our work contains a unification of the two grand themes of Kolchin's work: differential Galois theory, and the theory of differential algebraic groups.

Various "modern" treatments of Kolchin's theory have recently appeared (such as [13]). In the present paper model-theoretic language and methods are used throughout, basically because we find this the most efficient language in which to develop and

Received October 10, 1997.
1991 Mathematics Subject Classification. Primary 03C60; Secondary 12H05.
Supported in part by grants from the National Science Foundation.

express the general theory. A summary of the model-theoretic approach occurs below.

This paper ties together various important pieces of work in model theory. The recognition that in suitable model-theoretic contexts, automorphism groups have the structure of definable groups, is due to Zilber [24], and later Hrushovski [6]. Using such ideas, Poizat, in his fundamental paper "Une theorie de Galois imaginaire" [22], gave a model-theoretic treatment of Kolchin's differential Galois theory. He even notes that any definable set can replace the role of the constants, although he does not give any explicit definition of "generalised" strongly normal extensions (and in fact it was not so easy for us to come up with the "right" definition). One thing missing in Poizat's work was an explication of the "G-primitive extensions" part of the Kolchin theory. In [20], this was carried out, and the proof generalises to yield Proposition 3.2 in the present paper. The result in Section 4 of the present paper (that any finite-dimensional differential algebraic group is a Galois group) is new. In the background to the work here lies the identification of groups definable in differentially closed fields with differential algebraic groups, proved in [17]. In any case, in this paper we pull together the various strands mentioned above into a coherent account of a differential Galois theory which generalises and extends the classical Picard-Vessiot theory and the Kolchin theory. Somewhat deeper model-theoretic results will appear in [18], where it is shown that superstable differential fields are closed with respect to generalised strongly normal extensions. Also in [16], we obtain some results around the inverse problem for our new differential Galois theory.

I would like to thank Bruno Poizat and Christine Charretton for their generous hospitality during May 1994 when this work was begun (and when I was an invited Professor at Universite Lyon-Claude Bernard, whom I also thank).

We will work throughout with ordinary differential fields of characteristic 0, namely fields F of characteristic 0, equipped with a distinguished derivation δ. For $a \in F$ we will often write a' in place of $\delta(a)$. Everything we say extends to the context of fields with finitely many commuting derivations. We will usually just write F for the field equipped with the derivation, so $F < K$ means that that K is a *differential field* extension of F. By an automorphism of a differential field we mean a field automorphism which respects the derivation.

$\mathcal{U}$ will denote a "universal" differential field of some uncountable cardinality κ. What this means is that

(i) any differential field of cardinality $< \kappa$ is embeddable in $\mathcal{U}$,
(ii) whenever $F < \mathcal{U}$, $F < K$ and both F and K have cardinality $< \kappa$, then there is an embedding of K into $\mathcal{U}$ over F,
(iii) whenever $F < K_1 < \mathcal{U}$, $F < K_2 < \mathcal{U}$, F, K_1 and K_2 have cardinality $< \kappa$, and f is an isomorphism between K_1 and K_2 over F, then f extends to an automorphism of $\mathcal{U}$.

In fact, in (ii) and (iii), it is enough if F has cardinality $< \kappa$ and K, K_1, and K_2 are finitely generated over F.

In the remainder of this paper F, K etc. will denote differential subfields of $\mathcal{U}$ of cardinality $< \kappa$. If F is such and Y is some subset of $\mathcal{U}$ or even of $\mathcal{U}^n$, $F\langle Y\rangle$ denotes the differential subfield of $\mathcal{U}$ generated by F and the coordinates of all points in Y. Note that $F\langle Y\rangle$ may very well have cardinality κ. We will say that K is finitely generated over F if $K = F\langle a\rangle$ for some finite tuple a of elements of $\mathcal{U}$.

From the point of view of model theory, $\mathcal{U}$ is precisely a saturated, differentially closed field of cardinality κ. We explain now what this means, assuming the rudiments of first order logic. For more detailed background on model theory and the model theory of differential fields, as well as attributions of basic results, see [21], [5] and [15].

The first order language we work in contains symbols for the binary operations $+, -, .$, for the distinguished elements 0, 1 and for the unary function δ (and nothing else). From now on, by a formula, we mean a first order formula in this language. DCF_0 (the theory of differentially closed fields of chararacteristic 0) is the set of first order sentences in this language consisting of

(i) the axioms for differential fields of characteristic 0,
(ii) axioms expressing that whenever $P(X)$, $Q(X)$ are differential polynomials (in the single differential indeterminate X, with coefficients in some differential field) and order$(P) >$ order(Q), then the system $P(X) = 0$, $Q(X) \neq 0$ has a solution.

By definition, a differentially closed field (of characteristic 0) is precisely a model of DCF_0, namely a differential field of characteristic 0 in which (ii) holds.

The central fact is:

FACT 1.1. *DCF_0 is complete and has quantifier elimination.*

Completeness means that if F_1, F_2 are differentially closed fields then any (first order) sentence of the language is true in F_1 iff it is true in F_2. Quantifier elimination means that if $\phi(x_1, \ldots, x_n)$ is any formula then there is a formula $\psi(x_1, \ldots, x_n)$ without quantifiers, such that for any differentially closed field F,

$$F \models \forall x_1, \ldots, x_n(\phi(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n)).$$

By a *definable set* in F (F a differential field), we mean a subset X of F^n (some n) such that, for some formula $\phi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ and tuple $(b_1, \ldots, b_m)$ from F, $X = \{(a_1, \ldots, a_n) \in F^n\colon F \models \phi(a_1, \ldots, a_n, b_1, \ldots, b_m)\}$ If A is a subset of F and ϕ and the tuple of b's can be chosen from A we say that X is A-definable in F. By a *differential algebraic* subset of F^n, we mean the zero-set of some finite number of differential polynomials in n differential indeterminates, with coefficients from F. Again if the coefficients can be chosen from a subset A of F, we say the differential

algebraic set is *defined over A* or *A-definable*. Clearly a differential algebraic set is a special case of a definable set. On the other hand, Fact 1.1 implies:

FACT 1.2. *If F is differentially closed, $A \subseteq F$ and $X \subseteq F^n$ is a set definable over A in F, then X is a finite Boolean combination of differential algebraic subsets of F^n, each defined over A.*

Let $\mathcal{U}$ be a universal diferential field. It turns out that $\mathcal{U}$ is differentially closed, and moreover κ-saturated. The latter means that if A is a subset of $\mathcal{U}$ of cardinality $< \kappa$ and $\{X_i: i \in I\}$ is a family of A-definable subsets of $\mathcal{U}^n$ every finite subset of which has nonempty intersection, then $\cap\{X_i: i \in I\} \neq \emptyset$.

All elements and tuples we consider will come from $\mathcal{U}$. For $\phi(x_1, \ldots, x_n)$ a formula, and $a_1, \ldots, a_n$ elements of $\mathcal{U}$, we use $\models \phi(a_1, \ldots, a_n)$ to mean the formula ϕ is true of the tuple $(a_1, \ldots, a_n)$ in $\mathcal{U}$. By a definable set we will mean a $\mathcal{U}$-definable subset of $\mathcal{U}^n$ for some n. Quantifier elimination of DCF_0 implies that if $F \prec \mathcal{U}$ and F is differentially closed, then whenever X is a set definable over F, then $X \cap F^n \neq \emptyset$ (or in model-theoretic parlance, F is an elementary substructure of $\mathcal{U}$).

From now on we write a, b etc. for abitrary finite tuples of elements of $\mathcal{U}$. (Similarly, x, y etc. denote finite tuples of variables.) We may write $a \in F$ if every coordinate of a is in F. If $A \subset \mathcal{U}$, by $tp(a/A)$ we mean the set of formulas $\phi(x)$ (where x is a suitable tuple of variables) with parameters from A such that $\models \phi(a)$, or equivalently (identifying formulas with the sets they define), the set of A-definable sets containing a. p, q etc. are often used to denote such (complete) types. $tp(a/A)$ is said to be *isolated* if it contains a formula $\phi(x)$ such that whenever $b \in \mathcal{U}$ and $\models \phi(b)$, then $tp(b/A) = tp(a/A)$.

Definition 1.3. Let $F \prec F_1$. We say that F_1 is a differential closure of F if whenever $K \succ F$ and K is differentially closed, then there is an embedding of F_1 into K over F.

Given F there is always a differentially closed K containing F of the same cardinality, so the same is true of any differential closure of F.

