LECTURES IN MATHEMATICS

Department of Mathematics
KYOTO UNIVERSITY

15

# Lectures on Algebraic Solutions of Hypergeometric Differential Equations

BY

Michihiko MATSUDA

Published by
KINOKUNIYA CO., Ltd.
Tokyo, Japan

LECTURES IN MATHEMATICS

Department of Mathematics
KYOTO UNIVERSITY

15

# Lectures on Algebraic Solutions of Hypergeometric Differential Equations

By

Michihiko MATSUDA

Published by
KINOKUNIYA CO., Ltd.

printed in Japan

to his teacher Hisaaki Yoshizawa

who taught the author kindly
with a perspicacious mind
when he was a student
in Kyoto University

## Preface

In the first four chapters we shall describe several proofs of the celebrated theorem due to Schwarz: The first will be devoted to Schwarz' proof, the second and the fourth to Landau and A. Errera's and the third to Klein's. In the last chapter transcendental liouvillian solutions will be treated.

In 1873 Schwarz [35] succeeded in determination of all algebraic solutions of hypergeometric differential equations by Steiner's classification of all finite subgroups of the rotation group. An important role was played by the Schwarzian derivative which appears in Kummer's equation [25], who considered rational transformations of hypergeometric differential equations. A proof without the Schwarzian derivative can be found in Goursat's book [9, Chap.VI].

An algebraic proof of this theorem was given by Klein [16], who reduced the algebraic function fields defined by algebraic solutions to those of genus zero through Kummer's equations. Explicit description of algebraic solutions was made by Schwarz, Brioschi [3], O. Fischer and Klein himself (cf. footnote of [16, II, §10] in Gesammelte Abhandlungen, Springer, 1922).

Landau [26], [27] attempted to gain Schwarz' table arithmetically by Eisenstein's theorem on power series expression of algebraic functions, where we can see a beautiful application of Dirichlet's theorem on prime numbers in arithmetical progressions, and it was accomplished by A. Errera [4].

The first two chapters are based on the lectures delivered

by the author at Kyoto University in Autumn of 1981. There Landau's second theorem was stated without knowing that it is due to him. K. Okamoto, who happened to be visiting Kyoto University, kindly informed the author of Landau's work. Those lectures will be completed by the third and fourth chapters.

In the last chapter the following works will be treated: M. Hukuhara - S. Ōhasi [11] and T. Kimura [15] proved that there are no new liouvillian solutions in hypergeometric differential equations other than those considered by Gauss (cf. Klein [18, §61]). The proof is based on M. Kuga's theorem that the Zariski closure of the monodromy group of a Fuchsian equation is its Picard-Vessiot group [24, p.173]. Recently M. Setoyanagi [36], a student of the author, gave an algebraic proof of this theorem by Liouville's lemma [30, p.448] on Riccati's equation in case there is no logarithmic singularity, without making use of Kuga's theorem. H. P. Rehm's comments have enabled us to improve §13.

Note on the second chapter will be offered to prove T. Honda's theorem on the sufficiency of Eisenstein's criterion [10, §1].

Note on the fifth chapter will be offered to prove Liouville's theorem [29], [30], [31] on elementary solutions in Bessel's equation.

Goursat's works [7], [8] on Kummer's equation will not be treated here.

For an application of N. Katz' general theory [14] to our problem confer with F. Baldassarri - B. Dwork [1].

The author would like to express his sincere gratitude to K. Nishioka and M. Setoyanagi for fruitful discussions with them.

November 1984

Michihiko Matsuda

## Preliminaries

The analytic treatment in this note is based on the following existence theorem. In the complex plane let us consider a homogeneous linear differential equation whose coefficients are polynomials of the independent variable x:

$$P_0(x)\frac{d^n y}{dx^n} + P_1(x)\frac{d^{n-1} y}{dx^{n-1}} + \ldots + P_n(x)y = 0.$$

If the absolute value of every root of $P_0(x)$ is greater than a positive constant r, then a formal solution

$$y(x) = \sum_{k=0}^{\infty} \frac{a_k}{k!} x^k,$$

which is determined by the initial values at x = 0:

$$\frac{d^k y}{dx^k}(0) = a_k, \quad 0 \leq k < n,$$

converges for $|x| < r$. It will be proved as follows. Setting

$$z_k = \frac{d^k y}{dx^k} - a_k, \quad 0 \leq k < n,$$

we have a system of linear differential equations:

$$\frac{dz_{k-1}}{dx} = z_k + a_k, \quad 1 \leq k < n,$$

$$\frac{dz_{n-1}}{dx} = -\sum_{k=0}^{n-1} \frac{P_{n-k}(x)}{P_0(x)}(z_k + a_k)$$

with the initial condition:

$$z_k(0) = 0, \quad 0 \leq k < n.$$

For the right hand sides of our equation we can take a majorant

power series:

$$\frac{M}{1 - \frac{X}{r}} \sum_{k=0}^{n-1} (Z_k + A) = M \sum_{k=0}^{n-1} \sum_{h=0}^{\infty} r^{-h} X^h (A + Z_k)$$

with positive constants A and M. A formal solution Z of

$$\frac{dZ}{dX} = \frac{nM(Z + A)}{1 - \frac{X}{r}}, \qquad Z(0) = 0$$

is given by

$$Z = A[(1 - \frac{X}{r})^{-nMr} - 1]$$

$$= A \sum_{k=1}^{\infty} \frac{c(c+1)....(c+k-1)}{k!} r^{-k} X^k, \qquad c = nMr,$$

whose radius of convergence is r. Hence, our formal solution y(x) converges for $|x| < r$.

Table of contents

# Chapter I. Schwarz' theorem.

## §1. Kummer's table and Gauss' transformations.

Consider a hypergeometric differential equation

$$(E) \qquad x(1-x)\frac{d^2y}{dx^2} + [\gamma - (1+\alpha+\beta)x]\frac{dy}{dx} - \alpha\beta y = 0$$

with complex numbers $\alpha$, $\beta$ and $\gamma$, which will be indicated by $E(\alpha, \beta, \gamma)$. It has the symmetry in $\alpha$ and $\beta$. A solution is given by a hypergeometric series

$$(1) \qquad F(\alpha, \beta, \gamma, x) = \sum_{n=0}^{\infty} \frac{\alpha(\alpha+1)\ldots(\alpha+n-1)\beta(\beta+1)\ldots(\beta+n-1)}{1.2\ldots n.\gamma(\gamma+1)\ldots(\gamma+n-1)} x^n$$

unless $\gamma$ is a rational integer not greater than 0, which converges in $|x| < 1$.

If we change the dependent variable y into z by $y = x^{1-\gamma}z$ then (E) is transformed to $E(\alpha+1-\gamma, \beta+1-\gamma, 2-\gamma)$ for z, whence

$$(2) \qquad x^{1-\gamma}F(\alpha+1-\gamma, \beta+1-\gamma, 2-\gamma, x)$$

is a solution of (E).

If we change the independent variable x into t by $x = 1-t$ then (E) is transformed to $E(\alpha, \beta, 1+\alpha+\beta-\gamma)$ for t. Hence,

$$z = F(\alpha+1-\gamma, \beta+1-\gamma, \alpha+\beta+1-\gamma, 1-x)$$

is a solution of $E(\alpha+1-\gamma, \beta+1-\gamma, 2-\gamma)$, and $y = x^{1-\gamma}z$ is a solution of (E). Here we replace $\gamma$ by $1+\alpha+\beta-\gamma$ and x by $1 - x$, and obtain a solution of (E):

$$(3) \qquad (1-x)^{\gamma-\alpha-\beta}F(\gamma-\alpha, \gamma-\beta, \gamma, x).$$

In (3) we replace $\alpha$, $\beta$ and $\gamma$ by

$$\alpha' = \alpha + 1 - \gamma, \quad \beta' = \beta + 1 - \gamma, \quad \gamma' = 2 - \gamma$$

and multiply it by $x^{1-\gamma}$ then

(4) $\quad x^{1-\gamma}(1 - x)^{\gamma-\alpha-\beta}F(1-\alpha, 1-\beta, 2-\gamma, x)$

is a solution of (E).

In (1) - (4) we replace $\gamma$ and x by

$$\gamma' = 1 + \alpha + \beta-\gamma, \quad x' = 1 - x$$

and obtain solutions of (E):

(5) $\quad F(\alpha, \beta, 1+\alpha+\beta -\gamma, 1 - x),$

(6) $\quad (1 - x)^{\gamma-\alpha-\beta}F(\gamma-\alpha, \gamma-\beta, 1+ \alpha-\beta-\gamma, 1 - x),$

(7) $\quad x^{1-\gamma}F(1+\alpha-\gamma, 1+\beta-\gamma, 1+\alpha+\beta-\gamma, 1 - x),$

(8) $\quad x^{1-\gamma}(1 - x)^{\gamma-\alpha-\beta}F(1-\alpha, 1-\beta, 1+\alpha-\beta-\gamma, 1 - x).$

If we change the independent variable x into t by $x = t^{-}$ then (E) is transformed to

$$t^2(1 - t)\frac{d^2y}{dt^2} - t[\alpha + \beta - 1 - (\gamma - 2)t]\frac{dy}{dt} + \alpha\beta y = 0.$$

Here, let us change the dependent variable y into z by $y = t^{\alpha}z$. Then this equation is transformed to $E(\alpha, \alpha-\gamma+1, \alpha-\beta+1)$ for t and z.

In (1) - (8) we replace $\beta$, $\gamma$ and x by

$$\beta' = \alpha - \gamma + 1, \quad \gamma' = \alpha - \beta + 1, \quad x' = x^{-1}$$

and multiply them by $x^{-\alpha}$ then

(9) $x^{-\alpha}F(\alpha,\ \alpha-\gamma+1,\ \alpha-\beta+1,\ x^{-1})$,

(10) $x^{-\beta}F(\beta,\ \beta-\gamma+1,\ \beta-\alpha+1,\ x^{-1})$,

(11) $x^{\alpha-\gamma}(1-x)^{\gamma-\alpha-\beta}F(1-\alpha,\ \gamma-\alpha,\ \beta-\alpha+1,\ x^{-1})$,

(12) $x^{\beta-\gamma}(1-x)^{\gamma-\alpha-\beta}F(1-\beta,\ \gamma-\beta,\ \alpha-\beta+1,\ x^{-1})$

(13) $x^{-\alpha}F(\alpha,\ \alpha+1-\gamma,\ \alpha+\beta+1-\gamma,\ 1-x^{-1})$,

(14) $x^{\beta-\gamma}(1-x)^{\gamma-\alpha-\beta}F(\gamma-\beta,\ 1-\beta,\ \gamma+1-\alpha-\beta,\ 1-x^{-1})$,

(15) $x^{-\beta}F(\beta,\ \beta+1-\gamma,\ \alpha+\beta+1-\gamma,\ 1-x^{-1})$,

(16) $x^{\alpha-\gamma}(1-x)^{\gamma-\alpha-\beta}F(\gamma-\alpha,\ 1-\alpha,\ \gamma+1-\alpha-\beta,\ 1-x^{-1})$

are solutions of (E).

In (9) - (16) we replace $\gamma$ and $x$ by

$$\gamma' = 1 + \alpha + \beta - \gamma, \quad x' = 1 - x$$

and obtain solutions of (E):

(17) $(1-x)^{-\alpha}F(\alpha,\ \gamma-\beta,\ \alpha-\beta+1,\ (1-x)^{-1})$,

(18) $(1-x)^{-\beta}F(\beta,\ \gamma-\alpha,\ \beta-\alpha+1,\ (1-x)^{-1})$,

(19) $x^{1-\gamma}(1-x)^{\gamma-\beta-1}F(\beta+1-\gamma,\ 1-\alpha,\ \beta-\alpha+1,\ (1-x)^{-1})$,

(20) $x^{1-\gamma}(1-x)^{\gamma-\alpha-1}F(\alpha+1-\gamma,\ 1-\beta,\ \alpha-\beta+1,\ (1-x)^{-1})$,

(21) $(1-x)^{-\alpha}F(\alpha,\ \gamma-\beta,\ \alpha-\beta+1,\ x(x-1)^{-1})$,

(22) $x^{1-\gamma}(1-x)^{\gamma-\alpha-1}F(\alpha+1-\gamma,\ 1-\beta,\ 2-\gamma,\ x(x-1)^{-1})$,

(23) $(1 - x)^{-\beta}F(\beta, \gamma-\alpha, \beta-\alpha+1, x(x-1)^{-1})$,

(24) $x^{1-\gamma}(1 - x)^{\gamma-\beta-1}F(\beta+1-\gamma, 1-\alpha, 2-\gamma, x(x-1)^{-1})$.

Thus we have completed Kummer's table of twenty four solutions of (E) [25].

Let us set

$$\lambda = 1 - \gamma, \quad \mu = \gamma - \alpha - \beta, \quad \nu = \alpha - \beta.$$

Then in the equation $E(\alpha', \beta', \gamma')$ for $t = 1 - x$ we have

$$\alpha' = \alpha, \quad \beta' = \beta, \quad \gamma' = \alpha + \beta + 1 - \gamma$$

and

$$\lambda' = 1 - \gamma' = \mu, \quad \mu' = \gamma' - \alpha' - \beta' = \lambda, \quad \nu' = \alpha' - \beta' = \nu.$$

In the equation $E(\alpha'', \beta'', \gamma'')$ for $t = x^{-1}$ and $z = x^{\alpha}y$ we have

$$\alpha'' = \alpha, \quad \beta'' = \alpha - \gamma + 1, \quad \gamma'' = \alpha - \beta + 1$$

and

$$\lambda'' = 1 - \gamma'' = -\nu, \quad \mu'' = \gamma'' - \alpha'' - \beta'' = \mu, \quad \nu'' = \alpha'' - \beta'' = \lambda.$$

In the equation $E(\alpha^*, \beta^*, \gamma^*)$ for $z = x^{\gamma-1}y$ we have

$$\alpha^* = \alpha + 1 - \gamma, \quad \beta^* = \beta + 1 - \gamma, \quad \gamma^* = 2 - \gamma$$

and

$$\lambda^* = 1 - \gamma^* = -\lambda, \quad \mu^* = \gamma^* - \alpha^* - \beta^* = \mu, \quad \nu^* = \alpha^* - \beta^* = \nu.$$

Thus, $\pm\lambda$, $\pm\mu$, $\pm\nu$ are permuted on Kummer's table.

Let us consider Gauss' transformations of hypergeometric differential equations (cf. Goursat[ 9, §34]). If we set

$$z = \alpha y + xy'$$

for a non-trivial solution y of $E(\alpha, \beta, \gamma)$, then z is a solution of $E(\alpha + 1, \beta, \gamma)$, which can be zero if and only if

$$\alpha(\alpha + 1 - \gamma) = 0.$$

For, we have the identity

$$E = (1 - x)z' - \{\beta + (1 + \alpha - \gamma)x^{-1}\}z + \alpha(1 + \alpha - \gamma)x^{-1}y,$$

where E is the left hand side of (E). For a non-trivial solution y of (E) we set

$$z_1 = (\gamma - \alpha - \beta x)y + x(1 - x)y',$$

$$z_2 = (\gamma - 1)y + xy',$$

$$z_3 = (\gamma - \alpha - \beta)y + (1 - x)y'.$$

Then $z_1$ is a solution of $E(\alpha - 1, \beta, \gamma)$, which can be zero if and only if

$$(1 - \alpha)(\gamma - \alpha) = 0;$$

$z_2$ is a solution of $E(\alpha, \beta, \gamma - 1)$, which can be zero if and only if

$$(\alpha + 1 - \gamma)(\beta + 1 - \gamma) = 0;$$

$z_3$ is a solution of $E(\alpha, \beta, \gamma + 1)$, which can be zero if and only if

$$(\gamma - \alpha)(\gamma - \beta) = 0.$$

For, we have the identities:

$$E = z_1' - (1 - \alpha)x^{-1}z_1 + (1 - \alpha)(\gamma - \alpha)x^{-1}y$$

$$= (1 - x)z_2' + (\gamma - \alpha - \beta - 1)z_2 - (\alpha+1-\gamma)(\beta+1-\gamma)y$$

$$= xz_3' + \gamma z_3 - (\gamma - \alpha)(\gamma - \beta)y.$$

If we set

$$y = x^{-\alpha}\eta, \quad y_1 = x^{\alpha-\gamma}(1 - x)^{\gamma-\alpha-\beta}\eta_1,$$

$$y_2 = x^{1-\gamma}\eta_2, \quad y_3 = (1 - x)^{\gamma-\alpha-\beta}\eta_3$$

and

$$z = x^{-\alpha-1}\zeta, \quad z_1 = x^{\alpha-\gamma-1}(1 - x)^{\gamma-\alpha-\beta+1}\zeta_1,$$

$$z_2 = x^{2-\gamma}\zeta_2, \quad z_3 = (1 - x)^{1+\gamma-\alpha-\beta}\zeta_3,$$

then we have

$$\zeta = -\frac{d}{dt}\eta, \quad \zeta_1 = -\frac{d}{dt}\eta_1, \quad t = x^{-1}$$

and

$$\zeta_2 = \frac{d}{dx}\eta_2, \quad \zeta_3 = \frac{d}{dx}\eta_3.$$

## §2. Reducibility and logarithmic singularity.

The equation (E) is said to be reducible if it has a solution y whose logarithmic derivative $y'/y$ is a rational function of x. The necessary and sufficient condition is that one of $\alpha$, $\beta$, $\gamma - \alpha$, $\gamma - \beta$ is a rational integer (Schwarz[35, Art. I]).

The sufficiency can be proved by finding a solution of this property from Kummer's table as follows. Let us assume that $\alpha$ is an integer. If $\gamma$ is not an integer then a polynomial solution is given by (1) in case $\alpha \leq 0$ and in the other case $F(1-\alpha, 1-\beta, 2-\gamma, x)$ is a polynomial of x, where the solution (4) has our property. Suppose that $\gamma$ is an integer. First we assume that $\gamma > 0$. Then a polynomial solution is given by (1) in case $\alpha \leq 0$, and $F(\beta, \gamma-\alpha, \gamma, x(x-1)^{-1})$ is a polynomial of $x(x-1)^{-1}$ in case $\alpha \geq \gamma$, where the solution (23) has our property. If $0 < \alpha < \gamma$ then $F(\alpha, \alpha-\gamma+1, \alpha-\beta+1, x^{-1})$ is a polynomial of $x^{-1}$ in case $\beta$ is not an integer and the solution (9) has our property. Suppose that $\beta$ is an integer. Then a polynomial solution is given by (1) in case $\beta \leq 0$. If $\beta > 0$ then $F(\alpha+1-\gamma, 1-\beta, \alpha-\beta+1, (1-x)^{-1})$ is a polynomial of $(1-x)^{-1}$ in case $\alpha \geq \beta$, where the solution (20) has our property and in the other case $F(\beta+1-\gamma, 1-\alpha, \beta-\alpha+1, (1-x)^{-1})$ is a polynomial of $(1-x)^{-1}$, where the solution (19) has our property. Secondly let us assume that $\gamma \leq 0$. Then $F(1-\alpha, 1-\beta, 2-\gamma, x)$ is a polynomial of x in case $\alpha \geq 1$ where the solution (4) has our property and in case $\gamma \leq \alpha \leq 0$ a polynomial solution is given by (1). If $\alpha < \gamma$

then $F(\alpha+1-\gamma,\ 1-\beta,\ 2-\gamma,\ x(x-1)^{-1})$ is a polynomial of $x(x-1)^{-1}$ and the solution (22) has our property. Thus (E) is reducible if $\alpha$ is an integer. Suppose now that $\gamma-\alpha$ is an integer. Then, $\beta$ is an integer if $\gamma-\alpha-\beta$ is an integer and $\alpha$ is an integer if $\gamma$ is an integer. Hence, we may assume that neither $\gamma-\alpha-\beta$ nor $\gamma$ is an integer. In case $\alpha \leqq \beta$, $F(\gamma-\alpha,\ \gamma-\beta,\ \gamma-\alpha-\beta+1,\ 1-x)$ is a polynomial of $1-x$ where the solution (6) has our property, and in the other case $F(\alpha+1-\gamma,\ \beta+1-\gamma,\ 2-\gamma,\ x)$ is a polynomial of x where the solution(2) has our property. Therefore, (E) is reducible if $\gamma-\alpha$ is an integer. The sufficiency has been proved.

In order to prove the necessity it is sufficient to show that one of $\pm\lambda \pm \mu \pm \nu$ is an odd integer, since we have

$$\alpha = \frac{1}{2}(1-\lambda-\mu+\nu), \qquad \beta = \frac{1}{2}(1-\lambda-\mu-\nu),$$

$$\gamma-\alpha = \frac{1}{2}(1-\lambda+\mu-\nu), \qquad \alpha-\beta = \frac{1}{2}(1-\lambda+\mu+\nu).$$

For a non-trivial solution y of (E) we set $z = y'/y$. Then it satisfies

$$z' + z^2 + \frac{\gamma-(1+\alpha+\beta)x}{x(1-x)}\,z - \frac{\alpha\beta}{x(1-x)} = 0,$$

that is

$$z' + z^2 + \left(\frac{1-\lambda}{x} + \frac{1-\mu}{x-1}\right)z - \alpha\beta\left(\frac{1}{x} - \frac{1}{x-1}\right) = 0.$$

If the logarithmic derivative of our solution y is a rational function of x we can express z as the sum of partial fractions:

$$z = P(x) + \sum_i \sum_j \frac{e_{ij}}{(x-c_i)^j}, \qquad 0 \leqq i \leqq n+1, \quad 1 \leqq j \leqq r_i,$$

where $P(x)$ is a polynomial of $x$ and $c_i$, $e_{ij}$ are complex numbers By the differentiation

$$z' = P'(x) - \sum_i \sum_j \frac{je_{ij}}{(x - c_i)^{j+1}} .$$

Comparing the order of the pole at $x = c_i$ we have $r_i = 1$ for every $i$, and $P(x) = 0$ at $x = \infty$ by comparing the order of the pole at that point. Hence,

$$z = \sum_i \frac{e_i}{x - c_i} , \qquad z' = - \sum_i \frac{e_i}{(x - c_i)^2} .$$

Let us set $c_0 = 0$ and $c_1 = 1$. Then comparing the coefficient of $(x - c_i)^2$ we have

$$- e_i + e_i^2 = o, \quad e_i = 1$$

for every $i$ different from 0 and 1. Comparing the coefficient of $x^{-2}$ and $(x - 1)^{-2}$ we have

$$- e_0 + e_0^2 + (1 - \lambda)e_0 = 0$$

and

$$- e_1 + e_1^2 + (1 - \mu)e_1 = 0.$$

Hence, $e_0$ is either 0 or $\lambda$ and $e_1$ is either 0 or $\mu$. Multiplying the equation for $z$ by $x^2$ we have

$$x^2z' + (xz)^2 + (1 - \lambda + x\frac{1 - \mu}{x - 1})xz + \alpha\beta \frac{x}{x - 1} = 0.$$

If we set $X = \sum_i e_i$ then for $x = \infty$ we obtain

$$- X + X^2 + (2 - \lambda - \mu)X + \alpha\beta = 0,$$

and

$$X = \frac{1}{2}(\lambda + \mu - 1 \pm \nu),$$

which takes one of the following four values:

$$n, \quad n + \lambda, \quad n + \mu, \quad n + \lambda + \mu.$$

Hence, one of $\pm\lambda$ $\pm\mu$ $\pm\nu$ is an odd integer (cf. M. Kuga[24, §19]).

