DIFFERENTIAL OPERATORS WITH NILPOTENT p-CURVATURE

By BERNARD DWORK

Introduction. Let K be a field of characteristic p, let $D = d/dX$ and let

$$L = D^n + \alpha_1 D^{n-1} + \cdots + \alpha_n, \tag{I.1}$$

be an ordinary differential operation with coefficients in $K(X)$ the field of rational functions in one variable with coefficients in K.

We say that L has *nilpotent p-curvature* if $D^{p\mu} \in K(X)[D]L$ for some $\mu \in \mathbb{N}$. An elementary account of such operators has been provided by Honda [Ho] and in particular he proved (cf. 1.5 below) a local form of Katz's theorem [Ka] which implies that theorem.

I.2. If L has nilpotent p-curvature then L is fuchsian and the exponents lie in $\mathbb{F}_p$.

(In other words for β algebraic over K, the order of pole of α_j at β is bounded by j $(1 \leq j \leq n)$ and hence for $s \in \mathbb{N}$ we have

$$L(X-\beta)^s \in \chi_{L,\beta}(s)(X-\beta)^{s-n} + (X-\beta)^{s-n+1}K(\beta)[[X-\beta]]$$

where $\chi_{L,\beta}$, the indicial polynomial for L at β, is of degree n and splits in $\mathbb{F}_p$. Furthermore a similar condition holds at infinity.)

The Riemann data of L consists of a tabulation of the singular points together with a list of the exponents at each singular point. We shall use the expression, *restricted Riemann* data, to indicate that the exponents are specified (together of course with the number of singular points) but that the singular points themselves are not necessarily specified (except for ∞ and possibly two other points).

Manuscript received 7 March 1988.
American Journal of Mathematics 112 (1990), 749–786.

Letting $m + 1$ be the number of singular points, we may insist that the restricted Riemann data satisfy the fuchs condition,

I.3. The sum of the exponents equals

$$(m - 1)\binom{n}{2}.$$

Precisely as in the characteristic zero case we construct moduli for fuchsian differential operators with given restricted Riemann data. Specifically let $\gamma = (\gamma_1, \ldots, \gamma_m)$, let $\{\gamma_1, \ldots, \gamma_m, \infty\}$ be the set of singular points. Put

$$\psi(X) = \prod_{i=1}^{m} (X - \gamma_i).$$

Then

$$L = D^n + \sum_{j=1}^{n} A_j \psi^{-j} D^{n-j} \tag{I.4}$$

where each A_j is a polynomial in X.

$$\deg A_j \leqslant j(m - 1) \tag{I.4.1}$$

and for $1 \leqslant j \leqslant n$

$$A_j = A_{j,0} + \psi B_j \tag{I.4.2}$$

with

$$\deg A_{j,0} \leqslant m - 1, \qquad 1 \leqslant j \leqslant n \tag{I.4.3}$$

$$B_1 = 0 \tag{I.4.4}$$

$$B_j = \beta_j X^{q(j)} + \sum_{\ell=0}^{q(j)-1} \nu_{j,\ell} X^{\ell}, \qquad 2 \leqslant j \leqslant n \tag{I.4.5}$$

and here

$$q(j) = j(m - 1) - m. \tag{I.4.6}$$

Both the polynomials $A_{j,0}$ and the coefficients β_j are completely determined by the Riemann data. (If we write the monic indicial polynomial at γ_i in the form

$$\sum_{j=0}^{n} f_j(s)\lambda_j^{(i)} \quad \text{where} \quad f_j(s) = \prod_{i=0}^{n-j-1} (s - i),$$

$f_0 = 1$ so that $\lambda_j^{(i)} \in \mathbb{F}_p$, then by the Lagrange interpolation formula

$$A_{j,0} = \sum_{i=1}^{m} \lambda_j^{(i)}\psi'(\gamma_i)^{j-1}\psi(x)/(x - \gamma_i) \in \mathbb{F}_p[\gamma, X].) \tag{I.4.7}$$

Thus L is parametrized by γ and by the

$$\mathrm{v}_n(m) = (n - 1)[n(m - 1) - 2]/2$$

accessory parameters $\nu = (\ldots, \nu_{j,\ell}, \ldots)$.

We observe that the moduli space is the open subset of $m - 2 + \mathrm{v}_n(m)$ affine space defined by the condition that $\gamma_j \neq \gamma_i$ for $i \neq j$.

It is well known (cf 0.6.3 below) that L is nilpotent if and only if $D^{pn} \in K(X)[D]L$ and hence $L_{\gamma,\nu}$ being nilpotent and having given restricted Riemann data is equivalent to the condition that (γ, ν) lies in an algebraic subset V_N of the moduli space.

We show

I.5. If $(\gamma, \nu) \in V_N$ then ν is integral over $\mathbb{F}_p[\gamma]$.

I.6. V_N is a complete intersection if $n = 2$.

In Section 0 we give a characterization of nilpotent p-curvature in terms of generalizations of Honda's log functions. This is used to eliminate the restriction that $n < p$. For the applications it could be eliminated by means of the remark following Lemma 1.1.

In Section 6 we give the relation between the present theory and the classical invariants associated with Lamé's equation.

Global nilpotence is discussed in Section 7. Our results are fragmentary.

We have been helped by conversations with S. Sperber and N. Katz. We have benefitted from G. Christol's preliminary account of our work in writing Sections 2, 7. We have also benefitted from the advice of S. Kochen in writing Section 7. Our Section 5 is based on methods of F. Baldassarri. B. Chiarellotto's proof of Proposition 0.2 has been helpful.

0. Generalized logarithms in characteristic p. It follows from the definitions that if L is a nilpotent differential operator then the solutions of $Ly = 0$ in any abstract differential field, lie among the solutions of $D^{p^\mu}y = 0$ for μ sufficiently large (in fact $\mu \geqslant$ order L is sufficient). The object of this section is to give for $s \geqslant 0$ the explicit construction of a differential field in which $D^{p^{s+1}}y = 0$ has "sufficiently many solutions," i.e. in which $D^{p^{s+1}}$ becomes trivial in the sense of 0.5 below. The case of $s = 0$ is trivial, the case $s = 1$ has been treated by Honda. Familiarity with the work of Honda will not be assumed.

Let K be a field of characteristic p. Let $\mathcal{F}_0 = K(X)$ be a field which is inseparable (of degree p) over $\Omega_0 = K(X^p)$. Thus the space $\mathcal{D}_{\mathcal{F}_0/\Omega_0}$ of derivations of $\mathcal{F}_0$ (with values in $\mathcal{F}_0$) which are trivial on Ω_0 is a one-dimensional $\mathcal{F}_0$ space [Z-S, Chapter II, Section 17, Theorem 41]. Let D be a nontrivial element of this space whose p^{th} power annihilates $\mathcal{F}_0$. Then $\Omega_0 = \operatorname{Ker}(D, \mathcal{F}_0)$.

Note. We insist neither that X be transcendental over K nor that $D = d/dX$.

The ring $\mathcal{R} = \mathcal{F}_0[D]$ is independent of the choice of D.

Definition. $L \in \mathcal{R}$ has nilpotent p-curvature if for some $\mu \geqslant 0$, $D^{p^\mu} \in \mathcal{R}L$.

Remark. It will follow from 0.6.1 that nilpotence is independent of the choice of D.

Let $z_1, z_2, \ldots$ be an infinite sequence of elements algebraically independent over $K(X)$. Setting $z_0 = X$, $\mathcal{F}_{-1} = K$ we consider the tower of fields $\mathcal{F}_{-1} \subset \mathcal{F}_0 \subset \mathcal{F}_1 \cdots$ defined by setting $\mathcal{F}_s = \mathcal{F}_{s-1}(z_s)$ for $s \geqslant 0$. We extend the differential field structure of $\mathcal{F}_0$ successively to $\mathcal{F}_1, \mathcal{F}_2, \ldots$ etc. by setting

$$Dz_s = \frac{Dz_{s-1}}{z_{s-1}}, \qquad s \geqslant 1.$$

We note that if $\xi \in \mathcal{F}_0$, $D_\xi = \xi D \in \mathcal{D}_{\mathcal{F}_0/\mathcal{F}}$ then D_ξ may be extended to $\mathcal{F} = \lim \mathcal{F}_s$ so as to satisfy the same system of relations. Thus the construction of $\mathcal{F}_s$ may depend upon the choice of z_0 but not upon the choice of D.

PROPOSITION. *For* $s \geq 0$.

$$(0.1)_s \qquad z_s \notin \mathcal{F}_{s-1} + \operatorname{Ker}(D, \mathcal{F}_s)$$

$$(0.2)_s \qquad \operatorname{Ker}(D, \mathcal{F}_s) = \Omega_0(z_1^p, \ldots, z_s^p).$$

Proof (after Bruno Chiarellotto). Both assertions are trivial for $s = 0$. We use induction on s. Let $s \geq 1$. If $(0.1)_s$ is false then there exists $b \in \mathcal{F}_{s-1}$ such that $z_s \in b + \operatorname{Ker}(D, \mathcal{F}_s)$. We write b as a ratio of elements of $\Omega_0[z_0, z_1, \ldots, z_{s-1}]$ and after multiplying numerator and denominator by the $(p-1)^{\text{st}}$ power of the latter we obtain $b = P/Q$ where $P \in \Omega_0[z_0, z_1, \ldots, z_{s-1}]$, $Q \in \Omega_0[z_1^p, \ldots, z_{s-1}^p]$, $Q \neq 0$. Thus

$$Qz_s' = P'.$$

We write

$$Q = \sum_{u \in \mathbb{N}^{s-1}} A_u z_1^{pu_1} \cdots z_{s-1}^{pu_{s-1}}$$

$$P = \sum_{v} B_v z_0^{v_0} z_1^{v_1} \cdots z_{s-1}^{v_{s-1}}$$

where v runs through $S = \mathbb{F}_p \times \mathbb{N}^{s-1}$ and $A_u, B_v \in \Omega_0$. Thus since $Dz_0 \neq 0$,

$$\frac{1}{z_0 z_1 \cdots z_{s-1}} \sum A_u z_1^{pu_1} \cdots z_{s-1}^{pu_{s-1}}$$

$$= \sum_{v \in S} \sum_{i=0}^{s-1} v_i B_v z_0^{v_0 - 1} z_1^{v_1 - 1} \cdots z_i^{v_i - 1} z_{i+1}^{v_{i+1}} \cdots z_{s-1}^{v_{s-1}}$$

and so for fixed $u \in \mathbb{N}^{s-1}$

$$A_u = \sum v_i B_v$$

the sum being over all $i \in \{0, 1, \ldots, s-1\}$, $v \in S$ such that

$$v_j = pu_j - 1 \quad \text{if} \quad j > i$$

$$v_j = pu_j \qquad \text{if} \quad j \leq i.$$

This shows that $v_i = 0$ in $\mathbb{F}_p$ and hence $Q = 0$, a contradiction.

