Can. J. Math., Vol. XXV, No. 4, 1973, pp. 881–887

SUBGROUPS OF CENTRAL SEPARABLE ALGEBRAS

E. D. ELGETHUN

Introduction. In [**8**] I. N. Herstein conjectured that all the finite odd order sub-groups of the multiplicative group in a division ring are cyclic. This conjecture was proved false in general by S. A. Amitsur in [**1**]. In his paper Amitsur classifies all finite groups which can appear as a multiplicative subgroup of a division ring. Let D be a division ring with prime field k and let G be a finite group isomorphic to a multiplicative subgroup of D. If kG is the group algebra of G over k, the natural k-algebra homomorphism from kG to D has as its image a division subring D^* of D which is finite dimensional over its center F and generated as a vector space over F by the images of the elements of G. Thus the problem of analyzing the finite subgroups of a division ring can be reduced to the situation where the division ring is finite dimensional as a vector space over its center. M. Auslander and O. Goldman laid the foundations for the study of central separable algebras and the Brauer group $\mathbf{B}(R)$ of a commutative ring [**3**]. It was shown in [**6**, Chapter V] that if R is a commutative ring with no idempotents other than 0 and 1 then every class in $\mathbf{B}(R)$ is represented by a not necessarily unique central separable algebra D whose only idempotents are 0 and 1 and any central separable R-algebra A is isomorphic to $\mathrm{Hom}_D(E, E)$ for some such D and some finitely generated, projective D-module E. Thus in $\mathbf{B}(R)$, the central separable algebras with no idempotents other than 0 and 1 play a role analogous to the role division algebras play when R is a field. We study the finite subgroups of the multiplicative group of a central separable R-algebra A with no idempotents other than 0 and 1 which generate A as an R-module. It is necessary to limit the classification to these generating groups G since subalgebras of arbitrary central separable R-algebras need not be separable over their centers. This problem is not encountered in finite dimensional central division algebras. We obtain the following classification of the groups G which can appear as generating subgroups of A over R. If R has finite characteristic then $G \simeq H \times K$ where H is an abelian p-group and K is a cyclic group of order relatively prime to p. In case the order of G is a unit in R, G is cyclic. If R has characteristic 0 the results are only partially complete. If R is a Dedekind domain or if the order of G is a unit in R, then G is isomorphic to a subgroup of the multiplicative group of a division ring. We conjecture that in the characteristic 0 case G is always a subgroup of the multiplicative group of a division ring. Since every division ring which is finite dimensional over its center is central separable, we see that

Received May 1, 1972. This research constitutes part of the author's Ph.D. thesis written at Colorado State University under the direction of Professor F. R. DeMeyer.

all finite subgroups of the multiplicative group of a division ring appear. Section 2 contains some related examples and applications.

This paper draws heavily on the results of M. Auslander and O. Goldman in [**2**] and [**3**] which contain the undefined terminology used here. We will refer to the groups classified by Amitsur in [**1**] as A-groups. Throughout this paper Z will denote the ring of rational integers and an unadorned "$\otimes$" will mean "$\otimes_R$". All rings have a unit denoted "1" and all ring homomorphisms carry 1 to 1.

1. The classification. The classification of the groups G which generate a central separable algebra with no idempotents other than 0 and 1 over a commutative ring divides into two cases depending whether or not the characteristic of the ring is finite.

We consider first the case where the characteristic of R is finite.

PROPOSITION 1. *Let R be a commutative ring of finite characteristic and let A be a central separable R-algebra with no idempotents other than* 0 *and* 1. *Let G be a finite multiplicative group and let $\phi : RG \to A$ be an R-algebra homomorphism from RG onto A. Then $R = A$.*

Proof. Case 1: R has characteristic p. In this case the prime ring of R is the field $k \simeq Z/(p)$. Form the group algebra kG which is a ring with minimum condition. Then $kG \simeq \oplus\sum B_i$ where B_i is an indecomposable two-sided ideal of kG [**4**, p. 378]. Let N be the radical of kG. Then $B_i \simeq kGe_i$ for some central idempotent e_i and the radical of B_i is Ne_i.

$$RG \simeq R \otimes_k kG \simeq R \otimes_k (\oplus\sum B_i) \simeq \oplus\sum (R \otimes_k B_i).$$

