SOME APPLICATIONS OF THE EULERIAN FUNCTIONS OF A FINITE GROUP

G. E. WALL

(received 27 July 1960)

1. Introduction

This paper is chiefly concerned with inequalities for the numbers of subgroups of a finite p-group. The following are typical results. Let G be a p-group of order p^a, and let $n_G(p^k)$ denote the number of subgroups of G of order p^k.

(1.1) *If A is the elementary abelian group of the same order as G, then $n_G(p^k) \leqq n_A(p^k)$ $(k = 1, 2, \cdots)$. If equality holds for a value of k such that $1 < k < a$, then $G \cong A$.*

(1.2) *If G is a regular p-group, and if B is the abelian p-group with the same basis invariants as G, then $n_G(p^k) \leqq n_B(p^k)$ $(k = 1, 2, \cdots)$. If G has the same total number of subgroups as B, then G is lattice-isomorphic to B.*

We mention in passing that (at any rate for $p = 2, 3$) two p-groups may have the same number of subgroups of each order without being lattice-isomorphic. See § 7, figs. 1 and 2.

Results like (1.1) and (1.2) are relevant to the problem of the "lattice embeddings" of p-groups: a lattice embedding of a group G in a group H is a meet isomorphism of the lattice of subgroups of G into that of H. Whenever a p-group G can be lattice-embedded in a p-group H of the same order, the series of inequalities

$$n_G(p^k) \leqq n_H(p^k) \qquad (k = 1, 2, \cdots)$$

is a necessary consequence; for such a lattice embedding maps each subgroup of G onto a subgroup of H of the same order. Lattice embeddings of p-groups have been recently studied by D. W. Barnes ([1]).

(1.1) immediately suggests the possibility that every p-group G can be lattice-embedded in the elementary abelian group of the same order; but Barnes has shown that this is false, even when G is abelian. However, the problem for groups of exponent p, and the corresponding problem suggested

by (1.2), remain open. With regard to the latter, Dr. Graham Higman has pointed out that the answer is affirmative when every subgroup of G which can be generated by 3 elements has class less than p; this is an immediate consequence of a theorem of M. Lazard ([7]).

Our method is enumerative, and relies on the properties of the *Eulerian functions* of a group (cf. P. Hall, [4]). Let G be any finite group. The n-th Eulerian function $\phi_n(G)$ of G is defined to be the total number of sequences of n elements of G which generate G. By counting the number of sequences of n elements of G in two ways, we get the analogue of the Eulerian summation formula of arithmetic:

$$\sum_{H \leqq G} \phi_n(H) = |G|^n, \tag{1.3}$$

where summation is over the subgroups H of G. The value of $\phi_n(G)$ is given explicitly by the inversion formula

$$\sum_{H \leqq G} \mu_G(H)|H|^n = \phi_n(G), \tag{1.4}$$

where μ_G is the Möbius function of G (Hall, *l.c.*; L. Weisner, [9]). For technical reasons, we shall deal with the *Eulerian polynomial* $\phi(G)$ of G rather than the series of Eulerian functions $\phi_n(G)$ $(n = 1, 2, \cdots)$. $\phi(G)$ is a polynomial, in variables $x, y, \cdots$ corresponding to the distinct prime divisors $p, q, \cdots$ of $|G|$, which reduces to $\phi_n(G)$ for the particular values $x = p^n$, $y = q^n, \cdots$.

The inequality (1.1) is a fairly easy consequence of (1.3) in the case of a p-group (§ 4). (1.2) follows similarly from a more general formula in which $\phi_n(G)$ is replaced by another function of Eulerian type (§ 7). One by-product of our formulae is the (known) enumeration of the subgroups of given isomorphism type in an abelian group.

The above results for p-groups give some information about groups of composite order, for it is quite easy to get upper bounds (though rather crude ones) for the numbers of subgroups of a group in terms of the numbers of subgroups of its Sylow subgroups. E.g. if $|G| = p^a q^b \cdots$, and if $P, Q, \cdots$ are Sylow subgroups corresponding to the t distinct prime divisors $p, q, \cdots$, then

$$n_G(p^\alpha q^\beta \cdots) \leqq |G|^{t-1} n_P(p^\alpha) n_Q(q^\beta) \cdots \tag{1.5}$$

Again, if G is soluble, $|G|^{t-1}$ can be replaced by $|G|$ in (1.5).

The problem of finding *direct* generalizations of results like (1.1), (1.2) to groups of composite order seems to be more difficult. First, our method succeeds for p-groups largely because of the simplicity of their Eulerian polynomials—the complexity of $\phi(G)$ depends on the complexity of the Frattini factor group $G/\Phi(G)$, which, for a p-group, is elementary abelian. Second, it is not easy to see which groups are to play the part of the "universal" groups

A, B in (1.1), (1.2). E.g. the simple group of order 168 has more subgroups of order 24 than any soluble group of order 168, though less of order 56. Such considerations suggest that it may be more fruitful to restrict attention to composition subgroups.

Recently, W. Gaschütz ([3]) has proved an interesting theorem about the Eulerian polynomial of a *soluble* group G, viz. that

$$\phi(G) = \rho(x)\sigma(y)\cdots, \tag{1.6}$$

where the polynomials $\rho, \sigma, \cdots$ depend on the chief factors of G. Gaschütz's method shows, in fact, that if G is p-soluble, then

$$\phi(G) = \rho(x)\sigma(y, z, \cdots), \tag{1.7}$$

where ρ is determined just as in the soluble case. It would be very interesting to know whether every group with Eulerian polynomial of the form (1.6) is necessarily soluble. The concluding § 8 contains several partial results on this problem. First, a group G has a normal subgroup of prime index p if, and only if, $(x - 1)$ is a divisor of $\phi(G)$. It is easily deduced that if $\phi(G)$ has the form (1.6) then G is not perfect, i.e. $G' < G$. Second, if $\phi(G)$ has the form (1.6) and $\mu_G(1) \neq 0$, then G is soluble. We remark that, for soluble groups G, $\mu_G(1) \neq 0$ if, and only if, the Frattini subgroup of every homomorphic image of G is the identity (this follows from Gaschütz's formula for $\phi(G)$). On the other hand, $\mu_G(1) = -60$ when G is the icosahedral group and $\mu_G(1) = 0$ when G is the simple group of order 168.

We also prove in § 8, using Gaschütz's methods, that the number of maximal subgroups of a soluble group is less than the group order. The same result for a general finite group would have important consequences. E.g. it would follow that every group G which cannot be generated by 2 elements has a proper subgroup H such that $|G : H| < |H|$.

2. Sum Functions*

Let G be a finite group and A an additively written abelian group. A *subgroup function on G to A* is a mapping of the lattice of subgroups of G into A. In the sequel, A is either the group of ordinary integers or the underlying group of a polynomial domain over the integers. The notations $H \leqq G$, $H < G$, $H \lhd G$ mean respectively that H is a subgroup of G, a subgroup of G distinct from G, a normal subgroup of G.

If the subgroup functions g, h satisfy

$$g(H) = \sum_{K \leqq H} h(K) \qquad \text{for all } H \leqq G, \tag{2.1}$$

we call g the *sum function* of h and write

* For further details on the (known) results of this section see Hall [4], Gaschütz [3].

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

$$g = \sum h. \tag{2.2}$$

For given g, the system of equations (2.1) determines h uniquely; for, if $h(K)$ is known for all $K < H$, then $h(H)$ is given by

$$h(H) = g(H) - \sum_{K<H} h(K).$$

We call h the *summand function* of G and write

$$h = \sum^{-1} g. \tag{2.3}$$

The equations

$$\mu_G(G) = 1, \qquad \sum_{K \geqq H} \mu_G(K) = 0 \qquad \text{whenever } H < G, \tag{2.4}$$

define the *Möbius function* μ_G of G; μ_G is a subgroup function on G to the group of ordinary integers. It is easily verified that

$$h(G) = \sum_{H \leqq G} \mu_G(H) g(H) \tag{2.5}$$

by showing that g is the sum function of the right hand side.

An explicit formula for $\mu_G(H)$ can be got as follows. Let $M_1, \cdots, M_r$ be the maximal subgroups of G (not including G itself). If $S = [i_1, \cdots, i_s]$ is a subset of $I = [1, 2, \cdots, r]$, we write

$$(-1)^S = (-1)^s,$$
$$M_S = M_{i_1} \wedge M_{i_2} \wedge \cdots \wedge M_{i_s};$$

in particular, $M_\phi = G$, and M_I is the Frattini subgroup $\Phi(G)$ of G. Let S_H denote the set of indices i such that $H \leqq M_i$. Then

$$\sum_{M_S \geqq H} (-1)^S = \sum_{S \leqq S_H} (-1)^S = \left.\begin{matrix} 1 & (H = G) \\ 0 & (H < G) \end{matrix}\right\},$$

and so

$$\mu_G(H) = \sum_{M_S = H} (-1)^S. \tag{2.6}$$

It follows that $\mu_G(H) = 0$ unless H is an intersection of maximal subgroups of G; in particular, $\mu_G(H) = 0$ unless $\Phi(G) \leqq H$. In view of (2.6), we may write (2.5) as

$$h(G) = \sum_{S \leqq I} (-1)^S g(M_S). \tag{2.7}$$

We remark that if $N \lhd G$, $N \leqq H \lneqq G$, then

$$\mu_{G/N}(H/N) = \mu_G(H). \tag{2.8}$$

This is clear from the defining equations (2.4).

