Illinois Journal of Mathematics
Volume 47, Number 3, Fall 2003, Pages 593–618
S 0019-2082

ASYMPTOTIC THEORIES OF DIFFERENTIAL FIELDS

ZOÉ CHATZIDAKIS AND EHUD HRUSHOVSKI

Abstract. We relate the integrability of vector fields, and of the vanishing of p-torsion, to model-theoretic questions concerning separably closed fields, endowed canonically with a derivation. While each differential field $(F_p(t)^s, D_p)$ is known to be decidable, we show that the asymptotic theory of these fields as a class is undecidable in a strong sense. This precludes a geometric answer to certain generalizations of the Grothendieck-Katz conjecture.

Introduction

For a prime $p > 0$, let $\mathbb{F}_p(t)^s$ be the field of separably algebraic functions in one variable over the algebraic closure of the prime field. This field admits a unique derivation D_p with $D_p(t) = 1$; viewed as a *differential field*, we denote it by K_p. For each given prime p, it follows from results of Ershov [Er] that K_p has a decidable theory. We show however that the asymptotic theory, as $p \to \infty$, is undecidable. Indeed, the finite field $\mathbb{F}_p$ together with the space of maps $\mathbb{F}_p \to \mathbb{F}_p(t)^s$ is *uniformly* interpretable in these differential fields; they are indeed uniformly bi-interpretable with this essentially second-order structure (Theorem (3.12)).

With some additional effort, we show (Theorem (2.11)) that the asymptotic *Diophantine theory* of these differential fields is already undecidable (to the second degree, $0''$). Indeed, given an *arbitrary* Σ^0_2-set A in the sense of recursion theory, one can exhibit a differential equation $E(c, \bar{x})$ over $\mathbb{Q}(t)$, such that the set

$$\big\{c \in \mathbb{N} \mid E(c, \bar{x}) \text{ has a separable algebraic solution over } \mathbb{F}_p(t) \text{ for large enough } p\big\}$$

coincides with A.

Received April 9, 2002; received in final form April 4, 2003.
2000 *Mathematics Subject Classification.* Primary 03C98, 14D10. Secondary 14D05, 12H99.
The second author was supported by the Israel Science Foundation. The research was carried out for the Clay Mathematics Institute as a Clay Prize research fellow.

This work constitutes a first attempt to investigate the logical environment of some conjectures of Grothendieck and Katz, in a generalized nonlinear version that we heard from Kazhdan. We later found that the same conjecture (in somewhat greater generality) was formulated in [ESBT], as well as by Bost; [Ch-L] is an excellent reference.

Let E be a system of algebraic ordinary differential equations over $\mathbb{Q}(t)^{\mathrm{alg}}$ of finite differential order, say, a single differential polynomial in one variable, $F(x, Dx, \ldots, D^n x) = 0$, $0 \neq F \in \mathbb{Q}(t)^{\mathrm{alg}}[X_0, \ldots, X_n]$. For almost all primes p, one can reduce the coefficients modulo p to obtain a system of ODE's E_p over $\mathbb{F}_p(t)^s$. The conjectures can be interpreted as regarding the set X_p of separably algebraic solutions of the E_p; they give criteria for the existence of a *Kolchin dense set* of such solutions. This will be explained in Section 5; we point out here that the conjectures imply that for an equation to have a dense set of solutions modulo p, for almost all p, is a recursively enumerable property.

Our results address the simple existence of a separable algebraic solution, not the existence of a dense set thereof. Thus they do not yield any direct information on the conjectures. They do indicate however that these questions live in a dangerous neighbourhood. The set of equations admitting separable algebraic solutions modulo almost every prime is not recursively enumerable, and cannot be governed by a geometric principle analogous to the conjectures cited above.

Integrability of a vector field in characteristic 0 is a natural model theoretic notion, meaning that a corresponding Kolchin closed set, definable with parameters in the theory of differentially closed fields, is in the algebraic closure of the constants, over parameters. The other side of the conjectures, in all formulations except for Grothendieck's original one, mentions p-curvature and is more frightening to model theorists. We show therefore that vanishing p-curvature is equivalent to the existence of a dense set of separable algebraic solutions. For linear equations, this is a well-known theorem of Cartier (cf. Katz [K1, Theorem 7.1]). In the general case, it is a consequence of [E]. However, the logical proof is natural and connects nicely to standard theorems of model theoretic algebra, and we thought it worth leaving in.

This paper is organised as follows. In Section 1, we introduce a family of structures, $\mathcal{F}_p$, for p ranging over all odd prime numbers. We then consider the theory T' of sentences true in all but finitely many of the $\mathcal{F}_p$, and show that its universal and existential parts are Σ_2^0-complete (Theorem (1.5)). In Section 2, we show how to interpret the structure $\mathcal{F}_p$ in the differential field K_p, uniformly in p and using formulas of low complexity. This allows us to derive Theorem (2.11). In Section 3, we show the bi-interpretability (uniformly in p) of the differential field K_p with a second-order structure. Section 4 gives some examples of linear differential equations over $\mathbb{Q}(t)$, whose reductions modulo p have solutions in $\mathbb{F}_p(t)^s$ for infinitely many p's, or for all but finitely

many p's. In Section 5 we discuss the conjecture, and give a model-theoretic formulation.

1. The structures $\mathcal{F}_p$ and their asymptotic Diophantine theory

(1.1) Setting, definitions and notation. Let $\mathcal{L}_e = \{R_+, R_\times, R_e, 0, 1\}$, where R_+ and $R_\times$ are ternary relations, R_e is a binary relation, and 0, 1 are constant symbols. For each *odd* prime p, consider the $\mathcal{L}_e$-structure $\mathcal{F}_p$ with universe $\{0, \dots, p-1\}$ viewed as the initial segment $[0, p-1]$ of $\mathbb{N}$, and where R_+ and $R_\times$ are the restrictions to $[0, p-1]^3$ of the graphs of addition and multiplication on $\mathbb{N}$, and where R_e is the graph of the function $e : x \mapsto 2^x \mod (p)$ defined on $[0, p-1]$. The constants 0 and 1 are interpreted as 0 and 1. We let T' be the set of $\mathcal{L}_e$-sentences which hold in all but finitely many of the $\mathcal{L}_e$-structures $\mathcal{F}_p$.

Let $P(\bar{X}) \in \mathbb{N}[\bar{X}]$. There is a positive existential $\mathcal{L}_e$-formula $\exists \bar{z} \varphi(\bar{x}, y, \bar{z})$ such that for any odd prime p and for any $\bar{a}$, b in $\mathcal{F}_p$ we have

$$\mathbb{N} \models P(\bar{a}) = b \iff \mathcal{F}_p \models \exists \bar{z}\, \varphi(\bar{a}, b, \bar{z}).$$

To simplify notation, if $P_1(\bar{X})$ and $P_2(\bar{X})$ are two polynomials over $\mathbb{N}$, we will denote by "$P_1(\bar{x}) =^* P_2(\bar{x})$" the positive existential $\mathcal{L}_e$-formula (in the variable $\bar{x}$) such that, for any odd prime p and tuple $\bar{a}$ in $\mathcal{F}_p$,

$$\mathbb{N} \models P_1(\bar{a}) = P_2(\bar{a}) < p \iff \mathcal{F}_p \models P_1(\bar{a}) =^* P_2(\bar{a}).$$

Let us immediately remark that the induced order relation on $\mathcal{F}_p$ is positively existentially definable:

$$x < y \iff \exists z\, (x + z + 1 =^* y).$$

(1.2) Bounds on witnesses of Diophantine definitions of Δ_0-sets. We work in the language $\mathcal{L}_{\mathrm{ar}}$ of arithmetic, $\mathcal{L}_{\mathrm{ar}} = \{+, \cdot, 0, 1, <\}$. We define $\exp^k(x)$ by induction as follows: $\exp^0(x) = x$, $\exp(x) = \exp^1(x) = 2^x$, and $\exp^{k+1}(x) = 2^{\exp^k(x)}$. Recall that a Δ_0-formula $\varphi(x_1, \dots, x_n)$ is a formula of the form

$$Q_m x_{n+m} \le x_{i(m)}\, Q_{m-1} x_{n+m-1} \le x_{i(m-1)} \cdots Q_1 x_{n+1} \le x_{i(1)} \psi(x_1, \dots, x_{n+m}),$$

where $1 \le i(j) \le n$, ψ is a quantifier-free $\mathcal{L}_{\mathrm{ar}}$-formula, and the Q_i are quantifiers. (Note: Some authors allow the bounds on the variables $x_{n+1}, \dots, x_{n+m}$ to be $\mathcal{L}_{\mathrm{ar}}$-terms in the variables $x_1, \dots, x_n$. The two definitions however coincide up to equivalence in $\mathbb{N}$, as one easily sees. For instance, the formula $\exists x \le y^2 \psi(x, y, \dots)$ is equivalent to the formula $\exists x_1 \le y\, \exists x_2 \le y\ (x_1 \ne y \wedge \psi(x_1 y + x_2, y, \dots))$.)

The arithmetic hierarchy is defined as follows: Σ_0- and Π_0-formulas are Δ_0-formulas; a Σ_{i+1}-formula is one of the form $\exists \bar{x} \varphi(\bar{x}, \bar{y})$, where $\varphi(\bar{x}, \bar{y})$ is a Π_i-formula, and a Π_{i+1}-formula is the negation of a Σ_{i+1}-formula.

By classical results of Matijasevič and Robinson, Davis, Putnam, any subset of $\mathbb{N}^k$ which is definable by a Δ_0-formula is definable by a Diophantine formula, i.e., by a formula of the form $\exists \bar{y}\, P_1(\bar{x}, \bar{y}) = P_2(\bar{x}, \bar{y})$, where the P_i's are polynomials over $\mathbb{N}$. The following result give us bounds on the size of the witnesses $\bar{y}$ in terms of the size of the elements of $\bar{x}$.

Proposition (Gaifman-Dimitracopoulos). *Let $\varphi(\bar{x})$ be a Δ_0-formula. There are $k \in \mathbb{N}$, $n = n(\varphi) \in \mathbb{N}$, and polynomials $P_1(\bar{X}, \bar{Y})$ and $P_2(\bar{X}, \bar{Y}) \in \mathbb{N}[\bar{X}, \bar{Y}]$, such that for all tuples $\bar{a}$ in $\mathbb{N}$ and $N = \sup\{\bar{a}, n\}$*

$$\begin{aligned} \mathbb{N} \models \varphi(\bar{a}) &\iff \mathbb{N} \models \exists \bar{y} \left(P_1(\bar{a}, \bar{y}) = P_2(\bar{a}, \bar{y})\right) \\ &\iff \mathbb{N} \models \exists \bar{y} < \exp^k(N) \left(P_1(\bar{a}, \bar{y}) = P_2(\bar{a}, \bar{y}) < \exp^k(N)\right). \end{aligned}$$

This result appears in [DG], with $k = 3$, with only an indication of the proof ("checking the proof of the Matijasevič-Robinson-Davis-Putnam Theorem"). Before learning of the Gaifman-Dimitracopoulos result, we had checked the proof of the Matijasevič-Robinson-Davis-Putnam Theorem given in Smoryński's book [S], and obtained the value $k = 4$; and in the particular case of the Δ_0-formula expressing $y = 2^x$, that $k = 2$. In what follows we will use our bounds. Our calculations of the bounds can be found at `http://www.logique.jussieu.fr/www.zoe/papiers/DFptbounds.dvi`. They are completely straightforward.

