BULLETIN DE LA S. M. F.

NICHOLAS M. KATZ

A conjecture in the arithmetic theory of differential equations

Bulletin de la S. M. F., tome 110 (1982), p. 203-239

<http://www.numdam.org/item?id=BSMF_1982__110__203_0>

Bull. Soc. math. France.
110, 1982, p. 203-239.

A CONJECTURE IN THE ARITHMETIC THEORY OF DIFFERENTIAL EQUATIONS

BY

NICHOLAS M. KATZ (*)

ABSTRACT. — This article discusses a conjectural description of the Lie algebra of the differential Galois group attached to a linear differential equation as being the smallest algebraic Lie algebra whose reduction mod p contains, for almost all p, the p-curvature of the reduction mod p of the differential equation in question.

RÉSUMÉ. — On discute une description conjecturale de l'algèbre de Lie du groupe de Galois différentiel d'une équation différentielle linéaire comme étant la plus petite algébre de Lie algébrique dont la réduction modulo p contient, pour presque tout p, la p-courbure de la réduction modulo p de l'équation différentielle dont il s'agit.

TABLE OF CONTENTS

(*) Texte reçu le 19 septembre 1981.

N. M. KATZ, Department of Mathematics, Princeton University, Princeton, New Jersey, 08544 USA.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE — 0037-9484/1982/203/$ 5.00

Introduction

Consider a first order $n \times n$ system of homogeneous linear differential equations in one variable T

$$\frac{d}{dT}\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} + A \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = 0,$$

in which the matrix A is an $n \times n$ matrix

$$A = \begin{pmatrix} & \vdots & \\ \dots & a_{ij} & \dots \\ & \vdots & \end{pmatrix},$$

of rational functions of T, say with complex coefficients. Denote by S the finite subset of $\mathbb{C}$ constisting of the points $s \in \mathbb{C}$ at which any of the functions a_{ij} has a pole, and denote by $g(T) \in \mathbb{C}[T]$ the polynomial

$$g(T) = \textstyle\prod_{s \in S}(T - s).$$

Then each of the coefficient functions a_{ij} lies in the ring $\mathbb{C}[T][1/g(T)]$ of all rational functions holomorphic on the open Riemann surface $\mathbb{C} - S$.

For each point $t \in \mathbb{C} - S$, we denote by $\mathrm{Soln}(t)$ the space of germs at t of solutions of the differential equation; this is a $\mathbb{C}$-vector space of dimension n. Analytic continuation of solutions yields for each $t \in \mathbb{C} - S$ an n-dimensional complex representation of the fundamental group $\pi_1(\mathbb{C} - S;\ t)$ on the space $\mathrm{Soln}(t)$, the "monodromy representation". For variable $t \in \mathbb{C} - S$, these representations are all conjugate to each other. (Equivalently, the spaces $\mathrm{Soln}(t)$, $t \in \mathbb{C} - S$, form a local system on $\mathbb{C} - S$ of n-dimensional complex vector spaces.) The *image* of "the" monodromy representation is called "the" monodromy group of the equation; up to conjugation, it is a well-defined subgroup of $GL(n.\ \mathbb{C})$.

Question. — Can one "calculate" the monodromy group of the equation "algebraically" in terms of the matrix (a_{ij}) ? Can one give "algebraic" criteria that the monodromy group be finite?

Let us define the "algebraic monodromy group" G_{mono} of the equation to be the Zariski closure, in $GL(n, \mathbb{C})$, of the monodromy group. Thus G_{mono} is the smallest algebraic subgroup of $GL(n, \mathbb{C})$ which contains the monodromy group. Then we get an apparently more algebraic version of the first question by replacing "monodromy group" by "algebraic monodromy group" throughout. (Notice, however, that the monodromy group will be finite if and only if its Zariski closure is finite, so that this aspect of the question remains unchanged.)

Because G_{mono} is by definition an algebraic subgroup of $GL(n, \mathbb{C})$, we may speak of its Lie algebra Lie (G_{mono}), which is an algebraic Lie sub-algebra of $M(n, \mathbb{C})$. We may ask for an "algebraic" description of Lie (G_{mono}), and for "algebraic" criteria that it vanish. (Notice that $\text{Lie}(G_{\text{mono}})=0$ if and only if G_{mono} is finite if and only if the monodromy group is finite, so again this aspect of the question remains unchanged.)

There is yet another algebraic group attached to our differential equation, the "differential galois group" G_{gal}. (In the case when our $n \times n$ system is the system version of a single n'th order equation, this group G_{gal} is precisely the differential galois group of the n-th order equation, whence the terminology.) The definition of G_{gal} is purely algebraic, but none the less, one does not "really" know how to calculate either G_{gal} or its Lie algebra Lie G_{gal}).

The relation of G_{gal} to G_{mono} is this. One always has an inclusion

$$G_{\text{mono}} \subset G_{\text{gal}} = GL(n, \mathbb{C}),$$

and one has equality

$$G_{\text{mono}} = G_{\text{gal}},$$

whenever the differential equation involved has regular singular points (but not conversely; one can have $G_{\text{mono}} = GL(n, \mathbb{C})$ but irregular singularities).

In this paper, we will put forth a conjectural description of the Lie algebra of G_{gal} (or more precisely of a certain "form" $G_{\text{gal}/\mathbb{C}(T)}$ of G_{gal} defined not over $\mathbb{C}$ but over the field $\mathbb{C}(T)$ of rational functions on $\mathbb{C}-S$)in terms of certain invariants, the "p-curvatures", of the "reductions mod p" of our differential equation, which are the obstructions to the reduction mod p's having a full set of solutions.

Let us recall briefly the notion of "reduction mod p" we have in mind. The n^2 rational functions a_{ij} all lie in the ring $\mathbb{C}[T][1/g(T)]$, so each a_{ij} may be written

$$a_{ij}(T)=\frac{P_{i,j}(T)}{g(T)^{n_{ij}}},$$

where $P_{i,j}$ lies in $\mathbb{C}[T]$, and where $n_{i,j}\geqslant 0$ is an integer. Let R denote the subring of $\mathbb{C}$ generated over $\mathbb{Z}$ generated over $\mathbb{Z}$ by the finitely many coefficients of the polynomials $P_{i,j}(T)$ and of $g(T)$.

Then all the functions a_{ij} lie in $R[T][1/g(T)]$, and R is a subring of $\mathbb{C}$ which is finitely generated as a $\mathbb{Z}$-algebra. For any such ring R, the natural map

$$R \to \textstyle\prod_p R/pR,$$

is injective, so long as the product extends over any *infinite* set of prime numbers p. In principle, then, we lose no information if, instead of studying the operator

$$\frac{d}{dT}+A,$$

operating, say, on n-triples of elements of $R[T][1/g(T)]$, we simultaneously consider its reductions mod p, operating on n-triples of elements of $(R/pR)[T][1/g(T)]$, for all but some finite set of primes. The "p-curvature" ψ_p of this mod p operator is simply its p-th iterate

$$\psi_p=\left(\frac{d}{dT}+A\right)^p, \quad \text{taken mod } p,$$

which turns out (oh miracle!) to be a *linear* operator rather than a differential one. In absolutely down-to-earth terms, if we define a sequence $A(k)$, $k\geqslant 1$, of $n\times n$ matrices over $R[T][1(g(T)]$ by the inductive formulas

$$\begin{cases} A(1)=A, \\ A(k+1)=\dfrac{d}{dT}(A(k))+A.A(k), \end{cases}$$

then we have

$$\psi_p = A(p), \quad \text{taken mod } p.$$

Roughly speaking, our conjecture is that the algebra $\mathrm{Lie}(G_{\mathrm{gal}/\mathbb{C}(T)})$ is the smallest algebraic Lie sub-algebra of $M(n, \mathbb{C}(T))$ with the property that its "reduction mod p" contains ψ_p for all but finitely many p. As a special case, this conjecture contains a conjecture of Grothendieck's, according to which the *vanishing* of ψ_p for all but finitely many primes p should be equivalent to the existence of a full set of algebraic solutions for our original differential equation, a condition equivalent to the finiteness of G_{gal}, i.e. to the vanishing of $\mathrm{Lie}(G_{\mathrm{gal}})$.

It turns out that the two conjectures are equivalent (the universal truth of Grothendieck's conjecture would imply ours).

In the text we work on an arbitrary connected smooth complex algebraic variety, rather than on $\mathbb{C} - S$, but this generality should not disguise the fact that $\mathbb{C} - S$ is the crucial case; the universal truth of our conjecture on all $\mathbb{C} - S$ would imply its universal truth in the general case.

In an Appendix, we give a fundamental formula for p-curvature due to O. Gabber.

I. The algebraic picture (*cf.* [6] and [8], pp. 307-321)

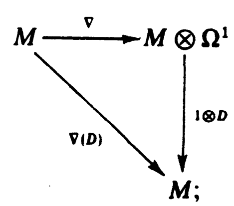
Let X be a smooth connected algebraic variety over $\mathbb{C}$. By an algebraic differential equation on $X/\mathbb{C}$, we mean a pair (M, ∇) consisting of a locally free coherent sheaf M on X, together with an integrable connection

$$\nabla : \quad M \to M \bigotimes_{\mathcal{O}_X} \Omega^1_{X/\mathbb{C}}.$$

This means that ∇ is a $\mathbb{C}$-linear mapping which satisfies the connection-rule

$$\nabla(fm) = f\,\nabla(m) + m \otimes df$$

(for f a local section of $\mathcal{O}_X$, and m a local section of M) and which is integrable in the following sense: for any local section D of $\underline{\mathrm{Det}}_{\mathbb{C}}(\mathcal{O}_X, \mathcal{O}_X)$, define the additive endomorphism $\nabla(D)$ of M as the composite



the requirement of integrability is that for any two local sections D_1, D_2 of $\underline{\text{Der}}$, we have

$$[\nabla(D_1), \nabla(D_2)] = \nabla([D_1, D_2]).$$

When X is one-dimensional, any connection is automatically integrable. [In the introduction, we consider $X = A^1 - S$, $M = (\mathcal{O}_X)^n$, and ∇ the map

$$\vec{f} \to \vec{df} + A\vec{f};$$

the operator $\nabla(d/dT)$ on M is the map

$$\vec{f} \to \frac{d}{dT}(\vec{f}) + A\vec{f}\,\Big].$$

Because $\mathbb{C}$ is a field of characteristic zero, and X is smooth over $\mathbb{C}$, any *coherent* sheaf on X with integrable connection is *automatically* locally free. It follows from this that, with the obvious notion of horizontal morphism ($\mathcal{O}_X$-linear maps compatible with ∇'s), the categorie $D.E.(X/\mathbb{C})$ of all algebraic differential equations on X is a $\mathbb{C}$-linear abelian category. Given two algebraic differential equations (M_1, ∇_1) and (M_2, ∇_2) on X, one can form their "internal hom" $(\underline{\text{Hom}}(M_1, M_2), \nabla_{1,2})$ and their tensor product $(M_1 \otimes_{\mathcal{O}_X} M_2, \nabla_1 \otimes 1 + 1 \otimes \nabla_2)$ in the expected way. Thus the category $D.E.(X/\mathbb{C})$ is a tanakian category in the sense of Saavedra. Given an algebraic differential equation (M, ∇), with M locally free of rank n, we may apply to (M, ∇) any "construction of linear algebra" obtained by finitely iterating the basic constructions $\otimes^i$, $\wedge^j$, Symm^k, $\oplus$. [Strictly speaking, such a "construction" is nothing other than a polynomial representation of the algebraic group $GL(n)$ over $\mathbb{Z}$ in a free $\mathbb{Z}$-module, but we will make do with the above more naive point of view.]

