Some model-theoretical and geometric properties of fields with jet operators

Piotr Kowalski

Contents

0 Introduction

The paper deals with jet operators on fields, and geometric and model-theoretical properties of them. Jet operators (Definition 2.1.5(iii)) were introduced by Alexandru Buium in [Bu3]. Jet operators generalize both derivations and endomorphisms, so the geometric properties of fields with them may be considered as those properties of difference or differential fields, which do not reflect the difference between derivations and automorphisms.

Differential algebra (the theory of fields with derivations) was invented by Ritt, who was interested in finding algebraic methods of solving differential equations. But it was Ellis Kolchin who developed differential algebra [Ko], and also introduced differential algebraic geometry, mainly differential algebraic group theory. Buium found a way to connect diophantine geometry with differential algebraic geometry. Many diophantine problems may be interpreted as questions about abstract subgroups of algebraic groups. The main problem is that it is difficult to apply the algebro-geometric methods to an abstract subgroup of an algebraic group. Buium in [Bu1] proposed another method. He was able to find an intermediate group, still well describing the original diophantine problem, but defined in a wider setting of differential algebraic geometry. This justifies an interest in differential algebraic group theory. From the model-theoretical point of view, fields with derivations or automorphisms yield interesting examples of theories, where deep model-theoretical methods, as geometric stability theory, may be applied. These methods were recently used to obtain new diophantine results (see [Hr2], [Hr3], [HP], [Sc2], [Sc3]).

The main results of this paper are:

1. Classification of jet operators on a field K, in any characteristic (Theorem 2.3.1). Buium [Bu3] classified such jet operators in characteristic 0, in a more general context (for local domains). This classification leads to some results on model companions of theories of fields with operators (Theorem 3.2.1).

2. Corollary 2.4.15, which says that for every jet operator δ on a field K in any characteristic, every affine polynomial δ-algebraic group embeds into $GL_n(K)$ by a δ-morphism. The above result was obtained by Cassidy [Ca1] in the case of differentially closed field of characteristic 0.

3. Theorem 2.4.18, saying that for every jet operator δ on a field K each affine polynomial δ-algebraic group living on an affine space embedds into a unipotent algebraic group. The proof uses Corollary 2.4.15, mentioned above, as well as the theorem of Marcin Chałupnik and the author about proaffine algebraic groups [CK] (a sketch of the proof of the last result is included in the Appendix).
Intermediate results were obtained by Anand Pillay and the author [KP] (the case of differentially closed field of characteristic 0, which was a question of Buium and Cassidy, see 2.4.1 in [BC]) and by Marcin Chałupnik and the author [CK] (the case of any differential field). A proof for difference fields appeared in [KP2].

4. The 1-step conjecture for differential algebraic groups, that is groups definable in DCF_0 (Theorem 3.2.10). This is a model-theoretical property of groups, introduced by Newelski [Ne]. Earlier, in the case of ACF (that is algebraic groups) the author proved [K], that the 1-step conjecture is equivalent to a part of Mordell-Lang conjecture from diophantine geometry (Theorem 3.2.8). Then, based on this equivalence, the proof of this conjecture in the case of algebraic groups in characteristic 0 was pointed out to the author by Anand Pillay and Felipe Voloch [K, Theorem 3.2].

The crucial notion for the proofs of these results is that of prolongation. In our paper there are 3 kinds of prolongations considered: prolongations of algebras (Section 2.2), prolongations of varieties (Section 2.4) and prolongations of types (Section 3.2).

The paper is composed as follows: after Preliminaries, in Chapter 2 we introduce jet operators δ and certain category of δ-algebras. The properties of jet operators proved in Section 2.1 are then used in Section 2.3 to classify jet operators on fields (Theorem 2.3.1). In Section 2.2 we introduce certain category Alg_δ of algebras with jet operators. In Section 2.4 we develope affine δ-algebraic geometry and using results from Sections 2.1 and 2.2 prove results on embeddings of δ-algebraic groups. Section 3 is model-theoretic, we prove there results mentioned in 1. and 4. above. The proofs use the classification from Section 2.3 and model-theoretic prolongations.

We finish with the appendix containing a sketch of the proof from [CK] of prounipotency of any group scheme on a proaffine space.

I would like to express my deepest gratitude to my advisor Ludomir Newelski for his guidance throughout my undergraduate and graduate study. I would like to thank also Anand Pillay, from whom I benefited a lot, particularly during the year 98/99 I spent at the University of Illinois. Thanks also are due to Marcin Chałupnik for many stimulating discussions.

I would like to thank the referees for suggestions for improving the presentation.

1 Preliminaries

In this paragraph we collect the necessary notions and facts, and set up the notation.

1.1 Categories and Functors

We assume the reader is familiar with the basic notions of category theory, like these of category, its objects, morphisms between them and co(ntra)variant functors. $X \in C$ means that X is an object of category C. Alg_R denotes the category of R-algebras with unity (for R, a commutative ring with unity). A functor F between categories C and D is denoted by $F : C \longrightarrow D$.

An inverse system consists of a set of objects $(X_i)_{i \in I}$ indexed by an ordered set I and a set of morphisms $(f_{ij} : X_i \longrightarrow X_j)_{i \geq j}$ such that $f_{ii} = Id_{X_i}$ and $f_{ik} = f_{jk} \circ f_{ij}$ for any $i \geq j \geq k$. A direct system is the dual notion to an inverse system. An inverse limit (lim) of an inverse system $(X_i)_{i \in I}$ is an object X with morphisms $f_i : X \longrightarrow X_i$ commuting with f_{ij}'s such that for any other X' and $f'_i : X \longrightarrow X_i$ commuting with f_{ij}'s there is a unique morphism $X \longrightarrow X'$ commuting with f_i's and f'_i's. A direct limit (colim) is the dual notion to the inverse limit.

A terminal object of the category C is an object $*$ such that for any $X \in C$, $Mor(X, *)$ consists of one element, which will be denoted also by $*$. An initial object is the dual notion to the terminal object. Any two initial or terminal objects are unique up to a unique isomorphism. If $X, Y \in C$, then their product is an object Z with morphisms $Z \longrightarrow X, Y$ such that for any other $Z' \longrightarrow X, Y$ there is a unique morphism $Z' \longrightarrow Z$ commuting with the previous morphisms. The product (unique up to a unique isomorphism) is denoted by $X \times Y$. Coproduct (denoted by $\otimes$) is the dual notion to the notion of product.

Definition 1.1.1 *X is a group object in category, if it is equipped with a multiplication morphism $m : X \times X \longrightarrow X$, an inverse morphism $l : X \longrightarrow X$, and a unit morphism $e : * \longrightarrow X$ satisfying the group axioms expressed in terms of diagrams:*
associativity: $m \circ (m \times Id) = m \circ (Id \times m)$
left unit: $m \circ (e \times Id) = p_X$*, where* $p_X : * \times X \longrightarrow X$ *is the canonical projection*
left inverse: $m \circ (l, Id) = e \circ *$

A cogroup object is the dual notion to the group object (i.e. there is a comultiplication morphism from X into its coproduct with itself, satisfying "cogroup axioms", e.g. counit is a morphism form G into the initial object).

Fact 1.1.2 *Suppose $F : C \longrightarrow D$ is a contravariant functor such that for any $X, Y \in C$, $F(X \times Y) = F(X) \otimes F(Y)$. Suppose also that the image by F of a terminal object in C is an initial object in D. Then for any G, a group object in C, $F(G)$ is a cogroup object in D.*

The proof is obvious. The previous fact can be strengthened by adding to the conclusions that each of the functors considered becomes a functor between (co)group objects (so morphisms preserve (co)group structures) while restricted to the subcategory of (co)group objects.

Definition 1.1.3 *A functor is faithful if it induces monomorphisms on the sets of morphisms, it is full if induces epimorphisms on the sets of morphisms. A functor is faithfully full if it is faithful and full.*

Fact 1.1.4 *If a faithfully full functor satisfies assumptioms of 1.1.2 , then it remains faithfully full when regarded as a functor between the category of group objects in C (i.e. morphisms preserve group object morphisms) and the category of cogroup objects in D (i.e. morphisms preserve cogroup object morphisms).*

1.2 Model Theory

A language L is any collection of function, relation and constant symbols. An L-structure is a set with specified interpretations of the symbols of L. An L-formula is inductively constructed from symbols of L and logical symbols (including equality $=$). An L-theory T is any set of L-formulas (closed under logical consequence), a model of T is an L-structure, in which all the sentences from T are true. We will work in the language of rings $L_r = \{+, \cdot, 0, 1\}$ and the language of rings expanded by one unary function symbol $L_\delta = L_r \cup \{\delta\}$. So for example an L_r-structure is any abstract algebra with distinguished elements 0 and 1, and 2 binary operations. If T is the theory of rings, then its models are those L_r-structures, which are rings. An example of L_δ-theory is the theory of differential rings, which is the theory of rings with additional axioms about δ (additivity and the Leibniz rule): $\delta(x + y) = \delta(x) + \delta(y)$, $\delta(x \cdot y) = \delta(x) \cdot y + x \cdot \delta(y)$. Its models are called differential rings.

A model M of a theory T is existentially closed, if any quantifier free formula over M, which has a realization in some model of T extending M, is realized in M. A theory $\bar{T}$ is a model companion of T, if it axiomatises all the existentially closed models of T. A theory T has quantifier elimination if any formula is equivalent modulo T to a quantifier-free one. A theory is complete if for any sentence ϕ, ϕ or $\neg\phi$ is a logical consequence of T.

We fix a language L, an L-structure M and a theory $T = Th(M)$, which is the set of all L-sentences true in M. If ϕ is a sentence with parameters from M, then $M \models \phi$ means that ϕ holds in M. Any formula $\phi(x, a)$ in L with additional parameters a from M defines a set $\phi(M, a) = \{b \in M^n : M \models \phi(b, a)\}$ (n is the length of x). Such sets are called definable. If $A \subset M$, then a type in M over A is any collection of formulas $\phi(x, a)$ such that $a \subset A$, and the family of sets $\phi(M, a)$ has the finite intersection property. Any type p in M defines a set $p(M) = \bigcap\{\phi(M) : \phi \in p\}$. Such sets are called type-definable. A type p over A is called complete if for any formula $\phi(x)$ over A, $\phi \in p$ or $\neg\phi \in p$. If a is a finite subset of M and $A \subset M$, then $tp_M(a/A)$ is the set of all formulas with parameters in A, which are true of a in M, $tp_M(a/A)$ is obviously a complete type, M is omitted in the notation, when it is obvious from the context. We abbreviate $p = tp(a/A)$ as $a \models p$.

A model M is κ-saturated (κ is a cardinal number) if for any A such that $|A| < \kappa$, any type in M over A has a realization in M. For any κ, a κ-saturated model exists. If we work with a fixed, complete theory T, then it is convenient to fix its κ-saturated and strongly κ-homogenous model M (a monster model) for a big κ, and assume that all other models are submodels of M, and all sets of parameters under consideration are subsets of M. A subset $A \subset M$ is called small, if $|A| < \kappa$. Type-definable sets being loci of complete types over a small set A are exactly orbits under $Aut(M/A)$. From now on all the types will be computed in a fixed monster model M, so we write $tp(a/A)$ without the subscript M. For a tuple $a \in M$, and a small subset $A \subset M$, we say that $a \in acl(A)$, if $tp(a/A)(M)$ is finite, and $a \in dcl(A)$, if $tp(a/A)(M)$ consists of a single element.

We will need the theory of stability, in particular the theory of stable groups. We will give the definitions and recall the main theorems, however the reader is referred to [Pi1] for a systematic exposition. A theory T is stable if it does not interpret an infinite linear order. Stability of T is equivalent to existence of a unique independence relation $\downarrow$ on triples of small subsets of a monster model $M \models T$ having natural properties listed in [Pi1]. The type $tp(a/B)$ does not fork over A if $a\mathop{\smile\!\!\!\!\!\!|}_A B$. A type is stationary if it has a unique nonforking extension over any set. By adding extra elements to M naming elements of M^k/E, for any k and any definable equivalence relation on M^k, we obtain a structure M^{eq}. This is an L^{eq}-structure, where L^{eq} is obtained from L in a similar manner (for details see [Pi1]). The structure M^{eq} is convenient to work with, in particular if A is a small subset of M, then the complete types over $acl^{eq}(A)$ are always stationary (they are called strong types).

We have the following examples of stable theories: the theory of algebraically closed fields ACF, the theory of differentially closed fields DCF, the theory of any module. In the theory of algebraically closed fields $\mathop{\smile\!\!\!\!\!\!|}$ is the algebraic independence, and in the theory of vector spaces $\mathop{\smile\!\!\!\!\!\!|}$ is the linear independence.

We can extend the notion of a type-definable set to the sets of infinite tuples of elements of a given model M. Let $(x_i)_{i\in I}$ be a tuple of variables of an appropriate length. Then any formula $\phi(x_{i_1},...,x_{i_n})$, for $i_1,...,i_n \in I$, may be regarded as a formula in the variables $(x_i)_{i\in I}$. A $*$-definable set is a set defined by a collection of formulas in variables $(x_i)_{i\in I}$.

The class of simple theories contains all stable theories, we can still define a well-behaved independence relation in a saturated model of a simple theory (for the definition see [KiP]).

1.3 Algebraic Geometry

Throughout the paper K denotes an infinite field. If $char(K) = p > 0$, then Fr denotes the Frobenius endomorphism, $Fr(x) = x^p$. An affine variety over a field K is a Zariski closed subset of some power of K. A morphism between affine algebraic varieties is a restriction of a polynomial function. If V is an affine variety, then $I(V) = \{f \in K[\bar{X}] : f(V) = 0\}$, and $K[V] = K[\bar{X}]/I(V)$ is the ring of regular functions on V. We denote the category of affine algebraic varieties over K by AfV_K. An affine algebraic group is a group object in the category of affine algebraic varieties.

Let $*$ denote a point in K. Note that this is a terminal object in AfV_K. Obviously, $K[*] = K$ and K is an initial object in Alg_K. For any affine algebraic varieties V, W, $K[V \times W] = K[V] \otimes K[W]$. Hence, by 1.1.2, if G is an affine algebraic group, then $K[V]$ is a cogroup object in Alg_K.

Following [Wat] we will call cogroup objects in Alg_K Hopf algebras. Here is the precise definition, which we give for any commutative ring with unity R instead of K.

Definition 1.3.1 *A Hopf Algebra over a ring R is an algebra A over R together with a comultiplication $\Delta : A \longrightarrow A \otimes A$, counit (augmentation) $\epsilon : A \longrightarrow R$, coinverse (antipode) $S : A \longrightarrow A$ satisfying axioms dual to the group axioms:*
coassiociativity: $(\Delta \otimes Id) \circ \Delta = (Id \otimes \Delta) \circ \Delta$
left counit: $\epsilon \otimes Id \circ \Delta = c_A$ *($c_A : A \longrightarrow R \otimes A$ is the canonical injection)*
left coinverse: $(S, Id) \circ \Delta = i_A \circ \epsilon$ *(i_A is the canonical map from R into A)*

We adopt the definition of Hopf algebra from [Wat], where Hopf algebras were considered for purposes of the theory of group schemes. In other contexts (like algebraic topology, see [Sp]) Hopf algebras are usually graded and may have no antipode.

We will need a fact about infinitely generated Hopf algebras.

Fact 1.3.2 *Any Hopf algebra is a direct limit of its finitely generated Hopf subalgebras.*

For the proof see [Wat] page 24.

Let $F : V \longrightarrow W$ be a morphism between affine algebraic varieties. We call f dominant, if $f(V)$ is Zariski dense in W.

Consider now a field extension $K \subset L$. Then any affine algebraic variety V defines an affine algebraic variety $V(L)$ (the set of L-rational points of V) over L. If $V \subset K^n$, then $V(L)$ is just the Zariski closure of V in L^n. Note that V is Zariski dense in $V(L)$, $L[V(L)] = K[V] \otimes L$ and that $V \mapsto V(L)$ is a functor from AfV_K to AfV_L (see 4.1 and 4.4 in [Wat]). This implies the following fact.

Fact 1.3.3 *If G is an affine algebraic group over K, then $G(L)$ is an affine algebraic group over L. If $G \longrightarrow H$ is a dominant homomorphism of affine algebraic groups with kernel N, then there is a dominant homomorphism of affine algebraic groups over L, $G(L) \longrightarrow H(L)$ with kernel $N(L)$. If any element of G has order n, then any element of $G(L)$ has order n.*

Proof Each of the considered properties of groups is given by some equality of polynomials. Hence if it holds over K, it holds over L, too. $\square$

In Section 2.3, we will need a well-known fact about algebraic group structures on the affine line.

Fact 1.3.4 *Suppose* G *is an affine algebraic group,* K *is the underlying affine variety of* G*, i.e.* $G = (K, \diamond)$*, and* $0 \in K$ *is the unit of* G*. Then* G *is the additive group of* K*, i.e.* $\diamond = +$ *not only up to isomorphism, but as a function.*

Proof Take $a \in G$ and let $L_a(X) = a \diamond X$. Then $L_a \circ L_{a^{-1}}$ is the identity polynomial for any a. Since a^{-1} is given by a polynomial, $L_{a^{-1}}(X) = W_a(X)$ for some $W_{X'}(X) = W(X, X') \in K[X', X]$. Hence $L_{X'}(X)$ has a composition inverse, meaning that for some $L'_{X'}(X) \in K[X', X]$ we have $L_{X'}(L'_{X'}(X)) = X = L'_{X'}(L_{X'}(X))$.

