THE RING OF NUMBER-THEORETIC FUNCTIONS

E. D. CASHWELL AND C. J. EVERETT

Introduction. The set Ω of all functions $\alpha(n)$ on $N = \{1, 2, 3, \cdots\}$ to the complex field F forms a domain of integrity under ordinary addition, and *arithmetic product* defined by: $(\alpha \cdot \beta)(n) = \sum \alpha(d)\beta(n/d)$, summed over all $d \mid n$, $d \in N$. The group of units of this domain contains as a subgroup the set of all multiplicative functions. Against this background, the "inversion theorems" of number theory appear as obvious consequences of ring operations, and generalizations of the standard functions arise in a natural way. The domain Ω is isomorphic to the domain P of formal power series over F in a countable set of indeterminates. The latter part of the paper is devoted to proving that the theorem on unique factorization into primes, up to order and units, holds in P and hence in Ω.

1. Definition. The class Ω of all number-theoretic functions α, [4; Ch. IV], i.e., functions $\alpha(n)$ on the set N of natural numbers $n = 1, 2, 3 \cdots$ to the complex field F, forms a domain of integrity (commutative, associative ring with identity and no proper divisors of zero) under ordinary addition: $(\alpha + \beta)(n) \equiv \alpha(n) + \beta(n)$, and an operation, frequently occurring in number theory in various disguises, which we call the arithmetic product:

$$(\alpha \cdot \beta)(n) \equiv \sum \alpha(d)\beta(d')$$

the summation extending over all ordered pairs (d, d') of natural numbers such that $dd' = n$.

The commutativity $\alpha \cdot \beta = \beta \cdot \alpha$ follows from the fact that the correspondence $(d, d') \to (d', d)$ is one-to-one on such a set of ordered pairs to (all of) itself, while the associative law $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ can be verified by observing that, in either association, $(\alpha \cdot \beta \cdot \gamma)(n) = \sum \alpha(d)\beta(d')\gamma(d'')$, summed over all ordered triples (d, d', d'') with $dd'd'' = n$.

The zero 0 and additive inverse $-\alpha$ of α are of course the functions defined by $0(n) \equiv 0$, and $(-\alpha)(n) \equiv -\alpha(n)$, and one sees at once that the function ε with $\varepsilon(1) = 1$, $\varepsilon(n) = 0$ for $n > 1$, is the identity: $\varepsilon \cdot \alpha = \alpha$ for all α of Ω.

That the ring Ω has no proper divisors of zero may be seen in various ways, three of which occur incidentally in the following sections (2, 4, 5).

2. A norm for number-theoretic functions. A function $N(\alpha)$ on

Received March 8, 1959.

Ω to the set of non-negative integers $0, 1, 2, \cdots$ which is zero if and only if $\alpha = 0$, and has the property $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$ for *all* α, β of Ω, may be defined by setting $N(0) = 0$, and, for all $\alpha \neq 0$, taking $N(\alpha)$ to be the least natural number n for which $\alpha(n) \neq 0$.

Indeed, we find that, if α and β are non-zero functions of Ω with $N(\alpha) = a$ and $N(\beta) = b$, then $(\alpha \cdot \beta)(n) \equiv 0$ for all (if any) n of N with $n < ab$, and $(\alpha \cdot \beta)(ab) = \alpha(a)\beta(b) \neq 0$. It follows that Ω is domain of integrity, and that the norm $N(\alpha)$ has the multiplicative property.

3. Group of units. If for α, β in the domain of integrity Ω, there exists a γ in Ω such that $\alpha = \beta \cdot \gamma$, we say β divides α and write $\beta | \alpha$. The set Υ of all units ν, i.e., elements of Ω which divide the identity ε, forms a commutative group under $(\cdot)$ with identity ε. Two functions α, β of Ω are called associates (notation $\alpha \sim \beta$) in case there is a unit ν such that $\beta = \alpha \cdot \nu$. One sees that $\alpha \sim \beta$ if and only if $\alpha | \beta$ and $\beta | \alpha$, and that $(\sim)$ is an equivalence relation which splits Ω into disjoint classes [ ] of associates. For example, the class [0] contains only 0, while $[\varepsilon] = \Upsilon$. These trivial properties are shared by all domains of integrity.

