Canad. Math. Bull. Vol. **104** (1), 1995 pp. 104–111

ON TRACES OF SEPARABLE SIMPLE SUBALGEBRAS IN MATRIX RINGS

Dedicated to Professor Kazuo Kishimoto on his 60th birthday

TAKASI NAGAHARA AND SEIYA YOKOTA

ABSTRACT. For the trace map on an irreducible semigroup of $n \times n$ matrices over a field, I. N. Herstein presented a theorem in [3] which enables us to limit the nature of matrix groups of a certain kind. However, this is incorrect in general. For the theorem, we shall present a counter example, a revision, and some generalizations to non-irreducible semigroups.

Throughout this note, F will mean a commutative field, $F^{(n)}$ an F-module which is a direct sum of n-copies of F, and F_n the ring of $n \times n$ matrices over F where n is any positive integer. We identify F_n with $\mathrm{Hom}_F(F^{(n)}, F^{(n)})$. For an F-subalgebra R of F_n, $F^{(n)}$ is said to be *irreducible* over R if $F^{(n)}$ is an irreducible R-module, that is, $F^{(n)} = vR$ for all $v \neq 0 \in F^{(n)}$. By $\chi(F)$, we denote the characteristic of F. For any $a \in F_n$, $\mathrm{t}_{F_n/F}(a)$ denotes the trace of a as a matrix. For a (multiplicative) sub-semigroup S of F_n, FS denotes the F-subalgebra of F_n generated by S over F, that is, $FS = \sum_{s \in S} Fs$. Moreover, for a simple ring T and its a subset E, we denote by $r(T)$ (resp. by $|E|$ (resp. by $V_T(E)$,)) the rank of T over its center (resp. the cardinality of E (resp. the set of elements a in T such that $ax = xa$ for all $x \in E$)).

In [3], I. N. Herstein presented the following theorem.

THEOREM A [3, THEOREM 2.3.3]. *Let S be a sub-semigroup of F_n such that $F^{(n)}$ is irreducible over FS, and $K = \{\mathrm{t}_{F_n/F}(s)\ ;\ s \in S\}$. Then $|S| \leq |K|^{n^2}$.*

He proved this theorem only in the case where F is algebraically closed. The proof is somewhat simpler than that of I. Kaplansky [7, p. 19, Theorem B]. However, in the other cases, this does not hold in general. In this note, we shall first present a counter example, and next, we shall prove that in Theorem A, the inequality $|S| \leq |K|^{n^2}$ holds if and only if FS is a separable F-algebra such that $r\big(V_{F_n}(FS)\big)$ is not a multiple of $\chi(F)$, and whence this theorem holds, provided that $\chi(F) = 0$ (Corollary 6 and Theorem 8). Moreover, this result will be generalized to a sub-semigroup S of F_n such that FS is a simple F-subalgebra of F_n containing F (Theorems 4, 5 and 7).

Received by the editors December 17, 1992; revised August 16, 1993.
AMS subject classification: Primary: 16H05; secondary: 16S50.
Key words and phrases: trace maps, separable algebras, matrix rings.

EXAMPLE 1. Let E be a field which is a purely inseparable simple extension of F of rank $n = p^m > 1$ where $\chi(F) = p > 0$. Let α be a generating element of E over F. Now, we consider a regular representation φ of E into $F_n = \mathrm{Hom}_F(F^{(n)}, F^{(n)})$ with respect to the F-basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of E. Then $S = \{\varphi(\alpha)^m \ ; \ m = 1, 2, \ldots\}$ is a sub-semigroup of F_n with $|S| \geq n > 1$. Clearly $FS = \varphi(E)$ which is an F-algebra isomorphic to E. Hence, for any $v \neq 0 \in F^{(n)}$, $v(FS)$ is an F-submodule of $F^{(n)}$ of rank n, which implies $v(FS) = F^{(n)}$. Therefore $F^{(n)}$ is irreducible over FS. We set $(a_{ij}) = \varphi(\alpha) \in F_n$. Then, since $\alpha^n \in F$, we have $a_{1n} = \alpha^n$, $a_{ii-1} = 1$ for $i = 2, \ldots, n$, and the other a_{ij}'s are zero. Hence $\mathrm{t}_{F_n/F}\left(\varphi(\alpha)^m\right) = 0$ for $m = 1, 2, \ldots$, that is, $\mathrm{t}_{F_n/F}(s) = 0$ for all $s \in S$. Therefore Theorem A does not hold. Next, we consider the algebraic closure $\bar{F}$ of F and $\varphi(E) = FS \subset F_n \subset \bar{F}_n$. Clearly $\bar{F}S$ is a commutative $\bar{F}$-subalgebra of $\bar{F}_n$. Hence $\bar{F}S \neq \bar{F}_n$. This implies that $\bar{F}^{(n)}$ is not irreducible over $\bar{F}S$. For example, if $F = \mathrm{GF}(2)(x)$ (the ring of rational functions of an indeterminate x over $\mathrm{GF}(2) = \{0, 1\}$) then, for $\alpha = (a_{ij}) \in F_2$ with $a_{11} = a_{22} = 0, a_{21} = 1$ and $a_{12} = x$, the set $S = \{\alpha^m \ ; \ m = 1, 2, \ldots\}$ is a sub-semigroup of F_2 such that FS is a subfield of F_2 which is a purely inseparable simple extension of F of rank 2. Hence $F^{(2)}$ is irreducible over FS and $|S| = \infty > 1 = |\{\mathrm{t}_{F_2/F}(s) \ ; \ s \in S\}|^4$.

