Separable Endomorphisms and Higher-Order Commutators

DONALD W. ROBINSON
Brigham Young University
Provo, Utah

Communicated by Olga Taussky Todd

1. INTRODUCTION

Let X be a vector space of finite dimension n over an arbitrary field F, and let $\mathfrak{A} = \hom_F(X, X)$ be the algebra of (vector space) endomorphisms on X. For τ and φ in $\mathfrak{A}$, the well-known "double centralizer" theorem states that, if φ commutes with every endomorphism that commutes with τ, then φ is a polynomial in τ over F. In other words, in terms of the commutator mapping Δ_τ: $\mathfrak{A} \to \mathfrak{A}$ given by $\eta\Delta_\tau = \eta\tau - \tau\eta$, if $\varphi\Delta_\eta = 0$ whenever $\eta\Delta_\tau = 0$, then $\varphi \in F(\tau)$. An extension of this result has recently been considered. Specifically, for m any positive integer, it is known that $\varphi\Delta_\eta{}^m = 0$ whenever $\eta\Delta_\tau{}^m = 0$ implies $\varphi \in F(\tau)$. (See [9]; also [6, 12, 14].)

The converse of the classical result $m = 1$ is clearly valid. However, for $m \geqslant 2$, the converse of the extension is not valid. This paper is motivated by the problem of identifying the collection $P_m(\tau)$ of all endomorphisms φ such that $\varphi\Delta_\eta{}^m = 0$ whenever $\eta\Delta_\tau{}^m = 0$. As is shown below, the description of $P_m(\tau)$ depends upon the concept of a separable and semisimple endomorphism. Thus we are lead to an investigation of the relationship between such endomorphisms and higher-order commutators.

2. CHARACTERIZATIONS OF SEMISIMPLE AND SEPARABLE ENDOMORPHISMS

Let μ be the minimum polynomial of τ in $\mathfrak{A}$. The endomorphism τ is said to be semisimple provided that μ is the product of distinct irreducible

Linear Algebra and Its Applications 4(1971), 285–296

polynomials, and is said to be separable provided that each of the irreducible factors of μ is separable (i.e., has a nonzero derivative). (See, for example, [15, p. 679].)

LEMMA 2.1. *Let μ' be the derivative of the minimum polynomial μ of τ in $\mathfrak{A}$. Then the following statements are equivalent:*

(i) *τ is both semisimple and separable.*

(ii) *μ and μ' are relatively prime.*

(iii) *$\mu'(\tau)$ is invertible.*

Proof. Since $\mu = \pi_1^{r_1} \cdots \pi_k^{r_k}$ implies $\mu' = \sum_{i=1}^k r_i \pi_i^{r_i - 1} \pi_i'(\prod_{j \neq i} \cdot \pi_j^{r_j})$, and since an irreducible polynomial π divides both π^r and its derivative $r\pi^{r-1}\pi'$ if and only if either $r > 1$ or both $r = 1$ and $\pi' = 0$, it is clear that $r_i = 1$ and $\pi_i' \neq 0$ for each i if and only if μ and μ' are relatively prime. The lemma is now a consequence of the fact that, for any polynomial ν over F, ν and μ are relatively prime if and only if $\nu(\tau)$ is invertible.

We shall on occasion abbreviate the statement that τ is both semisimple and separable with τ is s.s.s.

Next, for Δ_τ: $\mathfrak{A} \to \mathfrak{A}$, given by $\varphi\Delta_\tau = \varphi\tau - \tau\varphi$, it is easily established by induction on the positive integer m that

$$\varphi\Delta_\tau^m = \sum_{k=0}^{m} (-1)^k \binom{m}{k} \tau^k \varphi \tau^{m-k}.$$

In particular, if F is of characteristic prime p, then, for m a power of p,

$$\varphi\Delta_\tau^{p^e} = \varphi\Delta_{\tau^{p^e}}.$$

Also, for any polynomial f with coefficients in F, it is easily established that

$$\varphi\Delta_\tau^2 = 0 \quad \text{implies} \quad \varphi\Delta_{f(\tau)} = f'(\tau)(\varphi\Delta_\tau),$$

where f' is the derivative of f. (See [10, p. 487].) Finally, let $K(\Delta_\tau^m)$ denote the kernel of Δ_τ^m and let $R(\Delta_\tau) = \bigcup_{m \geq 1} K(\Delta_\tau^m)$ denote the radical of Δ_τ. (See [3, Vol. I, p. 155].) By Fitting's lemma, $R(\Delta_\tau) = K(\Delta_\tau^r)$ for some sufficiently large integer r.