In our ring Ω, an element α is a unit if and only if $\alpha(1) \neq 0$, equivalently $N(\alpha) = 1$. For, if $\alpha\alpha' = \varepsilon$, $1 = \varepsilon(1) = \alpha(1)\alpha'(1)$ implies $\alpha(1) \neq 0$. To see that this is also sufficient, we first introduce the (number-theoretic) function $\lambda(n)$ defined by $\lambda(1) = 0$, $\lambda(p_1 \cdots p_l) = l$ for any product of l (not necessarily distinct) primes. We have $\lambda(a) = 0$ if and only if $a = 1$, and $\lambda(ab) = \lambda(a) + \lambda(b)$ always. This function has the property of classifying all natural numbers according to their *length*. We have now to construct a function α' in Ω with $(\alpha \cdot \alpha')(n) \equiv \varepsilon(n)$ from a given α for which $\alpha(1) = A \neq 0$. Manifestly, for $n > 1$, this relation itself defines the value of $\alpha'(n)$ unambiguously for each n of length $\lambda(n) = l$ in terms of values $\alpha'(d')$ with $\lambda(d') < l$. Thus, if we define $\alpha'(1) = 1/A$ for the single n of length 0, and proceed inductively on $\lambda(n)$, we automatically obtain the desired α'.

We note in passing that if α, β are any two number-theoretic functions and $\nu \cdot \nu' = \varepsilon$, then $\beta = \alpha \cdot \nu$ if and only if $\alpha = \beta \cdot \nu'$. This trivial relation between associates is the basis for the so-called inversion theorems of number theory. (Cf. § 7).

4. The degree of a number-theoretic function. Just as a natural order $1 < 2 < 3 < \cdots$ of the set N permitted the definition of a norm, so does the order implicit in the λ function enable us to introduce what we may call the *degree* $D(\alpha)$ of a non-zero function α of Ω.

Specifically we take $D(\alpha) = d$ to mean that $\alpha(n) = 0$ for all (if any) n of N with $\lambda(n) < d$, and that there exists an n with $\lambda(n) = d$ for which $\alpha(n) \neq 0$. Thus $D(\alpha)$ is a function on all non-zero α of Ω to the

non-negative integers, with $D(\alpha) = 0$ if and only if α is a unit, and $D(\alpha \cdot \beta) = D(\alpha) + D(\beta)$ for all non-zero α, β.

We may indeed show somewhat more. Let $D(\alpha) = d$, $D(\beta) = e$, and suppose a and b are respectively the least integers with $\lambda(a) = d$, $\lambda(b) = e$, for which $\alpha(a) \neq 0$, $\beta(b) \neq 0$. Then $(\alpha \cdot \beta)(n) = 0$ for all (if any) n with $\lambda(n) < d + e$; $(\alpha \cdot \beta)(ab) = \alpha(a)\beta(b) \neq 0$, where, of course, $\lambda(ab) = d + e$; and finally, indeed, $(\alpha \cdot \beta)(n) = 0$ for all $n < ab$ with $\lambda(n) = d + e$, that is to say, ab is itself the least integer of its length at which $\alpha \cdot \beta$ does not vanish.

5. A second norm. The final remarks of the preceding section make it clear that another norm $M(\alpha)$ is available. Specifically, set $M(0) = 0$, and for $\alpha \neq 0$ with $D(\alpha) = d$, set $M(\alpha) = a$, where a is the least integer of length $\lambda(a) = d$ for which $\alpha(a) \neq 0$. It follows that $M(\alpha)$ is a function on all α of Ω to the non-negative integers such that $M(\alpha) = 0$ if and only if $\alpha = 0$, $M(\alpha) = 1$ if and only if α is a unit, and $M(\alpha \cdot \beta) = M(\alpha)M(\beta)$ always.

Thus $M(\alpha)$ has all the properties proved for $N(\alpha)$ and moreover determines $D(\alpha) = \lambda(M(\alpha))$ for $\alpha \neq 0$.

6. The multiplicative functions. This and the following few sections (7-10) are to some extent expository, our object being to observe how familiar results appear when considered from the point of view of the ring Ω or to propose some natural generalizations suggested by the new notation. After this we return to the "arithmetic" of the domain Ω itself.

A number-theoretic function α is said to be multiplicative in case $(a, b) = 1$ implies $\alpha(ab) = \alpha(a)\alpha(b)$ and (to exclude the trivial $\alpha = 0$) there is an integer n for which $\alpha(n) \neq 0$. In the presence of the former property, the latter is equivalent to the condition $\alpha(1) = 1$, which signifies for us that the set M of all multiplicative functions is a subset of the group Γ of units of Ω.

Clearly (1) a function α for which $\alpha(1) = 1$ and $\alpha(\Pi p^a) = \Pi\alpha(p^a)$ is multiplicative, $\alpha(p^a)$ being quite arbitrary for each power $a = 1, 2, \cdots$ of each prime p; and (2) two *multiplicative* functions identical on all such p^a are equal.

