Differential Galois Theory III: some inverse problems.

David Marker [*]
University of Illinois at Chicago

Anand Pillay [†]
University of Notre Dame

February 16, 1996

1 Introduction

In [16] a theory of generalised strongly normal extensions of differential fields was developed, generalising Kolchin's theory ([8]). It was shown that arbitrary finite-dimensional differential algebraic groups can arise as differential Galois groups for this new theory. The fact that our theory is a proper generalisation of Kolchin's is due precisely to the existence of finite-dimensional differential algebraic groups which are not isomorphic to algebraic groups in the constants. In this paper we initiate a study of the inverse problem for generalised strongly normal extensions. We will henceforth call generalised strongly normal extensions, *differential Galois extensions*. We may as well begin by stating a general conjecture, where notation will be explained subsequently.

Conjecture 1.1 *Suppose F is an algebraically closed differential field of finite transcendence degree over its field of constants, and G is a connected*

[*]Partially supported by a grant from the NSF and an AMS Centennial Fellowship
[†]Partially supported by a grant from the NSF

finite-dimensional differential algebraic group defined over F such that $G(F)$ $= G(\hat{F})$. Then F has a differential Galois extension K with Galois group G.

A considerable amount of work has been done on this conjecture in the case where G is an algebraic group in the constants (namely G is the group of constant-rational points of an algebraic group defined over the constants). In this case our differential Galois extensions are exactly Kolchin's strongly normal extensions. We mention in particular the papers [10], [11], [20], [12] and [15]. In fact the problem is completely solved in the latter paper.

In this paper we study the situation for some of the "new" finite-dimensional differential algebraic groups. For an abelian variety A defined over a function field, Manin [13] constructs a differential algebraic homomorphism from A into some vector group, with "finite-dimensional" kernel. Such a kernel will be one of the "new" groups (assuming that A does not descend to the constants). Such homomorphisms were also constructed by Buium [1], by different methods. We will slightly tinker with the hypotheses of Conjecture 1.1, assuming on the one hand that the field of constants of F has infinite transcendence degree, but on the other hand only that F is the algebraic closure of a differential field F_1 which is finitely generated (as a differential field) over the constants of F. In this situation we will prove that if A is either a simple abelian variety or a 1-dimensional algebraic torus defined over F, and G is the smallest differential algebraic subgroup of A, then F has a differential Galois extension with Galois group G. Our proof uses model-theoretic methods. We also give an application (depending on [17]) to the model theory of differential fields, showing that the closure under (Kolchin) strongly normal extensions of a field of constants of infinite transcendence degree, is not superstable.

We will freely use model-theoretic notation. The reader is referred to [16] where some explanations are given for the non model-theorist, as well as to [5] for general model theory, [14] for the model theory of differential fields, and [19] for stable groups. DCF_0 denotes the theory of differentially closed fields of characteristic 0 (in the language $+$, $-$, $\cdot$, 0, 1, δ). Recall that this theory is complete, ω-stable, with elimination of quantifiers as well as elimination of imaginaries. $\mathcal{U}$ denotes a very saturated model of DCF_0. Any differential field F of cardinality at most that of $\mathcal{U}$ will embed in $\mathcal{U}$. Let F, K,.. denote differential subfields of $\mathcal{U}$ of cardinality stricty less than that of $\mathcal{U}$, and let $\hat{F}$ denote (a copy of) the prime model over F (or differential closure of F).

(So F is differentially closed iff $\hat{F} = F$ iff F is an elementary substructure of $\mathcal{U}$.) By "definable" we mean definable (with parameters) in the structure $(\mathcal{U}, +, -, \cdot, 0, 1, \delta)$, unless stated otherwise. If X is an F-definable set, then $X(F)$ denotes the points of X every coordinate of which is in F. Let C denote the constants of $\mathcal{U}$. From now on a, b, etc. denote (finite) tuples from $\mathcal{U}$, and $F < a >$ denotes the differential field generated by $F \cup a$. We identify the class of differential algebraic groups (in the sense of [2], [8], or [1]) with the class of groups definable in $\mathcal{U}$ (this identification is proved in [18]). To say that such G is "finite-dimensional" is the same as saying that it has finite Morley rank in the structure $\mathcal{U}$. Algebraic groups (taking $\mathcal{U}$ as a universal domain for algebraic geometry) are special cases of definable groups, in fact they are precisely the groups definable in $\mathcal{U}$ by formulas involving only the field structure.

