SUBGROUP-DETERMINING FUNCTIONS ON GROUPS

BY
ANNE PENFOLD STREET[1]

I. Introduction and notation

Let G be a group and let S be a subset of G. Suppose that S is a subgroup of G if and only if for every $x, y \in S, f(x, y) \in S$. What forms may the function f take?

This question was first raised by Higman and Neumann [6] and investigated by Hulanicki and Świerczkowski [8], who introduced the following definition:

DEFINITION. A group G has *property P* if and only if there exist integers $a_i, b_i, i = 1, \cdots, r$, and $m_j, n_j, j = 1, \cdots, s$, such that

(i) the word

$$x \circ y = x^{a_1}y^{b_1} \cdots x^{a_r}y^{b_r} \tag{1}$$

defines a binary operation in G, not identically equal in G to xy or to yx;

(ii) the elements of G form a group $G_\circ$ under the operation $x \circ y$, in which the m^{th} power of x is denoted by $[x]_\circ^m$, the inverse of x by $x^{[-1]}$ and the commutator of y and x by $[y, x]_\circ$;

(iii) the operation xy is a word in $G_\circ$, i.e. the law

$$xy = [x]_\circ^{m_1} \circ [y]_\circ^{n_1} \circ \cdots \circ [x]_\circ^{m_s} \circ [y]_\circ^{n_s} \tag{2}$$

holds identically for every $x, y \in G$.

In this case, $x \circ y$ is called an *s-function* on G.

They pointed out that, if G has property P, then $x \circ y^{[-1]}$ is a subgroup-determining function on G, different from the obvious ones, namely $f_1(x, y) = xy^{-1}, f_2(x, y) = x^{-1}y$ and their transposes.

It follows from results in [6], [10] and [16] that neither an Abelian nor a free group possesses property P, and that no s-function may be defined on the variety of all groups, nor on the class of all finite nilpotent groups, nor on the class of all finite p-groups, for p a given prime. However, in [8] it is shown that if G is nilpotent of class 2 and if its commutator subgroup, G', has finite exponent, then G has property P, and all possible s-functions on such a group are determined. G and $G_\circ$ are shown to be isomorphic if G is also periodic.

In this paper, we discuss further classes of groups with property P, the s-functions that can be defined on them and the relation between G and $G_\circ$. In II, we prove the following:

Received January 12, 1967.

[1] This paper is taken from the author's doctoral dissertation written under the direction of Professor Michio Suzuki at the University of Illinois.

THEOREM 1. *The transformation from G to $G_\circ$ preserves the following:*

(i) *the group identity*
(ii) *the inverse, powers and order of each element*
(iii) *the order and exponent of each subgroup*
(iv) *the lattice of subgroups*
(v) *the normaliser and commutator subgroup of each subgroup*
(vi) *the mixed commutator subgroup of each pair of subgroups*
(vii) *the centraliser of each element.*

Any s-function on G must have the form

$$x \circ y = xy \prod_i u_i^{f_i} \tag{3}$$

where, if $H = \langle x, y \rangle$, the subgroup generated by x and y, then $u_i \in H'$ and f_i is an integer modulo the exponent of H', for every i.

COROLLARY. *This transformation preserves central and derived series and, consequently, nilpotency, nilpotency class, solvability and derived length.*

In III, we consider nilpotent groups whose commutator subgroups have finite exponent, and find five additional classes of such groups with property P. We assume the standard properties of finite p-groups and nilpotent groups, as set out in [3], [5], [9] or [13], the collecting process of P. Hall [4], and the method due to Meier-Wunderli [14] for writing down a standard set of basic commutators. G_i ($G^{(i)}$) denotes the i^{th} lower central (derived) subgroup of $G = G_1 = G^{(0)}$. n_i (m_i) denotes the exponent of G_i ($G^{(i)}$) and $n_i(k)$ ($m_i(k)$) denotes the least common multiple of the exponents of the i^{th} lower central (derived) subgroups of the k-generator subgroups of G. $G_2 = G^{(1)}$ is also denoted by G'. For $x, y \in G$, the commutator of x and y is defined as

$$(x, y) = x^{-1}y^{-1}xy$$

and for $w > 2$, a left-normed commutator of weight w is defined inductively as

$$(x_1, \cdots, x_{w-1}, x_w) = ((x_1, \cdots, x_{w-1}), x_w).$$

G is called j-metabelian if and only if every j-generator subgroup of G is metabelian.

The nilpotent groups which we find to have property P are of two types, both of which may be regarded as generalisations of class 2 groups. The first type are those for which $(y, x^a) = (y, x)^a$ is true for some integers a; using this property, we obtain the following results:

THEOREM 2. *Let G be a nilpotent group of class k, such that n_2 is finite and the least prime divisor of $n_3 \geq k$. Let a, b be any two integers satisfying*

$$(n_2, 2a - 1) = 1 \tag{4}$$

$$n_2/a + b - 2ab \tag{5}$$

$$n_3/a(a-1) \tag{6}$$

$$n_2 \nmid a \tag{7}$$

$$n_2 \nmid a-1. \tag{8}$$

Then G has property P and $x \circ y = xy(y, x)^a$ *is an s-function, such that*

$$xy = x \circ y \circ [y, x]_\circ^b \quad in\ G_\circ.$$

THEOREM 3. *Let G be a p-group such that* n_2 *is finite and for every 3-generator subgroup, H, of G, H′ is a regular p-group. Let a, b be any two integers satisfying* (4), (5), (7) *and*

$$n_3/a. \tag{9}$$

Then G has property P and $x \circ y = xy(y, x)^a$ *is an s-function, such that*

$$xy = x \circ y \circ [y, x]_\circ^b \ in\ G_\circ.$$

The second type are those in which the Lie-Jacobi identity takes on a particularly strong form: in any group G, this identity is true in the form

$$(x, y, z)(y, z, x)(z, x, y) \equiv 1 \pmod{G_4} \tag{10}$$

but, under special circumstances, this statement may be strengthened. Thus

$$(x, y, z)(y, z, x)(z, x, y) = 1 \tag{11}$$

if and only if G is 3-metabelian [1], and if G is nilpotent of class 4, then

$$(x, y, z, w)(y, z, x, w)(z, x, y, w) = 1. \tag{12}$$

Many groups in which either (11) or (12) is true have property P, as shown in the following theorems:

THEOREM 4. *Let G be a nilpotent group of class 3, such that* n_2 *is finite. Then G has property P and* $x \circ y$ *is an s-function if and only if*

$$x \circ y = xy(y, x)^a(y, x, x)^f(y, x, y)^{-f}$$

where a, f are any integers satisfying (4) *and*

$$n_3/a(a-1) - 3f \tag{13}$$

and at least one of (7), (8) *and*

$$n_3(2) \nmid f. \tag{14}$$

Then, if and only if b, g are integers satisfying (5) *and*

$$n_3(2)/f + g + 12fg \tag{15}$$

we have

$$xy = x \circ y \circ [y, x]_\circ^b \circ [y, x, x]_\circ^g \circ [y, x, y]_\circ^{-g} \quad in\ G_\circ.$$

THEOREM 5. *Let G be a nilpotent group of class 4, containing no elements of order 2 or 3, and such that* n_2 *is finite. Then G has property P and* $x \circ y$ *is an* *s-function if and only if*

$$x \circ y = xy(y, x)^a (y, x, x)^f (y, x, y)^{-f} (y, x, x, x)^d (y, x, x, y)^{-d} (y, x, y, y)^{-d}$$

where a, f, d are integers satisfying (4), (13) *and*

$$n_4 / f + 2d \tag{16}$$

$$n_4 / af \tag{17}$$

$$m_2(3) / a + 2f \tag{18}$$

and at least one of (7), (8), (14) *and*

$$n_4(2) \nmid d. \tag{19}$$

Then, if and only if b, g are integers satisfying (5), (15) *and*

$$n_4(2) / fg \tag{20}$$

we have

$$xy = x \circ y \circ [y, x]_\circ^b \circ [y, x, x]_\circ^g \circ [y, x, y]_\circ^{-g} \circ [y, x, x, x]_\circ^{-d} \circ [y, x, x, y]_\circ^d \circ [y, x, y, y]_\circ^d$$

in $G_\circ$.

