MAXIMAL SUBALGEBRAS OF CENTRAL SEPARABLE ALGEBRAS

M. L. RACINE

ABSTRACT. Let A be a central separable algebra over a commutative ring R. A proper R-subalgebra of A is said to be maximal if it is maximal with respect to inclusion.

Theorem. Any proper subalgebra of A is contained in a maximal one. Any maximal subalgebra B of A contains a maximal ideal mA of A, m a maximal ideal of R, and B/mA is a maximal subalgebra of the central simple R/m algebra A/mA.

More intrinsic characterizations are obtained when R is a Dedekind domain.

In [3] and [4] Dynkin studied maximal subalgebras of simple Lie algebras over an algebraically closed field of characteristic zero and the connection between these and the maximal subgroups of the classical groups. In [7] and [8] the maximal subalgebras of the following classes of central simple algebras were determined: associative, associative with involution, alternative and Jordan. In this paper maximal subalgebras of central separable algebras over a commutative ring R are considered. The ideal structure of such algebras is entirely determined by that of R so it is interesting to consider one-sided ideals and to a lesser extent subalgebras.

We recall some results of [7]. Let F be a field and A a (finite dimensional) central simple algebra over F. So A = M_n(D), D a finite dimensional division algebra over its center F and A acts on an n-dimensional left D vector space V. By a subalgebra of A we understand an F subspace of A which is closed under multiplication, and by maximal subalgebra, a proper subalgebra which is maximal with respect to inclusion. If A = F then 0 is the unique maximal subalgebra of A. If A = F then all maximal subalgebras of A contain 1 and they are exactly the subalgebras of the form:

(I) S(W) = {a ∈ A | Wa ⊆ W}, W any nonzero proper subspace of V.

(II) C_1(E) the centralizer of E a field extension of F lying in A, without intermediate subfields (i.e. F ⊆ L ⊆ E, L a field ⇒ L = E).

Subalgebras of type I can be described intrinsically. If e ∈ A is a projection of V onto W and f = 1 - e then...
While \( W = V \text{Rad}(S(W)) \) is uniquely determined, \( e \), of course, is not.

Our aim is to extend these results to central separable algebras over a commutative ring \( R \). All facts concerning these for which no precise reference is given can be found in [2]. We will need the following

**Lemma.** Let \( N \) be a proper submodule of a finitely generated module \( M \) over a commutative ring \( R \). Then there exists a maximal ideal \( m \) of \( R \) such that \( N + mM \) is a proper submodule of \( M \).

**Proof.** If not, then \( N + mM = M \) \( \forall m \in \text{Max}(R) \). The \( R \) module \( M/N \) is still finitely generated and since \( M = N + mM \) then \( m(M/N) = M/N \) \( \forall m \in \text{Max}(R) \). Therefore \( M/N = 0 \) ([2, 1.8]) a contradiction.

**Theorem.** Let \( A \) be a central separable \( R \) algebra. Then any proper subalgebra of \( A \) is contained in a maximal one. Any maximal subalgebra \( B \) of \( A \) contains a maximal ideal \( mA \) of \( A \), \( m \) a maximal ideal of \( R \), and \( B/mA \) is a maximal subalgebra of the central simple \( R/m \) algebra \( A/mA \).

**Proof.** If \( B \) is a proper subalgebra of \( A \), since \( A \) is finitely generated as an \( R \) module, the Lemma implies that \( B + mA \) is a proper submodule of \( A \) for some \( m \in \text{Max}(R) \). \( B + mA \) is a subalgebra and \( B + mA/mA \) is a proper subalgebra of \( A/mA \) and hence contained in a maximal one, say \( C' \). Let \( C \) be the inverse image of \( C' \) in \( A \). Then \( B \subset C \) which is a maximal subalgebra of \( A \). If \( B \) were maximal to start with, then \( mA \subset B \) since \( B + mA \) is a proper subalgebra, and \( B/mA \) is a maximal \( R/m \) subalgebra of \( A/mA \).

Given a maximal subalgebra \( B \) of a central separable \( R \)-algebra \( A \) then \( m = \{ \alpha \in R | \alpha A \subset B \} \) is uniquely determined. We say that \( B \) is of type \( I \), of type \( II \), or trivial according as \( B = B/mA \) is maximal of type \( I \) or \( II \), or 0 as a subalgebra of the central simple \( R/m \) algebra \( A = A/mA \). The type of \( B \) is well-defined by the uniqueness of \( m \) and that of the type of \( B/mA \). It would be nice to give an intrinsic description of \( B \), that is, without passing to \( A/mA \).

