Yamasaki, Y.
Osaka J. Math.
12 (1975), 457-472

ON THE ENDOMORPHISM RINGS OF HONDA GROUPS $H_{n,m}$ OVER $\mathfrak{p}$-ADIC INTEGER RINGS

YŌHEI YAMASAKI

(Received June 5, 1974)
(Revised February 7, 1975)

1. Introduction

Dieudonné [1] showed that a commutative formal group over a perfect field k of characteristic $p>0$ corresponds to a certain type of matrix whose entries are elements of a certain non-commutative formal power series ring over the ring $W(k)$of Witt vectors over k. He also showed in [2] that if k is an algebraically closed field, then any commutative formal group over k is isogenous to a direct product of simple commutative formal groups $G_{n,0,m}$ with $(n, m)=1$ and commutative formal groups of Witt vectors of finite length.

Honda [3] studied the theory of commutative formal groups over a certain type of local ring $\mathfrak{o}$ which is a generalization of the ring of Witt vectors $W(k)$. He lifted a commutative formal group over the residue field k to a commutative formal group over o so that the both groups correspond to the same matrix. As a special case, he obtained the Honda groups $H_{n,m}(=G_{n,m}$ in [3]), whose reductions coincide to the Dieudonné groups $G_{n,0,m}$ if k is a perfect field and $\mathfrak{o}=W(k)$. He also found that the endomorphism ring of a n-dimensional commutative formal group over o is isomorphic to a certain subring of $M_n(\mathfrak{o})$.

The purpose of this paper is to determine the endomorphism rings $\mathrm{End}_{\mathfrak{o}}(H_{n,m})$of the Honda groups $H_{n.m}$ explicitly, by calculating the inverse of a certain element of a non-commutative formal power series ring. Since the ring is not commutative, we must distinguish many words in the expansion of the above-mentioned inverse. The basic fact is that the word vanishes unless it has an exceptionally regular form. As an application of present results we shall study the relationship between the commutative formal groups and their endomorphism rings in the forthcomming paper.

The author thanks Professor Honda for suggesting the problem.

2. Preparations

Throughout this paper, we shall use the same notation and terminology as in Honda [3].

Let K be a field of characteristic zero, v a normalized discrete valuation of K and $\mathfrak{o}$ its valuation ring. We shall denote by $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$, by π a prime element of $\mathfrak{p}$ and by k the residue field of o. We shall assume that $\mathfrak{p} \Pi Z$ contains a rational prime p and we shall set $v(p)=e(>0)$. Moreover we assume that there exists an endomorphism σ of o such that

$$\alpha^{\sigma} = \alpha^{q} \bmod \mathfrak{p}$$

for any a in o, where q is a power of$p$. We shall fix σ and π throughout this paper.

Let n be a positive integer and m a non-negative integer. Let $\mathfrak{B}_n = M_n(K)_{\sigma}[[T]]$ be the formal power series ring over the matrix ring $M_n(K)$ with the commutation rule

$$TA = A^{\sigma}T \qquad \cdots\cdots\cdots\cdots\cdots\cdots (*)$$

for any A in $M_n(K)$. Let $\mathfrak{A}_n$ be the subring of $\mathfrak{B}_n$ consisting of the elements whose coefficients are in $M_n(\mathfrak{o})$. We define nxn matrices N_+, N_- and D_{α} with a in K in the following way:

$$N_+ = \begin{bmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{bmatrix}, \quad N_- = \begin{bmatrix} 0 & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} \alpha^{\sigma^{n-1}} & & & 0 \\ & \ddots & & \\ & & \alpha^{\sigma} & \\ 0 & & & a \end{bmatrix}.$$

We shall set

$$u = \pi(I_n - D_{\pi}{}^{-1}N_+T - D_{\pi}{}^{-1}N_-{}^{n-1}T^{m+1})$$

where I_n is the unit matrix of order n. We shall easily see that

$$N_-{}^{n-1} = \begin{bmatrix} 0 & & 0 \\ \vdots & & \\ 0 & & \\ 1 & 0 & 0 \end{bmatrix}.$$

We adopt here the convention that $N_+=0$ and $N_-{}^{n-1}=1$ in case $n=1$. As is easily seen $\pi^{-1}u$ is invertible in $\mathfrak{B}_n$. We shall define the matrices B_r's by the relation:

$$(\pi^{-1}u)^{-1} = u^{-1}\pi = I_n + \sum_{r=1}^{\infty} B_r T^r .$$

For any column vector $x = {}^t(x_1, \cdots, x_n)$ of variables x_i's, we shall define a column vector $h(x) = {}^t(h_1(x), \cdots, h_n(x))$ of formal power series in $K[[x]]$ by

$$h(x) = x + \sum_{r=1}^{\infty} B_r x^{q^r} ,$$

where $x^{q^r} = {}^t(x_1{}^{q^r}, \cdots, x_n{}^{q^r})$ for any positive integer r. After these preparations we shall define the formal group $H(=H_{n,m})$ by the equation:

$$H(x, y) = h^{-1}(h(x)+h(y))\,.$$

This H is defined over $\mathfrak{o}$ (cf. Theorem 2, [3]).

Now we are going to determine the endomorphism ring $\mathrm{End}_{\mathfrak{o}}(H)$ of H over $\mathfrak{o}$. For this purpose several preparatory considerations will be required.

Lemma 1. *For any non-negative integer k, we have*

$$N_-^{\,n-1}N_+^{\,k}N_-^{\,n-1}=\delta_{k,n-1}N_-^{\,n-1},$$

where δ *denotes the Kronecker's* δ.

The proof is elementary and will be omitted. For notational simplicity we set

$$\tau = \sigma^{m+n},$$

throughout the rest of this paper.