FACT 1.4. *Any F has a differential closure, which is moreover unique up to F-isomorphism (although not necessarily unique as a differential subfield of $\mathcal{U}$). Any such differential closure F_1 of F has these features:*

(i) *For any $a \in F_1$, $tp(a/F)$ is isolated, and* tr.degree$(F\langle a\rangle/F)$ *is finite.*
(ii) *Whenever a, b are finite tuples from F_1 such that $tp(a/F) = tp(b/F)$ then there is an automorphism of F_1 over F which takes a to b.*

Often we let $\hat{F}$ denote some differential closure of F.

One can also consider sets which are *interpretable* in $\mathcal{U}$, that is sets of the form X/E where $X \subset \mathcal{U}^n$ is a definable set, and E is a definable equivalence relation on

X. Again the notion of such a set being defined over A makes sense. The following "elimination of imaginaries" result ([22]) shows that such "imaginary" definable sets can be identified with normal definable sets.

FACT 1.5. *Let Y be an interpretable set, defined over A. Then there is some A-definable set $Z \subseteq \mathcal{U}^n$ (for some n) and some A-definable bijection f between Y and Z.*

It should be noted that we have not equipped definable sets with any geometric structure. On the other hand, Kolchin [12] develops a theory of abstract differential algebraic varieties. This theory is developed in a more "natural" manner by Buium [2], [3]. In any case we have seen above the notion of "affine" differential algebraic subsets of $\mathcal{U}^n$. One can define various notions of differential polynomial functions and differential rational functions, and much as in algebraic geometry, construct a category of abstract differential algebraic varieties by piecing together "affine" differential algebraic sets along differential rational transition maps. A group object in this category is what is called a "differential algebraic group".There is a natural notion of such an object being "defined over F". Any such object will be naturally interpretable in $\mathcal{U}$, and so, by virtue of Fact 1.5, can be identified with a definable subset of $\mathcal{U}^n$, although in doing so the geometry may disappear. We do not really need to concern ourselves with such differential algebraic varieties, except to point out, that insofar as differential algebraic *groups* are concerned, nothing is lost by working in the (a priori nongeometric) category of definable sets. By a *definable* group we mean a group whose underlying set and group operation are both definable. The following is proved in [17].

FACT 1.6. *Suppose G to be an F-definable group. Then there is a unique differential algebraic group H, defined over F which is F-definably isomorphic to G.*

An important fact about any definable group G is that it has a unique smallest definable subgroup of finite index, which we call G^0, the connected component of G. (This corresponds to the connected component of a differential algebraic group, defined using the differential Zariski topology.)

In any case we will talk interchangeably about definable groups and differential algebraic groups.

If X is an F-definable set, then, in accordance with Kolchin's definitions, we define the *typical* δ-dimension of X to be $\max\{\text{tr.degree}(F\langle a\rangle/F)\colon a \in X\}$. (If for all $a \in X$, $\text{tr.degree}(F\langle a\rangle/F)$ is finite then there will be a maximum.) For brevity we will call a definable set with finite typical δ-dimension *finite-dimensional*. When this typical δ-dimension of X is infinite (so countable) it does not give much information. Better measures are given by various ordinal-valued model-theoretic dimension functions, or what we call "ranks". One such is Lascar's U-rank. Its definition depends on another crucial notion: independence (the analogue of algebraic disjointness in algebraic geometry).

Definition 1.7. Let A, B and D be subsets of $\mathcal{U}$. Let F be the differential field generated by D. We say that A is independent from B over D, if $F\langle A\rangle$ and $F\langle B\rangle$ are algebraically disjoint (or free) over F (as fields).

Definition 1.8. Let a be a tuple from $\mathcal{U}$, and $A \subseteq \mathcal{U}$. We inductively define $U(a/A) \geq \alpha$ (α an ordinal) by: $U(a/A) \geq \alpha + 1$ if there is $B \supseteq A$ such that a is not independent from B over A, and $U(a/B) \geq \alpha$; and for a limit ordinal β, $U(a/A) \geq \beta$ if $U(a/A) \geq \alpha$ for all $\alpha \leq \beta$.

We emphasize that in the next fact a, b etc. denote (finite) tuples from $\mathcal{U}$. Also $\oplus$ is Cantor's symmetric sum of ordinals.

FACT 1.9. (i) $U(a/A) < \omega^2$ *for all* a, A.

(ii) $U(a/F) < \omega$ *iff* $tr.deg(F\langle a\rangle/F) < \omega$.
(iii) *For* $A \subseteq B$, $U(a/A) = U(a/B)$ *iff* a *is independent from* B *over* A.
(iv) $U(a/B \cup b) + U(b/A) \leq U(a, b/A) \leq U(a/B \cup a) \oplus U(b/A)$.

If $p(x) = tp(a/A)$ we will also write $U(p)$ for $U(a/A)$.

If X is an A-definable set, then by $U(X)$ we mean $\max\{U(a/A)\colon a \in X\}$. This does not depend on the choice of A. In our situation (DCF_0) this maximum will exist. Moreover $U(X)$ will be finite just if X is finite-dimensional in the sense above. In general $U(X)$ may not so useful a notion, but if X happens to be a definable group, it is quite useful.

Definition 1.10. Suppose G is an A-definable group, with $U(G) = \alpha$. Let $a \in G$. We say that a is a generic point of G over A (and $tp(a/A)$ a generic type of G over A), if $U(a/A) = \alpha$.

FACT 1.11. *Let* G *be a definable group, defined over* A. *Then there are only finitely many generic types of* G *over* A (*namely there are finitely many generic points* $a_1, \ldots, a_n$ *of* G *over* A, *such that whenever* b *is a generic point of* G *over* A *then* $tp(b/A) = tp(a_i/A)$ *for some* $i = 1, \ldots, n$). *Moreover* G *is connected if and only if it has a unique generic type over* A.

Now $\mathcal{U}$ can also be considered as a universal domain for algebraic geometry. By an algebraic group we mean an algebraic group with respect to this universal domain. From the point of view of definability, an algebraic group will then be simply a group which is (quantifier-free) definable in $\mathcal{U}$ just using the field language $(+, ., 0, 1)$ and parameters from $\mathcal{U}$. The following in proved in [11]; another proof appears in [7].

FACT 1.12. *Let* G *be a connected algebraic group of* (*algebraic-geometrical*) *dimension* n. *Then, as a group definable in* $\mathcal{U}$, G *is connected and* $U(G) = \omega.n$.

$\mathcal{C}$ denotes the field of constants of $\mathcal{U}$, namely $\{a \in \mathcal{U}: a' = 0\}$. So $\mathcal{C}$ is a definable subset of $\mathcal{U}$ (defined over $\emptyset$). We have $U(\mathcal{C}) = 1$. $\mathcal{C}$ is also a universal domain for algebraic geometry (and it is worth remarking that any $\mathcal{U}$-definable set X which is a subset of $\mathcal{C}^m$ for some m, is a constructible set relative to the algebraically closed field $\mathcal{C}$). If G is an algebraic group defined over some $A \subseteq \mathcal{C}$, then note that $G(\mathcal{C})$ will be an algebraic group in the sense of the universal domain $\mathcal{C}$ as well as a group definable in $\mathcal{U}$. We call such an object an algebraic group in the constants. On the other hand if H is a definable group whose underlying set happens to be a subset of $\mathcal{C}^m$ for some m, then actually H will be of the form $G(\mathcal{C})$ for some algebraic group defined over $\mathcal{C}$. Such H is a special case of a finite-dimensional differential algebraic group. Finite-dimensional differential algebraic groups were studied in detail in [2].

In general, if X is a definable set, defined over F, then by $X(F)$ we mean the set of points of X all of whose coordinates are in F. In the special case where $X = \mathcal{C}$ we may also write $\mathcal{C}_F$ in place of $\mathcal{C}(F)$.

The model theoretic notions of the *definable closure* and the model theoretic *algebraic closure* have a simple meaning in the present context. We say that a is in the definable closure of A ($\mathrm{dcl}(A)$) if there is a formula $\phi(x)$ over A such that a is the unique element (or tuple) satisfying the formula $\phi(x)$ (or equivalently $\{a\}$ is A-definable). We say that a is in the algebraic closure of A ($\mathrm{acl}(A)$) if there is a formula $\phi(x)$ over A satisfied by a which has only finitely many solutions.

FACT 1.13. (*i*) $\mathrm{dcl}(A)$ *is the differential field generated by* A. (*ii*) $\mathrm{acl}(A)$ *is the (field-theoretic) algebraic closure of the differential field generated by* A.