That $M \cdot M \subset M$ follows readily from the definition of M, and the identity ε is in M, seen perhaps most trivially from (1) above. To see that M is a *subgroup* of Γ requires only the further fact that the inverse α' of a multiplicative function α, which we know exists uniquely, is itself multiplicative. This we prove in a way which provides a second construction of the inverse in the case of a multiplicative function. [5; p. 89]

Given α in M, define a function β in Ω as follows. Set $\beta(1) = 1$. For each p, define $\beta(p^a)$ for $a = 1, 2, \cdots$ successively by the relation $\sum \alpha(d)\beta(d') = 0$, summed over all pairs (d, d') with $dd' = p^a$. Finally, define $\beta(\Pi p^a) = \Pi\beta(p^a)$. The β thus defined is in M by (1) above. Since α is also in M, we know $\alpha \cdot \beta \in M \cdot M \subset M$. To verify that the functions $\alpha \cdot \beta$ and ε of M are equal, it suffices, by (2) above, to observe that $(\alpha \cdot \beta)(p^a) = \varepsilon(p^a) = 0$, which is the defining equation for $\beta(p^a)$. Since the inverse of any unit is unique, the β so constructed must coincide with that obtainable by the λ construction of § 3.

7. The special multiplicative functions n^k. Define the (multiplicative) function ν_k for arbitrary real k by $\nu_k(n) = n^k$. Its inverse ν_k' is seen by the preceding construction to be: $\nu_k'(1) = 1$, $\nu_k'(n) = (-1)^l n^k$ when n is a product of l *distinct* primes, and zero otherwise.

Now (a) $\nu_k' \cdot \nu_k = \varepsilon$, and (b) if α, β are any two number-theoretic functions, we have $\beta = \alpha \cdot \nu_k$ if and only if $\alpha = \beta \cdot \nu_k'$. For the special case $k = 0$, (a) yields the familiar equation $\sum_{d|n}\mu(d) = \varepsilon(n)$, and (b) becomes the "Möbius inversion theorem" [Cf. 4; Th. 35, 38], since ν_0' is the Möbius function μ. Indeed, we may write $\nu_k'(n) \equiv \mu(n)n^k$ for all k, n.

We may note one further generalization in this direction. If α and β are any two number-theoretic functions, we see that

$$(1) \qquad \sum_{m=1}^{n} (\alpha \cdot \beta)(m) = \sum_{m=1}^{n} \sum_{d|m} \alpha(d)\beta(m/d) = \sum_{d=1}^{n} \alpha(d) \sum_{l=1}^{[n/d]} \beta(l) .$$

In particular, if β is a unit, and $\alpha = \beta'$, we obtain

$$1 = \sum_{d=1}^{n} \beta'(d) \sum_{l=1}^{[n/d]} \beta(l) .$$

Further specializing to $\beta = \nu_k$,

$$1 = \sum_{d=1}^{n} \mu(d) d^k \sum_{l=1}^{[n/d]} l^k .$$

Finally, $k = 0$ gives the familiar [4; Th. 36]

$$1 = \sum_{d=1}^{n} \mu(d)[n/d] .$$

8. The sum of the k-th powers of the divisors. It is clear that the transform $\beta(n) = \sum_{d|n}\alpha(d)$ of number theory [5, Th. 6–8] appears in our notation as $\beta = \alpha \cdot \nu_0$. Thus in particular the number theoretic function $\sigma_k(n) = \sum_{d|n} d^k$ is seen to be the (multiplicative) function $\sigma_k = \nu_k \cdot \nu_0 \in M \cdot M \subset M$. The most familiar are $\tau = \sigma_0 = \nu_0 \cdot \nu_0$, the number of divisors, and $\sigma = \sigma_1 = \nu_1 \cdot \nu_0$, the sum of the divisors.

As an illustration, note that equation (1) of the preceding section

yields

$$\sum_{m=1}^{n}(\alpha \cdot \nu_0)(m) = \sum_{d=1}^{n}\alpha(d)[n/d] ;$$

in particular, for $\alpha = \nu_0$,

$$\sum_{m=1}^{n}\tau(m) = \sum_{d=1}^{n}[n/d] ,$$

and for $\alpha = \nu_1$,

$$\sum_{m=1}^{n}\sigma(m) = \sum_{d=1}^{n}d[n/d] .$$

The inverse $\sigma'_k(n)$ is 1 for $n=1$, $(-1)^{\lambda}\Pi_i(p_i^k+2-a_i)$ for $n=p_1^{a_1}\cdots p_l^{a_l}$, where $1 \leqq a_i \leqq 2$ and $\lambda = \lambda(n)$, and zero otherwise. This may be seen from $\sigma'_k = \nu'_0 \cdot \nu'_k$ and the value of $(\nu'_0 \cdot \nu'_k)(p^a)$ obtained from § 7. For the special case $k = 0$, we may write $\tau'(n)$, for n of the second type, as $(-1)^{\lambda}2^l/a_1 \cdots a_l$.

