MASCHKE MODULES OVER DEDEKIND RINGS

IRVING REINER

1. Introduction. We use the following notation throughout:

$\mathfrak{o}$ = Dedekind ring (**8**; **12**, p. 83).
K = quotient field of $\mathfrak{o}$.
A = finite-dimensional separable algebra over K, with identity element e (**6**, p. 115).
G = $\mathfrak{o}$-order in A (**2**, p. 69).
$\mathfrak{p}$ = prime ideal in $\mathfrak{o}$.
$K_{\mathfrak{p}}$ = $\mathfrak{p}$-adic completion of K.
$\mathfrak{o}_{\mathfrak{p}}$ = $\mathfrak{p}$-adic integers in $K_{\mathfrak{p}}$.
$\mathfrak{p}^* = \pi\mathfrak{o}_{\mathfrak{p}}$ = unique prime ideal in $\mathfrak{o}_{\mathfrak{p}}$.
$\bar{K} = \mathfrak{o}/\mathfrak{p} = \mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}^*$ = residue class field.

By a *G-module* we shall mean a left G-module R satisfying

1. R is a finitely generated torsion-free left $\mathfrak{o}$-module.
2. For $x, y \in G, r, s \in R$:

$$(xy)r = x(yr), \quad (x + y)r = xr + yr, \quad x(r + s) = xr + xs, \quad er = r.$$

Following Gaschütz and Ikeda (**3**; **5**; see also **7**; **10**) we call a G-module R an *M_u-G-module* (unterer Maschke Modul) if, whenever R is an $\mathfrak{o}$-direct summand of a G-module S, R is a G-direct summand of S. Likewise, R is an *$M_{\mathfrak{o}}$-G-module* (oberer Maschke Modul) if, whenever S/R_1 is G-isomorphic to R where the G-module S contains the G-module R_1 as $\mathfrak{o}$-direct summand, R_1 is a G-direct summand of S.

If all modules considered happen to have $\mathfrak{o}$-bases (for example, when $\mathfrak{o}$ is a principal ideal ring), then we may interpret these concepts in terms of matrix representations over $\mathfrak{o}$. Thus, a representation Γ of G in $\mathfrak{o}$ is an *$M_{\mathfrak{o}}$-representation* if for every reduced representation

$$\begin{pmatrix} \Gamma & \Lambda \\ 0 & \Delta \end{pmatrix}$$

of G in $\mathfrak{o}$, the binding system Λ is strongly-equivalent (**13**) to zero, that is, there exists a matrix T (over $\mathfrak{o}$) such that

$$\Lambda(x) = \Gamma(x)T - T\Delta(x) \qquad \text{for all } x \in G.$$

(Likewise we may define an M_u-representation of G in $\mathfrak{o}$.)

Received September 19, 1955; in revised form December 14, 1955. This work was supported in part by a contract with the National Science Foundation. The author wishes to thank Dr. P. Roquette for some helpful conversations during the preparation of this paper.

Starting with a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, we may form $\bar{G} = G/\mathfrak{p}G$, an algebra over $\bar{K}$. If R is a G-module, then $\bar{R} = R/\mathfrak{p}R$ can be made into a $\bar{G}$-module in obvious fashion, and $\bar{R}$ is then a vector space over $\bar{K}$. The main results of this note are as follows:

THEOREM 1. *If for each $\mathfrak{p}$, $\bar{R}$ is an M_u-$\bar{G}$-module (or $M_{\mathfrak{o}}$-$\bar{G}$-module), then R is an M_u-G-module (or $M_{\mathfrak{o}}$-G-module).*

THEOREM 2. *If G is a Frobenius algebra over $\mathfrak{o}$, and R is an M_u-G-module (or $M_{\mathfrak{o}}$-G-module), then for each $\mathfrak{p}$, $\bar{R}$ is an M_u-$\bar{G}$-module (or $M_{\mathfrak{o}}$-$\bar{G}$-module).*

The significance of Theorem 1 is that it reduces the problem of deciding whether an $\mathfrak{o}$-module R is an M_u-G-module to that of determining for each $\mathfrak{p}$ whether the vector space $\bar{R}$ over $\bar{K}$ is an M_u-$\bar{G}$-module. Thus, we pass from a *ring* problem to a *field* problem, which is in general much simpler.