Let us consider the logarithmic singularity of (E). If $\lambda$ is not a rational integer there is no logarithmic singularity at $x = 0$. We assume that $\lambda$ is an integer. If it is zero, that is $\gamma = 1$, then we have a solution of the form

$$\Phi(x) = F(\alpha, \beta, 1, x)\log x + \sum_{m=1}^{\infty} A_m B_m x^m,$$

where

$$A_m = \frac{\alpha(\alpha+1)\cdot \cdots \cdot(\alpha+m-1)\beta(\beta+1)\cdot \cdots \cdot(\beta+m-1)}{(m!)^2}$$

which is the coefficient of $x^m$ in $F(\alpha, \beta, 1, x)$ and

$$B_m = \frac{1}{\alpha} + \frac{1}{\alpha+1} + \cdots + \frac{1}{\alpha+m-1} + \frac{1}{\beta} + \frac{1}{\beta+1} + \cdots + \frac{1}{\beta+m-1}$$

$$- 2\left(1 + \frac{1}{2} + \cdots + \frac{1}{m}\right).$$

The power series $\sum A_m B_m x^m$ converges in $|x| < 1$. Here, we assumed that neither $\alpha$ nor $\beta$ is an integer less than 1. If either $\alpha$ or $\beta$ is an integer less than 1 we set

$$B_m = 0, \quad m > N,$$

where N is the minimum of m such that

$$(\alpha + m)(\beta + m) = 0.$$

In this case $\sum A_m B_m x^m$ is a polynomial of x, and in each case $x = 0$ is a logarithmic singular point of (E).

Suppose that $\gamma < 1$. Then (E) has a solution of the form

$$x^{1-\gamma} \frac{d^{1-\gamma}}{dx^{1-\gamma}} \Phi(x)$$

by Gauss' transformations, and we have

$$\frac{d^{1-\gamma}}{dx^{1-\gamma}} F(\alpha, \beta, 1, x) = 0$$

if and only if

$$\alpha(\alpha+1)\cdot \cdots \cdot(\alpha-\gamma)\beta(\beta+1)\cdot \cdots \cdot(\beta-\gamma) = 0.$$

In this case we have a polynomial solution of the form

$$\sum \frac{\alpha\cdot \cdots \cdot(\alpha+m-1)\beta\cdot \cdots \cdot(\beta+m-1)}{1\cdot \cdots \cdot m\cdot \gamma\cdot \cdots \cdot(\gamma+m-1)} x^m, \quad 0 \leq m \leq -\gamma,$$

which forms a fundamental system of solutions with (2).

Suppose that $\gamma > 1$. Then (E) has a solution of the form

$$(1-x)^{\gamma-\alpha-\beta} \frac{d^{\gamma-1}}{dx^{\gamma-1}}\{(1-x)^{\alpha+\beta-1}\Phi(x)\}$$

by Gauss' transformations, and we have

$$\frac{d^{\gamma-1}}{dx^{\gamma-1}}\{(1-x)^{\alpha+\beta-1}F(\alpha, \beta, 1, x)\} = 0$$

if and only if

$$(1-\alpha)(2-\alpha)\cdot \cdots \cdot(\gamma-\alpha-1)(1-\beta)(2-\beta)\cdot \cdots \cdot(\gamma-\beta-1) = 0,$$

since

$$(1-x)^{\alpha+\beta-1}F(\alpha, \beta, 1, x) = F(1-\alpha, 1-\beta, 1, x)$$

by (3). In this case we have a rational function solution of the form

$$x^{1-\gamma} \sum \frac{(\alpha+1-\gamma)\cdot \cdots \cdot(\alpha+m-\gamma)(\beta+1-\gamma)\cdot \cdots \cdot(\beta+m-\gamma)}{1\cdot \cdots \cdot m\cdot(2-\gamma)\cdot \cdots \cdot(m+1-\gamma)} x^m$$

with $0 \leq m \leq \gamma - 2$, which forms a fundamental system of solu-

tions with (1).

Therefore, under the condition that $\lambda$ is an integer, there is no logarithmic singularity at $x = 0$ if and only if $\alpha$ and $\beta$ are such integers that one of the couples $(\alpha, \alpha+1-\gamma)$ and $(\beta, \beta+1-\gamma)$ consists of numbers h and k satisfying $h \leqq 0 < k$ (cf. Goursat[9 , §18]).

It follows that an irreducible equation (E) has a logarithmic singularity if one of $\lambda$, $\mu$ and $\nu$ is a rational integer.

## §3. Schwarz' table.

We shall assume that our equation (E) is irreducible, that is, neither $\alpha$, $\beta$, $\gamma - \alpha$ nor $\gamma - \beta$ is a rational integer. It will be proved that every solution of (E) is algebraic if it has a non-trivial algebraic solution in §7. Hence, we may assume that there is no logarithmic singularity, that is, neither $\lambda$, $\mu$ nor $\nu$ is a rational integer. We write (E) as

$$(E) \qquad \frac{d^2y}{dx^2} + p(x)\frac{dy}{dx} + q(x)y = 0,$$

where

$$p(x) = \frac{\gamma}{x} + \frac{1 + \alpha + \beta - \gamma}{x - 1}, \qquad q(x) = \alpha\beta\left(\frac{1}{x} - \frac{1}{x - 1}\right).$$

Take a fundamental system of solutions $y_1$ and $y_2$ of (E). If we denote the ratio $y_1/y_2$ of them by $z$ then we have

$$z' = (y_1'y_2 - y_1y_2')y_2^{-2},$$

$$\frac{z''}{z'} = \frac{y_1''y_2 - y_1y_2''}{y_1'y_2 - y_1y_2'} - 2\frac{y_2'}{y_2} = -p(x) - 2\frac{y_2'}{y_2},$$

$$\frac{d}{dx}\left(\frac{z''}{z'}\right) = -p' - 2\frac{y_2''}{y_2} + 2\frac{y_2'^2}{y_2^2} = -p' + 2q + 2p\frac{y_2'}{y_2} + 2\frac{y_2'^2}{y_2^2}$$

$$= -p' + 2q - \frac{1}{2}p^2 + 2\left(\frac{y_2'}{y_2} + \frac{p}{2}\right)^2,$$

whence $z = y_1/y_2$ satisfies

$$(S) \qquad \frac{d}{dx}\left(\frac{z''}{z'}\right) - \frac{1}{2}\left(\frac{z''}{z'}\right)^2 = -p' + 2q - \frac{1}{2}p^2$$

$$= \frac{1}{2}\left[\frac{1 - \lambda^2}{x^2} + \frac{1 - \mu^2}{(1-x)^2} + \frac{\lambda^2 + \mu^2 - \nu^2 - 1}{x(1-x)}\right].$$

The left hand side is the Schwarzian derivative of z.

The wronskian $W = y_1'y_2 - y_1y_2'$ satisfies $W' = -pW$, and

$$W = Cx^{\lambda-1}(x - 1)^{\mu-1}$$

with a constant C distinct from 0. If we set $y = \sqrt{W/Z'}$ for a solution Z of (S) then

$$y' = \frac{1}{2}\left(\frac{W'}{W} - \frac{Z''}{Z'}\right)y = -\frac{1}{2}\left(p + \frac{Z''}{Z'}\right)y,$$

$$y'' = -\frac{1}{2}\left(p + \frac{Z''}{Z'}\right)y' - \frac{1}{2}\left[p' + \frac{d}{dx}\left(\frac{Z''}{Z'}\right)\right]y$$

and

$$y'' = -py' + \frac{1}{4}\left(-p + \frac{Z''}{Z'}\right)\left(p + \frac{Z''}{Z'}\right)y - \frac{1}{2}\left[p' + \frac{d}{dx}\left(\frac{Z''}{Z'}\right)\right]y$$

$$= -py' - qy - \frac{1}{2}\left[\frac{d}{dx}\left(\frac{Z''}{Z'}\right) - \frac{1}{2}\left(\frac{Z''}{Z'}\right)^2 + p' - 2q^2 + \frac{1}{2}p^2\right]y$$

$$= -py' - qy,$$

whence y is a solution of (E). If we set $y_3 = yZ$ then

$$y_3' = y'Z + yZ' = (y'y_3 + W)y^{-1},$$

$$y_3'' = (y''y_3 + y'y_3' + W')y^{-1} - y_3'y'y^{-1}$$

$$= -(py' + qy)y_3y^{-1} - pWy^{-1}$$

$$= -p(y'y_3 + W)y^{-1} - qy_3 = -py_3' - qy_3,$$

whence $y_3$ is a solution of (E). Therefore, Z is expressed in the form

$$Z = \frac{C_1 y_1 + C_2 y_2}{C_1' y_1 + C_2' y_2} = \frac{C_1 z + C_2}{C_1' z + C_2'}$$

with constants $C_1$, $C_2$, $C_1'$ and $C_2'$.

At every point different from 0, 1 and $\infty$ we can take a fundamental system of solutions $y_1$ and $y_2$ such that $y_1(x_0) = 0$ and $y_2(x_0) = 1$ at this point $x_0$. Hence, $y_1'(x_0) \neq 0$ by the uniqueness theorem of solutions, and we have

$$\frac{dz}{dx}(x_0) \neq 0.$$

We shall assume that our equation (E) has only algebraic singularities, that is, $\alpha$, $\beta$ and $\gamma$ are rational numbers. If z is algebraic then $y_1$ and $y_2$ are algebraic. For, we have

$$y_1 = zy_2, \quad y_2 = \sqrt{W/z'}$$

and W is algebraic by our assumption. This is due to Heine (cf. Schwarz [35, p.298]).

At the point 0, 1 and $\infty$ we can take $y_1$ and $y_2$ such that z takes the following form:

$$z_0 = x^{\lambda}\xi(x), \quad \xi(0) \neq 0,$$

$$z_1 = (x - 1)^{\mu}\eta(x-1), \quad \eta(0) \neq 0,$$

$$z_\infty = x^{-\nu}\zeta(x^{-1}), \quad \zeta(0) \neq 0,$$

where $\xi(x)$, $\eta(x-1)$ and $\zeta(x^{-1})$ are convergent power series with real coefficients. Hence, the line segments $(-\infty, 0)$, $(0, 1)$ and

$(1, +\infty)$ of real numbers are transformed to segments of lines passing through the origin by $z_0$, $z_1$ and $z_\infty$ respectively.

If (E) has an algebraic solution then by Gauss' transformations $E(\alpha+\ell, \beta+m, \gamma+n)$ has this property for all integers $\ell$, m and n. Hence, we may assume that

$$0 < \lambda < 1, \quad 0 < \mu < 1, \quad 0 < \pm\nu < 1.$$

The upper plane of complex numbers is transformed to the interior of a circular triangle with vertical angles $\lambda\pi$, $\mu\pi$ and $\nu\pi$ by z. By a suitable choice of z we may suppose that the two circles are two lines crossing at the origin. Then the origin is contained either in the interior or in the exterior of the third circle. The former case occurs if and only if the following condition is satisfied:

(L) $$\lambda + \mu + \nu > 1, \quad \mu + \nu > 1 + \lambda,$$

$$\nu + \lambda > 1 + \mu, \quad \lambda + \mu > 1 + \nu.$$

If a function $f(x)$ is holomorphic at $\bar{x}_0$ then the function $\overline{f(\bar{x})}$ is holomorphic at $x_0$ by definition, where the bar indicates the conjugate. The functions $z_0$, $z_1$ and $z_\infty$ have the property that $z(\bar{x}) = \overline{z(x)}$ by a proper choice of its branch in a domain which is symmetric in the line of real numbers. Hence, the analytic continuation of z across the line segments $(-\infty, 0)$, $(0, 1)$ and $(1, +\infty)$ of real numbers induces the reflections in the circles corresponding to them. Thus the lower plane of complex numbers is transformed to the interior of an adjacent cir-

cular triangle.

A many-valued analytic function which has only algebraic singularities is algebraic if and only if it is finitely many-valued (cf. for instance Bieberbach [2, p.230]).

By geometric consideration Schwarz proved that the condition (L) is satisfied if (E) has an algebraic solution (cf. Goursat [9, Chap. VI]). It will be proved here by Landau's first theorem in §5.

Suppose that the condition (L) is satisfied. Then we have a great-circular triangle on the unit sphere with vertical angles $\lambda\pi$, $\mu\pi$ and $\nu\pi$ by a stereographic projection. The composition of the reflections in two sides is the rotation around the common vertex of them with the negative rotation angle equal to the twice of this vertical angle. Thus we have three rotations around the vertices, and they generate a finite group if and only if (E) has an algebraic solution.

Such finite groups are the dihedral group, the tetrahedral group, the octahedral group and the icosahedral group: The second is contained in the third and the fourth as a subgroup (cf. for instance Weber [40, Chap.VIII]).

The three great circles form four triangles whose vertical angles have the following values multiplied by $\pi$:

$$\{\lambda, \mu, \nu\}, \quad \{\lambda, 1 - \mu, 1 - \nu\},$$

$$\{1 - \lambda, \mu, 1 - \nu\}, \quad \{1 - \lambda, 1 - \mu, \nu\}.$$

A solution corresponding to $\{\lambda, 1 - \mu, 1 - \nu\}$ is given by $(1 - x)^{1+\alpha+\beta-\gamma}F(\alpha, \beta + 1, \gamma, x)$.

We assume that the triangle corresponding to $\{\lambda, \mu, \nu\}$ has the least area among them and $\lambda \geq \mu \geq \nu$. Then (E) has an algebraic solution if and only if $\{\lambda, \mu, \nu\}$ is in the following table due to Schwarz [35]:

Dihedral group:

(I) $\{\frac{1}{2}, \frac{1}{2}, \nu\}$, $\nu$ is arbitrary, Area/$\pi$ = $\nu$.

Tetrahedral group:

(II) $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{3}\}$, Area/$\pi$ = $\frac{1}{6}$ = A,

(III) $\{\frac{2}{3}, \frac{1}{3}, \frac{1}{3}\}$, $\frac{1}{3}$ = 2A.

Octahedral group:

(IV) $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}\}$, Area/$\pi$ = $\frac{1}{12}$ = B,

(V) $\{\frac{1}{3}, \frac{1}{4}, \frac{1}{4}\}$, $\frac{1}{6}$ = 2B.

Icosahedral group:

(VI) $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{5}\}$, Area/$\pi$ = $\frac{1}{30}$ = C,

(VII) $\{\frac{2}{5}, \frac{1}{3}, \frac{1}{5}\}$, $\frac{1}{15}$ = 2C,

(VIII) $\{\frac{1}{3}, \frac{1}{5}, \frac{1}{5}\}$, $\frac{1}{15}$ = 2C,

(IX) $\{\frac{1}{2}, \frac{2}{5}, \frac{1}{5}\}$, $\frac{1}{10}$ = 3C,

(X) $\{\frac{3}{5}, \frac{1}{3}, \frac{1}{5}\}$, $\frac{2}{15}$ = 4C,

(XI) $\{\frac{1}{5}, \frac{1}{5}, \frac{1}{5}\}$, $\frac{1}{5}$ = 6C,

(XII) $\{\frac{2}{3}, \frac{1}{3}, \frac{1}{5}\}$, Area/$\pi$ = $\frac{1}{5}$ = 6C,

(XIII) $\{\frac{4}{5}, \frac{1}{5}, \frac{1}{5}\}$, $\frac{1}{5}$ = 6C,

(XIV) $\{\frac{1}{2}, \frac{2}{5}, \frac{1}{3}\}$, $\frac{7}{30}$ = 7C,

(XV) $\{\frac{3}{5}, \frac{2}{5}, \frac{1}{3}\}$, $\frac{1}{3}$ = 10C.

The order N of these groups are respectively 2n, 12, 24 and 60, where n is the denominator of $\nu$. The irreducible algebraic equation F(x, z) = 0 has its degree with respect to x and z equal to $M^{-1}N/2$ and N respectively, where $M\pi$ is the area of the corresponding triangle. In particular x is a rational function of z in the case of (I) with $\nu$ = 1/n, (II), (IV) and (VI).

## Chapter II. Landau's criterion.

### §4. Eisenstein's theorem.

If a convergent power series $y = \sum_{n=0}^{\infty} c_n x^n$ whose coefficients are rational numbers expresses an algebraic function of x over the field $\mathbb{C}$ of complex numbers then there exists an integer A distinct from 0 such that $A^n c_n$ is an integer for every n.

This is known as a theorem of Eisenstein (cf. Landau[26]), which will be proved as follows.

We shall see that y is an algebraic function of x over the field $\mathbb{Q}$ of rational numbers. Let F(X, Y) be a polynomial over $\mathbb{C}$ such that F(x, y) = 0, which we write as

$$F(X, Y) = \sum_{k \geq 0} A_k(X) Y^k, \quad A_k(X) = \sum_{j \geq 0} a_{kj} X^j, \quad a_{kj} \in \mathbb{C}.$$

We may assume that $c_0 = 0$, and under this assumption

$$y^k = x^k \sum_{n=1}^{\infty} c_{nk} x^n, \quad c_{nk} \in \mathbb{Q}, \quad k \geq 1.$$

For every m we have

$$\sum a_{kj} c_{nk} = 0 \quad (j + k + n = m).$$

We can take a system of finite complex numbers $e_h$ $(h \geq 1)$ such that they are linearly independent over $\mathbb{Q}$ and

$$a_{kj} = \sum_h b_{kjh} e_h, \quad b_{kjh} \in \mathbb{Q}$$

for all k and j. Then for every m we have

$$\sum_h e_h \sum b_{kjh} c_{nk} = 0 \quad (j + k + n = m)$$

and

$$\sum b_{kjh}c_{nk} = 0 \quad (j + k + n = m)$$

for every h. Hence, y satisfies

$$\sum_k \Big(\sum_j b_{kjh}x^j\Big)y^k = 0$$

for all h, and one of them gives us a non-trivial relation.

Thus we may assume that all $a_{kj}$ are rational numbers and that they are integers multiplying F(X, Y) by a common multiple of their denominators. They satisfy

$$a_{00} = 0, \quad a_{01} + a_{10}c_1 = 0,$$

$$a_{02} + a_{10}c_2 + a_{11}c_1 + a_{20}c_1^2 = 0$$

and

$$a_{0j} + a_{10}c_j + a_{11}c_{j-1} + \cdots + a_{1,j-1}c_1 + \sum_{i\geq 2} \sum_{h=0}^{j-1} a_{ih}c_{k_1}c_{k_2}\cdots c_{k_i} = 0 \quad (k_1 + \cdots + k_i = j - h)$$

for $j > 2$.

First we assume that $a_{10}$ does not vanish. If we set $a = a_{10}$ then

$$ac_1 = -a_{01}, \quad a^3c_2 = -a^2(a_{02} + a_{11}c_1 + a_{20}c_1^2)$$

are integers. If we assume that

$$a^{2k-3}c_{k-1}, \quad 2 \leq k \leq j$$

are integers, then

$$a^{2j-1}c_j = -a^{2j-2}\Big(a_{0j} + \sum_{h=1}^{j-1} a_{1h}c_{j-h} + \sum_{i\geq 2} \sum_{h=0}^{j-1} a_{ih} \times \Big) \times \sum c_{k_1}c_{k_2}\cdots c_{k_i}\Big), \quad k_1 + \cdots + k_i = j - h$$

is an integer, because

$$a^{2j-2}c_{k_1}\cdots c_{k_i}$$

$$= a^{2j-2-2k_1-\cdots-2k_i+i}\cdot a^{2k_1-1}c_{k_1}\cdots a^{2k_i-1}c_{k_i}$$

and

$$2j - 2 - 2k_1 - \cdots - 2k_i + i = 2j - 2 - 2(j - h) + i$$

$$= 2(h - 1) + i \geqq 0$$

for $i \geqq 2$. Therefore, we can take $a_{10}^2$ as A in our theorem.

Secondly we assume that $a_{10}$ vanishes. For a power series $B = \sum_{n=0}^{\infty} b_n X^n$ we define its order $O(B)$ as the minimum of such n that $b_n$ does not vanish, and for a polynomial $H = \sum B_n Z^n$ of Z whose coefficients are power series of X we define its order $O(H)$ as the minimum of $O(B_n)$. We write y and $A_i$ which does not vanish as

$$y = cx^{\gamma} + c'x^{\gamma'} + \cdots, \quad c^{(i)} \neq 0, \quad 0 < \gamma < \gamma' < \cdots,$$

$$A_i(X) = a_i X^{\alpha_i} + a_i' X^{\alpha_i'} + \cdots, \quad a_i^{(j)} \neq 0, \quad 0 \leqq \alpha_i < \alpha_i' < \cdots$$

and define z by

$$y = cx^{\gamma} + x^{\gamma}z, \quad z = c'x^{\gamma'-\gamma} + c''x^{\gamma''-\gamma} + \cdots.$$

If we replace Y in $F(X, Y)$ by $Y = X^{\gamma}(C + Z)$ then it is expressed in the form

$$F(X, Y) = F(X, X^{\gamma}(C + Z)) = F(X, CX^{\gamma}) + F_Y(X, CX^{\gamma})\cdot X^{\gamma}Z$$

$$+ \frac{1}{2!} F_{YY}(X, CX^{\gamma})\cdot X^{2\gamma}Z^2 + \cdots .$$

If we set

$$E(X, C) = F(X, CX^{\gamma})$$

then we have

$$E_C(X, C) = X^{\gamma}F_Y(X, CX^{\gamma}),\ E_{CC}(X, C) = X^{2\gamma}F_{YY}(X, CX^{\gamma}),\ \cdots$$

and

$$F(X, Y) = E(X, C) + E_C(X, C)Z + \frac{1}{2!}E_{CC}(X, C)Z^2 + \cdots .$$

It satisfies

$$0 = F(x, y) = E(x, c) + E_C(x, c)z + \frac{1}{2!}E_{CC}(x, c)z^2 + \cdots ,$$

where we have

$$O(E(X, c)) \leqq O(E_C(X, c)) \leqq O(E_{CC}(X, c)) \leqq \cdots .$$

If we write $E(X, C)$ as

$$E(X, C) = \Phi(C)X + \Phi_1(C)X^{\beta'} + \cdots,\quad 0 < \beta < \beta' < \cdots ,$$

then we have

$$\Phi(C) = \sum a_i C^i \qquad (\beta = \alpha_i + i\gamma)$$

and $\Phi(c) = 0$. Let us set

$$L = O(F(X, X(c + Z))$$

and

$$G(X, Z) = X^{-L}F(X, X^{\gamma}(c + Z)).$$

We have

$$G(X, Z) = X^{-L}\{E(X, c) + E_C(X, c)Z + \frac{1}{2!}E_{CC}(X, c)Z^2 + \cdots\}$$

and

$$E_C(X, c) = \Phi'(c)X^{\beta} + \Phi_1'(c)X^{\beta'} + \cdots,$$

$$E_{CC}(X, c) = \Phi''(c)X^{\beta} + \Phi_1''(c)X^{\beta'} + \cdots,$$

$$\cdots .$$

Suppose that c is a root of $\Phi(C)$ of multiplicity s. Then we have $\Phi^{(s)}(c) \neq 0$ and

$$O(\frac{\partial^s}{\partial C^s}E(X, c)) = 0,$$

whence $L = \beta$. If c is a simple root of $\Phi(C)$, then $\Phi'(c) \neq 0$ and we are in the first case for z. If c is a multiple root of $\Phi(C)$, then $\Phi(C)$ can not consist of less than three terms and there is an index j distinct from 0 and 1 such that $\alpha_j + j\gamma = \beta$. We have $\beta \geq j\gamma > \gamma$ and $L = \beta > \gamma$. By the definition

$$F_Y(X, X^\gamma(c + Z)) = X^{L-\gamma}G_Z(X, Z).$$

We may assume that $F(X, Y)$ is irreducible over $\mathbb{Q}$. Then we have

$$F_Y(X, \sum c_n X^n) \neq 0$$

and its order M is finite. Therefore, if we define $z_m$ by

$$y = cx^\gamma + c'x^{\gamma'} + \cdots + c^{(m-1)}x^{\gamma^{(m-1)}} + x^{\gamma^m}z_m ,$$

then there is an index m not greater than M such that we are in the first case for $z_m$.

