

Title	On a theorem of Gaschütz
Author(s)	Ikeda, Masatoshi
Citation	Osaka Mathematical Journal. 5(1) P.53-P.58
Issue Date	1953
Text Version	publisher
URL	<a href="https://doi.org/10.18910/12624">https://doi.org/10.18910/12624</a>
DOI	10.18910/12624
rights	

*Osaka University Knowledge Archive : OUKA*

<https://ir.library.osaka-u.ac.jp/repo/ouka/all/>

## On a Theorem of Gaschütz

By Masatoshi IKEDA

In his paper "Über den Fundamentalsatz von Maschke zur Darstellungstheorie der endlichen Gruppen",<sup>1)</sup> W. Gaschütz studied two types of  $G$ - $\Omega$ -modules, named  $M_u$ - and  $M_0$ -modules, where  $G$  and  $\Omega$  are a finite group and an arbitrary domain of  $G$ -endomorphisms of the modules respectively. There he obtained a criterion for a  $G$ - $\Omega$ -module to be an  $M_u$ - or  $M_0$ -module, which is a generalization of the well-known theorem of I. Schur that every representation of a finite group of order  $g$  in a field with characteristic  $p(\nmid g)$  is completely reducible.

In the present note we take, instead of  $G$  and  $\Omega$ , a Frobenius algebra  $A$  over a commutative ring  $R$  and a ring  $P$  which contains  $R$  in its centre respectively, and derive a criterion for an  $A$ - $P$ -module to be an  $M_u$ - or  $M_0$ -module, which is essentially a generalization of Gaschütz's result.

Let  $R$  be a commutative ring with the unit element 1.

DEFINITION.  $A$  is called an *algebra* over  $R$  if  $A$  is an associative ring as well as a two-sided  $R$ -module with a right linearly independent  $R$ -basis  $\{u_i\}$  which satisfies  $u_i\omega = \omega u_i$  and  $u_i 1 = 1 u_i = u_i$  for every  $\omega \in R$  and  $i$ .

Now let  $\{u_i\}$  ( $i = 1, \dots, n$ ) be an  $R$ -basis of  $A$  and  $u_i u_j = \sum_k \alpha_{i,j}^k u_k$  ( $\alpha_{i,j}^k \in R$ ); then we obtain the right and left regular representations with respect to  $\{u_i\}$  in the usual manner.

DEFINITION. An algebra  $A$  over  $R$  is called a *Frobenius algebra* if  $A$  has a unit element and its right and left regular representations with respect to an  $R$ -basis are equivalent.

DEFINITION. Let  $\{u_i\}$  ( $i = 1, \dots, n$ ) be an  $R$ -basis of an algebra  $A$  over  $R$  and  $u_i u_j = \sum_k \alpha_{i,j}^k u_k$ . Then the matrix  $(\sum_k \alpha_{i,j}^k \lambda_k)_{i,j}$  is called a *parastrophic matrix* belonging to the basis  $\{u_i\}$  and the parameters  $\lambda_i \in R$  ( $i = 1, \dots, n$ ).

---

1) W. Gaschütz, Math. Zeitschr. 56, 1952.

Then we have

**Lemma.**<sup>2)</sup> *An algebra  $A$  over  $R$  is a Frobenius algebra if and only if  $A$  has a non-singular parastrophic matrix. Moreover if  $A$  is a Frobenius algebra over  $R$ , then every matrix intertwining right and left regular representations is expressed as a parastrophic matrix belonging to suitable parameters.*

If  $A$  is a Frobenius algebra over  $R$  then, for every  $R$ -basis  $\{u_i\}$ , there exists an  $R$ -basis  $\{v_i\}$  such that the right regular representation with respect to  $\{v_i\}$  coincides with the left regular representation with respect to  $\{u_i\}$ . We say that  $\{v_i\}$  is dual to  $\{u_i\}$ .

**DEFINITION.** Let  $A$  be an algebra over  $R$  and  $P$  a ring whose centre contains  $R$ .

- i) A module  $m$  is called an  $A$ - $P$ -module if  $m$  is a left  $A$ -module as well as a right  $P$ -module and satisfies

$$(a\omega)m = (am)\omega, \quad (am)\rho = a(m\rho)$$

for every  $a \in A$ ,  $m \in m$ ,  $\omega \in R$  and  $\rho \in P$ .

