PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 110, Number 2, October 1990

ON RANGES OF POLYNOMIALS IN FINITE MATRIX RINGS

CHEN-LIAN CHUANG

(Communicated by Maurice Auslander)

ABSTRACT. Let C be a finite field and let C_m denote the ring consisting of all $m \times m$ matrices over C. By a polynomial, we mean a polynomial in noncommuting indeterminates with coefficients in C. It is shown here that a subset A of C_m is the range of a polynomial without constant term if and only if $0 \in A$ and $uAu^{-1} \subseteq A$ for all invertible elements $u \in C_m$.

Let C be a field and let $X = \{x_0, x_1, x_2, \dots\}$ be an infinite set of *noncommuting* indeterminates. By a *polynomial* in noncommuting indeterminates in X, we mean an element of $C\{X\}$, the free noncommutative C-algebra (with the identity) generated by X. Elements of $C\{X\}$ with the constant term 0 are specially called polynomials *without* the constant term. For $m \geq 1$, let C_m denote the ring consisting of all $m \times m$ matrices over C. We recall two definitions: A polynomial is said to be a *polynomial identity* of C_m if all of its evaluations on C_m assume the value 0. A polynomial is said to be *central* on C_m if (1) all of its evaluations on C_m are in the center of C_m; (2) some of its evaluations on C_m are nonzero; and (3) its constant term is zero. Thus, polynomial identities and central polynomials of C_m are, by their definitions, *without* constant terms. Also, a central polynomial of C_m, by its definition, must *not* be an identity of C_m.

Our main aim here is to prove the following:

Theorem. *Assume that C is a finite field. A subset A of C_m $(m \geq 1)$ is the range of a polynomial without constant term in $C\{x\}$ if and only if $0 \in A$ and $uAu^{-1} \subseteq A$ for any invertible element $u \in C_m$.*

Our theorem can immediately be generalized to polynomials with arbitrary constant terms:

Corollary. *Assume that C is a finite field and A is a subset of C_m $(m \geq 1)$.* (1) *The set A is the range of a polynomial in $C\{X\}$ with the constant term $\alpha \in C$ if and only if $\alpha \in A$ and $uAu^{-1} \subseteq A$ for any invertible element $u \in C_m$.* (2) *The set A is the range of a polynomial in $C\{X\}$ (with or without a constant*

Received by the editors May 9, 1989 and, in revised form, November 30, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 16A38, 16A44.
Key words and phrases. Polynomial, central polynomial, finite field.

term) if and only if $A \cap C$ *is nonempty and* $uAu^{-1} \subseteq A$ *for any invertible element* $u \in C_m$.

In the literature known to the author, there are two special instances of our main theorem, both of which appear as an attempt to solve the problem of the existence of central polynomials for full matrix rings over arbitrary fields: In [5], Latyšev and Šmel′kin prove the existence of central polynomials for the matrix rings over finite fields. In [4], Kaplansky announces that, for matrix rings over finite fields, a central polynomial in only *one* variable was known to Herstein. (But, as said in [4], Herstein credits the observation to John Thompson.) Now, the existence of central polynomials for full matrix rings over arbitrary fields has been solved independently by Formanek and by Razmyslov. It might be interesting to observe that our proof of the main theorem depends heavily on their solutions.

The corresponding problem for the ranges of generalized polynomials has been solved in [1]: Assume that C is a finite field. As is shown in [1], any function (in one variable) from C_m $(m \geq 1)$ into C_m can be represented as a generalized polynomial (in one indeterminate). In particular, *any* subset of C_m is the range of a generalized polynomial in one indeterminate.

Before proceeding to the proof, we remark that our main theorem is *false*, in general, if the field C is *infinite*:

Example. The set A consisting of all square zero elements of C_m is obviously invariant under any automorphism of C_m and also contains the zero element 0. Suppose that A is the range of a polynomial, say, $f(x_1, \ldots, x_n)$. Then for any given $r_1, \ldots, r_n \in C_m$, $f(r_1, \ldots, r_m) \in A$ and hence $f(r_1, \ldots, r_n)^2 = 0$. Thus, the polynomial $f(x_1, \ldots, x_n)^2$ must be an identity of C_m. Let θ_m denote the set of all identities of C_m. If the field C is infinite, then, by a famous result of Amitsur [7, Theorem 3.26, p. 176], $C\{X\}/\theta_m$ is a domain and hence $f(x_1, \ldots, x_n)^2 \in \theta_m$ would imply $f(x_1, \ldots, x_n) \in \theta_m$. But the range of $f(x_1, \ldots, x_n)$ is assumed to be the set A and, if $m > 1$, the set A must contain nonzero elements. This is a contradiction.