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

3. The Eulerian Polynomial

Let G be a finite group of order $p^a q^b \cdots$, where $p, q, \cdots$ are distinct primes. Choose variables $x, y, \cdots$ corresponding to $p, q, \cdots$. (When it is necessary to indicate the precise correspondence between primes and variables, we shall write $x_p, x_q, \cdots$ instead of $x, y, \cdots$.) We define the *order polynomial* $f(G)$ to be

$$f(G) = f(G; x, y, \cdots) = x^a y^b \cdots, \tag{3.1}$$

and the *Eulerian polynomial* $\phi(G)$ to be the summand function of $f(G)$:

$$\phi(G) = \sum_{H \leqq G} \mu_G(H) f(H). \tag{3.2}$$

Since $\mu_G(H) = 0$ unless H contains the Frattini subgroup $\Phi(G)$ of G, we have

$$\phi(G) = \phi(G/\Phi(G)) f(\Phi(G)). \tag{3.3}$$

Thus, e.g., in order to calculate the Eulerian polynomial of a p-group it is sufficient to know the Eulerian polynomial of an elementary abelian group.

Since $\phi_n(G)$ is the summand function of

$$|G|^n = f(G; p^n, q^n, \cdots),$$

we have

$$\phi_n(G) = \phi(G; p^n, q^n, \cdots) \qquad (n = 0, 1, \cdots). \tag{3.4}$$

In particular,

$$\phi(G; 1, 1, \cdots) = 0 \qquad (G > 1).$$

Since

$$f(G; 0, 0, \cdots) = \left.\begin{matrix} 1 & (G = 1) \\ 0 & (G > 1) \end{matrix}\right\},$$

$$\phi(H; 0, 0, \cdots) = \mu_G^*(H),$$

where μ_G^* is the "dual" Möbius function of G (Hall, [4]). By (3.2),

$$\phi(G; 0, 0, \cdots) = \mu_G^*(G) = \mu_G(1). \tag{3.5}$$

THEOREM 1.† If $N \lhd G$,

$$f(N)\phi(G/N) = \sum_{HN=G} \phi(H). \tag{3.6}$$

PROOF.

$$\begin{aligned} f(N)\phi(G/N) &= \sum_{K/N \leqq G/N} f(N)\mu_{G/N}(K/N) f(K/N) \\ &= \sum_{K \geqq N} \mu_G(K) f(K) \\ &= \sum_{K \geqq N} \mu_G(K) \sum_{H \leqq K} \phi(H) \\ &= \sum_{H \leqq G} \phi(H) \sum_{K \geqq NH} \mu_G(K) \\ &= \sum_{NH=G} \phi(H). \end{aligned}$$

Q.E.D.

† This theorem is a slight variant of theorem 1 in Gaschütz [3].

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

E.g., let G be the symmetric group S_4, N its normal subgroup of order 4; then $x_2^2\phi(S_3) = \phi(S_4) + 4\phi(S_3)$, so that $\phi(S_4) = (x_2^2 - 4)\phi(S_3) = (x_2 - 1)(x_2^2 - 4)(x_3 - 3)$. Thus, there are $(2^2 - 1)(2^4 - 4)(3^2 - 3) = 216$ ordered pairs of generators of S_4, $(2^3 - 1)(2^6 - 4)(3^3 - 3) = 10080$ ordered triples of generators, etc.

COROLLARY. $\phi(G/N)|\phi(G)$.

PROOF. We may assume, by induction on the group order, that each term on the right of (3.6) except $\phi(G)$ is divisible by $\phi(G/N)$, for

$$H/H \wedge N \cong G/N \qquad \text{if } HN = G.$$

Hence, by (3.6),

$$\phi(G/N)|\phi(G).$$

4. Numbers of Subgroups of a p-Group

In the present section, G is a p-group such that

$$|G| = p^m, \qquad |G : \Phi(G)| = p^d.$$

The significance of the index d is that G can be generated by d, but no fewer, elements. We shall therefore say that G is a d-generator group.

Let A_k denote the elementary abelian group of order p^k. If A_1 is any subgroup of A_k of order p, there are p^{k-1} A_{k-1}'s such that $A_1 A_{k-1} = A_k$. Therefore, by theorem 1,

$$x\phi(A_{k-1}) = \phi(A_k) + p^{k-1}\phi(A_{k-1}),$$

i.e.

$$\phi(A_k) = (x - p^{k-1})\phi(A_{k-1}).$$

Hence

$$\phi(A_k) = X_k(x),$$

where

$$X_k(x) = \prod_{\lambda=0}^{k-1} (x - p^\lambda). \tag{4.1}'$$

Now, $G/\Phi(G) \cong A_d$. Therefore, by (3.3),

$$\phi(G) = x^{m-d} X_d(x). \tag{4.1}$$

In view of (4.1), the Euler summation formula for G can be written

$$x^m = \sum_{r,s} N_{r,s}(G) x^{s-r} X_r(x), \tag{4.2}$$

where $N_{r,s}(G)$ is the number of r-generator subgroups of G of order p^s. The identity obtained by putting $x = 0$ in (4.2) is perhaps of some interest:

$$\sum_{k=0}^{m} (-1)^k p^{\frac{1}{2}k(k-1)} a_k(G) = 0,$$

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

where $a_k(G)$ is the number of elementary abelian subgroups of G of order p^k.

Taking $G = A_m$ in (4.2), we get

$$x^m = \sum_{k=0}^{m} \omega(m, k) X_k(x), \tag{4.3}$$

where

$$\omega(m, k) = \omega(m, m-k) = \frac{(p^m - 1)(p^{m-1} - 1) \cdots (p^{m-k+1} - 1)}{(p^k - 1)(p^{k-1} - 1) \cdots (p - 1)}$$

is the number of subgroups of A_m of order p^k. By (2.8) and (3.5), the Möbius function $\mu = \mu_{A_m}$ of A_m is given by

$$\mu(A_{m-k}) = (-1)^k p^{\frac{1}{2}k(k-1)}.$$

Hence the inversion formula corresponding to (4.3) is

$$X_m(x) = \sum_{k=0}^{m} (-1)^k \omega(m, k) p^{\frac{1}{2}k(k-1)} x^{m-k}. \tag{4.4}$$

THEOREM 2.

$$\omega(m, k) = \sum_{r \leqq k \leqq s} \omega(s - r, k - r) p^{r(s-k)} N_{r,s}(G) \qquad (0 \leqq k \leqq m). \tag{4.5}$$

PROOF. Replacing x by xp^{-t} in (4.3) and then simplifying, we get,

$$x^m X_t(x) = \sum_{k=0}^{m} \omega(m, k) p^{t(m-k)} X_{t+k}(x). \tag{4.5}'$$

Using (4.5)', we can write (4.2) as

$$x^m = \sum_{r,s} N_{r,s}(G) \sum_{k=r}^{s} \omega(s - r, k - r) p^{r(s-k)} X_k(x). \tag{4.6}$$

Comparison of the coefficients of $X_k(x)$ in (4.3) and (4.6) now gives the theorem.

Let $n_k(G)$ denote* the number of subgroups of G of order p^k, $N_k(G)$ the number of subgroups of G which can be generated by k (or fewer) elements and have order $\geqq p^k$. Since

$$n_k(G) = \sum_{r \leqq k} N_{r,k}(G),$$

$$N_k(G) = \sum_{r \leqq k \leqq s} N_{r,s}(G),$$

we have

COROLLARY 1. $N_k(G) \leqq N_k(A_m) = \omega(m, k).$

COROLLARY 2. $n_k(G) \leqq n_k(A_m) = \omega(m, k).$

* The notation $n_k(G)$ is more convenient for our present purposes than the systematic notation $n_G(p^k)$ used in § 1.

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

Since $\omega(m, 1) = (p^m - 1)/(p - 1)$, it is clear that $N_1(G) = N_1(A_m)$ if, and only if, G has exponent p. On the other hand, if $N_k(G) = N_k(A_m)$ and $1 < k < m$ then $G \cong A_m$. For, by (4.5), $N_{r,s}(G) = 0$ whenever $0 < r \leqq k < s$. It follows that

(a) every r-generator subgroup of G $(r \leqq k)$ has order $\leqq p^k$;

(b) every subgroup of G of order p^{k+1} is elementary abelian.

Let $x, y \in G$. By (a), and because $k \geqq 2$, $|\{x, y\}| \leqq p^k$. Therefore, by (b), $\{x, y\}$ is contained in an elementary abelian subgroup of G. Hence $x^p = y^p = xyx^{-1}y^{-1} = 1$, and so G is elementary abelian.

Theorem 2 throws some light on the well known enumeration theorems of p-group theory. E.g., let $C_r(G)$ denote the number of cyclic subgroups of G of order p^r; taking congruences (mod p^2) in (4.5), we get, for $0 < k \leqq m$,

$$n_k(G) + C_{k+1}(G)p \equiv \omega(m, k) \pmod{p^2}, \tag{4.7}$$

and so, for $0 < k < m$,

$$n_k(G) + C_{k+1}(G)p \equiv 1 + p \pmod{p^2}.* \tag{4.8}$$

(4.8) is to be compared with the theorems of Kulakoff and Miller that, when G is non-cyclic, $p > 2$ and $0 < k < m$,

$$n_k(G) \equiv 1 + p \pmod{p^2},$$
$$C_{k+1}(G) \equiv 0 \pmod{p}.$$

Again, if $0 \leqq k \leqq d$ and if G is not elementary abelian, (4.5) yields the congruence

$$n_{m-k}(G) \equiv \omega(m, k) - N_{d-k+1,m-k+1}(G)p^{d-k+1} \pmod{p^{d-k+2}};$$

$N_{d-k+1,m-k+1}(G)$ being the number of subgroups H of G of order p^{m-k+1} such that $\Phi(H) = \Phi(G)$. This is a slight refinement of P. Hall's congruence

$$n_{m-k}(G) \equiv \omega(d, k) \pmod{p^{d-k+1}}.$$

(Cf. Zassenhaus [11]).