Thus for any set Y contained in $\mathcal{U}$ (or even in $\mathcal{U}^n$), and any F, $\mathrm{dcl}(F \cup Y)$ will be $F\langle Y\rangle$.

Note that if $a \in \mathrm{dcl}(A \cup b)$ there will be an A-definable partial function $f(-)$ such that $f(b) = a$.

Finally we mention Kolchin's notion of strongly normal extensions. An isomorphic embedding of K into $\mathcal{U}$ will be called an *isomorphism* of K into $\mathcal{U}$. For $F < K$ we will say that such an isomorphism is over F it it fixes F pointwise.

Definition 1.14. Suppose $F < K$. Then K is a strongly normal extension of F if

(i) $\mathcal{C}_F$ is an algebraically closed field,
(ii) $\mathcal{C}_F = \mathcal{C}_K$,
(iii) K is finitely generated over F, and
(iv) whenever σ is an isomorphism of K into $\mathcal{U}$ over F, then $\sigma(K) \subseteq K\langle\mathcal{C}\rangle$.

Following Kolchin we will define $\mathrm{Gal}(K/F)$ to be not $\mathrm{Aut}(K/F)$ but the larger group $\mathrm{Aut}(K\langle\mathcal{C}\rangle/F\langle\mathcal{C}\rangle)$. Kolchin shows that this group has, naturally, the structure of an algebraic group in the constants.

2. Generalised strongly normal extensions

For a given differential field F, insofar as we are interested in developing a Galois theory for extensions K of F, it is natural to restrict one's attention to subfields K of some fixed copy $\hat{F}$ of a differential closure of F. As in Kolchin's approach, we will *not* build this into our definition, but rather deduce it from the definitions.

Definition 2.1. Let F be a differential field, X an F-definable set, and K a differential field containing F. Call K an X-strongly normal extension of F if the following hold:

(i) $X(F) = X(\hat{F})$ for some (any) differential closure $\hat{F}$ of F.
(ii) $\mathrm{dcl}(X \cup F) \cap K = F$.
(iii) K is finitely generated over F as a differential field,
(iv) for any isomorphism σ of K into $\mathcal{U}$ over F we have $\sigma(K) \subset K\langle X\rangle$

We will call K a generalised strongly normal extension of F if it is an X-strongly normal extension of F for some F-definable set X.

Remark 2.2. K is a C-strongly normal extension of F iff K is a strongly normal extension of F in the sense of Kolchin, Definition 1.14. The reason for this is that $\mathcal{C}_F = \mathcal{C}_{\hat{F}}$ iff $\mathcal{C}_F$ is algebraically closed, and also $\mathrm{dcl}(C \cup F) \cap K = F$ iff $\mathcal{C}_F = \mathcal{C}_K$.

Before continuing with the main theme of the paper, we digress a little on the meaning of (i) and (ii) in Definition 2.1.

LEMMA 2.3. *Let $F < K$ be differential fields, and X some F-definable set. The following are equivalent*:

(a) $X(F) = X(\hat{F})$ *and* $\mathrm{dcl}(X \cup F) \cap K = F$,
(b) $X(F) = X(\hat{K})$ (*for some (any) differential closure $\hat{K}$ of K*).

Proof. (b) $\Rightarrow$ (a). Suppose $X(F) = X(\hat{K})$. As $\hat{F}$ embeds in $\hat{K}$ over F, it follows that $X(F) = X(\hat{F})$. Let $c \in \mathrm{dcl}(X \cup F) \cap K$. Then there is some finite tuple d from $X(\hat{K})$ such that $c \in \mathrm{dcl}(d, F)$. But d is contained in $X(F)$, so $c \in F$.

(a) $\Rightarrow$ (b). Let $c \in X(\hat{K})$. Then there is some formula $\psi(y)$ over K isolating $tp(c/K)$. Let d be a canonical parameter for $\psi(y)$ (by Fact 1.5: elimination of imaginaries). Any automorphism of $\mathcal{U}$ which fixes $X \cup F$ pointwise will also fix the formula $\psi(y)$ (up to equivalence) and so will fix d. Thus $d \in \mathrm{dcl}(X \cup F)$. Clearly also $d \in K$. By assumption $d \in F$. Thus the formula $\psi(y)$ is defined over F, which means $tp(c/F)$ is isolated. Thus $c \in X(\hat{F})$ for some differential closure $\hat{F}$ of F. By assumption $c \in X(F)$. We have shown that $X(\hat{K}) = X(F)$. □

The next lemma gives some information on the strength of the assumption $X(F) = X(\hat{F})$. By a *strongly minimal* set we mean an infinite definable set X every definable subset of which is finite or cofinite (in X). For example C is strongly minimal.

LEMMA 2.4. *Suppose X is strongly minimal and defined over F. Then $X(F) = X(\hat{F})$ if and only if $X(F)$ is infinite and* $\mathrm{acl}(F) \cap X = X(F)$. *In particular, if $X(F)$ is infinite and $F = \mathrm{acl}(F)$, then $X(F) = X(\hat{F})$.*

Proof. Left to right is easy.

Right to left. Assume that $c \in X(\hat{F})$, $c \notin X(F)$. Then our assumption implies that $c \notin \mathrm{acl}(F)$. Now $tp(c/F)$ is isolated by a formula $\phi(x)$, and $\models \phi(x) \to x \in X$. $\phi(x)$ has infinitely many solutions, and also $\models \phi(x) \to x \neq a$ for each $a \in X(F)$. So the formula $\phi(x)$ contradicts strong minimality of X. □

We will now see that any generalised strongly normal extension of F is contained in a differential closure of F, and so in Definition 2.1, we could replace condition (ii) by the condition $F < K < \hat{F}$.

LEMMA 2.5. *Suppose K to be an X-strongly normal extension of F. Then K is contained in some differential closure $\hat{F}$ of F.*

Proof. Let $K = F\langle a \rangle$, and let $p(x) = tp(a/F)$. By 2.1(iv), for any b realising p, $b \in \mathrm{dcl}(a, F, X)$. The compactness theorem, yields an F-definable (partial) function $f(-, -)$, and a formula $\phi(x) \in p(x)$ such that whenever a_1, b_1 both satisfy $\phi(x)$, there is some tuple c from X such that $a_1 = f(b_1, c)$. (Actually the compactness theorem yields finitely many functions, but a standard trick, together with the infiniteness of F, gives us a single function.) Now let $\hat{F}$ be a differential closure of F inside $\hat{K}$. Let $b_1 \in \hat{F}$ satisfy $\phi(x)$. So clearly there is some tuple c from $X(\hat{K})$ such that $a = f(b_1, c)$. By Lemma 2.3, c is contained in $X(F)$, and thus a is contained in $\hat{F}$. So $K < \hat{F}$. □

We now continue with the main line of the analysis.

Remark 2.6. Let K be an X-strongly normal extension of F. Let σ be an isomorphism of K into $\mathcal{U}$ over F. Then σ extends to a unique automorphism τ of $K\langle X \rangle$ fixing X pointwise.

Proof. Let $K = F\langle a \rangle$ and let $\phi(x)$ be a formula over F isolating $tp(a/F)$. We claim that $\phi(x)$ isolates a complete type over $F\langle X \rangle$. If not then there are a_1, a_2 in $\mathcal{U}$, a tuple b from X and some formula $\psi(x, y)$ over F such that $\mathcal{U} \models \phi(a_1) \wedge \phi(a_2) \wedge \psi(a_1, b) \wedge \neg\psi(a_2, b)$. As $\hat{F}$ is an elementary substructure of $\mathcal{U}$, we can find such a_1, a_2 and b inside $\hat{F}$. But as $X(\hat{F})$ is contained in F the tuple b is from F, contradicting the fact that $\phi(x)$ isolates a complete type over F.

Thus $tp(a/F\langle X \rangle) = tp(\sigma(a)/F\langle X \rangle)$, and hence σ extends to a unique isomorphism τ between $K\langle X \rangle$ and $\sigma(K)\langle X \rangle$ which fixes X and F pointwise. But it follows easily from (iv) of Definition 2.1 that $K\langle X \rangle = \sigma(K)\langle X \rangle$. This proves the remark. □

Definition 2.7. Let K be an X-strongly normal extension of F. Then by $\mathrm{Gal}(K/F)$ we mean the group of automorphisms of $K\langle X\rangle$ which fix F and X pointwise. By $\mathrm{gal}(K/F)$ we will mean simply the group of automorphisms of K which fix F pointwise. Moreover $\mathrm{gal}(K/F)$ can be considered naturally as a subgroup of $\mathrm{Gal}(K/F)$.

