J. Math. Kyoto Univ. (JMKYAZ)
13-1 (1973) 149-158

On the unique factorization theorem for formal power series II

By

Hajime NISHIMURA

(Communicated by Professor Nagata, July 31, 1972)

Let R be a ring,[1] $X=\{x_1, x_2, \cdots, x_n, \cdots\}$ be a set of infinitely many independent variables over R. We have two notions of formal power series with coefficients in R and variables in X, [1, p. 152]. The one called $\aleph_0$-*series*, is a formal sum of X-monomials with coefficients in R. The other, called *usual formal power series*, is such a $\aleph_0$-series whose homogeneous part of degree n is a finite sum for all n.

We denote by $R\{X\}_{\aleph_0}$ the ring of $\aleph_0$-series, and by $R\{X\}$ the ring of usual formal power series, which is a subring of $R\{X\}_{\aleph_0}$. In other words, $R\{X\}$ means the (X)-adic completion of the polynomial ring $R[X]$, where (X) is the ideal generated by the set X.

In this note, we shall prove that the unique factorization theorem still holds for $R\{X\}$, if R satisfies the following condition:

(*) $R\{x_1, \cdots, x_n\}$ *is a unique factorization domain, for any* n *(finite).*

The idea of the proof is as follows: Given $F\in R\{X\}$, we factorize F viewed as an element of $R\{X\}_{\aleph_0}$ into irreducible factors. Here we note that $R\{X\}_{\aleph_0}$ is a unique factorization domain, provided R satisfies (*), [1, Theorem 1]. Then we connect each irreducible factor of F, which is an $\aleph_0$-series, to a usual formal power series

1) A *ring* in this note always means a commutative ring with unity.

(Proposition 1 and 2 below).

In our theorem, X need not be a countable set, but card. X may be arbitrary. Later we shall reduce the general case to the case where card. $X=\aleph_0$, until then we assume X is a countable set.

1. Let f be an element of $R\{X\}_{\aleph_0}$, then f is written $f=f_0+f_1+\cdots$, where f_j is the homogeneous part of degree j in f, $f_0\in R$ is the constant term of f. The following reduction of f to a certain special type of $\aleph_0$-series is our essential tool. First we define

Definition. *Let $f\in R\{X\}_{\aleph_0}$. f is said to be reduced in $R\{X\}_{\aleph_0}$, when $f_0\neq 0$ and any coefficient of monomial of degree $\geqslant 1$ which actually appears in f is not divisible by f_0.*

Lemma 1. *Let $f\in R\{X\}_{\aleph_0}$ with $f_0\neq 0$. Then there exists a reduced element g in $R\{X\}_{\aleph_0}$ such that $f\sim g$.*[2)]

Proof. As in [1], we order all X-monomials by their degree and then for X-monomials of the same degree we order lexicographically. Since X is countable, all X-monomials are arranged in this order

$$m_0=1<m_1<\cdots<m_\nu<\cdots \qquad .$$

By induction on ν, we shall define a sequence of units $\{h_\nu\}_{\nu=1,2,\cdots}$, $h_\nu\in R\{X\}_{\aleph_0}$ such that

(i) the coefficient $a_\nu\in R$ of m_ν in $f\cdot h_1\cdots h_\nu$ is not divisible by f_0, if $a_\nu\neq 0$; and

(ii) h_ν has the form $h_\nu=1+c_\nu\cdot m_\nu$, $c_\nu\in R$.

Assume we have defined $h_1,\cdots,h_{\nu-1}$. If the coefficient of m_ν in $f\cdot h_1\cdots h_{\nu-1}$ is not divisible by f_0, then define $h_\nu=1$. If the coefficient of m_ν in $f\cdot h_1\cdots h_{\nu-1}$ is $f_0 b_\nu$, with $b_\nu\in R$, then we define $h_\nu=1-b_\nu\cdot m_\nu$; if follows that $f\cdot h_1\cdots h_{\nu-1}\cdot h_\nu$ does not contain the monomial m_ν.

2) $f\sim g$ means f and g are associates with each other.

Now, we consider the formal product $\prod_{\nu=1}^{\infty} h_\nu$. It is clear by (ii) above that, for any monomial m_μ, the coefficient of m_μ in a finite product $\prod_{\nu=1}^{\rho} h_\nu$ with $\rho \geqslant \mu$ is independent of the length ρ. Therefore, infinite product $\prod_{\nu=1}^{\infty} h_\nu$ defines just an element of $R\{X\}_{\aleph_0}$, which we denote by h. We note that h, with constant term 1, is a unit of $R\{X\}_{\aleph_0}$.

Set $f \cdot h = g$. Then g has the required properties; because $f \sim g$ and, for any monomial m_μ, the coefficient of m_μ in g is equal to that in $f \cdot \prod_{\nu=1}^{\mu} h_\nu$. q.e.d.

The following lemma may be well-known in the case of a finite number of variables, e.g. [2, Theorem 3]. We extend for $\aleph_0$-series, with characteristic arbitrary.

Lemma 2. *Let R be an integral domain, and K be its quotient field. Let p be the characteristic of R and ν be a natural number such that $p \nmid \nu$.*[3] *Then for any element h of $R\{X\}_{\aleph_0}$ with constant term* 1, *there corresponds unique $k \in K\{X\}_{\aleph_0}$ with constant term* 1 *such that $h = k^\nu$, i.e. $k = h^{1/\nu}$.*

Proof. Let $h = 1 + h_1 + h_2 + \cdots$, $k = 1 + k_1 + k_2 + \cdots$. The condition that $h = k^\nu$ is satisfied if and only if

$$(1) \qquad h_1 = \nu k_1, \quad h_j = \nu k_j + f_{\nu,j}(k_1, \cdots, k_{j-1}) \qquad j = 2, 3, \cdots,$$

where $f_{\nu,j}$ is an appropriate polynomial in $k_1, \cdots, k_{j-1}$ with integral coefficients. Since $p \nmid \nu$, we can solve these equations successively for $k_1, k_2, \cdots$:

$$(2) \qquad k_1 = \frac{1}{\nu} h_1, \quad k_2 = \frac{1}{\nu} h_2 - \frac{1}{\nu} f_{\nu,2}\left(\frac{1}{\nu} h_1\right), \quad \cdots. \qquad \text{q.e.d.}$$

It is noted that by (2) we see also $h^{1/\nu} \in R[1/\nu]\{X\}_{\aleph_0}$.

For a fixed n, let $R_1 = R\{x_1, \cdots, x_n\}$; and let ρ_n: $R\{X\}_{\aleph_0} \to R_1$

3) The characteristic $p \nmid \nu$ means either $p = 0$, or $p > 0$ and $p \nmid \nu$.

be the ring homomorphism to take the residue class of each element of $R\{X\}_{\aleph_0}$ modulo the ideal generated by $\{x_{n+1}, x_{n+2}, \cdots\}$ as in [1, (4)]. Let $i: R_1 \to R\{X\}_{\aleph_0}$ be natural injection. Let $Y=\{y_1, y_2, \cdots\}$ be a countable set of independent variables over R_1. We consider the ring $R_1\{Y\}_{\aleph_0}$, the following is immediate.

Lemma 3. *There is a unique ring isomorphism* $\iota: R_1\{Y\}_{\aleph_0} \to R\{X\}_{\aleph_0}$, *such that* $\iota | R_1 = i$ *and* $\iota(y_j) = x_{n+j}$ *for* $j=1, 2, \cdots$. *Moreover,* $R_1\{Y\}$ *is isomorphic to* $R\{X\}$ *by* ι.

