Applications of Padé approximations to the Grothendieck conjecture on linear differential equations

D.V. Chudnovsky*, G.V. Chudnovsky*

Department of Mathematics, Columbia University
New York, New York 10027

To Professor Bers on his 70th birthday.

Introduction

The Grothendieck conjecture [1], [2] predicts the global algebraic behavior of solutions of linear differential equations, provided that these equations have "sufficiently many" solutions after reductions (mod p) for almost all primes p. In-depth studies of this conjecture and its interesting generalizations belong to Katz [1], [3]. For example, Katz [3] showed that from the universal truth of the Grothendieck conjecture follows the description of a Lie algebra of a Galois group of a linear differential equation in terms of the operators of its p-adic curvature. The Grothendieck conjecture remains open in many crucial cases. Among the most important cases, pointed out in [1], [4] are the case of rank one equations over an elliptic curve and the case of Lamé equations. The general problem of the proof of the Grothendieck conjecture for arbitrary rank one equations over an algebraic curve is formulated as a question (I log) in [1].

In this report we apply methods of Padé approximations to study the Grothendieck conjecture in many important cases. Our methods were inspired by our similar studies of G-function properties [5], and one can find many similarities between our present approach and the one used earlier in [6]. In our proofs of particular cases of the Grothendieck conjecture we establish the algebraicity of $f(x)$ by considering the Padé approximations to $f(x)^j$: $j = 0,1,\dots$ and comparing the analytic properties of Padé approximations with the heights of the coefficients of Padé approximants (determined using the assumptions of the Grothendieck conjecture). In our results we assume that the solutions of linear differential equations can be uniformized using meromorphic functions in $\mathbb{C}^n$ of finite order of growth. This assumption determines the scope of applications of the presented methods.

*)This work was supported in part by the U.S. Air Force, Grant AFOSR-81-0190.

Among the results proved in this paper is the proof of the Grothendieck conjecture for arbitrary rank one equations over algebraic curves of any genus $g \geq 0$. We also prove the Grothendieck conjecture for the class of Lamé equations, thus solving Dwork's problem [4].

The exposition is, essentially, self-contained. We assume little knowledge of algebraic number theory and elementary complex analysis. In order to follow a completely elementary style, we avoided cohomology language and connections. In this respect the papers of Honda [2], Dwork [4] and Dwork-Robba [7] were particularly useful to us.

Our methods, derived from our G-function work [5], have good chances of being useful in more complicated situations, including other cases of the Grothendieck conjecture and applications to problems of diophantine geometry. We shall return to this subject in further reports.

The paper is organized as follows. In §§1-2 we have collected various properties of linear differential equations over $\bar{\mathbb{Q}}(x)$ in the p-adic domain and after reduction (mod p). These include the characterization of equations with the global nilpotence property (having "sufficiently many solutions in a weak sense" (mod p) for almost all p) and Katz's result on their Fuchsianity and the finitness of the local monodromy for equations satisfying the assumptions of the Grothendieck conjecture. Particularly important for our purposes are bounds on denominators of power series expansions of solutions of equations, satisfying the assumptions of the Grothendieck conjecture given in Corollary 2.5. In §3 we formulate the Grothendieck conjecture and present Honda's [2] proof that the Grothendieck conjecture for rank one equations over rational function fields is elementary equivalent to the important case--Principle (C)--of the Chebotarev theorem. In §4 we prove the Grothendieck conjecture for rank one equations over $\bar{\mathbb{Q}}(x)$ (and, thus, the Principle (C)) using Hermite's system of Padé approximations to binomial functions. Then, in §5 we prove Main Theorem 5.2, which relates the algebraicity (transcendence)of a function $f(x_1,\dots,x_g)$, that can be uniformized by meromorphic functions of finite order of growth in $\mathbb{C}^g$, to the growth of denominators of coefficients in the expansions of $f(x_1,\dots,x_g)^i$: $i = 1,2,\dots$. Main Theorem 5.2 is applied in §§6-8. In §6 we prove the Grothendieck conjecture for rank one equations $df = \omega f$ over an elliptic curve E for an elliptic differential ω on E. We also touch upon the problems of the distribution of supersingular and anomalous primes. §7 is devoted to the solution of Dwork's problem on the characterization of all globally nilpotent cases of Lamé equations. In §8 we use the solution of the Jacobi-Abel inversion problem and the Abelian functions on the Jacobian of an algebraic curve of genus $g \geq 1$. This leads to the proof of the Grothendieck conjecture for rank one equations over arbitrary algebraic curves. In the conclusion we discuss the problem of effectiveness and further generalizations of our results.

§1. Linear Differential Equations (mod p).

Let us present a short exposition of the p-adic properties of linear differential equations connected with the Grothendieck conjecture. We follow in this exposition the works of Dwork [4], Dwork-Robba

[7], Katz [1], [3], [8] and Honda [2]. Since our language is elementary, we rely mainly on Honda's [2] translation of connections' formulation into a standard differential equations setting.

The linear differential equations we consider are defined over a rational function field $K(x)$ for an algebraic number field K and over their reductions (mod p). Here and everywhere in this section, K denotes an algebraic number field over $\mathbb{Q}$, and, for a prime ideal $\wp$ of K, $\bar{K}_{\wp}$ denotes the residue field of K (mod $\wp$). Also we denote by k, a field of characteristic $p > 0$, by $k[x]$, the ring of polynomials in x over k, by $k[[x]]$, the ring of formal power series in x over k, and by $k(x)$ and $k((x))$, respectively, the quotient fields of $k[x]$ and $k[[x]]$. We consider $k((x))$ to be a differential field with the standard differentiation in x: $\alpha' = 0$ for $\alpha \in k$ and $(x^n)' = n \cdot x^{n-1}$. Consequently, the field of constants of $k((x))$ is $k((x^p))$.

We start with a linear differential equation over $K(x)$:

$$(1.1) \qquad a_n(x)y^{(n)}(x) + \dots + a_1(x)y'(x) + a_0(x)y(x) = 0,$$

$a_i(x) \in K[x]$ $(i = 0,\dots,n)$ and its reductions (mod $\wp$) in $\bar{K}_{\wp}(x)$, denoted by $(1.1)_{\wp}$. Thus, together with (1.1), we consider a linear differential equation over $k(x)$:

$$(1.1)_p \qquad a_n(x)y^{(n)}(x) + \dots + a_0(x)y(x) = 0 \text{ for}$$

$$a_i(x) \in K[x]: (i = 0,\dots,n).$$

Clearly, if $(1.1)_p$ has a solution in $k((x))$, then, after multiplication by a constant, it has a solution in $k[[x]]$.

We say that the equation $(1.1)_p$ has sufficiently many solutions, if $(1.1)_p$ has n linearly independent solutions in $k[[x]]$.

The definition of "sufficiently many solutions in the weak sense" proceeds by induction in the rank(order) n of the equation $(1.1)_p$. If $n = 1$, we say that $(1.1)_p$ has sufficiently many solutions in a weak sense, if $(1.1)_p$ has a non-zero solution. By induction in n, we say that $(1.1)_p$ has sufficiently many solutions in a weak sense, if: a) $(1.1)_p$ has a non-zero solution $y_1 \in k[x]$; b) for an arbitrary solution y_1 from a) and a new differential variable u, $u = y/y_1$, the differential equation obtained from $(1.1)_p$ by the substitution $y = y_1 \cdot u$ and having rank $n-1$ in u', has sufficiently many solutions in a weak sense.

The notions of "sufficiently many solutions (in a weak sense)" can be reformulated in the more traditional language of zero and nilpotent p-curvature.

These notions are also connected with the Fuchsianity (or regular singularity) of differential equations. Namely, for an equation $(1.1)_p$ we call a zero α of $a_n(x)$ a regular singularity, if $(x-\alpha)^{m-i}$ divides

$a_{n-i}(x)$, whenever m is the largest exponent such that $(x-\alpha)^m$ divides $a_n(x)$. Similarly, $x = \infty$ is called a regular singularity of $(1.1)_p$, if the degree of $a_i(x)$ is at most $\deg_x(a_n(x)) - n + i$ $(i = 0,\ldots,n)$. The equations $(1.1)_p$ is called Fuchsian, if all the roots of $a_n(x) = 0$ and $x = \infty$ are regular singularities of $(1.1)_p$.

It is easy to prove by induction, following this definition, the next result (Honda [2], Theorem 1):

Theorem 1.1: If $(1.1)_p$ has sufficiently many solutions in a weak sense, then $(1.1)_p$ is Fuchsian.

Clearly, comparing the p-adic and the usual definitions of Fuchsianity [9], the equation (1.1) is Fuchsian if and only if infinitely many (or almost all) of its reductions $(1.1)_{\mathcal{P}}$ are Fuchsian. Hence we have Katz's [8] result:

Corollary 1.2: If $(1.1)_{\mathcal{P}}$ has sufficiently many solutions in a weak sense for infinitely many prime ideals $\mathcal{P}$ of K, then the equation (1.1) is Fuchsian.

Another of Katz's famous results [8] states that equation (1.1), for which $(1.1)_{\mathcal{P}}$ has sufficiently many solutions is a weak sense for almost all $\mathcal{P}$, has all exponents at regular singularities, being rational numbers. To prove this result we need one form of Chebotarev's density theorem that will be proved below by means of Padé approximations. This version (or rather a corollary of) Chebotarev's density theorem is itself equivalent to the simplest case of the Grothendieck conjecture, as was demonstrated by Honda [2].

The corollary of the Chebotarev's density theorem that we use is the following result (asserted by Kronecker):

Principle (C): If a polynomial in $K[x]$ is completely decomposable (mod $\mathcal{P}$) for almost all $\mathcal{P}$, then it is completely decomposable in $K[x]$.

This principle can be reformulated in the language of ideals, if we use the following version of Hensel's lemma known as Kummer's theorem:

Let $f(x) \in K[x]$ be an irreducible polynomial and θ be a zero of $f(x)$. Then for a prime ideal $\mathcal{P}$ of K, almost all $\mathcal{P}$ are decomposable in $K[\theta]$ in the same way as $f(x)$ is decomposable into factors over $\bar{K}_{\mathcal{P}}[x]$.

By considering the principle (C) and the Kummer theorem in the rational number case we arrive at the following algebraic statement, equivalent to (C):

Principle (C_1). 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.

As we shall see later in Theorem 3.1, the principles (C) or (C_1) are equivalent to the validity of the Grothendieck conjecture for rank one equations over $K(x)$. As such, principles (C)-(C_1) shall get their Padé approximation (elementary) proofs in §4 .

We remind the reader that an indicial polynomial of a Fuchsian linear differential equation (1.1) at a regular singularity $x = \alpha$ (i.e. at a zero α of $a_n(x)$) is defined as a polynomial $f(x)$ of degree n such that the substitution of $y = (x-\alpha)^{\nu} + \Sigma_{m=1}^{\infty} c_m(x-\alpha)^{\nu+m}$ in (1.1) gives a power series in $(x-\alpha)$, whose coefficient at $(x-\alpha)^{\nu}$ vanishes if and only if $f(\nu) = 0$.

The equation $f(\nu) = 0$ is called the indicial equation of (1.1) at a regular singularity $x = \alpha$, and its roots are called exponents of (1.1) at $x = \alpha$.

Proposition1.3[2]:If $(1.1)_p$ has sufficiently many solutions in a weak sense, then its indicial equations at every regular singularity have precisely n roots in the prime field.

Proof: If $n = 1$, then $(1.1)_p$ has a non-zero solution in $k[[x]]$ according to the assumption which implies the proposition. Let us assume that the proposition is true for every equation of rank of at most $n - 1$. Let $x = \alpha$ be a regular singularity of $(1.1)_p$. Then $(1.1)_p$ can be represented in the form

$$b_n(x)\cdot(x-\alpha)^n y^{(n)}(x) +\ldots+ b_0(x)y(x) = 0, \quad b_n(\alpha) \neq 0.$$

Then the indicial polynomial at $x = \alpha$ has the form $f_1(\nu) = b_n(\alpha)\nu\ldots(\nu-n+1) +\ldots+ b_0(\alpha)$. Now we take a solution $y_1(x)$ lf $(1.1)_p$ in $k[x]$, $y_1(x) = (x-\alpha)^m\cdot z_1(x)$, $z_1(\alpha) \neq 0$. Then the differential equation obtained by substituting $y = y_1\cdot u$ in $(1.1)_p$ has sufficiently many solutions in a weak sense. Then the indicial polynomial of a new differential equation with respect to u has the form $f_2(\nu) = f_1(\nu+m)$. Let us denote by $f_3(\nu)$ the indicial polynomial of a differential equation of rank $n-1$ for u'. Then by induction assumptions, all zeroes of $f_3(\nu)$ belong to a prime field, while $f_2(\nu) = \nu\cdot f_3(\nu)$. Hence all zeroes of $f_1(\nu)$ also belong to the prime field, and the proposition is proved.

Combining Principle (C) with Proposition 1.3 we arrive at

Corollary 1.4 (Katz): If $(1.1)_{\mathcal{P}}$ has sufficiently many solutions in a weak sense for almost all $\mathcal{P}$, then all exponents at regular singularities of (1.1) are rational numbers.

We note that all of these statements have their elementary proofs in our paper, because Principle (C) is proved below in §4 as part of our solution of the Grothendieck conjecture in the rank one case.

Corollary 1.4 does not imply that the local monodromy is always finite at every regular singularity under the assumptions of Corollary 1.4, because there might be logarithmic terms (when exponents differ by integers). Nevertheless the monodromy is locally finite for any equation (1.1), for which $(1.1)_{\mathcal{P}}$ has sufficiently many solutions for almost all $\mathcal{P}$. In fact, the following statement is immediately clear, if Corollary 1.4 is taken into account:

Proposition 1.5: Let $(1.1)_{\mathcal{P}}$ have sufficiently many solutions in $\bar{K}_{\mathcal{P}}[x]$, then n exponents of $(1.1)_{\mathcal{P}}$ at any regular singularity are all distinct (mod $\mathcal{P}$). If $(1.1)_{\mathcal{P}}$ has sufficiently many solutions for almost all $\mathcal{P}$, then n exponents at regular singularities are distinct rational numbers.

Following Honda [2], we can prove the following:

Proposition 1.6 (Katz): Let $(1.1)_{\mathcal{P}}$ have sufficiently many solutions in $\bar{K}_{\mathcal{P}}[x]$ for almost all $\mathcal{P}$. Then the local monodromy of (1.1) is finite and cyclic in the neighborhood of any point.

Proof: It is sufficient to prove the proposition for regular singular points of (1.1). Let, say, $x = 0$ be a regular singularity of (1.1) with exponents $\nu_1,\ldots,\nu_n$. According to Proposition 1.5 ν_i are distinct rational numbers. We have to show that for $\nu = \nu_i$ there exists a solution of (1.1) of the form $y(x) = x^{\nu}(1 + \Sigma_{m=1}^{\infty} c_m x^m)$. This clearly implies that the monodromy group of (1.1) is generated by the matrix $\mathrm{diag}(e^{2\pi i\nu_1},\ldots,e^{2\pi i\nu_n})$ of finite order. Let $f(x)$ be an indicial polynomial of (1.1) (with roots ν_i). Then, by substituting $y(x)$ into (1.1), we obtain the following recurrence on coefficients c_m:

$$(1.2) \qquad f(\nu+m)c_m = \Sigma_{i>0} A_{m,i}c_{m-i} + A_{m,0}$$

for some constants $A_{m,j}$. Whenever $\nu_i - \nu_j$ is a (negative) integer, the system (1.2) does not determine $c_{\nu_j-\nu_i}$. Thus, for $N \geq \max_{j\neq i}(\nu_j-\nu_i)$, if we can find a $y_0 = x^{\nu}.(1 + \Sigma_{m=1}^{N} c_m x^m)$, for which

$$(1.3) \qquad L[y_0] \overset{\mathrm{def}}{=} a_n(x)y_0^{(n)} +\ldots+ a_0(x)y_0 = O(x^{\nu+N+1}),$$

then we can find the solution y of (1.1) using the recurrence (1.2) for $m > N$. The condition (1.3) is to be understood in terms of power series expansions. The condition (1.3), according to (1.2), is equivalent to a certain system $A\bar{c} = \bar{b}$ of linear equations on $\bar{c} = (c_1,\ldots,c_N)$ with constant matrices A and $\bar{b}$ (with coefficients from K). To show that this system of equations has a solution in K, it is sufficient to show that for almost all (or infinitely many) $\mathcal{P}$'s this system has solutions (mod $\mathcal{P}$). Let us take such $\mathcal{P}$ for which $(1.1)_{\mathcal{P}}$ has sufficiently many solutions. According to Propositions 1.3 and 1.5, we have a nonnegative integer ν such that $(1.1)_{\mathcal{P}}$ has a solution $y_0^*(x) = x^{\nu}(1 + \Sigma_{m=1}^{\infty} c_m^* x^m) \in \bar{K}_{\mathcal{P}}[[x]]$ with $\nu_i \equiv \nu(\mathrm{mod}\ \mathcal{P})$. Hence

$L_0[y_0^*] = O(x^{\nu+N+1})$ and $\bar{c}^* = (c_1^*,\dots,c_N^*)$ is a solution of $A\bar{c}^* \equiv \bar{b}$ (mod $\mathcal{P}$). Consequently (1.3) has a nontrivial solution and (1.1) has a nonlogarithmic solution with an exponent ν_i. Proposition 1.6 is proved.

§2. P - curvature and the denominators problem.

Our purpose now is to determine the bounds for the denominators of power series expansions of functions belonging to K[x]-modules generated by symmetric powers of solutions of linear differential equations with nilpotent p-curvature for almost all p. We follow mainly the papers of Dwork [4] and Dwork and Robba [7], [10]. As above, we start with a linear differential operator over K[x] for an algebraic number field K:

$$(2.1) \qquad L \overset{\mathrm{def}}{=} \Sigma_{i=0}^{n} a_i (\frac{d}{dx})^i$$

for $a_i = a_i(x) \in K[x]$: $i = 0,\dots,n$. According to Corollary 1.2, a linear operator L is of Fuchsian type (and according to Corollary 1.4, exponents at regular singularities are rational integers). We are interested in the differential ideal generated by L. It is obvious that for $a_0 \neq 0$, all derivatives $(d/dx)^i$ are expressed as linear combinations of $(d/dx)^j$, $j = 0,\dots,n-1$ with coefficients from $K(x)$, modulo the ideal generated by L, i.e. mod $K(x)[d/dx]\cdot L$. In fact, we have $(d/dx)^n = -\Sigma_{i=0}^{n-1} a_i/a_n\cdot(d/dx)^i + 1/a_n L$. Thus, we have for $m \geq 0$,

$$(2.2) \qquad (\frac{d}{dx})^m \equiv \Sigma_{i=0}^{n-1} H_{m,i}\cdot(\frac{d}{dx})^i \bmod K(x)[\frac{d}{dx}]\cdot L$$

where $H_{m,i} \in K[x]$ $(i = 0,\dots,n-1)$ and satisfy the following inductive properties:

$$H_{m+1,i} = H'_{m,i} + H_{m,i-1} - \frac{a_i}{a_n} H_{m,n-1},$$

$i = 0,\dots,n-1$. In particular, all rational functions $H_{m,i}$ belong to a differential ring generated by a_i/a_n: $i = 0,\dots,n$ over $\mathbb{Z}$. Thus rational functions $H_{m,i}$ are p-integral (or $\mathcal{P}$-integral) for almost all p (or $\mathcal{P}$). The rational functions $H_{m,i}$ can be used to determine an expansion of an arbitrary solution of an equation $Ly = 0$ in the neighborhood of an arbitrary (regular) point. To study the p-adic properties of these expansions, we introduce a "generic" p-adic point. Following Dwork, for any prime p, this is a generic point t, generating a transcendental extension of $\mathbb{Q}_p$ such that the residue class of t is transcendental over the prime field $\mathbb{F}_p$, and $|t|_p = 1$. Similarly, for $\mathcal{P}$ lying over p, $|t|_{\mathcal{P}} = 1$. Whenever a prime p is such that $a_n(x)$ has no zeroes in the $\mathcal{P}$-adic unit circle $D(t,1^-)$ and the Gauss norm of $a_i(x)/a_n(x)$ does not exceed 1 $(i = 0,\dots,n-1)$, we have

$|H_{m,i}(t)|_{\text{Gauss}} \leq 1$. In particular, power series solutions $y(x)$ of $Ly = 0$ converge near $x = t$ at a disc $\text{ord}_p(x-t) > 1/(p-1)$. The last observation is a consequence of a trivial bound on a p-adic valuation of $m!$: $\text{ord}_p(m!) = [m/p] + [m/p^2] + \ldots \leq m/(p-1)$.