- ii) An  $A$ - $P$ -module  $m$  on which the unit element of  $A$  acts as the identity operator is called an  $M_u$ -module if, for every  $A$ - $P$ -module  $n$  containing  $m$ , a direct decomposition  $n = m + m'$  as a  $P$ -module implies a direct decomposition  $n = m + m''$  as an  $A$ - $P$ -module.
- iii) An  $A$ - $P$ -module  $m$  on which the unit element of  $A$  acts as the identity operator is called an  $M_0$ -module if, for every  $A$ - $P$ -module  $n$  which contains an  $A$ - $P$ -submodule  $n'$  such that  $n/n' \cong m$ , a direct decomposition  $n = n' + m'$  as a  $P$ -module implies a direct decomposition  $n = n' + m''$  as an  $A$ - $P$ -module.

**Theorem.** *Let  $A$  be a Frobenius algebra over a commutative ring  $R$  with an  $R$ -basis containing the unit element of  $A$  and  $P$  a ring whose centre contains  $R$ . Then an  $A$ - $P$ -module  $m$  is an  $M_u$ - or  $M_0$ -module if and only if there exists a  $P$ -endomorphism  $\beta$  of  $m$  such that  $\sum_i u_i \beta v_i$  is the identity endomorphism of  $m$  for every  $R$ -basis  $\{u_i\}$  of  $A$  and its dual basis  $\{v_i\}$ .*

**Proof.** 1) Proof of sufficiency. Let  $n$  be an  $A$ - $P$ -module which contains  $m$  and  $n = m + m'$  as a  $P$ -module. By our assumption, there exists a  $P$ -endomorphism  $\beta$  of  $m$ . Let  $\beta^*$  be a  $P$ -endomorphism which

---

2) The proof of this lemma is quite similar to that of footnotes 6) and 7) in Nakayama & Nesbitt: Note on symmetric algebras, Annals of Math. 39, 1938.

coincides with  $\beta$  on  $m$  and  $\beta^*m' = 0$ . Then  $\sum_i u_i \beta^* v_i = \varepsilon$  is a  $P$ -endomorphism and  $\varepsilon m = (\sum_i u_i \beta^* v_i)m = \sum_i u_i \beta^*(v_i m) = \sum_i u_i \beta(v_i m) = (\sum_i u_i \beta v_i)m = m$  for every  $m \in m$ , by our assumption. Moreover it can easily be seen that  $\varepsilon n = m$ . Therefore  $\varepsilon^2 = \varepsilon$ . Now we show that  $\varepsilon$  is an  $A$ - $P$ -endomorphism. Let  $n$  be an arbitrary element of  $n$  and  $a$  an arbitrary element of  $A$ . Since  $\{v_i\}$  is dual to  $\{u_i\}$ , if  $\alpha(u_1, \dots, u_n) = (u_1, \dots, u_n)(\alpha_{i,j})$ , then  $\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} a = (\alpha_{i,j}) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ . Then

$$(a\varepsilon)n = (a \sum_i u_i \beta^* v_i)n = \sum_i a u_i (\beta^* v_i n) = \sum_{i,k} (u_k \alpha_{k,i}) (\beta^* v_i n).$$

By the definition of  $A$ - $P$ -modules and the fact that  $\beta^*$  is a  $P$ -endomorphism,

$$(u_k \alpha_{k,i}) (\beta^* v_i n) = u_k ((\beta^* v_i n) \alpha_{k,i}) = u_k (\beta^* ((v_i n) \alpha_{k,i})) = (u_k \beta^* (v_i \alpha_{k,i})) n.$$

Therefore

$$(a\varepsilon)n = \sum_{i,k} (u_k \beta^* (v_i \alpha_{k,i})) n = (\sum_k u_k \beta^* (\sum_i v_i \alpha_{k,i})) n.$$

On the other hand

$$(\varepsilon a)n = (\sum_k u_k \beta^* (v_k a)) n = (\sum_k u_k \beta^* (\sum_i v_i \alpha_{k,i})) n.$$

Thus  $a\varepsilon = \varepsilon a$  and consequently  $\varepsilon$  is an  $A$ - $P$ -endomorphism. Therefore we have the direct decomposition of  $n$ :  $n = m + (1 - \varepsilon)n$ , where  $1$  is the identity endomorphism of  $n$ . This shows that  $m$  is an  $M_a$ -module.

Next we show that  $m$  is also an  $M_0$ -module. Let  $n$  be an  $A$ - $P$ -module which contains an  $A$ - $P$ -submodule  $n'$  such that  $n/n' \cong m$  and  $n = n' + m'$  as a  $P$ -module. Since  $m' \cong m$  as a  $P$ -module, we can see  $\beta$  as a  $P$ -endomorphism of  $m'$ . Let  $\beta^*$  be a  $P$ -endomorphism of  $n$  which coincides with  $\beta$  on  $m'$  and  $\beta^*n' = 0$ . From our assumption,  $(\sum_i u_i \beta^* v_i)n \equiv n \pmod{n'}$  for  $n \in n$ . In the same way as above, we see that the  $P$ -endomorphism  $\sum_i u_i \beta^* v_i = \varepsilon$  is an  $A$ - $P$ -endomorphism and  $\varepsilon^2 = \varepsilon$ . Therefore  $\varepsilon' = 1 - \varepsilon$  is also an  $A$ - $P$ -endomorphism and  $\varepsilon'^2 = \varepsilon'$ . Moreover it is easy to see that  $\varepsilon'n = n'$ . Consequently we have that  $n = n' + \varepsilon n$  and  $m$  is an  $M_0$ -module.

2. Proof of necessity. Let  $M_A$  be a module satisfying the following conditions:

(i)  $M_A$  is a module of linear forms  $\sum_i x_{u_i} a_{u_i}$  ( $a_{u_i} \in m$ ).

(ii)  $\sum_i x_{u_i} a_{u_i} + \sum_i x_{u_i} b_{u_i} = \sum_i x_{u_i} (a_{u_i} + b_{u_i})$ .

- (iii)  $(\sum_i x_{u_i} a_{u_i})^\rho = \sum_i x_{u_i} (a_{u_i}^\rho)$  for  $\rho \in P$ .
- (iv)  $u_j(\sum_i x_{u_i} a_{u_i}) = \sum_i x_{u_i} (\sum_k a_{u_k} \alpha_{i,j}^k)$ , if  $u_i u_j = \sum_k u_k \alpha_{i,j}^k$ .
- (v)  $a(\sum_i x_{u_i} a_{u_i}) = \sum_j (u_j(\sum_i x_{u_i} a_{u_i})) \alpha_j$ , if  $a = \sum_j u_j \alpha_j$ .

Then it is not hard to verify that  $M_A$  is an  $A$ - $P$ -module.

Now, since  $\{v_i\}$  is dual to  $\{u_i\}$ ,  $\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = P^{-1} \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$ , where  $P = (\sum_k \alpha_{i,j}^k \lambda_k)_{i,j}$  is a non-singular parastrophic matrix belonging to  $\{u_i\}$  and  $\{\lambda_i\}$ . We write  $P = (p_{i,j})_{i,j}$  and  $P^{-1} = (p_{i,j}^*)_{i,j}$ . We assume that  $\sum_i u_i \eta_i = 1$ , the unit element of  $A$ . Then the mapping  $\beta: \sum_i x_{u_i} a_{u_i} \rightarrow \sum_i x_{u_i} (\sum_j a_{u_j} \eta_j) \lambda_i$  satisfies our condition, that is,  $\beta$  is a  $P$ -endomorphism and  $\sum_i u_i \beta v_i$  is the identity endomorphism of  $M_A$ . Since  $\beta$  is obviously a  $P$ -endomorphism, we are only to prove that  $\sum_i u_i \beta v_i$  is the identity endomorphism.

$$\begin{aligned} (\sum_j u_j \beta v_j) (\sum_i x_{u_i} a_{u_i}) &= \sum_j u_j \beta (v_j \sum_i x_{u_i} a_{u_i}) = \sum_j u_j \beta ((\sum_k u_k p_{j,k}^*) (\sum_i x_{u_i} a_{u_i})) \\ &= \sum_j u_j \beta (\sum_i x_{u_i} (\sum_{h,k} a_{u_h} \alpha_{i,k}^h p_{j,k}^*)) = \sum_j u_j (\sum_i x_{u_i} (\sum_{h,k} a_{u_h} p_{j,k}^* \alpha_{i,k}^h \eta_i) \lambda_i). \end{aligned}$$

