Smoothness of stabilisers in generic characteristic

Martin, Benjamin; Stewart, David; Topley, Lewis

Publication date:
2018

Document Version
Early version, also known as pre-print

SMOOTHNESS OF STABILISERS IN GENERIC CHARACTERISTIC

BENJAMIN MARTIN, DAVID STEWART AND LEWIS TOPLEY

Abstract. Let R be a commutative unital ring. Given a finitely-presented affine R-group G acting on a finitely-presented R-scheme X of finite type, we show that there is a prime p_0 so that for any R-algebra k which is a field of characteristic $p \geqslant p_0$, then the centralisers in G_k of all subsets $U \subseteq X(k)$ are smooth. We prove this using the Lefschetz principle together with careful application of Gröbner basis techniques.

1. Introduction

Let R be a commutative unital ring. We propose to prove the following.

Theorem. *Let G be a finitely presented affine R-group and let X be a finitely presented G-scheme of finite type*[1]*. Then there exists $p_0 \in \mathbb{N}$ such that whenever k is an R-algebra which is also a field of characteristic $p \geqslant p_0$, the centralisers $\mathrm{Cent}_{G_k}(S)$ of all subsets $S \subseteq X(k)$ are smooth.*

Examples of affine group schemes over rings abound. The split reductive groups are $\mathbb{Z}$-defined; so too are the subgroups normalised by a split maximal torus—so called subsystem subgroups. This class includes all parabolic subgroups, for example.

There are several known special cases of the theorem already in the literature. Possibly the most influential—at least for Lie theory—is where G is split reductive and X is either G itself or its Lie algebra, on which G acts by the relevant adjoint action. Then it is well-known that everything is defined over $\mathbb{Z}$ and the centralisers of single elements of $X(\bar{k})$ are smooth whenever p is a very good prime for G. This was first shown by Richardson [Ric67], and enabled him to give an elegant proof that the number of unipotent and nilpotent orbits of G is finite, among other things. Richardson's result was generalised in [BMRT10], to cover arbitrary subgroups of $G(\bar{k})$ and subalgebras of $\mathrm{Lie}(G)$. The hypotheses were further weakened in [Her13]. Normalisers, while much less well-behaved, were thoroughly considered in [HS16], where it was shown that (necessarily large) bounds on the characteristic exist, depending on the root system, which ensure the normalisers of subspaces of the Lie algebras in reductive groups are smooth. These results have all found applications in developing the subgroup structure of simple algebraic groups and their Lie algebras; recent examples include [LT18] and [PS18]. Beyond that, there have been consequences for combinatorics, representation theory and geometric invariant theory.

The second author computed explicitly in [Ste16] the orbits of exceptional groups on their Lie algebras, finding when centralisers and stabilisers of lines were smooth in their actions on their minimal induced (or dual-Weyl) modules; that non-smoothness only occurred in characteristics 2 or 3 motivated [*op. cit.*, Question 1.4] to which our theorem provides the following strong answer.

Corollary. *With the hypotheses of the theorem, let M be a finitely generated G-module. Then there is a prime p_M such that whenever k is an R-field of characteristic $p \geqslant p_M$, the stabilisers and centralisers of all subspaces of M are all smooth.*

[1]This means that X is a functor from R-algebras to sets admitting an action $\alpha : G \times X \to X$ such that $X = X_1 \cup \cdots \cup X_n$ with each X_i an open affine subscheme of X which is finitely presented, i.e. $X_i \cong \mathrm{Spec}_R(A)$ for A a finitely-presented R-algebra.

We should mention that bounding the dimension of modules even for fixed G will certainly not suffice for there to exist a p_0 satisfying the hypotheses of the theorem—see Remark 3.26 below.

Let us say some words on the proof and the structure of the paper. The key model-theoretic technique we use is the Lefschetz principle. An elementary survey of this powerful concept, along with a sketch of the proof, is given in Section 2.2. The version which we employ states that if there is a sentence ϕ in the first-order language of rings which is true when interpreted in some algebraically closed field of characteristic zero, then the same sentence is true when interpreted in any algebraically closed field of sufficiently large characteristic. The strategy, roughly speaking, is to use this together with Cartier's famous theorem, which says that all affine algebraic groups are smooth in characteristic 0.

Since any first-order statement in the language of rings about algebraically closed fields must ultimately be a concatenated collection of statements about the solutions of certain polynomial equations, it is by no means trivial to apply the Lefschetz principle. (Some evidence of this is provided by Remark 3.26.) To employ Lefschetz, we have had to call on a wide range of techniques from the theory of Gröbner bases, showing that there are uniform bounds on the output of various algorithms, given any input bounded in terms of some integer d, say. We can then quantify over all tuples of elements of k bounded in terms of d which can be put together to form the ingredients of a Hopf algebra, and ask in a first order way whether this is the Hopf algebra of a smooth group. (We call such a collection of data a *d-bounded Hopf quadruple*.) The Lefschetz principle tells us that it will be if $p \gg d$.

Lastly, given the hypotheses of the theorem, we show there is an integer d such that any centraliser appearing the the hypotheses of the theorem must correspond to a d-bouded Hopf quadruple. The theorem follows from this.

Acknowledgements: The third author is grateful for the support of EPSRC grant EP/N034449/1.

2. Preliminaries

Throughout the paper we fix a commutative unital ring R.

2.1. Schemes, group schemes and Hopf algebras.

We take the functorial approach to schemes, as per [DG70] and [Jan03]. Thus for an R-algebra A we think of $\mathrm{Spec}_R(A)$ as the functor $\mathrm{Hom}_{R\text{-Alg}}(A, -) : \underline{R\text{-Alg}} \to \underline{\mathrm{Set}}$. A functor $X : \underline{R\text{-Alg}} \to \underline{\mathrm{Set}}$ is *affine* if it is isomorphic to $\mathrm{Spec}_R(R[X])$ for some R-algebra $R[X]$. We say a subfunctor Y of a functor $X : \underline{R\text{-Alg}} \to \underline{\mathrm{Set}}$ is *open* if for every R-algebra A and natural transformation $\beta : \mathrm{Spec}_R A \to X$, the subfunctor $\beta^{-1}(Y)$ of $\mathrm{Spec}_R A$ is isomorphic to $\mathrm{Spec}_R(A/I)$ for some ideal I. Then X is a *scheme* if it is *local*[2] and admits a decomposition $X = \bigcup_{i\in\mathbb{I}} X_i$ for some indexing set $\mathbb{I}$, where the X_i are open affine subfunctors of X. We say X is of *finite type* if $\mathbb{I}$ is finite and that it is *finitely presented* if each $k[X_i]$ is isomorphic to $k[t_1, \ldots, t_n]/I$ for I a finitely generated ideal.

An affine algebraic group scheme G over R is a functor from $\underline{R\text{-Alg}}$ to $\underline{\mathrm{Grp}}$, which as a functor to $\underline{\mathrm{Set}}$, is naturally equivalent to one of the form $\mathrm{Spec}_R(R[G])$ for some finitely generated R-algebra $R[G]$; consistent with [Jan03], we consider only the case where $R[G]$ is in fact finitely presented. The archetypal example of an algebraic group scheme is GL_d, which is also an example of a split reductive group.

A Hopf R-algebra consists of data $(R[G], \Delta, \sigma, \epsilon)$ where $R[G]$ is an R-algebra, and $\Delta : R[G] \to R[G] \otimes_R R[G]$, $\sigma : R[G] \to R[G]$ and $\epsilon : R[G] \to R$ are R-algebra homomorphisms satisfying the dual of the group axioms [Jan03, I.2.3(1–3)]:

[2]See [DG70, Definition I.1.3.11]

$$(\Delta \otimes \mathrm{id}) \circ \Delta = (\mathrm{id} \otimes \Delta) \circ \Delta \tag{2.1}$$

$$(\epsilon \bar{\otimes} \mathrm{id}) \circ \Delta = (\mathrm{id} \bar{\otimes} \epsilon) \circ \Delta \tag{2.2}$$

$$(\sigma \bar{\otimes} \mathrm{id}) \circ \Delta = \bar{\epsilon} = (\mathrm{id} \bar{\otimes} \sigma) \circ \Delta. \tag{2.3}$$

Hence by definition, the category of algebraic group schemes over R is dual to the category of finitely presented Hopf algebras over R.

The Lie algebra $\mathrm{Lie}(G)$ of a group scheme G over R corresponding to a Hopf algebra $(R[G], \Delta, \sigma, \epsilon)$ is defined to be the R-module of all R-linear maps $I/I^2 \to R$ where $I = \mathrm{Ker}(\epsilon)$; in other words it is $\ker\left(G(R[\epsilon]/(\epsilon^2)) \to G(R)\right)$ where $R[\epsilon]/(\epsilon^2)$ is the algebra of dual numbers and the map takes ϵ to 0. Following [Jan03, I.7.7(3)] there is a natural R-linear Lie bracket on $\mathrm{Lie}(G)$ induced by the comultiplication Δ. Every morphism of group schemes over R induces a natural R-linear homomorphism of Lie algebras.