Let $U \subset X$ be a non-empty Zariski open set. There is a natural "restriction to U" functor

$$D.E.(X/\mathbb{C}) \to D.E.(U/\mathbb{C}),$$

which is exact, fully faithful, and compatible with all constructions of linear algebra. Moreover, given an (M, ∇) on X, every sub-equation (N', ∇') of $(M, \nabla)\,|\,U$ extends uniquely to a sub-equation (N, ∇) of (M, ∇). (Proof : if

$j : U \to X$ is the inclusion, then $(j * N') \cap M$ is a coherent subsheaf of M stable by ∇.)

Passing to the limit, we obtain an exact fully faithful functor compatible with the constructions of linear algebra

$$D.E.(S/\mathbb{C}) \to D.E.(\mathbb{C}(X)/\mathbb{C}),$$

with target the category of finite-dimensional vector-spaces over the function field $\mathbb{C}(X)$ of X endowed with integrable connections relative to $\mathbb{C}(X)/\mathbb{C}$. Given (M, ∇) in X, the underlying $\mathbb{C}(X)$-vector space of its image is simply the *generic fibre* $M \otimes_{\mathcal{O}_X} \mathbb{C}(X)$ of the underlying M. Just as above, any ∇-stable subspace of $M \otimes \mathbb{C}(X)$ is the generic fibre of a unique sub-equation of (M, ∇).

For any non-empty X-*scheme*

$$f: \quad Y \to X,$$

the "functor" inverse image by f" is an exact faithful functor

$$D.E.(X/\mathbb{C}) \to \text{Loc Free}(Y),$$

to the category of all locally free sheaves of finite rank on Y, which is compatible with all constructions of linear algebra. For example, if $f : Y \to X$ is the inclusion of a $\mathbb{C}$-valued point $y \in X$, the corresponding functor

$$D.E.(X/\mathbb{C}) \to \text{Fin. Dim. } \mathbb{C}\text{-vector spaces},$$

is just the functor "fibre of M at y"

$$(M, \nabla) \to M(y).$$

The faithfulness of this functor amounts to the fact, applied to the internal hom differential equation, that a global horizontal section of an (M, ∇) is uniquely determined by its *value* in any fibre $M(y)$ of M. Similarly, if $f: Y \to X$ is the inclusion of the *generic point* $\text{Spec}(\mathbb{C}(X))$ of X, then the corresponding functor

$$D.E.(X/\mathbb{C}) \to \text{Fin. Dim. } \mathbb{C}(X)\text{-vector spaces},$$

is just the functor "generic fibre of M"

$$(M, \nabla) \mapsto M \otimes \mathbb{C}(X).$$

II. The analytic picture

Let us denote by X^{an} the connected complex manifold underlying the algebraic variety X. In complete analogy with the algebraic case, we have the category $D.E.(X^{an})$, whose objects are the pairs (M, ∇) consisting of a locally free coherent sheaf M on X^{an} together with an integrable connection ∇, with morphisms the horizontal ones. Just as in the algebraic case, the category $D.E.(X^{an})$ is a $\mathbb{C}$-linear abelian category in which one can perform all the constructions of linear algebra.

Unlike the algebraic case, however, we have in principle a complete understanding of this category in terms of the fundamental group of X^{an}. In the analytic category, the functor "sheaf of germs of horizontal sections" defines an equivalence of categories

$$D.E.(X^{an}) \xrightarrow{\sim} \text{Loc. System}\ (X^{an}),$$

with the category of all local systems of finite-dimensional $\mathbb{C}$-vector speces on X^{an}. If we fix a base point $y \in X^{an}$, the functor "fibre at y" defines an equivalence of categories

$$\text{Loc. System}\,(X^{an}) \xrightarrow{\sim} \text{Rep}\,(\pi_1\,(X^{an}, y)),$$

with the category of finite-dimensional complex representations of the fundamental group $\pi_1\,(X^{an}, y)$. Both of these functors are compatible with the constructions of linear algebra.

There is a natural G.A.G.A. functor

$$D.E.(X/\mathbb{C}) \overset{\text{"an"}}{\rightarrow} D.E.(X^{an}),$$

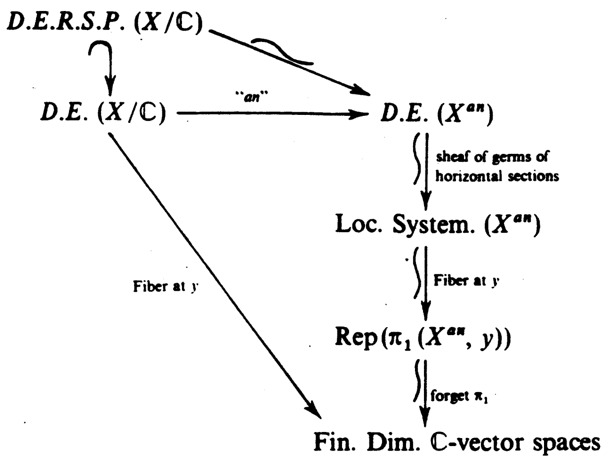
which is exact, faithful (but not in general fully faithful, unless X is complete) and compatible with the construction of linear algebra. Let us denote by

$$D.E.R.S.P.(X/\mathbb{C}) \subset D.E.(X/\mathbb{C}),$$

the full subcategory of $D.E.(X/\mathbb{C})$ consisting of those algebraic (M, ∇) on X which have regular singular points in the sense of Deligne. This subcategory is stable by sub-object and quotient, as well as by the constructions of linear algebra. DELIGNE [2] has shown that the composite functor

$$\begin{array}{ccc} D.E.R.S.P.\ (X/\mathbb{C}) & \searrow^{\sim} & \\ \downarrow & & \\ D.E.\ (X/\mathbb{C}) & \longrightarrow & D.E.\ (X^{an}), \end{array}$$

in an equivalence of categories. All in all, we may summarize the situation by the following diagram, in which all functors occuring are exact, faithful, and compatible with the constructions of linear algebra:



III. Interlude: Review of algebraic groups

Let k a field, and V a finite-dimensional k-vector space. Given any construction of linear algebra, we denote by Constr(V) the finite-dimensional k-vector space obtained by applying the construction to V. By functoriality, the algebraic group $GL(V)$ operates on Constr(V), as does its Lie algebra End(V). [For example, $g \in GK(V)$ acts on $v_1 \otimes v_2 \in V^{\otimes 2}$ by $v_1 \otimes v_2 \to g(v_1) \otimes g(v_2)$, while $\gamma \in \mathrm{End}(V)$ acts by $v_1 \otimes v_2 \to \gamma(v_1) \otimes v_2 + v_1 \otimes \gamma(v_2)$].

Given a family Constr$_i$ of constructions of linear algebra, and a collection of subspaces of the Constr$_i(V)$

$$\{W_{i,j} \subset \mathrm{Constr}_i(V)\}_j,$$

we may attach the following algebraic subgroup G of $GL(V)$:

$$G = \{g \in GL(V) \mid \forall_{i,j},\ g(W_{i,j}) \subset W_{i,j}\}.$$

The Lie algebra Lie(G) of this G is the algebraic Lie sub-algebra of End(V) defined by

$$\mathrm{Lie}(G) = \{\gamma \in \mathrm{End}(V) \mid \forall_{i,j},\ \gamma(W_{i,j}) \subset W_{i,j}\}.$$

The key to understanding algebraic subgroups of $GL(V)$ is provided by the following fundamental theorem of CHEVALLEY [1].

THEOREM. — *Every algebraic subgroup of* $GL(V)$ *(respectively, every algebraic Lie sub-algebra of* $\mathrm{End}(V)$*) may be defined by the above procedure. In fact, it can be defined as the stabilizer of a* single *line in a single* construction.

One striking consequencee of the theorem is that an algebraic subgroup G of $GL(V)$ (resp. an algebraic Lie sub-algebra Lie (G) of End (V)) is determined by the list of *all* G-Stable subspace in *all* possible Constr(V)'s: namely G (resp. Lie (G)) is precisely the stabilizer of all these subspaces.

Another consequence is this. Given an "abstract" subgroup H of $GL(V)$, its Zariski closure in $GL(V)$ is the algebraic subgroup defined as the stabilizer of all H-stable subspaces in all Constr(V)'s.

IV. The differential Galois group G_{gal} (compare [5], [8])

Let us fix an algebraic differential equation (M, ∇) on X, i.e., (M, ∇) is an object of $D.E.(X/\mathbb{C})$. For any construction of linear algebra, we may form the corresponding object Constr(M, ∇) of $D.E.(X/\mathbb{C})$. In each such construction, we next list all of its algebraic sub-equations, i.e. all of its sub-objects in the category $D.E.(X/\mathbb{C})$. In this way we obtain the (rather long) list

$$(W_{ij}, \nabla) \subset \mathrm{Constr}_i(M, \nabla),$$

of *all* algebraic sub-equations of *all* constructions.

Now let $y \in X(\mathbb{C})$ be any closed point of X. We will apply the preceding discussion of algebraic groups to the vector space $V = M(y)$ over the field $k = \mathbb{C}$. The list of subspaces of all the Constr$_i(M(y))$'s,

$$W_{ij}(y) \subset \mathrm{Constr}_i(M(y)) = (\mathrm{Constr}_i(\mathrm{M}))(y),$$

provided by the fibres at y of all algebraic sub-equations of the Constr$_i(M, \nabla)$'s defines an algebraic group over $\mathbb{C}$,

$$G_{gal}(M, \nabla; y) \subset GL(M(y)),$$

the "differential galois group" of (M, ∇), with base point y.

Instead of a closed point $y \in X(\mathbb{C})$, we could carry out the same construction with the generic point of X, i.e., we consider the vector space

$V=M\otimes\mathbb{C}(X)$ over the field $k=\mathbb{C}(X)$, and the list of subspaces of all constructions.

$$W_{ij}\otimes\mathbb{C}(X)\subset\mathrm{Constr}_i(M\otimes\mathbb{C}(X)),$$

provided by the generic fibres of all algebraic sub-equations of all the $\mathrm{Constr}_i(M,\nabla)$'s. The associated algebraic group over the function field $\mathbb{C}(X)$,

$$G_{\mathrm{gal}}(M,\nabla;\mathbb{C}(X))\subset GL(M\otimes\mathbb{C}(X)),$$

is the differential galois group of (M,∇), with base point the generic point of X.

What is the relation among the G_{gal}'s of a fixed (M,∇) based at different points ? It follows from the general theory of Tanakien categories that the groups attached to any two "fibre functors" are "inner forms" of each other. However, in the concrete situation at hand, we can see this explicitly.

