SOME PROPERTIES OF PRIME-POWER GROUPS*

BY
LOUIS WEISNER

1. **Introduction.** I have shown in a recent paper† that inversion formulas, analogous to Dedekind's inversion formula, exist in any hierarchy. As the class of all subgroups of a finite group is a hierarchy, it is to be expected that the inversion formulas will prove useful in the theory of groups. The number of applications is at present limited because of insufficient knowledge of the generalized Möbius function, in terms of which the inversion formulas are expressed. The obstacles which present themselves in the general case do not arise in the case of prime-power groups. In the present paper I evaluate the generalized Möbius function for the hierarchy consisting of the subgroups of a prime-power group, and deduce some properties of these groups therefrom. The theorems derived, while of interest in themselves, serve to illustrate the usefulness of the inversion formulas, but by no means exhaust the list of possible applications.

2. **The inversion formulas.** Except for some obvious changes, made to conform to conventional notations of the theory of groups, I shall follow the notations of my earlier paper. For convenience of reference, I shall restate the inversion theorems and pertinent definitions.

For every pair of subgroups X_1 and X_2 of a finite group G, such that X_1 is a subgroup of X_2 (notation: X_1/X_2), the function $Q_k(X_1/X_2)$ $(k \geqq 1)$ is defined as the number of sets of k distinct maximal subgroups of X_2, such that the cross-cut of each set is X_1. The function $\mu(X_1/X_2)$ is defined by

$$\mu(X_2/X_2) = 1, \qquad \mu(X_1/X_2) = \sum_k (-1)^k Q_k(X_1/X_2) \quad (X_1 \neq X_2). \tag{1}$$

The series terminates naturally. It is not difficult to prove that if X_2 is a cyclic group, and the orders of X_1 and X_2 are x_1 and x_2 respectively, then

$$\mu(X_1/X_2) = \mu(x_2 \div x_1),$$

the function in the right member being Möbius' function.

The function $\mu(X_1/X_2)$ has the following properties:

$$\sum_{X_1/D/X_2} \mu(D/X_2) = \begin{cases} 1 \text{ if } X_1 = X_2, \\ 0 \text{ if } X_1 \neq X_2. \end{cases} \tag{2}$$

* Presented to the Society, February 23, 1935; received by the editors February 3, 1935.

† In the present issue of these Transactions, 474–484.

$$\sum_{X_1/D/X_2} \mu(X_1/D) = \begin{cases} 1 \text{ if } X_1 = X_2, \\ 0 \text{ if } X_1 \neq X_2. \end{cases} \tag{3}$$

$$\sum_{(D,X_2)=X_1} \mu(D/X_3) = 0 \qquad (X_1/X_2/X_3;\ X_2 \neq X_3). \tag{4}$$

In (2) and (3) D ranges over all subgroups of X_2 that contain X_1 (including X_1 and X_2). In (4) D ranges over all subgroups of X_3 that satisfy $(D, X_2) = X_1$, where (D, X_2) denotes the cross-cut of D and X_2.

There are two inversion formulas:

I. If Γ is a subgroup of a group G and, for every subgroup X of G that contains Γ,

$$A'(\Gamma/X) = \sum_{\Gamma/D/X} A(\Gamma/D),$$

then

$$A(\Gamma/X) = \sum_{\Gamma/D/X} \mu(D/X)A'(\Gamma/D).$$

II. If Γ is a subgroup of a group G and, for every subgroup X of Γ,

$$B'(X/\Gamma) = \sum_{X/D/\Gamma} B(D/\Gamma),$$

then

$$B(X/\Gamma) = \sum_{X/D/\Gamma} \mu(X/D)B'(D/\Gamma).$$

In the first formula, $A(\Gamma/X)$ and $A'(\Gamma/X)$ are single-valued functions of Γ and X, defined for every subgroup X of G that contains Γ. The functions are not necessarily defined for *every* subgroup Γ of G. The symbols in the second formula have similar connotations. Finally we remark that $A(\Gamma/X)$ and $B(X/\Gamma)$ may be functions of X alone, in which case they may be denoted by $A(X)$ and $B(X)$ respectively; but that the same need not necessarily be the case of the corresponding functions $A'(\Gamma/X)$ and $B'(X/\Gamma)$.

While the groups considered in subsequent sections are prime-power groups, we note at this point the following general theorem which we shall find useful.

THEOREM 1. *If X_1 is an invariant subgroup of X_2, then*

$$\mu(X_1/X_2) = \mu\left(1 \Big/ \frac{X_2}{X_1}\right).$$

(Here and elsewhere 1 denotes the identity group.)

The theorem is an immediate consequence of the definition of the function $\mu(X_1/X_2)$ and the fact that there is a one-one correspondence between

the sets of maximal subgroups of X_2 whose cross-cut is X_1 and the sets of maximal subgroups of $X_2 \div X_1$ whose cross-cut is 1.

