ANNALS OF MATHEMATICS
Vol. 49, No. 1, January, 1948

ALGEBRAIC MATRIC GROUPS AND THE PICARD-VESSIOT THEORY OF HOMOGENEOUS LINEAR ORDINARY DIFFERENTIAL EQUATIONS

BY E. R. KOLCHIN

(Received December 4, 1946)

TABLE OF CONTENTS

INTRODUCTION

Historical background

A central role in the Galois theory of homogeneous linear ordinary differential equations as developed by Picard and Vessiot at the end of the last century,[1]

[1] For an account of the early (and most important) papers see Vessiot [3] (numbers in square brackets refer to the References at the end of the present paper). The theory began

is played by the concept of algebraic matric group, that is, broadly speaking, multiplicative group of matrices defined by algebraic equations in the elements of the matrices. Special cases of such groups (for example: the full matric group, the unimodular group, the orthogonal group, finite matric groups) have been subject to more or less exhaustive research for many decades, but the literature seems to be devoid of any basic theory of algebraic matric groups as such. For lack of such a theory, these groups, when encountered on a large scale (as in the Picard-Vessiot theory), have been treated as special cases of Lie groups. As a result the generally brilliant theory of Picard and Vessiot suffered on the one hand from the lack of rigor of the early theory of Lie groups, and on the other hand from being too intimately bound up with the analytic point of view of the Lie theory, thereby obscuring the algebraic nature of the subject matter.

It is doubtless possible to bring the rigor of the group-theoretic aspects of the Picard-Vessiot theory up to modern standards by making reference to modern developments concerning Lie groups. But not only would this not answer the second of the above mentioned points, it would make the Picard-Vessiot theory depend on a discipline far deeper and more extensive than itself. Moreover, if it is desired to extend the theory to abstract coefficient fields, it is necessary to extend the whole machinery of Lie groups and Lie algebras to algebraic matric groups over such fields.[2]

Not only does the Picard-Vessiot theory suffer from a lack of an algebraic point of view, but some of it seems to be afflicted with a lack of clarity of ideas, or at least a lack of precise formulation of ideas. A most striking example of this affliction is afforded by Vessiot's beautiful and celebrate theorem that a homogeneous linear ordinary differential equation is "solvable by quadratures" if and only if the group is "integrable." Just what "solvable by quadratures" means is not clearly stated. A close examination of the proof reveals that solving by quadratures must permit not only the operation of integration, but also that of exponentiation (of integrals). But the confusion in terminology is sufficient to induce Picard [5] to use "quadrature" as equivalent to "integral" in the proof of the necessity, and yet to permit exponentiation in the proof of the

with Picard [1], a note amplified by Picard [2], and received great impetus from Vessiot [1] and [2]. After Picard and Vessiot, the most important contributions are those of Loewy. The presentation of the theory by Picard [5] is as full as any, but suffers from all the criticism made below. The most recent remarks published on the subject are those made in 1932 by Baer [1], who critically surveyed the general state of the theory. The theory partially outlined by Freudenthal [1] evidently is concerned with only linear phenomena, whereas the theory of Picard-Vessiot is essentially a study of certain types of differential field extensions.

[2] In the case of fields of characteristic 0, this labor could be avoided, as remarked to me orally by Professor C. Chavalley, by embedding the abstract field in the field of complex numbers, if the former field has cardinal number $\leq$ that of the continuum, or (with a slight argument) by so embedding part of the abstract field if its cardinal number is greater. Of course, if it is desired to include fields of nonzero characteristic this procedure can not be used.

sufficiency. Indeed, it seems as though the solving of any differential equation of the first order could be used, instead of integration, in the necessity arguments as given by Picard [5] and Vessiot [2]. Furthermore, the question of whether algebraic operations are permitted is not always made clear. The relationship between the necessity of using algebraic operations and the disconnectedness of the group was realized, especially by Marotte [1] and by Fano [1], but these algebraic questions were sufficiently neglected so that it was never thought necessary by anyone to ask whether the connected component of the group containing the identity matrix was actually the group of the equation over some enlarged coefficient field. Indeed, as Baer [1] points out, one of the outstanding tasks in the theory, after algebraization, is to establish an analogue to the theorem in Galois theory which asserts the one-to-one correspondence between intermediate fields and subgroups of the Galois group.

A beginning at algebraization and departure from the Lie tradition was made by Loewy [4], but he carried his work in this direction barely far enough to define in rigorous fashion the group of an equation (with respect to more general coefficient domains than thitherto) and to make clear some of its elementary properties. Beyond this there is nothing in the literature that recasts the pioneering papers of Picard and Vessiot. It seems likely that two factors contributed to this state of affairs. One is the aforementioned absence of a general theory of algebraic matric groups. The other is the inadequacy of the classical theory of differential equations for handling the algebraic aspects of differential equations. The second of these factors has been removed in recent years by the emergence of the penetrating and elegant Ritt theory of algebraic differential equations (for a general account of this theory as of 1938 see Ritt [2]). Indeed, it is difficult to imagine how this work of Picard and Vessiot could be put on a sound footing without making use of the Ritt theory.

Summary

The purposes of the present paper are, first to develop a set of theorems on algebraic matric groups, at least adequate to meet the demands of the Picard-Vessiot theory, and second, to algebraize, rigorize, round out, and augment that theory. The paper is organized into five chapters plus a list of references.

Chapter I deals with algebraic matric groups over an algebraically closed field. To emphasize the purely algebraic nature of the subject matter the proofs are carried through in a manner valid for fields of nonzero as well a zero characteristic. A matrix can be regarded as a point in n^2-dimensional space. The set of matrices in an algebraic matric group constitutes an algebraic manifold (from which is deleted an algebraic manifold of lower dimension composed of singular matrices), the underlying manifold of the group. The interplay between the group properties and the algebraic manifold properties of the algebraic matric group forms the basis for the theory. It is shown that the irreducible components of the underlying manifold are pairwise disjoint (save, perhaps, for singular matrices), and all have the same dimension; the component con-

taining the identity matrix is the underlying manifold of a normal algebraic subgroup of finite index (the component of the identity). Following three lemmas, a Jordan-Hölder-Schreier theorem is proved in the manner of Zassenhaus [1]. Solvable algebraic matric groups are defined by means of normal chains and there is derived a necessary and sufficient condition that a set of matrices be simultaneously reducible to triangular form. This result is the same as Lie's theorem that a connected solvable Lie group of matrices is reducible to triangular form, but on the one hand is proved without recourse to infinitesimal transformations and is valid for fields of any characteristic, and on the other hand is restricted to algebraic groups. The concepts of "anticompact" and "quasicompact" algebraic matric groups are defined ($\mathfrak{G}$ is anticompact if it contains no element of finite order exceeding unity and not divisible by the field characteristic; $\mathfrak{G}$ is quasicompact if every algebraic subgroup of order greater than unity contains such an element). It is shown that an algebraic matric group is anticompact if and only if each matrix in the group has all its characteristic roots equal to unity, whereas the group is quasicompact if and only if any given matrix in it is reducible to diagonal form. Also, the influence of anticompactness and quasicompactness on triangular form is investigated. Finally, algebraic matric groups which have normal chains with certain properties different from those used in defining solvability, are studied.

Chapter II is a compilation of just those results from the Ritt theory which are needed in the sequel.

The short Chapter III contains a beginning of a Galois theory for differential fields. With the hope of some day broadening the scope of the Picard-Vessiot theory, I have carried out the first few (trivial) steps thereof in a very general setting. Without reference to linear differential equations, there is considered an extension of an arbitrary differential field (ordinary or partial) of characteristic 0. There is defined for such an extension the property of being normal, in a manner consistant with the familiar concept of normality for algebraic field extensions. The comparatively complicated nature of this definition is due to the fact that, for differential fields, the concept analogous to the splitting field of a polynomial is lacking. It is shown that an "abundant" (that is, large enough, in a precisely defined sense) group of automorphisms of the normal differential field over the ground differential field enjoys some properties similar to those of a Galois group. Namely: there is a one-to-one correspondence between intermediate differential fields and *certain* subgroups; an intermediate differential field satisfies a certain condition perhaps stronger than that of normality if and only if the corresponding subgroup is normal; and in this case the factor group is isomorphic with an abundant group of automorphisms of the intermediate differential field over the ground differential field. It is in connection with the last property that the use of abundant groups of automorphisms instead of the group of all automorphisms (which of course is abundant) is indicated. For, when the group of all automorphisms is used the factor group need not be isomorphic with the group of all automorphisms of the intermediate

differential field over the ground differential field, but merely with an abundant subgroup thereof. Here, at least for the present, the general theory ends.[3] In particular, there is no characterization of those "certain" subgroups which correspond to intermediate differential fields.

Chapter IV carries this general theory forward for the special case provided by the Picard-Vessiot theory. There is defined the concept of "Picard-Vessiot extension" of a given ordinary differential field $\mathcal{F}$ of characteristic 0 with algebraically closed field of constants ($\mathcal{G}$ is a Picard-Vessiot extension of $\mathcal{F}$ if every constant in $\mathcal{G}$ is in $\mathcal{F}$ and $\mathcal{G}$ can be obtained by adjoining to $\mathcal{F}$ a fundamental system of solutions of a homogeneous linear ordinary differential equation with coefficients in $\mathcal{F}$), and such an extension is shown to be normal in the sense of Chapter III. The group of all automorphisms over the given differential field is shown to be isomorphic with an algebraic matric group. This makes immediately available the theorems of Chapters I and III. The set of all subgroups that correspond to intermediate differential fields is characterized as the set of all algebraic subgroups. The equality between the dimension of the group and the degree of transcendency of the extension is proved, the isomorphism between factor group and group of *all* automorphisms of the intermediate differential field over the ground differential field is established, and a few special topics (largely necessary for the sequel) are treated.

Chapter V is concerned with the above mentioned extension of Vessiot's big theorem. An extension of a given differential field is defined as "liouvillian"[4] if it contains no new constants and it is an extension by integrals, exponentials of integrals, and algebraic functions, that is, if the extension can be obtained by repeated adjunction of solutions of equations of the types $y' - a = 0$, $y' - ay = 0$, and $y^m + a_1 y^{m-1} + \cdots + a_m = 0$. Furthermore, a hierarchy of ten different classes of liouvillian extensions is recognized, each class being defined by restricting the type of adjunctions permitted. It is then proved that a Picard-Vessiot extension is (contained in) a liouvillian extension if and only if the corresponding algebraic matric group has a solvable component of the identity. Moreover, for each of the ten classes, necessary and sufficient conditions are found for the liouvillian extension to be of that class. For example, a Picard-Vessiot extension is an extension by integrals alone if the group is solvable and anticompact, by exponentials of integrals alone if the group is solvable and quasicompact. Several consequences are pointed out. For example, if a Picard-Vessiot extension is liouvillian, it can be obtained by first making a purely algebraic adjunction and then making adjunctions solely by means of integrals and exponentials of integrals. Again, if a Picard-Vessiot

[3] An attempt at a general Galois theory for differential fields has been made by J. E., EATON (*A Galois theory for differential fields*, Duke Mathematical Journal, vol. 10 (1943), pp. 751–760), but his whole paper depends on his false Theorem 1.

[4] This term was suggested by Professor Ritt, who has used the term "l-function" for elements of such fields in connection with his research in and exposition of the Liouville theory of the solvability of certain differential equations.

extension is contained in an extension by exponentials of integrals, with no new constants, then the given linear differential equation has a fundamental system of solutions such that each solution in the fundamental system is the exponential of an integral of an element of a certain extension by radicals.

It should, perhaps, be mentioned that a generalization of the Picard-Vessiot theory to allow fields of positive characteristic must await a similar generalization of at least part of the Ritt theory. As yet little has been done in this direction beyond the treatment of the Ritt-Raudenbush basis theorem in Kolchin [2].

Notation and terminology

The inclusion of an element in a set is denoted by $\in$. The set inclusion relations of being contained in and of containing are denoted by $\subseteq$ and $\supseteq$, respectively, proper inclusion by $\subset$ and $\supset$. The negation of any of these relations is indicated by a transverse line: $\notin$, $\not\subseteq$, etc.

The union (set-theoretic sum) of two sets $\mathfrak{M}$ and $\mathfrak{N}$ is denoted by $\mathfrak{M} \cup \mathfrak{N}$, their intersection by $\mathfrak{M} \cap \mathfrak{N}$. For a system of sets $\mathfrak{M}_\lambda$ the notation for union is $\bigcup \mathfrak{M}_\lambda$, for intersection is $\bigcap \mathfrak{M}_\lambda$. The set of all elements contained in $\mathfrak{M}$ but not in $\mathfrak{N}$ is denoted by $\mathfrak{M} - \mathfrak{N}$.

A subgroup $\mathfrak{H}$ of a group $\mathfrak{G}$ such that $\sigma^{-1}\mathfrak{H}\sigma = \mathfrak{H}$ for all $\sigma \in \mathfrak{G}$ is called *normal*.

Algebraic notation used is generally as in van der Waerden [1]. Ring adjunction is indicated by square brackets $\mathcal{R}[\cdots]$, field adjunction by parentheses $\mathcal{F}(\cdots)$. The degree of transcendency of a field $\mathcal{G}$ over a subfield $\mathcal{F}$ is denoted by $\partial^\circ \mathcal{G}/\mathcal{F}$.

For an algebraic manifold $\mathfrak{M}$ in m-dimensional affine space over a field $\mathcal{C}$, the set $\mathfrak{m}$ of all polynomials in $\mathcal{C}[x_1, \cdots, x_m]$ which vanish at all points of $\mathfrak{M}$ is called the *defining ideal* of $\mathfrak{M}$. A *generic zero* of $\mathfrak{m}$ or a *generic point* of $\mathfrak{M}$ is a generalized point (i.e. a point with coordinates in some extension of $\mathcal{C}$) such that $f \in \mathcal{C}[x_1, \cdots, x_m]$ vanishes at this point if and only if $f \in \mathfrak{m}$. A generic zero exists if and only if $\mathfrak{m}$ is prime and $\mathfrak{m} \subset \mathcal{C}[x_1, \cdots, x_m]$ (i.e. $\mathfrak{M}$ is irreducible and nonempty). If σ is a generalized point then $\partial^\circ \mathcal{C}(\sigma)/\mathcal{C}$ is the *dimension* of σ. If $\mathfrak{M}$ is irreducible and nonempty the dimension of a generic point of $\mathfrak{M}$ is the *dimension* of $\mathfrak{M}$ or of $\mathfrak{m}$.

A generic point of an irreducible algebraic manifold may be regarded as an ordered set of alebraic functions of a certain number (the dimension) of indeterminates or parameters. If we have several generic points (of the same or different manifolds) and if all the parameters taken together are algebraically independent over $\mathcal{C}$, then the generic points are *independent*.

For two generalized points σ and τ the substitution $\sigma \to \tau$ is a *specialization* if every polynomial in $\mathcal{C}[x_1, \cdots, x_m]$ vanishing at σ also vanishes at τ, that is, if $\sigma \to \tau$ generates a homomorphism of $\mathcal{C}[\sigma]$ onto $\mathcal{C}[\tau]$. If σ is a generic point and τ any generalized point of an algebraic manifold then $\sigma \to \tau$ is a specialization.

Every algebraic manifold is the union of a finite number of irreducible algebraic manifolds none of which contains another. These irreducible manifolds, which are unique, are the *irreducible components* of the given manifold.

CHAPTER I. ALGEBRAIC MATRIC GROUPS

1. Reducibility of sets of matrices

All matrices considered in this chapter are square with elements in an algebraically closed commutative field $\mathcal{C}$. The characteristic of $\mathcal{C}$ will be denoted by p. The zero matrix will be denoted by 0, the identity matrix by ι.

Two sets $\mathfrak{M}$ and $\mathfrak{N}$ of matrices of degree n are *equivalent* if there exists a non-singular matrix ρ of degree n such that $\rho^{-1}\mathfrak{M}\rho = \mathfrak{N}$.

We shall often find it useful to think of matrices of degree n as linear operators on an n-dimensional vector space over $\mathcal{C}$. That is, if σ is a matrix (a_{ij}) we may consider an n-dimensional vector space $\mathfrak{N}$ with basis vectors $\eta_1, \cdots, \eta_n$, and think of σ as the operator defined by

$$\sigma\eta_j = \sum_i a_{ij}\eta_i, \qquad j = 1, \cdots, n.$$

If $\mathfrak{M}$ is a set of matrices, considered as linear operators on $\mathfrak{N}$, and $\mathfrak{N} = \rho^{-1}\mathfrak{M}\rho$ is an equivalent set, then $\mathfrak{N}$ can be thought of as the same set of operators, expressed with respect to the set of basis vectors $\rho\eta_1, \cdots, \rho\eta_n$ instead of $\eta_1, \cdots, \eta_n$.

A set $\mathfrak{M}$ of matrices of degree n is *reducible* if there exists an equivalent set $\mathfrak{N}$ of the form

$$\mathfrak{N} = \begin{pmatrix} \mathfrak{N}_1 & * \\ 0 & \mathfrak{N}_2 \end{pmatrix},$$

that is, for a positive integer $q < n$, every σ in $\mathfrak{N}$ has the form

$$\sigma = \begin{pmatrix} a_{11} & \cdots & a_{1q} & a_{1,q+1} & \cdots & a_{1n} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ a_{q1} & \cdots & a_{qq} & a_{q,q+1} & \cdots & a_{qn} \\ 0 & \cdots & 0 & a_{q+1,q+1} & \cdots & a_{q+1,n} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & 0 & a_{n,q+1} & \cdots & a_{nn} \end{pmatrix}.$$

This is the same as saying that $\mathfrak{N}$ has a linear subspace of dimension q which is invariant under each matrix in $\mathfrak{M}$. If $\mathfrak{M}$ is not reducible then it is *irreducible*. $\mathfrak{M}$ *is completely reducible* if there is an equivalent set $\mathfrak{N}$ of the form

$$\mathfrak{N} = \begin{pmatrix} \mathfrak{N}_1 & & 0 \\ & \ddots & \\ 0 & & \mathfrak{N}_r \end{pmatrix}, \tag{1}$$

where each square block $\mathfrak{N}_i$ is irreducible, that is if $\mathfrak{N}$ can be written as the direct sum of linear subspaces invariant under every matrix in $\mathfrak{M}$, none of the linear subspaces having a subspace of lower positive dimension invariant under every matrix in $\mathfrak{M}$. It is easy to see that if a set $\mathfrak{M}$ of the form

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{M}_1 & 0 \\ 0 & \mathfrak{M}_2 \end{pmatrix}$$

is completely reducible, then so are $\mathfrak{M}_1$ and $\mathfrak{M}_2$.

The following result is classical (see, e.g., Weyl [1], p. 81).

SCHUR'S LEMMA. *Let $\mathfrak{M}$ be an irreducible set of matrices. If a matrix σ commutes with every matrix in $\mathfrak{M}$, then either $\sigma = 0$ or σ is nonsingular. Thus, since $\mathcal{C}$ is algebraically closed, the only matrices commuting with every matrix in $\mathfrak{M}$ are of the form $c\iota$ (element of $\mathcal{C}$ times the identity matrix).*

A set $\mathfrak{M}$ of matrices is in *triangular form* if, for every (a_{ij}) in $\mathfrak{M}$, $a_{ij} = 0$ whenever $i > j$. We shall say that $\mathfrak{M}$ is in *special triangular form* if $\mathfrak{M}$ is in triangular form and every matrix in $\mathfrak{M}$ has all the elements on the main diagonal equal to 1. $\mathfrak{M}$ is in *diagonal form* if $a_{ij} = 0$ whenever $i \neq j$. $\mathfrak{M}$ is *reducible* to a given one of these three forms if there is an equivalent set in the given form.

By means of Schur's lemma it is easy to see that every abelian set of matrices is reducible to triangular form.[5] Indeed, the assertion is obviously true for degree $n = 1$. Let $n > 1$ and suppose the assertion true for matrices of lower degree. If the abelian set of matrices $\mathfrak{M}$ were irreducible and σ were any matrix in $\mathfrak{M}$ then σ would commute with every matrix in $\mathfrak{M}$ and therefore would be of the form $c\iota$, contradicting the irreducibility of $\mathfrak{M}$. Hence $\mathfrak{M}$ is reducible, and the result follows from the induction assumption. Actually, the form to which $\mathfrak{M}$ can be reduced may be specified more narrowly, as follows.

LEMMA 1. *An abelian set $\mathfrak{M}$ of matrices is equivalent to a set $\mathfrak{N}$ of the form* (1), *where $\mathfrak{N}_i$ is a square block of n_i rows ($n_1 + \cdots + n_r = n$, the degree of $\mathfrak{M}$) and the $\mathfrak{N}_i$-block of every σ in $\mathfrak{N}$ is in triangular form with equal elements on the main diagonal.*

For $n = 1$ this is obvious. Let $n > 1$ and suppose the result true for matrices of degree $< n$. If every matrix in $\mathfrak{M}$, assumed already in triangular form, has all its characteristic roots equal then the conclusion follows. Let $\sigma \in \mathfrak{M}$ have the characteristic equation $f(x) = (x - a_1)^{m_1} \cdots (x - a_q)^{m_q}$, $q > 1$, where $a_i \neq a_j$ when $i \neq j$. Writing $f_i(x) = f(x)\ (x - a_i)^{-m_i}$, we see that there are polynomials $p_i(x) \in \mathcal{C}[x]$ such that $1 = \sum_i p_i(x) f_i(x)$, so that $\iota = \sum_i p_i(\sigma) f_i(\sigma)$. Since a matrix satisfies its own characteristic equation, we have $f(\sigma) = 0$, and for any ζ in the vector space $\mathfrak{R}$ the element $\zeta_i = p_i(\sigma) f_i(\sigma) \zeta$ is in the linear subspace $\mathfrak{R}_i$ consisting of all η's such that $(\sigma - a_i\iota)^{m_i}\eta = 0$. It follows that $\mathfrak{R}$ is the direct sum

$$\mathfrak{R} = \mathfrak{R}_1 + \cdots + \mathfrak{R}_q$$

of the linear subspaces $\mathfrak{R}_i$. For any $\tau \in \mathfrak{M}$ we have

$$(\sigma - a_i\iota)^{m_i}\tau\mathfrak{R}_i = \tau(\sigma - a_i\iota)^{m_i}\mathfrak{R}_i = 0,$$

so that $\tau\mathfrak{R}_i \subseteq \mathfrak{R}_i$. Therefore, by choosing a set of basis vectors for $\mathfrak{R}$ consisting of bases of the individual subspaces $\mathfrak{R}_i$, we can reduce $\mathfrak{M}$ to the form

---

[5] This is false when $\mathcal{C}$ is not algebraically closed. E.g. the group of all matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ with real a and b not both 0, is abelian. But the characteristic roots are $a \pm b\sqrt{-1}$, so that in any reduction of this group to triangular form complex diagonal elements must appear.

