MINIMAL IDENTITIES FOR ALGEBRAS

A. S. AMITSUR AND J. LEVITZKI

1. **Introduction.** Let F be the underlying field of an algebra A and $x_1, x_2, \cdots, x_m$ a set of indeterminates. Consider a polynomial $f(x_1, \cdots, x_m)$ over F, that is, an element of the free algebra $F(x_1, \cdots, x_m)$ generated by the indeterminates x_i over the field F. If this polynomial is not identically zero and if the equation

$$f(x_1, \cdots, x_m) = 0 \tag{1}$$

is satisfied by all elements of A, then we say (see [1][1]) that the polynomial identity (1) holds in A. Such identities are satisfied, for example, by each algebra of finite dimensionality.[2] An identity of minimal degree will be called a *minimal identity*, and the corresponding polynomial a minimal polynomial.[3] In a previous communication (see [4]) it has been shown by one of the present authors that the degree of the minimal identities for the total matric-algebra A_n of all n by n matrices is at least $2n$. In the present note we show (§2) that *this degree is exactly* $2n$, and that we may choose as a polynomial identity one having the form

$$S(x_1, \cdots, x_{2n}) = \sum_{(i)} \pm x_{i_1} x_{i_2} \cdots x_{i_{2n}} \tag{2}$$

where the sum on the right ranges over all permutations of $2n$ letters and the sign is positive for even permutations and negative for odd permutations. We shall use for (2) occasionally also the shorter notation $S_{2n}(x)$. Polynomials of type (2) were previously studied in the same context by I. Kaplansky [2] and F. W. Levi [3], and we adopt for these polynomials and the corresponding identities the terms *standard polynomials*, respectively *standard identities*, suggested by Kaplansky.

In §3 we deal with the problem of determining all minimal polynomials of A_n. It turns out that all minimal polynomials are homogeneous and linear in each of the indeterminates. Moreover, if $x_1, x_2, \cdots, x_k$ is a given set of indeterminates, then minimal polynomials depending on the x's only may be constructed if and only if

Received by the editors May 8, 1949.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

[2] For further details compare [1] and [4].

[3] Minimal polynomials in the ordinary sense will not be referred to in this paper, so that no confusion will arise.

$k \geqq 2n$ and the set of all minimal polynomials in the x's forms (if supplemented by zero) a module over the underlying field whose dimensionality is $C_{k,2n}$. As a basis for this module we may choose the $C_{k,2n}$ standard polynomials $S(x_{i_1}, \cdots, x_{i_{2n}})$, where $(i_1, \cdots, i_{2n})$ is an arbitrary combination of $2n$ letters out of k. For $k=2n$ we have in particular the following uniqueness theorem: The minimal polynomial depending on no more than $2n$ indeterminates is uniquely determined (up to a numerical factor) as the standard polynomial $S_{2n}(x)$. The case $n \leqq 2$, $F=$prime field of characteristic 2 requires a special treatment.

In §4 we apply our results to general algebras of finite dimensionality.

2. **The main theorem.** We begin with a few remarks concerning some simple properties of the standard polynomials which will be needed in the proof of the main theorem.

REMARK 1. Since the standard polynomial is homogeneous and linear in each of its indeterminates, we have

$$S(x_1, \cdots, x_i, \alpha u + \beta v, x_{i+2}, \cdots) = \alpha S(x_1, \cdots, x_i, u, \cdots, x_{2n}) + \beta S(x_1, \cdots, x_i, v, \cdots, x_{2n}).$$

REMARK 2. The standard polynomial vanishes if two of the indeterminates are identified.

REMARK 3. If $(i_1, \cdots, i_m)$ is any permutation of m letters, then $S(x_{i_1}, \cdots, x_{i_m}) = \pm S(x_1, \cdots, x_m)$.

REMARK 4. Denote by $(i_1, \cdots, i_m)$ any permutation of m letters, and by S' the sum of all terms in $S_m(x)$ having in common the left factor $x_{i_1}x_{i_2} \cdots x_{i_r}$ where $r<m$, then $S' = \pm x_{i_1}x_{i_2} \cdots x_{i_r} S(x_{i_{r+1}}, \cdots, x_{i_m})$.

REMARK 5. Denote by $a_1, a_2, \cdots, a_m$ a set of m matrices of order m, such that the rth row and the rth column of each of these matrices consists of zeros. Denote by a_i' the matrix derived from a_i by deleting the rth row and the rth column. If $S(a_1, \cdots, a_m)=0$, then also $S(a_1', \cdots, a_m')=0$ and conversely. This is a consequence of the fact that the correspondence $a \to a'$ determines an isomorphism between the rings generated by the a_i and the a_i' respectively.

REMARK 6. If an algebra satisfies an identity $S_m(x)=0$, then it satisfies also each identity $S_k(x)=0$ with $k>m$.