When G is a group scheme and k is any R-algebra we can consider the base change G_k, which is a group scheme over k obtained by viewing k-algebras as R-algebras. If $G \cong \mathrm{Spec}_R(R[X])$ is algebraic and $R[X] \cong R[x_1, ..., x_n]/(g_1, ..., g_m)$ then we obtain a map $\omega : R[x_1, ..., x_n] \to k[x_1, ..., x_n]$ and we have

$$G_k \cong \mathrm{Spec}_k\left(k[x_1, ..., x_n]/(\omega(g_1), ..., \omega(g_m))\right). \tag{2.4}$$

An action of G on an R-scheme X is a natural transformation $\alpha : G \times X \to X$, such that $\alpha(A) : G(A) \times X(A) \to X(A)$ is a group action. In case X is an R-module and $G(A)$ acts through A-linear transformations of $X(A)$, then we say X is a G-module. Note that if X is affine, then we get a coaction map of R-algebras $\Delta_X : R[X] \to R[X] \otimes R[G]$. In case X is a G-module, this is the *comodule map* of [Jan03, I.2.8].

2.2. **Model theory and the Lefschetz principle.** We include here a short recap of some of the elements of model theory; a more detailed introduction to the theory may be read in [Mar02]. Since our goal is to explain the Lefschetz principle, we work exclusively with the language of rings.

The *language of rings* $\mathcal{L}_{\mathrm{ring}}$ is the collection of first-order formulas which can be built from the symbols $\{\forall, \exists, \vee, \wedge, \neg, +, -, \times, 0, 1, =\}$ along with arbitrary choice of variables. For example, for $n > 0$ fixed the following are formulas in $\mathcal{L}_{\mathrm{ring}}$:

$$(\forall x)(\forall y)(x^n + y^n = z^n); \tag{2.5}$$

$$(\forall x)(\exists y)\left((xy = 1) \vee (x = 0)\right); \tag{2.6}$$

$$(\forall x_0)(\forall x_1) \cdots (\forall x_{n-1})(\exists y)(y^n + x_{n-1}y^{n-1} + \cdots + x_0 = 0). \tag{2.7}$$

We say that a formula is a *sentence* if every variable is bound to a quantifier; for example for formula (2.5) is not a sentence because z is a free variable, whilst (2.6) and (2.7) are both sentences in $\mathcal{L}_{\mathrm{ring}}$. For $p \geqslant 0$ we record one more first-order sentence ψ_p in $\mathcal{L}_{\mathrm{ring}}$:

$$\psi_p \quad : \quad \underbrace{1 + \cdots + 1}_{p \text{ times}} = 0. \tag{2.8}$$

An $\mathcal{L}_{\mathrm{ring}}$-*structure* is a set R together with elements $0_R, 1_R \in R$, binary operations $+_R, -_R, \times_R : R \times R \to R$, and the binary relation $=_R$ which is always taken to be the diagonal embedding $R \subseteq R \times R$. For example, every ring R gives rise to an $\mathcal{L}_{\mathrm{ring}}$-structure in the obvious way.

An $\mathcal{L}_{\mathrm{ring}}$-*theory* is a set T of first order sentences in $\mathcal{L}_{\mathrm{ring}}$. A theory should be thought of as a collection of axioms of some class of mathematical object, and in this article our primary interest is the $\mathcal{L}_{\mathrm{ring}}$-theory of fields. The axioms of a field can obviously be written as first-order sentences in $\mathcal{L}_{\mathrm{ring}}$; for instance (2.6) expresses the existence of multiplicative inverses. The theory AC of algebraically closed fields is obtained by including the sentences (2.7) for all $n > 0$. If

$p > 0$ is prime then we may include the sentence ψ_p, defined in (2.8), to obtain the theory AC_p of algebraically closed fields of characteristic $p > 0$. Alternatively we may include the sentences $\{\neg\psi_p \mid p > 0\}$ to obtain the theory AC_0.

If ϕ is a sentence and $M := (R, +_R, -_R, \times_R, 0_R, 1_R, =_R)$ is an $\mathcal{L}_{\text{ring}}$-structure then we say that M *is a model of* ϕ, and write $M \vDash \phi$, if the sentence ϕ is true when interpreted in M. If T is an $\mathcal{L}_{\text{ring}}$-theory then we say that M *is a model of* T and write $M \vDash T$ if $M \vDash \phi$ for all $\phi \in T$. For example, $M \vDash \mathsf{AC}_p$ is equivalent to the statement that $(R, +_R, -_R, \times_R, 0_R, 1_R)$ is an algebraically closed field with $\text{char}(R) = p$. As such we may slightly abuse terminology and identify the class of models of AC_p with the class of algebraically closed fields of characteristic p. The following result is Gödel's first completeness theorem.

Lemma 2.1. *Let ϕ be a first-order sentence and T be any theory in $\mathcal{L}_{\text{ring}}$. Then ϕ is true when interpreted in every model of T if and only if ϕ can be deduced from T by means of a formal proof in $\mathcal{L}_{\text{ring}}$.*

We say that an $\mathcal{L}_{\text{ring}}$-theory T is *complete* if, for every first-order sentence ϕ in $\mathcal{L}_{\text{ring}}$, either ϕ is true when interpreted in every model of T, or $\neg\phi$ is true when interpreted in every model of T. By Lemma 2.1 this is equivalent to saying that for every sentence ϕ we can derive either ϕ or $\neg\phi$ from T by means of a formal proof. The following well-known result is proven by quantifier elimination [Mar02, Corollary 3.2.3].

Theorem 2.2. *For $p = 0$ or p prime, the theory AC_p is complete.*

As an immediate consequence we obtain:

Corollary 2.3. *(Lefschetz principle) If ϕ is a sentence in $\mathcal{L}_{\text{ring}}$ then:*

(1) *If ϕ is true in some model of AC_p where $p \geqslant 0$ then ϕ is true in every model of AC_p.*
(2) *If ϕ is true in some model of AC_0 then there exists a $p_0 \in \mathbb{N}$ such that ϕ is true in any model of AC_p for $p > p_0$.*

Proof. Part (1) is precisely Theorem 2.2. For part (2) suppose that ϕ is true over some field satisfying the axioms AC_0. Then by part (1) it is true for every such field, and by Lemma 2.1 we conclude that there exists a formal proof for ϕ in $\mathcal{L}_{\text{ring}}$ using only the axioms of AC_0. Since the proof of ϕ can be written as a finite sequence of sentences in $\mathcal{L}_{\text{ring}}$ joined by logical connectives, it follows that the set of primes

$$P_\phi := \{p \mid \neg\psi_p \text{ occurs in the proof of } \phi\}$$

is finite, where ψ_p is defined in (2.8). Hence for $p > \max(P_\phi)$ there is a formal proof of ϕ using the axioms of AC_p. Using Lemma 2.1 once more we see that ϕ is true for every algebraically closed field satisfying the axioms of AC_p. □

3. Smoothness of centralisers: Proof of the Theorem

3.1. **Bounded polynomials and Gröbner bases.** For a field k, we will want to quantify over all k-algebras of bounded presentation, equipped with the structure of a Hopf algebra of bounded presentation. That is to say that the lengths and degrees of the expressions which appear in the defining ideal of the underlying affine algebra, together with the comultiplication, antipode and counit are all of bounded presentation. To do so, we need to formulate statements to say that the Hopf algebra axioms are satisfied. Our main tool to this end will be to quantify over all Gröbner bases of bounded degree.

We refer to [Eis95, Ch. 15] for a fulsome introduction to Gröbner bases, but for our purposes we collect a simplified version here.

The basic principle is to provide a process for reduction of elements of $S := k[x_1, \dots x_n]$ by elements of an ideal which will terminate in a finite number of steps. Hence one wants to know when the size of an expression is reduced by an operation, and for this one first needs to choose a total order on monomials. This order needs to be *admissible* in the sense that $m_1 > m_2$ implies $nm_1 > nm_2 > m_2$ for any monomials m_1, m_2, n such that n is non-trivial monomial.

We will mostly demand of the order that for any monomial $m \in S$, there are only finitely many $m' < m$. Hence we may use the homogeneous lexicographic ordering, in which

$$m := x_1^{a_1} \dots x_n^{a_n} > m' := x_1^{b_1} \dots x_n^{b_n} \text{ if and only if } \deg m > \deg m'$$
$$\text{or if } \deg m = \deg m' \text{ then } a_i > b_i \text{ for the first index } i \text{ with } a_i \neq b_i.$$

Thus the set of monomials is isomorphic to $\mathbb{N}$ as a totally ordered set. We define m_k to be the *kth monomial in* S and observe that $\mathsf{m}_1 = 1$. For a polynomial expression $f \in S$, we then define a *term* of f to be any monomial appearing in f with a nonzero coefficient and the *initial term* $\mathrm{in}(f)$ to be the greatest term appearing in f with respect to $>$. For an ideal $I \subseteq S$, we define $\mathrm{in}(I)$ to be the ideal generated by the elements $\mathrm{in}(f)$ for all $f \in I$.

