ALGEBRAIC DIFFERENTIAL EQUATIONS (*)

TAIRA HONDA

Translator's preface.

This is a translation of the Seminar Notes 38 issued by the Department of Mathematics, University of Tokyo. It is a faithful translation, except for minor corrections (misprints, a part of the proof of Theorem 7). As for the references, the original Seminar Note contained a general bibliography, but we have restricted ourselves here to those references which are most directly related to the present subject. The translator would like to express his hearty thanks to Professor Barsotti who gave him an opportunity to present a part of Honda's work in this form, and to the Department of Mathematics, University of Tokyo, for kindly allowing the translation of this Seminar Note.

Isao Miyawaki

Preface.

These notes were prepared by Mr. T. Ibukiyama (University of Tokyo), and based on lectures delivered by the late Professor Taira Honda (Osaka City University) at the Department of Mathematics, University of Tokyo, during October 21-24, 1974. It seems that Professor Honda did not intend to publish these results at this stage. But by his sudden death, the development of this work of Honda was passed to those left behind. So we shall present this work of Honda in this form. The bibliography was prepared by Ibukiyama and myself.

Yasutaka Ihara

(*) Comunicazione inviata all'Istituto Nazionale di Alta Matematica Francesco Severi.

Contents.

0. Introduction.

We shall denote by k a field of characteristic $p > 0$, and by K an algebraic number field. For a prime ideal $\mathfrak{p}$ of K, $\bar{K}_{\mathfrak{p}}$ denotes the residue field. Throughout this paper we use these symbols.

We shall denote by (1) the following differential equation:

$$a_0(x)y^{(n)} + a_1(x)y^{(n-1)} + \cdots + a_n(x)y = 0\,, \tag{1}$$

where $a_i(x) \in K[x]$ $(0 \leqq i \leqq n)$; instead, $(1)_{\mathfrak{p}}$ will denote the reduction modulo $\mathfrak{p}$ of (1). We shall also consider the same equation with $a_i(x) \in k[x]$ $(0 \leqq i \leqq n)$, in which case we shall denote the equation by $(1)_p$. Beginning with the next section, we intend to study some elementary properties of such differential equations. As motives for the study of such differential equations we mention the following problems.

i) Characterize algebraic functions as solutions of differential equations, by the arithmetical properties of the latter.

Grothendieck's problem: If, for almost all prime ideals $\mathfrak{p}$, $(1)_{\mathfrak{p}}$ has n solutions in $\bar{K}_{\mathfrak{p}}(x)$ which are independent over $\bar{K}_{\mathfrak{p}}(x^p)$, are all solutions of (1) algebraic functions?

In the case $n = 1$ it can be shown, by using Tchebotarev's density theorem, that the answer to this problem is affirmative. When the equations are of Picard-Fuchs type, Katz also solved this problem affirmatively. In general, it can be easily shown that the monodromy group at one point is finite. But this problem has not been solved globally.

ii) Find and study arithmetically interesting functions which are solutions of some suitable differential equation.

EXAMPLE. Consider an elliptic curve C: $Y^2 = X^3 - g_2X - g_3$, and let ω be a differential of the first kind on C. By taking a local parameter x at the origin such that $X = x^{-2}$, we have

$$\omega = \frac{dx}{\sqrt{1 - g_2x^4 - g_3x^6}}.$$

Define the formal power series $F(x, y)$ by the following process:

$$\begin{aligned} P(x) &= 1 - g_2x^4 - g_3x^6, \\ g(x) &= (P(x))^{-\frac{1}{2}} = 1 + \sum_{n=2}^{\infty} a_n x^{n-1}, \\ f(x) &= \int_0^x g(t)\,dt = \sum (a_n/n)x^n, \\ F(x, y) &= f^{-1}(f(x) + f(y)). \end{aligned}$$

Then $F(x, y)$ is a formal model of C. On the other hand, we obtain the following differential equation as a consequence of $g(x)^2P(x) = 1$:

$$2g' \cdot P(x) + g \cdot P'(x) = 0.$$

Thus, in general, in order to obtain a formal group $F(x, y)$, it is natural to seek a $g(x)$ which is a solution of a differential equation of this type. For a solution $g(x) = 1 + a_2x + a_3x^2 + \ldots$ of the above differential equation, we define the formal group $F(x, y)$ in the same way as above. If this formal group $F(x, y)$ is $\mathfrak{p}$-integral and of finite height for almost all $\mathfrak{p}$, can we say that $F(x, y)$ is obtained from an algebraic group? If so, it is interesting. If not so, then quite a new zeta-function might correspond to such an example, and it would also be very interesting.

1. Linear algebraic differential equations.

For a field k of characteristic $p > 0$, we denote by $k[x]$ the ring of polynomials of one variable over k, and by $k[\![x]\!]$ the ring of formal power series of one variable over k. Moreover, we denote by $k(x)$ and $k((x))$ the quotient fields of $k[x]$ and $k[\![x]\!]$ respectively. Now we shall consider the following ordinary differential equation:

$$(1)_p \quad a_0(x)y^{(n)} + a_1(x)y^{(n-1)} + \ldots + a_n(x)y = 0, \qquad a_i(x) \in k[x] \quad (0 \leqq i \leqq n).$$

Here, we consider $k((x))$ as a differential field, with the following natural derivation:

$$\begin{cases} d\alpha = 0 & (\alpha \in k)\,, \\ dx^n = nx^{n-1}\,. \end{cases}$$

REMARK. The constant field of the differential field $k((x))$ is $k((x^p))$. Hence if $(1)_p$ has a solution in $k((x))$, multiplication by a suitable constant yields a solution in $k[\![x]\!]$.

For any differential field, a set of solutions $\{y_1, \ldots, y_m\}$ of a linear differential equation is independent over its constant field if and only if the following Wronskian

$$W(y_1, \ldots, y_m) = \begin{vmatrix} y_1 & \cdots & y_m \\ y_1' & \cdots & y_m' \\ \vdots & & \vdots \\ y_1^{(m-1)} & \cdots & y_m^{(m-1)} \end{vmatrix}$$

does not vanish. Hence the dimension of the space of solutions is not greater than the rank of the differential equation. More precisely, if $W(y_1, \ldots, y_m) = 0$, then $y_1, \ldots, y_m$ are linearly dependent over the constant field of the differential field generated over the prime field by the y_i's and their derivatives. Therefore, for a differential field F and its differential extension field L, if $y_1, \ldots, y_m \in F$ are linearly dependent over the costant field of L, then $y, \ldots, y_m$ are also linearly dependent over the constant field of F. For convenience of the reader, we shall quote the proof by Kolchin [8].

LEMMA (Kolchin). *If the Wronskian of elements $y_1, \ldots, y_m$ of an (ordinary) differential field vanishes, then $y_1, \ldots, y_m$ are linearly dependent over the constant field.*

PROOF. The proof is by induction on m. If $m = 1$, then our Lemma is obviously true. Assume that it is true when the number of elements is at most $m-1$, and set

$$\mu_i = (-1)^{m+i} \begin{vmatrix} y_1 & \cdots & y_{i-1} & y_{i+1} & \cdots & y_m \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ y_1^{(m-2)} & \cdots & y_{i-1}^{(m-2)} & y_{i+1}^{(m-2)} & \cdots & y_m^{(m-2)} \end{vmatrix}, \qquad (i = 1, \ldots, m)\,.$$

If $\mu_m = 0$, we are reduced to the case of $m-1$ elements; hence we may assume $\mu_m \neq 0$. Now we can easily show that

$$\sum_{i=1}^{m} y_i^{(r)} \mu_i = 0\,, \qquad (0 \leqq r \leqq m-1)\,.$$

In fact, if $r = m-1$ this is obvious from the assumption of the Lemma; otherwise it is a consequence of

$$\begin{vmatrix} y_1 & \cdots & y_m \\ \cdots & \cdots & \cdots \\ y_1^{(m-2)} & \cdots & y_m^{(m-2)} \\ y_1^{(r)} & \cdots & y_m^{(r)} \end{vmatrix} = 0 .$$

By differentiating $\sum_{i=1}^{m} y_i^{(r)} \mu_i = 0$ we have

$$\sum_{i=1}^{m} y_i^{(r+1)} \mu_i + \sum_{i=1}^{m} y_i^{(r)} \mu_i' = 0 .$$

If $r \leqq m-2$, then we have already shown that

$$\sum_{i=1}^{m} y_i^{(r+1)} \mu_i = 0 ,$$

which implies that

$$\sum_{i=1}^{m} y_i^{(r)} \mu_i' = 0 .$$

On the other hand we have

$$y_m = -\sum_{i=1}^{m-1} \frac{\mu_i}{\mu_m} y_i ;$$

hence in order to complete the proof of the Lemma we must show that

$$\left(\frac{\mu_i}{\mu_m}\right)' = 0 .$$

From $\sum_{i=1}^{m} y_i^{(r)} \mu_i' = 0$ we have

$$\sum_{i=1}^{m-1} y_i^{(r)} \mu_i' = -\mu_m' y_m^{(r)} ,$$

which is equivalent to

$$\begin{pmatrix} y_1 & \cdots & y_{m-1} \\ \cdots & \cdots & \cdots \\ y_1^{(m-2)} & \cdots & y_{m-1}^{(m-2)} \end{pmatrix} \begin{pmatrix} \mu_1' \\ \vdots \\ \mu_{m-1}' \end{pmatrix} = -\mu_m \begin{pmatrix} y_m \\ \vdots \\ y_m^{(m-2)} \end{pmatrix} .$$

Thus we have by Cramer's formula:

$$\mu_i' = \frac{\mu_m' \mu_i}{\mu_m}.$$

From this we can easily see that $(\mu_i/\mu_m)' = 0$, which completes the proof of Lemma.

In the case of positive characteristic, the rank of the space of solutions is generally less than the rank of the differential equation.

EXAMPLE. The differential equation $y = y'$ has no solutions in $k((x))$.

LEMMA 1. *Let $y_1, \ldots, y_m \in k[\![x]\!]$ be linearly independent solutions (over $k((x^p))$) of $(1)_p$. For any sufficiently large natural number N, there exist solutions $z_1, \ldots, z_m \in k[x]$ of $(1)_p$ such that*

$$y_i \equiv z_i \bmod \deg N \qquad (1 \leqq i \leqq N),$$

(i.e., $y_i - z_i$ belongs to $x^N k[\![x]\!]$).