COROLLARY. *Let G be a 3-group, such that G is nilpotent of class 4 and n_2 is finite. Then if $n_2 > 3$, G has property P and $x \circ y$ is an s-function if it is of the form defined above, with $d = 0$.*

THEOREM 6. *Let G be a 3-metabelian nilpotent group of finite class, such that n_2 is finite. Let a, b, f, g be any integers satisfying* (4), (5), (13), (15) *and*

$$n_4 / f \tag{21}$$

and at least one of (7), (8) *and* (14). *Then G has property P and*

$$x \circ y = xy(y, x)^a (y, x, x)^f (y, x, y)^{-f}$$

is an s-function such that

$$xy = x \circ y \circ [y, x]_\circ^b \circ [y, x, x]_\circ^g \circ [y, x, y]_\circ^{-g} \quad \text{in } G_\circ .$$

In certain special cases, we prove the isomorphism of G and $G_\circ$:

THEOREM 7. *Let G be a periodic group such that n_2 is finite and either*

(i) *G is nilpotent of class 3 and contains no elements of order 3, or*

(ii) *G is nilpotent of class 4 and contains no elements of order 2 or 3.*

If $x \circ y = xy(y, x)^a$ where a is an integer satisfying (4) *and* (9), *then G is isomorphic to $G_\circ$.*

It follows from Theorem 5 that, in metabelian groups of class 4 where (11) holds, two distinct families of s-functions may be defined, but in the general case where only the weaker statement (12) is true, the functions in one of these families are no longer associative.

In IV, we consider metabelian, but not necessarily nilpotent, groups. They are of special interest because all the known pairs of strictly index-preserving, normaliser-preserving, lattice-isomorphic groups are either Abelian (and thus do not possess property P) or metabelian, and by Theorem 1, it is only among such pairs of groups that there exist examples where G is not isomorphic to $G_\circ$. We write $(y,_1 x) = (y, x)$ and inductively

$$(y,_k x) = (y,_{k-1} x, x);$$

in a commutator $(x_1, x_2, x_3, \cdots, x_w)$, each x_i is called a component of the commutator, x_1 and x_2 being the inner components and $x_3, \cdots, x_w$ the outer components. Using this notation, we may state the following results:

THEOREM 8. *Let G be a metabelian group. Then*

(i) *permutations of the outer components of a commutator do not affect the value of the commutator,*

(ii) *the basic commutators of the 2-generator subgroups of G are all of the form $(y,_k x,_j y)$ for some integers j, k,*

(iii) $(y, x^n) = \prod_{k=1}^{n} (y,_k x)^{C(n,k)}$ *where* $C(n, k) = \binom{n}{k}$.

If the commutator factor group, G/G', has exponent r, then

(iv) $(z, y, x^{-1}) = \prod_{k=1}^{r-1} (z, y,_k x)^{C(r-1,k)}$,

(v) $(z, y,_r x) = \prod_{k=1}^{r-1} (z, y,_k x)^{-C(r,k)}$,

(vi) *any commutator containing r identical outer components may be deleted from the basic set,*

(vii) *for every 2-generator subgroup of G, there exists a complete set of basic commutators containing $(r^2 + 2)$ commutators, namely x, y, (y, x), $(y,_2 x)$, (y, x, y), $\cdots$, $(y,_r x)$, $(y,_{r-1} x, y)$, $\cdots$, $(y, r,_{r-1} y)$, $(y,_r x, y)$, $(y,_{r-1} x,_2 y)$, $\cdots$, $(y,_2 x,_{r-1} y)$, $\cdots$, $(y,_r x,_{r-2} y)$, $(y,_{r-1} x,_{r-1} y)$, $(y,_r x,_{r-1} y)$.*

If, in addition, G' has exponent t, then

(viii) *any s-function on G must be of the form*

$$x \circ y = xy \prod_{i=1}^{r^2} u_i^{f_i}$$

where $u_1 = (y, x), \cdots, u_{r^2} = (y,_r x,_{r-1} y)$ and each f_i is an integer modulo t.

Given a presentation of a specific metabelian group in terms of generators and relations, we may then test each function in this finite set to see whether any of them is, in fact, an s-function.

THEOREM 9. *Let G be a metabelian (but not nilpotent) group, such that G/G' has exponent 2, and G' has exponent an odd prime. Then no s-function may be defined on G.*

In V, we discuss several examples, which show to what extent the results obtained earlier are best possible. In particular, an example is constructed of a group G which is not isomorphic to $G_\circ$.

We make the following convention: in any expression involving both the original group operation and the $\circ$ operation, the original operation will be performed first, unless indicated otherwise by parentheses.

II. The relation between G and $G_\circ$

Proof of Theorem 1. (i) Any binary operation on G can be written in the form (1). Let 1 denote the identity of G. Then $1 \circ 1 = 1$, and hence 1 is also the identity of $G_\circ$.

(ii) By (i), $x = x \circ 1 = x^{\Sigma_i a_i} = 1 \circ x = x^{\Sigma_i b_i}$. Thus $\sum_i a_i = \sum_i b_i = 1$.

$$x \circ x^{-1} = x^{\Sigma_i a_i - \Sigma_i b_i} = x^0 = 1$$

and hence $x^{[-1]} = x^{-1}$. $x \circ x = x^{\Sigma_i a_i + \Sigma_i b_i} = x^2$ and by induction $[x]^m = x^m$ for m any integer. Since the group identity and the powers of each element are preserved, so is the order of each element.

(iii) The underlying sets of G and $G_\circ$ are the same. We denote by ϕ both the identity mapping of this set onto itself and the identity mapping of the power set of G onto itself. S is a subgroup (subset) of G is denoted by $S \leq (\subseteq) G$.

Let $S \leq G$. Then $S^\phi \subseteq G_\circ$. By the definition of s-function, $x, y \in S = S^\phi$ implies $x \circ y^{-1} \in S^\phi$; thus $S^\phi \leq G_\circ$. Similarly $S_\circ \leq G_\circ$ implies $S^{\phi^{-1}} \leq G$.

Hence there is a one-one correspondence between the subgroups of G and of $G_\circ$ where $S^\phi = S_\circ$. By (ii), this correspondence preserves the exponent of each subgroup; since ϕ is the identity mapping, it also preserves the order of each subgroup.

(iv) The one-one correspondence defined in (iii) is also a lattice-isomorphism. Firstly,

$$x \in S^\phi \cap T^\phi \iff x \in S \cap T \iff x \in (S \cap T)^\phi,$$

hence $S^\phi \cap T^\phi = (S \cap T)^\phi$ and ϕ preserves greatest lower bounds. Secondly, $x \in \langle S^\phi, T^\phi \rangle$ if and only if

$$x = s_1^{c_1} \circ t_1^{d_1} \circ \cdots \circ s_k^{c_k} \circ t_k^{d_k}$$

for some integers c_i, d_i and some $s_i \in S$, $t_i \in T$, $i = 1, \cdots, k$. By repeated applications of (1), we may write x as a word in s_i, t_i, $i = 1, \cdots, k$, with respect to the original group operation. Hence

$$x \in \langle S, T \rangle = \langle S, T \rangle^\phi \quad \text{and} \quad \langle S^\phi, T^\phi \rangle \subseteq \langle S, T \rangle^\phi.$$

A similar application of (2) to $x \in \langle S, T \rangle$ shows that

$$\langle S, T \rangle = \langle S, T \rangle^\phi \subseteq \langle S^\phi, T^\phi \rangle.$$

Hence $\langle S, T \rangle = \langle S, T \rangle^\phi = \langle S^\phi, T^\phi \rangle$ and ϕ preserves least upper bounds. By (iii), ϕ is a strictly index-preserving lattice isomorphism.