**Proposition 1.** If \( B \) is a trivial maximal subalgebra of a central separable \( R \) algebra \( A \) then either \( A = R \) and \( B = mA \) is a maximal ideal of \( R \), or \( R = S \oplus T \), where \( S \) and \( T \) are subrings of \( R \), \( A = S \oplus A_0 \), \( A_0 \) a central separable \( T \) algebra, and \( B = mA \) where \( m = m' + T \), \( m' \) a maximal ideal of \( S \). Conversely if \( A \) is as above then for any \( m' \in \text{Max}(S) \) the subalgebra \( m' + A_0 \) is maximal and trivial.

**Proof.** Let \( B \) be a trivial maximal subalgebra of a central separable \( R \) algebra \( A \). Then \( B = mA \) for some \( m \in \text{Max}(R) \) and \( A/mA \) is a field. Therefore \( A/mA = R/m \). Now \( R \) is an \( R \) module direct summand of \( A \). If \( A = R \) then we are in the first case above. If not then \( A = R \oplus M \) as an \( R \) module. Therefore \( mA = m \oplus mM = m + M \) and \( mM = M \). Since \( A \) is finitely generated projective so is \( M \). Let \( m_1, \ldots, m_k \in M, f_1, \ldots, f_k \in \text{Hom}_R(M, R) \) be a dual basis for \( M \). Since \( m_i \in mA \) we have
\[ m_i = \sum_{j=1}^{k} a_{ij} m_j, \quad a_{ij} \in \mathfrak{m} \] and the trace ideal of \( M, \tau M \subset \mathfrak{m}. \) But \( R = \text{Ann} \ M \oplus \tau M, \) \( \text{Ann} \ M \) the annihilator of \( M. \) Let \( \pi: R \oplus \tau M \rightarrow R \) be the canonical projection and \( g_i: M \rightarrow R \) be defined by \( g_i(m) = \pi(m m_i), \) \( 1 < i < k. \) Then \( g_i \in \text{Hom}_R(M, R) \) and \( g_i(M) \subset \tau M. \) Thus \( A_0 = \tau M + M \) is a subalgebra of \( A. \) Let \( S = \text{Ann} \ M, T = \tau M. \) Since \( A \) is \( R \) central, \( A_0 \) must be \( T \) central. Taking the component of a separability idempotent of \( A \) coming from \( A_0 \otimes_T A_0^o, \) where \( A_0^o \) denotes the opposite algebra of \( A_0, \) we obtain a separability idempotent for \( A_0 \) which is therefore a central separable \( T \) algebra. The maximality of \( m \) implies the maximality of \( m' = m \cap S \) and we have the first half of the proposition. The converse is clear.

Let us consider next subalgebras of type I. If \( e \neq 0, 1 \) is an idempotent of \( A, \) let \( f = 1 - e. \) Then \( B = eAe + fA + mA \) is a maximal subalgebra of \( A \) of type I for any \( m \in \text{Max}(R). \) The converse, namely, if \( B \) is a maximal subalgebra of \( A \) of type I containing \( mA \) then \( B = eAe + fA + mA \) for some idempotent \( e \in A, \) is not true in general as the following example will show. Let \( R = \mathbb{Z}(p) \) the integers localized at \( p \) an odd prime and let \( 1, i, j, k \) be the standard basis for the Hamiltonian quaternions. The algebra \( A = R 1 + Ri + Rj + Rk \) is a central separable \( R \)-algebra (see [6]) which contains no nontrivial idempotent. However \( A/(p)A \cong M_2(\mathbb{Z}/p\mathbb{Z}) \) the \( 2 \times 2 \) matrices with entries in the field with \( p \) elements. Therefore \( A \) has maximal subalgebras of type I, but none of the form \( eAe + fA + (p)A. \) Some positive results are given in

**Proposition 2.** If (1) \( R \) is Henselian, \( A \) any central separable \( R \)-algebra, or (2) \( R \) is a Dedekind domain and \( A = \text{End}_R M, M \) an \( R \) progenerator, then any maximal subalgebra of \( A \) of type I has the form \( eAe + fA + mA \) for a suitably chosen idempotent \( e \in A, f = 1 - e, \) and a maximal ideal \( m \) of \( R. \)

**Proof.** (1) follows immediately from Azumaya's result [1] that idempotents of \( A/mA \) lift to idempotents of \( A. \)

