ON THE UNIQUE FACTORIZATION THEOREM IN THE RING OF NUMBER THEORETIC FUNCTIONS

BY

CHIN-PI LU

1. Introduction

The set Ω of all functions $\psi(n)$ on $Z = \{1, 2, 3, \cdots\}$ into a commutative ring R with identity forms a commutative ring with identity under ordinary addition and the multiplication $*$; $(\psi * \chi)(n) = \sum_{d|n} \psi(d) \cdot \chi(n/d)$. It was proved by Cashwell and Everett [2] that when R is the field of complex numbers Ω is a unique factorization domain. In this paper we extend and prove the unique factorization theorem in Ω for a wider class of commutative rings R. The method is indirect and it uses the isomorphism between Ω and the ring of formal power series R_ω in a countably infinite number of indeterminates over R. The theorem is proved for R_ω by introducing a topology.

2. The ring of number theoretic functions

The class Ω of all number theoretic functions ψ, i.e., all functions $\psi(n)$ on the set Z of natural numbers n into a commutative ring with identity forms a commutative ring with identity under the addition $+$,

$$(\psi + \chi)(n) = \psi(n) + \chi(n),$$

and the multiplication $*$ which is called *convolution*,

$$(\psi * \chi)(n) = \textstyle\sum_{d|n} \psi(d) \cdot \chi(n/d).$$

The zero 0 and the additive inverse $-\psi$ of ψ are of course the functions defined by $0(n) = 0$ and $(-\psi)(n) = -\psi(n)$ for every n. The function E with $E(1) =$ the identity of R, $E(n) = 0$ for all $n \neq 1$, is the identity: $E * \psi = \psi * E = \psi$ for all ψ in Ω. We say that Ω is the ring of number theoretic functions over R if each function of Ω takes values from R. A function $N(\psi)$ on Ω to Z is defined by taking $N(\psi)$ to be the smallest number n for which $\psi(n) \neq 0$ if $\psi \neq 0$ and $N(\psi) = \infty$ if and only if $\psi = 0$. Clearly $N(\psi) \geqq 1$ for all ψ. If R has no zero divisors, then $N(\psi * \chi) = N(\psi) \cdot N(\chi)$ for all ψ, χ of Ω. Indeed, we find that, if $\psi \neq 0$, $\chi \neq 0$ with $N(\psi) = i$ and $N(\chi) = j$, then

$$(\psi * \chi)(i \cdot j) = \textstyle\sum_{m \cdot n = i \cdot j} \psi(m) \cdot \chi(n) = \psi(i) \cdot \chi(j) \neq 0$$

since $\psi(m) = 0$, $\chi(n) = 0$ for all $m < i$ and $n < j$.

PROPOSITION 1. *The ring Ω of number theoretic functions over a domain of integrity (i.e., a commutative domain with identity) has no zero divisors.*

Received September 3, 1963; received in revised form October 10, 1963.

Proof. If $\psi, \chi \in \Omega$ and $\psi * \chi = 0$, then $N(\psi * \chi) = N(0) = \infty$. Hence either $N(\psi)$ or $N(\chi)$ is ∞, i.e., ψ or χ is 0.

In our ring Ω, an element ψ is a unit if and only if $\psi(1)$ is a unit of R. (Cf. [2; §3].)

3. The weight topology

Let R be a commutative ring with identity, and put

$$\bar{R} = \bigcup_{i=1}^{\infty} R[x_1, x_2, \cdots, x_i].$$

We say that a non-zero monomial $cx_1^{\lambda_1}x_1^{\lambda_2} \cdots x_k^{\lambda_k}$, $c \in R$, is of weight r if $1 \cdot \lambda_1 + 2 \cdot \lambda_2 + \cdots + k \cdot \lambda_k = r$. It is easy to see that the product of two monomials, whose weights are t_1 and t_2 respectively and whose coefficients are not zero divisors, is of weight $t_1 + t_2$. For each $f \in \bar{R}$, we write

$$f = f_0 + f_1 + \cdots + f_m,$$

where each f_i is a sum of all monomials of weight i. Then we define an order function v on $\bar{R}$ as follows:

$$\begin{aligned} v(f) &= \min \{n \mid f_n \neq 0\} \quad \text{if} \quad f \neq 0 \\ &= \infty \qquad\qquad\qquad\quad \text{if and only if} \quad f = 0. \end{aligned}$$

