The Galois or Rationality Group of a Linear Homogeneous Differential Equation.

1. Integration of Differential Equations in Finite Terms Containing Elementary Functions.

The solution of $y'' + y = 0$ is $y = c_1 \sin x + c_2 \cos x$. One solution of $y'' + (1 - \frac{1}{x^2})y = 0$ for $x > 0$ is $y = \sqrt{x}\, J_{\frac{\sqrt{5}}{2}}(x)$ and the general solution is then easily found.

An apparent difference between these two examples is that the solution of the first differential equation is expressed in terms of elementary functions, whereas the Bessel functions are usually regarded as not so elementary.

It is always possible to take any reasonable differential equation and to name and study its solutions. The general existence theorems assure the existence of a solution among the class of all differentiable functions. The question of interest in this course is to discover conditions which insure that the solutions of a differential equation can be expressed in finite terms relative to certain elementary functions.

The elementary functions are obtained from rational functions, algebraic functions, exponentials, and integrations. Because of identities such as

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i}$$

$$\arcsin x = -i \ln[ix + \sqrt{1-x^2}]$$

$$\ln x = \int \frac{dx}{x}$$

we can state that the additional processes of taking logarithms, trigonometric functions, and inverse trigonometric functions yield no new elementary functions.

The situation is quite analogous to the classical theory of polynomial equations in algebra. By the fundamental theorem of algebra every polynomial with complex coefficients has complex roots. In practice we would like to express these roots by formulas, as for the quadratic, cubic, and quartic, where only radicals and rational operations occur. But the general quintic is not solvable in terms of radicals. The solvability of a polynomial equation, with rational coefficients, in terms of radicals means that the roots can be obtained from the rational numbers by solving a succession of equations $x^n = a$, where a has been obtained by the preceding steps. The criterion for the solvability of a polynomial equation is expressed by the solvability of the Galois group of the equation.

We shall consider linear homogeneous differential equations with rational functions as coefficients. The solvability in terms of elementary functions turns out to mean that the solutions can be obtained from the rational functions by algebraic operations and solving a succession of first order differential equations $y' = a(x)$ and $y' = a(x) y$. We shall define the Galois group of the differential equation as a certain Lie group. The solvability of the differential equation in terms of elementary functions shall be determined by the solvability of the Galois group.

Every first order linear differential equation

$$y' + P(x)\, y = Q(x)$$

is solvable in elementary terms,

$$y = e^{-\int P dx}\left[\int Q(x)\, e^{\int P dx}\, dx + C\right].$$

But the general second order differential equation, and in particular Bessel's equation, is not solvable in elementary functions.

In considering an elementary function,

$$\int \arctan\left[\ln\sqrt{1+e^{2\sin(x^2+1)}}\right] dx - \ln\left[\ln \frac{x^2\cos x}{1+e^x}\right]$$

one is uncertain of the domain of definition, the branch, or even the meaning of the function. We shall usually mean any branch defined in an appropriately restricted domain. However we shall later avoid the problem by dealing with the theory of differential polynomials in a purely algebraic manner. Then the question of the interpretation in the case of meromorphic or rational coefficients can be studied separately.

Thus we shall be led to the theory of differential algebra. As an important application of this theory we shall study the concept of the general and singular solutions of a non-linear differential equation.

2. Differential Field Extensions and Liouville Elementary Functions.

Definition. A differential field is an algebraic field F, of characteristic zero, together with a derivation $f \to f'$ satisfying

1.) $(f+g)' = f' + g'$

2.) $(fg)' = f'g + fg'$.

Differential isomorphisms and automorphisms are defined to commute with differentiation.

Definition. Let F be a differential field. A subset $G \subset F$, which is a field and is such that the derivative of each element of G lies in G, is a differential subfield of F. We say that F is an extension of G. The subset of F consisting of elements with zero derivative is the differential subfield C of constants.

Remark. In any differential field F the set of all elements c with $c' = 0$ forms a differential subfield C which contains all the rational numbers in F.

For $(f+0)' = f' + 0'$ so $0' \in C$, and $(1 \cdot f)' = 1' \cdot f + 1 \cdot f'$ so $1' \cdot f = 0$ and (if $f \neq 0$) $1' = 0$ so $1 \in C$.

Example. The set $\mathbb{C}(z)$ of all rational functions of one complex variable z, with complex coefficients, is a differential field with the usual differentiation. The constants of the differential field are the complex numbers.

Definition. Let F be a differential field. A differential field F_1 is called a finite algebraic extension of F in case:

1. F_1 is an extension of the differential field F and
$$F_1 = F(v) .$$

2. There exists a polynomial $p(x)$, irreducible over F such that
$$p(v) = 0 \quad \text{in } F_1 .$$

Note. Every finite algebraic extension of the algebraic field F can be generated by a single element V satisfying an irreducible polynomial equation over F. It is easy to see that $F(V)$ might contain more constants than F.

Theorem 1. Let F be a differential field and let $p(x)$ be an irreducible polynomial over F. Then there exists a finite algebraic extension $F_1 = F(v_1)$ of the differential field F with $p(v_1) = 0$. Furthermore if $F_2 = F(v_2)$ is another such extension of F then there exists a differential isomorphism of F_2 onto F_1 with $v_2 \rightarrow v_1$ and $F \rightarrow F$ elementwise.

Proof.

Consider the algebraic field $F_1 = F(v_1)$ generated by a root v_1 of $p(x)$. Define the derivation on F_1 by
$$v_1' = -\frac{a_n' v^n + a_{n-1}' v^{n-1} + \cdots + a_0'}{a_n n v^{n-1} + \cdots + a_1}$$

where $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_n \neq 0$. Note that $p'(v) = a_n n v^{n-1} + a_{n-1}(n-1)v^{n-2} + \cdots + a_1 \neq 0$ since $p(x)$ is irreducible and hence separable. Then F_1 is the required differential field extension of F .

If $F_2 = F(v_2)$ is another finite algebraic extension of F by a root v_2 of $p(x)$, then there is an algebraic isomorphism of F_2 onto F_1 with $v_2 \longrightarrow v_1$ and $F \longrightarrow F$ elementwise. But this is also a differential isomorphism. Q. E. D.

<u>Theorem 2.</u> Let F be a differential field with a constant field K which is algebraically closed. Let $F_1 = F(v_1)$ be the differential field extension of F for a root v_1 of a polynomial $p(x)$ irreducible over F . Then the constant field K_1 of F_1 is the same as K .

<u>Proof.</u>

Let $u \in F_1$ be a constant and let the minimal polynomial for u over F be $q(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$, $m \leq n$. Then

$$u^m + b_{m-1}u^{m-1} + \cdots + b_0 = 0 .$$

Differentiate and use $u' = 0$ to get $b'_{m-1}u^{m-1} + \cdots + b'_0 = 0$. Thus $b'_{m-1} = 0$, $b'_{m-2} = 0, \ldots, b'_0 = 0$ and $b_{m-1}, \ldots, b_0$ are in K . Thus u is algebraic over K and so $u \in K$.

Q. E. D.

<u>Example.</u> Let $F = \mathbb{C}(z)$, the rational functions of one complex variable, with complex coefficients. Let $p(x) = (1 - z^2)x^2 - 1$, irreducible over F . Then the algebraic function $v(z) = \frac{1}{\sqrt{1-z^2}}$ generates the differential field $F_1 = \mathbb{C}(z, \frac{1}{\sqrt{1-z^2}})$. The functions in F_1 are of the form

$$\frac{a_1(z)\, v(z) + a_2(z)}{a_3(z)\, v(z) + a_4(z)}$$

with $a_1(z), a_2(z), a_3(z), a_4(z)$ in F. By the algebraic function $\frac{1}{\sqrt{1-z^2}}$ we mean the totality of all holomorphic power series which can be obtained by analytic continuation from one power series element $P(z)$ which satisfies $p(P(z)) \equiv 0$. The formula for $V'(z)$ is computed by implicit differentiation of $(1-z^2)V_1(z^2)-1 \equiv 0$.

Definition. Let F be a differential field. A differential field F_1 is called an extension of F by an integral in case:

1. F_1 is an extension of the differential field F and $F_1 = F(V)$.
2. $V' = a$ is in F and there is no element of F whose derivative is a.

Theorem 3. Let F be a differential field and let $a \in F$ be a non-derivative. Then the simple transcendental extension $F_1 = F(V_1)$ is a differential field extension of F with $V_1' = a$. Furthermore if $F_2 = F(V_2)$ is another extension of F by an integral of a, then there exists a differential isomorphism of F_2 onto F_1 with $V_2 \rightarrow V_1$ and $F \rightarrow F$ elementwise.

Proof.

Let $F_1 = F(V_1)$ be the simple transcendental extension of F. Define $V_1' = a$ and then F_1 is an extension of the differential field by the integral of a.

Now let $F_2 = F(V_2)$ be another extension of F by an integral V_2 of a. If V_2 is algebraic over F it satisfies an irreducible polynomial equation, with coefficients in F,

$$V^n + bV^{n-1} + \cdots = 0 \quad , \quad n \geqslant 2 .$$

Differentiating we get an $(n-1)$ degree polynomial

$$nV^{n-1}a + b'V^{n-1} + b(n-1)V^{n-2}a + \cdots = 0$$

Hence α is the derivative of $-b/n$ in F, which is impossible. Thus F_2 is also a simple transcendental extension of F.

Hence $F(v_1)$ is algebraically isomorphic to $F(v_2)$ with $v_2 \to v_1$ and $F \to F$ elementwise. Since $v_1' = \alpha$ and $v_2' = \alpha$ we obtain a differential isomorphism of F_2 onto F_1, as required.

Q. E. D.

Theorem 4. Let F be a differential field and let $F_1 = F(v)$, where $v' = \alpha$, be an extension of F by an integral. Then the constant field K of F_1 is the same as K.

Proof.

Suppose $u = b_1 v^n + b_2 v^{n-1} + \cdots$, $b_1 \neq 0$, $n \geq 1$ is a constant in F_1. Differentiate to get $b_1' v^n + (n b_1 \alpha + b_2') v^{n-1} + \cdots = 0$. Since v is transcendental over F, $b_1' = 0$, $n b_1 \alpha + b_2' = 0$ and $\alpha = -(b_2/n b_1)$, which is impossible.

Next suppose $u = f(v)/g(v)$ is constant in F_1 where f/g is a rational function in lowest terms and g contains v and has a leading coefficient of 1. Then we compute $\frac{f}{g} = \frac{f'}{g'}$, from $u' = 0$, where g' is a non-zero polynomial of lower degree than g and $g'(v) \neq 0$. This contradicts the assumption that f/g is in lowest terms.

Q. E. D.

Example. Let $F = \mathbb{C}(z)$ be the rational functions of one complex variable, with complex coefficients. Take $\frac{1}{z}$, which is not a derivative in F, and form the extension by the integral of $\frac{1}{z}$, that is $F_1 = F(\ln z)$. Here the functions of F_1 are of the form

$$\frac{a_n(z)(\ln z)^n + \cdots + a_0(z)}{b_m(z)(\ln z)^m + \cdots + b_0(z)}$$

where the $a_0(z), \cdots, a_n(z), b_0(z), \cdots, b_m(z)$ are in F.

Next consider the irreducible equation $(1-z^2)x^2-1=0$ over F. This generates a finite algebraic extension F_2 of F_1. A typical element of F_2 is

$$\frac{\left(z^2+\frac{z}{\sqrt{1-z^2}}\right)(\ln z)^2+\sqrt{1-z^2}\,\ln z}{\frac{z^2}{1+z^{10}}(\ln z)^5+(z+1+\sqrt{1-z^2})}$$

Such a function means one branch, or one connected set of power series elements, which can be obtained by analytic continuation from a power series $P(z)$, using power series $P_1(z)$, $P_2(z)$ where

$$(1-z)^2[P_1(z)]^2-1\equiv 0$$

$$\frac{d}{dz}P_2(z)=\frac{1}{z}=1+(1-z)+(1-z)^2+\cdots$$

and

$$P(z)=\frac{\left(z^2+\frac{z}{P_1}\right)(P_2)^2+P_1P_2}{\frac{z^2}{1+z^{10}}(P_2)^5+(z+1+P_1)}$$

in some region of the complex plane.

Definition. Let F be a differential field. A differential field F_1 is called an extension by the exponential of an integral in case:

1.) F_1 is an extension of the differential field F and

$$F_1=F(v),\quad v\neq 0$$

2.) $v'=av$ for some $a\in F$, $a\neq 0$.

Note. If there is a non-zero $b\in F$ with $b'=ab$ and if $K_1=K$, then $F(v)=F$. For $\frac{v}{b}\in K_1=K$ and so $v\in K$.

Example. Let A be the algebraic numbers and consider the differential field $F=A(z,e^z)$. The equation $y'=\frac{1}{z}y$ has no non-zero solution in F . The extension $F_1 = F(e^{z/2})$ has no new constants, whereas $F_2 = F(\pi e^{z/2})$ has the new constant $\pi^2 = (\pi e^{z/2})^2/e^z$.

Example. Let R be the rational numbers and $F = R(z, e^z)$. Then $y' = \frac{1}{2}y$ has no non-zero solution in F . The extensions $F_1 = F(e^{z/2})$ and $F_1 = F(2^{1/2}e^{z/2})$ have the constant field R , yet they are not isomorphic over F .

Theorem 5. Let F be a differential field with an algebraically closed field of constants K . Take $a \in F$, $a \neq 0$. Then there exists an extension $F_1 = F(V_1)$ by an exponential of an integral a, $V_1' = aV_1$, such that the constant field K_1 of F_1 is K . Furthermore if $F_2 = F(V_2)$ is another extension of F by an exponential of an integral of a and $K_2 = K$, then there is a differential isomorphism of F_2 onto F_1 with $V_2 \to V_1 k_1$, $k_1 \in K$ and $F \to F$ elementwise.

Proof.

We first prove the existence of F_1 . Suppose the equation $y' = any$ has no non-zero solution in F for each $n = 1, 2, 3, \dots$. Then consider the simple transcendental extension $F_1 = F(V_1)$ and define $V_1' = aV$. It is easy to see that F_1 is a differential field extension of F . We must show that F_1 contains no constants other than K .

Let

$$u = P(V_1) = a_n V_1^n + a_{n-1} V_1^{n-1} + \dots + a_0 , \quad n \geq 1$$

be a constant. Then

$$(a_n' + a_n n a) V_1^n + (a_{n-1}' + a_{n-1}(n-1)a) V_1^{n-1} + \dots + (a_1' + a_1 a) V_1 + a_0' = 0$$

Since V_1 is transcendental

$$a_n = 0 , \ a_{n-1} = 0 , \ \dots , \ a_1 = 0 , \ a_0' = 0$$

Then $u \in K$ as required. Let $P(V_1)/Q(V_1)$ be a constant.

Here the rational function p/q is in lowest terms, and $q(v) = b_m v^m + \cdots + b_0$, $b_m \neq 0$. If $a_0 \neq 0$, take $a_0 = 1$. Then

$$q(v_1)[p(v_1)]' - p(v_1)[q(v_1)]' = 0 \quad \text{so}$$

$$\frac{p(v_1)}{q(v_1)} = \frac{p(v_1)'}{q(v_1)'} = \frac{(a_n' + a_n n a) v_1^n + \cdots + (a_1' + a_1 a) v}{(b_m' + b_m m a) v_1^m + \cdots + b_0'}$$

Then we compare the terms not containing v_1 to get $b_0' = 0$. But this contradicts the assumption that p/q is in lowest terms. Therefore the field of constants K_1 of F_1 is just K.

Next assume $y' = nay$ does have non-zero solutions in F for some $n = 1, 2, 3, \ldots$ and let N be the smallest such integer and let $Y \neq 0$ be a corresponding solution in F. If $N = 1$, then take $F_1 = F$ as the required extension. Consider $N > 1$.

Consider the finite algebraic extension $F_1 = F(v_1)$ of F generated by a root v_1 of the irreducible polynomial (or an irreducible factor) $X^N - Y$ (for $z = Y^{\frac{1}{n}}$ satisfies $z' = az$ which is impossible in F). Then $v_1^N = Y$ and $v_1' = a v_1$ as required. Now we must show that $F_1 = F(v_1)$ contains no new constants.

Suppose $c_\ell v_1^\ell + \cdots + c_1 v_1 + c_0$, $0 < \ell < N$, $c_\ell \neq 0$ is a constant. Then $(c_\ell' + c_\ell \ell a) v_1^\ell + \cdots + (c_1' + c_1 a) v_1 + c_0' = 0.$ Then $c_\ell' = -\ell a c_\ell$ and $(c_\ell^{-1})' = \ell a (c_\ell^{-1})$ with $\ell < N$. This is impossible so $K_1 = K$.

Next we prove the uniqueness of the required extension. Suppose $F_1 = F(v_1)$ and $F_2 = F(v_2)$ are extensions of F by the exponential of an integral of a, as stated in the theorem. If both v_1 and v_2 are transcendental over F, then we have the required differential isomorphism of F_2 onto F_1 with $v_2 \rightarrow v_1$ and $F \rightarrow F$ elementwise.

Suppose v_1 is algebraic over F and v_2 is transcendental, or is algebraic with a degree not less than that of v_1. Write the minimal polynomial for V_1 over F as $p(V_1) = V_1^n + a_{n-1}V_1^{n-1} + \cdots + a_0 = 0$, $n \geqslant 0$. If $V_1 \in F$, then V_2/V_1 is a constant in $K_2 = K$ and hence $V_2 \in F$ and the uniqueness is obtained. Hence take $n \geqslant 1$.

Compute

$$naV_1^n + (a_{n-1}' + (n-1)a_{n-1}a)V_1^{n-1} + \cdots + (a_1' + a_1 a)V_1 + a_0' = 0$$

Thus $$n a a_{n-1} = a_{n-1}' + (n-1)a_{n-1}a \quad \text{or} \quad a_{n-1}' = a a_{n-1}$$
$$\vdots$$
$$n a a_0 = a_0'$$

Thus $[p(V_1)]' = na[p(V_1)]$ and $[p(V_2)]' = na[p(V_2)]$.

Thus $p(V_2)/V_2^n = k$ is in $K_2 = K$.

Thus

$$(1-k)V_2^n + a_{n-1}V_2^{n-1} + \cdots + a_1 V_2 + a_0 = 0,$$

and V_2 is algebraic of degree n over F.

We can assume that n is the smallest positive integer for which $y' = nay$ has a non-zero solution in F. Then $a_{n-1} = 0, \ldots, a_1 = 0$ so $p(V_1) = V_1^n + a_0 = 0$ and $(1-k)V_2^n + a_0 = 0$, $k \neq 1$. Thus the irreducible polynomial for $(1-k)^{1/n}V_2$ is just $p(x)$.