We note that the relation $\sigma'_k = \nu'_k \cdot \nu'_0$, besides determining the function σ'_k explicitly as indicated above, yields also the equation $\sigma'_k(n) \equiv \sum_{d|n}d^k\mu(d)\mu(n/d)$, in particular $\tau'(n) \equiv \sum_{d|n}\mu(d)\mu(n/d)$.

9. A generalized φ-function. The well-known relations $\varphi \cdot \nu_0 = \nu_1$ and $\varphi = \nu'_0 \cdot \nu_1$ satisfied by the Euler φ-function [4; Th. 39, 40] suggest definition of a general function $\varphi_{k,l} = \nu'_k \cdot \nu_l$, specifically

$$\varphi_{k,l}(n) = n^l \sum_{d|n}\mu(d)d^{k-l}$$

which has the value $n^l\Pi_i(1 - p_i^{k-l})$ for $n = p_1^{a_1}\cdots p_t^{a_t}$. We should then have the relation $\nu_k \cdot \varphi_{k,l} = \nu_l$ or $\sum_{d|n}\varphi_{k,l}(d)d^{-k} = n^{l-k}$.

It is clear that the derivation of relations between arithmetic functions becomes simplified by employing the algebra of the ring Ω, or of the groups Γ or M. Consider for instance how easily $\sigma = \nu_0 \cdot \nu_1$, $\nu_1 = \nu_0 \cdot \varphi$, and $\nu_0 \cdot \nu_0 = \tau$ implies $\sigma = \tau \cdot \varphi$.

Not quite so elegant is the generalization:

(1) $$n^k\sigma_{l-k}(n) = (\nu_k \cdot \nu_l)(n) ,$$

(2) $$\nu_l = \nu_k \cdot \varphi_{k,l} ,$$

(3) $$\nu_k \cdot \nu_k(n) = n^k\tau(n) \qquad \text{(special case of (1))},$$

imply $n^k\sigma_{l-k}(n) = \sum_{d|n}d^k\tau(d)\varphi_{k,l}(n/d)$.

10. The Φ-function. Define the number-theoretic function $\Phi(n)$ to be the *sum* of the integers in N which are prime to n and do not exceed n. Obviously $\Phi(n) = n\varphi(n)/2$ unless $n = 1$ and $\Phi(1) = 1$. Although

Φ is thus a unit in Υ, $\Phi(ab) = 2\Phi(a)\Phi(b)$ for $(a, b) = 1$, $a > 1$, $b > 1$, and therefore Φ is not in M.

If we classify the integers $1, 2, \cdots, n$ according to their greatest common divisor d with n, we find in the d-class the integers a with $(a, n) = d$, $1 \leqq a \leqq n$. There are exactly as many such a as there are b with $(b, n/d) = 1$, $1 \leqq b \leqq n/d$. This yields for Landau [4; Th. 39] the relation $\sum_{d|n}\varphi(n/d) = n$ and the formula for φ by Möbius inversion. We may note that the same partition suggests the additional relation:

$$\kappa(n) = \frac{n(n+1)}{2} = \sum_{a=1}^{n} a = \sum_{d|n} d\Phi(n/d) = (\Phi \cdot \nu_1)(n) .$$

As a final example, we note that, since $\nu_1 \cdot \nu_0 = \sigma$,

$$\kappa \cdot \nu_0 = \Phi \cdot \sigma .$$

11. Primes. A number-theoretic function α is said to be a prime in case $\alpha \neq 0$, α is not a unit, and $\alpha = \beta \cdot \gamma$ implies β or γ is a unit. The associates of a prime are also prime. The remaining functions, neither 0, units, nor primes, are called composite. The associates of a composite function are composite.

Any function with $N(\alpha)$ a prime natural number is prime; more generally any function with $M(\alpha)$ a prime, or equivalently, any function with $D(\alpha) = 1$. As an example, note that from § 9 $\delta \equiv \sigma - \nu_1 = \tau \cdot \varphi - \nu_0 \cdot \varphi = (\tau - \nu_0) \cdot \varphi$. Since $\delta(1) = 0$ and $\delta(2) = 1$, we see that $M(\delta) = 2$ and so $\sigma - \nu_1$ and $\tau - \nu_0$ are associated primes. If two non-unit functions α, β are associates, we see that $\beta(p) = (\nu \cdot \alpha)(p) = \nu(1)\alpha(p)$ for all prime p, where $\nu(1) \neq 0$. Hence there is a continuum of non-associated primes even of this simple type.

Naturally there are many other kinds of primes, a fact which will become glaringly obvious in § 16.

12. The chain condition. If $\alpha_0 \neq 0$, $\alpha_1 | \alpha_0$, and in the corresponding equation $\alpha_0 = \alpha_1 \cdot \beta_1$ the (uniquely determined) β_1 is not a unit, we say α_1 properly divides α_0 and write $\alpha_1 || \alpha_0$. For example, every composite element α has a factorization $\alpha = \beta \cdot \gamma$ in which $\beta || \alpha$ and $\gamma || \alpha$. If in a domain of integrity, every chain of proper divisors $\cdots \alpha_2 || \alpha_1 || \alpha_0 \neq 0$ is finite, we say the domain satisfies the chain condition. In any such domain it is easy to see [2; p. 117] first that every α not zero and not a unit has a prime divisor, and from this that every such α is expressible as a finite product of primes.

That our ring satisfies the chain condition is an obvious consequence of the properties of either the norm or the degree functions. For example, $\alpha_1 || \alpha_0 \neq 0$, $\alpha_0 = \alpha_1 \cdot \beta_1$, β_1 not a unit, implies $D(\beta_1) > 0$ and $D(\alpha_0) = D(\alpha_1) + D(\beta_1) > D(\alpha_1)$, where D has non-negative integral values.

Having come this far, it is natural to ask whether the expression of a non-zero, non-unit number-theoretic function as a product of primes is unique (up to order and units). We have been unable to find a reference for such a theorem, and offer a proof in the remaining sections.

In the presence of the chain condition, the existence of a greatest common divisor for every two elements is necessary and sufficient for the uniqueness property. [2; p. 120]. Although we have an abundance of norms, we cannot hope to obtain a Euclidean algorithm, since we certainly could not have linear expressibility of the g.c.d. For suppose α, β are non-associated primes. Then (α, β) certainly exists and is ε. whereas a linear relation $\varepsilon = \gamma \cdot \alpha + \delta \cdot \beta$ is impossible (consider $n = 1$),

13. A reduction theorem. It simplifies matters to show first that if the uniqueness of factorization fails, it must fail in a particularly simple way. Suppose indeed that uniqueness in false in Ω. Following an argument of Lindemann and Davenport [1; § 2.11] let us divide the set of all non-zero non-unit elements of Ω into normal elements, whose factorization into primes *is* unique, and *abnormal* elements, which can be factored into primes in two essentially different ways. Clearly a prime α is normal by definition.

We prove that if α is an abnormal element of minimal norm $N(\alpha)$, and $\alpha = \sigma_1 \cdots \sigma_m = \tau_1 \cdots \tau_n$ are two essentially different factorizations of α into primes, σ_i, τ_j, then necessarily $m = n = 2$ and $\sigma_1, \sigma_2, \tau_1, \tau_2$ all have the same norm N.

Note first that neither m nor n is unity, since a prime is normal. Moreover, no σ_j is the associate of any τ_j, for if so, cancellation would produce an abnormal element of norm $N < N(\alpha)$. Without loss of generality, we may assume $N(\sigma_1) \leqq N(\sigma_2) \leqq \cdots \leqq N(\sigma_m)$, $N((\tau_1) \leqq N(\tau_2) \leqq \cdots \leqq N(\tau_n)$, and $N(\sigma_1) \leqq N(\tau_1)$. Then $N(\sigma_1 \cdot \tau_1) = N(\sigma_1) \cdot N(\tau_1) \leqq N(\tau_1)N(\tau_1) \leqq N(\tau_1)N(\tau_2) \leqq N(\alpha)$. If any one of these $(\leqq)$ relations is actually $(<)$, we have $N(\sigma_1 \cdot \tau_1) < N(\alpha)$, which we will see leads to a contradiction.

Suppose indeed that $N(\sigma_1 \cdot \tau_1) < N(\alpha)$, and consider $\beta = \alpha - \sigma_1 \cdot \tau_1$. Certainly $\beta \neq 0$, for $\alpha = \sigma_1 \cdot \tau_1$ implies $\sigma_2 \cdots \sigma_m = \tau_1$, and since τ_1 is prime, we have $m = 2$ and $\tau_1 \sim \sigma_2$, contradiction. Also β is not a unit, since $\sigma_1 | \beta$. From the definition of norm N and the assumption $N(\sigma_1 \cdot \tau_1) < N(\alpha)$ it follows that $N(\beta) = N(\sigma_1 \cdot \tau_1) < N(\alpha)$. Hence β is *normal*. However, the non-associates σ_1, τ_1 both divide β, and, β being normal, $\sigma_1 \cdot \tau_1 | \beta$. Hence $\sigma_1 \cdot \tau_1 | \alpha = \sigma_1 \cdots \sigma_m = \sigma_1 \cdot \tau_1 \cdot \gamma$. Thus $\sigma_2 \cdots \sigma_m = \tau_1 \cdot \gamma$. But $N(\sigma_2 \cdots \sigma_m) < N(\alpha)$, and $\sigma_2 \cdots \sigma_m$ is not zero and not a unit $(m \geqq 2)$. It follows that $\sigma_2 \cdots \sigma_m = \tau_1 \cdot \gamma$ is normal and τ_1 is associated with some σ_j, a contradiction.

We are forced to conclude that $N(\sigma_1)N(\tau_1) = N(\tau_1)N(\tau_1) = N(\tau_1)N(\tau_2) = N(\alpha)$ and so $N(\sigma_1) = N(\tau_1) = N(\tau_2) \equiv N$ and $n = 2$. Hence $N^2 =$

$N(\tau_1)N(\tau_2) = N(\alpha) = N(\sigma_1) \cdots N(\sigma_m) \geqq N^m$ implies $m \leqq 2$. But $m > 1$ so $m = 2$, $N(\sigma_2) = N$, and all is proved.

Thus if unique prime factorization fails in Ω, we should have an element of form $\alpha \cdot \beta = \gamma \cdot \delta$, α, β, γ, δ primes (of identical norm N) and α not associated with either γ or δ.

14. The ring of formal power series. Let the primes p of N be listed in *any* definite order $p_1, p_2, p_3, \cdots$. Then every integer n may be written uniquely in the form $n = p_1^{a_1}p_2^{a_2} \cdots$ and uniquely described by a vector $(a_1, a_2, \cdots)$ with non-negative integral components, finitely many of which are non-zero, all such vectors being realized as n ranges over N. Hence a number-theoretic function $\alpha = \alpha(n)$ may be associated with a definite "formal power series" in a countably infinite number of indeterminates $x_1, x_2, \cdots$, having coefficients in the complex field F, by means of the correspondence

$$\alpha \rightarrow P(\alpha) = \Sigma\alpha(n)x_1^{a_1}x_2^{a_2} \cdots .$$

Here, the summation extends over all $n = p_1^{a_1}p_2^{a_2} \cdots$ of N.

This correspondence is clearly one to one on Ω to the set $F_\omega = F\{x_1, x_2, \cdots\}$ of *all* such power series. Moreover, addition is preserved, and $P(\alpha \cdot \beta) = P(\alpha)P(\beta)$, the latter operation being the usual formal operation on power series involving multiplication and collection of (finite numbers of) "like terms."

Thus the ring of all number-theoretic functions is isomorphic to the ring of all formal power series $F_\omega = F\{x_1, x_2, \cdots\}$. We emphasize that the only restriction on these series is that only a *finite* number of x_i actually appear (i.e., have $a_i > 0$) in any *term*. However, infinitely many x_i may well occur (in terms with non-zero coefficients) in the *same* series, so that we have here a more general ring than that discussed by Krull [3; § 4]. Indeed, each series of Krull's ring of power series (over F) corresponds to a number theoretic function zero except on a set of integers generated by *some* finite set of primes.

15. Some preliminaries. We deal in the remainder of the paper only with the power series representation $A = A\{x_1, x_2, \cdots\} = \Sigma\alpha(n)x_1^{a_1}x_2^{a_2} \cdots$ of number-theoretic functions. The domain $F_\omega = F\{x_1, x_2, \cdots\}$ contains (in the sense of isomorphism) for every $l = 1, 2, \cdots$ the domain $F_l = F\{x_1, \cdots, x_l\}$ of power series in l "variables." For the latter domains, the theorem on unique factorization into primes is known. [3; § 4 and 6; § 2]. The units of F_l are again the series with non-zero constant term.

If l is any integer $1, 2, \cdots$ and if $A = A\{x_1, x_2, \cdots\}$ is in F_ω or some F_m with $m \geqq l$, we mean by $(A)_l$ the series $A\{x_1, \cdots, x_l, 0, 0, \cdots\}$

obtained from A by deleting all terms of A actually involving any x_i with $i > l$. Indeed, the mapping $A \to (A)_l$ is a ring homomorphism of F_ω or F_m onto F_l. One can write $A = (A)_l + A_l^*$, where the latter series involves only terms containing at least one x_i with $i > l$, and in this way one sees that $(AB)_l = (A)_l(B)_l$.

