Regular Representations of Semisimple Algebras, Separable Field Extensions, Group Characters, Generalized Circulants, and Generalized Cyclic Codes

David Chillag

Department of Mathematics
Technion—Israel Institute of Technology
Haifa 32000, Israel

Submitted by Moshe Goldberg

ABSTRACT

Let $A$ be a semisimple, $n$-dimensional, commutative algebra over a field $F$. Fix a basis $B$ of $A$, and denote by $M(a; B)$ the transpose of the matrix over $F$ that represents $a \in A$ regularly with respect to $B$. It is easy to see that the set $\{M(a; B) | a \in A\}$ can be simultaneously diagonalized over many fields (including all perfect fields). We use this fact in order to give an elementary proof that such an algebra over an infinite field is generated by a single element, and to describe the subalgebras of $A$ in terms of certain partitions of the set $\{1, 2, 3, \ldots, n\}$. Several applications of these results are shown: (1) We give a new proof for the theorem stating that every finite-dimensional, separable field extension has a primitive element. (2) We show that every finite group $G$ has a character $\theta$ such that every other generalized character of $G$ is a polynomial in $\theta$ with rational coefficients. (This is true for Brauer characters as well.) (3) We give a necessary condition for two generalized characters (or Brauer characters) $\xi$ and $\chi$ that forces the field of values of $\xi$ to contain that of $\chi$. (4) Many collections of patterned matrices over a field $F$, such as circulant matrices and some of their generalizations are known to be algebras generated by a single matrix. We observe that each subalgebra of such a collection is also generated by a single matrix. Also, if $a$ and $b$ are two elements of such a collection, we give a necessary and sufficient condition, in terms of the eigenvalue pattern of $a$ and $b$, for $a$ to be a polynomial in $b$ with coefficients in $F$. (5) We show that if $A$ is a (generalized) cyclic code, then the eigenvalues of $M(a; B)$ are the so-called...
Matteson-Solomon coefficients of the codeword $a$. Other applications to coding, to groups, and to field extensions are discussed as well.

I. STATEMENTS OF MAIN RESULTS AND APPLICATIONS

Values of characters of finite groups, Galois conjugates of an element of a Galois extension of a field, eigenvalues of some generalized circulant matrices, and the Matteson-Solomon coefficients of a codeword of a cyclic code are all examples of eigenvalues of elements of semisimple finite-dimensional, commutative algebras. The purpose of this paper is to exhibit elementary properties of such algebras and to apply these properties in various situations. This will yield both new and known results. The point we are trying to make is that all these results are, in fact, consequences of general properties of regular representations of certain algebras.

We start with a description of the basic properties of our algebras, and then discuss the applications.

DEFINITIONS AND NOTATION. Let $A$ be a finite-dimensional commutative algebra with an identity $1$ over a field $F$. For each $a \in A$ let $T_a$ be the linear transformation $T_a : A \to A$ defined by $T_a(u) = au$ for all $u \in A$. Then the mapping $a \to T_a$ is the regular representation of $A$. Let $B = \{b_1, b_2, \ldots, b_n\}$ be a basis of $A$. For every $a \in A$ define the $n \times n$ matrix $M(a; B) = (m_{ij}(a; B))$, where the $m_{ij}(a; B)$ are the elements of $F$ defined by the equalities $ab_i = \sum_{j=1}^{n} m_{ij}(a; B)b_j$. In fact, $(M(a; B))^t$ is the representing matrix of $T_a$ with respect to the basis $B$. It is not hard to see that the algebras $A$ and $M(A; B) = \{M(a; B) | a \in A\}$ are isomorphic over $F$. Next, let $f(z) = a_0 + a_1z + a_2z^2 + \cdots + a_rz^r \in F[z]$, and let $a \in A$; then $f(a)$ is defined to be the element $a_0 \cdot 1 + a_1 a + a_2 a^2 + \cdots + a_r a^r \in A$. For $u \in A$, let $F[u]$ be the subalgebra of $A$ generated by $u$, that is, the algebra spanned over $F$ by the powers of $u$. Evidently, $F[u] = \{f(u) | f(x) \in F[x]\}$.

For each $a \in A$ we denote by $m_a(x)$ the minimal polynomial of $T_a$ over $F$, and by $p_a(x)$ the characteristic polynomial of $T_a$. As the mapping $a \to T_a$ is linear and multiplicative, we see that $m_a(x)$ is the unique monic polynomial of minimal degree with $m_a(a) = 0$. An element $a \in A$ is called separable if the irreducible factors of $m_a(x)$ over $F$ do not have multiple
roots in the splitting field of $m_a(x)$ over $F$. We say that $A$ is separable if every element of $A$ is separable over $F$.

If $F$ is a perfect field, then the irreducible factors of every polynomial in $F[x]$ do not have multiple roots. Thus, every finite-dimensional, commutative algebra with $1$ over a perfect field is separable.

In this article we are interested in semisimple, finite-dimensional, commutative algebras (SFCA for short) over a field $F$. Such an algebra always contains $1$ (see [11, p. 9]). Most of our proofs are based on the known fact that if an SFCA $A$ is separable, then all elements of $M(A; F)$ can be simultaneously diagonalized over some finite extension field of $F$. With this we shall prove:

**Theorem 1.1.** Let $A$ be a separable, semisimple, finite-dimensional, commutative algebra over a field $F$. Then:

(a) If $F$ is infinite, then there exists $u \in A$ such that $A = F[u]$; that is, every element of $A$ is a polynomial in $u$ with coefficients in $F$.

(b) Let $v \in A$. Then $A = F[v]$ if and only if all the roots of $p_v(x)$ in its splitting field over $F$ are distinct.

**Remarks.**

(a) We shall need the fact that if $A$ is a separable SFCA over $F$, then $A$ is a direct sum of finite extensions of $F$. This is a simple special case of Wedderburn's theorem. Besides this mildly nonelementary result, we use only basic linear algebra to prove the properties of the SFCA we need. We shall not use the known fact that each of the finite extensions of $F$ which are the direct summands of $A$, has a primitive element over $F$. In fact, the primitive-element theorem will become a consequence of Theorem 1.1. See also remark (b) following Corollary 2.6.

(b) Theorem 1.1 is false in general if $F$ is finite. For example, let $A = Z_2 \oplus Z_2 \oplus Z_2$. Then $A$ is a separable, semisimple, 3-dimensional, commutative algebra over $Z_2$. Pick $u = (a, b, c) \in A$ where $a, b, c$ are in $Z_2$. Then $a^i = a$, $b^i = b$, and $c^i = c$ for every positive integer $i$. Let $f(x) = \sum_{i=0}^{m} d_i x^i \in Z_2[x]$. Then

$$f(u) = d_0(1,1,1) + \sum_{i=1}^{m} d_i u = d_0(1,1,1) + du$$

for some $d_0, d \in Z_2$.

So $\{ f(u) | f(x) \in Z_2[x] \}$ contains at most four of the eight elements of $A$. Thus no $u$ satisfies $A = Z_2[u]$.

(c) Theorem 1.1 states that if $p_v(x)$ has no repeated roots then $a \in F[w]$ for all $a \in A$. Given $c, d \in A$, this statement will be generalized
by providing a necessary and sufficient condition [in terms of the “root pattern” of $p_c(x)$ and $p_d(x)$] for $c$ to belong to $\mathbb{F}[d]$. This will be done by describing the subalgebras of a separable SFCA $A$ in terms of certain partitions of the set $\{1, 2, 3, \ldots, n\}$, where $n$ is the dimension of $A$ over $\mathbb{F}$. We shall need the following notation.

Let $n$ be a positive integer, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ be an $n$-tuple, where the $\alpha_i$ belong to some field. Then the type of $\alpha$, denoted by $T(\alpha)$, is the partition $\{T(\alpha)_1, T(\alpha)_2, \ldots, T(\alpha)_n\}$ of $\{1, 2, 3, \ldots, n\}$ with the property that $\{i, j\} \subseteq T(\alpha)_s$ for some $s$ if and only if $\alpha_i = \alpha_j$. So each $T(\alpha)_s$ contains indices $k$ for which the corresponding $\alpha_k$ are equal, and distinct $T(\alpha)_s$ contain indices $r$ for which the corresponding $\alpha_r$ are distinct. For example, for $\alpha = (1, 1, 1, \sqrt{2}, \sqrt{2}, 1, 3, 3, \sqrt{2})$ we have

$$T(\alpha) = \{\{1, 3, 4, 7\}, \{2\}, \{5, 6, 10\}, \{8, 9\}\}.$$ 

Let $P = \{P_1, P_2, \ldots, P_s\}$ and $Q = \{Q_1, Q_2, \ldots, Q_r\}$ be two partitions of $\{1, 2, 3, \ldots, n\}$. If for each $i$, $1 \leq i \leq s$, there exists a $j$, $1 \leq j \leq r$, such that $P_i \subseteq Q_j$, then we say that $P$ is a refinement of $Q$ and write $P \leq Q$. Clearly, $P \leq Q$ means that each $Q_j$ is the union of some of the $P_i$.

Let $A$ be a separable SFCA of dimension $n$ over a field $\mathbb{F}$, and select a basis $B$ of $A$. It is known (see Lemma 2.1) that there exists a finite extension $\mathbb{K}$ of $\mathbb{F}$ and an $n \times n$ matrix $X$ over $\mathbb{K}$ such that $X^{-1}M(a; B)X$ is diagonal for all $a \in A$. Such an $X$ will be called a diagonalizing matrix of $A$ with respect to the basis $B$. Fix such a matrix $X$; and for every $a \in A$ write

$$X^{-1}M(a; B)X = \text{diag}(a(1), a(2), \ldots, a(n)),$$

where the $a(i)$ are the eigenvalues of $T_a$ in $\mathbb{K}$ with the ordering prescribed by $X$. Here, diag$(s_1, s_2, \ldots, s_m)$ is the diagonal matrix whose diagonal entries are $s_1, s_2, \ldots, s_m$.

We now define the type of $a \in A$, denoted by $T(a)$, as the type of $(a(1), a(2), \ldots, a(n))$. That is, $T(a) = T(a(1), a(2), \ldots, a(n))$.

Finally, let $P$ be any partition of $\{1, 2, 3, \ldots, n\}$. Set $\mathbb{F}(P) = \{a \in A \mid P \leq T(a)\}$. We shall prove (see Lemma 2.5) that $\mathbb{F}(P)$ is a subalgebra of $A$. The fact that the definitions of $\mathbb{F}(P)$ and $T(a)$ depend on the choice of $B$ and $X$ is not reflected in the notation. The reason is that in most cases $B$ and $X$ will be fixed.

With this notation we shall prove:

**Theorem 1.2.** Let $A$ be a separable, semisimple, $n$-dimensional, commutative algebra over an infinite field $\mathbb{F}$, and let $C$ be a subalgebra of $A$. Let $B$ be a basis of $A$, and let $X$ be a diagonalizing matrix of $A$ with respect $B$. Let $T$ be the type defined by $B$ and $X$. Then:

(a) There exists $u \in C$ such that $C = \mathbb{F}[u] = \mathbb{F}(T(u))$. In particular, ev-
Every subalgebra of $A$ has the form $\mathbb{F}(P)$ for some partition $P$ of \{1, 2, \ldots, n\}.

(b) Let $a, b \in A$. Then $\mathbb{F}[a] \subseteq \mathbb{F}[b]$ if and only if $T(b) \leq T(a)$. In particular, the inequality $T(b) \leq T(a)$ depends only on $a$ and $b$ and not on the choice of the basis $\mathcal{B}$ and the diagonalizing matrix $X$.

The proofs of Theorems 1.1 and 1.2 are given in Section II.

**Example.** Let $A = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $A$ is a separable SFCA of dimension 4 over the rationals $\mathbb{Q}$. We pick a basis $\mathcal{B} = \{b_1, b_2, b_3, b_4\}$ with $b_1 = 1$, $b_2 = \sqrt{2}$, $b_3 = \sqrt{3}$, $b_4 = \sqrt{6}$, and compute the matrices $M(b_i; \mathcal{B})$, $i = 1, 2, 3, 4$. Since $b_1 b_i = b_i$ for all $i$, we get $M(b_1; \mathcal{B}) = \text{diag}(1, 1, 1, 1)$. Next, $b_2 b_1 = b_2$, $b_2 b_2 = 2b_1$, $b_2 b_3 = b_4$, $b_2 b_4 = 2b_3$. This implies

$$M(b_2; \mathcal{B}) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 \end{bmatrix}.$$ Further, $b_3 b_1 = b_3$, $b_3 b_2 = b_4$, $b_3 b_3 = 3b_1$, $b_3 b_4 = 3b_2$; hence,

$$M(b_3; \mathcal{B}) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{bmatrix}.$$ Finally, $b_4 b_1 = b_4$, $b_4 b_2 = 2b_3$, $b_4 b_3 = 3b_2$, $b_4 b_4 = 6b_1$; thus,

$$M(b_4; \mathcal{B}) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 3 & 0 & 0 \\ 6 & 0 & 0 & 0 \end{bmatrix}.$$ Let

$$X = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -\sqrt{2} & -\sqrt{2} & \sqrt{2} & \sqrt{2} \\ -\sqrt{3} & \sqrt{3} & -\sqrt{3} & \sqrt{3} \\ \sqrt{6} & -\sqrt{6} & -\sqrt{6} & \sqrt{6} \end{bmatrix}. \quad (1.1)$$

One can see that $X$ diagonalizes each $M(b_i; \mathcal{B})$. In fact, we have

$$X^{-1}M(b_1; \mathcal{B})X = \text{diag}(1, 1, 1, 1),$$
\[ X^{-1}M(b_2; B)X = \text{diag}(-\sqrt{2}, -\sqrt{2}, \sqrt{2}, \sqrt{2}), \]
\[ X^{-1}M(b_3; B)X = \text{diag}(-\sqrt{3}, \sqrt{3}, -\sqrt{3}, \sqrt{3}), \]  
\[ X^{-1}M(b_4; B)X = \text{diag}(\sqrt{6}, -\sqrt{6}, -\sqrt{6}, \sqrt{6}). \]  

(1.2)

It follows that
\[
T(b_1) = \{\{1, 2, 3, 4\}\}, \quad T(b_2) = \{\{1, 2\}, \{3, 4\}\}, \]
\[
T(b_3) = \{\{1, 3\}, \{2, 4\}\}, \quad T(b_4) = \{\{1, 4\}, \{2, 3\}\}.
\]

The fact that the rows of \(X\) are the diagonals of the matrices \(X^{-1}M(b_i; B)X\), \(i = 1, 2, 3, 4\), is no coincidence (see Theorem 2.3).

