AZUMAYA ALGEBRAS
AND DERIVATIONS

by

Harold J. Stolberg

Report 71-12

February, 1971

Introduction

Let k be a field of prime characteristic p, C a purely inseparable finite dimensional field extension of exponent 1, and & the restricted C-Lie algebra of k derivations in C. It was shown by Jacobson that there is a Galois correspondence between subfields of C over R and restricted C-Lie subspaces of)9. In the classical theory of central simple R algebras, where C over k is a Galois extension, group extensions of the multiplicative group of C by the Galois group of C over k give rise, via an appropriate embedding into a ring, to central simple k algebras split by C. Hochschild, [5], worked out an analogue of this theorem for the purely inseparable case where the group extensions are replaced by certain regular Lie algebra extensions of C by D, C regarded as an abelian Lie algebra. In [8], Jacobson gave a more explicit construction of central simple k algebras split by C using the existence of a derivation 9 in \$ such that $\mathrm{Ker}\ 3 = k$ and $C[B] = \mathrm{End}_{v}(C)$o This was generalized by Hoechsmann in [6] to discuss embeddings of simple k algebras using the 'cyclic' derivation approach of Jacobson,

Recently, S. Yuan [11] has generalized Hochschild's results to purely inseparable commutative ring extensions of exponent 1. It is natural to inquire whether Jacobson's approach can also be generalized to such ring extensions. In this paper we show that indeed it can if we assume the existence of a derivation d which will play the role of Jacobson's 'cyclic' derivation. In particular if R is a commutative ring of prime characteristic.

C a purely inseparable commutative R algebra such that C is finitely generated projective as an R module and there exists an R derivation 9 such that Ker g = R and C[d] = End$_R$(C), then we obtain Azumaya R algebras split by C (equivalently central separable R algebras split by C)y as certain quotients of the ring of differential polynomials over C. We use this result to compute the Chase-Rosenberg group of equivalence classes of Azumaya R algebras split by C and ultimately^ under additional hypotheses^ the relative Brauer group of C over R.

The main results in this paper arose from the possibility of interpreting Hochschild's results in a Hopf algebra setting and obtaining Azumaya R algebras via Hopf algebra extensions. We hope to report on this project in a latter paper.

1. Preliminaries

Throughout this paper R will be a fixed commutative ring with unit of prime characteristic $p > 0$.

Let C be a commutative R algebra and let ∂ be a derivation on C such that $\operatorname{Ker} \partial = R$. Assume ∂ satisfies a polynomial

$$X = a_0 t + a_1 t^{p} + \dots + a_i t^{p^i} + \dots + a_n t^{p^n}$$

with the a_i in R. For c in C denote by L_c the endomorphism of C effected by multiplication by c. From the formula

$$(\partial + L_c)^p = \partial^p + L(\partial^{p-1}c + c^p) \qquad ([3]\ p.201)$$

it is easy to see that

$$X(\partial + L_c) = L(\delta c)$$

where

$$\delta(c) = \sum_{i=0}^{n} a_i[c^{p^i} + (\partial c)^{p^{i-1}} + (\partial c^{p})^{p^{i-2}} + \dots + (\partial c^{p^{i-1}})]$$

is an element of R. Furthermore

$$\delta : C^+ \to R^+$$

is a group homorphism.

Let A be an Azumaya R algebra [4]. Following [11], we call C a splitting subalgebra of A if C is a maximal commutative subalgebra of A such that A is a projective left C module. By [3, Prop, 2.4, p. 37] the map $\varphi : C \otimes A^\circ \to \operatorname{End}_C(A)$ given by $\varphi(c \otimes a^\circ)x = cxa$ is an isomorphism. Let A(C,R) denote the group of equivalence classes of Azumaya R algebras with splitting subalgebra C, defined in [3,p,38]. We refer the reader to that paper for more details.

