

Pacific Journal of Mathematics

SPLITTING OF GROUP REPRESENTATIONS

ROBERT PATRICK MARTINEAU

SPLITTING OF GROUP REPRESENTATIONS

R. PATRICK MARTINEAU

Let G be a finite group, and V, W two modules over the group-ring KG , where K is some field. In this note is described a method for proving that every KG -extension of V by W is a split extension. The method is applied to the groups $PSL(2, 2^a)$ when $K = GF(2^a)$, giving in this case an alternative proof of a theorem of G. Higman.

1. The method. Fix the finite group G and the field K . If A is any left KG -module, we let $Cr(G, A)$ denote the K -vector space of crossed homomorphisms from G to A , that is,

$$Cr(G, A) = \{f: G \longrightarrow A / f(gh) = gf(h) + f(g), \text{ all } g, h \in G\}.$$

Suppose G is generated by the elements g_1, \dots, g_s with relations w_1, \dots, w_t . Here w_1, \dots, w_t are elements of the free group F , freely generated by x_1, \dots, x_s , and we say that g_1, \dots, g_s satisfy the relation w if $\alpha(w) = 1$ where α is the homomorphism from F to G defined by $\alpha(x_i) = g_i, i = 1, \dots, s$.

We shall devise a criterion, in terms of w_1, \dots, w_t , to decide whether or not a map from G to A is a crossed homomorphism. Let \mathcal{C} be the set of maps $f: \{g_1, \dots, g_s\} \rightarrow A$ which satisfy the following condition: for any $i \in \{1, \dots, s\}$ for which $g_i^{-1} \in \{g_1, \dots, g_s\}$, $f(g_i^{-1}) = -g_i^{-1}f(g_i)$.

Now let $w \in F$ and $f \in \mathcal{C}$. We shall define, by induction on the length of w , an element $w^*(f)$ of A . If $w = 1$, put $w^*(f) = 0$. If $w = x_k^\varepsilon$ for some $\varepsilon = \pm 1$, then we define $w^*(f) = f(g_k^\varepsilon)$ if $g_k^\varepsilon \in \{g_1, \dots, g_s\}$, and if $g_k^\varepsilon \notin \{g_1, \dots, g_s\}$, we put $w^*(f) = -g_k^{-1}f(g_k)$. Finally, if $w = v \cdot x_k^\varepsilon$ for some $\varepsilon = \pm 1$, we define $w^*(f) = \alpha(v) \cdot f(g_k^\varepsilon) + v^*(f)$.

Notice that we do not need w to be in reduced form, since according to the definition,

$$\begin{aligned} (wx_i x_i^{-1})^*(f) &= \alpha(w) \cdot g_i f(g_i^{-1}) + \alpha(w) f(g_i) + w^*(f) \\ &= \alpha(w) g_i [f(g_i^{-1}) + g_i^{-1} f(g_i)] + w^*(f) \\ &= w^*(f), \end{aligned}$$

and similarly for $w x_i^{-1} x_i$.

[As an example, if $w = x_1 x_2^2$, then $w^*(f) = g_1 g_2 f(g_2) + g_1 f(g_2) + f(g_1)$.]

LEMMA 1. If $v, w \in F$ and $f \in \mathcal{C}$, then

$$(wv)^*(f) = \alpha(w) \cdot v^*(f) + w^*(f).$$

Proof. This is true by definition if $v = 1$ or $v = x_i^\varepsilon$, $\varepsilon = \pm 1$. If we have $(wv)^*(f) = \alpha(w) \cdot v^*(f) + w^*(f)$ for two elements w, v of F , and $\varepsilon = \pm 1$, then we have

$$\begin{aligned} (wvx_i^\varepsilon)^*(f) &= \alpha(wv)f(g_i^\varepsilon) + (wv)^*(f) \\ &= \alpha(w) \cdot \alpha(v)f(g_i^\varepsilon) + \alpha(w)v^*(f) + w^*(f) \\ &= \alpha(w)[\alpha(v)f(g_i^\varepsilon) + v^*(f)] + w^*(f) \\ &= \alpha(w)(vx_i^\varepsilon)^*(f) + w^*(f). \end{aligned}$$

Thus the lemma holds by induction on the length of v .

LEMMA 2. If $f \in Cr(G, A)$, then

- (i) $f \in \mathcal{C}$
- (ii) if $w \in F$ then $w^*(f) = f(\alpha(w))$, and
- (iii) for $i = 1, \dots, t$, $w_i^*(f) = 0$.

Proof. If $f \in Cr(G, A)$ then $f(1 \cdot 1) = 1 \cdot f(1) + f(1)$, so $f(1) = 0$. Then $0 = f(1) = f(g_i \cdot g_i^{-1}) = g_i f(g_i^{-1}) + f(g_i)$, so that $f \in \mathcal{C}$.