The general notion of a "differential Galois extension" was developed in [16].

Definition 1.2 *We call K a differential Galois extension of F, if there are an F-definable group G of finite Morley rank, an F-definable set X, and an F-definable regular action of G on X such that:*
(i) $G(F) = G(\hat{F})$,
(ii) for any $a \in X$, and $g \in G$, $tp(a/F \cup G) = tp(g \cdot a/F \cup G)$,
(iii) $K = F < a >$ for some $a \in X(\hat{F})$.
If $C(F)$ is algebraically closed, and for some algebraic group H defined over $C(F)$ we have that $G = H(C)$, then (assuming that (i),(ii) and (iii) hold) we call K a strongly normal extension of F. (This agrees with Kolchin's original definition of strongly normal extensions.)

Fact 1.3 *Let F, K, G, X, a be as in Definition 1.2. Let $Aut(X/F \cup G)$ be the group of permutations of X induced by elementary maps which fix $F \cup G$ pointwise. Let $Aut(K/F)$ be the group of (differential field) automorphisms of K which fix F pointwise. Let G^* be G with multiplication reversed (also an F-definable group of finite U-rank). Then there is an $F \cup a$-definable regular action $*$ of G^* on X and an isomorphism h: $Aut(X/F \cup G) \to G^*$ such that for any $\sigma \in Aut(X/F \cup G)$ and $b \in X$, $\sigma(b) = h(\sigma) * b$. Moreover the restriction of h to $X(\hat{F})$ induces an isomorphism between $Aut(K/F)$ and $G^*(\hat{F})$ ($= G^*(F)$). We call G^* the Galois group of K over F (with the understanding that the isomorphism is really between $G^*(\hat{F})$ and $Aut(K/F)$.)*

The following is proved in [16].

Lemma 1.4 *Suppose $F < K < \hat{F}$, and F is algebraically closed, and let G be a connected F-definable group of finite Morley rank, such that $G(F) = G(\hat{F})$. Then the following are equivalent:*
(i) K is a differential Galois extension of F with Galois group G;
(ii) there is a connected algebraic group H, defined over F, in which G F-definably embeds, there is $a \in (H/G)(F)$, and there is $\alpha \in H$ such that $\nu(\alpha) = a$, $K = F < \alpha >$) and the formula $\nu(x) = a$ isolates a complete type over F.(Here H/G denotes the F-definable set of left cosets of G in H, and ν denotes the canonical F-definable projection from H onto H/G.)

We now recall some stability-theoretic notions and facts.

Definition 1.5 *(We work in some saturated model M of a stable theory.)*
(i) The definable set X is said to be strongly minimal if any definable subset of X is finite or cofinite (in X).
(ii) Let A be a small set of parameters, and X, Y, A-definable sets. We say X is orthogonal to Y if for any $B \supset A$, and tuples a from X and b from Y, a is independent from b over B.
(iii) Let D be a strongly minimal set, and X a definable set. We say X is almost strongly minimal with respect to D if for some small set of parameters A over which both D and X are defined, $X \subseteq acl(D \cup A)$.

The following elementary piece of commutative finite Morley rank group theory was proved in [6] (Lemma 4.6).

Fact 1.6 *Again we work in a structure M as in Definition 1.5.*
Let A be a small set of parameters, let D_1,..,D_n be strongly minimal sets defined over A. Let G be a definable connected commutative group contained in $acl(A \cup D_1 \cup ... \cup D_n)$. Then A is a finite almost direct product of connected definable subgroups, each of which is almost strongly minimal with respect to some D_i.

The above applies to $\mathcal{U}$. It should be noted that in this context, independence has the following characterisation: Let A be a small set, and a, b tuples. Let F be the algebraic closure of the differential field generated by A. Then a is independent from b over A iff $F < a >$ is algebraically disjoint from $F < b >$ over F.

