

D-GROUPS AND THE DIXMIER-MOEGLIN EQUIVALENCE

JASON BELL, OMAR LEÓN SÁNCHEZ, AND RAHIM MOOSA

ABSTRACT. A differential-algebraic geometric analogue of the Dixmier-Moeglin equivalence is articulated, and proven to hold for D -groups over the constants. The model theory of differentially closed fields of characteristic zero, in particular the notion of analysability in the constants, plays a central role. As an application it is shown that if R is a commutative affine Hopf algebra over a field of characteristic zero, and A is an Ore extension to which the Hopf algebra structure extends, then A satisfies the classical Dixmier-Moeglin equivalence. Along the way it is shown that all such A are Hopf Ore extensions in the sense of [Brown et al., “Connected Hopf algebras and iterated Ore extensions”, *Journal of Pure and Applied Algebra*, 219(6), 2015].

CONTENTS

1. Introduction	1
2. The δ -DME for D -groups over the constants	4
3. Twisting by a group-like element	16
4. The DME for Ore extensions of commutative Hopf algebras	24
References	32

1. INTRODUCTION

This article is about an analogue of the Dixmier-Moeglin equivalence for differential-algebraic geometry. (The immediate motivation is an application to the classical noncommutative Dixmier-Moeglin problem, which we will describe later in this introduction.) The main objects of study here are D -varieties. An introduction to this category is given in §2.1, but let us at least recall here that a D -variety (over the constants) is an algebraic variety V over a field k of characteristic zero, equipped with a regular section to the tangent bundle $s : V \rightarrow TV$. A D -subvariety is an algebraic subvariety W for which the restriction $s|_W$ is a section to the tangent bundle of W . There are natural notions of D -morphism and D -rational map. For convenience, let us assume that k is algebraically closed. We are interested in the following properties of an irreducible D -subvariety $W \subseteq V$ over k :

Date: November 30, 2016.

2010 Mathematics Subject Classification: 03C98, 12H05, 16T05, 16S36.

Keywords: D -groups, model theory of differentially closed fields, Dixmier-Moeglin equivalence, Hopf Ore extensions.

Acknowledgements: J. Bell and R. Moosa were partially supported by their respective NSERC Discovery Grants.

- δ -primitivity. There is a k -point of W that is not contained in any proper D -subvariety of W over k .
- δ -local-closedness. There is a maximum proper D -subvariety of W over k .
- δ -rationality. There is no nonconstant rational map from (W, s) to $(\mathbb{A}^1, 0)$ over k , where here 0 denotes the zero section to the tangent bundle of the affine line.

The question is, for which ambient D -varieties (V, s) are these three properties equivalent for all D -subvarieties? It is not hard to see, and is spelled out in the proof of Corollary 2.13 below, that in general

$$\delta\text{-local-closedness} \implies \delta\text{-primitivity} \implies \delta\text{-rationality}.$$

In earlier work [1], together with Stéphane Launois, we used the model theory of the Manin kernel to produce (in any dimension ≥ 3) a D -variety which is itself δ -rational but not δ -locally-closed. Here we focus on positive results. The main one, which appears as Corollary 2.16 below, is the following:

Theorem A. *Suppose (G, s) is a D -group over the constants – that is, G is an algebraic group and $s : G \rightarrow TG$ is a homomorphism of algebraic groups. Then for any D -subvariety of (G, s) , δ -rationality implies δ -local-closedness. In particular, for every D -subvariety of (G, s) , δ -rationality, δ -primitivity, and δ -local-closedness are equivalent properties.*

The proof of Theorem A relies on the model theory of differentially closed fields. In model-theoretic parlance, the point is that δ -rationality of (V, s) is equivalent to the generic type of the corresponding Kolchin closed set being weakly orthogonal to the constants, while δ -local-closedness means that the type is isolated. One context in which one can prove, using model-theoretic binding groups, for example, that weak orthogonality to the constants implies isolation, is when the type in question is analysable in the constants. We give a geometric explanation of analysability in §2.5 in terms of what we call *compound isotriviality* of D -varieties. The reader can look there for a precise definition, but suffice it to say that a compound isotrivial D -variety is one that admits a finite sequence of fibrations where at each stage the fibres are isomorphic (possibly over a differential field extension of the base) to D -varieties where the section is the zero section. We show that for compound isotrivial D -varieties δ -rationality implies δ -local-closedness (Proposition 2.12). Then we show, using known results about the structure of differential-algebraic groups, that every D -subvariety of a D -group over the constants is compound isotrivial (Proposition 2.15). Theorem A follows.

It turns out that for our intended application, namely Theorem B2 appearing later in this introduction, we need Theorem A to work for D -varieties that are slightly more general than D -groups. Given an affine algebraic group G , we may as well assume that $G \subseteq \mathrm{GL}_n$, so that a regular section to the tangent bundle is then of the form $s = (\mathrm{id}, \bar{s})$ where $\bar{s} : G \rightarrow \mathrm{Mat}_n$. It is not hard to check from how the algebraic group structure is defined on the tangent bundle, that $s : G \rightarrow TG$ being a homomorphism is equivalent to the following identity: $\bar{s}(gh) = \bar{s}(g)h + g\bar{s}(h)$, where $g, h \in G$ are matrices and all addition and multiplication here is matrix addition and multiplication. Now suppose we are given a homomorphism to the multiplicative group, $a : G \rightarrow \mathbb{G}_m$. By an *a -twisted D -group* we mean a D -variety (G, s) where G is an affine algebraic group and $s = (\mathrm{id}, \bar{s})$ satisfies the identity: $\bar{s}(gh) = \bar{s}(g)h + a(g)g\bar{s}(h)$. So an a -twisted D -group is a D -group exactly

when $a = 1$. We are able to show that D -subvarieties of a -twisted D -groups are also compound isotrivial. This yields the following generalisation of Theorem A: *For any D -subvariety of an a -twisted D -group over the constants, δ -rationality, δ -primitivity, and δ -local-closedness are equivalent properties.* The passage from D -groups to a -twisted D -groups turns out to be technically quite difficult, and is done in Section 3.

It is worth pointing out that we have been intentionally ambiguous about the field of definitions in the statements of Theorem A and its a -twisted generalisation. The reason for this is that the results actually hold true for D -subvarieties of (G, s) that are defined over differential field extensions of the base field k . To make this precise one has to give a more general definition of D -variety using prolongations rather than tangent bundles, and we have decided to delay this to the main body of the article. While the final conclusion we are interested in is about D -subvarieties over k , this possibility of passing to base extensions is an important part of the inductive arguments involved.

Now for the application to noncommutative algebra, to which Section 4 is dedicated. The classical Dixmier-Moeglin equivalence (DME) is about prime ideals in a noetherian associative algebra over a field of characteristic zero; it asserts the equivalence between three properties of such prime ideals: primitivity (a representation-theoretic property), local-closedness (a geometric property), and rationality (an algebraic property). Precise definitions are given at the beginning of §4. We are interested in the question of when the DME holds for skew polynomial rings $R[x; \delta]$ over finitely generated commutative integral differential k -algebras (R, δ) . Recall that $R[x; \delta]$ is the noncommutative polynomial ring in x over R where $xr = rx + \delta(r)$. This question is not vacuous since examples of such skew polynomial rings failing the DME were given in [1]; indeed, these were the first counterexamples to the DME of finite Gelfand-Kirillov dimension. The connection to D -varieties should be clear: $R = k[V]$ for some irreducible algebraic variety V , and the k -linear derivation δ induces a regular section $s : V \rightarrow TV$. So the study of such (R, δ) is precisely the same thing as the study of D -varieties. We are able to prove (this is Proposition 4.6 below) that $R[x; \delta]$ will satisfy the DME if δ -rationality implies δ -locally-closedness for all D -subvarieties of the D -variety (V, s) associated to (R, δ) . Theorem A therefore answers our question in the special case of differential Hopf algebras.

Theorem B1. *If (R, δ) is a finitely generated commutative integral differential Hopf k -algebra then $R[x; \delta]$ satisfies the DME.*

Being a differential Hopf algebra means that R has the structure of a Hopf algebra and that δ commutes with the coproduct – this is equivalent to saying that (R, δ) comes from an affine D -group (G, s) .

More generally than skew polynomial rings, we consider Ore extensions: Suppose R is a finitely generated commutative integral k -algebra, σ is a k -algebra automorphism of R , and δ is a k -linear σ -derivation of R – meaning that $\delta(rs) = \sigma(r)\delta(s) + \delta(r)s$. Recall that the Ore extension $R[x; \sigma, \delta]$ is the noncommutative polynomial ring in the variable x over R where $xr = \sigma(r)x + \delta(r)$. So when $\sigma = \text{id}$ we are in the skew polynomial case discussed above. What about the DME for $R[x; \sigma, \delta]$?

Theorem B2. *Suppose R is a finitely generated commutative integral Hopf k -algebra. If an Ore extension $R[x; \sigma, \delta]$ admits a Hopf algebra structure extending that on R , then $R[x; \sigma, \delta]$ satisfies the DME.*

That Theorem B1 is a special case of Theorem B2 uses the (known) fact that one can always extend the Hopf structure on a differential algebra R to the skew polynomial ring extension $R[x; \delta]$, namely by the coproduct induced by $\Delta(x) = x \otimes 1 + 1 \otimes x$. Theorem B2 appears as Theorem 4.1 below. Its proof goes via a reduction to the case when $\sigma = \text{id}$ and then an application of the stronger a -twisted version of Theorem A discussed above. Both of these steps use the work of Brown et al. [5] on Hopf Ore extensions. One obstacle is that while their results hold for much more general R than we are considering, they are conditional on the coproduct of the variable x in the Ore extension taking the special form

$$\Delta(x) = a \otimes x + x \otimes b + v(x \otimes x) + w$$

where $a, b \in R$ and $v, w \in R \otimes_k R$. This is part of their definition of a Hopf Ore extension, though they speculate about its necessity. We prove that when k is algebraically closed, after a linear change of variable, $\Delta(x)$ always has the above form. This is Theorem 4.2 below, and may be of independent interest:

Theorem C. *Suppose k is algebraically closed and R is a finitely generated commutative integral Hopf k -algebra. If an Ore extension $R[x; \sigma, \delta]$ admits a Hopf algebra structure extending that of R then, after a linear change of the variable x ,*

$$\Delta(x) = a \otimes x + x \otimes b + w$$

for some $a, b \in R$, each of which is either 0 or group-like, and some $w \in R \otimes_k R$. In particular, $R[x; \sigma, \delta]$ is a Hopf Ore extension of R .

It has been conjectured [3] that all finitely generated complex noetherian Hopf algebras of finite Gelfand-Kirillov dimension satisfy the DME. Theorem B2 verifies a special case. To make more significant progress on this conjecture one would like to pass from Hopf Ore extensions to iterated Hopf Ore extensions. As of now, this appears to be beyond the scope of the techniques used here.

Throughout this paper, by an *affine* k -algebra we mean a finitely generated commutative k -algebra that is an integral domain.

2. THE δ -DME FOR D -GROUPS OVER THE CONSTANTS

In this chapter we prove Theorem A of the introduction. After some preliminaries, we articulate in §2.3 the differential-algebraic geometric analogue of the DME suggested in the introduction, and call it the δ -DME. A sufficient condition for this to hold in terms of the model-theoretic notion of analysability to the constants is given in §2.5, and then applied to show that D -groups over the constants satisfy the δ -DME in §2.6. In a final section we reformulate δ -DME algebraically, as a statement about commutative differential Hopf algebras, thereby preparing the stage for the application to the classical DME in chapter 4.

2.1. Preliminaries on D -varieties. Suppose k is a field of characteristic zero equipped with a derivation δ . In this section we review the notion of a D -variety over k . Several more detailed expositions can be found in the literature, for instance Buium [6] who introduced the notion, and also [13, §2].

We first need to recall what prolongations are. If $V \subseteq \mathbb{A}^n$ is an affine algebraic variety over k , then by the δ -prolongation of V is meant the algebraic variety $\tau V \subseteq \mathbb{A}^{2n}$ over k whose defining equations are

$$\begin{aligned} P(X_1, \dots, X_n) &= 0 \\ P^\delta(X_1, \dots, X_n) + \sum_{i=1}^n \frac{\partial P}{\partial X_i}(X_1, \dots, X_n) \cdot X_i &= 0 \end{aligned}$$

for each $P \in I(V) \subset k[X_1, \dots, X_n]$. Here P^δ denotes the polynomial obtained by applying δ to all the coefficients of P . The projection onto the first n coordinates gives us a surjective morphism $\pi : \tau V \rightarrow V$.

Note that if K is any δ -field extension of k , and $a \in V(K)$, then

$$\nabla(a) := (a, \delta a) \in \tau V(K).$$

If V is defined over the constant field of (k, δ) then τV is nothing other than the tangent bundle TV . In general, τV will be a torsor for the tangent bundle; for each $a \in V$ the fibre $\tau_a V$ is an affine translate of the tangent space $T_a V$. In particular, if V is smooth and irreducible then so is τV .

Taking prolongations is a functor which acts on morphisms $f : V \rightarrow W$ by acting on their graphs. It preserves the following properties of a morphism: étaleness, being a closed embedding, and being smooth. The functor τ acts naturally on rational maps also; this is because for U a Zariski open subset of an irreducible variety V , $\tau V \upharpoonright_U = \tau(U)$ is Zariski open in $\tau(V)$. Moreover, prolongations commute with base extension to δ -field extensions.

We have restricted our attention here to the affine case merely for concreteness. The prolongation construction extends to abstract varieties by patching over an affine cover in a natural and canonical way.

A D -variety over k is an algebraic variety V over k equipped with a regular section $s : V \rightarrow \tau V$ over k . An example is when V is defined over the constants and $s : V \rightarrow TV$ is the zero section.

If V is affine then a D -variety structure on V is nothing other than an extension of δ to the co-ordinate ring $k[V]$. Indeed, if $s : V \rightarrow \tau V$ is given by $s(X) = (X, s_1(X), \dots, s_n(X))$ in variables $X = (X_1, \dots, X_n)$, then we can extend δ to $k[X]$ by $X_j \mapsto s_j(X)$, and this will induce a derivation on $k[V]$. Conversely, given an extension of δ to $k[V]$, and choosing $s_j(X)$ to be such that $\delta(X_j + I(V)) = s_j(X) + I(V)$, we get that $s := (\text{id}, s_1, \dots, s_n) : V \rightarrow \tau V$ is a regular section.

A D -subvariety of (V, s) is a closed algebraic subvariety $W \subseteq V$, over a possibly larger δ -field K , such that $s(W) \subseteq \tau W$. In principle one should talk about the base extension of V to K before talking about subvarieties over K , but as prolongations commute with base extension, and following standard model-theoretic practices, we allow D -subvarieties to be defined over arbitrary δ -field extensions unless explicitly stated otherwise.

