One-headed representation modules of abelian p-groups over a field of characteristic p

By GERHARD PAZDERSKI (Rostock)

Dedicated to the memory of Andor Kertész

Let G be a p-group and F be a field of characteristic p. As well known there only exists a finite number of indecomposable (F, G)-modules, if G is cyclic and there are indecomposable (F, G)-modules of arbitrarily large dimension, if G is non-cyclic (see [1], [3]). In this paper we are concerned with a special kind of indecomposable (F, G)-modules that is to say with (F, G)-modules possessing only one maximal submodule, so called one-headed modules. We shall prove that there exists only a finite number of one-headed (F, G)-modules provided that G is abelian; moreover we shall construct a universal one-headed (F, G)-module the factor modules of which will cover all the possible one-headed (F, G)-modules.

Notations

$H \leqq G$, $H < G$ respectively means: H is a subgroup, proper subgroup of the group G; ord a=order of the group element a; $\langle a \rangle$=cyclic group generated by a; deg $\mathbf{A}$=degree of the matrix $\mathbf{A}$; rank $\mathbf{A}$=rank of $\mathbf{A}$; $\mathbf{A} \times \mathbf{B}$=Kronecker product of matrices $\mathbf{A}, \mathbf{B}$; $\mathbf{I}$=identity matrix; F denotes a field of characteristic $p > 0$; $\langle M \rangle_F$=submodule spanned over F by the subset M of an F-module.

Any matrix group G over F of order a power of p can be transformed in such a manner that every matrix of G becomes the shape

$$\begin{pmatrix} 1 & \alpha_{12} & \alpha_{13} \cdots & & \alpha_{1n} \\ & 1 & \alpha_{23} \cdots & & \alpha_{2n} \\ & & 1 \quad \cdots & & \alpha_{3n} \\ & & & \ddots & \vdots \\ & 0 & & 1 & \alpha_{n-1,n} \\ & & & & 1 \end{pmatrix}. \tag{1}$$

This follows from the fact that besides the 1-representation there is no other irreducible representation of G over F (see [2], p. 484).

Conversely all matrices (1) with coefficients in F form a group, the exponent of which is the smallest power of p exceeding $n-1$.

Let

$$\mathbf{A}_n = \begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & 0 \\ & & 1 & \ddots & \\ & 0 & & \ddots & 1 \\ & & & & 1 \end{pmatrix}$$

with degree n. Then

$$\mathbf{A}_n^j = \begin{pmatrix} \binom{j}{0} & \binom{j}{1} & \binom{j}{2} \dots \binom{j}{n-1} \\ & \binom{j}{0} & \binom{j}{1} \dots \binom{j}{n-2} \\ & 0 & \ddots \quad \vdots \\ & & \binom{j}{0} \end{pmatrix} \quad (j \geqq 0).$$

This shows that over F the order of $\mathbf{A}_n$ is the smallest power of p being $\geqq n$.

Further let

$$(2) \qquad \mathbf{A}_{n_1, \dots, n_r} = \begin{pmatrix} \mathbf{A}_{n_1} & & & \\ & \mathbf{A}_{n_2} & & 0 \\ & 0 & \ddots & \\ & & & \mathbf{A}_{n_r} \end{pmatrix}.$$

Then the order of $\mathbf{A}_{n_1, \dots, n_r}$ as a matrix over F is the smallest power of p which is $\geqq \max \{n_1, \dots, n_r\}$.

Now we have the

Lemma 1. *The following statements concerning a matrix* $\mathbf{A}$ *over a field of characteristic* p *are equivalent:*

(i) ord $\mathbf{A}$ *is a power of* p.

(ii) *All eigen-values of* $\mathbf{A}$ *are* 1.

(iii) $\mathbf{A}$ *is similar to a matrix* (2) *(which is the Jordan normal form of* $\mathbf{A}$*).*

PROOF. (i)$\Rightarrow$(ii). We already have seen that $\mathbf{A}$ is similar to a matrix of the shape (1). Therefore all the eigen-values of $\mathbf{A}$ are 1.

(ii)$\Rightarrow$(iii). If all the eigen-values of $\mathbf{A}$ are 1, then the Jordan normal form of $\mathbf{A}$ is a matrix (2).

