LOWEST ORDER EQUATION FOR ZEROS OF A HOMOGENEOUS LINEAR DIFFERENTIAL POLYNOMIAL

BY

LAWRENCE GOLDMAN

Introduction

If $\mathfrak{F}$ is a field and x belongs to an algebraic extension of $\mathfrak{F}$, then the algebraic properties of x are completely determined by the irreducible polynomial over $\mathfrak{F}$ which vanishes at x. Similarly, if $\mathfrak{F}$ is an ordinary differential field (i.e., a field with given derivation) of characteristic zero and x belongs to a differentially algebraic differential field extension of $\mathfrak{F}$, the differential algebraic properties of x are completely determined by the irreducible differential polynomial $F(y) \in \mathfrak{F}\{y\}$ of lowest order which vanishes at x. We shall call $F(y)$, which is unique up to a nonzero factor in $\mathfrak{F}$, the *lowest differential polynomial* of x over $\mathfrak{F}$, and we shall call the differential equation $F(y) = 0$ the *lowest equation* for x over $\mathfrak{F}$.

Let $\mathfrak{F}$ be an ordinary differential field of characteristic zero, and let C, the field of constants of $\mathfrak{F}$, be algebraically closed. Let $(x_1, \cdots, x_n)$ be a fundamental system of zeros of a homogeneous linear differential polynomial $L_n(y) \in \mathfrak{F}\{y\}$ such that the field of constants of $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ is C. $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ is called a Picard-Vessiot extension of $\mathfrak{F}$ (hereafter denoted by P.V.E.), and the group G of automorphisms of $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ over $\mathfrak{F}$ can be identified with an algebraic group of linear transformations of the vector space V_n over C with basis $(x_1, \cdots, x_n)$. (See [3].) We sometimes call G the group of $L_n(y)$ over $\mathfrak{F}$.

It is the purpose of this paper to obtain information about G when the lowest equation over $\mathfrak{F}$ for some $x \in V_n$ is known, and about the lowest equation for every $x \in V_n$ when G is one of the classical groups.

Notation. Throughout this paper $\mathfrak{F}$ will stand for an ordinary differential field of characteristic zero whose field of constants C is algebraically closed. $L_n(y)$ will always stand for a homogeneous linear differential polynomial of order n. Whenever we speak of zeros of $L_n(y) \in \mathfrak{F}\{y\}$, we restrict ourselves to zeros which belong to a P.V.E. of $\mathfrak{F}$. We shall therefore be able to say, for some $L_n(y) \in \mathfrak{F}\{y\}$, that every one of its zeros satisfies a differential equation over $\mathfrak{F}$ of lower order. If, for a given $L_n(y) \in \mathfrak{F}\{y\}$, there exist an integer r and $L_r(y)$, $L_{n-r}(y) \in \mathfrak{F}\{y\}$ such that $1 \leqq r \leqq n - 1$ and

$$L_n(y) = L_{n-r}(L_r(y)),$$

we say that $L_n(y)$ is *composite* over $\mathfrak{F}$, that $L_n(y)$ is *the composite* of $L_r(y)$ and $L_{n-r}(y)$, and that $L_n(y)$ is *decomposable* by $L_r(y)$ on the *right*. If an

Received September 3, 1957.

element x of an extension of $\mathfrak{F}$ has a lowest equation over $\mathfrak{F}$ which is of order r, we shall say that x is of order r over $\mathfrak{F}$.

We repeatedly make use of the following:

(A) If $F(y)$ is the lowest differential polynomial of x over $\mathfrak{F}$, then x is a generic zero of the general component of $F(y)$ over $\mathfrak{F}$, and the transcendence degree of $\mathfrak{F}\langle x\rangle$ over $\mathfrak{F}$ equals the order of x over $\mathfrak{F}$. For any $P(y) \in \mathfrak{F}\{y\}$ vanishing at x there exists a natural number t such that $S^tP \in [F]$, where S is the separant of F; if the order of P equals that of F, then P is divisible by F. (See [4].)

(B) If G is the algebraic group of $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ over $\mathfrak{F}$, where $(x_1, \cdots, x_n)$ is a fundamental system of zeros of $L_n(y) \in \mathfrak{F}\{y\}$, then the dimension of G equals the transcendence degree of $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ over $\mathfrak{F}$. If G_0 is the component of the identity of G, then G_0 is the group of $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ over the (relative) algebraic closure $\mathfrak{F}_0$ of $\mathfrak{F}$ in $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$, and also of $\mathfrak{F}_1\langle x_1, \cdots, x_n\rangle$ over $\mathfrak{F}_1$, where $\mathfrak{F}_1$ is the (absolute) algebraic closure of $\mathfrak{F}$. G is reducible (maps a nontrivial proper subspace of V_n into itself) if and only if $L_n(y)$ is composite over $\mathfrak{F}$. G_0 is reducible to triangular form if and only if G_0 is solvable. (See [3].)