A D -variety (V, s) over k is said to be k -irreducible if V is k -irreducible as an algebraic variety. In this case s induces on $k(V)$ the structure of a δ -field extending k . A D -variety (V, s) is called *irreducible* if V is absolutely irreducible. In

general, every irreducible component of V is a D -subvariety over k^{alg} and these are called the *irreducible components* of (V, s) .

A *morphism* of D -varieties $(V, s) \rightarrow (W, t)$ is a morphism of algebraic varieties $f : V \rightarrow W$ such that

$$\begin{array}{ccc} \tau V & \xrightarrow{\tau f} & \tau W \\ \uparrow s & & \uparrow t \\ V & \xrightarrow{f} & W \end{array}$$

commutes. It is not hard to verify that the pull-back of a D -variety, and the Zariski closure of the image of a D -variety, under a D -morphism, are again D -varieties.

In the same way, we can talk about *rational maps* between D -varieties. A useful fact is that if U is a nonempty Zariski open subset of V , then the prolongation of U is the restriction of τV to U , and so $(U, s|_U)$ is a D -variety in its own right. So a rational map on V is a D -rational map if it is a D -morphism when restricted to the Zariski open subset on which it is defined.

A D -constant rational function on a D -variety (V, s) over k is a rational map over k from (V, s) to $(\mathbb{A}^1, 0)$ where 0 denotes the zero section to the tangent bundle of the affine line. In the case when (V, s) is k -irreducible, they correspond precisely to the δ -constants of $(k(V), \delta)$.

2.2. Differentially closed fields and the Kolchin topology. Underlying our approach to the study of D -varieties is the model theory of *existentially closed* δ -fields (of characteristic zero). These are δ -fields K with the property that any finite sequence of δ -polynomial equations and inequations over K which have a solution in some δ -field extension, already have a solution in K . The class of existentially closed δ -fields of characteristic zero is axiomatisable in first-order logic, and its theory is denoted by DCF_0 . We will work in a fixed model of this theory, an existentially closed δ -field K . In particular, K is algebraically closed. We let K^δ denote the field of constants of K ; it is an algebraically closed field that is *pure* in the sense that the structure induced on it by DCF_0 is simply that given by the language of rings.

Suppose (V, s) is a D -variety over K . Let $x \in V(K)$. Note that $\{x\}$ is a D -subvariety if and only if $\nabla(x) = s(x)$ where recall that $\nabla : V(K) \rightarrow \tau V(K)$ is given by $x \mapsto (x, \delta x)$. We call such points *D -points*, and denote the set of all D -points in $V(K)$ by $(V, s)^\sharp(K)$. It is an example, the main example we will encounter, of a *Kolchin closed* subset of $V(K)$. In general a Kolchin closed subset of the K -points of an algebraic variety is one that is defined Zariski-locally by the vanishing of δ -polynomials. Note that when (V, s) is defined over the constants and s is the zero section, $(V, s)^\sharp(K) = V(K^\delta)$.

One of the main consequences of working in an existential closed δ -field is that $(V, s)^\sharp(K)$ is Zariski-dense in $V(K)$. In particular, for any subvariety $W \subseteq V$, we have that W is D -subvariety if and only if $W \cap (V, s)^\sharp(K)$ is Zariski dense in $W(K)$.

Suppose (V, s) is k -irreducible for some δ -subfield k . If we allow ourselves to pass to a larger existentially closed δ -field, then we can always find a *k -generic D -point* of (V, s) , that is, a D -point $x \in (V, s)^\sharp(K)$ that is Zariski-generic over k in V . Note that such a point is also Kolchin-generic in $(V, s)^\sharp(K)$ over k in the sense that it is not contained in any proper Kolchin closed subset defined over k .

In order to ensure the existence of generic D -points without having to pass to larger δ -fields, it is convenient to assume that K is already sufficiently large, namely *saturated*. This means that if k is a δ -subfield of strictly smaller cardinality than K , and \mathcal{F} is a collection of Kolchin constructible sets over k every finite subcollection of which has a nonempty intersection, then \mathcal{F} has a nonempty intersection.

2.3. An analogue of the DME for D -varieties. We fix from now on a saturated existentially closed δ -field K of sufficiently great cardinality. So K serves as a universal domain for δ -algebraic geometry (and hence, in particular, algebraic geometry). We also fix a small δ -subfield $k \subset K$ that will serve as the field of coefficients.

Definition 2.1 (δ -DME for D -varieties). Suppose (V, s) is a D -variety over k . We say that (V, s) *satisfies the δ -DME over k* , if for every k -irreducible D -subvariety $W \subseteq V$, the following are equivalent:

- (i) (W, s) is δ -*primitive*: there exists a point $p \in W(k^{\text{alg}})$ that is not contained in any proper D -subvariety of W over k .
- (ii) (W, s) is δ -*locally-closed*: it has a maximum proper D -subvariety over k .
- (iii) (W, s) is δ -*rational*: $k(W)^\delta \subseteq k^{\text{alg}}$.

Remark 2.2. As the model-theorist will notice, and as we will prove in the next section, W being δ -locally closed means that the Kolchin generic type p of $(W, s)^\#(K)$ over k is isolated. The model-theoretic meaning of δ -rationality is that p is weakly orthogonal to the constants. On the other hand, it is not clear how to express *a priori* the δ -primitivity of W as a model-theoretic property of p .

Without additional assumptions on k there is no hope for the δ -DME being satisfied. For example, there are positive-dimensional δ -rational D -varieties over any k , but if k is differentially closed then the only δ -locally closed D -varieties over k are zero-dimensional. This is because every D -variety over a differentially closed field k will have a Zariski dense set of D -points over k , and so a D -subvariety over k containing all of them could not be proper. We are interested, however, in the case when k is very much not differentially closed; namely, when δ is trivial on k .

Proposition 2.3. *For any k -irreducible D -variety, δ -local-closedness implies δ -primitivity. Moreover, if $k \subseteq K^\delta$ then δ -primitivity implies δ -rationality.*

Proof. Let (W, s) be a k -irreducible D -variety.

Suppose (W, s) is δ -locally-closed, and denote by A the maximum proper D -subvariety of W over k . Then $p \in W(k^{\text{alg}}) \setminus A(k^{\text{alg}})$ witnesses δ -primitivity.

Now suppose that (W, s) is δ -primitive, and $p \in W(k^{\text{alg}})$ is not contained in any proper D -subvariety over k . Suppose $f \in k(W)$ is a δ -constant. We view it as a rational map between D -varieties, $f : (W, s) \rightarrow (\mathbb{A}^1, 0)$, and claim that it must be defined at p . If not, writing $f = \frac{a}{b}$ with $a, b \in k[W]$, we must have $b(p) = 0$. The fact that f is a δ -constant implies, by repeated use of the quotient rule, that $\frac{\delta^\ell a}{\delta^\ell b} = \frac{a}{b} = f$, for all $\ell \geq 0$. Hence $\delta^\ell b(p) = 0$ also. It follows that p is contained in the D -subvariety $V(I)$ where I is the δ -ideal of $k[W]$ generated by b . But the assumption on p would then imply that $V(I) = W$, contradicting the fact that $b \neq 0$. So f is defined at p and we may consider $f(p) \in \mathbb{A}^1(k^{\text{alg}})$. Because of our additional assumption that $k \subseteq K^\delta$, and hence $k^{\text{alg}} \subseteq K^\delta$, we have that $f(p)$ is a D -point of $(\mathbb{A}^1, 0)$. Now, let Λ be the orbit of $f(p)$ under the action of the

absolute Galois group of k . Then Λ is a finite D -subvariety of $(\mathbb{A}^1, 0)$ over k . Hence the Zariski closure of $f^{-1}(\Lambda)$ is a D -subvariety of W over k that contains p . It follows that $f^{-1}(\Lambda) = W$. So f is k^{alg} -valued on all of W . We have shown that $k(W)^\delta \subseteq k^{\text{alg}}$, as desired. \square

So the question becomes:

Question 2.4. Under the assumption that δ is trivial on k , for which D -varieties does δ -rationality imply δ -local-closedness?

In [1] it was pointed out that Manin kernels can be used to construct, in all Krull dimensions at least three, examples that were δ -rational but not δ -locally closed. It follows from the results there, moreover, that in Krull dimension at most two the δ -DME does hold. Question 2.4 should be, we think, of general interest in differential-algebraic geometry.

We will give a sufficient condition for δ -rationality to imply δ -local-closedness, having to do with analysability to the constants in the model theory of differentially closed fields. We will then use this condition to prove the δ -DME for D -groups over the constants.

2.4. Maximum D -subvarieties. Here we look closer at which D -varieties over k have a proper D -subvariety over k that contains all other proper D -subvarieties over k . This is something that never happens in the pure algebraic geometry setting: every variety over k has a Zariski dense set of k^{alg} -points, and each k^{alg} -point is contained in a finite subvariety defined over k . So a k -irreducible variety cannot have a maximum proper subvariety over k . In the enriched context of D -varieties there will be many D -points over a differential closure of k , say \tilde{k} , but a \tilde{k} -point need not live in a proper D -subvariety defined over k . So D -points are not an obstacle to the existence of a maximum proper D -subvariety. In fact, as the following lemma points out, the existence of a maximum proper D -subvariety is a natural property to consider from both the Kolchin topological and model-theoretic points of view.

We continue to work in our sufficiently saturated differentially closed field (K, δ) , and fix a δ -subfield k of coefficients.

Lemma 2.5. *Suppose (V, s) is a k -irreducible D -variety. The following are equivalent.*

- (i) (V, s) is δ -locally closed.
- (ii) (V, s) has finitely many maximal proper k -irreducible D -subvarieties.
- (iii) $\Lambda := (V, s)^\sharp(K) \setminus \bigcup\{(W, s)^\sharp(K) : W \subsetneq V \text{ } D\text{-subvariety over } k\}$ is Kolchin constructible.
- (iv) The Kolchin generic type of $(V, s)^\sharp(K)$ over k is an isolated type.

Proof. (i) \implies (ii). Let W be the maximum proper D -subvariety over k . The k -irreducible components of W are D -subvarieties of V , see for example [12, Theorem 2.1]. Every proper k -irreducible D -subvariety of V is contained in one of these components. So the maximal proper k -irreducible D -subvarieties of V are precisely the k -irreducible components of W .

(ii) \implies (iii). Let W_1, \dots, W_ℓ be the maximal proper k -irreducible D -subvarieties of V . Then

$$\bigcup\{(W, s)^\sharp(K) : W \subsetneq V \text{ } D\text{-subvariety over } k\} = (W_1, s)^\sharp(K) \cup \dots \cup (W_\ell, s)^\sharp(K).$$

(iii) \implies (iv). The Kolchin generic type of $(V, s)^\sharp(K)$ over k is the complete type $p(X)$ in DCF_0 axiomatised by the formulas saying that “ $X \in (V, s)^\sharp(K)$ ”, and, for each proper Kolchin closed subset A of $(V, s)^\sharp(K)$ over k , the formula “ $X \notin A$ ”. Note that as $(V, s)^\sharp(K)$ is defined by $\nabla(X) = s(X)$, the occurrences of $\delta_i X$ in the defining equations of A can be replaced by polynomials, so that $A = A^{\text{Zar}} \cap (V, s)^\sharp(K)$, where A^{Zar} denotes the Zariski closure of A in V . When A is over k , we have that A^{Zar} is a D -subvariety of V over k . It follows that the set of realisations of p is precisely Λ , so that Λ being Kolchin constructible implies that p is axiomatised by a single formula, that is, it is isolated.

(iv) \implies (i). Let Λ be as in statement (iii). As we have seen, this is the set of realisations of the Kolchin generic type of $(V, s)^\sharp(K)$ over k . The latter being isolated implies, by quantifier elimination, that Λ is Kolchin constructible. By saturation, this in turn implies that $A := \bigcup\{(W, s)^\sharp(K) : W \subsetneq V \text{ } D\text{-subvariety over } k\}$ is a finite union, and hence is itself a proper Kolchin closed subset over k . Then A^{Zar} is the maximum proper D -subvariety over k . \square

The following lemma will be useful in showing that certain D -varieties satisfy the equivalent conditions of Lemma 2.5.

Lemma 2.6. *Suppose $f : (V, s) \rightarrow (W, t)$ is a dominant D -rational map of k -irreducible D -varieties over k . The following are equivalent*

- (i) (V, s) has a maximum proper D -subvariety over k .
- (ii) (W, t) has a maximum proper D -subvariety over k , and for some (equivalently every) k -generic D -point η of W , the fibre $V_\eta := f^{-1}(\eta)^{\text{Zar}}$ has a maximum proper D -subvariety over $k(\eta)$.

Proof. This follows from the basic model-theoretic fact that “isolated over isolated is isolated”, using characterisation (iv) of the previous lemma. But it may be worth giving a self-contained algebro-geometric argument.

Note that since η is a D -point, $k(\eta)$ is a δ -field extension of k .

Let $V^\circ \subseteq V$ and $W^\circ \subseteq W$ be nonempty k -definable Zariski open subsets such that f restricts to a surjective D -morphism $f : V^\circ \rightarrow W^\circ$. Let E_V be the Zariski closure in V of $(V, s)^\sharp(K) \setminus V^\circ(K)$. Note that E_V is a proper D -subvariety of V over k with the property that any D -subvariety which is disjoint from V° must be contained in E_V . Similarly, we have E_W in W .

(i) \implies (ii). Let V' be the maximum proper D -subvariety of V over k .

The maximum proper D -subvariety of V_η over $k(\eta)$ will be $V_\eta \cap V'$. Indeed, if A_η is a proper D -subvariety of V_η over $k(\eta)$, then either A_η is disjoint from V° , or, considering the D -morphism $f : V^\circ \rightarrow W^\circ$, we have that $A_\eta \cap V^\circ$ is a proper D -subvariety of $f^{-1}(\eta)$ over $k(\eta)$ and hence is of the form $A^\circ \cap f^{-1}(\eta)$ for some proper D -subvariety A° of V° over k . In the former case A_η is contained in $E_V \subseteq V'$, and in the latter case, A_η is contained in the Zariski closure of A° which is also contained in V' .

The maximum proper D -subvariety of W over k will be $E_W \cup f(V')^{\text{Zar}}$. This follows from the fact that if B is a proper D -subvariety of W over k then either it is disjoint from W° , or $f^{-1}(B \cap W^\circ)$ is a proper D -subvariety of V° over k and hence contained in $V' \cap V^\circ$. In the former case $B \subseteq E_W$, and in the latter $B \subseteq f(V')^{\text{Zar}}$.

