静岡県立大学短期大学部
研究紀要 12–3 号（1998 年度）– 1

Lubin-Tate 形式群と Carlitz-Wagner の定理

舘山光一

Lubin-Tate group and Carlitz-Wagner theorem

TATEYAMA, Koichi

1. 序

k を局所体, R を k の整数環, K を k の有限次拡大体とする。$C(R, K)$ を R 上定義され K 上に値をとる連続関数全体とする。$C(R, K)$ は sup-norm により完備なノルム空間となる。本稿の目的は, $C(R, K)$ の base の構成法を示すことにある。ここで, base とは単にベクトル空間のそれとしてではなく, Banach 空間の base をさすものとする。即ち, $\{v_i\}$ が Banach 空間 H の base であるとは

a. $\{v_i\}$ はベクトル空間の base である。

b. $\{v_i\}$ によって生成される H の部分空間は H 内で dense である。

ということを意味する。

$C(R, K)$ の base を最初に構成したのは Amice([A])で, Newton polygon を利用している。Amice の証明の基礎となるのは $R = \mathbf{Z}_p$ の場合に証明された有名な Mahler の定理([M])である。 Amice の結果の欠点は, base の存在は示しているが構成していないという点であると思われるが, 実は数列に関する簡単な命題をひとつ入れると, explicit な構成になっている。また、一つの base が構成されると, 多項式関数の集合が base となる条件を導くことができることから, 本質的にはほぼ explicit な構成をしているといってよいであろう。多項式関数全体が $C(R, K)$ 上 dense であることは, 本質的には Mahler によって証明されている。従って, $C(R, K)$ の base を構成することは, Banach 空間 $C(R, K)$ の base となるような多項式関数全体の base を構成することに等しい（詳細は [T] を参照)。ここで述べるのは, 値域が R に含まれる多項式関数全体（ 以下 $P(R, R)$ と書くことにする） の base を Lubin-Tate 群の endomorphism の係数を用いて記述することである。Mahler の用いた二項関数は, formal multiplicative group の endomorphism の係数になっている。もちろん, すべての Lubin-Tate 群の場合にうまくいくというわけではない。係数を直接使えるのは Mahler の場合に限られ, 一般には係数の一部を使って base の構成をすることになる。この方法を, 有限体上の一変数冪級数環に適用すると Carlitz-Wagner の定理([W1], [W2]) が導かれる。

本稿の具体的な内容は次のようになる。 最初に Lubin-Tate 群の endomorphism の係数を用いて $P(R, R)$ の base を構成する。次に, Carlitz module と Lubin-Tate group の関係を

述べ， その系として Carlitz-Wagner の定理の証明を述べる。尚， これらの内容は "Continuos Functions on Discrete Valuation Rings（Journal of Number Theory に掲載予定）" に結果だけ述べてある。以下この論文は（[T]）と書いて引用する。

2. Lubin-Tate group と連続関数

R を剰余体が有限体となる complete discrete valuation ring, k をその商体とする。また, $\wp$ を R の maximal ideal, π を $\wp$ の素元とする。ここで, $f(T)$ を次の条件を満たす R 係数の冪級数とする。

(a) $f(T) \equiv T^q \mod \wp$

(b) $f(T) \equiv \pi T \mod \deg 2$

q は剰余体 $R/\wp$ の元の数を表すこととする。このとき， R の元 α に対して $[\alpha](T) \in R[[T]]$ と $A(X, Y) \in R[[X, Y]]$ が存在し

(c) $[\alpha](T) \equiv \alpha T \mod \deg 2$

(d) $A([\alpha](X), [\alpha](Y)) = [\alpha](A(X, Y))$

を満たす（cf. [LT]）。$[\alpha](T)$ の T^n の係数を $C_n(\alpha)$ 即ち

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

とすると， $[\alpha](T)$ は任意の R の元 α に対して存在するので $\alpha \to C_n(\alpha)$ によって R 上の関数を定義することができる。この関数を $C_n(a)$ と書くことにすると、次の命題が成立する。

命題 2.1 n を自然数とするとき,

(1) $C_n(a)$ は $\deg C_n(a) \le n$ となる多項式関数である。

(2) $n = q^t$ のとき， $\deg C_n(a) = n$ かつ $\operatorname{ord}_{\wp} \operatorname{lc}(C_n(a)) = -\dfrac{n - s(n)}{q-1}$ である。

ここで， $\operatorname{lc}(F)$ は多項式 $F \in k[a]$ の最高次の係数を表し， $n = n_0 + n_1 q + n_2 q^2 + \ldots\ldots + n_r q^r$ $(0 \le n_i \le q-1)$ と q-進展開したとき $s(n) = n_0 + n_1 + n_2 + \ldots\ldots + n_r$ を表すものとする。

この命題を証明するためには， 任意の $\alpha \in R$ に対し次の条件を満たす冪級数 $e(T) \in k[[T]]$ が必要になる。

$$e(\alpha T) = [\alpha](e(T)), \quad e(0) = 0$$

k の標数が 0 の場合は formal group の一般論から $e(T)$ の存在が知られているが([S]), 一般の場合は次のようにしてその存在を示すことができる。

$\lambda(T) \in k[[T]]$ を， $\lambda(e(T)) = e(\lambda(T)) = T$ を満たすものとすると， 上の関係式は $\lambda([\alpha](T)) = \alpha\lambda(T)$ と同値になる。 $\lambda(T)$ が存在すれば， $e(T)$ が存在することは明らかであるから， 次

の Wiles の補題を証明すればよい。ただし， Wiles の論文では標数が 0 の場合しか扱っていないが，証明を読むと補題は標数と関係なく成立することが容易にわかる。尚，後半部分の内容が Wiles のものと若干異なっているが，本質的には同じである。

補題 1（Wiles[W]）

$\dfrac{[\pi^n](T)}{\pi^n} = \sum_{m=1}^{\infty} l_m(n) T^m$ とおくと， $\lim_{n\to\infty} l_m(n) = l_m$ は存在し， $\lambda(T) = \sum_{m=1}^{\infty} l_m T^m$ とおくと， $\lambda([\alpha](T)) = \alpha\lambda(T)$ を満たす。

証明）前半の部分の証明は Wiles の論文（[W]）または Lang の本（[L]）を参照されたい。ここでは後半を証明する。

$$\frac{[\pi^n]([\alpha](T))}{\pi^n} = \frac{[\alpha]([\pi^n](T))}{\pi^n}$$

$$= \sum_{m=1}^{\infty} \frac{C_m(\alpha)}{\pi^n} ([\pi^n](T))^m$$

$$= \alpha \frac{[\pi^n](T)}{\pi^n} + \sum_{m=2}^{\infty} \frac{C_m(\alpha)}{\pi^n} ([\pi^n](T))^m$$

より， 最後の和が 0 に収束すればよい。この補題の前半部分より，

$$\lim_{n\to\infty} \frac{([\pi^n](T))^2}{\pi^n} = \lambda(T) \times 0 = 0 .$$

$m \geq 3$ の場合も同様である。よって補題 1 は証明された。

命題 2.1 の証明）

$e(T) = \sum_{n=1}^{\infty} e_n T^n$ とおいて， $e(aT) = [a](e(T))$ の係数を比較すると

$$a^N e_N = \sum_{m=1}^{N} C_m(a)\, t_N(m) = C_N(a) + \sum_{m=1}^{N-1} C_m(a)\, t_N(m)$$

となる。ここで， $t_N(m)$ は $(e(T))^m$ を展開したときの T^N の係数である。$e_1 = 1$ より， $\deg C_1(a) = 1$ である。上の等式より， 帰納法で $\deg C_N(a) \leq N$ が導かれる。ここで， n を自然数とするとき， 多項式関数 $\varphi(n, a)$ を次のように定義する。

$$\varphi(1, a) = a, \quad \varphi(q, a) = \frac{a - a^q}{\pi}, \quad \varphi(q^{t+1}, a) = \varphi(q, \varphi(q^t, a)) \ (t = 0, 1, 2, \dots)$$

$n = n_0 + n_1 q + n_2 q^2 + \dots + n_r q^r \ (0 \leq n_i \leq q - 1)$ のとき， $\varphi(n, a) = \prod_{i=1}^{r} \varphi(q^i, a)^{n_i}$

このとき， 次の命題が証明できる。証明は，（[T]; Prop. 2.1, Th.2.3. Lemma 3.1）参照。

命題 2.2 (1) $\deg \varphi(n, a) = n$ かつ $\mathrm{ord}_{\wp}\mathrm{lc}(\varphi(n, a)) = -\dfrac{n - s(n)}{q-1}$ である。

(2) $\{\varphi(n, a)\}$ は $P(R, R)$ の R-加群としての基底となる。ただし, $\varphi(0, a) = 1$ とする。

(3) $n < q^t$ のとき $\varphi(n, \pi^t) \equiv 0 \bmod \pi$ かつ $\varphi(q^t, \pi^t) \equiv 1 \bmod \pi$

この命題を用いると $\deg C_N(a) \le N$ より, $C_N(a)$ は次のように表すことができる。

$$C_N(a) = \sum_{i=1}^{N} d_i \varphi(i, a) \quad (d_i \in R)$$

よって, $N = q^t$ のときは

$$C_N(\pi^t) = \sum_{i=1}^{N} d_i \varphi(i, \pi^t) \equiv d_N \equiv 1 \mod \pi$$

となる。従って, $C_N(a)$ は N 次の多項式関数となり, $\mathrm{ord}_{\wp}\mathrm{lc}(C_N(a)) = \mathrm{ord}_{\wp}\mathrm{lc}(\varphi(N, a))$ であるから, 命題 2.1 が証明された。

以上の証明より, $P(R, R)$ の基底の構成はほとんど完了している。即ち,

$$D(0, a) = 1, \quad D(q^t, a) = C(q^t, a) \ (t = 1, 2, ...)$$

$n = n_0 + n_1 q + n_2 q^2 + ... + n_r q^r \ (0 \le n_i \le q-1)$ のとき, $D(n, a) = \prod_{i=1}^{r} C(q^i, a)^{n_i}$

とすると,

定理 2.3 $\{D(n, a)\}$ は R-加群としての $P(R, R)$ の基底であり, Banach space としての $C(R, R)$ の base である。

証明）$\deg D(n, a) = n$, $\mathrm{ord}_{\wp}(\mathrm{lc}(D(n, a)) = \dfrac{n - s(n)}{q-1}$ より $P(R, R)$ の基底である（[T], Cor.2.4）。また, $\deg D(n, a) = n$ より $C(R, R)$ の base となる（[T], Th.3.3）。

注意）$g(a)$ を $C(R, k)$ の元とすると, R は compact であるから適当な R の元 α によって $\alpha g(a) \in C(R, R)$ となる。従って, $\{D(n, a)\}$ は $C(R, k)$ の base となる。また, F を k の有限次拡大体とすると, F の k 上の基底を適当に取ることにより容易に $\{D(n, a)\}$ が $C(R, F)$ の base になることを証明することができる。

3. Carlitz-module

ここでは, $\mathbf{F}_q$ を元の個数が q である有限体, $A = \mathbf{F}_q[t]$ とする。k^{ac} を k 代数閉包とするとき, $\mathrm{End}(k^{ac})$ を $\mathbf{F}_q$-algebra としての endomorphism 全体とする。Carlitz （[C]）は次のようにして $\phi : A \to \mathrm{End}(k^{ac})$ の homomorphism を与えた。

$$\phi(t)(u) = u^q + tu, \quad \phi(c)(u) = cu \quad (u \in k^{ac}, \quad c \in \mathbf{F}_q)$$

ここで M を A の元とするとき,

$$\phi(M)(u) = \{M\}(u) \quad (\forall u \in k^{ac})$$

という式で $A[T]$ の元 $\{M\}(T)$ を定める。例えば, $\{t\}(T) = T^q + tT$ となる。Lubin-Tate group との関係という観点から考えると, 次の命題が基本的となる。

命題 3.1 M を A の元とすると,

(1) $\{M\}(X+Y) = \{M\}(X)+\{M\}(Y)$

(2) $\{M\}(T) \equiv MT \mod \deg 2$

(3) M が既約多項式ならば, $\{M\}(T) \equiv T^{q'} \mod M$。ここで, $q' = q^{\deg M}$ である。

証明） (1) は定義より明らか。

(2) は $\{t\}(T) \equiv tT \mod \deg 2$, $\{c\}(T) = cT$ $(c \in \mathbf{F}_q)$ より明らか。

(3) は Hayes ([H]) によって, $\{M\}(T)$ が Eisenstein polynomial であることが証明されている。よって, 最高次の係数以外は M で割り切れる。また, 帰納的に $\deg \{M\}(T) = q^{\deg M}$ も容易に証明できる。

以上で, 命題 3.1 は証明された。

P を既約な A の元とする。K を k の素イデアル (P) 上での完備化, R を A の closure とする。$\mathbf{F} = \mathbf{F}_{q'}$ $(q' = q^{\deg P})$とおくと, $K = \mathbf{F}((P))$, $R = \mathbf{F}[[P]]$ と表すことができる。Lubin-Tate によると（[LT]）, $\{P\}(T) \in \mathrm{End}_R(G)$ を満たす R 上の formal group $G = G(X, Y)$ はただ一つ存在する（当然 G は formal additive group になる）。また, 任意の元 $M \in R$ に対し

$$\{P\}(\psi(T)) = \psi(P\{T\}), \quad \psi(T) \equiv MT \mod \deg 2$$

を満たす R 係数の冪級数 $\psi(T)$ がただ一つ存在する。以下この元を $[M](T)$ と書くことにする。まず, 定義より $\{P\}(T) = [P](T)$ である。さらに, M が A の元ならば $\{M\}(T)$ の定義および命題 3.1 の(2) より, 上の 2 つの条件を満たすことから $\{M\}(T) = [M](T)$ である。よって, Carlitz module の一般論は局所的には Lubin-Tate group の一般論として扱うことができる。この場合, $\{M\}(e(T)) = e(MT)$ を満たす冪級数 $e(T) \in K[[T]]$ は Carlitz によって explicit に構成されている（[C]）。Carlitz によると, $e(T)$ は linear な項だけでできている冪級数である。即ち,

$$e(T) = \sum_{n=0}^{\infty} e_{q'^n} T^{q'^n}$$

となる。命題 2.1 の証明より

命題 3.2 $\mathrm{ord}_P\, e_{q'^n} = -\dfrac{q'^n - 1}{q' - 1}$

また, 定理 2.3 のように $D(n, M)$ を構成すると $\{D(n, M)\}$ は $C(R, K)$ の base となる。

これが Carlitz-Wagner の定理である（[W1], [W2]）。

4. Lubin-Tate group と *p*-adic measure

本稿の目的は Carlitz-Wagner の定理を Carlitz-module からではなく，Lubin-Tate group を用いて証明することにあった。それはすでに終わっているが，ここで何故 Lubin-Tate group をもちだしたか若干の説明をしておきたい。

記号は以前と同じに R を局所体の整数環，k をその商体，$\wp$ を R の prime ideal とする。ここで，$C(R, R)$ から R への R-linear map を R 上の measure と呼ぶことにする。正確に言えば non-archimedean measure とか呼ぶべきなのであろうが，通常の measure はここでは扱わないので混乱は生じないと思われる。尚，k の標数が 0 の場合は剰余体の標数 p を用いて p-adic measure と一般的には呼ばれているが，今回は標数が正の場合も含まれるのでこれは用いないこととする（表題を除いて！）。また，一般論から言えば $C(R, k)$ から k への k-linear map で bounded なものを measure とするべきだが，適当に定数倍することにより $C(R, R)$ から R への map とすることができるので，この定義を採用することとする。次に，$M(R)$ を R 上の measure 全体とする。以下述べるように，Lubin-Tate group を用いると $M(R)$ から $R[[T]]$ への R-linear map を構成できるというのが本節の主張である。そのために，Lubin-Tate group を 1 つ固定し $[a](T)$ や $e(T)$ 等は今までと同じ意味で使用する。$M(R)$ の元を δ，$C(R, R)$ の元を h とするとき $\delta(h)$ を今までの習慣に従って

$$\int h(a)\, d\delta = \int_R h(a)\, d\delta(a)$$

と表すこととする。このとき，R-linear map $L : M(R) \to R[[T]]$ を次のように定義する。

$$L(\delta)(T) = \int d\delta + \sum_{n=1}^{\infty} T^n \int C_n(a)\, d\delta$$

$L(\delta)(T) = f(T)$ のとき，$\delta = \delta_f$ と書くことにすると次の等式が成立する。

M1: $\int [a](z)\, d\delta_f = f(z) - f(0) \quad (z \in \wp)$

M2: $e_k \int a^k\, d\delta_f(a) = \left(\dfrac{d}{dT}\right)^k f(e(T))\Big|_{T=0} \quad (k \geq 0)$

ここで，$s \in \mathbf{Z}_p$ とするとき $L(s, f)$ を次のように定義する。

$$L(s, \quad f) = \lim_{\substack{n \to s \\ n \to \infty}} \int a^n\, d\delta_f(a)$$

ここで極限は，n は正の整数で $\mathbf{Z}_p$（p は $R/\wp$ の標数）の中では s に収束し，実数としては無限大になるように選ぶものとする。この関数は，formal group が formal multiplicative group，f として Bernoulli 数の生成関数を選ぶと $\mathbf{Q}$ 上の p-進 L-関数（余分な factor は出てくる）になることが知られている。また，formal group として虚数乗法を

もつ楕円曲線の torsion point から構成されるものを選び, f として楕円単数から構成された Coleman power series の対数をとり, その上に reduction が ordinary の場合は, 量指標をもつ虚二次体上の L-関数の p-adic 化になる。これらの結果から予想すると, この関数 $L(s, f)$ はいろいろな L-関数の p-adic 化を表す可能性がある。可能性というのには次のような理由がある。実は $L(s, f)$ を用いて構成できている例は formal multiplicative group $\mathbf{G}_m$ の場合に限られている。 虚数乗法を持つ楕円曲線の場合でも, reduction が ordinary ならば formal group は係数を拡大すれば $\mathbf{G}_m$ になることが知られている。M1, M2 は reduction が supersingular の場合でも当然成立する。冪級数 $f(T)$ は reduction に関係なく構成されている。問題は $L(\delta) = f$ となる measure δ の存在が言えないのである。$\mathbf{G}_m$ のみ endomorphism を標準的にとれば R-linear map L が同型写像となることが証明できる。Lang はこの場合の L を Iwasawa isomorphism と呼んでいる。$\deg C_n(a) = n$ がすべての n について言えれば L は injective になる。onto になるためには $\{C_n(a)\}$ が $C(R, R)$ の base にならなくてはならない。例えば $L \otimes k$ が onto になるような Lubin-Tate group の存在だけでも証明されれば, p-進 L-関数の理論も豊かになるであろう。

References

[A] Y.Amice, Interpolation *p*-adique, *Bull.Soc.Math.France* 92(1964), 117-180

[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, 1978

[LT] 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 ed.). Cambridge tracts, 76. Cambridge University Press (1984)

[S] J.H.Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1985

[T] K.Tateyama, Continuous functions on discrete valuation rings.

[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

[W] A. Wiles, Higher explicit reciprocity laws, *Ann. of Math*. **107**(1978), 235-254

（1998 年　12 月 21 日　受理）