A CLASS OF BILINEAR FORMS

BY
HOWARD A. OSBORN

1. **Introduction.** Let K be an arbitrary field of characteristic $\neq 2$, E a finite dimensional vector space over K, and A an endomorphism of E. What is the structure of the class $\mathcal{C}(A)$ of bilinear forms f on $E \times E$ such that A is self-adjoint with respect to f? The forms in $\mathcal{C}(A)$ need not be positive definite in any sense, or even symmetric; the only requirement is that $f(Au, v) = f(u, Av)$ for all $(u, v) \in E \times E$.

It will be convenient to treat two related problems first. Define the bilinear form fA by setting $fA(u, v) = f(u, Av)$, let $\mathcal{S}(A)$ denote the class of symmetric forms f such that fA is also symmetric, and let $\mathcal{A}(A)$ denote the class of alternating forms f such that fA is also alternating. Then $\mathcal{S}(A)$ and $\mathcal{A}(A)$ may be described explicitly, and one easily shows that $\mathcal{C}(A) = \mathcal{S}(A) \oplus_K \mathcal{A}(A)$, which solves the original problem.

Let $\mathfrak{C}(A)$ denote the centralizer of A in the ring $\mathfrak{R}$ of all endomorphisms of E. Then $\mathcal{C}(A)$ is a right $\mathfrak{C}(A)$-module in a natural way, which is isomorphic to the right $\mathfrak{C}(A)$-module $\mathfrak{C}(A)$. This isomorphism may be developed further by considering $\mathcal{C}(A)$ and $\mathfrak{C}(A)$ as modules for the ring $\mathfrak{A}$ of endomorphisms of E which is generated by A and scalar multiplications. By means of the induced $\mathfrak{A}$-isomorphism one easily describes $\mathfrak{C}(A)$ as an $\mathfrak{A}$-module, obtaining Frobenius' theorem on $\dim_K \mathfrak{C}(A)$ as a trivial corollary. In fact, $\mathfrak{C}(A)$ may be considered as an algebra over $\mathfrak{A}$, that is, $\mathfrak{C}(A)$ admits $\mathfrak{A}$ as a ring of operators, and the submodules $\mathfrak{S}(A)$ and $\mathfrak{L}(A)$ which are $\mathfrak{A}$-isomorphic to $\mathcal{S}(A)$ and $\mathcal{A}(A)$, respectively, become Jordan and Lie algebras over $\mathfrak{A}$, with the usual definitions of products. Multiplication tables may be written out explicitly.

The final portions of the paper are devoted to matrix representations of $\mathcal{C}(A)$ and $\mathfrak{C}(A)$.

The author wishes to thank Professor Nathan Jacobson for his interest in the problem.

2. **The vector spaces** $\mathcal{S}(A)$, $\mathcal{A}(A)$, **and** $\mathcal{C}(A)$. Let $\mathfrak{A}$ be the commutative ring of endomorphisms of E which is generated by A and scalar multiplications, and regard E as an $\mathfrak{A}$-module. E is *cyclic* if it contains an element z such that $\mathfrak{A}z = E$, and a classical decomposition theorem states that in any event E is the direct sum of cyclic submodules, $E = E_1 \oplus \cdots \oplus E_t$, such that if $\mathfrak{J}(E_i)$ is the order ideal of E_i, then $i \leqq j$ implies that $\mathfrak{J}(E_i) \supseteq \mathfrak{J}(E_j)$. The decomposition is unique except in the case of submodules of equal dimension over K.

Presented to the Society, June 15, 1957; received by the editors May 10, 1957.

Since each E_i is cyclic, there exists an element $z_i \in E_i$, called an E_i-*generator*, such that $\mathfrak{A}z_i = \mathfrak{A}/\mathfrak{J}(E_i)z_i = E_i$, $i=1, \cdots, t$. We shall assume that $z_1, \cdots, z_t$ have been chosen once and for all.

LEMMA 1. *There is a unique isomorphism $u_i \to u_i^*$ of E_i onto $\mathfrak{A}/\mathfrak{J}(E_i)$ such that $u_i^* z_i = u_i$ for any $u_i \in E_i$.*

Proof. Clearly any such map is a homomorphism of E_i into $\mathfrak{A}/\mathfrak{J}(E_i)$, and at least one u_i^* exists, since z_i is an E_i-generator. Suppose that $Bz_i = 0$ for some $B \in \mathfrak{A}$. Then $BE_i = B\mathfrak{A}z_i = \mathfrak{A}Bz_i = 0$ so that $B \in \mathfrak{J}(E_i)$. Finally, to prove that the isomorphism is onto, let B be any element of $\mathfrak{A}/\mathfrak{J}(E_i)$, and set $Bz_i = y_i$. Then for any $x_i \in E_i, Bx_i = Bx_i^* z_i = x_i^* B z_i = x_i^* y_i = x_i^* y_i^* z_i = y_i^* x_i^* z_i = y_i^* x_i$, so that $B = y_i^*$.

Clearly z_i^* is the identity of $\mathfrak{A}/\mathfrak{J}(E_i)$ and $u_i^* v_i = u_i^* v_i^* z_i = v_i^* u_i^* z_i = v_i^* u_i$. Furthermore, if $i \leqq j$, $u_j^* v_i$ is a well-defined element of E_i, since $\mathfrak{J}(E_i) \supseteq \mathfrak{J}(E_j)$.

LEMMA 2. *If $B \in \mathfrak{A}/\mathfrak{J}(E_i)$ and $u_i \in E_i$, then $(Bu_i)^* = Bu_i^*$.*

Proof. Let v_i be any element of E_i. Then $(Bu_i)^* v_i = (Bu_i)^* v_i^* z_i = v_i^* (Bu_i)^* z_i = v_i^* B u_i = v_i^* B u_i^* z_i = B u_i^* v_i^* z_i = B u_i^* v_i$.

Let E_i' be the conjugate space of E_i. Then E_i' is also an $\mathfrak{A}/\mathfrak{J}(E_i)$-module. In fact, if $\mathfrak{R}_i$ represents the ring of all endomorphisms of E_i, then E_i is a left $\mathfrak{R}_i$-module and E_i' is a right $\mathfrak{R}_i$-module. We shall follow this convention and consider E_i' as a right $\mathfrak{A}/\mathfrak{J}(E_i)$-module even though $\mathfrak{A}/\mathfrak{J}(E_i)$ is commutative. The bilinear pairing of $E_i \times E_i'$ into K will be written as $u_i \times u_i' \to \langle u_i', u_i \rangle$ so that $\langle u_i' B, u_i \rangle = \langle u_i', Bu_i \rangle$ for all $B \in \mathfrak{A}/\mathfrak{J}(E_i)$.

