A GENERALIZATION OF A THEOREM ON LINEAR DIFFERENTIAL EQUATIONS

A. S. AMITSUR

1. **Introduction.** It is well known that the number of independent solutions of a linear homogeneous differential equation equals its order, and the general solution is a linear combination of these independent solutions. The object of this paper is to prove that in the general case, that is, the derivation is defined in an abstract field (not necessarily commutative), the number of independent solutions does not exceed the order of the equation.

Applying this theorem to the case of inner derivation one obtains a new proof of a theorem due to Artin and Whaples.[1] Another application concerning cyclic fields will be given elsewhere.

2. **Abstract linear differential equations.** F will denote a field (not necessarily commutative) with an automorphism S: $a \to aS$. A right S-derivation D of F is a mapping of F into a part of itself satisfying:[2]

$$(1) \quad (a+b)D = aD + bD, \qquad (2) \quad (ab)D = (aS)(bD) + (aD)b.$$

If condition (2′) $(ab)D = a(bD) + (aD)(bS)$ holds instead of (2), D will be called a left S-derivation. The constants of the derivation (elements of F whose derivatives are zero) form a subfield C.

REMARK. Given a left S-derivation in F, one can define a right S-derivation in a field F^* which is anti-isomorphic to F. Hence any theorem about right derivation can be translated into a theorem on left derivation by suitable changes of "right" into "left."

As usual we denote $a^{(0)} = a$, $a' = aD$, $\cdots$, $a^{(n)} = (a^{(n-1)})D$. An equation:

$$(1) \qquad a_n z^{(n)} + a_{n-1} z^{(n-1)} + \cdots + a_0 z^{(0)} = 0, \qquad (a_n \neq 0,\ a_i \in F)$$

is called a right homogeneous linear differential equation (r.e.) of order n. When the $z^{(i)}$ are written on the left the equation is a left differential equation (l.e.).

THEOREM 1. *The elements of F which are solutions of the r.e.* (1) *form a right C-module of dimension at most n.*

Received by the editors August 23, 1947, and, in revised form, November 7, 1947.

[1] Artin and Whaples, *The theory of simple rings*, Amer. J. Math. vol. 65 (1943) pp. 87–107.

[2] In the present paper operators are written multiplicatively on the right of the element on which they operate.

PROOF. From (1) and (2) follows $(y_1-y_2)^{(\nu)}=y_1^{(\nu)}-y_2^{(\nu)}$ and $(y_1c)^{(\nu)}=y_1^{(\nu)}c$ for any $c\in C$, $\nu\geqq 0$.

Hence with two solutions y_1, y_2 of (1) also y_1-y_2 and $y_1\cdot c$, $c\in C$, are solutions of the r.e. (1). The solutions of (1) form, therefore, a right C-module. Let $y_1, y_2, \cdots, y_{n+1}$ be $n+1$ solutions. The $n+1$ rows of the Wronskian matrix of these solutions

$$W=\begin{pmatrix} y_1^{(0)} & y_2^{(0)} & \cdots & y_{n+1}^{(0)} \\ y_1' & y_2' & \cdots & y_{n+1}' \\ \cdots & \cdots & \cdots & \cdots \\ y_1^{(n)} & y_2^{(n)} & \cdots & y_{n+1}^{(n)} \end{pmatrix}$$

are left dependent because $\sum_{\nu=0}^{n} a_\nu y_\mu^{(\nu)}=0$, $\mu=1, 2, \cdots, n+1$ and $a_n\neq 0$. Hence the columns of W are right dependent.[3] Let r be the right-hand rank of the columns of W. We may assume that the first r columns are the independent, and the $(r+1)$th column is expressed as a linear combination of the columns as follows:

$$y_{r+1}^{(\nu)}=\sum_{\mu=1}^{r} y_\mu^{(\nu)} b_\mu, \qquad \nu=0, 1, \cdots, n. \tag{2}$$

We shall prove now that (2) holds also for $\nu=n+1$. In fact for any solution y of (1):

$$y^{(n)}=-\sum_{\nu=0}^{n-1}(a_n^{-1}a_\nu)y^{(\nu)}. \tag{3}$$

By differentiating (3) we have:

$$y^{(n+1)}=-\sum_{\nu=0}^{n-1}[(a_n^{-1}a_\nu)S]y^{(\nu+1)}-\sum_{\nu=0}^{n-1}(a_n^{-1}a_\nu)'y^{(\nu)}=\sum_{\nu=0}^{n} d_\nu y^{(\nu)}.$$

By (2) and (3) we have:

$$y_{r+1}^{(n+1)}=\sum_{\nu=0}^{n} d_\nu y_{r+1}^{(\nu)}=\sum_{\nu=0}^{n}\sum_{\mu=1}^{r} d_\nu y_\mu^{(\nu)} b_\mu$$

$$=\sum_{\mu=1}^{r}\left(\sum_{\nu=0}^{n} d_\nu y_\mu^{(\nu)}\right)b_\mu=\sum_{\mu=1}^{r} y_\mu^{(n+1)} b_\mu$$

which proves (2) for $\nu=n+1$.