We turn now to the correspondence between subalgebras and certain partitions of \(\{1, 2, 3, 4\}\). It is easy to see that the subalgebras of \(A\) are the intermediate fields of the extension \(\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})\). This holds because \(u \in A\) implies \(u^{-1} = f(u)\) for some \(f(x) \in \mathbb{Q}[x]\). So there are five subalgebras: \(\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})\), and \(\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})\). The corresponding partitions are
\[
\mathbb{Q} = \mathbb{Q}(1) \rightarrow \{\{1, 2, 3, 4\}\}, \quad \mathbb{Q}(\sqrt{2}) \rightarrow \{\{1, 2\}, \{3, 4\}\},
\]
\[
\mathbb{Q}(\sqrt{3}) \rightarrow \{\{1, 3\}, \{2, 4\}\}, \quad \mathbb{Q}(\sqrt{6}) \rightarrow \{\{1, 4\}, \{2, 3\}\},
\]
\[
\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \rightarrow \{\{1\}, \{2\}, \{3\}, \{4\}\}.
\]

The last correspondence follows from Theorem 1.1, and independently from the equality
\[ M(\sqrt{2} + \sqrt{3}; B) = M(\sqrt{2}; B) + M(\sqrt{3}; B), \]

from which we obtain
\[
X^{-1}M(\sqrt{2} + \sqrt{3}; B)X = X^{-1}M(\sqrt{2}; B)X + X^{-1}M(\sqrt{3}; B)X
\]
\[
= \text{diag}(-\sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, \sqrt{2} + \sqrt{3}).
\]

**Remarks.**

(a) Theorem 1.2 states that the "eigenvalue pattern" of an element \(u \in A\) determines the subalgebra \(\mathbb{F}[u]\). For instance, in the above example we have \(a \in \mathbb{Q}(\sqrt{2})\) if and only if \(X^{-1}M(a; B)X\) has the form \(\text{diag}(y, y, z, z)\). If \(c \in \mathbb{Q}(\sqrt{2})\), then \(X^{-1}M(c; B)X\) is never of the form \(\text{diag}(y, y, x, z)\), \(x \neq z\). This means that if \(c \in \mathbb{Q}(\sqrt{2}, \sqrt{3})\) and \(T_c\) has three distinct eigenvalues, then all four eigenvalues of \(T_c\) are distinct.
(b) By Theorems 1.1 and 1.2, we know that if \( \mathcal{P} \) is a partition of \( \{1,2,\ldots,n\} \) then \( \mathbb{F}(\mathcal{P}) = \mathbb{F}[v] \) for some \( v \in \mathcal{A} \). It is not true, however, that \( \mathcal{P} = T[v] \) for some \( v \in \mathcal{A} \). For instance, in the above example, there is no \( v \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) such that \( \{\{1,2\}, \{3\}, \{4\}\} = T(v) \).

We now turn to applications.

Separable Field Extensions. Most of the applications we present for separable field extensions are illustrated by the above example. We sum up the consequences in the following theorem, all whose parts either are well known or can be proved using Galois theory. We, however, shall make a point in proving the theorem using elementary properties of regular representations of SFCAs. In particular, Galois theory will not be used in the proofs of parts (a)-(c). In (d) and (e) (where \( K \) is assumed to be a Galois extension of \( F \)), the only Galois-theoretical fact we use is that \( \prod_{\sigma \in \text{Gal}(K/F)} (x - \sigma(a)) \) is in \( \mathbb{F}[x] \).

**Theorem 1.3.** Let \( F \) be a field, \( K \) a separable extension of \( F \) of degree \( n \), \( B \) a basis for \( K \) over \( F \), and \( X \) a diagonalizing matrix of \( K \) with respect to \( B \). For each \( a \in K \) let \( T(a) \) be the type of \( a \) with respect to \( B \) and \( X \). Then:

(a) The collection of intermediate fields between \( F \) and \( K \) (including \( K \) itself) is the finite set \( \{\mathbb{F}(T(a)) \mid a \in K\} \), where each \( T(a) \) partitions the set \( \{1,2,\ldots,n\} \) into \( [F[a] : F] \) parts of equal size. Moreover, \( \mathbb{F}(T(a)) = \mathbb{F}(a) \) for all \( a \in K \). In particular, \( K = \mathbb{F}(b) \) for some \( b \in K \).

(b) Let \( a, b \in K \). Then \( \mathbb{F}(a) \subseteq \mathbb{F}(b) \) if and only if \( T(b) \leq T(a) \). In particular, the inequality \( T(b) \leq T(a) \) is independent of the choice of \( B \) and \( X \).

(c) For \( a, b \in K \) we have \( \mathbb{F}(a) = K \) if and only if \( T(a) = \{\{1\}, \{2\}, \ldots, \{n\}\} \). Further, \( b \in F \) if and only if \( T(b) = \{\{1,2,\ldots,n\}\} \).

(d) If \( K \) is a Galois extension of \( F \), then the eigenvalues of \( M(a; B) \) are the elements \( \sigma(a) \) where \( \sigma \in \text{Gal}(K/F) \).

(e) Suppose \( K \) is a Galois extension of \( F \), and let \( c_1, c_2, \ldots, c_n \) be elements of \( K \). Set \( \text{Gal}(K/F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\} \). Then \( \{c_1, c_2, \ldots, c_n\} \) is a basis for \( K \) over \( F \) if and only if the matrix \( (\sigma_i(c_j)) \) is nonsingular.

The proof can be found in Section III. We remark that part (e) (which is well known) will be obtained here as a corollary of a general result on SFCAs. Our proof uses neither the Dedekind independence theorem nor extensions of automorphisms that are used, for example, in the proof of (e) in [9, p. 293].

*Ordinary Characters, Brauer Characters, and Conjugacy Classes of Fi-
nite Groups. We use standard notation of character theory (see [8]). Let $G$ be a finite group. There are four natural SFCAs associated with $G$ that will be described below.

Denote by $C_1 = \{1\}, C_2, \ldots, C_k$ the conjugacy classes of $G$, and by $\text{Irr}(G)$ the set of all irreducible ordinary characters of $G$. Set $\text{Irr}(G) = \{\chi_1 = 1_G, \chi_2, \ldots, \chi_k\}$. The value of a class function $f$ of $G$ on the conjugacy class $C$ is denoted by $f(C)$. Let $X = (\chi_i(C_j))$ be the character table matrix of $G$. Denote by $\mathbb{Z}(\text{Irr}(G))$ the set of all irreducible ordinary characters of $G$ (namely, all the linear combinations of elements of $\text{Irr}(G)$ with integer coefficients), and by $\mathbb{Q}(\text{Irr}(G))$ the set of all linear combinations of elements of $\text{Irr}(G)$ with rational coefficients. Next, if $f$ is a class function on $G$, we denote by $\mathbb{Q}_f$ the smallest subfield of the complex number field $\mathbb{C}$, which contains the field of rationals $\mathbb{Q}$ and the numbers $f(C_1), f(C_2), \ldots, f(C_k)$. We say that $f$ is realized in the field $\mathbb{Q}_f$. The smallest subfield of $\mathbb{C}$ which contains the set $\cup\{\mathbb{Q}_\chi | \chi \in \text{Irr}(G)\}$ is denoted by $\mathbb{Q}_G$. Finally, the type of a class function $f$ of $G$, denoted by $\mathcal{T}(f)$, is defined by $\mathcal{T}(f) = \mathcal{T}(f(C_1), f(C_2), \ldots, f(C_k))$. Note that if $f \in \text{Irr}(G)$ then $\mathcal{T}(f)$ is the type of the row of $f$ in the character table of $G$.

We know that $\mathbb{Q}(\text{Irr}(G))$ is an SFC over $\mathbb{Q}$ in which $\text{Irr}(G)$ is a basis. It is known that:

$$X^{-1}M(f; \text{Irr}(G))X = \text{diag}(f(C_1), f(C_2), \ldots, f(C_k))$$

for every class function $f$ of $G$. Applying Theorems 1.1, 1.2 and other results on SFC to $\mathbb{Q}(\text{Irr}(G))$, we shall prove in Section IV:

**Theorem 1.4.** Let $G$ be a finite group with conjugacy classes $C_1 = \{1\}, C_2, \ldots, C_k$. Then:

(a) There exists a character $\theta$ of $G$ such that $\mathbb{Q}(\text{Irr}(G)) = \mathbb{Q}[\theta]$. In particular, every generalized character of $G$ is a polynomial in $\theta$ with rational coefficients, so that $\mathbb{Q}_G = \mathbb{Q}_\theta$. Moreover, $\theta(C_i) \neq \theta(C_j)$ for $i \neq j$.

(b) For every generalized character $\eta$ of $G$, the equality $\mathbb{Q}[\eta] = \mathbb{Q}(\mathcal{T}(\eta))$ holds.

(c) Let $\eta$ and $\psi$ be generalized characters of $G$. Then the following statements are equivalent: (i) $\mathcal{T}(\psi) \geq \mathcal{T}(\eta)$; (ii) $\mathbb{Q}[\psi] \subseteq \mathbb{Q}[\eta]$. Each of these statements implies $\mathbb{Q}_\psi \subseteq \mathbb{Q}_\eta$.

From Theorem 1.4 it follows that if two rows of the character table have the same "pattern" (i.e. are of the same type), then they are realized in the same field.

Theorem 1.4 holds for Brauer characters as well. Let $p$ be a prime, $\text{Ibr}(G)$ the set of irreducible Brauer characters, and $\text{Ipi}(G)$ the set of principal indecomposable characters of $G$ in characteristic $p$. Considering the
SFCAs $Q(Ibr(G))$ and $Q(Ipi(G))$, defined analogously to $Q(Irr(G))$, we get analogs of Theorem 1.4 for generalized Brauer characters and generalized principal indecomposable characters of $G$. For details see Section IV.

The fourth SFC associated with the group $G$ we wish to consider is $Z(QG)$, the center of the group algebra over $Q$. Denote by $\bar{C}$ the class sum corresponding to a conjugacy class $C$ of $G$. That is, $\bar{C} = \sum x \in C, x$. Let $B = \{\bar{C}_1, \bar{C}_2, \ldots, \bar{C}_k\}$. It is well known that $B$ is a basis of $Z(QG)$. For every conjugacy class $C$ of $G$ let

$$M(C; B) = M(\bar{C}; B),$$

and set the matrix

$$Y = \begin{bmatrix} |C| \chi_j(C_1) \\ \chi_j(1) \end{bmatrix}.$$

It is known that

$$Y^{-1} M(C; B) Y = \operatorname{diag} \left[ \frac{|C| \chi_1(C)}{\chi_1(1)}, \frac{|C| \chi_2(C)}{\chi_2(1)}, \ldots, \frac{|C| \chi_k(C)}{\chi_k(1)} \right].$$

Next, let $T(C)$, the type of the conjugacy class $C$, be defined by

$$T(C) = T \left[ \frac{\chi_1(C)}{\chi_1(1)}, \frac{\chi_2(C)}{\chi_2(1)}, \ldots, \frac{\chi_k(C)}{\chi_k(1)} \right].$$

The smallest subfield of $\mathbb{C}$ containing $Q$ and the numbers $\chi_1(C)/\chi_1(1)$, $\chi_2(C)/\chi_2(1)$, $\ldots$, $\chi_k(C)/\chi_k(1)$ is denoted by $Q_C$ and is referred to as the field in which $C$ is realized. Applying our results on SFCAs to $Z(QG)$, we shall obtain in Section IV:

**Theorem 1.5.** Let $G$ be a finite group. Then:

(a) There exists an element $u \in Z(QG)$ such that each element of $Z(QG)$ is a polynomial in $u$ with rational coefficients.

(b) For every conjugacy class $C$ of $G$ the equality $Q_C = Q(T(C))$ holds.

(c) Let $C$ and $D$ be conjugacy classes of $G$. Then the following statements are equivalent: (i) $T(D) \geq T(C)$; (ii) $Q_D \subseteq Q_C$. Each of these statements implies $Q_D \subseteq Q_C$.

**Remark.** The matrices $M(\theta; \text{Irr}(G))$ for a character $\theta$ of $G$, $M(\eta; \text{Ibr}(G))$ for a Brauer character $\eta$ of $C$, and $M(C; B)$ (where $B$ is the set of all class sums of $G$) for a conjugacy class $C$ of $G$ have non-negative integer entries. Hence, much more can be deduced about them.
using the theory of nonnegative matrices. This has been done separately for characters, for Brauer characters, and for conjugacy classes in [2, 5]. A unified approach to SFCAs with basis $\mathcal{B}$ in which $M(a; \mathcal{B})$ are matrices with nonnegative entries is the subject of a forthcoming paper.

**Generalized Circulants.** Our matrix-theoretical notation here is the standard one, taken mainly from [6]. Let $\mathbb{F}$ be an arbitrary field, and let $f(x) \in \mathbb{F}[x]$ be a polynomial with no repeated roots in its splitting field over $\mathbb{F}$. Denote the companion matrix of $f(x)$ over $\mathbb{F}$ by $C_f$ (see [6, pp. 77-78]), and let $\mathbb{F}[C_f] = \{ g(C_f) | g(x) \in \mathbb{F}[x] \}$. As pointed out in [6, pp. 77-78]), $\mathbb{F}[C_f]$ can be viewed as a generalization of the algebra of circulant matrices over $\mathbb{F}$ (in [6] $\mathbb{F} = \mathbb{C}$). We call the elements of $\mathbb{F}[C_f]$ $f(x)$-circulants. In Section V we use the results of Section II to conclude that if $\mathbb{F}$ is infinite, then every subalgebra of $\mathbb{F}[C_f]$ is of the form $\mathbb{F}[M]$ for some matrix $M$ in $\mathbb{F}[C_f]$. Moreover, if $M_1, M_2$ are $f(x)$-circulants, we give a necessary and sufficient condition, in terms of the types of $M_1$ and $M_2$, for $M_1$ to be in $\mathbb{F}[M_2]$. We shall see that $f(x)$-circulants enjoy many properties of the circulants. We shall also comment on block construction of $f(x)$-circulants. We point out that properties of circulants and many of their generalizations follow directly from results on the algebra $\mathbb{F}[C_f]$.

