SUBMODULES OF RINGS

CARL C. FAITH

1. Introduction. Let G be a subgroup of the group $\mathfrak{J}$ of all quasi-inner automorphisms of a ring $\mathfrak{A}$. A subset $\mathfrak{S}$ of $\mathfrak{A}$ is a *GI-subset* of $\mathfrak{A}$ (*G*-Invariant subset of $\mathfrak{A}$) in case $\mathfrak{S}$ is invariant under G in the sense that $\mathfrak{S}G = \mathfrak{S}$. The well-known Cartan-Brauer-Hua theorem states: *If $\mathfrak{A}$ is a division ring, and if $\mathfrak{S}$ is a proper GI-division subring not contained in the center of $\mathfrak{A}$, then $G \neq \mathfrak{J}$.* In [2] this result was extended as follows: *Then G has infinite index in $\mathfrak{J}$, that is, $\mathfrak{A}$ contains infinitely many subrings conjugate to $\mathfrak{S}$.* [1] The first purpose of this article is to present a suitable analog of this latter result for rings where the Cartan-Brauer-Hua theorem has been extensively generalized, namely, for the simple rings studied by Amitsur [1], and the matrix and local matrix rings of Rosenberg [5]. As in their work results first are obtained for (noninvariant) submodules of $\mathfrak{A}$.

At least two kinds of divisibility properties are inherent in the notions of subspaces of an algebra $\mathfrak{A}$ over a field ϕ: (1) divisibility of ϕ and (2) ϕ-divisibility of a subspace $\mathfrak{S}$ of $\mathfrak{A}$ (in the sense that $\alpha\phi = \phi$, and $\alpha\mathfrak{S} = \mathfrak{S}$, for every $0 \neq \alpha \in \phi$). Now assume only that $\mathfrak{A}$ is a ϕ-ring, [2] and that ϕ is an arbitrary ring. An additive subgroup $\mathfrak{S}$ of $\mathfrak{A}$ is a subspace if $\alpha\mathfrak{S} \subseteq \mathfrak{S}$ for each $\alpha \in \phi$, $\alpha \neq 0$. If ϕ has an identity element which is the identity operator on $\mathfrak{A}$, then clearly (1) implies (2) but (2) is independent of (1) in the sense that (2) is meaningful even if (1) fails. Although [1] is a study of invariant subspaces of simple algebras over fields, (1) seems to play no rôle in the theory developed there, other than guaranteeing (2). This observation is the starting point for the present article, that is, whenever feasible, the requirement (1) is dropped and (2) is only assumed "locally."

Following Amitsur [1], we shall be exclusively concerned with subgroups of $\mathfrak{J}$ generated by quasi-inner automorphisms effected by elements $u \in \mathfrak{A}$ which are 2-*potent* in the sense that $u^2 = 0$. Inasmuch as

---

[1] In case $\mathfrak{A}$ is a division algebra of finite dimensions, and $\mathfrak{S}$ is a division subalgebra, this result is a corollary to a theorem of Hattori [3].

[2] $\mathfrak{A}$ is a left-Φ-module satisfying $\alpha(xy) = (\alpha x)y = x(\alpha y)$ for all $\alpha \in \Phi$, and all $x, y \in \mathfrak{A}$ (cf. N. Jacobson's, *Theory of rings*, p. 55). It is clear that $\mathfrak{A}$ is Φ-simple if and only if $\mathfrak{A}$ is simple, and, also, that if A contains a nonzero ϕ-divisible subspace, then ϕ can contain no proper zero divisors.

these transformations include, in the case $\mathfrak{A}$ is a matrix ring of degree >1, the inner automorphisms effected by the transvections of $\mathfrak{A}$ (§3), a uniform approach to the papers cited above is possible. This uniformity, together with the recasting of Amitsur's results [1] in greater generality (and in the perspective outlined in the preceding paragraph), constitutes the second main objective of the present article.

Finally (§5) several useful results on the generation of simple algebras with minimum condition are given new proofs and simultaneously extended to simple algebras over fields $\neq GF(2)$ containing idempotents $\neq 0, 1$, as an application of a theorem of Amitsur. These latter algebras contain no invariant nontrivial one-sided ideals, are generated by idempotent elements (also by 2-potent elements), and each element is a sum of quasi-regular elements.