By differentiating (2) we obtain:

---

[3] See, for example, J. Levitzki, *On the equivalence of the nilpotent elements of a semi-simple ring*, Compositio Math. vol. 5 (1938) Theorem 7, p. 401.

$$y_{r+1}^{(\nu+1)} = \sum_{\mu=1}^{r} (y_\mu^{(\nu)} S) b_\mu' + \sum_{\mu=1}^{r} y_\mu^{(\nu+1)} b_\mu = \sum_{\mu=1}^{r} (y_\mu^{(\nu)} S) b_\mu' + y_{r+1}^{(\nu+1)},$$

hence $0 = \sum_{\mu=1}^{r} (y_\mu^{(\nu)} S) b_\mu' = [\sum_{\mu=1}^{r} y_\mu^{(\nu)} (b_\mu' S^{-1})] S$ and therefore $\sum_{\mu=1}^{r} y_\mu^{(\nu)} (b_\mu' S^{-1}) = 0$; by the independence of the first r columns it follows that $(b_\mu') S = 0$, and hence $b_\mu' = 0, \mu = 1, 2, \cdots, r$; in other words the b_μ are constants. Thus we have proved that the $n+1$ solutions are right dependent over C. q.e.d.

THEOREM 2. *Let $N \leqq F$ be a right C-module of dimension n, then there exists a right differential equation in F of order n whose module of solutions coincides with N.*

PROOF. Let $y_1, y_2, \cdots, y_n$ be a base of N. The "Wronskian matrix"

$$W = \begin{pmatrix} y_1^{(0)} & y_2^{(0)} & \cdots & y_n^{(0)} \\ y_1' & y' & \cdots & y' \\ \cdots & \cdots & \cdots & \cdots \\ y_1^{(n)} & y_2^{(n)} & \cdots & y_n^{(n)} \end{pmatrix}$$

has n columns and $n+1$ rows, hence its rows are left dependent.[3] Therefore $n+1$ elements $a_0, a_1, \cdots, a_n$, not all zero, can be found so that: $\sum_{\nu=0}^{n} a_\nu y_\mu^{(\nu)} = 0$, $\mu = 1, 2, \cdots, n$. As above it follows that the elements of N will be solutions of a r.e. (1). Hence the module of solutions of (1) is of dimension at least n, which by Theorem 1 implies that the order of (1) must be exactly n, and the elements of N constitute the only solutions of (1).

3. **An application.** For any element a of F, the mapping $x \to xa$ of F is an endomorphism of F and will be denoted by a_r. The correspondence $a \to a_r$ is an isomorphism between F and F_r, where F_r is the set of all a_r. F_r is a subfield of the ring of endomorphisms $E(F)$.[4] Similarly the correspondence $a \to a_l$ is an anti-isomorphism between F and F_l, where a_l is the mapping $x \to ax$. For any $a_r \in F_r$ and $b_l \in F_l$ we have $a_r b_l = b_l a_r$.[4]

THEOREM 3. *Let F be a noncommutative field with a centre M. $a \in F$ is algebraic over M of degree n if and only if F is a right or left module of dimension n over F_a, where F_a is the centralizer of a in F (that is, the field of all the elements of F which are commutative with a).*

First we shall prove the following lemma.[5]

[4] N. Jacobson, *Theory of rings*, Mathematical Surveys, vol. 2, 1943, pp. 15–16.

[5] I am indebted to the referee for the present proof which is simpler than that which was previously given.