Definition 3.1. A *Gröbner basis* with respect to $>$ is an ordered list of elements $(g_1, \dots, g_t) \in S^t$ such that if I is the ideal of S generated by $g_1, \dots, g_t$, then $\mathrm{in}(g_1), \dots, \mathrm{in}(g_t)$ generate $\mathrm{in}(I)$.[3]

Fix $d \in \mathbb{N}$. We wish to view a polynomial as a finite list of its coefficients, where we will ultimately be quantifying over all possible lists of those coefficients. To that end, we say that a polynomial $f \in S$ is *d-bounded* if it is a linear combination of the first d monomials. Throughout this section we identify the set S_d of d-bounded polynomials with the Cartesian product k^d: the polynomial $\sum_{i=1}^d \lambda_i \mathsf{m}_i$ corresponds to $(\lambda_1, \lambda_2, \dots, \lambda_d) \in k^d$. We say that an ordered list $\mathscr{B}$ of polynomials is *d-bounded* if $|\mathscr{B}| = d$ and $\mathscr{B}$ consists of of d-bounded polynomials. We identify the d-bounded lists $\mathscr{B}$ with $S_d^d = k^{d^2}$. Observe the following:

Remarks 3.2. (i) Any Gröbner basis consisting of d-bounded polynomials can be reduced to a d-bounded Gröbner basis. If there are at least $d+1$ elements then two, f and g say, must have the same leading monomial. So for some λ, $g - \lambda f$ has a lower leading monomial and replacing g by $g - \lambda f$ we still have a Gröbner basis, directly from Definition 3.1. Inductively we may assume g is zero, thus it can be removed to produce a smaller Gröbner basis.

(ii) Any finite set of polynomials (resp. Gröbner basis) can be embedded into a d-bounded set of polynomials (resp. Gröbner basis) for some d by appending an appropriate number of zeros.

(iii) A monomial ordering makes sense for $\mathcal{S} := R[x_1, \dots, x_n]$ where R is a ring. Hence, so do the concepts of a d-bounded polynomial $f \in \mathcal{S}$, and a d-bounded ordered list of polynomials in $\mathcal{S}^d$. If $(f_1, \dots, f_d)$ is d-bounded, generating an ideal I, and $\omega : R \to k$ is a homomorphism, then $I \otimes_R k$ is generated by the d-bounded list $(\omega(f_1), \dots, \omega(f_d))$.

Lemma 3.3. *Let $d \in \mathbb{N}$ and let $1 \leqslant e \leqslant d$. Then there is a first order formula $\phi_{e,d}$ in the language $\mathcal{L}_{\mathrm{ring}}$ of rings with d free variables such that for any d-bounded polynomial $f \in S$,*

$$\phi_{e,d}(f) \text{ holds } \iff \mathrm{in}(f) = \mathsf{m}_e.$$

Proof. After identifying S^d with k^d and $f = \sum_{i=1}^d \lambda_i \mathsf{m}_i$ with $(\lambda_1, ..., \lambda_d)$ the required formula is

$$(\lambda_e \neq 0) \wedge (\lambda_{e+1} = 0) \wedge (\lambda_{e+2} = 0) \wedge (\lambda_d = 0). \qquad \square$$

Given a d-bounded list of polynomials, we need to check with a first order formula that it forms a Gröbner basis. For this, we appeal to Buchberger's criterion [Eis95, Theorem 15.8], which we reproduce here.

[3] In contrast to [BW93], but consistently with [Eis95] we do not insist that the elements of a Gröbner basis are all non-zero.

Let $\mathscr{B} = (g_1, ..., g_d) \in S^d$. For each pair of indices $1 \leqslant i, j \leqslant d$, we define

$$m_{ij} = \mathrm{in}(g_i)/\gcd(\mathrm{in}(g_i), \mathrm{in}(g_j)) \in S.$$

Then it follows from the division algorithm, [Eis95, Prop. 15.6] that

$$m_{ji}g_i - m_{ij}g_j = \left(\sum f_u^{(ij)} g_u\right) + h_{ij} \tag{3.1}$$

for some $f_u^{(ij)} \in S$ with $\mathrm{in}(m_{ji}g_i - m_{ij}g_j) \geqslant \mathrm{in}(f_u^{(ij)} g_u)$ for each $1 \leqslant u \leqslant d$, and remainders h_{ij}, none of whose monomials is in $(\mathrm{in}(g_1), \ldots, \mathrm{in}(g_d))$. Set also $h_{ij} = 0$ if there does not exist an x_k upon which both m_{ij} and m_{ji} depend.

Theorem 3.4 (Buchberger's Criterion)**.** *The set $\mathscr{B}$ is a Gröbner basis if and only if $h_{ij} = 0$ for all i and j.*

Lemma 3.5. *Let $d \in \mathbb{N}$. Then there is a first order formula β_d in the language of rings with d^2 free variables such that if $\mathscr{B}$ is d-bounded list of elements of S, then*

$$\beta_d(\mathscr{B}) \text{ holds} \iff \mathscr{B} \text{ is a Gröbner basis.}$$

Proof. Suppose $\mathscr{B} = (g_1, \ldots, g_d) \in S_d^d$. We will produce a first order formula which calculates the expressions in (3.1) for each pair (g_i, g_j). Suppose $\mathrm{in}(g_i) = \mathsf{m}_a$ and $\mathrm{in}(g_j) = \mathsf{m}_b$ and that there is a formula $\chi_{a,b}$ such that $\chi_{a,b}(g_i, g_j)$ is true when the relevant $h_{ij} = 0$ in Buchberger's criterion. Then using Lemma 3.3 we set $\beta_d(\mathscr{B})$ to be the formula

$$\bigwedge_{1,\leqslant i,j\leqslant d} \left(\bigvee_{1\leqslant a,b\leqslant d} (\chi_{a,b}(g_i, g_j) \wedge \phi_{a,d}(g_i) \wedge \phi_{b,d}(g_j)) \right),$$

and we see that $\beta_d(\mathscr{B})$ is true whenever $\mathscr{B}$ satisfies the hypotheses of Buchberger's Criterion.

Thus we have reduced the problem, without loss of generality, to showing the existence of $\chi_{a,b}(g_1, g_2)$. For fixed a and b, $\mathsf{m}_{e'} := \gcd(\mathsf{m}_a, \mathsf{m}_b)$ is also fixed, depending just on the bijection between $\mathbb{N}$ and the monomials in S, hence, so are the monomials $m_{1,2}$ and $m_{2,1}$. Now, the highest monomial appearing in the left-hand side of (*) is at most that d'th monomial where $\mathsf{m}_{d'+1} = (\mathsf{m}_a\mathsf{m}_b/\mathsf{m}_{e'})$. Suppose $\mathrm{in}(m_{ji}g_i - m_{ij}g_j) = \mathsf{m}_e$. Then there is a finite set of pairs $P = \{(g_{a_b}, \mathsf{m}_{a_b})\}_{1\leqslant b\leqslant p}$ such that $\mathrm{in}(g_{a_b}\mathsf{m}_{a_b}) \leqslant \mathsf{m}_e$. Hence, setting $\chi_{e,a,b}(g_1, g_2)$ to be the formula

$$(\exists\lambda_1)\ldots(\exists\lambda_p)(m_{21}g_1 - m_{12}g_2 - \sum_{1\leqslant b\leqslant p} \lambda_b g_{a_b}\mathsf{m}_{a_b} = 0),$$

we see that $\chi_{e,a,b}(g_1, g_2)$ holds whenever Buchberger's criterion holds for g_1 and g_2 (given $\mathrm{in}(m_{ji}g_i - m_{ij}g_j) = \mathsf{m}_e$). Lastly, let $\chi_{a,b}(g_1, g_2)$ be the formula

$$\bigvee_{e=1}^{d'} (\phi_{e,d}(m_{21}g_1 - m_{12}g_2) \wedge \chi_{e,a,b}(g_1, g_2)).$$ □

Another important thing we need to be able to encode with a first order statement is the dimension $\dim(I) = \dim(\mathrm{Spec}_k(S/I))$ of the scheme determined by an ideal $I \subseteq S = k[x_1, ..., x_n]$. If $I = (g_1, ..., g_d)$ then in general it is not easy to read off $\dim I$ from the elements $\{g_1, ..., g_d\}$; however, when $\{g_1, ..., g_d\}$ form a Gröbner basis for I there is a simple method: the dimension is the maximal size of a subset $X \subseteq \{x_1, ..., x_n\}$ such that $\mathrm{in}(g_1), ..., \mathrm{in}(g_n)$ depend only on the elements of $\{x_1, ..., x_n\}\backslash X$ [BW93, Defn. 9.22 & Cor. 9.28]. Using this fact along with Lemma 3.3, we can determine dimension with a first order formula.