(C) If the dimension of G is $\leqq 2$, then G_0 is solvable.

(B) and (C) imply (D).

(D) If the transcendence degree of $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ over $\mathfrak{F}$ is $\leqq 2$, then $L_n(y)$ is the composite of n homogeneous linear differential polynomials of order 1 in $\mathfrak{F}_0\{y\}$, $\mathfrak{F}_0$ denoting the algebraic closure of $\mathfrak{F}$ in $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$.

(E) If G is irreducible and a nontrivial zero x of $L_n(y)$ is a zero of $F(y)$, then there exists a fundamental system of zeros of $L_n(y)$ consisting of zeros of $F(y)$.

(F) If $L_n(y) = L_{n-r}(L_r(y))$ and $(x_1, \cdots, x_n)$ is a fundamental system of zeros of $L_n(y)$ such that $(x_1, \cdots, x_r)$ is a fundamental system of zeros of $L_r(y)$, then $(L_r(x_{r+1}), \cdots, L_r(x_n))$ is a fundamental system of zeros of $L_{n-r}(y)$.

1. Homogeneous elements

Definition. An element x in a differential field extension of $\mathfrak{F}$ is said to be homogeneous over $\mathfrak{F}$ if x is differentially algebraic over $\mathfrak{F}$ and $x \to cx$ is a specialization over $\mathfrak{F}$, where c is a transcendental constant over $\mathfrak{F}\langle x\rangle$.

Lemma 1. *A necessary and sufficient condition for x to be homogeneous over $\mathfrak{F}$ is that the lowest equation for x over $\mathfrak{F}$ be homogeneous.*

Proof. Let $F(y)$ be the lowest differential polynomial of x. Suppose x

homogeneous over $\mathfrak{F}$. Then $F(cx) = 0 = \sum_{i=0}^{m} c^i F_i(x)$, where F_i is homogeneous of degree i. Since c is transcendental over $\mathfrak{F}\langle x\rangle$,

$$F_i(x) = 0 \qquad (i = 0, 1, \cdots, m),$$

so that each F_i is a multiple of F, which is possible only if F is homogeneous. Suppose $F(y)$ is homogeneous. Then $F(cx) = c^m F(x) = 0$. If $P(y) \in \mathfrak{F}\{y\}$ is any differential polynomial such that $P(x) = 0$, then $S^t P(y) \in [F(y)]$, where S is the separant of F. Since $S(cx) = c^{m-1}S(x) \neq 0$, $P(cx) = 0$ and $x \to cx$ is a specialization over $\mathfrak{F}$, and x is homogeneous over $\mathfrak{F}$.

2. Decomposition of $L_n(y)$

THEOREM 1. *Let x be a zero of $L_n(y) \in \mathfrak{F}\{y\}$ of order r over $\mathfrak{F}$, let $F(y)$ be the lowest differential polynomial of x over $\mathfrak{F}$, and let*

$$L_r(y) = \sum_{j=0}^{r} \frac{\partial F}{\partial y^{(j)}}(x) y^{(j)}.$$

(a) *There exists an $L_{n-r}(y) \in \mathfrak{F}\langle x\rangle\{y\}$ such that $L_n(y) = L_{n-r}(L_r(y))$.*

(b) *x is a zero of $L_r(y)$ if and only if x is homogeneous over $\mathfrak{F}$.*

(c) *If $(u_1, \cdots, u_{n-r})$ is a fundamental system of zeros of $L_{n-r}(y)$ and $K(y)$ is the sum of the terms of $F(y)$ of highest degree, then every zero of $L_r(y)$ which is homogeneous over $\mathfrak{F}\langle x, u_1, \cdots, u_{n-r}\rangle$ is a zero of $K(y)$.*

Proof. Let $F(y)$ be of degree m, and let $v = x + z = x + \sum_{i=1}^{\infty} z_i e^i$ (formal power series) where the z_i, $1 \leqq i < \infty$, are in some differential field extension of $\mathfrak{F}$ and e is a transcendental constant over $\mathfrak{F}\langle x, (z_i)_{1 \leqq i < \infty}\rangle$. v is a zero of $F(y)$ if and only if $F(v)$, when written as a power series in e, vanishes identically in e.

