COMMUTATIVE LINEAR DIFFERENTIAL OPERATORS

S. A. AMITSUR

1 Introduction. Let $D=d/dx$ be the operator of differentiation with respect to a variable x. Let $f(D)=a_0D^n+\cdots+a_n$, $a_0\neq 0$ be a differential operator of degree n. The problem we intend to study in this paper is to determine the set $C[f]$ of all linear operators which commute with f. This problem, is old and for a complete discussion of old and new results see the report of H. Flanders [2]. The most pronounced result in this subject is the fact that $C[f]$ is a commutative ring and that it is finitely generated over the algebra of all polynomials in $f(D)$ with constant coefficients.

In his report [2], Flanders obtains this theorem by algebraic methods with the aid of a deep theorem of Tsen on division algebras over the field of all rational functions in one variable. The first part of the present paper contains a simple algebraic proof of this result which uses only elementary facts of linear algebra.

In the second part of this paper we obtain necessary and sufficient conditions for the existence of non-trivial differential operators which commute with $f(D)$. This is obtained by adjoining a parameter λ to the domain of definition of the coefficient of $f(D)$ and by considering the invariant ring [1] of the operator $f(D)-\lambda$. It is shown that the structure of the $C[f]$ is closely related with the factorization of $f(D)-\lambda$. In this part, use is made of the theory of abstract differential polynomials as developed in [4], [3] and [1]. All proofs are purely algebraic.

2. The centralizer of $f(D)$. To be more precise we make the following assumptions: Let K be a field of characteristic zero with a derivation D: $a\to a'$. Let F denote the field of constants of K. That is: $F=\{a\,;\ a\in K.\ \ a'=0\}$.

Let $K[D]$ be the ring of all *formal* differential polynomials $p(D)=p_0D^n+\cdots+p_m$, $p_i\in K$ with multiplication defined in $K[D]$ by the relation

$$Da=aD+a'\,, \qquad a\in K\,.$$

Clearly $K[D]$ can be considered also the ring of linear differential operators on K.

Let $f(D)=a_0D^n+a_1D^{n-1}+\cdots+a_n$, $n\geqq 1$, $a_0\neq 0$ be a polynomial of degree n in $K[D]$. We shall denote by $C[f]$ the centralizer of f in $K[D]$. That is, $C[f]=\{g(D)\,;\ g(D)\in K[D],\ gf=fg\}$. Clearly $C[f]$ is a subring of $K[D]$ and it contains the ring $F[f]$ of all polynomials in $f(D)$ with constant coefficients.

Received November 14, 1957.

The main object of the first section is to prove the following.

THEOREM 1. (1) *$C[f]$ is a free $F[f]$-module of dimension ρ, where ρ is a divisor of n (=the degree of $f(D)$)*

(2) *$C[f]$ is a commutative ring.*

We shall need the following two known lemmas.

LEMMA 1. ([2] Lemma 10.1) *If p_0, q_0 are respectively the leading coefficients of two polynomials $p(D)$, $q(D)$ of the same degree which commute with $f(D)$ then $p_0 = cq_0$ for some constant $c \in F$.*

LEMMA 2. ([2] Lemma 10.2) *The set of all polynomials of $C[f]$ of degree$\leqq m$ is a finite—dimensional vector space over the field of constants F.*

For completeness we include the proof of these lemmas in the abstract case we are dealing with.

Indeed, if $p(D)f(D) = f(D)p(D)$ and $p(D) = p_0D^m + p_1D^{m-1} + \cdots + p_m$, then by comparing the coefficient of D^{n+m-1} on both sides we obtain:

$$ma_0'p_0 + a_0p_1 + p_0a_1 = np_0'a_0 + p_0a_1 + p_1a_0$$

Thus, the leading coefficient p_0 satisfies the homogeneous linear differential equation: $na_0p_0' - ma_0'p_0 = 0$. Hence if $q(D) = q_0D^m + \cdots + q_m$ also commutes with $f(D)$, q_0 satisfies the same differential equation and, therefore $q_0 = cp_0$ for some constant c, which proves Lemma 1.

The proof of Lemma 2 follows immediately from Lemma 1, by induction on the degree m.

