Journal of Pure and Applied Algebra 35 (1985) 321-328
North-Holland

AN EXTENSION OF THE NOETHER-SKOLEM THEOREM

Florian POP and Horia POP
Department of Mathematics, Increst, Bdul Pacii 220, 79622 Bucharest, Rumania

Communicated by C.J. Mulvey
Received 29 April 1983

The classical theorem of Noether and Skolem asserts that any K-isomorphism between two simple K-subalgebras of a central simple algebra R can be extended to an inner automorphism of R (see [2], [5], [8]).

The main result of this paper is to prove the following extension of the above theorem: if A is a semisimple k-algebra over a field and B is a separable k-algebra (not necessarily central over k), then the number of orbits under the action of the group of all inner automorphisms of B on $\mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ is finite (Theorems 2 and 3).

A similar result is true for separable algebras over a henselian local ring (Theorem 4).

The result arises in connection with a question of one of the authors concerning the structure of certain artinian rings [12].

The simplest case (which suggested the general results) concerns the k-embeddings of a finite extension K of k in $M_n(K)$ (Theorem 1).

Results

We assume throughout this paper that all rings have identity elements, all subrings contain the identity of the ring, all ring homomorphisms carry identity to identity and all algebras are finite-dimensional.

The simplest case, which we consider first, is the following:

Theorem 1. *Let $k \subset K$ be a finite separable field extension. Then the number of classes of k-algebra homomorphisms $\phi : K \to M_n(K)$, with respect to conjugation under an inner automorphism of $M_n(K)$, is finite.*

Moreover if $k \subset K$ is a Galois extension, then any k-algebra homomorphism is conjugate to a diagonal mapping $x \mapsto \mathrm{diag}(\sigma_1(x), \sigma_2(x), \dots, \sigma_n(x))$ where $\sigma_i \in \mathrm{Gal}(K/k)$.

Proof. Observe first that if $K = k(\theta)$, then $\phi(\theta)$ determines the k-algebra homomorphism ϕ. What remains to be done is an exercise in linear algebra. Remark that for similar ϕ's, $\phi(\theta)$ has the same rational (Frobenius) canonical form which is built up from companion matrices of the invariant factors of $\phi(\theta)$. Since they are divisors of the irreducible polynomial of θ over k, the rational form of $\phi(\theta)$ may have only a finite number of values. If K is a Galois extension of k, then the minimal polynomial of θ over k splits as a product of distinct linear factors over K, hence (see [7, Ch. 11, Theorem 4]) $\phi(\theta)$ is diagonalisable. $\square$

Now let A be a semisimple k-algebra, B a separable k-algebra with center K and $f: A \to B$ a k-algebra homomorphism. Then denote by $B(f) = f(A) \cdot K$. With any $f \in \mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ we can associate $F \in \mathrm{Hom}_{\mathrm{Alg}(K)}(A \otimes_k K, B(f))$ defined by $F(a \otimes b) = f(a)b$.

One can see that the mapping $f \mapsto F$ from $\mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ to $\mathrm{Hom}_{\mathrm{Alg}(K)}(A \otimes_k K, B)$ is one-to-one and onto, hence a bijection. By a simple verification we have also:

Lemma 1. *The correspondence $f \mapsto F$ defined above is compatible with the action of the group G of all inner automorphism of B. Moreover $Gf_1 = Gf_2$ iff $GF_1 = GF_2$.*

Theorem 2. *Let A be a semisimple algebra over a field k and B a simple separable algebra over k. Then the number of orbits of* $\mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ *under the action of the group of all inner automorphisms of B is finite.*

Proof. Denote by K the center of B. As K/k is a separable extension $A \otimes_k K$ is semisimple so we can write

$$A \otimes_k K = T_1 \oplus \cdots \oplus T_t$$

with each T_i a simple K-algebra and we have also

$$F(A \otimes_k K) = S_1 \oplus \cdots \oplus S_s, \quad s \leq t$$

with $S_i \simeq T_i$ as K-algebras for the T_i numbered properly.