The following simple proposition is true for *arbitrary* fields, *not* necessarily finite, and might be interesting in itself.

Proposition. *Let* C *be an arbitrary field, finite or infinite. For each* $k \in \{1, \ldots, m\}$, *there exists a central polynomial* $f_k(x, x_1, \ldots, x_s)$ *of* C_m *such that, for any given* $a \in C_m$, *the range of* $f_k(a, x_1, \ldots, x_s)$ *is* C *or* $\{0\}$ *according to* $\operatorname{rank}(a) \geq k$ *or* $\operatorname{rank}(a) < k$ *respectively.*

Proof. Observe that, for $a \in C_m$, $\operatorname{rank}(a) \geq k$ if and only if $\dim_C(aC_m) \geq km$. Let $C_{2km-1}(y_1, \ldots, y_{2km-1})$ be the Capelli polynomial of degree $2km-1$ as defined on [7, p. 12]. Let

$$g_k(x, x_1, \ldots, x_{2km-1}) = C_{2km-1}(xx_1, \ldots, xx_{km}, x_{km+1}, \ldots, x_{2km-1}).$$

By [7, Theorem 1.4.34, p. 31], for given $a \in C_m$, $g_k(a, x_1, \ldots, x_{2km-1})$ vanishes for all $x_1, \ldots, x_{2km-1}$ if and only if $ax_1, \ldots, ax_{km}$ are C-dependent for any $x_1, \ldots, x_{km} \in C_m$, and hence, if and only if $\operatorname{rank}(a) < k$. Next, observe that, if $b \neq 0$, then any $r \in C_m$ can be written in the form $r = \sum_{i=1}^{m} r_i b r_i'$, where $r_i, r_i' \in C_m$. Define

$$h_k(x, x_1, \ldots, x_{2(k+1)m-1}) = \sum_{i=0}^{m-1} x_{2km+2i} g_k(x, x_1, \ldots, x_{2km-1}) x_{2km+2i+1}.$$

Then, for $a \in C_m$, the range of $h_k(a, x_1, \ldots, x_{2(k+1)m-1})$ is C_m or $\{0\}$ if $\operatorname{rank}(a) \geq k$ or $\operatorname{rank}(a) < k$, respectively. Finally, let $c(y, y_1, \ldots, y_t)$ be any central polynomial of C_m with range C and $c(0, y_1, \ldots, y_t) = 0$. (Such central polynomials exist either by Formanek's construction [7, Theorem A.9, p. 317] or by Razmyslov's construction [7, Theorem 1.4.14, p. 26]. Let $s = 2(k+1)m + t - 1$. Now we define our desired

$$f_k(x, x_1, \ldots, x_s) = c(h_k(x, x_1, \ldots, x_{2(k+1)m-1}), x_{2(k+1)m}, \ldots, x_{2(k+1)m+t-1}).$$

The central polynomials $f_k(x, x_1, \ldots, x_s)$ obviously have the desired property.

We need the following simple

Fact 1. For any finite (multiplicative) semigroup G, there exists an integer $n > 0$ such that, for any $a \in G$, a^n is an idempotent.

Proof. Assume that G is a finite (multiplicative) semigroup. Given $a \in G$, the set $\{a, a^2, a^3, \ldots\}$ is finite. So $a^{m+n} = a^m$ for some integers $m, n > 0$. Then

$$a^{mn+n} = a^{m(n-1)+m+n} = a^{m(n-1)} a^{m+n} = a^{m(n-1)} a^m = a^{mn}.$$

So

$$\begin{aligned}(a^{mn})^2 &= a^{mn+mn} = a^{mn+n} a^{(m-1)n} \\ &= a^{mn} a^{(m-1)n} = a^{mn+n} a^{(m-2)n} \\ &= a^{mn} a^{(m-2)n} = a^{mn} a^{(m-3)n} = \cdots = a^{mn}.\end{aligned}$$

Thus a^{mn} is an idempotent. We have thus shown that, for any $a \in G$, there exists an integer $n(a) > 0$ such that $a^{n(a)}$ is an idempotent. If we set our desired n to be the product of all $n(a)$ $(a \in G)$, then for any $a \in G$, $a^n = a^{n(a)}$ is an idempotent.