(1.3) Lemma. *For each $k \geq 1$, there is a positive existential formula $\theta_k(x)$ such that for every odd prime p and $a < p$ we have*

$$\mathcal{F}_p \models \theta_k(a) \iff \mathbb{N} \models \exp^k(a) > p.$$

Proof. Let

$$\begin{aligned} \theta_1(x) = \exists y < x\, \exists y' \exists z_1 \exists z_2 \ \big[&(y' =^* y + 1) \\ &\wedge R_e(y, z_1) \wedge R_e(y', z_2) \wedge (z_2 < z_1)\big]. \end{aligned}$$

By the remark made at the end of (1.1), this is a positive existential formula, which says that $e(y + 1) < e(y)$ for some $y < x$. Assume that $2^a > p$, and let $b \leq a$ be smallest such that $2^b > p$. Then $2^{b-1} = e(b - 1) < p$, and $e(b) = e(b - 1) + e(b - 1) - p < e(b - 1)$. This shows one direction for $k = 1$, and the other direction is clear.

Note that $\exp^k(a) > p$ if and only if $\bigvee_{i=1}^{k} \exp^i(a) > p$, if and only if $\bigvee_{i=0}^{k-1} 2^{e^i(a)} > p$, where e^i denotes e iterated i times. Hence, for $k > 1$, we

define

$$\theta_k(x) = \exists y_0, \dots, y_{k-1}\ \big[y_0 = x \wedge \bigwedge_{i=0}^{k-2} R_e(y_i, y_{i+1})\big] \wedge \bigvee_{i=0}^{k-1} \theta_1(y_i).$$

(1.4) Lemma. *There is an integer n_0 and for each $\ell \geq 1$ there is a positive existential $\mathcal{L}_e$-formula $E_\ell(x, y)$ such that for all $a \in \mathbb{N}$ and every odd prime p we have:*

(1) *If $p > \exp^2(\sup\{n_0, \exp^\ell(a)\})$ then $\mathcal{F}_p \models E_\ell(a, \exp^\ell(a))$.*
(2) *If $b \in \mathcal{F}_p$ and $\mathcal{F}_p \models E_\ell(a, b)$ then $b = \exp^\ell(a)$.*

Proof. Consider the Δ_0-formula defining $y = 2^x$, and let n_0 and polynomials P_1, P_2 be given by Proposition (1.2), i.e., such that for all $a, b \in \mathbb{N}$ and $N = \sup\{n_0, a, b\}$, we have

$$\begin{aligned}\mathbb{N} \models 2^a = b &\iff \exists \bar{v}\,(P_1(a, b, \bar{v}) = P_2(a, b, \bar{v})) \\ &\iff \exists \bar{v} < \exp^2(N)\,(P_1(a, b, \bar{v}) = P_2(a, b, \bar{v}) < \exp^2(N)).\end{aligned}$$

We set, for $\ell \in \mathbb{N}$, $\ell > 1$,

$$E_1(x, y) = \exists \bar{v}\,\big[R_e(x, y) \wedge P_1(x, y, \bar{v}) =^* P_2(x, y, \bar{v})\big],$$

$$E_\ell(x, y) = \exists y_0, \dots, y_\ell (y_0 = x \wedge y_\ell = y) \wedge \bigwedge_{i=0}^{\ell-1} E_1(y_i, y_{i+1})$$

Let $a \in \mathbb{N}$, and let $a_i = \exp^i(a)$ for $i = 0, \dots, \ell$. Our choice of n_0 implies that for each $i < \ell$ there is $\bar{v} < \exp^2(\sup\{n_0, a_{i+1}\})$ such that

$$P_1(a_i, a_{i+1}, \bar{v}) = P_2(a_i, a_{i+1}, \bar{v}) < \exp^2(\sup\{n_0, a_{i+1}\}).$$

Hence, if $p > \exp^2(\sup\{n_0, a_\ell\})$, then all a_i's are in $\mathcal{F}_p$, and

$$\mathcal{F}_p \models \exists \bar{v}\,(P_1(a_i, a_{i+1}, \bar{v}) =^* P_2(a_i, a_{i+1}, \bar{v}))$$

for $i = 0, \dots, \ell - 1$. This shows that $\mathcal{F}_p \models E_\ell(a, \exp^\ell(a))$ and proves (1).

(2) is clear.

(1.5) Theorem. *Let $\alpha(z)$ be a Σ_2-formula (of $\mathcal{L}_{\mathrm{ar}}$). There are $\mathcal{L}_e$-formulas $\beta(z)$ and $\gamma(z)$, with β universal and γ positive existential, such that for any $c \in \mathbb{N}$*

$$\mathbb{N} \models \alpha(c) \iff T' \vdash \beta(c) \iff T' \vdash \gamma(c).$$

Proof. By standard results, we may assume that $\alpha(z) = \exists x\, \forall y \geq x\ \varphi(y, z)$, where $\varphi(y, z)$ is Δ_0.

Part 1: Finding β. We will in fact find a positive existential $\mathcal{L}_e$-formula $\delta(z)$ such that for any $c \in \mathbb{N}$

$$\mathbb{N} \models \neg\alpha(c) \iff T' \cup \{\delta(c)\} \text{ is consistent.}$$

Then $\beta(z) = \neg\delta(z)$ will be our desired universal formula.

Note that $\neg\alpha(z)$ simply says that there are infinitely many y such that $\neg\varphi(y,z)$ holds. Let $n = n(\neg\varphi)$ and $P_1, P_2 \in \mathbb{N}[Y, Z, \bar{V}]$ be given by Proposition (1.2), i.e., such that for any $N \geq n$ and $\ell, c \leq N$

$$\begin{aligned}\mathbb{N} \models \neg\varphi(\ell,c) &\iff \exists \bar{v}\ (P_1(\ell,c,\bar{v}) = P_2(\ell,c,\bar{v}))\\ &\iff \exists \bar{v} < \exp^4(N)\ (P_1(\ell,c,\bar{v}) = P_2(\ell,c,\bar{v}) < \exp^4(N)).\end{aligned}$$

Consider the $\mathcal{L}_e$-sentence $\delta(z)$

$$\exists y \exists \bar{v}\ [P_1(y,z,\bar{v}) =^* P_2(y,z,\bar{v}) \wedge \theta_5(y)].$$

By (1.3), this is a positive existential $\mathcal{L}_e$-formula. Assume that $c \in \mathbb{N}$ satisfies $\neg\alpha(z)$. We want to show that $T' \cup \{\delta(c)\}$ is consistent, that is, that there are arbitrarily large prime numbers p such that $\delta(c)$ holds in $\mathcal{F}_p$.

Let $d \in \mathbb{N}$, $d > n(\neg\varphi)$, and $d > c$. By assumption, there is $\ell > d$ such that $\mathbb{N} \models \neg\varphi(\ell, c)$. Let p be the largest prime such that $\exp^5(\ell) > p$. Then $\exp^4(\ell) < p$, and there is a tuple $\bar{b}$ in $\mathbb{N}$ such that $\bar{b} < \exp^4(\ell)$ and $P_1(\ell,c,\bar{b}) = P_2(\ell,c,\bar{b}) < \exp^4(\ell)$. Thus we have

$$\bar{b} < p, \quad P_1(\ell,c,\bar{b}) = P_2(\ell,c,\bar{b}) < p, \quad \exp^5(\ell) > p,$$

so that

$$\mathcal{F}_p \models P_1(\ell,c,\bar{b}) =^* P_2(\ell,c,\bar{b}) \wedge \theta_5(\ell).$$

From $\ell < p$ we deduce that $p > d$. This shows that $T' \cup \{\delta(c)\}$ is consistent.

Conversely, assume that $T' \cup \{\delta(c)\}$ is consistent. We want to show that there are arbitrarily large ℓ's such that $\neg\varphi(\ell, c)$ holds. Let $d \in \mathbb{N}$, $d > c$. Our assumption implies that there is a prime p larger than $\exp^5(d)$ such that $\mathcal{F}_p \models \delta(c)$. Fix such a p and let ℓ and $\bar{b} < p$ be such that

$$\mathcal{F}_p \models P_1(\ell,c,\bar{b}) =^* P_2(\ell,c,\bar{b}) \wedge \theta_5(\ell).$$

Then

$$\mathbb{N} \models \neg\varphi(\ell,c) \wedge \exp^5(\ell) > p.$$

From $\exp^5(d) < p < \exp^5(\ell)$ we deduce that $d < \ell$. This being true for all d, we get $\mathbb{N} \models \neg\alpha(c)$.

Part 2: Finding γ. Consider the formula

$$\psi(z,u_1,u_2) = (u_1 < u_2) \wedge \forall y \leq u_2\, (\neg\varphi(y,z) \to y < u_1).$$

This is a Δ_0-formula, which says that there are no solutions of $\neg\varphi(y,z)$ in the interval $[u_1, u_2]$. Let $n = n(\psi)$, and $Q_1, Q_2 \in \mathbb{N}[Z, U_1, U_2, \bar{V}]$ be given by Proposition (1.2), i.e., such that for $a, b, c \in \mathbb{N}$ and $N = \sup\{a,b,c,n\}$

$$\begin{aligned}\mathbb{N} \models \psi(a,b,c) &\iff \exists \bar{v}\ (Q_1(a,b,c,\bar{v}) = Q_2(a,b,c,\bar{v}))\\ &\iff \exists \bar{v} < \exp^4(N)\,(Q_1(a,b,c,\bar{v}) = Q_2(a,b,c,\bar{v}) < \exp^4(N)).\end{aligned}$$

Consider the formula

$$\gamma(z) = \exists u_1, u_2, \bar{v}\ [E_6(u_1,u_2) \wedge \theta_5(u_2) \wedge Q_1(z,u_1,u_2,\bar{v}) =^* Q_2(z,u_1,u_2,\bar{v})].$$

Let us assume that $\mathbb{N} \models \alpha(c)$, and let $d \in \mathbb{N}$ be such that

$$\mathbb{N} \models \forall y \geq d\ \varphi(y, c).$$

Let p be a prime greater than $\exp^{11}(\sup\{c, d\})$, $\exp^2(n_0)$, and $\exp^4(n(\psi))$. We will show that $\mathcal{F}_p \models \gamma(c)$. Let ℓ_1 be smallest such that $\exp^{11}(\ell_1) > p$, and let $\ell_2 = \exp^6(\ell_1)$. Then $\exp^4(\ell_2) < p < \exp^5(\ell_2)$, and by (1.3)

$$\mathcal{F}_p \models E_6(\ell_1, \ell_2) \wedge \theta_5(\ell_2).$$

Moreover, $\ell_1 > d$, whence

$$\mathbb{N} \models \forall y \leq \ell_2\ (\neg\varphi(y, c) \to y < \ell_1).$$

If $N = \sup\{\ell_2, n(\psi)\}$, there is $\bar{b} < \exp^4(N)$ such that $Q_1(c, \ell_1, \ell_2, \bar{b}) = Q_2(c, \ell_1, \ell_2, \bar{b}) < \exp^4(N)$, and therefore

$$\mathcal{F}_p \models Q_1(c, \ell_1, \ell_2, \bar{b}) =^* Q_2(c, \ell_1, \ell_2, \bar{b}).$$

This shows that $\mathcal{F}_p \models \gamma(c)$.

