A NON-DISTRIBUTIVE CALCULUS

OF NUMERICAL FUNCTIONS

By

J. LAMBEK

Submitted in partial fulfillment of
the requirements for the degree of
Master of Science. April, 1946.

- - - - - - - - - - - - - - - - - -

I am grateful to Professors
Pall and Williams for having
initiated me into this realm
of abstraction.

TABLE OF CONTENTS.

\- - - - - - - -

§ 1. INTRODUCTION

1.1. An infinite series such as

$$\sum_{n=1}^{\infty} f(n)\, n^{-s} \qquad \text{...... (i)}$$

is called a Dirichlet series. It is completely determined by the sequence of coefficients f(n), which may be regarded as a function of n. The series (i), if convergent, is itself a function of s; as such it is called the generating function of f(n). Numerical functions which are generated by Dirichlet series are of great importance in the multiplicative theory of numbers.

If we multiply two Dirichlet series together, we obtain another series of the same type. Thus, leaving aside questions of convergence, we have:

$$\left(\sum_{n=1}^{\infty} f(n)\, n^{-s}\right)\left(\sum_{n=1}^{\infty} g(n)\, n^{-s}\right) = \sum_{n=1}^{\infty} h(n)\, n^{-s},$$

where

$$h(n) = \sum_{n=d\delta} f(d)\, g(\delta) \qquad \text{...... (ii)}$$

the latter sum extending over all the pairs of positive integers (d, δ) such that $d\delta = n$.

1.2. Instead of (ii) we shall write symbolically: h = f o g, and call o the Dirichlet operation. This turns out to be an associative and commutative operation, as will be shown in § 3, and greatly serves to simplify both statement and demonstration of many a familiar identity in the theory of numbers, as will be illustrated in a few examples. First, however, let us collect here some of the numerical functions that occur most frequently in the literature:

$\tau(n)$ . . . the number of divisors of n;

$\sigma(n)$ . . . the sum of divisors of n;

$\varphi(n)$ . . . the number of positive integers less than and prime to n;

$\mu(n)$ . . . the Moebius function, which is 0 if n contains a square other than 1, and is $(-1)^{\nu}$ if n contains ν distinct prime factors;

$\Lambda(n)$ . . . which vanishes unless n is the power of a prime p, in which case $\Lambda(n) = \log p$.

Let us abbreviate

$$\text{'}\sum_{n=d\delta} f(d)\text{'} \qquad \text{as} \qquad \text{'}\sum_{d|n} f(d)\text{'}$$

meaning that the sum extends over all the divisors of n. Of the following theorems, all but one follow immediately from the definitions; the last requires some argument, but is so well established that we need not prove it here

$$\sum_{d|n} \mu(d) = 1 \qquad \text{if } n = 1, = 0 \text{ otherwise;}$$

$$\sum_{d|n} 1 = \tau(n) \quad ;$$

$$\sum_{d|n} d = \sigma(n) \quad ;$$

$$\sum_{d|n} \Lambda(d) = \log n \quad ;$$

$$\sum_{d|n} \varphi(d) = n \quad .$$

In order to put these theorems into symbolic form, we must define a few more numerical functions of a very simple nature:

$$\epsilon(n) = 1 \qquad \text{for all } n;$$

$$\omega(n) = 1 \qquad \text{if } n = 1, = 0 \text{ otherwise;}$$

$$\eta(n) = n \quad ;$$

In our notation the above theorems then become:

<u>1.21.</u> $\epsilon \circ \mu = \omega$, $\epsilon \circ \epsilon = \tau$, $\epsilon \circ \eta = \sigma$, $\epsilon \circ \Lambda = L$, $\epsilon \circ \varphi = \eta$.

It will be noticed that w is the unit element for the Dirichlet operation o; thus f o w = f, for any numerical function f. Suppose now that f o ϵ = g. Hence, using the associative property of o, we have:

$$f = f \circ w = f \circ \epsilon \circ \mu = g \circ \mu.$$

This result, if written in non-symbolic form, constitutes, of course, the well known Moebius inversion formula. In particular, the equations in 1.21 may be inverted to give:

<u>1.22.</u> $\epsilon = \tau \circ \mu$, $\eta = \sigma \circ \mu$, $\Lambda = L \circ \mu$, $\varphi = \eta \circ \mu$

Again, if these be written out in ordinary notation, familiar results will be recognized.

It is by no means necessary to confine attention to cases where one of the operants is ϵ or μ (in these cases we have what is sometimes referred to as numerical integration and differentiation). Thus it can easily be verified algebraically that

<u>1.23.</u> $\tau \circ \varphi = \sigma$, $\sigma \circ \varphi = \eta \circ \eta$, $\eta \circ \tau = \epsilon \circ \sigma$

<u>1.3.</u> To exemplify the condensation of theory afforded by use of the Dirichlet operation o, we shall briefly consider an interesting, though well known, application to the function $[x]$ (read: greatest integer in x).

We defined g = f o ϵ to mean:

$$g(n) = \sum_{n=d\delta} f(d)\,\epsilon(\delta) = \sum_{d|n} f(d) \qquad \ldots\ldots \text{(i)}$$

Now $\left[\frac{n}{d}\right] - \left[\frac{n-1}{d}\right] = 1$ if $d \mid n$, $= 0$ if $d \nmid n$, so that (i) may be written:

$$g(n) = \sum_{d=1}^{n} \left(\left[\frac{n}{d} \right] - \left[\frac{n-1}{d} \right] \right) f(d) \qquad \ldots\ldots \text{(ii)}$$

Replacing n by k in (ii), and summing from k = 1 to k = n, we obtain the following theorem:

1.31. $$\sum_{k=1}^{n} (f \circ \epsilon)(k) = \sum_{k=1}^{n} f(k) \left[\frac{n}{k} \right].$$

An alternate way of proving this is to show that both sides can be written: $\sum_{d\delta \leq n} f(d)$.

By taking $f = \mu, \varphi, \epsilon, \eta, \Lambda$ in 1.31, we obtain:

$$\sum \mu(k) \left[\frac{n}{k} \right] = 1 \quad ;$$

$$\sum \varphi(k) \left[\frac{n}{k} \right] = \tfrac{1}{2} n(n+1) \quad ;$$

$$\sum \left[\frac{n}{k} \right] = \sum \tau(k) \quad ;$$

$$\sum k \left[\frac{n}{k} \right] = \sum \sigma(k) \quad ;$$

$$\sum_{p^s \leq n} \log p \left[\frac{n}{p^s} \right] = \log \underline{|n} \quad ;$$

identities which are frequently made use of in the analytic theory of numbers. If we put $n = \prod p^{\alpha}$, the last equation implies that:

$$\underline{|n} = \prod p^{\sum [n/p^s]}$$

whence it follows that the highest power of p in $\underline{|n}$ is $\sum_{s=1}^{\alpha} [n/p^s]$.

1.4. The matter set forth so far has been extensively discussed by various writers (e.g. Hardy and Bell). As far as we have been able to ascertain, all these authors refer to the Dirichlet operation o as a type of multiplication, presumably because it gives rise to formal multiplication of Dirichlet series. However, we shall endeavcur to show presently that the Dirichlet operation should be interpreted as a type of addition. It may be argued that it cannot possibly make any difference whether we write '$+$' or '$\cdot$' for '$\circ$', as long as we recognize the abstract properties of the operation, such as associativity and commutativity; yet terminology greatly influences our unconscious outlook, it enables us to re-interpret known theorems and to envision new ones.

If we desire to introduce (define) addition and multiplication of numerical functions (as distinct from their values), we may proceed in an "obvious" fashion. Thus we may write:

$h = f + g$ if $h(n) = f(n) + g(n)$ for all n;

$h = f \cdot g$ if $h(n) = f(n) \cdot g(n)$ for all n.

Addition thus defined has one great disadvantage: Except in rare instances (one of which will be encountered later), it serves no purpose but that of formally completing the algebraic system of numerical functions. As Prof. Bell remarks: "It is reasonable to expect nothing natural when we introduce addition, which is now done merely for completeness." If this "obvious" definition of addition is nevertheless adopted, we are forced to look at the Dirichlet operation o as a species of multiplication; for, as may easily be verified, we have a distributive law:

$$f \circ (g + h) = (f \circ g) + (f \circ h).$$

On the other hand, the "obvious" multiplication cannot be avoided, since, as later examples will show, "obvious" products of numerical functions are frequently required. Hence, if we also accept a "Dirichlet" multiplication, two species of multiplication will exist side by side, to the confusion of everybody concerned.

1.5. We shall now consider three examples that will indicate a road of escape from this muddle.

Ex. 1. We have:

$$\sum_{n=d\delta} \eta(d)\,\eta(\delta) = \sum_{d|n} d\,\frac{n}{d} = n\sum_{d|n} 1 = \eta(n)\,\tau(n),$$

or symbolically: $\eta \circ \eta = \tau\eta$. Substituting for τ, this becomes:

$$\eta \circ \eta = \eta(\epsilon \circ \epsilon).$$

Let us tentatively replace o by $+$, then

$$\eta + \eta = \eta(\epsilon + \epsilon).$$

Bearing in mind that ϵ is the unit under multiplication, we immediately recognize this as an instance of the distributive law.

Ex. 2. Again we have:

$$\sum_{n=d\delta} \eta(d)\,\mu(\delta)\,\eta(\delta) = \sum_{\delta|n} n\mu(\delta) = n\sum_{\delta|n}\mu(\delta) = n\,\omega(n) = \omega(n);$$

for w(n) vanishes unless n = 1. Symbolically:

$$\eta \circ \mu\eta = \omega.$$

If again we replace o by +, this becomes:

$$\eta + \mu\eta = \omega.$$

But w is the zero under addition, thus defined, hence we may write this tentatively:

$$-\eta = \mu\eta.$$

Now $\epsilon + \mu = \omega$, so that $\mu = -\epsilon$, whence

$$-\eta = (-\epsilon)\,\eta,$$

which again is a plausible result.

Ex. 3. Uspensky states as an example:

$$\sum_{d|n} \tau^3(d) = \Big(\sum_{d|n} \tau(d)\Big)^2$$

Symbolically this would be written: $\epsilon \circ \tau^3 = (\epsilon \circ \tau)^2$

Writing + for o, and substituting for τ, we obtain:

$$\epsilon + (\epsilon + \epsilon)^3 = (\epsilon + \epsilon + \epsilon)^2,$$

a result which reminds us of the arithmetical theorem that $1 + 2^3 = 3^2$.

