

## A Scalar Expression for Matrices With Symplectic Involution\*

By Louis Halle Rowen and Uri Schild

**Abstract.** Various algebraic reductions are made to facilitate computer verification of the following result: If  $x$  and  $y$  are  $8 \times 8$  matrices such that  $[x, y]$  is regular,  $\text{tr}(x) = 0$ , and, with respect to the canonical symplectic involution,  $x$  is symmetric and  $y$  is antisymmetric, then the element  $(x + [x, y]x[x, y]^{-1})^2$  satisfies a minimal equation of degree  $\leq 2$ .

The purpose of this paper is to show how the computer can be used in conjunction with various algebraic tools, to prove nice results in the theory of rings. One fundamental concept in ring theory is a *simple* ring, a ring having no proper nonzero ideals. Recall that the *center* of a ring  $R$  is  $\{c \in R | cr = rc \text{ for all } r \text{ in } R\}$ . The center  $F$  of a simple ring  $R$  is obviously a field, over which  $R$  can be viewed as a vector space; if the dimension of  $R$  over  $F$  is finite,  $R$  is called a *central simple  $F$ -algebra*. The obvious example is  $M_n(F)$ , the ring of  $n \times n$  matrices over a field  $F$ , which clearly has dimension  $n^2$  over  $F$ . In fact, the dimension of any central simple algebra (over its center) is a perfect square, cf. Albert [1], which is the standard reference on central simple algebras. (Albert calls them "normal simple".) Thus, if  $R$  is central simple of dimension  $n^2$ , we call  $n$  the *degree* of  $R$ . For  $n = 2, 3, 4, 6$ , and  $12$ , the nature of central simple  $F$ -algebras has been very well understood for 40 years (cf. [1]). For other  $n$ , very little positive information is known unless some arithmetic assumption is made about  $F$ . There is another piece of structure intrinsic to  $M_n(F)$ —the transpose, which we denote as the map  $x \rightarrow x^t$ .

Algebraically, the transpose is an anti-automorphism of degree 2 which fixes the elements of the center; in general, such a map is called an *involution*. Another example of ring with involution is any ring of generalized quaternions. Of course, the transpose gives rise to many different involutions on  $M_n(F)$ , via change of basis. However, if  $n$  is even (and if  $1 + 1 \neq 0$  in  $F$ ), then there is another involution not realizable in this way. Namely, given a matrix  $x$  partitioned into  $(n/2) \times (n/2)$  matrices  $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ , we define the *canonical symplectic involution*(s), by

$$x^s = \begin{pmatrix} D^t & -B^t \\ -C^t & A^t \end{pmatrix} = yx^t y^{-1},$$

where  $y = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ ,  $I$  denoting the identity  $(n/2) \times (n/2)$  matrix. This involution has

---

Received March 21, 1977.

AMS (MOS) subject classifications (1970). Primary 15-04, 16-04, 16A42; Secondary 15A09, 15A30, 15A57.

\*This work was supported in part by the Israel Committee for Basic Research.

Copyright © 1978, American Mathematical Society

some very nice properties, and is often more useful than the transpose in proving theorems; the reason will become clearer later (cf. Lemma 5). Using symplectic involutions, one can prove

**THEOREM A (ROWEN [5]).** *If  $R$  is a division algebra of degree 8 with involution, then  $R$  has a subfield which is a Galois extension of dimension 8 over the center, having Galois group  $Z_2 \oplus Z_2 \oplus Z_2$ .*

Theorem A is nice, because there are ways of characterizing central simple algebras of degree  $n$  if we know they contain a Galois extension of the center of dimension  $n$  (cf. [1, Chapter V]). The key step in the proof of Theorem A was, interestingly, a statement about matrices which could be verified formally on the computer. We shall present this theorem, and spend the rest of the paper simplifying the statement to the stage where it can be verified formally by a computer. The actual program was carried out at Bar-Ilan; the details of the run are given at the end of the paper.