By Remark 6, any $\sigma \in \mathrm{gal}(K/F)$ extends to a unique $\tau \in \mathrm{Gal}(K/F)$. Thus we can, and will, identify $\mathrm{gal}(K/F)$ with a subgroup of $\mathrm{Gal}(K/F)$. The purpose of this section will be to show that there is a canonical isomorphism μ of $\mathrm{Gal}(K/F)$ with a finite-dimensional F-definable group G, where moreover $G \subseteq \mathrm{dcl}(X \cup F)$, and that μ takes $\mathrm{gal}(K/F)$ to $G(\hat{F})$. We now carry this out (via a well-known model-theoretic construction of definable automorphism groups; cf. [24] and [6]).

Construction 2.8. We assume K to be an X-strongly normal extension of F, and by (2.5), that $K < \hat{F}$. We will construct the group G and isomorphism μ using certain data, and then point out that a different choice of data yields the same group, up to F-definable isomorphism.

Let a be some tuple such that $K = F\langle a\rangle$. By Fact 1.4, $tp(a/F)$ is isolated, by the formula $\phi(x)$ say, and also K has finite transcendence degree over F. Let Z be the set of solutions of $\phi(x)$ in $\mathcal{U}$. So $b \in Z$ iff there is an F-automorphism of $\mathcal{U}$ taking a to b, or equivalently if $b = \sigma(a)$ for some isomorphism σ of K into $\mathcal{U}$. By (iv) of Definition 2.1, $b \in \mathrm{dcl}(F \cup X \cup a)$ for any $b \in Z$. By the compactness theorem (and remarks following 1.13), there is an F-definable function $f_0(-,-)$ such that for any $b \in Z$, there is some tuple c from X such that $b = f_0(a, c)$. Let Y_0 be the set of tuples c from X such that $f_0(a, c)$ is defined and in Z. Equivalently, by Remark 2.6, Y_0 is the set of c from X such that for any $b \in Z$, $f_0(b, c)$ is defined and in Z. Y_0 is then an F-definable set of tuples from X.

Define the following equivalence relation E on Y_0: $E(c_1, c_2)$ iff $f_0(a, c_1) = f_0(a, c_2)$. Again by 2.6, this is equivalent to $f_0(b, c_1) = f_0(b, c_2)$ for all $b \in Z$. E is thus F-definable. Let $Y = Y_0/E$. By Fact 1.5, we can (and do) identify Y with an F-definable set contained in $\mathrm{dcl}(F \cup X)$. For $d \in Y$, and $b \in Z$, let $f(b, d)$ be defined to be $f_0(b, c)$ for some (any) $c \in Y_0$ such that $c/E = d$. Noting that $\mathrm{Aut}(\mathcal{U}/F)$ acts transitively on Z, we then have:

(*) For any $b_1, b_2 \in Z$, there is unique $d \in Y$ such that $f(b_1, b_2) = d$, and so we can write $d = h(b_1, b_2)$ for some F-definable function $h(-,-)$.

Also note that (as $Z \subseteq K\langle X\rangle$), $\mathrm{Gal}(K/F)$ acts on Z, and moreover by 2.6, for any $b \in Z$ there is unique $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(a) = b$. Thus:

(**) $\mathrm{Gal}(K/F)$ acts regularly on Z.

Define μ: $\mathrm{Gal}(K/F) \to Y$ by $\mu(\sigma) = h(a, \sigma(a))$; that is to say, $\mu(\sigma)$ is the unique $d \in Y$ such that $f(a, d) = \sigma(a)$.

Then by the definition of Y and $(*)$ and $(**)$, we have:

LEMMA 2.9. *μ is a bijection between* $\mathrm{Gal}(K/F)$ *and* Y.

Let G denote the group whose underlying set is Y and whose group operation is induced from μ.

LEMMA 2.10. *The group G is F-definable and finite-dimensional, and $G \subseteq \mathrm{dcl}(X \cup F)$. The induced (regular) action of G on Z is $(F \cup a)$-definable.*

Proof. We start by considering the action of Y on Z induced by μ; namely, for $g \in Y$, and $b \in Z$, $g.b = \mu^{-1}(g)(b)$. We show this to be definable. Let $\mu^{-1}(g) = \sigma$ (a member of $\mathrm{Gal}(K/F)$). Let $a_1 = \sigma(a) = f(a, g)$. Let $b \in Z$, and let $g_1 \in Y$ such that $b = f(a, g_1)$. Then (as $\sigma(g_1) = g_1$) $\sigma(b) = \sigma(f(a, g_1)) = f(\sigma(a), g_1)$ $= f(f(a, g), g_1)$. Thus $g.b = f(f(a, g), g_1)$, where $g_1 = h(a, b)$. This shows the $(F \cup a)$-definability of the action of Y on Z. It easily follows that the induced group operation on Y, is F-definable. We give the details. Let $g_1, g_2 \in Y$. Let $\sigma_i = \mu^{-1}(g_i)$ for $i = 1, 2$.

Then $\sigma_1.\sigma_2(a) = \sigma_1(\sigma_2(a)) = \sigma_1(f(a, g_2) = f(\sigma_1(a), g_2) = f(f(a, g_1), g_2)$. Thus $g_1.g_2 =_{\mathrm{def}} \mu(\sigma_1.\sigma_2)$ is the unique $g_3 \in Y$ such that $f(a, g_3) = f(f(a, g_1), g_2)$. But $Y \subseteq \mathrm{dcl}(F \cup X)$ so by 2.6, this condition holds for a iff it holds for all (some) $b \in Z$. This shows the group operation on G to be F-definable. As $\mathrm{tr.degree}(F\langle b\rangle/F)$ $= \mathrm{tr.degree}(K/F)$ is finite for all $b \in Z$ and G acts regularly on Z, clearly G is finite-dimensional □

We briefly discuss how canonical the above construction of G is. It clearly depends on the choice of $a \in K$ (and so of Z), of Y (coming from choice of f_0) and of f. A different choice of these data (say a_1, Z_1, Y_1, f_1) would give rise to an F-definable group G_1 and an isomorphism μ_1: $\mathrm{Gal}(K/F) \cong G_1$. It is easy to check that the isomorphism $\mu_1.\mu^{-1}$: $G \cong G_1$ is then F-definable. Moreover there is clearly an F-definable bijection between Z and Z_1 (as $K = F\langle a\rangle = F\langle a_1\rangle$) which (together with $\mu_1.\mu^{-1}$ will induce an isomorphism between the above defined actions of G on Z and G_1 on Z_1. On the other hand, if G_1 is F-definable and F-definably isomorphic to G, then clearly G_1 can arise by a suitable choice of data. It can similarly be seen that (up to F-definable isomorphism) the choice of G does not even depend on X, only on the extension $F < K$. Thus attached to any generalised strongly normal extension $F < K$ is a finite-dimensional F-definable group, unique up to F-definable isomorphism. We will sometimes refer to G as *the* Galois group of K over F, hopefully without confusion.

Before continuing, let us remark on the situation when $X = C$. Then the Galois group G of L over F is F-definable and contained in $\mathrm{dcl}(F \cup C)$. Thus there is an

F-definable subset V of C^n (some n), an F-definable equivalence relation E on V, and an F-definable bijection of V/E with G. Now stability implies that both V, E and the induced group structure on V/E are C_F-definable. As mentioned earlier, C with all induced structure from $\mathcal{U}$ is simply an algebraically closed field. It follows that V/E with the induced group structure is an algebraic group defined over C_F in the sense of the universal domain C. We may of course assume G to be this group, and we see that the Galois group of K over F is an algebraic group in the constants, defined over C_F.

Let us return to the notation coming from the original data in Construction 2.8.

LEMMA 2.11. *$\mu(\mathrm{gal}(K/F)) = G(\hat{F}) = G(F)$, and this induces an isomorphism between the (faithful) action of $\mathrm{gal}(K/F)$ on $Z(\hat{F})$ and the action of $G(\hat{F})$ on $Z(\hat{F})$.*

Proof. Let $\sigma \in \mathrm{Gal}(K/F)$. First note that

(i) $\sigma(a) \in \hat{F}$ iff $\mu(\sigma) \in G(\hat{F})$. This is because
(ii) $\sigma(a) \in F\langle a, \mu(\sigma)\rangle$ and $\mu(\sigma) \in F\langle a, \sigma(a)\rangle$. On the other hand, as G is contained in $\mathrm{dcl}(X \cup F)$ and $X(\hat{F}) = X(F)$, we see that
(iii) $G(\hat{F}) = G(F)$.