(1) where each block $\mathfrak{N}_i$ is an abelian set of matrices of degree $<n$, and is, by the induction assumption, reducible to the desired form. But when each $\mathfrak{N}_i$ is so reduced then $\mathfrak{M}$ obviously is, too.

For a single matrix the form may be prescribed even more narrowly in various ways. For our purposes the following *Jordan normal form* (van der Waerden [1], vol. 2, §111) will be of importance.

LEMMA 2. *For any matrix τ there is an equivalent matrix σ of the form*

$$\sigma = \begin{pmatrix} \boxed{\begin{matrix} a_1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & a_1 \end{matrix}} & & & 0 \\ & \ddots & & \\ & & \boxed{\begin{matrix} a_t & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & a_t \end{matrix}} & \\ 0 & & & \end{pmatrix} \tag{2}$$

composed of square blocks along the main diagonal of the indicated type (zeros everywhere except in the main diagonal and the diagonal just above it) and zeros elsewhere.

2. Algebraic matric groups

A matrix of degree n may be regarded as a point in an n^2-dimensional affine space, the coordinates of the point being the elements of the matrix. Therefore we may speak of an algebraic manifold of matrices, and use the concepts of "defining ideal," "dimension," "generic zero" or "generic point," "specialization," etc., of modern algebraic geometry.

A (multiplicative) group $\mathfrak{G}$ of matrices of degree n is called *algebraic* if there exists an algebraic manifold in n^2-dimensional space such that: (a) every matrix σ in $\mathfrak{G}$ is a point on the algebraic manifold; and (b) every point σ on the algebraic manifold that is not a singular matrix is a matrix in $\mathfrak{G}$. If it is specified that the algebraic manifold not have an irreducible component consisting solely of singular matrices then the algebraic manifold is unique. This unique algebraic manifold will be called the *underlying manifold* of $\mathfrak{G}$.[6] The defining ideal of the underlying manifold of $\mathfrak{G}$ will be called the *defining ideal* of $\mathfrak{G}$.

EXAMPLES. 1. The *full matric group*, consisting of all nonsingular matrices of a given degree.

[6] Care must be exercised in using the words "reducible" and "irreducible." An algebraic matric group is reducible if the set of matrices in it is reducible in the sense of §1. The underlying manifold is reducible if it is the union of two algebraic manifolds neither of which contains the other.

2. The *full unimodular group*, consisting of all matrices of given degree with determinant 1.

3. The *identity group* $\mathfrak{E}$, consisting solely of the matrix ι.

4. Any *finite* matric group.

5. The *full triangular group* $\mathfrak{T}$, consisting of all matrices of given degree n which are in triangular form; and its subgroups $\mathfrak{T}_1, \cdots, \mathfrak{T}_n$ defined as follows: $\mathfrak{T}_1$ is the set of all matrices in special triangular form; for $2 \leqq i \leqq n$ $\mathfrak{T}_i$ is the set of all matrices in $\mathfrak{T}_1$ in which all the elements of the first $i - 1$ diagonals above the main diagonal are 0 (thus $\mathfrak{T}_n = \mathfrak{E}$).

6. The *full diagonal group* $\mathfrak{D}$, consisting of all nonsingular matrices of given degree which are in diagonal form.

THEOREM. *Let $\mathfrak{G}$ be an algebraic matric group. The irreducible components of the underlying manifold of $\mathfrak{G}$ are pairwise disjoint (except, possibly, for singular matrices), and all have the same dimension. The irreducible component which contains ι is the underlying manifold of a normal algebraic subgroup of $\mathfrak{G}$ of finite index equal to the number of irreducible components.*

PROOF. Let $\mathfrak{G}^*$ be the underlying manifold of $\mathfrak{G}$, and denote the irreducible components of $\mathfrak{G}^*$ by $\mathfrak{G}_0^*, \cdots, \mathfrak{G}_{h-1}^*$. Let $\mathfrak{G}_0^*, \cdots, \mathfrak{G}_g^*$ be those irreducible components which contain ι, and let $\sigma_0^*, \cdots, \sigma_g^*$ be independent generic points of $\mathfrak{G}_0^*, \cdots, \mathfrak{G}_g^*$, respectively. Now $\sigma_i^*\sigma_j^*$ is a generalized point of $\mathfrak{G}^*$, and therefore of some irreducible component $\mathfrak{G}_l^*$ of $\mathfrak{G}^*$. Since $\sigma_i^*\sigma_j^* \to \sigma_i^*\,\iota = \sigma_i^*$ is a specialization, we see that $\mathfrak{G}_l^* \supseteq \mathfrak{G}_i^*$, so that $l = i$. In the same way, $\sigma_i^*\sigma_j^* \to \iota\sigma_j^* = \sigma_j^*$ is a specialization, so that $l = j$, whence $i = j$. Since this holds for all i, j from 0 to g, we see that $g = 0$, and there is only one irreducible component $\mathfrak{G}_0^*$ containing ι.

Now let σ_j be any nonsingular matrix in $\mathfrak{G}_j^*$ $(j = 0, \cdots, h - 1)$. For each j, $\sigma_j^{-1}\mathfrak{G}_j^*$ is an irreducible algebraic manifold contained in $\mathfrak{G}^*$, and containing ι. Therefore $\sigma_j^{-1}\mathfrak{G}_j^* \subseteq \mathfrak{G}_0^*$, $\mathfrak{G}_j^* \subseteq \sigma_j\mathfrak{G}_0^*$, and $\mathfrak{G}^* = \sigma_0\mathfrak{G}_0^* \cup \cdots \cup \sigma_{h-1}\mathfrak{G}_0^*$. Since each $\sigma_j\mathfrak{G}_0^*$ is an irreducible algebraic manifold, and since the decomposition of an algebraic manifold into irreducible components is unique, it easily follows that

$$\mathfrak{G}_j^* = \sigma_j\mathfrak{G}_0^*, \qquad j = 0, \cdots, h - 1. \tag{3}$$

In the same way we find that

$$\mathfrak{G}_j^* = \mathfrak{G}_0^*\sigma_j, \qquad j = 0, \cdots, h - 1. \tag{4}$$

It follows from (3) that no element of $\mathfrak{G}$ (that is, no nonsingular matrix in $\mathfrak{G}^*$) is contained in more than one $\mathfrak{G}_j^*$, for if $\sigma \in \mathfrak{G}_{j_1}^* \cap \mathfrak{G}_{j_2}^*$ then $\mathfrak{G}_{j_1}^* = \sigma\mathfrak{G}_0^* = \mathfrak{G}_{j_2}^*$. It also follows from (3) that the dimension of every $\mathfrak{G}_j^*$ is the same as that of $\mathfrak{G}_0^*$.

Letting $j = 0$ in (3) we see that the product of any two nonsingular matrices in $\mathfrak{G}_0^*$ is itself in $\mathfrak{G}_0^*$. Also, for any nonsingular $\sigma_0 \in \mathfrak{G}_0^*$ we have $\sigma_0^{-1} \in \mathfrak{G}_0^*$, because if $\sigma_0^{-1} \in \mathfrak{G}_j^*$ then $\mathfrak{G}_j^* = \sigma_0^{-1}\mathfrak{G}_0^*$, $\iota \in \mathfrak{G}_j^*$, and $j = 0$. Consequently the set of nonsingular matrices in $\mathfrak{G}_0^*$ forms an algebraic group. From (3) and (4)

it is evident that this group is a normal subgroup of $\mathfrak{G}$ of index h. Thus the theorem is proved.

Henceforth, by the dimension of an algebraic matric group $\mathfrak{G}$ (notation: $\dim \mathfrak{G}$) we shall mean the dimension of its underlying manifold, that is, the dimension of each of the irreducible components. The algebraic subgroup of $\mathfrak{G}$ of which the underlying manifold is the irreducible component which contains ι will be called the *component of the identity* of $\mathfrak{G}$, and will be denoted by $\mathfrak{G}^0$. $\mathfrak{G}$ will be called *connected* if its underlying manifold is irreducible, that is, if $\mathfrak{G} = \mathfrak{G}^0$.

It follows from the theorem just proved that if $\mathfrak{G}$ is not connected then $\mathfrak{G}$ contains an algebraic subgroup of finite index > 1 (for example $\mathfrak{G}^0$). Conversely, *if $\mathfrak{G}$ contains an algebraic subgroup of finite index > 1 then $\mathfrak{G}$ is not connected.* For, if the index of the algebraic subgroup $\mathfrak{H}$ is h then $\mathfrak{G} = \sigma_1\mathfrak{H} \cup \cdots \cup \sigma_h\mathfrak{H}$, so that if $\mathfrak{G}^*$ and $\mathfrak{H}^*$ are the underlying manifolds of $\mathfrak{G}$ and $\mathfrak{H}$, respectively, then $\mathfrak{G}^* = \sigma_1\mathfrak{H}^* \cup \cdots \cup \sigma_h\mathfrak{H}^*$. It is easy to see that $\sigma_i\mathfrak{H}^* \not\subseteq \sigma_i\mathfrak{H}^*$ if $i \neq j$, so that $\mathfrak{G}$ can not be connected if $h > 1$.

3. Jordan-Hölder-Schreier theorem

The following lemma will be used to show that certain subgroups of an algebraic matric group are algebraic.

LEMMA 1. *Let $\mathfrak{G}$ be an algebraic matric group, $\mathfrak{H}$ a subgroup (not assumed algebraic) such that $\mathfrak{G} - \mathfrak{H}$ is contained in an algebraic manifold of lower dimension than $\mathfrak{G}$. Then $\mathfrak{H} = \mathfrak{G}$.*

PROOF. Expressing $\mathfrak{G}$ as the union of the cosets of $\mathfrak{H}$,

$$\mathfrak{G} = \bigcup_{\lambda \geqq 1} \sigma_\lambda \mathfrak{H} \qquad (\sigma_1 = \iota),$$

we see that if there are more than one coset then $\sigma_2\mathfrak{H} \subseteq \mathfrak{G} - \mathfrak{H}$ is contained in an algebraic maifold of dimension lower than that of $\mathfrak{G}$. Hence $\mathfrak{H}$, which is a linear mapping of $\sigma_2\mathfrak{H}$, is contained in such a manifold, so that $\mathfrak{G} = \mathfrak{H} \cup (\mathfrak{G} - \mathfrak{H})$ is contained in the union of two algebraic manifolds of lower dimension, which is impossible. Therefore there is only one coset, that is, $\mathfrak{H} = \mathfrak{G}$.

By contrast with Lemma 1, the following lemma will be used to show that certain algebraic manifolds are the underlying manifolds of algebraic matric groups.

LEMMA 2. *If $\mathfrak{G}$ is a group of matrices (not assumed algebraic) and $\mathfrak{G}^*$ is the smallest algebraic manifold containing $\mathfrak{G}$, then $\mathfrak{G}^*$ is the underlying manifold of an algebraic matric group.*

PROOF. Let $\mathfrak{g}$ be the set of all polynomials in n^2 indeterminates (n = the degree of the matrices) with coefficients in $\mathcal{C}$ which vanish for all matrices in $\mathfrak{G}$, that is, let $\mathfrak{g}$ be the defining ideal of $\mathfrak{G}^*$. If $f(\xi) \in \mathfrak{g}$ then $f(\sigma\xi) \in \mathfrak{g}$ for any $\sigma \in \mathfrak{G}$, because $\sigma\tau \in \mathfrak{G}$ whenever $\sigma, \tau \in \mathfrak{G}$. Consequently, $f(\xi\tau) \in \mathfrak{g}$ for any $\tau \in \mathfrak{G}^*$, whence $\sigma\tau \in \mathfrak{G}^*$ whenever $\sigma, \tau \in \mathfrak{G}^*$. Again, since $\sigma^{-1} \in \mathfrak{G}$ whenever $\sigma \in \mathfrak{G}$, it is clear that $f(\xi^{-1})$ multiplied by a sufficiently high power of the determinant

of ξ is a polynomial in $\mathfrak{g}$. Therefore the inverse of every nonsingular matrix in $\mathfrak{G}^*$ is itself in $\mathfrak{G}^*$. Thus, the set of all nonsingular matrices in $\mathfrak{G}^*$ forms an algebraic group.

It is obvious that the intersection of two algebraic matric groups is an algebraic group. As the first application of Lemmas 1 and 2 we derive another lemma.

LEMMA 3. *Let $\mathfrak{G}$ be an algebraic matric group, $\mathfrak{H}$ an algebraic subgroup, $\mathfrak{N}$ a normal algebraic subgroup. Then $\mathfrak{H}\mathfrak{N}$ is an algebraic subgroup of $\mathfrak{G}$.*

PROOF. $\mathfrak{H}\mathfrak{N}$ is a group; we must prove it algebraic. Let $\mathfrak{H}^*$ and $\mathfrak{N}^*$ be the underlying manifolds of $\mathfrak{H}$ and $\mathfrak{N}$, respectively, and let $\mathfrak{M}^*$ be the smallest algebraic manifold containing $\mathfrak{H}\mathfrak{N}$. By Lemma 2 $\mathfrak{M}^*$ is the underlying manifold of an algebraic group $\mathfrak{M}$. Clearly $\mathfrak{H}\mathfrak{N} \subseteq \mathfrak{M}$ and $\mathfrak{M} - \mathfrak{H}\mathfrak{N} \subseteq \mathfrak{M}^* - \mathfrak{H}^*\mathfrak{N}^*$. By Lemma 1 it suffices to show that $\mathfrak{M}^* - \mathfrak{H}^*\mathfrak{N}^*$ is contained in an algebraic manifold of lower dimension than $\mathfrak{M}^*$, for then $\mathfrak{H}\mathfrak{N} = \mathfrak{M}$, so that $\mathfrak{H}\mathfrak{N}$ is algebraic. To this end let $\chi_1, \cdots, \chi_r, \nu_1, \cdots, \nu_s$ be independent generic points of the r irreducible components of $\mathfrak{H}^*$ and the s irreducible components of $\mathfrak{N}^*$. If $\mathfrak{M}^*_{ij}$ is the irreducible algebraic manifold with generic point $\chi_i\nu_j$ then clearly $\mathfrak{M}^* = \bigcup_{i,j} \mathfrak{M}^*_{ij}$. Therefore every $\sigma \in \mathfrak{M}^*$ is obtained by a specialization $\chi_i\nu_j \to \sigma$. Such a specialization can be extended to a specialization of the form $(\chi_i\nu_j, \chi_i, \nu_j) \to (\sigma, \chi_{0i}, \nu_{0j})$ provided the ideal of all polynomials in $\mathcal{C}[\cdots, x_{ab}, \cdots; \cdots, y_{cd}, \cdots; \cdots, z_{ef}, \cdots]$ which vanish for $(x_{ab}) = \chi_i\nu_j$, $(y_{cd}) = \chi_i$, $(z_{ef}) = \nu_j$ still has a zero when (x_{ab}) is replaced by σ, that is, if for a finite basis of this ideal the polynomials obtained by replacing (x_{ab}) by σ have a common zero. By the general theory of resultants (van der Waerden [1], vol. 2, chapter 11) this will be the case provided a certain polynomial in $\mathcal{C}[\cdots, x_{ab}, \cdots]$ which does not vanish at $\chi_i\nu_j$ still fails to vanish at σ. Thus, whenever σ does not lie on a certain algebraic submanifold of $\mathfrak{M}^*$ of lower dimension than $\mathfrak{M}^*$, there exist $\chi \in \mathfrak{H}$, $\nu \in \mathfrak{N}$ such that $\sigma = \chi\nu$.

We are now in a position to establish the following Jordan-Hölder-Schreier theorem.

THEOREM. *Any two normal chains of an algebraic matric group have isomorphic refinements.*

PROOF. Here "normal chain" means a sequence $\mathfrak{G} \supseteq \mathfrak{G}_1 \supseteq \cdots \supseteq \mathfrak{G}_{r-1} \supseteq \mathfrak{E}$ in which each member is a normal *algebraic* subgroup of its predecessor. The proof of the classical Jordan-Hölder-Schreier theorem as give by Zassenhaus [1] (pp. 50–52) consists in actually constructing groups yielding the desired refinements. Zassenhaus' construction suffices in the present case provided the constructed groups turn out to be algebraic. That this is the case follows from Lemma 3 and the fact that all the constructed groups are of the form $\mathfrak{G}_i(\mathfrak{G}_{i-1} \cap \mathfrak{H}_k)$, where $\mathfrak{G} = \mathfrak{G}_0 \supseteq \cdots \supseteq \mathfrak{G}_r = \mathfrak{E}$ and $\mathfrak{G} = \mathfrak{H}_0 \supseteq \cdots \supseteq \mathfrak{H}_s = \mathfrak{E}$ are the given normal chains.

4. Commutator groups

The *commutator* of two elements σ, τ of a group is the element $\sigma\tau\sigma^{-1}\tau^{-1}$. By the *commutator group* of an algebraic matric group we shall mean the smallest

algebraic subgroup of $\mathfrak{G}$ that contains the commutator of every pair of matrices in $\mathfrak{G}$. We shall denote the commutator group of $\mathfrak{G}$ by $\mathfrak{G}'$.

Since $\mathfrak{G}'$ is an algebraic group we can form its commutator group $\mathfrak{G}''$, etc., thus obtaining the *sequence of commutator groups* $\mathfrak{G}, \mathfrak{G}', \cdots, \mathfrak{G}^{(i)}, \cdots$. Since the underlying manifolds of the groups of this sequence form a decreasing sequence, they must, beginning with some index j, all be the same. We say, in this case, that the sequence of commutator groups terminates with $\mathfrak{G}^{(j)}$.

It is easy to see that $\mathfrak{G}'$ is the smallest normal algebraic subgroup of $\mathfrak{G}$ for which the factor group is abelian.

EXAMPLE. Consider the algebraic matric groups $\mathfrak{T} = \mathfrak{T}_0, \mathfrak{T}_1, \cdots, \mathfrak{T}_n = \mathfrak{E}$ (§2 Example 5). In the product of two matrices in $\mathfrak{T}$ the elements on the main diagonal are the products of the corresponding elements in the two factor matrices. Therefore the commutator of two matrices in $\mathfrak{T}$ is always in $\mathfrak{T}_1$. In the product of two matrices in $\mathfrak{T}_i (1 \leqq i \leqq n-1)$ the elements on the i^{th} diagonal above the main one are the sums of the corresponding elements in the two factor matrices. Therefore the commutator of two elements in $\mathfrak{T}_i$ is always in $\mathfrak{T}_{i+1}$.

LEMMA. *If an algebraic matric group $\mathfrak{G}$ is connected then so is $\mathfrak{G}'$.*

PROOF. Let $\sigma_1, \tau_1, \sigma_2, \tau_2, \cdots$ be a sequence of independent generic points of $\mathfrak{G}^*$, the underlying manifold of $\mathfrak{G}$. Let $\mathfrak{H}_i^*$ be the irreducible manifold with generic point $\chi_i = \sigma_1\tau_1\sigma_1^{-1}\tau_1^{-1} \cdots \sigma_i\tau_i\sigma_i^{-1}\tau_i^{-1}$. Now $\chi_i = \chi_{i-1}\sigma_i\tau_i\sigma_i^{-1}\tau_i^{-1}$, so that $\chi_i \to \chi_{i-1}$ is a specialization, and $\mathfrak{H}_{i-1}^* \subseteq \mathfrak{H}_i^*$. Since each $\mathfrak{H}_i^*$ is irreducible, the dimension of $\mathfrak{H}_{i-1}^*$ is less than that of $\mathfrak{H}_i^*$ when $\mathfrak{H}_{i-1}^* \subset \mathfrak{H}_i^*$, so that there is a j such that $\mathfrak{H}_k^* = \mathfrak{H}_j^*$ for all $k \geqq j$. It is clear that $\mathfrak{H}_j^*$ is the smallest algebraic manifold containing the set $\mathfrak{K}$ of all produts of commutators of matrices in $\mathfrak{G}$. Since $\mathfrak{K}$ obviously is a group, it follows from §3 Lemma 2 that $\mathfrak{H}_j^*$ is the underlying manifold of an algebraic matric group, which is clearly $\mathfrak{G}'$. As $\mathfrak{H}_j^*$ is irreducible, $\mathfrak{G}'$ is connected.

5. Solvable algebraic matric groups

An algebraic matric group $\mathfrak{G}$ will be called *solvable* if it has a normal chain in which all the factor groups are abelian.