$$F(v) = F(x) + \left(\sum_{k=1}^{m} \frac{1}{k!}\left(\sum_{j=0}^{r} z^{(j)} \frac{\partial}{\partial y^{(j)}}\right)^k F(y)\right)_{y=x}$$
$$= \sum_{s=1}^{\infty} (L_r(z_s) + Q_s(z_1, \cdots z_{s-1}))e^s,$$

where

$$Q_1 = 0$$

and

$$Q_s \in \mathfrak{F}\{x, z_1, \cdots, z_{s-1}\}, \qquad 1 \leqq s < \infty;$$

$L_r(y)$ is of order r, for $(\partial F/\partial y^{(r)})(x) \neq 0$. If we choose the z_s, successively, to be zeros of

$$L_r(y) + Q_s(z_1, \cdots, z_{s-1}),$$

v will be a zero of $F(y)$. Now x is a specialization of v over $\mathfrak{F}$. Since x is of order r, v must also be of order r. Therefore $v \to x$ is a generic specialization over $\mathfrak{F}$ and $L_n(v) = 0$. Since $L_n(y)$ is linear, $L_n(v) = \sum_{i=1}^{\infty} L_n(z_i)e^i = 0$, so that $L_n(z_i) = 0$, $1 \leqq i < \infty$. Since we may choose z_1 to be any zero of $L_r(y)$, any zero of $L_r(y)$ must be a zero of $L_n(y)$, so that

$$L_n(y) = L_{n-r}(L_r(y)) \qquad \text{with} \qquad L_{n-r}(y) \in \mathfrak{F}\langle x\rangle\{y\}.$$

To prove (b) note that if $F(y)$ is homogeneous then the differential polynomial $P(y) = \sum_{j=0}^{r} y^{(j)}\partial F/\partial y^{(j)}$ equals $mF(y)$. Conversely, if $L_r(x) = 0$, x is a zero of $P(y) \in \mathfrak{F}\{y\}$, and consequently $P(y) = aF(y)$, $a \in \mathfrak{F}$. Equating coefficients we see that a is an integer, and by Euler's theorem $F(y)$ is homogeneous.

To prove (c) we note that, for $1 < s \leqq m$,

$$Q_s = \left(\frac{1}{s!}\left(\sum_{j=0}^{r} z_1^{(j)} \frac{\partial}{\partial y^{(j)}}\right)^s F(y)\right)_{y=x}$$

plus terms all of which have at least one factor $z_i^{(j)}$ with $1 < i < s$ and $0 \leqq j \leqq r$. Let w be any zero of $L_r(y)$ which is homogeneous over $\mathfrak{F}\langle x, u_1, \cdots, u_{n-r}\rangle$. Let $z_1 = w$ and suppose that

$$\left(\left(\sum_{j=0}^{r} w^{(j)} \frac{\partial}{\partial y^{(j)}}\right)^s F(y)\right)_{y=x} = 0, \qquad 1 < s < t,$$

where t is a natural number $\leqq m$, while

$$\left(\left(\sum_{j=0}^{r} w^{(j)} \frac{\partial}{\partial y^{(j)}}\right)^t F(y)\right)_{y=x} \neq 0.$$

Then we may set, successively, $z_s = 0$ for $1 < s < t$, and z_t a solution of

$$L_r(y) = -\left(\left(\sum_{j=0}^{r} w^{(j)} \frac{\partial}{\partial y^{(j)}}\right)^t F(y)\right)_{y=x}. \tag{1}$$

Since $L_n(z_t) = 0$, $L_r(z_t)$ is a zero of $L_{n-r}(y)$ and $L_r(z_t) \in \mathfrak{F}\langle x, u_1, \cdots, u_{n-r}\rangle$. Now the specialization $w \to cw$ over $\mathfrak{F}\langle x, u_1, \cdots, u_{n-r}\rangle$ leaves the left-hand side of (1) invariant while it multiplies the right-hand side of (1) by c^t, which is impossible. Hence

$$\left(\left(\sum_{j=0}^{r} w^{(j)} \frac{\partial}{\partial y^{(j)}}\right)^s F(y)\right)_{y=x} = 0, \qquad 1 < s \leqq m.$$

Since

$$\left(\left(\sum_{j=0}^{r} y^{(j)} \frac{\partial}{\partial y^{(j)}}\right)^m F(y)\right)_{y=x} = m!\, K(y),$$

we see that w is a zero of $K(y)$.