If the field C is finite, then, by using the fact above, our proposition can be strengthened to the following:

Lemma 1. *Assume that C is a finite field. Then for each $k \in \{0, 1, \ldots, m\}$, there exists a central polynomial $\rho_k(x, y_1, \ldots, y_t)$ of C_m such that, for any $a \in C_m$, the range of $\rho_k(a, y_1, \ldots, y_t)$ is $\{0, 1\}$ or $\{0\}$ if $\operatorname{rank}(a) = k$ or $\operatorname{rank}(a) \neq k$, respectively.*

For simplicity of notation, we use vector notation to abbreviate sequences of indeterminates in X: For example, $\vec{x} = (x_1, \ldots, x_s)$, $g(\vec{x}) = g(x_1, \ldots, x_s)$, $f(x, \vec{x}) = f(x, x_1, \ldots, x_s)$, etc.

Proof of Lemma 1. Assume that C is a finite field. Let n be the positive integer asserted in Fact 1 above such that, for any $a \in C_m$, a^n is an idempotent. Let $f_k(x, \vec{x})$ $(k = 1, \ldots, m)$ be the central polynomials of C_m as described in our proposition above. The $(f_k(x, \vec{x}))^n$ assumes only central idempotents as its values. Note that the only central idempotents of C_m are 0 and 1. Therefore, by replacing $f_k(x, \vec{x})$ by $(f_k(x, \vec{x}))^n$, we may assume from the start that $f_k(x, \vec{x})$ assumes only the values 0, 1 and, for any $a \in C_m$, the range of $f_k(a, \vec{x})$ is $\{0, 1\}$ or $\{0\}$ if $\operatorname{rank}(a) \geq k$ or $\operatorname{rank}(a) < k$, respectively. In the particular case of $k = 1$, for any $a \in C_m$, the range of $f_1(a, \vec{x})$ is $\{0\}$ or $\{0, 1\}$ if $a = 0$ or $a \neq 0$, respectively. Assume that the ring C_m has exactly M distinct elements. (Hence m is equal to the (m^2)th power of the cardinality of the field C.) For each pair (i, j) such that $1 \leq i < j \leq M$, we introduce a sequence of new distinct indeterminates $\vec{w}(i, j) = (w_1^{(i,j)}, \ldots, w_s^{(i,j)})$, each of the same length s as $\vec{x}$ in $f_1(x, \vec{x})$. Let $\vec{w}$ be the sequence obtained by arranging all $w_k^{(i,j)}$ $(k = 1, \ldots, s)$ in some arbitrary but fixed order. Define

$$\eta(z_1, \ldots, z_M, \vec{w}) = \prod_{1 \leq i < j \leq M} f_1(x_i - x_j, \vec{w}^{(i,j)}).$$

The central polynomial $\eta(z_1, \ldots, z_M, \vec{w})$ also assumes only the values 0 and 1. Also, for $a_1, \ldots, a_M \in C_m$,

the range of $\eta(a_1, \ldots, a_M, \vec{w})$ is $\{0, 1\}$
$\Leftrightarrow$ $a_1, \ldots, a_M$ are distinct,
$\Leftrightarrow$ $C_m = \{a_1, \ldots, a_M\}$.

The last equivalence above holds since C_m has exactly M distinct elements. For each $i = 1, \ldots, M$, we introduce a sequence of new indeterminates $\vec{y}^{(i)} = (y_1^{(i)}, \ldots, y_s^{(i)})$, each of the same length s as $\vec{x}$ in $f_k(x, \vec{x})$. Let $\vec{y}$ be the sequence of indeterminates $y_j^{(i)}$ $(i = 1, \ldots, M,\ j = 1, \ldots, s)$ arranged in some arbitrary but fixed order. For each $k \in \{0, 1, \ldots, m-1\}$, define

$$g_k(x, z_1, \ldots, z_M, \vec{y}, \vec{w}) = \eta(z_1, \ldots, z_M, \vec{w}) \cdot \prod_{i=1}^{M} f_{m-k}(1 - (xz_i)^n, \vec{y}^{(i)}).$$

The central polynomial $g_k(x, z_1, \ldots, z_M, \vec{y}, \vec{w})$ assumes only the values 0 and 1, since so do the polynomials η and f_{m-k}. Also, for $a, a_1, \ldots, a_M \in C_m$,

the range of $g_k(a, a_1, \ldots, a_M, \vec{y}, \vec{w})$ is $\{0, 1\}$
$\Leftrightarrow$ $C_m = \{a_1, \ldots, a_M\}$ and, for $i = 1, \ldots, M$, $\operatorname{rank}(1-(aa_i)^n) \geq m-k$,
$\Leftrightarrow$ for all $r \in C_m$, $\operatorname{rank}(1 - (ar)^n) \geq m - k$,

$\Leftrightarrow$ for all $r \in C_m$, $\operatorname{rank}((ar)^n) \leq k$,
$\Leftrightarrow$ $\operatorname{rank}(a) \leq k$.

The third equivalence above holds because $(ar)^n$ is an idempotent and, since for any idempotent e of C_m, $\operatorname{rank}(e) + \operatorname{rank}(1-e) = m$. The reason why the last equivalence above holds is as follows: If $\operatorname{rank}(a) \leq k$, then, for any $r \in C_m$, $\operatorname{rank}((ar)^n) \leq \operatorname{rank}(a) \leq k$. Conversely, for any $a \in C_m$, there exists $r_0 \in C_m$ such that ar_0 is an idempotent of the same rank as a. So, if $\operatorname{rank}((ar)^n) \leq k$ for all $r \in C_m$, then, in particular, $k \geq \operatorname{rank}((ar_0)^n) = \operatorname{rank}(ar_0) = \operatorname{rank}(a)$. By renaming and reindexing indeterminates, we write $g_k(x, z_1, \ldots, z_M, \vec{y}, \vec{w})$ as $g_k(x, \vec{v})$ for short. For $k \in \{1, \ldots, m-1\}$, define

$$\rho_k(x, \vec{x}, \vec{v}) = f_k(x, \vec{x}) g_k(x, \vec{v}).$$

The central polynomial $\rho_k(x, \vec{x}, \vec{v})$ assumes only the values 0 and 1 since so do $f_k(x, \vec{x})$ and $g_k(x, \vec{v})$. Also, it is obvious from the corresponding properties for $f_k(x, \vec{x})$ and $g_k(x, \vec{v})$ that, for $a \in C_m$,

the range of $\rho_k(a, \vec{x}, \vec{v})$ is $\{0, 1\}$
$\Leftrightarrow$ the ranges of $f_k(a, \vec{x})$ and of $g_k(a, \vec{v})$ are both $\{0, 1\}$,
$\Leftrightarrow$ $\operatorname{rank}(a) \geq k$ and $\operatorname{rank}(a) \leq k$,
$\Leftrightarrow$ $\operatorname{rank}(a) = k$.

By renaming the indeterminates, we write $\rho_k(x, \vec{x}, \vec{v})$ as $\rho_k(x, \vec{y})$. So, $\rho_k(x, \vec{y})$ $(k = 1, \ldots, m-1)$ thus defined have the desired property. Now, we define $\rho_0(x, \vec{y})$ to be $g_0(x, \vec{y})$. Then, for $a \in C_m$, we have:

the range of $\rho_0(x, \vec{y})$ is $\{0, 1\}$
$\Leftrightarrow$ the range of $g_0(x, \vec{y})$ is $\{0, 1\}$,
$\Leftrightarrow$ $\operatorname{rank}(a) \leq 0$,
$\Leftrightarrow$ $\operatorname{rank}(a) = 0$.

Similarly, we define $\rho_m(x, \vec{y})$ to be $f_m(x, \vec{y})$. Then, for $a \in C_m$, we have:

the range of $\rho_m(a, \vec{y})$ is $\{0, 1\}$
$\Leftrightarrow$ the range of $f_m(a, \vec{y})$ is $\{0, 1\}$,
$\Leftrightarrow$ $\operatorname{rank}(a) \geq m$,
$\Leftrightarrow$ $\operatorname{rank}(a) = m$.

The proof of Lemma 1 is thus finished.

Let $C[\lambda]$ denote the commutative ring of all polynomials in the single indeterminate λ and with their coefficients in the field C. For $a \in C_m$ and for a polynomial $\phi(\lambda) = \alpha_0 + \alpha_1\lambda + \cdots + \alpha_s\lambda^s \in C[\lambda]$, we define, as usual, $\phi(a) = \alpha_0 + \alpha_1 a + \cdots + \alpha_s a^s$. We need the following simple lemma from linear algebra.

Lemma 2. *Let C be a finite field. Then, for each $m \geq 1$, there exists a finite set of polynomials $\phi_1(\lambda), \ldots, \phi_q(\lambda) \in C[\lambda]$ such that, for any $a, b \in C_m$, $a = ubu^{-1}$ for some invertible element $u \in C_m$ if and only if* $\operatorname{rank}(\phi_i(a)) = \operatorname{rank}(\phi_i(b))$ *for* $i = 1, \ldots, q$.