## §5. Landau's first and second theorems.

We shall assume that $\alpha$, $\beta$, $\gamma$ are rational numbers and that neither $\lambda$, $\mu$, $\nu$, $\alpha$, $\beta$, $\gamma - \alpha$ nor $\gamma - \beta$ is an integer. Suppose that the equation (E) has an algebraic solution. Then every solution is algebraic, since (E) is irreducible (§7). The power series $F(\alpha, \beta, \gamma, x)$ which is algebraic by our assumption has its coefficient $c_n$ of the form:

$$c_n = \frac{\alpha(\alpha+1)\ldots(\alpha+n-1)\beta(\beta+1)\ldots(\beta+n-1)}{1.2\ldots n.\gamma(\gamma+1)\ldots(\gamma+n-1)}.$$

We write $\alpha$, $\beta$ and $\gamma$ as

$$\alpha = u + \frac{a}{m}, \quad \beta = v + \frac{b}{m}, \quad \gamma = w + \frac{c}{m}, \quad a, b, c < m,$$

where a, b, c, m are natural numbers and u, v, w are integers. Then $c_n$ takes the form:

$$c_n = \frac{a(a+mu)\ldots\{a+(u+n-1)m\}(b+vm)\ldots\{b+(v+n-1)m\}}{1.2\ldots n.(c+wm)\ldots\{c+(w+n-1)m\}} m^{-n}.$$

By Eisenstein's theorem there is an integer A distinct from 0 such that $A^n c_n$ is an integer. Suppose that a prime number p does not divide A. Then if a non-negative integer x satisfies the congruence

$$c + (w + x)m \equiv 0 \pmod{p},$$

there is a non-negative integer y not greater than x which satisfies the congruence

$$\{a + (u + y)m\}\{b + (v + ym)\} \equiv 0 \pmod{p}.$$

We have infinitely many prime numbers p which take the form $p = 1 + km$ with a positive integer k. This is a special case of Dirichlet's theorem and can be proved elementarily (cf. for instance Takagi [37, §10], Landau [28, §108]). If we set $x = ck - w$ then

$$c + (w + x)m = c + ckm = cp \equiv 0 \pmod{p}.$$

Here, we may assume that k is greater than $|u| + |v| + |w|$ and $|A|$. We may suppose that

$$a + (u + y)m \equiv 0 \pmod{p}.$$

Then we have

$$0 \equiv a + (u+y)m \equiv a(p-km) + (u+y)m \equiv m(u+y-ak) \pmod{p}$$

and $u + y - ak = ph$ with an integer h. Since $0 \leq y \leq x$, we get

$$ak - u \geq -ph, \qquad ck + u - w \geq ph,$$

whence $h = 0$ because $p > km$ and $k > |u| + |w|$. Therefore, we have $y = ak + u$ and $a < c$ by $k > |u| + |w|$. Thus we obtain either $a < c$ or $b < c$.

From Kummer's table let us take a solution of (E) of the form:

$$x^{1-\gamma}F(\alpha + 1 - \gamma, \beta + 1 - \gamma, 2 - \gamma, x).$$

Then $F(\alpha+1-\gamma, \beta+1-\gamma, 2-\gamma, x)$ is an algebraic function of x. Here, we have

$$2 - \gamma = \frac{m - c}{m} + 1 + w$$

and

$$\alpha + 1 - \gamma = \frac{a - c}{m} + 1 + u - w, \quad 0 < \frac{a - c}{m} < 1$$

in case $a > c$,

$$\alpha + 1 - \gamma = \frac{a - c + m}{m} + u - w, \quad 0 < \frac{a - c + m}{m} < 1$$

in the other case. Similarly

$$\beta + 1 - \gamma = \frac{b - c}{m} + 1 + v - w, \quad 0 < \frac{b - c}{m} < 1$$

in case $b > c$,

$$\beta + 1 - \gamma = \frac{b - c + m}{m} + v - w, \quad 0 < \frac{b - c + m}{m} < 1$$

in the other case. Since both of

$$\frac{a - c + m}{m}, \qquad \frac{b - c + m}{m}$$

are greater than $(m - c)/m$, we have either $a > c$ or $b > c$.

Suppose that $0 < \lambda < 1$, $0 < \mu < 1$ and $0 < \nu < 1$. Then we have $-1 < \alpha < 1$, $-1 < \beta < 1$ and $0 < \gamma < 1$. Since $\alpha + \beta < \gamma$ and $(\alpha + 1) + (\beta + 1) > \gamma + 1$, we obtain $\alpha > 0 > \beta$ by $\alpha - \beta > 0$. Therefore, we get

$$\lambda + \mu + \nu = 1 - 2\beta > 1$$

and

$$1 + \nu = 1 + \alpha - \beta > 1 - \alpha - \beta = \lambda + \mu.$$

We have

$$\alpha = \frac{a}{m}, \qquad \beta = \frac{b}{m} - 1$$

and

$$1 > \alpha - \beta = \frac{a - b}{m} + 1.$$

Therefore, $a < b$ and $a < c < b$, that is $\alpha < \gamma < 1 + \beta$. Hence,

$$1 + \lambda = 2 - \gamma > \gamma - 2\beta = \mu + \nu$$

and

$$1 + \mu = 1 + \gamma - \alpha - \beta > 1 - \gamma + \alpha - \beta = \lambda + \nu.$$

Thus the condition (L) in §3 is satisfied if (E) has an algebraic solution. This is Landau's first theorem [26].

If we make use of another special case of Dirichlet's theorem that there are infinitely many prime numbers p of the form $p = -1 + km$ with a natural number k (Landau [28, §108]), then we can prove our result that either $a > c$ or $b > c$ independently of the discussions of §1. This remark is due to Landau [27].

There are infinitely many prime numbers p of the form $p = e + km$ with a natural number k for a given integer e which is relatively prime to m.

This is Dirichlet's theorem (cf. for instance Weber [40, §198]). Take a natural number e which is relatively prime to m. Then we can write a, b and c as

$$a = a_0 e + hm, \quad b = b_0 e + im, \quad c = c_0 e + jm$$

with natural numbers $a_0$, $b_0$, $c_0$ less than m and integers h, i, j. By Dirichlet's theorem there is a prime number p of the form $p = e + km$ such that k is greater than $|A|$ and

$$|h| + |i| + |j| + |u| + |v| + |w|.$$

If we set $x = c_0k - j - w$, then we have

$$c + (x + w)m = c_0e + (j + x + w)m = c_0(e + km) = c_0p.$$

We may suppose that

$$a + (u + y)m \equiv 0 \pmod{p}.$$

Then we have

$$0 \equiv a + (u + y)m = a_0e + (h + u + y)m$$

$$\equiv (h + u + y - a_0k)m \pmod{p}$$

and

$$h + u + y - a_0k = Hp$$

with an integer H. Since $0 \leq y \leq x$, we get

$$a_0k - h - u \geq - Hp$$

and

$$c_0k + h + u - j - w > Hp,$$

whence $H = 0$ because $p > mk$ and $k > |h| + |j| + |u| + |w|$. Therefore, we have

$$y = a_0k - h - u$$

and $a_0 < c_0$ by $k > |h| + |j| + |u| + |w|$. Thus, we obtain either $a_0 < c_0$ or $b_0 < c_0$.

If we replace e by $m - e$ with $e < m$, then

$$a = (m - a_0)(m - e) + (a_0 + e - m + h)m,$$

$$b = (m - b_0)(m - e) + (b_0 + e - m + i)m,$$

$$c = (m - c_0)(m - e) + (c_0 + e - m + j)m.$$

Hence, we have either $m - a_0 < m - c_0$ or $m - b_0 < m - c_0$, that is, either $a_0 > c_0$ or $b_0 > c_0$. Following Landau we write

$$A < B \pmod m$$

for two integers A and B which are not multiples of m if they satisfy

$$A \equiv A_0, \quad B \equiv B_0 \pmod m, \quad 0 < A_0 < B_0 < m.$$

We have obtained the second theorem of Landau [27]:

For every integer $\rho$ which is relatively prime to m we have either

$$\rho a < \rho c < \rho b \pmod m$$

or

$$\rho b < \rho c < \rho a \pmod m$$

if (E) has an algebraic solution.

Suppose that $A < C < B \pmod m$. Then we have

$$A < A + B - C < B \pmod m, \quad A < C < C - B \pmod m,$$

$$C - A < C < B \pmod m, \quad B - C < -C < A - C \pmod m$$

and

$$C - A < C < C - B \pmod m$$

if C - A and C - B are not multiples of m. Hence, every triple $\alpha'$, $\beta'$ and $\gamma'$ in Kummer's table satisfies the criterion in Landau's second theorem independently of the discussions in §1. This remark is due to Landau [27], and we have the following table:

1. $\{\lambda, \mu, \nu\}$: $\{a, b, c\}$,

2. $\{\lambda, -\mu, -\nu\}$: $\{c - a, m + c - b, c\}$,

3. $\{\lambda, -\nu, -\mu\}$: $\{a, m + c - b, c\}$,

4. $\{\lambda, \nu, \mu\}$: $\{c - a, b, c\}$,

5. $\{-\lambda, \mu, -\nu\}$: $\{b - c, m + a - c, m - c\}$,

6. $\{-\lambda, -\mu, \nu\}$: $\{m - b, m - a, m - c\}$,

7. $\{-\lambda, -\nu, \mu\}$: $\{m - b, m + a - c, m - c\}$,

8. $\{-\lambda, \nu, -\mu\}$: $\{b - c, m - a, m - c\}$,

9. $\{\mu, \lambda, \nu\}$: $\{a, b, a + b - c\}$,

10. $\{\mu, -\lambda, -\nu\}$: $\{b - c, m + a - c, a + b - c\}$,

11. $\{\mu, -\nu, -\lambda\}$: $\{a, m + a - c, a + b - c\}$,

12. $\{\mu, \nu, \lambda\}$: $\{b - c, b, a + b - c\}$,

13. $\{-\mu, \lambda, -\nu\}$: $\{c - a, m + c - b, m - a - b + c\}$,

14. $\{-\mu, -\lambda, \nu\}$: $\{m - b, m - a, m - a - b + c\}$,

15. $\{-\mu, \nu, -\lambda\}$: $\{c - a, m + c - b, m - a - b + c\}$,

16. $\{-\mu, -\nu, \lambda\}$: $\{m - b, m + c - b, m - a - b + c\}$,

17. $\{-\nu, \mu, -\lambda\}$: $\{a, m + a - c, m + a - b\}$,

18. $\{-\nu, -\mu, \lambda\}$: $\{m - b, m + c - b, m + a - b\}$,

19. $\{-\nu, \lambda, -\mu\}$: $\{a, m + c - b, m + a - b\}$,

20. $\{-\nu, -\lambda, \mu\}$: $\{m - b, m + a - c, m + a - b\}$,

21. $\{\nu, \mu, \lambda\}$: $\{b - c, b, b - a\}$,

22. $\{\nu, -\mu, -\lambda\}$: $\{c - a, m - a, b - a\}$,

23. $\{\nu, \lambda, \mu\}$: $\{c - a, b, b - a\}$,

24. $\{\nu, -\lambda, -\mu\}$: $\{b - c, m - a, b - a\}$.

## §6. Rough estimation.

For a given natural number m we consider a triple of natural numbers a, b and c less than m with (a, b, c, m) = 1 satisfying Landau's criterion that for every integer $\rho$ relatively prime to m we have either $\rho a < \rho c < \rho b \pmod m$ or $\rho b < \rho c < \rho a \pmod m$. Let $c_0$ be the greatest common divisor of c and m. Then there is an integer $\rho$ relatively prime to m such that $\rho c \equiv c_0 \pmod m$. We may assume that

$$0 < a_0 < c_0 < b_0 < m, \quad a_0\rho \equiv a, \quad b_0\rho \equiv b \pmod m.$$

Suppose that $\rho_0$ is relatively prime to $c_0$ and satisfies

$$\rho_0 \equiv 1 \pmod{n_0}, \quad m = c_0 n_0.$$

We are in one of the following two cases (A) and (B):

(A) For every $\rho_0$ we have $a_0\rho_0 < c_0 \pmod m$;

(B) There is such $\rho_0$ that $c_0 < a_0\rho_0 \pmod m$.

Suppose that $\lambda = \mu = 1/2$ and $\nu = s/r$, where r and s are mutually prime natural numbers with $s < r$. Then from the table at the end of §5 we have the following six triples with $m = 2r$:

$\{s, 2r - s, r\}$, $\{r - s, r + s, r\}$, $\{s, r + s, r\}$,

$\{r - s, 2r - s, r\}$, $\{s, r + s, 2s\}$,

$\{r - s, 2r - s, 2r - 2s\}$.

If we set $r' = r$ and $s' = r - s$ then the second, the fourth and the sixth are derived from the first, the third and the fifth respectively. In the first and the third cases we have $c_0 = r$, and we are in the case (B). In the fifth case $c_0 = 2$ and we

are in the case (A) if r is odd, in the case (B) if r is even.

We shall prove that we are in one of the three cases above stated if m is sufficiently great in the following discussions, which are unnecessary in order to establish Landau-Errera's theorem. We define $n_1$ and $n_2$ by

$$m = (a, m)n_1 = (b, m)n_2.$$

Let $n_{ij}$ be the least common multiple of $n_i$ and $n_j$ with $i, j = 0, 1, 2$. The number of natural numbers t less than m satisfying

$$t \equiv 1 \pmod{n_{ij}}, \quad (t, m) = 1$$

is $\phi(m)/\phi(n_{ij})$, where $\phi$ is the Euler function. The number of natural numbers $\varepsilon$ less than m such that

$$\varepsilon \equiv a\rho_0 \pmod{m}, \quad \rho_0 \equiv 1 \pmod{n_0}, \quad (\rho_0, c_0) = 1$$

is $\phi(n_{01})/\phi(n_0)$.

Let us suppose that we are in the case (A). If $\rho_0$ and $\rho_0'$ satisfy the above conditions then we have

$$a\rho_0 \equiv a\rho_0' \pmod{e},$$

where e is the greatest common divisor of m and $(m, a)n_0$. Hence, we have

$$e\{\phi(n_{01})/\phi(n_0) - 1\} < c_0.$$

Suppose that $\phi(n_{01})/\phi(n_0)$ is greater than one. Then we have

$$2\{\phi(n_{01})/\phi(n_0) - 1\} \geqq \phi(n_{01})/\phi(n_0)$$

and

$$e\phi(n_{01})/\phi(n_0) < 2c_0.$$

Here, if we write $n_0$ and $n_1$ as

$$n_0 = df_0, \quad n_1 = df_1, \quad d = (n_0, n_1),$$

then we have

$$e = (m, (m, a)n_0) = (m, a)(n_0, n_1) = (m, a)d = (m, a)n_0/f_0$$

and

$$n_{01} = n_1 f_0, \quad m = (m, a)n_1 = (m, a)n_{01}/f_0, \quad m = c_0 df_0.$$

Hence, we obtain

$$e\phi(n_{01}) = (m, a)n_0 f_0^{-1}\phi(mf_0(m, a)^{-1}) \geqq n_0 f_0^{-1}\ (mf_0),$$

and

$$\phi(mf_0) = f_0\phi(m)$$

because m is divisible by $f_0$. Therefore, we have

$$\phi(m/n_0) \leqq \phi(m)/\phi(n_0) \leqq en_0^{-1}\phi(n_{01})/\phi(n_0)$$

$$< 2c_0 n_0^{-1} = 2m/n_0^2.$$

Suppose that $\phi(n_{01})/\phi(n_0)$ is equal to one. Since $a_0$ is divisible by $(m, a)$, we have $n_0 < n_1$ and $n_{01} = 2n_0$ with $(n_0, 2) = 1$. Hence, we obtain $n_1 = 2n_0$ and $a_0 = (m, a)$. There is an integer $\rho$ relatively prime to m such that $\rho \equiv 2 \pmod{n_0}$. Here, $\rho$ is odd and $\rho \not\equiv 1, 2, 3 \pmod{n_1}$. We have

$$\rho c_0 \equiv 2c_0 \pmod{m}, \quad 2c_0 = 4a_0 < m,$$

and

$$\rho a_0 \not\equiv a_0, 2a_0, 3a_0 \pmod{m}.$$

Hence, $\rho a_0 > \rho c_0 \pmod m$, and $\rho b_0 < \rho c_0 \pmod m$. The number of natural numbers $\rho$ less than m satisfying

$$\rho \equiv 2 \pmod{n_0}, \quad (\rho, m) = 1$$

is $\phi(m)/\phi(n_0)$. For these $\rho$ and $\rho'$ we have $\rho b_0 \not\equiv \rho' b_0 \pmod m$, since $n_0^{-1}(\rho - \rho')$ is even and $b_0$ is relatively prime to $a_0 = c_0/2$. Therefore, we obtain

$$e'\{\phi(m)/\phi(n_0) - 1\} < 2c_0,$$

where e' is the greatest common divisor of m and $(m, b)n_0$. Let us suppose that $\phi(m)/\phi(n_0)$ is greater than one. Then we have

$$\phi(m/n_0) < 4m/n_0^2.$$

Thus, we have either

$$\phi(n_{01})/\phi(n_0) = \phi(m)/\phi(n_0) = 1$$

or $\phi(m/n_0) < 4m/n_0^2$. We shall assume that the above equalities hold. Then we have $m = 2n_0 = n_1$ and $n_0$ is odd. Since $c_0 = 2$ and $(m, b) < 2c_0$, we obtain $(m, b) = 1, 2, 3$. If it is equal to 2, then we have

$$\rho a_0 \equiv 2 \pmod{n_0}, \quad \rho b_0 \equiv 2 \pmod m,$$

and $\{2, n_0 + 2, 4\}$ is the fifth triple given above with $s = 2$ and $r = n_0$. Suppose that $(m, b) \neq 2$. Then,

$$\rho a_0 \equiv n_0 + 2, \quad \rho c_0 \equiv 4, \quad \rho b_0 \equiv 1, 3 \pmod m.$$

Hence, we have

$$\rho^2 a_0 \equiv n_0 + 4, \quad \rho^2 c_0 \equiv 8, \quad \rho^2 b_0 \equiv n_0 + 2, n_0 + 6 \pmod m.$$

Therefore, we obtain $n_0 \leqq 5$ and $m \leqq 10$.

Let us suppose that we are in the case (B). Take a natural number $\rho$ less than m satisfying $\rho \equiv 1 \pmod{n_0}$, $(\rho, m) = 1$ We have either $a_0\rho < c_0$ or $a_0\rho > c_0 \pmod{m}$. We may assume that the number of $\rho$ for which we have the former is not less than that of $\rho$ for which we have the latter. Let us indicate it by A. Then $A \geqq \frac{1}{2}\phi(m)/\phi(n_0)$. We have $a_0\rho \equiv a_0\rho' \pmod{m}$ if and only if $\rho \equiv \rho' \pmod{n_{01}}$. Hence, we obtain

$$e\{A\phi(n_{01})/\phi(m) - 1\} < c_0$$

and

$$e\{\phi(n_{01})/\phi(n_0) - 2\} < 2c_0.$$

Suppose that $\phi(n_{01})/\phi(n_0)$ is greater than 2. Then we have

$$3\{\phi(n_{01})/\phi(n_0) - 2\} \geqq \phi(n_{01})/\phi(n_0)$$

and

$$\phi(m/n_0) < 6m/n_0^2.$$

By our assumption there is an integer $\rho_0$ relatively prime to m such that $a_0\rho_0 > c_0\rho_0 \equiv c_0 \pmod{m}$. If $\tau$ satisfies

$$\tau \equiv 1 \pmod{n_{01}}, \quad (\tau, m) = 1,$$

then $b_0\rho_0\tau < c_0 \pmod{m}$ and they are distinct from each other. Hence, we have

$$n_{01}\{\phi(m)/\phi(n_{01}) - 1\} < c_0.$$

Suppose that $\phi(m)/\phi(n_{01})$ is greater than 1. Then we have

$$n_{01}\phi(m)/\phi(n_{01}) < 2c_0.$$

Since

$$\phi(n_{01}) = \phi(n_0 n_{01}/n_0) \leq (n_{01}/n_0)\phi(n_0),$$

we obtain

$$\phi(m/n_0) \leq \phi(m)/\phi(n_0) \leq n_{01}n_0^{-1}\phi(m)/\phi(n_{01}) < 2m/n_0^2.$$

Therefore, either

$$\phi(n_{01})/\phi(n_0) = 2, \quad \phi(m)/\phi(n_{01}) = 1$$

or $\phi(m/n_0) < 6m/n_0^2$. We shall assume that the above equalities hold. One of the following four cases is possible:

(i) $m = n_{01} = 4n_0$, $n_0 \equiv 1 \pmod 2$;

(ii) $m = n_{01} = 3n_0$, $(n_0, 3) = 1$;

(iii) $m = 2n_{01}$, $n_{01} = 3n_0$, $(n_0, 6) = 1$;

(iv) $m = n_{01} = 2n_0$, $n_0 \equiv 0 \pmod 2$.

If we are in the case (iv) then $c_0 = 2$, $a_0 = 1$ and $b_0 = n_0+1$. This is the fifth case stated at the beginning with $r = n_0$ and $s = 1$. Suppose that we are in the case (i). Then, $c_0 = 4$ and we have either $a_0 = 1$, $b_0 = 2n_0 + 1$ or $a_0 = 3$, $b_0 = 2n_0 + 3$. Let us set $\rho = n_0 + 2$. Then, $\rho c_0 \equiv 8 \pmod m$ and we have

$$\rho a_0 \equiv n_0 + 2, \quad \rho b_0 \equiv 3n_0 + 2 \pmod m$$

in the former case,

$$\rho a_0 \equiv 3n_0 + 6, \quad \rho b_0 \equiv n_0 + 6 \pmod m$$

in the latter case. Hence, $n_0 \leq 5$ and $m \leq 20$. Suppose that we are in the case (ii). Then, $c_0 = 3$ and $a_0 = 1, 2$. We have

$$b_0 \equiv n_0 + 1,\quad 2n_0 + 2 \pmod m$$

in case $n_0 \equiv 1 \pmod 3$, and

$$b_0 \equiv 2n_0 + 1,\quad n_0 + 2 \pmod m$$

in case $n_0 \equiv 2 \pmod 3$. Let us set $\rho = n_0 + 3$. Then $\rho c_0 \equiv 9 \pmod m$. We have

$$\rho a_0 \equiv n_0 + 3,\quad 2n_0 + 6 \pmod m,$$

and

$$b_0 \equiv 2n_0 + 3,\quad n_0 + 6 \pmod m$$

in each case. Hence, $n_0 \leq 5$ and $m \leq 15$. Suppose that we are in the case (iii). Then, $c_0 = 6$ and $a_0 = 2, 4, 5$. We have

$$b_0 \equiv 2n_0 + 2,\quad 4n_0 + 4,\quad 2n_0 + 5 \pmod m$$

in case $n_0 \equiv 1 \pmod 6$, and

$$b_0 \equiv 4n_0 + 2,\quad 2n_0 + 4,\quad 4n_0 + 5 \pmod m$$

in case $n_0 \equiv 5 \pmod 6$. Let us set $\rho = n_0 + 6$. Then $c_0 \equiv 36 \pmod m$. We have

$$a_0 \equiv 2n_0 + 12,\quad 4n_0 + 24,\quad 5n_0 + 30 \pmod m$$

and

$$b_0 \equiv 4n_0 + 12,\quad 2n_0 + 24,\quad n_0 + 30 \pmod m$$

in each case. Hence, $n_0 < 30$ and $m \leq 174$.