It is easy to see that $\mathfrak{G}$ is solvable if and only if its sequence of commutator groups terminates with $\mathfrak{E}$. Moreover, if $\mathfrak{G}$ is solvable then so is every algebraic subgroup of $\mathfrak{G}$. Consequently, if $\mathfrak{G}$ is solvable then, for a suitable j,

$$\mathfrak{G} \supseteq \mathfrak{G}^0 \supseteq \mathfrak{G}^{0'} \supseteq \cdots \supseteq \mathfrak{G}^{0(j)} = \mathfrak{E}$$

is a normal chain in which every member after the first is connected, all the factor groups after the first are abelian, and $\mathfrak{G}/\mathfrak{G}^0$ is a solvable finite group.

EXAMPLE. By the example in §4, we have $\mathfrak{T}_i' \subseteq \mathfrak{T}_{i+1}$ $(i = 0, \cdots, n-1)$. Therefore $\mathfrak{T} = \mathfrak{T}_0 \supset \cdots \supset \mathfrak{T}_n = \mathfrak{E}$ is a normal chain of $\mathfrak{T}$ in which all the factor groups are abelian. Hence $\mathfrak{T}$ is solvable.

The following lemma will be used in §7 to permit an induction on the degree of the matrices of a group.

LEMMA. *Let $\mathfrak{G}$ be an algebraic group of matrices of degree n of the form*

$$\mathfrak{G} = \begin{pmatrix} \mathfrak{G}_1 & * \\ 0 & \mathfrak{G}_2 \end{pmatrix},$$

where the blocks $\mathfrak{G}_1$ and $\mathfrak{G}_2$ are of degree n_1 and n_2, respectively ($n_1 + n_2 = n$, $0 < n_1 < n$). Then $\mathfrak{G}_1$ and $\mathfrak{G}_2$ are algebraic matric groups homomorphic to $\mathfrak{G}$. If $\mathfrak{G}$ is connected then so are $\mathfrak{G}_1$ and $\mathfrak{G}_2$. If $\mathfrak{H}$ is a normal algebraic subgroup of $\mathfrak{G}$, and $\mathfrak{H}_k$ the corresponding subgroup of $\mathfrak{G}_k$ ($k = 1, 2$), then $\mathfrak{H}_k$ is a normal algebraic subgroup of $\mathfrak{G}_k$. If, moreover, $\mathfrak{G}/\mathfrak{H}$ is abelian then $\mathfrak{G}_k/\mathfrak{H}_k$, is, too. Consequently, if $\mathfrak{G}$ is solvable then so is $\mathfrak{G}_k$.

PROOF. It is clear that $\mathfrak{G}_k$ is a group and that if $\sigma = \begin{pmatrix} \tau_1 & * \\ 0 & \tau_2 \end{pmatrix}$ then $\sigma \to \tau_k$ is a homomorphism of $\mathfrak{G}$ onto $\mathfrak{G}_k$. To show that $\mathfrak{G}_k$ is algebraic let $\mathfrak{K}_k^*$ be the smallest algebraic manifold (in n_k^2-dimensional affine space) containing $\mathfrak{G}_k$. By §3 Lemma 2, $\mathfrak{K}_k^*$ is the underlying manifold of an algebraic group $\mathfrak{K}_k$. As in the proof of Lemma 3 in §3, we see that $\mathfrak{K}_k - \mathfrak{G}_k$ is contained in an algebraic manifold of lower dimension. Therefore, by §3 Lemma 1, $\mathfrak{G}_k = \mathfrak{K}_k$, so that $\mathfrak{G}_k$ is algebraic. The defining ideal of $\mathfrak{G}_k$ consists of all those polynomials in the defining ideal of $\mathfrak{G}$ which involve only the appropriate n_k^2 indeterminates, so that the former ideal is prime whenever the latter is, that is, $\mathfrak{G}_k$ is connected whenever $\mathfrak{G}$ is. By the part of the lemma already proved, the homomorphism $\sigma \to \tau_k$ maps $\mathfrak{H}$ onto an algebraic subgroup $\mathfrak{H}_k$ of $\mathfrak{G}_k$. It is now obvious that $\mathfrak{H}_k$ is normal in $\mathfrak{G}_k$, and that $\mathfrak{G}_k/\mathfrak{H}_k$ is abelian if $\mathfrak{G}/\mathfrak{H}$ is.

6. Anticompact and quasicompact algebraic matric groups

An algebraic matric group $\mathfrak{G}$ will be called *anticompact* if it contains no element other than ι of finite order not divisible by p (the characteristic of $\mathcal{C}$). $\mathfrak{G}$ will be called *quasicompact* if no algebraic subgroup of $\mathfrak{G}$ of order > 1 is anticompact (equivalently: $\mathfrak{G}$ will be called quasicompact if every algebraic subgroup of $\mathfrak{G}$ of order > 1 contains an element other than ι of finite order not divisible by p, and will be called anticompact if no algebraic subgroup of $\mathfrak{G}$ of order > 1 is quasicompact). It is clear that an algebraic subgroup of $\mathfrak{G}$ is anticompact (or is quasicompact) whenever $\mathfrak{G}$ is.

The following two theorems provide characterizations of these two types of groups.

THEOREM 1. *Let u be a positive integer, $\mathfrak{G}$ be an algebraic matric group. A necessary and sufficient condition that $\mathfrak{G}$ contain no matrix of finite order not divisible by p and not dividing u, is that every matrix in $\mathfrak{G}$ have all its characteristic roots equal to u^{th} roots of unity. Thus (taking $u = 1$), $\mathfrak{G}$ is anticompact if and only if every matrix in $\mathfrak{G}$ has all its characteristic roots equal to 1, that is, each matrix in $\mathfrak{G}$ is reducible to special triangular form.*

PROOF. SUFFICIENCY. Suppose every matrix in $\mathfrak{G}$ has characteristic roots as stated. Let σ be any matrix in $\mathfrak{G}$ of finite order m not dividing u, and choose

a basis for the vector space $\mathfrak{N}$ so that σ is in its Jordan normal form (2). Since m does not divide u, σ actually has a 1 in the diagonal just above the main one. Raising σ to the m^{th} power replaces this 1 by ma_i^{m-1}. Since $\sigma^m = \iota$ and $a_i \neq 0$, m must be divisible by p.

NE ESSI Y. Suppose $\mathfrak{G}$ contains a matrix σ which has a characteristic root not a u^{th} root of unity. We must show that $\mathfrak{G}$ then contains a matrix of finite order not divisible by p and not dividing u.

As before, choose a basis of $\mathfrak{N}$ such that σ is given by (2). It is easy to see that the element in the i^{th} row and j^{th} column of the h^{th} block of σ^k ($k = 0, \pm 1, \pm 2, \cdots$) is $\binom{k}{j-i} a_h^{i-j+k}$ where, as is customary,

$$\binom{x}{m} = \begin{cases} 0 & \text{for } m < 0, \\ 1 & \text{for } m = 0 \\ \dfrac{x(x-1)\cdots(x-m+1)}{m!} & \text{for } m > 0 \end{cases}$$

(this binomial coefficient $\binom{x}{m}$ is defined for any element x in an extension of $\mathcal{C}$ if $p = 0$, for any integer x if $p \neq 0$).

Let $\tau_n(a, b, c) = (t_{ij})$ be the matrix of degree n defined by

$$t_{ij} = \binom{c}{j-i} a^{i-j} b.$$

By the easily established relation

$$\sum_{i=0}^{k} \binom{c}{k-i}\binom{c'}{i} = \binom{c+c'}{k}$$

it readily follows that

$$\tau_n(a, b, c) \cdot \tau_n(a, b', c') = \tau_n(a, bb', c + c').$$

Now let $\mathfrak{H}$ be the algebraic subgroup of $\mathfrak{G}$ consisting of all matrices $\tau(b_1, \cdots, b_\iota, c_1, \cdots, c_\iota)$ in $\mathfrak{G}$ of the form

$$\tau(b_1, \cdots, b_\iota, c_1 \cdots, c_\iota) = \begin{pmatrix} \boxed{\tau_{n_1}(a_1, b_1, c_1)} & & 0 \\ & \ddots & \\ 0 & & \boxed{\tau_{n_\iota}(a_\iota, b_\iota, c_\iota)} \end{pmatrix}$$

(same number of blocks as in σ; each block of the same degree as the corresponding block in σ; $a_1, \cdots, a_\iota$ the same as in σ; $b_1, \cdots, b_\iota \in \mathcal{C}$; $c_1, \cdots, c_\iota \in \mathcal{C}$ if $p = 0$, $c_1, \cdots, c_\iota$ integers if $p \neq 0$).

If $\tau(b_1, \cdots, b_\iota, c_1, \cdots, c_\iota)$ now denotes a generic point of the underlying manifold of the component of the identity $\mathfrak{H}^0$ then each b_i either is 1 or is trans-

cendental over $\mathcal{C}$ (because $\tau(b_1, \cdots, b_t, c_1, \cdots, c_t) \to \iota = \tau(1, \cdots, 1, 0, \cdots, 0)$ is a specialization). We first show that

$$\partial^0\mathcal{C}(b_1, \cdots, b_t, c_1, \cdots, c_t)/\mathcal{C}(b_1, \cdots, b_t) = \partial^0\mathcal{C}(c_1, \cdots, c_t)/\mathcal{C}$$

To do this it suffices to show that if some of the c_i's are algebraically dependent over $\mathcal{C}(b_1, \cdots, b_t)$ then they are over $\mathcal{C}$, too. Suppose, say, that $c_1, \cdots, c_q$ are algebraically dependent over $\mathcal{C}(b_1, \cdots, b_t)$, or what is the same thing, over $\mathcal{C}(b_{i_1}, \cdots, b_{i_r})$, where $b_{i_1}, \cdots, b_{i_r}$ is a maximal set of the b_i's algebraically independent over $\mathcal{C}$. Then there is a nonzero polynomial

$$f(x_1, \cdots, x_q) \neq \cdots + \phi(b_{i_1}, \cdots, b_{i_r})x_1^{j_1} \cdots x_q^{j_q} + \cdots,$$

with coefficients which are rational functions over $\mathcal{C}$ of $b_{i_1}, \cdots, b_{i_r}$, which vanishes for $x_1 = c_1, \cdots, x_q = c_q$. We choose such a polynomial $f(x_1, \cdots, x_q)$ with as few terms as possible, and denote its degree by d. We suppose, as we may, that the coefficient in one of the terms of $f(x_1, \cdots, x_q)$ of degree d is 1.

Now $\tau(b_1, \cdots, b_t, c_1, \cdots, c_t)^k = \tau(b_1^k, \cdots, b_t^k, kc_1, \cdots, kc_t)$ is a generalized point of $\mathfrak{H}^0$ for every integral k, so that $x_1 = kc_1, \cdots, x_t = kc_t$ annuls

$$\cdots + \phi(b_{i_1}^k, \cdots, b_{i_r}^k)x_1^{j_1} \cdots x_q^{j_q} + \cdots,$$

that is, $x_1 = c_1, \cdots, x_q = c_q$ annuls the polynomials

$$\cdots + \phi(b_{i_1}^k, \cdots, b_{i_r}^k)k^{j_1+\cdots+j_q}x_1^{j_1} \cdots x_q^{j_q} \cdot + \cdots.$$

Since the coefficient in one of the terms of $f(x_1, \cdots, x_q)$ is 1, the difference between $f(x_1, \cdots, x_q)$ and one of these polynomials divided by k^d has fewer terms than $f(x_1, \cdots, x_q)$ has. Therefore this difference must be 0, and for each coefficient $\phi(b_{i_1}, \cdots, b_{i_r})$ we must have

$$\phi(b_{i_1}^k, \cdots, b_{i_r}^k) = k^{d-j_1-\cdots-j_q}\phi(b_{i_1}, \cdots, b_{i_r}).$$

Since $b_{i_1}, \cdots, b_{i_r}$ are algebraically independent over $\mathcal{C}$, it follows that each $\phi(b_{i_1}, \cdots, b_{i_r})$ is in $\mathcal{C}$, so that $c_1, \cdots, c_q$ are algebraically dependent over $\mathcal{C}$ This proves our remark concerning degrees of transcendency.

It now follows that

$$\partial^0\mathcal{C}(b_1, \cdots, b_t, c_1, \cdots, c_t)/\mathcal{C} = \partial^0\mathcal{C}(b_1, \cdots, b_t)/\mathcal{C} + \partial^0\mathcal{C}(c_1, \cdots, c_t)/\mathcal{C}.$$

Therefore, letting $\mathfrak{m}$ be the prime ideal in $\mathcal{C}[x_1, \cdots, x_t, y_1, \cdots, t_t]$ with generic zero $b_1, \cdots, b_t, c_1, \cdots, c_t$, and letting $\mathfrak{p} = \mathfrak{m} \cap \mathcal{C}[x_1, \cdots, x_t]$, $\mathfrak{q} = \mathfrak{m} \cap \mathcal{C}[y_1, \cdots, y_n]$, we see that $b_1, \cdots, b_t$ and $c_1, \cdots, c_t$ are independent generic zeros of $\mathfrak{p}$ and $\mathfrak{q}$, respectively. This implies that a specialization of $b_1, \cdots, b_t$ and a specialization of $c_1, \cdots, c_t$ can always be combined to form a specialization of $b_1, \cdots, b_t, c_1, \cdots, c_t$.

If $b_1, \cdots, b_t$ are not all 1 then $r > 0$, and we may find a positive integer v not dividing u and specialize

$$(5) \qquad b_1 \to \beta_1, \cdots, b_t \to \beta_t \qquad (\beta_1 \cdots \beta_t \neq 0)$$

in such a way that $\beta_i, \cdots, \beta_{i_r}$ are all v^{th} roots of unity other than u^{th} roots of unity. But then we may suppose that every β_i is a root of unity. To see this consider, for any $i \neq i_1, \cdots, i_r$, an irreducible nonzero polynomial $f_i(x_i, b_{i_1}, \cdots, b_{i_r}) \in \mathcal{C}[x_1, b_{i_1}, \cdots, b_{i_r}]$ which vanishes for $x_i = b_i$. Referring to $\tau(b_1, \cdots, b_t, c_1, \cdots, c_t)^{kv+1}$ we see that

$$f_i(\beta_i^{kv+1}, \beta_{i_1}, \cdots, \beta_{i_r}) = 0, \qquad k = 0, 1, 2, \cdots$$

We assume, as we may, that the specialization (5) is such that $f_i(x_i, \beta_{i_1}, \cdots, \beta_{i_r}) \neq 0$. Then we see that β_i^{kv+1} is the same for two different values of k, so that β_i is a root of unity.

Now, since $\tau(1, \cdots, 1, 0; \cdots, 0) = \iota \in \mathfrak{H}^0$,

$$c_1 \to 0, \cdots, c_t \to 0 \tag{6}$$

is a specialization. Therefore, if $b_1, \cdots, b_t$ are not all 1, we may combine the specializations (5) and (6) to obtain a matrix in $\mathfrak{H}^0$ which is in diagonal form and in which all the elements on the main diagonal are roots of unity (not all these roots of unity being u^{th} roots of unity). Such a matrix is of finite order not divisible by p and not dividing u.

It remains to consider the case in which $b_1, \cdots, b_t$ are all 1. In this case, since $\sigma^h \in \mathfrak{H}^0$ (h = index of $\mathfrak{H}^0$ in $\mathfrak{H}$), there is a smallest positive integer k such that the diagonal elements $a_1, \cdots, a_t$ af σ are all k^{th} roots of unity, and this k is not divisible by p and does not divide u (for the characteristic roots $a_1, \cdots, a_t$ are by hypothesis not all u^{th} roots of unity).

Now $\sigma = \tau(a_1, \cdots, a_t, 1, \cdots, 1)$, so that for all $j = 0, 1, 2, \cdots$

$$\tau(1, \cdots, 1, kj, \cdots, kj) = \sigma^{kj} \in \mathfrak{H}.$$

In the case $p = 0$, this means that $\mathfrak{H}$ contains an infinite number of points of the one-dimensional algebraic manifold of all matrices $\tau(1, \cdots, 1, \gamma, \cdots, \gamma)$ with $\gamma \in \mathcal{C}$, so that $\mathfrak{H}$ contains every nonsingular such matrix, and in particular contains $\tau(1, \cdots, 1, -1, \cdots, -1)$. In the case $p \neq 0$, $\tau(1, \cdots, 1, p^m, \cdots, p^m) = \iota$ provided $p^m \geqq n$. Since k is relatively prime to p, there is a j such that $kj \equiv -1 \pmod{p^m}$, whence $\sigma^{kj} = \tau(1, \cdots, 1, -1, \cdots, -1)$. Hence, in either case, $\mathfrak{H}$ contains $\sigma \cdot \tau(1, \cdots, 1, -1, \cdots, -1) = \tau(a_1, \cdots, a_t, 1, \cdots, 1) \cdot \tau(1, \cdots, 1, -1, \cdots, -1) = \tau(a_1, \cdots, a_t, 0, \cdots, 0)$, which is in diagonal form with diagonal elements $a_1, \cdots, a_t$. Thus $\mathfrak{H}$ contains a matrix of order k not divisible by p and not dividing u. This completes the proof.

THEOREM 2. *Let $\mathfrak{G}$ be an algebraic matric group. A necessary and sufficient condition that $\mathfrak{G}$ be quasicompact is that each matrix in $\mathfrak{G}$ be reducible to diagonal form.*

PROOF. SUFFICIENCY. Suppose every matrix in $\mathfrak{G}$ is so reducible. Let $\mathfrak{G}_1$ be an algebraic subgroup of $\mathfrak{G}$ of order > 1. We must show that $\mathfrak{G}_1$ contains an element of finite order not divisible by p. Let σ be an element of $\mathfrak{G}_1$ other than ι, and choose a basis for the vector space $\mathfrak{R}$ in such a way that σ is in diagonal form. Let $\mathfrak{G}_2$ be the set of all matrices in $\mathfrak{G}_1$ which are in diagonal

form. If $\mathfrak{G}_2^0 = \mathfrak{E}$ then each diagonal element of σ is a root of unity and σ itself is of finite order not divisible by p. If $\mathfrak{G}_2^0 \neq \mathfrak{E}$ then a generic point of the underlying manifold of $\mathfrak{G}_2^0$ can be specialized to a matrix τ_0 in which all the diagonal elements are roots of unity not all 1. Then τ_0 is of finite order not divisible by p.

NECESSITY. Suppose $\mathfrak{G}$ is quasicompact, and let σ be any matrix in $\mathfrak{G}$ other than ι. We must show that σ is reducible to diagonal form. As in the proof of Theorem 1, let σ be give by (2), and introduce the groups $\mathfrak{H}$, $\mathfrak{H}^0$ and the generic point $\tau(b_1, \cdots, b_t, c_1, \cdots, c_t)$ of the underlying manifold of $\mathfrak{H}^0$.

We first show that $\tau(b_1, \cdots, b_t, c_1, \cdots, c_t)$ is in diagonal form. Suppose that this is false. Then there is a specialization

$$c_1 \to \gamma_1, \cdots, c_t \to \gamma_t \quad (\gamma_1, \cdots, \gamma_t \in \mathfrak{C}, \text{ not every } \gamma_i = 0).$$

Again, since $\iota \in \mathfrak{H}^0$,

$$b_1 \to 1, \cdots, b_t \to 1$$

is a specialization. As we saw in the proof of Theorem 1, we can combine these two specializations to obtain a specialization of $\tau(b_1, \cdots, b_t, c_1, \cdots, c_t)$. Therefore the algebraic group $\mathfrak{K}$, consisting of all matrices in $\mathfrak{H}$ in which all elements on the main diagonal are 1, properly contains $\mathfrak{E}$. But by Theorem 1, $\mathfrak{K}$ is anticompact, so that $\mathfrak{K} = \mathfrak{E}$. This contradiction shows that every matrix in $\mathfrak{H}^0$ is in diagonal form.

Now suppose that σ is not in diagonal form, that is, that not every block of σ in (2) is of degree 1. Then σ is contained in an irreducible component $\mathfrak{H}_1^*$ of the underlying manifold of $\mathfrak{H}$ for which

$$\sigma \cdot \tau(b_1, \cdots, b_t, 0, \cdots, 0) = \tau(a_1, \cdots, a_t, 1, \cdots, 1) \cdot \tau(b_1, \cdots, b_t, 0, \cdots, 0)$$
$$= \tau(a_1 b_1, \cdots, a_t b_t, 1, \cdots, 1)$$

is a generic point (see §2). As in the proof of Theorem 1, let $b_{i_1}, \cdots, b_{i_r}$ be a maximal set of b_i's algebraically independent over $\mathfrak{C}$. For each $i \neq i_1, \cdots, i_r$ there is a nonzero polynomial $g_i(x_i, a_{i_1} b_{i_1}, \cdots, a_{i_r} b_{i_r}) \in \mathfrak{C}[x_i, a_{i_1} b_{i_1}, \cdots, a_{i_r} b_{i_r}]$ such that $g_i(a_i b_i, a_{i_1} b_{i_1}, \cdots, a_{i_r} b_{i_r}) = 0$. We now specialize

$$b_1 \to \beta_1, \cdots, b_t \to \beta_t \qquad (\beta_1 \cdots \beta_t \neq 0)$$

in such a way that $a_{i_1}\beta_{i_1}, \cdots, a_{i_r}\beta_{i_r}$ are all roots of unity and every $g_i(x_i, a_{i_1}\beta_{i_1}, \cdots, a_{i_r}\beta_{i_r}) \neq 0$. If v is a multiple of the order of $\mathfrak{H}/\mathfrak{H}^0$ such that $(a_{i_1}\beta_{i_1})^v = \cdots = (a_{i_r}\beta_{i_r})^v = 1$, then $\tau(a_1\beta_1, \cdots, a_t\beta_t, 1, \cdots, 1)^{kv+1} \in \mathfrak{H}_1^*$ for $k = 0, 1, \cdots$. Therefore

$$g((a_i\beta_i)^{kv+1}, a_{i_1}\beta_{i_1}, \cdots, a_{i_r}\beta_{i_r}) = 0, k = 0, 1, \cdots,$$

so that every $a_i\beta_i$ is a root of unity.