Therefore there exists a differential isomorphism of $F(V_2)$ onto $F(V_1)$ with $(1-k)^{1/n}V_2 \rightarrow V_1$ and $F \rightarrow F$ elementwise.

Q. E. D.

Definition. Let F be a differential field and L a differential field extension. We say that L is a generalized Liouville extension of F in case there exists a finite chain of intermediate differential fields

$$F \subset F_1 \subset F_2 \subset \cdots \subset F_m \subset L.$$

Each differential field is either a finite algebraic extension, the adjuction of an integral, or the adjuction of the exponential of an integral, of the preceding differential field of the chain.

Remark. We shall usually take the fields L and F to have the same constant field, which is algebraically closed.

Definition. A Liouville elementary function is the complete analytic continuation of a power series element, which lies in a differential field L of quotients of power series elements, where L is a generalized Liouville extension of the rational function field $\mathbb{C}(z)$, restricted to some subdomain of the complex plane.

Remark. Liouville began with rational functions in $\mathbb{C}(z)$, and chose an algebraic function, and formed the corresponding field F_1. Then he constructed either an integral or an exponential of a function in F_1 to obtain the field F_2. Again make an algebraic extension of F_2 to F_3 and then construct either an integral or an exponential of a function in F_3. Proceed a finite number of steps and obtain the class of elementary functions. The class of functions obtained by Liouville agrees with the class specified in our definition since $e^{\int a'} = e^{a}$, and, using the identity function as an algebraic function, there is no significance to the order of the steps indicated in the classical procedure of Liouville.

Definition. Let $\xi_1(z_1,\ldots,z_n),\ldots,\xi_p(z_1,\ldots,z_n)$ be p holomorphic functions of n complex variables in a region R of $\mathbb{C}^n$. Consider the function field $F = \mathbb{C}(\xi_1,\ldots,\xi_p)$ of quotients of holomorphic functions of $\mathbb{C}^n$. Let $u(z_1,\ldots,z_n)$be holomorphic in a subregion of R' and there $u(z_1,\ldots,z_n)$ is algebraic over $F_{R'}$. That is,

$$C_m u(z)^m + C_{m-1} u(z)^{m-1} + \cdots + C_1 u(z) + C_0 \equiv 0$$

where each C_j is a polynomial in $\xi_1,\ldots,\xi_p$ with complex coefficients. Then $u(z_1,\ldots,z_n)$, and its total analytic continuation, is called an algebraic combination of the functions $\xi_1,\ldots,\xi_p$.

If $\xi_1(z_1, \ldots, z_n), \ldots, \xi_p(z_1, \ldots, z_n)$ are rational functions of $z_1, \ldots, z_n$, then $u(z_1, \ldots, z_n)$ is an algebraic function of n complex variables.

Remark. If $u(z_1, \ldots, z_n)$ and $v(z_1, \ldots, z_n)$ are holomorphic in a region $R \subset \mathbb{C}^n$ and both are algebraic functions, then each rational function of u, v with complex coefficients is also algebraic. Also the partial derivatives of an algebraic function are algebraic functions — which follows from our theory of differential field extensions.

3. Transcendental and Hypertranscendental Field Extensions. Hölder's Theorem on the Γ Function.

Let $F_1 \supset F$ be fields (in the ordinary sense of algebra). If an element $v \in F_1$ satisfies a polynomial equation over F (with coefficients in F), then v is algebraic over F. If each element of F_1 is algebraic over F, then F_1 is called algebraic over F; otherwise F_1 is transcendental over F.

Definition. A finite set $v_1, v_2, \ldots, v_n$ of elements of a field $F_1 \supset F$ is called algebraically independent over F in case: if a polynomial P in n variables and with coefficients in F is such that

$$P(v_1, v_2, \ldots, v_n) = 0$$

then P is trivial (has all zero coefficients). An infinite set of elements of F_1 is called algebraically independent in case each finite subset is algebraically independent over F. If a set of elements of F_1 is not algebraically independent over F, it is algebraically dependent.

Definition. Consider fields $F_1 \supset F$. A set Σ of elements of F_1 forms a transcendence basis for F_1 over F in case Σ is algebraically independent over F and furthermore F_1 is an algebraic extension of $F(\Sigma)$.

<u>Theorem 6.</u> Consider fields $F_1 \supset F$. Then there exists a transcendence basis for F_1 over F. Moreover each two such transcendence bases have the same cardinality, the transcendence degree of F_1 over F.

<u>Proof.</u>

If F_1 is algebraic over F take the empty set of F as a transcendence basis and the transcendence degree of F_1 over F is zero. Now assume that F_1 contains at least one element V_1 transcendental over F. Consider all the subsets $\{\Sigma_\alpha\}$ of F_1 which are algebraically independent over F. Such subsets $\{\Sigma_\alpha\}$ of F_1 are partially ordered by inclusion and select a maximal set Σ (which is contained in no larger algebraically independent set). By Zorn's lemma we find Σ as the union of the sets comprising a maximal linearly ordered set $\Sigma_{\alpha_\lambda} \subset \Sigma_{\alpha_\mu} \subset \cdots$. Clearly Σ is algebraically independent over F.

Suppose there is an element $V \in F_1$ which is transcendental over $F(\Sigma)$. Then the set $\Sigma + V$ is algebraically independent over F, which is impossible. Thus Σ is a transcendence basis for F_1 over F.

Now let Σ_1 be another transcendence basis of F_1 over F and suppose $\operatorname{card}\Sigma_1 \neq \operatorname{card}\Sigma$. We consider here only the case $\operatorname{card}\Sigma = n$ is finite. Then $\Sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ algebraically spans F_1. Suppose $\Sigma_1 = (u_1, u_2, \ldots)$ has cardinality $\geqslant n$. Then select algebraically independent elements $(u_1, u_2, \ldots, u_m)$. We shall show that $m \leqslant n$, which proves the theorem. We shall show that a spanning set cannot have cardinal smaller than that of a finite independent set. Now $(u_1, \sigma_1, \sigma_2, \ldots, \sigma_n)$ spans F_1 but is algebraically dependent over F, and some σ_i is algebraically dependent on u_1 and the preceding σ's. Delete this σ_i. Continue in this way (cf. Van der Waerden) to obtain a spanning set $(u_1, u_2, \cdots, u_m, \sigma_\ell, \cdots, \sigma_n)$ with cardinality $n \geqslant m$.

Q. E. D.

<u>Theorem 7.</u> Consider fields $F_1 \supset F$ with transcendence degree D. A set $\Sigma' \subset F_1$ of elements, algebraically independent over F, has $\mathrm{card}\,\Sigma' \leq D$ and Σ' can be extended to a transcendence basis. Also a set $\Sigma'' \subset F_1$ such that F_1 is algebraic over $F(\Sigma'')$ has $\mathrm{card}\,\Sigma'' \geqslant D$ and Σ'' contains a transcendence basis of F_1 over F.

<u>Proof.</u>

Take $\Sigma' \subset F_1$ and extend it to a maximal set $\bar{\Sigma}$ of algebraically independent elements. Then F_1 is algebraic over $F(\bar{\Sigma})$ and hence $\bar{\Sigma}$ is a transcendence basis with $\mathrm{card}\,\Sigma' \leq \mathrm{card}\,\bar{\Sigma} = D$.

On the other hand assume F_1 is algebraic over $F(\Sigma'')$. If $F(\Sigma'')$ is algebraic over F, then F_1 is algebraic over F and $D = 0$ and the transcendence basis is the empty subset of Σ''. Assume Σ'' contains elements which are transcendental over F. Take a maximal algebraically independent subset $\hat{\Sigma}$ of Σ''. But $F(\Sigma'')$ is algebraic over $F(\hat{\Sigma})$ and hence F_1 is algebraic over F. Thus $\hat{\Sigma}$ is a transcendence basis for F_1 over F.

Q. E. D.

<u>Definition.</u> Let $F_1 \supset F$ be fields and let $\Sigma = \{v_1, v_2, \ldots\}$ be a transcendence basis for F_1 over F. If $F_1 = F(v_1, v_2, \ldots) = F(\Sigma)$ then we say that F_1 is a pure transcendental extension of F.

<u>Theorem 8.</u> Let F be a field and assume that F_1 and F_2 are pure transcendental extensions of F having the same transcendence degree. Then there exists an isomorphism of F_1 onto F_2, leaving each element of F fixed.

<u>Proof.</u>

Let $\Sigma_1 = (v_1, v_2, \ldots)$ and $\Sigma_2 = (u_1, u_2, \ldots)$ be transcendence bases of F_1 over F and F_2 over F, respectively. Since

$$\mathrm{card}\,\Sigma_1 = \mathrm{card}\,\Sigma_2$$

we can establish a one-to-one correspondence of Σ_1 and Σ_2,

$$f : \Sigma_1 \rightarrow \Sigma_2$$

Define f as the identity on F. Each element of F_1 is a finite rational combination of a finite subset of Σ_1, with coefficients in F. Define f to map such an element to the same rational combination of the corresponding elements of Σ_2. This defines the required F-isomorphism.

Q. E. D.

<u>Theorem 9.</u> Consider field extensions $F_2 \supset F_1 \supset F$. Then

$$\operatorname{tr} \partial^\circ F_2/F = \operatorname{tr} \partial^\circ F_2/F_1 + \operatorname{tr} \partial^\circ F_1/F$$

<u>Proof.</u>

Let $\Sigma_1 \subset F_1$ be a transcendence basis for F_1 over F and let $\Sigma_2 \subset F_2$ be a transcendence basis for F_2 over F_1. Consider the set $\Sigma = \Sigma_1 \cup \Sigma_2$ in F_2.

First note that F_2 is algebraic over $F(\Sigma)$. For each element $v \in F_2$ satisfies a polynomial equation, with a finite number of coefficients from $F_1(\Sigma_2)$; and each such coefficient is algebraic over $F(\Sigma_1 \cup \Sigma_2)$.

It is easy to see that Σ is algebraically independent over F. Thus Σ is a transcendence basis for F_2 over F. Since Σ_2 does not intersect F_1, and thus Σ_2 does not intersect Σ_1 we have

$$\operatorname{card} \Sigma = \operatorname{card} \Sigma_1 + \operatorname{card} \Sigma_2$$

Q. E. D.

<u>Definition.</u> Let F_1 be a differential field extension of the differential field F. An element $y \in F_1$ is called differential over F in case there exists a polynomial P in $n+1$ indeterminants and with

coefficients in F, such that $P(y,y',y'',\ldots,y^{(n)})=0$ in F_1. If each element of F_1 is differential over F, then we say that F_1 is differential over F. If F_1 is not differential over F, then F_1 is hypertranscendental over F.

Example 1. Let F be a differential field and consider the algebraic field $F_1 = F(x_0, x_1, x_2, \ldots)$ where $x_0, x_1, x_2, \ldots, x_n, \ldots$ are algebraically independent indeterminants. Define $x_0' = x_1,\ x_1' = x_2, \ldots, x_n' = x_{n+1}, \ldots$ to make F_1 a differential field extension of F. Then F_1 is the simple hypertranscendental extension of F. We write $F_1 = F\langle x\rangle$ and call x a differential indeterminant.

Example 2. Let L be a generalized Liouville extension of a differential field F. Then there is a chain of intermediate differential fields

$$F \subset F_1 \subset F_2 \subset \cdots \subset F_m \subset L$$

each of which is either algebraic or is generated by a transcendental element over the preceding field. Then L has a finite transcendence degree n over F. Take $v \in L$ and consider the $(n+1)$ elements $v, v', v'', \ldots, v^{(n)}$. These must be algebraically dependent over F and thus there exists a non-trivial polynomial $P(v, v', v'', \ldots, v^{(n)}) = 0$, with coefficients in F. Therefore L is differential over F.

Remark. A famous theorem of Hölder states that $\Gamma(z)$ is hypertranscendental over $\mathbb{C}(z)$, that is, $\Gamma(z)$ satisfies no polynomial differential equation.

Remark. Let $F_1 \supset F$ be a differential field extension of a differential field F. If $\operatorname{tr} \partial^\circ F_1/F = n$ is finite, then F_1 is differential over F. For take $v \in F_1$ and consider the algebraically dependent $n+1$ elements $v, v', v'', \ldots, v^{(n)}$. Then there is a non-trivial polynomial differential equation for V , with coefficients in F .

Problem. Let $F_2 \supset F_1 \supset F$ be differential field extensions. If F_1 is differential over F and F_2 is differential over F_1 , is F_2 differential over F ? This certainly holds if $\operatorname{tr} \partial^\circ F_1/F$ and $\operatorname{tr} \partial^\circ F_2/F_1$ are finite.

Problem. Let $F_1 = F\langle \xi \rangle$ be a differential field extension of a differential field F , and moreover F_1 is the smallest differential subfield of F_1 which contains F and $\xi \in F_1$. If ξ is differential over F is F_1 differential over F ?

Theorem 10. (**Hölder's Theorem on the Gamma Function**).

The function $\Gamma(z)$ satisfies no polynomial differential equation.

(1) Let $F(w, w', w'', \dots, w^{(n)}, z) = 0$, . . . 1. be a polynomial differential equation in $w, w', \dots, w^{(n)}$ with coefficients which are entire rational (i.e. polynomials) functions of z . If we replace W by W_0 , W' by W_1 , . . . , $W^{(n)}$ by W_n then

$$F(w_0, w_1, w_2, \dots, w_n, z) \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad 2.$$

is a polynomial in $n+2$ variables whose general term is of the form

$$A(z)\, w_0^{k_0} w_1^{k_1} \cdots w_n^{k_n} \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad 3.$$

where $A(z)$ is a polynomial in z and the exponents $k_0, k_1, \dots, k_n$ are non-negative integers.

(2) We call $(k_0, k_1, \dots, k_n)$ the height of 3. and we define

$$(k_0, k_1, \dots, k_n) > (l_0, l_1, \dots, l_n)$$

in case the last non-vanishing term in $k_0 - l_0, k_1 - l_1, \dots, k_n - l_n$ is positive. Or, equivalently, let $M = \max(k_0, \dots, k_n, l_0, \dots, l_n)$ then we define $(k_0, k_1, \dots, k_n) > (l_0, l_1, \dots, l_n)$ if

$$k_n M^n + k_{n-1} M^{n-1} + \dots + k_1 M + k_0 > l_n M^n + l_{n-1} M^{n-1} + \dots + l_1 M + l_0$$

(numerical inequality). This provides a $1-1$ map of any finite set of $(n+1)$-tuples onto the integers, thus we have a well ordering of any finite set and it is meaningful to speak of the <u>highest</u> term or <u>lowest</u> term of 2.

(3) Now <u>assume that $\Gamma(z)$ satisfies some differential equation of the form 1</u>. Then select, from the class of all such differential equations that $\Gamma(z)$ satisfies, that subset for which "the highest term is as low as possible". Denote this set of differential equations by $\mathcal{M}$ and <u>note</u> that all the polynomials in $\mathcal{M}$ will have the same sequence of exponents in their highest term. Now, from the equations in $\mathcal{M}$, select one for which the degree of the coefficient $A(z)$ of the highest term is as small as possible. We can further assume that the (constant) coefficient of the highest power of z, appearing in $A(z)$, is equal to 1. Call this distinguished polynomial $F(w_0, w_1, \ldots, w_n, z)$. From now on we will <u>assume</u> that 1. is the equation made from this member of $\mathcal{M}$.

(4) Some observations on $F(w_0, w_1, \ldots, w_n, z)$.

i) F <u>is not divisible by</u> w_0. For if it were then we could write $F(w_0, \ldots, z) = w_0 \overline{F}(w_0, \ldots, z)$ and the highest term of $\overline{F}$ would be lower than the highest term of F.

ii) F <u>is not divisible by</u> $(z-\alpha)$ for any α. Again, if it were we could write $F = (z-\alpha)\overline{F}$ and the degree of the coefficient $\overline{A}(z)$ of the highest term of $\overline{F}$ would be lower than the degree of $A(z)$ in F.

(5) <u>A Lemma</u>. If $\overline{F}(w_0, \ldots, w_n, z)$ is any other member of $\mathcal{M}$, then there exists a polynomial $Q(z)$ such that

$$\overline{F}(w_0, w_1, \ldots, w_n, z) = Q(z)\, F(w_0, w_1, \ldots, w_n, z) \quad \ldots \quad 4.$$

<u>Proof</u>.

Let $\overline{A}(z) w_0^{k_0} w_1^{k_1} \ldots w_n^{k_n}$ be the highest term of $\overline{F}$ and $A(z) w_0^{k_0} \ldots w_n^{k_n}$ the highest term of F. Since $\overline{A}$ + A are polynomials, and the degree of $\bar{A}$ is at least as large as the degree of A, we can write

$$\bar{A}(z) = Q(z)\,A(z) + P(z)$$

where Q and P are polynomials and the degree of P is less than the degree of A.

a) Suppose $P(z) = \bar{A}(z) - Q(z)\,A(z)$ is not identically zero. Consider the polynomial F^*(Note: Since $\Gamma(z)$ satisfies $\bar{F}$ and F it also satisfies F^* therefore $F^* \in \mathfrak{m}$.)

$$\begin{aligned} F^*(w_0,\dots,z) &= \bar{F}(w_0,\dots,z) - Q(z)\,F(w_0,\dots,z) \\ &= \left[\bar{A}(z)\,w_0^{k_0}\cdots w_n^{k_n} + \dots\right] - Q(z)\left[A(z)\,w_0^{k_0}\cdots w_n^{k_n} + \dots\right] \\ &= \left[\bar{A}(z) - Q(z)\,A(z)\right] w_0^{k_0}\cdots w_n^{k_n} + \dots \\ &= P(z)\,w_0^{k_0}\cdots w_n^{k_n} + \dots \end{aligned}$$

Thus the coefficient $P(z)$ of the highest term in F^* is of lower degree than $A(z)$, this contradicts the definition of $A(z)$. Therefore $P(z) \equiv 0$.

b) Now assume that $F^*(w_0,\dots,z)$ is not identically zero but $P(z) \equiv 0$. Then the highest term of $F^*(w_0,\dots,z)$ is lower than the highest term of F and this is a contradiction. Therefore $\bar{F} \equiv Q(z)\,F$

Q. E. D.

The elements of $\mathfrak{m}$ therefore all come from multiplying 1. by a polynomial in z. ($\mathfrak{m}$ is a prime ideal.)

(6) The differential equation for $\Gamma(z+1)$.