**Generalized Cyclic Codes.** Our coding-theoretical notation and notions are generalizations of the ones in [10]. Let $\mathbb{F}$ be a field, and let $f(x)$ be a reducible polynomial of degree $n$ over $\mathbb{F}$ with distinct roots in its splitting field. The algebra $A = \mathbb{F}[x]/f(x)$ is a SFCA over $\mathbb{F}$. Its ideals are subalgebras, which we call generalized cyclic codes or $f(x)$-codes (a cyclic code is an ideal of $\mathbb{F}[x]/(x^n - 1)$ for some $n$). Elements of $f(x)$-codes are called codewords.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(x)$ in its splitting field $\mathbb{K}$ over $\mathbb{F}$. The elements $a(\alpha_1), a(\alpha_2), \ldots, a(\alpha_n)$ of $\mathbb{K}$ are the coefficients of the so-called Matteson-Solomon polynomial of $a(x) + (f(x)) \in A$, where $\deg(a(x)) < n$ (see [10, p. 239]). We observe here that these elements are in fact the eigenvalues of the regular representation of $A$. Using this observation, the isomorphism presented in [10, pp. 240-242] between $A$ and the set of the corresponding Matteson-Solomon polynomials can be shown to be "natural" and can be obtained without the computations done in [10].

It is known that every $f(x)$-code $C$ is generated (as an ideal) by a unique idempotent polynomial $e(x)$ [modulo $f(x)$]. It follows that $C = \mathbb{F}[xe(x)]$, which mean that each codeword is a polynomial in $xe(x)$ with coefficients in $\mathbb{F}$. We give a necessary and sufficient condition, in term of the Matteson-Solomon coefficients, for a code word $a(x)$ to satisfy $C = \mathbb{F}[a(x)]$. Other observations on generalized cyclic codes are made in Section VI.
II. REGULAR REPRESENTATIONS OF SEMISIMPLE ALGEBRAS

We start with several preliminary facts.

**Lemma 2.1.** Let $A$ be an $n$-dimensional, commutative algebra with 1 over a field $\mathbb{F}$, and let $\mathcal{B}$ be a basis of $A$.

(a) If $a, b \in A$ then $M(ab; \mathcal{B}) = M(a; \mathcal{B})M(b; \mathcal{B})$. In particular, the elements of $M(A; \mathcal{B})$ commute.

(b) The mapping $a \to M(a; \mathcal{B})$ is an algebra isomorphism between $A$ and $M(A; \mathcal{B}) = \{M(a; \mathcal{B}) | a \in A\}$. Moreover, for every basis $\mathcal{C}$ of $A$ the set $\{M(c; \mathcal{B}) | c \in \mathcal{C}\}$ is a basis of $M(A; \mathcal{B})$ over $\mathbb{F}$. Furthermore, $M(1; \mathcal{B})$ is an identity matrix, and if $c$ is invertible in $A$ then $M(c^{-1}; \mathcal{B}) = M(c; \mathcal{B})^{-1}$.

(c) If $A$ is a semisimple and separable, then there exists an $n \times n$ matrix $X$ over some extension field of $\mathbb{F}$ such that $X^{-1}M(a; \mathcal{B})X$ is diagonal for every $a \in A$.

**Proof.** (a): Let $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$. Write

$$M(a; \mathcal{B}) = (m_{ij}(a; \mathcal{B})), \quad M(b; \mathcal{B}) = (m_{ij}(b; \mathcal{B})), \quad M(ab; \mathcal{B}) = (m_{ij}(ab; \mathcal{B})).$$

Then

$$\sum_{j=1}^{n} m_{ij}(ab; \mathcal{B})b_j = ab \cdot b_i = a(b \cdot b_i) = a \cdot \sum_{k=1}^{n} m_{ik}(b; \mathcal{B})b_k$$

$$= \sum_{k=1}^{n} m_{ik}(b; \mathcal{B})a \cdot b_k$$

$$= \sum_{k=1}^{n} m_{ik}(b; \mathcal{B}) \left( \sum_{j=1}^{n} m_{kj}(a; \mathcal{B}) \cdot b_j \right)$$

$$= \sum_{j=1}^{n} \left( \sum_{k=1}^{n} m_{ik}(b; \mathcal{B}) \cdot m_{kj}(a; \mathcal{B}) \right) b_j.$$

It follows that

$$m_{ij}(ab; \mathcal{B}) = \sum_{k=1}^{n} m_{ik}(b; \mathcal{B}) \cdot m_{kj}(a; \mathcal{B}).$$
As \( ab = ba \), we get
\[
m_{ij}(ba; \mathcal{B}) = \sum_{k=1}^{n} m_{ik}(b; \mathcal{B}) \cdot m_{kj}(a; \mathcal{B}),
\]
and so \( M(ba; \mathcal{B}) = M(b; \mathcal{B}) \cdot M(a; \mathcal{B}) \) as claimed. This and the fact that \( ab = ba \), imply now that \( M(b; \mathcal{B}) \cdot M(a; \mathcal{B}) = M(a; \mathcal{B}) \cdot M(b; \mathcal{B}) \).

(b): The mapping \( a \rightarrow M(a; \mathcal{B}) \) is the composition of three algebra isomorphisms:

\[
A \xrightarrow{f_1} \{ T_a \mid a \in A \} \xrightarrow{f_2} \{ M^t \mid M \in M(A; \mathcal{B}) \} \xrightarrow{f_3} M(A; \mathcal{B}),
\]

where \( f_1 \) is the regular representation of \( A \), \( f_2(T_a) = [M(a; \mathcal{B})]^t \) is the matrix representation of \( T_a \) relative to the basis \( \mathcal{B} \), and \( f_3(M^t) = M \). To see that \( f_1 \) is injective, let \( a, b \in A \) satisfy \( T_a = T_b \). Then \( a = a \cdot 1 = b \cdot 1 = b \). Note that as elements of \( \{ M^t \mid M \in M(A; \mathcal{B}) \} \) commute, \( f_3 \) is an isomorphism. The second and third statements of part (b) are clear. (This proof is that of [4, Proposition 1.11 with \( C \) replaced by \( \mathbb{F} \).)

(c): See the proof of the corollary in [11, p. 13]. Note that there, the field need not be perfect as long as the algebra is separable.

**NOTATION.** Let \( A \) be a separable SFCA of dimension \( n \) over a field \( \mathbb{F} \), and let \( \mathcal{B} \) be a basis of \( A \). Recall that a matrix \( X \) such that \( X^{-1} M(a; \mathcal{B}) X \) is diagonal for every \( a \in A \) is called a diagonalizing matrix of \( A \) with respect to \( \mathcal{B} \). By the previous lemma such a matrix exists.

The following simple fact from linear algebra will be needed:

**Lemma 2.2.** Let \( \mathbb{F} \) be a field, and let \( \mathbb{K} \) be an extension field. Let \( M_1, M_2, \ldots, M_k \) be \( n \times n \) matrices with entries in \( \mathbb{F} \) that are linearly independent over \( \mathbb{F} \). Then:

(a) \( M_1, M_2, \ldots, M_k \) are linearly independent over \( \mathbb{K} \) as well.

(b) \( X^{-1} M_1 X, X^{-1} M_2 X, \ldots, X^{-1} M_k X \) are linearly independent over \( \mathbb{K} \) for every \( n \times n \) matrix \( X \) over \( \mathbb{K} \).

**Proof.** Set \( M_\alpha = (m_{\alpha ij}), \alpha = 1, 2, \ldots, k \). Suppose \( \sum_{\alpha=1}^{k} a_\alpha M_\alpha = 0 \) for \( a_\alpha \in \mathbb{K} \), where not all the \( a_\alpha \) vanish. Then

\[
\sum_{\alpha=1}^{k} a_\alpha m_{\alpha ij} = 0, \quad \text{for all } i \text{ and } j.
\]
Consider the following system of $n^2$ linear equations with the $k$ unknowns $x_1, x_2, \ldots, x_k$:

$$\sum_{\alpha=1}^{k} m_{\alpha ij} x_{\alpha} = 0 \quad i, j = 1, 2, \ldots, n.$$ 

This is a homogeneous system over $\mathbb{F}$, as well as over $\mathbb{K}$. Let $C$ be the coefficient matrix of the system. Then $C$ is an $n^2 \times k$ matrix over $\mathbb{F}$ (and over $\mathbb{K}$). By (2.1) the system has a nontrivial solution in $\mathbb{K}$. Thus the rank of $C$ is less than $k$. But since $C$ is a matrix over $\mathbb{F}$, its rank over $\mathbb{F}$ equals its rank over $\mathbb{K}$. It follows that $Cx = 0$ has a nontrivial solution $x = (c_1, c_2, \ldots, c_k)^t$ in $\mathbb{F}$. So $\sum_{\alpha=1}^{k} c_\alpha m_{\alpha ij} = 0$ for all $i$ and $j$; thus $\sum_{\alpha=1}^{k} c_\alpha M_\alpha = 0$ for $c_\alpha \in \mathbb{F}$, where not all the $c_\alpha$ vanish. This contradicts the fact that the $M_\alpha$ are linearly independent over $\mathbb{F}$, and (a) follows. Now part (b) is obvious. 

The next result explains why in the example of Section I, the rows of the diagonalizing matrix $X$ in (1.1) are the diagonals of the matrices $X^{-1} M(b_i; B) X$, $i = 1, 2, 3, 4$ in (1.2).

**Theorem 2.3.** Let $A$ be a separable, semisimple, $n$-dimensional, commutative algebra over a field $\mathbb{F}$. Let $B = \{b_1, b_2, \ldots, b_n\}$ be a basis of $A$, and let $X$ be a diagonalizing matrix of $A$ with respect to $B$. For all $b \in A$ set $X^{-1} M(b; B) X = \text{diag}(b(1), b(2), \ldots, b(n))$, and put $Y = (b_i(j))$. Then $Y$ (which is an $n \times n$ matrix over some extension of $\mathbb{F}$) is also a diagonalizing matrix of $A$ with respect to $B$. In fact,

$$Y^{-1} M(a; B) Y = \text{diag}(a(1), a(2), \ldots, a(n)) = X^{-1} M(a; B) X \quad \text{for all} \quad a \in A.$$ 

**Proof.** Let $E_i$ be the matrix whose $(i, i)$th entry is 1 and all other entries are zero. Then $E_i E_j = \delta_{ij} E_i$. Set $F_i = X E_i X^{-1}$. Then

$$F_i F_j = X E_i E_j X^{-1} = X \delta_{ij} E_i X^{-1} = \delta_{ij} F_i.$$ 

Take $a \in A$; then

$$X^{-1} M(a; B) X = \text{diag}(a(1), a(2), \ldots, a(n)) = \sum_{j=1}^{n} a(j) E_j,$$
and therefore
\[ M(a; B) = \sum_{j=1}^{n} a(j)F_j. \] (2.2)

We know that \( X \) is a matrix over some extension field \( \mathbb{K} \) of \( \mathbb{F} \), and that \( a(i) \in \mathbb{K} \) for all \( a \in A \) and \( i = 1, 2, \ldots, n \). Set \( \mathcal{F} = \{F_1, F_2, \ldots, F_n\} \), and let \( L \) be the vector space spanned over \( \mathbb{K} \) by \( \mathcal{F} \). As \( F_iF_j = \delta_{ij}F_i \), it follows that \( L \) is a commutative \( \mathbb{K} \)-algebra. Since the \( E_i \) are linearly independent over \( \mathbb{K} \), so are the \( F_i \). Further, from (2.2) we see that \( M(a; B) \in L \) for all \( a \in A \). Moreover, we obviously have \( I = \sum_{j=1}^{n} F_j \in L \).

By part \((b)\) of Lemma 2.1, \( \mathcal{B}' = \{M(b_i; B) \mid i = 1, 2, \ldots, n\} \) is a basis of \( M(A; B) \). Hence the \( M(b_i; B) \) are matrices over \( \mathbb{F} \) which are linearly independent over \( \mathbb{F} \). Now, by Lemma 2.2 these \( n \) matrices are linearly independent over \( \mathbb{K} \) as well; and since \( \mathcal{B}' \subseteq L \), it follows that \( \mathcal{B}' \) is a basis of \( L \). So both \( \mathcal{B}' \) and \( \mathcal{F} \) are bases of \( L \). By (2.2) we get \( M(b_i; B) = \sum_{j=1}^{n} b_i(j)F_j \). Hence the matrix \( Y^t \) is the transition matrix from the basis \( \mathcal{F} \) to the basis \( \mathcal{B}' \).

Let \( a \in A \). Define a linear mapping \( R_a : L \rightarrow L \) by \( R_a(N) = M(a; B)N \) for all \( N \in L \). Let us find the representing matrices of \( R_a \) with respect to \( \mathcal{B}' \) and \( \mathcal{F} \). First,

\[
R_a(M(b_i; B)) = M(a; B)M(b_i; B) = M(ab_i; B)
\]

\[
= M \left( \sum_{j=1}^{n} m_{ij}(a; B)b_j ; B \right) = \sum_{j=1}^{n} m_{ij}(a; B)M(b_j; B).
\]

Thus the representing matrix of \( R_a \) in the basis \( \mathcal{B}' \) is \((m_{ij}(a; B))^t = (M(a; B))^t \). Next, we use (2.2) to obtain

\[ R_a(F_i) = M(a; B)F_i = \sum_{j=1}^{n} a(j)F_jF_i = a(i)F_i. \]

Thus the representing matrix of \( R_a \) with respect to \( \mathcal{F} \) is

\[ D = \text{diag}(a(1), a(2), \ldots, a(n)) = X^{-1}M(a; B)X. \]

It follows that \((M(a; B))^t = (Y^t)^{-1}DY^t = (YDY^{-1})^t \), and so \( M(a; B) = YDY^{-1} \), which implies that \( Y^{-1}M(a; B)Y = D \) as claimed.
REMARK. By Theorem 2.3 we know that there exists a diagonalizing matrix $Y$ whose $i$th row consists of some arrangement of the eigenvalues of $M(b_i, B)$, $i = 1, 2, \ldots, n$. We shall show later that in fact every diagonalizing matrix can be obtained from this $Y$ by multiplying each column of $Y$ by a suitable element of the field $K$ in which $Y$ resides.