5. The Eulerian Polynomial of a Chain

In the present section, G is once more an arbitrary finite group. The general Eulerian polynomials considered below are, so to speak, "polarized" forms of the basic Eulerian polynomial $\phi(G)$.

Let

$$\mathcal{G} : 1 = G_0 \leqq G_1 \leqq \cdots \leqq G_r = G \tag{5.1}$$

be a chain of subgroups, of formal length r, joining the identity to G. If $H \leqq G$, we call

* (4.7) reduces to $1 + p \equiv \omega(m, k) \pmod{p^2}$ when G is the cyclic group of order p^m.

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

$$\mathscr{H} : 1 = H_0 \leqq \cdots \leqq H_r = H, \qquad (H_i = G_i \wedge H) \tag{5.2}$$

the *subchain* of $\mathscr{G}$ corresponding to H. If $H \lhd G$, we call

$$\mathscr{G}/\mathscr{H} : 1 = (G/H)_0 \leqq \cdots \leqq (G/H)_r = G/H \qquad ((G/H)_i = G_i H/H) \tag{5.3}$$

the *factor chain* of $\mathscr{G}$ corresponding to G/H. We write $\mathscr{H} \leqq \mathscr{G}$ when $H \leqq G$, $\mathscr{H} \lhd \mathscr{G}$ when $H \lhd G$. Corresponding subgroups and subchains are denoted by corresponding Italian and script capitals. The following easily proved facts justify this convention:

(a) if $H \leqq K \leqq G$, then $\mathscr{H} \leqq \mathscr{K}$;

(b) if $H \lhd G$ and $H \leqq K \leqq G$, then $\mathscr{K}/\mathscr{H} \leqq \mathscr{G}/\mathscr{H}$;

(c) if $H \lhd G$, $K \lhd G$ and $H \leqq K \leqq G$, then the natural homomorphism of $(G/H)/(K/H)$ onto G/K maps $(\mathscr{G}/\mathscr{H})/(\mathscr{K}/\mathscr{H})$ onto $\mathscr{G}/\mathscr{K}$.

The subchains corresponding to the subgroups $HK\cdots$ (where $H, K, \cdots$ are permutable), $H \wedge K \wedge \cdots$, $\{H, K, \cdots\}$ are denoted by $\mathscr{H}\mathscr{K}\cdots$, $\mathscr{H} \wedge \mathscr{K} \wedge \cdots$, $\{\mathscr{H}, \mathscr{K}, \cdots\}$ respectively.

We define now the order, and Eulerian, polynomials of the chain $\mathscr{G}$. For each "link" $G_{i-1} \leqq G_i$, we choose variables $x_i, y_i, \cdots$ corresponding to the distinct prime divisors $p, q, \cdots$ of $|G|$. Let

$$|G_i : G_{i-1}| = p^{a_i} q^{b_i} \cdots \qquad (1 \leqq i \leqq r),$$

and let ξ_i stand collectively for the variables $x_i, y_i, \cdots$. Then we define

$$f(\mathscr{G}) = f(\mathscr{G}; \xi_1, \cdots, \xi_r) = \prod_{i=1}^{r} (x_i^{a_i} y_i^{b_i} \cdots), \tag{5.4}$$

$$\phi(\mathscr{G}) = \sum\nolimits^{-1} f(\mathscr{G}). \tag{5.5}$$

The domain of summation in (5.5) is the set of subchains of $\mathscr{G}$ or, what is essentially the same, the set of subgroups of G. Thus,

$$\phi(\mathscr{G}) = \sum_{H \leqq G} \mu_G(H) f(\mathscr{H}). \tag{5.6}$$

Clearly, $\phi(\mathscr{G})$ reduces to $\phi(G)$ when $r = 1$.

As before, $\phi(\mathscr{G})$ corresponds to a series of (generalized) Eulerian functions. Let $\boldsymbol{N} = (N_1, \cdots, N_r)$ be a row of r integers such that $N_1 \geqq N_2 \geqq \cdots \geqq N_r \geqq 0$. Write

$$n_i = N_i - N_{i+1} \qquad (1 \leqq i \leqq r;\ N_{r+1} = 0),$$

so that

$$N_i = \sum_{j=i}^{r} n_j \qquad (1 \leqq i \leqq r).$$

By an *$\boldsymbol{N}$-sequence for $\mathscr{G}$* we shall mean a sequence of N_1 elements of G whose first n_1 members belong to G_1, next n_2 to G_2, etc. By a *generating $\boldsymbol{N}$-sequence for $\mathscr{G}$* we mean an $\boldsymbol{N}$-sequence for $\mathscr{G}$ whose members generate G. The ***$\boldsymbol{N}$-th Eulerian***

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

function $\phi_N(\mathscr{G})$ of $\mathscr{G}$ is defined as the total number of generating N-sequences for $\mathscr{G}$. Let $\mathscr{H} \leqq \mathscr{G}$. It is easy to see that the total number of N-sequences for $\mathscr{H}$ is

$$f_N(\mathscr{H}) = f(\mathscr{H}; p^{N_1}, q^{N_1}, \cdots, p^{N_r}, q^{N_r}, \cdots).$$

Also, each N-sequence for $\mathscr{H}$ is generating N-sequence for a unique $\mathscr{K} \leqq \mathscr{H}$. Hence

$$f_N = \sum \phi_N,$$

and therefore

$$\phi_N(\mathscr{G}) = \phi(\mathscr{G}; p^{N_1}, q^{N_1}, \cdots, p^{N_r}, q^{N_r}, \cdots). \tag{5.7}$$

The fundamental property of the order polynomial is that

$$f(\mathscr{G}) = f(\mathscr{N})f(\mathscr{G}/\mathscr{N}) \qquad (\mathscr{N} \lhd \mathscr{G}). \tag{5.8}$$

In fact, since

$$G_\kappa N/N = G_\kappa/N_\kappa \qquad (\kappa = i-1, i),$$

we have the index formula

$$|\Gamma_i : \Gamma_{i-1}|\,|N_i : N_{i-1}| = |G_i : G_{i-1}| \qquad (\Gamma = G/N), \tag{5.9}$$

of which (5.8) is an immediate consequence.

In view of (5.8), both (3.3) and theorem 1 carry over to the present case.

$$\phi(\mathscr{G}) = f(\Phi(\mathscr{G}))\phi(\mathscr{G}/\Phi(\mathscr{G})), \tag{5.10}$$

where $\Phi(\mathscr{G})$ *is the subchain corresponding to* $\Phi(G)$.

THEOREM 3. *If* $\mathscr{N} \lhd \mathscr{G}$,

$$f(\mathscr{N})\phi(\mathscr{G}/\mathscr{N}) = \sum_{\mathscr{K}\mathscr{N} = \mathscr{G}} \phi(\mathscr{H}). \tag{5.11}$$

It is *not* in general true that $\phi(\mathscr{G}/\mathscr{N})|\phi(\mathscr{G})$. However, the following result does include the corollary to theorem 1 as a special case.

COROLLARY. *If* $\mathscr{N} \lhd \mathscr{G}$ *and if* $G_{\kappa-1} \leqq N \leqq G_\kappa$ *for some* κ, *then* $\phi(\mathscr{G}/\mathscr{N})|\phi(\mathscr{G})$.

PROOF. The proof of the corollary to theorem 1 shows that it is sufficient to prove the statement:

$$\text{If } \mathscr{K}\mathscr{N} = \mathscr{G}, \text{ then } \phi(\mathscr{K}/\mathscr{K} \wedge \mathscr{N}) = \phi(\mathscr{G}/\mathscr{N}). \tag{5.12}$$

(5.12) is proved by showing that the natural homomorphism of $K/K \wedge N$ onto $KN/N = G/N$ maps $\mathscr{K}/\mathscr{K} \wedge \mathscr{N}$ onto $\mathscr{G}/\mathscr{N}$; i.e.

$$K_i N = G_i N \qquad (0 \leqq i \leqq r). \tag{5.13}$$

By hypothesis, $G_{\kappa-1} \leqq N \leqq G_\kappa$. If $i < \kappa$, clearly $K_i N = G_i N = N$. If $i \geqq \kappa$, $K_i N = (K \wedge G_i)N = (KN) \wedge G_i = G_i = G_i N$ because $G_i \geqq N$ and $KN = G$. This proves (5.13) and the corollary.

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

6. Chains in a p-Group

In this section, G is a p-group and $\mathscr{G}$ the corresponding chain (5.1) of formal length r. In order to simplify the notation, we observe the following conventions.

(a) Boldface letters (lower and upper case) stand for row vectors of length r with non-negative integral components:

$$\boldsymbol{m} = (m_1, \cdots, m_r), \qquad \boldsymbol{M} = (M_1, \cdots, M_r), \cdots$$

where

$$m_i \geqq 0, \ M_i \geqq 0, \cdots \qquad (1 \leqq i \leqq r).$$

(b) Corresponding lower and upper case vectors $\boldsymbol{m}$, $\boldsymbol{M}$ are related by:

$$M_i = \sum_{j=i}^{r} m_j, \quad m_i = M_i - M_{i+1} \quad (M_{r+1} = 0) \qquad (1 \leqq i \leqq r).$$

Thus, the upper case vectors $\boldsymbol{M}$ are those which satisfy:

$$M_1 \geqq M_2 \geqq \cdots \geqq M_r \geqq M_{r+1} = 0$$

(c) Inequality $\boldsymbol{m} \geqq \boldsymbol{n}$ means that $m_i \geqq n_i$ $(1 \leqq i \leqq r)$.

Writing

$$\boldsymbol{m} = \boldsymbol{m}(\mathscr{G}) = (m_1, \cdots, m_r),$$
$$\boldsymbol{D} = \boldsymbol{D}(\mathscr{G}) = (D_1, \cdots, D_r),$$

where

$$\left.\begin{aligned} |G_i : G_{i-1}| &= p^{m_i} \\ |\Gamma : \Gamma_{i-1}| &= p^{D_i} \quad (\Gamma = G/\Phi(G)) \end{aligned}\right\} \qquad (1 \leqq i \leqq r),$$

we call $\mathscr{G}$ a $\boldsymbol{D}$-*generator* chain of *reduced order* $\boldsymbol{m}$. We first set down some fairly obvious properties of $\boldsymbol{m}$, $\boldsymbol{D}$.

(6.1) *If $\mathscr{H}$ is a subchain or factor chain of $\mathscr{G}$,*

$$\boldsymbol{m}(\mathscr{H}) \leqq \boldsymbol{m}(\mathscr{G}).$$

(6.2) $\boldsymbol{m}(\Phi(\mathscr{G})) = \boldsymbol{m}(\mathscr{G}) - \boldsymbol{d}(\mathscr{G})$; *hence, if* $\mathscr{H} \leqq \mathscr{G}$,

$$\boldsymbol{0} \leqq \boldsymbol{m}(\mathscr{H}) - \boldsymbol{d}(\mathscr{H}) \leqq \boldsymbol{m}(\mathscr{G}) - \boldsymbol{d}(\mathscr{G}).$$

(6.3) *If $D_i = 0$, then M_i $(= m_i + \cdots + m_r) = 0$.*

For if $D_i = 0$, then $G_{i-1}\Phi(G) = G$ and so $G_{i-1} = G$; thus $p^{M_i} = |G : G_{i-1}| = p^0$.

The Eulerian polynomial of $\mathscr{G}$ is calculated in much the same way as that of G, and we therefore omit the proof.

(6.4) *If $\mathscr{G}$ is a $\boldsymbol{D}$-generator chain of reduced order $\boldsymbol{m}$, then*

$$\phi(\mathscr{G}; x_1, \cdots, x_r) = \prod_{i=1}^{r} x_i^{m_i - d_i} \prod_{\lambda_i = D_{i+1}}^{D_i - 1} (x_i - p^{\lambda_i}).$$

The following immediate corollary justifies the term "$\boldsymbol{D}$-generator chain".

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

(6.5) *Let $\mathscr{G}$ be a $\boldsymbol{D}$-generator chain and $\boldsymbol{N}$ an upper case vector. Then $\phi_{\boldsymbol{N}}(\mathscr{G}) > 0$ if, and only if, $\boldsymbol{N} \geqq \boldsymbol{D}$.*

From now on we confine attention to *regular* chains in the sense of the following definition.

Definition. $\mathscr{G}$ is called regular if $\boldsymbol{m}(\mathscr{H}) - \boldsymbol{D}(\mathscr{H})$ is upper case for each $\mathscr{H} \leqq \mathscr{G}$. If

$$\boldsymbol{m}(\mathscr{H}) - \boldsymbol{D}(\mathscr{H}) = \boldsymbol{T}(\mathscr{H}),$$

then the pair of vectors

$$\sigma(\mathscr{H}) = (\boldsymbol{t}(\mathscr{H}), \boldsymbol{D}(\mathscr{H}))$$

is called the signature of $\mathscr{H}$.

Clearly, every subchain of a regular chain is regular (though the corresponding statement for factor chains is easily seen to be false). The Eulerian polynomial of a regular chain of signature $(\boldsymbol{t}, \boldsymbol{D})$ can be written in the form

$$\phi(\mathscr{G}; x_1, \cdots, x_r) = Y_{\boldsymbol{t},\boldsymbol{D}}(1, y_1, \cdots, y_r) \tag{6.6}$$

where

$$y_i = x_1 x_2 \cdots x_i \qquad (1 \leqq i \leqq r),$$

$$Y_{\boldsymbol{t},\boldsymbol{D}}(z_0, z_1, \cdots, z_r) = \prod_{i=1}^{r} z_i^{t_i} \prod_{\lambda_i = D_{i+1}}^{D_i - 1} (z_i - p^{\lambda_i} z_{i-1}). \tag{6.7}$$

We remark that $\boldsymbol{m}(\mathscr{H}) - \boldsymbol{D}(\mathscr{H})$ is upper case if, and only if,

$$m_i(\mathscr{H}) - d_i(\mathscr{H}) \geqq m_{i+1}(\mathscr{H}) \qquad (1 \leqq i \leqq r;\ m_{r+1}(\mathscr{H}) = 0)$$

i.e.

$$m_i(\Phi(\mathscr{H})) \geqq m_{i+1}(\mathscr{H}) \qquad (1 \leqq i \leqq r). \tag{6.8}$$

Examples.

(1) If $r = 1$, $\mathscr{G}$ is regular.

(2) Let G be a regular group of exponent p^k (P. Hall [5]). Then the elements of G of order $\leqq p^i$ form a subgroup $\Omega_i(G)$ $(i = 0, 1, \cdots)$. Consider the chain

$$\mathscr{G} : 1 = \Omega_0(G) \leqq \Omega_1(G) \leqq \cdots \leqq \Omega_r(G) = G,$$

where $r \geqq k$. It is known that $m_i = m_i(\mathscr{G})$ is the number of elements of order $\geqq p^i$ in a basis of G. If $H \leqq G$, H is regular and

$$\mathscr{H} : 1 = \Omega_0(H) \leqq \cdots \leqq \Omega_r(H) = H$$

is the corresponding subchain of $\mathscr{G}$. We prove now that $\mathscr{G}$ is regular.

By the remarks above, it is sufficient to verify (6.8) for $\mathscr{G}$. Let K be the subgroup of G formed by the p-th powers of the elements of G, $\mathscr{K}$ the corresponding subchain of $\mathscr{G}$. It is known that the number of elements of order $\geqq p^i$ in a basis of K is the number of elements of order $\geqq p^{i+1}$ in a basis of G. Therefore, since $K \leqq \Phi(G)$, we have

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

$$m_i(\Phi(\mathscr{G})) \geqq m_i(\mathscr{K}) = m_{i+1}(\mathscr{G}),$$

as required.

In general, if G is a p-group in which the elements of order $\leqq p^i$ form a subgroup $\Omega_i(G)$ for $i = 1, 2, \cdots$, then we shall call a chain

$$\mathscr{G} : 1 = \Omega_0(G) \leqq \Omega_1(G) \leqq \cdots \leqq \Omega_r(G) = G$$

an *Ω-series* of G. The example of the quaternion group shows that an Ω-series need not be regular.

(3) If the regular group G in (2) is abelian then $K = \Phi(G)$ and so

$$m_i(\Phi(\mathscr{G})) = m_{i+1}(\mathscr{G}) \qquad (1 \leqq i \leqq r);$$

thus the signature of $\mathscr{G}$ (and of each subchain) has the form $(\boldsymbol{0}, \boldsymbol{D}(\mathscr{G}))$. Following P. Delsarte ([2]), we shall call G the abelian group of signature $\boldsymbol{D}(\mathscr{G})$.

In general, if $\mathscr{G}$ is a regular chain in the p-group G and if $\mathscr{H} \leqq \mathscr{G}$ has signature $(\boldsymbol{0}, \boldsymbol{D})$, then we shall say that the subgroup H corresponding to $\mathscr{H}$ has *zero type* with respect to $\mathscr{G}$. Since the vector $\boldsymbol{m}(\mathscr{H}) - \boldsymbol{D}(\mathscr{H})$ is upper case, H has zero type if, and only if, $m_1(\mathscr{H}) = D_1(\mathscr{H})$. Simple examples show that a regular group may have zero type with respect to its Ω-series and yet not be lattice-isomorphic to an abelian group.

(4) Let

$$\mathscr{G}^* : 1 = G_0^* \leqq \cdots \leqq G_s^* = G$$

be any regular chain. Form a new chain

$$\mathscr{G} : 1 = G_0 \leqq \cdots \leqq G_r = G$$

by taking

$$G_i = G^*_{N_1+N_2+\cdots+N_i} \qquad (1 \leqq i \leqq r),$$

where $\boldsymbol{N} = (N_1, \cdots, N_r)$ is upper case. It is easily verified (using (6.8)) that $\mathscr{G}$ is regular.

The results which follow deal with the property of having zero type.

(6.9) *Let $\mathscr{G}$ be a regular chain in the p-group G. Then G_i contains every element of G of order $\leqq p^i$ $(i = 1, 2, \cdots)$.*

Proof. Let H be a cyclic subgroup of G of order $p^k \leqq p^i$, $\mathscr{H}$ the corresponding subchain of $\mathscr{G}$. Write

$$m_j = m_j(\mathscr{H}), \qquad D_j = D_j(\mathscr{H}).$$

Then

(6.10) $$m_1 \geqq m_2 \geqq \cdots \text{ and } \sum m_j = k,$$

whence $m_{k+1} = m_{k+2} = \cdots = 0$. Thus, $H \leqq G_k \leqq G_i$.