LEMMA 2.2. *Let τ and σ be in $\mathfrak{A}$ such that σ is semisimple and separable. Then $K(\Delta_\tau) \subseteq K(\Delta_\sigma)$ implies $R(\Delta_\tau) \subseteq K(\Delta_\sigma)$.*

Proof. First, let $K(\Delta_\tau) \subseteq K(\Delta_\sigma)$. Since τ is in $K(\Delta_\tau)$, it follows that τ is in $K(\Delta_\sigma)$. That is, τ and σ commute. Hence Δ_τ and Δ_σ commute; this implies by induction on m that $K(\Delta_\tau{}^m) \subseteq K(\Delta_\sigma{}^m)$. Second, let μ be the minimum polynomial of σ. If $\varphi\Delta_\sigma{}^2 = 0$, then $0 = \varphi\Delta_{\mu(\sigma)} = \mu'(\sigma)(\varphi\Delta_\sigma)$; this implies by Lemma 2.1 that $\varphi\Delta_\sigma = 0$. That is, $K(\Delta_\sigma{}^2) \subseteq K(\Delta_\sigma)$; this implies by induction on m that $K(\Delta_\sigma{}^m) \subseteq K(\Delta_\sigma)$. Finally, by the definition of $R(\Delta_\tau)$, the conclusion follows from these two results. (It is of interest to compare this proof with the analogous result in [8] for arbitrary rings.)

It is well known that if τ is cyclic, then the dimension of $K(\Delta_\tau)$ as a subspace of $\mathfrak{A}$ is n, the dimension of X. We now determine the nullity of $\Delta_\tau{}^2$ in this case by the following

LEMMA 2.3. *Let μ be the minimum polynomial of τ in $\mathfrak{A}$. If τ is cyclic, then the dimension of $K(\Delta_\tau{}^2)$ is the dimension of $K(\Delta_\tau)$ plus the nullity of $\mu'(\tau)$.*

Proof. Since τ is cyclic, let X be generated by x relative to τ. Thus each element of X is of the form $xf(\tau)$, where f is a polynomial with coefficients in F. If $xf(\tau) = xg(\tau)$, then $f - g = \mu q$ for some polynomial q, and $f' - g' = \mu' q + \mu q'$; hence $xh(\tau)(f'(\tau) - g'(\tau)) = xh(\tau)\mu'(\tau)q(\tau) = 0$ provided $xh(\tau)$ is in the kernel of $\mu'(\tau)$. That is, for each $xh(\tau) \in \operatorname{Ker} \mu'(\tau)$,

$$\varphi_h\colon \quad X \to X; \quad xf(\tau) \mapsto xh(\tau)f'(\tau)$$

is well defined. Indeed, it is clear that $\varphi_h \in \mathfrak{A}$. Furthermore, if K' is the collection of all such φ_h, then $xh(\tau) \mapsto \varphi_h$ is a (vector space) isomorphism of $\operatorname{Ker} \mu'(\tau)$ to K'. In particular, the mapping is injective since $\varphi_h = \varphi_g$ implies $xh(\tau) = (x\tau)\varphi_h = (x\tau)\varphi_g = xg(\tau)$.

Next, $K(\Delta_\tau{}^2) = K(\Delta_\tau) \oplus K'$. For, by direct computation, $\varphi_h\Delta_\tau = -h(\tau)$. In particular, $\varphi_h\Delta_\tau{}^2 = 0$ and $K' \subseteq K(\Delta_\tau{}^2)$. Also, if $\varphi_h \in K(\Delta_\tau) \cap K'$, then $0 = \varphi_h\Delta_\tau = -h(\tau)$ and $\varphi_h = 0$. Finally, suppose $\varphi \in K(\Delta_\tau{}^2)$. Since X is cyclic with respect to τ and $(\varphi\Delta_\tau)\Delta_\tau = 0$, it follows that $\varphi\Delta_\tau = -h(\tau)$ for some polynomial h, with $0 = \varphi\Delta_{\mu(\tau)} = \mu'(\tau)(\varphi\Delta_\tau) = -\mu'(\tau)h(\tau)$; in other words, $xh(\tau) \in \operatorname{Ker} \mu'(\tau)$. Consequently, since $\varphi\Delta_{f(\tau)} = f'(\tau)(\varphi\Delta_\tau)$ and $x\varphi = xg(\tau)$ for some polynomial g,

$$xf(\tau)\varphi = x\varphi f(\tau) - xf'(\tau)(\varphi\Delta_\tau) = xg(\tau)f(\tau) + xh(\tau)f'(\tau)$$

and $\varphi = g(\tau) + \varphi_h$, where $g(\tau) \in K(\Delta_\tau)$ and $\varphi_h \in K'$.

