ABSTRACT THEORY OF INVERSION OF FINITE SERIES*

BY
LOUIS WEISNER

1. Introduction. The summation of a number-theoretic function $f(n)$ over the divisors of n, and the inversion of a series of this type by means of Dedekind's inversion formula, occupy a prominent place in the elementary theory of numbers.† A similar inversion formula is valid in any system whose elements are commutative with respect to a multiplication operation with respect to which a unique factorization law holds, if every element has only a finite number of divisors: for example, primary polynomials in a field, and ideals of an algebraic field.

There are, however, systems for which a *divisor relation* may be properly defined, but for which no unique factorization law holds, and, indeed, in which no rule of multiplication may be defined, as the concept of a divisor is abstractly independent of that of multiplication. For a system of this character the extension of Dedekind's inversion formula is not obvious.

An important example is the class of all subgroups of a finite group, with "divisor" defined to mean "subgroup." The problem suggested by Dedekind's inversion formula may be stated as follows: Suppose we are given two group-theoretic functions $\alpha(G)$ and $\beta(G)$, such that

$$\beta(G) = \sum\alpha(D),$$

where D ranges over the subgroups of G. Can $\alpha(G)$ be expressed in terms of $\beta(G)$ by means of a generalized Dedekind inversion formula with the aid of a generalized Möbius function? One of the objects of this paper is to answer this question.

Instead of confining my attention to this particular question I have treated the subject abstractly, showing that an inversion formula exists in any *hierarchy* (a system satisfying the axioms of §2). A hierarchy is somewhat similar to what has been called a *dual group*,‡ an *A-Menge*,§ a

* Presented to the Society, February 23, 1935; received by the editors December 5, 1934.

† Dickson, *History of the Theory of Numbers*, vol. 1, chapter XIX.

‡ R. Dedekind, *Über Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler*, Werke, vol. 2, p. 112; *Über die von drei Moduln erzeugte Dualgruppe*, Werke, vol. 2, p. 236.

§ Fritz Klein, *Zur Theorie der abstrakten Verknüpfungen*, Mathematische Annalen, vol. 105 (1931), p. 310.

*lattice** and a structure.† These are systems which are closed with respect to two operations defined abstractly so as to have the essential properties of a greatest common divisor and a least common multiple respectively, or of a logical product and a logical sum respectively. I mention them because many examples of hierarchies will be found among those of dual groups, etc. However, inversion formulas of the type referred to do not exist in the most general type of dual groups.

2. **Hierarchy axioms.** A class H, consisting of at least one element, is a *hierarchy* with respect to a relation / if the following axioms (in which a, b, $\cdots$ denote elements of H) are satisfied:

1. The relation / is reflexive: a/a.‡
2. The relation / is asymmetric: if a/b and b/a, then $a=b$.
3. The relation / is transitive: if a/b and b/c, then a/c.
4. For every pair of elements a and b of H an element d of H exists such that d/a and d/b; and such that if c is an element of H satisfying c/a and c/b, then c/d.
5. For every pair of elements a and b of H an element l of H exists such that a/l and b/l; and such that if c is an element of H satisfying a/c and b/c, then l/c.
6. For every pair of elements a and b of H only a finite number of elements x of H exist such that $a/x/b$.

A simple example of a hierarchy is the class of all positive integers with respect to the divisor relation, so that a/b means "a is a divisor of b."§ In view of this example and the previously described purpose of this paper, the notation a/b may be read "a is a divisor of b" for any abstract hierarchy, *divisor* being regarded as an undefined term subject to the hierarchy axioms.

The converse of the relation / will be denoted by \. Thus a/b and $b\backslash a$ are equivalent. The notation $b\backslash a$ may be read "b is a *multiple* of a."

To every term defined in terms of the relation / there corresponds a *dual*, obtained by replacing / by \ in the definition. For example, *divisor* and *multiple* are duals.

We shall call the elements d and l of Axioms 4 and 5 a *greatest common divisor* and a *least common multiple* respectively of a and b. (After proving their uniqueness, we shall call them *the* g.c.d. and *the* l.c.m. respectively.) These terms are duals.

---

* Garrett Birkhoff, *On the combination of subalgebras*, Proceedings of the Cambridge Philosophical Society, vol. 29 (1933), p. 441; *On the lattice theory of ideals*, Bulletin of the American Mathematical Society, vol. 40 (1934), p. 613.

