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

By Masatoshi Ikeda

In his paper "Über den Fundamentalsatz von Maschke zur Darstellungstheorie der endlichen Gruppen," W. Gaschütz studied two types of $G$-$\Omega$-modules, named $M_\omega$- and $M_\sigma$-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 $M_\omega$- or $M_\sigma$-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 $p | g$ 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 $M_\omega$- or $M_\sigma$-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 $u_i1 = 1u_i = u_i$ for every $\omega \in R$ and $i$.

Now let $\{u_i\} (i = 1, \ldots, n)$ be an $R$-basis of $A$ and $u_iu_j = \sum \alpha_{i,j}^k u_k$ ($\alpha_{i,j}^k \in R$); 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 $\{u_i\} (i = 1, \ldots, n)$ be an $R$-basis of an algebra $A$ over $R$ and $u_iu_j = \sum \alpha_{i,j}^k u_k$. Then the matrix $(\sum \alpha_{i,j}^k \lambda_k)_{i,j}$ is called a parastrophic matrix belonging to the basis $\{u_i\}$ and the parameters $\lambda_i \in R (i = 1, \ldots, n)$.

Then we have

**Lemma.** 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 $R$.

1) 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

$$(a)m = (am)_\omega, \quad (am)p = a(mp)$$

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

2) 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 $n$ containing $m$, a direct decomposition $n = m + m'$ as a $P$-module implies a direct decomposition $n = m + m''$ as an $A$-$P$-module.

3) 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 $M_0$- 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.
On a Theorem of Gaschütz

coincides with $\beta$ on $m$ and $\beta^*m' = 0$. Then $\sum u_i \beta^* v_i = \epsilon$ is a $P$-endomorphism and $\epsilon m = (\sum u_i \beta^* v_i)m = \sum u_i \beta^*(v_i m) = (\sum u_i \beta v_i)m = m$ for every $m \in m$, by our assumption. Moreover it can easily be seen that $\epsilon n = m$. Therefore $\epsilon^2 = \epsilon$. Now we show that $\epsilon$ 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 $a(u_1, \ldots, u_n) = (u_1, \ldots, u_n)(\alpha_{i, j})$, then $\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} a = (\alpha_{i, j}) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$. Then

$$(a\epsilon)n = (\sum u_i \beta^* v_i)n = \sum u_i(\beta^* v_i n) = \sum u_i \alpha_{i, j}(\beta^* v_i n).$$

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

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

Therefore

$$(a\epsilon)n = \left(\sum u_i \beta^* (v_i \alpha_{i, j})\right)n = \left(\sum u_i \beta^* (\sum v_i \alpha_{i, j})\right)n.$$

On the other hand

$$(\epsilon a)n = \left(\sum u_i \beta^* (v_i a)\right)n = \left(\sum u_i \beta^* (\sum v_i \alpha_{i, j})\right)n.$$

Thus $a\epsilon = \epsilon a$ and consequently $\epsilon$ is an $A-P$-endomorphism. Therefore we have the direct decomposition of $n$: $n = m + (1 - \epsilon)n$, where $1$ is the identity endomorphism of $n$. This shows that $m$ is an $M_n$-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, $\left(\sum u_i \beta^* v_i\right)n = n$ (mod $n'$) for $n \in n$. In the same way as above, we see that the $P$-endomorphism $\sum u_i \beta^* v_i = \epsilon$ is an $A-P$-endomorphism and $\epsilon^2 = \epsilon$. Therefore $\epsilon' = 1 - \epsilon$ is also an $A-P$-endomorphism and $\epsilon'^2 = \epsilon'$. Moreover it is easy to see that $\epsilon'n' = n'$. Consequently we have that $n = n' + \epsilon n$ 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 $\sum u_i a_{i, u_i} (a_{i, u_i} \in m)$.

(ii) $\sum u_i a_{i, u_i} + \sum u_i b_{u_i} = \sum u_i (a_{i, u_i} + b_{u_i}).$
(iii) \((\sum x_{i\mu}a_{\mu i})\rho = \sum x_{i\mu}(a_{\mu i}\rho)\) for \(\rho \in P\).
(iv) \(u_j(\sum x_{i\mu}a_{\mu i}) = \sum x_{i\mu}(\sum a_{\mu k}\alpha_{i\mu})\), if \(u_j = \sum u_k\alpha_{i\mu}\).
(v) \(a(\sum x_{i\mu}a_{\mu i}) = \sum_j (u_j(\sum x_{i\mu}a_{\mu i}))\alpha_j\), if \(a = \sum u_j\alpha_j\).

