中央大学集中講義

形式群の本田理論

西来路文朗
広島国際大学工学部

まえがき

本稿は，2004 年 9 月 23 日から 10 月 1 日に中央大学で開講された集中講義「形式群の本田理論」の講義録です．本田平氏による形式群の分類理論 [10] は，$\mathfrak{p}$-進整数環や，代数体の整数環，有限体上定義された形式群をほぼ[1]完全に分類し，応用も多い理論ですが，本田氏の着想により証明は初等的な命題の積み重ねでなされています．そのため，講義では，各命題を自己完結的に証明することに力点をおき，p-進整数環上定義された 1 次元形式群を話題の中心としました．話題を制限したことが本田理論の理解の妨げにならないよう注意したつもりですが，いたらないところはお許しいただきたいと思います．本稿が，これから本田理論を勉強する方々の参考になれば幸いです．

当初予定になかったことなのですが，集中講義初日から話が盛り上がり，講義終了翌日，10 月 2 日に第 1 回春日形式群セミナー (講演者：谷戸光昭氏[2]，新妻康弘氏，原口幸氏，以上中央大，筆者，大西良博氏 (岩手大)，栗谷剛志氏 (都立大)) が開かれました．講義に出席して下さった皆様の熱気を伝えるひとつの話題として紹介したいと思います．毎日有益な議論をしていただいたことに，あらためて講義に出席して下さった方々に，感謝いたします．

講義録の第 1，2 章は，1996 年に行われた中島匠一先生の神戸大学理学部での集中講義のノートが元になっています．内容だけでなく，講義の進め方等も，今回参考にさせていただきました．丁寧でわかりやすい講義をしてくださったこと感謝いたします．

また，諏訪紀幸先生に，今回の講義の機会を与えてくださったこと，本稿をまとめるようすすめてくださり，出版にご尽力くださったこと，そして，いつも励まし続けてくださることに，感謝いたします．

最後になりましたが，筆者の指導教官，山本芳彦先生のお導きに感謝し，本稿を捧げたいと思います．

2007 年 12 月 17 日　西来路文朗

[1] $\mathfrak{p}$ が不分岐ならば完全

[2] 世話人

目 次

第1章　形式的べき級数環

この章では，本稿で用いる形式的べき級数の諸性質をまとめ，形式的べき級数の陰関数定理 (命題 1.5.1) を示します.

1.1　形式的べき級数

R を可換環とする．x を変数とし，R 係数の形式的べき級数

$$\sum_{n\geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots \quad (a_n \in R)$$

の全体を $R[[x]]$ とおく．2 つの形式的べき級数が等しいとは，x に関するすべての係数が一致することである.

例 1.1.1. $\mathbb{Q} \subset R$，α を R の元とする．形式的べき級数の例を挙げる.

$$\begin{aligned}
e^x &:= \sum_{n\geq 0} \frac{1}{n!} x^n = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \cdots, \\
\log(1+x) &:= \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} x^n = x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \cdots, \\
(1+x)^\alpha &:= \sum_{n\geq 0} \binom{\alpha}{n} x^n = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{6}x^3 + \cdots, \\
&\qquad \text{ただし，} \binom{\alpha}{n} := \prod_{i=0}^{n-1} \frac{\alpha - i}{n-i}, \quad \binom{\alpha}{n} := 1 \text{ と定める.}
\end{aligned}$$

右辺は，左辺の関数を原点のまわりで Taylor 展開して得られるべき級数を，収束を無視して形式的べき級数と考えたものである.

定義 1.1.2. $R[[x]]$ の 2 元 $\sum_{n\geq 0} a_n x^n$，$\sum_{n\geq 0} b_n x^n$ に対し，

$$\begin{aligned}
\sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n &:= \sum_{n\geq 0} (a_n + b_n) x^n, \\
\Big(\sum_{n\geq 0} a_n x^n\Big)\Big(\sum_{n\geq 0} b_n x^n\Big) &:= \sum_{n\geq 0} c_n x^n, \quad \text{ただし，} c_n := \sum_{k=0}^{n} a_k b_{n-k},
\end{aligned}$$

により加法，乗法を定義する．このとき，$R[[x]]$ は環になる．単位元は1，零元は0である．環 $R[[x]]$ を R 上1変数**形式的べき級数環**という．

命題 1.1.3. (i) $R[[x]]$ の単数群は，$R[[x]]^* = \{\varphi(x) \in R[[x]] \mid \varphi(0) \in R^*\}$ である．

(ii) R が整域ならば，$R[[x]]$ も整域である．

[**証明**] (i) $\sum_{n\geq 0} a_n x^n$ を $R[[x]]$ の元とする．$\sum_{n\geq 0} a_n x^n$ が単数であること，すなわち，

$$\Big(\sum_{n\geq 0} a_n x^n\Big)\Big(\sum_{n\geq 0} b_n x^n\Big) = 1$$

を満たす $R[[x]]$ の元 $\sum_{n\geq 0} b_n x^n$ が存在することは，

$$\begin{cases} a_0 b_0 = 1 \\ a_0 b_1 + a_1 b_0 = 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \\ \cdots \end{cases} \tag{1.1}$$

を満たす R の元 b_0,b_1,b_2,... が存在することと同値である．

$\sum_{n\geq 0} a_n x^n$ が単数ならば，(1.1) より $a_0 b_0 = 1$ を得るので，a_0 は R の単数である．

逆に，a_0 は R の単数であるとき，$b_0 = a_0^{-1}$, $b_n := -a_0^{-1} \sum_{k=1}^{n} a_k b_{n-k}$ $(n \geq 1)$ が (1.1) を満たす．

(ii) (i) と同様にして示せる． □

定義 1.1.4. $R[x]$ の2元 $\varphi(x)$, $\psi(x)$ が，

$$\varphi(x) \equiv \psi(x) \bmod \deg d$$

とは，$\varphi(x) - \psi(x)$ が $d-1$ 次[1]以下の項を含まないことをいう．I を R のイデアルとするとき，

$$\varphi(x) \equiv \psi(x) \bmod I$$

とは，$\varphi(x) - \psi(x)$ のすべての係数が I に属することをいう．さらに，

$$\varphi(x) \equiv \psi(x) \bmod \deg d,\ \bmod I$$

とは，$\varphi(x) - \psi(x)$ の $d-1$ 次以下の項の係数が I に属することをいう．

$\bmod \deg d$ や，$\bmod I$，そして，$\bmod \deg d$, $\bmod I$ は，$R[[x]]$ の同値関係となる．

[1] 多変数形式的べき級数環の場合は total degree について，$\bmod \deg d$ を定義する

$\varphi(x) = \sum_{n\geq 0} a_n x^n$ を $R[[x]]$ の元とし，α を R のべき零元とする．このとき，$\alpha^m = 0$ を満たす自然数 m が存在し，

$$\sum_{n\geq 0} a_n \alpha^n = \sum_{n=0}^{m-1} a_n \alpha^n \in R$$

が成り立つ．この値を $\varphi(\alpha)$ で表す.

$$R[[x]]_0 := \{\varphi(x) \in R[[x]] \mid \varphi(x) \equiv 0 \bmod \deg 1\}$$

とおく．$\varphi(x) \equiv 0 \bmod \deg 1$ は，$\varphi(0) = 0$ と同値である．

1.2 合成

定義 1.2.1. $\psi(x) = \sum_{n\geq 0} a_n x^n$ を $R[[x]]$ の元，$\varphi(x) = \sum_{n\geq 1} b_n x^n$ を $R[[x]]_0$ の元とする．**合成** $\psi(\varphi(x))$，または，$(\psi \circ \varphi)(x)$ を，

$$\begin{aligned} \psi(\varphi(x)) &:= \sum_{n\geq 0} a_n \{\varphi(x)\}^n \\ &= a_0 + a_1 b_1 x + (a_1 b_2 + a_2 b_1^2)x^2 + (a_1 b_3 + 2a_2 b_1 b_2 + a_3 b_1^3)x^3 + \cdots \end{aligned}$$

と定義する．$\varphi(x)$ の定数項は 0 だから，$\psi(\varphi(x))$ は well-defined である．

定義 1.2.2. $\varphi(x)$ を $R[[x]]_0$ の元とする．

$$\varphi(\psi(x)) = \psi(\varphi(x)) = x$$

を満たす $R[[x]]_0$ の元 $\psi(x)$ が存在するとき，$\varphi(x)$ は**可逆である**という．この $\psi(x)$ を $\varphi^{-1}(x)$ と書く．

問題 1.2.3. 以下を示せ.

(i) $R[[x]]$ の任意の元 $f(x)$，$R[[x]]_0$ の任意の元 $\varphi(x)$, $\psi(x)$ に対し，$((f \circ \varphi) \circ \psi)(x) = (f \circ (\varphi \circ \psi))(x)$ が成り立つ.

(ii) $(\varphi \circ \psi)(x) = x$ を満たす $R[[x]]_0$ の元 $\psi(x)$ が存在することと，$(\psi \circ \varphi)(x) = x$ を満たす $R[[x]]_0$ の元 $\psi(x)$ が存在することは同値である.

(iii) $\varphi^{-1}(x)$ は存在すれば一意的である.

1.3 (項別) 微分・(項別) 積分

定義 1.3.1. $f(x)=\sum_{n\geq 0}a_nx^n$ を $R[[x]]$ の元とする．$f(x)$ の x に関する (項別) **微分**を

$$f'(x):=\sum_{n\geq 1}na_nx^{n-1}$$

により定義する．x を明記する必要があるときには，$f'(x)$ を df/dx や，$f_x(x)$ 等の記号で表すことにする．また，$\mathbb{Q}\subset R$ のときには，$f(x)$ の x に関する (項別) **積分**を

$$\int f(x)dx:=\sum_{n\geq 0}\frac{a_n}{n+1}x^{n+1}$$

により定義する．

命題 1.3.2. $f(x)$，$g(x)$ を $R[[x]]$ の元とする．$\varphi(x)$ を $R[[x]]_0$ の元とする．このとき，次が成立する．

(i) $(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$.

(ii) $(f\circ\varphi)'(x)=(f'\circ\varphi)(x)\varphi'(x)$.

[**証明**] (i) $f(x)=\sum_{n\geq 0}a_nx^n$，$g(x)=\sum_{n\geq 0}b_nx^n$ とおく．

$$\begin{aligned}\big(f(x)g(x)\big)' &= \Big(\sum_{n\geq 0}\big(\sum_{k=0}^{n}a_kb_{n-k}\big)x^n\Big)'=\sum_{n\geq 1}\big(\sum_{k=0}^{n}na_kb_{n-k}\big)x^{n-1}\\ &= \sum_{n\geq 1}\big(\sum_{k=0}^{n}ka_kb_{n-k}+(n-k)a_kb_{n-k}\big)x^{n-1}\\ &= f'(x)g(x)+f(x)g'(x).\end{aligned}$$

(ii) (i) より

$$\big(\varphi(x)^n\big)'=(n-1)\varphi(x)^{n-1}\varphi'(x)$$

が成り立つ．$f_n(x)$ で $f(x)$ の n 次以下の項のなす多項式を表す．このとき，任意の n に対し，次式が成り立つ．

$$\begin{aligned}(f\circ\varphi)'(x) &\equiv (f_n(x)\circ\varphi(x))'\\ &\equiv (f_n'\circ\varphi)(x)\varphi'(x)\quad(\because\ f_n(x)\text{ は多項式})\\ &\equiv (f'\circ\varphi)(x)\varphi'(x)\ \bmod \deg n.\end{aligned}$$

よって，(ii) が従う． □

命題 1.3.3. $\mathbb{Q} \subset R$ とする．このとき，$e^{x+y} = e^x e^y$ が成立する．

[**証明**] 形式的べき級数 ce^x は，

$$f'(x) = f(x), \quad f(0) = c \tag{1.2}$$

を満たすただひとつの形式的べき級数である．$\varphi(x) := e^{x+y} \in (R[[y]])[[x]]$ とおくとき，命題 1.3.2 より，x についての項別微分は

$$\varphi'(x) = e^{x+y}(x+y)' = e^{x+y} = \varphi(x)$$

となる．よって，$\varphi(x)$ は，$c = \varphi(0) = e^y$ に対し，微分方程式 (1.2) を満たすので，

$$e^{x+y} = e^x e^y$$

が成立する． □

問題 1.3.4. (i) $e^{\alpha \log(1+x)} = (1+x)^\alpha$ を示せ．
(ii) $\log(1+x)(1+y) = \log(1+x) + \log(1+y)$ を示せ．

1.4 R-導分・微分形式

$A := R[[x]]$ とおく．

定義 1.4.1. A 上の R-線型写像 D が

$$D(fg) = D(f)g + fD(g) \quad ({}^\forall f,\ g \in A)$$

を満たすとき，A の **R-導分**という．A の R-導分全体 $\mathrm{Der}(A : R)$ は，d/dx で生成される A-自由加群になる．

$\mathrm{Der}(A : R)$ の A-双対加群を $\Omega^1(A : R)$ と表し，その元を**微分形式**と呼ぶ．A の元 f に対し，微分形式 df を

$$df :\ \mathrm{Der}(A : R) \to A :\ D \mapsto D(f)$$

と定義する．このとき，dx は d/dx の双対基底であり，$df = f'(x)dx$ が成り立つ．

注意 1.4.2. t を x と独立な変数とするとき，$R[[x]]$ から $(R[[t]])[[x]]$ への自然な埋め込みは，埋め込み

$$\Omega^1(A : R) \to \Omega^1(A[[t]] : R[[t]])$$

を引き起こす．

定義 1.4.3. $\varphi(x)$ を $R[[x]]_0$ の元，$\omega = f(x)dx$ を $\Omega^1(A, R)$ の元とする．ω の $\varphi(x)$ による引き戻しを

$$\varphi^*\omega = f(\varphi(x))d\varphi(x)$$

で定義する．

1.5 陰関数定理

R を可換整域，$R[[x,y]]$ を 2 変数形式的べき級数環とする．$R[[x,y]]$ の元 $F(x,y)$ に対し，$F_x(x,y)$, $F_y(x,y)$ で x, y に関する偏微分 (項別微分) を表す.

命題 1.5.1 (形式的陰関数定理). $F(x,y)$ を $R[[x,y]]$ の元とする．このとき，

$$F(0,0)=0,\ \text{かつ}\ F_y(0,0)\in R^*$$

が成り立つならば,

$$F(x,\varphi(x))=0$$

を満たす $R[[x]]_0$ の元 $\varphi(x)$ がただひとつ存在する.

[**証明**] $n=0,1,2,\dots$ に対し，$R[[x]]$ の元 $f_n(x)$ を

$$F(x,y)=\sum_{n\geq 0} f_n(x)y^n = f_0(x)+f_1(x)y+f_2(x)y^2+\cdots \tag{1.3}$$

により定める．仮定より,

$$f_0(0)=0,\ \text{かつ}\ f_1(0)\in R^*$$

である．$n=0,1,2,\dots$ に対し,

$$g_n(x):=-f_n(x)/f_1(x)$$

とおく．$f_1(x)\in R[[x]]^*$ より，$g_n(x)\in R[[x]]$ である.
$F(x,y)=0$ の両辺を (1.3) に注意して $f_1(x)$ で割ることにより,

$$y=g_0(x)+g_2(x)y^2+g_3(x)y^3+\cdots \tag{1.4}$$

を得る．$y=\varphi(x)=\sum_{n\geq 1}c_nx^n$ とおいて (1.4) に代入すると,

$$\sum_{n\geq 1}c_nx^n = g_0(x)+g_2(x)(c_1^2x^2+2c_1c_2x^3+\cdots)+\cdots \tag{1.5}$$

が成り立つ．(1.5) の両辺を係数比較して,

$$\begin{aligned}
c_1 &= g_0(x)\ \text{の}\ 1\ \text{次の係数}\\
c_2 &= (g_0(x)\ \text{の}\ 2\ \text{次の係数})+c_1^2(g_1(x)\ \text{の}\ 1\ \text{次の係数})\\
&\cdots\\
c_n &= g_0(x),\dots,g_{n-1}(x)\ \text{の係数と}\ c_1,\dots,c_{n-1}\ \text{の式}
\end{aligned}$$

が成り立つ．よって，帰納的に $\varphi(x)$ がただひとつ定まる． □

命題 1.5.2 (形式的逆関数定理). $\varphi(x)$ を $R[[x]]_0$ の元とするとき，以下の 2 条件は同値である．

(i) $\varphi(x)$ は可逆である．

(ii) $\varphi'(0)$ は R の単数である．

[**証明**] (i)⇒(ii) $\varphi(\psi(x)) = x$ の両辺を x で微分すると，

$$\varphi'(\psi(x))\psi'(x) = 1$$

を得る．両辺に $x = 0$ を代入すると，

$$1 = \varphi'(\psi(0))\psi'(0) = \varphi'(0)\psi'(0)$$

が成り立つ．よって，(ii) が成立する．

(ii)⇒(i) $F(x, y) := x - \varphi(y)$ とおく．$\varphi(0) = 0$，$\varphi'(0) \in R^*$ より，

$$F(0, 0) = 0, \text{ かつ } F_y(0, 0) \in R^*$$

が成立する．よって，命題 1.5.1 より，

$$F(x, \psi(x)) = x - \varphi(\psi(x)) = 0$$

を満たす $R[[x]]_0$ の元 $\psi(x)$ がただひとつ存在する．したがって，(i) が成り立つ． □

第2章　形式群

この章では，形式群や形式群の準同型の定義，諸性質をまとめ，標数 0 の体上の形式群が本質的にひとつであることを示します (定理 2.4.1)．1 次元可換形式群を話題の中心とし，高次元形式群については，2.5 節に結果のみをまとめます.