† O. Ore, *On the foundations of abstract algebra*, I, Annals of Mathematics, vol. 36 (1935), p. 408.

‡ The notation a/b means "a has the relation / to b." The notation $a/x/b$ means "a/x and x/b."

§ Other examples will be found among those given in the papers cited in §1.

If, in the hierarchy axioms, the symbol / is replaced by \, six theorems are obtained which are immediate consequences of the axioms. Hence: *A class which is a hierarchy with respect to a certain relation is also a hierarchy with respect to the converse relation.* It follows that *a true proposition is obtained on replacing each term by its dual in any theorem which is a consequence of the hierarchy axioms.* This is the principle of duality for hierarchies. For example, Axioms 4 and 5 are duals, while each of the other axioms is self-dual.

3. **The g.c.d. and l.c.m. of a set of elements.*** Let $a_1, \cdots, a_n (n \geqq 1)$ be a set of elements of a hierarchy H. If an element d of H exists such that

$$d/a_i \qquad (i = 1, \cdots, n),$$

and such that if c is an element of H satisfying

$$c/a_i \qquad (i = 1, \cdots, n),$$

then c/d, we shall call d a g.c.d. of $a_1, \cdots, a_n$. If an element l of H exists such that

$$a_i/l \qquad (i = 1, \cdots, n),$$

and such that if c is an element of H satisfying

$$a_i/c \qquad (i = 1, \cdots, n),$$

then l/c, we shall call l a l.c.m. of $a_1, \cdots, a_n$.

THEOREM 1. *A g.c.d. and a l.c.m. of any finite set of elements of a hierarchy exist and are unique elements of the hierarchy.*

In view of the principle of duality it is sufficient to prove the existence and uniqueness of a g.c.d.

The existence of a g.c.d. of a set consisting of only one element follows from Axiom 1: the element itself is a g.c.d. (as well as a l.c.m.). The existence of a g.c.d. of a set consisting of two elements is asserted by Axiom 4. We shall prove the theorem by complete induction, assuming that every set of $n-1$ $(n \geqq 3)$ elements of H has at least one g.c.d., and proving that the same is true of a given set of n elements $a_1, \cdots, a_n$.

By assumption, $a_1, \cdots, a_{n-1}$ have a g.c.d., δ. Let d be a g.c.d. of δ and a_n. As d/a_n and d/δ,

$$d/a_i \qquad (i = 1, \cdots, n),$$

by Axiom 3. Suppose that

$$c/a_i \qquad (i = 1, \cdots, n).$$

* No use is made of Axiom 6 in this section.

Writing these n statements in two parts

$$c/a_n, \quad c/a_i \qquad (i = 1, \cdots, n-1),$$

we infer that c/a_n and c/δ. Hence c/d. It follows from the definition that d is a g.c.d. of $a_1, \cdots, a_n$.

If d' is also a g.c.d. of $a_1, \cdots, a_n$, then d/d' and d'/d by the definition of g.c.d. Hence $d = d'$ by Axiom 2. The proof of the theorem is complete.

The notation $(a_1, \cdots, a_n)$ and $a_1 \wedge \cdots \wedge a_n$ will be employed for the g.c.d. and l.c.m. respectively of $a_1, \cdots, a_n$. The uniqueness part of Theorem 1 implis that the g.c.d. and l.c.m. of a set of elements are independent of the order in which these elements are taken. The following relations are readily established:

(1) $(a, a) = a \wedge a = a$.

(2) $(a_1, a_2) = (a_2, a_1)$, $a_1 \wedge a_2 = a_2 \wedge a_1$.

(3) $((a_1, \cdots, a_n), (b_1, \cdots, b_m)) = (a_1, \cdots, a_n, b_1, \cdots, b_m)$,
$(a_1 \wedge \cdots \wedge a_n) \wedge (b_1 \wedge \cdots \wedge b_m) = a_1 \wedge \cdots \wedge a_n \wedge b_1 \wedge \cdots \wedge b_m$.

(4) $a \wedge (a, b) = a$, $(a, a \wedge b) = a$.

(5) If c/a, then $(b, c)/(b, a)$ and $(b \wedge c)/(b \wedge a)$.

4. **Finite subhierarchies.** Let $\tau(x_1, x_2)$ be the number of divisors of x_2 that are multiplies of x_1. By Axiom 6, this number is finite. If x_1/x_2, we shall write $\tau(x_1/x_2)$ for $\tau(x_1, x_2)$. Evidently $\tau(x_1, x_2) = 0$ if x_1 is not a divisor of x_2; $\tau(x/x) = 1$; while $\tau(x_1/x_2) \geqq 2$ if $x_1 \neq x_2$.