Clearly

$$v(f + g) \geqq \min \{v(f), v(g)\} \quad \text{and} \quad v(fg) \geqq v(f) + v(g).$$

Denote by B_r the ideal of $\bar{R}$ consisting of all elements f whose order $v(f) \geqq r$, where $r = 0, 1, 2, 3, \cdots$. Evidently $\bar{R} = B_0 \supset B_1 \supset B_2 \supset B_3 \supset \cdots$, and $\bigcap_{r=0}^{\infty} B_r = \{0\}$ by the definitions of v and B_r. Now we topologize $\bar{R}$ by taking the set of ideals $\{B_r\}_{r=0}^{\infty}$ as a basis of neighborhoods of 0. Clearly $\bar{R}$ is a Hausdorff space for the induced topology. We call this topology *the weight topology of* $\bar{R}$. Let R^* be a completion of $\bar{R}$ for the weight topology. The extended topology in R^* is also called the weight topology of R^*.

4. The ring of formal power series in a countably infinite number of indeterminates

Let R be a commutative ring with an identity 1. By a formal power series in a countably infinite number of indeterminates $\{x_1, x_2, x_3, \cdots\}$ over R we mean an infinite sequence

$$f = (f_0, f_1, f_2, \cdots, f_q, \cdots)$$

of polynomials $f_q \in \bigcup_{i=1}^{\infty} R[x_1, x_2, \cdots, x_i]$, each f_q being either 0 or a sum of monomials of weight q. We define addition and multiplication of two power series

$$f = (f_0, f_1, \cdots, f_q, \cdots) \quad \text{and} \quad g = (g_0, g_1, \cdots, g_q, \cdots)$$

as follows:

$$f + g = (f_0 + g_0, f_1 + g_1, \cdots, f_q + g_q, \cdots),$$

$$f \cdot g = (h_0, h_1, \cdots, h_q, \cdots),$$

where $h_q = \sum_{i+j=q} f_i g_j$. With these definitions of addition and multiplication the set of all formal power series in a countably infinite number of indeterminates over R forms a commutative ring with the identity 1. We denote it by $R[[x_1, x_2, \cdots]]$ or R_ω. Every polynomial $f = f_0 + f_1 + \cdots + f_n$ in $\bar{R}$, where each f_i is either 0 or a form of weight i, can be identified with a formal power series $(f_0, f_1, \cdots, f_n, 0, 0, \cdots)$ in R_ω. By this identification $\bar{R}$ becomes a subring of R_ω. Every element f of R_ω can also be expressed in the form $f = (f_0, f_1, \cdots, f_q, \cdots)$, where each f_q is either 0 or a finite or infinite sum of monomials of degree q in $\bar{R}$. An order function similar to v can be defined in R_ω. This will also be denoted by v.

THEOREM 1. *For every commutative ring R with identity, R_ω is the completion of $\bar{R} = \bigcup_{i=1}^{\infty} R[x_1, x_2, \cdots, x_i]$ for the weight topology.*