The conclusion of the lemma is now evident from the preceding facts.

We now state and prove

THEOREM 2.1. *The endomorphism* τ *is semisimple and separable if and only if* $K(\Delta_\tau^2) = K(\Delta_\tau)$.

Proof. First, suppose τ is s.s.s. By use of Lemma 2.2 with $\sigma = \tau$, it follows that $K(\Delta_\tau) \subseteq K(\Delta_\tau^2) \subseteq R(\Delta_\tau) \subseteq K(\Delta_\tau)$. That is, $K(\Delta_\tau^2) = K(\Delta_\tau)$.

Conversely, suppose $K(\Delta_\tau^2) = K(\Delta_\tau)$. Let X be decomposed into a direct sum of subspaces, each of which is invariant and cyclic with respect to τ. In particular, let τ_1 be the restriction on one of these subspaces such that the minimum polynomial of τ_1 is the minimum polynomial μ of τ. Clearly, $K(\Delta_{\tau_1}^2) = K(\Delta_{\tau_1})$. Thus, by Lemma 2.3, the nullity of $\mu'(\tau_1)$ is zero and $\mu'(\tau_1)$ is invertible. Therefore, by Lemma 2.1, μ and μ' are relatively prime and τ is s.s.s.

COROLLARY 2.1. *The endomorphism* τ *is semisimple and separable if and only if* $R(\Delta_\tau) = K(\Delta_\tau)$.

We remark at this point that there are, of course, other ways to prove Theorem 2.1. One way is to introduce the splitting field of the minimum polynomial of τ. Since some of the problems below are not amenable to this technique, we have preferred to avoid it here.

3. SEPARABLE ENDOMORPHISMS AND HIGHER-ORDER COMMUTATORS

We begin with

LEMMA 3.1. *The endomorphism* τ *in* $\mathfrak{A}$ *is separable if and only if there exist in* $\mathfrak{A}$ *a semisimple and separable* σ *and a nilpotent* ρ *such that* $\tau = \sigma + \rho$ *with* $\rho\sigma = \sigma\rho$. *In this case,* σ *and* ρ *are uniquely determined and each is a polynomial in* τ *with coefficients in* F.

Proof. If τ is separable, then the existence and uniqueness of σ and ρ are well known. (See, for example, [15, p. 679].) Conversely, suppose s.s.s. σ and nilpotent ρ exist such that $\tau = \sigma + \rho$ and $\rho\sigma = \sigma\rho$. Let μ be the minimum polynomial of σ. Since

$$\mu(\tau) = \mu(\sigma + \rho) = \mu(\sigma) + \nu(\sigma, \rho)\rho = \nu(\sigma, \rho)\rho$$

for some polynomial ν in two commuting arguments, and ρ is nilpotent, the minimum polynomial of τ divides some power of μ. Thus, since the irreducible factors of μ are separable, the irreducible factors of the minimum polynomial of τ are separable. That is, τ is separable.

The unique endomorphisms σ and ρ of this lemma are called, respectively, the semisimple and nilpotent parts of the separable endomorphism τ.

THEOREM 3.1. *If τ is a separable endomorphism with semisimple part σ, then $R(\Delta_\tau) = K(\Delta_\sigma)$.*

Proof. Since σ is a polynomial in τ, it follows from Lemma 2.2 that $R(\Delta_\tau) \subseteq K(\Delta_\sigma)$. On the other hand, let ρ be the nilpotent part of τ and suppose $\varphi \in K(\Delta_\sigma)$. Since τ and ρ commute, Δ_τ and Δ_ρ commute. Thus, from the fact that $\varphi\Delta_\sigma = 0$, by induction on k

$$\varphi\Delta_\tau{}^k = \varphi\Delta_\rho{}^k = \sum_{j=0}^{k} (-1)^j \binom{k}{j} \rho^j \varphi \rho^{k-j},$$

which is zero for k sufficiently large. That is, $\varphi \in R(\Delta_\tau)$ and $K(\Delta_\sigma) \subseteq R(\Delta_\tau)$.

COROLLARY 3.1. *Let τ be separable with nilpotent part ρ of nilpotent index m. If $\varphi \in R(\Delta_\tau)$, then $\varphi\Delta_\tau{}^k = 0$ for some $k \leqslant 2m - 1$.*

Theorem 3.1 and its corollary extend known results on higher-order commutators under the assumption that the irreducible factors of the minimum polynomial μ of τ are linear. (See [7, 10].)

4. INSEPARABLE ENDOMORPHISMS AND HIGHER-ORDER COMMUTATORS

If the endomorphism τ is not separable, then the base field F is necessarily of prime characteristic p and we proceed as follows.