3. **Value of $\mu(X_1/X_2)$ for a prime-power group.** We begin with the case in which $X_1 = 1$ and $X_2 = X$ is a group of order p^x (p prime). We shall write $\mu(X)$ for $\mu(1/X)$. We shall prove that

$$\mu(X) = (-1)^x p^{x(x-1)/2} \quad \text{or} \quad 0, \tag{5}$$

according as X is or is not an abelian group of type $(1, 1, 1, \cdots)$.

If X is not an abelian group of type $(1, 1, 1, \cdots)$, the cross-cut of *all* its maximal subgroups (the subgroups of index p) is not 1.* It follows from the definition that $\mu(X) = 0$.

We now suppose that X is an abelian group of type $(1, 1, 1, \cdots)$. Because of the importance of the result, two proofs of (5) follow.

First proof. For the case in which $x = 1$, (5) is an immediate consequence of

$$\sum_{D/X} \mu(D) = 0 \tag{6}$$

(see (3)), as this equation then involves only two terms and $\mu(1) = 1$. We proceed to prove (5) by induction. Suppose we have verified that if D is an abelian group of order p^d ($d < x$) and type $(1, 1, 1, \cdots)$, then $\mu(D) = (-1)^d p^{d(d-1)/2}$. An abelian group of order p^x and type $(1, 1, 1, \cdots)$ contains exactly

$$\frac{(p^x - 1) \cdots (p^{x-d+1} - 1)}{(p - 1) \cdots (p^d - 1)} \qquad (1 \leqq d \leqq x) \tag{7}$$

subgroups of order p^d, and each of them is an abelian group of type $(1, 1, 1, \cdots)$. Hence, by (6),

$$\mu(X) = -1 - \sum_{d=1}^{x-1} \frac{(p^x - 1) \cdots (p^{x-d+1} - 1)}{(p - 1) \cdots (p^d - 1)} (-1)^d p^{d(d-1)/2}. \tag{8}$$

Substituting $y = -1$ in *Cauchy's identity*†

$$\prod_{r=0}^{x-1} (1 + p^r y) = 1 + \sum_{d=1}^{x} \frac{(p^x - 1) \cdots (p^{x-d+1} - 1)}{(p - 1) \cdots (p^d - 1)} p^{d(d-1)/2} y^d, \tag{9}$$

we obtain

$$0 = 1 + \sum_{d=1}^{x} \frac{(p^x - 1) \cdots (p^{x-d+1} - 1)}{(p - 1) \cdots (p^d - 1)} (-1)^d p^{d(d-1)/2}.$$

Comparing with (8), we have (5).

* Michael Bauer, *Note sur les groupes d'order p^α*, Nouvelles Annales de Mathématiques, vol. 19 (1900), p. 510. See also Miller, Blichfeldt and Dickson, *Finite Groups*, 1916, pp. 123, 127.

† A. L. Cauchy, Oeuvres, (1), vol. 8, p. 50. The identity is valid if p is an indeterminate.

Second proof. As already noted, (5) is verified for $x=1$. We shall suppose that $x \geqq 2$. Let Y be any subgroup of order p^{x-1} of X. Taking $X_1=1$, $X_2=Y$, $X_3=X$ in (4), we have

$$\sum_{(D,Y)=1} \mu(D/X) = 0. \tag{10}$$

Aside from $D=1$, the only subgroups of X that satisfy $(D, Y)=1$ are those subgroups of order p of X that are not contained in Y. This follows from the theorem that the order of the group generated by two permutable groups equals the product of their orders divided by the order of their cross-cut. Now the number of subgroups of order p of X that are not contained in Y is

$$\frac{p^x - p^{x-1}}{p-1} = p^{x-1}.$$

Applying Theorem 1, we have by (10),

$$\mu(X) = -p^{x-1}\mu(A_{x-1}),$$

where A_{x-1} is an abelian group of order p^{x-1} and type $(1, 1, 1, \cdots)$. Again,

$$\mu(A_{x-1}) = -p^{x-2}\mu(A_{x-2}),\ \mu(A_{x-2}) = -p^{x-2}\mu(A_{x-3}),\ \cdots,$$

where A_k is an abelian group of order p^k and type $(1, 1, 1, \cdots)$. Hence, as $\mu(A_1)=-1$,

$$\mu(X) = (-p^{x-1})(-p^{x-2})\cdots(-p)(-1) = (-1)^x p^{x(x-1)/2}.$$

THEOREM 2. *Let X_1 be a subgroup of order p^{x_1} of a group X_2 of order p^{x_2} $(0 \leqq x_1 < x_2$; p prime). If X_1 is not an invariant subgroup of X_2, $\mu(X_1/X_2)=0$. If X_1 is an invariant subgroup of X_2,*

$$\mu(X_1/X_2) = (-1)^{x_2-x_1} p^{(x_2-x_1)(x_2-x_1-1)/2} \quad \textit{or} \quad 0,$$

according as $X_2 \div X_1$ is or is not an abelian group of type $(1, 1, 1, \cdots)$.