If X is an algebraic variety (in the sense of the universal domain $\mathcal{U}$) and k is a subfield, we say that X descends to k is X is isomorphic (as an algebraic variety) to one defined over k.

Fact 1.7 *(i) Let G_m denote the multiplicative group of $\mathcal{U}$. Then $G_m(C)$ is the unique smallest infinite definable subgroup of G_m. Moreover the map taking x to x'/x is a definable homomorphism from G_m onto (the additive group) $\mathcal{U}$, with kernel $G_m(C)$.*
(ii) Suppose A to be a simple d-dimensional abelian variety defined over F. Then A has a unique smallest infinite definable subgroup G say. G has finite Morley rank, is F-definable, and there is an F-definable surjective homomorphism μ from A onto the vector group $\mathcal{U}^d$ whose kernel is G. If A is defined over C, then G is precisely $A(C)$. If A does not descend to C then G is strongly minimal, and orthogonal to the definable set C.

Explanation. (i) is proved by Cassidy [2].
(ii). Buium [1] proves that A has a unique smallest differential algebraic subgroup G, that G is "finite-dimensional" andd that A/G is isomorphic (as a differential algebraic group) to some subgroup L of some $\mathcal{U}^n$. As pointed out in [17], work of Cassidy [3] together with the fact that L must have monomial U-rank, implies that L is definably isomorphic to some $\mathcal{U}^m$. The finite-dimensionality of G forces $m = d$. Also all these definable maps are defined over F. If A is defined over C (so over $C(F)$), then $A(C)$ is an infinite definable subgroup of A, which has no proper infinite definable subgroups, so $A(C) = G$. The remainder of (ii) is due to Hrushovski and Sokolvic [7].

2 The main result

In this section we prove:

Theorem 2.1 *Suppose F to be a differential field with the following features:*
(i) $C(F)$ has infinite transcendence degree, and
(ii) for some finite tuple b from F, F is the algebraic closure of $C(F) < b >$.
Let A be a simple abelian variety, or a 1-dimensional algebraic torus, defined over F. Let G the smallest infinite definable subgroup of A. Then F has a differential Galois extension K with Galois group G.

For the remainder of this section F, b, A and G will be as in the hypotheses of the Theorem. First note that as F is algebraically closed, so is $C(F)$ and thus $C(F) = C(\hat{F})$.

Throughout the proof, there will be three different cases to consider: A is a simple abelian variety which does not descend to C, A is a simple abelian variety which does descend to C, and A is a 1-dimensional algebraic torus. We will call these case (a), case (b) and case (c), respectively. We begin with some reductions. In case (b) it is clear that A is rationally isomorphic to a simple abelian variety B defined over $C(\hat{F}) = C(F)$. Moreover the isomorphism is defined over F. The image of G under this isomorphism will then be the smallest infinite definable subgroup of B, which by Fact 1.7 is precisely $B(C)$. Thus we may assume, in case (b), that A is defined over $C(F)$ and that $G = A(C)$. In case (c), it is well-known that A is F-rationally isomorphic to G_m. Again, by Fact 1.7, we may assume that $A = G_m$ and $G = G_m(C)$.

By Fact 1.7, A/G can be F-definably identified with $\mathcal{U}^n$ (where $n = dim(A)$). The main job will be to show that the restriction of μ to $A(F)$ is not onto F^n. We may assume that A, G and μ are all defined over b. We will need a few lemmas.

Lemma 2.2 *$G(F) = G(\hat{F})$.*

Proof. In cases (b) and (c), $G(F) = G(C(F))$ and the lemma follows because, as remarked above, $C(F) = C(\hat{F})$. So we may assume case (a). In this case by Fact 1.7, G is strongly minimal. Since G contains $Tor(A)$, and the latter is contained in $acl(F) = F$, $G(F)$ is infinite. If the lemma were false there would be $\alpha \in G(\hat{F}) - G(F)$. $tp(\alpha/F)$ is isolated by a formula $\phi(x)$. As F is algebraically closed (in the sense of DCF_0 too!), $\phi(x)$ has infinitely many solutions, all in G and none in $G(F)$. As $G(F)$ is infinite, this contradicts the strong minimality of G.