Letting s be the smallest positive integer such that every $(a_i\beta_i)^s = 1$, we see that s is not divisible by p, and $\tau(a_1\beta_1, \cdots, a_t\beta_t, 1, \cdots, 1)^s = \tau(1, \cdots, 1, s, \cdots, s)$ is a matrix in $\mathfrak{H}$ which is not in diagonal form and in which all the

elements on the main diagonal are 1. As above, this leads to a contradiction. Therefore σ is in diagonal form and the proof is complete.

7. Reducibility to triangular form

In this section a necessary and sufficient condition is derived for a set of matrices to be reducible to triangular form, and the bearing of anticompactness and quasicompactness on reducibility to triangular form is studied.

THEOREM 1. *A necessary and sufficient condition that a set of matrices of degree n be reducible to triangular form is that the set be contained in the underlying manifold of a connected solvable algebraic matric group.*

PROOF. SUFFICIENCY. It is enough to show that a connected solvable algebraic matric group $\mathfrak{G}$ is reducible to triangular form. For $n = 1$ this is obvious. Let $n > 1$ and suppose the theorem verified for matrices of lower degree. If $\mathfrak{G}$ is reducible then by the induction assumption and the lemma of §5, $\mathfrak{G}$ is clearly reducible to triangular form. We suppose, then, that $\mathfrak{G}$ is irreducible and seek a contradiction.

By §5, $\mathfrak{G}$ has a normal chain

$$\mathfrak{G} = \mathfrak{G}_0 \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_h = \mathfrak{E}$$

in which each $\mathfrak{G}_i$ is connected and each $\mathfrak{G}_{i-1}/\mathfrak{G}_i$ is abelian. If the chain length h equals 1 then $\mathfrak{G}$ is abelian and (by §1 Lemma 1) reducible to triangular form, and therefore is reducible. Suppose that $h > 1$, and that every connected solvable algebraic matric group of degree n which has a normal chain as above of length $< h$ is reducible. Then $\mathfrak{G}_1$ is reducible, and therefore reducible to triangular form. Consequently the vector space $\mathfrak{N}$ contains a vector η which is a characteristic vector for every $\sigma_1 \in \mathfrak{G}_1$. Let $\mathfrak{N}_1$ be the linear subspace of $\mathfrak{N}$ spanned by all such vectors η. For any $\sigma \in \mathfrak{G}$, $\sigma_1 \in \mathfrak{G}_1$ we have $\sigma^{-1}\sigma_1\sigma \in \mathfrak{G}_1$, so that, for any given vector η as above, there exists a $c \in \mathfrak{C}$ such that $\sigma^{-1}\sigma_1\sigma\eta = c\eta$, $\sigma_1\sigma\eta = c\sigma\eta$. That is, $\sigma\eta$ is a characteistic vector for every $\sigma_1 \in \mathfrak{G}_1$, whence $\sigma\eta \in \mathfrak{N}_1$, and $\mathfrak{G}\mathfrak{N}_1 = \mathfrak{N}_1$. Since $\mathfrak{G}$ is irreducible this means that $\mathfrak{N}_1 = \mathfrak{N}$, so that $\mathfrak{G}_1$ is reducible to diagonal form.

We now write $\mathfrak{N}$ as a direct sum

$$\mathfrak{N} = \mathfrak{N}' + \cdots + \mathfrak{N}^{(k)}$$

of linear subspaces $\mathfrak{N}^{(i)}$ such that:

(a) for each $\sigma_1 \in \mathfrak{G}_1$ there is a $c_i \in \mathfrak{C}$ such that $\sigma_1\zeta = c_i\zeta$ for all $\zeta \in \mathfrak{N}^{(i)}$;

(b) if $i \neq j$ there is a $\sigma_1 \in \mathfrak{G}_1$ for which $c_i \neq c_j$. For any $\sigma \in \mathfrak{G}$, $\sigma_1 \in \mathfrak{G}_1$ we have $\sigma^{-1}\sigma_1\sigma \in \mathfrak{G}_1$, so that, for each i, there is a $c_i \in \mathfrak{C}$ such that for every $\zeta \in \mathfrak{N}^{(i)}$ we have $\sigma^{-1}\sigma_1\sigma\zeta = c_i\zeta$, $\sigma_1\sigma\zeta = c_i\sigma\zeta$. This shows that all the vectors in $\sigma\mathfrak{N}^{(i)}$ are in the same $\mathfrak{N}^{(j)}$, whence $\sigma\mathfrak{N}^{(i)} = \mathfrak{N}^{(j)}$. Thus, the matrices of $\mathfrak{G}$ permute the linear subspaces $\mathfrak{N}', \cdots, \mathfrak{N}^{(k)}$ among themselves, so that there is a homomorphism of $\mathfrak{G}$ onto a group of permutations of k objects. The kernel of this homomorphism is the group $\mathfrak{H}$ consisting of all matrices in $\mathfrak{G}$ which leave each $\mathfrak{N}^{(i)}$ invariant. $\mathfrak{H}$ is clearly an algebraic subgroup of $\mathfrak{G}$ of finite index (equal to

the order of the permutation group). Since $\mathfrak{G}$ is connected, it follows from the remark at the end of §2 that $\mathfrak{G} = \mathfrak{H}$. Since $\mathfrak{G}$ is irreducible we must have $\mathfrak{R}' = \mathfrak{R}$, that is, every matrix in $\mathfrak{G}_1$ is of the form $c\iota$.

The commutator of any two matrices σ, τ in $\mathfrak{G}$ is in $\mathfrak{G}_1$, so that $\sigma\tau\sigma^{-1} = c\tau$ for some c in $\mathcal{C}$. Taking determinants we see that $c^n = 1$, so that the underlying manifold of $\mathfrak{G}$ falls apart into a finite number of algebraic submanifolds, each one characterized by a different n^{th} root of unity c in the equation $\sigma\tau\sigma^{-1} = c\tau$ for τ. Since the underlying manifold of $\mathfrak{G}$ is irreducible, and since no matrix $\tau \neq 0$ can satisfy two such equations, c can assume only one value, which must be 1. Therefore $\mathfrak{G}$ is abelian. This contradicts the assumption $h > 1$, and completes the proof of the sufficiency.

NECESSITY. It suffices to show that the full triangular group $\mathfrak{T}$ (§2 Example 5) is connected and solvable. $\mathfrak{T}$ is obviously connected, for its underlying manifold is linear. $\mathfrak{T}$ is solvable by the example of §5.

THEOREM 2. *An algebraic matric group is solvable and anticompact if and only if it is reducible to special triangular form.*

PROOF. By the example of §5 and Theorem 1 of §6, $\mathfrak{G}$ is solvable and anticompact if it is reducible to special triangular form. Conversely, let $\mathfrak{G}$ be solvable and anticompact. By Theorem 1 $\mathfrak{G}^0$ is reducible to triangular form, and by §6 Theorem 1 every matrix in $\mathfrak{G}$ has all its characteristic roots equal to 1. Now $\mathfrak{G}/\mathfrak{G}^0$ is solvable, so that there is a segment of a normal chain

$$\mathfrak{G} \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_{h-1} \supset \mathfrak{G}^0$$

in which each factor group is abelian. Therefore, to prove the theorem it suffices to prove the following

LEMMA. *If $\mathfrak{G}$ is an algebraic matric group, and $\mathfrak{N}$ is a normal algebraic subgroup such that $\mathfrak{N}$ is in special triangular form and $\mathfrak{G}/\mathfrak{N}$ is abelian, then $\mathfrak{G}$ is reducible to triangular form.*

PROOF. For degree $n = 1$ this is obvious. Let $n > 1$ and assume the lemma established for matrices of lower degree. Let $\mathfrak{N}_1$ be the linear subspace of the vector space $\mathfrak{N}$ consisting of all vectors η such that $\nu\eta = \eta$ for all $\nu \in \mathfrak{N}$. Since $\mathfrak{N} \subseteq \mathfrak{T}_1$, the dimension n_1 of $\mathfrak{N}_1$ is at least 1. If $n_1 = n$ then $\mathfrak{N} = \mathfrak{E}$, $\mathfrak{G}$ is abelian and (by §1 Lemma 1) reducible to triangular form. Suppose $n_1 < n$. For any $\sigma \in \mathfrak{G}$, $\nu \in \mathfrak{N}$ we have $\sigma^{-1}\nu\sigma \in \mathfrak{N}$, so that for any $\eta \in \mathfrak{N}_1$ we have $\sigma^{-1}\nu\sigma\eta = \eta$, $\nu\sigma\eta = \sigma\eta$. It follows that $\mathfrak{N}_1$ is invariant under every matrix in $\mathfrak{G}$ so that there is a matrix ρ for which

$$\rho^{-1}\mathfrak{G}\rho = \begin{pmatrix} \mathfrak{G}_1 & * \\ 0 & \mathfrak{G}_2 \end{pmatrix}.$$

Since $\mathfrak{N} \subseteq \mathfrak{G}$ we have, correspondigly,

$$\rho^{-1}\mathfrak{N}\rho = \begin{pmatrix} \mathfrak{N}_1 & * \\ 0 & \mathfrak{N}_2 \end{pmatrix},$$

and (by the lemma of §5) $\mathfrak{N}_i$ is a normal algebraic subgroup of the algebraic

matric group $\mathfrak{G}_i$ such that $\mathfrak{G}_i/\mathfrak{N}_i$ is abelian ($i = 1, 2$). But $\mathfrak{N}_1$ consists solely of the identity matrix, so that on the one hand $\mathfrak{G}_1$ is abelian and therefore reducible to triangular form, and on the other there is an obvious homomorphism between $\mathfrak{N}$ and $\mathfrak{N}_2$. Since $\mathfrak{N} \subseteq \mathfrak{T}_1$ we see (by Theorem 1 and §6 Theorem 1) that $\mathfrak{N}$ is solvable and anticompact. By virtue of the homomorphism and §6 Theorem 1 the same may be said of $\mathfrak{N}_2$. Consequently there is a normal chain

$$\mathfrak{G}_2 \supseteq \mathfrak{N}_2 \supset \mathfrak{N}_{21} \supset \cdots \supset \mathfrak{N}_{2u} = \mathfrak{E}$$

in which each factor group is abelian. By the induction assumption we may start with $\mathfrak{N}_{2u} = \mathfrak{E}$ and prove successively that $\mathfrak{N}_{2,u-1}, \cdots, \mathfrak{N}_{21}, \mathfrak{N}_2, \mathfrak{G}_2$ are reducible to triangular form. Since $\mathfrak{G}_1$ and $\mathfrak{G}_2$ are both reducible to triangular form, so is $\mathfrak{G}$.

THEOREM 3. *If a quasicompact algebraic matric group is reducible to triangular form then it is reducible to diagonal form.*

PROOF. Let $\mathfrak{G}$ be quasicompact, and assume, without loss of generality, that $\mathfrak{G}$ is already in triangular form: $\mathfrak{G} \subseteq \mathfrak{T}$. Since $\mathfrak{G}$ is quasicompact it contains no anticompact algebraic subgroup of order > 1. Therefore $\mathfrak{G} \cap \mathfrak{T}_1$ (which by §6 Theorem 1 is anticompact) must be $\mathfrak{E}$. But $\mathfrak{G} = \mathfrak{G}/\mathfrak{E} = \mathfrak{G}/\mathfrak{G} \cap \mathfrak{T}_1$ is isomorphic with $\mathfrak{G}\mathfrak{T}_1/\mathfrak{T}_1 \subseteq \mathfrak{T}/\mathfrak{T}_1$.[7] By the example of §5, $\mathfrak{T}/\mathfrak{T}_1$ is abelian; hence $\mathfrak{G}$ is abelian, too. By §1, Lemma 1, $\mathfrak{G}$ is therefore equivalent to a group $\mathfrak{N}$ of the form (1), where for each i the $\mathfrak{N}_i$-block of every matrix in $\mathfrak{N}$ is in triangular form with equal elements on the main diagonal. Since every matrix in $\mathfrak{G}$ is reducible to diagonal form (§6 Theorem 2), the same is true of the $\mathfrak{N}_i$-block of every matrix in $\mathfrak{N}$ (see the remark on complete reducibility made in §1); and since all the elements on the main diagonal of the $\mathfrak{N}_i$-block are equal, the $\mathfrak{N}_i$-block is already in diagonal form. This holds for every i, so that $\mathfrak{N}$ is in diagonal form.

8. Algebraic matric groups with certain types of normal chains

An algebraic matric group is solvable if it has a normal chain in which each factor group is abelian. We now investigate groups which contain normal chains with certain other types of factor groups.

THEOREM 1. *If an algebraic matric group $\mathfrak{G}$ has a normal chain*

$$\mathfrak{G} = \mathfrak{G}_0 \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_r = \mathfrak{E} \tag{7}$$

in which each factor group is either abelian or finite, then $\mathfrak{G}^0$ is solvable.

PROOF. For any algebraic subgroup $\mathfrak{H}$ of $\mathfrak{G}$, $\mathfrak{H} \cap \mathfrak{G}_{i-1}/\mathfrak{H} \cap \mathfrak{G}_i$ is isomorphic with a subgroup of $\mathfrak{G}_{i-1}/\mathfrak{G}_i$. Therefore every algebraic subgroup $\mathfrak{H} \neq \mathfrak{E}$ has a normal chain of positive length with the same properties as (7). Now consider the sequence of commutator groups for $\mathfrak{G}^0$: $\mathfrak{G}^0$, $\mathfrak{G}^{0\prime}$, $\cdots$, $\mathfrak{G}^{0(j)}$, $\cdots$. By §4 this sequence terminates with some $\mathfrak{G}^{0(j)}$. This $\mathfrak{G}^{0(j)}$ contains no normal

[7] VAN DER WAERDEN [1] vol. 1, p. 148, or ZASSENHAUS [1] p. 32.

algebraic proper subgroup with abelian factor group. Also, by the lemma of §3, this $\mathfrak{G}^{0(j)}$ is connected, and therefore, by the final remark of §2, contains no algebraic proper subgroup of finite index. Consequently $\mathfrak{G}^{0(j)}$ does not have a normal chain of positive length like (7), so that $\mathfrak{G}^{0(j)} = \mathfrak{E}$. This means that the sequence of commutator groups of $\mathfrak{G}^0$ terminates with $\mathfrak{E}$, whence $\mathfrak{G}^0$ is solvable.

We now extend the concepts of "anticompact" and "quasicompact" to factor groups, in the following natural manner. Let $\mathfrak{G}$ be an algebraic matric group, $\mathfrak{N}$ a normal algebraic subgroup thereof. The factor group $\mathfrak{G}/\mathfrak{N}$ is anticompact if it contains no element, other than the identity, of finite order not divisible by p; $\mathfrak{G}/\mathfrak{N}$ is quasicompact if there is no algebraic group $\mathfrak{H}$, with $\mathfrak{N} \subset \mathfrak{H} \subseteq \mathfrak{G}$, such that $\mathfrak{H}/\mathfrak{N}$ is anticompact.

THEOREM 2. *If an algebraic matric group $\mathfrak{G}$ has a normal chain* (7) *in which each factor group is either anticompact or finite, then $\mathfrak{G}^0$ is anticompact. If all the factor groups are anticompact then $\mathfrak{G}$ is anticompact.*

PROOF. Every algebraic subgroup $\mathfrak{H} \neq \mathfrak{E}$ of $\mathfrak{G}$ has a normal chain of positive length with the same properties as (7). In particular, if $\mathfrak{G}^0 \neq \mathfrak{E}$ then $\mathfrak{G}^0$ has such a normal chain:

$$\mathfrak{G}^0 \supset \mathfrak{H}_1 \supset \cdots \supset \mathfrak{H}_s = \mathfrak{E}.$$

Since $\mathfrak{G}^0$ is connected, $\mathfrak{G}^0/\mathfrak{H}_1$ is not finite, so that $\mathfrak{G}^0/\mathfrak{H}_1$ is anticompact and $\dim \mathfrak{G}^0 > \dim \mathfrak{H}_1$. We now use induction on $\dim \mathfrak{G}^0$. If $\dim \mathfrak{G}^0 = 0$ (that is, if $\mathfrak{G}^0 = \mathfrak{E}$) then $\mathfrak{G}^0$ is anticompact. Let $\dim \mathfrak{G}^0 > 0$ and suppose the theorem established for groups of lower dimension. Then $\mathfrak{H}_1^0$ is anticompact, and, by §6 Theorem 1, all the charateristic roots of each matrix in $\mathfrak{H}_1^0$ are 1. If $\mathfrak{G}^0$ contains a matrix σ of finite order j not divisible by p then $\sigma \in \mathfrak{H}_1$, for otherwise $\mathfrak{G}^0/\mathfrak{H}_1$ would not be anticompact. On the other hand $\sigma \notin \mathfrak{H}_1^0$, for $\mathfrak{H}_1^0$ is anticompact. Therefore j divides the order of $\mathfrak{H}_1/\mathfrak{H}_1^0$. If this order is u then it follows from §6 Theorem 1 that all the characteristic roots of each matrix in $\mathfrak{G}^0$ are u^{th} roots of unity. But $\mathfrak{G}^0$ is connected, so it easily follows that all these u^{th} roots of unity are actually 1. Therefore, by §6 Theorem 1, $\mathfrak{G}^0$ is anticompact.

If all the factor groups are anticompact and σ is any element of $\mathfrak{G}$ other than ι, consider the $\mathfrak{G}_j$ of highest subscript such that $\sigma \in \mathfrak{G}_j$. Since $\mathfrak{G}_j/\mathfrak{G}_{j+1}$ is anticompact, no finite power σ^k with k not divisible by p is contained in $\mathfrak{G}_{j+1}$, so that no $\sigma^k = \iota$. Thus $\mathfrak{G}$ is anticompact.

THEOREM 3. *If an algebraic matric group $\mathfrak{G}$ has a normal chain* (7) *in which each factor group is quasicompact, then $\mathfrak{G}$ is quasicompact.*[8]

PROOF. Let $\mathfrak{H} \neq \mathfrak{E}$ be any algebraic subgroup of $\mathfrak{G}$, and consider the $\mathfrak{G}_j$ of highest subscript such that $\mathfrak{G}_j \cap \mathfrak{H} \neq \mathfrak{E}$. Since $\mathfrak{G}_j/\mathfrak{G}_{j+1}$ is quasicompact,

[8] It would be of interest to know whether or not the following is true: *If each factor group is either quasicompact or finite then $\mathfrak{G}^0$ is quasicompact.* When $p = 0$ this is implied by Theorem 3, for then every finite group is quasicompact. But when $p \neq 0$ there are finite groups (groups of order divisible by p) which are not quasicompact.

$\mathfrak{G}_j \cap \mathfrak{H}$ contains a matrix $\sigma \neq \iota$ such that $\sigma^k \in \mathfrak{G}_{j+1}$ for some positive k not divisible by p. But $\mathfrak{G}_{j+1} \cap \mathfrak{H} = \mathfrak{E}$, so that $\sigma^k = \iota$, $\mathfrak{H}$ contains an element other than ι of finite order not divisible by p, and $\mathfrak{G}$ is quasicompact.

CHAPTER II. SOME RESULTS FROM THE THEORY OF ALGEBRAIC DIFFERENTIAL EQUATIONS

9. Differential rings, fields, and ideals

Let m be a positive integer. A *differential ring with m types of differentiation* is a (commutative) ring together with m operators $\delta_1, \cdots, \delta_m$ (called *derivatives*) such that:

(a) $\delta_i a$ is defined and is an element of the ring for every element a in the ring, $i = 1, \cdots, m$;

(b) $\delta_i \delta_j = \delta_j \delta_i$, $i, j = 1, \cdots, m$;

(c) $\delta_i(a + b) = \delta_i a + \delta_i b$ for all a, b in the ring, $i = 1, \cdots, m$;

(d) $\delta_i(ab) = \delta_i a \cdot b + a \cdot \delta_i b$ for all a, b in the ring, $i = 1, \cdots, m$.

A *differential field* is defined similarly. A differential ring or field is *ordinary* or *partial* according as $m = 1$ or $m > 1$. In the ordinary case we shall write a' for $\delta_1 a$.

If $\mathfrak{R}_1$ and $\mathfrak{R}_2$ are two differential rings with m types of differentiation, $\mathfrak{R}_1$ is a *differential subring* of $\mathfrak{R}_2$, and $\mathfrak{R}_2$ is a *differential extension ring* of $\mathfrak{R}_1$, provided $\mathfrak{R}_1$ is a subring of $\mathfrak{R}_2$ and $\delta_i a$ for $\mathfrak{R}_2$ coincides with $\delta_i a$ for $\mathfrak{R}_1$ whenever $a \in \mathfrak{R}_1$ $(i = 1, \cdots, m)$. *Differential subfields* and *differential extension fields* are defined similarly.

Let $\mathfrak{R}_1$ be a differential subring of the differential ring $\mathfrak{R}_2$ and consider a subset Φ of $\mathfrak{R}_2$. The set of all polynomials with coefficients in $\mathfrak{R}_1$ in a finite number of elements of the form $\delta_1^{i_1} \cdots \delta_m^{i_m} a$ ($a \in \Phi$; each i_ν a nonnegative integer), forms a differential extension ring of $\mathfrak{R}_1$, denoted by $\mathfrak{R}_1\{\Phi\}$. If Φ is a finite set $a_1, \cdots, a_n$ then we write $\mathfrak{R}_1\{a_1, \cdots, a_n\}$.