Proof. Let $\bar{B}_r = \{f \in R_\omega ; v(f) \geqq r\}$. We show that $\bar{R}$ is dense in R_ω for $\bar{B}_r$-topology, i.e., the topology induced by taking $\{\bar{B}_r\}_{r=0}^{\infty}$ as a basis of neighborhoods of 0. Let $f = (f_0, f_1, \cdots, f_q, \cdots) \in R_\omega$, where each f_q is either 0 or a form of weight q. Put $F^{(n)} = (f_0, f_1, \cdots, f_n, 0, 0, \cdots)$; then clearly $F^{(n)} \in \bar{R}$ and $(F^{(n)})$ is a Cauchy sequence with f as a limit. Next we assert that R_ω is complete for $\bar{B}_r$-topology. Let $(f^{(n)})$ be a Cauchy sequence of elements of R_ω. Then for every integer $j \geqq 0$, there exists an integer $T(j)$ such that $f^{(n)} - f^{(m)} \in \bar{B}_j$ if $n, m \geqq T(j)$; hence $f_k^{(n)} = f_k^{(m)}$ for all $k < j$. Put $f = (f_0^{T(0)}, f_1^{T(1)}, f_2^{T(2)}, \cdots)$. Since each $f_q^{T(q)} \in \bar{R}$ and is of weight q, $f \in R_\omega$. We can easily see that for every j, $f_k = f_k^{(n)}$ for all $k < j$ if $n \geqq T(j)$; therefore $f^{(n)} \to f$ as $n \to \infty$ for $\bar{B}_r$-topology. Finally we show that $\bar{R}$ is a subspace of R_ω. This follows from the fact that $\bar{B}_r \cap \bar{R} = B_r$ for every r, by the definitions of $\bar{B}_r$, B_r and v. Hence R_ω is a completion of $\bar{R}$, and $\bar{B}_r$-topology is the weight topology of R_ω.

Now let $\{p_1, p_2, p_3, \cdots\}$ be the set of all prime integers (positive) arranged in the natural order. Then every integer n of Z may be written uniquely in the form $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$ for some k, where each λ_k is zero or a non-zero positive integer. Hence every number theoretic function ψ may be associated with a definite formal power series in R_ω by means of the correspondence:

$$(*) \qquad \psi \to f_\psi = \sum \psi(n) x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_k^{\lambda_k},$$

where the summation extends over all $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$ of Z; obviously the sum f_ψ can be identified with some formal power series in R_ω. We can easily verify that the correspondence is an isomorphism. As a consequence of this we have the following propositions.

PROPOSITION 2. *The ring R_ω of formal power series over a domain of integrity R is also a domain of integrity.*

PROPOSITION 3. *An element $f = (f_0, f_1, \cdots, f_q, \cdots)$ of R_ω is a unit if and only if f_0 is a unit of R.*

Now we define Z_k to be the set consisting of all integers of the form

$$p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k},$$

$\lambda_i \geqq 0$ for each $i = 1, 2, 3, \cdots, k$. Then clearly

$$Z_1 \subset Z_2 \subset Z_3 \subset \cdots \subset Z_k \subset \cdots$$

and $\bigcup_{k=1}^{\infty} Z_k = Z$. Let Ω_k be the subset of Ω consisting of those number theoretic functions ψ such that $\psi(n) = 0$ for all $n \notin Z_k$. Then, the set Ω_k is the collection of all functions on Z_k into R. It can be easily verified that $\Omega_k \cong R[[x_1, \cdots, x_k]]$ under the correspondence $(*)$.

Definition 1. Set $f = f(x_1, x_2, \cdots, x_i, \cdots) \in R_\omega$; then for any integer $j \geqq 0$ the formal power series

$$f(x_1, x_2, \cdots, x_j, 0, 0, 0, \cdots) \quad \text{in} \quad R_j = R[[x_1, x_2, \cdots, x_j]],$$

which is denoted by $(f)_j$, is called *the projection of f on R_j* (we set $R_0 = R$).

Clearly the mapping $f \rightarrow (f)_j$ is a ring homomorphism of R_ω on R_j, i.e.,

$$(f + g)_j = (f)_j + (g)_j \quad \text{and} \quad (fg)_j = (f)_j \cdot (g)_j .$$

Definition 2. A chain $[f^{(0)}, f^{(1)}, \cdots, f^{(i)}, \cdots, f^{(m)}]$ of $f^{(i)} \in R_i$ is said to be *telescopic* if $f^{(i)} = (f^{(i+1)})_i$ for each $i = 0, 1, \cdots, m - 1$.

5. The unique factorization in R_ω

We know that a domain of integrity F is a unique factorization domain if it satisfies the following conditions:

[UF1] Every non-zero non-unit element of F is a finite product of irreducible factors.