(ii) \implies (i). Let V'_η be the maximum proper D -subvariety of V_η over $k(\eta)$, and W' the maximum proper D -subvariety of W over k . We will show that V has only finitely many maximal proper k -irreducible D -subvarieties; by Lemma 2.5,

this will suffice. Suppose A is such. If A is disjoint from V° then $A \subseteq E_V$, and hence by maximality is a k -irreducible component of E_V . So this only accounts for finitely many, and we can restrict attention to those A that do meet V° . Then $A^\circ := A \cap V^\circ$ is a maximal proper k -irreducible D -subvariety of V° , and consider $f : V^\circ \rightarrow W^\circ$. If $f(A^\circ)$ is not Zariski-dense in W° , then $A^\circ \subseteq f^{-1}(W' \cap W^\circ)$, and so again by maximality it is a k -irreducible component of this set, and there are only finitely many such. So we can restrict to the case when $f(A^\circ)$ is Zariski-dense in W° . In that case, A° meets the generic fibre $f^{-1}(\eta)$, and the intersection is a maximal proper $k(\eta)$ -irreducible D -subvariety of $f^{-1}(\eta)$. Hence it is a $k(\eta)$ -irreducible component of $V'_\eta \cap V^\circ$. So there are only finitely many possibilities for $A^\circ \cap f^{-1}(\eta)$. But if two k -irreducible subvarieties map dominantly onto W° and have the same generic fibre above W° , then they are equal. That is, there are only finitely many possible such A , as desired. \square

2.5. Compound isotriviality. Our sufficient condition for δ -rationality to imply δ -local-closedness will come from looking at isotrivial D -varieties.

Definition 2.7. An irreducible D -variety (V, s) over k is said to be *isotrivial* if there is some δ -field extension $F \supseteq k$ such that (V, s) is D -birationally equivalent over F to a D -variety of the form $(W, 0)$ where W is defined over the constants F^δ and 0 is the zero section. We will say that a possibly reducible D -variety is isotrivial if every irreducible component is.

This definition comes from model theory, it is a geometric translation of the statement that the Kolchin generic type of $(V, s)^\sharp(K)$ over k is K^δ -internal. Note that there is some tension, but no inconsistency, between isotriviality and δ -rationality; for example, $(W, 0)$ is far from being δ -rational, instead of there being no new δ -constants in the rational function field we have that δ is trivial on all of $k(W)$. The reason these notions are not inconsistent is that the isotrivial (V, s) is only of the form $(W, 0)$ after base change – that is, over additional parameters – and that makes all the difference.

Fact 2.8. *A k -irreducible D -variety that is at once both δ -rational and isotrivial must be δ -locally closed.*

Proof. Suppose (V, s) is a k -irreducible isotrivial D -variety with $k(V)^\delta \subseteq k^{\text{alg}}$. We want to show that V has a maximum proper D -subvariety over k . The proof we give makes apparently essential use of model theory. We will show how the statement translates to the well-known fact that a type internal to the constants but weakly orthogonal to the constants is isolated.

Let p be the Kolchin generic type of $(V, s)^\sharp(K)$ over k . By Lemma 2.5, it suffices to show that p is isolated. That in turn reduces to showing that every extension of p to k^{alg} is isolated. Fix q an extension of p to k^{alg} . So q is the Kolchin generic type of $(\widehat{V}, s)^\sharp(K)$ over k^{alg} , for some irreducible component \widehat{V} of V . Isotriviality of (V, s) implies isotriviality of (\widehat{V}, s) , and this means that q is internal to the constants K^δ , see for example [13, Fact 2.6]. By stability, this implies that the binding group $\mathcal{G} = \text{Aut}(q/k^{\text{alg}}(K^\delta))$ is type-definable over k^{alg} , see for instance [9, Appendix B]. In fact, \mathcal{G} is definable: \mathcal{G} lives in the constants and by ω -stability of the induced structure on the constants, every type-definable group in K^δ is a definable group. So we have a definable group acting definably on the set of realisations of q .

On the other hand, for all $a \models q$ we have that

$$k^{\text{alg}}(a)^\delta \subseteq (k(a)^{\text{alg}})^\delta = (k(a)^\delta)^{\text{alg}} \subseteq k^{\text{alg}},$$

where the last containment uses our assumption on $k(V) = k(a)$. This shows that q is weakly orthogonal to K^δ . So the action of \mathcal{G} on the set of realisations of q is transitive. As \mathcal{G} is definable, the set of realisations of q must be definable – that is, q is isolated. \square

Using Lemma 2.6 we can extend Fact 2.8 to the case of D -varieties that are built up by a finite sequence of fibrations by isotrivial D -subvarieties.

Definition 2.9. An irreducible D -variety (V, s) over k is said to be *compound isotrivial* if there exists a sequence of irreducible D -varieties (V_i, s_i) over k , for $i = 0, \dots, \ell$, with dominant D -rational maps over k

$$V = V_0 \xrightarrow{f_0} V_1 \xrightarrow{f_1} \dots \longrightarrow V_{\ell-1} \xrightarrow{f_{\ell-1}} V_\ell = 0$$

where 0 denotes the zero-dimensional D -variety, and such that the generic fibres of each f_i are isotrivial. That is, for each $i = 0, \dots, \ell - 1$, if η is a k -generic D -point in V_{i+1} , then $f_i^{-1}(\eta)^{\text{Zar}}$, which is a $k(\eta)$ -irreducible D -subvariety of (V_i, s_i) , is isotrivial. We say (V, s) is compound isotrivial in ℓ steps.

While isotriviality is equivalent to the Kolchin generic type being internal to the constants, compound isotriviality corresponds to that type being *analysable* in the constants. As this is a less familiar notion, even among model theorists, we spell out the equivalence here.

Lemma 2.10. *Suppose (V, s) is an irreducible D -variety over k , and $a \in (V, s)^\sharp(K)$ is a k -generic D -point. Then (V, s) is compound isotrivial if and only if the type of a over k in DCF_0 is analysable in K^δ .*

Proof. Analysability in K^δ means that there are tuples $a = a_0, a_1, \dots, a_\ell$, such that

- (i) a_i is in the δ -field generated by a_{i-1} over k , for $i = 1, \dots, \ell - 1$, $a_\ell \in k$, and
- (ii) the type of a_i over the algebraic closure of the δ -field generated by $k(a_{i+1})$ is internal to K^δ .

If (V, s) is compound isotrivial one simply takes $a_i = f_{i-1}(a_{i-1})$ for $i = 1, \dots, \ell$. Condition (i) is clear – in fact with “ δ -field generated by” replaced by “field generated by” – and condition (ii) follows from the fact that a_i will be a $k(a_{i+1})^{\text{alg}}$ -generic D -point of one of the irreducible components of $f_i^{-1}(a_{i+1})^{\text{Zar}}$, all of which are isotrivial. For the converse, given $a = a_0, a_1, \dots, a_\ell$ satisfying condition (i) and (ii), one first replaces a_i with $(a_i, \delta(a_i), \dots, \delta^n(a_i))$ for some sufficiently large n so that a_i is a k -generic D -point of an irreducible D -variety (V_i, s_i) over k . This sequence of D -varieties will witness the compound isotriviality, using the fact that the irreducible components of $f_i^{-1}(a_{i+1})^{\text{Zar}}$ are all conjugate over $k(a_{i+1})$ and hence the isotriviality of one implies the isotriviality of them all. \square

Remark 2.11 (Stability under base change). The definition of compound isotriviality seems to be sensitive to parameters; the D -varieties V_i and the D -rational maps f_i need also be defined over k . In fact the notion is stable under base change: if an irreducible D -variety (V, s) over k is compound isotrivial when viewed as a D -variety over some δ -field extension $F \supseteq k$ then it was already compound isotrivial

over k . A model-theoretic re-statement of this is the well-known fact that a stationary type with a nonforking extension that is analysable in the constants is already analysable in the constants. We leave it to the reader to formulate a geometric argument.

Proposition 2.12. *For an irreducible compound isotrivial D -variety over k , δ -rationality implies δ -local-closedness.*

Proof. Suppose (V, s) is an irreducible compound isotrivial D -variety over k with $k(V)^\delta \subseteq k^{\text{alg}}$. We need to show that V has a maximum proper D -subvariety over k . We proceed by induction on the number of steps witnessing the compound isotriviality. The $\ell = 0$ case is vacuous. Suppose we have a compound isotrivial (V, s) witnessed by

$$V = V_0 \xrightarrow{f_0} V_1 \xrightarrow{f_1} \cdots \longrightarrow V_{\ell-1} \xrightarrow{f_{\ell-1}} V_\ell = 0$$

with $\ell \geq 1$. Then V_1 is compound isotrivial in $\ell - 1$ steps, and as $k(V_1)$ is a δ -subfield of $k(V)$ by dominance of f_0 , the induction hypothesis applies to give us a maximum proper D -subvariety of V_1 over k .

On the other hand, the generic fibre $V_\eta := f_0^{-1}(\eta)^{\text{Zar}}$ is an isotrivial $k(\eta)$ -irreducible D -subvariety of V ; where η is a k -generic D -point of V_1 . Moreover, as $k(\eta)(V_\eta) = k(V)$, Fact 2.8 therefore applies to V_η and we obtain a maximum proper D -subvariety over $k(\eta)$. Now Lemma 2.6 implies that V has a maximum proper D -subvariety over k . \square

Corollary 2.13. *Suppose $k \subseteq K^\delta$ and (V, s) is a D -variety over k with the property that every irreducible D -subvariety of V over k^{alg} is compound isotrivial. Then (V, s) satisfies δ -DME.*

Proof. By Proposition 2.3, it suffices to show that every δ -rational k -irreducible D -subvariety (W, s) is δ -locally closed. Note that if $k = k^{\text{alg}}$ then (W, s) is absolutely irreducible, and compound isotrivial by assumption, so that δ -local-closedness follows by Proposition 2.12. In general, let (W_0, s) be an absolutely irreducible component of (W, s) . It is over k^{alg} . The δ -rationality of (W, s) over k implies the δ -rationality of (W_0, s) over k^{alg} – see for example the last paragraph of the proof of Fact 2.8. By assumption (W_0, s) is compound isotrivial, and so by Proposition 2.12 it is δ -locally closed over k^{alg} . We have shown that every irreducible component of (W, s) is δ -locally closed over k^{alg} , and it is not hard to see, by taking the union of the maximum proper D -subvarieties of these components, for example, that this implies that (W, s) is δ -locally closed, as desired. \square

2.6. D -groups over the constants. A D -group is a D -variety (G, s) over k whose underlying variety G is an algebraic group, and such that the section $s : G \rightarrow \tau G$ is a morphism of algebraic groups. (Note that the prolongation of an algebraic group is naturally an algebraic group.) The notions of D -subgroup and homomorphism of D -groups are the natural ones, with the caveat that, unless stated otherwise, parameters may come from a larger δ -field. The quotient of a D -group by a normal D -subgroup admits a natural D -group structure. The terms k -connected and k -connected component of identity when applied to D -groups refer just to the underlying algebraic group, though note that the k -connected component of identity of a D -group over k is a D -subgroup.

In the context of D -groups isotriviality is better behaved. A connected D -group (G, s) is isotrivial if and only if it is isomorphic as a D -group to one of the form $(H, 0)$ where H is an algebraic group over the constants and 0 is the zero section. So one remains in the category of D -groups, and D -birational equivalence is replaced by D -isomorphism. See the discussion around Fact 2.6 of [13] for a proof of this. In particular, every D -subvariety of an isotrivial D -group is itself isotrivial. Quotients of isotrivial D -groups are also isotrivial. Moreover, by [18, Corollary 3.10], if a D -group (G, s) has a finite normal D -subgroup H such that G/H is isotrivial, then (G, s) must have been isotrivial to start with.

The following fact is mostly a matter of putting together various results in the literature on D -groups. As we will see, it will imply that every D -subvariety of a D -group over the constants is compound isotrivial in at most 3 steps.

Fact 2.14. *Suppose (G, s) is a connected D -group over the constants.*

- (a) *The centre $Z(G)$ is a normal D -subgroup of G over the constants, and the quotient $G/Z(G)$ is an isotrivial D -group.*
- (b) *Let H be the algebraic subgroup of points in $Z(G)$ where s agrees with the zero section. Then $Z(G)/H$ is an isotrivial D -group.*

Proof. For a proof that $Z(G)$ is a D -subgroup see [13, 2.7(iii)]. That $G/Z(G)$ is isotrivial was originally proved by Buium [6], though another proof is [13, 2.10].

For part (b), note first of all that H is D -subgroup of $Z(G)$ by definition; the zero section does map to the tangent bundle of H . Now, it suffices to show that Z°/H° is isotrivial where Z° is the connected component of identity of $Z(G)$ and $H^\circ := Z^\circ \cap H$. Let $\mathcal{Z} := (Z^\circ, s)^\sharp(K)$, the subgroup of D -points of Z . Then $(H^\circ, s)^\sharp(K) = \mathcal{Z}(K^\delta)$, the δ -constant points of \mathcal{Z} . These are now commutative δ -algebraic groups. As the \sharp functor is an equivalence of categories, isotriviality of Z°/H° will follow once we show that $\mathcal{Z}/\mathcal{Z}(K^\delta)$ is definably isomorphic (over some parameters) to $(K^\delta)^n$ for some n , see [13, Fact 2.6]. Because Z° is a connected commutative algebraic group over the constants, there exists a δ -algebraic group homomorphism $\ell d : Z^\circ \rightarrow L(Z^\circ)$ over k_0 , where $L(Z^\circ)$ is the Lie algebra of Z° , the tangent space at the identity. This homomorphism is called the *logarithmic derivative*; see [14, §3] for the definition, and for a proof of the fact that ℓd is surjective with kernel $Z^\circ(K^\delta)$. So $\mathcal{Z}/\mathcal{Z}(K^\delta)$ is definably isomorphic to a δ -algebraic subgroup, \mathcal{F} , of $L(Z^\circ)$. Since $L(Z^\circ)$ is a vector group, \mathcal{F} is a finite-dimensional K^δ -vector subspace (see, for example, [17, Fact 1.3]), and hence definably isomorphic over a basis to some $(K^\delta)^n$. \square

Suppose (G, s) is a D -group over a δ -field k and (H, s) is a D -subgroup over k . Even when H is not normal, it makes sense to consider the quotient space G/H as an algebraic variety, and s will induce on G/H the natural structure of a D -variety $(G/H, \bar{s})$ over k , in such a way that the quotient map $\pi : G \rightarrow G/H$ is a D -morphism. See [13, Fact 2.7(ii)], for details. Now if α is a D -point of $(G/H, \bar{s})$, then the fibre $\pi^{-1}(\alpha)$ is a D -subvariety over $k(\alpha)$; and for β a D -point of this fibre we have $\pi^{-1}(\alpha) = \beta + H$. So each fibre $(\pi^{-1}(\alpha), s)$ is isomorphic to (H, s) over $k(\beta)$. One could develop in this context the notion of “ D -homogeneous spaces”.