A *finite* hierarchy is one which contains only a finite number elements. This number is the *order* of the hierarchy.

THEOREM 2. *If x_1/x_2, the class of all elements x of H which satisfy $x_1/x/x_2$ is a finite hierarchy, of order $\tau(x_1/x_2)$, with respect to the relation /.*

The proof is immediate, consisting principally in showing that the elements of H which satisfy $x_1/x/x_2$ verify the hierarchy axioms. We shall denote this *subhierarchy* of H by $H(x_1/x_2)$.

If x_1/x_2, but $x_1 \neq x_2$, x_1 is a *proper* divisor of x_2, and x_2 is a *proper* multiple of x_1. If x_1 is a proper divisor of x_2 and the order of the finite hierarchy $H(x_1/x_2)$ is 2, x_1 is a *maximal* divisor of x_2, and x_2 is a *minimal* multiple of x_1.

THEOREM 3. *If x_1 is a proper divisor of x_2, H contains at least one divisor of x_2 that is a minimal multiple of x_1; and H contains at least one multiple of x_1 that is a maximal divisor of x_2.*

If $\tau(x_1/x_2) = 2$, x_2 is a minimal multiple of x_1. In the contrary case $H(x_1/x_2)$

contains at least one element x_3 different from x_1 and x_2. Evidently $\tau(x_1/x_2) > \tau(x_1/x_3) \geqq 2$. If $\tau(x_1/x_3) > 2$, the preceding argument is repeated for $H(x_1/x_3)$; etc. Finally an x_n is obtained such that $\tau(x_1/x_n) = 2$. This element x_n is a divisor of x_2 and a minimal multiple of x_1.

The second part of the theorem is the dual of the first.

5. **Functions of the elements of a hierarchy.** The symbol $f(x_1/x_2)$ (and similarly $g(x_1/x_2), \cdots$) denotes a single-valued function of two independent variables, defined for every pair of elements x_1 and x_2 of a hierarchy, subject to x_1/x_2, the values which the function assumes being elements of some module. Similarly $f(a/x)$ denotes a function of a single variable x, defined for every x which is a multiple of a *fixed* element a. Dually, we have $f(x/a)$. The functions $f(a/x)$ and $f(x/a)$ are not necessarily defined for *every* a. However, for every $f(x_1/x_2)$ we have an $f(a/x)$ and an $f(x/a)$, where a is any element of the hierarchy.

The symbol

$$\sum_{x_1/x_2/\cdots/x_{n-1}/x_n}$$

pertains to a summation extended over all elements $x_2, \cdots, x_{n-1}$ of a hierarchy H satisfying $x_1/x_2/\cdots/x_{n-1}/x_n$, where x_1 and x_n are *fixed* elements of H. Hence $n \geqq 3$. In particular,

$$\sum_{a/d/b}$$

pertains to a summation extended over all elements d of H that are divisors of b and multiples of a; that is, over the elements of the finite hierarchy $H(a/b)$.

THEOREM 4. *If, for every multiple x of a,*

$$\sum_{a/d/x} f(a/d) = \sum_{a/d/x} g(a/d),$$

then $f(a/x) = g(a/x)$.

We shall prove the theorem by complete induction. For $x = a$ we have $f(a/a) = g(a/a)$. Now let b be a proper multiple of a. Suppose that we have verified that, for every multiple d of a that is a proper divisor of b, $f(a/d) = g(a/d)$. Then

$$\sum_{\substack{a/d/b \\ d \neq b}} f(a/d) = \sum_{\substack{a/d/b \\ d \neq b}} g(a/d).$$

By hypothesis,

$$\sum_{a/d/b} f(a/d) = \sum_{a/d/b} g(a/d).$$

Subtracting, we have $f(a/b) = g(a/b)$.

The dual of this theorem is

THEOREM 5. *If, for every divisor x of a,*

$$\sum_{x/d/a} f(d/a) = \sum_{x/d/a} g(d/b),$$

then $f(x/a) = g(x/a)$.

6. **The function $\mu(x_1/x_2)$ and related functions.** A *P-divisor* of an element x_2 of a hierarchy H is a divisor of x_2 that has the property P or the relation P to x_2. If x_1 is a P-divisor of x_2, x_2 is a *P'-multiple of* x_1. Examples: $P = P'$ = proper; P = maximal, P' = minimal.