Then it is not hard to verify that \(M_d\) 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 \(P = (\sum \alpha_{i,j}^\nu, \lambda_{i,j}^\nu)_{i,j}\) is a non-singular parastrophic matrix belonging to \(\{u_i\}\) and \(\{x_i\}\). We write \(P = (p_{i,j})_{i,j}\) and \(P^{-1} = (p_{i,j}^\nu)_{i,j}\). We assume that \(\sum u_i\eta_i = 1\), the unit element of \(A\). Then the mapping \(\beta: \sum x_{i\mu}a_{\mu i}\rightarrow \sum x_{i\mu}(\sum a_{\mu k}\lambda_{i\mu})\) satisfies our condition, that is, \(\beta\) is a \(P\)-endomorphism and \(\sum u_i\beta v_i\) is the identity endomorphism of \(M_d\). Since \(\beta\) is obviously a \(P\)-endomorphism, we are only to prove that \(\sum u_i\beta v_i\) is the identity endomorphism.

\[
(\sum_j u_j\beta v_j)(\sum_i x_{i\mu}a_{\mu i}) = \sum_j u_j(\sum_i x_{i\mu}(\sum \alpha_{i,k}^\nu, p_{i,k}^\nu)) = \sum_j u_j(\sum_i x_{i\mu}(\sum \alpha_{i,k}^\nu, p_{i,k}^\nu, \lambda_{i,k})) = \sum_j u_j(\sum_i x_{i\mu}(\sum \alpha_{i,k}^\nu, \lambda_{i,k})) = \sum_i x_{i\mu}(\sum \alpha_{i,k}^\nu, \lambda_{i,k}).
\]

Since \(\sum_i u_i\eta_i = 1\), \(\sum i \alpha_{i,k}^\nu, \eta_i = \delta_{i,k}\) and consequently

\[
(\sum_j u_j\beta v_j)(\sum_i x_{i\mu}a_{\mu i}) = \sum_j u_j(\sum_i x_{i\mu}(\sum \alpha_{i,k}^\nu, p_{i,k}^\nu, \lambda_{i,k})) = \sum_i x_{i\mu}(\sum_k \alpha_{i,k}^\nu, p_{i,k}).
\]

Thus \(\beta\) satisfies our condition.

Next we show that \(M_d\) contains \(A-P\)-modules \(M\) and \(N\) such that \(M \simeq m\) and \(M_d/N \simeq m\). The module \(M = \{\sum x_{i\mu}(u_i,a)\} a \in m\) is \(P\)-isomorphic to \(m\) by the correspondence \(m \ni a \mapsto \sum x_{i\mu}(u_i,a) \in M\). For, if \(\sum x_{i\mu}(u_i,a) = 0\) then \(u_i a = 0\) for all \(i\) and consequently \(a = \sum i u_i \eta_i a = \sum (u_i a) \eta_i = 0\). Therefore this correspondence is one-to-one and obviously \(P\)-isomorphism. Moreover this correspondence is \(A\)-isomorphism. For \(u_j(\sum x_{i\mu}(u_i,a)) = \sum x_{i\mu}(\sum (u_i a) \alpha_{i,j}^\nu) = \sum x_{i\mu}(\sum u_k \alpha_{i,j}^\nu a)\) that is, \(u_j a\) corresponds to \(u_j(\sum x_{i\mu}(u_i,a))\). Therefore \(M\) is \(A-P\)-isomorphic to \(m\). Since \(A\) has an \(R\)-basis containing \(1\), say \(w_1, w_2, \ldots, w_n\), we can construct the module \(M_d\) satisfying (i), ..., (v) with respect to \(\{w_i\}\). Let \(Q\) be a non-singular matrix such that \((w_i) = (w_i)Q'\). Then it is not hard to see that \(M_d\)
and $M_A$ are $A$-$P$-isomorphic by the correspondence $\varphi: \sum x_{u_i} a_{w_i} \rightarrow \sum x_{u_i} b_{w_i}$, where $(b_{u_1}, \ldots, b_{u_n}) = (a_{w_1}, \ldots, a_{w_n})q'$. By $\varphi$, $M$ corresponds to $M' = \{ \sum x_{u_i} (w_i a) | a \in m \}$. It is obvious that $M_A = M' + M''$ as a $P$-module, where $M'' = \{ \sum x_{u_i} a_{w_i} | a_{w_i} = 0 \}$. 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 $M_0$-$A$-module. Next we consider the mapping $\psi: \sum x_{u_i} a_{u_i} \rightarrow \sum u_i (\sum a_{w_i} p_{i,j}^w) \in m$. Since $(p_{i,j}^w) = P^{-1}$ is non-singular, the linear equation $\sum x_{u_i} a_{u_i} = \alpha_{\eta_i} (a \in m, i = 1, \ldots, n)$ have a unique solution $\{a_i\}$ in $m$. Then $\sum x_{u_i} a_{u_i}$ corresponds to $\sum u_i (\alpha_{\eta_i}) = (\sum u_i \eta_i) a = 1 a = a$. 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.

\[
\psi(u_i (\sum x_{u_i} a_{u_i})) = \psi(\sum x_{u_i} (\sum a_{w_i} \alpha_{\eta_i}^w)) = \sum u_i (\sum a_{w_i} \alpha_{\eta_i}^w) p_{i,m}^w
\]

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

\[
\psi(u_i (\sum x_{u_i} a_{u_i})) = \sum u_i (\sum a_{u_i} (\sum \alpha_{\eta_i}^j p_{i,m}^w)) = \sum u_i \alpha_{\eta_i}^j a_{u_i} p_{i,m}^w
\]

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 $N' = \{ \sum x_{u_i} a_{u_i} | \sum a_{u_i} p_{i,j}^w = \alpha_{\eta_i}, a \in m \}$ 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 $M_0$-$A$-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 $G = \{ g_i | i = 1, \ldots, n \}$ 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 $G = \{g_i \mid i = 1, \ldots, n\}$, $m$ 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 $M_n$- 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)