There is an obvious relationship between the p-divisibility of $H_{m,i}$ and the p-adic radius of the convergence of solutions of $Ly = 0$. Moreover, this relationship is closely connected with the nilpotence of the p-curvature associated with a linear operator L. To state this relationship we need, first, a short translation from Honda's elementary language used above [2] to Katz's [1], [8] connection language. This translation can be found in Honda [2] (appendix), Katz [1], [8] and Dwork [4]:

<u>Proposition 2.1</u>: For an equation $(1.1)_p$ corresponding to the operator $L_p = L(\text{mod } p)$, the existence of sufficiently many solutions (mod p) is equivalent to the annihilation of the p-curvature of L_p. This condition can be expressed as:

$$\left(\frac{d}{dx}\right)^p \equiv 0 \text{ mod } \mathbf{F}_p(x)\left[\frac{d}{dx}\right]\cdot L_p.$$

The existence of sufficiently many solutions of $(1.1)_p$ in a weak sense is equivalent to the nilpotence of the p-curvature of L_p. This last condition means the existence of an integer $\ell \geq 1$ such that

$$\left(\frac{d}{dx}\right)^{\ell p} \equiv 0 \text{ mod } \mathbf{F}_p(x)\left[\frac{d}{dx}\right]\cdot L_p.$$

Moreover, if such $\ell \geq 1$ exists we can always choose $\ell = n$.

In this proposition we, for simplicity, have chosen $K = \mathbb{Q}$. (In general, one has to substitute p for $\mathcal{P}$, a prime field $\mathbf{F}_p$ for a prime field $\bar{K}_{\mathcal{P}}$ and L_p for $L_{\mathcal{P}}$.)

To see why $\ell \leq n$ in the last part of this proposition, and to see the relationship between nilpotence of the p-curvature and p-adic convergence, we borrow the following lemma and its proof from Dwork [4]:

<u>Lemma 2.2 (Katz)</u>: Let L be defined over $\mathbb{Q}[x]$ and $|a_i(x)/a_n(x)|_{\text{Gauss}} \leq 1$ $(i = 0,\ldots,n)$. If all solutions of $Ly = 0$ at the generic point t converge in a nontrivial disk $\text{ord}_p(x-t) > 1/(p-1)-\epsilon$ for some $\epsilon > 0$, then $(d/dx)^{p\cdot n} \equiv 0(\text{mod } \mathbf{F}_p(x)[d/dx]\cdot L_p)$--i.e. the p-curvature of L is nilpotent. Also all solutions of $Ly = 0$ converge in a disk $\text{ord}_p(x-t) > 1/(p-1)-1/(pn)$.

<u>Proof</u>: It follows from the "overconvergence" of solutions of $Ly = 0$ that for all $i = 0,\ldots,n-1$, $|H_{m,i}|_{\text{Gauss}} \to 0$ as $m \to \infty$. This means that

there exists $v \geq 1$ such that $(d/dx)^{pv} \equiv 0(\text{mod } \mathbf{F}_p((x))[D]\cdot L_p)$. Consequently, the p-adic curvature of L_p is nilpotent, and according to Proposition 2.1, the equation $(1.1)_p$ has sufficiently many solutions in a weak sense. According to an inductive definition, this implies that there is a decomposition $L_p = L_1 \ldots L_n$, where L_i are differential operators from $\mathbf{F}_p((x))[d/dx]$ of order one. Thus $(d/dx)^p \equiv 0(\text{mod } \mathbf{F}_p((x))[d/dx]\cdot L_i)$ and, consequently $(d/dx)^{pn} \equiv 0(\text{mod } \mathbf{F}_p((x))[d/dx]\cdot L)$. This implies

$$\text{ord}_p H_{pn,i}(t) \geq 1: i = 0,\ldots,n-1.$$

Applying differentiation we obtain by induction: $\text{ord}_p H_{m,i}(t) \geq [m/pn]: i = 0,1,\ldots,n-1$. This clearly implies the convergence of all solutions of $Ly = 0$ at $x = t$ in the disk $\text{ord}_p(x-t) > 1/(p-1)-1/(pn)$. Lemma 2.2 is proved.

For the study of the Grothendieck conjecture we are interested in the case, when the p-adic curvature of L_p is zero for almost all p (or, according to Proposition 2.1, when equation $(1.1)_p$ has sufficiently many solutions for almost all p).

Lemma 2.3: Let $L \in \mathbb{Q}[x][d/dx]$ and let $L = \Sigma_{i=0}^n a_i(d/dx)^i$, where $a_i = a_i(x)$ $(i = 0,\ldots,n)$ are polynomials with integral coefficients. Let $p \geq n$ be a prime number such that $|a_i/a_n|_{\text{Gauss},p} \leq 1$ for $i = 0,\ldots,n$ and such that the p-curvature of $L_p \equiv L$ (mod p) is zero, i.e. $(d/dx)^p \equiv 0$ (mod $\mathbf{F}_p((x))[d/dx]$). Then for $m \geq 0$, $\text{ord}_p H_{m,i}(x) \geq [m/p]$ $(i = 0,\ldots,n-1)$. In particular, every solution $y(x)$ of $Ly = 0$ converges near $x = t$ at the disk $\text{ord}_p(x-t) > 1/(p(p-1))$. Here for $m \geq n$, $i = 0,\ldots,n-1$, $\text{ord}_p H_{m,i}(x) \geq [m/p]$ means that $a_n(x)^{m-n+1} \times H_{m,i}(x)$ is a polynomial from $\mathbf{Z}[x]$, whose coefficients are all divisible by $p^{[m/p]}$.

Proof: It is clear from the definition of $H_{m,i}$ that $a_n(x)^{m-n+1}\cdot H_{m,i}(x)$ is a polynomial for $m \geq n$, $i = 0,\ldots,n-1$. Then for $m \geq n$,

$$(2.3) \qquad a_n(x)^{m-n+1}\cdot(d/dx)^m$$
$$= \Sigma_{i=0}^{n-1} a_n(x)^{m-n+1}\cdot H_{m,i}(x)\left(\frac{d}{dx}\right)^i (\text{mod } \mathbb{Q}(x)\left[\frac{d}{dx}\right]\cdot L).$$

Here $a_n(x)^{m-n+1}\cdot H_{m,i}(x) \in \mathbf{Z}[x]$ $(m \geq n,\ i = 0,\ldots,n-1)$. We assume that $p \geq n$ and that not all coefficients of the polynomial $a_n(x)$ are divisible by p. Let us assume that the p-curvature of L_p is zero. Then $H_{p,i} \equiv 0 \pmod{\mathbf{F}_p(x))}$, $i = 0,\dots,n-1$ which means that the polynomials $a_n(x)^{p-n+1}\cdot H_{p,i}(x)$ have all their coefficients divisible by p: $i = 0,\dots,n-1$. We now prove by induction that $\mathrm{ord}_p H_{m,i}(x) \geq [m/p]$, $i = 0,\dots,n-1$. This is true by assumption for $m \leq p$. Let us assume that $\mathrm{ord}_p H_{m,i}(x) \geq [m/p]$, $i = 0,\dots,n-1$ for $m \leq pk$, and prove that the same is true for $m \leq p(k+1)$. To do this it is sufficient to apply $(d/dx)^p$ to (2.3) with $m \leq pk$. Then the assumption and $H_{p,i} \equiv 0 \pmod{\mathbf{F}_p(x))}$, $i = 0,\dots,n-1$ clearly imply $\mathrm{ord}_p H_{m,i}(x) \geq [m/p]$, $i = 0,\dots,n-1$ for $m \leq p(k+1)$. An arbitrary solution $y(x)$ of $Ly = 0$ is given by the power series expansion at $x = t$, which is a linear combination of expressions $\Sigma_{m=0}^{\infty} H_{m,i}(t)\cdot(x-t)^m/m!$, $i = 0,\dots,n-1$. This implies the convergence of any such solution in a p-adic disk $\mathrm{ord}_p(x-t) > 1/(p(p-1))$. Lemma 2.3 is proved.

We now explicitly bound the denominators of the power series expansions of solutions of $Ly = 0$ for operators L having p-curvature zero for almost all p. Hence we assume from now on that L_p has p-curvature zero for almost all p. Let S_0 be a set of exceptional primes p, i.e. p such that $p \leq n$ or $|a_i(x)/a_n(x)|_{\mathrm{Gauss},p} > 1$ for some $i = 0,\dots,n-1$ or L_p has a non-zero p-curvature. Then, obviously, S_0 is a finite set. We take an arbitrary algebraic number ξ which is distinct from the singularities of an operator L, i.e. $a_n(\xi) \neq 0$. We expand a set S_0 to a set $S \supseteq S_0$ to contain all primes p for which $|a_n(\xi)|_p \neq 1$. We estimate denominators of coefficients of an expansion of an arbitrary solution $y(x)$ of $Ly = 0$ at $x = \xi$ in terms of S and ξ:

<u>Lemma 2.4</u>: Let, as above, L have p-curvature zero for all $p \notin S$ and let S be defined as above for a regular algebraic point $x = \xi$. Let $y(x) = \Sigma_{m=0}^{\infty} c_m(x-\xi)^m$ be a solution of $Ly = 0$ with algebraic initial conditions $y^{(i)}(\xi) = i!\cdot c_i$: $i = 0,\dots,n-1$ for algebraic $c_0,\dots,c_{n-1}$. Then the common denominator D_m of $\{c_0,\dots,c_m\}$ is bounded by C_0^m, where $C_0 > 1$ depends only on S and ξ. We present the following explicit representation of D_m:

$$D_m = \prod_{p\in S} \alpha^{\mathrm{ord}_\alpha(m!)} \cdot \prod_{p\notin S} p^{\mathrm{ord}_p(m!)-[m/p]}$$
$$\times\ \mathrm{Norm}[a_n(\xi)]^{\max\{0,m-n+1\}} \cdot \mathrm{den}(\xi)^{\max\{0,(\deg(a_n)-1)\cdot(m-n+1)\}d(\xi)}$$

* $\mathrm{Denom}\{c_0,\dots,c_{n-1}\}$, and $\mathrm{den}(\xi)$ is a denominator of ξ, $d(\xi)=[\mathbb{Q}(\xi):\mathbb{Q}]$.

Proof: A power series solution $y(x) = \Sigma_{m=0}^{\infty} c_m(x-\xi)^m$ of $Ly = 0$ with initial conditions $y^{(i)}(\xi) = i!\cdot c_i$: $i = 0,\ldots,n-1$, has the form $y(x) = \Sigma_{i=0}^{n-1} c_i \Sigma_{m=0}^{\infty} H_{m,i}(\xi)\cdot(x-\xi)^m/m!$. According to Corollary 1.2 the equation $Ly = 0$ is Fuchsian, which implies that for $m \geq n$, the polynomials $H_{m,i}(x)\cdot a_n(x)^{m-n+1}$ are polynomials of degree of at most $(\deg(a_n)-1)\cdot(m-n+1)$; $i = 0,\ldots,n-1$. Thus Norm $[a_n(\xi)]^{m-n+1} \times$ $\mathrm{den}(\xi)^{(\deg(a_n)-1)(m-n+1)d(\xi)} \cdot H_{m,i}(\xi)$ is an algebraic integer, $m \geq n$, $i = 0,\ldots,n-1$. Moreover, according to Lemma 2.3, $H_{m,i}(\xi)$ is divisible by $p^{[m/p]}$, whenever $p \notin S$, $i = 0,\ldots,n-1$. This establishes the representation of D_m above. To bound D_m from above we use the explicit formula $\mathrm{ord}_p(m!) = [m/p] + [m/p^2] +\ldots \leq [m/p-1]$. Thus

$$|D_m| \leq \exp\{m\ \Sigma_{p\in S} \frac{\log p}{p-1}\}\cdot\exp\{m\ \Sigma_{p\notin S} \frac{\log p}{p(p-1)}\}$$

$$\times\ |\mathrm{Norm}[a_n(\xi)]|^m \cdot |\mathrm{den}(\xi)|^{m(\deg(a_n)-1)d(\xi)} \leq C_0^M$$

Since $\Sigma_{p>1} \log p/(p(p-1))<\infty$, $|D_m| \leq C_0^m$ for $C_0 > 1$, depending only on S, ξ and $a_n(\xi)$. Lemma 2.4 is proved.

Lemma 2.4 [4], in particular, shows that any solution of an equation $Ly = 0$ with algebraic initial conditions at a regular point is a G-function [5], [6], [11]. Moreover (and this distinguishes between G-functions and solution of equations with zero p-curvatures for almost all p), the same kind of bound for denominators of the coefficients holds for arbitrary powers of solutions of $Ly = 0$:

Corollary 2.5: Let all assumptions be as in Lemma 2.4, and let $y(x) = \Sigma_{m=0}^{\infty} c_m(x-\xi)^m$ be a solution of $Ly = 0$ with $y^{(i)}(\xi) = i!\cdot c_i$, $i = 0,\ldots,n-1$ with algebraic $c_0,\ldots,c_{n-1}$. Let us put $y(x)^j = \Sigma_{m=0}^{\infty} c_{m,j}(x-\xi)^m$: $j = 1,2,\ldots$. Then the common denominator of numbers $\{c_{m_1} \cdots c_{m_j} : m_1 +\ldots+ m_j \leq M;\ j = 1,\ldots,k\}$ and the common denominator of numbers $\{c_{m,j}: m = 0,1,\ldots,M;\ j = 1,\ldots,k\}$ both divide the number

$$\Delta_{M;k} = \prod_{p\in S} p^{[M/(p-1)]} \cdot \prod_{p\notin S} p^{[M/(p(p-1))]} \cdot \mathrm{Norm}[a_n(\xi)]^M \times$$

$$\mathrm{den}(\xi)^{d(\xi)M(\deg(a_n)-1)} \cdot \mathrm{Denom}\{c_0,\ldots,c_{n-1}\}^k.$$

Here $\log|\Delta_{M;k}| \leq M\cdot\{\Sigma_{p\in S} \log p/(p-1) + \Sigma_{p\notin S} \log p/(p(p-1))$

$$+ \log[\,|\mathrm{Norm}(a_n(\xi))|\cdot|\mathrm{den}(\xi)|^{(\deg(a_n)-1)d(\xi)}]\}$$

$$+ N \log|\mathrm{Denom}\{c_0,\dots,c_{n-1}\}| \leq M \log C_1$$

$$+ N \log |\mathrm{Denom}\{c_0,\dots,c_{n-1}\}|.$$

Proof: We have $c_{m,j} = \Sigma_{m_1+\dots+m_j=m} c_{m_1}\cdots c_{m_j}$. Also $\Sigma_{s=1}^{j} \mathrm{ord}_p(m_s!) \leq \mathrm{ord}_p(m!)$, $\Sigma_{s=1}^{j}\{\mathrm{ord}_p(m_s!) - [m_s/p]\} \leq [m/(p(p-1))]$, whenever $m_1 +\dots+ m_j = m$. Combining this with the bound $D_m = \Delta_{m;1}$ of the common denominator of $\{c_0,\dots,c_{m-1}\}$ from Lemma 2.4, we obtain results of Corollary 2.5.

Crucial for applications is the limit case: $\lim\sup_{M\to\infty}|\Delta_{M;k}|^{1/M} \leq C_1$ for any fixed k (see the conditions of Main Theorem 5.2).

We remark that the result of Corollary 2.5 holds for an arbitrary $L \in K[x][d/dx]$ such that the equation $L(\mathrm{mod}\ \wp)y = 0$ has sufficiently many solutions in $\bar{K}_\wp((x))$ for almost all $\wp$. The proof is identical to that of Lemmas 2.3-2.4 and Corollary 2.5.

There are similar (nontrivial)bounds on $\Delta_{m;k}$ in the case when there exists a positive density of primes p for which L has zero p-curvature, and L is globally nilpotent.*) We present one such result, proof of which follows the line of [4], [7] and proofs of Lemmas 2.3-4 and Corollary 2.5:

Proposition 2.6: Let $L \in \mathbb{Z}[x][d/dx]$ be an operator such that for almost all p, every solution of $Ly = 0$ is convergent at a "generic point" t, in the p-adic disk $|x-t|_p < 1$. Let there exist a positive (natural) density χ of those primes p for which L has zero p-curvature. Then for an algebraic number ξ, distinct from singularities of L and a solution $y(x)$ of $Ly = 0$ with the expansion $y(x) = \Sigma_{m=0}^{\infty} c_m(x-\xi)^m$ with algebraic $c_0,\dots,c_{n-1}$ we have the following bound on the common denominator $D_{M;k}$ of $\{c_{m_1}\cdots c_{m_j} : m_1 +\dots+ m_j \leq M;$ $j = 1,\dots,k\}$: $\log |D_{M;k}| \leq M \log C_2 + (n-1)(1-\chi)\{\Sigma_{j=1}^{k} 1/j\}M + kC_3$, where $C_2 = C_2(L,\xi) \geq 1$, $C_2 = C_2(y)$. Thus $\lim\sup_{M\to\infty}|D_{M;k}|^{1/M} \leq C_2\cdot k^{(n-1)(1-\chi)}$ for a large k.

The assumptions of Proposition 2.7 imply, by Lemma 2.2,that L has a nilpotent p-curvature for almost all p. Also, we can weaken the assumptions of Proposition 2.7 by demanding that L is "of arithmetic type" in Bombieri's [11] sense: $\Sigma_p \log^+ r_p(t) < \infty$.

*) and when L has "the arithmetic type" [11] i.e. $\Sigma_p \log^+ r_p(t) < \infty$, where $r_p(t)$ denotes the p-adic radius of convergence of an arbitrary solution of $Ly = 0$ at a "generic" point t.

§3. The Grothendieck conjecture and one of its particular cases.

Let, as above, K be an algebraic number field and we consider a scalar linear differential equation over K(x):

$$(3.1)\qquad a_n(x)y^{(n)}(x) + \ldots + a_1(x)y'(x) + a_0(x)y(x) = 0,$$

where we assume that $a_i(x) \in K[x]$ $(0 \leq i \leq n)$. For a prime ideal $\mathcal{P}$ of K, we consider the reduction $(3.1)_{\mathcal{P}}$ of (3.1) (mod $\mathcal{P}$).

For scalar (linear) differential equations (3.1) the Grothendieck conjecture reads:

The Grothendieck Conjecture: Let for almost all prime ideals $\mathcal{P}$ of K, $(3.1)_{\mathcal{P}}$ has n solutions in $\bar{K}_{\mathcal{P}}(x)$, linearly independent over $\bar{K}_{\mathcal{P}}(x^p)$, i.e. let $(3.1)_{\mathcal{P}}$ have sufficiently many solutions for almost all $\mathcal{P}$. Then all solutions of (3.1) are algebraic functions.

According to Proposition 2.1, the condition "$(3.1)_{\mathcal{P}}$ has sufficiently many solutions for almost all $\mathcal{P}$" can be substituted by the condition "the p-curvature of (3.1) is zero for almost all p" or by the equivalent condition" for almost all p, $(d/dx)^p \equiv 0$ (mod $(3.1)_p$)"

We now follow Honda [2] to show that the Grothendieck conjecture for rank one case, n = 1, over K(x) is (elementary!) equivalent to the principles (C)-(C_1) of §1:

Theorem 3.1: The truth of the Grothendieck conjecture for rank one equations, n = 1, over $\bar{\mathbb{Q}}(x)$ is equivalent to the following:

a) the truth of the Grothendieck conjecture for the equations $xy' - \alpha y = 0$ with $\alpha \in \bar{\mathbb{Q}}$;

b) the truth of Principles (C) - (C_1) of §1.

Proof: Let us assume first that the Grothendieck conjecture is true for a particular equation of rank one over K(x) from a). Then we prove Principle (C). Let $K = \mathbb{Q}(\alpha)$ and let us consider differential equation

$$(3.2)\qquad xy' - \alpha y = 0.$$

If almost all prime ideals of K are of degree one, then for all such prime ideals $\mathcal{P}$, there exists a rational integer $\alpha(\mathcal{P})$, such that

$$\alpha \equiv \alpha(\mathcal{P}) \pmod{\mathcal{P}}.$$

Hence the differential equation $(3.2)_{\mathcal{P}}$ has a solution $x^{\alpha(\mathcal{P})}$, and by the Grothendieck conjecture, the solution x^{α} of (3.2) is an algebraic function, i.e., $\alpha \in \mathbb{Q}$ and $K = \mathbb{Q}$. The principle (C) is proved.