Let $P(x_1/x_2)$ be the number of multiples of x_1 that are P-divisors of x_2; let $P'(x_1/x_2)$ be the number of divisors of x_2 that are P'-multiples of x_1. These functions are duals. For each integer $k \geqq 1$, let $Q_k(x_1/x_2)$ be the number of sets of k distinct elements of H that are P-divisors of x_2 and such that the g.c.d. of the elements of each set is x_1; let $Q_k'(x_1/x_2)$ be the number of sets of k distinct elements of H that are P'-multiples of x_1 and such that the l.c.m. of the elements of each set is x_2.

There are

$$\binom{P(x_1/x_2)}{k}$$

sets of k distinct elements of H that are multiples of x_1 and P-divisors of x_2. Form the g.c.d. of the elements of each set. The number of times that a particular element d of H, satisfying $x_1/d/x_2$, occurs among these g.c.d.'s is, by definition, $Q_k(d/x_2)$. Hence

$$\sum_{x_1/d/x_2} Q_k(d/x_2) = \binom{P(x_1/x_2)}{k} \qquad (k = 1, 2, \cdots). \tag{6}$$

Dualizing, we have

$$\sum_{x_1/d/x_2} Q_k'(x_1/d) = \binom{P'(x_1/x_2)}{k} \qquad (k = 1, 2, \cdots). \tag{7}$$

For the further development of the theory we find it necessary to restrict P so that

$$P(x/x) = P'(x/x) = 0, \tag{8}$$

$$P(x_1/x_2)P'(x_1/x_2) \neq 0 \qquad (x_1 \neq x_2). \tag{9}$$

These conditions are satisfied if P = proper, or P = maximal (Theorem 3). It follows from (8) that

$$Q_k(x/x) = Q_k'(x/x) = 0 \qquad (k = 1, 2, \cdots). \tag{10}$$

The function $\mu(x_1/x_2)$ is defined by

$$\mu(x/x) = 1, \tag{11}$$

$$\mu(x_1/x_2) = \sum_{k=1}^{\infty} (-1)^k Q_k(x_1/x_2) \qquad (x_1 \neq x_2). \tag{12}$$

The series involves only a finite number of terms, as

$$Q_k(x_1/x_2) = 0 \qquad (k > P(x_1/x_2)). \tag{13}$$

The dual function $\mu'(x_1/x_2)$ is defined by

$$\mu'(x/x) = 1, \tag{14}$$

$$\mu'(x_1/x_2) = \sum_{k=1}^{\infty} (-1)^k Q_k'(x_1/x_2) \qquad (x_1 \neq x_2). \tag{15}$$

It is noteworthy that $\mu(x_1/x_2)$ and $\mu'(x_1/x_2)$ *are independent of* P *if* (8) *and* (9) *are satisfied, and that* $\mu(x_1/x_2) = \mu'(x_1/x_2)$.* We proceed to prove these statements.

THEOREM 6.

$$\sum_{x_1/d/x_2} \mu(d/x_2) = \begin{cases} 1 \text{ if } x_1 = x_2, \\ 0 \text{ if } x_1 \neq x_2. \end{cases}$$

The theorem being obvious if $x_1 = x_2$, we suppose $x_1 \neq x_2$. By (12),

$$\begin{aligned} \sum_{x_1/d/x_2} \mu(d/x_2) &= \mu(x_2/x_2) + \sum_{\substack{x_1/d/x_2 \\ d \neq x_2}} \sum_{k=1}^{\infty} (-1)^k Q_k(d/x_2) \\ &= 1 + \sum_{x_1/d/x_2} \sum_{k=1}^{\infty} (-1)^k Q_k(d/x_2) \qquad \text{(by (11) and (10))} \\ &= 1 + \sum_{k=1}^{P(x_1/x_2)} (-1)^k \binom{P(x_1/x_2)}{k} \qquad \text{(by (6)),} \\ &= (1-1)^{P(x_1/x_2)} = 0 \qquad \text{(by (9)).} \end{aligned}$$

Dualizing, we have

$$\sum_{x_1/d/x_2} \mu'(x_1/d) = \begin{cases} 1 \text{ if } x_1 = x_2, \\ 0 \text{ if } x_1 \neq x_2. \end{cases} \tag{16}$$

* Consider, for example, the hierarchy, with respect to the subgroup relation, formed by the subgroups of a finite group G. If P = maximal, the equation $\mu(1/G) = \mu'(1/G)$, in which 1 stands for the identity group, embodies a relation between the maximal and the minimal subgroups of G, the minimal subgroups being those of prime order if the order of G is not a prime. This relation would be too cumbersome to be expressed in words.

