AN INDEPENDENCE PROPERTY OF CENTRAL POLYNOMIALS

Chen-Lian Huang
AN INDEPENDENCE PROPERTY
OF CENTRAL POLYNOMIALS

CHEN-LIAN CHUANG

Let $\Phi_n$ be the ring of $n \times n$ matrices over a commutative field $\Phi$. Let $f_i(x_1, \ldots, x_m)$ and $g_i(y_1, \ldots, y_m)$ $(i = 1, \ldots, k)$ be polynomials with coefficients in $\Phi$ and with noncommuting indeterminates in the disjoint sets $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_m\}$. Assume that $f_i(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m)$ are $\Phi$-independent modulo the $T$-ideal of polynomial identities of $\Phi_n$. Consider the following two statements:

1. Whenever $\sum_{i=1}^{k} f_i(x_1, \ldots, x_m)g_i(y_1, \ldots, y_m)$ is central on $\Phi_n$, then so is each $g_i(y_1, \ldots, y_m)$ ($i = 1, \ldots, k$).
2. Whenever $\sum_{i=1}^{k} f_i(x_1, \ldots, x_m)g_i(y_1, \ldots, y_m)$ is a polynomial identity for $\Phi_n$, then so is each $g_i(y_1, \ldots, y_m)$ ($i = 1, \ldots, k$).

It is shown here that statement (2) is always true and that statement (1) holds but for the exceptional case: $n = 2$ and $\Phi$ is the ring of integers modulo 2.

I. Results. Throughout, $\Phi$ always denotes a (commutative) field and, for $n \geq 1$, $\Phi_n$ denotes the ring consisting of all $n \times n$ matrices over $\Phi$. Let $Z$ be an infinite set of noncommuting indeterminates and let $\Phi\{Z\}$ be the free $\Phi$-algebra generated by the set $Z$. By a polynomial, in noncommuting indeterminates in the set $Z$ and with its coefficients in the field $\Phi$, we mean an element of the free $\Phi$-algebra $\Phi\{Z\}$. A polynomial $f(z_1, \ldots, z_m) \in \Phi\{Z\}$ is said to be a polynomial identity of $\Phi_n$ if for any $a_1, \ldots, a_m \in \Phi_n$, $f(a_1, \ldots, a_m) = 0$. A polynomial $f(z_1, \ldots, z_m) \in \Phi\{Z\}$ is said to be central on $\Phi_n$, if for any $a_1, \ldots, a_m \in \Phi_n$, $f(a_1, \ldots, a_m)$ is always in the center of $\Phi_n$. We let $J_n$ denote the set of all polynomial identities of $\Phi_n$. Then $J_n$ is a $T$-ideal in $\Phi\{Z\}$.

As we will consider polynomials in indeterminates in two disjoint sets, we make this notion precise as follows: Let $X$ and $Y$ be two disjoint sets of noncommuting indeterminates. Polynomials in $\Phi\{X\}$ and polynomials in $\Phi\{Y\}$ are said to be in noncommuting indeterminates in the disjoint sets $X$ and $Y$ respectively. Set $Z = X \cup Y$. The free $\Phi$-algebras $\Phi\{X\}$ and $\Phi\{Y\}$ can be regarded as $\Phi$-subalgebras of $\Phi\{Z\}$ in a natural way. Hence the products and sums of elements in $\Phi\{X\} \cup \Phi\{Y\}$ can be taken in $\Phi\{Z\}$. 

237
Assume that $\Phi$ is an infinite field. Let $f(x_1, \ldots, x_m)$ and $g(y_1, \ldots, y_m)$ be two polynomials in noncommuting indeterminates in the two disjoint sets $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_m\}$ respectively. It is proved in [2] by Regev that, if $f(x_1, \ldots, x_m)g(y_1, \ldots, y_m)$ is central on $\Phi_n$, then both $f(x_1, \ldots, x_m)$ and $g(y_1, \ldots, y_m)$ must be also central. Our primary objective here is to prove the following natural generalization

**THEOREM.** Let $\Phi_n$ be the ring of $n \times n$ matrices over a field $\Phi$ and let $\mathcal{I}_n$ be the $T$-ideal of polynomial identities of $\Phi_n$. For $i = 1, \ldots, k$, let $f_i(x_1, \ldots, x_m)$ and $g_i(y_1, \ldots, y_m)$ be polynomials with their coefficients in $\Phi$ and in noncommuting indeterminates in the disjoint sets $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_m\}$ respectively. Assume that the polynomial $\sum_{i=1}^k f_i(x_1, \ldots, x_m)g_i(y_1, \ldots, y_m)$ is central on $\Phi_n$. Then, except only when $k \geq 2$, $n = 2$ and $\Phi$ is the Galois field with only two elements, the following hold:

1. If $f_i(x_1, \ldots, x_m)$, $i = 1, \ldots, k$, are $\Phi$-independent modulo $\mathcal{I}_n$, then all $g_i(y_1, \ldots, y_m)$, $i = 1, \ldots, k$, must be central on $\Phi_n$.
2. If $g_i(y_1, \ldots, y_m)$, $i = 1, \ldots, k$, are $\Phi$-independent modulo $\mathcal{I}_n$, then all $f_i(x_1, \ldots, x_m)$, $i = 1, \ldots, k$, must be central on $\Phi_n$.
3. If both the sets $\{f_i(x_1, \ldots, x_m): i = 1, \ldots, k\}$ and $\{g_i(y_1, \ldots, y_m): i = 1, \ldots, k\}$ are $\Phi$-independent modulo $\mathcal{I}_n$, then all $f_i(x_1, \ldots, x_m)$ and $g_i(y_1, \ldots, y_m)$, $i = 1, \ldots, k$, must be central on $\Phi_n$.