Lemma 3.6. *Let $d \in \mathbb{N}$ and $0 \leqslant e \leqslant d$. Then there is a first order formula $\delta_{e,d}$ in the language $\mathcal{L}_{\mathrm{ring}}$ of rings, with d^2 free variables, such that if $\mathscr{B}$ is any d-bounded Gröbner basis with $I = (\mathscr{B})$, then*

$$\delta_{e,d}(\mathscr{B}) \text{ holds} \iff \dim(I) = e.$$

Proof. There is obviously a finite collection of lists of monomials which could play the role of initial terms of the elements of a d-bounded Gröbner basis which define an ideal of dimension e. More formally, there is a finite set $\mathcal{X}_e = \{X_j\}$ where X_j is a d-bounded list of monomials in S satisfying (i) $|X_j| = d$; (ii) there is some $\{i_1, \dots, i_e\}$ such that each $m \in X_j$ does not involve $x_{i_1}, \dots, x_{i_e}$; (iii) for any $\{i_1, \dots, i_{e+1}\}$, there is $m \in X_j$ depending on x_{i_k} for some $1 \leqslant k \leqslant e+1$. For convenience we assume that the X_j are ordered sets and identify the monomials with their ordinal via the bijection of monomials of S with $\mathbb{N}$. Then we may set $\delta_{e,d}(\mathscr{B})$ to be the formula

$$\bigvee_{X_j=(a_1,\dots,a_d)\in\mathcal{X}_e} \phi_{a_1,d}(g_1) \wedge \phi_{a_2,d}(g_2) \wedge \cdots \wedge \phi_{a_d,d}(g_d). \qquad \square$$

The next lemma uses the ideal membership algorithm for Gröbner bases to write a first order formula whose truth determines whether an element is in an ideal. If $\mathscr{B}$ is a d-bounded Gröbner basis and $f \in S_d$ then we may identify $(\mathscr{B}, f)$ with an element of k^{d^2+d} in the usual manner.

Lemma 3.7. *Let $d \in \mathbb{N}$. Then there is a first-order formula ι_d in $\mathcal{L}_{\mathrm{ring}}$ with $d^2 + d$ free variables, so that for any d-bounded polynomial $f \in S$ and d-bounded Gröbner basis $\mathscr{B}$ with $I := (\mathscr{B})$, then*

$$\iota_d(\mathscr{B}, f) \text{ holds} \iff f \in I.$$

Proof. Since the highest monomial amongst those occuring in f and the elements of $\mathscr{B}$ has bounded degree d' say, then since $<$ is a homogeneous order, there is only a finite number of monomials m such that $\mathrm{in}(mg) \leqslant \mathrm{in}(f)$ for some $g \in f$, where this number depends only on d. Let $\mathsf{m}_{d''}$ be the highest such. Thus we set $\iota_d(\mathscr{B}, f)$ to be the formula

$$(\exists \lambda_{i,j})_{1\leqslant i\leqslant d'', 1\leqslant j\leqslant d} f = g_1(\sum_{i=0}^{d''} \lambda_{i,1}\mathsf{m}_i) + g_2(\sum_{i=0}^{d''} \lambda_{i,2}\mathsf{m}_i) + \cdots + g_d(\sum_{i=0}^{d''} \lambda_{i,d}\mathsf{m}_i). \qquad (\dagger)$$

We claim that $\iota_d(\mathscr{B}, f)$ is true if and only if $f \in I$. This follows by induction on e where $\mathrm{in}(f) = \mathsf{m}_e$: Since $\mathscr{B}$ is a Gröbner basis, by [BW93, 5.35(vii)], f is *top-reducible* by some g_i or is not in I. In the former case, this means that there is a monomial m such that $\mathrm{in}(f - g_i m) < \mathrm{in}(f)$. By the inductive hypothesis, $\iota_d(\mathscr{B}, f - g_i m)$ is true whenever $f - g_i m \in I \iff f \in I$. If $f - g_i m \in I$ this says that there is an expression of the form (†) with f replaced by $f - g_i m$; moving $g_i m$ to the other side of the equation, this says that there is also one for f. $\square$

In the next lemma we consider certain types of homomorphisms $S \to S^{\otimes r}$. Observe that $S^{\otimes r} \cong k[x_{1,1}, \dots, x_{1,n}, \dots, x_{r,1}, \dots, x_{r,n}]$ and place the homogeneous lexicographic monomial order on $S^{\otimes r}$. The monomial order on S induces monomial orders on $1^{\otimes i} \otimes S \otimes 1^{\otimes r-i+1}$ for $i = 1, ..., r$ which are simultaneously refined by our choice of monomial order on $S^{\otimes r}$. We say that an algebra homomorphism $\Lambda : S \to S^{\otimes r}$ is *d-bounded* if $\Lambda(x_1), ..., \Lambda(x_n) \in S_d^{\otimes r}$, and we write $\mathrm{Hom}_{k-\mathrm{alg}}(S, S^{\otimes r})_d$ for the set of d-bounded algebra homomorphisms. Since every d-bounded homomorphism Λ satisfies $\Lambda(x_i) = \sum_{j_1,\dots,j_r=1}^{d} \lambda_{i,j_1,\dots,j_r} \mathsf{m}_{j_1} \otimes \cdots \otimes \mathsf{m}_{j_r}$ for elements $(\lambda_{i,j_1,\dots,j_r})_{1\leqslant i\leqslant n, 1\leqslant j_k\leqslant r}$ of k, and since the elements $\Lambda(x_1), ..., \Lambda(x_n)$ determine Λ uniquely, we may identify $\mathrm{Hom}_{k-\mathrm{alg}}(S, S^{\otimes r})_d$ with the set k^{nd^r}. Note also that if $r = 0$ then every homomorphism is d-bounded for any $d \in \mathbb{N}$.

Now if $I = (\mathscr{B}) \subseteq S$ is an ideal generated by a d-bounded list $\mathscr{B} = \{f_1, \dots, f_d\}$ of elements of S, then we have an isomorphism

$$\varphi_r : (S/I)^{\otimes r} \to k[x_{1,1}, \dots, x_{1,n}, \dots, x_{r,1}, \dots, x_{r,n}]/J_r, \qquad (3.2)$$

where the ideal J_r is generated by the f_i's taking values in each set $\{x_{j,1}, \ldots, x_{j,n}\}$. More formally, write $f_i = f_i(x_1, \ldots, x_n)$; then $J_r = (\mathscr{B}_r)$ where $\mathscr{B}_r = \{f_{1,1}, \ldots, f_{1,d}, \ldots, f_{r,1}, \ldots, f_{r,d}\}$ and $f_{i,j} = f_i(x_{j,1}, \ldots, x_{j,n})$.

Lemma 3.8. *Let $d, r \in \mathbb{N}$. Then there is a first order formula $\zeta_{d,r}$ in $\mathcal{L}_{\text{ring}}$ with $nd^r + d^2$ free variables such that if $\Lambda : S \to S^{\otimes r}$ is any d-bounded homomomorphism and $\mathscr{B} = \{f_1, \ldots, f_d\}$ is any d-bounded Gröbner basis, with $I := (\mathscr{B})$, then*

$$\zeta_{d,r}(\mathscr{B}, \Lambda) \text{ holds} \iff \Lambda \text{ factors to a homomorphism } S/I \to (S/I)^{\otimes r}.$$

Proof. We claim that $\mathscr{B}_r$ as above is a Gröbner basis for the homogeneous lexicographic monomial order on the monomials in $x_{i,j}$. Since this order extends the monomial orders on the subalgebras $k[x_{i,1}, ..., x_{i,n}]$ for any fixed i we see that Buchburger's criterion (Theorem 3.4) holds for all pairs $(f_{i,j}, f_{i,k})$; furthermore if $i \neq i'$ then $\gcd(\text{in}(f_{i,j}), \text{in}(f_{i,k})) = 1$, so the m_{ij} and m_{ji} in (3.1) admit no common divisor amongst the variables $\{x_{i,j}\}$, and therefore the h_{ij} are zero by assumption.