The inclusion of $\mu(\mathrm{gal}(K/F))$ in $G(\hat{F})$ follows from (i). On the other hand, if $\mu(\sigma) \in G(F)$ then also $\mu(\sigma^{-1}) \in G(F)$, so by (ii) $\sigma(a) \in F\langle a\rangle$ and $a \in F\langle\sigma(a)\rangle$, whereby the restriction of σ to K clearly determines an automorphism of K, and $\sigma \in \mathrm{gal}(K/F)$. The rest of the lemma is left to the reader. □

We proceed to specify the Galois correspondence. We again make use of data as in Construction 2.8.

THEOREM 2.12. *Let K be an X-strongly normal extension of F with Galois group G. For L an intermediate differential field $(F < L < K)$, let $G_L = \{g \in G: g(c) = c$ for all $c \in L\}$. Then K is an X-strongly normal extension of L, G_L is an F-definable subgroup of G and is the Galois group of L over K. Moreover the correspondence taking L to G_L establishes a 1-1 correspondence between the intermediate differential fields and the F-definable subgroups of G. Also L is an X-strongly normal extension of F if and only if G_L is a normal subgroup of G, in which case the quotient group G/G_L is the Galois group of L over F.*

Proof. It is easy to see that L is finitely generated over F, say $L = F\langle b\rangle$. Thus $\hat{F} = \hat{L}$. Let $b = t(a)$ for some F-definable function t. Then clearly, for $g \in G$, $g.b = b$ iff $t(a) = t(g.a)$ $(= t(f(a, g)))$ iff $t(b) = t(f(b, g))$ for any $b \in Z$. Thus G_L is an F-definable subgroup of G. Now if σ is an isomorphism of K into $\mathcal{U}$ over L, then in particular σ is an isomorphism of K into $\mathcal{U}$ over F, so $\sigma(K) \subseteq \langle K, X\rangle$, and thus K is an X-strongly normal extension of L. Let now $\sigma \in \mathrm{Gal}(K/L)$.

Let $g \in G = \mu(\sigma)$. Then $t(a) = t(\sigma(a) = t(g.a)$. Thus $g \in G_L$. Similarly if $\sigma \in \mu^{-1}(G_L)$ then $\sigma \in Gal(K/L)$. Thus G_L is the Galois group of L over K.

Now let H be any F-definable subgroup of G. Let $W = \{g.a: g \in H\}$. W is then a K-definable set. Let (by 1.5) b be a canonical parameter for W. Then $b \in K$. Let $L = F\langle b\rangle$. So by the paragraph above K is an X-strongly normal extension of L with Galois group G_L. We claim that $H = G_L$. Firstly, if $g \in H$, then for any $h \in H$, $g.(h.a) = (g.h).a$ is in W (as $g.h \in H$). Thus $\mu^{-1}(g)(W) = W$, so $\mu^{-1}(g)(b) = b$. Thus $g \in G_L$. Conversely if $g \in G_L$, then $g.W = W$, so $g.a \in W$. So $g.a = h.a$ for some $h \in H$, whereby $g = h \in H$.

The rest is left to the reader.

COROLLARY 2.13. *Let K be a generalised strongly normal extension of F, with Galois group G. Then G is connected if and only if F is relatively algebraically closed in K.*

We complete this section with some remarks connecting our point of view with that of [1]. For the sake of the next lemma, let us fix X, F and K an X-strongly normal extension of F. Let a, Z, Y, f, be as above, and let G be the Galois group of K over F, with isomorphism μ: $\mathrm{Gal}(K/F) \to G$. Let $G^* = G^{\mathrm{op}}$; i.e., G^* has the same underlying set as G (namely Y), but the multiplication $*$ on G^* is defined by: $g * h = h.g$.

LEMMA 2.14. *Let $*$ denote the map from $G^* \times Z$ to Z defined by $g * b = f(b, g)$. Then $*$ defines a regular (group) action of G^* on Z. (So Z becomes an F-definable principal homogeneous space for G^*.)*

Proof. From the proof of Lemma 2.10 we see that for any $g, h \in Y$, $f(a, g.h) = f(f(a, g), h)$. Thus $(h * g) * a\ (= f(a, g.h)) = h * (g * a)$. This remains true for any $b \in Z$ in place of a. So G^* acts on Z. It is clear that the action is regular. □

The following extends Bialynicki-Birula's characterization of strongly normal extensions to generalised strongly normal extensions. It is convenient to restrict our attention to the case where F is relatively algebraically closed in K (as is also done in [1]).

PROPOSITION 2.15. *Let $F < K\ (< \mathcal{U})$ be differential fields where F is relatively algebraically closed in K. The following are equivalent.*

(i) *K is a generalised strongly normal extension of F.*

(ii) *There are a connected algebraic group H_1, defined over F, an (algebraic) principal homogeneous space W for H_1, defined over F, and an F-definable connected (differential algebraic) subgroup H of H_1 such that:*

(a) $\dim(H_1)$ *(as an algebraic group) = typical* δ $\dim(H)$;

(b) $H(F) = H(\hat{F})$, *and* $F = \mathrm{dcl}(H \cup F) \cap K$;

(c) $K = F(W)$ (*here meaning the function field of* W), *that is to say,* $K = F(a)$ *where* a *is a generic point of* W *over* F *in the algebraic-geometrical sense.*

(d) *For* $g \in H(F)$, $tp(a/F) = tp(g.a/F)$, *or equivalently the map taking any* $P(a) \in K$ *to* $P(g.a)$ (P *an* F*-rational function*) *determines an automorphism of the differential field* K *over* F.

Proof. For the (i) $\Rightarrow$ (ii) direction we will be brief. Suppose first K is an X-strongly normal extension of F, with Galois group G. By Corollary 2.13, G is connected (as a definable group). We may assume that in Construction 2.8, a, f and Y are chosen such that:

(i) $K = F(a)$.
(ii) For generic c in Y ($\approx G$) over F, $F\langle c\rangle = F(c)$.
(iii) For any $c \in Y$, $f(a, c) \in F(a, c)$ and $c \in F(a, f(a, c))$ (in particular f is F-definable in the field language).

By (ii) we have:

(iv) For generic, independent $g, h \in G$, $g.h \in F(g, h)$. □

Now let G^* be as above. Let g be a generic point of G^* over F. Let V_0 the irreducible variety over F of which c is the generic point. Similarly, let W_0 be the irreducible variety over F of which a is the generic point. By (iii), the map $f(-, g)$ determines a birational isomorphism of W_0 with itself. Let g_1, g_2 be independent generic points of G^* over $F(a)$ (in the sense of differential fields). Then clearly g_1, g_2, a are generic independent points (over F) of V_0, V_0, W_0 in the algebraic geometrical sense, and moreover $(g_1 * g_2) * a = g_1 * (g_2 * a)$; namely $f(a, g_1 * g_2) = f(f(a, g_2), g_1)$. By (iii) and (iv) and Weil's Theorem [23], there is a connected algebraic group H_1 over F, and a (algebraic) homogeneous space W for H_1, defined over F, such that g is a generic point of H_1 over F, a is a generic point of W over F, the multiplication on H_1 agrees with $*$ generically, and the action of H_1 agrees with $*$ generically. As $g \in F(a, g * a)$, clearly W is a principal homogeneous space. Clearly Z is a subset of W (every element of Z is a generic element of W over F in the algebraic geometrical sense). Also the identity map (on generic elements of G^*) extends to an F-definable embedding of G^* into H_1. So we may suppose G^* to be equal to its image, and thus a subgroup of H_1. Define $H = G^*$. Note the action of H on Z (by $*$) is the restriction of the action of H_1 on W (which we will also call $*$). Note that $\dim(H_1) = \mathrm{tr.deg}(F(g)/F) = \text{typical } \delta\text{-dim}(H)$. So (a) holds. (b)–(d) are clear.

We now prove the converse. Suppose (ii) holds. We will show that K is an H-strongly normal extension of F. We use the model theory of DCF_0. First, as F is

relatively algebraically closed in K, $tp(a/F)$ is stationary (meaning that whenever $tp(a_1/F) = tp(a_2/F) = tp(a/F)$ and each of a_1, a_2 is independent from L over F then $tp(a_1/L) = tp(a_2/L)$). We will first show:

Claim. For some b realising $tp(a/F)$ with b independent from a over F, there is $g \in H$ such that $g.a = b$.