In case (2) while not every idempotent of \( A/mA \) lifts to an idempotent of \( A \) we will show that given a subspace \( W \) of the \( R/m \) vector space \( V = M/mM \) then there is always a projection of \( V \) onto \( W \) that does lift. Since \( M \) is a progenerator, \( M \) is a faithful finitely generated projective \( R \) module. If \( B \) is a maximal subalgebra of \( A \) of type I containing \( mA \) then \( \overline{B} = B/mA = \{ a \in \overline{A} \mid Wa \subset W \} \) where \( \overline{A} = A/mA \) and \( W \neq 0 \) is a proper subspace of \( V = M/mM (A = \text{End}_{R/m} V). \) Choose a set of preimages in \( M \) of some \( R/m \) basis of \( W \) and let \( N \) be the \( R \) submodule of \( M \) they generate. So \( W = N + mA/mM. \) By Theorem 81.11 of [5] one can choose \( x_1, \ldots, x_n \in M \) such that \( M = a_1 x_1 \oplus \cdots \oplus a_n x_n, N = a_1 b_1 x_1 \oplus \cdots \oplus a_n b_n x_n \) where \( a_i \) are fractional ideals of \( R \) and \( b_1 \supset b_2 \supset \cdots \supset b_n \) are uniquely determined ideals of \( R. \) Let \( k \) be the first index such that \( b_k \subset m \) and let \( P = a_1 x_1 \oplus \cdots \oplus a_{k-1} x_{k-1}. \) Since \( b_i \not\subset m \) for \( i < k, b_i + m = R \) and \( a_i b_i + a_i m = a_i. \) Therefore \( P + mA = N + mA \) and \( P + mA/mM = W. \) Now \( P \) is a direct summand of \( M, \) so let \( e \) be a projection of \( M \) onto \( P \) and \( f = 1 - e. \)
Then $eAe + fA + mA = B$ and therefore $B = eAe + fA + mA$.

In the case where $R$ is arbitrary and $A = \text{End}_R M$, $M$ an $R$ progenerator, then arguing as above one sees that if $B$ is a maximal subalgebra of type I then

$$B = \{ a \in A | (N + mM)a \subset N + mM \} = S(N + mM).$$

Finally let us consider maximal subalgebras of type II. Let $A$ be a central separable algebra over a Dedekind domain $R$, $K$ the quotient field of $R$. Then $\Sigma = \bigotimes R A$ is central simple algebra over $K$ of dimension say, $n^2$ and $A$ is a maximal order of $\Sigma$. If $a \in A$ then its minimal polynomial, $\mu_a(x)$, as an element of $\Sigma$ belongs to $R[x]$, $[9, \text{Theorem IV 1.4'}]$. Let $m \in \text{Max}(R)$. If $\mu_a$, the image of $\mu_a$ in $R/m[x]$ under the canonical homomorphism, is irreducible in $R/m[a]$ then so is $\mu_a$ in $K[a]$. In this case $K[a]$ and $R/m[a]$ are fields ($\bar{a} \in A/mA$). If there are no intermediate subfields between $R/m$ and $R/m[a]$ then we claim that $K[a]$ is a field extension of $K$ without intermediate subfields. Since $R/m \cong R_m/mR_m$ where $R_m$ denotes the localisation of $R$ at $m$, it suffices to prove the claim for principal ideal domains so assume $m = (\pi), \pi \in R$. If $K \subset L \subset K[a]$, we may assume $L = K[b]$ and after clearing denominators and subtracting an element of $K$ we may take $b = \alpha_1 a + \cdots + \alpha_r a_r$, $\alpha_i \in R$, $r < \deg \mu_a$. Dividing by an appropriate power of $\pi$ we may assume that at least one $\alpha_i$ is a unit of $R$. Therefore the image of $b$ in $R/m[a]$ does not belong to $R/m$. So the extension of $R/m$ it generates is $R/m[a]$ contradicting the fact that $\deg \mu_b < \deg \mu_a$. Thus there are no intermediate subfields between $K$ and $K[a]$. Since $[K[a]: K] = [R/m[a]: R/m]$ and $[\Sigma: K] = [A: R/m] = n^2$, the classical double centralizer theorem (e.g. [7, Theorem 4']) implies $[C(a): K] = [C_A(a): R/m]$. Thus if $B$ is the inverse image in $A$ of $C_A(a) \subset A$, then $B = C_A(a) + mA$ and we have proved the first half of

**Proposition 3.** Let $A$ be a central separable algebra over a Dedekind domain $R$. Let $a \in A$ is such that $\mu_a(x)$ is irreducible in $R/m[x]$ for some $m \in \text{Max}(R)$ and if the extension $R/m[a]$ of $R/m$ has no intermediate subfields then $C_A(a) + mA$ is a maximal subalgebra of $A$ of type II. Conversely any maximal subalgebra of $A$ of type II is of that form.

**Proof.** We consider first the case when $A = \text{End}_R(M)$, $M$ an $R$ progenerator. If $B$ is a maximal subalgebra of $A$ of type II then for some $m \in \text{Max}(R)$ there is a $b \in B$ such that $\bar{B} = \bar{C_A(b)}$, where $\bar{A} = A/mA$ and $R/m[b]$ is a field extension of $R/m$ without intermediate subfields. The minimal polynomial of $b$, $\mu_b(x)$, is irreducible in $R/m[x]$ and, by the discussion preceding the proposition, it suffices to show that one can choose an $a \in B$ such that $\bar{a} = \bar{b}$ and $\bar{\mu}_a = \mu_a$. Now $\bar{A} \cong M_n(R/m)$ and if $R/m[b]$ is of degree $k$ then the regular representation provides an embedding $\rho: R/m[b] \to M_k(R/m)$. Since $k|n$, say $n = kq$, this provides us with an embedding of $R/m[b]$ in $M_q(R/m)$ such that $\bar{b}$ corresponds to $q$ blocks $\rho(\bar{b})$ along the diagonal. By the Skolem-Noether Theorem we may write $M/mM = V$ as
$V_1 \oplus \cdots \oplus V_q$, where $V_i$'s are subspaces of dimension $k$ such that $V_i \subset V_i'$. Arguing as in the proof of Proposition 2 we may find submodules $M_i$, $1 \leq i \leq q$ of $M$ such that $M = \bigoplus_{i=1}^q M_i$ and $M_i + mM/mM = V_i$. Let $e_i \in A$ be the corresponding projections. Thus $1 = \sum_{i=1}^q e_i$ and the $e_i$ are mutually orthogonal. Let $b \in B$ be a preimage of $b$ and let $a = \sum_{i=1}^q e_i be_i$. Since $b \in \bigoplus_{i=1}^q e_i A e_i$, $\tilde{a} = \tilde{b}$. Moreover $\mu_a(x)$ has degree $\leq k$. But $\mu_a(b) = 0$. Therefore the degree of $\mu_a = k$ and $\tilde{\mu}_a = \mu_b$.

Let $A$ be any central separable algebra, $B$ a maximal subalgebra of $A$ of type II and $m$ the maximal ideal of $R$ mapping $A$ into $B$. Consider $A^e = A \otimes_R A^o$, where $A^o$ denotes the opposite algebra of $A$; $\rho: A \otimes_R A^o \to \text{End}_R(A)$ induced by

$$\rho(a_1 \otimes a_2)(b) = a_1 ba_2$$

is an isomorphism and $A^e$ is central separable since $A$ is an $R$ progenerator. If $\tilde{B} = C_{\tilde{a}}(\tilde{b})$ with $R/m[\tilde{b}]$ a field extension of $R/m$ without intermediate subfields then identify $\tilde{b}$ with $\tilde{b} \otimes 1 \in A^e/mA^e \cong \tilde{A} \otimes_R \tilde{A}^o \cong \tilde{A} \otimes_{R/m[\tilde{b}]} \tilde{A}^o$.

By the previous case one can find $c \in A^e$ with $\tilde{c} = \tilde{b} \otimes 1$ and $\deg \tilde{\mu}_c = \deg \mu_c$. Let $\nu: A^e \to A$ be induced by $\nu(d) = \rho(d)(1)$. Since

$$\begin{array}{ccc}
A^e & \to & \tilde{A}^e \\
\nu & \downarrow & \downarrow \nu \\
A & \to & \tilde{A}
\end{array}$$

commutes, if we let $a = \nu(c) \in A$ then $\tilde{a} = \tilde{b}$ and $a$ satisfies $\mu_a(x)$ which is therefore equal to $\mu_a(x)$.

We end with an example. Let $n \in \mathbb{Z}$, $n > 1$ and $A = M_n(\mathbb{Z})$. By Propositions 2 and 3 the maximal subalgebras of $A$ are exactly

(I) $B = eAe + fAe + fAf + pA$, where $e \in A$, $e^2 = e \neq 0$, $1$, $f = 1 - e$ and $p$ is any prime of $\mathbb{Z}$.

(II) $B = C_A(a) + pA$, where $p$ is any prime of $\mathbb{Z}$, $a \in A$ whose minimal polynomial $\mu_a$ is of degree $q$ a prime divisor of $n$ and is irreducible modulo $p$.

REFERENCES