Under φ_r, expressions $\mathsf{m}_{j_1} \otimes \cdots \otimes \mathsf{m}_{j_r}$ are mapped to monomials in the $x_{i,j}$ where the kth tensor factor is evaluated in indeterminates $x_{k,1}, \ldots x_{k,n}$ and the tensor products replaced by multiplication. Choose $d_r = d_r(d)$ sufficiently large so that for any choice of d-bounded homomorphism Λ and d-bounded Gröbner basis $\mathscr{B}$, we have that the elements of $\mathscr{B}_r$ and $\Lambda(x_i)$ are all contained in the span of the first d_r monomials of $S^{\otimes r}$. We can extend the basis $\mathscr{B}_r$, adding zeroes to the list, to get a d_r-bounded Gröbner basis, which we also denote $\mathscr{B}_r$. Now we may appeal to Lemma 3.7 to get first order formulas ι_{d_r} such that $\iota_{d_r}(\mathscr{B}_r, \varphi_r(\Lambda(x_i)))$ holds whenever $\varphi_r(\Lambda(x_i)) \in J_r$. Hence we set $\zeta_{d,r}$ to be the formula

$$\bigwedge_{i=1}^{n} \iota_{d_r}(\mathscr{B}_r, \varphi_r(\Lambda(x_i))) \qquad \square$$

3.2. **Bounded Hopf quadruples.** Recall the Hopf algebra axioms (2.1–2.3)

Lemma 3.9. *Let $d \in \mathbb{N}$. There is a formula $\eta_d \in \mathcal{L}_{\text{ring}}$ with $d^2 + n(d^2 + d + 1)$ free variables such that if $\mathscr{B}$ is any d-bounded Gröbner basis, with $I = (\mathscr{B})$ and $\Delta : S \to S^{\otimes 2}$, $\sigma : S \to S$ and $\epsilon : S \to k$ any d-bounded homomorphisms, then*

$$\eta_d(\mathscr{B}, \Delta, \sigma, \epsilon) \text{ holds} \iff (S/I, \Delta, \sigma, \epsilon) \text{ is a Hopf algebra.}$$

Proof. Suppose Δ, σ and ϵ factor as $S/I \to S/I^{\otimes r}$. We must find formulas $\eta_d^{(1)}$, (resp. $\eta_d^{(2)}, \eta_d^{(3)}$) which hold if and only if (2.1), (resp. (2.2), (2.3)) are satisfied. Since the constructions are almost identical for each formula, we give the details for $\eta_d^{(1)}$. To see that (2.1) holds, it clearly suffices to check that $(\Delta \otimes \text{id}) \circ \Delta(x_i + I) - (\text{id} \otimes \Delta) \circ \Delta(x_i + I) = 0 \in (S/I)^{\otimes 3} \cong S^{\otimes 3}/J_3$ for each $1 \leqslant i \leqslant n$, where $J_3 = (\mathscr{B}_3)$ is as in (3.2). This amounts to checking that $(\Delta \otimes \text{id}) \circ \Delta(x_i) - (\text{id} \otimes \Delta) \circ \Delta(x_i) \in J$. By the same argument as used in the previous proof, since Δ is d-bounded, $\varphi_2(\Delta(x_i))$ is a d'-bounded polynomial in $S^{\otimes 2}$ for some $d' = d'(d)$; similarly $f_i := \varphi_3((\Delta \otimes \text{id}) \circ (\Delta(x_i)))$ is a d''-bounded polynomial in $S^{\otimes 3}$ for some $d'' = d''(d)$. As in the previous proof we can also arrange that $\mathscr{B}_3$ is e-bounded for some $e \geqslant d''$. Thus we may set $\eta_d^{(1)}(\mathscr{B}, \Delta, \sigma, \epsilon)$ to be the formula

$$\bigwedge_{i=1}^{n} \iota_e(\mathscr{B}_3, f_i).$$

Finally, we set $\eta_d(\mathscr{B}, \Delta, \sigma, \epsilon)$ to be the formula

$$\zeta_{d,2}(\Delta) \wedge \zeta_{d,1}(\sigma) \wedge \zeta_{d,0}(\epsilon) \wedge \eta_d^{(1)}(\mathscr{B}, \Delta, \sigma, \epsilon) \wedge \eta_d^{(2)}(\mathscr{B}, \Delta, \sigma, \epsilon) \wedge \eta_d^{(3)}(\mathscr{B}, \Delta, \sigma, \epsilon). \qquad \square$$

For a quadruple $H := (\mathscr{B}, \Delta, \sigma, \epsilon)$ as in Lemma 3.9 satisfying $\eta_d(H)$, we call H a *d-bounded Hopf quadruple*. If $I = (f_1, \ldots, f_d)$ and $(S/I, \Delta, \sigma, \epsilon)$ is a Hopf algebra, then there is a corresponding

affine algebraic group $G = (\mathrm{Spec}(S/I), \Delta^*, \sigma^*, \epsilon^*)$, [Jan03, I.2.3] and we say that the Hopf quadruple H *describes* the k-group G. As a k-vector space, the Lie algebra $\mathrm{Lie}(G)$ is the tangent space $T_e(G)$, where $e = \epsilon^*$ is the identity point of G. Thus its dimension is the nullity of the $d \times n$ matrix $\mathscr{J}$ where $\mathscr{J}_{kl} = \epsilon(\partial f_k/\partial x_l)$.

Lemma 3.10. *Let $d \in \mathbb{N}$, and $0 \leqslant e \leqslant d$. There is a first order formula $\tau_{e,d}$ in $\mathcal{L}_{\mathrm{ring}}$ with d^2 free variables such that for any d-bounded Hopf quadruple $(\mathscr{B}, \Delta, \sigma, \epsilon)$ defining the affine algebraic k-group scheme G we have*

$$\tau_{e,d}(\mathscr{B}) \text{ holds} \iff \dim \mathrm{Lie}(G) = e.$$

Proof. As we identify each f_i with its d coefficients λ_{ij}, partial differentiation by $\partial/\partial x_i$ gives a map $k^d \to k^d$. Composing with ϵ is then a map $k^d \to k$. Hence each $\mathscr{J}_{kl}$ is a fixed linear combination of the λ_{ij}'s. The statement that the nullity of $\mathscr{J}$ is e is equivalent to the statement that there are e linearly independent vectors $v_1, \ldots, v_e \in k^d$ satisfying $J \cdot v_i = 0$ and any $e+1$ linearly independent set of $v_1, \ldots, v_{e+1} \in k^d$ contains v_j such that $J \cdot v_j \neq 0$. This statement can be given as a formula in $\mathcal{L}_{\mathrm{ring}}$ in an obvious way. □

3.3. **Generic smoothness of bounded group schemes.** We put together the results of the previous sections with the Lefschetz principle to show that bounded group schemes are generically smooth. We use the fact that a group scheme G is smooth if and only if $\dim(G) = \dim(\mathrm{Lie}(G))$, [Jan03, I.7.17].

Lemma 3.11. *Let $d \in \mathbb{N}$. Then there is a first order formula θ_d with d^2 free variables such that for any d-bounded Hopf quadruple $H := (\mathscr{B}, \Delta, \sigma, \epsilon)$,*

$$\theta_d(\mathscr{B}) \text{ holds} \iff H \text{ describes a smooth } k\text{-group.}$$

Proof. The k-group G described by H is a subscheme of $\mathrm{Spec}(S) \cong \mathbb{A}^n$, so $0 \leqslant \dim G \leqslant n$. Then invoking Lemmas 3.10 and 3.6 we may set $\theta_d(\mathscr{B}, \Delta, \sigma, \epsilon)$ to be the following formula:

$$\bigvee_{e=0}^{n} \left(\delta_{e,d}(\mathscr{B}) \wedge \tau_{e,d}(\mathscr{B})\right). \qquad \square$$

Theorem 3.12. *Let $d \in \mathbb{N}$. Then there is a prime $p_0 = p_0(d)$ such that whenever* $\mathrm{char} k \geqslant p_0$, *any d-bounded Hopf quadruple, $(\mathscr{B}, \Delta, \sigma, \epsilon)$, describes a smooth group scheme G.*

Proof. Recall we identify $(\mathscr{B}, \Delta, \sigma, \epsilon)$ with a string of $d^2 + n(d^2 + 2d + 1)$ coefficients in the field, which we write $(\lambda_i)_{i=1}^{d^2+n(d^2+2d+1)}$. Then invoking Lemmas 3.5, 3.9 and 3.11, the following formula Φ_d is a *sentence* in $\mathcal{L}_{\mathrm{ring}}$, which is true if and only if all d-bounded Hopf quadruples describe smooth group schemes:

$$(\forall \lambda_1) \cdots (\forall \lambda_{d^2+n(d^2+2d+1)})(\beta_d(\mathscr{B}) \wedge \eta_d(\mathscr{B}, \Delta, \sigma, \epsilon) \wedge \theta_d(\mathscr{B})).$$

By [Jan03, I.7.17(2)], Φ is true for all (algebraically closed) fields of characteristic 0. Therefore the Lefschetz principle (Corollary 2.3) guarantees a prime p_0 so that the same is true for all algebraically closed fields of characteristic $p \geqslant p_0$. But smoothness is a geometric property, meaning that a k-group G is smooth if and only if $G_{\bar{k}}$ is smooth. The theorem follows. □

3.4. **Primary decomposition and algebraic groups.** Recall that for a ring R, an ideal I is *primary* if $ab \in I \Rightarrow a \in I$ or $b^r \in I$ for some integer r. If I is primary, it follows that the radical $\sqrt{I}$ of I is prime, called its *associated prime*. For R a Noetherian ring, there is [Eis95, Thm. 3.10] a *primary decomposition* of any ideal I as an intersection $I_1 \cap \cdots \cap I_n$ of primary ideals which is *irredundant*, in the sense that $I \neq I_1 \cap \cdots \cap \widehat{I_j} \cap \cdots \cap I_n$ where we delete the jth term of the intersection. We say a primary ideal I_j appearing in a primary decomposition is *isolated* if $\sqrt{I_j}$ does not properly contain $\sqrt{I_k}$ for any $k \neq j$ and is *embedded* otherwise.

