Continuous Functions on Discrete Valuation Rings

Koichi Tateyama

University of Shizuoka Prefecture, Hamamatsu College 3-2-3 Nunohashi, Hamamatsu, Shizuoka, 432, Japan

Let R be a complete discrete valuation ring with finite residue field, let K be its quotient field. We construct polynomial functions $\varphi(n, a)(n = 0, 1, ...)$ such that any continuous function f from R into K has the following expansion

$$f(a) = \sum_{n=0}^{\infty} a_n \varphi(n, a)$$

where the sequence $\{a_n\} \subset K$ is uniquely determined by f and satisfies that $\lim_{n \to \infty} a_n = 0$. When $K = \mathbf{Q}_p$, if we replace $\varphi(n, a)$ by the binomial coefficient $a(a-1)\cdots(a-n+1)/n!$ we have Mahler's expansion theorem. © 1999 Academic Press

1. INTRODUCTION

Let p be a rational prime and let A be the ring of integers in a finite extension field F over $\mathbf{Q}_p$. Let $C(\mathbf{Z}_p, \text{A})$ be the space of continuous functions on $\mathbf{Z}_p$ into A, with sup norm. For any non-negative integer k we define the binomial function $\binom{a}{k}$ by

$$\binom{a}{k} = \frac{a(a-1)\cdots(a-k+1)}{k!}.$$

Since the set of positive integers is dense in $\mathbf{Z}_p$, $\binom{a}{k}$ is an element in $C(\mathbf{Z}_p, \mathbf{Z}_p)$.

The following theorem is due to Mahler [M].

THEOREM 1.1. *A function f from $\mathbf{Z}_p$ into F is continuous if and only if there exist elements $a_n \in F$ such that $\lim_{n \to \infty} a_n = 0$ and*

$$f(a) = \sum_{n=0}^{\infty} a_n \binom{a}{n}.$$

The sequence $\{a_n\}$ is uniquely determined by f.

23

In this paper we shall give a generalization of Mahler's theorem. Let R be a complete discrete valuation ring with field of fractions K and $\wp$ the prime ideal of R. We denote by $P(R, R)$ the R-module generated by polynomial functions from R into R. In Section 2 we construct an R-base of $P(R, R)$. Our base depends only on the cardinality of the residue field $R/\wp$ and a uniformizing element π of $\wp$. In Section 3 we study the closure of $P(R, R)$ in $C(R, R)$. If $R/\wp$ is a finite field (i.e., K is a local field) then we show that $P(R, R)$ is dense in $C(R, R)$. In this case, by using our base $\{\varphi(n, a)\}$, we can state the main theorem of this paper.

THEOREM 1.2. *Let F be a finite extension field over K. A function f from R into F is continuous if and only if there exist elements $a_n \in F$ such that $\lim_{n \to \infty} a_n = 0$ and*

$$f(a) = \sum_{n=0}^{\infty} a_n \varphi(n, a).$$

The sequence $\{a_n\}$ is uniquely determined by f.

We note that this theorem can be deduced from a theorem of Amice [A, pp. 143–145], but his paper does not give explicit bases in general. Our base is constructive and we give an explicit base of Amice's type (Remark in Section 2). The finite characteristic case of Theorem 1.2 follows from Carlitz–Wagner Theorem [Ca, W1, W2]. Their approach is based on the theory of Carlitz modules. We formulate their theorem in terms of Lubin–Tate groups without proofs in Section 4. Our proof of Theorem 1.2 is given in Section 3 (Theorem 3.3).

2. R-BASE OF $P(R, R)$

Let R be a complete discrete valuation ring with field of fractions K. Let f be a function from R into K. We say that f is a polynomial function if there is a polynomial $P(T) \in K[T]$ such that $P(a) = f(a)$ for any $a \in R$. We fix a uniformizing element π of R. Let p be the characteristic of the residue field $R/(\pi)$. We first suppose that $R/(\pi)$ is a finite field with $q = p^r$ elements. Then we inductively define polynomial functions $\varphi(q^t, a)$ for non-negative integers t by

$$\varphi(1, a) = a, \qquad \varphi(q, a) = \frac{a - a^q}{\pi}, \qquad \varphi(q^{t+1}, a) = \varphi(q, \varphi(g^t, a)).$$

Furthermore, for any non-negative integer $n = n_0 + n_1 q + \cdots + n_i q^r (0 \leqslant n_i \leqslant q - 1)$, we define $\varphi(n, a)$ by

$$\varphi(0, a) = 1, \qquad \varphi(n, a) = \prod_{i=0}^{r} \varphi(q^i, a)^{n_i}.$$

For any polynomial function f we denote by $\mathrm{lc}(f)$ the leading coefficient of f.