In reality all series we consider are actually in F_ω, but we do not hesitate to say $A\{x_1, \cdots, x_l, 0, 0, \cdots\}$ is "in F_l." Our objective is to throw the proof of unique factorization in F_ω back onto the rings F_l, $l = 1, 2, \cdots$, in which the theorem is known to be true. But first we have to show that the primes of F_ω are all of a special kind.

16. The nature of a prime. If a series A of F_ω is neither zero nor a unit, then there is some minimal $L = L(A)$ for which $(A)_l$ is neither zero nor a unit of F_l, $l \geqq L$. For $A\{0, 0, \cdots\} = 0$, and since $A \neq 0$, A must contain with non-zero coefficient some product $x_1^{a_1}x_2^{a_2}\cdots$ with $(a_1, a_2, \cdots) \neq (0, 0, \cdots)$. If in this term x_k is the last variable with $a_k > 0$, then $(A)_k \neq 0$. Hence there is a *minimal* L with $(A)_L \neq 0$, $L \geqq 1$. But then $(A)_l$ is not zero or a unit for any $l \geqq L$.

Now if A is not zero or a unit in F_ω, and any $(A)_l$ is prime in F_l, where of course $l \geqq L = L(A)$, then $(A)_m$ is prime in F_m for all $m \geqq l$, and also A is prime in F_ω. For example, if $(A)_m = R_mS_m$, where R_m, S_m are non-units in F_m, then $(A)_l = (A_m)_l = (R_m)_l(S_m)_l$, where neither of the latter factors in F_l are units. For such A, there is a minimal integer $P = P(A) \geqq L(A)$ such that $(A)_l$ is prime in F_l for all $l \geqq P(A)$. We say such primes are *finitely prime*.

The remaining logical possibility is that for some A, not zero or a unit, we have $(A)_l$ composite in F_l for all $l \geqq L(A)$. We shall show that such an A is composite in F_ω, and hence the

Principal Lemma: all primes of F_ω are finitely prime.

17. Proof of the principal lemma. Let A be a fixed non-zero non-unit series in F_ω with $L = L(A)$, and suppose that, for every $l \geqq L$, $(A)_l = R_lS_l$ where R_l and S_l are non-units of F_l. We say R_l and S_l are true factors of $(A)_l$ and R_lS_l is a true factorization of $(A)_l$. A true factor of $(A)_l$ is thus a non-unit proper divisor of $(A)_l$ in F_l, and so has a companion of the same kind.

We shall call any chain $[R_L, R_{L+1}, \cdots, R_M]$ of true factors of the corresponding $(A)_l$, $l = L, \cdots, M$ *telescopic* if each $R_{l-1} = R_l(x_1, \cdots, x_{l-1}, 0) = (R_l)_{l-1}$. Now observe that any true factorization $(A)_m = R_mS_m$, $m > L$ induces a true factorization of $(A)_{m-1} = ((A)_m)_{m-1} = (R_m)_{m-1}(S_m)_{m-1} \equiv R_{m-1}S_{m-1}$ and so down to $(A)_L = R_LS_L$, where the chain of true factors $[R_L, \cdots, R_m]$ *is* telescopic. Thus we have from the original assumption on A, the existence of a sequence

$$\kappa_0 = [R_{00}]$$
$$\kappa_1 = [R_{10}, R_{11}]$$
$$\kappa_2 = [R_{20}, R_{21}, R_{22}]$$
$$\vdots$$

of *telescopic* chains κ_i of *true* factors R_{ij}, $j = 0, 1, \cdots, i$ of $(A)_{L+j}$.

We want to prove the existence of an *infinite* chain of *true* factors $\kappa^* = [R_0^*, R_1^*, R_2^*, \cdots]$ which is telescopic throughout. If we could do so, we should have $(A)_{L+j} = R_j^* S_j^*$ for all $j \geqq 0$. Clearly the chain $[S_0^*, S_1^*, \cdots]$ is also telescopic, since $(R_{j-1}^* S_{j-1}^*) = (R_j^* S_j^*)_{L+j-1} = (R_j^*)_{L+j-1} \cdot (S_j^*)_{L+j-1} = R_{j-1}^* (S_j^*)_{L+j-1}$. But any infinite telescopic chain *defines* unambiguously a series of F_ω. If R^* and S^* are the (non-unit) series defined by the R_j^* and S_j^* chains, we must have $A = R^* S^*$, since we can prove identity of the left and right coefficients of any term by regarding $(A)_{L+j} = R_j^* S_j^*$ for suitable j. Thus the principal lemma would be proved.