In the important case where $G = \mathfrak{o}(H)$ is the group ring of a finite group H, then $\bar{G}$ is semi-simple whenever $\mathfrak{p}$ does not divide the order of H, and for such $\mathfrak{p}$ the module $\bar{R}$ is automatically an M-$\bar{G}$-module. More generally, we may form the ideal $I(G)$ of G defined by Higman **(4)**; his results show that $I(G) \neq 0$ in this case. From **(9)** we deduce at once that $\bar{G}$ is semi-simple whenever $\mathfrak{p}$ does not divide $I(G)$. Therefore:

COROLLARY 1. *R is an M_u-G-module (or $M_{\mathfrak{o}}$-G-module) if for each $\mathfrak{p}$ dividing $I(G)$, $\bar{R}$ is an M_u-$\bar{G}$-module (or $M_{\mathfrak{o}}$-$\bar{G}$-module).* (Note that only finitely many $\mathfrak{p}$'s are involved.)

Now let G be a Frobenius algebra over $\mathfrak{o}$, for example, $G = \mathfrak{o}(H)$. Then by **(5)** there is no distinction between $M_{\mathfrak{o}}$- and M_u-modules, and Theorems 1 and 2 tell us that R is an M-G-module if and only if for each $\mathfrak{p}$, $\bar{R}$ is an M-$\bar{G}$-module. Using the concept of *genus* introduced by Maranda in **(9)**, we have:

COROLLARY 2. *Let G be a Frobenius algebra over $\mathfrak{o}$, and let R, S be G-modules in the same genus. Then R is an M-G-module if and only if S is an M-G-module.*

2. $\mathfrak{p}$-adic completion.

Theorem 1 will follow at once from two lemmas, of which we prove the more difficult first. Let R be a G-module, and define

$$G_{\mathfrak{p}} = G \otimes \mathfrak{o}_{\mathfrak{p}}, \quad R_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}} \otimes R,$$

both products being taken over $\mathfrak{o}$.

LEMMA 1. *If for each $\mathfrak{p}$, $R_{\mathfrak{p}}$ is an M_u-$G_{\mathfrak{p}}$-module (or $M_{\mathfrak{o}}$-$G_{\mathfrak{p}}$-module), then R is an M_u-G-module (or $M_{\mathfrak{o}}$-G-module).*

Proof. (We give the proof only for M_u-modules.) Let R be an $\mathfrak{o}$-direct summand of a G-module S. We wish to show that R is a G-direct summand of S, that is, that there exists $f \in \mathrm{Hom}_G(S, R)$ such that $f|R =$ identity. Using the Steinitz-Chevalley theory **(1; 11)** of the structure of finitely generated torsion-free modules over Dedekind rings, and taking into account the hypothesis that R is an $\mathfrak{o}$-direct summand of S, we may write

$$S = \mathfrak{A}_1 s_1 \oplus \ldots \oplus \mathfrak{A}_n s_n, \quad R = \mathfrak{A}_1 s_1 \oplus \ldots \oplus \mathfrak{A}_m s_m,$$

with $m \leqslant n$, where each $\mathfrak{A}_i$ is an $\mathfrak{o}$-ideal in K, and where $s_1, \ldots, s_n$ are linearly independent over K. For the remainder of this proof, let the index i range from 1 to n, and j from 1 to m.