Therefore $X' \diamond X = aX + F(X')$ for some $a \in K$ and $F(X') \in K[X']$. Similarly, by looking at $P_a(X) = X \diamond a$, we get that $X' \diamond X = bX' + G(X)$ for some $b \in K$ and $G(X) \in K[X]$. Hence $X' \diamond X = aX + bX' + c$. Since $\diamond$ is a group operation and 0 is the unit element, we get that $a = b = 1$ and $c = 0$. □

For one result we will need non-affine varieties, which are obtained from affine varieties by glueing along open subsets by morphisms. The notion of morphism naturally extends to non-affine varieties. A group object in the category of varieties is called an algebraic group. Note that a variety can be thought of as a disjoint union of affine varieties divided by a definable equivalence relation. So it is a definable set in K^{eq}. The following theorem was proved by van den Dries (see Theorem 3 in [vdD]) and by Hrushovski.

Theorem 1.3.5 *Suppose* G *is a group definable in* K^{eq}*, where* K *is algebraically closed. Then there is an algebraic group* H *and a definable isomorphism between* G *and* H*.*

2 Fields with jet operators – some algebra and geometry

2.1 General Properties of Jet Operators

Let us fix a commutative ring with unity R. In this section we introduce jet operators and prove their basic properties. Jet operators occured first in [Bu3]. Our presentation follows essentially [Bu3], although we generalize some of the definitions and results from there. Jet operators are the special kind of operators on R, a generalization of derivations.

Definition 2.1.1 ([Bu3]) *A map $\delta : R \longrightarrow R$ is an operator on R, if there exist polynomials $P, Q \in R[X, X', Y, Y']$ such that for any $a, b \in R$ the following (P, Q)-rule holds:*

$$\delta(a + b) = P(a, \delta(a), b, \delta(b))$$

$$\delta(a \cdot b) = Q(a, \delta(a), b, \delta(b))$$

We call the pair (P, Q) a type of δ, and we refer to δ as a $(P, Q) - operator$.

The (P, Q)-rule does not determine uniquely a (P, Q)-operator, e.g. the 0 map is an operator of many types. Also for some (P, Q), there are no (P, Q)-operators (see Section 2.3).

Examples of operators arise naturally in algebra and geometry. Any derivation of a ring R is an operator, and Q is provided by the Leibniz rule, namely $P = X' + Y'$, $Q = X \cdot Y' + Y \cdot X'$. A ring with derivation is called a differential ring. A natural example is (C^∞, δ_x), the ring of differentiable functions on $\mathbb{R}$ with the usual derivation, and $(K[X], d/dX)$, the ring of polynomials with the usual derivation.

An endomorphism of a ring is an operator of the type $P = X' + Y'$, $Q = X' \cdot Y'$. A difference operator is an operator of the following type: $P = X' + Y'$, $Q = X \cdot Y' + Y \cdot X' + X' \cdot Y'$. It is easy to check that δ is a difference operator if and only if $\delta + Id$ is an endomorphism. So every endomorphism ϕ determines a diffrerence operator $\phi - Id$. If $R = K[X]$ (K is a field), then for $F \in R$, $(\delta F)(X) = F(X + 1) - F(X)$ is the original difference operator (see Preface in [Co]), which explains the name of these operators.

In [Bu2] Buium introduced a new kind of operators – the p-derivations (p is a prime integer). The (P, Q)-rule of a p-derivation is the following:

$$P = X' + Y' + [(X + Y)^p - X^p - Y^p)]/p, \ Q = X^p \cdot Y' + Y^p \cdot X' + p \cdot Y' \cdot X'$$

Such operators occur in situations, where the usual derivation can not be present, e.g. if R is a discrete valuation ring with algebraically closed residue field k of characteristic p, pR is the kernel of $R \longrightarrow k$, and there is $\phi : R \longrightarrow R$, a lifting of the Frobenius map on k. Then $\delta(x) = (\phi(x) - x^p)/p$ is a p-derivation (see [Bu2] p. 350).

The exponential function $\exp : \mathbb{R} \longrightarrow \mathbb{R}$ is not an operator, since there is no polynomial function Q such that $Q(x, \exp(x), x, \exp(x))$ is asymptotically $\exp(x^2)$.

To algebraise rings with operators, we need a structure controlling the type of an operator.

Definition 2.1.2 ([Bu3]) *Let $P, Q \in R[X, X', Y, Y']$ ((P, Q) is thought of as a type of some operators). Then $R_{P,Q} = (R^2, \oplus, *)$, where $\oplus, *$ are defined in the following way:*

$$(a_0, a_1) \oplus (b_0, b_1) = (a_0 + b_0, P(a_0, a_1, b_0, b_1))$$

$$(a_0, a_1) * (b_0, b_1) = (a_0 \cdot b_0, Q(a_0, a_1, b_0, b_1))$$

It should be remarked that $R_{P,Q}$ in general is not a ring, it is just an abstract structure (an algebra in the sense of universal algebra). For any $B \in Alg_R$, we define $B_{P,Q}$ as $B_{i(P),i(Q)}$, where $i : R \longrightarrow B$ is the canonical morphism, extended to the ring of polynomials in the usual way.

Definition 2.1.3 *Let (R, δ), (S, δ') be rings with operators.*
i) The homomorphism $f : R \longrightarrow S$ is a morphism of rings with operators if $\delta' \circ f = f \circ \delta$.
ii) We say that δ' extends δ, if f above is an inclusion and δ', δ admit the same type.

Lemma 2.1.4 *Let δ be an operator on R and $P, Q \in K[X, X', Y, Y']$.*
i) δ is a (P, Q)-operator if and only if the map $(Id, \delta) : R \longrightarrow R_{P,Q}$ is a homomorphism.

ii) Suppose we have a ring homomorphism $\alpha : R \longrightarrow S$, and δ' is an operator on S. The following conditions are equivalent:
$(*)$ α is a morphism of rings with operators, (P,Q) is a type of δ, (P',Q') is a type of δ'
$(**)$ The following diagram consists of homomorphisms of structures and is commutative:

$$\begin{array}{ccc} R & \xrightarrow{\quad \alpha \quad} & S \\ {\scriptstyle (Id,\delta)}\downarrow & & \downarrow{\scriptstyle (Id,\delta')} \\ R_{P,Q} & \xrightarrow[\alpha \times \alpha]{\qquad} & S_{P',Q'} \end{array}$$

iii) For any ring homomorphism $f : R \longrightarrow S$, we have an induced morphism of structures $f \times f : R_{(P,Q)} \longrightarrow S_{(f(P),f(Q))}$.

Proof It is just a straightforward checking. $\square$

Now, following [Bu3], we can define jet operators.

Definition 2.1.5
i) An operator δ on R is generic if any $F \in R[X,Y]$ vanishing on the graph of δ is equal 0.
ii) An operator δ is a jet operator if it admits a generic extension on some ring $S \supset R$ and $\delta(0) = \delta(1) = 0$.
iii) A type of a jet operator δ is a pair (P,Q) such that there exists a generic extension of δ of the type (P,Q).

Below, we will show that any derivation is a jet operator. Indeed, jet operators were defined so, that for a jet operator δ it is possible to develop a theory of δ-varieties, generalizing the theory of differential algebraic varieties. This is the motivation for the above definition.

It is not immediate to verify, if a given operator is a jet operator. For this we will need criteria from Theorem 2.1.7. After the proof of Theorem 2.1.7

we will give some examples of jet operators. For the proof of this theorem the following lemma will be used.

Lemma 2.1.6 ([Bu3]) *If δ is a generic operator and $F \in R[X_1, ..., X_{2n}]$ vanishes on $(x_1, ..., x_n, \delta x_1, ..., \delta x_n)$ for any $x_1, ..., x_n \in R$, then $F = 0$.*

Proof Easy induction. □

The next theorem yields criteria, which enable us to check if a given operator is a jet operator. The implication i) $\Rightarrow$ ii) is [Bu3, Lemma 2]. Also the implication iii) $\Rightarrow$ i) was used there to check that certain operators are jet operators. The implication ii) $\Rightarrow$ iii) is new but easy to prove.

Theorem 2.1.7 *Suppose δ is an operator such that $\delta(0) = \delta(1) = 0$ and $P, Q \in R[X, X', Y, Y']$. Then the following are equivalent:*
i) δ is a jet operator of type (P, Q).
ii) $B_{P,Q}$ is a commutative ring for any R-algebra B.
iii) δ extends to a (P, Q)-operator δ' on the ring of polynomials $R[X, X', X'', ...]$, such that $\delta'(X^{(n)}) = X^{(n+1)}$ ($X^{(0)} = X$).

Proof (i) $\Rightarrow$ (ii)
Suppose δ extends to a generic (P, Q)-operator δ' on a bigger ring S. Take any $a, b, c \in S$. Obviously $a + (b + c) = (a + b) + c$. Applying δ' to both sides, and using twice the (P, Q)-rule, we get:

$$P(a, \delta'(a), b + c, P(b, \delta'(b), c, \delta'(c)) = P(a + b, P(a, \delta'(a), b, \delta'(b)), c, \delta'(c))$$

By Lemma 2.1.6 we have an equality in the ring of polynomials with coefficients in R:

$$P(X, X', Y + Z, P(Y, Y', Z, Z')) = P(X + Y, P(X, X', Y, Y'), Z, Z')$$

Now take any $B \in Alg_R$, and $(a_0, a_1), (b_0, b_1), (c_0, c_1) \in B_{P,Q}$. Then:

$$(a_0, a_1) \oplus [(b_0, b_1) \oplus (c_0, c_1)] = (a_0 + b_0 + c_0, P(a_0, a_1, b_0 + c_0, P(b_0, b_1, c_0, c_1)) =$$

$$(a_0 + b_0 + c_0, P(a_0 + b_0, P(a_0, a_1, b_0, b_1), c_0, c_1)) = [(a_0, a_1) \oplus (b_0, b_1)] \oplus (c_0, c_1)$$

The remaining ring axioms follow in the same way, and $1 = (1, 0), 0 = (0, 0)$.
(ii) $\Rightarrow$ (iii)

$R[X,X',X'',...]_{P,Q}$ is a ring by (ii). Since $\delta(0) = \delta(1) = 0$, we have that $(Id,\delta) : R \longrightarrow R_{P,Q}$ takes 0 to $(0,0)$ and 1 to $(1,0)$. By (ii) and 2.1.4(i) (Id,δ) is a homorphism of rings. Using the universal property of the ring of polynomials we get a ring homomorphism

$$\Psi : R[X,X',X'',...] \longrightarrow R[X,X',X'',...]_{P,Q}$$

such that: $\Psi(X^{(n)}) = (X^{(n)}, X^{(n+1)})$. So Ψ is of the form (Id,δ') and δ' satisfies (iii) by Lemma 2.1.4(i).

(iii) $\Rightarrow$ (i)

We show that the extension δ' from (iii) is generic. Take F, a polynomial in two variables with coefficients in $R[X,X',X'',...]$. There is always an N such that all the coefficients of F belongs to $R[X,...,X^{(N-1)}]$. Suppose that $F(graph(\delta')) = 0$. Then $0 = F(X^{(N)}, \delta'(X^{(N)})) = F(X^{(N)}, X^{(N+1)})$, so $F = 0$. $\square$

Now, we can provide examples of jet operators. We use condition (ii) from the previous theorem. Suppose B is an R-algebra. Let δ be a derivation on R. Then $P = X' + Y'$, $Q = XY' + YX'$. We see that $B_{P,Q}$ is isomorphic to the ring of dual numbers $B[X]/X^2$, so δ is a jet operator.

If δ is a difference operator on R, then $P = X' + Y'$, $Q = XY' + YX' + X'Y'$. In this case $B_{P,Q}$ is isomorphic to $B \times B$, so δ is again a jet operator.

Finally if δ is a p-derivation and (P,Q) is its type, then $B_{P,Q}$ is isomorphic to the ring of Witt vectors of length 2 (see [Bu2, 1.1]). Hence p-derivations are jet operators, too.

The next corollary shows that sometimes being a (P,Q)-operator implies being a jet operator.

Corollary 2.1.8 *Assume $P,Q \in R[X,X',Y,Y']$, $B \in Alg_R$ and δ is a jet operator on R of type (P,Q). Then any (P,Q)-operator on B (not necessarily extending δ) is a jet operator.*

Proof By Theorem 2.1.7 it is enough to check that $S_{P,Q}$ is a ring for each B-algebra S. But S is also an R-algebra, so $S_{P,Q}$ is a ring by 2.1.7 . $\square$

For a jet operator δ on R, we call the ring $R_{P,Q}$ with the structure of an R-algebra given by $(Id,\delta) : R \longrightarrow R_{P,Q}$, the structure ring of δ. We will be able (Theorem 2.3.1) to classify the jet operators on fields up to a certain notion of equivalence introduced in [Bu3].

Definition 2.1.9 *Two operators δ_0, δ_1 (not necessarily of the same type) on the ring R are equivalent, if there exist $\lambda \in R^\star$ and $f \in R[X]$ such that $f(0) = f(1) = 0$ and $\delta_0(x) = \lambda \cdot \delta_1(x) + f(x)$ for each $x \in R$.*

Buium [Bu3] observed that if δ and δ' are equivalent, then δ is generic if and only if δ' is generic and δ is a jet operator if and only if δ' is a jet operator.

To classify jet operators, we need to express their equivalence in terms of their structure rings.

Fact 2.1.10 ([Bu3]) *Two jet operators δ_0, δ_1 are equivalent if and only if there exist types (P, Q), (P', Q') of them such that there is an isomorphism of rings $\phi : R_{P,Q} \longrightarrow R_{P',Q'}$ such that ϕ, ϕ^{-1} are given by polynomials in variables X, X', $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = (X, X')$ as polynomials and the following diagram is commutative:*

$$(*) \qquad \begin{array}{ccc} R & \xrightarrow{\;Id\;} & R \\ {\scriptstyle (Id,\delta_0)}\downarrow & & \downarrow{\scriptstyle (Id,\delta_1)} \\ R_{P,Q} & \xrightarrow[\;\phi\;]{} & R_{P',Q'} \end{array}$$

Proof

$\Rightarrow$

Suppose that $\delta_1(x) = \lambda \cdot \delta_0(x) + f(x)$ for each $x \in R$. Choose a generic extension δ_0' of δ_0 on some ring $S \supset R$, of type (P, Q). Then the formula $\delta_1'(x) = \lambda \cdot \delta_0'(x) + f(x)$ defines a generic operator on S extending δ_1, of some type (P', Q'). It is enough to show the assertion for S and δ_0', δ_1', so we may assume that $S = R$ and our original operators δ_0, δ_1 are generic of types $(P, Q), (P', Q')$ respectively.

Define $\phi(X, X') = (X, \lambda \cdot X' + f(X))$. We check the additivity of ϕ in a special case first:

$$\phi((x, \delta_0 x) \oplus (y, \delta_0 y)) = \phi(x + y, P(x, \delta_0 x, y, \delta_0 y)) = \phi(x + y, \delta_0(x + y)) =$$

$$= (x+y, \lambda\cdot\delta_0(x+y)+f(x+y)) = (x+y, \delta_1(x+y)) = (x+y, P'(x, \delta_1(x), y, \delta_1(y)) =$$

$$= (x, \delta_1(x)) \oplus (y, \delta_1(y)) = (x, \lambda \cdot \delta_0(x) + f(x)) \oplus (y, \lambda \cdot \delta_0(y) + f(y)) =$$

$$= \phi(x, \delta_0(x)) \oplus \phi(y, \delta_0(y))$$

ϕ is additive if and only if a certain polynomial vanishes on R^4. But this polynomial vanishes on $(x, \delta_0(x), y, \delta_0(y))$ for each $x, y \in R$ by the previous checking, so by Lemma 2.1.6 and genericity of δ_0 it equals 0.

To prove that ϕ preserves multiplication, we can proceed in the same way. Since $f(0) = f(1) = 0$, ϕ preserves 0 and 1. If we define $\phi^{-1}(X, X') = (X, X'/\lambda - f(X)/\lambda)$, then $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = (X, X')$ as polynomials.
$\Leftarrow$
Suppose that an isomorphism $\phi : R_{P,Q} \longrightarrow R_{P',Q'}$ as in $(*)$ is given by a pair of polynomials $H(X, X'), G(X, X')$. Since it is over R, we see that $H(X, X') = X$. Write $G(X, X')$ as $G_X(X') \in R[X][X']$, so we consider G as a polynomial of X' with coefficients in $R[X]$. By the assumption $G_X(X')$ is invertible composition-wise (as in the proof of 1.3.4) in $R[X][X']$. Hence $G_X(X') = w(X)X' + f(X)$ for some $f \in R[X]$ and w, an invertible element in $R[X]$. But the invertible elements in $R[X]$ coincide with the invertible elements of R, so $w = \lambda \in R^*$. Therefore $G(X, X') = \lambda \cdot X' + f(X)$. Now the condition $\delta_1'(x) = \lambda \cdot \delta_0'(x) + f(x)$ for each $x \in R$ follows from the commutativity of the diagram $(*)$. $\square$

2.2 The category of δ-algebras

In this section we introduce the category of δ-R-algebras, which will be used in Section 2.4 to describe δ-varieties for a jet operator δ. The correspondence betwen affine varieties and their coordinate rings transfers to differential algebraic geometry. It is precisely the δ-varieties for jet operators, for which this correspondence can also be formulated, for a suitably modified notion of a coordinate ring.