LEMMA 4.1. *Let F be of characteristic prime p. If $\tau \in \mathfrak{A}$, then there exists a nonnegative integer e such that τ^{p^e} is semisimple and separable.*

Proof. Since $R(\Delta_\tau)$ is the radical of Δ_τ, there is an e such that $K(\Delta_\tau{}^{p^e}) = R(\Delta_\tau)$. If $\varphi\Delta^2_{\tau^{p^e}} = 0$, then $\varphi\Delta_\tau{}^{2p^e} = 0$ and therefore $\varphi\Delta_{\tau^{p^e}} = \varphi\Delta_\tau{}^{p^e} = 0$. By Theorem 2.1, τ^{p^e} is s.s.s.

In particular, there is a nonnegative integer e such that τ^{p^e} is separable.

THEOREM 4.1. *Let F be of characteristic prime p and let τ be in $\mathfrak{A}$. If τ^{p^e} is separable with semisimple part σ, then $R(\Delta_\tau) = K(\Delta_\sigma)$.*

Proof. Let σ and ρ be the semisimple and nilpotent parts of τ^{p^e}. Since σ is a polynomial in τ^{p^e}, it follows from Lemma 2.2 that $R(\Delta_\tau) \subseteq K(\Delta_\sigma)$. On the other hand, let ρ be nilpotent of index m and suppose $\varphi \in K(\Delta_\sigma)$. As in the separable case above, $\varphi\Delta^k_{\tau^{p^e}} = \varphi\Delta_\rho{}^k$ for every positive integer k. In particular,

$$\varphi\Delta_\tau{}^{(2m-1)p^e} = \varphi\Delta^{2m-1}_{\tau^{p^e}} = \varphi\Delta_\rho{}^{2m-1} = 0.$$

That is, $\varphi \in R(\Delta_\tau)$ and $K(\Delta_\sigma) \subseteq R(\Delta_\tau)$.

COROLLARY 4.1. *Let the conditions be as in Theorem 4.1 and let the nilpotent part of τ^{p^e} be nilpotent of index m. If $\varphi \in R(\Delta_\tau)$, then $\varphi\Delta_\tau{}^k = 0$ for some $k \leqslant (2m-1)p^e$.*

COROLLARY 4.2. *Let d be the least nonnegative integer e such that τ^{p^e} is separable, and let σ and ρ be the semisimple and nilpotent parts of τ^{p^d}. Then*

(i) *τ^{p^e} is separable and $F(\sigma^{p^{e-d}}) = F(\sigma)$ for every $e \geqslant d$;*

(ii) *τ^{p^e} is semisimple and separable and $F(\tau^{p^e}) = F(\sigma)$ whenever $\rho^{p^{e-d}} = 0$.*

Proof. Since $\tau^{p^d} = \sigma + \rho$ and $\sigma\rho = \rho\sigma$ with σ s.s.s. and ρ nilpotent, it follows that $\tau^{p^e} = \sigma^{p^{e-d}} + \rho^{p^{e-d}}$, $\sigma^{p^{e-d}}$ commutes with $\rho^{p^{e-d}}$, $\sigma^{p^{e-d}}$ is s.s.s. and $\rho^{p^{e-d}}$ is nilpotent. Hence, by Lemma 3.1, τ^{p^e} is separable, and $\tau^{p^e} = \sigma^{p^{e-d}}$ is s.s.s. whenever $\rho^{p^{e-d}} = 0$. Therefore, by Theorem 4.1, $K(\Delta_\sigma) = R(\Delta_\tau) = K(\Delta_{\sigma^{p^{e-d}}})$. Consequently, since σ commutes with every endomorphism that commutes with $\sigma^{p^{e-d}}$, σ is a polynomial in $\sigma^{p^{e-d}}$ and $F(\sigma^{p^{e-d}}) = F(\sigma)$. Furthermore, if $\rho^{p^{e-d}} = 0$, then $\tau^{p^e} = \sigma^{p^{e-d}}$ and $F(\tau^{p^e}) = F(\sigma)$.

This completes the proof of the corollary, which says in particular that τ^{p^e} is s.s.s. and $F(\tau^{p^e}) = F(\sigma)$ for all e sufficiently large.

5. APPLICATIONS

In this section we apply the preceding results to several problems. The first is an extension of a theorem due to W. E. Roth. (See [10]; also [7].)

THEOREM 5.1. *If f and g are polynomials with coefficients in F, then $\varphi \in R(\Delta_\tau)$ implies $f(\varphi) \in R(\Delta_{g(\tau)})$.*

Proof. Suppose F is of characteristic zero. It is evident from Lemma 3.1 that, if σ is the semisimple part of τ, then $g(\sigma)$ is the semisimple part of $g(\tau)$. Thus, if $\varphi \in R(\Delta_\tau) = K(\Delta_\sigma)$, then $f(\varphi) \in K(\Delta_{g(\sigma)}) = R(\Delta_{g(\tau)})$.

