Simple Algebras, Skolem–Noether, ...

October 29, 2010

Throughout this section let A be a central simple algebra of finite dimension over a field k. We identify k with the center of A.

Lemma 1. *Let $b_1, b_2, \ldots, b_n$ be a k–basis of A. For each k–linear map $\phi : A \to A$ there are unique $a_1, a_2, \ldots, a_n \in A$ such that $\phi(x) = \sum_i a_i x b_i$ for all $x \in A$.*

Proof. Let $\psi : A^n \to \operatorname{End}_k(A)$ be the k–linear map which sends $(a_1, a_2, \ldots, a_n)$ to the map $x \mapsto \sum_i a_i x b_i$. Since $\dim A^n = n^2 = \dim \operatorname{End}_k(A)$, we are done once we know that ψ is injective.

Thus suppose that ψ is not injective. Pick a nonzero n-tuple in the kernel for which the number of nonzero entries is minimal. Upon renumbering the b_i's, we may assume that $\phi(x) = \sum_{i=1}^m a_i x b_i = 0$ for all $x \in A$, and m is minimal in such a relation.

In particular, $a_m \neq 0$. Now $A = A a_m A$ by simplicity of A, hence $\sum_j u_j a_m v_j = 1$ for certain $u_j, v_j \in A$. Summing $0 = u_j \phi(v_j x)$ over j gives

$$0 = \sum_j \sum_{i=1}^m u_j a_i v_j x b_i = x b_m + \sum_{i=1}^{m-1} c_i x b_i =: \rho(x) \tag{1}$$

where

$$c_i = \sum_j u_j a_i v_j.$$

Since ρ vanishes on A, we have $\rho(yx) - y\rho(x) = 0$ for any $x, y \in A$. This yields

$$\sum_{i=1}^{m-1} (c_i y - y c_i) x b_i = 0$$

for all $x, y \in A$. The minimality of m yields $c_i y = y c_i$ for all i and $y \in A$, hence $c_i \in k$. Setting $x = 1$ in (1) gives

$$b_m + \sum_{i=1}^{m-1} c_i b_i = 0,$$

contrary to the assumption that the $b_i's$ are linearly independent over k. $\square$

Theorem 2 (Skolem–Noether)**.** *Let $x \mapsto \phi(x)$ be a k–algebra automorphism of A. Then there is a unit $a \in A$ such that $\phi(x) = axa^{-1}$ for all $x \in A$.*

Proof. Write $\phi(x) = \sum_i a_i x b_i$ according to the lemma. For $x, y \in A$ we get

$$\sum_i (a_i y) x b_i = \phi(yx) = \phi(y)\phi(x) = \sum_i (\phi(y) a_i) x b_i.$$

Since this holds for any fixed y, the uniqueness statement in the lemma gives

$$\phi(y) a_i = a_i y$$

for all i and $y \in A$.

Clearly, there is an index i such that $a_i \neq 0$. Since $A = Aa_iA$ and ϕ is surjective, there are u_j, v_j such that

$$\sum_j \phi(u_j) a_i v_j = 1.$$

But $\phi(u_j)a_i = a_i u_j$, hence $1 = a_i \sum_j u_j v_j$, so a_i is a unit and we are done. $\square$