Let $\mathfrak{F}_1$ be a differential subfield of the differential field $\mathfrak{F}_2$ and consider a subset Φ of $\mathfrak{F}_2$. The set of all rational functions, in a finite number of elements of the form $\delta_1^{i_1} \cdots \delta_m^{i_m} a$ ($a \in \Phi$; each i_ν a nonnegative integer), with coefficients in $\mathfrak{F}_1$ and with nonvanishing denominator, forms a differential extension field of $\mathfrak{F}_1$ denoted by $\mathfrak{F}_1\langle\Phi\rangle$ (in the finite case: $\mathfrak{F}_1 < a_1, \cdots, a_n >$).

An element c of a differential ring or field with m types of differentiation is a *constant* if $\delta_i c = 0$, $i = 1, \cdots, m$. The set of all constants is a differential subring or subfield, respectively, of the original differential ring or field, and is called the *ring* or *field of constants* thereof.

Let $\mathfrak{R}$ be a differential ring. A *differential ideal* in $\mathfrak{R}$ is a subset of $\mathfrak{R}$ which is an ideal in $\mathfrak{R}$ when $\mathfrak{R}$ is considered as a ring, and which is closed with respect to differentiation. A differential ideal is *perfect* if it contains an element of $\mathfrak{R}$ whenever it contains some power of the element. A differential ideal is *prime* if, whenever it contains the product of two elements in $\mathfrak{R}$, it contains one of those elements. Clearly, a prime differential ideal is perfect.

If Φ is a subset of $\mathfrak{R}$, the intersection of all differential ideals containing Φ

is itself a differential ideal, the differential ideal generated by Φ, denoted by $[\Phi]$. If $\mathcal{R}$ contains a unit element then $[\Phi]$ consists of all linear combinations, with coefficients in $\mathcal{R}$, of a finite number of elements of the form $\delta_1^{i_1} \cdots \delta_m^{i_m} a$ ($a \in \Phi$; each i_ν a nonnegative integer). The intersection of all perfect differential ideals containing Φ is itself a perfect differential ideal, the perfect differential ideal generated by Φ, denoted by $\{\Phi\}$. If $\mathcal{R}$ contains all the rational numbers, then $\{\Phi\}$ consists of all elements a in R for which there is a positive integer k such that $a^k \in [\Phi]$.[9]

10. Differential polynomials

Let $\mathcal{F}$ be a differential field of characteristic 0, and introduce a symbol y, called an *unknown* (unknowns play the same rôle in the theory of differential fields as indeterminates do in the theory of fields). A *differential polynomial* in y with coefficients in $\mathcal{F}$, is a polynomial, with coefficients in $\mathcal{F}$, in a finite number of the new symbols $\delta_1^{i_1} \cdots \delta_m^{i_m} y$ ($i_1, \cdots, i_m$ nonnegative integers). When the derivatives of differential polynomials are defined in the obvious way, the set of all differential polynomials in y with coefficients in $\mathcal{F}$ becomes a differential ring, denoted by $\mathcal{F}\{y\}$. Similarly, it is possible to introduce any finite number n of unknowns $y_1, \cdots, y_n$ and to form the differential ring $\mathcal{F}\{y_1, \cdots, y_n\}$ of differential polynomials in $y_1, \cdots, y_n$ with coefficients in $\mathcal{F}$.

THEOREM. *If Σ is a perfect differential ideal in $\mathcal{F}\{y_1, \cdots, y_n\}$, then there exist a finite number of prime differential ideals $\Pi_1, \cdots, \Pi_r$ in $\mathcal{F}\{y_1, \cdots, y_n\}$ such that*

$$\Sigma = \Pi_1 \cap \cdots \cap \Pi_r, \qquad \Pi_i \not\subseteq \Pi_j \text{ for } i \neq j.$$

The set $\Pi_1, \cdots, \Pi_r$ is unique.[10]

We shall call the prime differential ideals $\Pi_1, \cdots, \Pi_r$ the *prime components of Σ*.

11. Solutions

Let $\mathcal{F}$ be a differential field of characteristic 0, and let $y_1, \cdots, y_n$ be unknowns. If Φ is a set of differential polynomials in $\mathcal{F}\{y_1, \cdots, y_n\}$, a *solution* of Φ is an ordered set of n elements $\eta_1, \cdots, \eta_n$ of a differential extension field of $\mathcal{F}$ such that every member of Φ becomes 0 when each $\delta_1^{i_1} \cdots \delta_m^{i_m} y_j$ is replaced by the corresponding $\delta_1^{i_1} \cdots \delta_m^{i_m} \eta_j$. Clearly the solutions of Φ are identical with those of $\{\Phi\}$.

A solution of Φ is a *generic solution* of Φ if it is a solution of no differential polynomial in $\mathcal{F}\{y_1, \cdots, y_n\}$ other than those in Φ. Φ has a generic solution if and only if Φ is a prime differential ideal $\subset \mathcal{F}\{y_1, \cdots, y_n\}$. If $\eta_1, \cdots, \eta_n$

[9] For proof in the ordinary case see RAUDENBUSH [1], p. 363.

[10] This theorem, first proved by Ritt for differential fields of meromorphic functions, is an easy consequence of the Ritt-Raudenbush basis theorem. See RAUDENBUSH [1] where the basis theorem and the present theorem are proved in the ordinary case for abstract differential fields. Since the abstract basis theorem also holds in the partial case (see KOLCHIN [2]), the same is true of the present theorem.

is a generic solution and $\bar{\eta}_1, \cdots, \bar{\eta}_n$ a solution of the same prime differential ideal, then the substitution $\eta_1 \to \bar{\eta}_1, \cdots, \eta_n \to \bar{\eta}_n$ generates a homomorphism[11] of $\mathcal{F}\{\eta_1, \cdots, \eta_n\}$ onto $\mathcal{F}\{\bar{\eta}_1, \cdots, \bar{\eta}_n\}$.

THEOREM. *Let* $F \in \mathcal{F}\{y_1, \cdots, y_n\}$, $\Phi \subseteq \mathcal{F}\{y_1, \cdots, y_n\}$. *If every solution of* Φ *is a solution of* F, *then* $\mathcal{F} \in \{\Phi\}$.[12]

12. Relative isomorphisms

Let $\mathcal{F}$ be a differential field of characteristic 0, $\mathcal{G}$ a differential extension field of $\mathcal{F}$. An *isomorphism of* $\mathcal{G}$ *with respect to* or *over* $\mathcal{F}$ is an isomorphism[13] of $\mathcal{G}$ onto a differential field $\mathcal{G}'$ such that:

(a) $\mathcal{G}'$ is a differential extension field of $\mathcal{F}$;

(b) $\mathcal{G}$ and $\mathcal{G}'$ have a common differential extension field;

(c) the isomorphism leaves each element of $\mathcal{F}$ invariant. An isomorphism σ of $\mathcal{G}$ over $\mathcal{F}$ can be extended to an isomorphism over $\mathcal{F}$ of any common differential extension field of $\mathcal{G}$ and $\sigma\mathcal{G}$.[14]

THEOREM. *Let* $\gamma \in \mathcal{G}$. *A necessary and sufficient condition that* $\gamma \in \mathcal{F}$ *is that every isomorphism of* $\mathcal{G}$ *over* $\mathcal{F}$ *leave* γ *invariant.*[15]

13. Order

Let $\mathcal{F}$ be an ordinary differential field of characteristic 0. If $\eta_1, \cdots, \eta_n$ are elements of a differential extension field, then we may think of $\mathcal{F}$ and $\mathcal{F} < \eta_1, \cdots, \eta_n >$ as fields (not differential fields), and consider the degree of transcendency $\partial^0\mathcal{F} < \eta_1, \cdots, \eta_n > / \mathcal{F}$. We shall call this number the *order of* $\eta_1, \cdots, \eta_n$ over $\mathcal{F}$. When each η_i is a solution of a nonzero differential polynomial in $\mathcal{F}\{y\}$ then the order of $\eta_1, \cdots, \eta_n$ over $\mathcal{F}$ is finite.

The *order* of a prime differential ideal Π in $\mathcal{F}\{y_1, \cdots, y_n\}$ is defined as the order over $\mathcal{F}$ of a generic solution $\eta_1, \cdots, \eta_n$ of Π, and will be denoted by ord Π. If, for each i, Π contains a nonzero differential polynomial in y_i alone, then ord Π is finite.

THEOREM 1. *If* Π *is a prime differential ideal in* $\mathcal{F}\{y_1, \cdots, y_n\}$ *of finite order,*

---

[11] That is, a single valued mapping which preserves addition, multiplication, and the m types of differentiation.

[12] This analog of the Hilbert-Netto *Nullstellensatz* is due to Ritt ([1] ch. 7) who proved it for the case in which the elements of $\mathcal{F}$ are meromorphic functions of a complex variable. A simple proof for abstract ordinary differential fields of characteristic 0 appears in RAUDENBUSH [1]. Raudenbush's proof is obviously applicable in the partial case, too.

[13] That is, a one-to-one mapping which preserves addition, multiplication, and the m types of differentiation.

[14] See KOLCHIN [3], where this is incorrectly stated. To correct the error there: on p. 726 15th line from the bottom for "automorphism of the" read "isomorphism of any"; on p. 726 1st line from the bottom for "automorphism" read "isomorphism"; on p. 727 1st line for "automorphism" read "isomorphism."

[15] For proof see KOLCHIN [3].

and if $\eta_1, \cdots, \eta_n$ *is a solution of* Π *with order equal to* ord Π, *then* $\eta_1, \cdots, \eta_n$ *is a generic solution of* Π.[16]

THEOREM 2. *Let* $\mathcal{G}$ *be a differential extension field of* $\mathcal{F}$. *If* Π *is a prime differential ideal in* $\mathcal{F}\{y_1, \cdots, y_n\}$ *and if, in* $\mathcal{G}\{y_1, \cdots, y_n\}$, Π_1 *is a prime component of* $\{\Pi\}$, *then* ord Π_1 = ord Π.[17]

14. Dependence

Let $\mathcal{F}$ be an ordinary[18] differential field, and denote the field of constants of $\mathcal{F}$ by $\mathcal{C}$.

THEOREM 1. *A finite set of elements* $\eta_1, \cdots, \eta_n$ *in* $\mathcal{F}$ *is linearly dependent over* $\mathcal{C}$ *if and only if the wronskian determinant*

$$W(\eta_1, \cdots, \eta_n) = \begin{vmatrix} \eta_1 & \cdots & \eta_n \\ \eta_1' & \cdots & \eta_n' \\ \cdot & \cdots & \cdot \\ \eta_1^{(n-1)} & \cdots & \eta_n^{(n-1)} \end{vmatrix}$$

vanishes.[19]

Since the form of $W(\eta_1, \cdots, \eta_n)$ is independent of $\mathcal{F}$ the vanishing of $W(\eta_1, \cdots, \eta_n)$ is a necessary and sufficient condition for the linear dependence of $\eta_1, \cdots, \eta_n$ over the field of constants of *any* differential field containing $\eta_1, \cdots, \eta_n$, so that we may speak simply of linear dependence (or independence) over constants.

THEOREM 2. *Let* $\mathfrak{m}'$ *be a set of polynomials in* $\mathcal{F}[x_1, \cdots, x_n]$. *Then there is a set* $\mathfrak{m}$ *of polynomials in* $\mathcal{C}[x_1, \cdots, x_n]$ *such that n constants in a differential extension field of* $\mathcal{F}$ *form a zero of* $\mathfrak{m}'$ *if and only if they form a zero of* $\mathfrak{m}$. *In particular, if* $\gamma_1, \cdots, \gamma_n$ *are constants in a differential extension field of* $\mathcal{F}$, *then* $\partial^0\mathcal{F}(\gamma_1, \cdots, \gamma_n)/\mathcal{F} = \partial^0\mathcal{C}(\gamma_1, \cdots, \gamma_n)/\mathcal{C}$.

PROOF. By the Hilbert basis theorem $\mathfrak{m}'$ may be replaced by a finite subset $\mathfrak{m}''$. Of the coefficients appearing in the various polynomials of $\mathfrak{m}''$, let $\alpha_1, \cdots, \alpha_h$ be a maximal set that is linearly independent over $\mathcal{C}$ (and therefore over any set of constants). Then every P in $\mathfrak{m}''$ can be written in the form $P = Q_1\alpha_1 + \cdots + Q_h\alpha_a$, where each $Q_i \in \mathcal{C}[x_1, \cdots, x_n]$. By the linear independence

[16] In case $\mathcal{F}$ contains nonconstants this is a special case of a theorem due to Gourin [1]. The case in which $\mathcal{F}$ consists solely of constants can, as indicated by Gourin, be reverted to the former case by the differential field adjunction of an unknown to $\mathcal{F}$. Gourin's proof made use of Ritt's concept of resolvent, which at the time had been developed only for differential fields of meromorphic functions of a complex variable (see RITT [1] ch. 2). Subsequently, Ritt's results have been obtained for abstract differential fields of characteristic 0 (see KOLCHIN [4], or [1] p. 776), so that Gourin's theorem may be regarded as proved in the abstract case.

[17] This is part of a result due to RITT [1], §75. Ritt's proof is function-theoretic. For an abstract proof see KOLCHIN [4].

[18] The results of this section can be extended to partial differential fields, but as this is not necessary for the purposes of the present paper, we avoid the longer discussion this would require.

[19] The proof in the abstract case is straightforward; e.g., see KOLCHIN [1].

of $\alpha_1, \cdots, \alpha_h$ we see that n constants form a zero of P if and only if they do so for $Q_1, \cdots, Q_h$. The theorem now quickly follows.

15. Homogeneous linear ordinary differential equations

Let $\mathcal{F}$ be an ordinary differential field of characteristic 0 with field of constants $\mathcal{C}$, let y be an unknown, n a positive integer, $p_1, \cdots, p_n \in \mathcal{F}$, and consider the homogeneous linear differential polynomial

$$L(y) = y^{(n)} + p_1 y^{(n-1)} + \cdots + p_n y_n .$$

THEOREM. *There exists a differential extension field of $\mathcal{F}$ which contains n solutions of $L(y)$ which are linearly independent over constants.*[20] *No such extension of $\mathcal{F}$ contains more than n solutions of $L(y)$ linearly independent over constants.*

PROOF. Let $y_1, \cdots, y_n$ be new unknowns. Since the order of the wronskian determinant $W(y_1, \cdots, y_n)$ is $< n$ it is easy to see that $W(y_1, \cdots, y_n) \notin \{L(y_1), \cdots, L(y_n)\}$. By the theorem of §11 there therefore exists a solution $\eta_1, \cdots, \eta_n$ of $\{L(y_1), \cdots, L(y_n)\}$ for which $W(\eta_1, \cdots, \eta_n) \neq 0$. By §14 Theorem 1, $\eta_1, \cdots, \eta_n$ are solutions of $L(y)$, linearly independent over constants. Now suppose we have $n + 1$ solutions $\eta_1, \cdots, \eta_{n+1}$ of $L(y)$. Then $L(\eta_i) = 0$ $(i = 1, \cdots, n + 1)$ is a system of $n + 1$ homogeneous linear equations in the $n + 1$ quantities $1, p_1, \cdots, p_n$. Since not all these quantities are 0, the determinant of the system vanishes. But the determinant is the wronskian $W(\eta_1, \cdots, \eta_{n+1})$, so that $\eta_1, \cdots, \eta_{n+1}$ are linearly dependent over constants.

A set of n linearly independent solutions as above is a *fundamental system of solutions of $L(y)$*.

CHAPTER III. NORMAL DIFFERENTIAL EXTENSION FIELDS

16. Normal differential extension fields

Let $\mathcal{F}$ be a differential subfield of a differential field $\mathcal{G}$ of characteristic 0. Denote by $\mathbf{F}$ the set of all differential subfields of $\mathcal{G}$ which contain $\mathcal{F}$.

A set of isomorphisms of $\mathcal{G}$ over $\mathcal{F}$ will be called *abundant* if, for each $\mathcal{F}_1 \in \mathbf{F}$ and each $\alpha \in \mathcal{G} - \mathcal{F}_1$, there is an isomorphism in the set which leaves invariant each element of $\mathcal{F}_1$ but which does not leave α invariant. It follows from Chapter II §12 that an abundant set of such isomorphisms always exists.

$\mathcal{G}$ will be called a *normal* extension of $\mathcal{F}$ if the set of all *auto*morphisms of $\mathcal{G}$ over $\mathcal{F}$ is abundant. E.g., if $\mathcal{G}$ is a finite algebraic extension of $\mathcal{F}$ and if $\mathcal{G}$ is normal in the sense of Galois theory, then $\mathcal{G}$ is normal in the sense just defined. In general, if $\mathcal{G}$ is a normal extension of $\mathcal{F}$ then obviously $\mathcal{G}$ is a normal extension of any $\mathcal{F}_1 \in \mathbf{F}$.

We define the product $\sigma\tau$ of two automorphisms σ, τ as the automorphism obtained by first operating with τ and then with σ. Then the set of all auto-

[20] As remarked by BAER [1], it would be of interest to know whether there exist n such solutions $\eta_1, \ldots, \eta_n$ such that $\mathcal{F}\langle\eta_1, \ldots, \eta_n\rangle$ contains no constant transcendental over $\mathcal{C}$.

morphisms of $\mathfrak{G}$ over $\mathfrak{F}$ is a group. In the above mentioned case in which $\mathfrak{G}$ is a normal finite algebraic extension of $\mathfrak{F}$, this group coincides with the Galois group of $\mathfrak{G}$ over $\mathfrak{F}$.

Let $\mathfrak{G}$ be a normal extension of $\mathfrak{F}$ and let $\mathfrak{H}$ be an abundant group of automorphisms of $\mathfrak{G}$ over $\mathfrak{F}$ (not necessarily the group of all such automorphisms). For each $\mathfrak{F}_1 \in \mathbf{F}$ let $\mathfrak{H}(\mathfrak{F}_1)$ be the subgroup of $\mathfrak{H}$ consisting of all automorphisms which leave invariant every element of $\mathfrak{F}_1$. In particular, $\mathfrak{H}(\mathfrak{F}) = \mathfrak{H}$, $\mathfrak{H}(\mathfrak{G}) = \mathfrak{E}$ (the group consisting solely of the identity automorphism ι).

Let $\mathbf{G}$ denote the set of all subgroups of $\mathfrak{H}$ of the form $\mathfrak{H}(\mathfrak{F}_1)$, where $\mathfrak{F}_1 \in \mathbf{F}$.

THEOREM 1. *For any $\mathfrak{F}_1$ in $\mathbf{F}$ the set of all elements in $\mathfrak{G}$ invariant under every automorphism in $\mathfrak{H}(\mathfrak{F}_1)$ is $\mathfrak{F}_1$. Therefore the correspondence $\mathfrak{F}_1 \to \mathfrak{H}(\mathfrak{F}_1)$ is a one-to-one mapping of $\mathbf{F}$ onto $\mathbf{G}$.*

PROOF. $\mathfrak{F}_1$ is clearly contained in the set mentioned in the theorem. To show that this set has no other elements consider any $\alpha \in \mathfrak{G} - \mathfrak{F}_1$. Since $\mathfrak{G}$ is a normal extension of $\mathfrak{F}$, there exists a $\sigma \in \mathfrak{H}$ which leaves invariant each element of $\mathfrak{F}_1$ (so that $\sigma \in \mathfrak{H}(\mathfrak{F}_1)$, but which does not leave α invariant. Therefore α is not contained in the set in question, and the theorem follows.

It is easy to see that for any set of differential fields $\mathfrak{F}_\lambda$ in $\mathbf{F}$ we have

$$\mathfrak{H}(\mathfrak{F}\langle \bigcup \mathfrak{F}_\lambda \rangle) = \bigcap \mathfrak{H}(\mathfrak{F}_\lambda),$$

$$\mathfrak{H}(\bigcap \mathfrak{F}_\lambda) = \text{smallest group in } \mathbf{G} \text{ containing } \bigcup \mathfrak{H}(\mathfrak{F}_\lambda).$$

THEOREM 2. *Let $\mathfrak{F}_1 \in \mathbf{F}$. A necessary and sufficient condition that $\mathfrak{H}(\mathfrak{F}_1)$ be a normal subgroup of $\mathfrak{H}$ is that $\sigma\mathfrak{F}_1 = \mathfrak{F}_1$ for every σ in $\mathfrak{H}$. When this condition is fulfilled the factor group $\mathfrak{H}/\mathfrak{H}(\mathfrak{F}_1)$ is isomorphic with an abundant group of automorphisms of $\mathfrak{F}_1$ over $\mathfrak{F}$ (in particular, $\mathfrak{F}_1$ is a normal extension of $\mathfrak{F}$).*

PROOF. If $\sigma\mathfrak{F}_1 = \mathfrak{F}_1$ for every $\sigma \in \mathfrak{H}$ then, for each $\tau \in \mathfrak{H}(\mathfrak{F}_1)$, $\sigma^{-1}\tau\sigma$ leaves each element of $\mathfrak{F}_1$ invariant; that is, $\sigma^{-1}\tau\sigma \in \mathfrak{H}(\mathfrak{F}_1)$, and $\mathfrak{H}(\mathfrak{F}_1)$ is a normal subgroup of $\mathfrak{H}$.