We proceed now with the proof of Theorem 1:

Let Z_f be the set of all integers which are the degrees of the polynomials of $C[f]$. Since $C[f]$ is a ring, and since $\deg(p(D)q(D)) = \deg p(D) + \deg q(D)$, it follows that Z_f is closed under addition. Let $\overline{m}$ denote the residue class modulo $n(=\deg f(D))$ of the integer m, and let $\overline{Z}_f = \{\overline{m}\,;\, m \in Z_f\}$. Then clearly $\overline{Z}_f$ is a subgroup of the additive cyclic group of all residue classes mod n. Hence $\overline{Z}_f$ is cyclic of order ρ and ρ is a divisor of n.

Let $\overline{o} = \overline{m}_1, \cdots, \overline{m}_\rho$ be the ρ classes mod n of $\overline{Z}_f$ and let m_i be the minimal integer of its class $\overline{m}_i$. Let $g_i(D) \in C[f]$ be a polynomial of degree m_i and we can clearly choose $g_1 = 1$. We shall show that these polynomials g_i are free generators of $C[f]$ over $F[f]$.

Indeed, if $g_1\varphi_1(f) + \cdots + g_\rho\varphi_\rho(f) = 0$ for some polynomials $\varphi_i(f) \in F(f)$, then evidently: if $\varphi_h(f) \neq 0$, for some h, then

$$\deg\,[g_i\varphi_i(f)] = \deg\,[g_j\varphi_j(f) \text{ for some } i \neq j.$$

But, since deg $[g_i\varphi_i(f)]\equiv$deg $g_i\equiv m_i$(mod n) and deg $[g_j\varphi_j(f)]\equiv m$; (mod n), and $m_i\not\equiv m_j$ (mod n), we are led to a contradiction. Consequently $\varphi_i(f)=0$ for all i.

It remains now to show that if $g\in C[f]$ then $g=g_1\varphi_1(f)+\cdots+g_\rho\varphi_\rho(f)$ for some $\varphi_i(f)\in F[f]$. This is obtained by induction on deg g. It deg $g=0$, then it follows by Lemma 1 that $g=c\in F$, and hence $g=cg_1$. Now, let deg $g=k$. Since $k\in Z_f$, it follows that $k\equiv m_i$(mod n) for some i. By the minimality of m_i, it follows that $k\geqq m_i$. Hence $k=m_i+nq$, which implies that deg $g=$deg g_if^q. It follows, therefore, by Lemma 1 that $g'=g-cg_if^q\in C[f]$ for some $c\in F$ and deg $g'<$deg g. Hence, by induction we obtain $g-cg_if^q=g_1\varphi_1(f)+\cdots+g_\rho\varphi_\rho(f)$, and the proof is readily completed. This proves the validity of (1) of Theorem 1.

We turn now to the proof of (2). Let $g(D)\in C[f]$ be a polynomial whose residue class of deg $g(D)$ mod n generates the cyclic group $\overline{Z}_f$. One readily verifies that in this case, the set of all degrees of the polynomials of the form

$$H(g,f)=\varphi_0(f)+g\varphi_1(f)+\cdots+g^{\rho-1}\varphi_{\rho-1}(f),\ \varphi_i(f)\in C[f]\ ,$$

contains all integers of Z_f with at most an exception of a finite number of integers. Hence, we may assume that this set contain all integers $m\in Z_f$ for which $m\geqq t$, for some fixed t. One then proves as in the preceding part that every polynomial $h(D)\in C[f]$ can be written in the form $h(D)=H_0(g,f)+h_0(D)$, where $h_0\in C[f]$ and deg $h_0\leqq t$. From Lemma 2 we know that the set of all polynomials h_0 is an F-space of dimension T, for some T. Let $f^\nu h=H_\nu(g,f)+h_\nu$, $\nu=0,1,\cdots,T$, and deg $h_\nu\leqq t$; thus the polynomials h_ν are F-dependent and, therefore, $\sum c_\nu h_\nu=0$, for $c_\nu\in F$ and not all $c_\nu=0$. This yield that $(\sum c_\nu f^\nu)h=\sum c_\nu H_\nu(g,f)$, which proves that for every $h\in C[f]$ there exists polynomials $H(g,f)$ and $F(f)$ with constant coefficients such that: $F(f)h=H(g,f)$.