(6.11) *Let $\mathscr{G}$ be a regular chain in the p-group G. Then $\mathscr{G}$ is an Ω-series of G if, and only if, each cyclic subgroup of G has zero type with respect to $\mathscr{G}$.*

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

PROOF. Suppose that the cyclic subgroup H of G has zero type. In the notation of the previous proof,

$$m_1 - D_1 = 0, \qquad D_1 = 1,$$

so that, by (6.10),

$$m_1 = m_2 = \cdots = m_k = 1.$$

Hence H is a subgroup of G_k but not of G_{k-1}. It follows that if every cyclic subgroup of G has zero type then $G_i - G_{i-1}$ is the set of elements of G of order p^i $(i = 1, 2, \cdots)$, i.e. $\mathscr{G}$ is an Ω-series of G. The converse is easily proved by reversing the steps of the argument.

(6.12) *Let $\mathscr{G}$ be a regular chain in the p-group G and suppose that every subgroup of G which can be generated by 2 elements has zero type with respect to $\mathscr{G}$. Then, if $p > 3$, or if G is regular, G is lattice-isomorphic to an abelian group and $\mathscr{G}$ is an Ω-series of G.*

PROOF. Since every regular 2-group is abelian (Kemhadze [12]), we assume that $p > 2$. We first prove, by induction on the order of G, that any two cyclic subgroups of G permute. We know already (by (6.11)) that $\mathscr{G}$ is an Ω-series of G. This implies, in particular, that each G_i is a normal subgroup of G.

Suppose that the cyclic subgroups $X = \{x\}$, $Y = \{y\}$ did not permute. By induction, $\{X, Y\} = G$ and so, in particular, $D_1(\mathscr{G}) = 2$. Since G has zero type, $m_1(\mathscr{G}) = 2$ i.e.

$$|G_1| = p^2. \tag{6.13}$$

Write $|G| = p^\alpha$, $|X| = p^\lambda$, $|Y| = p^\mu$. If λ (say) were 1, we should have $XY = Y$ or YG_1, contrary to the assumption that XY is not a subgroup; hence $\lambda > 1$, $\mu > 1$.

It is a straightforward matter to verify that the chain

$$\mathscr{G}' : 1 = G_1/G_1 < G_2/G_1 < \cdots < G_r/G_1 = G/G_1$$

is regular and that every subgroup of G/G_1 which can be generated by 2 elements has zero type with respect to $\mathscr{G}'$. By induction, $\{xG_1\}$ and $\{yG_1\}$ permute, so that

$$XYG_1 = G. \tag{6.14}$$

Consider now the subgroups

$$X^* = \{x^p\}, \qquad Y^* = \{y^p\}, \qquad H = \{X^*, Y\}, \qquad K = \{X, Y^*\}.$$

Since X^*, Y^* are subgroups of $\Phi(G)$, H, K are proper subgroups of G. By induction, $H = X^*Y$, $K = XY^*$. If $H_1 = G_1$ then, by (6.14), $XY = G$, contrary to the assumption that X, Y do not permute. Hence $|H_1| = p$

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

and similarly $|K_1| = p$. Since H, K have zero type, they must be cyclic groups. Thus, $X^* = Y^* = X \wedge Y$. It follows that $\lambda = \mu$, $|XY| = p^{\lambda+1}$, and from (6.14) that $|XY| = p^{a-1}$. Thus $\lambda = a - 2$.

It is now clear that X^* is a central normal subgroup of G of index p^3 and order $\geqq p$. The factor group G/X^* is non-commutative and is generated by the elements xX^*, yY^* of order p; it is therefore the non-commutative group of order p^3 and exponent p. Writing $u = yxy^{-1}x^{-1}$, we have:

$$yuy^{-1}u^{-1} = c, \qquad xux^{-1}u^{-1} = d \qquad (c, d \in X^*), \qquad |\{uX^*\}| = p,$$

(6.15) $x^\alpha y^\beta \in \{uX^*\}$ if, and only if, $\alpha \equiv \beta \equiv 0 \pmod{p}$.

Since y^p, x^p are in the centre of G, $c^p = d^p = c^{\binom{p}{2}} u^p = 1$. Therefore, since $p > 2$, $u^p = 1$.

It follows from the above and (6.13) that

$$G_1 = \{u, x^{p^{a-2}}\}. \tag{6.16}$$

On the other hand, a direct calculation shows that

$$(xy)^p = u^{\binom{p}{2}} x^p y^p c^{\binom{p}{3}} d^{\binom{p}{2}+2\binom{p}{3}}$$

and therefore, if $p > 3$,

$$(xy)^p = x^p y^p.$$

This also holds if $p = 3$, for then G is regular and so

$$(xy)^3 = x^3 y^3 u^{3\alpha} c^{3\beta} d^{3\gamma} = x^3 y^3.$$

Hence, in all cases, for a suitable choice of the generators x, y, we have $xy \in G_1$. This contradiction to (6.15) and (6.16) establishes our result.

It now follows that any two subgroups of G permute and thence that the lattice of subgroups of G is modular. Since $p > 2$, G is lattice-isomorphic to an abelian group (M. Suzuki [8]). Q.E.D.

(6.12) is not true for non-regular 2- and 3-groups, as the Ω-series in the following groups show †:

(6.17) $G = \{x, y, u\}$ of order 3^4; $x^9 = u^3 = x^3 y^3 = [x, u] = 1$, $[y, x] = u$, $[y, u] = y^3$.

(6.18) $G = \{x, y\}$ of order $2^{r+2} \geqq 2^4$; $x^{2^r} = y^4 = 1$, $[y, x] = y^2$.

(6.19) $G = \{x, y\}$ of order $2^{r+2} \geqq 2^6$; $x^{2^r} = y^4 = 1$, $[y, x] = y^2 x^{2^{r-1}}$.

These examples are all "minimal" in the sense that every proper subgroup of G is lattice-isomorphic to an abelian group. G itself is not lattice-isomorphic to an abelian group because (in each case) $G/\{x^p\}$ is the group of order p^3 generated by 2 elements of order p.

We end this section by deriving the analogue of (4.5)′ for the polynomials $Y_{t,D}$ (cf. (6.7)).

† $[s, t]$ stands for the commutator $sts^{-1}t^{-1}$.

LEMMA. *Let d, D, s, t be integers $\geqq 0$. Then*

$$(6.20)\quad x^t \prod_{\lambda=0}^{d-1}(x-yp^{D+\lambda}) = \sum_{i=0}^{\min(d,s)} \sum_{j=0}^{t} \theta(d,D,s,t;i,j) y^{t-j+i} \prod_{\mu=0}^{d+j-i-1}(x-yp^{D+s+\mu}),$$

where

$$(6.21)\quad \theta(d,D,s,t;i,j) = \omega(s,i)\omega(d,i)\omega(t,j)X_i(p^i)p^{(t-j)(D+d+s-i)+iD}.$$

(For the notation $\omega(k,l)$, $X_k(x)$ see (4.1)′, (4.3)′.)

PROOF. It is easily proved by induction that

$$X_d(z)X_s(z) = \sum_{i=0}^{\min(d,s)} \omega(d,i)\omega(s,i)X_i(p^i)X_{d+s-i}(z).$$

Combining this formula with (4.5)′, we get

$$z^t X_d(z)X_s(z) = \sum_{i=0}^{\min(d,s)} \omega(d,i)\omega(s,i)X_i(p^i) \sum_{j=0}^{t} \omega(t,j)p^{(t-j)(d+s-i)} X_{d+s+j-i}(z).$$

Finally, dividing through by $X_s(z)$, then putting $z = xy^{-1}p^{-D}$ and simplifying, we get (6.20).

THEOREM 4.

$$(6.22)\quad Y_{t,\boldsymbol{D}}(z_0,\cdots,z_r) = \sum_{\boldsymbol{U}} \left(\sum_{\boldsymbol{i}} \prod_{\kappa=1}^{r} \beta_\kappa(\boldsymbol{i},\boldsymbol{U}) \right) z_0^{T_1+D_1-U_1} Y_{\boldsymbol{0},\boldsymbol{U}}(z_0,\cdots,z_r),$$

where (cf. (6.21))

$$\beta_\kappa(\boldsymbol{i},\boldsymbol{U}) = \theta(d_\kappa, D_{\kappa+1}, U_{\kappa+1}-D_{\kappa+1}, T_\kappa+D_{\kappa+1}-U_{\kappa+1}; i_\kappa, u_\kappa-d_\kappa+i_\kappa) \quad (1\leqq\kappa\leqq r),$$

and where summation is over the vectors $\boldsymbol{U}, \boldsymbol{i}$ such that

$$(6.23)\qquad \boldsymbol{D} \leqq \boldsymbol{U} \leqq \boldsymbol{T} + \boldsymbol{D},$$

$$(6.24)\quad d_\kappa - u_\kappa \leqq i_\kappa \leqq \min(d_\kappa, U_{\kappa+1}-D_{\kappa+1}, T_\kappa + D_\kappa - U_\kappa) \qquad (1 \leqq \kappa \leqq r).$$

($\boldsymbol{D}, \boldsymbol{U}, \cdots$ are the upper case vectors corresponding to $\boldsymbol{d}, \boldsymbol{u}, \cdots$; D_{r+1}, $U_{r+1}, \cdots$ are taken to be zero.)