Since  $\sum_i u_i \eta_i = 1$ ,  $\sum_i \alpha_{i,k}^h \eta_i = \delta_{k,h}$  and consequently

$$\begin{aligned} (\sum_j u_j \beta v_j) (\sum_i x_{u_i} a_{u_i}) &= \sum_j u_j (\sum_i x_{u_i} (\sum_k a_{u_k} p_{j,k}^* \lambda_i)) = \sum_{i,j} x_{u_i} (\sum_m (\sum_k a_{u_k} p_{j,k}^* \lambda_m) \alpha_{i,j}^m) \\ &= \sum_{i,j} x_{u_i} (\sum_k a_{u_k} p_{j,k}^* (\sum_m \lambda_m \alpha_{i,j}^m)) = \sum_{i,j} x_{u_i} (\sum_k a_{u_k} p_{j,k}^* p_{i,j}) \\ &= \sum_i x_{u_i} (\sum_k a_{u_k} (\sum_j p_{i,j} p_{j,k}^*)) = \sum_i x_{u_i} (\sum_k a_{u_k} \delta_{i,k}) = \sum_i x_{u_i} a_{u_i}. \end{aligned}$$

Thus  $\beta$  satisfies our condition.

Next we show that  $M_A$  contains  $A$ - $P$ -modules  $M$  and  $N$  such that  $M \cong \mathfrak{m}$  and  $M_A/N \cong \mathfrak{m}$ . The module  $M = \{\sum_i x_{u_i} (u_i a) \mid a \in \mathfrak{m}\}$  is  $P$ -isomorphic to  $\mathfrak{m}$  by the correspondence  $\mathfrak{m} \ni a \leftrightarrow \sum_i x_{u_i} (u_i a) \in M$ . For, if  $\sum_i x_{u_i} (u_i a) = 0$  then  $u_i a = 0$  for all  $i$  and consequently  $a = 1$   $a = (\sum_i u_i \eta_i) a = \sum_i (u_i a) \eta_i = 0$ . Therefore this correspondence is one-to-one and obviously  $P$ -isomorphism. Moreover this correspondence is  $A$ -isomorphism. For  $u_j (\sum_i x_{u_i} (u_i a)) = \sum_i x_{u_i} (\sum_k (u_k a) \alpha_{i,j}^k) = \sum_i x_{u_i} ((\sum_k u_k \alpha_{i,j}^k) a) = \sum_i x_{u_i} (u_i (u_j a))$ , that is,  $u_j a$  corresponds to  $u_j (\sum_i x_{u_i} (u_i a))$ . Therefore  $M$  is  $A$ - $P$ -isomorphic to  $\mathfrak{m}$ . Since  $A$  has an  $R$ -basis containing 1, say  $w_1 = 1, w_2, \dots, w_n$ , we can construct the module  $M'_A$  satisfying (i), ..., (v) with respect to  $\{w_i\}$ . Let  $Q$  be a non-singular matrix such that  $(u_i) = (w_i) Q'$ . Then it is not hard to see that  $M'_A$

and  $M_A$  are  $A$ - $P$ -isomorphic by the correspondence  $\varphi: M'_A \ni \sum_i x_{w_i} a_{w_i} \rightarrow \sum_i x_{u_i} b_{u_i}$ , where  $(b_{u_1}, \dots, b_{u_n}) = (a_{w_1}, \dots, a_{w_n})Q'$ . By  $\varphi$ ,  $M$  corresponds to  $M' = \{\sum_i x_{w_i}(w_i a) | a \in m\}$ . It is obvious that  $M'_A = M' + M''$  as a  $P$ -module, where  $M'' = \{\sum_i x_{w_i} a_{w_i} | a_{w_1} = 0\}$ . Therefore we have that  $M_A = M + \varphi M''$  as a  $P$ -module and consequently  $M_A = M + M'''$  as an  $A$ - $P$ -module if  $m$  is an  $M_u$ -module. Next we consider the mapping  $\psi: M_A \ni \sum_i x_{u_i} a_{u_i} \rightarrow \sum_i u_i(\sum_j a_{u_j} p_{i,j}^*) \in m$ . Since  $(p_{i,j}^*) = P^{-1}$  is non-singular, the linear equation  $\sum_j x_j p_{i,j}^* = a_{\eta_i} (a \in m, i = 1, \dots, n)$  have a unique solution  $\{a_j\}$  in  $m$ . Then  $\sum_i x_{u_i} a_i$  corresponds to  $\sum_i u_i(a_{\eta_i}) = (\sum_i u_i \eta_i) a = 1 a = a$ . This shows that  $\psi$  is an "onto" mapping. Furthermore it is easy to see that  $\psi$  is a  $P$ -homomorphism. We show that  $\psi$  is an  $A$ - $P$ -homomorphism.