Lemma 2. *For any a in K we have*

$$N_+TD_\alpha = D_\alpha N_+T\,,$$

and

$$N_-^{\,n-1}T^{m+1}D_\alpha = D_\alpha^{\,\tau}N_-^{\,n-1}T^{m+1}\,.$$

Proof. By the commutation rule $(*)$ we have

$$N_+TD_\alpha = N_+D_\alpha^{\,\sigma}T = \begin{bmatrix} 0 & \alpha^{\sigma^{n-1}} & & 0 \\ & \ddots & \ddots & \\ & & \ddots & \alpha^{\sigma} \\ 0 & & & 0 \end{bmatrix} T = D_\alpha N_+T\,,$$

similarly we have

$$N_-^{\,n-1}T^{m+1}D_\alpha = N_-^{\,n-1}D_\alpha^{\,\sigma^{m+1}}T^{m+1} = \begin{bmatrix} 0 & & & 0 \\ \vdots & & & \\ 0 & & & \\ \alpha^{\sigma^{m+n}} & 0 & \cdots & 0 \end{bmatrix} T^{m+1}$$

$$= D_\alpha^{\,\tau}N_-^{\,n-1}T^{m+1}\,.$$

Theorem 1. *Let U and V be defined by*

$$U = D_\pi^{-1}N_+T\,, \qquad V = D_\pi^{-1}N_-^{\,n-1}T^{m+1}\,.$$

Then we have the fallowings:

a) $U^k = D_\pi^{-k}N_+^{\,k}T^k$.

For any positive integer λ *and non-negative integers* $r(1), \cdots, r(\lambda-1)$; i, j *we have the following two assertions.*

b) *If $r(s)\neq n-1$ for some s, then we have*

$$U^iVU^{r(1)}VU^{r(2)}\cdots VU^{r(\lambda-1)}VU^j=0.$$

c) *If $r(s)=n-1$ for any s, then we have*

$$U^iVU^{r(1)}VU^{r(2)}\cdots VU^{r(\lambda-1)}VU^j$$

$$=D_\pi^{j(1-\tau\lambda)-n\sum_{s=0}^{\lambda-1}\tau^s-k}N_+^iN_-^{n-1}N_+^jT^{(m+n)\lambda+k}$$

where $k=i+j-(n-1)$.

Proof. Since D_π^{-1} commutes with N_+T by Lemma *2,* we have

$$\begin{aligned}U^k&=(D_\pi^{-1}N_+T)\cdots(D_\pi^{-1}N_+T)\\&=D_\pi^{-1}\cdots D_\pi^{-1}(N_+T)\cdots(N_+T)\\&=D_\pi^{-k}N_+^kT^k.\end{aligned}$$

This proves a). Next we shall prove b). We suppose that there exists s_0 such that $r(s_0)\neq n-1$. Then by Lemma 1, *2* and the fact that any diagonal matrices commute each other, we have

$$\begin{aligned}&VU^{r(s_0)}V\\&=(D_\pi^{-1}(N_-^{n-1}T^{m+1}))(D_\pi^{-1}(N_+T))^{r(s_0)}(D_\pi^{-1}(N_-^{n-1}T^{m+1}))\\&=D_\pi^{-1}(N_-^{n-1}T^{m+1})D_\pi^{-(r(s_0)+1)}(N_+T)^{r(s_0)}N_-^{n-1}T^{m+1}\\&=D_\pi^{-1}D_\pi^{-(r(s_0)+1)\tau}N_-^{n-1}T^{m+1}(N_+T)^{r(s_0)}N_-^{n-1}T^{m+1}\\&=D_\pi^{-1-(r(s_0)+1)\tau}N_-^{n-1}N_+^{r(s_0)}N_-^{n-1}T^{2(m+1)+r(s_0)}=0,\end{aligned}$$

by Lemma 2. Therefore

$$U^iVU^{r(1)}V\cdots VU^{r(s_0)}V\cdots VU^{r(\lambda-1)}VU^j=0.$$

This proves b). Similaly if $r(s)=n-1$ for any s, we have the following by the first part of this theorem.

$$\begin{aligned}&U^iV(U^{n-1}V)^{\lambda-1}U^j\\&=(D_\pi^{-i}N_+^iT^i)(D_\pi^{-1}N_-^{n-1}T^{m+1})(D_\pi^{-n}N_+^{n-1}N_-^{n-1}T^{m+n})^{\lambda-1}(D_\pi^{-j}N_+^jT^j)\\&=D_\pi^{-(i+1)}D_\pi^{-n\sum_{s=1}^{\lambda-1}\tau^s}D_\pi^{-j\tau\lambda}N_+^iN_-^{n-1}N_+^jT^{(m+n)(\lambda-1)+m+1+j+j}\\&=D_\pi^{j(1-\tau\lambda)-n\sum_{s=0}^{\lambda-1}\tau^s-k}N_+^iN_-^{n-1}N_+^jT^{(m+n)\lambda+k}.\end{aligned}$$

Now the theorem is proved.

In Theorem 1 we have defined U and V. We shall define here $W_k^{(\lambda)}$ as follows and these notation will be fixed throughout this paper.

$$W^{(0)}_k = U^k$$

for $0 \leqq k < n$, and

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

for $\lambda \geqq 1$, $|k| < n$. Then we have the following.

Lemma 3. a) *$W^{(\lambda)}_k$ is a monomial of degree $(m+n)\lambda+k$ in T.*

b) $u^{-1}\pi = \sum_{|k|<n,(m+n)\lambda+k\geqq 0} W^{(\lambda)}_k$. .... *(E)*

Proof. The first assertion is an immediate consequence of Theorem 1. Now we have

$$\begin{aligned} u^{-1}\pi &= (I_n-(U+V))^{-1} = \sum_{r\geqq 0}(U+V)^r \\ &= I_n + U + V + U^2 + UV + VU + V^2 + \quad . \end{aligned}$$

From Theorem 1 it follows easily that

$$\begin{aligned} u^{-1}\pi &= \sum_{k=0}^{\infty} U^k + \sum_{i\geqq 0, j\geqq 0, \lambda\geqq 1} U^i V (U^{n-1}V)^{\lambda-1} U^j \\ &= \sum_{k=0}^{n-1} U^k + \sum_{\lambda,k} \sum_{i+j=n-1+k} U^i V (U^{n-1}V)^{\lambda-1} U^j \\ &= \sum W^{(\lambda)}_k . \end{aligned}$$

Corollary. *If $\pi^{\tau}=\pi$ we have*

$$u^{-1}\pi = \sum D_{\pi}^{-(n\lambda+k)} N_k T^{(m+n)\lambda+k}$$

where N_k denotes N_+^{k} fork>0, I_n for $k=0$ and N_-^{-k} fork<0.