PROOF. Let us change the variables of summation from $\boldsymbol{i}, \boldsymbol{U}$ to $\boldsymbol{i}$ and $\boldsymbol{j} = \boldsymbol{u} + \boldsymbol{i} - \boldsymbol{d}$. Then (6.22) becomes the final formula P_1 of a series $P_{r+1}, P_r, \cdots, P_1$ defined as follows: P_{r+1} is the trivial formula $1 = 1$; P_ρ $(1 \leqq \rho \leqq r)$ is the formula

$$\prod_{\kappa=\rho}^{r} z_\kappa^{t_\kappa} Y_\kappa = \sum_{i,j} z_{\rho-1}^{T_\rho - J_\rho + I_\rho} \prod_{\kappa=\rho}^{r} Z_\kappa(\boldsymbol{i},\boldsymbol{j})$$

where

$$Y_\kappa = \prod_{\lambda=D_{\kappa+1}}^{D_\kappa-1} (z_\kappa - z_{\kappa-1}p^\lambda),$$

$$Z_\kappa(\boldsymbol{i},\boldsymbol{j}) = \beta_\kappa \prod_{\lambda=D_{\kappa+1}+J_{\kappa+1}-I_{\kappa+1}}^{D_\kappa+J_\kappa-I_\kappa-1} (z_\kappa - z_{\kappa-1}p^\lambda),$$

and where summation is over the indices i_κ, j_κ $(\rho \leqq \kappa \leqq r)$ which satisfy

$$\left.\begin{aligned} 0 &\leqq i_\kappa \leqq \min\,(d_\kappa, J_{\kappa+1} - I_{\kappa+1}), \\ 0 &\leqq j_\kappa \leqq T_\kappa - J_{\kappa+1} + I_{\kappa+1} \end{aligned}\right\} \qquad (\rho \leqq \kappa \leqq r).$$

Now, by the lemma,

$$z_{\rho-1}^{t_{\rho-1}+T_\rho-J_\rho+I_\rho} Y_{\rho-1} = \sum z_{\rho-2}^{T_{\rho-1}-J_{\rho-1}+I_{\rho-1}} Z_{\rho-1}(\boldsymbol{i}, \boldsymbol{j}), \tag{6.25}$$

where summation is over the indices $i_{\rho-1}$, $j_{\rho-1}$ such that

$$0 \leqq i_{\rho-1} \leqq \min\,(d_{\rho-1}, J_\rho - I_\rho),$$
$$0 \leqq j_{\rho-1} \leqq T_{\rho-1} - J_\rho + I_\rho.$$

Multiply both sides of P_ρ by $z_{\rho-1}^{t_{\rho-1}} Y_{\rho-1}$, and using (6.25), we get $P_{\rho-1}$. The theorem follows by induction.

COROLLARY. *Let G be the abelian p-group of (Delsarte) signature $\boldsymbol{T}$. Then the number of subgroups of G of signature $\boldsymbol{U}$ $(\leqq \boldsymbol{T})$ is*

$$\Omega(\boldsymbol{T}, \boldsymbol{U}) = \prod_{\kappa=1}^{r} \omega(T_\kappa - U_{\kappa+1}, u_\kappa) p^{(T_\kappa - U_\kappa)U_{\kappa+1}}. \tag{6.26}$$

In fact, taking $\boldsymbol{D} = \boldsymbol{0}$ in (6.22), we get

$$Y_{\boldsymbol{t}, \boldsymbol{0}} = \sum_{\boldsymbol{U} \leqq \boldsymbol{T}} \Omega(\boldsymbol{T}, \boldsymbol{U}) Y_{\boldsymbol{0}, \boldsymbol{U}},$$

which is essentially the Euler summation formula for the Ω-series of G.

Formulae equivalent to (6.26) have been given by Delsarte [2], Kinosita [6], Yeh [10].

7. Numbers of Subgroups of a p-Group

We are now in a position to generalize the results of § 4. Throughout the present section,

$$\mathscr{G} : 1 = G_0 \leqq G_1 \leqq \cdots \leqq G_r = G \tag{7.1}$$

is a *regular* chain, of formal length r, in the p-group G. $\boldsymbol{m} = \boldsymbol{m}(\mathscr{G})$ is the reduced order of $\mathscr{G}$. B is the abelian group of signature $\boldsymbol{m}$, and

$$\mathscr{B} : 1 = B_0 \leqq B_1 \leqq \cdots \leqq B_r = B \tag{7.2}$$

an Ω-series of B. Since $\boldsymbol{m}(\mathscr{G}) = \boldsymbol{m}(\mathscr{B})$, we have

$$f(\mathscr{G}) = f(\mathscr{B}). \tag{7.3}$$

THEOREM 5. *Let $N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}} = N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}}(\mathscr{G})$ denote the number of subchains of $\mathscr{G}$ of signature $(\boldsymbol{\gamma}, \boldsymbol{\Delta})$. Then*

$$\Omega(\boldsymbol{m}, \boldsymbol{U}) = \sum_{\boldsymbol{\Delta} \leqq \boldsymbol{U} \leqq \boldsymbol{\Gamma} + \boldsymbol{\Delta}} \beta(\boldsymbol{\gamma}, \boldsymbol{\Delta}; \boldsymbol{U}) N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}} \qquad (\boldsymbol{U} \leqq \boldsymbol{m}), \tag{7.4}$$

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

where $\Omega(\boldsymbol{m}, \boldsymbol{U})$ *is given by* (6.26) *and* $\beta(\boldsymbol{\gamma}, \boldsymbol{\Delta}; \boldsymbol{U})$ *is the coefficient of* $z_0^{\Gamma_1+\Delta_1-U_1} Y_{\boldsymbol{0}, \boldsymbol{U}}$ *in the expansion* (6.22) *of* $Y_{\boldsymbol{\gamma}, \boldsymbol{\Delta}}$.

PROOF. Let us denote the Eulerian polynomial (6.6) by $\bar{Y}_{\boldsymbol{t}, \boldsymbol{D}}$. Then, by the Euler summation formulae for $\mathscr{G}, \mathscr{B}$,

$$f(\mathscr{G}) = \sum_{\boldsymbol{\gamma}, \boldsymbol{\Delta}} N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}} \bar{Y}_{\boldsymbol{\gamma}, \boldsymbol{\Delta}},$$

$$f(\mathscr{B}) = \sum_{\boldsymbol{U}} \Omega(\boldsymbol{m}, \boldsymbol{U}) \bar{Y}_{\boldsymbol{0}, \boldsymbol{U}},$$

and so, by (7.3) and theorem 4,

$$\sum \Omega(\boldsymbol{m}, \boldsymbol{U}) \bar{Y}_{\boldsymbol{0}, \boldsymbol{U}} = \sum N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}} \beta(\boldsymbol{\gamma}, \boldsymbol{\Delta}; \boldsymbol{U}) \bar{Y}_{\boldsymbol{0}, \boldsymbol{U}}.$$

Since the $\bar{Y}_{\boldsymbol{0}, \boldsymbol{U}}$ are linearly independent, (7.4) follows. Q.E.D.

LEMMA. $\beta = \beta(\boldsymbol{\gamma}, \boldsymbol{\Delta}; \boldsymbol{U})$ *is a positive integer whenever* $\boldsymbol{\Gamma} \leqq \boldsymbol{U} \leqq \boldsymbol{\Gamma} + \boldsymbol{\Delta}$, *If* $\boldsymbol{U} = \boldsymbol{\Gamma} + \boldsymbol{\Delta}$, $\beta = 1$. *If* $\boldsymbol{U} \neq \boldsymbol{\Gamma} + \boldsymbol{\Delta}$ (*and* $\boldsymbol{\Gamma} \leqq \boldsymbol{U} \leqq \boldsymbol{\Gamma} + \boldsymbol{\Delta}$), *either* $N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}} = 0$ *or* $\beta \equiv 0 \pmod{p}$.

PROOF. The first two statements are seen by inspection. To prove the third, we show that if $\boldsymbol{U} \neq \boldsymbol{\Gamma} + \boldsymbol{\Delta}$ and $N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}} \neq 0$ then each term $\beta(\boldsymbol{i}) = \prod_\kappa \beta_\kappa(\boldsymbol{i})$ in the sum $\beta = \sum_{\boldsymbol{i}} \beta(\boldsymbol{i})$ is divisible by p (cf. (6.22)).

Suppose, contrary to our assertion, that $\beta(\boldsymbol{i}) \not\equiv 0 \pmod{p}$ for some value of $\boldsymbol{i}$. By (6.21) and (6.22),

$$\left.\begin{aligned} &\tfrac{1}{2} i_\kappa (i_\kappa - 1) = 0, \\ &(\Gamma_\kappa + \Delta_\kappa - U_\kappa - i_\kappa)(\delta_\kappa + U_{\kappa+1} - i_\kappa) = 0, \\ &i_\kappa \Delta_{\kappa+1} = 0 \end{aligned}\right\} \qquad (1 \leqq \kappa \leqq r). \tag{7.4}'$$

By assumption, $\Gamma_\lambda + \Delta_\lambda - U_\lambda \neq 0$ for some value λ. By (7.4)', $i_\lambda = 1$ or 0. If $i_\lambda = 1$, then, by (7.4)', $\Delta_{\lambda+1} = 0$. By (6.3) and since $N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}} \neq 0$, $\Gamma_{\lambda+1} + \Delta_{\lambda+1} = 0$. Therefore, since $\boldsymbol{U} \leqq \boldsymbol{\Gamma} + \boldsymbol{\Delta}$, $U_{\lambda+1} = 0$. This is impossible for, by (6.24), $i_\lambda \leqq \Delta_{\lambda+1} + U_{\lambda+1}$. Hence $i_\lambda = 0$. By (7.4)', $\delta_\lambda = U_{\lambda+1} = 0$. Since $\boldsymbol{\Delta} \leqq \boldsymbol{U}$, $\Delta_{\lambda+1} = 0$ and so $\Delta_\lambda = \delta_\lambda + \Delta_{\lambda+1} = 0$. Arguing as before, we get $U_\lambda = \Gamma_\lambda + \Delta_\lambda = 0$, contrary to the assumption that $\Gamma_\lambda + \Delta_\lambda - U_\lambda \neq 0$. This establishes the lemma.