In what follows, we shall assume that  $F$  is a field in which  $1 + 1 \neq 0$ . (This assumption can be removed at the end, using well-known but somewhat intricate methods.) The symbol  $[a, b]$  means  $ab - ba$ .

**THEOREM 1.** *If  $x, y \in M_8(F)$ , such that  $[x, y]$  is invertible,  $\text{tr}(x) = 0$ ,  $x^s = x$ , and  $y^s = -y$ , then  $z = (x + [x, y]x[x, y]^{-1})^2$  satisfies a minimal equation of degree  $\leq 2$  over  $F$ .*

*Proof.* This is mostly a sequence of reductions. If

$$x = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix},$$

then the hypotheses on  $x$  and  $y$  are equivalent to  $\text{tr}(A_1) = 0$ ,  $D_1 = A_1^t$ ,  $B_1 = -B_1^t$ ,  $C_1^t = -C_1$ ,  $D_2 = -A_2^t$ ,  $B_2 = B_2^t$ , and  $C_2 = C_2^t$ .

Consider the field  $F(\xi)$  generated over  $F$  by commuting indeterminates  $\xi_{ij}^{(k)}$ ,  $1 \leq i, j \leq 8$ ,  $1 \leq k \leq 2$ . Letting  $\{e_{ij} \mid 1 \leq i, j \leq 4\}$  be a set of usual matrix units for  $M_4(F)$ , the most general situation is clearly achieved when we replace the entries of  $x$  and  $y$  by indeterminates  $\xi_{ij}^{(k)}$ , subject to the hypotheses on  $x$  and  $y$ . In other words write

$$x_0 = \begin{pmatrix} A_1 & B_1 \\ C_1 & A_1^t \end{pmatrix}, \quad y_0 = \begin{pmatrix} A_2 & B_2 \\ C_2 & -A_2^t \end{pmatrix},$$

where

$$A_1 = \sum_{i=1}^3 \xi_{ii}^{(1)} e_{ii} - (\xi_{11}^{(1)} + \xi_{22}^{(1)} + \xi_{33}^{(1)}) e_{44} + \sum_{i < j} (\xi_{ij}^{(1)} e_{ij} + \xi_{ji}^{(1)} e_{ji}),$$

$$B_1 = \sum_{i < j} \xi_{i,j+4}^{(1)} (e_{ij} - e_{ji}), \quad C_1 = \sum_{i < j} \xi_{i+4,j}^{(1)} (e_{ij} - e_{ji}),$$

$$A_2 = \sum_{i=1}^4 \sum_{j=1}^4 \xi_{ij}^{(2)} e_{ij}, \quad B_2 = \sum_{i < j} \xi_{i,j+4}^{(2)} (e_{ij} + e_{ji}),$$

$$C_2 = \sum_{i < j} \xi_{i+4,j}^{(2)} (e_{ij} + e_{ji}).$$

*N.B.* In all of the sums taken over “ $i < j$ ”, we mean all  $(i, j)$  such that  $1 \leq i < j \leq 4$ .

Thus, the question of proving this theorem is equivalent to evaluating our expression on  $x_0$  and  $y_0$ . Indeed, writing  $z_0 = (x_0 + [x_0, y_0]x_0[x_0, y_0]^{-1})^2$ , we need to show  $z_0$  is not scalar, but that  $z_0$  satisfies some equation of degree 2 over  $F(\xi)$ . First we want an easily computable characterization of this property. The following result can be found in [1, Theorem 8.13].

LEMMA 1. *Suppose  $K$  is a subfield (containing  $F$ ) of  $M_n(F)$ . For any element  $r$  in  $K$ , the characteristic polynomial of  $r$  is a power of the minimal polynomial of  $r$ .*

Let  $\text{tr}(\ )$  denote the trace function of a matrix.