Let us now assume that $T' \vdash \gamma(c)$. Choose $d > 1$ such that $\gamma(c)$ holds in all structures $\mathcal{F}_p$ with $p > d$. For each prime $p > d$, let $\ell_1(p)$, $\ell_2(p)$ be such that

$$\mathcal{F}_p \models \exists \bar{v}\ \big[E_6(\ell_1(p), \ell_2(p)) \wedge \theta_5(\ell_2(p)) \wedge (Q_1(c, \ell_1(p), \ell_2(p), \bar{v}) =^* Q_2(c, \ell_1(p), \ell_2(p), \bar{v})\big].$$

Then

$$\mathbb{N} \models \exists \bar{v}\ Q_1(c, \ell_1(p), \ell_2(p), \bar{v}) = Q_2(c, \ell_1(p), \ell_2(p), \bar{v}) \wedge \ell_2(p) = \exp^6(\ell_1(p)) \wedge \exp^5(\ell_2(p)) > p$$

and therefore

$$\mathbb{N} \models \forall y \leq \ell_2(p)(\neg\varphi(y, c) \to y < \ell_1(p)).$$

Hence we have shown the following: If $\ell \in \bigcup_{d<p \text{ prime}}[\ell_1(p), \ell_2(p)]$, then $\mathbb{N} \models \varphi(\ell, c)$. Clearly, as the prime p goes to infinity, so does $\ell_2(p)$, because $\exp^5(\ell_2(p)) > p$. Hence, to finish the proof, it is enough to show that if p' is the prime immediately after p, then

$$\ell_1(p') < \ell_2(p).$$

We know that $\ell_2(p') < p' < 2p$. Hence $\exp^6(\ell_1(p')) = \ell_2(p') < 2p$. Since $p > 2$, we have $2p < 2^p$, and therefore $\exp^5(\ell_1(p')) < p < \exp^5(\ell_2(p))$, whence $\ell_1(p') < \ell_2(p)$. This being true for all primes greater than d, we have that $\mathbb{N} \models \alpha(c)$.

2. Uniform definition of $\mathcal{F}_p$

We fix $p > 2$ and consider a separably closed field K of characteristic p and degree of imperfection 1 (that is, $[K : K^p] = p$), equipped with a derivation $D : K \to K$ with range containing 1. Fix any element t such that $Dt = 1$. Then $t \notin K^p$, and therefore $K = K^p \oplus K^p t \oplus \cdots \oplus K^p t^{p-1}$.

Given $a \in K$ and $0 \leq i < p$ we will denote by $a_{(i)}$ the t^i-coordinate of a in the K^p-vector space K with respect to the basis $\{1, t, \ldots, t^{p-1}\}$, so that we have

$$a = \sum_{i=0}^{p-1} a_{(i)} t^i.$$

In this notation, we have $D(\sum_{i=0}^{p-1} a_{(i)} t^i) = \sum_{i=1}^{p-1} i a_{(i)} t^{i-1}$. Note that the field K^p coincides with the field of constants $\{a \in K \mid Da = 0\}$ of the derivation D.

Let $\mathcal{L}_D = \{+, -, \cdot, D, 0, 1\}$ be the language of differential fields. We will work in the language $\mathcal{L}_D \cup \{t\}$, and show that we can define uniformly in p the $\mathcal{L}_e$-structure $\mathcal{F}_p$ in the differential field K. (It may be helpful to keep in mind a particular model such as $K = \mathbb{F}_p(t)^s$, and $D = D_p$ defined earlier, but all such differential fields are elementarily equivalent.)

(2.1) Consider the set $S = \bigcup_{i=0}^{p-1} K^p t^i$. Then S is quantifier-free definable (uniformly in p) in K_p by the formula $x = 0 \vee D(tDx/x) = 0)$. Indeed, assume that $a \neq 0$ and tDa/a is a constant c. Then we get $ca = tDa$, i.e.,

$$\sum_{i=0}^{p-1} c a_{(i)} t^i = \sum_{i=0}^{p-1} i a_{(i)} t^i,$$

which implies $ca_{(i)} = ia_{(i)}$ for $i = 0, \ldots, p-1$, so that at most one $a_{(i)}$ is non-zero.

(2.2) The map $f : x \mapsto tDx/x$ sends a non-zero element ct^i of S to i, and therefore sends $S \setminus \{0\}$ onto $\{0, 1, \ldots, p-1\} \subset K^p$. We extend f to all of S by setting $f(0) = 0$ and let $\mathcal{F}$ denote the image of f. (In fact, the set $\mathcal{F}$ coincides with the subfield $\mathbb{F}_p$ of K).

(2.3) Note that for $a \in K$, $a_{(p-1)} = 0 \iff \exists y\, Dy = a$. Hence, given $b \in S$, $b \neq 0$, we have

$$a_{(f(b))} = 0 \iff \exists y\, Dy = (bt)^{-1} a.$$

(2.4) Let $a \in K^p$ and consider the element $\widehat{a} = \sum_{i=0}^{p-1} a^i t^i$. Then $\widehat{a}_{(i)} = a^i$, and $\widehat{a}$ is uniquely defined by the formula

$$D(x - atx) = 0 \wedge x_{(0)} = 1.$$

Hence the graph of the function $\widehat{\ }: K^p \to K$ is positively existentially definable (uniformly in p) (by (2.3)).

(2.5) The elements $\widehat{1}$, t^p, and $\widehat{t^p}$ are positively existentially definable (uniformly in p).

Indeed, $\widehat{1}$ is defined by $D(x - tx) = 0 \wedge x_{(0)} = 1$. Also, $t^p = \widehat{1}(t - 1) + 1$. Hence the second and third assertions follow by (2.4).

(2.6) The graph of the function $g : \mathcal{F} \to S$, $b \mapsto t^b$, is positively existentially definable (uniformly in p).

Let $b \in \mathcal{F}$. Then

$$c = g(b) \iff (f(c) = b) \wedge ((\widehat{1} - c)_{(b)} = 0).$$

Use (2.3).

(2.7) Consider the function $h : K \times \mathcal{F} \to K^p$, $(a, b) \mapsto a_{(b)}$. Then the graph of h is positively existentially definable (uniformly in p): For $a \in K$, $b \in \mathcal{F}$, $c \in K^p$,

$$h(a, b) = c \iff (a - cg(b))_{(b)} = 0.$$

The result follows from (2.3) and (2.6).

(2.8) Definition of R_+ and $R_\times$. Let $a, b, c \in \mathcal{F} \subseteq \mathbb{N}$. Then $R_+(a, b, c)$ holds if and only if $a + b = c$, if and only if $t^{pa}t^{pb} = t^{pc}$. Hence,

$$R_+(a, b, c) \iff \widehat{t^p}_{(a)}\widehat{t^p}_{(b)} = \widehat{t^p}_{(c)}$$

This shows that R_+ is positively existentially definable (uniformly in p). Similarly, $R_\times(a, b, c)$ holds if and only if $t^{pab} = t^{pc}$, so that

$$R_\times(a, b, c) \iff \widehat{\widehat{t^p}_{(a)}}_{(b)} = \widehat{t^p}_{(c)},$$

and $R_\times$ is positively existentially definable (uniformly in p).

(2.9) Definition of R_e. For $a \in \mathcal{F}$, we have

$$e(a) = \widehat{2}_{(a)},$$

so that the graph R_e of the function e is positively existentially definable (uniformly in p).

(2.10) We will not use this here, but it is interesting to remark that the graph of the restriction of the function $x \mapsto x^p$ to K^p is positively existentially definable (uniformly in p), since

$$a^p = (\widehat{a}(at - 1) + 1)/t^p.$$

Similarly, the shift operator $\mathrm{Sh} : K \to K$, defined by

$$(\mathrm{Sh}(x))_{(i)} = \begin{cases} x_{(p-1)} & \text{if } i = 0, \\ x_{(i-1)} & \text{otherwise,} \end{cases}$$

is positively existentially definable, using

$$\mathrm{Sh}(a) = ta + (1 - t^p)a_{(p-1)}.$$

(2.11) Theorem. *Let T be the set of $\mathcal{L}_D$-sentences which hold in all but finitely many of the differential fields $(\mathbb{F}_p(t)^s, D_p)$. Let $\alpha(z)$ be a Σ_2-formula (of $\mathcal{L}_{\mathrm{ar}}$). There are $\mathcal{L}_D$-formulas $\beta^*(z)$ and $\gamma^*(z)$, with β^* universal and γ^* existential, such that for every $c \in \mathbb{N}$*

$$\mathbb{N} \models \alpha(c) \iff T \vdash \beta^*(c) \iff T \vdash \gamma^*(c).$$

Proof. The formulas $\delta(z)$ and $\gamma(z)$ constructed in Theorem (1.5) are positive existential formulas of $\mathcal{L}_e$. By (2.2), (2.8) and (2.9), there are positive existential $\mathcal{L}_D$-formulas $\delta'(z,t')$ and $\gamma'(z,t')$ such that for any prime p and $c < p$, we have

$$\mathcal{F}_p \models \delta(c) \iff \mathbb{F}_p(t)^s \models \exists t' \, (Dt' = 1 \wedge \delta'(c,t')),$$
$$\mathcal{F}_p \models \gamma(c) \iff \mathbb{F}_p(t)^s \models \exists t' \, (Dt' = 1 \wedge \gamma'(c,t')).$$

Then $\beta^*(z) = \neg(\exists t' \, Dt' = 1 \wedge \delta'(z,t'))$ and $\gamma^*(z) = \exists t' \, (Dt' = 1 \wedge \gamma'(z,t'))$ are our desired $\mathcal{L}_D$-formulas.

(2.12) Additional remarks.

(1) Going to the complement, it follows that the existence of solutions of systems of differential equations for infinitely many p is therefore Π_2-complete, as is the non-existence of solutions for infinitely many p.

(2) Our proof only used $K = K^p \oplus tK^p \oplus \cdots \oplus t^{p-1}K^p$, and not the fact that K is separably closed.

(3) Note that the set defined by $\gamma^*(z)$ is the projection of a differential algebraic set of finite order.

(4) If $(K, D) \models T$, then K is an algebraically closed field of characteristic 0.

3. Bi-interpretability of K with a second-order structure

Fix p, and let $K = \mathbb{F}_p(t)^s$, with derivation $D = D_p$. Consider the structure L, with universe the set of functions from $\mathcal{F} = \mathbb{Z}/p\mathbb{Z}$ to $C = K^p$. We view L as a 3-sorted structure $(L, C, \mathcal{F})$, in the language $\mathcal{L}_f = \{+, \times, 0, 1, t^p, +_F, -_F, 0_F, 1_F, h\}$, where:

(i) $+$, $\times$ are addition and multiplication on the field C, with distinguished constants 0, 1 and t^p.