Since $w = \Gamma(z)$ satisfies 1.) we see that $\Gamma(z+1)$ satisfies $F(\Gamma(z+1), \Gamma'(z+1), \dots, \Gamma^{(n)}(z+1), z+1) = 0$. If we use the relationship $\Gamma(z+1) = z\,\Gamma(z)$ then the polynomial form of the equation is

$$F(zw_0,\ zw_1 + w_0,\ zw_2 + 2w_1,\ \dots,\ zw_n + nw_{n-1},\ z+1) = 0 \quad \dots \quad 5.$$

The highest term in this polynomial arises when we make the indicated substitutions into 3. $A(z+1)(zw_0)^{k_0}(zw_1+w_0)^{k_1}\cdots(zw_n+nw_{n-1})^{k_n} =$

$$= A(z+1)z^k w_0^{k_0} w_1^{k_1} \cdots w_n^{k_n} + \text{other terms},$$

where $k = k_0 + k_1 + \cdots + k_n$. Each of the monomials in this expansion contains, as a factor, exactly one term from the binomial expansion of each of the factors $(zw_r + rw_{r-1})^{k_r}$, $r = 0, 1, \ldots, n$. To construct the highest of these monomials we use the largest power of w_n, it is k_n since w_n appears only in the last factor; then the largest power of w_{n-1} in the remaining factors is k_{n-1} since w_{n-1} appears only in the last two factors; etc. Therefore none of the "other terms" is as high as $A(z+1)z^k w_0^{k_0} \cdots w_n^{k_n}$.

Now 5. is also a polynomial differential equation with polynomial coefficients that is satisfied by $\Gamma(z)$. Also the highest term has the same array of exponents as occurs in the members of $\mathfrak{M}$, therefore 5. is in $\mathfrak{M}$. Thus we can write

$$F(zw_0, zw_1+w_0, \ldots, z+1) \equiv D(z)F(w_0, w_1, \ldots, z) \quad \ldots\ldots 6.$$
$$D(z) = \text{a polynomial in } z.$$

by the lemma in paragraph (5).

(7) Determination of $D(z)$

The highest term in $F(zw_0, \ldots, z+1)$ is $A(z+1)z^k w_0^{k_0} \cdots w_n^{k_n}$ and the highest term in $D(z)F(w_0, \ldots, z)$ is $A(z)a_0 z^\ell w_0^{k_0} \cdots w_n^{k_n}$ where $D(z) = a_0 z^\ell + a_1 z^{\ell-1} + \cdots + a_\ell$. These two terms must be identical and since $A(z)$ and $A(z+1)$ are of the same degree in z and both have leading coefficients of 1 we see that $a_0 z^\ell = z^k$, i.e. $D(z) = z^k + \cdots$.

Next make a change of variable so that the left side of 6. becomes $F(x_0, x_1, \ldots, x_n, t)$. That is

$$z + 1 = t \qquad\qquad z = t - 1$$

$$zw_0 = x_0 \qquad\qquad w_0 = \frac{x_0}{t-1}$$

$$zw_1 + w_0 = x_1 \qquad w_1 = \frac{x_1(t-1) - x_0}{(t-1)^2}$$

$$\vdots \qquad\qquad\qquad \vdots$$

in general let $w_\nu = \frac{P_\nu(x_0, x_1, \dots, x_\nu, t)}{(t-1)^{\nu+1}}$

where $P(x_0, \dots, x_\nu, t)$ is a polynomial in $x_0, \dots, x_\nu, t$. With this substitution 6. becomes:

$$F(x_0, x_1, \dots, x_\nu, t) \equiv D(t-1)\, F\left(\frac{x_0}{t-1}, \frac{P_1(x_0, x_1, t)}{(t-1)^2}, \dots, t\right)$$

The right side of this expression is a polynomial in $t, \frac{x_0}{t-1}, \frac{P_1}{(t-1)^2}, \dots$ thus there is an integer J such that $(t-1)^J \times$ "right side" is a polynomial in $t, x_0, P_1, \dots, P_n$. Therefore, for this J we have

$$(t-1)^J F(x_0, \dots, t) \equiv D(t-1)\, G(x_0, \dots, x_n, t) \quad , \dots, 7.$$

where $G(x_0, \dots, x_n, t)$ is also a polynomial in $n+2$ variables. Now suppose that the right side of 7. has a factor of $(t - \alpha)$ for some $\alpha \neq 1$. Then $F(x_0, \dots, t)$ must have this same factor but we proved earlier that $F(w_0, \dots, z)$ had no factors of $(z - \alpha)$ for any α. Therefore the only possible factors of the right side are $(t-1)$ and since $D(t-1)$ is a polynomial of degree k in t we must have $D(t-1) = (t-1)^k$ or $D(z) \equiv z^k$, and 6. becomes

$$F(zw_0, zw_1 + w_0, \dots, z+1) \equiv z^k F(w_0, w_1, \dots, z) \quad , \dots, 8.$$

(Note that this is a polynomial identity.)

(8) Final contradiction.

Consider the polynomial identity 8. for $w_0 = 0$.

$$F(0, zw_1, zw_2 + zw_1, \dots, z+1) \equiv z^k F(0, w_1, \dots, z) \quad .$$

Since $F(w_0, w_1, \dots, z)$ does not have a factor of w_0, the right side is not identically zero. Let the highest term of $F(0, w_1, \dots, z)$ be

$C(z)w_1^{l_1}\cdots w_n^{l_n}$. Then the highest term on the left side of this identity is $C(z+1)z^{l_1+\cdots+l_n}w_1^{l_1}\cdots w_n^{l_n}$. Since the two highest terms must be the same we have $C(z+1)z^{l_1+\cdots+l_n} = z^k C(z)$. Therefore $l_1+l_2+\cdots+l_n = k$ and $C(z+1) = C(z)$. Thus $C(z) \not\equiv 0$ is a polynomial with period 1, i.e. $C(z) = \text{constant} = K \neq 0$. We can write

$$F(0,w_1,\dots,w_n,z) = K w_1^{l_1}\cdots w_n^{l_n} + \text{other terms,}$$

therefore

$$F(0,w_1,\dots,w_n,1) = K w_1^{l_1}\cdots w_n^{l_n} + \text{other terms} \not\equiv 0 \quad \dots 9.$$

But, let $z = 0$ in 8., thus

$$F(0,w_0,2w_1,\dots,nw_{n-1},1) \equiv 0$$

whereas by making the symbolic substitution $w_0 \to w_1,\ 2w_1 \to w_2, \dots$ in 9. we see that this is a contradiction.

4. Functions of Finite Order and Liouville's Principle.

We follow closely Integration in Finite Terms, chapters 1, 5, and 6 by J. Ritt.

Definition. An algebraic function of the complex variable z is called a function of order 0. A function is called a monomial of order 1 if it is not algebraic but it is the integral or the exponential of an algebraic function. A function is of order 1 if it is not algebraic but it is an algebraic combination of a finite set of functions of order 0 and monomials of order 1. That is, a function of order 1 is algebraic over a field generated over $\mathbb{C}$ by a finite number of functions of order 0 and monomials of order 1.

An n-monomial is a complex function which is not of order 0, 1, 2, ..., n-1 but which is either the integral or the exponential of a function of order n-1. A function of order n is an algebraic combination of a finite set of functions of order $\leq n-1$ and of n-monomials, provided the function is not of order $\leq n-1$. The set of all functions so obtained are the functions of finite order.

Remark. By use of analytic continuation and the permanence of functional equations we can show that the order of a function of finite order is a well determined integer.

Theorem 11. The set of all functions of finite order is precisely the set of elementary functions of Liouville.

Proof.

Algebraic functions of a complex variable are Liouville elementary functions. Assume that functions of orders 0, 1, 2, ..., n-1 are known to be elementary. Let f be a function of order n. Then f is an algebraic combination of $g_1, g_2, \ldots, g_\ell$ and $\theta_1, \theta_2, \ldots, \theta_r$ where $g_1, \ldots, g_\ell$ are functions of order $\leq n-1$ and $\theta_1, \ldots, \theta_r$ are each an integral or an exponential of a function $\varphi_1, \ldots, \varphi_r$ (respectively) of order n-1.

Let $F = \mathbb{C}(z)$ be the field of rational functions with complex coefficients. Then f lies in a finite algebraic extension K of $F(g_1, \ldots, g_\ell, \theta_1, \ldots, \theta_r)$. But $F(g_1, \ldots, g_\ell, \varphi_1, \ldots, \varphi_r)$ lies in a generalized Liouville extension L_1 of F and

$$L_1 \subset L_1(\theta_1) \subset L_1(\theta_1, \theta_2) \subset \cdots \subset L_1(\theta_1, \ldots, \theta_r) \subset K_0$$

provides the required generalized Liouville extension of $F = \mathbb{C}(z)$. Thus f is an elementary function.

Conversely, let h be an elementary function, say in a generalized Liouville extension L of $F = \mathbb{C}(z)$. Consider the corresponding chain of intermediate fields, $F \subset F_1 \subset F_2 \subset \cdots \subset L$.

Certainly each function of F is rational and thus of order 0. If F_1 is a finite algebraic extension of F, each function of F_1 is of order 0; otherwise each function of F_1 is of order ≤ 2.

If F_2 is a finite algebraic extension of F_1, each function of F_2 is of order ≤ 2. If F_2 is an extension by an integral, or by an exponential of an integral, and if F_2 is not algebraic over F_1, then F_2 is generated by just one monomial and each function in F_2 has order ≤ 4.

Continuing for a finite number of steps in this way, we find that each function in L is of finite order.

Q.E.D.

Theorem 12. (Liouville's Principle). Let u be an elementary function of order $n \geq 1$. Let u be expressed as an algebraic function of n-monomials $\theta_1, \theta_2, \dots, \theta_r$ and functions of order $\leq n-1$. Choose the representation of u for which $r \geq 1$ is the least possible.

Let $\xi_1(z), \dots, \xi_p(z)$ be any finite set of functions of order $\leq n-1$ and let $f(x_1, \dots, x_r, y_1, \dots, y_p)$ be an algebraic function of $r+p$ complex variables. If $f(\theta_1(z), \theta_2(z), \dots, \theta_r(z), \xi_1(z), \dots, \xi_p(z)) \equiv 0$ in a neighborhood of $\theta_1(a), \dots, \theta_r(a), \xi_1(a), \dots, \xi_p(a)$ where f is holomorphic, then

$$f(x_1, x_2, \dots, x_r, \xi_1(z), \dots, \xi_p(z)) \equiv 0$$

for all nearby values $(x_1, \dots, x_r, z)$.

Proof.

Let $f(\theta_1(z), \dots, \theta_r(z), \xi_1(z), \dots, \xi_p(z)) \equiv 0$ for a neighborhood of $z = a$. Suppose there exist points $z = b$, arbitrarily near $z = a$, for which $f(x_1, \dots, x_r, \xi_1(b), \dots, \xi_p(b)) \neq 0$. The set of such values b fill an open set B in the complex plane.

Now

$$f(\theta_1(b), \dots, \theta_r(b), \xi_1(b), \dots, \xi_p(b)) = 0$$

and suppose $\frac{\partial f}{\partial x_1}(\theta_1(b), \dots, \theta_r(b), \xi_1(b), \dots, \xi_p(b)) \neq 0$.

Then solve for $x_1 = Q_1(x_2, \dots, x_r, y_1, \dots, y_p)$ where Q_1 is an algebraic function which is analytic near $x_2 = \theta_2(b), \dots, x_r = \theta_r(b), y_1 = \xi_1(b), \dots, y_p = \xi_p(b)$. By the uniqueness guaranteed by the implicit function theorem we note that

$$\theta_1(z) = Q_1(\theta_2(z), \dots, \theta_r(z), \xi_1(z), \dots, \xi_p(z)) .$$

But this contradicts the minimality in the choice of r in the representation of u.

However suppose at every $\bar{b} \in B$ we have

$$\frac{\partial f}{\partial x_1}(\theta_1(\bar{b}), \dots, \theta_r(\bar{b}), \xi_1(\bar{b}), \dots, \xi_p(\bar{b})) = 0.$$

Then

$$\frac{\partial f}{\partial x_1}(\theta_1(z), \dots, \theta_r(z), \xi_1(z), \dots, \xi_p(z)) \equiv 0$$ in B. Take a higher derivative, say,

$$\frac{\partial^2 f}{\partial x_1 \partial x_2}(\theta_1(b), \dots, \theta_r(b), \xi_1(b), \dots, \xi_p(b)) \neq 0$$

Then solve for

$$\theta_2(z) = Q_2(\theta_1(z), \theta_3(z), \dots, \theta_r(z), \xi_1(z), \dots, \xi_p(z))$$

and proceed as above.

Consider all the partial derivatives of $f(x_1, x_2, \dots, x_r, y_1, \dots, y_p)$ with respect to the variables $x_1, \dots, x_r$ and evaluated at $x_1 = \theta_1(b), \dots, x_r = \theta_r(b), y_1 = \xi_1(b), \dots, y_p = \xi_p(b)$. Not all these derivatives vanish for otherwise $f(x_1, \dots, x_r, \xi_1(b), \dots, \xi_p(b)) \equiv 0$ for all nearby values of $(x_1, \dots, x_r)$, which contradicts the definition of $b \in B$.

Thus a finite repetition of the argument described above finally leads to a use of the implicit function theorem and a proof of our theorem.

Q. E. D.

5. <u>Liouville's Theory of the Bessel and Riccati Differential Equations.</u>

Theorem 13. Consider

1) $y'' + P(z)y' + Q(z)y = R(z)$

where $P(z), Q(z), R(z)$ are elementary functions. If there is a non-zero elementary function $y_1(z)$, which is a solution of the homogeneous equation $y'' + P(z)y' + Q(z)y = 0$, then every solution of 1) is an elementary function.

Proof.

We consider 1) in a region where $y_1(z)$, $P(z)$, $Q(z)$ and $R(z)$ are holomorphic. An independent solution of the homogeneous equation is

$$y_2(z) = y_1(z)\int \exp\left[\int -\frac{2y_1' + Py_1}{y_1}\,dz\right]dz$$

Thus $y_2(z)$ is elementary. The formula of variation of parameters yields an elementary solution $y(z)$ of 1) and thus every solution of 1) is elementary.

Q. E. D.

Corollary. If $u' + u^2 + P(z)u + Q(z) = 0$, where $P(z)$ and $Q(z)$ are elementary, has one elementary solution, then every solution is elementary.

Proof.

Let $u_1(z)$ be an elementary solution of the Riccati equation and let $y_1(z) = e^{\int u_1 dz}$. Then $y_1(z)$ is a non-zero solution of the linear differential equation

$$y'' + P(z)y' + Q(z)y = 0$$

and hence each solution of the linear equation is elementary.

Let $u_2(z)$ be a solution of the Riccati equation. Then $u_2(z) = y_2'(z)/y_2(z)$ where $y_2(z)$ is an elementary solution of the linear equation. Hence $u_2(z)$ is elementary.

Q. E. D.

Theorem 14. (D. Bernouilli). The Bessel equation

$$z^2y'' + zy' + (z^2 - \nu^2)y = 0$$

with $2\nu = \pm 1, \pm 3, \pm 5, \dots$ an odd integer, has elementary solutions.

The Riccati equation

$$y' + y^2 = z^\alpha,$$

with $\alpha = -2$ or $\alpha = -4p/(1+2p)$ for $p = 0, \pm 1, \pm 2, \dots$ an integer, has elementary solutions.

Proof.

Consider the Bessel equation with $2\nu = 1, 3, 5, \dots$. Put $y(z) = z^{-1/2}u(z)$ and also write $z = ix$ to get

$$\frac{d^2u}{dx^2} = \left[1 + \frac{p(p+1)}{x^2}\right]u$$

, where $p = \nu - \frac{1}{2} \geqslant 0$ is an integer.

We can consider only the case $p \geqslant 1$. Now let $u(x) = e^x x^{-p}\varphi(x)$ to get

$$\frac{d^2\varphi}{dx^2} + 2\left(1 - \frac{p}{x}\right)\frac{d\varphi}{dx} - \frac{2p\varphi}{x} = 0 .$$

We show that there exists a polynomial solution $\varphi(x) \neq 0$, and hence

$$y(z) = z^{-1/2} e^{-iz} (-iz)^{-p} \varphi(-iz)$$

is an elementary solution of Bessel's equation.

We find a power series solution $\varphi(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m + \dots$ and choose $a_0 = 1$, $a_m = 0$ for $m \geqslant p+1$.

Consider the Riccati equation

$$\frac{dy}{dz} + y^2 = z^\alpha \qquad \text{for } \alpha = -2 \text{ or } \alpha = \frac{-4\bar{p}}{1+2\bar{p}}$$

where $\bar{p} = 0, \pm 1, \pm 2, \dots$. For $\alpha = -2$ let $y(z) = zV(z)$, separate the variables, and obtain an elementary solution. Now assume $\alpha \neq -2$. Put $y(z) = w'(z)/w(z)$ to get $\dfrac{d^2w}{dz^2} = z^\alpha w$

Let $\alpha = 2q - 2,\ q \neq 0$ and put $x = z^q/q$ to get

$$\frac{d^2w}{dx^2} + \frac{q-1}{qx}\frac{dw}{dx} - w = 0 .$$

Put $p = \dfrac{1-q}{2q}$ and put $w(x) = x^p u(x)$ to get,

$$\frac{d^2u}{dx^2} = \left[1 + \frac{p(p+1)}{x^2}\right]u$$

. Here $p = \dfrac{1-q}{2q} = \bar{p}$.

If $p = 0$, $u(x) = e^x$ and $y(z) \equiv 1$. If $p = -1$, $u(x) = e^x$ and $y(z) = -z^{-2} + z^{-1}$. If $p < -1$ note $p'[p'+1] = p(p+1)$ where $p' = -p-1 > 0$. Thus we can assume $p > 0$. As was seen above there is an elementary solution $u(x) = e^{x} x^{-p} \varphi(x)$, where $\varphi(x)$ is a polynomial. Then take $w(z) = e^{\frac{z^q}{q}} \varphi(\frac{z^q}{q})$ where $q = \frac{1}{2p+1}$. Thus $y(z) = w'(z)/w(z)$ is an elementary solution of the Riccati equation.

Q. E. D.

Theorem 15. Let $P(x) \not\equiv 0$ be algebraic. If R), $y' + y^2 = P(x)$ has an elementary solution, then R) has an algebraic function as solution.

Proof.

Consider holomorphic solutions $y(x)$ in a region where $P(x)$ is a holomorphic power series.

Let E be the totality of all elementary functions satisfying R) and E_1 those of least order $m > 0$ (unless R) has an algebraic solution). Write each function of E_1 with as few m-monomials as possible. Let $y(x)$ be a solution of R) in E_1 involving no more monomials than appear in any other function in E_1. Write

$$y = F(\theta_1, \theta_2, \cdots, \theta_r, g_1, \cdots, g_\ell)$$

where F is an algebraic function of $r + \ell$ variables, $\theta_1(x), \cdots, \theta_r(x)$ are m-monomials, and $g_1(x), \cdots, g_\ell(x)$ are functions of order $< m$.