It follows from Theorems 4 and 5 that the functions $\mu(x_1/x_2)$ *and* $\mu'(x_1/x_2)$ *are independent of* P *if* P *satisfies* (8) *and* (9).

Let

$$f(x_1/x_2) = \sum_{x_1/\delta/x_2} \mu(x_1/\delta).$$

Then

$$\sum_{x_1/d/x_2} f(d/x_2) = \sum_{x_1/d/\delta/x_2} \mu(d/\delta) = \sum_{x_1/\delta/x_2} \sum_{x_1/d/\delta} \mu(d/\delta).$$

Hence, by Theorem 6,

$$\sum_{x_1/d/x_2} f(d/x_2) = 1. \tag{17}$$

Let $g(x_1/x_2) = 1$ or 0 according as $x_1 = x_2$ or $x_1 \neq x_2$. Then

$$\sum_{x_1/d/x_2} g(d/x_2) = 1.$$

Comparing with (17), we have $f(x_1/x_2) = g(x_1/x_2)$ by Theorem 5. Hence, from the definitions of these functions, we have

THEOREM 7.

$$\sum_{x_1/d/x_2} \mu(x_1/d) = \begin{cases} 1 \text{ if } x_1 = x_2, \\ 0 \text{ if } x_1 \neq x_2. \end{cases}$$

Comparing with (16), we have

THEOREM 8. $\mu(x_1/x_2) = \mu'(x_1/x_2)$.

THEOREM 9. *If* $x_1/x_2/x_3$, *and* $x_2 \neq x_3$, *then*

$$\sum_{(d, x_2)=x_1} \mu(d/x_3) = 0,$$

where d *ranges over all divisors of* x_3 *that satisfy* $(d, x_2) = x_1$.

Separate the elements of the finite hierarchy $H(x_1/x_2)$ into classes, placing in the same class those elements which have the same g.c.d. with x_2. Each of these g.c.d.'s is an element of $H(x_1/x_2)$, and every element of $H(x_1/x_3)$ occurs in one and in only one of the classes. Hence, if

$$f(x_1/x_2/x_3) = \sum_{(d, x_2)=x_1} \mu(d/x_3),$$

then

$$\sum_{x_1/\delta/x_2} f(\delta/x_2/x_3) = \sum_{x_1/\delta/x_2} \sum_{(d, x_2)=\delta} \mu(d/x_3) = \sum_{x_1/d/x_3} \mu(d/x_3).$$

Hence, by Theorem 6, as $x_1 \neq x_3$,

$$\sum_{x_1/\delta/x_2} f(\delta/x_2/x_3) = 0.$$

From this equation it follows by induction, as in the proof of Theorem 4, that $f(x_1/x_2/x_3)=0$ if $x_2 \neq x_3$. The theorem follows from the definition of $f(x_1/x_2/x_3)$.

The dual of this theorem is

THEOREM 10. *If* $x_1/x_2/x_3$, *and* $x_2 \neq x_1$, *then*

$$\sum_{d \wedge x_2 = x_3} \mu(x_1/d) = 0,$$

where d ranges over all multiples of x_1 *that satisfy* $d \wedge x_2 = x_3$.

7. **Inversion formulas.** We proceed to answer in the affirmative the question raised in §1.

THEOREM 11. *If*

$$g(a/x) = \sum_{a/d/x} f(a/d),$$

then

$$f(a/x) = \sum_{a/d/x} \mu(d/x) g(a/d).$$

We have

$$\begin{aligned} \sum_{a/\delta/x} \mu(\delta/x) g(a/\delta) &= \sum_{a/d/\delta/x} \mu(\delta/x) f(a/d) \\ &= \sum_{a/d/x} \Big(\sum_{d/\delta/x} \mu(\delta/x) \Big) f(a/d) \\ &= f(a/x) \qquad \text{(by Theorem 6).} \end{aligned}$$

The dual of this theorem is

THEOREM 12. *If*

$$g(x/a) = \sum_{x/d/a} f(d/a),$$

then

$$f(x/a) = \sum_{x/d/a} \mu(x/d) g(d/a).$$

It is noteworthy that these inversion formulas are valid in any system S satisfying Axioms 1, 2, 3, and 6. In other words, there exists for such a system S a function $\mu(x_1/x_2)$ such that Theorems 11 and 12 are valid. The values assumed by this function may be calculated by induction with the aid of Theorems 6 and 7. This is clearly unsatisfactory if S is an infinite set. What is desired is a definition of the function $\mu(x_1/x_2)$ in terms of the internal struc-

ture of the system. I have been unable to provide a definition of this character without assuming Axioms 4 and 5. These axioms are verified in a sufficiently large number of important cases to warrant their inclusion in the present paper.