We may assume that $R\{X\}_{\aleph_0}$ is identified with $R_1\{Y\}_{\aleph_0}$, by virtue of the above isomorphism ι. For any element $f \in R\{X\}_{\aleph_0}$, we may regard f also as an element of $R_1\{Y\}_{\aleph_0}$ and write

$$f = f_0 + f_1 + \cdots + f_r + \cdots, \tag{3}$$

where f_r is the homogeneous part of f (may be an infinite sum) of degree r in variables y's, coefficients in R_1. We note that $f \in R\{X\} = R_1\{Y\}$ if and only if every f_r in (3) is a finite sum of Y-monomials.

The following two lemmas give sufficient conditions for $f \in R\{X\}_{\aleph_0}$ to be in $R\{X\}$.

Lemma 4. [1, Lemma 2] *Let* R *be an integral domain and* $f \in R\{X\}_{\aleph_0}$, $F \in R\{X\}$. *If* $f \cdot F \in R\{X\}$, *then* $f \in R\{X\}$.

Lemma 5. *Let* R *be an integral domain,* p *be its characteristic. Let* ν *be a natural number such that* $p \nmid \nu$. *For any* $f \in R\{X\}_{\aleph_0}$, *if* $f^\nu \in R\{X\}$ *then* $f \in R\{X\}$.

Proof. We may assume $f \neq 0$. It is clear that if n is sufficiently large, $\rho_n f \neq 0$ in $R_1 = R\{x_1, \cdots, x_n\}$. We fix such a n, and identify $R\{X\}_{\aleph_0}$ with $R_1\{Y\}_{\aleph_0}$. Set $f^\nu = F \in R_1\{Y\}$. We have in $R_1\{Y\}_{\aleph_0}$

$$\left\{\begin{array}{ll} f = f_0 + f_1 + \cdots + f_r + \cdots, & \rho_n f = f_0 \neq 0 \\ F = F_0 + F_1 + \cdots + F_s + \cdots. & \end{array}\right. \tag{4}$$

Assume $f \notin R_1\{Y\}$. Let f_r be the first term in f which is not a finite sum.

Take the homogeneous part of degree r in both sides of $F=f^\nu$, and we have

$$F_r = \nu f_0^{\nu-1} f_r + \sum f_{j_1} \cdots f_{j_\nu}, \tag{5}$$

where $\sum$ means the summation taken over all lists of ν indices $(j_1, \cdots, j_\nu)$ such that $j_1 + \cdots + j_\nu = r$, $0 \leqslant j_1 < r, \cdots, 0 \leqslant j_\nu < r$.

Each of F_r, $f_{j_1} \cdots f_{j_\nu}$ in (5) is a finite sum of Y-monomials; while, $\nu f_0^{\nu-1} f_r$ is not a finite sum, since $p \nmid \nu$ and $\nu f_0^{\nu-1} \neq 0$; a contradiction. q.e.d.

2. Throughout this section we shall assume that R satisfies the condition $(*)$. We use the fact that $R\{X\}_{\aleph_0}$ is a unique factorization domain, [1, Theorem 1]. Recall that, for given $f \in R\{X\}_{\aleph_0}$, the factorization of f into irreducible factors is obtained in accordance with that of $\rho_n f$ in $R_1 = R\{x_1, \cdots, x_n\}$ with $n \gg 0$. In particular, the following statements hold true:

(6)
- a) *f is irreducible in $R\{X\}_{\aleph_0}$ if and only if $\rho_n f$ is so in R_1 for $n \gg 0$.*
- b) *f, g are relatively prime in $R\{X\}_{\aleph_0}$ if and only if $\rho_n f$, $\rho_n g$ are so in R_1 for $n \gg 0$.*

Lemma 6. *Let $f = f_0 + f_1 + \cdots$, $g = g_0 + g_1 + \cdots$ be elements of $R_1\{Y\}_{\aleph_0}$ with $f_0 \neq 0$, $g_0 \neq 0$. If f, g satisfy the following conditions:*

i) *$f \cdot g \in R_1\{Y\}$,*

ii) *f_0, g_0 are relatively prime in R_1, and*

iii) *f is reduced in $R_1\{Y\}_{\aleph_0}$;*

then both f and g are in $R_1\{Y\}$.

Proof. Put $f \cdot g = F \in R_1\{Y\}$. Assume that either f or $g \notin R_1\{Y\}$, then by Lemma 4 both $f \notin R_1\{Y\}$ and $g \notin R_1\{Y\}$. Let $f_r (, g_s)$ be the homogeneous part of the least degree which is not a finite sum, in the $\aleph_0$-series $f($, g respectively).

Taking the homogeneous part of degree r in $F=f\cdot g$, we have

(7) $$F_r=f_r\cdot g_0+(f_{r-1}g_1+\cdots f_1g_{r-1})+f_0g_r.$$

If $r\neq s$, say $r<s$, all terms except for f_rg_0 in both sides of (7) contain only a finite number of variables. Nevertheless, since $g_0\neq 0$, f_rg_0 is not a finite sum of monomials, a contradiction.

If $r=s$, there exists a monomial m which appears in f_r with non-zero coefficient, but not in each of $F_r, f_{r-1}g_1, \cdots, f_1g_{r-1}$. Let the coefficients of m in f_r, g_r be $a, b\in R_1$ respectively, with $a\neq 0$. From (7) we have $0=a\cdot g_0+b\cdot f_0$. Since f_0, g_0 are relatively prime, it follows $f_0|a$, which contradicts the assumption iii). q.e.d.

Proposition 1. *Let $f, g\in R\{X\}_{\aleph_0}$, $f\neq 0$, $g\neq 0$ and f, g be ralatively prime. If $f\cdot g\in R\{X\}$, then there exist $F, G\in R\{X\}$, such that $f\sim F$, $g\sim G$.*

Proof. By (6. b), $\rho_nf\neq 0$, $\rho_ng\neq 0$ are relatively prime in $R_1=R\{x_1, \cdots, x_n\}$, if n is sufficiently large. We fix such a n, and identify $R\{X\}_{\aleph_0}=R_1\{Y\}_{\aleph_0}$, $R\{X\}=R_1\{Y\}$, by Lemma 3. We write $f=f_0+f_1+\cdots$, $g=g_0+g_1+\cdots$ viewed as elements in $R_1\{Y\}_{\aleph_0}$, where $f_0=\rho_nf$, $g_0=\rho_ng$.

By Lemma 1, there exists a unit $h\in R_1\{Y\}_{\aleph_0}$ such that $f'=hf$ is reduced in $R_1\{Y\}_{\aleph_0}$. Let $g'=h^{-1}\cdot g$. Then the assumptions i), ii), iii) of Lemma 6 are all fulfiled by f', g'. Thus we have $f\sim f'\in R_1\{Y\}=R\{X\}$, $g\sim g'\in R_1\{Y\}=R\{X\}$, as was to be proved.

q.e.d.

Proposition 2. *Let $f\in R\{X\}_{\aleph_0}$, $f\neq 0$. If some power f^ν is an associate of an element of $R\{X\}$, then so is f itself.*

Proof. By Proposition 1, we may assume that f is irreducible in $R\{X\}_{\aleph_0}$, without loss of generality.

By (6. a), $\rho_nf\neq 0$ is irreducible in $R_1=R\{x_1, \cdots, x_n\}$, if n is sufficiently large. As before, fix such a n, identify $R\{X\}_{\aleph_0}=R_1\{Y\}_{\aleph_0}$, $R\{X\}=R_1\{Y\}$.

By Lemma 1, there exists a reduced element $g\in R_1\{Y\}_{\aleph_0}$ such that:

$$(8)\qquad \begin{cases} f\sim g=g_0+g_1+\cdots+g_r+\cdots, & g \textit{ is reduced,} \\ f_0=\rho_n f\sim g_0 \textit{ in } R_1, & \\ \textit{and hence } g_0 \textit{ is irreducible.} & \end{cases}$$

By the assumption of our proposition, there is a unit h in $R_1\{Y\}_{\aleph_0}$ such that:

$$(9)\qquad \begin{cases} hg^{\nu}\in R_1\{Y\}, & \\ h=h_0+h_1+\cdots, & h_0 \textit{ is a unit in } R_1. \end{cases}$$

For our purpose, it is enough to show that $g\in R_1\{Y\}$.

(i) Assume $\nu=p^e$, where p is the characteristic of R.

From (8), we have

$$(10)\qquad g^{\nu}=g_0^{p^e}+g_1^{p^e}+\cdots.$$

It is readily seen that g^{ν} is also a reduced element, since any coefficient in $g_j^{p^e}$ is a^{p^e} where a is some coefficient in g_j. Now apply Lemma 6 for h and g^{ν}, and we see $g^{\nu}\in R_1\{Y\}$. Therefore in (10) each $g_j^{p^e}$ is a finite sum, and hence g_j is so. Thus we see $g\in R_1\{Y\}$.

(ii) Assume $p\nmid\nu$.

If f is an associate of an element of R (constant), the assertion of our proposition is trivial; so we may assume $f\nsim$ an element of R. It follows from this $g_0\sim\rho_n f\nsim$ an element of R, if $n\gg 0$. Since any irreducible factor of $\nu\in R$[4] in R_1 is an associate of an element of R, we have $g_0\nmid\nu$.

We write the unit h of (9) as $h=h_0h'$, where $h'=1+h_0^{-1}\cdot h_1+\cdots\in R_1\{Y\}_{\aleph_0}$. By Lemma 2, there corresponds $k=h'^{1/\nu}\in R_1[1/\nu]\{Y\}_{\aleph_0}$. Then by (9), $h'g^{\nu}=(kg)^{\nu}\in R_1\{Y\}\subset R_1[1/\nu]\{Y\}$. Using Lemma 5

4) We regard ν as $\nu=\nu\cdot 1\in R$, where 1 is the unity of R. We note that $\nu\neq 0$ since $p\nmid\nu$.

for the element kg of $R_1[1/\nu]\{Y\}_{\aleph_0}$, we see that $kg \in R_1[1/\nu]\{Y\}$.

By Lemma 2, k is expressed as

$$(11) \qquad k=1+k_1+\cdots+k_s+\cdots,$$

where k_j is a homogeneous form of degree j with coefficients in $R_1[1/\nu]$. Assume $g \notin R_1\{Y\}$. Then by Lemma 4 also $k \notin R_1[1/\nu]\{Y\}$. In (8) (, in (11) respectively) let g_r(, k_s) be the first term which is not a finite sum. Taking the homogeneous part of degree r in $kg=G \in R_1[1/\nu]\{Y\}$, we have

$$(12) \qquad G_r=g_r+(k_1g_{r-1}+\cdots)+k_rg_0.$$

If $r \neq s$, say $r<s$, all terms except for g_r in both sides of (12) contain only a finite number of variables, which leads to a contradiction.

If $r=s$, there is a monomial m which appears in g_r with non-zero coefficient, but not in each of G_r, k_1g_{r-1}, $\cdots$, $k_{r-1}g_1$. Let the coefficients of m in g_r, k_r be a, $(1/\nu')b$ respectively, where $a \in R_1$, $a \neq 0$, $b \in R_1$ and ν' is some power of ν. By (12) we have

$$0=a+(1/\nu')bg_0,$$

so that

$$a\nu'=-bg_0.$$

Since g_0 is irreducible by (9), and $g_0 \nmid \nu$; we have $g_0 | a$; which contradicts the fact that g is reduced. Hence we conclude $g \in R_1\{Y\}$.

Thus we have established Proposition 2 in the cases (i), (ii). Let in general, $\nu=dp^e$, $p \nmid d$, suppose $(f^{p^e})^d \sim$ an element of $R\{X\}$. We use the result for (ii), and then that for (i), and we see $f \sim$ an element of $R\{X\}$, as was to be shown. q.e.d.

Theorem. *Let R be a ring, and X be a set of independent variables over R. Let* card. X *be arbitrary. If R satisfies the condition* (*), *then $R\{X\}$ is a unique factorization domain.*

Proof. We may assume card. $X=\aleph_0$. Indeed, if card. $X>\aleph_0$, letting Y run over all those subsets of X whose cardinality is $\aleph_0$, we have $R\{X\}=\bigcup R\{Y\}$. It is clear that any finite number of elements of $R\{X\}$ can be contained in a suitable $R\{Y\}$, and that $F\in R\{Y\}$ is irreducible in $R\{X\}$ if and only if F is so in $R\{Y\}$. From this we see that if each $R\{Y\}$ is a unique factorization domain then so is $R\{X\}$.

First we shall show

UF 1. *Every element $F\neq 0$ of $R\{X\}$ is expressed as a product of a finite number of irreducible elements.*

By means of [1, Theorem 1], we factorize F in $R\{X\}_{\aleph_0}$

$$(13)\qquad \begin{cases} F=h\prod_{i=1}^{m} q_i^{e_i} \qquad h, q_i\in R\{X\}_{\aleph_0}, \\ h \text{ is a unit, } q_i \text{ is an irreducible non-unit such that} \\ q_i\nsim q_j \text{ for } i\neq j. \end{cases}$$

By using Proposition 1 and 2 repeatedly, we can find $Q_i\in R\{X\}$, such that $q_i\sim Q_i$ for $1\leqslant i\leqslant m$. Then if follows $F=H\prod_{i=1}^{m} Q_i^{e_i}$, where H is a unit in $R\{X\}_{\aleph_0}$, and hence $H\in R\{X\}$ by virtue of Lemma 4.

Now each Q_i is irreducible in $R\{X\}$, because if it were not, Q_i would be factorized into two non-units in $R\{X\}$, and hence in $R\{X\}_{\aleph_0}$ a fortiori. This completes the proof of UF 1.

Remark. The following is also a consequence of the argument above.

$Q\in R\{X\}$ is irreducible in $R\{X\}$ if and only if it is so in $R\{X\}_{\aleph_0}$.

Proof. It is enough to show "*only if*" part. Suppose that Q is not irreducible in $R\{X\}_{\aleph_0}$. Then as in (13), $Q=h\prod_{i=1}^{m} q_i^{e_i}$ with $\sum_{i=1}^{m} e_i>1$. As above, we can find an irreducible non-unit $Q_i\in R\{X\}$ $1\leqslant i\leqslant m$, so that we have $Q=H\prod_{i=1}^{m} Q_i^{e_i}$, $\sum e_i>1$; which shows Q is not irreducible in $R\{X\}$.

Finally we shall show

UF 2. *If* $P|F\cdot G$ *with* $P, F, G \in R\{X\}$ *and if* P *is irreducible, then either* $P|F$ *or* $P|G$.

Indeed, from the assumption P is irreducible also in $R\{X\}_{\aleph_0}$, by means of Remark above. From $P|F\cdot G$, we have in $R\{X\}_{\aleph_0}$ either $P|F$ or $P|G$, since $R\{X\}_{\aleph_0}$ is a unique factorization domain. From this it follows that either $P|F$ or $P|G$ in $R\{X\}$ by Lemma 4. This completes the proof of UF 2, and hence of our theorem.

YOSHIDA COLLEGE,
KYOTO UNIVERSITY

References

[1] H. Nishimura, On the unique factorization theorem for formal power series, J. Math. Kyoto Univ., **7** (1967), 151-160.

[2] Ivan Niven, Formal power series, Amer. Math. Monthly, **76** (1969), 871-889.