ISRAEL JOURNAL OF MATHEMATICS **96** (1996), 15–22

FINITE-DIMENSIONAL SUBALGEBRAS OF DIVISION RINGS

BY

S. A. AMITSUR AND D. BAUM

Institutė of Mathematics, The Hebrew University of Jerusalem
Jerusalem 91904, Israel
e-mail: dalbaum@math.huji.ac.il

ABSTRACT

For any division ring D and any two simple Artinian algebras finite dimensional over $F = \text{Center}(D)$ we characterize the minimal size of an F-extension of D that contains commuting images of these algebras. In particular we show that if D contains subalgebras of coprime dimensions n and m then they have commuting conjugates in D, and D contains a subalgebra of dimension nm.

1. Introduction

Throughout this paper, D will denote an arbitrary division ring, and F its center. All rings are F-algebras, all embeddings and isomorphisms are over F.

The study of algebraic elements in division rings goes back to Wedderburn [6], who proved that every irreducible polynomial in $F[x]$ which has a root $a \in D$, splits to linear factors over D, all of the form $x - a'$, for a' conjugates of a in D. Hence, any two algebraic elements of D are conjugate if and only if they have the same minimal polynomial over F. Jacobson [3] used a module-theoretic approach to improve Wedderburn's method. His results include a theory of algebraic matrices over D, and the same approach will be used here.

In this paper, we characterize the minimal extension of D which contains an image of a given finite-dimensional simple algebra A (Lemma 4), using the same

Received June 1, 1995 and in revised form March 25, 1996

lemma used by Schofield [5, Chapter 9] in his analysis of finite-dimensional subalgebras in coproducts of division rings. Then we go on to characterize the minimal extension of D that contains commuting (elementwise) images of two given finite-dimensional F-algebras A and B (Theorem 6). In particular, if A and B are subalgebras of D, of coprime dimensions n and m over F, then they are shown to have commuting conjugates in D itself (Theorem 5) and thus D contains a subalgebra of dimension nm. In section 4, we apply the results from the first two sections to find the minimal extension of D which contains a root for a given irreducible polynomial over F (Proposition 9). Finally (Corollary 11) we take two irreducible polynomials over F and explicitly find all commuting pairs of roots in finite extensions of D.

Historical Note: This paper represents an attempt to formalize and generalize an idea presented by the late Prof. Amitsur prior to his untimely death. The second author hopes this might serve as a fitting tribute to his memory.

2. The canonical embedding

Throughout this section, we look for the minimal size of matrices over D that contain a homomorphic image of a given simple finite-dimensional F-algebra A. Our main tool is the following lemma, noted by Schofield in [5, Lemma 9.1]; we repeat the proof for the reader's convenience.

SCHOFIELD'S LEMMA: *If A is a simple ring, finite dimensional over F, and if $D \otimes_F A^\circ$ has a simple module M which is of dimension ν over D, then for all t,*

$$A \text{ is embeddable in } M_t(D) \iff \nu \mid t.$$

Proof: Note that $D \otimes_F A^\circ$ is simple Artinian and so all its modules are isomorphic to direct sums of copies of M. By hypothesis M is isomorphic to $D^{(\nu)}$ over D. Hence:

$$\begin{gathered} A \hookrightarrow M_t(D) \iff A^\circ \hookrightarrow M_t(D^\circ) \cong \operatorname{End}_D D^{(t)} \iff \\ D^{(t)} \text{ is a left } D \otimes_F A^\circ\text{-module} \iff \nu \mid t. \qquad \blacksquare \end{gathered}$$

The following are straightforward consequences:

LEMMA 1: *If A is embeddable into R, for R any D-ring such that $[R : D]_r = t$, then $\nu \mid t$.*

Proof: Because $R \cong \operatorname{End} R_R \hookrightarrow \operatorname{End} R_D \cong M_t(D)$. $\blacksquare$

LEMMA 2: *If A is embeddable in $M_n(D)$ and in $M_m(D)$, then it is embeddable in $M_{\gcd(n,m)}(D)$.*

Denote the dimension of A over F by n, the dimension of the simple $D\otimes_F A^\circ$-module over D by $\nu = (A \mid D)$, an image of A inside $M_\nu(D)$ by $\overline{A}$ (it is unique up to conjugacy), and the centralizer of $\overline{A}$ in $M_\nu(D)$ by D_A (again, it is unique up to conjugacy in $M_\nu(D)$).

