A Constructive Elementary Proof of the Skolem–Noether Theorem for Matrix Algebras

Jenő Szigeti and Leon van Wyk

Abstract. We give a constructive elementary proof for the fact that any K-automorphism of the full $n \times n$ matrix algebra over a field K is conjugation by some invertible $n \times n$ matrix over K.

The theorem stating that any two embeddings of an extension of a field K into a finite-dimensional central simple algebra over K are conjugate was first published by Skolem in 1927 (see [**5**]). This theorem was rediscovered by Noether in 1933 (see [**2**]). The Skolem–Noether theorem is now considered to be a fundamental result in the theory of central simple algebras, linear groups, and representation theory. See, for example, [**1**] and [**3**].

A short constructive proof of the following form of the Skolem–Noether theorem for matrix algebras can be found in [**4**].

Theorem 1. *Any K-automorphism $\varphi : \mathrm{M}_{n\times n}(K) \longrightarrow \mathrm{M}_{n\times n}(K)$ of the full $n \times n$ matrix algebra over a field K is conjugation by some invertible matrix $A \in \mathrm{M}_{n\times n}(K)$, i.e., $\varphi(X) = AXA^{-1}$ for all $X \in \mathrm{M}_{n\times n}(K)$.*

Although there are many alternative proofs of the Skolem–Noether theorem in the literature, they are generally not constructive. The value of the present note is that it provides an elementary proof of the theorem above, which is entirely constructive and gives the matrix A explicitly, using the φ-images of only two matrices (irrespective of the value of n), a nonzero vector in a certain kernel, and matrix multiplication. The proof in [**4**] is different from ours and requires the images of n matrices.

Our procedure comprises the following standard operations.

(1) For $1 \leq i, j \leq n$, let $E_{i,j}$ denote the matrix in $\mathrm{M}_{n\times n}(K)$ having 1 in the (i, j) position and zeros in all other positions, and let $S = E_{1,2} + E_{2,3} + \cdots + E_{n-1,n}$. In other words,

$$E_{n,1} = \begin{bmatrix} 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix} \text{ and } S = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{bmatrix}.$$

(2) Let $H = \varphi(E_{n,1})$ and $G = \varphi(S)$, and let $\mathbf{a}$ be a nonzero column vector in the kernel of $I_n - G^{n-1}H = I_n - \varphi(E_{1,1})$, where I_n is the $n \times n$ identity matrix.

http://dx.doi.org/10.4169/amer.math.monthly.124.10.966
MSC: Primary 15A18, Secondary 16S50; 16W20

(3) Take the matrix

$$A = \left[G^{n-1}H\mathbf{a} \mid G^{n-2}H\mathbf{a} \mid \cdots \mid GH\mathbf{a} \mid H\mathbf{a}\right]$$

with column vectors $G^{n-i}H\mathbf{a}$, $1 \le i \le n$.

Proof. Observe that

$$I_n - \varphi(E_{1,1}) = \varphi(I_n - E_{1,1}) = \varphi(E_{2,2} + E_{3,3} + \cdots + E_{n,n})$$

is not invertible, otherwise $E_{2,2} + E_{3,3} + \cdots + E_{n,n}$ would also be invertible. Since $\det(I_n - \varphi(E_{1,1})) = 0$, there exists an $\mathbf{a} \in \mathrm{M}_{n\times 1}(K)$, $\mathbf{a} \neq \mathbf{0}$, such that $(I_n - \varphi(E_{1,1}))\mathbf{a} = \mathbf{0}$. Clearly, $S^{n-1} = E_{1,n}$ and $S^{n-1}E_{n,1} = E_{1,1}$ give that $G^{n-1}H = \varphi(E_{1,1})$ and $G^{n-1}H\mathbf{a} = \mathbf{a}$. Notice that $S^i E_{j,1} = E_{j-i,1}$ for $1 \le i < j \le n$, and so $S^n = E_{n,1}S^{n-2}E_{n,1} = \cdots = E_{n,1}SE_{n,1} = E_{n,1}^2 = 0$ implies $G^n = HG^{n-2}H = \cdots = HGH = H^2 = 0$.

We claim that $AE_{n,1} = HA$ and $AS = GA$, where

$$A = \left[G^{n-1}H\mathbf{a} \mid G^{n-2}H\mathbf{a} \mid \cdots \mid GH\mathbf{a} \mid H\mathbf{a}\right]$$

is the matrix in $\mathrm{M}_{n\times n}(K)$ with column vectors $G^{n-i}H\mathbf{a}$, $1 \le i \le n$. Since

$$AE_{n,1} = [H\mathbf{a} \mid \mathbf{0} \mid \cdots \mid \mathbf{0} \mid \mathbf{0}]$$

and

$$HA = \left[HG^{n-1}H\mathbf{a} \mid HG^{n-2}H\mathbf{a} \mid \cdots \mid HGH\mathbf{a} \mid H^2\mathbf{a}\right],$$

the fact that $G^{n-1}H\mathbf{a} = \mathbf{a}$ and $HG^{n-2}H = \cdots = HGH = H^2 = 0$ gives that $AE_{n,1} = HA$. Since

$$AS = AE_{1,2} + AE_{2,3} + \cdots + AE_{n-1,n} = \left[\mathbf{0} \mid G^{n-1}H\mathbf{a} \mid \cdots \mid G^2H\mathbf{a} \mid GH\mathbf{a}\right]$$

and

$$GA = \left[G^nH\mathbf{a} \mid G^{n-1}H\mathbf{a} \mid \cdots \mid G^2H\mathbf{a} \mid GH\mathbf{a}\right],$$

the fact that $G^n = 0$ gives that $AS = GA$. To prove that A is invertible, take a zero linear combination of the column vectors of A:

$$\lambda_{n-1}G^{n-1}H\mathbf{a} + \lambda_{n-2}G^{n-2}H\mathbf{a} + \cdots + \lambda_1 GH\mathbf{a} + \lambda_0 H\mathbf{a} = \mathbf{0}.$$

In view of $G^{n-1}H\mathbf{a} = \mathbf{a} \neq \mathbf{0}$ and $G^n = 0$, left multiplication by G^{n-1} gives that $\lambda_0\mathbf{a} = \lambda_0 G^{n-1}H\mathbf{a} = \mathbf{0}$, whence $\lambda_0 = 0$ follows. Then left multiplication by G^{n-2} gives $\lambda_1\mathbf{a} = \lambda_1 G^{n-1}H\mathbf{a} = \mathbf{0}$, whence $\lambda_1 = 0$ follows. Repeating the left multiplications, we obtain that $\lambda_0 = \lambda_1 = \cdots = \lambda_{n-1} = 0$. Thus, the columns of A are linearly independent, whence the invertibility of A follows.

Now $AE_{n,1} = HA$ and $AS = GA$ imply that $AE_{n,1}A^{-1} = \varphi(E_{n,1})$ and $ASA^{-1} = \varphi(S)$. Since $E_{i,j} = S^{n-i}E_{n,1}S^{j-1}$ for all $1 \le i, j \le n$, the matrices $E_{n,1}$ and S generate $\mathrm{M}_{n\times n}(K)$ as a K-algebra, and so $AXA^{-1} = \varphi(X)$ for all $X \in \mathrm{M}_{n\times n}(K)$. ■

Although this proof does not directly translate to the more general case, the theorem immediately implies the statement for central simple algebras by invoking Hilbert's theorem 90. That is how the Skolem–Noether theorem is proved in [**1**]; however, [**1**] gives a nonconstructive proof of the theorem about matrices.

The advantage of our proof is that it may help to characterize the automorphisms of certain two-generator algebras, where the generators satisfy some of the relations satisfied by our two simple generating matrices. Put more precisely, our methods may help to determine the K-automorphisms of the quotient of the two-generated free associative (polynomial) algebra $K\langle x, y\rangle/N$, where the ideal N is generated by the monomials $x^n, yx^{n-2}y, \ldots, yxy, y^2$ (perhaps under some additional conditions).

ACKNOWLEDGMENTS. The first author was partially supported by the National Research, Development, and Innovation Office of Hungary (NKFIH) K119934. The second author was supported by the National Research Foundation of South Africa under Grant No. UID 72375. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors, and therefore the National Research Foundation does not accept any liability in regard thereto. The authors wish to thank the referees for their helpful comments.

REFERENCES

1. P. Gille, T. Szamuely, *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics 101. Cambridge Univ. Press, Cambridge, 2006.
2. E. Noether, Nichtkommutative Algebra, *Math. Z.* **37** (1933) 514–541.
3. L. H. Rowen, *Ring Theory, Vol. II*. Academic Press, New York, 1988.
4. P. Semrl, Maps on matrix spaces, *Linear Algebra Appl.* **413** (2006) 364–393.
5. T. Skolem, Zur Theorie der assoziativen Zahlensysteme, *Skrifter Oslo* **12** (1927) 50.

Institute of Mathematics, University of Miskolc, Miskolc, Hungary 3515
jeno.szigeti@uni-miskolc.hu

Department of Mathematical Sciences, Stellenbosch University, P/Bag X1, Matieland 7602, Stellenbosch, South Africa
LvW@sun.ac.za