This corollary is easily verified by Theorem 1 and by the fact **that** $D_{\pi}^{\tau}=D_{\pi}$.

Proposition 1. *If $m=0$ wehave*

$$u^{-1}\pi - \sum_{r=0}^{\infty} (D_{\pi}^{-1}CT)^s = \sum_{s=0}^{\infty} D^{(s)} C^s T^s$$

where $C=N_+ + N_-^{n-1}$ and $D^{(s)}$ is a ***diagonalmatrix*** *whose (i, i)-th entry $\delta^{(s)}_i$ satisfies the condition:*

$$\nu(\delta^{(s)}_i) = -s$$

for any i.

Proof. We have

$$u^{-1}\pi = (I_n - D_{\pi}^{-1}CT)^{-1} = \sum_{s=0}^{\infty} (D_{\pi}^{-1}CT)^s$$

and

$$(D_{\pi}^{-1}CT)^s = (D_{\pi}^{-1}C)(D_{\pi}^{-1}C)^{\sigma} \cdots (D_{\pi}^{-1}C)^{\sigma^{s-1}} T^s .$$

We shall see

$$(D_\pi^{-1}CT)^s = D^{(s)}C^sT^s$$

with the desired $D^{(s)}$ by induction on s. First we have

$$(D_\pi^{-1}CT)^0 = I_nC^0T^0.$$

Next we assume

$$(D_\pi^{-1}CT)^s = D^{(s)}C^sT^s = \begin{bmatrix} \delta_1^{(s)} & & 0 \\ & \ddots & \\ 0 & & \delta_n^{(s)} \end{bmatrix} C^sT^s$$

with $\nu(\delta_i^{(s)}) = -\acute{\iota}$ for any ι. Then we have

$$(D_\pi^{-1}CT)^{s+1} = (D_\pi^{-1}CT)D^{(s)}C^sT^s = D_\pi^{-1}CD^{(s)\sigma}C^sT^{s+1}$$

$$= D_\pi^{-1} \begin{bmatrix} 0 & 1 & & 0 \\ \vdots & \ddots & \ddots & \\ 0 & & \ddots & 1 \\ 1 & 0 & & 0 \end{bmatrix} \begin{bmatrix} \delta_1^{(s)\sigma} & & 0 \\ & \ddots & \\ 0 & & \delta_n^{(s)\sigma} \end{bmatrix} C^sT^{s+1}$$

$$= D_\pi^{-1} \begin{bmatrix} \delta_2^{(s)\sigma} & & & 0 \\ & \ddots & & \\ & & \delta_n^{(s)\sigma} & \\ 0 & & & \delta_1^{(s)\sigma} \end{bmatrix} C^{s+1}T^{s+1}.$$

We shall set

$$D^{(s+1)} = \begin{bmatrix} \delta_1^{(s+1)} & & 0 \\ & \ddots & \\ 0 & & \delta_n^{(s+1)} \end{bmatrix} = D_\pi^{-1} \begin{bmatrix} \delta_2^{(s)\sigma} & & & 0 \\ & \ddots & & \\ & & \delta_n^{(s)\sigma} & \\ 0 & & & \delta_1^{(s)\sigma} \end{bmatrix}.$$

It is easy to see that

$$\nu(\delta_i^{(s+1)}) = -(s+1),$$

and this $D^{(s+1)}$ satisfies the condition

$$(D_\pi^{-1}CT)^{s+1} = D^{(s+1)}C^{s+1}T^{s+1}.$$

This completes the induction process.

Now we shall see the relationship between $W_k^{(\lambda)}$.

Lemma 4. a) $W_k^{(\lambda)} = W_{k-1}^{(\lambda)}U + U^{n-1+k}V(U^{n-1}V)^{\lambda-1}$
$= UW_{k-1}^{(\lambda)} + (VU^{n-1})^{\lambda-1}VU^{n-1+k}$

for $\lambda \geqq 1$.

b) $W_{k+1}^{(\lambda)} = UW_{k-1}^{(\lambda)}U$

for $k \geqq 0$, $\lambda \geqq 1$.

Proof. From the defining equation of $W_k^{(\lambda)}$we have

$$\begin{aligned} W_k^{(\lambda)} &= \textstyle\sum_{i\geqq 0,n-1+k-i\geqq 0} U^iV(U^{n-1}V)^{\lambda-1}U^{n-1+k-i} \\ &= (\textstyle\sum_{i\geqq 0,n-2+k-i\geqq 0} U^iV(U^{n-1}V)^{\lambda-1}U^{n-2+k-i})U \\ &\quad +U^{n-1+k}V(U^{n-1}V)^{\lambda-1} \\ &= W_{k-1}^{(\lambda)}U+U^{n-1+k}V(U^{n-1}V)^{\lambda-1}\,. \end{aligned}$$

The second equation of a) is obtained in a similar way. b) is an immediate consequence of a) and the fact $U^{n+k}=0$ for $k\geqq 0$ (cf. Theorem 1).

Lemma 5. *Suppose* $\lambda\geqq 1$. *Let* $X^{(\lambda)}=[x_i{}_j^{(\lambda)}]$, $Y^{(\lambda)}=[y_i{}_k^{(\lambda)}]$ *and* $Z^{(\lambda)}=[z_i{}_j^{(\lambda)}]$ *be matrices in* $M_n(K)$ *satisfying the following equations (cf. Theorem* 1) *respectively*:

$$\begin{aligned} X^{(\lambda)}T^{(m+n)\lambda} &= (U^{n-1}V)^{\lambda} \\ Y^{(\lambda)}T^{(m+n)\lambda} &= (VU^{n-1})^{\lambda} \\ Z^{(\lambda)}T^{(m+n)\lambda-1} &= W_{-1}^{(\lambda)}\,. \end{aligned}$$

Then we have the fallowings :

a) $x_i{}_j^{(\lambda)}=0$ *for* $(i,j)\neq(1,1)$, *and* $v(x_1{}_1^{(\lambda)})=-n\lambda$.

b) $y_i{}_j^{(\lambda)}=0$ *for* $(i,j)\neq(n,n)$, *and* $v(y_n{}_n^{(\lambda)})=-n\lambda$.

c) $z_i{}_j^{(\lambda)}=0$ *for* $i-\neq 1$, *and* $v(z_{j+1\,j}^{(\lambda)})=-n\lambda+1$

for tf/zy *j withj*$<n$.

Proof. This lemma is an immediate consequence of Theorem 1 and the fact that π^{σ^s} is a prime element of $\mathfrak{p}$ for any s.

We shall set $\xi_1^{(\lambda)}=x_1{}_1^{(\lambda)}$, $\xi_n^{(\lambda)}=y_n{}_n^{(\lambda}$ and $\eta_j^{(\lambda)}=z_{j+1\,j}^{(\lambda)}$for any$j<n$. These notation will be fixed throughout the rest of this paper.

Lemma 6. $\mathrm{End}_{\mathfrak{o}}(H)\simeq M_n(\mathfrak{o}\cap u^{-1}\mathfrak{A}_nu$.

We owe this lemma to Honda [3] (Corollary of Theorem 3). We shall identify $\mathrm{End}_{\mathfrak{o}}$ *(H)* with $M_n(\mathfrak{o})\cap u^{-1}\mathfrak{A}_nu$ by the above isomorphism.

3. The ring $\mathrm{End}_{\mathfrak{o}}$ *(H)* in case $m>0$

In this section we shall determine the structure of $\mathrm{End}_{\mathfrak{o}}$ *(H)* more explicitly, in case $m>0$. We shall set

$$\mathfrak{o}'=\{\alpha\in\mathfrak{o}\,|\,\alpha^{\tau}=\alpha\}$$

and shall see the following theorem.

Theorem 2. *If* $m>0$, *then* $\mathrm{End}_{\mathfrak{o}}(H) \simeq \mathfrak{o}'$.

Proof. As is easily seen the following three conditions for a matrix A in $M_n(\mathfrak{o})$ are equivalent:

(1) $A \in \mathrm{End}_{\mathfrak{o}}(H)$.

(2) $uAu^{-1} \in \mathfrak{A}_n$.

(3) $\pi^{-1}uAu^{-1}\pi \in \mathfrak{A}_n$.

We shall express $\pi^{-1}uAu^{-1}\pi$ in a formal power series in T as

$$\pi^{-1}uAu^{-1}\pi = \textstyle\sum_{s=0}^{\infty} M(s)T^s .$$

We shall denote by $\boldsymbol{m}_i(s)$ the i-th row vector of $M(s)$.

First we shall prove that

$$\mathrm{End}_{\mathfrak{o}}(H) \subset \{D_\alpha \in M_n(\mathfrak{o}) | \alpha^\tau = \alpha\} .$$

Let $A=[\alpha_{ij}]$ be a matrix in $M_n(\mathfrak{o})$ such that

$$\pi^{-1}uAu^{-1}\pi \in \mathfrak{A}_n .$$

We shall denote by $\boldsymbol{a}_i=(\alpha_{i1}, \cdots, \alpha_{in})$ the i-th row vector of A.
Then we have

$$\begin{aligned} \pi^{-1}uA &= (I_n - D_\pi{}^{-1}N_+T - D_\pi{}^{-1}N_-{}^{n-1}T^{m+1})A \\ &= A - D_\pi{}^{-1}N_+A^\sigma T - D_\pi{}^{-1}N_-{}^{n-1}A^{\sigma^{m+1}}T^{m+1} \\ &= \begin{bmatrix} \boldsymbol{a}_1 - \pi^{-\sigma^{n-1}}\boldsymbol{a}_2{}^\sigma T \\ \vdots \\ \boldsymbol{a}_{n-1} - \pi^{-\sigma}\boldsymbol{a}_n{}^\sigma T \\ \boldsymbol{a}_n - \pi^{-1}\boldsymbol{a}_1{}^{\sigma^{m+1}}T^{m+1} \end{bmatrix} \end{aligned}$$

which imply

$$\pi^{-1}uAu^{-1}\pi = \pi^{-1}uA\sum W_k^{(\lambda)} = \begin{bmatrix} (\boldsymbol{a}_1 - \pi^{-\sigma^{n-1}}\boldsymbol{a}_2{}^\sigma T)\sum W_k^{(\lambda)} \\ \vdots \\ (\boldsymbol{a}_{n-1} - \pi^{-\sigma}\boldsymbol{a}_n{}^\sigma T)\sum W_k^{(\lambda)} \\ (\boldsymbol{a}_n - \pi^{-1}\boldsymbol{a}_1{}^{\sigma^{m+1}}T^{n+1})\sum W_k^{(\lambda)} \end{bmatrix}$$

Thus we have

$$(\boldsymbol{a}_i - \pi^{-\sigma^{n-i}}\boldsymbol{a}_{i+1}{}^\sigma T)\sum W_k^{(\lambda)} = \textstyle\sum_{s=0}^{\infty} \boldsymbol{m}_i(s)T^s = 0 \qquad \mathrm{mod}\ \mathfrak{o}$$

for any $\imath$ with $\imath<n$ and

$$(\boldsymbol{a}_n - \pi^{-1}\boldsymbol{a}_1{}^{\sigma^{m+1}}T^{m+1})\,\Sigma\, W_k^{(\lambda)} = \textstyle\sum_{s=0}^{\infty} \boldsymbol{m}_n(s)T^s = 0 \qquad \mathrm{mod}\ \mathrm{o} .$$

We shall look for the condition for $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ so that the coefficient vectors $\boldsymbol{m}_i(s)$ of T^s have integral entries.