LEMMA 1. *If for an odd positive integer r we put $y=x_{i+1} \cdots x_{i+r}$ and if S' denotes the sum of all terms of $S_m(x)$ containing the common factor y, then*

$$S' = S(x_1, \cdots, x_i, y, x_{i+r+1}, \cdots, x_m). \tag{3}$$

PROOF. The right member of (3) is a sum of terms with coefficients ± 1 each being a product of $m-r+1$ factors. If p and q are any two such terms, then let π denote the permutation transforming p into q. If y is replaced by the product $x_{i+1} \cdots x_{i+r}$, then p and q become products of m factors each, and the permutation π induces a permutation π' of these m factors. Relation (3) will be proved if we show that these two permutations are of the same type, that is, that π and π' are even or odd simultaneously. It is evidently sufficient to show that if π is a transposition, then π' is odd. Now this is evident in case π does not involve the factor y, since in this case π' is also a transposition. Suppose now that π permutes y and x_j, and denote by k the number of factors separating y from x_j. It follows easily that the permutation π' may be resolved into $k(r+1)+r$ transpositions of adjacent factors. Since r is odd, also $k(r+1)+r$ is odd, that is, the permutation π' is odd, q.e.d.

We now turn to the total matric-algebra A_n and introduce the n^2 matric-units e_{ij}, which are subject to the relations

$$e_{ij}e_{j'k} = \begin{cases} e_{ik} & j = j', \\ 0 & j \neq j', \end{cases} \tag{4}$$

and consider sets of $2n$ matric-units

$$e_{i_1 j_1}, e_{i_2 j_2}, \cdots, e_{i_{2n} i_{2n}}. \tag{5}$$

Our chief concern will be to investigate the quantity

$$S(e_{i_1 j_1}, e_{i_2 j_2}, \cdots, e_{i_{2n} i_{2n}}) \tag{6}$$

and to show that this quantity vanishes. It will be convenient to introduce a function $f(u)$ defined for $1 \leqq u \leqq n$ which denotes the number of occurrences of u among the $4n$ subscripts in (5). Evidently

$$0 \leqq f(u) \leqq 4n, \qquad \sum_{u=1}^{n} f(u) = 4n. \tag{7}$$

We now prove the following lemma.

LEMMA 2. *Suppose that the identity* $S_{2n-2}(x) = 0$ *holds for any system of* $2n-2$ *units in* A_{n-1}. *Suppose further that at least one of the units* (5) *is idempotent, and that for this unit* e_{uu} *we have* $f(u) \leqq 4$. *Then the quantity* (6) *is equal to* 0.

PROOF. In case any two of the units (5) are equal, this is true by Remark 2, and thus we may assume that all units in (5) are dif-

ferent from each other. Since $2 \leqq f(u) \leqq 4$, we have to consider three cases. The case $f(u)=2$ is trivial, since here the idempotent e_{uu} is the only unit with a subscript equal to u, and hence by (4) each term in (6) vanishes. In case $f(u)=3$, we have aside from e_{uu} a unit of the form e_{uk}(resp. e_{ku}) while the remaining $2n-2$ units have no subscripts equal to u. By (4) it follows that the only terms which are possibly not equal to 0 are those with the left (resp. right) factor $e_{uu}e_{uk}$ (resp. $e_{ku}e_{uu}$). If therefore we denote the remaining $2n-2$ factors by $e^{(1)}, e^{(2)}, \cdots, e^{(2n-2)}$, it follows in view of Remark 4 that (6) is equal to $\pm e_{uu}e_{uk}S(e^{(1)}, \cdots, e^{(2n-2)})$ (resp. $= \pm S(e^{(1)}, \cdots, e^{(2n-2)})e_{ku}e_{uu}$). Since none of the units $e^{(i)}$ has a subscript equal to u, it follows by the assumption of the lemma in view of Remark 5 that $S(e^{(1)}, \cdots, e^{(2n-2)})=0$, and hence also (6) vanishes. It remains to deal with the case $f(u)=4$. Here we have exactly three units having a subscript equal to u. If these units are of the form e_{uu}, e_{uk}, e_{uj} or of the form e_{uu}, e_{ku}, e_{ju}, then by (4) each term in (6) vanishes, that is, (6) is equal to 0. We may therefore assume that the three units with the subscript u are of the form e_{uu}, e_{uk}, e_{ju}. Denote the remaining $2n-3$ units by $e^{(1)}, \cdots, e^{(2n-3)}$ and define the three partial sums S', S'', S''' of (6) as follows: S' is the sum of all terms with the left factor $e_{uu}e_{uk}$ and the right factor e_{ju}; S'' is the sum of all terms with the right factor $e_{ju}e_{uu}$ and the left factor e_{uk}; S''' is the sum of all terms with the common factor $e_{ju}e_{uu}e_{uk}=e_{jk}$. Since by (4) all other terms in (6) vanish, we have

$$S(e_{i_1 j_1}, \cdots, e_{i_{2n} j_{2n}}) = S' + S'' + S'''. \tag{8}$$

Each nonzero term of S' is of the form $e_{uu}e_{uk}ae_{ju}=\pm e_{uu}$, where a is a product of $2n-3$ units. To this term uniquely corresponds a term with an opposite sign belonging to S'', namely $\mp e_{uk}ae_{ju}e_{uu}=\mp e_{uu}$. The signs of the corresponding terms are indeed opposite since the number of factors is even $(=2n)$ and hence the cyclic permutation which transforms the corresponding terms in one another is odd. Hence it follows that $S'+S''=0$. As to the partial sum S''' we have in view of Remark 3 and Lemma 1

$$S''' = \pm S(e_{jk}, e^{(1)}, e^{(2)}, \cdots, e^{(2n-3)}). \tag{9}$$

Since the subscripts of the $2n-2$ units participating in (9) are different from u, it follows by the assumption of the lemma in view of Remark 5 that $S'''=0$. This completes the proof of the lemma.