Unlike the result of [2], our field $\Phi$ need not be infinite. The only exception in our theorem is the ring of $2 \times 2$ matrices over GF(2), the integers modulo 2, and even in this exceptional ring, our theorem above still holds when $k = 1$. Thus, the special instance of our theorem above when $k = 1$ already generalizes the result of [2] by removing the assumption that $\Phi$ is infinite.

An interesting immediate consequence is the following

**COROLLARY.** Let $\Phi_n$, $\mathcal{I}_n$, $f_i(x_1, \ldots, x_m)$ and $g_i(y_1, \ldots, y_m)$, $i = 1, \ldots, k$, be as explained in the theorem above. Assume that $\sum_{i=1}^k f_i(x_1, \ldots, x_m)g_i(y_1, \ldots, y_m) \in \mathcal{I}_n$. Then, without any exception on $k$, $n$ and $\Phi$, the following hold always:

1. If $f_i(x_1, \ldots, x_m)$, $i = 1, \ldots, k$, are $\Phi$-independent modulo $\mathcal{I}_n$, then $g_i(y_1, \ldots, y_m) \in \mathcal{I}_n$ for all $i = 1, \ldots, k$.
2. If $g_i(y_1, \ldots, y_m)$, $i = 1, \ldots, k$, are $\Phi$-independent modulo $\mathcal{I}_n$, then $f_i(y_1, \ldots, y_m) \in \mathcal{I}_n$ for all $i = 1, \ldots, k$.
It is interesting to observe that, in the notation of the corollary above, if both the sets \( \{ f_i(x_1, \ldots, x_m): i = 1, \ldots, k \} \) and \( \{ g_i(y_1, \ldots, y_m): i = 1, \ldots, k \} \) are \( \Phi \)-independent modulo \( \mathcal{J}_n \), then the polynomial \( \sum_{i=1}^{k} f_i(x_1, \ldots, x_m) g_i(y_1, \ldots, y_m) \) can never be an identity of \( \Phi_n \).

Before proceeding to the proofs, let us give an example showing that the exceptional case of our theorem above really happens:

**Example.** Let \( \Phi \) the Galois field with only two elements 0 and 1. Let \( \lambda \) be a new indeterminate intended to range over \( \Phi_2 \). The possible minimum polynomials for elements in \( \Phi_2 \) are \( \lambda \), \( \lambda - 1 \), \( \lambda^2 - \lambda \), \( \lambda^2 \), \( (\lambda - 1)^2 \) and \( \lambda^2 + \lambda + 1 \). Let \( h(\lambda) = \lambda^2 (\lambda - 1)^2 \). If the minimum polynomial of \( a \in \Phi_2 \) is \( \lambda \), \( \lambda - 1 \), \( \lambda^2 - \lambda \), \( \lambda^2 \) or \( (\lambda - 1)^2 \), then \( h(a) = 0 \). If the minimum polynomial of \( a \in \Phi \) is \( \lambda^2 + \lambda + 1 \), then, since \( h(\lambda) = (\lambda^2 + \lambda + 1)^2 + 1 \), we have \( h(a) = 1 \). Hence \( h(\lambda) \) is a central polynomial of \( \Phi \), and, for \( a \in \Phi_2 \), \( h(a) = 1 \) when and only when the minimum polynomial of \( a \) is \( \lambda^2 + \lambda + 1 \). It is also easy to see that there are only two elements whose minimum polynomials are \( \lambda^2 + \lambda + 1 \), namely, \( a_1 = \left( \begin{array}{c} 1 \\ 1 \end{array} \right) \) and \( a_2 = 1 + a_1 = \left( \begin{array}{c} 1 \\ 1 \end{array} \right) \). Let \( x \), \( y \) be two distinct indeterminates. Set \( f_1(x) = x h(x) \), \( f_2(x) = (f_1(x))^2 \), \( g_1(y) = y h(y) \) and \( g_2(y) = (g_1(y))^2 \). Observe that, for \( a \in \Phi_2 \),

\[
ah(a) = \begin{cases} a, & \text{if } a = a_1 \text{ or } a = a_2, \\ 0, & \text{otherwise}. \end{cases}
\]