LEMMA 3: *(Using the above notations)*

(i) *$\nu \mid n$, $D\otimes_F A^\circ \cong M_{\frac{n}{\nu}}(D_A)$ and D_A is a division ring.*

(ii) *If A has an isomorphic image $\widetilde{A}$ in $M_t(D)$, then $M_t(D)\otimes_F A^\circ \cong M_n(C_{M_t(D)}(\widetilde{A}))$, for $C_{M_t(D)}(\widetilde{A})$ the centralizer of $\widetilde{A}$ in $M_t(D)$. Furthermore, $C_{M_t(D)}(\widetilde{A})$ is a division ring if and only if $t=\nu$, $\widetilde{A}$ is conjugate to $\overline{A}$, and $C_{M_t(D)}(\widetilde{A})$ is conjugate to D_A.*

Proof: Assume that A has an isomorphic image $\widetilde{A}$ in $M_t(D)$. Since $[\widetilde{A}:F]=n$ (as in [1, p. 42]) $\widetilde{A}$ can be imbedded in $M_n(F)$ by the left regular representation, and its centralizer there is isomorphic to $(\widetilde{A})^\circ$. So we can calculate the centralizer of $F\otimes_F \widetilde{A} \cong \widetilde{A}\otimes_F F$ inside $M_t(D)\otimes_F M_n(F)$ and get $M_t(D)\otimes_F A^\circ \cong M_n(C_{M_t(D)}(\widetilde{A}))$.

Now $A \hookrightarrow M_n(F) \subseteq M_n(D)$, hence $\nu \mid n$. So take $t=\nu$ in the last isomorphism to get $M_\nu(D\otimes_F A^\circ) \cong M_\nu(M_{\frac{n}{\nu}}(D_A))$ which implies $D\otimes_F A^\circ \cong M_{\frac{n}{\nu}}(D_A)$. The underlying division ring of $D\otimes_F A^\circ$, by the density theorem, is $\operatorname{End}_{D\otimes_F A^\circ} D^{(\nu)} \subseteq \operatorname{End}_D D^{(\nu)}$; this division ring consists of all endomorphisms over D of our simple module $D^{(\nu)}$ that commute with the right multiplication by elements of $\overline{A}$. Using the right regular representation, $\operatorname{End}_D D^{(\nu)} \cong M_\nu(D)$, and our division ring is $C_{M_\nu(D)}(\overline{A}) = D_A$. This completes the proof of (i).

Since $\nu \mid t$,

$$M_n(M_{\frac{t}{\nu}}(D_A)) = M_{t\frac{n}{\nu}}(D_A) \cong M_t(D\otimes_F A^\circ) \cong M_t(D)\otimes_F A^\circ \cong M_n(C_{M_t(D)}(\widetilde{A}))$$

hence $C_{M_t(D)}(\widetilde{A}) \cong M_{\frac{t}{\nu}}(D_A)$ cannot be a division ring unless $t=\nu$, and then $\widetilde{A}$ and $\overline{A}$ are finite-dimensional subalgebras of $M_\nu(D)$, isomorphic over F, and therefore conjugate. ∎

Furthemore, when A is not necessarily a simple algebra, we can still use Schofield's lemma to find the minimal size of matrices over D which contain a homomorphic image of A:

LEMMA 4: *If A is a finite-dimensional algebra over F, and t is the minimal integer such that $M_t(D)$ contains a homomorphic image of A, then that image must be simple.*