COROLLARY 1. *With notation and hypotheses as in Theorem 1, let $L_r(y)$ have a zero of order r over $\mathfrak{F}\langle x, u_1, \cdots, u_{n-r}\rangle$, and set $L_r^*(y) = (\partial F/\partial y^{(r)})^{-1}L_r(y)$. The coefficients of $L_r^*(y)$ are algebraic over $\mathfrak{F}$, and $K(y)$ is divisible by $L_r^*(y)$.*

Proof. Let w be a zero of $L_r(y)$ of order r over $\mathfrak{F}\langle x, u_1, \cdots, u_{n-r}\rangle$. Then w is homogeneous over $\mathfrak{F}\langle x, u_1, \cdots, u_{n-r}\rangle$ and, by Theorem 1, w is a zero of $K(y)$. Since the order of $K(y)$ is $\leqq r$, $K(y)$ is divisible by $L_r(y)$ and therefore by $L_r^*(y)$; because one of the coefficients in the latter is 1 and the coefficients in $K(y)$ all belong to $\mathfrak{F}$, all the coefficients in $L_r^*(y)$ are algebraic over $\mathfrak{F}$.

Remark. It is well known (e.g. see [2]) that if an $L_2(y) \in \mathfrak{F}\{y\}$ has a nontrivial zero of order $\leqq 1$ over $\mathfrak{F}$ then $L_2(y)$ is composite over an algebraic extension of $\mathfrak{F}$. Indeed, if $L_2(y)$ is not composite over $\mathfrak{F}$, and if $F(y)$ denotes the lowest differential polynomial of x over $\mathfrak{F}$, then $L_2(y)$ has a fundamental system of zeros (v_1, v_2) consisting of zeros of $F(y)$; as the transcendence degree of $\mathfrak{F}\langle v_1, v_2\rangle$ over $\mathfrak{F}$ is then $\leqq 2$, $L_2(y)$ is composite over an algebraic extension of $\mathfrak{F}$.

COROLLARY 2. *If $L_3(y) \in \mathfrak{F}\{y\}$ has a nontrivial zero of order $\leqq 1$ over $\mathfrak{F}$, then $L_3(y)$ is decomposable on the right by a homogeneous linear differemtial polynomial of order* 1 *with coefficients which are algebraic over $\mathfrak{F}$.*

Proof. Let x be a nontrivial zero of $L_3(y)$ of order $\leqq 1$ over $\mathfrak{F}$; denote the lowest differential polynomial of x over $\mathfrak{F}$ by F, and set

$$L_1(y) = \sum_{j=0}^{1} (\partial F/\partial y^{(j)})(x)y^{(j)}.$$

As $L_3(y)$ is decomposable on the right by $y' - (x'/x)y$, we may suppose that x'/x is not algebraic over $\mathfrak{F}$, so that F is of order 1 and not homogeneous. By Theorem 1 we may write $L_3(y) = L_2(L_1(y))$, with $L_2(y) \in \mathfrak{F}\langle x\rangle\{y\}$, and $L_1(x) \neq 0$. Let w be a nontrivial zero of $L_1(y)$. By the remark preceding the present corollary, we may suppose that x is not a zero of any homogeneous linear differential polynomial in $\mathfrak{F}\{y\}$ of order 2. It easily follows that $F(y)$ has a zero v such that (x, v, w) is a fundamental system of zeros of $L_3(y)$. Obviously $(L_1(x), L_1(v))$ is a fundamental system of zeros of $L_2(y)$. If w is of order 0 over $\mathfrak{F}\langle x, L_1(v)\rangle$, then the transcendence degree of $\mathfrak{F}\langle x, v, w\rangle$ over $\mathfrak{F}$ is $\leqq 2$, and our result follows from (D) of the introduction. If w is of order 1 over $\mathfrak{F}\langle x, L_1(v)\rangle$, then, by Corollary 1, the coefficients in

$$L_1^*(y) = (\partial F/\partial y'(x))^{-1}L_1(y)$$

are algebraic over $\mathfrak{F}$, and obviously $L_3(y)$ is decomposable by $L_1^*(y)$ on the right.

3. Dimension of G

A group of linear transformations of an n-dimensional vector space is said to be reducible to diagonal form if the space is a direct sum of n invariant one-dimensional subspaces. We shall say, for any divisor r of n, that the group is reducible to *r-diagonal* form, if the space is a direct sum of n/r invariant r-dimensional subspaces.

