



THEOREM OF THE DAY

The Skolem-Noether Theorem Let R, S be finite dimensional algebras, R simple and S central simple. If $f, g : R \rightarrow S$ are homomorphisms then there is an element $s \in S$ such that, for all $r \in R$, $g(r) = s^{-1}f(r)s$.

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 1 | 1 | 0 | 3 | 2 | 7 | D | C | 4 | E | B | F | 9 | 6 | 5 | 8 | A |
| 2 | 2 | 3 | 0 | 1 | A | 9 | E | F | C | 5 | 4 | D | 8 | B | 6 | 7 |
| 3 | 3 | 2 | 1 | 0 | F | B | 8 | A | 6 | D | 7 | 5 | E | 9 | C | 4 |
| 4 | 4 | 7 | A | F | 0 | 6 | 5 | 1 | B | E | 2 | 8 | D | C | 9 | 3 |
| 5 | 5 | D | 9 | B | 6 | 0 | 4 | C | F | 2 | E | 3 | 7 | 1 | A | 8 |
| 6 | 6 | C | E | 8 | 5 | 4 | 0 | D | 3 | A | 9 | F | 1 | 7 | 2 | B |
| 7 | 7 | 4 | F | A | 1 | C | D | 0 | 9 | 8 | 3 | E | 5 | 6 | B | 2 |
| 8 | 8 | E | C | 6 | B | F | 3 | 9 | 0 | 7 | D | 4 | 2 | A | 1 | 5 |
| 9 | 9 | B | 5 | D | E | 2 | A | 8 | 7 | 0 | 6 | 1 | F | 3 | 4 | C |
| A | A | F | 4 | 7 | 2 | E | 9 | 3 | D | 6 | 0 | C | B | 8 | 5 | 1 |
| B | B | 9 | D | 5 | 8 | 3 | F | E | 4 | 1 | C | 0 | A | 2 | 7 | 6 |
| C | C | 6 | 8 | E | D | 7 | 1 | 5 | 2 | F | B | A | 0 | 4 | 3 | 9 |
| D | D | 5 | B | 9 | C | 1 | 7 | 6 | A | 3 | 8 | 2 | 4 | 0 | F | E |
| E | E | 8 | 6 | C | 9 | A | 2 | B | 1 | 4 | 5 | 7 | 3 | F | 0 | D |
| F | F | A | 7 | 4 | 3 | 8 | B | 2 | 5 | C | 1 | 6 | 9 | E | D | 0 |

The matrix ring $M_2(\mathbb{F}_2)$

| × | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 2 | 2 | 3 | 1 | 6 | 4 | 5 | E | D | F | 8 | 7 | 9 | A | B | C |
| 3 | 3 | 1 | 2 | 5 | 6 | 4 | B | A | C | D | E | F | 8 | 7 | 9 |
| 4 | 4 | 5 | 6 | 1 | 2 | 3 | 7 | 8 | 9 | D | E | F | A | B | C |
| 5 | 5 | 6 | 4 | 3 | 1 | 2 | B | A | C | 8 | 7 | 9 | D | E | F |
| 6 | 6 | 4 | 5 | 2 | 3 | 1 | E | D | F | A | B | C | 8 | 7 | 9 |
| 7 | 7 | 9 | 8 | 7 | 9 | 8 | 0 | 0 | 0 | 8 | 7 | 9 | 8 | 7 | 9 |
| 8 | 8 | 7 | 9 | 9 | 8 | 7 | 7 | 8 | 9 | 8 | 7 | 9 | 0 | 0 | 0 |
| 9 | 9 | 8 | 7 | 8 | 7 | 9 | 7 | 8 | 9 | 0 | 0 | 0 | 8 | 7 | 9 |
| A | A | B | C | C | A | B | B | A | C | A | B | C | 0 | 0 | 0 |
| B | B | C | A | B | C | A | 0 | 0 | 0 | A | B | C | A | B | C |
| C | C | A | B | A | B | C | B | A | C | 0 | 0 | 0 | A | B | C |
| D | D | E | F | F | D | E | E | D | F | D | E | F | 0 | 0 | 0 |
| E | E | F | D | E | F | D | 0 | 0 | 0 | D | E | F | D | E | F |
| F | F | D | E | D | E | F | E | D | F | 0 | 0 | 0 | D | E | F |

$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ $3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

$4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $5 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ $6 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$7 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ $8 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ $9 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$

$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ $C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$D = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ $E = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ $F = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

Algebras here are assumed to be associative, with identity, over the same field K ; they are *simple* if no non-trivial subspace remains closed under multiplication by the algebra (no non-empty, proper subspace X satisfies $aX = Xa = X$, for all elements a); and *central* if only scalar multiples of the identity commute with everything. The prototypical finite dimensional central simple algebra is the ring of $n \times n$ matrices over a division ring. In the example shown here, n is 2, and the division ring is the finite field \mathbb{F}_2 of integers mod 2. We can see the power of Skolem-Noether in the corollary that any automorphism of $M_n(\mathbb{F}_2)$ (that is any permutation of its elements which respects addition and multiplication) must be a so-called *inner* automorphism, of the form $x \mapsto s^{-1}xs$, for some invertible matrix $s \in M_n(\mathbb{F}_2)$. Only the matrices numbered 1 to 6, above right, are invertible; so of the $16!$ permutations of $M_n(\mathbb{F}_2)$, only 6 are automorphisms. E.g., suppose permutation p transposes the matrices E and F while fixing all other elements. Then, say, $p(F.8) = p(D) = D$ but $p(F).p(8) = E.8 = 0$. So p is one of the 2092 27898 87994 unlucky ones.

This theorem was first published in 1927 by Thoralf Skolem, best remembered for his work in mathematical logic. Emmy Noether rediscovered it in 1933 and it is perhaps due to her recognition of its significance in the architecture of modern algebra that it is sometimes known as the first fundamental theorem of the theory of division algebras.

Web link: www.math.virginia.edu/~ww9c/divalgebras.pdf.

Further reading: *Advanced Algebra* by Anthony W. Knap, Birkhauser Boston, 2007, chapter 2.