From the table at the end of §5 we may replace c by

$$c' = a + b - c,\quad c'' = b - a.$$

Let $n_0'$ and $n_0''$ be the numbers defined by

$$m = (m, c')n_0' = (m, c'')n_0'',$$

and n be the least common multiple of $n_0$, $n_0'$ and $n_0''$. Then, m is either n or 2n, since

$$a = \frac{1}{2}(c + c' - c''), \quad b = \frac{1}{2}(c + c' + c'').$$

By the inequality

$$3 > (1 + \frac{1}{N})^N$$

for a natural number N we have

$$N > (N + 1)^{N/(N+1)}, \quad N > 2.$$

For a given natural number t greater than 3, let us decompose N into the product of prime numbers as follows:

$$N = \Pi p^a \Pi q^b, \quad p \geq t > q.$$

Then,

$$\begin{aligned}\phi(N) &= \Pi p^{a-1}(p - 1)\Pi q^b(1 - \frac{1}{q}) \\ &> \Pi p^{a-1+(t-1)/t}\Pi q^b \cdot \frac{q - 1}{q} \\ &> \Pi p^{a(t-1)/t}\Pi q^{b(t-1)/t} \cdot \frac{q - 1}{q} \\ &\geq N^{(t-1)/t} \cdot \frac{t - 2}{t - 1} \cdot \frac{t - 3}{t - 2} \cdot \ldots \frac{1}{2} = N^{(t-1)/t}(t - 1)^{-1}.\end{aligned}$$

If we have

$$\phi(m/n_0) < 6m/n_0^2,$$

then

$$(m/n_0)^{(t-1)/t} < 6(t - 1)m/n_0^2, \quad t > 3$$

and

$$n_0^{(t+1)/t} < 6(t-1)m^{1/t}, \quad t > 3.$$

Let us suppose that this inequality holds for each of $n_0$, $n_0'$ and $n_0''$. Then we obtain

$$(n_0 n_0' n_0'')^{(t+1)/t} < [6(t-1)]^3 m^{3/t} \leq [6(t-1)]^3 (\varepsilon n_0 n_0' n_0'')^{3/t}$$

for $t > 3$ with $\varepsilon = 1, 2$, since $m \leq \varepsilon n_0 n_0' n_0''$. Therefore,

$$(\varepsilon n_0 n_0' n_0'')^{1/(t+1)} < [6(t-1)]^{3t/(t-2)(t+1)} \varepsilon^{1/(t-2)}$$

and

$$n_0 < [6(t-1)]^{t/(t+1)} (\varepsilon n_0 n_0' n_0'')^{1/(t+1)}$$

$$< [6(t-1)]^{t/(t-2)} 2^{1/(t-2)}.$$

For $t = 10$ we have

$$6(t-1)^{t/(t-2)} = 54^{5/4} < (162)\frac{11}{12}, \quad 2^{1/(t-2)} = 2^{1/8} < \frac{9}{8}$$

and $n_0 \leq 167$. Hence, if $m$ is greater than $2(167)^3$ then we are in the case (I) of Schwarz' table.

## Note. Honda's theorem.

Consider a homogeneous linear differential equation of the first order over $\mathbb{C}(x)$:

$$\frac{dy}{dx} = q(x), \quad q \in \mathbb{C}(x).$$

If $q(x)$ takes the form:

$$q(x) = \sum_i \frac{e_i}{x - c_i}, \quad c_i \in \mathbb{C}, \quad e_i \in \mathbb{Q},$$

then it has an algebraic solution

$$y = \prod_i (x - c_i)^{e_i}.$$

We shall show this converse that if there is an algebraic solution then $q(x)$ takes the form as above. Let $F(X, Y)$ be an irreducible polynomial over $\mathbb{C}$ satisfying $F(x, y) = 0$. We write $F(X, Y)$ as

$$F(X, Y) = \sum_{n=0}^{m} A_n(X) Y^n, \quad A_n \in \mathbb{C}[X], \quad A_m \neq 0,$$

then the differentiation of $F(x, y) = 0$ gives as

$$\sum_n A_n'(x) y^n + \sum_n n A_n(x) y^{n-1} y' = \sum_n [A_n'(x) + n A_n(x) q(x)] y^n = 0.$$

Since $F(X, Y)$ is irreducible, we have

$$(A_n' + n A_n q)/A_n = A_0'/A_0$$

for every $n$. In particular it holds for $n = m$, and we obtain

$$q = \frac{1}{m}\left(\frac{A_0'}{A_0} - \frac{A_m'}{A_m}\right),$$

which takes the form as above.

A convergent power series $y = \Sigma c_n x^n$ $(0 \leq n < \infty)$ whose coefficients are rational numbers satisfying a linear homogeneous differential equation of the first order over $\mathbb{C}(x)$ is an algebraic function of $x$ over $\mathbb{Q}$ if there is a rational integer $A$ distinct from 0 such that $A^n c_n$ is an integer for every $n$.

This is due to T. Honda [10, §1] and will be proved as follows. He prepared a lemma:

Let $K$ be an algebraic number field of finite degree and $\alpha$ be an element of $K$. If there is a rational number $a$ satisfying the congruence $a \equiv \alpha \pmod{\mathfrak{P}}$ for all prime ideals $\mathfrak{P}$ in $K$ with exception of finite number of them, then $\alpha$ is a rational number.

A proof will be given as follows. Since there is a rational integer $A$ distinct from 0 such that $A\alpha$ is an integer, we may assume that $\alpha$ is an integer in $K$. Let $k$ denote $\mathbb{Q}(\alpha)$ and $n$ be $[k : \mathbb{Q}]$. A prime ideal $\mathfrak{p}$ in $k$ is decomposed into the product of prime ideals in $K$:

$$\mathfrak{p} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}.$$

Suppose that every $\mathfrak{P}_i$ is not an exceptional one. Then there is a rational integer $a_i$ satisfying the congruence $a_i \equiv \alpha \pmod{\mathfrak{P}_i}$ for every $i$. We have

$$\Pi(\alpha - a_i)^{e_i} \equiv 0 \pmod{\mathfrak{p}}$$

and there is an index $i$ such that $\alpha \equiv a_i \pmod{\mathfrak{p}}$. Suppose

that $\mathfrak{p}$ does not divide the discriminant of an irreducible equation defining $\alpha$ over the ring $\mathbb{Z}$ of rational integers. Then for every integer w in k there is a rational integer a satisfying the congruence $w \equiv a \pmod{\mathfrak{p}}$. Hence, the degree of all prime ideals in k is one with the exception of finite number of them, and all prime numbers p with the exception of finite number of them are decomposed into the product of n prime ideals in k:

$$p = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n .$$

A fundamental formula in algebraic number theory gives us

$$\lim_{s \to 1+} \Sigma p^{-s} / \log \frac{1}{s-1} = 1$$

and

$$\lim_{s \to 1+} \Sigma (N\mathfrak{p})^{-s} / \log \frac{1}{s-1} = 1,$$

where p and $\mathfrak{p}$ run over all prime numbers and all prime ideals of degree 1 in k respectively (cf. Weber [40, p.727], Takagi [38, Chap.12 and p.255]). Since $p = N\mathfrak{p}_1 = \ldots = N\mathfrak{p}_n$ in the decomposition of p, we obtain

$$1 = \lim_{s \to 1+} \Sigma (N\mathfrak{p})^{-s} / \log \frac{1}{s-1} = \lim_{s \to 1+} n \Sigma p^{-s} / \log \frac{1}{s-1} = n.$$

This completes the proof of our lemma.

As stated there by Honda, if we make use of Tschebotareff -Artin's theorem (Takagi [38, Chap.16]) then the equality n = 1 is an immediate consequence of our result that all prime numbers with the exception of finite number of them are decomposed

into the product of n prime ideals of degree 1 in k.

He prepared another lemma:

Consider a homogeneous linear differential equation of the first order with the prime field $\mathbb{F}_p$ of characteristic p:

$$\frac{dy}{dx} = r(x)y, \quad r \in \mathbb{F}_p(x).$$

If it has a non-trivial power series solution $y = \Sigma c_n x^n$ over $\mathbb{F}_p$ then there is a non-trivial polynomial solution over $\mathbb{F}_p$.

It will be proved as follows. If we write r(x) as

$$r(x) = \sum_{n=0}^{N} a_n x^n / \sum_{n=0}^{N} b_n x^n,$$

then the coefficients $c_n$ of y satisfy

$$b_0 c_1 = a_0 c_0, \quad b_0(2c_2) + b_1 c_1 = a_0 c_1 + a_1 c_0, \ \cdots,$$

$$b_0(Nc_N) + b_1(N-1)c_{N-1} + \cdots + b_N c_0$$

$$= a_0 c_{N-1} + a_1 c_{N-2} + \cdots + a_{N-1} c_0, \ \cdots,$$

$$b_0(nc_n) + b_1(n-1)c_{n-1} + \cdots + b_N(n-N)c_{n-N}$$

$$= a_0 c_{n-1} + \cdots + a_N c_{n-N-1}, \ \cdots .$$

Hence, if we have

$$c_{n-1} = c_{n-2} = \cdots = c_{n-N-1} = 0$$

then

$$c_0 + c_1 x + c_2 x^2 + \cdots c_{n-N-2} x^{n-N-2}$$

is a solution. Take an integer s such that $ps > N$ and there is an index n less than ps for which $c_n \neq 0$. Then, if we write y

as

$$y = v_0 + v_1 x^{ps} + v_2 x^{2ps} + \dots$$

with

$$v_0 = c_0 + c_1 x + \dots + c_{ps-1} x^{ps-1},$$

$$v_1 = c_{ps} + c_{ps+1} x + \dots + c_{2ps-1} x^{ps-1}, \dots ,$$

then there is an index m such that

$$v_m = d_0 v_0 + d_1 v_1 + \dots + d_{m-1} v_{m-1}, \quad d_i \in \mathbb{F}_p.$$

If we set

$$w = y(1 - d_0 x^{mps} - d_1 x^{(m-1)ps} - \dots - d_{m-1} x^{ps}),$$

then

$$w = v_0 + (v_1 - d_{m-1} v_0) x^{ps} + (v_2 - d_{m-1} v_1 - d_{m-2} v_0) x^{2ps} +$$

$$\dots + (v_m - d_{m-1} v_{m-1} - \dots - d_0 v_0) x^{mps} + \dots ,$$

where the coefficient of $x^i$ $[mps \leq i < (m+1)ps]$ vanishes. Hence, from w we have a non-trivial polynomial solution, because w is a solution by

$$\frac{d}{dx}(x^p) = p x^{p-1} = 0.$$

By these two lemmas we shall prove our theorem as follows. Since all $c_n$ are rational numbers, $q(x) = y'/y$ is a rational function of x over $\mathbb{Q}$. We write q(x) as

$$q(x) = P(x)/Q(x), \quad P, Q \in \mathbb{Z}[x].$$

In the splitting field K of $\mathbb{Q}(x)$ let us decompose q(x) into the sum of partial fractions:

$$q(x) = R(x) + \Sigma\frac{e}{x - c} + \Sigma\frac{e'}{(x - c)^2} + \ldots ,$$

where $R \in K[x]$ and c, e, e', ... are elements of K. Take a prime number p which does not divide A, the leading coefficient of $Q(x)$ and one of $A^n c_n$ distinct from 0. Then y satisfies the congruence $y' \equiv q(x)y \pmod{p}$ and there is a non-trivial polynomial solution $z(x)$ over $\mathbb{Z}$ of the congruence $z' \equiv q(x)z \pmod{p}$ by the second lemma. Let us decompose $z(x)$ into the product of powers of irreducible divisors over $\mathbb{Z}$:

$$z(x) = \Pi g(x)^a .$$

Then we have

$$\frac{z'(x)}{z(x)} = \Sigma a \frac{g'(x)}{g(x)} .$$

Hence, for a prime ideal $\mathfrak{P}$ in K which divides p we have

$$R(x) \equiv 0, \quad e' \equiv e'' \equiv \ldots \equiv 0 \pmod{\mathfrak{P}}$$

and

$$e \equiv a \pmod{\mathfrak{P}} .$$

Since these congruences are satisfied for all prime ideals in K with exception of finite number, we obtain

$$R(x) = 0, \quad e' = e'' = \ldots = 0,$$

and e is a rational number by the first lemma. Therefore, y is an algebraic function of x over $\mathbb{C}$, and it is an algebraic function over $\mathbb{Q}$ (cf. §4).

## Chapter III. Klein's settling.

### §7. Reduction through Kummer's equation.

We assume that our equation (E) is irreducible, that is, neither $\alpha$, $\beta$, $\gamma - \alpha$ nor $\gamma - \beta$ is a rational integer. The field of Puiseux series $\mathbb{C}\{\{x\}\}$ over $\mathbb{C}$ is algebraically closed (cf. for instance K. Iwasawa [12, p.64]). Let us suppose that we have an algebraic solution $y$ in $\mathbb{C}\{\{x\}\}$. Then there is an isomorphism $\sigma$ of $\mathbb{C}(x, y)$ over $\mathbb{C}(x)$ which does not leave $y'/y$ invariant and we have

$$y'\sigma y - y(\sigma y)' = y\sigma y[\frac{y'}{y} - \sigma(\frac{y'}{y})] \neq 0.$$

Hence, $\sigma y$ is a solution of (E) which is linearly independent of $y$, and every solution of (E) is algebraic.

There is a natural number $n$ such that we have

$$y = z_0 + x^{\frac{1}{n}}z_1 + \ldots + x^{\frac{n-1}{n}}z_{n-1}$$

with

$$z_i = x^{e_i}\sum_{j=0}^{\infty} c_{ij}x^j, \quad e_i \in \mathbb{Z}, \quad c_{ij} \in \mathbb{C}.$$

Since we have

$$[x^{\frac{i}{n}}z_i]' = x^{\frac{i}{n}}[\frac{i}{n}x^{-1}z_i + z_i'],$$

each of $z_i$ is a solution of (E). Hence, there are two solutions $y_1$ and $y_2$ of (E) which take the form:

$$y_i = x^{\rho_i}\sum_{j=0}^{\infty} c_{ij}x^j, \quad \rho_i \in \mathbb{Q}, \quad c_{ij} \in \mathbb{C}, \quad c_{i0} \neq 0$$

with $\rho_1 \neq \rho_2$. The indices $\rho_1$ and $\rho_2$ are determined by

$$\rho(\rho - 1) - \gamma\rho = \rho(\rho - 1 + \gamma) = 0.$$

Therefore, they are 0 and $\lambda$, and $\lambda$ is a rational number distinct from 0. By Kummer's table $\mu$ and $\nu$ are rational numbers. Hence, $\alpha$, $\beta$ and $\gamma$ are rational numbers.

We shall see that $\lambda$ is not an integer. To the contrary suppose that $\lambda$ is an integer. The coefficients $c_n$ of a solution y of the form:

$$y = \sum_{n=0}^{\infty} c_n x^n, \quad c_0 \neq 0$$

satisfies

$$(n + 1)(\gamma + n)c_{n+1} = (\alpha + n)(\beta + n)c_n, \quad n \geq 0,$$

and we have $c_{-\gamma} = 0$ in case $\gamma \leq 0$ because neither $\alpha$ nor $\beta$ is an integer. Therefore, we get $c_{-\gamma-1} = c_{-\gamma-2} = \cdots = c_0 = 0$, which contradicts our assumption that $c_0 \neq 0$. Similarly there is no solution y of the form:

$$y = x^{\lambda} \sum_{n=0}^{\infty} c_n x^n, \quad c_0 \neq 0$$

in case $\gamma > 1$. Thus, $\lambda$ is not an integer, and neither $\mu$ nor $\nu$ is an integer by Kummer's table.

The derivation d/dx of $\mathbb{C}(x)$ is uniquely enlarged into a derivation of every algebraic extension K of $\mathbb{C}(x)$ of finite degree (cf. for instance A. Weil [41, p.13]). Hence, every isomorphism of K over $\mathbb{C}(x)$ is a differential one.

Take a fundamental system of solutions $y_1$ and $y_2$ of (E). Then the ratio $z = y_1/y_2$ satisfies

$$(S)\qquad \frac{d}{dx}\left(\frac{z''}{z'}\right) - \frac{1}{2}\left(\frac{z''}{z'}\right)^2 = \frac{1}{2}\left[\frac{1-\lambda^2}{x^2} + \frac{1-\mu^2}{(1-x)^2} + \frac{\lambda^2+\mu^2-\nu^2-1}{x(x-1)}\right],$$

where the left hand side, the Schwarzian derivative of z, will be denoted by $\{z, x\}$. For its calculus confer for instance H. Morikawa [33, Chap.3,§1].

The field $\mathbb{C}(x, z)$ is a normal extension of $\mathbb{C}(x)$, since every isomorphism $\sigma$ of $\mathbb{C}(x, z)$ over $\mathbb{C}(x)$ gives a solution $\sigma z$ of (S) and it takes the form:

$$\sigma z = (C_1 z + C_2)/(C_3 z + C_4), \quad C_i \in \mathbb{C},$$

which belongs to $\mathbb{C}(z)$. Let $F(X, Z) = 0$ be an irreducible equation for z over $\mathbb{C}(x)$ and $F(X, Z)$ be of the form:

$$F(X, Z) = Z^n + A_1(X)Z^{n-1} + \ldots + A_n(X), \quad A_i \in \mathbb{C}(X).$$

Then there is an element $\xi$ of $\mathbb{C}(x)$ such that

$$\mathbb{C}(A_1(x), \ldots, A_n(x)) = \mathbb{C}(\xi)$$

by Lüroth's theorem. It is contained in $\mathbb{C}(z)$ and the latter is a normal extension of the former, since every root of $F(x, Z)$ is in $\mathbb{C}(z)$. We have $[\mathbb{C}(z): \mathbb{C}(\xi)] = n$ and $\mathbb{C}(z) \cap \mathbb{C}(x) = \mathbb{C}(\xi)$.

For an element u of $\mathbb{C}(x)$ with $u' \neq 0$ we define a derivation $d/du$ of $\mathbb{C}\{\{x\}\}$ by

$$\frac{d}{du} = \left(\frac{du}{dx}\right)^{-1}\frac{d}{dx}$$

and $\{w, u\}$ for an element w of $\mathbb{C}\{\{x\}\}$ by this derivation.

The Schwarzian derivative $\{z, \xi\}$ is an element of $\mathbb{C}(\xi)$, since for every isomorphism $\sigma$ of $\mathbb{C}(z)$ over $\mathbb{C}(\xi)$ we have

$$\sigma\{z, \xi\} = \{\sigma z, \xi\} = \{\frac{C_1 z + C_2}{C_3 z + C_4}, \xi\} = \{z, \xi\}.$$

The identity

$$\{\xi, x\} + \{z, \xi\}(\frac{d\xi}{dx})^2 = \{z, x\}$$

holds, and $\xi$ is a solution of the differential equation

$$\{\xi, x\} + \{z, \xi\}(\frac{d\xi}{dx})^2 = s(x),$$

where $s(x)$ is the right hand side of (S). This is Kummer's equation [25]. The coefficient $\{z, \xi\}$ will be determined later in this section.

If we have

$$\xi - \xi_0 = (z - z_0)^e \Phi_1(z)/\Phi_2(z), \quad e \in \mathbb{Z}, \quad \xi_0, z_0 \in \mathbb{C},$$

$$\Phi_i \in \mathbb{C}[z], \quad \Phi_1(z_0)\Phi_2(z_0) \neq 0$$

with the ramification exponent $e$, then

$$(\xi - \xi_0)^{\frac{1}{e}} = (z - z_0)[\Phi_1(z)/\Phi_2(z)]^{\frac{1}{e}}$$

and by the implicit function theorem

$$z - z_0 = t^{\frac{1}{e}}\psi(t^{\frac{1}{e}}), \quad t = \xi - \xi_0$$

in $\mathbb{C}\{\{t\}\}$, where $\psi(u)$ is a convergent power series of $u$ with $\psi(0) \neq 0$. Hence, we obtain

$$\{z, \xi\} = \{z - z_0, \xi - \xi_0\} = \frac{1}{2}(1 - e^{-2})t^{-2} + c_{-1}t^{-1}$$

$$+ c_0 + c_1 t + \ldots, \quad c_i \in \mathbb{C}.$$

For $\xi = \infty$ we have

$$\{z, \xi\} = \xi^{-4}\{z, \xi^{-1}\},$$

and for $z = \infty$

$$\{z, \xi\} = \{z^{-1}, \xi\}.$$

Hence, $\{z, \xi\}$ takes the form:

$$\{z, \xi\} = \Sigma\frac{a}{(\xi - c)^2} + \Sigma\frac{b}{\xi - c}, \quad a \in \mathbb{Q}, \quad b, c \in \mathbb{C}, \quad \Sigma b = 0,$$

where c runs over all branching points of $\xi$.

If Y is a rational function of X of the form

$$Y = \frac{\Phi(X)}{\Psi(X)}, \quad \Phi, \Psi \in \mathbb{C}[X], \quad (\Phi, \Psi) = 1,$$

then

$$2N - 2 = \Sigma(e_x - 1), \quad N = \max\{\deg \Phi, \deg \Psi\}.$$

Here, $e_x$ is the ramification exponent of $Y - y$ at $X = x$ with $y = \Phi(x)/\Psi(x)$. We replace $Y - y$ by $Y^{-1}$ in case $\Psi(x) = 0$ and $X - x$ by $X^{-1}$ in case $x = \infty$. This is Klein's formula [17, Part I, Chap.V], which is a special case of Riemann's one and can be proved elementarily (cf. Forsyth [5, §59]).