THEOREM 2. *Let $L_n(y) \in \mathfrak{F}\{y\}$, and suppose that the group G of $L_n(y)$ over $\mathfrak{F}$ is irreducible. If $L_n(y)$ has a nontrivial zero x of order r over $\mathfrak{F}$, then either* *the dimension of G is $\leqq (n-1)r$, or the dimension of G is $(n-1)r+1$ and x is homogeneous over $\mathfrak{F}$, or r divides n and the component of the identity G_0 of G is reducible to r-diagonal form.*

Proof. Let V_n denote the vector space over C formed by the zeros of $L_n(y)$, and let x be an element of V_n of order r over $\mathfrak{F}$. Using the notation of Theorem 1, we may write $L_n(y) = L_{n-r}(L_r(y))$. Suppose $L_r(y)$ has a nontrivial zero w of order r over $\mathfrak{F}\langle x, u_1, \cdots, u_{n-r}\rangle$, where $(u_1, \cdots, u_{n-r})$ is some fundamental system of zeros of $L_{n-r}(y)$; then the coefficients in the differential polynomial $L_r^*(y)$ of Corollary 1 to Theorem 1 are algebraic over $\mathfrak{F}$, so that $L_r^*(y) \in \mathfrak{F}_0\{y\}$, where $\mathfrak{F}_0$ is the algebraic closure of $\mathfrak{F}$ in $\mathfrak{F}\langle V_n\rangle$, whence $gL_r^*(y) \in \mathfrak{F}_0\{y\}$ for every $g \in G_0$. Denoting the set of zeros of $L_r^*(y)$ by V_r, we see that gV_r, which is the set of zeros of $gL_r^*(y)$, is an r-dimensional subspace of V_n invariant under G_0. If V_r contains a nontrivial proper subspace invariant under G_0, then $L_n(y)$ has a nontrivial zero of order $< r$ over $\mathfrak{F}_0$ and therefore over $\mathfrak{F}$, so that (because G is irreducible) V_n has a basis consisting of such zeros, and the transcendence degree of $\mathfrak{F}\langle V_n\rangle$ over $\mathfrak{F}$, that is, the dimension of G, is $\leqq n(r-1) \leqq (n-1)r$; on the other hand, if V_r (and therefore each gV_r) contains no such invariant subspace, then V_n, which because of the irreducibility of G is the sum of the subspaces gV_r, is the direct sum of certain of them, whence r divides n and G_0 is reducible to r-diagonal form.

Suppose, then, that $L_r(y)$ has no nontrivial zero w as above. By Theorem 1 and the irreducibility of G there exists a fundamental system of zeros, $(x_1, \cdots, x_{n-r}, w_1, \cdots, w_r)$ of $L_n(y)$, such that each $F(x_i) = 0$, $(w_1, \cdots, w_r)$ is a fundamental system of zeros of $L_r(y)$, and either x is not homogeneous over $\mathfrak{F}$ and $x = x_1$, or x is homogeneous over $\mathfrak{F}$ and $x = w_1$. Since

$$(L_r(x_1), \cdots, L_r(x_{n-r}))$$

is a fundamental system of zeros of $L_{n-r}(y)$, the order of w_i, for each i with $1 \leqq i \leqq r$ in the nonhomogeneous case and for each i with $2 \leqq i \leqq r$ in the homogeneous case, over

$$\mathfrak{F}\langle x, L_r(x_1), \cdots, L_r(x_{n-r})\rangle \subset \mathfrak{F}\langle x, x_1, \cdots, x_{n-r}\rangle,$$

is $< r$. As x and each x_j have order $\leqq r$ over $\mathfrak{F}$, the transcendence degree of $\mathfrak{F}\langle x_1, \cdots, x_{n-r}, w_1, \cdots, w_r\rangle$ over $\mathfrak{F}$ is $\leqq (n-r)r + r(r-1) = (n-1)r$ in the nonhomogeneous case and is $\leqq (n-r+1)r + (r-1)^2 = (n-1)r+1$ in the homogeneous case.