THEOREM 1. *Let x_j' be an arbitrary linear functional on $E_1 \oplus \cdots \oplus E_j$, $j=1, \cdots, t$. Then there exists a unique $f \in \mathcal{S}(A)$ such that $\langle x_j', x_j \rangle = f(x_j, z_j)$ for all $x_j \in E_1 \oplus \cdots \oplus E_j$, $j=1, \cdots, t$.*

Proof. The functional x_j' is uniquely the sum of functionals $x_{1j}', \cdots, x_{jj}'$ on $E_1, \cdots, E_j$, respectively. If u_i and v_i are the projections of $u \in E$ and $v \in E$ on E_i, then the bilinear form f such that

$$f(u, v) = \sum_{1 \leq j \leq t} \langle x_{jj}', \overset{*}{u}_j v_j \rangle + \sum_{1 \leq i < j \leq t} \langle x_{ij}', \overset{*}{v}_j u_i + \overset{*}{u}_j v_i \rangle$$

is an element of $\mathcal{S}(A)$ satisfying the conditions of the theorem. To show uniqueness suppose that $x_j' = 0$, $j=1, \cdots, t$. Then for any $f \in \mathcal{S}(A)$ corresponding to these functionals,

$$f(u_i, v_j) = f(u_i, \overset{*}{v}_j z_j) = f(\overset{*}{v}_j u_i, z_j) = 0$$

when $i \leqq j$, and since f is symmetric it follows that $f = 0$.

THEOREM 2. *Suppose that E is not cyclic and let y_j' be an arbitrary linear functional on $E_1 \oplus \cdots \oplus E_{j-1}$, $j=2, \cdots, t$. Then there exists a unique*

$f \in \mathcal{A}(A)$ such that $\langle y'_j, y_j\rangle = f(y_j, z_j)$ for all $y_j \in E_1 \oplus \cdots \oplus E_{j-1}$, $j = 2, \cdots, t$.

Proof. The functional y'_j is uniquely the sum of functionals $y'_{1j}, \cdots, y'_{j-1,j}$ on $E_1, \cdots, E_{j-1}$, and one verifies that the bilinear form f such that

$$f(u, v) = \sum_{1 \leq i < j \leq t} \langle y'_{ij}, \overset{*}{v}_j u_i - \overset{*}{u}_j v_i\rangle$$

is an element of $\mathcal{A}(A)$ satisfying the conditions of the theorem. Uniqueness follows as in the preceding theorem.

THEOREM 3. $\mathcal{C}(A) = \mathcal{S}(A) \oplus_K \mathcal{A}(A)$.

Proof. If $f \in \mathcal{C}(A)$ then decompose f into its symmetric and alternating parts, $f = s + a$; the decomposition is unique since char $K \neq 2$. For any $(u, v) \in E \times E$ one obtains $sA(v, u) - sA(u, v) = aA(u, v) + aA(v, u)$, and since the left- and right-hand sides are alternating and symmetric, respectively, it follows that both sides vanish. Hence sA and aA are symmetric and alternating, respectively, so that $s \in \mathcal{S}(A)$ and $a \in \mathcal{A}(A)$ as asserted.

Note that even in the absence of the hypothesis char $K \neq 2$, $\mathcal{C}(A)$ is spanned by forms of the types given by $f(u, v) = \langle x'_{ij}, v_j^* u_i\rangle$ and $f(u, v) = \langle x'_{ij}, u_j^* v_i\rangle$.

COROLLARY 1. *$\dim_K \mathcal{S}(A) = \sum_{j=1}^{t} (t - j + 1) \dim_K E_j$, $\dim_K \mathcal{A}(A) = \sum_{j=1}^{t} (t - j) \dim_K E_j$, and $\dim_K \mathcal{C}(A) = \sum_{j=1}^{t} (2t - 2j + 1) \dim_K E_j$.*

THEOREM 4. *$\mathcal{S}(A)$ contains a nondegenerate form.*

Proof. The conjugate spaces $E'_1, \cdots, E'_t$ are also cyclic. Let z'_j generate E'_j and consider the element $f \in \mathcal{S}(A)$ given by $f(u, v) = \sum_{1 \leq j \leq t} \langle z'_j, u_j^* v_j\rangle$.

Theorem 4 may be used to express the similarity of an arbitrary matrix (A) to its transpose. If f is any nondegenerate form there exists an isomorphism $\bar{f}$ of E onto E' such that $\langle \bar{f}(v), u\rangle = f(u, v)$, that is, $\bar{f}$ is the correlation corresponding to f. The matrix representations (f) and $(\bar{f})$ of f and $\bar{f}$ are identical and invertible since f is nondegenerate. Furthermore if $f \in \mathcal{S}(A)$ then $(\bar{f})$ and $(\bar{f})(A)$ are symmetric so that $(\bar{f})(A) = {}^t(A)^t(\bar{f}) = {}^t(A)(\bar{f})$; that is, ${}^t(A) = (\bar{f})(A)(\bar{f})^{-1}$ as desired.

3. **The $\mathfrak{A}$-modules $\mathcal{C}(A)$ and $\mathfrak{S}(A)$.** Let $\mathfrak{R}$ be the ring of all endomorphisms of E, and consider E and E' as left and right $\mathfrak{R}$-modules, respectively. Let $B \in \mathfrak{R}$ and $C \in \mathfrak{R}$, and let f be an arbitrary bilinear form on $E \times E$. Then for all $(u, v) \in E \times E$, $(fB)\mathcal{C}(u, v) = fB(u, Cv) = f(u, BCv) = f(BC)(u, v)$, so that $(fB)C = f(BC)$. Thus the K-linear space $\mathcal{B}$ of all bilinear forms on $E \times E$ is a right $\mathfrak{R}$-module with the composition $f \cdot B = fB$. The following lemma is well-known.

LEMMA 3. *If f is any nondegenerate bilinear form on $E \times E$, then the map $B \rightarrow fB$ is an isomorphism of the right $\mathfrak{R}$-module $\mathfrak{R}$ onto the right $\mathfrak{R}$-module $\mathcal{B}$.*

Proof. Trivially $B \to fB$ is a homomorphism of $\mathfrak{R}$ into $\mathcal{B}$. Now let $\bar{f}$ represent the correlation $E \to E'$ which corresponds to f. If $fB=0$ then $\bar{f} \circ B=0$ hence $B=\bar{f}^{-1} \circ \bar{f} \circ B=0$, so that $B \to fB$ is an isomorphism. Furthermore for any $g \in \mathcal{B}$ we may define $\bar{g}\colon E \to E'$ by $\langle \bar{g}(v), u\rangle = g(u, v)$ and note that $g(u, v) = \langle \bar{g}(v), u\rangle = \langle \bar{f}(\bar{f}^{-1} \circ \bar{g}(v)), u\rangle = f(u, \bar{f}^{-1} \circ \bar{g}(v)) = f(\bar{f}^{-1} \circ \bar{g})(u, v)$; that is, $g=f(\bar{f}^{-1} \circ \bar{g})$, so that $B \to fB$ is onto.

Let $\mathfrak{C}(A)$ be the centralizer of A in $\mathfrak{R}$; that is, the ring of all endomorphisms which commute with A. If $f \in \mathcal{C}(A)$, and $B \in \mathfrak{C}(A)$ then for all $(u, v) \in E \times E$, $fB(u, Av)=f(u, BAv)=f(u, ABv)=f(Au, Bv)=fB(Au, v)$ so that $\mathcal{C}(A)$ is a right $\mathfrak{C}(A)$-module with the composition $f \cdot B=fB$. Now let f be the nondegenerate element of $\mathcal{S}(A)$ given in Theorem 4 and let Φ denote the corresponding isomorphism of $\mathfrak{R}$ onto $\mathcal{B}$ as in Lemma 3.

LEMMA 4. *Φ induces an isomorphism, which will also be denoted Φ, of the right $\mathfrak{C}(A)$-module $\mathfrak{C}(A)$ onto the right $\mathfrak{C}(A)$-module $\mathcal{C}(A)$.*

Proof. Clearly Φ is a module isomorphism of $\mathfrak{C}(A)$ into $\mathcal{C}(A)$, by Lemma 3 and the preceding remarks. It remains to show that $fB \in \mathcal{C}(A)$ implies $B \in \mathfrak{C}(A)$; that is, that Φ is onto. If $fB \in \mathcal{C}(A)$ then $\langle \bar{f}(ABv), u\rangle = f(u, ABv) = f(Au, Bv) = fB(Au, v) = fB(u, Av) = f(u, BAv) = \langle \bar{f}(BAv), u\rangle$ for all $(u, v) \in E \times E$, hence $\bar{f}(ABv)=\bar{f}(BAv)$ for all $v \in E$. Since $\bar{f}$ possesses an inverse, $ABv=BAv$ for all $v \in E$, hence $AB=BA$; that is, $B \in \mathfrak{C}(A)$ as asserted.

Since $\mathfrak{A} \subset \mathfrak{C}(A)$, $\mathfrak{C}(A)$ and $\mathcal{C}(A)$ are a fortiori isomorphic as $\mathfrak{A}$-modules. We shall study $\mathcal{C}(A)$ as an $\mathfrak{A}$-module and use the results to obtain information about $\mathfrak{C}(A)$.

If $i \leqq j$ let $\mathcal{C}_{ij}$ denote the class of bilinear forms of the type given by $f(u, v) = \langle x'_{ij}, v_j^* u_i\rangle$, and in particular let c_{ij} be defined by $c_{ij}(u, v) = \langle z'_i, v_j^* u_i\rangle$, where z'_i generates E'_i. Then if $f \in \mathcal{C}_{ij}$ and $B \in \mathfrak{A}$ it follows that $fB(u, v) = f(u, Bv) = \langle x'_{ij}, (Bv_j)^* u_i\rangle = \langle x'_{ij}, Bv_j^* u_i\rangle = \langle x'_{ij}B, v_j^* u_i\rangle$ so that $fB \in \mathcal{C}_{ij}$. Thus $\mathcal{C}_{ij}$ is a cyclic $\mathfrak{A}$-module which is isomorphic to E'_i, and which is generated by c_{ij}, $i \leqq j$.

Similarly let $\mathcal{C}_{ji}$ denote the class of bilinear forms of the type given by $f(u, v) = \langle x'_{ij}, u_j^* v_i\rangle$, where $i \leqq j$, and in particular let c_{ji} be defined by $c_{ji}(u, v) = \langle z'_i, u_j^* v_i\rangle$. Then $\mathcal{C}_{ji}$ is a cyclic $\mathfrak{A}$-module which is isomorphic to E'_i and which is generated by c_{ji}, $i \leqq j$.

The preceding results imply

THEOREM 5. *$\mathcal{C}(A)$ and $\mathfrak{C}(A)$ are isomorphic $\mathfrak{A}$-modules, each being the direct sum of t^2 cyclic $\mathfrak{A}$-modules, $2t-2j+1$ of them isomorphic to E'_j, $j=1, \cdots, t$.*

The following corollary is a well-known result of Frobenius.

COROLLARY 2. $\dim_K \mathfrak{C}(A) = \sum_{j=1}^{t} (2t-2j+1) \dim_K E'_j$.

In the sequel we shall let $\mathfrak{C}_{ij} \subset \mathfrak{C}(A)$ and $C_{ij} \in \mathfrak{C}_{ij}$ denote the modules and generators, respectively, which are isomorphic to $\mathcal{C}_{ij} \subset \mathcal{C}(A)$ and $c_{ij} \in \mathcal{C}_{ij}$.

4. **An alternate development of the cyclic case.** In the cyclic case it is perhaps easier to describe $\mathfrak{E}(A)$ directly and then to use Theorem 5 to study $\mathcal{C}(A)$. We begin with the following well-known result.

LEMMA 5. *If E is cyclic then $\mathfrak{E}(A)=\mathfrak{A}$.*

Proof. For any $B\in\mathfrak{E}(A)$ set $u=Bz$, where z generates E. Then for any $v\in E$, $Bv=Bv^*z=v^*Bz=v^*u=v^*u^*z=u^*v^*z=u^*v$, hence $B=u^*\in\mathfrak{A}$.

In place of the more exact statement that each $\mathcal{C}_{ij}$ is an $\mathfrak{A}$-module we need only

LEMMA 6. *$\mathcal{S}(A)$ and $\mathcal{a}(A)$ are $\mathfrak{A}$-modules under the composition $f\cdot B=fB$.*

Proof. Suppose that $f\in\mathcal{S}(A)$; that is, that f and fA are symmetric. We shall show by induction that $fA^k\in\mathcal{S}(A)$ for all k. If $fA^{k-1}\in\mathcal{S}(A)$, then fA^k is symmetric by the inductive hypothesis, and $(fA^k)A(u, v)=fA^k(u, Av)$ $=fA^k(Av, u)=fA^{k-1}(Av, Au)$, so that $(fA^k)A$ is also symmetric, as desired. A similar technique may be used to show that $\mathcal{a}(A)$ is an $\mathfrak{A}$-module.

THEOREM 6. *If E is cyclic then the $\mathfrak{A}$-modules $\mathcal{S}(A)$ and $\mathfrak{A}$ are isomorphic, and $\mathcal{a}(A)$ is the zero $\mathfrak{A}$-module.*

Proof. Let f be that bilinear form such that $f(u, v)=\langle z', v^*u\rangle$, where z' generates E'. Then $f\in\mathcal{S}(A)$, by direct verification, and f is nondegenerate since $f(u, v)=\langle z'v^*, u\rangle$, where u and $z'v^*$ may be arbitrary elements of E and E', respectively. Trivially $fB\in\mathcal{S}(A)$ for all $B\in\mathfrak{A}$, and Lemmas 4 and 6 imply that every element of $\mathcal{S}(A)$ is of this form, as before. The second assertion follows from the observation that $\mathcal{C}(A)=\mathcal{S}(A)\oplus_{\mathfrak{A}}\mathcal{U}(A)$ where both $\mathcal{C}(A)$ and $\mathcal{S}(A)$ are isomorphic to $\mathfrak{A}$.

5. **The $\mathfrak{A}$-algebra** $\mathfrak{E}(A)$. Since $\mathfrak{A}$ lies in the center of $\mathfrak{E}(A)$, the latter admits the former as a ring of operators. Briefly, $\mathfrak{E}(A)$ is an algebra over the commutative ring $\mathfrak{A}$. Clearly $\mathfrak{E}(A)$ is generated as an $\mathfrak{A}$-algebra by elements which carry one cyclic submodule into another, and such endomorphisms of E are induced in a natural way by the corresponding $\mathfrak{A}$-homomorphisms of one cyclic submodule into another. An $\mathfrak{A}$-homomorphism of E_j into E_i is uniquely determined by assigning the image of any generator z_j of E_j, and it is tempting to conjecture that the image may simply by chosen to be a generator z_i of E_i. Such a conjecture only makes sense when $\mathfrak{J}(E_i)\supseteq\mathfrak{J}(E_j)$, however. This is the case when $\dim_K E_i\leqq\dim_K E_j$, and in particular when $i\leqq j$. A little more effort is needed to treat the remaining case.

Let ρ_j denote the jth invariant factor of A. If $i\leqq j$, $\rho_j=\pi_{ji}\rho_i$ for some polynomial π_{ji} whose degree is dim E_j-dim E_i and whose leading coefficient is 1.

LEMMA 7. *Suppose that $z_1, \cdots, z_t$ generate $E_1, \cdots, E_t$, respectively, and that z_t' generates E_t'. Then there exist unique $z_1', \cdots, z_{t-1}'$ which generate $E_1', \cdots, E_{t-1}'$, respectively, and which satisfy $\langle z_j', B\pi_{ji}(A)z_j\rangle=\langle z_i', Bz_i\rangle$ whenever $1\leqq i\leqq j\leqq t$, for all $B\in\mathfrak{A}$.*

Proof. The uniqueness of $z_1', \cdots, z_{t-1}'$ is an immediate consequence of the equality $\langle z_i', Bz_i\rangle = \langle z_t', B\pi_{ti}(A)z_t\rangle$. In order to show that $z_1', \cdots, z_{t-1}'$ exist we first note that the cyclic $\mathfrak{A}$-modules generated by z_i and $\pi_{ji}(A)z_j$ are $\mathfrak{A}$-isomorphic since each possesses the minimum polynomial ρ_i. Let Γ_{ji} denote the $\mathfrak{A}$-homomorphism of E_i into E_j induced by setting $\Gamma_{ji}(z_i) = \pi_{ji}(A)z_j$. Since $\pi_{kj}\pi_{ji} = \pi_{ki}$ whenever $i \leqq j \leqq k$, it follows that $\Gamma_{kj} \circ \Gamma_{ji} = \Gamma_{ki}$ whenever $i \leqq j \leqq k$. Γ_{ji} induces a dual homomorphism Γ_{ji}' of E_j' into E_i' which satisfies $\Gamma_{ji}' \circ \Gamma_{kj}' = \Gamma_{ki}'$, and for any $B \in \mathfrak{A}$ it follows that

$$\langle \Gamma_{ti}'(z_t'),\ Bz_i\rangle = \langle \Gamma_{ji}'(\Gamma_{tj}'(z_t')),\ Bz_i\rangle = \langle \Gamma_{tj}'(z_t'), \Gamma_{ji}(Bz_i)\rangle = \langle \Gamma_{tj}'(z_t'),\ B\pi_{ji}(A)z_j\rangle.$$

Thus $\langle z_i', Bz_i\rangle = \langle z_j', B\pi_{ji}(A)z_j\rangle$ if $z_j' = \Gamma_{tj}'(z_t')$, $j = 1, \cdots, t$, and it remains to show that this z_j' generates E_j'. Let u_t be any element of E_t. Then $\langle z_t' B\pi_{tj}(A),\ u_t\rangle = \langle z_t',\ Bu_t^*\pi_{tj}(A)z_t\rangle = \langle z_j',\ Bu_t^*z_j\rangle = \langle z_j' B,\ u_t^*z_j\rangle$, so that if σ_j is a polynomial of minimum degree such that $z_j'\sigma_j(A) = 0$ it follows that $z_t'\sigma_j(A)\pi_{tj}(A) = 0$. But this implies that degree $\sigma_j\pi_{tj} \geqq \dim E_t'$, since E_t' is cyclic, hence that degree $\sigma_j =$ degree $\sigma_j\pi_{tj} -$ degree $\pi_{tj} \geqq \dim E_j'$. The opposite inequality, degree $\sigma_j \leqq$ degree $\rho_j = \dim E_j'$, is a trivial consequence of the fact that E_j' is cyclic. Hence degree $\sigma_j = \dim E_j'$ so that $(z_j', z_j'A, \cdots, z_j'A^{\dim E_j'-1})$ is a basis of E_j'; that is, z_j' generates E_j' as asserted.

We shall say that a set $(z_1', \cdots, z_t')$ of generators of $E_1', \cdots, E_t'$ is *coherently related* to a set $(z_1, \cdots, z_t)$ of generators of $E_1, \cdots, E_t$ if it satisfies the conditions of Lemma 7. Clearly $(z_1', \cdots, z_t')$ is coherently related to $(z_1, \cdots, z_t)$ if and only if $(z_1, \cdots, z_t)$ is coherently related to $(z_1', \cdots, z_t')$.

We return to the problem of describing the $\mathfrak{A}$-algebra $\mathfrak{C}(A)$. If $i \leqq j$ let Γ_{ji} denote the $\mathfrak{A}$-homomorphism $E_i \rightarrow E_j$ generated by $\Gamma_{ji}(z_i) = \pi_{ji}(A)z_j$, as in Lemma 7, and let Γ_{ij} denote the $\mathfrak{A}$-homomorphism $E_j \rightarrow E_i$ generated by $\Gamma_{ij}(z_j) = z_i$. For the convenience of the notation we define π_{ij} in the case $i \leqq j$ by setting $\pi_{ij}(\lambda) = 1$. Then $\Gamma_{ji}(z_i) = \pi_{ji}(A)z_j$ for all indices $i, j = 1, \cdots, t$.

Let C_{ij} denote the endomorphism of E which is induced by Γ_{ij}; that is, if v_j is the projection of any $v \in E$ in E_j, then $C_{ij}v = v_j^*\pi_{ij}(A)z_i$, $i, j = 1, \cdots, t$. We shall show that $\Phi(C_{ij}) = c_{ij}$ as indicated at the end of §3, where Φ is the isomorphism defined in Lemma 4. If $(z_1, \cdots, z_t)$ and $(z_1', \cdots, z_t')$ are coherently related, and if f is the nondegenerate element of $\mathcal{S}(A)$ given in Theorem 4, then for $i \leqq j$ we have $fC_{ij}(u, v) = f(u, C_{ij}v) = f(u, v_j^*\pi_{ij}(A)z_i)$ $= f(u, v_j^*z_i) = \langle z_i', u_i^*v_j^*z_i\rangle = c_{ij}(u, v)$, since $\pi_{ij}(A)$ is the identity, and $fC_{ji}(u, v)$ $= f(u, v_i^*\pi_{ji}(A)z_j) = \langle z_j', u_j^*v_i^*\pi_{ji}(A)z_j\rangle = \langle z_i', u_j^*v_i^*z_i\rangle = c_{ji}(u, v)$, since $(z_1, \cdots, z_t)$ and $(z_1', \cdots, z_t')$ are coherently related. Thus $fC_{ij} = c_{ij}$ for all values of i and j, as asserted.

In order to describe $\mathfrak{C}(A)$ as an $\mathfrak{A}$-algebra it suffices to display a multiplication table of the C_{ij}'s. Since $C_{ij}z_k = \delta_{jk}\pi_{ij}(A)z_i$ for all $i, j, k = 1, \cdots, t$, where δ_{jk} is the Kronecker δ, one easily verifies that

THEOREM 7.

$$C_{ij}C_{kl} = \begin{cases} \delta_{jk}\pi_{ij}(A)\pi_{kl}(A)C_{il} \text{ if } i \leqq l, \\ \delta_{jk}\pi_{lk}(A)\pi_{ji}(A)C_{il} \text{ if } i \geqq l. \end{cases}$$

Incidentally, it should be noted that $\pi_{kj}\pi_{ji}=\pi_{ki}$ if and only if $i \leqq j \leqq k$ or $i \geqq j \geqq k$, so that in general this result cannot be simplified further.

It is to be expected that the $\mathfrak{A}$-submodules of $\mathfrak{C}(A)$ which correspond to $\mathcal{S}(A)$ and $\mathcal{A}(A)$ might have special properties as $\mathfrak{A}$-algebras. If $\mathfrak{S}(A) =\Phi^{-1}(\mathcal{S}(A))$ and $\mathfrak{L}(A)=\Phi^{-1}(\mathcal{A}(A))$, then it is clear that the $\mathfrak{A}$-modules $\mathfrak{S}(A)$ and $\mathfrak{L}(A)$ are generated by elements of the types $C_{ij}+C_{ji}$ and $C_{ij}-C_{ji}$ respectively.

Define Jordan and Lie multiplication by $\{B, C\}=BC+CB$ and $[B, C] =BC-CB$, respectively. Then if f, fB, and fC are symmetric,

$$\begin{aligned} fBC(u, v) &= fB(u, Cv) = fB(Cv, u) = f(Cv, Bu) = f(Bu, Cv) \\ &= fC(Bu, v) = fC(v, Bu) = fCB(v, u), \end{aligned}$$

so that $f(BC+CB)$ is also symmetric. Hence $\mathfrak{S}(A)$ is closed under Jordan multiplication, and in a similar fashion $\mathfrak{L}(A)$ is closed under Lie multiplication.

Thus, since $\mathfrak{S}(A)$ and $\mathfrak{L}(A)$ are the direct sums of the cyclic $\mathfrak{A}$-modules generated by $C_{ij}+C_{ji}$ and $C_{ij}-C_{ji}$, respectively, we obtain

THEOREM 8. *$\mathfrak{C}(A)=\mathfrak{S}(A)\oplus_{\mathfrak{A}}\mathfrak{L}(A)$ where $\mathfrak{S}(A)$ is closed under Jordan multiplication and $\mathfrak{L}(A)$ is closed under Lie multiplication. Furthermore $\mathfrak{S}(A)$ is the direct sum of $t(t+1)/2$ cyclic $\mathfrak{A}$-modules, $t-i+1$ of which are isomorphic to E_i', $i=1, \cdots, t$, and $\mathfrak{L}(A)$ is the direct sum of $t(t-1)/2$ cyclic $\mathfrak{A}$-modules, $t-i$ of which are isomorphic to E_i', $i=1, \cdots, t-1$.*

Since elements of the types $C_{ij}+C_{ji}$ and $C_{ij}-C_{ji}$ generate $\mathfrak{S}(A)$ and $\mathfrak{L}(A)$, respectively, the appropriate multiplication tables may be computed directly from Theorem 7.

6. **Matrix representations of $\mathfrak{C}(A)$ in the cyclic case.** If E is cyclic, with a generator z, then $(z, Az, \cdots, A^{n-1}z)$ will be called a *left canonical basis* of E. If z' generates E', then the basis $(u_1, \cdots, u_n)$ of E which is the dual of the basis $(z', z'A, \cdots, z'A^{n-1})$ of E' will be called a *right canonical basis* of E. If the elements of E are regarded as column vectors, then the matrices $(A)_l$ and $(A)_r$ which represent A with respect to left and right canonical bases, are companion matrices with 1's below and above the main diagonal, respectively. For convenience we shall simply refer to $(A)_l$ and $(A)_r$ as left and right representations of A. If f is any bilinear form f on $E \times E$, we define $(f)_l$ and $(f)_r$ in a similar fashion, these being the left and right representations of f. Clearly $(A)_r={}^t(A)_l$, where ${}^t(A)_l$ is the transpose of $(A)_l$.

Since E is cyclic, $\mathfrak{A}=\mathfrak{E}(A)$ according to Lemma 5, so that the matrix representations of $\mathfrak{E}(A)$ with respect to any basis may be obtained from the powers of the representation of A. The representations of $\mathcal{C}(A)$ are not so trivial, however, and will be developed in this section.

We begin with the left representation of $\mathcal{C}(A)$.

Let α represent the characteristic polynomial of A, $\alpha(\lambda)=\alpha_0+\alpha_1\lambda+\cdots+\alpha_{n-1}\lambda^{n-1}-\lambda^n$, and let $(A]$ represent the $n\times(2n-1)$ matrix whose kth column is the first column of $(A)_l^{k-1}$. Thus if $n=3$,

$$(A] = \begin{bmatrix} 1 & 0 & 0 & \alpha_0 & \alpha_2\alpha_0 \\ 0 & 1 & 0 & \alpha_1 & \alpha_0+\alpha_2\alpha_1 \\ 0 & 0 & 1 & \alpha_2 & \alpha_1+\alpha_2^2 \end{bmatrix}.$$

It should be noted that $(A]$ may be computed in terms of the first $n-1$ powers of $(A)_l$.

Any matrix (a_{ij}) such that a_{ij} depends only on $i+j$ is called a *Hankel matrix*, and such a matrix is uniquely defined by assigning elements of K to each of $2n-1$ values of $i+j$, $i+j=2,\cdots,2n$.

THEOREM 9. *If E is cyclic, then the n Hankel matrices corresponding to the n rows of $(A]$ constitute a basis of the left representation of $\mathcal{C}(A)$.*

Thus if $n=3$ the basis is

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & \alpha_0 \\ 0 & \alpha_2 & \alpha_2\alpha_0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & \alpha_1 \\ 0 & \alpha_1 & \alpha_0+\alpha_2\alpha_1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & \alpha_2 \\ 1 & \alpha_2 & \alpha_1+\alpha_2^2 \end{bmatrix},$$

and one easily checks that multiplication on the right by $(A)_l$ yields linear combinations of these matrices. In fact, these matrices correspond to the basis elements (1, 0, 0), (0, 1, 0), (0, 0, 1) of the right $\mathfrak{A}$-module E'.

Proof. Let $(u_1,\cdots,u_n)$ represent the left canonical basis $(z,\cdots,A^{n-1}z)$ of E, and let $(u_1',\cdots,u_n')$ be the dual basis of E'. Let f_k be that member of $\mathcal{C}(A)$ whose values are given by $f_k(u,v)=\langle u_k',u^*v\rangle$. Then $f_1,\cdots,f_n$ span $\mathcal{C}(A)$ as a vector space over K, and the element in the ith row and jth column of $(f_k)_l$ is $f_k(u_i,u_j)=\langle u_k',A^{i+j-2}z\rangle$, which is the element in the kth row and $(i+j-1)$st column of $(A]$, as asserted.

Note that f_n is nondegenerate, so that we might also take the matrices $(f_n)_l$, $(f_n)_l(A)_l,\cdots,(f_n)_l(A)_l^{n-1}$ as a basis of the left representation of $\mathcal{C}(A)$. These matrices correspond to the elements of a left canonical basis of the left $\mathfrak{A}$-module E.

For convenience we write $\alpha_n=-1$ and $\alpha_j=0$ if $j<0$ or $j>n$. Let $[A)$ represent the $(2n-1)\times(n-1)$ matrix whose kth column contains the entries $\alpha_{1-k},\cdots,\alpha_{2n-k-1}$. Thus if $n=3$,

$$[A) = \begin{pmatrix} \alpha_0 & 0 \\ \alpha_1 & \alpha_0 \\ \alpha_2 & \alpha_1 \\ -1 & \alpha_2 \\ 0 & -1 \end{pmatrix}.$$

Corollary 3. *Let (w) be any row vector with $2n-1$ entries. Then the Hankel matrix corresponding to the entries of (w) is a left representation of an element of $\mathcal{C}(A)$ if and only if $(w)[A)=0$.*

Proof. The Cayley-Hamilton theorem implies $\sum_{k=0}^{n} \alpha_k \langle u_i', A^{k+j-1}z\rangle = 0$, $j=1, \cdots, n-1$, so that $(A][A)=0$, and the result follows from the observation that $[A)$ is of rank $n-1$.

Now suppose that $(u_1, \cdots, u_n)$ is a right canonical basis and set $u_0=0$.

Lemma 8. $Au_i = u_{i-1} + \alpha_{i-1}u_n$, $i=1, \cdots, n$.

Proof. If $j<n$ then $\langle z'A^{j-1}, Au_i\rangle = \langle z'A^j, u^i\rangle = \delta_{j+1,i} = \delta_{j,i-1} = \langle z'A^{j-1}, u_{i-1}\rangle$, and if $j=n$ then

$$\langle z'A^{j-1}, Au_i\rangle = \langle z'A^n, u_i\rangle = \left\langle z' \sum_{k=0}^{n-1} \alpha_k A^k, u_i \right\rangle = \alpha_{i-1} = \langle z'A^{j-1}, \alpha_{i-1}u_n\rangle.$$

Consequently u_n generates E, and we may define $u_i^* \in \mathfrak{A}$ by setting $u_i = u_i^* u_n$.

Lemma 9.

$$A^{k-1}u_i^* = \begin{cases} -\sum\limits_{j=i}^{n} \alpha_j A^{j-i+k-1} & \text{if } 0 < k \leqq i, \\ +\sum\limits_{j=0}^{i-1} \alpha_j A^{j-i+k-1} & \text{if } i < k \leqq n. \end{cases}$$

Proof. Since u_n^* is the identity I on E, Lemma 8 implies that $u_{i-1}^* = Au_i^* - \alpha_{i-1}I$, and one may proceed by induction on $n-i$ to prove that $u_i^* = \sum_{j=i}^{n} \alpha_j A^{j-i}$. If $0<k\leqq i$, the first result is obtained upon multiplication by A^{k-1}. If $i<k\leqq n$, then $A^{k-1}u_i^* = A^{-i+k-1}(A^i u_i^*) = A^{-i+k-1}(-\sum_{j=i}^{n} \alpha_j A^j) = A^{-i+k-1}(+\sum_{j=0}^{i-1} \alpha_j A^j)$, as asserted since $\sum_{j=0}^{i-1} \alpha_j A^j + \sum_{j=i}^{n} \alpha_j A^j = 0$ by the Cayley-Hamilton theorem.

In order to obtain a basis of the right representations of $\mathcal{C}(A)$, we let f be the nondegenerate form which is defined in Theorem 4. In the present case f is given by $f(u, v) = \langle z', u^*v\rangle$, where $u = u^*u_n$. Then $f, fA, \cdots, fA^{n-1}$ span $\mathcal{C}(A)$ as a vector space over K, and we need only to compute $fA^{k-1}(u_i, u_j)$, $i, j, k=1, \cdots, n$.

THEOREM 10. *If E is cyclic, and if $(u_1, \cdots, u_n)$ is a right canonical basis of E, then*

$$fA^{k-1}(u_i, u_j) = \begin{cases} -a_{i+j-k} & \textit{if } 0 < k \leqq i, 0 < k \leqq j, \\ +a_{i+j-k} & \textit{if } i < k \leqq n, j < k \leqq n, \\ 0 & \textit{otherwise.} \end{cases}$$

Thus if $n=3$ the right representations $(f)_r$, $(fA)_r$, $(fA^2)_r$ are

$$\begin{pmatrix} -\alpha_1 & -\alpha_2 & 1 \\ -\alpha_2 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} \alpha_0 & 0 & 0 \\ 0 & -\alpha_2 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \alpha_0 & 0 \\ \alpha_0 & \alpha_1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and one easily checks that multiplication on the right by $(A)_r$ yields linear combinations of these matrices. In fact, these matrices correspond to the basis elements (1, 0, 0), (0, 1, 0), (0, 0, 1) of the right $\mathfrak{A}$-module E'.

Proof. Since $fA^{k-1}(u_i, u_j) = \langle z'A^{k-1}u_i^*, u_j\rangle$, we may apply Lemma 9. If $0 < k \leqq i$ then

$$fA^{k-1}(u_i, u_j) = -\sum_{h=i}^{n} \alpha_h \langle z'A^{h-i+k-1}, u_j\rangle = \begin{cases} -\alpha_{i+j-k} & \text{if } 0 < k \leqq j \\ 0 & \text{otherwise} \end{cases}$$

and similarly if $i < k \leqq n$ then

$$fA^{k-1}(u_i, u_j) = \begin{cases} +\alpha_{i+j-k} & \text{if } j < k \leqq n, \\ 0 & \text{otherwise} \end{cases}.$$

The right representation has the advantage that its entries are linear and homogeneous in the coefficients $\alpha_0, \cdots, \alpha_n$ of the characteristic polynomial of A.

Note that $(f_n)_l$ and $(f)_r$ are inverse matrices. This is an immediate consequence of the fact that if a left canonical basis of E is employed, then any representation of a bilinear form on $E \times E$ with respect to a right canonical basis may be considered as a bilinear form on $E' \times E'$.

7. **Matrix representations of $\mathfrak{S}(A)$ in the general case.** Suppose that $z_1, \cdots, z_t$ generate $E_1, \cdots, E_t$, respectively. Then, if $n_j = \dim E_j$,

$$(z_1, Az_1, \cdots, A^{n_1-1}z_1; \cdots; z_t, Az_t, \cdots, A^{n_t-1}z_t)$$

is a basis of E which we shall call a *left canonical basis* of E. Let $(u'_{1,1}, \cdots, u'_{1,n_1}; \cdots; u'_{t,1}, \cdots, u'_{t,n_t})$ denote the dual basis, and note that u'_{j,n_j} generates E'_j, by an obvious generalization of Lemma 8 to the ring $\mathfrak{A}/\mathfrak{T}(E_j)$, $j = 1, \cdots, t$.

The following lemma will not be used explicitly in the sequel. It is of crucial importance in establishing the matrix correspondence of elements in a left representation of $\mathfrak{C}(A)$ with the representations of their images in $\mathcal{C}(A)$ under the $\mathfrak{A}$-isomorphism Φ, however, and is presented here for this reason.

Lemma 10. *$(z_1, \cdots, z_t)$ and $(u'_{1,n_1}, \cdots, u'_{t,n_t})$ are coherently related.*

Proof. It suffices to show that if $i \leqq j$ then

$$\langle u'_{i,n_i}, A^{k-1}z_i\rangle = \langle u'_{j,n_j}, A^{k-1}\pi_{ji}(A)z_j\rangle, \qquad k = 1, \cdots, n_i.$$

But since $(z_i, \cdots, A^{n_i-1}z_i)$ and $(u'_{i,1}, \cdots, u'_{i,n_i})$ are dual bases of E_i and E'_i it follows that $\langle u'_{i,n_i}, A^{k-1}z_i\rangle = \delta_{k,n_i}$. Similarly since $(z_j, \cdots, A^{n_j-1}z_j)$ and $(u'_j, \cdots, u'_{j,n_j})$ are dual bases of E_j and E'_j, and since the leading coefficient of π_{ji} is 1, it follows that $\langle u'_{j,n_j}, A^{k-1}\pi_{ji}(A)z_j\rangle = \delta_{k,n_i}$.

Suppose that $z'_1, \cdots, z'_t$ are arbitrarily chosen generators of $E'_1, \cdots, E'_t$, respectively. Then $(z'_1, z'_1A, \cdots, z'_1A^{n_1-1}; \cdots; z'_t, z'_tA, \cdots, z'_tA^{n_t-1})$ is a basis of E', and its dual basis $(u_{1,1}, \cdots, u_{1,n_1}; \cdots; u_{t,1}, \cdots, u_{t,n_t})$ will be called a *right canonical basis* of E. As in the preceding case, u_{j,n_j} generates E_j, and $(z'_1, \cdots, z'_t)$ and $(u_{1,n_1}, \cdots, u_{t,n_t})$ are coherently related.

In general $\mathfrak{C}(A) \neq \mathfrak{A}$ so that the representations of $\mathfrak{C}(A)$ can no longer be obtained in terms of the representations of powers of A. However, since $\mathfrak{C}(A)$ is the direct sum of the cyclic $\mathfrak{A}$-modules $\mathfrak{C}_{ij}$ generated by C_{ij}, $i, j = 1, \cdots, t$, it will suffice to obtain matrix representations of C_{ij}. Furthermore, since C_{ij} takes E_j into E_i and vanishes outside of E_j, we shall consider only the corresponding homomorphism Γ_{ij} of E_j into E_i.

Let A_i and A_j denote the restrictions of A to E_i and E_j, respectively. Then since $AC_{ij} = C_{ij}A$, it follows that $A_i\Gamma_{ij} = \Gamma_{ij}A_j$. Thus we may represent $\mathfrak{C}_{ij}$ in terms of the representations of $\Gamma_{ij}, A_i\Gamma_{ij}, \cdots, A_i^{n_i-1}\Gamma_{ij}$ if $i \leqq j$, and in terms of the representations of $\Gamma_{ij}, \Gamma_{ij}A_j, \cdots, \Gamma_{ij}A_j^{n_j-1}$ if $j \leqq i$. Since E_i and E_j are cyclic modules for the rings generated by A_i and A_j, it remains to find the representations of Γ_{ij} in the two cases $i \leqq j$ and $i \geqq j$. Furthermore, since the dual of a left canonical basis is a right canonical basis, the right representation $(\Gamma_{ij})_r$ of Γ_{ij} is simply the transpose of the left representation $(\Gamma_{ji})_l$ of Γ_{ji}. Thus it will suffice to find $(\Gamma_{ij})_l$ in the two cases $i \leqq j$ and $i \geqq j$.

We shall always take $i \leqq j$ in the sequel, so that Γ_{ij} and Γ_{ji} will be understood to be the two distinct cases. For convenience we write r, s, ρ, π in place of n_i, n_j, ρ_i, π_{ji}, respectively, where ρ is the ith invariant factor, $\rho(\lambda) = \rho_0 + \rho_1\lambda + \cdots + \rho_{r-1}\lambda^{r-1} - \lambda^r$, and where $\pi(\lambda) = \pi_0 + \pi_1\lambda + \cdots + \pi_{s-r-1}\lambda^{s-r-1} + \lambda^{s-r}$. Also we set $\rho_r = -1$, $\pi_{s-r} = +1$, and $\pi_j = 0$ if $j < 0$ or $j > s - r$.

Recall that the elements of E are taken as column vectors, so that if $r = 2$,

$$(A_i)_l = \begin{pmatrix} 0 & \rho_0 \\ 1 & \rho_1 \end{pmatrix} \quad \text{and} \quad (A_i)_r = \begin{pmatrix} 0 & 1 \\ \rho_0 & \rho_1 \end{pmatrix}, \ \textit{e.g.}$$

Let $[\Gamma_{ij}]$ represent the $r \times s$ matrix whose hth column is the first column of $(A_i)_l^{h-1}$. Thus if $r = 2$ and $s = 3$,

$$[\Gamma_{ij}] = \begin{pmatrix} 1 & 0 & \rho_0 \\ 0 & 1 & \rho_1 \end{pmatrix}.$$

LEMMA 11. *If* $i \leqq j$ *then* $(\Gamma_{ij})_l = [\Gamma_{ij}]$.

Proof. Since $\Gamma_{ij}(A^{h-1}z_j) = A^{h-1}z_i$, the element in the kth row and hth column of $(\Gamma_{ij})_l$ is $\langle u'_{i,k}, A^{h-1}z_i\rangle$, which is precisely the element in the kth row and hth column of $[\Gamma_{ij}]$, $k=1, \cdots, r$, $h=1, \cdots, s$.

One easily verifies that $(\Gamma_{ij})_l$ is of rank r and that $(A_i)_l(\Gamma_{ij})_l = (\Gamma_{ij})_l(A_j)_l$ as desired.

Let $[\Gamma_{ji}]$ denote the $s \times r$ matrix whose kth column contains the entries $\pi_{1-k}, \cdots, \pi_{s-k}$. Thus if $r=2$ and $s=3$,

$$[\Gamma_{ji}] = \begin{bmatrix} \pi_0 & 0 \\ 1 & \pi_0 \\ 0 & 1 \end{bmatrix}.$$

LEMMA 12. *If* $i \leqq j$ *then* $(\Gamma_i)_l = [\Gamma_{ji}]$.

Proof. Since $\Gamma_{ji}(A^{k-1}z_i) = A^{k-1}\pi(A)z_j$, the element in the hth row and kth column of $(\Gamma_{ji})_l$ is $\langle u'_{j,h}, A^{k-1}\pi(A)z_j\rangle$, which is precisely the element in the hth row and kth column of $[\Gamma_{ji}]$, $k=1, \cdots, r$, $h=1, \cdots, s$.

Summarizing, we have

THEOREM 11. *If* $i \leqq j$ *then the left representation of* $\mathfrak{C}_{ij}$ *consists of zeros except in an* $r \times s$ *block on or above the diagonal, which contains linear combinations of* $(A_i)_l^{k-1}[\Gamma_{ij}]$, $k=1, \cdots, r$, *and the left representation of* $\mathfrak{C}_{ji}$ *consists of zeros except in an* $s \times r$ *block on or below the diagonal, which contains linear combinations of* $[\Gamma_{ji}]$ $(A_i)_l^{k-1}$, $k=1, \cdots, r$.

8. **Matrix representations of $\mathcal{C}(A)$ in the general case.** Since $\mathfrak{C}(A)$ is the direct sum of the $\mathfrak{A}$-modules $\mathcal{C}_{ij}$ we shall find the matrix representations of the latter modules. Each $\mathcal{C}_{ij}$ is generated by a bilinear form c_{ij} on $E \times E$ which vanishes except on $E_i \times E_j$, so that it will suffice to consider the restriction γ_{ij} of c_{ij} to $E_i \times E_j$. If $i \leqq j$, then if $u \in E_i$ and $v \in E_j$, $\gamma_{ij}(u, v) = \langle z_i', v^*u\rangle$ by definition. Since any representation (c_{ji}) of c_{ji} is the transpose of the corresponding representation of c_{ij}, we do not need to consider the case $i > j$.

Let f be the nondegenerate element of $\mathcal{C}(A)$ given in Theorem 4. Then $c_{ij} = fC_{ij}$ provided that one chooses coherently related sets of generators of $E_1, \cdots, E_t$ and $E_1', \cdots, E_t'$ in defining f. If γ represents the restriction of f to $E_i \times E_i$, it follows that $\gamma_{ij} = \gamma\Gamma_{ij}$, and since E_i is cyclic we may use Theorems 9 and 10 to obtain $(\gamma)_l$ and $(\gamma)_r$. The following two theorems are immediate consequences of these results.

THEOREM 12. *Let* $i \leqq j$ *and let* $(\gamma_k)_l$ *be the kth element of the basis of the left canonical representation of* $\mathcal{C}(A_i)$, *as in Theorem* 9. *Then the left representation* *of $\mathcal{C}_{ij}$ consists of zeros except in an $r \times s$ block on or above the diagonal, which contains linear combinations of $(\gamma_1)_l(\Gamma_{ij})_l, \cdots, (\gamma_r)_l(\Gamma_{ij})_l$. The left representation of $\mathcal{C}_{ji}$ is the transpose of this.*

Thus if $r=2$ and $s=3$ the nonzero block above the diagonal consists of linear combinations of

$$\begin{pmatrix} 1 & 0 \\ 0 & \rho_0 \end{pmatrix}\begin{pmatrix} 1 & 0 & \rho_0 \\ 0 & 1 & \rho_1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & \rho_1 \end{pmatrix}\begin{pmatrix} 1 & 0 & \rho_0 \\ 0 & 1 & \rho_1 \end{pmatrix}.$$

It should be noted that if the indicated multiplications are performed one obtains further Hankel matrices, as in Theorem 9. In fact, one may even prove Theorem 12 directly by using the technique of Theorem 9.

THEOREM 13. *Let $i \leqq j$ and let $(\gamma A^{k-1})_r$ be the kth element of the basis of the right canonical representation of $\mathcal{C}(A_i)$, as in Theorem 10. Then the right representation of $\mathcal{C}_{ij}$ consists of zeros except in an $r \times s$ block on or above the diagonal, which contains linear combinations of $(\gamma)_r(\Gamma_{ij})_r, \cdots, (\gamma A_i^{r-1})_r(\Gamma_{ij})_r$. The right representation of $\mathcal{C}_{ji}$ is the transpose of this.*

In order to compute $(\Gamma_{ij})_r$ we note that $(\Gamma_{ij})_r = {}^t(\Gamma_{ji})_l = {}^t[\Gamma_{ji}]$. Thus if $r=2$ and $s=3$ the nonzero block above the diagonal consists of linear combinations of

$$\begin{pmatrix} -\rho_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \pi_0 & 1 & 0 \\ 0 & \pi_0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} \rho_0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \pi_0 & 1 & 0 \\ 0 & \pi_0 & 1 \end{pmatrix}.$$

9. **Remarks on the nondegenerate forms in $\mathcal{S}(A)$.** Suppose that A is cyclic and that z generates E. Then the nth element of the dual of the left canonical basis $(z, Az, \cdots, A^{n-1}z)$ generated by z is an E'-generator z', by the dual of Lemma 8. Similarly the nth element of the dual basis of $(z', z'A, \cdots, z'A^{n-1})$ is an E-generator z'', and one easily checks that $z''=z$. Thus this construction provides a natural one-to-one correspondence of E-generators and E'-generators. Unfortunately the correspondence is not linear and cannot be extended to a correlation; however, it does provide a natural way for applying Theorem 4, in the cyclic case, to find a nondegenerate form merely by specifying an E-generator rather than both an E-generator and an E'-generator. Similar remarks apply in the general case.

If z generates E and $v=v^*z$ and $w=w^*z$, then the form g given by setting $g(v, w) = \text{trace } v^*w^*$ is clearly an element of $\mathcal{S}(A)$, and one might expect that it could itself be used to generate $\mathcal{S}(A)$ in place of the construction of Theorem 4. However, g is degenerate in some cases, as shown below, and in any event it is no more "natural" than Theorem 4, since one must still prescribe z in order to compute v^* and w^*.

Let $(u_1, \cdots, u_n)$ be a left canonical basis of E, $(u_1', \cdots, u_n')$ its dual basis, and define v^* and w^* by setting $v=v^*u_1$ and $w=w^*u_1$. Then any of the n^2 forms f_{ij} given by setting $f_{ij}(v, w) = \langle u_i', v^* w^* u_j \rangle$ is an element of $\mathcal{S}(A)$. One easily shows that

$$\begin{pmatrix} f_{1j} \\ \cdot \\ \cdot \\ \cdot \\ f_{nj} \end{pmatrix} = (A)_l^{j-1} \begin{pmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_n \end{pmatrix}$$

where the forms $f_1, \cdots, f_n$ span $\mathcal{S}(A)$ as in Theorem 9, so that $g = \sum_{j=1}^n f_{jj} = \sum_{j=1}^n (\text{trace } A^{j-1}) f_j$. Hence g is nondegenerate if and only if

$$\det \sum_{j=1}^{n} (\text{trace } A^{j-1}) f_j \neq 0,$$

which is an algebraic inequality in $\alpha_0, \cdots, \alpha_{n-1}$. For example, if $n = 2$ then g is degenerate whenever $4\alpha_0 + \alpha_1^2 = 0$.

University of Illinois,
Urbana, Ill.