Using Fact 2.14 we obtain the following highly restrictive property on the structure of D -subvarieties of D -groups over the constants.

Proposition 2.15. *Suppose (G, s) is a connected D -group over $k_0 \subseteq K^\delta$. If k is any δ -field extension of k_0 and W is any irreducible D -subvariety of G over k , then W is compound isotrivial in at most 3 steps.*

In particular, if W is δ -rational then it is δ -locally closed.

Proof. Consider the normal sequence of D -subgroups

$$G \triangleright Z(G) \triangleright H \triangleright 0$$

where $Z(G)$ is the centre of G and H is the algebraic subgroup of points in $Z(G)$ where s agrees with the zero section. Consider the corresponding sequence of irreducible D -varieties and D -morphisms over k_0

$$G \xrightarrow{\pi_0} G/H \xrightarrow{\pi_1} G/Z(G) \xrightarrow{\pi_2} 0.$$

Now, if $W \subseteq G$ is an irreducible D -variety over k , then we get a sequence of dominant D -morphisms

$$W \xrightarrow{f_0} W_1 \xrightarrow{f_1} W_2 \xrightarrow{f_2} 0$$

where $W_1 \subseteq G/H$ is the Zariski closure of $\pi_0(W)$, and $W_2 \subseteq G/Z(G)$ is the Zariski closure of $\pi_1(W_1)$, and the f_i are the appropriate restrictions of the π_i .

Note that W_2 is isotrivial since it is a D -subvariety of the isotrivial D -group $G/Z(G)$ by Fact 2.14(a).

If α is a D -point of W_2 then $f_1^{-1}(\alpha)$ is a D -subvariety of $\pi_1^{-1}(\alpha)$ which is isomorphic as a D -variety to $Z(G)/H$. The latter is an isotrivial D -group by Fact 2.14(b). So the fibres of f_1 over D -points are all isotrivial D -subvarieties of W_1 .

If β is a D -point of W_1 then $f_0^{-1}(\beta)$ is a D -subvariety of $\pi_0^{-1}(\beta)$ which is isomorphic as a D -variety to H . The latter is an isotrivial D -group by definition as s is the zero section on H . So the fibres of f_0 over D -points are all isotrivial.

Hence W is compound isotrivial in 3 steps.

The ‘‘in particular’’ clause is by Proposition 2.12. \square

We have now proved Theorem A of the introduction:

Corollary 2.16. *If $k \subseteq K^\delta$ then every D -group over k satisfies δ -DME.*

Proof. Suppose (G, s) is a D -group over k and W is an irreducible D -subvariety of G over k^{alg} . Then, over k^{alg} , it is isomorphic to an irreducible D -subvariety of the connected component of identity, G_0 . Applying Proposition 2.15 to G_0 , we have that W is compound isotrivial. So every irreducible D -subvariety of G over k^{alg} is compound isotrivial. The δ -DME now follows from Corollary 2.13. \square

2.7. Differential Hopf algebras. In this section we give equivalent algebraic formulations of the δ -DME and our results so far. This will help us make the connection to the classical DME, which is about noncommutative associative algebras and as such does not have a direct geometric formulation.

We restrict our attention to the case when δ is trivial on the base field k .

As explained in §2.1, the standard geometry-algebra duality which assigns to a variety its co-ordinate ring, induces an equivalence between the category of k -irreducible affine D -varieties (V, s) and that of differential rings (R, δ) where R is an affine k -algebra and δ is a k -linear derivation. This equivalence associates to a k -irreducible D -subvariety of V a prime δ -ideal of R . Using this dictionary, we can

easily translate the geometric Definition 2.1, in the case when $k \subseteq K^\delta$, into the following algebraic counterpart.

Definition 2.17 (δ -DME for affine differential algebras). Suppose R is an affine k -algebra equipped with a k -linear derivation δ . We say that (R, δ) satisfies the δ -DME if for every prime δ -ideal P of R , the following conditions are equivalent:

- (i) P is δ -primitive: There exists a maximal ideal \mathfrak{m} of R such that P is maximal among the prime δ -ideals contained in \mathfrak{m} .
- (ii) P is δ -locally-closed: The intersection of all the prime δ -ideals of R that properly contain P is a proper extension of P .
- (iii) P is δ -rational: $\text{Frac}(R/P)^\delta$ is contained in k^{alg} .

The algebraic counterpart of an affine algebraic group G over k is the commutative Hopf k -algebra $R = k[G]$, where the group law $G \times G \rightarrow G$ induces a co-product $\Delta : R \rightarrow R \otimes_k R$. So what is the algebraic counterpart of a D -group (G, s) over k ? The following lemma says that it is a *differential Hopf k -algebra*, a commutative Hopf k -algebra R equipped with a k -linear derivation δ that commutes with the coproduct, where δ acts on $R \otimes_k R$ by $\delta(r_1 \otimes r_2) = \delta r_1 \otimes r_2 + r_1 \otimes \delta r_2$.

Lemma 2.18. *Suppose $k \subseteq K^\delta$ and let (G, s) be a D -variety defined over k such that G is a k -connected affine algebraic group. Let δ on $R = k[G]$ be the corresponding k -linear derivation. Then $s : G \rightarrow TG$ is a group homomorphism if and only if δ commutes with the coproduct.*

Proof. Unravelling the fact that s induces the derivation δ on $k[G]$ and that the group operation $m : G \times G \rightarrow G$ induces the coproduct Δ on $k[G]$, we have that for all $f \in k[G]$,

$$(2.1) \quad \Delta(\delta f) = \delta \Delta(f) \iff df(s(m(y, z))) = d(f \circ m)(s(y), s(z))$$

where (y, z) are coordinates for $G \times G$. But

$$d(f \circ m)(s(y), s(z)) = df \circ dm(s(y), s(z)) = df(s(y) * s(z)),$$

where $*$ denotes the group operation $dm : TG \times TG \rightarrow TG$. And so the right hand side of (2.1) is equivalent to

$$df(s(m(y, z))) = df(s(y) * s(z)).$$

But this, asserted for all $f \in k[G]$, is equivalent to $s(m(y, z)) = s(y) * s(z)$, i.e., that s is a group homomorphism. \square

In other words, the study of k -connected affine D -groups over the constants is the same thing as the study of affine differential Hopf k -algebras. So our Theorem A becomes:

Theorem 2.19. *Every commutative affine differential Hopf algebra over a field of characteristic zero satisfies δ -DME.*

Proof. By Lemma 2.18 our differential Hopf algebra is of the form $k[G]$ for some k -connected affine D -group (G, s) with $k \subseteq K^\delta$. By Corollary 2.16 (G, s) satisfies the δ -DME. So $(k[G], \delta)$ satisfies δ -DME. \square

3. TWISTING BY A GROUP-LIKE ELEMENT

As it turns out, the application to the classical Dixmier-Moeglin problem that we have in mind, and that will be treated in §4, requires a generalisation of Theorem 2.19. Instead of working with differential Hopf algebras, we need to consider Hopf algebras equipped with derivations that do not quite commute with the coproduct. Suppose R is a commutative affine Hopf k -algebra. We will use Sweedler notation¹ and write $\Delta(r) = \sum r_1 \otimes r_2$ for any $r \in R$. Now, for a k -linear derivation δ to commute with Δ on R means that for all $r \in R$,

$$\Delta(\delta r) = \sum \delta r_1 \otimes r_2 + r_1 \otimes \delta r_2.$$

We wish to weaken this condition by asking instead simply that there exists some $a \in R$ satisfying $\Delta(a) = a \otimes a$ – that is, a is a *group-like* element of R – such that for all $r \in R$,

$$(3.1) \quad \Delta(\delta r) = \sum \delta r_1 \otimes r_2 + ar_1 \otimes \delta r_2.$$

That is, we ask δ to be what Panov [16] calls an *a-coderivation*. We wish to prove:

Theorem 3.1. *Suppose k is an algebraically closed field of characteristic zero, R is a commutative affine Hopf k -algebra, and δ is a k -linear derivation on R that is an a -coderivation for some group-like $a \in R$. Then (R, δ) satisfies the δ -DME.*

When $a = 1$ this is just the case of affine differential Hopf k -algebras, and hence is dealt with by Theorem 2.19. The general case requires some work.

Throughout this section k is a fixed algebraically closed field of characteristic zero. The assumption that k is algebraically closed is probably not necessary.

Let us begin with a geometric explanation of what this twisting by a group-like element means. First of all, we have $R = k[G]$ for some connected affine algebraic group G over k , with the coproduct Δ on R induced by the group operation on G , and the derivation δ on R induced by a D -variety structure $s : G \rightarrow TG$. Now, as G is an affine algebraic group, we may assume it is an algebraic subgroup of GL_n , so that $TG \subseteq G \times \mathrm{Mat}_n$. Writing $s = (\mathrm{id}, \bar{s})$ where $\bar{s} : G \rightarrow \mathrm{Mat}_n$, we want to express as a property of \bar{s} what it means for δ to be an a -coderivation. That $a \in R$ is group-like means that $a : G \rightarrow \mathbb{G}_m$ is a homomorphism of algebraic groups.

Lemma 3.2. *Suppose $G \subseteq \mathrm{GL}_n$ is a connected affine algebraic group over k , $a : G \rightarrow \mathbb{G}_m$ is a homomorphism, and $s = (\mathrm{id}, \bar{s}) : G \rightarrow TG \subseteq G \times \mathrm{Mat}_n$ is a D -variety structure on G over k . Then the corresponding k -linear derivation δ on $k[G]$ is an a -coderivation if and only if*

$$(3.2) \quad \bar{s}(gh) = \bar{s}(g)h + a(g)g\bar{s}(h)$$

for all $g, h \in G$, where all addition and multiplication is in the sense of matrices.

Proof. Note that for $r \in k[G]$, $\Delta(\delta r) \in k[G \times G]$ is given by

$$\Delta(\delta r)(g, h) = d_{gh}r(\bar{s}(gh))$$

¹Recall that in Sweedler notation $\sum r_1 \otimes r_2$ is used to denote an expression of the form $\sum_{j=1}^d r_{j,1} \otimes r_{j,2}$. We will use Sweedler notation throughout, hopefully without confusion.

for all $g, h \in G$, where $dr : TG \rightarrow \mathbb{A}^2$ is the differential of $r : G \rightarrow \mathbb{A}^1$. On the other hand, writing $\Delta(r) = \sum r_1 \otimes r_2$ we have

$$\begin{aligned} \sum (\delta r_1 \otimes r_2 + ar_1 \otimes \delta r_2)(g, h) &= \sum d_g r_1(\bar{s}(g)) r_2(h) + a(g) r_1(g) d_h r_2(\bar{s}(h)) \\ &= d_{(g,h)} \left(\sum r_1 \otimes r_2 \right) (\bar{s}(g), a(g)\bar{s}(h)) \\ &= d_{(g,h)}(\Delta r)(\bar{s}(g), a(g)\bar{s}(h)) \end{aligned}$$

where the second equality uses the fact that $a(g)$ is a scalar. Now, as an element of $k[G \times G]$, $\Delta(r) = r \circ m$ where $m : G \times G \rightarrow G$ is the restriction of matrix multiplication on GL_n . Note that when we differentiate matrix multiplication we get $d_{(g,h)}m(A, B) = Ah + gB$, for all $g, h \in \mathrm{GL}_n$ and $A, B \in \mathrm{Mat}_n$. Hence,

$$\begin{aligned} \sum (\delta r_1 \otimes r_2 + ar_1 \otimes \delta r_2)(g, h) &= d_{(g,h)}(\Delta r)(\bar{s}(g), a(g)\bar{s}(h)) \\ &= d_{gh}r \circ d_{(g,h)}m(\bar{s}(g), a(g)\bar{s}(h)) \\ &= d_{gh}r(\bar{s}(g)h + ga(g)\bar{s}(h)) \\ &= d_{gh}r(\bar{s}(g)h + a(g)g\bar{s}(h)). \end{aligned}$$

Hence, δ being an a -coderivation, that is equation (3.1), is equivalent to

$$d_{gh}r(\bar{s}(gh)) = d_{gh}r(\bar{s}(g)h + a(g)g\bar{s}(h))$$

for all $r \in k[G]$. But this implies

$$\bar{s}(gh) = \bar{s}(g)h + a(g)g\bar{s}(h)$$

as desired. \square

Definition 3.3. When G is an affine algebraic group and (G, s) is a D -variety structure such that (3.2) holds, we will say that (G, s) is an a -twisted D -group.

Example 3.4. The following example of a twisted D -group (E, t) will play an important role. Let $R = k[x, \frac{1}{x}, y]$ with δ the k -linear derivation induced by $\delta(x) = xy$ and $\delta(y) = \frac{y^2}{2}$. Note that R is the co-ordinate ring of the algebraic subgroup $E \leq \mathrm{GL}_2$ made up of matrices of the form

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix},$$

and hence is a commutative affine Hopf k -algebra. Denoting by $t = (\mathrm{id}, \bar{t})$ the D -variety structure on E induced by δ , we have

$$\bar{t} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ab & \frac{b^2}{2} \\ 0 & 0 \end{pmatrix}.$$

Now a straightforward computation shows that

$$\begin{aligned} \bar{t} \left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \right) &= \begin{pmatrix} a^2 a' b' + aa' b & \frac{a^2 (b')^2}{2} + abb' + \frac{b^2}{2} \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} aa' b & abb' + \frac{b^2}{2} \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a^2 a' b' & \frac{a^2 (b')^2}{2} \\ 0 & 0 \end{pmatrix} \\ &= \bar{t} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} + a \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \bar{t} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

That is, (E, t) is an x -twisted D -group. (Note that $x \in R$ is group-like.) Since (E, t) is not a D -group, we cannot use Theorem 2.19 to deduce the δ -DME for (R, δ) . However, as Ruizhang Jin pointed out to us, (E, t) , and indeed every D -subvariety of it, is isotrivial. To see this, note first of all that the subvariety of E defined by $y = 0$ is a D -subvariety on which t is the zero section, and hence that D -subvariety is isotrivial. If $W \subseteq E$ is any other D -subvariety, then it has a generic D -point $(a, b) \in (E, t)^\sharp(K)$ with $b \neq 0$, and one can compute that $\delta^3(\frac{1}{a}) = \delta^2(\frac{1}{b}) = 0$, so that the type of (a, b) is internal to the constants, and hence (W, t) is isotrivial. Since every D -subvariety of (E, t) is isotrivial, Corollary 2.13 implies that (E, t) , and hence (R, δ) , satisfies δ -DME after all. Actually, we can also deduce δ -DME from [1] since the Krull dimension of R is 2. But the isotriviality of all the D -subvarieties of (E, t) says more and will be of use.