Proof of claim. Let $\hat{K}$ be some differential closure of K. By (b) and Lemma 2.3, $H(\hat{K}) = H(F)$. Let $g \in H$ be generic over F, such that g is independent from $F(a)$ in the differential field sense. Let $b = g.a$ (where . denotes the (F-rational) action of H_1 on W). Now (a) implies that $F\langle g\rangle = F(g)$ and tr.deg$(F(g)/F) = d = \dim(H_1) =$ tr.deg$(F(a)/F)$. As $F\langle a\rangle = F(a)$, clearly $F\langle b\rangle = F\langle b\rangle$, and note tr.deg$(F(b)/F) \leq d$. Now (as H_1 acts regularly on W), $F(a, g, b) = F(a, g) = F(a, b)$, and this field has transcendence degree $2d$ over F. It follows that a is independent from b in the differential field sense. To prove the claim all we need show is that $tp(b/F) = tp(a/F)$. Let $\psi(x)$ be a formula over F true of a. By (d) and the fact mentioned above that $H(F) = H(\hat{K})$, it follows that the sentence $\forall y(y \in H \rightarrow \psi(y.a))$ is true in $\hat{K}$. As $\hat{K}$ is an elementary substructure of $\mathcal{U}$, this sentence is true in $\mathcal{U}$, whereby $\psi(x)$ is true of b. The claim is proved.

Now let σ be an arbitrary isomorphism of K into $\mathcal{U}$ over F. Let $c = \sigma(a)$. Let d be a realisation of $tp(a/F)$ which is independent of a,c over F. Then $tp(a, d/F) = tp(d, c/F) = tp(a, b/F)$ (as $tp(a/F)$ is stationary). By the claim, there are $g, h \in H$ such that $g.a = d$ and $h.d = c$. As $a, c, d \in W$, it follows that $(h.g).a = c$. As $h.g \in H$, we see that $c \in \langle K, H\rangle$, and so $\sigma(K) \subseteq \langle K, H\rangle$. We have shown that K is an H-strongly normal extension of F.

We complete this section with a clean characterisation of generalised strongly normal extensions, the proof of which should be clear to the reader.

LEMMA. *K is a generalised strongly normal extension of F if and only if*

(i) $F < K < \hat{F}$, *and*
(ii) *there is an F-definable group G and F-definable principal homogeneous G-space X such that $G(F) = G(\hat{F})$ and $K = F\langle a\rangle$ for some $a \in X$.*

3. Galois cohomology and *(G,H)*-primitive elements

In this section we give a "canonical form" for generalised strongly normal extensions; namely, we show that a generalised strongly normal extension K of F is generated over F by an element α of some F-algebraic group which satisfies some formula or "differential equation" (over F) of a specific form. In fact the result follows easily from (i) the embeddability of differential algebraic groups into algebraic

groups, and (ii) the triviality of certain "constrained cohomology" groups. The required result (ii) was proved by Kolchin, but we give another proof here, working in the a priori more general definable category.

We start by defining what are essentially Kolchin's first constrained cohomology groups (see [12] and also [19]).

Definition 3.1. Let F be a differential field, and $\hat{F}$ a differential closure. Let G be an F-definable differential algebraic group. Let $\mathcal{G}$ be $\mathrm{Aut}(\hat{F}/F)$.

(i) By a definable cocycle from $\mathcal{G}$ to G we mean a map s from $\mathcal{G}$ to $G(\hat{F})$ such that for $\sigma, \tau \in \mathcal{G}$, $s(\sigma.\tau) = s(\sigma).\sigma(s(\tau))$, and also, for some tuple $a \in \hat{F}$ and some F-definable partial function h, $s(\sigma) = h(a, \sigma(a))$ for all $\sigma \in \mathcal{G}$. The set of such definable cocycles is denoted by $Z^1_{\mathrm{def}}(\mathcal{G}, G)$.

(ii) If $s, t \in Z^1_{\mathrm{def}}(\mathcal{G}, G)$, we say s and t are cohomologous if there is some $b \in G$ such that for all $\sigma \in \mathcal{G}$, $t(\sigma) = b^{-1}.s(\sigma).\sigma(b)$. (This is easily seen to be an equivalence relation, which we call E_c).

(iii) A definable cocycle s is said to be trivial if for some $b \in G$, $s(\sigma) = b^{-1}.\sigma(b)$ for all $\sigma \in \mathcal{G}$. (Note that the trivial cocycles are cohomologous to each other.)

(iv) By $H^1_{\mathrm{def}}(\mathcal{G}, G)$ (or sometimes $H^1_{\mathrm{def}}(\hat{F}/F, G)$) we mean $Z^1_{\mathrm{def}}(\mathcal{G}, G)/E_c$, the set of cohomology classes of the set of definable cocycles. This is a pointed set, the distinguished element being the class of trivial cocycles.

The following is essentially proved in [12].

PROPOSITION 3.2. *Suppose F to be algebraically closed and G to be an algebraic group defined over F (namely a group defined over F in the field language). Then $H^1_{\mathrm{def}}(\hat{F}/F, G)$ is trivial.*

Proof. Let $\mathcal{G} = \mathrm{Aut}(\hat{F}/F)$ and let $s \in Z^1_{\mathrm{def}}(\mathcal{G}, G)$. We must show s to be a trivial cocycle. Let a be a tuple from $\hat{F}$ and h an F-definable function, such that for any $\sigma \in \mathcal{G}$, $s(\sigma) = h(a, \sigma(a))$. Let $\phi(x)$ be a formula over F isolating $tp(a/F)$. For any b in $\hat{F}$ satisfying $\phi(x)$ there is $\sigma \in \mathcal{G}$ with $\sigma(a) = b$, and thus $h(a, b)$ is defined (and in $G(\hat{F})$).Thus for all realisations a_1, b_1 of $\phi(x)$ in $\mathcal{U}$, $h(a_1, b_1)$ is defined and in G. For each such a_1, b_1, $f(a_1, b_1)$ is in $F\langle a_1, b_1\rangle$, so in $F(a_1, a_1', a_1'', \ldots, b_1, b_1', b_1'', \ldots)$. So by compactness (and a standard trick) there is some function h_0, definable over F in the field language, and some n, such that for all realisations a_1, b_1 of $\phi(x)$, $h(a_1, b_1) = h_0(a_1, \ldots, a_1^{(n)}, b_1, \ldots, b_1^{(n)})$. So replacing a by $(a, a', \ldots, a^{(n)})$ we may assume that h is definable over F in the field language.

Claim. For any realisations b, c of $\phi(x)$ in $\hat{F}$, $h(a, b).h(b.c) = h(a, c)$.

Proof of Claim 1. Let $\tau, \sigma \in \mathcal{G}$ be such that $\tau(a) = b$, and $\tau.\sigma(a) = c$. Then $s(\tau.\sigma) = s(\tau).\tau(s(\sigma)) = h(a, b).\tau(h(a, \sigma(a)) = h(a, b).h(\tau(a), \tau.\sigma(a)) = h(a, b).h(b, c)$ as required.

As $\hat{F}$ is an elementary substructure of $\mathcal{U}$, the claim holds for any realisations b, c of $\phi(x)$ in $\mathcal{U}$.

Let us choose realisations b, c of $\phi(x)$ in $\mathcal{U}$ such that $\{(b, c, \hat{F}\}$ is F-independent in the sense of differential fields. In particular, $\{a, b, c\}$ is independent over F in the algebraic-geometrical sense, and we also have that $h(a, b).h(b.c) = h(a, c)$. The latter formula is one over F in the field language (as multiplication on G is F-rational). As F is algebraically closed there is $d \in F$ such that

$(*)$ $h(a, b).h(b, d) = h(a, d)$, and $h(a, d), h(b, d) \in G$.

Now let $\sigma \in \mathcal{G}$. Then (as F is algebraically closed, so the type over F determined by $\phi(x)$ is stationary) we have that $tp(a, b/F) = tp(b, \sigma(a)/F)$, and thus

$(**)$ $h(b, \sigma(a)).h(\sigma(a), d) = h(b, d)$.

From $(*)$ and $(**)$ we obtain

$(***)$ $h(a, b).h(b, \sigma(a)).h(\sigma(a), d) = h(a, d)$.