PROPOSITION 4.1. — *Let $y\in X(\mathbb{C})$ be a closed point of X, $\hat{\mathcal{O}}_{X,y}$ the complete local ring of X at y, and K the fraction field of $\hat{\mathcal{O}}_{X,y}$. Then we have a canonical isomorphism, for any (M,∇) in D.E.$(X/\mathbb{C})$*

$$M(y)\otimes K\xrightarrow{\sim}(M\otimes_{\mathcal{O}_X}\mathbb{C}(X))\otimes_{\mathbb{C}(X)}K,$$

which is compatible with all constructions of linear algebra, and which induces a canonical isomorphism of algebraic groups over K

$$G_{\mathrm{gal}}(M,\nabla;y)\otimes K\simeq G_{\mathrm{gal}}(M,\nabla;\mathbb{C}(X))\otimes_{\mathbb{C}(X)}K.$$

Proof. — Let us denote by $(M\otimes_{\mathcal{O}_X}\hat{\mathcal{O}}_{X,y})^{\nabla}$ the space of formal horizontal sections at y. By the formal version of the Frobenius integrability theorem, this is an $n=\mathrm{rank}(M)$-dimensional $\mathbb{C}$-vector space, which by reduction modulo Max_y is isomorphic to the fibre $M(y)$ of M at y:

$$(M\otimes\hat{\mathcal{O}}_{X,y})^{\nabla}\xrightarrow{\sim}M(y).$$

Moreover, the natural map

$$(M\otimes_{\mathcal{O}_X}\hat{\mathcal{O}}_{X,y})^{\nabla}\otimes_{\mathbb{C}}\hat{\mathcal{O}}_{X,y}\to M\otimes_{\mathcal{O}_X}\hat{\mathcal{O}}_{X,y},$$

is an isomorphism of $\hat{\mathcal{O}}_{X,y}$-modules. Combining these two isomorphisms, we find a canonical isomorphism of $\hat{\mathcal{O}}_{X,y}$-modules

$$M(y)\otimes_{\mathbb{C}}\hat{\mathcal{O}}_{X,y}\simeq M\otimes_{\mathcal{O}_X}\hat{\mathcal{O}}_{X,y}.$$

Extending scalars from $\hat{\mathcal{O}}_{X,y}$ to its fraction field K yields the required isomorphism

$$M(y)\otimes_{\mathbb{C}} K \simeq (M \otimes_{\mathcal{O}_X} \mathbb{C}(X)) \otimes_{\mathbb{C}(X)} K,$$

which, in view of its construction, is visibly compatible with the constructions of linear algebra. In particular, for any construction of linear algebra, and for any algebraic sub-equation

$$(W, \nabla) \subset \mathrm{Constr}(M, \nabla),$$

these isomorphisms give a canonical identification

$$W(y)\otimes_{\mathbb{C}} K = (W \otimes_{\mathcal{O}_X} \mathbb{C}(X)) \otimes_{\mathbb{C}(X)} K,$$

inside

$$\mathrm{Constr}(M(y))\otimes_{\mathbb{C}} K \simeq (M \otimes \mathbb{C}(X)) \otimes_{\mathbb{C}(X)} K.$$

These canonical identifications (of the subspaces to be stabilized) give a canonical isomorphism of algebraic groups over K

$$G_{\mathrm{gal}}(M, \nabla; y)\otimes_{\mathbb{C}} K \simeq G_{\mathrm{gal}}(M, \nabla; \mathbb{C}(X)) \otimes_{\mathbb{C}(X)} K.$$

Q.E.D.

PROPOSITION 4.2. — *The group $G_{\mathrm{gal}}(M, \nabla; \mathbb{C}(X))$ is a* birational *invariant of (M, ∇), in the sense that it depends only on the restriction of (M, ∇) to the function field $\mathbb{C}(X)$.*

Proof. — This group is defined by the list of *all* ∇-stable $\mathbb{C}(X)$-subspaces of all $\mathrm{Constr}(M \otimes \mathbb{C}(X)$'s, for these are precisely the generic fibres of the algebraic sub-equations, defined on all of X, of the $\mathrm{Constr}(M, \nabla)$'s.

Q.E.D.

PROPOSITION 4.3. — *Given a finite etale covering of X by a smooth connected complex variety Y,*

$$\begin{array}{c} Y \\ {\scriptstyle f}\downarrow, \\ X \end{array}$$

we have a natural injective homomorphism of differential galois groups:

$$G_{\mathrm{gal}}(f^*(M, \nabla), \mathbb{C}(Y)) \to G_{\mathrm{gal}}(M, \nabla, \mathbb{C}(X)) \otimes_{\mathbb{C}(X)} \mathbb{C}(Y),$$

which induces an isomorphism between their Lie algebras:

$$\operatorname{Lie}(G_{\mathrm{gal}}(f^*(M, \nabla), \mathbb{C}(Y)) \simeq \operatorname{Lie}(G_{\mathrm{gal}}(M, \nabla, \mathbb{C}(X))) \otimes_{\mathbb{C}(X)} \mathbb{C}(Y).$$

Proof. – We have an injective homomorphism simply because the list of ∇-stable $\mathbb{C}(Y)$-subspaces of $\operatorname{Constr}((M \otimes_{\mathcal{O}_X} \mathbb{C}(Y)))$'s includes those obtained, by extending scalars from $\mathbb{C}(X)$ to $\mathbb{C}(Y)$, from the ∇-stable $\mathbb{C}(X)$-subspaces of $\operatorname{Constr}(M \otimes_{\mathcal{O}_X} \mathbb{C}(X))$'s. To see that this injective homomorphism is bijective on Lie algebras, we must show that $\gamma \in \operatorname{End}(M \otimes \mathbb{C}(X))$ which stabilizes all ∇-stable $\mathbb{C}(X)$-subspaces of $\operatorname{Constr}(M \otimes \mathbb{C}(X))$'s necessarily stabilizes all ∇-stable $\mathbb{C}(Y)$ subspaces of the $\operatorname{Constr}(M \otimes \mathbb{C}(Y)) \simeq (\operatorname{Constr}(M \otimes \mathbb{C}(X))) \otimes_{\mathbb{C}(X)} \mathbb{C}(Y)$. Thus let W be a ∇-stable $\mathbb{C}(Y)$-subspace of some $\operatorname{Constr}(M \otimes \mathbb{C}(Y))$. To show that γ stabilizes W, it suffices to show that γ stabilizes the $\mathbb{C}(Y)$-line $\wedge^{\dim W}(W)$ in $\wedge^{\dim W}(\operatorname{Constr}(M \otimes \mathbb{C}(Y))$. Thus we may assume that W is itself a ∇-stable line L in some $\operatorname{Constr}(M \otimes \mathbb{C}(Y))$. Replacing (M, ∇) by $\operatorname{Constr}(M, \nabla)$, we see that it suffices to treat (universally) the case of a ∇-stable line L in $M \otimes C(Y)$. Replacing Y by a finite etale covering of itself, we see that it suffices to prove the theorem under the additional hypothesis that Y is a finite etale galois covering of X, say with galois group Σ:

$$\begin{array}{c} Y \\ f \downarrow \Sigma \\ X \end{array}$$

For each $\sigma \in \Sigma = \operatorname{Gal}(Y/X)$, the conjugate line $\sigma(L)$ is another ∇-stable line in $M \otimes \mathbb{C}(Y)$. Among all the conjugates $\sigma(L)$, $\sigma \in \Sigma$, let $L_1, \ldots, L_r$ be the *distinct* lines which occur. We must show that γ stabilizes each L_i. For every integer $n \geqslant 1$, the subspaces:

$$\textstyle\sum_i L_i^{\otimes n} \subset \operatorname{Symm}^n(M \otimes \mathbb{C}(Y)),$$
$$\textstyle\sum L_i^{\otimes 2n} \subset \operatorname{Symm}^2(\operatorname{Symm}^n(M \otimes \mathbb{C}(Y)),$$

will be γ-stable, because they are ∇-stable and are "defined over $\mathbb{C}(X)$" (because Σ-stable).

Let $l_i \in L_i$ be a non-zero vector. Suppose we knew that for some $n \geqslant 1$, the vectors $l_i^{\otimes n}$ are linearly independent in Symm^n. Then the vectors $\{l_i^{\otimes n} l_j^{\otimes n}\}$,

$i \leqslant j$, are of course linearly independent in $\mathrm{Symm}^2(\mathrm{Symm}^n)$. By the γ-stability of $\Sigma L_i^{\otimes n}$, we can write:

$$\gamma(l_i^{\otimes n})=\sum_j A_{i,j} l_j^{\otimes n},$$

whence:

$$\gamma(l_i^{\otimes 2n})=2\, l_i^{\otimes n}\gamma(l_i^{\otimes n})=2\sum_j A_{i,j} l_i^{\otimes} l_j^{\otimes n}.$$

As the products $l_i^{\otimes n} l_j^{\otimes n}$ are linearly independent in $\mathrm{Symm}^2(\mathrm{Symm}^n)$, this last equation is incompatible with the γ-stability of $\Sigma L_i^{\otimes 2n}$ unless we have $A_{ij}=0$ for $i \neq j$. Then we obtain:

$$\gamma(l_i^{\otimes n})=A_{i,i} l_i^{\otimes n}, \quad \text{in } \mathrm{Symm}^n.$$

On the other hand we have:

$$\gamma(l_i^{\otimes n})=n l_i^{\otimes(n-1)}\gamma(l_i), \quad \text{in } \mathrm{Symm}^n;$$

because the symmetric algebra Symm is an integral domain over a field $\mathbb{C}(Y)$ of characteristic zero, and $l_i \neq 0$, we may divide by $n l_i^{\otimes(n-1)}$ to infer that:

$$\gamma(l_i)=\frac{A_{i,i}}{n}\, l_i.$$

To conclude the proof, we need the following lemma.

LEMMA 4.4. — *Let k be a field of characteristic zero, V a finite dimensional vector space over k, and $v_1, \ldots, v_r$ a set of non-zero vectors in V which span* distinct *lines. Then for any integer $n \geqslant r-1$, the vector $v_1^{\otimes n}, \ldots, v_r^{\otimes n}$ are linearly independent in* $\mathrm{Symm}^n(V)$.

Proof. — Extending scalars if necessary we may suppose that k is algebraically closed. If $\dim(V)=1$, then $r=1$ and there is nothing to prove. Suppose $\dim(V) \geqslant 2$. We first reduce to the case $\dim V=2$. Given any finite set of non-zero vectors in V, we can find a hyperplane in V which contains none of them. Let λ be a linear form on V whose kernel is such a hyperplane, so that $\lambda(v_i) \neq 0$ for $i=1, \ldots, r$. Multiplying the v_i's by non-zero scalars, we may assume that:

$$\lambda(v_i)=1 \qquad \text{for} \quad i=1, \ldots, r.$$

Because the v_i span distinct lines, the differences v_i-v_j, $i<j$, are all non-zero. So we may find a linear form μ on V such that:

$$\mu(v_i-v_j) \neq 0 \qquad \text{if} \quad i<j.$$

The pair (λ, μ) defines a map of V onto a 2-dimensional quotient space k^2, under which the images of $v_1, \ldots, v_r$ are r vectors of the form:

$$(1, A_i)=(\lambda(v_i), \mu(v_i)),$$

in which the r scalars $A_1, \ldots, A_r$ are distinct. Because $\mathrm{Symm}^n(k^2)$ will be a quotient of $\mathrm{Symm}^n(V)$, it suffices to prove our theorem for $V=k^2$, and r vectors $v_i=(1, A_i)$, $1\leqslant i\leqslant r$, with distinct A_i's. In this case the vectors $v_i^{\otimes n}$ in $\mathrm{Symm}^n(k^2)$ have coordinates relative to the standard basis given by:

$$v_i^{\otimes n}\sim\left(1, nA_i, \binom{n}{2}A_i^2, \ldots, \binom{n}{j}A_i^j, \ldots, A_i^n\right).$$

That these vectors are linear independent, for $n\geqslant r-1$, results from the non-vanishing of the van der Monde determinant on $A_1, \ldots, A_r$.