COROLLARY 1. *Let G be an irreducible algebraic group of linear transformations of an n-dimensional vector space V over an algebraically closed field of characteristic zero, let H be the subgroup of G leaving invariant a fixed nonzero element $v \in V$, and denote the dimension of G and H by s and t respectively. Then, either $s-t=n$, or $s-t<n$ and $s-t$ divides n and the component of the identity G_0 is reducible to $(s-t)$-diagonal form, or*

$$(s-1)/(n-1) \leqq s-t < n.$$

Proof. It is known (see e.g. [3]) that we may regard V as the space of zeros of some $L_n(y) \in \mathfrak{F}\{y\}$ with group G; then s equals t plus the order of v over $\mathfrak{F}$, so that $s - t \leqq n$. If $s - t < n$, then by Theorem 2 either

$$s \leqq (n - 1)(s - t) + 1,$$

that is, $s - t \geqq (s - 1)/(n - 1)$, or else $s - t$ divides n and G_0 is reducible to $(s - t)$-diagonal form.

COROLLARY 2. *Let G be an irreducible algebraic group of linear transformations of an n-dimensional vector space V over an algebraically closed field of characteristic zero, and suppose that the component of the identity G_0 leaves invariant an r-dimensional subspace of V, $0 < r < n$. Then either the dimension of G is $\leqq (n - 1)r + 1$, or else r divides n and G_0 is reducible to r-diagonal form.*

Proof. As in the proof of Corollary 1, we may suppose that V is the space of zeros of some $L_n(y) \in \mathfrak{F}\{y\}$ with group G. If there exists a nontrivial zero v of $L_n(y)$ such that order of v over $\mathfrak{F}$ is $< r$, it follows from the irreducibility of G that the dimension of G is $\leqq n(r - 1) \leqq (n - 1)r + 1$. Since G_0 leaves invariant an r-dimensional subspace of V, $L_n(y)$ has a nontrivial zero v such that the order of v over F is r, and the conclusion follows from Theorem 2.

4. Transitivity of G

LEMMA 2. *Let $L_n(y) \in \mathfrak{F}\{y\}$. A necessary and sufficient condition that every nontrivial zero of $L_n(y)$ be of order n over $\mathfrak{F}$ is that the group G of $L_n(y)$ over $\mathfrak{F}$ operate transitively on the space of zeros of $L_n(y)$.*

Proof. Let every zero of $L_n(y)$ be of order n over $\mathfrak{F}$. Then every nontrivial zero is a generic zero of the prime differential ideal $[L_n(y)]$. Hence given any two nontrivial zeros u, v of $L_n(y)$, there exists an automorphism $g \in G$ such that $g(u) = v$. Therefore G is transitive.

Conversely, let G be transitive, and let x be any nontrivial zero of $L_n(y)$. Every $F(y) \in \mathfrak{F}\{y\}$ vanishing at x must vanish at every zero of $L_n(y)$ and therefore belongs to $[L_n(y)]$; every such $F(y)$ has order $\geqq n$ so that the order of x over $\mathfrak{F}$ is n.

COROLLARY. *Let the group of $L_n(y)$ over $\mathfrak{F}$ be either the general linear group $GL_n(C)$, the unimodular group $SL_n(C)$ ($n \geqq 2$), or the symplectic group $Sp_n(C)$ (n even). Then $L_n(y)$ is the lowest differential polynomial over $\mathfrak{F}$ of each of its nontrivial zeros.*

5. The orthogonal group

THEOREM 3. *Let $L_n(y) \in \mathfrak{F}\{y\}$, suppose the coefficient of $y^{(n)}$ in $L_n(y)$ is 1, and let $F(y)$ be the lowest differential polynomial over $\mathfrak{F}$ of a nontrivial zero of $L_n(y)$ of order $n - 1$ over $\mathfrak{F}$. There exists $p \in \mathfrak{F}$ such that*

$$(\partial F/\partial y^{(n-1)})L_n = F' + pF.$$

If F_i denotes the homogeneous part of F of degree i, then, for every i for which

$F_i \neq 0$, each irreducible factor of F_i is of order $n - 1$, and every nonsingular zero of such a factor is a zero of L_n; if $c_i \in C$ and $\sum c_i F_i \neq 0$, then every nonsingular zero of $\sum c_i F_i$ is a zero of L_n.