Suppose $\theta_1 = e^{\varphi_1}$, where φ_1 is of order $m-1$. Then

$$F_{\theta_1} \theta_1 \varphi_1' + F_{\theta_2} \theta_2' + \cdots + F_{\theta_r} \theta_r' + F_{g_1} g_1' + \cdots + F_{g_\ell} g_\ell' + F^2 = P$$

But this is an algebraic combination of $\theta_1, \cdots, \theta_r$ and functions of order $< m$, and hence this is an identity in $\theta_1, \theta_2, \cdots, \theta_r$. In particular, if we define $F(\theta_1, x) = F(\theta_1, \theta_2(x), \cdots, \theta_r(x), g_1(x), \cdots, g_\ell(x))$ then $F_{\theta_1}(\theta_1, x)\, \theta_1 \varphi_1'(x) + F_x(\theta_1, x) + F^2(\theta_1, x) = P(x)$ is an identity in (θ_1, x).

In the same way if $\theta_1 = \int \hat{\varphi}_1$ for $\hat{\varphi}_1$ of order $m-1$, we obtain an identity in (θ_1, x),

$$F_{\theta_1}(\theta_1, x)\, \hat{\varphi}_1(x) + F_x(\theta_1, x) + F^2(\theta_1, x) = P(x).$$

Now $F(\theta_1, \cdots, \theta_r, g_1, \cdots, g_\ell)$ is an algebraic combination of $(\theta_1, \cdots, \theta_r, g_1, \cdots, g_\ell)$ and hence there is a polynomial equation

$$A_n(\theta_1, \cdots, \theta_r, g_1, \cdots, g_\ell) F^n + \cdots + A_0(\theta_1, \cdots, \theta_r, g_1, \cdots, g_\ell) = 0$$

where each A_i is a polynomial in $(\theta_1, \cdots, \theta_r, g_1, \cdots, g_\ell)$ with complex coefficients. Again write $A(\theta_1(x), \ldots, \theta_r(x), g_1(x), \cdots, g_\ell(x)) = A(\theta_1(x), x)$. Here $A(\theta_1, x) = a_0(x) + a_1(x)\,\theta_1 + \cdots + a_k(x)\,\theta_1^k$ where each $a(x)$ is a polynomial in $\theta_2(x), \cdots, \theta_r(x), g_1(x), \cdots, g_\ell(x)$. Then we can write (see appendix to this section 5)

$$F(\theta_1, x) = c_1(x)\,\theta_1^{\frac{p}{q}} + c_2(x)\,\theta_1^{\frac{p-1}{q}} + c_3(x)\,\theta_1^{\frac{p-2}{q}} + \cdots, \quad c_1 \neq 0,$$

where $q > 0$ and p are integers and each $C(x)$ is an algebraic combination of the coefficients $a(x)$ occurring in the $A(\theta_1, x)$. Thus each $C(x)$ is an algebraic function of $\theta_2(x), \cdots, \theta_r(x)$ and functions of order $< m$.

In case $\theta_1 = e^{\varphi_1}$ we obtain

$$F_{\theta_1}(\theta_1, x)\,\theta_1 \varphi_1'(x) + F_x(\theta_1, x) + F(\theta_1, x)^2 \equiv P(x) \quad \text{in} \quad (\theta_1, x) \qquad \text{so}$$

$$\left[c_1(x)\tfrac{p}{q}\,\theta_1^{\frac{p}{q}-1} + c_2(x)\tfrac{p-1}{q}\,\theta_1^{\frac{p-1}{q}-1} + \cdots\right]\theta_1 \varphi_1'(x)$$
$$+ \left[C_1'(x)\,\theta_1^{\frac{p}{q}} + C_2'(x)\,\theta_2^{\frac{p-1}{q}} + \cdots\right]$$
$$+ \left[C_1^2\,\theta_1^{\frac{2p}{q}} + 2c_1C_2\,\theta_1^{\frac{2p-1}{q}} + \cdots\right] \equiv P(x).$$

Thus

$$\left[c_1\tfrac{p}{q}\,\varphi_1'(x) + c_1'\right]\theta_1^{\frac{p}{q}} + \cdots + \left[c_1^2\,\theta_1^{\frac{2p}{q}} + \cdots\right] \equiv P(x).$$

If $\frac{p}{q} > 0$, there is a term in $\theta_1^{\frac{2p}{q}}$ which does not cancel in this identity. But there must be a term in θ_1^0 and hence $\frac{p}{q} \geq 0$. Thus $\frac{p}{q} = 0$. This yields $C_1'(x) + C_1(x)^2 = P(x)$

Thus $C_1(x)$ is a solution of $R)$ which is algebraically dependent on $\theta_2, \cdots, \theta_r$ and functions of order $< m$. This is impossible and hence we must have $m = 0$ and an algebraic solution of $R)$.

In the case where $\theta_1 = \int \hat{\varphi}_1$ we obtain

$$F_{\theta_1}(\theta_1, x)\,\hat{\varphi}_1(x) + F_x(\theta_1, x) + F(\theta_1, x)^2 \equiv P(x) \quad \text{in } (\theta_1, x). \quad \text{Again use}$$

the same fractional power series representation of $F(\theta_1, x)$ to get

$$\left[c_1(x) \frac{-p}{q} \theta_1^{\frac{-p}{q}-1} + c_2(x) \frac{-p-1}{q} \theta_1^{\frac{-p-1}{q}-1} + \dots \right] \hat{\varphi}_1(x)$$
$$+ \left[c_1'(x)\, \theta_1^{\frac{-p}{q}} + c_2'(x)\, \theta_1^{\frac{-p-1}{q}} + \dots \right]$$
$$+ \left[c_1^2 \theta_1^{\frac{2-p}{q}} + 2 c_1 c_2 \theta_1^{\frac{2-p-1}{q}} + \dots \right] = P(x) .$$

Thus

$$\left[c_1'(x) \theta_1^{\frac{-p}{q}} + \dots \right] + \left[c_1^2 \theta_1^{\frac{2-p}{q}} + \dots \right] \equiv P(x) .$$

Again $\frac{-p}{q} \geqslant 0$ and if $\frac{-p}{q} > 0$ the term $\theta_1^{\frac{2-p}{q}}$ fails to cancel. Thus $\frac{-p}{q} = 0$. Equating terms without θ_1 we obtain

$c_1'(x) + c_1(x)^2 = P(x)$. Thus $c_1(x)$ is again a solution of $R)$ containing fewer than r m-monomials. Hence we have $m = 0$.

Q. E. D.

Lemma 1. Each algebraic solution of

$R)$ $\frac{dv}{dz} + v^2 = 1 + \frac{-p(-p+1)}{z^2}$, for a complex constant $-p$ is rational.

Proof.

Let $v(z)$ be an algebraic function which is a solution of $R)$. Suppose $v(z)$ has a branch point at $z = \infty$. Then

$v(z) = a_1 z^{P_1} + a_2 z^{P_2} + \dots$, near $z = \infty$, where

$P_1 > P_2 > \cdots$ are fractions with a common denominator and each

$a_1 \neq 0, a_2 \neq 0, \dots$. By substitution,

$$(a_1 P_1 z^{P_1 - 1} + a_2 P_2 z^{P_2 - 1} + \dots) + (a_1^2 z^{2P_1} + 2 a_1 a_2 z^{P_1 + P_2}) = 1 + p(-p+1) z^{-2}.$$

Thus $P_1 \geqslant 0$ and so $P_1 = 0$.

Let P_i be the largest exponent which is not an integer. Then the largest non-integral power in v^2 is found in $2 a_1 a_i z^{P_i}$. The largest non-integral power of z in v' comes from $a_i P_i z^{P_i - 1}$. These cannot cancel and so $v(z)$ does not have a branch point at ∞ .

Next suppose $V(z)$ has a branch point at $z = c \neq 0$. Write the expansion $V = a_1(z-c)^{p_1} + a_2(z-c)^{p_2} + \cdots \; ; \; a_1 \neq 0, a_2 \neq 0, \ldots$ where the $p_1 < p_2 < \cdots$ are fractions with a common denominator. Now $p_1 \geq -1$ for otherwise the function $V' + V^2$ must have a pole-like singularity of exponent < -2 and $1 + \frac{\rho(\rho+1)}{z^2}$ has at most a pole of order -2.

Suppose that p_1 is not an integer. The first term in V' is $a_1 p_1 (z-c)^{p_1 - 1}$ with a non-integral exponent. There must be a term in V^2 to cancel this and so $p_1 - 1 = p_i + p_j$ for some i, j. But $p_i + p_j \geq 2p_1$ and so $2p_1 \leq p_1 - 1$ or $p_1 \leq -1$. Thus we conclude that p_1 is an integer.

Suppose now that some exponent of V is non-integral and let p_i, $i > 1$ be the smallest such exponent. The smallest non-integral exponents in V' and V^2 are found in $p_i a_i z^{p_i - 1}$ and $2 a_1 a_i z^{p_i + p_1}$, respectively. Therefore $p_1 = -1$ and $p_i = -2a_i$. Also the lowest degree terms in V' and V^2, respectively, are $-a_1(z-c)^{-2}$ and $a_1^2(z-c)^{-2}$. But $1 + \frac{\rho(\rho+1)}{z^2}$ does not have a pole at $z = c \neq 0$ and hence $a_1 = a_1^2$ so $a_1 = 1$. Hence $p_i = -2a_1 = -2$ is an integer. Thus we conclude that V is meromorphic at $z = c$ and does not have a branch point anywhere on the Riemann sphere, except possibly at $z = 0$.

But, by considering the change in argument of $V(z)$ around a curve encircling $z = 0$, and then swelling this curve to a neighborhood at $z = \infty$, we find that $V(z)$ has no branch point at $z = 0$. Thus $V(z)$ has at most poles on the Riemann sphere and is a rational function.

Q. E. D.

<u>Lemma 2.</u> If

$$R) \qquad \frac{dV}{dz} + V^2 = 1 + \frac{\rho(\rho+1)}{z^2}$$

has a rational function solution, then ρ is an integer.

Proof.

Let $V = \frac{P(z)}{Q(z)}$ where P and Q are polynomials having no zero in common (relatively prime polynomials). Near $z = \infty$ write $\zeta = \frac{1}{z}$ and consider

$$\frac{dV}{d\zeta} = -\frac{1}{\zeta^2} - p(p+1) + \frac{V^2}{\zeta^2}$$

It is easily seen that there is no solution of the form $C_{-m}\zeta^{-m} + C_{-m+1}\zeta^{-m+1} + \cdots$, for $m \geq 1$. Thus $V = \frac{P(z)}{Q(z)}$ has no pole at $z = \infty$.

Try $V = C_{-m}(z-C)^{-m} + C_{-m+1}(z-C)^{-m+1} + \cdots$, $m > 1$, and note that V^2 contains the term $C_{-m}^2 (z-C)^{-2m}$ which cannot cancel. Thus $V(z)$ has at most simple poles in the complex plane. Let $V(\infty) = h$ and let the r non-zero roots of Q be $C_1, C_2, \ldots, C_r$. Then the partial fraction

$$V = h + \frac{K}{z} + \frac{K_1}{z-C_1} + \cdots + \frac{K_r}{z-C_r}.$$

Again, substitution in the differential equation R) shows

$$-\frac{K}{z^2} - \frac{K_1}{(z-C_1)^2} - \cdots - \frac{K_r}{(z-C_r)^2} + h^2 + \frac{K^2}{z^2} + \frac{K_1^2}{(z-C_1)^2} + \cdots + \frac{K_r^2}{(z-C_r)^2}$$
$$+ \frac{2hK}{z} + \frac{2hK_1}{z-C_1} + \cdots + \frac{2hK_r}{z-C_r} + \frac{2KK_1}{z(z-C_1)} + \cdots + \frac{2K_{r-1}K_r}{(z-C_{r-1})(z-C_r)} = 1 + \frac{p(p+1)}{z^2}.$$

Thus $h = \pm 1$ and $-K_1 + K_1^2 = 0$ so $K_1 = 1$ and $K_2 = \cdots = K_r = 1$. Also $-K + K^2 = p(p+1)$. Thus $K = (p+1)$ or $K = -p$ are the two roots. Thus $V = h + \frac{K}{z} + \frac{1}{z-C_1} + \cdots + \frac{1}{z-C_r}$ and in a Laurent expansion around $z = \infty$ we have $V = h + \frac{K+r}{z} + \frac{l}{z^2} + \cdots$.

Here

$$-\frac{(K+r)}{z^2} - \frac{2l}{z^3} - \cdots + h^2 + \frac{2h(K+r)}{z} + \cdots = 1 + \frac{p(p+1)}{z^2}.$$

Thus $2h(K+r) = 0$ so $K = -r$ is an integer. Thus p is an integer.

Q. E. D.

Theorem 16. The Bessel equation

$$z^2 y'' + z y' + (z^2 - \nu^2) y = 0$$

has no (non-zero) elementary solution if 2ν is not an odd integer

$(2\nu \neq \pm 1, \pm 3, \pm 5, \ldots)$. The Riccati equation $y' + y^2 = z^\alpha$ has no elementary solution, if $\alpha \neq -2$ and $\alpha \neq \frac{-4p}{(1+2p)}$ for every integer $p = 0, \pm 1, \pm 2, \ldots$.

Proof.

If $y(z) \not\equiv 0$ is an elementary solution of the Bessel equation, then set $u(z) = z^{1/2} y(z)$ and $z = ix$ to define $u(x) \not\equiv 0$, an elementary solution of $\frac{d^2u}{dx^2} = \left[1 + \frac{p(p+1)}{x^2}\right]u$ where $p = \nu - 1/2$. Define $v(x) = u'(x)/u(x)$, an elementary solution of $\frac{dv}{dx} + v^2 = 1 + \frac{p(p+1)}{x^2}$. This is impossible, by the lemmas, since p is not an integer.

In the case of the Riccati equation suppose $y(z)$ is an elementary solution. Define $w(z) = \exp \int y(z)$, an elementary solution of $\frac{d^2w}{dz^2} = z^\alpha w$. Let $\alpha = 2q - 2$ so $q \neq 0$ and put $x = z^q/q$ to define the elementary solution $w(x) \not\equiv 0$ of $\frac{d^2w}{dx^2} + \frac{q-1}{qx}\frac{dw}{dx} - w = 0$. Put $\bar{p} = \frac{1-q}{2q}$ and $w(x) = x^{\bar{p}} u(x)$ to get $\frac{d^2u}{dx^2} = \left[1 + \frac{p(p+1)}{x^2}\right]u$. Here $\bar{p} = \frac{1-q}{2q} = p$. Define the elementary function $v(x) = u'(x)/u(x)$, which is a solution of $\frac{dv}{dx} + v^2 = 1 + \frac{p(p+1)}{x^2}$. If p were an integer, then $\alpha = \frac{-4p}{2p+1}$ which is denied in the hypotheses. Thus p is not an integer and the existence of $v(x)$ contradicts the lemmas.

Q. E. D.

Appendix to 5. A Theorem on Polynomials

Let $\phi(y, \theta) = A_0(\theta) y^k + A_1(\theta) y^{k-1} + \cdots + A_k(\theta)$ be a polynomial in y and θ, where the $A_\alpha(\theta)$ are themselves polynomials in θ whose coefficients will be denoted by $A_{\alpha\beta}$. Then there exists a natural number q such that $\phi(y, \theta)$ can be decomposed into k linear factors $\phi(y, \theta) = A_0(\theta)[y - f_1(\theta)] \cdots [y - f_k(\theta)]$, where the $f_j(\theta)$ are power series in $\theta^{\frac{1}{q}}$ (near ∞) with only finitely many terms of positive order. The coefficients of these power series are all algebraic functions of the $A_{\alpha\beta}$. We will first prove:

Theorem 17 (Weierstrass' Preparation Theorem).

Let $P(w,z) = p_0(z)w^k + \dots + p_k(z)$ be a polynomial in w with coefficients that are regular power series in z near $z=0$. Assume that $P(w,0)$ starts with the term $b_0 w^\nu$, $b_0 \neq 0$, $\nu > 0$. Then $P(w,z) = \left(w^\nu + q_1(z)w^{\nu-1} + \dots + q_\nu(z)\right) Q(w,z)$ where the $q_j(z)$ designate power series regular in z and vanishing at $z = 0$, and where $Q(0,0) = b_0 \neq 0$. Furthermore $Q(w,z)$ is a polynomial of $(k-\nu)$th degree in w whose coefficients $Q_\ell(z)$ are regular power series in z near $z = 0$. The coefficients of the power series $q_j(z)$ and $Q_\ell(z)$ are all rational functions of only finitely many of the coefficients of the power series $p_i(z)$.

Proof.

Let $P(w,0) = b_0 w^\nu + b_1 w^{\nu+1} + \dots + b_{k-\nu} w^k$, $b_0 \neq 0$.

Choose $\rho > 0$ such that $P(w,0) \neq 0$ in $0 < |w| \leq \rho$, and let

$$\min_{|w|=\rho} |P(w,0)| = m > 0 .$$

Choose $\delta > 0$ such that $|P(w,z) - P(w,0)| < m$ for $|w| = \rho$ and $|z| \leq \delta$.

By the theorem of Rouché, $P(w,z)$ has exactly as many zeros inside $|w| < \rho$ (for $|z| < \delta$) as does $P(w,0)$, that is, exactly ν branches. Let these branches be $w_1(z), w_2(z), \dots, w_\nu(z)$.

Then for each natural number σ we have

$$w_1^\sigma + w_2^\sigma + \dots + w_\nu^\sigma = \frac{1}{2\pi i}\int_{|w|=\rho} w^\sigma \frac{P_w(w,z)}{P(w,z)}\, dw .$$

But

$$\frac{P_w(w,z)}{P(w,z)} = \frac{k p_0 w^{k-1} + \cdots + p_{k-1}}{p_0 w^k + \cdots + p_k}$$

is regular in $|z| \leq \delta$ for $|w| = \rho$. The development of the right-hand-side in power series of z shows that each coefficient of the development is a rational function of finitely many of the coefficients of $p_j(z)$. The same is true for the integral of the right-hand-side, and, therefore, the sums

$$\sum_{i=1}^{\nu} [w_i(z)]^{\sigma} , \quad \sigma = 1, 2, 3, \cdots$$

are regular power series in z , near $z = 0$, whose coefficients are rational functions of only finitely many coefficients of the $p_i(z)$. By the theory of elementary symmetric functions, the coefficients $q_i(z)$ of

$$(w - w_1)(w - w_2) \cdots (w - w_\nu) = w^{\nu} + q_1(z) w^{\nu-1} + \cdots + q_\nu(z)$$

also have the just-mentioned property of the sums.