If $\xi - \xi_0$ has the ramification exponent e at $z = z_1$, then it has the same exponent for $z = z_i$ which satisfies $\xi(z_i) = \xi_0$ and takes the form:

$$\xi - \xi_0 = \prod_{i=1}^{M}(z - z_i)^e/\Psi(z), \quad z_i \in \mathbb{C}, \quad \Psi \in \mathbb{C}[z],$$

$$z_i \neq z_j \ (i \neq j), \quad \Pi\Psi(z_i) \neq 0,$$

where $\deg\Psi = e(M + 1)$ in case $\deg\Psi > eM$. Suppose that the branching points of $\xi$ are $\xi_1, \ldots, \xi_r$ and that $\xi - \xi_i$ has the

ramification exponent $e_i$. Then the degree n of $\xi(z)$ is divided by $e_i$ and $n = e_i f_i$. By Klein's formula we have

$$2n - 2 = \sum_{i=1}^{r} f_i(e_i - 1)$$

and

$$\sum_{i=1}^{r} \frac{1}{e_i} = r - 2 + \frac{2}{n}.$$

Here, we have $r = 0$ if and only if $n = 1$, and in the other case

$$r > 2 - \frac{2}{n} \geq 1.$$

Since

$$\sum_{i=1}^{r} \frac{1}{e_i} \leq \sum_{i=1}^{r} \frac{1}{2} = \frac{r}{2},$$

we obtain

$$r - 2 + \frac{2}{n} \leq \frac{r}{2}$$

and $r \leq 3$. We shall show that $r \neq 0, 2$. To the contrary suppose that r is either 0 or 2. We have

$$\frac{y_2'}{y_2} = -\frac{1}{2}\left[\frac{z''}{z'} + \frac{\gamma - (1 + \alpha + \beta)x}{x(x - 1)}\right]$$

and the identity

$$\frac{z''}{z'} = \xi' \frac{d^2z}{d\xi^2} \Big/ \frac{dz}{d\xi} + \frac{\xi''}{\xi'}.$$

If $r = 0$ then $d^2z/d\xi^2 = 0$ and $y_2'/y_2$ is contained in $\mathbb{C}(x)$. If $r = 2$, then we have

$$n\left(\frac{1}{e_1} + \frac{1}{e_2}\right) = 2$$

and $e_1 = e_2 = n$. We may take 0 and $\infty$ as $\xi_1$ and $\xi_2$, and in this

setting

$$\xi = cz^n, \quad c \in \mathbb{C}, \quad c \neq 0.$$

Hence,

$$\frac{d^2z}{d\xi^2} \Big/ \frac{dz}{d\xi} = \frac{1 - n}{n} \xi^{-1}$$

and $y_2'/y_2$ is in $\mathbb{C}(x)$. Thus in each case the conclusion contradicts our assumption that (E) is irreducible. Therefore, $r = 3$ because $r > 1$ unless $r = 0$. Since

$$\frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3} - 1 = \frac{2}{n} > 0,$$

we are in one of the following four cases with $e_1 \leq e_2 \leq e_3$:

(i) $e_1 = e_2 = 2, \quad n = 2e_3;$

(ii) $e_1 = 2, \quad e_2 = e_3 = 3, \quad n = 12;$

(iii) $e_1 = 2, \quad e_2 = 3, \quad e_3 = 4, \quad n = 24;$

(iv) $e_1 = 2, \quad e_2 = 3, \quad e_3 = 5, \quad n = 60.$

We may take 0, 1 and $\infty$ as $\xi_1$, $\xi_2$ and $\xi_3$. Then $\{z, \xi\}$ takes the form:

$$\text{(K)} \qquad \{z, \xi\} = -\left[\frac{1-e_1^{-2}}{\xi^2} + \frac{1 - e_2^{-2}}{(\xi - 1)^2} + \frac{e_1^{-2}+e_2^{-2}-e_3^{-2}-1}{\xi(\xi - 1)}\right]$$

with (i) - (iv). This equation will be solved at the end of the section.

Conversely, for a given finite group G of linear transformations of z we have a subfield $\mathbb{C}(\xi)$ of $\mathbb{C}(z)$ consisting of all elements of $\mathbb{C}(z)$ each of which is left invariant under the

action of G by Lüroth's theorem. The Schwarzian $\{z, \xi\}$ is contained in $\mathbb{C}(\xi)$ and $\mathbb{C}(z)$ is a normal extension of $\mathbb{C}(\xi)$. Hence, G is the Galois group of $\mathbb{C}(z)$ over $\mathbb{C}(\xi)$. The subfield $\mathbb{C}(\xi)$ is determined by a solution of (K) with (i)-(iv) unless G is a cyclic group. Therefore, G is one of the four groups stated in §3 unless it is cyclic.

Suppose that $\xi$ takes the form:

$$\xi = \frac{\Phi(z)^a}{F(z)^b}, \quad \Phi, F \in \mathbb{C}[z], \quad (\Phi, F) = 1$$

such that

$$1 - \xi = \frac{\Psi(z)^c}{F(z)^b}, \quad \Psi \in \mathbb{C}[z];$$

here we have

$$a.\deg \Phi = b(\deg F + 1)$$

in case $a.\deg \Phi > b.\deg F$,

$$b.\deg F = a(\deg \Phi + 1)$$

in case $b.\deg F > a.\deg \Phi$ and

$$b.\deg F = c(\deg \Psi + 1)$$

in case $b.\deg F > c.\deg \Psi$. Let us assume that

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 = \frac{2}{n}, \quad n = \max\{a.\deg\Phi, c.\deg \Psi, b.\deg F\}.$$

Then we have

$$(a - 1)\frac{n}{a} + (b - 1)\frac{n}{b} + (c - 1)\frac{n}{c} = 2n - 2.$$

By Klein's formula, $\Phi$, $\Psi$ and F do not possess multiple roots,

and there are no branching points of $\xi$ other than 0, 1 and $\infty$. Hence, z is a solution of (K) with $a = e_1$, $b = e_2$ and $c = e_3$. Our solution z of (K) with (i)-(iv) is given as follows (cf. for instance Weber [40, Chap.9]):

(i) $z = e^{2\frac{i}{r}t}$, $\xi = \sin^2 t$, $i = \sqrt{-1}$, $n = 2r$,

$$\xi = -\frac{(z^r - 1)^2}{4z^r}, \quad 1 - \xi = \frac{(z^r + 1)^2}{4z^r};$$

(ii) $\Phi_1 = z^4 + 2\sqrt{-3}z^2 + 1$,

$\Phi_2 = z^4 - 2\sqrt{-3}z^2 + 1$, $f = z(z^4 - 1)$,

$12\sqrt{-3}f^2 = \Phi_1^3 - \Phi_2^3$, $\xi = 12\sqrt{-3}f^2\Phi_1^{-3}$;

(iii) $W = z^8 + 14z^4 + 1$,

$K = z^{12} - 33z^8 - 33z^4 + 1$, $f = z(z^4 - 1)$,

$W^3 - K^2 = 108f^4$, $\xi = -\frac{1}{108}K^2f^{-4}$;

(iv) $T = z^{30} + 1 + 522(z^{25} - z^5) - 10005(z^{20} + z^{10})$,

$H = -(z^{20} + 1) + 228(z^{15} - z^5) - 494z^{10}$,

$f = z(z^{10} + 11z^5 - 1)$,

$T^2 + H^3 = 1728f^5$, $\xi = \frac{1}{1728}T^2f^{-5}$.

The Galois group is the dihedral group, the tetrahedral group, the octahedral group and the icosahedral group respectively.

## §8. Explicit description of algebraic solutions.

We shall solve Kummer's equation for $\xi$:

$$\{\xi, x\} + \{z, \xi\}\left(\frac{d\xi}{dx}\right)^2 = \{z, x\}.$$

Here, $z$ is the ratio $y_1/y_2$ of linearly independent algebraic solutions $y_1$ and $y_2$ of (E) which is assumed to be irreducible. It may be supposed that the branching points of $\xi$ as a function of $z$ are $0$, $1$ and $\infty$. By Gauss' transformations we may assume that $\lambda$, $\mu$ and $\nu$ have their values in Schwarz' table, and they can be permuted in each other. Our equation has been solved in case of (I) with $\nu^{-1} \in \mathbb{Z}$ and (II), (IV), (VI). We shall solve it in the remained cases, where (XII) and (XV) will be replaced by

(XII)' $\quad \lambda = \frac{4}{5}, \quad \mu = \frac{1}{3}, \quad \nu = \frac{1}{3}, \quad \text{Area}/\pi = \frac{7}{15} = 14C$

and

(XV)' $\quad \lambda = \frac{2}{3}, \quad \mu = \frac{2}{5}, \quad \nu = \frac{2}{5}, \quad \frac{7}{15} = 14C.$

By $s(\lambda, \mu, \nu, x)$ we indicate

$$s(x) = \frac{1}{2}\left[\frac{1 - \lambda^2}{x^2} + \frac{1 - \mu^2}{(x - 1)^2} + \frac{\lambda^2 + \mu^2 - \nu^2 - 1}{x(x - 1)}\right].$$

If we are in the case of (i)-(iv) of the previous section, then for a rational function $\xi(x)$ we have a normal extension $\mathbb{C}(x, z)$ of $\mathbb{C}(x)$ by the translation theorem because $\mathbb{C}(z)$ is a normal extension of $\mathbb{C}(\xi)$. Under the action of the Galois group $\{z, x\}$ is left invariant and it is an element of $\mathbb{C}(x)$.

(I) Suppose that we are in the case (i). If we set

$$x = \sin^2 \frac{t}{s}$$

with a natural number s which is relatively prime to r, then we have

$$\xi = xH(x)^2, \quad 1 - \xi = (1 - x)K(x)^2, \quad H, K \in \mathbb{Z}[x]$$

with

$$\deg H = \deg K = \frac{1}{2}(s - 1)$$

in case s is odd, and

$$\xi = x(1 - x)H(x)^2, \quad 1 - \xi = K(x)^2, \quad H, K \in \mathbb{Z}[x]$$

with

$$\deg H = \frac{s}{2} - 1, \quad \deg K = \frac{s}{2}$$

in case s is even. In each case

$$\deg H + \deg K + s - 1 = 2s - 2.$$

Hence, by Klein's formula H(x) and K(x) satisfy

$$(H, H_x) = (K, K_x) = 1, \quad H(0)H(1)K(0)K(1) \neq 0,$$

and there are no branching points of $\xi$ other than 0, 1 and $\infty$. The ramification exponent of $\xi^{-1}$ at $x = \infty$ as a function of x is s, and that of $\xi^{-1}$ at $z = 0$ as a function of z is r. Therefore, we have

$$\{z, x\} = s(\frac{1}{2}, \frac{1}{2}, \frac{s}{r}, x).$$

For, at $x = \infty$ we get

$$\xi^{-1} = x^{-s}\Phi(x^{-1}) = z^r\Psi(z), \quad \Phi \in \mathbb{C}(x^{-1}), \quad \Psi \in \mathbb{C}(z)$$

and

$$x^{-\frac{s}{r}}[\Phi(x^{-1})]^{\frac{1}{r}} = z[\Psi(z)]^{\frac{1}{r}}.$$

By the implicit function theorem we obtain

$$z = x^{-\frac{s}{r}} \sum_{j=0}^{\infty} a_j x^{-\frac{j}{r}}, \quad a_j \in \mathbb{C}, \quad a_0 \neq 0$$

and

$$\{z, x^{-1}\} = \frac{1}{2}[1 - (\frac{s}{r})^{-2}]x^2 + b_{-1}x + b_0 + b_1 x^{-1} + \ldots$$

with $b_j \in \mathbb{C}$.

Suppose that $\xi(x)$ takes the form:

$$\xi = x^a(x - 1)^b\Phi(x)^d/F(x)^e, \quad F(0)F(1) \neq 0,$$

$$1 - \xi = \Psi(x)^f/F(x)^e, \quad (\Phi, F) = (\Psi, F) = 1,$$

$$\Phi, \Psi, F \in \mathbb{C}[x]$$

with natural numbers a, b, e, d and f; here we set

$$c = f.\deg \Psi - e.\deg F$$

in case $f.\deg \Psi > e.\deg F$, and

$$c = \max\{e.\deg F - a - b - d.\deg \Phi, e.\deg F - f.\deg \Psi\}$$

in the other case. We assume that

$$a - 1 + b - 1 + c - 1 + (d - 1)\deg \Phi$$

$$+ (e - 1)\deg F + (f - 1)\deg \Psi = 2n - 2$$

with

$$n = \max\{a + b + d.\deg \Phi, e.\deg F, f.\deg \Psi\}.$$

Then, by Klein's formula there are no branching points of $\xi$

other than 0, 1 and $\infty$.

(III), (V), (VIII). Suppose that we are in one of the cases (ii), (iii) and (iv). Let us set

$$\xi = \frac{(2 - x)^2}{4(1 - x)}, \quad 1 - \xi = \frac{- x^2}{4(1 - x)}.$$

Then in a function $z(x)$, $x = 2$ is not a branching point. If we write $\{z, \xi\}$ as

$$\{z, \xi\} = s(\tfrac{1}{2}, \tfrac{1}{p}, \tfrac{1}{q}, \xi),$$

then we have

$$\{z, x\} = s(\tfrac{2}{p}, \tfrac{1}{q}, \tfrac{1}{q}, x).$$

In the following discussions for the cases (VII), (IX), (X), (XI) and (XIII) we are in the case (iv), where we set

$$\xi = \frac{T^2 f^{-5}}{1728}, \quad 1 - \xi = - \frac{H^3 f^{-5}}{1728}, \quad \{z, \xi\} = s(\tfrac{1}{2}, \tfrac{1}{3}, \tfrac{1}{5}, \xi)$$

in (VIII),

$$\xi = 1728 f^5 T^{-2}, \quad 1 - \xi = - H^3 T^{-2},$$

$$\{z, \xi\} = s(\tfrac{1}{5}, \tfrac{1}{3}, \tfrac{1}{2}, \xi)$$

in (IX), (X), and

$$\xi = 1728 f^5 H^{-3}, \quad 1 - \xi = - 1728 f^5 T^{-2},$$

$$\{z, \xi\} = s(\tfrac{1}{5}, \tfrac{1}{2}, \tfrac{1}{3}, \xi)$$

in (XI), (XIII).

(VII) Let us set

$$\xi = (2 - x)^2 x^{-2}, \quad 1 - \xi = - 4(1 - x) x^{-2}.$$

Then we have

$$\{z, x\} = s(\tfrac{2}{5}, \tfrac{1}{3}, \tfrac{1}{3}, x).$$

(IX) We have the identity:

$$27x^2(x - 1) - (3x - 4)^3 = (9x - 8)^2.$$

Let us set

$$\xi = 27x^2(x - 1)(9x - 8)^{-2},$$

$$1 - \xi = -(3x - 4)^3(9x - 8)^{-2}.$$

Then we have

$$\{z, x\} = s(\tfrac{2}{5}, \tfrac{1}{5}, \tfrac{1}{2}, x).$$

(X) We have the identity:

$$64x^3(x - 1) - (8x - 9)^3 = (8x^2 - 36x + 27)^2.$$

Let us set

$$\xi = 64x^3(x - 1)(8x^2 - 36x + 27)^{-2},$$

$$1 - \xi = -(8x - 9)^3(8x^2 - 36x + 27)^{-2}.$$

Then we have

$$\{z, x\} = s(\tfrac{3}{5}, \tfrac{1}{5}, \tfrac{1}{3}, x).$$

(XI) We have the identity:

$$(2x^3 - 3x^2 - 3x + 2)^2 + 27x^2(x - 1)^2 = 4(x^2 - x + 1)^3.$$

Let us set

$$\xi = \tfrac{27}{4}x^2(x - 1)^2(x^2 - x + 1)^{-3},$$

$$1 - \xi = \frac{1}{4}(2x^3 - 3x^2 - 3x + 2)^2(x^2 - x + 1)^{-3}.$$

Then we have

$$\{z, x\} = s(\tfrac{2}{5}, \tfrac{2}{5}, \tfrac{2}{5}, x).$$

(XIII) We have the identity:

$$(x^3 + 30x^2 - 96x + 64)^2 = (x^2 - 16x + 16)^3 + 108x^4(x - 1)$$

Let us set

$$\xi = - 108x^4(x - 1)(x^2 - 16x + 16)^{-3},$$

$$1 - \xi = (x^3 + 30x^2 - 96x + 64)^2(x^2 - 16x + 16)^{-3}.$$

Then we have

$$\{z, x\} = s(\tfrac{4}{5}, \tfrac{1}{5}, \tfrac{1}{5}, x).$$

Thus, Kummer's equation has been solved in the twelve cases of Schwarz' table. These are those treated by Brioschi [3].

The icosahedral group is generated by

$$\zeta' = \varepsilon\zeta, \quad \varepsilon^5 = 1, \quad \zeta' = - \zeta^{-1}$$

and

$$\zeta' = (\omega\zeta + 1)(\zeta - \omega)^{-1}, \quad \omega^2 = 1 - \omega,$$

if we consider it a group of linear transformations of $\zeta$. It consists of

$$\zeta' = \varepsilon^r\zeta, \quad \zeta' = - \varepsilon^r\zeta^{-1},$$

$$\zeta' = (\varepsilon^r\omega\zeta + \varepsilon^{r-s})(\zeta - \varepsilon^{-s}\omega)^{-1},$$

$$\zeta' = -(\varepsilon^{r+s}\zeta - \varepsilon^{r}\omega)(\varepsilon^{s}\omega\zeta + 1)^{-1}$$

with $r = 0, 1, 2, 3, 4$ (cf. for instance Weber [40, §74]).

Let us set

$$z = g(\zeta) = \zeta^{2}(\zeta^{5} - 7)(7\zeta^{5} + 1)^{-1}.$$

Then we have

$$g(\varepsilon\zeta) = \varepsilon^{2}z, \quad g(-\zeta^{-1}) = -z^{-1},$$

and

$$g\left(\frac{\omega\zeta + 1}{\zeta - \omega}\right) = -\frac{z - \omega}{\omega z + 1}.$$

This is due to Gordan [6]. Hence, $g(\zeta')$ is a linear transform of $g(\zeta)$ for every transformation of the group.

The roots of

$$f(\zeta)/\zeta = \zeta^{10} + 11\zeta^{5} - 1$$

are

$$\varepsilon^{r}\omega, \quad \varepsilon^{r}\omega', \quad \omega\omega' = -1, \quad r = 0, 1, 2, 3, 4,$$

where

$$\omega = \varepsilon + \varepsilon^{4}, \quad \omega' = \varepsilon^{2} + \varepsilon^{3}.$$

The polynomial

$$\zeta^{2}(\zeta^{5} - 7) + \zeta^{2}(1 + \omega)(7\zeta^{5} + 1)$$

has a multiple root $\varepsilon\omega$. Hence, the branching points of $\zeta$ in $z = g(\zeta)$ are

$$0, \infty, \varepsilon^{r}\omega, \varepsilon^{r}\omega', \quad r = 0, 1, 2, 3, 4$$

with the ramification exponents 2 at each point by Klein's

formula.

In the following discussions for the cases (XII)', (XIV) and (XV)' we suppose that

$$\xi = H(\zeta)^3 T(\zeta)^{-2}, \quad 1 - \xi = 1728 f(\zeta)^5 T(\zeta)^{-2},$$

$$\{\zeta, \xi\} = s(\tfrac{1}{3}, \tfrac{1}{5}, \tfrac{1}{2}, \xi)$$

in (XII)' and

$$\xi = 1728 f(\zeta)^5 T(\zeta)^{-2}, \quad 1 - \xi = H(\zeta)^3 T(\zeta)^{-2},$$

$$\{\zeta, \xi\} = s(\tfrac{1}{5}, \tfrac{1}{3}, \tfrac{1}{2}, \xi)$$

in (XIV), (XV)'.

(XII)' If we set

$$\xi = 4x(x - 1)(2x - 1)^{-2}, \quad 1 - \xi = (2x - 1)^{-2},$$

then we have

$$\{\zeta, x\} = s(\tfrac{1}{3}, \tfrac{1}{3}, \tfrac{2}{5}, x) \qquad \text{(VII)}$$

and by the translation theorem $\mathbb{C}(x, z)$ is a normal extension of $\mathbb{C}(x)$, since $\mathbb{C}(\zeta)$ is a normal extension of $\mathbb{C}(\xi)$. The Galois group is the icosahedral group because there is no proper intermediate field between $\mathbb{C}(x)$ and $\mathbb{C}(\xi)$. Under the action of the Galois group $\{z, x\} = \{g(\zeta), x\}$ is left invariant, and it is an element of $\mathbb{C}(x)$. Hence, we have

$$\{z, x\} = s(\tfrac{1}{3}, \tfrac{1}{3}, \tfrac{4}{5}, x).$$

(XIV) Let us set $\xi = x$. Then we have

$$\{z, x\} = \{g(\zeta), x\} = s(\tfrac{2}{5}, \tfrac{1}{3}, \tfrac{1}{2}, x).$$

(XV)' Let us set

$$\xi = 4x(x - 1)(2x - 1)^{-2}, \quad 1 - \xi = (2x - 1)^{-2}$$

Then we have

$$\{\zeta, x\} = s(\tfrac{1}{5}, \tfrac{1}{5}, \tfrac{2}{5}, x) \qquad \text{(VIII)}$$

and

$$\{z, x\} = \{g(\zeta), x\} = s(\tfrac{2}{5}, \tfrac{2}{5}, \tfrac{2}{3}, x).$$

## Chapter IV. Landau-Errera's theorem.

### §9. Errera's lemma.

For a given natural number c we call a divisor v of $\phi(c)$ an E-number of c if the number of integers r relatively prime to c which satisfy the inequality

$$\frac{k-1}{v}\,c < r < \frac{k}{v}\,c$$

is equal to $\phi(c)/v$ for every integer k. This notion is due to Errera [4]. Suppose that $c = ap$ with p prime and that a has an E-number v. If p divides a, then the number of r satisfying

$$\frac{k-1}{vp}\,c < r < \frac{k}{vp}\,c, \quad (r, c) = 1$$

is equal to $\phi(a)/v = \phi(c)/(vp)$. Hence, vp is an E-number of c. If p does not divide a, then the number of r satisfying

$$\frac{k-1}{v}\,ap < r < \frac{k}{v}\,ap, \quad (r, a) = 1$$

is equal to $p\phi(a)/v$. For a multiple $r = ps$ of p we have

$$\frac{k-1}{v}\,a < s < \frac{k}{v}\,a.$$

Hence, the number of r satisfying our inequality with $(r, ap) = 1$ is equal to

$$p\phi(a)/v - \phi(a)/v = (p-1)\phi(a)/v = \phi(c)/v.$$

Hence, v is an E-number of c. This is due to Errera [4].

If p is prime, then for every integer k the inequality

$$\frac{k-1}{p-1}\,p < r < \frac{k}{p-1}\,p$$

is satisfied only by $r = k$. Hence, $p - 1$ is an E-number of p.

The number of r satisfying

$$\frac{k-1}{c}c^2 < r < \frac{k}{c}c^2, \quad (r, c) = 1$$

is equal to $\phi(c) = \phi(c^2)/c$. Hence, c is an E-number of $c^2$. Suppose that $c = \Pi p^e$ and $v = \Pi p^{e-1}$ with prime numbers p. Then, $c/v = \Pi p$ and the number of r satisfying our inequality with $(r, c) = 1$ is equal to

$$\phi(\Pi p) = \Pi\phi(p) = \phi(c)/v.$$

Hence, v is an E-number of c. For our c we have another E-number $p^{e-1}(p - 1)$.

Suppose that three natural numbers n, k and c are given such that

$$n > 1, \quad k < c, \quad (k, c) = 1.$$

Let q be the number of natural numbers r satisfying

$$r < cn, \quad r \equiv k \pmod{n}, \quad (r, c) = 1,$$

and s be the number of r which satisfy additional condition that $r < c$. In the following case (i) we have $s/q = 1$:

(i) $c = 2$, $(n, 2) = 1$, $k = 1$;

the number r satisfying our condition with $r < cn$ is 1. In the following eleven cases (ii)-(xii) we have $s/q = 1/2$:

(ii) $c = 2$, $n \equiv 0 \pmod{2}$, $k = 1$;

the numbers r satisfying our condition with $r < cn$ are 1 and $n + 1$.