From now on until the end of this section we fix the ring R, a jet operator δ on R and a type (P, Q) of δ. We introduce the category of δ-R-algebras (the R will be omitted in the notation). Its objects are R-algebras S with a (P, Q)-operator such that the canonical morphism from R into S is a morphism of rings with operators (see 2.1.3(i)). If the canonical map from R into an R-algebra B is an embedding, then this condition means that the operator on B extends δ (see 2.1.3(ii)). A morphism between δ-algebras, called a δ-morphism, is an R-algebra homomorphism commuting with given (P,Q)-operators. We denote this category by $Alg_{R,\delta}$ or just Alg_δ. Obviously, for any $B \in Alg_\delta$, the canonical morphism $R \longrightarrow B$ is a δ-morphism. We will also use δ to denote the (P,Q)-operator on any δ-algebra. By Corollary 2.1.8, this operator is again a jet operator.

The ring $R[X, X', X'', ...]$ with the generic operator, which showed up in 2.1.7(iii), will play a role of a polynomial ring in Alg_δ. According to our convention, we denote the generic operator on $R[X, X', X'', ...]$ by δ, too. We denote $(R[X, X', X'', ...], \delta)$ by $R\{X\}_\delta$ or just $R\{X\}$ if δ is understood, and call it the ring of δ-polynomials. The order of a δ-polynomial F is the maximal n, such that $X^{(n)}$ appears in F. $R\{X_1, ..., X_n\}$ is defined inductively as $R\{X_1, ..., X_{n-1}\}\{X_n\}$. Its elements act naturally as functions from R^n into R, and they will be regarded in such a way. Moreover, for any $B \in Alg_\delta$ and $F \in R\{X_1, ..., X_n\}$, F acts as a function from B^n into B, since the canonical map $R \longrightarrow B$ induces a δ-morphism $R\{X_1, ..., X_n\} \longrightarrow B\{X_1, ..., X_n\}$. Similarly, we define $R\{\bar{X}\}$ for any set of variables $\bar{X}$. Item (i) from the next lemma will be used in Section 2.4 to define coordinate rings for δ-varieties. Item (ii) says that $R\{\bar{X}\}$ may be seen as a free δ-algebra over R.

Lemma 2.2.1
i) Let $B \in Alg_\delta$, $F \in R\{X_1, ..., X_n\}$ and $a \in B^n$. Then $(\delta(F))(a) = \delta(F(a))$ (F is regarded as a function between B^n and B as above).
ii) Suppose $B \in Alg_\delta$ and $\bar{X}$ is a set of variables. Then any map $f : \bar{X} \longrightarrow B$ can be uniquely extended to a δ-morphism $f_0 : R\{\bar{X}\} \longrightarrow B$.

Proof
(i) Suppose first that $B = R$. If $F = X_i^{(j)}$, then the assertion is true for F by the definition of the (P,Q)-operator on $R\{X_1, ..., X_n\}$. For constant polynomials there is nothing to check. We will proceed by induction on the complexity of δ-polynomial. Suppose that (i) is true for $F, G \in R\{X\}$. Then:

$$\delta(F+G)(a) = P(F, \delta F, G, \delta G)(a) = P(F(a), \delta F(a), G(a), \delta G(a)) =$$

$$= P(F(a), \delta(F(a)), G(a), \delta(G(a))) = \delta((F+G)(a))$$

Similarly for products. So our asertion is true, since every $F \in R\{X_1, ..., X_n\}$ is a sum of monomials in variables $X_i^{(j)}$.

Let B be any δ-algebra. By the previous case, for any $F \in B\{X_1, ..., X_n\}$, we have $\delta(F)(a) = \delta(F(a))$. Since $R\{X_1, ..., X_n\} \longrightarrow B\{X_1, ..., X_n\}$ is a δ-morphism, the above equality remains true for $F \in R\{X_1, ..., X_n\}$.

(ii) For any $F \in R\{\bar{X}\}$, there are $X_{i_1}, ..., X_{i_n}$ such that $F \in R\{X_{i_1}, ..., X_{i_n}\}$. Let $a = (f(X_{i_1}), ..., f(X_{i_n})) \in B^n$ and define $f_0(F) = F(a)$ (we regard F as a map from B^n to B). Now (i) means exactly that f_0 is a δ-morphism. □

Now we can introduce a natural (P, Q)-operator δ on the tensor product over R of two δ-algebras B and S such that $(B \otimes S, \delta)$ is a δ-algebra. The (P, Q)-operators on B and S give morphisms $B \longrightarrow B_{P,Q}, S \longrightarrow S_{P,Q}$. By functoriality of the structure ring (2.1.4(iii)) we have also morphisms $B_{P,Q}, S_{P,Q} \longrightarrow (B \otimes S)_{P,Q}$. By composing, we get morphisms $B, S \longrightarrow (B \otimes S)_{P,Q}$. Since $\otimes$ is the coproduct, we obtain a morphism $B \otimes S \longrightarrow (B \otimes S)_{P,Q}$. It is easy to see that this morphism is of the form (Id, δ') which gives a (P, Q)-operator δ' on $B \otimes S$. According to our convention we still denote this (P, Q)-operator by δ. It is obvious that $\otimes$ in Alg_δ is still the coproduct.

Explicitly $\delta(b \otimes s) = Q(b \otimes 1, \delta b \otimes 1, 1 \otimes s, 1 \otimes \delta s)$ and is extended to finite sums of tensors using the P-rule. For example if $P = X' + Y'$, $Q = XY' + X'Y$ (that is, all (P, Q)-operators on δ-R-algebras are derivations), then $\delta(b \otimes s) = \delta b \otimes s + b \otimes \delta s$.

Having defined coproduct in Alg_δ, we can define δ-Hopf algebras, which will be cogroup objects in Alg_δ.

Definition 2.2.2 *Suppose $B \in Alg_{R,\delta}$ and $\Delta : B \longrightarrow B \otimes B$, $S : B \longrightarrow B$, $\epsilon : B \longrightarrow R$ are δ-morphisms making B into a Hopf algebra. We call the structure (B, Δ, ϵ, S) a δ-Hopf algebra.*

It is straightforward that δ-Hopf algebras are cogroup objects in $Alg_{R,\delta}$.

In the category Alg_δ we can also define quotients. It is obvious how the δ-ideals should be defined.

Definition 2.2.3 *Let $B \in Alg_\delta$. An R-ideal $I \subset B$ (i.e. an ideal being an R-module) is a δ-ideal, if $\delta(I) \subset I$.*

It is easy to see that kernels of morphisms in Alg_δ are δ-ideals. The next fact shows that quotients of δ-algebras by δ-ideals are still δ-algebras.

Fact 2.2.4 *Suppose $B \in Alg_\delta$ and $I \subset B$ is a δ-ideal. Then there is a (P, Q)-operator on B/I making it a δ-algebra such that the quotient map $B \longrightarrow B/I$ is a δ-morphism.*

Proof

Denote by f the quotient map $B \longrightarrow B/I$. By Lemma 2.1.4(iii) and Theorem 2.1.7, $f \times f : B_{P,Q} \longrightarrow (B/I)_{P,Q}$ is a homomorphism of rings. Since I is a δ-ideal, we have $(Id, \delta)(I) \subset I \times I = ker(f \times f)$. Hence $(f \times f) \circ (Id, \delta)(I) = 0$, so there is an operator δ' on B/I such that the following diagram commutes:

$$\begin{array}{ccc} B & \xrightarrow{\quad f \quad} & B/I \\ {\scriptstyle (Id,\delta)}\downarrow & & \downarrow{\scriptstyle (Id,\delta')} \\ B_{P,Q} & \xrightarrow[\quad f \times f \quad]{} & (B/I)_{P,Q} \end{array}$$

By Lemma 2.1.4(ii) we are done. □

Let B and I be as in the above fact and δ denotes also the operator on B/I. Then, by the above construction, $\delta(a/I) = \delta(a)/I$.

Let $B \in Alg_\delta$ and $X \subset B$. We say that X δ-generates B, if B does not have a proper δ-subalgebra (a subalgebra, closed under δ) containing X.

We define the n-th jet algebra of B when B is an algebra equipped with a (P, Q)-operator extending δ and is δ-finitely generated over R. The aim is to understand the δ-structure of B by means of an infinite sequence of R-algebras, called prolongations of B. We will do it in the simplest possible way (suggested in [Sc1]), however the definition depends on a set of δ-generators.

Definition 2.2.5 *Suppose X is a finite set of δ-generators of B. Define $B_X^{(n)}$ as the R-subalgebra of B generated by the set $\{X, \delta(X), ..., \delta^{(n)}(X)\}$. We call $B_X^{(n)}$ the n-th prolongation of B with respect to X.*

Lemma 2.2.6 *Suppose H is a Hopf subalgebra of a δ-Hopf algebra B. Then the R-subalgebra generated by $\{H, \delta(H), ..., \delta^{(n)}(H)\}$ is a Hopf subalgebra for any n.*

Proof Let $H(n)$ be the R-algebra generated by $H, \delta(H), ..., \delta^{(n)}(H)$. From the definition of δ-structure on a tensor product, we have $\delta(H \otimes H) \subset H(1) \otimes H(1)$ and inductively $\delta^{(n)}(H \otimes H) \subset H(n) \otimes H(n)$. Denote the comultiplication in B by Δ. Since Δ commutes with δ, and H is a Hopf subalgebra, we have a commutative diagram:

$$\begin{array}{ccc} H & \xrightarrow{\Delta} & H \otimes H \\ \downarrow{\scriptstyle \delta^{(n)}} & & \downarrow{\scriptstyle \delta^{(n)}} \\ H(n) & \xrightarrow{\Delta} & H(n) \otimes H(n) \end{array}$$

Similarly the antipode S commutes with δ, so $\delta^{(n)} \circ S = S \circ \delta^{(n)}$. The same holds for the counit ϵ.
Hence $H(n)$ is a Hopf subalgebra of B. $\square$

Proposition 2.2.7 *If B is a δ-finitely generated δ-Hopf algebra, then there exists X, a finite set of δ-generators of B, such that for any n, $B_X^{(n)}$ is a Hopf algebra.*

Proof By 1.3.2 B, regarded as Hopf algebra in Alg_R, is a direct limit of a system (B_i) of its finitely generated Hopf subalgebras. Then there exists N such that B_N contains a finite set X' of δ-generators of B. Then we can take as X any finite subset of B_N generating it as an R-algebra. By the previous lemma $B_X^{(n)}$ is a Hopf subalgebra of B for any n. $\square$

2.3 Classification of jet operators on fields

From now on K denotes a fixed infinite field. Fact 2.1.10 yields a classification of jet operators on fields up to equivalence of operators. In characteristic zero a more general classification (for local domains) was obtained by Buium in [Bu3] and we borrow the idea of the proof from there. Throughout this section G_a is the additive group of K, G_m the multiplicative group of K and for any algebraic group G over K and a field extension $K \subset L$, $G(L)$ denotes the algebraic group over L given as before 1.3.3 (the set of L-rational points of G).

Theorem 2.3.1 *Suppose δ is a jet operator on an infinite field K. Then δ is equivalent to a difference operator or a derivation or a derivation of a power of the Frobenius map.*

By a derivation of the n-th power of Frobenius we mean an operator δ on K such that:

$$\delta(x+y) = \delta(x) + \delta(y), \quad \delta(xy) = x^q\delta(y) + y^q\delta(x),$$

where $q = p^n$, $p = char(K)$. One can check via 2.1.7 that this is a jet operator. Note that an operator δ on a field of characteristic p is a derivation if and only if $Fr^{(n)} \circ \delta$ is a derivation of the n-th power of Frobenius.

Before the proof let us look at the possible types of some operators. Let δ be an endomorphism, F be an additive polynomial with $F(0) = 0, F(1) = 1$ (note that $\delta(1) = 1$) and $\delta' = \delta - F$. We will call such a δ' an F-difference operator. It is equivalent to a difference operator. Its multiplicative rule is the following one:

$$\delta'(xy) = \delta'(x)F(y) + F(x)\delta'(y) + \delta'(x)\delta'(y) + F(x)F(y) - F(xy),$$

so an F-difference operator is an operator of the type $(X' + Y', Q)$, where:

$$(*)\ Q(X, X', Y, Y') = X'F(Y) + F(X)Y' + X'Y' + F(X)F(Y) - F(XY)$$

For $F = X$ an F-difference operator is a usual difference operator.

Now let δ be a derivation of $x \mapsto x^q$, where $q = 1$ if $char(K) = 0$ and $q = p^n$, if $char(K) = p$. So, δ is a derivation of the n-th power of Frobenius, provided $char(K) \neq 0$. Let s be a polynomial with $s(0) = 0, s(1) = 0$ and let $\delta' = \delta + s$. We will call such a δ' an s-derivation of $x \mapsto x^q$. Here we have the following multiplicative rule:

$$\delta'(xy) = \delta'(x)y^q + x^q\delta'(y) - y^q s(x) - x^q s(y) + s(xy),$$

so an s-derivation of $x \mapsto x^q$ is an operator of the type $(X' + Y', Q)$, where:

$$(**)\ Q(X, X', Y, Y') = X'Y^q + X^qY' - Y^q s(X) - X^q s(Y) + s(XY)$$

For $s = 0$ an s-derivation of the n-th power of Frobenius is a usual derivation of the n-th power of Frobenius.

Proof of Theorem 2.3.1 Assume that δ is a jet operator on K of type (P, Q).

Step I: δ is equivalent to an additive operator.
To prove this consider the structure $K_{P,Q}$. It is an algebraic ring (i.e. the ring operations are given by polynomial maps) by 2.1.2. Denote by G the additive group of $K_{P,Q}$. By 2.1.4(i) $(Id, \delta) : K \longrightarrow K_{P,Q}$ makes G a vector space over K. In particular, if $char(K) = p > 0$, then each element of G has order p.

The projection on the first coordinate gives an epimomorphism of algebraic groups $F : G \longrightarrow G_a$. Let N denote the kernel of $G \longrightarrow G_a$. We can identify the underlying affine variety of N with the affine line, so by 1.3.4 (since $(0, 0)$ is the unit in N), after this identification $N = G_a$. Explicitly, for any $a, b \in K$, we have $(0, a) \oplus (0, b) = (0, a + b)$. So G is an extension of G_a by G_a. We will prove that this extension splits.

We proceed as in the proof that the second cohomology group classifies group extensions (see Section 4.3 in [Br]). Take a natural section of F (so far not a homomorphism), $s(a) = (a, 0)$. For any $a, b \in G_a$, let $g(a, b) = (a, 0) \oplus (b, 0) \ominus (a + b, 0) \in N$, so $g(a, b) = (0, f(a, b))$ for some $f \in K[X, Y]$. We have now:

$$(a_0, 0) \oplus (0, a_1) \oplus (b_0, 0) \oplus (0, b_1) = (a_0 + b_0, 0) \oplus (0, f(a_0, b_0)) \oplus (0, a_1 + b_1) =$$

$$= (a_0 + b_0, 0) \oplus (0, f(a_0, b_0) + a_1 + b_1)$$

Consider the polynomial map:

$$\Phi : K^2 \longrightarrow K^2, \quad \Phi(a_0, a_1) = (a_0, 0) \oplus (0, a_1)$$

Since s is a section of F, Φ is a bijection and its inverse is given by polynomials, too. By definition, Φ preserves the first coordinate. Hence Φ, Φ^{-1} are of the form:

$$\Phi(a, b) = (a, r(a, b)), \quad \Phi^{-1}(a, b) = (a, t(a, b))$$

for some $r, t \in K[X, X']$. We define operations $\oplus', *'$ on K^2 in such a way that $\Phi : (K^2, \oplus', *') \longrightarrow (K^2, \oplus, *)$ is a ring homomorphism. $(K^2, \oplus', *')$ is of the form $K_{P',Q'}$ for certain $P', Q' \in K[X, X', Y, Y']$. By the computation above:

$$P'(X, X', Y, Y') = X' + Y' + f(X, Y)$$

If we define $\delta'(x) = t(x, \delta(x))$, then Φ satisfies assumptions of 2.1.10 , hence δ' is equivalent to δ.

We can assume that δ is of the type (P', Q'). Hence G is an algebraic group on K^2, with the group operation given by:

$$(a_0, a_1) \oplus (b_0, b_1) = (a_0 + b_0, a_1 + b_1 + f(a_0, b_0))$$

By [Br] (see also [Se]), f is a cocycle, and $G \longrightarrow G_a$ splits if and only if there is $w \in K[X]$ such that $f(X, Y) = w(X + Y) - w(X) - w(Y)$.