PROOF. An element $y = \sum_{i=0}^{\infty} c_i x^i$ of $k[\![x]\!]$ is a solution of $(1)_p$ if and only if the coefficients $c_0, c_1, \ldots$ satisfy the equations

$$A_{l,1} c_l + \ldots + A_{l,t} c_{l+t-1} = 0 \qquad (l = 0, 1, 2, \ldots),$$

where t is a natural number dependent on $a_0(x), \ldots, a_n(x)$, and $A_{l,j}$ is an element of k dependent on $a_0(x), \ldots, a_n(x), l, j$. Hence if t successive coefficients $c_{i+1}, \ldots, c_{i+t}$ vanish, the polynomial $c_0 + c_1 x + \ldots + c_i x^i$ is also a solution of $(1)_p$.

Let s be a natural number such that $ps \geqq t$. For a solution $y = \sum_{i=0}^{\infty} c_i x^i$ of $(1)_p$ we put

$$v_m = c_{mps} + c_{mps+1} x + \ldots + c_{(m+1)ps-1} x^{ps-1}, \qquad m = 0, 1, 2, \ldots.$$

Let $\{v_{i_1}, v_{i_2}, \ldots, v_{i_r}\}$ $(i_1 < i_2 < \ldots < i_r)$ be a basis of the vector space spanned by the above vectors over k, and, for any natural number N, let λ be a natural number such that $ps(\lambda - i_r) > N$. If we put

$$v_\lambda = b_1 v_{i_1} + \ldots + b_r v_{i_r},$$

then $y_1 = y(1 - b_1 x^{ps(\lambda - i_1)} - \ldots - b_r x^{ps(\lambda - i_r)})$ is also a solution of $(1)_p$, and all the coefficients of $x^{\lambda ps}, \ldots, x^{(\lambda+1)ps-1}$ in y_1 vanish. Hence if we take the first λps terms of y_1 as the polynomial z, this z is also a solution of $(1)_p$ such that $y \equiv z \bmod \deg N$.

Now, for independent solutions $y_1, \ldots, y_m$ of $(1)_p$, we take corresponding new solutions $z_1, \ldots, z_m$ by the above procedure. By $W(y_1, \ldots, y_m) \neq 0$ we have $W(z_1, \ldots, z_m) \neq 0$ for sufficiently large N. Thus the proof of our lemma is complete.

Next we shall consider a differential equation of rank one as the simplest case. Tchebotarev's density theorem implies the following:

(*) *Let K be an algebraic number field of finite degree. If almost all prime ideals of K are of degree one, then K is the rational number field.*

In the case $n = 1$, Grothendieck's problem is equivalent to (*), and hence is solved affirmatively.

PROOF. Grothendieck's problem implies Tchebotarev's density theorem. Let α be a generating element of K, i.e., $K = \boldsymbol{Q}(\alpha)$, and consider the following differential equation:

$$xy' - \alpha y = 0 . \tag{2}$$

If almost all prime ideals of K are of degree one, then for each such prime ideal $\mathfrak{p}$ there exists an integer $\alpha(\mathfrak{p}) \in \boldsymbol{Z}$ such that

$$\alpha \equiv \alpha(\mathfrak{p}) \bmod \mathfrak{p} .$$

Hence the differential equation $(2)_{\mathfrak{p}}$ has a solution $x^{\alpha(\mathfrak{p})}$, and this implies that the solution x^{α} of (2) is an algebraic function. Thus α is a rational number, and $K = \boldsymbol{Q}$.

Tchebotarev's density theorem implies Grothendieck's problem. Consider the following differential equation:

$$y' = P(x)\, y , \qquad P(x) \in K(x) . \tag{3}$$

If $(3)_{\mathfrak{p}}$ has a solution in $\bar{K}_{\mathfrak{p}}(x)$, then $(3)_{\mathfrak{p}}$ has also a solution $y_{\mathfrak{p}}$ in $\bar{K}_{\mathfrak{p}}[x]$. If we put

$$y_{\mathfrak{p}} = \prod_i (x - \bar{\alpha}_i)^{e_i}$$

we have

$$P(x) \bmod \mathfrak{p} = \frac{y'_{\mathfrak{p}}}{y_{\mathfrak{p}}} = \sum_i \frac{e_i}{(x - \bar{\alpha}_i)} .$$

This equation is valid for almost all $\mathfrak{p}$'s in K. Hence, in some suitable extension field of K we have

$$P(x) = \sum_i \frac{\beta_i}{(x - \alpha_i)} ,$$

and we can easily see that

$$\beta_i \equiv (\text{a rational integer}) \bmod \mathfrak{p} .$$

Hence we see that $\beta_i \in \boldsymbol{Q}$ by (*). If we put

$$y = c \prod_i (x - \alpha_i)^{\beta_i} ,$$

this solution of (3) is an algebraic function.

2. The differential equations of Fuchsian type.

DEFINITION 1. We say that $(1)_p$ *has sufficiently many solutions* if $(1)_p$ has n independent solutions in $k[\![x]\!]$.

DEFINITION 2. The concept « $(1)_p$ *has sufficiently many solutions in a weak sense* » is defined as follows, by induction on the rank n of the differential equation $(1)_p$.

In the case $n = 1$, we say that $(1)_p$ has sufficiently many solutions in a weak sense if $(1)_p$ has a non-zero solution.

Next, we assume that this concept is defined for any differential equation $(1)_p$ of rank $n-1$. Then we say that $(1)_p$ has sufficiently many solutions in a weak sense, if the following conditions are satisfied:

(i) $(1)_p$ has a non-zero solution $y_1 \in k[x]$.

(ii) if we take a suitable solution y_1 of such type and put $y = y_1 u$, then the new differential equation with respect to u' of rank $n-1$ obtained by the substitution $y = y_1 u$ in $(1)_p$, has sufficiently many solutions in a weak sense.

REMARK. In the terminology of Katz, this Definition 2 is equivalent to saying that the connection associated with $(1)_p$ has nilpotent p-curvature. Moreover, in the above condition (ii), « a suitable » can be equivalently replaced by « an arbitrary » (see Appendix).

REMARK. « Sufficiently many solutions in a weak sense » does not imply « sufficiently many solutions ».

EXAMPLE. $x^2y''-xy'+y=0$.

We define the regular singular points of the differential equation

$$(1)_p \qquad a_0(x)y^{(n)}+a_1(x)y^{(n-1)}+\ldots+a_n(x)y=0\,, \qquad a_i(x)\in k[x]$$

by the same method as in the case over $\boldsymbol{C}$. Namely:

DEFINITION 3. If $a_0(\alpha)=0$ and $(x-\alpha)^{e-i}$ divides $a_i(x)$ whenever e is the largest integer such that $(x-\alpha)^e$ divides $a_0(x)$, then we say that $x=\alpha$ is a regular singular point of $(1)_p$. If we then set $x=1/t$, thus obtaining a differential equation with coefficients in $k[t]$, we say that $x=\infty$ is a regular singular point of $(1)_p$ if $t=0$ is a regular singular point of this new differential equation.

Thus $x=\infty$ is a regular singular point if and only if $\deg a_i(x)\leqq \deg a_0(x)-i$.

DEFINITION 4. We say that $(1)_p$ is of Fuchsian type if and only if all the roots of the equation $a_0(x)=0$ and ∞ are regular singular points of $(1)_p$.

REMARK. (1) is of Fuchsian type if and only if $(1)_\mathfrak{p}$ is of Fuchsian type for infinitely many prime ideals $\mathfrak{p}$.

THEOREM 1. *If* $(1)_\mathfrak{p}$ *has sufficiently many solutions in a weak sense, then* $(1)_\mathfrak{p}$ *is of Fuchsian type.*

PROOF. If $n=1$, then $(1)_\mathfrak{p}$ has a non-zero polynomial solution y. Using this solution we have $y'/y=-a_1(x)/a_0(x)$. From this we can easily prove our Theorem.

Next, we assume our Theorem for any such differential equation of rank $n-1$. Let α be a root of $a_0(x)=0$ such that $(x-\alpha)^e$, but not $(x-\alpha)^{e+1}$, divides $a_0(x)$. If we choose a suitable solution $y_1=(x-\alpha)^s z$ with $0\leqq s<p$ and $(x-\alpha)$ not dividing z, and put

$y = y_1 u$, then the following differential equation with respect to u':

$$a_0(x)y_1u^{(n)} + \left\{\binom{n}{1}a_0(x)y_1' + a_1(x)y\right\}u^{(n-1)} + \cdots$$
$$\cdots + \left\{\binom{n}{i}a_0(x)y_1^{(i)} + \binom{n-1}{i-1}a_1(x)y_1^{(i-1)} + \cdots + a_i(x)y_1\right\}u^{(n-i)} + \cdots$$
$$\cdots + \left\{\binom{n}{n-1}a_0(x)y_1^{(n-1)} + \cdots + a_{n-1}(x)y_1\right\}u' = 0$$

has sufficiently many solutions in a weak sense. Here, we see that $(x-\alpha)^{e+s}$ divides $a_0(x)y_1$, but that $(x-\alpha)^{e+s+1}$ does not. Therefore

$$(x-\alpha)^{e+s-1} \text{ divides } \left\{\binom{n}{1}a_0(x)y_1' + a_1(x)y_1\right\}.$$

But we can easily see that $(x-\alpha)^{e+s-1}$ divides $a_0(x)y_1'$. Hence

$$(x-\alpha)^{e-1} \text{ divides } a_1(x).$$

By the same method as above, we can show that

$$(x-\alpha)^{e-i} \text{ divides } a_i(x) \qquad (0 \leqq i \leqq n-1).$$

As for the coefficient $a_n(x)$, we see that

$$a_0(x)y_1^{(n)} + \cdots + a_n(x)y_1 = 0,$$

and that

$$(x-\alpha)^{e+s-n} \text{ divides } a_i(x)y_1^{(n-i)} \qquad (0 \leqq i \leqq n-1).$$

From this, we conclude that $(x-\alpha)^{e-n}$ divides $a_n(x)$.

We can also show that $x = \infty$ is a regular singular point of $(1)_\mathfrak{p}$ by the same method as above.

