The Australian National University

53

ON THE FIRST COHOMOLOGY OF A FINITE GROUP WITH COEFFICIENTS IN A SIMPLE MODULE

L.G. Kovács

RESEARCH REPORT No. 43 - 1984

Department of Mathematics, IAS

Mathematical Sciences Research Centre

ANU MSRC Research Report 43-1984

ON THE FIRST COHOMOLOGY OF A FINITE GROUP WITH COEFFICIENTS IN A SIMPLE MODULE

L.G. Kovács[*]

Abstract

The aim of this report is to describe (in as elementary terms as possible) a reduction of the calculation of the first cohomology group of a finite group with coefficients in a simple module, to the case of faithful modules and groups with nonabelian simple socle. As applications, estimates are derived for the size of the first cohomology group, for the minimum number of generators of certain semidirect products, and for the generation gap and presentation rank.

[*] The essential part of the work reported here was done, over ten years ago, jointly or simultaneously with Dr John Cossey of this University and Professor K.W. Gruenberg of Queen Mary College, London. We hoped to write a joint paper for publication but so far this has proved impossible. While the present version owes much to their influence, the responsibility for its failings is all mine.

1. Introduction

As is well known, if G is a group and V is a G-module, the first cohomology group $H^1(G,V)$ is bijective with the set of conjugacy classes of complements of V in the semidirect product GV, and can be defined simply (without any reference to the homology of cochain complexes) in terms of the derivations of G into V. The first of these points makes $H^1(G,V)$ relevant even to those users of groups who are neither interested nor experienced in cohomology, while the second makes it possible to keep this exposition easily accessible to such readers. No cohomology will be assumed (directly or indirectly) in the main body of the paper, where the problem of determining $H^1(G,V)$ for finite G and simple V is reduced to the case of nearly simple G and faithful V. (We call a finite group nearly simple if it has only one minimal normal subgroup and that is nonabelian and simple.) This reduction has been around for some time but deserves to be better known, especially now that all nearly simple groups are believed to have been "classified".

Except in Section 3, all G-modules considered will be right $\mathbb{Z}G$-modules. Whether we call a (sub)module "trivial" or "nontrivial" depends only on the action on it: we use "nonzero" or "proper" to exclude the zero (sub)module or the whole module. Each simple module is naturally an $\mathbb{F}_pG$-module for some finite prime field $\mathbb{F}_p$; we refer to the relevant prime p as the characteristic of the module. [If one wants cohomology with coefficients in a simple $\mathbb{F}G$-module U for some other field $\mathbb{F}$, one notes that $H^1(G,U) = 0$ unless $\mathbb{F}$ contains some $\mathbb{F}_p$, in which case there is a unique simple $\mathbb{F}_pG$-module V such that $V \otimes_{\mathbb{F}_p} \mathbb{F}$ is the direct sum of the Galois-conjugates of U, and then

$H^1(G,V) \otimes_{\mathbb{F}_p} \mathbb{F}$ is the direct sum of n copies of $H^1(G,U)$ where n is the number of isomorphism types of Galois conjugates of U. This reduces the calculation of $H^1(G,U)$ to that of $H^1(G,V)$.]

In order to state the Reduction Theorem, we have to introduce some technicalities. Let G be finite and V a simple G-module. The G-endomorphisms of V form a finite field $\mathrm{End}_G V$, and $H^1(G,V)$ is a vector space over this field. Let C stand for the centralizer of V in G (that is, for the kernel of the action of G on V). Choose a chief series in G, and denote by k the number of chief factors in this series that are G-isomorphic to V and complemented in G.

REDUCTION THEOREM. The dimension of $H^1(G,V)$ over $\mathrm{End}_G V$ is k, except perhaps when the following hold. There is only one minimal normal subgroup in G/C, say N/C; this is nonabelian and has order divisible by the characteristic of V. Let S/C be a simple direct factor of N/C; write A and B for the normalizer and the centralizer of S/C, respectively, so A/B is a nearly simple group with socle BN/B $(\cong S/C)$; and let W be the largest trivial $(B \cap N)$-submodule of V. If $W = 0$ or if B acts nontrivially on W, the dimension is still k. Otherwise W is a faithful simple A/B-module with $\mathrm{End}_{A/B} W \cong \mathrm{End}_G V$, and the dimension is k plus the dimension of $H^1(A/B,W)$.

In the last case, V is W induced from A to G, and of course it can still happen that $H^1(A/B,W) = 0$ so the dimension is k. The proof of the theorem will not amount to a mere dimension count: instead, it will be obtained in terms of certain homomorphisms which are all "natural" in a strict technical sense (that will not be elaborated here). Naming these homomorphisms (in Section 5) makes the theorem stronger than what can be made explicit in this Introduction.

After the first draft of this note was completed, we learned that a forthcoming paper [1] of Aschbacher and Scott will contain a variant of the reduction discussed here under the extra hypothesis that $C = 1$ (with different proof and motivation). We gratefully acknowledge the opportunity to see a draft of that paper.

2. Some group theory

Our preparations start with some elementary facts on finite groups. While we have no entirely convenient reference, all the ideas go back to Gaschütz [6], [7] (see also Section 15 in Chapter VII of Huppert and Blackburn [15]).

Let G be a finite group and V a simple G-module. Set

$$C = \{g \in G \mid vg = v \text{ for all } v \text{ in } V\} .$$

Let D denote the intersection of all subgroups H of G that complement chief factors K/L of G which are (G-) isomorphic to V (so $H \cap K = L$ and $HK = G$) ; if there is no such H, put $D = C$.

2.1 LEMMA. A chief factor K/L of G is complemented and isomorphic to V if and only if $C \geqq KD > LD$.

Proof. Suppose first that at least one chief factor K/L is isomorphic to V and has a complement H. We derive some general information before adressing the proof of the Lemma. Obviously, $C \geq K > L$. As $(H\cap C)/L$ is normal in H/L and centralized by K/L, it is normal in HK/L : thus $H \cap C$ is normal in G. By Dedekind's Law $C = (H\cap C)K$, and so $C/(H\cap C) = (H\cap C)K/(H\cap C) \cong K/(H\cap C\cap K) = K/L \cong V$.