PROPOSITION 2.1. *For each $n \geqslant 0$,*

(1) $\varphi(n, a)$ *is a polynomial function from R into R;*

(2) $\deg \varphi(n, a) = n$;

(3)   *suppose $n = n_0 + n_1 q + \cdots + n_i q^r (0 \leqslant n_i \leqslant q - 1)$, then $\mathrm{ord}_\pi \mathrm{lc}(\varphi(n, a)) = -(n - s(n))/(q - 1)$, where $s(n) = n_0 + n_1 + \cdots + n_r$.*

Proof. It is easy to check (1) and (2) by our definition. If $n < q$ then $\varphi(n, a) = a^n$ and $(n - s(n))/(q - 1) = 0$. Let $t \geqslant 0$. By induction we have

$$\mathrm{ord}_\pi \mathrm{lc}(\varphi(q^{t+1}, a)) = q \, \mathrm{ord}_\pi \mathrm{lc}(\varphi(q^t, a)) - 1 = -q \frac{q^t - s(q^t)}{q - 1} - 1$$

$$= -\frac{q^{t+1} - s(q^{t+1})}{q - 1}.$$

Furthermore,

$$\mathrm{ord}_\pi \mathrm{lc}(\varphi(n, a)) = \sum_{i=0}^{r} \mathrm{ord}_\pi \mathrm{lc}(\varphi(q^i, a))^{n_i} = -\sum_{i=0}^{r} n_i \frac{q^i - 1}{q - 1} = -\frac{n - s(n)}{q - 1}. \quad \blacksquare$$

Let η be a primitive $(q-1)$th root of unity in R and $\eta(0) = 0$, $\eta(i) = \eta^i$ for $1 \leqslant i \leqslant q - 1$. For any non-negative integer $n = n_0 + n_1 q + \cdots + n_i q^r (0 \leqslant n_i \leqslant q - 1)$, we define α_n by

$$\alpha_n = \eta(n_0) + \eta(n_1) \pi + \cdots + \eta(n_i) \pi^r.$$

It is not difficult to show that $\alpha_n \equiv \alpha_m \bmod \pi^k$ if and only if $n \equiv m \bmod q^k$. For the proof of the main theorem in this section we need the following lemma.

LEMMA 2.2. *For every $n \geqslant 1$, $\mathrm{ord}_\pi \prod_{i=0}^{n-1} (\alpha_i - \alpha_n) = (n - s(n))/(q - 1)$.*

Proof. Let $n = n_0 + n_1 q + \cdots + n_i q^r$. If $\alpha_i - \alpha_n \equiv 0 \mod \pi$ then $i = n - q, n - 2q, ..., n_0$. If $\alpha_i - \alpha_n \equiv 0 \mod \pi^2$ then $i = n - q^2, n - 2q^2, ..., n_0 + n_1 q$. Hence we have

$$\operatorname{ord}_\pi \prod_{i=0}^{n-1} (\alpha_i - \alpha_n) = \frac{n - n_0}{q} + \frac{n - (n_0 + n_1 q)}{q^2} + \cdots$$

$$+ \frac{n - (n_0 + n_1 q + \cdots + n_{r-1} q^{r-1})}{q^r}$$

$$= n_1 + n_2(1 + q) + \cdots + n_r(1 + q + \cdots + q^{r-1})$$

$$= \frac{n - s(n)}{q - 1}. \quad \blacksquare$$

THEOREM 2.3.

(1) *Suppose that the residue field $R/(\pi)$ is a finite field with q elements. Then $\{\varphi(n, a)\}$ ($n = 0, 1, \ldots$) is an R-base of* P(R, R).