There exists a central idempotent f_i in $R \otimes_k B_i$ with $\phi(f_i) = 1$ for some i. Then for any central idempotent f_j in $R \otimes_k B_j$ orthogonal to f_i we have $0 = \phi(f_i f_j) = \phi(f_i)\phi(f_j) = \phi(f_j)$. Let $B = B_i$ and $U = Ne_i$. Then we have $\phi : R \otimes_k B \to A \to 0$. Let I be the least two-sided ideal in $R \otimes_k B$ containing $(0) \subseteq R$ and $U \subseteq B$. By [**12**, p. 184] we have $(R \otimes_k B)/I \simeq R \otimes_k B/U$. We have the short exact sequence

$$0 \to U \to B \xrightarrow{\pi} B/U \to 0$$

so tensoring with R over k gives

$$0 \longrightarrow R \otimes_k U \longrightarrow R \otimes_k B \xrightarrow{1 \otimes \pi} R \otimes_k B/U \longrightarrow 0$$

and $R \otimes_k U = \text{kernel}(1 \otimes \pi) \simeq I$. We have the following diagram:

$$\begin{array}{ccccc} R \otimes_k B & \xrightarrow{\phi} & A & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \\ (R \otimes_k B)/I & \xrightarrow{\theta} & A/\phi(I) & \longrightarrow & 0 \end{array}$$

where α and β are the natural homomorphisms and $\theta : (R \otimes_k B)/I \to A/\phi(I)$ defined by $\theta(\sum r_i \otimes b_i + I) = \phi(\sum r_i \otimes b_i) + \phi(I)$ so θ is an R-algebra epimorphism. Now B/U is a semi-simple ring with minimum condition so $B/U \simeq \oplus\sum C_i$ where C_i is a simple ring. By Wedderburn's theorem, $C_i \simeq M_{n_i}(D_i)$ where D_i is a division ring and since C_i is finite, D_i is a finite field extension F of k.

$$R \otimes_k B/U \simeq R \otimes_k (\oplus \sum C_i) \simeq \oplus\sum (R \otimes_k C_i) \simeq (R \otimes_k B)/I \to A/\phi(I) \to 0.$$

Since $\phi(I)$ is nilpotent, $A/\phi(I)$ is a ring suitable for building idempotents [**9**, p.54] and hence has no idempotents other than 0 and 1. Arguing as before, for $C = C_i$. $F = D_i$, $n = n_i$, we have that

$$R \otimes_k C \simeq R \otimes_k M_n(F) \simeq M_n(R \otimes_k F) \xrightarrow{\theta} A/\phi(I).$$

Let kernel$(\theta) = K$. Then $M_n(R \otimes_k F)/K \simeq A/\phi(I)$. By [**9**, p. 40], $K = M_n(L)$ where L is an ideal in $R \otimes_k F$. Since $A/\phi(I)$ has no idempotents other than 0 and 1 and

$$M_n(R \otimes_k F)/M_n(L) \simeq M_n(R \otimes_k F/L) \simeq A/\phi(I),$$

$M_n(R \otimes_k F/L)$ has no idempotents other than 0 and 1 so $n = 1$ and $(R \otimes_k F)/L \simeq A/\phi(I)$ and $A/\phi(I)$ is commutative. Now $\phi(I)$ is nilpotent so [**6**, p. 54] $\phi(I) = mA$ for some nilpotent ideal m of R. Since A/mA is commutative and central separable over R/m by [**6**, p. 46] we have $A/mA = R/m$ and $\text{rank}_R(A) = \text{rank}_{R/m}(A/mA) = 1$ so $R = A$.

Case 2: The characteristic of R is n. Let $n = \prod {p_i}^{e_i}$ where $\{p_i\}$ is the complete set of primes dividing n. The prime ring of R is isomorphic to $Z/(n)$ and by the Chinese Remainder Theorem, $Z/(n) \simeq \oplus \sum Z/({p_i}^{e_i})$. Since R has no idempotents other than 0 and 1, $p = p_i$, $e = e_i$ and $n = p^e$ for some i. Thus pR is a nilpotent ideal in R and R/pR has characteristic p. By [**6**, p. 54], pR corresponds to the nilpotent two-sided ideal pA in A so $pA \subseteq$ radical(A). By the same procedure for constructing idempotents modulo the radical in [**9**, p. 53], A/pA has no idempotents other than 0 and 1 and is central separable over R/pR by [**6**, p. 44]. Consider the diagram

$$\begin{array}{ccccc} RG & \xrightarrow{\phi} & A & \longrightarrow & 0 \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\delta} & & \\ (R/pR)G & \xrightarrow{\theta} & A/pA & \longrightarrow & 0 \end{array}$$

where η and δ are the natural R-algebra homomorphisms and

$$\theta : (R/pR)G \to A/pA$$

is defined by

$$\theta(\sum (r_i + pR)g_i) = \delta\phi(\sum r_i g_i) = \sum \phi(r_i g_i) + pA.$$

https://doi.org/10.4153/CJM-1973-092-8 Published online by Cambridge University Press

Then θ is an R-algebra epimorphism and the diagram commutes. By Case 1, $A/pA = R/pR$. Since $\text{rank}_R(A) = \text{rank}_{R/pR}(A/pA) = 1$ we have $A = R$.

By Proposition 1 we have reduced the problem of classifying the finite multiplicative subgroups of a central separable R-algebra A with no idempotents other than 0 and 1 which generate A as an R-module to classifying the finite multiplicative subgroups of a commutative ring of finite characteristic with no idempotents other than 0 and 1.

PROPOSITION 2. *Let R be a commutative ring of finite characteristic with no idempotents other than* 0 *and* 1. *Let G be a finite multiplicative subgroup of R. Then $G = H \times K$ where H is an abelian p-group and K is a cyclic group of order relatively prime to p.*

Proof. Let B be the ring generated by G and $P = Z/(p^e)$. Then B is a subring of R so has no idempotents other than 0 and 1 and is a finite commutative ring with minimum condition. By [**12**, p. 205], B is a primary ring. Let $N = \text{radical}(B)$. Then $B/N \simeq M_n(F)$ where F is a finite field. Since N is nilpotent, B/N has no idempotents other than 0 and 1 so $B/N \simeq F$ and B is local. Let $f : B \to B/N \simeq F$ be the natural epimorphism. Let $\mathbf{G}(B)$ and $\mathbf{G}(F)$ denote the group of units of B and F respectively. Then f induces a group epimorphism $\mathbf{G}(B) \to \mathbf{G}(F) \to 0$ with kernel $\mathbf{K}(B) = 1_B + N$ and $\mathbf{G}(B)/\mathbf{K}(B) \simeq \mathbf{G}(F)$. Let $\delta(B) = \text{card}\,\mathbf{G}(B)/\text{card}\,B$. Then by [**7**, p. 380], $\delta(B) = \delta(F)$. Now $\text{card}\,B = p^k$, $\text{card}\,N = p^s$ and $\text{card}\,F = p^{k-s}$ for some integers k and s so we have

$$\text{card}\,\mathbf{G}(B) = p^k(p^{k-s} - 1)/p^{k-s} = p^s(p^{k-s} - 1).$$

Since $\mathbf{G}(B) \simeq \mathbf{K}(B) \times \mathbf{G}(F)$ and $\text{card}\,\mathbf{K}(B) = p^s$, $G \subseteq \mathbf{K}(B) \times \mathbf{G}(F)$. Since $(\text{card}\,\mathbf{K}(B), \text{card}\,\mathbf{G}(F)) = 1$, $G = H \times K$ where H is an abelian p-group and K is a cyclic group of order relatively prime to p.

THEOREM 3. *Let R be a commutative ring of finite characteristic and let A be a central separable R-algebra with no idempotents other than* 0 *and* 1. *Let G be a finite multiplicative group and let $\phi : RG \to A$ be an R-algebra homomorphism. If ϕ is an epimorphism then $\phi(G) = H \times K$ where H is an abelian p-group and K is a cyclic group of order relatively prime to p. If ϕ is not necessarily onto but if the order of G is a unit in R then $\phi(G)$ is cyclic.*

Proof. If ϕ is an epimorphism then we have the result by Propositions 1 and 2. If the order of G is a unit in R so that RG is separable over R let B be the image of ϕ. Then B is a separable subalgebra of A with no idempotents other than 0 and 1. If C is the center of B then B is central separable over C and by Propositions 1 and 2, $\phi(G) = H \times K$ where H is an abelian p-group and K is a cyclic group of order relatively prime to p. Since $R \subseteq C$, the order of G is a unit in C so p does not divide the order of G so $\phi(G) = K$ and is cyclic.

We now consider the case where the characteristic of R is zero.

https://doi.org/10.4153/CJM-1973-092-8 Published online by Cambridge University Press

LEMMA 4. *Let R be a Dedekind domain and let A be a central separable R-algebra with no idempotents other than* 0 *and* 1. *Let K be the quotient field of R. Then $A \otimes K$ is a division ring.*

Proof. Let $\Lambda = A \otimes K$. Then Λ is a central simple K-algebra so by [**3**, p. 387] A is a maximal order in Λ over R and A is a heriditary R-algebra. By [**2**, p. 12] there is a maximal order Ω in the division algebra Δ equivalent to Λ^0 in the Brauer group of K, $\mathbf{B}(K)$, and a finitely generated and projective Ω-module E such that $A \simeq \mathrm{Hom}_\Omega(E, E)$, where E is indecomposable, finitely generated and projective over A and $\Omega = \mathrm{Hom}_A(E, E)$. Now A is contained in the central separable R-algebra $\mathrm{Hom}_R(E, E)$ and Ω is its commutator subalgebra so Ω is central separable and heriditary over R. Since A has no idempotents other than 0 and 1, E is indecomposable over Ω so by [**2**, p. 8], $E \otimes K$ is a simple $\Omega \otimes K$-module so

$$A \otimes K \simeq \mathrm{Hom}_\Omega(E, E) \otimes K \simeq \mathrm{Hom}_{\Omega \otimes K}(E \otimes K, E \otimes K)$$

[**6**, p. 14] which is a division ring by Schur's lemma.

We see that any finite subgroup of A is an **A**-group. If the order of the group G in A is a unit in R it is no longer necessary to assume R is a Dedekind domain.

LEMMA 5. *Let R be a commutative ring of characteristic* 0 *and let A be a central separable R-algebra with no idempotents other than* 0 *and* 1. *Let G be a finite multiplicative group and let $\phi : RG \to A$ be an R-algebra homomorphism from RG onto A. If the order of G is a unit in R then $\phi(G)$ is an* **A**-*group.*

Proof. Let the order of G be n and let P be the ring of quotients of Z with respect to the multiplicatively closed set $\{n, n^2, \ldots\}$. Form the group algebra PG and let B be the image under ϕ of PG in A. PG is separable over P so B is separable over P and has no idempotents other than 0 and 1. Let C be the center of B. By [**6**, p. 55], B is separable over C and C is a separable P-algebra. P is a noetherian integrally closed domain and C is a finitely generated separable P-algebra with no idempotents other than 0 and 1 so by [**10**, p. 473], C is a noetherian integrally closed domain which is finitely generated, projective and separable over P. Thus by [**10**, p. 475], C is a Dedekind domain and B is central separable over C with no idempotents other than 0 and 1 so by Lemma 4, $B \otimes_C K$ is a division ring where K is the quotient field of C.

We note here that if the order of G is a unit in R then RG is a separable R-algebra and a homomorphic image B of RG is central separable over its center C and C is a separable R-algebra. Thus the hypothesis that A be a central separable R-algebra is not necessary since we can reduce to that situation using C in place of R. This also applies to the finite characteristic case when the order of G is a unit in R.

At present it is not known if the restriction that the order of the group be a unit in R is necessary for Lemma 5. Combining Lemmas 4 and 5 we have

THEOREM 6. *Let R be a commutative ring of characteristic 0 and let A be a central separable R-algebra with no idempotents other than 0 and 1. Let G be a finite multiplicative group and let $\phi : RG \to A$ be an R-algebra homomorphism from RG into A. If R is a Dedekind domain or if the order of G is a unit in R then $\phi(G)$ is an* **A***-group.*

Proof. If R is a Dedekind domain we have the result by Lemma 4. If the order of G is a unit in R, consider $\phi(RG) = B \subseteq A$. Then since RG is separable over R, B is central separable over its center C with no idempotents other than 0 and 1 and $\phi : RG \to B \to 0$. The order of G is a unit in C so by Lemma 5, $\phi(G)$ is an **A**-group.

2. Examples and applications. (1) (See [**6**, Problem 3, p. 147]). Let D be the algebra of real quaternions. Then D is a division algebra over the real numbers with basis $1, i, j, k$ with the usual rules for multiplication. Let G be the binary octahedral group of order 48 [**1**, p. 374] generated by $\{x, y, z\}$ with

$$x^8 = 1,\ x^4 = y^2,\ yxy^{-1} = x^{-1}$$
$$zx^2z^{-1} = y,\ zyz^{-1} = x^2y,\ z^3 = 1.$$

In [**1**, p. 376], Amitsur shows we can choose

$$x = (1 + i)/\sqrt{2},\ y = j,\ z = -(1 + i + j + k)/2.$$

Let $R = Z(\sqrt{2})$ which is a principal ideal domain and let $A = R \cdot 1 + R \cdot a + R \cdot b + R \cdot ab$ where

$$a = x = (1 + i)/\sqrt{2},\ b = -zx = (i + j)/\sqrt{2},$$
$$ab = z^{-1} = (-1 + i + j + k)/2.$$

Then A is a central separable R-algebra with no idempotents other than 0 and 1 not in the zero class of $\mathbf{B}(R)$. We have that G is a subgroup of A and $RG \to A \to 0$ with RG a non-separable R-algebra and G an **A**-group.

(2) (See [**3**, p. 388]). Let k = real numbers, $R = k[x, y]$ with $x^2 + y^2 = 0$. R is an integral domain. Let Δ be the algebra of quaternions over k and $A = \Delta \otimes_k R$. Then A is central separable with no idempotents other than 0 and 1 over R. If m is the ideal generated by x and y then $A/mA \simeq \Delta$ so A is not in the zero class of $\mathbf{B}(R)$. Since $-1 = (x/y)^2$ in K, the quotient field of R, K is a splitting field for Δ so K splits A. Thus $A \otimes K \simeq (\Delta \otimes_k R) \otimes K$ is the ring of 2×2 matrices over K. We see by this example that R is an integral domain and all subgroups of A are **A**-groups but there are subgroups of $A \otimes K$ which are not **A**-groups. In Lemma 4 where R is a Dedekind domain, this cannot happen.

(3) The following application is due to F. R. DeMeyer. Let $\mathbf{C}$ be the complex numbers and let ξ be any indecomposable complex vector bundle over a compact, connected Hausdorff space $\mathbf{X}$. Let R be the ring of continuous complex valued functions on $\mathbf{X}$. Then R is a commutative ring whose only idempotents are 0 and 1. R. Swan [**11**] has given a one-to-one correspondence between the indecomposable, finitely generated, projective modules E over R and the indecomposable complex vector bundles ξ over $\mathbf{X}$ so that the finite subgroups of $\mathrm{Hom}_R(E, E)$ correspond to the finite groups of bundle automorphisms of ξ. Now $\mathrm{Hom}_R(E, E)$ is a central separable R-algebra with no idempotents other than 0 and 1 and every positive integer is invertible in R so by Theorem 6, the only finite subgroups of $\mathrm{Hom}_R(E, E)$ are $\mathbf{A}$-groups. But let G be a finite subgroup of $\mathrm{Hom}_R(E, E)$ and consider the natural $\mathbf{C}$-algebra homomorphisn ϕ from $\mathbf{C}G$ into $\mathrm{Hom}_R(E, E)$. If B is the image of ϕ then B has no idempotents other than 0 and 1, B is separable over its center C, and C is a finitely generated, separable $\mathbf{C}$-algebra with no idempotents other than 0 and 1. Thus, $C = \mathbf{C}$ and $B = \mathbf{C}$ so G is contained in $\mathbf{C}$ and is, therefore, cyclic. We conclude that the only finite groups of automorphisms of indecomposable complex vector bundles are cyclic. We conjecture that the same result is true for the finite subgroups of the automorphism group of indecomposable real vector bundles.

References

1. S. A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. *80* (1955), 361–386.
2. M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc. *97* (1960), 1–24.
3. ——— *The Brauer group of a commutative ring*, Trans. Amer. Soc. *97* (1960), 347–409.
4. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras* (Interscience, New York, 1962).
5. F. R. DeMeyer, *Projective modules over central separable algebras*, Can. J. Math. *21* (1969), 39–43.
6. F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Mathematics, No. *181* (Springer-Verlag, Heidelberg, 1971).
7. H. K. Farahat, *The multiplicative group of a ring*, Math. Z. *87* (1965), 378–384.
8. I. N. Herstein, *Finite multiplicative subgroups in division rings*, Pacific J. Math. *3* (1953), 121–126.
9. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloq. Publ. Vol. XXXVII (Providence, R.I., 1956).
10. G. J. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. *122* (1966), 461–479.
11. R. Swan, *Vector bundles and projective modules*, Trans. Amer. Math. Soc. *105* (1962), 264–277.
12. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I (Princeton U. Press, Princeton, 1958).

Colorado State University,
Fort Collins, Colorado;
University of North Florida,
Jacksonville, Florida