Proof. Let x be a nontrivial zero of $L_n(y)$ of order $n - 1$ over $\mathfrak{F}$ having $F(y)$ as lowest differential polynomial over $\mathfrak{F}$. $(\partial F/\partial y^{(n-1)})L_n - F'$ vanishes at x and obviously has order $\leqq n - 1$, and therefore is divisible by F; consideration of degrees shows that $(\partial F/\partial y^{(n-1)})L_n - F' = pF$ with $p \in \mathfrak{F}$. It immediately follows that

$$(\partial F_i/\partial y^{(n-1)})L_n = F_i' + pF_i$$

for each i. Suppose $F_i \neq 0$, let Q be an irreducible factor of F_i, and write $F_i = Q^t P$ with P not divisible by Q. If the order of Q were less than $n - 1$, the above equation would show that Q' is divisible by Q, which is impossible as Q' has the same degree as Q but higher order. The same equation then shows that

$$(t(\partial Q/\partial y^{(n-1)})P + Q(\partial P/\partial y^{(n-1)}))L_n = tQ'P + QP' + pQP;$$

it follows that a generic point over $\mathfrak{F}$ of the general manifold of Q over $\mathfrak{F}$ is a zero of L_n, so that every nonsingular zero of Q is a zero of L_n. Finally, again by the same equation,

$$(\partial(\sum c_i F_i)/\partial y^{(n-1)})L_n = (\sum c_i F_i)' + p\sum c_i F_i,$$

so that every zero of $\sum c_i F_i$ which is not a zero of $\partial(\sum c_i F_i)/\partial y^{(n-1)}$ is a zero of L_n.

THEOREM 4. *Let $L_n(y) \in \mathfrak{F}\{y\}$, and suppose that the group of $L_n(y)$ over $\mathfrak{F}$ is the orthogonal group $O_n(C)$, $n \geqq 2$. Then there exists an irreducible nonzero homogeneous differential polynomial $Q(y) \in \mathfrak{F}\{y\}$ of degree 2 and order $n - 1$ such that, for every nontrivial zero x of $L_n(y)$, $Q(x) \in C$ and $Q(y) - Q(x)$ is the lowest differential polynomial of x over $\mathfrak{F}$.*

Proof.[1] By hypothesis there exists a fundamental system of zeros $(x_1, \cdots, x_n)$ of $L_n(y)$ such that the equations

$$gx_j = \sum_{1 \leqq i \leqq n} a_{ij} x_i, \qquad 1 \leqq j \leqq n, \quad g \in G,$$

establish an isomorphism of the group of automorphisms G of $\mathfrak{F}\langle x_1, \cdots, x_n\rangle$ over $\mathfrak{F}$ onto the group $O_n(C)$ of orthogonal matrices (a_{ij}) with coefficients in C. For the matrix

$$(x_j^{(i-1)})_{1 \leqq i \leqq n, 1 \leqq j \leqq n}$$

we obviously have $(gx_j^{(i-1)}) = (x_j^{(i-1)})(a_{ij})$, so that if we denote the inverse of (x_j^{i-1}) by (w_{ij}) then $(gw_{ij}) = (a_{ij})^{-1}(w_{ij}) = {}^t(a_{ij})(w_{ij})$. It follows that if we set $(q_{ij}) = {}^t(w_{ij})(w_{ij})$ then

$$(gq_{ij}) = {}^t(w_{ij})(a_{ij})\, {}^t(a_{ij})(w_{ij}) = (q_{ij}),$$

so that $q_{ij} \in \mathfrak{F}$, and also $q_{ij} = q_{ji}$.

[1] This proof was conveyed to me by E. R. Kolchin.

Define the differential polynomial $B(y, z) \in \mathfrak{F}\{y, z\}$ by the formula

$$B(y, z) = \sum_{1 \leqq i \leqq n, 1 \leqq j \leqq n} q_{ij}\, y^{(i-1)} z^{(j-1)}.$$

For any zeros u, v of $L_n(y)$ we may write $u = \sum c_h x_h$, $v = \sum d_k x_k$, where each c_h and d_k is an element of C; clearly $u^{(i-1)} = \sum c_h x_h^{(i-1)}$, so that $c_h = \sum_i w_{hi} u^{(i-1)}$, and similarly $d_k = \sum_j w_{kj} v^{(j-1)}$. Thus

$$c_h d_h = \sum_{i,j} w_{hi} w_{hj} u^{(i-1)} v^{(j-1)},$$

whence $\sum_h c_h d_h = \sum q_{ij} u^{(i-1)} v^{(j-1)}$, so that $B(u, v) = \sum c_i d_i$. Defining the differential polynomial $Q(y) \in \mathfrak{F}\{y\}$ by the formula $Q(y) = B(y, y)$, we see that for every zero $u = \sum c_i x_i$ of $L_n(y)$, $Q(u) = \sum c_i^2 \in C$.