Q.E.D.

The following proposition will be proven further on. We state it here for the sake of continuity of exposition.

PROPOSITION 4.5. — *The following conditions are equivalent:*

(1) (M, ∇) *becomes trivial on a finite etale covering Y of X;*

(2) *the group G_{gal} attached to (M, ∇) is finite;*

(3) *the Lie algebra* $\mathrm{Lie}(G_{\mathrm{gal}})$ *vanishes.*

There is a last functoriality concerning the G_{gal} which is worth pointing out explicitly. If we begin with an (M, ∇) on X and perform a "construction of linear algebra" that very construction defines a homomorphism of algebraic groups (with $\star=$any chosen base point):

$$G_{\mathrm{gal}}(M, \nabla, \star)\rightarrow G_{\mathrm{gal}}(\mathrm{Constr}(M, \nabla), \star).$$

Similarly, if (W, ∇) is an algebraic sub-equation of a $\mathrm{Constr}(M, \nabla)$, we have a natural "restriction to (W, ∇)" homomorphism of algebraic groups:

$$G_{\mathrm{gal}}(\mathrm{Constr}(M, \nabla), \star)\rightarrow G_{\mathrm{gal}}(W, \nabla, \star).$$

Their composition is the homomorphism

$$G_{\mathrm{gal}}(M, \nabla, \star)\rightarrow G_{\mathrm{gal}}(W, \nabla, \star)\subset GL(W(\star)),$$

by which $G_{\mathrm{gal}}(M, \nabla, \star)$ acts on the subspace $W(\star)\subset\mathrm{Constr}(M(\star))$.

V. The algebraic monodromy group G_{mono}

We continue to work with a fixed algebraic differential equation (M, ∇) on X. We denote by $(M, \nabla)^{an}$ the corresponding analytic differential equation on X^{an}. For each construction of linear algebra, we form the corresponding object $\text{Constr}(M, \nabla)^{an}) \simeq (\text{Constr}(M, \nabla))^{an}$ in the analytic category $D.E.(X^{an})$. In each such construction, we list all of its *analytic* sub-equations, i.e., all of its sub-objects in the category $D.E.(X^{an})$. In this way, we obtain the list:

$$(V_{ij}, \nabla) \subset \text{Constr}(M, \nabla)^{an}.$$

of all *analytic* sub-equations of all constructions.

For any point $y \in X^{an} = X(\mathbb{C})$, we apply the discussion of algebraic groups to the vector space $V = M(y)$ over the field $k = \mathbb{C}$, and the list of sub-spaces of all $\text{Constr}(M(y))$'s provided by the fibres at y of all *analytic* sub-equations of the $\text{Constr}(M, \nabla)^{an}$'s. The corresponding algebraic group

$$G_{\text{mono}}(M, \nabla, y) \subset GL(M(y)),$$

is called the algebraic monodromy group of (M, ∇), based at y.

PROPOSITION 5.1. — *Let $\rho: \pi_1(X^{an}, y) \to GL(M(y))$ be the monodromy representation attached to the analytic differential equation $(M, \nabla)^{an}$ on X^{an}. The algebraic group*

$$G_{\text{mono}}(M, \nabla, y) \subset GL(M(y)),$$

is the Zariski closure in $GL(M(y))$ of the image $\rho(\pi_1(X^{an}, y))$ in $GL(M(y))$ of $\pi_1(X^{an}, y)$, i.e. $G_{\text{mono}}(M, \nabla, y)$ is the Zariski closure of the monodromy group of $(M, \nabla)^{an}$.

Proof. — Under the equivalence of categories

$$D.E.(X^{an}) \simeq \text{Rep}(\pi_1(X^{an}, y)),$$

induced by the functor "fibre at y", the list of all analytic sub-equations of all $\text{Constr}(M, \nabla)^{an}$'s becomes the list of all $\pi_1(X^{an}, y)$-stable subspaces of all $\text{Constr}(M(y))$'s where $\pi_1(X^{an}, y)$ acts on $M(y)$ by the monodromy representations of $(M, \nabla)^{an}$. As we have already noted, the algebraic group defined by this list is none other that the Zariski closure in $GL(M(y))$ of the "abstract" subgroup $\rho(\pi_1(X^{an}, y))$.

Q.E.D.

PROPOSITION 5.2. — *For any* (M, ∇) *on* X, *and any point* $y \in X(\mathbb{C})$, *we have an inclusion of algebraic groups (both inside* $GL(M(y))$)

$$G_{\text{mono}}(M, \nabla, y) \subset G_{\text{gal}}(M, \nabla, y).$$

If (M, ∇) *has regular singular points, then we have an equality*

$$G_{\text{mono}}(M, \nabla, y) = G_{\text{gal}}(M, \nabla, y).$$

Proof. — We have an inclusion because the list of *analytic* subequations of $\text{Constr}(M, \nabla)^{an}$'s includes the list of "analytifications" of all algebraic subequations of $\text{Constr}(M, \nabla)$'s. If (M, ∇) has regular singular points, it follows from Deligne's equivalence of categories

$$D.E.R.S.P.(X/\mathbb{C}) \overset{\sim}{\to} D.E.(X^{an}),$$

that these two lists actually coincide.

Q.E.D.

Caution. — It may very well happen that we have the equality $G_{\text{mono}} = G_{\text{gal}}$ for an (M, ∇) which does not have regular singular points, e.g., this will happen for any (M, ∇), regular or not, whose monodromy group is Zariski dense in GL.

PROPOSITION 5.3. — *Suppose that* (M, ∇) *on* X *has regular singular points. Then the following conditions are equivalent:*

(1) (M, ∇) *becomes trivial on a finite etale covering of* X;

(2) *the algebraic monodromy group* G_{mono} *attached to* (M, ∇) *is finite;*

(2 bis) *the differential galois group* G_{gal} *is finite;*

(3) *the Lie algebra* $\text{Lie}(G_{\text{mono}})$ *vanishes;*

(3 bis) *the Lie algebra Lie* (G_{gal}) *vanishes.*

Proof. — The equivalences (2) (3), (2 *bis*)$\Leftrightarrow$(3 *bis*) are obvious. The equivalence (2)$\Leftrightarrow$(2 *bis*) is clear from the equality $G_{\text{mono}} = G_{\text{gal}}$. Clearly (1)$\Leftrightarrow$(2), while (2) implies that $(M, \nabla)^{an}$ becomes trivial on a finite etale covering Y^{an} of X^{an}. Such a covering is the analyticification of a unique finite etale covering $Y \xrightarrow{f} X$, on which $f^*(M, \nabla)^{an}$ has trivial monodromy. As $f^*(M, \nabla)$ has regular singular points on Y, it follows from Deligne's equivalence on Y

$$D.E.R.S.P.(Y(\mathbb{C})) \overset{\sim}{\to} D.E.(Y^{an}),$$

that $f^*(M, \nabla)$ on Y is trivial.

Q.E.D.

The unproven Proposition 4.5, stated at the end of the previous section, is an immediate consequence of this Proposition 5.3 taken together with the following one, whose proof will be given further on!

PROPOSITION 5.4. — *Let* (M, ∇) *be an algebraic differential equation on* X. *If the Lie algebra* $Lie(G_{gal})$ *vanishes, then* (M, ∇) *has regular singular points.*

VI. Spreading out

Let X be a connected smooth $\mathbb{C}$-scheme of finite type. It is standard that we can find a sub-ring $R \subset \mathbb{C}$ which is finitely generated as a $\mathbb{Z}$-algebra, and a connected smooth R-scheme $\mathbb{X}/R$ of finite type, with geometrically connected fibres, from which we recover $X/\mathbb{C}$ by making the extension of scalars $R \hookrightarrow \mathbb{C}$.

If in addition we are given an algebraic differential equation (M, ∇) on $X/\mathbb{C}$, we can choose $\mathbb{X}/R$ in such a way that there exists on $\mathbb{X}/R$ a locally free coherent sheaf $\mathbb{M}$, together with an integrable (relative to $\mathbb{X}/R$) connection ∇ on $\mathbb{M}$, such that we recover (M, ∇) on $\mathbb{X}/\mathbb{R}$ from $(\mathbb{M}, \nabla)$ on $\mathbb{X}/R$ by making the extension of scalars $R \hookrightarrow \mathbb{C}$.

Of course the choice of such an R, and of such data $\mathbb{X}/R, (\mathbb{M}, \nabla)$ on $\mathbb{X}/R$, is highly non-unique. One can say only that given any two such data

$$R_i, \mathbb{X}_i/R_i, (\mathbb{M}_i, \nabla_i) \quad \text{on } \mathbb{X}_i/R_i,$$

for $i=1, 2$, there exists a third

$$R_3, \mathbb{X}_3/R_3, (\mathbb{M}_3, \nabla_3) \quad \text{on } \mathbb{X}_3/R_3,$$

such that

$$R_1 \subset R_3, \qquad R_2 \subset R_3,$$

and there exist isomorphisms, for $i=1, 2$:

$$(\mathbb{X}_i, (\mathbb{M}_i, \nabla_i)) \otimes_{R_i} R_3 \simeq (X_3, (\mathbb{M}_3, \nabla_3)).$$

The following lemma, applied to both the rings R_i and the coordinate rings of affine open sets of the $\mathbb{X}_i$, provided the technical justification of our non-concern with this plethora of choice.

LEMMA 6.1. — *Let* R_1 *and* R_2 *be two integral domains with fraction fields of characteristic zero, which are both finitely generated as* $\mathbb{Z}$*-algebras. Suppose* *that $R_1 \subset R_2$. Then for all but finitely many primes p, the induced map between their reductions mod p is injective:*

$$R_1/pR_1 \hookrightarrow R_2/pR_2 \quad \textit{for almost all } p.$$

Proof. — We may first reduce to the case when R_2 is flat over R_1 (Because for some $f \neq 0$ in R_2, $R_2[1/f]$ will be flat over R_1, and if the theorem is true for $R_1 \subset R_2[1/f]$, it is certainly true for $R_1 \subset R_2$ with at worst the same set of exceptional primes). If R_2 is flat over R_1, then by Chevalley's "constructible image" theorem, there exists an element $g \neq 0$ in R_1 such that $R_2[1/g]$ is faithfully flat over $R_1[1/g]$. Therefore $R_1[1/g] \rightarrow R_2[1/g]$ is universally injective, in particular injective mod p for all p. Therefore we are reduced to treating the case $R_1 \subset R_1[1/g]$. Now the map of reductions mod p

$$R_1 \otimes \mathbb{F}_p \rightarrow (R_1[1/g]) \otimes \mathbb{F}_p = (R_1 \otimes \mathbb{F}_p)[1/g] = \varinjlim_{\times g} R_1 \otimes \mathbb{F}_p,$$

is injective if (and only if) the endomorphism "multiplication by g" is injective on $R_1 \otimes \mathbb{F}_p$.

Consider the short exact sequence

$$0 \rightarrow R_1 \xrightarrow{\times g} R_1 \rightarrow R_1/gR_1 \rightarrow 0.$$

The quotient R_1/gR_1 is a finitely generated $\mathbb{Z}$-algebra, and therefore if we invert some integer $N \geq 1$ the algebra $(R_1/gR_1)[1/N]$ will be flat over $\mathbb{Z}[1/N]$. For such an N, we have a short exact sequence

$$0 \rightarrow R_1[1/N] \xrightarrow{\times g} R_1[1/N] \rightarrow (R_1/gR_1)[1/N] \rightarrow 0,$$

whose last term is $\mathbb{Z}[1/N]$-flat. Therefore our sequence remains exact if we tensor over $\mathbb{Z}[1/N]$ with *any* $\mathbb{Z}[1/N]$-module, in particular with $\mathbb{F}_p$ for p a prime not dividing N. Thus for p not dividing N, we have an exact sense:

$$0 \rightarrow R_1 \otimes \mathbb{F}_p \xrightarrow{\times g} R_1 \otimes \mathbb{F}_p \rightarrow (R_1/gR_1) \otimes \mathbb{F}_p \rightarrow 0,$$

and in particular the required injectivity of "multiplication by g" on $R_1 \otimes \mathbb{F}_p$.

Q.E.D.

The point of spreading out an (M, ∇) on $X/\mathbb{C}$ to an $(\mathbb{M}, \nabla)$ on $\mathbb{X}/R$ is that the spread-out object is susceptible to reduction mod p, i. e. we can form, for each p, the locally free coherent sheaf with integrable connection $(\mathbb{M}, \nabla)\otimes_R(R\otimes_{\mathbb{Z}}\mathbb{F}_p)$ on the smooth $R\otimes\mathbb{F}_p$-scheme $\mathbb{X}\otimes_R(R\otimes\mathbb{F}_p)$. It then makes sense to ask what can be inferred about the original (M, ∇) on $X/\mathbb{C}$ from mod p knowledge about sufficient many reductions mod p of such a "spreading-out".

VII. The p-curvature (*cf.* [6])

In this section, we consider an $\mathbb{F}_p$-algebra R, a smooth R-scheme X, and a pair (M, ∇) consisting of a locally free coherent sheaf M on X together with an integrable connection

$$\nabla:\quad M \to M\otimes\Omega^1_{X/R}.$$

The associated construction $D \to \nabla(D)$, viewed as an $\mathcal{O}_X$-linear map

$$\underline{\mathrm{Der}}_R(\mathcal{O}_X, \mathcal{O}_X) \to \underline{\mathrm{End}}_R(M),$$

need not be compatible with the operation "p-power" (remember that by the Liebnitz rule, the p-power of a derivation in characteristic p is again a derivation), i.e., it need not be the case that $\nabla(D^p)=(\nabla(D))^p$. The p-curvature $\psi_p(D)$ is the obvious measure of this failure:

$$\psi_p(D) \overset{\mathrm{dfn}}{=} (\nabla(D))^p - \nabla(D^p).$$

One verifies easily that $\psi_p(D)$ is an $\mathcal{O}_X$-linear endomorphism of M, and somewhat less easily that the assignment. $D \to \psi_p(D)$ is p-linear, i. e. we have:

$$\psi_p(f_1 D_1 + f_2 D_2) = f_1^p \psi_p(D_1) + f_2^p \psi_p(D_2).$$

for f_1, f_2 local sections of $\mathcal{O}_X$, and D_1, D_2 local sections of $\underline{\mathrm{Der}}_R(\mathcal{O}_X, \mathcal{O}_X)$. It follows easily from this that the various $\psi_p(D)$'s mutually commute, and that each of them is a horizontal endomorphism of M. Under the constructions of linear algebra, $\psi_p(D)$ behaves in a "Lie-like" manner, e.g. if we take a tensor product

$$(M_1\otimes M_2,\ \nabla_1\otimes 1 + 1\otimes\nabla_2),$$

its p-curvature is given by the formula:

$$\psi_{p;\, M_1\otimes M_2}(D)=\psi_{p;\, M_1}(D)\otimes 1+1\otimes\psi_{p,\, M_2}(D).$$

Because ψ_p is a differential invariant, it is compatible with etale localization. To be precise, let $f: Y\rightarrow X$ be an etale morphism, D a derivation on X, $f^*(D)$ the pulled-back derivation on Y. For any (M, ∇) on X/R, the p-curvature of $f^*(M, \nabla)$ on Y/R is given by:

$$\psi_{p, f^*(M, \nabla)}(f^* D)=f^*(\psi_{p, (M, \nabla)}(D)) \quad \text{in } \operatorname{End}_{\mathcal{O}_Y}(f^*(M)).$$

The importance of p-curvature is that it is the obstruction to the Zariski-local existence of enough horizontal sections, a fundamental fact discovered by Cartier.

THEOREM 7.1 (Cartier). — *Hypotheses as above, let $M^\nabla\subset M$ denote the kernel of ∇: $M\rightarrow M\otimes\Omega^1$, i.e. M^∇ is the sheaf of germs of horizontal sections of M. Then M is spanned over $\mathcal{O}_X$ by M^∇ if and only if all $\psi_p(D)$'s vanish.*

VIII. Influence of p-curvature

We return to the situation of an algebraic differential equation (M, ∇) on a smooth connected algebraic variety X over $\mathbb{C}$. We will say that (M, ∇) has "quasi-unipotent (resp. finite) local monodromy at infinity" if for every smooth connected complete complex curve C, every finite subset S of C, and every morphism:

$$f:\quad C-S\rightarrow X,$$

the pulled-back equation $f^*(M, \nabla)$ on $C-S$ has quasi-unipotent (resp. finite) local monodromy around every point $s\in S$. (Along the same lines, we should recall that (M, ∇) on X has regular singular points if and only if all of its pull-backs to curves as above have regular singular points in the classical sense.)

Now consider a "spreading out" $(\mathbb{M}, \nabla)$ on $\mathbb{X}/R$ of our (M, ∇) on $X/\mathbb{C}$. We have the following theorem.

THEOREM 8.1 (*cf.* [6], [7]).

(1) *If, for an infinite set of primes p, the p-curvatures $\psi_p(D)$ of $(\mathbb{M}, \nabla)\otimes\mathbb{F}_p$ are all nilpotent (in the sense that $\psi_p(D)$ is a nilpotent endomorphism of $\mathbb{M}\otimes\mathbb{F}_p$), then (M, ∇) on X has regular singular points.*

(2) *If the ψ_p's are nilpotent for a set of primes p of (Dirichlet) density one, in particular if the ψ_p are nilpotent for almost all p, then (M, ∇) has quasi-unipotent local monodromy at infinity.*

(3) *If the ψ_p's vanish for a set of primes of density one, then (M, ∇) has finite local monodromy at infinity.*

(4) *If (M, ∇) becomes trivial on a finite etale covering of X, then $\psi_p = 0$ for almost all primes p.*

(5) *If ψ_p vanishes for almost all p, and if (M, ∇) is a "suitable direct factor" of a Picard-Fuchs equation on X, (the relative de Rham cohomology, with its Gauss-Manin connection, of a proper smooth X-scheme minus a relative "divisor with normal crossings") then (M, ∇) becomes trivial on a finite etale covering of X.*

IX. A conjectural description of Lie (G_{gal})

We consider an algebraic differential equation (M, ∇) on our smooth connected X over $\mathbb{C}$. Let

$$\mathscr{G} \subset \mathrm{End}(M \otimes \mathbb{C}(X)),$$

be an algebraic Lie sub-algebra of the $\mathbb{C}(X)$-Lie algebra End $(M \otimes \mathbb{C}(X))$. We will say that $\mathscr{G}$ "contains the p-curvatures ψ_p for almost all p" if the following criterion is satisfied:

CRITERION 9.1. — Pick a *finite* collection of subspaces of constructions:

$$W_i \subset \mathrm{Constr}_i(M \otimes \mathbb{C}(X)),$$

which defines $\mathscr{G}$. Pick a non-void Zariski open set $U \subset X$ such that the named $\mathbb{C}(X)$-subspaces W_i are the generic fibres of locally free sheaves $W_{i, v}$ on U which themselves are locally direct factors, over U, of the corresponding constructs:

$$W_{i, U} \subset \mathrm{Constr}_i(M) \mid U \quad \text{with locally free quotient.}$$

Now "spread out" this data on $U/\mathbb{C}$ to:

$$\mathbb{U}/R, \quad (\mathbb{M}, \nabla) \quad \text{on } \mathbb{U}/R,$$

$$\text{locally free sheaves } \mathbb{W}_i \text{ on } \mathbb{U},$$

$$\mathbb{W}_i \subset \mathrm{Constr}_i(\mathbb{M}) \text{ with locally free quotient.}$$

Then for almost all primes p, the p-curvatures $\psi_p(D)$ attached to $(\mathbb{M}, \nabla)\otimes\mathbb{F}_p$ on $\mathbb{U}\otimes\mathbb{F}_p$ over $R\otimes\mathbb{F}_p$, are required to stabilize the sub-sheaves $\mathbb{W}_i\otimes\mathbb{F}_p\subset\mathrm{Constr}_i(\mathbb{M})\otimes\mathbb{F}_p=\mathrm{Constr}_i(\mathbb{M}\otimes\mathbb{F}_p)$.

It follows easily from Lemma 6.1 that if this criterion is satisfied for *one* collection of choices involved, then it is satisfied for any collection of choices.

Clearly the *intersection* of any two algebraic Lie-subalgebras of $\mathrm{End}(\mathbb{M}\otimes\mathbb{C}(X))$ which "contain the ψ_p for almost all p" is another one (simply work with the union of two finite collections of subspaces of constructions which define the two). Because any descending chain of Lie subalgebras of a finite-dimensional Lie algebra must stabilize after finitely many steps, it makes sense to talk about the *smallest* algebraic Lie-subalgebra of $\mathrm{End}(M\otimes\mathbb{C}(X))$ which "contains the ψ_p for almost all p".

CONJECTURE 9.2. — *The Lie algebra Lie* $(G_{\mathrm{gal}}(M, \nabla, \mathbb{C}(X)))$ *is the smallest algebraic Lie sub-algebra of* $\mathrm{End}(M\otimes\mathbb{C}(X))$ *which contains the* ψ_p *for almost all p.*

One inclusion, at least, is easy.

PROPOSITION 9.3. — *The Lie algebra Lie* $(G_{\mathrm{gal}}(M, \mathbb{C}(X)))$ *contains the* ψ_p *for almost all p.*

Proof. — The group G_{gal} is defined by the list of all horizontal subspaces of all $\mathrm{Constr}(M\otimes\mathbb{C}(X))$'s. Because GL is noetherian, G_{gal} is defined by some finite sublist, say $\{W_i\subset\mathrm{Constr}_i\}_i$, then by $\oplus W_i\subset\oplus\mathrm{Constr}_i$, and finally by the horizontal line $L=\Lambda^{\max}(\oplus W_i)$ in the corresponding exterior power of $\oplus\mathrm{Constr}_i$. Thus G_{gal} is defined by a single horizontal line L in a single $\mathrm{Constr}(M\otimes\mathbb{C}(X))$. As already noted, such an L is the generic fibre of a unique rank-one sub-equation (L_X, ∇) on all of X:

$$(L_X, \nabla)\subset\mathrm{Constr}(M, \nabla)$$

(the quotient M/L_X is automatically free on $\mathbb{X}$, thanks to ∇). We may choose a thickening of this situation:

$$\mathbb{X}/R,\quad (\mathbb{M}, \nabla)\quad \text{on } \mathbb{X}/R,\quad (\mathbb{L}, \nabla)\quad \text{on } \mathbb{X}/R,$$

$(\mathbb{L}, \nabla)\subset\mathrm{Constr}(\mathbb{M}, \nabla)$ with locally free quotient.

Then for any prime p, $\mathbb{L}\otimes\mathbb{F}_p$ is a ∇-stable line in $\mathrm{Constr}(\mathbb{M}\otimes\mathbb{F}_p)$, and is therefore stable by ψ_p.

Q.E.D.

COROLLARY 9.4. — *If Lie* $(G_{gal}(M, \nabla, \mathbb{C}(X))=0$, *then* (M, ∇) *has regular singular points (and therefore becomes trivial on a finite etale covering of* X, *cf. Proposition* 5.3).

Proof. — By the preceding proposition 9.3, if $\mathrm{Lie}(G_{gal})=0$, then we must have $\psi_p=0$ for almost all p. And as already noted (8.1, (1)), the vanishing of ψ_p for almost all p guarantees regular singular points.

Q.E.D.

X. Reduction to a conjecture of Grothendieck, and applications

In 1969, Grothendieck formulated the following conjecture.

CONJECTURE 10.1 (Grothendieck). — *If* (M, ∇) *has* $\psi_p=0$ *for almost all* p, *then* (M, ∇) *becomes trivial on a finite etale covering of* X.

In view of Corollary 9.4, this amounts to asking that $\mathrm{Lie}(G_{gal})$ vanish if almost all the ψ_p vanish. It is therefore the special case "$\psi_p=0$ for almost all p" of our general conjecture. In fact, our general conjecture is a consequence of Grothendieck's.

THEOREM 10.2. — *Let* (M, ∇) *on* X *be given. Then Conjecture* 9.2 *is true for* (M, ∇) *on* X *if Grothendieck's conjecture is true for all equations on* X *of the form* $(W_1, \nabla_1)\otimes(W_2, \nabla_2)^{\vee}$, *where the equations* (W_i, ∇_i) *for* $i=1, 2$ *are each subequations of* $\mathrm{Constr}(M, \nabla)$*'s, and* (W_2, ∇_2) *is of rank one.*

Proof. — Let $\mathcal{G}$ be the smallest algebraic Lie subalgebra of $\mathrm{End}(M\otimes\mathbb{C}(X))$ which contains the ψ_p for almost all p. We must show that $\mathrm{Lie}(G_{gal}(M, \nabla, \mathbb{C}(X)))$ lies in $\mathcal{G}$.

Because $\mathcal{G}$ is algebraic, it is definable by *one* line L in *one* construction $\mathrm{Constr}(M\otimes\mathbb{C}(X))$. We must show that this line is stable by $\mathrm{Lie}(G_{gal})$. If this line L is ∇-stable, then, by the very definition of G_{gal}, L will be stable by $\mathrm{Lie}(G_{gal})$. Suppose that L is not ∇-stable, and let W be the $\mathbb{C}(X)$-space spanned by some non-zero vector $l\in L$ and all its various higher derivatives:

$$\left(\Pi\nabla\left(\frac{\partial}{\partial x_i}\right)^{n_i}\right)(l)$$

(where $\{x_i\}$ is some separating transcendence basis of $\mathbb{C}(X)$ over $\mathbb{C}$).

Thus we have:

$$L\subset W\subset \mathrm{Constr}(M\otimes\mathbb{C}(X)),$$

and W is clearly the smallest ∇-stable $\mathbb{C}(X)$-subspace of $\operatorname{Constr}(M \otimes \mathbb{C}(X))$ which contains L. Because W is ∇-stable, it is the generic fibre of some algebraic sub-equation:

$$(W_X, \nabla) \subset \operatorname{Constr}(M, \nabla).$$

We will now show that (W_X, ∇) has *scalar* p-curvature for almost all p.

If we choose a small enough affine open set $V \subset X$, the functions $\Psi_1, \ldots, \Psi_n$ will be a "local coordinate system on V" (i.e. an etale map $V \to A^n_{\mathbb{C}}$), the line L will extend to an invertible sheaf L_V on V, the vector $l \in L$ will extend to a basis, still noted l, of L_V, and the locally free sheaf $W_X \mid V$ will be free on a basis of the form:

$$\left\{ l, \text{ certain } \Pi\nabla\left(\frac{\partial}{\partial x_i}\right)^{n_i}(l) \right\}.$$

We may further assume that this basis is adapted to the "filtration by order of differential operator" in the sense that for *any* monomial, $\Pi\nabla(\partial/\partial x_i)^{M_i}$ the expression of $\Pi\nabla(\partial/\partial x_i)^{M_i}(l)$ in terms of our chosen basis involves only those basis vectors $\nabla(\partial/\partial x_i)^{n_i}(l)$ with $\Sigma n_i \leqslant \Sigma M_i$.

Now "spread out" this entire situation, to some U/R, and reduce mod $p \gg 0$. We know that $\mathbb{L} \otimes \mathbb{F}_p$ is ψ_p-stable (because we chose $L \subset \operatorname{Constr}(M \otimes \mathbb{C}(X))$ to *define* the *smallest* algebraic Lie sub-algebra of $\operatorname{End}(M \otimes \mathbb{C}(X))$ which contains ψ_p for almost all p). Therefore we have:

$$\psi_p(D)(l) = a(p, D)\, l \bmod p.$$

Because the endomorphism $\psi_p(D)$ of $W \otimes \mathbb{F}_p$ is *horizontal*, when we compute $\psi_p(D)$ of one of the other basis vectors, we find:

$$\begin{aligned}\psi_p(D)\left(\Pi\nabla\left(\frac{\partial}{\partial x_i}\right)^{n_i}\right)(l) &= \left(\Pi\nabla\left(\frac{\partial}{\partial x_i}\right)^{n_i}\right)(\psi_p(D)(l)) \\ &= \left(\Pi\nabla\left(\frac{\partial}{\partial x_i}\right)^{n_i}\right)(a(p, D)\, l) \\ &= a(p, D).\Pi\nabla\left(\frac{\partial}{\partial x_i}\right)^{n_i}(l) \\ &\qquad + \text{lower-order derivatives of } l.\end{aligned}$$

Therefore the matrix of $\psi_p(D)$ acting on $W \otimes \mathbb{F}_p$ in the basis:

$$\left\{ l, \Pi \nabla\left(\frac{\partial}{\partial x_i}\right)^{n_i}(l) \right\},$$

which we have assumed adapted to the "filtration by order of differential operator", is *upper triangular*, with $a(p, D)$ along the diagonal:

$$\begin{pmatrix} a(p, D) & & ? \\ & \ddots & \\ 0 & & a(p, D) \end{pmatrix}.$$

We will show that for $p > \operatorname{rank}(W)$ this matrix is *diagonal*.

Let r denote the rank of W. Then the p-curvature of $\det(W, \nabla) \otimes \mathbb{F}_p$, which in general is the *trace* of the p-curvature of $(W, \nabla) \otimes \mathbb{F}_p$, is given by the formula:

$$\psi_p(D) \,|\, \det(W, \nabla) \otimes \mathbb{F}_p = r.a(p, D).$$

But the p-curvature of any rank one equation $(\mathscr{L}, \nabla)$ is a horizontal section of $\underline{\mathscr{E}\mathrm{nd}}(\mathscr{L}, \nabla) \simeq (\mathcal{O}, d)$. Therefore the function $r.a(p, D)$ on $U \otimes \mathbb{F}_p$ is killed by the operator $\nabla(\partial/\partial x_i)$. For $p \gg 0$, we certainly have $p > r = \operatorname{rank}(W)$, and for such p we may infer:

$$\nabla\left(\frac{\partial}{\partial x_i}\right)(a(p, D)) = 0 \quad \text{for all } i.$$

Going back to the earlier calculation of the matrix of $\psi_p(D)$ on $W \otimes \mathbb{F}_p$, we see that it is the scalar matrix $a(p, D)$, as claimed.

Now consider the algebraic differential equation:

$$(\operatorname{Symm}^r(W_X, \nabla)) \otimes \det(W_X, \nabla)^{\vee}.$$

Because (W_X, ∇) has *scalar* p-curvature for almost all p, an immediate calculation shows that this equation has $\psi_p = 0$ for almost all p.

This equation is of the required form $(W_1, \nabla_1) \otimes (W_2, \nabla_2)^{\vee}$, with:

$$\begin{cases} (W_1, \nabla_1) = \operatorname{Symm}^r(W_X, \nabla) \subset \operatorname{Symm}^r(\operatorname{Constr}(M, \nabla)), \\ (W_2, \nabla_2) = \det(W_X, \nabla) \subset \Lambda^r(\operatorname{Constr}(M, \nabla)). \end{cases}$$

Therefore by the hypothesis of the theorem being proven, we may conclude that the equation:

$$\mathrm{Symm}^r(W_X, \nabla) \otimes \det(W_X, \nabla)^{\check{}},$$

has *its* Lie $(G_{\mathrm{gal}})=0$. It follows immediately that:

$$\mathrm{Symm}^r(W_X, \nabla),$$

has *its* Lie (G_{gal}) contained in the Lie algebra of scalar matrices, whence it follows that (W_X, ∇) itself must have *its* Lie (G_{gal}) contained in the Lie algebra of scalar matrices.

Therefore *every* line in the generic fibre $W_X \otimes \mathbb{C}(X) = W$, in particular L, is stable by Lie (G_{gal}), as required.

COROLLARY 10.3. — *Let (M, ∇) be an algebraic differential equation on $\mathbb{P}^1 - S$, an open set in $\mathbb{P}^1$. Suppose that $(M, \nabla)^{an}$ has abelian monodromy (a condition which is automatically fulfilled if $(S) \leqslant 2$, for in that case $\pi_1(\mathbb{P}^1 - S)$ is itself abelian). Then the general conjecture holds for (M, ∇) on $\mathbb{P}^1 - S$.*

Proof. — Any sub-equation (W, ∇) of any Constr(M, ∇) will also have abelian monodromy, also any $(W_1, \nabla_1) \otimes (W_2, \nabla_2)^{\check{}}$. So we are reduced to proving Grothendieck's conjecture on $\mathbb{P}^1 - S$ for (M, ∇)'s with abelian monodromy. Suppose $\psi_p = 0$ for almost all p. Then (M, ∇) has regular singular points (8.1), so it suffices to show that (M, ∇) has finite global monodromy. As $\pi_1(\mathbb{P}^1 - S)$ is generated by the local monodromies around the missing points S, it suffices to show that these local monodromy transformations are of finite order (since we have *assumed* that they commute). But the finiteness of local monodromy is also a consequence of the hypothesis "$\psi_p = 0$ for almost all p" (8.1, (3)).

Q.E.D.

Here are some examples to which the corollary applies.

EXAMPLES 10.4. — (1) The Airey equation on $\mathbb{A}^1$, indeed any equation on $\mathbb{A}^1$, satisfies the general conjecture, because $\mathbb{A}^1$ is simply connected. The Airey equation,

$$\left(\frac{d}{dT}\right)^2 f = Tf,$$

written in system form

$$\frac{d}{dT}\begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ T & 0 \end{pmatrix}\begin{pmatrix} f \\ g \end{pmatrix},$$

to provide us with an (M, ∇), is known [5] to have $G_{gal} = SL(2)$. Therefore $\mathfrak{S}\mathfrak{l}(2)$ is the smallest algebraic Lie subalgebra of 2×2 matrices which contains the ψ_p for almost all p. Can one see this "directly"?

(2) The confluent hypergeometric (Whittaker) equation on $\mathbb{G}_m$:

$$\frac{d^2}{dT}(W) + \left\{ -\frac{1}{4} + \frac{k}{T} + \frac{(1/4)-m^2}{T^2} \right\} W = 0.$$

Here again the general conjecture holds, because π_1 is abelian. Can one calculate Lie (G_{gal}), as a function of the parameters (k, m)?

(3) Any first order equation on any $\mathbb{P}^1 - S$ necessarily has abelian monodromy, hence the conjecture holds for it.

THEOREM 10.5. — *Suppose that the general conjecture is true for all (M, ∇)'s on all open subsets of $\mathbb{P}^1$. Then the general conjecture is universally true on all smooth connected algebraic varieties over $\mathbb{C}$.*

Proof. — In view of (10.2), it suffices to prove that Grothendieck's conjecture holds universally. Because the condition "$\psi_p = 0$ for almost all p" implies regular singular points, Grothendieck's conjecture may be restated as the conjecture:

($\star$) if (M, ∇) has $\psi_p = 0$ for almost all p, then $(M, \nabla)^{an}$ has finite monodromy.

Let $f : Y \to X$ be a morphism of smooth connected $\mathbb{C}$-schemes, such that the image $f_*(\pi_1(Y^{an}))$ is a subgroup of finite index in $\pi_1(X^{an})$. Because the condition "$\psi_p = 0$ for almost all p" is preserved by arbitrary inverse image, to prove the universal truth of $\star$ for X it suffices to prove the universal truth of $\star$ for Y. But whatever X, we can choose a smooth connected curve $Y \subset X$ such that $\pi_1(Y^{an})$ maps *onto* $\pi_1(X^{an})$.

[*Proof.* — We may replace X by a non-empty quasi-projective open set $U \subset X$, since $\pi_1(U^{an}) \twoheadrightarrow \pi_1(X^{an})$. Take some projective embedding $U \subset \mathbb{P}^N$. For a general linear-space section W of $\mathbb{P}^N$ with $\text{codim}(W) = \dim(U) - 1$, the curve $Y = W \cap U$ in U has $\pi_1(Y^{an}) \twoheadrightarrow \pi_1(U^{an})$ (*cf.* [3], 1.4 *or* [4]).]

Thus we are reduced to proving ★ on smooth connected curves. If X is a smooth connected curve, we may replace it by any non-void open set $U \subset X$ (because $\pi_1(U^{an}) \twoheadrightarrow \pi_1(X^{an})$).

Shrinking X if necessary, we may assume that X is finite etale over some non-empty open set $\mathbb{P}^1 - S$ of $\mathbb{P}^1$. Now replacing this X by a finite etale covering Y of X (allowable because $\pi_1(Y^{an}) \hookrightarrow \pi_1(X^{an})$ as a subgroup of finite index), we may assume that X is finite etale galois over some $\mathbb{P}^1 - S$:

$$\left.\begin{matrix} X \\ \pi \downarrow \\ \mathbb{P}^1 - S \end{matrix}\right) \text{galois group } \Sigma.$$

If (M, ∇) on X has $\psi_p = 0$ for almost all p, then $\pi_*(M, \nabla)$ has $\psi_p = 0$ for almost all p. By assumption, then, $\pi_*(M, \nabla)^{ss}$ has finite monodromy on $\mathbb{P}^1 - S$. Therefore its pull-back to X has finite monodromy on X. But (M, ∇) is itself a direct factor of $\pi_* \pi^*(M, \nabla)$ indeed we have:

$$\pi_* \pi^*(M, \nabla) \simeq \bigoplus_{\sigma \in \Sigma} (M, \nabla)^{(\sigma)}.$$

These (M, ∇) has finite monodromy on X, as required.

Q.E.D.

(10.6). To conclude this section, we will give a *direct* proof that the general conjecture holds for any equation on $\mathbb{G}_m$ of the form:

$$T \frac{d}{dT} \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} + \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = 0.$$

where $\lambda_1, \ldots, \lambda_n$ are complex constants (although it is a special case of Corollary 10.3).

This equation visibly has regular singular points, so $G_{gal} = G_{mono}$. The monodromy representation carries the generator "turning counterclockwise once around the origin" of $\pi_1(\mathbb{G}_m)$ to the automorphism:

$$A = \exp\left(-2\pi i \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}\right).$$

Therefore $G_{gal}=G_{mono}$ is simply the Zariski closure in $GL(n)$ of the abstract subgroup $\{A^r\}\, r\in\mathbb{Z}$. The Lie algebra $\mathrm{Lie}(G_{gal})$ is the smallest algebraic Lie sub-algebra of $M(n)$ which contains the endomorphism:

$$\begin{pmatrix} 2\pi i\lambda_1 & & \\ & \ddots & \\ & & 2\pi i\lambda_n \end{pmatrix},$$

In particular, $\mathrm{Lie}(G_{gal})$ is the Lie algebra of an algebraic sub-torus of the standard diagonal torus. Therefore $\mathrm{Lie}(G_{gal})$ is defined inside *all* diagonal matrices:

$$\begin{pmatrix} X_1 & & \\ & \ddots & \\ & & X_n \end{pmatrix},$$

by the vanishing of all linear forms:

$$\Sigma N_i X_i = 0,$$

where $(N_1, \ldots, N_n)$ is any n-triple of integers such that:

$$\Sigma N_i \lambda_i \in \mathbb{Q}.$$

Now let us compute p-curvatures (for the obvious "spreading out" over the subring $R=\mathbb{Z}[\lambda_1, \ldots, \lambda_n] \subset \mathbb{C}$). We have:

$$\begin{aligned}\psi_p\left(T\frac{d}{dT}\right) &\overset{\text{dfn}}{=} \left(\nabla\left(T\frac{d}{dT}\right)^p\right)-\left(\left(T\frac{d}{dT}\right)^p\right)\\ &=\left(\nabla\left(T\frac{d}{dT}\right)\right)^p-\nabla\left(T\frac{d}{dT}\right)\\ &=\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}^p-\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}\\ &=\begin{pmatrix} (\lambda_1)^p-\lambda_1 & & \\ & \ddots & \\ & & (\lambda_n)^p-\lambda_n \end{pmatrix}.\end{aligned}$$

The smallest algebraic Lie subalgebra of $M(n)$ containing the ψ_p for almost all p is a sub-algebra of Lie (G_{gal}), so it is itself defined inside all diagonal matrices:

$$\begin{pmatrix} X_1 & & \\ & \ddots & \\ & & X_n \end{pmatrix}.$$

by certain equations:

$$\Sigma M_i X_i = 0,$$

with integers M_i. The n-triples $(M_1, \ldots, M_n)$ which occur are precisely those for which we have:

$$\textstyle\sum_i M_i((\lambda_i)^p - \lambda_i) \equiv \quad \bmod p,$$

for almost all p. What must be shown is that for any such n-triple $(M_1, \ldots, M_n)$, we have:

$$\Sigma M_i \lambda_i \in \mathbb{Q}.$$

But this is clear, because the quantity $\mu \in R = \mathbb{Z}[\lambda_1, \ldots, \lambda_n]$ defined by:

$$\mu = \Sigma M_i \lambda_i,$$

satisfies the congruence:

$$\mu \equiv \mu^p \bmod pR,$$

for almost all p (*cf.* [6]).

XI. Equations of low rank

We will first discuss the case of equations of rank one, about which we know embarrassingly little (*cf.* [7]). Thus let $(\mathscr{L}, \nabla)$ be a rank one equation on an arbitrary X. Then Lie (G_{gal}) is either reduced to zero, or it is the entire one-dimensional Lie algebra Lie $(GL(1))$.

Let $\mathscr{G}$ be the smallest algebraic Lie sub-algebra of Lie $(GL(1))$ which contains the ψ_p for almost all p. Thus:

$$\mathscr{G} = \begin{cases} 0 & \text{if } \psi_p = 0 \text{ for almost all } p, \\ \text{Lie}(GL(1)) & \text{if } \psi_p \neq 0 \text{ for infinitely many } p. \end{cases}$$

We have the inclusions:

$$0 \subseteq \mathscr{G} \subseteq \mathrm{Lie}\,(G_{\mathrm{gal}}) \subseteq \mathrm{Lie}\,(GL(1)).$$

PROPOSITION 11.1. — *If* $(\mathscr{L}, \nabla)$ *on* X *does* not *have regular singular points, or if it does* not *have finite local monodromy at infinity, then the general conjecture* (9.2) *is true for* $(\mathscr{L}, \nabla)$ *on* X, *and we have* $\mathscr{G} = Lie\, G_{\mathrm{gal}}) = Lie\,(GL(1))$.

Proof. — Thanks to (8.1), we know that neither of the possibilities envisaged can arise if $\psi_p = 0$ for almost all p. Therefore we must have $\psi_p \neq 0$ for infinitely many p, whence $\mathscr{G} = \mathrm{Lie}\,(\mathrm{GL}\,(1))$.

Q.E.D.

Here is an example. Take $X = \mathbb{A}^1$, and $(\mathscr{L}, \nabla) = (\mathscr{O}, d + dT)$, the differential equation for $\exp(-\mathrm{T})$:

$$\frac{d}{dT}(f) + f = 0.$$

The p-curvature is given by the simple formula:

$$\psi_p\left(\frac{d}{dT}\right) = \nabla\left(\frac{d}{dT}\right)^p = \left(\frac{d}{dT} + 1\right)^p = 1.$$

We have already pointed out (10.4, (3)) that on an open set $\mathbb{P}^1 - S$ of $\mathbb{P}^1$, the general conjecture (9.2) holds for *any* equation of rank one.

We now turn to the case of equations of rank two. For simplicity of exposition, we will consider only those rank two equations (M, ∇), on an arbitrary X, whose *determinant* $\det(M, \nabla)$ is either trivial, or becomes trivial on a finite etale covering of X. As before, we denote by $\mathscr{G}$ the smallest algebraic Lie subalgebra of $\mathrm{End}(M \otimes \mathbb{C}(X))$ which contains the ψ_p for almost all p. We have the inclusions:

$$0 \subseteq \mathscr{G} \subseteq \mathrm{Lie}(G_{\mathrm{gal}}) \subseteq \mathfrak{Sl}(2).$$

THEOREM 11.2. — *Let* (M, ∇) *be a rank two equation on an arbitrary* X, *whose determinant becomes trivial on a finite etale covering of* X. *Suppose that* $\mathscr{G} \neq 0$, *i.e. that* (M, ∇) *has non-zero* ψ_p *for infinitely many* p. (*This is automatically the case if* (M, ∇) *does not have regular singular points, or if it does* not *have finite local monodromy at infinity.*) *Then the general conjecture* (9.2) *holds for* (M, ∇) *on* X, *i.e. we have* $\mathscr{G} = Lie(G_{\mathrm{gal}})$.

Proof. — We will suppose successively that $\mathscr{G}$ is one of the short list of non-zero algebraic Lie sub-algebras of $\mathfrak{Sl}(2, \mathbb{C}(X))$, and show that in each case we have Lie $(G_{gal}) \subset \mathscr{G}$.

Case 1. — $\mathscr{G} = \mathfrak{Sl}(2)$. There is nothing to prove.

Case 2. — $\mathscr{G}$ = a non-split Cartan. This means that there is a quadratic extension $\mathbb{C}(Y)$ of $\mathbb{C}(X)$, and a pair of conjugate irrational lines L_1, L_2 in $M \bigotimes_{\mathbb{C}(X)} \mathbb{C}(Y)$, such that $\mathscr{G}$ is their stabilizer in $Sl(2)$. If these lines are both ∇-stable, then they are both stabilized by Lie (G_{gal}), whence Lie $(G_{gal}) \subset \mathscr{G}$. If, say, L_1 is *not* horizontal, then it and its derivatives span $M \otimes \mathbb{C}(Y)$. Because L_1 (and L_2) are each *stable* by ψ_p for almost all p, it follows that (M, ∇) has *scalar* ψ_p for almost all p (*cf.* the proof of 10.2), whence $\mathscr{G} \subset$ (scalars) $\cap \mathfrak{Sl}(2) = 0$, a contradiction.

Case 3. — $\mathscr{G}$ = a split Cartan. There are two distinct lines L_1, $L_2 \subset M \otimes \mathbb{C}(X)$ such that $\mathscr{G}$ is their stabilizer in $Sl(2)$. Same argument as in case 2.

Case 4. — $\mathscr{G}$ = a Borel. There is one line $L \subset M \otimes \mathbb{C}(X)$ such that $\mathscr{G}$ is its stabilizer in $Sl(2)$. Same argument as in case 2.

Q.E.D.

EXAMPLE 11.3. — Let Λ be a lattice in $\mathbb{C}$, $E = \mathbb{C}/\Lambda$ the corresponding elliptic curve, and $\mathscr{P}(z) = \mathscr{P}(z; \Lambda)$ the associated Weierstrass $\mathscr{P}$-function. Let a, b be complex constants, and consider the Lamé equation on $E - \{0\}$:

$$\left(\frac{d}{dz}\right)^2 (f) = (a\mathscr{P}(z) + b) f,$$

which visibly has trivial determinant. This has a regular singular point at the origin $z = 0$ of E, with exponents the roots of the polynomial $\lambda^2 - \lambda = a$. Therefore if a is *not* of the form $\alpha(\alpha - 1)$ with $\alpha \in \mathbb{Q}$, the exponents are irrational, and the local monodromy around $z = 0$ is necessarily of infinite order. The theorem (11.2) then applies, to show that the general conjecture (9.2) is true for this Lamé equation, so long as a is *not* of the form $\alpha(\alpha - 1)$ with $\alpha \in \mathbb{Q}$. [Unfortunately it is precisely the case in which $a = \alpha(\alpha - 1)$ with $\alpha \in \mathbb{Q}$ that is in many ways the most interesting.]

THEOREM 11.4. — *For any rational numbers a, b, c, the hypergeometric equation on* $\mathbb{P}^1 - \{0, 1, \infty\}$ *with parameters* (a, b, c):

$$T(T-1)\frac{d^2 f}{dT^2} + (c - \{a+b+1\}\, T)\frac{df}{dT} + abf = 0,$$

satisfies the general conjecture (9.2), *i.e. its* Lie (G_{gal}) *is the smallest algebraic Lie sub-algebra of* $\mathfrak{Sl}(2)$ containing the ψ_p *for almost all* p.

Proof. — Because a, b, c are rational, the determinant becomes trivial on the *finite* etale covering defined by the function $T^{-c}(T-1)^{c-a-b-1}$. Therefore we may conclude by theorem (11.2), except in the case $\mathscr{G}=0$. In the case $\mathscr{G}=0$, the required vanishing of Lie (G_{gal}) is proven in ([7], 6.2) for the hypergeometric equation.

Appendix: A formula of O. Gabber

Let S be an arbitrary $\mathbb{F}_p$-scheme, X/S a smooth S-scheme, and (M, ∇) a pair consisting of an $\mathcal{O}_X$-module M together with an integrable connection relative to S

$$\nabla: \quad M \to M \otimes \Omega^1_{X/S}.$$

The p-curvature of (M, ∇) defines a p-linear map of $\mathcal{O}_X$-modules

$$\underline{\mathrm{Der}}_S(\mathcal{O}_X, \mathcal{O}_X) \to \underline{\mathrm{End}}_{\mathcal{O}_X}(M),$$
$$D \to \Psi_p(D).$$

By transposition, this map may be viewed as a global section Ψ_p over X of the $\mathcal{O}_X$-module

$$\underline{\mathrm{End}}_{\mathcal{O}_X}(M) \bigotimes_{\mathcal{O}_X} (\Omega^1_{X/S})^{(p)},$$

where for any $\mathcal{O}_X$-module N, we denote by $N^{(p)}$ its inverse image by the absolute Frobenius endomorphism F_{abs} of X (elevation to the p'th power):

$$N^{(p)} \overset{\mathrm{dfn}}{=} F^*_{abs}(N) = N \bigotimes_{\mathcal{O}_X, F_{abs}} \mathcal{O}_X.$$

In local coordinates $x_1, \ldots, x_n$ for X/S, the expression of Ψ_p as section of $\underline{\mathrm{End}}_{\mathcal{O}_X}(M) \times (\Omega^1_{X/S})^{(p)}$ is simply:

$$\Psi_p = \Sigma \Psi_p \left(\frac{\partial}{\partial x_i}\right) \times (dx_i)^{(p)}.$$

Now consider a second $\mathbb{F}_p$-scheme T, a smooth T-scheme Y/T, and a commutative diagram:

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ \downarrow & & \downarrow \\ T & \xrightarrow{g} & S \end{array}$$

On Y/T, we dispose of the inverse image $(f, g)^* (M, \nabla)$ of (M, ∇) on X/S, which is the $\mathcal{O}_Y$-module $f^* (M)$ together with the induced connection. It's p-curvature, which we note $\Psi_{p, (f, g)^* (M, \nabla)}$, is a global section on Y of the $\mathcal{O}_Y$-module:

$$\underline{\mathrm{End}}_{\mathcal{O}_Y} (f^* (M)) \bigotimes_{\mathcal{O}_Y} (\Omega^1_{Y/T})^{(p)}.$$

It is natural to ask how to compute $\Psi_{p, (f, g)^* (M, \nabla)}$ in terms of the Ψ_p for (M, ∇) itself. There is an obvious "candidate solution" to this problem, defined as follows.

First, there is a natural "extension of scalars" homomorphism of $\mathcal{O}_Y$-modules:

$$\text{(A)} \qquad f^* (\underline{\mathrm{End}}_{\mathcal{O}_X} (M)) \to \underline{\mathrm{End}}_{\mathcal{O}_Y} (f^* (M)).$$

Second, the functoriality of Ω^1 yields a natural homomorphism of $\mathcal{O}_Y$-modules (pull-back of a one form):

$$f^* \Omega^1_{X/S} \to \Omega^1_{Y/T},$$

which in turn may be "pulled back" by absolute Frobenius to yield an $\mathcal{O}_Y$-homomorphism:

$$\text{(B)} \qquad f^* ((\Omega^1_{X/S})^{(p)}) \simeq (f^* \Omega^1_{X/S})^{(p)} \to (\Omega^1_{Y/T})^{(p)}.$$

The tensor product of (A) and (B) yields an $\mathcal{O}_Y$-homomorphism:

$$(\mathrm{A} \otimes \mathrm{B}) \quad f^* (\mathrm{End}_{\mathcal{O}_X} (M) \bigotimes_{\mathcal{O}_X} (\Omega^1_{X/S})^{(p)}) \to \underline{\mathrm{End}}_{\mathcal{O}_Y} (f^* M) \bigotimes_{\mathcal{O}_Y} (\Omega^1_{Y/T})^{(p)};$$

given in local coordinates $x_1, \ldots, x_n$ for X/S by the formula:

$$\Sigma A_i \otimes (dx_i)^{(p)} \to \Sigma f^* (A_i) \otimes (d (f^* (x_i)))^{(p)}.$$

Given any global section over X:

$$\Lambda \in \underline{\mathrm{End}}_{\mathcal{O}_X} (M) \otimes (\Omega^1_{X/S})^{(p)},$$

we denote by:

$$(f, g)^* (\Lambda) \in \underline{\mathrm{End}}_{\mathcal{O}_Y} (f^* (M)) \bigotimes_{\mathcal{O}_Y} (\Omega^1_{Y/T})^{(p)},$$

the global section over Y obtained by applying (A ⊗ B) to $f^* (\Lambda)$.

FORMULA (O. Gabber). — *With the notations and hypotheses as above, the p-curvature* $\psi_{p, (f, g)^* (M, \nabla)}$ *of* $(f, g)^* (M, \nabla)$ *on* Y/T *is obtained from the p-curvature* Ψ_p *of* (M, ∇) *on* X/S *by the formula:*

$$\Psi_{p, (f, g)^* (M, \nabla)} = (f, g)^* (\Psi_p)$$

(*equality inside* $\underline{\mathrm{End}}_{\mathcal{O}_Y} (f^* M) \bigotimes_{\mathcal{O}_Y} (\Omega^1_{Y/T})^{(p)}$.

Proof. — We may factor the given morphism through the fibre product:

$$\begin{array}{ccccc} Y & \longrightarrow & T \times_S X & \longrightarrow & X \\ \downarrow & & \downarrow & & \downarrow \\ T & = & T & \longrightarrow & S \end{array}$$

and the assertion is obvious for the right-hand square (use local coordinates).

Therefore it suffices to treat the case when $S = T$. The question is local (Zariski) on Y, so we may assume that Y is affine over S, say:

$$Y \hookrightarrow \mathbb{A}^N_S.$$

Then we may factor the given S-morphism $Y \to X$ as:

$$Y \hookrightarrow \mathbb{A}^N_S \times_S Y \xrightarrow{pr_2} Y.$$

Once again (via local coordinates) the assertion is obvious for the right hand map pr_2. Thus we are reduced to the case of a closed immersion of smooth S-schemes:

$$\begin{array}{ccc} Y & \hookrightarrow & X \\ & \searrow \quad \swarrow & \\ & S & \end{array}$$

Because the question is Zariski-local on X, we may assume that X admits local coordinates $x_1, \ldots, x_n$ (i.e. an etale map $X \to \mathbb{A}_S^N$) *and* that Y is defined inside X by the vanishing of $x_1, \ldots, x_d$. Again in this case, the formula becomes obvious in local coordinates.

Q.E.D.

REFERENCES

[1] CHEVALLEY (C.). – Théorie Des Groupes De Lie, *Groupes algébriques, Théorèmes généraux sur les algèbres de Lie*, Hermann, Paris, 1968.

[2] DELIGNE (P.). – Equations Différentielles à Points Singuliers Réguliers, *Springer Lecture Notes in Mathematics*, No. 163, 1970.

[3] DELIGNE (P.). – Le groupe fondamental du complément d'une courbe plane n'ayant que des points doubles ordinaires est abélien (d'après W. Fulton), *Séminaire Bourbaki* 1979/1980, Exposé 543, *Springer Lecture Notes in Mathematics* No. 842, 1981, pp. 1-10.

[4] FULTON (W.). – and LAZARSFELD (R.). – Connectivity and its applications in algebraic geometry, to appear in *Proceedings of the Midwest Algebraic Geometry Conference*, 1980; *Springer Lecture Notes in Mathematics.*

[5] KAPLANSKY (I.). – *An Introduction to Differential Algebra*, Hermann, Paris, 19 .

[6] KATZ (N.). – Nilpotent connections and the monodromy theorem – applications of a result of Turritin, *Publ. Math. I.H.E.S.* No. 39, 1970, pp. 355-412.

[7] KATZ (N.). – Algebraic solutions of differential equations; *p*-curvature and the Hodge filtration, *Inv. Math.* Vol. 18, 1972, pp. 1-118.

[8] SAAVEDRA RIVANO (N.). – Categories Tanakiennes, *Springer Lecture Notes in Mathematics*, No. 265, 1972.