Conversely, let $\mathfrak{H}(\mathfrak{F}_1)$ be a normal subgroup of $\mathfrak{H}$. Then, for all $\sigma \in \mathfrak{H}$ and $\tau \in \mathfrak{H}(\mathfrak{F}_1)$ we have $\sigma^{-1}\tau\sigma \in \mathfrak{H}(\mathfrak{F}_1)$, so that $\tau\sigma\alpha = \sigma\alpha$ for all $\alpha \in \mathfrak{F}_1$. Thus $\sigma\alpha$ is invariant under every $\tau \in \mathfrak{H}(\mathfrak{F}_1)$ and is, by Theorem 1, in $\mathfrak{F}_1$. It follows that $\sigma\mathfrak{F}_1 = \mathfrak{F}_1$. This implies that every $\sigma \in \mathfrak{H}$ induces an automorphism of $\mathfrak{F}_1$ over $\mathfrak{F}$ (the contraction of σ to the domain $\mathfrak{F}_1$). Two elements σ, σ_1 of $\mathfrak{H}$ induce the same automorphism of $\mathfrak{F}_1$ if and only if $\sigma^{-1}\sigma_1 \in \mathfrak{H}(\mathfrak{F}_1)$, that is, if and only if they are in the same coset of $\mathfrak{H}(\mathfrak{F}_1)$ in $\mathfrak{H}$. For any differential field $\mathfrak{F}_2$ between $\mathfrak{F}$ and $\mathfrak{F}_1$, and any $\alpha \in \mathfrak{F}_1 - \mathfrak{F}_2$, there is (since $\mathfrak{G}$ is a normal extension of $\mathfrak{F}$) a σ in $\mathfrak{H}$ which leaves invariant every element of $\mathfrak{F}_2$ but which does not leave α invariant. The automorphism of $\mathfrak{F}_1$ induced by σ has the same properties. Therefore the set of all automorphisms of $\mathfrak{F}_1$ over $\mathfrak{F}$ induced by elements of $\mathfrak{H}$ is an abundant group, isomorphic with $\mathfrak{H}/\mathfrak{H}(\mathfrak{F}_1)$.

REMARK 1. Theorem 2 does not assert that the normality of $\mathfrak{F}_1$ over $\mathfrak{F}$ implies the normality of $\mathfrak{H}(\mathfrak{F}_1)$ in $\mathfrak{H}$. Nor does it assert, in the case in which $\mathfrak{H}$ is the group of *all* automorphisms of $\mathfrak{G}$ over $\mathfrak{F}$, that $\mathfrak{H}/\mathfrak{H}(\mathfrak{F}_1)$ is isomorphic

with the group of all automorphisms of $\mathcal{F}_1$ over $\mathcal{F}$, but merely with an abundant subgroup thereof.[21]

REMARK 2. If $\mathcal{F}_1$ is a normal *algebraic* extension of F of *finite* degree, then $\mathcal{F}_1$ contains with any element α all the roots of the defining equation of α over $\mathcal{F}$, so that $\sigma\alpha \in \mathcal{F}_1$ for all α in $\mathcal{F}_1$ and every σ in $\mathfrak{G}$. Therefore $\sigma\mathcal{F}_1 = \mathcal{F}_1$ and $\mathfrak{G}(\mathcal{F}_1)$ is a normal subgroup of $\mathfrak{G}$. Furthermore, $\mathfrak{G}/\mathfrak{G}(\mathcal{F}_1)$ is isomorphic with the group of all automorphisms of $\mathcal{F}_1$ over $\mathcal{F}$, that is, with the Galois group of $\mathcal{F}_1$ over $\mathcal{F}$; for a Galois group can contain no abundant proper subgroup.

REMARK 3. A non-trivial characterization of **G** remains an open problem. If $\mathcal{G}$ is a normal infinite algebraic extension then the group $\mathfrak{G}$ of all automorphisms of $\mathcal{G}$ over $\mathcal{F}$ is the Galois group of $\mathcal{G}$ over $\mathcal{F}$ (for the Galois theory of infinite algebraic extensions see Krull [1]), and **G** is the set of all subgroups of $\mathfrak{G}$ which are closed in a certain natural topology (see Krull [1]). A subgroup of $\mathfrak{G}$ is abundant it if is everywhere dense in $\mathfrak{G}$ in the abovementioned topology. When $\mathfrak{G}$ is not the whole group of automorphisms, but merely an abundant group, then **G** is the set of all subgroups of $\mathfrak{G}$ closed in $\mathfrak{G}$.

CHAPTER IV. PICARD-VESSIOT EXTENSIONS

17. Picard-Vessiot extensions and their isomorphisms

Throughout this chapter $\mathcal{F}$ is an ordinary differential field of characteristic 0. The field of constants of $\mathcal{F}$, denoted by $\mathcal{C}$, is assumed to be algebraically closed. The letters $y, y_1, \cdots, y_n$ are used for unknowns.

A differential extension field $\mathcal{G}$ of $\mathcal{F}$ will be called a *Picard-Vessiot extension* of $\mathcal{F}$ if:

(a) there exists a homogeneous linear ordinary differential polynomial

$$L(y) = y^{(n)} + p_1 y^{(n-1)} + \cdots + p_n y \quad (n \geqq 1, \text{each } p_i \in \mathcal{F})$$

with a fundamental system of solutions $\eta_1, \cdots, \eta_n$ such that

$$\mathcal{F} < \eta_1, \cdots, \eta_n > = \mathcal{G};$$

(b) the field of constants of $\mathcal{G}$ is $\mathcal{C}$.

We consider a Picard-Vessiot extension $\mathcal{G} = \mathcal{F}<\eta_1, \cdots, \eta_n>$ as above, and investigate the nature of the isomorphisms of $\mathcal{G}$ over $\mathcal{F}$. To do this, let Γ be the prime differential ideal in $\mathcal{F}\{y_1, \cdots, y_n\}$ consising of all differential polynomials which vanish for $y_1 = \eta_1, \cdots, y_n = \eta_n$ (so that $\eta_1, \cdots, \eta_n$ is a generic solution of Γ).

If κ_{ij} $(i, j = 1, \cdots, n)$ are n^2 indeterminate constants then the substitution

$$y_j \to \sum_{i=1}^{n} \kappa_{ij}\eta_i \qquad (j = 1, \cdots, n)$$

[21] Whether such assertions are possible is an open question. In the following chapter it will be shown that, for a special type of differential field extension, the second assertion may be made.

defines a mapping of $\mathcal{G}\{y_1, \cdots, y_n\}$ into $\mathcal{G}[\cdots, \kappa_{ij}, \cdots]$. Let $\mathfrak{g}'$ be the image of Γ under this mapping. By Chapter II §14 Theorem 2 there is an ideal $\mathfrak{g}$ in $\mathcal{C}[\cdots, \kappa_{ij}, \cdots]$ such that n^2 constants k_{ij} $(i, j = 1, \cdots, n)$ in an extension of $\mathcal{G}$ form a zero of $\mathfrak{g}'$ if and only if they do so for $\mathfrak{g}$. We take $\mathfrak{g}$ as large as possible, so that any polynomial some power of which is in $\mathfrak{g}$ is itself in $\mathfrak{g}$.

If σ is any isomorphism of $\mathcal{G}$ over $\mathcal{F}$ then, for $j = 1, \cdots, n$, $\sigma\eta_j, \eta_1, \cdots, \eta_n$ are $n + 1$ solutions of $L(y)$, so that (Chapter II §15) there are n^2 constants k_{ij} in $\mathcal{F}<\mathcal{G}, \sigma\mathcal{G}>$ such that

$$\sigma\eta_j = \sum_{i=1}^{n} k_{ij}\eta_i, \qquad j = 1, \cdots, n. \tag{8}$$

Since $\sigma\eta_1, \cdots, \sigma\eta_n$ is a solution of Γ, the k_{ij}'s must form a zero of $\mathfrak{g}$. Since $\sigma\eta_1, \cdots, \sigma\eta_n$ (like $\eta_1, \cdots, \eta_n$) are linearly independent over constants, the determinant $|k_{ij}| \neq 0$.

Conversely, let k_{ij} $(i, j = 1, \cdots, n)$ be constants in an extension of $\mathcal{G}$ which form a zero of $\mathfrak{g}$ for which $|k_{ij}| \neq 0$. The equations (8) define a mapping σ of $\mathcal{F}\{\eta_1, \cdots, \eta_n\}$ for which $\sigma\eta_1, \cdots, \sigma\eta_n$ is a solution of Γ. Therefore σ is a homomorphism of $\mathcal{F}\{\eta_1, \cdots, \eta_n\}$ onto $\mathcal{F}\{\sigma\eta_1, \cdots, \sigma\eta_n\}$. Now

$$\partial^0\mathcal{F}<\eta_1, \cdots, \eta_n, \sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F} = \partial^0\mathcal{F}<\eta_1, \cdots, \eta_n>/\mathcal{F} + \partial^0\mathcal{F}<\eta_1, \cdots, \eta_n, \sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F}<\eta_1, \cdots, \eta_n>$$

$$\partial^0\mathcal{F}<\eta_1, \cdots, \eta_n, \sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F} = \partial^0\mathcal{F}<\sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F} + \partial^0\mathcal{F}<\eta_1, \cdots, \eta_n, \sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F}<\sigma\eta_1, \cdots, \sigma\eta_n>$$

so that

$$\partial^0\mathcal{F}<\eta_1, \cdots, \eta_n>/\mathcal{F} - \partial^0\mathcal{F}<\sigma\eta_1, \cdots, \sigma\eta_n>\mathcal{F} = \partial^0\mathcal{F}<\eta_1, \cdots, \eta_n, \sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F}<\sigma\eta_1, \cdots, \sigma\eta_n> - \partial^0\mathcal{F}<\eta_1, \cdots, \eta_n, \sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F}<\eta_1, \cdots, \eta_n>.$$

But clearly

$$\mathcal{F}<\eta_1, \cdots, \eta_n, \sigma\eta_1, \cdots, \sigma\eta_n> = \mathcal{F}<\eta_1, \cdots, \eta_n, k_{11}, k_{12}, \cdots, k_{nn}> = \mathcal{F}<\sigma\eta_1, \cdots, \sigma\eta_n, k_{11}, k_{12}, \cdots, k_{nn}>.$$

Therefore, if we let $\mathcal{C}'$ be the field of constants of $\mathcal{F}<\sigma\eta_1, \cdots, \sigma\eta_n>$ (so that $\mathcal{C}' \supseteq \mathcal{C}$), we find (using Chapter II §15 Theorem 2):

$$\partial^0\mathcal{F}<\eta_1, \cdots, \eta_n>/\mathcal{F} - \partial^0\mathcal{F}<\sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F} = \partial^0\mathcal{C}'(\cdots, k_{ij}, \cdots)/\mathcal{C}' - \partial^0\mathcal{C}(\cdots, k_{ij}, \cdots)/\mathcal{C} \leqq 0.$$

But σ is a homomorphism, so that we obviously have

$$\partial^0\mathcal{F}<\eta_1, \cdots, \eta_n>/\mathcal{F} \geqq \partial^0\mathcal{F}<\sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F}.$$

Therefore

$$\partial^0\mathcal{F}<\eta_1, \cdots, \eta_n>/\mathcal{F} = \partial^0\mathcal{F}<\sigma\eta_1, \cdots, \sigma\eta_n>/\mathcal{F}.$$

It follows, by Gourin's theorem (Chapter II §13 Theorem 1), that $\sigma\eta_1, \cdots, \sigma\eta_n$ is a generic solution of Γ, so that the homomorphism σ is actually an isomorphism of $\mathcal{F}\{\eta_1, \cdots, \eta_n\}$, and can clearly be extended in a unique way to an isomorphism of $\mathcal{G}$ over $\mathcal{F}$. Thus we have proved:

The equations (8) define a one-to-one correspondence between isomorphisms σ of $\mathcal{G}$ over $\mathcal{F}$ and nonsingular matrices (k_{ij}) of degree n in which the elements k_{ij} are constants contained in some differential extention field of $\mathcal{G}$ which form a solution of $\mathfrak{g}$.

Since $\mathcal{F}<\mathcal{G}, \sigma\mathcal{G}> = \mathcal{G}<\cdots, k_{ij}, \cdots>$, it is easy to see that the isomorphism σ is an automorphism if and only if $k_{ij} \in \mathcal{C} (i, j = 1, \cdots, n)$. It is also easy to see that the product of two automorphisms of $\mathcal{G}$ over $\mathcal{F}$ corresponds through (8) to the product of the respective matrices of the automorphisms. Therefore we have proved:

THEOREM. *The equations* (8) *establish an isomorphism between the group of all automorphisms of* $\mathcal{G}$ *over* $\mathcal{F}$ *and an algebraic matric group over* $\mathcal{C}$ *of degree* n.

We shall, when danger of confusion does not arise, use the same letter to denote both the automorphism and its matrix, and shall regard the group of automorphisms as an algebraic matric group. We denote this group by $\mathfrak{G}$. The defining ideal of $\mathfrak{G}$ is $\mathfrak{g}$.

EXAMPLE 1. The *general* homogeneous linear ordinary differential equation of order n is $y^{(n)} + u_1 y^{(n-1)} + \cdots + u_n y = 0$, where $u_1, \cdots, u_n$ are new unknowns. If $\mathcal{F}_0$ is any ordinary differential field of characteristic 0 with respect to which $u_1, \cdots, u_n$ are still unknowns, if $\mathcal{C}$ is the field of constants of $\mathcal{F}_0$ (and therefore of $\mathcal{F}_0<u_1, \cdots, u_n>$), and if $\eta_1, \cdots, \eta_n$ are any n solutions of the general equation, linearly independent over constants, contained in some extension of $\mathcal{F}_0<u_1, \cdots, u_n>$, then $\eta_1, \cdots, \eta_n$ annul no nonzero differential polynomial in $\mathcal{F}_0\{y_1, \cdots, y_n\}$. $\mathcal{G} = \mathcal{F}_0<u_1, \cdots, u_n, \eta_1, \cdots, \eta_n>$ is a Picard-Vessiot extension of $\mathcal{F} = \mathcal{F}_0<u_1, \cdots, u_r>$ for which the group of automorphisms is the full matric group over $\mathcal{C}$ of degree n.

EXAMPLE 2. If the coefficients $p_1, \cdots, p_n$ in $L(y)$ are all constants then it is easy to see that $\mathfrak{G}$ is reducible to triangular form. If $\mathcal{F}$ contains an element x such that $x' = 1$ then $\mathfrak{G}$ is reducible to diagonal form.

18. Normality

Let $\alpha = P(\eta_1, \cdots, \eta_n)/Q(\eta_1, \cdots, \eta_n)$ and $\beta = R(\eta_1, \cdots, \eta_n)/S(\eta_1, \cdots, \eta_n)$ be any two elements of $\mathcal{G}$. An isomorphism τ of $\mathcal{G}$ over $\mathcal{F}$ will satisfy $\tau\alpha = \beta$ if and only if the elements of the matrix of τ satisfy the equation

$$S(\eta_1, \cdots, \eta_n)P(\sum \kappa_{i1}\eta_i, \cdots, \sum \kappa_{in}\eta_i) = R(\eta_1, \cdots, \eta_n)Q(\sum \kappa_{i1}\eta_i, \cdots, \sum \kappa_{in}\eta_i)$$

in the indeterminates κ_{ij}. By Chapter II §14 Theorem 2 we see that the conditon $\tau\alpha = \beta$ can be expressed algebraically over $\mathcal{C}$.

Now, since $\mathcal{C}$ is algebraically closed, a set of polynomials over $\mathcal{C}$ which has a zero, has a zero with coordinates in $\mathcal{C}$. Therefore, if there exists an isomorphism of $\mathcal{G}$ over $\mathcal{F}$ the matrix of which has elements satisfying a given set of algebraic conditions over $\mathcal{C}$, then there exists an automorphism of $\mathcal{G}$ over $\mathcal{F}$ (that is, an element of $\mathfrak{G}$) satisfying the same conditions.

In particular, if $\mathcal{F}_1$ is any differential field such that $\mathcal{F} \subseteq \mathcal{F}_1 \subseteq \mathcal{G}$, if $\alpha \in \mathcal{G} - \mathcal{F}_1$, and if there exists an isomorphism σ' of $\mathcal{G}$ over $\mathcal{F}$ such that $\sigma'\alpha_1 = \alpha_1$ for all $\alpha_1 \in \mathcal{F}_1$ and $\sigma'\alpha \neq \alpha$, then there exists a $\sigma \in \mathfrak{G}$ with the same properties. But by Chapter II §12 such an isomorphism σ' always exists. Thus, we have the following result.

THEOREM 1. *Every Picard-Vessiot extension of $\mathcal{F}$ is a normal extension of $\mathcal{F}$.*

In conformity with Chapter III we shall denote the set of all differential fields $\mathcal{F}_1$ such that $\mathcal{F} \subseteq \mathcal{F}_1 \subseteq \mathcal{G}$ by $\mathbf{F}$, the subgroup of $\mathfrak{G}$ consisting of all automorphisms of $\mathcal{G}$ over $\mathcal{F}_1$ ($\mathcal{F}_1 \in \mathbf{F}$) by $\mathfrak{G}(\mathcal{F}_1)$, the set of all groups $\mathfrak{G}(\mathcal{F}_1)$ with $\mathcal{F}_1 \in \mathbf{F}$ by $\mathbf{G}$.

Since $\mathcal{G}$ is a normal extension of $\mathcal{F}$ we have at our disposal the theorems of Chapter III. In the special case of Picard-Vessiot extensions, however, Theorem 2 of Chapter III can be strengthened (see Remarks 1 and 2 at the end of that chapter) by the following result.

THEOREM 2. *Let $\mathcal{F}_1 \in \mathbf{F}$. If $\mathfrak{G}(\mathcal{F}_1)$ is a normal subgroup of $\mathfrak{G}$ then $\mathfrak{G}/\mathfrak{G}(\mathcal{F}_1)$ is isomorphic with the group of all automorphisms of $\mathcal{F}_1$ over $\mathcal{F}$.*

PROOF. We know from Chapter III that $\sigma\mathcal{F}_1 = \mathcal{F}_1$, so that σ induces an automorphism σ_0 of $\mathcal{F}_1$ over $\mathcal{F}$, and the set of automorphisms σ_0 so induced is a group isomorphic with $\mathfrak{G}/\mathfrak{G}(\mathcal{F}_1)$. It remains to show that every automorphism σ_0 of $\mathcal{F}_1$ over $\mathcal{F}$ can be so induced, that is, that every such σ_0 can be extended to an automorphism of $\mathcal{G}$ over $\mathcal{F}$. That this can be done is shown by the following more general result.

LEMMA. *Let $\mathcal{F}_1, \mathcal{F}_2 \in \mathbf{F}$. If σ_0 is an isomorphism over $\mathcal{F}$ of $\mathcal{F}_1$ onto $\mathcal{F}_2$ then σ_0 can be extended to an automorphism $\sigma \in \mathfrak{G}$.*

PROOF. By Chapter II, §12, σ_0 can be extended to an isomorphism σ' of $\mathcal{G}$ over $\mathcal{F}$. By the first two paragraphs of the present section there is an automorphism $\sigma \in \mathfrak{G}$ coinciding with σ' for all α in $\mathcal{G}$ for which $\sigma'\alpha \in \mathcal{G}$.

19. Characterization of G

For any $\mathcal{F}_1 \in \mathbf{F}$ we have $\mathcal{F}_1\langle\eta_1, \cdots, \eta_n\rangle = \mathcal{G}$, so that $\mathcal{G}$ is a Picard-Vessiot extension of F_1. Therefore $\mathfrak{G}(\mathcal{F}_1)$ is an algebraic group, that is, every element of $\mathbf{G}$ is an algebraic subgroup of $\mathfrak{G}$. We shall now prove the converse thereby obtaining the following result.

THEOREM. *$\mathbf{G}$ is the set of all algebraic subgroups of $\mathfrak{G}$.*

PROOF. It remains to show that if $\mathfrak{G}_1$ is an algebraic subgroup of $\mathfrak{G}$ then $\mathfrak{G}_1 \in \mathbf{G}$. Let $\mathcal{F}_1$ be the set of all elements of $\mathcal{G}$ invariant under every $\tau \in \mathfrak{G}_1$. Clearly $\mathfrak{G}_1 \subseteq \mathfrak{G}(\mathcal{F}_1)$. If $\mathfrak{G}_1 = \mathfrak{G}(\mathcal{F}_1)$ then $\mathfrak{G}_1 \in \mathbf{G}$. Suppose $\mathfrak{G}_1 \subset \mathfrak{G}(\mathcal{F}_1)$.

There is a polynomial $f(\cdots, \kappa_{ij}, \cdots) \in \mathcal{C}[\cdots, \kappa_{ij}, \cdots]$ which vanishes for every $\sigma = (k_{ij}) \in \mathfrak{G}_1$ but not for every $\sigma = (k_{ij}) \in \mathfrak{G}(\mathcal{F}_1)$. If we denote the inverse of the wronskian matrix $(\eta_j^{(i)})$ by (H_{ij}), then

$$f\left(\cdots, \sum_{l=0}^{n-1} H_{li} y_j^{(l)}, \cdots\right)$$

is a differential polynomial in $\mathcal{G}\{y_1, \cdots, y_n\}$ which has the solution

$$y_1 = \sigma\eta_1, \cdots, y_n = \sigma\eta_n \tag{9}$$

for all $\sigma \in \mathfrak{G}_1$ but not for all $\sigma \in \mathfrak{G}(\mathcal{F}_1)$. Of all differential polynomials in $\mathcal{G}\{y_1, \cdots, y_n\}$ which have this property let $F = F(y_1, \cdots, y_n)$ be one with fewest possible terms. We assume without loss of generality that one of the coefficients in F is 1.