Now let d be a finite tuple from $C(F)$ such that b is independent from $C(F)$ over d (in the sense of DCF_0). This exists (and is finite) by ω-stabiity of DCF_0. Let $c = (c_1, .., c_n)$ be chosen from $C(F)$ to be algebraically independent over d (as $C(F)$ is assumed to have infinite transcendence degree).We may assume that d is a tuple of algebraically independent elements. Extend d to a subset D of $C(F)$ such that $D \cup \{c_1, .., c_n\}$ is a transcendence basis for $C(F)$. Let F_0 be the algebraic closure of the differential field generated by $D \cup b$. We then have:

Fact 2.3 *(i) c is a generic point of C^n over F_0 (in the sense of DCF_0). (ii) F is the algebraic closure of $F_0(c)$.*

Proof. (ii) is clear. For (i) note first that c is a generic point of C^n over $\emptyset$. By the choice of d, b is independent from c over D. By symmetry, c is independent from $D \cup b$ over D. But c is independent from D over $\emptyset$. Thus c is independent from $D \cup b$ and so also from F_0 over $\emptyset$. Together with the first sentence, this shows that c is a generic point of C^n over F_0.

Proposition 2.4 *There is no $\alpha \in A(F)$ such that $\mu(\alpha) = c$*

Proof. Suppose by way of contradiction that there is such α. Let $G_1 = \mu^{-1}(C^n)$. It is clear that G_1 is F_0-definable, and connected.
Claim. $G_1 \subseteq acl(F_0 \cup G \cup C)$.
Proof of claim. Let β be a generic point of G_1 over F_0. Let $e = \mu(\beta)$. It is clear that e is a generic point of C^n over F_0. So by Fact 2.3 (i), $tp(e/F_0) = tp(c/F_0)$. Thus there is $\gamma \in G_1$ such that $tp(\gamma, e/F_0) = tp(\alpha, c/F_0)$. In particular (using Fact 2.3 (ii)), $\gamma \in acl(F_0, e)$. As $\mu(\gamma) = \mu(\beta)$, there is $\epsilon \in G$ such that $\beta = \gamma.\epsilon$. Thus $\beta \in acl(F_0, G, C)$. Now any element of G_1 is a product of generic elements. Thus $G_1 \subseteq acl(F_0 \cup G \cup C)$, proving the claim.
We now separate into the three cases again.
Case (a). So by Fact 1.7, G is strongly minimal and orthogonal to C. Also note C is strongly minimal. By the Claim above, and Fact 1.6, we can write G_1 as an almost direct product $G_2 \cdot G_3$ where G_2 is almost strongly minimal with respect to G and G_3 is almost strongly minimal with respect to C. As G is orthogonal to C, G is a subgroup of G_1 and C^n is a quotient of G_1, it follows that G_1 can neither be almost strongly minimal with respect to G nor almost strongly minimal with respect to C. Thus neither G_2 nor G_3 can be trivial. But then we easily contradict the fact (contained in 1.7) that A has a unique minimal infinite definable subgroup.
Case (b) Here clearly $G_1 \subseteq acl(F_0 \cup C)$. A basic result in stable groups implies that for some finite normal subgroup N of G_1, $(G_1/N) \subseteq dcl(F_0 \cup C)$. We will assume for now that N is trivial, get a contradiction, and then justify the assumption. By separation of parameters, and the fact that C