Clearly the set of all polynomials $H(g,f)$ commute with each other, and the polynomials of $C[f]$ commute with the polynomial of $F[f]$; hence, if $F_i(f)h_i=H_i(g,f)$ for $h_i\in C[f]$ $i=1,2,$ then

$$F_1(f)F_2(f)h_1h_2=(F_1h_1)(F_2h_2)=H_1H_2=H_2H_1=(F_2h_2)(F_1h_1)=F_2F_1h_2h_1\ .$$

Now $K[D]$ is a ring without zero divisors, hence $h_1h_2=h_2h_1$ and the proof of Theorem 1 is completed.

It was thus shown that $C[f]$ is an integral domain, let $C(f)$ denote the quotient field of $C[f]$. If $F(f)$ denotes the field of all rational functions in f over F, that is the quotient field of $F[f]$, then clearly $F(f)\subseteqq C(f)$. Actually, the preceding proof shows that the chosen polynomial g is algebraic of degree ρ over $C(f)$, since $F(f)g^\rho=H(g,f)$ and moreover $C(f)$ is an algebraic extension of $F(f)$ generated by g. Thus we have shown :

COROLLARY 1. *$C(f)$ is an algebraic extension of degree ρ of $F(f)$ and if the residue class of a polynomial $g \in C[f]$ generates the group of residue classes $\bar{Z}_F$, then g is of degree ρ over $F(f)$ and $C(f)=F(f)\ [g]$.*

This clearly implies the following.

COROLLARY 2. *If $h \in C[f]$ then h is algebraic over $F(f)$ and its degree is a divisor of ρ, that is, there exists a polynomial $H(h,f) \equiv 0$ with constant coefficient and where degree in h is a divisor of ρ.*
This follows from the fact that $F(f) \subseteqq F(f)[h] \subseteqq F(f)[g]$.

REMARK. The fact that h is algebraic is well known, but here we obtained some additional information on its degree. In fact, one can prove by the previous methods that the degree of the minimal polynomial $H(h, f)$ in h is equal to the order of the subgroup of the additive group of all residue classes mod n generated by the degree of h.

Additional information on the degree ρ of $C(f)$ over $F(f)$ will be obtained in the following section.

3. **The field** $C(f)$. Let λ be a commutative indeterminate over the field K. We extend the derivation of K to a derivation of the field of all rational functions $K(\lambda)$ so that $F(\lambda)$ will be the field of constants of the extended derivation. Consider the ring $K(\lambda)[D]$ of all differential polynomials in D with coefficients in $K(\lambda)$.

LEMMA 3. *Every polynomial $g(D) \in K(\lambda)[D]$ can be expressed in the form $g=a(\lambda)^{-1}\ G[\lambda, D]$, where $G[\lambda, D]=\sum g_\nu(\lambda)D^\nu$ is of the same degree as $g(D)$, and $g_\nu(\lambda), a(\lambda)$ are relatively prime polynomials in λ. Similarly $g=G_1[\lambda, D]b(\lambda)^{-1}$ with similar restrictions for G_1 and $b(\lambda)$.*
The proof is evident.

Let $\bar{F}_\lambda$ be the algebraic closure of $F(\lambda)$, and let $\bar{K}_\lambda=K(\bar{F}_\lambda)$ be the field obtained by adjoining $\bar{F}_\lambda$ to K. that is, $\bar{K}_\lambda$ is the composition field of K and $\bar{F}_\lambda$ over $F(\lambda)$. One extends the deviation of K to $\bar{K}_\lambda$ so that $\bar{F}_\lambda$ is the new field of constants. These extended derivations yield the following sequence of rings of differential polynomials

$$K[D] \subset K(\lambda)[D] \subset \bar{K}_\lambda[D]\ .$$

If $f(D) \in K[D]$ then $f(D)-\lambda \in K(\lambda)[D]$ and first we show the following.

LEMMA 4. *$f(D)-\lambda$ is an irreducible polynomial in $K(\lambda)\ [D]$.*

PROOF. Suppose $f(D)-\lambda=f_1(D)f_2(D)$ and $\deg\ f_i<\deg\ f,\ \ f_i(D) \in$

$K(\lambda)[D]$. In view of Lemma 3 we set $f_1(D)=g_1[D, \lambda]a^{-1}(\lambda)$ and $a^{-1}(\lambda)f_2(D)=g_2[D, \lambda]b^{-1}(\lambda)$. Thus $(f(D)-\lambda)b(\lambda)=g_1[D, \lambda]g_2[D, \lambda]$.

