

THE GROUP CHARACTER AND SPLIT GROUP ALGEBRAS

GEORGE SZETO

G. J. Janusz defined a splitting ring R for a group G of order n invertible in R . Then, the Brauer splitting theorem was given by G. Szeto which proves the existence of a finitely generated projective and separable splitting ring for G . Let M be a RG -module and R_0 be a subring of R . Then we say that M is realizable in R_0 if and only if there exists a R_0G -module N such that $M \cong R \otimes_{R_0} N$ as left RG -modules. This paper gives a characterization of splitting rings in terms of the concept of realizability as in the field case. The other main results in this paper are the structure theorem for split group algebras and some properties of group characters.

Throughout this paper we assume that the ring R is a commutative ring with no idempotents except 0 and 1, that the group G has order n invertible in R , and that all RG -modules are unitary left RG -modules. We know that the order of G , n , is invertible in R if and only if RG is separable.

1. In this section we study splitting rings in two ways. That is, splitting rings can be characterized in terms of the concept of realizability and structure theorem for split group algebras will be given.

PROPOSITION 1. *Assume the ring R has no idempotents except 0 and 1, and P is a finitely generated and projective R -module. Then P is a faithful R -module.*

Proof. Because P is a finitely generated and projective R -module, $R = \alpha(P) + \text{Tr}(P)$ where $\alpha(P)$ is the kernel of the operation of R on P and $\text{Tr}(P)$ is the trace ideal of P in R ([3], Proposition A.3). Thus $\alpha(P)$ is a left direct summand of R ([3], Th. A.2(d)). But R has no idempotents except 0 and 1 so that $\alpha(P) = 0$. Therefore P is a faithful R -module.

Using the above proposition we can have the following definition given by G. J. Janusz.

DEFINITION 1. A ring R is a splitting ring for G if the group algebra RG is the direct sum of central separable R -algebras, each equivalent to R in the Brauer group of R ; that is,

$$RG \cong \bigoplus_{i=1}^s \text{Hom}_R(P_i, P_i),$$

where $\{P_i\}$ are finitely generated and projective R -modules. The number of different conjugate classes in G is equal to s ([5], Definition 6).

DEFINITION 2. Let M be a RG -module and R_0 be a subring of R . Then we say that M is realizable in R_0 if and only if there exists a R_0G -module N such that $M \cong R \otimes_{R_0} N$ as left RG -modules.

THEOREM 2. If R is strongly separable over R_0 and R is a splitting ring for G , $RG \cong \bigoplus_{i=1}^s \text{Hom}_R(P_i, P_i)$; then P_i is realizable in R_0 for all i if and only if R_0 is a splitting ring for G .

Proof. If R_0 is a splitting ring for G , that is, if

$$R_0G \cong \bigoplus_{i=1}^s \text{Hom}_{R_0}(P_i, P_i),$$

then $P_i \cong R_0 \otimes_{R_0} P_i$. This means that P_i is realizable in R_0 for all i .

Conversely, if P_i is realizable in R_0 for all i , then there is R_0G -module M_i such that $P_i \cong R \otimes_{R_0} M_i$ for all i . Since R is a strongly separable R_0 -algebra, $R_0 \cdot 1$ is a R_0 -direct summand of R . By the definition of a split group algebra, P_i is a finitely generated and projective R -module for each i ; so M_i is a finitely generated and projective R_0 -module for each i . In fact, because $R \cong (R_0 \cdot 1 \oplus R'_0)$ for some R_0 -module R'_0 ,

$$P_i \cong (R_0 \cdot 1 \oplus R'_0) \otimes_{R_0} M_i \cong (R_0 \cdot 1 \otimes_{R_0} M_i) \oplus (R'_0 \otimes_{R_0} M_i).$$

Thus $M_i \cong R_0 \cdot 1 \otimes_{R_0} M_i$ is a R_0 -direct summand of P_i . On the other hand, P_i is finitely generated and projective over R and R is finitely generated and projective over R_0 ; so P_i is finitely generated and projective over R_0 . Therefore M_i is a finitely generated and projective R_0 -module. We then have

$$\begin{aligned} RG &\cong \bigoplus_{i=1}^s \text{Hom}_R(P_i, P_i) \cong \bigoplus_{i=1}^s \text{Hom}_R(R \otimes_{R_0} M_i, R \otimes_{R_0} M_i) \\ &\cong R \otimes_{R_0} \left(\bigoplus_{i=1}^s \text{Hom}_{R_0}(M_i, M_i) \right). \end{aligned}$$

Noting that M_i is a finitely generated projective and faithful R_0 -module for each i by Proposition 1, we have that $\text{Hom}_{R_0}(M_i, M_i)$ is a central separable R_0 -algebra with a unique central idempotent in R_0G for each i ([2], Proposition 5.1). Therefore $R_0G \cong \bigoplus_{i=1}^s \text{Hom}_{R_0}(M_i, M_i)$. This proves that R_0 is a splitting ring for G .

We are going to discuss the structure of a split group algebra over some kinds of rings, in particular, over a Dedekind ring.

THEOREM 3. *Let P denote a finitely generated and projective R -module. (a) If R is a Dedekind domain, then $\text{Hom}_R(P, P)$ is free as a R -module. Consequently, a split group algebra is a free R -module. (b) If R is a local ring or a semi-local ring or a principal ideal Dedekind domain, then $\text{Hom}_R(P, P)$ is a matrix ring over R .*

Proof. Because P is a finitely generated and projective R -module, $\text{Hom}_R(P, P) \cong P \otimes_R \text{Hom}_R(P, R)$. Let the rank of P be k . Then $P \cong \bigoplus_{i=1}^{k-1} R \oplus I$, $\sum_{i=1}^{k-1} R$ are $k - 1$ copies of R and I is in the class group of R . By substitution,

$$\begin{aligned} P \otimes_R \text{Hom}_R(P, R) &\cong \left(\bigoplus_{i=1}^{k-1} R \oplus I \right) \otimes_R \text{Hom}_R \left(\bigoplus_{i=1}^{k-1} R \oplus I, R \right) \\ &\cong \left(\bigoplus_{i=1}^{k-1} R \oplus I \right) \otimes_R \left(\bigoplus_{i=1}^{k-1} \text{Hom}_R(R, R) \oplus \text{Hom}_R(I, R) \right) \\ &\cong \left(\bigoplus_{i=1}^{k-1} R \oplus I \right) \otimes_R \left(\bigoplus_{i=1}^{k-1} R \oplus I^{-1} \right) \\ &\cong \left(\bigoplus_{i=1}^{(k-1)^2} R \right) \oplus \left(\bigoplus_{i=1}^{k-1} R \otimes_R I^{-1} \right) \oplus \left(\bigoplus_{i=1}^{k-1} R \otimes_R I \right) \oplus (I \otimes_R I^{-1}) \\ &\cong \left(\bigoplus_{i=1}^{(k-1)^2} R \right) \oplus \left(\bigoplus_{i=1}^{k-1} I^{-1} \right) \oplus \left(\bigoplus_{i=1}^{k-1} I \right) \oplus R \\ &\cong \left(\bigoplus_{i=1}^{(k-1)^2+1} R \right) \oplus \left(\bigoplus_{i=1}^{2k-2} R \right) \\ &\cong \left(\bigoplus_{i=1}^{k^2} R \right). \text{ This proves part (a).} \end{aligned}$$

For part (b), because P is a free module of finite rank over each of these rings, $\text{Hom}_R(P, P)$ is a matrix ring over R . For a local ring R , see Theorem 12 in Chapter 9 in [6]. For a semi-local ring R , see the remark on Theorem 3.6 in [2]. For a principal ideal Dedekind domain, see Exercises 22.5 and 56.6 in [4].

REMARK. There exist split group algebras over those rings in the above theorem from the proof of the Brauer splitting theorem ([8], Th. 2).

THEOREM 4. *Let R denote a Dedekind domain, P a finitely generated and projective R -module and $P(R)$ the class group of R . Then, for $P \cong \bigoplus_{i=1}^{k-1} R \oplus J$, there is I in $P(R)$ such that $I^k = J^{-1}$ where $k = \text{rank}(P)$ and J is in $P(R)$ if and only if $\text{Hom}_R(P, P)$ is a matrix ring over R of order k by k .*

Proof. Because $\text{Hom}_R(P, P)$ is a matrix ring over R if and only if there exists I in $P(R)$ such that $P \otimes_R I \cong \bigoplus \sum_{i=1}^k R$, a direct sum of k -copies of R (Lemma 9, [7]). But $P \cong \bigoplus \sum_{i=1}^{k-1} R \oplus J$ for some

$$\begin{aligned} J \text{ in } P(R); \text{ so } & \left(\left(\bigoplus_{i=1}^{k-1} R \right) \oplus J \right) \otimes_R I \cong \bigoplus \sum_{i=1}^k R, \\ & \left(\bigoplus_{i=1}^{k-1} I \right) \oplus (J \otimes_R I) \cong \bigoplus \sum_{i=1}^k R, \\ & \left(\bigoplus_{i=1}^{k-1} I \right) \oplus (J \cdot I) \cong \bigoplus \sum_{i=1}^k R \end{aligned}$$

where we use the fact that $J \otimes_R I \cong J \cdot I$. But

$$\left(\bigoplus_{i=1}^{k-1} I \right) \oplus (J \cdot I) \cong \bigoplus \sum_{i=1}^{k-1} R \oplus I^k \cdot J;$$

then $I^k \cdot J = R$. So, if we can prove the fact that $J \otimes_R I \cong J \cdot I$, the theorem is proved. In fact, because $J \cdot I$ is in $P(R)$ and $J \cdot I$ is projective and finitely generated, the exact sequence

$$0 \longrightarrow \text{Ker}(\pi) \longrightarrow J \otimes_R I \xrightarrow{\pi} J \cdot I \longrightarrow 0$$

splits. Thus $J \otimes_R I \cong \text{Ker}(\pi) \oplus J \cdot I$. Let R_M denote the quotient ring with respect to a prime ideal M .

$$R_M \otimes_R (J \otimes_R I) \cong R_M \otimes_R \text{Ker}(\pi) \oplus R_M \otimes_R (J \cdot I),$$

that is, $R_M \cong R_M \otimes_R \text{Ker}(\pi) \oplus R_M$. Hence $R_M \otimes_R \text{Ker}(\pi) = 0$ for all prime ideals M . On the other hand, because $\text{Ker}(\pi)$ is finitely generated, $\text{Ker}(\pi) = 0$ by Nakayama's lemma. This proves that $J \otimes_R I \cong J \cdot I$. Therefore the theorem is completed.

COROLLARY 5. *Keep the same notations as Theorem 4. If the rank of P and the order of J are relative prime, then $\text{Hom}_R(P, P)$ is a matrix ring over R .*

Proof. It suffices to prove that there exists I in $P(R)$ such that $J^{-1} = I^k$ by Theorem 4. Consider the subgroup generated by J^k . Because k , the rank of P and the order of J are relative prime, this subgroup is the same as the subgroup generated by J . Hence $J = J^{ik}$ for some i from 1 to the order of J minus 1. Thus $I = (J^{-1})^i$ is what we want. In fact, $I^k = (J^{-1})^{ik} = (J^{ik})^{-1} = J^{-1}$.

DEFINITION 3. The subgroup of $P(R)$, U , is called the $R - Z$ group for a finitely generated and projective R -module P if $U = \{I \text{ such that } I \text{ is in } P(R) \text{ and } I \cdot P = P\}$. (For this group see Theorem 14 and Theorem 15 in [7]).

THEOREM 6. (a) Let R be a Dedekind domain and $H = \{J \text{ such that } P \cong \bigoplus_{i=1}^{k-1} R \oplus J \text{ and } \text{Hom}_R(P, P) \text{ is a matrix ring over } R \text{ where } J \text{ is in } P(R)\}$. Then H is a subgroup of $P(R)$. (b) Assume the $R - Z$ group is equal to $P(R)$. Then, P is a free R -module if and only if $\text{Hom}_R(P, P)$ is a matrix ring over R .

Proof. For any J' and J'' in H , there are I' and I'' in $P(R)$ such that $J' \cdot (I')^k = R$ and $J'' \cdot (I'')^k = R$ by Theorem 4. We then have $J' \cdot J'' \cdot (I' \cdot I'')^k = (J' \cdot I'^k)(J'' \cdot I''^k) = R$. Thus $J' \cdot J''$ is in H . Also, for any J in H , there is I in $P(R)$ such that $J \cdot I^k = R$. We then have $J^{-1} \cdot (I^k)^{-1} = R$, that is, $J^{-1} \cdot (I^{-1})^k = R$. Thus J^{-1} is in H . Therefore H is a subgroup of $P(R)$. This proves part (a).

For part (b), one way is clear. If P is free, then $\text{Hom}_R(P, P)$ is a matrix ring over R . Conversely, if $\text{Hom}_R(P, P)$ is a matrix ring over R , $P \cong \bigoplus_{i=1}^{k-1} R \oplus J$ with J in H by Theorem 4. But the $R - Z$ group is equal to $P(R)$; then $I^k = R$ for all I in $P(R)$. Thus $H = 0$. Therefore P is a free R -module.

REMARK. (a) Corollary 5 can be expressed in terms of the $R - Z$ group as following. If the exponent of the $R - Z$ group and the order of J is relative prime, then $\text{Hom}_R(P, P)$ is a matrix ring over R .

(b) Theorem 4, Corollary 5, and Theorem 6 tell us the structure of $\text{Hom}_R(P, P)$, any component of a split group algebra. We thus have the similar structure theorems for group algebras by considering P_1, P_2, \dots, P_s and J_1, J_2, \dots, J_s in the same time where $P_i, i = 1, 2, \dots, s$ are in the definition of a split group algebra RG with

$$P_i \cong \bigoplus_{i=1}^{k_i-1} R \oplus J_i \text{ as in Theorem 4.}$$

2. Let us recall the group character of a finitely generated and projective RG -module.

DEFINITION 4. Let M be a finitely generated and projective RG -module with dual basis $\{F_1, F_2, \dots, F_u; X_1, X_2, \dots, X_u\}$. Then the group character $T_M: G \rightarrow R$ is defined by $T_M(g) = \sum_{i=1}^u F_i(gX_i)$ for any g in G ([8], § 2).

In this section some properties of group characters will be given. Let K be a field and $K(\varphi)$ be $K(\varphi(g_1), \varphi(g_2), \dots, \varphi(g_n))$ where φ is a group character for $G = \{g_1, g_2, \dots, g_n\}$. We know that $K(\varphi)$ is a separable extension over K . In the ring case, $R[T^i]$ can be proved as a strongly separable R -algebra where T^i is a group character for G . Finally, we point out the usual orthogonality relations on group

characters in the ring case.

THEOREM 1. (a) Let T^i be T_{P_i} where P_i is in the definition of a split group algebra RG (see Definition 1). Then $T^i(g)$ is a constant for all splitting rings R with the same prime ring R_0 for a given group G , where g is in G . (b) $T^i(g)$ is a sum of n_i^{th} -roots of 1 where g is in G and $g^{n_i} = 1_G$, the identity of G .

Proof. Since R is a splitting ring for G , $RG \cong \bigoplus_{i=1}^s \text{Hom}_R(P_i, P_i)$. Setting $R' = R[\sqrt[m]{1}]$ where $\sqrt[m]{1}$ is a primitive m^{th} -root of 1 and m is the exponent of G , we have

$$\begin{aligned} R'G &\cong R' \otimes_R RG \cong R' \otimes_R \left(\bigoplus_{i=1}^s \text{Hom}_R(P_i, P_i) \right) \\ &\cong \bigoplus_{i=1}^s \text{Hom}_{R'}(R' \otimes_R P_i, R' \otimes_R P_i) . \end{aligned}$$

By Lemma 1 in [8], R' is also a splitting ring for G . Clearly,

$$T_{R' \otimes_R P_i} = T^i \dots (1) .$$

Next, consider $R'' = R_0[\sqrt[m]{1}]$. It is a splitting ring for G ([8], Th. 2); that is, $R''G \cong \bigoplus_{i=1}^s \text{Hom}_{R''}(P_i'', P_i'')$. We then have

$$R'G \cong R' \otimes_{R''} R''G \cong \bigoplus_{i=1}^s \text{Hom}_{R'}(R' \otimes_{R''} P_i'', R' \otimes_{R''} P_i'') .$$

Thus $T_{P_i''} = T_{R' \otimes_{R''} P_i''} \dots (2)$, and for each i

$$\text{Hom}_{R'}(R' \otimes_{R''} P_i'', R' \otimes_{R''} P_i'') = \text{Hom}_{R'}(R' \otimes_R P_i, R' \otimes_R P_i) .$$

The later implies that $R' \otimes_{R''} P_i'' \cong (R' \otimes_R P_i) \otimes_{R'} J$, where J is in the class group of R' ([7], Lemma 9). Consequently,

$$T_{R' \otimes_{R''} P_i''} = T_{R' \otimes_R P_i} \dots (3) .$$

From (1), (2) and (3), $T^i = T_{P_i''}$. But R'' depends on R_0 and G only so that T^i is a constant for all splitting rings R with the same prime ring R_0 for a given group G , $i = 1, 2, \dots, s$. This proves part (a).

The proof for part (b) divides into two cases. Case 1. $\text{Char}(R)$ is equal to p^r where p is a prime integer and r is a positive integer. Then the prime ring of R is $Z/(p^r)$ where Z is the set of integers. Let $\sqrt[m]{1}$ be a primitive m^{th} -root of 1 where m is the exponent of G . Then $R' = Z/(p^r)[\sqrt[m]{1}]$ is a splitting ring for G ([8], Th. 2); that is, $R'G \cong \bigoplus_{i=1}^s \text{Hom}_{R'}(P_i, P_i)$. Since R' is a local ring (see the proof of Theorem 2 in [8]) and P_i is a finitely generated and projective R' -module for each i , P_i is a free R' -module for each i ([6], Th. 12 in Chapter 9). Therefore $T^i(g)$ is a sum of n_i^{th} -roots of 1 where g is in

G and $g^{n_i} = 1_G$, the identity of G .

$\text{Char}(R)$ is equal to 0. Then the prime ring of R is $Z(n)$, the quotient ring of Z with respect to the multiplicative closed set $\{n, n^2, \dots\}$. By the Brauer splitting theorem again, $R' = Z(n)[\sqrt[n]{1}]$ is a splitting ring for G ; that is $R'G \cong \bigoplus_{i=1}^n \text{Hom}_{R'}(P_i, P_i)$. Since R' is a principal ideal Dedekind domain, P_i is a free R' -module for each i ([4], Exercises 22.5 and 56.6). Therefore $T^i(g)$ is a sum of n_i^{th} -roots of 1 as in Case 1.

THEOREM 2. *Let $R[T^i]$ denote $R[T^i(g_1), T^i(g_2), \dots]$ where G is equal to $\{g_1, g_2, \dots, g_n\}$. Then $R[T^i]$ is a strongly separable R -algebra for each i .*

Proof. As in the above theorem, R divides into two cases. Case 1. $\text{Char}(R) = 0$. Then the prime ring of R is $Z(n)$, the quotient ring of integers with respect to the multiplicative closed set $\{n, n^2, \dots\}$. We know that the quotient field of $Z(n)[T^i(g)]$ is $Q(T^i(g))$ for each g in G and the quotient field of $Z(n)[\sqrt[n]{1}]$ is $Q(\sqrt[n]{1})$, where Q is the set of rationals. Because $Z(n)[\sqrt[n]{1}]$ is separable over $Z(n)$ by the Brauer splitting theorem, $Q(\sqrt[n]{1})$ is unramified over Q ([1], Th. 2.5). But $Q(T^i(g))$ is a subset of $Q(\sqrt[n]{1})$ and contains Q ; so $Q(T^i(g))$ is unramified over Q ([9], Proposition 3.2.4). Thus $Z(n)[T^i(g)]$ is separable over $Z(n)$ by Theorem 2.5 in [1] again. This implies that $R \otimes_{Z(n)} Z(n)[T^i(g)]$ is a separable R -algebra ([2], Corollary 1.6); so $R[T^i(g)]$, the homomorphic image of $R \otimes_{Z(n)} Z(n)[T^i(g)]$, is also a separable R -algebra. On the other hand, because $T^i(g)$ is integral over R , $R[T^i(g)]$ is a strongly separable R -algebra. Therefore $R[T^i]$ is a strongly separable R -algebra.

Case 2. $\text{Char}(R)$ is p^r for some prime integer p and a positive integer r . Then the prime ring of R is $Z/(p^r)$. We know that $Z/(p^r)[T^i(g)]$ is a local ring with the nilpotent maximal ideal $(p)/(p^r)[T^i(g)]$. Also, $Z/(p^r)[T^i(g)]$ is a Noetherian ring such that

$$(p)/(p^r)[T^i(g)] \cap Z/(p^r) = (p)/(p^r).$$

Let M denote $(p)/(p^r)[T^i(g)]$. Then $(p)/(p^r) \cdot (Z/(p^r)[T^i(g)])_M$ is equal to $M \cdot (Z/(p^r)[T^i(g)])_M$ for $T^i(g)$ is in M , $(\)_M$ is a local ring at M .

$$Z/(p^r)[T^i(g)]/(p)/(p^r)[T^i(g)] \cong Z/(p)(T^i(g))$$

is a separable $Z/(p)$ extension. Therefore $Z/(p^r)[T^i(g)]$ is a separable $Z/(p^r)$ -algebra ([1], § 1). Then as in Case 1, $R[T^i]$ is a strongly separable R -algebra by the same arguments. This proves the theorem.

REMARK. We know that an element α in the separable closure of R is separable means that it satisfies a separable polynomial over R . This is also equivalent to that $R[\alpha]$ is a separable R -algebra ([5], Lemma 2.7). Then $T^i(g)$ is a separable element such that $T^i(g)$ is a sum of n_i^{th} -roots of 1. Because these roots satisfy the separable polynomial, $X^{n_i} - 1 = 0$, all roots are also separable elements. But it is not true that a sum of separable elements is separable. The following example is due to G. J. Janusz. Let R be $Z(2)$, the quotient ring of Z with respect to the multiplicative closed set $\{2, 2^2, \dots\}$, S be $R[i]$ where $i^2 = -1$. Then S is strongly separable over R . An element $a + ib$ is a separable element if and only if $(a + ib) - (a - ib) = 2ib$ is invertible in S ([5], Lemma 2.1). Hence the separable elements are of the form $a + i2^j$ where a is in $Z(2)$ and $j = 0, 1, 2, \dots$. Clearly, $1 + i$ and $1 + i2$ are separable elements but $(1 + i) + (1 + i2) = (2 + i3)$ is not.

We conclude this section by pointing out the usual orthogonality relations on group characters as in the field case.

THEOREM 3. *If $T^i = T_{P_i}$, for $i = 1, 2, \dots, s$, then*

$$\sum_g T^i(g)T^j(g^{-1}) = n\delta_{ij},$$

where n is the order of G and δ_{ij} is the Kronecker delta.

Proof. Let E_i be the i^{th} -central primitive idempotent of RG ,

$$E_i = \sum_g \frac{k_i T^i(g^{-1})}{n} g,$$

where $k_i = \text{rank}(P_i)$ ([8], Lemma 5). Taking the characters in both sides, we have the answer.

REMARK. By using the above theorem and standard methods, the other usual orthogonality relations on group characters can be proved (see § 31 in [4]).

The author wishes to thank Professors F. R. DeMeyer and G. J. Janusz for their many valuable suggestions and discussions.

BIBLIOGRAPHY

1. M. Auslander and D. Buchsbaum, *On ramification theory in Noetherian rings*, Amer. J. Math. **81** (1959), 749-765.
2. M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367-409.
3. ———, *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960), 1-24.

4. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associated Algebras*, New York, Interscience, 1962.
5. G. J. Janusz, *Separable algebra over commutative rings*, Trans. Amer. Math. Soc. **122** (1966), 461-479.
6. D. G. Northcott, *An introduction to homological algebra*, Cambridge University Press, London, 1962.
7. A. Rosenberg and D. Zelinsky, *Automorphisms of separable algebras*, Pacific J. Math. **2** (1961), 1109-1118.
8. G. Szeto, *On the Brauer splitting theorem*, Pacific J. Math. **31** (1969), 505-512.
9. E. Weiss, *Algebraic number theory*, McGraw Hill Book Co., 1963.

Received August 18, 1969.

BRADLEY UNIVERSITY
PEORIA, ILLINOIS