2. **Simple rings.** If a is an element of a ring A with quasi-inverse a', then the mapping $x \to x + ax + xa' + axa'$ is an automorphism of A, called the *quasi-inner automorphism of A determined by a*. The quantity on the right of the arrow will be denoted by $(1+a)x(1+a)^{-1}$ whether A has an identity or not. Of course, when A has an identity e, then $(1+a)x(1+a)^{-1} = (e+a)x(e+a)^{-1}$ so that every quasi-inner automorphism is inner.

As usual, for all $a, b \in A$, $[a, b]$ denotes the commutator $ab - ba$. If B and C are subsets of A, then $[B, C]$ denotes the submodule ($=$additive subgroup) of A generated by all $\{[b, c] \mid b \in B, c \in C\}$.

Now let A be a Φ-ring[2] over a commutative ring Φ, and let M be a submodule ($=$additive subgroup) of A. In this article, any $u \in A$ whose square is zero will be designated as a *2-potent element of A*. If u is any 2-potent element of A, $t_u(\alpha)$ will denote the mapping

$$t_u(\alpha): M \to (1 + \alpha u)^{-1} M (1 + \alpha u)$$

of M onto its conjugate $(1+\alpha u)^{-1}M(1+\alpha u)$, where $\alpha \in \Phi$; $T_M(u)$ will signify the multiplicative group of all mappings $\{t_u(\alpha) \mid \alpha \in \Phi\}$; $N_M(u)$ is the kernel of the homomorphism $\alpha \to t_u(\alpha)$ of $(\Phi, +)$ on $T_M(u)$. Thus $T_M(u) \cong (\Phi, +) - N_M(u)$, where $N_M(u) = \{\alpha \in \Phi \mid (1+\alpha u)^{-1}M(1+\alpha u) = M\}$. When there can be no confusion resulting from this, $T(u)$ and $N(u)$ will represent $T_M(u)$ and $N_M(u)$ respectively. In what follows $J = (J, +)$ will denote the additive group of integers. The submodule M is *divisible by* $\alpha \in \Phi$ in case $\alpha M = M$, and $\alpha \neq 0$; M is *Φ-divisible* if M is divisible by each nonzero $\alpha \in \Phi$. The concept "*M is J-divisible*" is defined inasmuch as A is also a J-ring. In this case M will be said to be, simply, *divisible*.

LEMMA 1. *Let A be a Φ-ring[2] over a commutative ring Φ; let M be any submodule divisible by α, β, and $\alpha - \beta$ for different nonzero α, $\beta \in \Phi$; let u be any 2-potent element in A. Then α, $\beta \in N_M(u)$ if and only if both $[u, M]$ and uMu are contained in M. Then $(1+u)^{-1}M(1+u) = M$.*

PROOF. SUFFICIENCY. Assume that $[u, M]$, and uMu are contained in M. Then so are $[u, \alpha M]$ and $u(\alpha^2 M)u$. Therefore,

$$(1 + \alpha u)^{-1} m(1 + \alpha u) = m + [u, \alpha m] + u(\alpha^2 m)u \in M,$$

and also

$$(1 + \alpha u)m(1 + \alpha u)^{-1} \in M, \quad \text{when} \quad m \in M.$$

Thus, $(1+\alpha u)^{-1}M(1+\alpha u) = M$, that is, α (also $\beta) \in N_M(u)$.

NECESSITY. Clearly $x = [\alpha u, m] - (\alpha u)m(\alpha u) \in M$, and $y = [\beta u, m] - (\beta u)m(\beta u) \in M$, for all $m \in M$. Then

$$\alpha^2 y - \beta^2 x = \lambda[u, m] \in M,$$

where $\lambda = (\alpha - \beta)\alpha\beta$. Hence $\lambda[u, M] = [u, \lambda M] = [u, M] \subseteq M$. Furthermore, $u(\alpha^2 m)u = \alpha[u, m] - x \in M$, for all m. Since $\alpha^2 M = M$, it follows that $uMu \subseteq M$.