The maximal subgroups of X_2 are those of index p. They are all invariant in X_2. Hence, if X_1 is not invariant in X_2, X_1 cannot be the cross-cut of a set of maximal subgroups of X_2. It follows from the definition that $\mu(X_1/X_2)=0$.

If X_1 is an invariant subgroup of X_2, $\mu(X_1/X_2)=\mu(X_2 \div X_1)$ by Theorem 1. The value of $\mu(X_2 \div X_1)$ is given by (5), with x replaced by x_2-x_1.

4. Explicit forms of the inversion formulas. The inversion formulas of §2 may now be stated as follows:

I. If Γ is a subgroup of a group G of order p^g and, for every subgroup X of G that contains Γ,

$$A'(\Gamma/X) = \sum_{\Gamma/D/X} A(\Gamma/D),$$

then

$$A(\Gamma/X) = \sum_{r=0}^{x} (-1)^r p^{r(r-1)/2} \sum A'(\Gamma/X_{x-r}),$$

where p^x is the order of X and, in $\sum A'(\Gamma/X_i)$, X_i ranges over all invariant subgroups of order p^i of X such that $X \div X_i$ is an abelian group of type $(1, 1, 1, \cdots)$, the identity group being regarded as a limiting case of a group of this type.

II. If Γ is a subgroup of order p^γ of a group G of order p^α and, for every subgroup X of Γ,

$$B'(X/\Gamma) = \sum_{X/D/\Gamma} B(D/\Gamma),$$

then

$$B(X/\Gamma) = \sum_{r=0}^{\gamma-x} (-1)^r p^{r(r-1)/2} \sum B'(X_{x+r}/\Gamma),$$

where p^x is the order of X and, in $\sum B'(X_i/\Gamma)$, X_i ranges over all subgroups of order p^i of Γ of which X is an invariant subgroup such that $X_i \div X$ is an abelian group of type $(1, 1, 1, \cdots)$.

5. **Number of subgroups having certain properties.** We proceed to give a few applications of the inversion formulas.

THEOREM 3. *The number of subgroups of order p^s of a group of order p^α that contain a particular subgroup of order p^h is* $\equiv 1 \pmod{p}$ $(0 \leqq h \leqq s \leqq g)$.*

Let $B(X) = 1$ or 0 according as X is or is not of order p^s. Then

$$B'(X/G) = \sum_{X/D/G} B(D)$$

is the number of subgroups of order p^s of G that contain X. By the second inversion formula,

$$B(X) \equiv B'(X/G) - \sum B'(X_{x+1}/G) \pmod{p}.$$

As the theorem is trivial if $s = h$, we suppose $s > h$. Taking $X = H$ (the particular subgroup of order p^h) we have, as $B(H) = 0$,

$$B'(H/G) \equiv \sum B'(H_{h+1}/G) \pmod{p}, \tag{11}$$

where H_{h+1} ranges over all subgroups of order p^{h+1} of G that contain H. The

* When $h=0$, the theorem reduces to a well known theorem of Frobenius.

number of these subgroups is known to be $\equiv 1 \pmod{p}$; that is, the theorem is verified for $s = h+1$.

We proceed to prove the theorem by induction on $s-h$, where s is fixed; that is, we assume that $B'(K/G) \equiv 1 \pmod{p}$ if K is a subgroup of G whose order p^k satisfies $p^s > p^k > p^h$, so that $1 \leqq s-k < s-h$; and infer that $B'(H/G) \equiv 1 \pmod{p}$.

By assumption, each term of the right member of (11) is $\equiv 1 \pmod{p}$. We have seen that the number of terms is $\equiv 1 \pmod{p}$. We conclude that $B'(H/G) \equiv 1 \pmod{p}$.

THEOREM 4. *The number of non-cyclic subgroups of order p^s of a non-cyclic group of order p^g that contain a particular cyclic subgroup of order p^γ is* $\equiv 1 \pmod{p}$ $(p>2, 0 \leqq \gamma < s, 2 \leqq s \leqq g)$.*

Let Γ be the subgroup of order p^γ. Let $A(\Gamma/X) = 1$ if X is a non-cyclic group of order p^s that contains Γ, and 0 otherwise. Then

$$A'(\Gamma/X) = \sum_{\Gamma/D/X} A(\Gamma/D)$$

is the number of non-cyclic subgroups of order p^s that contain Γ. The theorem being trivial if $s = g$, we suppose $s < g$. We shall prove the theorem by induction on g, assuming that $A'(\Gamma/K) \equiv 1 \pmod{p}$ if K is a non-cyclic group of order p^k $(s < k < g)$, and proving that $A'(\Gamma/G) \equiv 1 \pmod{p}$, where G is a group of order p^g.