$$\begin{aligned} \psi(u_j(\sum_i x_{u_i} a_{u_i})) &= \psi(\sum_i x_{u_i}(\sum_k a_{u_k} \alpha_{i,j}^k)) = \sum_i u_i(\sum_m (\sum_k a_{u_k} \alpha_{m,j}^k) p_{i,m}^*) \\ &= \sum_i u_i(\sum_k a_{u_k}(\sum_m \alpha_{m,j}^k p_{i,m}^*)). \end{aligned}$$

Since  $P = (p_{i,j})$  intertwines right and left regular representations, we have  $\sum p_{i,m}^* \alpha_{m,j}^k = \sum \alpha_{j,m}^i p_{m,k}^*$  and consequently

$$\begin{aligned} \psi(u_j(\sum_i x_{u_i} a_{u_i})) &= \sum_i u_i(\sum_k a_{u_k}(\sum_m \alpha_{j,m}^i p_{m,k}^*)) = \sum_{k,m} (\sum_i u_i \alpha_{j,m}^i) a_{u_k} p_{m,k}^* \\ &= u_j(\sum_m u_m(\sum_k a_{u_k} p_{m,k}^*)) = u_j \psi(\sum_i x_{u_i} a_{u_i}). \end{aligned}$$

This shows that  $\psi$  is an  $A$ - $P$ -homomorphism and consequently  $M_A$  contains an  $A$ - $P$ -submodule  $N$  such that  $M_A/N \cong m$ . Moreover, as was shown above, the  $P$ -submodule  $N' = \{\sum_i x_{u_i} a_{u_i} | \sum_i a_{u_i} p_{i,j}^* = a_{\eta_j}, a \in m\}$  is mapped onto  $m$  by  $\psi$ . Therefore  $M_A = N + N'$  as a  $P$ -module and consequently  $M_A = N + N''$  as an  $A$ - $P$ -module if  $m$  is an  $M_0$ -module. Thus we have that  $M_A$  is directly decomposable into  $m$  and an  $A$ - $P$ -module. Since  $M_A$  has a  $P$ -endomorphism  $\beta$  satisfying our condition, we can easily construct a  $P$ -endomorphism satisfying our condition for  $m$ .

Next we show that our result is essentially a generalization of Gaschütz's result. Let  $m$  be a  $G$ -module, where  $G = \{g_i | i = 1, \dots, n\}$  is a finite group and  $\Omega$  an arbitrary domain of  $G$ -endomorphisms of  $m$ . Let  $P$  be the ring of endomorphisms generated by  $\Omega$  and the identity endomorphism of  $m$ , and  $C$  the centre of  $P$ . Then the group ring  $G(C)$  of  $G$  over  $C$  is a Frobenius algebra with a  $C$ -basis containing the unit element of  $G$ . Furthermore  $\{g_i^{-1}\}$  is a dual basis to  $\{g_i\}$ . Considering  $m$  as  $G(C)$ - $P$ -module in the natural way, we have

**Theorem.** (Gaschütz). *Let  $G = \{g_i | i = 1, \dots, n\}$ ,  $m$  and  $\Omega$  be a finite group, a  $G$ -module and an arbitrary domain of  $G$ -endomorphisms of  $m$  respectively. Then  $G$ - $\Omega$ -module  $m$  is an  $M_u$ - or  $M_0$ -module if and only if  $m$  has an  $\Omega$ -endomorphism  $\beta$  such that  $\sum g_i \beta g_i^{-1}$  is the identity endomorphism of  $m$ .*

(Received March 9, 1953)