For any $\tau \in \mathfrak{G}_1$ denote by $F_\tau = F_\tau(y_1, \cdots, y_n)$ the differential polynomial obtained by replacing each coefficient in F by its image under τ. Then

$$F_\tau(\sigma\eta_1, \cdots, \sigma\eta_n) = \tau F(\tau^{-1}\sigma\eta_1, \cdots, \tau^{-1}\sigma\eta_n) = 0$$

whenever $\sigma \in \mathfrak{G}_1$, so that (9) is a solution of $F - F_\tau$ whenever $\sigma \in \mathfrak{G}_1$. Since $F - F_\tau$ has fewer terms than F has, $F - F_\tau$ must admit the solution (9) for all $\sigma \in \mathfrak{G}(\mathcal{F}_1)$. Therefore, for any $\gamma \in \mathcal{G}$, $F - \gamma(F - F_\tau)$ has (9) as a solution for every $\sigma \in \mathfrak{G}_1$ but not for every $\sigma \in \mathfrak{G}(\mathcal{F}_1)$. If $F - F_\tau$ were not 0 there would be a $\gamma \in \mathcal{G}$ for which $F - \gamma(F - F_\tau)$ had fewer terms than F, which would contradict the definition of F. Hence $F - F_\tau = 0$, that is, each coefficient in F is invariant under every $\tau \in \mathfrak{G}_1$ and is therefore in $\mathcal{F}_1$. It follows that $F(\sigma\eta_1, \cdots, \sigma\eta_n) = \sigma F(\eta_1, \cdots, \eta_n) = 0$ for all $\sigma \in \mathfrak{G}(\mathcal{F}_1)$. This contradiction completes the proof.

20. Dimension

For each j, η_j is a solution of the differential polynomial $L(y)$ so that every $\eta_j^{(i)}$ with $i \geqq n$ can be expressed linearly (and therefore rationally) in terms of $\eta_j, \eta_j', \cdots, \eta_j^{(n-1)}$. It follows that the degree of transcendency of $\mathcal{G}$ over $\mathcal{F}$ is at most n^2: $\partial^0\mathcal{G}/\mathcal{F} \leqq n^2$.

Again, $\mathfrak{G}$ is contained in the full matric group, which is an algebraic matric group of dimension n^2. Therefore the dimension of $\mathfrak{G}$ is at most n^2: $\dim \mathfrak{G} \leqq n^2$.

THEOREM. $\dim \mathfrak{G} = \partial^0\mathcal{G}/\mathcal{F}$.

As in §17, let Γ be the prime differential ideal in $\mathcal{F}\{y_1, \cdots, y_n\}$ consisting of all differential polynomials vanishing for $y_1 = \eta_1, \cdots, y_n = \eta_n$. Let Γ' be the perfect differential ideal generated by Γ in $\mathcal{G}\{y_1, \cdots, y_n\}$, and let

$$\Gamma' = \Gamma_1 \cap \cdots \cap \Gamma_s$$

be the representation of Γ' as the intersection of its prime components Γ_i in $\mathcal{G}\{y_1, \cdots, y_n\}$ (see Chapter II §10).

The substitution $y_j \to \sum_i \kappa_{ij}\eta_i$ $(j = 1, \cdots, n)$ defines a mapping which sends every element of $\mathcal{G}\{y_1, \cdots, y_n\}$ into an element of $\mathcal{G}[\cdots, \kappa_{ij}, \cdots]$. By con-

sidering the matrix (H_{ij}) inverse to $(\eta_j^{(i)})$ we see as in §4 that this is a mapping of $\mathfrak{G}\{y_1, \cdots, y_n\}$ *onto* $\mathfrak{G}[\cdots, \kappa_{ij}, \cdots]$. By considering generic solutions of the Γ_i's, it is not difficult to see that if an element of $\mathfrak{G}\{y_1, \cdots, y_n\}$ is mapped thus onto 0, then the element is contained in Γ'.

For each h let $\mathfrak{g}_h'$ be the image under this mapping of Γ_h. Since Γ_h is a prime ideal, and every element of $\mathfrak{G}[\cdots, \kappa_{ij}, \cdots]$ is the image of some element of $\mathfrak{G}\{y_1, \cdots, y_n\}$, it is easy to see that $\mathfrak{g}_h'$ is a prime ideal in $\mathfrak{G}[\cdots, \kappa_{ij}, \cdots]$.

Let $\eta_1^*, \cdots, \eta_n^*$ be a generic solution of Γ_h. Then each η_j^* is a solution of $L(y)$, so that

$$\eta_j^* = \sum_{i=1}^{n} k_{ij}^* \eta_i \qquad (j = 1, \cdots, n)$$

where the k_{ij}^*'s are constants in some extension of $\mathfrak{G}$. Clearly every element of $\mathfrak{g}_h'$ vanishes for $(\kappa_{ij}) = (k_{ij}^*)$. Conversely, if $f(\cdots, \kappa_{ij}, \cdots) \in \mathfrak{G}[\cdots, \kappa_{ij}, \cdots]$ vanishes for $(\kappa_{ij}) = (k_{ij}^*)$ then $f(\cdots, \sum_l H_{li} y_j^{(l)}, \cdots) \in \mathfrak{G}\{y_1, \cdots, y_n\}$ vanishes for $y_1 = \eta_1^*, \cdots, y_n = \eta_n^*$, so that $f(\cdots, \sum_l H_{li} y_j^{(l)}, \cdots) \in \Gamma_h$, and $f(\cdots, \kappa_{ij}, \cdots) \in \mathfrak{g}_h'$. Thus (k_{ij}^*) is a generic zero of $\mathfrak{g}_h'$.

By Chapter I §14 Theorem 2, we see that $\mathfrak{g}_h'$ is equivalent to a prime ideal $\mathfrak{g}_h$ in $\mathcal{C}[\cdots, \kappa_{ij}, \cdots]$ of which (k_{ij}^*) is again a generic zero. Now, $(\kappa_{ij}) = (k_{ij})$ will be a solution of $\mathfrak{g}_1 \cap \cdots \cap \mathfrak{g}_s$ if and only if $y_1 = \sum k_{i1}\eta_i, \cdots, y_n = \sum k_{in}\eta_i$ is a solution of Γ, that is, if and only if $(\kappa_{ij}) = (k_{ij})$ is a solution of $\mathfrak{g}$, the defining ideal of $\mathfrak{G}$. Therefore $\mathfrak{g} = \mathfrak{g}_1 \cap \cdots \cap \mathfrak{g}_s$.

For each h we have

$$\dim \mathfrak{g}_h = \partial^0\mathcal{C}(\cdots, k_{ij}^*, \cdots)/\mathcal{C} = \partial^0\mathfrak{G}(\cdots, k_{ij}^*, \cdots)/\mathfrak{G} = \partial^0\mathfrak{G}<\eta_1^*, \cdots, \eta_n^*>/\mathfrak{G} = \operatorname{ord}\Gamma_h.$$

But by Ritt's theorem (Chapter II §13 Theorem 2), $\operatorname{ord}\Gamma_h = \operatorname{ord}\Gamma$, and, since $\eta_1, \cdots, \eta_n$ is a generic solution of Γ, $\operatorname{ord}\Gamma = \partial^0\mathcal{F}<\eta_1, \cdots, \eta_n>/\mathcal{F} \leqq \partial^0\mathfrak{G}/\mathcal{F}$. Therefore $\dim \mathfrak{g}_h = \partial^0\mathfrak{G}/\mathcal{F}$. Since this holds for $h = 1, \cdots, s$ this proves anew that the underlying manifold of $\mathfrak{G}$ breaks up into irreducible manifolds of equal dimension (Chapter I §2), and also shows that $\dim \mathfrak{G} = \partial^0\mathfrak{G}/\mathcal{F}$.

21. Adjunction of new elements

Let $\mathfrak{M}$ be a set of elements in some differential extension field of $\mathfrak{G}$ in which every constant is an element of $\mathcal{C}$, and write $\mathcal{F}^\dagger = \mathcal{F}<\mathfrak{M}>$, $\mathfrak{G}^\dagger = \mathfrak{G}<\mathfrak{M}>$. Then $\mathfrak{G}^\dagger = \mathcal{F}^\dagger<\eta_1, \cdots, \eta_n>$, so that $\mathfrak{G}^\dagger$ is a Picard-Vessiot extension of $\mathcal{F}^\dagger$. Denote the group of all automorphisms of $\mathfrak{G}^\dagger$ over $\mathcal{F}^\dagger$ by $\mathfrak{G}^\dagger$.

THEOREM. *$\mathfrak{G}^\dagger$ is isomorphic with $\mathfrak{G}(\mathcal{F}^\dagger \cap \mathfrak{G})$.*

PROOF. If $\sigma^\dagger \in \mathfrak{G}^\dagger$ then $\sigma^\dagger$ obviously leaves invariant each element of $\mathcal{F}$. Also, if we denote the matrix of $\sigma^\dagger$ by $(k_{ij}^\dagger)$, then $\sigma^\dagger \eta_j = \sum_i k_{ij}^\dagger \eta_i$, and each $k_{ij}^\dagger \in \mathcal{C}$, so that $\sigma^\dagger\mathfrak{G} = \mathfrak{G}$. Therefore $\sigma^\dagger$ induces an automorphism σ of $\mathfrak{G}$ over $\mathcal{F}$: $\sigma\alpha = \sigma^\dagger\alpha (\alpha \in \mathfrak{G})$. The matrix of σ is identical with that of $\sigma^\dagger$. Therefore $\mathfrak{G}^\dagger$ is isomorphic with a subgroup $\mathfrak{G}(\mathcal{F}_1)$ of $\mathfrak{G}$, where $\mathcal{F}_1 \in \mathbf{F}$. Now, every element of $\mathcal{F}^\dagger \cap \mathfrak{G}$ is invariant under every $\sigma^\dagger \in \mathfrak{G}^\dagger$ and therefore under every $\sigma \in \mathfrak{G}(\mathcal{F}_1)$.

On the other hand, an element of $\mathfrak{S}$ which is invariant under every $\sigma \in \mathfrak{G}(\mathcal{F}_1)$, that is, under every $\sigma^\ddagger \in \mathfrak{G}^\ddagger$, must be in $\mathcal{F}^\ddagger$ and therefore in $\mathcal{F}^\ddagger \cap \mathfrak{S}$. Therefore the set of all elements of $\mathfrak{S}$ invariant under every $\sigma \in \mathfrak{G}(\mathcal{F}_1)$ is $\mathcal{F}^\ddagger \cap \mathfrak{S}$, so that $\mathcal{F}_1 = \mathcal{F}^\ddagger \cap \mathfrak{S}$.

22. Linear reducibility of $L(y)$

The homogeneous linear ordinary differential polynomial $L(y)$ is called *linearly reducible* over $\mathcal{F}$ if there exist two homogeneous linear differential polynomials $J(y), K(y) \in \mathcal{F}\{y\}$ of positive order such that $L(y) = K(J(y))$.[22]

THEOREM 1. *$L(y)$ is linearly reducible if and only if the algebraic matric group $\mathfrak{G}$ of degree n is reducible.*[23]

PROOF. Let $L(y) = K(J(y))$, with $J(y)$ of order $m (0 < m < n)$. A solution of $J(y)$ is a solution of $L(y)$, so that every solution of $J(y)$ lying in an extension of $\mathfrak{S}$ is a linear combination with constant coefficients of $\eta_1, \cdots, \eta_n$. Since such linear combinations exist, and since $\mathcal{C}$ is algebraically closed, it is easy to see that such linear combinations exist with coefficients in $\mathcal{C}$, that is, there exists a $\zeta = c_1\eta_1 + \cdots + c_n\eta_n \in \mathfrak{S}$ such that $J(\zeta) = 0$. Therefore the set of all solutions of $J(y)$ in $\mathfrak{S}$, which is a linear subspace of the n-dimensional linear space spaned by $\eta_1, \cdots, \eta_n$, has dimension > 0 and $< n$. But this subspace is clearly an invariant one for each $\sigma \in \mathfrak{G}$, so that $\mathfrak{G}$ is reducible.

Conversely, let $\mathfrak{G}$ be reducible. Then, after a proper choice of the fundamental system of solutions $\eta_1, \cdots, \eta_n$, we may suppose that there is an m $(0 < m < n)$ such that every $\sigma \in \mathfrak{G}$ is of the form

$$\sigma = \begin{pmatrix} \sigma_1 & * \\ 0 & \sigma_2 \end{pmatrix},$$

where σ_1 is a square matrix of degree m and σ_2 is a square matrix of degree $n - m$. From this it follows that the coefficients in the homogeneous linear differential polynomial $J(y) = W(y, \eta_1, \cdots, \eta_m)/W(\eta_1, \cdots, \eta_m)$ in y (quotient of two wronskian determinants) are all invariant under every $\sigma \in \mathfrak{G}$, so that $J(y)$ has all its coefficients in $\mathcal{F}$. Since every solution of $J(y)$ is a solution of $L(y)$ it is easy to see that there exists a homogeneous linear $K(y) \in \mathcal{F}\{y\}$ such that $L(y) = K(J(y))$.

Using the same methods it is easy to prove

THEOREM 2. *$\mathfrak{G}$ is reducible to the form*

$$\begin{pmatrix} \mathfrak{G}_1 & & * \\ & \ddots & \\ 0 & & \mathfrak{G}_k \end{pmatrix},$$

[22] This definition is equivalent to one first given by FROBENIUS [1] for more special coefficient domains.

[23] First proved by BEKE [1].

where $\mathfrak{G}_i$ is a group of matrices of degree n_i ($n_1 + \cdots + n_k = n$), if and only if there exist k homogeneous linear differential polynomials $L_1(y), \cdots, L_k(y)$, with coefficients in $\mathcal{F}$, of orders $n_1, \cdots, n_k$, respectively, such that $L(y) = L_k(\cdots L_1(y) \cdots)$. When this is the case then $\mathfrak{G}_i$ is isomorphic with the group of all automorphisms of $\mathcal{F}<\zeta_{i1}, \cdots, \zeta_{in_i}>$ over $\mathcal{F}$, where $\zeta_{i1}, \cdots, \zeta_{in_i}$ are n_i solutions of $L_i(y)$ in $\mathcal{G}$, linearly independent over constants.

This theorem was first stated by Loewy [1]. Loewy's proof seems to show merely that $\mathfrak{G}_i$ is an abundant subgroup of the group of all automorphisms. That $\mathfrak{G}_i$ is an algebraic group, and therefore the full group of automorphisms, follows from the lemma in Chater I §5.

Chapter V. Liouvillian Extensions

23. Integrals and exponentials of integrals

By an *integral* of an element a of a differential field, we shall mean any solution of the differential equation $y' = a$.

Two integrals of a which are contained in the same extension of the given differential field containing a clearly differ by a constant.

As in Chapter IV, let $\mathcal{F}$ be a differential field of characteristic 0 with an algebraically closed field of constants $\mathcal{C}$.

Let α be an integral of $a \in \mathcal{F}$ such that $\alpha \notin \mathcal{F}$ and every constant in $\mathcal{F}<\alpha>$ is in $\mathcal{C}$. Then $a \neq 0$, and $1, \alpha$ are linearly independent over constants. Since $1, \alpha$ are solutions of the homogeneous linear ordinary differential polynomial $y'' - (a'/a)y'$, we see that $\mathcal{F}<\alpha>$ is a Picard-Vessiot extension of $\mathcal{F}$. For any σ in the group $\mathfrak{G}_I$ of all automorphisms of $\mathcal{F}<\alpha>$ over $\mathcal{F}$ we have $\sigma 1 = 1$, $\sigma\alpha = c + \alpha$ (because $\sigma\alpha$, like α, is a solution of $y' = a$), so that the matrix of σ is $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$. For every $\sigma \neq \iota$ we have $c \neq 0$. Because $\mathfrak{G}_I$ is algebraic and contains the matrix $\begin{pmatrix} 1 & hc \\ 0 & 1 \end{pmatrix}$ of σ^h for $h = 0, 1, \cdots$, it follows that $\mathfrak{G}_I$ contains the matrix $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ for every $k \in \mathcal{C}$. Thus $\mathfrak{G}_I$ is isomorphic with the additive group of $\mathcal{C}$, and contains no proper algebraic subgroup other than $\mathfrak{E}$ (in particular, $\mathfrak{G}_I$ is abelian and anticompact. It follows that α is transcendental over $\mathcal{F}$, and that there is no differential field properly between $\mathcal{F}$ and $\mathcal{F}<\alpha>$.

By an *exponential of an integral* of an element a of a differential field we shall mean any solution of the differential polynomial $y' - ay$.[24] If α and $\beta \neq 0$ are both exponentials of an integral of a contained in a common differential field then $(\alpha/\beta)' = (\beta\alpha' - \alpha\beta')/\beta^2 = (\beta a\alpha - \alpha a\beta)/\beta^2 = 0$, so that $\alpha = k\beta$, with k a constant.

[24] Thus, the concept "exponential of a" has not been defined. It could be defined as an exponential of an integral of a', but for the purposes of the present paper nothing would be gained thereby.

Let α be an exponential of an integral of $a \in \mathcal{F}$ such that every constant in $\mathcal{F}<\alpha>$ is in $\mathcal{C}$. Then $\mathcal{F}<\alpha>$ is a Picard-Vessiot extension of $\mathcal{F}$. For each automorphism σ of $\mathcal{F}<\alpha>$ over $\mathcal{F}$ we have $\sigma\alpha = k\alpha$ ($k \in \mathcal{C}$), so that σ has the matrix (k) of degree 1. If α is algebraic over $\mathcal{F}$ then the group of all such automorphisms is of finite order h, $\sigma^h = \iota$, and $k^h = 1$. Therefore $\sigma(\alpha^h) = (\sigma\alpha)^h = (k\alpha)^h = \alpha^h$ for each σ, so that $\alpha^h \in \mathcal{F}$. If α is transcendental over $\mathcal{F}$ then the group of all automorphisms of $\mathcal{F}<\alpha>$ over $\mathcal{F}$, which group we now call $\mathfrak{G}_E$, is of dimension 1 and is isomorphic with the group of all matrices (k) of degree 1 with nonzero $k \in \mathcal{C}$ (i.e., isomorphic with the multiplicative group of $\mathcal{C}$). The only algebraic subgroups of $\mathfrak{G}_E$ are cyclic groups of finite order, and precisely one such subgroup of each order exists (thus, $\mathfrak{G}_E$ is abelian and quasicompact). If $\mathfrak{G}_E^h$ is the one of order h and $\mathcal{F}^h$ is the differential subfield of $\mathcal{F}<\alpha>$ corresponding to $\mathfrak{G}_E^h$, then $\mathcal{F}^h = \mathcal{F}<\alpha^h>$. Now, α^h is an exponential of an integral of ha, so that $\mathfrak{G}_E/\mathfrak{G}_E^h$, which is isomorphic with the group of automorphisms of $\mathcal{F}<\alpha^h>$ over $\mathcal{F}$, is isomorphic with $\mathfrak{G}_E$.

24. Liouvillian extensions

A differential extension field $\mathcal{H} \supseteq \mathcal{F}$, all the constants of which are in $\mathcal{C}$, will be called a *liouvillian* extension of $\mathcal{F}$ if $\mathcal{H}$ is an extension of $\mathcal{F}$ by integrals, exponentials of integrals, and algebraic functions, i.e., if there exists a finite sequence of elements $\alpha_1, \cdots, \alpha_r \in \mathcal{H}$ such that:

(a) for each i, either α_i is an integral of an element of $\mathcal{F}<\alpha_1, \cdots, \alpha_{i-1}>$, or α_i is an exponential of an integral of such an element, or α_i is algebraic over $\mathcal{F}<\alpha_1, \cdots, \alpha_{i-1}>$;

(b) $\mathcal{H} = \mathcal{F}<\alpha_1, \cdots, \alpha_r>$;

(c) every constant in $\mathcal{H}$ is in $\mathcal{F}$ (i.e., te field of constants of $\mathcal{H}$ is $\mathcal{C}$).

For a given liouvillian extension of $\mathcal{F}$ it may not be necessary to employ all three types of elements α_i. We shall distinguish ten types of liouvillian extensions, namely, extensions by

(1) integrals, exponentials of integrals, and algebraic functions,
(2) integrals and exponentials of integrals,
(3) exponentials of integrals, and algebraic functions,
(4) integrals and algebraic functions,
(5) integrals and radicals,
(6) exponentials of integrals,
(7) integrals,
(8) algebraic functions,
(9) radicals,
(10) rational functions.

Thus, every liouvillian extension is of the first type, and the only one of the last type is $\mathcal{F}$ itself. There is no need to discuss separately extensions by exponentials of integrals and radicals, for such an extension is an extension by exponentials of integrals (if $\alpha^h = a \in \mathcal{F}$, then $\alpha' - h^{-1}a^{-1}a'\alpha = 0$).

We remark that if $\mathcal{H} = \mathcal{F}\langle\alpha_1, \cdots, \alpha_r\rangle$ is a liouvillian extension of $\mathcal{F}$, with $\alpha_1, \cdots, \alpha_r$ as above, then $\mathcal{H}$ is contained in a liouvillian extension $\mathcal{F}\langle\beta_1, \cdots, \beta_r\rangle$, where $\beta_1, \cdots, \beta_r$ have the same properties as $\alpha_1, \cdots, \alpha_r$ above, and for each i $\mathcal{F}\langle\beta_1, \cdots, \beta_i\rangle$ is a normal extension of $\mathcal{F}\langle\beta_1, \cdots, \beta_{i-1}\rangle$. Indeed, when α_i is an integral or an exponential of an integral of an element of $\mathcal{F}\langle\alpha_1, \cdots, \alpha_{i-1}\rangle$ then by §23 $\mathcal{F}\langle\alpha_1, \cdots, \alpha_i\rangle$ is a Picard-Vessiot extension of $\mathcal{F}\langle\alpha_1, \cdots, \alpha_{i-1}\rangle$ and *a fortiori* normal. When α_i is algebraic over $\mathcal{F}\langle\alpha_1, \cdots, \alpha_{i-1}\rangle$ we may replace α_i by a primitive element of the splitting field over $\mathcal{F}\langle\alpha_1, \cdots, \alpha_{i-1}\rangle$ of the irreducible equation satisfied by α_i.