Step 1. Here we are looking for the condition

$$\boldsymbol{m}_i(s) = 0 \qquad \mathrm{mod}\ \mathfrak{o}$$

for any i with $\imath < n$. Since $m > 0$ we shall easily see that if $\lambda \geqq 1$, $k \geqq 1$ then $W^{(\lambda)}_k$ is the only monomial of degree $(m+n)\lambda + k$ in the expansion $(\boldsymbol{E})$ (cf. Lemma 3). We shall calculate $\boldsymbol{m}_i((m+n)\lambda)$and $\boldsymbol{m}_i((m+n)\lambda+1)$. We have

$$\boldsymbol{a}_i W^{(\lambda)}_0 - \pi^{-\sigma^{n-i}} \boldsymbol{a}_{i+1}{}^{\sigma} T W^{(\lambda)}_{-1} = 0 \qquad \mathrm{mod}\ \mathrm{o}$$

and

$$\boldsymbol{a}_i W^{(\lambda)}_1 - \pi^{-\sigma^{n-i}} \boldsymbol{a}_{i+1}{}^{\sigma} T W^{(\lambda)}_0 = 0 \quad \mathrm{mod}\ \mathrm{o}\,,$$

which imply by Lemma 4

$$\left.\begin{aligned} &\boldsymbol{a}_i(VU^{n-1})^{\lambda} + (\boldsymbol{a}_i U - \pi^{-\sigma^{n-i}} \boldsymbol{a}_{i+1}{}^{\sigma} T) W^{(\lambda)}_{-1} = 0 \qquad \mathrm{mod}\ \mathrm{o} \\ &\text{and} \\ &-\pi^{-\sigma^{n-}} \boldsymbol{a}_{i+1}{}^{\sigma} T(U^{n}\ {}^{1}V)^{\lambda} + (\boldsymbol{a}_i U - \pi^{-\sigma^{n-i}} \boldsymbol{a}_{i+1}{}^{\sigma} T) W^{(\lambda)}_{-1} U = 0 \qquad \mathrm{mod}\ \mathrm{o}\,. \end{aligned}\right\} \quad (\boldsymbol{C}_i)$$

By Lemma 5 we shall see that $\boldsymbol{a}_i(VU^{n-1})^{\lambda}$, $(\boldsymbol{a}_i U - \pi^{-\sigma^{n-i}} \boldsymbol{a}_{i+1}{}^{\sigma} T) W^{(\lambda)}_{-1}$,$(\boldsymbol{a}_i V - \pi^{-\sigma^{-}} \boldsymbol{a}_{i+1}{}^{\sigma} T) W^{(\lambda)}_{-1} U$ and $\pi^{-\sigma^{n-}} \boldsymbol{a}_{i+1}{}^{\sigma} T(U^{n-1}V)^{\lambda}$ are vectors of the following forms:

$$\begin{aligned} &\boldsymbol{a}_i(VU^{n-1})^{\lambda} = (0, \cdots, 0, *)\,, \\ &(\boldsymbol{a}_i U - \pi^{-\sigma^{n-i}} \boldsymbol{a}_{i+1}{}^{\sigma} T) W^{(\lambda)}_{-1} = (*, \cdots, *, *)\,, \\ &(\boldsymbol{a}_i U - \pi^{-\sigma^{n-i}} \boldsymbol{a}_{i+1}{}^{\sigma} T) W^{(\lambda)}_{-1} U = (0, *, \cdots, *)\,, \\ &\quad -\pi^{-\sigma^{n-i}} \boldsymbol{a}_{i+1}{}^{\sigma} T(U^{n-1}V)^{\lambda} = (*, 0, \cdots, 0)\,. \end{aligned}$$

Therefore each of the above four vectors is congruent to 0 mod o from the congrence $(\boldsymbol{C}_i)$. We shall consider only the first, second and fourth of these congruences. By Lemma 5, we shall reduce these three congruences respectively to the following forms:

$$\begin{aligned} &\alpha_{i\,n} \xi^{(\lambda)}_1 T^{(m+n)\lambda}\ \Xi\ 0 \qquad \mathrm{mod}\ \mathfrak{o}\,, \\ &(\pi^{-\sigma^{n-j}} \alpha_{i\,j} - \pi^{-\sigma^{n-i}} \alpha_{i+1\,j+1}{}^{\sigma}) \eta^{(\lambda)}_j T^{(m+n)\lambda} = 0 \qquad \mathrm{mod}\ \mathrm{o} \end{aligned}$$

for $j < n$, and

$$-\pi^{-\sigma^{n-}} \alpha_{i+1\,1}{}^{\sigma} \xi^{(\lambda)\sigma}_n T^{(m+n)\lambda+1} = 0 \qquad \mathrm{mod}\ \mathrm{o}\,.$$

Thus we have

$$\begin{aligned} &\alpha_{i\,n} \equiv 0 \qquad \mathrm{mod}\ \mathfrak{p}^{n\lambda}\,, \\ &\pi^{-\sigma^{n-i}} \alpha_{i\,j} - \pi^{-\sigma^{n-i}} \alpha_{i+1\,j+1}{}^{\sigma} = 0 \qquad \mathrm{mod}\ \mathfrak{p}^{n\lambda}\,, \\ &\pi^{-\sigma^{n-i}} \alpha_{i+1\,1}{}^{\sigma} \equiv 0 \qquad \mathrm{mod}\ \mathfrak{p}^{n\lambda+1}\,. \end{aligned}$$

Let λ increase. Then we have

$$\alpha_{in}=0\,,$$
$$\pi^{-\sigma^{n-j}}\alpha_{ij}-\pi^{-\sigma^{n-i}}\alpha_{i+1\,j+1}{}^{\sigma}=0$$

for $j<n$, and

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

respectively. Now by these equations, we have seen that

$$A=D_{\alpha}$$

where $\alpha=\alpha_{nn}$.

Step 2. Here we are looking for the condition for $A=D_{\alpha}$ so that the coefficient vector $\boldsymbol{m}_n(s)$ has integral entries. We shall easily see that there exists at most two monomials $W_{1-n}^{(\lambda+1)}$and $W_{m+1}^{(\lambda)}$whose degrees are $(m+n)\lambda+m+1$ and unique monomial $W_0^{(\lambda)}$ whose degree is $(m+n)\lambda$ in the expansion $(\boldsymbol{E})$ (cf. Lemma 3). We shall consider the congruence

$$\begin{aligned}&\boldsymbol{m}_n((m+n)\lambda+m+1)\\ &=\boldsymbol{a}_nW_{1-n}^{(\lambda+1)}+\boldsymbol{a}_nW_{m+1}^{(\lambda)}-\pi^{-1}\boldsymbol{a}_1{}^{\sigma^{m+1}}T^{m+1}W_0^{(\lambda)}\\ &=0\qquad \mathrm{mod}\ \mathfrak{o}\,.\qquad\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}\qquad(\boldsymbol{C}_n)$$