LEMMA 3. *Suppose that $S_{2n-2}(x)=0$ is valid for any system of $2n-2$ units in A_{n-1}. Suppose further that* (6) *vanishes whenever the number of*

the idempotents among the units (5) *is not less than* $r+1$, *where* $r \geqq 0$. *Then* (6) *also vanishes whenever the number of idempotents in* (5) *is equal to* r.

PROOF. As in the proof of Lemma 2 we easily dispense with the case that any of the units are equal, and in case $r>0$ may assume without loss of generality that the idempotents are $e_{11}, e_{22}, \cdots, e_{rr}$. If for some subscript u such that $1 \leqq u \leqq r$ we have $f(u) \leqq 4$, then (6) vanishes by Lemma 2. We may therefore restrict our attention to the case that $f(u) \geqq 5$ for $u \leqq r$ and consider the following two cases:

Case I. There exists in (5) a unit e_{ik} such that $i>r$, $k>r$. This holds, for example, for each unit in case $r=0$. Consider the matrix $c=e_{ii}+e_{ik}$. This matrix is idempotent of rank 1 and the elements

$$e_{11}, \cdots, e_{rr}, c \tag{10}$$

form an orthogonal system of $r+1$ idempotents,[4] each having the rank 1.

Case II. For each unit e_{ik} and e_{ki} with $i>r$ we have $k \leqq r$. This implies, for example, that $r \geqq 1$. Since $f(1) \geqq 5$, it follows that for some i such that $i>r$ we must have $f(i) \leqq 3$. We now reduce this to the case where we may assume that for some i we even have $f(i) \leqq 2$. To this end first note that it follows by (4) that if some term in (6) is not equal to 0, then either each $f(u)$ is even, or $f(u)$ is even for $2n-2$ indices and odd for 2 indices. Suppose now that $f(u) \geqq 3$ for all u's and $f(i)=3$ for some i. Then either each term in (6) vanishes and our lemma is proved, or else we are confronted by the following two possibilities:

(1) $f(i)=f(j)=3$ for a pair of indices $i \neq j$, and $f(u) \geqq 4$ for $u \neq i, j$.

(2) $f(i)=3$, and $f(u) \geqq 4$ for $u \neq i$.

We may assume in the first of these two cases that $f(1)$ is even, and since $f(1) \geqq 5$, we must have $f(1) \geqq 6$, and thus it follows in both cases in view of (7) that we must have $r=1$. This implies that each unit is either of the form e_{s1} or e_{1s}, which leaves us with at most $2n-1$ units instead of with $2n$. This contradiction shows that in Case II we may indeed assume that for some i we have

$$i > r, \qquad f(i) \leqq 2. \tag{11}$$

If for this i we have $f(i)=0$, our lemma is true by Remark 5. Thus Case II is reduced to the case where we have a unit e_{ik} (or e_{ki}) so that (11) holds and $k \leqq r$. We assume without loss of generality that $k=1$. By putting $c=e_{ii}+e_{i1}$ (respectively $c=e_{ii}+e_{1i}$) and $d=e_{11}-e_{i1}$ (respectively $d=e_{11}-e_{1i}$), we get the following orthogonal set of $r+1$

[4] In case $r=0$, this system reduces to the single idempotent c.

idempotents of rank 1

$$d, e_{22}, \cdots, e_{rr}, c. \tag{12}$$

In view of the properties of systems (10) and (12) it follows that there exists a regular matrix a with coefficients in F which transforms (10), respectively (12), into the system of $r+1$ idempotents

$$e_{11}, \cdots, e_{rr}, e_{r+1\,r+1}. \tag{13}$$

In both Cases I and II we may write our units in the form $e_{11}, \cdots, e_{rr}, e_{ik}, e^{(1)}, \cdots, e^{(2n-r-1)}$ (in Case II we must eventually replace e_{ik} by e_{ki}) and we have in view of Remark 3

$$\pm S(e_{i_1 j_1}, \cdots, e_{i_{2n} j_{2n}}) = S(e_{11}, \cdots, e_{rr}, e_{ik}, e^{(1)}, \cdots, e^{(2n-r-1)}). \tag{14}$$

If in (14) we replace e_{ik} by e_{ii} we shall have $r+1$ idempotent units participating, and hence by the assumption of the lemma

$$S(e_{11}, e_{22}, \cdots, e_{rr}, e_{ii}, e^{(1)}, \cdots, e^{(2n-r-1)}) = 0. \tag{15}$$

If further in Case II we replace e_{11} by e_{i1}, we shall have two equal units, and hence by Remark 2

$$S(e_{i1}, e_{22}, \cdots, e_{rr}, e_{i1}, e^{(1)}, \cdots, e^{(2n-r-1)}) = 0. \tag{16}$$

From (14) and (15) we obtain by addition

$$\pm S(e_{i_1 j_1}, \cdots, e_{i_{2n} j_{2n}}) = S(e_{11}, \cdots, e_{rr}, c, e^{(1)}, \cdots, e^{(2n-r-1)}), \tag{17}$$

while in Case II subtraction of (16) from (14) yields

$$\pm S(e_{i_1 j_1}, \cdots, e_{i_{2n} j_{2n}}) = S(d, e_{22}, \cdots, e_{rr}, e_{i1}, e^{(1)}, \cdots, e^{(2n-r-1)}). \tag{18}$$