[UF2] The foregoing factorization is unique to within order and unit factors.

Unique Factorization Theorem. *Let R be a unique factorization domain of integrity such that $R_j = R[[x_1, x_2, \cdots, x_j]]$ is a unique factorization domain for every finite integer $j \geqq 1$; then so is R_ω.*

In order to prove the theorem, we need the following Proposition 4 and lemmas.

Proposition 4. *If a domain R of integrity satisfies the ascending chain condition for principal ideals, then so does R_ω.*

Proof. We show that the ring Ω of number theoretic functions over R, which is isomorphic to R_ω, satisfies the ascending chain condition for principal ideals for such R. Let $(f^{(1)}) \subseteq (f^{(2)}) \subseteq (f^{(3)}) \subseteq \cdots$ be an ascending chain of principal ideals of Ω. Without loss of generality we may assume that $f^{(1)} \neq 0$; then clearly $f^{(i)} \neq 0$ for all $i \geqq 1$. Since $(f^{(i)}) \subseteq (f^{(i+1)})$, $f^{(i+1)} \mid f^{(i)}$; hence there exists a non-zero function g_i in Ω such that $f^{(i)} = f^{(i+1)} * g_i$. Then

$$N(f^{(i)}) = N(f^{(i+1)} * g_i) = N(f^{(i+1)}) \cdot N(g_i) \neq 0.$$

So $N(f^{(i)}) \geqq N(f^{(i+1)})$ and consequently we have a descending chain of non-zero integers $N(f^{(1)}) \geqq N(f^{(2)}) \geqq N(f^{(3)}) \geqq \cdots$. Evidently there must exist non-zero integers r and k such that

$$N(f^{(r)}) = N(f^{(r+p)}) = k$$

for every $p \geqq 0$. Set $f^{(r)} = f^{(r+1)} * g_r$; then

$$0 \neq f^{(r)}(k) = f^{(r+1)}(k) \cdot g_r(1) + \textstyle\sum_{m \cdot l = k, l \neq 1} f^{(r+1)}(m) \cdot g_r(l)$$
$$= f^{(r+1)}(k) \cdot g_r(1) + 0,$$

since $N(f^{(r+1)}) = k$ and $f^{(r+1)}(m) = 0$ for all $m < k$. It follows that

$$(f^{(r)}(k)) \subseteq (f^{(r+1)}(k)).$$

Similarly

$$(f^{(n+1)}(k)) \subseteq (f^{(n+2)}(k))$$

for every $n \geqq r$. Thus we have the following ascending chain of non-zero principal ideals of R:

$$(f^{(r)}(k)) \subseteq (f^{(r+1)}(k)) \subseteq (f^{(r+2)}(k)) \subseteq \cdots.$$

Then there must exist an integer M such that $(f^{(M)}(k)) = (f^{(M+p)}(k))$ for every $p \geqq 0$. Hence $f^{(M)}(k) = \varepsilon \cdot f^{(M+p)}(k)$ for some unit ε of R. On the other hand, since $f^{(M+p)} \mid f^{(M)}$, there exists a $g \in \Omega$ such that $f^{(M)} = f^{(M+p)} * g$. Accordingly

$$f^{(M)}(k) = g(1) \cdot f^{(M+p)}(k) = \varepsilon \cdot f^{(M+p)}(k),$$

hence $\varepsilon = g(1)$; this means that g is a unit of Ω. Therefore.

$$(f^{(M)}) = (f^{(M+p)})$$

for every $p \geqq 0$.

As an immediate consequence of Proposition 4, we have the following:

LEMMA 1. *For any domain of integrity R which satisfies the ascending chain condition for principal ideals, every non-zero non-unit element of R_ω is a product of a finite number of irreducible factors.*

LEMMA 2. *Every infinite telescopic chain $[f^{(0)}, f^{(1)}, \cdots, f^{(i)}, \cdots]$ is a Cauchy sequence for the weight topology, hence has a limit in R_ω.*

Proof. Since the chain is telescopic, for every integer $i \geqq 0$ and $q > 0$, each monomial of $f^{(i+q)} - f^{(i)}$ is either 0 or contains at least one x_k with $k > i$ as a factor. Hence $f^{(i+q)} - f^{(i)} \in \bar{B}_i$, where $\{\bar{B}_r\}_{r=0}^{\infty}$ is a basis of neighborhoods of 0 which induces the weight topology of R_ω. Thus the chain is a Cauchy sequence.