(ii) $+_F$ is the usual addition on the group $\mathcal{F}$, and $-_F$ the usual subtraction; we have distinguished constants 0_F and 1_F, where 0_F is interpreted as the zero element of the group $\mathcal{F}$ and 1_F is any generator of the group $\mathcal{F}$.

(iii) h is the evaluation map: $L \times \mathcal{F} \to C$, $(a, i) \mapsto a(i)$.

As a set, L is isomorphic to K via the map $a \mapsto \sum_{i=0}^{p-1} a(i)t^i$. By the results of the previous section, the $\mathcal{L}_f$-structure $(L, C, \mathcal{F})$ is definable in the differential field K. Moreover, the complexity of this definition is low: C is quantifier-free definable, and $\mathcal{F}$ is existentially definable. The graphs of all

functions are existentially definable (and therefore also universally definable), and the constants are existentially definable in $\mathcal{L}_D \cup \{t\}$.

Conversely, we will show that we can define in L the addition and multiplication of K (denoted by $\cdot$), and the derivation of K. For convenience we have added a constant symbol for t^p, but in fact any element of C which is not in C^p would do as well (the derivation would be slightly different, in the same way as in $\mathbb{F}_p(t)^s$ it depends on the choice of the element t). You will observe that the definitions given below also have a low complexity, modulo quantification over $\mathcal{F}$. We use some of the notation introduced in Section 2.

(3.1) For $a \in C$, let $\bar{a}$ denote the function in L which takes the constant value a. Then the map $a \mapsto \bar{a}$ is definable:

$$x = \bar{a} \iff \forall i \in \mathcal{F},\, x(i) = a.$$

(3.2) For $a \in C$, let $\widehat{a}$ denote the function in L defined by $\widehat{a}(i) = a^i$. Then the map $a \mapsto \widehat{a}$ is definable by the formula

$$x(0_F) = 1 \wedge \forall i \in \mathcal{F},\, (i +_F 1_F = 0_F) \vee x(i +_F 1_F) = a \times x(i).$$

(3.3) The sum map $\Sigma : L \to C$, $a \mapsto \sum_{i \in \mathcal{F}} a(i)$ is definable:

$$\begin{aligned}\Sigma(a) = b \iff \exists z\, z(0_F) = a(0_F) \wedge \forall i \in \mathcal{F}\, (i +_F 1_F = 0_F \wedge z(i) = b)\\ \vee\, z(i +_F 1_F) = z(i) + a(i +_F 1_F).\end{aligned}$$

(3.4) For $a \in C$, the function $a \mapsto a^p$ is definable: we have $a^p = \widehat{a}(-1_F) \times a$.

(3.5) Pointwise addition and multiplication are definable in L, and will be denoted also by $+$ and $\times$: $a + b = c \iff \forall i \in \mathcal{F}\, a(i) + b(i) = c(i)$, and similarly for $\times$.

(3.6) The identity function $\mathrm{id} : \mathcal{F} \to C$ is definable:

$$x(0_F) = 0 \wedge \forall i \in \mathcal{F}\, (x(i +_F 1_F) = x(i) + 1).$$

(3.7) Hence the derivation D is definable:

$$D(x) = y \iff \forall i \in \mathcal{F}\, y(i) = \mathrm{id}(i +_F 1_F) \times x(i +_F 1_F)).$$

(3.8) Each of the idempotent functions $\bar{1}_{|i}$ is definable (uniformly in $i \in \mathcal{F}$), where

$$\bar{1}_{|i}(j) = \begin{cases} 1 & \text{if } j \le i, \\ 0 & \text{otherwise.} \end{cases}$$

Indeed, we have

$$\begin{aligned}x = \bar{1}_{|i} \iff & x(0_F) = 1 \wedge (i +_F 1_F = 0_F \vee x(i +_F 1_F) = 1)\\ & \wedge \forall j \in \mathcal{F}\, (j = i \vee j +_F 1_F = 0_F \vee x(j +_F 1_F) = x(j)).\end{aligned}$$

(3.9) Multiplication of the field K is definable.

We will first show that the function $L^2 \times \mathcal{F} \to L$, which to (x, y, i) associates the function z_i defined by

$$z_i(j) = \begin{cases} x(j) \times y(i -_F j) & \text{if } j \leq i, \\ t^p \times x(j) \times y(i -_F j) & \text{otherwise,} \end{cases}$$

is definable. For each $i \in \mathcal{F}$ consider the element

$$d_i = \bar{1}|_i + \overline{t^p} \times (\bar{1} - \bar{1}|_i).$$

Then $v = z_i$ if and only if

$$\exists u(\forall j \in \mathcal{F},\, u(j) = x(j) \times y(i -_F j)) \wedge (v = d_i \times u).$$

It then follows that the element $z = x \cdot y$ is defined by

$$\forall i \in \mathcal{F}\, (z(i) = \Sigma(z_i)).$$

(3.10) We therefore can use all the definability results proved in Section 2. In particular, the map $C \times \mathcal{F} \to C$, $(a, i) \mapsto a^i$ is definable, so that the map $i \mapsto t^{pi}$ is also definable. We also saw that the restriction of $x \mapsto x^p$ to C is definable in K. This implies:

(3.11) The Frobenius map $L \to C$, $x \mapsto x^p$, is definable.

$$y = x^p \iff \exists z\, (\forall i \in \mathcal{F},\, z(i) = x(i)^p \times t^{pi}) \wedge y = \Sigma(z).$$

Thus we have shown the following result:

(3.12) Theorem. *The differential field (K, D) and the 3-sorted structure $(L, C, \mathcal{F})$ are bi-interpretable, uniformly in p. The interpretation of $(L, C, \mathcal{F})$ in (K, D) is done via existential formulas, and the interpretation of (K, D) in $(L, C, \mathcal{F})$ is done by formulas involving only existential quantifiers of the sort L, but universal quantifiers of the sort $\mathcal{F}$. The Frobenius map $x \mapsto x^p$ is definable in (K, D) uniformly in p.*

(3.13) Concluding remarks. The 3-sorted structure $(L, C, \mathcal{F})$ is in fact a second-order structure. Indeed, consider those elements of L with image contained in $\{0, 1\}$ (i.e., the idempotents of the ring $(L, +, \times)$). These functions are characteristic functions of (definable) subsets of $\mathcal{F}$. These elements allow us to quantify over *all* subsets of $\mathcal{F}$, thus giving us a second-order structure.

The function h is strongly related to the λ-functions of Delon [D]. Recall that, in our case, the λ-functions of the *field* L, denoted by $\lambda_0, \ldots, \lambda_{p-1}$, are defined uniquely by the equation

$$x = \sum_{i=0}^{p-1} \lambda_i(x)^p t^i.$$

The map h gives us, when composed with the inverse of the map defined in (3.11), a map $H : L \times \mathcal{F} \to L$, such that for every $a \in L$ and $i \in \mathcal{F}$, $H(a, i) = \lambda_i(a)$.

Note that in order to get bi-interpretability of $(L, C, \mathcal{F})$ with the differential field K, we had to use the evaluation map h. It would therefore be interesting to study reducts of the structures $(L, C, \mathcal{F})$, as p goes to ∞, in weaker languages. For instance, one could retain the ring structure on L given by pointwise addition and multiplication, but delete the function h and add the shift operator of (2.10) and the sum-map of (3.3). Another interesting reduct would be the field K, together with a predicate W for the K^p-subspace defined by $h(x, 0) = 0$. Again, as p tends to ∞, it is likely that the theory becomes quite complicated. While it is unlikely that we can define the λ-functions or the derivation, we are still able to define in (K, W), uniformly in p, the image of the derivation D_p (as it equals $t^{-1}W$). Other examples of reducts are the fields (K, f), where f is the function λ_0, or the function $\lambda_{(p-1)/2}$.

4. Some elementary examples

(4.1) As a consequence of Theorem (2.11), there exists a nonlinear differential equation (in several unknowns) over $\mathbb{Q}(t)$, having an accidental separable algebraic solution modulo p for almost every prime p, but for purely Gödelian reasons, without any global geometric reason at all. In fact, there exists a differential equation over $\mathbb{Q}(t)$ having a separable algebraic solution modulo p for almost every prime p, but such that this fact is not provable in ZFC. For let X be the set of differential equations over $\mathbb{Q}(t)$ admitting an algebraic solution, or more generally having a separable algebraic solution modulo p for almost all p *provably in ZFC*. Let Y be the set of differential equations over $\mathbb{Q}(t)$, having a separable algebraic solution modulo p for almost every prime p. Then $X \subset Y$. Now X is Σ_1, while Y is Σ_2-complete, so $X \neq Y$.

The formula $\gamma^*(z)$ of (2.11) is positive existential, and deciding which of the sentences $\gamma^*(c)$, $c \in \mathbb{N}$, holds in almost all differential fields $(\mathbb{F}_p(t)^s, D_p)$ is a Σ_2-complete problem. To this formula corresponds a family of Kolchin closed sets $X(z, t)$ which we will now describe. Consider the $\mathcal{L}_e$-formula $\gamma(z)$ defined in Part 2 of the proof of Theorem (1.5), and write it as $\exists \bar{v}\, \theta(\bar{v}, z)$, where $\theta(\bar{v}, z)$ is positive quantifier-free. One verifies that, given $c \in \mathbb{N}$ and a prime p sufficiently large, the set $\{\bar{a} \in \mathcal{F}_p \mid \mathcal{F}_p \models \theta(\bar{a}, c)\}$ is either empty (if $\mathbb{N} \models \neg\alpha(c)$), or else is finite but of size growing with p (of order of magnitude at least $\log_2^4(p)$), so that it will be infinite in any non-principal ultraproduct of the $\mathbb{F}_p(t)^s$'s. By the results of Section 2, there is an $\mathcal{L}_D$-formula $\exists \bar{w}\, \theta^*(\bar{w}, x, \bar{v}, z)$, where θ^* is quantifier-free positive, such that if (K, D) is a model of T, $t \in K$ satisfies $Dt = 1$ and $\mathcal{F} \subset K$ is defined by $Dx = 0 \wedge \exists y\ (y \neq 0) \wedge tDy = xy$,

then for any $(\bar{a}, c)$ in $\mathcal{F}$,

$$\mathcal{F} \models \theta(\bar{a}, c) \iff K \models \exists \bar{w}\, \theta^*(\bar{w}, t, \bar{a}, c).$$

Furthermore, one verifies that given $(\bar{a}, c) \in \mathcal{F}$, the set of $\bar{w} \in \mathbb{F}_p(t)^s$ satisfying $\theta^*(\bar{w}, t, \bar{a}, c)$ is either empty, or has fixed Kolchin order m not depending on the particular model of T. Let $X(z, t)$ be the family of Kolchin closed sets defined by the formula $\theta^*(\bar{w}, t, \bar{v}, z)$. If $c \in \mathbb{N}$ satisfies α, then the order of $X(c, t)$ is at least $m + 1$. On the other hand, for p sufficiently large, reducing modulo p the equations defining $X(c, t)$, we get a Kolchin closed set $X_p(c, t)$ defined over $\mathbb{F}_p(t)$, also of order $\geq m + 1$. However, the set of $\bar{a} \in K_p$ such that there is some $\bar{w}$ with $(\bar{w}, \bar{a}) \in X_p(c, t)$ is finite because it is contained in $\mathcal{F}$; thus the Kolchin closure of $X_p(c, t)(\mathbb{F}_p(t)^s)$ has order m, and the set of solutions of $X_p(c, t)$ in $\mathbb{F}_p(t)^s$ is never Kolchin dense in $X_p(c, t)$.