1.6. Our course of action is now clear. Let us discard as useless ballast the "obvious" addition defined above, call the Dirichlet operation addition, and retain the "obvious" multiplication. This decision having been made, one question calls for immediate attention. Will the distributive law, of which we have now seen three striking instances, be true in general? If it were, we should have:

$$\mu\tau = \mu(\epsilon+\epsilon) = \mu\epsilon+\mu\epsilon = \mu+\mu \qquad \ldots\ldots \text{(i)}$$

For the argument n = 4, the L.H.S. of (i) takes the value $\mu(4)\tau(4) = 0$, whereas the R.H.S. becomes $\mu(1)\mu(4)+\mu(2)\mu(2)+\mu(4)\mu(1) = 1$. Equation (i) is, therefore, false, and we are forced to conclude: The distributive law, under which in any orthodox algebraic system, addition and multiplication enter into postulational wedlock, is absent from our calculus of numerical functions, even though many instances of it are true.

We are thus compelled to investigate a novel variant of ordinary algebra, a system in which the distributive law does not necessarily hold. In want of a better name, we shall refer to such a system, subject to certain restrictions to be enumerated in § 2, as a calculus.

§ 2. SOME ABSTRACT PROPERTIES OF CALCULI.

2.1. A set $\mathfrak{R}$ will be called a calculus with respect to two operations, which we shall call addition and multiplication, provided the following postulates are satisfied:

I. ($\mathfrak{R}$ is closed under addition.
(Addition is associative and commutative in $\mathfrak{R}$.
($\mathfrak{R}$ has an element w such that $a + w = a$ for all of a of $\mathfrak{R}$.

II. ($\mathfrak{R}$ is closed under multiplication.
(Multiplication is associative and commutative in $\mathfrak{R}$.
($\mathfrak{R}$ has an element ϵ such that $a \cdot \epsilon = a$ for all of a of $\mathfrak{R}$.

III. w as defined above has the property that $w(a + b) = wa + wb$
w for all a, b belonging to $\mathfrak{R}$.

2.11. w and ϵ are unique.

For suppose there was another element w' such that $a + w' = a$ for all a of $\mathfrak{R}$, then

$$w' = w' + w = w + w' = w.$$

Similarly ϵ is seen to be unique.

We shall call w and ϵ the zero and unity of $\mathfrak{R}$.

2.12. If a belongs to $\mathfrak{R}$, and there is an element b of $\mathfrak{R}$ such that $a + b = w$ $[ab = \epsilon]$, then b is unique.

For suppose $a + b = w$, $a + b' = w$,

then $$b' = b' + \omega = b' + a + b = \omega + b = b.$$

The same argument holds if addition is replaced by multiplication.

For a given element a of $\mathfrak{R}$, if b exists in $\mathfrak{R}$ such that $a + b = w$ $[ab = \epsilon]$, we shall call b the negative [reciprocal] of a, and we shall write $b = -a$ $[b = a^{-1}]$. Whenever convenient, we shall replace '$a+(-b)$' by '$a-b$' and '$a\,b^{-1}$' by $\frac{a}{b}$. '$-\epsilon$' will be abbreviated as μ.

Since $a+b-a-b = a-a+b-b = \omega+\omega = \omega$,

$\therefore$ $$-a-b = -(a+b),$$

and since $a+(-a)=\omega$, $\therefore$ $-(-a) = a$,

and since $\omega+\omega=\omega$, $\therefore$ $-\omega = \omega$.

Three corresponding identities may be derived for multiplication. These results can be summarized as follows:

<u>2.13.</u> Those elements of a calculus which possess negatives [reciprocals] form an Abelian group under addition [multiplication].

An element a of $\mathfrak{K}$ will be called <u>distributive</u> in $\mathfrak{K}$, if $a(b+c) = ab+ac$ for all b, c of $\mathfrak{K}$. Postulate III then simply states that w is distributive.

<u>2.14.</u> The set of distributive elements in $\mathfrak{K}$ satisfies all the postulates of an Abelian group under multiplication, except (of course) that reciprocals will only pertain to this set if they exist in $\mathfrak{K}$.

We have to prove three statements regarding closure under multiplication, unity, and the existence of admissable inverses.

If a, b are distributive elements, c, d any two elements of $\mathfrak{K}$, then $$ab\,(c+d) = a\,(bc+bd) = abc+abd,$$ hence ab is also distributive. (Closure).

Since $\epsilon(a+b) = a+b = \epsilon a+\epsilon b$, ϵ is distributive. (Unity).

If a is distributive, and a^{-1} exists in $\mathfrak{K}$, then

$$\begin{aligned} a^{-1}(b+c) &= a^{-1}(\epsilon b+\epsilon c) = a^{-1}(aa^{-1}b+aa^{-1}c) \\ &= a^{-1}a(a^{-1}b+a^{-1}c) = \epsilon(a^{-1}b+a^{-1}c) \\ &= a^{-1}b+a^{-1}c \end{aligned}$$

whence it follows that a^{-1} is distributive. (Inverse) This completes the proof of our theorem.

<u>2.2.</u> If $\mathfrak{K}$ is a calculus with zero w and unity ϵ, then a subset $\mathfrak{K}_1$ of $\mathfrak{K}$ will be called a <u>sub-calculus</u> of $\mathfrak{K}$, provided it is a calculus and contains w and ϵ. It follows that w and ϵ are also the zero and unity of $\mathfrak{K}_1$.

In a calculus $\mathfrak{K}$ it is not true in general that w a = w. However, we shall prove:

<u>2.21.</u> If $\mathfrak{K}_1$ is the set of all elements a of $\mathfrak{K}$ such that w a = w, then $\mathfrak{K}_1$ is a sub-calculus of $\mathfrak{K}$, and moreover the negative [reciprocal] of an element of $\mathfrak{K}$ will also belong to $\mathfrak{K}_1$ if it belongs to $\mathfrak{K}$.

For if a and b are in $\mathfrak{K}_1$, then

$$\omega(a+b) = \omega a + \omega b = \omega + \omega = \omega ,$$

hence $a+b$ belongs to $\mathfrak{K}_1$. (Closure under addition.)

Since $\omega\omega = \omega^2 = \omega^2 + \omega = \omega(\omega+\epsilon) = \omega\epsilon = \omega$,

therefore w belongs to $\mathfrak{K}_1$. (Zero.)

If a is in $\mathfrak{K}_1$ and -a exists in $\mathfrak{K}$ then $\omega(-a) = \omega a + \omega(-a) = \omega(a-a) = \omega^2 = \omega$

hence -a belongs to $\mathfrak{K}_1$. (Negative.)

If a and b are elements of $\mathfrak{K}_1$, then $\omega a b = \omega b = \omega$,

so that ab belongs to $\mathfrak{K}_1$. (Closure under multiplication.)

w ϵ = w. (Unity)

If a belongs to $\mathfrak{K}_1$ and a^{-1} exists in $\mathfrak{K}$, then

$$a^{-1}\omega = a^{-1}a\omega = \epsilon\omega = \omega ,$$

hence a^{-1} belongs to $\mathfrak{K}_1$. (Reciprocal.) Q.E.D.

<u>2.22.</u> A distributive element of $\mathfrak{K}$ belongs to $\mathfrak{K}_1$ if it has a negative in $\mathfrak{K}$.

For let a be distributive, then

$$a = a\epsilon = a(\epsilon+\omega) = a\epsilon + a\omega = a + a\omega . \qquad \text{......} \quad (i)$$

If $-a$ exists, add it to both sides of (i) so that

$$\omega = -a+a = -a+a+a\omega = \omega+a\omega = a\omega,$$

whence it follows that a is in $\mathfrak{K}_1$.

<u>2.23.</u> If a is distributive and possesses a negative then $-a = \mu a$. $(\mu = -\epsilon.)$

For by 2.22, w a = w, hence

$$-a = \omega - a = \omega a - a = (\epsilon+\mu)a - a$$

$$= \epsilon a + \mu a - a = \mu a + a - a = \mu a + \omega = \mu a.$$

<u>2.3.</u> A calculus $\mathfrak{K}$ will be called a <u>subtraction calculus</u> if it is closed under subtraction, i.e. if in addition to postulates I to III it satisfies the following:

IV. Every element of $\mathfrak{K}$ has a negative.

Theorems 2.22 and 2.23 then give rise to the following obvious corollary:

<u>2.31.</u> If a is a distributive element of a subtraction calculus $\mathfrak{K}$, then w a = w and $-a = \mu$ a.

It might be thought natural to define a division calculus in an analogous manner. The following theorem will show why such an attempt would yield trivial results.

<u>2.32.</u> If w has a reciprocal in $\mathfrak{K}$ then $w = \epsilon$.

For suppose there is an element a of $\mathfrak{K}$ such that w a = ϵ. By 2.21, $w^2 = w$, so that $\epsilon = \omega a = \omega^2 a = \omega(\omega a) = \omega\epsilon = \omega$.

In general, however, there is a much larger class of elements which cannot have reciprocals. We shall say that a <u>divides</u> b (or a/b) in $\mathfrak{K}$ if there is a c in $\mathfrak{K}$ such that a c = b. To say that a possesses a reciprocal is the same as stating that a/ϵ. We shall say that a is a <u>zero-divisor</u> if there is a b in $\mathfrak{K}$ such that $w \nmid b$ and $ab = w$.

<u>2.33.</u> The zero-divisors of a calculus have no reciprocals. Suppose a/ϵ. Then there exists a c in $\mathfrak{K}$ such that c a = ϵ . If b be any element of $\mathfrak{K}$ such that $ab = \omega$, then

$$b = \epsilon b = cab = c\omega ,$$

so that ω / b . Hence a cannot be a zero-divisor. Q.E.D.

The converse of this theorem is not true in general. If it is we shall speak of a <u>regular calculus</u>. Hence $\mathfrak{K}$ is a regular calculus if in addition to postulates I to III it satisfies the following:

V. Every element of $\mathfrak{K}$ is either a zero-divisor or else possesses a reciprocal in $\mathfrak{K}$.

<u>2.4.</u> It is not true in general that $(-\epsilon)(-\epsilon) = \epsilon$. Yet this would be true if the distributive law were to hold. Whenever two members of a non-distributive calculus $\mathfrak{K}$ <u>would</u> be equal under the distributive law, we shall say that they are <u>similar</u> in $\mathfrak{K}$. Unfortunately no scrutinizing logician would accept the previous statement as a definition. We shall go into some length to establish a rigorous basis for our intuitive concept of similarity.