To prove the lemma, it suffices to exhibit $f \in \text{Hom}_A(KS, KR)$ such that $f|KR$ = identity, and f maps S into R. (We use KS to denote the K-module generated by S.) Let us set

$$(1) \qquad f(s_i) = \sum a_{ij} s_j, \quad a_{ij} \in K,$$

thereby defining $f \in \text{Hom}_K(KS, KR)$. Then f maps S into R if and only if for each $\alpha \in \mathfrak{A}_i$ we have $\alpha a_{ij} \in \mathfrak{A}_j$, that is, if and only if

$$(2) \qquad a_{ij} \in (\mathfrak{A}_j : \mathfrak{A}_i) \qquad \text{for all } i, j.$$

On the other hand, the map f defined by (1) will be an A-homomorphism with $f|KR$ = identity, if and only if for all $x \in G$, $s \in S$, $r \in R$:

$$f(xs) = xf(s), \quad f(r) = r.$$

Let us set

$$G = \mathfrak{o}x_1 + \ldots + \mathfrak{o}x_t.$$

This is possible since **(2**, p. 70**)** G is a finitely generated $\mathfrak{o}$-module. Then f is an A-homomorphism with $f|KR$ = identity, if and only if

$$(3) \qquad f(x_k s_i) = x_k f(s_i), \quad f(s_j) = s_j \qquad \text{for all } i, j, k,$$

where the index k ranges from 1 to t. Equations (3) are a set of linear equations with coefficients in K, to be solved for unknowns $\{a_{ij}\}$ satisfying (2).

From the hypotheses of the lemma we deduce that for each $\mathfrak{p}$, (3) has a solution $\{a_{ij}\}$ satisfying $a_{ij} \in (\mathfrak{A}_j : \mathfrak{A}_i)\mathfrak{o}_\mathfrak{p}$ for all i, j. Thus (3) is solvable over the extension field $K_\mathfrak{p}$ of K, and hence is also solvable over K. The general solution of (3) over K is given by

$$(4) \qquad a_{ij} = e_{ij}/d_{ij}, \; e_{ij} = e_{ij}(\mathfrak{t}) = b_{ij} + \sum_{\nu=1}^{N} c_{ij}^{(\nu)} t_\nu,$$

where the $b_{ij}, c_{ij}^{(\nu)}, d_{ij}$ are fixed elements of $\mathfrak{o}$, $d_{ij} \neq 0$, and where $\mathfrak{t}$ ranges over all N-tuples in K^N. The general solution of (3) over $K_\mathfrak{p}$ is also given by (4) by letting $\mathfrak{t}$ range over $K_\mathfrak{p}{}^N$. Then for each $\mathfrak{p}$, we can find $\mathfrak{t}(\mathfrak{p})$ for which

$$(5) \qquad e_{ij}(\mathfrak{t}(\mathfrak{p})) \in \mathfrak{B}_{ij}\mathfrak{o}_\mathfrak{p} \qquad \text{for all } i, j,$$

where $\mathfrak{B}_{ij} = (\mathfrak{A}_j : \mathfrak{A}_i) d_{ij}$.

For each $\mathfrak{p}$, let $b(\mathfrak{p})$ be the maximal exponent to which $\mathfrak{p}$ occurs in the prime ideal factorizations of the ideals $\mathfrak{B}_{ij}$. Then $b(\mathfrak{p}) = 0$ except for a finite set of primes. Set $P = \{\mathfrak{p}: b(\mathfrak{p}) > 0\}$, and choose an N-tuple $\mathfrak{t}$ with components in $\mathfrak{o}$ such that (componentwise)

$$\mathfrak{t} \equiv \mathfrak{t}(\mathfrak{p}) \pmod{\mathfrak{p}^{b(\mathfrak{p})}} \qquad \text{for each } \mathfrak{p} \in P.$$

In that case, $e_{ij}(\mathfrak{t}) \equiv e_{ij}(\mathfrak{t}(\mathfrak{p})) \pmod{\mathfrak{p}^{b(\mathfrak{p})}}$ for each $\mathfrak{p} \in P$, and all i, j, whence by (5) we have

$$(6) \qquad \operatorname{ord}_{\mathfrak{p}} e_{ij}(\mathfrak{t}) \geqslant \operatorname{ord}_{\mathfrak{p}} \mathfrak{B}_{ij} \qquad \text{for all } i, j,$$

for all $\mathfrak{p} \in P$. But for $\mathfrak{p} \notin P$, equation (6) is certainly valid because $e_{ij}(\mathfrak{t}) \in \mathfrak{o}$, and $\operatorname{ord}_{\mathfrak{p}} \mathfrak{B}_{ij} \leqslant 0$. Hence we deduce that $e_{ij}(\mathfrak{t}) \in \mathfrak{B}_{ij} = (\mathfrak{A}_j : \mathfrak{A}_i) d_{ij}$ for all i, j, whence (4) gives a solution of (3) for which (2) holds.

We may remark that this lemma is almost trivial when $\mathfrak{o}$ is a principal ideal ring.

3. Modular representations. Now let $R_{\mathfrak{p}}$ be a $G_{\mathfrak{p}}$-module, and define $\bar{R}_{\mathfrak{p}} = R_{\mathfrak{p}}/\pi R_{\mathfrak{p}}$, $\bar{G}_{\mathfrak{p}} = G_{\mathfrak{p}}/\pi G_{\mathfrak{p}}$. To complete the proof of Theorem 1, we need only show:

LEMMA 2. *If $\bar{R}_{\mathfrak{p}}$ is an M_u-$\bar{G}_{\mathfrak{p}}$-module (or $M_{\mathfrak{o}}$-$\bar{G}_{\mathfrak{p}}$-module), then $R_{\mathfrak{p}}$ is an M_u-$G_{\mathfrak{p}}$-module (or $M_{\mathfrak{o}}$-$G_{\mathfrak{p}}$-module).*

Proof. Since $\mathfrak{o}_{\mathfrak{p}}$ is a principal ideal ring, we may express the proof (given here only for $M_{\mathfrak{o}}$-modules) in terms of matrix representations. We must show that if Γ is a representation of $G_{\mathfrak{p}}$ in $\mathfrak{o}_{\mathfrak{p}}$ for which $\bar{\Gamma}$ (the induced modular representation of $\bar{G}_{\mathfrak{p}}$ in $\bar{K}$) is an M_0-representation, then in any reduced representation

$$(7) \qquad \begin{pmatrix} \Gamma & \Lambda \\ 0 & \Delta \end{pmatrix}$$

of $G_{\mathfrak{p}}$ in $\mathfrak{o}_{\mathfrak{p}}$, the binding system Λ is strongly-equivalent to zero.

We may write $G_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}} y_1 \oplus \ldots \oplus \mathfrak{o}_{\mathfrak{p}} y_n$, $\bar{G}_{\mathfrak{p}} = \bar{K} y_1 \oplus \ldots \oplus \bar{K} y_n$. We shall show the existence of a matrix T over $\mathfrak{o}_{\mathfrak{p}}$ such that

$$(8) \qquad \Lambda(y_i) = \Gamma(y_i) T - T \Delta(y_i) \qquad \text{for each } i,$$

where in this proof the index i ranges from 1 to n. By taking residue classes mod $\mathfrak{p}^*$, the representation (7) gives a representation

$$\begin{pmatrix} \bar{\Gamma} & \bar{\Lambda} \\ 0 & \bar{\Delta} \end{pmatrix}$$

of $\bar{G}_{\mathfrak{p}}$ in $\bar{K}$. Since Γ is by hypothesis an $M_{\mathfrak{o}}$-representation, the binding system $\bar{\Lambda}$ is strongly-equivalent to zero over $\bar{K}$. Therefore there exists V_1 over $\mathfrak{o}_{\mathfrak{p}}$ such that

$$(9) \qquad \Lambda(y_i) = \Gamma(y_i) V_1 - V_1 \Delta(y_i) + \pi \Lambda^{(1)}(y_i) \qquad \text{for each } i,$$

https://doi.org/10.4153/CJM-1956-037-3 Published online by Cambridge University Press

where $\Lambda^{(1)}$ is also over $\mathfrak{o}_{\mathfrak{p}}$. But then (7) with Λ replaced by $\Lambda^{(1)}$ gives another $\mathfrak{o}_{\mathfrak{p}}$-representation of $G_{\mathfrak{p}}$, whence the same argument shows

$$\Lambda^{(1)}(y_i) = \Gamma(y_i)\, V_2 - V_2\Delta(y_i) + \pi\, \Lambda^{(2)}(y_i) \qquad \text{for all } i,$$

where V_2 and $\Lambda^{(2)}$ are over $\mathfrak{o}_{\mathfrak{p}}$. Continuing in this way, we obtain a solution of (8) given by $T = V_1 + \pi V_2 + \pi^2 V_3 + \ldots$.

This proof could also have been stated in terms of cohomology groups.

4. Frobenius algebra. Suppose in this section that G is a Frobenius algebra over $\mathfrak{o}$, that is, there exist $\mathfrak{o}$-bases $\{u_i\}$, $\{v_i\}$ of G (called *dual* bases) such that the right regular representation of G with respect to $\{v_i\}$ coincides with the left regular representation with respect to $\{u_i\}$. Assume that G has an $\mathfrak{o}$-basis containing e. Ikeda showed **(5)** that M_0- and M_u-modules were the same, and that a G-module R is an M-G-module if and only if there exists an $\mathfrak{o}$-endomorphism ϕ of R such that

$$(10) \qquad \sum u_i\, \phi v_i = \text{identity endomorphism of } R.$$

Gaschütz **(3)** had shown this for the case where $G = \mathfrak{o}(H)$, H = finite group, with (10) replaced by:

$$(11) \qquad \sum_{h \in H} h\, \phi\, h^{-1} = \text{identity endomorphism of } R.$$

We may use Ikeda's result to obtain an immediate proof of Theorem 2. By hypothesis, R is an M-G-module, whence (10) holds for some $\mathfrak{o}$-endomorphism ϕ. But then clearly ϕ induces a $\bar{K}$-endomorphism $\bar{\phi}$ of $\bar{R}$, and $\sum u_i\, \phi\, v_i$ = identity endomorphism of $\bar{R}$, so that $\bar{R}$ is an M-$\bar{G}$-module.

References

1. C. Chevalley, *L'arithmétique dans les algèbres de matrices*, Act. Sci. et Ind. *229* (1935).
2. M. Deuring, *Algebren* (Berlin, 1949).
3. W. Gaschütz, *Ueber den Fundamentalsatz von Maschke zur Darstellungstheorie der endlichen Gruppen*, Math. Z., *56* (1952), 376–387.
4. D. G. Higman, *On orders in separable algebras*, Can. J. Math., *7* (1955), 509–515.
5. M. Ikeda, *On a theorem of Gaschütz*, Osaka Math. J., *5* (1953), 53–58.
6. N. Jacobson, *The Theory of Rings* (New York, 1943).
7. F. Kasch, *Grundlagen einer Theorie der Frobeniuserweiterungen*, Math. Ann., *127* (1954), 453–474.
8. I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc., *72* (1952), 327–340.
9. J.-M. Maranda, *On the equivalence of representations of finite groups by groups of automorphisms of modules over Dedekind rings*, Can. J. Math., *7* (1955), 516–526.
10. H. Nagao and T. Nakayama, *On the structure of* (M_0)*- and* (M_u)*-modules*, Math. Z., *59* (1953), 164–170.

11. E. Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern,* Math. Ann. I, *71* (1911), 328–354; II, *72* (1912), 297–345.
12. B. L. van der Waerden, *Modern Algebra,* II (New York, 1950).
13. H. Zassenhaus, *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen,* Hamb. Abh., *12* (1938), 276–288.

Institute for Advanced Study and
University of Illinois