COROLLARY 2.4. Let $A$ be a separable, semisimple, $n$-dimensional, commutative algebra over a field $F$. Let $B$ be a basis of $A$, and let $X$ be a diagonalizing matrix of $A$ with respect to $B$. For all $b \in A$ set $X^{-1}M(b; B)X = \text{diag}(b(1), b(2), \ldots , b(n))$. Then a subset $C = \{c_1, c_2, \ldots, c_n\}$ of $A$ is a basis of $A$ if and only if the matrix $(c_i(j))$ is nonsingular.

Proof. Set

$$M(C; B) = \{M(c_i; B) \mid 1 \leq i \leq n\} \subseteq M(A; B),$$

$$X^{-1}M(C; B)X = \{X^{-1}M(c_i; B)X \mid 1 \leq i \leq n\}.$$ 

The matrix $X$ and the members of $X^{-1}M(C; B)X$ are matrices over some extension field $K$ of $F$.

Clearly, the following four statements are equivalent: (i) $C$ is a basis of $A$; (ii) $C$ is a linearly independent set over $F$; (iii) $M(C; B)$ is a linearly independent set over $F$ [see Lemma 2.1(b)]; (iv) $X^{-1}M(C; B)X$ is a linearly independent set over $K$ (Lemma 2.2 is used here). Since the matrices in $X^{-1}M(C; B)X$ are diagonal, we find that (iv) holds if and only if the vectors \{(c_i(1), c_i(2), \ldots , c_i(n))\} $\subseteq K^n$, $i = 1, 2, \ldots , n$, are linearly independent over $K$. Now the corollary follows.

NOTATION. Let $n$ be a positive integer, and let $P = \{P_1, P_2, \ldots , P_r\}$ be a partition of $\{1, 2, 3, \ldots , n\}$. The size of $P$, denoted by $|P|$, is the number $r$. If $r = n$, we call the partition $P$ trivial. Each of the $P_i$ will be called a part of $P$. Clearly, if $Q$ is a refinement of $P$ then $|Q| \geq |P|$. 

The following is a preliminary lemma needed for the proof of Theorems 1.1 and 1.2.

LEMMA 2.5. Let $A$ be a separable, semisimple, $n$-dimensional, commutative algebra over a field $F$. Let $B$ be a basis of $A$, and let $X$ be a diagonalizing matrix of $A$ with respect to $B$.

(a) If $P$ is a partition of $\{1, 2, \ldots , n\}$, then $F(P)$ is a subalgebra of $A$. Moreover, if $a \in F(P)$ is invertible in $A$, then $a^{-1} \in F(P)$. 

(b) A partition $P$ of $\{1,2,\ldots,n\}$ is trivial if and only if $\mathbb{F}(P) = A$.

(c) Let $a \in A$. Then $\dim_{\mathbb{F}} F[a]$, the dimension of $F[a]$ over $\mathbb{F}$, satisfies

$$\dim_{\mathbb{F}} F[a] = \text{degree } m_a(x) = |T(a)|.$$ 

(d) Let $a, b \in A$ be such that $F[a] \subseteq F[b] = \mathbb{F}(T(a))$. Then $F[a] = F[b]$.

(e) If $\mathbb{F}$ is infinite and $A$ has only finitely many $\mathbb{F}$-subalgebras, then there exists an element $u \in A$ with $A = F[u]$.

(f) Let $a, b \in A$ be such that $F[a] \subseteq F[b] = \mathbb{F}(T(a))$. Then $F[a] = F[b]$.

(g) Let $a \in A$. If $m_a(x)$ is irreducible over $\mathbb{F}$, then $T(a)$ consists of $\dim_{\mathbb{F}} F[a]$ parts of equal size.

**Proof.** Let $w \in A$. We set $X^{-1}M(w;B)X = \text{diag}(w(1), w(2), \ldots, w(n))$, and write $B = \{b_1, b_2, \ldots, b_n\}$.

(a): Note that $a \in F \cdot 1$ if and only if $a = \alpha \cdot 1$ for some $\alpha \in F$. This holds precisely when $m_a(x) = x - \alpha$, which is equivalent to

$$M(a;B) = X^{-1}M(a;B)X = \text{diag}(\alpha, \alpha, \ldots, \alpha).$$

This is the same as $T(a) = \{1,2,\ldots,n\}$, i.e., $|T(a)| = 1$. Hence [in addition to proving part (f)], we get that $P \subseteq T(a)$ for all $a \in F \cdot 1$. Thus, $F \cdot 1 \subseteq \mathbb{F}(P)$. In particular, $\mathbb{F}(P)$ is not empty.

Set $P = \{P_1, P_2, \ldots, P_r\}$, and let $c, d \in \mathbb{F}(P)$. We now show that $\{c - d, cd\} \subseteq \mathbb{F}(P)$, and that if $c$ is invertible then $c^{-1} \in \mathbb{F}(P)$. By the definition of $\mathbb{F}(P)$ we have $P \subseteq T(c)$ and $P \subseteq T(d)$. Fix $i$, and set $P = P_i$. Then there exist $C \in T(c)$ and $D \in T(d)$ such that $P \subseteq C \cap D$. Using Lemma 2.1, we obtain

$$X^{-1}M(c - d;B)X = X^{-1}M(c;B)X - X^{-1}M(d;B)X$$

$$= \text{diag}(c(1) - d(1), c(2) - d(2), \ldots, c(n) - d(n))$$

and

$$X^{-1}M(cd;B)X = X^{-1}M(c;B)X \cdot X^{-1}M(d;B)X$$

$$= \text{diag}(c(1)d(1), c(2)d(2), \ldots, c(n)d(n)),$$ (2.3a)

and if $c$ is invertible in $A$, then

$$X^{-1}M(c^{-1};B)X = (X^{-1}M(c;B)X)^{-1}$$

and

$$X^{-1}M(cd;B)X = X^{-1}M(c;B)X \cdot X^{-1}M(d;B)X$$

$$= \text{diag}(c(1)d(1), c(2)d(2), \ldots, c(n)d(n)),$$ (2.3b)
(2.3c) \[
\text{diag} \left( \frac{1}{c(1)}, \frac{1}{c(2)}, \ldots, \frac{1}{c(n)} \right)
\]

Let \( \{\alpha, \beta\} \subseteq P \subseteq C \cap D \). Then \( c(\alpha) = c(\beta) \) and \( d(\alpha) = d(\beta) \). By (2.3),

\[
(c - d)(\alpha) = c(\alpha) - d(\alpha) = c(\beta) - d(\beta) = (c - d)(\beta),
\]

\[
(cd)(\alpha) = c(\alpha)d(\alpha) = c(\beta)d(\beta) = (cd)(\beta),
\]

and if \( c \) is invertible, then

\[
c^{-1}(\alpha) = \frac{1}{c(\alpha)} = \frac{1}{c(\beta)} = c^{-1}(\beta).
\]

Since this is true for all \( \{\alpha, \beta\} \subseteq P \), we conclude that \( P \) is contained in one of the parts of the partition \( T(c - d) \) as well as in one of the parts of \( T(cd) \). As \( P \) is an arbitrary part of \( P \), this means that \( P \subseteq T(c - d) \) and \( P \subseteq T(cd) \), which yields that \( \{c - d, cd\} \subseteq \mathbb{F}(P) \). Moreover, if \( c \) is invertible, then \( P \) is contained in one of the parts of the partition \( T(c^{-1}) \); so that \( P \subseteq T(c^{-1}) \), which implies \( c^{-1} \in \mathbb{F}(P) \). This proves that \( \mathbb{F}(P) \) is a subring of \( A \), containing all inverses of its invertible elements.

To prove that \( \mathbb{F}(P) \) is subalgebra we take \( \lambda \in \mathbb{F} \) and show that \( \lambda c \in \mathbb{F}(P) \). Clearly

\[
X^{-1}M(\lambda c; B)X = \lambda X^{-1}M(c; B)X = \text{diag} (\lambda c(1), \lambda c(2), \ldots, \lambda c(n)).
\]

Again for \( \{\alpha, \beta\} \subseteq P \) we get \( (\lambda c)(\alpha) = (\lambda c)(\beta) \), so \( P \) is contained in one of the parts of \( T(\lambda c) \). Thus \( P \subseteq T(\lambda c) \) and consequently \( \lambda c \in \mathbb{F}(P) \).

(b): Assume that \( A = \mathbb{F}(Q) \). If \( Q \) is not trivial, then there exists \( Q \in Q \) such that \( Q \) contains at least two elements. Let \( \{\alpha, \beta\} \subseteq Q \), \( \alpha \neq \beta \); and let \( a \in A \). Then \( Q \subseteq T(a) \), so that \( Q \) is contained in one of the parts of \( T(a) \). It follows that \( a(\alpha) = a(\beta) \) for all \( a \in A \). This implies that \( b_i(\alpha) = b_i(\beta) \) for \( i = 1, 2, \ldots, n \). Thus the \( o \)th and \( \beta \)th columns of the matrix \( (b_i(j)) \) are identical. This contradicts Corollary 2.4. Hence \( Q \) is trivial.

Conversely, assume \( Q \) is trivial. Then \( Q \subseteq T(a) \) for all \( a \in A \); so \( a \in \mathbb{F}(Q) \) for all \( a \in A \). Thus, \( A = \mathbb{F}(Q) \).

(c): Set \( m = |T(a)| \). By definition, \( m \) equals the number of distinct eigenvalues of \( M(a; B) \). As \( M(a; B) \) is diagonalizable, \( m \) is equal to the degree of \( m_a(x) \). Now, the set \( \{1, a, a^2, \ldots, a^{m-1}\} \) is linearly independent over \( \mathbb{F} \), because otherwise the degree of \( m_a(x) \) would be less than \( m \). As \( \{1, a, a^2, \ldots, a^m\} \) is a linearly dependent set over \( \mathbb{F} \), we get \( m = \dim_{\mathbb{F}} \mathbb{F}[a] \).

(d): Let \( a, b \in A \) with \( \mathbb{F}[a] \subseteq \mathbb{F}[b] = \mathbb{F}(T(a)) \). Then, \( \dim_{\mathbb{F}} \mathbb{F}[a] \leq \dim_{\mathbb{F}} \mathbb{F}[b] \). As \( b \in \mathbb{F}(T(a)) \), we know that \( T(a) \subseteq T(b) \), and therefore
\( |T(b)| \leq |T(a)| \). By part (c) \( \dim_F F[b] \leq \dim_F F[a] \). Hence \( \dim_F F[a] = \dim_F F[b] \), and as \( F[a] \subseteq F[b] \), we get \( F[a] = F[b] \).

(e): Let \( g_1, g_2, \ldots, g_s \) be generators of \( A \) as an algebra over \( F \), and let us prove our claim by induction on \( s \). The induction assumption implies that the subalgebra of \( A \) generated by \( g_2, \ldots, g_s \) has the form \( F[u] \) for some \( u \in A \). So \( A \) is generated by \( v = g_1 \) and \( u \). Consider the subalgebras of the form \( F[u + \lambda v] \) for \( \lambda \in F \). As \( F \) is infinite and \( A \) has only a finite number of subalgebras, we can find \( \gamma, \delta \in F \), \( \gamma \neq \delta \), such that \( F[u + \gamma v] = F[u + \delta v] \). Now,

\[
v = \frac{1}{\gamma - \delta} (u + \gamma v - u - \delta v) \in F[u + \gamma v].
\]

It follows that \( \gamma v \in F[u + \gamma v] \), so that \( u = u + \gamma v - \gamma v \in F[u + \gamma v] \). Thus \( A = F[u + \gamma v] \).

Note that the proof of (e) is the same as the one given in field theory (e.g. last ten lines of \([9, p. 290]\)).

(f): See the beginning of the proof of part (a).

(g): Let \( k \) be the largest integer for which \( (m_a(x))^k \) divides \( p_a(x) \). Set \( g(x) = p_a(x)/(m_a(x))^k \). Then \( g(x) \in F[x] \), and \( m_a(x) \) does not divide \( g(x) \). Suppose \( g(x) \) is not 1. If \( (g(x), m_a(x)) \neq 1 \) then \( m_a(x) \) divides \( g(x) \), as \( m_a(x) \) is irreducible. This is impossible. Therefore \( (g(x), m_a(x)) = 1 \). A known fact of linear algebra states that \( p_a(x) \) divides \( (m_a(x))^n \) for some \( n \). Thus \( g(x) \) divides some power of \( m_a(x) \) over \( F \). Since \( m_a(x) \) is irreducible, \( g(x) \) itself is a power of \( m_a(x) \), a contradiction. Thus \( g(x) = 1 \), and so \( p_a(x) = (m_a(x))^k \). Let \( m \) be the degree of \( m_a(x) \). Then \( M(a; B) \) has exactly \( m \) distinct eigenvalues, each of algebraic multiplicity \( k \). Let \( P \) be an arbitrary part of \( T(a) \). By definition, \( \{i, j\} \subseteq P \) if and only if \( a(i) = a(j) \). Since for every \( i \) there are exactly \( k \) indices \( j \) (including \( i \) itself) with \( a(i) = a(j) \), we find that the size of \( P \) is \( k \).

**COROLLARY 2.6.** Let \( A \) be a separable, semisimple, finite dimensional, commutative algebra over a field \( F \). Let \( a \in A \). Then \( A = F[a] \) if and only if all the roots of \( p_a(x) \) in its splitting field over \( F \) are distinct.

**Proof.** Let \( B \) be a fixed basis of \( A \), and let \( X \) be a diagonalizing matrix of \( A \) with respect to \( B \). Let \( n \) be the dimension of \( A \) over \( F \). Suppose first that \( p_a(x) \) has no repeated roots in its splitting field over \( F \). By our assumption, the minimal polynomial of \( M(a; B) \) equals the characteristic polynomial of \( M(a; B) \). By Theorem 5 in \([11, p. 23]\), every matrix commuting with \( M(a; B) \) is a polynomial in \( M(a; B) \) with coefficients in \( F \). Let \( c \in A \). Then \( M(c; B) \) commutes with \( M(a; B) \), as, by Lemma 2.1, \( M(A; B) \)
is a commutative algebra. It follows that

$$M(c; B) = \sum_{i=1}^{s} \alpha_i (M(a; B))^i$$

with $\alpha_i \in \mathbb{F}$, $i = 1, 2, \ldots, s$.

