p 進 L 関数セミナー

$\sim$ *Iwasawa Theory of Elliptic Curves with Complex Multiplication* $\sim$

目次

第 I 部

FORMAL GROUPS, LOCAL UNITS, AND MEASURES

1 RELATIVE LUBIN-TATE GROUPS

以下, R を単位的可換環とする. ここでは形式群の基本的事実を述べていくが, 形式群とは群ではなく演算を表すベキ級数のことなので, ややこしくないようこの pdf では**形式群則**と書くことにする.

Definition 1.1 (形式群則)**.** R 上の**形式群則** $F \in R[[X,Y]]$ とは, 以下の公理を満たすものである.

- $F(X,Y) \equiv X+Y \bmod \deg 2$.
- $F(X,0) = X, F(0,Y) = Y$.
- $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (結合法則).
- $F(X,Y) = F(Y,X)$ (交換法則).
- $^{\exists!}\iota(X) \in R[[X]]$ such that $F(X,\iota(X)) = 0$ (逆元).

ただし $f \equiv g \bmod \deg n$ とは, f と g が $n-1$ 次の項まで一致するということ, すなわち $\deg(f-g) \geq n$ を意味する.

形式群の条件の 2 つ目と 5 つ目は他の条件から導くことができる. しかしめんどくさいので定義に含めておいた.

Example 1.2 (加法群則)**.** $\hat{\mathbb{G}}_a(X,Y) := X+Y$ と定めると, すぐ分かるようにこれは形式群則の公理を満たす. この $\mathbb{G}_a \in R[[X,Y]]$ を**加法 (形式) 群則**という. ちなみに $\iota(X) = -X$ である.

Example 1.3 (乗法形式則)**.** $\hat{\mathbb{G}}_m(X,Y) := X+Y+XY = (X+1)(Y+1)-1$ と定めると, すぐ分かるように形式群則の公理を満たす. この $\mathbb{G}_m \in R[[X,Y]]$ を**加法 (形式) 群則**という. ちなみに $\iota(X)$ は $\hat{\mathbb{G}}_m(X,Y) = 0$ を Y について解けばいいので

$$\iota(X) = \frac{1}{1+X} - 1 = (1 - X + X^2 - X^3 + \dots) - 1 = -X + X^2 - X^3 + \dots$$

となる.

A を R 代数でイデアル $\mathfrak{a}$ について完備かつ分離的であるとする. すなわち $A \cong \varprojlim_n A/\mathfrak{a}^n$ とする. (この本で想定しているのは $A = R[[X]], \mathfrak{a} = (X)$ または $A = R, \mathfrak{a} = (R \text{ の極大イデアル})$ である.) このとき $f, g \in \mathfrak{a}$ に対して加法と逆元を

$$f[+]g := F(f,g), \quad [-]f := \iota(f)$$

と定める. このとき A が $\mathfrak{a}$ について完備であることから演算 $[+]$ は閉じている, すなわち $(\mathfrak{a}, [+])$ は群となる. 通常の加法と区別するために, これを $F(\mathfrak{a})$ と書く.

> 演算 $[+]$ が $\mathfrak{a}$ で閉じていることを示す. 形式群則を $F = \sum_{i,j\geq 0} c_{ij} X^i Y^j \in R[[X,Y]]$, また, $f, g \in \mathfrak{a}$ とする. このとき $F(f,g) = \sum_{i,j\geq 0} c_{ij} f^i g^j \in \mathfrak{a}$ を示したい. まず A が完備であることから $F(f,g) \in A$ となることは分かる. 次に, $F(f,g) = \lim_n (\sum_{i,j=1}^n c_{ij} f^i g^j)$ であって, $\sum_{i,j=1}^n c_{ij} f^i g^j \in \mathfrak{a}$ である. 従って $\mathfrak{a}$ の点列が $\mathfrak{a}$ に収束するか, つまり $\mathfrak{a}$ が閉集合であることを見ればよい. 今, $\{\mathfrak{a}^n\}_n$ を 0 の開近傍として設定していて, 位相環では開集合は閉集合なので, ok.

Definition 1.4 (形式群則の準同型)**.** R 上の形式群則 $F, G \in R[[X,Y]]$ に対して

$$G(f(X), f(Y)) = f(F(X,Y)) \qquad (\text{すなわち } f(X)[+]_G f(Y) = f(X[+]_F Y))$$

を満たす $f \in XR[[X]]$ のことを, F から G への R 上の**準同型**という. F から G への R 上の準同型全体の集合を $\mathrm{Hom}_R(F,G)$ とか, R を省略して $\mathrm{Hom}(F,G)$ と書く. 特に $F = G$ のときは $\mathrm{End}(F)$ と書く.
また, $f \in \mathrm{End}(F)$ に対して $g \in \mathrm{End}(F)$ が存在して $g \circ f(X) = f \circ g(X) = X$ が成り立つとき, f を同型写像という. 同型写像全体を $\mathrm{Aut}(F)$ と書く.

以下の演算により $\mathrm{Hom}(F,F')$ には群, $\mathrm{End}(F)$ に環の構造が入る.

$$f[+]g=(X\mapsto f(X)[+]_G g(X)),\quad fg=(X\mapsto (f\circ g)(X))$$

加法単位元は 0 であり, 加法逆元は $\iota(X)$, 乗法単位元は X である.

Definition 1.5 (cf. [3, 定義 1.4.1]). $R[[X]]:=R[[X_1,\dots,X_n]]$ とする. R 準同型 $D:R[[X]]\to R[[X]]$ が R **導分**であるとは

$$^\forall f,g\in R[[X]],\ D(fg)=D(f)g+fD(g)$$

を満たすことをいう. R 導分全体を $\mathrm{Der}_R(R[[X]])$ と書き, 自然に $R[[X]]$ 加群の構造が入る. また, $R[[X]]$ 加群の $\mathrm{Der}_R(R[[X]])$ の双対, すなわち

$$\hat{\Omega}^1_{R[[X]]/R}:=(\mathrm{Der}_R(R[[X]]))^*=\mathrm{Hom}_{R[[X]]}\left(\mathrm{Der}_R(R[[X]]),R[[X]]\right)$$

を形式 **1-微分形式**という.

Proposition 1.6 (cf. [3, 定義 1.4.1]). $R[[X]]=R[[X_1,\dots,X_n]](=\varprojlim_m R[X]/I_m)$ に対し, $\mathrm{Der}_R(R[[X]])$ は, $\frac{\partial}{\partial X_i}(X_j)=\delta_{ij}$ となる $\frac{\partial}{\partial X_i}$ を基底にもつ $\mathrm{rank}\,n$ の自由 $R[[X]]$ 加群である. 従って特に $\hat{\Omega}^n_{R[[X]]/R}$ も, $dX_i(\frac{\partial}{\partial X_j})=\delta_{ij}$ なる dX_i を基底とする $\mathrm{rank}\,n$ の自由加群である.

Proof. I_m を m 次斉次多項式全体のなすイデアルとする. このとき導分の定義より任意の $D\in\mathrm{Der}_R(R[[X]])$ に対し $D(I_m)\subset I_{m-1}$ ($^\forall m\in\mathbb{Z}$) が成り立つ. よって D は $R[[X]]$ の位相に関して連続なので $f=\sum_{i_1,\dots,i_n}a_{i_1,\dots,i_n}X_1^{i_1}\cdots X_n^{i_n}\in R[[X]]$ とすると

$$\begin{aligned}D(f)&=\sum_{i_1,\dots,i_n}a_{i_1,\dots,i_n}D(X_1^{i_1}\cdots X_n^{i_n})\\&=\sum_{j=1}^n\left(\sum_{i_1,\dots,i_n}X_1^{i_1}\cdots\widehat{X_j}^{i_j}\cdots X_n^{i_n}\cdot\frac{\partial}{\partial X_j}(X_j^{i_j})\right)D(X_j)\\&=\sum_{j=1}^n D(X_j)\frac{\partial f}{\partial X_j}\end{aligned}$$

よって $\frac{\partial}{\partial X_j}:f\mapsto\frac{\partial f}{\partial X_j}$ と対応させる導分を基底にもつ. 一次独立は容易に示せるので省略する. □

定義 1.5 より, 双線形な pairing

$$(\cdot,\cdot):\mathrm{Der}_R(R[[X]])\times\hat{\Omega}^1_{R[[X]]/R}\to R[[X]];(D,\omega)\mapsto\omega(D)$$

を得る. このとき $a_i,b_i\in R[[X]]$ に対して

$$\left(\sum_{i=1}^n a_i\frac{\partial}{\partial X_i},\sum_{i=1}^n b_i dX_i\right)=\sum_{i,j}a_ib_jdX_j\left(\frac{\partial}{\partial X_i}\right)=\sum_{i=1}^n a_ib_i$$

と計算できる.

Definition 1.7 (cf. [3, 定義 1.4.3]). $f(X_1,\dots,X_n)\in R[[X_1,\dots,X_n]], f(0)=0,\omega=u(X)dX\in\hat{\Omega}^1_{R[[X]]/R}$ とする. このとき

$$f^*\omega:=u\left(f(X_1,\dots,X_n)\right)\left(\frac{\partial f}{\partial X_1}dX_1+\cdots+\frac{\partial f}{\partial X_n}dX_n\right)$$

と定める. ただし, $\frac{\partial}{\partial X_i}$ は通常の偏微分である. 特に $u(X)=1$ のとき $df:=f^*dX$ とする. ($n=1$ のとき $f^*\omega=u(f(X))f'(X)dX$ となる.) さらに $f\in\mathrm{Hom}_R(F,G)$ のとき $f^*\omega$ を ω の f による**引き戻し (pull back)** という.

$\omega = u(X)dX \in \hat{\Omega}^1_{R[[X]]/R}$ とおき, $D := \omega^* = u(X)\frac{d}{dX} \in \mathrm{Der}_R(R[[X]])$ とする. ただし双対の双対は元に戻ることに注意. このとき

$$^\forall f(X) \in XR[[X]],\ Df = u(f(X))\frac{df}{dX} = u(f(X))f'(X)\frac{d}{dX}$$

であるから $(Df)^* = u(f(X))f'(X)dX = f^*\omega$ となることを述べておく.

Example 1.8. $f(X) = e^X - 1 = \sum_{n\geq 1}\frac{X^n}{n!} \in \mathbb{Q}[[X]]$ とおくと $f \in \mathrm{Hom}_{\mathbb{Q}}(\hat{\mathbb{G}}_a, \hat{\mathbb{G}}_m)$ である. (指数法則 $e^{X+Y} = e^Xe^Y$ より.) このとき $\omega = \frac{1}{X+1}dX = \sum_{n\geq 1}(-X)^n dX$ とおくと, ω の f による引き戻しは

$$f^*\omega = \frac{1}{f(X)+1}f'(X)dX = \frac{1}{e^X}e^X dX = dX$$

と計算できる. (実は ω は $\hat{\mathbb{G}}_m$ の不変微分と呼ばれる性質の良いものであって, dX は $\hat{\mathbb{G}}_a$ の不変微分となっている. つまり今計算したものは「$f \in \mathrm{Hom}_R(F, G)$ と G の不変微分 ω に対して, その引き戻し $f^*\omega$ は F の不変微分である」という事実の具体例となっている. その命題は命題 1.13 で, 例は例 1.11 で挙げる.)

Definition 1.9 (cf. [3, 定義 2.3.1]). $F(X,Y) \in R[[X,Y]]$ を形式群則, T を X, Y と独立な変数, $\varphi_T(X) := F(X,T) \in (R[[T]])[[X]]$ とおく. このとき

- $D \in \mathrm{Der}_R(R[[X]])$ が F の不変導分 $\overset{\mathrm{def}}{\iff}$ $^\forall f \in R[[X]], D(f\circ\varphi_T) = Df(\varphi_T)$.
- $\omega \in \hat{\Omega}^1_{R[[X]]/R}$ が F の不変微分 $\overset{\mathrm{def}}{\iff}$ $\omega^* \in \mathrm{Der}_R(R[[X]])$ が不変導分 $\overset{\mathrm{iff}}{\iff}$ $\varphi_T^*\omega = \omega$.

と定義する. F の不変微分全体の集合を $\hat{\Omega}^{\mathrm{inv}}_{F/R}$ と書き, 自然に R 加群の構造が入る. また, $\omega = u(X)dX \in \hat{\Omega}^{\mathrm{inv}}_{F/R}$ が**正規化された不変微分**であるとは, $u'(0) = 1$ であることとする.

$\omega = u(X)dX$ が不変微分であることをチェックするのは, 微分形式をいじることになるため少しやっかいである. しかし以下の計算により, べき級数 $u(X)$ をいじるだけで不変微分であるかどうかの判断が出来ることが分かる.

$$\varphi_T^*\omega = \omega \iff u(F(X,T))F_X(X,T)dX = u(X)dX \iff u(F(X,T))F_X(X,T) = u(X) \tag{1.10}$$

以降の命題の証明では上の式を多用する.

Example 1.11. dX は $\hat{\mathbb{G}}_a$ の不変微分である. 実際, $u(X) = 1, \varphi_T(X) = \hat{\mathbb{G}}_a(X,T) = X + T$ であるから

$$u(\hat{\mathbb{G}}_a(X,T))\hat{\mathbb{G}}_{aX}(X,T) = 1\cdot 1 = u(X)$$

が成り立つので (1.10) より ok. また, $\frac{1}{1+X}dX$ は $\hat{\mathbb{G}}_m$ の不変微分である. 実際, $u(X) = \frac{1}{1+X}, \varphi_T(X) = \hat{\mathbb{G}}_m(X,T) = X + T + XT$ であるから

$$u(\hat{\mathbb{G}}_m(X,T))\hat{\mathbb{G}}_{mX}(X,T) = \frac{1}{1+X+T+XT}(1+T) = \frac{1}{1+X} = u(X)$$

が成り立つので (1.10) より ok. $\hat{\mathbb{G}}_m$ の不変導分は $(1+X)\frac{d}{dX}$ である.

$F(X,Y) \in R[[X,Y]]$ を形式群則とし, $\psi(Y) := F_X(0,Y)^{-1}$ とおく. このとき $F_X(0,0) = 1$ であるから $\psi(Y) \in R[[Y]]^\times$ である.

Proposition 1.12 ([3, 命題 2.3.2]). $\omega \in \hat{\Omega}^1_{R[[X]]/R}$ のとき, 以下は同値である.

- ω は形式群則 F の不変微分.
- $^\exists c \in R$ such that $\omega = c\psi(X)dX$.

従って $\hat{\Omega}^{\mathrm{inv}}_{R[[X]]/R}$ は rank 1 の自由 R 加群である.

Proof. $[\Rightarrow]$ $\omega = f(X)dX$ とおく．このとき ω が不変微分となる必要十分条件は

$$f(F(X,T))F_X(X,T) = f(X)$$

であった．((1.10)) 両辺 $X=0$ を代入すれば $f(T)F_X(0,T) = f(0)$, すなわち $f(T) = f(0)\psi(T)$ が得られ, ok.

$[\Leftarrow]$ 形式群則の結合法則 $F(F(X,Y),Z) = F(X,F(Y,Z))$ の両辺を X で微分すると

$$F_X(F(X,Y),Z)F_X(X,Y) = F_X(X,F(Y,Z))$$

を得る．$X=0$ を代入することで

$$F_X(Y,Z)F_X(0,Y) = F_X(0,F(Y,Z)) \iff F_X(Y,Z)F_X(0,F(Y,Z))^{-1} = F_X(0,Y)^{-1} \iff F_X(Y,Z)\psi(F(Y,Z)) = \psi(Y)$$

が得られる．従って (1.10) より ok. □

Proposition 1.13. F,G を R 上の形式群則, $f \in \mathrm{Hom}_R(F,G), \omega_G \in \hat{\Omega}^{\mathrm{inv}}_{G/R}$ とする．このとき $f^*\omega_G \in \hat{\Omega}^{\mathrm{inv}}_{F/R}$ が成り立つ．特に $\omega^{\mathrm{inv}}_F, \omega^{\mathrm{inv}}_G$ が正規化不変微分ならば $f^*\omega^{\mathrm{inv}}_G = f'(0)\omega^{\mathrm{inv}}_F$ が成り立つ．従って f は不変微分の準同型

$$f^* : \hat{\Omega}^{\mathrm{inv}}_{G/R} \to \hat{\Omega}^{\mathrm{inv}}_{F/R}; \omega_G \mapsto f^*\omega_F$$

を誘導する．

Proof. $\omega_G = u(X)dX, \varphi_T = F(X,T)$ とおく．このとき最初の主張は $\varphi_T^*(f^*\omega_G) = f^*\omega_G$ を示せばよい．

$$\begin{aligned}
\varphi_T^*(f^*\omega_G) &= \varphi_T^*(u(f(X))f'(X)dX) \quad (\because f^*\text{の定義}) \\
&= u(f(F(X,T)))f'(F(X,T))F_X(X,T)dX \quad (\because \varphi_T^*\text{の定義}) \\
&= u(G(f(X),f(T)))f'(F(X,T))F_X(X,T)dX \quad (\because f \in \mathrm{Hom}_R(F,G)) \\
&= u(f(X))G_X(f(X),f(T))^{-1}f'(F(X,T))F_X(X,T)dX \quad (\because \omega_G\text{は不変微分より } u(G(X,T))G_X(X,T) = u(X)) \\
&= u(f(X))G_X(f(X),f(T))^{-1}G_X(f(X),f(T))f'(X)dX \quad (\because f(F(X,T)) = G(f(X),f(T)) \text{ の両辺を } X \text{ で微分}) \\
&= u(f(X))f'(X)dX
\end{aligned}$$

となって ok. 二つ目の主張を示す．まず命題 1.12 より, ある $c \in R$ を用いて $f^*\omega^{\mathrm{inv}}_G = c\omega^{\mathrm{inv}}_F$ と書ける．ω^{inv}_G は正規化されているので $f^*\omega^{\mathrm{inv}}_G = u(f(X))f'(X)dX = (f'(0)X + \dots)dX$ であるが, ω^{inv}_F も正規化されているので $c\omega^{\mathrm{inv}}_F = (cX + \dots)dX$ という形をしている．よって $c = f'(0)$ でなければならない．ok. □

Proposition 1.14. R を標数 0 の環, $R_{\mathbb{Q}} := R \otimes_{\mathbb{Z}} \mathbb{Q}$ として $R \subset R_{\mathbb{Q}}$ とみなし, さらに $F(X,Y)$ を R 上の形式群則とする．このとき $\lambda \in \mathrm{Hom}_{R_{\mathbb{Q}}}(F, \hat{\mathbb{G}}_a)$ を F の**形式対数関数**という．特に $\lambda'(0) = 1$ のとき**正規化された形式対数関数**という．

Example 1.15. $f(X) = \log(1+X)$ は $\hat{\mathbb{G}}_m$ の形式対数である．確かに

$$f(\hat{\mathbb{G}}_m(X,Y)) = f((1+X)(1+Y)-1) = \log((1+X)(1+Y)) = \log(1+X) + \log(1+Y) = \hat{\mathbb{G}}_a(f(X),f(Y))$$

となっている．

$\omega = f(X)dX \in \hat{\Omega}^1_{R[[X]]/R}$ に対して

$$\exists! F(X) \in R_{\mathbb{Q}}[[X]] \text{ such that } F'(X) = f(X), \quad F(0) = 0$$

が成り立つ．(形式的に $f(X)$ を積分すればよい．その際積分定数のずれが生じるが, $F(0)=0$ により存在が一意に定まる．) この $F(X)$ を ω の**原始関数**といい, $F_\omega(X)$ と表す．

Proposition 1.16. F を R 上の形式群則とする. このとき以下は全単射である.

$$\Phi : \{\lambda : F \text{ の形式対数} \mid \lambda'(0) \in R\} \xrightarrow{1:1} \hat{\Omega}^{\mathrm{inv}}_{F/R}; \quad \lambda \mapsto \lambda'(X)dX$$

逆写像は $\Psi : \omega \mapsto F_\omega$ で与えられる. 特に左辺は $\mathrm{rank}\,1$ の R 自由加群であって, 正規化形式対数と正規化不変微分が対応する.