Write

$$\begin{aligned} N_{\boldsymbol{U}}(\mathscr{G}) &= \sum_{\boldsymbol{\Delta} \leqq \boldsymbol{U} \leqq \boldsymbol{\Gamma} + \boldsymbol{\Delta}} N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}}(\mathscr{G}), \\ n_{\boldsymbol{U}}(\mathscr{G}) &= \sum_{\boldsymbol{U} = \boldsymbol{\Gamma} + \boldsymbol{\Delta}} N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}}(\mathscr{G}), \\ N_k(G) &= \sum_{\Delta_1 \leqq k \leqq \Sigma(\Gamma_t + \Delta_t)} N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}}(\mathscr{G}), \\ n_k(G) &= \sum_{k = \Sigma(\Gamma_t + \Delta_t)} N_{\boldsymbol{\gamma}, \boldsymbol{\Delta}}(\mathscr{G}), \\ n(G) &= \sum_k n_k(G). \end{aligned}$$

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

In words: N_U is the number of subchains which have a generating U-sequence and reduced order $\geqq U$; n_U is the number of subchains of reduced order U; N_k, n_k are the functions already considered in § 4; $n(G)$ is the total number of subgroups of G. Clearly,

$$N_U(\mathscr{B}) = n_U(\mathscr{B}) = \Omega(\boldsymbol{m}, \boldsymbol{U}).$$

The following two results are immediate consequences of theorem 5 and the lemma.

(7.5) *Either* $n_U(\mathscr{G}) < N_U(\mathscr{G}) < \Omega(\boldsymbol{m}, \boldsymbol{U})$ *or* $n_U(\mathscr{G}) = N_U(\mathscr{G}) = \Omega(\boldsymbol{m}, \boldsymbol{U})$.

(7.6) $n_U(\mathscr{G}) \equiv \Omega(\boldsymbol{m}, \boldsymbol{U}) \pmod{p}$.

The congruence class of $\Omega(\boldsymbol{m}, \boldsymbol{U})$ modulo p is easily determined. Suppose that $U_s \neq 0$ but $U_\lambda = 0$ for all $\lambda > s$. Then, by (6.26), $\Omega \equiv 1 \pmod{p}$ if $m_\lambda = U_\lambda$ for $\lambda = 1, \cdots, s-1$, and $\Omega \equiv 0 \pmod{p}$ otherwise. Hence we have

(7.7) $n_U(\mathscr{G}) \equiv 1$ *or* $0 \pmod{p}$ *according as* U *is, or is not, the signature of a subgroup of* B *which lies between two consecutive members of its* Ω*-series.*

(7.8) $N_k(G) \leqq N_k(B)$, *with equality if, and only if, every subgroup of* G *which has order* $> p^k$ *and can be generated by* k *elements has zero type with respect to* $\mathscr{G}$ (*Cf.* § 6, *example* (3)).

PROOF. By the definition of N_k and theorem 5, we have

$$N_k(G) = \sum_{\Delta_1 \leqq k \leqq \Sigma(\Gamma_i + \Delta_i)} N_{\gamma, \Delta}(\mathscr{G}),$$

$$N_k(B) = \sum_{U_1 \leqq k \leqq \Sigma U_i} \Omega(\boldsymbol{m}, \boldsymbol{U}) \tag{7.9}$$

$$= \sum_{U_1 \leqq k \leqq \Sigma U_i} \sum_{\Delta \leqq U \leqq \Gamma + \Delta} \beta(\gamma, \Delta; U) N_{\gamma, \Delta}(\mathscr{G}).$$

Now, if the vectors γ, Δ satisfy $\Delta_1 \leqq k \leqq \sum (\Gamma_i + \Delta_i)$, then the vector V defined by

$$V_i = \min (k, \Gamma_i + \Delta_i) \qquad (1 \leqq i \leqq r)$$

is upper case and satisfies

$$V_1 \leqq k \leqq V_i, \qquad \Delta \leqq V \leqq \Gamma + \Delta. \tag{7.10}$$

In view of (7.9), $N_k(G) \leqq N_k(B)$ with equality if, and only if, the conditions

$$\Delta_1 \leqq k \leqq \sum (\Gamma_i + \Delta_i), \qquad N_{\gamma, \Delta}(\mathscr{G}) \neq 0, \tag{7.11}$$

imply that

(a) (7.10) has a unique solution V;

(b) $\beta(\gamma, \Delta; V) = 1$, i.e., by the lemma, $V = \Gamma + \Delta$.

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

We remark now that (7.11) and either of the two conditions

$$\sum (\Gamma_i + \Delta_i) = k, \qquad \boldsymbol{\Gamma} = \boldsymbol{0}, \tag{7.12}$$

imply (a) and (b). On the other hand, if neither of the two conditions (7.12) holds then (7.11) does not imply (a) and (b); for it is easy to see that there exists an upper case vector $\boldsymbol{R}$ such that

$$\boldsymbol{\Delta} \leqq \boldsymbol{R} \leqq \boldsymbol{\Gamma} + \boldsymbol{\Delta}, \qquad \sum R_i = \sum (\Gamma_i + \Delta_i) - 1,$$

and then the equations

$$V_i = \min (k, R_i) \qquad (1 \leqq i \leqq r)$$

define a solution $\boldsymbol{V}$ of (7.10) distinct from $\boldsymbol{\Gamma} + \boldsymbol{\Delta}$.

It follows that $N_k(G) = N_k(B)$ if, and only if, the conditions

$$\Delta_1 \leqq k < \sum (\Gamma_i + \Delta_i), \qquad \boldsymbol{\Gamma} \neq \boldsymbol{0},$$

imply that $N_{\boldsymbol{\gamma},\boldsymbol{\Delta}}(\mathscr{G}) = 0$. This is precisely the condition for equality stated in (7.8).

(7.13) *$n_k(G) \leqq n_k(B)$, with equality if, and only if, every subgroup H of G which satisfies $\sum D_i(\mathscr{H}) \leqq k$ has order $\leqq p^k$.*

Thus, the conditions for equality in (7.8) and (7.13) are

$$\Delta_1 \leqq k < \sum (\Gamma_i + \Delta_i) \text{ and } \boldsymbol{\Gamma} \neq \boldsymbol{0} \Rightarrow N_{\boldsymbol{\gamma},\boldsymbol{\Delta}} = 0,$$

$$\sum \Delta_i \leqq k < \sum (\Gamma_i + \Delta_i) \Rightarrow N_{\boldsymbol{\gamma},\boldsymbol{\Delta}} = 0,$$

respectively. Obviously, the equality $N_k(G) = N_k(B)$ implies the equality $n_k(G) = n_k(B)$. We omit the proof of (7.13), which is similar to that of (7.8).

(7.14) *The number of subgroups of G which can be generated by k elements cannot exceed the number of subgroups of B which can be generated by k elements. Each of the following is a necessary and sufficient condition for equality:*
(i) *$n_\lambda(G) = n_\lambda(B)$ $(\lambda = 1, \cdots, k-1)$ and $N_k(G) = N_k(B)$;*
(ii) *every subgroup of G which can be generated by k elements has zero type with respect to $\mathscr{G}$.*

This follows easily from the results above and the fact that the number of subgroups of G which can be generated by k elements is $\sum_{\lambda=0}^{k-1} n_\lambda(G) + N_k(G)$. The next result is an immediate consequence.

(7.15) *The following conditions are equivalent:*
(i) *$n_k(G) = n_k(B)$ for all k;*
(ii) *$N_k(G) = N_k(B)$ for all k;*
(iii) *$n(G) = n(B)$;*
(iv) *every subgroup of G has zero type with respect to $\mathscr{G}$.*

Together with (6.12), these results give

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

(7.16) *Suppose that $p > 3$ or that G is regular. Then the following conditions are equivalent:*

(i) *the total number of subgroups of G equals the total number of subgroups of B;*

(ii) *the number of subgroups of G which can be generated by 2 elements equals the number of subgroups of B which can be generated by 2 elements;*

(iii) *$\mathscr{G}$ is an Ω-series of G and G is lattice-isomorphic to B.*

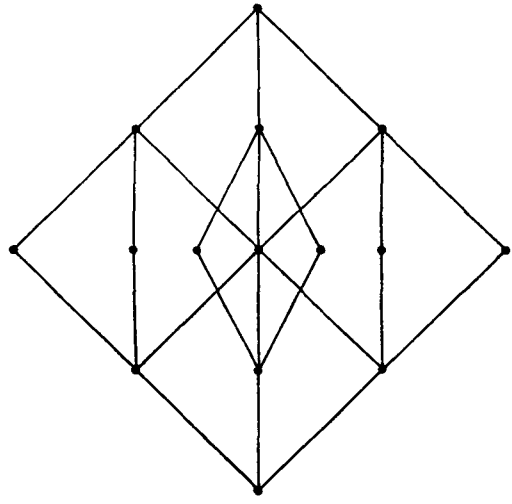

Fig. 1(a)

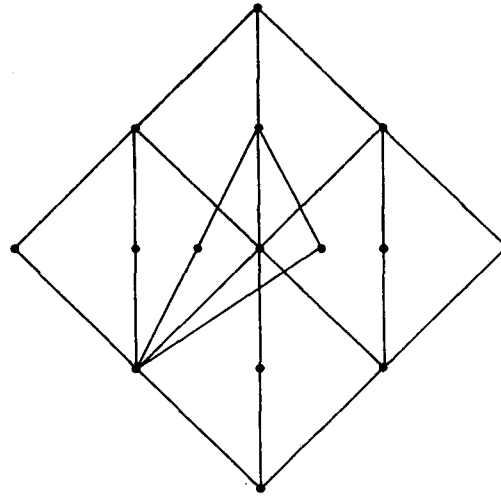

Fig. 1(b)

The subgroup lattices in figures 1, 2 show that (7.16) (i) does not imply (7.16) (iii) when G is a non-regular 2- or 3-group. Fig. 1a is the Abelian group of type $(2^2, 2^2)$, fig. 1b the group (6.18) of order 2^4. Fig. 2a is the Abelian group of type $(3^2, 3^2)$, fig. 2b the group (6.17) of order 3^4.

