ISRAEL JOURNAL OF MATHEMATICS, Vol 27, Nos 3-4, 1977

NORMAL COMPLEMENTS IN MOD p-ENVELOPES

BY

L. E MORAN AND R N. TENCH

ABSTRACT

Suppose G is a finite p-group and k is the field of p elements, and let U be the augmentation ideal of the group algebra kG. We investigate which p-groups, G, have normal complements in their mod p-envelope, G^*. G^* is defined by $G^* = \{1 - u : u \in U\}$.

The type of groups under consideration here are finite p-groups and their mod p-envelopes. The mod p-envelope, G^*, of a finite p-group, G, can be constructed as follows.

Suppose k is the field of p elements, then G^* is given by

$$G^* = \{1 - u : u \in U\},$$

where U is the augmentation ideal of the group algebra kG. Clearly this definition is equivalent to

$$G^* = \left\{ \sum_{x \in G} \lambda_x x : \sum_{x \in G} \lambda_x = 1 \right\}.$$

k is the only irreducible kG module thus U is also the Jacobson radical of kG and therefore nilpotent. Thus the inverse of $1 - u$, $u \in U$, can be expressed as the finite sum

$$1 + u + u^2 + \cdots + u^t,$$

where $u^{t+1} = 0$. G^* therefore forms a group under multiplication in kG, containing G as a subgroup.

For a group H let H' denote the derived group of H, $\phi(H)$ the Frattini subgroup of H and H^p be the subgroup of H generated by the pth powers of elements of H.

Received April 17, 1975

D. B. Coleman [1] has proved that for all p-groups, G,

i) $(G^*)' \cap G = G'$, and

ii) if N is the normalizer of G in G^* and C the centralizer of G in G^* then $N = CG$.

For those p-groups which have a normal complement in their mod p-envelope (i.e. there exists a normal subgroup, N, such that $N \cap G = 1$ and $NG = G^*$) there are simple proofs of these results. It can also be shown that for these groups

iii) $\phi(G^*) \cap G = \phi(G)$, and

iv) $(G^*)^p \cap G = G^p$.

The problem is now to determine which finite p-groups have normal complements in their mod p-envelopes. Let L_p denote the set of such groups. It is clear that a finite p-group, G, belongs to L_p if and only if there exists an epimorphism from G^* to G fixing G elementwise. This immediately gives the first class of groups belonging to L_p.

THEOREM 1. *If G is a finite p-group, then its mod p-envelope, G^*, belongs to L_p.*

PROOF. Define the mapping π as follows:

$$\pi : (G^*)^* \to G^*$$

$$\sum_{x \in G^*} \lambda_x x \mapsto \sum_{g \in G} \left(\sum_{x \in G^*} \lambda_x \mu_g^{(x)} \right) g,$$

where $x = \Sigma_{g \in G} \mu_g^{(x)} g \in G^*$.

It is easily shown that π is a homomorphism and also for all $x \in G^*$

$$(x)\pi = x.$$

The most important class of p-groups known to belong to L_p is that of all finite abelian p-groups, but before this is proved some further results are established.

THEOREM 2[†]. *If H and K are finite p-groups and $G = H \times K$, then G belongs to L_p if and only if H and K both belong to L_p.*

PROOF. Suppose both H and K belong to L_p and their normal complements are L and M respectively. Let α denote a typical element of G^*, i.e.

$$\alpha = \sum_{h \in H} \sum_{k \in K} \lambda_{(h,k)}(h, k) \in G^*.$$

[†] The proof given here of the sufficiency condition of Theorem 2 is due to D. L. Johnson.

Define the epimorphism ϕ as follows:

$$\phi : G^* \to H^*$$

$$\alpha \mapsto \sum_{h \in H} \sum_{k \in K} \lambda_{(h,k)} h.$$

Now let $\bar{L}$ denote the set

$$\bar{L} = \{\alpha \in G^* : (\alpha)\phi \in L\}.$$

In a similar manner define $\bar{M}$. Now let $N = \bar{L} \cap \bar{M}$, then N is normal in G^*. It is easily seen that $N \cap G = 1$ and it remains to show the order of N is the same as the index of G in G^*.

$$|N| = \frac{|\bar{L}|\,|\bar{M}|}{|\bar{L}\bar{M}|} \geqq \frac{|\bar{L}|}{|G^*|} \cdot \frac{|\bar{M}|}{|G^*|} \cdot |G^*| = \frac{|G^*|}{|H|\,|K|} = \frac{|G^*|}{|G|}.$$

Since $N \cap G = 1$ it is clear that $|N| \leqq |G^*|/|G|$.