Then, $(1+u)^{-1}m(1+u) = m + [m, u] - umu \in M$, for all $m \in M$. Thus $(1+u)^{-1}M(1+u) \subseteq M$. Since $N_M(u) = N_M(-u)$, the calculations above show that $(1+u)M(1+u)^{-1} \subseteq M$ as well, that is, that $(1+u)^{-1}M(1+u) = M$.

If $\Phi = J$ in the lemma, and if α, $\beta \in N_M(u)$ are relatively prime, then $1 = p\alpha + q\beta \in N_M(u)$ for suitable p, $q \in J$. That $1 \in N(u)$ even if α and β are not relatively prime is a notable consequence of the lemma. In fact, if Φ is any commutative ring with identity 1 such that A is unital in the sense that $1a = a$ for each $a \in A$,[3] the lemma shows that $1 \in N(u)$ whenever M is Φ-divisible and card $N(u) > 2$.

A $\mathfrak{T}I$-*subgroup* of A is a subgroup of $(A, +)$ such that

$$(1 + u)^{-1}M(1 + u) = M$$

for each 2-potent $u \in A$. (In the context of §1, $\mathfrak{T}$ is the subgroup of the group $\mathfrak{F}$ generated by all quasi-inner automorphisms effected by 2-potent elements.) Above, and below, card S denotes the cardinality of any set S.

LEMMA 2. *Let M be a not $\mathfrak{T}I$-subgroup of a Φ-ring A, where Φ is commutative. Then, there exists a 2-potent $u \in A$ such that:*
(I) *Card $N_M(u) \leq 2$ in case M is Φ-divisible.*

---

[3] In this case A is an algebra over Φ (cf. [4, p. 16]).

(II) $T_M(u)\cong(\Phi, +)$ *in case M is Φ-divisible and $2\alpha=0$ implies $\alpha=0$*
for each $\alpha\in\Phi$.

(III) $T_M(u)$ *contains an isomorph of $(J, +)$ in case M is divisible,*
and $\gamma M = M$ for at least one $0\neq\gamma\in\Phi$.

PROOF. (I) Since M is Φ-divisible, Lemma 1 shows that

$$(1 + u)^{-1}M(1 + u) = M$$

whenever card $N_M(u) > 2$. Since M is not $\mathfrak{X}I$, clearly (I) holds. (II) If
u is 2-potent, and if card $N_M(u)\leq 2$, then, as a matter of fact, it is
true that $N_M(u) = \{0\}$, since $0\neq\alpha\in N_M(u)$ would imply that $2\alpha\in N$,
whereas $2\alpha\neq 0$, α. (III) First consider A as a J-ring. Since M is
divisible, by (II), there is a 2-potent $u\in A$ such that $(1+u)^{-1}M(1+u)$
$\neq M$. If $\gamma M = M$, $0\neq\gamma\in\Phi$, and if $\alpha=q\gamma\in N(u)$ for some $0\neq q\in J$,
then also $\beta = 2\alpha = 2q\gamma\in N(u)$. Since $(k\gamma)M = k(\gamma M) = kM = M$ for
each $0\neq k\in J$, by Lemma 1, $(1+u)^{-1}M(1+u) = M$. This contradic-
tion shows that the homomorphism $k\to t_{k\gamma}(u)$ of J on the subgroup
$\{t_{k\gamma}(u)\,|\,k\in J\}$ of $T_M(u)$ is actually an isomorphism.

In [1] Amitsur made a blanket hypothesis on the simple ring A:
A is an algebra over a field $\neq GF(2)$. Although it is readily apparent
that certain of his calculations are valid for rings under a more general
hypothesis, partly in order to avoid the appearance of applying re-
sults under incorrect hypotheses, and partly for the convenience of
the reader, [1, p. 988] is summarized in greater generality in a lemma
below. In it $e\neq 1$ signifies the existence of some $a\in A$ such that the
equality $ea = ae = a$ fails; F_2 is the full matrix ring of degree 2 over F;
Z is the center of A.