We now observe that

$$Q(w,z) = \frac{P(w,z)}{(w-w_1)(w-w_2) \cdots (w-w_\nu)}$$

is regular in $|w| \leq \rho$ for each single z from $|z| < \delta$. At each point z either the numerator and denominator are regular and the denominator is not zero, or the numerator and denominator have vanishing factors of the same multiplicity. For each single z from $|z| < \delta$ we have

$$Q(w,z) = \frac{1}{2\pi i} \int_{|t|=\rho} \frac{Q(t,z)}{t-w}\, dt .$$

Since $Q(t,z)$ is regular in $|z| < \delta$ for t on $|t| = \rho$, we conclude that $Q(w,z)$ is regular in $|z| < \delta$ for each w from $|w| < \rho$. The above remarks show that $Q(w,z)$ is an analytic function of <u>both</u> variables in $|z| < \delta, |w| < \rho$. The development in powers of w of $Q(w,z) = \sum_{j=0}^{\infty} Q_j(z) w^j$ has coefficients $Q_j(z) = \frac{1}{2\pi i} \int_{|t|=\rho} \frac{Q(t,z)}{t^{j+1}}\, dt$.

If we develop $Q(t,z)$ on $|t| = \rho$ in powers of z, then the coefficients of the corresponding power series will be rational functions of only finitely many of the coefficients of $p_i(z)$. (This follows from the consideration of the quotient

$$Q(w,z) = \frac{p_0(z)\, w^k + \cdots + p_k(z)}{w^\nu + \cdots + q_\nu(z)} .)$$

Hence the coefficients of the power series of $Q_j(z)$ in z are rational functions of finitely many of the $p_i(z)$. We finally have $Q(0,0) = b_0 \neq 0$. Thus the Preparation Theorem is proved up to the remark that Q is a polynomial in w of degree $k-\nu$. **Q. E. D.**

We now prove the following theorem:

<u>Theorem 18.</u> Let

$$F(v,u) = v^k + F_1(u)\, v^{k-1} + \cdots + F_k(u)$$

be a polynomial of k th degree with coefficients $F_j(u)$ which are power series in u near $u = 0$ with only finitely many terms of negative order. Then there exists a natural number q such that $F(v,u)$ can be decomposed into k linear factors,

$$F(v,u) = \prod_{1}^{k} (v - v_j(u)),$$

where the $v_j(u)$ are power series in $u^{\frac{1}{q}}$, with only finitely many terms of negative order, which are convergent in a neighborhood of $u = 0$. The coefficients of these power series are algebraic functions of only finitely many of the coefficients of the power series $F_i(u)$.

The earlier-given theorem on polynomials reduces to the present theorem if we take $v = y$, $u = \frac{1}{\theta}$ and set $F(v,u) = \dfrac{\Phi(v,\frac{1}{u})}{A_0(\frac{1}{u})}$.

<u>Proof.</u>

Let $K(u)$ be the field of all power series in u with only a finite number of terms of negative order whose coefficients are algebraic functions of only finitely many coefficients of the power series $F_j(u)$. The coefficients

$F_j(u)$ of $F(u,v)$ belong to this field. If we adjoin to this field a root $u^{\frac{1}{\omega}}$ of u, with an integer ω, we obtain the field $K(u^{\frac{1}{\omega}})$ of all power series in $u^{\frac{1}{\omega}}$ with only a finite number of terms of negative order and with coefficients which are algebraic functions of only finitely many of the coefficients of the power series $F_j(u)$.

We can assume $F_1 \equiv 0$ (because if $F_1 \not\equiv 0$ we can introduce a new variable $v + \frac{F_1(u)}{k}$; then the new equation will still have its coefficients in $K(u)$). Now if $F_j(u) \equiv 0$ for all j, then $F(u,v)$ is already decomposed into linear factors. If $F_i(u) \not\equiv 0$ for some i, then let $a_i u^{\rho_i}$ be the term of lowest order in the power series $F_i(u)$ with $a_i \neq 0$. Let χ be the smallest among the numbers ρ_i/i for all $F_i(u) \not\equiv 0$, and let $\frac{\rho_i}{i} = \chi$ for $i = i_1, i_2, \dots, i_e$ with $i_1 < i_2 < \dots < i_e$. Then we always have $\rho_i - i\chi \geqslant 0$ and the equality is obtained only for $i = i_1, i_2, \dots, i_e$. We now set

$$v = y u^{\chi}$$

and write

$$F(v,u) = u^{\chi k}\left(y^k + F_1(u) u^{-\chi} y^{k-1} + \dots + F_k(u) u^{-\chi k}\right).$$

If $\chi = \frac{r}{s}$ with $s \geqslant 1$ and with $(r,s) = 1$ set $z = u^{\frac{1}{s}}$ and obtain $F(v,u) = u^{\chi k}\phi(y,z)$

$$\phi(y,z) = y^k + B_1(z) y^{k-1} + \dots + B_k(z)$$

where $B_1(z) \equiv 0$ and the $B_i(z)$ are power series from $K(z)$ and are regular at $z = 0$. The term of lowest order in $B_i(z)$ is

$$a_i z^{s(\rho_i - i\chi)} = a_i z^{s(\rho_i - r_i)}$$

where the exponent of z is always non-negative (equal to zero only for $i = i_1, i_2, \dots, i_e$). Thus we have

$$\phi(y,z) = y^k + a_{i_1} y^{k-i} + \dots + a_{i_e} y^{k-i_e} + z\,\phi^*(y,z),$$

where $\phi^*(y,z)$ is again a polynomial in y with coefficients from

$K(z)$, which are regular at $z=0$. The polynomial

$$\varphi(y) = y^{k} + a_{i_1} y^{k-i_1} + \dots + a_{i_\ell} y^{k-i_\ell}$$

has at least two terms which are not identically zero; since the coefficient of y^{k-1} is zero, $\varphi(y)$ is not a power of some linear factor. Thus $\varphi(y)$ has at least two distinct roots. Let α be one of them with multiplicity $\nu < k$. Set $y - \alpha = w$. Then

$$\varphi(y) = w^{\nu}(b_0 + \dots + b_{k-\nu} w^{k-\nu}), \quad b_0 \neq 0, \quad \nu < k,$$

where the b_j are constants from $K(u)$. We have

$$\phi(y,z) = P(w,z) = w^{\nu}(b_0 + \dots + b_{k-\nu} w^{k-\nu}) + z\,\phi^{**}(w,z),$$

where the coefficients of the polynomial $\phi^{**}(w,z)$ in w are again elements of the field $K(z)$ and are regular at $z=0$. We now apply Weierstrass' Preparation Theorem to $P(w,z)$ and obtain

$$P(w,z) = \left[w^{\nu} + q_1(z)\, w^{\nu-1} + \dots + q_{\nu}(z)\right] Q(w,z)$$

where the $q_j(z)$ designate power series from $K(z)$ which are regular at $z=0$ and vanish there. According to our presentation of the proof of the Preparation Theorem, $Q(w,z)$ is a regular power series near $w = z = 0$. We have $Q(0,0) = b_0 \neq 0$ and the coefficients $a_j(z)$ in the formula $Q(w,z) = \sum_{0}^{\infty} Q_j(z)\, w^j$ are elements of $K(z)$, regular at $z=0$.

We will proceed by induction: Assume that the theorem holds for all polynomials of degree less than k (For $k=1$, it is trivially true). Since $\nu < k$, there exists a natural number t and power series

$$w_1, w_2, \dots, w_{\nu}$$

from $K(z^{t})$, such that

$$w^{\nu} + q_1 w^{\nu-1} + \dots + q_{\nu}(z) = \prod_{1}^{\nu}(w - w_j).$$

Hence $$P(w,z) = \prod_{1}^{\nu}(w - w_j)\, Q(w,z).$$

If we divide, in the field $K(z^{t})$, both sides of the above equation by the polynomial $\prod_{1}^{\nu}(w-w_j)$, which has coefficients in $K(z^{\frac{1}{t}})$, we obtain, on the left-hand-side, a polynomial of degree $k-\nu$ in $K(z^{\frac{1}{t}})$, which is equal to the function $Q(w,z)$ on the right-hand-side. This function is also a polynomial in w and of degree *less than* k, with coefficients from $K(z)$. Thus we can, by using the induction hypothesis, decompose this polynomial in a field $K(z^{\frac{1}{\tau}})$ with a new natural number τ. Therefore $\phi(w,z)$ is decomposed into linear factors and indeed in a field obtained from $K(u)$ through a multiple adjunction of "roots". This multiple adjunction is obviously equivalent to a single adjunction of $u^{\frac{1}{q}}$ for some integer $q > 0$. Thus the proofs of the theorem on Polynomials and Weierstrass' Preparation Theorem are complete.

6. Liouville, Generalized Liouville, and Picard-Vessiot Extensions of Differential Fields, and Solvability of Differential Equations.

For the remainder of the course we follow the book of Kaplansky very closely.

Definition. Let K be a differential field and M a differential field extension. We say that M is a Liouville extension of K in case there exists a finite chain of intermediate differential fields

$$K = K_1 \subset K_2 \subset \cdots \subset K_n = M$$

Each differential field is either an adjunction of an integral, or an adjunction of the exponential of an integral, of the preceding differential field of the chain.

Remark. A generalized Liouville extension M of K allows intermediate fields which are finite algebraic extensions as well as adjunction of integrals and exponentials of integrals. From now on we shall require that *M has the same constant field C as has K* and that *C is algebraically closed.*

We take these as standing hypotheses for the remainder of the course.

Definition. Let

$$L(y) = y^{(n)} + a_1 y^{(n-1)} + \cdots + a_{n-1} y' + a_n y = 0$$

be a linear homogeneous differential equation with coefficients in a differential field K. We say that a differential field M containing K is a Picard-Vessiot extension of K (for the linear equation $L(y) = 0$) in case:

1) $M = K < u_1, \ldots, u_n >$ where $u_1, \ldots, u_n$ are n solutions of $L(y) = 0$, linearly independent over the constant field C, and

2) M has the same constant field (algebraically closed) C as has K.

Note. If $M \supset K$ is a differential field extension, and S is a subset of M, then $K < S >$ means the smallest differential subfield of M containing all the elements of $K \cup S$. The phrase "linearly independent over C" does not depend on the superfield M because of the following theorem.

Theorem 19. Let F be a differential field with constant field C. Then n elements of F are linearly independent over C if and only if the Wronskian vanishes,

$$W(y_1, y_2, \cdots, y_n) = \begin{vmatrix} y_1, & y_2, & \cdots, & y_n \\ y_1', & y_2', & \cdots, & y_n' \\ \vdots & \vdots & & \vdots \\ y_1^{(n-1)}, & y_2^{(n-1)}, & \cdots, & y_n^{(n-1)} \end{vmatrix} = 0.$$

Proof. Easy.

Remark. In C^∞ the above theorem does not hold — but C^∞ is not a differential field.

Remark. It is known that there exists a unique (up to a differential isomorphism over K) Picard-Vessiot extension M of K for each linear differential equation $L(y)=0$. See Kaplansky, Differential Algebra, p. 21-22.

Definition. Let

$$L(y) = y^{(n)} + a_1 y^{(n-1)} + \dots + a_{n-1} y' + a_n y = 0$$

be a differential equation with coefficients in a differential field K . We say that $L(y)=0$ is solvable in elementary functions in case its Picard-Vessiot extension M of K lies in some generalized Liouville extension (with constant field C of K) of K .

We say that $L(y)=0$ is solvable by integrals and exponentials in case M lies in some Liouville extension (with constant field C of K) of K .

Remark. Let $L(y)=0$ be linearly irreducible over K , that is, L is not the product (composition) of two linear differential operators with coefficients in K . It is known that if $L(y)$ is linearly irreducible over K and has one (non-zero) solution in a generalized Liouville extension of K , then $L(y)=0$ is solvable in elementary functions. If $L(y)$ is linearly irreducible over K and has one (non-zero) solution in a Liouville extension of K , then $L(y)=0$ is solvable by integrals and exponentials.

7. Galois Group and Galois Correspondence.

Definition. Let M be a differential field extension of K . The differential Galois group G of M over K is the group of all differential automorphisms of M leaving K elementwise fixed.

Definition. Let M be a differential field extension of K and let G be the differential Galois group of M over K. For each intermediate differential field L ($M \supset L \supset K$) define L' to be the subgroup of G which is the differential Galois group of M over L. For each subgroup H of G define H' as the intermediate differential field of all elements of M left fixed by H. Every Galois group of an intermediate field, that is L', is called closed. Every fixed field under a subgroup of G, that is H', is called closed.

Note. For the identity $e \in G$ we have $e' = M$ and $M' = e$, and also $K' = G$ so M, G and e are closed. The intersection of two closed subgroups of G is closed.

Theorem 20. Let M be a differential field extension of K with differential Galois group G. For each closed intermediate differential field H' we correspond the differential Galois group H'' of M over H'. This correspondence, known as the Galois correspondence, is a one-to-one map of the set of all closed intermediate differential fields between M and K onto the set of all closed subgroups of the differential Galois group G of M over K. If $H_1' \supset H_2'$ are closed fields, then $H_1'' \subset H_2''$ and if $L_1' \supset L_2'$ are closed groups then $L_1'' \subset L_2''$.

Proof.

Let L' be a closed subgroup of G, that is, L' is the Galois group of an intermediate differential field L. Consider the fixed field L'' under L'. Then L' is also the Galois group of the closed field L''. That is $L' = L'''$ and the Galois correspondence is onto the set of all closed subgroups of G.

Now let H_1' and H_2' be two closed intermediate differential fields, which are the fixed fields under groups H_1 and H_2, respectively. The Galois groups of H_1' and H_2' are H_1'' and H_2'', respectively. Suppose $H_1'' = H_2''$. Now H_1' and H_2' are the fixed fields under H_1'' and H_2'', respectively, so $H_1' = H_1'''$ and $H_2' = H_2'''$. But $H_1''' = H_2'''$ and hence $H_1' = H_2'$. This shows that the Galois correspondence is one-to-one. It is trivial that the Galois correspondence reverses the partial ordering relation of inclusion.

Q. E. D.

<u>**Definition**</u>. Let M be a differential field extension of K with differential Galois group G. We say that M is normal over K in case every intermediate differential field is closed; that is, if L is a differential field $M \supset L \supset K$, and $v \in M - L$ then there exists $\sigma \in G$ such that σ is the identity on L but $\sigma v \neq v$.

<u>**Note.**</u> In ordinary algebra we say M is normal over K in case K is closed, and then we prove that each intermediate field is closed.

<u>**Remark**</u>. We shall later prove that every Picard-Vessiot extension is normal.

<u>**Theorem 21**</u>. Let M be a differential field extension of K with differential Galois group G. Assume

1.) M is normal over K

2.) The intersection of every collection of closed subgroups of G is a closed subgroup.

Then the set of all closed subgroups of G forms a lattice $\mathcal{G}$ under inclusion with

$$g.l.b.(H_1, H_2) = H_1 \cap H_2$$ (intersection)

$$l.u.b.(H_1, H_2) = H_1 \cup H_2$$ (intersection of all closed subgroups of G containing both H_1 and H_2).

The set of all intermediate differential fields similarly forms a lattice $\mathcal{F}$. The Galois correspondence is a dual lattice isomorphism of $\mathcal{F}$ onto $\mathcal{G}$. That is,

$$L_1 \subset L_2 \text{ implies } L_1' \supset L_2'$$

$$[L_1 \cup L_2]' = L_1' \cap L_2'$$

$$[L_1 \cap L_2]' = L_1' \cup L_2'$$

and $M' = e$, $G' = K$

Proof. Trivial.

8. Examples of the Galois Group of a Picard-Vessiot Extension.

Theorem 22. Let K be a differential field with an algebraically closed constant field C . Let M be a Piard-Vessiot extension of K , for $L(y) = y^{(n)} + a_1 y^{(n-1)} + \dots + a_n y = 0, a_i \in K$, with differential Galois group G . Then G is a subgroup of $GL(n, C)$, the $n \times n$ nonsingular matrices with elements from C .

Proof.

Let $u_1, u_2, \dots, u_n$ be a fundamental solution set for $L(y) = 0$ and write $M = K < u_1, u_2, \dots, u_n >$.

Here $u_1, u_2, \dots, u_n$ are linearly independent over C .

Write $L(y) = y^{(n)} + a_1 y^{(n-1)} + \dots + a_n y$ with $a_i \in K$.

If $v_1, v_2, \dots, v_n, v_{n+1}$ are solutions of $L(y) = 0$ then we have $n+1$ linear equations for the coefficients $1, a_1, \dots, a_n$. Thus the determinant of the linear system vanishes, or

$$W(v_1, v_2, \dots, v_n, v_{n+1}) = 0 .$$

Thus $v_1, v_2, \dots, v_n, v_{n+1}$ are linearly dependent over C .

Now take $\sigma \in G$. Then σu_i is a solution of $L(y) = 0$ so $\sigma u_i = \sum_{j=1}^{n} c_{ij} u_j$ where $c_{ij} \in C$. Thus we map $G \rightarrow GL(n, C)$

by $\sigma \to (c_{ij})$. This is an isomorphism into $GL(n,C)$ since the assignment of the images of the u_i fixes the automorphism of M over K.

Q. E. D.

Theorem 23. Let K be a differential field with algebraically closed constant field C. Consider any element $a \in K$ which is not a derivative. Consider the differential equation

$$L(y) = y'' - \left(\frac{a'}{a}\right) y' = 0 .$$

The Picard-Vessiot extension M of K for $L(y) = 0$ is the adjunction of the integral u of a. Hence $M = K\langle u \rangle$ and the differential Galois group G is isomorphic to the additive group of constants of C.

Proof.

Consider the differential field $K\langle u \rangle$ obtained by the adjunction of an integral of a. Then in $K\langle u \rangle$ we find a solution basis for $L(y) = 0$, namely, $u, 1$. Thus $M = K\langle u \rangle$ is the Picard-Vessiot extension of K for $L(y) = 0$.

Let $\sigma \in G$. Now $u' = a$ and hence $(\sigma u)' = a$. Thus $\sigma u - u = c \in C$, or $\sigma u = u + c$. For $\tau \in G$ we compute $\tau u = u + c_1$, and $\tau(\sigma u) = \tau(u+c) = u + c_1 + c$. Thus we have a homomorphism of G into C_+, the additive group of C. But if $\sigma u = u$, then $\sigma 1 = 1$ and σ is the identity of G. Hence $G \to C_+$ is an isomorphism. For each $c \in C$ there exists an automorphism $\sigma \in G$ for

$$\sigma u = u + c$$
$$\sigma 1 = 1$$

is easily verified to be an automorphism of M over K. This is known since $K\langle u \rangle$ is merely the transcendental extension of K with the differentiation defined by $u' = a$. Q. E. D.