Proof of 0.2. Let $\xi \in \operatorname{Ker}(D, \mathcal{F}_s)$. Certainly ξ is a ratio of elements of $\mathcal{F}_{s-1}[z_s]$ and hence there exists $\eta \in \mathcal{F}_s$ such that $\xi\eta^p \in \mathcal{F}_{s-1}[z_s]$. Certainly $D(\xi\eta^p) = 0$ and we may assume that $\xi \in \mathcal{F}_{s-1}[z_s]$. Thus we may write

$$(0.2.1) \qquad \xi = \sum_{j=0}^{m} a_j z_s^j \qquad a_j \in \mathcal{F}_{s-1}.$$

We assert

$$(0.2.1.1) \qquad a_j' = 0 \quad 0 \leq j \leq m$$

$$(0.2.1.2) \qquad a_j = 0 \quad \text{if} \quad p \text{ does not divide } j.$$

Indeed differentiating ξ, using the fact that $z_s' \in \mathcal{F}_{s-1}$ and that z_s is transcendental over $\mathcal{F}_{s-1}$, we have

$$(0.2.2) \qquad a_j' + (j+1)a_{j+1}z_s' = 0 \qquad 0 \leq j \leq m$$

where $a_{m+1} = 0$.

Let $j \in [0, m-1]$ be maximal such that $a_j' \neq 0$. Then $(j+1)a_{j+1} \neq 0$ while $a_{j+1} \in \operatorname{Ker}(D, \mathcal{F}_{s-1})$. This shows that $z_s \in -a_j/(j+1)a_{j+1} + \operatorname{Ker}(D, \mathcal{F}_s)$ contrary to (0.1). This demonstrates 0.2.1.1 and so by equation 0.2.2, assertion 0.2.1.2 also holds. Thus for $0 \leq j \leq m$,

$$a_j \in \operatorname{Ker}(D, \mathcal{F}_{s-1}) \in \Omega_0[z_1^p, \ldots, z_s^{p-1}]$$

by induction on s and the assertion now follows from property 0.2.1.2.

PROPOSITION.

$$(0.3)_s \qquad D^{p^{s+1}}\mathcal{F}_s = \{0\}.$$

Proof. The assertion is obvious for $s = 0$. We introduce a further assertion. For $\mu \in [0, p - 1]$

$$(0.3.1)_{s,\mu} \qquad D^{(1+\mu)p^s}(z_s^\mu \mathcal{F}_{s-1}) = \{0\}.$$

Trivially $(0.3)_{s-1}$ implies $(0.3.1)_{s,0}$ while $(0.3.1)_{s,\mu}$ for $\mu = 0, 1, \ldots, p - 1$ implies assertion $(0.3)_s$. We now use induction on μ. Let $y \in \mathcal{F}_{s-1}$ then by Leibnitz

$$(0.3.2) \qquad D^{(1+\mu)p^s}(z_s^\mu y) \in \sum_{i+j=(1+\mu)p^s} D^i(z_s^\mu) D^j y \mathbb{F}_p.$$

By $(0.3)_{s-1}$, $D^j y = 0$ for $j \geqslant p^s$ and so we may assume $j \leqslant p^s - 1$, i.e. $i \geqslant \mu p^s + 1$ in the sum on the right hand side. We observe that by $(0.3.1)_{s,\mu-1}$,

$$D^{\mu p^s + 1} z_s^\mu \in D^{\mu p^s} z_s^{\mu - 1} \mathcal{F}_{s-1} = 0.$$

This completes the proof.

Let $\Omega_s = K(x^p, \ldots, z_s^p)$.

By (0.2) $\Omega_s = \operatorname{Ker}(D, \mathcal{F}^s)$.

0.4. PROPOSITION.

$$\dim_{\Omega_s} \mathcal{F}_s = p^{s+1}.$$

Proof. The chain $\Omega_s \subset \Omega_s(X) \subset \Omega_s(X, z_1) \subset \cdots \subset \cdot\, \Omega_s(x, z_1, \ldots, z_s) = \mathcal{F}_s$ consists of $s + 1$ successive extensions each of degree p.

0.5. Let H be a differential field $L \in H[D]$ and let $H_0 = \operatorname{Ker}(D, H)$. By the theory of the wronskian, if $L \neq 0$ then

$$(0.5.1) \qquad \dim_{H_0} \operatorname{Ker}(L, H) \leqslant \text{order } L.$$

If the maximum value is attained, i.e. if equality holds then we say that L becomes trivial in H.

This is far *stronger* than the assertion that L is a product of elements of $H[D]$ of order unity.

PROPOSITION. *If a product $L = L_1 \circ \cdots \circ L_m$ of elements of $H[D]$ becomes trivial in H then each L_i becomes trivial in H.* (*Note: The converse is false.*)

Proof. The L_i constitute a set of endomorphisms of H as H_0 space. Let n_i = order L_i, $n = \Sigma\, n_i$ = order L. Then $n = \dim_{H_0} \operatorname{Ker}(L, H) \leqslant \Sigma_{i=1}^m \dim_{H_0} \operatorname{Ker}(L_i, H) \leqslant \Sigma\, n_i = n$. Thus we have equality which shows that for each i, $n_i = \dim_{H_0} \operatorname{Ker}(L_i, H)$.

We observe that by (0.3), (0.4), $D^{p^{s+1}}$ becomes trivial in $\mathcal{F}_s$.

Let $\mathcal{R} = \mathcal{F}_0[D]$.

0.6. LEMMA.

0.6.1. $L \in \mathcal{R}$ has nilpotent p-curvature if and only if L becomes trivial in $\mathcal{F}_s$ for some s.

0.6.1.1. Nilpotence is independent of the choice of $D \in \mathcal{D}_{\mathcal{F}_0/\Omega_0}$.

0.6.2. A product $L = L_1 \circ \cdots \circ L_m$ of elements of $\mathcal{R}$ has nilpotent p-curvature if and only if each L_i has nilpotent p-curvature.

0.6.3. If n is the order of L, an operator with nilpotent p-curvature then L is a product of not more than n elements of $\mathcal{R}$ each of which becomes trivial in $\mathcal{F}_0$, $D^{pn} \in \mathcal{R}L$ and L becomes trivial in $\mathcal{F}_s$ if $p^s \geqslant n$.

Proof. If L has nilpotent p-curvature then there exists μ such that $D^{p\mu} \in \mathcal{R}L$ and hence choosing $p^{s+1} \geqslant p\mu$ we have $D^{p^{s+1}} = AL$, $A \in \mathcal{R}$. Since $D^{p^{s+1}}$ becomes trivial in $\mathcal{F}_s$, it follows from 0.5 that L also becomes trivial in $\mathcal{F}_s$.

For the converse part of 0.6.1, since $\mathcal{R}$ is euclidean, $D^{p^{s+1}} = AL + B$ where $A, B \in \mathcal{R}$, order $B <$ order L. Clearly $\operatorname{Ker}(B, \mathcal{F}_s) \supset \operatorname{Ker}(L, \mathcal{F}_s)$, and hence if $B \neq 0$, and if L becomes trivial in $\mathcal{F}_s$ then order $B \geqslant \dim_{\Omega_s} \operatorname{Ker}(B, \mathcal{F}_s) \geqslant \dim_{\Omega_s} \operatorname{Ker}(L, \mathcal{F}_s)$ = order L a contradiction which shows that $B = 0$.

For the proof of 0.6.1.1 we again let $L \in \mathcal{R}$ have nilpotent p-curvature relative to D. Then for some s, L becomes trivial in $\mathcal{F}_s$ relative to D. How does this property depend upon D? Only in that we must check the dimension of $\operatorname{Ker}(L, \mathcal{F}_s)$ as vector space over $\operatorname{Ker}(D, \mathcal{F}_s)$. Thus if $D_\xi = \xi D$ ($\xi \in \mathcal{F}_0$, $\xi \neq 0$) is some other nontrivial element of $\mathcal{D}_{\mathcal{F}_0/\Omega_0}$ then it is enough to check that for D_ξ extended to $\mathcal{F}_s$, $\operatorname{Ker}(D_\xi, \mathcal{F}_s)$ coincides with $\operatorname{Ker}(D, \mathcal{F}_s)$.

For 0.6.2, if L has nilpotent p-curvature then by 0.6.1 L becomes trivial in $\mathcal{F}_s$ for some s and hence by 0.5 each L_i becomes trivial in $\mathcal{F}_s$ and so again by 0.6.1 each L_i has nilpotent p-curvature.

For the converse part of 0.6.2 we may assume that $m = 2$. Thus there exist $A_1, A_2 \in \mathcal{R}$, $\mu_1, \mu_2 \in \mathbb{N}$ such that

(0.6.2.1) $$D^{p\mu_i} = A_i L_i \qquad i = 1, 2.$$

It follows that

(0.6.2.2) $$D^{p(\mu_1+\mu_2)} = D^{p\mu_1} A_2 L_2 = A_2 D^{p\mu_1} L_2$$
$$= A_2 A_1 L_1 L_2$$

which shows that $L_1 L_2$ also has nilpotent p-curvature.

For 0.6.3, let L have nilpotent p-curvature. The assertion is trivial if L is of order zero. Hence we may assume $n \geqslant 1$. Let μ be minimal such that $D^{p\mu} \in \mathcal{R}L$. Certainly $\mu \geqslant 1$. We assert that $1 \notin \mathcal{R}D^p + \mathcal{R}L$, indeed otherwise

(0.6.3.1) $$1 \in \mathcal{R}D^p + \mathcal{R}L.$$

Since D^p lies in the center of $\mathcal{R}$, multiplying on the left by $D^{p(\mu-1)}$ shows that

$$D^{p(\mu-1)} \in \mathcal{R}D^{p\mu} + \mathcal{R}L \subset \mathcal{R}L$$

contradicting the minimality of μ. We conclude that there exists $L_1 \in \mathcal{R}$, order $L_1 \geqslant 1$ such that

(0.6.3.2) $$\mathcal{R}L_1 = \mathcal{R}D^p + \mathcal{R}L.$$

This shows that

(0.6.3.3) $$L = A_1 L_1$$

(0.6.3.4) $$D^p \in \mathcal{R}L_1.$$

The second relation shows that L_1 becomes trivial in $\mathcal{F}_0$. The first relation together with 0.6.2 shows that the operator A_1 also has nilpotent

p-curvature. Applying induction on the order of L we conclude that L has a decomposition

$$L = L_m L_{m-1} \cdots L_1$$

into operators which become trivial in $\mathscr{F}_0$, i.e. $D^p = A_j L_j$ for $1 \leqslant j \leqslant m$. It follows from the calculation 0.6.2.2 that $D^{pm} \in \mathscr{R}L$. Certainly $m \leqslant n$. Thus $D^{pn} \in \mathscr{R}L$ as asserted and hence by 0.6.1 L becomes trivial in $\mathscr{F}_{s+1}$ for each s such that $p^{s+1} \geqslant pn$.