(3) can be proved in two different ways. Since no s-function can be defined on an Abelian group [6], we know that for all $x, y \in G$, $x \circ y \equiv xy \pmod{H'}$ where $H = \langle x, y \rangle \leq G$, and (3) follows. Alternatively, we could apply Hall's collecting process to (1) and since, by (ii), $\sum_i a_i = \sum_i b_i = 1$, (3) follows.

(v) In the expression for $x \circ y$, we write each $u_i = u_i(y, x)$ to avoid confusion while calculating the commutators in $G_\circ$.

$$\begin{aligned}
[x, y]_\circ &= x^{-1} \circ y^{-1} \circ x \circ y \\
&= x^{-1}y^{-1} \textstyle\prod_{i=1}^{k} u_i(y^{-1}, x^{-1})^{f_i} \circ xy \prod_{i=1}^{k} u_i(y, x)^{f_i} \\
&= x^{-1}y^{-1} \textstyle\prod_{i=1}^{k} u_i(y^{-1}, x^{-1})^{f_i} xy \prod_{i=1}^{k} u_i(y, x)^{f_i} \\
&\quad \cdot \textstyle\prod_{i=1}^{k} u_i(xy \prod_{i=1}^{k} u_i(y, x)^{f_i}, x^{-1}y^{-1} \prod_{i=1}^{k} u_i(y^{-1}, x^{-1})^{f_i})^{f_i} \qquad (22) \\
&= (x, y) \textstyle\prod_{i=1}^{k} u_i(y^{-1}, x^{-1})^{f_i} (\prod_{i=1}^{k} u_i(y^{-1}, x^{-1})^{f_i}, xy) \\
&\quad \cdot \textstyle\prod_{i=1}^{k} u_i(y, x)^{f_i} \\
&\quad \cdot \textstyle\prod_{i=1}^{k} u_i(xy \prod_{i=1}^{k} u_i(y, x)^{f_i}, x^{-1}y^{-1} \prod_{i=1}^{k} u_i(y^{-1}, x^{-1})^{f_i})^{f_i}
\end{aligned}$$

Hence $[x, y]_\circ$ may be expressed as a product of commutators in G and $H'_\circ \subseteq H'$. Since xy may be written as a word in $G_\circ$, a similar argument shows that (x, y) may be expressed as a product of commutators in $H_\circ$ and hence $H' \subseteq H'_\circ$. Thus $H' = H'_\bullet$. (v) and (vi) follow from this result, by Theorem 1 of [2].

(vii) Let $C_G(S)$ denote the centraliser in G of $S \subseteq G$ and let $x \in C_G(S)$. For all $s \in S$, $x \circ s = xs = sx = s \circ x$, hence $x \in C_{G_\circ}(S_\circ)$ and $C_G(S) \subseteq C_{G_\circ}(S_\circ)$. Similarly, $C_{G_\circ}(S_\circ) \subseteq C_G(S)$ showing that $C_G(S) = C_{G_\circ}(S_\circ)$ and ϕ preserves centralisers.

III. Nilpotent groups with property P

The following identities will be used:

$$(x, yz) = (x, z)(x, y)^z = (x, z)(x, y)(x, y, z) \qquad (23)$$

$$(xy, z) = (x, z)^y(y, z) = (x, z)(x, z, y)(y, z) \qquad (24)$$

$$(x^{-1}, y)^x = (x, y^{-1})^y = (x, y)^{-1} \qquad (25)$$

$$(y^{-1}, x^{-1}) = (y, x)^{x^{-1}y^{-1}} = (y, x)(y, x, x^{-1}y^{-1}) \qquad (26)$$

$$\begin{aligned}(x, y, z)&(y, z, x)(z, x, y) \\ &= (y, x)(z, x)(z, y)^x(x, y)(x, z)^y(y, z)^x(x, z)(z, x)^y \qquad (27)\end{aligned}$$

$$\text{Witt identity:} \quad (x, y^{-1}, z)^y(y, z^{-1}, x)^z(z, x^{-1}, y)^x = 1 \qquad (28)$$

$$\begin{aligned}\text{Macdonald identity [12]:} \quad &(u, v; x, y) \\ &= (u, v, y^{-1}, x^{(u,v)})^y(u, v, x^{-1}, y^{-1})^{xy} \qquad (29)\end{aligned}$$

where $(u, v; x, y) = (u, v, (x, y))$.

Proof of Theorem 2. (i) (7) and (8) are sufficient to ensure that $x \circ y$ does not reduce to xy or to yx.

(ii) $$(y^a, x) = y^{-a}(y(y, x))^a = (y, x)^a \textstyle\prod_i u_i^{f_i(a)} \qquad (30)$$

by Hall's collecting process, where, for each integer i, each u_i is a basic commutator of weight w_i in y and (y, x), and

$$f_i(a) = c_{i1}\binom{a}{1} + \cdots + c_{iw_i}\binom{a}{w_i} \tag{31}$$

for some rational integers c_{ij}.

If $a = 0, 1$ then $(y^a, x) = (y, x)^a$; hence $f_i(0) = f_i(1) = 0$. By induction, as in [4], $c_{i1} = 0$ for all integers i.

Since G is of class k, the weight of u_i as a commutator in x and y cannot exceed k, and thus the weight of u_i as a commutator in y and (y, x) cannot exceed $(k-1)$, i.e. $w_i \leq k-1$. Hence (31) becomes

$$f_i(a) = c_{i2}\binom{a}{2} + \cdots + c_{i,k-1}\binom{a}{k-1}. \tag{31$'$}$$

By (6), since no prime divisor of n_3 is less than k, $n_3/f_i(a)$ for each i and

$$(y^a, x) = (y, x)^a. \tag{32}$$

Similarly,

$$(x(y, z))^a = x^a(y, z)^a \tag{33}$$

and by (5),

$$(x^{2ab-a-b}, y) = 1. \tag{34}$$

(iii)

$$\begin{aligned} x \circ (y \circ z) &= xyz(z, y)^a(yz(z, y)^a, x)^a \\ &= xyz(z, y)^{a-1}(yz, x)^a(z, y)(z, y, x)^a \quad \text{by (24), (32), (33)} \\ &= xyz(z, y)^a(zy, x)^a \quad \text{by (33)} \\ &= xyz(z, xy)^a(y, x)^a \quad \text{by (23) and (24).} \end{aligned} \tag{35}$$

$$\begin{aligned} (x \circ y) \circ z &= xy(y, x)^a z(z, xy(y, x)^a)^a \\ &= xyz(z, xy)^a(y, x)^a \quad \text{by (6), (23), (32) and (33).} \end{aligned} \tag{35$'$}$$

By (35) and (35′), the $\circ$ operation is associative.

(iv) By (4), (5) and (6), it follows that $(n_2, 2b-1) = 1$ and

$$n_3/b(b-1). \tag{36}$$

$$\begin{aligned} x \circ y = xy(y, x)^a &= xy(y, x^a) \quad \text{by (32)} \\ &= x^{1-a}yx^a. \end{aligned} \tag{37}$$

$$\begin{aligned} x \circ y \circ [y, x]_\circ^b &= x^{1-b} \circ y \circ x^b \quad \text{by (36) and (37)} \\ &= x^{(1-b)(1-a)}y^{1-a}x^b y^a x^{a(1-b)} \quad \text{by (37)} \\ &= x^{1-ab}y^{1-a}x^b y^a x^{b(a-1)} \quad \text{by (34)} \\ &= xyx^{-ab}(x^{-ab}, y)y^{-a}x^b y^a x^{b(a-1)} \\ &= xy \quad \text{by (32).} \end{aligned}$$

Proof of Theorem 3. (i) (7) is sufficient to ensure that $x \circ y$ does not reduce to xy or to yx.