By Lemma 2.1(b),

$$M(c; B) = \sum_{i=1}^{s} \alpha_i a_i^i$$

Lemma 2.1 now implies that $c = \sum_{i=1}^{s} \alpha_i a_i \in \mathbb{F}[a]$, as claimed.

Conversely, assume that $A = \mathbb{F}[a]$. For every $b \in A$ we write $X^{-1} M(b; B) X = \text{diag}(b(1), b(2), \ldots, b(n))$. If $p_a(x)$ has repeated roots in its splitting field, then $a(i) = a(j)$ for some $i$ and $j$, $i \neq j$. Thus, $T(a)$ is nontrivial. As $a$ belongs to the subalgebra $\mathbb{F}(T(a))$, we get $A = \mathbb{F}[a] \subseteq \mathbb{F}(T(a))$. This contradicts Lemma 2.5(b). We conclude that $p_a(x)$ has no repeated roots.

**REMARKS.** (a) The assumptions that $A$ is separable and semisimple are used only in one of the parts of the above proof. In fact, the first part of the proof shows that if $A$ is any finite-dimensional, commutative algebra over $\mathbb{F}$, and $a \in A$ is such that $p_a(x)$ has no repeated roots in its splitting field over $\mathbb{F}$, then $A = \mathbb{F}[a]$.

(b) In the first part of the proof of Corollary 2.6, we manage to obtain scalars $\alpha_1, \alpha_2, \ldots, \alpha_s$ such that $c = \sum_{i=1}^{s} \alpha_i a_i$. The existence of such $\alpha_i$ in the splitting field of $p_a(x)$ over $\mathbb{F}$ follows easily, since the coefficient matrix of the system $c(j) = \sum_{i=1}^{n} x_i a(j)^i$ is a Vandermonde. What we have shown is that the $\alpha_i$ are in fact in $\mathbb{F}$.

**Proof of Theorem 1.1.** Part (b) of the theorem coincides with Corollary 2.6, so let us prove part (a). We prove it by induction on the dimension $n$ of $A$ over $\mathbb{F}$. If $n = 1$ then $A = \mathbb{F} \cdot 1 = \mathbb{F}[1]$, so take $n > 1$. Fix a basis $B$ of $A$ and a diagonalizing matrix $X$ of $A$ with respect to $B$. Let $S$ be an arbitrary proper subalgebra of $A$. Clearly $S$ is separable, and by induction we get $S = \mathbb{F}[a]$ for some $a \in A$. As $a$ belongs to the subalgebra $\mathbb{F}(T(a))$, we obtain $S = \mathbb{F}[a] \subseteq \mathbb{F}(T(a))$. If $T(a)$ is trivial, then $p_a(x)$ has no repeated roots in its splitting field over $\mathbb{F}$, and by Corollary 2.6 we have $A = \mathbb{F}[a]$, contradicting the choice of $S$ as a proper subalgebra. Thus $T(a)$ is not trivial.

We now use Lemma 2.5(b) to conclude that $\mathbb{F}(T(a))$ is a proper separable subalgebra of $A$. By induction we get $\mathbb{F}(T(a)) = \mathbb{F}[b]$ for some $b \in A$,
and consequently $S = \mathbb{F}[a] \subseteq \mathbb{F}[b] = \mathbb{F}(T(a))$. Lemma 2.5(d) now implies that $S = \mathbb{F}[a] = \mathbb{F}[b] = \mathbb{F}(T(a))$. It follows that every proper subalgebra of $A$ is of the form $\mathbb{F}(P)$ for some partition $P$ of $\{1, 2, \ldots, n\}$. Since the number of the partitions of $\{1, 2, \ldots, n\}$ is finite, we conclude that the number of subalgebras of $A$ is finite. Now the theorem follows from Lemma 2.5(e).

**Proof of Theorem 1.2.** (a): Let $C$ be a subalgebra of $A$. As $C$ satisfies the assumptions of Theorem 1.1, we get $C = \mathbb{F}[u]$ for some $u \in C$. Then clearly $C = \mathbb{F}[u] \subseteq \mathbb{F}(T(u))$, and again by Theorem 1.1 we obtain $\mathbb{F}(T(u)) = \mathbb{F}[b]$ for some $b \in A$; so $C = \mathbb{F}[u] \subseteq \mathbb{F}(T(u)) = \mathbb{F}[b]$. Lemma 2.5(d) implies now that $C = \mathbb{F}[b] = \mathbb{F}(T(u)) = \mathbb{F}[u]$.

(b): The inequality $T(b) \leq T(a)$ is equivalent to $a \in \mathbb{F}(T(b)) = \mathbb{F}[b]$. This is the same as $\mathbb{F}[a] \subseteq \mathbb{F}[b]$.

**Remark.** Let $A$ be a separable, semisimple, finite-dimensional, commutative algebra over a field $\mathbb{F}$. Assume that every subalgebra of $A$ has the form $\mathbb{F}[u]$ for some $u \in A$. Then evidently, the proof and conclusions of Theorem 1.2 hold even if $\mathbb{F}$ is finite.

**Corollary 2.7.** Let $A$ be a separable, semisimple, finite-dimensional, commutative algebra over an infinite field $\mathbb{F}$. Let $B = \{b_1, b_2, \ldots, b_n\}$ be a basis of $A$, and $X$ a diagonalizing matrix of $A$ with respect to $B$. For all $b \in A$ set $X^{-1}M(b; B)X = \text{diag}(b(1), b(2), \ldots, b(n))$, and let $Y$ be the $n \times n$ matrix defined by $Y = (b_i(j))$. Then each column of $X$ is of the form $a\gamma$, where $\gamma$ is some column of $Y$, and $a$ an element in an extension field of $\mathbb{F}$.

**Proof.** By Theorem 1.1 there exists $u \in A$ such that $A = \mathbb{F}[u]$. Corollary 2.6 implies that $p_u(x)$ has $n$ distinct roots in its splitting field over $\mathbb{F}$. Let $K$ be an extension of $\mathbb{F}$ that contains the entries of $X$. Then $b(i) \in K$ for all $b \in A$, and in particular $Y$ is a matrix over $K$. Let $z$ be a column of $X$. Then $z$ is an eigenvector of $M(b; B)$ for all $b \in B$. So $M(u; B)z = u(i)z$ for some $i$. The eigenvalues of $M(u; B)$ are of algebraic multiplicity 1, so that $z$ spans (over $K$) the eigenspace $V$ of $u(i)$. By Theorem 2.3, each of the columns of $Y$ is also an eigenvector for all $M(b; B), b \in B$; so $M(u; B)y = u(i)y$ for some column $y$ of $Y$. Thus $y$ spans $V$ over $K$ as well, and the proof is complete.

The following definition and two propositions are needed for the applications discussed in the proceeding sections.
DEFINITION. Let $A$ be a semisimple, $n$-dimensional algebra over a field $F$. A set $E = \{e_1, e_2, \ldots, e_n\}$ satisfying $e_ie_j = \delta_{ij}e_i$ is called a set of orthogonal (central) idempotents of $A$.

PROPOSITION 2.8. Let $A$ be a semisimple, $n$-dimensional, commutative algebra over an algebraically closed field $F$. Then:

(a) $A$ has a unique set of orthogonal idempotents $E = \{e_1, e_2, \ldots, e_n\}$.
(b) $E$ is a basis of $A$, and $\sum_{i=1}^{n} e_i = 1$.
(c) Each $e_i$ is a common eigenvector of $T_a$ for all $a \in A$. Further, if $a(i)$ is the eigenvalue in $F$ of $T_a$ corresponding to the eigenvector $e_i$, then $ae_i = a(i)e_i$, $i = 1, 2, \ldots, n$. Moreover, $a = \sum_{j=1}^{n} a(j)e_j$ for all $a \in A$.
(d) Let $B = \{b_1, b_2, \ldots, b_n\}$ be a basis of $A$. Then the matrix of eigenvalues $Y = (b_i(j))$ is a diagonalizing matrix of $A$ with respect to $B$. In fact,

$$Y^{-1}M(a; B)Y = \text{diag}(a(1), a(2), \ldots, a(n)) \quad \text{for all } a \in A.$$ 

Proof. There exists an isomorphism $\phi : F \oplus F \oplus \cdots \oplus F \to A$ from the direct sum of $n$ copies of $F$ into $A$. Let $e_i$ be the image (via $\phi$) in $A$ of the identity element of the $i$th copy of $F$. Then clearly, $E = \{e_1, e_2, \ldots, e_n\}$ is a set of orthogonal idempotents. The proof of the uniqueness is standard. This proves (a).

As part (b) is a well known, we now prove (c). Let $a \in A$. Then by part (b) we have $a = \sum_{i=1}^{n} a_ie_i$ for some $a_i \in F$. Thus, $T_a(e_i) = ae_i = a_ie_i$ for all $i = 1, 2, \ldots, n$, so (c) follows. To show part (d), let $a \in A$. As $T_a(e_i) = a(i)e_i$, we get $M(a; E) = \text{diag}(a(1), a(2), \ldots, a(n))$. Note that $h_i = \sum_{j=1}^{n} b_i(j)e_j$, which means that $Y^t = (b_i(j))$ is the transition matrix from the basis $E$ to the basis $B$ of $A$. It follows that $(Y^t)^{-1}M(a; E)Y^t = (M(a; B))^t$. So $YM(a; E)Y^{-1} = M(a; B)$, as claimed.

PROPOSITION 2.9. Let $C$ be a finite-dimensional algebra with 1 over a field $F$. Let $u \in C$, and set $A = \mathbb{F}[u]$. Let $T_u : A \to A$ be defined by $T_u(a) = ua$ for all $a \in A$, and let $p_u(x)$ be the characteristic polynomial of $T_u$. Assume that $p_u(x)$ has no repeated roots in its splitting field over $F$, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $p_u(x)$. Then:

(a) $A$ is a separable, semisimple, finite-dimensional, commutative algebra over $F$. 


(b) The matrix

\[
Y = \begin{bmatrix}
1 & 1 & 1 & \ldots & 1 \\
\alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \\
(\alpha_1)^2 & (\alpha_2)^2 & (\alpha_3)^2 & \ldots & (\alpha_n)^2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(\alpha_1)^{n-1} & (\alpha_2)^{n-1} & (\alpha_3)^{n-1} & \ldots & (\alpha_n)^{n-1}
\end{bmatrix}
\]

is a diagonalizing matrix of \( A \) with respect to the basis \( B = \{1, u, u^2, \ldots, u^{n-1}\} \). Moreover, if \( f(u) \) is an arbitrary element of \( A \) for some \( f(x) \in \mathbb{F}[x] \), then

\[
Y^{-1}M(f(u); B)Y = \text{diag}(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)).
\]

(c) If \( M \) is the companion matrix of \( p_u(x) \) over \( \mathbb{F} \), then \( M(A; B) = \mathbb{F}[M] \).

Proof. Clearly \( A \) is commutative and finite-dimensional. Let \( \mathbb{K} \) be the splitting field of \( m_u(x) = p_u(x) \) over \( \mathbb{F} \). By assumption, an arbitrary element of \( A \) has the form \( f(u) \) where \( f(x) \in \mathbb{F}[x] \). To see that \( A \) is semisimple, we prove next that \( A \) has no nonzero nilpotent elements. Indeed, suppose \( f(u)^m = 0 \) for some positive integer \( m \) and \( f(x) \in \mathbb{F}[x] \). It follows that \( 0 = T_{f(u)}^m = f(T_u)^m \). Thus \( m_u(x) \) divides \( f(x)^m \) in \( \mathbb{F}[x] \). It follows that \( (x - \alpha_i) \mid f(x) \) in \( \mathbb{K}[x] \) for all \( i \), so that \( p_u(x) \mid f(x) \). Hence, \( T_{f(u)} = f(T_u) = 0 \), which implies that \( f(u) = 0 \); and therefore \( A \) is semisimple.

Clearly \( M = M(u; B) \). A straightforward calculation shows that \( Y^{-1}MY = \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n) \), hence

\[
Y^{-1}M(f(u); B) = Y^{-1}f(M)Y = f(Y^{-1}MY) = \text{diag}(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n))
\]

for all \( f(x) \in \mathbb{F}[x] \), which proves (b).

Now, (b) implies that \( T_a \) is diagonalizable for every \( a \in A \), so that \( m_a(x) \) has no repeated roots in its splitting field. It follows that \( A \) is separable, which concludes the proof of part (a).

Part (c) follow from the fact that \( M(f(u); B) = f(M) \) for all \( f(x) \in \mathbb{F}[x] \).

Remark. It is interesting to note that the equality \( Y^{-1}MY = \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n) \) can be obtained from Theorem 2.3 without any calcula-
tions. Indeed, as $M$ has only simple eigenvalues, we know that $M$ is diagonalizable. Let $X$ be a matrix satisfying $X^{-1}MX = \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. As above, $X$ is a diagonalizing matrix for $A$ with respect to $B$. Set $b_i = u^i - 1$; then

$$X^{-1}M(b_i; B)X = \text{diag}((\alpha_1)^{i-1}, (\alpha_2)^{i-1}, \ldots, (\alpha_n)^{i-1})$$

$$= \text{diag}(b_1(1), b_1(2), \ldots, b_1(n)).$$

Now apply Theorem 2.3 to obtain the desired equality.

III. SEPARABLE FIELD EXTENSIONS

Proof of Theorem 1.3. We begin by noting that the field $\mathbb{K}$ in our theorem (and, in fact, any subfield of $\mathbb{K}$ containing $\mathbb{F}$) is a separable, semisimple, $n$-dimensional, commutative algebra over $\mathbb{F}$. Further, if $\mathcal{P}$ is a partition of \{1, 2, \ldots, n\} then by Lemma 2.5 we know that $\mathbb{F}(\mathcal{P})$ is a subfield of $\mathbb{K}$. We also note that $\mathbb{F}[a] = \mathbb{F}(a)$ for all $a \in A$.

Now, let $\mathcal{L}$ be an intermediate field $\mathbb{F} \subseteq \mathcal{L} \subseteq \mathbb{K}$. By Theorem 1.1, if $\mathbb{L}$ is infinite, then $\mathcal{L} = \mathbb{F}(u)$ for some $u \in \mathbb{K}$. If $\mathbb{F}$ finite the same is true, because the multiplicative group of $\mathcal{L}$ is a finite cyclic group. With this, parts (a)-(c) of our theorem follow from Theorems 1.1 and 1.2, the remark preceding the proof of Theorem 1.2, and Lemma 2.5.

Next, suppose $\mathbb{K}$ is a Galois extension of $\mathbb{F}$. Set $\text{Gal}(\mathbb{K}/\mathbb{F}) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Let $u \in \mathbb{K}$ be a primitive element; that is, $\mathbb{K} = \mathbb{F}(u)$. By Corollary 2.6, $p_u(x)$ has no repeated roots in its splitting field $\mathbb{K}$ over $\mathbb{F}$. So $p_u(x) = m_u(x)$. By Galois theory, $f(x) = \prod_{i=1}^{n}(x - \sigma_i(u)) \in \mathbb{F}[x]$ and $f(u) = 0$. It follows that $m_u(x) = f(x)$. So the $\sigma_i(u)$ are the eigenvalues of $T_u$.

Fix a basis $B$ of $\mathbb{K}$ over $\mathbb{F}$, and choose a diagonalizing matrix (which exists by Lemma 2.1), such that $X^{-1}M(u; B)X = \text{diag}(\sigma_1(u), \sigma_2(u), \ldots, \sigma_n(u))$. For every $a \in \mathbb{K}$ set $X^{-1}M(a; B)X = \text{diag}(a(1), a(2), \ldots, a(n))$. As $\mathbb{K} = \mathbb{F}(u)$, we can write $a = g(u)$ for $g(x) \in \mathbb{F}[x]$. So

$$X^{-1}M(a; B)X = X^{-1}M(g(u); B)X = g(X^{-1}M(u; B)X)$$

$$= \text{diag}(g(\sigma_1(u)), g(\sigma_2(u)), \ldots, g(\sigma_n(u)))$$

$$= \text{diag}(\sigma_1(g(u)), \sigma_2(g(u)), \ldots, \sigma_n(g(u)))$$

$$= \text{diag}(\sigma_1(a), \sigma_2(a), \ldots, \sigma_n(a)).$$

It follows that $a(i) = \sigma_i(a)$ for all $a \in \mathbb{K}$. This proves part (d). Part (e) now follows from (d) and Corollary 2.4.
IV. ORDINARY CHARACTERS, MODULAR CHARACTERS, AND CONJUGACY CLASSES OF FINITE GROUPS

NOTATION. Let $G$ be a finite group, and let $p$ be a prime number. In addition to the notation introduced in Section I we use the following notation for various sets associated with $G$:

- $\text{Con}(G)$: The set of all conjugacy classes of $G$.
- $\mathcal{L}_p(G)$: The set of $p$-regular elements of $G$ (a $p$-regular element is an element whose order is relatively prime to $p$).
- $\text{Con}_p(G)$: The set of all conjugacy classes of $p$-regular elements. These classes are called the $p$-regular classes of $G$.
- $\text{Cf}(G)$: The set of all complex class functions of $G$, that is, all complex functions $f$ such that $f(g) = f(x^{-1}gx)$ for all $x$ and $g$ in $G$.
- $\text{Cf}_p(G)$: The set of all complex-values functions $f$ on $\mathcal{L}_p(G)$ such that $f(g) = f(x^{-1}gx)$ for all $x$ in $G$ and $g \in \mathcal{L}_p(G)$.

If $f \in \text{Cf}(G)$ and $C \in \text{Con}(G)$ [or if $f \in \text{Cf}_p(G)$ and $C \in \text{Con}_p(G)$], we denote by $f(C)$ the value of $f$ on each element of $C$.

Recall that $\text{Irr}(G)$ is a basis of $\text{Cf}(G)$, and that both $\text{Ibr}(G)$ and $\text{Ipi}(G)$ are bases of $\text{Cf}_p(G)$. Evidently, both $\text{Cf}(G)$ and $\text{Cf}_p(G)$ are SFCAs over $\mathbb{C}$.

We note that the functions in $\text{Ipi}(G)$ vanish outside $\mathcal{L}_p(G)$. Throughout this section we view the elements of $\text{Ipi}(G)$ as functions on $\mathcal{L}_p(G)$.

Further recall that $\{\bar{C}_1, \bar{C}_2, \ldots, \bar{C}_k\}$, the set of class sums, is a basis of $Z(CG)$, the center of the group algebra over $\mathbb{C}$. Clearly $Z(CG)$ is a SFCA over $\mathbb{C}$.

Parts (a)--(c) of the following proposition were proved in [2, 4], where we used different arguments for each of the three algebras involved. Here we show that all three parts are special cases of Proposition 2.8.

PROPOSITION 4.1. Let $G$ be a finite group, and let $p$ be a prime number. Set

\[
\text{Con}(G) = \{C_1 = \{1\}, C_2, \ldots, C_k\},
\]
\[
\text{Con}_p(G) = \{K_1 = \{1\}, K_2, \ldots, K_s\},
\]
\[
\text{Irr}(G) = \{\chi_1 = 1_G, \chi_2, \ldots, \chi_k\},
\]
\[
\text{Ibr}(G) = \{\varphi_1 = 1_G, \varphi_2, \ldots, \varphi_s\},
\]
\[
\text{Ipi}(G) = \{\phi_1 = 1_G, \phi_2, \ldots, \phi_s\}.
\]

Then:
(a) The $k \times k$ matrix $X(G) = \left( x_i(C_j) \right)$ is a diagonalizing matrix of $C_f(G)$ with respect to $Irr(G)$, and
\[
(X(G))^{-1} M(f; Irr(G)) X(G) = \text{diag}(f(C_1), f(C_2), \ldots, f(C_k))
\]
for all $f \in C_f(G)$.

(b) The $k \times k$ matrix
\[
Y(G) = \begin{pmatrix}
|C| x_j(C_j) \\
\chi_j(1)
\end{pmatrix}
\]
is a diagonalizing matrix of $Z(CG)$ with respect to $B = \{\tilde{C}_1, \tilde{C}_2, \ldots, \tilde{C}_k\}$, and
\[
(Y(G))^{-1} M(C; B) Y(G) = \text{diag} \left[ \frac{|C| x_1(C)}{\chi_1(1)}, \frac{|C| x_2(C)}{\chi_2(1)}, \ldots, \frac{|C| x_k(C)}{\chi_k(1)} \right]
\]
for all $C \in Con(G)$.

(c) The $s \times s$ matrix $Z(G) = \left( \varphi_i(K_j) \right)$ is a diagonalizing matrix of $C_{\pi p}(G)$ with respect to $I_{\pi p}(G)$, and
\[
(Z(G))^{-1} M(f; I_{\pi p}(G)) Z(G) = \text{diag}(f(K_1), f(K_2), \ldots, f(K_s))
\]
for all $f \in C_{\pi p}(G)$.

(d) The $s \times s$ matrix $W(G) = \left( \phi_i(K_j) \right)$ is a diagonalizing matrix of $C_{\pi p}(G)$ with respect to $I_{\pi p}(G)$, and
\[
(W(G))^{-1} M(f; I_{\pi p}(G)) W(G) = \text{diag}(f(K_1), f(K_2), \ldots, f(K_s))
\]
for all $f \in C_{\pi p}(G)$.

Proof. For each $i = 1, 2, \ldots, k$, define $e_i \in C_f(G)$ by $e_i(C_j) = \delta_{ij}$. Then $E = \{e_1, e_2, \ldots, e_k\}$ is a set of orthogonal idempotents of $C_f(G)$. Note that for every $f \in C_f(G)$ and $i = 1, 2, \ldots, k$ we have $f e_i = f(C_i) e_i$. So according to Proposition 2.8 we get $f(i) = f(C_i)$, where $f(i)$ is the eigenvalue of $T_f$ corresponding to the eigenvector $e_i$. Now part (a) follows from Proposition 2.8(d).

For each $i = 1, 2, \ldots, s$ define $e_i \in C_{\pi p}(G)$ by $e_i(K_j) = \delta_{ij}$. Then $E = \{e_1, e_2, \ldots, e_s\}$ is a set of orthogonal idempotents of $C_{\pi p}(G)$. As above, for every $f \in C_{\pi p}(G)$ and $i = 1, 2, \ldots, s$ we have $f e_i = f(K_i) e_i$. So again by Proposition 2.8 we get that $f(i) = f(K_i)$. Parts (c) and (d) now follow from Proposition 2.8(d).
We finally turn to the proof of part (b). For each \(i = 1, 2, \ldots, k\), define \(e_i \in \mathbb{Z}(\mathbb{C}G)\) by \(e_i = 1/|G| \sum_{g \in G} \chi_i(1) \chi_i(g^{-1}) g\). By [8, p. 191], \(E = \{e_1, e_2, \ldots, e_k\}\) is a set of orthogonal idempotents of \(\mathbb{Z}(\mathbb{C}G)\). Hence part (b) will follow from Proposition 2.8 once we show that \(\chi_i(C_j)|C_j|/\chi_i(1)\) is the eigenvalue of \(T_{C_j}\) corresponding to the eigenvector \(e_i\); i.e.,

\[
\overline{C}_j e_i = \frac{\chi_i(C_j)|C_j|}{\chi_i(1)} \cdot e_i, \quad i, j = 1, 2, \ldots, k.
\]

Clearly,

\[
e_i = \frac{\chi_i(1)}{|G|} \sum_{d=1}^{k} \frac{\chi_i(C_d)}{|C_d|} \overline{C}_d.
\]

So

\[
\overline{C}_j e_i = \frac{\chi_i(1)}{|G|} \sum_{d=1}^{k} \frac{\chi_i(C_d)}{|C_d|} \overline{C}_d \cdot \overline{C}_j = \frac{\chi_i(1)}{|G|} \sum_{d=1}^{k} \frac{\chi_i(C_d)}{|C_d|} \left( \sum_{b=1}^{k} a_{djb} \overline{C}_b \right),
\]

where (see [8, p. 45]) the \(a_{djb}\) are nonnegative integers given by

\[
a_{djb} = \frac{|C_d| |C_j|}{|G|} \sum_{t=1}^{k} \frac{\chi_t(C_d) \chi_t(C_j) \chi_t(C_b)}{\chi_t(1)}.
\]

It follows that if we write \(\overline{C}_j e_i = \sum_{b=1}^{k} A_b \overline{C}_b\) with \(A_b \in \mathbb{C}\), then the coefficients \(A_b\) satisfy

\[
A_b = \frac{\chi_i(1)}{|G|} \sum_{d=1}^{k} \frac{\chi_i(C_d)}{|C_d|} \left[ \frac{|C_d| |C_j|}{|G|} \sum_{t=1}^{k} \frac{\chi_t(C_d) \chi_t(C_j) \chi_t(C_b)}{\chi_t(1)} \right] = \frac{\chi_i(1) |C_j|}{|G|} \sum_{t=1}^{k} \left( \frac{1}{|G|} \sum_{d=1}^{k} \frac{\chi_t(C_d) \chi_t(C_d) |C_d|}{\chi_t(1)} \right) \frac{\chi_t(C_j) \chi_t(C_b)}{\chi_t(1)}
\]

Now, the first character orthogonality relation implies that

\[
A_b = \frac{\chi_i(1) |C_j|}{|G|} \sum_{t=1}^{k} \delta_{it} \frac{\chi_t(C_j) \chi_t(C_b)}{\chi_t(1)} = \frac{\chi_i(1) |C_j| \chi_i(C_j) \chi_i(C_b)}{|G| \chi_i(1)},
\]

where \(\delta_{it}\) is the Kronecker delta function.
so that

\[ A_b = \frac{|C_j|\chi_i(C_j)\overline{\chi_i(C_b)}}{|G|} \]

Therefore,

\[ \overline{C_j}e_i = \sum_{b=1}^{k} A_b\overline{C_b} = \frac{|C_j|\chi_i(C_j)}{|G|} \sum_{b=1}^{k} \overline{\chi_i(C_b)} \cdot \overline{C_b} = \frac{\chi_i(C_j)|C_j|}{\chi_i(1)} \cdot e_i, \]

as desired.

**Proof of Theorem 1.4.** Set \( \text{Irr}(G) = \{\chi_1 = 1_G, \chi_2, \ldots, \chi_k\} \) and \( \text{Con}(G) = \{C_1 = \{1\}, C_2, \ldots, C_k\} \). By Proposition 4.1 the character table matrix \( X(G) = (\chi_i(C_j)) \) is a diagonalizing matrix of the separable, semisimple, finite-dimensional, commutative \( \mathbb{Q} \)-algebra \( \mathbb{Q}(\text{Irr}(G)) \) with respect to the basis \( \text{Irr}(G) \). Further,

\[ (X(G))^{-1}M(f; \text{Irr}(G))X(G) = \text{diag}(f(C_1), f(C_2), \ldots, f(C_k)) \]

for all \( f \in \mathbb{Q}(\text{Irr}(G)) \).

Hence the type of \( f \) corresponding to \( \text{Irr}(G) \) and \( X(G) \) is the type of \( (f(C_1), f(C_2), \ldots, f(C_k)) \), which in turn coincides with \( T(f) \) whose definition precedes the statement of Theorem 1.4. Now Theorem 1.1(a) implies that there exists \( \sigma \in \mathbb{Q}(\text{Irr}(G)) \) such that \( \mathbb{Q}(\text{Irr}(G)) = \mathbb{Q}[\sigma] \) and \( \sigma(C_i) \neq \sigma(C_j) \) for \( i \neq j \). Write

\[ \sigma = \sum_{i=1}^{k} \frac{p_i}{q_i} \chi_i, \]

where the \( p_i \) and \( q_i \) are integers. Let \( q = \prod_{i=1}^{k} q_i \), and set \( \delta = q\sigma \). Then \( \delta \) is a generalized character satisfying \( \delta(C_i) \neq \delta(C_j) \) for \( i \neq j \).