We consider now $g,[D, \lambda]$ as a polynomial in λ with coefficients in the ring $K[D]$, and we obtain by the remainder theorem[1]

$$g_1[D, \lambda]=(f(D)-\lambda)H[D, \lambda]+R[D]$$

where $R[D]\in K[D]$. Hence, it follows readily that

$$R[D]g_2[D, \lambda]=(f(D)-\lambda)G[D, \lambda]\ .$$

Let $g_2[D, \lambda]=\sum\lambda^\nu h_\nu(D)$. Then the fact that $f(D)-\lambda$ is a left divisor of $R[D]g_2[D, \lambda]$ implies by the remainder theorem that $\sum f^\nu Rh_\nu=0$. If $R\neq 0$, then we must have that deg $(f^\nu Rh_\nu)=$deg $(f^\mu Rh_\mu)\neq 0$ for some $\nu\neq\mu$. But suppose $\nu>\mu$ then we have

$$\deg\ h_\mu=\deg\ h_\nu+(\nu-\mu)\ \deg\ f\geqq\deg\ f.$$

On the other hand, clearly,

$$\deg\ h_\mu\leqq\deg\ g_2=\deg\ f_2<\deg\ f$$

which is impossible. Hence $R=0$, which means that $g_1[D, \lambda]=(f(D)-\lambda)H[D, \lambda]$. But this leads to a contradiction since deg $F_1<$deg f, and proof of the lemma is completed.

The polynomial $f(D)-\lambda$, when considered as a polynomial in $\bar{K}_\lambda[D]$, may be reducible, and indeed its factorization in the extended field $\bar{K}_\lambda$ is closely connected with the field $C(f)$. This we propose to show in what follows, and we begin with some preliminary lemmas.

Let $K[D, \lambda]$ be the ring of all polynomials in λ and D, and let $K[\lambda]$ be the polynomial ring in λ.

LEMMA 5. *Let $0\neq p\in K(\lambda)$, $A, G, H\in K[\lambda, D]$ such that $AG=Hp$, and $A=f_0D^n+\cdots+f_n$ where $f_i\in K[\lambda]$ and $(f_0, p)=1$, then $G=G_1p$ for some $G_1\in K[\lambda, D]$.*

PROOF. If the lemma is not valid, then let G be a polynomial of minimum degree in D which is not a left multiple of p and which satisfies the conditions of the lemma. Let[2] $G=D^mg_0+\cdots+g_m$. Since $AG=Hp$. It follows by comparison of the leading coefficients of both sides that $f_0g_0=h_0p$. Now $(f_0p)=1$, hence p divides g_0 and we have $g_0=qp$ for some polynomial $q\in K(\lambda)$. But then $G-(D^mq)p$ is of degree $<$

[1] See, e.g. A. A. Albert, Modern Higher Algebra, Chicago 1937 p. 25.

[2] Note that the polynominal $G(D)$ may be written with coefficients either on the right or on the left of the power of D.

deg G; it is not a left multiple of p, since G is not, but nevertheless $A(G-D^m qp)=(H-FD^m q)p$, which contradicts the minimality of G.

LEMMA 6. *Every polynomial* $p(\lambda)\in K[\lambda]$ *can be written as* $p(\lambda)=c(\lambda)q(\lambda)$ *where* $c(\lambda)$ *is a monic polynomial in* λ *and* $c'(\lambda)=0$, *and in the factorization of* $q(\lambda)=aq_1^{\nu_1}\cdots q_k^{\nu_k}$, $a\in K$, *into prime factors, the polynomials* $q_i(\lambda)$ *are relatively prime to their derivatives* $q_i'(\lambda)$.

Let $p(\lambda)=ap_1^{\nu_1}(\lambda)p_2^{\nu_2}(\lambda)\cdots p_n^{\nu_n}(\lambda)$ be the factorization of $p(\lambda)$ into prime factors. We may assume that each p_i is a monic polynomial, i.e. its leading coefficient is 1. For each p_i, the polynomial $p_i'(\lambda)$ is of lower degree in λ than p_i; hence, since p_i is prime, it follows that either $(p_i, p_i')=1$ or p_i divides p_i', which in the latter case must yield that $p_i'=0$. Thus, $c(\lambda)$ is the product of all p_i for which $p_i'=0$ and $q(\lambda)$ is the product of the rest.