Since unique factorization holds in F_l, there are only a finite number of classes of associates into which the true factors of any $(A)_l$ can fall. Hence (pigeon-hole principal!) an *infinite* set of the chains κ_i have their *first* entry equivalent to some *one* true factor T_0 of $(A)_L$. Choose one of these and call it κ_0'. Of *this* infinite set, there is an infinite *subset* of κ_i whose *second* entry is equivalent to some one true factor T_1 of $(A)_{L+1}$. Choose one and call it κ_1'. Continuing in this way we are led to a *subsequence* of (telescopic) chains

$$\kappa_0' = [R_{00}', \cdots]$$
$$\kappa_1' = [R_{10}', R_{11}', \cdots]$$
$$\kappa_2' = [R_{20}', R_{21}', R_{22}', \cdots]$$

each of which extends at least to the main diagonal, such that the entries on *this diagonal and below* have the property that, for each $j = 0, 1, 2, \cdots$ $R_{ij}' \sim T_j$ for all $i \geqq j$.

We can now construct the telescopic infinite chain κ^* working only with the main diagonal and the diagonal next below it, as follows. Define $R_0^* = R_{00}'$. Since $R_{10}' \sim T_0 \sim R_0^*$ in F_L, there is a unit U_L of F_L such that $R_0^* = R_{10}' U_L = (R_{11}' U_L)_L$. Define $R_1^* = R_{11}' U_L$ in F_{L+1}, and note that R_1^* is a true factor of $(A)_{L+1}$, $(R_1^*)_L = R_0^*$, and $R_1^* \sim T_1$ in F_{L+1}.

To make the process perfectly clear and to avoid a formal induction, we carry the construction through one more step. Since $R_{21}' \sim T_1 \sim R_1^*$ in F_{L+1}, there is a unit U_{L+1} of F_{L+1} such that $R_1^* = R_{21}' U_{L+1} = (R_{22}' U_{L+1})_{L+1}$. Define $R_2^* = R_{22}' U_{L+1}$ in F_{L+2} and note that R_2^* is a true factor of $(A)_{L+2}$, $(R_2^*)_{L+1} = R_1^*$, and $R_2^* \sim T_2$ in F_{L+2}. The proof of the lemma is now clear.

18. Proof of unique factorization. Suppose unique factorization into primes fails in $\Omega \cong F_\omega$. By § 13, we must have a series of the form $AB = CD$ where A, B, C, D are primes in F_ω and A is not associated with C or D. Since all primes are of finite type, there exists an integer P such that, in the equation $(AB)_l = (A)_l(B)_l = (C)_l(D)_l = (CD)_l$, $(A)_l$, $(B)_l$, $(C)_l$, $(D)_l$ are primes in F_l for all $l \geqq P$. Since factorization in each F_l is unique, $(A)_l$ must be associated with either $(C)_l$ or $(D)_l$ in F_l for each $l \geqq P$. Hence there must be an infinite increasing subsequence $\sigma = \{m\}$ of integers $m \geqq P$ such that either $(A)_m \sim (C)_m$ in F_m or $(A)_m \sim (D)_m$ in F_m for all $m \in \sigma$. Without loss of generality we may suppose the former case. Then $(A)_m = U_m(C)_m$, where U_m is a unit of F_m, for each m of σ. If $m < n$ are any two integers of the sequence σ, $U_m(C)_m = (A)_m = (A_n)_m = (U_n)_m(C_n)_m = (U_n)_m(C)_m$, and U_n is an extension of U_m by terms each of which involves a variable x_i with $i > m$ and so does not occur in U_m. Thus the sequence U_m, $m \in \sigma$ defines a unit U of F_ω, and $A = UC$, by the same type of argument used in the preceding section in showing $A = R^*S^*$. But then $A \sim C$ in F_ω, which is a contradiction. Hence *factorization into primes exists and is unique in the rings* Ω *and* F_ω, *up to order and units.*

References

1. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 3rd Ed. (1954) Oxford Univ. Press, London.
2. N. Jacobson, *Lectures in abstract algebra*, **1** (1951) D. Van Nostrand Co., N. Y.
3. W. Krull, *Beiträge zur Arithmetik kommutativer Integritätsbereiche, III. zum Dimensionsbegriff der Idealtheorie*, Math. Zeit. **42** (1937), 745–766.
4. E. Landau, *Elementary number theory*, (1927) Chelsea Pub. Co., N. Y.
5. W. J. LeVeque, *Topics in number theory*, **1** (1956), Addison-Wesley Pub. Co., Reading, Mass.
6. W. Rückert, *Zum Eliminationsproblem der Potenzreihenideale*, Math. Ann. **107** (1933), 259–281.

University of California
Los Alamos Scientific Laboratory
Los Alamos, New Mexico