Next we write \( \delta = \theta_1 - \theta_2 \), where \( \theta_1 \) and \( \theta_2 \) are characters of \( G \). Let \( m \) be a positive integer satisfying

\[ m > \left| \frac{\delta(C_i) - \delta(C_j)}{\theta_2(C_i) - \theta_2(C_j)} \right| \]

for all \( i \) and \( j \) with \( \theta_2(C_i) - \theta_2(C_j) \neq 0 \). Then the character \( \theta - \delta + m\theta_2 \) satisfies \( \theta(C_i) \neq \theta(C_j) \) for all \( i \neq j \). Part (a) of the theorem now follows from Theorem 1.1(b).
Finally, Theorem 1.2 implies that $Q[\eta] = Q(\mathcal{T}(\eta))$ for all $\eta \in Q(Irr(G))$, and that $\mathcal{T}(\psi) \supseteq \mathcal{T}(\eta)$ if and only if $Q[\psi] \subseteq Q[\eta]$. Clearly, $\psi \in Q[\eta]$ if and only if $Q[\psi] \subseteq Q[\eta]$. Note that $\psi \in Q[\eta]$ implies $Q_\psi \subseteq Q_\eta$. This proves (b) and (c).

Proof of Theorem 1.5. As in the proof of Theorem 1.4, set $Irr(G) = \{x_1 = 1_G, x_2, \ldots, x_k\}$ and $Con(G) = \{C_1 = \{1\}, C_2, \ldots, C_k\}$. By Proposition 4.1, the matrix $Y = \{\chi_j(C_1/C_i) / \chi_j(1)\}$ is a diagonalizing matrix of the separable, semisimple, finite-dimensional, commutative $Q$-algebra $Z(QG)$ with respect to the basis $B = \{\tilde{C}_1, \tilde{C}_2, \ldots, \tilde{C}_k\}$; and

$$Y^{-1}M(C; B)Y = \text{diag} \left[\frac{|C|\chi_1(C)}{\chi_1(1)}, \frac{|C|\chi_2(C)}{\chi_2(1)}, \ldots, \frac{|C|\chi_k(C)}{\chi_k(1)}\right]$$

for any $C \in Con(G)$.

It follows that the type of $\tilde{C}$ corresponding to $B$ and $Y$ is precisely $T(C)$ as defined before stating Theorem 1.5. Now parts (a) and (b) of the theorem, as well as the equivalence of (i) and (ii) in part (c), are implied by Theorems 1.1 and 1.2. Clearly $Q[D] \subseteq Q[C]$ implies $D = \sum_{i=1}^k \alpha_i \tilde{C}_i$ for some $\alpha_i \in Q$. Hence,

$$\text{diag} \left[\frac{|D|\chi_1(D)}{\chi_1(1)}, \frac{|D|\chi_2(D)}{\chi_2(1)}, \ldots, \frac{|D|\chi_k(D)}{\chi_k(1)}\right] = Y^{-1}M(D; B)Y$$

$$= \sum_{i=1}^k (\alpha_i(Y^{-1}M(C; B))Y)^i$$

$$= \sum_{i=1}^k \alpha_i \cdot \text{diag} \left[\frac{|C|\chi_1(C)}{\chi_1(1)}, \frac{|C|\chi_2(C)}{\chi_2(1)}, \ldots, \frac{|C|\chi_k(C)}{\chi_k(1)}\right]^i$$

$$= \text{diag} \left[\sum_{i=1}^k \alpha_i \cdot \left[\frac{|C|\chi_1(C)}{\chi_1(1)}\right]^i, \ldots, \sum_{i=1}^k \alpha_i \cdot \left[\frac{|C|\chi_k(C)}{\chi_k(1)}\right]^i\right],$$

and so $Q_D \subseteq Q_C$.

We conclude this section by stating without proof an analog of Theorem 1.4 for Brauer characters and for principal indecomposable characters. The proof is identical to that of Theorem 1.4, except that here we use parts (c)
and (d) of Proposition 4.1 instead of part (a) of that proposition. We need to set up analogous notation as well.

**NOTATION.** Fix a prime number \( p \), and set \( \text{Con}_p(G) = \{ K_1 = \{1\}, K_2, \ldots, K_s \} \). For every subring \( K \) of \( \mathbb{C} \), denote by \( K(\text{Ibr}(G)) \) the linear span of \( \text{Ibr}(G) \) over \( K \), and by \( K(\text{Ipi}(G)) \) the linear span of \( \text{Ipi}(G) \) over \( K \). Thus, \( \mathbb{Z}(\text{Ibr}(G)) \), is the set of all generalized Brauer characters. Clearly, if \( K \) is a subfield of \( \mathbb{C} \), then \( K(\text{Ibr}(G)) \) and \( K(\text{Ipi}(G)) \) are separable SFCAs over \( K \).

Let \( f \in \text{Con}_p(G) \). We denote by \( \mathbb{Q}_f \) the smallest subfield of \( \mathbb{C} \) containing \( \mathbb{Q} \) and the numbers \( f(K_1), f(K_2), \ldots, f(K_s) \). We say in this case that \( f \) is realized in \( \mathbb{Q}_f \). The smallest subfield of \( \mathbb{C} \) containing \( \bigcup \{ \mathbb{Q}_f \mid f \in \text{Ibr}(G) \} \) is denoted by \( \mathbb{Q}_{BG} \). Similarly, the smallest subfield of \( \mathbb{C} \) containing \( \bigcup \{ \mathbb{Q}_f \mid f \in \text{Ipi}(G) \} \) is denoted by \( \mathbb{Q}_{IG} \). Finally, the type of \( f \in \text{Con}_p(G) \), denoted by \( \tau(f) \), is defined by \( \tau(f) = \tau(f(K_1), f(K_2), \ldots, f(K_s)) \).

**Theorem 4.2.** Let \( G \) be a finite group, and let \( p \) be a fixed prime. Then:

(a) There exist a Brauer character \( \theta \) and \( \eta \in \mathbb{Z}(\text{Ipi}(G)) \) such that \( \mathbb{Q}(\text{Ibr}(G)) = \mathbb{Q}[\theta] \) and \( \mathbb{Q}(\text{Ipi}(G)) = \mathbb{Q}[\eta] \). In particular, \( \mathbb{Q}_{BG} = \mathbb{Q}_\theta \) and \( \mathbb{Q}_{IG} = \mathbb{Q}_\eta \).

(b) For every \( \tau \in \mathbb{Z}(\text{Ibr}(G)) \) or \( \tau \in \mathbb{Z}(\text{Ipi}(G)) \) we have \( \mathbb{Q}[\tau] = \mathbb{Q}(T(\tau)) \).

(c) Let \( \eta \) and \( \psi \) be in \( \mathbb{Z}(\text{Ibr}(G)) \) (respectively in \( \mathbb{Z}(\text{Ipi}(G)) \)). Then the following statements are equivalent: (i). \( T(\psi) \geq T(\eta) \); (ii). \( \mathbb{Q}[\psi] \subseteq \mathbb{Q}[\eta] \). Each of these statements implies that \( \mathbb{Q}_\psi \subseteq \mathbb{Q}_\eta \).

**V. GENERALIZED CIRCULANTS**

Let \( \mathbb{F} \) be a field, and let \( f(x) = x^n - a_{n-1}x^{n-1} - a_{n-2}x^{n-2} \ldots - a_0 \in \mathbb{F}[x] \) be a monic polynomial with no repeated roots in its splitting field over \( \mathbb{F} \). Then \( C_f \), the companion matrix of \( f(x) \), is given by

\[
C_f = \begin{bmatrix}
0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 \\
a_0 & a_1 & a_2 & a_3 & \cdots & a_{n-1}
\end{bmatrix}.
\]

Each matrix \( \mathbb{F}[C_f] \) has a unique representation as a linear combination of the form \( \sum_{i=0}^{n-1} c_i(C_f)^i \), whose first row is clearly \( (c_0, c_1, \ldots, c_{n-1}) \),
and the other rows are patterned as dictated by \( f(x) \). As stated in Section I, the elements of \( \mathbb{F}[C_f] \) are called \( f(x) \)-circulants. The \( f(x) \)-circulant \( \sum_{i=0}^{n-1} c_i (C_f)^i \) is denoted by \( f(x) \)-circ \((c_0, c_1, \ldots, c_{n-1}) \). If \( u = f(x) \)-circ \((u_0, u_1, \ldots, u_{n-1}) \), we denote by \( g_u(x) \) the polynomial \( g_u(x) = \sum_{i=0}^{n-1} u_i x^i \).

**Examples.** (a) Let \( f(x) = x^n - k \) where \( k \in \mathbb{F} \). Then

\[
C_f = \begin{bmatrix}
0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 \\
k & 0 & 0 & 0 & \cdots & 0
\end{bmatrix}
\]

As \( (C_f)^n = kI \), we see that every element of \( \mathbb{F}[C_f] \) has the form

\[
\sum_{i=0}^{n-1} a_i (C_f)^i = \begin{bmatrix}
a_0 & a_1 & a_2 & a_3 & \cdots & a_{n-1} \\
ka_{n-1} & a_0 & a_1 & a_2 & \cdots & a_{n-2} \\
ka_{n-2} & ka_{n-1} & a_0 & a_1 & \cdots & A_{n-3} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
ka_1 & ka_2 & ka_3 & ka_4 & \cdots & a_0
\end{bmatrix}
\]

It follows that \( \mathbb{F}[C_f] \) is the collection of the so-called \( \{k\} \)-circulants (see [6, pp. 83–85]). For \( k = 1 \), \( \mathbb{F}[C_f] \) is the set of all circulant matrices, and for \( k = -1 \) we get the so-called skew-circulants.

(b) Let \( f(x) = x^n - x - 1 \). It can be seen that the collection of \( f(x) \)-circulants in this case is the set of all \( n \times n \) matrices over \( \mathbb{F} \) with an arbitrary first row and the following rule for obtaining any other row from the previous one: Get the \( i+1 \)st row by adding the last element of the \( i \)th row to the first element of the \( i \)th row, and then shifting the elements of the \( i \)th row (cyclically) one position to the right. For example, if \( n = 6 \), then the \( f(x) \)-circulants are all the matrices over \( \mathbb{F} \) of the form

\[
\begin{bmatrix}
a & b & c & d & e & f \\
f & a+f & b & c & d & e \\
c & f+c & a+f & b & c & d \\
d & e+d & f+e & a+f & b & c \\
c & d+c & e+d & f+e & a+f & b \\
b & c+b & d+c & e+d & f+e & a+f
\end{bmatrix}
\]

Clearly, the choice of different polynomials yields different families of
patterned matrices. As the next proposition shows, these families share many of the properties of known families of generalized circulants.

**Proposition 5.1.** Let \( \mathbb{F} \) be a field, and let \( f(x) \in \mathbb{F}[x] \). Denote that roots of \( f(x) \) in its splitting field over \( \mathbb{F} \) by \( \alpha_1, \alpha_2, \ldots, \alpha_n \). Assume that \( \alpha_i \neq \alpha_j \) for \( i \neq j \). Let \( A = \mathbb{F}[C_f] \) be the collection of all \( f(x) \)-circulants. Then:

(a) \( A \) is a separable, semisimple, \( n \)-dimensional, commutative algebra over \( \mathbb{F} \), and the matrix

\[
Y = \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
\alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\
(\alpha_1)^2 & (\alpha_2)^2 & (\alpha_3)^2 & \cdots & (\alpha_n)^2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(\alpha_1)^{n-1} & (\alpha_2)^{n-1} & (\alpha_3)^{n-1} & \cdots & (\alpha_n)^{n-1}
\end{pmatrix}
\]

is a diagonalizing matrix for \( A \) with respect to the basis \( \{I, C_f, (C_f)^2, \ldots, (C_f)^{n-1}\} \). In fact, if \( w \) is an \( f(x) \)-circulant then

\[
Y^{-1}wY = \text{diag}(g_w(\alpha_1), g_w(\alpha_2), \ldots, g_w(\alpha_n)).
\]

(b) Suppose \( \mathbb{F} \) is infinite, and let \( w \) and \( v \) be \( f \)-circulants. Then \( w \) can be written as \( h(v) \) for some \( h(x) \in \mathbb{F}[x] \) if and only if

\[
T((g_v(\alpha_1), g_v(\alpha_2), \ldots, g_v(\alpha_n)) \leq T(g_w(\alpha_1), g_w(\alpha_2), \ldots, g_w(\alpha_n)).
\]

(c) An \( n \times n \) matrix is an \( f(x) \)-circulant if and only if it commutes with \( C_f \).

(d) Assume that \( \alpha_i \in \mathbb{F}, i = 1, 2, \ldots, n \). Then an \( n \times n \) matrix is an \( f(x) \)-circulant if and only if it is of the form \( YDY^{-1} \), where \( D \) is a diagonal matrix over \( \mathbb{F} \).

(e) If \( \mathbb{F} \) is infinite, then every subalgebra of \( A \) is of the form \( \mathbb{F}[u] \) for some \( u \in A \).

*Proof.* Let \( B \) be the algebra of all \( n \times n \) matrices over \( \mathbb{F} \). Set \( u = C_f \). Then \( u \in B \) and \( A = \mathbb{F}[u] \). Let \( B = \{1, u, u^2, \ldots, u^{n-1}\} \). Clearly, \( M(u; B) = u \); so \( M(a(u); B) = a(u) \) for all \( a(x) \in \mathbb{F}[x] \). Also, \( f(x) = p_u(x) \). Part (a) now follows from Proposition 2.9, and parts (b) and (e) are consequences of Theorem 1.2.

(c): Clearly, every \( f(x) \)-circulant commutes with \( u = C_f \). Conversely, if \( b \) is an \( n \times n \) matrix over \( \mathbb{F} \) commuting with \( C_f \), then \( b \) must be of the
form $g(u)$ for some $g(x) \in F[x]$ (see [11, p. 23]), so $b \in A$ as claimed.

(d): By assumption, $Y$ and $\text{diag}(g_w(\alpha_1), g_w(\alpha_2), \ldots, g_w(\alpha_n))$ are matrices over $F$ for all $w \in A$. Set

$$A' = \{YDY^{-1} \mid D \text{ a diagonal matrix over } F\}.$$ 

Clearly, $A'$ is a vector space of dimension $n$ over $F$. By part (a) $A \subseteq A'$, so $A$ is an $n$-dimensional subspace of $A'$. Hence $A = A'$ as required.