COROLLARY. *If* $(1)_\mathfrak{p}$ *has sufficiently many solutions in a weak sense for infinitely many prime ideals* $\mathfrak{p}$, *then the differential equation* (1) *is of Fuchsian type.*

Now let $x = 0$ be a regular singular point of (1). We rewrite (1) as follows:

$$(4) \qquad b_0(x)x^n y^{(n)} + b_1(x)x^{n-1}y^{(n-1)} + \cdots + b_n(x)y = 0, \quad b_0(0) \neq 0.$$

If we substitute $y = x^{\varrho}\left(1 + \sum_{\nu=1}^{\infty} c_\nu x^\nu\right)$ in (4), then there exists a polynomial $f(x)$ of degree n such that the coefficient of x^{ϱ} in (4) vanishes if and only if $f(\varrho) = 0$.

DEFINITION 5. We call this equation $f(\varrho) = 0$ the *indicial equation* of (1) at $x = 0$. And its roots are called the *exponents* of (1).

THEOREM 2. *The exponents of the differential equation* (1) *are rational numbers when* $(1)_{\mathfrak{p}}$ *has sufficiently many solutions in a weak sense for almost all* $\mathfrak{p}$.

PROOF. This can be proved easily from the next Proposition and the density theorem.

PROPOSITION 2.1. *If* $(1)_p$ *has sufficiently many solutions in a weak sense, then its indicial equation has n roots in the prime field (the multiplicities being taken into account).*

PROOF. We prove this proposition by induction on n. If $n = 1$, then $(1)_p$ has a non-zero solution in $k[\![x]\!]$ by the assumption of the proposition, and this implies the proposition.

Next, we assume the proposition for any differential equation of rank $n-1$. The indicial equation of $(4)_p$ is given by

$$f_1(\varrho) = b_0(0)\varrho(\varrho-1)\dots(\varrho-n+1) + \dots + b_n(0) = 0\,.$$

Now we take a suitable polynomial solution $y_1 = x^{e_1}z_1(x)$ $(z_1(0) \neq 0)$ so that the differential equation obtained by substituting y with $y_1 u$ in $(4)_p$ has sufficiently many solutions in a weak sense. Let $f_2(\varrho) = 0$ be the indicial equation of this new differential equation with respect to u. Then we can easily see that $f_2(\varrho) = f_1(\varrho + e_1)$. Moreover, let $f_3(\varrho) = 0$ be the indicial equation of the differential equation with respect to u'. Then all roots of $f_3(\varrho) = 0$ belong to the prime field by the induction assumption. And we can easily see that $f_2(\varrho) = \varrho f_3(\varrho)$. Hence all the roots of $f_1(\varrho) = 0$ also belong to the prime field.

PROPOSITION 2.2. *If* $(1)_{\mathfrak{p}}$ *has a solution* $y_1 \in \bar{K}_{\mathfrak{p}}[x]$, *then there exists an exponent* ϱ *of* (1) *at* $x = \infty$ *such that*

$$\deg y_1 \equiv -\varrho \bmod \mathfrak{p}\,.$$

PROOF. *If we put*

$$y_1 = a_0 + a_1 x + \dots + x^m$$
$$= x^m(1 + a_{m-1}x^{-1} + \dots + a_0 x^{-m}),$$

then $-m = -\deg y_1$ is an exponent of $(1)_p$ at $x = \infty$. From this we can easily obtain our proposition.

REMARK. The converse of Theorem 1 is not necessarily true.

EXAMPLE. The equation $x^2y'' - y = 0$ is of Fuchsian type, and its indicial equation is $\varrho^2 - \varrho - 1 = 0$. If we consider the case $p = 2$, then this indicial equation has no solution in the prime field. Hence, by Theorem 2, this differential equation does not have sufficiently many solutions in a weak sense.

PROPOSITION 2.3. *Let k be a field of characteristic $p > 0$. If each of the following differential equations*

(a) $a_0(x)y'' + a_1(x)y' + a_2(x)y = 0$,

(b) $a_0(x)y' + a_1(x)y = 0$,

has a non-zero solution, then equation (a) has sufficiently many solutions in a weak sense.

PROOF. We take a solution $y_1 \in k[x]$ of (a) and a solution $z_1 \in k[x]$ of (b) which are non-zero. After substituting $y = y_1 u$ for (a), we obtain

$$a_0(x)y_1u'' + (2a_0(x)y_1' + a_1(x)y_1)u' = 0,$$

$$\frac{u''}{u'} + \frac{2y_1'}{y_1} + \frac{a_1(x)}{a_0(x)} = 0.$$

Hence we have

$$\frac{u''}{u'} + \frac{2y_1'}{y_1} - \frac{z_1'}{z_1} = 0.$$

This equation has a solution $u' = z_1/y_1^2$. This completes the proof of our proposition.

COROLLARY 1. *If $(1)_p$ satisfies the following conditions*

$n = 2$,
Fuchsian type,
All regular singular points belong to $GF(p)$,
$a_0(x)$, $a_1(x) \in GF(p)[x]$,
$(1)_p$ has a non-zero solution,

then $(1)_p$ has sufficiently many solutions in a weak sense.

PROOF. We may put $a_0(x) = \prod_{i=1}^{s} (x-\alpha_i)^2$, $\alpha_i \in GF(p)$, $\alpha_i \neq \alpha_j$ $(i \neq j)$. Then we have

$$\frac{a_1(x)}{a_0(x)} = \sum_{i=1}^{s} \frac{\beta_i}{x-\alpha_i}, \qquad \beta_i \in GF(p).$$

Let $e_i \in \boldsymbol{Z}$ be an integer such that $e_i \bmod p = \beta_i$. Then the equation

$$a_0(x)y' + a_1(x)y = 0$$

has a non-zero solution $y = \prod_{1=1}^{s} (x-\alpha_i)^{e_i}$. Hence $(1)_p$ has sufficiently many solutions in a weak sense by Proposition 2.3.

COROLLARY 2. *Gauss' differential equation*

$$x(x-1)y'' + \{(\alpha+\beta+1)x-\gamma\}y' + \alpha\beta y = 0, \qquad \alpha, \beta, \gamma \in GF(p),$$

has sufficiently many solutions in a weak sense.

PROOF. It is well-known that this equation has a solution. Moreover, we can easily check that the other conditions of Corollary 1 are satisfied.

3. Application to number theory.

Let $p \geqq 5$ be an odd prime number. We define the number $\varepsilon = \pm 1$ by $\varepsilon p \equiv 1 \bmod 4$. Let χ be the non-trivial character of $GF(p)^\times$ of order 2 (i.e., χ is the quadratic residue symbol). Then we put

$$S_{++} = \{a \in GF(p)^\times \mid \chi(a) = 1, \chi(1-a) = 1\},$$

$$S_{+-} = \{a \in GF(p)^\times \mid \chi(a) = 1, \chi(1-a) = -1\},$$

and we also define S_{-+} and S_{--} in a similar manner. Moreover, put

$$F_{--}(x) = \prod_{a \in S_{--}} (x-a),$$

$$F_{-+}(x) = \prod_{a \in S_{-+}} (x-a).$$

Then:

THEOREM 3. *If* $\varepsilon = 1$, *then*

$$F_{--}(x) = (-1)^{(p-1)/4} 2 \left(\frac{2}{p}\right) \sum_{i=0}^{(p-1)/4} \frac{(\frac{1}{4})_i (-\frac{1}{4})_i}{i!(\frac{1}{2})_i} x^i ,$$

$$F_{-+}(x) = (-1)^{(p-1)/4} \frac{1}{2} \left(\frac{2}{p}\right) \sum_{i=0}^{(p-1)/4} \frac{(\frac{3}{4})_i (\frac{1}{4})_i}{i!(\frac{3}{2})_i} x^i .$$

If $\varepsilon = -1$, *then*

$$F_{--}(x) = (-1)^{(p+1)/4} \left(\frac{2}{p}\right) \sum_{i=0}^{(p+1)/4} \frac{(\frac{1}{4})_i (-\frac{1}{4})_i}{i!(\frac{1}{2})_i} x^i ,$$

$$F_{-+}(x) = (-1)^{(p+1)/4} \left(\frac{2}{p}\right) \sum_{i=0}^{(p+1)/4} \frac{(\frac{3}{4})_i (\frac{1}{4})_i}{i!(\frac{3}{2})_i} x^i .$$

Here, the symbol $(\theta)_i$ *is defined as follows*:

$$(\theta)_0 = 1 ,$$

$$(\theta)_i = \theta(\theta+1)\dots(\theta+i-1) \qquad \text{if } i \geqq 1 .$$

METHOD OF PROOF. We shall consider the differential equation

$$x(x-1)y'' + \left(x - \frac{1}{2}\right)y' - \frac{y}{16} = 0 . \tag{5}$$

This equation has solutions $\sqrt{\sqrt{x} \pm \sqrt{x-1}}$ in characteristic zero. For any prime $p > 3$, equation $(5)_p$ has two polynomial solutions as follows. Let F_1 be the first $1 + (p-\varepsilon)/2$ terms of Gauss' hypergeometric function $F(\frac{1}{4}, -\frac{1}{4}, \frac{1}{2}; x)$, and let F_2 be the first $1 + (p-2+\varepsilon)/2$ terms of $F(\frac{3}{4}, \frac{1}{4}, \frac{3}{2}; x)$. Then $F_1(x)$ and $x^{(p+1)/2}F_2(x)$ are linearly independent solutions of $(5)_p$. We can easily show the above by considering the fundamental solutions in characteristic zero.

Noting that

$$\deg F_{--} = \deg F_1 \quad \text{and} \quad \deg F_{-+} = \deg F_2 ,$$

if we show that $F_{--}(x)$ and $x^{(p+1)/2}F_{-+}(x)$ satisfy the equation $(5)_p$, then we can obtain Theorem 3 by comparing the coefficients of the terms of highest degree.

To show that $y = F_{--}(x)$ satisfy $(5)_p$, we may compute

$$\frac{y'}{y} \quad \text{and} \quad \frac{y''}{y} = \left(\frac{y'}{y}\right)' + \left(\frac{y'}{y}\right)^2 .$$

But we have

$$(y^2)' = 2yy' \quad \text{and then} \quad \frac{y'}{y} = \frac{(y^2)'}{2y^2}.$$

On the other hand, we can show that

$$\text{const} \times F^2_{--}(x) = \frac{\{(1-x)^{(p-1)/2}+1\}\{1+x^{(p-1)/2}\}}{x^{(p-1)/2}+(1-x)^{(p-1)/2}}.$$

Thus we can avoid irrational calculations.