Conversely assume $G = H \times K$ has a normal complement in G^* and thus there must exist a splitting epimorphism, ϕ, from G^* to G. The composite of the inclusion from H^* to G^*, ϕ and the natural mapping from G to H is the splitting epimorphism from H^* to H. Thus H, and similarly K, belongs to L_p.

The necessary condition of Theorem 2 can be given in the slightly stronger form of Corollary 2.1 without any alteration to the proof.

COROLLARY 2.1. *If G is the semi-direct product of the finite p-groups H and K (K normal in G), then H belongs to L_p if G does.*

LEMMA 1. *If G is a finite abelian p-group, then G and G^* have the same exponent.*

PROOF. Since the coefficients in the sum

$$\alpha = \sum_{x \in G} \lambda_x x$$

belong to $GF(p)$, then for any integer k

$$\alpha^{p^k} = \sum_{x \in G} \lambda_x x^{p^k}.$$

Hence $\alpha^{p^k} = 1$ for all $\alpha \in G^*$ if and only if, for all $x \in G$, $x^{p^k} = 1$.

Now since the cyclic group of order n (n a power of p), Z_n, has the same exponent as $(Z_n)^*$, Z_n is a direct factor of $(Z_n)^*$ and thus Theorem 2 gives the following result.

THEOREM 3. *All finite abelian p-groups belong to L_p.*

By establishing another sufficiency condition, more non-abelian p-groups can be shown to be elements of L_p. Assume G is a finite p-group with its binary operation denoted by juxtaposition and with identity e.

THEOREM 4. *Suppose there exists a binary operation, $*$, on the set G such that G becomes an elementary abelian p-group under $*$ with identity e. Then G belongs to L_p if for all $a, b, c \in G$,*

$$[c(a*b)]*c = (ca)*(cb) \tag{1}$$

and

$$[(a*b)c]*c = (ac)*(bc). \tag{2}$$

PROOF. Let Σ^* denote summation in G over $*$ and let $\lambda * x = x*x*\cdots*x$ (λ times) for any $\lambda \in GF(p)$ and $x \in G$.

Firstly note that (1) is equivalent to

$$z\sum_{x\in G}^{*} \lambda_x * x = \sum_{x\in G}^{*} \lambda_x * (zx) \tag{1a}$$

for all $\Sigma_{x\in G}\lambda_x x \in G^*$ and all $z \in G$. For if (1) holds, then by induction

$$\left[z\left(\sum_{x\in G}^{*} \lambda_x * x\right)\right] * \left[\left(-1 + \sum_{x\in G} \lambda_x\right) * z\right] = \sum_{x\in G}^{*} \lambda_x * (zx),$$

but

$$\sum_{x\in G} \lambda_x \equiv 1 \pmod{p}.$$

Conversely if (1a) holds

$$c(a*b*(-1*e)) = (ca)*(cb)*(-1*c),$$

but under $*$, e is the identity and thus

$$c(a*b) = (ca)*(cb)*(-1*c)$$

or

$$[c(a*b)]*c = (ca)*(cb).$$

Similarly

$$\left(\sum_{x\in G}^{*} \lambda_x * x\right) z = \sum_{x\in G}^{*} \lambda_x * (xz). \tag{2a}$$

Define the mapping π as follows:

$$\pi : G^* \to G$$

$$\sum_{x \in G} \lambda_x x \mapsto \sum_{x \in G}^* \lambda_x^* x .$$

Since for all $x \in G$ $(x)\pi = x$, it now remains to show that π is a homomorphism.

$$\begin{aligned}
\left[\left(\sum_{g \in G} \lambda_g g\right)\left(\sum_{h \in G} \mu_h h\right)\right]\pi &= \left[\sum_{x \in G}\left(\sum_{y \in G} \lambda_{xy^{-1}} \mu_y\right) x\right]\pi, \\
&= \sum_{x \in G}^*\left(\sum_{y \in G} \lambda_{xy^{-1}} \mu_y\right)^* x \\
&= \sum_{x \in G}^*\left[\sum_{y \in G}^* (\lambda_{xy^{-1}} \mu_y)^* x\right] \\
&= \sum_{g \in G}^*\left[\sum_{h \in G}^* (\lambda_g \mu_h)^* gh\right] \\
&= \sum_{g \in G}^* \lambda_g^*\left(g \sum_{h \in G}^* \mu_h^* h\right) \qquad \text{by (1a)} \\
&= \left(\sum_{g \in G}^* \lambda_g^* g\right)\left(\sum_{h \in G}^* \mu_h^* h\right) \qquad \text{by (2a).}
\end{aligned}$$