25. The principal theorem and some consequences

We return now to a Picard-Vessiot extension $\mathcal{G} = \mathcal{F}\langle\eta_1, \cdots, \eta_n\rangle$ as in Chapter IV, and list certain properties which the group $\mathfrak{G}$ of all automorphisms of $\mathcal{G}$ over $\mathcal{F}$ and its component of the identity $\mathfrak{G}^0$ may possess:

(1) $\mathfrak{G}^0$ is solvable:
(2) $\mathfrak{G}$ is solvable;
(3) $\mathfrak{G}^0$ is solvable and quasicompact;
(4) $\mathfrak{G}^0$ is solvable and anticompact;
(5) $\mathfrak{G}$ is solvable and $\mathfrak{G}^0$ is anticompact;
(6) $\mathfrak{G}$ is solvable and quasicompact;
(7) $\mathfrak{G}$ is solvable and anticompact;
(8) $\mathfrak{G}$ is finite;
(9) $\mathfrak{G}$ is solvable and finite;
(10) $\mathfrak{G} = \mathfrak{E}$.

It will be observed that we have here distinguished as many types of algebraic matric groups as we have of liouvillian extensions in §24.

THEOREM. *Let i be a positive integer $\leqq 10$. If $\mathcal{G}$ is contained in a liouvillian extension of $\mathcal{F}$ of type (i) then $\mathfrak{G}$ is an algebraic matric group of type (i). Conversely, if $\mathfrak{G}$ is an algebraic matric group of type (i) then $\mathcal{G}$ is a liouvillian extension of $\mathcal{F}$ of type (i).*

Several remarks can be made on the basis of this theorem:

1. If $\mathcal{G}$ is a liouvillian extension of $\mathcal{F}$, then there is an $\mathcal{F}^0$ between $\mathcal{F}$ and $\mathcal{G}$ such that $\mathcal{F}^0$ is a normal algebraic extension of $\mathcal{F}$, and $\mathcal{G}$ is an extension of $\mathcal{F}^0$ by integrals and exponentials of integrals (indeed, $\mathcal{F}^0$ is the differential field such that $\mathfrak{G}(\mathcal{F}^0) = \mathfrak{G}^0$). If $\mathcal{G}$ is a liouvillian extension of $\mathcal{F}$ of one of the types (3), (4), (5) then $\mathcal{G}$ is a liouvillian extension of $\mathcal{F}^0$ of, respectively, the types (6), (7), (7) (and in the last case $\mathcal{F}^0$ is an extension of $\mathcal{F}$ by radicals).

2. If $\mathcal{G}$ is a liouvillian extension of $\mathcal{F}$ and $\mathcal{F}^0$ is as above, then the homogeneous linear differential polynomial $L(y)$ splits completely over $\mathcal{F}^0$ into "factors" of order 1, i.e., there are n differential polynomials $L_i(y) = y' - a_i y$ $(a_i \in \mathcal{F}^0)$ such that $L(y) = L_n(\cdots L_1(y) \cdots)$ (see Chapter I §7 Theorem 1 and Chapter IV §22 Theorem 2). If $\mathcal{G}$ is an extension of $\mathcal{F}$ by integrals then $L(y)$ splits completely over $\mathcal{F}$ (see Chapter I §7 Theorem 2).

3. If $\mathcal{G}$ is an extension by exponentials of integrals and algebraic functions then $L(y)$ has a fundamental system of solutions in $\mathcal{G}$ composed of exponentials of integrals of elements of $\mathcal{F}^0$ ($\mathcal{F}^0$ as above) (see Chapter I §7 Theorems 1 and 2).

4. If $\mathcal{G}$ is an extension of $\mathcal{F}$ by integrals and also an extension of $\mathcal{F}$ by exponentials of integrals, then $\mathcal{G} = \mathcal{F}$. If $\mathcal{G}$ is an extension by integrals and algebraic functions, and also by exponentials of integrals and algebraic functions, then $\mathcal{G}$ is algebraic over $\mathcal{F}$.

5. If $\dim \mathfrak{G} > n(n-1)/2$ (the dimension of the full triangular group $\mathfrak{T}$) then $\mathcal{G}$ is not contained in a liouvillian extension of $\mathcal{F}$. In particular, the general homogeneous linear ordinary differential equation of order $n > 1$ does not have a fundamental system of solutions in any liouvillian extension of $\mathcal{F}_0\langle u, \cdots, u_n\rangle$, where $\mathcal{F}_0$ is any differential field of characteristic zero over which $u_1, \cdots, u_n$ are unknowns (see Chapter I §7 Theorem 1 and Chapter IV §17 Example 1).

26. The proof, first half

Let $\mathcal{G}$ be contained in a liouvillian extension $\mathcal{F}\langle\alpha_1, \cdots, \alpha_r\rangle$ where $\alpha_1, \cdots, \alpha_r$ are as in §24 (see final remark in §24).

We shall show that $\mathfrak{G}$ has a normal chain in which each factor group is abelian or finite. This is obvious for $r = 0$. Assume, inductively, that $r > 0$ and that this result is verified for lower values of r.

By Chapter IV §21, $\mathcal{G}\langle\alpha_1\rangle$ is a Picard-Vessiot extension of $\mathcal{F}\langle\alpha_1\rangle$, and the group of all automorphisms of $\mathcal{G}\langle\alpha_1\rangle$ over $\mathcal{F}\langle\alpha_1\rangle$ is isomorphic with $\mathfrak{G}(\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle)$. By the induction assumption, then, $\mathfrak{G}(\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle)$ has a normal chain in which each factor group is abelian or finite. Now, $\mathcal{F} \subseteq \mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle \subseteq \mathcal{F}\langle\alpha_1\rangle$.

If α_1 is an integral of an element of $\mathcal{F}$ then (§23) either $\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle = \mathcal{F}$, in which case $\mathfrak{G}(\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle) = \mathfrak{G}$, or $\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle = \mathcal{F}\langle\alpha_1\rangle$. In the latter case, by §23, $\sigma(\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle) = \sigma\mathcal{F}\langle\alpha_1\rangle = \mathcal{F}\langle\sigma\alpha_1\rangle = \mathcal{F}\langle\alpha_1 + c\rangle = \mathcal{F}\langle\alpha_1\rangle = \mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle$ for every $\sigma \in \mathfrak{G}$, so that (Chapter III Theorem 2) $\mathfrak{G}(\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle)$ is a normal subgroup of $\mathfrak{G}$ with (Chapter IV §18 Therem 2) factor group isomorphic with the group of all automorphisms of $\mathcal{F}\langle\alpha_1\rangle$ over $\mathcal{F}$, i.e., with the abelian group $\mathfrak{G}_I$ (see §23).

If α_1 is an exponential of an integral of an element of $\mathcal{G}$ then (§23) either $\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle = \mathcal{F}\langle\beta\rangle$, where β is an h^{th} root of an element of $\mathcal{F}$, or $\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle = \mathcal{F}\langle\alpha_1^h\rangle$, for some positive integer h. In the former case $\sigma(\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle) = \mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle$ is obviously true for all $\sigma \in \mathfrak{G}$ so that $\mathfrak{G}(\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle)$ is a normal subgroup of $\mathfrak{G}$ with factor group isomorphic with the group of all automorphisms of $\mathcal{F}\langle\beta\rangle$ over $\mathcal{F}$, i.e., with a cyclic group of finite order. In the latter case, by §23, $\sigma(\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle) = \sigma\mathcal{F}\langle\alpha_1^h\rangle = \mathcal{F}\langle\sigma\alpha_1^h\rangle = \mathcal{F}\langle c^h\alpha_1^h\rangle = \mathcal{F}\langle\alpha_1^h\rangle = \mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle$ for all $\sigma \in \mathfrak{G}$, so that $\mathfrak{G}(\mathcal{G} \cap \mathcal{F}\langle\alpha_1\rangle)$ is a normal subgroup of $\mathfrak{G}$ with factor group isomorphic with the group of all automorphisms of $\mathcal{F}\langle\alpha_1^h\rangle$ over $\mathcal{F}$, i.e. with the abelian group $\mathfrak{G}_E$ (see §23).

If $\mathcal{F}\langle\alpha_1\rangle$ is a normal algebraic extension of $\mathcal{F}$, then all the roots of the

defining equation of α_1 over $\mathcal{F}$ are contained in $\mathcal{F}<\alpha_1>$, so that $\sigma(\mathcal{G} \cap \mathcal{F}<\alpha_1>) = \mathcal{G} \cap \mathcal{F}<\alpha_1>$ for all $\sigma \in \mathfrak{G}$, and $\mathfrak{G}(\mathcal{G} \cap \mathcal{F}<\alpha_1>)$ is a normal subgroup of $\mathfrak{G}$ with factor group isomorphic with the group of all automorphisms of $\mathcal{G} \cap \mathcal{F}<\alpha_1>$ over $\mathcal{F}$, i.e., with a finite group.

Thus, in any case, $\mathfrak{G}$ has a normal chain $\mathfrak{G} \supseteq \mathfrak{G}(\mathcal{G} \cap \mathcal{F}<\alpha_1>) \supseteq \cdots \supseteq \mathfrak{E}$ in which every factor group is abelian or finite.

A glance at the proof reveals, furthermore, that when α_1 is an integral of an element of $\mathcal{F}$ then $\mathfrak{G}/\mathfrak{G}(\mathcal{G} \cap \mathcal{F}<\alpha_1>)$ is not only abelian but also anticompact, when α_1 is an exponential of an integral of an element of $\mathcal{F}$ then $\mathfrak{G}/\mathfrak{G}(\mathcal{G} \cap \mathcal{F}<\alpha_1>)$ is not only abelian but also quasicompact, when α_1 is expressible over $\mathcal{F}$ by means of radicals then $\mathfrak{G}/\mathfrak{G}(\mathcal{G} \cap \mathcal{F}<\alpha_1>)$ is not only finite but also solvable.

It follows, using Theorems 1, 2, and 3 of Chapter I §8, that $\mathfrak{G}^0$ is solvable, and, when the liouvillian extension $\mathcal{F}<\alpha_1, \cdots, \alpha_r>$ is of one of the types (1), $\cdots$, (10), then $\mathfrak{G}$ is an algebraic matric group of the corresponding type.

27. The proof, second half

Now let $\mathfrak{G}$ be an algebraic matric group of one of the ten types introduced above. In the case of type (10) ($\mathfrak{G} = \mathfrak{E}$) it is obvious that $\mathcal{G} = \mathcal{F}$, so that $\mathcal{G}$ is a liouvillian extension of $\mathcal{F}$ of type (10). In the case of type (8) ($\mathfrak{G}$ is finite) then $\mathcal{G}$ is a normal finite algebraic extension of $\mathcal{F}$ with $\mathfrak{G}$ as its Galois group (so that $\mathcal{G}$ is a liouvillian extension of $\mathcal{F}$ of type (8)), and if $\mathfrak{G}$ is moreover solvable (type (9)) then $\mathcal{G}$ is an extension of $\mathcal{F}$ by radicals (a liouvillian extension of $\mathcal{F}$ of type (9)).

Types (1), (2), (3), (4), (5), (6) can be reduced to the cases in which $\mathfrak{G}$ is connected and of type (2), (2), (6), (7), (7), (6), respectively, by observing that if $\mathfrak{G}^0 = \mathfrak{G}(\mathcal{F}^0)$ then $\mathcal{F}^0$ is a normal finite algebraic extension of $\mathcal{F}$ (an extension by radicals when $\mathfrak{G}$ is of type (2), (5), or (6)), and $\mathcal{G}$ is a Picard-Vessiot extension of $\mathcal{F}^0$ such that the group of all automorphisms of $\mathcal{G}$ over $\mathcal{F}^0$ is an algebraic matric group of type (2), (2), (6), (7), (7), (6), in the respective instances.

We consider, then, three cases. Suppose, firstly, that $\mathfrak{G}$ is solvable and anticompact (type (7)). By Chapter I, §7, Theorem 2, $\mathfrak{G}$ is reducible to special triangular form, that is, $L(y)$ has a fundamental system of solutions $\eta_1, \cdots, \eta_n$ in $\mathcal{G} = \mathcal{F}<\eta_1, \cdots, \eta_n>$ such that, for every $\sigma \in \mathfrak{G}$,

$$\sigma\eta_j = \sum_{i=1}^{j} k_{ij}\eta_i, \qquad j = 1, \cdots, n, \tag{10}$$

where each $k_{jj} = 1$. If we divide through all these equations by $\sigma\eta_1 = \eta_1$, and differentiate once, we find

$$\sigma\left(\frac{\eta_j}{\eta_1}\right)' = \sum_{i=2}^{j} k_{ij}\left(\frac{\eta_i}{\eta_1}\right)', \qquad j = 2, \cdots, n.$$

This is a system of relations in the $n - 1$ elements $(\eta_2/\eta_1)', \cdots, (\eta_n/\eta_1)'$ of the same form as the relations (10) in the n elements $\eta_1, \cdots, \eta_n$. Therefore, by making the appropriate induction assumption, we may suppose that $\mathcal{F}<(\eta_2/\eta_1)',$

$\cdots, (\eta_n/\eta_1)'>$ is an extension of $\mathcal{F}$ by integrals. Since, for $j = 2, \cdots, n$, η_j is η_1 (an element of $\mathcal{F}$) multiplied by an integral of $(\eta_j/\eta_1)'$ it follows that $\mathcal{G}$ is an extension of $\mathcal{F}$ by integrals (and therefore a liouvillian extension of $\mathcal{F}$ of type (7)).

Suppose, secondly, that $\mathfrak{G}$ is connected, solvable and quasicompact (type (6)). By Chapter I, §7, Theorems 1 and 3, $\mathfrak{G}$ is reducible to diagonal form. Thus, we may assume that $\eta_1, \cdots, \eta_n$ is a fundamental system of solutions of $L(y)$ such that

$$\sigma\eta_j = k_j\eta_j, \qquad j = 1, \cdots, n,$$

for every $\sigma \in \mathfrak{G}$. It follows that

$$\sigma(\eta_j'/\eta_j) = \eta_j'/\eta_j, \qquad j = 1, \cdots, n,$$

for every $\sigma \in \mathfrak{G}$, so that $\eta_j'/\eta_j \in \mathcal{F}$ $(j = 1, \cdots, n)$, and each η_j is an exponential of an integral of an element of $\mathcal{F}$. In particular, $\mathcal{G}$ is a liouvillian extension of $\mathcal{F}$ of type (6).

Suppose, finally, that $\mathfrak{G}$ is connected and solvable (type (2)). By Chapter I, §7, Theorem 1, we may assume that every $\sigma \in \mathfrak{G}$ satisfies equations of the form (10), where we no longer assume that $k_{jj} = 1$. Dividing through all the equations (10) by $\sigma\eta_1 = k_{11}\eta_1$ and differentiating once, we find that

$$\sigma\left(\frac{\eta_j}{\eta_1}\right)' = \sum_{i=2}^{j} \frac{k_{ij}}{k_{11}}\left(\frac{\eta_i}{\eta_1}\right)', \qquad j = 2, \cdots, n.$$

These are relations in the $n - 1$ elements $(\eta_2/\eta_1)', \cdots, (\eta_n/\eta_1)'$ of the same form as the relations (10) in the n elements $\eta_1, \cdots, \eta_n$. Therefore, by making the appropriate induction assumption, we may suppose that $\mathcal{F}<(\eta_2/\eta_1)', \cdots, (\eta_n/\eta_1)'>$ is an extension of $\mathcal{F}$ by integrals and exponentials of integrals. Since, for $j = 2, \cdots, n$, η_j is η_1 (an exponential of an integral of an element of $\mathcal{F}$) multiplied by an integral of $(\eta_j/\eta_1)'$, it follows that $\mathcal{G}$ is an extension of $\mathcal{F}$ by integrals and exponentials of integrals, and therefore a liouvillian extension of $\mathcal{F}$ of type (2).

References

R. Baer. 1. A note on the status of the Picard-Vessiot theory, included among comments by O. Haupt in Felix Klein's *Vorlesungen über hypergeometrische Funktionen*, Berlin, 1933.

E. Beke. 1. *Die Irreducibilität der homogenen linearen Differentialgleichungen*, Math. Ann., vol. 45 (1894), pp. 278–294.

G. Fano. 1. *Ueber lineare homogene Differentialgleichungen mit algebraischen Relationen zwischen den Fundamentallösungen*, Math. Ann., vol. 53 (1900), pp. 493–590.

H. Freudenthal. 1. *Zur "Galoisschen" Theorie der linearen Differentialgleichungen*, K. Akad. van Wetensch. Amsterdam, Proceedings of the section of Sciences, vol. 34 (1931), pp. 1124–1126.

G. Frobenius. 1. *Ueber den Begriff der Irreducibilität in den Theorie der linearen Differentialgleichungen*, Journal f. d. r. u. a. Math., vol. 76 (1873), pp. 236–270.

E. Gourin. 1. *On irreducible systems of algebraic differential equations*, Bull. Amer. Math. Soc., vol. 39 (1933), pp. 593–595.

E. R. KOLCHIN. 1. *On the exponents of differential ideals*, Ann. of Math., (2) vol. 42 (1941), pp. 740–777.
2. *On the basis theorem for differential systems*, Trans. Amer. Math. Soc., vol. 52 (1942), pp. 115–127.
3. *Extensions of differential fields, I*, Ann. of Math., (2) vol. 43 (1942), pp. 724–729.
4. *Extensions of differential fields, III*, Bull. Amer. Math. Soc., vol. 53 (1947), pp. 397–401.

W. KRULL. 1. *Galoissche Theorie der unendlichen algebraischen Erweiterungen*, Math. Ann., vol. 100 (1928), pp. 687–698.

A. LOEWY. 1. *Ueber die irreduciblen Factoren eines linearen homogenen Differentialausdrückes*, Ber. über die Verh. der Königlich Sächsischen Gesellschaft der Wissenschaften zu Leipzig, Math.-phys. Kl., vol. 51 (1902), pp. 1–13.
2. *Über reduzible lineare homogene Differentialgleichungen*, Math. Ann., vol. 56 (1902), pp. 549–584.
3. *Über die Adjunktion von Integralen linearer homogener Differentialgleichungen*, Math. Ann., vol. 59 (1904), pp. 435–448.
4. *Die Rationalitätsgruppe einer linearen homogenen Differentialgleichungen*, Math. Ann., vol. 65 (1908), pp. 129–160.
5. *Über die Irreduzibilität der linearen homogenen Substitutsionsgruppen und Differentialgleichungen*, Math. Ann., vol. 70 (1911), pp. 94–109.

F. MAROTTE. 1. *Les équations différentielles linéaires et la théorie des groupes*, Ann. de la Fac. des Sci. de Toulouse, (1) vol. 12 (1898), pp. H1–H92.

É. PICARD. 1. *Sur les groupes de transformation des équations différentielles linéaires*, Comptes rendus, Paris, vol. 96 (1883), pp. 1131–1134.
2. *Sur les équations différentielles linéaires et les groupes algébriques de transformations*, Ann. de la Fac. des Sci. de Toulouse, (1) vol. 1 (1887), pp. A1–A15.
3. *Sur les groupes de transformations des équations différentielles linéaires*, Comptes rendus, Paris, vol. 119 (1894), pp. 584–589 or Math. Ann., vol. 46 (1895), pp. 161–166.
4. *Sur l'extension des idées de Galois à la théorie des équations différentielles*, Comptes rendus, Paris, vol. 121 (1895), pp. 789–792 or Math. Ann., vol. 47 (1896), pp. 155–156.
5. *Traité d'Analyse*, vol. 3, chapter 17, Paris, 1898 or 1908 or 1928 (reprinted as *Analogies entre la théorie des équations différentielles linéaires et la théorie des equations algébriques*, Paris, 1936).

H. W. RAUDENBUSH. 1. *Ideal theory and algebraic differential equations*, Trans. Amer. Math. Soc., vol. 36 (1934), pp. 361–368.

J. F. RITT. 1. *Differential equations from the algebraic standpoint*, Amer. Math. Soc. Colloq. Publications, vol. 14, New York, 1932.
2. *Algebraic aspects of the theory of differential equations*, Amer. Math. Soc. Semicentennial Publications, vol. 2 (1938), pp. 35–55.

E. VESSIOT. 1. *Sur les équations différentielles linéaires*, Comptes rendus, Paris, vol. 112 (1891), pp. 778–780.
2. *Sur les intégrations des équations différentielles linéaires*, Ann. Sci. de l'École Norm. Sup., (3) vol. 9 (1892), pp. 192–280.
3. *Methodes d'intégration elémentaires*, Encyclopédie des sci. math. pures et appliquées, tome II, vol. 3, fascicule 1 (1910), pp. 58–170 (esp. pp. 152–165).

B. L. VAN DER WAERDEN. 1. *Moderne Algebra*; vol. I, Berlin, 1937; vol. II, Berlin, 1940.

HERMANN WEYL. 1. *The classical groups*, Princeton, 1939.

HANS ZASSENHAUS. 1. *Lehrbuch der Gruppentheorie*, vol. 1, Leipzig and Berlin, 1937.

COLUMBIA UNIVERSITY