As for the coefficient of the term of highest degree, as an example we give the following congruences in the case $\varepsilon = 1$ and $m = (p-1)/4$:

$$\frac{(\frac{1}{4})_m(-\frac{1}{4})_m}{m!(\frac{1}{2})_m} = \frac{\{1\cdot 5\cdot\ldots\cdot(4m-3)\}\{(-1)\cdot 3\cdot\ldots\cdot(4m-5)\}}{m!\,1\cdot 3\cdot\ldots\cdot(2m-1)}\cdot\frac{2^m}{2^{4m}} \equiv$$

$$-\frac{1\cdot 3\cdot 5\cdot\ldots\cdot(p-4)}{\{2\cdot 4\cdot\ldots\cdot 2m\}\{(p-1)\cdot(p-3)\cdot\ldots\cdot(2m+2)\}}\cdot\frac{(-1)^m}{2^{2m}} \equiv$$

$$(-1)^{(p-1)/4}\left(\frac{2}{p}\right)\frac{1}{2}\cdot\frac{1\cdot 3\cdot 5\cdot\ldots\cdot(p-2)}{2\cdot 4\cdot 6\cdot\ldots\cdot(p-1)} \equiv (-1)^{(p-1)/4}\left(\frac{2}{p}\right)\frac{1}{2} \bmod p,$$

where we used the fact $2^{2m} = 2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \bmod p$.

The facts that equation (5) has the solution $\sqrt{\sqrt{x}+\sqrt{x-1}}$ and that equation $(5)_p$ has independent solutions $F_{--}(x)$ and $F_{-+}(x)$ are more directly related to each other in the following way. If we put $u = \sqrt{\sqrt{x}+\sqrt{x-1}}$, then u and u^{-1} are fundamental solutions of (5). And we can show that

$$u^{p-\varepsilon} + u^{-(p-\varepsilon)} \quad \text{and} \quad x^{-\frac{1}{2}}(u^{p+\varepsilon} + u^{-(p+\varepsilon)})$$

are elements of $\boldsymbol{Z}[x]$. If we note that $u^p \bmod p$ is an element of the constant field, then we see that

$$u^{p-\varepsilon} + u^{-(p-\varepsilon)} \bmod p \quad \text{and} \quad x^{-\frac{1}{2}}(u^{p+\varepsilon} + u^{-(p+\varepsilon)}) \bmod p$$

are fundamental solutions of $(5)_p$.

But we can easily show that

$$c_1 F_{--}(x) \equiv u^{p-\varepsilon} + u^{-(p-\varepsilon)} \bmod p,$$

$$c_2 F_{-+}(x) \equiv x^{-\frac{1}{2}}(u^{p+\varepsilon} + u^{-(p+\varepsilon)}) \bmod p,$$

where c_1 and c_2 are elements of $\boldsymbol{F}_p^\times$ $(p \neq 2)$. Therefore $F_{--}(x)$ and $x^{(p+1)/2}F_{-+}(x)$ are fundamental solutions of $(5)_p$.

As for $F_{++}(x)$ and $F_{+-}(x)$, there exist similar expressions of them by u, but it seems that the polynomial expansions of them are not so simple as those described in Theorem 3.

4. Introduction of the logarithmic functions (characteristic $p>0$).

Let ξ be a transcendental element over $k(\!(x)\!)$. We shall turn $k(\!(x)\!)(\xi)$ into a differential extension field by setting $\xi' = 1/x$.

$k(\!(x^p)\!)(\xi^p)$ is the constant field of $k(\!(x)\!)(\xi)$.

Proof. Take an element g/f of $k(\!(x)\!)(\xi)$ with $f, g \in k(\!(x)\!)[\xi]$. We may assume that f and g are prime to each other as polynomials with respect to ξ.

Now we suppose $(g/f)' = 0$, hence we have $fg' = f'g$. From this we derive that f divides f'. But we see that $\deg f$ (= the degree of f with respect to ξ) $\geqq \deg f'$. This shows that

$$f' = cf \qquad \text{with } c \in k(\!(x)\!) \ (c \text{ may be zero}).$$

If we display $f \in k(\!(x)\!)[\xi]$ as follows

$$f = b_0(x) + b_1(x)\xi + \cdots + b_n(x)\xi^n, \qquad b_i(x) \in k(\!(x)\!),\ b_n(x) \neq 0,$$

we have

$$f' = \left(b_0'(x) + \frac{b_1(x)}{x}\right) + \left(b_1'(x) + \frac{b_2(x)}{x}\right)\xi + \cdots + \left(b_{n-1}'(x) + \frac{b_n(x)}{x}\right)\xi^{n-1} + b_n'(x)\xi^n.$$

Therefore c must be equal to $b_n'(x)/b_n(x)$. Set $c_i(x) = b_i(x)/b_n(x)$. By equating the coefficients of $f' - (b_n'(x)/b_n x)f$ to zero, we obtain

$$\begin{cases} c_i'(x) + \dfrac{(i+1)c_{i+1}(x)}{x} = 0, & (0 \leqq i \leqq n-1), \\ c_n(x) = 1. \end{cases}$$

In particular, $c_n(x)$ belongs to $k(\!(x^p)\!)$.

Now we suppose that $c_{i+1}(x) \in k((x^p))$, and consider the equation

$$c_i'(x) = -\frac{(i+1)\,c_{i+1}(x)}{x}\,.$$

Each non-zero term on the right hand side is of type x^{pm-1} with $m \in \boldsymbol{Z}$. If $i+1 \not\equiv 0 \bmod p$, then $c_{i+1}(x)$ must be zero, otherwise $c_i'(x)$ cannot have a primitive function $c_i(x)$ in $k((x))$. Moreover if $i+1 \equiv 0 \bmod p$, then we have $c_i'(x) = 0$, i.e. $c_i(x) \in k((x^p))$. Thus we have by induction

$$\begin{cases} c_i(x) = 0\,, & \text{if } i \not\equiv 0 \bmod p\,, \\ c_i(x) \in k((x^p)) & \text{if } i \equiv 0 \bmod p\,. \end{cases}$$

Therefore we have

$$f/b_n(x) \in k((x^p))[\xi^p]\,.$$

Let $d_m(x)$ be the coefficient of the highest term of g. Then, by the same method as above, we can show that

$$g/d_m(x) \in k((x^p))[\xi^p]\,.$$

On the other hand, we see that

$$f\left(\frac{d_m'}{d_m}g\right) = g\left(\frac{b_n'}{b_n}f\right)$$

(from $fg' = f'g$). This implies that

$$\left(\frac{b_n}{d_m}\right)' = 0 \quad \text{i.e.} \quad \frac{b_n}{d_m} \in k((x^p))\,.$$

Therefore we have

$$\frac{g}{f} = \frac{g/d_m}{f/b_n} \times \frac{d_m}{b_n} \in k((x^p))(\xi^p)\,.$$

Conversely, it is trivially true that any element of $k((x^p))(\xi^p)$ is a constant. This completes the proof.

We put $R = k[x, \xi]$ and $\hat{R} = k[\![x]\!][\xi]$.

LEMMA 4.1. *If the degree of an element u of $\hat{R}$ (resp. R) with respect to ξ is less than or equal to $p-2$, then u has a primitive function in $\hat{R}$ (resp. R).*

PROOF. We shall prove this lemma by induction on the degree of u.

If $u = f(x) \in k[\![x]\!]$, then we can write it as follows:

$$f(x) = f_1(x) + \frac{f_2(x^p)}{x},$$

where $f_1(x)$ has no term of degree $pv-1$. Thus we have

$$\int f(x)\,dx = \int f_1(x)\,dx + f_2(x^p)\xi \in k[\![x]\!][\xi].$$

Hence, if the degree of u is zero our lemma is proved.

Next we consider the case $u = f\xi^n$, $f \in k[\![x]\!]$. Then we have

$$\int f\xi^n\,dx = \xi^n \int f\,dx - n\int \left(\frac{\xi^{n-1}}{x}\int f\,dx\right)dx.$$

If we put $\int f\,dx = xf_2(x) + c$, we see that

$$\int \frac{\xi^{n-1}}{x}(xf_2(x)+c)\,dx = \int \xi^{n-1}f_2(x)\,dx + c\int \frac{\xi^{n-1}}{x}\,dx,$$

$$\int \frac{\xi^{n-1}}{x}\,dx = \frac{1}{n}\xi^n.$$

This shows that the proof of our lemma in the present case is reduced to the case of degree $n-1$. Therefore the proof of our lemma is completed by induction.

PROPOSITION 4.1. *Assume $n \leqq p$. If equation $(1)_p$ has sufficiently many solutions in a weak sense, then $(1)_p$ has sufficiently many solutions in R.*

PROOF. We prove this proposition by induction on n.

If $n = 1$ the proposition is obviously true.

Next, we suppose that the proposition is true for equations $(1)_p$ of ranks less than n. If we take a suitable solution $y_1(\neq 0) \in k[x]$ and put $y = y_1 u$, the new differential equation of rank $n-1$ with respect to u' has sufficiently many solutions in a weak sense. This equation has independent solutions $v_2, \ldots, v_n$ by the induction assumption. Moreover, we may assume inductively that the degrees of these solutions are less than or equal to $n-2$. Therefore they have primitive functions $u_2, \ldots, u_n$ in R. Then $y_1, y_1u_2, \ldots, y_1u_n$ are solutions

of $(1)_p$. If we suppose

$$c_1y_1 + c_2y_1u_2 + \dots + c_ny_1u_n = 0\,, \qquad c_i \in k[x^p, \xi^p]\,,$$

then we see that

$$c_2v_2 + \dots + c_nv_n = 0\,.$$

Therefore we have

$$c_2 = \dots = c_n = 0 \quad \text{and} \quad c_1 = 0\,.$$

Thus we have completed the proof of our proposition.