Our strategy for proving Theorem 3.1 is to show that every a -twisted D -group over the constants admits the example described above as an image with each fibre D -isomorphic (over possibly nonconstant parameters) to a D -group over the constants. It will follow (using Proposition 2.15) that every D -subvariety of an a -twisted D -group over the constants is compound isotrivial (in at most 4 steps), and so Corollary 2.13 will yield the δ -DME.

We will require the following proposition, whose proof is rather technical, and for which it would be nice to give a conceptual explanation.

Proposition 3.5. *Suppose R is a commutative affine Hopf k -algebra, and δ is a k -linear derivation on R that is an a -coderivation for some group-like $a \in R$. Then $a\delta^2 a = \frac{3}{2}(\delta a)^2$.*

We delay the proof of this proposition until we have established the preliminary Lemmas 3.6 and 3.7 below, for which we fix a commutative affine Hopf k -algebra, R , equipped with a k -linear derivation, δ , such that δ is also an a -coderivation for some group-like $a \in R$. As a is group-like it is invertible in R . We fix the following sequence of elements in R :

$$\begin{aligned} u_0 &:= a \\ u_1 &:= \frac{\delta a}{a} \\ u_2 &:= \delta u_1 - \frac{u_1^2}{2} \\ u_m &:= \delta(u_{m-1}) \quad \text{for } m \geq 3. \end{aligned}$$

Note that the desired identity $a\delta^2 a = \frac{3}{2}(\delta a)^2$ is equivalent to $u_2 = 0$; this is our eventual aim.

Lemma 3.6. *For all $m \geq 1$, we have*

$$\Delta(u_m) = u_m \otimes 1 + a^m \otimes u_m + \sum_{j=2}^{m-1} c_{j,m} a^j u_{m-j} \otimes u_j + \sum f_i \otimes g_i$$

where the $c_{j,m}$ are positive integers, the $f_i \in (u_1, \dots, u_{m-1})^2 k[u_0, \dots, u_{m-1}]$, and the $g_i \in k[u_0, \dots, u_{m-1}]$.

Proof. We can compute the coproducts of the elements u_0, u_1, \dots using the fact that $a = u_0$ is group-like and δ is an a -coderivation:

$$\begin{aligned}\Delta(u_0) &= a \otimes a \\ \Delta(u_1) &= \left(\frac{1}{a} \otimes \frac{1}{a}\right)(\delta a \otimes a + a^2 \otimes \delta a) \\ &= u_1 \otimes 1 + a \otimes u_1 \\ \Delta(u_2) &= \delta u_1 \otimes 1 + \delta a \otimes u_1 + a^2 \otimes \delta u_1 - \frac{u_1^2}{2} \otimes 1 - a u_1 \otimes u_1 - a^2 \otimes \frac{u_1^2}{2} \\ &= u_2 \otimes 1 + a^2 \otimes u_2\end{aligned}$$

Then for $m = 1, 2$, the conclusion of the statement of the lemma follows from the above computations with $f_i = g_i = 0$ and the middle sum being empty. Now one computes $\Delta(u_{m+1}) = \Delta(\delta u_m)$ for $m \geq 2$, using the inductively given expression for $\Delta(u_m)$ and the fact that δ is an a -coderivation. The rest is a straightforward brute force computation that we leave to the reader. \square

Lemma 3.7. *There exist $n \geq 1$, a polynomial $P \in k[u_0, \dots, u_{n-1}]$ and some $r \geq 0$ such that*

$$u_n = \frac{P(u_0, \dots, u_{n-1})}{u_0^r}.$$

Proof. Since R is finitely generated as a k -algebra, this sequence (u_m) cannot be algebraically independent over k . Choose n minimal such that (u_0, \dots, u_n) is algebraically dependent over k . Note that if $n = 0$ then $a = u_0$ is a constant and so $u_1 = u_2 = 0$ by definition. So we will assume that $n > 0$.

So there is some $d \geq 1$ such that

$$(3.3) \quad u_n^d + \sum_{i < d} A_i(u_0, \dots, u_{n-1}) u_n^i = 0,$$

with A_0, \dots, A_{d-1} rational functions over k . We may assume that d is minimal. Our first step is to show that $d = 1$.

Since k is algebraically closed, $R \otimes_k R$ is a domain and we can work inside its fraction field. Let F be the subfield which is the fraction field of $k[u_0, \dots, u_{n-1}] \otimes_k k[u_0, \dots, u_{n-1}]$. Note that by the minimality of d , $\{1, u_n, \dots, u_n^{d-1}\}$ is linearly independent over $k(u_0, \dots, u_{n-1})$, from which it follows that $\{u_n^i \otimes u_n^j : 0 \leq i, j < d\}$ is linearly independent over F . Applying Δ to both sides of Equation (3.3), Lemma 3.6 gives us that

$$(u_n \otimes 1 + a^n \otimes u_n)^d \in \sum_{i < d} F \cdot (u_n \otimes 1 + a^n \otimes u_n)^i \subseteq \sum_{i+j < d} F u_n^i \otimes u_n^j.$$

On the other hand, $u_n^d \otimes 1$ and $a^{nd} \otimes u_n^d$ are also in $\sum_{i+j < d} F u_n^i \otimes u_n^j$ by (3.3). It follows that

$$\sum_{i=1}^{d-1} \binom{d}{i} a^{n(d-i)} u_n^i \otimes u_n^{d-i} \in \sum_{i+j < d} F u_n^i \otimes u_n^j.$$

If $d > 1$ then $u_n^{d-1} \otimes u_n$ appears with a nonzero coefficient on the left-hand side but with zero coefficient on the right-hand side. This contradicts the F -linear independence of $(u_n^i \otimes u_n^j : 0 \leq i, j < d)$.

So $d = 1$, and we have that

$$(3.4) \quad u_n = \frac{P(u_0, \dots, u_{n-1})}{Q(u_0, \dots, u_{n-1})},$$

for some relatively prime polynomials P and Q over k . We aim to show that Q is a monomial in u_0 .

First we argue that $Q \otimes Q$ divides $\Delta(Q)$ in $S := k[u_0, \dots, u_{n-1}] \otimes_k k[u_0, \dots, u_{n-1}]$, which note is the polynomial ring over k in the variables $u_i \otimes 1, 1 \otimes u_j$, and hence is a UFD. Indeed,

$$\begin{aligned} \Delta(P) &= \Delta(Q)\Delta(u_n) && \text{by applying } \Delta \text{ to both sides of Equation (3.4)} \\ &= \Delta(Q)(u_n \otimes 1 + a^n \otimes u_n + y) && \text{by Lemma 3.6, for some } y \in S \\ &= \Delta(Q)((P/Q) \otimes 1 + a^n \otimes (P/Q) + y) \end{aligned}$$

We can then multiply both sides by $1 \otimes Q$ to see that $\Delta(Q)(P/Q) \otimes Q \in S$. Hence $Q \otimes 1$ divides $\Delta(Q)P \otimes Q = \Delta(Q)(P \otimes 1)(1 \otimes Q)$. Since P and Q are relatively prime, $Q \otimes 1$ divides $\Delta(Q)$. A similar argument shows that $1 \otimes Q$ divides $\Delta(Q)$. Since we are working in a UFD and $1 \otimes Q$ and $Q \otimes 1$ are relatively prime, we see that $Q \otimes Q$ divides $\Delta(Q)$, as desired.

Let $i \leq n-1$ be the largest index for which u_i appears in Q . Then we can write $Q = \sum_{j=0}^M u_i^j Q_j(u_0, u_1, \dots, u_{i-1})$ with $M > 0$ and Q_M nonzero. So

$$Q \otimes Q = (u_i^M \otimes u_i^M)Q_M \otimes Q_M + \sum_{j,k < M} (u_i^j \otimes u_i^k)Q_j \otimes Q_k$$

while, if $i \geq 1$, then

$$\Delta(Q) = \sum_{j=0}^M \Delta(u_i)^j Q_j(\Delta(u_0), \dots, \Delta(u_{i-1})) = \sum_{\ell+m \leq M} f_{\ell,m} u_i^\ell \otimes u_i^m.$$

where $f_{\ell,m} \in k[u_0, \dots, u_{i-1}] \otimes_k k[u_0, \dots, u_{i-1}]$, by Lemma 3.6. (Note that Lemma 3.6 fails for u_0 , so we are using that $i \geq 1$ in the above calculation.) But this contradicts $Q \otimes Q$ dividing $\Delta(Q)$, since $u_i^M \otimes u_i^M$ appears in the former while in the latter no $u_i^\ell \otimes u_i^m$ appears with $\ell, m \geq M$. So it must be that $i = 0$ and we have shown that Q is a polynomial in u_0 .

Multiplying by a nonzero scalar if necessary, we may assume that Q is in fact a polynomial in u_0 with leading coefficient 1. Let M denote the degree of Q . Then $Q(u_0) \otimes Q(u_0)$ divides $\Delta(Q) = Q(u_0 \otimes u_0)$ in S , recalling that $u_0 = a$ is group-like. Since both $Q(u_0) \otimes Q(u_0)$ and $Q(u_0 \otimes u_0)$ are polynomials of total degree $2M$ in the variables $u_0 \otimes 1$ and $1 \otimes u_0$ and since they both have leading coefficient 1, we see that they must be the same. In particular, $Q(u_0) \otimes Q(u_0)$ is a polynomial in $u_0 \otimes u_0$ with leading coefficient 1, which implies that $Q(u_0)$ is of the form u_0^r . \square

Proof of Proposition 3.5. Let (R, δ) , a , and the u_i be as above. We need to show that $u_2 = 0$. By Lemma 3.7 we have that there is some $n \geq 1$, some $r \geq 0$ and some polynomial $P \in k[u_0, \dots, u_{n-1}]$ such that

$$(3.5) \quad u_n = \frac{P(u_0, \dots, u_{n-1})}{u_0^r},$$

for some polynomial P over k . Our first step is to show that $n \leq 2$.

Let $S := k[u_0, \dots, u_{n-1}] \otimes_k k[u_0, \dots, u_{n-1}]$. Let $I := (u_1, \dots, u_{n-1})^2 k[u_0, \dots, u_{n-1}]$ and consider the ideal of S given by

$$J := I \otimes k[u_0, \dots, u_{n-1}] + k[u_0, \dots, u_{n-1}] \otimes I.$$

So these are the elements of S in which each monomial has degree at least 2 in either the variables $u_1 \otimes 1, \dots, u_{n-1} \otimes 1$, or in the variables $1 \otimes u_1, \dots, 1 \otimes u_{n-1}$. Using Lemma 3.6 we can compute that for $1 \leq i, j, \ell \leq n-1$

$$(3.6) \quad \Delta(u_i u_j u_\ell) \in J.$$

Moreover, for $1 \leq i, j \leq n-1$, Lemma 3.6 gives

$$(3.7) \quad \Delta(u_i u_j) = u_0^j u_i \otimes u_j + u_0^i u_j \otimes u_i \pmod{J}.$$

Now, write the polynomial P of Equation (3.5) as

$$P = P_0(u_0) + \sum_{i=1}^{n-1} P_i(u_0) u_i + \sum_{1 \leq i \leq j \leq n-1} P_{i,j}(u_0) u_i u_j + H,$$

where H is of degree at least three in u_1, \dots, u_{n-1} . Applying Δ to both sides of Equation (3.5) gives that

$$(u_0 \otimes u_0)^r \Delta(u_n) = \Delta(P).$$

Considering both sides as elements in the polynomial ring

$$k(u_0 \otimes 1, 1 \otimes u_0)[u_1 \otimes 1, \dots, u_{n-1} \otimes 1, 1 \otimes u_1, \dots, 1 \otimes u_{n-1}]$$

and extracting the coefficient of $u_i \otimes 1$ for $i \in \{1, \dots, n-1\}$, we see that $P_i(u_0 \otimes u_0) = 0$ and so $P_i = 0$ for $i = 1, \dots, n-1$; similarly, extracting the constant coefficient gives that $P_0 = 0$. Then using again the fact that

$$(u_0 \otimes u_0)^r \Delta(u_n) = \Delta(P)$$

and using (3.6) and (3.7), it follows that

$$(u_0 \otimes u_0)^r \Delta(u_n) = \sum_{1 \leq i \leq j \leq n-1} P_{i,j}(u_0 \otimes u_0) (u_0^j u_i \otimes u_j + u_0^i u_j \otimes u_i) \pmod{J}.$$

Assume towards a contradiction that $n \geq 3$. Then by Lemma 3.6 we must have $u_1 \otimes u_{n-1}$ appearing in $\Delta(u_n)$ on the left with a nonzero coefficient. So $P_{1,n-1} \neq 0$. But then $P_{1,n-1}(u_0 \otimes u_0)(u_0 u_{n-1} \otimes u_1)$ appears on the right, while it does not appear on the left since $u_{n-1} \otimes u_1$ does not appear in $\Delta(u_n)$ by Lemma 3.6.

This contradiction proves that $n \leq 2$. Suppose $n = 1$. Then Equation (3.5) says $u_1 = \frac{P(u_0)}{u_0^r}$. Applying Δ to both sides yields

$$P(u_0) \otimes u_0^r + u_0^{r+1} \otimes P(u_0) = P(u_0 \otimes u_0)$$

which is only possible if $P_0 = 0$. Hence $u_1 = u_2 = 0$, as desired.

So we are left to consider the case when $n = 2$. Equation (3.5) becomes

$$u_2 = \frac{1}{u_0^r} \sum_{j=0}^M P_j(u_0) u_1^j$$

with $M \geq 1$, the P_j are polynomials over k , and P_M is nonzero. Applying Δ gives

$$(a^r \otimes a^r) (u_2 \otimes 1 + a^2 \otimes u_2) = \sum_{j=0}^M P_j(a \otimes a) (u_1 \otimes 1 + a \otimes u_1)^j$$

which we can write as

$$(a^r \otimes a^r) \left(\sum_{j=0}^M P_j(a) u_1^j \otimes 1 + \sum_{j=0}^M a^2 \otimes P_j(a) u_1^j \right) = \sum_{j=0}^M P_j(a \otimes a) (u_1 \otimes 1 + a \otimes u_1)^j.$$

Notice that if $M > 1$ then the right-hand side involves terms with $u_1^i \otimes u_1^j$ with $i, j \geq 1$ while the left-hand side does not, and so we cannot have equality. Thus $M = 1$. Writing out the above equation with this in mind we get that

$$(a^r \otimes a^r) (P_0(a) \otimes 1 + P_1(a) u_1 \otimes 1 + a^2 \otimes P_0(a) + a^2 \otimes P_1(a) u_1)$$

is equal to

$$P_0(a \otimes a) + P_1(a \otimes a) (u_1 \otimes 1 + a \otimes u_1).$$

Look at this as an equation in $\mathbb{C}[a \otimes 1, 1 \otimes a][u_1 \otimes 1, 1 \otimes u_1]$. Then taking the coefficient of $u_1 \otimes 1$ gives that

$$a^r P_1(a) \otimes a^r = P_1(a \otimes a),$$

which can only occur if $P_1 \in k$. Write $P_1 = c$. Then extracting the coefficient of $1 \otimes u_1$ gives $a^{r+2} \otimes c = c(a \otimes 1)$, and so $c = 0$. Now taking the constant coefficient (regarding constants as being in $\mathbb{C}[a \otimes 1, 1 \otimes a]$) gives that

$$a^r P_0(a) \otimes a^r + a^{r+2} \otimes P_0(a) = P_0(a \otimes a).$$

This forces $P_0 = 0$. So $u_2 = \frac{1}{u_0} (P_0(u_0) + P_1(u_0) u_1) = 0$, as desired. \square

The following is a geometric interpretation of the proposition.

Proposition 3.8. *Suppose $k \subseteq K^\delta$ is algebraically closed and (G, s) is an affine connected a -twisted D -group over k where $a \in k[G]$ is group-like. Then*

$$g \mapsto \begin{pmatrix} a(g) & \frac{\delta a(g)}{a(g)} \\ 0 & 1 \end{pmatrix}$$

defines a homomorphism $\pi : G \rightarrow E$ of algebraic groups where E is as in Example 3.4. Moreover, $\pi : (G, s) \rightarrow (E, t)$ is a D -morphism.

Proof. Recall that as $a \in k[G]$ is group-like, $a : G \rightarrow \mathbb{G}_m$ is a homomorphism of algebraic groups. It follows immediately that π is well-defined and does indeed map G to E . We check that it is a group homomorphism: given $g, h \in G$, note first of all that as $\Delta(a) = a \otimes a$ and δ is an a -coderivation we have $\Delta(\delta a) = \delta a \otimes a + a^2 \otimes \delta a$ and so

$$(3.8) \quad \delta a(gh) = \Delta(\delta a)(g, h) = \delta a(g) a(h) + a(g)^2 \delta a(h).$$

We can therefore compute

$$\begin{aligned}
\pi(g)\pi(h) &= \begin{pmatrix} a(g) & \frac{\delta a(g)}{a(g)} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a(h) & \frac{\delta a(h)}{a(h)} \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a(gh) & a(g)\frac{\delta a(h)}{a(h)} + \frac{\delta a(g)}{a(g)} \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a(gh) & \frac{a(g)^2\delta a(h) + \delta a(g)a(h)}{a(gh)} \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a(gh) & \frac{\delta a(gh)}{a(gh)} \\ 0 & 1 \end{pmatrix} \quad \text{by (3.8)} \\
&= \pi(gh)
\end{aligned}$$

where we have used repeatedly that $a(gh) = a(g)a(h)$.

It remains to show that π is a D -morphism. For this it suffices to show that π takes D -points to D -points. That is, if $g \in (G, s)^\sharp(K)$ then $\begin{pmatrix} a(g) & \frac{\delta a(g)}{a(g)} \\ 0 & 1 \end{pmatrix}$ should be a D -point of (E, t) . Writing $t = (\text{id}, \bar{t})$ we have that

$$\begin{aligned}
\bar{t} \begin{pmatrix} a(g) & \frac{\delta a(g)}{a(g)} \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} \delta a(g) & \frac{\delta a(g)^2}{2a(g)^2} \\ 0 & 0 \end{pmatrix} \quad \text{by Example 3.4} \\
&= \begin{pmatrix} \delta a(g) & \frac{a(g)\delta^2 a(g) - \delta a(g)^2}{a(g)^2} \\ 0 & 0 \end{pmatrix} \quad \text{by Proposition 3.5} \\
&= \delta \begin{pmatrix} a(g) & \frac{\delta a(g)}{a(g)} \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

where in the final equality we are using the fact that as g is a D -point of G , $\delta(r(g)) = (\delta r)(g)$ for all $r \in k[G]$. This shows that $\pi(g) \in (E, t)^\sharp(K)$, as desired. \square

We can now complete the proof of the theorem.

Proof of Theorem 3.1. We have already established that (R, δ) is the co-ordinate ring of an affine connected a -twisted D -group (G, s) where $a \in k[G]$ is group-like. Here recall that $k \subseteq K^\delta$ is algebraically closed. By Corollary 2.13, the δ -DME for (R, δ) will follow if we can show that every irreducible D -subvariety of G over k is compound isotrivial.

Let $H = \ker(\pi)$ where $\pi : (G, s) \rightarrow (E, t)$ is the D -morphism from Proposition 3.8. Since π is a D -morphism, (H, s) is a D -subvariety of (G, s) . Since π is an algebraic group homomorphism H is an algebraic subgroup of G . It follows that (H, s) is an $a \upharpoonright_H$ -twisted D -group also. On the other hand, $a \upharpoonright_H = 1$ by the definition of π . So (H, s) is an actual D -group. Applying Proposition 2.15 to the connected component of (H, s) we have that every irreducible D -subvariety of H , over any δ -field extension of k , is compound isotrivial.

What about fibres of π over D -points of (E, t) other than the kernel? Any such fibre is a D -subvariety of (G, s) of the form Hg , for some $g \in (G, s)^\sharp(K)$. Since (G, s) is not necessarily a D -group, the multiplication-by- g -on-the-right map, $\rho_g : G \rightarrow G$, is not necessarily a D -automorphism. Nevertheless, when we restrict

this map to H we do get a D -isomorphism between H and Hg . To see this we need only check that ρ_g takes D -points of H to D -points of Hg . Letting $h \in (H, s)^\sharp(K)$ we compute

$$\begin{aligned} \bar{s}(hg) &= \bar{s}(h)g + a(h)h\bar{s}(g) && \text{by (3.2)} \\ &= \bar{s}(h)g + h\bar{s}(g) && \text{as } a \upharpoonright_H = 1 \\ &= \delta(h)g + h\delta(g) && \text{as } h \text{ and } g \text{ are } D\text{-points} \\ &= \delta(hg) && \text{as } \nabla : G \rightarrow TG \text{ is a group homomorphism} \end{aligned}$$

as desired. So H and Hg are D -isomorphic over $k(g)$, so that every irreducible D -subvariety of Hg , over any δ -field, is compound isotrivial.

Now suppose that $W \subseteq G$ is an irreducible D -subvariety (over k but in fact that is not necessary), and we show that it is compound isotrivial. The Zariski closure of $\pi(W)$ is an irreducible D -subvariety of (E, t) , and hence is isotrivial by Example 3.4. Using the characterisation of compound isotriviality in terms of analysability (Lemma 2.10), for example, one sees that it suffices to show that every irreducible component of the generic fibre of $\pi \upharpoonright_W$ is compound isotrivial. Indeed, if this were the case, and if $a \in (W, s)^\sharp(K)$ is a k -generic point, then we have that both $\text{tp}(\pi(a)/k)$ and $\text{tp}(a/k(\pi(a))^{\text{alg}})$ are analysable in K^δ , from which it follows that $\text{tp}(a/k)$ is too. So fix $\eta \in (W, t)^\sharp(K)$ a k -generic D -point and consider the fibre $W_\eta := \pi^{-1}(\eta) \cap W$. Fixing $g \in \pi^{-1}(\eta)$, we know that $\pi^{-1}(\eta) = Hg$ and W_η is a $k(\eta)$ -irreducible D -subvariety of Hg . But all irreducible D -subvarieties of Hg are compound isotrivial by the previous paragraph, and hence every irreducible component of W_η is. Therefore, W is compound isotrivial, as desired. \square

4. THE DME FOR ORE EXTENSIONS OF COMMUTATIVE HOPF ALGEBRAS

We will now apply the results of the previous sections to the classical study of certain (noncommutative) Hopf algebras. Recall that if A is a noetherian associative algebra over a field k of characteristic zero, then we say that the *Dixmier-Moeglin equivalence* (DME) holds for A if for every (two-sided) prime ideal P of A , the following are equivalent:

- (i) P is *primitive*: it is the annihilator of a simple left A -module.
- (ii) P is *locally closed*: the intersection of all the prime ideals of A that properly contain P is a proper extension of P .
- (iii) P is *rational*: the centre of the Goldie quotient ring² $\text{Frac}(A/P)$ is an algebraic field extension of k .

Of course, for commutative algebras the DME always holds as the notions of primitive, locally closed and rational all coincide with maximal.

It is known that in any algebra that satisfies the Nullstellensatz locally closed implies primitive and primitive implies rational, see [4, II.7.16]. Thus, the central question is: when does rational imply locally closed? Certainly this is not always the case; even in finite Gelfand-Kirillov dimension a counterexample was found in [1]. In [3] the DME was conjectured specifically about all Hopf algebras of finite Gelfand-Kirillov dimension.

²The Goldie quotient is an artinian ring of quotients for any prime noetherian ring that imitates the field of fractions construction for integral domains in the commutative case. See [15, Chapter 2] for details.

We will show here that the DME holds for Hopf algebras that arise as certain twisted polynomial rings over commutative Hopf algebras. Recall that if R is a k -algebra equipped with an automorphism σ then a k -linear σ -derivation is a k -linear map δ satisfying the twisted Leibniz rule:

$$\delta(rs) = \sigma(r)\delta(s) + \delta(r)s.$$

Given σ and δ , the *Ore extension* of R , denoted by $R[x; \sigma, \delta]$ is the ring extension of R with the property that it is a free left R -module with basis $\{x^n : n \geq 0\}$ and such that $xr = \sigma(r)x + \delta(r)$ for all $r \in R$. We aim to prove the DME for Hopf algebras that arise as the Ore extensions of commutative Hopf algebras. More precisely,

Theorem 4.1. *Suppose k is a field of characteristic zero and R is a commutative affine Hopf k -algebra equipped with a k -algebra automorphism σ and a k -linear σ -derivation δ . Assume that the Ore extension $A := R[x; \sigma, \delta]$ admits a Hopf algebra structure extending that of R . Then A satisfies the DME.*

This is Theorem B2 of the introduction. Its proof is preceded by a number of preliminaries.

4.1. Hopf Ore extensions. In this section we prove a result (Corollary 4.4, below) that severely restricts what $(R, \Delta, \sigma, \delta)$ can be if $A = R[x; \sigma, \delta]$ is to admit a Hopf algebra structure extending that on R . Actually this was already done by Brown et al. in [5], answering a question of Panov [16], in a more general context where R is not necessarily commutative, but under the additional assumption on A that

$$(4.1) \quad \Delta(x) = a \otimes x + x \otimes b + v(x \otimes x) + w$$

for some $a, b \in R$ and $v, w \in R \otimes_k R$. When (4.1) holds, possibly after a change of the variable x , Brown et al. call $R[x; \sigma, \delta]$ a *Hopf Ore extension*. They ask if every Ore extension admitting a Hopf algebra structure extending that on R is a Hopf Ore extension. We prove that this is the case, in a strong way, when R is commutative and affine (this is Theorem C of the introduction):

Theorem 4.2. *Suppose k is an algebraically closed field of characteristic zero and R is a commutative affine Hopf k -algebra equipped with a k -algebra automorphism σ and a k -linear σ -derivation δ . If $R[x; \sigma, \delta]$ admits a Hopf algebra structure extending that of R then, after a linear change of the variable x ,*

$$\Delta(x) = a \otimes x + x \otimes b + w$$

for some $a, b \in R$, each of which is either 0 or group-like, and some $w \in R \otimes_k R$.

Proof. Our starting point is [5, §2.2, Lemma 1] which says that if $R \otimes_k R$ is a domain (which is true here as R is a commutative domain and k is algebraically closed) then

$$(4.2) \quad \Delta(x) = s(1 \otimes x) + t(x \otimes 1) + v(x \otimes x) + w$$

where $s, t, v, w \in R \otimes_k R$. By making a substitution $x \mapsto x - \lambda$ for some $\lambda \in k$, we may assume that $\epsilon(x) = 0$ where $\epsilon : A \rightarrow k$ is the counit. This substitution does not change the form of $\Delta(x)$ given in (4.2).

Our first goal is to show that $v = 0$. Recall that since R is commutative it is of the form $R = k[G]$ for a connected affine algebraic group G . We can therefore view $v \in R \otimes_k R$ as a regular function on $G \times G$. We show first that $v(g^{-1}, g) = 0$ for all $g \in G$, and then that in fact $v = 0$.

Let $A := R[x; \sigma, \delta]$ and let S denote the antipode of A . Then by [22, Corollary 1], S is bijective on A and its restriction to R is bijective on R . Thus we can write

$$S(x) = a_0 + a_1x + \cdots + a_dx^d$$

for some $d \geq 1$ and $a_0, \dots, a_d \in R$ with $a_d \neq 0$. Writing $m : A \otimes_k A \rightarrow A$ for the homomorphism induced by multiplication, we have the identity

$$m \circ (S \otimes \text{id}) \circ \Delta(x) = \epsilon(x).$$

So, as $\epsilon(x) = 0$, we use (4.2) to write

$$0 = m \circ (S \otimes \text{id})(s)x + m \circ (S \otimes \text{id})(t)S(x) + m \circ (S \otimes \text{id})(v)S(x)x + m \circ (S \otimes \text{id})(w).$$

Notice that $m \circ (S \otimes \text{id})(R \otimes R) \subseteq R$ and so if we look at the coefficient of x^{d+1} on the right-hand side, we see that it is $m \circ (S \otimes \text{id})(v)a_d$. Since $R \otimes R$ is a domain and a_d is nonzero, we see that $m \circ (S \otimes \text{id})(v) = 0$. Geometrically, this means precisely that $v(g^{-1}, g) = 0$ for all $g \in G$.

Next we apply coassociativity, which tells us that $(\Delta \otimes \text{id})(\Delta(x)) = (\text{id} \otimes \Delta)(\Delta(x))$ in $R \otimes_k R \otimes_k R = k[G \times G \times G]$. Writing this out using (4.2), and equating the coefficients of $x \otimes x \otimes x$, yields

$$(\Delta \otimes \text{id})(v) \cdot (v \otimes 1) = (\text{id} \otimes \Delta)(v) \cdot (1 \otimes v).$$

Evaluating at (g, h^{-1}, h) for any fixed $g, h \in G$ we get

$$v(gh^{-1}, h)v(g, h^{-1}) = v(g, 1_G)v(h^{-1}, h) = 0$$

where the final equality uses what we proved in the previous paragraph. Now, if $v \neq 0$ then for a Zariski dense set of $(g, h) \in G \times G$, $v(g, h^{-1}) \neq 0$. But then for each such (g, h) the above equation implies that $v(gh^{-1}, h) = 0$. Hence, in fact, $v(gh^{-1}, h) = 0$ for all $(g, h) \in G \times G$. As every element of $G \times G$ can be written in the form (gh^{-1}, h) , we have shown that $v = 0$.

