ON FUNCTIONS ASSOCIATED WITH VAIDYANATHASWAMY'S ALGEBRA OF CLASSES MOD N

by P. KESAVA MENON, F.N.A., *Director, Joint Cipher Bureau, Ministry of Defence, R.K. Puram, New Delhi*

(Received 17 January 1970)

If C_d is the class of residues mod n having g.c.d. n/d with n then the aggregate formed by taking the sum of the residues in $C_{d'}$ with those in $C_{d''}$ contains each residue of a class C_d the same number of times. This is expressed in the form

$$C_{d'}C_{d''} = \Sigma N(d', d''; d)C_d$$

where $N(d', d''; d)$ are non-negative integers. In this paper the algebra based on the above relation is considerably generalized and properties of the associated functions are obtained by purely arithmetical methods.

§ 1. Vaidyanathaswamy (1937) has shown that if the set of residues mod n be separated into classes by putting the residues having the same g.c.d. with n into one class then these classes combine among themselves by addition in the sense that the aggregate of sums of the residues of any one class with those of another contains each element of a class the same number of times. This fact is stated in the form

$$C_iC_j = \Sigma \nu(i, j; k)C_k$$

where the summation is extended to all the classes so that the classes form the basis of an algebra which we call Vaidyanathaswamy's (1937) class algebra. The close connection between this algebra and Ramanujan's sums has been brought out by the author elsewhere (Menon 1962). The object of this paper is to extend the scope of this algebra and to generalize it. While the extension is based upon considerations of a more general group than the additive group of residues mod n and its group ring, the generalization depends purely on properties of arithmetic functions without having anything to do with groups or group rings, a fact which makes it all the more remarkable.

§ 2. Let G be the additive group of rational numbers mod 1 and let G_n be the unique cyclic subgroup of G of order n, namely, that generated by $\frac{1}{n}$ mod 1. We also define the class C_n as the set of elements of G which in their reduced form have n for denominator. Then we have obviously

$$G = \bigcup_{n=1}^{\infty} G_n$$

$$G = \bigcup_{n=1}^{\infty} C_n$$

$$G_n = \bigcup_{d|n} C_d$$

the last two set unions being disjoint.

By an aggregate of elements of G we shall mean a *finite* collection of elements of G, repetitions being allowed. The sum $A+B$ of two aggregates A, B is defined as the union of the latter into a single aggregate so that the number of times each element of G occurs in $A+B$ is the sum of the number of times it occurs in A and the number of times it occurs in B. For each natural number n, $nA = A+A+\ldots n$ times, or in other words nA is the aggregate in which the occurrence of each element of G is n times as that of its occurrence in A. By OA we shall mean the null aggregate 0 containing no elements. We shall define inclusion $A \supset B$ or $B \subset A$ to mean that every element occurs in A at least as many times as it occurs in B. If $A \supset B$ then $A-B$ is defined as the aggregate which when added to B gives A. A similar meaning is given to $\Sigma \pm A_i$ when the sum of the positive summands includes the sum of the negative summands (taken positively). Finally we define the product AB as the aggregate obtained by 'adding' each element of A to each element of B, repetitions being reckoned separately.

As per the above definitions we may write

$$G_n = \sum_{d|n} C_d \qquad \ldots\ldots\ldots\ldots\ldots \quad (2.1)$$

or, equivalently,

$$C_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) G_d \qquad \ldots\ldots\ldots\ldots\ldots \quad (2.2)$$

where $\mu(n)$ is Mobius function defined by

$$\mu(n) = \begin{cases} (-1)^k, \text{ if } n \text{ is the product of } k \geqslant 0 \text{ distinct primes} \\ 0, \text{ otherwise.} \end{cases} \quad (2.3)$$

Moreover, if $A(a)$ is the number of times the element a occurs in A, we may write

$$A = \sum_{a \in G} A(a)\{a\} \qquad \ldots\ldots\ldots\ldots\ldots \quad (2.4)$$

where $\{a\}$ is the aggregate containing the single element a, since $A(a)$ is zero except for a finite number of elements a.

Let R be the group ring of G over the field of complex numbers. Then the mapping

$$A \to \sum_{a \in G} A(a)\, a \qquad \ldots\ldots\ldots\ldots\ldots \quad (2.5)$$

is obviously an isomorphism of the set of aggregates of G into R under which the aggregate operations are preserved so that we may identify the aggregates with their images in R under the above mapping.

Now, let the character ψ^m of G defined by

$$\psi^m(a) = e^{2\pi i m a}, \quad a \in G \qquad \ldots\ldots\ldots\ldots\ldots \quad (2.6)$$

be extended to R so that we have, in particular,

$$\left.\begin{aligned} \psi^m(A) &= \sum_{a \in G} A(a)e^{2\pi i m a} \\ \psi^m(A+B) &= \psi^m(A)+\psi^m(B) \\ \psi^m(rA) &= r\psi^m(A),\ r = 0,\ 1, \ldots, \\ \psi^m(AB) &= \psi^m(A)\psi^m(B), \end{aligned}\right\} \quad \ldots \quad (2.7)$$

where A and B are any aggregates.

We define the functions $G(m, n)$ and $C(m, n)$ by

$$\left.\begin{aligned} G(m, n) = \psi^m(G_n) &= \sum_{x \bmod n} e^{2\pi i m x/n} \\ C(m, n) = \psi^m(C_n) &= \sum_{\substack{x \bmod n \\ (x, n)=1}} e^{2\pi i m x/n} \end{aligned}\right\} \quad \ldots \quad (2.8)$$

Then

$$G(m, n) = \begin{cases} n, & \text{if } n \mid m \\ 0, & \text{otherwise} \end{cases} \quad \ldots \quad (2.9)$$

and $C(m, n)$ is the Ramanujan's sum (Hardy and Wright 1960), whose value, as is well known, is given by

$$C(m, n) = \varphi(n)\mu(n/g)/\varphi(n/g) \quad \ldots \quad (2.10)$$

where $\varphi(n)$ is Euler's function representing the number of prime residues mod n and $g = (m, n)$, the g.c.d. of m and n.

Applying ψ^m to (2.1) and (2.2) we get the well-known relations satisfied by Ramanujan's sums (Hardy and Wright 1960)

$$\left.\begin{aligned} \sum_{d \mid n} C(m, d) &= G(m, n) \\ C(m, n) &= \sum_{d \mid n} \mu\left(\frac{n}{d}\right) G(m, d) \\ &= \sum_{d \mid (m,\ n)} \mu\left(\frac{n}{d}\right) d, \text{ by (2.9).} \end{aligned}\right\} \quad \ldots \quad (2.11)$$

More generally, if we have somehow established the equality of two aggregates we may apply ψ^m to both sides of the equality and get a numerical relation. The converse is also true. In fact we have, more generally, the following Lemma.

Lemma—An element $\alpha \in R$ is completely determined by its character values $\psi^m(\alpha)$ for all m.

In fact, we need show only that $\psi^m(\alpha) = 0$ for all m implies $\alpha = 0$. But this follows at once from the fact that α is contained in the group ring R_n of some subgroup G_n of G and if ψ^m is restricted to R_n then $\psi^m(\alpha) = 0$ for $m = 1, \ldots, n$ implies that $\alpha = 0$ since ψ^m $(m = 1, \ldots, n)$ are all the characters of G_n.

As application of the lemma we have the following theorem.

Theorem 1—If $n_1, \ldots, n_k$ are any natural numbers, then

$$G_{n_1} \ldots G_{n_k} = \frac{n_1 \ldots n_k}{[n_1, \ldots, n_k]} G_{[n_1, \ldots, n_k]} \quad \ldots \quad (2.12)$$

where $[n_1, \ldots, n_k]$ is the l.c.m. of $n_1, \ldots, n_k$.

PROOF: In view of Lemma 1 we need only to show that

$$G(m, n_1) \ldots G(m, n_k) = \frac{n_1 \ldots n_k}{[n_1, \ldots, n_k]} G(m, [n_1, \ldots, n_k]) \quad \ldots \quad (2.13)$$

for all m which, however, follows at once from (2.9) since both sides of (2.13) are easily seen to reduce to $n_1 \ldots n_k$ if $n_i \mid m$ $(i = 1 \ldots k)$ and to 0 otherwise.