(2) *If $R/(\pi)$ is infinite then $\{a^n\}$ ($n = 0, 1, \ldots$) is an R-base of* P(R, R).

Proof. Let f be a polynomial function of degree n in P(R, R). Then there exist f_j ($j = 0, 1, \ldots, n$) in K such that

$$f(a) = f_0 \varphi(0, a) + f_1 \varphi(1, a) + \cdots + f_n \varphi(n, a).$$

Obviously, f_j is uniquely determined by f.

In order to prove (1) we may show that $\det\{\varphi(i, a_j)\}$ is a unit for some elements $a_0, a_1, \ldots, a_n$ in R. By elementary computations we have

$$\det\{\varphi(i, a_j)\} = \pm \begin{vmatrix} 1 & a_0 & \cdots & a_0^n \\ 1 & a_1 & \cdots & a_0^1 \\ \vdots & \vdots & \cdots & \vdots \\ 1 & a_n & \cdots & a_n^n \end{vmatrix} \times \prod_{i=0}^{n} \mathrm{lc}(\varphi(i, a_j))$$

$$= \pm \prod_{l < k} (a_l - a_k) \times \prod_{i=0}^{n} \mathrm{lc}(\varphi(i, a)).$$

We note

$$\prod_{l < k} (a_l - a_k) = \prod_{k=0}^{n} \prod_{l=0}^{k-1} (a_l - a_k).$$

We set $a_0 = \alpha_0, a_1 = \alpha_1, \ldots, a_n = \alpha_n$. By Lemma 2.2, we have

$$\operatorname{ord}_l \prod_{l < k} (\alpha_l - \alpha_k) = \sum_{k=1}^{n} \frac{k - s(k)}{q - 1}.$$

Therefore, the statement of (1) follows from Proposition 2.1.

Let f be a polynomial function from R into R. We write

$$f(a) = f_0 + f_1 a + \cdots + f_n a^n.$$

If $R/(\pi)$ is infinite then we can select $a_i (i = 0, 1, \ldots, n)$ from distinct class modulo π. Since

$$\det(a_i^j) = \pm \prod_{i < j} (a_i - a_j)$$

is a unit in R, the theorem follows. ∎

If f is an element in $P(R, R)$ then f is an R-linear combination of $\varphi(i, a) (i \leqslant \deg f)$. By comparing the leading coefficients, we have the following corollary.

COROLLARY 2.4. *Suppose $R/(\pi)$ is finite.*

(1) *Let f be an element in $P(R, R)$ of degree n. Then*

$$\operatorname{ord}_\pi \operatorname{lc}(f) \geqslant -\frac{n - s(n)}{q - 1}.$$

(2) *For a non-negative integer n let f_n be an element in $P(R, R)$ of degree n. Then $\{f_n\}$ is an R-base of $P(R, R)$ if and only if*

$$\operatorname{ord}_\pi \operatorname{lc}(f_\pi(a)) = -\frac{n - s(n)}{q - 1}$$

holds for all n.

Remark. By using α_n in Lemma 2.2, we define the following polynomials

$$Q(n, T) = \frac{(T - \alpha_0)(T - \alpha_1) \cdots (T - \alpha_{n-1})}{(\alpha_0 - \alpha_0)(\alpha_n - \alpha_1) \cdots (\alpha_n - \alpha_{n-1})}.$$

It is not difficult to prove that $Q(n, a)$ is an elements of $P(R, R)$ and

$$\operatorname{ord}_\pi \operatorname{lc}(Q(n, a)) = -\frac{n - s(n)}{q - 1}.$$

Hence $\{Q(n, a)\}$ is a base of $P(R, R)$. This fact can be also deduced from Lemma 2.2 and a theorem of Amice [A, Section 6.2, Theorem 1 and Section 2.2, Corollary 1].

3. THE COMPLETION OF P(R, R).

Let $C(R, R)$ be the space of continuous functions on R into R, with sup norm. In this section we assume that $R/(\pi)$ is finite. Then R is compact and $C(R, R)$ is complete. Now we can state the generalization of Mahler's theorem. For this proof we need the following lemma.

LEMMA 3.1.

(1) If $t \geqslant m \geqslant 1$, then $\varphi(q^m, a + u\pi^t) = \varphi(q^m, a) + u_m \pi^{t-m}$ and $u_m \equiv u \bmod \pi$.

(2) If $a \equiv b \bmod \pi^t$, then $\varphi(n, a) \equiv \varphi(n, b) \bmod \pi$ for any $n < q^t$.

Proof. We set $\varphi(a) = \varphi(q, a)$. Then

$$\varphi(a + u\pi^t) = \frac{a + u\pi^t - (a + u\pi^t)^q}{\pi} = \frac{a - a^q + u\pi^t - (a + u\pi^t)^q + a^q}{\pi}.$$

since

$$\frac{u\pi^t - (a + u\pi^t)^q + a^q}{\pi} \equiv u\pi^{t-1} \bmod \pi^t$$

we have

$$\varphi(a + u\pi^t) = \varphi(a) + u_1 \pi^{t-1} \qquad \text{and} \qquad u_1 \equiv u \bmod \pi.$$

By induction,

$$\varphi(q^m, a + u\pi^t) = \varphi(\varphi(q^{m-1}, a + u\pi^t))$$

$$= \varphi(\varphi(q^{m-1}, a) + u_{m-1}\pi^{t-m+1})$$

$$= \varphi(q^m, a) + u_m \pi^{t-m}$$

and $u_m \equiv u_{m-1} \equiv u \bmod \pi$. This proves (1).
   Let

$$n = n_0 + n_1 q + \cdots + n_n q^r (0 \leqslant n_i < q, r < t)$$

then

$$\varphi(n, a + u\pi^t) = \prod_{i=0}^{r} \varphi(q^i, a + u\pi^t)^{n_i}$$

$$= \prod_{i=0}^{r} (\varphi(q^i, a) + u_i \pi^{t-i})^{n_i} \equiv \varphi(n, a) \bmod \pi. \quad \blacksquare$$

PROPOSITION 3.2. $P(R, R)$ is dense in $C(R, R)$.

Proof. Since $\bigcap_{n \geqslant 1} \pi^n C(R, R) = \{0\}$, it is enough to prove that $P(R, R) + \pi C(R, R) = C(R, R)$. Let f be a continuos function on R into R. Since R is compact and $R/(\pi)$ discrete, there is some integer N such that

$$f(a) \equiv f(b) \bmod \pi \qquad \text{if} \quad a \equiv b \bmod \pi^N.$$

We consider the following linear equations,

$$\sum_{j=0}^{q^N-1} x_j \varphi(j, \alpha_i) = f(\alpha_i) \qquad (i = 0, 1, ..., q^N - 1),$$

where α_i is as in Lemma 2.2. Since $\det\{\varphi(j, \alpha_i)\}$ is a unit in R, we obtain the unique solution in R. Furthermore, by Lemma 3.1, we have

$$\sum_{j=0}^{q^N-1} x_j \varphi(j, a) \equiv f(a) \bmod \pi$$

for any a in R. This implies that f is an element of $P(R, R) + \pi C(R, R)$. $\quad \blacksquare$

Our proof of Proposition 3.2 is essentially due to Mahler (see [M, L, and C]). According to Proposition 3.2, we can state the following expansion theorem.

THEOREM 3.3. *Let* $\{\psi_n(a)\}$ *be an R-base of* $P(R, R)$ *and we assume that* $\deg \psi_n = n$ *for all* $n \geqslant 0$. *Suppose that F is a finite extension field over K, then any continuous function* $f \in C(R, F)$ *is uniquely of the form*

$$f(a) = \sum_{n=0}^{\infty} f_n \psi_n(a) \qquad (f_n \in F),$$

where the f_n *satisfy*

$$\lim_{n \to \infty} f_n = 0.$$

Furthermore,

$$\sup_{a \in R} |f(a)| = \sup_n |f_n|.$$

Proof. By taking a base for the field of values over K and projecting on the coordinates, it is enough to prove that any element in $C(R, K)$ is uniquely of the above form. Since R is compact, there is an integer N such that $\pi^N f(a) \in C(R, R)$. Therefore, we may assume that f is an element of $C(R, R)$. By Proposition 3.2, we have

$$f(a) \equiv \sum_{k=0}^{k(n)} f_k(n)\, \psi_k(a) \bmod \pi^n$$

for some $k(n) \geqslant 0$. Moreover,

$$\frac{1}{\pi^n} \left(f(a) - \sum_{k=0}^{k(n)} f_k(n)\, \psi_k(a) \right)$$

is an element of $C(R, R)$. Hence,

$$\frac{1}{\pi^n} \left(f(a) - \sum_{k=0}^{k(n)} f_k(n)\, \psi_k(a) \right) \equiv \sum_{k=0}^{k(n)'} g_k \psi_k(a) \bmod \pi.$$

If we set $f_k(n+1) = f_k(n) + \pi^n g_k$ and $k(n+1) = \max\{k(n), k(n)')\}$, recursively, then

$$f(a) \equiv \sum_{k=0}^{k(n+1)} f_k(n+1)\, \psi_k(a) \bmod \pi^{n+1}.$$

Let $f_k = \lim_{n \to \infty} f_k(n)$. Since $f_k \equiv 0 \mod \pi^n$ for $k > k(n)$, we have $\lim_{k \to \infty} f_k = 0$. This implies that the series

$$\sum_{n=0}^{\infty} f_n \psi_n(a)$$

is convergent and so

$$f(a) - \sum_{n=0}^{\infty} f_n \psi_n(a) \equiv f(a) - \sum_{k=0}^{k(n)} f_k(n)\, \psi_k(a) \bmod \pi^n.$$

Hence we conclude

$$f(a) = \sum_{n=0}^{\infty} f_k \psi_n(a).$$

Let $h = \min_n\{\mathrm{ord}_\pi(f_n)\}$ and $g_n = \pi^{-h} f_n$. Since $\lim_{k \to \infty} g_k = 0$, there is an integer m such that

$$\pi^{-h} f(a) \equiv \sum_{n=0}^{m} g_n \psi_n(a) \bmod \pi.$$

Furthermore, we may assume that g_m is a unit. The proof of Proposition 3.2 shows that $\{\varphi(j, a) \bmod \pi: j < q^n\}$ generates $\mathrm{Map}(R/\pi^n, R/\pi)$ as a vector space. By counting the dimension of $\mathrm{Map}(R/\pi^n, R/\pi)$ we know that $\{\varphi(j, a) \bmod \pi: j < q^n\}$ is a base of $\mathrm{Map}(R/\pi^n, R/\pi)$. Since $\{\psi_j(a)\}$ is an R-base of $\mathrm{P}(R, R)$ and $\deg \psi_n(a) = n$, $\varphi(j, a)$ is an R-linear combination of $\psi_k(a) (k \leqslant j)$. Hence $\{\psi_j(a) \bmod \pi: j < q^n\}$ is also a base of $\mathrm{Map}(R/\pi^n, R/\pi)$. Therefore there is an element $\alpha \in R$ such that $\pi^{-h} f(\alpha)$ is a unit. This implies

$$\sup_a |\pi^{-h} f(a)| = 1,$$

so

$$\sup_a |f(a)| = |\pi^h| = \sup_n |f_n|.$$

If

$$f(a) = \sum_{n=0}^{\infty} f'_n \psi_n(a)$$

is an another expansion then

$$0 = \sup_a |f(a) - f(a)| = \sup_n |f_n - f'_n|.$$

This implies the uniqueness of $\{f_n\}$. ∎

Remark. If R/π is infinite, then Proposition 3.2 is not valid. For example, let K_{nr} be the maximal unramified extension field over $\mathbf{Q}_p$ and R the ring of integers in K_{nr}. By Theorem 2.3 we can identify $\mathrm{P}(R, R)$ with the polynomial ring $R[T]$. Let $R\langle T \rangle$ be the set of all power series $g(T) = \sum_{n=0}^{\infty} b_n T^n$ in $R[[T]]$ such that $\lim_{n \to \infty} |b_n| = 0$. Furthermore, for any power series $f(T) = \sum_{n=0}^{\infty} a_n T^n R\langle T \rangle$, it is easy to check that $\sup_{a \in R} |f(a)| = \sup_n |a_n|$. Then $R\langle T \rangle$ is complete and $R[T]$ dense in $R\langle T \rangle$ with sup norm (see [B-G-R]).

The units in R have a product decomposition

$$R^\times = \mu \times U_1$$

where μ is the group of roots of unity in K_n of order prime to p and $U_1 = 1 + pR$. For each unit u we let $\omega(u)$ be its projection on μ. Furthermore, we extend ω to a function on R by $\omega(a) = 0$ when $a \equiv 0 \mod p$. It is easy to see that ω is continuous on R. Suppose $\omega(a) = f(a)$ for some element f in $R\langle T \rangle$. Since $\omega(a + up) = \omega(a)$ for any a and any u in R, we have

$$\lim_{n \to \infty} \frac{f(a + p^n) - f(a)}{p^n} = 0.$$

Obviously, ω is not a constant function. Therefore, ω is not an element of the completion of P(R, R). This implies P$(R, R) + pC(R, R) \neq C(R, R)$.

4. LUBIN–TATE GROUP AND CONTINUOUS FUNCTIONS

Let R be a complete discrete valuation ring with a finite residue class field and let $q = (R: \pi R)$. Let G be a Lubin–Tate group associated with the prime element π and for each $a \in R$, let

$$[a](T) = \sum_{n=1}^\infty C_n(a) T^n \in R[[T]]$$

be an endomorphism of G. If $\mathrm{char}(k) = 0$, it is well known to exist a unique series $e(T) \in k[[T]]$ such that $[a](e(T)) = e(aT)$ for any $a \in R$. We note that the existence of $e(T)$ in any characteristic case is essentially proved by Wiles [Wi]. By comparing coefficients of both power series $[a](e(T))$ and $e(aT)$, we have

PROPOSITION 4.1. *For each $m \geq 1$, $C_m(a)$ is a polynomial function of* $\deg C_m(a) \leq m$. *If* $m = q^r$, *then* $\deg C_m(a) = m$ *and* $\mathrm{ord}_\pi lc(C_m(a)) = -(m - s(m))/(q - 1)$.

Now for each non-negative integer r, we set $D(q^r, a) = C_{q^r}(a)$, and for $n = n_0 + n_1 q + \cdots + n_i q^i (0 \leq n_i < q)$ we set $D(n, a) = \prod_{i=0}^t C_{q^i}(a)^{n_i}$. From Corollary 2.4 and Theorem 3.3, we have the following theorem.

THEOREM 4.2. *Any continuous function $f \in C(R, F)$ is uniquely of the form*

$$f(a) = \sum_{n=0}^\infty f_n D(n, a) \qquad (f_n \in F),$$

where $D(0, a) = 1$.

We note that Carlitz–Wagner's theorem is a special case of Theorem 4.2 (for details, see [Ca, W1, W2, Th, and see also [H])

REFERENCES

[A]   Y. Amice, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964), 117–180.
[B-G-R]   S. Bosch, U. Güntzer, and R. Remmert, "Non-Archimedean Analysis," Springer-Verlag, Berlin/New York, 1984.
[C]   J. W. S. Cassels, "Local Fields," Cambridge Univ. Press, Cambridge, UK, 1986.
[Ca]   L. Carlitz, A set of polynomials, *Duke Math. J.* **6** (1940), 486–504.
[H]   D. Hayes, Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189** (1974), 77–91.
[L]   S. Lang, "Cyclotomic Fields," Springer-Verlag, Berlin/New York, 1978.
[L-T]   J. Lubin and J. Tate, Formal complex multiplication in local fields, *Ann. of Math.* **81** (1965), 380–387.
[M]   K. Mahler, "p-adic Numbers and Their Functions," Second Edition, Cambridge Tracts in Math., Vol. 76, Cambridge Univ. Press, Cambridge, UK, 1984.
[Th]   D. Thakur, Zeta measure associated to $\mathbf{F}_q^\beta[T]$, *J. Number Theory* **35** (1990), 1–17.
[W1]   C. Wagner, Interpolation series for continuous functions on π-adic completions of $GF(q, x)$, *Acta Arith.* **17** (1971), 398–406.
[W2]   C. Wagner, Linear operators in local fields of prime characteristic, *J. Math.* **251** (1971), 153–160.
[Wi]   A. Wiles, Higher explicit reciprocity laws, *Ann. of Math.* **107** (1978), 235–254.