EXAMPLE.

$$x(x-1)y'' + (2x-1)y' + \tfrac{1}{4}y = 0\,.$$

In characteristic zero, the space of the solutions of this equation is spanned by

$$W_1(x)\,, \qquad W_1(x)\log x + W_2(x)\,,$$

where we define $W_1(x)$ and $W_2(x)$ by

$$W_1(x) = 1 + \sum_{n=1}^{\infty} \binom{-\frac{1}{2}}{n}^2 x^n\,,$$

$$W_2(x) = 4\sum_{n=1}^{\infty} \binom{-\frac{1}{2}}{n}^2 \left(1 - \frac{1}{2} + \frac{1}{3} - \dots - \frac{1}{2n}\right) x^n\,.$$

$W_2(x)$ is not p-integral for all primes p. But in characteristic $p > 2$, the functions

$$y_1 = 1 + \sum_{n=1}^{(p-1)/2} \binom{-\frac{1}{2}}{n}^2 x^n\,, \qquad y_2 = 4\sum_{n=1}^{(p-1)/2} \binom{-\frac{1}{2}}{n}^2 \left(1 - \frac{1}{2} + \frac{1}{3} - \dots - \frac{1}{2n}\right) x^n$$

are well-defined, and the two functions y_1 and $y_1\xi + y_2$ are solutions of this equation.

PROPOSITION 4.2. *If equation* $(1)_p$ *has sufficiently many solutions in* $\hat{R}$, *it also has sufficiently many solutions in a weak sense.*

PROOF. We also prove this proposition by induction. Case $n = 1$: let an element

$$y_0\xi^r + y_1\xi^{r-1} + \dots + y_r\,, \qquad \text{where } y_i \in k[\![x]\!] \text{ and } y_0 \neq 0\,,$$

be a solution of the equation $a_0(x)y' + a_1(x)y = 0$. Then we have

$$(a_0(x)y_0' + a_1(x)y_0)\xi^r + \left(a_0(x)\left(r\frac{y_0}{x} + y_1'\right) + a_1(x)y_1\right)\xi^{r-1} + \ldots = 0 .$$

As the element ξ is transcendental over $k(\!(x)\!)$, we get $a_0(x)y_0' + a_1(x)y_0 = 0$. Thus there exists a non-trivial solution y_0 in $k[\![x]\!]$. Therefore we get a non-zero polynomial solution, which implies the proposition in our case.

Next, we suppose the proposition to be true for equations of rank $n-1$, and find a polynomial solution y_1 by the same method as above. Let $y_2, \ldots, y_n$ be other solutions of $(1)_p$ in $\hat{R}$ such that $y_1, \ldots, y_n$ are linearly independent over the constant field. If we put $y = y_1 u$, the new equation with respect to u' is of rank $n-1$ and has solutions $(y_2/y_1)', \ldots, (y_n/y_1)'$. Therefore $y_1^p(y_2/y_1)', \ldots, y_1^p(y_n/y_1)'$ are also solutions of that equation. Assume

$$c_2 y_1^p(y_2/y_1)' + \ldots + c_n y_1^p(y_n/y_1)' = 0 ,$$

where c_i belongs to the constant field.

After integration we obtain

$$c_1 + c_2 y_1^p(y_2/y_1) + \ldots + c_n y_1^p(y_n/y_1) = 0 ,$$

i.e.

$$c_1 y_1 + c_2 y_1^p y_2 + \ldots + c_n y_1^p y_n = 0 ,$$

hence $c_1 = c_2 = \ldots = c_n = 0$. This shows that the new equation with respect to u' has sufficiently many solutions in $\hat{R}$. Hence, by the induction assumption, that equation and also $(1)_p$ has sufficiently many solutions in a weak sense. This completes the proof of our proposition.

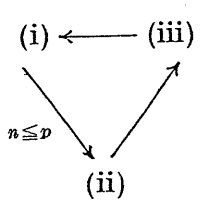
Summing up the above results we have the following theorem:

THEOREM 4. *If $n \leqq p$ the following three conditions are equivalent:*

(i) $(1)_p$ has sufficiently many solutions in a weak sense.

(ii) $(1)_p$ has sufficiently many solutions in R.

(iii) $(1)_p$ has sufficiently many solutions in $\hat{R}$.



COROLLARY. *If* $(1)_p$ *satisfies one of the conditions of Theorem* 4, *then* $(1)_p$ *has* n *independent solutions, of degree* $n-1$ *with respect to* ξ, *in* R.

5. Differential equations having sufficiently many solutions.

PROPOSITION 5.1. *Assume that equation* $(1)_p$ *has* n *independent solutions in* $k[x]$; *if* $y_1, \ldots, y_n$ *are independent solutions for which* $\sum_{i=1}^{n} \deg y_i$ *is minimal, the set* $\{\deg y_i \bmod p\}_{i=1}^{n}$ *is uniquely determined by* $(1)_p$ *independently of the choice of* $\{y_i\}$. *Moreover, the elements* $\deg y_i$ *are mutually incongruent modulo* p.

PROOF. Set $g_i = \deg y_i$. If we assume for instance

$$g_1 - g_2 = vp > 0 ,$$

there exists a constant c such that

$$\deg (y_1 - cx^{vp} y_2) < \deg y_1 .$$

Hence, if we put $z_1 = y_1 - cx^{vp} y_2$, also

$$z_1, y_2, \ldots, y_n$$

are independent solutions of $(1)_p$. But this contradicts the fact that $\sum_{i=1}^{n} g_i$ is minimal. Therefore $\deg y_i$ are mutually incongruent modulo p.

Let $\varrho_1, \ldots, \varrho_n \in GF(p)$ be the exponents of $(1)_p$ at ∞. We already know that each $-g_i$ is congruent modulo p to some ϱ_j. Since the $g_i \bmod p$ are distinct, we conclude that

$$\{\varrho_1, \ldots, \varrho_n\} = \{-g_i \bmod p\}_{i=1}^{n} .$$

COROLLARY. *If the equation* $(1)_p$ *has sufficiently many solutions in* $k[\![x]\!]$, *then* $n \leqq p$.

PROPOSITION 5.2. *Let* (1) *be a differential equation over* $K[x]$. *If* $(1)_{\mathfrak{p}}$ *has sufficiently many solutions in* $\overline{K}_{\mathfrak{p}}[x]$, *then* n *exponents of* $(1)_{\mathfrak{p}}$ *are incongruent modulo* $\mathfrak{p}$ *to each other. If the above condition is satisfied for almost all prime ideals* $\mathfrak{p}$, *then the exponents of* (1) *are* n *distinct rational numbers.*

PROOF. Easy.

PROPOSITION 5.3. *We suppose that* $(1)_p$ *has sufficiently many solutions. Let* $y_1, \ldots, y_n$ *be independent solutions of* $(1)_p$ *such that* $\sum_{i=1}^{n} \deg y_i$ *is minimal. Then the set of the degrees of the* y_i *is uniquely determined.*

PROOF. As the set $\{\deg y_i \bmod p\}$ is uniquely determined and all its elements are distinct, for each ϱ_i we can find a solution y_i such that $\varrho_i \equiv -\deg y_i \bmod p$ and that $\deg y_i$ is minimal. If these solutions $y_1, \ldots, y_n$ are independent, then it is obvious that $\sum_{i=1}^{n} \deg y_i$ is minimal. We put

$$c_i y_1 + \ldots + c_n y_n = 0 , \qquad c_i \in k[x^p] .$$

Let C be the set of the non-vanishing c_i's, and if C is not empty let $\deg c_1 y_1$ be the largest $\deg c_i y_i$ for $c_i \in C$; then the $\deg c_i y_i \bmod p$ for $c_i \in C$ are all distinct. But the coefficient of the highest term of $c_1 y_1$ is zero, and this is a contradiction. Hence we have

$$c_1 = \ldots = c_n = 0 .$$

Thus we have completed the proof of our proposition.

LEMMA 5.4. *Let* $y_1, \ldots, y_n$ *be elements of* $K[\![x]\!]$. *If* $y_1 \bmod \mathfrak{p}, \ldots, y_n \bmod \mathfrak{p}$ *are independent over* $\bar{K}_{\mathfrak{p}}((x^p))$ *for almost all prime ideals* $\mathfrak{p}$, *then* $y_1, \ldots, y_n$ *are independent over* K.

PROOF. We can easily prove this lemma by using the Wronskian.

PROPOSITION. *If equation* (1) *has* n *independent algebraic solutions, then* $(1)_{\mathfrak{p}}$ *has* n *independent polynomial solutions for almost all* $\mathfrak{p}$.

PROOF. Easy.

LEMMA 5.5. *Let* $\boldsymbol{A}\boldsymbol{y} = \boldsymbol{b}$ *be a system of linear equations in* K. *If the linear system* $\boldsymbol{A}\boldsymbol{y} \equiv \boldsymbol{b} \bmod \mathfrak{p}$ *has a solution for infinitely many prime ideals* $\mathfrak{p}$, *then* $\boldsymbol{A}\boldsymbol{y} = \boldsymbol{b}$ *has a solution.*

PROOF. It is trivial.

THEOREM 5. *For a given differential equation* (1), *if* $(1)_{\mathfrak{p}}$ *has sufficiently many solutions in* $\bar{K}_{\mathfrak{p}}[x]$ *for almost all prime ideals* $\mathfrak{p}$, *then its local monodromy group (of a neighborhood of one point) is finite and cyclic* (Katz).

PROOF. We may suppose that $x = 0$ is a regular singular point. By the assumption all the exponents of (1) are distinct rational numbers. Taking one of them we put $\varrho = \varrho_i$. We may show that there exists a solution of type $x^{\varrho}\left(1 + \sum_{\nu=1}^{\infty} c_\nu x^\nu\right)$ in characteristic zero. If there exist such solutions for all exponents, then it is obvious that they are linearly independent over $\mathbf{C}$ and that the local monodromy group is

$$\left\{ \begin{pmatrix} \exp[2\pi i\varrho_1] & & 0 \\ & \ddots & \\ 0 & & \exp[2\pi i\varrho_n] \end{pmatrix}^m \right\}.$$

Now let $f(x) = 0$ be the indicial equation of (1). By comparing the coefficient of $x^{\varrho+\nu}$, c_ν can be found by the following recursive equation

$$f(\varrho + \nu)\, c_\nu = A_{\nu,\nu-1} c_{\nu-1} + \ldots + A_{\nu,\nu-l} c_{\nu-l} + B_\nu ,$$

where A and B are determined by (1) and its suffix independently of c_ν.