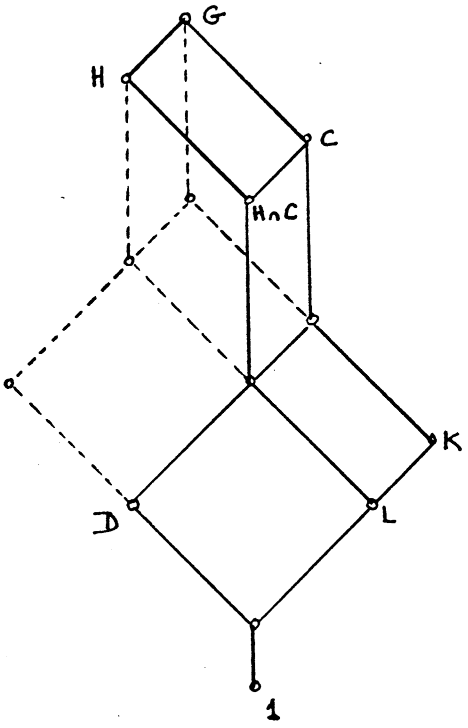

Fig. 1

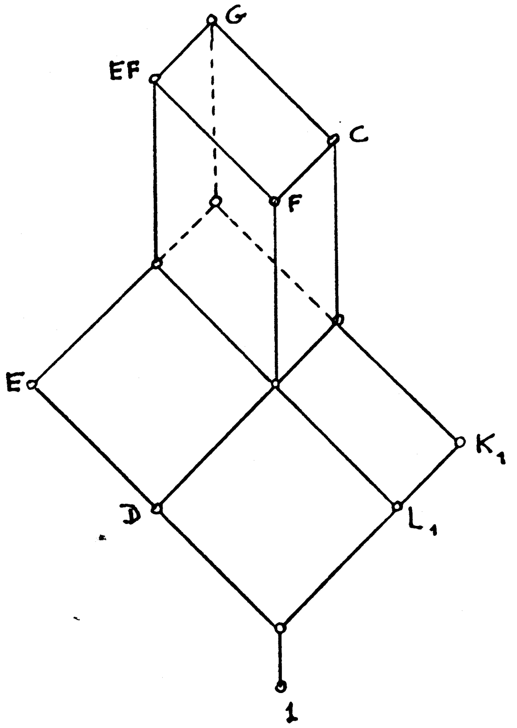

Fig. 2

It follows that $C/(H\cap C)$ is a self-centralizing minimal normal subgroup complemented by $H/(H\cap C)$ in $G/(H\cap C)$: hence H is a maximal subgroup of G , and $H \cap C$ is the intersection of the conjugates of H . Therefore D is normal, C/D ($\neq 1$) is a direct product of isomorphic copies of V , and the Frattini subgroup of G/D is trivial: so (see III.4.4 in Huppert [14]) C/D has a complement, say E/D , in G/D . Of course in this case $C \geq KD > LD$, for $LD \leqq H \ngeq K$, so the "only if" part of the lemma is proved.

For the proof of the converse, suppose that K_1/L_1 is a chief factor and $C \geqq K_1D > L_1D$. Then $K_1 \cap L_1D$ is a normal subgroup of G and $K_1 > K_1 \cap L_1D \geqq L_1$, so we must have $K_1 \cap L_1D = L_1$ (Fig.2). Hence K_1/L_1 is isomorphic to K_1D/L_1D which, as each composition factor of the G-module C/D , is isomorphic to V and complemented in C/D . Let F/D be such a complement : that is, F is normal in G , $F \cap K_1D = L_1D$, $FK_1D = C$. It is now easy to see that EF is a subgroup which complements K_1/L_1 in G .

This discussion also showed that $C/D = 1$ if and only if no complemented chief factor of G is isomorphic to V . As $C/D = 1$ obviously if and only if no chief factor K/L satisfies $C \geqq KD > LD$, the proof is complete.

2.2 THEOREM. The number k of complemented chief factors isomorphic to V in any one chief series of G is independent of the choice of the chief series; C/D is the direct product of k copies of V .

Proof. If $G = G_1 > \ldots > G_i > \ldots$ is a chief series of G , the distinct G_iD/D with $C \geqq G_i$ form a composition series of the G-module C/D . Lemma 2.1, and the observation in its proof on the structure of C/D , then yield the theorem.

2.3 COROLLARY. No chief factor of the form D/L can be complemented and isomorphic to V .

2.4 COROLLARY. Each chief factor of the form C/L with $L \geqq D$ is complemented and isomorphic to V .

In comparing our reduction with previously published material, we shall make use of one more point : see VII.15.4a (and its proof) in Huppert and Blackburn [15].

2.5 If G is p-soluble where p is the characteristic of V , then $O_{p'}(G/C) > 1$ (unless $G/C = 1$) , and each chief factor C/L isomorphic to V is complemented (and therefore has $L \geqq D$) .

The notation of this section will be used again from Section 5 onwards. We stress that C , D , and k depend on (the isomorphism type of) V . This dependence could have been indicated by using, say, C_V , D_V , and k_V : we trust that the simple notation adopted will not lead to confusion.

3. Some representation theory

The main result we shall need from representation theory is Clifford's Theorem : let us recall the relevant part of the usual statement (III.17.3 in Huppert [14], 11.1 in Curtis and Reiner [4]).

3.1 CLIFFORD'S THEOREM. Let $\mathbb{F}$ be any field, N a normal subgroup in a (not necessarily finite) group G , V a finite dimensional simple $\mathbb{F}G$-module , and U a simple $\mathbb{F}N$-submodule of V . For each g in G , Ug is a simple $\mathbb{F}N$-submodule, and V is the sum of the Ug (so in particular V is semi-simple). The "stabilizer" or "inertia group" T of U in G is defined by

$$T = \{g \in G \mid Ug \cong_{\mathbb{F}N} U\} .$$

The sum $\sum_{t \in T} Ut$ is a simple $\mathbb{F}T$-submodule in V , and V is (isomorphic to) the induced module $(\Sigma Ut) \otimes_{\mathbb{F}T} \mathbb{F}G$.