Let us show that the principle (C) implies the Grothendieck conjecture for arbitrary equations of rank one. For a differential equation

$$(3.3) \qquad y' = r(x)y, r(x) \in K(x),$$

if $(3.3)_{\mathcal{P}}$ has a solution $y_{\mathcal{P}}$ in $\bar{K}_{\mathcal{P}}(x)$, then

$$y_{\mathcal{P}} = \Pi_i (x-\alpha_i)^{e_i}.$$

From $(3.3)_{\mathcal{P}}$ we have

$$r(x)(\text{mod } \mathcal{P}) = \frac{y'_{\mathcal{P}}}{y_{\mathcal{P}}} = \Sigma_i \frac{e_i}{x-\bar{\alpha}_i} .$$

If this equation is valid for almost all $\mathcal{P}$ in K, then in some finite extension of K,

$$r(x) = \Sigma_i \frac{\beta_i}{x-\alpha_i},$$

and, because of above congruences,

$$\beta_i \equiv (\text{a rational integer})(\text{mod } \mathcal{P})$$

for almost all $\mathcal{P}$. Hence, by the principle (C), $\beta_i \in \mathbb{Q}$. Thus the general solution of (3.3) is

$$y = c.\Pi_i (x-d_i)^{\beta_i}$$

and is an algebraic function

In the next chapter we will prove a) of Theorem 3.1 by elementary means, thus establishing the Principles (C)-(C_1), used in §1 for Corollaries 1.2, 1.4.

We conclude this chapter with the formulation of the Grothendieck conjecture for matrix linear differential equations in terms of p-curvature operators Ψ_p [3]. Let us consider an arbitrary matrix linear differential equation with coefficients from K(x):

$$(3.4) \qquad (\frac{d}{dx}I + A(x))\bar{f}^t = 0,$$

for $I_{i,j} = \delta_{i,j}$ and $A(x) \in M(n,K(x))$. The p-curvature operator Ψ_p of (3.4) (mod p) is

$$\Psi_p = (\frac{d}{dx} I + A(x))^p (\text{mod } p).$$

In fact, Ψ_p is a linear operator [2], [3] and $\Psi_p = A_p(\text{mod } p)$, where A_n are defined inductively as follows: $A_1 = A(x), A_{n+1} = d/dx\ A_n + A_nA_1 (n \geq 0)$.

<u>The Grothendieck Conjecture:</u> If for almost all p, p-adic curvature operator Ψ_p of (3.4) is zero, $\Psi_p = 0$, then all solution of the equation (3.4) are algebraic functions.

§4. Padé approximations to binomial functions.

We use here methods of Padé approximations to prove that the equation

$$(4.1) \qquad y' = \frac{\alpha}{x} y$$

has a global nilpotence (≡ "nilpotent p-curvature for almost all p" ≡ "sufficiently many solutions (mod p) for almost all p"), when and only when $\alpha \in \mathbb{Q}$. Thus, according to Theorem 3.1, we prove an important part--Principles (C)-(C_1)--of Chebotarev's theorem. Our proof will be a model of proofs of more complicated results of §§5-8.

We note that for equations of rank one, the global nilpotence (i.e. Ψ_p--nilpotent for almost all p) is equivalent to the assumptions of the Grothendieck conjecture.

Let us assume that the equation (4.1) is globally nilpotent. We want to prove that its solution--x^α--is an algebraic function or, equivalently, that α is a rational number. Hence, we have to prove that functions $1, x^\alpha, \dots, x^{\alpha(m-1)}$ are linearly dependent over $\mathbb{C}(x)$. This is clearly equivalent to the assertion that Padé approximations to $1, x^\alpha, \dots, x^{\alpha(m-1)}$ at $x = 1$ with weights $\underbrace{(N, \dots, N)}_{m}$ are trivial for large m and N.

We know explicit Padé approximations to binomial functions x^{ω_i}: $i = 1, \dots, m$ at $x = 1$, for they were constructed by Hermite in 1873 [12]. This system of Padé approximations were studied by Mahler [13], Jager [14] and authors [15]. Here we present a brief summary of some properties and an explicit representation of this system of Padé approximations. Let $\omega_1, \dots, \omega_m$ be complex numbers such that $\omega_i - \omega_j$: $i \neq j$--are not rational integers. The Padé approximations to $(1-z)^{\omega_i}$: $i = 1, \dots, m$ at $z = 0$ with weights $\underbrace{(N, \dots, N)}_{m}$ has the following form:

$$(4.2) \qquad R(z) = P_1(z)(1-z)^{\omega_1} + \dots + P_m(z)(1-z)^{\omega_m},$$

where

$$(4.3) \qquad R(z) = \frac{N!^m}{\sigma!} z^\sigma + O(z^{\sigma+1})$$

at $z \sim 0$ and $\sigma \overset{\mathrm{def}}{=} Nm + m-1$.

The polynomials $P_i(z)$: $i = 1, \dots, m$ are the following:

$$(4.4) \qquad \begin{aligned} P_i(x) &= \Sigma_{h=0}^{N} p_{i,h} z^h, \\ p_{i,h} &= \binom{N}{h} \cdot \frac{(N!)^{m-1}}{\prod_{j=1, j\neq i}^{m} \{(\omega_j - \omega_i + N - h - 1) \dots (\omega_j - \omega_i) \dots (\omega_j - \omega_i - h)\}} \end{aligned}$$

for $k = 0,1,\dots,N$ and $i = 1,\dots,m$.

Let the equation (4.1) be globally nilpotent, i.e. the p-curvature of (4.1) is zero for almost all p. Equivalently, by Proposition 2.1, whenever the p-curvature is zero, the equation (4.1) has a solution $y_{\wp}$ in $\bar{K}_{\wp}[x]$ for $K = \mathbb{Q}(\alpha)$ and $\wp$ lying over p. Then $y_{\wp} = x^{a}$ for a rational integer a. Hence,

$$\alpha \equiv a (\mathrm{mod}\ \wp)$$

for a rational integer a. In particular, for almost all prime ideals $\wp$ in K all binomial coefficients $\binom{\alpha}{n}$ are $\wp$-integral for <u>all</u> n.

For simplicity, let us put in the Padé approximation scheme above, $m = 2M + 1$, $\omega_i = (i-1)\alpha$, $i = 1,\dots,2M + 1$.

We multiply (4.2) by the following product of binomial coefficients:

$$(4.5)\qquad \Omega = \{\prod_{i=1}^{2M}\binom{i\alpha}{N}\cdot\binom{-i\alpha}{N}\}\cdot\{\prod_{i=1}^{M}\binom{i\alpha}{N}\cdot\binom{-i\alpha}{N}\}.$$

Then it is easy to see from (4.5) that

$$\Omega P_i(z) = \Sigma_{h=0}^{N} p'_{i,h}\cdot z^{h};\quad i = 1,\dots,2M + 1$$

where $p'_{i,h}$ is a product of integers and binomial coefficients of the form $\binom{j\alpha}{N}$ (for $j = \pm 1,\dots,\pm 2M$) by numbers of the form

$$\binom{N}{h}\prod_{k=1}^{2M+1}\{\binom{(k-i)\alpha+N}{k}\binom{(i-k)\alpha+N}{N-k}/\binom{N}{h}\},$$

for all $k = 0,1,\dots,N$ and $i = 1,\dots, 2M+1$.

Since for almost all $\wp$, $\binom{i\alpha+j}{n}$ are $\wp$-integral numbers for all n, i, j, the polynomials $\Omega P_i(z)$: $i = 1,\dots,2M + 1$, after multiplication by $\mathrm{lcm}\{\binom{N}{h}^{2M}: h = 0,1,\dots,N\}$, become polynomials with $\wp$-integral coefficients for almost all $\wp$. We remark that $\mathrm{lcm}\{\binom{N}{h}^{2M}: h = 0,\dots,N\}$ divides $\mathrm{lcm}\{1,\dots,N\}^{2M}$. Even without the use of the prime number theorem, we get $\mathrm{lcm}\{1,\dots,N\} \le c_0^{N}$ (Chebicheff's arguments). A simple (mod $\wp$) analysis of coefficients of (4.4) shows that, for a fixed $\wp$, polynomials $\wp^{B}\cdot\Omega P_i(x)$ $(i = 1,\dots,n)$ have $\wp$-integral coefficients for $B \le c_1 MN$.

Thus for a sufficiently large N, the common denominator D of coefficients of all polynomials $\Omega P_i(z)$: $i = 1,\dots,2M + 1$, is bounded by c_2^{MN} for some $c_2 > 0$ depending only on K and on $\wp$'s with non-zero curvature.

Now we expand the left side of (the remainder function) $R(z)$ in (4.3) in powers of z at $z = 0$:

$$\Sigma_{i=1}^{2M+1} \Omega P_i(z)\cdot\{\Sigma_{k=0}^{\infty} (-1)^k \binom{(i-1)\alpha}{k} z^k\}$$

(4.6)

$$= \frac{N!^{2M+1}\cdot\Omega}{\{(2M+1)N+2M\}!} z^{(2M+1)N+2M} +\ldots$$

We can equate in both sides of (4.6) the coefficients at z^σ for $\sigma = (2M+1)N + 2M$. Because of the $\mathcal{P}$-integrality of binomial coefficients $\binom{\alpha k}{n}$ for almost all $\mathcal{P}$, we obtain an equation for the coefficient at z^σ:

$$(4.7) \qquad A_{N,M}(\alpha) = \Omega\cdot\frac{N!^{2M+1}}{\sigma!}$$

where the denominator $D_{N,M}$ of $A_{N,M}(\alpha)$ is bounded by C_3^{MN}, with $C_3 > 0$. Also the expressions (4.4)-(4.6) show that the size of $A_{N,M}(\alpha) \in \mathbb{Q}(\alpha)$ is bounded by C_4^{MN} for $C_4 = C_4(\alpha) > 0$.

However, for large N (with respect to M and the size of α) we have asymptotically:

$$(4.8) \qquad \frac{N!^{2M+1}}{\sigma!} \sim (2M + 1)^{-(2M+1)N} \quad \text{and} \quad \Omega \sim 1,$$

whenever $\alpha \notin \mathbb{Q}$. We can use now the product formula $|D_{N,M}^{[K:\mathbb{Q}]}\cdot\mathrm{Norm}(A_{N,M}(\alpha))| \geq 1$ (for $\Omega \neq 0$). This inequality is clearly impossible, according to (4.7) and (4.8), whenever M is sufficiently large with respect to C_3, C_4 and when N is sufficiently large with respect to M. Thus $A_{N,M}(\alpha) = 0$, which means that Padé approximations to functions $z^{i\alpha}$: $i = 0,\ldots,2M$ are trivial. Hence, z^α is algebraic or $\alpha \in \mathbb{Q}$ and $K = \mathbb{Q}$.

One obviously notices similarity between this proof and Chebicheff's or Gelfond-Schnirelman approach to prime number theorem. These similarities become even more transparent, if one appeals to integral representations of Padé approximations and integrals arising from the Gelfond-Schnirelman approach [16].

The proof of Principles (C)-(C_1), presented above, is effective and one can try to apply these (and similar) elementary arguments to classical problems of algebraic number theory. One of the possible applications is the problem of the least quadratic nonresidue and its algebraic number field analogs, though the elementary approach, as above, does not imply particularly interesting results for quadratic fields.

An alternative, and simpler, proof of the Grothendieck conjecture for equations (4.1) can be given using only Wronskians of the functions $z^{i\alpha+j}$ for $i,j = 0,1,\ldots$. However such proof cannot be immediately generalized for a larger class of equations studied by means of Padé approximation technique. This justifies an extravagant proof of the particular case of Chebotarev's theorem that we presented.

One can ask for the proof of full Chebotarev's theorem. At least a part of it can be proved using Padé approximations. It concerns the establishment of positive densities of those primes for which a given law of decomposition can occur infinitely often (though precise expressions for densities is harder to prove, see [16]). One of the ways to do this is to use Padé approximations to Abelian integrals with complex multiplications and the Main Theorem 5.2 of §5. Such a complicated approach, of course, cannot be very useful, but is interesting as a demonstration of (though limited) powers of Padé approximation techniques.

§5. Main Theorem on Padé Approximations.

Our methods of proof of the Grothendieck conjecture for a large class of equations defined over algebraic curves is based on the construction of Padé-type approximations in variables $x_1,\dots,x_g$ to a function $f(x_1,\dots,x_g)$ satisfying a system of Fuchsian (Pfaffian) differential equations in $x_1,\dots,x_g$. In applications $f(x_1,\dots,x_g)$ is typically a symmetric function of $f(x_1),\dots,f(x_g)$ for a solution $f(x)$ of a Fuchsian linear differential equation in x, satisfying assumptions of the Grothendieck conjecture. The main analytic assymption is an assumption of simultaneous uniformization of $f(x_1,\dots,x_g),x_1,\dots,x_g$ by means of $g+1$ meromorphic functions of finite order of growth in $\mathbb{C}^g$. To be more precise, we fix a point $\bar{x}_0 = (x_{1,0},\dots,x_{g,0})$ which is a non-singular point of $f(\bar{x}) \overset{\mathrm{def}}{=} f(x_1,\dots,x_g)$, and we assume that there are $g+1$ meromorphic functions $U_0(\bar{u}),U_1(\bar{u}),\dots,U_g(\bar{u})$ in g variables $\bar{u} = (u_1,\dots,u_g)$ such that

$$f(\bar{x}_0) = U_0(\bar{u}_0), \qquad x_{i,0} = U_i(\bar{u}_0) \qquad (i = 1,\dots,g)$$

for some $\bar{u}_0 = (u_{1,0},\dots,u_{g,0})$ in $\mathbb{C}^g$, such that $U_i(\bar{u})$ are analytic at (a disk including) $\bar{u} = \bar{u}_0$ $(i = 1,\dots,g)$ and the Jacobian is non-zero:

$$\frac{D(U_1,\dots,U_g)}{D(u_1,\dots,u_g)}\Big|_{\bar{u}=\bar{u}_0} \neq 0.$$

Meromorphic functions $U_0(\bar{u}), U_1(\bar{u}),\dots,U_g(\bar{u})$ are assumed to have a finite order of growth in $\mathbb{C}^g$. This means that there exist entire functions $H(\bar{u}), H_0(\bar{u}),\dots,H_g(\bar{u})$ in $\mathbb{C}^g$ such that $U_i(\bar{u}) = H_i(\bar{u})/H(\bar{u})$: $i = 1,\dots,g$ and $H(\bar{u}_0) \neq 0$ and such that all functions $H(\bar{u})$, $H_0(\bar{u}),\dots,H_g(\bar{u})$ all have order of growth $\leq \rho$, $\rho < \infty$. Thus, there exists a constant $\alpha = \alpha(H,H_1,\dots,H_g)$ such that on polydisks

$D_T = \{\bar u \in \mathbb{C}^g: |u_i - u_{i,0}| \le T;\ i = 1,\dots,g\}$ we have the following bound of growth of $H, H_1,\dots,H_g$:

$$\max\{|H(\bar u)|, |H_1(\bar u)|,\dots,|H_g(\bar u)|\} \le \exp\{\alpha T^\rho\}$$

for all $\bar u \in D_T$. Now we are ready to formulate one of the main results on the growth of coefficients of Padé-type approximants to $f(x_1,\dots,x_g)$ at $\bar x = \bar x_0$:

Let us use the following vector notations. We put $\vec m = (m_1,\dots,m_g)$ for non-negative integers $m_i \ge 0$ $(i = 1,\dots,g)$ and we denote $|\vec m| = m_1 +\dots+ m_g$ and $(\bar x - \bar x_0)^{\vec m} = (x_1 - x_{1,0})^{m_1} \dots (x_g - x_{g,0})^{m_g}$.

Lemma 5.1: Let there exist a polynomial $P(x_0,x_1,\dots,x_g)$ of degree at most N in x_0, of degree at most D in $x_1,\dots,x_g$ and of height at most H, such that the function $R(x_1,\dots,x_g) \overset{\text{def}}{=} P(f(x_1,\dots,x_g), x_1,\dots,x_g)$ has a zero at $\bar x = \bar x_0$ of order at least M: $R(x_1,\dots,x_g) = \Sigma_{\vec m}\, a_{\vec m}(\bar x - \bar x_0)^{\vec m}$. Let, in the notations above, $f(x) = U_0(\bar x)$, $x_i = U_i(\bar u)$ $(i = 1,\dots,g)$ where $U_j(\bar u)$ are meromorphic functions of the finite order of growth $\le \rho$, analytic at $\bar u = \bar u_0$ $(j = 0,\dots,g)$ and such that $f(\bar x_0) = U_0(\bar u_0)$, $x_{i,0} = U_i(\bar u_0)$ $(i = 1,\dots,g)$ and the Jacobian $D(U_1,\dots,U_g)/D(u_1,\dots,u_g)$ is non-singular at $\bar u = \bar u_0$. Then for $m_1 +\dots+ m_g = M$,

$$|a_{m_1,\dots,m_g}| = \left|\frac{\partial^{m_1+\dots+m_g} R(\bar x)}{m_1!\,\partial x_1^{m_1}\dots m_g!\cdot\partial x_g^{m_g}}\Big|_{\bar x=\bar x_0}\right| \le c_1^M\cdot\left(\frac{M}{D}\right)^{-M/\rho}\cdot H,$$

for $c_1 = c_1(\bar u_0, g, H, H_1,\dots,H_g) > 0$, provided that $M > D$ and D is sufficiently large with respect to N: $D \ge D_0(N,\bar u_0,H,H_1,\dots,H_g)$.

Proof: Let us put, in accordance with the notations above, $U_i(\bar u) = H_i(\bar u)/H(\bar u)$ $(i = 0,\dots,g)$ where $H(\bar u)$, $H_1(\bar u),\dots,H_g(\bar u)$ are entire functions of $\bar u$ in $\mathbb{C}^g$ with orders of growth $\le \rho$ and such that $H(\bar u_0) \ne 0$. We define $F(\bar u) \overset{\text{def}}{=} H(\bar u)^{D+N}\cdot P(U_0(\bar u), U_1(\bar u),\dots,U_g(\bar u))$. Since $f(\bar x) = U_0(\bar u)$, $x_i = U_i(\bar u)$ $(i = 1,\dots,g)$ near $\bar u = \bar u_0$, we have $F(\bar u) = H(\bar u)^{D+N}\cdot R(U_1(\bar u),\dots,U_g(\bar u))$. By the definition of $P(x_0,x_1,\dots,x_g)$ and $H(\bar u)$, $H_1(\bar u),\dots,H_g(\bar u)$ it follows that $F(\bar u)$ is an entire function with the following growth in the polydisk $D_T = \{\bar u \in \mathbb{C}^g: |u_i - u_{i,0}| \le T;$ $i = 1,\dots,g\}$: $|F(\bar u)| \le (N+1)\cdot\binom{D+g}{g}\cdot H\cdot\exp\{\alpha\cdot(D+N)\cdot T^\rho\}$ for $\bar u \in D_T$.

According to the assumptions, $F(\bar u)$ has a zero of order at least

M at $\bar{u} = \bar{u}_0$. We can now apply the Cauchy integral formula in the polydisk D_T to an entire function $F(\bar{u})$:

$$(5.1)\qquad \frac{\partial_{u_1}^{m_1}\cdots\partial_{u_g}^{m_g}F(\bar{u}_0)}{m_1!\cdots m_g!} = \frac{1}{(2\pi i)^g}\cdot\int\cdots\int_{\partial_0 D_T} \frac{F(\zeta_1,\ldots,\zeta_g)\,d\zeta_1\cdots d\zeta_g}{(\zeta_1-u_{1,0})^{m_1+1}\cdots(\zeta_g-u_{g,0})^{m_g+1}},$$

where $\partial_{u_i} = \partial/\partial u_i$ $(i = 1,\ldots,g)$ and $m_1 +\ldots+ m_g = M$ for a hull $\partial_0 D_T$ of the polydisk D_T. Thus from (5.1) it follows that

$$(5.2)\qquad \left|\frac{\partial_{u_1}^{m_1}\cdots\partial_{u_g}^{m_g}\,F(\bar{u}_0)}{m_1!\cdots m_g!}\right| \le (N+1)\cdot\binom{D+g}{g}\cdot H\cdot \exp\{\alpha\cdot(D+N)\cdot T^{\rho}\}\ \cdot\ T^{-M},$$

when $m_1 +\ldots+ m_g = M$.