with all the structure induced from $\mathcal{U}$ is an algebraically closed field without additional structure, there is a group G_2 definable in the structure $(C, +, \cdot)$ and a definable (in $\mathcal{U}$) isomorphism of G_1 with G_2. So (by Theorem 4.13 of [19]) we may assume G_2 to be an algebraic group in the sense of the universal domain C (namely an algebraic group in the constants). Note that G_2 is connected as an algebraic group (as G_1 is connected as a definable group). Now f induces an isomorphism between G and some definable subgroup G_3 of G_2. As $G = A(C)$ is also an algebraic group in the constants, and by separation of parameters, f is definable by a formula with parameters in C, actually f must be an isomorphism of algebraic groups in the sense of the universal domain C. Thus G_3 is an abelian variety in the sense of C. But it is well-known that any abelian variety which is a subgroup of an commutative algebraic group has a complement, namely there is an algebraic subgroup G_4 of G_2 (in the sense of C) such that G_2 is an almost direct product of G_3 and G_4. Pulling back G_4 to G_1 by f, we again contradict the fact that G is the unique smallest infinite definable subgroup of A. So we have a contradiction in this case, assuming N to be trivial. In general, N is clearly a finite subgroup of $Tor(G)$, and G/N is also an abelian variety in the sense of the constants. The argument above goes through with G_1/N in place of G_1 and G/N in place of G, and we still get a contradiction after pulling back G_4 and lifting from G_1/N to G_1.
Case (c). In this case $n = 1$, A is the multiplicative group of $\mathcal{U}$ and G is the multiplicative group of the constants. As in case (b), we obtain a definable isomorphism f of G_1 with an algebraic group in the constants G_2. Again the image G_3 of G under f must be a 1-dimensional algebraic torus. On the other hand, as G_1/G is definably identified with the additive group of C, we see, for the same reason, that G_2/G_3 is unipotent, in particular linear. Thus G_2 is a commutative linear algebraic group in the sense of C, and G_3 is a maximal algebraic torus in G_2. It is again well-known (see [4]) that G_2 is an almost direct product $G_3 \cdot G_4$ for some unipotent algebraic subgroup G_4 of G_2. Pulling back G_4 to G_1 again contradicts G being the unique smallest infinite definable subgroup of A.
The proposition is proved.

Remark 2.5 *The proposition above generalises, by a similar style of proof, to the situation where A is an arbitrary semi-abelian variety defined over F, G is the smallest definable subgroup of A containing $Tor(A)$, and μ is the* *homomorphism from A onto some suitable $\mathcal{U}^m$ with kernel G.*

We can now complete the proof of Theorem 2.1. Let $\alpha \in A(\hat{F})$, $\alpha \notin A(F)$ be such that $\mu(\alpha) = c$. By Proposition 2.4, $\alpha \notin A(F)$. Let $K = F < \alpha >$. By Lemmas 1.4 and 2.2, K will be a differential Galois extension of F with Galois group G once we have shown that the formula $\mu(x) = c$ isolates a complete type over F. Let $\phi(x)$ be a formula over F which *does* isolate $tp(\alpha/F)$. Then $\phi(x)$ has infinitely many solutions in $\hat{F}$ (as F is algebraically closed), all satisfying $\mu(x) = c$. So for each such solution β there is $g \in G(\hat{F})$ such that $\alpha \cdot g = \beta$. Remember that $G(\hat{F}) = G(F)$. Thus $\{g \in G(\hat{F}) : tp(\alpha \cdot g/F) = tp(\alpha/F)\}$ is a infinite definable subgroup of G. But in case (a), we know G is strongly minimal, so has no proper infinite definable subgroups, whereas in cases (b) and (c), G is either a simple abelian variety or a 1-dimensional torus, in the sense of the constants, so has no proper infinite definable subgroups. As $G(\hat{F})$ acts transitively on the set of solutions of $\mu(x) = c$ it follows that all solutions of $\mu(x) = c$ have the same type over F, which is what we had to prove.

3 An application

There has been some interest in the question of whether any (nontrivial) differential fields other than differentially closed fields can be superstable. In [17] it was shown that a nontrivial superstable differential field has no proper differential Galois extension (moreover it is known that any superstable field must be algebraically closed). On the other hand, it had also been wondered whether the closure under algebraic and strongly normal extensions of a field of constants, could be superstable. Using Theorem 2.1, we will give a negative answer to this question, at least if the field of constants in question has infinite transcendence degree.