But (by the truth of the claim in $\mathcal{U}$), $h(a, b).h(b, \sigma(a)) = h(a, \sigma(a))$. Thus $s(\sigma) = h(a, \sigma(a)) = h(a, d).h(\sigma(a), d)^{-1}$. Put $\alpha = h(a, d)^{-1}$ (a member of $G(\hat{F})$). Then $h(\sigma(a), d) = \sigma(\alpha^{-1})$. Thus $s(\sigma) = \alpha^{-1}.\sigma(\alpha)$. As this is true for all $\sigma \in \mathcal{G}$ (the choice of α did not depend on σ), we have shown that the cocycle s is trivial, completing the proof of the proposition. □

Finally in this section, we give an analogue of Kolchin's notion of "G-primitive" elements, and show that generalised strongly normal extensions are generated by such elements (at least when the base field is algebraically closed).

First suppose that F is a differential field, and G, H are F-definable groups (i.e., differential algebraic groups, defined over F) with $G < H$. Let H/G denote the set of left cosets of G in H. By Fact 1.5 there is some F-definable set W (a subset of $\mathcal{U}^n$ for some n), and an F-definable bijection between H/G and W, in other words W is an F-definable homogeneous space for H, isomorphic to H/G. We will identify H/G with such a set W. Thus we are able to write $(H/G)(F)$ for the set of F-points of H/G. Note that if F is differentially closed then $(H/G)(F) = H(F)/G(F)$, but this will not hold in general for arbitrary F. Let ν denote the canonical projection from H to H/G. If H happens to be a connected algebraic group defined over the constants $C_{\mathcal{U}}$, and $G = H(C_{\mathcal{U}})$, then H/G can be identified with the Lie algebra of H and ν is Kolchin's logarithmic derivative.

Definition 3.3. Suppose $G < H$ are F-definable groups. α is said to be an (H, G)-primitive element over F, if $\alpha \in H$ and $\nu(\alpha) \in (H/G)(F)$.

Before the next proposition, it should be remarked that any connected definable (differential algebraic) group defined over F, can be F-definably embedded in a

connected algebraic group H defined over F. (This is proved in [17] and also in [2] for finite-dimensional differential algebraic groups.)

PROPOSITION 3.4. (*i*) *Suppose α is an (H, G)-primitive element over F (where $G < H$ are F-definable groups), $K = F\langle\alpha\rangle$, $G(F) = G(\hat{F})$ and* $\mathrm{dcl}(G \cup F) \cap K = F$. *Then K is a generalised strongly normal extension of F (in fact a G-strongly normal extension of F), and moreover the map taking $\sigma \in \mathrm{Gal}(K/F)$ to $\alpha^{-1}.\sigma(\alpha) \in H$ is an isomorphism between* $\mathrm{Gal}(K/F)$ *and an F-definable subgroup of G.*

(*ii*) *On the other hand, suppose F is algebraically closed, and K is a generalised strongly normal extension of F. Let G be the Galois group of K over F (with canonical isomorphism μ:* $\mathrm{Gal}(K/F) \to G$). *Let H be any algebraic group defined over F in which G definably (over F) embeds. Then $K = F\langle\alpha\rangle$ where α is some (H, G)-primitive element over F. Moreover for any $\sigma \in \mathrm{Gal}(K/F)$, $\mu(\sigma) = \alpha^{-1}.\sigma(\alpha)$.*

Proof. (i) If σ is an isomorphism of K into $\mathcal{U}$ over F, and $\beta = \sigma(\alpha)$, then $v(\beta) = v(\alpha)$, and thus $\alpha^{-1}.\beta \in G$. So $\sigma(K) \subseteq (K, G)$. Together with the other hypotheses of (i) this means that K is a G-strongly normal extension of F. The rest is clear.

(ii) We may assume G is an F-definable subgroup of H. Let $K = F\langle a\rangle$ (which by Lemma 2.5 we may assume to be contained in $\hat{F}$). Let μ be the canonical isomorphism of $\mathrm{Gal}(K/F)$ with G. So for some F-definable function h(-,-), $\mu(\sigma) = h(a, \sigma(a))$ for all $\sigma \in \mathrm{Gal}(K/F)$ .Then the map s from $\mathrm{Aut}(\hat{F}/F)$ to $G(\hat{F})$ defined by $s(\sigma) = h(a, \sigma(a))$ is clearly a homomorphism. But $G(\hat{F}) = G(F)$, so $\mathrm{Aut}(\hat{F}/F)$ acts trivially on $G(F)$, and thus s is a definable cocycle from $\mathrm{Aut}(\hat{F}/F)$ into $G(\hat{F})$. As G is a subgroup of the algebraic group H (which is defined over F), s is actually in $Z^1_{\mathrm{def}}(\hat{F}/F, H)$. By Proposition 3.2, s is trivial, namely there is $\alpha \in H(\hat{F})$ such that for any $\sigma \in \mathrm{Aut}(\hat{F}/F)$, $h(a, \sigma(a)) = \alpha^{-1}.\sigma(\alpha)$. Thus for $\sigma \in \mathrm{Aut}(\hat{F}/F)$, σ fixes a iff σ fixes α. By 1.4, $K = F\langle a\rangle = F\langle\alpha\rangle$. Let $\phi(x)$ isolate $tp(a/F)$, $\chi(y)$ isolate $tp(\alpha/F)$, and let $t(x)$, $k(y)$ be F-definable functions such that $\alpha = t(a)$ and $a = \chi(\alpha)$. Then the sentences $\forall x(\phi(x) \to h(a, x) = \alpha^{-1}.t(x))$, and $\forall y(\chi(y) \to \alpha^{-1}.y = h(a, k(y))$ are both true in $\hat{F}$, so also in $\mathcal{U}$. So clearly for $\sigma \in \mathrm{Gal}(K/F)$, $\mu(\sigma) = \alpha^{-1}.\sigma(\alpha)$.

Finally, let $d = v(\alpha) = \alpha/G \in H/G$. For any automorphism σ of $\mathcal{U}$ over F, we know that $\alpha^{-1}.\sigma(\alpha)$ is in G, hence $\alpha/G = \sigma(\alpha/G)$. Thus d is in F. So α is an (H, G)-primitive element over F. This completes the proof of the proposition.

4. Existence of generalised strongly normal extensions

In this section we show that any finite-dimensional differential algebraic group is the Galois group of some generalised strongly normal extension K of some F. (We do not fix F in advance. This would constitute the inverse Galois problem, which is

treated in [16].) We make more serious use of stability theory (independence and the U-rank). For ease of exposition we will work with connected G.

PROPOSITION 4.1. *Let G be a connected definable group of finite U-rank. Then there are differential fields $F < K$ (with G defined over F) such that K is a generalised strongly normal extension of F, with Galois group G.*

Proof. Let F_0 be some differentially closed field over which G is defined. By [17], there is a connected algebraic group H defined over F_0 and an F_0-definable embedding of G in H. We may assume G to be a subgroup of H. By Fact 1.12, the U-rank of H is $\omega.m$ (some $m > 0$). As above we treat the homogeneous space H/G as an F_0-definable subset of U^n for some n. Let v be the (F_0-definable) projection from H to H/G. Now choose α to be a generic point of H over F_0, in the sense of differential fields (see 1.10). Let $c = v(\alpha)$. Let $F = F_0\langle c\rangle$ and $K = F_0\langle\alpha\rangle$. Note that $F < K$, and $K = F\langle\alpha\rangle$.

By Fact 1.9 (iv) we have

$$(*)\ U(\alpha/F_0\langle c\rangle) + U(c/F_0) \leq U(\alpha, c/F_0) \leq U(\alpha/F_0\langle c\rangle) \oplus U(c/F_0).$$

Now the set defined by $v(y) = c$ is clearly in definable bijection with G, and the latter has finite U-rank. Thus

$$(**)\ U(\alpha/F_0\langle c\rangle) < \omega.$$

Now 1.4 also yields $U(\alpha, c/F_0) = U(\alpha/F_0)$ which we know to be $\omega.m$. Together with $(*)$ and $(**)$ this yields

$$(***)\ U(c/F_0) = \omega.m.$$

Claim 1. $tp(\alpha/F)$ is isolated, by the formula $v(x) = c$. Thus we have $F < K < \hat{F}$.

Proof of Claim 1. Let $\beta \in H$ with $v(\beta) = c$. As in $(**)$, $U(tp(\beta/F_0\langle c\rangle)) < \omega$. $(***)$ together with 1.4 (iv) implies that $U(\beta/F_0) = \omega.m$. By 1.12 and 1.11, $tp(\beta/F_0) = tp(\alpha/F_0)$. Thus $tp(\beta, v(\beta)/F_0) = tp(\alpha, v(\alpha)/F_0)$, and $tp(\beta/F) = tp(\alpha/F)$, as required.

Claim 2. $G(F) = G(\hat{K})\ (= G(F_0))$.