Denote by $e_1, \ldots, e_s$ the identity elements of $S_1, \ldots, S_s$; it follows that they are orthogonal idempotents of B and $e_1 + \cdots + e_s = 1_B$. Any such idempotent e_i can be written as a sum of orthogonal idempotents of S_i and any such an idempotent is a sum of primitive (minimal) orthogonal idempotents of B, $e_i = \sum_{j \in I_i} f_j$, $i = 1, \ldots, s$ and $I = \bigcup_{i=1}^{s} I_i$. For any regular $u \in B$ we shall denote by i_u the inner automorphism associated to u by $i_u(x) = uxu^{-1}$.

Fix now a maximal set of orthogonal primitive idempotents $\{e_1^0, \ldots, e_n^0\}$ of B; by the uniqueness part of Wedderburn's Theorem [1, Ch. IV, Theorem 1] expressing B in two ways as a matrix algebra over $\{e_1^0, \ldots, e_n^0\}$ or over $\{f_j\}_{j \in I}$ there is a regular element $u \in B$ such that the two sets of primitive idempotents are conjugated under u. Then $i_u(f_j) = e_{k(j)}^0$, so that $\bar{e}_i = i_u(e_i) = \sum_{j \in I_i} e_{k(j)}^0$.

Hence we can associate to F (and also to f) a partition $P(f) = \{I_i\}$ of $\{1, \ldots, n\}$ in s subsets.

The image of i_uF will be $\bigoplus_{i=1}^{s} i_u(S_i)$ where $\bar{e}_i = i_u(e_i)$ are central idempotents of B and $i_u(S_i)$ are K-simple subalgebras of $\bar{e}_iB\bar{e}_i$.

Now let $F_1, F_2 \in \mathrm{Hom}_{\mathrm{Alg}(K)}(A \otimes_k K, B)$ corresponding to $f_1, f_2 \in \mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ have the following properties:

(a) $F_1(A \otimes_k K)$ and $F_2(A \otimes_k K)$ have the same simple components

$$F_1(A \otimes_k K) = \bigoplus_{i=1}^{s} S_i, \qquad F_2(A \otimes_k K) = \bigoplus_{i=1}^{s} S_i'$$

with $S_i \simeq S_i' \simeq T_i$ and identities of S_i respectively S_i', e_i respectively e_i'.

(b) The partitions $P(f_1), P(f_2)$ defined by $\{\bar{e}_i\}$ and $\{\bar{e}_i'\}$ for the fixed $\{e_i^0\}$ are the same. That means there are some regular $u_1, u_2 \in B$ such that

$$i_{u_1}(e_i) = i_{u_2}(e_i') = \sum_{j \in I_i} e_{k(j)}^0.$$

We can now apply the Noether–Skolem Theorem to the isomorphic K-subalgebras $i_{u_1}(S_i) \simeq i_{u_2}(S_i')$ included in the central simple K-algebra $\bar{e}_iB\bar{e}_i$, hence there exists some regular elements $w_i \in \bar{e}_iB\bar{e}_i$ with $i_{w_i}i_{u_1}F_1|_{T_i} = i_{u_2}F_2|_{T_i}$.

If $w = \sum_{i=1}^{s} w_i$, we have $i_w i_{u_1}F_1 = i_{u_2}F_2$, so F_1 and F_2 are in the same orbit and by Lemma 1 so are f_1 and f_2.

Note that the number of nonisomorphic homomorphic images of $A \otimes_k K$ is bounded by the number of ideals of $A \otimes_k K$ and hence is finite. Also the number of partitions of $\{1, \dots, n\}$ into s subsets is finite. Hence the number of orbits of $\mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ under the action of the group of all inner automorphisms of B is finite. □

Remark 1. One can estimate an upper bound for the number of orbits. Let n be the cardinal of a maximal set of primitive orthogonal idempotents of B, let s be the number of simple components of A and t the number of simple components of $A \otimes_k K$. Denote by $N(r, n)$ the number of partitions of $\{1, \dots, n\}$ in exactly r subsets.