If $\varrho_i - \varrho_j$ is a natural integer, there is an obstruction to the determinaton of $c_{\varrho_i - \varrho_i}$. Fix an integer $N \geqq \max(\varrho_i - \varrho_j)$; if we take a formal series $y = x^{\varrho}\left(1 + \sum_{\nu=1}^{N} c_\nu x^\nu\right)$ which satisfies the equation

(*) $\qquad$ (*left hand side of* (1)) $\equiv 0 \bmod \deg(\varrho + N + 1)$,

all c_ν $(\nu > N)$ are automatically determined by the above recursive equation. Equation (*) is equivalent to a linear system with respect to $c_1, \ldots, c_N$, and we denote this system by (**). For a prime ideal $\mathfrak{p}$ such that $(1)_{\mathfrak{p}}$ has sufficiently many solutions, we take a non-negative integer e such that $\varrho \equiv e \bmod \mathfrak{p}$. Then $(1)_{\mathfrak{p}}$ has a solution of the following form:

$$x^e\left(1 + \sum_{\nu=1}^{\infty} \tilde{c}_\nu x^\nu\right) \in \bar{K}_{\mathfrak{p}}[\![x]\!] .$$

Hence $x^e\left(1 + \sum_{\nu=1}^{N} \tilde{c}_\nu x^\nu\right)$ is a solution of the equation

$(*)_{\mathfrak{p}}$ $\qquad$ (*ledt hand side of* $(1)_{\mathfrak{p}}$) $\equiv 0 \bmod \deg(e + N + 1)$.

Hence $\tilde{c}_1, \ldots, \tilde{c}_N$ is a solution of $(**)_{\mathfrak{p}}$. Therefore $(**)_{\mathfrak{p}}$ has a solution

for infinitely many prime ideals $\mathfrak{p}$. By Lemma 5.5 the linear system (**) has a solution. Hence (*) also has a solution, and this shows that (1) has a solution of the form $x^{\varrho}\left(1+\sum_{\nu=1}^{\infty} c_\nu x^\nu\right)$. It can be easily verified that this formal solution is convergent.

THEOREM 6. *For a given differential equation* (1) *assume that* $(1)_{\mathfrak{p}}$ *has sufficiently many solutions for almost all* $\mathfrak{p}$*'s, and that* $(1)_{\mathfrak{p}}$ *has solutions* $y_1^{(\mathfrak{p})}, \ldots, y_n^{(\mathfrak{p})}$ *such that* $\sum_{i=1}^{n} \deg y_i^{(\mathfrak{p})}$ *is bounded for infinitely many* $\mathfrak{p}$*'s. Then all the solutions of* (1) *are polynomials.*

PROOF. As the exponents of (1) at ∞ are rational numbers, we display them as follows:

$$-\frac{\mu_i}{\nu_i}, \qquad (\nu_i \geqq 1\ ,\ (\mu_i, \nu_i) = 1)\ .$$

Let S be the set of primes $\mathfrak{p}$ which satisfy the latter assumption of the theorem. Moreover, for an element $\mathfrak{p}$ of S, let p be the rational prime such that $\mathfrak{p}$ divides p. Then we have

$$\frac{\mu_i}{\nu_i} \equiv \deg y_j^{(\mathfrak{p})} \bmod p\ , \qquad \text{for some } 1 \leqq j \leqq n\ .$$

Hence there exists a non-negative integer $\lambda_{\mathfrak{p}}$ such that

$$0 \leqq \deg y_j^{(\mathfrak{p})} = \frac{\lambda_{\mathfrak{p}} p + \mu_i}{\nu_i}\ .$$

If $\mu_i < 0$, then it is trivial that $\lambda_{\mathfrak{p}} \geqq 1$. And if $\nu_i > 1$, then it is also trivial that $\lambda_{\mathfrak{p}} \neq 0$. Thus we see that $\lambda_{\mathfrak{p}} \geqq 1$ in these cases. But $\lambda_{\mathfrak{p}} \geqq 1$ implies that $\deg y_i^{(\mathfrak{p})}$ is not bounded if $p \to \infty$, which is a contradiction. Therefore have $\mu_i \geqq 0$ and $\nu_i = 1$.

For any element $\mathfrak{p}$ of S set $\deg y_j^{(\mathfrak{p})} = g_j^{(\mathfrak{p})}$; then we have $0 \leqq g_j^{(\mathfrak{p})}$, $\mu_i < p$ for a sufficiently large prime p. Hence we may suppose that

$$g_i^{(\mathfrak{p})} = \mu_i\ , \qquad (i = 1, \ldots, n)\ .$$

Now we can verify that (1) has a polynomial solution of degree μ, if $(1)_{\mathfrak{p}}$ has a polynomial solution of degree μ for infinitely many prime ideals $\mathfrak{p}$.

In fact, set

$$y = x^{\mu} + c_1 x^{\mu-1} + \ldots + c_{\mu} x \qquad \text{in (1)}.$$

Then we have a linear system with respect to $c_1, \ldots, c_{\mu}$, which has a solution modulo $\mathfrak{p}$ for infinitely many prime ideals $\mathfrak{p}$. Therefore this linear system has a solution in K by Lemma 5.5, which shows that (1) has a polynomial solution of degree μ. Thus we have completed the proof of the theorem.

On the degree of solutions (*characteristic* $p > 0$).

Hereafter, we suppose that $(1)_p$ satisfies the following conditions

$$\begin{cases} (a_0(x), \ldots, a_n(x)) = 1 & \text{and Fuchsian type}, \\ \deg a_0(x) = t + n, & 0 \leqq t \leqq p-1. \end{cases}$$

We put

$$D = a_0(x)\frac{d^n}{dx^n} + a_1(x)\frac{d^{n-1}}{dx^{n-1}} + \ldots + a_n(x).$$

Since $(1)_p$ is a Fuchsian type differential equation, we have

$$\deg a_i(x) \leqq t + n - i.$$

Hence, if we take an element y of $k[x]$, we have

$$\deg Dy = \deg y = t.$$

DEFINITION OF SYMBOL: For a polynomial $u = c_0 + c_1 x + \ldots + c_{p-1}x^{p-1}$ of $k[x]$ we denote by $\bar{u}$ the polynomial

$$\bar{u} = c_{p-t}x^{p-t} + c_{p-t+1}x^{p-t+1} + \ldots + c_{p-1}x^{p-1}.$$

LEMMA 5.6. *Let y be a polynomial of the following form:*

$$y = u_0 + u_1 x^p + \ldots + u_m x^{pm} + \ldots,$$

where $u_i, y \in k[x]$ and $\deg u_i \leqq p-1$.

If y is a solution of $(1)_p$ and $\bar{u}_m$ is zero for some $m \geqq 0$, the polynomial

$$y_1 = u_0 + u_1 x^p + \ldots + u_m x^{pm}$$

is also a solution of $(1)_p$.

PROOF. We put $y=y_1+x^{p(m+1)}z$ for a suitable polynomial z of $k[z]$. Then we have

$$Dy_1+x^{p(m+1)}Dz=0$$

and

$$\deg Dy_1 \leqq \deg y_1 + t \leqq pm+p-t-1+t<p(m+1)\,.$$

Hence $Dy_1=0$, which shows that y_1 is a solution of $(1)_p$.

EXAMPLE. In the case $t=0$ in $(1)_p$, we can evaluate the minimal value of $\sum_i \deg y_i$: For each exponent ϱ_i, there exists a solution y_i such that $\deg y_i \equiv \varrho_i \bmod p$. Relations $\deg u_1 \leqq p-1$ and $t=0$ entail $\bar{u}_1=0$. Hence we can find a solution y_i such that $0 \leqq \deg y_i \leqq p-1$. Therefore we have

$$\min \sum_i \deg y_i \leqq p-1+(p-2)+\ldots+(p-n) \leqq np-\frac{n(n+1)}{2}\,.$$

In general we have the following theorem.

THEOREM 7.

(A) If $p<n$, then $(1)_p$ does not have n independent solutions.

(B) If $p=n$, then $(1)_p$ has n indipendent solutions if and only if it is of the following type:

$$(1)_p \qquad y^{(n)}=0\,.$$

In this case, the solutions $1, x, \ldots, x^{p-1}$ are independent solutions of $(1)_p$

(C) In cases $n<p$ and $0 \leqq t \leqq p-1$, assume that $(1)_p$ has independent polynomial solutions. For any set of n independent solutions $y_1, \ldots, y_n$ set $\deg y_i = g_i$. Then the minimal value $g=\min \sum_{i=1}^{n} g_i$ satisfies the inequality

$$t+\frac{n(n+1)}{2} \leqq g \leqq (n+t)p-\left(nt+\frac{n(n+1)}{2}\right).$$

COROLLARY. *If $p=n+1$, then $g=t+n(n+1)/2$.*

PROOF OF THEOREM 7. (*A*) is already contained in the Corollary of Proposition 5.1. Let us prove (*B*). In this case the indicial equation of $(1)_p$ at $x=0$ is of degree p and has p distinct roots. Hence the indicial equation must be $\varrho(\varrho-1)\ldots(\varrho-p+1)=0$. Therefore the differential equation must be $y^{(n)}=0$. Next we shall prove sta-

tement (C). Let

$$y_i = u_{i,0} + u_{i,1}x^p + u_{i,2}x^{2p} + \cdots \qquad (1 \leqq i \leqq n)$$

be independent polynomial solutions of $(1)_p$ such that $\sum_{i=1}^{n} \deg y_i$ attains the minimal value. We already know that $\deg y_i \bmod p$ are distinct. Changing the suffixes, if necessary, we may suppose that $S = \{\bar{u}_{1,0}, \bar{u}_{2,0}, \cdots, \bar{u}_{s_0,0}\}$ is a set of linearly independent vectors over k and that the other $\bar{u}_{i,0}$ are dependent on these vectors. Moreover we may take S so that s_0 is minimal. Then we shall show that we may assume $\bar{u}_{i,0} = 0$, $y_{i,0} = u_{i,0}$ for $i \geqq s_0 + 1$.