2.1　形式群

定義 2.1.1. $R[[x,y]]$ の元 $F(x,y)$ が以下の 3 条件を満たすとき，$F(x,y)$ は R 上 (1 次元可換) **形式群**であるという.

$$\begin{aligned} &\text{(i)} && F(x,y) \equiv x+y \bmod \deg 2. \\ &\text{(ii)} && F(F(x,y),z) = F(x,F(y,z)). \\ &\text{(iii)} && F(x,y) = F(y,x). \end{aligned}$$

命題 2.1.2. R を整域とする．定義 2.1.1 において，(ii)，(iii) の仮定の下，(i) は次の条件 (i)$'$ と同値である.

$$\text{(i)}' \quad F(x,0) = x, \qquad F(0,y) = y.$$

[**証明**] (i)⇒(i)$'$ $\varphi(x) := F(x,0)$ とおく.

$$\varphi(0) = F(0,0) = 0, \qquad \varphi'(0) = F_x(0,0) = 1$$

である．よって，命題 1.5.2 により，$\varphi(x)$ は可逆である．(ii) の両辺に $y = z = 0$ を代入すると，

$$\varphi(\varphi(x)) = F(F(x,0),0) = F(x,0) = \varphi(x)$$

が成り立つ．よって，$\varphi(x) = x$，すなわち，(i)$'$ が成立する.

(i)$'$ ⇒(i) 明らか. □

命題 2.1.3. $F(x,y)$ を R 上の形式群とする．$F(\mathrm{inv}_F(x),x) = F(x,\mathrm{inv}_F(x)) = 0$ を満たす $R[[x]]_0$ の元 $\mathrm{inv}_F(x)$ がただひとつ存在する.

問題 2.1.4. 命題 1.5.1 を用いて，命題 2.1.3 を証明せよ.

定義 2.1.1 において，(i) は群の公理における単位元の存在に，(ii) は結合則に，(iii) は可換則に対応する．また，命題 2.1.3 が逆元の存在に対応する．

例 2.1.5. (i) $\hat{\mathbb{G}}_a(x,y) := x+y$ は $\mathbb{Z}$ 上の形式群である．$\hat{\mathbb{G}}_a(x,y)$ は**加法群**と呼ばれる．

(ii) $\hat{\mathbb{G}}_m(x,y) := x+y-xy$ は $\mathbb{Z}$ 上の形式群である．$\hat{\mathbb{G}}_m(x,y)$ は**乗法群**と呼ばれ，

$$(1-x)(1-y) = 1-\hat{\mathbb{G}}_m(x,y)$$

を満たす．

(iii) $F_t(x,y) := (x+y)/(1-xy) = (x+y)(1+xy+x^2y^2+\cdots)$ は $\mathbb{Z}$ 上の形式群である．$F_t(x,y)$ は

$$\tan(x+y) = F_t(\tan x, \tan y) \tag{2.1}$$

を満たす．

(iv) $F_s(x,y) := x\sqrt{1-y^2}+y\sqrt{1-x^2}$ は $\mathbb{Z}[2^{-1}]$ 上の形式群である．$F_s(x,y)$ は

$$\sin(x+y) = F_s(\sin x, \sin y) \tag{2.2}$$

を満たす．さらに，$F_s^*(x,y) := F(2x,2y)/2$ とおくとき，$F_s^*(x,y)$ は $\mathbb{Z}$ 上の形式群になる[1]．

注意 2.1.6. φ を R から R' への環準同型，$F(x,y) = \sum a_{ij}x^iy^j$ を R 上定義された形式群とする．このとき，${}^{\varphi}F(x,y) := \sum \varphi(a_{ij})x^iy^j$ は R' 上定義された形式群となる．

命題 2.1.7. R を整域とする．$R[x,y]$ の多項式 $F(x,y)$ が形式群ならば，R の元 c が存在して，

$$F(x,y) = x+y+cxy$$

と書かれる．

[**証明**] $F(x,y)$ の x についての次数を d とおく．R が整域だから，$F(F(x,y),z) = F(x,F(y,z))$ の両辺の x についての次数を比較することにより，

$$d^2 = d.$$

よって，$d=1$ である．同様に y についても 1 次式となる．定義 2.1.1(i) に注意して，$F(x,y)$ は命題の形になる． □

[1] 諏訪紀幸氏の指摘による

注意 2.1.8. $\overline{\mathbb{Q}}(x,y)$ の有理式 $F(x,y)$ が $\overline{\mathbb{Q}}$ 上の形式群ならば，$\overline{\mathbb{Q}}$ の元 c, m が存在して，

$$F(x,y) = \frac{x+y+cxy}{1+mxy}$$

と書かれる (cf. e.g. [4]).

2.2 準同型

$F(x,y)$，$G(x,y)$ を R 上の形式群とする．

定義 2.2.1. $R[[x]]_0$ の元 $\varphi(x)$ が

$$\varphi(F(x,y)) = G(\varphi(x),\varphi(y))$$

を満たすとき，$\varphi(x)$ を $F(x,y)$ から $G(x,y)$ への R 上の**準同型**という．さらに，$\varphi(x)$ が可逆のとき，$\varphi(x)$ を**弱同型**，$\varphi(x) \equiv x \bmod \deg 2$ のとき，$\varphi(x)$ を**強同型**という．

$F(x,y)$ から $G(x,y)$ への R 上の強同型 (resp. 弱同型) が存在することを，

$$F \approx_R G \qquad (\text{resp. } F \sim_R G)$$

と書く．

問題 2.2.2. 関係 $\approx_R$, $\sim_R$ は，R 上の形式群の同値関係になる．このことを示せ．

例 2.2.3. $\mathbb{Q} \subset R$ とする．

(i) $$f(x) := -\log(1-x) = \sum_{n\geq 1} \frac{1}{n} x^n$$

は $\hat{\mathbb{G}}_m(x,y)$ から $\hat{\mathbb{G}}_a(x,y)$ への強同型である．実際，

$$\begin{aligned} f(\hat{\mathbb{G}}_m(x,y)) &= -\log(1-\hat{\mathbb{G}}_m(x,y)) = -\log(1-x)(1-y) \\ &= -\log(1-x) - \log(1-y) = f(x)+f(y) \\ &= \hat{\mathbb{G}}_a(f(x),f(y)) \end{aligned}$$

が成り立つ．また，

$$f^{-1}(x) = 1 - e^{-x} = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n!} x^n$$

が，$\hat{\mathbb{G}}_a(x,y)$ から $\hat{\mathbb{G}}_m(x,y)$ への強同型である．

(ii) $F_t(x,y) := (x+y)/(1-xy)$ とする．(2.1) により，$\tan x$ は $\hat{\mathbb{G}}_a(x,y)$ から $F_t(x,y)$ への強同型だから，

$$\arctan x = \sum_{n\geq 0} \frac{(-1)^n}{2n+1} x^{2n+1}$$

は $F_t(x,y)$ から $\hat{\mathbb{G}}_a(x,y)$ への強同型である．

(iii) $F_s(x,y) := x\sqrt{1-y^2} + y\sqrt{1-x^2}$ とする．(2.2) により，$\sin x$ は $\hat{\mathbb{G}}_a(x,y)$ から $F_s(x,y)$ への強同型だから，

$$\arcsin x = \sum_{n\geq 0} \binom{-\frac{1}{2}}{n} \frac{(-1)^n}{2n+1} x^{2n+1}$$

は，$F_s(x,y)$ から $\hat{\mathbb{G}}_a(x,y)$ への強同型である．また，

$$f(x) := \tan(\arcsin x) = \frac{x}{\sqrt{1-x^2}} = \sum_{n\geq 0} \binom{-\frac{1}{2}}{n} (-1)^n x^{2n+1}$$

は，$F_s(x,y)$ から $F_t(x,y)$ への強同型である．$\binom{-\frac{1}{2}}{n} \in \mathbb{Z}[2^{-1}]$ より，$f(x)$ は $\mathbb{Z}[2^{-1}]$ 上定義される．

$F(x,y)$ から $G(x,y)$ への R 上の準同型全体を $\mathrm{Hom}_R(F,G)$ とおく．$\mathrm{Hom}_R(F,G)$ は

$$(\varphi+\psi)(x) := G(\varphi(x), \psi(x))$$

を加法とする加群になる．零元は 0 である．$\mathrm{End}_R(F) := \mathrm{Hom}_R(F,F)$ とおく．加群 $\mathrm{End}_R(F)$ は

$$(\varphi\circ\psi)(x) := \varphi(\psi(x))$$

を乗法とする環になる．単位元は x である．

問題 2.2.4. $\mathrm{Hom}_R(F,G)$ が加群であること，$\mathrm{End}_R(F)$ が環であること，を示せ．

$F(x,y)$ を R 上の形式群とする．環準同型

$$\mathbb{Z} \to \mathrm{End}_R(F)$$

による整数 n の像を $[n]_F(x)$ と書く．

$$[-1]_F(x) = \mathrm{inv}_F(x)$$

が成り立つ．

例 2.2.5. $[n]_{\hat{\mathbb{G}}_a}(x) = nx$, $[n]_{\hat{\mathbb{G}}_m}(x) = 1-(1-x)^n$ である.

命題 2.2.6. R が標数 0 の体のとき,

$$\mathrm{End}_R(\hat{\mathbb{G}}_a) = \{ax \mid a \in R\} \tag{2.3}$$

である.

[**証明**] R の任意の元 a に対し, $f(x) = ax$ が $\hat{\mathbb{G}}_a(x,y)$ の自己準同型となることは, 定義より明らかである. 逆に, $f(x)$ が $\hat{\mathbb{G}}_a(x,y)$ の自己準同型ならば,

$$f(x+y) = f(x) + f(y)$$

が満たされる. この両辺を y で偏微分し,

$$f'(x+y) = f'(y)$$

を得る. $y = 0$ を代入すると,

$$f'(x) = f'(0) \in R$$

を得る. R の標数は 0 だから, $f(x) = ax$ と書ける. よって, (2.3) が示された. □

定義 2.2.7. $F(x,y)$ を有限体 $\mathbb{F}_p$ 上の形式群とし,

$$f(x) := x^p$$

とおく. このとき, $f(x)$ は $F(x,y)$ の自己準同型である. Frobenius p **乗自己準同型**と呼ばれる.

問題 2.2.8. 以下を示せ.
(i) r が素数 p のべきでなければ, $(x+y)^r - x^r - y^r$ は原始多項式である. また, r が素数 p のべきならば, $\{(x+y)^r - x^r - y^r\}/p$ は原始多項式である.
(ii) R を標数 $p > 0$ の整域とする.

$$\mathrm{End}_R(\hat{\mathbb{G}}_a) = \{ \sum_{n \geq 0} a_n x^{p^n} \mid a_n \in R\}$$

を示せ.

命題 2.2.9. R の標数 $p > 0$ の整域とする. $\varphi(x)$ を $F(x,y)$ から $G(x,y)$ への R 上の準同型とする. このとき, $\varphi(x) \neq 0$ ならば, 自然数 h と R の元 $a \neq 0$ が存在して,

$$\varphi(x) \equiv ax^{p^h} \bmod \deg\, p^h + 1$$

が成り立つ.

[**証明**] $\varphi(x) \neq 0$ より，自然数 n，R の元 $a \neq 0$ が存在して，

$$\varphi(x) \equiv ax^n \bmod \deg\, n+1$$

が成り立つ．$\varphi(F(x,y)) = G(\varphi(x), \varphi(y))$ より，

$$a(x+y)^n \equiv ax^n + ay^n \bmod \deg\, n+1$$

を得る．R は整域だから，

$$(x+y)^n = x^n + y^n$$

が成立する．問題 2.2.8(i) より，n は p のべきである． □

定義 2.2.10. 命題 2.2.9 の h を準同型 $\varphi(x)$ の**高さ** (height) という．$\varphi(x) = 0$ のときは，$\varphi(x)$ の高さを ∞ と定義する．また，形式群 $F(x,y)$ の p 倍写像 $[p]_F(x)$ の高さを，$F(x,y)$ の高さという．

例 2.2.11. 例 2.2.5 より，$[p]_{\hat{\mathbb{G}}_a}(x) = px \equiv 0 \bmod p$，$[p]_{\hat{\mathbb{G}}_m}(x) = x^p \equiv 0 \bmod p$ が従う．よって，$\hat{\mathbb{G}}_a(x,y)$，$\hat{\mathbb{G}}_m(x,y)$ の高さは，それぞれ，∞，1 である．

2.3 不変微分

定義 2.3.1. $F(x,y)$ を R 上の形式群，t を x，y と独立な変数とし，$\varphi_t(x) := F(x,t) \in (R[[t]])[[x]]$ とおく．$\Omega^1(R[[x]], R)$ の元 ω が，$\Omega^1(R[[x,t]], R[[t]])$ において

$$\varphi_t^* \omega = \omega$$

を満たすとき，ω を $F(x,y)$ **の不変微分**という．

$F(x,y)$ を R 上の形式群とする．$\psi(y) := F_x(0,y)^{-1}$ とおく．$F_x(0,0) = 1$ により，$\psi(y) \in R[[y]]^*$ である．

命題 2.3.2. ω を $\Omega^1(R[[x]], R)$ の元とする．このとき，以下は同値である．
(i) ω は $F(x,y)$ の不変微分である．
(ii) R のある元 c に対し，$\omega = c\psi(x)dx$ と書ける．

[**証明**] (i)⇒(ii) $\omega = f(x)dx$ とおく．ω が $F(x,y)$ の不変微分となるための必要十分条件は，

$$\begin{aligned} f(F(x,t))dF(x,t) &= f(x)dx, \\ f(F(x,t))F_x(x,t)dx &= f(x)dx, \\ f(F(x,t))F_x(x,t) &= f(x) \end{aligned} \tag{2.4}$$

である．両辺に，$x=0$ を代入して，

$$f(t)F_x(0,t)=f(0)$$

を得る．よって，

$$f(t)=f(0)F_x(0,t)^{-1}$$

が成立する．

(ii)⇒(i) $F(x,y)$ は形式群だから，

$$F(F(x,y),z)=F(x,F(y,z))$$

が成り立つ．両辺を x で偏微分すると，

$$F_x(F(x,y),z)F_x(x,y)=F_x(x,F(y,z))$$

を得る．$x=0$ を代入すると，

$$\begin{aligned} F_x(y,z)F_x(0,y) &= F_x(0,F(y,z)),\\ F_x(y,z)F_x(0,F(y,z))^{-1} &= F_x(0,y)^{-1},\\ \psi(F(y,z))F_x(y,z) &= \psi(y) \end{aligned}$$

を得る．(2.4) 式により，(i) が従う． □

2.4 標数 0 の体上の形式群

定理 2.4.1. R を標数 0 の体，$F(x,y)$ を R 上の形式群とする．このとき，$F(x,y)$ から $\hat{\mathbb{G}}_a(x,y)$ への強同型がただひとつ存在する．

[**証明**] $\psi(x)dx$ を $F(x,y)$ の不変微分とする．

$$f(x):=\int \psi(x)dx$$

とおく．$\psi(x)dx=f'(x)dx$ は $F(x,y)$ の不変微分だから，

$$f'(F(x,t))F_x(x,t)dx=f'(x)dx$$

が成立する．両辺を x について積分して，

$$f(F(x,t))=f(x)+g(t),\quad \text{ただし，}g(t)\text{ は積分定数,}$$

を得る．$x=0$ を代入すると，

$$f(t)=g(t)$$

を得る．よって，

$$f(F(x,t))=f(x)+f(t)=\hat{\mathbb{G}}_a(f(x),f(t))$$

が成立する． □

定義 2.4.2. 定理 2.4.1 の $f(x)$ を形式群 $F(x,y)$ の**変換子**という．

$$F(x,y) = f^{-1}(f(x)+f(y))$$

が成立する．

例 2.4.3. $R=\mathbb{Q}$ とする．例 2.2.3 より，$\hat{\mathbb{G}}_a(x,y)$，$\hat{\mathbb{G}}_m(x,y)$ の変換子は，それぞれ，x，$-\log(1-x)$ である．

命題 2.4.4. R を標数 0 の体，$F(x,y)$，$G(x,y)$ を R 上の形式群，$f(x)$，$g(x)$ をそれぞれの変換子とする．このとき，次は同値である．
(i) $\varphi(x)$ は $F(x,y)$ から $G(x,y)$ への準同型である．
(ii) R の元 c が存在し，$\varphi(x) = g^{-1}(cf(x))$ と表される．
(iii) R の元 c が存在し，$\varphi^*(dg) = c\,df$ と表される．

[**証明**] (i) $\Longleftrightarrow$ (ii) $\varphi(x)$ を $F(x,y)$ から $G(x,y)$ への準同型とすると，$(g\circ\varphi\circ f^{-1})(x)$ は $\hat{\mathbb{G}}_a(x,y)$ の自己準同型である．命題 2.2.6 により，R のある元 c があって，

$$(g\circ\varphi\circ f^{-1})(x) = cx$$

が成り立つ．よって，$\varphi(x) = g^{-1}(cf(x))$ が成り立つ．逆に，$g^{-1}(cf(x))$ は $F(x,y)$ から $G(x,y)$ への準同型である．
(ii) $\Longleftrightarrow$ (iii) $\varphi(x) := g^{-1}(cf(x))$ とおく．

$$(g\circ\varphi)(x) = cf(x)$$

が成り立つ．両辺を x で微分することにより，

$$\varphi^*(dg) = g'(\varphi(x))\varphi'(x)dx = cf'(x)dx = df$$

を得る．逆に，$\varphi^*(dg) = c\,df$ のとき，両辺を積分して，$(g\circ\varphi)(x) = cf(x)$ を得る．よって，$\varphi(x) = g^{-1}(cf(x))$ が成り立つ． □

$F(x,y)=G(x,y)$ のとき，命題 2.4.4(ii) の自己準同型 $\varphi(x)$ を $[c]_F(x)$ で表す．R が標数 0 の体のとき，環準同型

$$R \to \mathrm{End}_R(F):\ c \mapsto [c]_F(x)$$

は単射になる．

2.5　付記　高次元形式群

この節では，$\boldsymbol{x}$ を列ベクトル ${}^t(x_1,\dots,x_n)$ とし，$R[[\boldsymbol{x}]] := R[[x_1,\dots,x_n]]$ とおく．

定義 2.5.1. $R[[\boldsymbol{x}]]^n$ の元 $F(\boldsymbol{x},\boldsymbol{y}) = {}^t(F_1(\boldsymbol{x},\boldsymbol{y}),\dots,F_n(\boldsymbol{x},\boldsymbol{y}))$ が n 次元形式群であるとは，以下をみたすことをいう．

$$\begin{aligned} &\text{(i)} && F(\boldsymbol{x},\boldsymbol{y}) \equiv \boldsymbol{x}+\boldsymbol{y} \bmod \deg 2.\\ &\text{(ii)} && F(F(\boldsymbol{x},\boldsymbol{y}),\boldsymbol{z}) = F(\boldsymbol{x},F(\boldsymbol{y},\boldsymbol{z})).\\ &\text{(iii)} && F(\boldsymbol{x},\boldsymbol{y}) = F(\boldsymbol{y},\boldsymbol{x}). \end{aligned}$$

定義 2.5.2. $F(\boldsymbol{x},\boldsymbol{y})$ を n 次元形式群，$G(\boldsymbol{x},\boldsymbol{y})$ を m 次元形式群とする．$R[[\boldsymbol{x}]]_0^m$ の元 $\varphi(\boldsymbol{x}) = {}^t(\varphi_1(\boldsymbol{x}),\dots,\varphi_m(\boldsymbol{x}))$ が $F(\boldsymbol{x},\boldsymbol{y})$ から $G(\boldsymbol{x},\boldsymbol{y})$ への R 上の準同型であるとは，

$$\varphi(F(\boldsymbol{x},\boldsymbol{y})) = G(\varphi(\boldsymbol{x}),\varphi(\boldsymbol{y}))$$

をみたすことをいう．また，$n=m$ とし，準同型 $\varphi(\boldsymbol{x})$ が可逆[2]のとき**弱同型**，

$$\varphi(\boldsymbol{x}) \equiv I_n\boldsymbol{x} \bmod \deg 2 \quad \text{ただし，} I_n \text{は単位行列}$$

をみたすとき**強同型**という．

命題 2.5.3.

$$\big(\psi_{ij}(\boldsymbol{z})\big) := \big(\frac{\partial}{\partial x_j}F_i(0,\boldsymbol{z})\big)^{-1}$$

とおくとき，

$$\omega_i := \sum_{j=1}^{n}\psi_{ij}(\boldsymbol{x})dx_j \quad (i=1,\dots,n)$$

が F の不変微分の基底となる．

命題 2.5.4. R を標数 0 の体とする．$F(\boldsymbol{x},\boldsymbol{y})$ を R 上の形式群とするとき，$F(\boldsymbol{x},\boldsymbol{y})$ から加法群 $\boldsymbol{x}+\boldsymbol{y}$ への強同型 $f(\boldsymbol{x})$ がただひとつ存在する．

注意 2.5.5. 命題 2.5.4 の強同型 $f(\boldsymbol{x})$ を $F(\boldsymbol{x},\boldsymbol{y})$ の変換子という．$f(\boldsymbol{x})$ は，

$$df(\boldsymbol{x}) = \big(df_i(\boldsymbol{x})\big) = \big(\sum_{j=1}^{n}\psi_{ij}(\boldsymbol{x})dx_j\big)$$

を満たす．

[2] $\varphi(\boldsymbol{x}) \equiv P\boldsymbol{x} \bmod \deg 2$ を満たす $\mathrm{GL}_n(R)$ の元 P が存在することと同値である．

第3章　形式群の本田理論(紹介)

標語的に言うと，$\mathfrak{p}$-進整数環上の形式群は，変換子を消す特殊元で決まる，というのが本田理論です．この事実と Hasse の原理により，代数体の整数環上定義された形式群が，ほぼ完全に分類できます．

3 章では，形式群の本田理論を概観し，特殊元についての計算例を与えます．その後に，4 章で証明について述べたいと思います．なお，簡単の為，説明の中心は $\mathbb{Z}_p$ 上 1 次元形式群の本田理論とし，$\mathfrak{p}$-進整数環上の高次元形式群については，結果のみを，4.5 節でまとめます．

3.1　p-進整数環上の形式群

p を素数とする．T を変数とする．$\mathbb{Q}_p[[T]]$ の元 $u=\sum_{\nu\geq 0} c_\nu T^\nu$，$\mathbb{Q}_p[[x_1,\dots,x_n]]_0$ の元 $f(x_1,\dots,x_n)$ に対し，

$$(u*f)(x_1,\dots,x_n) := \sum_{\nu\geq 0} c_\nu f(x_1^{p^\nu},\dots,x_n^{p^\nu})$$

と定義する．

$u=\sum_{\nu\geq 0} c_\nu T^\nu$，$v=\sum_{\mu\geq 0} d_\mu T^\mu$ のとき，

$$\begin{aligned}(u*(v*f))(x) &= u*\Big(\sum_{\mu\geq 0} d_\mu f(x_1^{p^\mu},\dots,x_n^{p^\mu})\Big)\\ &= \sum_{\nu,\mu\geq 0} c_\nu d_\mu f((x_1^{p^\nu})^{p^\mu},\dots,(x_n^{p^\nu})^{p^\mu}) = ((uv)*f)(x)\end{aligned}$$

であるから，$*$ により $\mathbb{Z}_p[[T]]$ が $\mathbb{Z}_p[[x]]$ に左から作用する．

定義 3.1.1. $\mathbb{Z}_p[[T]]$ の元 u が**特殊元**であるとは，

$$u = p + \sum_{\nu\geq 1} c_\nu T^\nu$$

と書けることをいう．

定義 3.1.2. u を特殊元，$f(x)$ を $\mathbb{Q}_p[[x]]_0$ の元とする．$f(x)$ が**特殊元 u に属する** (type u) とは，

$$\text{(i) } f(x) \equiv x \bmod \deg 2, \qquad \text{(ii) } u * f \equiv 0 \bmod p$$

を満たすことをいう．

本稿においては，$\mathbb{Q}_p$ 上定義された形式群 $F(x,y)$ の変換子 $f(x)$ が特殊元 u に属することを，単に，$F(x,y)$ は u に属するという．

例 3.1.3. (i) $\hat{\mathbb{G}}_a(x,y)$ は特殊元 p に属する．実際，$\hat{\mathbb{G}}_a(x,y)$ の変換子は x であり，

$$p * x = px \equiv 0 \bmod p$$

が成立する．

(ii) $\hat{\mathbb{G}}_m(x,y)$ は特殊元 $p-T$ に属する．実際，$\hat{\mathbb{G}}_m(x,y)$ の変換子は $-\log(1-x) = \sum_{n\geq 1} x^n/n$ であり，

$$\begin{aligned}(p-T) * \sum_{n\geq 1} \frac{1}{n}x^n &= p\sum_{n\geq 1}\frac{1}{n}x^n - \sum_{n\geq 1}\frac{1}{n}x^{np} \\ &= p\Big(\sum_{\substack{n\geq 1\\(n,p)=1}}\frac{1}{n}x^n + \sum_{n\geq 1}\frac{1}{np}x^{np}\Big) - \sum_{n\geq 1}\frac{1}{n}x^{np} \\ &= p\sum_{\substack{n\geq 1\\(n,p)=1}}\frac{1}{n}x^n \equiv 0 \bmod p\end{aligned}$$

が成立する．

問題 3.1.4. 形式群 $F_t(x,y) = (x+y)/(1-xy)$ が特殊元 $p - (\frac{-4}{p})T$ に属することを示せ．ただし，$(\frac{-4}{p})$ は Kronecker symbol とする．

定理 3.1.5. $F(x,y)$ を $\mathbb{Q}_p$ 上の形式群とする．このとき，以下は同値である．
(i) $F(x,y)$ は $\mathbb{Z}_p$ 上の形式群である．
(ii) $F(x,y)$ はある特殊元に属する．

定理 3.1.6. $F(x,y), G(x,y)$ を $\mathbb{Z}_p$ 上の形式群とし，$f(x), g(x)$ をそれぞれの変換子とする．$F(x,y), G(x,y)$ が特殊元 u, v に属しているとき，

$$\mathrm{Hom}_{\mathbb{Z}_p}(F,G) = \{g^{-1}(cf(x)) \mid c \in \mathbb{Z}_p,\ vc = tu \quad (^{\exists}t \in \mathbb{Z}_p[[T]])\}$$

が成り立つ．とくに，$F \approx_{\mathbb{Z}_p} G$ となる為の必要十分条件は，$v = tu$ を満たす $\mathbb{Z}_p[[T]]^*$ の元 t が存在することである．

定理 3.1.6 により，$\mathbb{Z}_p$ 上の形式群の強同型による分類は，特殊元を同伴類により分類することと同値である．

p-進 Weierstrass 予備定理 (命題 4.3.3) より次が従う．

定理 3.1.7. 特殊元の同伴類は，

$$\{p\} \cup \cup_{h\geq 1}\{p + \sum_{\nu=1}^{h} c_\nu T^\nu \mid c_1, \ldots, c_{h-1} \in p\mathbb{Z}_p,\ c_h \in \mathbb{Z}_p^*\}$$

と 1 : 1 に対応する．

h は形式群の高さに対応する．また，次のように $\mathbb{Z}[[T]]$ の元で代表元を与えることもできる．

定理 3.1.8. 特殊元の同伴類は，

$$\{p + \sum_{\nu\geq 1} a_\nu T^\nu \mid a_\nu \in \mathbb{Z},\ 0 \leq a_\nu < p\}$$

と 1 : 1 に対応する．

[**証明**] $u = p + \sum_{\nu\geq 1} c_\nu T^\nu$ を特殊元，$t = \sum_{\nu\geq 0} b_\nu T^\nu$ を $\mathbb{Z}_p[[T]]^*$ の元とする．このとき，

$$tu = (\sum_{\nu\geq 0} b_\nu T^\nu)(p + \sum_{\nu\geq 1} c_\nu T^\nu) = \sum_{n\geq 0}(pb_n + c_1 b_{n-1} + \cdots + c_n b_0)T^n$$

が成立する．よって，与えられた特殊元 u に対し，帰納的に，

$$\begin{aligned} a_n &\equiv c_1 b_{n-1} + \cdots + c_n b_0 \bmod p, \qquad 0 \leq a_n < p, \\ b_n &= (a_n - c_1 b_{n-1} - \cdots - c_n b_0)/p \end{aligned}$$

を満たす $\mathbb{Z}$ の元 a_n，$\mathbb{Z}_p$ の元 b_n が一意的に定まり，tu は定理の形になる． □

3.2 $\mathbb{Z}$ 上の形式群

3.1 節の定理を用いて，$\mathbb{Z}$ 上の形式群を分類する．

命題 3.2.1 (Hasse の原理). (i) $F(x,y)$ を $\mathbb{Q}$ 上の形式群とする．このとき，形式群 $F(x,y)$ が $\mathbb{Z}$ 上定義されることと，すべての素数 p に対し $F(x,y)$ が $\mathbb{Z}_p$ 上定義されることは同値である．
(ii) $F(x,y), G(x,y)$ を $\mathbb{Z}$ 上の形式群とする．このとき，$F(x,y)$ と $G(x,y)$ が $\mathbb{Z}$ 上で強同型であることと，すべての素数 p に対し $F(x,y)$ と $G(x,y)$ が $\mathbb{Z}_p$ 上で強同型であることは同値である．

[**証明**] (i) は明らか．(ii) を示す．$f(x)$，$g(x)$ を $F(x,y)$，$G(x,y)$ の変換子とする．定理 2.4.1 により，$F(x,y)$ から $G(x,y)$ への $\mathbb{Q}$ 上の強同型はただひとつであり，$g^{-1}(f(x))$ で与えられる．よって，$F(x,y)$ から $G(x,y)$ への $\mathbb{Q}_p$ 上の強同型も $g^{-1}(f(x))$ で与えられる．$g^{-1}(f(x))$ が $\mathbb{Z}[[x]]$ の元であることと，すべての p に対し，$g^{-1}(f(x))$ が $\mathbb{Z}_p[[x]]$ の元であることとは同値だから，(ii) が成り立つ． □

定理 3.2.2. $\{c_{p^\nu}\}_{p,\nu\geq 0}$ を $c_0 = 1$ を満たす整数の数列とする．$\{a_n\}_{n\geq 0}$ を形式的オイラー積

$$\sum_{n\geq 1}\frac{a_n}{n^s} := \prod_p \frac{1}{1+\sum_{\nu\geq 1} c_{p^\nu} p^{\nu-1-\nu s}} \tag{3.1}$$

で定義し，

$$f(x) := \sum_{n\geq 1}\frac{a_n}{n}x^n, \qquad F(x,y) := f^{-1}(f(x)+f(y))$$

とおく．このとき，任意の素数 p に対し，$\mathbb{Q}_p$ 上の形式群 $F(x,y)$ は，特殊元 $p + \sum_{\nu\geq 1} c_{p^\nu} T^\nu$ に属する．とくに，$F(x,y)$ は $\mathbb{Z}$ 上定義される．

[**証明**] $\sum_{n\geq 1} a_n n^{-s}$ が Euler 積表示を持つので，

$$a_{mn} = a_m a_n \qquad ((m,n)=1) \tag{3.2}$$

が成立する．$\sum_{n\geq 1} a_n n^{-s}$ の p-factor に着目して，

$$\begin{aligned} 1 &= \left(\sum_{\mu\geq 0}\frac{a_{p^\mu}}{p^{\mu s}}\right)\left(1+\sum_{\nu\geq 1}\frac{p^{\nu-1}c_{p^\nu}}{p^{\nu s}}\right) = \sum_{\mu\geq 0}\frac{a_{p^\mu}}{p^{\mu s}} + \sum_{\substack{\mu\geq 0\\ \nu\geq 1}}\frac{p^{\nu-1}a_{p^\mu}c_{p^\nu}}{p^{(\mu+\nu)s}} \\ &= 1+\sum_{\kappa\geq 1}\left(\frac{a_{p^\kappa}}{p^{\kappa s}} + \sum_{\nu\geq 1}^{\kappa}\frac{p^{\nu-1}a_{p^{\kappa-\nu}}c_{p^\nu}}{p^{\kappa s}}\right) \end{aligned}$$

が成立する．ゆえに，

$$a_{p^\kappa} + \sum_{\nu\geq 1}^{\kappa} p^{\nu-1} a_{p^{\kappa-\nu}} c_{p^\nu} = 0 \quad (^\forall\kappa \geq 1). \tag{3.3}$$

(3.2) と (3.3) を用いると，

$$\begin{aligned}
&\left(p+\sum_{\nu\geq 1}c_{p^\nu}T^\nu\right)*\sum_{n\geq 1}\frac{a_n}{n}x^n\\
=\ &\left(p+\sum_{\nu\geq 1}c_{p^\nu}T^\nu\right)*\sum_{\substack{m\geq 1\\(m,p)=1}}\sum_{\mu\geq 0}\frac{a_{mp^\mu}}{mp^\mu}x^{mp^\mu}\\
=\ &\left(p+\sum_{\nu\geq 1}c_{p^\nu}T^\nu\right)*\sum_{\substack{m\geq 1\\(m,p)=1}}\left(\frac{a_m}{m}\sum_{\mu\geq 0}\frac{a_{p^\mu}}{p^\mu}x^{mp^\mu}\right)\quad\because (3.2)\\
=\ &\sum_{\substack{m\geq 1\\(m,p)=1}}\frac{a_m}{m}\left(\sum_{\mu\geq 0}\frac{pa_{p^\mu}}{p^\mu}x^{mp^\mu}+\sum_{\substack{\mu\geq 0\\\nu\geq 1}}\frac{c_{p^\nu}a_{p^\mu}}{p^\mu}(x^{p^\nu})^{mp^\mu}\right)\\
=\ &\sum_{\substack{m\geq 1\\(m,p)=1}}\frac{a_m}{m}\left(\sum_{\mu\geq 0}\frac{pa_{p^\mu}}{p^\mu}x^{mp^\mu}+\sum_{\substack{\mu\geq 0\\\nu\geq 1}}\frac{p^\nu c_{p^\nu}a_{p^\mu}}{p^{\nu+\mu}}x^{mp^{\nu+\mu}}\right)\\
=\ &\sum_{\substack{m\geq 1\\(m,p)=1}}\frac{a_m}{m}\left(px^m+\sum_{\kappa\geq 1}\frac{pa_{p^\kappa}}{p^\kappa}x^{mp^\kappa}+\sum_{\kappa\geq 1}\sum_{\nu=1}^{\kappa}\frac{p^\nu c_{p^\nu}a_{p^{\kappa-\nu}}}{p^\kappa}x^{mp^\kappa}\right)\\
=\ &p\sum_{\substack{m\geq 1\\(m,p)=1}}\frac{a_m}{m}x^m\equiv 0 \bmod p\quad\because (3.3)
\end{aligned}$$

が成立する．よって，$\mathbb{Q}_p$ 上の形式群 $F(x,y)$ は特殊元 $p+\sum_{\nu\geq 1}c_{p^\nu}T^\nu$ に属する．

定理 3.1.5，命題 3.2.1 より，$F(x,y)$ は $\mathbb{Z}$ 上の形式群となる． □

自然な写像

$$\{\text{形式群}/\mathbb{Z}\}/\underset{\mathbb{Z}}{\approx}\ \to\prod_p\{\text{形式群}/\mathbb{Z}_p\}/\underset{\mathbb{Z}_p}{\approx} \tag{3.4}$$

を考える．この写像の単射性が Hasse の原理により従い，全射性が定理 3.1.8 と定理 3.2.2 から従う．すなわち，写像 (3.4) は全単射である．

また，定理 3.2.2 において，$0\leq c_{p^\nu}<p\quad(^\forall\nu\geq 1)$ を満たす形式群が，$\mathbb{Z}$ 上の形式群の強同型類の完全代表系となる．

定理 3.2.2 において，形式的 Dirichlet 級数 $\sum a_n n^{-s}$ が Euler 積を持つことは，各 p-factor に $\mathbb{Z}_p$ 上の形式群が対応し，$F(x,y)$ がいわばそれらの局所的形式群の直積として得られた大域的形式群であることを意味する [12, p.210].

例 3.2.3. (i) $\mathbb{Z}_p$ 上の乗法群 $\hat{\mathbb{G}}_m(x,y)$ は特殊元 $p-T$ に属する．なぜならば，$\hat{\mathbb{G}}_m(x,y)$ の変換子は，$\sum x^n/n$ であり，対応する Dirichlet 級数は Riemann zeta 関数 $\sum_{n\geq 1}n^{-s}$ である．Riemann zeta 関数は，Euler 積表示

$$\sum_{n\geq 1}\frac{1}{n^s}=\prod_p\frac{1}{1-p^{-s}}$$

を持つので，定理 3.2.2 より，$\hat{\mathbb{G}}_m(x,y)$ は特殊元 $p-T$ に属する．

(ii) $\mathbb{Z}_p$ 上の形式群 $F_t(x,y)$ は特殊元 $p-T$ に属する．なぜならば，$F_t(x,y)$ の変換子は，

$$\arctan x = \sum_{n\geq 0} \frac{(-1)^n}{2n+1} x^{2n+1} = \sum_{n\geq 1} \left(\frac{-4}{n}\right) x^n$$

であり，対応する Dirichlet 級数は Euler 積表示

$$\sum_{n\geq 1} \left(\frac{-4}{p}\right) \frac{1}{n^s} = \prod_p \frac{1}{1-(\frac{-4}{p})p^{-s}}$$

を持つので，定理 3.2.2 より，$F_t(x,y)$ は特殊元 $p-(\frac{-4}{p})T$ に属する．

第4章　形式群の本田理論(証明)

この章では，本田理論の証明について述べます．引き続き $\mathbb{Z}_p$ 上の 1 次元形式群に限定して話をすすめます．$\mathfrak{p}$ 進整数環上の高次元形式群の本田理論を考える場合，4.1 節は仮定無しに一般化できる命題，4.2 節は $\mathfrak{p}$ が不分岐な場合に一般化できる命題，4.3 節は $\mathfrak{p}$ が不分岐かつ 1 次元形式群という条件下で一般化できる命題です．また，4.4 節の命題は次章での議論で必要になります．

4.1　特殊元に属する形式群

命題 4.1.1. p を素数とし，$\nu \geq 0$，$m \geq 1$ とする．このとき，

$$p^{-\nu}(X+pY)^{mp^\nu} \equiv p^{-\nu}X^{mp^\nu} \bmod p$$

が成り立つ．さらに，

$$n^{-1}(X+pY)^{n} \equiv n^{-1}X^{n} \bmod p$$

が成立する．

[**証明**]　1　$m=1$ の場合を示す．

$$p^{-\nu}(X+pY)^{p^\nu} \equiv p^{-\nu}X^{p^\nu} \bmod p$$

が成り立つための必要十分条件は，2 項定理により，

$$\binom{p^\nu}{j}p^{j-\nu} \equiv 0 \bmod p \quad (1 \leq j \leq p^\nu)$$

である．$\displaystyle\binom{p^\nu}{j}p^{j-\nu} = \frac{p^j(p^\nu-1)\cdots(p^\nu-j+1)}{j!}$ より，

$$\mathrm{ord}_p(j!) < j \quad (1 \leq j \leq p^\nu)$$

を示せば十分である．

$$\mathrm{ord}_p(j!) = \sum_{k=1}^{j}\mathrm{ord}_p(k) = \sum_{t\geq 1} t \times \sharp\{k \mid 1 \leq k \leq j,\ \mathrm{ord}_p(k)=t\} = ①$$

である．$[j/p^t] = \sharp\{k \mid 1 \le k \le j,\ \mathrm{ord}_p(k) \ge t\}$，$p \ge 2$ より，

$$① = \sum_{t\ge1} t \times \left(\left[\frac{j}{p^t}\right] - \left[\frac{j}{p^{t+1}}\right] \right) = \sum_{t\ge1} \left[\frac{j}{p^t}\right] < \sum_{t\ge1} \frac{j}{p^t} = \frac{j}{p-1} \le j$$

を得る．

2 $m \ge 1$ の場合を示す．

$$p^{-\nu}(X+pY)^{mp^\nu} = p^{-\nu}\{(X+pY)^m\}^{p^\nu} = ②$$

である．$(X+pY)^m \equiv X^m \bmod p$ だから，1 により，

$$② \equiv p^{-\nu}(X^m)^{p^\nu} \equiv p^{-\nu}X^{mp^\nu} \bmod p$$

が成立する．

3 命題の後半は，$n = mp^\nu \quad (m,p) = 1$ と書けることより成立する． □

注意 4.1.2. 命題 4.1.1 は，

$$X, Y \in \mathbb{Z}_p[[x_1, \dots, x_n]],$$

$$X, Y \in \mathbb{Z}_p[[x_1, \dots, x_n]]/(x_1, \dots, x_n)^r$$

でも成立する．

命題 4.1.3. u を特殊元とする．$u^{-1}p = 1 + \sum_{\nu\ge1} b_\nu T^\nu$ とおくとき，

$$p^\nu b_\nu \in \mathbb{Z}_p \quad (^\forall \nu \ge 1)$$

が成立する．

[**証明**] $u := p + \sum_{\nu\ge1} a_\nu T^\nu$ とおく．$uu^{-1}p = p$ より，

$$\big(p + \sum_{\nu\ge1} a_\nu T^\nu\big)\big(1 + \sum_{\nu\ge1} b_\nu T^\nu\big) = p$$

が成り立つ．T に pT を代入して，

$$\big(p + \sum_{\nu\ge1} p^\nu a_\nu T^\nu\big)\big(1 + \sum_{\nu\ge1} p^\nu b_\nu T^\nu\big) = p$$

を得る．両辺を p で割ることにより，

$$\big(1 + \sum_{\nu\ge1} p^{\nu-1} a_\nu T^\nu\big)\big(1 + \sum_{\nu\ge1} p^\nu b_\nu T^\nu\big) = 1$$

を得る．$1+\sum_{\nu\geq 1}p^{\nu-1}a_\nu T^\nu \in \mathbb{Z}_p[[T]]^*$ より，

$$1+\sum_{\nu\geq 1}p^\nu b_\nu T^\nu \in \mathbb{Z}_p[[T]]^*$$

が成立する．とくに，

$$p^\nu b_\nu \in \mathbb{Z}_p \quad ({}^\forall\nu \geq 1)$$

が従う． □

命題 4.1.4. u, v を特殊元とする．$h(x) := u^{-1}p * x$ とおき，$\psi(x_1,\ldots,x_n)$ を $\mathbb{Z}_p[[x_1,\ldots,x_n]]_0$ の元とする．$p\psi \equiv 0 \bmod \deg r,\ \bmod p$ なる $r\geq 2$ が存在するならば，

$$v*(h\circ\psi) \equiv (v*h)\circ\psi \bmod \deg r,\ \bmod p$$

が成立する．

[**証明**] 1 $u^{-1}p=\sum_{\nu\geq 0}b_\nu T^\nu \quad (b_1=1)$ とおく．

$$h(x)=u^{-1}p*x=\sum_{\nu\geq 0}b_\nu T^\nu * x=\sum_{\nu\geq 0}b_\nu x^{p^\nu}$$

である．$v=\sum_{\nu\geq 0}a_\nu T^\nu$ とおく．

$$\begin{aligned} v*(h\circ\psi) &= \sum_{\nu\geq 0}a_\nu T^\nu * \sum_{\mu\geq 0}b_\mu\{\psi(x_1,\ldots,x_n)\}^{p^\mu} \\ &= \sum_{\nu,\mu}a_\nu b_\mu\{\psi(x_1^{p^\nu},\ldots,x_n^{p^\nu})\}^{p^\mu} \\ &= \sum_{\nu,\mu}a_\nu(p^\mu b_\mu)p^{-\mu}\{\psi(x_1^{p^\nu},\ldots,x_n^{p^\nu})\}^{p^\mu} \end{aligned}$$

が成立する．一方，

$$v*h=\sum_{\nu,\mu}a_\nu b_\mu x^{p^{\mu+\nu}},$$

$$\begin{aligned} (v*h)\circ\psi &= \sum_{\nu,\mu}a_\nu b_\mu\{\psi(x_1,\ldots,x_n)\}^{p^{\mu+\nu}} \\ &= \sum_{\nu,\mu}a_\nu p^\mu b_\mu p^{-\mu}\{\psi(x_1,\ldots,x_n)\}^{p^{\mu+\nu}} \end{aligned}$$

が成立する．よって，

$$p^{-\mu}\{\psi(x_1^{p^\nu},\ldots,x_n^{p^\nu})\}^{p^\mu} \equiv p^{-\mu}\{\psi(x_1,\ldots,x_n)\}^{p^{\mu+\nu}} \bmod p \tag{4.1}$$

を示せば十分である.

2 $\mu = 0$ の場合を示す.

$\nu = 0$ のときは (4.1) は明らかに成立するので, $\nu \geq 1$ と仮定する.

ψ の total degree が r 以上の項の和と r 未満の項の和を, それぞれ, ψ_0, ψ_1 とおく. $\psi = \psi_0 + \psi_1$ である. 仮定 $p\psi \equiv 0 \mod \deg r, \mod p$ より, $\psi_0 \in \mathbb{Z}_p[[x_1, \ldots, x_n]]$. 従って,

$$\psi_0(x_1^{p^\nu}, \ldots, x_n^{p^\nu}) \equiv \{\psi_0(x_1, \ldots, x_n)\}^{p^\nu} \mod p, \tag{4.2}$$

$$\psi(x_1^{p^\nu}, \ldots, x_n^{p^\nu}) - \psi_0(x_1^{p^\nu}, \ldots, x_n^{p^\nu}) = \psi_1(x_1^{p^\nu}, \ldots, x_n^{p^\nu}) \equiv 0 \mod \deg rp^\nu$$

が成立する. また, $\psi(0) = \psi_0(0) = 0$ より,

$$\{\psi(x_1, \ldots, x_n)\}^{p^\nu} - \{\psi_0(x_1, \ldots, x_n)\}^{p^\nu} = \sum_{j=1}^{p^\nu} \binom{p^\nu}{j} \psi_0^{p^\nu - j} \psi_1^j \equiv 0 \bmod \deg r+1$$

が成立する. よって, (4.2) より,

$$\psi(x_1^{p^\nu}, \ldots, x_n^{p^\nu}) \equiv \{\psi(x_1, \ldots, x_n)\}^{p^\nu} \mod \deg r+1, \mod p$$

が成り立つ.

3 $\mu > 0$ の場合を示す.

$\nu = 0$ のときは (4.1) は明らかに成立するので, $\nu \geq 1$ と仮定する.

命題 4.1.1 と 2 により,

$$p^{-\mu}\{\psi(x_1^{p^\nu}, \ldots, x_n^{p^\nu})\}^{p^\mu} \equiv p^{-\mu}\{\psi(x_1, \ldots, x_n)\}^{p^{\mu+\nu}} \mod \deg r+1, \mod p$$

が成り立つ. □

命題 4.1.5. $f(x)$, $g(x)$ を $\mathbb{Q}_p[[x]]_0$ の元とする. $f(x)$, $g(x)$ が特殊元 u に属するならば, $(f^{-1} \circ g)(x)$ は $\mathbb{Z}_p[[x]]$ の元である.

[**証明**] 1 $h(x) := u^{-1}p * x$ とおく.

$$u * h(x) = u * (u^{-1}p * x) = p * x = px$$

に注意する.

2 $f(x) = h(x)$ と仮定する.

$$p(h^{-1} \circ g)(x) \equiv 0 \mod \deg r, \mod p \quad (^\forall r \geq 2) \tag{4.3}$$

を r に関する帰納法で示す.

(i) $r = 2$ のとき

$$p(h^{-1} \circ g)(x) \equiv px \equiv 0 \mod \deg 2, \mod p$$

が成立する.

(ii) $r = k$ のとき (4.3) が成立すると仮定する．命題 4.1.4 により，

$$\begin{aligned} p(h^{-1} \circ g) &= (u * h) \circ (h^{-1} \circ g) \\ &\equiv u * (h \circ h^{-1} \circ g) \bmod \deg k+1,\ \bmod p \\ &\equiv u * g \equiv 0 \bmod \deg k+1,\ \bmod p \end{aligned}$$

が成立する．

(iii) (i)，(ii) より，(4.3) は任意の r に対し成立する．よって，$p(h^{-1} \circ g) \equiv 0 \bmod p$ となり，$h^{-1} \circ g \in \mathbb{Z}_p[[x]]$ が示された．

3 $f(x) \neq h(x)$ のとき， 2 により，

$$f^{-1} \circ g = (h^{-1} \circ f)^{-1} \circ (h^{-1} \circ g) \in \mathbb{Z}_p[[x]]$$

が従う． □

命題 4.1.6. $\mathbb{Q}_p$ 上の形式群 $F(x,y)$ が特殊元 u に属するならば，$F(x,y)$ は $\mathbb{Z}_p$ 上の形式群である．

[**証明**] 1 $H(x,y) = h^{-1}(h(x)+h(y))$, $h(x) = u^{-1}p * x$ とおく．このとき，$H(x,y)$ は特殊元 u に属する．帰納法により，

$$pH(x,y) \equiv 0 \ \bmod \deg r,\ \bmod p \quad ({}^{\forall}r \geq 2) \tag{4.4}$$

を示す．

(i) $r = 2$ のとき，

$$pH(x,y) \equiv p(x+y) \equiv 0 \bmod \deg 2,\ \bmod p$$

が成立する．

(ii) $r = k$ のとき，(4.4) が成り立つと仮定する．

$$\begin{aligned} pH(x,y) &= (u * h) \circ h^{-1}(h(x)+h(y)) \\ &\equiv u * \{h \circ h^{-1}(h(x)+h(y))\} \ \bmod \deg k+1,\ \bmod p \quad (\because \text{命題 4.1.4}) \\ &\equiv u * h(x) + u * h(y) \bmod \deg k+1,\ \bmod p \\ &\equiv 0 \ \bmod \deg k+1,\ \bmod p \quad (\because h(x) \text{ は特殊元 } u \text{ に属する}) \end{aligned}$$

が成立する．

(iii) (i)，(ii) よりすべての r に対し，(4.4) が成立する．

2 命題 4.1.4 より，$\varphi(x) := (h^{-1} \circ f)(x)$ は $\mathbb{Z}_p[[x]]$ の元である．$\varphi(x)$ は $F(x,y)$ から $H(x,y)$ への $\mathbb{Z}_p$ 上の強同型であるから，

$$F(x,y) = \varphi^{-1}(H(\varphi(x), \varphi(y))) \in \mathbb{Z}_p[[x,y]]$$

が成り立つ． □

命題 4.1.7. $f(x)$ を $\mathbb{Q}_p[[x]]_0$ の元とする．$f(x)$ が特殊元 u に属するならば，

$$\{v \in \mathbb{Z}_p[[T]] \mid v * f \equiv 0 \bmod p\} = (u)$$

である．ただし，(u) は u で生成される $\mathbb{Z}_p[[T]]$ のイデアルとする．

[**証明**] 1 (左辺) $\supset$ (右辺) を示す.
$v = tu$ のとき，

$$v * f = tu * f = t * (u * f) \equiv 0 \bmod p \quad (\because f(x) \text{ は特殊元 } u \text{ に属する})$$

が成り立つ.
2 (左辺) $\subset$ (右辺) を示す.
$h(x) := u^{-1}p * x$，$\varphi(x) := (h^{-1} \circ f)(x) \in \mathbb{Z}_p[[x]]$ とおく.
(i) $v * f \equiv 0 \bmod p$ ならば $v * h \equiv 0 \bmod p$ を示す.

$$\begin{aligned}(v * h) \circ \varphi &\equiv v * (h \circ \varphi) \bmod p \quad (\because \varphi(x) \in \mathbb{Z}_p[[x]], \text{ 命題 4.1.4}) \\ &\equiv v * (h \circ \varphi) \bmod p\end{aligned}$$

が成立する．ゆえに，

$$v * h = (v * h) \circ \varphi \circ \varphi^{-1} \equiv 0 \bmod p \quad (\because\ \varphi^{-1}(x) \in \mathbb{Z}_p[[x]])$$

が成り立つ.
(ii) $v * h \equiv 0 \bmod p$ ならば，$t \in \mathbb{Z}_p[[T]]$ が存在して，$v = tu$ を示す.
$vu^{-1}p = \sum_{\nu \geq 0} a_\nu T^\nu$ とおく.

$$v * h = v * (u^{-1}p * x) = \sum_{\nu \geq 0} a_\nu T^\nu * x = \sum_{\nu \geq 0} a_\nu x^{p^\nu}$$

が成り立つ．$v * h \equiv 0 \bmod p$ より，

$$a_\nu \equiv 0 \bmod p \quad (^\forall \nu \geq 0)$$

を得る．よって，$t = vu^{-1}$ とおくとき，

$$t = \frac{1}{p} \sum_{\nu \geq 0} a_\nu T^\nu \in \mathbb{Z}_p[[T]]$$

が成り立つ. □

命題 4.1.8. $\mathbb{Q}_p$ 上の形式群 $F(x, y)$，$G(x, y)$ が，それぞれ，特殊元 u，v に属すると仮定する．$f(x)$，$g(x)$ を $F(x, y)$，$G(x, y)$ の変換子とするとき，

$$\mathrm{Hom}_{\mathbb{Z}_p}(F, G) = \{g^{-1}(cf(x)) \mid vc = tu \quad (^\exists t \in \mathbb{Z}_p[[T]])\}$$

が成り立つ.

[**証明**] $f(x) := u^{-1}p*x$, $g(x) := v^{-1}p*x$ と仮定してよい. $\varphi(x) := g^{-1}(cf(x))$ とおく.
1 $\varphi(x) \in \mathrm{Hom}_{\mathbb{Z}_p}(F,G)$ ならば, $vc = tu$ を示す.

$$\begin{aligned} vc*f &= v*cf = v*(g\circ\varphi) \\ &= (v*g)\circ\varphi \quad (\because \varphi(x) \in \mathbb{Z}_p[[x]], \text{命題 4.1.4}) \\ &\equiv 0 \bmod p \quad (\because g(x) \text{は特殊元 } v \text{ に属する}) \end{aligned}$$

が成り立つ. ゆえに, 命題 4.1.7 より, $\mathbb{Z}_p[[T]]$ の元 t が存在して, $vc = tu$ を得る.
2 $vc = tu$ ならば, $\varphi \in \mathrm{Hom}_{\mathbb{Z}_p}(F,G)$ を示す.

$$p\varphi \equiv 0 \bmod \deg r, \bmod p \quad (^\forall r \geq 2) \tag{4.5}$$

を r に関する帰納法で示せば十分である.
(i) $r = 2$ のとき,

$$p\varphi \equiv pcx \equiv 0 \bmod \deg 2, \bmod p$$

が成立する.
(ii) $r = k$ のとき, (4.5) が成立すると仮定する.

$$\begin{aligned} p\varphi &\equiv (v*g)\circ\varphi \\ &\equiv v*(g\circ\varphi) \bmod \deg k+1, \bmod p \quad (\because \text{命題 4.1.4}) \\ &\equiv v*cf \equiv vc*f \equiv tu*f \bmod \deg k+1, \bmod p \\ &\equiv t*u*f \equiv 0 \bmod \deg k+1, \bmod p \quad (\because f(x) \text{は特殊元 } u \text{ に属する}) \end{aligned}$$

が成立する.
(iii) (i), (ii) より, (4.5) はすべての r に対し成立する. □

4.2 $\mathbb{Z}_p$ 上の形式群と特殊元

命題 4.2.1. $F(x,y)$ を $\mathbb{Q}_p$ 上定義された形式群とする. $F(x,y)$ が $\mathbb{Z}_p$ 上定義されるならば, ある特殊元 u が存在し, $F(x,y)$ は特殊元 u に属する.

[**証明**] $f(x) = \sum_{n\geq 1} a_n x^n/n$ を $F(x,y)$ の変換子とする. 任意の $\mu \geq 0$ に対し, $\mathbb{Z}_p$ の元 $c_0, \ldots, c_\mu$ が存在し,

$$\sum_{\nu=0}^{\mu} c_\nu f(x^{p^\nu}) \equiv 0 \bmod \deg p^\mu + 1, \bmod p \tag{4.6}$$

が成立することを μ に関する帰納法で証明する.
(i) $\mu = 0$ のとき,

$$pf(x) \equiv px \equiv 0 \bmod \deg 2, \bmod p$$

より, $c_0 = p$ として, (4.6) が成立する.

(ii) $\mu = k$ に対し，(4.6) が成立すると仮定する．このとき，$n \geq p^{\mu}+1$ に対し，$\mathbb{Q}_p$ の元 b_n が存在し，

$$\sum_{\nu=0}^{k} c_\nu f(x^{p^\nu}) \equiv \sum_{n \geq p^k+1} b_n x^n \bmod p \tag{4.7}$$

が成り立つ．ここで，$b_n \in p\mathbb{Z}_p \quad (^\forall n \geq p^k+1)$ ならば，$c_{k+1} = 0$ ととり，(4.6) が成り立つ．$b_n \notin p\mathbb{Z}_p$ となる $n \geq p^k+1$ が存在すると仮定する．(4.7) の x に $F(x,y)$ を代入し，

$$\sum_{\nu=0}^{k} c_\nu f(F(x,y)^{p^\nu}) \equiv \sum_{n \geq p^k+1} b_n F(x,y)^n \bmod p \tag{4.8}$$

を得る．ここで，$F(x,y)$ は $\mathbb{Z}_p[[x,y]]$ の元だから，

$$F(x,y)^{p^\nu} \equiv F(x^{p^\nu}, y^{p^\nu}) \bmod p$$

が成立する．命題 4.1.1 より，

$$\frac{a_n}{n} F(x,y)^{np^\nu} \equiv \frac{a_n}{n} F(x^{p^\nu}, y^{p^\nu})^n \bmod p$$

を得る．両辺の n についての和をとって，

$$f(F(x,y)^{p^\nu}) \equiv f(F(x^{p^\nu}, y^{p^\nu})) \bmod p$$

を得る．よって，(4.8) より，

$$\begin{aligned} \sum_{\nu=0}^{k} c_\nu f(F(x^{p^\nu}, y^{p^\nu})) &\equiv \sum_{n \geq p^k+1} b_n F(x,y)^n \bmod p, \\ \sum_{\nu=0}^{k} c_\nu \{f(x^{p^\nu}) + f(y^{p^\nu})\} &\equiv \sum_{n \geq p^k+1} b_n F(x,y)^n \bmod p \end{aligned} \tag{4.9}$$

が成立する．(4.9) に $y = 0$ を代入することにより，

$$\sum_{\nu=0}^{k} c_\nu f(x^{p^\nu}) \equiv \sum_{n \geq p^k+1} b_n x^n \bmod p \quad (\because F(x,0) = x)$$

が成立する．同様にして

$$\sum_{\nu=0}^{k} c_\nu f(y^{p^\nu}) \equiv \sum_{n \geq p^k+1} b_n y^n \bmod p$$

を得る．これら 2 式の左辺の和が (4.9) の左辺であることに注意して，

$$\sum_{n \geq p^k+1} b_n \{F(x,y)^n - x^n - y^n\} \equiv 0 \bmod p \tag{4.10}$$

を得る．n を $b_n \notin p\mathbb{Z}_p$ となる最小の n とする．(4.10) の total degree が n の項に着目して，

$$b_n\{(x+y)^n - x^n - y^n\} \equiv 0 \bmod p$$

が成り立つ．よって，問題2.2.8(i)により，n は p のべき，かつ，$pb_n \in p\mathbb{Z}_p$ である．$n \geq p^k+1$ より，$n \geq p^{k+1}$ となるので，ゆえに，

$$pb_{p^{k+1}} \in p\mathbb{Z}_p \text{ ，すなわち，} b_{p^{k+1}} \in \mathbb{Z}_p$$

を得る．よって，(4.8) より，

$$\sum_{\nu=0}^{k} c_\nu f(x^{p^\nu}) - b_{p^{k+1}} x^{p^{k+1}} \equiv \sum_{\nu=0}^{k} c_\nu f(x^{p^\nu}) - b_{p^{k+1}} f(x^{p^{k+1}}) \equiv 0 \bmod \deg p^{k+1}+1, \bmod p$$

が成り立つ．よって，$\mu = k+1$ に対して，(4.6) が成立する．

(iii) (i)，(ii) より，すべての μ に対し，(4.6) が成立する．

以上により，$u = p + \sum_{\mu \geq 1} c_\mu T^\mu$ に対し，$F(x,y)$ が特殊元 u に属することが示された．

□

4.3 特殊元の同伴類

命題 4.3.1. $f := \sum_{n=0}^{h} a_n T^n \quad (a_0, \ldots, a_{h-1} \in p\mathbb{Z}_p,\ a_h \in \mathbb{Z}_p^*)$ とする．このとき，$\mathbb{Z}_p[[T]]$ の任意の元 g に対し，ただ1組 $\mathbb{Z}_p[[T]]$ の元 q，$h-1$ 次以下の $\mathbb{Z}_p[T]$ の元 r が存在し，$g = qf + r$ が成立する．

[**証明**] 1 q,r の存在を示す．

まず，f の最高次の係数 a_h は単数だから，$\mathbb{Z}_p[[T]]^*$ の元 u が存在し，

$$f \equiv T^h u \bmod p$$

が成り立つ．

任意の自然数 n に対し，$\{q_j\}_{j=1}^n, \{r_j\}_{j=1}^n$ が存在し，

$$\begin{aligned} &g \equiv q_j f + r_j \bmod p^j \quad (1 \leq j \leq n), \\ &q_j \equiv q_{j-1} \bmod p^j \quad (2 \leq j \leq n), \\ &r_j \equiv r_{j-1} \bmod p^j \quad (2 \leq j \leq n), \\ &\deg(r_j) \leq h-1 \quad (1 \leq j \leq n) \end{aligned} \tag{4.11}$$

を満たすことを n に関する帰納法で示す．

(i) $n=1$ のとき，g の次数 $h-1$ 次以下の項の和を r_1 とおき，

$$q_1 := \frac{g - r_1}{uT^h} \in \mathbb{Z}_p[[T]]$$

とおく．このとき，

$$g - r_1 = q_1 u T^h \equiv q_1 f \bmod p$$

を得る．よって，$n = 1$ に対し，(4.11) が示された．

(ii) $n = k$ に対し，(4.11) が成立すると仮定する．

$$q_{k+1} = q_k + p^k a,\ r_{k+1} = r_k + p^k b$$

とおく．このとき，次式は同値である．

$$\begin{aligned} & g \equiv q_{k+1} f + r_{k+1} \bmod p^{k+1} \\ & g \equiv (q_k + p^k a) f + (r_k + p^k b) \bmod p^{k+1} \\ & \frac{g - q_k f - r_k}{p^k} \equiv af + b \bmod p \end{aligned} \tag{4.12}$$

(i) と同様にして，(4.12) を満たす $\mathbb{Z}_p[[T]]$ の元 a，次数 $h-1$ 次以下の多項式 b が存在するので，$n = k+1$ に対し，(4.11) が成立する．

(iii) (i)，(ii) より，任意の n に対して (4.11) 成立する．$q := \lim q_j$，$r := \lim r_j$ とおくことにより，q，r の存在が示された．

2 q，r の一意性を示す．

$$g = 0 \text{ のとき}, q = r = 0$$

を示せば十分である．

$0 = qf + r$ と仮定する．このとき，$f \equiv 0 \bmod \deg h, \bmod p$ より，

$$r \equiv 0 \bmod \deg h, \bmod p$$

である．$\deg r \leq h - 1$ より，

$$r \equiv 0 \bmod p$$

が成り立つ．$0 = qf + r \equiv qT^h u \bmod p$，$u \in \mathbb{Z}_p[[T]]^*$ より，

$$q \equiv 0 \bmod p$$

を得る．ゆえに，

$$\frac{r}{p}, \frac{q}{p} \in \mathbb{Z}_p[[T]], \qquad \frac{q}{p} f + \frac{r}{p} = 0$$

を得る．この議論を繰り返して，すべての n に対し，

$$r \equiv 0 \bmod p^n, \qquad q \equiv 0 \bmod p^n$$

が成立する．ゆえに，

$$r = 0, \qquad q = 0$$

となる． □

定義 4.3.2. $\mathbb{Z}_p[T]$ の h 次の元 g が **distinguished 多項式**であるとは，monic，かつ $g \equiv T^h \bmod p$ を満たすことをいう．

命題 4.3.3 (Weierstrass 予備定理). $f = \sum_{n\geq 0} a_n T^n$ を $\mathbb{Z}_p[[T]]$ の元とし，$h := \min\{n \mid a_n \in \mathbb{Z}_p^*\} < +\infty$ と仮定する．このとき，$\mathbb{Z}_p[[T]]^*$ の元 u と distinguished 多項式 g がただ 1 組存在し，

$$f = ug$$

を満たす.

[**証明**] 命題 4.3.1 より，$q \in \mathbb{Z}_p[[T]]$，$h-1$ 次以下の多項式 $r \in \mathbb{Z}_p[T]$ がただ 1 組存在し，

$$qf = T^h + r \tag{4.13}$$

を満たす．$g := T^h + r$ とおく．g は h 次，monic である．また，$f \equiv 0 \bmod \deg h$, $\bmod p$ より，$r \equiv 0 \bmod p$ である．よって，

$$g \equiv T^h \bmod p$$

となり，g は distinguished である．(4.13) 式の h 次の項に着目すると，

$$q(0)a_h \equiv 1 \bmod p$$

を得る．$a_h \in \mathbb{Z}_p^*$ より，$q(0) \in \mathbb{Z}_p^*$ である．ゆえに，$q \in \mathbb{Z}_p[[T]]^*$ となる．$u := q^{-1}$ とおくことにより，命題が成立する． □

命題 4.3.4. 特殊元の同伴類は,

$$\{p\} \cup \cup_{h\geq 1}\{p + \sum_{\nu=1}^{h} c_\nu T^\nu \mid c_1, \ldots, c_{h-1} \in p\mathbb{Z}_p,\ c_h \in \mathbb{Z}_p^*\} \tag{4.14}$$

の元と 1 : 1 に対応する.

[**証明**] $u := p + \sum_{\nu\geq 1} a_\nu T^\nu$ を特殊元とする．$h := \min\{a_\nu \mid a_\nu \in \mathbb{Z}_p^*\}$ とおく．$h = +\infty$ を仮定すると，$u(0)/p = 1$ より，$up^{-1} \in \mathbb{Z}_p[[T]]^*$ が成立する．また，$h < +\infty$ のとき，命題 4.3.3 により，$\mathbb{Z}_p[[T]]^*$ の元 ε，h 次の distinguished 多項式 v が存在し，$u = \varepsilon v$ を満たす．$u(0) = p$ より，$\varepsilon(0)v$ は (4.14) の右辺の形の特殊元となる． □

4.4 $F_s(x, y)$ の属する特殊元

命題 4.4.1. $\mathbb{Q}_p[[x]]_0$ の元 $f(x)$ が特殊元 u に属すると仮定する．このとき，

$$f^{-1}(px) \equiv 0 \bmod p$$

が成立する.

[**証明**] $f(x)=h(x)=u^{-1}p*x$ の場合に示せば十分である．命題 4.1.3 により，

$$h(x)=\sum_{\nu\geq 0}\frac{a_\nu}{p^\nu}x^{p^\nu}\quad ({}^\exists a_\nu\in\mathbb{Z}_p)$$

とおける．$\varphi(x):=h^{-1}(px)$ とおく．

$$\varphi(x)\equiv 0 \bmod \deg r,\ \bmod p\quad ({}^\forall r\geq 2) \tag{4.15}$$

を r に関する帰納法で示す．

(i) $r=2$ のとき，

$$\varphi(x)\equiv px \bmod \deg 2$$

より，(4.15) が成立する．

(ii) $r=k$ のとき，(4.15) が成立すると仮定する．$\varphi_0(x)$，$\varphi_1(x)$ を，それぞれ，$\varphi(x)$ の次数 $k-1$ 以下の項の和，次数 k 以上の項の和とおく．仮定より，

$$\varphi_0(x)\equiv 0 \bmod p$$

を得る．$h\circ\varphi(x)=px$ より，

$$\varphi_0+\varphi_1+\sum_{\nu\geq 1}\frac{a_\nu}{p^\nu}(\varphi_0+\varphi_1)^{p^\nu}=px$$

を得る．$\varphi_1\equiv 0 \bmod \deg k$ より，

$$\varphi_0+\varphi_1+\sum_{\nu\geq 1}\frac{a_\nu}{p^\nu}\varphi_0^{p^\nu}\equiv px \bmod \deg k+1 \tag{4.16}$$

を得る．$\varphi_0\equiv 0 \bmod p$ より，

$$\frac{\varphi_0^{p^\nu}}{p^\nu}\equiv 0 \bmod p$$

を得る．よって，(4.16) より，

$$\varphi=\varphi_0+\varphi_1\equiv 0 \bmod \deg k+1,\ \bmod p$$

が成り立つ．

(iii) (i)，(ii) より，(4.15) は任意の $r\geq 2$ で成立する． □

命題 4.4.2. $\mathbb{Q}_p[[x]]_0$ の元 $f(x)$ が特殊元 u に属すると仮定する．$\psi_1(x)$ を $\mathbb{Q}_p[[x]]_0$ の元，$\psi_2(x)$ を $\mathbb{Z}_p[[x]]$ の元とする．このとき，次は同値である．

(i) $(f\circ\psi_1)(x)\equiv(f\circ\psi_2)(x) \bmod p$.

(ii) $\psi_1(x)\equiv\psi_2(x) \bmod p$.

[**証明**] (ii)⇒(i) $\psi_1(x) \equiv \psi_2(x) \bmod p$, $\psi_2(x) \in \mathbb{Z}_p[[x]]$ より，$\psi_1(x) \in \mathbb{Z}_p[[x]]$ である．$h(x) := u^{-1}p * x$ とおく．命題 4.1.3 により，$h(x) = \sum(a_\nu/p^\nu)x^{p^\nu}$ $(a_0 = 1,\ a_\nu \in \mathbb{Z}_p)$ とおける．$\varphi(x) := (h^{-1} \circ f)(x)$ とおく．命題 4.1.7 により，$\varphi(x) \in \mathbb{Z}_p[[x]]$ である．よって，

$$(\varphi \circ \psi_1)(x) \equiv (\varphi \circ \psi_2)(x) \bmod p$$

が成り立つ．命題 4.1.1 により，

$$\frac{a_\nu}{p^\nu}(\varphi \circ \psi_1)^{p^\nu} \equiv \frac{a_\nu}{p^\nu}(\varphi \circ \psi_2)^{p^\nu} \bmod p$$

を得る．両辺の ν についての和をとって，

$$h \circ \varphi \circ \psi_1 \equiv h \circ \varphi \circ \psi_2 \bmod p$$

を得る．ゆえに，

$$f \circ \psi_1 \equiv f \circ \psi_2 \bmod p$$

が成立する．

(i)⇒(ii) $p\lambda(x) := f^{-1}(f \circ \psi_1(x) - f \circ \psi_2(x))$ とおく．$f(x)$ は特殊元 u に属し，$f \circ \psi_1(x) - f \circ \psi_2(x) \equiv 0 \bmod p$ だから，命題 4.4.1 により，$\lambda(x)$ は $\mathbb{Z}_p[[x]]$ の元である．$f(x)$ は特殊元 u に属するので，$F(x,y) := f^{-1}(f(x) + f(y)) \in \mathbb{Z}_p[[x,y]]$．よって，

$$\psi_1(x) = F(\psi_2(x), p\lambda(x)) \equiv F(\psi_2(x), 0) \equiv \psi_2(x) \bmod p \quad (\because \psi_2(x) \in \mathbb{Z}_p[[x]])$$

が成り立つ． □

例 4.4.3. $p \neq 2$ とする．$\mathbb{Z}_p$ 上の形式群 $F_s(x,y) := x\sqrt{1-y^2} + y\sqrt{1-x^2}$ は特殊元 $p - (\frac{-1}{p})T$ に属する．なぜならば，$F_s(\sin x, \sin y) = \sin(x+y)$ より，

$$[p]_F(\sin x) = \sin px$$

が成立する．一方，

$$\cos px + i \sin px = (\cos x + i \sin x)^p \equiv \cos^p x + i^p \sin^p x \bmod p$$

である．従って，

$$\sin px \equiv i^{p-1} \sin^p x \bmod p$$

である．ゆえに，

$$[p]_F(x) \equiv (-1)^{\frac{p-1}{2}} x^p \bmod p$$

が成り立つ．$F_s(x,y)$ の変換子を $f(x)$ とおくと，

$$f^{-1}(pf(x)) \equiv (-1)^{\frac{p-1}{2}} x^p \bmod p$$

が成り立つ．命題4.2.1より，$f(x)$はある特殊元に属するので，命題4.4.2を用いて，

$$pf(x) \equiv f((-1)^{\frac{p-1}{2}}x^p) \bmod p$$

を得る．$f(-x) = -f(x)$に注意して，

$$pf(x) - (-1)^{\frac{p-1}{2}}f(x^p) \equiv 0 \bmod p$$

が成り立つ．よって，$F_s(x,y)$は特殊元$p - (\frac{-1}{p})T$に属する．

4.5 付記 $\mathfrak{p}$-進整数環上の高次元形式群

Kを標数0の離散付値体，$\mathcal{O}$をKの整数環，$\mathfrak{p}$を$\mathcal{O}$の極大整数環，πを素元とする．剰余体$\mathcal{O}/\mathfrak{p}$の標数pは正であると仮定する．さらに，あるKの自己同型σとpのべきqが存在し，

$$^{\sigma}\alpha \equiv \alpha^q \bmod \mathfrak{p} \quad (^{\forall}\alpha \in \mathcal{O})$$

が成り立つと仮定する．$K_\sigma[[T]]$ (resp. $\mathcal{O}_\sigma[[T]]$)を加群$K[[T]]$ (resp. $\mathcal{O}[[T]]$)に乗法を

$$T\alpha = {}^{\sigma}\alpha T \quad (^{\forall}\alpha \in K \text{ (resp. } ^{\forall}\alpha \in \mathcal{O}))$$

により定義した非可換環とする．

$$M_n(K_\sigma[[T]]) \times K[[\boldsymbol{x}]]_0^n \to K[[\boldsymbol{x}]]_0^n : \ (\sum c_\nu T^\nu, f(\boldsymbol{x})) \mapsto \sum {c_\nu}^{\sigma^\nu} f(\boldsymbol{x}^{q^\nu})$$

により，作用$*$を定義する．

定義 4.5.1. $u = \sum_{\nu\geq 0} c_\nu T^\nu \in M_n(\mathcal{O}_\sigma[[T]])$が特殊元であるとは，$c_0 = \pi I_n$を満たすことと定義する，また，$f(\boldsymbol{x}) \in K[[\boldsymbol{x}]]_0^n$が特殊元$u$に属するとは，$f(\boldsymbol{x}) \equiv \boldsymbol{x} \bmod \deg 2$, $u * f(\boldsymbol{x}) \equiv 0 \bmod p$を満たすことと定義する．

この定義の下，定理3.1.5，3.1.6，3.1.8，3.2.2は高次元化できる．また，4.1節は仮定無しに一般化できる命題，4.2節は$\mathfrak{p}$が不分岐な場合に一般化できる命題，4.3節は$\mathfrak{p}$が不分岐かつ1次元形式群という条件下で一般化できる命題である．

$\mathfrak{p}$-進整数環上の形式群の本田理論の計算例として，次の命題を示す．

命題 4.5.2. $q = p$，かつ$\mathfrak{p}$は不分岐であると仮定する．λが$\mathcal{O}^*$の元であるとき，$\mathcal{O}$上の形式群$x + y - \lambda xy$は特殊元$p - {}^{\sigma}\lambda\lambda^{-1}T$に属する．

[**証明**] 定理 2.4.1(証明) により，$x+y-\lambda xy$ の変換子 $f(x)$ は，

$$f(x)=\int\frac{dx}{1-\lambda x}=\sum_{n\geq 1}\frac{\lambda^{n-1}}{n}x^n$$

となる．

$$\begin{aligned}(p-{}^{\sigma}\lambda\lambda^{-1}T)*f &= p\sum_{n\geq 1}\frac{\lambda^{n-1}}{n}x^n-{}^{\sigma}\lambda\lambda^{-1}\sum_{n\geq 1}\frac{{}^{\sigma}\lambda^{n-1}}{n}x^{np}\\ &\equiv \sum_{n\geq 1}\frac{\lambda^{np-1}}{n}x^{np}-{}^{\sigma}\lambda\lambda^{-1}\sum_{n\geq 1}\frac{{}^{\sigma}\lambda^{n-1}}{n}x^{np} \bmod \mathfrak{p}\\ &\equiv \sum_{n\geq 1}\frac{\lambda^{np}-{}^{\sigma}\lambda^{n}}{\lambda n}x^{np} \bmod \mathfrak{p} \qquad (4.17)\end{aligned}$$

が成立する．ここで，$q=p$，σ はフロベニウス写像だから，

$$\lambda^p\equiv{}^{\sigma}\lambda \bmod \mathfrak{p}$$

を得る．また，$\mathfrak{p}$ は不分岐だから，命題 4.1.1(の一般化) が適用でき，

$$\frac{\lambda^{np}}{n}\equiv\frac{{}^{\sigma}\lambda^{n}}{n} \bmod \mathfrak{p}$$

が成り立つ．よって，$\lambda\in\mathcal{O}^*$ と (4.17) より，

$$(p-{}^{\sigma}\lambda\lambda^{-1}T)*f\equiv 0 \bmod \mathfrak{p}$$

が従う． □

注意 4.5.3. λ を $\mathfrak{p}$ の元とする．$\mathrm{ord}_{\mathfrak{p}}(p)<p$ ならば，$x+y-\lambda xy$ は特殊元 π に属する．すなわち，$x+y-\lambda xy$ は $\hat{\mathbb{G}}_a(x,y)$ と強同型である．実際，$n=mp^{\nu}$，ただし，$\nu\geq 0$, $(m,p)=1$ とおくとき，

$$\mathrm{ord}_{\mathfrak{p}}\left(\pi\frac{\lambda^{np-1}}{np}\right)>1+p^{\nu+1}-1-(\nu+1)p\geq 0$$

が成り立つので，

$$\pi*f=\pi\sum_{n\geq 1}\frac{\lambda^{n-1}}{n}x^n\equiv\pi\sum_{n\geq 1}\frac{\lambda^{np-1}}{np}x^{np}\equiv 0 \bmod \mathfrak{p}$$

である．

第5章　形式群の本田理論(応用)

この章では，本田理論の応用例を 3 つ述べます.

5.1　平方剰余の相互法則

この節では，平方剰余の相互法則を証明します．証明は，本田 [11] によるもので，形式群を用います.

q を奇素数，$\zeta = \zeta_q$ を 1 の原始 q 乗根とする．$\chi(n) = (\frac{n}{q})$ を Legendre symbol とし，

$$S := \sum_{n=1}^{q-1} \chi(n)\zeta^n : \text{ Gauss 和}$$

とおく．このとき，

$$S^2 = \chi(-1)q =: q^*, \qquad \sum_{n=1}^{q-1} \chi(n)\zeta^{nm} = \chi(m)S$$

が成立する (cf. e.g. [14]).

$k := \mathbb{Q}(\sqrt{q^*})$，$\mathcal{O}_k$ をその整数環とし，$\langle\sigma\rangle = \mathrm{Gal}(k/\mathbb{Q})$ おく.

$$g(x) := \sum_{n\geq 1} \chi(n)\frac{x^n}{n}, \qquad G(x,y) := g^{-1}(g(x)+g(y))$$

とおく．定理 3.2.2 により，$G(x,y)$ は $\mathbb{Z}$ 上の形式群である．また，

$$H(x,y) := x + y + Sxy$$

とおく．$H(x,y)$ は $\mathcal{O}_k$ 上の形式群である．命題 2.3.2，定理 2.4.1(証明) により，$H(x,y)$ の不変微分，変換子 $h(x)$ は，それぞれ，

$$\frac{dx}{1+Sx}, \qquad h(x) = \sum_{n\geq 1} \frac{(-S)^{n-1}}{n} x^n$$

で与えられる.

命題 5.1.1. $G(x,y)$ と $H(x,y)$ は $\mathcal{O}_k$ 上で強同型である.

[**証明**]

$$P(x) := \prod_{1\le a\le q-1,\chi(a)=1} (1-\zeta^a x), \qquad Q(x) := \prod_{1\le b\le q-1,\chi(b)=-1} (1-\zeta^b x)$$

とおく.

$$P(x),\ Q(x) \in \mathcal{O}_k[x], \qquad {}^{\sigma}P = Q,\ {}^{\sigma}Q = P \tag{5.1}$$

が成立する.

$$\varphi(x) := \frac{Q(x)-P(x)}{SP(x)}$$

とおく. $\varphi(x)$ が $G(x,y)$ から $H(x,y)$ への $\mathcal{O}_k$ 上の強同型であることを示す.

(5.1) より,

$${}^{\sigma}(Q(x)-P(x)) = -(P(x)-Q(x))$$

が成立する. $S = \pm\sqrt{q^*}$ より,

$$\frac{Q(x)-P(x)}{S} \in \mathbb{Z}[x]$$

が成立する. $P(x) \in \mathcal{O}_k[[x]]^*$ より,

$$\varphi(x) \in \mathcal{O}_k[[x]] \tag{5.2}$$

が成り立つ. さらに,

$$\varphi(x) \equiv \frac{-\sum \zeta^b x + \sum \zeta^a x}{S} \equiv \frac{\sum \chi(n)\zeta^n x}{S} \equiv x \bmod \deg 2 \tag{5.3}$$

が成立する. また,

$$\begin{aligned}
\varphi'(x) &= \frac{Q}{SP}\left(\log\frac{Q}{P}\right)' = \frac{Q}{SP}\left(\sum_b \frac{-\zeta^b}{1-\zeta^b x} - \sum_a \frac{-\zeta^a}{1-\zeta^a x}\right) \\
&= \frac{Q}{SP}\sum_{n=1}^{q-1}\frac{\chi(n)\zeta^n}{1-\zeta^n x} = \frac{Q}{SP}\sum_{n=1}^{q-1}\sum_{m\ge 1}\chi(n)\zeta^n\zeta^{n(m-1)}x^{m-1} \\
&= \frac{Q}{SP}\sum_{m\ge 1}\sum_{n=1}^{q-1}\chi(n)\zeta^{nm}x^{m-1} = \frac{Q}{P}\sum_{m\ge 1}\chi(m)x^{m-1}
\end{aligned}$$

だから,

$$\frac{d\varphi}{1+S\varphi} = \frac{\frac{Q}{P}\sum\chi(m)x^{m-1}dx}{1+S\frac{Q-P}{SP}} = \sum_{m\ge 1}\chi(m)x^{m-1}dx$$

を得る. よって, 命題 2.4.4(iii) により, φ は $G(x,y)$ から $H(x,y)$ への準同型である.

以上により, $\varphi(x)$ は形式群 $G(x,y)$ から $H(x,y)$ への $\mathcal{O}_k$ 上の強同型であることが示された. □

系 5.1.2 (平方剰余の相互法則). 任意の奇素数 p に対し,

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$$

が成り立つ.

[**証明**] $g(x) = (h \circ \varphi)(x)$ より,

$$\sum_{m\geq 1} \frac{\chi(m)}{m} x^m = \sum_{m\geq 1} (-S)^{m-1} \frac{\varphi^m}{m}$$

である. よって,

$$p \sum_{m=1}^{p} \frac{\chi(m)}{m} x^m = p \sum_{m=1}^{p} (-S)^{m-1} \frac{\varphi^m}{m} \bmod \deg p+1,\ \bmod p$$

となる. $m < p$ で m は p と素だから,

$$\chi(p) x^p \equiv (q^*)^{\frac{p-1}{2}} x^p \bmod \deg p+1,\ \bmod p$$

が成立する. よって, Euler の規準より,

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$$

が成り立つ. □

注意 5.1.3. 平方剰余の相互法則と $\mathfrak{p}$-進整数環上の本田理論を用いると, 命題 5.1.1 は次の様に証明できる.

p を素数, $\mathfrak{p}$ を p の上にある k の素イデアルとし, $\mathcal{O}_\mathfrak{p}$ を $\mathcal{O}_k$ の $\mathfrak{p}$-進完備化, $\sigma_\mathfrak{p}$ を $\mathfrak{p}$ に対するフロベニウス自己準同型とおく. $\mathfrak{p}$ が不分岐ならば, 命題 4.5.2 により, $\mathcal{O}_\mathfrak{p}$ 上の形式群 $H(x,y)$ は特殊元 $p - {}^{\sigma_\mathfrak{p}}SS^{-1}T = p - (\frac{q^*}{p})T$ に属する. 平方剰余の相互法則を用いてまとめると, $H(x,y)$ は特殊元 $p - \chi(p)T$ に属する. よって, $G(x,y)$ と $\mathcal{O}_\mathfrak{p}$ 上で強同型である.

また, $\mathfrak{p}$ が分岐のときには, 注意 4.5.3 により, $H(x,y)$ は特殊元 π に属する. ただし, π は $\mathfrak{p}$ の素元である. 一方, $G(x,y)$ の変換子 $g(x)$ の x^n 係数は n が p の倍数であるとき 0 となるので, $G(x,y)$ も特殊元 π に属する. よって, $G(x,y)$ と $H(x,y)$ は $\mathcal{O}_\mathfrak{p}$ 上で強同型となる.

以上により, $G(x,y)$ と $H(x,y)$ は $\mathcal{O}_k$ 上で強同型となることが示された.

5.2 楕円曲線の形式群

この節では，$\mathbb{Q}$ 上定義された楕円曲線の形式群に関する本田 [10] の結果を紹介します．本田氏は最初，本田 [9] において supersingular prime に関する仮定の下で結果を得ていましたが，[10] において仮定を外しています．

本田の定理は，Deninger-Nart により実数乗法を持つ GL_2-type の abel 多様体の場合に高次元化され，さらに筆者により building block の場合に定義体に関しても一般化されています．この節の後半で，筆者の結果を，1 次元 building block，すなわち，$\mathbb{Q}$-曲線に限定して説明します．

k を $\mathbb{Q}$ 上の Galois 拡大とし，E を k 上定義された虚数乗法を持たない楕円曲線とする．

定義 5.2.1. 楕円曲線 E が，k 上定義された **$\mathbb{Q}$-曲線**であるとは，$G_{\mathbb{Q}}$ の任意の元 σ に対し，k 上定義された ${}^{\sigma}E$ から E への零射でない同種写像が存在することをいう．[1]

$\mathbb{Q}$ 上の楕円曲線は $\mathbb{Q}$-曲線である．

E を $\mathcal{O}_k$ 係数の Weierstrass モデル

$$E:\ Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \tag{5.4}$$

で定義された楕円曲線とする．不変微分 $\omega_E := dX/(2Y + A_1X + A_3)$ を

$$\omega_E = \sum b_n z^{n-1} dz, \qquad z := -\frac{X}{Y}$$

と零点における局所変数 z で展開する．このとき，

$$b_1 = 1, \qquad b_n \in \mathcal{O}_k \quad ({}^{\forall}n \geq 1)$$

が成立する．

$$f(x) = \sum_{n\geq 1} \frac{b_n}{n} x^n, \qquad \hat{E}(x,y) := f^{-1}(f(x) + f(y))$$

とおくとき，$\hat{E}(x,y)$ は $\mathcal{O}_k$ 上の形式群になる．

[1] 正確には $\mathbb{Q}$-curve completely defined over k といいます．

$k=\mathbb{Q}$ とし，E は $\mathbb{Z}$ 上の極小モデルであると仮定する．

$$L(E/\mathbb{Q},s)=\prod_p \frac{1}{1-a_p p^{-s}+\varepsilon_p p^{1-2s}}=\sum_{n\geq 1}\frac{a_n}{n^s}$$

を E 上の l-進表現に付随する L-関数とする．このとき，

$$a_1=1, \qquad a_n\in\mathbb{Z} \quad (^\forall n\geq 1)$$

が l のとり方によらず成立し，p が E の good prime か bad prime かに応じて，$\varepsilon_p=1$ または $\varepsilon_p=0$ となる．

$$g(x):=\sum_{n\geq 1}\frac{a_n}{n}x^n, \qquad \hat{L}(x,y):=g^{-1}(g(x)+g(y))$$

とおく．

定理 5.2.2 (本田 [10]). $\hat{L}(x,y)$ は $\mathbb{Z}$ 上定義された形式群である．また，$\hat{L}(x,y)$ と $\hat{E}(x,y)$ は $\mathbb{Z}$ 上強同型である．

[**証明**] 命題 3.2.2 より，$\mathbb{Q}_p$ 上の形式群 $\hat{L}(x,y)$ は特殊元 $p-a_pT+\varepsilon_pT^2$ に属する．とくに，$\hat{L}(x,y)$ は $\mathbb{Z}$ 上定義される．

p が good prime であるとき，E の p を法とする reduction 上の Frobenius の自己準同型 π_p が

$$p-a_p\pi_p+\pi_p^2=0$$

を満たすので，

$$f^{-1}(pf(x)-a_pf(x^p)+f(x^{p^2}))\equiv 0 \bmod p$$

が成り立つ．さらに，命題 4.4.2 により，

$$pf(x)-a_pf(x^p)+f(x^{p^2})\equiv 0 \bmod p$$

を得る．よって，$\mathbb{Z}_p$ 上の形式群 $\hat{E}(x,y)$ は特殊元 $p-a_pT+T^2$ に属する．

p が bad prime であるとき，reduction の型に応じて，

$$\hat{E} \bmod p \cong_{\mathbb{F}_p} \hat{\mathbb{G}}_a \quad (p\text{: additive}),$$
$$\hat{E} \bmod p \cong_{\mathbb{F}_p} \hat{\mathbb{G}}_m \quad (p\text{: split multiplicative}),$$
$$\hat{E} \bmod p \ncong_{\mathbb{F}_p} \hat{\mathbb{G}}_m,\ \hat{E} \bmod p \cong_{\mathbb{F}_{p^2}} \hat{\mathbb{G}}_m \quad (p\text{: non split multiplicative})$$

が成立する．これより，$\mathbb{Z}_p$ 上の形式群 $\hat{E}(x,y)$ は，それぞれ，特殊元 p，$p-T$，$p+T$ に属する．a_p, ε_p の定義より，p が bad prime のとき，$\hat{E}(x,y)$ は特殊元 $p-a_pT+\varepsilon_pT^2$ に属する．

以上により，任意の p に対し，$\mathbb{Z}_p$ 上の形式群 $\hat{L}(x,y)$ と $\hat{E}(x,y)$ は同じ特殊元 $p-a_pT+\varepsilon_pT^2$ に属する．よって，命題が成立する． □

$(p-a_pT+\varepsilon_pT^2)*f(x)\equiv 0 \bmod p$ の x^p の項に着目して次を得る．

系 5.2.3. 任意の素数 p に対し，$a_p \equiv b_p \bmod p$ が成立する．

注意 5.2.4. Hasse-Weil の不等式 : $|a_p| \leq 2\sqrt{p}$ より，$p \geq 17$ ならば,

$$a_p = b_p \text{ の } p \text{ を法とする絶対値最小の剰余}$$

が成り立つ.

注意 5.2.5. $\varphi(x)$ を $\hat{L}(x,y)$ から $\hat{E}(x,y)$ への $\mathbb{Z}$ 上の強同型とする．このとき，命題 2.4.4(iii) により,

$$\varphi^*\left(\sum_{n\geq 1} b_n z^{n-1}dz\right) = \sum_{n\geq 1} a_n z^{n-1}dz$$

が成り立つ.

次に筆者による本田の定理の一般化を紹介する．k を $\mathbb{Q}$ 上の有限次 abel 拡大とする．簡単のため，E の Weierstrass model は $\mathcal{O}_k$ 上極小であると仮定する．

$$c(\sigma,\tau) := \phi_\sigma{}^\sigma\phi_\tau\phi_{\sigma\tau}^{-1} \quad ({}^\forall\sigma,\tau \in G_{\mathbb{Q}})$$

とおく．c は $\mathbb{Q}^*$ に値を持つ 2-cocycle となる．2-cocycle c は symmetric であると仮定する．このとき，$G_{\mathbb{Q}}$ から $\mathbb{Q}^*$ への写像 β が存在し,

$$c(\sigma,\tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$$

が成り立つ．$F := \mathbb{Q}(\beta)$ を $\mathbb{Q}$ に $\beta(\sigma)$ の値をすべて添加した体とする．$d := [F:\mathbb{Q}]$ とおく．このとき，Pyle [19] により，次を満たす GL_2-type の abel 多様体 A と，A から B^d への零射でない同種写像 κ が存在し,

$$\mathrm{End}_{\mathbb{Q}}(A) \cong F, \qquad \begin{array}{ccc} A & \xrightarrow{\beta(\sigma)} & A \\ {\scriptstyle\sigma\kappa}\downarrow & & \downarrow{\scriptstyle\kappa} \\ {}^\sigma B^d & \xrightarrow{\prod\phi_\sigma} & B^d \end{array}$$

を満たす．$L(A/\mathbb{Q},s) = \sum_{n\geq 1} a_n n^{-s}$ を λ-進表現の L-関数とする．a_n は λ のとり方によらず,

$$a_1 = 1,\ a_n \in \mathcal{O}_F \quad ({}^\forall n \geq 1)$$

が成立する.

自然数 n に対し，$\mathrm{Gal}(k/\mathbb{Q})$ の元 σ_n を，n が素数 p のときには Frobenius 自己同型で，n が合成数のときには関係式 $\sigma_{n_1n_2} = \sigma_{n_1}\sigma_{n_2}$ により定義する．このとき，

$$a_n\beta(\sigma_n) \in \mathbb{Z}$$

が成立する．

$\varphi \in \mathrm{Hom}_k({}^{\sigma}E, E)$ に対し，

$$\varphi^*\omega_E = \alpha(\varphi)^{\sigma}\omega_E$$

により，$\alpha(\varphi) \in k$ を定義する．

以上の記号の準備の下，$\mathbb{Q}$-曲線 E の L-関数を

$$L(E/k, s) := \sum_{n\geq 1} \frac{a_n \beta(\sigma_n)}{\deg\, \phi_\sigma} \alpha(\phi_{\sigma_n}) n^{-s}$$

により定義する．$L(E/k, s)$ は ϕ_σ，β，A のとり方によらず k-係数となる．このとき，判別式 D_k，E の bad prime，$\deg\, \phi_\sigma$ により定まる k の素イデアルの有限集合 S が存在[2] して，以下が成立する．

定理 5.2.6 (S. [21]). $\hat{L}(x, y)$ は $\mathcal{O}_{K,S}$ 定義された形式群となる．また，$\hat{L}(x, y)$ と $\hat{E}(x, y)$ とは $\mathcal{O}_{k,S}$ 上強同型である．ただし，$\mathcal{O}_{K,S}$ は S-整数のなす環である．

5.3 Kummer 合同式

大西-安田により，Bernoulli 数や Hurwitz 数の Kummer 合同式が一般化されました (定理 5.3.4)．定理の証明には，形式群が用いられています．この節では，形式群に付随するある Hurwitz 級数の Kummer 合同式について，Snyder の結果，Bernoulli 数の Kummer 合同式，大西-安田の結果の順に，簡単に述べたいと思います．この節の内容，とくに命題の証明の方針は，大西 [18] に従っています．

$$\mathbb{Z}_p\langle\langle x\rangle\rangle := \left\{ \sum_{n\geq 0} \frac{a_n}{n!} x^n \;\middle|\; a_n \in \mathbb{Z}_p \right\}$$

とおく．$\mathbb{Z}_p\langle\langle x\rangle\rangle$ は $\mathbb{Q}_p[[x]]$ の部分環になり，$\mathbb{Z}_p\langle\langle x\rangle\rangle$ の元を Hurwitz 整級数と呼ぶ．e^x，$\log(1-x)$，$\tan x$，$\sin x$ 等はすべて Hurwitz 整級数となる．また，Hurwitz 整級数 $h(x)$ が可逆であるとき，$h^{-1}(x)$ も Hurwitz 整級数となる．

$F(x, y)$ を $\mathbb{Z}_p$ 上の形式群，$z = f(x) = \sum_{n\geq 1} a_n x^n/n$ を $F(x, y)$ の変換子，$x = f^{-1}(z) = \sum_{n\geq 1} b_n x^n/n!$ とおく．

[2] 判別式 D_k，E の bad prime，$\deg\, \phi_\sigma$ を割る素イデアルとその $\mathbb{Q}$ 上共役な素イデアルをすべて含むようにとればよい．

命題 5.3.1 (Snyder[23]). 自然数 r と n，ただし $n \geq r$，について，

$$\sum_{j=0}^{r}(-1)^{r-j}\binom{r}{j}a_p^{r-j}b_{n+j(p-1)} \equiv 0 \bmod p^r\mathbb{Z}_p$$

が成り立つ．

[**証明**] 1 $\dfrac{d^p z}{dx^p} + a_p\left(\dfrac{dz}{dx}\right)^p \equiv 0 \bmod p$ を示す．

$F(x,y)$ は $\mathbb{Z}_p$ 上の形式群だから，定理 3.1.5 により，特殊元 $p + \sum_{\nu\geq 1} c_\nu T^\nu$ が存在し，

$$pf(x) + \sum_{\nu\geq 1} c_\nu f(x^{p^\nu}) = p\psi(x) \quad ({}^{\exists}\psi(x) \in \mathbb{Z}_p[[x]])$$

が成り立つ．両辺を微分して，

$$pf'(x) + \sum_{\nu\geq 1} c_\nu f'(x^{p^\nu})p^\nu x^{p^\nu-1} = p\psi'(x)$$

となる．p で割って，

$$f'(x) + \sum_{\nu\geq 1} c_\nu f'(x^{p^\nu})p^{\nu-1}x^{p^\nu-1} = \psi'(x),$$

$$f'(x) + c_1 f'(x^p)x^{p-1} \equiv \psi'(x) \bmod p$$

を得る．両辺を $(p-1)$ 回微分して，

$$f^{(p)}(x) + c_1 f'(x^p)(p-1)! \equiv \psi^{(p)}(x) \bmod p$$

が成立する．$c_1 \equiv -a_p \bmod p$，$(p-1)! \equiv -1 \bmod p$，$f'(x) \in \mathbb{Z}_p[[x]]$，$\psi^{(p)}(x) \equiv 0 \bmod p$ より，

$$f^{(p)}(x) + a_p(f'(x))^p \equiv \psi^{(p)}(x) \bmod p$$

が成立する．

2 $\dfrac{d}{dz}$ が $\mathbb{Z}_p[[x]]$ 上の $\mathbb{Z}_p$-導分であることを示す．

$\dfrac{dx}{dz} = \left(\dfrac{dz}{dx}\right)^{-1}$，$\dfrac{dz}{dx} \in \mathbb{Z}_p[[x]]$，$\dfrac{dz}{dx}(0) = 1$ より，$\dfrac{dz}{dx} \in \mathbb{Z}_p[[x]]^*$．

3 任意の $\varphi(x) \in \mathbb{Z}_p[[x]]$ に対し，$\dfrac{d^p\varphi}{dz^p} - a_p\dfrac{d\varphi}{dz} \in p\mathbb{Z}_p[[x]]$ を示す．

R を標数 p の可換環，D を R 上の導分とする．このとき，

$$\text{Hochschild の公式}: \ (bD)^p = b^pD^p + ((bD)^{p-1}(b))\cdot D \quad ({}^{\forall}b \in R)$$

が成立する (cf. e.g. [17] p.240)．この公式を用いる．

$$\begin{aligned} 0 &\equiv \left(\frac{d}{dx}\right)^p \varphi \bmod p \\ &\equiv \left(\frac{dz}{dx}\frac{d}{dz}\right)^p \varphi \bmod p \end{aligned}$$

に対し，$b = \dfrac{dz}{dx}$，$D = \dfrac{d}{dz}$ とおいて，Hochschild の公式に代入すると，

$$\begin{aligned} 0 &\equiv \left(\frac{dz}{dx}\right)^p \frac{d^p\varphi}{dz^p} + \left(\frac{dz}{dx}\frac{d}{dz}\right)^{p-1} \frac{dz}{dx} \cdot \frac{d\varphi}{dz} \\ &\equiv \left(\frac{dz}{dx}\right)^p \frac{d^p\varphi}{dz^p} + \frac{d^pz}{dx^p}\frac{d\varphi}{dz} \bmod p \end{aligned}$$

を得る．ゆえに，

$$\frac{d^p\varphi}{dz^p} + \left(\frac{dz}{dx}\right)^{-p} \frac{d^pz}{dx^p}\frac{d\varphi}{dz} \equiv 0 \bmod p$$

が成り立つ．よって，$\boxed{1}$ より，

$$\frac{d^p\varphi}{dz^p} - a_p\frac{d\varphi}{dz} \equiv 0 \bmod p$$

が成立する．

$\boxed{4}$ $\Omega_p := \dfrac{d^p}{dz^p} - a_p\dfrac{d}{dz}$ とおく．このとき，$\boxed{3}$ より，

$$\Omega_p^r(x) \in p^r\mathbb{Z}_p[[x]] \subset p^r\mathbb{Z}_p\langle\langle z\rangle\rangle,$$

$$\Omega_p^r(x) = \Omega_p^r\left(\sum_{n\geq 1}\frac{b_n}{n!}z^n\right) = \sum_{n\geq r}\left(\sum_{j=0}^{r}(-1)^{r-j}\binom{r}{j}a_p^{r-j}b_{n+j(p-1)}\right)\frac{z^{n-r}}{(n-r)!}$$

が成り立つ．したがって，命題 5.3.1 が成立する． □

例 5.3.2. $F_t(x,y) := (x+y)/(1-xy)$ とおく．このとき，$F_t(x,y)$ の変換子は

$$z = \arctan x = \sum_{n\geq 0}\frac{(-1)^n}{2n+1}x^{2n+1}$$

であり，

$$x = \tan z = \sum_{n\geq 1}(-1)^{n-1}2^{2n}(2^{2n}-1)\frac{B_{2n}}{2n}\frac{z^{2n-1}}{(2n-1)!},$$ ただし，B_{2n} は Bernoulli 数，

が成立する．だから，命題 5.3.1 により $(-1)^{n-1}2^{2n}(2^{2n}-1)B_{2n}/2n$ に関する合同式が得られる．

命題 5.3.3 (Kummer 合同式). p を奇素数とする．自然数 r と n，ただし $2n-2 \geq r$，について，$(p-1)\nmid 2n$ のとき，

$$\sum_{j=0}^{r}(-1)^{r-j}\binom{r}{j}\frac{B_{2n+j(p-1)}}{2n+j(p-1)} \equiv 0 \bmod p$$

が成り立つ．

[**証明**] $F_s(x,y) := x\sqrt{1-y^2}+y\sqrt{1-x^2}$ とおく．$F_s(x,y)$ は $\mathbb{Z}[2^{-1}]$ 上の形式群となる．また，$F_s(x,y)/\mathbb{Z}_p$ は特殊元 $p-(-1)^{\frac{p-1}{2}}T$ に属する．このとき，$F_s(x,y)$ の変換子は

$$z = f(x) = \sum_{n\geq 1}\frac{a_n}{n}x^n = \arcsin x$$

である．

$\zeta \in \mathbb{Z}_p$ を 1 の原始 $(p-1)$-乗根とする．このとき，

$$\sin(\zeta \arcsin(x)) = f^{-1}(\zeta f(x)) = [\zeta]_{F_s}(x) \in \mathrm{End}_{\mathbb{Z}_p}(F_s).$$

よって，

$$\frac{1}{\sin^2 z}-\frac{\zeta^2}{\sin^2(\zeta z)} = \frac{1}{x^2}-\frac{\zeta^2}{\zeta^2x^2+\cdots} = \frac{1}{x^2}-\frac{1}{x^2}(1+\cdots) \in \mathbb{Z}_p[[x]] \subset \mathbb{Z}_p\langle\langle z\rangle\rangle.$$

$\gamma_p := (-1)^{\frac{p-1}{2}}2^{p-1}$，$\Omega_p := \dfrac{d^p}{dz^p}-\gamma_p\dfrac{d}{dz}$ とおく．$\gamma_p \equiv a_p \bmod p$ に注意する．命題 5.3.1 の証明 3 により，

$$\Omega_p^r\left(\frac{1}{\sin^2 z}-\frac{\zeta^2}{\sin^2(\zeta z)}\right) \in p^r\mathbb{Z}_p[[x]] \subset p^r\mathbb{Z}_p\langle\langle z\rangle\rangle \tag{5.5}$$

が成り立つ．一方，

$$\begin{aligned}\frac{1}{\sin^2 z}-\frac{\zeta^2}{\sin^2(\zeta z)} &= \sum_{n\geq 1}(-1)^{n-1}2^{2n}\frac{B_{2n}}{2n}\frac{z^{2n-2}}{(2n-2)!}-\sum_{n\geq 1}(-1)^{n-1}2^{2n}\frac{B_{2n}}{2n}\frac{\zeta^{2n}z^{2n-2}}{(2n-2)!}\\ &= \sum_{n\geq 1}(-1)^{n-1}2^{2n}(1-\zeta^{2n})\frac{B_{2n}}{2n}\frac{z^{2n-2}}{(2n-2)!} \in \mathbb{Z}_p\langle\langle z\rangle\rangle.\end{aligned}$$

よって，(5.5) より，

$$\sum_{j=0}^{r}(-1)^{r-j}\binom{r}{j}\gamma_p^{r-j}(-1)^{n-1+j\frac{p-1}{2}}2^{2n+j(p-1)}(1-\zeta^{2n+j(p-1)})\frac{B_{2n+j(p-1)}}{2n+j(p-1)} \equiv 0 \bmod p^r\mathbb{Z}_p,$$

$$(-1)^{n-1+r\frac{p-1}{2}}2^{2n+r(p-1)}(1-\zeta^{2n})\sum_{j=0}^{r}(-1)^{r-j}\binom{r}{j}\frac{B_{2n+j(p-1)}}{2n+j(p-1)} \equiv 0 \bmod p^r\mathbb{Z}_p,$$

ただし，$2n-2 \geq r$，を得る．$(p-1)\nmid 2n$ のとき，$1-\zeta^{2n} \neq 0$ だから，

$$\sum_{j=0}^{r}(-1)^{r-j}\binom{r}{j}\frac{B_{2n+j(p-1)}}{2n+j(p-1)} \equiv 0 \bmod p^r\mathbb{Z}_p \quad (2n-2\geq r)$$

が成立する． □

C を

$$C:\ v^2 = u^{2g+1} - 1$$

で定義された種数 g の $\mathbb{Q}$ 上の超楕円曲線とする．無限遠点における局所変数 z を

$$dz = u^{g-1}\frac{du}{2v}$$

を満たすようにとる．このとき，u，v の Laurant 展開は

$$u = \frac{1}{z^2} + \sum_{\substack{n\geq 2\\ (4g+2)|n}} \frac{C_n}{n}\frac{z^{n-2}}{(n-2)!},\quad v = \frac{-1}{z^{2g+1}} + \sum_{\substack{n\geq 2\\ (4g+2)|n}} \frac{D_n}{n}\frac{z^{n-2}}{(n-2)!}$$

とおける．

定理 5.3.4 (Ônishi-Yasuda). 素数 $p \equiv 1 \bmod (2g+1)$ と自然数 r と n，ただし $(4g+2)n - 2 \geq r$，について，$(p-1) \nmid (4g+2)n$ ならば，

$$\sum_{j=0}^{r} \binom{r}{j} (-A_p)^{r-j} \cdot \frac{C_{(4g+2)n+j(p-1)}}{(4g+2)n + j(p-1)} \equiv 0 \bmod p^r\mathbb{Z}_p,$$
$$\sum_{j=0}^{r} \binom{r}{j} (-A_p)^{r-j} \cdot \frac{D_{(4g+2)n+j(p-1)}}{(4g+2)n + j(p-1)} \equiv 0 \bmod p^r\mathbb{Z}_p$$

が成り立つ．ただし，

$$A_p = (-1)^{(p-1)/(4g+2)} \cdot \binom{(p-1)/2}{(p-1)/(4g+2)}.$$

証明は

$$x = \frac{1}{\sqrt{u}} = z + \cdots$$

の逆関数を $z = f(x)$ とおくとき，$f(x)$ を変換子とする形式群 $F(x,y)$ が $\mathbb{Z}_p$ 上定義されることを示した後，命題 5.3.3 と同様にしてなされる．

とくに，$g = 0$ のとき，$u = \dfrac{1}{\sin^2 z}$，$v = -\cot z$，$x = \sin z$ となり，定理 5.3.4 は命題 5.3.3 の一般化である．

また，超楕円曲線 $v^2 = u^{2g+1} - u$ の場合にも同様の合同式が得られている．

関連図書

[1] 荒川恒男-伊吹山知義-金子昌信, 'ベルヌーイ数とゼータ関数', 牧野書店, 2001.

[2] N. Childress and D. Grant, 'Formal groups of twisted multiplicative groups and L-series', *Proc. Symp. in Pure Math.* 58 (1995) 89-102.

[3] N. Childress and J. Stopple, 'Formal groups and Dirichlet L-functions, I and II', *J. Number Theory* 41 (1992), I 283-294, II 295-302.

[4] R. F. Coleman and F. O. McGuiness, 'Rational formal group laws', *Pacific J. Math.* 147 (1991) 25-27.

[5] C. Deninger and E. Nart, 'Formal groups and L-series', *Comment. Math. Helv.* 65 (1990) 318-333.

[6] E. J. Ditters, 'On the classification of commutative formal group laws over p-Hilbert domains and a finiteness theorem for higher Hasse-Witt matrices', *Math. Z.* 202 (1989) 83-109.

[7] D. Grant, 'A proof of quintic reciprocity using the arithmetic of $y^2 = x^5 + 1/4$', *Acta Arithmetica* 75 (1996) 321-327.

[8] W. L. Hill, 'Formal groups and zeta-functions of elliptic curves', *Invent. Math.* 12 (1971) 321-336.

[9] T. Honda, 'Formal groups and zeta-functions', *Osaka J. Math.* 5 (1968) 199-213.

[10] T. Honda, 'On the theory of commutative formal groups', *J. Math. Soc. Japan* 22 (1970) 213-246.

[11] T. Honda, 'Invariant Differentials and L-functions –Reciplocity law for quadratic fields and elliptic curves over $\mathbb{Q}$', *Rend. Sem. Mat. Univ. Padova* 49 (1973) 323-335.

[12] 本田平, '可換形式群について', 数学 205-213.

[13] N. M. Katz, 'Formal groups and p-adic interpolation', *Astérisque* 41-42 (1977) 55-65.

[14] S. Lang, 'Algebraic number theory', Springer GTM 110.

[15] J. Lubin, 'One-parameter formal Lie groups over $\mathfrak{p}$-adic integer ring', *Ann. of Math.* 80 (1964) 464-484.

[16] J. Lubin and J. Tate, 'Formal complex multiplication in local fields', *Ann. of Math.* 81 (1965) 380-387.

[17] 松村英之, '可換環論', 共立出版, 1980.

[18] Y. Ônishi, 'Theory of generalized Bernoulli-Hurwitz numbers for algebraic functions of cyclotomic type and universal Bernoulli numbers', preprint, http://jinsha2.hss.iwate-u.ac.jp/~onishi/

[19] E. E. Pyle, 'Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$', *Modular curves and abelian varieties*, (eds J. Cremona, J. -C. Lario, J. Quer and K. Ribet), Progress in Mathematics 224, Birkhäuser, 2004. 189-239.

[20] F. Sairaiji, 'Formal groups of certain $\mathbb{Q}$-curves over quadratic fields', *Osaka J. Math.* 39 (2002) 223-243.

[21] F. Sairaiji, 'Formal groups of building blocks completely defined over finite abelian extensions of $\mathbb{Q}$', to appear in *Bull. London Math. Soc.*.

[22] C. Snyder, 'A concept of Bernoulli numbers in algebraic function fields (II)', *Manuscripta Math.* 35 (1981) 69-89.

[23] C. Snyder, 'Kummer congruences in formal groups and algebraic groups of dimension one', *Rocky Mountain J.* 15 (1985) 1-11.

[24] A. Weil, 'On algebraic groups of transformations', *Amer. J. Math.* 77 (1955) 355-391.