8. **Hierarchies containing a unit element.** *A unit element* of a hierarchy is an element which is a divisor of every element of the hierarchy. A hierarchy need not contain a unit element. For example, the class of all rational integers is a hierarchy with respect to the relation $\leqq$. The g.c.d. and l.c.m. of two elements x_1 and x_2 of this hierarchy are $\min(x_1, x_2)$ and $\max(x_1, x_2)$ respectively. The hierarchy clearly contains no unit element.

If a hierarchy contains a unit element, the number of divisors of each element of the hierarchy is finite by Axiom 6. Summations extended over all the divisors of an element are particularly important in a hierarchy having this property. Let $f(x)$ be defined for every element x of a hierarchy H containing a unit element u. Contrary to the notation of §5, we denote by

$$\sum_{d/x} f(d)$$

the sum of $f(d_1), \cdots, f(d_n)$, where $d_1, \cdots, d_n$ are the divisors of x. Define $f(u/x)$ by $f(u/x) = f(x)$. We have, by Theorem 11,

THEOREM 13. *If*

$$g(x) = \sum_{d/x} f(d),$$

then

$$f(x) = \sum_{d/x} \mu(d/x) g(d).$$

This theorem can be dualized only if H contains a *predominant* element: an element which is a multiple of every element of H and which is therefore the dual of the unit element. A hierarchy which contains a predominant element as well as a unit element is finite by Axiom 4.

For the hierarchy consisting of the positive integers, in which a/b has its usual meaning, Theorem 13 reduces to Dedekind's inversion formula; for it is readily proved from the definitions of §6 that, in this hierarchy,

$$\mu(x_1/x_2) = \mu\left(\frac{x_2}{x_1}\right),$$

the function in the right member being Möbius' function.

9. **An elementary application to the theory of groups.** The subgroups of a finite group G form a hierarchy with respect to the subgroup relation. In this

hierarchy D/G means that D is a subgroup of G. The g.c.d. and l.c.m. of two elements are their cross-cut and the group which they generate, respectively.

Let $\beta(\Gamma)$ be the number of subgroups of order n of the group Γ, where n is a fixed positive integer; and let $\alpha(\Gamma)$ be the number of pairs of distinct subgroups of order n of Γ that generate Γ. G contains exactly $\frac{1}{2}\beta(G)(\beta(G)-1)$ pairs of distinct subgroups of order n, and each pair generates some subgroup of G. Hence

$$\sum_{D/G} \alpha(D) = \tfrac{1}{2}\beta(G)(\beta(G) - 1).$$

By Theorem 13,

$$\alpha(G) = \frac{1}{2}\sum_{D/G} \mu(D/G)\beta(D)(\beta(D) - 1). \tag{18}$$

Now let $n = p^s$ be a prime-power integer. If p^s is not a divisor of the order of D, $\beta(D) = 0$; while if p^s is a divisor of the order of D, $\beta(D) \equiv 1 \pmod{p}$.* In either case,

$$\tfrac{1}{2}\beta(D)(\beta(D) - 1) \equiv 0 \pmod{p} \qquad (p > 2).$$

Hence $\alpha(G) \equiv 0 \pmod{p}$, by (18).

THEOREM 14. *If p^s $(p \neq 2)$ is a prime-power integer, the number of pairs of distinct subgroups of order p^s of a group G, that generate G, is either zero or a multiple of p.*

To obtain more important results, a detailed investigation must be made of the numerical properties of the function $\mu(D/G)$. I have completed this investigation for the case in which G is a prime-power group, obtaining the precise value of $\mu(D/G)$, and have deduced new and interesting properties of prime-power groups therefrom. These results will be communicated in a subsequent paper.

* G. Frobenius, *Verallgemeinerung des Sylowschen Satzes*, Berliner Sitzungsberichte, 1895, p. 989; Miller, Blichfeldt and Dickson, *Finite Groups*, 1916, p. 125.

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