Remark 3.13. Let G be an affine algebraic group over a field k with $k[G] \cong k[t_1, \ldots, t_n]/I$. Then of course G is a disjoint union of its irreducible components $G = G^\circ \sqcup G_1 \sqcup \cdots \sqcup G_r$.[4] Thus

$$k[G] \cong k[G^\circ] \times k[G_1] \times \cdots \times k[G_r]$$

with $k[G_i] = I_i$; as each G_i is irreducible, we have I_i primary. Since $I_i + I_j = 1$ for $i \neq j$ we have $I_i \cdot I_j = I_i \cap I_j$ and $I = I_0 \cap \cdots \cap I_r$. Clearly this is an irredundant intersection thus a primary decomposition of I. The disjunction of G_i implies that each I_i is isolated. In this case, the primary decomposition of I is therefore unique by [BW93, Thm. 8.56] and so any primary decomposition computes the connected components of G.

3.5. **Bounded primary decompositions.** The purpose of this section is to take the reader through algorithms of [BW93, §8] and [GTZ88] which calculate primary decompositions of ideals, where we progressively emphasise the existence of bounds on the degrees of any output monomial which are independent of k.

Several times we will need to use the following important theorem of Dubé.

Theorem 3.14 ([Dub90])**.** *Let $I = (f_1, \ldots, f_r) \subseteq S$ be an ideal generated by polynomials whose maximal degree is d. Then for any admissible monomial ordering there is a Gröbner basis generated by polynomials whose terms have degree at most $2(\frac{d^2}{2} + d)^{2^{n-1}} \leqslant 2d^{2^n}$.*

To calculate closures, radical ideals and ultimately primary decomposition we must appeal to elimination. If $I \subseteq S = k[x_1, \ldots, x_n]$ is an ideal then for any $r \leqslant n$, $I \cap k[x_1, \ldots, x_r]$ is an ideal. This ideal can be computed easily from a Gröbner basis $\mathscr{B}$ of I provided we choose a monomial ordering so that the monomials in $k[x_1, \ldots, x_r]$ are all less than the monomials in $S \backslash k[x_1, \ldots, x_r]$. For then, by [Eis95, Prop. 15.29], we have that $I \cap k[x_1, \ldots, x_r]$ has a Gröbner basis $\mathscr{B} \cap k[x_1, \ldots, x_r]$. To this end, a suitable monomial ordering is supplied by the lexicographic ordering.

Lemma 3.15. *Let $d \in \mathbb{N}$. Then there is an integer $e = e(d)$ such that for any d-bounded list of polynomials $B \subset S$, there is an e-bounded Gröbner basis $\mathscr{B}$ of the ideal $(B) \cap k[x_1, \ldots, x_r]$ for any $r \leqslant n$.*

Proof. The lexicographic order is admissible, so Theorem 3.14 gives a bound on the degrees of the monomials in a Gröbner basis $\mathscr{B}$ of the set B having monomials of a bounded degree depending only on d. □

Note that elimination in the case $r = 1$ produces an ideal of the principal ideal domain $k[x_1]$ which has a unique monic generator f, say. We will need the following corollary of Theorem 1.5 of the celebrated paper [Kol88].

Lemma 3.16. *For any $d \in \mathbb{N}$, there is $e = e(d) \in \mathbb{N}$ such that whenever I is generated by a d-bounded list of polynomials of $K[x_1, \ldots, x_n]$ then $f \in \sqrt{I} \Rightarrow f^e \in I$.*

[4] If G is smooth then its k_s points are dense and we therefore see that the G_i are cosets of $G_0 := G^\circ$, but perhaps this need not be true if G is not smooth?

We now turn to [GTZ88, Prop. 6.1] which explains how to calculate a primary decomposition inductively from a zero-dimensional ideal in a polynomial ring over a commutative ring. We will only need to consider the case where the coefficient ring is the field of fractions of a polynomial ring over a field. Let $R = k[t_1, \ldots, t_m]$, $K = k(t_1, \ldots, t_m)$, $\mathscr{S} = k[t_1, \ldots, t_m, x_1, \ldots, x_n] = S \otimes_k K$ and $\mathcal{S} = K[x_1, \ldots, x_n] = S \otimes_k K = \mathscr{S} \otimes_R K$. Note that the image of an ideal $J \subset \mathscr{S}$ in $\mathcal{S}$ is canonically isomorphic to $J \otimes_R K$.

Lemma 3.17. *Let $d \in \mathbb{N}$. Then there is an integer $e = e(d)$ such that whenever $J \subsetneq \mathscr{S}$ is an ideal of $\mathscr{S}$ generated by a d-bounded list of polynomials, and $J \otimes_R K$ is zero-dimensional in $\mathcal{S}$, there is a list of ideals $J_1, \ldots, J_u \subseteq \mathscr{S}$, each generated by an e-bounded list of polynomials, such that $J \otimes_R K = \bigcap (J_i \otimes_R K)$ is a primary decomposition of $J \otimes_R K$.*

Proof. We exhibit e inductively on r, by taking intersections with $\mathcal{S}' := K[x_1, \ldots, x_r]$. Let also $\mathscr{S}' := k[t_1, \ldots, t_m, x_1, \ldots, x_r]$. We start with $r = 0$, so that $\mathcal{S}' = K$, and note that $(J \otimes_R K) \cap \mathcal{S}' = 0$ since J is proper; observe that $M = 0$ is then a maximal ideal of $\mathcal{S}'$ such that $(J \otimes_R K) \cap \mathcal{S}'$ is M-primary. For the inductive step, assume we are given an ideal $I \subseteq \mathscr{S}$ generated by a d_r-bounded list of polynomials and a maximal ideal M of $\mathcal{S}'$ such that $(I \otimes_R K) \cap \mathcal{S}'$ is M-primary.

Claim: *there is $d_{r+1} = d_{r+1}(d_r)$ and a list $I_1 \ldots I_{u'}$ of ideals of $\mathscr{S}$, each generated by an d_{r+1}-bounded list of polynomials, together with distinct maximal ideals $M_1, \ldots, M_{u'} \subset \mathcal{S}'[x_{r+1}]$ such that $I \otimes_R K$ is the intersection of the $I_i \otimes_R K$ and $(I_i \otimes_R K) \cap \mathcal{S}'[x_{r+1}]$ is both zero-dimensional and M_i-primary.*

Let $I^c = I \cap \mathscr{S}'[x_{r+1}]$. By taking a Gröbner basis of $I \subset \mathscr{S}$ according to an admissible monomial order in which terms in the variables $x_1, \ldots, x_{r+1}$ are less than any other, we have, by Lemma 3.15, that I^c is generated by an $e' = e'(d_r)$-bounded Gröbner basis $\mathscr{B}$ in those variables. Evidently $\mathscr{B} \otimes_R K$ is a (not necessarily reduced) Gröbner basis for the zero-dimensional ideal $I^c \otimes_R K \subset \mathcal{S}'[x_{r+1}]$, thus by [GTZ88, Lemma 5.5] we can find $g \in \mathscr{B}$ such that its leading term in $\mathscr{S}'[x_{r+1}]$ is $\alpha \cdot x_{r+1}^q$ and α is a unit modulo $(I^c \otimes_R K) \cap \mathcal{S}' = (I \otimes_R K) \cap \mathcal{S}'$; e'-boundedness implies $q \leqslant e'$. Now it follows from [GTZ88, Lemma 5.7] that $\sqrt{I^c \otimes_R K} = \sqrt{g, (I \otimes_R K) \cap \mathcal{S}'} = \sqrt{g, M}$. Since for some field $F \supset K$, $(\mathcal{S}'/M)[x_{r+1}] \cong F[x_{r+1}]$ is a principal ideal domain, we may take a factorisation

$$g(x_{r+1}) \otimes 1 = \prod p_i(x_{r+1})^{s_i} \in \mathcal{S}'[x_{r+1}] \tag{3.3}$$

such that the images in $F[x_{r+1}]$ the $p_i(x_{r+1})$ are all pairwise comaximal irreducible non-units. Moreover, as $\mathscr{S}'$ is a gcd domain, by Gauss's lemma we may assume $p_i(x_{r+1})$ is each in $\mathscr{S}'[x_{r+1}]$, so that $g(x_{r+1}) = \prod p_i(x_{r+1})^{s_i}$ is a factorisation in $\mathscr{S}'[x_{r+1}]$. Since $\prod p_i^{s_i} \otimes 1 \in (g \otimes 1, M) \subset \sqrt{I^c \otimes_R K}$, we have, by Lemma 3.16 an $s = s(e')$ such that $(\prod p_i^{s_i})^s \otimes 1 \in I^c \otimes_R K$.