Denote by $\bar{K}$ the algebraic closure of K. By 1.3.3 $\oplus$ gives an algebraic group structure on $\bar{K}^2$, which is denoted by $G(\bar{K})$ and $G(\bar{K})$ is still an extension of $G_a(\bar{K})$ by $G_a(\bar{K})$. If $char(K) = 0$, then any such extension splits (see Corollaire on p. 172 in [Se]). If $char(K) = p > 0$, then there are nontrivial extensions called Witt groups (see Proposition 8 on p. 172 in [Se]). By 1.3.3 each element of $G(\bar{K})$ has order p. But any nontrivial extension of $G_a(\bar{K})$ by $G_a(\bar{K})$ does have elements of order bigger than p (e.g. see Exercise 8(c) on p. 67 in [Wat]). Hence $G(\bar{K}) \longrightarrow G_a(\bar{K})$ splits in positive characteristic, too.

Hence there exists $w \in \bar{K}[X]$ such that $f(X, Y) = w(X + Y) - w(X) - w(Y)$. Any additive monomial in w does not change $w(X+Y)-w(X)-w(Y)$, so we can assume that w does not have such monomials. Write $w(X) = \sum_{i \leq n} \alpha_i X^i$. Take any $i \leq n$. Since f has coefficients in K, we get that for any i the polynomial $\alpha_i(X+Y)^i - \alpha_i X^i - \alpha_i Y^i$ has coefficients in K. By our non-additivity assumption, this polynomial is non-zero. Therefore $\alpha_i \in K$ and $w \in K[X]$. Hence $G \longrightarrow G_a$ splits, so there exists a polynomial isomorphism $\Psi : G \cong G_a^2$. It preserves the first coordinate, so, by transporting the multiplicative structure from $K_{P',Q'}$ by Ψ, we get an additive operator δ' equivalent to δ in a similar way as above for Φ.

From now on we can assume that δ is additive, hence $P(X, X', Y, Y') = X' + Y'$ and in $K_{P,Q}$ we have $(a_0, a_1) \oplus (b_0, b_1) = (a_0 + b_0, a_1 + b_1)$.

Step II: $Q(X, X', Y, Y')$ is either of the form $(*)$ or of the form $(**)$
We look closer at the axiom of associativity of multiplication in $K_{P,Q}$. For all $a, a_1, b, b_1, c, c_1 \in K$ we have:

$$(a, a_1) * [(b, b_1) * (c, c_1)] = [(a, a_1) * (b, b_1)] * (c, c_1) \qquad (1)$$

By the obvious computation (1) yields:

$$Q(a \cdot b, Q(a, a_1, b, b_1), c, c_1) = Q(a, a_1, b \cdot c, Q(b, b_1, c, c_1)) \tag{2}$$

Since K is infinite (2) implies the following equality of polynomials in variables X, X', Y, Y', Z, Z':

$$Q(X \cdot Y, Q(X, X', Y, Y'), Z, Z') = Q(X, X', Y \cdot Z, Q(Y, Y', Z, Z')) \tag{3}$$

Looking at X' in (3), we get: $deg_{X'}(Q) = (deg_{X'}(Q))^2$, so $deg_{X'}(Q) \leq 1$.
Since $Q(X, X', Y, Y') = Q(Y, Y', X, X')$ (by commutativity of $K_{P,Q}$), we get $deg_{Y'}(Q) \leq 1$.
Considering the distributivity axiom in $K_{P,Q}$:

$$(a, a_1) * [(b, b_1) \oplus (c, c_1)] = (a, a_1) * (b, b_1) \oplus (a, a_1) * (c, c_1) \tag{4}$$

we get the polynomial equalities:

$$Q(X, X', Y + Z, Y' + Z') = Q(X, X', Y, Y') + Q(X, X', Z, Z')$$

$$Q(X + Y, X' + Y', Z, Z') = Q(X, X', Z, Z') + Q(Y, Y', Z, Z')$$

Hence Q, regarded as a function from $K^2 \times K^2$ into K, is biadditive. So the variables X and X' (and similarly Y, Y') are separated in Q.
Summarizing what we have got so far, Q is of the form:

$$Q(X, X', Y, Y') = X' \cdot F(Y) + Y' \cdot F(X) + \alpha \cdot X' \cdot Y' + G(X, Y), \tag{5}$$

where F is additive and G is biadditive and symmetric. Since $(0, 0)*(y_0, y_1) = (0, 0)$ for any $y_1, y_2 \in K$, we get:

$$0 = Q(0, 0, Y, Y') = 0 \cdot F(Y) + Y' \cdot F(0) + \alpha \cdot 0 \cdot Y' + G(0, Y) = Y' \cdot F(0) + G(0, Y)$$

Hence $F(0) = 0$ and $G(0, Y) = G(Y, 0) = 0$.
Similarly using that $(1, 0) * (y_0, y_1) = (y_0, y_1)$ we get:

$$Y' = Q(1, 0, Y, Y') = 0 \cdot F(Y) + Y' \cdot F(1) + \alpha \cdot 0 \cdot Y' + G(1, Y) = Y' \cdot F(1) + G(1, Y)$$

Hence $F(1) = 1$ and $G(1, Y) = G(Y, 1) = 0$.
Multiplying δ by a scalar from K, we can assume that $\alpha = 0, 1$, which will correspond to either the differential case or the difference case.

Case 1: $\alpha = 1$
Plugging $X = 0, X' = 1, Y' = Z' = 0$ in (3) we get:

$$Q(0, Q(0, 1, Y, 0), Z, 0) = Q(0, 1, YZ, Q(Y, 0, Z, 0))$$

Applying (5), we get $G(Y, Z) = F(Y)F(Z) - F(YZ)$.
Hence Q is of the form $(*)$. We know that F is additive, and $F(0) = 0, F(1) = 1$, so δ is an F-difference operator. Hence δ is equivalent to a difference operator.

Case 2: $\alpha = 0$
Denote the multiplicative group of $K_{P,Q}$ by H. By (5):

$$H = \{(a, b) : a \neq 0, \exists c\, bF(1/a) + cF(a) + G(a, 1/a) = 0\} = \{(a, b) : aF(a) \neq 0\}$$

Hence H is naturally an affine variety with the group operation given by polynomials. By embedding H into a group of matrices, we see that inverse is given by polynomials, too, therefore H is an algebraic group.

The projection on the first coordinate gives an epimorphism of algebraic groups $H \longrightarrow G_m$, because for $a \neq 0$, we have:

$$(a, \delta(a)) * (1/a, \delta(1/a)) = (1, \delta(1)) = (1, 0)$$

Denote the kernel of $H \longrightarrow G_m$ by N. Then $N = \{(1, a) : a \in K\}$. Therefore we can identify N with the affine line. After this identification N becomes G_a by 1.3.4 .

We proceed now in a similar way as in Step I. Consider $H(\bar{K})$. It is an extension of $G_m(\bar{K})$ by $G_a(\bar{K})$. By the classification of commutative linear groups (see 9.3 on p. 69 in [Wat]) any such extension is trivial. So there is a section $(Id, s) : G_m(\bar{K}) \longrightarrow H(\bar{K})$ of the projection map $H(\bar{K}) \longrightarrow G_m(\bar{K})$, which gives rise to an isomorphism of algebraic groups $\Phi : G_m(\bar{K}) \times G_a(\bar{K}) \longrightarrow H(\bar{K})$. By (5) Φ is of the form:

$$\Phi(a, a_1) = (a, s(a)) * (1, a_1) = (a, F(a)a_1 + F(1)s(a) + G(a, 1)),$$

where s is a rational function over $\bar{K}$, which has poles at most at $0 \in \bar{K}$. We will show that s is actually a polynomial function with coefficients in K. Since $F(1) = 1$ and $G(X, 1) = 0$, we get $\Phi(a, a_1) = (a, F(a)a_1 + s(a))$. Φ is a homomorphism, therefore for any $a, a_1, b, b_1 \in \bar{K}$ we have $\Phi(ab, a_1 + b_1) = \Phi(a, a_1) * \Phi(b, b_1)$, which yields:

$$F(ab)(a_1+b_1)+s(ab) = F(a)(F(b)b_1+s(b))+F(b)(F(a)a_1+s(a))+G(a,b)$$

As $\bar{K}$ is infinite, the above equality remains true in the field of rational functions after replacing a, a_1, b, b_1 by variables X, X', Y, Y'.

Considering the parts of this equality containing X', Y', we get:

$$F(XY)(X'+Y') = F(X)F(Y)(X'+Y'),$$

so F is multiplicative. As $F(1) = 1$, we have $F(X) = X^q$, where $q = 1$, if $char(K) = 0$, and $q = p^n$, if $char(K) = p > 0$.

We have also that $s(XY) = F(Y)s(X) + F(X)s(Y) + G(X, Y)$, so

$$G(X,Y) = s(XY) - Y^q s(X) - X^q s(Y)$$

If s has a pole of order n at 0, then $X \mapsto G(X, X)$ has a pole of order $2n$ at 0. But the latter is a polynomial map, so s has no poles, hence s is a polynomial map, too. Let $s(X) = \sum_i \alpha_i X^i$. Then the polynomial:

$$G(X,Y) = \sum_i \alpha_i (XY)^i - Y^q \sum_i \alpha_i X^i - X^q \sum_i \alpha_i Y^i$$

has coefficients in K. If $i \neq q$, then automatically $\alpha_i \in K$. For $i = q$, we get that $-\alpha_q X^q Y^q \in K[X, Y]$, so $\alpha_q \in K$, too. Finally, we get that $s \in K[X]$.

Since $G(X, 1) = 0$, we get $-X^q s(1) = 0$, so $s(1) = 0$. Similarly $G(0, Y) = 0$ implies $s(0) = 0$. Hence δ is an s-derivation of $x \mapsto x^q$, so δ is equivalent to a derivation of $x \mapsto x^q$. If $n = 0$, then we get a derivation, and if $n > 0$, we get a derivation of the n-th power of the Frobenius map. $\square$

In the proof of the above theorem we encountered some phenomena not present in the case of characteristic 0, considered by Buium. In characteristic 0 the first step of the proof is more immediate, while the second step practically vanishes. In characteristic p we have to analyze more deeply the multiplicative structure of the ring $K_{P,Q}$.

There is an essential difference between the case of characteristic 0 and the positive characteristic case. Namely, by 2.1.7, types of jet operators correspond to certain algebraic ring structures on K^2. Equivalence of operators corresponds to isomorphism of rings. In characteristic 0, up to isomorphism, the possible ring structures on K^2 are the product structure and the ring of dual numbers, $K[X]/(X^2)$. These ring structures correspond to difference operators (the first case) and to derivations (the second case).

In characteristic $p > 0$, there are more possible types, coming from algebraic ring structures on K^2 given by rings of Witt vectors. However there are no operators of these types, which was used in Step I of our proof. It was noted also in [Sc1].

One could wonder, if derivations of Frobenius exist. But the 0 map is a derivation of Frobenius on any field K, and by Theorem 2.1.7 it extends to a non-zero derivation of Frobenius on $K\{X\}$, which can be further extended. Also, it is easy to check that δ is a derivation if and only if $Fr \circ \delta$ is a derivation of Frobenius, but there are derivations of Frobenius, which can not be obtained in such a way.

Jet operators of other types over a ring R, like p-derivations, can occur in the non-equicharacteristic case, i.e. if R is a local ring of characteristic 0 and its residue field has positive characteristic (see [Bu2], [Bu3]).

2.4 Affine δ-varieties and δ-groups

We fix an infinite field K with a jet operator δ. From now on, Alg_δ will denote the category of δ-K-algebras (that is, $R = K$), called δ-algebras as before. In this section we will extend the "naive" definitions from algebraic geometry to the case of a field with a jet operator. This generalizes in some way the differential algebraic geometry case (see [BC], [Ca1]). We could have proceeded in a more sophisticated way, suggested in [Sc1], and pursue the theory of δ-schemes. However, as we are going to deal with the affine case exclusively, and we are not going to let the ground field vary, we content ourselves with the "naive" approach.

We will prove (Corollary 2.4.15) that any polynomial δ-algebraic group embedds into $GL_n(K)$. Using this result we show that any polynomial δ-algebraic group on K^m embedds into a unipotent algebraic group (Theorem 2.4.18), generalizing a theorem of Lazard about algebraic groups.

Definition 2.4.1 *A subset V of K^n is called δ-closed or an affine δ-variety if it is a set of zeros of some set of δ-polynomials.*

As in the case of algebraic geometry, if K is finite, then any subset of K^n is δ-closed and we would obtain just the category of finite sets. That is why we assume K is infinite.

It is obvious that any affine algebraic variety over K is an affine δ-variety, because any polynomial is a δ-polynomial (of order 0). If δ is a derivation, then δ-algebraic varieties are called affine differential algebraic varieties (see [BC]). Differential algebraic subvarieties of K are sets of solutions of differential equations.

By the discussion before 2.1.7(iii) $K\{\bar{X}\}$ is δ-algebra such that $\delta(X^{(n)}) = X^{(n+1)}$. If $\Sigma \subset K\{\bar{X}\}$, then the set of zeroes of Σ is denoted by $Z(\Sigma)$ and if $V \subset A^n$, then its δ-ideal is the set $I\{V\} = \{F \in K\{\bar{X}\} : \forall v \in V \quad F(v) = 0\}$. It is a δ-ideal in $K\{\bar{X}\}$ by 2.2.1(i) (for $B = R = K$). We note some properties of the correspondence between affine δ-varieties and δ-ideals, which are parallel to the ones known from elementary algebraic geometry and have the same proofs (see [Ha]).

Lemma 2.4.2
i) The maps $V \mapsto I\{V\}$, $\Sigma \mapsto Z(\Sigma)$ are inclusion reversing.
ii) If V is δ-closed, then $Z(I\{V\}) = V$.
iii) Suppose (Σ_i) is a family of subsets of $K\{X\}$. Then $\bigcap Z(\Sigma_i) = Z(\bigcup \Sigma_i)$.
iv) Suppose $\Sigma_1, \Sigma_2 \subset K\{X\}$, then $Z(\Sigma_1) \cup Z(\Sigma_2) = Z(\Sigma_1 \cdot \Sigma_2)$.

By ii) and iv) from the above lemma we see that δ-closed sets are the closed sets of some topology. We call it the δ-topology. If $V \subset K^n$ is δ-closed, then we make it a topological space by taking the subspace topology. The δ-topology is obviously finer than the Zariski topology. Namely, any affine algebraic variety is naturally affine δ-algebraic variety. The closure in the δ-topology is denoted by cl_δ and in the Zariski topology by cl_Z.

We continue in the same way, as in the classical case. Note that, if $V \subset K^n$ is an affine algebraic variety, then its ring of regular functions is denoted by $K[V]$ (see Section 1.3).

Definition 2.4.3
i) Suppose $V \subset K^n$, $W \subset K^m$ are affine δ-varieties and $F : V \longrightarrow W$. F is a δ-morphism if there exist $F_1, ..., F_m \in K\{X_1, ..., X_n\}$ such that $F = (F_1, ..., F_m)$ on V.
ii) If V is an affine δ-variety, then $K\{V\} = K\{\bar{X}\}/I\{V\}$ is called the algebra of δ-polynomial functions on V.

Since $I\{V\}$ is a δ-ideal in $K\{\bar{X}\}$, we get by 2.2.4 that $K\{V\}$ is a δ-algebra, too.

Our approach here differs from the classical one in the case of differential algebraic geometry ([BC], [Ca1]). Namely the classical definition of morphism allows it to be locally obtained as a quotient of differential polynomials. We discuss the difference between these two approaches at the end of this section.

It is easy to see that affine δ-varieties and δ-morphisms give rise to a category, which will be denoted by AfV_δ.

Definition 2.4.4 *A polynomial δ-algebraic group is a group object in AfV_δ.*

As in the case of δ-algebraic varieties, any affine algebraic group over K yields an example of δ-algebraic group. For a nontrivial example suppose that δ is a derivation. δ-algebraic groups are now differential algebraic groups in the sense of [BC]. Let $C = \delta^{-1}(0)$ be the field of constants of K. Consider the differential logarithmic map:

$$\mathrm{dlog} : K^* \longrightarrow K, \quad \mathrm{dlog}(x) = \delta(x)/x$$

It is a homomorphism of groups, and let $G = \mathrm{dlog}^{-1}(C)$. It can be shown that G is a nontrivial extension of the additive group in C by the multiplicative group in C. Such extensions do not exist (see Proposition 12 on p. 50 in [Se]) in the category of algebraic groups. G as a subset of K^* is a set of zeros of $F(X) = X''X - X'^2$, so it is a differential algebraic subvariety of K^2 given as $Z(YX-1, X''X - X'^2)$.

As another example of differential algebraic group (see (4) on p. 105 in [Bu4]) we take:

$$G = \left\{ \begin{bmatrix} x & 0 & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \in GL_3(K) : \; x' = xz, \; z' = 0 \right\}$$

We will look closer at this example later, after fact 2.4.7.

Both examples are actually subgroups of algebraic groups given by zeros of differential polynomials. This is not accidental. In 2.4.15 we show that any δ-algebraic group arises in such a way.