LEMMA. *An element a of F is algebraic over the centre M if and only if there exists a polynomial $h(\lambda)=\sum_{\nu=0}^{n}h_\nu\lambda^\nu$ $(h_\nu\in F,\ h_n\neq 0)$, which vanishes for all the transforms of a, that is $\sum_{\nu=0}^{n}h_\nu(yay^{-1})^\nu=0$ for each y of F, $y\neq 0$.*

PROOF. If there exist polynomials which vanish for all the transforms of a, then let $g(\lambda)=\sum_{\nu=0}^{m}b_\nu\lambda^\nu$ $(b_\nu\in F,\ b_m\neq 0)$ be a polynomial with this property with minimum degree. We may evidently assume that $b_m=1$. Then for every nonzero element z of F:

$$z\left[\sum_{\nu=0}^{m}b_\nu(yay^{-1})^\nu\right]z^{-1}=\sum_{\nu=0}^{m}zb_\nu z^{-1}[(zy)a(zy)^{-1}]^\nu=0.$$

Hence the polynomial $g_z(\lambda)=\sum_{\nu=0}^{m}zb_\nu z^{-1}\lambda^\nu$, where $zb_mz^{-1}=1$ also vanishes for all the transforms of a.

Since all the transforms of a are zeros of the difference polynomial $g(\lambda)-g_z(\lambda)$, whose degree is less than m, it follows by the minimum property of $g(\lambda)$ that all the coefficients of $g(\lambda)-g_z(\lambda)$ are zeros, that is, $b_\nu=zb_\nu z^{-1}$, $\nu=0, 1, \cdots, m$, for every z of F, $z\neq 0$. But this implies that all the coefficients of $g(\lambda)$ are in M, that is, a is algebraic over M.

The converse of the theorem follows from the fact that with a also all its transforms are zeros of the minimum polynomial of a over M.

We turn now to the proof of Theorem 3.

The mapping $x\to xa-ax$ is a right as well as a left derivation of F with $S=E$ the identical automorphism.[6] The field of constants of this inner derivation is the centralizer F_a of F. In the ring of endomorphisms $E(F)$: $D=a_r-a_l$, so $a_r=D+a_l$. a_l is commutative with a_r, hence also with D.

Let F be a right F_a-module of a finite dimension m, then there exists a r.e. of order m (Theorem 2) $z^{(m)}+a_1z^{(m-1)}+\cdots+a_mz^{(0)}=0$ satisfied by all elements of F, so that in the ring of endomorphism,

$$E(F): \qquad h(D)=D^m+D^{m-1}a_{1,l}+\cdots+a_{m,l}=0.$$

Hence

$$h(D)=h(a_r-a_l)=a_r^m+a_r^{m-1}C_{1,l}+a_r^{m-2}C_{2,l}+\cdots+C_{m,l}=0,$$

where

$$C_i=(-1)^i\left[\binom{m}{i}a^i-\binom{m-1}{i-1}a_1a^{i-1}+\cdots+(-1)^ia_i\right].$$

Operating with $h(D)$ on $x\in F$, $x\neq 0$, and multiplying on the right

[6] N. Jacobson, *Theory of rings*, p. 102.

by x^{-1} we get: $[xh(D)]x^{-1}=(xa^m+C_1xa^{m-1}\cdots C_mx)x^{-1}=(xax^{-1})^m+C_1(xax^{-1})^{m-1}+\cdots+C_m=0$.

The polynomial $k(\lambda)=\lambda^m+C_1\lambda^{m-1}+\cdots+C_m$ is in F and vanishes for all the transforms of a. Therefore, by the preceding lemma, a is algebraic over M, and its degree is at most m. Our theorem will be completely proved if we show that when a is algebraic over M then F is both a right and left F_a-module of dimension not greater than its degree, as from the preceding part of our proof it follows that $(F:F_a)$ must be equal to the degree of a over the centre M.

Now, let $g(\lambda)=\lambda^n+\alpha_1\lambda^{n-1}+\cdots+\alpha_n$ be the minimum polynomial of a over M. The isomorphism between F and F_r yields: $0=g(a)\rightarrow g_r(a_r)=g_r(D+a_l)=D^n+D^{n-1}b_{1,l}+\cdots+b_{n,l}=0$ where the $b_{i,l}$ are polynomials in a_l with coefficients in $M_r=M_l$, and therefore belong to F_l. Hence operating with $g_r(D+a_l)=0$ on $x\in F$ we have $xg_r(D+a_l)=x^{(n)}+b_1x^{n-1}+\cdots+b_nx^{(0)}=0$ where b_i is the image of $b_{i,l}$ in the anti-isomorphism between F_l and F. Theorem 1 yields, therefore, that F is a right F_a-module of dimension at most n, q.e.d.

Similarly one proves that F is a left F_a-module of dimension at most n. From the proof follows also that if F is a right F_a-module of finite dimension, then it is also a left F_a-module with the same dimension which is equal to the degree of a over the centre M.

HEBREW UNIVERSITY