1. Structure of V_N. Let R be a valuation ring with quotient field $\mathscr{F}$ (of characteristic p) which is a differential field with operator D. Let K be the kernel of D in $\mathscr{F}$.

LEMMA 1.1. *Let $\mathscr{L}$ be a monic element of $\mathscr{F}[D]$ of order n. We assume that*

(i) *D is stable on R.*
(ii) *The natural map of $K^\times$ into the value group of $\mathscr{F}$ is surjective.*
(iii) *The kernel of $\mathscr{L}$ in $\mathscr{F}$ is of dimension n as K space, i.e. $\mathscr{L}$ becomes trivial in $\mathscr{F}$ in the sense of* 0.5.

We conclude that $\mathscr{L}$ is a monic element of $R[D]$.

Proof. Let $u \neq 0$ be an element of the kernel of $\mathscr{L}$ in $\mathscr{F}$. By hypothesis we may choose $\alpha \in K$ such that αu is a unit in R. It follows that

$$\mathscr{L} = \mathscr{L}_1 \circ (D - z) \tag{1.1.1}$$

where $z = u'/u = (\alpha u)'/\alpha u \in R$ and $\mathscr{L}_1$ is monic element of $\mathscr{F}[D]$ of order $n - 1$. By (0.5) the operator $\mathscr{L}_1$ becomes trivial in $\mathscr{F}$.

By induction on the order, $\mathscr{L}_1$ is a monic element of $R[D]$ and so the lemma follows from 1.1.(i).

Remark. The lemma remains valid if (iii) is replaced by (iii′) $\mathscr{L}$ is the composition of elements which become trivial in $\mathscr{F}$.

1.2. COROLLARY. *Let $\mathscr{F}_0$, D, Ω_0 be as in Section* 0. *Let L be a monic element of $\mathscr{F}_0[D]$ which has nilpotent p-curvature. Let R_0 be a valuation ring of $\mathscr{F}_0$ with the properties*

(i) *D is stable on R_0.*

(ii) *The natural mapping of $\Omega_0^\times$ into the value group of $\mathcal{F}_0$ is surjective.*

Then L is a monic element of $R_0[D]$.

Proof. This is an immediate consequence of 0.6.2 and the preceding remark.

1.3. Corollary. *Let X be transcendental over the field K of characteristic p. Let $\mathcal{F}_0 = K(X)$, $D = d/dX$, L be a monic element of $\mathfrak{R} = \mathcal{F}_0[D]$ which has nilpotent p-curvature. Let R be any valuation ring of K and let R_0 be its extension to $\mathcal{F}_0$ by the gauss norm relative to X. Then L is a monic element of $R_0[D]$.*

Proof. Certainly the value group of $\mathcal{F}_0$ coincides with the image of K in that group. Stability of R_0 under D is clear. The assertion follows from 1.2.

1.4. Corollary. *Let (γ, v) lie in the algebraic set, V_N defined over $\mathbb{F}_p$ by the nilpotence of the operator L of* I.4 *with given restricted Riemann data. Then v is integral over $\mathbb{F}_p[\gamma]$. (Hence in particular v is algebraic over $\mathbb{F}_p(\gamma)$, and the dimension of V_N is at most $m - 2$.)*

Proof. Let R be any valuation ring of $\mathbb{F}_p(\gamma, v) = K$. Let R_0 be its extension to $\mathcal{F}_0 = K(X)$ by the gauss norm relative to X. By 1.3 A_j/ψ^j lies in R_0 $(1 \leq j \leq n)$. If R contains $\mathbb{F}_p[\gamma]$ then $\psi = \Pi_{i=1}^m (X - \gamma_i) \in R_0$ and so $A_j \in R_0$. Further B_j is the quotient (with remainder $A_{j,0}$) in the division of A_j by ψ, a monic element with coefficients in R and hence B_j lies in R_0. Thus $v_{j,\ell} \in R$ for each R which contains $\mathbb{F}_p[\gamma]$. The assertion follows from a well known theorem in valuation theory (Z.-S. Chapter 6, Section 4, Theorem 6].

The Lamé and Brioschi invariants of Section 6 are illustrations of this corollary.

1.5. Corollary. (Honda). *Let L be as in* 1.3. *Then the singularities of L are fuchsian and the exponents lie in $\mathbb{F}_p$.*

Proof. Let K be replaced by $K(t) = \tilde{K}$ with t, X algebraically independent over K, $Dt = 0$. Let $y = X/t$ and let R be the valuation of $\tilde{K}$ trivial on K such that $|t| < 1$.

Let $L = D^n + A_1 D^{n-1} + \cdots + A_n \in K(X)[D]$, $D = d/dX$. Then relative to $d/dy = tD$, the operator may be written

$$t^n L = \frac{d^n}{dy^n} + tA_1(ty)\frac{d^{n-1}}{dy^{n-1}} + \cdots + t^n A_n(ty).$$

We extend the valuation of $\tilde{K}$ to the valuation $\tilde{R}_0$ of $\tilde{K}(y)$ by the gauss norm relative to y. By 1.3

$$t^j A_j(ty) \in \tilde{R}_0 \qquad 1 \leqslant j \leqslant n.$$

If $X = 0$ is a pole of A_j of order μ then in $K((X))$ we have

$$A_j = X^{-\mu}(\alpha_0 + \alpha_1 X + \cdots), \qquad \alpha_0 \neq 0, \qquad \alpha_i \in K$$

and so

$$t^j A_j(ty) = t^{j-\mu} y^{-\mu}(\alpha_0 + \alpha_1 ty + \cdots)$$

so that

$$1 \geqslant |t^j A_j(ty)| = |t|^{j-\mu}$$

which shows that $j \geqslant \mu$ as asserted.

We now follow Honda's argument to show that the exponents of L lie in $\mathbb{F}_p$. By 0.6.3 $L = L_1 \circ L_2$ where L_1, L_2 are monic, L_1 is nilpotent, L_2 is of order 1 and has a solution in $K(X)$. It follows that χ_{L_2}, the indicial polynomial at zero of L_2, is of first degree with root in $\mathbb{F}_p$ and that $\chi_L(s) = \chi_{L_1}(s - 1)\chi_{L_2}(s)$. The assertion now follows by induction on n.

1.6. We generalize the preceding result.

COROLLARY. *Let X be transcendental over the field k of characteristic p. Let $\mathcal{F}_0 = k((X))$, $D = d/dX$ and let*

$$L = D^n + A_1 D^{n-1} + \cdots + A_n$$

be an element of $\mathcal{F}_0[D]$ with nilpotent p-curvature. Then L satisfies the Fuchs condition at zero, X^jA_j has no pole at $X = 0$ and the exponents at zero lie in $\mathbb{F}_p$.

Proof. Let t be transcendental over $k((X))$. We put $\tilde{k} = k(t)$, a field with valuation trivial on k and with ord $t = 1$. Let $\mathcal{B} = \{\sum a_jX^j \in \tilde{k}[[X]] \mid \inf_j \operatorname{ord}(t^ja_j) > -\infty\}$. Thus $\mathcal{B}$ is the ring of functions analytic and bounded on the disk $|X| > |t|$. The obvious norm

$$\operatorname{ord} \sum_{j=0}^{\infty} a_jX^j = \operatorname*{Inf}_j \operatorname{ord} a_jt^j$$

of $\mathcal{B}$ may be used to define a valuation of the quotient field $\tilde{\mathcal{F}}_0$. We extend the derivation d/dX to $\tilde{\mathcal{F}}_0$ by insisting that $dt/dX = 0$. Trivially $t(d/dX)$ is stable on the valuation ring of $\tilde{\mathcal{F}}_0$ and the value group of $\tilde{\mathcal{F}}_0$ coincides with the natural image of $K(t)^\times \subset \operatorname{Ker}(t(d/dX), \tilde{\mathcal{F}}_0)$. Once again we have

$$t^nL = (tD)^n + tA_1(tD)^{n-1} + \cdots + t^nA_n$$

and so by 1.2 t^jA_j lies in the valuation ring of $\tilde{\mathcal{F}}_0$. If we write

$$A_j = X^{-\mu}(\alpha_0 + \alpha_1X + \cdots), \qquad \alpha_0 \neq 0, \qquad \alpha_i \in k,$$

then

$$0 \leqslant \operatorname{ord} t^jA_j = j - \mu$$

which again demonstrates the Fuchs condition. The exponents lie in $\mathbb{F}_p$ by the argument of 1.5.

2. Second order equations. Part I.

2.1. We recall generalities for n^{th} order equations in characteristic p.

Let $\mathcal{F}$ be a differential field with D as derivation such that D^p annihilates $\mathcal{F}$. Let $G \in \mathcal{M}_n(\mathcal{F})$, the ring of $n \times n$ matrices with coefficients in $\mathcal{F}$. We consider the system

$$(2.1.1) \qquad (D - G)Y = 0.$$

We define recursively $G_0 = I_n$, $G_1 = G$, $G_2, \ldots$ by

$$G_{m+1} = G'_m + G_m G.$$

2.1.2. PROPOSITION. *In a suitable differential extension field* $\mathscr{E}$, G_p *is equivalent to an element of* $\mathcal{M}_n(\operatorname{Ker}(D, \mathscr{E}))$.