LEMMA 2. *Suppose  $K$  is a subfield (containing  $F$ ) of  $M_n(F)$ ,  $1/n \in F$ , and  $K$  is generated algebraically by the element  $r$  over  $F$ . Then the minimal polynomial of  $r$  has degree 2, if and only if  $n$  is even and  $(r - (1/n)\text{tr}(r))^2$  is scalar.*

*Proof.* If  $(r - (1/n)\text{tr}(r))^2 = \alpha \in F$ , then  $r^2 - ((2/n)\text{tr}(r))r + ((1/n)\text{tr}(r))^2 - \alpha = 0$ , so  $r$  satisfies a polynomial of degree 2. Conversely, if  $r^2 + \beta_1 r + \beta_2 = 0$  for suitable elements  $\beta_1, \beta_2$ , of  $F$ , then, from Lemma 1,  $n$  is even and  $(\lambda^2 + \beta_1 \lambda + \beta_2)^{n/2}$  is the characteristic polynomial of  $r$ . Hence  $-(\beta_1 n)/2 = \text{tr}(r)$ , so  $(r - (1/n)\text{tr}(r))^2 = (r + \beta_1/2)^2 = r^2 + \beta_1 r + \beta_1^2/4 = \beta_1^2/4 - \beta_2$ , a scalar matrix.

Note that  $1/n \in F$  if and only if  $n \cdot 1 \neq 0$ , if and only if  $p \cdot 1 \neq 0$  for every prime number dividing  $n$ . A nontrivial fact which can be culled from [4, Theorem 29] is that our element  $z_0$  generates a field over  $F(\xi)$ . (This kind of result can be stated in very general terms.) Thus, we have

*Reduction 1.* Theorem 1 is true if and only if  $(z_0 - (1/8)\text{tr}(z_0))^2$  is scalar.

Now we have a problem which, in theory, can be verified via a computer. Indeed, all we need to show is that the matrix  $z_0$  (of  $M_8(F(\xi))$ ) is not scalar and  $(z_0 - (1/8)\text{tr}(z_0))^2$  is scalar. The rest of this paper comprises simplification of the computation, in order to make the problem manageable for the computer.

First, note that the verification in Reduction 1 does not depend on the field of coefficients, so we could replace  $F(\xi)$  by its algebraic closure, which we call  $\bar{F}$ .

LEMMA 3. *There is a nonsingular matrix  $a$  in  $M_8(\bar{F})$ , such that  $a^s = a^{-1}$  and  $axa^s$  is diagonal.*

*Proof.* An easy induction argument on the number of nondiagonal terms, which we omit.

*Reduction 2.* On the definition of  $z_0$ , we may replace  $x_0$  by

$$x'_0 = \sum_{i=1}^3 \xi_{ii}^{(1)} (e_{ii} + e_{i+4,i+4} - e_{44} - e_{88}).$$

*Proof.*  $(z_0 - (1/8)\text{tr}(z_0))^2$  is scalar if and only if  $(az_0 a^s - (1/8)\text{tr}(az_0 a^s))^2$  is scalar, where  $a$  is as in Lemma 3, and  $az_0 a^s = x' + [x', y']x'[x', y']^{-1}$ , where  $x' =$

$ax_0a^s$  and  $y' = ay_0a^s$ . But clearly  $\text{tr}(x') = 0$ ,  $(x')^s = x'$ , and  $(y')^s = -y'$ . Moreover,  $x'$  is diagonal. Thus, in view of Reduction 1, we can prove Theorem 1 if we can verify the case when  $x$  is diagonal. Now, once again, to prove this, we need only check the situation where the nonzero entries of  $x$  and  $y$  are replaced by indeterminates. In other words, since  $x$  is now diagonal, we can replace  $x_0$  by  $x'_0$  of the form  $\begin{pmatrix} A_1 & 0 \\ 0 & A_1^t \end{pmatrix}$ , where  $A_1 = \sum_{i=1}^3 \xi_{ii}^{(1)} e_{ii} - (\xi_{11}^{(1)} + \xi_{22}^{(1)} + \xi_{33}^{(1)}) e_{44}$ ;  $y_0$  remains as previously stated. This proves Reduction 2.