We remark that Theorem 1 has the simple interpretation that for any reduced fraction $\frac{a}{n}$ mod 1 the number of solutions of

$$\sum_{i=1}^{k} \frac{x_i}{n_i} \equiv \frac{a}{n} \bmod 1 \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad (2.14)$$

in residues mod n_i $(i = 1, \ldots, k)$ is $\frac{n_1 \ldots n_k}{[n_1, \ldots, n_k]}$ or 0 according as n is or is not a divisor of $[n_1, \ldots, n_k]$, since the left-hand side of (2.12) is precisely the aggregate of the elements $\sum_{i=1}^{k} \frac{x_i}{n_i}$ mod 1 with x_i mod n_i $(i = 1, \ldots, k)$, and the right-hand side is, by (2.1) and (2.7), the aggregate of the elements of the form $\frac{a}{n}$ mod 1, $(a, n) = 1$, each repeated $\frac{n_1 \ldots n_k}{[n_1, \ldots, n_k]}$ times. Theorem 1 can be deduced in turn by first evaluating the number of solutions of (2.14) directly. From Theorem 1, and (2.1) and (2.2), we at once deduce the following:

Theorem 2—If $n_1, \ldots, n_k$ are any natural numbers, then

$$C_{n_1} \ldots C_{n_k} = \sum_{n \mid [n_1, \ldots, n_k]} N(n_1, \ldots, n_k;\ n) C_n$$

$$= \sum_{n=1}^{\infty} N(n_1, \ldots, n_k;\ n) C_n \quad \ldots \quad \ldots \quad \ldots \quad (2.15)$$

where

$$N(n_1, \ldots, n_k;\ n) = \sum_{\substack{d_i \mid n_i \\ n \mid [d_1, \ldots, d_k]}} \mu\left(\frac{n_1}{d_1}\right) \ldots \mu\left(\frac{n_k}{d_k}\right) \frac{d_1 \ldots d_k}{[d_1, \ldots, d_k]} . \quad \ldots \quad (2.16)$$

PROOF: The second part of the equality in (2.15) follows at once from the first by observing that the function $N(n_1, \ldots, n_k; n)$ given by (2.16) has the value 0 if n is not a divisor of $[n_1, \ldots, n_k]$ (in which case there are no terms on the right hand of (2.16)). To prove the first part we observe that by (2.2),

Theorem 1 and (2.1), we have

$$C_{n_1} \dots C_{n_k} = \sum_{d_i | n_i} \mu\left(\frac{n_1}{d_1}\right) \dots \mu\left(\frac{n_k}{d_k}\right) G_{d_1} \dots G_{d_k}$$

$$= \sum_{d_i | n_i} \mu\left(\frac{n_1}{d_1}\right) \dots \mu\left(\frac{n_k}{d_k}\right) \frac{d_1 \dots d_k}{[d_1, \dots, d_k]} G_{[d_1, \dots, d_k]}$$

$$= \sum_{d_i | n_i} \mu\left(\frac{n_1}{d_1}\right) \dots \mu\left(\frac{n_k}{d_k}\right) \frac{d_1 \dots d_k}{[d_1, \dots, d_k]} \sum_{n | [d_1, \dots, d_k]} C_n . \qquad (2.17)$$

Interchanging the order of summation in the last expression on the right-hand side of (2.17) it takes the form

$$\sum_{n | [n_1, \dots, n_k]} \left\{ \sum_{\substack{d_i | n_i \\ n | [d_1, \dots, d_k]}} \mu\left(\frac{n_1}{d_1}\right) \dots \mu\left(\frac{n_k}{d_k}\right) \frac{d_1 \dots d_k}{[d_1, \dots, d_k]} \right\} C_n$$

$$= \sum_{n | [n_1, \dots, n_k]} N(n_1, \dots, n_k ; n) C_n .$$

Hence the proof.

We could have proved Theorem 2 with a different definition of $N(n_1, \dots, n_k ; n)$ by observing that $C_{n_1} \dots C_{n_k}$ is the aggregate of the elements

$$\sum_{i=1}^{k} \frac{x_i}{n_i} \bmod 1, \; x_i \bmod n_i, \; (x_i, n_i) = 1 \; (i = 1, \dots, k). \qquad .. \qquad .. \qquad (2.18)$$

In fact, it can easily be shown that in this aggregate an element $\frac{a}{n} \bmod 1$, $(a, n) = 1$, occurs the same number of times for all a so that C_n is included completely a certain number of times without any of its elements being left over in the aggregate. Thus we get

$$C_{n_1} \dots C_{n_k} = \sum_{n=1}^{\infty} N(n_1, \dots, n_k ; n) C_n \qquad .. \qquad .. \qquad (2.19)$$

where, now, $N(n_1, \dots, n_k ; n)$ is to be interpreted as the number of solutions of the equation

$$\sum_{i=1}^{k} \frac{x_i}{n_i} \equiv \frac{1}{n} \bmod 1, \; x_i \bmod n_i, \; (x_i, n_i) = 1 \; (i = 1, \dots, k). \qquad .. \qquad (2.20)$$

Further, it is obvious that (2.20) has no solutions if n is not a divisor of $[n_1, \dots, n_k]$ from which it follows that (2.19) may also be written as

$$C_{n_1} \dots C_{n_k} = \sum_{n | [n_1, \dots, n_k]} N(n_1, \dots, n_k ; n) C_n . \qquad .. \qquad (2.21)$$

The number of solutions of (2.20) can be evaluated by first observing that if we write

$$N(n_1, \dots, n_k) = N(n_1, \dots, n_k ; 1) \qquad .. \qquad .. \qquad .. \qquad (2.22)$$

then from (2.20) it at once follows that $N(n_1, \ldots, n_k)$ is the number of solutions of

$$\sum_{i=1}^{k} \frac{x_i}{n_i} \equiv 0 \bmod 1,\ x_i \bmod n_i,\ (x_i, n_i) = 1\ (i = 1, \ldots, k). \quad \ldots \quad (2.23)$$

Next, we observe that since the number of solutions of

$$\sum_{i=1}^{k} \frac{x_i}{n_i} \equiv \frac{a}{n} \bmod 1,\ x_i \bmod n_i,\ (x_i, n_i) = 1\ (i = 1, \ldots, k) \quad \ldots \quad (2.24)$$

for any given $a \bmod n$, $(a, n) = 1$, is the same as the number of solutions of (2.20) it follows on bringing the term $\frac{a}{n}$ to the left-hand side and replacing a by $-x$ that the number of solutions of

$$\frac{x}{n} + \frac{x_1}{n_1} + \ldots + \frac{x_k}{n_k} \equiv 0 \bmod 1$$

in prime residues $x \bmod n$ and $x_i \bmod n_i$ $(i = 1, \ldots, k)$ is $\varphi(n)N(n_1, \ldots, n_k; n)$. However, this number is, by definition $N(n, n_1, \ldots, n_k)$, so that we get

$$N(n_1, \ldots, n_k;\ n) = \frac{N(n, n_1, \ldots, n_k)}{\varphi(n)}. \quad \ldots \quad \ldots \quad (2.25)$$

Thus the problem of evaluating $N(n_1, \ldots, n_k; n)$ reduces to that of the evaluation of $N(n_1, \ldots, n_k)$.

Next, we show that $N(n_1, \ldots, n_k)$ is multiplicative in the sense that

$$N(n_1 n'_1, \ldots, n_k n'_k) = N(n_1, \ldots, n_k)N(n'_1, \ldots, n'_k) \quad \ldots \quad (2.26)$$

if $(n_1, \ldots, n_k, n'_1, \ldots, n'_k) = 1$. This follows readily from the fact that if $(n, n') = 1$, then any $\frac{x}{nn'} \bmod 1$ with $(x, nn') = 1$ splits up in a unique manner into a sum $\frac{x'}{n} + \frac{x''}{n'} \bmod 1$ with $(x', n) = 1$, $(x'', n') = 1$ and vice versa so that we have

$$\sum \frac{x_i}{n_i n'_i} \equiv \sum \frac{x'_i}{n_i} + \sum \frac{x''_i}{n'_i} \bmod 1$$

which shows that the relation

$$\sum \frac{x_i}{n_i n'_i} \equiv 0 \bmod 1\ (x_i, n_i n'_i) = 1,\ x_i \bmod n_i n'_i\ (i = 1, \ldots, k) \quad (2.27)$$

is equivalent to the two separate relations

$$\left.\begin{aligned} &\sum \frac{x'_i}{n_i} \equiv 0 \bmod 1,\ (x'_i, n_i) = 1,\ x'_i \bmod n_i \\ &\sum \frac{x''_i}{n'_i} \equiv 0 \bmod 1,\ (x''_i, n'_i) = 1,\ x''_i \bmod n'_i \\ &\qquad\qquad (i = 1, \ldots, k) \end{aligned}\right\} \quad \ldots \quad \ldots \quad (2.28)$$

from which the multiplicativity of $N(n_1, \ldots, n_k)$ follows at once.

As an immediate consequence we have

$$N(n_1, \ldots, n_k) = \prod_p N(p^{\nu_1}, \ldots, p^{\nu_k}) \quad .. \quad .. \quad (2.29)$$

when $n = \prod_p p^{\nu_i}$ is the unique factorization of n into prime factors so that the evaluation of $N(n_1, \ldots, n_k)$ reduces to that of $N(p^{\nu_1}, \ldots, p^{\nu_k})$ for all primes p.

