PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 39, Number 1, June 1973

AN EXTENSION OF DEDEKIND'S LINEAR INDEPENDENCE THEOREM

CHARLES M. WALTERS[1]

ABSTRACT. Dedekind's theorem on the linear independence of isomorphisms of a field is extended to the case of linear independence of compositions of isomorphisms and powers of a derivation, D, for fields of characteristic zero which contain an element s such that $D(s)=1$.

In this paper we present an extension of the following classical theorem on the linear independence of isomorphisms of a field [**1**, p. 25].

THEOREM 1 [DEDEKIND]. *Let E and P be fields. Then the collection $\{F|F$ is an isomorphism of E into $P\}$ is left linearly independent over P; i.e., $\sum_{i=1}^{n} p_iF_i=0$, p_i in P, $n\geqq 1$ an integer, and $F_i\neq F_j$ for $i\neq j$ implies $p_i=0$ for $i=1, 2, \cdots, n$.*

For fields of characteristic zero, the above theorem may be extended to the case of compositions of isomorphisms and powers of a derivation on E as in the following theorem. This result is useful in the study of linear transformations on the field of Mikusiński operators [**2**].

THEOREM 2. *Let E and P be fields of characteristic zero, D a derivation of E into E, and s an element in E such that $D(s)=1$. Then, the collection $\{FD^n|F$ is an isomorphism of E into P and $n\geqq 0$ is an integer$\}$ is left linearly independent over P.*

In the following we consider elements of a field E as endomorphisms of E defined for b in E by $b(x)=bx$ for each x in E. (A field E can be embedded in the ring of group endomorphisms on the additive group E.) For the proof of Theorem 2, we will need a lemma.

LEMMA. *Let E and P be fields of characteristic zero, D a derivation of E into E, and s an element in E such that $D(s)=1$. If F and G are homomorphisms of E into P such that $FD^p=GD^q$ for some integers p, $q\geqq 0$, then $p=q$ and $F=G$.*

Received by the editors August 28, 1972.
AMS (MOS) subject classifications (1970). Primary 13B10.
Key words and phrases. Derivation, linearly independent.

[1] These results are contained in the author's doctoral dissertation written with the guidance of Professor Raimond A. Struble at North Carolina State University, Raleigh.

PROOF. If $p=q=0$, the result is trivial. It is easily verified that for integers $p, q\geqq 0$

$$\begin{aligned} D^p(s^q) &= 0 && \text{if } p > q, \\ &= q(q-1)\cdots(q-p+1)s^{q-p} && \text{if } p \leqq q. \end{aligned}$$

Hence if $p>q\geqq 0$, then $0=FD^p(s^q)=GD^q(s^q)=q!$ is a contradiction and by the symmetry of this argument we conclude that $p=q$. Now suppose $m>0$ is the smallest integer such that $FD^m=GD^m$. Then, if x is an element of E, from Leibnitz' formula

$$D^m(sx) = \sum_{r=0}^{m} \binom{m}{r} D^r(s)D^{m-r}(x)$$

it follows that

$$D^m s = \sum_{r=0}^{m} \binom{m}{r} D^r(s)D^{m-r}. \tag{1}$$

But $D^0(s)=s$, $D(s)=1$, and $D^r(s)=0$ for $r\geqq 2$. Thus, (1) reduces to

$$D^m s = sD^m + mD^{m-1}. \tag{2}$$

Since F is multiplicative, if x is in E then $Fs(x)=F(sx)=F(s)F(x)$ and so $Fs=F(s)F$. Therefore, from (2) we obtain

$$\begin{aligned} FD^m s &= F(sD^m + mD^{m-1}) = F(s)FD^m + mFD^{m-1} \\ &= G(s)GD^m + mGD^{m-1} = GD^m s \end{aligned}$$

so that

$$[F(s) - G(s)]FD^m = m[GD^{m-1} - FD^{m-1}].$$

Moreover, $FD^m(s^{m+1})=GD^m(s^{m+1})$ implies $F(s)=G(s)$ and so from the above we have $GD^{m-1}=FD^{m-1}$, a contradiction of the choice of m.

PROOF OF THEOREM 2. Suppose there exists a set of elements $b_1, b_2, \cdots, b_m$ in P, not all zero, and a set of m distinct mappings $F_1D^{n_1}, F_2D^{n_2}, \cdots, F_mD^{n_m}$ such that

$$\sum_{i=1}^{m} b_iF_iD^{n_i} = 0$$

where we assume without loss of generality that $n_1\geqq n_2\geqq\cdots\geqq n_m\geqq 0$. Then there exists such a relation exhibiting a smallest value n_1; *i.e.*, exhibiting a minimum largest power of D, say

$$\sum_{i=1}^{p} b_iF_iD^{n_i} = 0 \tag{3}$$

with $F_1D^{n_1}, F_2D^{n_2}, \cdots, F_pD^{n_p}$ distinct, $b_1, b_2, \cdots, b_p$ not all zero, and $n_1\geqq n_2\geqq\cdots\geqq n_p\geqq 0$. Now if $n_1=0$, then Theorem 1 applies. Hence we may assume that $n_1>0$ If $p=1$, then $b_1F_1D^{n_1}(x)=0$ for all x in E means $F_1D^{n_1}=0$. But $F_1D^{n_1}\neq 0$ since if so $F_1=0$ by the lemma. Thus we may assume that $p>1$. We rewrite the relation (3) as

$$\sum_{i=1}^{l} b_iF_iD^{n_1} + \sum_{i=l+1}^{p} b_iF_iD^{n_i} = 0 \tag{4}$$

where $n_i<n_1$ for $l+1\leqq i\leqq p$. Now if (4) holds then we may choose such a relation having a minimum l; *i.e.*, having a minimum number of terms involving the maximum power n_1 of D. Thus we assume that in (4) l is minimum. Multiplying (4) on the right by s, in view of (2) and the fact that each F_i is multiplicative we obtain

$$\begin{aligned}&\sum_{i=1}^{l} b_iF_i(s)F_iD^{n_1} + \sum_{i=1}^{l} n_1b_iF_iD^{n_1-1}\\ &\qquad + \sum_{i=l+1}^{p} b_iF_i(s)F_iD^{n_i} + \sum_{i=l+1}^{p} n_ib_iF_iD^{n_i-1} = 0.\end{aligned} \tag{5}$$

Multiplying (4) on the left by $F_1(s)$ and subtracting the result from (5) yields

$$\begin{aligned}&\sum_{i=2}^{l} b_i[F_i(s) - F_1(s)]F_iD^{n_1} + \sum_{i=1}^{l} n_1b_iF_iD^{n_1-1}\\ &\qquad + \sum_{i=l+1}^{p} b_i[F_i(s) - F_1(s)]F_iD^{n_i} + \sum_{i=l+1}^{p} n_ib_iF_iD^{n_i-1} = 0.\end{aligned} \tag{6}$$

Suppose $l=1$ in (4). Then (6) reduces to

$$n_1b_1F_1D^{n_1-1} + \sum_{i=2}^{p} b_i[F_i(s) - F_1(s)]F_iD^{n_i} + \sum_{i=2}^{p} n_ib_iF_iD^{n_i-1} = 0. \tag{7}$$

Now in (7) no term in the last sum corresponds to $F_1D^{n_1-1}$ since if $F_1D^{n_1-1}=F_iD^{n_i-1}$ for some $i\geqq 2$, then $F_1D^{n_1}=F_iD^{n_i}$ which contradicts the assumption that the $F_jD^{n_j}$ are distinct. Moreover if $F_1D^{n_1-1}$ appears in a term in the first sum in (7), say $F_1D^{n_1-1}=F_iD^{n_i}$ for some $i\geqq 2$, then its coefficient is zero since $F_1=F_i$ by the lemma. Therefore $F_1D^{n_1-1}$ appears in (7) with the nonzero coefficient n_1b_1. Hence if $l=1$, (7) contradicts the choice of n_1. Suppose $l>1$ in (4). Then, since $n_1>n_1-1\geqq n_{l+1}\geqq n_{l+2}\geqq\cdots\geqq n_p\geqq 0$, in (6) only the first sum contains terms in which D appears to the power n_1. Thus if $F_i(s)\neq F_1(s)$ for some $2\leqq i\leqq l$, then (6) contradicts the choice of l. If, on the other hand, $F_i(s)=F_1(s)$ for each $2\leqq i\leqq l$ then as before (6) contradicts the choice of n_1 since the first sum vanishes and $F_1 D^{n_1-1}$ appears with the nonzero coefficient $n_1 b_1$. Therefore we conclude that no minimum l exists and so the relation (3) holds only if $b_i=0$ for $i=1, 2, \cdots, p$ which concludes the proof.

COROLLARY. *Let E be a field of characteristic zero, D a derivation of E into E, and s an element in E such that $D(s)=1$. Then the collection $\{D^n | n \geqq 0$ is an integer$\}$ is left linearly independent over E.*

ACKNOWLEDGEMENT. The author is grateful to Professor Jiang Luh for his valuable comments.

REFERENCES

1. N. Jacobson, *Lectures in abstract algebra.* Vol. III: *Theory of fields and Galois theory*, Van Nostrand, Princeton, N.J., 1964. MR **30** #3087.

2. C. M. Walters, *Continuous linear transformations on the field of Mikusiński operators*, Ph.D. Thesis, North Carolina State University, Raleigh, N.C., 1971.

AIR FORCE WEAPONS LABORATORY, KIRTLAND AIR FORCE BASE, NEW MEXICO 87117

Current address: Research and Analysis Division, Directorate of Personnel Planning, Headquarters USAF, Washington, D.C. 20330