Now since $p_i \otimes 1$ and $p_j \otimes 1$ are coprime inside $\mathcal{S}'[x_{r+1}]$, we have

$$\bigcap_i (p_i^{s_i s} \otimes 1, I \otimes_R K) = (\prod p_i^{s_i s} \otimes 1, I \otimes_R K) = (g \otimes 1, I \otimes_R K) = I \otimes_R K.$$

Let $I_i = (I, p_i^{s_i s})$; then the intersection $(I_i \otimes_R K) \cap \mathcal{S}'[x_{r+1}]$ contains a power of the maximal proper ideal $M_i = (p_i, M) \subseteq \mathcal{S}'[x_{r+1}]$. Provided $I_i \otimes_R K$ is proper, we will have $I_i \otimes_R K \cap \mathcal{S}'[x_{r+1}]$ being M_i-primary. However if $I_i \otimes_R K = (1)$ then $\prod_{j \neq i} p_j \in I^c \otimes_R K = \sqrt{(g \otimes 1, M)}$, which is a contradiction of the fact that p_i is not a unit. Clearly the given set of generators of I_i is d_{r+1}-bounded for some d_{r+1} depending on s, s_i, e', e_r. Since each of these can be bounded just in terms of d_r we are done and the claim is proved.

To finish off, we set $e = d_n$. The ideals in the primary decomposition are computed recursively by the above process; see the algorithm in [GTZ88] for more details. Note that the irredundancy follows by the evident distinctness of the maximal ideals M_i produced at each stage. □

Question 3.18. In Lemma 3.17, can one also bound the integer u in terms of d?

For zero-dimensional ideals $I \subset S$, Lemma 3.17 gives a bound for a list of generators of a primary decomposition, if a bound is known for the generators of the ideal—just take $m = 0$, so that $R = K = k$. The next lemma uses [BW93] to reduce the general case to the zero-dimensional one. Suppose $I \subset S$ is of arbitrary dimension. Without loss of generality, we may assume $0 \leqslant r \leqslant n$ is such that $x_{r+1}, \ldots, x_n$ are a maximally independent set of variables with respect to I. (So $\dim(I) = n - r$.) We will apply Lemma 3.17 in the case $R = k[x_{r+1}, \ldots, x_n]$, $K = k(x_{r+1}, \ldots, x_n)$, $\mathscr{S} = R[x_1, \ldots, x_r] \cong S$ and $\mathcal{S} = K[x_1, \ldots, x_r]$; we have $I \otimes_R K \subset \mathcal{S}$ is evidently zero-dimensional.

The following result is [BW93, Lem. 8.97(iii)], and explains how one can recover a primary decomposition and radical of I from that of I^e.

Lemma 3.19. *Let R be a ring and M a multiplicative subset of R. Let J^c denote the intersection of an ideal $J \subseteq R_M$ with R. Then J^c is a primary ideal of R.*

Let us set up some notation. For a ring R, $f \in R$ and $I \subset R$ an ideal, let $(I : f) = \{g \in R \mid g \cdot f \in I\}$. Then $(I : f^i) \subseteq (I : f^{i+1})$; denote the union by $(I : f^\infty)$.

Recall the notation just before the above lemma. If $J \subset \mathscr{S}$ then the contraction $J^c := \mathscr{S} \cap (J \otimes_R K)$ can be computed from the highest coefficents of a Gröbner basis $\mathscr{B}$ of J in a monomial order in which the terms in variables $x_1, \ldots, x_r$ are lower than any other. More specifically, define

$$f := \operatorname{lcm}\{HC(g) \mid g \in \mathscr{B}\},$$

where $HC(g)$ is a polynomial in $x_{r+1}, \ldots, x_n$. Then by [BW93, Lem. 8.91] we have $J^c = (J : f^\infty)$. As S is Noetherian, there must be s such that $(J : f^\infty) = (J : f^s)$

Lemma 3.20. *Let $d \in \mathbb{N}$. Then there is $s = s(d)$ such that whenever $I \subset S$ is an ideal generated by a d-bounded set of polynomials, and f is a d-bounded polynomial, then $(I : f^s) = (I : f^\infty)$.*

Proof. By [BW93, Prop. 6.37], $(I : f^\infty)$ is the ideal $J := (I, 1 - yf) \cap S[y]$, which can be generated by an $e = e(d)$-bounded list of polynomials using Lemma 3.15. Moreover, if $\{f_1, \ldots, f_k\}$ is a basis of I and $\{g_1, \ldots, g_m\}$ is a basis of J with

$$g_i = h_i(1 - yf) + \sum_{j=1}^{k} h_{ij} f_j$$

then *loc. cit.* gives

$$s = \max\{\deg_y(h_{ij}) \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant k\}.$$

Evidently the latter is bounded just in terms of d. □

Since $(J : f^\infty) = J^c = (J \otimes_R K) \cap S$, it is easy to see:

Corollary 3.21. *Let $d \in \mathbb{N}$. Then there is $e = e(d)$ such that if $J \subseteq \mathscr{S}$, the contraction J^c is generated by an e-bounded list of polynomials.*

We are ready to put this together. Take $I \subseteq S$, generated by a d-bounded list of polynomials. From Lemma 3.17 we can create a primary decomposition of $I \otimes_R K$, and by Lemma 3.19 this intersects with S to give one for I^c, say $I^c = \bigcap I_i$. By [BW93, Lem. 8.95, Prop. 8.96] it is possible to find $f \in k[x_{r+1}, \ldots, x_n]$ such that $I = (I + (f^s)) \cap I^{ec} = (I + (f^s)) \cap (I : f^s)$ where f and s are as predicated in Lemma 3.20 above. In particular, by Corollary 3.21 each term in the intersection is generated by a list of polynomials bounded just in terms of d. Necessarily, we have $I \subsetneqq I + (f^s)$ so by Noetherian induction, we may assume there is a primary decomposition of $I + (f^s)$. Indeed, as $I + f^s$ is e-bounded, by [Sei71, Theorem], the maximal length of a chain of ascending ideals starting at $I + (f^s)$ is bounded just in terms of e. Thus we may assume that a full primary decomposition of $I + f^s$ together with that of I^c is a collection of ideals which are generated by

lists of polynomials which are bounded just in terms of d. We have therefore proved the arbitrary dimensional analogue of Lemma 3.17.

Proposition 3.22. *Let $d \in \mathbb{N}$. Then there is $e = e(d)$ such that whenever $I \subset k[x_1, \dots, x_n]$ is an ideal generated by a d-bounded list of polynomials in the x_i, there is a list of ideals $I_1, \dots, I_u$, each generated by an e-bounded list of polynomials, such that $I = \bigcap I_i$ is a primary decomposition of I.*

3.6. **Bounded actions on schemes: end of the proof.** If G is an affine algebraic R-group with corresponding Hopf algebra $R[G] = R[x_1, \dots, x_n]/I_G$ with $I_G = (g_1, \dots, g_m)$ then let $X = \bigcup_{i \in \mathbb{I}} X_i$ be a finitely presented G-scheme (not necessarily of finite type) with action map $\alpha : G \times X \to X$ and fix isomorphisms $R[X_i] \cong k[t_1, \dots, t_{r_i}]/I_i$ with $I_i = (h_1, \dots, h_{s_j})$. Let $Y_{ij} := \alpha^{-1}(X_i) \cap (G \times X_j)$. Observe that Y_{ij} is an open subscheme of the open affine scheme $G \times X_j \subseteq G \times X$. In general Y_{ij} will not be affine, but by dominance, we have $R[G \times X_j] \cong R[G] \otimes R[X_j] \subseteq R[Y_{ij}]$; moreover, we have that Y_{ij} is a finite union $\bigcup_{k=1}^{a_{ij}} D_{ijk}$ of principal open subschemes $D_{ijk} = D_{ijk}(f_{ijk}) \subseteq G \times X_j$ for some $f_{ijk} \in R[G \times X_j]$, which we may assume to be irreducible over R. By standard results, D_{ijk} is an affine scheme with coordinate ring

$$\begin{aligned} R[D_{ijk}] &\cong R[G \times X_j] \otimes_R R[u]/(uf - 1) \\ &\cong R[u_1, \dots, u_n, t_1, \dots, t_{r_i}, u]/(g_1, \dots, g_m, h_1, \dots, h_{s_j}, uf - 1). \end{aligned}$$

Dominance of the inclusion map $D_{ijk} \to Y_{ij}$ gives us $R[Y_{ij}] \subseteq R[D_{ijk}]$ and so we get maps $\overline{\alpha_{ijk}} : R[X_i] \cong R[t_1, \dots, t_{r_i}]/I_i \to R[D_{ijk}]$.