We can now express $\partial_{x_1}^{n_1}\cdots\partial_{x_g}^{n_g}\,R(\bar{x})\,|_{\bar{x}=\bar{x}_0}$ for $n_1 +\ldots+ n_g = M$ in terms of $\partial_{u_1}^{m_1}\cdots\partial_{u_g}^{m_g}\,F(\bar{u})\,|_{\bar{u}=\bar{u}_0}$, using the fact that $\partial_{u_1}^{m_1}\cdots\partial_{u_g}^{m_g}F(\bar{u})\,|_{\bar{u}=\bar{u}_0} = 0$ whenever $m_1 +\ldots+ m_g < M$. To do this we use the following formula for partial differentiation $\partial_{u_i}\varphi = \Sigma_{j=1}^{g}(\frac{\partial U_j}{\partial u_i})\cdot\partial_{x_j}\varphi$ and $\partial_{x_i}\varphi = \Sigma_{j=1}^{g} M_{i,j}\partial_{u_j}\varphi$, where $M(\bar{u}) = (M_{i,j})_{i,j=1}^{g}$ is a matrix inverse to the Jacobian matrix $J(\bar{u}) = (\frac{\partial U_j(\bar{u})}{\partial u_i})_{i,j=1}^{g}$. Here, by our assumption, the matrix $J(\bar{u}_0)$ is nonsingular, and hence its inverse $M(\bar{u}_0) = (M_{i,j}(\bar{u}_0))_{i,j=1}^{g}$ exists. Applying this differentiation rule M times and taking into account the fact that $F(\bar{u})$ has a zero at $\bar{u} = \bar{u}_0$ of order at least M, we obtain

$$\partial_{x_{i_1}}\cdots\partial_{x_{i_M}}\,R(\bar{x})\,|_{\bar{x}=\bar{x}_0} = H(\bar{u}_0)^{-(D+N)}\cdot\Sigma_{j_1,\ldots,j_M=1}^{g}\prod_{\alpha=1}^{M}M_{i_\alpha,j_\alpha}(\bar{u}_0)$$
$$\times\ \partial_{u_{j_1}}\cdots\partial_{u_{j_M}}\,F(\bar{u})\,|_{\bar{u}=\bar{u}_0}.$$

Let $c_0 = c_0(\bar{u}_0) > 0$ be the bound on absolute values of all elements of the matrix $M(\bar{u}_0)$. Then for $\vec{n} = (n_1,\ldots,n_g)$ such that $|\vec{n}| = M$, we obtain

$$\left|\left.\frac{\partial_{x_1}^{n_1}\cdots\partial_{x_g}^{n_g}R(\bar{x})}{n_1!\cdots n_g!}\right|_{\bar{x}=\bar{x}_0}\ \right| \le |H(\bar{u}_0)|^{-(D+N)}\cdot\frac{M!}{n_1!\cdots n_g!}$$

$$\times\ g^M c_0^M \cdot \max\Big\{ \Big| \frac{\partial_{u_1}^{m_1}\cdots\partial_{u_g}^{m_g} F(\bar{u})}{m_1!\cdots m_g!}\Big|_{\bar{u}=\bar{u}_0}\Big| : m_1 +\ldots+ m_g = M\Big\}.$$

Hence (5.2) implies

$$(5.3)\qquad \Big|\frac{\partial_{x_1}^{n_1}\cdots\partial_{x_g}^{n_g} R(\bar{x})}{n_1!\cdots n_g!}\Big|_{\bar{x}=\bar{x}_0}\Big| \le |H(\bar{u}_0)|^{-(D+N)}\, c_0^M\, (N+1)\cdot H\cdot g^M \times \binom{D+g}{g}\cdot \exp\{\alpha\cdot (D+N)\cdot T^{\rho}\}\cdot T^{-M}\,\frac{M!}{\Gamma(\frac{M}{g})^g}\ ,$$

whenever $n_1 +\ldots+ n_g = M$. We assume now that D is sufficiently large, $D \ge D_0(N,\bar{u}_0,H,H_1,\ldots,H_g)$ and that $M > D$. Let us take now $T = (M/D)^{1/\rho} > 1$. Then from (5.3) we obtain

$$(5.4)\qquad \Big|\frac{\partial_{x_1}^{n_1}\cdots\partial_{x_g}^{n_g} R(\bar{x})}{n_1!\cdots n_g!}\Big|_{\bar{x}=\bar{x}_0}\Big| \le c_1^M\cdot \Big(\frac{M}{D}\Big)^{-M/\rho}\cdot H,$$

for $n_1 +\ldots+ n_g = M$ for $c_1 = c_1(\bar{u}_0,g,H,H_1,\ldots,H_g) > 0$, provided that $M > D \ge D_0$. Lemma 5.1 is proved.

The estimates of Lemma 5.1 allow us to show that a function $f(x_1,\ldots,x_g)$, which can be uniformized by means of meromorphic function (of finite order of growth), cannot have too small denominators of algebraic coefficients in its power series expansions. We will start with some standard algebraic preliminaries [17], [18].

For an algebraic number field K of degree $d = [K:\mathbb{Q}]$ we consider d imbeddings $\alpha \to \alpha^{(\sigma)}$ of K into $\mathbb{C}$: $\sigma = 1,\ldots,d$. Then the size $|\overline{\alpha}|$ of an algebraic number $\alpha \in K$ is defined as $|\overline{\alpha}| = \max\{|\alpha^{(\sigma)}|: \sigma = 1,\ldots,d\}$. The "Liouville inequality" means that $|\mathrm{den}(\alpha)^d\cdot \Pi_{\sigma=1}^d \alpha^{(\sigma)}| \ge 1$, whenever $\alpha \in K$, $\alpha \ne 0$ and $\mathrm{den}(\alpha)$ is a denominator of $\alpha \in K$. Also $\mathrm{den}\{\alpha_0,\ldots,\alpha_n\}$ denotes the common denominator of $\alpha_0,\ldots,\alpha_n$.

<u>Main Theorem 5.2</u>: Let $f(x_1,\ldots,x_g)$ be a function analytic at $\bar{x} = \bar{x}_0$, where $\bar{x}_0 = (x_{1,0},\ldots,x_{g,0})$ and $x_{i,0}$ $(i = 1,\ldots,g)$ are algebraic numbers from K. Let us assume that there are meromorphic functions $U_j(\bar{u})$ $(j = 0,\ldots,g)$ in $\mathbb{C}^g$ of finite order of growth $\le \rho$ analytic at $\bar{u} = \bar{u}_0$ and such that in the neighborhood of $\bar{u} = \bar{u}_0$, for $x_i = U_i(\bar{u})$ $(i = 1,\ldots,g)$ we have $f(\bar{x}) = U_0(\bar{x})$ with $x_{i,0} = U_i(\bar{u}_0)$ $(i = 1,\ldots,g)$

and $D(U_1,\dots,U_g)/D(u_1,\dots,u_g)|_{\bar{u}=\bar{u}_0} \neq 0$. If the expansions of $f(\bar{x})^j$ at $\bar{x} = \bar{x}_0$ have the form $f(\bar{x})^j = \Sigma_{n_1,\dots,n_g=0}^{\infty} a_{n_1,\dots,n_g;j}(x-x_{1,0})^{n_1}\dots$ $\dots(x_g-x_{g,0})^{n_g}$, $j = 1,2,\dots$, with algebraic $a_{n_1,\dots,n_g;j} \in K$ $(n_1,\dots,n_g = 0,1,\dots;\ j = 1,2,\dots)$ and if $\Delta_{M,k}$ is a common denominator of $\{a_{n_1,\dots,n_g;j}: n_1 +\dots+ n_g \le M,\ j = 1,\dots,k\}$, then we define

$$\tilde{\sigma} = \lim\sup_{M\to\infty} \max\{\overline{|a_{n_1,\dots,n_g;1}|}^{1/M}: n_1 +\dots+ n_g = M\};$$

$$\gamma_k = \lim\sup_{M\to\infty} \frac{1}{M} \log|\Delta_{M\ ;k}|.$$

If $\tilde{\sigma} < \infty$ and if $\lim\sup_{k\to\infty} \gamma_k/\log k < \frac{1}{d\rho g}$ (e.g. if $\lim\sup_{k\to\infty}\gamma_k < \infty$), then $f(x_1,\dots,x_g)$ is an algebraic function.

Remark 5.3: If for every $\sigma = 1,\dots,d$ the function $f^{(\sigma)}(\bar{x}) = \Sigma_{\vec{m}}\, a^{(\sigma)}_{\vec{m};1}\,(\bar{x}-\bar{x}_0)^{\vec{m}}$ is regular at $\bar{x} = \bar{x}_0$, then $\sigma < \infty$. In particular,if $f^{(\sigma)}(\bar{x})$ satisfy (Fuchsian) linear differential equations and $\bar{x}_0$ is different from (finitely many) singularities of these equations, then $\tilde{\sigma} < \infty$. We also note that the assumptions of the Grothendieck conjecture (zero p-curvature for almost all p) correspond , according to Corollary 2.5,, to $\sup_k\gamma_k < \infty$.

Proof of Theorem 5.2: To prove this theorem, we construct Padé approximations to $f(x_1,\dots,x_g)$ at $\bar{x} = \bar{x}_0$. The construction of Padé approximations is achieved, following standard diophantine approximation procedures, by means of Siegel's lemma [17], representing a version of Dirichlet's box principle. We borrow a simple version of Siegel's lemma from ([17], Chapter 6, Lemma 1):

Lemma 5.4: Let M and N be integers, $N > M > 0$ and let $u_{i,j}$ $(i = 1,\dots,M;\ j = 1,\dots,N)$ be algebraic integers in K with sizes at most U (≥ 1). Then there exist algebraic integers $x_1,\dots,x_N$ in K, not all zero, satisfying $\Sigma_{j=1}^{N} u_{i,j}\cdot x_j = 0$: $i = 1,\dots,M$ and such that $\overline{|x_j|} \le c_1(c_1NU)^{M/(N-M)}$: $j = 1,\dots,M$. Here $c_1 = c_1(K) > 0$.

To prove Theorem 5.2, we assume that $\sigma < \infty$ and that for some $\delta > 0$, we have $\gamma_k < \frac{(1-\delta)}{d\rho g} \log k$ for (infinitely many) sufficiently large k. We choose a sufficiently large integer N, $N \ge N_0$, $N_0 = N_0(K,\delta,\bar{u}_0,H,H_0,\dots,H_g)$ such that $\gamma_N < \frac{(1-\delta)}{d\rho g} \log N$. Hence, we have the following bounds on the coefficients of expansions of $f(\bar{x})^i$ at $\bar{x} = \bar{x}_0$. If $f(\bar{x})^i = \Sigma_{\vec{m}}\, a_{\vec{m};i}(\bar{x}-\bar{x}_0)^{\vec{m}}$, then $a_{\vec{m};i} \in K$ and

$$(5.5) \qquad \overline{|a_{\vec{m},i}|} \le c_2^{m_1+\dots+m_g}$$

for $|\vec{m}| \geq c_3$, $c_3 = c_3(N)$ and $c_2 \geq \sigma$; $i = 0,\ldots,N$. Also the common denominator $\Delta_{M;N}$ of $\{a_{\vec{m},i}: |\vec{m}| \leq M;\ i = 1,\ldots,N\}$ is bounded by $N^{[(1-\delta)/d\rho g]M}$ for $M \geq c_3$. In these notations, we have

Lemma 5.5: Let, as above, $N \geq N_0$ and let the inequalities (5.51) and $|\Delta_{M;N}| \leq N^{[(1-\delta)/d\rho g]M}$, $M \geq c_3$ are satisfied. Then for $1/4 > \epsilon > 0$ and a sufficiently large integer D, $D \geq D_0(N,K,f,\bar{x}_0,\delta,\epsilon)$, there exists a non-zero polynomial $P(x_0,x_1,\ldots,x_g) \in K[x_0,x_1,\ldots,x_g]$ with integer coefficients of degree at most D in $x_1,\ldots,x_g$ and of degree at most N in x_0 with the following properties. The sizes of coefficients of $P(x_0,x_1,\ldots,x_g)$ are bounded by

$$c_4^{DN^{1/g}} \cdot N^{\frac{(1-\delta)}{d\rho g}N^{1/g}D\frac{2\varepsilon^{1+1/g}}{(1-\varepsilon)}},$$

where $c_4 = c_4(K,f,\bar{x}_0,\epsilon) > 0$. The function $R(x_1,\ldots,x_g) \overset{\text{def}}{=} P(f(x_1,\ldots,x_g),x_1,\ldots,x_g)$ has a zero of order at least $[\epsilon^{1/g}.N^{1/g}.D]-1$ at $\bar{x} = \bar{x}_0$.

Proof of Lemma 5.5: Let $P(x_0,x_1,\ldots,x_g) =$

$$= \Sigma_{m_0=0}^{N}\Sigma_{m_1,\ldots,m_g=0,m_1+\ldots+m_g\leq D}^{D} p_{m_0,m_1,\ldots,m_g} \cdot x_0^{m_0} \cdot (x_1-x_{1,0})^{m_1} \ldots$$

$\ldots(x_g-x_{g,0})^{m_g}$, where $p_{m_0,m_1,\ldots,m_g}$ are undertermined integers from K ($m_0 = 0,\ldots,N; m_1 +\ldots+ m_g \leq D$). Then, in the notations above,

$f(\bar{x})^i = \Sigma_{\vec{m}}\, a_{\vec{m};i}(\bar{x}-\bar{x}_0)^{\vec{m}}$ and $R(\bar{x}) = \Sigma_{\vec{m}=(m_1,\ldots,m_g)}(\bar{x}-\bar{x}_0)^{\vec{m}} \times$

$$\{\Sigma_{m_0=0}^{N}\Sigma_{0\leq k_1\leq m_1,\ldots,0\leq k_g\leq m_g;k_1+\ldots+k_g\leq D} p_{m_0,k_1,\ldots,k_g} \cdot a_{m_1-k_1,\ldots,m_g-k_g;m_0}\}.$$

Hence, the system of linear equations on $p_{m_0,m_1,\ldots,m_g}$ equivalent to the condition $\mathrm{ord}_{\bar{x}=\bar{x}_0} R(\bar{x}) \geq S$ has the form

$$\Sigma_{m_0=0}^{N}\Sigma_{0\leq k_1\leq m_1,\ldots,0\leq k_g\leq m_g;k_1+\ldots+k_g\leq D}\, p_{m_0,k_1,\ldots,k_g} \cdot a_{m_1-k_1,\ldots,m_g-k_g;m_0}$$

$= 0$ for all non-negative integers $m_1,\ldots,m_g$ such that $m_1 +\ldots+m_g < S$. This system of equation can be represented in the form:

$$\Sigma_{m_0=0}^{N}\Sigma_{0\leq k_1\leq m_1,\ldots,0\leq k_g\leq m_g;k_1+\ldots+k_g\leq D}\Delta_{S-1,N} \cdot a_{m_1-k_1,\ldots,m_g-k_g;m_0}$$

(5.6)

$$\times\, p_{m_0,k_1,\ldots,k_g} = 0 \text{ for all } m_i \geq 0 (1 \leq i \leq g), m_1+\ldots+m_g < S.$$

In (5.6), $\Delta_{S-1,N}\cdot a_{j_1,\ldots,j_g;m_0}$ are algebraic integers from K whenever $m_0 = 0,1,\ldots,N$ and $j_1 +\ldots+ j_g \le S-1$, of sizes bounded by $N^{[(1-\delta)/d\rho g]S}\cdot c_2^S$. The system of equations (5.6) has $\binom{S-1+g}{g}$ equations on $(N+1)\cdot\binom{D+g}{g}$ unknowns $p_{m_0,m_1,\ldots,m_g}$ $(m_0=0,\ldots,N;m_1+\ldots+m_g \le D)$.

Let $\frac{1}{4} > \epsilon > 0$ and we put $S = [\epsilon^{1/g}.D\cdot N^{1/g}]$. Then for $D \ge D_1(N,g,\epsilon)$ we have $\binom{S-1+g}{g}/\{(N+1)\cdot\binom{D+g}{g} - \binom{S-1+g}{g}\} \le 2\epsilon/(1-\epsilon)$ and, hence, applying Lemma 5.4, we deduce the existence a system of algebraic integers $p_{m_0,m_1,\ldots,m_g}$ $(m_0 = 0,\ldots,N;m_1 +\ldots+ m_g \le D)$ from K, not all zero, such that all equations (5.6) are satisfied and such that

$$\max\{|\overline{p_{m_0,m_1,\ldots,m_g}}|: m_0 = 0,\ldots,N;m_1+\ldots+m_g \le D\}$$
$$\le c_4^{D\cdot N^{1/g}}\cdot N^{\frac{(1-\delta)}{d\rho g}\cdot\epsilon^{1/g}\cdot N^{1/g}\cdot D\frac{2\epsilon}{(1-\epsilon)}}$$

where $c_4 = c_4(K,f,\bar{x}_0,\epsilon)$. Then the polynomial $P(x_0,x_1,\ldots,x_g)$ with the coefficients $p_{m_0,m_1,\ldots,m_g}$ $(m_0=0,\ldots,N;m_1+\ldots+m_g \le D)$ satisfies all the conditions stated in Lemma 5.5. Lemma 5.5 is proved.

To finish the proof of Theorem 5.2, we assume that $R(\bar{x}) \not\equiv 0$, where $R(\bar{x}) = R(x_1,\ldots,x_g)$ is defined as in Lemma 5.5, $R(\bar{x}) \overset{\text{def}}{=} P(f(x_1,\ldots,x_g),x_1,\ldots,x_g)$ for a polynomial $P(x_0,x_1,\ldots,x_g) \in K[x_0,x_1,\ldots,x_g], P(x_0,x_1,\ldots,x_g) \not\equiv 0$, satisfying all conditions of Lemma 5.5. Let us denote then by M the order of zero of $R(\bar{x})$ at $\bar{x} = \bar{x}_0$: $M = \text{ord}_{\bar{x}=\bar{x}_0} R(\bar{x}) < \infty$. If we put $R(\bar{x}) = \Sigma_{\vec{m}}\, c_{\vec{m}}(\bar{x}-\bar{x}_0)^{\vec{m}}$, then, by the definition of M, $c_{\vec{m}} = 0$ whenever $|\vec{m}| < M$. Also there exist non-negative integers $m_1^0,\ldots,m_g^0$ such that $m_1^0 +\ldots+ m_g^0 = M$ and $c_{m_1^0,\ldots,m_g^0} \ne 0$. We put $c \overset{\text{def}}{=} c_{m_1^0,\ldots,m_g^0}$. Following the formulae displayed in the proof of Lemma 5.5, we have the following representation of the number c in terms of coefficients of the expansions of $f(\bar{x})^{m_0}$ $(m_0 = 0,\ldots,N)$ and the coefficients of the polynomial $P(x_0,x_1,\ldots,x_g)$:

$$(5.7)\qquad c = \Sigma_{m_0=0}^{N}\Sigma_{0\le k_1\le m_1,\ldots,0\le k_g\le m_g,k_1+\ldots+k_g\le D}\,p_{m_0,k_1,\ldots,k_g}$$
$$\times a_{m_1-k_1,\ldots,m_g-k_g;m_0}.$$

According to Lemma 5.5 and the bounds $|\Delta_{M,N}| \le N^{\frac{(1-\delta)}{d\rho g}M}$ on the denominator of $\{a_{m_1,\dots,m_g;m_0}: m_0=0,\dots,N; m_1+\dots+m_g \le M\}$, we conclude that c is an algebraic number from K, of the size not higher than $(N+1)\cdot\binom{D+g}{g}\cdot H\cdot c_2^M$ and of denominator bounded by $N^{[(1-\delta)/d\rho g]M}$. Here H bounds the size of the coefficients of the polynomial $P(x_0,x_1,\dots,x_g)$:

$$(5.8) \qquad H \le c_4^{N^{1/g}\cdot D}\cdot N^{\frac{(1-\delta)}{d\rho g}N^{1/g}\cdot D\cdot\frac{2\epsilon^{1+1/g}}{(1-\epsilon)}}$$

Now we use the upper bound on $|c|$ from Lemma 5.1. We get:

$$(5.9) \qquad |c| \le c_1^M\cdot\left(\frac{M}{D}\right)^{-M/\rho}\cdot H.$$

Also, according to Lemma 5.5, $M \ge [\epsilon^{1/g}\cdot N^{1/g}\cdot D]$. Consequently, from (5.9) we get

$$(5.10) \qquad |c| \le c_5^M\cdot N^{-\frac{M}{\rho g}}\cdot H$$

for $c_5 = c_5(\epsilon,g,\bar{u}_0,H,H_1,\dots,H_g) > 0$. Since $c \ne 0$, we can use the product-formula $|\mathrm{den}(c)^d\prod_{\sigma=1}^d c^{(\sigma)}| \ge 1$, where $c^{(\sigma)}$: $\sigma = 1,\dots,d$--are numbers algebraically conjugate to c and we can put $c^{(1)} = c$. Since $|c^{(\sigma)}| \le |\bar{c}|$, we obtain from the Liouville's inequality:

$$(5.11) \qquad |\mathrm{den}(c)|^d\cdot|\bar{c}|^{d-1}\cdot|c| \ge 1.$$

Using the bounds on den(c) and $|\bar{c}|$ above and (5.10), we get from (5.11)

$$(5.12) \qquad c_6^M\cdot H^d\cdot N^{\frac{(1-\delta)}{\rho g}M}\cdot N^{-\frac{M}{\rho g}} \ge 1,$$

where $c_6 = c_6(K,\epsilon,g,\bar{u}_0,H,H_1,\dots,H_g) > 0$ and $D \ge D_2(N,\epsilon)$. Combining this bound with (5.8) we get:

$$(5.13) \qquad c_7^M\cdot N^{\frac{(1-\delta)}{\rho g}\frac{2\epsilon}{1-\epsilon}M}\cdot N^{-\frac{\delta}{\rho g}M} \ge 1$$

for $c_7 = c_7(K,\epsilon,g,\bar{u}_0,H,H_1,\dots,H_g) > 0$. The inequality (5.13) is clearly impossible whenever $2\epsilon(1-\delta)/(1-\epsilon) < \delta/2$ for sufficiently large N. Hence choosing ϵ, $1/2 > \epsilon > 0$ and such that $2\epsilon(1-\delta)/(1-\epsilon) < \delta/2$, we obtain from (5.13), $c_7^{\rho g}\cdot N^{-\delta/2} \ge 1$, which is impossible whenever $c_1^{2\rho g/\delta} < N$. Hence, for $N \geq N_2(K,\epsilon,g,\bar{u}_0,H,H_1,\ldots,H_g)$, we get $R(\bar{x}) \equiv 0$. This shows that $f(x_1,\ldots,x_g)$ is an algebraic function and Theorem 5.2 is proved.

Remark 5.6: As the proof of Main Theorem 5.2 shows, its assumptions and conclusions can be modified in various ways. One such modification is suggested by applications to Abelian integrals. In this modification we consider g algebraic functions $\alpha_1(\bar{x}),\ldots,\alpha_g(\bar{x})$ of $\bar{x} = (x_1,\ldots,x_g)$ over $\bar{\mathbb{Q}}(\bar{x})$ such that $D(\bar{x}) \overset{\text{def}}{=} D(\alpha_1,\ldots,\alpha_g)/D(x_1,\ldots,x_g)$ $\not\equiv 0$ and such that $f(\bar{x}),\alpha_1(x),\ldots,\alpha_g(\bar{x})$ [and not $f(\bar{x}),x_1,\ldots,x_g$!] are simultaneously uniformized near $\bar{x} = \bar{x}_0$ by meromorphic functions $U_0(\bar{u})$, $U_1(\bar{u}),\ldots,U_g(\bar{u})$ of $\bar{u} = (u_1,\ldots,u_g)$ having order of growth $\leq \rho$ in $\mathbb{C}^g$. We thus assume, like in Theorem 5.2, that $\alpha_i(\bar{x}_0) = U_i(\bar{x}_0)$ $(i = 1,\ldots,g)$, that $U_j(\bar{u})$ are analytic at $\bar{u} = \bar{u}_0$ $(j = 0,\ldots,g)$ and, additionally, that the Jacobian $D(\bar{x})$ is non-singular at $\bar{x} = \bar{x}_0$. Under these assumptions, together with the assumptions on σ and γ_k in Theorem 5.2, we conclude that $f(\bar{x})$ is an algebraic function. To see why such modification of Theorem 5.2 is true, we note that we can reduce the new formulation to an old one using the change of variables:

$$z_i = \alpha_i(\bar{x}): i = 1,\ldots,g; \quad f_1(\bar{z}) \overset{\text{def}}{=} f(\bar{x}).$$

Then the new set of functions $(f_1(\bar{z}), z_1,\ldots,z_g)$ satisfy all uniformization and non-degeneracy assumptions of Theorem 5.2. Also, we have an expansion of x_i in power series of variable $z_1 = \alpha_1(\bar{x}),\ldots,z_g = \alpha_g(\bar{x})$ at $(z_1,\ldots,z_g) = \bar{z}_0 \overset{\text{def}}{=} (\alpha_1(\bar{x}_0),\ldots,\alpha_g(\bar{x}_0))$,

$$x_i = \Sigma_{m_1,\ldots,m_g=0}^{\infty} d_{m_1,\ldots,m_{g;i}} (z_1-\alpha_1(\bar{x}_0))^{m_1}\ldots(z_g-\alpha_g(\bar{x}_0))^{m_g} : i = 1,\ldots,g.$$

Then, by Eisenstein's theorem, there exists an integer $A \geq 1$ such that $A^{m_1+\ldots+m_g} \cdot d_{m_1,\ldots,m_{g;i}}$ are algebraic integers, $m_1,\ldots,m_g = 0,1,\ldots;$ $i = 1,\ldots,g$. Consequently, the new parameters $\bar{\tilde{\sigma}}$ and $\bar{\gamma}_k$ for the expansion of $f_1(z_1,\ldots,z_n)^j$ at $\bar{z} = \bar{z}_0$, satisfy again $\bar{\tilde{\sigma}} < \infty$ and also $\limsup_{k\to\infty} \bar{\gamma}_k/\log k \leq \limsup_{k\to\infty} \gamma_k/\log k$. Thus $f_1(\bar{z})$ is algebraic, and hence, $f(\bar{x})$ is algebraic function. (See the amplification of these arguments below in §8.)

Remark 5.7: Another version of Theorem 5.2 corresponds to the case, when more than one function is uniformized by meromorphic functions. Such statements are very useful when we study the density of primes p for which the p-curvature is zero. We present one general result in this direction, whose proof is almost identical to the proof of Main Theorem 5.2.

Theorem 5.8: Let $n \geq g + 1$ and let $f_1(\bar{x}),\dots,f_n(\bar{x})$ be functions analytic at $\bar{x} = \bar{x}_0 \in K^g$. Let there exist meromorphic functions $U_1(\bar{u}),\dots,U_{g+1}(\bar{u})$ of finite order of growth $\leq \rho$ of variables $\bar{u} = (u_1,\dots,u_g)$ in $\mathbb{C}^g$ analytic at $\bar{u} = \bar{u}_0$ with the following properties. The Jacobian $D(u_1,\dots,u_g)/D(x_1,\dots,x_g)$ is nonsingular at $\bar{x} = \bar{x}_0$ (or $\bar{u} = \bar{u}_0$) and in the neighborhood of $\bar{u} = \bar{u}_0$ we have the uniformization: $f_j(\bar{x}) = U_j(\bar{u})$ and $f_j(\bar{x}_0) = U_j(\bar{u}_0)$ $(j = 1,\dots,n)$. We put for non-negative integers k_j $(j = 1,\dots,n)$: $f_1(\bar{x})^{k_1}\dots f_n(\bar{x})^{k_n} =$ $= \Sigma_{\vec{m}}\, a_{\vec{m};k_1,\dots,k_n}(\bar{x}-\bar{x}_0)^{\vec{m}}, a_{\vec{m};k_1,\dots,k_n} \in K$ and denote by $D_{M;k}$ the common denominator of $\{a_{\vec{m};k_1,\dots,k_n} : |m| \leq M;\ k_1 +\dots+ k_n \leq k\}$. Let

$$\tilde{\sigma} = \limsup_{M\to\infty} \max\{\overline{|a_{\vec{m};k_1,\dots,k_n}|}^{1/M} : |\vec{m}| \leq M;\ k_j = 0,1\ (j=1,\dots,n)\}$$

$$\gamma_k = \limsup_{M\to\infty} \frac{1}{M} \log|\Delta_{M;k}|.$$

Then $\tilde{\sigma} < \infty$ and $\limsup_{k\to\infty} \gamma_k/\log k < (n-g)/(d\rho g)$ implies that functions $f_1(\bar{x}),\dots,f_n(\bar{x})$ are algebraically dependent over K.

Instead of proving Theorem 5.8 we prove a different result, where the bounds on denominators of the coefficients of the expansion of $f_1(\bar{x})^{k_1}\dots f_n(\bar{x})^{k_n}$ are presented in the sharpest form.

Theorem 5.9: Let $n \geq g + 1$ and let $f_1(\bar{x}),\dots,f_n(\bar{x})$ be functions analytic at $\bar{x} = \bar{x}_0$. Let there exist meromorphic functions $U_1(\bar{u}),\dots,U_n(\bar{u})$ of finite order of growth $\leq \rho$ of variables $\bar{u} = (u_1,\dots,u_g)$ in $\mathbb{C}^g$ analytic at $\bar{u} = \bar{u}_0$ with the following properties. The Jacobian of the transformation $(x_1,\dots,x_g) \rightleftarrows (u_1,\dots,u_g)$, $D(u_1,\dots,u_g)/D(x_1,\dots,x_g)$ is nonsingular at $\bar{x} = \bar{x}_0$ (or $\bar{u} = \bar{u}_0$) and in the neighborhood of $\bar{u} = \bar{u}_0$ we have the uniformization: $f_j(\bar{x}) = U_j(\bar{u})$ and $f_j(\bar{x}_0) = U_j(\bar{u}_0)$ $(j = 1,\dots,n)$. We put for non-negative integers k_j $(j = 1,\dots,n)$: $f_1(\bar{x})^{k_1}\dots f_n(\bar{x})^{k_n} = \Sigma_{\vec{m}}\, a_{\vec{m};k_1,\dots,k_n}(\bar{x}-\bar{x}_0)^{\vec{m}}$ where $a_{\vec{m};k_1,\dots,k_n} \in K$, and denote by D_M the common denominator over K of $\{a_{\vec{m};k_1,\dots,k_n} : |\vec{m}| \leq M,\ k_1 +\dots+ k_n < M\}$. Let

$$\tilde{\sigma} = \lim\sup_{M\to\infty} \max\{\overline{|a_{\vec{m};k_1,\dots,k_n}|}^{1/M} : |\vec{m}| \leq M;\ k_j = 0,1\ (j = 1,\dots,n)\},$$

$$\xi = \lim\sup_{M\to\infty} \frac{\log|D_M|}{M \log M}.$$

Then $\tilde{\sigma} < \infty$ and $\xi < (1-g/n)/d\rho$ implies that the functions $f_1(\bar{x}),\ldots,f_n(\bar{x})$ are algebraically dependent over K.

<u>Proof of Theorem 5.9</u>: Let us assume that $\tilde{\sigma} < \infty$ and that for some $\delta > 0$ we have $\xi < |1-g/(n-\delta)|/d\rho$. Thus, we may assume that, $\log|D_M| < [1-g/(n-\delta)]M\log M/d\rho$ for any sufficiently large M. We choose a sufficiently large integer D and follow the method of proof of Theorem 5.2, starting from the following analog of Lemma 5.5:

<u>Lemma 5.10</u>: Let $D \geq D_2(\bar{u}_0,K,\varepsilon,\delta,f_1,\ldots,f_n)$, and $1/4 > \delta > 0$, as above. Then for $n - g > \varepsilon > 0$ there exists a nonzero polynomial $P(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$ with integral coefficients of degree at most D in each of the variables x_i $(i = 1,\ldots,n)$ and with the following properties. The sizes of coefficients of $P(x_1,\ldots,x_n)$ are bounded by $D^{c_8 D^{(n-\varepsilon)/g-\varepsilon}}$, where $c_8 = c_8(K,g,\delta,\varepsilon) > 0$. The function $R(x_1,\ldots,x_g) \overset{\text{def}}{=} P(f_1(x_1,\ldots,x_g),\ldots,f_n(x_1,\ldots,x_g))$ has a zero of order at least $D^{(n-\varepsilon)/g}\cdot D$ at $\bar{x} = \bar{x}_0$.

<u>Proof of Lemma 5.10</u>: Let us denote $P(x_1,\ldots,x_g) = \Sigma^D_{k_1=0}\cdots\Sigma^D_{k_n=0}\, p_{k_1,\ldots,k_n}\, x_1^{k_1}\ldots x_n^{k_n}$. Then, in the notations of Theorem 5.9, we have the following expansion $R(\bar{x})$ $(\overset{\text{def}}{=} R(x_1,\ldots,x_g))$ at $\bar{x} = \bar{x}_0$: $R(\bar{x}) = \Sigma_{\vec{m}}(\bar{x}-\bar{x}_0)^{\vec{m}} \cdot \{\Sigma^D_{k_1=0}\cdots\Sigma^D_{k_n=0}\, p_{k_1,\ldots,k_n}\, a_{\vec{m};k_1,\ldots,k_n}\}$. Hence the system of linear equations on $p_{k_1,\ldots,k_n}$ equivalent to the condition $\mathrm{ord}_{\bar{x}=\bar{x}_0} R(\bar{x}) \geq S$ has the form

$$(5.14)\qquad \Sigma^D_{k_1=0}\cdots\Sigma^D_{k_n=0}\, D_S\cdot a_{\vec{m};k_1,\ldots,k_n}\cdot p_{k_1,\ldots,k_n} = 0$$

for all $\vec{m} = (m_1,\ldots,m_g)$ with $|\vec{m}| < S$, when $S \geq nD$. In (5.14) all coefficients at $p_{k_1,\ldots,k_n}$ are algebraic integers from K of sizes bounded by $S^{[1-g/(n-\delta)]S/d\rho}\, c_9^S$ according to assumptions of Theorem 5.9. The system of equations (5.14) has $\binom{S-1+g}{g}$ equations on $n(D+1)^n$ unknowns $p_{k_1,\ldots,k_n}$ $(k_i = 0,\ldots,D;\ i = 1,\ldots,n)$. We can put $S = [D^{(n-\varepsilon)/g}]$. Then for sufficient large D we apply Lemma 5.4 and deduce the existence of a system of algebraic integers $p_{k_1,\ldots,k_n}$ from K, not all zero, satisfying all equations (5.14) and such that

$$\max\{|\overline{p_{k_1,\ldots,k_n}}|: k_i = 0,\ldots,D;\ i = 1,\ldots,n\} \leq D^{c_{10}D^{(n-\varepsilon)/g-\varepsilon}}$$

Let us assume that $R(\bar{x}) \not\equiv 0$, where $R(\bar{x})$ is defined as in Lemma 5.10. (We will eventually come to the contradiction, thus establishing that functions $f_1(\bar{x}),\dots,f_n(\bar{x})$ are algebraically independent and, moreover, exhibiting the relation $R(\bar{x}) \equiv 0$, connecting them.) Let us denote then by M the order of zero of $R(\bar{x})$ at $\bar{x} = \bar{x}_0$: $M = \mathrm{ord}_{\bar{x}=\bar{x}_0} R(\bar{x}) < \infty$. If we put $R(\bar{x}) = \Sigma_{\vec{m}} c_{\vec{m}} (\bar{x}-\bar{x}_0)^{\vec{m}}$, then, by the definition of M, $c_{\vec{m}} = 0$, whenever $|\vec{m}| < M$. Also there exists $\vec{m}_0 = (m_{1,0},\dots,m_{g,0})$ such that $|\vec{m}_0| = M$ and $c \overset{\mathrm{def}}{=} c_{\vec{m}_0} \neq 0$. Following the formula displayed in the proof of Lemma 5.10, we have the following representation of the number c in terms of coefficients of the expansions of $f_1(\bar{x})^{k_1} \dots f_n(\bar{x})^{k_n}$ and the coefficients of the polynomial $P(x_1,\dots,x_n)$:

$$c = \Sigma_{k_1=0}^{D} \dots \Sigma_{k_n=0}^{D} p_{k_1,\dots,k_n} \cdot a_{\vec{m}_0,k_1,\dots,k_n}. \tag{5.15}$$

Obviously, the denominator of $c \in K$ divides D_M, while $|\bar{c}| \leq (D+1)^n \cdot H \cdot c_{11}^M$, for $c_{11} = c_{11}(\bar{x}_0,f_1,\dots,f_n) > 0$, where H bounds the sizes of the coefficients of the polynomial $P(x_1,\dots,x_g)$:

$$H \leq D^{c_8 D^{(n-\epsilon)/g-\epsilon}}. \tag{5.16}$$

Consequently, we have:

$$\begin{aligned} &\mathrm{den}(c) < M^{[1-g/(n-\delta)]M/d\rho}; \\ &|\bar{c}| \leq c_{11}^M \cdot D^{c_{12} D^{(n-\epsilon)/g-\epsilon}}. \end{aligned} \tag{5.17}$$

To bound $|c|$ from above, we use extimates identical to those from Lemma 5.1. Here according to assumptions of Theorem 5.9, $U_i(\bar{u}) = H_i(\bar{u})/H(\bar{u})$ $(i = 1,\dots,n)$, where $H(\bar{u}),H_1(\bar{u}),\dots,H_n(\bar{u})$ are entire functions of $\bar{u}$ in $\mathbb{C}^g$ of order of growth $\leq \rho$ and such that $H(\bar{u}_0) \neq 0$. We can apply then the estimate (5.3) from the proof of Lemma 5.1 with modifications due to different notations and the uniform bound nD of the total degree of the polynomial $P(x_1,\dots,x_n)$. This way we obtain for $\vec{m}_0 = (m_{1,0},\dots,m_{g,0})$,

$$\begin{aligned} \left| \frac{\partial_{x_1}^{m_{1,0}} \dots \partial_{x_g}^{m_{g,0}} R(\bar{x})}{m_{1,0}! \dots m_{g,0}!} \Bigg|_{\bar{x}=\bar{x}_0} \right| &\leq |H(\bar{u}_0)|^{-nD} \\ &\times g^M c_0^M (D+1)^n \cdot H \cdot \exp\{\alpha nD \cdot T^\rho\} \cdot T^{-M} \cdot \frac{M!}{\Gamma(\frac{M}{g})^g}, \end{aligned} \tag{5.18}$$

$|\vec{m}_0| = M$ and $M > nD$. We can now choose a parameter T in the following way $T = (M/(nD))^{1/\rho} > 1$. We remark now that $M \geq D^{(n-\varepsilon)/g}$ according to Lemma 5.10 and $(n-\varepsilon)/g \geq 1$ by the choice of ε. Thus for a sufficiently large D, $D \geq D_3(\bar{u}_0, K, \varepsilon, \delta, H, H_1, \dots, H_n)$, the estimate (5.18) implies, very much like in (5.4), the following estimate:

$$|c| \leq c_{13}^{M} \cdot \left(\frac{M}{nD}\right)^{-M/\rho} \cdot D^{c_8 D^{(n-\varepsilon)/g-\varepsilon}} . \tag{5.19}$$

Here we used the bound (5.16) on H. We use now the Liouville inequality (5.11) over K:

$$|\mathrm{den}(c)^d| \cdot |\bar{c}|^{d-1} \cdot |c| \geq 1.$$

Combining this with (5.17), (5.19) we obtain

$$M^{[1-g/(n-\delta)] \cdot M/\rho} c_{14}^{M} \cdot \left(\frac{M}{nD}\right)^{-M/\rho} \cdot D^{c_{15} D^{(n-\varepsilon)/g-\varepsilon}} \geq 1.$$

However, $M \geq D^{(n-\varepsilon)/g}$, according to Lemma 5.10. Thus

$$M^{[1-g/(n-\delta)]/\rho} \cdot c_{14} \cdot M^{c_{16} M^{-\varepsilon g/(n-\varepsilon)}} \geq \left(\frac{M}{2M^{g/(n-\varepsilon)}}\right)^{1/\rho} . \tag{5.20}$$

For sufficiently large D (and M) and $\varepsilon < \delta$, the inequality (5.20) is impossible. This shows that $R(\bar{x})$ and functions $f_1(\bar{x}), \dots, f_n(\bar{x})$ are algebraically dependent over K.