Theorem 24. Let K be a differential field with algebraically closed constant field C. Consider the Picard-Vessiot extension M of K for

$$L(y) = y' - ay = 0 \quad , \quad a \neq 0 \quad \text{in } K .$$

Then M is the adjunction of K by u, the exponential of the integral of a, $M = K<u>$. The differential Galois group G of M over K is isomorphic with a subgroup of the multiplicative group of non-zero constants in C.

Proof.

Consider the differential field $K<u>$, where $u' = au$, and $u \neq 0$. Then $K<u>$, which might be just K, is the Picard-Vessiot extension of K for $L(y)$.

Take $\sigma \in G$. Then $\left(\frac{\sigma u}{u}\right)' = 0$ so $\sigma u = cu$ with $c \in C$. This defines an isomorphism of G into the multiplicative group of non-zero constants of C. Q. E. D.

Example. Consider K as the rational functions of a complex variable z with complex coefficients.

For $L(y) = y' - ay = 0$ where $a \in K$ we have a Picard-Vessiot extension generated by $v = e^{\int a}$ over K, with differential Galois group G. This differential equation can also be considered on the Riemann sphere and we compute the monodromy group Ψ. Note Ψ is a subgroup of G.

1.) $y' = y$. Here G is the multiplicative group of all non-zero complex numbers and $\Psi = 1$.

2.) $y' = \frac{r}{z} y$ so $y = e^{r \ln z} = z^r$. If $r = \frac{1}{p}$ for a positive prime p, then both Ψ and G are isomorphic with the multiplicative group of p-th roots of unity.

3.) $y' = \frac{r}{z} y$ with r a real irrational. Then Ψ is the multiplicative group of complex numbers $e^{2\pi i r n}$ $n = 0, \pm 1, \pm 2, \cdots$ which is isomorphic with $\mathbb{Z}$. But G is isomorphic with the multiplicative group of all non-zero complex numbers.

9. Ideals and Algebraic Varieties. Zariski Topology.

Definition. A differential ring A is a commutative ring with unit and a derivation satisfying

$$(a+b)' = a' + b'$$
$$(ab)' = a'b + ab'$$

Remark. If A has no zero divisors, A is a differential integral domain and there is a unique extension of the derivation to the quotient field.

Remark. By defining $a' = 0$ we can consider the theory of uniqueness as a special case of differential rings.

Definition. A subring I of a differential ring A is a differential subring if $I' \subset I$. If I is an ideal with $I' \subset I$, then I is a differential ideal. Differential isomorphisms, homomorphisms and automorphisms are defined to commute with differentiation.

Example. The subring C of constants of A is a differential ring and contains 1 .

Theorem 25. Let I be the kernel of a differential homomorphism defined on a differential ring A . Then I is a differential ideal in A and the quotient ring $A \to A/I$ is differential-isomorphic to the image.

Definition. Let A be a differential ring. A differential ideal I is maximal if A/I is a field; I is prime if A/I is an integral domain.

Definition. Let A be a differential ring and let S be a differential ideal. The radical T of S is the set of all $a \in A$ with $a^n \in S$ for some integer $n > 0$. An ideal I is radical in case I is its own radical, that is, $x^n \in I$ implies $x \in I$.

The intersection of any collection of radical differential ideals in a differential ring A is itself a radical differential ideal. Thus if S is a subset of A define $\{S\}$ as the smallest radical differential ideal containing S.

Lemma 1. If ab lies in a radical differential ideal I, then $ab' \in I$ and $a'b \in I$.

Proof.

Now $(ab)' = a'b + ab' \in I$. Multiply by ab' to find $(ab')^2 \in I$ so $ab' \in I$. Q. E. D.

Lemma 2. Let I be a radical differential ideal in a differential ring A, and let S be a subset of A. Define T as the set of all $x \in A$ with $xS \subset I$. Then T is a radical differential ideal in A.

Proof.

Now it is easy to see that T is an ideal and hence, by lemma 1, a differential ideal. Suppose $x^n \in T$. Then for any $s \in S$ we have $x^n s^n \in I$ so $xs \in I$ and $x \in T$.

Q. E. D.

Lemma 3. Let $a \in A$ and S a subset of a differential ring A. Then $a\{S\} \subset \{aS\}$.

Proof.

The set of all $x \in A$ with $ax \in \{aS\}$ is, by lemma 2, a radical differential ideal T. Since T contains S, T contains $\{S\}$. Since $aT \subset \{aS\}$ we have $a\{S\} \subset \{aS\}$.

Q. E. D.

Lemma 4. Let S and T be subsets of a differential ring A. Then $\{S\} \cdot \{T\} \subset \{ST\}$.

Proof.

Here the product of two ideals is the smallest ideal containing all the products of their elements. The set of all x with $x\{T\} \subset \{ST\}$ contains S by lemma 3 and is a radical differential ideal by lemma 2, and hence it contains $\{S\}$. Q. E. D.

Theorem 26. Let I be a radical differential ideal in a differential ring A. Then I is an intersection of prime differential ideals.

Proof.

Now A is prime so assume $A - I$ is not empty. Take $x \in A - I$. We shall produce a prime differential ideal containing I but not x. Take T as the set of all powers of x. By Zorn's lemma select a radical differential ideal Q containing I and maximal with respect to the exclusion of T.

We show that Q is prime. Suppose $ab \in Q$ with $a \notin Q$ and $b \notin Q$. Then the intersection of all radical differential ideals containing Q and a, $\{Q, a\}$, and also $\{Q, b\}$ are each radical differential ideals properly containing Q. Hence they contain elements of

T , say t_1 and t_2 , respectively.

We have, by lemma 4, $t_1 t_2 \in \{Q,a\}\cdot\{Q,b\} \subset \{Q\} = Q$.

This states that a power of x lies in Q and hence $x \in Q$ which is a contradiction. Thus Q is prime.

Q. E. D.

Definition. A Ritt algebra is a differential ring containing the field of rational numbers in the subring of constants.

Theorem 27. In a Ritt algebra A the radical T of a differential ideal I is a differential ideal.

Proof.

Take $a \in T, b \in T$ so $a^n \in I$, $b^m \in I$. Use the binomial theorem to show that $(a+b)^{m+n} \in I$. Also for $\alpha \in A$ we find $(a\alpha)^n = a^n \alpha^n \in I$, so T is an ideal containing I .

Now

$$(a^n)' = n a^{n-1} a' \in I$$

. Thus $a^{n-1} a' \in I$.

Proceed by induction to prove $a^{n-k}(a')^{2k-1} \in I$ for $k < n$. Differentiate this hypothesis to get $(n-k)a^{n-k-1}(a')^{2k-1} + (2k-1)a^{n-k}(a')^{2k-2}a'' \in I$. Thus $(n-k)a^{n-k-1}(a')^{2k-1} \in I$ and so $a^{n-k-1}(a')^{2k+1} \in I$, as required. For $k = n-1$ we get $(a')^{2n-1} \in I$ so T is a differential ideal.

Q. E. D.

Now we return to ordinary algebra without derivations. Let F be a field and V an n-dimensional vector space over F , that is, all n-tuples of elements of F . Let $F[x_1, x_2, \ldots, x_n]$ be the polynomial ring in n indeterminants over F .

Definition. An algebraic variety M of a finite set of polynomials $P_1, \dots, P_r$ of $F[x_1, \dots, x_n]$ is the set of all points of V which are zeros of all these polynomials. Note that M is the locus of zeros of the ideal I in $F[x_1, \dots, x_n]$ generated by $P_1, \dots, P_r$.

Remark. The Hilbert Nullstellen Satz states that the set of all polynomials which vanish on M is precisely the radical of I.

Remark. Each ideal I in $F[x_1, \dots, x_n]$ has a finite basis (Hilbert) and hence the locus in V of points which annihilate I is an algebraic variety.

Remark. Given ideals I_1 and I_2 in $F[x_1, \dots, x_n]$ and corresponding algebraic varieties $M(I_1)$ and $M(I_2)$ in V, If $I_1 \subset I_2$, then $M(I_1) \supset M(I_2)$.

Theorem 28. In V define a subset S to be closed in case S is an algebraic variety of some ideal in $F[x_1, \dots, x_n]$. Then V is a T_1-topological space with this Zariski topology.

Proof.

Let S_1 and S_2 be algebraic varieties for ideals I_1 and I_2 of $F[x_1, \dots, x_n]$, respectively. Then $S_1 \cup S_2$ is the algebraic variety of the ideal $I_1 \cap I_2$. Also $S_1 \cap S_2$ is the algebraic variety of the ideal $I_1 + I_2$.

Now let S_α be a family of algebraic varieties of the ideals I_α. By the Hilbert basis theorem $\bigcap S_\alpha$ is the algebraic variety of an ideal in $F[x_1, \dots, x_n]$.

For, well-order S_α as $S_1, S_2, S_3, \dots$ and define the intersection as the limit of S_1, $S_1 \cap S_2$, $S_1 \cap S_2 \cap S_3, \dots$. The corresponding ideals are $J_1 \subset J_2 \subset J_3 \subset \cdots$. By the Hilbert basis theorem (finite ascending chain condition) $J_m = J_{m+1} = J_{m+2}$ etc. Thus $\bigcap S_\alpha = S_1 \cap S_2 \cap \cdots \cap S_m$ is the algebraic variety of the ideal J_m.

Since a hyperplane can be passed through one prescribed point so as to avoid a different prescribed point, V is a T_1-space.

Q. E. D.

Definition. A T_1-space with the finite descending chain condition on closed sets (or a finite ascending chain condition on open sets) is a Zariski-space.

Theorem 29. Every subspace of a Z-space is a Z-space. If a T_1-space is the continuous image of a Z-space, then it is itself a Z-space. A Hausdorf Z-space is finite. A Z-space is the union of a finite number of disjoint connected subsets which are both open and closed.

10. Algebraic Matrix Groups.

Definition. A C-group G is a group and a T_1-space such that each left multiplication, right multiplication, and inversion are homeomorphisms of G onto G; and the map $a \rightarrow a^{-1} x a$, for each fixed $x \in G$, is continuous.

Theorem 30. Let F be a field and V the n^2-dimensional vector space over F. Consider $GL(n,F)$ coordinatized by V. Then $GL(n,F)$ is a Z-space and a C-group.

Proof.

Since the determinant is a polynomial in the entries of a matrix, $GL(n,F)$ is an open subset of the Z-space V. Thus $GL(n,F)$

is a Z-space.

Let X be a fixed nonsingular matrix and consider the map of $GL(n,F)$ onto itself by $A \to XA$. An algebraic variety M for an ideal I in $F[x^1, \cdots, x^{n^2}]$ defines a closed set $M \cap GL(n,F)$ in the matrix space. The set of all matrices A such that XA lies in M is $X^{-1}M$ and this is an algebraic variety. Thus it is easy to see that left and right multiplications of $GL(n,F)$ are continuous and hence are homeomorphisms of the Z-space $GL(n,F)$.

Now consider the inverse map $A \to A^{-1}$ of $GL(n,F)$ onto itself. This and the map $A \to A^{-1}XA$ for fixed $X \in GL(n,F)$ are continuous as follows from the lemma below.

Lemma. Let V and W be m-dimensional and n-dimensional vector spaces of F, and consider the Zariski topology. Let $r_1, \cdots, r_n$ be rational functions in m-variables $x_1, \cdots, x_m$. Let S be the set where any denominator of any one of the $r_1, \cdots, r_n$ vanish and let T be the complement of S in V. Then the map from T into W, $(x_1, \cdots, x_m) \to (y_1, \cdots, y_n)$, $y_i = r_i(x_1, \cdots, x_m)$ is continuous.

Proof.

A closed set in W consists of the common zeros of a finite set of polynomials $g_j(y_1, \cdots, y_n)$. The inverse image consists of all common zeros in T of the rational functions $g_j(r_1, \cdots, r_m)$ which is the same as the set of common zeros of their numerators. This set in T is closed in the Zariski topology. Thus the theorem is proved.

Q. E. D.

Definition. Let F be a field and consider $GL(n,F)$ as a Z-space and C-group. An algebraic matrix group G over F is a closed subgroup of $GL(n, F)$. Hence an algebraic matrix group is a C-group and Z-space, that is, a CZ-group.

Theorem 31. Let G be an algebraic group over a field F . Let G_1 be an abstract subgroup of G . Then $\overline{G}_1$ is a closed subgroup of G. If G_1 is abelian or normal, then $\overline{G}_1$ is abelian or normal, respectively.

Proof. (This holds for any C-group.)

We must first show that the closure $\overline{G}_1$ of G_1 , in the Zariski topology, is an abstract subgroup of G . For each $h \in G_1$ the map $x \rightarrow hx$ is a homeomorphism of G onto itself. Hence the inverse image of $\overline{G}_1$ is closed and contains G_1 so it contains $\overline{G}_1$, that is, $h\overline{G}_1 \subset \overline{G}_1$. Again take t in $\overline{G}_1$ and consider the inverse image of $\overline{G}_1$ under the map $x \rightarrow xt$. This image contains G_1 and is closed so it contains $\overline{G}_1$. Thus $\overline{G}_1\overline{G}_1 \subset \overline{G}_1$. Since the inverse map is continuous $\overline{G}_1^{-1}$ is closed and contains G_1 so $\overline{G}_1^{-1} \subset \overline{G}_1$. Thus $\overline{G}_1$ is a closed subgroup of G.

Let G_1 be normal in G . Then, for a fixed $a \in G$, $a\overline{G}_1a^{-1}$ is closed and contains G_1 and hence it contains $\overline{G}_1$. Thus $a^{-1}\overline{G}_1a \subset \overline{G}_1$ so $\overline{G}_1$ is normal in G .

Let G_1 be commutative. For a fixed $b \in G_1$ the map $a \rightarrow (aba^{-1})b^{-1}$ is continuous for G into G . The inverse image of $e \in G$ is closed and contains $\overline{G}_1$. But the mapping $b \rightarrow a(ba^{-1}b^{-1})$ is continuous, for a fixed $a \in \overline{G}_1$. Again the inverse image of $e \in G$ is closed and contains $\overline{G}_1$. Thus $\overline{G}_1$ is commutative.

Q. E. D.

Corollary. A C-group G modulo a closed normal subgroup G_1 is a C-group. If G is also a Z-space, so is G/G_1 .

Theorem 32. Let G be an algebraic group over a field F. The component G_0 of the identity of G is a closed normal subgroup of finite index.

Proof.

The component of the identity G_0 is a closed subset of G. Now G_0^{-1} is connected and contains $e \in G$. Hence $G_0^{-1} \subset G_0$. For $g \in G_0$ we have $g G_0$ is connected and contains g so $g G_0 \subset G_0$. Thus G_0 is a closed subgroup of G. For any x in G, $x^{-1} G_0 x$ is connected and contains e so $x^{-1} G_0 x \subset G_0$ and G_0 is normal.

Since G is the union of a finite number of disjoint open and closed connected subsets, each of these is a coset of G_0. Thus G_0 has a finite index in G. Q. E. D.

Theorem 33. Let G be an algebraic group over a field F. The normalizer of a closed subgroup G_1 is closed.

Proof.

The normalizer of G_1 is the subgroup of G consisting of elements x such that $x G_1 x^{-1} \subset G_1$ and $x^{-1} G_1 x \subset G_1$. For a fixed $g \in G_1$ consider the map $a \to a g a^{-1}$. The inverse image of G_1 is closed and consists of all a with $a g a^{-1} \in G_1$. Take the intersection of these closed sets for all $g \in G_1$. Then the set of $a \in G$ with $a G_1 a^{-1} \subset G_1$ is closed. Likewise the set of $a \in G$ with $a^{-1} G_1 a \subset G_1$ is closed. The intersection of these two closed sets is the normalizer of G_1.

Q. E. D.

11. Solvable Algebraic Matrix Groups.

In an abstract group G the commutator subgroup G_1 is the smallest subgroup containing all the commutators $aba^{-1}b^{-1}$. Now G_1 is normal and

G/G_1 is abelian, in fact, G_1 is the intersection of all normal subgroups such that the factor group is abelian. We form the sequence of commutator subgroups $G \supset G_1 \supset G_2 \supset \cdots \supset G_i \supset \cdots$ where G_{i+1} is the commutator of G_i. All the G_i are normal in G.

Definition. An abstract group G is solvable in case the sequence of commutator subgroups terminates with $e \in G$ after a finite number of steps.

If G contains a finite sequence of subgroups $G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(n)} = e$ each normal in the preceding group and such that $G^{(K)}/G^{(K+1)}$ is commutative, then G is solvable. A subgroup and a homomorphic image of a solvable group are also solvable.

Definition. A C-group G is topologically solvable if there exists a finite chain $G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$ of closed subgroups, each normal in its predecessor, and such that G_i/G_{i+1} is abelian.

Note. For an algebraic group G over a field F define the algebraic commutator as the closure of the commutator group. Then G is topologically solvable if and only if the sequence of algebraic commutator subgroups terminates with 1. If F is algebraically closed it is known that the commutator subgroup of G is itself closed.

Lemma. In a C-group the closure of a solvable group is solvable.

Proof.

Let G be a C-group, H a solvable subgroup and K the closure of H. Let $H = H_1 \supset H_2 \supset \cdots \supset H_n = 1$ be the derived series of H and let K_i be the closure of H_i. We show that K_i contains the commutator subgroup of K_{i+1}.

For a fixed $b \in H_i$ the map $a \rightarrow aba^{-1}b^{-1}$ of G into G is continuous. The inverse image of K_{i+1} contains H_i and hence it contains K_i, that is, $k_i h_i k_i^{-1} h_i^{-1} \in K_{i+1}$. Next fix $a \in K_i$. The map $b \rightarrow aba^{-1}b^{-1}$ is continuous on G into G. The inverse image of K_{i+1} contains H_i and hence it contains K_i. Hence K_{i+1} contains all the commutators of K_i.

Hence K_i/K_{i+1} is abelian and thus K is solvable as an abstract group.

Q. E. D.

Theorem 34. A C-group G is solvable if and only if G is topologically solvable.

Proof.

If the group G is topologically solvable, then G is solvable as an abstract group.

Conversely suppose the commutator subgroups of the abstract group G are $G = G_0 \supset G_1 \supset \cdots \supset G_K = 1$. Then G_{K-1} is an abelian normal subgroup of G. The closure of G_{K-1} is H, an abelian normal subgroup of G. The group G/H is again a C-group and its derived series is shorter than that of G. By induction G/H is topologically solvable. Hence G is topologically solvable.