LEMMA (AMITSUR). *Let A be a simple ring with an idempotent
$e\neq 0$, 1, and let M be a submodule of A such that $[u, M]\subseteq M$ for all
2-potent $u\in A$. Then: if $A \neq F_2$, when F is a field of characteristic 2,
then $M\supseteq[A, A]$, or else $M\subseteq Z$.*

PROOF. It is easy to see that Amitsur's proof of [1, Lemma 3] de-
pends only on the result of [1, Lemma 1], and on [1, Lemma 2].
Since this latter lemma holds quite generally for simple rings,[4] it
follows that [1, Lemma 3] can be restated: *If A is simple, and if
$[u, M]\subseteq M$ for all 2-potent $u\in A$, then $[M, [A, A]]\subseteq M$.* That
$M\supseteq[A, A]$, or $M\subseteq Z$ follows from this inclusion in the same way
as in [1].

Amitsur's lemma and Lemma 1 can be used to "determine" the

---

[4] More specifically, it is only required that $AeA = A$, and $Ae'A = A$, where (for-
mally) $e' = 1 - e$.

not $\mathfrak{X}I$-subgroups in some cases. This determination, together with Lemma 2, produces

THEOREM 1. *If A is a simple Φ-ring[2] with an idempotent $\neq 0$, 1, and Φ commutative; if $A \neq F_2$ when F is a field of characteristic 2; if M is any submodule of A such that $M \not\supseteq [A, A]$, and $M \not\subseteq$ the center Z of A, then there exists a 2-potent $u \in A$ such that (I–III) of Lemma 2 hold.*

Now suppose that A is an algebra over ϕ, where ϕ is commutative.[2,3] If A contains an identity element 1, then in order that every subspace of A be ϕ-divisible, it is necessary that $\phi \cong \phi 1$ be a field. As was remarked in §1, this condition is also sufficient. Hence, in order to insure "global" ϕ-divisibility of subspaces, there is no loss of generality, at least when $1 \in A$, in assuming, as in the next theorem, that ϕ is a field.

THEOREM 2. *Let A be a simple algebra with an idempotent $\neq 0$, 1, over a field ϕ such that $A \neq F_2$ when F is a field of characteristic 2. Let B be any proper subalgebra $\not\subseteq$ the center Z of A. Then, there exists a 2-potent $u \in A$ such that: (1) card $\{(1 + \alpha u)^{-1} B(1 + \alpha u) \mid \alpha \in \phi\} =$ card ϕ, when ϕ is infinite; (2) different $k \in J$ determine different subrings $(1 + ku)^{-1} B(1 + ku)$, when ϕ has characteristic 0.*

PROOF. Now $B \not\supseteq [A, A]$ (see the proof of [1, Theorem 2] for this computation), and $B \not\subseteq Z$, so that the hypotheses of Theorem 1 (I) hold. Thus, there is a 2-potent $u \in A$ with card $N_B(u) \leq 2$, and such that $T_B(u) \cong (\phi, +) - N_B(u)$. (1) follows immediately from this; (2) is a direct consequence of Theorem 1 (III).

As Amitsur noted in [1, p. 989, §3], there exist simple central algebras even over fields of characteristic 0 containing characteristic proper subalgebras. Furthermore, O. F. G. Schilling has constructed a division algebra D with a valuation V having the property that the valuation ring $O = \{d \in D \mid Vd \geq 0\}$ is a proper invariant subalgebra not contained in the center. (See his *The theory of valuations*, Mathematical Surveys, Amer. Math. Soc., vol. 4, 1950, p. 24, Example VI). However, if Δ is a division subalgebra of a division algebra D over the field ϕ, $\Delta \neq D$, and $\Delta \not\subseteq$ not contained in the center C of D, then (Cartan-Brauer-Hua) Δ is not invariant. Let S' denote the centralizer in D of any subset S of D. Then the results of [2] show: (1) if $d \in \Delta$, $d \notin C$, if Q_d is an infinite set $\subseteq d' \cap \Delta$, then

$$\text{card } \{(1 + \alpha v)^{-1} \Delta (1 + \alpha v) \mid \alpha \in Q_d\} = \text{card } Q_d,$$

for any $v \in D$, $v \notin \Delta$, $v \notin d'$. (2) If $d' \cap \Delta$ is finite for each $d \in \Delta$, $d \notin C$, then (Δ is finite and) card $\{a^{-1} \Delta a \mid 0 \neq a \in D\} =$ card $D \geq \aleph_0$. (1) has the following immediate corollary which we duly record because of its similarity to Theorem 2 (1).