As in the algebro-geometric case any δ-morphism $F : W \longrightarrow V$ functorially induces a δ-homomorphism $F^* : K\{V\} \longrightarrow K\{W\}$, $F^*(G) = G \circ F$.

So, we obtain a contravariant functor from AfV_δ into Alg_δ. Note that any $W \in K\{X_1, ..., X_n\}$ gives a δ-polynomial map $B^n \longrightarrow B$ for any $B \in Alg_\delta$ $((b_1, ..., b_n) \mapsto W(b_1, ..., b_n))$, in particular $W : K\{V\}^n \longrightarrow K\{V\}$.

Fact 2.4.5 *Let $V \in AfV_\delta$, $F_1, ..., F_n \in K\{V\}$, $W \in K\{X_1, ..., X_n\}$ and $a \in V$. Then $(W(F_1, ..., F_n))(a) = W(F_1(a), ..., F_n(a))$.*

Proof Assume first that $n = 1$, and $W = X'$. We need to check that $(\delta(F))(a) = \delta(F(a))$. By 2.2.1(i) this is true for $V = K^n$. Take any affine δ-variety $V \subset K^n$. Then $K\{V\} = K\{\bar{X}\}/I\{V\}$ and by the remark after 2.2.4 $\delta(F/I\{V\}) = \delta(F)/I\{V\}$. So for any $F \in K\{\bar{X}\}$, we have:

$$\delta(F/I\{V\})(a) = (\delta(F)/I\{V\})(a) = \delta(F)(a) = \delta(F(a)) = \delta(F/I\{V\}(a))$$

The result follows by induction on complexity of δ-polynomial W. □

Fact 2.4.6 *Suppose V_1, V_2 are affine δ-algebraic varieties, and $\Phi : K\{V_1\} \longrightarrow K\{V_2\}$ is a δ-morphism. Then there exists a δ-morphism $F : V_2 \longrightarrow V_1$ such that $F^* = \Phi$.*

We proceed as in the algebro-geometric case ([Ha]). The proof is rather obvious, however we point out the details.

Suppose $V_1 \subset K^n$, therefore $K\{V_1\} = K\{X_1, ..., X_n\}/I\{V_1\}$. Let $F_i = \Phi(X_i/I\{V_1\})$, and define $F : V_2 \longrightarrow K^n$ as $(F_1, ..., F_n)$. We need to check that $Im(F_2) \subset V_1$. By 2.4.5, for any $W \in K\{X_1, ..., X_n\}$ and $a \in V_2$, we have $W(F(a)) = W(F)(a)$. But:

$$W(F) = W(\Phi(X_1/I\{V_1\}), ..., \Phi(X_n/I\{V_1\})) = \Phi(W/I\{V_1\})$$

Then $W(F) = 0$ for any $W \in I\{V_1\}$, so $Im(F) \subset Z(I\{V_1\}) = V_1$.

By the construction, for any i we have $F^*(X_i/I\{V_1\}) = \Phi(X_i/I\{V_1\})$. Hence $F^* = \Phi$, because they agree on a set of δ-generators of $K\{V_2\}$. □

Fact 2.4.7 *$V \mapsto K\{V\}$ is a contravariant faithfully full functor from AfV_δ into Alg_δ. It takes polynomial δ-algebraic groups into δ-Hopf algebras.*

Proof This functor is obviously contravariant. We need to prove that it induces bijections on the sets of morphisms. Since δ-polynomial functions from $K\{V\}$ (actually, just the coordinate functions) separate points, the functor induces injections on the sets of morphisms. By 2.4.6 they are also surjections, so it is faithfully full.

For the last clause, note that by definitions (2.4.4 and 2.2.2) polynomial δ-algebraic groups are exactly group objects in AfV_δ and δ-Hopf algebras are exactly cogroup objects in Alg_δ. So it is enough to show that the assumptions of 1.1.2 hold. Let $*$ be a point in K. Then $*$ is a terminal object in AfV_δ. Obviously, $K\{*\} = K$ and K is an initial object in Alg_δ. Take any $V, W \in AfV_\delta$. It remains to show that $K\{V \otimes W\} \cong K\{V\} \otimes K\{W\}$ (for the definition of a δ-algebra structure on a tensor product of δ-algebras see the discussion before 2.2.2). This follows in exactly the same way as for algebraic varieties (see [Ha]). □

We give another example from [Bu4] (see pp. 115/116). Suppose δ is a derivation and $G \subset GL_3(K)$ is a group from the last example, namely:

$$G = \left\{ \begin{bmatrix} x & 0 & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \in GL_3(K) : \ x' = xz, \ z' = 0 \right\}$$

Since as a variety G may be given in K^4 as $Z(Z', X' - XZ, XT - 1)$, we get that as an δ-algebra:

$$K\{G\} = K\{X, Y, Z, T\}/I\{G\} = K[X, X^{-1}, Z, Y, Y', Y'', ...]$$

Denote the comultiplication in $K\{G\}$ by Δ. Since multiplication is given by:

$$(a_1, b_1, c_1) \cdot (a_2, b_2, c_2) = (a_1 a_2, a_1 b_2 + b_1, c_1 + c_2)$$

we get that for example:

$$\Delta(Y)((a_1, b_1, c_1), (a_2, b_2, c_2)) = Y((a_1, b_1, c_1) \cdot (a_2, b_2, c_2)) = Y(a_1 b_2 + b_1) =$$

$$= a_1 b_2 + b_1 = (X \otimes Y + Y \otimes 1)((a_1, b_1, c_1), (a_2, b_2, c_2))$$

Hence $\Delta(Y) = X \otimes Y + Y \otimes 1$. Similarly we get the full "comultiplication table":

$$\Delta(X) = X \otimes X$$

$$\Delta(Y) = X \otimes Y + Y \otimes 1$$

$$\Delta(Z) = Z \otimes 1 + 1 \otimes Z$$

To get $\Delta(Y^{(n)})$ we can just differentiate $\Delta(Y)$. For example:

$$\Delta(Y') = \delta(X \otimes Y + Y \otimes 1) = \delta X \otimes Y + X \otimes \delta Y + \delta Y \otimes 1 + Y \otimes \delta(1) =$$

$$= XZ \otimes Y + X \otimes \delta Y + \delta Y \otimes 1$$

We can describe the image of the functor $V \mapsto K\{V\}$ in a similar way as in 4.5 of [Wat].

Fact 2.4.8 *A δ-finitely generated δ-algebra B is of the form $K\{V\}$ if and only if for each nonzero $b \in B$, there is a δ-morphism $B \longrightarrow K$ sending b to a nonzero element of K.*

Proof For any nonzero $F \in K\{V\}$, there exists $v \in V$ such that $F(v) \neq 0$. Take the evaluation map $\Phi_v : K\{V\} \longrightarrow K$, $\Phi_v(G) = G(v)$. This is δ-morphism by 2.4.5 and $\Phi_v(F) = F(v) \neq 0$.

Conversely, if B satisfies our assumptions, then write $B = K\{X_1, ..., X_n\}/I$ and let $V = Z(I)$. We want to show that $K\{V\} = B$, i.e. that $I\{V\} = I$. It is obvious that $I \subset I\{V\}$. Take any δ-morphism $\Phi : B \longrightarrow K$. Let $a = \Phi(X_1/I, ..., X_n/I)$. We see, as in the proof of 2.4.6, then $a \in V$ and $\Phi = \Phi_a$. So any $F \in B$ vanishing on V goes to 0 under each δ-morphism $B \longrightarrow K$. Hence any such F equals 0, and $I = I\{V\}$. $\square$

Corollary 2.4.9 *Let I be a δ-ideal in $K\{X_1, ..., X_n\}$, $B = K\{X_1, ..., X_n\}/I$, $V = Z(I)$, and $p : B \longrightarrow K\{V\}$ be the quotient map. Take any affine δ-algebraic variety W. Then for any δ-morphism $\Phi : B \longrightarrow K\{W\}$, there is a unique δ-morphism $\Phi' : K\{V\} \longrightarrow K\{W\}$ such that $\Phi = \Phi' \circ p$.*

Proof Let J denote the set of all elements of B going to 0 under each δ-morphism $B \longrightarrow K$. It is obviously a δ-ideal, and by 2.4.8, $J = ker(p)$. It is enough to show that $\Phi(J) = 0$. Take any $a \in J$ and let $\Psi : K\{W\} \longrightarrow K$ be a δ-morphism. Then $\Psi(\Phi(a)) = \Psi \circ \Phi(a) = 0$. Hence $\Phi(a)$ is mapped to 0 by each δ morphism into K. By 2.4.8 $\Phi(a) = 0$, so $\Phi(J) = 0$. $\square$

Now, we need to connect properties of $K[V]$ and $K\{V\}$ for an affine algebraic variety V. Note that $K[V]$ embedds into $K\{V\}$, because $I\{V\} \cap K[\bar{X}] = I(V)$. If G is an algebraic group, then this embedding is a morphism of Hopf algebras.

Lemma 2.4.10 *Suppose V is an affine algebraic variety and W is an affine δ-algebraic variety. Then for any morphism $\phi : K[V] \longrightarrow K\{W\}$ there is a unique δ-morphism $\Phi : K\{V\} \longrightarrow K\{W\}$ such that $\Phi \circ i = \phi$, where i is the embedding of $K[V]$ into $K\{V\}$.*
Moroever, if V is an algebraic group, W is a δ-algebraic group and ϕ is a morphism of Hopf algebras, then Φ is a morphism of δ-Hopf algebras, too.

Proof Suppose $V \subset K^n$, so $K[V] = K[X_1, ..., X_n]/I(V)$ and $K\{V\} = K\{X_1, ..., X_n\}/I\{V\}$. Let J denote the δ-ideal in $K\{X_1, ..., X_n\}$ generated by $I(V)$ and $B = K\{X_1, ..., X_n\}/J$. Obviously $I(V) \subset J \subset I\{V\}$, so $Z(J) = V$ and the map $i_1 : K[V] \longrightarrow B$ is also an embedding. By 2.2.1(ii) ϕ induces a unique δ-morphism $\Phi_1 : B \longrightarrow K\{W\}$ such that $\Phi_1 \circ i_1 = \phi$. By 2.4.9 we get the required Φ.

The moreover clause follows from uniqueness of Φ and the fact that i is a morphism of Hopf algebras. For example, we need to check that $\Delta \circ \Phi = (\Phi \otimes \Phi) \circ \Delta$. But both morphisms are the unique morphism coming from $\Delta \circ \phi$, so they coincide. $\square$

Now, we define prolongations of algebraic varieties.

Definition 2.4.11 *Assume $V \subset K^n$ is an affine δ-variety. We define $\Phi_m : K^n \longrightarrow K^{n(m+1)}$ and $V^{(n)}$ (the n-th prolongation of V) as:*

$$\Phi_m(x) = (x, \delta(x), ..., \delta^{(m)}(x)), \quad V^{(m)} = cl_Z(\Phi(V))$$

Prolongations of δ-varieties are nicely related with prolongations of δ-algebras.

Fact 2.4.12 *Let $V \subset A^n$ be an affine δ-variety. Let X_V denote the tuple $(X_1/I\{V\}, ..., X_n/I\{V\})$ of generators of $K\{V\}$. Then $K[V^{(m)}]$ is naturally isomorphic to $K\{V\}^{(m)}_{X_V}$ (see 2.2.5).*

Proof Note that $K\{V\}^{(m)}_{X_V}$ is presented as $K[X_1, ..., X_n, ..., X_1^{(m)}, ..., X_n^{(m)}]/J$, where $J = I\{V\} \cap K[X_1, ..., X_n, ..., X_1^{(m)}, ..., X_n^{(m)}]$.

For any $F \in J$, if we regard F as a δ-polynomial, then it vanishes on V. Hence F vanishes on $V^{(m)}$ and $J \subset I(V^{(m)})$. Take any $F \in I(V^{(m)})$. Then F regarded as a δ-polynomial vanishes on V, so $F \in J$ and $J = I(V^{(m)})$. $\square$

We will use prolongations to understand an affine δ-algebraic variety by means of an inverse system of algebraic varieties.

Fact 2.4.13 *Assume V is an affine δ-variety. Then:*
i) $(V^{(n)})$ is an inverse system of affine algebraic varieties, with connecting maps being projections.
ii) There are δ-embeddings $V \longrightarrow V^{(n)}$, which commute with the maps from the inverse system $(V^{(n)})$.

Proof Obvious from the definition of $V^{(n)}$. □

Proposition 2.4.14 *If G is an affine δ-algebraic group, then there exists a δ-algebraic group H such that G is δ-isomorphic to H and $(H^{(n)})$ is an inverse system of affine algebraic groups, and the embeddings $H \longrightarrow H^{(n)}$ are group homomorphisms.*

Proof
By 2.2.7 there exists a finite tuple Y of δ-generators of $K\{G\}$ such that $K\{G\}_Y^{(n)}$ is a Hopf algebra for each n. Choosing such a tuple of generators Y corresponds to finding $H \cong G$ such that all $H^{(n)}$'s are algebraic groups. We need to check that the δ-morphism $H \longrightarrow H^{(n)}$ is a homomorphism of groups. By 1.1.4, it is enough to check that the corresponding δ-morphism $K\{H^{(n)}\} \longrightarrow K\{H\}$ is a morphism of Hopf algebras. This follows from 2.4.10, since the inclusion morphism $K[H^{(n)}] \longrightarrow K\{H\}$ is a morphism of Hopf algebras. □

Corollary 2.4.15 *Assume K is an infinite field with a jet operator δ. Assume G is a polynomial δ-algebraic group. Then G can be embedded into $GL_n(K)$ by a δ-morphism.*

Proof By the previous proposition G embeds into an affine algebraic group. Any affine algebraic group is a Zariski closed subgroup of $GL_n(K)$ ([Wat]). □

The above result was obtained by Cassidy ([Ca1]) in the case of differentially closed field of characteristic 0.

Consider another example of a differential algebraic group (so we assume here that δ is a derivation). Suppose $char(K) = 0$ and K is algebraically closed. Then the only algebraic group structure on K^2 is the product $K^+ \times K^+$. However Cassidy showed [Ca2] that if we define:

$$(u_1, u_2) \cdot (v_1, v_2) = (u_1 + v_1, u_2 + v_2 + \sum_{i<j} a_{ij}\delta^{(i)}(u_1)\delta^{(j)}(v_1))$$

for certain $a_{ij} \in K$, then we get a new differential algebraic group structure on K^2.

By 2.4.15 each δ-algebraic group living on an affine space is δ-linear. We will show that such a group is unipotent (i.e. δ-embeds into a unipotent algebraic group), generalizing a result of Lazard [La]. This generalization of the Lazard theorem was obtained with Anand Pillay [KP1] in the case of differentially closed field of characteristic 0, and with Marcin Chalupnik [CK] in a much more general case of any differential field. Also the proof in the case of transformally closed fields is contained in [KP2].

There is another obstacle coming from the "naivety" of our definition, which is not present in the case of algebraic geometry. Namely, we can not a priori guarantee that $K\{A^1\} = K\{X\}$, even in the case where K is infinite, since there can occur a nonzero δ-polynomial, which vanishes on the whole K. For instance if we take $\delta = 0$, then $f = X'$ is a trivial example of such a polynomial. However in such a case δ-geometry reduces to algebraic geometry. We will see that essentially it is always the case. We will need the lemma below about the structure of "δ-algebraic" fields with a jet operator δ, for types of δ from 2.3.1 . It is well-known for derivations, see Theorem 3 in [Sei]. However the proof in [Sei] does not generalize to the case of derivation of Frobenius. Item (ii) below was obtained by Rahim Moosa [Mo] by a nice algebro-geometric argument, however it follows also from classical algebra.

Lemma 2.4.16
i) Assume K is infinite and δ is a derivation or a derivation of some power of the Frobenius map. Assume also that there is a non-zero δ-polynomial W of order n vanishing on K. Then there exists a δ-polynomial W_0 of order $< n$, such that $X^{(n)} + W_0$ vanishes on K.
ii) Assume δ is an endomorphism and there is $F \in K[X_0, ..., X_n]$ of order n such that for any $a \in K$, $F(a, \delta(a), ..., \delta^{(n)}(a)) = 0$ and n is minimal. Then, in the characterictic 0 case, $\delta^{(n)} = Id$, and in the case of characteristic $p > 0$, $\delta^{(n)p^m} = Id$, or $\delta^{(n)} = Fr^m$ for some m.

Proof
i) We want to give a uniform proof for derivations and derivations of a power of Frobenius. So we adopt an a bit awkward convention that a derivation is a derivation of the 0-th power of Frobenius, which is identity also in characteristic 0. Assume δ is a derivation of the m-th power of Frobenius.

Let n be minimal such that there exists a non-zero differential polynomial W of order n vanishing on K. Let G_a denotes the additive group of K. Consider a map:

$$\Phi : G_a \longrightarrow G_a^{n+1}, \quad \Phi(x) = (x, \delta(x), ..., \delta^{(n)}(x))$$

Since δ is additive, Φ is a homomorphism. By Theorem 18 in Chapter VIII from [L], there is a polynomial $H \in K[X_0, ..., X_n]$ of the form $H = \sum_{i,j} d_{i,j} X_i^{p^j}$, which vanishes on $\Phi(K)$.

Hence we get a δ-polynomial $F(X) = \sum_{i,j} d_{i,j} X^{(i)^{p^j}}$, which vanishes on K.

We can assume F has the minimal possible number of monomials, and they are of minimal degrees.

The next step is to show that for any i there exists at most one j such that $d_{i,j} \neq 0$. Suppose not, and take $i, j < k$ such that $d_{i,j} \neq 0, d_{i,k} \neq 0$. Note that we have assumed that δ is a derivation of the m-th power of Frobenius, and m may equal 0 to include the case of derivation. Let $q = p^m$.

Let $C = \{c \in K : \delta(c) = 0\}$. If $char(K) = 0$, then $\mathbb{Q} \subset C$, and if $char(K) = p > 0$, then $K^p \subset C$ (note that for any $a \in K$, $\delta(a^i) = ia^{q(i-1)}\delta(a)$). In either case C is infinite, since K is assumed to be infinite. For $c \in C, k \in K$, we have $\delta(ck) = c^q \delta(k)$ and $\delta^{(i)}(ck) = c^{qi}\delta(k)$.

Take $c \in C$ such that $c^{qip^k} \neq c^{qip^j}$. Consider the polynomial $F_1(X) = F(cX) - c^{qip^k} F(X)$. Then obviously, F_1 vanishes on K, has no more monomials than F, and has no term $X^{(i)^{p^k}}$. This contradicts the minimality assumptions made on F.

Hence F is of the form $F = \sum_{i \leq n} d_i X^{(i)^{q_i}}$, where q_i is a power of p.

By a similar argument as above $q_n \leq q_i$ for any other q_i (if not, then for a suitable $c \in C$, $F(cX) - c^{qnq_n} F(X)$ is non-zero, vanishes on K and has order $< n$, contradicting the choice of n).

We want $q_n = 1$. Suppose not. We can assume that $K \neq K^{q_n}$, since if K is perfect, then δ is already 0. View K as a K^l-vector space, and let $\{b_1, \ldots, b_k\}$ be the maximal subset of $\{d_0, ..., d_{n-1}, 1\}$, which is linearly independent over K^l (we assume that $d_n = 1$). Then $F = \sum b_j (L_j(X, \ldots, X^{(n)}))^{q_n} = 0$ for some δ-polynomials L_i of lower degree that $\deg(F)$ (we use here that j_n

is not bigger than any other j_i). Since F vanishes on K and the b_j's are linearly independent over K^{q_n}, we get that all L_j's vanish on K, contradicting minimality of $\deg(F)$.

ii) Assume $char(K) = p$, a prime number or 0. As in i) we get $H(X) = \sum_{i,j} d_{i,j} X^{(i)^{p^j}}$ (all $p^j = 1$ if $char(K) = 0$) such that $H(a, \delta(a), ..., \delta^{(n)}(a)) = 0$ for any $a \in K$. Hence a set of endomorphisms $(((\delta^i)^{p^j})_{ij})$ is linearly dependent over K. By the theorem of Artin about linear independence of characters (Theorem 7 in Chapter VIII from [L]) we get that:

$$(\delta^{(i)})^{p^j} = (\delta^{(i')})^{p^{j'}}$$

for some $i, i' \leq n$ and j, j' such that $i \neq i'$ or $j \neq j'$. Since δ is $1-1$ and n is minimal, we get that $i = 0$ and $i' = n$. Hence:

$$Fr^j = (\delta^{(n)})^{p^{j'}}$$

If $j = j'$, then we get $\delta^{(n)} = Id$. Let $j \neq j'$ and we can assume that either j or j' equals 0. Let $m = \max(j, j')$. Then we have that either $(\delta^{(n)})^{p^m} = Id$ or $\delta^{(n)} = Fr^m$. □

With not much additional effort, we could get that if δ is a derivation satisfying assumptions of the above lemma, then in the characteristic 0 case $\delta = 0$, and in the case of characteristic $p > 0$ a δ-polynomial of the form: $X^{(p^n)} + d_{m-1}X^{(p^{n-1})} + ... + d_0 X$ vanishes on K (see Exercise 3 on p. 190 in [Ja]). We will not use this later.

But it is easy to find a field K of positive characteristic with nonzero derivation, and a nonzero differential polynomial vanishing on K:
Suppose $[K : K^p] = n < \infty$. Take $a_1, ..., a_m \in K$, a p-basis of K. Now, we can define a derivation δ on K extending $a_1 \mapsto 1, a_2 \mapsto a_1, ..., a_n \mapsto a_{n-1}$. This is obviously a nonzero derivation, but if $\sum \alpha_i X^i$ is the characteristic polynomial of δ, regarded as a K^p-linear map, then $\sum \alpha_i X^{(i)}$ is a differential polynomial vanishing on K.

Fact 2.4.17 *For any m, $K\{K^m\}$ as an R-algebra is a direct limit of its finitely generated subalgebras isomorphic to rings of polynomials.*

Proof To avoid symbols like $K\{K\}$, we denote in this proof K^m by A^m.

As $K\{A^m\} \cong K\{A^1\}^{\otimes m}$, we can assume that $m = 1$.

Suppose first that the only δ-polynomial vanishing on K is the 0 polynomial. Then $K\{A^1\}$ is $K\{X\}$, which obviously satisfies the conclusion of the fact.

Suppose now, that there is a non-zero δ-polynomial vanishing on K. We want to use the classification theorem 2.3.1 . Note that if δ is equivalent to δ', then $K^\delta\{A^1\}$ is isomorphic over K, to $K^{\delta'}\{A^1\}$. Suppose n is smallest such that there exists a δ-polynomial of order n vanishing on K. We consider the following two cases:

Case 1: δ is a derivation or a derivation of a power of Frobenius.
By 2.4.16(i), we can assume that $W = X^{(n)} + W_0$, for a δ-polynomial W_0 such that $\mathrm{ord}(W_0) < n$. Since for any i, $W(X^{(i)})$ vanishes on K, and no δ-polynomial of order smaller than n vanishes on K, we get that $K\{A^1\} \cong K[X, X', ..., X^{(n-1)}]$.

Case 2: δ is a difference operator.
Let $\delta' = \delta + Id$. It is an endomorphism (see an example after 2.1.1). Suppose first that $char(K) = 0$. By 2.4.16(ii), $\delta'^{(n)} = Id$, hence $(\delta + Id)^{(n)} = Id$. Therefore a δ-polynomial $\sum_{i=1}^{n} \begin{pmatrix} n \\ i \end{pmatrix} X^{(i)}$ vanishes on K. Then, as in Case 1, $K\{A^1\} \cong K[X, X', ..., X^{(n-1)}]$.

Suppose now that $char(K) = p > 0$. By 2.4.16(ii), either $\delta'^{(n)^{p^m}} = Id$, or $\delta'^{(n)} = Fr^m$ for some m. In the latter case we get that $K\{A^1\} \cong K[X, X', ..., X^{(n-1)}]$ as before. Hence we assume that $(\delta + Id)^{(n)^{p^m}} = Id$. We get that a δ-polynomial:

$$(*) \quad \sum_{i=0}^{n} \begin{pmatrix} n \\ i \end{pmatrix} X^{(i)^{p^m}} - X = (X^{(n)} + X)^{p^m} - X + \sum_{i=1}^{n-1} \begin{pmatrix} n \\ i \end{pmatrix} X^{(i)^{p^m}}$$

vanishes on K.

Let B_j be the subalgebra of $K\{A^1\}$ generated by $X/I\{A^1\}, ..., X^{(j)}/I\{A^1\}$. It is clear that B_j embeds into B_{j+1} for any j. For $j < n$, B_j is isomorphic to a ring of polynomials $K[X, X', ..., X^{(j)}]$. If $j = n + s$ for some $s \geq 0$, then the following polynomial vanishes on K (by substituting X by $X^{(s)}$ in $(*)$):

$$(X^{(j)} + X^{(s)})^{p^m} - X^{(s)} + \sum_{i=s+1}^{j-1} \begin{pmatrix} n \\ i \end{pmatrix} X^{(i)^{p^m}}$$

Inductively, we get that B_j is generated by $(X^{(j)}+X^{(s)}, X^{(s+1)}, ..., X^{(j-1)})$, so B_j is isomorphic to the ring of polynomials of n variables, since B_{n-1}, which is isomorphic to the ring of polynomials of n variables embeds into B_j.

We are done, since $K\{A^1\} = \text{colim } B_i$. $\square$

Now we are in a position to prove our generalization of the Lazard theorem.

Theorem 2.4.18 *Each δ-algebraic group G living on an affine space can be embedded into a unipotent algebraic group.*

Proof By 2.4.14 there exists a δ-algebraic group H such that $G \cong H$, $(H^{(n)})$ is an inverse system of algebraic groups, $K\{G\} \cong K\{H\}$ as δ-algebras, $K\{H\} = \text{colim } (K[H^{(n)}])$ as K-algebras and $H \longrightarrow H^{(n)}$ is an embedding. If the underlying δ-variety of G is A^m, then by 2.4.17 we have $K\{G\} = \text{colim } (B_i)$ as K-algebras, where each B_i is isomorphic to a ring of polynomials. Hence, as K-algebras, $\text{colim } (K[H^{(n)}]) \cong \text{colim } (B_i)$. By A.2 each $H^{(n)}$ is unipotent, hence G embeds into a unipotent group. $\square$

It should be remarked that if δ is a derivation then our definition of morphism is simpler than the usual one (see [BC], [Ca1]), which asserts that a morphism is locally given by quotients of polynomial functions. We will call a morphism in the above sense, a BC-morphism. In the case of algebraic geometry BC-morphisms and morphisms coincide over an algebraically closed field, but for differential algebraic geometry the two definitions are not the same, even if the field is differentially closed (for the definition see Section 3.2), since there can be everywhere defined differential rational functions, which are not differential polynomials. The following example is from [Ca1]: take $V = Z(X' - X)$, then $f(x) = 1/(x+1)$ is everywhere defined on V, and it can not be represented by a polynomial function on V.

In [BC] and [Ca1] an affine differential algebraic group means a group object in the category of affine δ-varieties and BC-morphisms. Our δ-polynomial algebraic groups correspond exactly to their polynomial (or strictly affine) differential algebraic groups. In fact the definition of BC-morphism is better, since it can be used to define non-affine δ-schemes, by glueing along δ-rational maps. However we do not deal in this thesis with non-affine varieties, so we decided to stick with a simpler definition. A differential algebraic group satisfying our definition is called a strictly-affine group in [Ca1]. It was shown in [Ca1] (Proposition 12) that a strictly-affine group δ-embeds into $GL_n(K)$

for K differentially closed of characteristic 0. So our results may be regarded as a generalization of the Cassidy result to any jet operator. Hrushovski and Sokolovic proved in [HS] that any differential algebraic group of "finite dimension" can be embedded into an affine space, so differential algebraic groups of finite dimension are affine, but there are many such groups which are not strictly-affine (e.g. a group of constant points on an abelian variety defined over $\mathbb{Q}$).

Nevertheless, in this more general setting our version of the Lazard theorem is still true, as was pointed out by Alexandru Buium during a model theory seminar at the University of Illinois at Urbana-Champaign.

Lemma 2.4.19 *Suppose V is a differential affine variety such that $K\{V\}$ is UFD. Then any BC-morphism $\phi : V \longrightarrow K$ is of the form F/G for $F, G \in K\{V\}$ such that G has no zeros in V.*

Proof Suppose $F : V \longrightarrow K$ is a BC-morphism. Let $V = \bigcup U_i$ and $F_i, G_i \in K\{V\}$ such that $F = F_i/G_i$ on U_i. We can assume that $\gcd(F_i, G_i) = 1$. Take any $i \neq j$. Since $K\{V\}$ is domain, any open subset in V is dense. So $F_iG_j = G_iF_j$ on $U_i \cap U_j$ implies $F_iG_j = G_iF_j$. Since $\gcd(F_i, G_i) = \gcd(F_j, G_j) = 1$, we get $F_i = F_j$ and $G_i = G_j$ for any i, j. □

Corollary 2.4.20 *If K is differentially closed, then any δ-algebraic group structure on K^n is a polynomial differential algebraic group. Hence the Lazard theorem is true for differential algebraic groups.*

Proof K is differentially closed, so any non-constant δ-polynomial has a zero in K. Hence $K\{K^n\}$ is isomorphic as an R-algebra to a ring of polynomials in infinitely many variable. Therefore $K\{K^n\}$ is UFD, so by the previous lemma any BC-morphism on K^n is of the form F/G for δ-polynomials F, G. Using that K is differentially closed again, we get that $G = 1$ and the result follows from 2.4.18. □

3 Fields with jet operators – some model theory

3.1 Groups type-definable in simple and stable theories

As in this section we are going to deal with groups definable in some theories of fields with jet operators, we recall some model-theoretical notions and facts concerning definable groups. We fix a complete theory T, and its monster model $\mathcal{M}$. A group G is called type-definable if its underlying set as well as the graphs of group operation and inverse are type-definable. In the study of groups definable in simple and stable theories the crucial notion is that of generic type. We fix a type-definable group G defined over $\emptyset$.

Definition 3.1.1 ([Pi4]) *Assume T is simple, A is a small subset of $\mathcal{M}$, and p is the type over A of an element of G. Then p is a generic type of G, if for any $b \in G$ and $a \models p$ such that $a \mathop{\smile\!\!\!\!\!\!|}_A b$, we have $b \cdot a \mathop{\smile\!\!\!\!\!\!|} A \cup \{b\}$.*

G is connected if it does not have definable subgroups of finite index. We say that $a \in G$ is generic over A, if $tp(a/A)$ is generic, and that a is generic, if $tp(a)$ is generic.

Fact 3.1.2 *Assume T is simple. Then:*
i) Generic types exist.
ii) If T is stable, then G is connected if and only if it has a unique generic type.

If G is a connected group and T is stable, then we have an "independent group operation" on its generic type p, which is stationary: for $a, b \models p$, with $a \mathop{\smile\!\!\!\!\!\!|} b$, we have $a \cdot b \models p$, $a \cdot b \mathop{\smile\!\!\!\!\!\!|} a$, $a \cdot b \mathop{\smile\!\!\!\!\!\!|} b$ and $\cdot$ is associative on independent triples of realizations of p. Such a partial operation on a stationary type is called a group chunk on p. There is a natural notion of morphism of group chunks: for $(p, \bullet), (q, \bullet)$ group chunks f is a morphism between them, if f is a type-definable function defined over $\emptyset$ between $p(\mathcal{M})$ and $q(\mathcal{M})$ such that for independent $a, b \models p$, we have $f(a \bullet b) = f(a) \bullet f(b)$ (note that $a \mathop{\smile\!\!\!\!\!\!|} b$ implies $f(a) \mathop{\smile\!\!\!\!\!\!|} f(b)$). So, we obtain a category of group chunks. We get a functor from the category of connected type-definable groups into a category of group chunks, a group is mapped into its generic type. We will use the following theorems of Hrushovski (see [Hr1]), which shows among others (iii) that the above functor gives an equivalence of categories.

Theorem 3.1.3 *Assume T is stable. Then:*
i) Any $*$-definable group is an inverse limit of definable groups.
ii) Suppose $(p, \bullet)$ is a ($*$-)group chunk. Then there is a ($*$-)definable group $(G, \cdot)$ and a type-definable embedding $f : p(\mathcal{M}) \longrightarrow G$ such that for independent $a, b \models p$, $f(a \bullet b) = f(a) \cdot f(b)$.
iii) Let $f : (p, \bullet) \longrightarrow (q, \bullet)$ be a morphism of group chunks. Take a connected type-definable group G (resp. H) such that p (resp. q) is the generic type of G (resp. H). Then there is a type definable homomorphism $F : G \longrightarrow H$ such that $F = f$ on $p(\mathcal{M})$.

Proof (i) is 3.4 from [Hr1] and (ii) is Theorem 1 from [Hr1] in the case of finite tuples. The proof easily generalizes to $*$-tuples. (iii) is not stated there, however easily follows. If f is a morphism between group chunks p and q, then the graph of f is a group chunk. By (ii) p is a generic type of a type-definable group G, q is a generic type of a type-definable group H, and the graph of f is a generic type of V, a type-definable subgroup of $G \times H$. Then V is the graph of a type-definable group homomorphism F and $F = f$ on $p(\mathcal{M})$. $\square$

Hrushovski has showed (see [Pi1]) that we can recover a group even from the algebraic relations between small subsets of a monster model . The statement of the Hrushovski group existence theorem below comes from [KP2]. For the notion of canonical base (Cb) in stable theories see [Pi1] for stable and [HKP] for simple theories. The assumptions in the theorem below concerning canonical bases say that, in some sense, the set $\{a, b, c, x, y, z\}$ is minimal.

Theorem 3.1.4 *Let M be a saturated model of the stable theory T. Let a, b, c, x, y, z be $*$-tuples of length strictly less than the cardinality of M. Suppose that the following are true:*
(i) $acl(M, a, b) = acl(M, a, c) = acl(M, b, c)$,
(ii) $acl(M, a, x) = acl(M, a, y)$ and $Cb(stp(x, y/M, a))$ is interalgebraic with a over M.
(iii) As in (ii) with b, z, y in place of a, x, y.
(iv) As in (ii) with c, z, x in place of a, x, y.
(v) Other than $\{a, b, c\}$, $\{a, x, y\}$, $\{b, z, y\}$ and $\{c, z, x\}$, any 3-element subset

of $\{a,b,c,x,y,z\}$ is M-independent.
Then there is a $*$-definable (over M) homogeneous space (G,S) and generic (over M) elements a',b',c' of G and x',y',z' of S such that $a'\cdot x' = y'$, $b'\cdot y' = z'$, and $c'\cdot x' = z'$ (so $a'\cdot b' = c'$) such that each nonprimed element is interalgebraic over M with the corresponding primed element.

We call a set $X = \{a,b,c,x,y,z\}$ satisfying assumptions of 3.1.4, a group configuration. If $X' = \{a',b',c',x',y',z'\}$ is another group configuration, then we say that X is interalgebraic with X', if for any $\alpha \in X$, $acl(\alpha) = acl(\alpha')$, where α' is the corresponding element from X'.

It is not known if the group existence theorem for simple theories is true.

We will need a technical fact from [KP2] about algebraic closure inside a group definable in simple theory.

Proposition 3.1.5 *Suppose that G,H are groups type-definable over a small model M and that there are elements a,b,c of G and a',b',c' of H such that*
(i) a,b are generic independent over M.
(ii) $a\cdot b = c$ and $a'\cdot b' = c'$,
(iii) a is interalgebraic with a' over M, and similarly for b,b' and c,c'.
Then there is a type-definable over M subgroup G_1 of bounded index in G and a type-definable over M subgroup H_1 of H, and a type-definable over M isomorphism f between G_1/K_1 and H_1/L_1 where K_1 is a finite normal subgroup of G_1, and L_1 is a finite normal subgroup of H_1.

For Z, a ($*$-)type-definable set over $\emptyset$, let $[Z]$ denote the set of complete types over $\emptyset$, which have realizations in Z. If we take such sets as closed sets we get a compact topology on the set of types, which is called the Stone topology. Let X, Y be type-definable sets, and if $X \longrightarrow Y$ is a type-definable map between them, then we have an induced map $[X] \longrightarrow [Y]$, which is continuous in the Stone topology.

Lemma 3.1.6 *Assume T is simple, and (G_i, f_{ij}) is an inverse limit of type-definable groups in T such that all f_{ij}'s are onto. Let $G^* = lim(G_i)$ and regard G^* as a $*$-definable group. Suppose $p^* \in [G^*]$, and denote by p_i its image in $[G_i]$. Then p^* is a generic type of G^* if and only if for each n, p_n is a generic type of G_n.*

Proof Denote the map $G^* \longrightarrow G_i$ by f_i. First we note that for any $a^* \in G^*$, $dcl(a^*) = dcl((f_i(a^*))_i)$ and for $i > j$, $f_j(a^*) = f_{ij}(f_i(a^*)) \in dcl(f_i(a^*))$.

Hence for $a^*, b^* \in G^*$ we have:

$$(\diamond) \quad a^* \perp b^* \iff (f_i(a^*))_i \perp (f_i(b^*))_i \iff \text{for each } i,\ f_i(a^*) \perp f_i(b^*)$$

$\Longrightarrow$
Let $b \in G_i$, $a \models p_i$ be such that $a \perp b$. We have to show that $b \cdot a \perp b$.

There exists $\alpha^* \in G^*$ such that $f_i(\alpha^*) = a$ and $tp(\alpha^*)$ is a generic type of G^*. There is also $a^* \in G$ such that $tp(a^*/a) = tp(\alpha^*/a)$, and $a^* \perp_a b$. Then still $f_i(a^*) = a$ and $tp(a^*)$ is a generic type of G^*. But, since $a \perp b$, we have $a^* \perp b$ by the transitivity of $\perp$. Take $b^* \in f_i^{-1}(b)$, such that $b^* \perp_b a^*$. Then $b^* \perp a^*$ from the transitivity again. Since $tp(a^*)$ is generic, $b^* \cdot a^* \perp b^*$, so $f_i(b^* \cdot a^*) = b \cdot a$ is independent from b by $(\diamond)$, which shows that p_i is generic.
$\Longleftarrow$
Let $b^* \in G^*$, $a^* \models p^*$ be such that $a^* \perp b^*$. We have to show that $b^* \cdot a^* \perp b^*$.

For each i, $tp(f_i(a^*))$ is generic by the assumption and $f_i(a^*) \perp f_i(b^*)$ by $(\diamond)$. Thus $f_i(b^*) \cdot f_i(a^*) \perp f_i(a^*)$. Hence for each i, $f_i(b^* \cdot a^*) \perp f_i(a^*)$, so by $(\diamond)$, $b^* \cdot a^* \perp a^*$, and p^* is generic. $\square$

Definable groups are more convenient to work with, than type-definable groups; for instance if we quotient by a type-definable group, then the resulting group does not have to be even $*$-definable. Hrushovski has proved (see the remark after Theorem 2 in [Hr1]) that the situation is smoothened if the theory is stable.

Theorem 3.1.7 *A type definable group in a stable theory is an intersection of definable groups.*

A theory T is ω-stable, if there are countably many complete types over any countable set. Groups definable in ω-stable theories behave particularly well: for instance they satisfy the descending chain condition on definable subgroups, so (by 3.1.7), any type-definable group in an ω-stable theory is definable. Wagner has shown (see [Wa] Theorem 5.5.4) that 3.1.7 remains true for certain simple theories.

Theorem 3.1.8 *A type definable group in a supersimple theory is an intersection of definable groups.*

For definition of supersimple see [KiP]. It is not known, if 3.1.7 holds for groups type-definable in simple theories. By 3.1.8 if we add to the assumptions of 3.1.5 that T is supersimple, then we obtain a definable group of finite index, and a definable map.

We will need a well-known fact about non-generic types in groups definable in simple theories.

Fact 3.1.9 *Suppose G is a group type-definable in a simple theory and p is a type of elements of G, which is not generic. Then for any $a \models p$ and $b \in G$ generic such that $b \perp a$, $b \cdot a$ is not independent from b and $b \cdot a$ is generic.*

Proof Suppose not, so $b \cdot a \perp b$. Then $b \cdot a \perp b^{-1}$ and b^{-1} is generic by 3.4 from [Pi4]. By 3.3 from [Pi4] b^{-1} is generic over $b \cdot a$. By 3.2 from [Pi4] (using that right-generic is left generic) a is generic over b^{-1}, so a is generic by 3.3 from [Pi4] again, a contradiction. Similarly $b \cdot a$ is generic. □

3.2 Model-theoretical Prolongations

In this section we obtain some results on existence of model companions of theories of fields with jet operators. Then, we introduce model-theoretic prolongations. In the previous chapter we applied prolongations of δ-algebras to get embeddings of polynomial δ-algebraic groups into linear groups. We include two results of Pillay [Pi2] and Pillay and myself [KP2] showing how model-theoretic prolongations may be applied to get analogous results for definable groups in some cases.

In model theory model companions of some theories of fields with additional operators played an important role for development of geometric model theory. Also they were crucial for the applications of model theory in diophantine geometry (see [Hr2], [Hr3], [HP], [Sc2], [Sc3]).

Recall that the theory of difference fields (fields with an endomorphisms) has a model companion and this model companion is denoted by $ACFA$. Axioms of $ACFA$ may be expressed in the following way [CH]. $(K, \delta) \models ACFA_p$ if K is an algebraically closed difference field of characteristic p, and for any irreducible K-variety V, and any $W \subset V \times \delta(V)$, an irreducible subvariety projecting generically on V and $\delta(V)$, the graph of δ meets each Zariski open subset of W. Such fields are called transformally closed.

The theory of differential fields (fields with a derivation) has a model companion and this model companion is denoted by DCF. For any pair of differential polynomials F, G we have an axiom saying that if $\mathrm{ord}(F) < \mathrm{ord}(G)$ and the separant of G (a partial derivative of G with respect to $X^{(ord(G))}$) is non-zero, then there is a such that $F(a) \neq 0$ and $G(a) = 0$ (see [Wo]). Models of DCF are called differentially closed fields.

So it is natural to inquire if the theory of fields with jet operators of a fixed type has a model companion. There was a hope we would get a new model compete theory of fields with operators.

Theorem 3.2.1 *Assume δ is a jet operator of type (P, Q) on a field K. Let T be a theory of fields extending K with jet operators of type (P, Q).*
1) If δ is equivalent to a derivation, then the model companion $\bar{T}$ of T exists and is biinterpretable with DCF.
2) If δ is equivalent to a difference operator, then the model companion $\bar{T}$ of T exists and is biinterpretable with $ACFA$.

Proof
(1) Take a polynomial $f \in K[X]$ and an invertible element $\lambda \in K^*$ such that $\delta' = \lambda\delta + f$ is a derivation. By 2.1.10 $K_{P,Q} \cong K[X]/X^2$ ($K[X]/X^2$ is the structure ring of derivations), this isomorphism is given by polynomials and preserves the first coordinate. Then for any field M containing λ and parameters of f, we have an isomorphism as in 2.1.10: $M_{P,Q} \cong M[X]/X^2$. Hence (by 2.1.10), δ_M is an operator of type (P, Q) on M if and only if $\delta'_M = \lambda\delta_M + f$ is a derivation and (M, δ_M) is existentially closed if and only if (M, δ'_M) is existentially closed. We know that DCF is the model companion of the theory of differential fields. So the class of existentially closed models of T is elementary, its theory is $\bar{T}$, the model companion of T, and $\bar{T}$ is biintepretable with DCF (strictly speaking, biintepretable with DCF_K, the theory of differentially closed fields extending K).
(2) A similar proof. A difference operator can be transformed into an endomorphism. □

By Theorem 2.3.1, every jet operator of type (P, Q) is equivalent either to derivation, difference operator or a derivation of a power of Frobenius. In the first two cases the above theorem shows that the theory T of fields with jet operators of type (P, Q) has a model companion. The remaining case is that of a derivation of a power of Frobenius. Unfortunately, I did not manage to settle the problem if the model companion exists in this case.

Let $\bar{T}$ be DCF_0 or $ACFA$. For the rest of the paper we assume that $K \models \bar{T}$. Then acl^- will mean acl computed in the pure field K. Similarly for dcl^- and $\downarrow^-$. For a tuple a from K, a^* denotes $(\delta^{(i)}(a))_{i<\omega}$ for $K \models DCF_0$, and $(\delta^{(i)}(a))_{i\in Z}$ for $K \models ACFA$. If $p = tp(a)$, then p^* denotes $tp^-(a^*)$. The theorem below was proved in the $ACFA$-case in [CH], and in the DCF_0-case in [Pi3].

Theorem 3.2.2
i) For $a, A, B \subset K$, $acl(a) = acl^-(a^*)$, and $a \downarrow_B A$ if and only if $a^* \downarrow^-_{B^*} A^*$.
ii) Suppose $K \models DCF_0$. Then $dcl(a) = dcl^-(a^*)$.

We define prolongations of a complete type in K.

Definition 3.2.3 *If $p \in S(K)$, then $p^{(n)} = tp^-(a, \delta a, ..., \delta^{(n)} a)$ and $p^* = tp(a^*)$ for any $a \models p$.*

Note that p^* may be regarded as an inverse limit of $(p^{(n)})$.

Proposition 3.2.4
i) If X is a group configuration in $\bar{T}$, then X^* is a $*$-group configuration in ACF_p.
ii) If $K \models DCF_0$ and p, a stationary type in K, is a group chunk, then p^* is a $*$-group chunk in ACF_p, and there is a $*$-group chunk embedding of $p(K)$ into $p^*(K)$.

Proof
i) follows from 3.2.2 .
ii) If $a, b \models p$, and $a \downarrow b$, then $a^*, b^* \models p^*$, and $a^* \downarrow^- b^*$, by 3.2.2 . Define $a^* \cdot b^*$ as $(a \cdot b)^*$. Since $(a \cdot b) \in dcl(a, b) = dcl^-(a^*, b^*)$, we obtain a group chunk structure on p^*. The map $p(K) \ni a \mapsto a^* \in p^*(K)$ is the required embedding. $\square$

There were two ingredients in the proof of embeddability of an affine δ-algebraic group into an algebraic group: the prolongation, and a certain property (1.3.2) of Hopf algebras. The prolongations are still present in the definable setting, and the Hopf algebra argument can be replaced by 3.1.3(i). Item (i) in the following theorem was proved by Pillay in [Pi1], and (ii) was proved in [KP2].

Theorem 3.2.5
i) Every connected group G definable in DCF_0 can be definably embedded into an algebraic group.
ii) For each group G definable in $ACFA_p$ (p prime or 0), there is a finite index subgroup H of G, and a finite normal subgroup F of H such that H/F definably embeds into an algebraic group.

Proof
i) Take p, the generic type of G. Then p is a group chunk, so by 3.3.4(ii), p^* is a group chunk, and there is a group chunk embedding of $p(K)$ into $p^*(K)$. By 3.1.3(ii) there exists G^*, a $*$-definable group in ACF such that p^* is a generic type of G^*. By 3.1.3(iii), $p(K) \longrightarrow p^*(K)$ extends to a type-definable embedding of G into G^*. By 3.1.3(i) G^* is an inverse limit of a system (G_i) of definable groups, and by 1.3.5 we can assume that the G_i's are algebraic. Denote by α_n the definable homomorphism $G \longrightarrow G_n$. Then $\bigcap\{ker(\alpha_n) : n < \omega\} = \{0\}$. Since K is saturated, there is N such that $ker(\alpha_N) = 0$. Hence α_N is a type-definable embedding of G into an algebraic group G_N. Since DCF_0 is ω-stable, α_N is definable.

ii) Let p be a generic type of G, and a, b, x independent realizations of p. If $c = a \cdot b, y = a \cdot x, z = c \cdot x$, then (a, b, c, x, y, z) is a group configuration. By 3.3.4(i), $(a^*, b^*, c^*, x^*, y^*, z^*)$ is a $*$-group configuration in ACF. By 3.1.4, there is a $*$-definable group G^* in ACF and $\bar{a}, \bar{b} \in G^*$ such that if $\bar{c} = \bar{a} \cdot \bar{b}$, then:

$$acl^-(\bar{a}) = acl^-(a^*),\ acl^-(\bar{b}) = acl^-(b^*),\ acl^-(\bar{c}) = acl^-(c^*)$$

As in the proof of (i), we can assume that $G^* = lim(G_i)$, where the G_i's are algebraic groups. Denote the map $G^* \longrightarrow G_n$ by ϕ_n. Let x be any of a, b, c and denote $\phi_n(x)$ by x_n. Then as in the proof of 3.1.6 $dcl^-(\bar{x}) = dcl^-((x_n)_n)$. Hence:

$$acl((x_n)_n) = acl(\bar{x}) = acl(x^*) = acl(x)$$

But x is a finite tuple, so there is N such that $acl(x_N) = acl(x)$. Since $c_N = a_N \cdot b_N$, the assumptions of 3.1.5 are satisfied and we get the required embedding. □

Now, we restrict our attention to groups, which are type-definable in stable theories and connected. We focus on a condition on stable groups introduced by Newelski. In [Ne] he was interested in the "generic generation" of stable groups. Namely, suppose we are given a stationary type p, whose realizations generate a stable group G, as a type-definable group, that is, G is the smallest type-definable group containing $p(\mathcal{M})$. What is the simplest way to get a generic type of G starting from p? The question is rather vague, unless we specify what kind of operations we are allowed to perform on p.

For stationary types the group operation induces an independent product on types in the following way: if p, q are stationary types of elements of G, then $p * q$ is defined as $tp(a \cdot b)$, where $a \models p$, $b \models q$ and $a \perp b$, $p^n = p * \ldots * p$ (n times). We allow taking independent powers of p and limits in the Stone space of stationary types. Newelski proved that there is always some sequence of powers of p converging to a generic type of G. As we will see later not every nonconstant sequence of powers of p converges to a generic type. Newelski proved quite a startling theorem saying that this is true after taking another step.

Double Step Theorem 3.2.6 *Let p be a stationary type, whose set of realizations generates a stable group G. Suppose r is a limit of an infinite sequence of powers of p and s is a limit of an infinite sequence of powers of r. Then s is a generic type of G.*

Newelski went on asking for which class of groups only *one* step is enough, namely the r in the statement of the double step theorem is already a generic type of G. We abbreviate this property by saying that the 1-step conjecture is true for G and p. If it is true for any p, we say it is true for G, and if it is true for any group G definable in any model of the theory T we say it is true for T. It is obvious that the 1-step conjecture is true for any G of U-rank 1. I proved in [K] (Theorem 1.6) the following.

Reduction Theorem 3.2.7 *Suppose $U(T) < \omega$. Then the 1-step conjecture is true for T if and only if it is true for algebraic types.*

Using the above theorem the 1-step conjecture in ACF turned out in [K] (Proposition 2.4) to be a part of the Mordell-Lang conjecture.

Theorem 3.2.8 *The 1-step conjecture for ACF is equivalent to the following statement:*
Suppose G is an algebraic group, Γ a cyclic subgroup of G, and $X \subset G$ is an

irreducible algebraic variety such that $X \cap \Gamma$ is Zariski dense in X. Then X is a coset of an algebraic subgroup of G.

This implies, that the 1-step conjecture is not true for ACF_p, which was pointed out to me by Anand Pillay. We recall the counterexample from [K]. Take $G = G_m \times G_m$ (G_m is the multiplicative group of the field K). Let X be defined by the equation $y = x + 1$. Every algebraic subgroup of G is defined by an equation $x^n y^m = 1$ for some integers m, n, so it is easy to see that X is not a translate of an algebraic subgroup of G. Take $a = (x, x+1)$, where x is transcendental over F_p. Then X contains infinitely many powers of a namely $a^{p^n} = (x^{p^n}, x^{p^n} + 1)$, so $\Gamma \cap X$ is Zariski dense in X as X is a one-dimensional subvariety.

The above example shows that the 1-step conjecture fails even in the first possible case – for groups of the Morley rank 2. However, unless the Mordell-Lang conjecture is not true in characteristic 0 for an arbitrary algebraic group, the 1-step conjecture holds. The proof uses p-adic analysis and was pointed out to me by Anand Pillay and Felipe Voloch and appeared in [K] (Theorem 3.2).

Theorem 3.2.9 *The 1-step conjecture is true in ACF_0.*

Using prolongations we can deduce the truth of the 1-step conjecture for DCF_0.

Theorem 3.2.10 *The 1-step conjecture is true in DCF_0.*

Proof Our setting is as follows: we have a DCF_0-definable group G, and a strong type p of elements of G, which generates G, and a certain infinite sequence (p^{k_i}) converging to a type r in the Stone topology. We need to show that r is a generic type of G.

By 3.2.5(i) (and its proof) there is a $*$-definable in ACF_0 group G^* and a $*$-definable in DCF_0 embedding $f : G \hookrightarrow G^*$ such that for a generic $a \in G$, $f(a) = a^*$ (recall that $a^* = (a, \delta(a), \delta^{(2)}(a), ...)$). By 3.1.3(i) $G^* = \lim(G_i)$ for an inverse system of groups definable in ACF_0.

Let $[G] = \{stp(a) : a \in G\}$ and $[G_n]^- = \{stp^-(b) : b \in G_n\}$. Let ϕ_n denotes the composition of f with a map $G^* \longrightarrow G_n$. Using ϕ_n, we get a continuous function $[G] \longrightarrow [G_n]^-$. If $r \in [G]$, then r_n denotes the image of r by the above function.

If we take H_n to be a definable subgroup of G_n generated by the set of realizations of p_n, then G embeds into $\lim(H_n)$, so we can assume p_n generates G_n. Let $a, b \in G$ and $p, q \in [G]$. Since $a \downarrow b$ implies $\phi_n(a) \downarrow \phi_n(b)$ and ϕ_n is a homomorphism, we get that $(p * q)_n = p_n * q_n$.

By the truth of the 1-step conjecture in ACF_0 (3.2.9) and the continuity of $p \mapsto p_n$, r_n is a generic type of G_n for each n. Then by 3.1.6, $r^* = lim(r_n)$ (i.e. if $a_n \models r_n$, then $(a_i) \models r^*$) is a generic type of G^*.

Suppose now that r is not a generic type of G. Take $b \in G$, $a \models r$ such that $a \downarrow b$ and b is generic. By 3.1.9, $b \cdot a$ is not independent from b and $b \cdot a$ is generic. Hence $f(a \cdot b) = (a \cdot b)^*$ and $f(b) = b^*$, so, by 3.2.2(i), $f(a \cdot b) = f(a) \cdot f(b)$ is not independent in ACF_0 from $f(b)$. Since $a \downarrow b$, we get $f(a) \downarrow^- f(b)$, so $f(a)$ is not generic in G^*. But $f(a) \models r^*$ and r^* is generic in G^*, a contradiction. □

A Appendix: Proalgebraic group structures on an inverse limit of affine spaces

In this section we assume familiarity with the notions from algebraic topology and geometry. We refer the reader to [OV], [Mi], [Sp] for background.

Lazard in [La] proved the following theorem.

Theorem A.1 *Suppose K is an algebraically closed field, and G is an algebraic group structure on A^n. Then G is unipotent.*

We introduce the category of proalgebraic varieties (see [KP]): its objects are $\lim(V_i)$ (as sets) for inverse systems of algebraic varieties $(V_i), (W_i)$, $f : \lim(V_i) \longrightarrow \lim(W_i)$ is a morphism, if for any i there are increasing sequences n_i, m_i, and morphisms of algebraic varieties $f_i : V_{n_i} \longrightarrow W_{m_i}$, such that $f = \lim(f_i)$ (so, the f_i's have to agree with maps from inverse systems). A proalgebraic group is a group object in the category of proalgebraic varieties. Let K^∞ denotes $\lim(K^n)$, where (K^n) is an inverse system with morphisms being projections.

In this section we sketch the proof a generalization of the Lazard theorem to K^∞. This was proved in [KP1] in the case of K algebraically closed of characteristic zero, and generalized in [CK] to the case of any field. In fact, we will prove a somewhat more general result.

Theorem A.2 *Let $G^* = \lim(G_i)$ be a proalgebraic group over an infinite field K such that all $G_i \longrightarrow G_j$ are dominant and colim $(K[G_i])$ is isomorphic (as an K-algebra) to colim (B_i), where each B_i is isomorphic to a ring of polynomials in finitely many variables. Then each G_i is unipotent.*

Let ϕ denote an isomorphism between colim $(K[G_i])$ and colim (B_i). Since each $K[G_i]$ and B_i is a finitely generated R-algebra, $\phi =$ colim (ϕ_i) for certain $\phi_i : K[G_{m_i}] \longrightarrow B_{n_i}$, where n_i, m_i are certain increasing sequences of natural numbers. Let $B_i \cong K[K^{k_i}]$. Since the functor $V \mapsto K[V]$ is faithfully full, we get that $\lim(G_i) \cong \lim(K^{k_i})$, as proalgebraic varieties.

By the definition of a morphism in the category of proalgebraic varieties, for any i there exist L, R and morphisms $G_{m_L} \longrightarrow K^{k_R}, K^{k_R} \longrightarrow G_i$ such that their composition is a morphism from the inverse system (G_i). Let L be a field extension of K. By [Wat] (p. 64) $Q(L)$ is unipotent if and only if Q is, so we can assume that K is algebraically closed. In this case all the maps $G_i \longrightarrow G_j$ are surjective (since a dominant homomorphism of algebraic groups over an algebraically closed field is onto).

Hence it is enough to prove the following fact.

Proposition A.3 *Let $f : G \longrightarrow Q$ be an epimorphism of connected affine algebraic groups, and assume that f factors through an affine space. Then Q is unipotent.*

If Q is solvable, then $Q = U \times G_m^n$, where U is unipotent, and there are no nonconstant morphisms from an affine space to G_m, so $Q = U$ is unipotent. Hence it is enough to prove the following:

Proposition A.4 *Let $f : G \longrightarrow Q$ be an epimorphism of connected affine algebraic groups over an algebraically closed field K, and assume that f factors through an affine space. Then Q is solvable.*

Proof We give first the easier proof from [KP1] for $char(K) = 0$, and then show a sketch of the proof from [CK] in the general case.
Case 1: char(K)=0.
We can assume, by completeness of theory ACF_0, that $K = \mathbb{C}$, the field of complex numbers. In this case smooth algebraic varieties over $\mathbb{C}$ have structure of analytic manifolds, and we can use the $\mathbb{C}$-topology. Also an algebraic group over $\mathbb{C}$ has the structure of a complex Lie group (so also of a real Lie group). The following fact is 2.7 from [KP1].

Lemma A.5 *Let G be a complex Lie group. Then G is solvable if and only if $\pi_3(G) = 0$.*

Proof
$\Longrightarrow$
This implication is true also for real Lie groups. Since the composition sequence of G consists of commutative groups, and any commutative Lie group has trivial π_3 (being a torus or $\mathbb{R}^n$), we get from the long sequence of homotopy groups that $\pi_3(G)$ is trivial, too. In fact $\pi_n(G) = 0$, for any $n > 1$.
$\Longleftarrow$
Suppose G is not solvable. Let R be the solvable radical of G. Then there is a smooth nontrivial homomorphism $SL_2(C) \longrightarrow G/R$ yielding a nontrivial homomorphism $S^3 = SU(2) \longrightarrow G/R$. Any such homomorphism is homotopically nontrivial, since it carries the structure 3-form on G (given in the

de Rham $H^3(G)$ by the Lie bracket) to the structure 3-form on S^3, and the latter is nonzero. Hence $\pi_3(G/R) \neq 0$. By the long exact sequence of homotopy groups $\pi_3(G) \neq 0$, since $\pi_n(R) = 0$, for any $n > 1$ (see the proof of the other implication). □

We would like to thank Tadeusz Januszkiewicz for pointing out this argument. This lemma does not hold in the category of real Lie groups, as the universal cover of $SL_2(R)$ is contractible and simple.

We need one nontrivial fact about Lie groups, which was proved by Bott in [Bo].

Fact A.6 *If G is a Lie group, then $\pi_2(G) = 0$.*

Now we can finish the proof of Proposition 4. Since $G \longrightarrow Q$ is an epimorphism, it induces an epimorphism on π_3 by the long exact sequence of homotopy groups, and the previous fact. But it factors through a contractible space $\mathbb{C}^k$, so has to induce the 0 map on π_3. Hence $\pi_3(Q) = 0$, and Q is solvable by Lemma 5.

Case 2: char(K) is arbitrary.

We still would like to use topological invariants, however, as far as we know, we can not use the homotopy groups anymore. But there is a good cohomology theory even in the positive characteristic – the étale cohomology. $H^*(X)$ will denote the étale cohomology with coefficients in the finite field Z/l, where l is prime to the characteristic. Similarly as in the smooth case $H^n(A^k) = 0$ (see [Mi]), for $n > 0$, so if a map $f : G \longrightarrow Q$ factors through A^k, then $f^* : H^n(Q) \longrightarrow H^n(G)$ is a zero map. Hence it is enough to prove the following:

Theorem A.7 *Suppose $f : G \longrightarrow Q$ is an epimorphism, and Q is nonsolvable. Then there exists $n > 0$ such that $f^* : H^n(Q) \longrightarrow H^n(G)$ is nonzero.*

By functoriality of the étale cohomology and properties of algebraic groups we can reduce the proof of the above theorem to the case where $G = Q$ is simple and f is an isogeny. By using the Hohschild-Serre spectral sequence we can show that any isogeny of connected algebraic groups induces an isomorphism on the étale cohomology (see 3.3 from [CK]). By the Leray spectral sequence (see 3.2 in [CK]), for any nonsolvable (e.g. simple) algebraic group, there is $n > 0$ such that $H^n(G) \neq 0$ (see 3.4 in [CK]). This finishes the proof. □

I should say that the proofs of 3.2, 3.3, and 3.4 from [CK], which were crucial in the proof of Proposition 4 in the positive characteristic case, are mostly due to Marcin Chałupnik.

References

[Bl] L. Blum, Differencially closed fields: a model theoretic tour, in *Contributions to Algebra*, ed. H. Bass, P. Cassidy and J. Kovacic, Academic Press (1977).

[Bo] M. R. Bott, An application of the Morse theory to the topology of Lie groups, *Bull. Soc. Math. France* **84** (1956), 251-281.

[Bu1] A. Buium, Intersections in jet spaces and a conjecture of S. Lang, *Annals of Mathematics* **(2) 136** (1992), 557-567.

[Bu2] A. Buium, Geometry of p-jets, *Duke Mathematical Journal* **(2) 82** (1996), 349-367.

[Bu3] A. Buium, Arithmetic Analogues of Derivations, *Journal of Algebra* **198** (1997), 290-299.

[Bu4] A. Buium, **Differential Algebraic Groups of Finite Dimension**, Springer-Verlag (1992).

[BC] A. Buium, Ph.J. Cassidy, Differential algebraic geometry and differential algebraic groups, to appear in *Collected Works of E. Kolchin.*

[Br] K. S. Brown, **Cohomology of Groups**, Springer-Verlag (1982).

[Ca1] Ph. J. Cassidy, Differential algebraic groups, *American Journal of Mathematics* **94** (1972), 891-954.

[Ca2] Ph. J. Cassidy, Unipotent differential algebraic groups, in *Contributions to algebra*, Academic Press, 1977.

[CK] M. Chalupnik, P. Kowalski, Lazard Theorem for differential algebraic and proalgebraic groups, to appear in *Pacific Journal of Mathematics*

[CH] Z. Chatzidakis and E. Hrushovski, Model theory of difference fields, *Transactions of AMS* **351** (1999), 2997-3071.

[Co] R. M. Cohn, **Difference Algebra**, John Wiley and Sons, New York (1965).

[Ha] R. Hartshorne, **Algebraic geometry**, Springer-Verlag (1977).

[HKP] B. Hart, B. Kim, A. Pillay, Coordinatization and canonical bases in simple theories, *Journal of Symbolic Logic* **(1) 65** (2000), 293-309.

[HP] E. Hrushovski, A. Pillay, Effective bounds for the number of transcendental points on subvarieties of semi-abelian varieties, *American Journal of Mathematics* **122** (2000), 439-450.

[Hr1] E. Hrushovski, Unidimensional theories are superstable, *Annals of Pure and Applied Logic* **50** (1990), 117-138.

[Hr2] E. Hrushovski, The Mordell-Lang conjecture for function fields, *Journal of American Mathematical Society* **(3) 9** (1996), 667-690.

[Hr3] E. Hrushovski, The model theory of difference fields and the Munin-Mumford conjecture, to appear in *Annals of Pure and Applied logic*

[HS] E. Hrushovski, Z. Sokolovic Minimal subsets in differentially closed fields, preprint

[Ja] N. Jacobson, **Lectures in Abstract Algebra, vol. III**, D. Van Nostrand Company, Inc. (1964).

[KiP] B. Kim, A. Pillay, Simple theories, *Annals of Pure and Applied Logic* **88** (1997), 149-164.

[Ko] E. Kolchin, **Differential Algebra and Algebraic Groups**, Academic Press, New York (1973).

[KP1] P. Kowalski, A. Pillay, Proalgebraic and differential algebraic group structures on affine spaces, *Amer. J. Math.* **122** (2000), 213-221.

[KP2] P. Kowalski, A. Pillay, A Note on Groups Definable in Difference Fields, to appear in *Proc. of AMS.*

[K] P. Kowalski Stable Groups and Algebraic Groups, *J. London Math. Soc.* **(2) 61** (2000), 51-57.

[L] S. Lang, **Algebra**, Addison-Wesley (1965).

[La] M. Lazard, Sur nilpotence de certains groupes algébriques, C.R.A.S. Paris **241** (1955), 1687-1689.

[Mi] J. Milne, **Étale Cohomology**, Princeton University Press, Princeton (1980).

[Mo] R. Moosa, On difference fields with quantifier elimination, preprint

[Ne] L. Newelski, On Type Definable Subgroup of a Stable Group, *Notre Dame Journal of Formal Logic* **32** (1991), 173-187.

[OV] A.L. Onishchik and E.B. Vinberg, **Lie Groups and Algebraic Groups**, Springer-Verlag 1990.

[Pi1] A. Pillay, **Geometric Stability Theory**, Oxford University Press, 1996.

[Pi2] A. Pillay, Some foundational questions concerning differential algebraic groups, *Pacific Journal of Mathematics* **(1) 179** (1997), 179-200.

[Pi3] A. Pillay, Differential algebraic group chunks, *Journal of Symbolic Logic* **55** (1990), 1138-1142.

[Pi4] A. Pillay, *Definability and definable groups in simple theories, Journal of Symbolic Logic*, 63 (1998), 788-796.

[Sc1] T. Scanlon, Model Theory of Valued D-fields with Applications to Diophantine Approximations in Algebraic groups, *Ph.D. thesis*, Harvard University (1997).

[Sc2] T. Scanlon, The abc-theorem for commutative algebraic groups in characteristic p, *International Mathematics Research Notices* **18** (1997), 881-898.

[Sc3] T. Scanlon, The conjecture of Tate and Voloch on p-adic proximity to torsion , *International Mathematics Research Notices* **17** (1999), 909-914.

[Se] J.-P. Serre, **Groupes Algébriques et Corps de Classes**, Hermann (1959).

[Sei] A. Seidenberg, Some basic theorems in differential algebra (characteristic p, arbitrary), *Transactions of American Mathematical Society* **17** (1952) 174-190.

[Sp] E.H. Spanier, **Algebraic topology**, McGraw-Hill 1966.

[Wa] F. O. Wagner, Groups in simple theories, Kluwer Academic Publishers (2000).

[Wat] W. Waterhouse, **Introduction to Affine Group Schemes**, Springer, New York (1979).

[Wo] C. Wood, The model theory of differential fields revisited, *Israel Journal of Mathematics* **25** (1976), 331-352.

[vdD] L. van den Dries, Weil's group chunk theorem : a topological setting, *Illinois Journal of Mathematics* **34** (1990), 127-139.

Index