Here are some similar cases occurring for arithmetic and geometric rather than logical reasons.

(4.2) Example. There exist linear differential equations over $\mathbb{Q}(t)$, with a basis of solutions in $\mathbb{F}_p(t)$ for infinitely many primes p, but with no nonzero solution in $\mathbb{Q}(t)^{\mathrm{alg}}$.

Proof. Take the equation $(t^2D^2 + tD - 2)x = 0$. If $b^2 = 2$, we can factor it as

$$(tD - b)(tD + b)x = 0$$

(Note that the operators $(tD - c)$ commute with each other if $c \in \mathbb{Q}^{\mathrm{alg}}$.) If $b \in \{0, \ldots, p-1\}$, and $b^2 \equiv 2 \bmod p$, this has solutions t^b, t^{-b}. Conversely, if $0 \neq x \in \mathbb{F}_p(t)^s$ is a solution, write $x = \sum_{i=0}^{p-1} a_i t^i$. Then $(t^2D^2 + tD - 2)x = 0$ translates to $(i(i-1) + i - 2)a_i = 0$ for all $i \geq 1$. If $p > 2$ is such that 2 is not a square mod p, there are no nonzero solutions in $\mathbb{F}_p(t)^s$. Hence there can be no nonzero solutions in $\mathbb{Q}(t)^{\mathrm{alg}}$.

(4.3) Example. Linear differential equations over $\mathbb{Q}(t)$, with a solution in $\mathbb{F}_p(t)$ for almost all primes p, but with no nonzero solution in $\mathbb{Q}(t)^{\mathrm{alg}}$.

Proof. Let L be a non-cyclic finite Galois extension of $\mathbb{Q}$, $G = \mathrm{Gal}(L/\mathbb{Q})$. We form a (finite) set $S = \{a_1, \ldots, a_n\}$ by choosing for each $\sigma \in G$, $\sigma \neq 1$, an element $a \in \mathrm{Fix}(\sigma) \setminus \mathbb{Q}$. We impose furthermore the condition that the set S is closed under the action of G, and the a_i's are distinct. Then $F(T) = \prod_{i=1}^{n}(T - a_i) \in \mathbb{Q}[T]$, and the differential equation

$$(*) \qquad F(tD)x = \prod_{i=1}^{n}(tD - a_i)x = 0$$

has its coefficients in $\mathbb{Q}(t)$.

Then $(*)$ has a solution of the form t^b in $\mathbb{F}_p(t)$, for almost all p: Indeed, any pseudo-finite field containing $\mathbb{Q}$ must contain $\mathrm{Fix}(\sigma)$ for some $\sigma \in G$, and

hence a root b of $F(T)$. So for almost all p there exists $c = t^b \in \mathbb{F}_p(t)$ solving $F(tD)x = 0$.

On the other hand, $\mathbb{Q}(t)^{\mathrm{alg}}$ does not contain a non-trivial solution of this equation. Indeed, assume by way of contradiction that c is such a solution, and choose k largest such that $c_k \stackrel{\mathrm{def}}{=} \prod_{i=1}^{k}(tD - a_i)c \neq 0$. Then $k < n$, so that c_k is a non-trivial solution (in $\mathbb{Q}(t)^{\mathrm{alg}}$) of the equation $tDx = a_{k+1}x$. This gives us the desired contradiction, as $a_{k+1} \notin \mathbb{Q}$.

(4.4) Example. Here is an example of the same phenomenon, with geometric rather than arithmetic overtones. Consider the system of equations

$$Dy_1 = Dy_2 = 0,\ (t-1)^{-1}y_1 + t^{-1}y_2 = Dz.$$

This has a solution with $(y_1, y_2) \neq (0,0)$ iff $t^{-1}, (t-1)^{-1}$ are linearly dependent over the constants, modulo the image of D. This is the case for all p, since indeed the image of D has codimension 1 over the constants in $\mathbb{F}_p(t)^s$. But it is not the case in characteristic 0. Equivalently, the equation $Du = 0$, $(t-1)^{-1}(u-1) - t^{-1}u = Dz$, has a solution in $\mathbb{F}_p(t)^s$ for all primes p, but does not have a solution in $\mathbb{Q}(t)^{\mathrm{alg}}$.

(4.5) Let us now give an example of the kind of guess that the logic would immediately show to be false. The culprit in Examples (4.1) and (4.2) is the logarithmic derivative. It seems possible indeed that these derivatives have a special role in this story, at least for linear differential equations. If the ratio of the logarithmic derivatives of two elements is algebraic, then for infinitely many p it can become rational, and then a transcendental relation in characteristic 0 becomes algebraic modulo infinitely many primes. (The same phenomenon occurs for the Abelian analogues, but we feel too diffident to hazard a guess about their role in the general situation.)

Let $\mathbb{Q}(t) = L_0 \subset L_1 \subset \cdots \subset L_n$ be a sequence of fields of algebraic functions, where each L_{i+1} is either algebraic over L_i, or has the form $L_i(u^\alpha)$ for some $\alpha \in \mathbb{Q}^{\mathrm{alg}}$ and some $u \in L_i$. If a differential equation has a solution in such an L_n, then it has an algebraic solution mod p for infinitely many p (for those p splitting completely in the number field generated by the various α). By (4.1), the converse is false, nor would adding Abelian logarithms, etc., help.

5. Statement of the conjecture and generic solutions

We state here the conjecture referred to in the introduction, in the form we heard it from David Kazhdan. Our lemmas here were all anticipated by [ESBT], and by [E]. (A possible exception is a simple lemma showing the equivalence between a foliation and a vector field version of the conjecture.) Paragraphs (5.1)–(5.9) contain preliminary results, and (5.10)–(5.13) discuss

the problems in characteristic p and non-linear Cartier. The statements of the conjecture and its equivalent formulations appear in (5.15).

(5.1) Preliminaries. Our varieties will always be affine non-singular varieties, and we will always be working birationally. Recall that if K is an algebraically closed field, $f_1(\bar{X}), \ldots, f_m(\bar{X})$ generate a prime ideal of $K[\bar{X}]$, and $V \subset \mathbb{A}^n$ is defined by the equations $f_i(\bar{x}) = 0$, $i = 1, \ldots, m$, then the tangent bundle of V, $T(V)$, is the set of tuples $(\bar{x}, \bar{u}) \in \mathbb{A}^{2n}$ satisfying $\bar{x} \in V$, and $\sum_{j=1}^{n} \frac{\partial f_i}{\partial X_j}(\bar{x}) u_j = 0$ for $i = 1, \ldots, m$. If $\bar{x} \in V$, then $T_{\bar{x}}(V) = \{\bar{u} \mid (\bar{x}, \bar{u}) \in T(V)\}$. If $g, h \in K(V)$, then we define $hdg : T(V) \to \mathbb{A}^1$, by $hdg(\bar{x}, \bar{u}) = h(\bar{x}) dg_{\bar{x}}(\bar{u}) = h(\bar{x}) \sum_{j=1}^{n} \frac{\partial g}{\partial X_j}(\bar{x}) u_j$. A *1-form on V* is then a sum of functions as above, and an *exact 1-form* is one of the form dg for some $g \in K(V)$.

If the field K has a derivation D, then we also define the shifted tangent bundle $T_D(V)$, by the equations $\bar{x} \in V$, $\sum_{j=1}^{n} \frac{\partial f_i}{\partial X_j}(\bar{x}) u_j + f_i^D(\bar{x}) = 0$ for $i = 1, \ldots, m$ (where f_i^D is the polynomial obtained by applying D to the coefficients of f_i). Note that if V is defined over the constants of K, then $T_D(V) = T(V)$.

(5.2) Generalities regarding differential fields. We fix a field K with a derivation D, and a differentially closed field $\mathbb{U}$ containing K. A *Kolchin closed* subset of the affine n-space $\mathbb{A}^n(\mathbb{U})$ is one defined by a set of differential equations. When V is a smooth variety, and s is a *rational section of the shifted tangent bundle* $T_D(V)$ of V (that is, a rational map $V \to \mathbb{A}^n$, which to each point $\bar{x}$ in a Zariski open subset of V associates an element of $T_{\bar{x},D}(V)$), the equation

$$D\bar{x} = s(\bar{x})$$

is said to be in *standard form*, and defines a subset $X = X_s$ of V. The pair (V, s) is called a *standard presentation for X*. A rational section of $T(V)$ will also be called a *(rational) vector field on V*. A Kolchin-closed subset of X_s is then just the intersection with X_s of an algebraic variety. Hence, a subset of X is Kolchin-dense iff it is Zariski dense. We define the *Kolchin order of X_s* to be $\dim(V)$.

Note that being given standard presentations for X over K is equivalent to being given an extension D_s of the derivation D to $K(V)$. Note also that any Kolchin closed set of finite order is differentially birationally equivalent to a set given by an equation in standard form.

If $f = (f_1, \ldots, f_k) : V \to W$ is a morphism of varieties (defined over K), then for all $\bar{x}$ in a Zariski open subset of V and all $\bar{u} \in T_{\bar{x}}(V)$ we have $df_{\bar{x}}(\bar{u}) \in T_{f(\bar{x})}(W)$, and $\{df_{\bar{x}}(\bar{u}) \mid \bar{u} \in T_{\bar{x}}(V)\}$ describes the subspace $T_{f(\bar{x})}(f(V))$ of $T_{f(\bar{x})}(W)$. If f is onto and s is a rational section of the tangent bundle $T(V)$, then we obtain a rational section s' of $T(W)$, defined by $s'(f(\bar{x})) = df_{\bar{x}}(s(\bar{x}))$. We then write " $s' \circ f = df \circ s$ ". Note that in this case the map $f^* : K(W) \to$

$K(V)$ is an inclusion, and if $D_{s'}$ and D_s are the K-derivations on $K(W)$ and $K(V)$ corresponding to s' and s, then $f^* \circ D_{s'}$ is the restriction of D_s to $f^*(K(W))$.

A *foliation* on a variety V is (for us, working algebraically and birationally) a definable map f on V, such that $f(\bar{x})$ is a line in $T_{\bar{x}}(V)$. Equivalently, a foliation is given by a nonzero vector field s on V, but if $h \neq 0$ is a rational function on V, then s and hs define the same foliation.

(5.3) Computational lemma. *Let K be an infinite field of characteristic $p > 0$, and D a non-trivial derivation on K.*

(1) *D^p is a derivation, so is cD for any $c \in K$.*
(2) *If $1 < m < n < p$ and $L = \sum_{i=m}^{n} a_i D^i$ is a derivation, then $a_i = 0$ for each i, $m \leq i \leq n$.*
(3) *If D and cD commute, then $Dc = 0$.*
(4) *$(cD)^p = eD + c^p D^p$, where $e = (cD)^{p-1}c$. (Thus if $D = bD_1$, then $D^p = (D^{p-1}b)b^{-1}D + b^p {D_1}^p$.)*
(5) *If $D^p = 0$, then $(aD)^p$ is proportional to D. (More generally, if D^p is proportional to D, then so is $(aD)^p$.)*
(6) *Suppose $D^p = aD$. Let $D = bD_1$, where $a = (D^{p-1}b)b^{-1}$. Then $aD = D^p = (D^{p-1}b)b^{-1}D + b^p {D_1}^p$, so ${D_1}^p = 0$.*
(7) *If $D = bD_1$, then $-b^{p+1}D_1^{p-1}(b^{-1}) = D^{p-1}b$.*
(8) *If $D = bD_1$, then $(D_1^{p-2})(b^{-1}) = -b^{-p}D^{p-2}b$.*

Proof. (1) is standard. To see (2), expand

$$L(xy) - xLy - yLx = \sum_{i=m}^{n} \sum_{j=0}^{i} a_i \binom{i}{j} (D^j x)(D^{i-j} y) - \sum_{i=m}^{n} x a_i D^i y + y a_i D^i x.$$

This differential polynomial must vanish identically on K^2, and as K is infinite and D is not trivial, it must be 0. The coefficient of $(Dx)(D^{i-1}y)$ shows that $a_i = 0$.

(3) follows from $[D, cD] = (Dc)D$.

(4) follows from (2): $(cD)^p$ is a derivation, and is a linear combination of $D, D^2, \ldots, D^p$ and thus must be a linear combination of D, D^p alone. An easy computation gives the exact value of the coefficients.

(5) and (6) are immediate consequences of (4).

(7) can be derived by using (4) in two ways, once with $D = bD_1$ and once with $D_1 = b^{-1}D$, and comparing the two resulting expressions for $D^p - b^p {D_1}^p$. Now if one applies D_1 to (8) and multiplies by b^{p+1} one obtains (7). Thus in (8) we have at least that $D_1^{p-2}b^{-1} + b^{-p}D^{p-2}b$ is a constant (of D). However, an explicit evaluation would yield a polynomial in $Db, \ldots, D^{p-2}b$ that can only be a constant in general if it vanishes in general.

(5.4) Definition of $s^{(p)}$. Using the identification above of sections of $T_D(V)$ with derivations on $K(V)$, we write $s^{(p)}$ for the rational section t such that $D_t = (D_s)^p$, the iterated composition of p copies of D_s (which is a derivation by (5.3)).

Warning. We use this notation even if s is not defined over the constants. In particular, it may happen that V is defined over the constants while s is not. In this case $s^{(p)}$ *depends on the derivation* D *on* K, and not only on the algebraic data K, V, s. Nonetheless, we will write simply $s^{(p)}$ when this does not lead to confusion.

Lemma. *Let K be a separably closed field of characteristic $p > 0$.*

(1) *Let V be a smooth variety over K. Let ω be an exact 1-form on V, and let s be a vector field. Suppose $\omega \circ s = 0$. Then $\omega \circ s^{(p)} = 0$.*
(2) *In (1), assume instead $\omega \circ s = 1$. Then still $\omega \circ s^{(p)} = 0$.*

Proof. (1) We work in the function field $F = K(V)$. Let $\omega = dg_1$, and let $g_1, g_2, \ldots, g_n$ be a separating transcendence basis of $K(V)$ over K. (If $g_1 \in K(V)^p K$, then $\omega = 0$ and there is nothing to prove). So we have a basis $D_i = \partial/\partial g_i$ for the K-derivations of F. Observe first that, on the polynomial ring $K[g_1, \ldots, g_n]$, the analogue of (5.3)(2) is valid for the (partial) derivatives $D_1, \ldots, D_n$: If $L = \sum_\nu a_\nu D^\nu$ is a differential operator, where all the D^ν are of the form $D_1^{i(1)} \cdots D_n^{i(n)}$, with $0 \le i(j) < p$ for each $j \le n$ and $\sum_j i(j) \ge 2$, and if L is a derivation, then $L = 0$. This is proved in the same way as (5.3)(2), using the Leibniz rule for several commuting derivations. Observe also that each $D_i^p = 0$. Hence the same holds in $K(V)$.

Now write $D_s = \sum_{i=1}^n b_i D_i$. Then $0 = \omega \circ s = b_1$, so actually $D_s = \sum_{i=2}^n b_i D_i$. Thus D_s^p is a differential operator involving products of the D_i, $i \ge 2$. By the first paragraph, $D_s^p = \sum_{i=2}^p c_i D_i$ for appropriate $c_i \in K(V)$. Thus $\omega \circ s^{(p)} = 0$.

(2) Let $\omega = dg$. Let $W = V \times \mathbb{A}^1$, $t \in K(W)$ correspond to the projection $W \to \mathbb{A}^1$, and let $\omega' = d(g - t) = dg - dt$ (an exact 1-form on W). Let $s' = (s, 1)$. Then $\omega' \circ s' = dg \circ s - (dt) \circ 1 = 1 - 1 = 0$. By (1), we have $\omega' \circ (s')^{(p)} = 0$. But $(s')^{(p)} = (s^{(p)}, 0)$. So $dg \circ s^{(p)} = 0$.

(5.5) Definition of integrability. Let V be a smooth variety, s an everywhere defined rational vector field on V, and f the corresponding foliation.

(1) We say that C is an *algebraic integral curve of* f, if $C \subset V$ is an algebraic curve such that on some Zariski open subset C' of C, we have $s|_{C'} \subseteq T(C')$ (Note that this does not depend on the choice of s.) An integral curve of a vector field is then an integral curve of the corresponding foliation.
(2) We assume that the characteristic is 0. We say that f is (birationally) *integrable* if through every point in a Zariski open subset of V there

passes an algebraic integral curve of f. Similar terminology is used for s.

(5.6) Lemma (char. 0). *Let V be a smooth variety and s an everywhere defined rational vector field on V, defined over an algebraically closed field L, with $s \neq 0$, and f the corresponding foliation. Let $(\mathbb{U}, D)$ be a differentially closed field, with L contained in the field k of constants of $\mathbb{U}$. Let $X = X_s = \{x \in V \mid Dx = s(x)\}$. The following conditions are equivalent:*

(I1) *f is integrable.*

(I2) *There exists a Zariski open set $V^0 \subset V$ and a regular rational function $h : V^0 \to V'$ with irreducible fibres of dimension 1, all of whose fibres are integral curves of f.*

(I3) *There exists a differential rational function $g : X \to X'$ with $X' = V'(k)$ a definable subset of the constants, g defined over the constants, and with fibres of Kolchin order 1.*

Proof. Assume (I1), and $s \neq 0$. By compactness, there exists a Zariski-closed set $E \subset V$ and a constructible family $\{C_a \mid a \in M\}$ of (irreducible) curves on V, such that s does not vanish on $V^1 = V \setminus E$, and through any $p \in V^1$ there exists $a \in M$ with $p \in C_a$, and C_a an (irreducible) integral curve of s. We may assume that if $a \neq b \in M$, then the intersection $C_a \cap C_b$ is finite. (Otherwise we factor M by the definable equivalence relation $a \sim b$ if and only if $C_a \cap C_b$ is infinite.) Then, for any point $p \in V^1$, there exists a unique integral curve C_a through p. It follows that $a = h(p)$, for some rational function $h : V^0 \to M$, for some Zariski open subset V^0 of V with $C_a = h^{-1}(a)$ for $a \in V^0$. Thus (I2) holds, with $V' = M$. That (I2) implies (I1) is clear.

Assume (I2). Factoring V' by the relation $h^{-1}(a) = h^{-1}(b)$, we may assume that for each $p \in V^0$, $h(p)$ generates the field of definition of the curve $h^{-1}(h(p))$. Since everything said so far is purely algebraic, we may assume that h and V' are defined over k. We will now show that if $p \in X = X_s$, then $D(h(p)) = 0$. Let $p \in X$, $a = h(p)$, $C_a = h^{-1}(a)$. Then the tangent space $T_p(C_a)$ is defined by the equation $dh_p(\bar{u}) = 0$. Since h is defined over the constants and $p \in X$, we have $Da = Dh(p) = dh_p(Dp) = dh_p(s(p))$. Because C_a is an integral curve of s, we have $s(p) \in T_p(C_a)$, and therefore $Da = 0$. Clearly, if $a \in V'(k)$, then $h^{-1}(a) = C_a$ defines a subset of V of Kolchin order 1.

We now assume (I3). Let L' be an algebraically closed subfield of k over which everything is defined, and fix a generic $p \in X$ over L', and $a = g(p)$. Since $Dp = s(p)$, we may assume that g is a rational polynomial function. Then $g^{-1}(a)$ is a Kolchin closed subset of X of order 1. Let Y_a be an irreducible component of $g^{-1}(a)$ passing through p, of maximal order. If $\dim(Y_a) = 0$, then p is algebraic over $L'(a)$, i.e., $X \subset k$. Thus $s = 0$, a contradiction. It follows that $\dim(Y_a) = 1$, and the Zariski closure C_a of Y_a in V is an irreducible

algebraic curve, defined over some finite extension of $L'(a)$. Hence, replacing X' by some finite cover $Y' \to X'$, we may assume that $g^{-1}(a)$ is irreducible, of dimension 1. As p was generic, this holds on some Kolchin-dense subset X^0 of X.

Since g is defined over the constants, g extends to a rational polynomial map h defined on some Zariski open subset V^0 of V, taking its values in V'. From $Dh(p) = 0$ we deduce that $dh_p(Dp) = dh_p(s(p)) = 0$, so that $s(p) \in T_p(C_a)$. This being true at a generic point of V, it is true on some Zariski open subset of V and shows that for almost all $a \in V'$, $h^{-1}(a)$ defines an irreducible algebraic integral curve of s.

(5.7) Lemma (char. 0). *Let V and V' be varieties, and $f : V \to V'$ a finite-to-one onto rational map. Assume that s is a vector field on V, s' is a vector field on V', and that $df \circ s = s' \circ f$. Then (V, s) is integrable if and only if (V', s') is integrable.*

Proof. Our assumption implies that if $\mathbb{U}$ is a differentially closed field such that all data are defined over some subfield L of the constants k, then f induces a finite-to-one map $X \to Y$, where $X = X_s \subset V$, and $Y = X_{s'} \subset V'$. (I3) immediately gives that if (V', s') is integrable, then so is (V, s). Conversely, assume that $g : X \to X'$ is a rational map with fibres of dimension 1, and with $X' = W(k)$, for some variety W. By the proof of (5.6), we may assume that for each $a \in X'$, $g^{-1}(a)$ is an irreducible Kolchin closed subset of X of dimension 1, and that $a \neq b$ implies $g^{-1}(a) \neq g^{-1}(b)$. We factor X' by the equivalence relation E defined by $E(a, b)$ if and only if for some generic $p \in g^{-1}(a)$ and generic $p' \in g^{-1}(b)$ we have $f(p) = f(p')$. Because we are in a stable context, this is an equivalence relation, with finite classes as f is finite-to-one. By elimination of imaginaries, and because the structure induced on k by $\mathbb{U}$ is the pure field structure, we get $X'/E = W'(k)$, for some algebraic variety W' defined over k. This gives us a rational map $g' : Y \to W'(k)$ satisfying the assumptions of (I3).

Remark (char. 0). Let $f : V \to V'$ be as above, with everything defined over some algebraically closed field L. While not every vector field s on V is such that $df \circ s$ is of the form $s' \circ f$, the converse is true: If s' is a vector field on V', then there is a vector field s on V such that $df \circ s = s' \circ f$. This follows from the fact that the derivation $D_{s'}$ on $L(V')$ defined by s' extends uniquely to a derivation of $L(V)$. (As f is finite-to-one, $L(V)$ is a finite algebraic extension of $L(V')$.) This derivation in turn defines a rational vector field s on V, and s clearly satisfies $df \circ s = s' \circ f$. (In positive characteristic, one needs to assume in addition that f is separable.)

(5.8) Definition of parametric integrability. Let V be a smooth variety and s an everywhere defined rational vector field on V, and f the corresponding foliation. We say that (V, f) (or (V, s)) is *parametrically integrable*

if for a generic $v \in V$ there exists a curve C, a finite-to-one rational map $\pi : C \to \mathbb{A}^1$, and a rational map $g : C \to V$ such that, if s_1 is the vector field on C satisfying $d\pi \circ s_1 = 1 \circ \pi$ (where 1 is the constant vector field on $\mathbb{A}^1$), then $dg_a \circ s_1(a) = s(v)$ for some $a \in C$ with $g(a) = v$ and (v, a) a generic of $V \times C$ (over the field of definition of V and C). We then call $g(C)$ a *parametrised curve through* v.

(5.9) Lemma. *Let (V, s) be as above, defined over an algebraically closed field L of characteristic 0. Let $(\mathbb{U}, D)$ be a differentially closed field, with L contained in the field k of constants of $\mathbb{U}$, and fix $t \in \mathbb{U}$, $Dt = 1$. Let $X = X_s = \{x \in V \mid Dx = s(x)\}$. The following conditions are equivalent:*

(PI0) *s is parametrically integrable.*

(PI1) *Let $s^*(v, u) = (s(v), 1)$, so that s^* is a vector field on $V \times \mathbb{A}^1$. Then s^* is integrable.*

(PI2) *There exists a finite-to-one rational map $g : V \to V'$, a vector field s' on V' satisfying $dg \circ s = s' \circ g$, a variety W and a dominant map $f : W \times \mathbb{A}_1 \to V'$, such that for $w \in W$, $\{f(w, t') \mid t' \in \mathbb{A}^1\}$ describes an integral curve of s'.*

(PI3) *There exists (over L) a finite-to-one differentially rational map $h : X \to X'$, and with $X' \subset k(t)$.*

(PI3') *$X \subset k(t)^{\mathrm{alg}}$.*

Proof. Assume (PI0), let v be a generic of V, and let C, g, π, s_1, a be as in Definition (5.8), $b = \pi(a)$. Then $C' = \{(g(t'), \pi(t')) \mid t' \in C\}$ defines a curve C' on $V \times \mathbb{A}^1$. The tangent space $T_{(v,b)}(C')$ is then parallel to $(dg_a \circ s_1(a), d\pi_a \circ s_1(a)) = (s(v), 1)$. Hence C' is an algebraic integral curve for s_1. As (v, b) is a generic of $V \times \mathbb{A}^1$, this shows that $s_1 = s^*$ is integrable.

Conversely, assume (PI1), and let $C \subset V \times \mathbb{A}^1$ be an algebraic integral curve for s^* through some generic point (v, b) of $V \times \mathbb{A}^1$. Let $\pi : C \to \mathbb{A}^1$ be the restriction to C of the projection $V \times \mathbb{A}^1 \to \mathbb{A}^1$. By assumption $s^*|_C \subset T(C)$, so that $(s(v), 1) \in T_{(v,b)}(C)$, and this implies that the map π is not constant, i.e., that it is dominant and therefore finite-to-one. Define a vector field s_1 on C by $d\pi \circ s_1 = 1 \circ \pi$ (see Remark (5.7)), and let $g : C \to V$ be induced by the projection $V \times \mathbb{A}^1 \to V$. Then (g, π) corresponds to the inclusion $C \subset V \times \mathbb{A}^1$, so that $T_{(v,b)}(C)$ is parallel to $(dg_{(v,b)} \circ s_1(v, b), d\pi_{(v,b)} \circ s_1(v, b))$. This implies that $dg_{(v,b)} \circ s_1(v, b) = s(v)$, which is what we wanted to prove.

(PI2) clearly implies (PI1), using Lemma (5.7), as for $w \in W$, $\{(f(w, t), t) \mid t \in \mathbb{A}_1\}$ is an integral curve of $(s', 1)$.

(PI3) implies (PI2): Since X is in standard form, we may assume that the differential map h is in fact an algebraic (rational) map. Since X' is of finite order, we may also assume, changing h if necessary, that X' is in standard form: If $v \in X$, then $D(h(v)) \in L(v, Dv, \dots) = L(v)$. Let (V', s') be a standard presentation for X'.

If a is a generic element of X', then $a \in L(t, c_1, \ldots, c_m)$ for some $c_1, \ldots, c_m \in k$. Note that if $c = (c_1, \ldots, c_m)$, then c and t are independent, so the (differential) locus Z of c over $L(t)$ is in fact defined over L, and is a Kolchin closed subset of k^m. Thus there exists a dominant rational map (defined over $L(t)$) $g_0 : Z \to X'$. The map g_0 naturally defines a rational dominant map $g : W \to V'$, where W is the Zariski closure of Z (which is defined over L).

Let f be a tuple of elements of $L(W \times \mathbb{A}^1)$ such that for $z \in W$ we have $g(z) = f(z, t)$. We obtain an algebraic dominant map $f : W \times \mathbb{A}^1 \to V'$, which is defined over L. Let c and a be as in the previous paragraph. Then (c, t) is a generic point of the algebraic set $W \times \mathbb{A}^1$, and $a = f(c, t)$ is a generic point of V'. Since $f(c, t) \in X'$, $D(f(c, t)) = s'(f(c, t))$. Since f is defined over $L \subset k$ and $c \in k^m$, we obtain that $D(f(c, t)) = \frac{\partial f}{\partial T}(c, t) = s'(f(c, t))$. This shows that the curve $\{f(c, u) \mid u \in \mathbb{A}^1\}$ is an integral algebraic curve for s' passing through a. As a is a generic of V', this shows that (V', s') is integrable.

(PI3) clearly implies (PI3'). Assume that (PI3') holds, let a be a generic of X over L, and let b be the tuple of coefficients of the minimal polynomial of a over $k(t)$. Then $b \in \mathrm{dcl}(L, a)$: Any automorphism of $\mathbb{U}$ which fixes a induces an automorphism of $k(t)$ (as it is the smallest field containing k and the set of solutions of $Dx = 1$), and therefore fixes b. Hence there is a differential rational map h defined over L such that $h(a) = b$. This map h is defined on a Kolchin dense subset of X, and has for image a definable set X' consisting of tuples in $k(t)$, because $b \in k(t)$. Since a is algebraic over the tuple b, the map h is (generically) finite-to-one.

It remains to show that (PI1) implies (PI3'), or, since we are working birationally, that $X \setminus E \subset k(t)^{\mathrm{alg}}$ for some proper Kolchin closed $E \subset X$.

Let Y be the Kolchin set with standard presentation $(V \times \mathbb{A}^1, s^*)$, and let $(a, u) \in Y$ be generic. Let $g : Y \to Y' = V'(k)$ be given by (I3). As $Du = 1$, we know that u is a generic (over k) of the set defined by $Dx = 1$. Since the fibres of g have Kolchin order 1, it follows that a is algebraic over $k(u) = k(t)$, which proves (PI3').

(5.10) p-torsion and algebraic points. In characteristic $p > 0$, the differential field of separable algebraic functions $\mathbb{F}_p(t)^s$ satisfies an additional universal axiom, and indeed an equation: $D^p = 0$.

Proposition. *Let (L, D) be a differential field satisfying $p = 0$ and $D^p = 0$. Then (L, D) embeds into an elementary extension of $(\mathbb{F}_p(t)^s, D)$. If $u \in L$ satisfies $Du = 1$, one can demand $u \mapsto t$.*

Proof. If every element of L is a constant, i.e., if $D = 0$, then the (trivial) differential field L embeds into the field of constants of an elementary extension of $\mathbb{F}_p(t)^s$. Otherwise, we show that there exists $u \in L$, $Du = 1$. There exists $a \in L$, $Da \neq 0$. We still have $D^p a = 0$, so for some $i \geq 0$, $D^{i+1} a \neq 0$,

$D^{i+2}a = 0$. Let $c = D^{i+1}a$, so that $Dc = 0$, and set $u = (D^i a)/c$. Then $Du = 1$.

Now start with any $u \in L$ with $Du = 1$. By induction on $\ell < p$, observe that any element of $\ker(D^\ell)$ can be written as $x = \sum_{0 \le i \le \ell-1} a_i u^i$, with $a_i \in \ker(D)$. (Let $a_{\ell-1} = (1/(\ell-1)!)D^{\ell-1}x$. Then $Da_{\ell-1} = 0$, $x - a_{\ell-1}u^{\ell-1} \in \ker(D^{\ell-1})$, and use induction.) In particular, the field L has dimension p over $\ker(D)$.

If $b \in L$, $Db = 0$, then by standard lemmas on derivations there exists an extension D_M of D to $M = L(b^{1/p})$ satisfying $D_M(b^{1/p}) = 0$. We have $(D_M)^p = 0$ (on L and on $b^{1/p}$, and hence in general). Iterating this, we may enlarge L so that any D-constant is a p-th power in L.

Now view L as a pure field. Then $[L : L^p] = [L : \ker(D)] = p$, so that the separable closure of L is a separably closed field of degree of imperfection 1, with p-basis $\{u\}$. By Ershov's theorem, L^s embeds elementarily in some elementary extension F of $\mathbb{F}_p(t)^s$, with $u \mapsto t$. Since both F and L have a unique derivation satisfying $Dt = 1$, resp. $Du = 1$, this embedding is an embedding of differential fields.

In fact, the theory of the differential field $\mathbb{F}_p(t)^s$ is the model companion of the universal theory of differential fields satisfying $D^p = 0$. It would be easy to prove the proposition without quoting Ershov, but we preferred to make the connection with existing model theory.

(5.11) Proposition (nonlinear Cartier). *Let (V, s) be a standard presentation for X over $\mathbb{F}_p(t)^s$ ($Dt = 1$). Then X has densely many separable algebraic solutions iff $s^{(p)} = 0$.*

Proof. Suppose X has densely many separable algebraic solutions. Then in an elementary extension L of the differential field $\mathbb{F}_p(t)^s$ it has a generic solution a. Now $L \models (\forall x)(D^p x = 0)$. Thus $D^p a = s^{(p)}(a) = 0$. Since a is generic, $s^{(p)}$ vanishes on V.

Conversely, suppose $s^{(p)} = 0$. Let $K = \mathbb{F}_p(t)^s(a)$, where a is a generic point of V over $\mathbb{F}_p(t)^s$. Extend the derivation of $\mathbb{F}_p(t)^s$ to K by setting $Da = s(a)$. Then $D^p a = s^{(p)}(a) = 0$. As D^p is a derivation, vanishing on $\mathbb{F}_p(t)^s$ and on a, it vanishes on K. By Proposition (5.10), K embeds into an elementary extension L of $\mathbb{F}_p(t)^s$. In L, X has a generic solution (namely a), so in the elementary submodel $\mathbb{F}_p(t)^s$, it has a solution outside any given proper subvariety of V.

(5.12) Important remark. In finite characteristic, Kolchin density of the separable algebraic solutions implies finite order of the equation; since the set of separable algebraic solutions definitely satisfies a finite order equation ($D^p x = 0$ if nothing else).

(5.13) Discussion and problems: Nonlinear Cartier cycles. The view of the question presented here, via existence of dense sets of separable algebraic points, raises an interesting issue. If a differential equation has a Zariski dense set of separable algebraic solutions over $\mathbb{Q}(t)$, it does *not* follow that almost all reductions modulo p have such a set of solutions. For instance, the Manin kernel equations have a Zariski dense set of solutions—the torsion points at least—but they are rarely integrable.

The conjecture is saved by some interesting algebraic cycles occurring only in positive characteristic. In the case of the Manin kernels, for each p, one obtains a differential equation of lower order, describing the multiples of p in the Abelian variety; cf. [BV]. More generally, given an equation in standard form (V, s), one obtains the (possibly reducible) $C_p(V)$ defined by the vanishing of $s^{(p)}$. Another example may be the definition of the graph of Frobenius given in Section 3.

It appears very interesting to study the asymptotic theories of these varieties $C_p(V)$, in particular cases and in general.

(5.14) Notation. In what follows, we will reduce polynomials, varieties over $\mathbb{Q}^{\mathrm{alg}}$ or $\mathbb{Q}^{\mathrm{alg}}(t)$, etc., modulo p, and indicate the resulting object over $\mathbb{F}_p^s$, resp. $\mathbb{F}_p(t)^s$, by a lower index p.

(5.15) Statements of the conjectures. Our aim in this section and the next one is to prove the equivalence of the following two conjectures:

(K) *Let f be a rational algebraic foliation on a variety V over $\mathbb{Q}^{\mathrm{alg}}$, represented by the rational vector field s. Assume that for almost all primes p, the vector field $s_p^{(p)}$ is proportional to the vector field s_p. Then (V, f) is integrable.*

(MK) *Let X be a Kolchin closed set of finite order, defined over $\mathbb{Q}(t)^{\mathrm{alg}}$, where $Dt = 1$. Assume that for almost all primes p, X_p has a Kolchin dense set of solutions in $\mathbb{F}_p(t)^s$, where $Dt = 1$. Then, in any differentially closed field $\mathbb{U}$ containing $\mathbb{Q}(t)$ and in which $Dt = 1$, $X \subset k(t)^{\mathrm{alg}}$, where k stands for the constants of $\mathbb{U}$.*

In (5.6), we have discussed algebraic integrability (giving a more obviously recursively enumerable form). Our proof of the equivalence of the two conjectures passes through a parametrised version (PK) of (K), which is more model-theoretically convenient, and which we state below. We then prove the equivalence of the homogeneous version stated as (K) with (PK).

Let us state immediately the parametrised version.

(PK) *Let s be a rational vector field on a variety V over $\mathbb{Q}^{\mathrm{alg}}$. Assume that for almost all primes p, $s_p^{(p)} = 0$. Then (V, s) is parametrically integrable.*

(5.16) Equivalence of the conjectures (K), (PK), and (MK).

(MK) $\Rightarrow$ (PK): Let (V, s) satisfy the assumptions of (PK), and let X be the Kolchin closed set it defines. By (5.11), for almost all p the reduction of X modulo p has a Kolchin dense set of solutions in $\mathbb{F}_p(t)^s$. By (MK) and (5.9), (V, s) is parametrically integrable.

(PK) $\Rightarrow$ (MK): We work in a differentially closed field $\mathbb{U}$. Let (V, s) be a standard presentation over $\mathbb{Q}^{\mathrm{alg}}$ for a Kolchin set X of finite order satisfying the hypothesis of (MK). By (5.11), $s_p^{(p)} = 0$ for almost all p. By (PK) and (5.9), this implies that $X \subset k(t)^{\mathrm{alg}}$. We have therefore shown that the validity of (PK) implies the validity of (MK) for Kolchin closed sets defined over $\mathbb{Q}^{\mathrm{alg}}$. It remains to show that this restricted version of (MK) implies the general one.

Let X be a Kolchin closed set defined over $\mathbb{Q}(t)^{\mathrm{alg}}$, $Dt = 1$, which we may and will assume irreducible, and which satisfies the hypotheses of (MK). Then X is defined over $\mathbb{Q}^{\mathrm{alg}}(t, t')$, where $t' \in \mathbb{Q}(t)^{\mathrm{alg}}$, and has standard presentation (V, s), with V and s defined over $\mathbb{Q}^{\mathrm{alg}}(t, t')$. We write $V = W(t, t')$, $s = s'(x, t, t')$, where W and s' are defined over $\mathbb{Q}^{\mathrm{alg}}$. Let C be the curve locus of (t, t') over $\mathbb{Q}^{\mathrm{alg}}$. Then the formula $(y, y') \in C \wedge Dy = 1$ isolates $tp(t, t'/\mathbb{Q}^{\mathrm{alg}})$ (the type in the sense of $\mathbb{U}$).

We now consider the Kolchin set Y defined by $(x, y, y') \in W \wedge Dx = s'(x, y, y') \wedge Dy = 1$. It is defined over $\mathbb{Q}^{\mathrm{alg}}$ and has order $1 + \mathrm{ord}(X)$. Note that for almost all p, the reduction C_p of the curve C modulo p is absolutely irreducible, and there exists $t'' \in \mathbb{F}_p(t)^s$ such that (t, t'') belongs to C_p.

Let p be a prime such that X_p has a Kolchin dense set of solutions in $\mathbb{F}_p(t)^s$. Then, in some elementary extension L of the differential field $\mathbb{F}_p(t)^s$, X_p has a generic solution a over $\mathbb{F}_p(t)^s$. But then (a, t, t'') is a generic solution of Y_p over $\mathbb{F}_p^s$, because $Dt = 1$. Hence Y_p has a generic point in L, and this implies that the set of points of $Y_p(\mathbb{F}_p(t)^s)$ is Kolchin dense in Y_p. By (MK) over $\mathbb{Q}^{\mathrm{alg}}$, we have $Y \subset k(t)^{\mathrm{alg}}$, where k stands for the constants of $\mathbb{U}$. As $X \times \{t, t'\} \subset Y$, we get the result.

(K) $\Rightarrow$ (PK): Given (V, s) as in (PK), consider (W, s^*), where $W = V \times \mathbb{A}^1$ and $s^* = (s, 1)$. Note that for every p, $s_p^{*(p)} = (s_p^{(p)}, 0)$. Thus if $s_p^{(p)} = 0$ then also $s_p^{*(p)} = 0$. By (5.3)(4) and (5), if $h \in \mathbb{Q}^{\mathrm{alg}}(W)$, $h \neq 0$, then $(hs^*)_p^{(p)}$ is proportional to $(hs^*)_p$. By (K), (W, hs^*) is integrable, hence so is (W, s^*), and it follows that (V, s) is parametrically integrable.

(PK) $\Rightarrow$ (K): Let (V, f) be as in (K), and let s be a vector field representing f. Let g be a nonconstant rational function on V, such that $dg \circ s \neq 0$. Replace s by $s/(dg \circ s)$; then $dg \circ s = 1$.

By Lemma (5.4), $dg_p \circ s_p^{(p)} = 0$. However, by assumption, $s_p^{(p)} = rs_p$ for some $r \in \mathbb{F}_p^s(V)$. Thus $r(dg_p \circ s_p) = 0$. So (recalling $(dg \circ s) = 1$) we have $r = 0$, and $s_p^{(p)} = 0$ for almost all p. At this point (PK) applies, so that s is

parametrically integrable. But parametric integrability implies integrability, since an algebraic integral curve of $(s, 1)$ projects to an algebraic integral curve of s.

References

[BV] A. Buium and F. Voloch, *Reduction of the Manin map modulo p*, J. Reine Angew. Math. **460** (1995), 117–126.

[Ch-L] A. Chambert-Loir, *Théorèmes d'algébricité en géometrie diophantienne (d'apès J.-B. Bost, Y. André, D. & G. Chudnovsky)*, Séminaire Bourbaki, 53ème année, 2000/2001, Mars 2001.

[D] F. Delon, *Idéaux et types sur les corps séparablement clos*, Mém. Soc. Math. France (N.S.) No. 33 (1988).

[DG] H. Gaifman and C. Dimitracopoulos, *Fragments of Peano's arithmetic and MRDP theorem*, Logic and algorithmic (Zurich, 1980), Monograph. Enseign. Math., 30, Univ. Genève, Geneva, 1982, pp. 187–206.

[E] T. Ekedahl, *Foliations and inseparable morphisms*, Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), Proc. Sympos. Pure Math. vol. 46, part 2, Amer. Math. Soc., Providence, RI, 1987, pp. 139–150.

[ESBT] T. Ekedahl, N. Shepherd-Barron, and R. Taylor, *A conjecture on the existence of compact leaves of algebraic foliations*, preprint, 1999; available at `http://www.dpmms.cam.ac.uk/~nisb/`.

[Er] Yu. Ershov, *Fields with a solvable theory*, Soviet Math. Dokl. **8** (1967), 575–576.

[K1] N. M. Katz, *Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin*, Inst. Hautes Études Sci. Publ. Math. **39** (1970), 175–232.

[K2] ———, *A conjecture in the arithmetic theory of differential equations*, Bull. Soc. Math. France **110** (1982), 203–239, 347–348.

[S] C. Smoryński, *Logical number theory I. An introduction*, Universitext, Springer-Verlag, Berlin-Heidelberg, 1991.

Z. Chatzidakis, UFR de Mathématiques, Université Paris 7, Case 7012, 2, place Jussieu, 75251 Paris Cedex 05, France

E-mail address: `zoe@logique.jussieu.fr`

E. Hrushovski, Institute of Mathematics, The Hebrew University, Givat Ram, 91904 Jerusalem, Israel

E-mail address: `ehud@math.huji.ac.il`