Proof: Denote a homomorphic image of A in $M_t(D)$ by $\overline{A}$. By the minimality of t, $D^{(t)}$ is a simple module over $D\otimes_F \overline{A}^{\circ}$. $D^{(t)}$ is also a faithful module since no element of $\overline{A}^{\circ} \hookrightarrow M_t(D)^{\circ}$ annihilates $D^{(t)}$. Finally, $D\otimes_F \overline{A}^{\circ}$ is primitive Artinian hence a simple Artinian ring, which implies that $\overline{A}$ is a simple ring. ∎

3. Commuting subalgebras

Using only Lemma 2 we can deduce:

THEOREM 5: *If A and B are two finite-dimensional subalgebras of D, of coprime dimensions n and m (resp.) over F, then A has a conjugate in the centralizer of B in D.*

Proof: If we denote the center of A by K and the center of B by L, the center of $A\otimes_F B$ is $K\otimes_F L$ which is a field, because K and L are of coprime dimensions over F. Since every ideal of $A\otimes_F B$ must meet $K\otimes_F L$, $A\otimes_F B$ is a simple ring. It is of dimension nm over F. Moreover, $A\hookrightarrow M_n(F)$ and so $A\otimes_F B\hookrightarrow M_n(F)\otimes_F B\cong M_n(B)\hookrightarrow M_n(D)$. In the same manner, $A\otimes_F B\hookrightarrow M_m(D)$. Now we use Lemma 2 to deduce that $A\otimes_F B$ is embeddable in D itself. Using Skolem–Noether, this means that a conjugate of A commutes elementwise with a conjugate of B. ∎

In order to generalize this theorem, we take any two simple Artinian algebras A and B, finite dimensional over F, and try to find the minimal size of matrices over D which contain images of A and of B which commute elementwise. It is easy to see that containing such commuting images is the same as containing a homomorphic image of $A\otimes_F B$ (since all embeddings are over F). In fact, it suffices to look for simple images of $A\otimes_F B$ due to Lemma 4.

Notations:

- Denote the center of A by K, and the center of B by L.
- Note that $A\otimes_F B\cong A\otimes_K (K\otimes_F L)\otimes_L B$ and that any simple image of $A\otimes_F B$ is of the form $A\otimes_K E\otimes_L B$ for E a field image of $K\otimes_F L$. Choose one simple image and denote it by S.

- Further denote $[A:F]=n$, $[B:F]=m$, $(A\mid D)=\nu$, $(B\mid D)=\mu$, $[S:B]=[E\otimes_K A:L]=n'$, $[S:A]=[E\otimes_L B:K]=m'$.
- $(E\otimes_L B\mid D_A)$ (and symmetrically $(E\otimes_K A\mid D_B)$) is well defined since $E\otimes_L B$ is simple Artinian, it is of dimension m' over K, and K is the center of the division ring $C_{M_\nu(D)}(\overline{A})=D_A$ according to the double centralizer theorem. So denote $(E\otimes_L B\mid D_A)=\mu'$ and $(E\otimes_K A\mid D_B)=\nu'$.

Recall that by Lemma 3: $\nu\mid n$, $\mu\mid m$, $\nu'\mid n'$, $\mu'\mid m'$. Clearly $[S:F]=n\cdot m'=m\cdot n'$. We get the analog of this equality over D:

THEOREM 6: *(Using the above notations) For any simple image S of $A\otimes_F B$, and E its center,*

$$(S\mid D)=(A\mid D)\cdot(E\otimes_L B\mid D_A)=(B\mid D)\cdot(E\otimes_K A\mid D_B).$$