Proof. [Φの well-defined] $\lambda(X) \in R_{\mathbb{Q}}[[X]]$ を F の形式対数で $\lambda'(0) \in R$ を満たすものとする. このときまず $\omega := \lambda'(X)dX$ が $F/R_{\mathbb{Q}}$ の不変微分であること, すなわち $\lambda'(F(X,T))F_X(X,T) = \lambda'(X)$ を示せばよい. さて, 定義から $\lambda \in \mathrm{Hom}_{R_{\mathbb{Q}}}(F, \hat{\mathbb{G}}_a)$ であるから

$$\lambda(X[+]_F T) = \lambda(X) + \lambda(T)$$

が成り立つ. 両辺 X で微分することで $\lambda'(F(X,T))F_X(X,T) = \lambda'(X)$ となるので ok. あとは ω が"R 上の"不変微分であること, すなわち $\lambda'(X)$ が R 係数であることを見ればよい. $\omega^{\mathrm{inv}} \in \hat{\Omega}^1_{F/R}$ を正規化不変微分とすると命題 1.12 より $c \in R_{\mathbb{Q}}$ を用いて $\omega = c\omega^{\mathrm{inv}}$ と書ける. この両辺の初項を見比べれば $\lambda'(0) \in R$ より $c = \lambda'(0) \in R$ が分かる. ok.

[Ψの well-defined] $\omega = f(X)dX \in \hat{\Omega}^{\mathrm{inv}}_{F/R}$ に対して $F_\omega \in \mathrm{Hom}_R(F, \hat{\mathbb{G}}_a)$, すなわち $F_\omega(F(X,Y)) = F_\omega(X) + F_\omega(Y)$ を示す. まず ω は不変微分なので (1.10) より $f(F(X,Y))F_X(X,Y) = f(X)$ が成り立つ. F は形式群則なので X と Y を入れ替えてもよく, $f(F(X,Y))F_Y(X,Y) = f(Y)$ が成り立つ. 得られたこの二つの式を足し合わせることで

$$F^*\omega = fdX + fdY$$

が得られる. 従って両辺積分することで, ある $c \in R_{\mathbb{Q}}$ を用いて $F_\omega(F(X,Y)) = F_\omega(X) + F_\omega(Y) + c$ が成り立つ. さらに $X = 0$ を代入することで $c = 0$ が分かる. あとは $F'_\omega(0) \in R$ を示せばよい. $F'_\omega(0) = f(0) \in R$ であるから ok.

[互いに逆写像] 微分積分学の基本定理である. ちゃんと計算すると,

$$\Phi \circ \Psi(\omega) = \Phi(F_\omega) = F'_\omega(X)dX = f(X)dX = \omega$$
$$\Psi \circ \Phi(\lambda) = \Psi(\lambda'(X)dX) = \lambda(X)$$

である. □

Proposition 1.17. $\mathrm{Der}_R(F)$ を F の不変導分全体とする. $D \in \mathrm{Der}_R(F)$ と不変微分 $\omega \in \hat{\Omega}^{\mathrm{inv}}_{F/R}$ に対して $(D,\omega) \in R$ であり, 特に $(\cdot,\cdot) : \mathrm{Der}_R(F) \times \hat{\Omega}^{\mathrm{inv}}_{F/R} \to R$ は不変導分と不変微分に関して perfect pairing である. すなわち $\omega \in \hat{\Omega}^1_{R[[X]]}$ が任意の $D \in \mathrm{Der}_R(F)$ に対して $(D,\omega) \in R$ ならば $\omega \in \hat{\Omega}^{\mathrm{inv}}_{F/R}$ かつ $D \in \mathrm{Der}_R(R[[X]])$ が任意の $\omega \in \hat{\Omega}^{\mathrm{inv}}_{F/R}$ に対して $(D,\omega) \in R$ ならば $D \in \mathrm{Der}_R(F)$.

Corollary 1.18. R を標数 0 の環, F を R 上の形式群則, λ を F の正規化形式対数とする. このとき任意の F の不変導分 D は

$$^{\exists}c \in R \text{ such that } D = \frac{c}{\lambda'(X)}\frac{d}{dX}$$

と表せる. つまり F の不変導分全体の集合は $\frac{c}{\lambda'(X)}\frac{d}{dX}$ を基底とする $\mathrm{rank}\,1$ の R 自由加群である.

Proof. $D = f(X)\frac{d}{dX}$ と表し, $\omega \in \hat{\Omega}^{\mathrm{inv}}_{F/R}$ とすると, ある $c \in R$ により $\omega = c\lambda'(X)dX$ と書ける. よって命題 1.17 より $(D,\omega) = c\lambda'(X)f(X) \in R$ となる, すなわち $f(X) = \frac{c'}{\lambda'(X)}$ $(c' \in R)$ となる. □

Proposition 1.19. R を標数 0 の環とする. このとき以下が成り立つ.

- $R_{\mathbb{Q}}$ 上の形式群則は同型を除いて $\hat{\mathbb{G}}_a$ のみ. 特に標数 0 の体上の形式群則は $\hat{\mathbb{G}}_a$ のみ.
- $f(X) \in XR_{\mathbb{Q}}[[X]]$ を $f'(0) = 1$ を満たすベキ級数とする. このとき

$$F(X,Y) := f^{-1}\left(f(X) + f(Y)\right)$$

は $R_{\mathbb{Q}}$ 上の形式群則である.

Proof. (1) F を $R_{\mathbb{Q}}$ 上の形式群則, $\lambda(X)$ を F の正規化対数とする. 定義から $\lambda \in \mathrm{Hom}_{R_{\mathbb{Q}}}(F, \hat{\mathbb{G}}_a)$ であるから, あとは λ が可逆であること, すなわち $\lambda'(0) \in R_{\mathbb{Q}}^{\times}$ を示せばよい. しかし λ は正規化されているので $\lambda'(0) = 1 \in R_{\mathbb{Q}}^{\times}$ である. ok.

(2) $f^{-1}(X) \equiv X \bmod \deg 2$ に気を付けて計算するだけ.

$$\begin{aligned}
&F(X,Y) \equiv f(X) + f(Y) \equiv X + Y \mod \deg 2\\
&F(X,0) = f^{-1}(f(X)) = X \quad (\because f(0) = 0)\\
&F(F(X,Y),Z) = f^{-1}(f(X) + f(Y) + f(Z)) = F(X,F(Y,Z))
\end{aligned}$$

□

Definition 1.20. F を R 上の形式群則とする. このとき $^{\forall}n \in \mathbb{Z}$ に対して $[n]_F \in \mathrm{End}_R(F)$ を

$$[n]_F(X) := \begin{cases} \underbrace{X\ [+]_F \dots [+]_F\ X}_{n\text{ 個}} & (n > 0)\\ 0 & (n = 0)\\ \underbrace{\iota(X)\ [+]_F \dots [+]_F\ \iota(X)}_{n\text{ 個}} & (n < 0) \end{cases}$$

と定義する. これを F における n **倍写像**という.

$F(X,Y) \equiv X + Y \bmod \deg 2, \iota(X) \equiv -X \bmod \deg 2$ に注意すると $[n]_F \equiv nX \bmod \deg 2$ が得られる. 以下の命題により

$$\mathrm{Hom}_R(F,G) \to R; f = aX + \cdots \mapsto f'(0)$$

は単射である. このとき $[a]_{F,G} := f$ と書くことがあるが, $a \in \mathbb{Z}$ のときは上の写像の意味での $[a]_F := [a]_{F,F}$ と, a 倍写像という意味の $[a]_F$ は一致する.

Proposition 1.21. R を標数 0 の環, $f \in \mathrm{Hom}_R(F,G)$ とする. このとき以下は単射準同型である.

$$[a]_{F,F'} : \mathrm{Hom}_R(F,F') \to R; f = aX + \cdots \mapsto a$$

Proof. $f \in \mathrm{Hom}_R(F,G)$ とする. まず命題 1.16 より

$$\varphi : \mathrm{Hom}_R\left(\hat{\Omega}^{\mathrm{inv}}_{G/R}, \hat{\Omega}^{\mathrm{inv}}_{F/R}\right) \longrightarrow R; (\omega_G \mapsto f^*\omega_G = c\omega_F) \to c$$

なる R 加群の準同型が誘導される. $c = 0$ ならば $(\omega_G \to 0)$ なので φ は単射. 全射を示す. (???) 従ってあとは

$$\mathrm{Hom}_R(F,G) \to \mathrm{Hom}_R(\hat{\Omega}^{\mathrm{inv}}_{G/R}, \hat{\Omega}^{\mathrm{inv}}_{F/R}); f \mapsto \tilde{f}$$

が単射であることを示せばよい. $\tilde{f} = 0$, すなわち $\tilde{f}(\omega_G) = 0$, すなわち $f^*(\omega_G) = 0$ と仮定する. $\omega_G = u(X)dX$ と書くと $u(f(X))f'(X) = 0$ が成り立たなければならない. $f(X) \in XR[[X]]$ であることを考えると $f(X) = 0$ しかなり得ない. よって単射. ok. (あとでちゃんとやる.)

□

Proposition 1.22. $p \in \mathbb{Z}$ を素数とする. このときある $f(X), g(X) \in R[[X]]$ が存在して

$$[p]_F(X) = pf(X) + g(X^p)$$

が成り立つ.

Proof. $\omega^{\mathrm{inv}} := u(X)dX \in \hat{\Omega}^{\mathrm{inv}}_{F/R}$ を形式群則 F/R の正規化不変微分とする. このとき命題 1.16 より

$$p\omega^{\mathrm{inv}} = [p]_F^* \omega^{\mathrm{inv}} = u\left([p]_F(X)\right)[p]'_F(X)dX$$

が成り立つ. 従って $pu(X) = u\left([p]_F(X)\right)[p]'_F(X)$ を得る. ここで, $u'(0) = 1$ より $u(X), u\left([p]_X(X)\right) \in R[[X]]^\times$ なので

$$[p]'_F(X) = pu(X)u\left([p]_X(X)\right)^{-1} \in pR[[X]]$$

となる. $[p]_F(X) = \sum_{n\geq 1} a_n X^n$ とおけば, $p \not| n$ のとき $a_n \in pR$ とならなければならないので, f と g の存在が分かる. □

Definition 1.23. R を標数 $p > 0$ の環, $F(X, Y)$ を R 上の形式群則とする. このとき

$$F \text{ が高さ } h \text{ をもつ} \overset{\text{def}}{\iff} {}^\exists f \in R[[X]] \text{ such that } [p]_F(X) = f\left(X^{p^h}\right), \quad f'(0) \neq 0$$

と定義する. このような f が存在しないとき F の高さは ∞ とする.

Example 1.24. R を標数 $p > 0$ とする. このとき $[p]_{\hat{\mathbb{G}}_a}(X) = pX = 0$ より $\hat{\mathbb{G}}_a$ の高さは ∞ である. また, $[p]_{\hat{G}_m}(X) = (1 + X)^p - 1 = X^p$ となることが簡単に確かめられるから $\hat{\mathbb{G}}_m$ の高さは 1 である.

Proposition 1.25. R を標数 $p > 0$ の環, F を R 上の形式群則とする. このとき F は必ず高さをもつ.

Proof. まず命題 1.25 より, ある $f(X) \in R[[X]]$ が存在して $[p]_F(X) = f(X^p)$ が成り立つ. ここで, $F^{(p)}(X, Y), f^{(p)}(X)$ のように書いたら $F(X, Y), f(X)$ の係数をそれぞれ p 乗したものを表すことにする. このとき

- $(F(X, Y))^p = F^{(p)}(X^p, Y^p)$, 特に $F^{(p)}$ は R 上の形式群則
- $f : F^{(p)} \to F$: hom

が成り立つ. 実際, 前半はすぐ分かり, 後半は

$$f\left(F^{(p)}(X^p, Y^p)\right) = f\left(F(X, Y)^p\right) = [p]_F\left(F(X, Y)\right) = F\left([p]_X(X), [p]_F(Y)\right) = F(f(X^p), f(Y)^p)$$

において $X^p \mapsto X, Y^p \mapsto Y$ とすることで分かる. さて, $\omega^{\mathrm{inv}} \in \hat{\Omega}^{\mathrm{inv}}_{F/R}$ を正規化不変微分とする. もし $f'(0) \neq 0$ なら F の高さは 1 である. $f'(0) = 0$ ならば命題 1.13 より $f^*\omega^{\mathrm{inv}} = (1 + \ldots)f'(X)dX = 0$ となる. 従って $f'(X) = 0$ を得るので, ある $f_1(X) \in R[[X]]$ が存在して $f(X) = f_1(X^p)$ と書ける. $[p]_F(X) \neq 0$ ならばこれらの操作は有限回で止まらなければならないので, 必ず高さは存在する. □

以下の記号を統一して用いる.

- $k/\mathbb{Q}_p$: 有限次拡大
- $\mathcal{O}$: k の付値環, すなわち正規化乗法付値 $\nu : k \to \mathbb{Z} \cup \{\infty\}$ に対し $\mathcal{O} = \{x \in k \mid \nu(x) \leq 1\}$
- $\wp$: $\mathcal{O}$ の (唯一の) 極大イデアル, すなわち $\wp = \{x \in k \mid \nu(x) < 1\}$
- $q := \#(\mathcal{O}/\wp) < \infty$
- k'/k: d 次不分岐拡大
- k^{ur}/k: k の最大不分岐拡大
- k^{ur} の完備化, すなわち $\mathcal{O}_{k^{ur}}$ の極大イデアル $\mathfrak{m}$ から定まる $\mathfrak{m}$ 進距離による完備化
- $\mathcal{O}', \mathfrak{p}', \mathcal{O}^{ur}, \mathfrak{p}^{ur}$: 対応するそれぞれ

- $v : K^\times \to \mathbb{Z}$: 正規化付値
- $\varphi \in G(k^{ur}/k)$: Frobenius かつ位相的生成元, すなわち $^\forall x \in \mathcal{O}^{ur}$, $\varphi(x) \equiv x^q \bmod \mathfrak{p}^{ur}$ を満たし $G(k^{ur}/k) = \overline{\langle\varphi\rangle}$
  この φ を K に延長する, すなわち $^\exists\tilde{\varphi} \in G(K/k)$ such that $\tilde{\varphi}|_{k^{ur}} = \varphi$ として, この $\tilde{\varphi}$ も φ と書く.

Definition 1.26. $v(\xi) = d$ となる $\xi \in k^\times$ を一つ固定する. このとき

$$\mathcal{F}_\xi := \left\{ f \in \mathcal{O}[[X]] \mid N_{k'/k}(\pi') = \xi, f \equiv \pi' X \bmod \deg 2, f \equiv X^q \bmod \mathfrak{p}' \right\}$$

と定義する.

$\mathcal{F}_\xi$ の定義に現れる条件のうち, 後半の「$f \equiv X^q \bmod \mathfrak{p}'$」はまさに Frobenius の定義である. しかし Frobenius というのは, どこの群における Frobenius か, というのが重要である. その答えは少し後の定理 1.32 で出てくる, $\mathrm{Hom}_{\mathcal{O}'}(F_f, F_f^\varphi)$ という群である.

Example 1.27 (Lubin-Tate)**.** $d = 1$, すなわち $k' = k$ のときを考える. このとき $\mathcal{F}_\xi$ のノルム条件は自明に満たされる. また, $v(\xi) = 1$ となる $\xi \in k^\times$ というのはつまり素元のことであるので $\xi = \pi$ と書いておく. 従って $\mathcal{F}_\xi$ は

$$\mathcal{F}_\xi = \{ f \in \mathcal{O}[[X]] \mid f \equiv \pi X \bmod \deg 2, f \equiv X^q \bmod \mathfrak{p} \}$$

と書ける. この $\mathcal{F}_\xi$ が, Lubin-Tate が最初に構成した Frobenius である.