Proof. We choose $\mathscr{E}$ so as to contain the coefficients of a solution matrix U of 2.1.1. Thus $DG_sU = G_{s+1}U$. We put $C = U^{-1}G_pU$. We assert $DC = 0$.

$$UDC = U(DU^{-1})G_pU + D(G_pU) = -GG_pU + D^{p+1}U$$

and the assertion follows from

$$D^{p+1}U = D^pDU = D^pGU = GD^pU = GG_pU.$$

2.1.3. COROLLARY. *The characteristic polynomial of G_p has coefficients in $\mathscr{F}$ annihilated by D.*

Of course nilpotence of p-curvature for 2.1.1 is equivalent to the nilpotence of G_p, i.e. to the condition

$$\det(tI - G_p) = t^n.$$

By a routine argument if $w = \det U$, i.e. w is a wronskian of (2.1.1) then

$$D^pw = (\operatorname{Tr} G_p)w. \tag{2.1.4}$$

2.2. Let $\mathscr{F}$ be as in 2.1, $\ell = D^2 + \sigma D + \rho \in R = \mathscr{F}[D]$. For $s \geq 0$ we define $h_s, k_s \in \mathscr{F}$ by the condition

$$D^s \equiv h_sD + k_s \bmod R\ell.$$

The p-curvature matrix G_p of ℓ represents the action of D^p on (u, u') where u is an abstract solution of $\ell u = 0$. Thus

$$G_p = \begin{pmatrix} k_p & h_p \\ k_{p+1} & h_{p+1} \end{pmatrix}. \tag{2.2.1}$$

By 2.1.4 Tr $G_p = 0$ if and only if $D^p w = 0$ where w is the wronskian of ℓ. Thus if σ is the logarithmic derivative of an element of $\mathcal{F}$ then Tr $G_p = 0$ and ℓ has nilpotent p-curvature if and only if det $G_p = 0$.

2.2.2. LEMMA. *Let $p \neq 2$.*

If σ is the logarithmic derivative of a rational function then ℓ is nilpotent if and only if $\Delta = 0$ where

$$\Delta = h_p^2\left(\rho - \frac{\sigma'}{2} - \frac{1}{4}\sigma^2\right) - \frac{1}{4}h_p'^2 + \frac{1}{2}h_p h_p'' \in \ker D.$$

Proof. The recursion relation

$$\begin{pmatrix} h_{s+1} \\ k_{s+1} \end{pmatrix} = \begin{pmatrix} h_s \\ k_s \end{pmatrix}' + \begin{pmatrix} -\sigma & 1 \\ -\rho & 0 \end{pmatrix}\begin{pmatrix} h_s \\ k_s \end{pmatrix} \tag{2.2.2.1}$$

together with the relation

$$0 = \text{Tr } G_p = h_{p+1} + k_p$$

shows that

$$k_p = \frac{1}{2}(\sigma h_p - h_p')$$

and so h_{p+1}, k_{p+1}, k_p can all be computed in terms of h_p. The formula for Δ is simply the calculation of det $G_p = k_p h_{p+1} - h_p k_{p+1}$. By 2.1.3 $\Delta \in \operatorname{Ker} D$.

2.2.3. COROLLARY. *Let w be the wronskian of ℓ, then $\ell_2(wh_p) = 0$ where*

$$\ell_2 = D^3 + 3\sigma D^2 + (\sigma' + 4\rho + 2\sigma^2)D + 2\rho' + 4\sigma\rho$$

is the symmetric square of ℓ.

Proof. For $p \neq 2$, this is a direct consequence of Christol's identity, [Chr2].

$$w\,\frac{d\Delta}{dX} = \frac{1}{2}\,h_p\ell_2(wh_p)$$

which is most easily checked by first considering the case $\sigma = 0$.

If $p = 2$ then $h_p = -\sigma$ and $\ell_2(wh_p) = 0$ by a direct calculation which is simplified by the observation that $D(\sigma' + \sigma^2) = 0$.

2.3. We consider differential polynomials in σ, ρ, i.e. elements of $\mathbb{F}_p[\sigma, \sigma', \sigma'', \ldots, \rho, \rho', \rho'', \ldots]$. A monomial

$$M = \prod \sigma^{(j)^{\ell_j}} \cdot \prod \rho^{(j)^{m_j}}$$

has *weight* and *degree* defined by

$$\text{degree } M = \sum m_j$$

$$\text{weight } M = \sum \ell_j(1 + j) + \sum m_j(2 + j).$$

PROPOSITION 2.3.1. *h_s is a differential polynomial in σ, ρ which is isobaric of weight $s - 1$.*

k_s is isobaric of weight s.

$$\deg(h_p - (-\rho)^{((p-1)/2)}) < \frac{p-1}{2}. \tag{2.3.2}$$

Proof. The first assertion follows by induction from 2.2.2.1. For 2.3.2 we use induction on s for s odd.

3. Second order equations. Part II. We consider equation 0.2.1 in the case of $n = 2$, i.e.

$$L = D^2 + \frac{A_{1,0}}{\psi}\,D + \left(\frac{A_{2,0}}{\psi^2} + \frac{B_2}{\psi}\right) \tag{3.1.1}$$

where $A_{1,0}$, $A_{2,0}$ are polynomials of degree strictly bounded by m and $\deg B_2 \leqslant m - 2$. Let K be the field containing the singularities and the coefficients of these polynomials. Letting

$$\begin{pmatrix} \gamma_1 & \gamma_2 \cdots \gamma_m & \infty \\ e_1 & e_2 \cdots e_m & e_\infty \\ e_1' & e_2' \cdots e_m' & e_\infty' \end{pmatrix}$$

denote the Riemann data, then

$$e_i + e_i' = 1 - \frac{A_{1,0}(\gamma_i)}{\psi'(\gamma_i)} \tag{3.1.1.1}$$

$$e_i e_i' = A_{2,0}(\gamma_i)/\psi'(\gamma_i)^2 \qquad 1 \leqslant i \leqslant m \tag{3.1.1.2}$$

$$e_\infty + e_\infty' = -1 + \left.\frac{A_{1,0}}{X^{m-1}}\right|_{X=\infty} \tag{3.1.1.3}$$

$$e_\infty e_\infty' = \left.\frac{B_2}{X^{m-2}}\right|_{X=\infty} \tag{3.1.1.4}$$

from which the well known condition

$$m - 1 = \sum_{i=1}^{m} (e_i + e_i') + e_\infty + e_\infty' \tag{3.1.2}$$

easily follows. We may write

$$B_2 = e_\infty e_\infty' X^{m-2} + v_0 + v_1 X + \cdots + v_{m-3} X^{m-3} \tag{3.1.3}$$

where $v = (v_0, v_1, \ldots, v_{m-3})$ are the accessary parameters of Klein. Thus $K = \mathbb{F}_p(\gamma_1, \ldots, \gamma_m, v)$. We define $\alpha_s, \beta_s \in K(X)$ by the condition

$$D^s \equiv \alpha_s D + \beta_s \bmod K(X)[D]L. \tag{3.1.4}$$

Thus α_s, β_s in a special case of (h_s, k_s) of **2.2.**

3.2. LEMMA.

3.2.1. The order of pole of α_s (resp: β_s) at γ_i is bounded by $s - 1$ (resp: s).

3.2.2. The order of pole of α_p at γ_i is strictly less than (resp: exactly equal to) $p - 1$ if $e_i \neq -e_i'$ (resp: $e_i = e_i'$).

3.2.3. The order of zero of α_s at ∞ is not less than $s - 1$. The order of zero of β_s at ∞ is not less than s.

3.2.4. The order of zero of α_p at ∞ is strictly greater than (resp: exactly equal to) $p - 1$ if $e_\infty \neq e_\infty'$ (resp: $e_\infty = e_\infty'$).

Proof. We simplify the exposition by putting $\gamma_1 = 0$. The calculation at ∞ is similar. We write

$$(3.2.5)\qquad (\alpha_s, \beta_s) \in \left(\frac{u_s}{X^{s-1}}, \frac{v_s}{X^s}\right) + \left(\frac{1}{X^{s-2}} K[[X]], \frac{1}{X^{s-1}} K[[X]]\right)$$

and use the recursion formula 2.2.2.1 to deduce

$$(3.2.6)\qquad \begin{pmatrix} u_{s+1} \\ v_{s+1} \end{pmatrix} = (M - sI)\begin{pmatrix} u_s \\ v_s \end{pmatrix}$$

where

$$M = \begin{pmatrix} e_1 + e_1' & 1 \\ -e_1e_1' & 0 \end{pmatrix}.$$

Assertion 3.2.1 follows by induction using $(\alpha_0, \beta_0) = (0, 1)$ which shows that $(u_0, v_0) = (0, 1)$.

It is clear that

$$(3.2.7)\qquad \begin{pmatrix} u_p \\ v_p \end{pmatrix} = \prod_{s=0}^{p-1} (M - sI)\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

while by a trivial calculation

$$(3.2.8)\qquad (M - e_1I)(M - e_1'I) = 0.$$

If $e_1 \neq e_1'$ then both factors must occur in the right hand side of 3.2.7 and hence $u_p = 0$.

If $e_1 = e_1'$ then let

$$H = \begin{pmatrix} 1 & 0 \\ -e_1 & 1 \end{pmatrix}, \qquad N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Since

$$MH = H\begin{pmatrix} e_1 & 1 \\ 0 & e_1 \end{pmatrix} = H(e_1 I + N),$$

we have

$$\begin{aligned} H^{-1} \cdot \prod_{s=0}^{p-1} (M - sI) \cdot H &= \prod_{s=0}^{p-1} ((e_1 - s)I + N) \\ &= \prod_{s=0}^{p-1} (e_1 - s)I + \delta N = \delta N \end{aligned}$$

where δ is the $(p - 1)^{\mathrm{st}}$ elementary symmetric function in $\{e_1 - s\}_{s=0,1,\ldots,p-1}$, i.e. in all the elements of $\mathbb{F}_p$. Since

$$X^p - X = \prod_{s=0}^{p-1} (X - s)$$

we have $\delta = -1$ and so if $e_1 = e_1'$,

$$\begin{pmatrix} u_p \\ v_p \end{pmatrix} = -HNH^{-1}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ e_1 \end{pmatrix}.$$

This completes the proof of 3.2.2.

4. Nilpotent p-curvature for $n = 2$. Under the hypotheses of 3, with $e_i, e_i' \in \mathbb{F}_p$ for $i = 1, 2, \ldots, m, \infty$, the condition for nilpotence is given by 2.2.2 if $p \neq 2$. We rewrite this condition putting $H = \psi^{p-1}\alpha_p$,

(4.0.1) $$a = \frac{A_{1,0}}{\psi}$$

$$b = \frac{A_{2,0}}{\psi^2} + \frac{B_2}{\psi} \tag{4.0.2}$$

and replacing Δ by its product with ψ^{2p}. We obtain

$$\Delta = H^2\psi^2\left(b - \frac{1}{2}a' - \frac{1}{4}a^2\right) - \frac{1}{4}(H\psi)'^2 + \frac{1}{2}H\psi(H\psi)''. \tag{4.0.3}$$

Thus Δ lies in Ker D and its vanishing defines the variety of nilpotence V_N if $p \neq 2$.