Notations and Terminologies. In what follows, we shall use the following conventions: For a ring A and a right A-module M,

$l(M_A)$ = the length of composition series of right A-module M when M has such composition series,

$[M : A] = l(M_A)$ when A is a field,

$l(A) = l(A_A)$ when $l(A_A)$ is defined,

A_m = the ring of $m \times m$ matrices over A where m is any positive integer. For integers r, s,,

$r \mid s$ (resp. $r \nmid s$) means that r is (resp. is not) a divisor of s.

For a subset B of A and a map $f: A \longrightarrow C$ where C is a set,

$f|B$ = the restriction of f to B.

Now, let C be a commutative ring with the identity 1, A a C-algebra with identity which is finitely generated and projective over C. Then, there is a C-dual basis $\{x_1, \ldots, x_s\} \subset A \ ; \ \{f_1, \ldots, f_s\} \subset \mathrm{Hom}_C(A, C)$ such that $\sum_{i=1}^s x_i f_i(x) = x$ for all $x \in A$ (*cf.* [2, p. 4]). Define $\mathrm{T}_{A/C} \in \mathrm{Hom}_C(A, C)$ by

$$\mathrm{T}_{A/C}(x) = \sum_{i=1}^{s} f_i(xx_i), \quad x \in A.$$

If $\{y_1, \ldots, y_t\}$ is a system of generators for A over C and $x_k = \sum_{i=1}^t y_i c_{ik}$ $(k = 1, \ldots, s, c_{ik} \in C)$ then for $g_j = \sum_{k=1}^s c_{jk} f_k$, $\sum_{j=1}^t y_j g_j(x) = x$ and $\sum_{j=1}^t g_j(xy_j) = \sum_{i=1}^s f_i(xx_i)$ for all $x \in A$. For an other C-dual basis $\{y_1, \ldots, y_t\} \subset A \ ; \ \{h_1, \ldots, h_t\} \subset \mathrm{Hom}_C(A, C)$, we have $h_k = \sum_{j=1}^t h_k(y_j) g_j$ $(1 \leq k \leq t)$ and $\sum_{k=1}^t h_k(xy_k) = \sum_{k=1}^t \left(\sum_{j=1}^t h_k(y_j) g_j\right)(xy_k) = \sum_{j=1}^t g_j\left(x \sum_{k=1}^t h_k(y_j) y_k\right) = \sum_{j=1}^t g_j(xy_j)$. This shows that $\mathrm{T}_{A/C}$ is independent of the choice of a dual basis for A. We call $\mathrm{T}_{A/C}$ the *trace* from A to C. For any element $\alpha \in A_m$, we denote by $\mathrm{t}_{A_m/A}(\alpha)$ the sum of diagonal elements of α, and we write

https://doi.org/10.4153/CMB-1995-014-3 Published online by Cambridge University Press

$t_{A_m/C}(\alpha) = T_{A/C}\big(t_{A_m/A}(\alpha)\big)$. Clearly $t_{A_1/C}(\alpha) = T_{A/C}(\alpha)$ (for $m = 1$). The bilinear map $A_m \times A_m \longrightarrow C$ defined by $(x, y) \longmapsto t_{A_m/C}(xy)$ will be called *non-degenerate* if $t_{A_m/C}(A_m x) \neq \{0\}$ and $t_{A_m/C}(xA_m) \neq \{0\}$ for all $x \neq 0 \in A_m$. Further, A will be called *separable* over C if the left and right A-A-homomorphism $A \otimes_C A \longrightarrow A$ $(x \otimes y \longmapsto xy)$ splits. For a simple algebra R over a field F, R is separable over F if and only if R is a finitely generated F-module and the center of R is separable over F in the usual sense of field theory (*cf.* [2, p. 40 and p. 55, Theorem 2.3.8]).

REMARK 1. As in the preceding remarks, let A be a commutative C-algebra which is finitely generated and projective over C. Then, by [2, Theorem 3.2.1 and Corollary 3.2.2], A is separable over C if and only if the bilinear map $T_{A/C}(xy)$ $(x, y \in A)$ is non-degenerate. Hence, as is well known, for a field extension E/F, E is separable over F if and only if $T_{E/F} \neq 0$. Next, we refer to non-commutative separable algebras. Let F be a field with $\chi(F) = 2$. Then F_2 is a separable F-algebra, and $t_{F_2/F}(xy)$ $(x, y \in F_2)$ is non-degenerate. However, $T_{F_2/F}(xy)$ $(x, y \in F_2)$ is not non-degenerate. Indeed, if $d_1 = e_{11}$, $d_2 = e_{12}$, $d_3 = e_{21}$, $d_4 = e_{22}$ are the matrix units of F_2 then $\{d_i \,;\, 1 \leq i \leq 4\}$ is an F-basis for F_2, and the 4×4 matrix $(T_{F_2/F}(d_i d_j))$ is zero, as claimed, *cf.* [5, Theorem 5.3.2]. Thus, the assertion is holds. Hence, given a non-commutative separable C-algebra A, it doesn't always follow that $T_{A/C}(xy)$ $(x, y \in A)$ is non-degenerate.

Now, we shall start our study with the following

LEMMA 1. *Let D be a division F-algebra of finite rank, and m a positive integer. Then, the following conditions are equivalent.*

(a) D_m is separable over F and $\chi(F) \nmid r(D)$.

(b) $t_{D_m/F} \neq 0$.

(c) The bilinear map

$$D_m \times D_m \longrightarrow F \,;\, (x, y) \longmapsto t_{D_m/F}(xy)$$

is non-degenerate.

PROOF. Let B be the center of D, and M a maximal subfield. Then $D \otimes_B M \cong M_q$ where $q = \sqrt{[D : B]} = \sqrt{r(D)}$ (*cf.* [3, p. 96, Corollary]). Let $\{e_{ij} \,;\, 1 \leq i, j \leq q\}$ be the system of matrix units of M_q, and set $d_{q(i-1)+j} = e_{ij}$ $(1 \leq i, j \leq q)$. Then $\{d_k \,;\, 1 \leq k \leq q^2\}$ is a free B-basis for M_q. If $e_{uv} d_{q(i-1)+j} = d_{q(i-1)+j}$ then $e_{uv} e_{ij} = e_{ij}$ and so $u = v = i$ $(1 \leq j \leq q)$. This implies that $T_{M_q/M}(e_{uv}) = \delta_{uv} q1$ for all u, v, where δ_{uv} denotes the Kronecker's delta. Hence $T_{M_q/M}(e_{11}) = q1 \neq 0$ if and only if $T_{M_q/M} \neq 0$ which is equivalent to $T_{D/B} \neq 0$. Therefore, it follows that $T_{D/B} \neq 0$ if and only if $\chi(F) \nmid q$, equivalently $\chi(F) \nmid r(D)$. (a) $\Rightarrow$ (c): Clearly $t_{D_m/D}(xy)$ $(x, y \in D_m)$ is non-degenerate. Since $\chi(F) \nmid r(D)$, we have $T_{D/B} \neq 0$. Since D_m is separable over F, B is separable over F. Hence $T_{B/F} \neq 0$. Now, let a be a non-zero element of D_m. Then, there exists an element b in D_m such that $t_{D_m/D}(ab) \neq 0$. Clearly $t_{D_m/D}(abD) = t_{D_m/D}(ab)D = D$. This enables us to see that $t_{D_m/F}(abD) = T_{D/F} t_{D_m/D}(abD) = T_{B/F} T_{D/B} t_{D_m/D}(abD) = F$, and so $t_{D_m/F}(aD_m) = F$. Similarly, we have $t_{D_m/F}(D_m a) = F$. Therefore, it follows that $t_{D_m/F}(xy)$ $(x, y \in D_m)$ is non-degenerate. (c) $\Rightarrow$ (b): It is obvious. (b) $\Rightarrow$ (a): Let d be an element of D_m with

https://doi.org/10.4153/CMB-1995-014-3 Published online by Cambridge University Press

$t_{D_m/F}(d) \neq 0$. Then $t_{D_m/F}(d) = T_{B/F}T_{D/B}t_{D_m/D}(d) \neq 0$. Hence $T_{D/B} \neq 0$ and $T_{B/F} \neq 0$. Therefore $\chi(F) \nmid r(D)$ and B is separable over F. Therefore, D_m is separable over F.

LEMMA 2. *Let D be a division F-algebra with $s = [D : F]$, and m, l any positive integers. Then*

(i) There is an F-algebra isomorphism φ of D_m into F_{ms} with $\varphi(D_m) \supset F$. For any F-algebra isomorphism φ_1 of D_m into F_{ms} with $\varphi_1(D_m) \supset F$, $t_{D_m/F}(x) = t_{F_{ms}/F}\big(\varphi_1(x)\big)$ for all $x \in D_m$.

(ii) There is an F-algebra isomorphism ψ of D_m into F_{msl} with $\psi(D_m) \supset F$. For any F-algebra isomorphism ψ_1 of D_m into F_{msl} with $\psi_1(D_m) \supset F$, $lt_{D_m/F}(x) = t_{F_{msl}/F}\big(\psi_1(x)\big)$ for all $x \in D_m$.

(iii) Let σ be an F-algebra automorphism of $D_m = \sum_{i,j=1}^{m} e_{ij}D$ where $\{e_{ij} ; 1 \leq i,j \leq m\}$ is a system of matrix units of D_m and $D = V_{D_m}(\{e_{ij} ; 1 \leq i,j \leq m\})$. Then $t_{D_m/F}(x) = t_{D_m/F}\big(\sigma(x)\big) = t_{\sigma(D)_m/F}(x)$ for all $x \in D_m$ where $\sigma(D)_m = \sum_{i,j=1}^{m} \sigma(e_{ij})\sigma(D)$.

PROOF. Let ξ be a regular representation of the F-algebra D into F_s. We consider the map

$$\varphi: D_m \longrightarrow F_{ms} ; (a_{ij}) \longmapsto \big(\xi(a_{ij})\big) \quad (a_{ij} \in D).$$

Then φ is an F-algebra isomorphism such that $\varphi(D_m) \supset F$ and $t_{D_m/F}(x) = t_{F_{ms}/F}\big(\varphi(x)\big)$ for all $x \in D_m$. Let φ_1 be an arbitrary F-algebra isomorphism of D_m into F_{ms} with $\varphi_1(D_m) \supset F$. Then, by the theory of simple algebras (*cf.* [3, Theorem 4.3.1], [6] and [8]), there is a regular element u in F_{ms} such that $\varphi_1(x) = u\varphi(x)u^{-1}$ for all x in D. Hence $t_{D_m/F}(x) = t_{F_{ms}/F}\big(\varphi(x)\big) = t_{F_{ms}/F}\big(\varphi_1(x)\big)$ for all x in D_m. Next, we shall prove (ii). As is easily seen, there is an F-algebra isomorphism $\eta: F_{ms} \longrightarrow (F_{ms})_l = F_{msl}$ such that $\eta(F_{ms}) \supset F$ and $t_{F_{msl}/F}\big(\eta(y)\big) = lt_{F_{ms}/F}(y)$ for all $y \in F_{ms}$. By (i), there is an F-algebra isomorphism φ of D_m into F_{ms} with $\varphi(D_m) \supset F$. Then $\eta\varphi$ is an F-algebra isomorphism of D_m into F_{msl} such that $\eta\varphi(D_m) \supset F$. Moreover, for $x \in D_m$, $t_{F_{msl}/F}\big(\eta\varphi(x)\big) = lt_{F_{ms}/F}\big(\varphi(x)\big)$. Now, ψ_1 be an F-algebra isomorphism of D_m into F_{msl} such that $\psi_1(D_m) \supset F$. Then $\psi_1(D_m)$ is F-algebra isomorphic to $\eta\varphi(D_m)$. Hence there is a regular element u of F_{msl} such that $\psi_1(x) = u\eta\varphi(x)u^{-1}$ for all $x \in D_m$. Therefore, it follows that $t_{F_{msl}/F}\big(\psi_1(x)\big) = t_{F_{msl}/F}\big(\eta\varphi(x)\big) = lt_{F_{ms}/F}\big(\varphi(x)\big) = lt_{D_m/F}(x)$ for all $x \in D_m$. To see (iii), let φ be an F-algebra isomorphism of D_m into F_{ms} with $\varphi(D_m) \supset F$. Then, for any $x \in D_m$, we have $t_{D_m/F}(x) = t_{F_{ms}/F}\big(\varphi(x)\big) = t_{F_{ms}/F}(\varphi\sigma^{-1}\big(\sigma(x)\big) = t_{D_m/F}\big(\sigma(x)\big)$ and $t_{\sigma(D)_m/F}(x) = t_{F_{ms}/F}\big(\varphi(x)\big) = t_{D_m/F}(x)$.

LEMMA 3. *Let R be a simple F-subalgebra of F_n containing F, that is, $R = D_m$ where D is a division ring, and set $l = l\big(V_{F_n}(R)\big)$. Then $t_{F_n/F}(x) = lt_{D_m/F}(x)$ for all $x \in R$, and $V_{F_n}(R)$ is a simple ring with $r\big(V_{F_n}(R)\big) = l^2 r(D)$.*

PROOF. Clearly $\mathrm{Hom}_F(F^{(n)}, F^{(n)}) = F_n$. We set $T = V_{F_n}(R)$. Then, it follows from [6, p. 132, Theorem 6.4.2] that $T = D'_l$ for a division ring D' containing F which is F-linear anti-isomorphic to D, $r(T) = l^2 r(D') = l^2 r(D)$ and

$$n^2 = [F_n : F] = [R : F][T : F] = m^2[D : F]l^2[D' : F] = (ml[D : F])^2.$$

https://doi.org/10.4153/CMB-1995-014-3 Published online by Cambridge University Press

This implies $n = ml[D : F]$. Considering the inclusion map $D_m \longrightarrow R \subset F_n$, we obtain our assertion by Lemma 2 (ii).

Now we are at the position to prove the following theorem which is essential in our study.

THEOREM 4. *Let R be a simple F-subalgebra of F_n containing F, and $r = r\left(V_{F_n}(R)\right)$. Then, the following conditions are equivalent.*

(a) R is separable over F and $\chi(F) \nmid r$.

(b) $\mathrm{t}_{F_n/F}|R \neq 0$.

(c) $\mathrm{t}_{F_n/F}(xy)$ $(x, y \in R)$ is non-degenerate.

If $\chi(F) = 0$ then there hold the conditions (a)–(c).

PROOF. Since R is a simple ring, we may write $R = D_m$ where D is a division ring containing F. We set $l = l\left(V_{F_n}(R)\right)$. Then by Lemma 3, we have $r = r\left(V_{F_n}(R)\right) = l^2 r(D)$ and $\mathrm{t}_{F_n/F}(x) = l\mathrm{t}_{D_m/F}(x)$ for all $x \in R$. (a) $\Rightarrow$ (c): Since $\chi(F) \nmid r$, we have $\chi(F) \nmid l$ and $\chi(F) \nmid r(D)$. By Lemma 1 ((a) $\Rightarrow$ (c)), $\mathrm{t}_{D_m/F}(xy)$ $(x, y \in R)$ is non-degenerate. Hence $\mathrm{t}_{F_n/F}(xy)$ $(x, y \in R)$ is non-degenerate. (c) $\Rightarrow$ (b): It is obvious. (b) $\Rightarrow$ (a): Since $\mathrm{t}_{F_n/F}|R = l\mathrm{t}_{D_m/F} \neq 0$, we have $\chi(F) \nmid l$ and $\mathrm{t}_{D_m/F} \neq 0$. By Lemma 1 ((b) $\Rightarrow$ (a)), D_m is separable over F and $\chi(F) \nmid r(D)$, whence $\chi(F) \nmid r$.

THEOREM 5. *Let S be a sub-semigroup of F_n such that FS is a simple F-subalgebra of F_n containing F. Let $r = r\left(V_{F_n}(S)\right)$, and $K = \{\mathrm{t}_{F_n/F}(s)\ ;\ s \in S\}$. Then, the following conditions are equivalent.*

(a) $|S| \leq |K|^{[FS:F]}$.

(b) $|S| \leq |K|^{n^2}$.

(c) Either FS is separable over F and $\chi(F) \nmid r$ or $S = \{1\}$ and $\chi(F)|r$.

(d) Either $\mathrm{t}_{F_n/F}|S \neq 0$ or $\mathrm{t}_{F_n/F}|S = 0$ and $S = \{1\}$.

If $\chi(F) = 0$ then $|S| \leq |K|^{[FS:F]}$.

PROOF. If $|S| \leq |K|^{[FS:F]}$ then $|S| \leq |K|^{n^2}$. We assume that $|S| \leq |K|^{n^2}$. We shall distinguish two cases. Case $|S| = 1$: In this case, we see that $FS = F$ which is separable over F. Since S is a semigroup, we have $S = \{1\}$. If $\chi(F) \nmid r$ then there holds the first part of (c). Case $|S| > 1$: In this case, we have $|K| > 1$ which implies $K \neq \{0\}$. Hence, it follows that $\mathrm{t}_{F_n/F}|S \neq 0$ and so $\mathrm{t}_{F_n/F}|FS \neq 0$. Clearly $V_{F_n}(S) = V_{F_n}(FS)$. Applying Theorem 4 ((b) $\Rightarrow$ (a)), we see that FS is separable over F and $\chi(F) \nmid r$. Thus we obtain (c). Now, in case $S = \{1\}$, we have $r = n^2$, and so if $\chi(F) \mid r$ then $\mathrm{t}_{F_n/F}(S) = \mathrm{t}_{F_n/F}(1) = n = 0$. From this and Theorem 4, it follows that (c) implies (d). Next, we assume that $\mathrm{t}_{F_n/F} \mid S \neq 0$, the first part of (d). For convenience, we set $R = FS, t = \mathrm{t}_{F_n/F}$ and $q = [FS : F]$. Then, there is a F-basis $\{s_1, \ldots, s_q\}$ of R which is a subset of S. We consider the map φ of R into $F^{(q)}$ defined by

$$\varphi(x) = \left(t(s_1 x), \ldots, t(s_q x)\right), \quad x \in R.$$

Clearly φ is an F-linear homomorphism. Let $x \in \mathrm{Ker}\,\varphi$. Then $t(s_i x) = 0$ for $i = 1, \ldots, q$, and whence $t(yx) = 0$ for all $y \in R$ which implies $x = 0$, since $t(yx)$ $(x, y \in R)$ is non-degenerate by Theorem 4. Hence φ is injective and so $|S| = |\varphi(S)| \leq |K|^q$. The other assertions will be easily seen.

https://doi.org/10.4153/CMB-1995-014-3 Published online by Cambridge University Press

Now, we shall prove the following corollary which contain a revision of Hersteins' theorem [3, Theorem 2.3.3] (Theorem A).

COROLLARY 6. *Let S be a sub-semigroup of F_n such that $F^{(n)}$ is irreducible over FS, equivalently FS is a simple F-subalgebra of F_n containing F and $V_{F_n}(S)$ is a division ring. Let $r = r\big(V_{F_n}(S)\big)$ and $K = \{\mathrm{t}_{F_n/F}(s) \,;\, s \in S\}$. Then*

(i) The following conditions are equivalent.

(a) $|S| \leq |K|^{[FS:F]}$.

(b) $|S| \leq |K|^{n^2}$.

(c) FS is separable over F and $\chi(F) \nmid r$.

(d) $\mathrm{t}_{F_n/F}|S \neq 0$.

If $\chi(F) = 0$ or F is algebraically closed, then $|S| \leq |K|^{[FS:F]}$.

(ii) For an element a of F_n with $\mathrm{t}_{F_n/F}(a) \neq 0$, $FS[a]$ (the subring of F_n generated by a over FS) is a simple separable F-algebra with $\chi(F) \nmid r\big(V_{F_n}(FS[a])\big)$. In particular, if e is a primitive idempotent of F_n then $\mathrm{t}_{F_n/F}(e) = 1$ and $FS[e] = F_n$.

(iii) Let S be abelian. Then, $|S| \leq |K|^{[FS:F]}$ if and only if FS is separable over F.

PROOF. By [3, p. 41, Theorem 2.1.2 (Density Theorem)], we see that $F^{(n)}$ is irreducible over FS if and only if FS is a simple ring with $FS \supset F$ and $V_{F_n}(S)$ is a division ring. If F is algebraically closed then $V_{F_n}(S) = F$ and $FS = F_n$. In case $S = \{1\}$, we have $FS = F$ and $V_{F_n}(FS) = F$ which implies $\chi(F) \nmid r$ and $\mathrm{t}_{F_n/F} \neq 0$. Hence the assertion (i) is a direct consequence of Theorem 5. For any element a in F_n, $F^{(n)}$ is irreducible over $FS[a]$. Hence the first assertion in (ii) follows from Theorem 4 ((b) $\Rightarrow$ (a)). Now, we shall show that $FS[e] = F_n$ for any primitive idempotent e of F_n. By [6, Proposition 3.7.5], there exists a system $\{e_{ij} \,;\, 1 \leq i,j \leq n\}$ of matrix units for F_n such that $\sum_{i,j=1}^{n} e_{ij}F = F_n$ and $e_{11} = e$. Then $\mathrm{t}_{F_n/F}(e) = 1$ (*cf.* Lemma 2). Hence, it suffices to prove that if T is a simple subring of F_n containing F and e_{11} then $T = F_n$. Let $\{t_{ij} \,;\, 1 \leq i,j \leq m\}$ be a system of matrix units of T such that $T = \sum_{i,j} t_{ij}D = D_m$ where D is a division ring containing F. Clearly $e_{11}F_n$ is a minimal right ideal of F_n. Since $\sum_{i=1}^{m} t_{ii} = 1$, we have $t_{kk}e_{11} \neq 0$ for some k. Then

$$e_{11}F_n \cong t_{jk}e_{11}F_n \text{ (as right } F_n\text{-modules)}, \quad j = 1, \ldots, m.$$

Since $t_{jj}T \supset t_{jk}e_{11}T$ and $t_{jj}T$ is a minimal right ideal of T, it follows that $t_{jj} \in t_{jj}T = t_{jk}e_{11}T \subset t_{jk}e_{11}F_n$ $(1 \leq j \leq m)$, and so $\sum_{j=1}^{m} t_{jk}e_{11}F_n = F_n$ which implies that $l(F_n) = m = l(T)$. Hence $n = m$ and

$$n^2 = [F_n : F] \geq [T : F] = [T : D][D : F] = n^2[D : F].$$

Thus we obtain $[F_n : F] = [T : F]$ and $F_n = T$. Next, to see (iii), let S be abelian. Since FS is a commutative simple ring, FS is a field. Hence by [6, Theorem 6.4.2], we have $V_{F_n}(FS) = FS$ and $r = 1$. Therefore, our assertion follows immediately from (i).

Next, we shall look at the case where S is a finite sub-semigroup of F_n.

THEOREM 7. *Let S be a finite sub-semigroup of F_n such that FS is a simple F-subalgebra of F_n containing F. Let $r = r\big(V_{F_n}(S)\big)$ and $K = \{\mathrm{t}_{F_n/F}(s) \,;\, s \in S\}$. Then*

https://doi.org/10.4153/CMB-1995-014-3 Published online by Cambridge University Press

(i) FS is separable over F, and if $\chi(F) \neq 0$ then $FS = B_m$ and $V_{F_n}(S) = B_r$ ($mr[B : F] = n$) for the center B of FS.

(ii) $|S| \leq |K|^{[FS:F]}$ if and only if either $\chi(F) \nmid r$ or $S = \{1\}$ and $\chi(F)|r$.

PROOF. By Theorem 5, it suffice to prove the theorem for the case $\chi(F) \neq 0$. We set $FS = D_m$ where D is a division ring. Let B be the center of FS. Then $D \supset B \supset F$. Let P be the prime field of F, and set $T = P[S]$, the subring of F_n generated by S over P. Then $FT = FS$ and T is a finite ring whose Jacobson radical N is nilpotent. Clearly FN is a nilpotent ideal of $FT = FS$ (simple). This implies that $FN = \{0\}$ and so $N = \{0\}$. Thus T is semi-simple. If e a central idempotent of T with $e \neq 1$ then e is a central idempotent of $FT = FS$ (simple) with $e \neq 1$ and so $e = 0$. Therefore, it follows that T is a simple ring. Let C be the center of T. Then C is a finite field and FC is contained in the center B of $FT = FS = D_m$. Clearly FC is separable over F. Since $FC \otimes_C T$ is a simple ring, the ring homomorphism $FC \otimes_C T \longrightarrow FC \cdot T = FS$ ($\sum a_i \otimes b_i \longmapsto \sum a_i b_i$) is an isomorphism. Hence FC coincides with the center B of FS. Since T is a finite simple ring, T is a total matrix ring over C. Therefore, it follows that $B = FC = D$ and $FS = B_m$ which is a separable F-algebra. Moreover, by [6, p. 132, Theorem 6.4.2], we have $V_{F_n}(S) = B_r$ and $mr[B : F] = n$. The other assertions follow from Theorem 5.

In virtue of Theorem 7, we shall prove the following theorem which is a revision of Theorem A.

THEOREM 8. *Let S be a finite sub-semigroup of F_n such that $F^{(n)}$ is irreducible over FS, and $K = \{\mathrm{t}_{F_n/F}(s) \,;\, s \in S\}$. Then $|S| \leq |K|^{[FS:F]} \leq |K|^{n^2}$.*

PROOF. By Corollary 6 (i), it suffices to prove the theorem for the case $\chi(F) \neq 0$. Let B be the center of FS. Then, since FS is a simple F-subalgebra of F_n containing F, it follows from Theorem 7 that FS is separable over F, $V_{F_n}(S) = B$ and so $r\big(V_{F_n}(S)\big) = 1$. Therefore the assertion follows from Corollary 6 (i).

EXAMPLE 2. Let $F = \mathrm{GF}(2)(x)$ and $B = \mathrm{GF}(4)(x)$ where x is an indeterminate. By a regular representation of $\mathrm{GF}(4)$ into $\mathrm{GF}(2)_2$, we may set $\mathrm{GF}(4) \subset \mathrm{GF}(2)_2$. Let r be an arbitrary positive integer. Then

$$\begin{aligned} B_2 \otimes_B B_r = B_{2r} &= \big(F \otimes_{\mathrm{GF}(2)} \mathrm{GF}(4)\big)_{2r} \\ &= F_{2r} \otimes_{\mathrm{GF}(2)} \mathrm{GF}(4) \subset F_{2r} \otimes_{\mathrm{GF}(2)} \mathrm{GF}(2)_2 = F_{4r}. \end{aligned}$$

Moreover, we have $V_{F_{4r}}(B_2) = B_r$ and $V_{F_{4r}}(B_r) = B_2$. Clearly F_{4r} is irreducible over B_2 if and only if $r = 1$. Now, we set $S = \mathrm{GF}(4)_2 \subset B_2$. Then S is a finite sub-semigroup of B_2 and $B_2 = FS$ which is separable over F. By Theorem 5, we see that $2 \nmid r$ if and only if $\mathrm{t}_{F_{4r}/F}|S \neq 0$. Further, if $r = 1$ then $|S| = 2^8 = |\{\mathrm{t}_{F_4/F}(s) \,;\, s \in S\}|^{[FS:F]}$, since $B_2 = F \cdot \mathrm{GF}(4)_2 = F \otimes_{\mathrm{GF}(2)} \mathrm{GF}(4)_2$ and so $\mathrm{t}_{\mathrm{GF}(4)_2/\mathrm{GF}(2)}(s) = \mathrm{t}_{B_2/F}(s) = \mathrm{t}_{F_4/F}(s)$ ($\in \{0, 1\}$) for all $s \in \mathrm{GF}(4)_2 = S$ (Lemma 3). Next, let $e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $\alpha = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \in \mathrm{GF}(4)_2$ where $\mathrm{GF}(2)[\alpha] = \mathrm{GF}(4)$, and S' the (multiplicative) sub-semigroup of $\mathrm{GF}(4)_2$ generated by $\{e_{12}, e_{21}, \alpha\}$. Then $\mathrm{GF}(2)S' = \mathrm{GF}(4)_2$ and $FS' = B_2$. Hence, if $r = 1$ then $13 = |S'| < |\{\mathrm{t}_{F_4/F}(s) \,;\, s \in S'\}|^{[FS':F]} = 2^8$.

https://doi.org/10.4153/CMB-1995-014-3 Published online by Cambridge University Press

REMARK 2. As in Remark 1, let A be a commutative separable C-algebra which is projective over C. Then, by [2, Theorem 3.2.1 and Corollary 3.2.2], the bilinear map $T_{A/C}(xy)$ $(x, y \in A)$ is non-degenerate. Hence, for any positive integer m, $t_{A_m/C}(xy)$ $(x, y \in A_m)$ is non-degenerate. Now, let S be a sub-semigroup of A_m such that $A_m = CS = Cs_1 + \cdots + Cs_q$ for some $s_1, \ldots, s_q$ in S, and set $K = \{t_{A_m/C}(s) \ ; \ s \in S\}$. Then we can prove that $|S| \leq |K|^q$ by making use of the same methods as in the proof of Theorem 5.

ACKNOWLEDGEMENT. The authors would like to express their indebtedness and gratitude to Prof. K. Kaneta for his helpful suggestions and valuable comments.

REFERENCES

1. P. M. Cohn, *Algebra*, Vol. 2, Wiley, London, 1977.
2. F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes In Math. **181**, Springer-Verlag, 1971.
3. I. N. Herstein, *Noncommutative rings*, Carus Math. Monographs **15**, Math. Association of America, Washington, D. C., 1968.
4. N. Jacobson, *Basic Algebra II*, Freeman, San Francisco, 1980.
5. ———, *Lectures in abstract algebra II*, Linear algebra, New York, 1953.
6. ———, *Structure of rings*, Providence, 1956.
7. I. Kaplansky, *Notes on Ring Theory*, University of Chicago Math. Lecture Notes, 1965.
8. H. Tominaga and T. Nagahara, *Galois Theory of simple rings*, Okayama Math. Lectures, Okayama, 1970.

Department of Mathematics
Okayama University
Okayama 700
Japan