Theorem 5.9 is an embodyment of various analytic criteria of retionality, algebraicity and algebraic dependence of functions associated with such diverse results as E. Borel criterion of rationality of a meromorphic function of 1903 [36], results of T. Schneider and T. Schneider-S. Lang on a algebricity of values of meromorphic functions satisfying differential equations [37], [38]. (See, especially Remark 5.11.) Perhaps, the most significant difference between our results and the known ones is the expansion of functions on their Riemann surfaces and not in powers of the uniformizing variables.

Concerning the definition ξ of the rate of growth of denominators in the Theorem 5.9, it can be slightly modified to $\xi = \limsup_{M\to\infty} \log|D'_M|/M \log M$, with D'_M denoting the common denominator of $\{a_{\vec{m};k_1,\dots,k_n} \; |\vec{m}| \leq M,\ k_1 + \dots + k_n \leq M^{g/(n-\delta)}\}$ over K for some $\delta > 0$. The typical situation can be considered that of D_M (or D'_M) dividing $M!$. This happens whenever in the expansion of $f_i(\bar{x}) = \Sigma_{\vec{m}}\, a_{\vec{m}}^{(i)} (\bar{x}-\bar{x}_0)^{\vec{m}}$, $a_{\vec{m}}^{(i)}$ has the form $a_{\vec{m}}^{(i)} = A_{\vec{m}}^{(i)}/|\vec{m}|!$ for an algebraic inter $A_{\vec{m}}^{(i)}$: $i = 1, \dots, n$. If this happens and there exists a set C of primes p having density λ, such that every prime $p \in C$ is relatively prime with the denominator of any $a^{(i)}_{\vec{m}}$ $(i = 1,\dots,n)$, then

$$\xi \leq (1-\lambda) .$$

Consequently, Theorem 5.10 can be reformulated as a statement that under its general assumptions, $\tilde{\sigma} < \infty$ and $1-(1-g/n)/(\rho d) < \lambda$ implies the algebraic dependence of $f_1(\bar{x}),\dots,f_n(\bar{x})$ over K. Theorem 5.9 in this form, or in any similar form, is already close to (if not) the best possible.

Another peculiar set of applications is supplied by derivatives of a given function $f(\bar{x})$, which can be uniformized by meromorphic functions, and has "controllable" denominators of coefficients of its expansion at $\bar{x} = \bar{x}_0$. Then Theorem 5.9 implies that under suitable assumptions on the growth of denominators, $f(\bar{x})$ satisfies a system of algebraic partial differential equations.

Remark 5.11: In the spirit of Schneider-Lang theorem and its multidimensional generalizations (most notably the theorems of Bombieri and Lang [39], [40]), we can easily generalize Theorem 5.9 to the case of expansions at several points. We do not envision, however, any new applications of such results to transcendental problems where the sharpness of our estimates is unnecessary.

Theorem 5.12: Let $n \geq g + 1$ and let there be p points $\bar{x}_j (j = 1,\dots,p)$ such that we have Taylor expansions of functions $f_1(\bar{x}),\dots,f_n(\bar{x})$ at $\bar{x} = \bar{x}_j$ in the following notations $f_1(\bar{x})^{k_1}\dots f_n(\bar{x})^{k_n} = \Sigma_{\vec{m}}\, a_{\vec{m};k_1,\dots,k_n;j}(\bar{x}-\bar{x}_j)^{\vec{m}}$, $a_{\vec{m};k_1,\dots,k_n;j} \in K$, $j = 1,\dots,n$. We denote by $D_{M,j}$ the common denominator of $\{a_{\vec{m};k_1,\dots,k_n;j}: |\vec{m}| \leq M,$ $k_1 +\dots+ k_n < M\}$ over K. Let there exist meromorphic functions $U_1(\bar{u}),\dots,U_n(\bar{u})$ of order of growth $\leq \rho$ in $\mathbb{C}^g$ and the transformation $(x_1,\dots,x_g) \rightsquigarrow (u_1,\dots,u_g)$, such that $\bar{x}_j \rightsquigarrow \bar{u}_j$, the functions $U_i(\bar{u})$ are regular at $\bar{u} = \bar{u}_j$ $(i = 1,\dots,n; j = 1,\dots,p)$ and the Jacobian $D(u_1,\dots,u_g)/D(x_1,\dots,x_g)$ of the transformation is nonsingular at $\bar{x} = \bar{x}_j$ (or $\bar{u} = \bar{u}_j$), $j = 1,\dots,p$. Let, in the neighborhood of $\bar{u} = \bar{u}_j$ we have the uniformization $f_i(\bar{x}) = U_i(\bar{u})$, $f_i(\bar{x}_j) = U_i(\bar{u}_j)$ consisting of the expansion (branch) of $f_i(\bar{x})$ at $\bar{x} = \bar{x}_j$ $(i = 1,\dots,n;$ $j = 1,\dots,p)$. If points $\bar{u}_j$ do not lie on a hypersurface of degree $<$ m and if

$$\tilde{\sigma} = \lim\sup_{M\to\infty}\{\overline{|a_{\vec{m};k_1,\dots,k_n;j}|}^{1/M}: |\vec{m}| \leq M;\ k_i = 0,1;$$
$$j = 1,\dots,p\} < \infty,$$

$$\xi = \limsup_{M\to\infty} \frac{\log \max\{|D_{M,1}|,\ldots,|D_{M,p}|\}}{M \log M},$$

then $\xi < (1-g/n)\cdot m/d\rho$ implies that the functions $f_1(\bar{x}),\ldots,f_n(\bar{x})$ are algebraically independent over K.

The proof of Theorem 5.12 is essentially the same as that of Theorem 5.9 with the use of Lemma 5.1 substituted by the use of Schwartz's lemma (cf. [39],[40]).

We note that the condition on the sizes of coefficients in the expansion of functions $f_1(\bar{x}),\ldots,f_n(\bar{x})$, $\tilde{\sigma} < \infty$ can be considerably relaxed as well. In fact, we can assume the same growth of $\max\{\overline{|a_{\vec{m};k_1,\ldots,k_n}|}^{1/M}: |\vec{m}| \le M,\ k_j = 0,1\}$ with M as that of D_M. We do not do this because it is natural to assume the regularity of functions $f_i(\bar{x})$ and of all functions conjugate to them, cf. Remark 5.3.

Remark 5.13: (i). Let us put for every $\sigma = 1,\ldots,d$, $f^{(\sigma)}(\bar{x}) = \Sigma_{\vec{m}}\ a^{(\sigma)}_{\vec{m};1}\ (\bar{x}-\bar{x}_0)^{\vec{m}}$. If now for every $\sigma = 1,\ldots,d$, the system of functions $x_1,\ldots,x_g,f^{(\sigma)}(\bar{x})$ is uniformized near $\bar{x} = \bar{x}_0$by meromorphic functions of order of growth $\le \rho$ in $\mathbb{C}^g$ (see Theorem 5.2 for $\sigma = 1$), then the assumptions of Theorem 5.2 can be substituted by $\tilde{\sigma} < \infty$ and $\limsup_{k\to\infty} \gamma_k/\log k < 1/(\rho g)$. Under these assumptions, $f(x_1,\ldots,x_g)$ is an algebraic function over $K(x_1,\ldots,x_g)$.

(ii). Let us put for every $\sigma = 1,\ldots,d$ and $i = 1,\ldots,n$: $f_i^{(\sigma)}(\bar{x}) = \Sigma_{\vec{m}}\ a^{(\sigma)}_{\vec{m};0,\ldots,\underset{i}{1},\ldots,0}\ (\bar{x}-\bar{x}_0)^{\vec{m}}$. Let now for every $\sigma = 1,\ldots,d$, the system of functions $\{f_1^{(\sigma)}(\bar{x}),\ldots,f_n^{(\sigma)}(\bar{x})\}$ is uniformized near $\bar{x} = \bar{x}_0$ by meromorphic functions of order of growth $\le \rho$. Then the assumptions of Theorem 5.8 can be substituted by: $\tilde{\sigma} < \infty$ and $\limsup_{k\to\infty}\gamma_k/\log k < (n-g)/(\ \rho g\ )$ and the assumptions of Theorem 5.9 can be substituted by: $\tilde{\sigma} < \infty$ and $\xi < (1-g/n)/\rho$. Under either of these assumptions, $f_1(\bar{x}),\ldots,f_n(\bar{x})$ are algebraically dependent over K.

The proof of Remark 5.13 is trivial. One only has to add to (5.11) the bound on $|\bar{c}|$, identical to that of (5.10) to obtain (i), and one has to add to (5.19) the identical bound on $|\bar{c}|$ to obtain (ii).

§6. Elliptic functions.

We collect here some well-known results on elliptic curves, Abelian differentials on them, and on the Weierstrass's elliptic function parametrizations, see, e.g. [19]. Our starting point is the elliptic curve E given in its Weierstrass form by the equation $y^2 = 4x^3 - g_2x - g_3$, where $4x^3 - g_2x - g_3 = 4(x-e_1)(x-e_2)(x-e_3)$ and e_1,e_2,e_3 are distinct. Unique (up to a constant) differential of the firs kind on E is dx/y. Similarly, the unique (again up to a multiplicative constant) differential of the second kind on E is xdx/y. Now let ω be an arbitrary differential form on E and let (x_i,y_i): $i = 1,\dots,n$ be n finite points of E that are poles of ω and let c_i be a residue of ω at (x_i,y_i): $i = 1,\dots,n$. Then $\omega - 1/2\ \Sigma_{i=1}^{n} c_i \frac{y+y_i}{x-x_i} \cdot \frac{dx}{y}$ is a differential of the first or second kind. Hence there exist constants c_0, c_{-1} and a rational function $f = f(x,y)$ on E such that

$$(6.1) \qquad \omega = \frac{1}{2}\ \Sigma_{i=1}^{n} c_i \cdot \frac{y+y_i}{x-x_i}\frac{dx}{y} + c_0\frac{dx}{y} + c_{-1}\frac{xdx}{y} + df.$$

Let the curve E be defined over $\bar{\mathbb{Q}}$. This means that $4x^3 - g_2x-g_3 \in \bar{\mathbb{Q}}[x]$ or that e_1,e_2,e_3 are algebraic numbers. Then we say that a differential ω is defined over $\bar{\mathbb{Q}}$, when c_i are algebraic numbers; $i = -1,0,1,\dots,n$; and (x_i,y_i) are algebraic points on $E_{\bar{\mathbb{Q}}}$, and f is a rational function from $\bar{\mathbb{Q}}(E)$.

With the elliptic curve E we associate Weierstrass's elliptic functions corresponding to the lattice $L = 2\omega\mathbb{Z} + 2\omega'\mathbb{Z}$ in $\mathbb{C}$, where $\mathrm{Im}(\omega'/\omega) > 0$ and $g_2 = 60\ \Sigma_{w\in L, w\neq 0} w^{-4}$, $g_3 = 140\ \Sigma_{w\in L, w\neq 0} w^{-6}$. The initial object is the Weierstrass σ-function, $\sigma(u) = u \times \prod_{w\in L, w\neq 0}\{(1-u/w)\cdot\exp[u/w+1/2\cdot(u/w)^2]\}$. Then we define ζ- and $\wp$-functions of Weierstrass: $\zeta(u) = \frac{d}{du}\log\sigma(u)$, $\wp(u) = -\frac{d}{du}\log\zeta(u)$. The function $\sigma(u)$ is an entire function of order of growth two. (In fact, it is closely related to Jacobi's theta functions, for putting $\eta = \zeta(\omega)$, $q = e^{i\pi\omega'/\omega}$ and $\theta_1(v) = 2q^{1/4}\cdot\Sigma_{n=0}^{\infty}(-1)^n q^{n(n+1)}\sin[(2n+1)\pi v]$, we obtain: $\sigma(u) = 2\omega\cdot\exp[\eta u^2/2\omega]\cdot\theta_1(u/2\omega)/\theta_1'(0)]$. Consequently, $\zeta(u)$ and $\wp(u)$ are meromorphic functions of order of growth two. The functions $(\wp(u),\wp'(u)) = (x,y)$ parametrize $E_{\mathbb{C}}$. Similarly, we can parametrize an Abelian differential ω from (6.1) by Weierstrass's functions. For this (and for Lamé's equations studied below) it is convenient to introduce the following Hermite's function:

$$(6.2) \qquad H(v;u) = \frac{\sigma(u-v)}{\sigma(u)\sigma(v)}e^{\zeta(v)u}.$$

It is convenient to present, in the connection with the function (6.2), two identities, known as addition theorems for ζ- and σ-functions:

$$(6.3) \qquad \begin{aligned}\frac{d}{du}H(v;u) &= \zeta(u-v)+\zeta(v)-\zeta(u)\\ &= \frac{1}{2}\cdot\frac{\wp'(u)+\wp'(v)}{\wp(u)-\wp(v)}\end{aligned}$$

$$(6.4)\qquad \frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = \wp(v) - \wp(u).$$

For the parametrization of ω in (6.1), let u_i be a Weierstrass parameter of (x_i,y_i) on E, i.e. $\wp(u_i) = x_i$, $\wp'(u_i) = y_i$: $i = 1,\ldots,n$. Then (6.4) implies the following representation:

$$(6.5)\qquad \omega = \frac{1}{2}\,\Sigma_{i=1}^{n}\, c_i \,\frac{d}{du}\,\log H(u_i;u)du + c_0du + c_{-1}d\zeta(u) + df.$$

We also remark that ω is a differential of the third kind, when $n \geq 1$, $c_{-1} = 0$ and $f = 0$. (Also, ω has a zero sum of the residues of its poles on E--including at the point at infinity.)

The uniformization of Abelian differentials on E by means of meromorphic functions on $\mathbb{C}$ allows us to prove the Grothendieck conjecture for any rank one equation over E. This particular case of the Grothendieck conjecture was put forward by Katz ([1], Chapter 7), who presented in [1], §7.5 an interesting reformulation of this conjecture as an arithmetic version of Manin's theorem of the Kernel [20]. We have:

Theorem 6.1: If the elliptic curve E is defined over $\bar{\mathbb{Q}}$, then any linear differential equation of rank one over E satisfies the Grothendieck conjecture. I.e. if this equation has sufficiently many solutions (in a weak sense) (mod $\wp$) for almost all $\wp$, or if its p-curvature is niloptent for almost all p, then the solutions of the equation are algebraic.

Proof: We follow the discussion of [1], §7.1-7.4. If the linear differential equation of rank one over E has the form

$$(6.6)\qquad \frac{dF}{dx} = w,$$

for $w \in \bar{\mathbb{Q}}(F)$, then $\omega \overset{\text{def}}{=} w\,dx$ is an Abelian differential on E. According to Corollaries 1.2 and 1.4 we can assume that the equation (6.6) is Fuchsian with rational exponents at regular singularities of (6.6). Hence, ω has poles of at most first order with the residues at poles being the rational numbers. Hence, following([1],§7.4), the differential ω has the form (6.1) with $c_{-1} = 0$, $f = 0$ and rational numbers $c_1,\ldots,c_n$ (for algebraic numbers $x_1,y_1,\ldots,x_n,y_n,c_0$). Then, as in ([1], §§7.4-7.5), after the multiplication of ω by a (rational) integer $N \geq 1$, we can assume that all residues $c_i = 2k_i$; $i = 1,\ldots,n$ are rational even integers. Let now $P = (\zeta,\xi)$ be a finite algebraic point on E, different from branch points of E (i.e. $\zeta \neq e_i$; $i = 1,2,3$ and $\xi \neq 0$) and from the singularities of (6.6) (i.e. in the notations of (6.1), $(\zeta,\xi) \neq (x_i,y_i)$: $i = 1,\ldots,n$). Let $F = F(x)$ be a solution of (6.6), normalized at P: $F(\zeta) = 1$. We assume now that (6.6) satisfies all conditions of the Grothendieck conjectures i.e. the p-curvature of (6.6) is nilpotent (zero) for almost all p. We have to prove that $F(x)$ is an algebraic function. Let us consider the expansion of $F(x)^j$ at $x = \zeta$: $F(x)^j = \Sigma_{n=0}^{\infty} f_{n,j}(x-\zeta)^n$, for algebraic $f_{n,j}$ (from the field $\mathbb{Q}(g_2,g_3,c_0,x_1,\ldots,x_n,y_1,\ldots,y_n,\zeta)$). Then, according to the Corollary 2.5, the common denominator $\Delta_{M;k}$ of $\{f_{n,j}: n = 0,\ldots,M; j = 1,\ldots,k\}$ satisfies $\log|\Delta_{M;k}| \leq M\cdot\gamma_0 + k\cdot\gamma_1$ for constants γ_0, γ_1 depending only on E, (6.6), ζ and an exceptional set S of primes p (for which p-curvature is non-zero). Also, since ζ is not a singularity of (6.6), $|f_{n,1}|^{1/n} \leq \gamma_2$ for some $\gamma_2 > 0$. Thus in order to apply Main Theorem 5.2, we have to exhibit the meromorphic parametrization of x and $F(x)$. For this we use the Weierstrass parametrization $x = \wp(u)$, $y = \wp'(u)$ of E and (6.5). Let u_0 be a Weierstrass parameter such that $\zeta = \wp(u_0)$, $\xi = \wp'(u_0)$. According to (6.5)-(6.6), the solution $F(x)$ has the following uniformization:

$$\begin{aligned} F(x) &= \lambda\cdot \prod_{i=1}^{n} H(u_i;u)^{k_i}\cdot e^{c_0 u} \\ &= \lambda \prod_{i=1}^{n}\left\{\frac{\sigma(u-u_i)}{\sigma(u)\sigma(u_i)}\right\}^{k_i}\cdot \exp\{\Sigma_{i=1}^{n} k_i\zeta(u_i)\cdot u + c_0 u\}, \end{aligned} \tag{6.7}$$

for some constant $\lambda \neq 0$. In (6.7) all k_i are rational integers. Hence $x = \wp(u)$ and the representation $F(x) = G(u)$ in (6.7) give the uniformization by meromorphic functions of order of growth two. The non-degeneracy conditions of Main Theorem 5.2 are satisfied too, since $\wp(u)$, $G(u)$ are analytic at $u = u_0$ and $\wp'(u_0) \neq 0$ because u is distinct from period or half-periods of $\wp(u)$. Thus by Main Theorem 5.2, the function $F(x)$ is algebraic and Theorem 6.1 is proved.

Following ([1], §7.5) we conclude that Theorem 6.1 gives an interesting p-adic criterion for a point $P = (x,y)$ on E to be of finite order. Applications of this criterion to the construction of algorithms determining the reduction of elliptic integrals will be reported elsewhere.

We present one example on applications of Main Theorem 5.2 to the determination of density of primes p for which $c_p \equiv \text{const} \pmod p$ in the L-function $\Sigma_{n=1}^{\infty} c_n\cdot n^{-s}$ of an elliptic curve $E/\mathbb{Q}$. Though there exist analytic number theory approaches to this problem, the proposed method is particularly attractive because it does not require any knowledge of analytic properties of L-functions and relies only on formal groups connected with these L-functions. This makes it possible to extend our methods to a larger class of L-functions, associated with (arbitrary) algebraic varieties.

We start now with an arbitrary plane cubic model of an elliptic curve E defined by the equation: $y^2 + a_1xy + a_3y = x^3+a_2x^2+a_4x + a_6$.

The Weierstrass elliptic function parametrization of this model of E is given by the formulas:

$$\wp(u) = x + \frac{a_1^2 + 4a_2}{12}, \quad \wp'(u) = 2y + a_1x + a_3;$$

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3$$

(where $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, $12g_2 = b_2^2 - 24b_4$, $216g_3 = -b_2^3 + 36b_2b_4 - 216b_6$). As invariant differential ω on E has the form $\omega = dx/(2y + a_1x + a_3) = d\wp(u)/\wp'(u) = du$. Tate [21] has chosen the following local parameter: $z = - x/y$.