THEOREM 2′. *Let D be a division algebra over an infinite field ϕ, and let Δ be any proper division subalgebra not contained in C. Then, card $\{(1+\alpha v)^{-1}\Delta(1+\alpha v)|\alpha\in\phi\}$ = card ϕ, for each $v\in D$, $v\notin\Delta$, $v\notin\Delta'$.*

3. **Matrix rings.** Let A be a ring, and $R=A_n$ the ring of $n\times n$ matrices over A, $n\geq 2$. For each $a\in A$, a_{pq} denotes the matrix with a in the (p, q) position and zeros elsewhere. An additive subgroup S of R is a *TI-subgroup* (*Transvectionally Invariant subgroup*) in case S is invariant under all quasi-inner automorphisms effected by the a_{ij}, $i\neq j$, $a\in A$.[5] Rosenberg [5] has determined the structure of the *TI*-subgroups of A_n assuming that $1\in A$, and $n\geq 3$. These are the subgroups of the center, or they have the form $[A_n, K_n]+D$, where K is a nonzero 2-sided ideal of A (consisting of the off-diagonal entries of the elements of the *TI*-subgroup), and D is an additive group of diagonal matrices. Thus, in case $1\in A$, and $n\geq 3$, the not *TI*-subgroups in the following theorem are well-determined.

Let $(R', \circ)$ denote the group (under $a\circ b=a+b+ab$) of all quasi-regular elements of the ring R of the theorem. Then $(T, \circ)$ denotes the subgroup generated by all 2-potent elements of $(R', \circ)$.

THEOREM 3. *Let S be a not TI-subgroup of $A_n=R$, $n\geq 2$. If A is divisible, then (1) the set $\{(1+a)^{-1}S(1+a)|a\in(T, \circ)\}$ is infinite. If S is divisible, then (2) there exists $u=a_{ij}$, $i\neq j$, $a\in A$, such that different $k\in J$ determine different subgroups $(1+ku)^{-1}S(1+ku)$.*

PROOF. Negation of (1) amounts to the assertion that the subgroup $(N, \circ)=\{a\in(T, \circ)|(1+a)^{-1}S(1+a)=S\}$ has finite index in $(T, \circ)$. This means that there exists a fixed natural number q such that for any $a\in(T, \circ)$ that $a^{\circ q}=a\circ a\circ\cdots\circ a$ (q times)$\in(N, \circ)$. If a is 2-potent, then $a^{\circ q}=qa$. Thus for each $a\in A$, and each $i\neq j$, $qa_{ij}\in(N, \circ)$. Since $q(a_{ij})=(qa)_{ij}$, and since $qA=A$, clearly $(N, \circ)$ contains every b_{ij}, $i\neq j$, $b\in A$. Then S is a *TI*-subgroup. This contradiction establishes (1).

Next assume only that S is divisible, and consider R as an algebra over J. Then $T(u)$ and $N(u)$ are defined with respect to J, for all $u=a_{ij}$, $i\neq j$, $a\in A$. If $k\in N(u)$, and if $k\neq 0$, then $N(u)$ has order >2, since k, $2k$, $\cdots$, are distinct elements of $N(u)$. By Lemma 1, $(1+u)^{-1}S(1+u)=S$. Since S is not a *TI*-subgroup, there exists $u=a_{ij}$, $i\neq j$, $a\in A$, such that $N(u)=\{0\}$. Then, for this u, $T(u)\cong(J, +)$.

---

[5] In the context of §1, T is the subgroup of $\mathfrak{F}$ generated by all quasi-inner automorphisms effected by these elements. When $1\in A$, an element $1+a_{ij}$, $i\neq j$, $a\in A$, is a *transvection* [5].

COROLLARY 1. *Let A be a simple ring of characteristic 0, with identity, and let B be a proper subring of $R = A_n$, $n \geq 3$, such that $B \not\subseteq$ the center C of R. Then: (1) There exist infinitely many subrings*

$$\{(1 + a)^{-1} B (1 + a) \mid a \in (T, \circ)\};$$

(2) If there exists $r \in R$ such that $qr \notin B$ for all $0 \neq q \in J$, then there exists $u = a_{ij}$, $i \neq j$, $a \in A$, such that different $k \in J$ determine different subrings $(1 + ku)^{-1} B (1 + ku)$.[6]

PROOF. Since A is simple, so is A_n (cf., e.g., [4, p. 40, Proposition 2]). Now $B \not\supseteq [A_n, A_n]$, since, otherwise, $B = A$ in the same way as the proof of [1, Theorem 2]. Thus, by Rosenberg's structure theorem [5, Theorem 1], B is not TI-subgroup. Theorem 3 (1) now completes the proof of (1).