Lemma 1.28. $f, g \in \mathcal{F}_\xi, F(X_1, \dots, X_n) := a_1 X_1 + \cdots + a_n X_n \in \mathcal{O}[X_1, \dots, X_n]$ に対し, $f \circ F_1 \equiv F_1^\varphi \circ (g, \dots, g) \bmod \deg 2$ を仮定する. このとき以下が成り立つ.

$$^{\exists!} F \in \mathcal{O}[[X_1, \dots, X_n]] \text{ such that } \begin{cases} F \equiv F_1 \bmod \deg 2 \\ f \circ F \equiv F^\varphi \circ (g, \dots, g) \end{cases}$$

ただし $F \in \mathcal{O}[[X]]$ に対し $F^\varphi \in \mathcal{O}[[X]]$ とは, F の各係数に φ を作用させたものを表す.

Proof. $f = \pi_1 X + \dots, g = \pi_2 X + \cdots \in \mathcal{F}_\xi$ と書いておく. $F^{(m)} :\equiv F \bmod \deg m + 1$ とする. このとき冪級数環の定義から, 任意の $m \in \mathbb{Z}$ に対して

$$f \circ F^{(m)} \equiv F^{(m)\varphi} \circ (g, \dots, g) \bmod \deg m + 1 \tag{1.29}$$

なる $F^{(m)}$ を構成すればよい. $F^{(m)}$ を F_1 から帰納的に構成する前に, (1.29) の条件を使いやすい形に書き換えることにする. 以下, F_m を F の m 次斉次部分とする. このとき容易に分かるように $F^{(m)} = F^{(m-1)} + F_m$ である. このとき

$$\begin{aligned}
f \circ F^{(m)} &\equiv \pi_1(F^{(m-1)} + F_m) + *(F^{(m-1)} + F_m)^2 + \dots \\
&\equiv \pi_1 F^{(m-1)} + *(F^{(m-1)})^2 + \cdots + \pi_1 F_m \bmod \deg m + 1 \\
&= f \circ F^{(m-1)} + \pi_1 F_m \\
F^{(m)\varphi} \circ (g, \dots, g) &= (F^{(m-1)\varphi} + F_m^\varphi) \circ (g, \dots, g) \\
&= F^{(m-1)\varphi} \circ (g, \dots, g) + \sum_{i_1 + \cdots + i_n = m} c^\varphi_{i_1, \dots, i_n} g(X_1)^{i_1} \dots g(X_n)^{i_n} \\
&= F^{(m-1)\varphi} \circ (g, \dots, g) + \sum_{i_1 + \cdots + i_n = m} c^\varphi_{i_1, \dots, i_n} (\pi_2 X_1 + \dots)^{i_1} \dots (\pi_2 X_n + \dots)^{i_n} \\
&\equiv F^{(m-1)\varphi} \circ (g, \dots, g) + \pi_2^m \sum_{i_1 + \cdots + i_n = m} c^\varphi_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} \bmod \deg m + 1 \\
&= F^{(m-1)\varphi} \circ (g, \dots, g) + \pi_2^m F_m^\varphi
\end{aligned}$$

を得る. 従って条件 (1.29) は

$$\begin{aligned}
& f \circ F^{(m-1)} + \pi_1 F_m \equiv F^{(m-1)\varphi} \circ (g, \dots, g) + \pi_2^m F_m^\varphi \\
\iff & \pi_1 F_m - \pi_2^m F_m^\varphi \equiv F^{(m-1)\varphi} \circ (g, \dots, g) - f \circ F^{(m-1)} \bmod \deg m + 1
\end{aligned} \tag{1.30}$$

と書き換えられる. つまり今すべきことは, 任意の $m \in \mathbb{Z}$ に対し (1.30) を満たす $F^{(m)}$ を構成すればよいということである. $m \geq 2$ のときそのような $F^{(m)}$ が構成できたと仮定すると ($f, g \in \mathcal{F}_\xi$ であることに気を付けて)

$$\begin{aligned} F^{(m-1)} \circ (g, \dots, g) - f \circ F^{(m-1)} &\equiv F^{(m-1)\varphi} \circ (X_1^q, \dots, X_n^q) - (F^{(m-1)})^q \bmod \mathfrak{p}' \\ &\equiv (F^{(m-1)}(X_1, \dots, X_n))^q - (F^{(m-1)})^q \bmod \mathfrak{p}' \\ &= 0 \end{aligned}$$

であるので, 一意的に m 次斉次多項式 $t \in \mathcal{O}'[X_1, \dots, X_n]$ が存在して $F^{(m-1)} \circ (g, \dots, g) - f \circ F^{(m-1)} \equiv t \bmod \deg m+1$ かつ $t \equiv 0 \bmod \mathfrak{p}'$ が成り立つ. このとき $m+1$ か成り立つかどうか, すなわち

$$F_m - \pi_1^{-1} \pi_2^m F_m^\varphi = \pi_1^{-1} t$$

なる F_m が一意的に構成できることを示したい. 特に, 両辺の各係数が一致するような F_m が一意的に構成できればよい. そしてそれは次の補題から従う. □

Lemma 1.31. $a \in \mathfrak{p}', y \in \mathcal{O}'$ に対し, 一意に $x \in \mathcal{O}'$ が存在し $ax^\varphi - x = y$ が成り立つ.

Proof. まず $x \in \mathcal{O}'$ の存在性から示す. x を

$$x := -(y + a \cdot y^\varphi + a \cdot a^\varphi \cdot y^{\varphi^2} + a \cdot a^\varphi \cdot a^{\varphi^2} \cdot y^{\varphi^3} + \dots)$$

とおく. これが $ax^\varphi - x = y$ を満たすことは容易に分かるので, あとは収束性, すなわち $x \in \mathcal{O}'$ を示せばよい. 直接 $\mathfrak{p}'$ 進付値を計算すると

$$\left| a \cdot a^\varphi \cdot a^{\varphi^2} \cdot \dots \cdot a^{\varphi^r} \cdot y^{\varphi^{r+1}} \right|_{\mathfrak{p}'} = |a| \cdots |a| \cdot |y| \leq |a|^r \to 0 \ (r \to \infty)$$

となるので収束する.

次に一意性を示す. $ax_1^\varphi - x_1 = y$ かつ $ax_2^\varphi - x_2 = y$ が成り立つならば $x_1 = x_2$ を示せばよい. 前者の式から後者の式を引くことで, $a(x_1 - x_2)^\varphi - (x_1 - x_2) = 0$ ならば $x_1 - x_2 = 0$ を示せばよい. 従って $x_1 - x_2$ を改めて x とおくことで, $ax^\varphi - x = 0$ ならば $x = 0$ を示せばよい.

$$(|a|_{\mathfrak{p}'} - 1)|x|_{\mathfrak{p}'} = |ax^\varphi|_{\mathfrak{p}'} - |x|_{\mathfrak{p}'} = |x|_{\mathfrak{p}'} - |x|_{\mathfrak{p}'} = 0$$

であることがすぐに分かるが, $a \in \mathfrak{p}'$ より $|a|_{\mathfrak{p}'} < 1$ なので, $|x|_{\mathfrak{p}'} = 0$ となるしかない. それはすなわち $x = 0$ である. □

Theorem 1.32. 任意の $f \in \mathcal{F}_\xi$ に対し, 一意的に形式群則 $F_f/\mathcal{O}'$ が存在して

$$f \circ F_f = F_f^\varphi \circ f \quad (\text{ id est } \ f \in \mathrm{Hom}_{\mathcal{O}'}(F_f, F_f^\varphi))$$

が成り立つ. この F_f を, (f の)**relative Lubin-Tate formal group** という.

Proof. Lemma 1.28 において, $f = g = \pi X + \dots \in \mathcal{F}_\xi, F_1 := X + Y$ とおく. これは明らかに $f \circ F_1 \equiv F_1^\varphi \circ g$ を満たす. 従って

$$\exists! F_f \in \mathcal{O}'[[X, Y]] \text{ such that } \begin{cases} F_f \equiv X + Y \bmod \deg 2 \\ f \circ F_f = F_f^\varphi \circ g \end{cases}$$

が成り立つ. あとはこの F_f が形式群則であることを示せばよい. 一意性から $F_f(X, Y) = F_f(Y, X)$ が従うので, 結合則のみ示せばよい. また Lemma 1.28 において $G_1 := X + Y + Z \in \mathcal{O}'[X, Y, Z]$ とおくことで

$$\exists! G \in \mathcal{O}'[[X, Y, Z]] \text{ such that } \begin{cases} G \equiv X + Y + Z \bmod \deg 2 \\ f \circ G = G^\varphi \circ f \end{cases}$$

が成り立つ．このとき $F_f(F_f(X,Y),Z)$ が G の条件を満たすことをチェックすれば一意性よりこれらが等しくなることが分かる．同様に $F_f(X,F_f(Y,Z))$ でも G の条件を確かめることを見れば，G を通して $F_f(F_f(X,Y),Z) = G = F_f(X,F_f(Y,Z))$ となり証明が終わる．さて，$F_f(F_f(X,Y),Z) \equiv X+Y+Z \bmod \deg 2$ は明らかである．さらに

$$\begin{aligned} f \circ F_f(F_f(X,Y),Z) &= F_f^{\varphi}(f(F_f(X,Y)),f(Z)) \ (\because f\circ F_f = F_f^{\varphi}\circ f) \\ &= F_f^{\varphi}(F_f^{\varphi}(f(X),f(Y)),f(Z)) \ (\because f\circ F_f = F_f^{\varphi}\circ f) \end{aligned}$$

非常に見づらいが，これは確かに $f\circ F_f(F_f(X,Y),Z) = F_f(F_f(X,Y),Z)^{\varphi}\circ(f,f,f)$ を満たしていることが分かる．ok. □

Remark 1.33. $f \in \mathcal{F}_\xi$ に対して $\varphi(f) \in \mathcal{F}_\xi$ であり，$F_{\varphi(f)} = F_f^{\varphi}$ となることに注意する．後半の主張を示すには，

$$\begin{cases} f\circ F_f = F_f^{\varphi}\circ f \\ \varphi(f)\circ F_{\varphi(f)} = F_{\varphi(f)}^{\varphi}\circ\varphi(f) \end{cases} \Longrightarrow \varphi(f)\circ F_f^{\varphi} = (F_f^{\varphi})^{\varphi}\circ\varphi(f)$$

を示せばよい．何故ならば $\varphi(f)\circ * = *^{\varphi}\circ\varphi(f)$ を満たす形式群則は一つしかないので，上のことが示されれば，それは $F_{\varphi(f)}$ と F_f^{φ} と二つ存在することになり，等しくなるしかないためである．それでは上を示すにはどうするかというと，仮定の一つ目の式の両辺に φ を作用させればよい．ただしべき級数の合成関数への作用の計算に注意せよ．

Example 1.34. $d=1$ のとき $\mathcal{O} = \mathcal{O}'$ であるから $\varphi \in G(k^{ur}/k)$ の $F_f/\mathcal{O}'$ への作用は自明になる．従って $f \in \mathrm{End}_{\mathcal{O}}(F_f)$ となる．これにより $f \in \mathcal{F}_\xi$ はFrobenius の F_f への持ち上げと言える．

Proposition 1.35. $f = \pi_1 X + \cdots \in \mathcal{F}_\xi, g = \pi_2 X + \cdots \in \mathcal{F}_\xi$ とし，$a \in \mathcal{O}'$ を $a^{\varphi} = \frac{\pi_2}{\pi_1}a$ を満たすものとする．(cf. Remark 1.36) このとき以下が成り立つ．

$$^{\exists!}[a]_{f,g} \in \mathrm{Hom}_{\mathcal{O}'}(F_f,F_g) \text{ such that } \begin{cases} [a]_{f,g} \equiv aX \bmod \deg 2 \\ g\circ[a]_{f,g} = [a]_{f,g}^{\varphi}\circ f \end{cases}$$

また，$h = \pi_3 X + \cdots \in \mathcal{F}_\xi$ として $b \in \mathcal{O}'$ を $b^{\varphi} = \frac{\pi_3}{\pi_2}b$ を満たすものとすると $[ab]_{f,h} = [b]_{g,h}\circ[a]_{f,g}$ が成り立つ．さらに，

$$\Phi : \left\{ a \in \mathcal{O}' \mid a^{\varphi} = \frac{\pi_2}{\pi_1}a \right\} \to \mathrm{Hom}_{\mathcal{O}'}(F_f,F_g); a \mapsto [a]_{f,g}$$

は群同型であり，特に $f=g$ ならば $\mathcal{O}' \cong \mathrm{End}_{\mathcal{O}'}(F_f)$ であり，かつ $[\pi_1]_{f,\varphi(f)} = f$.

Proof. ($[a]_{f,g}$ の構成) 補題 1.28 において $F_1 := aX$ とおく．これは $g\circ F_1 \equiv F_1^{\varphi}\circ f \bmod \deg 2$ を満たすことがすぐ分かる．(実際，$g\circ F_1 \equiv \pi_2(aX) = a^{\varphi}(\pi_1 X) \equiv F_1^{\varphi}\circ f$ となって ok.) 従って

$$^{\exists!}[a]_{f,g} \in \mathcal{O}'[[X]] \text{ such that } \begin{cases} [a]_{f,g} \equiv aX \bmod \deg 2 \\ g\circ[a]_{f,g} = [a]_{f,g}^{\varphi}\circ f \end{cases}$$

が成り立つ．あとは $[a]_{f,g} \in \mathrm{Hom}_{\mathcal{O}'}(F_f,F_g)$, すなわち $[a]_{f,g}\circ F_f = F_g\circ[a]_{f,g}$ を示せば最初の主張が示される．特に ($k'[[X]]$ において)$[a]_{f,g}\circ F_f\circ[a]_{f,g}^{-1}$ が F_g の性質を満たせば一意性より $[a]_{f,g}\circ F_f = F_g\circ[a]_{f,g}$ が従う．F_g の性質とは $g\circ F_g = F_g^{\varphi}\circ g$ であったから，この F_g を $[a]_{f,g}\circ F_f\circ[a]_{f,g}^{-1}$ にしても成り立つことを見ればよい．

$$\begin{aligned} g\circ([a]_{f,g}\circ F_f\circ[a]_{f,g}^{-1}) &= (g\circ[a]_{f,g})\circ F_f\circ[a]_{f,g}^{-1} \ (\because \text{結合則}) \\ &= ([a]_{f,g}^{\varphi}\circ f)\circ F_f\circ[a]_{f,g}^{-1} \ (\because [a]_{f,g}\text{の性質}) \\ &= [a]_{f,g}^{\varphi}\circ(f\circ F_f)\circ[a]_{f,g}^{-1} \ (\because \text{結合則}) \\ &= [a]_{f,g}^{\varphi}\circ(F_f^{\varphi}\circ f)\circ[a]_{f,g}^{-1} \ (\because F_f\text{の性質}) \\ &= [a]_{f,g}^{\varphi}\circ F_f^{\varphi}\circ([a]_{f,g}^{\varphi,-1}\circ[a]_{f,g}^{\varphi})\circ f\circ[a]_{f,g}^{-1} \ (\because \text{真ん中に余計な項をかませた}) \\ &= [a]_{f,g}^{\varphi}\circ F_f^{\varphi}\circ[a]_{f,g}^{\varphi,-1}\circ([a]_{f,g}^{\varphi}\circ f\circ[a]_{f,g}^{-1}) \ (\because \text{結合則}) \\ &= ([a]_{f,g}\circ F_f\circ[a]_{f,g}^{-1})^{\varphi}\circ g \ (\because \text{前半は}\varphi\text{でくくった．後半は}[a]_{f,g}\text{の性質}) \end{aligned}$$

以上より確かに成り立つ.

(推移率) $[ab]_{f,h} = [b]_{g,h} \circ [a]_{f,g}$ を示すために, $[b]_{g,h} \circ [a]_{f,g}$ が $[ab]_{f,h}$ の性質を満たすことを示せば一意性より等式が従う. $[b]_{g,h} \circ [a]_{f,g} \equiv (ab)X \bmod \deg 2$ はすぐ分かる. また,

$$([b]_{g,h} \circ [a]_{f,g})^{\varphi} \circ f = [b]_{g,h}^{\varphi} \circ [a]_{f,g}^{\varphi} \circ f = [a]^{\varphi} \circ g \circ [a] = h \circ ([b]_{g,h} \circ [a]_{f,g})$$

となるから確かに ok.

(同型) 単射性は $[a]_{f,g}$ の一意性から従うので, 準同型であることと全射であることを示せばよい. Φ が準同型であること, すなわち $\Phi(a+b) = \Phi(a) + \Phi(b)$, すなわち $[a+b]_{f,g} = [a]_{f,g} + [b]_{f,g}$ を示す. これもまた, $[a]_{f,g} + [b]_{f,g}$ が $[a+b]_{f,g}$ の性質を満たせば一意性から等式が従う.

$$\begin{aligned}
&[a]_{f,g} + [b]_{f,g} \equiv aX + bX = (a+b)X \bmod \deg 2 \\
&([a]_{f,g} + [b]_{f,g})^{\varphi} \circ f \equiv [a]_{f,g}^{\varphi} \circ f + [b]_{f,g}^{\varphi} \circ f = g \circ [a]_{f,g} + g \circ [b]_{f,g} = g \circ ([a]_{f,g} + [b]_{f,g})
\end{aligned}$$

より ok. 全射であること, すなわち $\psi \in \mathrm{Hom}_{\mathcal{O}'}(F_f, F_g)$ に対して, ある a が存在して $\Phi(a) = \psi$ を示す. $a := \psi'(0)$ とする. このとき Proposition 1.21 より $\psi = [a]_{f,g}$ と書ける. あとは a が $a^{\varphi} = \frac{\pi_2}{\pi_1} a$ を満たすことを見ればよい. さて, $\psi = [a]_{f,g}$ の満たす性質から

$$\begin{aligned}
\psi^{\varphi} \circ f &\equiv a^{\varphi} \pi_1 X \bmod \deg 2 \\
g \circ \psi &\equiv \pi_2 a X \bmod \deg 2
\end{aligned}$$

の二つは等しいので, 係数を比べて $a^{\varphi} = \frac{\pi_2}{\pi_1} a$ が従う.