For $p = 2$ the condition for nilpotence is by 2.2.1

$$\operatorname{Tr} G_2 = a' + a^2 = 0 \tag{4.0.4}$$

$$\operatorname{Det} G_2 = b^2 + (ab)' = 0.$$

In the following lemma, $\nu = (\nu_0, \nu_1, \ldots, \nu_{m-3})$ refers to (3.1.3).

4.1. LEMMA. *Let $p \neq 2$. Then*

$$\Delta \in \mathbb{F}_p[\nu, \gamma, X^p] \tag{4.1.1}$$

$$\Delta \in \psi\mathbb{F}_p(\nu, \gamma)[X] \tag{4.1.2}$$

$$\deg_X \Delta < p(2m - 2) \tag{4.1.3}$$

and hence

$$\Delta = \psi^p\Delta_0(\nu, \gamma, X^p) \tag{4.1.4}$$

where

$$\Delta_0 \in \mathbb{F}_p[\nu, \gamma, X] \tag{4.1.5}$$

$$\deg_X \Delta_0 \leq m - 3. \tag{4.1.6}$$

Proof. By 2.3.1 α_p is isobaric of weight $p - 1$ as differential polynomial in a and b. Equations 4.0.1, 4.0.2 show that

(4.1.7) $$\psi^{1+j}a^{(j)} \in \mathbb{F}_p[\gamma, X]$$

(4.1.8) $$\psi^{2+j}b^{(j)} \in \mathbb{F}_p[\nu, \gamma, X].$$

It follows that $H = \psi^{p-1}\alpha_p \in \mathbb{F}_p[\nu, \gamma, X]$. Furthermore $b - (1/2)a' - (1/4)a^2$ is also isobaric of weight two and hence

(4.1.9) $$\psi^2\left(b - \frac{1}{2}a' - \frac{1}{4}a^2\right) \in \mathbb{F}_p[\nu, \gamma, X].$$

Assertion 4.1.1 is now clear.

We assert that $\Delta = 0$ at $X = \gamma_i$ for $1 \leqslant i \leqslant m$.

Case I. $e_i \neq e_i'$.

By 3.2.2 $H = 0$ at $X = \gamma_i$ and so $H\psi$ has a zero of order two at γ_i. It follows that $(H\psi)'$ and $H\psi(H\psi)''$ both vanish at γ_i. The assertion then follows in this case from 4.1.9.

Case II. $e_i = e_i'$.

In this case H does not vanish but $H\psi(H\psi)''$ does vanish at $X = \gamma_i$. Furthermore we may replace $(H\psi)'^2$ by $H^2\psi'^2$. Thus it is enough to show that

$$g \overset{\text{def}}{=} \psi^2\left(b - \frac{1}{2}a' - \frac{1}{4}a^2\right) - \frac{1}{4}\psi'^2$$

vanishes at $X = \gamma_i$. By 4.0.1, 4.0.2

$$g = \left(B_2 - \frac{1}{2}A_{1,0}'\right)\psi + \psi'^2\left[\frac{A_{2,0}}{\psi'^2} - \frac{1}{4}\left(\frac{A_{1,0}}{\psi'} - 1\right)^2\right].$$

The first term clearly vanishes at $X = \gamma_i$ and by 3.1.1.1, 3.1.1.2 the bracket at $X = \gamma_i$ is the same as $e_ie_i' - (1/4)(e_i + e_i')^2 = 0$ since $e_i = e_i'$. This completes the treatment of Case II and hence of 4.1.2.

To verify 4.1.3 we must again consider two cases.

Case I. $e_\infty \neq e_\infty'$.

By 3.2.4 $\deg_X H \leqslant m(p - 1) - p$ while by 3.1.1 b, a', a^2 all vanish at $X = \infty$ with order at least two. It follows easily from 4.0.3 that $\deg_X \Delta \leqslant 2 \deg H + 2 \deg \psi - 2$ which confirms 4.1.3 in this case.

Case II. $e_\infty = e'_\infty$.

In this case by 3.2.4 $\deg_X H = (p-1)(m-1)$. For this discussion we renormalize H so as to be monic. Thus $\deg_X H\psi = p(m-1)+1$, and so the coefficient of $X^{2p(m-1)}$ in $-(1/4)(H\psi)'^2 + (1/2)H\psi(H\psi)''$ is $-(1/4)$. Since

$$a = (e_\infty + e'_\infty + 1)\frac{1}{X} + O\left(\frac{1}{X^2}\right)$$

$$b = e_\infty e'_\infty \frac{1}{X^2} + O\left(\frac{1}{X^3}\right)$$

we easily compute the coefficient of $X^{2p(m-1)}$ in $H^2\psi^2(b - (1/2)a' - (1/4)a^2)$ to be $e_\infty e'_\infty + (1/2)(e_\infty + e'_\infty + 1) - (1/4)(e_\infty + e'_\infty + 1)^2 = e_\infty e'_\infty + (1/4) - (1/4)(e_\infty + e'_\infty)^2$. The coefficient of $X^{2p(m-1)}$ in Δ is thus $e_\infty e'_\infty - (1/4)(e_\infty + e'_\infty)^2 = 0$ since $e_\infty = e'_\infty$. This completes the discussion of Case II and hence of 4.1.3.

Assertions 4.1.4–4.1.6 now follow from the fact that ψ is monic as polynomial in X and that Δ lies in the kernel of D.

4.2. COROLLARY.

4.2.1. V_N is a complete intersection defined by the vanishing of $m-2$ polynomials

$$v_j^p = g_j(\gamma, v) \qquad 0 \leq j \leq m-3$$

$$g_j \in \mathbb{F}_p[\gamma, v]$$

$$\deg_v g_j \leq p-1.$$

4.2.2. For fixed γ, V_N is a finite set with cardinality (counting multiplicities) p^{m-2}. (Finiteness also follows from 1.4.)

4.2.3. For fixed γ, the cardinality of V_0, the variety of zero p-curvature, is at most $((p-1)/2)^{m-2}$ (resp: 1), if $p \neq 2$ (resp: $p = 2$). Each point of V_0 occurs in V_N with multiplicity at least two (if $p \neq 2$).

Proof. Case I. $p \neq 2$.

Let

$$\chi(\nu, X) = \sum_{i=0}^{m-3} \nu_i X^i.$$

By 2.3.2 the leading form of α_p relative to ν is $\pm(\chi(\nu, X)/\psi)^{(p-1)/2}$. Thus $\deg_V H = (p - 1)/2$ and so ν appears in $((H\psi)'^2$, in $H\psi(H\psi)''$ and in $H^2\psi^2(-(1/2)a' - (1/4)a^2)$ at most to the power $p - 1$. But the leading form of b relative to ν is $\chi(\nu, X)/\psi$. Thus the leading form of Δ relative to ν is $\chi^p\psi^p$. Thus by 4.1 the leading form of Δ_0 relative to ν is $\chi(\nu^p, X)$. Thus we may write

$$\Delta_0 = \sum_{j=0}^{m-3} (\nu_j^p - g_j(\gamma, \nu))X^j$$

where $g_j \in \mathbb{F}_p[\gamma, \nu]$, $\deg_\nu g_j \leq p - 1$. This completes the proof of 4.2.1 and 4.2.2 follows by setting $K_0 = \mathbb{F}_p(\gamma)$, $R = K_0[\nu]$, $\mathfrak{A} = \Sigma_{j=0}^{m-3} (\nu_j^p - g_j)R$ and observing that the ring $R/\mathfrak{A}$ has exactly p^{m-2} elements.

The variety V_0 is defined by the vanishing of H as polynomial in X. The leading form of α_p shows that V_0 is defined by elements of $K_0[\nu]$, $(h_1, \ldots, h_\ell)$ of degree bounded by $(p - 1)/2$. On the other hand V_0 being a subset of V_N must be finite. We may reorder the h_i so that $\{h_1, \ldots, h_{m-2}\}$ defines an algebraic set of dimension zero which contains V_0. The upper bound on card V_0 is now clear. By 4.0.3 each zero of H provides a double zero of Δ. Thus each point of V_0 appears at least twice in computing the cardinality of V_N.

Case II. $p = 2$.

We may assume that all e_i, $e_i' \in \mathbb{F}_2$ and that 3.1.2 is satisfied. Thus

$$a = \frac{A_{1,0}}{\psi} = \sum_{i=1}^{m} \frac{1 + e_i + e_i'}{X - \gamma_i}$$

certainly satisfies the condition $a' + a^2 = 0$. To make the second condition of 4.0.4 explicit we write $B_2 = \beta X^{m-2} + \chi(\nu, X)$ where χ is as in Case I and $\beta = e_\infty e_\infty'$. The second condition may be written

$$\chi^2 + (A_{1,0}\chi)' = \beta^2 X^{2(m-2)} + \beta(X^{m-2}A_{1,0})' + \frac{A_{2,0}^2}{\psi^2} + \left(\frac{A_{1,0}A_{2,0}}{\psi}\right)'. \tag{4.3.1}$$

It is clear that $(A_{1,0}\chi)'$ is a polynomial in X^2 whose degree in X is bounded by $2(m-3)$. It follows from 3.1.1.1, 3.1.1.2 that the right side of (4.3.1) is a polynomial and by 3.1.1.3 the leading term of $A_{1,0}$ is $(1 + e_\infty + e'_\infty)X^{m-1}$. If $\beta \neq 0$ then $\beta + 1 + e_\infty + e'_\infty = 0$. It follows that the right side of 4.3.1 is also a polynomial in X^2 whose degree in X is bounded by $2(m-3)$.Thus 4.2.1 holds in the case of $p = 2$.

Since $D^2 \equiv -b - aD \bmod L$, zero p-curvature implies $a = b = 0$. This completes the treatment of the case $p = 2$.

5. Lamé equation (characteristic zero). [Po, W.W., BA-1]. The object of this section is to recall some classical constructions associated with this differential equation. In the next section this will be related to the varieties V_N and V_0 in characteristic p. The operator is

$$L_n = D^2 + \frac{1}{2}\frac{f'}{f}D - \frac{n(n+1)X + B}{f} \tag{5.0.1}$$

where

$$f(X) = 4(X - e_1)(X - e_2)(X - e_3), \qquad e_1 + e_2 + e_3 = 0$$

$$= 4X^3 - g_2X - g_3$$

and e_1, e_2, e_3 are distinct. Here B is the accessory parameter and the Riemann data is

$$\begin{pmatrix} e_1 & e_2 & e_3 & \infty \\ 0 & 0 & 0 & -n/2 \\ 1/2 & 1/2 & 1/2 & (n+1)/2 \end{pmatrix}$$

We restrict our attention to the case in which $2n \in \mathbb{Z}$. Since L_n is invariant under $n \to -1 - n$, we may assume that $n \geqslant -1/2$.

5.1. $n \in \mathbb{Z}$.

We may assume $n \geqslant 0$. The symmetric square of L_n is given by

$$(5.1.1)\quad (L_n)_2 = fD^3 + \frac{3}{2}f'D^2 + \frac{1}{2}f''D - 4\{n(n+1)X + B\}D - 2n(n+1).$$

The following result is well known [W.W., Po].

LEMMA. (Hermite). *There exists $\theta_n \in (1/2)_n(2n)!)^{-1}\mathbb{Z}[1/2, e, B, X]$ of degree n separately in X and in B and monic in X such that $(L_n)_2\theta_n =$ 0.*

Proof. (We refer to θ_n as the Hermite polynomial.) The coefficient of D^j in $(L_n)_2$ is a polynomial in $\tau = X - e_2$ of degree j $(0 \leqslant j \leqslant 3)$ and the coefficient of D^3 is divisible by τ. Hence for arbitrary s we have

$$(5.1.2)\quad (L_n)_2\tau^s = \phi_0(s-2)\tau^{s-2} + \phi_1(s-1)\tau^{s-1} + \phi_2(s)\tau^s$$

where

$$(5.1.2.1)\quad \phi_0(s) = f'(e_2)(s+1)\left(s+\frac{3}{2}\right)(s+2)$$

$$(5.1.2.2)\quad \phi_1(s) = -4(s+1)e_2[-3(s+1)^2 + n(n+1) + Be_2^{-1}]$$

$$(5.1.2.3)\quad \phi_2(s) = 4\left(s+\frac{1}{2}\right)(s-n)(s+n+1).$$

We observe that

$$(5.1.3.1)\quad \phi_0(s) = -\phi_0(-3-s)$$

$$(5.1.3.2)\quad \phi_1(s) = -\phi_1(-2-s)$$

$$(5.1.3.3)\quad \phi_2(s) = -\phi_2(-1-s).$$

5.1.4. *Remark.* The verification of 5.1.2 is facilitated by observing that the exponents of e_2 of $(L_n)_2$ are 0, 1/2, 1 and these must be the zeros of $s \to \phi_0(s - 2)$. The exponents at ∞ are $-n$, 1/2, $n + 1$ and these must be the zeros of $s \to \phi_2(-s)$. This fixes ϕ_0, ϕ_2 up to factors independent of s. These factors may be computed from the values of $\phi_0(0)$, $\phi_2(0)$ which are given by

$$(5.1.4.1) \qquad -2n(n + 1) = (L_n)_2(1)$$

$$= \phi_0(-2)\tau^{-2} + \phi_1(-1)\tau^{-1} + \phi_2(0)$$

$$(5.1.4.2) \qquad 3f'(e_2) = (L_n)_2\tau^2\big|_{\tau=0} = \phi_0(0).$$

From 5.1.4.1 we deduce $\phi_1(-1) = 0$, while by differentiating 5.1.2 with respect to B,

$$-4s = \frac{d\phi_1}{dB}(s - 1).$$

This shows that

$$-\phi_1(s) = (s + 1)[4B + \phi_{11}(s)]$$

where ϕ_{11} is independent of B and a quadratic in s. Its determination can be carried out by computing $\phi_1(s)$ for $s = 0, 1, 2$.

We continue with the proof of the lemma. We use the vanishing of $\phi_0(-2)$, $\phi_1(-1)$, $\phi_0(-1)$ to conclude that $(L_n)_2$ is stable on polynomials in τ and in particular on the span $\langle 1, \tau, \ldots, \tau^n \rangle$. The matrix of $(L_n)_2$ on this space is the lower triangular $(n + 1) \times (n + 1)$ matrix

(5.1.5)

$$M_1 = \begin{pmatrix} \phi_2(0) & 0 & 0 & & \\ \phi_1(0) & \phi_2(1) & 0 & & \\ \phi_0(0) & \phi_1(1) & \phi_2(2) & & \\ & & & & \phi_0(n - 2), \phi_1(n - 1), \phi_2(n) \end{pmatrix}$$

whose diagonal elements are $\phi_2(0), \phi_2(1), \ldots, \phi_2(n)$ which are all nonzero except for $\phi_2(n) = 0$. Thus the rank is n and so up to a constant factor there exists exactly one polynomial of degree n,

$$\theta_n(B, e, X) = \sum_{j=0}^{n} c_{n-j}\tau^j, \qquad c_0 = 1 \tag{5.1.6}$$

which lies in the kernel. Here

$$(c_n, c_{n-1}, \ldots, c_0)M_1 = 0 \tag{5.1.7}$$

and computing the c_j recursively involves division by $\phi_2(n-1)$, $\phi_2(n-2), \ldots, \phi_2(0)$. The lemma follows by computing the product of these factors.

5.2. Corollary. *In the notation of the preceding lemma, let*

$$\Delta_n(e, B) = f'(e_2)c_{n-1}c_n - 4(B + n(n+1)e_2)c_n^2 \tag{5.2.1}$$

an element of $((1/2)_n(2n)!)^{-2}\mathbb{Z}[1/2, e, B]$ *of degree* $2n+1$ *relative to* B. *Then* $\sqrt{\theta_n}$ *is a solution of* L_n *if and only if* $\Delta_n(e, B) = 0$.

We refer to Δ_n as the *Lamé invariant.*

Proof. We use the formula of Fuchs [Ba-Dw (0.6)]. Let y_1, y_2 be solutions of L_n such that $y_1y_2 = \theta_n$. Let $w = y_1y_2' - y_2y_1'$ and let $w_0 = 1/\sqrt{f}$ a particular solution of the wronskian equation of L_n. Then (ignoring (5.2.1))

$$\Delta_n(B, e) \overset{\text{def}}{=} -\left(\frac{w}{w_0}\right)^2 \tag{5.2.2}$$

$$= f\theta_n^2\left[\left(\frac{\theta_n'}{\theta_n}\right)^2 + 2\left(\frac{\theta_n'}{\theta_n}\right)' + \left(\frac{\theta_n'}{\theta_n}\right)\frac{f'}{f} - 4\,\frac{n(n+1)X + B}{f}\right].$$

Trivially Δ_n is independent of x and hence may be computed by setting $X = e_2$. By use of $\theta_n(e_2) = c_n$, $\theta_n'(e_2) = c_{n-1}$ we deduce formula (5.2.1) for Δ_n. Trivially the vanishing of w is the criterion for θ_n being the square of a solution of L_n.

5.2.3. *Remark.* It is known [W.W., 23.41] that Δ_n as polynomial in B with coefficients in $\mathbb{C}(e)$ has no repeated roots.

5.2.4. It has been shown by Baldassarri [BA1] that if $\Delta_n(B) = 0$ then the monodromy group $L_{n,B}$ cannot be finite. In an otherwise important article (cf. 7.3.2 below) [Ch, Thm. 7.2] the Chudnovsky's assert without proof that this holds in any case without any hypothesis on $\Delta_n(B)$. A counter example has been given by Baldassarri [Ba2] $n = 1$, $B = 0$, $g_2 = 0$ whose monodromy group is dihedral of order 6 being the weak pullback by $\xi(x) = 1 - 4x^3/g_3$ of the hypergeometric equation whose exponent differences at 0, 1, ∞ are 1/2, 1/3, 1/2.

This counter example also disproved our own conjecture [Dw1] that $L_{n,B}$ is globally nilpotent only if $\Delta_n(B) = 0$.

5.2.5. The example of Baldassarri may also be investigated by writing $L_{n,B}$ in the form

$$L_{n,B} = -g_3D^2 - g_2\left(XD^2 + \frac{1}{2}D\right) - B$$
$$+ [4X^3D^2 + 6X^2D - n(n+1)X]$$

so that solutions at $X = 0$ involve a four term recursion formula but if $B = 0$ and either g_2 or g_3 vanish then the recursion formula involves only two terms and the equation may be reduced to the hypergeometric equation and finite monodromy determined from the Schwarz list.

5.3. We now consider the case in which n is a half integer $n = \ell - 1/2$, $\ell \in \mathbb{N}$.

We again put $\tau = X - e_2$ and consider

$$\Phi = \tau^{1/2} \circ (L_n)_2 \circ \tau^{1/2}$$

as operator on $K((\tau))$ where $K = \mathbb{Q}(e, B)$. We rewrite 5.1.2 in the form

$$\text{(5.3.1)} \quad \Phi\tau^s = \phi_0\left(s - \frac{3}{2}\right)\tau^{s-1} + \phi_1\left(s - \frac{1}{2}\right)\tau^s + \phi_2\left(s + \frac{1}{2}\right)\tau^{s+1}.$$

5.3.2. Proposition.

5.3.2.1. Φ is stable on $K[[\tau]]$ and on $\tau^{-1}K[[\tau^{-1}]]$.

5.3.2.2. If we write

$$\Phi\tau^s = \sum_{t=0}^{\infty} C_{s,t}\tau^t$$

then

$$-\Phi\tau^{-1-s} = \sum C_{t,s}\tau^{-1-t}.$$

5.3.2.3. Φ is stable on the K span of $1, \tau, \ldots, \tau^{\ell-1}$.

Proof. Stability on $K[[\tau]]$ (resp: $\tau^{-1}K[[-\tau]]$) follows from $\phi_0(-3/2) = 0$ (resp: $\phi_2(-1/2) = 0$).

Assertion 5.3.2.2 follows from 5.1.3.1–5.1.3.2.

Assertion 5.3.2.3 follows from $\phi_2(\ell - 1/2) = \phi_2(n) = 0$. This completes the proof of the proposition.

The matrix M of the action of Φ on the span of $1, \tau \ldots, \tau^{\ell-1}$ is

$$M = \begin{pmatrix} \phi_1\left(-\frac{1}{2}\right) & \phi_2\left(\frac{1}{2}\right) & 0 & & \\ \phi_0\left(-\frac{1}{2}\right) & \phi_1\left(\frac{1}{2}\right) & \phi_2\left(\frac{3}{2}\right) & & \\ & & & & \phi_2\left(\ell-\frac{3}{2}\right) \\ & & & \phi_0\left(\ell-\frac{5}{2}\right) & \phi_1\left(\ell-\frac{3}{2}\right) \end{pmatrix}.$$

We define the Brioschi invariant

$$h_n(e, B) = \det M. \tag{5.3.3}$$

It is clear that $h \in \mathbb{Z}[1/2, e, B]$, $\deg_B h = \ell$.

5.3.4. Lemma.

5.3.4.1. The algebraic set $h_n(e, B) = 0$ is invariant under permutation of (e_1, e_2, e_3).

5.3.4.2. The monodromy group of L_n is finite if and only if $h_n(e, B) = 0$.

Proof. In the following sketch we omit explanations of rings of definition and of reduction modulo p.

We restrict our attention to primes $p \geqslant 2\ell + 1$. The vanishing of $\phi_0(-2)$, $\phi_0(-1)$, $\phi_1(-1)$ shows that $(L_n)_2$ is stable on the span of $1, \tau, \ldots, \tau^{p-1}$ and hence $t^{-(p+1)/2} \circ (L_n)_2 \circ \tau^{(p+1)/2}$ is stable on the span of $\tau^{-(p+1)/2}, \tau^{-(p-1)/2}, \ldots, \tau^{(p-3)/2}$. Reducing mod p we conclude that $\tau^{-1} \circ \Phi$ is stable on this space with matrix which is lower triangular and with $\phi_2(1/2 + j)$, $-(p + 1)/2 \leqslant j \leqslant (p - 3)/2$ as the diagonal elements. These diagonal elements are zero for precisely 3 values of j, $j = -\ell - 1, -1, \ell - 1$.

The restriction of $\tau^{-1}\Phi$ to this space has the following $p \times p$ matrix in which asterisks indicate nonzero elements lying on the diagonal. Here $\tilde{M}$ is the image of M under reflection about the skew diagonal of M_2 perpendicular to the main one.

$$M_2 = \begin{pmatrix} \ddots &&&&&&&&&& \\ & * &&&&&&&&& \\ && * &&&&&&&& \\ &&& 0 &&&&&&& \\ &&&& \boxed{-\tilde{M}} &&&&&& \\ &&&&& 0 &&&&& \\ &&&&&& \boxed{M} &&&& \\ &&&&&&& 0 &&& \\ &&&&&&&& * && \\ &&&&&&&&& * & \\ &&&&&&&&&& \ddots \end{pmatrix}$$

(Note that M and M are not lower triangular but there is no contradiction as the main diagonal of M is offset from that of M_2). Multiplying by a row reducing matrix on the left we may remove all elements lying below the asterisks in the upper left (including those not shown in $\tilde{M}$) and multiplying on the right by a column reducing matrix we may remove all entries to the left of the asterisks in the lower right (including those not shown in M).

We conclude that the rank is $p - 1$ unless det M vanishes, i.e. $h_n(B, e) \bmod p$ vanishes, in which case the rank is $p - 3$. This is precisely the condition then that $(L_n)_2 \bmod p$ has three rational solutions and this then is the condition that L_n mod p have zero p-curvature. This last condition is invariant under permutation of e_1, e_2, e_3 and so the algebraic sets $h_n(e_1, e_2, e_3, B) = 0$, $h_n(e_2, e_1, e_3, B) = 0$ have the same reduction mod p for all $p \geqslant 2\ell + 1$. We conclude that the two algebraic sets must coincide in characteristic zero. This completes the proof of 5.3.4.1.

If L_n has finite monodromy then by the trivial part of the Grothendieck conjecture, L_n has zero p-curvature for almost all p and hence by the preceding analysis $h_n(e, B) \equiv 0$ for almost all p which shows that $h_n(e, B) = 0$ in characteristic zero. This completes the proof of 5.3.4.2 in one direction.

Conversely if $h_n(e, B) = 0$ then by 5.3.2.2 and the definition of M, $(L_n)_2$ has a nontrivial algebraic solution $u_2 = z_2\sqrt{x - e_2}$ where z_2 is a polynomial of degree $\ell - 1$. By 5.3.4.1 we may interchange e_1 and e_2 and obtain a solution $u_1 = z_1\sqrt{x - e_1}$, where z_1 is again a polynomial. Clearly u_1, u_2 are linearly independent over K. Let v_1, v_2 be independent solutions of L_n in some differential extension field. Then

$$u_1 = Q_1(v_1, v_2)$$

$$u_2 = Q_2(v_1, v_2)$$

where Q_1, Q_2 are quadratic forms with constant coefficients. Thus v_1, v_2 are algebraic over $C(u_1, u_2)$ for some constant field C. The finiteness of monodromy is now clear.

5.3.5. Corollary. *If $p \geqslant 2\ell + 1$ and if L_n* mod *p is well defined then the reduction has zero p-curvature if and only if $h_n(e, B) \equiv 0$ modulo p.*

5.3.6. We are indebted to F. Baldassarri for the methods used in this section. Previous treatments of L_n with n a half integer (Bal, Po, Cr] have all been based upon the Halphen transform, a process which is avoided here.

We show that our $h_{\hat{n}}$ coincides with the polynomial P_n appearing in the proof of [Ba1, Theorem 2.6], (which in turn coincides with [Po, p. 164, equation 21]. Crawford has shown [Cr] by Sturms theorem that for e_1, e_2 real, the polynomial P_n has ℓ distinct roots for B. It follows that P_n has no multiple factors as monic polynomial in B with coefficients in $\mathbb{C}[e_1, e_2]$. Our assertion now follows from the fact that h_n and P_n have the same degree as polynomial in B and define the same algebraic set.

6. Lamé equation (characteristic $p \neq 2$). Let $n \in \mathbb{F}_p$. We consider L_n given by 5.0.1 but now with f in characteristic p. We choose $\bar{n} \in [0, (p - 1)/2]$ such that the image of $\bar{n}$ in $\mathbb{F}_p$ coincides with either n or $-1 - n$. We define

$$\hat{n} = \frac{p-1}{2} - \bar{n} - \frac{1}{2} \equiv -1 - \bar{n} \bmod p.$$

We use the results of Section 5 to compute the α_p associated with L_n by 3.1.4.

In particular we define $\theta_{\bar{n}}(B, e, X)$, $\Delta_{\bar{n}}(B, E)$, $h_{\hat{n}}(B, e)$ by reducing mod p the corresponding formulae of Section 5. The main point here is that p does not divide $(1/2)_{\bar{n}}(2\bar{n})!$ in $\mathbb{Z}[1/2]$.

We choose $w_0 = f^{(p-1)/2}$, a solution in characteristic p of the wronskian equation of L_n. By (2.2.3)

$$(L_n)_2 w_0 \alpha_p = 0. \tag{6.1}$$

6.2. Lemma.

$$w_0 \alpha_p = \tilde{h}_n(B, e)\theta_{\bar{n}}(B, e, X)$$

where $\tilde{h}_{\hat{n}} \in \mathbb{F}_p[B, e]$ defines the same algebraic set as $h_{\hat{n}}$ and has the same degree in B.

Proof. If $\alpha_p = 0$ then L_n has zero p-curvature and since $p \geqslant 2(\hat{n} + 1/2) + 1$ we conclude from 5.3.5 that $h_n(B, e) = 0$ and so the assertion is trivial in this case.

If $\alpha_p \neq 0$ then $\phi_n \stackrel{\text{def}}{=} w_0\alpha_p$ and $\theta_{\bar{n}}$ are nontrivial solutions of $(L_{n,B})_2$. They cannot be linearly independent over the kernel of D as otherwise by an argument used in the proof of 5.3.4.2, $L_{n,B}$ would have zero p-curvature contrary to hypothesis. Thus $\phi_n/\theta_{\bar{n}}$ lies in the kernel of D. By 3.2.2 the order of pole of α_p at e_i is bounded by $p - 2$ and so that of ϕ_n is bounded by $(p - 2) - (p - 1)/2 < (p - 1)/2$. The exponents at e_i show the order of pole is congruent mod p to either $0, p - 1$, or $(p - 1)/2$. Thus ϕ_n has no pole at e_i and hence is a polynomial in X. It follows that $\phi_n \in \mathbb{F}_p[B, e, X]$.

The degrees of $\theta_{\bar{n}}$ and of ϕ_n are both bounded by $p - 1$ since by 5.1 $\deg_X \theta_{\bar{n}} = \bar{n}$ while by 3.2.3 $\deg_X \phi_n \leqslant (3/2)(p - 1) - (p - 1) \leqslant (p - 1)/2$. This shows that $\phi_n/\theta_{\bar{n}}$ is independent of X. Since $\theta_{\bar{n}}$ is monic in X, the quotient is the leading coefficient of ϕ_n: an element of $\mathbb{F}_p[B, e]$ which we designate as $\tilde{h}_n$ and hence the algebraic set defined by $\tilde{h}_n$ coincides with the set defined by h_n.

The leading form (relative to B) of ϕ_n is by 2.3.2 equal to $\pm f^{(p-1)/2}(B/f)^{(p-1)/2} = \pm B^{(p-1)/2}$ and so the degree in B of $\tilde{h}_n$ is $(p - 1)/2 - \deg_B \theta_{\bar{n}}$. (Alternatively in the notation of 5.1.7 $\tilde{h}_{\hat{n}} c_{\bar{n}} = \phi_n|_{T=0}$ a polynomial in B of degree $(p - 1)/2$). We conclude that $\deg_B \tilde{h}_{\hat{n}} = (p - 1)/2 - \bar{n} = \hat{n} + 1/2 = \deg_B h_{\hat{n}}$. This completes the proof of the lemma.

Using 6.2 it is easy to check that

$$\alpha_p^2\left(b - \frac{a'}{2} - \frac{1}{4}a^2\right) - \frac{1}{4}(\alpha_p')^2 + \frac{1}{2}\alpha_p\alpha_p''$$

$$= \tilde{h}_n^2\theta_n{}^2 w_0\left[\left(\frac{\theta_{\bar{n}}'}{\theta_{\bar{n}}}\right)^2 + 2\left(\frac{\theta_{\bar{n}}'}{\theta_{\bar{n}}}\right)' - 2\frac{w_0'}{w_0}\frac{\theta_{\bar{n}}'}{\theta_{\bar{n}}} + 4b\right]\Big/4$$

where $L_n = D^2 + aD + b$. Thus the invariant Δ of 2.2.2 may be written (after dropping the trivial factor f^p)

$$4\Delta = \tilde{h}_{\hat{n}}^2\Delta_{\bar{n}}(B, e)$$

in terms of the Lamé invariant (5.2.2). Here we have

$$\deg_B \Delta = p$$

$$\deg_B \Delta_{\bar{n}} = 2\bar{n} + 1$$

$$\deg \tilde{h}_{\hat{n}}^2 = 2\left(\hat{n} + \frac{1}{2}\right) = p - 1 - 2\bar{n}.$$

Thus for fixed e, the variety of nilpotence, $\Delta = 0$, has p points of which $\hat{n} + 1/2$ involve zero p-curvature and are counted twice.

7. Global nilpotence. We consider the family of n^{th} order differential equations in characteristic zero with given restricted Riemann data. For application to questions of global nilpotence we may [Ka] insist that the singularities are all fuchsian and that the exponents lie in $\mathbb{Q}$. Letting $m + 1$ be the number of singular points, one at infinity, the description of I.4 holds again and we may use (γ, ν) to designate an element of the moduli space in characteristic zero.

Let $\mathcal{V}_{\text{global}}$ be the set of all (γ, ν) algebraic over $\mathbb{Q}$ such that for almost all primes $\mathfrak{p}$ of $\mathbb{Q}(\gamma, \nu)$, the reduction mod $\mathfrak{p}$ of $L_{\gamma,\nu}$ has nilpotent p-curvature.

Let V be an algebraic subset (defined over an algebraic number field, K) of the moduli space. We consider three types of such subsets.

Type I. We say that V is of type I if each algebraic point of V lies in $\mathcal{V}_0$.

Type II. We say that V is of type II if there exists a finite set S of primes of K such that for each point (γ, ν) of V algebraic over K and for each prime $\mathfrak{p}$ of $K(\gamma, \nu)$ excluding

(a) primes above S
(b) primes at which (γ, ν) is not integral
(c) primes at which the reduction of γ does not consist of m distinct elements

we may conclude that the reduction modulo $\mathfrak{p}$ of $L_{\gamma,\nu}$ has nilpotent p-curvature.

Type III. We say that V is of type III if there exists a finite set, S of primes of K, such that for each $\mathfrak{p}$ not in S the reduced variety $V_{\mathfrak{p}}$ lies in V_N, the algebraic set associated with the reduction mod p of the given restricted Riemann data.

In 7.5.2 we give an example in which $\mathcal{V}_{\text{global}}$ is an algebraic set. We do not know that this is true in general. For algebraic sets of type I we have no effective method for determining the set of "bad" primes for each point. We believe that types II and III are the same.

If (γ, ν) is a generic point of an irreducible subvariety of the moduli space of type III then ν is algebraic over $K(\gamma)$ since for almost all primes $\mathfrak{p}$ of K the dimension of V is the same as that of $V_\mathfrak{p}$ the mod $\mathfrak{p}$ reduction of V. The assertion then follows from Corollary 1.4.

That corollary as well as the examples of the Lamé and Brioschi invariants of Section 5 suggest that for type III, ν is integral over $\mathbb{Z}[N^{-1}, \gamma]$ for suitable $N \in \mathbb{N}$. This is certainly the case if $K[\gamma]$ is a unique factorization domain. Let $0 = A_0 z^\ell + \cdots + A_1$ be the irreducible polynomial satisfied by one of the components of ν over $\mathbb{Z}[\gamma]$. It is enough to show $A_j/A_0 \in K[\gamma]$ for $1 \leqslant j \leqslant \ell$. Let $\gamma_1, \ldots, \gamma_r$ be a transcendence basis of $K(\gamma)$ over K. Each finite prime $\mathfrak{p}$ of K may be extended to $K(\gamma_1, \ldots, \gamma_r)$ by the gauss norm and then extended in a finite number of ways to the galois closure of $K(\gamma, \nu)$ over $K(\gamma_1, \ldots, \gamma_r)$. For almost all such extensions the reduction, $(\bar{\gamma}, \bar{\nu})$, lies in V_N and hence by Corollary 1.4 the reduction of z and of its conjugates are integral over $\mathbb{F}_p[\bar{\gamma}]$. Thus $\bar{A}_j \in \bar{A}_0 \mathbb{F}_p[\bar{\gamma}]$. Thus the variety $A_0 \equiv 0 \bmod \mathfrak{p}$ lies in the variety $A_j \equiv 0 \bmod \mathfrak{p}$ for almost all $\mathfrak{p}$ and so the same holds in characteristic zero. By the null stellensatz $A_j^\nu \in K[\gamma]A_0$ for some ν. By unique factorization each irreducible factor of A_0 divides A_j in $K[\gamma]$.

We are indebted to Christol [Chr2] for bringing this type of result to our attention.

7.2. An example of a type III subvariety of the moduli space is given in the case $n = 2$ by the problem of determining all $L_{\gamma,\nu}$ with given restricted Riemann data and a fixed finite projective monodromy group. It follows from Klein (cf. [Bu-Dw]) that the set of all such (γ, ν) constitutes an algebraic set defined over $\mathbb{Q}$.

The Brioschi invariant 5.3.5 is monic in B with coefficients in $\mathbb{Z}[1/2, e]$. The vanishing of this invariant is equivalent to the assertion that the Lamé equation $L_{n,e,B}$ (with fixed $n \in 1/2 + \mathbb{Z}$) have the Vierer group as projective monodromy group.

7.3. A very important example of a type III variety is provided by the variation of cohomology of an algebraic variety depending upon two parameters Γ, λ. Viewing periods as functions of Γ with λ as a parameter, we obtain a system of linear differential equations parametrized by λ which is of type III. An elementary description of such a situation may be found in [Dw1, Section 2.4.1].

7.4. For $n = 2$ we formulate a conjecture concerning $\mathcal{V}_{\text{global}}$.

CONJECTURE. *Let K be an algebraic number field and let L be an element of $K(t)[d/dt]$ of second order which is globally nilpotent. Then L has an algebraic wronskian and either*

7.4.1. *L has a solution which is the radical of a rational function.*

7.4.2. *L is obtained from a hypergeometric equation with rational exponents*

$$\mathcal{L} = X(1 - X)\frac{d^2}{dX^2} + (c - (a + b + 1)X)\frac{d}{dX} - ab$$

by an algebraic transformation $X = \phi(t)$ of the independent variable and a transformation

$$y = A(t)\frac{dz}{dt} + B(t)z \tag{7.4.4.1}$$

of the dependent variable where A, B are algebraic functions.

7.5. This conjecture is known in three cases.

7.5.1. If the monodromy group of L is finite, the result follows from Klein's theorem [Ba-Dw].

Note. In this case we may take $A = 0$ in 7.2.2.1 and B is needed only to adjust the wronskian. However this cannot hold in general. If y and z are contiguous ${}_2F_1$ with infinite monodromy groups, then relation 7.4.4.1 will hold but A need not be zero.

7.5.2. For the Lamé equation $L_{n,B}$, (5.0.1) with $n \in \mathbb{Z}$ the conjecture is known. Trivially $L_{n,B}$ is globally nilpotent if and only if either $\Delta_n(B) = 0$ or $L_{n,B}$ has globally zero p-curvature. The first case is covered by 7.4.1. In the second case (for $n \in \mathbb{Z}$) the Grothendieck conjecture has been proven by the Chudnovsky's [Ch] and hence the monodromy group is finite. Thus we reduce to 7.5.1.

7.5.3. Apery has given three examples of globally nilpotent second order differential equations

$$L_1 = (X - 11X^2 - X^3)D^2 + (1 - 22X - 3X^2)D - (3 + X)$$

$$L_2 = X(8X - 1)(X + 1)D^2 + (24X^2 + 14X - 1)D + (8X + 2)$$

$$L_4 = X(1 - 34X + X^2)D^2 + (1 - 51X + 2X^2)D + \frac{X - 10}{4}.$$

These equations arose in connection with the proofs of irrationality $\zeta(2)$ and $\zeta(3)$. The global nilpotence of these operators follows from explicit formulae (given by Apery) for solutions of L_1, L_2 and of L_3, the symmetric square of L_4, lying in $\mathbb{Z}[[X]]$ together with the fact that the remaining solutions of L_3 at $X = 0$ involved $\log X$ and $\log^2 X$. These explicit formulae led to integral formulae for the solutions which revealed their cohomological meaning [Dw1,2], [B-S], [Be]. These articles show that all three satisfy the conjecture and are related to ${}_2F_1(5/12, 1/12, 1, 1/j)$.

PRINCETON UNIVERSITY

REFERENCES

[Ba1] F. Baldassarri, On algebraic solutions of Lamé's differential equation, *J. of Diff. Equ.*, **41** (1981), 44–58.

[Ba2] ———, Towards a Schwarz list for Lamé's differential equation via division points on elliptic curves, *Group d'étude d'analyse ultramétrique*, Paris 1986/87, exp. 22.

[Ba-Dw] ——— and B. Dwork, Differential equations with algebraic solutions, *Amer. J. Math.*, **101** (1979), 42–76.

[Be] F. Beukers, Another congruence for Apery numbers, *J. of Number Theory*, **24** (1987), 201–210.

[B-S] ——— and J. Stenstra, On the Picard Fuchs equation and the formal Brauer group of certain elliptic K-3 surfaces, *Math. Ann.*, **271** (1985), 269–304.

[Chr1] B. Christol, Systèmes Différentiels Linéaires p-adiques; Structure de Frobenius Faible, *Bull. Soc. Math. France*, **109** (1981), pp. 83–122.

[Chr2] G. Christol, Equations differentielles du second ordre en charactéristique p (d'apres Dwork), *Group d'étude d'analyse ultramétrique*, Paris, 1986/87, exp. 19.

[Ch] D. V. Chudnovsky and G. F. Chudnovsky, Application of Padé approximation to the Grothendieck Conjecture on linear differential equations, *Number Theory*, New York, 1984, Springer Lec. Notes Math. 1135, 52–100.

[Cr] L. Crawford, On the solution of Lamé's equation in finite terms when $2n$ is an odd integer, *Quart. J. Math.*, **27** (1985), 93–98.

[Dw1] B. Dwork, Arithmetic theory of differential equations, *Symposia Math.*, **24**, Academic Press, N.Y., 1981, 225–243.

[Dw2] ———, On Apéry's differential operator, *Groupe d'étude d'analyse ultramétrique*, Paris, 1980/81, exp. 25.

[Ho] T. Honda, Algebraic differential equations, *Symposia Math.*, **24**, Academic Press, N.Y., 1981, 171–204.

[Ka] N. Katz, Application of a result of Turrittin, Nilpotent connections and the Monodromy theorem, *Pub. Math. IHES*, **39** (1970), 173–232.

[Me] W. Messing, On the nilpotence of the hypergeometric equation, *J. Math. Kyoto Univ.*, **23** (1972), 238–247.

[Po] E. Poole, *Introduction to Linear Diff. Equ.*, Oxford, 1936.

[W.W.] E. Whittaker and G. Watson, *Modern Analysis*, Cambridge, 1927.

[Z-S] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, Van Nostrand, 1960.