(2) R is evidently an algebra over the field of rational numbers. If $B' = \{a \in R \mid ka \in B \text{ for some } 0 \neq k \in J\}$, then the condition (2) implies that $B' \neq R$.[7] Now B' is the subalgebra generated by B, and moreover, $x^{-1} B x = B$ implies $x^{-1} B' x = B'$. Then (2) follows from Theorem 3 (2), since the proof of (1) shows that B' is not TI.

The next result shows that a proper subring B of $R = A_n$, $n > 1$, is noninvariant if B contains any element belonging to a set $M(n)$ of matrix units in R. This improves on a result of G. Ehrlich [Proc. Amer. Math. Soc. vol. 6 (1955) pp. 470–471] who proved the noninvariance any proper subring B containing $M(n)$.

PROPOSITION 1. *Let A be in a ring with identity 1, and let $M(n) = \{e_{ij} \mid i, j = 1, \cdots, n, \sum_1^n e_{ii} = 1\}$ be a complete set of matrix units for $R = A_n$, $n > 1$. Then R is generated (as a ring) by the conjugates of any element $e = e_{ij} \in M(n)$.*

PROOF. Let B denote the subring generated by the conjugates of $e = e_{11}$, say. Then B contains every $e_{jj} = x_j^{-1} e_{11} x_j$, $j \neq 1$, where $x_j = x_j^{-1} = 1 - e_{11} - e_{jj} + e_{1j} + e_{j1}$. For each $a \in A$, and $i \neq j$, set

$$t_{ij}(a) = (1 + ae_{ij}) e_{jj} (1 - ae_{ij}).$$

Then,

$$ae_{ij} = t_{ij}(a) - e_{jj} \in B,$$

for all $a \in A$, and all $i \neq j$. Then B contains every ae_{ii} as well,

---

[6] When A is simple, A_n is simple, so that Theorem 2 yields information for subalgebras in the $n = 2$ case, and even supplements (1) and (2) when $n \geq 3$ (and A need not have characteristic 0).

[7] In other words, the difference group $(R - J, +)$ is not torsion. I have not been able to answer the question (asked by the referee) whether this condition is necessary.

$i = 1, \cdots, n$, so that $B \supseteq R = A_n$. The case $e = e_{jj}$, j arbitrary, follows from this, since $e_{11} = x_j e_{jj} x_j^{-1}$. Finally, if $e = e_{ij}$, $i \neq j$, note that $e_{jj} = e_{ij} - (1 - e_{ji}) e_{ij} (1 + e_{ji}) e_{ij} \in B$, so that $B = R$ in this case too.

4. Local matrix rings. The first corollary to Theorem 3 is now extended to rings which are locally matrix rings over simple rings with units and characteristic 0 in the sense of Rosenberg [5].

THEOREM 4. *Let R be a ring which is locally matrix of degree ≥ 3 over simple rings with units and characteristic 0. Let B be a proper subring not contained in the center. Then R contains infinitely many subrings of the form $\{(1+a)B(1+a)^{-1} \mid a \in (R', 0)\}$.*[8]

PROOF. Let $x \in R$, $x \notin B$. Since B is not contained in the center there exists $b \in B$, $y \in R$ such that $yb \neq by$. Embed x, y and b in a matrix ring A_n, $n \geq 3$, where A is a simple ring of characteristic 0, and unit e. Let $M = B \cap A_n$. Then, since $M \neq A_n$, and since M is not contained in the center of A_n, by Corollary 1(1), the set $\{gMh \mid g, h \in A_n, gh = e\}$ is infinite. Then, since $gBh = B$, g, $h \in A_n$, $gh = e$, implies $gMh = M$, so is the set $\{gBh \mid g, h \in A_n, gh = e\}$. Then the set

$$\{(1 - e - g)B(1 - e - h) \mid g, h \in A_n, gh = e\}$$

is infinite too (cf. [5, Theorem 2]).