Suppose F is of characteristic prime p. By Lemma 4.1, let τ^{p^e} be s.s.s. Suppose $\varphi\Delta_\tau^{\,k} = 0$. Then $\varphi\Delta^{k}_{\tau^{p^e}} = \varphi\Delta_\tau^{\,kp^e} = 0$, which implies by Corollary 2.1 that $\varphi\Delta_{\tau^{p^e}} = 0$. Hence

$$f(\varphi)\Delta^{p^e}_{g(\tau)} = f(\varphi)\Delta_{(g(\tau))^{p^e}} = f(\varphi)\Delta_{g^{(p^e)}(\tau^{p^e})} = 0,$$

where $g^{(p^e)}$ is the polynomial whose coefficients are, respectively, the p^e powers of the coefficients of g. That is, $\varphi \in R(\Delta_\tau)$ implies $f(\varphi) \in R(\Delta_{g(\tau)})$.

An endomorphism is said to be primary provided its minimum polynomial is a power of an irreducible polynomial. We now provide a sufficient condition for a set of endomorphisms to be simultaneously decomposed into a direct sum of primary endomorphisms.

THEOREM 5.2. *Let Ω be a subset of $\mathfrak{A}$ and let Ω_0 be a nonempty subset of Ω. If $\varphi \in R(\Delta_\tau)$ for every $\varphi \in \Omega$ and every $\tau \in \Omega_0$, then there exist subspaces $X_1, \ldots, X_k$ of X such that $X = X_1 \oplus \cdots \oplus X_k$, each X_i is invariant under Ω, and the restriction of each endomorphism of Ω_0 to each X_i is primary.*

Proof. If the minimum polynomial of every endomorphism of Ω_0 is a prime power, then the conclusion is trivially valid for $k = 1$ and $X = X_1$. Otherwise, there is a $\tau \in \Omega_0$ that is not primary, and $X = X\varepsilon_1 \oplus \cdots \oplus X\varepsilon_s$, where $\varepsilon_1, \ldots, \varepsilon_s$ are the primary idempotents of τ. (See, for example, [3, Vol. II, p. 132].) Since ε_j is a polynomial in τ and is s.s.s., and since by hypothesis $\varphi \in R(\Delta_\tau)$, it follows from Theorem 5.1 that $\varphi \in R(\Delta_{\varepsilon_j}) = K(\Delta_{\varepsilon_j})$. Therefore φ commutes with ε_j and the primary component $X\varepsilon_j$ of τ is invariant under φ. If the restriction of each $\tau \in \Omega_0$ is primary on each $X\varepsilon_j$, the proof is complete. Otherwise, there is a $\tau' \in \Omega_0$ whose restriction to some component is not primary, and the argument can be repeated on this component. Since the dimension of X is finite, repetition of this argument a finite number of times leads to the desired conclusion.

This theorem contains as a special case an important result on nilpotent Lie algebras. (See [4, pp. 40–41].) It also includes Lemma 3 of [1]; compare also [13] and [11, Theorem 1].

The converse is not in general valid. For example, let F be the rational field, X have basis $\{x_1, x_2\}$, and the set $\Omega = \Omega_0$ consist of the two endomorphisms,

$$\tau\colon\quad x_1 \mapsto x_2, \quad x_2 \mapsto -x_1; \qquad \varphi\colon\quad x_1 \mapsto 2x_2, \quad x_2 \mapsto x_1.$$

Since the minimum polynomials of these endomorphisms are, respectively, $\lambda^2 - 1$ and $\lambda^2 - 2$, both of which are irreducible over the rational field, the conclusion of the theorem is trivially satisfied for $X = X_1$. But $\varphi \notin R(\Delta_\tau) = K(\Delta_\tau)$.

However, if, for every $\tau \in \Omega_0$ the minimum polynomial of τ is completely reducible over F, then the converse of the theorem is valid. Indeed, let such a decomposition be given, and let $\varphi \in \Omega$ and $\tau \in \Omega_0$. Under the assumption that the characteristic values of τ belong to F, τ is separable and the restriction of the semisimple part of τ is a scalar transformation on each component X_i. Thus φ commutes with the semisimple part of τ and $\varphi \in R(\Delta_\tau)$.

In particular, if F is taken to be the complex field rather than the rational field in the preceding example, we note that it is impossible to obtain a decomposition of X that meets the required conditions of the theorem.