We have thus proven that

$$(4.3) \quad \Delta(x) = s(1 \otimes x) + t(x \otimes 1) + w$$

for some $s, t, w \in R \otimes_k R$.

We claim now that either $t = 0$ or $t = 1 \otimes b$ for some group-like $b \in R$. We again apply coassociativity to x , this time using (4.3) and equating the coefficients of $x \otimes 1 \otimes 1$, to get

$$(\Delta \otimes \text{id})(t) \cdot (t \otimes 1) = (\text{id} \otimes \Delta)(t)$$

The geometric interpretation is that

$$(4.4) \quad t(fg, h)t(f, g) = t(f, gh)$$

for all $f, g, h \in G$.

Suppose $t(1_G, g_0) = 0$ for some $g_0 \in G$. We show in this case that $t = 0$. Indeed, for all $h \in G$ we have $0 = t(g_0, h)t(1_G, g_0) = t(1_G, g_0h)$, by (4.4) with $f = 1_G$. Hence, $t(1_G, h) = 0$ for all $h \in G$. But then, by (4.4) with $f = g^{-1}$, we get $0 = t(1_G, h) = t(g^{-1}g, h)t(g^{-1}, g) = t(g^{-1}, gh)$ for all $g, h \in G$. As every element of $G \times G$ is of the form (g^{-1}, gh) for some $g, h \in G$, we have $t = 0$, as desired.

Suppose on the contrary that $t(1_G, g) \neq 0$ for every $g \in G$. Then $t(g, h) = \frac{t(1_G, gh)}{t(1_G, g)}$ is a never vanishing regular function on $G \times G$, and hence $t = \lambda t'$ where

$\lambda \in k^*$ and $t' : G \times G \rightarrow \mathbb{G}_m$ is an algebraic group homomorphism (see [19, Theorem 3]). So $t' = b' \otimes b$ where $b', b \in R$ are group-like. But then we have

$$\lambda b'(g)b(h) = t(g, h) = \frac{t(1_G, gh)}{t(1_G, g)} = \frac{\lambda b(gh)}{\lambda b(g)} = \frac{\lambda b(g)b(h)}{\lambda b(g)}$$

for all $g, h \in G$. It follows that $b' = \lambda = 1$ and $t = 1 \otimes b$, as desired.

A similar argument shows that in (4.3) either $s = 0$ or $s = a \otimes 1$ for some group-like $a \in R$. This proves the theorem. \square

Remark 4.3. It may be worth pointing out that our proof of Theorem 4.2 made no use of σ and δ . We used only the properties of a Hopf algebra extension, as well as the fact that every element of A can be written as a left polynomial in x over R .

Corollary 4.4. *Suppose k is an algebraically closed field of characteristic zero and R is a commutative affine Hopf k -algebra equipped with a k -algebra automorphism σ and a k -linear σ -derivation δ . If $R[x; \sigma, \delta]$ admits a Hopf algebra structure extending that of R then $(R, \Delta, \sigma, \delta)$ must satisfy the following two conditions.*

- (1) *There exists $w \in R \otimes_k R$ and a group-like $a \in R$ such that, for all $r \in R$,*

$$\Delta(\delta(r)) = \sum (\delta(r_1) \otimes r_2 + ar_1 \otimes \delta(r_2)) + w(\Delta(r) - \Delta(\sigma(r)))$$

- (2) *There is a character $\chi : R \rightarrow k$ such that for all $r \in R$,*

$$\sigma(r) = \sum \chi(r_1)r_2 = \sum r_1\chi(r_2).$$

In the above we are using Sweedler notation, writing $\Delta(r) = \sum r_1 \otimes r_2$ for all $r \in R$.

Proof. Statements (1) and (2) are proven for Hopf Ore extensions in [5]. Indeed, remembering that in our case R is commutative, statement (2) is just part (i)(c) of the main theorem of [5] (see also Theorem 2.4(d) of [5]), and statement (1) is the identity labelled (21) in [5] which is asserted in part (i)(d) of the main theorem. So to prove the corollary it suffices to show that $A = R[x; \sigma, \delta]$ is a Hopf Ore extension, that is, after a change of variable $\Delta(x)$ has the form (4.1) discussed above. But Theorem 4.2 gives us an even stronger form for $\Delta(x)$. \square

Remark 4.5. The main theorem of [5] also includes a converse; namely, assuming that $(R, \Delta, \sigma, \delta)$ satisfies (1) and (2), with $w \in R \otimes_k R$ satisfying two other identities, one can always extend in a natural way the Hopf algebra structure from R to $R[x; \sigma, \delta]$. This gives many examples to which our Theorem 4.1 will apply.

4.2. The case when σ is the identity. When $\sigma = \text{id}$ note that a σ -derivation is just a derivation. In this case we write the Ore extension as $R[x; \delta]$; it is the skew polynomial ring in x over R where $xr = rx + \delta(r)$ for all $r \in R$. Statement (1) of Corollary 4.4 now says that if $R[x; \delta]$ admits a Hopf algebra structure extending that on R , then δ must have been an a -coderivation on R . So Theorem 3.1 applies and we have that (R, δ) satisfies the δ -DME. The following proposition relates the δ -DME for (R, δ) to the DME for $R[x; \delta]$.

Proposition 4.6. *Suppose k is a field of characteristic zero and R is a commutative affine k -algebra equipped with a k -linear derivation δ . If the δ -rational prime δ -ideals of (R, δ) are δ -locally-closed, then the rational prime ideals of $R[x; \delta]$ are locally closed.*

In particular if the δ -DME holds for (R, δ) then the DME holds for $R[x; \delta]$.

Proof. Suppose P is a rational prime ideal of $R[x; \delta]$. Let $I := P \cap R$. Then I is a prime ideal of R . Moreover, I is a δ -ideal since if $a \in P \cap R$ then $\delta(a) = [x, a] \in P \cap R$. It follows easily that $J := IR[x; \delta]$ is an ideal of $R[x; \delta]$ that is contained in P and that $R[x; \delta]/J \cong (R/I)[x; \delta]$ where we use δ to denote the induced derivation on $S := R/I$. Let $F = \text{Frac}(S)$ be the Goldie quotient ring and extend δ to F . We claim that the δ -constants of F are all algebraic over k . Indeed, note that if $f \in F$ with $\delta(f) = 0$ then f is a central element of $F[x; \delta]$. We let \tilde{P} denote the prime ideal in $S[x; \delta]$ corresponding to P under the isomorphism $R[x; \delta]/J \cong S[x; \delta]$. As $P \cap R = I$, we have that $\tilde{P} \cap S = 0$, so that \tilde{P} lifts to a prime ideal P_0 of $F[x; \delta]$. The image of f in $B := F[x; \delta]/P_0$ is again a central element of B . By construction B is a localization of $S[x; \delta]/\tilde{P} \cong R[x; \delta]/P$ and thus passing to the full localization gives that f is a central element of $\text{Frac}(R[x; \delta]/P)$. As P is rational f must be algebraic over k .

We have shown that the prime δ -ideal I is δ -rational. By assumption it is therefore δ -locally-closed. Consequently, there is some $g \in R \setminus I$ such that every prime δ -ideal of R properly containing I must contain g .

In order to prove that P is locally closed it now suffices to show that whenever $Q \supsetneq P$ is prime then $Q \cap R \supsetneq P \cap R = I$. Indeed, if this is the case, then we have that $g \in \bigcap \{Q \cap R : Q \supsetneq P \text{ prime}\}$. Since $g \notin P$, we have in particular that $\bigcap \{Q : Q \supsetneq P \text{ prime}\} \neq P$. That is, P is locally closed.

Towards a contradiction therefore, let us assume that there exists a prime ideal $Q \supsetneq P$ with $Q \cap R = P \cap R = I$. It follows that $F[x; \delta]$ is not simple: under the isomorphism $R[x; \delta]/J \cong S[x; \delta]$, Q corresponds to a nonzero prime ideal \tilde{Q} in $S[x; \delta]$ whose intersection with $S = R/I$ is trivial, so that \tilde{Q} lifts to a nonzero prime ideal Q_0 in $F[x; \delta]$. On the other hand, it is well-known that, as F is a field of characteristic zero, if δ is nontrivial on F then $F[x; \delta]$ is a simple ring (indeed this is a consequence of the fact that $F[x; \delta]$ is a left and right PID, see [21, §2.1]). Thus, δ is trivial on F and so $F[x; \delta] = F[x]$ is a PID. So P_0 , the lift of \tilde{P} from $S[x; \delta]$ to $F[x; \delta]$, as it is properly contained in Q_0 , must be 0. That is, $F[x; \delta]$ is a localisation of $R[x; \delta]/P$. Hence, $\text{Frac}(R[x; \delta]/P) = F(x)$, contradicting the rationality of P .

For the “in particular” clause, note that $R[x; \delta]$ satisfies the Nullstellensatz – by [10, Theorem 2] for example – and hence we already know that local-closedness implies primitivity and primitivity implies rationality. \square

Corollary 4.7. *Suppose k is an algebraically closed field of characteristic zero and R is a commutative affine Hopf k -algebra equipped with a k -linear derivation δ that is also an a -coderivation for some group-like $a \in R$. Then $R[x; \delta]$ satisfies the DME.*

Proof. Theorem 3.1 together with Proposition 4.6. \square

A special case of Corollary 4.7 is when R is a differential Hopf k -algebra – this yields Theorem B1 of the introduction. But the DME for $R[x; \delta]$ in that case is easier: one uses only Theorem 2.19 and the material in Section 3 is not necessary.

4.3. The case when δ is inner. If σ is an automorphism of R , and $a \in R$, then the map $r \mapsto a(r - \sigma(r))$ is a σ -derivation on R . Such σ -derivations are called *inner*. Here is a sufficient criterion for a σ -derivation δ being inner.³

³For a more general statement in the noncommutative case, see [8, Lemma 2.4(b)].

Lemma 4.8. *Suppose R is a commutative ring with an automorphism σ and a σ -derivation δ . Suppose there exists an element $f \in R$ such that $f - \sigma(f)$ is a unit. Then δ is inner.*

Proof. It is easy to see, using the commutativity of R , that $a := \frac{\delta(f)}{f - \sigma(f)}$ witnesses the inner-ness of (R, σ, δ) . \square

When δ is inner the Dixmier-Moeglin equivalence for $R[x; \sigma, \delta]$ follows easily from known results. It makes use however of one more notion:

Definition 4.9. Let A be a finitely generated algebra over a field k . We say that a k -vector subspace V of A is a *frame* for A if V is finite-dimensional, contains 1_A , and generates A as a k -algebra.

Lemma 4.10. *Suppose R is a commutative affine Hopf algebra over a field k of characteristic zero and σ is a k -algebra automorphism of R satisfying statement (2) of Corollary 4.4. Then there is a frame for R such that $\sigma(V) = V$.*

Proof. Suppose $R = k[G]$ where G is an affine algebraic group. Then G is linear and hence we may embed G into GL_n . This gives us a frame V of R spanned by the restriction to G of 1, the coordinate functions $x_{i,j}$, and $\frac{1}{\det}$. Now, $\Delta(x_{i,j}) = \sum x_{i,k} \otimes x_{k,j}$ and $\Delta(\frac{1}{\det}) = \frac{1}{\det} \otimes \frac{1}{\det}$. So $\Delta(V) \subseteq V \otimes V$. Statement (2) of Corollary 4.4 then implies that $\sigma(V) \subseteq V$, and hence by finite-dimensionality $\sigma(V) = V$. \square

Proposition 4.11. *Suppose k is an uncountable algebraically closed field of characteristic zero, R is a finitely generated commutative k -algebra, σ is a k -algebra automorphism of R that preserves a frame, and δ is an inner σ -derivation on R . Then $R[x; \sigma, \delta]$ satisfies the DME.*

Proof. When $\delta = 0$ this is [2, Theorem 1.6]; while the theorem there is stated for $k = \mathbb{C}$ it holds for any uncountable algebraically closed field. But if $a \in R$ is such that $\delta(r) = a(r - \sigma(r))$ for all $r \in R$, then $R[x; \sigma, \delta] = R[t; \sigma, 0]$ where $t := x - a$. Indeed,

$$\begin{aligned} tr &= (x - a)r \\ &= \sigma(r)x + \delta(r) - ar \\ &= \sigma(r)x - a\sigma(r) \\ &= \sigma(r)t \end{aligned}$$

for all $r \in R$, and $\{t^n : n \geq 0\}$ can be seen to be another left R -basis for $R[x; \sigma, \delta]$ using the fact that, for any polynomial P , $P(t)$ is equal to $P(x)$ plus terms of strictly lower degree. So the inner case reduces to the case when $\delta = 0$. \square

4.4. The general case. Let us fix from now on a field k of characteristic zero. Our proof of Theorem 4.1 will go via reducing either to the case when $\sigma = \mathrm{id}$ or when δ is inner. But it will require some preparatory lemmas. First, let us point out that statement (2) of Corollary 4.4 forces (R, σ) to be of a very restricted form.

Lemma 4.12. *Let G be a connected affine algebraic group over k and $\tau : G \rightarrow G$ an automorphism of G over k . Let $R = k[G]$, and $\sigma = \tau^*$ the corresponding k -algebra automorphism of R . If (R, σ) satisfies statement (2) of Corollary 4.4 then $\tau : G \rightarrow G$ is translation by some central element of $G(k)$.*

Proof. Since $\chi : R \rightarrow k$ is a homomorphism there is some $c \in G(k)$ such that $\chi(f) = f(c)$ for all $f \in R$. If we write $\Delta(f) = \sum f_1 \otimes f_2$, then by the definition of the coproduct on R we have $f(ab) = \sum f_1(a)f_2(b)$ for all $a, b \in G$. Now, property (2) gives us that for all $a \in G$, $\sigma(f)(a) = \sum \chi(f_1)f_2(a) = \sum f_1(c)f_2(a) = f(ca)$. The other half of the equality in (2) gives $\sigma(f)(a) = f(ac)$. So $f(ca) = f(ac)$ for all $f \in R$, and hence c is central in G . On the other hand, $f(ca) = \sigma(f)(a) = f(\tau a)$ for all $f \in R$, so τ is translation by c . \square

We will make use of the following notion from [8].

Definition 4.13. Suppose σ is an automorphism of a commutative ring R . By a σ -prime ideal is meant a σ -ideal I such that whenever J and K are σ -ideals with $JK \subseteq I$ then either $J \subseteq I$ or $K \subseteq I$.

Note that a σ -prime ideal need not be prime. But, at least in the case when R is a commutative noetherian ring, a σ -prime ideal is radical; this follows from the fact that the nilpotent radical of I is a σ -ideal and some power of it is contained in I . We will sometimes need to quotient out by σ -prime ideals that we do not know are prime, which means we will have to work with reduced difference rings that are not necessarily integral domains. The following lemma about such difference rings will be very useful.

Lemma 4.14. *Suppose R is a noetherian commutative k -algebra endowed with a k -algebra automorphism σ such that (0) is σ -prime. If $0 \neq f \in R$ satisfies $\sigma(f) = \lambda f$ for some $\lambda \in k^*$ then f is not a zero divisor in R .*

Proof. Let P_1, \dots, P_r be the minimal prime ideals of R . We have already pointed out that $\bigcap_j P_j = (0)$. Moreover, (0) being σ -prime implies that the group generated by σ must act transitively on $\{P_1, \dots, P_r\}$, see for example [7, Remark 5*].

Now suppose that $fh = 0$ for some nonzero $h \in R$. Since h is nonzero there is some i such that $h \notin P_i$. Thus $f \in P_i$. But now, since the group generated by σ acts transitively on $\{P_1, \dots, P_r\}$, for each j there is some n such that $\sigma^n(f) \in P_j$. As $\sigma^n(f) = \lambda^n f$ we get $f \in P_j$. So $f \in \bigcap_j P_j = (0)$, a contradiction. \square

Finally, we will make use of the following fundamental result on Ore extensions of commutative noetherian rings.

Fact 4.15 (Goodearl [8]). *Suppose R is a commutative noetherian ring, σ is an automorphism of R , and δ is a σ -derivation. Suppose P is a prime ideal of the Ore extension $R[x; \sigma, \delta]$, and let $I = P \cap R$. Then one of the following three statements must hold:*

- I. $R[x; \sigma, \delta]/P$ is commutative.
- II. I is a (σ, δ) -ideal of R – that is, I is preserved under σ and δ – and there is a prime ideal I' of R containing I such that $\sigma(r) - r \in I'$ for all $r \in R$.
- III. I is a σ -prime (σ, δ) -ideal of R and $IR[x; \sigma, \delta]$ is a prime ideal of $R[x; \sigma, \delta]$.

We can now prove the theorem.

Proof of Theorem 4.1. We have that R is a commutative affine Hopf k -algebra equipped with a k -algebra automorphism σ and a k -linear σ -derivation δ , and that the Ore extension $A := R[x; \sigma, \delta]$ admits a Hopf algebra structure extending that of R . We wish to show that A satisfies the DME. By [10, Theorem 2] we have that

A satisfies the Nullstellensatz, and so it suffices to prove that if P is a rational prime ideal of A then P is locally closed.

We first reduce to the case when k is algebraically closed. Since $R = k[G]$ where G is an affine algebraic group, and hence smooth, R is integrally closed. Let F denote the field of fractions of R and let $F_0 := k^{\text{alg}} \cap F$. Since R is integrally closed, $F_0 \subseteq R$. Since F is a finitely generated extension of k , F_0 is a finite extension of k . Let $R' := R \otimes_{F_0} k^{\text{alg}}$. Since F_0 is relatively algebraically closed in F , we see that R' is again an integral domain. Thus R' is a commutative affine Hopf k^{alg} -algebra to which we extend σ and δ by k^{alg} -linearity. Suppose we have proven the DME for $R'[x; \sigma, \delta]$. Then Irving-Small reduction techniques (see Irving-Small [11] and also Rowen [20, Theorem 8.4.27]) give that $A = R[x; \sigma, \delta]$ satisfies the DME over F_0 . But since F_0 is a finite extension of k , we get the DME over k also.

Next we reduce to the case when k is uncountable (in order to be able to use Proposition 4.11). Let L be an uncountable algebraically closed extension of k . Then since k is algebraically closed we see that $R \otimes_k L$ is a commutative affine Hopf L -algebra to which we extend σ and δ by L -linearity, and $B := A \otimes_k L \cong (R \otimes_k L)[x; \sigma, \delta]$. Assume the DME holds for B . Let P be a rational prime ideal of A and let $Q = P \otimes_k L$. Since k is algebraically closed, Q is a prime ideal of B . Since P is rational and $B/Q = (A/P) \otimes_k L$, we see that Q is a rational. Hence Q is locally closed. Since the primes in A containing P lift to primes in B containing Q , it follows that P is locally closed in A . So A satisfies the DME.

We may therefore assume that k is uncountable and algebraically closed.

If $\sigma = \text{id}$ then δ is a k -linear derivation on R and statement (1) of Corollary 4.4 tells us that it is also an a -coderivation on for some group-like $a \in R$. It follows by Corollary 4.7 that $A = R[x; \delta]$ satisfies the DME. So we may assume $\sigma \neq \text{id}$.

We may also assume that A/P is not commutative. Indeed, if it were, as P is rational, we would have that $\text{Frac}(A/P) \subseteq k$, so that P is a maximal ideal and hence locally closed.

Write $R = k[G]$ where G is a connected affine algebraic group over k . By Lemma 4.12 we know that $\sigma = \tau^*$ where $\tau : G \rightarrow G$ is translation by a central (non-identity) element $c \in G(k)$.

Our next goal is to reduce to the case that $P \cap R = (0)$, though in order to obtain this we will have to give up on R being an integral domain. Let $I = R \cap P$. We have already ruled out case (I) of Fact 4.15. On the other hand, case (II) cannot hold: σ would induce the identity map on R/I , implying that τ is the identity on $V(I')$, which contradicts the fact that it is translation on G by a non-identity element. Hence case (III) holds; I is a σ -prime (σ, δ)-ideal of R and $J := IA$ is a prime ideal of A . Consider now the reduced quotient ring $\bar{R} := R/I$ with the induced automorphism which we continue to denote by σ , and the induced σ -derivation which we continue to denote by δ . Let $\bar{A} = A/J \cong \bar{R}[x; \sigma, \delta]$ and \bar{P} the image of P in \bar{A} . Since J is contained in P , \bar{P} is rational in \bar{A} and it suffices to show that \bar{P} is locally closed in \bar{A} . Note that we have achieved $\bar{P} \cap \bar{R} = (0)$.

Next, we claim that there is some non zero-divisor $f \in \bar{R}$ such that (σ, δ) extends to $\tilde{R} := \bar{R}[1/f]$ and δ is inner on \tilde{R} . To see this, consider the frame V for R , given by Lemma 4.10, that is preserved by σ . The image \bar{V} of V in \bar{R} is then a frame for \bar{R} that is also preserved by σ . Using $k = k^{\text{alg}}$, let f be an eigenvector for the action of σ on \bar{V} , say $\sigma(f) = \lambda f$ for some $\lambda \in k^*$. By Lemma 4.14, f is not a zero divisor. Moreover, the multiplicatively closed subset $\{1, f, f^2, \dots\}$ of R is preserved by σ ,

and hence by [8, Lemma 1.3], (σ, δ) extends uniquely to the localisation at this set, namely to $\tilde{R} := \overline{R}[1/f]$. It remains to show that f can be chosen so that δ is inner on \tilde{R} . If the eigenvalue λ is not equal to 1, then $f - \sigma(f) = (1 - \lambda)f$ is a unit in \tilde{R} , and we get δ inner by Lemma 4.8. So suppose that 1 is the only eigenvalue for σ on \overline{V} . Note that σ is not the identity operator on \overline{R} because τ is not the identity on $V(I)$. Since \overline{V} generates \overline{R} as a k -algebra, σ is not the identity on \overline{V} either. Hence there must be some Jordan block that is of size greater than one, but with eigenvalue 1. So we can choose the eigenvector f in such a way that there exists nonzero $g \in \overline{V}$ with $\sigma(g) = g + f$. Hence $g - \sigma(g)$ is a unit in $\tilde{R} = \overline{R}[1/f]$, and so by Lemma 4.8 again, δ is inner on \tilde{R} .

To prove that \overline{P} is locally closed let us consider the following partition of the set of prime ideals of \overline{A} that properly extend \overline{P} .

$$\begin{aligned} S_1 &:= \{Q \supsetneq P : Q \text{ prime, and no power of } f \text{ is in } Q\} \\ S_2 &:= \{Q \supsetneq P : Q \text{ prime, not in } S_1, \text{ and } Q \cap \overline{R} \text{ is a } \sigma\text{-prime } (\sigma, \delta)\text{-ideal}\} \\ S_3 &:= \{Q \supsetneq P : Q \text{ prime, and not in } S_1 \text{ or } S_2\} \end{aligned}$$

It suffices to show that for each of $i = 1, 2, 3$, $\bigcap S_i \neq \overline{P}$.

For $i = 2$, note that as σ -prime implies radical, we have that $f \in Q$ for all $Q \in S_2$, but $f \notin \overline{P}$ as $\overline{P} \cap \overline{R} = (0)$.

For $i = 3$, applying Fact 4.15 to $Q \in S_3$, we have that either \overline{A}/Q is commutative or there is in $\overline{R} = \overline{R}/I$ a prime ideal $\overline{I} := I'/I$ extending $Q \cap \overline{R}$, and such that σ is the identity on $\overline{R}/\overline{I} = R/I'$. The latter case is impossible using again that $\sigma = \tau^*$ and τ is translation on G by a non-identity element. So \overline{A}/Q is commutative for all $Q \in S_3$. As $\overline{A}/\overline{P} = A/P$ is not commutative there exist $a, b \in \overline{A}$ such that $g := [a, b] \notin \overline{P}$. But $g \in Q$ for all $Q \in S_3$.

It remains therefore to consider S_1 . Let

$$\tilde{A} = \tilde{R}[x; \sigma, \delta] = R\left[\frac{1}{f}\right][x; \sigma, \delta].$$

As δ is inner on \tilde{R} , Proposition 4.11 tells us that \tilde{A} satisfies the Dixmier-Moeglin equivalence. As $\overline{P} \cap \overline{R} = (0)$, we know that no power of f is in \overline{P} , and hence $\tilde{P} := \overline{P}\tilde{A}$ is a prime ideal. As \tilde{A} is a localisation of \overline{A} we have that \tilde{P} is rational, and hence locally closed. If $Q \in S_1$ then $Q\tilde{A}$ is a prime ideal properly extending \tilde{P} . So there is $\alpha \in \tilde{A} \setminus \tilde{P}$ such that $\alpha \in Q\tilde{A}$ for all $Q \in S_1$. For some $n \geq 0$, $f^n \alpha \in \overline{A}$. So $f^n \alpha \in Q\tilde{A} \cap \overline{A} = Q$. But $f^n \alpha \notin \overline{P}$. So $\bigcap S_1 \neq \overline{P}$, as desired. \square

REFERENCES

- [1] J. Bell, S. Launois, O. León Sánchez, and R. Moosa. Poisson algebras via model theory and differential-algebraic geometry. To appear in the Journal of the European Math Society.
- [2] J. Bell, K. Wu, and S. Wu. The Dixmier-Moeglin equivalence for extensions of scalars and Ore extensions. To appear in Contemp. Math.
- [3] J. P. Bell and W. H. Leung. The Dixmier-Moeglin equivalence for cocommutative Hopf algebras of finite Gelfand-Kirillov dimension. *Algebras and Representation Theory*, 17(6):1843–1852, 2014.
- [4] K. A. Brown and K. R. Goodearl. Lectures on algebraic quantum groups. In *Advanced Courses in Mathematics*. CRM Barcelona, Birkhäuser Verlag, Basel, 2002.
- [5] K.A. Brown, S. O’Hagan, J.J. Zhang, and G. Zhuang. Connected Hopf algebras and iterated Ore extensions. *Journal of Pure and Applied Algebra*, 219(6):2405–2433, 2015.
- [6] A. Buium. *Differential algebraic groups of finite dimension*, volume 1506 of *Lecture Note in Mathematics*. Springer-Verlag, 1992.

- [7] A. Goldie and G. Michler. Ore extensions and polycyclic group rings. *Journal of the London Mathematical Society. Second Series*, 9:337–345, 1974/75.
- [8] K.R. Goodearl. Prime ideals in skew polynomial rings and quantized Weyl algebras. *Journal of Algebra*, 150(2):324–377, 1992.
- [9] E. Hrushovski. Computing the galois group of a linear differential equation. In *Differential Galois theory*, volume 58, pages 97–138. Banach Center Publications, Polish Academy of Sciences, 2002.
- [10] R. Irving. Generic flatness and the Nullstellensatz for Ore extensions. *Comm. Algebra*, 7(3):259–277, 1979.
- [11] R. Irving and L. Small. On the characterization of primitive ideals in enveloping algebras. *Math. Z.*, 173(3):217–221, 1980.
- [12] I. Kaplansky. *An introduction to differential algebra*. Hermann, Paris, second edition, 1976.
- [13] P. Kowalski and A. Pillay. Quantifier elimination for algebraic D -groups. *Trans. Amer. Math. Soc.*, 358(1):167–181, 2006.
- [14] D. Marker. Manin kernels. In *Connections between Model Theory and Algebraic and Analytic Geometry*, volume 6 of *Quaderni di Matematica*, pages 1–21. Dipartimento di Matematica Seconda Università di Napoli, 2000.
- [15] J. C. McConnell and J. C. Robson. *Noncommutative Noetherian rings*, volume 30 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, revised edition, 2001. With the cooperation of L. W. Small.
- [16] A. N. Panov. Ore extensions of Hopf algebras. *Mat. Zametki*, 74(3):425–434, 2003.
- [17] A. Pillay. Differential algebraic groups and the number of countable differentially closed fields. In *Model Theory of Fields*, volume 5 of *Lecture Notes in Logic*, pages 114–134. Springer, 1996.
- [18] A. Pillay. Remarks on algebraic D -varieties and the model theory of differential fields. In *Logic in Tehran*, volume 26 of *Lect. Notes Log.*, pages 256–269. Assoc. Symbol. Logic, La Jolla, CA, 2006.
- [19] M. Rosenlicht. Toroidal algebraic groups. *Proc. Amer. Math. Soc.*, 12:984–988, 1961.
- [20] L. Rowen. *Ring theory. Vol. II*, volume 128 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1988.
- [21] M. Singer and M. van der Put. *Galois theory of linear differential equations*, volume 328. Grundlehren der mathematischen Wissenschaften, Springer, 2003.
- [22] S. Skryabin. New results on the bijectivity of antipode of a Hopf algebra. *J. Algebra*, 306(2):622–633, 2006.

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF WATERLOO, 200 UNIVERSITY AVENUE
WEST, WATERLOO, ONTARIO, CANADA N2L 3G1
E-mail address: `jpbell@uwaterloo.ca`

SCHOOL OF MATHEMATICS, UNIVERSITY OF MANCHESTER, OXFORD ROAD, MANCHESTER, UNITED
KINGDOM M13 9PL
E-mail address: `omar.sanchez@manchester.ac.uk`

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF WATERLOO, 200 UNIVERSITY AVENUE
WEST, WATERLOO, ONTARIO, CANADA N2L 3G1
E-mail address: `rmoosa@uwaterloo.ca`