The equation $w^*(f) = f(\alpha(w))$ holds if $w = 1$ or x_i , by definition. If $w = x_i^{-1}$, then $w^*(f) = -g_i^{-1}f(g_i) = f(g_i^{-1})$ since $f \in Cr(G, A)$. If now $w = vx_i^\varepsilon$, $\varepsilon = \pm 1$, and $v^*(f) = f(\alpha(v))$, then

$$\begin{aligned} w^*(f) &= \alpha(v)f(g_i^\varepsilon) + v^*(f) \\ &= \alpha(v)f(g_i^\varepsilon) + f(\alpha(v)) \\ &= f(\alpha(v) \cdot g_i^\varepsilon) \quad \text{since } f \in Cr(G, A) \\ &= f(\alpha(w)). \end{aligned}$$

Thus (ii) holds by induction on the length of w . (iii) now follows immediately, since $\alpha(w_i) = 1$ and $f(1) = 0$.

We remark, though we shall not need this, that a converse of this result is also true, namely:

LEMMA 3. If w_1, \dots, w_t are defining relations for G , and if $f \in \mathcal{C}$ satisfies $w_i^*(f) = 0$ for $i = 1, \dots, t$, then f can be extended (uniquely) to an element of $Cr(G, A)$.

Proof. First of all we show that if $u \in \ker \alpha$, then $u^*(f) = 0$. Now $\ker \alpha = \langle w_1, \dots, w_t \rangle^F$, that is, the subgroup of F generated by all elements of the form $v^{-1}w_i v$, $v \in F$. By definition, $1^*(f) = 0$, so by Lemma 1, $\alpha(v^{-1}) \cdot v^*(f) + (v^{-1})^*(f) = 0$. Again by Lemma 1,

$$\begin{aligned} (v^{-1}w_i v)^*(f) &= \alpha(v^{-1}w_i) \cdot v^*(f) + (v^{-1}w_i)^*(f) \\ &= \alpha(v^{-1}) \cdot \alpha(w_i) \cdot v^*(f) + \alpha(v^{-1})w_i^*(f) + (v^{-1})^*(f). \end{aligned}$$

Since $\alpha(w_i) = 1$ and $w_i^*(f) = 0$, we have $(v^{-1}w_i v)^*(f) = 0$. Finally by Lemma 1, if $w^*(f) = 0$ and $v^*(f) = 0$ then $(wv)^*(f) = 0$. Thus $u^*(f) = 0$ for all $u \in \ker \alpha$.

Now if g is any element of G , then $g = \alpha(w)$ for some $w \in F$. Define $f(g) = w^*(f)$. Then this definition depends only on g , for if $g = \alpha(v)$ also, then $wv^{-1} \in \ker \alpha$, say $wv^{-1} = u$. But now $w = uv$, so by Lemma 1, $w^*(f) = \alpha(u) \cdot v^*(f) + u^*(f) = v^*(f)$ since $\alpha(u) = 1$ and $u^*(f) = 0$.

Now if $g, h \in G$, say $g = \alpha(w)$, $h = \alpha(v)$, then $f(gh) = (wv)^*(f) = \alpha(w)v^*(f) + w^*(f)$ by Lemma 1 so $f(gh) = gf(h) + f(g)$, as required.

The uniqueness of f is immediate from the fact that f is already defined on a set of generators of G .

Lemmas 2(iii) and 3 tell us how to find $\dim_K(Cr(G, A))$: we look in A for elements a_1, \dots, a_s satisfying the relations $w_j^*(f) = 0$ which are necessary if f is to be an element of $Cr(G, A)$ with $f(g_i) = a_i$, $i = 1, \dots, s$. The point of doing this is explained in the next result.

Let V, W be two left KG -modules. The dual module W^* is given the structure of a left KG -module by defining $(gw^*)(w) = w^*(g^{-1}w)$ for $g \in G$, $w^* \in W^*$ and $w \in W$. Then $V \otimes_K W^* = A$ is a left KG -module if we define $g(v \otimes w^*) = gv \otimes gw^*$. Let $C_A(G)$ denote $\{a \mid a \in A \text{ and } ga = a \text{ for all } g \in G\}$.

LEMMA 4. *If $\dim_K(Cr(G, A)) \leq \dim_K(A) - \dim_K(C_A(G))$, then every KG -extension of V by W is a split extension.*

Proof. By Theorem 10, page 235, of [2], there is a one-to-one correspondence between classes of equivalent KG -extensions of V by W , and elements of $H^1(G, A)$, and by [2], page 231, $H^1(G, A)$ is the quotient space $Cr(G, A)/P$, where P is the subspace of principal crossed homomorphisms, that is, $P = \{f: G \rightarrow A \mid \text{for some } a \in A, f(g) = ga - a \text{ for all } g \in G\}$.

