ON ORDERS IN SEPARABLE ALGEBRAS

D. G. HIGMAN

Introduction. The present note began from the observation that the arguments produced by J-M. Maranda in developing his very interesting theory of representations of groups by automorphisms of modules over Dedekind rings **(4, 5)** were applicable without essential change to arbitrary orders, instead of just group rings, provided that a suitable generalization of Theorem 1 of **(4)** could be supplied. We prove that when the ring of integers is a Dedekind ring a certain integral ideal $I(\mathfrak{G})$ vanishes if and only if $\mathfrak{G}$ is an order in a separable algebra, thus extending Maranda's results to these orders and indicating that an essential change can be expected in going beyond this case.

The author is indebted to Professor Maranda for the opportunity of studying **(5)** before its publication.

Notations. The following notations will be fixed throughout.

$\mathfrak{g}$ = Dedekind ring.
K = quotient field of $\mathfrak{g}$.
A = (finite dimensional linear associative) algebra over K with identity element e.
$\mathfrak{G}$ = $\mathfrak{g}$-order in A.

1. The ideal $I(\mathfrak{G})$. By a *two-sided G-module* we shall understand a module T having $\mathfrak{G}$ both as a ring of left and right operators such that

$$(\zeta u)\eta = \zeta(u\eta), \quad eu = ue = u \qquad (\zeta, \eta \in G, u \in T),$$

which is finitely generated over $\mathfrak{g}$.

For such a two-sided $\mathfrak{G}$-module T we shall denote by $Z(T)$ the $\mathfrak{g}$-module of all $\mathfrak{g}$-homomorphisms ϕ of $\mathfrak{G}$ into T such that

$$\phi(\zeta\eta) = \zeta\phi(\eta) + \phi(\zeta)\eta \qquad (\zeta, \eta \in \mathfrak{G}), \tag{1}$$

and by $B(T)$ the submodule of $\phi \in Z(T)$ for which there exist elements $u \in T$ such that

$$\phi(\omega) = \omega u - u\omega \qquad (\omega \in \mathfrak{G}). \tag{2}$$

We shall use $H(T)$ to denote the quotient module $Z(T)/B(T)$.

In the language of cohomology theory $Z(T)$ and $B(T)$ are modules of 1-*dimensional cocycles* and *coboundaries* respectively, and $H(T)$ is the 1-*dimensional cohomology* group for T.

Received October 2, 1954; in revised form May 31, 1955.

A *right* $\mathfrak{G}$*-module*, or simply a $\mathfrak{G}$*-module* will be understood to be a module having $\mathfrak{G}$ as a ring of right operators such that e acts as the identity operator, which is finitely generated over $\mathfrak{g}$. If M and N are $\mathfrak{G}$-modules, the module $\mathrm{Hom}(M, N)$ of all $\mathfrak{g}$-homomorphisms of M into N can be turned into a two-sided $\mathfrak{G}$-module by defining

$$(f\omega)(u) = \omega(f(u)), \quad (\omega f)(u) = f(u\omega) \qquad (\omega \in \mathfrak{G}).$$

Taking $T = \mathrm{Hom}(M, N)/\mathfrak{a}\mathrm{Hom}(M, N)$, where $\mathfrak{a}$ is an integral ideal of $\mathfrak{g}$, we obtain the module $Z(T)$ of $\mathfrak{a}$-*modular binding systems* of M and N and the submodule of $\mathfrak{a}$-modular binding systems *strongly equivalent to* 0 **(4)**.

We shall be particularly concerned with the annihilators $I(T)$ of the $\mathfrak{g}$-modules $Z(T)$, and the intersection for all two-sided $\mathfrak{G}$-modules T of the ideals $I(T)$, which intersection we shall denote by $I(\mathfrak{G})$. From the above we see that a theorem to the effect that $I(\mathfrak{G}) \neq 0$ would be a "suitable" generalization of Maranda's Theorem 1 in **(4)**. In §3 we shall prove that $I(\mathfrak{G}) \neq 0$ if and only if A is separable. In §4 we shall show how to construct $I(\mathfrak{G})$ from an invariant bilinear form on A; in particular, if $\mathfrak{G}$ is the group ring of a finite group of order N then $I(\mathfrak{G})$ is the principal ideal generated by N.

2. Separable algebras. In order to obtain the results mentioned in §1 we shall make use of a characterization of separable algebras which we established as a corollary to general results in **(2)**. For the convenience of the reader we include a direct proof here.

Assume that A is an algebra over a field K with identity element e. Assume furthermore that there exists an *invariant* bilinear form f on A, that is, f is a non-singular bilinear form defined on A with values in K such that

$$f(xy, z) = f(x, yz) \qquad (x, y, z \in A). \tag{3}$$

This is equivalent to the assumption that A is a *Frobenius algebra* **(2)**.

If g is a second invariant bilinear form on A, then

$$g(x, y) = f(x, yc) \tag{4}$$

with c a unit of A **(2)**.

Let $a_1, \ldots, a_n$ be a basis of A over K, then

$$f(a_i, \bar{a}_j) = \delta_{ij} = f(\hat{a}_j, a_i) \tag{5}$$

defines two dual bases $\bar{a}_1, \ldots, \bar{a}_n$ and $\hat{a}_1, \ldots, \hat{a}_n$ of A which coincide if and only if A is symmetric. Simple computation using (3) shows that, for $a \in A$,

$$a_i a = \sum s_{ij} a_j,\ s_{ij} \in K, \text{ if and only if } a\bar{a}_j = \sum \bar{a}_j s_{ji}, \tag{6}$$

while

$$aa_i = \sum a_j t_{ji},\ t_{ji} \in K, \text{ if and only if } \hat{a}_i a = \sum t_{ij} \hat{a}_j. \tag{6'}$$

Using (5), (6) and (6′) we verify that, for $a \in A$,

$$c_f(a) = \sum \bar{a}_j a a_j = \sum a_j a \hat{a}_j$$

https://doi.org/10.4153/CJM-1955-053-1 Published online by Cambridge University Press

is an element of the center Z of A, independent of the choice of basis $a_1, \ldots, a_n$, and that c_f is a Z-homomorphism of A into Z. In particular $c_f(A)$ is an ideal of Z. c_f can be referred to as the *Casimir operator* determined by f **(2)**.

If g is an invariant bilinear form related to f by (4) then clearly

$$c_f(a) = c_g(ca) \qquad (a \in A).$$

Hence $c_f(A)$ is independent of the choice of invariant bilinear form f, and we can write $c_f(A) = c(A)$.

THEOREM 1. *Each of the following conditions is necessary and sufficient for an algebra A with identity element e to be separable.*

(i) *A is a Frobenius algebra such that $c(A)$ = the center of A.*

(ii) *Corresponding to a basis $a_1, \ldots, a_n$ of A there is a set of elements $\tilde{a}_1, \ldots, \tilde{a}_n$ of A such that*

$$\sum \tilde{a}_i a_i = e \tag{7}$$

and such that, for $a \in A$,

$$a_i a = \sum s_{ij} a_j,\ s_{ij} \in K, \text{ implies } a\tilde{a}_i = \sum \tilde{a}_j s_{ji}. \tag{8}$$

We note that some time ago Hochschild **(3**, Theorem 5**)** established the equivalence with separability of a slightly different form of Condition (ii).

Proof of Theorem 1. *Separability implies* (i): If A is separable, there exists a finite extension E of K such that A_E is isomorphic with a direct sum of full matrix rings over E,

$$A_E \simeq \sum{}^{\circ} E_{n(\alpha)}.$$

For a basis of A_E over E choose the matrix units $e^{\alpha}{}_{ij}$ of the $E_{n(\alpha)}$. Then

$$f^*(e^{\alpha}{}_{ij}, e^{\beta}{}_{kl}) = \delta_{\alpha\beta}\delta_{il}\delta_{jk}$$

defines a symmetric invariant bilinear form f^* on A_E. In fact $f^*(x, y) = S(xy)$, where S is the reduced trace on A_E **(1**, p. 33**)**. For the dual basis of A_E determined by f^* we have

$$\overline{e^{\alpha}{}_{ij}} = e^{\alpha}{}_{ji}.$$

Setting $b^* = \sum e^{\alpha}{}_{ii}$ we can verify that

$$c_{f^*}(b^*) = \sum \overline{e^{\alpha}{}_{ij}} b^* e^{\alpha}{}_{ij} = I.$$

Now f^* induces an invariant bilinear form f on A. The existence of an element $b \in A$ such that $c_f(b) = e$ is seen to be equivalent to the existence in K of a solution of a system of linear equations with coefficients in K. What we have proved above implies that these equations have a solution in E, hence they already have a solution in K, proving that such an element $b \in A$ exists. Since $c_f(A)$ is an ideal of Z, this proves that $c(A) = c_f(A) = Z$.

It is clear that (ii) is a consequence of (i).

(ii) *implies separability*. Let Ξ be a representation of A in an extension F of K (with $\Xi(e) = I$), and consider a reduction

$$\Xi \backsim \begin{bmatrix} \Gamma & \phi \\ & \Delta \end{bmatrix}$$

of Ξ. Here Γ and Δ are representations of A in F and ϕ is a linear mapping of A into the vector module over K of all n $\times$ m matrices with coefficients in F, where m, n are respectively the degrees of Γ and Δ, and ϕ satisfies the identity

$$\phi(xy) = \Gamma(x)\,\phi(y) + \phi(x)\,\Delta(y) \qquad (x, y \in A). \tag{9}$$

Let $a_1, \ldots, a_n$ be a basis of A, and assume the existence of a set of elements $\tilde{a}_1, \ldots, \tilde{a}_n$ as in (ii). From (9) we have

$$\Gamma(a_i)\,\phi(a_j) = \phi(a_i a_j) - \phi(a_i)\,\Delta(a_j). \tag{10}$$

Multiplying (10) on the left by $\Gamma(\tilde{a}_i)$, summing over i, and making use of (7) and (8) we obtain $\phi(a_j) = \Gamma(a_j)\,T - T\Delta(a_j)$, $(j = 1, \ldots, n)$, where $T = \sum \Gamma(\tilde{a}_i)\,\phi(a_i)$. It follows that

$$\Xi \backsim \begin{bmatrix} I & T \\ & I \end{bmatrix}\begin{bmatrix} \Gamma & \phi \\ & \Delta \end{bmatrix}\begin{bmatrix} I & -T \\ & I \end{bmatrix} = \begin{bmatrix} \Gamma & 0 \\ & \Delta \end{bmatrix}$$

proving that Ξ is completely reducible, and consequently that A is separable

3. The generic cocycle. In order to study the ideal $I(\mathfrak{G})$ of $\mathfrak{g}$ defined in §1 we adapt a method of Hochschild **(3**, §4**)**. By $P = P(\mathfrak{G})$ we denote the product $\mathfrak{G} \otimes_{\mathfrak{g}} \mathfrak{G}$, with operators defined as follows

$$(\omega\zeta \otimes \eta) = \omega\zeta \otimes \eta$$
$$(\zeta \otimes \eta)\,\omega = (\zeta \otimes \eta\omega) - (\zeta\eta \otimes \omega) \qquad (\omega \in \mathfrak{G}).$$

P is a two-sided $\mathfrak{G}$-module as we are using the term except for the fact that e does not act as the identity operator on the right. But we may of course define $Z(P)$, $B(P)$, $H(P)$ and $I(P)$ as for ordinary two-sided $\mathfrak{G}$-modules. The *generic* 1-*cocycle* is the element $F \in Z(P)$ defined by

$$F(\omega) = e \otimes \omega \qquad (\omega \in \mathfrak{G}).$$

LEMMA 1. *$I(G) = I(P) = I(F)$, where $I(F) = \{\lambda \in g | \lambda F \in B(P)\}$.*

Proof. Clearly $I(P) \subseteq I(F)$. If now T is any two-sided $\mathfrak{G}$-module and $f \in Z(T)$, the $\mathfrak{g}$-homomorphism μ_f of P into T defined by

$$\mu_f\colon (\zeta \otimes \eta) = \zeta \,.\, f(\eta)$$

is seen to commute with the operators of $\mathfrak{G}$ on the left and on the right, and furthermore $F\mu_f = f$. Consequently for $\lambda \in \mathfrak{g}$, $\lambda F \in B(P)$ implies $\lambda f \in B(T)$, that is, $I(F) \subseteq I(T)$. Since this holds for all T, $I(F) \subseteq I(\mathfrak{G})$. On the other

hand, $P' = Pe$ is an ordinary two-sided $\mathfrak{G}$-module so that $I(\mathfrak{G}) \subseteq I(P')$, and, since $H(P) \simeq H(P')$, $I(P) = I(P')$. We have

$$I(P) \subseteq I(F) \subseteq I(\mathfrak{G}) \subseteq I(P)$$

proving the lemma.

Using this characterization of $I(\mathfrak{G})$ it is straightforward to verify

LEMMA 2. *If* $\mathfrak{o} = K$ *or* $\mathfrak{o} =$ *the ring of all elements of* K *regular with respect to a given finite set of prime ideals of* $\mathfrak{o}$ *then* $I(\mathfrak{o}\mathfrak{G}) = \mathfrak{o}I(\mathfrak{G})$.

Moreover we can prove

LEMMA 3. *If* $\mathfrak{G}$ *has a linearly independent* $\mathfrak{g}$*-basis* $\omega_1, \ldots, \omega_n$, *then* $I(\mathfrak{G}) =$ *the totality of elements* $\lambda \in \mathfrak{g}$ *which can be written in the form* $\lambda = \sum \tilde{\omega}_i \omega_i$ *where the elements* $\tilde{\omega}_i \in \mathfrak{G}$ *are such that for* $\omega \in \mathfrak{G}$

$$\omega_i \omega = \sum \mu_{ij} \omega_j, \quad \omega_j \in K \text{ implies } \omega \tilde{\omega}_i = \sum \tilde{\omega}_j \mu_{ji}. \tag{11}$$

Proof. By Lemma 1, $\lambda \in I(\mathfrak{G})$ if and only if $\lambda F \in B(P)$, that is, if and only if there exists an element $u \in P$ such that $\lambda F(\omega) = \omega u - u\omega$ for all $\omega \in \mathfrak{G}$. We can write u uniquely in the form $u = \sum \tilde{\omega}_i \otimes \omega_i$, $\tilde{\omega}_i \in \mathfrak{G}$, and hence

$$\lambda \otimes \omega = \sum \omega \tilde{\omega}_i \otimes \omega_i - \sum \tilde{\omega}_i \otimes \omega_i \omega + \sum \tilde{\omega}_i \omega_i \otimes \omega. \tag{12}$$

Putting $\omega = e$ in (12) we obtain $\lambda = \sum \tilde{\omega}_i \omega_i$, hence (12) reduces to

$$\sum \omega \tilde{\omega}_i \otimes \omega_i = \sum \tilde{\omega}_i \otimes \omega_i \omega$$

from which we readily deduce (11).

Now we obtain the theorem which is our generalization of Maranda's Theorem 1 in **(4)**, namely

THEOREM 2. $I(\mathfrak{G}) \neq 0$ *if and only if* A *is separable.*

Proof. Taking $\mathfrak{G} = A$ in Lemma 3 and applying (ii) of Theorem 1 we have that A is separable if and only if $I(A) = K$. But by Lemma 2, $I(A) = KI(\mathfrak{G})$, so that the theorem follows.

The reader of Maranda's papers **(4)** and **(5)** will now see that it is only necessary to replace the ideal generated by the group order N by the ideal $I(\mathfrak{G})$ in order to carry over Maranda's results to orders in separable algebras.

4. Construction of $I(\mathfrak{G})$. Let us assume that there exists an invariant bilinear form f on A. In order to construct $I(\mathfrak{G})$ we proceed as follows. We denote by $\mathfrak{G}_f$ the *inverse different* corresponding to f,

$$\mathfrak{G}_f = \{a \in A | f(\mathfrak{G}, a) \subseteq \mathfrak{g}\}. \tag{13}$$

The *different* $\mathscr{I}_f(G)$ is defined by

$$\mathscr{I}_f(\mathfrak{G}) = \{a \in A | \mathfrak{G}_f a \subseteq \mathfrak{G}\}. \tag{14}$$

https://doi.org/10.4153/CJM-1955-053-1 Published online by Cambridge University Press

Notice that in case $\mathfrak{G}$ has a linearly independent $\mathfrak{g}$-basis $\omega_1, \ldots, \omega_n$, and $f(\omega_i, \bar{\omega}_j) = \delta_{ij}$, the elements $\bar{\omega}_1, \ldots, \bar{\omega}_n$ constitute a $\mathfrak{g}$-basis of $\mathfrak{G}_f$, so that $a \in \mathscr{I}_f(\mathfrak{G})$ if and only if $\bar{\omega}_i a \in \mathfrak{G}$ (i = 1, ..., n).

If now $\mathfrak{o} = K$ or $\mathfrak{o}$ = the ring of all elements of K regular with respect to a finite set of prime ideals of $\mathfrak{o}$ we can readily verify that $(\mathfrak{o}\mathfrak{G})_f = \mathfrak{o}\mathfrak{G}_f$, and hence

LEMMA 4. $\mathscr{I}_f(\mathfrak{o}\mathfrak{G}) = \mathfrak{o}\mathscr{I}_f(\mathfrak{G})$.

We remark that (13) and (14) are not symmetric. Using our assumption that $\mathfrak{g}$ is a Dedekind ring, it is easy to prove that when f is *symmetric* the four possible definitions obtained by interchanging left and right in (13) and (14) produce the same $\mathscr{I}_f(\mathfrak{G})$.

Now we obtain $I(\mathfrak{G})$, namely, putting

$$D_f(\mathfrak{G}) = c_f(\mathscr{I}_f(\mathfrak{G}))$$

we can prove

THEOREM 3. *If f is an invariant bilinear form on A then*

$$I(\mathfrak{G}) = D_f(\mathfrak{G}) \cap \mathfrak{g}.$$

LEMMA 5. $D_f(\mathfrak{G}) \cap \mathfrak{g} \neq 0$ *if and only if A is separable.*

Proof. By (i) of Theorem 1 and the definition of D_f, A is separable if and only if $D_f(A) = Z$, i.e., $D_f(A) \cap K = K$. By Lemma 4, $D_f(A) \cap K = K[D_f(\mathfrak{G}) \cap \mathfrak{g}]$, so that the lemma follows.

Proof of Theorem 3. We proceed first under the assumption that G has a linearly independent g-basis $\omega_1, \ldots, \omega_n$. In this case it is clear from the definition of D_f and from Lemma 3 that $D_f(\mathfrak{G}) \cap \mathfrak{g} \subseteq I(\mathfrak{G})$.

If on the other hand $\lambda \in I(\mathfrak{G})$, then $\lambda = \sum \bar{\omega}_i \omega_i$ as in Lemma 3. Consider the linear endomorphism σ of A defined by $\sigma: \bar{\omega}_i \otimes \bar{\omega}_i$, where $f(\omega_i, \bar{\omega}_j) = \delta_{ij}$. For $\omega \in \mathfrak{G}$, $\omega_i \omega = \sum \mu_{ij} \omega_j$ with $\mu_{ij} \in g$. Then by (6), $\omega \bar{\omega}_i = \sum \bar{\omega}_j \mu_{ji}$, hence by (11), $\sigma: \omega \bar{\omega}_i \to \sum \bar{\omega}_j \mu_{ji} = \omega \bar{\omega}_i = \omega(\bar{\omega}_i \sigma)$, proving that σ is a $\mathfrak{G}$-endomorphism, and hence an A-endomorphism, of A considered as a left A-module. Thus σ is effected by right multiplication by an element $c \in A$, and $\bar{\omega}_i = \bar{\omega}_i c \in G$ so that $c \in \mathscr{I}^{-1}{}_f(\mathfrak{G})$. Hence $\lambda = \sum \bar{\omega}_i \omega_i = \sum \bar{\omega}_i c \omega_i \in D_f(\mathfrak{G})$, proving that $I(\mathfrak{G}) \subseteq D_f(\mathfrak{G})$. The desired equality is now proved in this case.

We now drop the assumption of the existence of a linearly independent $\mathfrak{g}$-basis for $\mathfrak{G}$. By Theorem 2 and Lemma 5, $I(\mathfrak{G}) = D_f(\mathfrak{G}) \cap \mathfrak{g} = 0$ if A is not separable, while if A is separable, $I(\mathfrak{G}) \neq 0$ and $D_f(\mathfrak{G}) \cap \mathfrak{g} \neq 0$. In the latter case let us denote by $\mathfrak{o}$ the ring of all elements of K regular with respect to all the prime divisors of $I(\mathfrak{G})$ and $D_f(\mathfrak{G}) \cap \mathfrak{g}$. Since $\mathfrak{o}$ is a principal ideal domain the $\mathfrak{o}$-order has a linearly independent $\mathfrak{o}$-basis. Hence, by Lemmas 2 and 4 and the case of our theorem proved above

$$\mathfrak{o}I(\mathfrak{G}) = I(\mathfrak{o}\mathfrak{G}) = D_f(\mathfrak{o}\mathfrak{G}) \cap \mathfrak{o} = \mathfrak{o}[D_f(\mathfrak{G}) \cap \mathfrak{g}].$$

It follows from the choice of $\mathfrak{o}$ that $I(\mathfrak{G}) = D_f(\mathfrak{G}) \cap \mathfrak{g}$, completing the proof of our theorem.

For an example, let us suppose that $\mathfrak{G}$ is the group ring of a finite group of order N. An invariant bilinear form f on A is defined by

$$f(g, h^{-1}) = \delta_{gh} \qquad (g, h \text{ group elements}).$$

Then $\mathfrak{G}_f = \mathfrak{G}$, $I(\mathfrak{G}) = D_f(\mathfrak{G}) \cap \mathfrak{g} = c_f(\mathfrak{G}) \cap \mathfrak{g} = N\mathfrak{g}$.

References

1. M. Deuring, *Algebren* (Berlin, 1937).
2. D. G. Higman, *Induced and produced modules*, Can. J. Math., *7* (1955), 490–508.
3. G. Hochschild, *On the cohomology theory for associative algebras*, Ann. Math., *47* (1946), 568–579.
4. J.-M. Maranda, *On the p-adic integral representations of finite groups*, Can. J. Math., *5* (1953), 344–355.
5. ———, *On the equivalence of representations of finite groups by groups of automorphisms of modules over Dedekind rings*, Can. J. Math., *7* (1955), 516–526.

Montana State University,
Missoula, Montana