To prepare for the intended applications of this result, we add some comments here. For each subgroup A of G containing T , "transitivity of induction" appears here in a very concrete form; namely, $\sum_{a \in A} Ua$ is the induced module $(\Sigma Ut) \otimes_{\mathbb{F}T} \mathbb{F}A$, and V is ΣUa induced from A to G :

3.2 $$V \cong (\sum_{a\in A} Ua) \otimes_{\mathbb{F}A} \mathbb{F}G \;.$$

A subgroup A of G contains T if and only if

3.3 $$Ug \underset{\mathbb{F}N}{\not\cong} Ua \quad \text{whenever} \quad g \in G \,,\; g \notin A \,,\; a \in A$$

(for, by definition of T, $Ug \underset{\mathbb{F}N}{\not\cong} Ua$ is equivalent to $ga^{-1} \notin T$). It follows that if $A \geqq T$ then there is no nonzero $\mathbb{F}N$-homomorphism from $\sum_{a\in A} Ua$ to $\sum_{g\notin A} Ug$, nor in the opposite direction; in particular,

3.4 $$V = (\Sigma Ua) \oplus (\Sigma Ug)$$

and *a fortiori* $\mathrm{End}_{\mathbb{F}A} V = \mathrm{End}_{\mathbb{F}A}(\Sigma Ua) \oplus \mathrm{End}_{\mathbb{F}A}(\Sigma Ug)$, a direct sum of $\mathbb{F}$-algebras. Thus there is an algebra homomorphism from the subalgebra $\mathrm{End}_{\mathbb{F}G} V$ of $\mathrm{End}_{\mathbb{F}A} V$ into $\mathrm{End}_{\mathbb{F}A}(\Sigma Ua)$, while the functorial nature of induction guarantees an algebra homomorphism in the opposite direction. As V is a simple $\mathbb{F}G$-module and ΣUa is a simple $\mathbb{F}A$-module, their endomorphism algebras are finite dimensional division algebras, so the two homomorphisms must in fact be isomorphisms :

3.5 $$\mathrm{End}_{\mathbb{F}G} V \cong \mathrm{End}_{\mathbb{F}A}(\Sigma Ua) \;.$$

Thus we have established that 3.3 implies 3.2, 3.4, and 3.5.

Finally, recall (say, from VII.4.11 in Huppert and Blackburn [15]) that if the index $|G:H|$ is finite and W is an $\mathbb{F}H$-module [or $\mathbb{Z}H$-module], then the induced module $W \otimes_{\mathbb{F}H} \mathbb{F}G$ [or $W \otimes_{\mathbb{Z}H} \mathbb{Z}G$] is naturally isomorphic to the coinduced module $\mathrm{Hom}_{\mathbb{F}H}(\mathbb{F}G,W)$ [or $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,W)$] .

4. Derivations

In this section we develop all relevant facts from first principles. Many a tedious verification is omitted, but (we hope) never more than one line at a time, and none that would call for a fresh idea.

Let G be any group and V any G-module. A map $d : G \to V$ is called a *derivation* if

$$(gh)d = (gd)h + hd \qquad \text{for all } g,h \text{ in } G$$

[so in particular $1d = 0$ and $g^{-1}d = -(gd)g^{-1}$] . The set $\mathrm{Der}(G,V)$ of all such maps is an abelian group with respect to the addition defined by $g(d+d') = gd + gd'$. Obviously, the exponent of $\mathrm{Der}(G,V)$ divides that of V . To each v in V there is a derivation

$$(\mathrm{ider}\ v) : g \mapsto v - vg .$$

These "inner" derivations form a subgroup $\mathrm{Ider}(G,V)$ in $\mathrm{Der}(G,V)$. For our purposes $H^1(G,V)$ is defined as the factor group :

$$H^1(G,V) = \mathrm{Der}(G,V)/\mathrm{Ider}(G,V) .$$

[The motivation relevant here is the following. If H is a complement of V in the semidirect product GV , then to each g in G there is a unique u in V such that $gu \in H$, and the map $g \mapsto u$ is then a derivation. Conversely, if $d \in \mathrm{Der}(G,V)$ then $\{g(gd) \mid g \in G\}$ is a complement of V in GV , equal to the conjugate vGv^{-1} of G if and only if $d = \mathrm{ider}\ v$. See Robinson [17], pp.304-305.]

Let N be a normal subgroup of G . As usual, write $\mathrm{Der}(N,V)$ for the derivations of N into the N-module obtained from V by restriction. There is a G-action on $\mathrm{Der}(N,V)$ given by

$$x(d^g) = [(gxg^{-1})d]g \qquad \text{for all } x \text{ in } N .$$

The map $\mathrm{ider} : V \to \mathrm{Der}(N,V)$ is a G-homomorphism; its image is $\mathrm{Ider}(N,V)$, and its kernel the largest trivial N-submodule V^N of V. Moreover, as

4.1 $$d^y = d - \mathrm{ider}(yd) \qquad \text{for all } y \text{ in } N ,$$

the action of N on the factor module $H^1(N,V) = \mathrm{Der}(N,V)/\mathrm{Ider}(N,V)$ is trivial. In particular (take $N = G$), the action of G on $H^1(G,V)$ is trivial.

We interrupt the general development to establish some other useful consequences of 4.1.

4.1' If $V^G = 0$, no nonzero G-submodule of $\mathrm{Der}(G,V)$ can avoid $\mathrm{Ider}(G,V)$.

Indeed, if d lies in a G-submodule V_1 which avoids $\mathrm{Ider}(G,V)$, then 4.1 (still with $N = G$) yields $\mathrm{ider}(gd) = d - d^g \in V_1 \cap \mathrm{Ider}(G,V) = 0$, so $gd \in V^G$ for all g, and hence $d = 0$.

4.1" If N is normal in G and $V^N = 0$, then $\mathrm{Der}(G,V)^N = 0$.

For, if $V^N = 0$ then also $V^G = 0$, so $\mathrm{Ider}(G,V)$ is isomorphic to V and hence avoids the largest trivial N-submodule $\mathrm{Der}(G,V)^N$; on the other hand, the latter is a G-submodule (because N is normal).

4.1"' If V has prime exponent p and G has a normal subgroup N of finite order prime to p with $V^N = 0$, then $H^1(G,V) = 0$.

For, by Maschke's Theorem $\mathrm{Ider}(G,V)$ has an N-admissible complement in $\mathrm{Der}(G,V)$; that complement is isomorphic to the trivial module $H^1(G,V)$, and so must be 0 by 4.1".

Let us return now to the general development. Restriction of maps gives the "restriction map" Der(G,V) → Der(N,V) ; clearly, this is a G-homomorphism. If d is in its kernel, then $Nd = 0$ and so

$$(gd)x = (gd)x + xd = (gx)d = [(gxg^{-1})g]d = [(gxg^{-1})d]g + gd = gd$$

(for all g in G and x in N) shows that d is constant on each coset of N in G and that the image of d lies in V^N : thus d may be viewed as a derivation of G/N into V^N (with V^N considered a G/N-module in the obvious way). Of course ider v lies in the kernel of the restriction map if and only if $v \in V^N$. Differently put : $\mathrm{Der}(G/N,V^N)$ embeds in Der(G,V) as the kernel of the restriction map, interesting Ider(G,V) precisely in $\mathrm{Ider}(G/N,V^N)$. On the other hand, the restriction map takes Ider(G,V) onto Ider(N,V) and so yields a G-homomorphism of $H^1(G,V)$ into $H^1(N,V)$. As noted above, $H^1(G,V)$ is a trivial G-module, so the image of this homomorphism must lie in the largest trivial submodule $H^1(N,V)^G$ of $H^1(N,V)$.

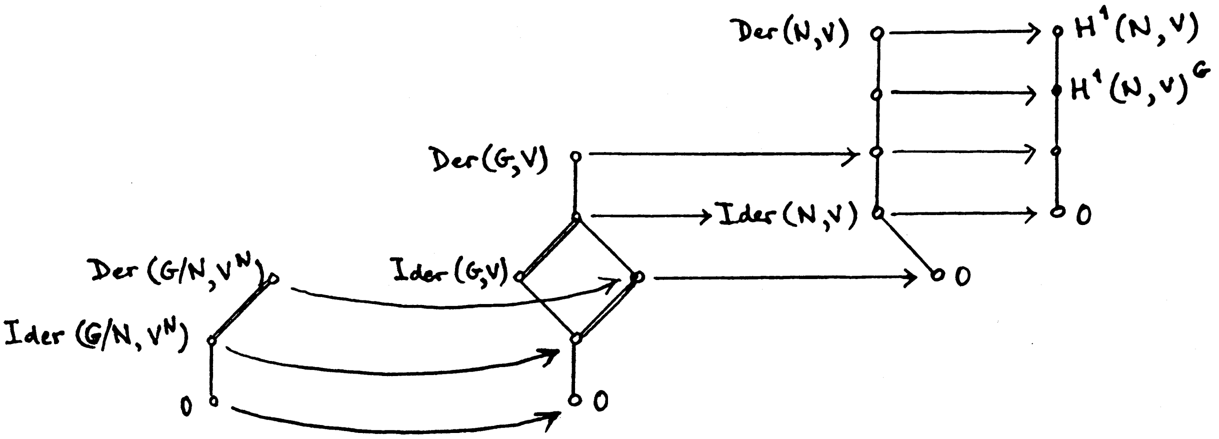

Fig. 3

These comments have established the "inflation-restriction exact sequence"

4.2 $$0 \to H^1(G/N,V^N) \xrightarrow{\text{inf}} H^1(G,V) \xrightarrow{\text{res}} H^1(N,V)^G .$$

The fact that the composite of a derivation and a module homomorphism is a derivation, leads to each term of this sequence being an $(\mathrm{End}_G V)$-module and each map an $(\mathrm{End}_G V)$-homomorphism. (This is just the first half of the so-called five term sequence well known in the context of spectral sequences : see for instance MacLane [16], XI §10.)

If N acts trivially on V (so $V^N = V$ and V itself may be viewed a G/N-module), then of course $\mathrm{Der}(N,V) = \mathrm{Hom}(N,V)$ and $\mathrm{Ider}(N,V) = 0$, so $H^1(N,V)^G = \mathrm{Hom}_G(N,V)$ and our exact sequence takes the form

4.2' $$0 \to H^1(G/N,V) \xrightarrow{\text{inf}} H^1(G,V) \xrightarrow{\text{res}} \mathrm{Hom}_G(N,V) .$$

Consider briefly also the other extreme : when $V^N = 0$. In this case res is an isomorphism :

4.2" $$H^1(G,V) \cong H^1(N,V)^G .$$

To see this, we only have to add to the foregoing that now res is surjective : indeed, if $d \in \mathrm{Der}(N,V)$ and $d + \mathrm{Ider}(N,V) \in H^1(N,V)^G$, then for each g in G there is a v_g in V such that $d - d^g = \mathrm{ider}\, v_g$; this v_g is unique because $V^N = 0$, and $g \mapsto v_g$ is easily seen to be a derivation of G that extends d .

Three other general facts will be needed. It is straightforward to prove that $\mathrm{Der}(G,-)$, $\mathrm{Ider}(G,-)$, and therefore also $H^1(G,-)$, respect direct sums :

4.3 $$H^1(G,V_1 \oplus V_2) \cong H^1(G,V_1) \oplus H^1(G,V_2) .$$

Also, that if N is a normal subgroup of G and U is an N-submodule of V, then for Ug (with $g \in G$), which is of course also an N-submodule, we have

4.4 $$H^1(N,Ug) \cong H^1(N,U) .$$

The third claim is not so trivial.

4.5 If H is a subgroup of G and V is coinduced from an H-module W, then $H^1(G,V) \cong H^1(H,W)$.

This is known (for all H^n) as Shapiro's Lemma (see for instance p.92 in [8], or III.6.2 in Brown [2]); to keep our promise of not assuming any cohomology, we sketch a bare-handed proof (for the case we require).