($[\pi_1]_{f,\varphi(f)} = f$) 定義より

$$\begin{aligned}
f &\equiv \pi_1 X \bmod \deg 2 \\
f^{\varphi} \circ f &= \varphi(f) \circ f
\end{aligned}$$

である. これはまさに f が $[\pi_1]_{f,\varphi(f)}$ の性質を満たしていることを述べている. 従って一意性より ok. □

Remark 1.36 (Hilbert 90)**.** L/K を有限次ガロア拡大とする. このとき Hilbert の定理 90 とは

$$H^1(\mathrm{Gal}(L/K), L^\times) = 0$$

が成り立つというものである. この 1 次ガロアコホモロジーを書き下すと

$$H^1(\mathrm{Gal}(L/K), K^\times) := \frac{\left\{f : \mathrm{Gal}(L/K) \to L^\times ; \text{cont. map} \mid {}^\forall g, h \in \mathrm{Gal}(L/K),\ f(gh) = f(g)\cdot f(h)^g\right\}}{\left\{f : \mathrm{Gal}(L/K) \to L^\times ; \text{cont. map} \mid {}^\exists x \in L^\times \text{ such that } {}^\forall g \in \mathrm{Gal}(L/K),\ f(g) = x^g/x\right\}}$$

となる. 従って Hilbert 90 より, (分子 $\supset$ 分母は当たり前であるから,) $f(gh) = f(g)f(h)^g$ を満たす連続写像 $f : \mathrm{Gal}(L/K) \to L^\times$ を見つければ, ある $x \in L^\times$ が存在して $f(g) = x^g/x$ と書ける.
さて, $\mathrm{Gal}(k'/k) = \langle\varphi\rangle$ は d 次巡回群であった. $u := \pi_2/\pi_1 \in \mathcal{O}'^\times$ とおく. このとき連続写像 $f : \mathrm{Gal}(k'/k) \to k'^\times$ を

$$f(\varphi^i) = u\varphi(u)\varphi^2(u)\cdots\varphi^{i-1}(u)$$

とする. このとき f は $f(gh) = f(g)f(h)^g$ を満たす. 実際,

$$\begin{aligned} f(\varphi^i)f(\varphi^j)^{\varphi^i} &= u\varphi(u)\varphi^2(u)\cdots\varphi^{i-1}(u)\cdot\varphi^i\left(u\varphi(u)\varphi^2(u)\cdots\varphi^{j-1}(u)\right) \\ &= u\varphi(u)\varphi^2(u)\cdots\varphi^{i-1}(u)\varphi^i(u)\cdots\varphi^{i+j-1}(u) \end{aligned}$$

であって, もし $i+j < d$ であればこれは確かに $f(\varphi^i\varphi^j) = f(\varphi^{i+j})$ に等しい. $i+j \geq d$ であれば $i+j = dn+k$ $(0 \leq k < d)$ と表せば

$$\begin{aligned} f(\varphi^i)f(\varphi^j)^{\varphi^i} &= u\varphi(u)\cdots\varphi^{i+j-1}(u) \\ &= u\varphi(u)\cdots\varphi^{d-1}(u)\cdot\varphi^d(u\varphi(u)\cdots\varphi^{d-1}(u))\cdots\varphi^{dn}(u\varphi(u)\cdots\varphi(u)^{k-1}) \\ &= u\varphi(u)\cdots\varphi(u)^{k-1} \quad (\because 1 = N_{k'/k}(u) = u\varphi(u)\cdots\varphi^{d-1}(u)) \\ &= f(\varphi^k) \\ &= f(\varphi^{i+j}) \end{aligned}$$

より分かる. 従って Hilbert 90 より, ある $b \in k'^\times$ が存在して $u = f(\varphi) = \varphi(b)/b$ が成り立つ. ここで k の素元 π を一つ固定する. k'/k は不分岐であるから π は k' の素元でもある. b の π 進展開を $b = \sum_{i=-n}^{\infty} b_i\pi^i$ とする. $m \geq n$ となるように $m \in \mathbb{Z}$ を取ると $\pi^m b \in \mathcal{O}'$ となる. π は k の元であるから φ で固定されることに気をつけると

$$u = \frac{\varphi(b)}{b} = \frac{\pi^m\varphi(b)}{\pi^m b} = \frac{\varphi(\pi^m b)}{\pi^m b}$$

を得る. すなわち $a := \pi^m b \in \mathcal{O}'$ とおくことにより $u = \varphi(a)/a$ なる $a \in \mathcal{O}'$ を得ることができる.

Corollary 1.37. $f, g \in \mathcal{F}_\xi$ ならば $\mathcal{O}'$ 上の同型 $F_f \simeq F_g$ が成り立つ.

Proof. $f = \pi_1 X + \ldots, g = \pi_2 X + \cdots \in \mathcal{F}_\xi$ と表しておく. Proposition 1.35 より $[a]_{f,g} \in \mathrm{Hom}_{\mathcal{O}'}(F_f, F_g)$ の存在は分かっているので, あとは $[a]_{f,g}$ が同型, すなわち

$${}^{\exists!}a \in \mathcal{O}'^\times \text{ such that } a^\varphi = \frac{\pi_1}{\pi_2}a$$

が成り立つことを示せばよいが, 既にこれは示している. □

形式群則 F_f に対して $\widetilde{F_f}$ で, 各係数を $\mathrm{mod}\mathfrak{p}'$ した $\mathcal{O}'/\mathfrak{p}'$ 上の形式群則を表すものとする. このとき Proposition 1.25 より $\widetilde{F_f}$ は高さをもつが, これは $[k : \mathbb{Q}_p]$ に等しい. これは以下のようにして分かる.
$v(p) = e$ とし, $\pi \in \mathfrak{p}$ を素元とする. $f = \pi X + \ldots$ と表しておき, $p = u\pi^e$ $(u \in \mathcal{O}'^\times)$ と書いておく. このとき

$$[p]_{\widetilde{F_f}} = [u\pi^e]_{\widetilde{F_f}} \sim [\pi]^e_{\widetilde{F_f}} = f^e \equiv X^{q^e} \bmod \mathfrak{p}'$$

が成り立つ. ここで, $p^{[k:\mathbb{Q}_p]} = q^e = p^{f[\mathcal{O}/\mathfrak{p}:\mathbb{F}_p]}$ であるので, $\widetilde{F_f}$ の高さが $[k : \mathbb{Q}_p]$ であることが分かる.

Proposition 1.38. $v(\xi)=v(\xi')=d, u=\xi'/\xi\in\mathcal{O}^\times, f\in\mathcal{F}_\xi$ とする. $u'\in\mathcal{O}'^\times$ を, $N_{k'/k}(u')=u$ となるものとする. (cf. Remark 1.39) また, $\Omega\in\mathcal{O}_K^\times$ を $\Omega^{\varphi-1}=u'$ となるものとする. (cf. Remark 1.36) このとき

$$\exists!\theta\in\mathcal{O}_K[[X]]\ \text{ such that }\begin{cases}\varphi^d(\theta)=\theta\circ[u]_f\\ \theta(X)\equiv\Omega X \bmod \deg 2\end{cases}$$

が成り立つ. さらに $f':=\theta^\varphi\circ f\circ\theta^{-1}$ とすると, $f'\in\mathcal{F}_{\xi'}$ であり

$$\theta: F_f\xrightarrow{\simeq}F_{f'}\text{ over }\mathcal{O}_K$$

が成り立つ.

Proof. (θ の構成) $\theta_1:=\Omega X$ とおく. このとき数学的帰納法により

$$\exists!\theta_r\in\mathcal{O}_K[X];\deg r\ \text{ such that }\begin{cases}\varphi^d(\theta_r)\equiv\theta_r\circ[u]_f \bmod \deg r+1\\ \theta_r(X)\equiv\Omega X \bmod \deg 2\end{cases}$$

を示せばよい. この先の構成から分かるように, 後者の条件は自明に従うので前者だけ示せばよい. まず $r=1$ のとき

$$\varphi^d(\theta_1)=\varphi^d(\Omega)X=\varphi^{d-1}(u'\Omega)X=\varphi^{d-2}(\varphi(u')u'\Omega)X=\cdots=\varphi^{d-1}(u')\cdots\varphi(u')u'\cdot\Omega X=N(u')\Omega X=u\Omega X\equiv\theta_1\circ[u]_f \bmod \deg$$

より ok. r で成り立つと仮定, すなわち

$$\exists!\theta_r\in\mathcal{O}_K[X];\deg r\ \text{ such that }\begin{cases}\varphi^d(\theta_r)\equiv\theta_r\circ[u]_f \bmod \deg r+1\end{cases}$$

が成り立つと仮定する. このとき $\theta_{r+1}=\theta_r(X)+bX^{r+1}$ が条件を満たすような $b\in\mathcal{O}_K$ を見つければよい.

$$\begin{aligned}\varphi^d(\theta_{r+1})&=\varphi^d(\theta_r)+\varphi^d(b)X^{r+1}\\ &\equiv(\theta_r\circ[u]_f+cX^{r+1})+\varphi^d(b)X^{r+1}\bmod\deg r+2\quad(\because\text{帰納法の仮定, }{}^\exists c\in\mathcal{O}_K)\\ \theta_{r+1}\circ[u]_f&=\theta_r\circ[u]_f+b[u]_f^{r+1}\\ &\equiv\theta_r\circ[u]_f+bu^{r+1}X^{r+1}\bmod\deg r+2\end{aligned}$$

であるから, $r+1$ で成り立つためには $(\theta_r\circ[u]_f+cX^{r+1})+\varphi^d(b)X^{r+1}\equiv\theta_r\circ[u]_f+bu^{r+1}X^{r+1}\bmod\deg r+2$, すなわち $(\varphi^d(b)-bu^{r+1})X^{r+1}\equiv-cX^{r+1}\bmod\deg r+2$, すなわち

$$\varphi^d(b)-bu^{r+1}=-c$$

を満たす $b\in\mathcal{O}_K$ を見つければよい. $a:=b/\Omega^{r+1}$ とする. このとき

$$\begin{aligned}\varphi^d(a\Omega^{r+1})-a(\Omega u)^{r+1}=-c&\iff\varphi^d(a)(u\Omega)^{r+1}-a(u\Omega)^{r+1}=-c\quad(\because\varphi^d(\Omega)=u\Omega)\\ &\iff\varphi^d(a)-a=\frac{-c}{(u\Omega)^{r+1}}\end{aligned}$$

となる $a\in\mathcal{O}_K$ を見つければよい. 特にヘンゼルの補題より, $\mathcal{O}_K/\mathfrak{p}_K$ で解が存在することを言えばよい. しかしそれは $\mathcal{O}_K/\mathfrak{p}_K\simeq\overline{\mathbb{F}_q}$ と代数閉体係数となるため必ず解が存在する. ok.

($f'\in\mathcal{F}_{\xi'}$) $f=\pi X+\cdots\in\mathcal{F}_\xi$ ($N_{k'/k}(\pi)=\xi$) とおく. このとき

$$f'=\theta^\varphi\circ f\circ\theta^{-1}\equiv\Omega^{\varphi-1}\pi X=u'\pi X \bmod\deg 2$$

であり, $N_{k'/k}(u'\pi)=N_{k'/k}(u')N_{k'/k}(\pi)=u\xi=\xi'$ より, 条件の一つを満たすことが分かった. あとは Frobenius 条件を示せばよい. これも

$$f'=\theta^\varphi\circ f\circ\theta^{-1}\equiv\theta^{(q)}(\theta^{-1(q)}(X^q))=X^q \bmod\mathfrak{p}'$$

より分かる.

(θ; 同型) $\Omega \in \mathcal{O}_K^\times$ であるから逆関数 $\theta^{-1} \in \mathcal{O}_K[[X]]^\times$ が存在する. あとは $\theta^{-1} \circ F_{f'} \circ \theta$ が F_f の性質を満たせば一意性より $\theta^{-1} \circ F_{f'} \circ \theta = F_f$, すなわち $F_{f'} \circ \theta = \theta \circ F_f$, すなわち $\theta \in \mathrm{Hom}_{\mathcal{O}_K}(F_f, F_f')$ となり証明が終わる. その F_f の性質とは $f \circ F_f = F_f^\varphi \circ f$ であったことを思い出すと

$$\begin{aligned} f \circ (\theta^{-1} \circ F_{f'} \circ \theta) &= (\theta^\varphi)^{-1} \circ f' \circ F_{f'} \circ \theta \quad (\because f' = \theta^\varphi \circ f \circ \theta^{-1}) \\ &= (\theta^\varphi)^{-1} \circ F_{f'}^\varphi \circ f' \circ \theta \quad (\because f' \circ F_{f'} = F_{f'}^\varphi \circ f') \\ &= (\theta^\varphi)^{-1} \circ F_{f'}^\varphi \circ \theta^\varphi \circ f \quad (\because f' = \theta^\varphi \circ f \circ \theta^{-1}) \\ &= (\theta^{-1} \circ F_{f'} \circ \theta)^\varphi \circ f \end{aligned}$$

となり確かに ok. □

Remark 1.39. k'/k を一般の局所体の有限次拡大とする. このとき $N_{k'/k}\mathcal{O}'^\times \subset \mathcal{O}^\times$ が成り立つ. k'/k が特に不分岐拡大であればこれは等式, すなわち $N_{k'/k}\mathcal{O}'^\times = \mathcal{O}^\times$, すなわち整数環の単元群においてはノルム写像が全射になる.

$i \geq 0$ と $f \in \mathcal{F}_\xi$ に対し

$$f^{(i)} = \varphi^{i-1}(f) \circ \cdots \circ \varphi(f) \circ f$$

と定義する. このとき $f^{(i)} \in \mathrm{Hom}_{\mathcal{O}'}(F_f, F_{\varphi^i(f)})$ であり, $v(\xi) = d$ ならば $f^{(d)} = [\xi]_f \in \mathrm{End}_{\mathcal{O}'}(F_f)$ である.

前半は $f \in \mathrm{Hom}_{\mathcal{O}'}(F_f, F_{\varphi(f)})$ より ok. 後半について, $f = \pi X + \cdots \in \mathcal{F}_\xi$ とおくと

$$\begin{aligned} f^{(d)} &\equiv \varphi^{d-1}(\pi) \dots \varphi(\pi) X = N_{k'/k}(\pi) X = \xi X \bmod \deg 2 \\ (f^{(d)})^\varphi \circ f &= \varphi^d(f) \circ \cdots \circ \varphi(f) \circ f = f \circ \varphi^{d-1}(f) \circ \dots f = f \circ f^{(d)} \end{aligned}$$

となり, $f^{(d)}$ が $[\xi]_f$ の性質を満たす. 従って一意性から $f^{(d)} = [\xi]_f$ となる.

以下, $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$, M を $\mathbb{C}_p$ の極大イデアル, $M_f := F_f(M)$ を F_f の M 値点とする.

Definition 1.40. $\pi \in \mathcal{O}'$ を $N_{k'/k}(\pi) = \xi$ を満たすものとし, $n \geq 0$ とする. このとき

$$\begin{aligned} W_f^n &:= \left\{ w \in M_f \mid {}^\forall a \in \mathfrak{p}^n, [a]_f(w) = 0 \right\} \\ &= \{ w \in M_f \mid [\pi^n]_f(w) = 0 \} \\ &= \mathrm{Ker}\left(f^{(n)} : M_f \longrightarrow M_{\varphi^n(f)} \right) \end{aligned}$$

と定義する. W_f^n の元を F_f の n **等分点 (division points of level n)** という.

二つ目の等号を示す. ${}^\forall a \in \mathfrak{p}^n$ に対して $[a]_f(w) = 0$ ならば当然 ${}^\forall a \in \mathfrak{p}^i$ $(i < n)$ に対して $[a]_f(\omega) = 0$ である. 従って $a \in \mathfrak{p}^n \setminus \mathfrak{p}^{n-1}$ と考えてよい. このとき $a = u\pi^n$ $(u \in \mathcal{O}'^\times)$ と表すことで $[a]_f = [u]_f \circ [\pi^n]_f \sim [\pi^n]$ となるから ok.

三つ目の等号を示す. 帰納法により $f^{(n)} = [\pi^n]_{f,\varphi^n(f)}$ を示す. $n = 1$ のときは既に Remark 1.38 の後で示した. $n-1$ のとき正しいと仮定すると

$$f^{(n)} = \varphi^{n-1}(f) \circ f^{(n-1)} = \varphi^{n-1}(f) \circ [\pi^{n-1}]_{f,\varphi^{n-1}(f)} = [\pi]_{\varphi^{n-1}(f),\varphi^n(f)} \circ [\pi^{n-1}]_{f,\varphi^{n-1}(f)} = [\pi^n]_{f,\varphi^n(f)}$$

より ok. ただし, 三つ目の等号は Corollary 1.37 より「F_f は f に依らないこと」から従う.

Proposition 1.41 (cf. Cassel, Fröhlich "ANT")**.**

- $W_f^n \subset M_f$ は $\mathcal{O}$ 加群であり, $\#W_f^n = q^n$. さらに任意の $n \in \mathbb{N}$ に対して $W_f^n \subset W_f^{n+1}$.
- $w \in \widetilde{W_f^n} := W_f^n \setminus W_f^{n-1}$ に対し

$$\mathcal{O}/\mathfrak{p} \xrightarrow{\simeq} W_f^n; a \mapsto [a]_f(w).$$

  従って $\mathcal{O}/\mathfrak{p}^n \simeq \mathrm{End}_{\mathcal{O}}(W_f^n)$.
- $W_f := \cup_n W_f^n$ は non-canonical に $k/\mathcal{O}$ と同型. また, $W_f = (M_f$の $\mathcal{O}-$torsion 全体).

Proof. (1) $a \in \mathcal{O}, w \in W_f^n$ に対し, $a \cdot w := [a]_f(w)$ により W_f^n は $\mathcal{O}$ 加群になる. Corollary 1.37 より F_f は f の取り方に依らないので $f = \pi X + X^q$ としてよい. このとき $f^{(n)}$ は q^n 次多項式となることが定義より分かるが, $\mathrm{char}(k) = 0$ であるから $f^{(n)}$ はちょうど q^n 個の異なる解をもつ. 従って $\#W_f^n = q$ が従う. 包含は明らかである.