(ii) By Hall's collecting process, as in the previous proof, and by (9),

$$\text{if} \quad a = n_3 = p^k, \qquad \text{then} \quad (y^a, x) = (y, x)^a. \tag{32}$$

If $a = hp^k$, for some integer h, then (32) follows from (9) by induction on h. In particular,

$$((y, x)^a, z) = (y, x, z)^a = 1 \quad \text{by (9)}, \tag{38}$$

and since H' is regular,

$$((x, y)(x, z))^a = (x, y)^a(x, z)^a. \tag{39}$$

$$\begin{aligned}(x^{-1}, y^{-1})^a &= ((x, y)(x, y, y^{-1}x^{-1}))^a \quad \text{by (26)}\\ &= (x, y)^a \quad \text{by (38) and (9)}.\end{aligned} \tag{40}$$

$$(yx, y^{-1}x^{-1})^a = (y, x, x^{-1}y^{-1})^a = 1 \quad \text{by (9)}. \tag{41}$$

(iii)
$$\begin{aligned}x \circ (y \circ z) &= xyz(z, y)^a(yz, x)^a \quad \text{by (38)}\\ &= xyz(z, y)^a(y, x)^a(z, x)^a \quad \text{by (38) and (39)}.\end{aligned} \tag{42}$$

$$\begin{aligned}(x \circ y) \circ z &= xyz(y, x)^a(z, xy)^a \quad \text{by (38)}\\ &= xyz(z, y)^a(y, x)^a(z, x)^a \quad \text{by (38) and (39)}.\end{aligned} \tag{42'}$$

By (42) and (42′), the $\circ$ operation is associative.

(iv)
$$[y, x]_\circ = (y, x)^{1-2a} \quad \text{by (40) and (41)}. \tag{43}$$

Hence, if b is an integer satisfying (5),

$$\begin{aligned}x \circ y \circ [y, x]_\circ^b &= xy(y, x)^a \circ (y, x)^{b(1-2a)} \quad \text{by (43)}\\ &= xy \quad \text{by (5) and (9)}.\end{aligned}$$

Proof of Theorem 4. (A) the properties of the integers a, b, f, g.

(i) Any one of (7), (8) or (14) is necessary and sufficient to ensure that $x \circ y$ does not reduce to xy or to yx.

(ii) Given an integer a satisfying (4), there exists an integer b such that (5) is satisfied.

By (5) and (13), $(n_3(2), 12f + 1) = 1$ and hence there exists an integer g such that (15) is satisfied.

By (5), $(n_2, 2b - 1) = 1$ and by (4), (5), (13) and (15), $n_3/b(b - 1) - 3g$.

(B) the necessity of the given conditions.

(i) Since G is nilpotent of class 3, the commutators (y, x), (y, x, x) and (y, x, y) form a basic set in the components x and y [14]. Thus, from equation (3), any s-function on G has the form

$$x \circ y = xy(y, x)^a(y, x, x)^{f_1}(y, x, y)^{f_2}.$$

By Theorem 1, (ii), inverses are the same in G and $G_\circ$; hence

$$(x^{-1} \circ y^{-1})(y \circ x) = 1$$

which implies

$$((y, x, x)(y, x, y))^{f_1+f_2} = 1$$

and hence

$$(y, x, x)^{f_1+f_2} = (y, x, y)^{f_1+f_2} = 1.$$

Thus we may write the s-function as

$$x \circ y = xy(y, x)^a (y, x, x)^f (y, x, y)^{-f}. \tag{44}$$

(ii) By direct computation, we find from the associative law that

$$(y, x, z)^{a^2-f}(x, z, y)^{a+2f}(z, y, x)^{a^2-f} = 1$$

and hence by (11),

$$(x, z, y)^{a(a-1)-3f} = 1.$$

Since G_3 is Abelian, this proves (13).

(iii) By (13) and (44),

$$\begin{aligned} [y, x]_\circ &= (y, x)^{1-2a}(y, x, x)^{a(2a-1)}(y, x, y)^{a(2a-1)} \\ &= (y, x)^{1-2a}(y, x, x)^{a+6f}(y, x, y)^{a+6f} \end{aligned} \tag{45}$$

$$[y, x, z]_\circ = (y, x, z)^{(2a-1)^2} = (y, x, z)^{12f+1}. \tag{46}$$

(iv) By Theorem 1, $G_\circ$ is nilpotent of class 3 and, by the proof of (44), xy, expressed as a word in $G_\circ$, must have the form

$$xy = x \circ y \circ [y, x]_\circ^b \circ [y, x, x]_\circ^g \circ [y, x, y]_\circ^{-g}$$

and hence by (45) and (46)

$$(y, x)^{a+b-2ab}(y, x, x)^{f+g+12fg}(y, x, y)^{-f-g-12fg} = 1. \tag{47}$$

Taking commutators of both sides of (47) gives

$$(y, x, z)^{a+b-2ab} = 1. \tag{48}$$

Putting xy for x in (47), we find by (23), (24) and (48) that

$$(y, x)^{a+b-2ab} = (y, x, x)^{f+g+12fg} = (y, x, y)^{f+g+12fg} = 1$$

which proves (5) and (15).

(C) the sufficiency of the given conditions.

The existence of an identity and inverses with respect to the $\circ$ operation follows from the definition of $x \circ y$ as in Theorem 1. $x \circ (y \circ z)$, $(x \circ y) \circ z$, $[y, x]_\circ$ and $[y, x, z]_\circ$ are evaluated as in (B). Associativity follows from the given conditions and (11), and by direct computation,

$$x \circ y \circ [y, x]_\circ^b \circ [y, x, x]_\circ^g \circ [y, x, y]_\circ^{-g} = xy.$$

Proof of Theorem 5. (A) the properties of the integers a, b, f, g, d.

(i) Any one of (7), (8), (14) or (19) is necessary and sufficient to ensure that $x \circ y$ does not reduce to xy or to yx.

(ii) Integers satisfying (4), (5), (13) and (15) must exist, as in the previous proof, but the existence of integers satisfying the remaining conditions depends on the values of n_2, n_3, n_4 and $m_2(3)$.

If there exist a, f, d satisfying (4), (7), (8), (13), (14) and (16)–(19), then there exist b, g satisfying (5), (15) and (20). The existence of b and g satisfying (5) and (15) follows as in the previous proof; that (20) is also satisfied follows from (13), (15), (17) and the fact that G contains no elements of order 3.

(B) the necessity of the given conditions.

(i) Since G is nilpotent of class 4, (y, x), (y, x, x), (y, x, y), (y, x, x, x), (y, x, x, y) and (y, x, y, y) form a basic set in the components x and y [14]. Since G/G_4 is nilpotent of class 3, by Theorems 1 and 4, an s-function on G must have the form

$$x \circ y = xy(y, x)^a(y, x, x)^f(y, x, y)^{-f}(y, x, x, x)^{d_1}(y, x, x, y)^{d_2}(y, x, y, y)^{d_3}.$$

Since inverses are the same in G and $G_\circ$, we have

$$(x^{-1} \circ y^{-1})(y \circ x) = 1$$

which implies

$$((y, x, x, x)(y, x, y, y)^{-1})^{f+d_1-d_3} = 1$$

and since G contains no involutions

$$(y, x, x, x)^{f+d_1-d_3} = (y, x, x, y)^{f+d_1-d_3} = (y, x, y, y)^{f+d_1-d_3} = 1.$$

Hence the s-function can be written

$$x \circ y = xy(y, x)^a(y, x, x)^f(y, x, y)^{-f}(y, x, x, x)^d(y, x, x, y)^{d_2}(y, x, y, y)^{d+f}.$$

(ii) The alternative law in the form

$$(x \circ x) \circ y = x \circ (x \circ y)$$

implies

$$(y, x, x)^{a(a-1)-3f}(y, x, x, x)^{af+d_2-5d-3f}(y, x, x, y)^{2f-2af+2d-2d_2} = 1. \tag{49}$$

By taking commutators with both sides of (49), we find

$$n_4(2)/a(a-1) - 3f.$$

By repeated substitutions of xy for x in (49) and by (23) and (24), since G contains no involutions,

$$n_4(2)/af + d_2 - 5d - 3f \tag{50}$$

and similarly, putting yx for y,

$$n_4(2)/f - af + d - d_2. \tag{51}$$

From (49), (50) and (51), we have

$$n_3(2)/a(a-1) - 3f \tag{52}$$

and

$$n_4(2)/f + 2d. \tag{53}$$

By (51) and (53), the s-function may be written

$$x \circ y = xy(y, x)^a(y, x, x)^f(y, x, y)^{-f}(y, x, x, x)^d(y, x, x, y)^{d(2a-1)}(y, x, y, y)^{-d}$$

assuming G contains no involutions.

We obtain additional information on the invariants and the divisibility conditions by applying the following lemma:

LEMMA 1. (Levi, [11]) *If every 2-generator subgroup of a group G is nilpotent of class 2, then G is nilpotent of class at most 3 and $n_3/3$.*

In our case, $G/Z(G)$ is nilpotent of class 3, where $Z(G)$ denotes the centre of G. Let n_3' denote the exponent of $(G/Z(G))_3$. Consider the 2-generator subgroups of the central quotient group; let $n_3'(2)$ denote the least common multiple of the exponents of the third terms in their respective lower central series. By (53), $n_3'(2)/f + 2d$, and by Lemma 1, $n_3'/3(f + 2d)$, i.e.

$$(y, x, z)^{3(f+2d)} \equiv 1 \pmod{Z(G)}$$

and

$$(y, x, z, w)^{3(f+2d)} = 1$$

which implies

$$n_4/3(f + 2d). \tag{54}$$

If G contains no elements of order 3, this implies (16); similarly, from (52),

$$n_4/a(a-1) - 3f.$$

(iii) By direct computation, the associative law implies

$$\begin{aligned}
&(y, x, z]^{a^2-f}(z, y, x)^{a^2-f}(x, z, y)^{a+2f}(z, z; y, x)^{-af-a(a+1)/2} \\
&(y, x; z, y)^{a^2}(z, x; z, y)^{-af+a(a+1)/2}(z, y, y, x)^{af-d}(z, y, x, y)^{-af-f-d} \\
&(z, y, z, x)^{-af}(z, y, x, z)^{-af-d(2a-1)}(y, x, z, x)^{f(1+a)}(z, y, x, x)^{af-d} \\
&(y, x, x, z)^{f(a-1)+d(2a-1)}(y, x, y, z)^{-d-af}(y, x, z, y)^{f(a-1)-d} \\
&(z, x, y, z)^{-2ad}(z, x, z, y)^{-d}(y, x, z, z)^{-f(a+1)-d}(z, x, x, y)^{-f+2d(a-1)} \\
&(z, x, y, y)^{-f-2d}(z, x, y, x)^{-f-d} = 1.
\end{aligned} \tag{55}$$

Putting yx for y in (55) and applying (23), (24), (52) and (53) gives

$$\begin{aligned}
&(y, x; z, x)^{a^2}(y, x, z, x)^{af-d-f}(z, x, y, x)^{-a-3f+af-3d} \\
&(z, y, x, x)^{a^2-2f-2d}(z, x, x, y)^{-af-2f-3d} \\
&(y, x, x, z)^{a^2-d-af-f} = 1.
\end{aligned} \tag{56}$$

Since G is nilpotent of class 4, by (29)

$$(y, x; z, x) = (y, x, z, x)(y, x, x, z)^{-1} = (z, x, y, x)^{-1}(z, x, x, y) \quad (57)$$

which, with (12), reduces (56) to

$$(z, x, y, x)^{3(f+2d)}(z, x, x, y)^{f+2d} = 1. \quad (58)$$

By (54) and (58),

$$(z, x, x, y)^{f+2d} = 1 \quad (59)$$

and by (56), (57) and (59),

$$(y, x, z, x)^{f+2d}(z, x, y, x)^{f+2d} = 1. \quad (60)$$

(59) and (60) are true provided only that G contains no involutions; if G contains no elements of order 3 either, then $(y, x, z, w)^{f+2d} = 1$ and (16) follows.

(iv) By (53), using the expression found in (ii) for the s-function,

$$\begin{aligned}[y, x]_\circ = {} & (y, x)^{1-2a}(y, x, x)^{a(2a-1)}(y, x, y)^{a(2a-1)}(y, x, x, x)^{-(a+2f)(2a-1)} \\ & \cdot (y, x, x, y)^{-(a+3f)(2a-1)}(y, x, y, y)^{-(a+2f)(2a-1)}\end{aligned} \quad (61)$$

$$\begin{aligned}[y, x, z]_\circ = {} & (y, x, z)^{(2a-1)^2}(y, x, x, z)^{-a(2a-1)^2}(y, x, y, z)^{-a(2a-1)^2} \\ & \cdot (y, x, z, z)^{-a(2a-1)^2}\end{aligned} \quad (62)$$

$$[y, x, z, w]_\circ = (y, x, z, w)^{-(2a-1)^3} \quad (63)$$

(v) By Theorem 1, $G_\circ$ is nilpotent of class 4 and xy must have the form

$$\begin{aligned}xy = {} & x \circ y \circ [y, x]_\circ^b \circ [y, x, x]_\circ^g \circ [y, x, y]_\circ^{-g} \circ [y, x, x, x]_\circ^e \\ & \circ [y, x, x, y]_\circ^{e(2b-1)} \circ [y, x, y, y]_\circ^{-e}\end{aligned}$$

where

$$n_3(2)/b(b-1) - 3g$$

$$n_4(2)/g + 2e$$

$$n_4/3(g + 2e).$$

By (23), (24), (61)–(63), we find

$$\begin{aligned}& (y, x)^{a-b(2a-1)}(y, x, x)^{f+g(2a-1)^2}(y, x, y)^{-f-g(2a-1)^2} \\ & (y, x, x, x)^{d-ag(2a-1)^2-e(2a-1)^3+bf(2a-1)} \\ & (y, x, x, y)^{(2a-1)(d-ab+ag(2a-1)-e(2b-1)(2a-1)^2)} \\ & (y, x, y, y)^{-d+ag(2a-1)^2+e(2a-1)^3+bf(2a-1)} = 1.\end{aligned} \quad (64)$$

Taking commutators of both sides of (64) gives

$$(y, x, z)^{a+b-2ab}(y, x, x, z)^{f+g+12fg}(y, x, y, z)^{-f-g-12fg} = 1 \quad (65)$$

and again with (65) gives

$$(y, x, z, w)^{a+b-2ab} = 1 \quad \text{which implies} \quad n_4/a + b - 2ab. \tag{66}$$

Putting y^2 for y in (65), by (65) and (66) we have

$$(y, x, x, z)^{f+g+12fg} = (y, x, y, z)^{f+g+12fg} = 1 \tag{67}$$

since G contains no involutions. Hence, by (65) and (67),

$$(y, x, z)^{a+b-2ab} = 1 \quad \text{which implies} \quad n_3/a + b - 2ab. \tag{68}$$