Definition 3.1 *Let F be a differential field. By the strongly normal closure of F (inside $\hat{F}$) we mean the smallest differential subfield K of $\hat{F}$ which contains F, is algebraically closed, and has no proper strongly normal extension (inside $\hat{F}$).*

Remark 3.2 *It is not difficult to see that the strongly normal closure of F, which we can think of as its "Kolchin hull" exists. It can also be described model-theoretically as $\{a \in \hat{F} : tp(a/F)$ is C-analysable$\}$.*

Theorem 3.3 *Let F_0 be a field of constants of infinite transcendence degree. Let F_1 be the strongly normal closure of F_0. Then $Th(F_1)$ is not superstable.*

Proof. We may assume F_0 to be algebraically closed. Let $t \in \hat{F}$ be such that $\delta(t) = 1$. Then $F_0 < t > (= F_0(t))$ is a strongly normal extension of F_0 (whose Galois group is the additive group of the constants). Let $F = acl(F_0 < t >)$. Then $F \subseteq F_1$. Let A be some elliptic curve $y^2 z = x(x-z)(x-tz)$. Then A is defined over F but is not rationally isomorphic to an elliptic curve defined over C. Let G be the smallest infinite definable subgroup of A. Theorem 2.1 applies to this situation, yielding a differential Galois extension $F < \alpha >$ of F with Galois group G (where $\alpha \in A$, and $\mu(\alpha) \in F$). $tp(\alpha/F)$ is the generic type of a translate of G, and hence, by Fact 1.7, is orthogonal to the definable set C. On the other hand, Remark 3.2 implies that α is independent from F_1 over F, in particular $\alpha \notin A(F_1)$. It is then easy to see that $F_1 < \alpha >$ is a differential Galois extension of F_1 with Galois group G. By [17], $Th(F_1)$ is not superstable.

References

[1] A. Buium, *Differential algebraic groups of finite dimension*, Lecture Notes in Mathematics 1506, Springer-Verlag, 1992.

[2] P.J. Cassidy, Differential algebraic groups, American Journal of Mathematics 94 (1972), 891-954.

[3] P. J. Cassidy, Unipotent differential algebraic groups, in *Contributions to Algebra*, Academic Press, 1977, 83-116.

[4] A. Borel, Linear Algebraic Groups,Springer-Verlag, 1991.

[5] W.A.Hodges, *Model Theory*, Encyclopedia of Mathematical Sciences, 42, Cambridge University Press, 1993.

[6] E. Hrushovski, The geometric case of the Mordell-Lang conjecture, to appear in Journal of A.M.S.

[7] E. Hrushovski and Z. Sokolovic, Minimal sets in differentially closed fields, to appear in Transactions of A.M.S.

[8] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, 1973.

[9] E.R. Kolchin, *Differential Algebraic Groups*, Academic Press, 1985.

[10] J. Kovacic, The inverse problem in the Galois theory of differential fields, Annals of Mathematics 89 (1969), 583-608.

[11] J. Kovacic, On the inverse problem in the Galois theory of differential fields, Annals of Mathematics 93 (1971), 269-284.

[12] A. Magid, *Lectures on Differential Galois Theory*, University Lecture Series, vol. 7, A.M.S., 1994.

[13] Ju. Manin, Algebraic curves over fields with differentiation, A.M.S. Translations,(2), vol. 37 (1964), 59-78.

[14] D. Marker, Model theory of differential fields, to appear in *Model Theory and Fields*, Lecture Notes in Logic, Springer-Verlag.

[15] C. Mitschi and M.F. Singer, Connected linear groups as differential Galois groups, preprint 1995.

[16] A. Pillay, Differential Galois theory I, submitted.

[17] A. Pillay, Differential Galois theory II, submitted.

[18] A. Pillay, Some foundational questions concerning differential algebraic groups, to appear in Pacific Journal of Mathematics.

[19] B. Poizat, *Groupes Stables*, Nur-al mantiq wa-ma'rifah, 1987, Villeurbanne.

[20] C. Tretkoff and M. Tretkoff, Solution of the inverse problem of differential Galois theory in the classical case, American Journal of Mathematics 101 (1979), 1327-1332.