In Case II our system of $2n$ units may be written in the form

$$e_{11}, \cdots, e_{rr}, e_{i1}, e^{(1)}, \cdots, e^{(2n-r-1)}. \tag{19}$$

Since we have chosen e_{i1} so that (11) holds, it follows that if in (19) we replace e_{i1} by e_{ii} and e_{11} by e_{i1}, we shall get a system of $2n$ units with an idempotent e_{ii} such that $f(i) \leqq 4$, and hence by Lemma 2

$$S(e_{i1}, e_{22}, \cdots, e_{rr}, e_{ii}, e^{(1)}, \cdots, e^{(2n-r-1)}) = 0. \tag{20}$$

From (15) and (20) we obtain by subtraction

$$S(d, e_{22}, \cdots, e_{rr}, e_{ii}, e^{(1)}, \cdots, e^{(2n-r-1)}) = 0 \tag{21}$$

while from (18) and (21) we get by addition

$$\pm S(e_{i_1 j_1}, \cdots, e_{i_{2n} j_{2n}}) = S(d, e_{22}, \cdots, e_{rr}, c, e^{(1)}, \cdots, e^{(2n-r-1)}). \tag{22}$$

Transforming now (17), respectively (22), with the matrix a defined

above, we obtain therefore in Case I as well as in Case II in view of the properties of a in relation to the three orthogonal systems (12), (15), and (14)

$$\pm a^{-1}S(e_{i_1j_1}, \cdots, e_{i_{2n}j_{2n}})\cdot a = S(e_{11}, e_{22}, \cdots, e_{rr}, e_{r+1\,r+1}, a^{-1}e^{(1)}a, \cdots, a^{-1}e^{(2n-r-1)}a). \tag{23}$$

Now express each of the matrices $a^{-1}e^{(j)}a$, $j=1, \cdots, 2n-r-1$, as a linear form of the n^2 units e_{st}, then by Remark 1 we shall be able to represent the right member of (23) as a sum of terms each having the form

$$\alpha S(e_{11}, \cdots, e_{rr}, e_{r+1\,r+1}, \cdots, e_{st}, \cdots) \tag{24}$$

where α is in the underlying field. Since the system of $2n$ units participating in (24) contains at least $r+1$ idempotents, it follows by the assumption of our lemma that (24) vanishes. Hence the left member of (23) is equal to 0, and this in turn shows that also (6) is equal to 0, q.e.d.

LEMMA 4. *For each n the standard identity* $S_{2n}(x)=0$ *is satisfied by each set* (5) *of* $2n$ *units.*

PROOF. We prove this lemma by induction. For $n=1$ this is trivial. Suppose now that $n>1$ and that the lemma is true for each positive integer less than n, then we have to show that (6) vanishes for an arbitrary system (5) of $2n$ units. Now by Remark 2 the quantity (6) vanishes if all $2n$ units in (5) are idempotent. Hence by repeatedly applying Lemma 3 it follows that (6) vanishes no matter how many of the units (5)—if any—are idempotent. This completes the proof of the lemma.

THEOREM 1 (THE MAIN THEOREM). *For each n the standard identity* $S_{2n}(x)=0$ *holds for the complete matric-algebra* A_n.

PROOF. Denote by $a_1, a_2, \cdots, a_{2n}$ a set of $2n$ arbitrary matrices belonging to A_n. We have to show that

$$S(a_1, a_2, \cdots, a_{2n}) = 0. \tag{25}$$

To this end express each a_i as a linear form (with coefficients in the underlying field) of the n^2 units e_{jk}. By Remark 1 we may express the left member of (25) as a sum of terms each having the form $\alpha S(e_{i_1j_1}, \cdots, e_{i_{2n}j_{2n}})$ where α is in the underlying field. By Lemma 4 each of these terms vanishes, and hence (25) holds.

3. **Uniqueness.** Each homogeneous polynomial identity of degree

m which is linear in each of its indeterminates $x_1, \cdots, x_m$ may be written in the form

$$\sum_{(i)} \alpha_{(i)} x_{i_1} x_{i_2} \cdots x_{i_m} = 0 \tag{26}$$

where $\alpha_{(i)}$ is in F and the sum on the left of (26) ranges over all permutations (i) of m letters. Some of the $\alpha_{(i)}$ may of course be equal to 0. We prove

THEOREM 2. *If the total matric-algebra A_n satisfies an identity* (26) *with $m \leqq 2n$, then $m = 2n$ and the left member of* (26) *is but for a numerical factor belonging to F the standard polynomial $S_{2n}(x)$.*

PROOF.[5] In [4] it has been shown that a minimal polynomial of A_n is at least of degree $2n$, hence we have $m = 2n$. Let us now compare two terms of the left member of (26) which but for the coefficients may be transformed in each other by transposing a pair of adjacent factors. We may assume without loss of generality that these terms are of the form

$$\alpha x_1 x_2 \cdots x_{r-1} x_r x_{r+1} \cdots x_{2n} \quad \text{and} \quad \beta x_1 x_2 \cdots x_{r-1} x_{r+1} x_r \cdots x_{2n}. \tag{27}$$

In case r is odd, that is, $r = 2i-1$, we perform the substitution

$$\begin{aligned} x_{2j} &= e_{j\,j+1}, \quad x_{2j-1} = e_{jj} && \text{for } j < i, \\ x_{2i-1} &= x_{2i} = e_{ii}, \\ x_{2j} &= e_{jj}, \quad x_{2j-1} = e_{j-1\,j} && \text{for } j > i. \end{aligned}$$

As is readily seen, under this substitution the sum of the two terms (27) yields $\alpha e_{1n} + \beta e_{1n} = (\alpha+\beta) e_{1n}$, while each other term vanishes. Hence we have $(\alpha+\beta) e_{1n} = 0$, or

$$\alpha + \beta = 0. \tag{28}$$

In case r is even, that is, $r = 2i$, we apply the substitution

$$\begin{aligned} x_{2j} &= e_{j+1\,j+1}, \quad x_{2j-1} = e_{j\,j+1} && \text{for } j < i, \\ x_{2i} &= x_{2i+1} = e_{ii}, \\ x_{2j} &= e_{j\,j+1}, \quad x_{2j-1} = e_{j-1\,j-1} && \text{for } i < j \leqq n-1, \\ x_{2n-1} &= e_{nn}, \quad x_{2n} = e_{n1}. \end{aligned}$$

Under this substitution the sum of the two terms (27) yields $\alpha e_{11} + \beta e_{11} = (\alpha+\beta) e_{11}$, while the only other summands which are possibly not

[5] This theorem was proved independently also by G. Goldring of Jerusalem University.

equal to 0 are those which correspond to the cyclic permutations of the product $e_{12}e_{22}\cdots e_{nn}e_{n1}$. Hence it follows that the left member of (26) has the form $(\alpha+\beta)e_{11}+\sum_{i=2}^{n}\alpha_i e_{ii}$. Since (26) holds, each coefficient of this sum must vanish, and this leads again to (28). Consider now an arbitrary term $\alpha_{(i)}x_{i_1}\cdots x_{i_{2n}}$ of the left member of (26). Since each permutation (i) may be derived from the identical permutation by successive transpositions of adjacent letters, it follows in view of (28) that $\alpha_{(i)}=\pm\alpha$, where the sign is positive or negative according as the permutation (i) is even or odd. Hence $\sum_{(i)}\alpha_{(i)}x_{i_1}\cdots x_{i_{2n}}=\alpha S_{2n}(x)$, q.e.d.

We now consider a polynomial $f(x_1, x_2, \cdots, x_m)$ whose degree in one of its indeterminates, say x_1, is equal to $r>1$. By applying the transformation

$$f(y+z, x_2, \cdots, x_m)-f(y, x_2, \cdots, x_m)-f(z, x_2, \cdots, x_m) = g(y, z, x_2, \cdots, x_m) \tag{29}$$

one obtains a polynomial whose general degree is not higher than that of $f(x_1, \cdots, x_m)$ and whose degree in y as well as in z is exactly $r-1$. By successive steps of this kind one obtains a polynomial whose general degree is not higher than that of $f(x_1, x_2, \cdots, x_m)$ and which is linear in each of its indeterminates (see [1, Lemma 2]). A nonlinear polynomial will be referred to in short as almost linear if each transformation of type (29) performed on this polynomial yields either zero or a polynomial linear in each of its indeterminates. One obtains easily the following lemmas.

LEMMA 5. *A nonlinear polynomial is either almost linear or it may be transformed into an almost linear polynomial by a finite number of operations of type* (29).

LEMMA 6. *A nonlinear polynomial* $f=f(x_1, x_2, \cdots, x_m)$ *is almost linear if and only if it has the form*

$$f=\sum_{i=0}^{m}f_i \tag{30}$$

where f_0 *is of degree not greater than* 1 *in each* x_i *while each* f_i, $i>0$, *is either of degree* 2 *in* x_i *and of degree not greater than* 1 *in each* x_k, $k\neq i$, *or identically equal to* 0. *Finally,* $f_i\neq 0$ *for some* $i>0$.

We shall need also the following lemma whose proof may also be omitted.

LEMMA 7. *Suppose that* $f=f_1+f_2$, *where each monomial of* f_1, *resp.* f_2,

is of degree not less than 1, *resp. of degree* 0 *in* x_1. *If identity* $f=0$ *holds in an algebra* A, *then both identities* $f_1=0$, $f_2=0$ *hold in* A.

THEOREM 3. *Let* $h(y_1, \cdots, y_k)=0$ *be a minimal identity for the total matric-algebra* A_n *such that* $k \leqq 2n$. *If either* $n>2$ *or the underlying field is not the prime field of characteristic* 2, *then* $k=2n$ *and* h *is but for a numerical factor the standard polynomial* $S_{2n}(y)$.

PROOF. We know by Theorem 1 and by [4] that the degree of h is $2n$. The case where h is linear in each y may be dispensed with[6] by Theorem 2 with the help of Lemma 7. We therefore assume that h is not linear. Since operations of type (29) transform polynomial identities into polynomial identities, it follows in view of Lemmas 5 and 6 that our identity may be transformed into an identity (1) whose corresponding polynomial f is almost linear, that is, of the form (30). By Lemma 7 we may assume that f_i, $i \geqq 0$, is of degree not less than 1 in each x (or $f_i=0$), f_0 has general degree $2n-1$ (or $f_0=0$), and f_i, $i \geqq 1$, is of general degree $2n$ in case $f_i \neq 0$. Thus it follows that we may put $m=2n-1$. We assume finally without impairing the generality of the case that $f_1 \neq 0$. Let us apply now the transformation (29). Since each f_i, $i \neq 1$, is either equal to 0 or linear in x_1 we get

$$g(y, z, x_2, \cdots, x_{2n-1}) = f_1(y+z, x_2, \cdots, x_{2n-1}) - f_1(y, x_2, \cdots, x_{2n-1}) - f_1(z, x_2, \cdots, x_{2n-1}). \tag{31}$$

The polynomial thus obtained is evidently homogeneous and linear in each of its indeterminates, and its degree is equal to $2n$. Hence by Theorem 2

$$g(y, z, x_2, \cdots, x_{2n-1}) = \alpha_1 S(y, z, x_2, \cdots, x_{2n-1}), \quad \alpha_1 \neq 0. \tag{32}$$

Our theorem will be proved if we arrive at the contradictory conclusion that $\alpha_1=0$. To this end consider an arbitrary monomial of f_1 and write it in the form $\gamma a x_1 b x_1 c$, where $\gamma \in F$ and a, b, c are products of certain x's which are not equal to x_1. Under transformation (29) this monomial yields $\gamma a(y+z)b(y+z)c-\gamma aybyc-\gamma azbzc=\gamma aybzc+\gamma azbyc$, that is, two monomials with the same coefficient γ.[7] Since on the other hand these monomials may be transformed into each other by transposing the factors y and z, it follows in view of (32) that they must have coefficients equal to $\pm\alpha_1$ with opposite signs,

[6] It follows that if h is linear in each x, then it must be homogeneous. Otherwise we would obtain by Lemma 7 an identity of degree less than $2n$, which by [4] is impossible.

[7] Apparently neither of these two monomials can be checked against any other monomial.

that is,

$$-\gamma = \gamma = \pm \alpha_1. \tag{33}$$

In case the characteristic of F is not equal to 2, it follows from (33) that $\alpha_1 = 0$, which completes the proof of the theorem in this case. In case the characteristic is equal to 2, it follows from (33) that $\gamma = \alpha_1$, that is, all coefficients of f_1 are equal. We get a similar result for each f_i, $i \geqq 1$. Denote by $p_i = p_i(x_1, \cdots, x_{2n-1})$ for $i \geqq 1$ the sum of all $(2n)!/2$ monomials which have degree equal to 2 in x_i and degree 1 in each x_k, $k \neq i$, then $f_i = \alpha_i p_i$, a relation which holds also for $f_i = 0$ (with $\alpha_i = 0$). Thus we have

$$f = f_0 + \sum_{i=1}^{2n-1} \alpha_i p_i. \tag{34}$$

Now apply the following substitution,

$$x_{2i-1} = e_{ii}, \quad i = 1, \cdots, n; \qquad x_{2i} = e_{i\,i+1}, \quad i = 1, \cdots, n-1. \tag{35}$$

The only monomial linear in each x_i which under substitution (35) yields the unit e_{1n} is $x_1 x_2 \cdots x_{2n-1}$. Each other monomial of this kind vanishes. Hence $f_0(e_{11}, e_{12}, \cdots) = \beta e_{1n}$, where $\beta \in F$. Since under (35) we get $x_{2i}^2 = 0$, $x_{2i-1}^2 = e_{ii}$, it follows easily that $p_{2i}(e_{11}, \cdots) = 0$; $p_{2i-1}(e_{11}, \cdots) = e_{1n}$. By (34) we have $0 = f(e_{11}, \cdots) = \beta e_{1n} + \sum_{i=1}^{n} \alpha_{2i-1} e_{1n}$, which implies $\beta + \sum_{i=1}^{n} \alpha_{2i-1} = 0$ or, since the characteristic is equal to 2,

$$\beta = \sum_{i=1}^{n} \alpha_{2i-1}. \tag{36}$$

Now apply the substitution

$$x_{2i-1} = e_{i\,i+1},\ i = 1, \cdots, n-1; \quad x_{2i} = e_{ii},\ i = 1, \cdots, n-1; \quad x_{2n-1} = e_{n1}. \tag{37}$$

The only monomial linear in each x which under (37) yields the unit e_{11} is again $x_1 x_2 \cdots x_{2n-1}$, and hence it follows that the coefficient of e_{11} in the matrix $f_0(e_{12}, e_{22}, \cdots)$ is equal to β. Since under (37) we have $x_{2i-1}^2 = 0$, $x_{2i}^2 = e_{ii}$, it follows that $e_{11} \cdot p_{2i}(e_{12}, e_{22}, \cdots) e_{11} = e_{11}$, while $e_{11} \cdot p_{2i-1}(e_{12}, e_{22}, \cdots) e_{11} = 0$. Hence the coefficient of e_{11} in the matrix $f(e_{12}, e_{22}, \cdots)$ is $\beta + \sum_{i=1}^{n} \alpha_{2i}$ and we have

$$\beta = \sum_{i=1}^{n} \alpha_{2i}. \tag{38}$$

Finally apply the substitution

$$(39)\qquad \begin{aligned} &x_i = e_{i\,i+1}, \qquad i = 1, \cdots, n-1; \qquad x_n = e_{nn}; \\ &x_i = e_{2n-i+1,2n-i}, \qquad\qquad\qquad i = n+1, \cdots, 2n-1 \end{aligned}$$

(thus for $n=3$: $x_1=e_{12}$, $x_2=e_{23}$, $x_3=e_{33}$, $x_4=e_{32}$, $x_5=e_{21}$). The monomials $x_1 x_2 \cdots x_n \cdots x_{2n-1}$ and $x_1 x_2 \cdots x_n^2 \cdots x_{2n-1}$ are the only ones participating in the f's which yield the unit e_{11}; all other monomials yield either zero or units not equal to e_{11}. Hence it follows that the coefficient of e_{11} in the matrix $f(e_{12}, \cdots, e_{21})$ is equal to $\beta+\alpha_n$, that is,

$$(40)\qquad \beta = \alpha_n.$$

If n is odd, that is, $n=2k-1$, we have by (36) and (40)

$$(41)\qquad \alpha_{2k-1} = \sum_{i=1}^{n} \alpha_{2i-1}.$$

Since the odd indices may be arbitrarily rearranged without altering the right member of (41), we obtain

$$(42)\qquad \alpha_1 = \alpha_3 = \cdots = \alpha_{n-1}.$$

If n is even, that is, $n=2k$, we have by (38) and (40)

$$(43)\qquad \alpha_{2k} = \sum_{i=1}^{n-1} \alpha_{2i}$$

which by rearranging the even indices yields

$$(44)\qquad \alpha_2 = \alpha_4 = \cdots = \alpha_{2n-2}.$$

In case $n>2$ it follows from (42) and (44) by rearranging the indices that all coefficients are equal, $\alpha_1=\alpha_2= \cdots =\alpha_{2n-1}$. By adding (36) and (38) we have $2\beta=\sum_{j=1}^{2n-1}\alpha_j=(2n-1)\alpha_1=\alpha_1$, or $\alpha_1=0$, which is the required contradiction. It remains to deal with the case where $n\leqq 2$, the field F has characteristic 2, and F contains an element δ such that $\delta\neq 0$, $\delta\neq 1$. Since all f_i, $i\neq 1$, are linear in x_1, we have in case $n=2$ the relation $f(\delta x_1, x_2, x_3)-\delta f(x_1, x_2, x_3)= =\alpha_1\delta(\delta-1)p_1(x_1, x_2, x_3)$, while for $n=1$ we obtain $f(\delta x_1)-\delta f(x_1) =\alpha_1\delta(\delta-1)x_1^2$. Since $\delta(\delta-1)\neq 0$, this implies the validity of the identity $\alpha_1 p_1(x_1, x_2, x_3)=0$, respectively $\alpha_1 x_1^2=0$. By substituting $x_1=e_{11}$, $x_2=e_{12}$, $x_3=e_{22}$, respectively $x_1=1$ one gets $\alpha_1 p_1(e_{11}, e_{12}, e_{22}) =\alpha_1 e_{11}^2 e_{12} e_{22}=\alpha_1 e_{12}=0$, respectively $\alpha_1 1=0$, that is, in both cases the desired contradiction $\alpha_1=0$. This completes the proof of the theorem.

THEOREM 4. *If either $n>2$ or F is not the prime field of characteristic 2, if further $f(x_1, x_2, \cdots, x_m)$ is a minimal polynomial of A_n, then $m\geqq 2n$ and f has the form*

$$f(x_1, \cdots, x_m) = \sum_{(i)} \alpha_{(i)} S(x_{i_1}, \cdots, x_{i_{2n}}) \tag{45}$$

where the sum ranges over all $C_{m,2n}$ combinations (i) of $2n$ letters out of m, and the $\alpha_{(i)}$ are in the underlying field.

PROOF. If $m \leqq 2n$, then by Theorem 3 we have $m = 2n$ and $f(x_1, \cdots, x_m) = \alpha S(x_1, \cdots, x_{2n})$, in which case (45) is valid. Suppose now that $m > 2n$ and consider an arbitrary monomial $\alpha_1 x_{k_1} \cdots x_{k_r}$ of F, where $\alpha \neq 0$ and each x_{k_i} is some x_j. We do not assume linearity beforehand, so that some of the factors may coincide. Suppose that $x_{i_1}, x_{i_2}, \cdots, x_{i_s}$ are the distinct factors participating in this monomial, and denote by f_1, respectively f_2, the sum of all monomials which depend on those s factors only, respectively the sum of the remaining monomials, that is, $f = f_1 + f_2$. By Lemma 7 it follows that both identities $f_1 = 0, f_2 = 0$ hold in A_n. Since the degree of f is equal to $2n$, we have $s \leqq r \leqq 2n$, and hence in view of Theorem 3 it follows that $s = 2n$ and $f_1(x_{i_1}, x_{i_2}, \cdots, x_{i_s}) = \alpha_1 S(x_{i_1}, \cdots, x_{i_{2n}})$. We may repeat now the same argument with f_2, and thus proceeding, after a finite number of steps obtain the required representation (45).

It follows readily that the $C_{m,2n}$ standard polynomials defined above are linearly independent, and since each linear combination of these polynomials yields a minimal polynomial (or zero), we have the following theorem.

THEOREM 5. *If either $n > 2$ or F is not the prime field of characteristic 2, and if $x_1, x_2, \cdots, x_m$ is a set of indeterminates, then minimal polynomials of A_n depending on the x's only exist if and only if $m \geqq 2n$. The set of all such polynomials forms (if supplemented by 0) a module over whose F dimensionality is equal to $C_{m,2n}$. As a basis for this module we may choose the $C_{m,2n}$ standard polynomials defined in the previous theorem.*

The exceptional case where $n \leqq 2$ and F is the prime field of characteristic 2 is settled by the following theorem.

THEOREM 6. *The condition of Theorems 3, 4, 5 is necessary for the validity of these theorems, or in other words: The total matric-algebras A_1 and A_2 over the prime field of characteristic 2 possess nonlinear minimal identities, for example, $x + x^2 = 0$, respectively*

$$xy^3 + yxy^2 + y^2xy + y^3x + xy^2 + y^2x = 0. \tag{46}$$

PROOF. Denote by e the unit of A_2. Each element of A_2 satisfies one of the following 4 equations

$$y^2 = 0, \qquad y^2 = e, \qquad y^2 = y, \qquad y^2 = y + e.$$

By substituting each of these equations into the polynomial on the left of (46), one finds that this polynomial vanishes for each x. This completes the proof of the theorem, the case of A_1 being trivial.

REMARK. It remains to be settled by which processes—if at all—each polynomial identity of A_n may be derived from the minimal ones.

4. **Algebras.** If A is an algebra over F, and $B = A \times G$, where G is a field containing F, then evidently each identity which holds in B holds also in A. On the other hand, if an identity linear in each of its indeterminates holds in A, then this identity holds also in B (see [1, Lemma 3]). In view of Theorems 1 and 2 we have therefore the following theorem.

THEOREM 7. *If A is a simple algebra of degree n^2 over its centre F, then the degree of a minimal identity satisfied by A is exactly $2n$. A minimal identity depending on $2n$ indeterminates only and linear in each of these indeterminates $x_1, x_2, \cdots, x_{2n}$ is uniquely determined but for a numerical factor as the standard identity $S_{2n}(x) = 0$.*

Consider now a semi-simple algebra A and suppose that A is the direct sum of the ideals A' and A'', each of which satisfies an identity (1). Then identity (1) holds also in A. Indeed, let e' and e'' be the units of A', resp. A'' so that $e = e' + e''$ is the unit of A, and consider a set of m elements $a_1, a_2, \cdots, a_m$ in A. We have then $f(a_1, a_2, \cdots, a_m) = f(e'a_1, \cdots, e'a_m) + f(e''a_1, \cdots, e''a_m)$. Since (1) holds in A' as well as in A'', each of these summands vanishes, and we have in fact $f(a_1, \cdots, a_m) = 0$. This leads to the following theorem.

THEOREM 8. *Let A be a semi-simple algebra and $A', A'', \cdots, A^{(k)}$ its simple constituents. Denote by n_i^2 the order of $A^{(i)}$ over its centre. If $n^2 = \max(n_1^2, \cdots, n_k^2)$, then the degree of any minimal polynomial of A is exactly $2n$. If a minimal polynomial depends on $2n$ indeterminates only and is linear[8] in each of these indeterminates $x_1, \cdots, x_{2n}$, then this polynomial is uniquely determined but for a numerical factor as the standard polynomial $S_{2n}(x)$.*

For an arbitrary algebra of finite dimensionality we have the following theorem.

THEOREM 9. *Let r be the index of the radical N of an algebra B, and $n^2 = \max(n_1^2, \cdots, n_k^2)$ where the n_i^2 are the orders of the simple con-*

[8] As will be shown in a following communication Theorems 3–6 also retain their validity for general semi-simple algebras.

stituents of the difference algebra $A-N$. Then B satisfies the following identity of degree $2nk$.

$$[S(x_1, \cdots, x_{2n})]^k = 0.$$

PROOF. By Theorem 8 the difference algebra $A-N$ satisfies the identity $S_{2n}(x)=0$. If $b_1, \cdots, b_{2n}$ is a set of $2n$ elements belonging to B, we evidently have the relation $S(b_1, \cdots, b_{2n}) \in N$; hence, $[S(b_1, \cdots, b_{2n})]^k = 0$.

REMARK. If x_{ij}, $i=1, \cdots, 2n$; $j=1, \cdots, k$, is a set of $2nk$ indeterminates, then evidently also the identity

$$\prod_{j=1}^{k} S(x_{1j}, \cdots, x_{2n,j}) = 0$$

holds in B. This identity is homogeneous and linear in each of its indeterminates.

BIBLIOGRAPHY

1. I. Kaplansky, *Rings with a polynomial identity*, Bull. Amer. Math. Soc. vol. 54 (1948) pp. 575–580.

2. ———, *Groups with representations of bounded degree*, Canadian Journal of Mathematics vol. 1 (1949) pp. 105–112.

3. F. W. Levi, *On skew fields of a given degree*, Indian Math. Soc. (1948) pp. 85–88.

4. J. Levitzki, *A theorem on polynomial identities*, Proceedings of the American Mathematical Society vol. 1 (1950) pp. 334–341.

JERUSALEM UNIVERSITY