(iii)$\Rightarrow$(i). This has been noted above.

Corollary 1. $\mathbf{A}_n$ *is indecomposable over* F.

PROOF. Assume not, then $\mathbf{A}$ is over F similar to a matrix

$$\begin{pmatrix} \mathbf{A} & 0 \\ 0 & \mathbf{B} \end{pmatrix}$$

with $\deg \mathbf{A} \geqq 1$, $\deg \mathbf{B} \geqq 1$. Since both matrices $\mathbf{A}, \mathbf{B}$ only have eigen-values 1, their Jordan normal forms are shaped like (2). Therefore $\mathbf{A}_n$ is similar to a matrix

$\mathbf{A}_{m_1, \ldots, m_s}$ with $s \geqq 2$. It follows that $\mathbf{A}_n - \mathbf{I}$ is similar to $\mathbf{A}_{m_1, \ldots, m_s} - \mathbf{I}$ and we find $n-1 = \text{rank}\,(\mathbf{A}_n - \mathbf{I}) = \text{rank}\,(\mathbf{A}_{m_1, \ldots, m_s} - \mathbf{I}) = n - s$, which is impossible.

Corollary 2. *If the matrix* $\mathbf{A}$ *over* F *has a power of* p *as its order, then* $\deg \mathbf{A} - \text{rank}\,(\mathbf{A} - \mathbf{I})$ *is the number of indecomposable constituents of* $\mathbf{A}$ *over* F.

Corollary 3. *All non similar indecomposable representations of a cyclic group* $\langle a \rangle$ *of order* p^m *over a field of characteristic* p *are given by*

$$a \to \mathbf{A}_n, \tag{3}$$

where $n = 1, \ldots, p^m$. *The kernel of the representation given by* (3) *is* $\langle a^{p^k} \rangle$, *where* $p^{k-1} < n \leqq p^k$.

Corollary 4. *Keeping the notation of the foregoing Corollary we can say that the extension of* (3) *to a representation of the group algebra of* $\langle a \rangle$ *over* F *is faithful if and only if* $n = p^m$.

PROOF. The relation

$$\sum_{j=0}^{p^m-1} \alpha_j \mathbf{A}_n^j = 0$$

with coefficients $\alpha_j \in F$ is equivalent to the system of linear equations

$$\sum_{j=0}^{p^m-1} \alpha_j \binom{j}{i} = 0 \quad (i = 0, \ldots, n-1).$$

If $n < p^m$, this system admits a non trivial solution. But if $n = p^m$ then there is only the trivial solution, since the determinant $\det \binom{j}{i}$ has value 1.

Now let G be a finite abelian group with the basis $a_1, \ldots, a_r$ and let $\text{ord}\, a_j = p^{m}$ for $j = 1, \ldots, r$. Given integers $n_1, \ldots, n_r$ with $1 \leqq n_j \leqq p^{m_j}$ the mapping

$$a_1^{x_1} \ldots a_r^{x_r} \to \mathbf{A}_{n_1}^{x_1} \times \ldots \times \mathbf{A}_{n_r}^{x_r}, \tag{4}$$

is a representation of G over F. We may choose a basis

$$u_{i_1, \ldots, i_r} \quad \text{with} \quad i_j = 1, \ldots, n_j \quad \text{for} \quad j = 1, \ldots, r \tag{5}$$

of the underlying representation module M in such a manner that G acts accordingly

$$u_{i_1, \ldots, i_r} a_j = \begin{cases} u_{i_1, \ldots, i_r} + u_{i_1, \ldots, i_j+1, \ldots, i_r} & \text{if} \quad i_j < n_j \\ u_{i_1, \ldots, i_r} & \text{if} \quad i_j = n_j \end{cases} \quad (j = 1, \ldots, r). \tag{6}$$

We often write $M(n_1, \ldots, n_r)$ instead of M, indicating the dependence on $n_1, \ldots, n_r$.

Let us define a partial order between the $u_{i_1, \ldots, i_r}$ by setting $u_{i_1, \ldots, i_r}$ before $u_{i'_1, \ldots, i'_r}$ if $i_1 \leqq i'_1, \ldots, i_r \leqq i'_r$. We shall call $\sum_{j=1}^{r} (n_j - i_j)$ the hight of $u_{i_1, \ldots, i_r}$. There is only one element of hight 0 namely $u_{n_1, \ldots, n_r}$. Further we transfer this partial order to the summands $\alpha_{i_1, \ldots, i_r} u_{i_1, \ldots, i_r}$ having $\alpha_{i_1, \ldots, i_r} \neq 0$ of an arbitrary element

$$u = \sum \alpha_{i_1, \ldots, i_r} u_{i_1, \ldots, i_r} \tag{7}$$

of M. So we may speak of the first, the second etc. summands of an element $u \in M$. By the hight of $\alpha u_{i_1,\dots,i_r} (\alpha \neq 0)$ we understand the hight of $u_{i_1,\dots,i_r}$.

For an arbitrary element $g = a_1^{x_1} \dots a_r^{x_r}$ of G with $0 \leqq x_j < p^{m_j}$ for $j = 1, \dots, r$ we define the mapping

$$(8) \qquad u_{i_1,\dots,i_r} \to u_{i_1,\dots,i_r} \circ g = u_{i_1+x_1,\dots,i_r+x_r},$$

where the image at the right hand side is declared to be zero if $i_j + x_j > n_j$ for at least one j. This mapping preserves the partial order if elements with image zero are omitted. We may extend (8) to an F-operator-homomorphism of M by setting

$$(9) \qquad (\sum \alpha_{i_1,\dots,i_r} u_{i_1,\dots,i_r}) \circ g = \sum \alpha_{i_1,\dots,i_r} (u_{i_1,\dots,i_r} \circ g).$$

Besides g let $h = a_1^{y_1} \dots a_r^{y_r}$ with $0 \leqq y_j < p^{m_j}$ for $j = 1, \dots, r$ be another element of G. If $x_j + y_j < p^{m_j}$ for $j = 1, \dots, r$, then

$$u \circ (gh) = (u \circ g) \circ h \quad \text{for} \quad u \in M.$$

(6) and (9) yield

$$u \circ a_j = u a_j - u = u(a_j - 1) \quad \text{for} \quad u \in M, \quad j = 1, \dots, r,$$

where $(a_j - 1)$ is to be seen as an element of the group algebra of G over F. For $g \in G$, $u \in M$ we have

$$(ug) \circ a_j = u g a_j - ug = u a_j g - ug = (u a_j - u) g = (u \circ a_j) g.$$

Repeated application supplies

$$(ug) \circ h = (u \circ h) g \quad \text{for} \quad u \in M, \quad g, h \in G.$$

i.e. the mapping $u \to u \circ g (u \in M, g \in G)$ also is G-operator-homomorphic.

For subsets $M_0 \subseteqq M$, $G_0 \subseteqq G$ we define $M_0 \circ G_0 = \{u \circ g \mid u \in M_0, g \in G_0\}$. If $0 \neq u \in M$, $1 \neq g \in G$, then $u \circ g$ has a smaller hight than u, provided that $u \circ g \neq 0$. Especially $M_0 \circ g$ is a proper (F, G)-submodule of M_0 if M_0 is an (F, G)-submodule $\neq 0$ of M.

Lemma 2. *If N is an (F, G)-submodule of M containing an element* (7) *with only one first summand $\alpha_{j_1,\dots,j_r} u_{j_1,\dots,j_r}$ $(\alpha_{j_1,\dots,j_r} \neq 0)$, then $u_{j_1,\dots,j_r}$ and all the elements* (5) *situated behind it in the partial order are elements of N.*

Proof. We apply induction on the hight k of the first summand u_0 of u. If $k = 0$ then $u = u_0 = \alpha_{n_1,\dots,n_r} u_{n_1,\dots,n_r}$ and we are ready. Now let $k > 0$. The element $u \circ a_l$ lies in N. It has like u precisely one first summand, provided that $j_l < n_l$. This summand is $\alpha_{j_1,\dots,j_r} u_{j_1,\dots,j_l+1,\dots,j_r}$ and has a hight lower than that of u_0. By taking $l = 1, \dots, r$ as far as $j_l < n_l$ and applying induction argument on each sum $u \circ a_l$ it follows that all the basis elements situated properly behind $u_{j_1,\dots,j_r}$ in the partial order are contained in N. Whence $u_0 \in N$ and so $u_{j_1,\dots,j_r} \in N$.

Theorem 1. *$M(n_1, \dots, n_r)$ possesses only one maximal (F, G)-submodule namely the set of all elements* (7) *with $\alpha_{1,\dots,1} = 0$.*

Proof. Clearly the set of sums (7) with $\alpha_{1,\dots,1} = 0$ forms a proper submodule N of M, which is admissible to F and G. Moreover N is maximal, because a module

L with $N < L \leqq M$ must contain an element (7) with $\alpha_{1,\dots,1} \neq 0$, whence Lemma 2 yields $L \geqq M$.

Following a notation due to WIELANDT (see [4], p. 225), we will call a group *one-headed,* if it has a unique maximal proper normal subgroup. A little more generally one can define: N is *one-headed in* G, where N is a normal subgroup of the group G, if the lattice of all the normal subgroups of G properly contained in N has precisely one maximal element. A representation belonging to a one-headed representation module we also will call one-headed.

Now we have the

Corollary. *Every factor module of the* (F, G)*-module* $M(n_1, \dots, n_r)$ *is one-headed and therefore indecomposable.*

We shall see in Theorem 3 that by the factor modules of $M(p^{m_1}, \dots, p^{m_r})$ all possible one-headed (F, G)-modules are obtainable.

As a dual to Theorem 1 we have

Theorem 2. $M(n_1, \dots, n_r)$ *possesses only one minimal* (F, G)*-submodule namely* $\{\alpha u_{n_1,\dots,n_r} | \alpha \in F\}$.

PROOF. If N is a minimal (F, G)-submodule of $M(n_1, \dots, n_r)$, then $N \circ G = 0$. Therefore N contains no other elements than $\alpha u_{n_1,\dots,n_r}$ $(\alpha \in F)$.

Theorem 3. *Each* (F, G)*-module possessing only one maximal* (F, G)*-submodule is isomorphic to a factor module of* $M(p^{m_1}, \dots, p^{m_r})$.

PROOF. Let N be an (F, G)-module with only one maximal (F, G)-submodule L. We choose an element of N outside L and sign it by $v_{1,\dots,1}$ with so many indices 1, as the rank r of G states. Then we define elements $v_{i_1,\dots,i_r}$ inductively by

$$v_{i_1,\dots,i_r} a_j = v_{i_1,\dots,i_r} + v_{i_1,\dots,i_j+1,\dots,i_r} \quad \text{if} \quad i_j < p^{p^{m_j}}.$$

Employing the group algebra of $\langle a \rangle$ over F we also can write $v_{i_1,\dots,i_r}$ in the form

$$v_{i_1,\dots,i_r} = v_{1,\dots,1}(a_1-1)^{i_1-1} \dots (a_r-1)^{i_r-1}.$$

By reason of $(a_j-1)^{p^{m_j}} = 0$, we have

$$(a_j-1)^{p^{m_j}-1} a_j = (a_j-1)^{p^{m_j}-1}$$

and so

$$v_{p^{m_1},\dots,p^{m_r}} a_j = v_{p^{m_1},\dots,p^{m_r}}.$$

It follows that the F-submodule of N generated by the $v_{i_1,\dots,i_r}$ admits G. This submodule must coincide with N, because otherwise it must lie in L, which implies $v_{1,\dots,1} \in L$ a contradiction. The elements of G effect on the generators $v_{i_1,\dots,i_r}$ of L in the same manner as on the basis elements $u_{i_1,\dots,i_r}$ of $M(p^{m_1}, \dots, p^{m_r})$. Hence

$$\sum \alpha_{i_1,\dots,i_r} u_{i_1,\dots,i_r} \to \sum \alpha_{i_1,\dots,i_r} v_{i_1,\dots,i_r}$$

is an (F, G)-operator-homomorphism from $M(p^{m_1}, \dots, p^{m_r})$ onto N, and consequently L is isomorphic to a factor module of $M(p^{m_1}, \dots, p^{m_r})$.

As an instance we notice

$$M(p^{m_1}, \dots, p^{m_r})/L \cong M(n_1, \dots, n_r),$$

where L is the submodule of $M(p^{m_1}, \ldots, p^{m_r})$ generated by all the elements which are properly behind $u_{n_1, \ldots, n_r}$.