Proof: Use Lemma 3 twice:

$$\begin{aligned} D\otimes_F(S)^\circ &\cong (D\otimes_F A^\circ)\otimes_K(E\otimes_L B)^\circ\cong M_{\frac{n}{\nu}}\left(D_A\otimes_K(E\otimes_L B)^\circ\right)\\ &\cong M_{\frac{n}{\nu}\cdot\frac{m'}{\mu'}}\left((D_A)_{E\otimes B}\right)=M_{\frac{n}{\nu}\cdot\frac{m'}{\mu'}}\left(C_{M_{\nu\mu'}(D)}(\overline{A},\overline{B})\right)\end{aligned}$$

since $(D_A)_{E\otimes B}=C_{M_{\mu'}(D_A)}(\overline{E\otimes_L B})=C_{M_{\nu\mu'}(D)}(\overline{A},\overline{B})$ is a division ring and $[S:F]=n\cdot m'$, $(S\mid D)=\nu\cdot\mu'$. We can reverse the order and adjoin B before A, and thus get that $\frac{n}{\nu}\cdot\frac{m'}{\mu'}=\frac{m}{\mu}\cdot\frac{n'}{\nu'}\Longrightarrow\nu\cdot\mu'=\mu\cdot\nu'$, which is the required equality. ∎

COROLLARY 7: *If A and B are subalgebras of D, and S is any simple image of $A\otimes_F B$, then $(S\mid D)$ divides both $n'=[S:A]$ and $m'=[S:B]$.*

Remark 8: Other facts that might come handy when trying to evaluate $(S\mid D)$:

1. When K/F is a Galois extension, so is E/L and $E=K\otimes_{K\cap L}L$. Then $[E:L]$ divides $[K:F]$, which translates to $n'\mid n$ (because $n'=[S:B]=[A:K][E:L]$ divides $[A:K][K:L]=n$).
2. $A\otimes_F B$ is simple $\iff S=A\otimes_F B\iff K\otimes_F L$ is a field (K and L are F-linearly disjoint) $\iff n'=n\iff m'=m$. (For example, when one of the subalgebras is central, or if $[K:F]$ and $[L:F]$ are coprime, which covers the case of Theorem 5.)
3. If both K/F and L/F are Galois, or if K and L are F-linearly disjoint, then $(S\mid D)$ divides both $\gcd(n,m)\cdot\operatorname{lcm}(\nu,\mu)$ and $\gcd(n,m)\cdot\operatorname{lcm}(\nu',\mu')$.

4. Looking for roots

In this section, we apply the former results to simple algebraic field extensions of F, to characterize roots of irreducible polynomials over F, in finite extensions of D.

If $f(x) \in F[x]$ is an irreducible polynomial of degree n, and if $f(x) = f_k(x)\cdots f_1(x)$ for $f_i(x) \in D[x]$ irreducible over D, then the decomposition is not unique, but the degrees of all irreducible factors are equal [3, p. 45]. If we take $A = F[x]/\langle f(x)\rangle$, an n-dimensional simple extension of F, then $\deg f_i(x) = \nu = (A \mid D)$.

Jacobson proves this fact by taking the maximal ideal $D[x]f(x) \lhd D[x]$ and noting that it is contained in each maximal left ideal $D[x]f_i(x)$ ($\forall i = 1,\ldots,k$):

$$(f_k(x)\cdots f_i(x))f(x) = f(x)(f_k(x)\cdots f_i(x))$$
$$\Longrightarrow f(x) = f_{i-1}(x)\cdots f_1(x)\cdot f_k(x)\cdots f_i(x).$$

Therefore, the simple Artinian ring $D \otimes_F A^\circ = D \otimes_F F[x]/\langle f(x)\rangle \cong D[x]/D[x]f(x)$ has the simple module $D[x]/D[x]f_i(x)$ for all $i = 1,\ldots,k$. All such modules are isomorphic and, in particular, of the same left dimension ν over D. Hence $\deg f_i(x) = \nu$ for all i, and $n = \nu\cdot k$. Now we apply Lemma 3:

PROPOSITION 9: *Write $f_1(x) = x^\nu - d_{\nu-1}x^{\nu-1} - \cdots - d_0$, and denote*

$$\overline{a} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & & & 0 & 1 \\ d_0 & d_1 & \ldots & & d_{\nu-1} \end{pmatrix} \quad \textit{inside } M_\nu(D).$$

Then:

(i) *$\overline{a}$ is a root of $f(x)$ in $M_\nu(D)$.*

(ii) *([4, Prop. 3.8(ii)]) $f(x)$ has a root $a \in R = M_t(D)$ if and only if $\nu \mid t$ and a is conjugate to a diagonal block matrix* $\mathrm{diag}(\overline{a},\ldots,\overline{a})$. *[In particular, all roots of $f(x)$ in $M_t(D)$ are conjugate.]*

(iii) $D[x]/D[x]f(x) \cong M_{\frac{n}{\nu}}\left(C_{M_\nu(D)}(\overline{a})\right)$.

(iv) *For $a \in R$ as in* (ii), $\mathrm{End}_{R[x]} R[x]/R[x](x-a) \cong C_R(a)$ *and, in addition, $R[x](x-a)$ is a maximal ideal of $R[x]$ if and only if $C_R(a)$ is a division ring, if and only if $\nu = t$ and a is conjugate to $\overline{a}$.*

Proof: (i) The matrix $\overline{a}$ is the matrix associated with right multiplication by x, on the simple module $D[x]/D[x]f_i(x)$, with respect to the canonical basis

$\{\overline{1}, \overline{x}, \ldots, \overline{x}^{\nu-1}\}$. Since right multiplication by $f(x)$ is obviously zero, $\overline{a}$ is a root of $f(x)$.

(ii) In [4, Prop. 3.7] Rowen gives a canonical form for all algebraic elements in $R = M_t(D)$, not necessarily those with irreducible minimal polynomials over F as in our case.

Identifying with $a \in M_t(D)$ a linear transformation $T(v) = va$ of the module $D^{(t)}$ over D, define on $D^{(t)}$ a structure of a $D[x]/\,D[x]f(x)$ module by $x{\cdot}v = T(v)$. So if we choose the basis $\{\overline{1}, \overline{x}, \ldots, \overline{x}^{\nu-1}\}$ for each copy of the simple module $D^{(\nu)}$ in $D^{(t)}$, T corresponds to the matrix $\operatorname{diag}(\overline{a}, \ldots, \overline{a})$.

(iii) This is just Lemma 3(ii) for $A = F[x]/\langle f(x)\rangle \cong F(\overline{a})$.

(iv) Again, use Lemma 3(ii). The isomorphism $\operatorname{End}_{R[x]} R[x]/\,R[x]\,(x-a) \cong C_R(a)$ is obtained by sending each endomorphism φ to $\varphi(\overline{1}) = c_\varphi \in R$ and noting that for every $h(x) \in R[x]$, $\varphi\left(\overline{h(x)}\right) = \varphi\left(h\,(x)\,\overline{1}\right) = \overline{h\,(x)\,c_\varphi}$. In particular, for $h(x) = x - a$, $\overline{0} = \varphi\left(\overline{x-a}\right) = \overline{(x-a)\,c_\varphi}$, hence $(x-a)\,c_\varphi = s\cdot(x-a) \Longrightarrow s = c_\varphi \in C_R\,(a)$. ∎

The previous proposition deals with roots of polynomials in f.d. extensions of D, i.e. monic factors of degree one over such extensions. A slightly more general approach yields:

PROPOSITION 10: *Let $f(x)$ be an irreducible polynomial over F, $f_1(x)$ one of its irreducible factors over D, of degree ν. If $f_1(x)$ has a monic right factor $\varphi\,(x) \in M_t(D)[x]$ of degree l (or if $f_1(x)$ has a monic right factor of degree l in any D-ring of right dimension t over D), then $\nu \mid l\cdot t$.*

Furthermore, $\varphi(x)$ generates a maximal left ideal in $M_t(D)[x]$ if and only if $\nu = l\cdot t$.

Proof: Just take $M_t(D)[x]/\,M_t(D)[x]\varphi(x)$ as a left module over

$$M_t(D)[x]/ < f(x) > \cong M_t\left(D[x]/ < f(x) >\right).$$

This module is of degree $l\cdot t^2$ over D. Using Morita equivalence, the simple module over $M_t(D)[x]/ < f(x) >$ is of degree $\nu\cdot t$ over D. Hence $\nu \mid l\cdot t$, and that module is simple if and only if $\nu = l\cdot t$. ∎

Finally, we take two irreducible polynomials over F: $f(x)$ and $g(y)$ of degrees n and m (resp.), and we look for all pairs of roots (a, b) in finite extensions over D, such that a is a root of $f(x)$ and b is a root of $g(y)$ and they **commute**.

Fix I any maximal ideal containing $\langle f(x), g(y)\rangle$ in $F[x,y]$. Then in our case $S = E = F[x,y]/I = F(a,b)$ for $a = x+I$ and $b = y+I$. Write $I = \langle f(x), \varphi(x,y)\rangle = \langle g(y), \psi(x,y)\rangle$, so $\varphi(a,y)$ is an irreducible factor of $g(y)$ over $F(a)$ of degree m', and $\psi(x,b)$ is an irreducible factor of $f(x)$ over $F(b)$ of degree n'. Of course any choice of I corresponds to another choice of irreducible factors and to another choice of S.

The degree of all irreducible factors of $f(x)$ (resp. $g(y)$) over D is ν (resp. μ), and the degree of all irreducible factors of $\varphi(a,y)$ (resp. $\psi(x,b)$) over $D_{F(a)}$ (resp. $D_{F(b)}$) is μ' (resp. ν'). Denote, as in Proposition 9, by $\overline{a} \in M_\nu(D)$ the matrix associated to an irreducible factor of $f(x)$ over D, and by $\overline{b} \in M_{\nu\mu'}(D)$ the matrix associated to an irreducible factor of $\varphi(\overline{a},y)$ over $D_{F(\overline{a})}$. (We do not distinguish between a matrix $c \in M_k(S)$ and its image $\operatorname{diag}(c,\ldots,c) \in M_{kl}(S)$.) Now Theorem 6 together with Proposition 9 give:

COROLLARY 11: *$M_t(D)$ contains a root of $f(x)$ and a root of $g(y)$ which commute if and only if $\nu\mu' = \mu\nu'$ divides t (for one of the possible choices for I and hence for μ' and ν'). Moreover, $(\widetilde{a},\widetilde{b}) \in M_t(D)$ is such a commuting pair of roots if and only if $\left(\widetilde{a},\widetilde{b}\right) = \left(c\overline{a}c^{-1}, (cd)\overline{b}(cd)^{-1}\right)$ for some $c,d \in M_t(D)$, s.t. d commutes with $\overline{a}$.*

References

[1] P. K. Draxl, *Skew fields*, London Mathematical Society Lecture Note Series **81**, Cambridge University Press, 1983.

[2] D. Haile and L. H. Rowen, *Factorizations of polynomials over division algebras*, Algebra Colloquium **2** (1995), 145–156.

[3] N. Jacobson, *The Theory of Rings*, American Mathematical Society Surveys II, 1943.

[4] L. H. Rowen, *Wedderburn's method and algebraic elements of simple Artinian rings*, in *Azumaya Algebras, Actions and Modules in Honor of G. Azumaya* (D. Haile, ed.), Contemporary Mathematics **124** (1992), 179–202.

[5] A. H. Schofield, *Representations of rings over skew fields*, London Mathematical Society Lecture Note Series **92**, Cambridge University Press, 1985.

[6] J. H. M. Wedderburn, *On division algebras*, Transactions of the American Mathematical Society **22** (1921), 129–135.