A relation R is called an <u>equivalence-relation</u> in a calculus $\mathfrak{K}$, provided:

(1) R is transitive, symmetric, reflexive.

(2) If a, b, c are elements of $\mathfrak{K}$ such that $a R b$, then $(a+c) R (b+c)$ and $(ac) R (bc)$.

Clearly equality is a trivial equivalence relation, and so is the relation which treats all elements of $\mathfrak{K}$ as equivalent. We shall prove two simple properties of equivalence relations:

<u>2.41.</u> If R is an equivalence relation in a calculus $\mathfrak{K}$, and a, b, c, d are members of $\mathfrak{K}$ such that a R b and c R d, then

$$(a+c) R (b+d) \quad , \quad (ac) R (b,d) .$$

We need only prove this for addition.

By (2) $(a+c)\, R\, (b+c)$, $(b+c)\, R\, (b+d)$,

hence by transitivity $(a+c)\, R\, (b+d)$. Q.E.D.

2.42. If -a, -b $[a^{-1}, b^{-1}]$ exist in $\mathfrak{K}$, and if a R b, then $-a \cdot R \cdot -b$ $[a^{-1} R\, b^{-1}]$.

Again it will suffice to prove this for negatives only. If a R b, then by repeated application of (2):

$$-b = (-a) + a + (-b) \cdot R \cdot (-a) + b + (-b) = -a,$$
Q.E.D.

We shall say that an equivalence relation R in $\mathfrak{K}$ is distributive if

$$a(b+c) \cdot R \cdot ab + ac$$

for all a, b, c of $\mathfrak{K}$. At last we are in a position to define similarity. Two elements a, b of $\mathfrak{K}$ are said to be similar in $\mathfrak{K}$, provided a R b for all distributive equivalence relations R of $\mathfrak{K}$. We write a S b.

2.43. Similarity is a distributive equivalence relation in $\mathfrak{K}$.

The proof of this theorem is quite simple; but to write it out in full would be rather a laborious task, unless we were to use the facilities of symbolic logic. It will suffice to prove transitivity of S here, whence it will become apparent how to show that S satisfies the other conditions ~~deman~~ demanded of an equivalence relation.

Suppose a S b and b S c. Then, if R be any distributive equivalence relation in $\mathfrak{K}$, a R b and b R c. But R is transitive and, therefore, a R c. This is true for all distributive equivalence relations R of $\mathfrak{K}$ whence a S c.

We have thus shown that S is transitive. Q.E.D.

We shall prove one more theorem concerning similarity:

__2.44.__ If $\mathfrak{K}_1$ is a sub-calculus of $\mathfrak{K}$, then elements of $\mathfrak{K}_1$ which are similar in $\mathfrak{K}_1$ are also similar in $\mathfrak{K}$.

Suppose a, b are members of $\mathfrak{K}_1$ such that a S b in $\mathfrak{K}_1$, i.e. a R b for all distributive equivalence relations R of $\mathfrak{K}_1$. Now every distributive equivalence relation R of $\mathfrak{K}$ gives rise to a distributive equivalence relation R_1 of $\mathfrak{K}_1$, R_1 being obtained from R by deleting all those pairs (x, y) from R, for which x and y do not both belong to $\mathfrak{K}_1$. (A relation, it will be remembered, is a set of pairs.) Hence, a fortiori, a R b for all distributive equivalence relations R of $\mathfrak{K}$, i.e. a S b in $\mathfrak{K}$. Q.E.D.

§ 3. THE CALCULUS $\mathfrak{D}$.

3.1. By a D-function we shall understand a numerical function which assigns to each positive integer a unique complex number. In general we shall assume that a D-function is undefined for arguments that are not positive integers, but we will not commit ourselves to this point of view; for, on occasion, a proof may be technically facilitated by stipulating that a D-function merely vanishes for an argument that is not a positive integer. Considered as an entity, a numerical function must be distinguished from its value for a variable argument (if this means anything); it should rather be construed as a relation which pairs off all positive integers with certain complex numbers.

Since functions are thus essentially different from their values, we cannot talk about sums and products of functions, unless we introduce such operations by special definitions. We shall be concerned with two conventions in particular, as to what these operations may mean with regard to D-functions.

Convention A:

'$h = f+g$' means '$h(n) = f(n)+g(n)$';

'$h = f\cdot g$' means '$h(n) = \sum_{n=d\delta} f(d)\, g(\delta)$'.

Convention B:

'$h = f+g$' means '$h(n) = \sum_{n=d\delta} f(d)\, g(\delta)$';

'$h = f\cdot g$' means '$h(n) = f(n)\cdot g(n)$'.

For reasons indicated in § 1, we shall adopt Convention B from now on, unless otherwise stated.

3.2. Let $\mathfrak{D}$ be the class of all D-functions. Then we have the following theorem:

3.21. $\mathfrak{D}$ is a calculus with respect to addition and multiplication (as defined by Convention B).

To prove this, we have to show that postulates I to III are satisfied.

(1) It is obvious that $\mathfrak{D}$ is closed under addition, and that the latter is commutative. To prove the associative law:

$$f + (g + h) \quad = \quad (f + g) + h \quad ,$$

we must show that

$$\sum_{n=d_1\delta} f(d_1)\Big(\sum_{\delta=d_2d_3} g(d_2)\, h(d_3)\Big) = \sum_{n=\delta d_3}\Big(\sum_{\delta=d_1d_2} f(d_1)\, g(d_2)\Big) h(d_3) \ ,$$

which is, of course, true since both sides simplify to:

$$\sum_{n=d_1d_2d_3} f(d_1)\, g(d_2)\, h(d_3) \quad ,$$

the sum extending over all triplets of positive integers (d_1 , d_2 , d_3) such that n = $d_1 d_2 d_3$.

The zero of addition is given by the function w, defined in 1.2. For if we put $g = f + \omega$ so that

$$g(n) = \sum_{n=d\delta} f(d)\,\omega(\delta) = f(n)\,\omega(1) = f(n) \ ,$$

whence $g = f$.

(2) It is obvious that $\mathfrak{D}$ is closed under multiplication, and that the latter is associative and commutative in $\mathfrak{D}$. The unit of multiplication is given by the function ϵ also defined in 1.2.

(3) It remains to show that w is distributive in $\mathfrak{D}$, i.e. that

$$\omega(f+g) = \omega f + \omega g$$

for all D-functions f and g. The functions represented by both sides of this equation take the value f (1) g (1) for n = 1, and vanish otherwise. Hence the identity holds for all f and g, and our theorem is proved.

If f is any D-function such that $f(n) \neq 0$ for all positive integers n, we may define a function g such that $f(n)\, g(n) = 1$, i.e. $f g = \epsilon$, so that g is a reciprocal of f. As such it is unique (2.12), whence we may write $g = f^{-1}$. The following theorem has thus been proved:

<u>3.22.</u> A D-function f has a reciprocal if and only if $f(n) \neq 0$ for all positive integers n.

If f is any D-function such that $f(1) \neq 0$, we can step by step solve the system of equations:

$$f(1)\, g(1) = 1$$

$$f(1)\, g(2) + f(2)\, g(1) = 0$$

$$- - - - - - - - -$$

$$\sum_{n=d\delta} f(d)\, g(\delta) = \omega(n)$$

for $g(n)$. Hence $f + g = w$, and g is a unique negative of f. We are justified in putting $g = -f$. On the other hand, if $f(1) = 0$, we cannot even solve for $g(1)$. Hence:

<u>3.23.</u> A D-function f has a negative if and only if $f(1) \neq 0$.

We know already from 1.21 that $-\epsilon = \mu$. In general, $-f$ may be calculated, as will be shown in 3.4. The following theorem is self-evident:

<u>3.24.</u> If f is a function in $\mathfrak{D}$, then $w f = w$ if and only if $f(1) = 1$.

<u>3.3.</u> We shall say that a D-function f is <u>multiplicative</u> provided

$$f(d)\, f(\delta) = f(d\delta)$$

for all positive integers d, δ.

Clearly ϵ and w, the product of two multiplicative functions, and the reciprocal of a multiplicative function (if it exists in $\mathfrak{D}$) are multiplicative. Hence all the conditions stated in 2.4 are satisfied, and we should not be surprised at the following theorem:

3.31. Every multiplicative D-function is a distributive element of $\mathfrak{D}$, and conversely.

In order to prove this theorem, we shall consider four lemmas: 3.32 - 3.35.

3.32. Every multiplicative D-function is distributive in $\mathfrak{D}$.

Suppose f is multiplicative. Then

$$\sum_{n=d\delta} f(d)\, g(d)\, f(\delta)\, h(\delta) = f(n) \sum_{n=d\delta} g(d)\, h(\delta),$$

i.e.
$$f\cdot g + f\cdot h = f\cdot(g+h),$$

where g and h are arbitrary functions of $\mathfrak{D}$. Hence our first lemma.

For the purpose of stating our next lemma, we shall introduce a function Ω, such that Ω (n) = 0 for all n (not to be confused with w, the zero of addition, for which w (1) = 1). Ω has the peculiar property that

$$\Omega + f = \Omega, \quad \Omega f = \Omega,$$

for any D-function f. It follows that Ω is distributive in $\mathfrak{D}$, and we shall prove:

3.33. The only distributive element f of $\mathfrak{D}$ for which f (1) = 0 is f = Ω.

Consider the function g_k for which g_k(n) = 1 if k = n, = 0 otherwise. Let f be a distributive element of $\mathfrak{D}$ such that f (1) = 0. Then

$$f\,(g_k + \epsilon) = f g_k + f,$$

i.e.
$$f(n) \sum_{d|n} g_k(d) = \sum_{n=d\delta} f(d)\, g_k(d)\, f(\delta).$$

In particular, when n = k, this becomes:

$$f(k)\; g_k(k) = f(k)\, g_k(k)\, f(1).$$

But $f(1) = 0$, $g_k(k) = 1$, so that $f(k) = 0$.

The argument may be repeated for other values of k, whence f (n) = 0 for all n, i.e. $f = \Omega$. Q.E.D.

<u>3.34.</u> If f is a distributive element of $\mathfrak{D}$, such that f (1) $\neq$ 0, then $f(1) = 1$, $f(n) = f(p_1)f(p_2)\dots f(p_k)$, n being the product of k distinct primes $p_1, p_2, \dots p_k$.

To prove this, consider the divisor function $\tau = \epsilon + \epsilon$, which was mentioned in 1.2. Let f be any distributive element of $\mathfrak{D}$, f (1) $\neq$ 0, then $f\tau = f(\epsilon+\epsilon) = f\epsilon + f\epsilon = f+f$.

This means, of course:

$$f(n)\tau(n) = \sum_{n=d\delta} f(d)f(\delta) . \qquad \text{......(i)}$$

If in (i) we take n = 1, we obtain $f(1)\tau(1) = f(1)f(1)$; but $f(1) \neq 0$, $\tau(1) = 1$, so that f (1) = 1. Next let $n = p_1p_2\cdots p_k$, the p_i being all distinct primes. We want to prove that

$$f(n) = f(p_1)f(p_2)\dots f(p_k) \qquad \text{......(ii)}$$

This is easily accomplished by induction. For k = 1, (ii) is trivially satisfied. Let us assume then that (ii) holds for all $k < l$, say, where $l > 1$. It remains to prove (ii) for k = l. Taking $n = p_1p_2\cdots p_l$, equation (i) becomes:

$$2^l f(n) = 2f(1)f(n) + \sum{}' f(d)f(\delta) , \qquad \text{......(iii)}$$

the primed sum extending over all ordered factorizations n = $d\delta$, with neither d nor δ = n. It follows that in each term of $\sum'$ the d and δ both contain less than l (distinct) prime factors, whence by our induction hypothesis

$$\begin{aligned}\sum{}' f(d)f(\delta) &= \sum_{r=1}^{l-1}\binom{n}{r} f(p_1)\cdots f(p_l)\\ &= (2^l-2)f(p_1)\cdots f(p_l) .\end{aligned}$$

Substituting this into (iii), in virtue of the fact that f (1) = 1, we obtain:

$$(2^l - 2)\, f(n) = (2^l - 2)\, f(p_1) \dots f(p_l)\ .$$

Since $l > 1$ we may divide by $2^l - 2$, whence the required result. This completes the proof of our third lemma.

3.35. If f is distributive in $\mathfrak{D}$, then f is multiplicative.

If f (1) = 0, f = Ω (by 3.33), so that this is trivial. Let us assume then that f (1) $\neq$ 0, hence f (1) = 1, and

$$f(p_1 p_2 \cdots p_k) = f(p_1)\, f(p_2) \cdots f(p_k)\ .$$

As follows, we shall define a function f^* , which will also be of importance later:

$$f^*(1) = 1\ , \quad f^*(n) = \prod f(p^\alpha) \quad \text{for} \quad n = \prod p^\alpha .$$

Clearly then f and f^* have the same values for square-free arguments, so that

$$\mu f = \mu f^* \ , \qquad \text{......(i)}$$

μ being the Moebius function of 1.2. Now f is distributive by assumption, f (1) = 1; hence by 3.24:

$$\omega = f\omega = f(\epsilon + \mu) = f\epsilon + f\mu = f + \mu f\ ,$$

so that $\mu f = -f$. (We could have quoted 2.23 here.) On the other hand f^* is multiplicative by definition, and therefore distributive by 3.32; whence similarly $\mu f^* = -f^*$. Hence (i) becomes:

$$-f = -f^* \qquad \text{......(ii)}$$

If we add $f + f^*$ on both sides of (ii), we see that $f = f^*$. But f^* is multiplicative, and therefore f is, which proves lemma 3.35.

3.32, 3.33, and 3.35 together make up 3.31, which has thus been demonstrated.

3.4. In a field repeated addition can always be replaced by multiplication. Thus $x + x = 2x$. In a non-distributive calculus, we still have $x + x = (\epsilon + \epsilon)\, x$, provided x is a distributive element; but in general such notational economy is unwarranted. Yet it would be useful to have some short-hand device of indicating repeated addition. Let us write:

$$f^{(r)} = f + f + \cdots + f \qquad (r \text{ terms})$$

We might therefore define by induction:

$$f^{(1)} = f \quad , \quad f^{(r+1)} = f^{(r)} + f \quad , \qquad \ldots\ldots(\mathrm{i})$$

whence $f^{(r)}$ will be determined for all positive r. The question arises, can we find an interpretation for $f^{(r)}$ when r is zero or negative? To fit in with (i), we must have

$$f^{(1)} = f^{(0)} + f \quad .$$

If f has a negative, upon adding $-f$ on both sides, we find $f^{(0)} = w$. Similarly $f^{(-1)} = -f$, and in general $f^{(-r)} = -f^{(r)}$.

Now if $r > 0$,

$$f^{(r)}(n) = \sum f(d_1)\, f(d_2) \cdots f(d_r) \quad ,$$

the sum extending over all ordered factorizations $n = d_1 d_2 \cdots d_r$. Can we find a formula that will enable us to calculate $f^{(r)}(n)$ even when r is negative? This is clearly a generalization of the problem which arose in 3.23. We shall state the theorem:

3.41. $$f^{(r)}(n) = \sum_{s=0}^{\infty} \binom{r}{s} f'^{(s)}(n)\, f^{r-s}(1) \quad ,$$

where $$f'^{(s)}(n) = \sum{}' f(d_1)\, f(d_2) \cdots f(d_s) \quad ,$$

the primed sum extending over all permutations $(d_1, d_2, \ldots, d_s)$ such that $n = d_1 d_2 \cdots d_s$, no factor being unity.

A few remarks are in order:

(1) Theorem 3.41 is always valid for $r > 0$, in which case, of course, it is redundant.

(2) For $r < 0$ the theorem is only meaningful provided $f\ (1) \neq 0$.

(3) The sum in 3.41 is only infinite in appearance. For positive r, $\binom{r}{s}$ will vanish for $s > r$; but, at any rate, $f^{\prime(s)}(n)$ will vanish, once s exceeds the total number of prime factors of n.

In the particular case where $r = -1$, we obtain as a corollary a formula for $-f = f^{(-1)}$:

$$\underline{3.42.} \qquad f^{(-1)}(n) = \sum_{s=0}^{\infty} (-1)^s f^{\prime(s)}(n)\, f^{1-s}(1)\ .$$

[This was stated and proved as a theorem by Prof. Bell in the Tôhoku Mathematical Journal, in 1920. Its enunciation there, however, involves a slight error.]

We shall now proceed to prove theorem 3.41. For the purpose of this proof only, let us abandon convention B, and adopt convention A instead. Hence, within this proof,

$$\text{'}f + g = h\text{'} \qquad \text{means} \qquad \text{'}f(n) + g(n) = h(n)\text{'}\ ,$$

$$\text{'}f \cdot g = h\text{'} \qquad \text{means} \qquad \text{'}\sum_{n=d\delta} f(d)\, g(\delta) = h(n)\text{'}\ .$$

It is easily seen that $\mathfrak{D}$ forms a commutative algebra of infinite basis with respect to these two operations. The zero of addition is Ω, the unity of multiplication is w. If k is any complex number, let 'k f = g' mean that $g\ (n) = k\ f\ (n)$. Hence $f + f = 2\ f$ etc. The operator k behaves like the function k w. Repeated multiplication is indicated by powers; thus $f^r = ff \ldots f$ (r terms). If $f\ (1) \neq 0$, we have $f^0 = w$ and $f^{-r} = \frac{1}{f^r}$ division being defined in an obvious manner. It is seen that f^r here has the same meaning as f $^{(r)}$ under convention A.

Now let f $'$ be obtained from f by suppressing f (1). Then

$$f' = f - \omega f(1) , \quad f = \omega f(1) + f' ,$$

and

$$f^r = (\omega f(1) + f')^r .$$

Since all the laws of ordinary algebra hold true in $\mathfrak{D}$, we may expand the R.H.S. by means of the binomical theorem. Thus

$$f^r = \sum \omega^{r-s} f(1)^{r-s} \binom{r}{s} f'^s$$

$$= \sum \binom{r}{s} f'^s f(1)^{r-s} ,$$

since w $^{r-s}$ = w is the unit under multiplication. If we now return to convention B, we must change f ^{r} to f $^{(r)}$, whence

$$f^{(r)}(n) = \sum \binom{r}{s} f'^{(s)}(n) f^{r-s}(1) .$$

But f $'^{(s)}$ (n) = $\sum f'(d_1) f'(d_2) \dots f'(d_s)$, the sum extending over all ordered factorizations n = $d_1 d_2 \cdots d_s$. From the definition of f $'$ it is seen that this is the same as $\sum' f(d_1) f(d_2) \dots f(d_s)$, the sum extending over all ordered factorizations n = $d_1 d_2 \cdots d_s$ such that none of the d_i = 1.

This completes the proof of 3.41, or rather what would have been the proof of 3.41, had we replaced the phrase: "Since all the laws of ordinary algebra hold true in $\mathfrak{D}$, we may expand the R.H.S. by means of the binomical theorem," by an actual demonstration of the fact.

A rigorous proof of 3.41, involving no switch from convention B to A, is indeed quite simple, but not very illustrating. Using the recurrence - formula

$$f'^{(s+1)}(n) = \sum_{n=d\delta}' f(d) f'^{(s)}(\delta) ,$$

and putting

$$g_r(n) = \sum \binom{r}{s} f'^{(s)}(n) f^{r-s}(n) ,$$

we may show by straight forward calculation that

$$g_1 = f , \quad g_{r+1} = g_r + f ,$$

whence it follows from the definition of $f^{(r)}$ that $g_r = f^{(r)}$.

3.5. We have seen in 3.23 that all D-functions f possess an inverse under addition, unless f (1) = 0. Functions having this latter character, though being exduded from many important properties, are by no means uninteresting.

Ex. 1. Let $\pi(n) = 1$ if n is the positive power of a prime, $= 0$ otherwise. It follows that $(\mu^2\pi)(n) = 1$ if n is a prime, $= 0$ otherwise. Neither of the functions π and $\mu^2\pi$ possess a negative, yet they give rise to interesting combinations. Let $\epsilon + \pi = \lambda$, $\epsilon + \mu^2\pi = \gamma$.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, then

$$\lambda(n) = \alpha_1 + \alpha_2 + \cdots + \alpha_r \quad , \quad \gamma(n) = r .$$

$\lambda(n)$ and $\gamma(n)$ are known in the literature as the multiplicity and manifoldness of n respectively.

Ex. 2. Let $\Lambda = L + \mu$ where $L(n) = \log n$. It is clearly verified that

$$\Lambda(n) = \log p \quad \text{if} \quad n = p^\alpha, \ p \ \text{prime}, \ \alpha > 0 ;$$

$$= 0 \text{ otherwise}$$

However, the vast majority of D-functions that occur in the theory of numbers have the property that $f(1) \neq 0$. We shall denote their totality by $\mathfrak{D}_1$.

3.51. The set $\mathfrak{D}_1$, of all D-functions f, such that $f(1) \neq 0$, forms a regular subtraction sub-calculus of $\mathfrak{D}$.

We note that ϵ and w belong to $\mathfrak{D}_1$. Either $h = f + g$ or $h = f \cdot g$ implies that $h(1) = f(1)\, g(1)$, so that $\mathfrak{D}_1$, is closed under both addition and multiplication.

Furthermore, subtraction is always possible by theorem 3.23. Indeed $f^{(-1)}(1) = 1/f(1)$, so that $-f = f^{(-1)}$ belongs to $\mathfrak{D}_1$ if f does. This proves that $\mathfrak{D}_1$ is a subtraction calculus.

It remains to show that $\mathfrak{D}_1$ is regular. A zero-divisor f in $\mathfrak{D}_1$ is characterized by the existence of a function g such that $w \nmid g$ and $f \cdot g = w$. g must satisfy the conditions $g(1) \neq 0$, $g(n) \neq 0$ for some $n > 1$. But $f(n)\, g(n) = 0$, so that $f(n) = 0$ for this particular value of n. A non-zero-divisor f then has the property that $f(n) \neq 0$ for all positive integers n.

Such a function, however, has a reciprocal f^{-1} by theorem 3.22; and it is clear that f^{-1} will again be in $\mathfrak{D}_1$; for $f^{-1}(1) = 1/f(1) \neq 0$. Q.E.D.

If f is any function in $\mathfrak{D}_1$, we may always define a function f', such that $f(n) = f'(n)\, f(1)$, whence, by taking $n = 1$, it follows that $f'(1) = 1$. We should hardly have lost in generality, had we restricted f in the first place to satisfy the condition $f(1) = 1$. Let us consider such functions, and denote their totality by $\mathfrak{D}_2$.

<u>3.52.</u> The set $\mathfrak{D}_2$ of all D-functions f, such that $f(1) = 1$, forms a regular subtraction sub-calculus of $\mathfrak{D}_1$.

By 3.24, $w f = w$ if and only if $f(1) = 1$. Hence $\mathfrak{D}_2$ stands in the same relation to $\mathfrak{D}_1$ as $\mathfrak{K}_1$ stood to $\mathfrak{K}$ in 2.2. The present theorem is then merely a corollary of 2.21.

It is obvious that the argument used in the proof of 3.31 will still be valid for $\mathfrak{D}_1$ and $\mathfrak{D}_2$, with the simplification that the function Ω is now excluded from consideration altogether. We conclude that the distributive elements of either calculus are the multiplicative functions $\neq \Omega$. However, we shall have to consider other sub-calculi of and it will become wearisome to repeat the inevitable theorem regarding distributive elements. We shall, therefore, state once and for all:

3.53. If $\mathfrak{S}$ is any subtraction calculus of D-functions with unity ϵ and zero w, then the set of all its distributive elements coincides with the set of all multiplicative functions pertaining to it.

§ 4. FACTORABLE FUNCTIONS

4.1. We shall say that f is a factorable function, provided $f(d\delta) = f(d)\,f(\delta)$ whenever $(d, \delta) = 1$. Hence $n = \prod p^{\alpha}$ implies that $f(n) = \prod f(p^{\alpha})$, so that all the values of f can be determined when we know its values for prime arguments. To prove that two factorable functions f and g are equal, it will, therefore, suffice to show that $f(p^{\alpha}) = g(p^{\alpha})$ for all primes p and all non-negative integers α.

Factorable functions are of great importance in connection with Dirichlet series. For, when f is factorable, then the corresponding generating function can also be factored, thus:

$$\sum_{n=1}^{\infty} f(n)\, n^{-s} = \prod_{p} \sum_{\alpha=0}^{\infty} f(p^{\alpha})\, p^{-\alpha s} ,$$

So that the Dirichlet Series which generates f can be expressed as a product, extending over all primes p, of power-series in p^{-s}. This, however, is a purely analytic matter, into which we shall not enter here, except by way of illustration.

It turns out that the great majority of numerical functions, which are used in the multiplicative theory of numbers, are factorable. In fact, of the functions for which we have so far introduced special symbols in this paper, Ω, L, Λ, π, λ, and γ are the only ones that do not fall into this category. The reader is probably familiar with the formulae:

$$\tau(n) = \prod (1+\alpha), \quad \sigma(n) = \prod \frac{p^{\alpha+1}-1}{p-1}, \quad \varphi(n) = \prod (p^{\alpha} - p^{\alpha-1}),$$

if not he should now be able to prove them.

4.2. Before investigating the set of all factorable functions as a calculus, we shall consider a more general type of functions. These may be characterized by any one of the following three equivalent statements:

(1) μ f is factorable.

(2) if d δ is square-free, then $f(d\delta) = f(d)\,f(\delta)$

(3) if n $= p_1\, p_2 \cdots p_k$, the p_i being distinct primes, then $f(n) = f(p_1)\,f(p_2)\cdots f(p_k)$.

We are interested in the totality of all such functions. From the algebraic point of view, it is, however, convenient to exclude functions f for which f (1) = 0. It follows that f (1) = 1. The resulting set will be called $\mathfrak{D}_3$.

4.21. The set $\mathfrak{D}_3$ of all functions f, such that u f is factorable, and f (1) $\neq$ 0, forms a regular subtraction sub-calculus of $\mathfrak{D}_2$.

(1) Clearly w belongs to $\mathfrak{D}_3$. Let f and g be in $\mathfrak{D}_3$, and h = f + g. If n = $d\delta$ is square-free, then

$$h(d)\,h(\delta) = \sum_{d=d_1d_2} f(d_1)\,g(d_2) \sum_{\delta=\delta_1\delta_2} f(\delta_1)\,g(\delta_2)$$

$$= \sum f(d_1\delta_1)\,g(d_2\delta_2).$$

If we put $d_1\delta_1 = d'$, $d_2\delta_2 = \delta'$ it is clear that $n = d'\delta'$ and d' runs through all the divisors of n.

$$\therefore \qquad h(d)\,h(\delta) = \sum_{n=d'\delta'} f(d')\,g(\delta') = h(n) = h(d\delta).$$

Hence h will also belong to $\mathfrak{D}_3$ and postulate I is satisfied.

(2) Evidently $\mu\epsilon = \mu$ is factorable, so that ϵ belongs to $\mathfrak{D}_3$. If f and g are members of $\mathfrak{D}_3$, and $d\delta$ is square-free, then

$$(fg)(d)\,(fg)(\delta) = f(d)\,g(d)\,f(\delta)\,g(\delta)$$

$$= f(d\delta)\,g(d\delta)$$

$$= (fg)(d\delta),$$

so that f g belongs to $\mathfrak{D}_3$. Hence postulate II is satisfied.

(3) Let f be a member of $\mathfrak{D}_3$, such that f^{-1} exists. Then for square-free $d\delta$

$$f^{-1}(d\delta) = [f(d\delta)]^{-1} = [f(d)f(\delta)]^{-1} = f^{-1}(d)\, f^{-1}(\delta),$$

so that f^{-1} belongs to $\mathfrak{D}_3$. Hence postulate V is satisfied.

(4) Next let f be any member of $\mathfrak{D}_3$. Since f (1) = 1, we have by 3.42:

$$f^{(-1)}(n) = \sum (-1)^s f^{\prime(s)}(n),$$

where

$$f^{\prime(s)}(n) = \sum{}' f(d_1) \,..\, f(d_s).$$

Let f^* be defined as before (3.35). Then for square-free n, f (n) = $f^*(n)$. But if n is square-free, so are all the divisors of n, whence

$$f^{\prime(s)}(n) = f^{*\prime(s)}(n),$$

and consequently

$$f^{(-1)}(n) = f^{*(-1)}(n) = \mu(n) f^*(n)$$

by 2.23. Put n = $d\delta$

$$\therefore \quad f^{(-1)}(d)\, f^{(-1)}(\delta) = \mu(d) f^*(d) \mu(\delta) f^*(\delta)$$

$$= \mu(d\delta) f^*(d\delta)$$

$$= f^{(-1)}(d\delta) .$$

Hence - f = $f^{(-1)}$ also belongs to $\mathfrak{D}_3$, and postulate IV is satisfied. This completes the proof of 4.21.

We are able to prove a rather interesting result about elements which are similar in $\mathfrak{D}_3$.

<u>4.22.</u> Two elements f and g of $\mathfrak{D}_3$ are similar in $\mathfrak{D}_3$ if and only if μ f = μ g.

(1) Since S is a distributive equivalence-relation, we have:

$$\mu(\epsilon + \mu) \cdot S \cdot \mu\epsilon + \mu^2$$

i.e.

$$\omega \cdot S \cdot \mu + \mu^2$$

$$\therefore \quad \epsilon \cdot S \cdot \mu^2 . \qquad \text{......(i)}$$

Now suppose $$\mu f = \mu g$$

$\therefore$ $$\mu^2 f = \mu^2 g$$

But by (i) $f \cdot S \cdot \mu^2 f$ and $g \cdot S \cdot \mu^2 g$, whence $f \cdot S \cdot g$.

(2) Let us write '$f \cdot M \cdot g$' for '$\mu f = \mu g$'.

Then clearly, M is transitive, symmetric, and reflexive. Now assume that f M g, i.e. μ f = μ g. If p be any prime, it follows that f (p) = g (p). Let h be any other element of $\mathfrak{D}_3$. Then

$$f(p) + h(p) = g(p) + h(p)$$

i.e. $$(f+h)(p) = (g+h)(p)$$

$\therefore$ $$[\mu(f+h)](p) = [\mu(g+h)](p).$$

But μ (p^α) = 0 for $\alpha > 1$, hence

$$[\mu(f+h)](p^\alpha) = [\mu(g+h)](p^\alpha);$$

and therefore $$\mu(f+h) = \mu(g+h),$$

since both sides are factorable. That is, $(f+h)\ M\ (g+h)$, and similarly it can be shown that (f h) M (g h). It follows that M is an equivalence relation.

Furthermore, since

$$f(p)(g(p)+h(p)) = f(p)g(p) + f(p)h(p),$$

i.e. $$[f(g+h)](p) = [fg+fh](p),$$

we may infer by a similar argument that $f(g+h) \cdot M \cdot (fg+fh)$.

Hence M is a distributive equivalence-relation in $\mathfrak{D}_3$.

(3) Now suppose that f S g in $\mathfrak{D}_3$. By definition, this means that every distributive equivalence-relation in $\mathfrak{D}_3$ holds between f and g. But we have just shown that M is one such relation, hence f M g.

By (1) and (3), it follows that, in $\mathfrak{D}_3$, f M g if and only if f S g, i.e. M = S, which proves the theorem 4.22.

In the preceding argument we have used the fact that if f is in $\mathfrak{D}_3$, then μ f is factorable; but we never had to resort to the converse of this. To avoid future duplication, we may, therefore, state once and for all:

<u>4.23.</u> If $\mathfrak{S}$ is any subtraction sub-calculus of $\mathfrak{D}_3$, then two elements f and g of $\mathfrak{S}$ are similar in $\mathfrak{S}$ if and only if $\mu f = \mu g$.

As was already shown in the proof of 3.34, if f is in $\mathfrak{D}_3$, we have $\mu f = \mu f^* = - f^*$, where f^* is multiplicative and, therefore, distributive. Hence $f \mathrel{S} f^*$ in $\mathfrak{D}_3$. On the other hand f^* is the only distributive element of $\mathfrak{D}_3$ which is similar to f; for suppose $f \mathrel{S} g$, with g distributive. Then $\mu f = \mu g = - g$, so that $- f^* = - g$. Adding $f^* + g$ on both sides, we find that $g = f^*$. Hence we may sum up:

<u>4.24.</u> A function f of $\mathfrak{D}_3$ is similar to precisely one distributive element f^* of $\mathfrak{D}_3$, where $f^* = - \mu f$.

It is obvious that the argument used here will apply equally well to any subtraction sub-calculus $\mathfrak{S}$ of $\mathfrak{D}_3$ which still contains all the distributive elements of $\mathfrak{D}_3$. Hence in general:

<u>4.25.</u> If $\mathfrak{S}$ is a subtraction sub-calculus of $\mathfrak{D}_3$ which contains all multiplicative functions other than Ω, then a function f of $\mathfrak{S}$ is similar to precisely one distributive element f^* of $\mathfrak{S}$, where $f^* = - \mu f$.

<u>4.3.</u> We shall now turn to factorable functions. Again we find it convenient to exclude from consideration such functions f for which $f(1) = 0$. It follows that $f(1) = 1$.

<u>4.31.</u> The set $\mathfrak{D}_4$ of all factorable functions f such that $f(1) \neq 0$ is a regular subtraction sub-calculus of $\mathfrak{D}_3$.

To show that it is a regular calculus, we proceed as in the proof of 4.21; except the condition that $d\delta$ is square-free must now be replaced by $(d, \delta) = 1$. Since μ is factorable, factorability of f implies that of μf. Hence any element of $\mathfrak{D}_4$ is an element of $\mathfrak{D}_3$, so that the former becomes a sub-calculus of the latter. It remains to show that it is closed under subtraction.

Let f be a member of $\mathfrak{D}_4$. Let $g(n) = \prod f^{(-1)}(p^\alpha)$ for $n = \prod p^\alpha$ which is clearly factorable. Put $h = f + g$, then

$$h(p^\alpha) = \sum_{\alpha=\beta+\gamma} f(p^\beta)\, g(p^\gamma) = \sum f(p^\beta)\, f^{(-1)}(p^\gamma) = \omega(p^\alpha) .$$

Both h and w are factorable; hence $h = f + g = w$, and $g = -f$, so that $-f$ is factorable and consequently belongs to $\mathfrak{D}_4$. Q.E.D.

As an example of a factorable function let us consider the function $\epsilon^{(k)}$, which in reference to 3.4 is defined by induction on k:

$$\epsilon^{(1)} = \epsilon , \quad \epsilon^{(k+1)} = \epsilon^{(k)} + \epsilon \qquad \text{......(i)}$$

This yields for positive k: $\epsilon^{(k)} = \underbrace{\epsilon + \cdots + \epsilon}_{k\ \text{terms}}$, $\epsilon^{(-k)} = -\epsilon^{(k)}$, $\epsilon^{(0)} = \omega$,

which immediately implies that $\epsilon^{(k)}$ is factorable.

There is a neat formula which enables us to calculate $\epsilon^{(k)}(n)$ for all integers k, viz:

<u>4.32.</u> $\epsilon^{(k+1)}(n) = \prod \binom{k+\alpha}{\alpha}$, where $n = \prod p^\alpha$.

To prove this, let us put preliminarily

$$\delta_{k+1}(n) = \prod \binom{k+\alpha}{\alpha} = \prod \binom{k+\alpha}{k} .$$

Then

$$\delta_1(n) = \prod \binom{\alpha}{0} = 1 = \epsilon(n) ,$$

so that

$$\delta_1 = \epsilon . \qquad \text{......(ii)}$$

Also

$$\begin{aligned}[\delta_{k+1} + \mu](p^\alpha) &= \delta_{k+1}(p^\alpha) - \delta_{k+1}(p^{\alpha-1}) \\ &= \binom{k+\alpha}{k} - \binom{k+\alpha-1}{k} \\ &= \binom{k+\alpha-1}{k-1} = \delta_k(p^\alpha) .\end{aligned}$$

$$\therefore \qquad \delta_{k+1} + \mu = \delta_k ,$$

since both sides are factorable, whence

$$\delta_{k+1} = \delta_k + \epsilon . \qquad \text{...... (iii)}$$

But (ii) and (iii) together make up (i), with $\epsilon^{(k)}$ replaced by δ_k, $\therefore \epsilon^{(k)} = \delta_k$, which was to be proved.

In particular:

$$\mu(n) = \epsilon^{(-1)}(n) = \prod \binom{\alpha - 2}{\alpha} , \quad \tau(n) = \epsilon^{(2)}(n) = \prod \binom{1+\alpha}{1} = \prod (1+\alpha) .$$

As a further example, consider the three functions ϵ_k, ω_k, μ_k; defined for positive integers k as follows:

$\epsilon_k(n) = 1$ if $n = a^k$, a integral; = 0 otherwise;

$\omega_k(n) = 1$ if $p^k \nmid n$, p prime; = 0 otherwise;

$\mu_k(n) = (-1)^{\gamma(n)}$ if $n = b^k$, b square-free; = 0 otherwise.

By inspection we see that these functions are factorable. There exist certain relationships between them, which may be condensed as follows:

<u>4.33.</u> $\qquad \epsilon_k + \omega_k = \epsilon , \quad \epsilon_k + \mu_k = \omega .$

Clearly there is only one way in which n can be factored in the form $n = a^k b$, such that b is not divisible by the k^{th} power of a prime.

Hence $\quad (\epsilon_k + \omega_k)(n) = \sum_{n=d\delta} \epsilon_k(d)\, \omega_k(\delta) = \epsilon_k(a^k)\, \omega_k(b) = 1 = \epsilon(n)$

$$\therefore \qquad \epsilon_k + \omega_k = \epsilon .$$

Furthermore, $(\omega_k + \mu)(p^\alpha) = \omega_k(p^\alpha) - \omega_k(p^{\alpha-1})$,

which is 1 if $\alpha = 0$, -1 if $\alpha = k$, and 0 otherwise. But this is precisely $\mu_k(p^\alpha)$. Hence $\omega_k + \mu = \mu_k$, since both sides are factorable.

$\therefore \quad \epsilon_k + \mu_k = \epsilon_k + \omega_k + \mu = \epsilon + \mu = \omega ,$ as was to be proved.

In particular: $\quad \omega_1 = \omega , \quad \epsilon_1 = \epsilon , \quad \mu_1 = \mu ,$

$$\omega_2 = \mu^2 , \quad \epsilon_2 = \epsilon - \mu^2 = \epsilon + \mu^* , \quad \mu_2 = \mu^2 - \epsilon = \mu^2 + \mu .$$

It is clear that two elements of $\mathfrak{D}_4$ are similar in $\mathfrak{D}_4$ if and only if they are similar in $\mathfrak{D}_3$, i.e. if and only if $\mu f = \mu g$. This, indeed, follows from 4.23. We are going to prove a more specific though less useful result.

Since $\mathfrak{D}_4$ is a subtraction-calculus, we can replace

'f S g' by '(f - g) S w.'

Now h S w means that $\mu h = \mu w = w$, so that h (n) = 0 for all square-free $n \neq 1$. If h is factorable, this is the same as saying that h (p) = 0 for all primes p. Let us introduce the function k such that k (n) denotes the number of ways in which n can be factored in the form $n = a^2 b^3$ such that b is square-free. Clearly k (n) = 1 or 0 for all n. K is seen to be factorable; in fact, it is quite easy to show that $K = \epsilon_2 + \mu^* \mu_3$.

Clearly $k(p^\alpha) = 1$ for $\alpha \neq 1$, $k(p) = 0$.

It follows that h S w if and only if k/h.

Hence '$f\,S g$ in $\mathfrak{D}_4$' could be written: $k \mid f-g$, or $f \equiv g \pmod{k}$.

<u>4.4.</u> We have seen the important position held by multiplicative functions, for they constitute the distributive elements of our calculus of numerical functions. Their totality unfortunately does not itself form a calculus, or we should have been able to exhibit a distributive calculus of numerical functions. However, we may consider the smallest regular subtraction calculus which contains all multiplicative functions other than Ω ; we shall call this $\mathfrak{D}_5$. Clearly then $\mathfrak{D}_5$ is the set of all D-functions which may be obtained from multiplicative functions $\neq \Omega$ by a finite number of applications of the four. rational operations - (addition, subtraction, multiplication, division). It follows that all the elements of $\mathfrak{D}_5$ are factorable, so that $\mathfrak{D}_5$ is a sub-calculus of $\mathfrak{D}_4$.

We may further restrict the admissable operations to addition and subtraction only, in which case we obtain a set $\mathfrak{D}_5'$ which is included in $\mathfrak{D}_5$. If we can show that $\mathfrak{D}_5'$ is also a calculus, it will follow that it is the smallest subtraction calculus containing all multiplicative functions $\neq \Omega$; i.e. it will be the smallest calculus satisfying the conditions of theorem 4.25. In other words: $\mathfrak{D}_5'$ is the set of all functions f such that

$$f = u_1 + u_2 + \quad + u_\pi - v_1 - v_2 - \cdots - v_\nu ,$$

where u_i, v_i are multiplicative functions $\neq \Omega$. We shall try to find some practicable criterion by means of which it can be decided whether or not a given numerical function belongs to $\mathfrak{D}_5'$, and furthermore we shall endeavour to prove that $\mathfrak{D}_5'$ is a subtraction-calculus.

<u>4.41.</u> A factorable function f can be expressed in the form $f = -v_1 - v_2 - \cdots - v_\nu$ if and only if $f(p^\alpha) = 0$ for every prime p and every integer $\alpha > \nu$.

(1) Suppose $f = -v_1 - v_2 - \cdot \quad - v_\nu$

i.e. $f = \mu v_1 + \mu v_2 + \quad + \mu v_\nu$.

$$\therefore \quad f(p^\alpha) = \sum \prod_{i=1}^{\nu} \mu(p^{\alpha_i}) \, v_i(p^{\alpha_i}) , \qquad \ldots\ldots \quad (i)$$

the sum extending over all ordered sets $(\alpha_1, \alpha_2, \ \cdot, \alpha_\nu)$ such that $\alpha = \alpha_1 + \alpha_2 + \ \cdot + \alpha_\nu$. In order that in a given product none of the $\mu(p^{\alpha_i})$ should vanish, we must have $\alpha_i = 0$ or $= 1$. This is impossible when $\alpha > \nu$. Hence $f(p^\alpha) = 0$ for $\alpha > \nu$.

(2) On the other hand, suppose $f(p^\alpha)$ does vanish when α exceeds ν . In order that equation (i) should hold, we have to satisfy ν equations of the type:

$$f(p^\alpha) = (-1)^\alpha \sum v_{i_1}(p) \, v_{i_2}(p) \cdots v_{i_\alpha}(p) ,$$

which may be combined as:

$$x^{\nu} + f(p)\,x^{\nu-1} + \cdots + f(p^{\nu}) = 0 . \qquad \ldots\ldots(\text{ii})$$

The ν solutions for x are to be interpreted as $v_1(p),\ v_2(p),\ \ldots\ v_\nu(p)$. This process applies to all primes p, and the functions v_i are determined by $v_i(n) = \prod v_i(p)^{\alpha}$ for $n = \prod p^{\alpha}$. It should be noticed, however, that the v_i are not unique, since for a given p the order of the various $v_i(p)$ is not laid down.

As an example, consider the function ω_k, which was defined in the paragraph preceding 4.33. ω_k is factorable, and furthermore

$$\omega_k(p^{\alpha}) = 1 \quad \text{if} \quad \alpha < k\ , \ = 0 \ \text{if}\ \alpha \geq k .$$

Hence, by 4.41 we should expect a decomposition

$$\omega_k = -v_1 - v_2 - \cdots - v_{k-1} ,$$

since $\nu = k - 1$ in this case. Equation (ii) becomes:

$$x^{k-1} + x^{k-2} + \cdots + 1 = 0 ,$$

whence $v_s(p) = e^{2\pi i s/k}$. If we write $\epsilon^{s/k}(n) = e^{2\pi i \lambda(n) s/k}$ we may put $v_s = \epsilon^{s/k}$.

$$\therefore \qquad \omega_k = -\epsilon^{1/k} - \epsilon^{2/k} - \cdots - \epsilon^{(k-1)/k} .$$

Furthermore $\epsilon_k = \epsilon - \omega_k = \epsilon + \epsilon^{1/k} + \epsilon^{2/k} + \cdots + \epsilon^{(k-1)/k}$.

<u>4.42.</u> A factorable function f can be expressed in the form:

$$f = u_1 + \cdots + u_{\pi} - v_1 - \cdots - v_{\nu} \qquad \ldots\ldots(\text{i})$$

if and only if for every prime p there exist π constants $u(p, \alpha)$ ($\alpha = 1, 2, \ldots \pi$) such that

$$f(p^{\alpha}) + u(p,1)\,f(p^{\alpha-1}) + \cdots + u(p,\pi)\,f(p^{\alpha-\pi}) = 0 \qquad \ldots\ldots(\text{ii})$$

for all $\alpha > \nu$. [If $\alpha < \pi$ we interpret $f(p^{\alpha-\pi})$ as 0.]

(1) Equation (i) can be written: $u + f = v$,

where $-v = v_1 + \cdots + v_{\nu}$, $-u = u_1 + \cdots + u_{\pi}$.

By 4.41 it follows that $v(p^\alpha) = 0$ for $\alpha > \nu$, $u(p^\beta) = 0$ for $\beta > \pi$. Putting $u(p^\beta) = u(p,\beta)$, these two conditions imply (ii).

(2) On the other hand, if (ii) holds, we define $u(p^\beta) = u(p,\beta)$ for $\beta \leq \pi$, $= 0$ for $\beta > \pi$. Moreover we define $v = u + f$ so that by (ii) $v(p^\alpha) = 0$ for all $\alpha > \nu$. By 4.41, $-u$ and $-v$ are the sums of π and ν multiplicative functions respectively, whence $f = v - u$ is of the form (i).

As an example let us consider the function c (our notation) due to Cantor, which is defined as follows:

$$c(1) = 1, \quad c(n) = \alpha_1 \alpha_2 \cdots \quad for \quad n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots \neq 1.$$

The formula $\alpha - 2(\alpha-1) + (\alpha-2) = 0$

gives rise to: $c(p^\alpha) - 2c(p^{\alpha-1}) + c(p^{\alpha-2}) = 0$, for $\alpha > 2$,

which is condition (ii) of theorem 4.42 with $\pi = \nu = 2$, $u(p,1) = 1$, $u(p,2) = 2$.

Hence there exists a decomposition

$$c = v - u, \quad -u = u_1 + u_2, \quad -v = v_1 + v_2.$$

Putting $u(p,\alpha) = u(p^\alpha)$, equation (ii) of 4.41 becomes:

$$x^2 - 2x + 1 = 0$$

whence $x = 1$, $\therefore$ $u_1(p) = u_2(p) = 1 = \epsilon(p)$. We may take $u_1 = u_2 = \epsilon$, $-u = \epsilon + \epsilon = \tau$.

If we now put $v = c + u$, we calculate $v(p) = c(p) + u(p) = 1 - 2 = -1$; $v(p^2) = c(p^2) + c(p)u(p) + u(p^2) = 2 - 2 + 1 = 1$,

so that equation (ii) of 4.41 yields for v:

$$x^2 - x + 1 = 0,$$

whence $v_1(p) = e^{2\pi i/6}$, $v_2(p) = e^{10\pi i/6}$. We may take $v_1 = \epsilon^{1/6}$, $v_2 = \epsilon^{5/6}$.

The required decomposition is therefore: $c = \epsilon + \epsilon - \epsilon^{1/6} - \epsilon^{5/6}$.

This result may be thrown into another form. Clearly

$$c = \epsilon + (\epsilon + \epsilon^{1/2}) + (\epsilon + \epsilon^{1/3} + \epsilon^{2/3}) - (\epsilon + \epsilon^{1/6} + \cdots + \epsilon^{5/6}),$$

$$\therefore \quad c = \epsilon_1 + \epsilon_2 + \epsilon_3 - \epsilon_6.$$

If $\zeta(s)$ is the generating function of ϵ, then ϵ_k has generating function

$$\sum \epsilon_k(n)\, n^{-s} = \sum n^{-ks} = \zeta(ks)\,,$$

so that

$$\sum \frac{c(n)}{n^s} = \frac{\zeta(s)\,\zeta(2s)\,\zeta(3s)}{\zeta(6s)}\,,$$ a result mentioned by Bachmann.

<u>4.43.</u> f belongs to $\mathfrak{D}'_s$ if and only if for every prime p there exist constants $E_i(p)$ and polynomials $F_i(p,\alpha)$ in α of degree π_i, such that

$$f(p^\alpha) = \sum_i F_i(p,\alpha)\, E_i(p)^\alpha \qquad \text{......(i)}$$

for all $\alpha > \delta$, δ being some constant independent of p.

In theorem 4.42 we developed a necessary and sufficient condition (ii) for f to be a member of $\mathfrak{D}'_s$. This can be written:

$$f(p^{\pi+\beta}) + u(p,1)\, f(p^{\pi+\beta-1}) + \cdots + u(p,\pi)\, f(p^\beta) = 0,$$

for all $\beta > \nu - \pi$ and all primes p. For a given p this constitutes a difference equation in β; and, according to the theory of such equations, we must factor the operator $E^\pi + u(p,1)\,E^{\pi-1} + \cdots\ u(p,\pi)$

in the form $$\prod \left(E - E_i(p)\right)^{\pi_i}\,, \quad \sum \pi_i = \pi\,,$$

and then write $$f(p^\alpha) = \sum_i F_i(p,\alpha)\, E_i(p)^\alpha\,,$$

where $F_i(p,\alpha)$ is a polynomical of degree π_i in α.

Putting $\delta = \nu - \pi$, we obtain our theorem. The polynomicals $F_i(p,\alpha)$ may be calculated from the first π equations (i), α ranging from $\delta+1$ to ν. Clearly each E_i coincides with π_i of the u_j of the previous theorem.

<u>4.44.</u> The set $\mathfrak{D}'_s$ is a subtraction sub-calculus of $\mathfrak{D}_s$.

In virtue of what was stated at the beginning of 4.4, it only remains to show that the set under consideration is closed under multiplication. We use the expansion (i) of theorem 4.43. Clearly the product of two functions which allow of such an expansion will again be of the same type. Q.E.D.

4.5. The expression for the product of two functions in $\mathfrak{D}_S'$ which was indicated in the proof of 4.44 is, of course, not very practical. In special cases much simpler results may be obtained. In the following, let 'u_i' and 'v_i' always denote multiplicative functions $\neq \Omega$, so that $u_i(p^\alpha) = u_i(p)^\alpha$. If it is understood that we confine attention to some particular prime p, we shall abbreviate $u_i(p)$ as u_i, under which convention u_i^α will stand for $u_i(p^\alpha)$.

4.51. $$(u_1 - v_1)(u_2 - v_2) = u_1 u_2 + \mu(u_1 v_2 + v_1 u_2 - v_1 v_2).$$

For the argument $n = p^\alpha$, the L.H.S. becomes:

$$(u_1^\alpha - v_1 u_1^{\alpha-1})(u_2^\alpha - v_2 u_2^{\alpha-1}) = u_1^\alpha u_2^\alpha - u_1^{\alpha-1} u_2^{\alpha-1}(u_1 v_2 + v_1 u_2 - v_1 v_2);$$

but this is clearly the R.H.S. for the same argument. Since both sides are factorable, the theorem is proved.

If $u_1 v_2 + v_1 u_2 \cdot S \cdot v_1 v_2$, then $\mu(u_1 v_2 + v_1 u_2 - v_1 v_2) = \omega$. Hence we may state as a corollary:

4.52. If $u_1 v_2 + v_1 u_2 \cdot S \cdot v_1 v_2$, then $(u_1 - v_1)(u_2 - v_2) = u_1 u_2$.

Ex. 1. Since

$$\eta\mu^* + \epsilon\varphi^* \cdot S \quad -\eta + \varphi \cdot = \cdot \mu \cdot S \quad \epsilon\mu^*,$$

we have by theorem 4.52:

$$(\eta - \epsilon)(\varphi^* - \mu^*) = \eta\varphi^*,$$

i.e.

$$\varphi \quad (\varphi + \mu^2) = \eta\varphi^*.$$

Since $\varphi \, S \, \varphi^*$, $\therefore \quad \frac{\mu}{\varphi} = \frac{\mu}{\varphi^*}$, hence, on dividing by φ^*, which is distributive,

$$\varphi\,(\epsilon + \frac{\mu^2}{\varphi}) = \eta,$$

i.e.

$$\epsilon + \frac{\mu^2}{\varphi} = \frac{\eta}{\varphi},$$

or $$\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)},$$ an example given by Uspensky.

Ex. 2. It is customary to denote the sum of the k^{th} powers of the divisors of n by $\sigma_k(n)$, so that $\sigma_k = \epsilon + \eta^k$. In particular $\sigma_0 = \tau$, $\sigma_1 = \sigma$.

Since $\sigma_k{}^* \mu^* + \epsilon \eta^k \cdot S \cdot - \sigma_k + \eta^k \cdot = \cdot \mu \cdot S \cdot \epsilon \mu^*$,

therefore by theorem 4.52:

$$(\sigma_k{}^* - \epsilon)(\eta^k - \mu^*) = \sigma_k{}^* \eta^k \ ,$$

i.e.

$$(\sigma_k{}^* + \mu)(\eta^k + \mu^2) = \sigma_k{}^* \eta^k \ .$$

As above $\dfrac{\mu}{\sigma_k} = \dfrac{\mu}{\sigma_k{}^*}$; hence, on dividing by $\eta^k \sigma_k{}^*$, which is distributive:

$$\left(\epsilon + \frac{\mu}{\sigma_k}\right)\left(\epsilon + \frac{\mu^2}{\eta^k}\right) = \epsilon \ ;$$

or

$$\sum_{d|n} \frac{\mu(d)}{\sigma_k(d)} \sum_{d|n} \frac{\mu^2(d)}{d^k} = 1 \ .$$

<u>4.53.</u> $(u_1 + u_2)(u_3 + u_4) = u_1 u_3 + u_2 u_4 + u_1 u_4 + u_2 u_3 + \mu_2 (u_1 u_2 u_3 u_4)^{1/2}$,

where $\mu_2 = \mu + \mu^2$.

We need not worry about any ambiguity in sign in the last term of the R.H.S., since $\mu_2(n)$ vanishes whenever n is not a square. In fact, $\mu_2(p^\alpha) = 1, -1$, or 0, according as $\alpha = 0, 2$, or otherwise.

Let us put $x = u_1 u_3$, $y = u_2 u_4$, $z = u_1 u_4$, $w = u_2 u_3$, $U = x + y + z + w$.

The R.H.S. for the argument n = p may then be written

$$U(p^\alpha) - z(p)\, w(p)\, U(p^{\alpha-2}) .$$

Abbreviating x (p) as x etc., as before, we now have:

$$U(p^\alpha) = \sum_{i=0}^{\alpha} (x + x^{i-1}y + \cdots + y^i)(z^{\alpha-i} + \cdots + w^{\alpha-i})$$

$$= (x^\alpha + x^{\alpha-1}y + \cdots + y^\alpha) + (x^{\alpha-1} + \cdots + y^{\alpha-1})(z + w) + V(p^\alpha)$$

where

$$V(p^\alpha) = \sum_{i=0}^{\alpha-2} (x^i + x^{i-1}y + \cdots + y^i)(z^{\alpha-i} + \cdots + w^{\alpha-i})$$

$$= \sum_{i=0}^{\alpha-2} (x^i + x^{i-1}y + \cdots + y^i)(z^{\alpha-i} + w^{\alpha-i}) + zw\, U(p^{\alpha-2}) .$$

Hence R.H.S. (p^α) $= U(p^\alpha) - zw\,U(p^{\alpha-2})$

$$= \sum_{i=0}^{\alpha} (x^i + x^{i-1}y + \cdots + y^i)(z^{\alpha-i} + w^{\alpha-i}) - (x^\alpha + \cdots + y^\alpha)$$

$$= \sum_{i=0}^{\alpha}\sum_{j=0}^{i} x^j y^{i-j} z^{\alpha-i} + \sum_{i=0}^{\alpha}\sum_{j=0}^{i} x^j y^{i-j} w^{\alpha-i} - \sum_{i=0}^{\alpha} x^i y^{\alpha-i}$$

$$= \Sigma_1 + \Sigma_2 - \Sigma_3 \,, \qquad \text{say} .$$

Now $$\Sigma_1 = \sum_{i,j} (u_1 u_3)^j (u_2 u_4)^{i-j} (u_1 u_4)^{\alpha-i}$$

$$= \sum_{i,j} u_1^{\alpha-i+j} u_2^{i-j} u_3^j u_4^{\alpha-j} ,$$

with two conditions: $i \leq \alpha$, $j \leq i$. Put $\alpha - i + j = k$, so that $i = \alpha + j - k$ may be eliminated. The two conditions then become: $j \leq k$, $k \leq \alpha$. Hence

$$\Sigma_1 = \sum_{k=0}^{\alpha}\sum_{j=0}^{k} u_1^k u_2^{\alpha-k} u_3^j u_4^{\alpha-j} .$$

Similarly $$\Sigma_2 = \sum_{k=0}^{\alpha}\sum_{j=0}^{k} u_1^j u_2^{\alpha-j} u_3^k u_4^{\alpha-k} ,$$

and $$\Sigma_3 = \sum_{i=0}^{\alpha} u_1^i u_2^{\alpha-i} u_3^i u_4^{\alpha-i} .$$

Hence R.H.S. $$= \Sigma_1 + \Sigma_2 - \Sigma_3 = \Big(\sum_{k=0}^{\alpha}\sum_{j=0}^{k} + \sum_{j=0}^{\alpha}\sum_{k=0}^{j} - \sum_{j=k=0}^{\alpha} \Big) u_1^k u_2^{\alpha-k} u_3^j u_4^{\alpha-j}$$

$$= \sum_{k=0}^{\alpha}\sum_{j=0}^{\alpha} u_1^k u_2^{\alpha-k} u_3^j u_4^{\alpha-j}$$

$$= \Big(\sum_{k=0}^{\alpha} u_1^k u_2^{\alpha-k} \Big)\Big(\sum_{j=0}^{\alpha} u_3^j u_4^{\alpha-j} \Big) ,$$

which is, of course, the L.H.S. for $n = p^{\alpha}$. Since both sides are factorable, the identity is therefore proved.

As an application take $u_1 = \eta^a$, $u_3 = \eta^b$, $u_2 = u_4 = \epsilon$.

Then
$$\sigma_a \sigma_b = \epsilon + \eta^a + \eta^b + \eta^{a+b} + \mu_2 \eta^{(a+b)/2}$$
$$= \epsilon + \eta^a + \eta^b + \eta^{a+b} - \epsilon_2 \eta^{(a+b)/2}$$

since $\eta^{(a+b)/2}$ is distributive, and $\mu_2 = -\epsilon_2$. In terms of generating functions, this is a result due to Ramanujan. If $\zeta(s) = \sum n^{-s}$ is the generating function of ϵ, then η^k has $\zeta(s-k)$ and $\epsilon_2\eta^k$ has $\zeta(2(s-k))$ as generating function. Hence the above identity becomes:

$$\sum \frac{\sigma_a(n)\sigma_b(n)}{n^s} = \frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)} .$$

In particular we obtain in this manner:

$$\tau^2 = \epsilon + \epsilon + \epsilon + \mu^2 , \quad \sigma^2 = \epsilon + \eta + \eta^2 + \mu^2\eta .$$

Suppose a, b, c, d are multiplicative functions other than Ω.

Then by 4.53 we have:
$$(a+b)(c+d) = ac + bd + ad + bc + \mu_2 (abcd)^{1/2}$$
and
$$(a+c)(b+d) = ab + cd + ad + cb + \mu_2 (acbd)^{1/2}.$$

Subtracting, we obtain:

<u>4.54.</u> If a, b, c, d are multiplicative functions $\neq \Omega$, then
$$(a+b)(c+d) - (a+c)(b+d) = ac + bd - ab - cd .$$

This can be furthermore expressed as
$$a(c-b) + d(b-c) \quad \text{or} \quad c(a-d) + b(d-a)$$
but is in general $\neq$ (a-d) (c-b).

SUMMARY

The Dirichlet operation, which combines numerical functions, corresponding to the product of Dirichlet series, has been studied from an algebraic point of view, without reference to analytic questions, such as convergence of the series concerned. A new outlook was obtained by interpreting it as a species of addition rather than of multiplication, the latter operation being defined in an obvious manner. A calculus, such as the above calculus of numerical functions, is an algebraic system in which the distributive law is absent. In the investigation of calculi, two questions arose among others. (1) What instances of the distributive law do occur in a calculus? (2) What elements of a calculus would merge if the distributive law were to hold?

In abstract calculi, the answers to these two questions entailed two novel concepts: that of distributive elements, and that of similarity. We were able to decide what elements are distributive in the calculus of numerical functions associated with Dirichlet series; the second question was answered for certain of its sub-sets, in particular, for the calculus of factorable functions. Several interesting identities were developed for the smallest calculus that contained all multiplicative functions and is closed under subtraction.

It is our opinion that all this only touches the surface of a large field that still calls for investigation.

BIBLIOGRAPHY

P. Bachmann, Die Analytische Zahlentheorie, Leipzig, Teubner, 1894.

E.T. Bell, On a certain inversion in the theory of numbers, Tôhoku, Mathematical Journal, Vol. 17, 1920, pp. 261 - 231.

E.T. Bell, Algebraic Arithmetic, American Mathematical Society Colloquium Publications, Vol. 7, 1927.

G. Birkhoff and S. MacLane, A Survey of Modern Algebra, New York, Macmillan, 1941.

G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, Oxford, Clarendon Press, 1938.

E. Landau, Vorlesungen über Zahlentheorie, Vol. 1, Leipzig, Hirzel, 1927.

J.V. Uspensky and M.A. Heaslet, Elementary Number Theory, New York, McGraw Hill, 1939.

- - - - - - - - -