5. Generation of simple algebras. Let A' denote the totality of quasi-regular (q.r.) elements of a ring A. For any subset S of A, $M(S)$ and $R(S)$ will denote the submodule and subring, respectively, generated by S. In case A is also an algebra, $\alpha(S)$ is the subalgebra generated by S. Now each element of $R(A')$ is expressible as sums (and differences) of products of q.r. elements. Let $a, b \in A'$ have the quasi-inverses a', b' respectively. Then $c = a + b + ab$ has quasi-inverse $c' = a' + b' + b'a'$. Thus $ab = c - a - b \in M(A')$. An evident induction establishes that any product of q.r. elements belongs to $M(A')$. This shows that $R(A') \subseteq M(A')$. Trivially $R(A') \supseteq M(A')$ so the equality $R(A') = M(A')$ holds. In case $1 \in A$, the set A^* of all units of A is defined, and it is easily seen that $M(A^*) = R(A^*)$. Consequently any statement to the effect that A is generated by a subset S is independent of the type of generation $M(S)$, or $R(S)$, usually referred to, in the case $S = A'$, or A^*.

In the case $1 \in A$, $M(A^*) \supseteq M(A')$ but $M(A^*) \neq M(A')$ in some

---

[8] Corollary 1 (2) could be extended similarly by restricting B to be a subalgebra. But, since R is simple, one could also appeal to Theorem 2 (2) for a sharper result, and R would only have to be locally matrix of degree ≥ 2 at that. Furthermore, Theorem 2 (1) would yield information in the modular case.

cases (e.g., $A \cong GF(2)$). It is easily shown, however, that $M(A^*)$ $= M(A')$, when A is any algebra (with 1) over a field $\neq GF(2)$.

Now let $A = D_n$, where D is a division algebra. Shoda [6, p. 255, Hilfssatz 5] (cf. Zelinsky [7]) has shown that $M(A^*) = A$ in this case. In case D has center $\phi \neq GF(2)$, $M(A') = A$ as well. This latter equation can be extended in an obvious way to simple algebras A with minimal left ideals inasmuch as each $a \in A$ is contained in a subalgebra isomorphic to D_n, $n = n(a)$, (cf., [4, p. 90, Theorem 3]). On the other hand, neither $R(A') = A$, nor $R(A^*) = A$, can hold for every simple algebra with identity even over a field of characteristic 0. (See [1, p. 989, §3].) Since $R(A^*)$ is a characteristic subalgebra of an algebra A over ϕ, Amitsur's theorem [1, Theorem 2], together with Shoda's theorem just mentioned, shows that $R(A^*) = A$ whenever A is simple, contains an idempotent $e \neq 0$, 1, and $\phi \neq GF(2)$, since e and 0, $1 \neq \alpha \in \phi$ can be used to manufacture a unit of A not in the center of A. More generally one has

THEOREM 5. *Let A be a simple algebra with an idempotent $e \neq 0$, 1, over a field $\phi \neq GF(2)$. Then each $a \in A$ is a sum of quasi-regular elements.*

PROOF. In view of the preceding remarks, one may assume that $A \neq F_2$, when F is a field of characteristic 2. If T denotes the totality of 2-potent elements of A, then $R(T) = \alpha(T)$. One proceeds to pick $u \in T$, $u \notin$ the center Z of A. To do this it suffices to write

$$A = eAe + fAf + eAf + fAe$$

where (formally) $f = 1 - e$, and to note that it is impossible that $eAf = fAe = \{0\}$. Otherwise, $A = eAe \oplus fAf$ would contain the proper ideal eAe. Consequently there exists $0 \neq u = eaf \in T$ (or $u = fae$), and $u \notin Z$ since $uf = u \neq fu = 0$ (or $fu = u \neq uf = 0$). By Amitsur's theorem $R(T) = A$, so that each $a \in A$ is a sum of products of elements of T. Since $T \subseteq A'$, then $R(A') = A$ as well. Then $M(A') = A$ as indicated above.