Next, we consider some results that are related to the following classical theorem: φ commutes with every endomorphism that commutes with τ if and only if φ is a polynomial in τ. (See [3, Vol. II, p. 113], [5, p. 536], or [16, p. 106].) In other words, $\varphi \in K(\Delta_\eta)$ whenever $\eta \in K(\Delta_\tau)$ if and only if $\varphi \in F(\tau)$.

The first result to be given is the following

THEOREM 5.3. *Let τ and φ be in $\mathfrak{A}$. If F is of characteristic zero, then let σ be the semisimple part of τ. If F is of characteristic prime p, then let τ^{p^e} be separable with semisimple part σ. Then $\varphi \in R(\Delta_\eta)$ whenever $\eta \in R(\Delta_\tau)$ if and only if $\varphi \in F(\sigma)$.*

This theorem is a corollary of the following

LEMMA 5.1. *Let the conditions be as in Theorem* 5.3. *Then the following statements are equivalent*:

(i) $\varphi \in R(\Delta_\eta)$ *whenever* $\eta \in R(\Delta_\tau)$.

(ii) $\varphi \in F(\sigma)$.

(iii) $\varphi \in K(\Delta_\eta)$ *whenever* $\eta \in R(\Delta_\tau)$.

Proof. Let $\varphi \in R(\Delta_\eta)$ whenever $\eta \in R(\Delta_\tau)$. We show that φ is a polynomial in σ by showing that φ commutes with σ and with every idempotent that commutes with σ. (See [2].) First, since σ commutes with τ, it follows that $\sigma \in R(\Delta_\tau)$, which requires by hypothesis that $\varphi \in R(\Delta_\sigma)$. But, since σ is s.s.s., $\varphi \in K(\Delta_\sigma)$; that is, φ commutes with σ. Second, suppose ε is an idempotent endomorphism that commutes with σ; then $\varepsilon \in K(\Delta_\sigma) = R(\Delta_\tau)$. Again, by hypothesis and the fact that ε is s.s.s., $\varphi \in R(\Delta_\varepsilon) = K(\Delta_\varepsilon)$. Consequently, φ commutes with ε. That is, (i) implies (ii).

Next, to show that (ii) implies (iii), let $\varphi \in F(\sigma)$ and suppose $\eta \in R(\Delta_\tau)$. By Theorems 3.1 and 4.1, $\eta \in K(\Delta_\sigma)$. That is, since η commutes with σ and φ is a polynomial in σ, it follows that φ commutes with η and $\varphi \in K(\Delta_\eta)$.

Since (iii) obviously implies (i), the proof of the lemma is complete.

A related result is the following

THEOREM 5.4. *Let F be of characteristic zero or prime $p \geqslant n$, let $m \geqslant 2$ be an integer, and let τ and φ be in $\mathfrak{A}$. Then the following statements are equivalent*:

(i) $\varphi \in K(\Delta_\eta)$ *whenever* $\eta \in R(\Delta_\tau)$.

(ii) $\varphi \in K(\Delta_\eta^m)$ *whenever* $\eta \in K(\Delta_\tau^m)$.

(iii) $\varphi \in R(\Delta_\eta)$ *whenever* $\eta \in K(\Delta_\tau^2)$.

Proof. The implications (i) implies (ii) and (ii) implies (iii) are trivial. Moreover, since $R(\Delta_\eta) = K(\Delta_\eta)$ whenever η is s.s.s., it is also clear that (iii) implies

(iv) $\varphi \in K(\Delta_\eta)$ *whenever* $\eta \in K(\Delta_\tau^2)$ *and* η *is* s.s.s.

Thus we complete the proof of the theorem by showing, under the given restrictions on the characteristic of F, that (iv) implies (i).

Now, given F to be of characteristic zero or prime $p \geqslant n$, since the minimum polynomial of τ is of degree at most n, either τ is separable or $p = n$ and the minimum polynomial of τ is irreducible and of the form $\lambda^p - a$, where $a \in F$. (See, for example, [17, p. 65].)

We first consider the case where τ is separable and let φ satisfy (iv). By the first theorem of [9] it is known that $\varphi = f(\tau)$ is a polynomial in φ with coefficients in F. Thus, if σ and ρ are the semisimple and nilpotent parts of τ,

$$\varphi = f(\sigma + \rho) = f(\sigma) + f_1(\sigma)\rho + \cdots + f_{r-1}(\sigma)\rho^{r-1},$$

where r is the index of nilpotency of ρ. We now show that actually $\varphi = f(\sigma)$; hence, by Lemma 5.1, property (i) is satisfied.