Definition 3.23. For an integer d, we say that α is *a d-bounded action map* if for all i, j, k, l, we have $\overline{\alpha_{ijk}}(t_l)$ is a d-bounded polynomial in the x_m's after considering all other generators of $R[D_{ijk}]$ as constants.

Now let $R = k$. The goal is now to prove the following.

Proposition 3.24. *Let d, e be integers. Then for any d-bounded Hopf quadruple $(\mathscr{B}, \Delta, \sigma, \epsilon)$ describing a k-group G, a d-bounded action map $\alpha : G \times X \to X$ where X is a finitely presented k-scheme, and any subset $N \subseteq X(k)$, there is an e-bounded Hopf quadruple $(\mathscr{B}', \Delta, \sigma, \epsilon)$ describing $C_G(N)$, for some e depending just on d.*

Proof. For any $v \in N$, we may find $X_1(k)$, say, containing v. Then $\alpha^{-1}(X_1) \cap (G \times X_1)$ contains all $(g, v \otimes 1) \in G(A) \times X(A)$ such that $g \cdot (v \otimes 1) = v \otimes 1$; in particular, the projection of $Y_{11} \cap (G \times \{v\})$ to G contains $C_G(v)$. Now choose $f = f_{111} \in k[G \times X_1]$ such that $D_{111} = D(f)$, say, is a principal open subscheme with $(e, v) \in D_{111}$. Setting π to be projection to the first factor, we have $D := \pi(D_{111} \cap (C_G(v) \times \{v\}))$ is an open subset of $C_G(v)$ containing the identity point and so the closure $\overline{D}$ is a disjoint union of $C_G(v)^\circ$ and a closed set contained in the complement of $C_G(v)^\circ$ in $C_G(v)$. Let $g \in G(A)$. Then the condition $g \cdot (v \otimes 1) = v \otimes 1$ translates under $\overline{\alpha_{111}}$ to

$$(\forall l)\ \overline{\alpha_{111}}(t_l)(v) = t_l(v),$$

where $\overline{\alpha_{111}}(t_l)$ is evaluated on v as a polynomial in the t_j. Setting $j_l = \overline{\alpha_{111}}(t_l)(v) - t_l(v)$ we get that $k[D] = k[x_1, \dots, x_n, u]/I$, where

$$I = (g_1, \dots, g_m, j_1, \dots, j_{r_1}, u\bar{f} - 1),$$

where $\bar{f}$ denotes f similarly evaluated on v. Note that the g_i and j_i are all d-bounded by assumption.

By [Eis95, Prop. 15.30], the ideal of $k[x_1, \dots, x_n]$ defining $\bar{D}$ is $J := I \cap k[x_1, \dots, x_n]$. But from Lemma 3.15 we have J is e'-bounded for some $e' = e'(d)$. Finally, Proposition 3.22 gives a primary decomposition $J = \bigcap J_i$ generated by an e-bounded list of ideals. But Remark 3.13 explains why one of these ideals, J_1 say, defines the identity component of $C_G(v)$.

Now $C_G(N) = \bigcap_{v\in N}(C_G(v))$. If J_v denotes the ideal of S defining $C_G(v)^\circ$, then $C_G(N)$ is defined by $\sum_{v\in N} J_v$. By concatenating generators, and using the fact that S is Noetherian we see that $C_G(N) = S/\mathcal{J}$ for some e-bounded ideal $\mathcal{J}$. □

The Lefschetz principle now implies the main theorem. To wit, take a finite open cover $X = X_1 \cup \cdots \cup X_s$ and for each X_i, a finite collection of principal open sets $\{D_{iik}\}$ covering $\alpha^{-1}(X_i) \cap G \times X_i$. By finiteness and finite presentedness, $\bar{\alpha}_{iik}$ is d-bounded for some d. Proposition 3.24 now implies that all centralisers of all points are defined by e-bounded Hopf algebras for some e. Now use Theorem 3.12 to evince the existence of the desired bound on the characteristic.

To prove the corollary from the introduction, we need only explain how to see that the stabilisers of subspaces are generically smooth. For this, just observe that the action of an affine R-group G on a G-module M gives rise to the action of G on the Grassmannian X of the r-dimensional subspaces of M. Of course, X is a scheme (see [DG70, I.1.3.13] for a proof). Since the centraliser in G of a point of $X(k)$ is precisely the stabiliser of the corresponding subspace, we are done by the theorem.

3.7. **Remarks and examples.**

Remark 3.25. Taking X to be a single point with a trivial action, we recover the fact that an affine R-group is smooth after base change to fields of sufficiently high characteristic. This fact seems to be well known when $R = \mathbb{Z}$ under the maxim that 'a smooth projective variety over $\mathbb{Q}$ has only finitely many places of bad reduction'.[5]

Remark 3.26. Note that it is essential to our proof that the module M is d-bounded—it does not suffice that M be finitely generated. If G is a split reductive group over $\mathbb{Z}$ and $N = V_G(\lambda)$ is a Weyl module for G with minuscule highest weight λ, then N_k is irreducible for each field k. When $\mathrm{char} k = p > 0$, let $M_k = (N_k)^{[1]}$ be the Frobenius twist of N_k through $F : G_k \to G_k^{(1)}$; as $G_k \cong F(G_k) = G_k^{(1)}$ we have M_k irreducible too. By irreducibility, $C_{G_k}(m) \subsetneq G_k$ for any $0 \neq m \in M_k$. The k-group G being connected and smooth it follows that $\dim_k(C_{G_k}(m)) < \dim G_k$, yet $\mathrm{Lie}(G_k)$ is in the kernel of the action on M_k. Thus $\dim_k \mathrm{Lie}(C_{G_k}(m)) = \dim G_k$; it follows that $C_{G_k}(m)$ is not smooth.

Remark 3.27. Any hope to extend the theorem to deal with setwise stabilisers of subsets of $X(k)$ will fail without first imposing some further hypotheses. For example, [HS16, Ex. 11.11] gives a smooth subgroup of GL_3, the normaliser of which is non-smooth in any characteristic.

References

[BMRT10] M. Bate, B. Martin, G. Röhrle, and R. Tange, *Complete reducibility and separability*, Trans. Amer. Math. Soc. **362** (2010), no. 8, 4283–4311.

[BW93] Thomas Becker and Volker Weispfenning, *Gröbner bases*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, New York, 1993, A computational approach to commutative algebra, In cooperation with Heinz Kredel. MR 1213453

[DG70] M. Demazure and P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Éditeur, Paris, 1970, Avec un appendice ıt Corps de classes local par M. Hazewinkel.

[Dub90] Thomas W. Dubé, *The structure of polynomial ideals and Gröbner bases*, SIAM J. Comput. **19** (1990), no. 4, 750–775. MR 1053942

[Eis95] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 1322960

[GTZ88] Patrizia Gianni, Barry Trager, and Gail Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Comput. **6** (1988), no. 2-3, 149–167, Computational aspects of commutative algebra. MR 988410

[5] See MathOverflow Q59071 and MathOverflow Q182317.

[Her13] S. Herpel, *On the smoothness of centralizers in reductive groups*, Trans. Amer. Math. Soc. **365** (2013), no. 7, 3753–3774. MR 3042602

[HS16] Sebastian Herpel and David I. Stewart, *On the smoothness of normalisers, the subalgebra structure of modular Lie algebras, and the cohomology of small representations*, Doc. Math. **21** (2016), 1–37. MR 3465106

[Jan03] J. C. Jantzen, *Representations of algebraic groups*, second ed., Mathematical Surveys and Monographs, vol. 107, American Mathematical Society, Providence, RI, 2003. MR MR2015057 (2004h:20061)

[Kem02] Gregor Kemper, *The calculation of radical ideals in positive characteristic*, J. Symbolic Comput. **34** (2002), no. 3, 229–238. MR 1935080

[Kol88] János Kollár, *Sharp effective Nullstellensatz*, J. Amer. Math. Soc. **1** (1988), no. 4, 963–975. MR 944576

[LT18] Alastair J. Litterick and Adam R. Thomas, *Complete reducibility in good characteristic*, Trans. Amer. Math. Soc. **370** (2018), no. 8, 5279–5340. MR 3803140

[Mar02] David Marker, *Model theory*, Graduate Texts in Mathematics, vol. 217, Springer-Verlag, New York, 2002, An introduction. MR 1924282

[PS18] A. Premet and D. I. Stewart, *Classification of the maximal subalgebras of exceptional lie algebras*, arxiv:1711.06988 (2018).

[Ric67] R. W. Richardson, Jr., *Conjugacy classes in Lie algebras and algebraic groups*, Ann. of Math. (2) **86** (1967), 1–15. MR 0217079 (36 #173)

[Sei71] A. Seidenberg, *On the length of a Hilbert ascending chain*, Proc. Amer. Math. Soc. **29** (1971), 443–450. MR 0280473

[Ste16] David I. Stewart, *On the minimal modules for exceptional Lie algebras: Jordan blocks and stabilizers*, LMS J. Comput. Math. **19** (2016), no. 1, 235–258. MR 3530500