Write  $\xi_i$  for  $\xi_{ii}^{(1)}$ ,  $1 \leq i \leq 3$ , and write  $\xi_4$  for  $-\sum_{i=1}^3 \xi_{ii}^{(1)}$ . Set  $w_0 = [x'_0, y_0] = \begin{pmatrix} A_3 & B_3 \\ C_3 & D_3 \end{pmatrix}$ , where  $A_3 = [A_1, A_2]$ ,  $B_3 = [A_1, B_2]$ ,  $C_3 = [A_1, C_2]$ , and  $D_3 = [A_1, -A_2^t] = [-A_2, A_1]^t = [A_1, A_2]^t = A_3^t$ . Note that

$$A_3 = \sum_{i=1}^4 \sum_{j=1}^4 (\xi_i - \xi_j) \xi_{ij}^{(2)} e_{ij}, \quad B_3 = \sum_{i < j} (\xi_i - \xi_j) \xi_{i,j+4}^{(2)} (e_{ij} - e_{ji}),$$

$$C_3 = \sum_{i < j} (\xi_i - \xi_j) \xi_{i+4,j} (e_{ij} - e_{ji}).$$

Let us define a set of commuting indeterminates  $\mu_{ij}$ , and set  $w'_0 = \begin{pmatrix} A_4 & B_4 \\ C_4 & A_4^t \end{pmatrix}$ ,

where

$$A_4 = \sum_{i < j} (\mu_{ij} e_{ij} + \mu_{ji} e_{ji}), \quad B_4 = \sum_{i < j} \mu_{i,j+4} (e_{ij} - e_{ji}), \quad C_4 = \sum_{i < j} \mu_{i+4,j} (e_{ij} - e_{ji}).$$

*Reduction 3.* Let  $z'_0 = (x'_0 + w'_0 x'_0 (w'_0)^{-1})^2$ . Theorem 1 is true if and only if  $z'_0$  is not scalar and  $(z'_0 - (1/8)\text{tr}(z'_0))^2$  is scalar.

The sufficiency of Reduction 3 to prove the theorem is clear when we compare  $w_0$  and  $w'_0$  (since the entries of  $w'_0$  are indeterminates). Conversely,  $w'_0$  can be obtained as  $[x'_0, y]$ , where  $y = \begin{pmatrix} A & B \\ C & -A^t \end{pmatrix}$  with

$$A = \sum_{i < j} ((\mu_{ij} e_{ij} - \mu_{ji} e_{ji}) / (\xi_i - \xi_j)), \quad B = \sum_{i < j} (\mu_{i,j+4} / (\xi_i - \xi_j)) (e_{ij} + e_{ji}),$$

$$C = \sum_{i < j} (\mu_{i+4,j} / (\xi_i - \xi_j)) (e_{ij} + e_{ji}).$$

This shows the condition on Reduction 3 is a special case of the assertion of Theorem 1.

*Definition.* Say  $r$  has degree 2 if and only if  $r$  is not scalar and  $(r - (1/8)\text{tr}(r))^2$  is scalar.

*Remark 1.* An element  $r$  has degree 2 if and only if for some nonzero scalar  $\alpha$ ,  $\alpha r$  has degree 2.

In view of Remark 1, our strategy was to find a matrix  $w_1$ , such that  $w'_0 w_1$  is a scalar  $\alpha$ , and to prove that  $\alpha z'_0 = (\alpha x'_0 + w'_0 x'_0 w_1)^2$  has degree 2. The obvious choice for  $w_1$  was the adjoint matrix of  $w'_0$ . However, a straightforward computation of cofactors was out of the question, due to the sheer size of the algebraic expressions,

the real memory of our computer (1000 *K*-bytes of memory) and the not-so-efficient storage schemes of the FORMAC system.

In such cases a common approach is to use the explicit block structure of  $w'_0$  and to define a similar structure on  $w'^{-1}_0$ . Indeed, it is a simple matter to compute  $(w'_0)^{-1}$  in terms of  $A_4, B_4, C_4$ , and  $(B_4 - A_4C_4^{-1}A_4)^{-1}$ , and, noting that  $B_4 - A_4C_4^{-1}A_4$  is antisymmetric (with respect to  $(t)$ ), we can easily compute  $(B_4 - A_4C_4^{-1}A_4)^{-1}$ . This observation enabled us to find an expression for  $(z'_0 - (1/8)\text{tr}(z'_0))^2$ , but we could not open the expression (in order to cancel terms) because of limitations of memory.