To show that φ is a polynomial in σ we recall that X may be decomposed into a direct sum of subspaces X_j such that each is invariant under τ and the restriction τ_j of τ to X_j is cyclic and primary. Since each X_j is also invariant under $\varphi = f(\tau)$, it follows that property (iv) holds for the restrictions of the endomorphisms to X_j. Thus, if it can be shown that this requires $\varphi_j = f(\sigma_j)$, where φ_j and σ_j are the restrictions of φ and σ to X_j, then the conclusion follows. Consequently, without loss of generality, assume τ to be cyclic with minimum polynomial π^r, where π is irreducible and of degree s. In this case σ has minimum polynomial π and ρ is nilpotent of index r. Since τ is cyclic, there is an x such that every vector of X is of the form

$$xg(\tau) = xg(\sigma + \rho) = xg(\sigma) + xg_1(\sigma)\rho + \cdots + xg_{r-1}(\sigma)\rho^{r-1}.$$

That is, X is spanned by the rs vectors $\{x\sigma^i\rho^j | 0 \leqslant i < s,\ 0 \leqslant j < r\}$, and therefore this set is a basis of X. Let $\delta \in \mathfrak{A}$ be given by $\delta\colon\ x\sigma^i\rho^j \mapsto jx\sigma^i\rho^j$. By direct computation, $\delta\Delta_\tau = -\rho$, and δ has minimum polynomial $\lambda(\lambda - 1) \cdots (\lambda - (r-1))$. That is $\delta\Delta_\tau^2 = 0$ and δ is s.s.s. and, by property (iv), $\varphi\Delta_\delta = 0$. Therefore,

$$0 = x(\varphi\delta - \delta\varphi) = x(f_1(\sigma)\rho + 2f_2(\sigma)\rho^2 + \cdots + (r-1)f_{r-1}(\sigma)\rho^{r-1}),$$

and, since $\{x\sigma^i\rho^j\}$ is a basis of X, $f_1(\sigma) = 0, 2f_2(\sigma) = 0, \ldots, (r-1)f_{r-1}(\sigma) = 0$. But, since F is of characteristic zero or prime $p \geqslant n \geqslant r$, $f_1(\sigma) = 0$, $f_2(\sigma) = 0, \ldots, f_{r-1}(\sigma) = 0$ and $\varphi = f(\sigma)$, as was to be shown.

Next, let $p = n$ and let $\lambda^p - a$ be the irreducible minimum polynomial of τ. Since τ is cyclic, there is an x such that $\{x, x\tau, \ldots, x\tau^{p-1}\}$ is a basis of X. Define the endomorphism $\delta\colon\ x\tau^j \mapsto jx\tau^j$ and let $\omega = \delta + \tau\delta$. By direct calculation $\delta\Delta_\tau = -\tau$. Thus $\delta\Delta_\tau^2 = 0$ and $\omega\Delta_\tau^2 = 0$. Also, since $\lambda(\lambda-1)\cdots(\lambda-(p-1))$ is the minimum polynomial of both δ and ω, both are s.s.s. Thus property (iv) implies φ commutes with both δ and ω. But this requires φ to be a scalar endomorphism and (i) is satisfied.

This completes the proof of the theorem. Furthermore, from the proof it is clear that the properties of the theorem are also equivalent to the property that either τ is separable and φ is a polynomial in the semisimple part of τ or φ is simply a scalar endomorphism.

It is also of interest to note that the restriction on the characteristic of the field cannot be relaxed. Indeed let F be of characteristic prime $p < n$, and let τ be nilpotent of index n and $\varphi = \tau^p$.

First, if $m = p^e \geqslant n$, then (iii) is satisfied but not (ii). For, if $\eta\Delta_\tau^2 = 0$, then, since $p \geqslant 2$, $\eta\Delta_{\tau^p} = \eta\Delta_\tau^p = 0$ and $\varphi = \tau^p \in K(\Delta_\eta) \subseteq R(\Delta_\eta)$; that is, (iii) is satisfied. On the other hand, with $\{x, x\tau, \ldots, x\tau^{n-1}\}$ a basis of X, let $\zeta \in \mathfrak{A}$ be given by $\zeta\colon x \mapsto x,\ x\tau^j \to 0,\ j = 1, \ldots, n-1$. Since $m = p^e \geqslant n$, it follows that $\tau^m = 0$ and $\zeta\Delta_\tau^m = \zeta\Delta_{\tau m} = 0$. But, since ζ is s.s.s. and $\varphi\Delta_\zeta \neq 0$, it follows that $\varphi\Delta_\zeta^m \neq 0$ and (ii) is not satisfied.