By the first inversion formula we have, with $X = G$,

$$A'(\Gamma/G) \equiv \sum A'(\Gamma/G_{g-1}) \pmod{p},$$

where G_{g-1} ranges over the maximal subgroups of G that contain Γ. If G_{g-1} is cyclic, $A'(\Gamma/G_{g-1}) = 0$. If G_{g-1} is non-cyclic, $A'(\Gamma/G_{g-1}) \equiv 1 \pmod{p}$, by assumption. Hence, if exactly m maximal subgroups of G contain Γ, and of these n are cyclic,

$$A'(\Gamma/G) \equiv m - n \pmod{p}.$$

If $n \geqq 1$, G contains an element of order p^{g-1}. Now there are only two types of non-cyclic groups of order p^g $(p>2, g>2)$ containing an element of order p^{g-1}. For these groups the theorem may be verified directly. We therefore suppose that $n = 0$. As $m \equiv 1 \pmod{p}$ by Theorem 3, we conclude that $A'(\Gamma/G) \equiv 1 \pmod{p}$.

---

* The special case $\gamma = 0$ was first treated by G. A. Miller. See Miller, Blichfeldt and Dickson, *Finite Groups*, p. 128.

6. **Number of sets of generators.** When Γ is the identity group, the first inversion formula may be written*

$$A(X) = \sum_{r=0}^{x} (-1)^r p^{r(r-1)/2} \sum A'(X_{x-r}), \tag{12}$$

where X_i ranges over all invariant subgroups of order p^i of X such that $X \div X_i$ is an abelian group of type $(1, 1, 1, \cdots)$. Let X' be the cross-cut of all the maximal subgroups of X; and let $p^{\nu(X)}$ be the order of $X \div X'$. It is known that X' is characterized by the fact that it is the smallest invariant subgroup of X whose corresponding quotient is an abelian group of type $(1, 1, 1, \cdots)$. It is readily proved that X' is a subgroup of every invariant subgroup of X whose corresponding quotient group is an abelian group of type $(1, 1, 1, \cdots)$. It follows from (7) that *the number of terms of* $\sum A'(X_{x-r})$ *in* (12) *is*

$$\frac{(p^\nu - 1) \cdots (p^{\nu-r+1} - 1)}{(p - 1) \cdots (p^r - 1)} \qquad (r \geqq 1, \nu = \nu(X)). \tag{13}$$

These facts are useful in applying (12).

Let X be a subgroup of order p^x of a group G of order p^g, and let $f(X)$ be the number of ordered sets of k (not necessarily distinct) elements of X that generate X. As the number of ordered sets of k elements of X is p^{kx}, and each set generates some subgroup of X,

$$p^{kx} = \sum_{D/X} f(D).$$

Applying (12) and (13), observing that

$$A'(X_{x-r}) = p^{k(x-r)},$$

and taking $X = G$, we have

$$f(G) = p^{kg} + \sum_{r=1}^{\nu-1} (-1)^r p^{r(r-1)/2} p^{k(g-r)} \frac{(p^\nu - 1) \cdots (p^{\nu-r+1} - 1)}{(p - 1) \cdots (p^r - 1)} \qquad (\nu = \nu(G)).$$

This series is easily summed with the aid of Cauchy's identity (9).

THEOREM 5. *The number of ordered sets of k (not necessarily distinct) elements of a group G of order* p^g *that generate G is*

$$p^{(g-\nu)k} \prod_{r=0}^{\nu-1} (p^k - p^r) \qquad (\nu = \nu(G)).$$

* Compare with the enumeration principle of P. Hall, *A contribution to the theory of groups of prime-power order*, Proceedings of the London Mathematical Society, vol. 36 (1933), p. 39.

This number vanishes for $k<\nu$, confirming the known fact that G cannot be generated by $<\nu(G)$ of its elements.

The next theorem is proved in a similar manner.

THEOREM 6. *The number of sets of k distinct elements of a group G of order p^σ that generate G is*

$$\binom{p^\sigma}{k}+\sum_{r=1}^{\nu-1}(-1)^r p^{r(r-1)/2}\binom{p^{\sigma-r}}{k}\frac{(p^\nu-1)\cdots(p^{\nu-r+1}-1)}{(p-1)\cdots(p^r-1)} \qquad (\nu=\nu(G)).$$

HUNTER COLLEGE OF THE CITY OF NEW YORK,
NEW YORK, N. Y.