Next, we observe that $N(n_1, \ldots, n_k)$ is symmetrical in its arguments so that in evaluating $N(p^{\nu_1}, \ldots, p^{\nu_k})$ we may assume without loss of generality that

$$\nu_1 = \ldots = \nu_s (= \nu) > \nu_{s+1} \geqslant \ldots \geqslant \nu_k \ (1 \leqslant s \leqslant k). \quad .. \quad .. \quad (2.30)$$

Then $N(p^{\nu_1}, \ldots, p^{\nu_k})$ is the number of solutions of

$$\frac{x_1 + \ldots + x_s}{p^{\nu}} + \sum_{i=s+1} \frac{x_i}{p^{\nu_i}} \equiv 0 \bmod 1, \ x_i \bmod p^{\nu_i}, \ x_i \not\equiv 0 \bmod p, \ (i = 1, \ldots, k).$$

.. (2.31)

We may obviously restrict the value of x_i to the range $0 \leqslant x_i < p^{\nu_i}$ and express it in the scale of p in the form

$$x_i \equiv \sum_{j=0}^{\nu_i - 1} a_{ij} p^j, \quad 0 \leqslant a_{ij} < p \ (i = 1, \ldots, k). \quad .. \quad .. \quad (2.32)$$

The condition $x_i \not\equiv 0 \bmod p \ (i = 1, \ldots, k)$ reduces to

$$a_{i,0} \not\equiv 0 \ (i = 1, \ldots, k). \quad .. \quad .. \quad .. \quad (2.33)$$

A further necessary condition for the x_i to be a solution of (2.31) is that

$$\sum_{i=1}^{s} a_{i,0} \equiv 0 \bmod p. \quad .. \quad .. \quad .. \quad .. \quad (2.34)$$

It is easily seen that if (2.33) and (2.34) are satisfied then choosing the remaining a_{ij} for $i > 1$ arbitrarily and then choosing $a_{1,j} \ (j = 1, \ldots, \nu - 1)$ appropriately (which is always possible uniquely) we obtain a solution of (2.31). Hence it follows that the number of solutions of (2.31) is equal to

$$f(s) p^{(s-1)(\nu-1)} \prod_{i=s+1}^{k} \varphi(p^{\nu_i}) \quad .. \quad .. \quad .. \quad (2.35)$$

where $f(s)$ is the number of solutions of

$$x_1 + \ldots + x_s \equiv 0 \bmod p, \quad 0 < x_i < p. \quad .. \quad .. \quad (2.36)$$

By letting $x_2, \ldots, x_s$ range over all values from 1 to $p-1$ we at once get the recurrence relation

$$f(s) + f(s-1) = (p-1)^{s-1} \quad .. \quad .. \quad .. \quad (2.37)$$

from which, noting that $f(1) = 0$, we at once get

$$f(s) = \frac{(p-1)^s + (-1)^s (p-1)}{p}, \quad .. \quad .. \quad .. \quad (2.38)$$

It follows from (2.35) and (2.38) that

$$N(p^{\nu_1}, \ldots, p^{\nu_k}) = \frac{\{\varphi(p^\nu)\}^s}{p^\nu}\left\{\prod_{i=s+1}^{k}\varphi(p^{\nu_i})\right\}\left\{1-\frac{1}{(1-p)^{s-1}}\right\}. \quad .. \quad (2.39)$$

We may obviously write (2.39) without the restriction imposed in (2.30) in the form

$$N(p^{\nu_1}, \ldots, p^{\nu_k}) = \frac{\prod_{i=1}^{k}\varphi(p^{\nu_1})}{p^{\max(\nu_1, \ldots, \nu_k)}}\left(1-\frac{1}{(1-p)^{s-1}}\right). \quad .. \quad (2.40)$$

Thus we get

$$N(n_1, \ldots, n_k) = \frac{\prod_{i=1}^{k}\varphi(n_i)}{[n_1, \ldots, n_k]}\Pi'\left(1-\frac{1}{(1-p)^{s-1}}\right) \quad .. \quad .. \quad (2.41)$$

where s is the number of n_i $(i = 1, \ldots, k)$ which are divisible by the highest power of p dividing $[n_1, \ldots, n_k]$ and the product Π' is over all prime factors p of $[n_1, \ldots, n_k]$, so that from (2.25) and (2.41) we have, finally,

$$N(n_1, \ldots, n_k;\ n) = \frac{\prod_{i=1}^{k}\varphi(n_k)}{[n, n_1, \ldots, n_k]}\Pi'\left\{1-\frac{1}{(1-p)^{s-1}}\right\} \quad .. \quad (2.42)$$

where s is the number of numbers among $n, n_1, \ldots, n_k$ which are divisible by the highest power of p dividing $[n, n_1, \ldots, n_k]$ and Π' denotes product over all prime factors p of $[n, n_1, \ldots, n_k]$.

Comparing (2.16) and (2.42) we get the identity

$$\sum_{\substack{d_i \mid n_i \\ n \mid [d_1, \ldots, d_k]}} \mu\left(\frac{n_1}{d_1}\right)\cdots\mu\left(\frac{n_k}{d_k}\right)\frac{d_1 \ldots d_k}{[d_1, \ldots, d_k]}$$

$$= \frac{\prod_{i=1}^{k}\varphi(n_k)}{[n, n_1, \ldots, n_k]}\Pi'\left\{1-\frac{1}{(1-p)^{s-1}}\right\} \quad .. \quad (2.43)$$

where s and Π' have the same meaning as in (2.42).

We note also the following property of $N(n_1, \ldots, n_k)$:

For $1 \leqslant r \leqslant k-1$,

$$\sum_{n=1}^{\infty} N(n_1, \ldots, n_r;\ n)N(n_{r+1}, \ldots, n_k;\ n)\varphi(n) \quad .. \quad .. \quad (2.44)$$

$$= N(n_1, \ldots, n_k)$$

This follows at once from the fact that any solution of

$$\sum_{i=1}^{k}\frac{x_i}{n_i} \equiv 0 \bmod 1,\ (x_i, n_i) = 1,\ x_i \bmod n_i$$

$$(i = 1, \ldots, k)$$

corresponds to a solution of each of the equations

$$\sum_{i=1}^{r} \frac{x_i}{n_i} \equiv \frac{a}{n} \bmod 1,\ (x_i, n_i) = 1,\ x_i \bmod n_i \quad (i = 1, \ldots, r),$$

$$\sum_{i=r+1}^{k} \frac{x_i}{n_i} \equiv \frac{-a}{n} \bmod 1,\ (x_i, n_i) = 1,\ x_i \bmod n_i \quad (i = r+1, \ldots, k)$$

for some a, n with $(a, n) = 1$, and vice versa. By (2.25) we may write (2.44) also in the form

$$\sum_{n=1}^{\infty} \frac{N(n, n_1, \ldots, n_r)N(n, n_{r+1}, \ldots, n_k)}{\varphi(n)} = N(n_1, \ldots, n_k). \quad \ldots (2.45)$$

Other results of some interest are obtained by applying ψ^m to the first of the relations (2.17) and to (2.15). Thus we get

$$\begin{aligned} &C(m, n_1) \ldots C(m, n_k) \\ &= \sum_{d_i \mid n_i} \mu\left(\frac{n_1}{d_1}\right) \ldots \mu\left(\frac{n_k}{d_k}\right) \frac{d_1 \ldots d_k}{[d_1, \ldots, d_k]} G(m, [d_1, \ldots, d_k]) \\ &= \sum_{\substack{d_i \mid n_i \\ [d_1, \ldots, d_k] \mid m}} \mu\left(\frac{n_1}{d_1}\right) \ldots \mu\left(\frac{n_k}{d_k}\right) d_1 \ldots d_k \quad \ldots \quad \ldots \quad \ldots (2.46) \end{aligned}$$

and

$$\begin{aligned} &C(m, n_1) \ldots C(m, n_k) \\ &= \sum_{n \mid [n_1, \ldots, n_k]} N(n_1, \ldots, n_k; n)C(m, n) \\ &= \sum_{n=1}^{\infty} N(n_1, \ldots, n_k; n)C(m, n). \quad \ldots \quad \ldots \quad \ldots \quad \ldots (2.47) \end{aligned}$$

As particular cases of (2.47) we have

$$\sum_{n=1}^{\infty} N(n_1, \ldots, n_k; n)\varphi(n) = \varphi(n_1) \ldots \varphi(n_k), \quad \ldots \quad \ldots (2.48)$$

$$\sum_{n=1}^{\infty} N(n_1, \ldots, n_k; n)\mu(n) = \mu(n_1) \ldots \mu(n_k) \quad \ldots \quad \ldots (2.49)$$

The relation (2.47) is itself a special case of the following theorem.

Theorem 3—If $f(n)$ is any arithmetic function and $F(n) = \sum_{d \mid n} f(d)$, then

$$\begin{aligned} &\sum_{n=1}^{\infty} N(n_1, \ldots, n_k; n) f(n) \\ &= \sum_{d_i \mid n_i} \mu\left(\frac{n_1}{d_1}\right) \ldots \mu\left(\frac{n_k}{d_k}\right) \frac{d_1 \ldots d_k}{[d_1, \ldots, d_k]} F([d_1, \ldots, d_k]). \quad \ldots (2.50) \end{aligned}$$

This follows at once by multiplying both sides of (2.16) by $f(n)$ and summing over all n, where on summing the right-hand side we first change the order of summation. As a corollary to Theorem 3 we have

$$\sum_{n=1}^{\infty} N(n_1, \ldots, n_k; n)/n^s$$

$$= \sum_{d_i | n_i} \mu\left(\frac{n_1}{d_1}\right) \cdots \mu\left(\frac{n_k}{d_k}\right) \frac{d_1 \ldots d_k}{[d_1, \ldots, d_k]} \sigma_{-s}([d_1, \ldots, d_k]) \quad .. \quad (2.51)$$

where $\sigma_a(n)$ denotes the sum of the ath powers of the divisors of n.

Again, letting m in (2.46) take values from 1 to n where n is a common multiple of $n_1, \ldots, n_k$ and adding the relations so obtained we get the following theorem.

Theorem 4—If $n_i | n$ $(i = 1, \ldots, k)$, then

$$\sum_{m=1}^{n} C(m, n_1) \ldots C(m, n_k) = nN(n_1, \ldots, n_k). \quad .. \quad .. \quad (2.52)$$

In fact, we have only to observe that if $d|n$, then

$$\sum_{m=1}^{n} G(m, d) = n \quad .. \quad .. \quad .. \quad .. \quad (2.53)$$

which is an immediate consequence of (2.9).

Taking $k = 2$ in the theorem and noting that

$$N(n_1, n_2) = \begin{cases} \varphi(n_1), & \text{if } n_1 = n_2 \\ 0, & \text{if } n_1 \neq n_2. \end{cases} \quad .. \quad .. \quad .. \quad (2.54)$$

We get the following orthogonality relations:

Theorem 5—If $n_i | n$, $(i = 1, 2)$, then

$$\sum_{m=1}^{n} C(m, n_1) C(m, n_2) = \begin{cases} n\varphi(n_1), & \text{if } n_1 = n_2 \\ 0, & \text{if } n_1 \neq n_2. \end{cases} \quad .. \quad .. \quad (2.55)$$

We may restate Theorem 4 in a somewhat different form. We observe first of all that we may take $[n_1, \ldots, n_k]$ for n without loss of generality since the general case can be deduced from it by observing that the value of the term $\prod_{i=1}^{k} C(m, n_i)$ in the summation is not altered on adding any multiple of $[n_1, \ldots, n_k]$ to m so that the sum from $m = 1$ to $m = n$ is just $\frac{n}{[n_1, \ldots, n_k]}$ times the sum from $m = 1$ to $m = [n_1, \ldots, n_k]$. Next we observe that

$$\prod_{i=1}^{k} C(m, n_i) = \prod_{i=1}^{k} C(d_i, n_i) \quad .. \quad .. \quad .. \quad (2.56)$$

where

$$d_i = (m, n_i) \ (i = 1, \ldots, k). \quad .. \quad .. \quad .. \quad (2.57)$$

If, therefore, in carrying out the summation from $m = 1$ to $m = [n_1, \ldots, n_k]$ we keep $d_1, \ldots, d_k$ fixed as arbitrary divisors of $n_1, \ldots, n_k$ respectively and sum separately over all m for which (2.57) holds we get as part sum a multiple of $\prod_{i=1}^{k} C(d_i, n_i)$.

We shall presently see that this multiple is $\varphi\left(\left[\frac{n_1}{d_1}, \ldots, \frac{n_k}{d_k}\right]\right)$ or zero according as the condition:

$$([d_1, \ldots, d_k], n_i) = d_i \ (i = 1, \ldots, k) \quad .. \quad .. \quad (2.58)$$

is satisfied or is not satisfied so that Theorem 4 takes the form

$$\sum \varphi\left(\left[\frac{n_1}{d_1}, \ldots, \frac{n_k}{d_k}\right]\right) C(d_1, n_1) \ldots C(d_k, n_k) \quad .. \quad .. \quad (2.59)$$
$$= [n_1, \ldots, n_k] N(n_1, \ldots, n_k),$$

where the summation is over all divisors d_i of n_i $(i = 1, \ldots, k)$ satisfying (2.58).

We now proceed to prove the above assertion regarding the number of m's in the interval $1 \leqslant m \leqslant [n_1, \ldots, n_k]$ for which (2.57) holds. The condition (2.57) obviously implies that

$$[d_1, \ldots, d_k] \mid m$$

so that we may take

$$m = [d_1, \ldots, d_k]s, \ 1 \leqslant s \leqslant \frac{[n_1, \ldots, n_k]}{[d_1, \ldots, d_k]}. \quad .. \quad .. \quad (2.60)$$

Then (2.57) takes the form

$$\left(\frac{[d_1, \ldots, d_k]}{d_i} s, \frac{n_i}{d_i}\right) = 1 \ (i = 1, \ldots, k) \quad .. \quad .. \quad (2.61)$$

which is equivalent to the two separate conditions (2.58) and

$$\left(s, \left[\frac{n_1}{d_1}, \ldots, \frac{n_k}{d_k}\right]\right) = 1. \quad .. \quad .. \quad .. \quad (2.62)$$

But (2.58) implies that

$$[d_1, \ldots, d_k] n_i = d_i [d_1, \ldots, d_{i-1}, n_i, d_{i+1}, \ldots, d_k] \ (i = 1, \ldots, k)$$

from which it readily follows that

$$[d_1, \ldots, d_k]\left[\frac{n_1}{d_1}, \ldots, \frac{n_k}{d_k}\right] = [n_1, \ldots, n_k] \quad .. \quad .. \quad .. \quad (2.63)$$

since $d_i | n_i$ $(i = 1, \ldots, k)$. It follows that when (2.58) is satisfied the range of s in (2.60) is $1 \leqslant s \leqslant \left[\frac{n_1}{d_1}, \ldots, \frac{n_k}{d_k}\right]$. This, combined with (2.62), gives the required result.

§ 3. The results of the previous paragraphs can be generalized in a significant manner. This is because of the fact that although the formulation and derivation of these results apparently depend on the group property of G

and the definition of the product of aggregates based on it as well as on the properties of characters of the group-ring R and on the interpretation of $N(n_1, \ldots, n_k; n)$ as an enumerative function, it turns out that the entire subject can be approached from quite a different angle and in an even more general setting as we proceed to show below.

Let S be a given set whose general element we shall denote by P and let $\mathfrak{J}$ be the set of all finite aggregates of elements of S.

The characteristic function $A(p)$ of an aggregate A gives the number of occurrence of p in A. It is clear that at most a finite number of $A(p)$ are different from zero. If $A(p)$ is at most 1 for all p then we call A a *set*. The null aggregate O has the property that $O(p) = 0$ for all $p \in S$. Inclusion $A \supset B$ (or $B \subset A$) is defined by

$$A \supset B \longleftrightarrow A(p) \geqslant B(p) \text{ for all } p. \quad .. \quad .. \quad .. \quad (3.1)$$

The sum and difference of two aggregates and the product of an aggregate by a non-negative integer are defined exactly as for aggregates of elements of G but we note that there is no analogue to the product of aggregates. We note further that $\mathfrak{J}$ is a distributive lattice with lattice sum and product defined by

$$\left.\begin{aligned}(A \vee B)(p) &= \max(A(p), B(p)) \\ (A \wedge B)(p) &= \min(A(p), B(p)).\end{aligned}\right\} \quad .. \quad .. \quad .. \quad (3.2)$$

We shall write $\bigvee_{i=1}^{k} A_i$ for $A_1 \vee, \ldots, \vee A_k$ just as we write $\sum_{i=1}^{k} A_i$ for $A_1 + \ldots + A_k$. We also note that the aggregate A can be written in the form

$$A = \sum_p A(p)p. \quad .. \quad .. \quad .. \quad .. \quad (3.3)$$

A function f over $\mathfrak{J}$ with values in a given field shall be called *multiplicative* if

$$f(A+B) = f(A)f(B) \quad .. \quad .. \quad .. \quad .. \quad (3.4)$$

whenever $A \wedge B = O$. We call f *completely multiplicative* or *linear* if (3.4) holds for all A, B. More generally, we shall say that a function f of k arguments is *multiplicative* if

$$f(A_1+B_1, \ldots, A_k+B_k) = f(A_1, \ldots, A_k)f(B_1, \ldots, B_k) \quad .. \quad (3.5)$$

whenever

$$\sum_{i=1}^{k} A_i \wedge \sum_{i=1}^{k} B_i = O.$$

We shall suppose that a multiplicative function is not identically zero. It then follows readily that

$$f(O, \ldots, O) = 1 \quad .. \quad .. \quad .. \quad .. \quad (3.6)$$

and that

$$f(A_1, \ldots, A_k) = \prod_p f\{A_1(p)p, \ldots, A_k(p)p\}. \quad .. \quad .. \quad (3.7)$$

In particular for multiplicative functions of a single argument we have

$$f(O) = 1, f(A) = \prod_p f\{A(p)p\}. \quad .. \quad .. \quad .. \quad (3.8)$$

If f is linear then the second relation in (3.8) reduces further to

$$f(A) = \prod_p \{f(p)\}^{A(p)}. \quad .. \quad .. \quad .. \quad .. \quad (3.9)$$

The composite of two functions f_1, f_2 is defined by

$$(f_1 \cdot f_2)(A) = \sum_{D \subset A} f_1(A-D) f_2(D). \quad .. \quad .. \quad .. \quad (3.10)$$

It is easily seen that composition is a commutative and associative operation with unity given by

$$e(A) = \begin{cases} 1, & \text{if } A = O \\ 0, & \text{if } A \neq O. \end{cases} \quad .. \quad .. \quad .. \quad (3.11)$$

The necessary and sufficient condition for the existence of the inverse of f under composition is $f(O) \neq 0$. Thus the functions f for which $f(O)$ is not equal to zero form a commutative group under composition. It can be shown that the set of multiplicative functions forms a subgroup of the above group. If f is multiplicative we call the formal power series

$$f_p(x) = \sum_{k=0}^{\infty} f(kp) x^k$$

the generating series to the base p of f. It is easily seen that composition of multiplicative functions corresponds to the multiplication of the corresponding generating series. The inverse of f has generating series given by the formal expansion in power of x of $1/f_{(p)}(x)$.