Recall that the G-module V coinduced by W is defined as $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,W)$, with G-action given by $(vg)(x) = v(gx)$, and that $v \mapsto v(1)$ is an H-homomorphism of V onto W. Restriction $\mathrm{Der}(G,V) \to \mathrm{Der}(H,V)$ followed by composition with this module homomorphism yields a group homomorphism $\mathrm{Der}(G,V) \to \mathrm{Der}(H,W)$ which maps $\mathrm{Ider}(G,V)$ onto $\mathrm{Ider}(H,W)$. This in turn yields an isomorphism $H^1(G,V) \cong H^1(H,W)$ provided that

(i) if $d \in \mathrm{Der}(G,V)$ and $(hd)(1) = 0$ for all h in H, then d is inner; and

(ii) if $c \in \mathrm{Der}(H,W)$ then there exists a d in $\mathrm{Der}(G,V)$ such that $(hd)(1) = hc$ for all h in H.

To establish these two points, first take d as in (i); define v for x in G by $v(x) = (x^{-1}d)x$, and on $\mathbb{Z}G$ by linear extension of this. The hypothesis on d yields that $v(H) = 0$; this is used in showing that v is an H-homomorphism; and then $\mathrm{ider}\ v = d$ is virtually immediate. Next, let c be as in (ii), and let R be a complete set of representatives of the left cosets of H in G : thus $G = \dot{\bigcup}_{r\in R} rH$. Define first a map $G \to W$, $g \mapsto \bar{g}$ by $\overline{rh} = hc$, and verify that $\overline{gh} = \bar{g}h + \bar{h}$ whenever $g \in G$ and $h \in H$. Then define $d : G \to V$ by setting $(gd)(x) = \overline{gx} - \bar{x}$ for each $g , x \in G$; check that each gd is an H-map so $gd \in V$; that d is derivation; and that $(hd)(1) = hc$ whenever $h \in H$. This will complete the proof of 4.5.

What we shall actually use is the following combination of 4.5 with the reminder at the end of Section 3.

4.5' If H has finite index in G and V is the G-module induced from the H-module W , then $H^1(G,V) \cong H^1(H,W)$.

Next we note a simple estimate.

4.6 If V is simple and G is finitely generated, say, by m elements, and if the cardinality $|V|$ of V is finite, then $|H^1(G,V)| \leq |V|^{m-1}|V^G|$ with equality if and only if the semidirect product GV cannot be generated by m elements.

Proof. The inequality is clearly equivalent to $|\mathrm{Der}(G,V)| \leq |V|^m$. Let $g_1,\ldots,g_m$ generate G . Each complement of V in GV is generated by $g_1v_1,\ldots,g_mv_m$ with uniquely determined $v_1,\ldots,v_m$ in V . If for some choice of $v_1,\ldots,v_m$ the subgroup generated by $g_1v_1,\ldots,g_mv_m$ is not a complement, it must be GV itself (because of the simplicity of V) ; conversely if GV can be generated by m elements, by a result of Gaschütz [5] it must be generated by m elements of this form.

Finally, we shall need a result which we first proved using Lemma 2 of our [3] or the equivalent 6.11 of [9]. The proof we present here makes use of an idea of Professor I.M. Isaacs.

4.7 LEMMA. If G is finite, V is simple, M and N are (not necessarily distinct) normal subgroups of G such that each element of M commutes with each element of N and neither M nor N acts trivially on V, then $H^1(G,V) = 0$.

Proof. Now V is isomorphic to $\mathrm{Ider}(G,V)$: for ease of notation, identify these two modules and write U for $\mathrm{Der}(G,V)$. Let p denote the characteristic of V; then U is also of exponent p. Recall that U/V is a trivial G-module; thus if H is a subgroup of G such that U happens to be semi-simple as H-module then $U = U^H + V$. By assumption, neither V^M nor V^N is V; as they are G-submodules and V is simple, $V^M = V^N = V^G = 0$.

If M acted on V as a p-group, each simple M-submodule of V would be trivial, contrary to $V^M = 0$. Thus some element of order prime to p in M must act nontrivially on V; let L be a cyclic subgroup generated by such an element. By Maschke's Theorem, U is semisimple as L-module, so $U = U^L + V$; by the choice of L, $U^L < U$. Since N normalizes (even centralizes) L, U^L is an N-submodule. Let Y be a maximal N-submodule of U containing U^L; *a fortiori*, $U = Y + V$ so $Y \ngeq V$. Now Yg is also a maximal N-submodule, for each g in G, and the intersection of the Yg is a G-submodule which cannot contain and so must avoid the simple G-submodule V. By 4.1', that intersection is zero. It follows that U is a semisimple N-module, whence $U = U^N + V$. As $U^N = 0$ by 4.1", this completes the proof.

We note that if the hypothesis is modified so that M acts non-trivially on V but N acts trivially, then $\mathrm{Hom}_G(N,V) = 0$ (because M acts trivially on N while $V^M = 0$) and so in 4.2' inf must be an isomorphism. Combined with this observation, 4.7 yields 6.11 of [9] as a special case: the most elementary proof yet.

5. The proof of the Reduction Theorem

Let G be a finite group, V a simple G-module (say, of characteristic p), and let C, D, k be as in Section 2.

The first step in the proof of the Reduction Theorem is that in 4.2' with $N = D$,

5.1 $$H^1(G/D,V) \xrightarrow{\text{inf}} H^1(G,V) \text{ is an isomorphism.}$$

To this end, it suffices to prove that the image of $H^1(G,V) \xrightarrow{\text{res}} \text{Hom}_G(D,V)$ is 0. Suppose not: then there is a d in $\text{Der}(G,V)$ whose restriction $d_D : D \to V$ is nonzero. As d_D is a G-homomorphism and V is simple, d_D must be surjective. Let L be the kernel of d_D; then D/L is a chief factor of G isomorphic to V and easily seen to be complemented by $\{h \in G \mid hd = 0\}$, contrary to 2.3. This proves 5.1.

The second step is the application of 4.2' with G/D in place of G and C/D in place of N.

5.2 The sequence $0 \to H^1(G/C,V) \xrightarrow{\text{inf}} H^1(G/D,V) \xrightarrow{\text{res}} \text{Hom}_G(C/D,V) \to 0$ is exact, and the $(\text{End}_G V)$-dimension of $\text{Hom}_G(C/D,V)$ is k.

In view of 2.2 and 4.2', all that remains to establish is the surjectivity of res. To this end, let $\varphi : C/D \to V$ be a nonzero G-homomorphism; note that φ is surjective because V is simple. Let L/D be the kernel of φ; by 2.4, C/L has a complement H. Each element of G/D can be written as hx with $h \in H/D$, $x \in C/D$, and x unique modulo L/D: so $hx \mapsto x$ defines a map $G/D \to V$, and this is easily seen to be a derivation whose restriction to C/D is φ. This proves 5.2.

This much has been available for quite some time, for instance as an easy consequence of 4.1 of [10]; in turn, the present line of argument yields a "transgression-free" proof of that result.

It is also the end of the story if we can be sure that $H^1(G/C,V) = 0$. That is certainly the case if either $G/C = 1$ or $O_{p'}(G/C) > 1$ (cf. 4.1"'), and so for all simple V of characteristic p when G is p-soluble (cf. 2.5). Our result is then the well-known and very useful formula of Gaschütz (on p.93 of Gruenberg and Roggenkamp [13]; see also VII.15.5 and 15.6 in Huppert and Blackburn [15]): by 5.1, 5.2, and 2.5, if G is p-soluble then $H^1(G,V) \cong \mathrm{Hom}_G(C,V)$. (Stammbach [19] proved that if G is not p-soluble, there always exist simple V of characteristic p such that $H^1(G/C,V) \neq 0$.)

Lemma 4.7 yields another sufficient condition: $H^1(G/C,V) = 0$ except perhaps if G/C has only one minimal normal subgroup and that is nonabelian (and of order divisible by p, because of 4.1"). It remains to calculate $H^1(G/C,V)$ in this exceptional case. Let N/C be the unique minimal normal subgroup of G/C, and S/C a simple direct factor of N/C : so N/C is the direct product of the distinct conjugates of S/C. If $S = N$ then G/C is nearly simple and the reduction is complete: suppose this is not the case. Let A/C and B/C denote the normalizer and the centralizer of S/C in G/C, respectively: then N/C is the direct product of S/C and $(B\cap N)/C$, while SB/B $(\cong S/C)$ is the only minimal normal subgroup of A/B.

By Clifford's Theorem (3.1), V is semisimple as N-module. Since $S > C$, S must act nontrivially on some simple N-submodule U of V. If $B \cap N$ also acts nontrivially on U, then $H^1(N/C,U) = 0$ by 4.7; in this case $H^1(N/C,Ug) = 0$ for all g in G (by 4.4) and, as V is the direct sum of a suitable set of the Ug, 4.3 yields that $H^1(N/C,V) = 0$: hence 4.2" gives that also $H^1(G/C,V) = 0$. In particular, we have proved that if $V^{B\cap N} = 0$ then $H^1(G/C,V) = 0$.

Set $W = V^{B\cap N}$; assume $W \neq 0$, and let U be any simple N-submodule of W . Since W admits A and $W^S = V^N = 0$, S acts nontrivially on Ua whenever $a \in A$. On the other hand if $g \notin A$ then gSg^{-1}/C is a simple direct factor of N/C other than S/C and hence $gSg^{-1} \leq B \cap N$: consequently, gSg^{-1} acts trivially on U , that is, S acts trivially on Ug . Thus 3.3 is verified, and 3.2, 3.4, 3.5 follow. As $\Sigma Ua \leq W$ while $\Sigma Ug \leq V^S$ and $W \cap V^S = V^N = 0$, 3.4 yields that $\Sigma Ua = W$, $\Sigma Ug = V^S$, $V = W \oplus V^S$; 3.2 tells us that V is W induced from A to G , and 3.5 that the natural algebra homomorphism $\mathrm{End}_A W \to \mathrm{End}_G V$ is an isomorphism. One may also say that V as G/C-module is induced from the A/C-module W ; Shapiro's Lemma 4.5' then says that $H^1(G/C,V) \cong H^1(A/C,W)$. Since S/C acts nontrivially on W , 4.7 gives that $H^1(A/C,W) = 0$ except perhaps if B/C acts trivially. When B/C does act trivially, we use the fact that $\mathrm{Hom}_G(B/C,W) = 0$ because $W^S = 0$, so by 4.2' (with A/C , B/C, W in place of G , N , V) inf is an isomorphism: $H^1(A/B,W) \cong H^1(A/C,W)$. Finally we apply 4.2" (with A/B , SB/B , W in place of G , N , V) to deduce that res is an isomorphism: $H^1(A/B,W) \cong H^1(SB/B,W)^{A/B}$, that is, $H^1(A/B,W) \cong H^1(S/C,W)^A$. These conclusions may be summarized as follows.

5.3 If $W = 0$ or if B acts nontrivially on W , then $H^1(G,V) = 0$; otherwise W is a faithful simple module for the nearly simple group A/B with $\mathrm{End}_{A/B} W \cong \mathrm{End}_G V$ and $H^1(G,V) \cong H^1(A/B,W) \cong H^1(S/C,W)^A$, and V is W induced from A to G .

This completes the proof of the Reduction Theorem. We stress that all the isomorphisms in 5.3 are (composites of) natural maps (which arise from the functorial nature of induction, Shapiro's Lemma, and various instances of the inflation-restriction sequence 4.2).

6. The generation gap or presentation rank

Our first application will settle an old debt by establishing a result which was announced without proof as (30) in [11].

Let $d(G)$ denote the minimum of the cardinalities of the generating sets of G. For an arbitrary G-module U, let $\delta_{U,t}$ be 1 if U is trivial and 0 otherwise; also, write $d_G(U)$ for the minimum of the cardinalities of the G-module generating sets of U. For each real number x, let $\lceil x \rceil$ be the (unique) integer such that $\lceil x \rceil - 1 < x \leq \lceil x \rceil$; it is straightforward to see that

6.1 $\lceil x/n \rceil = \lceil \lceil x \rceil / n \rceil$ for each positive integer n.

Finally, denote the augmentation ideal of the integral group ring $\mathbb{Z}G$ by $\underline{\underline{g}}$.

The *generation gap* of a finite group G is defined by

$$\text{gap } G = d(G) - d_G(\underline{\underline{g}}) \;;$$

by a theorem of Roggenkamp [18] (Proposition 1 in our [3]), it is equal to the *presentation rank* of G: the context of these concepts was surveyed at length in [9] and [11]. Here we recall only that $\text{gap } G = 0$ if either G is soluble or G can be generated by two elements; and that $\text{gap } G > 0$ if and only if the standard wreath product of an infinite cycle by G can be generated by $d(G)$ elements.