Then the expansion of the invariant differential ω at $z = 0$ has the form [21]:

$$\omega = dz(1+a_1z + (a_1^2 + a_2)z^2+\dots), \quad \text{or}$$

$$\omega = dz.f(z), f(z) = \Sigma_{m=1}^{\infty} b_m z^{m-1}, \quad b_1 = 1,$$

where b_m belong to $\mathbb{Z}[a_1,a_2,a_3,a_4,a_6]$: $m = 1,2,\dots$. Thus $du/dz = f(z)$ and we have the following expansion of the"elliptic logarithm" u:

$$(6.8) \qquad u(\overset{\text{def}}{=} L(z)) = \int f(z)dz = \Sigma_{m=1}^{\infty} \frac{b_m}{m} z^m.$$

Then the theorem on the isomorphism of formal group laws of E over $\mathbb{Z}$ shows the strict isomorphism between the group laws on E arising from (6.8) and arising from the global L-series $L(E;s)$ of E over $\mathbb{Q}$ (whenever $a_i \in \mathbb{Z}$): $L(E;s) = \Sigma_{n=1}^{\infty} c_n n^{-s}$ [22]. This implies Atkin-Swinnerton-Dyer congruences [22], among which one finds $b_p \equiv c_p$ (mod p) and this determines c_p uniquely for any prime $p > 3$, whenever the expansion (6.8) is known.

We remind that c_p is defined in terms of the Frobenius endomorphism of $\tilde{E}(p) = E(\text{mod } p)$, that $N_p = 1 + p - c_p$ is the number of points of $\tilde{E}(p)$ rational over $\mathbb{F}_p$ [21]. Also, if we deal with the Neron's minimal model of E, then $L(E,s) = \prod_p L_p(s)$, where $L_p(s) = (1 - c_p p^{-s} + p^{1-2s})^{-1}$ for primes p of good reduction and $L_p(s) = (1 - c_p p^{-s})^{-1}$ otherwise [21].

Remark 6.2: There is no need to appeal to the theory of formal groups to deduce the congruences of the form $b_p \equiv c_p$ (mod p) for (some) expansions of the logarithmic function on E. This can be also achieved using the Picard-Fuchs theory (in the case of elliptic curves, we use Legendre differentiaon equations of hypergeometric type) and its connection with Serre's duality following Manin, Clemens [23], Ch. 2. Such an elementary point of view can be attractive because of its easy realization for interesting classes of curves and algebraic varieties.

We find ourselves in the situation where we can apply Main Theorem 5.2 to the functions $(z,L(z))$, parametrized by Weierstrass elliptic functions--meromorphic function of order of growth two:

$$(6.9) \qquad z = -\frac{2\{\wp(u) - \frac{a_1^2 + 4a_2}{12}\}}{\{\wp'(u) - a_1(\wp(u) - \frac{a_1^2 + 4a_2}{12}) - a_3\}}; \qquad L(z) = u.$$

As in (6.8), we consider an expansion of $L(z)$ at the point $z = 0$, corresponding in the uniformization to $u = 0$.

Here $L(z)$ satisfies a second-order scalar linear differential equation. Combining the expression of the expansion of $L(z)$ at $z = 0$ in (6.8) with Proposition 2.6 and Main Theorem 5.2 we get the following density result:

Corollary 6.3: In the notations above for $L(E;s) = \Sigma_{n=1}^{\infty} c_n n^{-s}$, the density of primes p for which $c_p \equiv 0 \pmod p$, or $c_p = 0$, never exceeds 1/2.

Here we used the congruences $c_p \equiv b_p \pmod p$, and we have $g = 1$, $\rho = 2$ in Main Theorem 5.2.

In the standard language, those primes p for which $c_p \equiv 0 \pmod p$ are called supersingular for E. Though the density of supersingular primes is zero for elliptic curves E without complex multiplications [24], Corollary 6.3 is, in fact, best possible for curves with a complex multiplication. For example, for curves $y^2 = x^3 - Dx$, with complex multiplications in $\mathbb{Q}(i)$, all primes p, $p \equiv 3 \pmod 4$ are supersingular [density = 1/2--the limit set by Corollary 6.3].

Another class of primes--anomalous primes of Mazur [24], [25]--are those for which $c_p = 1$. These primes naturally arise from the expansion of $e^{L(z)}$ at $z = 0$. Here $e^{L(z)} = e^u$ is also uniformized by a meromorphic (entire) function of u.

In the problem of distribution of anomalous primes and other similarly problems our results seems to be nontrivial but far from the conjectural results of the Tate-Sato form [24]. Their interest lies in an elementary approach that we use and in an easy multidimensional generalization. For example, in §8 we treat in detail the generalization of anomalous primes for an arbitrary algebraic curve of genus $g \geq 1$.

§7. The Lamé equation.

We will follow now Dwork's discussion in([4], §6) to determine all cases of global nilpotence of Lamé equations using results of previous chapters. Simultaneously we prove the Grothendieck conjecture for this class of equations. The Lamé equation has the following algebraic form:

$$(7.1) \qquad P(x)\frac{d^2F}{dx^2} + \frac{1}{2}P'(x)\frac{dF}{dx} - \{n(n+1)x+B\}F = 0,$$

where $P(x) \overset{\text{def}}{=} 4x^3 - g_2x - g_3 = 4(x-e_1)(x-e_2)(x-e_3) \in \bar{\mathbb{Q}}[x]$, n is a nonnegative integer and $B \in \bar{\mathbb{Q}}$. The theory of Lamé equations shows ([19], §23.7) that there exists two solutions F_+ and F_- of (7.1) such that $F_+ \cdot F_- = Q(x,B)$ for a polynomial $Q(x,B)$ from $\bar{\mathbb{Q}}[x,B]$ of degree n. To prove this we consider a linear differential equation satisfied by products of solutions of (7.1):

$$4P(x)\frac{d^3}{dx^3}X + 3P'(x)\frac{d^2}{dx^2}X - 4\{(n^2+n-3)x+B\}\frac{dX}{dx} - 2n(n+1)X = 0.$$

We are looking for a solution X of this equation of the form $X = \Sigma_{m=0}^{\infty} c_m(x-e_1)^{n-m}, c_0 = 1$. The recurrence defining c_m is the following:

$$\begin{aligned} &4m(n-m+\tfrac{1}{2})(2n-m+1)c_m \\ &= (n-m+1)\{12e_1(n-m)(n-m+2)-4e_2(n^2+n-3)-4B\}c_{m-1} \\ &\quad - 2(n-m+1)(n-m+2)(e_2-e_1)(e_1-e_3)2n-2m+3)c_{m-2}. \end{aligned}$$

Thus we can put $c_{n+1} = 0$, $c_{n+2} = 0$ and $c_m = 0$ for all $m > n$. Consequently, the Lamé equation (7.1) has two solutions F_+ and F_- whose product is a polynomial $Q(x,B) = \Sigma_{m=0}^{n} c_m(x-e_1)^{n-m} \in \bar{\mathbb{Q}}[x,B]$. We will write this polynomial $Q(x,B)$ as $Q(x,B) = \prod_{i=1}^{n}(x-\xi_i)$. Then, according to [19] there are two possibilities: (i) when F_+/F_- is a constant, and (ii) when F_+ and F_- are linearly independent over $\mathbb{C}$. In case (i), (7.1) has an algebraic solutions $\sqrt{Q(x,B)}$. In case (i), B is equal to one of $2n+1$ characteristic values $B_n^m (1 \le m \le 2n+1)$ [19] of Lamé equation (7.1) (called in physics ends of lacunae of the spectrum of Lamé equation in the transcendental form, see below). Each of the numbers B_n^m is an algebraic number and one of the solutions of (7.1) with $B = B_n^m$ is an algebraic function, while there is a non-algebraic solution as well: $m = 1,\dots,2n+1$. Hence in the case (i), the equation (7.1) is globally nilpotent, i.e., has nilpotent p-curvature for almost all p (see [4], 6.7.1). In the case (ii) as it is shown in ([4], 6.7.2) the global nilpotence of the Lamé equation (7.1) implies that p-curvature is zero, $\Psi_p = 0$, for almost all p. In other words, in the case (ii) the global nilpotence and the assumptions of the Grothendieck conjecture for (7.1) are equivalent.

To see this, we remark, following ([4], 6.5), that in the case (ii), the equation (7.1) (mod p) can be decomposed into two equations of rank one, each of which also has nilpotent p-curvature (and, hence, zero p-curvature). In fact, $dF_{\pm}/dx = \gamma_{\pm}(x)F_{\pm}$, where $\gamma_{\pm}(x)$ lie in the quadratic extension of $\bar{\mathbb{Q}}(x)$ (i.e. in $\mathbb{Q}(E)$) and are conjugate over $\bar{\mathbb{Q}}(x)$. Expressions of $\gamma_{\pm}(x)$ in the transcendental form is presented below.

Thus we need the transcendental form of the Lamé equation (7.1). For this purpose we use the Weierstrass elliptic functions $\sigma(u), \zeta(u)$, $\wp(u)$, introduced above for the uniformization of the curve E: $y^2 = P(x) = 4x^3 - g_2x - g_3$. Under the change of the variable $x = \wp(u)$, the equation (7.1) takes the form:

$$(7.2) \qquad \frac{d^2}{du^2}F = \{n(n+1)\wp(u) + B\}F.$$

Let now, in the notations above, $\xi_i = \wp(a_i)$: $i = 1,\dots,n$, i.e. $Q(x,B) = \prod_{i=1}^n(\wp(u) - \wp(a_i))$, for $x = \wp(u)$. Then (see [19], §23.7), two solutions F_+ and F_-, mentioned above has the form

$$(7.3) \qquad F_{\pm} = \{\prod_{i=1}^n \frac{\sigma(a_i \pm u)}{\sigma(u)\sigma(a_i)}\}\cdot\exp\{\mp u \Sigma_{i=1}^n \zeta(a_i)\},$$

where F_+F_-, according to (7.4), has the form $Q(x,B) = \prod_{i=1}^n(x-\xi_i)$ with $\xi_i = \wp(a_i)$: $i = 1,\dots,n$. Parameters a_i: $i = 1,\dots,n$ can be determined from (see [26]) the following system of equations on a_i:

$$(2n-1)\ \Sigma_{i=1}^n\ \wp(a_i) = B,$$

$$\Sigma_{j=1,j\neq i}^n(\wp'(a_i) + \wp'(a_j))/(\wp(a_i)-\wp(a_j)) = 0 \text{ for all}$$

$$i = 1,\dots,n\ .$$

Hence, according to (7.3), for every $B \neq B_n^m$ $(1 \leq m \leq 2n + 1)$, any solution $F = F(u)$ of (7.2) is a meromorphic function in u of order growth two. Moreover, for any $B = B_n^m$ $(1 \leq m \leq 2n + 1)$ all solutions of (7.2) are meromorphic functions in u. Indeed, one solution $F_1(x)$, algebraic in x, has one of the following four forms $F_1 = P_k(\wp(u))$; $F_1 = [\wp(u)-e_i]^{1/2}\cdot[\wp(u)-e_j]^{1/2}\cdot P_{k-1}(\wp(u))$ $(n = 2k)$; $F_1 = [\wp(u)-e_i]^{1/2}\cdot P_{k-1}(\wp(u))$;$F_1 = \wp'(u)P_{k-2}(\wp(u))$ $(n = 2k-1)$. The second, nonalgebraic solution $F_2(x)$ has the form ([19], 23.47) $F_2 = (\alpha + \beta\zeta(u))\cdot F_1 + w(u)$, where α, β are constants, $|\alpha| + |\beta| > 0$, and $w(u)$ is elliptic function (i.e. $w(u)$ in x-variable is algebraic). Consequently, <u>all</u> solutions of (7.2) are meromorphic functions in u of order of growth two.

We also remark that functions F_+, F_- from (7.3) are equal (up to a sign) to $\prod_{i=1}^{n} H(a_i,u)$ and $\prod_{i=1}^{n} H(-a_i,u)$, respectively, in the notations of §6. Consequently, $F_{\pm}$ satisfy the following rank one equations:

$$\frac{dF_{\pm}}{du} = \Sigma_{i=1}^{n}\{\pm\zeta(a_i \mp u) \mp \zeta(a_i) - \zeta(u)\}\cdot F_{\pm}$$

$$= \frac{1}{2}\,\Sigma_{i=1}^{n}\,\frac{\wp'(u)\mp\wp'(a_i)}{\wp(u)-\wp(a_i)}F_{\pm}.$$

Here we used (6.3). Thus $dF_{\pm}/dx = \gamma_{\pm}(x)F_{\pm}$, where $\gamma_{\pm}(x)$ are rational functions on E: $\gamma_{\pm} \in \bar{\mathbb{Q}}(E)$. Consequently, we can directly apply Theorem 6.1 for the proof of Grothendieck conjecture in case (ii).

Remark 7.1: There is another representation of $F_{\pm}$ in terms of the function $H(v;u)$ from §6 [26]. For $B \neq B_n^m$ $(1 \leq m \leq 2n+1)$, there are two linearly independent solutions of (7.2) that can be expressed in the form: $F = \Sigma_{j=0}^{n-1} b_j \; d^j/du^j\{H(v;u)\cdot e^{\rho u}\}$, where $H(v;u) = \frac{\sigma(u-v)}{\sigma(u)\sigma(v)}e^{\zeta(v)u}$ and $b_0,\ldots,b_{n-1},\rho,\wp(a)$ are determined algebraically in terms of B and g_2,g_3.

The main result of this chapter is an answer to Dwork's problem [4].

Theorem 7.2: For an integer $n \geq 0$ the Lamé equation (7.1) never satisfies the assumptions of the Grothendieck conjecture, i.e. p-curvature ψ_p is non-zero for infinitely many p (and even $\psi_p \neq 0$ for a positive density of p's). There are $2n + 1$ (algebraic) values of B—namely B_n^m: $m = 1,\ldots,2n+1$—for which the equation (7.1) is globally nilpotent (has nilpotent p-curvature for alsmot all p). For all other values of B, the equation (7.1) is not globally nilpotent.

Proof: In the case (ii), as we have seen, the global nilpotence and the assumptions of the Grothendieck conjecture for the equation (7.1) are equivalent. Since all solutions of (7.1), togehter with $x = \wp(u)$, are parametrized by meromorphic functions of u, Corollary 2.5 and Main Theorem 5.2 show that the assumptions of the Grothendieck conjecture for (7.1) imply that all solutions of (7.1) are algebraic functions, which is impossible for any B. This, and the discussion of the case (ii), proves Theorem 7.2.

We conclude this chapter with a few remarks on the generalized Lamé equation (7.1) with arbitrary (non-integer) n. Only cases $n \in \mathbb{Q}$ are interesting, since otherwise exponents at ∞ of (7.1) are not rational numbers. The case $n = -1/2$ is most interesting in view of its obvious connection with the uniformization of punctured torus by a Fuchsian group. In this and other cases we hope to prove that there exist only finitely many (algebraic) B in (7.1), for which (7.1) is globally nilpotent. More general conjecture of this sort was formulated by Dwork [4].

Another interesting generalization of Lamé equations is given by Sturm-Liouville equations $F_{zz} - \{U(z) + B\}F = 0$, having finite-band structure [27], [28]. In this case the potential U(z) satisfies a stationary Korteweg-de Vries equation and U(z), F(z) are meromorphic functions arising from Abelian functions on a Jacobian of some algebraic curve Γ of genus $g \geq 1$. Then for the algebraic forms (on Γ) of equations $F_{zz} - \{U(z) + B\}F = 0$ we can establish the truth of the Grothendieck conjecture. This subject is connected, however, with the results of the next chapter.

§8. Abelian functions and Abelian integrals.

Similarly to the theory of elliptic integrals and elliptic functions, there exists a theory of Abelian integrals and Abelian functions of arbitrary genus $g \geq 1$. We can use this theory (see [29]-[34]) to solve the Grothendieck problem for arbitrary linear differential equations of rank one over algebraic curves of genus $g \geq 1$. Moreover, the Grothendieck conjecture can be established for a large class of linear differential equations, generalizing Lamé equations from §7. These equations arise in the theory of completely integrable systems of isospectral deformation origin and correspond to families of vector bundles over algebraic curves [27], [28]. The particular case, corresponding to linear bundles over an albebraic curve [27], describes pairs of commuting linear differential operators of relatively prime orders [35]. This case is an immediate generalization of a trancendental form (7.2) of the Lamé equations. In the algebraic form, they represent Fuchsian linear differential equations, whose solutions can be parametrized by Abelian integrals and Abelian functions.

We treat now one particular case, when easy algebraic formulas are available since Abel. This case is of interest also because it is an immediate generalization to an arbitrary curve of Deline's example [4], [7] given by the Lamé equation with $\dot{n} = 0$. For $g = 1$ it is connected with the problem of anomalous primes, see §6.

Thus, let us start with the curve Γ, defined by an irreducible equation $p(z,w) = 0$ of genus g. Let $R_1(z,w),\dots,R_g(z,w)$ be rational functions on Γ such that $\int_a^z R_1(z,w)dz,\dots,\int_a^z R_g(z,w)dz$ are g linearly independent Abelian integrals of the first kind. (As usual, an Abelian integral $\int_\gamma R(z,w)dz$ on Γ is called an integral of the first kind, if its value remains finite after the integration along any path γ on the Riemann surface of Γ. For the genus g of (the Riemann surface of) Γ, there are exactly g linearly independent Abelian integrals of the first kind on Γ).

In the classical formulation of the Jacobi-Abel inversion problem one considers the following sums of values of Abelian integrals of the first kind:

$$(8.1)\qquad \begin{aligned} &\int_a^{z_1} R_1 dz + \ldots + \int_a^{z_g} R_1 dz = u_1 \\ &\int_a^{z_1} R_g dz + \ldots + \int_a^{z_g} R_g dz = u_g. \end{aligned}$$

Here $u_1,\ldots,u_g$ are multivalued functions of $z_1,\ldots,z_g$ since they are determined modulo the periods of Abelian integrals of the first kind.

The classical Jacobi-Abel inversion theorem (8.1) states that the symmetric functions of $z_1,\ldots,z_g$ from (8.1) are Abelian function of variables $u_1,\ldots,u_g$. In other words, symmetric functions of $z_1,\ldots,z_g$ are meromorphic (and 2g-periodic) functions of variables $u_1,\ldots,u_g$. From Riemann's Theta-function theory [29], [30], it follows that these meromorphic functions are always of order of growth two. Let us denote by x_k the k-th elementary symmetric function in $z_1,\ldots,z_n$: $x_k = \Sigma_{i_1<\ldots<i_k} z_{i_1}\cdots z_{i_k}$, $k = 1,\ldots,n$. Then according to the Jacobi-Abel inversion problem, $x_k = U_k(u_1,\ldots,u_g)$, where $U_k(u_1,\ldots,u_g)$ is a meromorphic function of $u_1,\ldots,u_g$ of order of growth 2, where $u_i = \Sigma_{j=1}^{g} \int_a^{z_j} R_i(z,w)dz$: $i,k = 1,\ldots,g$.

It is important to note that there is no need to assume that functions $x_i = U_i(u_1,\ldots,u_g)$ $(i = 1,\ldots,g)$ are elementary symmetric functions in $z_1,\ldots,z_g$. It is, in fact, sufficient to assume that there exists functions x_i $(i = 1,\ldots,g)$ algebraic in $z_1,\ldots,z_g$ with a non-zero Jacobian $D(x_1,\ldots,x_g)/D(z_1,\ldots,z_g)$, and such that $x_i = U_i(u_1,\ldots,u_g)(i = 1,\ldots,g)$ for Abelian (meromorphic) functions $U_i(u_1,\ldots,u_g)$ $(i = 1,\ldots,g)$. Such general point of view is more convenient, because in the explicit solutions of Jacobi-Abel inversion problem, often x_i $(i = 1,\ldots,g)$ are complicated symmetric functions of $z_1,\ldots,z_g$. For (arbitrary) algebraic functions $x_i (i = 1,\ldots,g)$ of $z_1,\ldots,z_g$ we use Main Theorem 5.2 in the form of Remark 5.6, with $x_i = \alpha_i (i = 1,\ldots,g)$.

Let us apply this formulation of the Jacobi-Abel inversion problem to the solution of the Grothendieck conjecture for a linear differential equation

$$(8.2)\qquad \frac{dF}{dz} = R(z,w)F,$$

where $\int_a^z R(z,w)dz$ is an arbitrary Abelian integral of the first kind on Γ. For $g = 1$ and the equation of Γ in the Weierstrass form, the equation (8.2) corresponds to the decomposition of the Lamé equation

(8.1) with $n = 0$ into two equations of rank one over Γ.

Let $\int_a^z R(z,w)dz = \Sigma_{i=1}^g b_i \int_a^z R_i(z,w)dz$ for g linearly independent Abelian integrals $\int_a^z R_i(z,w)dz$: $i = 1,\dots,g$ of the first kind on Γ. The general solution $F = F(z)$ of (8.2) has the form

$$F(z) = c\cdot\exp\{\int_a^z R(z,w)dz\},$$

for a constant c.