For an element $\bar{u}_{i,0}$ $(i \geqq s_0 + 1)$ we have

$$\bar{u}_{i,0} = \sum_{j=1}^{s_0} c_j \bar{u}_{j,0}\,, \qquad c_j \in k\,.$$

Hence we have

$$y_i - \sum_{j=1}^{s_0} c_j y_j = \left(u_{i,0} - \sum_{j=1}^{s_0} c_j u_{j,0}\right) + x^p z_i\,,$$

$$u_{i,0} - \sum_{j=1}^{s_0} c_j u_{j,0} = \bar{u}_{i,0} - \sum_{j=1}^{s_0} c_j \bar{u}_{j,0} = 0\,.$$

Here, if we remember that the elements $\deg y_j \bmod p$ are all distinct, we conclude that

$$\deg\left(y_i - \sum_{j=1}^{s_0} c_j y_j\right) = \deg y_k$$

for a suitable integer k in the set $\{1, 2, \cdots, s_0, i\}$. Hence we have

$$\deg y_k = \begin{cases} p + \deg z_i & \text{if } z_i \neq 0\,, \\ \deg\left(u_{i,0} - \sum_j c_j u_{j,0}\right) & \text{if } z_i = 0\,. \end{cases}$$

If $z_i \neq 0$, we have $\deg y_k > \deg z_i$ and $\deg y_k \equiv \deg z_i \bmod p$. As z_i is also a solution of $(1)_p$, we can show that the vectors

$$\{y_1, \cdots, y_{k-1}, z_i, y_{k+1}, \cdots, y_n\}$$

are independent solutions of $(1)_p$ by the same method used in the proof of Proposition 5.3. But this fact contradicts with minimality

of $\sum_i \deg y_i$. Therefore we see that $z_i = 0$ and that

$$y_i - \sum_{j=1}^{s_0} c_j y_j = u_{i,0} - \sum_{j=1}^{s_0} c_j u_{j,0} .$$

If it is not the case that $y_i = u_{i,0}$ with $\overline{u}_{i,0} = 0$, then we easily see that

$$\deg y_i \geqq p - t .$$

On the other hand, we have

$$\deg \left(u_{i,0} - \sum_{j=1}^{s_0} c_j u_{j,0}\right) < p - t \leqq \deg y_i \leqq \deg \left(y_i - \sum_{j=1}^{s_0} c_j y_j\right) .$$

But this is a contradiction. Thus we have shown that

$$y_i = u_{i,0} , \qquad \overline{u}_{i,0} = 0$$

for $i \geqq s_0 + 1$.

Under the above assumption we take a new set $S_1 = \{\overline{u}_{1,1}, \overline{u}_{2,1}, \ldots, \overline{u}_{s,1}\}$ so that all the elements of $S_0 \cup S_1$ are linearly independent over k and that the other $\overline{u}_{i,1}$, are linearly dependent on these vectors. Moreover, we may also take $\{y_i\}$ so that s_1 is minimal. Then we can show that $\overline{u}_{i,1} = 0$ and that $y_i = u_{i,0} + u_{i,1}x^p$ for any $i \geqq s_1 + 1$. We have already shown that $y_i = u_{i,0}$ for any $i \geqq s_0 + 1$. Hence we have $s_1 \leqq s_0$. If it is not the case that $\overline{u}_{i,1} = 0$ and $y_i = u_{i,0} + u_{i,1}x^p$ for some $s_1 + 1 \leqq i \leqq s_0$, we can easily see that $\deg y_i \geqq p + (p - t)$. Moreover we have, for such i,

$$\begin{cases} y_i - \sum_{j=1}^{s_1} c_j^{(1)} y_j - \sum_{j=1}^{s_0} c_j^{(2)} y_j x^p = v_{i,0} + v_{i,1}x^p + x^{2p} z_i , \\ \deg v_{i,0} , \ \deg v_{i,1} \leqq p - 1 , \qquad \overline{v}_{i,1} = 0 , \end{cases}$$

for suitable constants c_j of k. By the same method we can show that z_i must be zero. Therefore we have

$$y_i - \sum_{j=1}^{s_1} c_j^{(1)} y_j - \sum_{j=1}^{s_0} c_j^{(2)} y_j x^p = v_{i,0} + v_{i,1}x^p .$$

But we have

$$\deg (v_{i,0} + v_{i,1}x^p) < p + (p - t) \leqq \deg y_i \leqq \deg \left(y_i - \sum_{j=1}^{s_1} c_j^{(1)} y_j - \sum_{j=1}^{s_0} c_j^{(2)} y_j\right),$$

which is a contradiction.

By the above procedure we take the sets $S_1, S_2, \ldots, S_r$ with

$$S_j = \{\overline{u}_{1,j}, \ldots, \overline{u}_{s_j,j}\},$$

and put $S = S_1 \cup \ldots \cup S_r$. Thus we have a set of independent solutions $y_1, \ldots, y_n$ of the following type

$$y_i = u_{i,0} + u_{i,1}x^p + \ldots + u_{i,r_i}x^{r_i p}, \qquad (1 \leqq i \leqq n),$$

$$u_{i,0} \neq 0, \qquad u_{i,r_i} \neq 0,$$

$$\overline{u}_{i,0}, \overline{u}_{i,1}, \ldots, \overline{u}_{i,r_i-1} \in S, \qquad \overline{u}_{i,r_i} \neq 0.$$

Moreover, if we note that the elements $\deg y_i$ are mutually incongruent modulo p, we may assume $\deg u_{i,r_i} \leqq p-i-t$. And we have $r_1 + \ldots + r_n \leqq t$ by $\sharp S \leqq t$. Hence we have the following inequality

$$\sum_{i=1}^{n} \deg y_i \leqq \sum_{i=1}^{n} \left((p-i-t) + r_i p\right) = n(p-t) - \frac{n(n+1)}{2} + tp$$

$$= (n+t)p - \left(nt + \frac{n(n+1)}{2}\right).$$

To prove the other inequality we shall use the Wronskian. For n solutions $y_1, \ldots, y_n$ of $(1)_p$ we put

$$A(x) = \begin{pmatrix} y_1 & \cdots & y_n \\ y_1' & \cdots & y_n' \\ \cdots\cdots & \cdots & \cdots\cdots \\ y_1^{(n)} & \cdots & y_n^{(n)} \end{pmatrix}.$$

Let $c_0(x), \ldots, c_n(x)$ be the minors of degree n of $A(x)$. Then we have

$$c_0(x)y_i^{(n)} - c_1(x)y_i^{(n-1)} + \ldots \pm c_n(x)y_i = 0 \qquad (1 \leqq i \leqq n),$$

since

$$\begin{vmatrix} & & y_i \\ & A(x) & y_i' \\ & & \vdots \\ & & y_i^{(n)} \end{vmatrix} = 0.$$

In particular, $c_0(x)$ is the Wronskian $W(y_1, \ldots, y_n)$ of $y_1, \ldots, y_n$. We put

$$(c_0(x), \ldots, c_n(x)) = d(x).$$

Now we consider the linear equation $(X_0 \dots X_n)A(x) = 0$. As the rank of $A(x)$ is equal to n, the dimension of the space of solutions is one. But $(a_n(x), \dots, a_0(x))$ and $(\pm c_n(x), \dots, c_0(x))$ are solutions of this linear equation. Hence we have

$$a_0(x) = \frac{c_0(x)}{d(x)} .$$

Therefore we have the following inequality:

$$t + n = \deg a_0(x) \leqq \deg W(y_1, \dots, y_n)$$

$$\leqq g_{i_1} + (g_{i_2} - 1) + \dots + (g_{i_n} - n + 1) = g - \frac{n(n-1)}{2},$$

i.e.,

$$g \geqq t + \frac{n(n+1)}{2} .$$

Thus we have completed the proof of the theorem.

EXAMPLE. In the case $p = 5$, $n = 2$ and $t = 1$, the differential equation

$$(x^3 + 1)y'' + x^2 y' + xy = 0$$

has independent solutions

$$\begin{cases} y_1 = x^3 - 1 , \\ y_2 = x^7 - x^4 + x . \end{cases}$$

This pair of solutions attains the minimal value of $g = \deg y_1 + \deg y_2$ and

$$g = 10 = (t+2)p - (2t+3) .$$

Appendix. Correspondences of terminologies with Katz's theory.

In order to clarify the correspondences of terminologies between our theory and Katz's theory, we shall give a brief explanation of Katz's paper: *Nilpotent connections and the monodromy theorem; applications of a result of Turrittin*; just as much as necessary for this purpose. For more detailed results the reader should consult the original paper.

Let k be a field of characteristic $p > 0$ and let $k[x]$ be the ring of polynomials of one variable over k. For a fixed $f = f(x) \in k[x]$, we put $S = \operatorname{Spec} k[x]_f$. Regarding $k[x]_f^n$ as a global section over S, we obtain a free sheaf M over S naturally. Moreover, we denote by $\operatorname{Der}(S/k)$ the sheaf of derivations and by $\operatorname{End}_k(M)$ the sheaf of k-linear endomorphisms of M.

DEFINITION. Let $\nabla: \operatorname{Der}(S/k) \to \operatorname{End}_k(M)$ be an O_S-linear mapping. We call this ∇ a *k-connection* of M provided it satisfies the equation

$$\nabla(D)(fe) = D(f)\,e + f\,\nabla(D)(e)\,,$$

for arbitrary sections D, f and e of, respectively, $\operatorname{Der}(S/k)$, S and M, over a suitable open set of S.

For any section D of $\operatorname{Der}(S/k)$, D^p is also a derivation. Hence $\nabla(D^p)$ can be defined.

DEFINITION. We define the mapping $\psi_\nabla: \operatorname{Der}(S/k) \to \operatorname{End}_k(M)$ by

$$\psi_\nabla(D) = (\nabla(D))^p - \nabla(D^p)\,.$$

We call this ψ the *p-curvature* of ∇.

$\nabla(D)$ is a k-linear mapping. Moreover one can show that $\psi_\nabla(D)$ is, in fact, an O_S-linear mapping.

DEFINITION. We say that ψ is *nilpotent* if there exists a natural number m such that ψ satisfies the following equation for all sections $D_1, \ldots, D_m$ of $\operatorname{Der}(S/k)$:

$$\psi_\nabla(D_1) \ldots \psi_\nabla(D_m) = 0\,.$$

The dimension of the space of derivations is one. Hence ψ is nilpotent if and only if $\psi_\nabla(D)$ is nilpotent. In other words, select a basis e of M, and set

$$\psi(D)\,e = Be$$

for a suitable matrix B. Then $\psi(D)$ is nilpotent if and only if B is a nilpotent matrix.