**REMARKS.** (a) Some of the results in [6] (e.g., Theorems 3.1.1, 3.2.1, 3.3.1, and 3.2.3; most of the claims of Theorems 3.2.4; and the properties of \{k\}-circulants on pp. 83–84) are special cases of Proposition 5.1. Furthermore, under certain restrictions on the field $F$, one can obtain additional properties of $f(x)$-circulants that generalize results in [6]. We will not do this here.

(b) Proposition 5.1(b)(c) remain valid if $C_f$ is replaced by any matrix with no repeated eigenvalues. Thus, part (b) can be considered as a generalization of Corollary 6.2.7 of [6].

We next mention two methods for constructing other types of generalized circulants. We shall not go into details, as our purpose here is not to prove properties of generalized circulants, but to see how such properties relate to regular representations of algebras. The families of generalized circulants obtained here and elsewhere are in fact realizations of the regular representations of SFCAs under various bases.

**Remark on Other Generalizations of Circulants.** The so-called retrocirculants and the so-called $g$-circulants (see [6, Chapter 5]) are examples of families of generalized circulants that are not algebras. Each of these two families can be obtained from the algebra of circulants by multiplying each circulant by a particular nonsingular square matrix (see [6, Chapter 5]). Generalizations of $f(x)$-circulants can be obtained in the same way. In [4] the matrix-regular representations of semisimple, finite-dimensional $C$-algebras with respect to a pair of bases are shown to be generalizations of retrocirculants and $g$-circulants. The method used in [4] holds for arbitrary fields and can be applied to $f(x)$-circulants. The properties of these generalization are simple consequences of properties of the underlying algebras.

**Remark on Generalized Block Circulants.** Constructions and properties of generalized circulants can be found, for example, in [3, 4, 6, 7]. One constructs a generalized block circulants out of, say, two vector spaces $V_1$ and $V_2$ of generalized circulants, as follows: The family of block \{V_1, V_2\}-circulants is the family of the matrices “patterned” as dictated by $V_1$, each
of whose entry is a matrix "patterned" as prescribed by \( V_2 \). Such spaces are shown in [3, 4] to be a matrix regular representation of the tensor-product space \( V_1 \otimes V_2 \). Although in [3, 4] we assumed \( \mathbb{F} = \mathbb{C} \), the method works for any field. As building blocks one may take any type of generalized circulants, including \( f(x) \)-circulants. One can use more than two spaces to build multiple-level generalized block circulants. Again, properties of these generalizations are easy to obtain and they imply many of the results in [6].

VI. GENERALIZED CYCLIC CODES

Our coding-theoretical notation is taken from [10]. Let \( \mathbb{F} \) be a field, and let \( f(x) \in \mathbb{F}[x] \) be a monic polynomial with no repeated roots in its splitting field over \( \mathbb{F} \). An \( f(x) \)-code is an ideal of the quotient ring \( \mathbb{A} = \mathbb{F}[x]/(f(x)) \). The degree \( n \) of \( f(x) \) is called the length of the code. Elements of an \( f(x) \)-code are called codewords.

We denote images in \( \mathbb{A} \) by bars; that is, if \( a(x) \in \mathbb{F}[x] \) then \( \bar{a(x)} = a(x) + (f(x)) \). If \( a \in \mathbb{A} \), then there exists a unique polynomial \( a(x) \in \mathbb{F}[x] \) of degree less than \( n \) such that \( a = \bar{a(x)} \). Let

\[
\mathbb{F}_{f(x)}[x] = \{ a(x) \mid a(x) \in \mathbb{F}[x], \text{ degree } a(x) < n \}.
\]

Then \( \mathbb{F}_{f(x)}[x] \) is an \( \mathbb{F} \)-algebra with respect to the usual addition and scalar multiplication, and with products taken modulo \( f(x) \). The mapping \( a(x) \rightarrow \bar{a(x)} \) is an algebra isomorphism between \( \mathbb{F}_{f(x)}[x] \) and \( \mathbb{A} \). \( \mathbb{F}_{f(x)}[x] \) can be made into an \( \mathbb{F} \)-algebra in yet another way as follows: Define addition and scalar multiplication as usual, and define a product \( * \) by

\[
\left( \sum_{i=0}^{n-1} a_i x^i \right) * \left( \sum_{i=0}^{n-1} b_i x^i \right) = \left( \sum_{i=0}^{n-1} a_i b_i x^i \right).
\]

This algebra will be denoted by \( (\mathbb{F}_{f(x)}[x], *) \).

EXAMPLES. (a) Take \( f(x) = x^n - 1 \). Then the \( f(x) \)-codes are the cyclic codes of length \( n \). Writing the elements of the cyclic codes in vector notation, we see that whenever \((c_0, c_1, \ldots, c_{n-1})\) is a codeword, then so is \((c_{n-1}, c_0, c_1, \ldots, c_{n-1})\).

(b) Take \( f(x) = x^n - x - 1 \). Writing the codewords in vector notation, we have that whenever \((c_0, c_1, \ldots, c_{n-1})\) is a codeword, then so is \((c_{n-1}, c_0 + c_{n-1}, c_1, \ldots, c_{n-1})\).
DEFINITION. Let \( \alpha_1, \alpha_2, \ldots, \alpha_n \) be a fixed ordering of the roots of \( f(x) \) in its splitting field \( K \) over \( F \). Let \( a(x) \in \mathbb{K}_f(x)[x] \cong \mathbb{K}[x]/f(x) \). The polynomial \( A(z) = \sum_{i=1}^{n} a(\alpha_i) z^{n-i} \) is called the Matteson-Solomon (MS) polynomial of \( a(x) \).

Clearly, \( A(z) \in \mathbb{K}_f(z)[z] \) see [10, p. 239].

Theorem 6.1 below follows from results in Section II. Part (b)(ii) of the theorem is in fact Theorem 22(i), (ii) in [10, pp. 240-242]. Our proof of this part avoids the computations done in [10] by realizing that the "unnatural" product \( \ast \) (defined in [10, p. 240]) is actually the product of the diagonal matrices that correspond to the elements of \( \mathbb{K}_f(x)[x] \). The isomorphism of \( \mathbb{K}_f(x)[x] \) and \( (\mathbb{K}_f(x)[x], \ast) \) [10, p. 242] is essentially the simultaneous diagonalization of the elements of \( \mathbb{K}_f(x)[x] \).

**THEOREM 6.1.** Let \( F \) be a field, let \( f(x) \in F[x] \), and let \( \alpha_1, \alpha_2, \ldots, \alpha_n \) be a fixed ordering of the roots of \( f(x) \) in its splitting field \( K \) over \( F \). Assume that \( f(x) \) is monic and that \( \alpha_i \neq \alpha_j \) for \( i \neq j \). Set \( A = \mathbb{F}_f(Z)[x] \cong \mathbb{F}[x]/(f(x)) \) and \( B = \mathbb{K}_f(x)[x] \cong \mathbb{K}[x]/(f(x)) \). Then:

(a) \( A \) and \( B \) are separable, semisimple, \( n \)-dimensional, commutative algebras over \( F \) and \( K \), respectively.

(b) If \( \mathcal{B} \) be is a basis of \( B \), then there exists a diagonalizing matrix \( X \) of \( B \) with respect to \( \mathcal{B} \) such that

\[
X^{-1} M(a(x); \mathcal{B}) X = \text{diag}(a(\alpha_1), a(\alpha_2), \ldots, a(\alpha_n)) \quad \text{for all} \quad a(x) \in B.
\]

In particular:

(i) The eigenvalues of the linear transformation \( T_{a(x)} \) are the coefficients of the MS polynomial of \( a(x) \).

(ii) The mapping \( a(x) \to A(z) \) is an algebra isomorphism from \( \mathbb{K}_f(x)[x] \) to \( (\mathbb{K}_f(z)[z], \ast) \).

**Proof.** Let \( u = x + f(x) \). Then \( A \cong \mathbb{F}[u] \) and \( B \cong \mathbb{K}[u] \). In both cases \( p_u(x) = f(x) \). Now part (a) follows from Proposition 2.9(a). The main part of (b) may be seen to follow from Proposition 2.9(b). Here, however, we give a direct proof. Fix an \( i \), and set \( v_i(x) = f(x)/(x - \alpha_i) \). Then \( v_i(x) \in B \). Clearly, \( v_i(x)(x - \alpha_i) = 0 \) [modulo \( f(x) \)], so that \( xv_i(x) = \alpha_i v_i(x) \) in \( B \). This implies that \( a(x)v_i(x) = a(\alpha_i)v_i(x) \) for all \( a(x) \in B \). Thus \( v_i(x) \) is an eigenvector of \( T_{a(x)} \) belonging to the eigenvalue \( a(\alpha_i) \) for all \( i = 1, 2, \ldots, n \) and all \( a(x) \in A \). Since \( \alpha_i \neq \alpha_j \) for \( i \neq j \), we find that \( \mathcal{B}' = \{ v_i(x) | i = 1, 2, \ldots, n \} \) is a basis of \( B \), with respect to which each \( a(x) \in B \) is represented by the matrix \( \text{diag}(a(\alpha_1), a(\alpha_2), \ldots, a(\alpha_n)) \). So
the desired matrix $X$ exists. Part (b)(i) is now obvious. To obtain (b)(ii) we recall that the mapping

$$a(x) \to M(a(x); B') = \text{diag}(a(\alpha_1), a(\alpha_2), \ldots, a(\alpha_n))$$

is an algebra isomorphism [see Lemma 2.1(b)]. Obviously, the mapping sending the diagonal matrix \(\text{diag}(a(\alpha_1), a(\alpha_2), \ldots, a(\alpha_n))\) to the MS polynomial \(A(z) = \sum_{i=1}^{n} a(\alpha_i)z^{n-i}\) is an injective, linear, multiplicative map onto \((\mathbb{K}_f[z], *)\).

**NOTATION AND FACTS.** Let $F$ be a field, and let $f(x) \in F[x]$ be a monic reducible polynomial over $F$ with no repeated roots in its splitting field over $F$. Let $C$ be an $f(x)$-code of length $n$. As is customary in coding theory, we now identify $F[x]/(f(x))$ with $F[x]_{f(x)}$, where multiplication in $F[x]_{f(x)}$ is taken modulo $f(x)$. Let $g(x)$ be the unique monic polynomial of lowest degree in $C$. It is obvious that $g(x)|f(x)$ and that $C$ is generated (as an ideal) by $g(x)$; i.e., $C = (g(x))$. The polynomials $g(x)$ and $h(x) = f(x)/g(x)$ are called the **generator polynomial** of $C$ and the **check polynomial** of $C$, respectively. As in coding theory (and with the same proof), it can be shown that $C$ has a unique idempotent generator $e(x)$ (see [10, p. 217]). Clearly $C = F[xe(x)]$.

**REMARK.** The generator and check polynomials of an $f(x)$-code give rise to analogs of the so-called **generator matrix** and **parity-check matrix** for $C$ (see [10, pp. 190–191, 194–195]). In the example displayed earlier in this section, the generating matrices of the two codes are identical, while the parity-check matrices are, of course, distinct.

**THEOREM 6.2.** Let $F$ be a field, and let $f(x) \in F[x]$ be a monic reducible polynomial over $F$ with no repeated roots in its splitting field $\mathbb{K}$ over $F$. Let $C$ be an $f(x)$-code with generator polynomial $g(x)$ and check polynomial $h(x)$. Set $n = \text{degree } f(x)$, $r = \text{degree } g(x)$, $s = \text{degree } h(x)$, and let $\beta_1, \beta_2, \ldots, \beta_s$ be the roots of $h(x)$ in $\mathbb{K}$. Then:

(a) $C$ is a separable, semisimple, $s$-dimensional, commutative algebra over $F$ (and over $\mathbb{K}$).

(b) If $B$ is a basis of $C$ over $F$, then there exists a matrix $X$ over $\mathbb{K}$ such that

$$X^{-1}M(c(x); B)X = \text{diag}(c(\beta_1), c(\beta_2), \ldots, c(\beta_s))$$

for every codeword $c(x) \in C$.

(c) Let $c(x)$ be a codeword. Then $C = F[c(x)]$ if and only if $c(\beta_i) \neq \ldots$
Proof. As $C$ is a subalgebra of $\mathbb{F}[x]_{f(x)}$, part (a) follows from Theorem 6.1 and the fact that $\{g(x), xg(x), \ldots, x^{s-1}g(x)\}$ is a basis of $C$. To show (b), consider $C = (g(x))$ as an algebra over $\mathbb{K}$. Let $\beta = \beta_i$ for some $i$, and set

$$v(x) = g(x) \frac{h(x)}{x - \beta}.$$ 

Then $v(x)$ is a nonzero element of $C$. As in the proof of Theorem 6.1, it follows that $c(x)v(x) = c(\beta)v(x)$ for all $c(x) \in C$. The rest of the proof of (b) is similar to that of Theorem 6.1. Finally, (c) is a consequence of (b) and Theorem 1.1.

REMARK. Let $C$ be an $f(x)$-code with a generator polynomial $g(x)$ and a check polynomial $h(x)$. As $f(x)$ has no repeated roots, we have $(g(x), h(x)) = 1$, so that $\mathbb{F}[x]_{f(x)} = C \oplus C'$, where $C' = (h(x))$. Now choose bases $B$ for $C$ and $B'$ for $C'$. Then $D = B \cup B'$ is a basis of $\mathbb{F}[x]_{f(x)}$. Let $a(x) \in \mathbb{F}[x]_{f(x)}$, and write $a(x) = a_1(x) + a_2(x)$, where $a_1(x) \in C$ and $a_2 \in C'$. It follows that

$$M(a(x); D) = \begin{pmatrix} M(a_1(x); B) & 0 \\ 0 & M(a_2(x); B') \end{pmatrix}.$$ 

So $a(x)$ is a codeword if and only if $M(a_2(x); B') = 0$.

ACKNOWLEDGEMENT

I would like to thank Mario Blaun for useful discussions concerning the coding-theoretical part of this article.

REFERENCES


Received 1 March 1993; final manuscript accepted 30 June 1993