Note that every $f \in R_\omega$ is a limit of a finite or infinite telescopic chain

$$[(f)_0, (f)_1, \cdots, (f)_i, \cdots].$$

The following lemma is well known.

LEMMA 3. *Let F be a domain of integrity which satisfies* [$UF1$], *then the following assertions are equivalent*:
(1) *F is a UFD.*
(2) *Any two elements of F have a g.c.d.*

LEMMA 4. *Let R be a UFD such that R_j is a UFD for every finite integer $j \geqq 1$, f, g any elements of R_ω and $D^{(j)}$ a g.c.d. of $(f)_j$ and $(g)_j$ in R_j. Then $(D^{(j+1)})_j \sim D^{(j)}$ for all $j \geqq L(f, g)$, where $L(f, g)$ is a certain non-negative integer.*

Proof. When either f or g is zero the assertion is trivial, hence we assume that f and g are non-zero. Let n be the smallest integer such that $(f)_n \neq 0$, $(g)_n \neq 0$ and i any integer $\geqq n$. Since R_i is a UFD by hypothesis, we can represent $D^{(i)}$ as a finite product of prime elements of R_i; denote by $\lambda(D^{(i)})$ the number of all prime factors (not necessarily distinct) of $D^{(i)}$. Since $(D^{(i+1)})_i$ is a factor of $D^{(i)}$, $\lambda(D^{(i)}) \geqq \lambda(D^{(i+1)})$. Note that the projection of each prime factor of $D^{(i+1)}$ on R_i may not be prime in R_i. Thus we have the following descending chain of non-negative integers:

$$\lambda(D^{(n)}) \geqq \lambda(D^{(n+1)}) \geqq \lambda(D^{(n+2)}) \geqq \cdots.$$

It follows that there exist integers l and k such that $k = \lambda(D^{(n+l+p)})$ for all $p \geqq 0$. This means that for every $j \geqq n + l$, the projection of each prime factor of $D^{(j+1)}$ on R_j is also prime and moreover $(D^{(j+1)})_j \sim D^{(j)}$. We denote $n + l$ by $L(f, g)$.

Proof of Theorem. We have seen in Lemma 1 that every non-zero non-unit of R_ω is a finite product of irreducible factors. Hence applying Lemma 3 we prove the theorem by showing that any two elements f and g of R_ω have a g.c.d. Since the assertion is trivial for the case where $f = 0$ or $g = 0$, we assume that f and g are non-zero. Let $D^{(j)}$ be a g.c.d. of $(f)_j$ and $(g)_j$ for each $j \geqq 0$, then we can construct an infinite telescopic chain

$$[D^{(L)}, D^{(L+1)}, D^{(L+2)}, \cdots]$$

with the initial term in R_L, $L = L(f, g)$, as follows. Assume that $D^{(j)}, j \geqq L$, has been defined and let $\bar{D}^{(j+1)}$ be any g.c.d. of $(f)_{j+1}$ and $(g)_{j+1}$, then

$$(\bar{D}^{(j+1)})_j \sim D^{(j)}$$

by Lemma 4; hence there must exist a unit $\varepsilon^{(j)}$ in R_j such that

$$D^{(j)} = \varepsilon^{(j)}(\bar{D}^{(j+1)})_j = (\varepsilon^{(j)}\bar{D}^{(j+1)})_j ;$$