Q. E. D.

Remark. Consider an algebraic matrix group G over a field F which is either the real or complex numbers. Then G is a real Lie group since it is a closed (in uniform norm on matrices) subgroup of $GL(n, \mathbb{C})$. If G is not solvable as a real Lie group (real Lie algebra is not solvable), then G is not topologically solvable as an algebraic group.

Note. If an algebraic matrix group G is solvable, then the component of the identity G_0 is solvable and also the factor group G/G_0 is a solvable finite group.

Lemma 1. Let G be a C-group whose component G_0 of the identity has finite index k. Then any finite conjugate class of G has at most k elements.

Proof.

Suppose there is an element $x \in G$ with a finite conjugate class, containing more than k elements. The map $a \to a^{-1} x a$ is continuous. The inverse image of each conjugate is open and closed. This yields a decomposition of G into more than k open and closed sets, which is a contradiction. Q. E. D.

Lemma 2. In a connected C-group, any non-central element has an infinite conjugate class.

Theorem 35. If G is a connected C-group, the commutator subgroup G' is connected.

Proof.

Write $D_0 = e$ and D_K for the set of all products of K-commutators in G. Then $D_0 \subset D_1 \subset D_2 \subset \cdots$ and $G' = \bigcup_0^\infty D_K$. Consider the mapping $a_1 \to a_1^{-1} b_1^{-1} a_1 b_1 a_2^{-1} b_2^{-1} a_2 b_2 \,.\,.\,, a_K^{-1} b_K^{-1} a_K b_K$, for G into G, with all elements other than a_1 fixed. The map is continuous and so the image is connected. The image has a point in common with D_{K-1}, obtained when $a_1 = b_1$.

Assume $D_0, \ldots, D_{K-1}$ are connected as an induction hypothesis. But we have expressed D_K as the union of connected sets each having a point in common with $D_{k-1} \subset D_k$. Hence D_k is connected.

Q. E. D.

Lemma. Let G be a C-group, H a closed subgroup of G. Suppose either

1) H is of finite index in G

or 2) H is normal and G/H is abelian.

If the component H_0 of the identity in H is solvable, then so is the component G_0 of the identity in G.

Proof.

In case 1) $H_0 = G_0$. In case 2) write G' and G_0' for the commutator subgroups of G and G_0, respectively. Then H contains G' and hence H contains G_0'. But G_0' is connected. Hence $G_0' \subset H_0$. Since H_0 is solvable, G_0' is solvable, and so G_0 is solvable.

Q. E. D.

Theorem 36. Let G be an algebraic matrix group over an algebraically closed field F. Assume G is connected and solvable. Then G is similar (conjugate in $GL(n,F)$) to a simultaneous triangular group of matrices.

Proof.

If G is commutative then the theorem is elementary. If G is reducible (the vector space V on which G acts has a non-trivial invariant subspace), then the matrices of G have the form (in a suitable basis of V) $A_i = \begin{pmatrix} B_i & 0 \\ * & C_i \end{pmatrix}$. The maps $A_i \to B_i$ and $A_i \to C_i$ are continuous so B_i fill out a matrix group whose closure is a connected, solvable, algebraic group. By induction on the size of matrices B_i and C_i can be made triangular, which makes G triangular. Hence we assume that G is irreducible.

Let G' be the closure of the commutator subgroup of G and note that G' is connected and solvable. By induction on the length of the series of closed commutator subgroups, we may assume that G' is in triangular form.

Let W be the subspace of V spanned by all joint eigenvectors of G'. Now $W \neq 0$ is invariant under G. For let α be a joint eigenvector of G'; $T\alpha = c_T\alpha$ for all $T \in G'$. Then for any $S \in G$ we have $STS^{-1} \in G'$, $S^{-1}TS(\alpha) = c_1\alpha$, $TS\alpha = c_1 S\alpha$, so $TS(\alpha)$ is a constant multiple of $S\alpha$. Thus $S\alpha$ is a joint eigenvector of G' and $S\alpha \in W$. Since G is irreducible, $W = V$ and hence G' can be taken to consist of diagonal matrices.

An element $g \in G'$ is a diagonal matrix. The conjugates of g in G are also in G' and hence these are diagonal. Then the conjugates are obtained merely by permuting the eigenvalues. Hence g has a finite conjugate class in G and so g lies in the center of G.

Suppose there is a matrix T in G' which is not a scalar. Let c be an eigenvector of T and let W' be the set of all $\alpha \in V$ with

$$T\alpha = c\alpha .$$

Since T commutes with all G, it is easy to see that W' is invariant under all G. Hence $W' = V$ and $T = cI$, which is a contradiction. Therefore all matrices in G' are scalar.

Since G' is the closure of the commutator subgroup of G, its elements are matrices with determinant of 1. Hence the scalar values for matrices in G' must be n^{th} roots of unity. Thus G' is finite. Since G' is connected, $G' = 1$ and so G is commutative and the theorem is proved.

Q. E. D.

12. <u>The Galois Group of a Picard-Vessiot Extension Is an Algebraic Matrix Group</u>.

<u>Lemma 1.</u> Let K be a differential field with constant field C. Let $k_1, \dots, k_r$ be constants in some differential field extension of K. If $k_1, \dots, k_r$ are algebraically dependent over K, they are algebraically dependent over C.

Proof.

We have a polynomial relation $f(k_1, \dots, k_r) = 0$ with coefficients in K. Let u_β be a (Hamel) basis of K over C and write $f = \sum h_\beta u_\beta$. Here h_β are polynomials in r indeterminants with coefficients in C. Since u_β are linearly independent over constants, in K or in any differential extension of K, $h_\beta(k_1, \dots, k_r) = 0$.

Q. E. D.

<u>Lemma 2.</u> Let F be any field, I an integral domain containing F with finite transcendence degree over F. Let P be a prime ideal in I and $P \neq 0, P \neq I$. Then the transcendence degree of I/P over F is strictly less than that of I over F.

Proof.

Take a non-zero element $u \in P$. If u were algebraic over F, then the constant term in the polynomial equation for u would be in P and $1 \in P$ so $P = I$. Thus u is transcendental over F. Take $u = u_1$ as the first member of a transcendence basis $u_1, u_2, \dots, u_r$ of I. These elements map into $0, v_2, \dots, v_r$ in the integral domain I/P, which contains a homomorphic—thus isomorphic image of F (the unit of F is the unit of I and of I/P).

We show that any element $x \in I/P$ is algebraically dependent on $v_2, \dots, v_r$. Take $y \in I$ mapping onto $x \neq 0$. Then y satisfies a polynomial equation with coefficients which are polynomials in $(u_1, \dots, u_r)$. Consider

f as the polynomial of minimal degree in y which gives a value in P. Write $f(y) = r_k y^k + \cdots + r_1 y + r_0 \in P$. Mapping modulo P we get x as an algebraic combination of $v_2, \ldots, v_r$ — unless each $r_i(0, v_2, \ldots, v_r) \equiv 0$. But in this last case $r_0(u_1, \ldots, u_r) \in P$ so $(r_k y^{k-1} + \cdots + r_1) y \in P$. Since $y \notin P$, we have $r_k y^{k-1} + \cdots + r_1 \in P$ which contradicts the minimality of $f(y)$.

Q. E. D.

Lemma 3. Let K be a differential field with constant field C and let $M = K\langle u_1, \ldots, u_n\rangle$ be a Picard-Vessiot extension of K. There exists a finite set S of polynomials in n^2 (ordinary) indeterminants with coefficients in C such that:

1) every differential isomorphism of M into a superfield N, leaving K elementwise fixed, defines a matrix of constants of N satisfying S,

2) Given a differential field extension N of M, and a nonsingular matrix of constants (k_{ij}) of N satisfying S, there exists a differential isomorphism of M into N, leaving K elementwise fixed, sending $u_i \to \sum_j k_{ij} u_j$.

Proof.

Let $y_1, \ldots, y_n$ be differential indeterminants over K. Define a differential homomorphism of the integral domain $K\{y_1, \ldots, y_n\}$ into M by keeping K fixed and sending $y_i \to u_i$. The kernel Γ is a prime differential ideal in $K\{y_1, \ldots, y_n\}$.

Let c_{ij}, $i, j = 1, 2, \ldots, n$ be a set of n^2 ordinary indeterminants over M. By the map $y_i \to \sum_{j=1}^{n} c_{ij} u_j$ define a differential homomorphism of $K\{y_1, \ldots, y_n\}$ into $M[c_{ij}]$. Let Δ be the image of Γ under this map. Thus Δ is an ideal of (ordinary) polynomials with coefficients in M. Let w_α be a vector space basis of M over C . Write each polynomial in Δ as a linear combination of w_α with coefficients which are polynomials over C . The collection S of all these polynomials over C is our candidate (or a finite set of polynomials over C spanning the ideal generated by S).

1) Suppose $u_i \to \sum_{j=1}^{n} k_{ij} u_j$ is a differential isomorphism σ of M into N over K. Perform the above homomorphism from $K\{y_1, \dots, y_n\}$ into $K\{u_1, \dots, u_n\}$ followed by σ. In the product homomorphism Γ maps into zero. Again take the map given by $y_i \to \sum c_{ij} u_j$ followed by $c_{ij} \to k_{ij}$. The product is the same as before and we note that Γ goes into Δ evaluated at $c_{ij} = k_{ij}$. Hence all polynomials of Δ vanish at k_{ij}. After expanding in terms of the basis w_α , we see that the polynomials of S vanish at k_{ij} .

2) Let N be a superfield of M and k_{ij} constants of N satisfying the polynomials of S . Define a homomorphism of $K\{y_1, \dots, y_n\}$ onto N by $y_i \to \sum k_{ij} u_j$ in the two steps $y_i \to \sum c_{ij} u_j$ and $c_{ij} \to k_{ij}$. The kernel contains Γ and so we obtain a homomorphism σ of $K\{u_1, \dots, u_n\}$ onto $K\{u_1\sigma, \dots, u_n\sigma\}$, where $u_i\sigma = \sum k_{ij} u_j$. If σ is known to be one-to-one, we could extend σ to the quotient fields and the proof would be finished.

By lemma 2 we shall prove that σ is one-to-one. Assume the contrary and compute with transcendence degrees,

$$\partial K\langle u_1, \dots, u_n\rangle / K \;>\; \partial K\langle u_1\sigma, \dots, u_n\sigma\rangle / K \; .$$

Write $K\langle u\rangle$ for $K\langle u_1, \dots, u_n\rangle$. Then

$$\partial K\langle u, u\sigma\rangle / K\langle u\rangle \;<\; \partial K\langle u, u\sigma\rangle / K\langle u\sigma\rangle \; .$$

Thus

$$\partial K\langle u, u\sigma\rangle / K\langle u\rangle \;=\; \partial K\langle u, k\rangle / K\langle u\rangle \;=\; \partial C(k)/C \; ,$$

by lemma 1, and the fact that each u_i and its derivatives satisfy differential equations. Similarly, $\partial K\langle u, u\sigma\rangle / K\langle u\sigma\rangle = \partial C'(k)/C'$ where C' is the constant field in $K\langle u\sigma\rangle$. But $\partial C'(k)/C' \leq \partial C(k)/C$ which is a contradiction. Thus σ is one-to-one and defines the required differential isomorphism of M into N .

Q. E. D.

Theorem 37. The differential Galois group G of a Picard-Vessiot extension M over a differential field K is an algebraic matrix group over the constant field C of K .

Remark. It is also true that

$$\dim G = \partial M/_K$$

where the dimension of the algebraic variety G is defined as in algebraic geometry. If $C = \mathbb{C}$, then $\dim G$ is $\frac{1}{2}$ the topological dimension of the complex manifold G .

Example. Let K = rational functions of a complex variable z with constant field $C = \mathbb{C}$. Consider the differential equation

$$D) \quad y'' + y = 0$$

with Picard-Vessiot extension $M = K<u_1, u_2>$ where $u_1 = e^{iz}$, $u_2 = e^{-iz}$. Compute the Galois group of M over K .

1. Each differential automorphism of M over K must send solutions of D) into solutions of D) and thus be of the form

   $$u_1 \rightarrow k_{11} u_1 + k_{12} u_2$$
   $$u_2 \rightarrow k_{21} u_1 + k_{22} u_2$$

   where the complex constant matrix $(k_{ij}) \in GL(2, \mathbb{C})$. However not all matrices of $GL(2, \mathbb{C})$ arise in differential automorphisms of M over K , but certain algebraic conditions are required of the elements k_{ij} .

2. Each automorphism of M over K must preserve the differential and algebraic identities satisfied by $u_1 = e^{iz}$ and $u_2 = e^{-iz}$ over K . Thus $y_1'' + y_1$, $y_2'' + y_2$, $y_1 y_2 - 1$, $y_1 y_2' - y_1' y_2 + 2i$

and other differential polynomials of $K\{y_1, y_2\}$, for differential indeterminants y_1 and y_2, must vanish under $y_1 \to u_1 \to k_{11}u_1 + k_{12}u_2$ and $y_2 \to u_2 \to k_{21}u_1 + k_{22}u_2$.

3. Consider the differential homomorphism of the integral domain $K\{y_1, y_2\}$ into $M = K\langle u_1, u_2\rangle$ defined by leaving K fixed elementwise and $y_1 \to u_1$, $y_2 \to u_2$. The kernel Γ is a prime differential ideal containing $y_1'' + y_1$, $y_2'' + y_2$, $y_1 y_2 - 1$, $y_1 y_2' - y_1' y_2 + 2i$, and others.

4. The automorphism, M onto M, $u_i \to \sum_j k_{ij} u_j$ must preserve all the identities implied by Γ. That is, consider the differential homomorphism $K\{y_1, y_2\} \to M[C_{ij}]$, (C_{ij}) indeterminants over M,

$$y_i \to u_i \to \sum_j C_{ij} u_j .$$

The image of Γ is an ideal $\Delta \subset M[C_{ij}]$ and we demand that each polynomial of Δ vanish when $C_{ij} = k_{ij}$ — as a condition on k_{ij}.

5. In particular $(y_1 y_2 - 1) \in \Gamma$ and so Δ contains

$$(C_{11}e^{iz} + C_{12}e^{-iz})(C_{21}e^{iz} + C_{22}e^{-iz}) - 1 .$$

Thus a condition for (k_{ij}) to belong to the Galois group is that (k_{ij}) annihilate $C_{11}C_{12}e^{2iz} + (C_{11}C_{22} + C_{12}C_{21} - 1) + C_{12}C_{22}e^{-2iz}$. Working with $(y_1 y_2' - y_1' y_2 + 2i) \in \Gamma$ we find that (k_{ij}) must also annihilate $C_{11}C_{22} - C_{12}C_{21} - 1$.

6. But e^{2iz}, e^{-2iz}, 1 are linearly independent in the vector space M over $\mathbb{C}$ so (k_{ij}) must annihilate the polynomials

$$C_{11}C_{21} = 0, \ C_{11}C_{22} + C_{12}C_{21} - 1 = 0, \ C_{12}C_{22} = 0, \ C_{11}C_{22} - C_{12}C_{21} - 1 = 0 .$$

This shows that (k_{ij}) must annihilate $C_{12} = 0$, $C_{21} = 0$ and yield the value $k_{11}k_{22} = 1$. Thus the matrices (k_{ij}) have the form $\begin{pmatrix} k & 0 \\ 0 & 1/k \end{pmatrix}$ for a complex number $k \neq 0$. That is, the Galois group is contained in the algebraic subgroup $G \subset GL(2, \mathbb{C})$ defined by the ideal generated by

S : $C_{12} = 0$, $C_{21} = 0$, $C_{11}C_{22} - 1 = 0$. If we knew that

Γ is generated by $y_1 y_2 - 1$ and $y_1 y_2' - y_1' y_2 + 2i$ we could conclude that the Galois group is G.

7. We show that the Galois group is G by an ad hoc examination. Actually $M = K\langle e^{iz}, e^{-iz}\rangle = K\langle e^{iz}\rangle = K(e^{iz})$. It is easy to see that $e^{iz} \to k e^{iz}$ defines a differential automorphism of the simple transcendental extension $K(e^{iz})$ over K. But $e^{iz} \to k e^{iz}$ requires $e^{-iz} \to \frac{1}{k} e^{-iz}$. Thus the Galois group is all G.

13. A Picard-Vessiot Extension is Normal.

Let K be a subfield of M. An admissible isomorphism on M is an isomorphism of M into some superfield $N \supset M$. The admissible isomorphism is over K if K is left fixed elementwise.

Theorem 38. Let M be a differential field and K and L differential subfields of M. Let S be a differential isomorphism of K onto L. Then S can be extended to an admissible differential isomorphism defined on M.

Proof.

Given an element $u \in M - K$ we seek to define an extension of S of $K\langle u\rangle$ into a suitable extension of M. The proof is then finished by transfinite induction.

Use S to define a differential homomorphism of $K\{y\}$ onto $K\{u\}$ by sending the differential indeterminant $y \to u$. The kernel $P_1 \subset K\{y\}$ is a prime differential ideal. Use S to define a differential isomorphism of $K\{y\}$ onto $L\{y\}$ and P_1 corresponds to a prime differential ideal P in $L\{y\}$.

Using the lemmas in Chapter 2, Kaplansky, we find that there exists a prime differential ideal $Q \subset M\{y\}$ with $Q \cap L\{y\} = P$.

Note $Q \cap M = 0$.

Consider the natural homomorphism $M\{y\} \to M\{y\}/Q$ and write v for the image of y in the integral domain $M\{y\}/Q$, which contains M . Next define a differential homomorphism from $K\{y\}$ onto $L\{v\}$ by $K\{y\} \xrightarrow{S} L\{y\} \xrightarrow{S: y \to v} L\{v\}$. The kernel of the second map is $Q \cap L\{y\} = P$. Hence the kernel of the product homomorphism is P_1 . Thus there is defined a differential isomorphism of $K\{u\}$ onto $L\{v\}$ which extends S . But it is easy to extend this to a differential isomorphism between the quotient fields $K\langle v\rangle \to L\langle v\rangle$. Note $L\langle v\rangle \subset$ quotient field of $M\{y\}/Q$ which is an extension of M . Q. E. D.

Theorem 39. Let K be a differential subfield of a differential field L . Take an element $s \in L - K$. Then there exists an admissible differential isomorphism on L over K , which moves s .

Proof.

Similar to the above theorem and found in chapter 2, Kaplansky.

Lemma 1. Let K be a differential field with algebraically closed constant field C . Let L be a differential field extension of K , with constant field D . Let f_α , g be polynomials in a finite number of ordinary indeterminants over K , where α ranges over a (possibly infinite) index set. If $f_\alpha = 0 , g \neq 0$ have a common solution in D they must have a common solution in C .

Proof.