The function E defined by

$$E(A) = 1 \text{ for all } A \in \mathfrak{J} \quad .. \quad .. \quad .. \quad (3.12)$$

is obviously multiplicative and even linear and its generating series to any base p is given by

$$E_p(x) = 1+x+x^2+ \ldots = \frac{1}{1-x}. \quad .. \quad .. \quad .. \quad (3.13)$$

More generally, if λ is any linear function then we have

$$\lambda_p(x) = 1+\lambda(p)x+\{\lambda(p)\}^2x^2+ \ldots = \frac{1}{1-\lambda(p)x}. \quad .. \quad .. \quad (3.14)$$

The Mobius function μ is defined as the inverse of E so that its generating series to any base p is

$$\mu_p(x) = 1-x. \quad .. \quad .. \quad .. \quad .. \quad (3.15)$$

It follows from (3.15) that μ is given by

$$\mu(A) = \begin{cases} (-1)^k, & \text{if } A \text{ is a set of elements,} \\ 0 \quad , & \text{if } A \text{ is not a set.} \end{cases} \quad .. \quad .. \quad (3.16)$$

As in the classical case we have the inversion formula given by the following theorem:

Theorem 6—If $F(A) = \sum_{D \subset A} f(D)$,

then $f(A) = \sum_{D \subset A} \mu(A-D)\, F(D)$, and vice versa.

PROOF: We have $F = f.\, E$ so that $f = F.\, E^{-1}$.
As a corollary we have

$$\sum_{D \subset A} \mu(D) = \begin{cases} 1, & \text{if } A = O \\ 0, & \text{if } A \neq O. \end{cases} \quad .. \quad .. \quad .. \quad (3.17)$$

Corresponding to any multiplicative function F we define the Euler function φ_f by $\varphi_f = f.\, \mu$ so that

$$\varphi_f(A) = \sum_{D \subset A} \mu(A-D) f(D). \quad .. \quad .. \quad .. \quad (3.18)$$

Then from Theorem 6 we have

$$\sum_{D \subset A} \varphi_f(D) = f(A). \quad .. \quad .. \quad .. \quad .. \quad (3.19)$$

Moreover φ_f is multiplicative with generating series given by

$$\varphi_{f_p}(x) = (1-x) f_p(x) \quad .. \quad .. \quad .. \quad .. \quad (3.20)$$

so that we have

$$\varphi_f(A) = \prod_{p \in A} \{f(A\,(p)p) - f(\overline{A(p)-1}p)\} \quad .. \quad .. \quad .. (3.21)$$

where the product is over all distinct elements $p \in A$. In particular, if f is linear, we have

$$\varphi_f(A) = \prod_{p \in A} \{(f(p))^{A(p)} - (f(p))^{A(p)-1}\} \quad .. \quad .. \quad .. \quad (3.22)$$

which may also be written in the more elegant form

$$\varphi_f(A) = f(A) \prod_{p \in A} \left\{1 - \frac{1}{f(p)}\right\}, \quad .. \quad .. \quad .. \quad (3.23)$$

if none of the $f(p)$ are zero.

Given any multiplicative function f we define the Ramanujan's sum $C_f(A, B)$ corresponding to f by

$$C_f(A, B) = \sum_{D \subset A \wedge B} \mu(B-D) f(D) \quad .. \quad .. \quad .. \quad (3.24)$$

for all $A, B \in \mathfrak{J}$. We may obviously write (3.24) also in the form

$$C_f(A, B) = \sum_{D \subset B} \mu(B-D) G_f(A, D) \quad .. \quad .. \quad .. \quad (3.25)$$

where G_f is defined by

$$G_f(A, B) = \begin{cases} f(B), & \text{if } B \subset A \\ 0, & \text{if } B \not\subset A \end{cases} \quad .. \quad .. \quad .. \quad (3.26)$$

Hence we get, by inversion,

$$\sum_{D \subset B} C_f(A, D) = G_f(A, B). \quad .. \quad .. \quad .. \quad (3.27)$$

Corresponding to Theorem 1 we have the following theorem:

Theorem 7—If $f\left(\bigvee_{i=1}^{k} B\right) \neq 0$, then

$$\prod_{i=1}^{k} G_f(A, B_i) = \frac{\prod_{i=1}^{k} f(B_i)}{f\left(\bigvee_{i=1}^{k} B_i\right)} G_f\left(\bigvee_{i=1}^{k} B_i\right). \quad .. \quad .. \quad (3.28)$$

PROOF: Both sides of (3.28) reduce to $\prod_{i=1}^{k} f(B_i)$ or zero according as $B_i \subset A$ for all i or not.

From Theorem 7 and relations (3.25) and (3.27) we get the following:

Theorem 8—If $N_f(B_1, \ldots, B_k; B)$ is defined by

$$N_f(B_1, \ldots, B_k; B) = \sum_{\substack{D_i \subset B_i \ (i=1,\ldots,k) \\ \bigvee_{i=1}^{k} D_i \supset B}} \prod_{i=1}^{k} \frac{\{\mu(B_i - D_i) f(D_i)\}}{f\left(\bigvee_{i=1}^{k} D_i\right)} \quad .. \quad (3.29)$$

then

$$\prod_{i=1}^{k} C_f(A, B_i) = \sum_{B \subset \bigvee_{i=1}^{k} B_i} N_f(B_1, \ldots, B_k; B) C_f(A, B)$$

$$= \sum_{B \in \mathfrak{I}} N_f(B_1, \ldots, B_k; B) C_f(A, B). \quad .. \quad .. \quad (3.30)$$

The proof is exactly on the lines as that of Theorem 2 and is omitted.

We note that (3.29) implies

$$N(B_1, \ldots, B_k; B) = 0 \text{ if } B \not\subset B_1 \vee \ldots \vee B_k. \quad .. \quad .. \quad (3.31)$$

We define $N_f(B_1, \ldots, B_k)$ by

$$N_f(B_1, \ldots, B_k) = N_f(B_1, \ldots, B_k; O)$$

$$= \sum_{\substack{D_i \subset B_i \\ (i=1,\ldots,k)}} \frac{\left\{\prod_{i=1}^{k} \mu(B_i - D_i) f(D_i)\right\}}{f\left(\bigvee_{i=1}^{k} D_i\right)} \quad .. \quad .. \quad (3.32)$$

Then we have the following theorem.

Theorem 9—If φ_f is the Euler function associated with the multiplicative function f, then

$$N_f(B_1, \ldots, B_k; B) \varphi_f(B) = N_f(B, B_1, \ldots, B_k). \quad .. \quad .. \quad (3.33)$$

Obviously we cannot adopt the method of proof of (2.25) here.

We need a lemma.

Lemma—If f is multiplicative, then

$$\sum_{D \subset B} \mu(B-D)\frac{f(D)}{f(D \vee A)} = \begin{cases} \dfrac{\varphi_f(B)}{f(A)}, & \text{if } B \subset A \\ 0, & \text{if } B \not\subset A \end{cases}. \quad .. \quad .. \quad (3.34)$$

PROOF: Denoting the left-hand side of (3.34) by $F(A, B)$ it is easily seen that $F(A, B)$ is a multiplicative function of two arguments and so is the function on the right-hand side of (3.34). It is, therefore, sufficient to prove (3.34) for $A = mp$, $B = np$, where m, n are non-negative integers. First, suppose that $m \geqslant n$. Then we have

$$\begin{aligned} F(mp, np) &= \sum_{r=0}^{n} \mu\{(n-r)p\}\frac{f(rp)}{f(\max(r, m)p)} \\ &= \frac{1}{f(mp)} \sum_{r=0}^{n} \mu\{(n-r)p\}f(rp) \\ &= \frac{\varphi_f(np)}{f(mp)}. \end{aligned}$$

Next, suppose that $m < n$. Then we have

$$\begin{aligned} F(mp, np) &= \sum_{r=0}^{m-1} \mu\{(n-r)p\}\frac{f(rp)}{f(mp)} \\ &\quad + \sum_{r=m}^{n} \mu\{(n-r)p\} \\ &= \sum_{r=0}^{n-m} \mu(rp) = e((n-m)p) = 0 \end{aligned}$$

since $\mu(rp) = 0$ for $r > 1$ and $e(rp) = 0$ for $r > 0$, which proves the lemma.

PROOF OF THEOREM 9: By the lemma and the definition of $N_f(B, B_1, \ldots, B_k)$ and $N_f(B_1, \ldots, B_k; B)$ we have

$$\begin{aligned} &N_f(B, B_1, \ldots, B_k) \\ &= \sum_{\substack{D_i \subset B_i \\ (i=1,\ldots,k)}} \left\{\prod_{i=1}^{k} \mu(B_i-D_i)f(D_i)\right\} \sum_{D \subset B} \frac{\mu(B-D)f(D)}{f\left\{D \vee \left(\bigvee_{i=1}^{k} D_i\right)\right\}} \\ &= \sum_{\substack{D_i \subset B_i\ (i=1,\ldots,k) \\ \bigvee_{i=1}^{k} D_i \subset B}} \left\{\prod_{i=1}^{k} \mu(B_i-D_i)f(D_i)\right\} \frac{\varphi_f(B)}{f\left(\bigvee_{i=1}^{k} D_i\right)} \\ &= \varphi_f(B)N_f(B_1, \ldots, B_k; B). \end{aligned}$$

Corollary—$N_f(B_1, \ldots, B_k) = 0$ unless

$$B_i \subset B_1 \vee \ldots \vee B_{i-1} \vee B_{i+1} \vee \ldots \vee B_k \quad (i = 1, 2, \ldots, k). \quad .. \quad (3.35)$$

This follows from the fact that $N(B_1, \ldots, B_k)$ is symmetric in its arguments so that if (3.34) does not hold for a particular i, then we have

$$N_f(B_1, \ldots, B_k) = \varphi_f(B_i) N_f(B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_k;\ B_i)$$
$$= 0$$

by (3.29) and (3.33).

We shall now obtain a product formula for $N_f(B_1, \ldots, B_k;\ B)$ analogous to (2.42).

Theorem 10—If f is multiplicative, then

$$N_f(B_1, \ldots, B_k;\ B)$$
$$= \frac{\prod_{i=1}^{k} \varphi_f(B_i)}{f\left(B \vee \left(\bigvee_{i=1}^{k} B_i\right)\right)} \Pi' \left\{1 - \left(1 - \frac{f(np)}{\varphi_f(np)}\right)^{s-1}\right\} \quad \ldots \quad (3.36)$$

where Π' denotes product over all distinct p contained in $B \vee \left(\bigvee_{i=1}^{k} B_i\right)$, n is the number of times p occurs in $B \vee \left(\bigvee_{i=1}^{k} B_i\right)$ and s is the number of $B, B_1, \ldots, B_k$ which contain p n-times.

PROOF: Firstly we observe, on taking $B = \bigvee_{i=1}^{k} B_i$ in (3.29), that

$$N_f\left(B_1, \ldots, B_k;\ \bigvee_{i=1}^{k} B_i\right)$$
$$= \frac{1}{f\left(\bigvee_{i=1}^{k} B_i\right)} \sum_{\substack{D_i \subset B_i\ (i=1,\ldots,k) \\ \bigvee_{i=1}^{k} D_i = \bigvee_{i=1}^{k} B_i}} \left\{\prod_{i=1}^{k} \mu(B_i - D_i) f(D_i)\right\} \quad \ldots \quad (3.37)$$

so that, by Theorem 9,

$$N_f\left(\bigvee_{i=1}^{k} B_i, B_1, \ldots, B_k\right)$$
$$= \frac{\varphi_f\left(\bigvee_{i=1}^{k} B_i\right)}{f\left(\bigvee_{i=1}^{k} B_i\right)} \sum_{\substack{D_i \subset B_i\ (i=1,\ldots,k) \\ \bigvee_{i=1}^{k} D_i = \bigvee_{i=1}^{k} B_i}} \prod_{i=1}^{k} \mu(B_i - D_i) f(D_i). \quad \ldots \quad (3.38)$$

Next, we observe that $N_f(B, B_1, \ldots, B_k)$ is a multiplicative function of $k+1$ arguments from which it follows that

$$N_f(B, B_1, \ldots, B_k) = \prod_p N_f(np, n_1 p, \ldots, n_k p) \quad \ldots \quad (3.39)$$

where we have written, for brevity, $n = B(p)$, $n_i = B_i(p)$, $(i = 1, \ldots, k)$. Thirdly, we note that, since $N_f(B, B_1, \ldots, B_k)$ is symmetrical in its arguments

we may suppose, in evaluating $N_f(np, n_1p, \ldots, n_kp)$, that $n \geqslant n_1 \geqslant \ldots \geqslant n_k$. To be more specific let us suppose that

$$n = n_1 = \ldots = n_{s-1} > n_s \geqslant \ldots \geqslant n_k. \qquad \ldots \quad \ldots \quad (3.40)$$

We shall first suppose that $s > 1$. Then from (3.38) we have

$$\begin{aligned} & N_f(np, n_1p, \ldots, n_kp) \\ & = \frac{\varphi_f(np)}{f(np)} \sum_{\substack{0 \leqslant r_i \leqslant n_i \ (i=1,\ldots,k) \\ \max(r_1,\ldots,r_k)=n}} \prod_{i=1}^{k} \mu(\overline{n_i - r_i}p) f(r_ip) \\ & = \frac{\varphi_f(np)}{f(np)} \left[\left\{ \sum_{r=0}^{n} \mu(\overline{n-r}\,p) f(rp) \right\}^{s-1} - \left\{ \sum_{r=0}^{n-1} (\overline{n-r}p) f(rp) \right\}^{s-1} \right] \\ & \quad \times \prod_{i=s}^{k} \varphi_f(n_ip) \\ & = \frac{\varphi_f(np)}{f(np)} [\{\varphi_f(np)\}^{s-1} - \{\varphi_f(np) - f(np)\}^{s-1}] \prod_{i=s}^{k} \varphi_f(n_ip) \\ & = \frac{\varphi_f(np) \left\{ \prod_{i=1}^{k} \varphi_f(n_ip) \right\}}{f(np)} \left\{ 1 - \left(1 - \frac{f(np)}{\varphi_f(np)} \right)^{s-1} \right\}. \qquad \ldots \quad \ldots \quad (3.41) \end{aligned}$$

Obviously, the relation (3.41) holds also for $s = 1$ since in that case both sides have the value 0. Thus we get

$$N_f(B, B_1, \ldots, B_k) = \frac{\varphi_f(B) \prod_{i=1}^{k} \varphi_f(B_i)}{f\left(B \vee \left(\bigvee_{i=1}^{k} B_i \right) \right)} \Pi' \left\{ 1 - \left(1 - \frac{f(np)}{\varphi_f(np)} \right)^{s-1} \right\} \quad \ldots \quad (3.42)$$

where Π', n, s have the meanings assigned to them in the statement of the theorem. Finally we get, from (3.42) and Theorem 9,

$$N_f(B_1, \ldots, B_k;\ B) = \frac{\prod_{i=1}^{k} \varphi_f(B_i)}{f\left(B \vee \left(\bigvee_{i=1}^{k} B_i \right) \right)} \Pi' \left\{ 1 - \left(1 - \frac{f(np)}{\varphi_f(np)} \right)^{s-1} \right\}$$

as was to be proved.

Theorem 11—If f is multiplicative, then

$$\sum_{B \in \mathfrak{Z}} N_f(B_1, \ldots, B_r;\ B) N_f(B_{r+1}, \ldots, B_k;\ B) \varphi_f(B) = N_f(B_1, \ldots, B_k). \quad (3.43)$$

PROOF: Here again the method of proof of (2.44) fails. In view of Theorem 9 we may, however, express (3.43) in a form analogous to (2.45):

$$\sum_{B \in \mathfrak{Z}} N_f(B, B_1, \ldots, B_r) N_f(B, B_{r+1}, \ldots, B_k) / \varphi_f(B) = N_f(B_1, \ldots, B_k). \quad (3.44)$$

We shall, therefore, prove the theorem in the latter form. We need a simple lemma.

Lemma—If f is multiplicative, then

$$f(A \vee B)f(A \wedge B) = f(A)f(B). \quad .. \quad .. \quad .. \quad (3.45)$$

PROOF: It may be easily verified that either side of (3.45) is a multiplicative function of two arguments so that we need only prove the relation for $A = mp$, $B = np$, where m, n are non-negative integers. However, for these values of A and B, the relation (3.45) takes the form

$$f(\max(m, n)p)\, f(\min(m, n)p) = f(mp)\, f(np)$$

which is obviously true.