Proof of Claim 2. As F_0 is differentially closed, it is well known that any element of $F_0\hat{\langle}\alpha\rangle$ not in F_0 cannot be independent from α over F_0. But we know that $U(\alpha/F_0) = \omega.m$ and for any $g \in G$, $U(g/F_0) < \omega$. By 1.4 (iv), α is independent from g over F_0 for all $g \in G$. Thus $G(\hat{K}) = G(F_0)$. This proves Claim 2.

By Claims 1, 2, and (i) of Proposition 3.4, K is a G-strongly normal extension of F, whose Galois group is the image of the map μ: $\mathrm{Gal}(K/F) \to G$ defined by $\mu(\sigma) = \alpha^{-1}.\sigma(\alpha)$. So we must show that μ is onto G. Let $g \in G$. Let $\beta = \alpha.g$. Then $v(\alpha) = v(\beta)$. By Claim 1, $tp(\beta/F) = tp(\alpha/F)$ so there is an isomorphism σ of K into $\mathcal{U}$ over F taking α to β. σ extends to (unique) $\tau \in \mathrm{Gal}(K/F)$, and $\mu(\tau) = g$. □

5. Additional remarks

In this section we point out that the theory presented here properly generalises the Kolchin theory.

LEMMA 5.1. *Let K be a generalised strongly normal extension of F with Galois group G. Assume G to be connected. Then K is a strongly normal extension of F if and only if G is (definably) isomorphic to some algebraic group in the constants (i.e., to $H(C)$ for some algebraic group H defined over C).*

Proof. ($\Rightarrow$) Clear (from material in Section 2).

($\Leftarrow$) Note that the right hand condition does *not* specify that the isomorphism is defined over F. We will deduce this. In any case we have to show

(i) $C_F = C_{\hat{F}}$, and

(ii) G is definably isomorphic *over* F to $H(C)$ for some algebraic group H defined over C_F.

Proof of (i). First, as $\hat{F}$ is an elementary substructure of $\mathcal{U}$ and G is F-definable, we can assume that the algebraic group in the constants (say H_1) is defined over $C_{\hat{F}}$ and the isomorphism j: $G \cong H_1$ is defined over $\hat{F}$. Now there is some surjective map, say pr from H_1 onto C (where pr is defined over $\hat{F}$. Then composing pr with j yields an $\hat{F}$-definable map j_1 from G onto C. We obtain some $\hat{F}$ definable set $Y \subseteq \mathrm{dcl}(\hat{F} \cup G)$ and an $\hat{F}$-definable bijection k between Y and C. This induces an $\hat{F}$-definable field structure on Y, which we denote L. As G is F-definable and $G(\hat{F}) = G(F)$, it follows that K is F-definable, and $K(\hat{F}) = K(F)$. We claim that k is also F-definable. Otherwise, let $k' \neq k$ be the image of k under some F-automorphism of $\mathcal{U}$. Then the composition of k^{-1} with k' yields a nontrivial definable automorphism of C, which is known to be impossible. So k is F-definable. It follows (as $K(\hat{F}) = K(F)$) that $C_{\hat{F}}$, which is the image of $K(\hat{F})$ under k, is contained in F, yielding (i).

Proof of (ii). Let H_1 be as in the proof of (i). The parameters for the $\hat{F}$-definable isomorphism between G and H_1 can be chosen from $F \cup G(\hat{F}) \cup H_1(\hat{F})$. But $G(\hat{F}) = G(F)$ and by (i) the same is true of H_1. Thus G is F-definably isomorphic to H_1. This proves (ii).

It follows from (i) and (ii) that K is a $\mathcal{C}$-strongly normal extension of F with Galois group H_1.

In order to show that there are generalised strongly normal extensions which are not strongly normal extensions, we make use of the easy direction of the above lemma (together with Proposition 4.1); in particular, we exhibit connected finite-dimensional definable groups which are *not* definably isomorphic to algebraic groups in the constants (or in the language of Buium, are not split). Such examples are well-known (see [2]), but we mention a couple.

Let ϕ be the "logarithmic derivative" from the multiplicative group of $\mathcal{U}$ onto the additive group of $\mathcal{U}$, defined by $\phi(x) = x'/x$. $\mathrm{Ker}(\phi) = \mathcal{C}^*$. Let G be $\phi^{-1}(\mathcal{C})$. Then G is a definable subgroup of $\mathcal{C}^*$ of U-rank 2. We claim that G is not definably isomorphic to any group H which is an algebraic group in the sense of the universal domain $\mathcal{C}$. For then H would be 2-dimensional, commutative, so by virtue of its abstract structure it would be the direct product of a one-dimensional diagonalizable group and a one-dimensional unipotent group. Pulling back the unipotent subgroup to G we see that G has a definable subgroup which is torsion free. So $\mathcal{U}^*$ has a definable subgroup which is torsion free. This contradicts results of Cassidy [4] which state that any differential algebraic subgroup of $\mathcal{U}^*$ contains $\mathcal{C}^*$.

The next example is somewhat deeper. Let A be a simple abelian variety over $\mathcal{U}$, which is not isomorphic (as an algebraic group) to one defined over $\mathcal{C}$. Of course A is also a group definable in $\mathcal{U}$. Buium [2] shows that A has a unique smallest infinite definable subgroup G, that G is finite-dimensional, and is not definably isomorphic to any algebraic group in the constants. The existence of G is connected to Manin's "theorem of the kernel" in [14].

References

1. A. Bialynicki-Birula, *On Galois theory of fields with operators*, Amer. J. Math. **84** (1962), 89–109.
2. A. Buium, *Differential algebraic groups of finite dimension*, Lecture Notes in Math; no. 1506, Springer-Verlag, 1992.
3. ———, *Differential algebra and number theory*, Hermann, Paris, 1994.
4. Ph. J. Cassidy, *Differential algebraic groups*, Amer. J. Math. **94** (1972), 891–954.
5. W. A. Hodges, *Model theory*, Cambridge University Press, 1993.
6. E. Hrushovski, *Unidimensional theories are superstable*, Annals of Pure and Applied Logic **50** (1990), 117–138.
7. E. Hrushovski and Z. Sokolovic, *Minimal sets in differentially closed fields*, Trans. Amer. Math. Soc., to appear.
8. E. R. Kolchin, *Galois theory of differential fields*, Amer. J. Math. **75** (1953), 753–824.
9. ———, *On the Galois theory of differential fields*, Amer. J. Math. **77** (1955), 868–894.
10. ———, *Abelian extensions of differential fields*, Amer. J. Math. **82** (1960), 779–790.
11. ———, *Differential algebra and algebraic groups*, Academic Press, New York, 1973.
12. ———, *Differential algebraic groups*, Academic Press, New York, 1985.
13. A. Magid, *Differential Galois theory*, Mem. Amer. Math. Soc., 1994.
14. Y. I. Manin, *Rational points of algebraic curves over function fields*, Izvestia Akad. Nauk SSR **27** (1963), 1395–1440; translation in Amer. Math. Soc. Transl. Ser. II **59** (1966), 189–234.

15. D Marker, "Model theory of differential fields" in *Model theory of fields*, Lecture Notes in Logic, no. 5, Springer-Verlag, 1996.
16. D Marker and A. Pillay, *Differential Galois theory III: Some inverse problems*, Illinois J. Math. **41** (1996), 453–461.
17. A. Pillay, *Some foundational questions concerning differential algebraic groups*, Pacific J. Math. **179** (1997), 181–192.
18. ———, *Differential Galois theory II: superstable differential fields*, Annals of Pure and Applied Logic, **88** (1997), 181–192.
19. ———, *Remarks on Galois cohomology and definability*, J. Symbolic Logic **62**, (1997), 487–492.
20. A Pillay and Z. Sokolovic, *Superstable differential fields*, J. Symbolic Logic **57** (1992), 97–108.
21. B. Poizat, *Cours de Theorie des Modeles*, Nur al-Mantiq wal'Ma'rifah, Villeurbanne, 1985.
22. B. Poizat, *Une theorie de Galois imaginaire*, J. Symbolic Logic **48** (1983), 1151–1170.
23. A. Weil, *On algebraic groups of transformations*, Amer. J. Math. **77** (1955), 203–271.
24. B. I. Zilber, "Totally categorical theories: structural properties and non-finite axiomatizability" in *Model theory of algebra and arithmetic*, ed. L. Pacholski et al., Lecture Notes in Math., no. 834, Springer-Verlag, 1980, pp. 381–410.

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL 61801
pillay@math.uiuc.edu