数理解析研究所講究録
222巻 1974年 71-81

p-進整数環上の Honda group $H_{n,m}$ の自己準同形環について

阪大理　大学院　　山崎　洋平

§0. 序

"formal group" は J. Dieudonné によって導入された概念で、Abel 多様体との関連も深い。彼は [1] ~ [8] に於て、標数 $p > 0$ の代数的閉体（本質的には完全体）上の commutative formal group の理論を展開し、それらの間の準同形群を、k の Witt 環を用いて表わした。また、単純群 $G_{n,0,m}$ を発見し、isogenie による分解定理を得た。

この $k \leftarrow W(k)$ の構図は T. Honda により

discrete valuation ring :	R	$ch = 0$
	$\downarrow$	
residue field :	k	$ch = p$
$\sigma \in \mathrm{End}\, R$		s.t
q : p 巾 } 共に固定		$\alpha^{\sigma} \equiv \alpha^{q} \mod \pi$
π : R の素元 }		$\forall \alpha \in R$

と、とらえ直された。

Honda は、この構図により、"special element" が R 上の commutative formal group を与えること、及び、$q = p$, $\nu_{\pi}(p) = 1$ のとき、それらが R 上のすべての commutative formal group を、また、その reduction がすべての k 上の commutative formal group を表し尽くすことを示し、R 上の準同形についていくつかの結果を得た。

本稿では $G_{n,0,m}$ を R 上に持ち上げた群 $H_{n,m}$ の自己準同形環の決定を紹介する。詳しくは、Yamasaki [10] を見られたい。

§1，定義

R を、1 をもつ可換環．$\mathbb{X}, \mathbb{Y}, \mathbb{Z}$ を長さ n の変数縦ベクトル．$R[[\quad]]$ を与えられた変数 (vector) に関する R 上の巾級数環．$I = R[[\quad]]_0$ を定数項が 0 なる元からなる ideal．また $R[[\quad]]_0^n$ を、I の元を成分とする長さ n の縦ベクトルの全体とする。

Definition. R 上の n 次元 formal group law とは、$R[[\mathbb{X}, \mathbb{Y}]]_0^n$ の元 F であって次の (1)、(2) をみたすものをいう。

(1) $F(\mathbb{X}, \mathbb{Y}) \equiv \mathbb{X} + \mathbb{Y} \mod \deg 2$ 即ち $\mod I^2$

(2) $F(F(\mathbb{X}, \mathbb{Y}), \mathbb{Z}) = F(\mathbb{X}, F(\mathbb{Y}, \mathbb{Z}))$

更に (3) $F(\mathbb{X}, \mathbb{Y}) = F(\mathbb{Y}, \mathbb{X})$

であるとき F は commutative であるという。

Ω を長さ n の変数縦ベクトルの、十分大きな集合とするとき、F は、$R[[\Omega]]_0^n$ に群構造を与える。これを formal group というが、以下簡単に、F を formal group と呼ぶ。本稿では特に commutative なものを扱う。従って、以下使用する "formal group" は "commutative formal group law" を表わす。(略称 f.g を用いることも断っておく)

Definition. $\varphi \in R[[X]]_0^{n'}$ が n 次元 f.g F から n' 次元 f.g G への homomorphism であるとは

$$\varphi \circ F(X, Y) = G(\varphi(X), \varphi(Y))$$

をみたすことをいう。

Definition. $n' = n$ で、φ が可逆なとき isomorphism という。特に

$$\varphi(X) \equiv X \quad \text{mod deg } 2$$

のとき strong isomorphism という。

Example 1. $F_i(X, Y) = X_i + Y_i - a_i X_i Y_i \qquad a_i \in R$

特に、 $\forall a_i = 0$ のとき additive

$\forall a_i = 1$ のとき multiplicative

という。

Example 2. F を f.g

$f \in R[[X]]_0^n$ を $f(X) \equiv PX \mod \deg 2$

とする。(但し $P \in GL(n,R)$)

$$G(X,Y) = f^{-1}(F(f(X), f(Y)))$$

は F に isomorphic (特に $P = I_n$ のとき strongly isomorphic) な f.g を与える。

Theorem (Honda). R が $\mathbb{Q}$ - algebra のとき、すべての f.g は additive group に同形である。

以下、R を $ch=0$ の discrete valuation ring、k をその剰余体で $ch = p > 0$ とし、ある p 巾 $q (\neq 1)$ に対し、R の endomorphism σ で次のようなものが与えられているとする。

$$\alpha^\sigma \equiv \alpha^q \mod \pi \qquad \forall \alpha \in R$$

ここに、π は固定された素元とする。

R の商体を K とおき、$\mathcal{O}_n = M_n(K)_\sigma[[T]]$ を $M_n(K)$ の行列を係数とする T の巾級数全体に $TA = A^\sigma T$ ($A \in M_n(K)$) によって、かけ算を入れた環とし。$\mathfrak{O}_n$ を

$$\sum_{i=0}^{\infty} A_i T^i \qquad A_i \in M_n(R)$$

なる元からなる部分環とする。

Definition. $\mathbb{X} = {}^t(X_1, \cdots\cdots, X_n)$ に対し

$$\mathbb{X}^a = {}^t(X_1^a, \cdots, X_n^a)$$

Definition. $f \in K[[\mathbb{X}]]_0^n$, $u = \sum A_i T^i \in \mathfrak{S}_n$

に対し $u * f = \sum A_i f^{\sigma^i}(\mathbb{X}^{q^i})$

Definition. $u \in \mathfrak{O}_n$ が special element であるとは

$$u \equiv \pi I_n \mod \deg 1 \quad (\text{in } T)$$

なることをいう。

Theorem (Honda). u が special element のとき

$f = u^{-1}\pi * i_d$ とおくとき (i_d : identity)

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

は R 上の f.g を与える。

今.
$$\begin{array}{ccc} R \hookrightarrow K & \text{より} & \mathrm{End}_R(F) \hookrightarrow \mathrm{End}_K(F) \\ \downarrow & & \downarrow \\ k & & \mathrm{End}_k(F^{red}) \end{array}$$

となるが $F \underset{K}{\approx}$ Additive より $\mathrm{End}_K(F) \simeq M_n(K)$ である。

Lemma 1.(Honda).

$$\mathrm{End}_R(F) \simeq \mathfrak{O}_n \cap u M_n(R) u^{-1} \simeq \{A \in M_n(R) \mid uAu^{-1} \in \mathfrak{O}_n\}$$

Definition. $u = \pi(I_n - P^{-1}N_+T - P^{-1}N_-^{n-1}T^{m+1})$ から $f = u^{-1}\pi * id$, $H = f^{-1}(f(\ )+f(\ ))$ として得られた f.g. を (n, m) 型の Honda group という。$H_{n,m}$ と書く。

但し
$$P = \begin{bmatrix} \pi^{\sigma^{n-1}} & & 0 \\ & \ddots & \\ 0 & & \pi^{\sigma} \\ & & & \pi \end{bmatrix} \qquad N_+ = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ & \ddots & \ddots & & \vdots \\ & & & \ddots & 0 \\ & 0 & & \ddots & 1 \\ & & & & 0 \end{bmatrix}$$

$$N_- = \begin{bmatrix} 0 & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{bmatrix}$$
とおき $m \geqq 1$ とする。

また便宜上、$n = 1$ のとき $N_+ = 0$ $N_-^{n-1} = I_1$ とする。

§2. $\mathrm{End}_R(H_{n,m})$

$\mathrm{End}_R(\ )$ を調べることは、Lemma 1. により $uAu^{-1} \in \mathfrak{O}_n$ なる性質を調べることに帰するが、それは $\pi^{-1}uAu^{-1}\pi \in \mathfrak{O}_n$ と同値である。従って、まず、$u^{-1}\pi$ を知ることが肝要である。

今、$U = P^{-1}N_+T$, $V = P^{-1}N_-^{n-1}T^{m+1}$, $\sigma^{m+n} = \tau$ とおくとき

$$u^{-1}\pi = (\pi^{-1}u)^{-1} = (I_n - (U+V))^{-1}$$
$$= I_n + (U+V) + (U^2 + UV + VU + V^2) + \cdots\cdots$$

であるが、$\beta \in K$ に対し $B = \begin{bmatrix} \beta^{\sigma^{n-1}} & & 0 \\ & \ddots & \\ 0 & & \beta^{\sigma} \\ & & & \beta \end{bmatrix}$ とおくとき、

$$(N_+T)B = B(N_+T)$$

$$(N_-^{n-1}T^{m+1})B = B^{\tau}(N_-^{n-1}T^{m+1})$$

また、 $$(N_-^{n-1})N_+^{k}(N_-^{n-1}) = \delta_{n-1,k}\, N_-^{n-1}$$

なることに注目すれば次の式が得られる。

Theorem. $$u^{-1}\pi = \sum_{\substack{\lambda \geqq 0 \\ |k|<n \\ \lambda(m+n)+k \geqq 0}} W_k^{(\lambda)}$$

ここに、$W_k^{(0)} = U^k$ であり、$\lambda \geqq 1$ では、

$$W_k^{(\lambda)} = \sum_{i+j=n-1+k} U^i V (U^{n-1}V)^{\lambda-1} U^j$$

$$\begin{cases} = \begin{array}{c} \quad\ 1+k \\ \begin{bmatrix} & * & & O \\ & & \ddots & \\ & & & * \\ O & & & \end{bmatrix} \end{array} T^{\lambda(n+m)+k} & k \geqq 0 \\[2ex] = \begin{array}{cc} & \\ 1-k) & \begin{bmatrix} & & O \\ * & & \\ & \ddots & \\ O & & * \end{bmatrix} \end{array} T^{\lambda(n+m)+k} & k < 0 \end{cases}$$

また、$\nu_\pi(*) = -(\lambda n + k)$ が、すべての $*$ について成立する。

我々は $\pi^{-1}uAu^{-1}\pi = (I_n - (U+V))A\sum W_k^{(\lambda)}$ が $\mathfrak{O}_n$ の元となる条件を知りたい。その為に A を次のように表わす。

$$A = \begin{bmatrix} & \vdots & \\ \cdots & a_{ij} & \cdots \\ & \vdots & \end{bmatrix} = \begin{bmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_n \end{bmatrix}$$

これにより、$(I_n-(U+V))A$ は次のようになる。

$$(I_n-(U+V))\begin{bmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_n \end{bmatrix} = \begin{bmatrix} \vdots \\ \mathfrak{a}_i - \pi^{-\sigma^{n-i}} \mathfrak{a}_{i+1}^{\sigma} T \\ \vdots \\ \mathfrak{a}_n - \pi^{-1} \mathfrak{a}_1^{\sigma^{m+1}} T^{m+1} \end{bmatrix} \begin{matrix} \\ (i \quad i<n \\ \\ (n \end{matrix}$$

一方、$W_k^{(\lambda)}$ は $\lambda(n+m)+k$ 次の monomial であるから、$\sum W_k^{(\lambda)}$ の表示に於て、$|k_0|\leqq 1$ のとき、$\lambda(n+m)+k_0$ 次のものは $W_{k_0}^{(\lambda)}$ に限る。それに注意して、$\pi^{-1}u\,A\,u^{-1}\pi$ の $\lambda(m+n)$ 次、及び $\lambda(m+n)+1$ 次の項の第 i 行をみると(但し $i<n$)、

$$(\bigstar)_i \quad \left.\begin{aligned} \mathfrak{a}_i W_1^{(\lambda)} &\equiv \pi^{-\sigma^{n-i}} \mathfrak{a}_{i+1}^{\sigma} W_0^{(\lambda)} \\ \mathfrak{a}_i W_0^{(\lambda)} &\equiv \pi^{-\sigma^{n-i}} \mathfrak{a}_{i+1}^{\sigma} W_{-1}^{(\lambda)} \end{aligned}\right\} \bmod R$$

が得られる。ここで次の Lemma が必要になる。

Lemma 2.

i) $W_k^{(\lambda)} = W_{k-1}^{(\lambda)} U + U^{n-1+k} V (U^{n-1}V)^{\lambda-1}$

$\quad = U W_{k-1}^{(\lambda)} + (VU^{n-1})^{\lambda-1} V U^{n-1+k} \qquad \lambda \geqq 1$

ii) $W_{k+1}^{(\lambda)} = U W_{k-1}^{(\lambda)} U \qquad k\geqq 0,\ \lambda\geqq 1$

$W_{k_0}^{(\lambda)}$ の成分は λ が増大するに従って valuation が $-\infty$ に向う。それと、Lemma 2、をあわせてみると $(\bigstar)_i$ は次のよう

になる。

$$\alpha_{in} = 0$$

$$\alpha^{\sigma}_{i+1\,1} = 0$$

$$\pi^{-\sigma^{n-i}}\alpha^{\sigma}_{i+1\,j+1} = \pi^{-\sigma^{n-j}}\alpha_{ij}$$

これを総合すると $\begin{pmatrix} \alpha^{\sigma^{n-1}} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \alpha^{\sigma} & 0 \\ 0 & \cdots & 0 & \alpha \end{pmatrix}$ となる。

これに $\pi^{-1}uAu^{-1}\pi$ の第 n 行の条件 $(☆)_n$ を加えると

$$(\alpha^{\sigma^{n-1}})^{\sigma^{m+1}} = \alpha^{\tau} = \alpha$$

が必要となる。

一方、 $A = \begin{pmatrix} \alpha^{\sigma^{n-1}} & & & 0 \\ & \ddots & & \\ & & \alpha^{\sigma} & \\ 0 & & & \alpha \end{pmatrix}$ ， $\alpha^{\tau} = \alpha$ であれば、

A は P^{-1}, N_+T, $N_-^{n-1}T^{m+1}$ と可換であり、従って、U, V とも可換である。依って

$$\pi^{-1}uAu^{-1}\pi = (I_n - (U+V))Au^{-1}\pi = A(I_n - (U+V))u^{-1}\pi$$

$$= A \in \mathfrak{O}_n$$

である。即ちこれが必要十分条件である。

$$\mathrm{End}_R(H_{n,m}) \simeq \left\{ \begin{pmatrix} \alpha^{\sigma^{n-1}} & & & 0 \\ & \ddots & & \\ & & \alpha^{\sigma} & \\ 0 & & & \alpha \end{pmatrix} \in M_n(R) \;\middle|\; \alpha^{\tau} = \alpha \right\}$$

$$\simeq \{ \alpha \in R \mid \alpha^{\tau} = \alpha \}$$

特にR ⊇ $\mathbb{Z}_p$ のとき（簡単には complete のとき、更には p-進整数環のとき）、$\{\alpha \in R \mid \alpha^\tau = \alpha\}$ を調べて、次を得る。

Theorem. $\mathrm{End}_R(H_{n,m}) \cong \mathbb{Z}_p[w', \pi']$

ここに、w' は R に属する、1の $q^{m+n}-1$ 乗根のうち order が最大のもので、π' は τ-stable な R の元（例えば p）のうち valuation が minimal positive なもので、$\mathbb{Z}_p[w']$ 上 Eisenstein polynomial で定義される。

参考文献

[1] J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caracteristique $p>0$, Comm. Math. Helv. 28 (1954) 87–118.

[2] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p>0$ (II), Amer. J. Math. 77 (1955) 218–244.

[3] J. Dieudonné, Groups de Lie et hyperalgèbres de Lie sur un corps de caracteristique $p>0$ (III), Math. Z. 63 (1955) 53–75.

[4] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p>0$ (IV), Amer. J. Math. 77 (1955) 429-452.

[5] J. Dieudonné, Groups de Lie et hyperalgèbres de Lie sur un corps de caracteristique $p>0$ (V), Bull. Soc. Math. France 84 (1956) 207-239.

[6] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p>0$ (VI), Amer. J. Math. 79 (1957) 331-388.

[7] J. Dieudonné, Groups de Lie et hyperalgèbres, de Lie sur un corps de caracteristique $p>0$ (VII), Math. Ann. 134 (1957) 114-133.

[8] J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p>0$ (VIII), Amer. J. Math. 80 (1958) 740-772.

[9] T. Honda, On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970) 213-246

[10] Y. Yamasaki, On the endomorphism rings of Honda groups $H_{n,m}$ over $\mathfrak{p}$-adic integer rings, to appear.