Here we have

$$\begin{aligned}&\boldsymbol{a}_nW_{1-n}^{(\lambda+1)}=(0,\cdots,0,\alpha)(VU^{n-1})^{\lambda}V\,,\\ &\boldsymbol{a}_nW_{m+1}^{(\lambda)}=0\end{aligned}$$

and

$$\begin{aligned}&\pi^{-1}\boldsymbol{a}_1{}^{\sigma^{m+1}}T^{m+1}W_0^{(\lambda)}\\ &=\pi^{-1}(\alpha^{\tau},0,\cdots,0)T^{m+1}((U^{n-1}V)^{\lambda}+W_{-1}^{(\lambda)}U)\,.\end{aligned}$$

Therefore we have

$$\begin{aligned}&\boldsymbol{m}_n((m+n)\lambda+m+1)\\ &=(0,\cdot\cdot,0,\alpha)(VU^{n-1})^{\lambda}V\\ &\quad-\pi^{-1}(\alpha^{\tau},0,\cdot\cdot,0)T^{m-1}((U^{n-1}V)^{\lambda}+W_{-1}^{(\lambda)}U)\\ &=((0,\cdots,0,\alpha)V-\pi^{-1}(\alpha^{\tau},0,\cdots,0)T^{m+1})(U^{n-1}V)^{\lambda}\\ &=((\alpha,0,\cdots,0)\pi^{-1}T^{m+1}-\pi^{-1}(\alpha^{\tau},0,\cdots,0)T^{m+1})(U^{n-1}V)^{\lambda}\,.\end{aligned}$$

Hence by the congruence $(\boldsymbol{C}_n)$ we have

$$((\alpha,0,\cdots,0)-(\alpha^{\tau},0,\cdots,0))\pi^{-1}T^{m+1}(U^{n-1}V)^{\lambda}=0\qquad\mathrm{mod}\ \mathfrak{o}\,.$$

Let λ increase. Then we have

$$(\alpha, 0, \cdot\ ,0) = (\alpha^{\tau}, 0, \cdots, 0)$$

namely

$$\alpha^{\tau} = a\ .$$

Now we have proved that any matrix A in $M_n(\mathfrak{o})$ such that

$$\pi^{-1}uAu^{-1}\pi \in \mathfrak{A}_n$$

must be of the form

$$A = D_{\alpha}$$

with $\alpha^{\tau}=\alpha$.

Conversely if a matrix A in $M_n(\mathfrak{o})$ satisfies

$$A = D_{\alpha}$$

with $\alpha^{\tau}=\alpha$, then A commutes with $N_{-}^{n-1}T^{m+1}, N_{+}T$ and D_{π}^{-1}. So A commutes with $\pi^{-1}u = I_n - D_{\pi}^{-1}N_{+}T - D_{\pi}^{-1}N_{-}^{n-1}T^{m+1}$. Therefore

$$\pi^{-1}uAu^{-1}\pi = A\pi^{-1}uu^{-1}\pi = A \in \mathfrak{A}_n\ .$$

The ring consisting of such A is isomorphic to the ring $\mathfrak{o}'$ of a in o with $\alpha^{\tau}=\alpha$. Now Theorem 2 is proved.

4. The ring $\mathrm{End}_{\mathfrak{o}}(H)$ in case $m=0$

In this section we shall determine $\mathrm{End}_{\mathfrak{o}}(H)$ more explicitly in case $m=0$. First we shall prove the following proposition.

Proposition 2. *If $m=0$, then*

$$\mathrm{End}_{\mathfrak{o}}(H) \simeq \{A \in M_n(\mathfrak{o}) \mid D_{\pi}AD_{\pi}^{-1} = CA^{\sigma}C^{-1}\}\ .$$

Proof. As in Theorem 2 we shall identify $\mathrm{End}_{\mathfrak{o}}(H)$ with $M_n(\mathfrak{o}) \cap u^{-1}\pi\mathfrak{A}_n\pi^{-1}u$. We have seen in Proposition 1 that

$$u^{-1}\pi = \textstyle\sum_{s=0}^{\infty} (D_{\pi}^{-1}CT)^s = \sum_{s=0}^{\infty} D^{(s)}C^sT^s\ .$$

where C and $D^{(s)}$ are defined as in Proposition 1. Then for any A in $M_n(\mathfrak{o})$ we have

$$\begin{aligned}
&(I_n - D_{\pi}^{-1}CT)A \textstyle\sum_{s=0}^{\infty} (D_{\pi}^{-1}CT)^s \\
&= I_n + \textstyle\sum_{s=0}^{\infty}(AD_{\pi}^{-1}CT - D_{\pi}^{-1}CTA)(D_{\pi}^{-1}CT)^s \\
&= I_n + \textstyle\sum_{s=0}^{\infty} (AD_{\pi}^{-1}C - D_{\pi}^{-1}CA^{\sigma})TD^{(s)}C^sT^s \\
&= I_n + \textstyle\sum_{s=0}^{\infty} (AD_{\pi}^{-1}C - D_{\pi}^{-1}CA^{\sigma})D^{(s)\sigma}C^sT^{s+1}\ .
\end{aligned}$$

Since C and $D^{(s)\sigma}D_{\pi}^{-s}$ are invertible matrices in $M_n(\mathfrak{o})$, we have

$$A \in \mathrm{End}_{\mathfrak{O}}(H)$$

if and only if

$$AD_{\pi}^{-1}C - D_{\pi}^{-1}CA^{\sigma} \text{ s } 0 \qquad \mathrm{mod}\ \mathfrak{p}^{s}$$

for any s. Let s increase. Then we have that

$$A \in \mathrm{End}_{\mathfrak{O}}(H)$$

if and only if

$$AD_{\pi}^{-1}C = D_{\pi}^{-1}CA^{\sigma}\,;$$

i.e.

$$D_{\pi}AD_{\pi}^{-1} = CA^{\sigma}C^{-1}\,.$$

This is the desired result.

Corollary. *If $m=0$and $n-1$,*

$$\mathrm{End}_{\mathfrak{O}}(H) \simeq \{\alpha \in \mathfrak{o} \mid \alpha^{\tau} = \alpha\} = \mathfrak{o}'\,.$$

This corollary is easily verified and the proof will be omitted.

We shall define a left $\mathfrak{o}'$-module structure on $M_n(\mathfrak{o})$ by the following equation:

$$\alpha \circ X = D_{\alpha}X$$

for any a in $\mathfrak{o}'$ and X in $M_n(\mathfrak{o})$.

Proposition 3. *If $m=0$, $\mathrm{End}_{\mathfrak{O}}(H)$ is a $\mathfrak{o}'$-submodule of $M_n(\mathfrak{o})$.*

Proof. We shall only show that $\mathrm{End}_{\mathfrak{O}}(H)$ admits the multiplication of an element a in $\mathfrak{o}'$. For any A in $\mathrm{End}_{\mathfrak{O}}(H)$we have

$$\begin{aligned} D_{\pi}(\alpha\circ A)D_{\pi}^{-1} &= D_{\pi}D_{\alpha}AD_{\pi}^{-1} = D_{\alpha}D_{\pi}AD_{\pi}^{-1} \\ &= D_{\alpha}CA^{\sigma}C^{-1} = CD_{\alpha}^{\sigma}A^{\sigma}C^{-1} = C(D_{\alpha}A)^{\sigma}C^{-1} = C(\alpha\circ A)^{\sigma}C^{-1}\,. \end{aligned}$$

by Proposition 2. On the other hand $\alpha\circ A$ is an element of $M_n(\mathfrak{o})$. Therefore we have that $\alpha\circ A$ is an element of $\mathrm{End}_{\mathfrak{O}}(H)$. This is what we desire.

For any rational integer s we shall define a o'-submodule $\mathfrak{M}^{(s)}$ of $\mathrm{End}_{\mathfrak{O}}(H)$ consisting of matrices$A$'s in $\mathrm{End}_{\mathfrak{O}}(H)$ such that $X^{(s)} = AC^{-s}$ is a diagonal matrix. Since $C^{n} = I_{n}$we have

$$C^{s_1} = C^{s_2}$$

and

$$\mathfrak{M}^{(s_1)} = \mathfrak{M}^{(s_2)}$$

if $s_1 - s_2$ is divisible by n. By these equations we shall set $C^{\bar{s}} = C^s$ and TO$^{(5)}$=9J1$^{(5)}$ for any $\bar{s}$ in Z/nZ which is the reduction of a rational integer s mod n. We shall denote by $\bar{\mathrm{S}}$ the subset of $Z\backslash nZ$ consisting of $\bar{s}$'s such that

$$\mathfrak{M}^{(\bar{s})} \neq 0 .$$

It is easy to see that $\bar{\mathrm{S}}$ is a subgroup of $Z\backslash nZ$.

Proposition 4. *If $m=0$ we have the followings* ·:

a) $\mathrm{End}_{\mathfrak{o}}(H)$ *is isomorphic to* $\oplus_{\bar{s}\in\bar{S}}\mathfrak{M}^{(\bar{s})}$ *as a left* $\mathfrak{o}'$*-module.*

b) $\mathfrak{M}^{(\bar{s})}$ *is a free tf -module of rank one for any s in* $\bar{S}$.

Proof. Any matrix X in $M_n(\mathfrak{o})$ is uniquely expressed as

$$X = \textstyle\sum_{\bar{s}\in Z/nZ} X^{(\bar{s})} C^{\bar{s}}$$

where $X^{(s)}$ is a diagonal matrix for any s. It is easy to see

$$D_\pi X D_\pi^{-1} = C X^\sigma C^{-1}$$

if and only if

$$D_\pi(X^{(\bar{s})} C^{\bar{s}}) D_\pi^{-1} = C(X^{(\bar{s})} C^{\bar{s}})^\sigma C^{-1}$$

for any s. Therefore we have

$$\mathrm{End}_{\mathfrak{o}}(H) \simeq \oplus_{\bar{s}\in\bar{S}} \mathfrak{M}^{(\bar{s})}$$

as a left $\mathfrak{o}'$-module. Now we have proved a). Let $X_1^{(\bar{s})} C^{\bar{s}}$ and $X_2^{(\bar{s})} C^{\bar{s}}$ be non-zero elements of $\mathfrak{M}^{(\bar{s})}$. Then we have

$$D_\pi(X_i^{(\bar{s})} C^{\bar{s}}) D_\pi^{-1} = C(X_i^{(\bar{s})} C^{\bar{s}})^\sigma C^{-1}$$

for each i. As is easily seen any non-zero element of $\mathfrak{M}^{(\bar{s})}$ is invertible in $M_n(K)$. Therefore we have

$$\begin{aligned} &D_\pi(X_1^{(\bar{s})} C^{\bar{s}}) D_\pi^{-1} (D_\pi(X_2^{(\bar{s})} C^{\bar{s}}) D_\pi^{-1})^{-1} \\ &= (C(X_1^{(\bar{s})} C^{\bar{s}})^\sigma C^{-1})(C(X_2^{(\bar{s})} C^{\bar{s}})^\sigma C^{-1})^{-1} . \end{aligned}$$

This equation is equivalent to

$$X_1^{(\bar{s})} X_2^{(\bar{s})-1} = D_\pi(X_1^{(\bar{s})} X_2^{(\bar{s})-1}) D_\pi^{-1} = C(X_1^{(\bar{s})} X_2^{(\bar{s})-1})^\sigma C^{-1} .$$

Now we shall easily see that there exists an element x of the quotient field K' of $\mathfrak{o}'$ such that

$$X_1^{(\bar{s})} X_2^{(\bar{s})-1} = D_x .$$

Since $\mathfrak{M}^{(\bar{s})} \subset M_n(\mathfrak{o})$ and on the other hand $\mathfrak{o}$ is a discrete valuation ring, there exists an element $B^{(\bar{s})} C^{\bar{s}}$ of $\mathfrak{M}^{(\bar{s})}$ such that

$$\mathfrak{M}^{(\bar{s})} = \mathfrak{o}' \circ (B^{(\bar{s})} C^{\bar{s}}) .$$

Now we have also proved b).

Corollary. *If $m=0$ and $\pi^{\tau}=\pi$, then we have*

$$\text{Endo}\,(H) \simeq \{\textstyle\sum_{\bar{s}\in Z/nZ} D_{\alpha_{\bar{s}}} C^{\bar{s}} \in M_n(\mathfrak{o}) \,|\, \alpha_{\bar{s}}^{\tau} = \alpha_{\bar{s}} \quad \textit{for any } \bar{s}\} .$$

This corollary is easily verified and the proof will be omitted.

5. The ring $\mathfrak{o}'$

From now on we shall determine the ring $\mathfrak{o}'$ more explicitly. In this section we suppose that o is complete. Let ϕ be the natural map from o to k. For any element a of o such that $\alpha^{\tau}=\alpha$, we have

$$\phi(\alpha)^{q^{m+n}} = \phi(\alpha) .$$

Therefore we shall regard $\phi(\mathfrak{o}')$ as $GF(q^{m+n}) \cap k$.

Lemma 7. *Let k_0 be a perfect subfieldof k. Then the ring $W(k_0)$ of Witt vectors is naturally embedded into o so that the diagram below commutes*:

$$\begin{tikzcd}
\mathfrak{o} \arrow[r, "\phi"] & k \\
W(k_0) \arrow[u, "\iota_{W(k_0)}"] \arrow[r, "\phi_0"] & k_0 \arrow[u, "\iota_{k_0}"']
\end{tikzcd}$$

where $\iota_{W(k_0)}$is the desiredembedding and $\iota_{k_0}$is the natural embedding of $k_0$into k.

Proof. We shall only give the definition of $\iota_{W(k_0)}$ here, and the detail of the proof will be omitted. Now the mapping $\iota_{W(k_0)}$ is given as follows.

$$\iota_{W(k_0)}\colon \sum \psi_0(x_i)p^i \mapsto \sum \psi(x_i)p^i$$

where ψ (resp. ψ_0) denotes the unique multiplicative representation of k_0 to $\mathfrak{o}$(resp. $W(k_0)$). From now on we shall regard $W(k_0)$ as a subring of o by this embedding.

Now we shall show the following.

Theorem 3. *If $m>0$ or $n=1$, $m=0$ wdhave the followings*:

a) Endo *(H)* — $\mathfrak{o}' = \boldsymbol{Z}_p[w', \pi'\}$

where w' is a generator of the group of $(q^{m+n}-1)$-th roots of unity in $\mathfrak{o}$, and π' is an element of o such that $d=\nu(\pi')$ is minimal positive in $\nu(\mathfrak{o}')$.

b) *π' is a root of an Eisensteinpolynomial f of degree $e'=e/d$ over $\boldsymbol{Z}_p[w']$.*

Proof. We shall set $k_0=GF(q^{m+n})\cap k$. Then we easily obtain

$$W(k_0)\subset\mathfrak{o}',$$

and find a root $w'=\psi(g)$ of unity in $W(k_0)$where g is a generator of the multiplicative group $k_0{}^\times$. Here we shall easily see

$$W(k_0)=\boldsymbol{Z}_p[w'].$$

On the other hand p is contained in $\mathfrak{o}'$. For any non-zero element a in $\mathfrak{o}'$ with $\nu(\alpha)=d$, there exists a pair (x, y) of rational integers such that

$$dx+ey=(d, e),$$

therefore we have

$$\nu(p^y\alpha^x)=(d, e)$$

and

$$p^y\alpha^x\in\mathfrak{o}'.$$

Thus we can choose an element π' so that $\nu(\pi')$ is the minimal positive value in $\nu(\mathfrak{o}')$ For such π' we have

$$\nu(\pi')\,|\,e.$$

From now on we shall denote $d=\nu(\pi')$. For any element β of $\mathfrak{o}'$ we have

$$\psi\circ\phi(\beta)\in W(k_0)$$

and

$$\psi\circ\phi(\beta)=\beta \qquad \bmod \mathfrak{p}.$$

Since $\beta-\psi\circ\phi(\beta)$ is invariant under τ, we have

$$\beta-\psi\circ\phi(\beta)=0 \qquad \bmod \pi'\mathfrak{o}. \quad \cdots\cdots\cdots\cdots\cdots\cdots \quad (C_\tau)$$

Let α be an element of $\mathfrak{o}'$. We shall define a series $\{\alpha_i\}_{-1\leqq i<\infty}$ in $\mathfrak{o}'$ and a series $\{x_i\}_{0\leqq i<\infty}$ in $W(k_0)$ inductively in the following way:

$$\alpha_{-1}=0$$
$$x_i=\psi\circ\phi((\alpha-\alpha_{i-1})/\pi'^i)$$

and

$$\alpha_i=\alpha_{i-1}+x_i\pi'^i$$

for $i\geqq 0$. Then we have

$$\alpha=\textstyle\sum_{i=0}^{\infty} x_i\pi'^i.$$

As is easily seen $\mathfrak{o}'$ is complete as a subring of $\mathfrak{o}$. Therefore we have

$$\mathfrak{o}' = W(k_0)[[\pi']]$$

as a subring of o. Since $\nu(\pi'^{e/d})=\nu(p)$and other hand $W(k_0)$is complete, there exists an Eisenstein polynomial / of degree $e'=e/d$over $W(k_0)$such that

$$f(\pi')=0\,.$$

Thus we have

$$\mathfrak{o}' = W(k_0)[\pi']$$

as a subring of o, by approximation. Since / is irreducible over $W(k_0)$we can regard $W(k_0)[\pi']$as $W(k_0)[x]/(f(x))$. Therefore we have

$$\mathfrak{o}' = \boldsymbol{Z}_p[w', \pi']\,.$$

Now our proof is complete.

Corollary. *If $m>0$ or $m=0$, $n=1$ and moreover $e=1$, then we have*

$$\mathrm{End}_{\mathfrak{o}}(H) \simeq \boldsymbol{Z}_p[w']\,.$$

OSAKA UNIVERSITY

References

[1] J. Dieudonné: *Lie groups and Lie hyperalebras over a field of characteristic $p>0$ (IV)*, Amer. J. Math. 77 (1955), 429–452.

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

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

[4] J.P. Serre: Corps Locaux, Hermann, 1962.

[5] E. Witt: *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, J. Reine Angew. Math. 176 (1936), 126-140.