Let us assume that the curve Γ and the equation (8.2) are defined over $\bar{\mathbb{Q}}$, i.e. the $p(z,w) \in \bar{\mathbb{Q}}[z,w]$, $R(z,w) \in \bar{\mathbb{Q}}(z,w]$. Let us assume now that the equation (8.2) is globally nilpotent, i.e. that the equation (8.2) has sufficiently many solutions (mod p) (or that the p-curvature of (8.2) is nilpotent) for almost all p. Then for any algebraic point $P = (\zeta,\xi)$ on Γ, distinct from the singularities (branch points) of Γ and from the singularities of (8.2), the expansion of the solution $F(z)$ of (8.2) with the algebraic initial condition at P, $F(z)|_{z=\zeta} \in \bar{\mathbb{Q}}$ satisfies the following properties. If $F(z)|_{z=\zeta} \in \bar{\mathbb{Q}}$ and $F(z) = \Sigma_{n=0}^\infty f_n(z-\zeta)^n, F(z)^j = \Sigma_{n=1}^\infty f_{n,j}(z-\zeta)^n$, then $f_{n,j} \in K$ for a fixed algebraic number field K and the common denominator $\Delta_{M;k}$ of $\{f_{m_1}\dots f_{m_j} : m_1 +\dots+ m_j \le M;\ j = 1,\dots,k\}$ satisfies $\sup_k \lim\sup_{M\to\infty} |\Delta_{M;k}|^{1/M} < \infty$. This is a direct consequence of Corollary 2.5. We remark that the common denominator of $\{f_{n,j}: n=0,\dots,M;\ j=1,\dots,k\}$ divides $\Delta_{M;k}$.

Let $\bar{x}_0 = (\zeta_1,\dots,\zeta_g)$, where $P_i = (\zeta_i,\xi_i): i = 1,\dots,g$ are algebraic points on Γ satisfying the following "nondegeneracy" conditions: i) the Abelian functions $U_i(u_1,\dots,u_g)$ such that $x_i = U_i(u_1,\dots,u_g)$ $(i = 1,\dots,g)$ are analytic at a point $\bar{u}_0 \in \mathbb{C}^g$, where $\zeta_i = U_i(\bar{u}_0)$: $i = 1,\dots,g$; ii) the Jacobian $D(U_1,\dots,U_g)/D(u_1,\dots,u_g)$ is non-singular at $\bar{u} = \bar{u}_0$, or, equivalently, $D(u_1,\dots,u_g)/D(x_1,\dots,x_g)$ is non-singular at $\bar{x} = \bar{x}_0$; iii) the discriminant of the polynomial $x^g - \zeta_1 z^{g-1} +\dots+ (-1)^g \zeta_g = 0$ is non-zero *); and iv) all points P_i are distinct from the branch points of Γ and are distinct from the singularities of the equation (8.2). Thus $P_1 +\dots+ P_g$ is a generic (say, non-special) divisor on Γ. We note in the connection with ii), that $D(u_1,\dots,u_g)/D(x_1,\dots,x_g) \not\equiv 0$ since integrals $\int_a^z R_k(z,w)dz$ $(k = 1,\dots,g)$ are linearly independent. The non-degeneracy conditions i)-ii) correspond to the non-degeneracy requirements of the Main

*). If, as above, x_i $(i=1,\dots,g)$ are some algebraic functions in $z_1,\dots,z_g$, then we demand here that the Jacobian $D(z_1,\dots,z_g)/D(x_1,\dots,x_g)$ is nonsingular at $\bar{x} = \bar{x}_0$.

Theorem 5.2 on the uniformization of $x_1,\ldots,x_g, f(x_1,\ldots,x_g)$ by the meromorphic functions of $u_1,\ldots,u_g$.

We choose solutions $F_i = F_i(z)$ of (8.2) with algebraic initial conditions at $P_i = (\zeta_i,\xi_i)$: $F_i(z)|_{(z,w)=(\zeta_i,\xi_i)} \in \bar{\mathbb{Q}}$, so that $F_i(z) = c_i\cdot\exp\{\int_a^z R(z,w)dz\}$for constants $c_i \neq 0$: $i = 1,\ldots,g$. We form a new function

$$f(x_1,\ldots,x_g) = c_1\cdots c_g\cdot\exp\{\int_a^{z_1} R(z,w)dz +\ldots+ \int_a^{z_g} R(z,w)dz\}.$$

(Here $f(x_1,\ldots,x_g)$ is a symmetric function of $z_1,\ldots,z_g$). In the notation of (8.1) we get :$f(x_1,\ldots,x_g) = c_1\cdots c_g\cdot\exp\{\Sigma_{i=1}^g\Sigma_{j=1}^g b_j\int_a^{z_i} R_j(z,w)dz\}=c_1\cdots c_g \times \exp\{\Sigma_{j=1}^g b_ju_j\}$. Hence, the system of functions $x_1,\ldots,x_g$, $f(x_1,\ldots,x_g)$ are parametrized by meromorphic functions of $u_1,\ldots,u_g$ as follows: $x_k = U_k(u_1,\ldots,u_g)$ $(k = 1,\ldots,g)$ and $f(x_1,\ldots,x_g) = c_1\cdots c_g\ \exp\{\Sigma_{j=1}^g b_ju_j)$. We also note that

$$f(x_1,\ldots,x_g) = c_1\cdots c_g\cdot F_1(z_1)\cdots F_g(z_g).$$

Now let us choose g roots $z_{1,0},\ldots,z_{g,0}$ of the algebraic equation $r(z;\bar{x}_0) \overset{\text{def}}{=} z^g - \zeta_1 z^{g-1} +\ldots+ (-1)^g\zeta_g = 0$**),where $z_{i,0}$ $(i= 1,\ldots,g)$ are all distinct according to the non-degeneracy condition iii), and $\frac{\partial}{\partial z}\ r(z;\bar{x}_0)|_{z=z_{i,0}} \neq 0$ $(i = 1,\ldots,g)$. Thus we can expand a function $z_i = z_i(x_1,\ldots,x_g)$, satisfying an algebraic equation $r(z;\bar{x}) \overset{\text{def}}{=} z^g - x_1z^{g-1} +\ldots+ (-1)^g x_g = 0$**), with the initial condition $z_i(\bar{x}_0) = z_{i,0}$: $i = 1,\ldots,g$. Here we have $0 \equiv \frac{\partial}{\partial x_j} r(z_i;\bar{x}) = \frac{\partial z_i}{\partial x_j}\frac{\partial}{\partial z}\ r\ (z;\bar{x})|_{z=z_i} + (-1)^j z_i^{g-j}$. Since $\frac{\partial}{\partial z}\ r(z;\bar{x}_0)|_{z=z_i} \neq 0$ we obtain an expansion of $z_i = z_i(\bar{x})$ in the Taylor series at $\bar{x} = \bar{x}_0$: $z_i = \Sigma_{m_1,\ldots,m_g=0}^{\infty}\ c_{m_1,\ldots,m_g;i}\quad (x_1-x_{1,0})^{m_1}\ldots(x_g-x_{g,0})^{m_g}$, $i = 1,\ldots,g$. Here $c_{m_1,\ldots,m_{g;i}}$ are algebraic numbers from $\mathbb{Q}[\zeta_1,\ldots,\zeta_g,z_{i,0}]$ (in fact they are rational functions of variables

**) If, as above, x_i $(i = 1,\ldots,g)$ are some algebraic functions in $z_1,\ldots,z_g$ then $r(z;\bar{x}_0)$ and $r(z;\bar{x})$ denote the minimal polynomials defining z_i $(i = 1,\ldots,g)$ as algebraic functions of $x_{i,0}$ and x_i $(i = 1,\ldots,g)$ respectively.

$x_{i,0},\dots,x_{g,0},z_{i,0}$),and, according to the Eisenstein theorem, there exists an integer $A \geq 1$ such that $A^{m_1+\dots+m_g} \cdot c_{m_1,\dots,m_g;i}$ are algebraic integers for all $m_1,\dots,m_g = 0,1,\dots;\ i = 1,\dots,g$. Here $A = A(\bar{x}_0;g)$ can be determined in terms of g and the discriminant of the polynomial $r(z;\bar{x}_0)$ in z.

Let, as above, $\vec{m} = (m_1,\dots,m_g)$ for non-negative integers $m_i \geq 0 (i = 1,\dots,g)$ and $(\bar{x} - \bar{x}_0)^{\vec{m}} = (x_1 - x_{1,0})^{m_1} \cdots (x_g - x_{g,0})^{m_g}$, $|\vec{m}| = m_1 + \dots + m_g$. In these notations we have the expansion $z_i = \Sigma_{\vec{m}}\, c_{\vec{m};i}(\bar{x}-\bar{x}_0)^{\vec{m}}$; $c_{\vec{0};i} = z_{i,0}$ at $\bar{x} = \bar{x}_0$. We substitute this expansion of z_i into the expansion of $F_i(z_i) = \Sigma_{n=1}^{\infty}\ f_{n,i}(z_i-z_{i,0})^n$ at $z = z_{i,0}$, and obtain $F_i(z_i) = \Sigma_{\vec{k}}(\bar{x}-\bar{x}_0)^{\vec{k}}\,\Sigma_{n=0}^{\infty}\Sigma_{\vec{m}_\alpha\neq\vec{0},\vec{m}_1+\dots+\vec{m}_n=\vec{k}}\ f_{n,i}c_{\vec{m}_1;i}\cdots c_{\vec{m}_n;i}$, where, in this expansion, $n \leq |\vec{m}_1| + \dots + |\vec{m}_n| = |\vec{k}|$: $i = 1,\dots,g$. This gives us the expansion of $f(x_1,\dots,x_g)$ at $\bar{x} = \bar{x}_0$: $f(\bar{x}) = \Sigma_{\vec{m}}a_{\vec{m}}(\bar{x}-\bar{x}_0)^{\vec{m}}$, where $a_{\vec{m}}$ are algebraic numbers (lying in the field, generated by the coefficients of $p(z,w)$, $R(z,w)$ and $z_{1,0},\dots,z_{g,0}$),such that $\limsup_{|\vec{m}|\to\infty} |a_{\vec{m}}|^{1/|\vec{m}|} < \infty$. The last condition is satisfied, because of the non-degeneracy conditions iii) and iv) above, all functions $z_i = z_i(\bar{x})$ and $F_i(z_i)$ have non-zero radius of convergence. If to expand $f(\bar{x})^j$ at $\bar{x} = \bar{x}_0$, we obtain $f(\bar{x})^j = \Sigma_{\vec{m}}\ a_{\vec{m},j}\ (\bar{x}-\bar{x}_0)^{\vec{m}}$ and, following our description of coefficients in the expansion of $F_i(z_i)$ at $\bar{x} = \bar{x}_0$ and the common denominators $\Delta(\bar{x}_0)_{M;k}$ of $\{f_{n_1,i_1}\cdots f_{n_j,i_j}: n_1+\dots+n_j \leq M;\ i_1,\dots,i_j = 1,\dots,g;\ j = 1,\dots,k\}$ we deduce the following bound on the denominators of $a_{\vec{m},j}$. The common denominator $\mathfrak{D}_{M,k}$ of $\{a_{\vec{m},j}: |\vec{m}| \leq M,\ j = 1,\dots,k\}$ divides $\Delta(\bar{x}_0)_{M;k}\cdot A^M$ and, consequently, according to the assumptions of the Grothendieck conjecture, $\sup_k\{\limsup_{M\to\infty}|\mathfrak{D}_{M;k}|^{1/M}\} < \infty$.

Thus, all conditions of the Main Theorem 5.2 are satisfied, according to the description of sizes and denominators of coefficients of expansions of $f(\bar{x})^j$ at $\bar{x} = x_0$; according to the uniformization of $x_1,\dots,x_g,f(x_1,\dots,x_g)$ by meromorphic functions of $u_1,\dots,u_g$, and according to the non-degeneracy conditions i)-iv) on $\bar{x}_0$ above. Thus, Main Theorem 5.2 implies that $f(x_1,\dots,x_g)$ is an algebraic functions and so are $F_i(z_i)$. Hence, all solutions of the equation (8.2) are algebraic functions, provided that the equation (8.2) is globally nilpotent.

Similarly to the above treatment of (8.2) we can prove the Grothendieck conjecture for an arbitrary equation of rank one over Γ. To do this we start with Katz's result [1] that it is sufficient to establish the Grothendieck conjecture for equations

$$(8.3) \qquad dF = \omega(z,w)dz$$

and an Abelian differential ωdz of Γ having only first order poles on Γ and (rational) integer residues at them. To see this we can use Corollaries 1.2 and 1.4, according to which the equation (8.3)having sufficiently many solutions (mod $\mathcal{P}$)for almost all prime ideals $\mathcal{P}$, must be Fuchsian with rational exponents at regular singularities. This implies that residues at poles of ωdz are rational numbers, and a simple transformation of (8.3), proposed in [1], make these residues rational integers. Then we have the representation of ωdz and of $F(z)$ in terms of Prime Forms $E_{\bar{e}}(x,y)$ on Γ, very similar to σ-function representation of solutions of (8.3) above in §6 for $g = 1$. We refer to [29], [30], [34] for the theory of Prime Forms and explicit representations of the Abelian differentials of the third kind on Γ in terms of logarithmic derivatives of Riemann's theta functions on Γ. Combining these uniformizations of solutions of (8.3) by means of meromorphic functions in $\mathbb{C}^g$, with the Main Theorem 5.2 we can arrive to

Theorem 8.1: An arbitrary rank one linear differential equation (8.3) over an algebraic curve Γ satisfies the Grothendieck conjecture. I.e. if (8.3) has sufficiently many solutions (mod $\mathcal{P}$) for almost all $\mathcal{P}$ (or (8.3) has nilpotent p-curvature for almost all p), then the solutions of (8.3) are algebraic functions.

Conclusion.

One of the problems arising in the application of our results is the problem of effectiveness. Since all bounds of §2 are effective and all constants in the proof of Main Theorem 5.2 can be easily exhibited, all results of §§6-8 are effective. For example, in all these results for any P_0 we can explicitly bound the first prime $P \geq P_0$ for which p-curvature is nonzero provided that not all solutions are algebraic. Such effective bounds can be particularly useful in applications to the construction of algorithms determining the reducibility of Abelian integrals.

One immediate application of our results is the establishment of the generalized Grothendieck conjecture proposed by Katz [3] in several interesting cases. For example, from Theorem 11.2 [3] we obtain the following result. For an arbitrary rank 2 equation on a curve and the Lie algebra $\mathcal{Y}$, generated by p-curvature operators ψ_p for almost all p, if $\mathcal{Y} \neq 0$, then the Lie albebra of the Galois group of the equation coincides with $\mathcal{Y}$.

Finally, the Grothendieck conjecture in general is still unproved, and the presented approach has its limitations to be used in the proof of the full conjecture. Nevertheless, our methods present a new analytic approach to the proof of full conjecture and also provide new insights in other problems of diophantine geometry, that are pursued in our further reports.

References

[1] N. Katz, Algebraic solutions of differential equations, Invent. Math., 18 (1972), 1-118.

[2] T. Honda, Algebraic differential equations, Symposia Mathematica v.24, Academic Press, N.Y., 1981, 169-204.

[3] N. Katz, A conjecture in the arithmetic theory of differential equations, Bull. Soc. Math. France 110 (1982), 203-239; corr. 347-348.

[4] B. Dwork, Arithmetic theory of differential equations, Symposia Mathematica v.24, Academic Press, N.Y., 1981, 225-243.

[5] D.V. Chudnovsky, G.V. Chudnovsky, Applications of Padé approximations to diophantine inequalities in values of G-functions, see preceding paper, this volume.

[6] G.V. Chudnovsky, Measures of irrationality, transcendence and algebraic independence.Recent progress, in Journées Arithmétiques 1980 (ed. by J.V. Armitage), Cambridge University Press, 1982, 11-82

[7] B. Dwork, P. Robba, Effective p-adic bounds for solutions of homogeneous linear differential equations, Trans. Amer. Math. Soc. 259 (1980), 559-577.

[8] N. Katz, Nilpotent connections and the monodromy theorem, Publ. Math. I.H.E.S. 39 (1970), 355-412.

[9] E.L. Ince, Ordinary differential equations, Chelsea (reprint), N.Y., 1956.

[10] B. Dwork, P. Robba, On natural radii of p-adic convergence, Trans. Amer. Math. Soc. 256 (1979), 199-213.

[11] E. Bombieri , On G-functions, in Recent Progress in Analytic Number Theory (ed. by H. Halberstam and C. Hooley), Academic Press, N.Y., v.2, 1981, 1-67.

[12] Ch. Hermite, Sur la fonction exponentielle, C.R. Acad. Sci. Paris 77 (1873), 18-24, 74-79, 226-233, 285-293 (Oeuvres v. III, 150-181).

[13] K. Mahler, Ein Beweis des Thue-Siegelschen Satzes über die Approximation algebraischen Zahlen für binomische Gleichungen, Math. Ann. 105 (1931), 267-276.

[14] H. Jager, A multidimensional generalization of the Padé table, Indagat. Math. 26 (1964), 192-249.

[15] G.V. Chudnovsky, On the method of Thue-Siegel, Ann. of Math. 117 (1983), 325-382.

[16] G.V. Chudnovsky, Number-theoretic applications of polynomials with rational coefficients defined by extremality conditions, in Arithmetic and Geometry, v. 1 (ed. by M. Artin and J. Tate), Birkhauser, Boston, 1983, 61-106.

[17] A. Baker, Transcendental Number Theory, Cambridge University

Press, 1979.

[18] S. Lang, Algebra, Addison-Wesley, 1965.

[19] E. Whittaker, G. Watson, Modern Analysis, Cambridge, 1927.

[20] Ju.I. Manin, Rational points on algebraic curves over function fields, Amer. Math. Soc. Translations (2) 50 (1966), 189-234.

[21] J. Tate, The arithmetic of elliptic curves, Invent. Math. 23 (1974), 179-206.

[22] M. Hazewinkel, Formal Groups and Applications, Academic Press, 1978.

[23] C.H. Clemens, A Scrapbook of Complex Curve Theory, Plenum Press, N.Y., 1980.

[24] S. Lang, H. Trotter, Frobenius Distribution in GL_2-Extensions , Lecture Notes in Math., v.504, Springer, 1976.

[25] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math., 18 (1972), 183-266.

[26] D.V. Chudnovsky, G.V. Chudnovsky, Remark on the nature of the spectrum of Lame equation. Problem from transcendence theory, Lett. Nuovo Cimento 29 (1980),545-550.

[27] D. Mumford, An algebraico-geometric construction of commuting operators and of solutions to the Toda lattice equations, Kortewg-de Vries equations and related non linear equations, Proc. Intern. Symp. Algebraic Geometry, Kyoto, 1977, 115-153.

[28] H.P. McKean, P. van Moerbeke, The spectrum of Hill's equation, Invent. Math. 30 (1975), 217-274.

[29] J. Fay, Theta Functions on Riemann Surfaces, Lecture Notes in Math., v.352, Springer, 1973.

[30] A. Krazer, Lehrbush der Thetafunctionen, Teubner, 1903.

[31] H.F. Baker, Abel's Theorem and the Allied Theory Including the Theory of the Theta Functions, Cambridge, 1897.

[32] N.G. Chebotarev, Theory of Algebraic Functions, OGIZ, Moscow, 1948 (Russian).

[33] C.L. Siegel, Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss. Phys. Math. Kl. 1, 1929.

[34] D. Mumford, Tata lectures on Theta II, Birkhäuser, Boston, 1984.

[35] J.L. Burchall, T.W. Chaundy, Commutative ordinary differential operators, I,II, Proc. London Math. Soc. 21 (1922), 420-440; Proc. Royal Soc. London 118 (1928), 557-583.

[36] E. Borel, Leçons sur les fonctions meromorphes, Paris, 1903.

[37] S. Lang, Introduction to transcendental numbers, Addison-Wesley, 1966.

[38] T. Schneider, Enfuhrung in die transcendenten zahlen, Springer, 1957.

[39] E. Bombieri,S. Lang, Analytic subgroups of group varieties, Invent. Math. 11 (1970), 1-14.

[40] E. Bombieri, Algebraic values of meromoiphic maps, Invent. Math. 10 (1970), 267-287; addendum,ibid. 11 (1970), 163-166.