LEMMA 7. *Let* $p\in K[\lambda]$, $G,H\in K[D,\lambda]$ *and* $(p,p')=1$, *then* $pG=Hp$ *implies that* $G=G_0p$ *for some* $G_0\in K[D,\lambda]$.

PROOF. If the lemma is not true then let G be the polynomial of minimum degree in D which do not satisfy our lemma.

Let $G=D^n g_0+\cdots+g_n$, $H=D^n h_0+\cdots+h_n$, g_i and $h_i\in K[\lambda]$, and $g_0h_0\neq 0$. Compare the coefficient of D^n of both sides of the equation $pG=Hp$. This yields $pg_0=h_0p$ which gives $g_0=h_0$. The coefficient of D^{n-1} yields

$$-np'g_0+pg_1=h_1p.$$

Hence, $-np'g_0=p(h_1-g_1)$. Since $(p,p')=1$ it follows that $g_0=kp$ for some $k\in K[\lambda]$. But then the polynomial $G-D^n kp$ is of lower degree then G; it is not a left multiple of p, but nevertheless $p(G-D^n kp)=(H-pD^n k)p$. This contradicts the minimality of G.

We can now turn to the main object of this section, and we recall the notion of the invariant ring of a differential polynomial. ([1 §5 p.260] and [3 §10 p.502]).

Let $h(D)$ be a polynomial in $K[D]$. The invariant ring $\mathscr{R}(h)$ of h is the ring of all classes $g(D)+h(D)K[D]$ which have a representative $g(D)$ satisfying $g(D)h(D)=h(D)g_1(D)$. It is known [1, Theorem 9] that $\mathscr{R}(h)$ is a finite dimensional algebra over the constant field, and if h is irreducible, then $\mathscr{R}(h)$ is a division ring.

We shall consider the invariant ring $\mathscr{R}(f(D)-\lambda)$ in the ring $K(\lambda)[D]$. Since it was shown in Lemma 4 that $f(D)-\lambda$ is irreducible, it follows that $\mathscr{R}(f-\lambda)$ is a division ring (e.g. [1, Theorem 10]). First we show the following.

THEOREM 2. *The field* $C(f)$ *is isomorphic with* $\mathscr{R}(f-\lambda)$.

PROOF. This elements of $\mathscr{R}(f-\lambda)$ are classes of the form $g(D)+(f-\lambda)K(\lambda)[D]$, $g \in K(\lambda)[D]$, and the first part of the proof is to show that we may choose a representative of this class of the form $q(D)c(\lambda)^{-1}$, where $q(D) \in C[f]$ and $c(\lambda)$ is a polynomial in λ with constant coefficients. The converse, that is: that every class which has a representative of the form $q(D)c(\lambda)^{-1}$ belongs to $\mathscr{R}(f-\lambda)$, follows easily since $qc^{-1}(f-\lambda)=q(f-\lambda)c^{-1}= (f-\lambda)\ qc^{-1}$.

So let $g(D)$ be a representative of a class in $\mathscr{R}(f-\lambda)$, then $g(D)(f-\lambda)=(f-\lambda)h(D)$. We set $g(D)=a^{-1}(\lambda)G[D,\lambda]$ and $h(D) = H[D,\lambda]b(\lambda)^{-1}$, in accordance with Lemma 3, we may assume and that a, b and monic polynomials. Then we have

$$G[D,\lambda](f-\lambda)b(\lambda)=a(\lambda)(f-\lambda)H[D,\lambda]\ . \tag{3.1}$$

Suppose $b(\lambda)\neq 1$. Let $b(\lambda)=p_1p_2\cdots p_n$ be the factorisation of b into prime factors, then we may assume that $(p_1', p_i)=1$. Since if $(p_1', p_i)\neq 1$ we have seen that $p_1'=0$, and we may deal with $p_ig(D)$, which also belongs to $\mathscr{R}(f-\lambda)$, instead of $g(D)$.