we take $D^{(j+1)} = \varepsilon^{(j)}\bar{D}^{(j+1)}$. By Lemma 2 the telescopic chain has a limit D, say, in R_ω; note that $(D)_j = D^{(j)}$ or $(D^{(L)})_j$ according as $j \geqq L$ or $j < L$ for each $j \geqq 0$. Let $\bar{f}^{(j)}$ and $\bar{g}^{(j)}$ be two elements of R_j such that $(f)_j = \bar{f}^{(j)}(D)_j$ and $(g)_j = \bar{g}^{(j)}(D)_j$ for each $j \geqq L(f, g)$; then clearly $(\bar{f}^{(j+1)})_j = \bar{f}^{(j)}$ and $(\bar{g}^{(j+1)})_j = \bar{g}^{(j)}$. Hence we have two telescopic chains

$$[\bar{f}^{(L)}, \bar{f}^{(L+1)}, \bar{f}^{(L+2)}, \cdots] \quad \text{and} \quad [\bar{g}^{(L)}, \bar{g}^{(L+1)}, \bar{g}^{(L+2)}, \cdots]$$

with the initial terms in R_L. Let $\bar{f}$ and $\bar{g}$ be their limits in R_ω respectively, then $(\bar{f})_j = \bar{f}^{(j)}$ or $(\bar{f}^{(L)})_j$, and $(\bar{g})_j = \bar{g}^{(j)}$ or $(\bar{g}^{(L)})_j$ according as $j \geqq L$ or not respectively; hence $(f)_j = (\bar{f})_j(D)_j = (\bar{f}D)_j$ and $(g)_j = (\bar{g})_j(D)_j = (\bar{g}D)_j$ for every $j \geqq 0$. It follows that

$$f = \lim_{j\to\infty}(f)_j = \lim_{j\to\infty}(\bar{f}D)_j = \bar{f}D,$$

$$g = \lim_{j\to\infty}(g)_j = \lim_{j\to\infty}(\bar{g}D)_j = \bar{g}D$$

for the weight topology, namely D is a common divisor of f and g. Now let E be any other common divisor of f and g in R_ω; then $(E)_j$ is also a common divisor of $(f)_j$ and $(g)_j$ in R_j for each $j \geqq L(f, g)$. Since $(D)_j$ is a g.c.d. of $(f)_j$ and $(g)_j$ for such j, $(E)_j \mid (D)_j$. Hence there exists an element $\alpha^{(j)}$ in R_j such that $(D)_j = \alpha^{(j)}(E)_j$, $j \geqq L(f, g)$. It is easy to see that

$$[\alpha^{(L)}, \alpha^{(L+1)}, \alpha^{(L+2)}, \cdots]$$

is an infinite telescopic chain. Let α be its limit in R_ω, then we can conclude that $D = \alpha E$. Thus D is a g.c.d. of f and g.

COROLLARY 1. *If R is a field or a principal ideal domain or, more generally, a regular unique factorization domain, then R_ω is a UFD.* (*A regular ring is a Noetherian ring whose ring of quotient R_M is a regular local ring for every maximal ideal M of R, cf.* [3]).

COROLLARY 2. *Let R be a UFD such that the subring Ω_k of the ring Ω of number theoretic functions over R is a UFD for every finite integer $k \geqq 1$; then so is Ω. In particular, if R is a regular UFD, then Ω is also a UFD.*

After the completion of the manuscript the author found that E. D. Cashwell and C. J. Everett also generalized and proved the unique factorization theorem in the ring of number theoretic functions by a different method in their recent paper, *Formal power series*, Pacific Journal of Mathematics, vol. 13 (1963), pp. 45–64.

BIBLIOGRAPHY

1. D. A. BUCHSBAUM, *Some remarks on factorization in power series rings*, J. Math. Mech., vol. 10 (1961), pp. 749–753.
2. E. D. CASHWELL AND C. J. EVERETT, *The ring of number theoretic functions*, Pacific J. Math., vol. 9 (1959), pp. 975–985.
3. P. SAMUEL, *On unique factorization domains*, Illinois J. Math., vol. 5 (1961), pp. 1–17.
4. O. ZARISKI AND P. SAMUEL, *Commutative algebra, vol. II*, Princeton, Van Nostrand, 1960.

THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PENNSYLVANIA
UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS