A THEOREM ON THE REPRESENTATION THEORY OF
JORDAN ALGEBRAS

WILLIAM H. MILLS
1. Introduction. Let $J$ be a Jordan algebra over a field $\Phi$ of characteristic neither 2 nor 3. Let $a \rightarrow S_a$ be a (general) representation of $J$. If $\alpha$ is an algebraic element of $J$, then $S_\alpha$ is an algebraic element. The object of this paper is to determine the polynomial identity* satisfied by $S_\alpha$. The polynomial obtained depends only on the minimal polynomial of $\alpha$ and the characteristic of $\Phi$. It is the minimal polynomial of $S_\alpha$ if the associative algebra $U$ generated by the $S_a$ is the universal associative algebra of $J$ and if $J$ is generated by $\alpha$.

2. Preliminaries. A (nonassociative) commutative algebra $J$ over a field $\Phi$ is called a Jordan algebra if

\[ (a^2b)a = a^2(ba) \]

holds for all $a, b \in J$. In this paper it will be assumed that the characteristic of $\Phi$ is neither 2 nor 3.

It is well known that the Jordan algebra $J$ is power associative;** that is, the subalgebra generated by any single element $a$ is associative. An immediate consequence is that if $f(x)$ is a polynomial with no constant term then $f(a)$ is uniquely defined.

Let $R_a$ be the multiplicative mapping in $J$, $a \rightarrow xa = ax$, determined by the element $a$. From (1) it can be shown that we have

\[ [R_aR_b] + [R_bR_{ac}] + [R_cR_{ab}] = 0 \]

and

\[ R_aR_bR_c + R_cR_bR_a + R_{(ac)b} = R_aR_{bc} + R_bR_{ac} + R_cR_{ab} \]

for all $a, b, c \in J$, where $[AB]$ denotes $AB - BA$. Since the characteristic of $\Phi$ is not 3, either of these relations and the commutative law imply (1). Let

Received November 20, 1950.

*This problem was proposed by N. Jacobson.

**See, for example, Albert [1].

Let $a \rightarrow S_a$ be a linear mapping of $J$ into an associative algebra $U$ such that for all $a, b, c \in J$ we have

\[(2) \quad [S_a S_b c] + [S_b S_c a] + [S_c S_a b] = 0\]

and

\[(3) \quad S_a S_b S_c + S_c S_b S_a + S_{(ac)b} = S_a S_b c + S_b S_c a + S_c S_a b.\]

Such a mapping is called a representation.

It has been shown* that there exists a representation $a \rightarrow S_a$ of $J$ into an associative algebra $U$ such that (a) $U$ is generated by the elements $S_a$ and (b) if $a \rightarrow T_a$ is an arbitrary representation of $J$ then $S_a \rightarrow T_a$ defines a homomorphism of $U$. In this case the algebra $U$ is called the universal associative algebra of $J$.

We shall now suppose that $a \rightarrow S_a$ is an arbitrary representation of $J$, and $\alpha$ a fixed element of $J$. Let $s(r) = S_\alpha r$, $A = s(1)$, $B = s(2)$. If we put $a = b = c = \alpha$ in (2), we get $AB = BA$. If we put $a = b = \alpha$, $c = \alpha^{r-2}$, $r \geq 3$, then (3) becomes

\[(4) \quad s(r) = 2A s(r - 1) + s(r - 2) B - A^2 s(r - 2) - s(r - 2) A^2.\]

We now see that $A$ and $B$ generate a commutative subalgebra $U_\alpha$ containing $s(r)$ for all $r$. By the commutativity of $U_\alpha$, (4) becomes

\[(5) \quad s(r) = 2A s(r - 1) + (B - 2A^2) s(r - 2).\]

We now adjoin to the commutative associative algebra $U_\alpha$ an element $C$ commuting with the elements of $U_\alpha$ such that $C^2 = B - A^2$. We have the following result.

**Lemma 1.** For all positive integers $r$, we have

\[s(r) = \frac{1}{2}(A + C)^r + \frac{1}{2}(A - C)^r.\]

**Proof.** If $r = 1$, then

\[\frac{1}{2}(A + C)^r + \frac{1}{2}(A - C)^r = A = s(1).\]

*For a general discussion of the theory of representations of a Jordan algebra and a proof of the existence of the universal associative algebra, see Jacobson [2].
If \( r = 2 \), then
\[
\frac{1}{2}(A + C)^r + \frac{1}{2}(A - C)^r = A^2 + C^2 = s(2).
\]

Now suppose that \( r \geq 3 \) and that Lemma 1 holds for \( r - 1 \) and \( r - 2 \). By direct substitution it follows that \( A + C \) and \( A - C \) are roots of
\[
x^2 = 2Ax + B - 2A^2,
\]
and therefore of
\[
x^r = 2Ax^{r-1} + (B - 2A^2)x^{r-2}.
\]

Hence,
\[
(A + C)^r = 2A(A + C)^{r-1} + (B - 2A^2)(A + C)^{r-2}
\]
and
\[
(A - C)^r = 2A(A - C)^{r-1} + (B - 2A^2)(A - C)^{r-2}.
\]

Adding and dividing by 2, we have the desired result:
\[
\frac{1}{2}(A + C)^r + \frac{1}{2}(A - C)^r = 2As(r - 1) + (B - 2A^2)s(r - 2) = s(r).
\]

An immediate consequence of Lemma 1 is that if \( g(x) \) is an arbitrary polynomial with no constant term, then
\[
(6) \quad S_{g(\alpha)} = \frac{1}{2} g(A + C) + \frac{1}{2} g(A - C).
\]

Now suppose further that \( \alpha \) is an algebraic element of \( I \) and that \( f(x) \) is a polynomial with no constant term, such that \( f(\alpha) = 0 \). Then by (6) we have
\[
(7) \quad 0 = 2S_{f(\alpha)} = f(A + C) + f(A - C),
\]
\[
0 = 2S_{\alpha f(\alpha)} = (A + C)f(A + C) + (A - C)f(A - C).
\]

The next step is to eliminate \( C \) from the system (7). To do this we need some additional tools.

3. Theory of elimination. Let \( \Omega \) be the splitting field of \( f(x) \) over the field \( \Phi \). Let \( P = \Phi[x], \ Q = P[y], \ P' = \Omega[x], \ Q' = P'[y] \) be polynomial rings in one and two variables over \( \Phi \) and \( \Omega \), respectively. Then \( P \) and \( P' \) are principal ideal rings. If \( q_1 \) and \( q_2 \) are elements of \( Q \), let \( (q_1, q_2) \) be the ideal of \( Q \) generated by \( q_1 \) and \( q_2 \), and let \( \{q_1, q_2\} \) be a generator of the \( P \)-ideal \( (q_1, q_2) \cap P \). Similarly, if \( q_1 \) and \( q_2 \) are elements of \( Q' \), let \( ((q_1, q_2)) \) be the ideal of \( Q' \) generated
by \( q_1 \) and \( q_2 \). Furthermore, let \( \{q_1, q_2\} \) denote a generator of the \( P' \)-ideal \( ((q_1, q_2)) \cap P' \). We note that \( \{q_1, q_2\} \) and \( \{q_1, q_2\} \) are determined up to unit factors. The unit factors are nonzero elements of \( \Phi \) and \( \Omega \) respectively.

We shall establish the following lemma.

**Lemma 2.** If \( q_1 \) and \( q_2 \) are elements of \( Q \), then \( \{q_1, q_2\} = \{q_1, q_2\} \) up to a unit factor.

**Proof.** Let \( \omega_1, \omega_2, \cdots, \omega_m \) be a basis of \( \Omega \) over \( \Phi \). Then \( P' = \sum \omega_i P \) and \( Q' = \sum \omega_i Q \). Therefore

\[
((q_1, q_2)) = Q' q_1 + Q' q_2 = \sum \omega_i q_1 + \sum \omega_i q_2 = \sum \omega_i (q_1, q_2)
\]

and

\[
((q_1, q_2)) \cap P' = \sum \omega_i ((q_1, q_2) \cap P) = ((q_1, q_2) \cap P) P' = \{q_1, q_2\} P'.
\]

It follows that \( \{q_1, q_2\} = \{q_1, q_2\} \).

Let \( r \) and \( s \) be distinct elements of \( P' \), and let \( m \) and \( n \) be positive integers. We shall determine \( \{\{(y - r)^m, (y - s)^n\}\} \).

**Lemma 3.** Let \( S(m, n) \) be that positive integer satisfying

\[
S(m, n) \leq m + n - 1,
\]

\[
\left( \frac{S(m, n) - 1}{n - 1} \right) \neq 0,
\]

and

\[
\binom{N}{n - 1} = 0 \quad \text{if} \ S(m, n) \leq N \leq m + n - 2,
\]

where \( \binom{N}{M} \) is the binomial coefficient considered as an integer in \( \Phi \). Then we have

\[
\{\{(y - r)^m, (y - s)^n\}\} = (s - r)^{S(m, n)}.
\]

**Proof.** We note that \( S(m, n) \) depends only on \( m, n \), and the characteristic \( p \) of \( \Phi \). If \( p = 0 \), or if \( p \geq m + n - 1 \), then \( S(m, n) = m + n - 1 \). In any case,

\[
m + n - 1 \geq S(m, n) \geq n.
\]
Replacing \( y \) by \( y + r \), we may assume that \( r = 0 \), \( s \neq 0 \). Formally, modulo \( y^m \), we have

\[
(s - y)^{-n} = s^{-n}(1 - y/s)^{-n} \equiv s^{-n} \sum_{\mu=0}^{m-1} \binom{-n}{\mu} (-y/s)^{\mu} = s^{-n} \sum_{\mu=0}^{m-1} \binom{n + \mu - 1}{n - 1} y^{\mu} = \sum_{\nu=n}^{m-1} s^{-\nu} \binom{\nu - 1}{n - 1} y^{\nu - n}.
\]

Therefore there exists a \( q \in Q' \) such that

\[
q y^n + (y - s)^n (-1)^n \sum_{\nu=n}^{m-1} s^{S(m,n) - \nu} \binom{\nu - 1}{n - 1} y^{\nu - n} = s^{S(m,n)}.
\]

It follows that

\[
\{ y^n, (y - s)^n \} \mid s^{S(m,n)}.
\]

Put

\[
\{ y^n, (y - s)^n \} = G, \quad s^{S(m,n)} / G = H.
\]

Then \( G \) and \( H \) are elements of \( P' \). Furthermore, there exist \( q_1 \) and \( q_2 \) in \( Q' \) such that the \( y \)-degree of \( q_2 \) is less than \( m \) and such that \( q_1 y^m + q_2 (y - s)^n = G \). Hence

\[
q_1 H y^n + q_2 H (y - s)^n = GH = s^{S(m,n)}.
\]

Subtracting (9) from (10) and comparing terms not divisible by \( y^m \), we obtain

\[
q_2 H = (-1)^n \sum_{\nu=n}^{m-1} s^{S(m,n) - \nu} \binom{\nu - 1}{n - 1} y^{\nu - n}.
\]

Comparing coefficients of \( y^{S(m,n) - n} \) in (11), we get

\[
H \mid \binom{S(m,n) - 1}{n - 1},
\]
which is a nonzero element of $\Phi$. Therefore $H$ is a unit element, and this establishes Lemma 3.

In the following we shall use l.c.m. $(a_1, a_2, \ldots, a_n)$ for the least common multiple of $a_1, a_2, \ldots, a_n$.

**Lemma 4.** If $((q_1, q_2)) \supseteq P'$, then

\[
\{\{q_1 q_2, q_3\}\} = \text{l.c.m.}(\{\{q_1, q_3\}\}, \{\{q_2, q_3\}\}).
\]

**Proof.** Put $p_1 = \{\{q_1, q_3\}\}$, $p_2 = \{\{q_2, q_3\}\}$, and $p_3 = \text{l.c.m.}(p_1, p_2)$. We note that $((q_1, q_3)) \cap P' \supseteq ((q_1 q_2, q_3)) \cap P'$, and therefore $p_1 | \{\{q_1 q_2, q_3\}\}$.

Similarly, $p_2 | \{\{q_1 q_2, q_3\}\}$, and hence $p_3 | \{\{q_1 q_2, q_3\}\}$. Now there exist $D, E, F, G, H, l$ in $Q'$ such that

\[
D q_1 + E q_3 = p_1, \quad F q_2 + G q_3 = p_2, \quad H q_1 + I q_2 = 1.
\]

Therefore

\[
D q_1 q_2 + E q_2 q_3 = p_1 q_2 \quad \text{and} \quad F q_1 q_2 + G q_1 q_3 = p_2 q_1.
\]

Hence there exist $K, L, M, N$ in $Q'$ such that

\[
K q_1 q_2 + L q_3 = p_3 q_2 \quad \text{and} \quad M q_1 q_2 + N q_3 = p_3 q_1.
\]

Hence

\[
(HM + IK) q_1 q_2 + (HN + IL) q_3 = p_3.
\]

Therefore $\{\{q_1 q_2, q_3\}\} | p_3$, and the proof of Lemma 4 is complete.

We shall now determine $\{D, E\}$, where

\[
D = f(x + y) + f(x - y),
\]

\[
E = (x + y) f(x + y) + (x - y) f(x - y).
\]

By Lemma 2, we have $\{D, E\} = \{\{D, E\}\}$. Since

\[
E - (x - y)D = 2yf(x + y),
\]

we have

\[
\{\{D, E\}\} = \{\{D, yf(x + y)\}\}.
\]
Put

\[ \{\{f(x + y), f(x - y)\}\} = \Delta. \]

Let \( n \) be the degree of \( f(x) \). Choose \( F(y) \) and \( G(y) \) in \( Q' \), with \( y \)-degree less than \( n \), such that

\[ F(y) f(x + y) + G(y) f(x - y) = \Delta. \]

Then \( F(y) \) and \( G(y) \) are completely determined. Now

\[ F(-y) f(x - y) + G(-y) f(x + y) = \Delta. \]

Therefore we have \( F(-y) = G(y) \), from which it follows that \( F(0) = G(0) \), or \( y | [F(y) - G(y)] \). Now

\[ (F(y) - G(y)) f(x + y) + G(y) D = \Delta. \]

Therefore \( \{\{D, yf(x + y)\}\} | \Delta \). It is clear that \( \Delta | \{\{D, yf(x + y)\}\} \). Thus we have

\[ \{D, E\} = \{\{D, yf(x + y)\}\} = \Delta. \]

We must now determine

\[ \Delta = \{\{f(x + y), f(x - y)\}\}. \]

Let \( f(x) = \prod (x - \alpha_i)^{n_i} \), where the \( \alpha_i \) are distinct elements of \( \Omega \). Then

\[ f(x + y) = \prod (x + y - \alpha_i)^{n_i}, \quad f(x - y) = \prod (x - y - \alpha_j)^{n_j}. \]

If \( q_1 \) and \( q_2 \) are two relatively prime factors of \( f(x + y) \), or of \( f(x - y) \), then \( ((q_1, q_2)) \supseteq P' \). Therefore we can apply Lemmas 3 and 4 to obtain

(12) \[ \{D, E\} = \{\{f(x + y), f(x - y)\}\} = 1, \text{c.m.} (2x - \alpha_i - \alpha_j)^{S(n_i, n_j)}. \]

4. The equation for \( S_\alpha \). We shall establish the following result.

**Theorem.** Let \( \alpha \) be an algebraic element of \( J \) satisfying the equation \( f(\alpha) = 0 \), where \( f(x) \) is a polynomial with no constant term. Let

\[ f(x) = \prod (x - \alpha_i)^{n_i} , \]
where the $\alpha_i$ are distinct elements of the splitting field $\Omega$ of $f(x)$. Put

$$\psi(x) = \text{l.c.m}_{i,j} (x - (1/2)\alpha_i - (1/2)\alpha_j)^{s(n_i, n_j)}.$$  

Then $\psi(S_\alpha) = 0$. Furthermore, if the algebra $U$ generated by the $S_\alpha$, $\alpha \in I$, is the universal associative algebra of $I$, if $f(x)$ is the minimal polynomial of $\alpha$, and if $I$ is generated by $\alpha$, then $\psi(x)$ is the minimal polynomial satisfied by $S_\alpha$.

Proof. As before, we let $P = \mathbb{K}[x]$, $Q = P[y]$ be polynomial rings over $\Phi$ in one and two variables respectively, and put

$$D = f(x + y) + f(x - y)$$

and

$$E = (x + y) f(x + y) + (x - y) f(x - y).$$

From (7) and (12) it follows that $\psi(S_\alpha) = 0$. We must now show that $\psi(x)$ is the minimal polynomial of $S_\alpha$ under the three given conditions. If we let $(f(x))$ be the principal ideal of $P$ generated by $f(x)$, then $I$ is isomorphic to the quotient ring $P/(f(x))$ under the natural mapping $g(\alpha) \rightarrow g(x) + (f(x))$. Let $V$ be the quotient ring $Q/(D, E)$. We now consider the linear mapping

$$g(x) \rightarrow T_g(x) = (1/2)g(x + y) + (1/2)g(x - y) + (D, E)$$

of $P$ into $V$. By the commutativity of $V$ we have, for all $g, h, j \in P$,

$$[T_gT_h] + [T_hT_g] + [T_jT_{gh}] = 0,$$

since each of the three terms vanishes. Furthermore, by direct substitution we have

$$2T_gT_hT_j + T_{ghj} = T_gT_hj + T_jT_{gh}. $$

We now determine the kernel $K$ of the mapping (13). By definition, $g(x) \in K$ if and only if $g(x + y) + g(x - y) \in (D, E)$. Now

$$yf(x + y) = (1/2)E - (1/2)(x - y)D \in (D, E)$$

and

$$yf(x - y) = (1/2)(x + y)D - (1/2)E \in (D, E).$$

Let $q(x)$ be an arbitrary element of $P$. Then, for suitable $h(x, y) \in Q$, we have
Therefore \( q(x)f(x) \in K \) for all \( q(x) \), and thus \( K \supseteq (f(x)) \). Suppose \( g(x) \in K \), \( g(x) \notin (f(x)) \). We may suppose that the degree of \( g(x) \) is less than \( n \), the degree of \( f(x) \). Then \( g(x + y) + g(x - y) = h_1D + h_2E \) for suitable \( h_1 \) and \( h_2 \) in \( Q \). Since the degree of \( D \) is \( n \) and that of \( E \) is \( n + 1 \), it follows that \( h_1 = h_2 = 0 \). Therefore \( g(x + y) + g(x - y) \) is identically 0. This implies that \( g(x) \) is identically zero, a contradiction; hence we have \( K = (f(x)) \). It follows that

\[
g(\alpha) \rightarrow T_g(x) = (1/2)g(x + y) + (1/2)g(x - y) + (D,E)
\]

defines a single-valued linear mapping of \( J \) into \( V \). Furthermore, (14) and (15) imply that this mapping is a representation, and from (12) it follows that \( T_x \), the image of \( x \), has \( \psi(x) = \{D, E\} \) as its minimal polynomial. Now since \( U \) is the universal associative algebra of \( J \), the mapping \( S_g(\alpha) \rightarrow T_g(x) \) defines a homomorphism* of \( U \) into \( V \). It follows that \( \psi(x) \) is the minimal polynomial of \( S_\alpha \). This completes the proof.

We conclude by mentioning two simple consequences of the main theorem. If \( f(x) = x^n \), then \( \psi(x) = x^{S(n,n)} \). Now (8) yields \( S(n,n) \leq 2n - 1 \), and we have the following result.

**Corollary 1.** If \( \alpha^n = 0 \), then \( S_{\alpha}^{2n-1} = 0 \).

Similarly, we obtain the following result.

**Corollary 2.** Let \( f(\alpha) = 0 \), where

\[
f(x) = \prod_{\mu=1}^{n} (x - \beta_\mu) .
\]

Then \( \Lambda(S_\alpha) = 0 \), where

\[
\Lambda(x) = \prod_{\mu \geq \nu} (x - (1/2)\beta_\mu - (1/2)\beta_\nu).
\]

*In fact it can easily be shown that this mapping is an isomorphism of \( U \) onto \( V \).
Proof. Suppose
\[ f(x) = \prod (x - \alpha_i)^{n_i} , \]
where the \( \alpha_i \) are distinct. Now by (8),
\[ S(n_i, n_j) \leq n_i + n_j - 1 \leq n_i n_j , \]
and
\[ \Lambda(x) = \prod (x - \alpha_i)^{n_i(n_i+1)/2} \prod_{j > i} (x - (1/2) \alpha_i - (1/2) \alpha_j)^{n_i n_j} . \]
Therefore \( \psi(x) \mid \Lambda(x) \), and the second corollary follows.

References


Yale University
PACIFIC JOURNAL OF MATHEMATICS

EDITORS
HERBERT BUSEMANN R. M. ROBINSON
University of Southern California University of California
Los Angeles 7, California Berkeley 4, California

E. F. BECKENBACH, Managing Editor
University of California
Los Angeles 24, California

ASSOCIATE EDITORS
R. P. DILWORTH P. R. HALMOS BÖRGE JESSEN J. J. STOKER
HERBERT FEDERER HEINZ HOPF PAUL LÉVY E. G. STRAUS
MARSHALL HALL R. D. JAMES GEORGE PÓLYA KÔSAKU YOSIDA

SPONSORS
UNIVERSITY OF BRITISH COLUMBIA UNIVERSITY OF SOUTHERN CALIFORNIA
CALIFORNIA INSTITUTE OF TECHNOLOGY STANFORD UNIVERSITY
UNIVERSITY OF CALIFORNIA, BERKELEY WASHINGTON STATE COLLEGE
UNIVERSITY OF CALIFORNIA, DAVIS UNIVERSITY OF WASHINGTON
UNIVERSITY OF CALIFORNIA, LOS ANGELES
UNIVERSITY OF CALIFORNIA, SANTA BARBARA AMERICAN MATHEMATICAL SOCIETY
OREGON STATE COLLEGE NATIONAL BUREAU OF STANDARDS,
UNIVERSITY OF OREGON INSTITUTE FOR NUMERICAL ANALYSIS

Mathematical papers intended for publication in the Pacific Journal of Mathematics should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. All other communications to the editors should be addressed to the managing editor, E. F. Beckenbach, at the address given above.

Authors are entitled to receive 100 free reprints of their published papers and may obtain additional copies at cost.

The Pacific Journal of Mathematics is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $8.00; single issues, $2.50. Special price to individual faculty members of supporting institutions and to members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to the publishers, University of California Press, Berkeley 4, California.
Tom M. (Mike) Apostol, *On the Lerch zeta function* ......................... 161
Ross A. Beaumont and Herbert S. Zuckerman, *A characterization of the subgroups of the additive rationals* ................................. 169
Richard Bellman and Theodore Edward Harris, *Recurrence times for the Ehrenfest model* ......................................................... 179
Stephen P.L. Diliberto and Ernst Gabor Straus, *On the approximation of a function of several variables by the sum of functions of fewer variables* ........................................................................... 195
Isidore Isaac Hirschman, Jr. and D. V. Widder, *Convolution transforms with complex kernels* .................................................. 211
Irving Kaplansky, *A theorem on rings of operators* ....................... 227
W. Karush, *An iterative method for finding characteristic vectors of a symmetric matrix* ............................................................... 233
Henry B. Mann, *On the number of integers in the sum of two sets of positive integers* .............................................................. 249
Tibor Radó, *An approach to singular homology theory* .................. 265
Otto Szász, *On some trigonometric transforms* ............................. 291
James G. Wendel, *On isometric isomorphism of group algebras* .......... 305
George Milton Wing, *On the $L^p$ theory of Hankel transforms* ........ 313