Note that it is not sufficient to show that just one of the conditions (1) and (2) of Theorem 4 holds. A * operation can be defined on $Z_p \sim Z_p$ (p odd), the wreath product of the cyclic group of order p with itself, such that * defines an elementary abelian p-group satisfying (1) but not (2).

An application of Theorem 4, to show certain p-groups belong to L_p, is to use the construction of Cooper [2]†. This is to define the * operation by

$$a * b = W(a, b),$$

where $W(a, b)$ is a word in a, b. Cooper has shown that in nilpotent groups of class at most three, for * to define a group, $W(a, b)$ must have the form

$$ab\,[a, b]^r\,[a, b, a]^{-s}\,[a, b, b]^s,$$

where r and s satisfy certain congruence relations. If * is defined in this way $p * a = a^p$, and it is clear, only groups of exponent p can satisfy the conditions of Theorem 4. In general the conditions of Theorem 4 do not hold for p-groups of

† The authors wish to thank the referee for drawing their attention to [2] and its application in Theorem 5.

exponent p and of class three with the * operation defined in this way. Theorem 5, however, shows that for such p-groups (p odd) of class two this definition of the * operation does satisfy the conditions of Theorem 4.

THEOREM 5. *For p an odd prime, p-groups of exponent p and class two belong to L_p.*

PROOF. Define * by

$$a * b = ab\,[b, a]^{\frac{1}{2}(p+1)}.$$

This defines a commutative operation since

$$\begin{aligned} b * a &= ba\,[ab]^{\frac{1}{2}(p+1)} \\ &= ab\,[ba]^{\frac{1}{2}(p+1)}. \end{aligned}$$

To show condition (1) holds

$$\begin{aligned} [c(a * b)]*c &= cab\,[ba]^{\frac{1}{2}(p+1)}c\,[c, ab]^{\frac{1}{2}(p+1)} \\ &= cab\,c\,[ba]^{\frac{1}{2}(p+1)}[c, a]^{\frac{1}{2}(p+1)}[c, b]^{\frac{1}{2}(p+1)}. \end{aligned}$$

$$\begin{aligned} ca*cb &= cacb\,[cb, ca]^{\frac{1}{2}(p+1)} \\ &= cacb\,[b, a]^{\frac{1}{2}(p+1)}[c, a]^{\frac{1}{2}(p+1)}[b, c]^{\frac{1}{2}(p+1)} \\ &= cabc\,[b, a]^{\frac{1}{2}(p+1)}[c, a]^{\frac{1}{2}(p+1)}[c, b]^{\frac{1}{2}(p+1)}. \end{aligned}$$

Similarly $[c(a*b)]*c = ac*bc$.

It is, of course, not necessary to define $a*b$ as a word in a, b. The following examples of the application of Theorem 4 to p-groups of exponent greater than p show two other methods of defining the * operation.

An example of the use of Theorem 4 is the Sylow p-subgroup of the general linear group $GL(n, p)$ consisting of all upper triangular $(n \times n)$ matrices over the field $GF(p)$ with leading diagonal entries all one. Suppose A, B and C are matrices of this type, then define the binary operation * by

$$A * B = A + B - I,$$

where I is the identity matrix. This operation satisfies the conditions of Theorem 4 and so it remains to show that relations (1) and (2) are true.

$$\begin{aligned} [C(A*B)]*C &= C(A + B - I) + C - I \\ &= CA + CB - I \\ &= CA*CB. \end{aligned}$$

Similarly relation (2) is also true and thus these groups belong to L_p.

All 2-groups of order not greater than 8 belong to L_2. As seen before abelian 2-groups belong to L_2 and the only other 2-groups of order not greater than 8 are the dihedral and quaternion groups. Suppose the dihedral group of order 8 is represented as

$$\langle x, y \mid x^4 = y^2 = 1, xy = yx^{-1} \rangle$$

and its elements are expressed in the form $y^{\alpha}x^{2\beta+\gamma}$, where α, β and γ are either zero or one. Let

$$a = y^i x^{2j+k}, \quad b = y^l x^{2m+n} \quad \text{and} \quad c = y^r x^{2s+t}.$$

If the operation * is defined by

$$a*b = y^u x^{2v+w},$$

where $u \equiv i + l$, $v \equiv j + m$ and $w \equiv k + n \pmod 2$, then it can be easily shown that

$$ca*cb = y^d x^{2f+g},$$

where $d \equiv i + l \pmod 2$, $f \equiv j + m + [((-1)^i t + k)/2] + [((-1)^l t + n)/2] \pmod 2$ and $g \equiv k + n \pmod 2$. (Square brackets denote the integer part of the expression included.) Since for i, l, k, n and t either zero or one,

$$\left[\frac{(-1)^i t + k}{2}\right] + \left[\frac{(-1)^l t + n}{2}\right] \equiv \left[\frac{(-1)^{i+l} t + \{k + n \pmod 2\}}{2}\right] \pmod 2,$$

it can also be easily shown that

$$[c(a*b)]*c = y^d x^{2f+g}.$$

Hence relation (1) is established for the dihedral group of order eight and relation (2) is shown in a similar manner. Thus this group, by Theorem 4, is a member of L_2. The quaternion group of order eight,

$$\langle x, y \mid x^4 = 1, y^2 = x^2, xy = yx^{-1} \rangle,$$

is also a member of L_2 and this can be shown by an analogous method.

The groups of order 16 and of exponent not greater than four also belong to L_2. The three non-abelian groups of this type can be represented as follows:

i) $\langle x, y \mid x^4 = y^4 = 1, xy = yx^3 \rangle$,

ii) $\langle x, y, z \mid x^4 = y^2 = z^2 = 1, xy = yx, xz = zx, yz = zyx^2 \rangle$,

iii) $\langle x, y, z \mid x^4 = y^2 = z^2 = 1, xy = yx, yz = zy, xz = zxy \rangle$.

The methods for showing that these three groups all belong to L_2 are merely extensions of those used on the dihedral and quaternion groups of order eight. For example consider group (ii). Let the elements of this group be expressed in the form $z^{\alpha}y^{\beta}x^{2\gamma+\delta}$, where α, β, γ and δ are either zero or one and also let

$$a = z^{i}y^{j}x^{2k+l}, \quad b = z^{m}y^{n}x^{2r+s} \quad \text{and} \quad c = z^{t}y^{u}x^{2v+w}.$$

The operation * is defined by addition of corresponding indices modulo 2 in an analogous way to the previous example. Now

$$ca^{*}cb = z^{d}y^{f}x^{2g+h} = [c(a^{*}b)]^{*}c,$$

where $d \equiv i + m \pmod 2$, $f \equiv j + n \pmod 2$, $g \equiv k + r + u(i + m) + h(l + s) \pmod 2$ and $h \equiv l + s \pmod 2$.

Similarly relation (2) is shown and hence this group belongs to L_2.

Not every p-group does belong to L_p, for example, the dihedral group of order 16, D_{16}, does not have a normal complement in its mod 2-envelope. This has been shown by the use of a computer using the following argument. Suppose a normal complement, N, exists, then let $N^{\subset}$ be the set of elements of $(D_{16})^{*}$ not in N. The conjugates of the non-trivial elements of D_{16} belong to $N^{\subset}$. If $a, b \in (D_{16})^{*}$ and if $ab^{-1}ab \in N^{\subset}$, then so does a and all its conjugates, similarly the commutator (a, b) could also be used. By examining enough elements of this type, the order of $N^{\subset}$ can be shown to be greater than $2^{15} - 2^{11}$ (2^{15} is the order of $(D_{16})^{*}$ and 2^{11} is the required order of N).

References

1. D. B. Coleman, *On the modular group ring of a p-group*, Proc. Amer. Math. Soc. **15** (1964).

2. C. D. H. Cooper, *Words which give rise to another group operation for a given group*, Proc. Second Internat. Conf. Theory of Groups, Canberra, 1973 (Lecture Notes in Mathematics. Springer-Verlag, Berlin, Heidelberg, New York).

Department of Mathematics
University Park, Nottingham, England