At this point, we resorted to use of the Pfaffian, a well-known tool to Jordan algebraists, but not very well known in general. Let  $a$  be a matrix of the form  $\sum_{1 \leq i < j \leq n} a_{ij}(e_{ij} - e_{ji})$ , i.e.  $a^t = -a$ . Our first goal is to find a formal square root of  $\det(a)$ . If  $n$  is odd, then  $\det(a) = 0$ , so assume  $n$  is even and define  $\text{Pf}(a) = \sum \text{sg}(\pi) a_{\pi(1)\pi(2)} \cdots a_{\pi(n-1)\pi(n)}$ , summed over all permutations of  $\{1, 2, \dots, n\}$  satisfying  $\pi(2i - 1) < \pi(2i)$  for all  $i$  between 1 and  $n/2$ , and  $\pi(2i - 1) < \pi(2i + 1)$  for all  $i$  between 1 and  $(n/2) - 1$ . For example, if  $n = 2$ , then  $\text{Pf}(a) = a_{12}$ ; if  $n = 4$ , then  $\text{Pf}(a) = (a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23})$ . An easy induction based on [3, p. 394] yields the following fact:

LEMMA 4.  $\det(a) = (\text{Pf}(a))^2$ .

(Proof omitted.)

LEMMA 5. Suppose  $b \in M_n(F)$ ,  $n$  is even, and  $b^s = b$ . Let  $T$  denote the matrix  $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ , where  $I$  is the  $(n/2) \times (n/2)$  identity matrix. Then  $p_1(\lambda) = \text{Pf}(T\lambda - Tb)$  is a polynomial (in  $\lambda$ ) with coefficients in  $F$ , whose square is the characteristic polynomial of  $b$ , and  $p_1(b) = 0$ . (Here  $\lambda$  is a commuting indeterminate over  $M_n(F)$ .)

*Proof.*  $T\lambda - Tb \in M_n(F[\lambda])$  and is easily seen to be antisymmetric under  $(t)$ . Thus  $\text{Pf}(T\lambda - Tb) \in F[\lambda]$ , i.e.  $\text{Pf}(T\lambda - Tb)$  is a polynomial  $p_1(\lambda)$  with coefficients in  $F$ .  $(p_1(\lambda))^2 = \det(T\lambda - Tb) = (\det T)\det(\lambda - b) = \det(\lambda - b)$ , the characteristic polynomial of  $b$ , which we call  $p(\lambda)$ . Thus  $(p_1(b))^2 = p(b) = 0$ . At this point we would like to conclude  $p_1(b) = 0$ , and this can in fact be argued, through [4, Theorem 29]. However, a more palatable method for most people would be to mimic the usual proof of the Hamilton-Cayley Theorem [2, p. 101]. Q.E.D.

As mentioned above, Lemma 5 is an important tool in the study of Jordan algebras. One advantage of having an equation from the Pfaffian is that whenever  $b$  is nonsingular and  $b^m + \sum_{i=0}^{m-1} \alpha_i b^i = 0$  for suitable  $i$ , we have  $\alpha_0 b^{-1} = -(b^{m-1} + \sum_{i=1}^{m-1} \alpha_i b^{i-1})$ . Now  $(w'_0)^s = w'_0$ , as is obvious. Therefore, in the notation of Lemma 5,  $p_1(w'_0) = 0$ , where  $p_1(\lambda) = \text{Pf}(T\lambda - Tw'_0)$ , a polynomial of the form  $\lambda^4 + \alpha_3 \lambda^3 + \alpha_2 \lambda^2 + \alpha_1 \lambda + \alpha_0$ , which is easy to compute. Moreover,  $2\alpha_3 = \text{tr}(w'_0) = 0$ , seen by the fact  $(p_1(\lambda))^2$  is the characteristic polynomial of  $w'_0$ , implying  $\alpha_3 = 0$ . Thus, setting  $w_1 = (w^3 + \alpha_2 w + \alpha_1)$ , we have  $w'_0 w_1 = -\alpha_0$ .

Clearly, this is a huge improvement over the use of the determinant, since  $\alpha_0$  is  $\text{Pf}(w'_0)$ , a polynomial of degree 4 in the  $\mu_{ij}$ . (Using the determinant, one had a polynomial of degree 8 in the  $\mu_{ij}$ .) Using this notation, we need to check  $r = (-\alpha_0 x'_0 + w'_0 x'_0 w_1)^2$  has degree 2. Note that  $r$  is a polynomial of degree 2 in the  $\xi_i$  and

degree 8 in the  $\mu_{ij}$ , and is homogeneous in  $\xi$  and in  $\mu$ . Thus  $(r - (1/8)\text{tr}(r))^2 = r^2 - (1/4)r\text{tr}(r) + ((1/8)\text{tr}(r))^2$  is a polynomial of degree 4 in the  $\xi_i$  and degree 16 in the  $\mu_{ij}$ , which is still rather large for the computer. Since  $((1/8)\text{tr}(r))^2$  is scalar, it suffices to check that  $r^2 - (1/4)r\text{tr}(r)$  is scalar.

Another simplification is possible, when we write out  $r = \alpha_0^2(x'_0)^2 - \alpha_0x'_0w'_0x'_0w_1 - \alpha_0w'_0x'_0w_1x'_0 + w'_0x'_0w_1w'_0x'_0w_1$ ; since  $w_1w'_0 = w'_0w_1 = -\alpha_0$ , we have  $r = \alpha_0^2(x'_0)^2 - \alpha_0x'_0w'_0x'_0w_1 - \alpha_0w'_0x'_0w_1x'_0 - \alpha_0w'_0(x'_0)^2w_1$ , so we can replace  $r$  by  $r_1 = r\alpha_0^{-1} = \alpha_0(x'_0)^2 - x'_0w'_0x'_0w_1 - w'_0x'_0w_1x'_0 - w'_0(x'_0)^2w_1$ . Now  $r_1$  has degree 2 in the  $\xi_i$  and degree 4 in the  $\mu_{ij}$ . Also  $\text{tr}(r_1) = 2\alpha_0\text{tr}(x_0'^2) - 2\text{tr}(x_0'w_0'x_0'w_1)$ , which is very easy to compute.

Now let  $b = r_1^2 - (1/4)r_1\text{tr}(r_1)$ . The question arose as to how many of the 64 entries of the matrix  $b$  must be checked before we can conclude that  $b$  is scalar. Let  $b = \sum_{i,j=1}^8 b_{ij}e_{ij}$ . Arguing by symmetry, it is easy to see that if  $b_{12} = 0$  then  $b_{ij} = 0$  for each  $i, j$ , such that  $(i - j)$  is not a multiple of 4.

Similarly, if  $b_{11} - b_{22} = 0$ , then  $b_{ii} - b_{jj} = 0$  if  $(i - j)$  is not a multiple of 4, implying  $b_{11} = b_{22} = b_{33} = b_{44} = b_{55} = b_{66} = b_{77} = b_{88}$  (by iteration). Thus, if  $b_{11} = b_{22}$  and  $b_{12} = 0$ , we conclude  $b$  has the form

$$b_{11} \sum_{i=1}^8 e_{ii} + \sum_{i=1}^4 b_{i,i+4} e_{i,i+4} + \sum_{i=1}^4 b_{i+4,i} e_{i+4,i}.$$

**Reduction 4.** Theorem 1 is true if and only if, in the above notation,  $b_{11} = b_{22}$  and  $b_{12} = 0$ .

Indeed, all we need to show is that  $b_{i,i+4} = b_{i+4,i} = 0$  for all  $i, 1 \leq i \leq 4$ . So assume  $b_{11} = b_{22}$ ,  $b_{12} = 0$ , and some  $b_{i,i\pm 4} \neq 0$ . We may as well assume  $b_{51} \neq 0$ , by symmetry. Let  $d = (\sum_{i=1}^8 e_{ii}) + e_{15}$ . Then  $d^s = d^{-1}$  so, letting  $x''_0 = dx'_0d^s$  and  $w''_0 = dw'_0d^s$ , we see that  $\text{tr}(x''_0) = 0$ ,  $(x''_0)^s = x''_0$ ,  $(w''_0)^s = w''_0$ ,  $x''_0$  is diagonal, and, for each  $i$  between 1 and 4, the coefficients in  $w''_0$  of  $e_{ii}$ ,  $e_{i,i+4}$ ,  $e_{i+4,i}$ , and  $e_{i+4,i+4}$  are 0. Thus, we have a special case of the set-up of Reduction 4; letting  $r'_1 = x''_0 + w''_0x''_0(w''_0)^{-1}$  and  $b' = r'_1 - (1/4)r'_1\text{tr}(r'_1)$ , and writing  $b' = \sum b'_{ij}e_{ij}$ , we have  $b'_{ij} = 0$  if  $i$  and  $j$  are not congruent modulo 4, and also  $b'_{11} = b'_{22} = \dots = b'_{88}$ . On the other hand,  $b' = dbd^s = b + e_{15}b - be_{15} - e_{15}be_{15} = b + (b_{51}e_{11} + b_{55}e_{15}) - (b_{51}e_{55} + b_{11}e_{15}) - b_{51}e_{15} = b + b_{51}e_{11} - b_{51}e_{55} - b_{51}e_{15}$  (since  $b_{11} = b_{55}$ ) so  $b_{11} + b_{51} = b'_{11} = b'_{55} = b_{55} - b_{51} = b_{11} - b_{51}$ ; we conclude  $b_{51} = 0$ , contrary to assumption. Thus, all the  $b_{i,i\pm 4}$  are 0, verifying Reduction 4.

Thus, in the notation of Reduction 4, we need to show the terms  $(b_{11} - b_{12})$  and  $b_{12}$  are 0. Viewing  $b_{11} - b_{12}$  and  $b_{12}$  as polynomials in  $\xi_1, \xi_2$ , and  $\xi_3$  of total degree 4 (with coefficients in  $F[\mu]$ ), we calculated each coefficient of  $\xi_1^u \xi_2^v \xi_3^{4-u-v}$  separately, in order to save computer memory. (Clearly, if each coefficient is 0, then the whole polynomial is 0.) Since  $0 \leq u \leq 4$  and  $0 \leq v \leq 4 - u$  in each monomial, the number of coefficients is  $5 + 4 + 3 + 2 + 1 = 15$ .

Even with these reductions, calculating the 15 coefficients individually, the program (written in FORMAC) used 820 K-bytes of memory (and ran for approximately 30 minutes under VS), on the IBM 370/168 computer at the Bar-Ilan

University computer center. This concludes the proof of Theorem 1.

Incidentally, the four reductions used in the proof of Theorem 1, as well as Lemma 5, are valid in much more general computations. Also, in retrospect, we see why the involution(s) on  $8 \times 8$  matrices was preferable to the transpose; every symmetric element has degree  $\leq 4$ .

Bar-Ilan University  
Ramat-Gan, Israel

1. A. A. ALBERT, *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ., vol. 24, Amer. Math. Soc., Providence, R. I., 1961.
2. N. JACOBSON, *Lectures in Abstract Algebra II—Linear Algebra*, Van Nostrand, Princeton, N. J., 1953.
3. T. MUIR, *A Treatise on the Theory of Determinants*, Dover, New York, 1960.
4. L. H. ROWEN, "Identities in algebras," *Israel J. Math.*, v. 20, 1975, pp. 70–95.
5. L. H. ROWEN, "Central simple algebras," *Israel J. Math.*, 1978.