The outstanding claim gives a test for $\text{gap } G > 0$. Even its statement refers to the Reduction Theorem: call a simple G-module V *monolithically induced* if it comes under the last, exceptional case of that Theorem. Explicitly, V is monolithically induced if G/C has only one minimal normal subgroup N/C, this is nonabelian, and if

S/C is a simple direct factor of N/C with centralizer B/C then $V^B \neq 0$: the case of nearly simple G/C is included here, for then $B/C = 1$ and $V^B = V$.

6.2 THEOREM. Assume that $d(G) > d(S/C)$ for every composition factor S/C of the finite group G ($\neq 1$) . The following two conditions together are sufficient to ensure that gap $G > 0$.

(a) $d(G) - 2 \geqq d_G(C/D) - \delta_{V,t}$ whenever V is a complemented abelian chief factor of G that is not monolithically induced;

(b) $(d(G)-2)|G:A| \geqq d((A/B)W^k) - 1$ whenever V is a complemented abelian chief factor of G that is monolithically induced with k , A , B , W as in the Reduction Theorem, and with $(A/B)W^k$ the semidirect product of A/B and the direct product W^k of k copies of W .

If the automizers of the nonabelian composition factors of G are all 2-generator groups, then these conditions are also necessary.

The reason for $d(G) - 2$ on the left hand sides of these inequalities is that by definition gap $G > 0$ if and only if $d(G) - 2 \geqq d_G(\underline{\underline{g}}) - 1$. Theorem 3 of our [3] says in effect that

$$d_G(\underline{\underline{g}}) - 1 = \max\left\{\left\lceil\frac{\dim H^1(G,V)}{\dim V}\right\rceil - \delta_{V,t}\right\}$$

where the maximum is taken over all simple G-modules V : so gap $G > 0$ is equivalent to

(c) $$d(G) - 2 \geqq \left\lceil\frac{\dim H^1(G,V)}{\dim V}\right\rceil - \delta_{V,t} \qquad \text{for all simple } V .$$

By 2.2 and the simple rule (7.12 in [9]) for calculating $d_G(U)$,

$$d_G(C/V) = \left\lceil \frac{k \dim \mathrm{End}_G V}{\dim V} \right\rceil ;$$

hence the Reduction Theorem leads to the inequality in (a) when V is not monolithically induced. If V is of this kind but not isomorphic to any complemented chief factor, that inequality is automatically satisfied (for $d(G) > 1$ by assumption).

For monolithically induced V of course $\delta_{V,t} = 0$, and by the Reduction Theorem $\dim H^1(G,V) = k + \dim H^1(A/B,W)$ while $\dim V = |G:A| \dim W$, all dimensions being taken over the "same" finite field $\mathrm{End}_G V \cong \mathrm{End}_{A/B} W$. Substitute into the right hand side of the inequality in (c) and use 6.1 to move $|G:A|$ to the left hand side:

(d) $$(d(G)-2)|G:A| \geq \left\lceil \frac{k+\dim H^1(A/B,W)}{\dim W} \right\rceil .$$

When $k = 0$ this is automatic: for in the last part of the Reduction Theorem $W^S = 0$ and $|H^1(A/B,W)| \leq |H^1(S/C,W)| \leq |W|^{d(S/C)-1} \leq |W|^{d(G)-2}$ by 4.6 and because $d(G) > d(S/C)$ has been assumed. By the Corollary to Lemma 2 in Gruenberg and Roggenkamp [12] (note this can also be proved without transgressions, as the last line of p.265 in [12] is an easy variant of our 5.2),

$$d((A/B)W^k) - 1 = \max\left\{d(A/B)-1, \left\lceil \frac{k+\dim H^1(A/B,W)}{\dim W} \right\rceil \right\} .$$

Thus (b) certainly implies (d) and so (c) for all monolithically induced V, and the converse implication is also valid under the assumption that $d(A/B)$ is always 2. This completes the proof of 6.2.

6.3 REMARK. In condition (b), one can replace the externally constructed $(A/B)W^k$ by a section A/R of G chosen as follows. (We continue to use the notation of Section 5.) Since $B \cap N$ is normal in the normal subgroup N, repeated application of Clifford's Theorem tells us that V is semi-simple as $(B\cap N)$-module: thus $V = V^{B\cap N} \oplus [V,B\cap N]$. Here $V^{B\cap N} = W$ and in the relevant case all of B acts trivially on W, so we can conclude that $V/[V,B] \cong W$. We know from 2.2 that $C/D \cong V^k$, so $C/[C,B]D \cong W^k$. Also, we saw in Section 2 that C/D has a (usually far from unique) complement in G, which we called E in Fig.2. It is now easy to see that $(E\cap A)[C,B]D$ complements $C/[C,B]D$ in A, and so with $R = B \cap (E\cap A)[C,B]D = (E\cap B)[C,B]D$ we have $B/R \cong C/[C,B]D \cong W^k$ and $A/R \cong (A/B)W^k$. Incidentally, this discussion shows that for a V with $k > 0$, the condition $V^B \neq 0$ in the definition of "monolithically induced" is equivalent to $[C,B]D < C$.

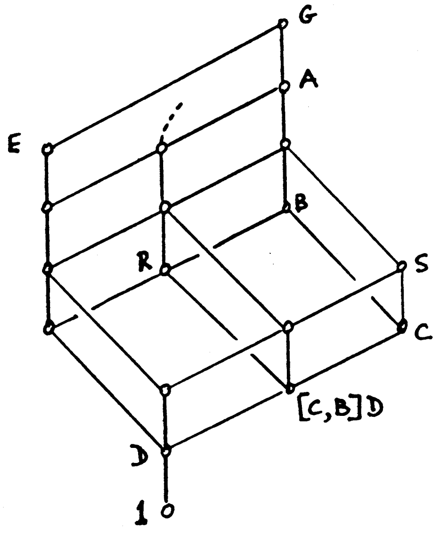

Fig. 4

(In contrast to Figs 1 and 2, Fig.4 gives only part of the sublattice generated in the subgroup lattice of G by the subgroups named: the dotted line is intended to suggest that the join of E and $[C,B]D$ is not shown.)

7. Some other estimates

We retain all the notation established so far; G is finite throughout.

7.1 THEOREM. Suppose that each nonabelian composition factor of G can be generated by two elements one of which has order 2, and let V be a simple G-module not isomorphic to any complemented chief factor of G. Then $|H^1(G,V)| < |V|$.

Proof. By assumption, now $k = 0$ and $C = D$, so $H^1(G,V) = 0$ except perhaps when V is "monolithically induced" in which case by 5.3 $|H^1(G,V)| \leqq |H^1(S/C,W)|$ and $|V| = |W|^{|G:A|}$. Recall from the proof of 5.3 that $W^S = 0$. Also, by Clifford's Theorem W is semisimple as S/C-module. Thus by 4.3 it suffices to prove that $|H^1(S/C,U)| < |U|$ whenever S/C is a nonabelian composition factor of G and U is a simple nontrivial (and therefore faithful) S/C-module.

Let S/C be generated by x and y, with $y^2 = 1$. If $d \in \mathrm{Der}(S/C,U)$, then $0 = y^2d = (yd)(y+1)$ so yd lies in the subspace $\{u \in U \mid u(y+1) = 0\}$. If this subspace U_1 were U itself, then y would act on U as the scalar -1 and so would lie in the centre of the faithfully acting, nonabelian simple S/C. This cannot happen, so $|\mathrm{Der}(S/C,U)| \leqq |U||U_1| < |U|^2$, whence $|H^1(S/C,U)| < |U|$. This completes the proof of 7.1.

7.2 REMARK. If the assumption on composition factors is eased to each being generatable by two elements, the last paragraph simplifies to a direct application of 4.6, and the conclusion is $|H^1(G,V)| \leq |V|$.

In view of 4.6, 7.1 implies the following.

7.3 COROLLARY. Let G be a noncyclic finite group such that each nonabelian composition factor of G can be generated by two elements one of which has order 2, and let V be a simple G-module such that $d(GV) > d(G)$. Then V must be isomorphic to some complemented chief factor of G (that is, $k > 0$).

This is very similar to Theorem A of Thomas [20]. In place of our assumption on composition factors, he requires

(ii) $\quad O_{p'}(G/C) > 1$

(and "complemented" is missing from his conclusion). If it should be proved that every nonabelian finite simple group satisfies our assumption, (ii) could be omitted from his Theorem A. Alternatively, one may keep to (ii) and strengthen his theorem, using 4.6, 5.1, and 5.2, to the following.

7.4 THEOREM. Let G be a noncyclic finite group and V a simple G-module such that $O_{p'}(G/C) > 1$. Then $d(GV) > d(G)$ if and only if $k = (d(G)-1) \dim V$ where the dimension is taken over $\mathrm{End}_G V$.

REFERENCES

[1] M. Aschbacher and L. Scott, Maximal subgroups of finite groups, J. Algebra (to appear).

[2] Kenneth S. Brown, Cohomology of groups (Graduate Texts in Mathematics 87), Springer-Verlag, New York etc., 1982.

[3] John Cossey, K.W. Gruenberg and L.G. Kovács, The presentation rank of a direct product of finite groups, J. Algebra 28 (1974), 597-603.

[4] Charles W. Curtis and Irving Reiner, Methods of representation theory with applications to finite groups and orders, vol. I, John Wiley & Sons, New York etc., 1981.

[5] Wolfgang Gaschütz, Zu einem von B.H. and H. Neumann gestellten Problem, Math. Nachr. 14 (1955), 249-252.

[6] Wolfgang Gaschütz, Die Eulersche Funktion endlicher auflösbarer Gruppen, Illinois J. Math. 3 (1959), 469-476.

[7] Wolfgang Gaschütz, Praefrattinigruppen, Arch. der Math. 13 (1962), 418-426.

[8] Karl W. Gruenberg, Cohomological methods in group theory (Lecture Notes in Mathematics 143), Springer-Verlag, Berlin etc.,1970.

[9] K.W. Gruenberg, Relation modules of finite groups (Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics 25), Amer. Math. Soc., Providence, 1976.

[10] K.W. Gruenberg, Groups of non-zero presentation rank, pp 215-224 in Symposia Mathematica, vol. XVII (Convegno sui Gruppi Infiniti, INDAM, Roma 1973), Academic Press, London, 1976.

[11] K.W. Gruenberg, Free abelianized extensions of finite groups, pp 71-104 in Homological group theory (London Math. Soc. Lecture Note Series 36), Cambridge University Press, Cambridge etc., 1979.

[12] K.W. Gruenberg and K.W. Roggenkamp, Decomposition of the relation modules of a finite group, J. London Math. Soc. (2) 12 (1976), 262-266.

[13] K.W. Gruenberg and K.W. Roggenkamp, The decomposition of relation modules: a correction, Proc. London Math. Soc. (3) 45 (1982), 89-96.

[14] B. Huppert, Endliche Gruppen I (Die Grundlehren der mathematischen Wissenschaften 134), Springer-Verlag, Berlin etc., 1967.

[15] B. Huppert and N. Blackburn, Finite groups II (Die Grundlehren der mathematischen Wissenschaften 242), Springer-Verlag, Berlin etc., 1982.

[16] Saunders Mac Lane, Homology (Die Grundlehren der mathematischen Wissenschaften 114), Springer-Verlag, Berlin etc., 1963.

[17] Derek J.S. Robinson, A course in the theory of groups (Graduate Texts in Mathematics 80), Springer-Verlag, New York etc., 1982.

[18] K.W. Roggenkamp, Relation modules of finite groups and related topics, Algebra i Logika 12 (1973), 351-359.

[19] Urs Stammbach, Cohomological characterisation of finite solvable and nilpotent groups, J. Pure Appl. Alg. 11 (1977), 293-301.

[20] Richard M. Thomas, On the number of generators for certain finite groups, J. Algebra 71 (1981), 576-582.

[21] Richard M. Thomas, On the number of generators for certain finite groups, II, J. Algebra 86 (1984), 14-22.

Received for Research Reports 1 November 1984.