(iii) $c = 3$, $(n, 3) = 1$, $k = 1, 2$;

our r are k and $k + jn$, where j is either 1 or 2 and $k + jn \neq$

$0 \pmod 3$.

(iv) $c = 4$, $n \equiv 1 \pmod 2$, $k = 1, 3$;

our r are k and k + 2n.

(v) $c = 6$, $(n, 6) = 1$, $k = 1, 5$;

our r are k and k + jn, where j is either 2 or 4 and $k + jn \not\equiv 0 \pmod 3$.

$(vi)_1$ $n = 2$, $(c, 2) = 1$;

$(vi)_2$ $n = 2$, $c \equiv 0 \pmod 2$, $(k, 2) = 1$;

if c is odd then $\phi(2c) = \phi(c)$ and for a natural number $\rho$ relatively prime to c which is less than c we have an even number $c - \rho$ in case $\rho$ is odd, an odd number $c + \rho$ in case $\rho$ is even; if c is even then $\phi(2c) = 2\phi(c)$.

(vii) $n = 3$, $c = 5$, $k \equiv 1 \pmod 3$;

our r are 1, 4 and 7, 13.

(viii) $n = 3$, $c = 8$, $k \equiv 1 \pmod 3$;

our r are 1, 7 and 13, 19.

(ix) $n = 3$, $c = 10$, $k \equiv 1 \pmod 3$;

our r are 1, 7 and 13, 19.

(x) $n = 3$, $c = 20$, $k \equiv 1 \pmod 3$;

our r are 1, 7, 13, 19 and 31, 37, 43, 49.

(xi) $n = 4$, $c = 6$, $k \equiv 1 \pmod 4$;

our r are 1, 5 and 13, 17.

(xii) $n = 5$, $c = 12$, $k \equiv 1 \pmod 5$;

our r are 1, 11 and 31, 41. We shall prove the following lemma due to Errera [4]:

Either $s/q \leq 1/2$ or $s/q = 1$. The latter case occurs

only if we are in the case (i). The case $s/q = 1/2$ occurs only if we are in one of the above eleven cases (ii)-(xii).

Before we begin the proof we note the following: Suppose that $(c, n) = 1$. Then there is an integer y satisfying $cy \equiv -k \pmod{n}$. If r satisfies $r \equiv k \pmod{n}$, then $r \equiv -cy \pmod{n}$ and it can be written as $r = nx - cy$ with an integer x. We have $(r, c) = 1$ if and only if $(x, c) = 1$, and $0 < r < jc$ if and only if

$$\frac{y}{n} c < x < \frac{y + j}{n} c$$

for every integer j.

First suppose that the greatest common divisor d of c and n is not 1. If r satisfies

$$r \equiv k \pmod{n}, \quad (r, c) = 1,$$

this condition is satisfied by $r' = r + cn/d$. Hence, the number of r satisfying our condition with $r < cn/d$ is equal to $q/d$. We have $s \leq q/d$ and $s/q \leq 1/d \leq 1/2$. If $s/q = 1/2$, then $d = 2$. Suppose that c is divisible by 4. Then, $r'' = r + cn/4$ is relatively prime to c, and the number of our r satisfying

$$j \frac{c}{4} n < r < (j + 1)\frac{c}{4} n$$

is equal to $q/4$ for every j. Therefore, $n = 2$. If c is not divisible by 4, then we can write c as $c = 2c'$ with $(c', n) = 1$. A number r satisfying

$$r \equiv k \pmod{n}, \quad (r, c') = 1$$

is relatively prime to c, since it is odd. If it is less than

c'n then it is less than 2c'. Suppose that v is an E-number of c'. Then we have

$$(v - 2)/v < 2/n,$$

and

$$v < 2n/(n - 2), \quad n/2 < 1 + 2/(v - 2).$$

If $v \geqq 3$, then $n < 6$. If $n = 4$, then $v < 4$ and $c' = 1, 3$. If $c' = 3$, then two of $k$, $k + n$ and $k + 2n$ are relatively prime to 3, since $(n, c') = 1$. Hence, $n < 6$ and $n = 2, 4$.

Secondly let us suppose that $(n, c) = 1$. For an E-number v of c we have a natural number h such that

$$(h - 1)/v < 1/n \leqq h/v.$$

Hence,

$$s/q \leqq (h + 1)/v < \frac{2}{v} + \frac{1}{n}.$$

We have $q = \phi(c)$, and $\phi(c) \leqq 2$ if and only if $c = 2, 3, 4, 6$. We may assume that $\phi(c) > 2$. Suppose that $n \geqq 6$. Then, if $v \geqq 6$, we have $s/q < 1/2$. Let us suppose that every E-number of c is less than 6. Then, a prime number different from 2, 3 and 5 can not divide c, and

$$c = 120, 60, 40, 30, 24, 20, 15, 12, 10, 8, 5.$$

We have $s - 1 < c/n$, and $s/q < 1/2$ if $n > c/[\phi(c)/2 - 1]$. In case c is even, we have $2(s - 1) < c/n$, and $s/q < 1/2$ if n is greater than $c/[\phi(c) - 2]$. For the above c these values are

$$\frac{120}{30}, \frac{60}{14}, \frac{40}{14}, \frac{30}{6}, \frac{24}{6}, \frac{20}{6}, \frac{15}{3}, \frac{12}{2}, \frac{10}{2}, \frac{8}{2}, \frac{5}{1}.$$

They are less than 6 except 12/2, but 12 is not relatively prime to 6. Thus, if $n \geq 6$ then $s/q < 1/2$. Suppose that $n = 5$. If $v \geq 7$ then $s/q < 1/2$. We have

$$\frac{1}{6} < \frac{1}{5} < \frac{2}{6} < \frac{2}{5} < \frac{3}{6} < \frac{3}{5} < \frac{4}{6} < \frac{4}{5} < \frac{5}{6}.$$

Hence, $s/q \leq 2/6 < 1/2$ if $v = 6$. Let us suppose that every E-number of c is less than 6. Then a prime number different from 2 and 3 can not divide c, since c is relatively prime to 5. We have $c = 24, 12, 8$. If $c = 24$, then the natural numbers less than 24 which are relatively prime to 24 are

$$1, 5, 7, 11, 13, 17, 19, 23.$$

Hence, $s/q \leq 2/8 < 1/2$. Suppose that $c = 12$. Our numbers are 1, 5, 7, 11. As above we define y by $cy \equiv -k \pmod{n}$. If $y \equiv 2 \pmod{5}$, then $s/q = 1/2$. In the other case we have $s/q < 1/2$. The former case occurs if and only if $k \equiv 1 \pmod{5}$. Suppose that $c = 8$. Our numbers are 1, 3, 5, 7. We have

$$1 < \frac{8}{5} < 3 < \frac{16}{5} < \frac{24}{5} < 5 < \frac{32}{5} < 7.$$

Hence, $s/q \leq 1/4 < 1/2$. Suppose that $n = 4$. If $v \geq 8$, then $s/q < 1/2$. If c is divisible by 7, then 6 is an E-number of c and

$$\frac{1}{6} < \frac{1}{4} < \frac{2}{6} < \frac{2}{4} = \frac{3}{6} < \frac{4}{6} < \frac{3}{4} < \frac{5}{6}.$$

Hence, $s/q \leq 2/6 < 1/2$. If c is divisible by 5, then 4 is an E-number of c and $s/q = 1/4 < 1/2$. Let us assume that every E-number of c is less than 8 and c is relatively prime to 35. Then $c = 9$. The natural numbers less than 9 which are relative-

ly prime to 9 are 1, 2, 4, 5, 7, 8, and

$$2 < \frac{9}{4} < 4 < \frac{18}{4} < 5 < \frac{27}{4} < 7.$$

Hence, $s/q \leq 2/6 < 1/2$. Suppose that $n = 3$. If $v \geq 12$, then $s/q < 1/2$. If $c$ is divisible by 11, then 10 is an E-number of $c$ and

$$\frac{3}{10} < \frac{1}{3} < \frac{4}{10}, \quad \frac{6}{10} < \frac{2}{3} < \frac{7}{10}.$$

Hence, $s/q \leq 4/10 < 1/2$. If $c$ is divisible by 7, then 6 is an E-number and $s/q = 2/6 < 1/2$. Let us assume that every E-number of $c$ is less than 12 and $c$ is relatively prime to 77. Then $c$ is divisible only by 2 and 5, and

$$c = 80, 40, 20, 16, 10, 8, 5.$$

If $c = 80$, then 8 is an E-number of $c$ and

$$20 < \frac{80}{3} < 30, \quad 50 < \frac{160}{3} < 60.$$

Here, 21 is relatively prime to 80 and less than 80/3. Hence, $s/q < 1/2$. If $c = 40$, then the numbers less than 40 which are relatively prime to 40 are

1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39,

and

$$13 < \frac{40}{3} < 17, \quad 23 < \frac{80}{3} < 27.$$

Hence, $s/q \leq 6/16 < 1/2$. Suppose that $c = 20$. Then our numbers are 1, 3, 7, 9, 11, 13, 17, 19, and

$$3 < \frac{20}{3} < 7, \quad 13 < \frac{40}{3} < 17.$$

If $y \equiv 1 \pmod 3$, then $s/q = 1/2$. In the other case $s/q = 1/4$. The former occurs if and only if $k \equiv 1 \pmod 3$. Suppose that $c = 16$. Then our numbers are 1, 3, 5, 7, 9, 11, 13, 15, and

$$5 < \frac{16}{3} < 7, \quad 9 < \frac{32}{3} < 11.$$

Hence, $s/q \leq 3/8 < 1/2$. Suppose that $c = 10$. Then our numbers are 1, 3, 7, 9, and

$$1 < \frac{8}{3} < 3, \quad 5 < \frac{16}{3} < 7.$$

If $y \equiv 1 \pmod 3$ then $s/q = 0$. In the other case $s/q = 1/2$. The latter occurs if and only if $k \equiv 1 \pmod 3$. Suppose that $c = 5$. Then our numbers are 1, 2, 3, 4, and

$$1 < \frac{5}{3} < 2, \quad 3 < \frac{10}{3} < 4.$$

If $y \equiv 1 \pmod 3$ then $s/q = 1/2$. In the other case $s/q = 1/4$. The former occurs if and only if $k \equiv 1 \pmod 3$.

## §10. Two lemmata.

Given natural numbers c, k and n, we shall prove the following lemma:

Suppose that for a divisor e of n every integer r satisfying

$$r \equiv k \pmod{n}, \quad (r, c) = 1, \quad 0 < r < cn$$

is less than ec. Then (n, c) = 1 and c = 1, 2, 3, 6 unless e = n. We have c = 3, 6 only if e/n = 1/2.

If d = (c, n) is greater than 1 then the number of r satisfying our condition with

$$\frac{j}{d} cn < r < \frac{j+1}{d} cn, \quad 0 < j < d$$

is equal to each other. Hence,

$$\frac{d-1}{d} n < e$$

and

$$\frac{n}{e} < \frac{d}{d-1} = 1 + \frac{1}{d-1} \leq 2.$$

Therefore, e = n. Suppose that d = 1. If v is an E-number of c then we have

$$\frac{v-2}{v} < \frac{e}{n}$$

by our note in the previous section. Hence,

$$\frac{n}{e} < 1 + \frac{2}{v-2}.$$

If $v \geq 4$ then n/e < 2. Suppose that every E-number of c is less than 4. Then, c = 6, 4, 3, 2. We have

$$\frac{n}{e} < \frac{c}{\phi(c) - 1},$$

and

$$\frac{n}{e} < \frac{1}{2}\,\frac{c}{\phi(c) - 1}$$

in case c is even. Hence, if c = 3, 6 then n/e < 3, and if c = 4 then n/e < 2.

We shall prove another lemma:

Suppose that n is an odd integer greater than 1 and $0 < k < 2c$. Let us assume that every integer r satisfying our condition with $0 < r < cn$ is less than 2c. Then we are in one of the following five cases (i)-(v):

(i) $c = 1,\ k = 1;$

(ii) $c = 2,\ k = 1, 3;$

(iii) $n = 3,\ c = 4,\ k = 1, 7;$

(iv) $n = 3,\ c = 10,\ k = 1, 7, 13, 19;$

(v) $n = 5,\ c = 6,\ k = 1, 11.$

If c = 1 then our r with $0 < r < cn$ is k, which is 1. If c = 2 then r is odd and our r with $0 < r < cn$ is either k or k + n. In case k is odd the latter is even and $r = k < 2c$. If k is even then we have $r = k + n < 2c = 4$. It is impossible, because $n \geq 3$. In the case (iii) our r are 1, 7, which are less than 2c. In the case (iv) our r are 1, 7, 13, 19, and they are less than 2c. In the case (v) our r are 1, 11, and they are less than 2c. Thus, the above five cases actually occur. If d = (n, c) is greater than 1 then we have

$$(d - 1)cn/d < 2c$$

and

$$\frac{1}{d} > 1 - \frac{2}{n} \geq \frac{1}{3}.$$

Hence, $d = 2$. It is impossible, since n is odd. Suppose that $d = 1$. We may assume that $\phi(c) > 1$. If v is an E-number of c then

$$\frac{v - 2}{v} < \frac{2}{n}, \qquad v < \frac{2n}{n - 2}$$

and

$$\frac{n}{2} < 1 + \frac{2}{v - 2}.$$

We have $n < 2c/[\phi(c) - 1]$, and $n < c/[\phi(c) - 1]$ in case c is even. Suppose that $n = 3$. There is no E-number of c greater than 5, and a prime number different from 2 and 5 can not divide c. A closed interval whose length is not less than 4 contains a number relatively prime to 10. Hence, $c/3 < 4$ and c is less than 12. Since

$$\frac{8}{\phi(8) - 1} = \frac{8}{3} < 3,$$

we have $c \neq 8$. If $c = 4$ then we have $r = 5, 11$ in case $k = 2$ and $r = 3, 9$ in case $k = 3$. These cases are impossible. If $c = 5$ then we have

$$r = 1, 4, 7, 13$$

in case $k = 1, 4$,

$$r = 2, 8, 11, 14$$

in case $k = 2$, and

$$r = 3, 6, 9, 12$$

in case $k = 3$. Hence, it is impossible. Suppose that $n \geq 5$. Then $v < 4$ and there is no E-number of c greater than 3. Hence,

$c = 6, 4, 3$. We have $c/[\phi(c) - 1] = c$, and $c \neq 4$. If $c = 6$ then $n = 5$, and we have

| | |
|---|---|
| $r = 7, 17$ | in case $k = 2, 7,$ |
| $3, 13$ | $3, 8,$ |
| $9, 19$ | $4, 9,$ |
| $5, 25$ | $5, 10.$ |

These cases are impossible. If $c = 3$ then $n = 5$, since $n$ is odd. We have

| | |
|---|---|
| $r = 1, 11$ | in case $k = 1,$ |
| $2, 7$ | $2,$ |
| $8, 13$ | $3,$ |
| $4, 14$ | $4,$ |
| $5, 10$ | $5.$ |

It is impossible.

## §11. Attainment of Schwarz' table.

In Schwarz' table we set

$$\alpha = a/m, \quad \beta = b/m, \quad \gamma = c/m,$$

where a, b, c and m are natural numbers satisfying (a, b, c, m) = 1. From each triple we have 24 triples by the table at the end of §5, which may not be distinct from each other. For the values of c there are six elements:

$$c,\ m - c,\ a + b - c,\ m - a - b + c,\ m + a - b,\ b - a.$$

If all of them are equal to m/2, then

$$\{a, b, c\} = \{1, 3, 2\}, \quad m = 4.$$

This triple satisfies Landau's criterion, and it belongs to (I) of Schwarz' table with $\nu = 1/2$. We shall assume that the greatest common divisor $c_0$ of c and m is not m/2. Under this assumption we have the following table of $\{a, b, c\}$ with $m \equiv 0 \pmod{c}$:

m = 2r with even r:

(1) $\{1, r + 1, 2\}, \quad (r \neq 2)$ (I)

m = 2r with odd r:

(2) $\{1, r + 1, 2\},$ (I)

m = 6:

(3) $\{1, 3, 2\}, \quad \{1, 5, 2\},$ (III)

m = 10:

(4) $\{1, 3, 2\}, \quad \{1, 9, 2\},$ (XIII)

m = 12:

(5) {1, 5, 3}, {1, 10, 3},
{2, 5, 3}, {2, 10, 3}, (V)

(6) {2, 5, 4}, {2, 11, 4}, (V)

(7) {1, 7, 4}, {1, 9, 4},
{3, 7, 4}, {3, 9, 4}, (II)

m = 15:

(8) {1, 7, 3}, {1, 11, 3},
{2, 7, 3}, {2, 11, 3}, (X)

(9) {1, 7, 5}, {1, 13, 5},
{4, 7, 5}, {4, 13, 5}, (X)

m = 20:

(10) {1, 11, 4}, {1, 13, 4},
{3, 11, 4}, {3, 13, 4}, (IX)

m = 24:

(11) {1, 13, 6}, {1, 17, 6},
{5, 13, 6}, {5, 17, 6}, (IV)

(12) {1, 13, 8}, {1, 19, 8},
{7, 13, 8}, {7, 19, 8}, (IV)

m = 30:

(13) {1, 11, 6}, {1, 25, 6},

{5, 11, 6}, {5, 25, 6}, (VIII)

(14) {3, 13, 6}, {3, 23, 6}, (XII)

(15) {1, 19, 10}, {1, 21, 10}, (VII)

(16) {3, 13, 10 , {3, 27, 10}, (XII)

(17) {5, 11, 10}, {5, 29, 10}, (VIII)

(18) {5, 17, 10}, {5, 23, 10}, (XV)

(19) {7, 13, 10}, {7, 27, 10}, (XII)

(20) {9, 19, 10}, {9, 21, 10}, (VII)

m = 60:

(21) {1, 31, 12}, {1, 41, 12},
{11, 31, 12}, {11, 41, 12}, (VI)

(22) {1, 31, 20}, {1, 49, 20}, (VI)

(23) {7, 37, 20}, {7, 43, 20}, (XIV)

(24) {7, 37, 20}, {7, 43, 20}, (XIV)

(25) {13, 37, 20}, {19, 49, 20}, (VI)

Given natural numbers a, b, c and m satisfying

$$a < c < b < m, \quad m \equiv 0 \pmod{c}, \quad (a, b, c) = 1,$$

we assume that for every integer $\rho$ relatively prime to m either

$$a\rho < c\rho < b\rho \pmod{m}$$

or

$$b\rho < c\rho < a\rho \pmod{m}.$$

If m/c is not equal to 2 then {a, b, c} is one of the above table. We shall prove this theorem due to Errera [4] as follows. Let us set $m = cn_0$ and

$$a = da', \quad c = dc', \quad d = (a, c), \quad m = m'd, \quad m' = c'n_0.$$

If $\rho'$ is relatively prime to m' then there is an integer $\rho$ relatively prime to m such that $\rho \equiv \rho' \pmod{m'}$. Suppose that we are in the case (A) of §6. If $\rho_0'$ satisfies

$$\rho_0' \equiv 1 \pmod{n_0}, \quad (\rho_0', c') = 1$$

then there is an integer $\rho_0$ such that

$$\rho_0 \equiv \rho_0' \pmod{m'}, \quad (\rho_0, m) = 1$$

and we have

$$\rho_0 a < \rho_0 c \equiv c \pmod{m},$$

that is, $\rho_0' a' < c' \pmod{m'}$. If $r = a' + xn$ is relatively prime to c' then there is an integer $\rho_0'$ satisfying our condition such that $\rho_0' a' \equiv r \pmod{m'}$. For, there is an integer y satisfying $a'y \equiv x \pmod{c'}$, and if we set $\rho_0' = 1 + yn_0$ then

$$a'\rho_0' \equiv a' + n_0 x \pmod{m'}, \quad (\rho_0', c') = 1.$$

By our assumption we have

$$r < c' \pmod{m'}.$$

If we set $k = a'$, $c = c'$ and $n = n_0$ in Errera's lemma, then we are in the case (i), since $s/q = 1$. Therefore, we have

$$c' = 2, \quad a' = 1, \quad (n_0, 2) = 1,$$

and

$$c = 2a, \quad m = 2an_0, \quad (a, b) = 1.$$

Here, $n_0 > 1$ because $c < m$. Let us set

$$b = d'b', \quad c = d'c", \quad (b, c) = d',$$

$$m" = c"n_0, \quad m = m"d'.$$

Here, $d' = 1, 2$, and the latter happens only if $c"$ is odd. There is an integer $\rho_1$ such that

$$\rho_1 \equiv 2 \pmod{n_0}, \quad (\rho_1, c) = 1,$$

and $\rho_1 = 2 + xn_0$ with an odd integer $x$, since $c$ is even. We have

$$\rho_1 a = c + x\frac{m}{2} \equiv c + \frac{m}{2} \pmod{m},$$

and

$$\rho_1 c \equiv 2c \pmod{m}, \quad 2c < c + \frac{m}{2} < m,$$

because $n_0 > 2$. Hence,

$$\rho_1 b < 2c \pmod{m},$$

that is,

$$\rho_1 b' < 2c" \pmod{m"}.$$

We define $k$ by

$$k \equiv \rho_1 b' \pmod{m"}, \quad 0 < k < m".$$

Then, $k$ is relatively prime to $c"$ and less than $2c"$. If $r = k + xn_0$ is relatively prime to $c"$ then there is an integer $\rho_1"$ relatively prime to $c"$ such that

$$\rho_1" b' \equiv k + xn_0 \pmod{m"}.$$

Hence, we have

$$r < 2c'' \pmod{m''}.$$

Let us set $c = c''$ and $n = n_0$ in the second lemma of the previous section. Then we are in one of the following five cases:

(i) $c'' = 1, \quad k = 1;$

(ii) $c'' = 2, \quad k = 1, 3;$

(iii) $n_0 = 3, \quad c'' = 4, \quad k = 1, 7;$

(iv) $n_0 = 3, \quad c'' = 10, \quad k = 1, 7, 13, 19;$

(v) $n_0 = 5, \quad c'' = 6, \quad k = 1, 11.$

In the last four cases $d' = 1$, since $c''$ is even. We shall discuss each case separately.

(i) Since $c > 1$, we have $d' = 2$, and

$$c = 2, \quad a = 1, \quad b \equiv 0 \pmod 2, \quad m = 2n_0, \quad n_0 \equiv 1 \pmod 2.$$

Let us set $\rho_1 = 2 + n_0$. Then it is relatively prime to m and

$$a\rho_1 \equiv 2 + n_0, \quad c\rho_1 \equiv 4, \quad b\rho_1 \equiv 2 \pmod m.$$

We have $b = 1 + n_0$. This is the case (2) of our table.

(ii) We have

$$c = 2, \quad a = 1, \quad b \equiv 1 \pmod 2, \quad m = 2n_0, \quad n_0 \equiv 1 \pmod 2.$$

Let us set $\rho_1 = 2 + n_0$. Then it is relatively prime to m and

$$a\rho_1 \equiv 2 + n_0, \quad c\rho_1 \equiv 4, \quad b\rho_1 \equiv 1, 3 \pmod m.$$

We have

$$a\rho_1^2 \equiv 4 + n_0, \quad c\rho_1^2 \equiv 8, \quad b\rho_1^2 \equiv 2 + n_0, 6 + n_0 \pmod m.$$

Therefore, if $n_0 > 6$ then each of $4 + n_0$, $2 + n_0$ and $6 + n_0$ is

greater than 8 and less than $2n_0$. It contradicts our assumption. Hence, $n_0 \leq 5$. Suppose that $n_0 = 3$. Then $\rho_1 = 5$ and $5^2 \equiv 1 \pmod 6$. Therefore, b is either 3 or 5. This is the case (3) of our table. Suppose that $n_0 = 5$. Then $\rho_1 = 7$ and $7.3 \equiv 1 \pmod{10}$. Hence, b is either 3 or 9. This is the case (4) of our table.

(iii) We have

$$c = 4, \quad a = 2, \quad m = 12, \quad \rho_1 = 5, \quad b\rho_1 \equiv 1, 7 \pmod{12},$$

and b = 5, 11. This is the case (6) of our table.

(iv) We have

$$c = 10, \quad a = 5, \quad m = 30, \quad \rho_1 = 11,$$

$$b\rho_1 \equiv 1, 7, 13, 19 \pmod{30},$$

and b = 11, 17, 23, 29. These are the cases (17) and (18) of our table.

(v) We have

$$c = 6, \quad a = 3, \quad m = 30, \quad \rho_1 = 7, \quad b\rho_1 \equiv 1, 11 \pmod{30},$$

and b = 13, 23. This is the case (14) of our table.

Let us assume that we are in the case (B) of §6. As above we set

$$a = da', \ c = dc', \ m' = c'n_0, \ m = m'd, \ d = (a, c)$$

and

$$b = d'b', \ c = d'c'', \ m'' = c''n_0, \ m = m''d', \ d' = (b, c).$$

We say that a natural number $\rho$ less than m belongs to C if it

is relatively prime to m and $\rho \equiv 1 \pmod{n_0}$. For an element $\rho$ of C we write $\rho \in C_1$ in case $a\rho < c \pmod{m}$ and $\rho \in C_2$ in case $b\rho < c \pmod{m}$. By our assumption $|C| = |C_1| + |C_2|$, where the absolute value indicates the cardinal number. We say that a natural number $\rho'$ less than m' belongs to C' if it is relatively prime to m' and $\rho' \equiv 1 \pmod{n_0}$. For an element $\rho'$ of C' we write $\rho' \in C_1'$ if $a'\rho' < c' \pmod{m'}$. We have $|C_1|/|C| = |C_1'|/|C'|$. If $r = a' + xn_0$ is relatively prime to c' then there is an element $\rho'$ of C' such that $a'\rho' \equiv r \pmod{m'}$. Let q' be the number of such r with $0 < r < m'$, and s' be that of such r with $0 < r < c'$. Then we have $s'/q' = |C_1'|/|C'|$. We say that a natural number $\rho''$ less than m" belongs to C" if it is relatively prime to m" and $\rho'' \equiv 1 \pmod{n_0}$. For an element $\rho''$ of C" we write $\rho'' \in C_2''$ if $b'\rho'' < c'' \pmod{m''}$. We have $|C_2|/|C| = |C_2''|/|C''|$. By Errera's lemma we have

$$|C_1'|/|C'| = |C_2''|/|C''|,$$

since both sides are positive by our assumption. If an integer $\rho_1$ satisfies

$$\rho_1 \equiv 1 \pmod{m''}, \quad (\rho_1, d') = 1$$

then we have

$$c\rho_1 \equiv c, \quad b\rho_1 \equiv b \pmod{m}$$

and $a\rho_1 < c \pmod{m}$. Here, a is relatively prime to d', and if $r = a + xm''$ is relatively prime to d' then there is an integer $\rho_1$ satisfying our condition such that $a\rho_1 \equiv r \pmod{m}$.

Hence, we have $r < c \pmod{m}$. Let us set $c = d'$, $k = a$, $n = m''$ and $e = c''$ in the first lemma of the previous section. Since $c'' \neq m''$, we have

$$(m'', d') = 1, \quad d' = 1, 2$$

by our assumption that $n_0 \neq 2$. Similarly we have

$$(m', d) = 1, \quad d = 1, 2.$$

By our assumption that $(a, b, c) = 1$ we have $(d, d') = 1$. Hence, either $d = 1$ or $d' = 1$. We may assume that $d = 1$, that is, $(a, c) = 1$. Let us set $k = a$ and $n = n_0$ in Errera's lemma. Then we are in one of the following ten cases (i)-(x) by $n_0 \neq 2$:

(i) $c = 2$, $n_0 \equiv 0 \pmod{2}$, $a = 1$;

(ii) $c = 3$, $(n_0, 3) = 1$, $a = 1, 2$;

(iii) $c = 4$, $n_0 \equiv 1 \pmod{2}$, $a = 1, 3$;

(iv) $c = 6$, $(n_0, 6) = 1$, $a = 1, 5$;

(v) $n_0 = 3$, $c = 5$, $a = 1, 4$;

(vi) $n_0 = 3$, $c = 8$, $a = 1, 7$;

(vii) $n_0 = 3$, $c = 10$, $a = 1, 3, 7, 9$;

(viii) $n_0 = 3$, $c = 20$, $a = 1, 7, 13, 19$;

(ix) $n_0 = 4$, $c = 6$, $a = 1, 5$;

(x) $n_0 = 5$, $c = 12$, $a = 1, 11$.

We shall treat them separately.

(i) If we set $\rho = 1 + n_0$ then it is relatively prime to $m = 2n_0$, since $n_0$ is even. We have $\rho^2 \equiv 1$, $c\rho \equiv 2 \pmod{m}$, and $b = 1 + n_0$. This is the case (1) of our table.

(ii) If $n_0 \equiv 1 \pmod{3}$ then we set $\rho = 1 + n_0$. We have

$\rho^2 \equiv 1$, $c\rho \equiv 3 \pmod{m}$. Hence, $b = 1 + n_0,\ 2 + 2n_0$. For $\tau = 3 + n_0$ we have

$$a\tau \equiv 3 + n_0,\ 6 + 2n_0,\quad c\tau \equiv 9,\quad b\tau \equiv 3 + 2n_0,\ 6 + n_0 \pmod{3n_0}.$$

Hence, $n_0 < 6$ and $n_0 = 4$. It is the case (5) of our table. If $n_0 \equiv 2 \pmod 3$ then we set $\sigma = 1 + 2n_0$. We have $\sigma^2 \equiv 1 \pmod{m}$ and $b = 1 + 2n_0,\ 2 + n_0$. For $\tau = 3 + n_0$ we get

$$b\tau \equiv 3 + 2n_0,\ 6 + n_0 \pmod{3n_0}.$$

Hence, $n_0 < 6$ and $n_0 = 5$. It is the case (8) of our table.

(iii) For $\rho = 1 + 2n_0$ we have $\rho^2 \equiv 1 \pmod{4n_0}$ and

$$b = 1 + 2n_0,\ 3 + 2n_0,$$

since $d' = 1$ by $(m'', d') = 1$. If we set $\tau = 2 + n_0$ then

$$a\tau \equiv 2 + n_0,\ 6 + 3n_0,\quad c\tau \equiv 8,$$

$$b\tau \equiv 2 + 3n_0,\ 6 + n_0 \pmod{4n_0}.$$

Hence, $n_0 < 6$. If $n_0 = 3$ it is the case (7), and if $n_0 = 5$ it is the case (10) of our table.

(iv) If $n_0 \equiv 1 \pmod 6$ then we set $\rho = 1 + 4n_0$. We have $\rho^2 \equiv 1 \pmod{6n_0}$ and $b = 1 + 4n_0,\ 5 + 2n_0$. For $\tau = 2 + 3n_0$ we get

$$a \equiv 2 + 3n_0,\ 10 + 3n_0,\quad c \equiv 12,$$

$$b \equiv 2 + 5n_0,\ 10 + n_0 \pmod{6n_0},$$

and $n_0 < 4$. This is impossible. If $n_0 \equiv 5 \pmod 6$ then we set

$\rho = 1 + 2n_0$. We have $\rho^2 \equiv 1 \pmod{6n_0}$ and $b = 1 + 2n_0,\ 5 + 4n_0$. For $\tau = 2 + 3n_0$ we get

$$b \equiv 2 + n_0,\ 10 + 5n_0 \pmod{6n_0},$$

and $n_0 \leq 10$. Hence, $n_0 = 5$. This is the case (13) of our table

(v) We have $\rho c \equiv c \pmod{15}$ if and only if

$$\rho \equiv 1, 4, 7, 13 \pmod{15}.$$

Hence, $b = 7, 13$. This is the case (9) of our table.

(vi) We have $\rho c \equiv c \pmod{24}$ if and only if

$$\rho \equiv 1, 13, 19 \pmod{24}.$$

Hence, $b = 13, 19$. This is the case (12) of our table.

(vii) We have $\rho c \equiv c \pmod{30}$ if and only if

$$\rho \equiv 1, 7, 13, 19 \pmod{30}.$$

We get the following table:

| $\rho$ | 1 | 7 | 11 | 13 |
|---|---|---|---|---|
| $\rho a$ | 1 | 7 | 11 | 13 |
| | 3 | 21 | 3 | 9 |
| | 7 | 19 | 17 | 1 |
| | 9 | 3 | 9 | 27 |
| $\rho c$ | 10 | 10 | 20 | 10 |
| $\rho b$ | 13 | 1 | 23 | 19 |
| | 19 | 13 | 29 | 7 |
| | 21 | 27 | 21 | 3 |
| | 27 | 9 | 27 | 21 |

Hence, we have the cases (15), (16), (19) and (20) of our table.

(viii) We have $\rho c \equiv c \pmod{60}$ if and only if

$$\rho \equiv 1, 7, 13, 31, 37, 49 \pmod{60}$$

and get the following table:

| $\rho$ | 1 | 7 | 11 | 13 | 23 | 29 |
|---|---|---|---|---|---|---|
| $\rho a$ | 1 | 7 | 11 | 13 | 23 | 29 |
| | 7 | 49 | 17 | 31 | 41 | 23 |
| | 13 | 31 | 23 | 49 | 19 | 17 |
| | 19 | 13 | 29 | 7 | 17 | 11 |
| $\rho c$ | 20 | 20 | 40 | 20 | 40 | 40 |
| $\rho b$ | 31 | 37 | 41 | 43 | 53 | 59 |
| | 37 | 19 | 47 | 1 | 31 | 13 |
| | 43 | 1 | 53 | 19 | 49 | 47 |
| | 49 | 43 | 59 | 37 | 47 | 41 |

Hence, we obtain the cases (22), (23), (24) and (25) of our table.

(ix) We have $\rho c \equiv c \pmod{24}$ if and only if

$\rho \equiv 1, 5, 13, 17 \pmod{24}$.

Hence, b = 13, 17. This is the case (11) of our table.

(x) We have $\rho c \equiv c \pmod{60}$ if and only if

$\rho \equiv 1, 11, 31 \pmod{60}$.

Hence, b = 31, 41, and we get the case (21), filling up our table.

Thus, we have proved Landau-Errera's theorem. We shall note that if $m/c = n_0$ is equal to 2 then either d = (a, c) or d' = (b, c) is equal to 1. To prove it we shall assume neither d nor d' is 1 to the contrary. By the first lemma of the previous section we have either d = 2 and d' = 3 or d = 3 and d' = 2. Let us suppose that the former occurs. Then c = 2c' = 3c" and b is odd. If we set $\rho = c + 1$, it is odd and relatively

prime to m = 2c. We have

$$a\rho \equiv a, \quad c\rho \equiv c, \quad b\rho \equiv b - c \pmod{2c},$$

which contradicts our assumption that they satisfy Landau's criterion. Hence, either d = 1 or d' = 1. If m/c = 2 then by our theorem we are in one of the following cases, which are derived from Schwarz' table:

m = 2r:

$\{s, r + s, r\}$, $(s, r) = 1$ (I)

$\{s, m - s, r\}$, $(s, r) = 1$ (I)

m = 12:

$\{1, 9, 6\}$, $\{3, 7, 6\}$, $\{3, 11, 6\}$, $\{5, 9, 6\}$, (II)

m = 20:

$\{1, 13, 10\}$, $\{1, 17, 10\}$, $\{3, 11, 10\}$,

$\{3, 19, 10\}$, $\{7, 11, 10\}$, $\{7, 19, 10\}$,

$\{9, 13, 10\}$, $\{9, 17, 10\}$, (IX)

m = 24:

$\{1, 17, 12\}$, $\{1, 19, 12\}$, $\{5, 11, 12\}$,

$\{5, 23, 12\}$, $\{7, 11, 12\}$, $\{7, 23, 12\}$,

$\{11, 17, 12\}$, $\{11, 19, 12\}$, (IV)

m = 60:

$\{1, 41, 30\}$, $\{1, 49, 30\}$, $\{11, 31, 30\}$,

$\{11, 59, 30\}$, $\{19, 31, 30\}$, $\{19, 59, 30\}$,

{29, 41, 30}, {29, 49, 30}, (VI)

{7, 43, 30}, {7, 47, 30}, {13, 37, 30},

{13, 43, 30}, {17, 37, 30}, {17, 53, 30},

{23, 43, 30}, {23, 47, 30}. (XIV)

In this case where m/c = 2 it was proved by Landau [27] under the assumption that either d = 1 or d' = 1.

# Chapter V. Transcendental liouvillian solutions.

## §12. Picard-Vessiot theory.

Let k be a differential field of characteristic 0. E. R. Kolchin [22] proved the existence of its universal extension $\Omega$, which has the following property. Suppose that K is a finitely generated differential extension of k in $\Omega$ and L is a finitely generated differential extension of K. Then L has a differential isomorphic image over K in $\Omega$. The proof is based on the following theorem in Ritt's book[34, p.51]: Let $\Pi$ be a prime differential ideal in $k\{y\}$ with the indeterminates $y_1, \cdots, y_n$ and K be a differential extension of k. Then the ideal in $K\{y\}$ generated by $\Pi$ is a prime ideal if k is algebraically closed.

If an element u of $\Omega$ is not contained in k then there is a differential isomorphism $\sigma$ of $k\langle u\rangle$ over k such that $\sigma u \neq u$ (cf. Kolchin[20, p.25], [19]). It will be proved as follows. We may assume that u is transcendental over k, since if u is algebraic over k then there is an algebraic isomorphism $\sigma$ of $k(u)$ with $\sigma u \neq u$ and it is a differential one. Let $\Pi$ denote the ideal composed of all differential polynomials with a single indeterminate y over $\bar{k}$ which vanishes at u, where $\bar{k}$ is the algebraic closure of k. Then it is a prime ideal in $\bar{k}\{y\}$. If we set $K = \bar{k}\langle u\rangle$ then the ideal $\Pi'$ in $K\{y\}$ generated by $\Pi$ is a prime ideal and does not contain $y - u$ because u is transcendental over k. Hence, a generic zero v of $\Pi'$ is not equal to u, and if we set $\sigma u = v$ then it gives a differential isomorphism over $\bar{k}$.

Let $\Pi$ be a prime differential ideal in $k\{y\}$. If a differential polynomial $D(y)$ is not contained in $\Pi$ then there is a zero $u$ of $\Pi$ such that $D(u) \neq 0$ and every constant of $k\langle u\rangle$ is algebraic over $k$. This existence theorem is due to Kolchin[21] (cf. M. Matsuda[32, pp.108-109]).

Consider a homogeneous linear differential equation over $k$:

$$y^{(n)} + a_1 y^{(n-1)} + \cdots + a_n y = 0, \quad a_i \in k.$$

We assume that the field of constants $k_0$ of $k$ is algebraically closed. Then, by the existence theorem there is a fundamental system of solutions $\eta_1, \cdots, \eta_n$ in $\Omega$ such that the field of constants of $k\langle\eta_1, \cdots, \eta_n\rangle$ is $k_0$, since the wronskian determinant $W(y_1, \cdots, y_n)$ is not contained in the differential ideal generated by

$$\sum a_i y_j^{(n-i)}, \quad 1 \leq j \leq n$$

in $k\{y\}$. This is a Picard-Vessiot extension for our equation.

Kolchin's work[20] tells us its fundamental properties. Let $G$ denote the group of all differential automorphisms of $\Sigma = k\langle\eta_1, \cdots, \eta_n\rangle$ over $k$. Then it is an algebraic matric group of degree $n$ over $k_0$. An element of $\Omega$ which is left invariant under every automorphism in $G$ belongs to $k$. The component $G_0$ of the identity in $G$ is a normal algebraic subgroup of $G$ of finite index. If $K$ is an algebraic subgroup of $G$ then there is a differential subfield $\Xi$ of $\Sigma$ such that $K$ consists of all automorphisms in $G$ which leave every element of $\Xi$ invariant. For the component $G_0$ we have

$$[G : G_0] = [\Sigma_0 : k]$$

where $\Sigma_0$ is the subfield of $\Sigma$ left invariant under $G_0$. If the wronskian determinant $W(\eta_1, \cdots, \eta_n)$ is constant, that is $a_1 = 0$, then every element $\sigma$ of G has its determinant equal to 1, since $\sigma W = \det\sigma \cdot W$. Extension $\Sigma$ of k is algebraic if and only if G is finite.

A differential extension L of k whose field of constants is $k_0$ is called a liouvillian extension of k if there is a finite chain of differential extensions of k:

$$k = L_0 \subset L_1 \subset \cdots \subset L_n = L$$

such that $L_i$ is an algegraic extension of $L_{i-1}(u_i)$ of finite degree and we have either $u_i' \in L_{i-1}$ or $u_i'/u_i \in L_{i-1}$ for each i. If $\Sigma = k\langle\eta_1, \cdots, \eta_n\rangle$ is contained in a liouvillian extension of k then the component $G_0$ is reducible to triangular form.

Suppose that the order of our equation is 2 and the coefficient $a_1$ of y' vanishes. We assume that our equation is irreducible over k, that is, the logarithmic derivative $\eta'/\eta$ of every non-trivial solution $\eta$ does not belong to k. Then, G can not be reduced to triangular form. If there is a non-trivial solution in a liouvillian extension of k then there is a Picard-Vessiot extension $\Sigma$ of k for our equation which is contained in a liouvillian extension of k. The component $G_0$ of the identity is reducible to triangular form. There is a non-singular solution $\xi$ of our equation such that

$$\tau\xi = c\xi, \quad c \in k_0$$

for every element $\tau$ of $G_0$. Since $G_0$ is normal in G, we have

$$\tau(\sigma\xi) = c'\sigma\xi, \quad c' \in k_0$$

for every element $\sigma$ of G. Here, $\sigma\xi$ is linearly independent of $\xi$ over $k_0$, because G is not reducible to triangular form. Hence, $G_0$ is reducible to diagonal form. We shall suppose that there is no algebraic solution. Then G is not finite and $G_0$ does not consist of a single element, the identity. Since $G_0$ is an algebraic group, it consists of

$$\begin{pmatrix} a, & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad a \in k_0, \quad a \neq 0.$$

For every element $\sigma$ of G which is not contained in $G_0$ we have

$$\sigma\eta_1 = c_1\eta_2, \quad \sigma\eta_2 = c_2\eta_1, \quad c_1, c_2 \in k_0.$$

Therefore, $[G : G_0] = 2$. This is due to I. Kaplansky[13, §19].

## §13. Liouville's lemma.

We shall suppose that $k = \mathbb{C}(x)$ with $x' = 1$ and consider a homogeneous linear differential equation of the second order over k:

$$\frac{d^2y}{dx^2} + p(x)\frac{dy}{dx} + q(x)y = 0, \quad p, q \in \mathbb{C}(x).$$

If we set $Y = y/\sqrt{W}$ with the wronskian W then it satisfies

$$Y'' + (s/2)Y = 0, \quad s = -p' + 2q - p^2/2$$

by $W' = -pW$. The logarithmic derivative $v = Y'/Y$ of Y is a solution of the Riccati equation:

$$v' + v^2 = -s/2.$$

Let us assume that our equation is irreducible over k and that it has a non-trivial solution in a liouvillian extension of k. Then there is a Picard-Vessiot extension $\Sigma$ of k for y which is contained in a liouvillian extension of k. The extension $\Sigma(\sqrt{W})$ contains a Picard-Vessiot extension $\Sigma'$ of k for Y. Let G' be the group of all automorphisms of $\Sigma'$ over k and $G'_0$ be the component of the identity in G'. In our hypergeometric case if Y is algebraic then $\lambda$ and $\mu$ are rational numbers, and W is algebraic: Hence, G' is finite if and only if G is finite. We shall assume that $\Sigma'$ is not an algebraic extension of k. Then $[G' : G'_0] = 2$ and there is a solution Y such that $\tau Y/Y$ is a constant for every automorphism $\tau$ in $G'_0$. Its logarithmic derivative v is left invariant under $\tau$ and it satisfies a quadratic equation over k:

$$v^2 + av + b = 0, \quad a, b \in \mathbb{C}(x).$$

The coefficients a and b satisfy

$$a' = a^2 + s - 2b, \quad b' = a(b + s/2)$$

because of $v' + v^2 = -s/2$. As the compatibility condition we have

$$a'' = 3aa' + s' - 2as - a^3,$$

which is due to I. Kaplansky[13, §25]. For Liouville's original treatment confer Watson[39, Chap.IV]. Due to him we obtain the following lemma:

The coefficient a is the half of the logarithmic derivative of the discriminant D of the quadratic equation for v.

For, we have

$$\begin{aligned} D' &= (a^2 - 4b)' = 2aa' - 4b' \\ &= 2a(a^2 + s - 2b) - 4a(b + s/2) \\ &= 2a(a^2 - 4b) = 2aD. \end{aligned}$$

Return to our hypergeometric differential equation, which will be assumed to be irreducible over k. Suppose that $\lambda$ and $\mu$ are equal to 1/2. Then a fundamental system of solutions is given by

$$y_1 = e^{i\nu t}, \quad y_2 = e^{-i\nu t}, \quad i = \sqrt{-1}, \quad x = \sin^2 t,$$

which lie in a liouvillian extension of k because

$$\left(\frac{dx}{dt}\right)^2 = 4x(1 - x).$$

Here, the problem on the field of constants can be solved by Kolchin's existence theorem in the previous section. If two of $\lambda$, $\mu$ and $\nu$ are half integers then our equation has a solution

in a liouvillian extension of k by Gauss' transformations. It is algebraic if and only if the remained one of $\lambda$, $\mu$ and $\nu$ is a rational number. We shall prove that this is the only case where our equation has a transcendental liouvillian solution under the assumption that neither $\lambda$, $\mu$ nor $\nu$ is a rational integer.