It follows by Lemma 3 that H was so chosen that it is not a left multiple of any prime factor of $b(\lambda)$ say p_1; furthermore, clearly $a(\lambda)(f-\lambda)=D^na(\lambda)a_0+\cdots$, where $f-\lambda=D^na_{0+}\cdots$ and $a_0\neq 0$. Hence, it follows by Lemma 5 that p_1 divides $a(\lambda)$. So let $a(\lambda)=p_1q_1$. Hence (3.1) yields

$$p_1q_1(f-\lambda)H[D,\lambda]=G_1p_1,\ \text{where}\ G_1=G(f-\lambda)p_2\cdots \mathrm{p}_r\ .$$

Since $(p_1, p_1')=1$, it follows by Lemma 7 that $q_1(f-\lambda)H=G_2p_1$. By similar reasons it follows from Lemma 5 that $q_1=p_1q_2$, and thus $p_1q_2(f-\lambda)H=G_2p_1$. Again Lemma 7 will yield that $q_2(f-\lambda)H=G_3p_1$. This cannot proceed indefinitely since the degrees of $a(\lambda)$, q_1, q_2, $\cdots$ in λ are reduced in each step. Thus we are led to a contradiction, which leads us to the result that $b(\lambda)=1$. Thus (3.1) states that $G(f-\lambda)=a(f-\lambda)H$. The leading coefficient of $f-\lambda$ is an element of K, hence if we assume that $a\neq 1$, we must have by a result parallel to Lemma 5, that $G=aG_1$ which contradicts the way we have chosen G and a by Lemma 3.

We thus have shown that by multiplying $g(D)$ by polynomials $c(\lambda)$ (that is the product of the p_i for which $p_i'=0$) we obtained a representative $G[D,\lambda]$ which is a polynomial both in λ and D. If $G[D,\lambda]=\sum\lambda^\nu g_\nu(D)$, then the remainder theorem yields that

$$G[D,\lambda]=\sum f^\nu g_\nu+(f-\lambda)H_1[D,\lambda]\ .$$

Thus $q(D)=\sum f^\nu g_\nu$ is a representative of the same class $\mathrm{mod}(f-\lambda)$ as $G[D,\lambda]$.

Since $q \in \mathscr{R}(f-\lambda)$, we have $q(D)(f-\lambda)=(f-\lambda)Q(D)$. Let, in view of Lemma 3, $Q(D)=P[D,\lambda]d(\lambda)^{-1}$. Then $q(D)(f-\lambda)d(\lambda)=(f-\lambda)P[D,\lambda]$. We must have $d(\lambda)=1$. For if the degree of $d(\lambda)$ in λ is >1, then since the leading coefficient of $f-\lambda \in K$, it is relatively prime with $d(\lambda)$, and hence Lemma 5 implies that $P[D, \lambda]=P_1 d(\lambda)$ which contradicts Lemma 3. Thus $q(D)(f-\lambda)=(f-\lambda)Q(D)$ and $Q(D) \in K[D, \lambda]$. By comparing the coefficients of the powers of λ of both sides, one readily obtains that $Q=q$, and $qf=fq$, that is $q \in C[f]$. Consequently, we obtained that class of $c(\lambda)g(D)$ has a representative $q \in C[f]$. Hence

$$g(D)+(f-\lambda)K(\lambda)[D]=c(\lambda)^{-1}q(D)+(f-\lambda)K(\lambda)[D]$$

which proves our assertion.

We prove now Theorem 2. Clearly every element of $C(f)$ has the form $q(D)c(f)^{-1}$ where $q \in C[f]$ and $c(f) \in F[f]$, and we map $C(f)$ onto $\mathscr{R}(f-\lambda)$ by the correspondence

$$q(D)c(f)^{-1} \rightarrow q(D)c(\lambda)^{-1}+(f-\lambda)K(\lambda)[D] .$$

From the previous part of the proof it follows that this mapping is onto, and one readily verifies that this is an isomorphism. We shall show here only that it is a one-to-one correspondence; namely, that $q_1(D)c_1(f)^{-1} =q_2(D)c_2(f)^{-1}$ if and only if

$$q_1(D)c_1(\lambda)^{-1}+(f-\lambda)K(\lambda)[D]=q_2(D)c_2(\lambda)^{-1}+(f-\lambda)K(\lambda)[D] .$$

Indeed, the first hold if and only if $q_1(D)c_2(f)=q_2(D)c_1(f)$, and one readily verifies by the remainder theorem, in view of the fact that $c_i(f)$ commute with q_i, that the latter is eqivalent to the fact that $q_1(D)c_2(\lambda)-q_2(D)c_1(\lambda)=(f-\lambda)H[\lambda, D]$, and the rest is evident.
We now apply Theorem 2 to show the following.

THEOREM 3. *The polynomial $f(D)-\lambda$ is completely reducible* [3, p. 489] *in $\overline{K}_\lambda[D]$; if $g(D)$ is an irreducible polynomial which is right (or left) divisor of $f[D]-\lambda$ in $\overline{K}_\lambda[D]$ then deg $f=\mu$deg g and $\mu=\rho=(C(f):F(f))$.*

PROOF. Let θ be any automorphism of $\overline{F}_\lambda$ over $F(\lambda)$ This automorphism is readily extended to $\overline{K}_\lambda$ over $K(\lambda)$, and to $\overline{K}_\lambda[D]$ over $K(\lambda)$ $[D]$. Since $f-\lambda=hg$, and $f-\lambda \in K(\lambda)[D]$, one readily verifies that $f-\lambda=(f-\lambda)^\theta=h^\theta g^\theta$. This means that $f-\lambda$ is a left common multiple of all g^θ, where θ ranges over all automorphisms of $\overline{K}_\lambda$ over $K(\lambda)$.

Let $G(D)$ be the least common left multiple of all g^θ whose leading coefficient is 1. Then, clearly $G^\varphi(D)$ will also be a least common multiple, whence one readily obtains that $G^\varphi=G$ for all automorphisms φ. This will yield that $G \in K(\lambda)[D]$. Now $f-\lambda$ is also a common left multiple, hence (Ore [4]) $f-\lambda=G_1G$, $G_1 \in \overline{K}_\lambda[D]$. Clearly, one obtains that also $G_1 \in K(\lambda)[D]$, but Lemma 4 states that $f-\lambda$ is irreducible. Consequently

$f-\lambda$ is the least left common multiple of all g^{θ}. From which one obtains (Ore [4]) that $f-\lambda$ is completely irreducible, and moreover, $f-\lambda=[g_1, \cdots, g_\mu]$, the least common multiple of all $g_i=g^{\theta_i}$ for some θ_i. In particular, this yields that all g_i have the same degree as g.

Thus (Ore [4]) μ deg $g=\deg(f-\lambda)=n$, or deg $g=\deg g_i=n/\mu$

To prove the second part of the theorem we need the following lemmas.

LEMMA 8. *Let* $\overline{\mathscr{R}}(f-\lambda)$ *be the invariant ring of* $f-\lambda$ *in* $\overline{K}_\lambda[D]$, *then* $\overline{\mathscr{R}}(f-\lambda)=\overline{\mathscr{R}}(f-\lambda)\otimes\overline{F}_\lambda$, *where the tensor product is taken with respect to* $F(\lambda)$.

For let (c_α) be a $F(\lambda)$-base of $\overline{F}_\lambda$, then clearly, this set is also a $K(\lambda)$-base of K as well as a $K(\lambda)[D]$-base of $\overline{K}_\lambda[D]$. Let $g(D)\in\overline{K}_\lambda[D]$ belong to $\overline{\mathscr{R}}(f-\lambda)$, and let $g=\sum g_\alpha c_\alpha$ where $g_\alpha\in K(\lambda)[D]$. One readily observes that since $f-\lambda\in K(\lambda)[D]$, the relation $g(f-\lambda)=(f-\lambda)h$ implies that $h=\sum h_\alpha c_\alpha$, $h_\alpha\in K(\lambda)[D]$ and $g_\alpha(f-\lambda)=(f-\lambda)h_\alpha$ for all α. That is $g_\alpha\in\mathscr{R}(f-\lambda)$. Conversely, if $g_\alpha\in\mathscr{R}(f-\lambda)$ and only a finite number of g_α is different from 0, then clearly $\sum c_\alpha g_\alpha\in\overline{\mathscr{R}}(f-\lambda)$; from which one readily deduces the lemma.

LEMMA 9. *If* $g(D)\in\overline{K}_\lambda[D]$ *is irreducible, then* $\overline{\mathscr{R}}(g)$ *is the field of constants* $\overline{F}_\lambda$ *that is, if* $hg=gh_1$, *then* $h=c+g\overline{K}_\lambda[D]$ *for some constant* $c\in\overline{F}_\lambda$.

Indeed, if g is irreducible, then it follows by [1] Theorem 10 that $\overline{\mathscr{R}}(g)$ is a finite dimensional division algebra over the field of constant $\overline{F}_\lambda$. But $\overline{F}_\lambda$ is algebraically closed, hence the only division algebra over $\overline{F}_\lambda$ is $\overline{F}_\lambda$ itself. Thus $\overline{\mathscr{R}}(g)=\overline{F}_\lambda$.

We return now to the proof of Theorem 3.

It follows by [3, Theorem 19] and by the relation between the invariant ring of differential polynomials and differential linear transformaions ([3, §10 p.503] and [4]) that the invariant ring of a completely reducible polynomial is a direct sum of complete matrix rings over division algebra, and each division algebra is isomorphic to the invariant ring of one of the prime factors of the polynomial considered. In our case, since $\overline{\mathscr{R}}(f-\lambda)$ is commutative (by Lemma 8 and Theorem 1), and the invariant rings of irreducible polynomials are isomorphic with $\overline{F}_\lambda$, it follows that $\overline{\mathscr{R}}(f-\lambda)=F_1\oplus\cdots\oplus F_\mu$, where each F_i is a field isomorphic with $\overline{F}_\lambda$ (compare with [3, Theorem 19]), and μ is the number of prime divisors given in the first part of Theorem 3.

On the other hand $\mathscr{R}(f-\lambda)$ is an algebraic extension of $F(\lambda)$; and from Theorem 2 and Theorem 1 it follows that $(\mathscr{R}(f-\lambda): F(\lambda))=\rho$.

Hence it is well known that $\mathscr{R}(f-\lambda)\otimes\bar{F}_\lambda$ is a direct sum of ρ fields isomorphic with the algebraic closed field $\bar{F}_\lambda$. Consequently Lemma 8 implies that $\bar{\mathscr{R}}(f-\lambda)$ has the same decomposition. Comparing the two results, we obtain that $\rho=\mu$.
From Theorem 3 we can conclude the following known result.

COROLLARY 3. *If $f(D)$ is a polynomial with constant coefficients then $C[f]$ is the ring $F[D]$ of all polynomials with constant coefficients.*

PROOF. The factorization of $f(D)-\lambda$ in $\bar{K}_\lambda[D]$ is readily obtained. Indeed, let $\mu_1, \cdots \mu_n$ be the roots of $f(x)-\lambda$ in $\bar{F}_\lambda$ where x is a commutative variable, then it is easily seen that the factorization of $f(D)-\lambda$ in $\bar{K}_\lambda[D]$ is $f(D)-\lambda=\Pi_{i=1}^n(D-\mu_i)$. It follows therefore by Theorem 3 that $(C(f)\colon F(f))=n$. But the field of all rational functions in D, that is $F(D)$, is of degree n over $F(f)$ and clearly $F(D)\subset C(f)$. Hence $C(f)=F(D)$. The rest is readily obtained.

We can also determine the dimension $(C(f)\colon F(f)=\rho$ by the methods of [1, §5]. In [1] we have introduced the notion of a resultant of two differential polynomials which was denoted by $f(D)\times g(D)$, and the notion of the nullity of a polynomial $f(D)$ in a field K. We recall here that the nullity of f in K was the number of independent solutions of the differential equation $f(D)z=O$ in K.

From Theorem 2 and [1, Theorem 2] we now obtain the following

THEOREM 4. *The dimension $\rho=(C(f)\colon F(f))=(\mathscr{R}(f-\lambda)\colon F(\lambda))$ is equal to the nullity of the polynomial $(f(D)-\lambda)\times(f^*(D)-\lambda)$ in $K(\lambda)$ where $f^*(D)$ is the adjoint polynomial of $f(D)$.*

REFERENCES

1. S. A. Amitsur, *Differential polynomials and division algebras*, Ann. of Math. **59** (1954), 245-278.
2. H. Flanders, *Commutative linear differential operators*, Report No. 1, University of California, Berkely 1955.
3. N. Jacobson, *Pseudo-linear transformations*, Ann. of Math., **38** (1937), 484-507.
4. O. Ore, *Theory of non commutative polynomials*, Ann. of Math. **34** (1933), 480-508.

THE HEBREW UNIVERSITY