2. Rings of differential polynomials

Let C be a commutative R algebra with 3 a derivation of C such that Ker S = R. Assume C is a finitely generated projective R module and $Horn_R(C^C) = C[d]$. It is well known that C determines a unique up to order decomposition of R into a direct sum $R = \oplus_{i=1}^{m} Re_i$, the e_i orthogonal idempotents such that Ce_i is a finitely generated projective Re_i module of rank r_i with $Horn_{Re_i}(Ce_i, Ce_i) = Ce_i[e_i d]$ [9,p.45]. It follows from [9. Thm.2.4] that $e_i d$ satisfies a unique monic polynomial

2.1 $$X_i(t) = a_0 t + a_1 t^P + \ldots + a_j t^{P^j} + \ldots + t^{P^{n_i}}$$

with $P^{n_i} = r_i$. Setting $X = SX_i(t)$ in $C[t] = \oplus_{i=1}^{m} Ce_i[t]$ we see that 9 satisfies a polynomial

$$X(t) = ct_0 L- -r a_1 t^P - r_{co} + a_1 t^{P^1} + \cdots + a_n t^{P^n}$$

with the a_i in R and a_n a non-zero idempotent. Furthermore

2.2 $$\{f \in C[t] | f(3) = 0\} = X(t)C[t] \qquad [9, Cor.2.5]$$

Let C[tjd] denote the noncommutative ring of differential polynomials with coefficients in C defined by tc = ct + d(c). An easy induction argument shows that

$$t^r c = ct^r + B_{r\,1}(Bc)t^{r-1} + B_{r\,2}(U^2c)t^{r-2} + \ldots + (a^r c)$$

where we use the notation $B_{r,I}$ for the binomial coefficients, and so X(t) is in the center of C[t,9] since $t^P c = ct^P + 3^P(c)$.

Let a be an element of R and define Cft^B^a] to be the quotient ring obtained by factoring C[tjd,cc] by the two-sided ideal J generated by X(t)-cc. Note that since X(t)*a is in the center of C[t,a], J = (X(t)-a)C[t,a] and

2.3 $C[t,a,a] = \oplus_{i=1}^{m} Ce_i[t,e_ia,ae_i]$,

where we use 2.2 to define $Ce_i[t,e_i\delta,ae_i]$ in the obvious manner.

3, Azumaya R algebras.

In this section we give a complete description of Azumaya R algebras split by C in terms of the rings C[t,3,,a] described in the previous section. We remind the reader that the term Azumaya R algebra is equivalent to central separable R algebra. We begin with a lemma.

Lemma 3.1. Let C be a commutative R algebra with a a derivation of C such that Ker d = R. Assume C is a finitely generated projective R module and $Hom_R(C,C) = C[3]$. Then for any a in R, C[t,a,a] is finitely generated projective as a C module and hence as an R module.

Proof: Assume first C is a finitely generated projective R module of rank r. Then by [9, Thm.2.4], a satisfies a unique monic polynomial

$$X(t) = a_0t + a_1t^p + \ldots + a_it^{p^i} + \ldots + t^{p^n}$$

with $p^n = r$. We will show C[tj9,a] is actually free over C of rank = p^n. By definition $\{t^i \mid i \geq 0\}$ is a left C basis for C[tjS]. Since X(t)-a has degree p^n, no nontrivial element of J = (X-a)C[t*d] can have degree less than p^n. Hence $(t^i \mid 0 \leq i < p^n)$ are C linearly independent and since they clearly generate C[t^a] modulo J, they form a basis over C for C[t,9,a]. In the general case we have by 2.3 that

$C[t,a,\alpha] = \oplus_{i=1}^{m} Ce_i[t,e_i\delta,\alpha e_i]$ where Ce_i is a finitely generated projective Re_i module of rank r_i and the conditions of the lemma are satisfied for Re_i, Ce_i, e_i. Hence by the first part of the proof, $Ce_i[t,e_i\delta,\alpha e_i]$ is a finitely generated projective Ce_i module. Thus $C[t,a,a]$ is finitely generated projective as a C module. Finally C being finitely generated projective as an R module implies $C[t,d,a]$ is also.