Thus none of \( f_1(x) \), \( f_2(x) \), \( g_1(y) \), \( g_2(y) \) can be central on \( \Phi_2 \). Also if \( a = a_1 \) or if \( a = a_2 \), then \( f_1(a) = g_1(a) = a \) and \( f_2(a) = g_2(a) = a^2 \). Since \( a \) and \( a^2 \) are \( \Phi \)-independent, both the sets \( \{ f_1(x), f_2(x) \} \) and \( \{ g_1(y), g_2(y) \} \) are \( \Phi \)-independent modulo \( \mathcal{J}_2 \). We show that the polynomial \( f_1(x) g_1(y) + f_2(x) g_2(y) \) is central. If \( a \neq a_1, a_2 \) or if \( b \neq a_1, a_2 \), then \( f_1(a) = f_2(a) = 0 \) or \( g_1(b) = g_2(b) = 0 \) respectively and hence \( f_1(a) g_1(b) + f_2(a) g_2(b) = 0 \). If \( a = b = a_1 \), then \( f_1(a) g_1(a) + f_2(a) g_2(b) = a_1^2 + a_1^4 = (a_1 + a_1^2)^2 = 1^2 = 1 \). Similarly, if \( a = b = a_2 \), then \( f_1(a) g_1(a) + f_2(b) g_2(b) = a_2^2 + a_2^4 = 1^2 = 1 \) also. If \( a = a_1 \) and \( b = a_2 \), then \( f_1(a) g_1(b) + f_2(a) g_2(b) = a_1 a_2 + a_1^2 a_2^2 = 0 \). Similarly, if \( a = a_2 \) and \( b = a_1 \), then \( f_1(a) g_1(b) + f_2(a) g_2(b) = 0 \) also. Thus we have constructed a counterexample for \( k = 2 \). For \( k > 2 \), we pick new indeterminates \( x_3, \ldots, x_k, y_3, \ldots, y_k \), so that they are distinct from each other and also distinct from \( x, y \). Set \( f_i(x_i) = h(x_i) \) and \( g_i(y_i) = h(y_i) \) for \( i = 3, \ldots, k \). Since all \( f_i(x_i) \) and \( g_i(y_i) \) \( (i = 3, \ldots, k) \) thus defined are central on \( \Phi_2 \) and since \( f_1(x) g_1(y) + f_2(x) g_2(y) \) has been already shown to be central on \( \Phi_2 \), so must be \( f_1(x) g_1(y) + f_2(x) g_2(y) + \sum_{i=3}^{k} f_i(x_i) g_i(y_i) \).
Since \( f_i(x_i) \) \((i = 3, \ldots, k)\) involve indeterminates distinct from each other and also from \( x, y, f_i(x_i) \) \((i = 3, \ldots, k)\) must be \( \Phi \)-independent from each other and also from \( f_1(x), f_2(x) \) modulo \( \mathcal{J}_2 \). So \( f_1(x), f_2(x), f_3(x_3), \ldots, f_k(x_k) \) are \( \Phi \)-independent modulo \( \mathcal{J}_2 \). Similarly, \( g_1(y), g_2(y), g_3(y_3), \ldots, g_k(y_k) \) are also \( \Phi \)-independent modulo \( \mathcal{J}_2 \). We have constructed the desired example for any \( k \geq 2 \).

II. Proofs. As our results are trivial when \( n = 1 \), we assume throughout that \( n > 1 \). We will let \( e_{ij} \in \Phi_n \) denote the \( n \times n \) matrix unit with 1 in its \((i, j)\)-entry and 0 elsewhere. Our argument is based on the following two simple facts:

**Fact 1.** Assume that \( n > 2 \) or \( \Phi \) contains more than two elements. If \( a \in \Phi_n \) is not central, then there exist finitely many invertible elements \( u_1, \ldots, u_s \) such that \( e_{12} = \sum_{i=1}^{s} u_i a u_i^{-1} \).

**Proof.** Let \( A \) be the additive subgroup generated by all conjugates of \( a \). Then the set \( A \) is obviously invariant under conjugations by invertible elements of \( \Phi_n \) and \( A \) is also noncentral since \( a \in A \) is noncentral. Since \([\Phi_n, \Phi_n]\) is the only proper (noncentral) Lie ideal of \( \Phi_n \), \( A \) must contain \([\Phi_n, \Phi_n]\) by Theorem 1 [1] and Theorem 2 [1] together. But \( e_{12} = e_{12} e_{22} - e_{22} e_{12} \in [\Phi_n, \Phi_n] \subseteq A \). So there exist finitely many invertible elements \( u_1, \ldots, u_s \in \Phi_n \) such that \( e_{12} = \sum_{i=1}^{s} u_i a u_i^{-1} \).

For \( a \in \Phi_n \), the centralizer of \( a \), denoted by \( C(a) \), is defined to be the set \( \{ x \in \Phi_n : ax = xa \} \). For simplicity of notation, we denote the center of \( \Phi_n \) by \( \Phi \).

**Fact 2.** Assume that \( n > 2 \) or \( \Phi \) contains more than two elements. If \( a \in \Phi_n \) is such that \( uau^{-1} - a \in \Phi \) for all invertible elements \( u \in C(e_{12}) \), then \( a = \alpha + \beta e_{12} \) for some \( \alpha, \beta \in \Phi \).

**Proof.** Let \( a = \sum_{s,t=1}^{n} \alpha_{st} e_{st} \in \Phi_n \) be such that, for all invertible elements \( u \in C(e_{12}) \), \( uau^{-1} - a \in \Phi \), that is, \( ua - au = \gamma u \) for some \( \gamma \in \Phi \). First, consider the case \( n \geq 3 \). For \( j \geq 2 \), since \( e_{1j} \in C(e_{12}) \) and \( (e_{1j})^2 = 0 \), \( 1 + e_{1j} \) is an invertible element in \( C(e_{12}) \). So \( e_{1j} a - ae_{1j} = (1 + e_{1j}) a - a(1 + e_{1j}) = \gamma (1 + e_{1j}) \) for some \( \gamma \in \Phi \). Since both \( e_{1j} a \) and \( ae_{1j} \) are of rank at most one, \( e_{1j} a - ae_{1j} \) is of rank at most two and hence cannot be invertible in \( \Phi_n \) \((n \geq 3)\).
So \( e_{ij}a - ae_{1j} = 0 \). By direct computation,

\[
e_{ij}a - ae_{1j} = \sum_{t=1}^{n} \alpha_{jt}e_{1t} - \sum_{s=1}^{n} \alpha_{s1}e_{sj} = 0.
\]

By comparing the coefficients of both sides, we have \( \alpha_{jj} = \alpha_{11} \) and \( \alpha_{jt} = 0 \) for all \( t \neq j \). Now, consider \( e_{i2} \), where \( i \neq 2 \). As before, we have \( 0 = e_{i2}a - ae_{i2} = \sum_{t=1}^{n} \alpha_{it}e_{it} - \sum_{s=1}^{n} \alpha_{si}e_{s2} \) and hence, by comparing the coefficients, \( \alpha_{si} = 0 \) for all \( s \neq i \). In particular, \( \alpha_{1i} = 0 \) for all \( i \geq 3 \). Combining all these together, we have \( a = \alpha + \beta e_{12} \), where \( \alpha = \alpha_{11} = \alpha_{22} = \cdots = \alpha_{nn} \) and \( \beta = \alpha_{12} \).

Now consider the case \( n = 2 \). By our assumption, \( \Phi \) contains an element, say \( \delta \), other than 0 and 1. Since both \( 1 + e_{12} \) and \( \delta + e_{12} \) are invertible elements in \( C(e_{12}) \), we have \( e_{12}a - ae_{12} = (1 + e_{12})a - a(1 + e_{12}) = \gamma(1 + e_{12}) \) for some \( \gamma \in \Phi \), and similarly, \( e_{12}a - ae_{12} = (\delta + e_{12})a - a(\delta + e_{12}) = \gamma'(\delta + e_{12}) \) for some \( \gamma' \in \Phi \). Hence \( \gamma(1 + e_{12}) = e_{12}a - ae_{12} = \gamma'(\delta + e_{12}) \). This can happen only when \( \gamma = \gamma' = 0 \), since \( 1 + e_{12} \) and \( \delta + e_{12} \) are obviously \( \Phi \)-independent. Now, as before, let

\[
a = \sum_{s,t=1}^{2} \alpha_{st}e_{st} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}.
\]

Then

\[
e_{12}a - ae_{12} = \begin{pmatrix} \alpha_{21} & \alpha_{22} - \alpha_{11} \\ 0 & -\alpha_{21} \end{pmatrix} = 0.
\]

So \( \alpha_{21} = 0 \) and \( \alpha_{11} = \alpha_{22} \). That is, \( a = \alpha + \beta e_{12} \), where \( \alpha = \alpha_{11} = \alpha_{22} \) and \( \beta = \alpha_{12} \).

For brevity, we introduce the following definition:

**Definition.** For \( a_1, \ldots, a_k, b_1, \ldots, b_k \in \Phi_n \), we write

\[
\langle a_1, \ldots, a_k \rangle \ast \langle b_1, \ldots, b_k \rangle \in \Phi
\]

if the following condition \( (*) \) is satisfied:

\[
(*) \quad \sum_{i=1}^{k} (u_{ai}u^{-1})(v_{bi}v^{-1}) \in \Phi
\]

for any invertible elements \( u, v \in \Phi_n \).

By conjugation \( (*) \) by \( u^{-1} \), we have \( \sum_{i=1}^{k} a_i(u^{-1}v)b_i(u^{-1}v)^{-1} \in \Phi \). Since \( u^{-1}v \) also ranges over all invertible elements of \( \Phi_n \), \( (*) \) is
equivalent to:

\[
(*)' \quad \sum_{i=1}^{k} a_i(vb_i v^{-1}) \in \Phi \quad \text{for all invertible elements } v \in \Phi_n.
\]

Symmetrically, \((*)\) is also equivalent to

\[
(*)'' \quad \sum_{i=1}^{k} (ua_i u^{-1})b_i \in \Phi \quad \text{for all invertible elements } u \in \Phi_n.
\]

In the following fact, we collect some simple properties about the condition \((*)\), which will be needed in the sequel:

\textbf{Fact 3.} Assume that \(a_1, \ldots, a_k, b_1, \ldots, b_k, b'_1, \ldots, b'_k \in \Phi_n\).

1. If both \(\langle a_1, \ldots, a_k \rangle \ast \langle b_1, \ldots, b_k \rangle \in \Phi \) and \(\langle a_1, \ldots, a_k \rangle \ast \langle b'_1, \ldots, b'_k \rangle \in \Phi \), then \(\langle a_1, \ldots, a_k \rangle \ast \langle b_1 + b'_1, \ldots, b_k + b'_k \rangle \in \Phi \).

2. If \(\langle a_1, \ldots, a_k \rangle \ast \langle b_1, \ldots, b_k \rangle \in \Phi \), then \(\langle a_1, \ldots, a_k \rangle \ast \langle vb_1 v^{-1}, \ldots, vb_k v^{-1} \rangle \in \Phi \) for any invertible element \(v \in \Phi_n\).

3. If \(\langle a_1, \ldots, a_k \rangle \ast \langle b_1, \ldots, b_k \rangle \in \Phi \) and \(b_k = \sum_{i=1}^{k-1} \beta_i b_i\), where \(\beta_i \in \Phi\) \((i = 1, \ldots, k-1)\), then \(\langle a_1 + \beta_1 a_k, a_2 + \beta_2 a_k, \ldots, a_{k-1} + \beta_{k-1} a_k \rangle \ast \langle b_1, b_2, \ldots, b_{k-1} \rangle \in \Phi\).

Proof. Immediate.

Our Fact 3 above is concerned about variations of \(\langle b_1, \ldots, b_k \rangle\) in the condition \((*)\). The corresponding properties concerning about variations of \(\langle a_1, \ldots, a_k \rangle\) in the condition \((*)\) can be formulated and proved similarly.

We start the proof of our main theorem with the following:

\textbf{Lemma 1.} Assume that \(n \neq 2\) or the field \(\Phi\) contains more than two elements. Let \(b_1, \ldots, b_k \in \Phi_n\) be \(\Phi\)-independent. For \(a_1, \ldots, a_k \in \Phi_n\), if \(\langle a_1, \ldots, a_k \rangle \ast \langle b_1, \ldots, b_k \rangle \in \Phi\), then \(a_1, \ldots, a_k \in \Phi\).

Proof. If \(n = 1\), then all elements of \(\Phi_n\) are central and Lemma 1 holds trivially. So let \(n \geq 2\). Assume on the contrary that Lemma 1 is false. Let \(k\) be the minimal integer such that the assertion of Lemma 1 fails. First, assume that \(k = 1\). Write \(a = a_1\) and \(b = b_1\) for brevity. By our assumption, \(a\) is not central and, since \(ab \in \Phi\), \(b\) cannot be central either. By Fact 1, there exist invertible elements \(u_1, \ldots, u_s, v_1, \ldots, v_t \in \Phi_n\) such that \(e_{12} = \sum_{i=1}^{s} u_i a_i a_i^{-1} = \sum_{j=1}^{t} v_j b_1 v_j^{-1}\). By Fact 3, \(\langle \sum_{i=1}^{s} u_i a_i a_i^{-1} \rangle \ast \langle \sum_{j=1}^{t} v_j b_1 v_j^{-1} \rangle \in \Phi\). So we
have \( \langle e_{12} \rangle \ast \langle e_{12} \rangle \in \Phi \). Let

\[
v = e_{12} + e_{21} + \sum_{j \geq 2} e_{jj} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.
\]

Then \( v \) is an invertible element of \( \Phi_n \) and \( ve_{12}v^{-1} = e_{21} \). Since \( \langle e_{12} \rangle \ast \langle e_{12} \rangle \in \Phi \), we have \( e_{11} = e_{12}e_{21} = e_{12}(ve_{12}v^{-1}) \in \Phi \), a contradiction.

Now, assume \( k \geq 2 \). By reindexing \( a_i, b_i \) \( (i = 1, \ldots, k) \) if necessary, we may assume that \( a_k \) is not central. By Fact 1, there exist invertible elements \( v_1, \ldots, v_s \in \Phi_n \) such that \( e_{12} = \sum_{j=1}^s v_j a_k v_j^{-1} \).

By Fact 3, \( \langle \sum_{j=1}^s v_j a_k v_j^{-1} \rangle, \ldots, \langle \sum_{j=1}^s v_j a_k v_j^{-1} \rangle \rangle \in \Phi \). Replacing each \( a_1, \ldots, a_k \) by \( \sum_{j=1}^s v_j a_k v_j^{-1} \) respectively, we may assume that \( a_k = e_{12} \) to start with. Let \( u \) be an invertible element of \( C(e_{12}) \). By Fact 3, \( \langle ua_1 u^{-1}, \ldots, ua_k u^{-1} \rangle \ast \langle b_1, \ldots, b_k \rangle \in \Phi \). Since \( ua_k u^{-1} - a_k = 0 \), we have \( \langle ua_1 u^{-1} - a_1, \ldots, ua_k u^{-1} - a_k \rangle \ast \langle b_1, \ldots, b_k \rangle \in \Phi \). By the minimality of \( k \), \( ua_1 u^{-1} - a_1, \ldots, ua_k u^{-1} - a_k \) are all central. Since this holds for any invertible elements \( u \in C(e_{12}) \), and since \( n > 2 \) or \( |\Phi| > 2 \), by Fact 2, \( a_1 = \alpha_1 + \beta_1e_{12}, \ldots, a_{k-1} = \alpha_{k-1} + \beta_{k-1}e_{12} \) for some \( \alpha_1, \ldots, \alpha_{k-1}, \beta_1, \ldots, \beta_{k-1} \in \Phi \). By (3) of Fact 3, \( \langle 1, e_{12} \rangle \ast \langle \alpha_1 b_1 + \cdots + \alpha_{k-1} b_{k-1}, \beta_1 b_1 + \cdots + \beta_{k-1} b_{k-1} + b_k \rangle \in \Phi \). Set \( b'_1 = \alpha_1 b_1 + \cdots + \alpha_{k-1} b_{k-1} \) and \( b'_2 = \beta_1 b_1 + \cdots + \beta_{k-1} b_{k-1} + b_k \). Then \( \langle 1, e_{12} \rangle \ast \langle b'_1, b'_2 \rangle \in \Phi \). Since \( b_1, \ldots, b_k \) are assumed to be \( \Phi \)-independent, \( b'_2 \) is \( \Phi \)-independent of \( b'_1 \) and, in particular, must be nonzero. Let \( v \) be an arbitrary invertible element of \( \Phi_n \). By Fact 3 again, \( \langle v(1)v^{-1} - 1, ve_{12}v^{-1} - e_{12} \rangle \ast \langle b'_1, b'_2 \rangle \in \Phi \), that is, \( \langle ve_{12}v^{-1} - e_{12} \rangle \ast \langle b'_2 \rangle \in \Phi \). By our result for the case \( k = 1 \) in the previous paragraph, \( ve_{12}v^{-1} - e_{12} \in \Phi \). Now let \( v = 1 + e_{21} \). Then \( v^{-1} = 1 - e_{12} \). We compute \( ve_{12}v^{-1} - e_{12} = (1 + e_{21})e_{12}(1 - e_{21}) - e_{12} = -e_{11} - e_{21} + e_{22} \). But, obviously, \( -e_{11} - e_{21} + e_{22} \) cannot be central, a contradiction. This completes our proof of Lemma 1.

**Lemma 2.** Assume that \( n \neq 2 \) or \( \Phi \) contains more than two elements. Let \( f_1(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m) \in \Phi \{x_1, \ldots, x_m\} \) be \( \Phi \)-independent modulo \( \mathcal{I}_n \). For any \( b_1, \ldots, b_k \in \Phi_n \), if
Proof. For any invertible element \( u \in \Phi_n \) and for any assignment of values in \( \Phi_n \) to \( x_1, \ldots, x_m \), we have, by our assumption, that

\[
\sum_{i=1}^{k} (u f_i(x_1, \ldots, x_m) u^{-1}) b_i = \sum_{i=1}^{k} f_i(u x_1 u^{-1}, \ldots, u x_m u^{-1}) b_i \in \Phi.
\]

Hence, for any assignment of values in \( \Phi_n \) to \( x_1, \ldots, x_m \), we have \( \langle f_1(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m) \rangle \ast \langle b_1, \ldots, b_k \rangle \in \Phi \).

First assume that \( b_1, \ldots, b_k \) are \( \Phi \)-independent modulo \( \Phi \), in the sense that for any \( \beta_1, \ldots, \beta_k \in \Phi \), \( \beta_1 b_1 + \cdots + \beta_k b_k \in \Phi \) implies \( \beta_1 = \cdots = \beta_k = 0 \), i.e., \( \{1, b_1, \ldots, b_k\} \) are linearly independent. Then, by Lemma 1, for any assignment of values in \( \Phi_n \) to \( x_1, \ldots, x_m \), \( f_i(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m) \in \Phi \) and, by our assumption on the \( \Phi \)-independence of \( b_1, \ldots, b_k \) modulo \( \Phi \), \( f_1(x_1, \ldots, x_m) = \cdots = f_k(x_1, \ldots, x_m) = 0 \). This is a contradiction to the \( \Phi \)-independence of \( f_i(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m) \) modulo \( \mathcal{S}_n \). Thus \( \{1, b_1, \ldots, b_k\} \) are linearly dependent. By reindexing \( b_1, \ldots, b_k \) if necessary, we may assume that \( \{1, b_1, \ldots, b_s\} \), where \( 0 \leq s < k \), forms a \( \Phi \)-basis of the \( \Phi \)-subspace spanned by \( \{1, b_1, \ldots, b_k\} \). For \( j = s+1, \ldots, k \), write \( b_j = \sum_{i=1}^{s} \beta_i^{(j)} b_i + \gamma^{(j)} \), where, for \( i = 1, \ldots, s \), \( \beta_i^{(j)}, \gamma^{(j)} \in \Phi \). Hence

\[
f_1(x_1, \ldots, x_m) b_1 + \cdots + f_k(x_1, \ldots, x_m) b_k
\]

\[
= \left( f_1(x_1, \ldots, x_m) + \sum_{j=s+1}^{k} f_j(x_1, \ldots, x_m) \beta_1^{(j)} \right) b_1 + \cdots
\]

\[
+ \left( f_s(x_1, \ldots, x_m) + \sum_{j=s+1}^{k} f_j(x_1, \ldots, x_m) \beta_s^{(j)} \right) b_s
\]

\[
+ \left( \sum_{j=s+1}^{k} f_j(x_1, \ldots, x_m) \gamma^{(j)} \right) 1.
\]

By Lemma 1 again, for any assignment of values in \( \Phi_n \) to \( x_1, \ldots, x_m \), the matrices \( f_i(x_1, \ldots, x_m) + \sum_{j=s+1}^{k} f_j(x_1, \ldots, x_m) \beta_i^{(j)} \),
(i = 1, ..., s), as well as the matrix \( \sum_{j=s+1}^{k} f_j(x_1, \ldots, x_m) \gamma^{(j)} \), are all central in \( \Phi_n \) and, since \( 1, b_1, \ldots, b_s \) are assumed to be \( \Phi \)-independent modulo \( \Phi \), we have

\[
\begin{align*}
  f_1(x_1, \ldots, x_m) + \sum_{j=s+1}^{k} f_j(x_1, \ldots, x_m) \beta_1^{(j)} &= 0, \\
  \vdots \\
  f_s(x_1, \ldots, x_m) + \sum_{j=s+1}^{k} f_j(x_1, \ldots, x_m) \beta_s^{(j)} &= 0.
\end{align*}
\]

But this contradicts with the \( \Phi \)-independence of \( f_1(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m) \) modulo \( \mathcal{S}_n \). Hence \( s \) must be 0 and the unit 1 spans the \( \Phi \)-subspace spanned by \( \{1, b_1, \ldots, b_k\} \). This is equivalent to the fact that \( b_1, \ldots, b_k \in \Phi \), as desired.

As with Lemma 1, there is also a symmetrical version of Lemma 2, which can be formulated and proved analogously.

Our last lemma treats the special case when \( n = 2 \) and \( \Phi \) contains only two elements.

**Lemma 3.** Let \( \Phi = \{0, 1\} \) be the ring of integers modulo 2.

1. For \( a, b \in \Phi_2 \setminus \{0\} \), if \( \langle a \rangle * \langle b \rangle \in \Phi \), then \( a, b \in \Phi \).

2. Let \( f_1(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m) \in \Phi\{x_1, \ldots, x_m\} \) be \( \Phi \)-independent modulo \( \mathcal{S}_2 \). For \( b_1, \ldots, b_k \in \Phi_2 \), if

\[
\sum_{i=1}^{k} f_i(x_1, \ldots, x_m) b_i = 0
\]

for all \( x_1, \ldots, x_m \in \Phi_2 \), then \( b_1 = \cdots = b_k = 0 \).

**Proof.** (1) Let us determine the conjugacy classes of \( \Phi_2 \). Two elements in \( \Phi_2 \) are similar if and only if they have the same minimum polynomials. The possible minimum polynomials in \( \Phi_2 \) are \( \lambda, \lambda + 1, \lambda^2, \lambda^2 + 1, \lambda^2 + \lambda, \lambda^2 + \lambda + 1 \). For a polynomial \( \phi(\lambda) \), in the indeterminate \( \lambda \) and with coefficients in \( \Phi \), let \( B(\phi(\lambda)) \) denote the set consisting of all elements in \( \Phi_2 \) whose minimum polynomials are \( \phi(\lambda) \) and also let \( A(\phi(\lambda)) \) denote the additive subgroup generated by
B(φ(λ)) . By direct computation, we have the following list of all possible B(φ(λ)) and A(φ(λ)):

\[
\begin{align*}
B(\lambda) &= \{0\}, \\
B(\lambda + 1) &= \{1\}, \\
B(\lambda^2) &= \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}, \\
B(\lambda^2 + 1) &= \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \\
B(\lambda^2 + \lambda) &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}, \\
B(\lambda^2 + \lambda + 1) &= \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}, \\
A(\lambda) &= \{0\}, \\
A(\lambda + 1) &= \{0, 1\}, \\
A(\lambda^2) &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}, \\
A(\lambda^2 + 1) &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \\
A(\lambda^2 + \lambda) &= \Phi_2, \\
A(\lambda^2 + \lambda + 1) &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.
\end{align*}
\]

For x, y ∈ Φ₂, if \langle x \rangle \ast \langle y \rangle ∈ Φ₂ and if one of x, y is central, then the other must also be central. So let us assume, towards a contradiction, that neither of a and b is central. Since \langle a \rangle \ast \langle b \rangle ∈ Φ, \langle a' \rangle \ast \langle b' \rangle ∈ Φ for any a' in the additive subgroup generated by the conjugates of a and for any b' in the additive subgroup generated by the conjugates of b. Observe that in the above list of A(φ(λ)), all but A(λ) and A(λ² + 1) contain the identity 1. If the minimum polynomial of b is not λ² + 1, then \langle a \rangle \ast \langle 1 \rangle ∈ Φ and hence a must be central, a contradiction. So the minimum polynomial of b is λ² + 1. Similarly, the minimum polynomial of a is also λ² + 1. But then \langle a'' \rangle \ast \langle b'' \rangle ∈ Φ
for any $a', b' \in A(\lambda^2 + 1)$. This is absurd: For instance,

$$
\begin{pmatrix}
1 & 0 \\
1 & 1
\end{pmatrix} ,
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix} \in A(\lambda^2 + 1) \quad \text{but}
$$

$$
\begin{pmatrix}
1 & 0 \\
1 & 1
\end{pmatrix} \begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix} = \begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix} \notin \Phi.
$$

This contradiction completes our proof of (1).

(2) Suppose not. Let $k \geq 1$ be the minimal integer such that the assertion of (2) of this lemma fails. By (1) of this lemma, $k \geq 2$. We divide the argument, into three cases.

Case 1. For some $i = 1, \ldots, k$, $b_i = 1$: By reindexing if necessary, we may assume $b_1 = 1$. For any invertible element $u \in \Phi_2$, we have

$$
\sum_{i=2}^{k} f_i(x_1, \ldots, x_m)(ub_iu^{-1} - b_i)
$$

$$
= u \left( \sum_{i=1}^{k} f_i(u^{-1}x_1u, \ldots, u^{-1}x_mu)b_i \right) u^{-1}
$$

$$
- \sum_{i=1}^{k} f_i(x_1, \ldots, x_m)b_i
$$

$$
= 0.
$$

By the minimality of $k$, $ub_iu^{-1} = b_i$ ($i = 2, \ldots, k$). Hence, for any invertible element $u \in \Phi_2$, $ub_i = b_iu$ ($i = 2, \ldots, k$). By a direct computation, $b_2, \ldots, b_k$ must be all central. This contradicts with the $\Phi$-independence of $f_1(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m)$ modulo $\mathcal{I}_2$.

Case 2. The minimum polynomial of some $b_i$ ($i = 1, \ldots, k$) is not $\lambda^2 + 1$: By reindexing if necessary, we may assume that the minimum polynomial $\phi(\lambda)$ of $b_1$ is not $\lambda^2 + 1$. By the list of all possible $A(\phi(\lambda))$ in the proof of (1), $1 \in A(\phi(\lambda))$. So there exist invertible elements $u_1, \ldots, u_s \in \Phi_2$ such that $\sum_{j=1}^{s} u_jb_1u_j^{-1} = 1$. Set $b'_i = \sum_{j=1}^{s} u_jb_iu_j^{-1}$ for $i = 1, \ldots, k$. Then we have $\sum_{i=1}^{k} f_i(x_1, \ldots, x_m)b'_i = 0$ for any assignment of values in $\Phi_2$ to $x_1, \ldots, x_m$. But $b'_i = 1$ and, by Case 1, this is impossible.
Case 3. The minimum polynomial of each $b_i$ ($i = 1, \ldots, k$) is $\lambda^2 + 1$: Without loss of generality, we may assume $b_1 = \left( \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right)$. Since $b_1$ is invertible, we have

$$
\sum_{i=2}^{k} f_i(x_1, \ldots, x_m)(b_1 b_i b_1^{-1} - b_i)
$$

\[= b_1 \left( \sum_{i=1}^{k} f_i(b_1^{-1} x_1 b_1, \ldots, b_1^{-1} x_m b_1) b_i \right) b_1^{-1}
\]

\[= \sum_{i=1}^{k} f_i(x_1, \ldots, x_m) b_i
\]

\[= 0.
\]

By the minimality of $k$, $b_1 b_i b_1^{-1} = b_i$, that is, $b_1 b_i = b_i b$. Since $b_i \in B(\lambda^2 + 1)$ and the only element in $B(\lambda^2 + 1)$ which commutes with $b_1 = \left( \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right)$ is $b_1$ itself, we have $b_1 = b_2 = \cdots = b_k$. Hence $(\sum_{i=1}^{k} f_i(x_1, \ldots, x_m)) b_1 = 0$ for any $x_1, \ldots, x_m \in \Phi$. By (1) of this lemma, $\sum_{i=1}^{k} f_i(x_1, \ldots, x_m) = 0$ for any $x_1, \ldots, x_m \in \Phi_2$. This contradicts with the $\Phi$-independence of $f_1(x_1, \ldots, x_m), \ldots, f_k(x_1, \ldots, x_m)$ modulo $\mathcal{J}_2$ and completes our proof.

Proof of Theorem. Observe that (3) follows from (1) and (2). As (1) and (2) can be proved analogously, we give here only the proof of (1): If $n \neq 2$ or the field $\Phi$ contains more than two elements, then our theorem follows immediately from Lemma 2. If $n = 2$ and $\Phi$ contains only two elements 0 and 1, then, according to the hypothesis of our theorem, $k$ must be one and the assertion of our theorem follows immediately from (1) of Lemma 3.

Proof of Corollary. If $n \neq 2$ or $\Phi$ contains more than two elements, then our corollary follows immediately from our theorem. If $n = 2$ and $\Phi$ contains only two elements 0 and 1, then our corollary follows immediately from (2) of Lemma 3.

Acknowledgment. The author wishes to thank the referee for correcting several errors of this paper and also for his valuable suggestions which clarify some arguments of this paper.
REFERENCES


Received August 15, 1989 and in revised form March 1, 1990.

NATIONAL TAIWAN UNIVERSITY
TAIPEI, TAIWAN 10764
REPUBLIC OF CHINA
PACIFIC JOURNAL OF MATHEMATICS
EDITORS
V. S. VARADARAJAN
(Managing Editor)
University of California
Los Angeles, CA 90024-1555-05
HERBERT CLEMENS
University of Utah
Salt Lake City, UT 84112
THOMAS ENRIGHT
University of California, San Diego
La Jolla, CA 92093
R. FINN
Stanford University
Stanford, CA 94305
HERMANN FLASCHKA
University of Arizona
Tucson, AZ 85721
VAUGHAN F. R. JONES
University of California
Berkeley, CA 94720
STEVEN KERCKHOFF
Stanford University
Stanford, CA 94305
C. C. MOORE
University of California
Berkeley, CA 94720
R. ARENS
(1906-1982)
E. F. BECKENBACH
(1904-1989)
B. H. NEUMANN
F. WOLF
K. YOSHIDA
ASSOCIATE EDITORS
SUPPORTING INSTITUTIONS
UNIVERSITY OF ARIZONA
UNIVERSITY OF OREGON
UNIVERSITY OF BRITISH COLUMBIA
UNIVERSITY OF SOUTHERN CALIFORNIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
STANFORD UNIVERSITY
UNIVERSITY OF CALIFORNIA
UNIVERSITY OF HAWAI'I
MONTANA STATE UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF NEVADA, RENO
UNIVERSITY OF UTAH
NEW MEXICO STATE UNIVERSITY
WASHINGTON STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the Pacific Journal of Mathematics should be in typed form or offset-reproduced (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph must be capable of being used separately as a synopsis of the entire paper. In particular it should contain no bibliographic references. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the 1991 Mathematics Subject Classification scheme which can be found in the December index volumes of Mathematical Reviews. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California 90024-1555-05.

There are page-charges associated with articles appearing in the Pacific Journal of Mathematics. These charges are expected to be paid by the author's University, Government Agency or Company. If the author or authors do not have access to such institutional support these charges are waived. Single authors will receive 50 free reprints; joint authors will receive a total of 100 free reprints. Additional copies may be obtained at cost in multiples of 50.

The Pacific Journal of Mathematics (ISSN 0030-8730) is published monthly except for July and August. Regular subscription rate: $190.00 a year (10 issues). Special rate: $95.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address should be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

The Pacific Journal of Mathematics at P.O. Box 969, Carmel Valley, CA 93924 (ISSN 0030-8730) is published monthly except for July and August. Second-class postage paid at Carmel Valley, California 93924, and additional mailing offices. Postmaster: send address changes to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION
Copyright © 1991 by Pacific Journal of Mathematics
Yuri A. Abramovich, Operators preserving disjointness on rearrangement invariant spaces .......................................................... 201
Andrew French Acker and Kirk Lancaster, Existence and geometry of a free boundary problem for the heat equation ................................................. 207
So-Chin Chen, Real analytic regularity of the Szegő projection on circular domains .......................................................... 225
Chen-Lian Chuang, An independence property of central polynomials ...... 237
Peter Larkin Duren and M. Schiffer, Robin functions and energy functionals of multiply connected domains .................................................. 251
Johan Henricus Bernardus Kemperman, Sets of uniqueness and systems of inequalities having a unique solution ........................................ 275
Ka-Lam Kueh, Fourier coefficients of nonholomorphic modular forms and sums of Kloosterman sums .......................................................... 303
Gerard J. Murphy, Ordered groups and crossed products of $C^*$-algebras ... 319
You-Qiang Wang, The $p$-parts of Brauer character degrees in $p$-solvable groups .......................................................... 351
Hidenobu Yoshida, Harmonic majorization of a subharmonic function on a cone or on a cylinder .......................................................... 369