(2) まず準同型

$$\phi_w : \mathcal{O} \to W_f^n; a \mapsto [a]_f(w)$$

を考える. このとき $\mathrm{Ker}(\phi_w) = \mathfrak{p}^n$ を示せば $\mathcal{O}/\mathfrak{p}^n \simeq \mathrm{Im}(\phi_w) \subset W_f^n$ となって, 位数を比べることにより $\mathcal{O}/\mathfrak{p}^n \simeq W_f^n$ が従う. 非自明な $\mathrm{Ker}(\phi_w) \subset \mathfrak{p}^n$ のみ示す. $a \in \mathrm{Ker}(\phi_w)$, すなわち $[a]_f(w) = 0$ と仮定する. $a = \sum_{i=m}^{\infty} a_i \pi^i$ と π 進展開しておくと, $w \in \widetilde{W_f^n}$ であるから $m \geq n$ でなければならない. よって $a \in \mathfrak{p}^n$ となる.

(3) 前者は

$$W_f = \varinjlim_n W_f^n \simeq \varinjlim_n \mathcal{O}/\mathfrak{p}^n \simeq k/\mathcal{O}$$

より従う. 後者を示す. 任意の $w \in W_f^n$ は定義より $\mathcal{O}$-torsion であるから, $x \in M_f \setminus \{0\}; \mathcal{O}$-torsion に対して, ある $n \in \mathbb{N}$ が存在して $x \in W_f^n$ を示せばよい. 今 x の取り方より, ある $a \in \mathcal{O}$ が存在して $a \cdot x = [a]_f(x) = 0$ である. もし $v(a) = 0$ ならば $x = [a^{-1}]_f \circ [a]_f(x) = 0$ より ok. もし $v(a) > 0$, すなわちある $n \in \mathbb{N}$ に対して $a \in \mathfrak{p}^n$ ならば $x \in W_f^n$ となり ok. □

Proposition 1.42. $k_\xi^n := k'(W_f^n)$ は f の choice に依らない k' の $(q-1)q^{n-1}$ 次 totally ramified 拡大であって, k 上 Abel 拡大である. また,

$$(\mathcal{O}/\mathfrak{p}^n)^\times \xrightarrow{\simeq} \mathrm{Gal}(k_\xi^n/k'); u \mapsto \sigma_u := (w \mapsto [u^{-1}]_f(w))$$

は f に依らない canonical な同型である. さらに任意の $w \in \widetilde{W_f^n}$ に対して, $k_\xi^n = k'(w)$ であり w は素元になる.

Proof. (k_ξ^n/k' が f に依らない totally ramified 拡大) $f(X) = \pi X + \pi(a_2 X^2 + \cdots + a_{q-1}X^{q-1}) + X^q$ とおく. このとき任意の $w \in W_f^n$ の k' 上の最小多項式は, $f^{(n)}$ で潰れるもので $f^{(n-1)}$ で潰れないものであるから $f^{(n)}/f^{(n-1)}$ である. 具体的に書き下すと

$$\begin{aligned}\phi_n(X) :&= \frac{f^{(n)}}{f^{(n-1)}} = \frac{\varphi^{n-1} \circ f^{(n-1)}}{f^{(n-1)}} \\ &= \varphi^{n-1}(\pi) + \varphi^{n-1}(\pi)(\varphi^{n-1}(a_2) f^{(n-1)} + \cdots + \varphi^{n-1}(a_{q-1})(f^{(n-1)})^{q-2}) + (f^{(n-1)})^{q-1}\end{aligned}$$

となり, これは $q^{n-1}(q-1)$ 次の Eisenstein 多項式である. また, $a_2, \ldots, a_{q-1}$ に依らないことがこれらの計算から分かるから, f に依らない. ok.

($(\mathcal{O}/\mathfrak{p}^n)^\times \simeq \mathrm{Gal}(k_\xi^n/k')$) k_ξ' の定義より, $\mathrm{Gal}(k_\xi^n/k')$ の元は $\mathrm{Aut}(W_f^n)$ の元を誘導する. この対応により

$$\mathrm{Gal}(k_\xi^n/k') \xrightarrow{\simeq} \mathrm{Aut}(W_f^n) \simeq (\mathcal{O}/\mathfrak{p}^n)^\times$$

を示す. 単射性は k_ξ^n が W_f^n から生成されていることから従う. ここで, 位数を比べると

$$\#\,\mathrm{Gal}(k_\xi^n/k') = [k_\xi^n : k'] = q^{n-1}(q-1) = \#(\mathcal{O}_K/\mathfrak{p}^n)^\times$$

となるので同型である.

$(k_\xi^n = k'(w))$ $w \in \widetilde{W_f^n}$ ならば明らかに $\phi_n(w) = f^{(n)}(\omega)/f^{(n-1)}(\omega) = 0$ より $k_\xi^n \supset k'(w)$. k' からの拡大次数を見ることで等号が分かる. w が素元になることは totally ramified の一般論から従う.

$(k_\xi^n/k$; Abel 拡大) まず

$$\mathrm{Gal}(k_\xi^n/k) \simeq \mathrm{Gal}(k_\xi^n/k') \times \mathrm{Gal}(k'/k)$$

であるから, $\mathrm{Gal}(k_\xi^n/k')$ の元が φ(の延長) と可換ならよい. τ を φ の k_ξ^n への延長とし, $\sigma = \sigma_u \in \mathrm{Gal}(k_\xi^n/k')$ とする. このとき

$$\begin{aligned}\tau\sigma_u(w) &= \tau([u^{-1}]_f(w)) \\ &= [u^{-1}]_{\varphi(f)}(\tau(w)) \quad (\because \varphi \circ [u^{-1}]_f = [u^{-1}]_{\varphi(f)} \circ \varphi) \\ &= \sigma_u(\tau(w)) \quad (f \text{ に依らない})\end{aligned}$$

より確かに可換である. ok. □

Remark 1.43. 命題 1.41 と命題 1.42 を用いることで, $\alpha \in W_f^n$ の $\omega \in G(k_\xi^n/k') = G(k'(\omega)/k')$ への作用の形が分かる. 命題 1.42 の証明中の同型 $G(k'(\omega)/k) \simeq \mathrm{Aut}(W_f^n) \simeq (\mathcal{O}/\mathfrak{p}^n)^\times$ をきちんと書くと

$$\big(\omega \mapsto \omega^i\big) \leftrightarrow \big(\omega \mapsto \omega^i\big) \leftrightarrow (a)$$

となる. ただし $[a]_f(\omega) = (\omega \mapsto \omega^i)$ である. 従って

$$\alpha \cdot \omega =$$

よくわからなくなってきた.

2 COLEMAN'S POWER SERIES

Proposition 2.1. 以下を満たす (乗法的) ノルム作用素 $N_f : R \to R$ が一意に存在する.

$$^\forall h \in R, \quad N_f(h)(f) = \prod_{\omega \in W_f^1} h(X[+]_f\omega) \tag{2.2}$$

この作用素は以下を満たす.

- $N_f(h) \equiv h^\varphi \bmod \mathfrak{p}'$.
- $N_{\varphi(f)} = \varphi \circ N_f \circ \varphi^{-1}$.
- $N_f^{(i)} := N_{\varphi^{i-1}(f)} \circ \cdots \circ N_{\varphi(f)} \circ N_f$ とすると

$$N_f^{(i)}(h)(f^{(i)}) = \prod_{\omega \in W_f^i} h(X[+]_f\omega).$$

- $h \in R$ が $h \equiv 1 \bmod \mathfrak{p}'^i$ $(i \geq 1)$ を満たすならば

$$N_f(h) \equiv 1 \bmod \mathfrak{p}'^{i+1}.$$

Proof. (乗法的, 一意性) 明らか.

(存在性) まず

$$g_0(X) := \prod_{\omega \in W_f^1} h(X[+]_f\omega)$$

とおく. $f \equiv X^q \bmod \mathfrak{p}'$ であることから Weierstrass の準備定理を適用ができ, その結果

$$^{\exists!} g_1 \in R, \ ^{\exists!} r(X) \in \mathcal{O}'[X] \text{ such that } g_0(X) - g_0(0) = g_1(X)f(X) + r(X), \ \deg r < q$$

が成り立つ. このとき $r(X)=0$ が分かる. 何故ならば, まず任意の $\alpha\in W_f^1$ に対し $(\omega\mapsto\omega[+]_f\alpha$ が W_f^1 の全単射を与えるので$)g_0(X[+]_f\alpha)=g_0(X)$ である. 従って $r(\alpha)=g_0(\alpha)-g_0(0)-g_1(\alpha)f(\alpha)=0-g_1(\alpha)\cdot 0=0$ より α は $r(X)$ の根である. α の取り方は q 個あったが, 一方 $\deg r<q$ より, これは $r=0$ となるしかない. ok.

次に, 任意の $\alpha\in W_f^1$ に対し $g_1(X[+]_f\alpha)=g_1(X)$ となることが以下のようにして分かる.

$$\begin{aligned}
g_1(X[+]_f\alpha)f(X[+]_f\alpha)&=g_0(X[+]_f\alpha)-g_0(0)\\
&=g_0(X)-g_0(0)\quad(\because g_0(X[+]_f\alpha)=g_0(X))\\
&=g_1(X)f(X)\\
&=g_1(X)F_f^{\varphi}(f(X),f(\alpha))\quad(\because f(\alpha)=0)\\
&=g_1(X)f(F_f(X,\alpha))\quad(\because f\circ F_f=F_f^{\varphi}\circ f)\\
&=g_1(X)f(X[+]_f\alpha)\quad(\because[+]_f\text{の定義})
\end{aligned}$$

従って g_1 を構成したときと同様の議論で

$$^{\exists!}g_2\in R\ \text{such that}\ \ g_1(X)-g_1(0)=g_2(X)f(X)$$

が成り立つことが分かる. この操作を繰り返すことで

$$\begin{aligned}
g_0(X)&=g_0(0)+g_1(X)f(X)\\
&=g_0(0)+(g_1(0)+f(X)g_2(X))f(X)=g_0(0)+g_1(0)f(X)+g_2(X)f(X)^2\\
&=\dots\\
&=g_0(0)+g_1(0)f(X)+g_2(0)f(X)^2+g_3(X)f(X)^3+\dots
\end{aligned}$$

を得ることができる. (収束性は $\mathcal{O}'$ の完備性と形式的冪級数環の定義より ok.) このとき $N_f(h):=g_0(0)+g_1(0)X+g_2(0)X^2+g_3(0)X^3+\dots$ が求めるものである. (f を代入すると $N_f(h)(f)=g_0(X)$ となる.)

(性質 1) $\mathfrak{p}_n$ を k_ξ^n の $\mathfrak{p}'$ の上にある素イデアルとする. このとき任意の $h\in R$ に対して

$$\begin{aligned}
N(h)(X^q)&\equiv N(h)(f)\bmod\mathfrak{p}_1\quad(\because f\equiv X^q\bmod\mathfrak{p}'\text{と}\ \mathfrak{p}_1\text{の取り方})\\
&\equiv(h(X))^q\bmod\mathfrak{p}_1\quad(\because N_f(h)(f)\text{の定義に現れる}\omega\text{は}\ \mathfrak{p}_1\text{の元})\\
&\equiv h^{\varphi}(X^q)\bmod\mathfrak{p}'\quad(\because\varphi\ \text{は}\ \bmod\mathfrak{p}'\text{で係数を}\ q\ \text{乗})
\end{aligned}$$

が成り立つ. しかし $N(h)-h^{\varphi}\in R$ であるからこの合同は $\bmod\mathfrak{p}'$ で成り立たなければならない. ok.

(性質 2) 一意性より $\varphi\circ N_f\circ\varphi^{-1}$ が $N_{\varphi(f)}$ の性質を満たせばよい. (2.2) の両辺に φ を作用させると

$$\begin{aligned}
&\varphi(N_f(h)(f))=\prod_{\omega\in W_f^1}\varphi(h(X[+]_f\omega))\\
\longrightarrow&\varphi(N_f(h))(\varphi(f))=\prod_{\omega\in W_f^1}h^{\varphi}(X[+]_{\varphi(f)}\omega^{\varphi})\\
\longrightarrow&(\varphi\circ N_f(h^{\varphi})\circ\varphi^{-1})(\varphi(f))=\prod_{\omega\in W^1_{\varphi(f)}}h^{\varphi}(X[+]_{\varphi(f)}\omega)\quad(\because\omega\in W_f^1\iff\omega^{\varphi}\in W^1_{\varphi(f)})
\end{aligned}$$

となり確かに ok.

(性質 3) 帰納法で示す. $i=1$ のときは (2.2) そのもので示すことはない. $i-1$ のとき成り立つと仮定する. このとき

$$\begin{aligned}
N_f^i(h)(f^{(i)})&=N^{(i-1)}_{\varphi(f)}(N_f(h))(f^{(i-1)}\circ f)\quad(\because\text{定義})\\
&=\prod_{\beta\in W^{i-1}_{\varphi(f)}}N_f(h)(f(X)[+]_{\varphi(f)}\beta)\quad(\because\text{帰納法の仮定})\\
&=\prod_{\alpha\in W_f^i/W_f^1}N_f(h)(f(X)[+]_{\varphi(f)}\beta)\quad(\because\text{同型}\ W_f^i/W_f^1\simeq W^{i-1}_{\varphi(f)};[\omega]\mapsto f(\omega))\\
&=\prod_{\alpha\in W_f^i/W_f^1}N_f(h)(f(X[+]_f\alpha))\quad(\because F_{\varphi(f)}(f(X),f(\alpha))=f(F_f(X,\alpha)))\\
&=\prod_{\alpha\in W_f^i/W_f^1}\prod_{\gamma\in W_f^1}h(X[+]_f\alpha[+]_f\gamma)\quad(\because\text{定義})\\
&=\prod_{\omega\in W_f^i}h(X[+]_f\omega)\quad(\because\alpha[+]_f\gamma\text{は}\ W_f^i\text{全体を渡る})
\end{aligned}$$

となり確かに ok.

(性質 4) 次の主張「$h \in R$ が $h(f) \equiv 1 \bmod \mathfrak{p}'^k$ を満たすならば $h(X) \equiv 1 \bmod \mathfrak{p}'^k$.」を用いる.

> 対偶を示す. 素元 $\pi \in \mathfrak{p}'$ を一つ固定し, $h(X) = 1 + \pi^\mu \sum_{i\geq 0} a_i X^i$ $(\mu < k)$ とおく. そして n を初めて $a_n \not\equiv \mathfrak{p}'$ となるものとする. (つまり $h(X) \not\equiv 1 \bmod \mathfrak{p}'^k$ と仮定する.) このとき
>
> $$\sum_{i\geq 0} a_i f^i \equiv a_n X^{q^n} + \sum_{i>n} a_i X^{q^i} \neq 0 \bmod \mathfrak{p}'$$
>
> が成り立つ. 従って
>
> $$h(f) = 1 + \pi^\mu \sum_{i\geq 0} a_i f^i \equiv 1 + \pi^n a_n X^{q^n} + \sum_{i>n} a_i X^{q^i} \neq 1 \bmod \mathfrak{p}'^k$$
>
> となり確かに示された.

まず $i = 1$ のとき $h \equiv 1 \bmod \mathfrak{p}'$ と仮定すると, ある $h_1 \in R$ を用いて $h = 1 + \pi h_1$ と書ける. このとき

$$\begin{aligned} N(h)(f) &\equiv (1 + \pi h_1)^q \bmod \mathfrak{p}_1 \\ &\equiv 1 \bmod \mathfrak{p}_1 \mathfrak{p}' \end{aligned}$$

である. $N(h)(f) - 1 \in R$ であるからこの合同は $\bmod \mathfrak{p}'^2$ で成り立たなければならない. 従って最初に示した主張より $N(h) \equiv 1 \bmod \mathfrak{p}'^2$ が成り立つ. 次に $i - 1$ で成り立つと仮定, すなわち「$h \equiv 1 \bmod \mathfrak{p}'^{i-1}$ ならば $N(h) \equiv 1 \bmod \mathfrak{p}'^i$」が成り立つと仮定する. また, $h \equiv 1 \bmod \mathfrak{p}'^i$ が成り立つと仮定する. このとき帰納法の仮定から $N(h) \equiv 1 \bmod \mathfrak{p}'^i$ が成り立つ. 従って

$$\begin{aligned} N(h)(X^q) &\equiv N(h)(f) \bmod \mathfrak{p}' \\ &\equiv (h(X))^q \bmod \mathfrak{p}' \mathfrak{p}_1 \\ &\equiv 1 \bmod \mathfrak{p}'^i \mathfrak{p}_1 \end{aligned}$$

を得る. $N(h) - 1 \in R$ であるから, この合同は $\bmod \mathfrak{p}'^{i+1}$ で成り立たなければならない. 従って確かに $N(h)(X) \equiv 1 \bmod \mathfrak{p}'^{i+1}$ が成り立つ. ok. □

$h \in X^i R^\times$ $(i \geq 0)$ ならば $N(h) \in X^i R^\times$ が成り立つ. これは以下のようにして分かる. まず $h = uX^i$ $(u \in R^\times)$ と表しておく. このとき N_f の乗法性から $N(h) = N(u)N(X)^i$ であるから, $N(u) \in R^\times, N(X) \in XR^\times$ を示せば十分である. 前者は

$$1 = N(uu^{-1}) = N(u)N(u^{-1})$$

より ok. 後者を示す. $N(X)$ は $N(X) = g_0(0) + g_1(0)X + \dots$ と構成されていて, $0 \in W_f^1$ より $g_0(0) = 0$ であるから, $g_1(0) = g_0(0)/f(0) \in \mathcal{O}'^\times$ を示せばよい. さらに $f(X) \equiv u\pi X \bmod \deg 2$ であるから $g_0(X) \equiv u'\pi X \bmod \deg 2$ を示せばよい. まず

$$\begin{aligned} g_0(X) &= \prod_{\omega \in W_f^1} (X[+]_f \omega) \\ &= X \prod_{0 \neq \omega \in W_f^1} (X[+]_f \omega) \\ &\equiv X \prod_{0 \neq \omega \in W_f^1} \omega \bmod \deg 2 \end{aligned}$$

が成り立つ. ここで, W_f^1 は $f = \pi X + \dots + X^q$ の根全体, すなわち $W_f^1 \setminus \{0\}$ は $f/X = \pi + \dots + X^{q-1}$ の根全体であったことを思い出す. 従って $\prod_{0\neq\omega\in W_f^1} \omega$ は f/X の定数項 (の ± 1 倍) に一致するので確かに $g_0(X) \equiv \pi X \bmod \deg 2$ となっている. ok.