COROLLARY 2. *Let A be any simple algebraic algebra over a field $\phi \neq GF(2)$. Then each $a \in A$ is a sum of quasi-regular elements.*

PROOF. The result is trivially true if A is a radical ring (that is a nil ring). Otherwise every nonzero left ideal of A contains an idempotent $e \neq 0$. Thus, A is either an algebra of the type of Theorem 5, or else A is a division algebra. In either case, $M(A') = A$.

Since every element of the radical of an algebra is q.r., $M(A') = A$ also whenever a modulo radical is a direct sum of algebras of the kind

in Theorem 5, or in Corollary 2 (or, as a matter of fact, of algebras generated by q.r. elements).

Theorem 5 has the following interesting consequence.

COROLLARY 3. *Let A be as in Theorem 5. Then A contains no invariant right ideals $\neq \{0\}$, A. Moreover, A is a sum of isomorphic principal right ideals with idempotent generators.*

PROOF. If $(1+a)Q(1+a)^{-1} \subseteq Q$ for any $a \in A'$, and any right ideal Q, then $(1+a)Q \subseteq Q$, so that $aQ \subseteq Q$. Since each $x \in A$ is a sum, $x = \sum_1^n a_i$, $a_i \in A'$, $i = 1, \cdots, n$, $n = n(a)$, if Q is invariant, then $xQ \subseteq Q$, for any $x \in A$. Thus, Q is a two-sided ideal of A. By the simplicity of A, $Q = \{0\}$, or A. Now let $(e^*)_R$ denote the principal right ideal generated by e^*, where e^* is a quasi-conjugate of the idempotent 0, $1 \neq e \in A$. Since each $(e^*)_R$ is isomorphic to $(e)_R$, and since $\sum (e^*)_R$ is an invariant right ideal of A not contained in Z, $A = \sum (e^*)_R$.

A ring A is a *radical extension* of a subring B in case some power of each $a \in A$ lies in B. If A is a simple ring, not a division ring, having minimum condition, an application of Proposition 1 (§3) indicates that A is not a radical extension of any proper subring. This result, a consequence of the fact that A is generated as a ring by idempotents, will be used to advantage in a subsequent paper dealing with radical extensions of rings.[9] The following corollary, which follows from the result just mentioned in the exceptional cases of Amitsur's theorem, and from the fact that A is also generated as an algebra by idempotents (in fact, by the conjugates of any idempotent $\neq 0$, 1) in the other cases, generalizes the result just mentioned but does not contain it.

COROLLARY 4. *Let A be as in Theorem 5. Then A is not a radical extension of any proper subalgebra B.*

In case $1 \in A$, "subalgebra B" in the corollary can be replaced by "subring B" provided the prime subfield $F \neq GF(2)$. For let $0 \neq \alpha \in F$. Then α is contained in every subring B, and, if A/B is radical, $(\alpha^{-1})^n \in B$. Hence, $\alpha^{-1} = \alpha^{-n}\alpha^{n-1} \in B$. This shows that B is a subalgebra of A considered as an algebra over F. Since $F \neq GF(2)$, the last corollary applies.

COROLLARY 5. *Let A be a simple ring with identity 1, and idempotent*

---

[9] See my article, *Algebraic division ring extensions*, forthcoming in these PROCEEDINGS.

$\neq 0, 1$. *If* A *has characteristic* $\neq 2$, *then* A *is not a radical extension of any subring* $B \neq A$.

References

1. S. A. Amitsur, *Invariant submodules of simple rings*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 987–989.

2. C. C. Faith, *On conjugates in division rings*, Canad. J. Math. vol. 10 (1958) pp. 374–380.

3. A. Hattori, *On the multiplicative group of simple algebras and orthogonal groups of three dimensions*, J. Math. Soc. Japan vol. 4 (1952) pp. 205–217.

4. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloquium Publications, vol. 37, Providence, 1956.

5. A. Rosenberg, *The Cartan-Brauer-Hua theorem for matrix and local matrix rings*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 891–898.

6. K. Shoda, *Über die Galoissche Theorie der halbeinfachen hyperkomplexen Systeme*, Math. Ann. vol. 107 (1932–1933) pp. 252–258.

7. D. Zelinsky, *Every linear transformation is a sum of nonsingular ones*, Proc. Amer. Math. Soc. vol. 5 (1954) pp. 627–630.

The Pennsylvania State University