Take a vector space basis u_β of K over C . Each f_α has a unique expression $f_\alpha = \sum h_{\alpha\beta} u_\beta$, where $h_{\alpha\beta}$ is a polynomial with coefficients in C . The independence of u_β over the constants of L is maintained.

Therefore in a constant solution of $f_\alpha = 0$ in D we have each $h_{\alpha\beta} = 0$. By the Hilbert Nullstellensatz the equations (finite set) have a solution in C.

Write $g = \sum t_\gamma u_\gamma$. If each solution of $h_{\alpha\beta} = 0$ in C is also a solution of $g = 0$, and hence of $t_\gamma = 0$, we have $(t_\gamma)^{r_\gamma} \in I$ where r_γ is a natural number and I is the ideal generated by $h_{\alpha\beta}$. But then every solution of $f_\alpha = 0$ in D would annihilate g , which is a contradiction. Q. E. D.

__Lemma 2.__ Let K be a differential field with an algebraically closed field of constants. Let M be a Picard-Vessiot extension of K . Suppose that $z \in M$ and two subsets $x_\alpha \in M$ and $y_\alpha \in M$, where α ranges over some index set. Suppose there exists an admissible differential isomorphism of M over K sending each x_α into y_α and moving z . Then there exists a differential automorphism of M over K sending x_α into y_α and moving z .

__Proof.__

Let σ be the given differential isomorphism of M . Say $u_i\sigma = \sum k_{ij} u_j$ for k_{ij} being constants in the larger field. Consider any two elements x, y in M . Each is a ratio of two differential polynomials in the u_i , say, $x = P(u)/Q(u)$ and $y = R(u)/S(u)$. The condition $y = x\sigma$ can be written

$$S(u)\,P(u\sigma) = R(u)\,Q(u\sigma).$$

Put $u_i\sigma = \sum k_{ij} u_j$ and get a polynomial in k_{ij} with coefficients in M . There is one such equation for each α , $x_\alpha\sigma = y_\alpha$. Combine these equations with the equations describing the algebraic variety of the Galois group of M over K . Also combine these with the inequalities $z\sigma \neq z$ with $\det(k_{ij}) \neq 0$. Since there is a constant solution for k_{ij} in the larger field there is already a solution in C . This defines the required differential automorphism.

Q. E. D.

Theorem 40. Let K be a differential field with an algebraically closed constant field C . Let M be a Picard-Vessiot extension of K . Then M is normal over K .

Proof.

We first show that K is a closed field under the Galois correspondence. Given $z \in M-K$ we must find a differential automorphism of M over K which moves z . By the theorem quoted above there exists an admissible differential isomorphism of M over K which moves z . By the lemma 2 we obtain the required differential automorphism of M .

Now let L be an intermediate differential field, $M \supset L \supset K$. But M is a Picard-Vessiot extension of L for the same differential equation which generates M over K . Repeating the above argument, we see that L is a closed subfield of M .

Q. E. D.

Theorem 41. Let K be a differential field with algebraically closed constant field C . Let M be a Picard-Vessiot extension of K . Then any differential isomorphism over K between two intermediate differential fields can be extended to a differential automorphism of M over K .

Proof.

First extend the differential isomorphism to an admissible differential isomorphism defined on all M and then use lemma 2.

Q. E. D.

14. Completion of the Galois Correspondence.

Theorem 42. Let K be a differential field with algebraically closed constant field C. Let M be a Picard-Vessiot extension of K with differential Galois group G. Then a subgroup H of G is the Galois group of some intermediate differential field L if and only if H is an algebraic matrix group. That is, the Galois-closed groups are precisely the Zariski-closed groups in G.

Proof.

Let H be the differential Galois group of M over the intermediate differential field L. Since M is a Picard-Vessiot extension of L, H is an algebraic matrix subgroup of G.

Now let H be a Zariski-closed subgroup of G. Let H' be the fixed field under H and H'' the Galois group of H'. We show that $H = H''$ in fact, we shall show that each subgroup H of G is Zariski-dense in H''. If H is not Zariski-dense in H'' then the smallest algebraic variety, in the n^2-dimensional vector space V over C, which contains H does not contain H''. Thus we suppose there exists a polynomial f in n^2-variables, with coefficients in C, which vanishes everywhere on H but which does not vanish identically on H''.

We now follow the calculation of Kaplansky illustrating the proof of the theorem for the case $n = 2$.

Let $M = K < u, v >$ and the Wronskian matrix $\begin{pmatrix} u & v \\ u' & v' \end{pmatrix}$ is non-singular. Write $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ for the inverse of the Wronkian matrix. Let y and z be differential indeterminants over M. Define a differential polynomial $F(y, z) \in M\{y, z\}$ by

$$F(y, z) = f(Ay + By', Az + Bz', Cy + Dy', Cz + Dz').$$

In $F(y, z)$ set $y = u\sigma$, $z = v\sigma$ where $\sigma \in H$.

Now
$$\begin{pmatrix} u\sigma & v\sigma \\ u'\sigma & v'\sigma \end{pmatrix} = \begin{pmatrix} u & v \\ u' & v' \end{pmatrix}\begin{pmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{pmatrix}$$

where (k_{ij}) is the matrix for σ and we have
$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} u\sigma & v\sigma \\ u'\sigma & v'\sigma \end{pmatrix} = \begin{pmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{pmatrix}.$$

Hence $F(u\sigma, v\sigma) = 0$ for $\sigma \in H$ but not for all $\sigma \in H''$.

Among all differential polynomials in $M\{y, z\}$ satisfying the above condition on F, choose one, say E, with the smallest possible number of terms when written out as a sum of monomials. Assume also that one of the coefficients of E is 1. For $\tau \in H$ write E_τ for the polynomial obtained by replacing each coefficient by its image under τ. Then
$$E_\tau(u\sigma, v\sigma) = \left[E(u\sigma\tau^{-1}, v\sigma\tau^{-1})\right]\tau$$
which is 0 for every $\sigma \in H$. The polynomial $E - E_\tau$ is shorter than E. Thus $E - E_\tau$ must vanish for every $u\sigma, v\sigma$ with $\sigma \in H''$. If $E - E_\tau$ is not identically zero, we can find an element $\gamma \in M$ such that $E - \gamma(E - E_\tau)$ is shorter than E. Since $E - \gamma(E - E_\tau)'$ also vanishes at $(u\sigma, v\sigma)$ for all σ in H but not for all $\sigma \in H''$, we have a contradiction unless $E - E_\tau \equiv 0$. This means that every coefficient of E lies in H' and is so left invariant by H''. But then $E(u\sigma, v\sigma) = 0$ for all $\sigma \in H''$, which is a contradiction.

Q. E. D.

Theorem 43. (Galois Correspondence). Let K be a differential field with algebraically closed constant field C. Let M be a Picard-Vessiot extension of K with differential Galois group G. Let $\mathcal{F}$ be the lattice of all intermediate differential fields and let $\mathcal{G}$ be the lattice of all algebraic matrix subgroups of G . For each $L \in \mathcal{F}$ let $L' \in \mathcal{G}$ be the differential Galois group of M over L . For each $H \in \mathcal{G}$ let $H' \in \mathcal{F}$ be the fixed differential field under H . This correspondence defines a one-to-one dual lattice isomorphism of $\mathcal{F}$ onto $\mathcal{G}$.

Proof.

Under the hypothesis that M is normal over K and that $\mathcal{G}$ is a lattice, this theorem has already been proved in section 7.

Q. E. D.

Theorem 44. Let K be a differential field with algebraically closed constant field C . Let M be a Picard-Vessiot extension of K with differential Galois group G . Let $\mathcal{F} \longleftrightarrow \mathcal{G}$ be the Galois correspondence. If $H \in \mathcal{G}$ is normal in G , then $H' = L$ is normal over K and the differential Galois group of L over K is G/H .

Proof.

Let L_1 be a differential field between L and K and take $s \in L - L_1$. There is an automorphism $\sigma \in G$ which is the identity on L_1 and which moves s . We shall show that $L\sigma = L$, since H is normal in G .

Take $x \in L$ and consider $x\sigma$. For $\tau \in H$ we have $\sigma\tau\sigma^{-1} \in H$ and $x\sigma\tau\sigma^{-1} = x$. Thus $x\sigma\tau = x\sigma$ so $x\sigma \in L$. Thus $L\sigma = L$.

Therefore σ belongs to the Galois group $G(L/K)$ of L over K and we have proved that L is normal over K .

Each differential automorphism of L over K can be extended to a differential automorphism of M over K , and each $\sigma \in G$ sends L onto L . Thus there is a homomorphism of G onto $G(L/K)$. The kernel consists of all those elements of G which are the identity on L . Thus $G/H = G(L/K)$.

Q. E. D.

Theorem 45. Let K be a differential field with algebraically closed constant field C. Let M be a Picard-Vessiot extension of K with differential Galois group G. Let $\mathcal{F} \leftrightarrow \mathcal{G}$ be the Galois correspondence. If $L \in \mathcal{F}$ is normal over K, then $L' = H \in \mathcal{G}$ is normal in G.

Proof.

Now H is a closed subgroup of G and hence its normalizer H_1 is also closed and $H_1 \in \mathcal{G}$. In order to show that H is normal we must only show that $H_1 = G$. Let $H_1' = L_1 \in \mathcal{F}$ and we show that $L_1 = K$.

Now it is easy to see that H_1 consists precisely of those $\sigma \in G$ that map L onto itself. Thus H_1 contains all differential automorphisms of L over K, each of which can be extended to an element of G. Since L is normal over K, no element of $L - K$ is fixed under H_1. Thus $H_1' = L_1 = K$, as required. Q. E. D.

15. Solution of Differential Equations in Elementary Functions.

Lemma 1. Let N be a differential field with differential subfield K. Let L and M be intermediate differential fields, $N \supset M \supset L \supset K$. Assume M is a finite algebraic extension of L and $[M:L] = n$. Let L' and M' be the corresponding subgroups of the differential Galois group of N over K. Then the index of M' in L' is $\leq n$.

Proof.

It is enough to prove the lemma for simple extensions so assume $M = L(u)$. Then the right cosets of L'/M' correspond exactly to the possible images of u (in the automorphisms of N keeping L fixed). There are at most n such images, the roots of the irreducible polynomial for u over L. Q. E. D.

Lemma 2. Let M be a Picard-Vessiot extension of the differential field K, with algebraically closed constant field C. Let $N = M\langle z\rangle$ be an extension of M with constant field C. Write $L = K\langle z\rangle$. Then N is a Picard-Vessiot extension of L and its differential Galois group is isomorphic to an algebraic subgroup of the differential Galois group of M over K, namely the subgroup leaving $M \cap L$ fixed.

Proof.

Clearly N is a Picard-Vessiot extension of L for the same differential equation which generates M over K. Thus any differential automorphism of N over L must send M onto itself. Thus there is a homomorphism of the differential Galois group of N/L onto a subgroup G_1, of the differential Galois group of M/K. The kernel leaves fixed both M and L and hence their union. The homomorphism is thus an isomorphism onto G_1, which is thereby an algebraic matrix group. The fixed field is $M \cap L$ and so G_1 is the whole Galois group of M over $M \cap L$.

Q. E. D.

Theorem 46. Let K be a differential field with algebraically closed constant field C. Let $D)$ be a linear homogeneous differential equation with coefficients in K. Let M be the Picard-Vessiot extension of K for the differential equation $D)$, with differential Galois group G. If the component G_0 of the identity of G is solvable, then M can be obtained from K by a finite-dimensional normal extension followed by a Liouville extension. Conversely, if M lies in a generalized Liouville extension of K (with constant field C), then G_0 is solvable.

Proof.

Assume G_0 is solvable and let L be the corresponding intermediate differential field. Then L is a finite dimensional normal extension of K and G_0 is the differential Galois group of M over L.

We next show that M is a Liouville extension of L. There is a basis for the solutions of the differential equation D) so that G_0 is triangular and we write $M = L\langle u_1, \ldots, u_n\rangle$ with

$$u_i\sigma = a_{i,i}u_i + a_{i,i+1}u_{i+1} + \cdots + a_{in}u_n, \quad i = 1, 2, \ldots, n$$

where $a_{ij} \in C$ depend on $\sigma \in G_0$.

Now

$$u_n\sigma = a_{nn}u_n$$

so

$$\left(\frac{u_n'}{u_n}\right)\sigma = \frac{(a_{nn}u_n)'}{a_{nn}u_n} = \frac{u_n'}{u_n}$$

and $\frac{u_n'}{u_n} \in L$. Thus $L_1 = L\langle u_n\rangle$ is the adjunction of an integral of an exponential. Now

$$\frac{u_i\sigma}{u_n\sigma} = \frac{a_{ii}}{a_{nn}}\frac{u_i}{u_n} + \frac{a_{i,i+1}}{a_{nn}}\frac{u_{i+1}}{u_n} + \cdots + \frac{a_{in}}{a_{nn}}\frac{u_n}{u_n}$$

and

$$\left(\frac{u_i}{u_n}\right)'\sigma = \frac{a_{ii}}{a_{nn}}\left(\frac{u_i}{u_n}\right)' + \cdots + \frac{a_{i,i-1}}{a_{nn}}\left(\frac{u_{n-1}}{u_n}\right)',$$

for $i = 1, 2, \ldots, n-1$. Call $(u_i/u_n)' = v_i$ and then, by induction on n, $L_1\langle v_1, \ldots, v_{n-1}\rangle$ is a Liouville extension of L_1 and hence of L. Then adjoin the integrals of $v_1, \ldots, v_{n-1}$ to obtain M as a Liouville extension of L.

On the other hand assume M lies in a generalized Liouville extension N of K. We make an induction on the number of steps in the chain of fields from K to N. Let $K\langle z\rangle$ be the first step. Then by induction the differential Galois group of $M\langle z\rangle$ over $K\langle z\rangle$

has a solvable component of the identity. By lemma 2, this group is isomorphic to the subgroup, say G_1, of G corresponding to the field $M \cap K\langle z\rangle$.

Suppose z is algebraic over K. By lemma 1, G_1 has finite index in G. Suppose otherwise that z is either an integral or an exponential of an integral. But then $K\langle z\rangle$ is a Picard-Vessiot extension of K with abelian Galois group. Thus all differential fields between K and $K\langle z\rangle$ are normal over K. In particular, $M \cap K\langle z\rangle$ is normal over K with an abelian differential Galois group. Thus G_1 is normal in G with G/G_1 abelian. In either case, we have seen earlier (cf. section 10) that G_0 is solvable. Q. E. D.

<u>Theorem 47</u>. Let

$$L(y) = y^{(n)} + a_1 y^{(n-1)} + \cdots + a_{n-1} y' + a_n y = 0$$

be a differential equation with coefficients in a differential field K, having an algebraically closed constant field. Let M be the Picard-Vessiot extension of K for this differential equation and let G_0 be the component of the identity of the differential Galois group of M over K. Then $L(y) = 0$ is solvable in elementary functions if and only if G_0 is solvable.

<u>Theorem 48</u>. Let K be a differential field with algebraically closed constant field C. Let $D)$ be a linear homogeneous differential equation with coefficients in K. Let M be the Picard-Vessiot extension of $D)$, with differential Galois group G. If G is solvable, then M is a Liouville extension of K. Conversely, if M lies in a Liouville extension of K (with constant field C), then G is solvable.

Proof.

If G is solvable, G_0 is solvable and so is G/G_0. Then M is a Liouville extension of L, the intermediate field corresponding to G_0. Also L is a finite dimensional normal extension of K and the Galois group of L over K in G/G_0. Thus L is an extension of K by radicals. But $u^{1/r} = e^{\int \frac{1}{r}\frac{u'}{u}}$ for an integer $r > 0$. Thus an extension by radicals is a Liouville extension. So M is a Liouville extension of K.

On the other hand assume $K \subset M \subset N$ where N is a Liouville extension of K. It is easy to see that the differential Galois group of N over K is solvable. Just as in the earlier theorem we proceed by induction on the number of steps from K to N. We find that there is a normal solvable group $G_1 \subset G$ with G/G_1 abelian. Then G is solvable.

Q. E. D.

Theorem 49. Let

$$L(y) = y^{(n)} + a_1 y^{(n-1)} + \cdots + a_{n-1} y' + a_n y = 0$$

be a differential equation with coefficients in a differential field K, having an algebraically closed constant field. Let M be the Picard-Vessiot extension of K for this differential equation and let G be the differential Galois group of M over K. Then $L(y) = 0$ is solvable by integrals and exponentials if and only if G is solvable.

Problems

1. Let K be the differential field of rational functions of one complex variable. Consider the Picard-Vessiot extension $M = K\langle u_1, u_2\rangle$ for $u_1 = e^{iz}$, $u_2 = e^{-iz}$, solutions of $y'' + y = 0$. Find the differential Galois group G of M over K. Find all algebraic subgroups of G, all intermediate differential fields between M and K, and discuss the Galois correspondence.

2. Let K be a differential field and $M = K\langle u\rangle$ where u is differential over K, that is, u satisfies a polynomial differential equation with coefficients in K. Show that every element of M is differential over K. (Hint: show that M has finite transcendence degree over K if and only if u is differential over K).

3. Show that the function $\Gamma(z)$ satisfies no polynomial differential equations with coefficients in the differential field $K\langle \wp(z)\rangle$. Here K consists of the rational functions of a complex variable z and the Weierstrass elliptic function $\wp(z)$ satisfies $\frac{d\wp}{dz} = \sqrt{4\,\wp(z)^3 - g_2\wp(z) - g_3}$ for complex constants g_2, g_3.

4. Use Hőlder's theorem for $\Gamma(z)$ and the functional equation

$$\zeta(1-z) = \frac{2}{(2\pi)^z}\cos\frac{\pi z}{2}\cdot\Gamma(z)\,\zeta(z)$$

to show that $\zeta(z)$ does not satisfy a polynomial differential equation (that is, $\zeta(z)$ is hyper-transcendental over the differential field of rational functions).

Bibliography

1. L. Bieberbach, *Theorie der Gewöhnlichen Differentialgleichungen auf Funktionentheoretischer Grundlage*. Berlin, 1953.

2. I. Kaplansky, *An Introduction to Differential Algebra*, Paris, 1957.

3. E. Kolchin, "Algebraic Matrix Groups and the Picard-Vessiot Theory of Homogeneous Linear Ordinary Differential Equations," *Ann. of Math* 49, pp. 1-42 (1948).

4. E. Kolchin, "Galois Theory of Differential Fields," *Am. J. of Math*. 75, pp. 753-824 (1953).

5. J. Ritt, *Differential Algebra*, New York 1950.

6. J. Ritt, *Integration in Finite Terms*, New York 1948.

7. E. Picard, *Traite d'Analyse* 3, ch. 17. Paris 1928.

8. Van der Vaerden, *Moderne Algebra*, New York 1943.