Now by (3.32) the left-hand side of (3.44) is equal to

$$\sum_{B \in \mathfrak{J}} \frac{1}{\varphi_f(B)} \sum_{\substack{D_i \subset B_i \\ (i=1,\ldots,k)}} \left\{ \prod_{i=1}^{k} \mu(B_i - D_i) f(D_i) \right\} \sum_{\substack{D \subset B \\ D' \subset B}} \frac{\mu(B-D)\mu(B-D')f(D)f(D')}{f\left\{D \vee \left(\bigvee_{i=1}^{r} D_i\right)\right\} f\left\{D' \vee \left(\bigvee_{i=r+1}^{k} D_i\right)\right\}} \quad .. \quad (3.46)$$

The inner sum in (3.46) can be written as a product:

$$\left[\sum_{D \subset B} \frac{\mu(B-D)f(D)}{f\left\{D \vee \left(\bigvee_{i=1}^{r} D_i\right)\right\}} \right] \left[\sum_{D' \subset B} \frac{\mu(B-D')f(D')}{f\left\{D' \vee \left(\bigvee_{i=r+1}^{k} D_i\right)\right\}} \right]$$

which, by the lemma under Theorem 9, reduces to

$$\frac{\varphi_f^2(B)}{f\left(\bigvee_{i=1}^{r} D_i\right) f\left(\bigvee_{i=r+1}^{k} D_i\right)}, \text{ if } B \subset \left(\bigvee_{i=1}^{r} D_i\right) \wedge \left(\bigvee_{i=r+1}^{k} D_i\right)$$

and to 0 otherwise. Substituting this in (3.46) and interchanging the order of summation and using (3.19) we see that (3.46) reduces to

$$\sum_{\substack{D_i \subset B_i \\ (i=1,\ldots,k)}} \left\{ \prod_{i=1}^{k} \mu(B_i - D_i) f(D_i) \right\} \frac{f\left(\bigvee_{i=1}^{r} D_i\right) \wedge \left(\bigvee_{i=r+1}^{k} D_i\right)}{f\left(\bigvee_{i=1}^{r} D_i\right) f\left(\bigvee_{i=r+1}^{k} D_i\right)}$$

which further reduces by the above lemma to

$$\sum_{\substack{D_i \subset B_i \\ (i=1,\ldots,k)}} \prod_{i=1}^{k} \frac{\mu(B_i - D_i) f(D_i)}{f\left(\bigvee_{i=1}^{k} D_i\right)} = N_f(B_1, \ldots, B_k)$$

on taking $A = \bigvee_{i=1}^{r} D_i$ and $B = \bigvee_{i=r+1}^{k} D_i$ respectively, which completes the proof.

The generalization of Theorem 3 is straightforward and we state it without proof.

Theorem 12—If ψ is any function over $\mathfrak{J}$, then

$$\sum_{B\in\mathfrak{J}} N_f(B_1, \ldots, B_k;\ B)\psi(B) = \sum_{D_i \subset B_i} \left\{ \prod_{i=1}^{k} \frac{\mu(B_i - D_i) f(D_i)}{f\left(\bigvee_{i=1}^{k} D_i\right)} \right\} (\psi . E)\left(\bigvee_{i=1}^{k} D_i\right). \quad .. \quad (3.47)$$

Theorem 4 cannot obviously be generalized in the form in which it is stated. However, it can be generalized in its equivalent form (2.59). In fact we have the following theorem.

Theorem 13—If f is a linear function, that is, a function satisfying

$$f(A+B) = f(A)f(B)$$

for all $A, B \in \mathfrak{J}$, then

$$\sum \varphi_f\left(\bigvee_{i=1}^{k} (B_i - D_i)\right) \prod_{i=1}^{k} C_f(D_i, B_i) = f\left(\bigvee_{i=1}^{k} B_i\right) N_f(B_1, \ldots, B_k) \quad .. \quad .. \quad .. \quad (3.48)$$

where the summation on the left-hand side is over all $D_i \subset B_i$ such that

$$\left(\bigvee_{i=1}^{k} D_i\right) \vee B_j = D_j (j = 1, \ldots, k). \quad .. \quad .. \quad (3.49)$$

We remark that the theorem is not valid in that form if f is only multiplicative without being linear.

Theorem 14—If f is multiplicative, then

$$\Sigma \varphi_f\left(\bigvee_{i=1}^{k} (B_i - D_i)\right) \prod_{i=1}^{k} C_f(D_i, B_i) = \sum_{\substack{C_i \subset B_i \\ (i=1,\ldots,k)}} f\left(\bigvee_{i=1}^{k} B_i - \bigvee_{i=1}^{k} C_i\right) \left\{ \prod_{i=1}^{k} \mu(B_i - C_i) f(C_i) \right\} \quad .. \quad (3.50)$$

where the summation on the left is over all D_i satisfying (3.49).

It is clear that when f is linear then the right-hand side of (3.50) reduces to

$$f\left(\bigvee_{i=1}^{k} B_i\right) \sum_{\substack{C_i \subset B_i \\ (i=1,\ldots,k)}} \frac{\prod_{i=1}^{k} \mu(B_i - C_i) f(C_i)}{f\left(\bigvee_{i=1}^{k} C_i\right)} = f\left(\bigvee_{i=1}^{k} B_i\right) N_f(B_1, \ldots, B_k)$$

by (3.32) so that we need only prove Theorem 14.

We shall first prove a lemma.

Lemma—If f is multiplicative, then

$$\sum_{\left(\bigvee_{i=1}^{k} D_i\right)\wedge B_j = D_j \supseteq C_j \atop (j=1,\ldots,k)} \varphi_f\left(\bigvee_{i=1}^{k}(B_i - D_i)\right) = f\left(\bigvee_{i=1}^{k} B_i - \bigvee_{i=1}^{k} C_i\right). \quad \ldots (3.51)$$

PROOF: We observe that both sides of (3.51) are multiplicative. To be more precise, if $B_i = B'_i + B''_i$, where $B'_i \wedge B''_i = 0$ $(i = 1, \ldots, k)$, then each $D_i \subset B_i$ has a unique decomposition in the form $D_i = D'_i + D''_i$ with $D'_i \subset B'_i$, $D''_i \subset B''_i$ and each $C_i \subset D_i$ has a unique decomposition in the form $C_i = C'_i + C''_i$ with $C'_i \subset D'_i$ and $C''_i \subset D''_i$ and then the condition

$$\left(\bigvee_{i=1}^{k} D_i\right) \wedge B_j = D_j \supset C_j \quad (j = 1, \ldots . k)$$

is equivalent to the two separate conditions

$$\left(\bigvee_{i=1}^{k} D'_i\right) \wedge B'_j = D'_j \supset C'_j$$

$$\left(\bigvee_{i=1}^{k} D''_i\right) \wedge B''_j = D''_j \supset C''_j \, (j = 1, \ldots, k)$$

as may be readily verified so that, in view of the multiplicativity of φ_f, the left-hand side of (3.51) reduces to the product

$$\left\{\sum_{\left(\bigvee_{i=1}^{k} D'_i\right)\wedge B'_j = D'_j \supset C'_j \atop (j=1,\ldots,k)} \varphi_f\left(\bigvee_{i=1}^{k}(B'_i - D'_i)\right)\right\}\left\{\sum_{\left(\bigvee_{i=1}^{k} D''_i\right)\wedge B''_j \supset C''_j \atop (j=1,\ldots,k)} \varphi_f\left(\bigvee_{i=1}^{k}(B''_i - D''_i)\right)\right\}$$

and likewise, in view of the multiplicativity of f, the right-hand side reduces to the product

$$f\left(\bigvee_{i=1}^{k} B'_i - \bigvee_{i=1}^{k} C'_i\right) f\left(\bigvee_{i=1}^{k} B''_i - \bigvee_{i=1}^{k} C''_i\right).$$

It follows that we need prove (3.51) only on the assumption that B_i, D_i, C_i $(i = 1, \ldots, k)$ are all multiples of a single element $p \in S$. Let, therefore,

$$B_i = b_i p, \; D_i = d_i p, \; C_i = c_i p \; (i = 1, \ldots, k). \quad \ldots \quad \ldots (3.52)$$

Then the left-hand side of (3.51) takes the form

$$\Sigma \varphi_f \left\{ \max_{1 \leqslant i \leqslant k} (b_i - d_i) p \right\} \quad \ldots \quad \ldots \quad \ldots (3.53)$$

where the summation is over all $d_i \leqslant b_i$ such that

$$\min \left\{ \max_{1 \leqslant i \leqslant k} d_i, \, b_j \right\} = d_j \geqslant c_j \; (j = 1, \ldots, k). \quad \ldots \quad \ldots (3.54)$$

Moreover, in view of symmetry, we may suppose without loss of generality that

$$b_1 \geqslant \ldots \geqslant b_k. \qquad \ldots\ldots\ldots\ldots \quad (3.55)$$

Denoting $\max d_i$ by d it at once follows from (3.54) that

$$1 \leqslant i \leqslant k$$

$d_i = b_i$ or d $(i = 1, \ldots, k)$. Hence either $d_i = b_i$ for all i or there exists an r such that

$$d_i = d < b_r \ (i = 1, \ldots, r)$$

$$d \geqslant b_i = d_i \ (i = r+1, \ldots, k).$$

Hence the sum (3.53) may be written as

$$\begin{aligned} 1 + \sum_{r=1}^{k} \sum_{\max(c_1, \ldots, c_r,\, b_r+1, \ldots, b_k) \leqslant d < b_r} & \varphi_f \left\{ \max_{1 \leqslant i \leqslant r} (b_i - d)p \right\} \\ &= \sum_{\substack{\max c_i < d < b_1 \\ 1 \leqslant i \leqslant k}} \varphi_f((b_1 - d)p) \\ &= \sum_{\substack{0 \leqslant d \leqslant b_1 - \max c_i \\ 1 \leqslant i \leqslant k}} \varphi_f(dp) \\ &= f\left\{ (\max_{1 \leqslant i \leqslant k} b_i = \max_{1 \leqslant i \leqslant k} c_i)p \right\} \end{aligned}$$

as was to be proved.