The proof of Lemma 2 seems irrelevant to our main theorem here and will be given at the end of this paper.

We remark that some of the polynomials $\phi_1(\lambda), \ldots, \phi_q(\lambda)$, described in Lemma 2, must involve *nonvanishing* constant terms.

Now we are ready to give

Proof of theorem. The necessity ($\Rightarrow$) is easy: Suppose that A is the range of a polynomial $f(x_1, \ldots, x_t)$ without constant term. For any invertible element $u \in C_m$, $uf(a_1, \ldots, a_t)u^{-1} = f(uau^{-1}, \ldots, ua_tu^{-1})$ holds for any $a_1, \ldots, a_t \in C_m$ and hence $uAu^{-1} \subseteq A$. Also since the polynomial $f(x_1, \ldots, x_t)$ does not have constant term, we have $0 = f(0, \ldots, 0) \in A$, as desired.

Now, we show the sufficiency ($\Leftarrow$): Let $\rho_k(x, \vec{y})$ $(k = 0, 1, \ldots, m)$ be the central polynomials described in Lemma 1 and let $\phi_i(\lambda)$ $(i = 1, \ldots, q)$ be the polynomials (in only one indeterminate λ) described in Lemma 2. For $a \in C_m$, we define

$$\Phi_a(\lambda, \vec{y}) = \prod_{i=1}^{q} \rho_{\operatorname{rank}(\phi_i(a))}(\phi_i(\lambda), \vec{y}).$$

Then $\Phi_a(\lambda, \vec{y})$ assumes only the values 0 and 1 since each $\rho_{\operatorname{rank}(\phi_i(a))}(x, \vec{y})$ does. Also, for $b \in C_m$,

the range of $\Phi_a(b, \vec{y})$ is $\{0, 1\}$

$\Leftrightarrow$ all the ranges of $\rho_{\operatorname{rank}(\phi_i(a))}(\phi_i(b), \vec{y})$ $(i = 1, \ldots, q)$ are $\{0, 1\}$,

$\Leftrightarrow$ $\operatorname{rank}(\phi_i(b)) = \operatorname{rank}(\phi_i(a))$ for $i = 1, \ldots, q$,

$\Leftrightarrow$ $a = ubu^{-1}$ for some invertible element $u \in C_m$.

(The last equivalences follow from Lemmas 2 and 1 respectively.) For $a \in C_m$, we define $[a] = \{b \in C_m : b = uau^{-1}$ for some invertible element $u \in C_m\}$. Then, for $b \in C_m$, $b \in [a]$ if and only if the range of $\Phi_a(b, \vec{y})$ is $\{0, 1\}$.

Suppose that A is a given subset of C_m such that $0 \in A$ and such that $uAu^{-1} \subseteq A$ for all invertible elements $u \in C_m$. Then the set A can be written in the form

$$A = \bigcup_{i=1}^{t} [a_i]$$

such that the sets $[a_i]$ $(i = 1, \ldots, t)$ are pairwise disjoint. Define

$$\chi_A(x, \vec{y}) = \sum_{i=1}^{t} \Phi_{a_i}(x, \vec{y}).$$

We claim that $\chi_A(x, \vec{y})$ assumes only the values 0, 1 and, for $a \in C_m$, the range of $\chi_A(a, \vec{y})$ is $\{0, 1\}$ or $\{0\}$ if $a \in A$ or $a \notin A$, respectively. Since $[a_1], \ldots, [a_t]$ are pairwise disjoint, an element $a \in C_m$ can belong to *at most one* of $[a_1], \ldots, [a_t]$. Also, unless a belongs to $[a_i]$, for $i = 1, \ldots, t$, $\Phi_{a_i}(a, \vec{y})$ will vanish identically. So we have

$$\chi_A(a, \vec{y}) = \begin{cases} \Phi_{a_i}(a, \vec{y}) & \text{if } a \text{ belongs to } [a_i] \ (i = 1, \ldots, t), \\ 0 & \text{if } a \text{ does not belong to any one of } [a_1], \ldots, [a_t]. \end{cases}$$

Our claim now follows. Now, define our desired polynomial $f(x, \vec{y})$ by

$$f(x, \vec{y}) = \chi_A(x, \vec{y})x.$$

The polynomial $f(x, \vec{y})$ thus defined has zero constant term. It is obvious from the claimed property of $\chi_A(x, \vec{y})$ that the range of $f(x, \vec{y})$ is precisely the set A.

Our theorem is sometimes useful in constructing counterexamples. Let us give the following two applications in this respect.

Application 1. A polynomial $f(x_1, \ldots, x_s)$, with coefficients in the field C, is said to be *nil* or *periodic* in a C-algebra R, if for all $a_1, \ldots, a_s \in R$, $f(a_1, \ldots, a_s)$ is nilpotent or periodic, respectively. (Recall that an element $a \in R$ is said to be nilpotent or periodic if, for some integer $n(a) > 1$, $a^{n(a)} = 0$, or $a^{n(a)} = a$ respectively.) We cite the following results from the literature:

(1) [6, Theorem 4] If every multilinear nil polynomial in a unital C-algebra R vanishes identically, then the same holds for the $n \times n$ matrix ring R_n over R.

(2) [3, Theorem 3] If a C-algebra R has *no* nonzero nil one-sided ideals, then any *multilinear* nil polynomial in R must vanish identically on R.

(3) [3, Theorem 2] If a C-algebra R has *no* nonzero nil two-sided ideals, then any *multilinear* periodic polynomial in R must also be central in R.

(4) [6, Theorem 10] Let n be a positive integer such that the field C contains *no* nth root of unity other than 1. Suppose that $m \geq 3$. If f is a *multilinear* polynomial such that f^n is central in C_m, then f itself is central in C_m.

Our theorem says that the *multilinearity* assumption in the above results *can not* be removed in general, at least in the case of the matrix rings over finite fields: Assume that C is finite. Let A_1, A_2, and A_3 respectively be the set of all nilpotent elements in C_m, the set of all periodic elements in C_m and the set of all $a \in C_m$ such that a^n is central, where n is a fixed integer given in (4) cited above. Apparently, the subsets A_1, A_2, and A_3 are invariant under conjugations by invertible elements of C_m and hence, by our theorem, are ranges of polynomials, say, f_1, f_2, f_3, respectively. Then f_1 is nil in C_m, f_2 is periodic in C_m, and f_3^n is central. But f_1 does not vanish identically on C_m and neither f_2 nor f_3 is central.

Application 2. Let $f(x_1, \ldots, x_s)$ be a polynomial with coefficients in the extended centroid C of a prime ring R and let I be a nonzero two-sided ideal of R. Assume that $f(x_1, \ldots, x_s)$ is *not* central valued on R. It is proved in [2] that the additive subgroup generated by $\{f(a_1, \ldots, a_s): a_1, \ldots, a_s \in I\}$ must contain a noncentral Lie ideal of R except in the only case where R is the ring of all 2×2 matrices over the field with only two elements. No counterexample was given in [2] to show that the assertion does fail in the exceptional case excluded. Here we provide one: Let $C = \{0, 1\}$, the Galois field with only two elements. Let A be the additive subgroup generated by those $a \in C_2$ with minimum polynomials $\lambda^2+\lambda+1 = 0$. The set A consists of only four elements 0, $\left(\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0 & 1\\ 1 & 1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ and does not contain any noncentral Lie ideal of C_2. Since A is obviously invariant under conjugations by invertible elements of C_2, by our theorem, A is the range of a polynomial, say $f(x_1, \ldots, x_s)$. This f provides the desired counterexample.

Before concluding this paper, let us prove Lemma 2. Two elements $a, b \in C_m$ are said to be *similar* if and only if $a = ubu^{-1}$ for some invertible element $u \in C_m$. We need the following simple fact from linear algebra, which is also true for arbitrary fields.

Fact 2. Assume that C is an arbitrary field, finite or infinite. Let a be an $m \times m$ matrix in C_m with the minimum polynomial $\phi(\lambda)$. Write $\phi(\lambda) = \pi_1(\lambda)^{k_1} \cdots \pi_s(\lambda)^{k_s}$, where $\pi_i(\lambda) \in C[\lambda]$ $(i = 1, \ldots, s)$ are distinct prime factors of $\phi(\lambda)$. Then an $m \times m$ matrix b in C_m is similar to a if and only if $\operatorname{rank}(\pi_i(b)^k) = \operatorname{rank}(\pi_i(a)^k)$ for $i = 1, \ldots, s$ and $1 \leq k \leq k_i + 1$.

Proof of Lemma 2. Since C is assumed to be finite, there are only finitely many irreducible polynomials in $C[\lambda]$ of degrees $\leq m$, say $\pi_1(\lambda), \ldots, \pi_t(\lambda)$. Let $\phi_1(\lambda), \ldots, \phi_q(\lambda)$ enumerate all $(\pi_i(\lambda))^j$ $(i = 1, \ldots, t,\ j = 1, \ldots, m+1)$ in some arbitrary but fixed way. By Fact 2 above, $\phi_1(\lambda), \ldots, \phi_q(\lambda)$ obviously enjoy the desired property asserted in Lemma 2.

As there is no ready reference of Fact 2 known to the author, its proof, elementary but somewhat lengthy, is also included here for the sake of completeness.

Proof of Fact 2. Fix an m-dimensional vector space V over C and interpret elements of C_m as linear transformations on V. With respect to an arbitrarily given $b \in C_m$, we make V a $C[\lambda]$-module by defining the action of a polynomial $\phi(\lambda) \in C[\lambda]$ on any vector $v \in V$ as $v\phi(\lambda) = v\phi(b)$. Express V as a direct sum of cyclic $C[\lambda]$-modules of prime power orders. (Such an expression is not unique in general but we just fix an arbitrary one.) For any irreducible polynomial $\pi(\lambda) \in C[\lambda]$ and for an integer $k \geq 1$, let $\nu(b, \pi^k)$ denote the number of cyclic direct $C[\lambda]$-summands with order $\pi(\lambda)^k$. (All but finitely many $\nu(b, \pi^k)$ are zero since the space V is finite dimensional.) The elementary divisors of b are defined to be those $\pi(\lambda)^k$ listed with *multiplicity*

$\nu(b, \pi^k)$. (That is, if $\nu(b, \pi^k) > 0$, then $\pi(\lambda)^k$ is listed $\nu(b, \pi^k)$ times as elementary divisors of b. But if $\nu(b, \pi^k) = 0$, then $\pi(\lambda)^k$ is simply *not* listed as an elementary divisor of b.) Thus the numbers $\nu(b, \pi^k)$ are uniquely determined by b, independent of the expression of V as a direct sum of cyclic $C[\lambda]$-modules of prime power orders. Conversely, the numbers $\nu(b, \pi^k)$ also determine b uniquely up to similarity.

We claim that, for $k \geq 1$,

$$(*) \qquad \operatorname{rank}(\pi(b)^{k-1}) - \operatorname{rank}(\pi(b)^k) = \operatorname{degree}(\pi) \cdot \sum_{j \geq k} \nu(b, \pi^j).$$

If we can prove that the equality $(*)$ holds on each $C[\lambda]$-summand of V, then the equality $(*)$ also holds on the whole V merely by adding up the equality $(*)$ on each summand. Replacing V by a cyclic direct $C[\lambda]$-summand of prime power order, we may assume from the start that V is a cyclic $C[\lambda]$-module of order $\mu(\lambda)^n$, where $n \geq 1$ and $\mu(\lambda) \in C[\lambda]$ is irreducible. First, suppose that $\pi(\lambda) \neq \mu(\lambda)$. Then there exist $\phi(\lambda)$, $\psi(\lambda) \in C[\lambda]$ such that $\pi(\lambda)^k \phi(\lambda) + \mu(\lambda)^n \psi(\lambda) = 1$ and hence $\pi(b)^k$ is invertible with inverse $\phi(b)$. So $\operatorname{rank}(\pi(b)^{k-1}) = \operatorname{rank}(\pi(b)^k) = \dim V = m$ and $\operatorname{rank}(\pi(b)^{k-1}) - \operatorname{rank}(\pi(b)^k) = 0$. But $\nu(\pi, j) = 0$ for all $j \geq 0$. So the identity $(*)$ holds in this case as desired. Now, suppose that $\pi(\lambda) = \mu(\lambda)$. If $k > n$, then $\pi(b)^{k-1} = \pi(b)^k = 0$. Since $\nu(\pi, j) = 0$ for $j \geq k > n$, the claim holds again. So assume that $k \leq n$. Let v be a generator of the cyclic $C[\lambda]$-module V. Then $v\pi(b)^k$ is a generator of $V\pi(b)^k$. Hence $V\pi(b)^k$ is also cyclic and has the order $\pi(\lambda)^{n-k}$. Similarly $V\pi(b)^{k-1}$ is a cyclic module of order $\pi(\lambda)^{n-k+1}$. Note that a cyclic $C[\lambda]$-module of order $\phi(\lambda)$ must be of the dimension $\operatorname{degree}(\phi)$, for if u is a generator, then $u, u\lambda, \ldots, u\lambda^{(\operatorname{degree}(\phi)-1)}$ form a basis. Hence $\operatorname{rank}(\pi(b)^k) = (n-k)\operatorname{degree}(\pi)$ and $\operatorname{rank}(\pi(b)^{k-1}) = (n-k+1)\operatorname{degree}(\pi)$. So $\operatorname{rank}(\pi(b)^{k-1}) - \operatorname{rank}(\pi(b)^k) = \operatorname{degree}(\pi)$. But $\nu(b, \pi^n) = 1$ and $\nu(b, \pi^j) = 0$ for $j \neq n$. Since we assume that $k \leq n$, $\sum_{j \geq k} \nu(b, \pi^j) = \nu(b, \pi^n) = 1$. The identity $(*)$ holds again. So the claim is proved.

Subtracting the identity $(*)$ for $k+1$ from the identity $(*)$ for k, we have, for $k \geq 1$,

$$(**) \quad \operatorname{degree}(\pi) \cdot \nu(b, \pi^k) = \operatorname{rank}(\pi(b)^{k-1}) - 2\operatorname{rank}(\pi(b)^k) + \operatorname{rank}(\pi(b)^{k+1}).$$

Now, let $a, b, \phi(\lambda) = \pi_1(\lambda)^{k_1} \cdots \pi_s(\lambda)^{k_s}$ be as stated in Fact 2. If a and b are similar, then certainly $\operatorname{rank}(\pi(a)^k) = \operatorname{rank}(\pi(b)^k)$ for any $k \geq 0$ and any $\pi(\lambda) \in C[\lambda]$. Conversely, assume that $\operatorname{rank}(\pi_i(a)^k) = \operatorname{rank}(\pi_i(b)^k)$ for $i = 1, \ldots, s$ and $1 \leq k \leq k_i + 1$. Then from $(**)$, we have $\nu(a, \pi_i^k) = \nu(b, \pi_i^k)$ for $i = 1, \ldots, s$ and $k = 1, \ldots, k_i$. Let D be the set consisting of all $\pi_i(\lambda)^k$ $(i = 1, \ldots, s, \ k = 1, \ldots, k_i)$. Since $\phi(\lambda)$ is assumed to be the minimum polynomial of a, we have $\nu(a, \pi^k) = 0$ for prime powers $\pi(\lambda)^k \notin D$. As in the previous paragraph, $\operatorname{degree}(\pi^k) \cdot \nu(a, \pi^k)$ is the total dimension of all cyclic

direct $C[\lambda]$-summands of order $\pi(\lambda)^k$. Hence $\sum_{\pi^k \in D} \text{degree}(\pi^k) \cdot \nu(a, \pi^k) = m$. Since $\nu(a, \pi^k) = \nu(b, \pi^k)$ for $\pi^k \in D$ as we have shown, we also have $\sum_{\pi^k \in D} \text{degree}(\pi^k) \cdot \nu(b, \pi^k) = m$. But this implies, in turn, that $\nu(b, \pi^k) = 0$ for prime powers $\pi(\lambda)^k \notin D$. So we have thus shown $\nu(a, \pi^k) = \nu(b, \pi^k)$ for any prime power $\pi(\lambda)^k$, and a and b are similar as desired.

ACKNOWLEDGMENT

The author would like to thank the referee for suggesting the presentation of the proof of the main theorem in this paper, which does improve the clarity of the whole argument.

REFERENCES

1. J. V. Brawley and L. Carlitz, *A characterization of the $n \times n$ matrices over a finite field*, Amer. Math. Monthly **80** (1973), 670–672.
2. C.-L. Chuang, *The additive subgroup generated by a polynomial*, Israel J. Math. **59** (1987), 98–106.
3. B. Felzenszwalb and A. Giambruno, *Periodic and nil polynomials in rings*, Canad. Math. Bull. **23** (1980), 473–476.
4. I. Kaplansky, *"Problems in the theory of rings" revisited*, Amer. Math. Monthly **77** (1970), 445–454.
5. V. N. Latyšev and A. L. Šmel′kin, *A certain problem of Kaplansky*, Algebra i Logika **8** (1969), 447–448; English transl., Algebra and Logic **8** (1969), 257.
6. U. Leron, *Nil and power central polynomials in rings*, Trans. Amer. Math. Soc. **202** (1975), 97–103.
7. L. H. Rowen, *Polynomial identities in ring theory*, Academic Press, New York, 1980.

DEPARTMENT OF MATHEMATICS, NATIONAL TAIWAN UNIVERSITY, TAIPEI, TAIWAN 10764, REPUBLIC OF CHINA