Second, if $m \leqslant p$, then (ii) is satisfied but not (i). For, if $\eta\Delta_\tau^m = 0$, then $\eta\Delta_\varphi = \eta\Delta_{\tau^p} = \eta\Delta_\tau^p = 0$; that is, $\varphi\Delta_\eta^m = 0$, and (ii) is satisfied. But ζ as given in the preceding paragraph does not commute with $\varphi = \tau^p$, yet, since τ is nilpotent, $\zeta \in R(\Delta_\tau)$; hence (i) is not satisfied.

We now conclude this paper with an identification of the collection $P_m(\tau)$ of endomorphisms φ such that $\varphi \in K(\Delta_\eta^m)$ whenever $\eta \in K(\Delta_\tau^m)$.

THEOREM 5.5. *Let τ be an endomorphism and let m be a positive integer. If F is of characteristic zero and σ is the semisimple part of τ, then $P_1(\tau) = F(\tau)$ and $P_m(\tau) = F(\sigma)$ for $m \geqslant 2$. If F is of characteristic prime p and e is the nonnegative integer determined by $p^{e-1} < m \leqslant p^e$, then $P_m(\tau) = F(\tau^{p^e})$.*

Proof. First, let F be of characteristic zero. If $m = 1$, then the conclusion is the classical result mentioned above. If $m \geqslant 2$, then, by Lemma 5.1 and Theorem 5.4, $P_m(\tau) = F(\sigma)$.

Second, let F be of characteristic prime p and let e be the nonnegative integer determined by $p^{e-1} < m \leqslant p^e$. By the second theorem of [9], $P_m(\tau) \subseteq F(\tau^{p^e})$. Conversely, let $\varphi \in F(\tau^{p^e})$ and suppose $\eta\Delta_\tau^m = 0$. Then $\eta\Delta_{\tau^{p^e}} = \eta\Delta_\tau^{p^e} = 0$. Therefore $\varphi\Delta_\eta = 0$ and $\varphi\Delta_\eta^m = 0$. That is, $F(\tau^{p^e}) \subseteq P_m(\tau)$, and the proof is complete.

It is of interest to note that, if τ^{p^d} is separable with semisimple part σ and nilpotent part ρ and $\rho^{p^{e-d}} = 0$, then by (ii) of Corollary 4.2, $F(\tau^{p^e}) = F(\sigma)$. That is, for all sufficiently large m, $P_m(\tau) = F(\sigma)$.

Finally, we remark that both Lemma 3 and Theorem 2 of [6] are special cases of Theorem 5.5.

REFERENCES

1 F. J. Gaines and R. C. Thompson, Sets of nearly triangular matrices, *Duke Math. J.* **35**(1968), 941–953.

2 H. L. Hamburger, A theorem on commutative matrices, *J. London Math. Soc.* **24**(1949), 200–206.

3 N. Jacobson, *Lectures in Abstract Algebra*, Vols. I, II, Van Nostrand, Princeton, N.J., 1951, 1953.

4 N. Jacobson, *Lie Algebras*, Interscience Tracts in Pure and Applied Mathematics, No. 10, Interscience Publishers, New York, 1962.

5 P. Lagerstrom, A proof of a theorem on commutative matrices, *Bull. Amer. Math. Soc.* **51**(1945), 535–536.

6 M. Marcus and N. A. Kahn, On matrix commutators, *Canad. J. Math.* **12**(1960), 269–277.

7 D. W. Robinson, A note on k-commutative matrices, *J. Mathematical Phys.* **2**(1961), 776–777.

8 D. W. Robinson, A note on additive commutators in a ring, *Amer. Math. Monthly* **72**(1965), 1106–1107.

9 D. W. Robinson, On matrix commutators of higher order, *Canad. J. Math.* **17** (1965), 527–532.

10 W. E. Roth, On k-commutative matrices, *Trans. Amer. Math. Soc.* **39**(1936), 483–495.

11 I. Sinha, Reduction of sets of matrices to a triangular form, *Pacific J. Math.* **15**(1965), 673–679.

12 M. F. Smiley, Matrix commutators, *Canad. J. Math.* **13**(1961), 353–355.

13 Olga Taussky, A generalization of matrix commutativity, *Linear Algebra* **2**(1969), 349–353.

14 Olga Taussky, Matrix commutators of higher order, *Bull. Amer. Math. Soc.* **69**(1963), 738.

15 S. Warner, *Modern Algebra*, Vol. II, Prentice-Hall, Englewood Cliffs, N.J., 1965.

16 J. H. M. Wedderburn, *Lectures on Matrices, Amer. Math. Soc. Colloq. Publ.*, Vol. 17, New York, 1934.

17 O. Zariski and P. Samuel, *Commutative Algebra*, Vol. I, Van Nostrand, Princeton, N.J., 1958.

Received September, 1969