To prove Lemma 4, therefore, it suffices to show that $\dim P \geq \dim(Cr(G, A))$, and so by the hypothesis, we need only prove $\dim P \geq \dim A - \dim(C_A(G))$.

Let $\{a_{r+1}, \dots, a_n\}$ be a basis for $C_A(G)$, and extend it to a basis $\{a_1, \dots, a_r, a_{r+1}, \dots, a_n\}$ for A . For $i = 1, \dots, r$ define $f_i(g) = ga_i - a_i$ for all $g \in G$, so that $f_i \in P$. If we have $\sum_{i=1}^r \alpha_i f_i = 0$ with $\alpha_i \in K$, $i = 1, \dots, r$, then for all $g \in G$, $\sum_{i=1}^r \alpha_i (ga_i - a_i) = 0$, so that for all $g \in G$, $\sum_{i=1}^r \alpha_i a_i = g(\sum_{i=1}^r \alpha_i a_i)$.

Thus $\sum_{i=1}^r \alpha_i a_i \in C_A(G)$, so $\alpha_i = 0$ for $i = 1, \dots, r$. Hence f_1, \dots, f_r are linearly independent, and the Lemma is proved.

2. $SL(2, 2^n)$. As an application we take $G = SL(2, 2^n)$ and $K = GF(2^n)$. Let $V = V_0$ be the 'natural' 2-dimensional representation of G over K . Then G is generated by elements g_1, g_2, g_3 whose action on V_0 can be represented by matrices $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix}$, where θ is

a primitive $(2^n - 1)$ st root of 1. A short calculation shows that g_1, g_2 and g_3 satisfy the relations

$$(*) \quad \begin{cases} w_1 = (x_1 x_2)^3 & w_2 = (x_1 x_3)^2 \\ w_3 = x_1^2, & w_4 = x_2^2, & w_5 = x_3^k, \quad \text{where } k = 2^n - 1. \end{cases}$$

We take $W = (V_i)^*$, where V_i is the (2-dimensional) representation of G over K obtained by applying the field automorphism $\beta \rightarrow \beta^{2^i}$ to the entries of the matrices above. (In fact, all 2-dimensional irreducible representations of G over K are of this form—see [1], Theorem 8.2). Thus W^* has a basis with respect to which the matrices of g_1, g_2, g_3 are respectively $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} \psi & 0 \\ 0 & \psi^{-1} \end{pmatrix}$, where $\psi = \theta^{2^i}$.

Let $A = V \otimes_K W^*$, take $f \in Cr(G, A)$ and suppose $f(g_i) = a_i$, $i = 1, 2, 3$. Then from (*) and Lemma 2(iii) we have

$$(1) \quad 0 = w_1^*(f) = (g_1 g_2 g_1 g_2 + g_1 g_2 + 1)a_1 + (g_1 g_2 g_1 g_2 g_1 + g_1 g_2 g_1 + g_1)a_2$$

$$(2) \quad 0 = w_2^*(f) = (g_1 g_3 + 1)a_1 + (g_1 g_3 g_1 + g_1)a_3$$

$$(3) \quad 0 = w_3^*(f) = (g_1 + 1)a_1$$

$$(4) \quad 0 = w_4^*(f) = (g_2 + 1)a_2$$

$$(5) \quad 0 = w_5^*(f) = (g_3^{k-1} + g_3^{k-2} + \dots + g_3 + 1)a_3.$$

If we use the relations (*), and equations (3) and (4), equation (1) can be re-written as

$$(1') \quad (g_2 + g_1 g_2 + 1)a_1 + (1 + g_2 g_1 + g_1)a_2 = 0.$$

If we multiply equation (2) by g_1 and note that $g_1^2 = 1$ and $g_1 a_1 = a_1$ (equation (3)), then we obtain

$$(2') \quad (g_3 + 1)a_1 + (g_3 g_1 + 1)a_3 = 0.$$

Let $\bar{g}_1, \bar{g}_2, \bar{g}_3$ be matrices representing g_1, g_2, g_3 respectively in A . Then it is straightforward to calculate that the rank of the matrix

$$M = \begin{pmatrix} \bar{g}_2 + \bar{g}_1 \bar{g}_2 + 1 & 1 + \bar{g}_2 \bar{g}_1 + \bar{g}_1 & 0 \\ \bar{g}_3 + 1 & 0 & \bar{g}_3 \bar{g}_1 + 1 \\ \bar{g}_1 + 1 & 0 & 0 \\ 0 & \bar{g}_2 + 1 & 0 \\ 0 & 0 & \bar{h} \end{pmatrix}$$

where $\bar{h} = \sum_{t=0}^{k-1} \bar{g}_3^t$, is 8 if $i \neq 0$ and 9 if $i = 0$.