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

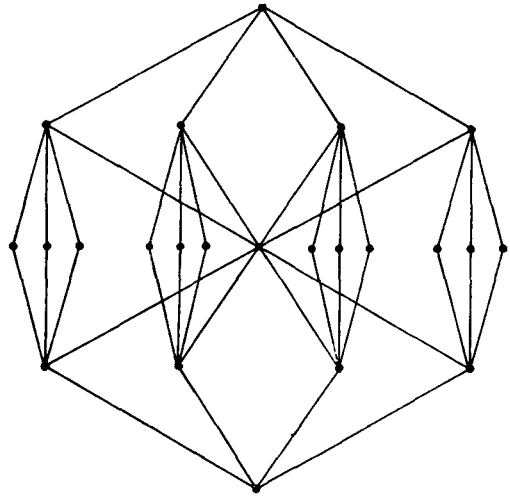

Fig. (2a)

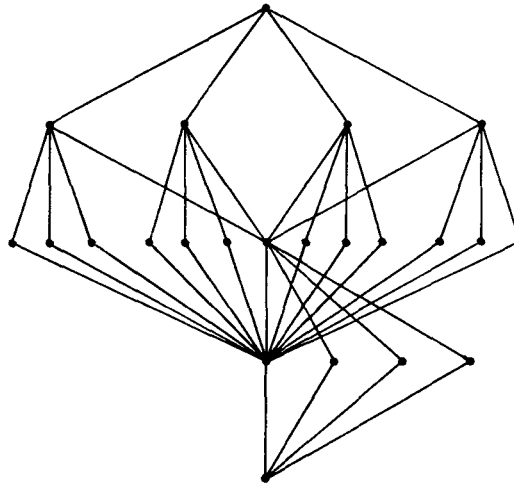

Fig. 2(b)

8. The Eulerian Polynomial of a Group of Composite Order

We end with some remarks on soluble and p-soluble groups. Let G be a group of order $p^a q^b \cdots$, where $p, q, \cdots$ are distinct primes, and let $x, y, \cdots$ be the variables in the Eulerian polynomial corresponding to $p, q, \cdots$ respectively. Let N be a normal subgroup of G of order n. By theorem 1 and induction on the group order

$$\phi(G) = \phi(G/N)\chi(x, y, \cdots),$$

where χ involves only those variables which correspond to prime divisors of n. Hence, if G be p-soluble,

https://doi.org/10.1017/S1446788700026367 Published online by Cambridge University Press

$$\phi(G) = \rho(x)\sigma(y, z, \cdots), \tag{8.1}$$

and if G be soluble,

$$\phi(G) = \rho(x)\sigma(y)\tau(z)\cdots. \tag{8.2}$$

The last result is due to W. Gaschütz ([3]).

Gaschütz's method for determining the factors $\rho, \sigma, \cdots$ when G is soluble applies equally well to determine the factor ρ when G is p-soluble. Suppose that G is p-soluble and consider the factors in a given chief series for G. Such a factor H/K is said to be *complemented* when H/K is complemented in G/K. Now, since G is p-soluble, either $|H/K|$ is prime to p or H/K is an elementary abelian p-group. In the latter case, H/K may be regarded, in the usual way, as an *irreducible* G-module; as such, it is a vector space over its *field*, E, of endomorphisms. If $|E| = p^e$ and $\dim_E (H/K) = f$, then $|H/K| = p^{ef}$.

Under the relation of G-module isomorphism, the complemented chief factors of p-power order fall into a certain number of equivalence classes, say $C_0, C_1, \cdots, C_r$. Suppose that C_0 consists of the (complemented) factors on which G acts trivially. Suppose also that C_i has k_i members and that the values of e, f corresponding to these members are e_i, f_i $(i = 0, 1, \cdots, r)$. Suppose finally that the product of the orders of the *uncomplemented* chief factors of p-power order is p^s. Then

$$\rho(x) = x^s \left(\prod_{j=0}^{k_0-1} (x - p^j)\right) \prod_{i=1}^{r} \prod_{\lambda_i=0}^{k_i-1} (x^{e_i f_i} - p^{e_i(f_i+\lambda_i)}). \tag{8.3}$$

It is easily proved that in any finite group the index of each maximal subgroup divides the order of at least one chief factor. Thus, in a p-soluble group, the index of each maximal subgroup is either a power of p or prime to p. Let $m_p(G)$ denote the number of maximal subgroups of G of p-power index (> 1), and write

$$\mu_0 = (p^{k_0} - 1)/(p - 1), \quad \mu_i = (p^{e_i(f_i+k_i)} - p^{e_i f_i})/(p^{e_i} - 1) \quad (i = 1, \cdots, r).$$

Gaschütz's method shows that

$$m_p(G) = \sum_{i=0}^{r} \mu_i; \tag{8.4}$$

and, more precisely, that the number of maximal subgroups of index p^k is

$$\sum_{e_i f_i = k} \mu_i.$$

Now, it is easily verified that

$$\mu_i \leqq p(p^{e_i f_i k_i} - 1)/(p - 1) \qquad (0 \leqq i \leqq r).$$

Therefore, since

$$\sum_{0}^{r} e_i f_i k_i = a - s \leqq a,$$

we have (for a p-soluble group G)

$$m_p(G) \leqq p(p^a - 1)/(p - 1). \tag{8.5}$$

Suppose now that G is soluble. It is easily proved that

$$p(p^a - 1)/(p - 1) + q(q^b - 1)/(q - 1) + \cdots < g$$

unless g is a prime power. Therefore, if $m(G)$ denotes the total number of maximal subgroups of G, we have

$$m(G) = m_p(G) + m_q(G) + \cdots < g. \tag{8.6}$$

It would be interesting to know whether (8.6) is valid for *all* finite groups. ((8.5) is certainly not universally true: the simple group of order 168 has 14 subgroups of index 7.)

It seems likely that every group with Eulerian polynomial of the form (8.2) is soluble, though I have not been able to prove this. The remarks which follow bear on this question.

(8.7) $p \mid |G : G'|$ *if, and only if,* $(x - 1) \mid \phi(G)$.

PROOF. If G has a normal subgroup of index p, then, by theorem 1, $(x - 1) \mid \phi(G)$. Conversely, suppose that G has no normal subgroup of index p. Then the number of groups in each conjugacy class of subgroups of p-power index is divisible by p. Comparing coefficients of $y^b z^c \cdots$ in the sum formula

$$f(G; 1, y, z, \cdots) = \sum_{H \leqq G} \phi(H; 1, y, z, \cdots),$$

we see that the coefficient of $y^b z^c \cdots$ in $\phi(G; 1, y, z, \cdots)$ is $\equiv 1 \pmod{p}$ and so $(x - 1) \nmid \phi(G)$.

(8.8) COROLLARY. *If* $\phi(G)$ *has the form* (8.2), $G' < G$.

In fact, if G is not cyclic, $\phi_1(G) = 0$. Hence one of $\rho(1), \sigma(1), \cdots$ is zero and so one of $(x - 1), (y - 1), \cdots$ divides $\phi(G)$. By (8.7), $G' < G$.

(8.9) *If* $\phi(G)$ *has the form* (8.2) *and* $\mu_G(1) \neq 0$, G *is soluble.*

In fact, since

$$\mu_G(1) = \phi(G; 0, 0, \cdots) = \rho(0)\sigma(0) \cdots,$$

the coefficients of $y^b z^c \cdots$, $x^a z^c \cdots$, in $\phi(G)$ are non-zero. Hence, by (3.2), G has subgroups of each order g/p^a, $g/q^b, \cdots$ and so, by Hall's theorem, is soluble.

References

[1] Barnes, D. W., Lattice embeddings of prime power group, D. Phil. thesis, Oxford University (1959).

[2] Delsarte, P., Fonctions de Möbius sur les groupes abéliens finis, Ann. of Math. (2) 49 (1948), 600–609.

[3] Gaschütz, W., Die Eulersche Funktion endlicher auflösbarer Gruppen, Illinois J. Maths. 3 (1959), 469—476.
[4] Hall, P., The Eulerian functions of a group, Quart. J. Maths. (Oxford Series) 7 (1936), 134—151.
[5] Hall, P., A contribution to the theory of groups of prime-power order, Proc. London Math. Soc. (2) 36 (1933), 29—95.
[6] Kinosita, Y., On the enumeration of certain subgroups of a p-group, J. Osaka Inst. Sci. Tech. Part I 1 (1949), 13—20.
[7] Lazard, M., Sur les groupes nilpotents et les anneaux de Lie, Ann. Sc. de l'École Normale Supérieure 71 (1954), 101—190, (theorem 4.6, p. 176).
[8] Suzuki, M., Structure of a group and the structure of its lattice of subgroups, Springer (1956).
[9] Weisner, L., Abstract theory of inversion of finite series, Trans. Amer. Math. Soc. 38 (1935), 474—484.
[10] Yeh, Y., On prime power abelian groups, Bull. Amer. Math. Soc. 54 (1948), 323—327.
[11] Zassenhaus, H., The theory of groups, Chelsea (1949).
[12] Kemhadze, Š. S., Soobščeniya Akad. Nauk Gruzin S.S.R. 11 (1950), 607—611.

University of Sydney.