Let us express the coefficient a of v in the sum of partial fractions:

$$a = \sum_{i=0}^{n+1} \frac{e_i}{x - c_i}, \quad c_0 = 0, \quad c_1 = 1, \quad c_i \in \mathbb{C},$$

where $e_i$ is either an integer or a half integer. Then we have

$$a' = \sum \frac{-e_i}{(x - c_i)^2}, \quad a'' = \sum \frac{2e_i}{(x - c_i)^3}.$$

Comparing the coefficients of $(x - c_i)^{-3}$ in the compatibility condition we get

$$2e_i = -3e_i^2 - e_i^3, \quad i \neq 0, 1.$$

Hence,

$$e_i = -1, -2, \quad i \neq 0, 1.$$

Comparing those of $x^{-3}$ and $(x - 1)^{-3}$ we obtain

$$2e_0 = -3e_0^2 - 2P - 2Pe_0 - e_0^3, \quad P = \frac{1}{2}(1 - \lambda^2)$$

and

$$2e_1 = -3e_1^2 - 2Q - 2Qe_1 - e_1^3, \quad Q = \frac{1}{2}(1 - \mu^2).$$

Hence,

$$e_0 = -1, -1 \pm \lambda, \quad e_1 = -1, -1 \pm \mu.$$

Let us multiply each term in our equation by $x^3$:

$$x^3a'' = \sum \frac{2e_i x^3}{(x - c_i)^3}, \qquad (xa)^3 = (\sum \frac{e_i x}{x - c_i})^3,$$

$$xax^2a' = (\sum \frac{e_i x}{x - c_i})(\sum \frac{-e_i x^2}{(x - c_i)^2}),$$

$$x^3s' = -2P - \frac{2Qx^3}{(x - 1)^3} + \frac{R(2x - 1)x}{(x - 1)^2},$$

$$xax^2s = (\sum \frac{e_i x}{x - c_i})[P + \frac{Qx^2}{(x - 1)^2} + \frac{Rx}{1 - x}],$$

where

$$R = \tfrac{1}{2}(1 + \nu^2 - \lambda^2 - \mu^2).$$

For $x = \infty$ we have

$$2X = -3X^2 - 2S - 2SX - X^3, \qquad S = P + Q - R,$$

where

$$X = \sum_{i=0}^{n+1} e_i.$$

Hence,

$$X = -1, \ -1 \pm \nu,$$

because $S = \frac{1}{2}(1 - \nu^2)$. If each of $e_0$ and $e_1$ is equal to -1, then X is a negative integer less than -1. Hence, $X = -1 \pm \nu$ and $\nu$ is an integer. If $e_0 = -1 \pm \lambda$ then $\lambda$ is either an integer or a half integer, since $2e_0$ is an integer by our lemma. Suppose that $\lambda$ is a half integer. Then, if $e_1 = -1$, X is a half integer and $\nu$ is a half integer. If $e_1 \neq -1$ then $\nu$ is either an integer or a half integer. As the last case let us assume

that $e_0 = -1$ and $e_1 = -1 \pm \mu$. Then $\mu$ is either an integer or a half integer. If $\mu$ is a half integer, then $\nu$ is a half integer.

This proof is due to M. Setoyanagi[36].

## §14. Kuga's theorem.

Consider a homogeneous linear differential equation over k. Take a simply connected domain U in the complex plane which does not contain any singular point of our equation. Then the differential field generated by a fundamental system of solutions and x over U is a Picard-Vessiot extension of k for our equation. It has an isomorphic image $\Xi$ over k in $\Omega$ and there is a regular matrix $\rho$ over the field of constants such that the group H of all automorphisms of $\Xi$ over k is equal to $\rho^{-1}G\rho$. We shall prove that the Zariski closure of the monodromy group is equal to H if our equation is Fuchsian. It is sufficient to show that an element f(x) of $\Xi$ which is returned to itself by every analytic continuation around the singular points is a rational function of x. Suppose that x = 0 is a singular point. Then f(x) takes the form f = u/v such that u and v are expressed in the form:

$$\sum_{h=1}^{m}\sum_{j=1}^{m'} \phi_{hj}(x)x^{\alpha_h}(\log x)^{\beta_j}, \quad \alpha_h \in \mathbb{C}$$

at the origin, where $\phi_{hj}(x)$ is holomorphic at 0 and $\phi_{hj}(0) \neq 0$ and $\beta_j$ is a non-negative integer. If $\sigma$ denotes the automorphism of $\Xi$ over k induced from the analytic continuation around the origin then $\sigma^n u/\sigma^n v = f$ for every n. Let us suppose that v takes the above form. If $\alpha_h = a_h + ib_n$ with real numbers $a_h$ and $b_h$ then we can suppose that

$$a_1 = \cdot \cdots \cdot = a_\ell < a_h, \quad h > \ell.$$

We may assume that we are in one of the following three cases:

(i) $b_1 > 0, \quad b_h < b_1, \quad 2 \leq h \leq \ell$:

(ii) $b_1 < 0, \quad b_h > b_1, \quad 2 \leq h \leq \ell$:

(iii) $b_1 = 0, \quad \ell = 1$.

We may suppose that $\beta_1 > \beta_j$, $2 \leq j \leq n$. Let us set

$$v(x) = x^{a_1}(\log x)^{\beta_1}[g_1(x) + g_2(x)],$$

where $g_1(x)$ is the sum of the terms with $1 \leq h \leq \ell$, $j = 1$ and $g_2(x)$ is the sum of the other terms. If the absolute value of the argument x is not greater than $\pi$ then we have

$$\lim_{x \to 0} \sigma^n g_2(x) = 0$$

for every n. Let us set

$$g_1(x) = \sum_{h=1}^{\ell} \phi_{h1}(0) x^{ib_h} + g_3(x).$$

Then under the above condition we get

$$\lim_{x \to 0} \sigma^n g_3(x) = 0$$

for every n. If we set

$$L(x) = \left| \sum_{h=1}^{\ell} \phi_{h1}(0) x^{ib_h} \right|,$$

then we obtain

$$L(x) \geq [|\phi_{11}(0)| - \sum_{h=2}^{\ell} |\phi_{h1}(0)| \, e^{(b_1 - b_h)\arg x}] \, e^{-b_1 \arg x}.$$

In the first case (i) we have $L(x) \to \infty$ if $\arg x \to -\infty$: In the second case (ii), $L(x) \to \infty$ if $\arg x \to +\infty$: In the third case

(iii), $L(x) = |\phi_{11}(0)| > 0$. Hence, there is an integer n which may be negative such that

$$\lim_{x\to 0} x^N \sigma^n u(x)/\sigma^n v(x) = 0$$

for a sufficiently great number N under the condition that the absolute value of arg x is not greater than $\pi$. Therefore, the origin is not an essential singular point of f(x). Thus, f(x) is a rational function of x. This theorem is due to M. Kuga [24, p.173], where a sketch of the proof is given. The condition that our equation be Fuchsian can not be removed. For instance, Bessel's equation

$$x^2y'' + xy' + (x^2 - \lambda^2)y = 0, \quad \lambda \in \mathbb{C}$$

gives a counter example.

Return to our hypergeometric differential equation. By this theorem we shall prove that two of $\lambda$, $\mu$ and $\nu$ are half integer if our equation has a transcendental liouvillian solution under the assumption that it is irreducible over k and there is no logarithmic singular point. Since it is irreducible, there is a logarithmic singular point if and only if one of $\lambda$, $\mu$ and $\nu$ is a rational integer. Let $\sigma_0$, $\sigma_1$ and $\sigma_\infty$ denote the automorphism of $\Xi$ which is induced from analytic continuation around 0, 1 and $\infty$ respectively; here $\Xi$ is a Picard-Vessiot extension of k for Y over a complex domain and

$$\sqrt{W} = cx^{(\lambda-1)/2}(x - 1)^{(\mu-1)/2}, \quad c\ (\neq 0) \in \mathbb{C}.$$

Then the component $H_0$ of the identity e in H can not contain

all of $\sigma_0$, $\sigma_1$ and $\sigma_\infty$, since they generate our monodromy group by van Kampen's theorem (cf. for instance A. Komatsu, M. Nakaoka and M. Sugawara[23, p.293]). They satisfy $\sigma_0\sigma_1\sigma_\infty = e$, and $H_0$ contains one and only one of them. Suppose that neither $\sigma_0$ nor $\sigma_1$ is contained in $H_0$. Then there is a fundamental system of solutions of $Y'' + (s/2)Y = 0$ such that

$$\sigma_0 = \begin{pmatrix} -e^{\lambda\pi i} & A \\ 0 & -e^{-\lambda\pi i} \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} -e^{\mu\pi i} & 0 \\ B & -e^{-\mu\pi i} \end{pmatrix};$$

here $AB \neq 0$ because of the irreducibility. Each of $\sigma_0^2$ and $\sigma_0\sigma_1$ $(= \sigma_\infty^{-1})$ is contained in $H_0$ which is reducible to diagonal form; here

$$\sigma_0^2 = \begin{pmatrix} e^{2\lambda\pi i} & -A(e^{\lambda\pi i} + e^{-\lambda\pi i}) \\ 0 & e^{-2\lambda\pi i} \end{pmatrix},$$

$$\sigma_0\sigma_1 = \begin{pmatrix} e^{(\lambda+\mu)\pi i} + AB & -Ae^{-\mu\pi i} \\ -Be^{-\lambda\pi i} & e^{-(\lambda+\mu)\pi i} \end{pmatrix}.$$

If the eigenvalues of $\sigma_0^2$ are distinct, that is $e^{2\lambda\pi i} \neq e^{-2\lambda\pi i}$, then we have $-Be^{-\lambda\pi i} = 0$, which contradicts our assumption. Hence, $\lambda$ is either an integer or a half integer, and similarly $\mu$ is either an integer or a half integer. This proof is due to T. Kimura[15].

We shall note that there is no transcendental liouvillian solution if our equation has a logarithmic singularity under the assumption that it is irreducible. There is no algebraic solution. Suppose that $x = 0$ is a logarithmic singular point. Then

there is a fundamental system of solutions $Y_1$, $Y_2$ such that $\sigma_0^2 Y_i / Y_i$ is a constant for each i. This contradicts our assumption that x = 0 is a logarithmic singular point. Our statement holds for an equation which is not Fuchsian.

## Note. Bessel's equation.

Consider Bessel's equation:

$$x^2 \frac{d^2y}{dx^2} + x \frac{dy}{dx} + (x^2 - \nu^2)y = 0, \quad \nu \in \mathbb{C}.$$

A solution is given by Bessel's function:

$$J_\nu(x) = \sum_{k=0}^{\infty} (-1)^k \frac{1}{\Gamma(k+1)\Gamma(n+k+1)} \left(\frac{x}{2}\right)^{n+2k}$$

unless $\nu$ is a negative integer. If $\nu$ is not an integer a fundamental system of solutions is given by $J_\nu(x)$ and $J_{-\nu}(x)$. For $\nu = 0$ we have a solution of the form:

$$J_0(x) \cdot \log x + \sum_{k=1}^{\infty} (-1)^{k-1} \frac{1}{(k!)^2} \left(1 + \frac{1}{2} + \cdots + \frac{1}{k}\right) \left(\frac{x}{2}\right)^{2k}.$$

If $\nu$ is a positive integer n then by the recurrence formula:

$$y_{n+1}(x) = \frac{n}{x} y_n(x) - \frac{dy_n}{dx}$$

we have a solution of the form:

$$J_n(x) \cdot \log x + \Phi_n(x),$$

where $\Phi_n(x)$ is defined inductively by

$$\Phi_{n+1}(x) = \frac{1}{x}[n\Phi_n(x) - J_n(x)] - \frac{d\Phi_n}{dx}.$$

Thus a logarithmic singularity appears if and only if $\nu$ is an integer. Let us set $Y = \sqrt{x}y$. Then we have

$$\frac{d^2Y}{dx^2} + \left[1 - \frac{1}{x^2}\left(\nu^2 - \frac{1}{4}\right)\right]Y = 0.$$

The logarithmic derivative $V = Y'/Y$ satisfies

$$\frac{dV}{dx} + V^2 + 1 - \frac{1}{x^2}\left(\nu^2 - \frac{1}{4}\right) = 0.$$

If we set

$$Y = P(t)e^{ix}, \quad t = x^{-1}, \quad i = \sqrt{-1}$$

then we get

$$t^2 \frac{d^2P}{dt^2} + (2t - 2i)\frac{dP}{dt} + (\frac{1}{4} - \nu^2)P = 0.$$

The coefficient $c_k$ of $P(t) = \sum_{k=0}^{\infty} c_k t^k$ is determined by

$$2ikc_k = (k - \frac{1}{2} + \nu)(k - \frac{1}{2} - \nu)c_{k-1}.$$

Hence, $P(t)$ is a polynomial of $t$ if and only if $\nu$ is a half integer. In this case $V$ is a rational function of $x$ and our equation is reducible. Conversely let us suppose that $V$ is a rational function of $x$. Then it takes the form:

$$V(x) = e_\infty + \sum_{j=0}^{n} \frac{e_j}{x - c_j}, \quad c_0 = 0, \quad c_j \in \mathbb{C}$$

and we have

$$e_\infty^2 = -1, \quad e_j = 1, \quad j \neq 0, \quad e_0 = \frac{1}{2} \pm \nu.$$

Let us multiply each term in Riccati's equation for $V$ by $x^2$ and set $x = \infty$. Then we obtain

$$e_\infty \sum_{j=0}^{n} e_j = 0$$

and hence

$$n + \frac{1}{2} \pm \nu = 0.$$

Therefore, $\nu$ is a half integer if our equation is reducible. We shall show that there is no algebraic solution. First suppose that $\nu$ is a half integer. Then every solution is expressed

in the form

$$Y(x) = f(x)e^{ix} + g(x)e^{-ix}, \quad f, g \in \mathbb{C}(x).$$

If $Y(x)$ would be algebraic then $e^{ix}$ would be so. It is impossible, since $e^{ix}$ is a transcendental function of $x$. Secondly suppose that $\nu$ is not a half integer. Then if our equation would have an algebraic solution $J_\nu(x)J_{-\nu}(x)$ would be an algebraic function of $x$, since our equation is irreducible over $\mathbb{C}(x)$. However, it is impossible because this function is an integral one which is not a polynomial. We shall prove that $\nu$ is a half integer if our equation has a liouvillian solution. There is a rational function $a(x)$ which satisfies the differential equation:

$$a'' = 3aa' + s' - 2as - a^3,$$

where

$$s = 2 - \frac{1}{x^2}(2\nu^2 - \frac{1}{2}).$$

It takes the form

$$a = \sum_{j=0}^{n} \frac{e_j}{x - c_j}, \quad c_0 = 0, \quad c_j \in \mathbb{C}.$$

Here, we have

$$e_j = -1, -2, \quad j \neq 0, \quad e_0 = -1, -1 \pm 2\nu.$$

Let us multiply each term in our differential equation for $a$ by $x$ and set $x = \infty$. Then we obtain

$$-4 \sum_{j=0}^{n} e_j = 0$$

and hence

$$- 1 \pm 2\nu + \sum_{j=1}^{n} e_j = 0,$$

because $e_0$ can not be equal to -1. Therefore, $\nu$ is either an integer or a half integer. The former is impossible, since a logarithmic singularity appears in this case. This epoch-making theorem is due to Liouville[29], [30], [31].

Michihiko Matsuda
Department of Mathematics
Kyoto Sangyo University
Kamigamo, Kyoto 603, Japan

Bibliography.

(The numbers in brackets indicate the pages where it is referred).


1. F. Baldassarri and B. Dwork, On second order linear differential equations with algebraic solutions, Amer. J. Math., 101(1979), 42-76. [iii].
2. L. Bieberbach, Lehrbuch der Funktionentheorie, Band I, 3te Auf., Teubner, Leipzig, 1930. [17].
3. F. Brioschi, La théorie des formes dans l'intégration des équations différentielles linéaires du second ordre, Math. Ann. 11(1877), 401-411. [ii, 62].
4. A. Errera, Zahlentheoretische Lösung einer functionentheoretischen Frage, Rend. Circ. Matem. Palermo, 35(1913), 107-144. [ii, 66, 68, 80].
5. A. R. Forsyth, Theory of differential equations, Part III, Ordinary linear equations, Cambridge Univ. Press, London, 1902. [52].
6. P. Gordan, Ueber die Auflösung der Gleichungen vom fünften Grade, Math. Ann. 13(1878), 375-404. [63].
7. E. Goursat, Sur les intégrales rationnelles de l'équation de Kummer, Math. Ann. 24(1884), 445-460. [iii].
8. ————————, Recherches sur l'équation de Kummer, Acta Soc. Sci. Fennicae 15(1888), 47-127. [iii].
9. ————————, Leçons sur les séries hypergéometriques et sur quelques fonctions qui s'y rattachent I, II, Hermann, Paris, 1936, 1938. [ii, 4, 12, 17].

10. T. Honda, Algebraic differential equations, Dept. Math. Tokyo Univ. Seminar Notes no.38, Tokyo, 1977 (in Japanese). [iii, 43].

11. M. Hukuhara and S. Ōhasi, On Riemann's P-functions which are expressible in terms of elementary functions (in Japanese), Sûgaku, 2(1949-50), 227-230; 8(1956), 27-29. [iii].

12. K. Iwasawa, Theory of algebraic function fields (in Japanese), Iwanami, Tokyo, 1952. [48].

13. I. Kaplansky, An introduction to differential algebra, Hermann, Paris, 1957. [95, 97].

14. N.Katz, Algebraic solutions of differential equations (p-curvature and the Hodge filtration), Invent. Math. 18 (1972), 1-118. [iii].

15. T. Kimura, On Riemann's equations which are solvable by quadratures, Funkcialaj Ekvacioj, 12(1969), 269-281. [iii, 104].

16. F. Klein, Über [algebraisch integrierbare] lineare Differentialgleichungen, I, II, Math. Ann. 11(1877), 115-118, 12(1877), 167-179. [ii].

17. ————, Vorlesungen über das Ikosaeder, Teubner, Leipzig, 1884. [52].

18. ————, Vorlesungen über die hypergeometrische Funktion, Springer, Berlin, 1933. [iii].

19. E. R. Kolchin, Extensions of differential fields I, Ann. Math., 43(1942), 724-729. [92].

20. ———— , Algebraic matric groups and the Picard-Vessiot

theory of homogeneous linear ordinary differential equations, Ann. Math., 49(1948), 1-42. [92, 93].

21. E. R. Kolchin, Existence theorems connected with the Picard-Vessiot theory of homogeneous linear ordinary differential equations, Bull. Amer. Math. Soc., 54(1948), 927-932. [93].

22. ————, Galois theory of differential fields, Amer. J. Math. 75(1953), 753-824. [92].

23. A. Komatsu, M. Nakaoka and M. Sugawara, Topology. I (in Japanese), Iwanami, Tokyo, 1967. [104].

24. M. Kuga, Galois no Yume ("Galois' Dream", in Japanese) Nippon Hyoron-sha, Tokyo, 1968. [iii, 10, 103].

25. E. E. Kummer, Ueber die hypergeometrische Reihe. $1 + \frac{\alpha\cdot\beta}{1\cdot\gamma}x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot2\cdot\gamma(\gamma+1)}x^2 + \frac{\alpha(\alpha+1)(\alpha+2)\beta(\beta+1)(\beta+2)}{1\cdot2\cdot3\cdot\gamma(\gamma+1)(\gamma+2)}x^3 + \cdots$, J. Reine Angew. Math. 15(1836), 39-83, 127-172. [ii, 4, 51].

26. E. Landau, Eine Anwendung des Eisensteinschen Satzes auf die Theorie der Gaussschen Differentialgleichung, J. Reine Angew. Math. 127(1904), 92-102. [ii, 20, 28].

27. ————, Über einen zahlentheoretischen Satz und seine Anwendung auf die hypergeometrische Reihe, S.-B. Heidelberger Akad. Wiss. 18(1911), 3-38. [ii, 28, 30, 91].

28. ————, Handbuch der Lehre von der Verteilung der Primzahlen, 3rd Ed., Chelsea, New York, 1974. [26, 28].

29. J. Liouville, Mémoire sur la classification des transcendantes et sur l'impossibilité d'exprimer les racines de certaines équations en fonction finie explicite des coef-

ficients, J. Math. Pures Appl., 2(1837), 56-105; 3(1838), 523-547. [iii, 109].

30. J. Liouville, Mémoire sur l'intégration d'une classe d'équations différentielles du second ordre en quantetés finies explicites, J. Math. Pures Appl., 4(1839), 423-456.[iii, 109].

31. ————————, Remarques nouvelles sur l'équation de Riccati, J. Math. Pures Appl., 6(1841), 1-13. [iii, 109].

32. M. Matsuda, First order algebraic differential equations, A differential algebraic approach, Lecture Notes Math., 804, Springer, Berlin, 1980. [93].

33. H. Morikawa, Theory of invariants (in Japanese), Kinokuniya, Tokyo, 1977. [50].

34. J. F. Ritt, Differential algebra, Amer. Math. Soc. Colloq. Publ. Vol. 33, New York, 1950. [92].

35. H. A. Schwarz, Ueber diejenigen Fälle, in welchen die Gaussische hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt, J. Reine Angew. Math. 75(1873), 292-335. [ii, 7, 15, 18].

36. M. Setoyanagi, Note on transcendental liouvillian solutions of hypergeometric differential equations, preprint, to appear. [iii, 100].

37. T. Takagi, Elementary number theory (in Japanese), Kyoritsusha, Tokyo, 1931. [26].

38. ————————, Algebraic number theory (in Japanese), Iwanami, Tokyo, 1948. [44].

39. G. N. Watson, A treatise on the theory of Bessel functions, 2nd Ed., Cambridge, London, 1944. [97].

40. H. Weber, Lehrbuch der Algebra. II, Zweite Aufl., Druck und Verlag von Friedr, Vieweg & Sohn Akt.-Ges., Braunschweig, 1899. [17, 28, 44, 56, 63].

41. A. Weil, Foundations of algebraic geometry, Amer. Math. Soc. 2nd Ed., Providence, 1962. [49].

## LECTURES IN MATHEMATICS, KYOTO UNIVERSITY

| | | |
|---|---|---|
| No. 1 | Peterson, F. P.—Lectures in Cobordism Theory | $ 5.00 |
| No. 2 | Kubota, T.—On Automorphic Functions and the Reciprocity Law in a Number Field | $ 5.00 |
| No. 3 | Maruyama, M.—On Classification of Ruled Surfaces | $ 5.00 |
| No. 4 | Monsky, P.—p-adic Analysis and Zeta Functions | $ 7.00 |
| No. 5 | Nagata, M.—On Automorphism Group of k[x, y] | $ 5.00 |
| No. 6 | Araki, S.—Typical Formal Groups in Complex Cobordism and K-Theory | $ 5.00 |
| No. 7 | Shin'ya, H.—Spherical Functions and Spherical Matrix Functions on Locally Compacts Groups | $ 5.00 |
| No. 8 | Saito, H.—Automorphic forms and Algebraic Extensions of Number Fields | $ 7.00 |
| No. 9 | Tanaka, N.—A Differential Geometric Study on Strongly Pseudo-Convex Manifolds | $ 7.00 |
| No. 10 | Kambayashi, T. and Miyanishi, M.—On Forms of the Affine Line Over a Field | $ 7.00 |
| No. 11 | Stroock, W. D.—Lectures on Infinite Interacting Systems | $ 7.00 |
| No. 12 | Brauer, R.—Theory of Group Characters | $ 7.00 |
| No. 13 | Lê Dũng Tráng—Geometry of Tangents on Singular Spaces and Chern Classes | o/s |
| No. 14. | Hirai, T. and Schiffman G. (Eds.)—Lectures on Harmonic Analysis on Lie Groups and Related Topics | $ 23.00 |

Printed by Tokyo Press Co., Ltd., Tokyo, Japan

Printed in Japan