Theorem 2.3 (Coleman ベキ級数)**.** $\beta=\{\beta_n\in(k_\xi)^\times\}_{n\geq 0}$ を $N_{m,n}(\beta_m)=\beta_n$ を満たす列とする. ただし, $m\geq n$ のとき $N_{m,n}:k_\xi^m\to k_\xi^n$ をノルムとする. (id est $\beta\in\varprojlim_n(k_\xi^n)^\times$, ただし逆系はノルムで取る.) また, $v(\beta)$ を任意の $n\geq 0$ に対して $\beta_n\mathcal{O}_n=\mathfrak{p}^{v(\beta)}$ を満たすものとする. (一般に L/K を局所体の拡大で v_L,v_K を L と K の正規化付値としたとき $v_L(x)=\frac{e}{[L:K]}v_K(x)$ が成り立つ. 従って今回の場合は v は体の取り方, すなわち n の取り方によらない.)
$f\in\mathcal{F}_\xi$ 一つ固定し, 任意の $i\geq 1$ に対して $\omega_i\in\tilde{W}^i_{\varphi^{-i}(f)}(=W^i_{\varphi^{-i}(f)}\setminus W^{i-1}_{\varphi^{-i}(f)})$ を, $\varphi^{-i}(f)(\omega_i)=\omega_{i-1}$ となるものを取る. (id est $\{\omega_i\}_{i\geq 1}\in\varprojlim_n\tilde{W}^i_{\varphi^{-i}(f)}$, ただし逆系は $\varphi^{-i}(f):\tilde{W}^i_{\varphi^{-i}(f)}\to W^{i-1}_{\varphi^{-(i-1)}}$ で取る.)
このとき一意に $g_\beta\in X^{v(\beta)}R^\times$ が存在して

$$^\forall i\geq 1,(\varphi^{-i}g_\beta)(\omega_i)=\beta_i$$

が成り立つ.

Proof. (存在性) $m\geq 1$ を固定する. 命題 1.42 より ω_n は k_ξ^n の素元であるから, β_m の ω_n 進展開を考えることで

$$^\exists h\in X^{v(\beta)}R^\times \text{ such that } h(\omega_n)=\beta_m$$

が成り立つ. もし $1\leq n\leq m$ ならば

$$\begin{aligned}(N^{(m-n)}_{\varphi^{-m}(f)}(h))(\omega_n)&=(N^{(m-n)}_{\varphi^{-m}(f)}(h))(\varphi^{-m}(f))^{(m-n)}(\omega_m)\\&=\prod_{\alpha\in W^{m-n}_{\varphi^{-m}(f)}}h(\omega_m[+]_{\varphi^{-m}(f)}\alpha)\ (\because \text{命題 2.1 の性質 3})\\&=\prod_{\sigma\in G(k_\xi^{m-n}/k')}h(\sigma(\omega_m))=\prod_{\sigma\in G(k_\xi^m/k_\xi^n)}h(\omega_m)^\sigma\ (\because Remark1.43)\\&=N_{m,n}(h(\omega_m))\\&=\beta_n\end{aligned}\tag{2.4}$$

が成り立つ. ただし一つ目の等号は

$$\begin{aligned}\varphi^{-m}(f)^{(m-n)}(\omega_m)&=\varphi^{(m-n-1)}(\varphi^{-m}(f))\circ\cdots\circ\varphi(\varphi^{-m}(f))\circ\varphi^{-m}(f)(\omega_m)\\&=\varphi^{-(n+1)}(f)\circ\cdots\circ\varphi^{-(m-1)}(f)\circ\varphi^{-m}(f)(\omega_m)\\&=\varphi^{-(n+1)}(f)\circ\cdots\circ\varphi^{-(m-1)}(f)(\omega_{m-1})\ (\because\varphi^{-i}(f)(\omega_i)=\omega_{i-1})\\&=\dots\\&=\varphi^{-(n+1)}(f)(\omega_{n+1})\\&=\omega_n\end{aligned}$$

となることから従う. 一方, 命題 2.1 の性質 2 を繰り返し用いることで

$$\begin{aligned}\varphi^n\circ N^{(i)}_f\circ\varphi^{-n}&=\varphi^n\circ N_{\varphi^{i-1}(f)}\circ\cdots\circ N_{\varphi(f)}\circ\varphi^{-n}\\&=\varphi^n\circ N_{\varphi^{i-1}(f)}\circ\varphi^{-n}\circ\varphi^n\circ\dots\varphi^n\circ N_{\varphi(f)}\circ\varphi^{-n}\\&=N_{\varphi^{n+i-1}(f)}\circ\cdots\circ N_{\varphi^{n+1}(f)}\circ N_{\varphi^n(f)}\\&=N^{(i)}_{\varphi^n(f)}\end{aligned}\tag{2.5}$$

を得る. 従ってノルムの乗法性を用いることで

$$\begin{aligned}\frac{N^{(m)}_{\varphi^{-m}(f)}(h)}{\varphi^n(N^{(m-n)}_{\varphi^{-m}(f)}(h))}&=\frac{N^{(m-n)}_{\varphi^{-(m-n)}(f)}(h)N^{(n)}_{\varphi^{-m}(f)}(h)}{\varphi^n(N^{(m-n)}_{\varphi^{-m}(f)}(\varphi^{-n}\circ\varphi^n(h)))}\\&=\frac{N^{(m-n)}_{\varphi^{-(m-n)}(f)}(N^{(n)}_{\varphi^{-m}(f)}(h))}{N^{(m-n)}_{\varphi^{-(m-n)}(f)}(\varphi^n(h))}\ (\because(2.5))\\&=N^{(m-n)}_{\varphi^{-(m-n)}(f)}\left(\frac{N^{(n)}_{\varphi^{-m}(f)}(h)}{\varphi^n(h)}\right)\end{aligned}$$

を得る. ただし一つ目の等号は

$$\begin{aligned} N^{(m)}_{\varphi^{-m}(f)} &= \left\{N_{\varphi^{m-1}(\varphi^{-m}(f))} \circ \cdots \circ N_{\varphi^{n}(\varphi^{-m}(f))}\right\} \circ \left\{N_{\varphi^{n-1}(\varphi^{-m}(f))} \circ \cdots \circ N_{\varphi^{-m}(f)}\right\} \\ &= N^{(m-n)}_{\varphi^{-(m-n)}(f)} \circ N^{(n)}_{\varphi^{-m}(f)} \end{aligned}$$

より従う. 従って命題 2.1 の性質 1 を繰り返し用いて

$$\begin{aligned} N^{(n)}_{\varphi^{-m}(f)}(h) &= N_{\varphi^{(n-1)-m}(f)} \circ \cdots \circ N_{\varphi^{1-m}} \circ N_{\varphi^{-m}}(h) \\ &\equiv \varphi \circ \cdots \circ \varphi \circ \varphi(h) \bmod \mathfrak{p}' \\ &= \varphi^n(h), \end{aligned}$$

すなわち $N^{(n)}_{\varphi^{-m}(f)}(h)/\varphi^n(h) \equiv 1 \bmod \mathfrak{p}'$ を得る. よって命題 2.1 の性質 4 をに繰り返し適用することで

$$\frac{N^{(m)}_{\varphi^{-m}(f)}(h)}{\varphi^n(N^{(m-n)}_{\varphi^{-m}(f)}(h))} \equiv 1 \bmod \mathfrak{p}'^{m-n+1} \tag{2.6}$$

を得る. そこで, $g_m := N^{(m)}_{\varphi^{-m}(f)}(h)$ とおくと (2.4) と (2.6) より

$$\begin{aligned} \frac{(\varphi^{-n}g_m)(\omega_n)}{\beta_n} &\equiv \frac{(N^{(m-n)}_{\varphi^{-m}(f)}(h))(\omega_n)}{\beta_n} \bmod \mathfrak{p}'^{m-n+1} \ (\because (2.6)) \\ &= 1 \ (\because (2.4)) \end{aligned}$$

が成り立つ. 最後に, $X^{v(\beta)}R^\times$ はコンパクトなので

$$^\exists g_\beta \in X^{v(\beta)}R^\times \ \text{ such that } \ g_m \to g_\beta \ (m \to \infty)$$

が成り立ち, 連続性から任意の $n \geq 1$ に対して $(\varphi^{-n}g_\beta)(\omega_n) = \beta_n$ が成り立つ.

(一意性) 背理法で示す. $g \neq g_\beta$ を, 任意の $n \geq 1$ に対し $(\varphi^{-n}g_\beta)(\omega_n) = \beta_n$ を満たすものとする. $g - g_\beta \neq 0$ であるから π^n でくくることで $(g - g_\beta)\pi^{-n}$ に Weierstrass の準備定理の系を適用できて,

$$^\exists n \geq 1, ^\exists P(X) : \text{distinguished}, ^\exists U(X) \in \mathcal{O}'[[X]]^\times \ \text{ such that } \ g - g_\beta = \pi^n P(X)U(X), \ \deg P < n$$

が成り立つ. ここで, $q^i > n$ なる i を一つ取ると, 任意の $\omega \in W^i_{\varphi^{-i}(f)}$ に対して

$$0 = \varphi^{-i}(g - g_\beta)(\omega) = \varphi^{-i}(\pi)^n\varphi^{-i}(P(\omega))\varphi^{-i}(U(\omega))$$

が成り立つ. しかし $U \in \mathcal{O}'[[X]]^\times$ であるから $U(\omega) \neq 0$ である. 従って $P(\omega) = 0$ でなければならないが, $\deg P < n < q^i$ より ($W^{-i}_\varphi(f)^i$ の元全体は $\varphi^{-i}(f)$ の根全体に一致するので)$P(X) = 0$ でなければならない. これは $g - g_\beta \neq 0$ に矛盾. □

Corollary 2.7.

- $g_{\beta\beta'} = g_\beta g_{\beta'}$.
- $N_f(g_\beta) = g_\beta^\varphi$.
- $v(\beta) = 0$ ならば $g_\beta(0)^{1-\varphi^{-1}} = \beta_0$.
- $k_\xi := \cup_n k_\xi^n$ とする. $\sigma \in G(k_\xi/k')$ に対して $\kappa(\sigma) \in \mathcal{O}^\times$ を, 任意の $\omega \in W_f$ に対して $\sigma(\omega) = [\kappa(\sigma)]_f(\omega)$ を満たすただ一つの元とする. (cf. 命題 1.42) このとき $g_{\sigma(\beta)} = g_\beta \circ [\kappa(\sigma)]_f$.

Proof. (1) $g_\beta g_{\beta'}$ が $g_{\beta\beta'}$ の性質を満たせば一意性より題意が従う. そしてそれは

$$\varphi^{-n}(g_\beta g_{\beta'})(\omega_n) = (\varphi^{-n}g_\beta)(\omega_n) \cdot (\varphi^{-n}g_{\beta'})(\omega_n) = \beta\beta'$$

より分かる.

(2) 主張の両辺に φ^{-i} を作用させた, $\varphi^{-(i-1)}g_\beta = \varphi^{-i}(N_f g_\beta)$ を示せばよい. (φ^i を作用させて復元すればよい.) そしてそれは

$$\begin{aligned}
(\varphi^{-(i-1)}g_\beta)(\omega_{i-1}) &= \beta_{i-1} \\
&= N_{i,i-1}\beta_i \ (\because (\beta_i)_i\text{の取り方}) \\
&= \prod_{\alpha \in W^1_{\varphi^{-i}(f)}} (\varphi^{-i}g_\beta)(\omega_i[+]_{\varphi^{-i}(f)}\alpha) \ (\because \text{ガロア作用の性質 (rf. Remark1.43)}) \\
&= N_{\varphi^{-i}(f)}(\varphi^{-i}g_\beta)(\varphi^{-i}(f))(\omega_i) \ (\because \text{命題 2.1}) \\
&= \varphi^{-i}(N_f g_\beta)(\omega_{i-1})
\end{aligned}$$

より分かる. ただし最後の等式は, 命題 2.1 の性質 2 を適用させたものと, $(\omega_i)_i$ の取り方より従う.

(3) $v(\beta) = 0$ とする. $g_\beta(0) = g_\beta^{\varphi^{-1}}(0)\cdot\beta_0$ を示せばよい.

$$\begin{aligned}
g_\beta(0) &= \varphi^{-1}(N_f g_\beta)(0) \ (\because (2)\text{ の結果}) \\
&= N_{\varphi^{-1}(f)}(\varphi^{-1}g_\beta)(0) \ (\because \text{命題 2.1 性質 2}) \\
&= N_{\varphi^{-1}(f)}(\varphi^{-1}g_\beta)(\varphi^{-1}(f)(0)) \ (\because \varphi^{-1}(f)(0) = 0) \\
&= \prod_{\alpha \in W^1_{\varphi^{-1}(f)}} \varphi^{-1}g_\beta(\alpha) \ (\because \text{命題 2.1}) \\
&= (\varphi^{-1}g_\beta)(0)\cdot N_{1,0}(\beta_1) \ (\because \alpha = 0 \text{ と} \alpha \neq 0 \text{ に分割})
\end{aligned}$$

より ok.

(4) 一意性より $g_\beta \circ [\kappa(\sigma)]_f$ が $g_{\sigma(\beta)}$ の性質を満たせばよい.

$$\begin{aligned}
\varphi^{-i}(g_\beta \circ [\kappa(\sigma)]_f)(\omega_i) &= (\varphi^{-i}g_\beta)\circ[\kappa(\sigma)]_{\varphi^{-i}(f)}(\omega_i) \\
&= (\varphi^{-i}g_\beta)(\sigma(\omega_i)) \\
&= \sigma((\varphi^{-i}g_\beta)(\omega_i)) \\
&= \sigma(\beta_i)
\end{aligned}$$

より ok. □

もう一度大事な性質をまとめると, 以下の通りであった.

- $^{\exists!}N_\beta : \mathcal{O}'[[X]] \to \mathcal{O}'[[X]]$ such that $N_f(h)(f) = \prod_{\alpha\in W_f^1} h(X[+]_f\alpha)$.
- $(\omega_i)_i \in \varprojlim_i W^i_{\varphi^{-i}(f)}$ とする. このとき任意の $\beta = (\beta_i)_i \in \varprojlim_n (k_\xi^n)^\times$ に対して

$$^{\exists!}g_\beta \in \mathcal{O}'((X))^\times \text{ such that } {}^{\forall}i \geq 1,\ (\varphi^{-i}g_\beta)(\omega_i) = \beta_i$$

Example 2.8 ([2, Theorem 13.38])**.** $k = k' = \mathbb{Q}_p, f = (1+X)^p - 1$ とする．このとき $F_f = \hat{\mathbb{G}}_m, f = [p]_{\hat{\mathbb{G}}_m}$ であったことを思い出す．このとき

$$W^i_{\varphi^{-i}(f)} = W^i_f = \operatorname{Ker} f^{(i)} = \left\{\zeta - 1 \mid \zeta \in \mu_{p^i}\right\}$$

であることが簡単に分かる．従って

$$k^i := k^i_\zeta = \mathbb{Q}_p(W^i_f) = \mathbb{Q}_p(\zeta_{p^i}) \ \ (\text{ただし,} \zeta^p_{p^i} = \zeta_{p^{i-1}} \ (^\forall i))$$

と，$\mathfrak{p}_i = (\zeta_{p^i} - 1)$ を得る．また，

$$U^{(1)}_i := 1 + \mathfrak{p}_i = \left\{x \in \mathcal{O}_i^\times \mid x \equiv 1 \bmod (\zeta_{p^i} - 1)\right\}$$
$$U := \varprojlim_i U^{(1)}_i \ \left(\overset{\text{analogy}}{\leftrightarrow} \varprojlim (k^n_\xi)^\times\right)$$

とする．$u = (u_i) \in U$ に対し定義より $v(u) = 0$ であり，定理 2.3 より

$$^{\exists!} g_u \in \mathbb{Z}_p[[X]]^\times \ \text{ such that } \ ^\forall i \geq 1, g_u(\zeta_{p^i} - 1) = u_i$$

が成り立つ．ここで，$g_u(0) \equiv g_u(\zeta_p - 1) = u_0 \bmod (\zeta_p - 1)$ であって，$g_u(0) - u_0 \in \mathbb{Z}_p$ であるから，結局 $g_u(0) \equiv u_0 \equiv 1 \bmod p$ を得る．また，系 2.7 より

$$g_u([p]) = N g_u([p]) = \prod_{\zeta \in \mu_p} g_u(\zeta(1+X) - 1)$$

が成り立つことが分かる．以上より，同型

$$U \simeq \left\{ g \in \mathbb{Z}_p[[X]]^\times \mid g(0) \equiv 1 \bmod p, \ g((X+1)^p - 1) = \prod_{\zeta \in \mu_p} g(\zeta(1+X) - 1) \right\}; u \mapsto g_u$$

を得る．逆写像は $g \mapsto (g(\zeta_{p^i} - 1)_i)$ である．

3 MEASURES FROM UNITS

まず p 進測度の復習から始める．以下の記法を統一する．

- G: 副有限群 (id est $G = \varprojlim_i G_i, G_i$: 有限群),
- $\pi_i : G \to G_i$: 射影,
- $\pi_{ij} : G_i \to G_j \ (i \geq j)$: 逆系,
- M: アーベル群.

特に $G = \mathbb{Z}_p$ ならば，$G_i = \mathbb{Z}_p/p^i\mathbb{Z}_p \simeq \mathbb{Z}/p^i\mathbb{Z}$ であることを思い出しておく．

Proposition 3.1. $X := \{U \subset G \mid \text{open, compact}\}, \operatorname{Step}(G) := \{f : G \to M \mid \text{局所定数関数 }\}$ とする．このとき以下の三つは同一視できる．

- $\{\mu_i : G_i \to M\}_i$ such that 「$i \geq j \Longrightarrow {}^\forall a \in G_i, \mu_i(a) = \sum_{\pi_{ij}(a)=b} \mu_i(b)$"」.
- $\mu : X \to M$ such that $\mu\left(\coprod_{i:\text{fin.}} U_i\right) = \sum_{i:\text{fin.}} \mu(U_i)$.
- $\phi : \operatorname{Step}(G) \to M$; 線形写像.

Proof. 証明の前に一つ補題を用意する．

Lemma 3.2. 任意の $U \in X$ に対して，ある i と有限個の $a_j \in G_i$ が存在して $U = \coprod_{i,j} \pi_i^{-1}(a_j)$ が成り立つ．

Proof. $U=\varnothing$ のときは自明に成り立つので, $U\neq\varnothing$ のときを考える. $x\in U$ を一つ取る. このとき G_i に離散位相が入っていることから $\{\pi_i(x)\}\subset G_i$ は open である. 従って $\pi_i^{-1}(\pi_i(x))$ は open の連続写像による引き戻しなので, (x を含む) G の open subset であり, 従って $\pi_i^{-1}(\pi_i(x))\subset U$ が成り立つ. (これどうしてだっけ.) 以上より

$$U=\bigcup_{x\in U}\pi_i^{-1}(\pi_i(x))=\bigcup_{x\in U,\pi_i(x)=a}\pi_i^{-1}(a)$$

が成り立つ. U はコンパクトであったから結局上の和は有限個の $\pi_i(x)=a_j$ で表せる. さらに $i>j$ ならば $b\in G_j$ に対して

$$\pi_j^{-1}(b)=\coprod_{\pi_{ij}(a)=b}\pi_i^{-1}(a) \tag{3.3}$$

より非交和で表せる. □

((2) ⇒ (1)) $i\geq j, b\in G_j$ とする. このとき

$$\mu_j(b):=\mu\left(\pi_j^{-1}(b)\right)$$

とすればよい. 実際,

$$\begin{aligned}\mu_j(b)&=\mu(\pi_j^{-1}(b))\\&=\mu\left(\coprod_{\pi_{ij}(a)=b}\pi_i^{-1}(a)\right)\quad(\because (3.3))\\&=\sum_{\pi_{ij}(a)=b}\mu\left(\pi_i^{-1}(a)\right)\quad(\because \mu\text{の取り方})\\&=\sum_{\pi_{ij}(a)=b}\mu_i(a)\quad(\because \mu_i\text{の定理})\end{aligned}$$

となることから分かる.

((1) ⇒ (3)) 任意の $f\in\mathrm{Step}(G)$ は補題 3.2 より

$$\chi_{i,a}(x)=\begin{cases}1 & (x\in\pi_i^{-1}(a))\\ 0 & (x\notin\pi_i^{-1}(a))\end{cases}$$

の M 係数の線形和で表せる. 従って $\phi(f)$ を $\phi(\chi_{i,a}):=\mu_i(a)$ の線形和として定義すれば ok.

((3) ⇒ (2)) $\phi:\mathrm{Step}(G)\to M$ に対して $\mu(U):=\phi(\chi_U)$ と定義すればよい. ここで

$$\chi_U(x)=\begin{cases}1 & (x\in U)\\ 0 & (x\notin U)\end{cases}$$

である. 実際,

$$\begin{aligned}\mu\left(\coprod_{i:\text{fin.}}U_i\right)&=\phi\left(\chi_{\coprod_{i:\text{fin.}}U_i}\right)\\&=\phi\left(\sum_{i:\text{fin.}}\chi_{U_i}\right)\\&=\sum_{i:\text{fin.}}\phi(\chi_{U_i})\\&=\sum_{i:\text{fin.}}\mu(U_i)\end{aligned}$$

となり ok. □

Definition 3.4. 命題 3.1 の条件のいずれか一つ (従って全て) を満たすものを, G **上の** M **値 distribution** という. これら全体の集合を $\Lambda(G,M)$ と表す.

Example 3.5 (Dirac distribution)**.** $a \in G$ を一つ取る. $\Lambda(G, M)$ の中には Dirac distribution という以下を満たす distribution がある.

- $\{\delta_{a,i} : G_i \to M\}_i$ で, $x \in G_i$ に対して

$$\delta_{a,i}(x) := \begin{cases} 1 & (a \in \pi_i^{-1}(x)), \\ 0 & (a \notin \pi_i^{-1}(x)). \end{cases}$$

- 任意の $U \in X$ に対し

$$\delta_a(U) := \begin{cases} 1 & (a \in U), \\ 0 & (a \notin U). \end{cases}$$

- 線形写像 $\delta_a : \mathrm{Step}(G) \to M$ で $\delta_a(f) := f(a)$.

任意の $\mu_1, \mu_2 \in \Lambda(G, M)$ に対し, 以下の演算により $\Lambda(G, M)$ はアーベル群になる.

$$\mu_1 + \mu_2 : U \mapsto \mu_1(U) + \mu_2(U).$$

特に A を可換環, M を A 代数とすると $\Lambda(G, M)$ は以下の (畳み込み) 積により A 代数となる.

$$\mu_1 * \mu_2; U \mapsto \sum_{i=1}^{n} \mu_1\left(U\sigma_i^{-1}\right) \mu_2\left(\sigma_i H\right)$$

ただし, $H := \{x \in G \mid Ux = U\} \leq G$ であり, $G = \cup_{i=1}^{n} \sigma_i H$ は剰余分解である.

Definition 3.6. $M \subset \mathbb{C}_p$ と仮定する. $\mu \in \Lambda(G, M)$ が G **上の** M **値 (p-adic) 測度 (measure)** であるとは

$$^{\forall} U \subset G; \text{open, compact}, \quad |\mu(U)| < \infty$$

であることをいう. 特に $|\mu(U)| \leq 1$ のとき, μ を **integral measure** という.

群 G が有限であればアーベル群としての同型

$$\Lambda(G, M) \xrightarrow{\simeq} M[G]; \mu \mapsto \sum_{x \in G} \mu(\{x\})x$$

が成り立つ. (逆写像は $\sum_{x \in G} \sigma_x x$ に対して $\mu(\{x\}) := \sigma_x$ なる μ を対応させればよい.) 特に M が A 代数ならば上の同型は A 代数としての同型である. 従って有限とは限らない G に対して命題 3.1 より

$$\begin{aligned} \Lambda(G, M) &\simeq \varprojlim_i \Lambda(G_i, M); \mu \mapsto \mu_i \\ &\simeq \varprojlim_i M[G_i] \\ &=: M[[G]] \end{aligned}$$

を得る. G が $\mathbb{Z}_p$ 拡大のガロア群, $M = \mathbb{Z}_p$ であったとき, $M[[G]]$ は岩澤加群という名前があった. つまりこの場合 p-adic distribution であることと岩澤加群であることは同値である.

$M \subset \mathbb{C}_p, \mu \in \Lambda(G, M)$ を測度とする. このとき $f \in \mathrm{Step}(G)$ に対し

$$\int_G f(x) d\mu := \mu(f)$$

と定義する. これを G 上の連続関数に延長したい. $C(G, \mathbb{C}_p)$ を G 上の連続関数で, ノルム

$$||f|| := \sup_{x \in G} |f(x)|$$

による $\mathbb{C}_p$-Banach 空間とする. (すなわちノルム $||\cdot||$ により完備な空間.)

Lemma 3.7. $\mathrm{Step}(G)$ は $C(G, \mathbb{C}_p)$ で稠密である.

Proof. 任意の $f \in C(G, \mathbb{C}_p)$ を一つ取り, $f_i := \sum_{a \in X_i} f(a)\chi_{a,i} \in \mathrm{Step}(G)$ とおく. ただし X_i は $G/\operatorname{Ker}\pi_i \simeq G_i$ の完全代表系であって, $a \in X_i$と$\pi_i(a) \in G_i$ を同一視する. このとき点列 $\{f_i\}_i$ が f に収束することを見ればよい.

任意に $\varepsilon > 0$, 任意に $x \in G$ を取る. このとき f の連続性から

$$^{\exists}\delta > 0 \text{ such that}「y \in (\delta\text{に依存した } x \text{ の近傍}) \Longrightarrow |f(x) - f(y)| < \varepsilon」 \tag{3.8}$$

が成り立つ. さて, $x \in G$ に対して $\pi_i(x) \in G_i$ が $[a] \in G/\operatorname{Ker}\pi_i$ に対応しているとすれば

$$\begin{aligned} ||f - f_i|| &= \sup_{x \in G} |f(x) - f_i(x)| \\ &= \sup_{x \in G} \left| f(x) - \sum_{a \in X_i} f(a)\chi_{a,i}(x) \right| \\ &= \sup_{x \in G} |f(x) - f(a)| \end{aligned}$$

である. あとは a が x の近傍であれば (3.8) より $||f - f_i|| < \varepsilon$ となって ok. a が x の近傍, すなわちある N が存在して $\pi_N(a) = \pi_N(x)$ を示せばよい. 特に $a \leftrightarrow \pi_i(x)$ なので $\pi_N \circ \pi_i(x) = \pi_N(x)$ を示せばよいが, これは射影極限の逆系の取り方の定義である. ok. □

Proposition 3.9. 任意の $f \in C(G, \mathbb{C}_p)$ に対して

$$\int_G f(x)d\mu$$

は一意的に存在する.

Proof. まず準備をする. $g = \sum_{i,a:\mathrm{fin.}} c_{i,a}\chi_{i,a} \in \mathrm{Step}(G)$ $(c_{i,a} \in M)$ に対して

$$\begin{aligned} \left| \int_G g(x)d\mu \right| &= |\mu(g)| \quad (\because \text{定義}) \\ &= \left| \sum_{i,a} c_{i,a}\mu(\chi_{i,a}) \right| \quad (\because \mu\text{の線形性}) \\ &\leq {}^{\exists}C \max_{i,a} |c_{i,a}| \quad (\because \mu\text{は測度, すなわち有界}) \\ &= C||g|| \end{aligned} \tag{3.10}$$

が成り立つ. ただし最後の等式は, $x \in G$ が $\pi_i(x) = a$ を満たすならば, すなわち $x \in \pi_i^{-1}(a)$ ならば, $g(x) = c_{i,a}$ となり従って $||g|| = \sup_{x \in G} |g(x)| = \max_{i,a} |c_{i,a}|$ となることより従う.

さて, 任意の $f \in C(G, \mathbb{C}_p)$ に対して補題 3.7 より

$$^{\exists}\{f_i\}_i \subset \mathrm{Step}(G); \text{Cauchy 列 such that } f_i \to f \ (i \to \infty)$$

が成り立つ. 任意の $\varepsilon > 0$ を一つ取る. このとき $\{f_i\}_i$ は Cauchy 列なので

$$^{\exists}N \in \mathbb{N} \text{ such that}「i, j \geq N \Longrightarrow ||f_i - f_j|| < \varepsilon」$$

を得る. 従って (3.10) より

$$\left| \int_G f_i(x)d\mu - \int_G f_j(x)d\mu \right| = |\mu(f_i - f_j)| \leq C||f_i - f_j|| < C\varepsilon$$

となるので $\{\int_G f_i(x)d\mu\}_i$ が $\mathbb{C}_p$ 内の Cauchy 列となり収束する. 従って

$$\int_G f(x)d\mu = \lim_{n \to \infty} \int_G f_n(x)d\mu \tag{3.11}$$

と定義すればよい.

次に well-defined, すなわち Cauchy 列 $\{f_i\}_i$ の取り方に依らず (3.11) が定まることを見る. $\{g_i\}_i \subset \mathrm{Step}(G)$ を f に収束する Cauchy 列で $\{f_i\}_i$ とは異なるものとする. 完備化の性質より任意の $\varepsilon > 0$ に対して n を十分大きく取れば

$$||f_n - g_n|| = ||f_n - f + f - g_n|| \leq ||f_n - f|| + ||g_n - f|| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

が成り立つ. 従って

$$\left| \int_G f_n(x)d\mu - \int_G g_n(x)d\mu \right| \leq C||f_n - g_n|| < C\varepsilon$$

となるので ok. また, 一意性は $\mathbb{C}_p$ が Hausdroff であって収束先が一意となることより従う. □

積分の定義 (3.11) だけを見ると計算が容易ではなさそうだが, 実は特性関数 $\chi_{i,a}$ についてのみ積分が計算できればよい. それは以下のようにして分かる. $f \in C(G, \mathbb{C}_p)$ に対して, f に収束する Cauchy 列 $\{f_i\}_i \subset \mathrm{Step}(G)$ は $f_i(x) := \sum_{i,a} f(a)\chi_{i,a}(x)$ と取れるのであった. このとき

$$\begin{aligned} \int_G f(x)d\mu &= \lim_{n\to\infty} \int_G f_n(x)d\mu \\ &= \lim_{n\to\infty} \sum_{a\in\chi_n} f(a) \int_G \chi_{n,a}(x)d\mu \quad (\because \sum_{i,a} \text{は有限和}) \end{aligned}$$

と計算できる.

Example 3.12. Dirac distribution δ_a は 0 と 1 のみしか値を取らないので測度である. このとき $f \in \mathrm{Step}(G)$ に対して

$$\int_G f(x)d\delta_a = \delta_a(f) = f(a)$$

である. 従って $f \in C(G, \mathbb{C}_p)$ に対しても $\int_G f(x)d\delta_a = f(a)$ である.

Fact 3.13 (Amith transform)**.** 以下の全単射が存在する.

$$\{\mu \in \Lambda(\mathbb{Z}_p, \mathbb{C}_p) \mid \mu : \text{measure}\} \xrightarrow{1:1} \mathcal{O}_{\mathbb{C}_p}[[T]] \otimes \mathbb{C}_p; \mu \mapsto \int_{\mathbb{Z}_p} (1+T)^x d\mu(x) = \sum_{n=0}^{\infty} \left\{ \int_{\mathbb{Z}_p} \binom{x}{n} d\mu \right\} T^n$$

測度の畳み込み積は積分の積に対応する.

$$\int_G f(x)d(\mu_1 * \mu_2) = \left(\int_G f(x)d\mu_1 \right) \left(\int_G f(x)d\mu_2 \right)$$

任意の $f \in C(G, \mathbb{C}_p)$ に対して $(\mu_1 * \mu_2)(f) = \mu_1(f)\mu_2(f)$ より.

Definition 3.14. G をアーベル群, A を可換環, M を A 代数とする. また, $S \subset \Lambda(G, M)$ を零因子でない元全体の集合とする. このとき局所化 $S^{-1}\Lambda(G, M)$ の元 $\frac{\mu}{s}$ で μ, s 共に測度であるものを**擬測度 (pseudo-measure)** という.

$\frac{\mu}{s} \in S^{-1}\Lambda(G, A)$ を擬測度で $\int_G f(x)ds \neq 0$ を満たすものとする. このとき

$$\int_G f(x)d\left(\frac{\mu}{s}\right) := \left(\int_G f d\mu \right) / \left(\int_G f ds \right)$$

が畳み込み積の式から well-defined に定まる.

$$\int_G f d\mu = \int_G f d\left(\frac{\mu}{s} * s\right) = \left(\int_G f d\left(\frac{\mu}{s}\right) \right) \left(\int_G f ds \right)$$

の両辺を $\int_G f ds$ で割ればよい.

Definition 3.15. $\Lambda(G,A)$ の添加イデアル **(augmentaion ideal)** を

$$\mathrm{Ker}\,(\Lambda(G,A)\to A;\mu\mapsto\mu(G))$$

と定義する.

測度の構成を行う. 以下では height 1 の Lubin-Tate 形式群のみを扱う, すなわち $k=\mathbb{Q}_p, k'/\mathbb{Q}_p$ を不分岐拡大とする. ちなみに, 楕円曲線に付随する形式群は height 1 の Lubin-Tate であることが知られているので, この設定は楕円曲線の p 進 L 関数を構成するのに問題はない.

命題 1.38 より

$$^{\exists}\theta:\hat{\mathbb{G}}_m\xrightarrow{\simeq}_{\mathcal{O}_K}F_f\ \text{ such that }\begin{cases}\theta(T)\equiv\Omega T \bmod \deg 2 & (\Omega^{\varphi-1}=\pi'/p)\\ f\circ\theta=\theta^{\varphi}\circ[p]_{\hat{\mathbb{G}}_m}\end{cases}$$

が成り立っていた. さらに任意の $n\geq 1$ に対して $\zeta_{p^n}\in\mu_{p^n}$ を, $\zeta_{p^n}^p=\zeta_{p^{n-1}}$ となるように取る. このとき

$$\omega_n:=\theta^{\varphi^{-n}}(\zeta_{p^n}-1)$$

とすると例 2.8 より $\omega_n\in\widetilde{W}^n_{\varphi^{-n}(f)}\left(=W^n_{\varphi^{-n}(f)}\setminus W^{n-1}_{\varphi^{-n}(f)}\right)$ かつ, $\varphi^{-n}(f)(\omega_n)=\omega_{n-1}$ が成り立つ. 以上より $(\omega_n)_n$ は F_f の Tate 加群の生成元となる.

任意の局所体 k に対して $U(k):=1+\mathfrak{p}$ として,

$$\beta=(\beta_n)\in\mathscr{U}:=\varprojlim_n U(k_\xi^n)$$

とすると

$$^{\exists!}g_\beta\in\mathcal{O}'[[T]]^\times\ \text{ such that }\ ^{\forall}n\geq 1,\ (\varphi^{-n}g_\beta)(\omega_n)=\beta_n$$

が成り立つ. また, 系 2.7(3) より $g_\beta\equiv 1 \bmod (\mathfrak{p}',T)$ なので $\log g_\beta$ は $k'[[T]]$ で収束することに注意する.