Theorem 3.2. Let C be a commutative R algebra with δ a derivation of C such that Ker $d = R$. Assume C is finitely generated projective as an R module and $End_R(C) = C[\delta]$. Let A be an R algebra containing C. Then A is an algebra with C as a splitting subalgebra if and only if $A \cong C[t;\delta,a]$ for some a in R.

Proof: To show that $C[t,\delta,a]$ is an Azumaya R algebra with C as a splitting subalgebra it suffices by (2.3) to assume C is finitely generated projective of rank r as an R module. In this case the minimal polynomial (2.1) of δ is monic of degree $p^n = r$. If q is a prime ideal of R, it is easy to see that

2.7 $$C[t,a,a]_q \cong C_q[t,\delta_q,\bar{\alpha}]$$

where δ_q is the unique extension of δ to C_q, $\bar{\alpha}$ is the image of a under the map $R \to R_q$ [lo^p. 2]. It follows from [2, p. 180], and Lemma 3.1 that $C[t,\delta,a]$ is an Azumaya R algebra if it is one locally at very prime q of R. The assertion that C is a splitting subalgebra of $C[t,\delta,\alpha]$ is again local, hence by (3.3) we need only show that $C[t,\delta,a]$ is an Azumaya R algebra with C as a splitting subalgebra under the additional hypothesis that R is a local ring. In this case C is a free R module of rank $r = p^m$ = degree of minimal polynomial $X(t)$ of δ, $x(t)$ as in 2.1. In view of Lemma 3.1, we may write every element of $C[t,\delta,a]$ uniquely as a polynomial $b_0 + b_1t + \ldots + b_lt^l$ where $l < p^m$. Let $c \in C$ be arbitrary. We have

$t^k c = L«_{1O}^{k}$_~ $B_{,K,1}$. $(d^X c)t^{k-i}$, and hence, using the Lie commutator brackets,

[b_Q + b_xt +...+ $b_j t$^c] = $S_{j=Q}^{\ell}$ bj(t^Jc - ct^J)

3.4

$= \Sigma_{J=1}^{\ell} b_J \Sigma_{i=1}^{J} B_{J,i}(\partial^i c)t^{J-i}$

Note that the last expression is a polynomial in t of degree less than *I* with constant term b-^c) + $b_2 d^2$ (c) +...+ b^3^I (c). Hence for b_- + b_nt -f..$_o$+ $b.t^{\ell}$ to commute with all c in C we must have b_1a(c) + $b_2 d^2$(c) +...+ b^B^{ℓ}(c) = 0 for all c in C. However it follows easily from (2.2) that the set fS^{3}"!^{0}_<1 i < p^n] is ^{a} C-linearly independent set in End$_-$(C) Thus the only polynomials in C[t,3,a] commuting with elements of C are the zero degree polynomials, the elements of C. We conclude that C is a maximal commutative subalgebra of C[t,d,a]. In addition we have shown that if b_O + b_It +...+ b^t^I, is an element of C[t,,S,al,t J≥ 1,, there exists some element c in C such that [b_o + b_it +...+ b_u.t^{ℓ},c] ^ 0 and the latter is a polynomial in t of degree < £. A central element u of C[t,d,cc] must be in C, and in order to commute with t it must have 3(u) = Oo Hence u is in R and C[t,d,a] is central. To show C[t,a,cc] is separable, observe that C[t,a,a]®R/m ≅ C/mC[t,3,$\bar{a}$] where m is the maximal ideal of R, 9 is extended to C/mC and $\bar{a}$ = a + mC[t,3,a]o Since C[£] = End_(C), we have C/mC[a] = End^$_m$ (c/mC). Let I be a non-zero 2-sided ideal of C/mC[t,a,$\bar{oc}$] o Setting $^{\pi}$t * t + mC[t,^,a] we effect the computations in (3.4) for a non-zero element $\bar{b}$ in I. By several applications of the Lie bracket with the appropriate elements in C/mC we obtain a non-zero element $\bar{c}$ in I D C/mC. Since I n C/mC is an ideal of C/mC stable under a and C/mCfa] = End_$_y$ (C/mC) this

implies I D C/mC = C/mC which in turn implies I = C/mC[t^3^ā]o
Hence C/mC[t^9^a] is simple and we conclude Ctt^djOt] is separable by [2, p.180]. Thus C[tjd,a] is an Azumaya R algebra^ and by lemma 3.1 and the above arguments,, C is a splitting subalgebra„

Let A be an Azumaya R algebra containing C as a splitting subalgebra. To finish the proof of theorem 3.2 we need the following lemma, a special case of a more general result proved in [11, Lemma 6]•

Lemma. Let A be an Azumaya R algebra containing C as a splitting subalgebrao Then every R derivation of C to itself can be extended to an inner derivation of Ao

Thus given an Azumaya R algebra A containing C as a splitting subalgebra, there exists a deA such that cd - dc = $\partial(c)$ for all c in C. We observe that X(d) commutes with every element of C, since $cd^{p^i} - d^{p^i}c = a^{p^i}(c)$ for all i, and hence is an element of C. However since 3(X(d)) =

= [X(d),d] = 2^=o a i [d $^{p^i}$ *d J = o* X<d) = a is an element of R. It is immediate that we have an R algebra homomorphism from C[t,3,oc] to A such that t —* d and the elements of C are mapped to themselves. By [4, Cor. 2.6] this is an isomorphism and $A \cong C[t,s,a]$ for some a in R as asserted.

Remark: Derivations satisfying the hypothesis $C[a] = End_R(C)$ exist* For example if C admits a p-basis u_i, $1 < i < r$ over R, then the R derivation on C given by $QU_1 = 1$,

a u i = ^u l##*u i-l^ $^{p-1}$, i > 1 satisfies the above relation. [11, Lemma 7]

Recall [4 ^ p. 38] that two Azumaya R algebras A_1 and A_2 with splitting subalgebra C are isomorphic under an admissible isomorphism a if $a : A_1 \to A_2$ is an isomorphism such that it is the identity on C. From here on until the end of this section, assume the hypothesis of theorem 3.2; that is, C is a commutative R algebra with 3 a derivation of C such that Ker S = R and C is finitely generated projective as an R module with $End_R(C) = C[a]$. The next theorem classifies admissible isomorphism classes of Azumaya R algebras containing C as a splitting subalgebra.

Theorem 3.5. The Azumaya R algebras Ctt^S^a-^] and $C[t_J,3,a_2]$ are isomorphic under an admissible isomorphism if and only if

a_1 " a_2 = 6 ^) for some *leC.*

Proof: Assume a : $C[t,3,a_1] \to C[t,B,a_2]$ is an admissible isomorphism. Since *[v(t) ,c]* = [a(t) ,cr(c)] = or[t,c] = a(S(c)) = a(c) we have [cr(t)-t, c] = 0 for all c in C. Hence a(t) = t + *I* for some -teC. In particular a]_ = cr(X(t)) = X(a(t))=X(t+^)=X(t) +6 *(I)* = = a« + 6(£) and thus a_1 - a^ = 6(£). Conversely^ it is clear that if cci - a_2 = M£) the correspondence t -~>t + *I* determines a well defined ring homomorphism a from C[t, a^oų] to C[t,ajOC$_2$l which is the identity on C. By [4 *9* Cor. 2.6] a is an admissible isomorphism.

The last theorem in this section deals with the multiplication in the abelian group A(C^R) of equivalence classes of Azumaya R algebras containing C as a splitting subalgebra. We refer the reader to [4_3 p.41] for the relevant definitions and further details.

Theorem 3.6. C[t^s^a]_ + a_2l =~ C[t,9,a_1] • C[^9,a_2] where • denotes the product in the group A(C^R).

Proof: Set *A^* = Ctt.a^aj^], A_2 = C[tJ,3,a_2]. By [4 , p.41] A_1 • A_2 = End$_{A_1 0A_2}$ ^1 ®C ^2^ *^S the product of A_1 and A_2 in A(C^R) where both A_1 and A_2 are viewed as left C modules, and A_1 $\otimes_C$ A_2 as a right A^ ® A_2 module. The product A_1 • A_2 is an Azumaya R algebra and the injection C«••••> End$_{A_1 \otimes A_2}$*(A_1* ^c A_2) given by c—?%L(c®l) embeds C as a splitting subalgebra of A_1 • A_2. Define <p : C[t^]- -^ End$_{A_1 A_2}$ (A^ 0$_C$ A_2) by cp(c) = L(c®l) for all c in C and cp(t) = L(t ® 1 + 1 ® t) • It is easy to see that cp(t) G End$_{A_1 0A_2}$ (A_1 $\otimes_C$ A_2) if and only if cp(t)(l®c) = cp(t) (c®l) for all c in C since l®c = c®l in A_1 $\otimes_C$ A_2. But cp(t) o L(1®C) - cp(t)o L(c®l)=t®c +ietx:-tc®l-c®t = (ct-tc)®l + + l®(tc-ct) = L[a(c)®l] = cp(a(c)). Hence cp is a well defined ring homomorphism. Finally cp(X(t)) = X(cp(t)) = X(L(t®l+l®t) = = Lta-^^l + l®a_2) = L[(ai+a_2)®l] = cp(a^ + a_2)^ hence cp extends to a homomorphism

$\bar{\varphi} : C[t,\beta,a_1+a_2] \to End_{A_1 \otimes A_2}(A_1 \otimes_C A_2)$ leaving C fixed,

By [4, Cor. 2.6] $\bar{\varphi}$ is an isomorphism. Thus $C[t,\beta,a_1+a_2] \cong$

$\cong C[t,\beta,a_1] \cdot C[t,\beta,a_2]$.

Corollary 3.7. $A(C,R) \cong R^+/b(C^*)$. If P(C) denotes the group of isomorphism classes of projective C modules of rank 1 and P(C) = 0; then $B(C/R) \cong R^+/\delta C^+$, where B(C/R) denotes the Brauer group of Azumaya R algebras split by C.

Proof: Theorem 3.2 and Theorem 3.6 define an onto group homomorphism from R^+ to A(C,R) via $a \mapsto C[t,\beta,a]$. The kernel of this homomorphism is $\delta(C^+)$ by Theorem 3.5. The last statement of the theorem follows from the fact that if P(C) = 0 then $B(C/R) \cong A(C,R)$. [4, Prop. 2.13].

Remarks: In the case that R is field of characteristic p and C a purely inseparable extension of exponent 1 the above results appear in Hoechsmann [6], and Jacobson [7],[8]. Our proofs follow theirs with minor changes.

JR.eferences

1. Auslander, M. and O. Goldman, The Brauer group of a commutative ring, Trans. Amer. Math. Soc, J7 (I960), 367-409.

2. Bourbaki, N., Algèbre Commutative, Chap. 1 et 2, Hermann, Paris, 1962.

3. Cartier, P., Questions de rationalité des diviseurs en géometrie algébrique, Bull. Soc. Math., France, 86 (1958), 177-251.

4. Chase, S., and A. Rosenberg, Amitsur cohomology and the Brauer group. Memoirs, Amer. Math. Soc., 5£ (1965), 34-79.

5. Hochschild, G., Simple algebras with purely inseparable splitting fields of exponent one, Trans. Amer. Math. Soc, 29 (1955), 477-489.

6. Hoechsmann, K., Simple algebras and derivations, Trans. Amer. Math. Soc., 108 (1963), 1-12.

7. Jacobson, N., Abstract derivation and Lie algebras, Trans. Amer. Math. Soc, £2 (1937), 206-224.

8. ______________, p-a.]gebras of exponent p, Bull. Amer. Math. Soc, £3 (1937), 667-670.

9. Yuan, Shuen, Logarithmic derivatives, Bull. Soc Math. France, 96 (1968), 41-52.

10. ______________, Inseparable galois theory of exponent one, Trans. Amer. Math. Soc, to appear.

11. ______________, Central separable algebras with purely inseparable splitting rings of exponent one, Trans. Amer. Math. Soc, to appear.

cs
2/15/71