Secondly, it is easy to show that $C_A(G) = 0$ if $i \neq 0$, and that $\dim_K(C_A(G)) = 1$ if $i = 0$. Thus in either case, $\dim_K(Cr(G, A)) \leq 3.4 - \text{rank}(M) \leq \dim_K A - \dim_K(C_A(G))$. Hence by Lemma 4, for any i , any KG -extensions of V by W is a split extension.

REFERENCES

1. G. Higman, *Odd Characterisations of Finite Simple Groups*, Lecture notes, University of Michigan, 1968.
2. D. G. Northcott, *An Introduction to Homological Algebra*, Cambridge University Press, 1962.

Received November 9, 1971.

MATHEMATICAL INSTITUTE
UNIVERSITY OF OXFORD
OXFORD OXI 3LB, ENGLAND

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. SAMELSON

Stanford University
Stanford, California 94305

J. DUGUNDJI

Department of Mathematics
University of Southern California
Los Angeles, California 90007

C. R. HOBBY

University of Washington
Seattle, Washington 98105

RICHARD ARENS

University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY

UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
NAVAL WEAPONS CENTER

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. The editorial "we" must not be used in the synopsis, and items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. Index to Vol. 39. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966. Regular subscription rate: \$48.00 a year (6 Vols., 12 issues). Special rate: \$24.00 a year to individual members of supporting institutions.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 270, 3-chome Totsuka-cho, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics

Vol. 45, No. 2

October, 1973

Kenneth Paul Baclawski and Kenneth Kapp, <i>Induced topologies for quasigroups and loops</i>	393
D. G. Bourgin, <i>Fixed point and min — max theorems</i>	403
J. L. Brenner, <i>Zolotarev's theorem on the Legendre symbol</i>	413
Jospeh Atkins Childress, Jr., <i>Restricting isotopies of spheres</i>	415
John Edward Coury, <i>Some results on lacunary Walsh series</i>	419
James B. Derr and N. P. Mukherjee, <i>Generalized Sylow tower groups. II</i>	427
Paul Frazier Duvall, Jr., Peter Fletcher and Robert Allen McCoy, <i>Isotopy Galois spaces</i>	435
Mary Rodriguez Embry, <i>Strictly cyclic operator algebras on a Banach space</i>	443
Abi (Abiadbollah) Fattahi, <i>On generalizations of Sylow tower groups</i>	453
Burton I. Fein and Murray M. Schacher, <i>Maximal subfields of tensor products</i> ...	479
Ervin Fried and J. Sichler, <i>Homomorphisms of commutative rings with unit element</i>	485
Kenneth R. Goodearl, <i>Essential products of nonsingular rings</i>	493
George Grätzer, Bjarni Jónsson and H. Lakser, <i>The amalgamation property in equational classes of modular lattices</i>	507
H. Groemer, <i>On some mean values associated with a randomly selected simplex in a convex set</i>	525
Marcel Herzog, <i>Central 2-Sylow intersections</i>	535
Joel Saul Hillel, <i>On the number of type-k translation-invariant groups</i>	539
Ronald Brian Kirk, <i>A note on the Mackey topology for $(C^b(X)^*, C^b(X))$</i>	543
J. W. Lea, <i>The peripherality of irreducible elements of lattice</i>	555
John Stewart Locker, <i>Self-adjointness for multi-point differential operators</i>	561
Robert Patrick Martineau, <i>Splitting of group representations</i>	571
Robert Massagli, <i>On a new radical in a topological ring</i>	577
James Murdoch McPherson, <i>Wild arcs in three-space. I. Families of Fox-Artin arcs</i>	585
James Murdoch McPherson, <i>Wild arcs in three-space. III. An invariant of oriented local type for exceptional arcs</i>	599
Fred Richman, <i>The constructive theory of countable abelian p-groups</i>	621
Edward Barry Saff and J. L. Walsh, <i>On the convergence of rational functions which interpolate in the roots of unity</i>	639
Harold Eugene Schlais, <i>Non-aposyndesis and non-hereditary decomposability</i>	643
Mark Lawrence Teply, <i>A class of divisible modules</i>	653
Edward Joseph Tully, Jr., <i>\mathcal{H}-commutative semigroups in which each homomorphism is uniquely determined by its kernel</i>	669
Garth William Warner, Jr., <i>Zeta functions on the real general linear group</i>	681
Keith Yale, <i>Cocycles with range $\{\pm 1\}$</i>	693
Chi-Lin Yen, <i>On the rest points of a nonlinear nonexpansive semigroup</i>	699