Lemma 3.16.

$$\begin{aligned}\widetilde{\log g_\beta}(T):&=\log g_\beta-\frac{1}{p}\log(g_\beta^{\varphi}\circ f)\\ &=\log g_\beta-\frac{1}{p}\sum_{\omega\in W_f^1}\log g_\beta(T[+]\omega)\end{aligned}$$

は整係数.

Proof. 二つ目の等号は系 2.7(2) を用いて

$$g_\beta^{\varphi}\circ f=N_f(g_\beta)(f)=\prod_{\omega\in W_f^1}g_\beta(T[+]\omega)$$

となることより従う. まず

$$(g_\beta(T))^p\equiv g_\beta^{\varphi}(T^p)\equiv g_\beta^{\varphi}\circ f=\prod_{\omega\in W_f^1}g_\beta(T[+]\omega)\bmod\mathfrak{p}'$$

が成り立つ. 両辺の log を取ることで

$$p\log g_\beta\equiv\sum_{\omega\in W_f^1}\log g_\beta(T[+]\omega)\bmod\mathfrak{p}'$$

を得るが, $k'/\mathbb{Q}_p$ は不分岐拡大なので $\mathfrak{p}'=(p)$ という形をしている. 従って

$$p\log g_\beta-\sum_{\omega\in W_f^1}\log g_\beta(T[+]\omega)=ph(X)\ (^{\exists}h(X)\in\mathcal{O}_K[[X]])$$

が得られ, 両辺 p で割ることで題意を得る. □

$\widetilde{a_\beta}(T) := \widetilde{\log g_\beta} \circ \theta(T) \in \mathcal{O}_K[[T]]$ とすると Amith transform より

$$^{\exists}\mu_\beta : \mathbb{Z}_p\text{上 } \mathcal{O}_K\text{値測度 such that } \widetilde{a_\beta}(T) = P_{\mu_\beta} := \int_{\mathbb{Z}_p} (1+T)^\alpha d\mu_\beta(\alpha)$$

が成り立つ. しかし実際 μ_β は $\mathbb{Z}_p^\times$ 上の値で定まる, すなわち $\mathbb{Z}_p^\times$ 上で定まれば自然に $\mathbb{Z}_p$ に拡張される.

$\mathbb{Z}_p^\times$ 上の測度 $\tilde{\mu}(= \mu_\beta|_{\mathbb{Z}_p^\times})$ に対して $\tilde{\mu}|_{p\mathbb{Z}_p} := 0$ とすると

$$\begin{aligned} P_{\tilde{\mu}}(T) &= \int_{\mathbb{Z}_p} (1+T)^\alpha d\tilde{\mu}(\alpha) \\ &= \int_{\mathbb{Z}_p^\times} (1+T)^\alpha d\tilde{\mu} + \int_{p\mathbb{Z}_p} (1+T)^\alpha d\tilde{\mu} \\ &= \int_{\mathbb{Z}_p^\times} (1+T)^\alpha d\mu_\beta \\ &= \int_{\mathbb{Z}_p} (1+T)^\alpha d\mu_\beta - \int_{p\mathbb{Z}_p} (1+T)^\alpha d\mu_\beta \end{aligned}$$

が成り立つ. ここで,

$$\begin{aligned} \int_{p\mathbb{Z}_p} (1+T)^\alpha d\mu_\beta &= \int_{\mathbb{Z}_p} (1+T)^\alpha 1_{p\mathbb{Z}_p}(\alpha) d\mu_\beta \\ &= \frac{1}{p} \sum_{\zeta^p=1} \int_{\mathbb{Z}_p} \zeta^\alpha (1+T)^\alpha d\mu_\beta \quad \left(\because 1_{a+p^N\mathbb{Z}_p} = \frac{1}{p^N} \sum_{\zeta^{p^N}=1} \zeta^{x-a} \right) \\ &= \frac{1}{p} \sum_{\zeta^p=1} P_{\mu_\beta}(\zeta(1+T)-1) \end{aligned}$$

であるから結局

$$P_{\tilde{\mu}}(T) = P_{\mu_\beta}(T) - \frac{1}{p} \sum_{\zeta^p=1} P_{\mu_\beta}(\zeta(1+T)-1)$$

を得る. ところが

$$\frac{1}{p} \sum_{\zeta^p=1} P_{\mu_\beta}(\zeta(1+T)-1) = \frac{1}{p} \sum_{\zeta^p=1} P_{\mu_\beta}(T[+]_{\hat{\mathbb{G}}_m}(\zeta-1)) = 0$$

となることが示せるので $P_{\tilde{\mu}} = P_{\mu_\beta}$, すなわち $\tilde{\mu} = \mu_\beta$ が得られる.

さて, この議論を $G := G(k_\xi/k')$ に適用する. そのために同型

$$^{\exists!}\kappa : G \xrightarrow{\simeq} \mathbb{Z}_p^\times; \sigma(\omega) = [\kappa(\sigma)]_f(\omega)\ (\omega \in W_f)$$

があったことを思い出す.

Definition 3.17. 任意の $\beta \in \mathscr{U}$ に対し $G := G(k_\xi/k')$ 上 $\mathcal{O}_K$ 値測度 μ_β を

$$\widetilde{\log g_\beta} \circ \theta(T) = \int_G (1+T)^{\kappa(\sigma)} d\mu_\beta(\sigma)$$

を満たすものとする.

Lemma 3.18.

- $\mu_{\beta\beta'} = \mu_\beta + \mu_{\beta'}$.
- $\gamma \in G \Longrightarrow \mu_{\gamma(\beta)}(\gamma U) = \mu_\beta(U)$.
- μ_β は $(\zeta_n)_n$ の選び方のみに依る. (すなわち π', Ω に依らない？) もし $\zeta'_n := \zeta_n^{\kappa(\gamma)}$ $(\gamma \in G)$ ならば $\mu'_\beta(U) = \mu_\beta(\gamma U)$ が成り立つ.

Proof. (1) 系 2.7(1) より $g_{\beta\beta'} = g_\beta g_{\beta'}$ なので

$$\widetilde{\log g_{\beta}g_{\beta'}} \circ \theta = \left(\widetilde{\log g_\beta} + \widetilde{\log g_{\beta'}}\right) \circ \theta = \widetilde{\log g_\beta} \circ \theta + \widetilde{\log g_{\beta'}} \circ \theta$$

より ok.

(2) ???

(3) ??? □

$\mathcal{G} := G(k_\xi/k)$ とすると $\mathcal{G}/G = G(k'/k)$ は位数 d の巡回群である. $U \subset \mathcal{G}$ を開かつコンパクトな部分集合で, $\mathcal{G}/G$ において G の同値類に含まれるものとする. $\gamma \in G$ に対して $\gamma U \subset G$ ならば $\mu_\beta(U) := \mu_{\gamma(\beta)}(\gamma U)$ と定義する. これは補題 3.18(2) より γ に依らず, 従って well-defined である. よって μ_β を $\mathcal{G}$ 上の測度に拡張でき, 写像

$$i : \mathscr{U} \to \Lambda(\mathcal{G}, \mathcal{O}_K); \beta \mapsto \mu_\beta$$

を得る.

Corollary 3.19. $i : \mathscr{U} \to \Lambda(\mathcal{G}, \mathcal{O}_K)$ は単射 $\mathbb{Z}_p[[\mathcal{G}]]$ 準同型である.

Proof. $\mathbb{Z}_p[[\mathcal{G}]]$ 準同型であることは 3.18(1)(2) より従うので単射だけ示す. $\mu_\beta = 0$ とすると μ_β の定義より $\widetilde{\log g_\beta} \circ \theta = 0$ である. θ は同型であったから $\widetilde{\log g_\beta} = 0$, さらに $g_\beta = 1$ であることが示せる. しかし任意の $n \geq 1$ に対して

$$1 = (\varphi^{-n} g_\beta)(\omega_n) = \beta_n$$

が成り立つので $\beta = (\beta_n) = 1$ でなければならない. □

Proposition 3.20. $G_n := G(k_\xi/k_\xi^n)(= \kappa^{-1}(1 + p^n\mathbb{Z}_p))$ に対して

$$\mu_\beta(G_n) = \frac{1}{p^n} \sum_{j=0}^{p^n-1} \widetilde{a_\beta}(\zeta_{p^n}^j - 1)\zeta_{p^n}^{-j}$$

が成り立つ. ここで ζ_{p^n} は任意の 1 の原始 p^n 乗根である.

Proof.

$$\begin{aligned}
\mu_\beta(G_n) &= \int_G 1_{G_n}(\sigma) d\mu_\beta(\sigma) \\
&= \int_{\mathbb{Z}_p} 1_{1+p^n\mathbb{Z}_p}(x) d\mu_\beta(x) \\
&= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \int_{\mathbb{Z}_p} \left(\zeta_{p^n}^j\right)^{x-1} d\mu_\beta(x) \\
&= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \left(\int_{\mathbb{Z}_p} (1 + (\zeta_{p^n}^j - 1))^x d\mu_\beta \right) \zeta_{p^n}^{-j} \\
&= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \widetilde{a_\beta}(\zeta_{p^n}^j - 1)\zeta_{p^n}^{-j}.
\end{aligned}$$

□

$F_f/\mathcal{O}_K$ の不変導分は $D = \frac{\Omega}{\lambda'(T)} \frac{d}{dT}$ と書ける. ただし $\lambda(T)$ は F_f の正規化形式対数である. このとき $T = \theta(S)$ と置換すると

$$D = \frac{\Omega}{\lambda'(\theta)} \frac{dS}{dT} \cdot \frac{d}{dS} = \frac{\Omega}{\lambda'(\theta)\theta'(S)} \frac{d}{dS}$$

と計算できる. ここで, $\lambda \circ \theta = \Omega \log(1 + S)$ より

θ は同型 $\hat{\mathbb{G}}_m \to F_f$ であって, $\log(1+S)$ は準同型 $\hat{\mathbb{G}}_m \to \hat{\mathbb{G}}_a$ であった. さらに Ω 倍準同型 $[\Omega] : \hat{\mathbb{G}}_a \to \hat{\mathbb{G}}_a$ も存在する. 従って準同型 $[\Omega] \circ \log(1+S) \circ \theta^{-1} : F_f \to \hat{\mathbb{G}}_a$ が得られるが, $[\Omega] \circ \log(1+S) \circ \theta^{-1}(T) = T + \dots$ という形をしていること, λ の一意性から $[\Omega] \circ \log(1+S) \circ \theta^{-1} = \lambda$, すなわち $\lambda \circ \theta = \Omega \log(1+S)$ が成り立たなければならない.

$\lambda'(\theta)\theta' = \frac{\Omega}{1+S}$ を得る. 従って $D = (1+S)\frac{d}{dS}$, すなわち $\hat{\mathbb{G}}_m$ の不変導分となる. このとき, 任意の $n \geq 0$ について

$$\int_G \kappa(\sigma)^n d\mu_\beta = D^n \left(\widetilde{\log g_\beta} \circ \theta \right)(0)$$

というモーメントと呼ばれる積分の計算が可能である.

$D^n(1+S)^{\kappa(\sigma)}|_{S=0} = \kappa(\sigma)^n$ であることが簡単に確かめられる. 従って

$$\begin{aligned} \int_G \kappa(\sigma)^n d\mu_\beta &= \int_G D^n (1+S)^{\kappa(\sigma)} d\mu_\beta \Big|_{S=0} \\ &\overset{(!)}{=} D^n \int_G (1+S)^{\kappa(\sigma)} d\mu_\beta \Big|_{S=0} \\ &= D^n \left(\widetilde{\log g_\beta} \circ \theta \right)(0) \end{aligned}$$

となり ok.

F_f が (absolute, すなわち $d=1$, すなわち $k' = k = \mathbb{Q}_p$) Lubin-Tate 形式群ならば Frobenius は g_β に自明に作用する. このとき以下が成り立つ.

$$\int_G \kappa(\sigma)^n d\mu_\beta = \left(1 - \frac{\pi^n}{p}\right) D^n \left(\log g_\beta \circ \theta\right)(0)$$

よく分からなかった.

Definition 3.21. 任意の $n \geq 0$ に対し, $\varphi_n : \mathscr{U} \to \mathcal{O}_K$ を

$$\varphi_n(\beta) := \int_G \kappa(\sigma)^n d\mu_\beta$$

と定義する. これを **n-th Coates-Wiles 準同型**という.

φ_n は $G = G(k_\xi/k')$ 上では μ_β のみで定まる. ただし $\mathcal{G} = G(k_\xi/k)$ 上で μ_β のみでは定まらない.

$\mu_\beta \in \Lambda(\mathcal{G}, \mathcal{O}_K)$ の定義より

$$\begin{aligned} \mu_\beta(\mathcal{G}) &= \sum_{i=0}^{d-1} \mu_\beta(\gamma^i G) \quad (G(k'/k) = \langle \gamma \rangle) \\ &= \sum_{i=0}^{d-1} \mu_{\gamma^{-i}(\beta)}(G) \quad (\because \mu_{\gamma(\beta)}(\gamma U) = \mu_\beta(U)) \end{aligned}$$

となって γ に依る.

Proposition 3.22.

- $\varphi_n(\beta\beta') = \varphi_n(\beta) + \varphi_n(\beta')$.
- $\varphi_n(\gamma(\beta)) = \kappa(\gamma)^n \varphi_n(\beta)$.

Proof. (1) $\mu_{\beta\beta'} = \mu_\beta + \mu_{\beta'}$ より明らか. (疲れた.)

(2) $\mu_{\gamma(\beta)}(\gamma G) = \mu_\beta(G)$ より

$$\begin{aligned}\varphi_n(\gamma(\beta)) &= \int_G \kappa(\sigma)^n d\mu_{\gamma(\beta)}(\sigma) \\ &= \int_G \kappa(\gamma\tau)^n d\mu_\beta(\tau) \quad (\sigma = \gamma\tau) \\ &= \kappa(\gamma)^n \int_G \kappa(\tau)^n d\mu_\beta(\tau) \\ &= \kappa(\gamma)^n \varphi_n(\beta)\end{aligned}$$

となって ok. □

$N \geq 0$ を, $\zeta_{p^N} \in k_\xi$ を満たす最大の整数とする. $d = [k' : \mathbb{Q}_p]$ のとき, 局所類体論からこの N は, $p^d \xi^{-1} \equiv 1 \bmod p^N$ を満たす最大の整数となるらしい. また, $N = \infty$ であることと, $F_f \simeq_{\mathcal{O}'} \hat{\mathbb{G}}_m$ となることが同値らしい. この N を F_f の (k' 上の)anomality index といい, $N > 0$ のとき F_f は anomalous という.

$\mathcal{G}$ は μ_{p^N} に作用するので

$$\mathcal{O}_K \otimes \mu_{p^N} =: (\mathcal{O}_K/p^N)(1) \text{ (Tate twist)}$$

は $\Lambda(\mathcal{G}, \mathcal{O}_K)$ 加群となる.

> $\Lambda(\mathcal{G}, \mathcal{O}_K) \simeq \mathcal{O}_K[[\mathcal{G}]]$ であったから, 準同型 $\mathcal{G} \times (\mathcal{O}_K \otimes \mu_{p^N}) \to \mathcal{O}_K \otimes \mu_{p^N}$ が存在すればよい. 今 $\mathcal{O}_K \otimes \mu_{p^N}$ の定義から, 双線形写像 $\mathcal{G} \times \mathcal{O}_K \times \mu_{p^N} \to \mathcal{G} \times (\mathcal{O}_K \otimes \mu_{p^N})$ がある. このとき
>
> $$\mathcal{G} \times \mathcal{O}_K \times \mu_{p^N} \to \mathcal{O}_K \otimes \mu_{p^N}; (\sigma, x, \zeta) \mapsto x^1 \otimes \sigma(\zeta)$$
>
> は双線形であるから, 普遍性より所望の準同型を得る.

$N : \mathcal{G} \to (\mathbb{Z}/p^N\mathbb{Z})^\times$ を, μ_{p^N} への作用を与える指標とする. このとき任意の $\gamma \in G$ に対して $N(\gamma) \equiv \kappa(\gamma) \bmod p^N$ が成り立つらしい. ここで

$$i : \Lambda(\mathcal{G}, \mathcal{O}_K) \to (\mathcal{O}_K/p^N)(1); \mu \mapsto \int_{\mathcal{G}} N(\sigma) d\mu(\sigma)$$

と定義する.

Theorem 3.23. 以下は完全列である.

$$0 \longrightarrow \mathscr{U} \hat{\otimes}_{\mathbb{Z}_p} \mathcal{O}_K \xrightarrow{i} \Lambda(\mathcal{G}, \mathcal{O}_K) \xrightarrow{j} (\mathcal{O}_K/p^N)(1) \longrightarrow 0$$

$N = \infty$ なら第四項は $\mathcal{O}_K(1)$ で, i は $\mathscr{U} \to \Lambda(\mathcal{G}, \mathcal{O}_K)$ を

$$\mathscr{U} \hat{\otimes}_{\mathbb{Z}_p} \mathcal{O}_K := \varprojlim_n \left(\mathscr{U}/U(k_\xi^n) \otimes \mathcal{O}^{ur}/(\mathfrak{p}^{ur})^n \right)$$

線形に拡張したものである.

残りはこの定理の証明を与えるためだけに費やされる. そろそろ疲れた.

4 THE EXPLICIT RECIPROCITY LAW

飛ばす.

第 II 部

p-ADIC L FUNTIONS

参考文献

[1] de Shalit, *Iwasawa theory of elliptic curves with complex multiplication. p-adic L functions.* Perspectives in Mathematics, 3. Academic Press, Inc., Boston, MA, 1987. x+154 pp. ISBN: 0-12-210255-X 11G05 (11G15 11G16 11R23 14K22)

[2] わしんとんえんぶんたい

[3] 西来寺文朗, 中央大学集中講義 形式群の本田理論