We now show that every nontrivial zero u of $L_n(y)$ is of order $n - 1$ over $\mathfrak{F}$. Indeed, if $Q(u) \neq 0$, the set of all solutions v of $L_n(y)$ with $B(u, v) = 0$ is an $(n - 1)$-dimensional vector space over C not containing u; the group pf $L_n(y)$ over $\mathfrak{F}\langle u \rangle$ is obviously isomorphic with $O_{n-1}(C)$ and therefore is of dimension $\frac{1}{2}(n - 1)(n - 2)$, so that the order of u over $\mathfrak{F}$ is equal to

$$\tfrac{1}{2}n(n - 1) - \tfrac{1}{2}(n - 1)(n - 2) = n - 1.$$

On the other hand, if $Q(u) = 0$, then u, $x_1 + \sqrt{(-1)}x_2$, $x_1 - \sqrt{(-1)}x_2$ all have the same order over $\mathfrak{F}$. For if u, v are any two nontrivial zeros of $L_n(y)$ such that $Q(u) = Q(v) = 0$, there exists an automorphism of

$$\mathfrak{F}\langle x_1, \cdots, x_n \rangle$$

over $\mathfrak{F}$ which maps u onto v (e.g., see [1] Proposition 5, p. 18). Since the group of $L_n(y)$ over $\mathfrak{F}\langle x_1 + \sqrt{(-1)}x_2, x_1 - \sqrt{(-1)}x_2 \rangle$ is $O_{n-2}(C)$ and is thus of dimension $\frac{1}{2}(n - 2)(n - 3)$, we conclude that the transcendence degree of $\mathfrak{F}\langle x_1 + \sqrt{(-1)}x_2, x_1 - \sqrt{(-1)}x_2 \rangle$ over $\mathfrak{F}$ is equal to

$$\tfrac{1}{2}n(n - 1) - \tfrac{1}{2}(n - 2)(n - 3) = 2n - 3.$$

If the order of u over $\mathfrak{F}$ were $\leqq n - 2$, then the transcendence degree of

$$\mathfrak{F}\langle x_1 + \sqrt{(-1)}x_2, x_1 - \sqrt{(-1)}x_2 \rangle$$

over $\mathfrak{F}$ would be $\leqq 2n - 4$. Therefore u is of order $n - 1$ over $\mathfrak{F}$.

This being the case, since $Q(y)$ has order $\leqq n - 1$ and vanishes at the zero $x_1 + \sqrt{(-1)}x_2$ of $L_n(y)$, the order of $Q(y)$ must be $n - 1$. If $Q(y)$ were reducible over $\mathfrak{F}$, one of its irreducible factors $L_{n-1}(y)$ would vanish at the nontrivial zero $x_1 + \sqrt{(-1)}x_2$ of $L_n(y)$, which is impossible since $O_n(C)$ is irreducible.

Remark. If $n \geqq 3$, the same theorem holds for the proper orthogonal group $O_n^+(C)$ (same proof). If $n = 2$, then $Q(y)$ is no longer irreducible, as then

$$Q(y) = (x_1 x_2' - x_2 x_1')^{-2}(x_1^2 + x_2^2) A_+(y) A_-(y),$$

where

$$A_\pm(y) = y' - (x_1^2 + x_2^2)^{-1}(x_1 x_1' + x_2 x_2' \pm \sqrt{(-1)}(x_1 x_2' - x_2 x_1'))y_2 .$$

For a zero x of $L_2(y)$ such that $Q(x) \neq 0$ the lowest differential polynomial over $\mathfrak{F}$ is still $Q(y) - Q(x)$, but for an x such that $Q(x) = 0$ the lowest differential polynomial over $\mathfrak{F}$ is one of the two linear factors $A_{\pm}(y)$ of $Q(y)$.

REFERENCES

1. J. DIEUDONNÉ, *Sur les groupes classiques*, Actualités scientifiques et industrielles, no. 1040, Paris, Hermann, 1948.
2. L. KOENIGSBERGER, *Lehrbuch der Theorie der Differentialgleichungen mit einer unabhängigen Variabeln*, Leipzig, B. G. Teubner, 1889.
3. E. R. KOLCHIN, *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Ann. of Math. (2), vol. 49 (1948), pp. 1–42.
4. J. F. RITT, *Differential algebra*, Amer. Math. Soc. Colloquium Publications, vol. 33, 1950.

STEVENS INSTITUTE OF TECHNOLOGY
HOBOKEN, NEW JERSEY