It can be shown that ψ is p-semilinear, *i.e.*, that $\psi_\nabla(SD) = S^p \psi_\nabla(D)$. So, if $\psi_\nabla(d/dx)$ is nilpotent, then ψ_∇ is nilpotent.

Next, we consider the relations with the differential equations.

We put $\check{M} = \operatorname{Hom}_{O_S}(M, O_S)$ and denote by $\langle\,,\,\rangle$ an inner product of M and $\check{M}$. Taking sections D, m and $\check{m}$ of $\operatorname{Der}(S/k)$, M and $\check{M}$

respectively, over a suitable open set, we define a k-connection $\check{\nabla}$ of $\check{M}$ by the following equation:

$$(*) \qquad \langle \nabla(D)(m), \check{m}\rangle + \langle m, \check{\nabla}(D)(\check{m})\rangle = D(\langle m, \check{m}\rangle)\,.$$

Then we can easily see that $\check{\nabla}$ is k-linear and that $\check{\nabla}$ is a connection of $\check{M}$. We call this $\check{\nabla}$ the *dual* connection of ∇. From

$$\langle \psi_\nabla(D)m, \check{m}\rangle + \langle m, \psi_{\check{\nabla}}(D)\check{m}\rangle = 0$$

we can see that ψ_∇ is nilpotent if and only if so is $\psi_{\check{\nabla}}$.

Now, for a basis $e = \langle e_0, \ldots, e_{n-1}\rangle$ of $\Gamma(M, S) = k[x]_f^n$, we put $\nabla(d/dx)e = Ae$, where A is a matrix of $M_n(k[x]_f)$. Let

$$\check{e} = \langle \check{e}_0, \ldots, \check{e}_{n-1}\rangle$$

be the dual basis of e. We next ask when an element

$$\sum_{i=0}^{n-1} f_i e_i\,, \qquad \text{where } f_i \in k[x]_f\,,$$

is annihilated by $\check{\nabla}(d/dx)$. After substituting the $\check{m}$ of $(*)$ with the above element, we can see that this happens when the following equation is satisfied:

$$\begin{pmatrix} f_0' \\ \vdots \\ f_{n-1}' \end{pmatrix} = A \begin{pmatrix} f_0 \\ \vdots \\ f_{n-1} \end{pmatrix}.$$

We call the above equation the differential equation *corresponding* to ∇. Of course, this differential equation depends on the choice of basis. Reciprocally, if a system of differential equations is given, we can construct a connection from it. In particular, if we take a basis of type

$$\nabla\left(\frac{d}{dx}\right)e_i = e_{i+1}\,, \qquad 0 \leqq i \leqq n-2\,,$$

$$\nabla\left(\frac{d}{dx}\right)e_{n-1} = \sum_{i=0}^{n-1} d_i e_i\,, \qquad d_i \in k[x]_f\,,$$

then ∇ corresponds to the following ordinary differential equation:

$$\begin{cases} f_i' = f_{i+1}\,, & 0 \leqq i \leqq n-2\,, \\ f_0^{(n)} - d_1 f_0^{(n-1)} - \ldots - d_{n-1} f_0 = 0\,. \end{cases}$$

And the roots of the polynomial f, which is used to construct the gradient ring $k[x]_f$, correspond to singular points of the differential equation.

PROPOSITION. *The differential equation*

$$(1)_p \qquad a_0(x)y^{(n)} + a_1(x)y^{(n-1)} + \cdots + a_n(x)y = 0\,, \qquad a_i(x) \in k[x]$$

has sufficiently many solutions in a weak sense if and only if the connection

$$\nabla\left(\frac{d}{dx}\right)e = \begin{pmatrix} 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 1 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 & 1 \\ -a_1/a_0 & \cdot & \cdot & \cdot & \cdot & -a_n/a_0 \end{pmatrix}$$

has a nilpotent p-curvature.

PROOF. We suppose that ψ_∇ is nilpotent. Then $\psi_{\check{\nabla}}$ is also nilpotent. And we have $\psi_{\check{\nabla}}(d/dx) = (\check{\nabla}(d/dx))^p$ by $(d/dx)^p = 0$. Hence if we put

$$V_i = \left\{ \check{e} \in \check{M} \,\middle|\, \left(\check{\nabla}\left(\frac{d}{dx}\right)\right)^i \check{e} = 0 \right\} \qquad (i \geqq 0)\,,$$

then V_i is a k-linear vector space. Moreover, we have $V_p \neq 0$ from the nilpotency of $(\check{\nabla}(d/dx))^p$. Thus we have

$$\{0\} \neq V_p \supset V_{p-1} \supset \cdots \supset V_0 = \{0\}\,.$$

Therefore, there exists a natural number i such that

$$V_{i+1} \neq \{0\}\,, \qquad V_i = \{0\}\,.$$

Let $\check{e}_0$ be a non-zero element of V_{i+1}. Then we have

$$\left(\check{\nabla}\left(\frac{d}{dx}\right)\right)^{i+1} \check{e}_0 = 0\,, \qquad \left(\check{\nabla}\left(\frac{d}{dx}\right)\right)^{i} \check{e}_0 \neq 0\,.$$

Hence, if we put $\check{e}_1 = (\check{\nabla}(d/dx))^i \check{e}_0$ we have

$$\check{\nabla}\left(\frac{d}{dx}\right)\check{e}_1 = 0\,.$$

Therefore there exists a non-trivial solution. We denote this solution by $y_1 \in k[x]$. We next put $y = y_1 u$. Then we have

$$\begin{pmatrix} y \\ y' \\ \vdots \\ y^{(n-1)} \end{pmatrix} = \begin{pmatrix} y_1 & & & \\ y_1' & y_1 & & 0 \\ y_1'' & 2y_1' & y_1 & \\ \vdots & \vdots & & \ddots \\ \cdot & \cdot & \cdot & y_1 \end{pmatrix} \begin{pmatrix} u \\ u' \\ \vdots \\ u^{(n-1)} \end{pmatrix}.$$

We denote this matrix by B. Let e be a basis of M such that

$$\nabla\left(\frac{d}{dx}\right) e = Ae\,,$$

where A is the matrix given in the statement, and set $Be_1 = e$. Then we have

$$\nabla\left(\frac{d}{dx}\right) Be_1 = Ae = ABe_1\,.$$

On the other hand we have

$$\nabla\left(\frac{d}{dx}\right) Be_1 = B' e_1 + B\nabla e_1$$

by the definition of connection. Hence we have

$$\nabla e_1 = B^{-1}(AB - B')\, e_1\,,$$

and this gives the differential equation with respect to $(u, u', \ldots, u^{(n-1)})$. As y_1 is a solution of $(1)_p$, we see that

$$AB - B' = \begin{pmatrix} 0 & y_1' & \cdots & y_1' \\ \vdots & & * & \\ 0 & & & \end{pmatrix},$$

i.e. that

$$B^{-1}(AB - B') = \begin{pmatrix} 0 & * \\ \vdots & C_{n-1} \\ 0 & \end{pmatrix}.$$

This matrix C_{n-1} gives a new connection which corresponds to the

differential equation with respect to u'. We can easily see that this connection is also nilpotent by the nilpotency of ψ_∇.

Thus the discussion is reduced to the case $n = 1$ by induction. But we have already proved the case $n = 1$.

Reciprocally, if $(1)_p$ has sufficiently many solutions in a weak sense, then the proof of the proposition can be inductively achieved by the same method. Let us study the case $n = 1$. In this case there exists an element $\check{e}$ of $\check{M}$ such that

$$\check{\nabla}\left(\frac{d}{dx}\right)\check{e} = 0 .$$

Hence we have

$$\left(\check{\nabla}\left(\frac{d}{dx}\right)\right)^p\check{e} = 0 .$$

As $\psi_{\check{\nabla}}(d/dx) = (\check{\nabla}(d/dx))^p$ is O_S-linear, we see that $\psi_{\check{\nabla}}$ is zero.

In general, it is known that the p-curvature is zero if and only if the differential equation has n independent solutions (N. Katz).

From the above proof we can see that, in the definition 2 of § 2, if the new differential equation with respect to u has sufficiently many solutions in a weak sense for a solution $y_1 \in k[x]$, then, for any other solution, the new differential equation has also sufficiently many solutions in a weak sense.

Now, in his paper, Katz defines regular singular points in characteristic zero. But his definition is essentially equivalent to that of our paper. For a Fuchsian type connection ∇, its indicial equation depends on the differential equation associated with ∇. But the exponents are invariant modulo $\boldsymbol{Z}$. Therefore, it is meaningful to say that the exponents are rational. In such case ∇ is said to be *quasi-unipotent.*

If we take $S = \operatorname{Spec} \boldsymbol{Z}[x]_f$, we can consider the reduction modulo p. If a connection ∇ is nilpotent for any reduction modulo p, then ∇ is said to be *globally nilpotent.* Katz showed that if ∇ is globally nilpotent, then ∇ is of Fuchsian type and quasi-unipotent (which is confirmed in the corollary to Theorem 2 of § 2 in our paper).

For a more general S the reader should consult the original paper. In addition to the above results, it is shown in that paper that a Gauss-Manin connection is globally nilpotent.

Testo pervenuto il 9 aprile 1979.
Bozze licenziate il 4 marzo 1980.

REFERENCES

[1] T. Honda, *Formal groups and zeta functions*, Osaka J. Math., 5 (1968), 199-213.
[2] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan, 22 (1970), 213-246.
[3] T. Honda, *Differential equations and formal groups*, U.S.-Japan Seminar on modern methods in number theory, Tokyo, 1971.
[4] T. Honda, *Formal groups obtained from generalized hypergeometric functions*, Osaka J. Math., 9 (1972), 447-462.
[5] N. Katz, *On the differential equations satisfied by period matrices*, Publ. Math. I.H.E.S., 35 (1968).
[6] N. Katz, *Nilpotent connections and the monodromy theorem; applications of a result of Turrittin*, Publ. Math. I.H.E.S., 39 (1970), 355-412.
[7] N. Katz, *Algebraic solutions of differential equations (p-curvature and the Hodge filtration)*, Inv. Math., 18 (1972), 1-118.
[8] E. R. Kolchin, *On the exponents of differential ideals*, Ann. of Math., 42 (1941), 740-777.