PROOF OF THEOREM 14. By (3.24) the left-hand side of (3.50) is equal to

$$\Sigma \varphi_f\left(\bigvee_{i=1}^{k} (B_i - D_i) \right) \sum_{\substack{c_i \subset D_i \\ (i = 1, \ldots, k)}} \left\{ \prod_{i=1}^{k} \mu(B_i - C_i) f(C_i) \right\} \qquad \ldots (3.56)$$

where the first summation is over all D_i satisfying (3.49). Interchanging the order of summation (3.56) may be written as

$$\begin{aligned} \sum_{C_i \subset B_i} \left\{ \prod_{i=1}^{k} \mu(B_i - C_i) f(C_i) \right\} & \sum_{C_i \subset D \subset B_i} \varphi_f \left\{ \bigvee_{i=1}^{k} (B_i - D_i) \right\} \\ & \left(\bigvee_{i=1}^{k} D_i \right) \wedge B_j = D_j \ (j = 1, \ldots, k) \\ = \sum_{\substack{C_i \subset B_i \\ (i = 1, \ldots, k)}} & f\left\{ \bigvee_{i=1}^{k} B_i - \bigvee_{i=1}^{k} C_i \right\} \left\{ \prod_{i=1}^{k} \mu(B_i - C_i) f(C_i) \right\}, \end{aligned}$$

by the lemma, which completes the proof.

We remark that in the left-hand sides of (3.48), (3.50) and (3.51) the argument $\bigvee_{i=1}^{k} (B_i - D_i)$ of φ_f may be replaced by $\bigvee_{i=1}^{k} B_i - \bigvee_{i=1}^{k} D_i$. In fact,

from (3.49) which holds in all the three cases and (3.2) we get

$$\left(\bigvee_{i=1}^{k} D_i\right)+B_j = D_j+\left\{\left(\bigvee_{i=1}^{k} D_i\right)\vee B_j\right\} \quad (j=1,\ldots,k)$$

which may be written in the form

$$\left(\bigvee_{i=1}^{k} D_i\right)+B_j-D_j = \left(\bigvee_{i=1}^{k} D_i\right)\vee B_j \quad (j=1,\ldots,k)$$

from which it at once follows that

$$\left(\bigvee_{i=1}^{k} D_i\right)+\bigvee_{j=1}^{k}(B_j-D_j) = \left(\bigvee_{i=1}^{k} D_i\right)\vee\left(\bigvee_{j=1}^{k} B_j\right) = \bigvee_{j=1}^{k} B_j$$

which proves our assertion.

Taking $k=2$ in (3.50) we get the orthogonality relation analogous to Theorem 5:

If f is linear then

$$\Sigma\,\varphi_f(B_1\vee B_2-D_1\vee D_2)C_f(D_1,B_1)C_f(D_2,B_2) = \begin{cases} 0 \text{ if } B_1\neq B_2, \\ f(B_1)\varphi_f(B_1), \quad \text{if } B_1=B_2 \end{cases} \quad .. \quad .. \quad .. \quad (3.57)$$

where the summation on the left is over all D_i such that

$$(D_1\vee D_2)\wedge B_i = D_i \quad (i=1,2).$$

PROOF: We have only to observe that

$$N_f(B_1,B_2) = \begin{cases} 0, & \text{if } B_1\neq B_2 \\ \varphi_f(B_1), & \text{if } B_1=B_2. \end{cases}$$

In fact by (3.31) and (3.33) we have $N_f(B_1,B_2)=0$ if $B_1\neq B_2$. If, on the other hand, $B_1=B_2$ then by (3.33) and (3.29) we get

$$\begin{aligned} N_f(B_1,B_2) &= \varphi_f(B_1)\sum_{B_1\subset D\subset B_1}\mu(B_1-D) \\ &= \varphi_f(B_1)\mu(O) = \varphi_f(B_1). \end{aligned}$$

We can also derive a product formula for the expression on the right-hand side of (3.50). In fact we have

Theorem 15—If f is multiplicative then

$$\sum_{\substack{C_i\subset B_i \\ (i=1,\ldots,k)}} f\left(\bigvee_{i=1}^{k} B_i-\bigvee_{i=1}^{k} C_i\right)\left\{\prod_{i=1}^{k}\mu(B_i-C_i)f(C_i)\right\}$$

$$= \left\{\prod_{i=1}^{k}\varphi_f(B_i)\right\}\prod\left\{1+(f(p)-1)\left(1-\frac{f(bp)}{\varphi(bp)}\right)^{s}\right\} \quad .. \quad .. \quad (3.58)$$

where the product is over all distinct p occurring in $\bigvee_{i=1}^{k} B_i$, b is the number of times p occurs in $\bigvee_{i=1}^{k} B_i$ and s is the number of $B_1,\ldots,B_k$ which contain p exactly b times.

PROOF: The function represented by either side of (3.58) is multiplicative, so that we may assume that $B_i = b_i p$, $C_i = c_i p$ where $0 \leqslant c_i \leqslant b_i$ $(i = 1, \ldots, k)$.

In view of symmetry we may also suppose without loss of generality that

$$b_1 = \ldots = b_r\ (= b) > b_{r+1} \geqslant \ldots \geqslant b_k.$$

Denoting $\max_{1 \leqslant i \leqslant k} c_i$ by c, the left-hand side of (3.58) reduces to

$$\sum_{\substack{0 \leqslant c_i \leqslant b_i \\ (i = 1, \ldots, k)}} f\{(b-c)p\} \prod_{i=1}^{k} \mu\{(b_i - c_i)p\} f(c_i p)$$

$$\sum_{\substack{= 0 \leqslant c_i \leqslant b_i \\ (i = 1, \ldots, k)}} f\{(b-c)p\} \prod_{i=1}^{r} \mu\{(b-c_i)p\} f(c_i p) \prod_{i=r+1}^{k} \mu\{(b_i - c_i)p\} f(c_i p) \quad \ldots \quad (3.59)$$

It is clear that only the values $c_i = b$ or $b-1$ $(i = 1, \ldots, r)$ contribute anything to the sum on the right-hand side so that in particular c may be taken to be b or $b-1$. Accordingly the right-hand side of (3.59) reduces to

$$\left[f(0) \left\{ \prod_{i=1}^{r} \sum_{c_i=0}^{b} \mu\{(b-c_i)p\} f(c_i p) - \prod_{i=1}^{r} \sum_{c_i=0}^{b-1} \mu\{(b-c_i)p\} f(c_i p) \right\} \right.$$

$$\left. + f(1) \prod_{i=1}^{r} \sum_{c_i=0}^{b-1} \mu\{(b_i - c_i)p\} f(c_i p) \right] \prod_{i=r+1}^{k} \sum_{c_i=0}^{b_i} \mu(b-c_i) f(c_i p)$$

$$= [\{\varphi_f(bp)\}^r - \{\varphi_f(bp) - f(bp)\}^r + f(1)\{\varphi_f(b) - f(b)\}^r] \prod_{i=r+1}^{k} \varphi_f(b_i p)$$

$$= \left\{ \prod_{i=1}^{k} \varphi_f(b_i p) \right\} \left[1 + \{f(1) - 1\} \left\{ 1 - \frac{f(bp)}{\varphi_f(bp)} \right\}^r \right]$$

from which the theorem follows.

REFERENCES

Hardy, G. H., and Wright, E. M. (1960). Introduction to the Theory of Numbers. Clarendon Press, Oxford.

Menon, P. Kesava (1962). On Vaidyanathaswamy's class division of the residue classes mod N. *J. Indian math. Soc.*, **26**, 167–86.

Vaidyanathaswamy, R. (1937). A remarkable property of integers mod N and its bearing on group theory. *Proc. Indian Acad. Sci.*, **5**, 63–75.