By means of the Corollary to Theorem 1 together with Theorem 3 the problem of finding out all one-headed (F, G)-modules is reduced to the problem of putting up all the factor modules of $M(p^{m_1}, \ldots, p^{m_r})$. In this paper we will not carry on the investigation of these factor modules. We mention that generally there are more than one non-equivalent faithful one-headed representations of an abelian group. The kernel of the representation (4) coincides with $\langle a_1^{p^{k_1}}\rangle \times \langle a_2^{p^{k_2}}\rangle \times \ldots \times \langle a_r^{p^{k_r}}\rangle$, where $p^{k_j-1} < n_j \leqq p^{k_j}$ for $j=1, \ldots, r$, as to be seen by means of Corollary 3 to Lemma 1. Consequently all the modules $M(n_1, \ldots, n_r)$ with $p^{m_j-1} < n_j \leqq p^{m_j}$ for $j=1, \ldots, r$ are representation modules of faithful representations of G.

We conclude with a remark on the possible form of a basis in a factor module of $M(n_1, \ldots, n_r)$.

Theorem 4. *Let N be a proper (F, G)-submodule of $M = M(n_1, \ldots, n_r)$. Then there exist chains of neighbouring elements* (5) *beginning with $u_{1, \ldots, 1}$, such that their union is modulo N a basis of M over F.*

PROOF. All linear notions are related to the ground field F. We apply induction on the dimension of M/N. If this dimension is 1, then N coincides with the single maximal submodule of M and the chain consisting of the element $u_{1, \ldots, 1}$ has the wanted property. Now let M/N have a dimension larger than 1 and let $u_{j_1, \ldots, j_r}$ be a last element (5) not belonging to N. Putting $L = \langle u_{j_1, \ldots, j_r}, N\rangle_F$, we have $u_{j_1, \ldots, j_r} a_k \in L$ $(k=1, \ldots, r)$, whence L is an (F, G)-module. By induction argument there exist chains of neighbouring elements (5) beginning with $u_{1, \ldots, 1}$, such that their union is a basis B of M mod L. Evidently $u_{j_1, \ldots, j_r}$ is linearly independent on B mod N. Let B' be the set of all immediate successors of the elements of B. If there exists in B' an element, which is linearly independent on B mod N, then we are ready. We finally show, that the assumption, each element of B' depends linearly on B mod N, leads to a contradiction. Clearly $u_{1, \ldots, 1}$ is connected with $u_{j_1, \ldots, j_r}$ by a chain of neighbouring elements (5). A certain peace $w_0, w_1, \ldots, w_s$ of this chain has the property $w_0 \in B$, $w_1 \in B' \setminus B$, $w_s = u_{j_1, \ldots, j_r}$. There exist elements $g_i \in \{a_1, \ldots, a_r)$ with $w_i \circ g_i = w_{i+1}$ for $i=1, \ldots, s-1$. By assumption we have a representation mod N of w_1 as a linear combination of elements of B, say $w_1 \equiv l_1(B)$ mod N. From this we get $w_1 \circ g_1 = w_2 \equiv l_1(B \circ g)$ mod N. This implies, since $B \circ g \subseteq B \cup B'$ and since by assumption each element of B' depends linear mod N on B, a representation of w_2 as a linear combination $w_2 \equiv l_2(B)$ mod N. Repeated application leads to a linear relation $w_s \equiv l_s(B)$ mod N, which is impossible as mentioned above.

References

[1] D. G. HIGMAN, Indecomposable representations at characteristic p. *Duke Math. J.* **21** (1954), 377—381.

[2] B. HUPPERT, Endliche Gruppen I., *Berlin—Heidelberg—New York* 1967.

[3] F. KASCH, M. KNESER, H. KUPISCH, Unzerlegbare modulare Darstellungen endlicher Gruppen mit zyklischer p-Sylowgruppe. *Arch. Math.* **8** (1957), 320—321.

[4] H. WIELANDT, Eine Verallgemeinerung der invarianten Untergruppen. *Math. Z.* **45** (1939), 209—244.

(Received November 20, 1975.)