It is clear that $t \leq [K : k] \cdot s$.

For a fixed partition of $\{1, \dots, n\}$ in $r \leq t$ subsets the t central idempotents of $A \otimes_k K$ can be mapped in at most $t!/(t-r)!$ ways to the r idempotents of B defined by the partition, so an upper bound is

$$\sum_{r=0}^{t} \frac{t!}{(t-r)!} N(r, n).$$

It means that there is a bound which depends only on n, s and $[K : k]$.

Theorem 3. *Let A be a semisimple algebra over a field k and B be a separable algebra over k. Then the number of orbits of* $\mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ *under the action of the group G of all inner automorphisms of B is finite.*

Proof. One may write $B = B_1 \oplus \cdots \oplus B_m$ with each B_i a simple separable algebra over k and any $f \in \mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$, may be written as a sum $f = f_1 + \cdots + f_m$ where $f_i \in \mathrm{Hom}_{\mathrm{Alg}(k)}(A, B_i)$.

By Theorem 2 it follows that the number of orbits of $\mathrm{Hom}_{\mathrm{Alg}(k)}(A, B_i)$ under the action of the group G_i of inner automorphism of B_i is finite. Thus $\mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ will have a finite number of orbits relatively to the action of $G = G_1 \times \cdots \times G_n$ the group of all inner automorphisms of B. □

Remark 2. It follows by Remark 1 that the number of orbits is bouned by a constant depending only on $\dim_k A$ and $\dim_k B$.

We shall consider now the same problem for separable algebras over a henselian local ring. The conditions demanded are those necessary in order for the Noether–Skolem theorem to work (see [6], [9], [11] and [14]) and to be able to handle idempotents in the center. We need the following preliminary results:

Lemma 2. *If $R \subset S \subset A$ are rings with S separable over R and commutative and A finitely generated and projective over R, then S is finitely generated and projective over R. If in addition R is semilocal, then S is semilocal.*

Proof. See [6, Lemma]. □

Noether–Skolem Theorem (for separable algebras over semilocal rings). *Let R be a semilocal ring, let B be separable finitely generated projective R-algebra with center K, let A be a separable R-subalgebra of B with connected center C containing K and let σ be an R-algebra monomorphism of A into B leaving K fixed, then σ can be extended to an inner automorphism of B.*

Proof. See [6, Theorem 1.2]. □

Theorem 4. *Let B be a projective separable algebra over a henselian local ring k with center K and let A be a projective separable algebra over k with center C. Then the number of orbits of* $\mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ *under the action of the group G of all inner automorphisms of B is finite.*

Proof. Denote by $\mathfrak{p}$ the unique maximal ideal of k and let $\bar{k} = k/\mathfrak{p}$. For any k-algebra homomorphism $f: A \to B$ define a K-algebra homomorphism $F: A \otimes_k K \to B$ by $F(a \otimes b) = f(a) \cdot b$. Then $F(A \otimes_k K) = f(A) \cdot K$ is a K-subalgebra of B. We shall prove that for a splitting of $A \otimes_k K$ in a direct sum of separable algebras over some connected local rings containing K, some of the components may vanish under the action of F while the restriction of F to the others will be an isomorphism; the Noether–Skolem theorem above can then be used in the same manner as in Theorem 2.

By a result of Villamayor and Zelinsky (see [3, Ch. 2, Proposition 2.1]) both A and B are finitely generated as k-modules, hence notherian. It follows that K and C are also finitely generated over k, which is henselian. Hence both K and C we have decomposition as product of henselian local rings.

If $K=K_1\oplus\cdots\oplus K_m$ we have a decomposition $B=B_1\oplus\cdots\oplus B_m$ given by the orthogonal idempotents of K and for $f:A\to B$ we can consider $f_i:A\to B_i$ such that $f=f_1+\cdots+f_m$. It will be sufficient to prove that the number of orbits for each f_i is finite, so we can suppose that the center K of B is a henselian local ring and B is a primary ring (see also [4, Theorem 27]).

From the decomposition of $C=C_1\oplus\cdots\oplus C_m$ in a sum of henselian local rings we can express $A=A_1\oplus\cdots\oplus A_m$ each A_i being a separable k-algebra with center C_i. Then as A_i is separable over k and projective, A_i is separable over C_i and C_i separable over k (see [3, Theorem 2.3]) and by Lemma 2, C_i is projective over the local ring k hence free.

Now as C_i is separable over k, $C_i/\mathfrak{p}C_i$ is a separable algebra over $\bar{k}=k/\mathfrak{p}$ (cf. [9, Ch. 2, Theorem 7.1]), hence semisimple, so that $\mathfrak{p}C_i$ is the Jacobson radical of the local ring C_i.

It follows that $\mathfrak{p}C_i$ is the unique maximal ideal of C_i or in the terminology of Azumaya [4], C_i is unramified over k. Using Lemma 5 and Theorem 28 of [4] it follows that

$$C_i=k[\alpha_i]=k[X]/(P_i(X))$$

where $P_i(X)$ is a monic polynomial whose image $\bar{P}_i(X)$ in $\bar{k}[X]$ is irrreducible and

$$\bar{C}_i=C_i/\mathfrak{p}C_i=\bar{k}[\bar{\alpha}_i].$$

We have $C_i\otimes_k K=\bigoplus_j K_{ij}$, $K\subset K_{ij}$ because

$$\begin{aligned} C_i\otimes_k K&=k[X]/(P_i(X))\otimes_k K=K[X]/(P_i(X))\\ &=\bigoplus_j K[X]/(P_{ij}(X))=\bigoplus_j K_{ij} \end{aligned}$$

where $P_{ij}(X)$ are the factors corresponding to a decomposition into irreducible factors of the image $\bar{P}_i(X)$ of $P_i(X)$ in $\bar{K}[X]$, $\bar{K}=K/\mathfrak{p}K$.

Notice that the separability implies that there are no repeated factors and the factors can be lifted to $K[X]$ as K is henselian.

So we have $K_{ij}=K[X]/(P_{ij}(X))=K[\alpha_{ij}]$ and each K_{ij} is a local (hence connected) henselian ring containing K.

As C_i and K are separable over k, $C_i\otimes K$ and each K_{ij} are k separable.

We can now write:

$$\begin{aligned} A\otimes_k K&=\left(\bigoplus_{i=1}^n A_i\right)\otimes_k K=\bigoplus_{i=1}^n (A_i\otimes_k K)=\bigoplus_{i=1}^n (A_i\otimes_{C_i} C_i)\otimes_k K\\ &=\bigoplus_{i=1}^n (A_i\otimes_{C_i}(C_i\otimes_k K))=\bigoplus_i\left(A_i\otimes_{C_i}\left(\bigoplus_j K_{ij}\right)\right) \end{aligned}$$

$$= \bigoplus_{(i,j)\in I} (A_i \otimes_{C_i} K_{ij}) = \bigoplus_{(i,j)\in I} A_{ij}$$

with each $A_{ij} = A_i \otimes_{C_i} K_{ij}$ a separable central K_{ij}-algebra, because $A \otimes_k K$ is separable central over $C \otimes_k K$ by Proposition 1.5 of [3] and then use Proposition 1.13 in Ch. 2 of [9].

In order to show that the restriction of F to A_{ij} (which is Azumaya algebra over K_{ij}) is zero or a monomorphism, it is sufficient to show that the restriction of F to K_{ij} is zero or one-to-one (because the ideals of A_{ij} and K_{ij} are in bijective correspondence by extensions and restriction, Corollary 3.2 of [3]).

Suppose now that $F|_{K_{ij}} \neq 0$; remember that F is a K-algebra homomorphism and notice that both $K_{ij} = K[\alpha_{ij}] = K[X]/(P_{ij}(X))$ and $F(K_{ij})$ are separable k-algebras (use Proposition 1.4 of [3]). Then by Lemma 2, K_{ij} and $F(K_{ij})$ are projective, hence free over k. Both K_{ij} and $F(K_{ij})$ are henselian local rings and separability implies (as we already proved for C_i over k) that they are unramified over k. As our rings are unramifed and free over k and have isomorphic residue fields, we can use again Lemma 5 of [4] to deduce that if $F(K_{ij})$ is not 0, then K_{ij} and $F(K_{ij})$ are isomorphic.

It follows that $F(A \otimes_k K) = \bigoplus_{(i,j)\in L} A'_{ij}$, $L \subset I$ with A'_{ij} K-isomorphic to A_{ij}, hence A'_{ij} are K-separable with connected center K_{ij} containing K. Denoting by e_{ij} the identity element of A_{ij} one has $\sum_{(i,j)\in L} e_{ij} = 1_B$.

Now using well known results on idempotents (see [4, Theorems 24 and 25]) there exists a system of orthogonal idempotents of $B, \{e_1^0, \dots, e_n^0\}$ (which comes from a system of orthogonal idempotents of the simple k-algebra $B/\mathfrak{p}B$) such that conjugates of e_{ij} by a regular element $u \in B$ are sums of e_{ij}^0's.

Denoting by i_u the inner automorphism $i_u(x) = uxu^{-1}$ we have

$$\bar{e}_{ij} = i_u(e_{ij}) = \sum_{i \in L_{ij}} e_i^0.$$

It follows that f defines a partition $\{L_{ij}\}$ of $\{1, \dots, n\}$.

Suppose now that for two homomorphisms $f_1, f_2 \in \mathrm{Hom}_{\mathrm{Alg}(k)}(A, B)$ we have:

(a) The same components in the decomposition of $F_1(A \otimes_k K)$ and $F_2(A \otimes_k K)$ vanish; that is:

$$F_1(A \otimes_k K) = \bigoplus_{(i,j)\in L} A'_{ij}, \qquad F_2(A \otimes_k K) = \bigoplus_{(i,j)\in L} A''_{ij}$$

where $A'_{ij} = F_1(A_{ij}) \simeq A''_{ij} = F_2(A_{ij})$ as K-algebras.

(b) The corresponding idempotents $\{e'_{ij}\}, \{e''_{ij}\}$ give the same partition of $\{1, \dots, n\}$ that is there are regular elements $u_1, u_2 \in B$ such that $i_{u_1}(e'_{ij}) = i_{u_2}(e''_{ij}) = \bar{e}_{ij}$.

Then $i_{u_1}F_1(A_{ij}), i_{u_2}F_2(A_{ij})$ are isomorphic K-subalgebras of $\bar{e}_{ij}B\bar{e}_{ij}$, so we can use the Noether–Skolem theorem for separable algebras over local rings to find regular elements $w_{ij} \in \bar{e}_{ij}B\bar{e}_{ij}$ such that $i_{w_{ij}} i_{u_1} F_1|_{A_{ij}} = i_{u_2} F_2|_{A_{ij}}$.

Then for $w = \sum w_{ij}$ one has $i_w i_{u_1} F_1 = i_{u_2} F_2$, so F_1 and F_2 are in the same orbit and so are f_1 and f_2 under the action of the group of all inner automorphisms of B.

But there are a finite number of choices for vanishing components in (a) and for partitions of $\{1, \dots, n\}$ in (b), hence the number of orbits is finite. $\square$

In a forthcoming paper [12] as applications of the above results we shall determine the structure of some classes of artinian rings. For these applications the following results will be useful.

Theorem 5. *Let A be a semisimple k-algebra such that each component of the center of A is a Galois extension of k.*

If $f: A \to M_m(A)$ is a k-algebra homomorphism, then f is conjugate under an inner automorphism of $M_m(A)$ to a diagonal mapping $\mathrm{diag}(g_1, \ldots, g_m)$, *each g_i being a k-endomorphism of A.*

Proof. Since A is a direct product of simple rings if is enough to prove the theorem for a simple ring $A = M_m(D)$ where D is a division algebra. Now, if $\{e_{ij} \mid 1 \le i, j \le n\}$ is a system of matrix units in A, then $\{f(e_{ij})\}_{i,j}$ is a system of matrix units and $f(D)$ is included in the centralizer of $\{f(e_{ij})\}$ which is isomorphic to $M_m(D)$, by an inner conjugation of $M_m(A)$. Therefore, the problem can be reduced to the case when A is a division algebra D.

Since K is a Galois extension of k, we have decompositions

$$K \otimes_k K = \bigoplus_{\sigma \in \mathrm{Gal}(K/k)} e_\sigma K \quad \text{and} \quad D \otimes_k K = \bigoplus_{\sigma \in \mathrm{Gal}(K/k)} (D \otimes e_\sigma K)$$

given by the orthogonal idempotents $\{e_\sigma\}_{\sigma \in \mathrm{Gal}(K/k)}$. Denoting $\bar{e}_\sigma = f(e_\sigma)$, if $\{e_{ij}^0\}$ is a system of matrix units in $M_m(D)$, then we can find as in the proof of Theorem 2 an inner conjugation i_u such that $i_u(\bar{e}_\sigma) = \sum_{i \in I_\sigma} e_{ii}^0$. Hence, $i_u f$ is a diagonal mapping. □

Notice that if A is a simple algebra, each g_i is a k-automorphism of A.

Let p be a prime number, A a separable k-algebra over a field k of characteristic p and $W_n(k)$ the truncated p-adic ring of residue field k. We shall denote by $W_n(A)$ the unique separable $W_n(k)$-algebra of characteristic p^n and residual algebra modulo its Jacobson radical $J(W_n(A)) = pW_n(A)$ equal to A (see [4, Theorem 32] and [13, Theorem 1]). Denote also $W_\infty(A) = \varprojlim W_n(A)$.

Theorem 6. *Let A be a separable k-algebra such that each component of the center of A is a Galois extension of k.*

If $f: W_n(A) \to M_m(W_n(A))$ is a $W_n(k)$-algebra homomorphism, ($n \in \mathbb{N}$ or $n = \infty$), then f is conjugate under an inner automorphism of $M_m(W_n(A))$ to a diagonal mapping $\mathrm{diag}(g_1, \ldots, g_m)$, *where each g_i is a $W_n(k)$ endomorphism of $W_n(A)$.*

The proof is similar to that of Theorem 5.

References

[1] A.A. Albert, Structure of Algebras, Amer. Math. Soc. Colloq. Publ. 24 (1939).

[2] E. Artin, C. Nesbitt and R. Thrall, Rings with minimum condition, Univ. of Michigan (1944).

[3] M. Auslander and O. Goldman, The Brauer group of a commutative ring, Trans. Amer. Math. Soc. 97 (1960) 367–409.
[4] G. Azumaya, On maximally central algebras, Nagoya Math. J. 2 (1951) 119–150.
[5] N. Bourbaki, Algèbre, Ch. 8 (Hermann, Paris, 1958).
[6] L.N. Childs and F.R. DeMeyer, On automorphisms of separable algebras, Pacific J. Math. 23 (1967) 25–34.
[7] P.M. Cohn, Algebra (Wiley, New York, 1974).
[8] M. Deuring, Algebren, Ergeb. Math. 4 (Springer, Berlin, 1935).
[9] F. DeMeyer and E. Ingraham, Separable algebras over commutative rings, Lecture Notes in Math. 181 (Springer, Berlin, 1971).
[10] N. Jacobson, Basic Algebra I (Freeman, San Francisco, 1974).
[11] M.A. Knus and M. Ojanguren, Théorie de la descente et algèbres d'Azumaya, Lecture Notes in Math. 389 (Springer, Berlin, 1974).
[12] H.C. Pop, On the structure of artinian rings, to apear.
[13] H.C. Pop, Noncommutative p-adic rings and Witt vectors in connection with a theorem of Azumaya, Preprint Increst 32/1983.
[14] A. Roy and R. Shridharan, Derivations in Azumaya algebras, J. Math. Kyoto Univ. 7 (1967) 161–167.