Repeated substitution of yx for y in (64) shows that

$$n_4(2)/-d + ag(2a - 1)^2 + e(2a - 1)^3 + bf(2a - 1) \tag{69}$$

and similarly, by repeated substitution of xy for x in (64)

$$n_4(2)/d - ag(2a - 1)^2 - e(2a - 1)^3 + bf(2a - 1). \tag{70}$$

By (69) and (70), since G contains no involutions,

$$n_4(2)/bf(2a - 1) \tag{71}$$

and

$$n_4(2)/d - ag(2a - 1)^2 - e(2a - 1)^3. \tag{72}$$

By (68) and (71),

$$n_4(2)/bf, \qquad n_4(2)/af, \qquad n_4(2)/bg, \qquad n_4(2)/ag. \tag{73}$$

By (72) and (73),

$$n_4(2)/d - e(2a - 1)^3. \tag{74}$$

By (73), since $n_4(2)/g + 2e$, we have

$$n_4(2)/ae, \qquad n_4(2)/d + e, \qquad n_4(2)/a\,d$$

and (20) is true. Hence the s-function may be written as

$$x \circ y = xy(y, x)^a(y, x, x)^f(y, x, y)^{-f}(y, x, x, x)^d(y, x, x, y)^{-d}(y, x, y, y)^{-d}$$

and xy as a word in $G_\circ$ becomes

$$xy = x \circ y \circ [y, x]_\circ^b \circ [y, x, x]_\circ^g \circ [y, x, y]_\circ^{-g} \circ [y, x, x, x]_\circ^{-d} \circ [y, x, x, y]_\circ^d \circ [y, x, y, y]_\circ^d .$$

If G contains no elements of order 3, so that (16) holds, then by these divisibility conditions and (12) applied to (55), we have

$$(y, x; z, x)^{a+2f}(y, x; z, y)^{a+2f}(z, x; z, y)^{a+2f} = 1$$

and hence

$$(y, x; z, x)^{a+2f} = 1. \tag{75}$$

(75) implies (18), since the second derived group of every 3-generator subgroup of G is Abelian and generated by commutators of this form. Applying the divisibility conditions to (64) gives

$$(y, x)^{a+b-2ab}(y, x, x)^{f+g(2a-1)^2}(y, x, y)^{-f-g(2a-1)^2} = 1 \tag{76}$$

and, substituting y^2 for y in (76), we find

$$(y, x, x)^{f+g(2a-1)^2} = (y, x, y)^{f+g(2a-1)^2} = 1$$

which implies $n_3(2)/f + g(2a - 1)^2$ or, equivalently, (15). From (15) and (76),

$$(y, x)^{a+b-2ab} = 1$$

which implies (5) and (4), since G contains no involutions and thus G' is a product of regular p-groups.

(C) the sufficiency of the given conditions follows as in Theorem 4.

Note. (1) *If* G contains elements of order 3, we know only that

$$n_4(2)/f + 2d \quad \text{and} \quad n_4/3(f + 2d).$$

In this case, the given conditions with $d = 0$ will satisfy the identities but may be more restrictive than necessary.

(2) Consider the case $d = 0$, for G a p-group, $p > 3$. (Analogous though more complicated statements are true for each permitted value of d and for direct products of p-groups.) Then $m_2(3) = p^k$, for some $k \geq 0$, and since p is odd, G is 3-metabelian if and only if G is metabelian [1]. If G is metabelian, $k = 0$, and the divisibility conditions become

$$(n_2, 2a - 1) = 1; \qquad n_3/a(a - 1) - 3f; \qquad n_2/a + b - 2ab; \qquad n_4/f$$

and hence $a \equiv 0$ or $1 \pmod p$ are both possible. If G is not metabelian, $k > 0$, p^k/a. This leaves only one possibility: $a \equiv 0 \pmod p$.

(3) Necessity can be proved in Theorems 4 and 5 because the sets of basic commutators in class 3 or 4 groups have only one commutator of given weight in each component, and hence appropriate substitutions and expansions will give equations involving only one basic commutator. But for groups of class 5 or higher, this technique will no longer work, since the sets of basic commutators contain more than one commutator of given weight in each component.

Proof of Theorem 6. (i) Any one of (7), (8) or (14) is sufficient to ensure that $x \circ y$ does not reduce to xy or to yx.

(ii) By (24) and induction on k, since G is 3-metabelian,

$$((y, x)^k, z) = (y, x, z)^k \tag{77}$$

and in particular, by (21),

$$((y, x, x)^f, z) = ((y, x, y)^f, z) = 1. \tag{78}$$

(iii) By (11) and (13),

$$(y, x, z)^{a(1-a)}(z, x, y)^{a+f}(z, y, x)^f = (y, x, z)^{a-f}(z, x, y)^{-f}(z, y, x)^{a^2} \tag{79}$$

and associativity of $x \circ y$ follows from (77)–(79) by direct computation.

(iv) By (77), (78) and (21),

$$[y, x]_\circ = (y, x)^{1-2a}(x, y, x^{-1}y^{-1})^{a(2a-1)} \tag{80}$$

and by (80) and (13),

$$[y, x, z]_\circ = (y, x, z)^{12f+1}(x, y, x^{-1}y^{-1}, z)^{-a}(y, x, z, z^{-1})^{a}(x, y, x^{-1}y^{-1}, z, z^{-1})^{-a} \tag{81}$$

(v) $x \circ y \circ [y, x]_\circ^b \circ [y, x, x]_\circ^g \circ [y, x, y]_\circ^{-g}$

$$= xy(x, y, x^{-1}y^{-1})a^2((y, x)^{-a}(x, y, x^{-1}y^{-1})^a, xy(y, x)^a)^a$$

by (80), (81), (5), (15) and (21)

$$= xy.$$

Proof of Theorem 7. Let b be any integer such that (5) is satisfied. By (9), n_3/b. Let

$$n = a + b - 2ab = p_1^{f_1} \cdots p_s^{f_s}$$

where $p_1, \cdots, p_s$ are distinct primes.

Since G is a periodic nilpotent group, $G = P \times Q$, where

$$P = P_1 \times \cdots \times P_s$$

is the direct product of the Sylow p_i-subgroups of G, $i = 1, \cdots, s$, and the Abelian subgroup, Q, is the direct product of the remaining Sylow subgroups of G. Also, $G_\circ = P_\circ \times Q_\circ$ where $P_\circ$ and $Q_\circ$ are the groups formed by the elements of P and Q respectively, under the operation $x \circ y$.

Let $m = 1 - 2b$. Then $(n, m) = 1$, by (4). Define a mapping, ϕ, of G onto $G_\circ$ as follows:

$$x^\phi = x^m \quad \text{for any } x \in P$$

$$y^\phi = y \quad \text{for any } y \in Q$$

$$(xy)^\phi = x^\phi \circ y^\phi \quad \text{for any } x \in P,\ y \in Q.$$

$(n, m) = 1$ implies that m is co-prime to the orders of the elements of P, hence ϕ is one-one and onto. Thus it suffices to prove that, if G satisfies (i) or (ii), ϕ is a homomorphism on P.

$$(xy)^m \equiv x^m y^m (y, x)^{\binom{m}{2}}(y, x, x)^{f_4(m)}(y, x, y)^{f_5(m)}(y, x, x, x)^{f_6(m)}$$

$$\cdot (y, x, x, y)^{f_7(m)}(y, x, y, y)^{f_8(m)} \pmod{G_5}$$

by Hall's collecting process, where $f_4(m)$ and $f_5(m)$ are integral linear combinations of $\binom{m}{2}$ and $\binom{m}{3}$, and $f_6(m)$, $f_7(m)$ and $f_8(m)$ are integral linear combinations of $\binom{m}{2}$, $\binom{m}{3}$ and $\binom{m}{4}$. Since n_3/b, either (i) or (ii) is sufficient to imply that

$$(xy)^m = (xy)^{1-2b} = x^{1-2b}y^{1-2b}(y, x)^{b(2b-1)}. \tag{82}$$

$$x^m \circ y^m = x^{1-2b} y^{1-2b} (y^{1-2b}, x^{1-2b})^a$$
$$\equiv x^{1-2b} y^{1-2b} (y, x)^{a(2b-1)^2} (y, x, x)^{-ab(2b-1)^2} (y, x, y)^{-ab(2b-1)^2}$$
$$\cdot (y, x, x, x)^{ab(2b-1)^2(2b+1)/3} (y, x, x, y)^{ab^2(2b-1)^2}$$
$$\cdot (y, x, y, y)^{ab(2b-1)^2(2b+1)/3} \pmod{G_5} \text{ by (23) and (24)}$$
$$= x^{1-2b} y^{1-2b} (y, x)^{a(2b-1)^2} \text{ by (i) or (ii) and (9).} \qquad (83)$$

By (82) and (83), since $n_2/a + b - 2ab$, $(xy)^m = x^m \circ y^m$. Hence

$$(xy)^\phi = x^\phi \circ y^\phi$$

which proves the theorem.

IV. Metabelian groups with property P

Proof of Theorem 8. (i) follows from (11) since

$$(x_1, x_2, \cdots, x_{i-1}, x_i, x_{i+1}, x_{i+2}, \cdots, x_n)$$
$$= ((x_i, x_{i+1}; x_1, \cdots, x_{i-1})^{-1}(x_{i+1}, (x_1, \cdots, x_{i-1}), x_i)^{-1}, x_{i+2}, \cdots, x_n)$$
$$= (x_1, \cdots, x_{i-1}, x_{i+1}, x_i, x_{i+2}, \cdots, x_n).$$

(ii) The inner components of a basic commutator in the subgroup $\langle x, y\rangle$ are y and x in that order. Since G is metabelian, only simple commutators are needed in the basic set. By (i), any basic commutator of weight w may be written $(y, {}_kx, {}_jy)$, for some integers j, k such that $j + k + 1 = w$.

(iii) $(y, x^2) = (y, x)^2(y, x, x)$ by (24) and (iii) follows by induction on n.

(iv) If G/G' has exponent r, then $x^r \in G'$ and hence $(z, y, x^r) = 1$ for every $x, y, z \in G$. This implies, by (24), that $(z, y, x^{r-1}) = (z, y, x^{-1})$ and (iv) follows from (iii).

(v) By (iii), $\prod_{k=1}^{r} (z, y, {}_kx)^{C(r,k)} = 1$ and (v) follows.

(vi) By (i), any commutator containing r identical outer components may be put into the form $(z, y, {}_rx)$. By (v), it may then be expressed as a product of powers of

$$(z, y, x), \cdots, (z, y, {}_{r-1}x),$$

and is therefore not needed in the basic set.

(vii) There are 2 basic commutators of weight 1 in $\langle x, y\rangle$, namely x and y. By (ii), there are $(w - 1)$ basic commutators of weight w, for every $w > 1$.

For $w \leq r + 1$, the commutators have not more than $(r - 1)$ outer components, and hence they all belong to the basic set. For $w \geq 2r + 1$, the commutators have at least $(2r - 1)$ outer components, each of which is either x or y. Hence at least r outer components are identical, and all these commutators may be deleted from the basic set. For $w = r + k$, $2 \leq k \leq r$, the commutators have $(r + k - 2)$ outer components. Those which belong to the basic set are those in which no more than $(r - 1)$ x's or y's occur among the outer components i.e. those of the form

$$(y, {}_kx, {}_{r-1}y), (y, {}_{k+1}x, {}_{r-2}y), \cdots, (y, {}_{r-1}x, {}_{k-2}y), (y, {}_rx, {}_{k-1}y).$$

There are $(r - k + 1) = (2r + 1 - w)$ such commutators for each k.

Hence, the number of commutators in the basic set is

$$2 + \sum_{w=2}^{r+1} (w - 1) + \sum_{w=r+2}^{2r} (2r + 1 - w)$$
$$= 2 + r(r + 1)/2 + r(r - 1)/2 = 2 + r^2.$$

(viii) If G' has exponent t, (vii) and (3) imply (viii). This gives a set of $t^{(r^2)}$ functions, among which all possible s-functions must occur.

Proof of Theorem 9. (i) Since G is metabelian and G/G' has exponent 2, we have by (11) and (29) that

$$(u, v, x, y, xy) = 1 \tag{84}$$

is a law in G.

By an argument similar to that of the preceding proof, a 3-generator subgroup $\langle x, y, z\rangle \leq G$ has a basic set of commutators

$$\begin{gathered} x, y, z, (y, x), (z, x), (z, y), (y, {}_2x), (z, {}_2x), (y, x, y), (z, x, y), (z, {}_2y), \\ (y, x, z), (z, x, z), (z, y, z)(y, {}_2x, y), (z, {}_2x, y), (z, {}_2x, z), (y, x, y, z), \\ (z, x, y, z), (z, {}_2y, z), (y, {}_2x, y, z). \end{gathered} \tag{85}$$

By (11) and (25),

$$(y, {}_2x, z) = (z, {}_2x, y)(y, x, z)^{-2}(z, x, y)^2. \tag{86}$$

(ii) By Theorem 8, any s-function on G must be of the form

$$x \circ y = xy(y, x)^c(y, {}_2x)^d(y, x, y)^e(y, {}_2x, y)^f$$

where c, d, e, f are integers modulo t, the exponent of G'.

Since inverses are preserved, by direct computation

$$(x^{-1} \circ y^{-1})(y \circ x) = 1 = (y, {}_2x)^{d-e}(y, x, y)^{e-d}$$

and hence either

$$d - e \equiv 0 \pmod t \tag{87}$$

or

$$(y, {}_2x) = (y, x, y) \text{ is a law in } G. \tag{88}$$

Suppose (88) is true. Choose any two elements $u, v \in G$ and let $y = (u, v)$. Then (88) implies $(u, v, {}_2x) = (u, v, x)^{-2} = 1$, and since t is odd, $(u, v, x) = 1$ is a law in G, i.e. G is nilpotent of class 2, which is a contradiction. Hence (87) holds, and any s-function on G is of the form

$$x \circ y = xy(y, x)^c(y, {}_2x)^d(y, x, y)^d(y, {}_2x, y)^f. \tag{89}$$

(iii) By (84) and the associative law, direct computation shows that

$$(z, x, y)^A(z, {}_2x, y)^B(y, x, y, z)^C(y, {}_2x, y, z)^D = 1 \tag{90}$$

is a law in G, where

$$\begin{aligned} A &= c - c^2 + 2cd + 8d^2 - 3d - 8df - 4cf + 6f \\ B &= 8d^2 - 2cd - 8df + 2f \\ C &= 8d^2 - 2cd - 8df + 2f + 4cf \\ D &= 4d^2 - cd + f. \end{aligned}$$

Choosing $x = y$ in (90) implies that $(z, {}_2x)^{A-2B} = 1$ is a law in G and, as in (ii) above, we find that

$$A - 2B \equiv 0 \pmod{t}. \tag{91}$$

Choosing $z = x$ in (90) implies similarly that

$$C - 2D \equiv 0 \pmod{t}. \tag{92}$$

Taking commutators of both sides of (90) with yz twice, expanding and comparing with (90) shows that

$$((y, x, z)^2(y, x, y, z))^B = 1$$

and letting $z = x$,

$$((y, {}_2x)^2(y, {}_2x, y))^B = 1. \tag{93}$$

As in (ii), since G is not nilpotent, (93) implies that $B \equiv 0$ (t), and hence by (91), $A \equiv 0$ (t).

Thus (90) becomes $(y, x, y, z)^C(y, {}_2x, y, z)^D = 1$, and letting $x = (u, v)$ this leads to

$$(u, v, y, z)^C = 1.$$

Since G is not nilpotent, $C \equiv 0$ (t), and hence by (92), $D \equiv 0$ (t).

Since t is an odd prime, the only solutions of these four simultaneous congruences are $c \equiv 0$ or 1, $d \equiv 0, f \equiv 0$ (t), which lead to

$$x \circ y = xy \text{ or } yx.$$

V. Examples

(i) Let p and q be primes such that

$$p \equiv 1 \quad (3), \qquad q \equiv 1 \quad (3), \qquad p \equiv 1 \quad (q). \tag{94}$$

Let $G(m, n)$ be the group of order $2pq$ defined by

$$G(m, n) = \langle s, t, u \mid s^p = t^q = u^3 = (s, t) = 1; s^u = s^m, t^u = t^n \rangle$$

where m, n are integers modulo p, q respectively such that

$$m \not\equiv 1, \quad m^3 \equiv 1 \pmod{p}, \qquad n \not\equiv 1, \quad n^3 \equiv 1 \pmod{q}.$$

By the Ramification Theorem of Honda [7], if m is fixed, the two values n, n^2 lead to isomorphic groups, but the two values m, m^2 lead to two non-isomorphic, strictly index-preserving, normaliser-preserving, lattice-isomorphic groups.

The operation $x \circ y = xy(y, x)^k$ is associative on $G = G(m, n)$ if and only if

$$k(k-1) \equiv 0 \pmod{pq}$$

and by the congruences (94), this allows $k = 0, 1, p, 1-p$.

The choice of $k = 1 - p$ gives $G_\circ = G(m^2, n)$, which is not isomorphic to G. Thus the results of Theorem 1 are best possible.

(ii) Let T be the 2-Sylow subgroup of the symmetric group of degree 8. B. H. Neumann [15] has shown that T is nilpotent of class 4, 2-metabelian but not 3-metabelian and of exponent 8. We show two additional properties of T:

(A) no s-function may be defined on T, even though integers exist which satisfy the divisibility and co-primeness conditions of Theorem 5.

(B) a binary operation can be defined on T which induces an s-function on a maximal subgroup, H, of T, such that H' has exponent 4.

This shows that Theorems 3, 5 and 6 are best possible in the sense that we cannot remove the restrictions from their hypotheses i.e., we must in general require that the commutator subgroups of the 3-generator sub-groups of G be regular p-groups (in Theorem 3), that G contain no involutions (in Theorem 5), and that G be 3-metabelian (in Theorem 6).

Using the permutation representation of T given in [15], we find $n_2 = 4$, $n_3 = n_4 = 2$ and $T_4 = Z(T)$; hence any s-function on T must induce an s-function on T/T_4. Let n_i' be the exponent of $(T/T_4)_i$. Then $n_2' = n_3' = 2$. By Theorem 4, since T/T_4 is nilpotent of class 3, the only possible s-functions on T/T_4 are

$$x \circ y = xy(y, x)^a \quad \text{for } a = 0 \text{ or } 1.$$

Hence the only possible s-functions on T must be of the form

$$x \circ y = xy(y, x)^a (y, x, x, x)^{d_1} (y, x, x, y)^{d_2} (y, x, y, y)^{d_3} \tag{95}$$

where $a = 0, 1, 2, 3$ and $d_i = 0, 1$ for each i.

Suppose there exists an s-function of the form (95) for $a = 1$ or 3. Then since $d_i \equiv -d_i \pmod{n_4}$, and since $(x, y, x, y) = (x, y, y, x)$ in a nilpotent group of class 4,

$$x \# y = y \circ x = xy(y, x)^{a-1} (y, x, x, x)^{d_1} (y, x, x, y)^{d_2} (y, x, y, y)^{d_3}$$

is also an s-function of the form (95), where $a = 0$ or 2 respectively. Hence it suffices to show that no s-function can be defined on T with $a = 0$ or 2.

We consider each function of the form (95) for $a = 0, 2$ and each $d_i = 0, 1$, and exhibit for each such function, three elements of T which do not associate. In the notation of [15], these are as follows:

if $a = 0, d_1 = 1,$ then $a_3 \circ (a_2 \circ a_1) \neq (a_3 \circ a_2) \circ a_1$.

if $a = 0, d_2 = 1,$ then $a_1 \circ (a_3 \circ a_2 a_3) \neq (a_1 \circ a_3) \circ a_2 a_3$.

if $a = 0, d_3 = 1$ or if $a = 2, d_1 = d_3 = 0, d_2 = 1$,

then $a_1 \circ (a_2 \circ a_3) \neq (a_1 \circ a_2) \circ a_3$.

if $a = 2, d_1 + d_2 + d_3 \equiv 0 \ (2)$, then $(a_1 a_2 \circ a_3) \circ a_3 a_1 \neq a_1 a_2 \circ (a_3 \circ a_3 a_1)$.

if $a = 2, d_1 = 1, d_2 = d_3 = 0$ or $d_1 = d_2 = 0, d_3 = 1$ or $d_1 = d_2 = d_3 = 1$,

then $a_1 a_3 \circ (a_2 \circ a_1 a_3) \neq (a_1 a_3 \circ a_2) \circ a_1 a_3$.

On the maximal subgroup $H = \langle T', a_1 a_2, a_3 \rangle$, two s-functions can be defined, namely

$$x \circ y = xy(y, x)^a \quad \text{for } a = 2, 3.$$

(iii) Let M be the example (due to B. H. Neumann [15]) of a 3-metabelian but not metabelian group. M is nilpotent of class 4, and $n_1 = 8$, $n_2 = 4$, $n_3 = n_4 = 2$. Hence from Theorem 6, we know that two s-functions may be defined on M, namely

$$x \circ y = xy(y, x)^a \quad \text{for } a = 2, 3.$$

However, we find that for this particular group, there are 4 additional s-functions, namely

$$x \circ y = xy(y, x)^a(y, x, x, x)(y, x, x, y)(y, x, y, y) \quad \text{for } a = 0, 1, 2, 3.$$

The associativity of these additional s-functions follows from (11), and from the properties of M quoted above. In each case, for the s-function as stated, we have

$$xy = x \circ y \circ [y, x]_\circ^a \circ [y, x, x, x]_\circ \circ [y, x, x, y]_\circ \circ [y, x, y, y]_\circ .$$

This example shows that the conditions stated in Theorem 6, while sufficient for the existence of s-functions, may be more restrictive than necessary.

References

1. S. Bachmuth and J. Lewin, *The Jacobi identity in groups*, Math. Zeitschr., vol. 83 (1964), pp. 170–176.
2. D. W. Barnes and G. E. Wall, *On normalizer preserving lattice isomorphisms between nilpotent groups*, Austral. J. Math., vol. 4 (1964), pp. 454–469.
3. M. Hall, *The theory of groups*, Macmillan, New York 1959.
4. P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. (2), vol. 36 (1933), pp. 29–95.
5. ———, *Nilpotent groups*, Lecture notes of summer seminar, Canadian Math. Congress, University of Alberta, 1957.
6. G. Higman and B. H. Neumann, *Groups as groupoids with one law*, Publ. Math. Debrecen, vol. 2 (1951–2), pp. 215–221.

7. K. HONDA, *On finite groups whose Sylow-groups are all cyclic*, Comm. Math. Univ. St. Paul., vol. 1 (1952–3), pp. 5–39.
8. A. HULANICKI AND S. ŚWIERCZKOWSKI, *On group operations other than xy or yx*, Publ. Math. Debrecen, vol. 9 (1962), pp. 142–148.
9. B. HUPPERT, *Endliche Gruppen*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, in press.
10. N. IWAHORI AND A. HATTORI, *On associative compositions in finite nilpotent groups*, Nagoya Math. J., vol. 7 (1954), pp. 145–148.
11. F. W. LEVI, *Groups in which the commutator operation satisfies certain algebraic conditions*, J. Indian Math. Soc., (N. S.), vol. 6 (1942), pp. 87–97.
12. I. D. MACDONALD, *Some metabelian-like varieties of groups*, Amer. Math. Monthly, vol. 72 (1965), pp. 159–162).
13. W. MAGNUS, A. KARRASS AND D. SOLITAR, *Combinatorial group theory*, Interscience, New York, 1966.
14. H. MEIER-WUNDERLI, *Note on a basis of P. Hall for the higher commutators in free groups*, Comm. Math. Helv., vol. 16 (1951), pp. 1–5.
15. B. H. NEUMANN, *On a conjecture of Hanna Neumann*, Proc. Glascow Math. Assoc., vol. 3 (1956), pp. 13–17.
16. HANNA NEUMANN, *On a question of Kertesz*, Publ. Math. Debrecen, vol. 8 (1961), pp. 75–78.

UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS