<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>On the endomorphism rings of Honda groups $H_{n,m}$ over p-adic integer rings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Yamasaki, Yōhei</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Journal of Mathematics. 12(2) P.457–P.472</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>1975</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/10678">https://doi.org/10.18910/10678</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/10678</td>
</tr>
</tbody>
</table>

*Osaka University Knowledge Archive: OUKA*

https://ir.library.osaka-u.ac.jp/repo/ouka/all/

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

YÔHEI 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 $\mathfrak{o}$ 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 $\mathfrak{o}$ is isomorphic to a certain subring of $M_n(\mathfrak{o})$.

The purpose of this paper is to determine the endomorphism rings $\text{End}_\mathfrak{o}(H_{n,m})$ 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 forthcoming 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, $\nu$ 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 $\pi$ a prime element of $\mathfrak{p}$ and by $k$ the residue field of $\mathfrak{o}$. We shall assume that $\mathfrak{p} \cap \mathbb{Z}$ contains a rational prime $p$ and we shall set $\nu(p) = e(>0)$. Moreover we assume that there exists an endomorphism $\sigma$ of $\mathfrak{o}$ such that

$$\sigma^e = \sigma^q \mod \mathfrak{p}$$

for any $a$ in $\mathfrak{o}$, where $q$ is a power of $p$. We shall fix $\sigma$ and $\pi$ throughout this paper.

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

$$TA = A^{\sigma}T \quad \text{(*)}$$

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 $n \times n$ matrices $N_+$, $N_-$ and $D_\sigma$ with $a$ in $K$ in the following way:

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

We shall set

$$u = \pi(I_n - D^{-1}_\sigma N_+ T - D^{-1}_\sigma N_- T^{m+1})$$

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

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

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

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

For any column vector $x = (x_1, \cdots, x_n)$ of variables $x_i$'s, we shall define a column vector $h(x) = (h_1(x), \cdots, h_n(x))$ of formal power series in $K[[x]]$ by

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

where $x^r = (x_1^r, \cdots, x_n^r)$ for any positive integer $r$. After these preparations we shall define the formal group $H(=H_{n,m})$ by the equation:
This $H$ is defined over $\mathfrak{o}$ (cf. Theorem 2, [3]).

Now we are going to determine the endomorphism ring $\text{End}_0(H)$ of $H$ over $\mathfrak{o}$. For this purpose several preparatory considerations will be required.

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

$$N_{n-1}N_+^kN_{n-1}^\delta = 0,$$

where $\delta$ denotes the Kronecker's $\delta$.

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

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

throughout the rest of this paper.

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

$$N_+TD_a = D_aN_+T,$$

and

$$N_{n-1}T^{m+1}D_a = D_a^\sigma N_{n-1}T^{m+1}.$$

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

$$N_+TD_a = N_+D_a^\sigma T = \begin{bmatrix} 0 & \alpha^{r-1} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \alpha^r \\ \end{bmatrix} T = D_a N_+T,$$

similarly we have

$$N_{n-1}T^{m+1}D_a = N_{n-1}D_a^\sigma T^{m+1} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha^{r+1} & \cdots & 0 \\ \end{bmatrix} T^{m+1} = D_a^\sigma N_{n-1}T^{m+1}.$$

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

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

Then we have the followings:

a) $U^k = D_{\sigma^{-k}}N_+^kT^k$.

For any positive integer $\lambda$ 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
\[
U^iVU^{r(1)}VU^{r(2)} \cdots VU^{r(\lambda-1)}VU^j = \sum_{k=0}^{\lambda-1} \sum_{l=0}^{\lambda-1} \sum_{m=0}^{\lambda-1} \sum_{n=0}^{\lambda-1} T^{(m+n)\lambda+k}.
\]
where $k = i+j-(n-1)$.

Proof. Since $D_\varepsilon^{-1}$ commutes with $N_+T$ by Lemma 2, we have
\[
U^k = (D_\varepsilon^{-1}N_+T) \cdots (D_\varepsilon^{-1}N_+T)
\]
\[
= D_\varepsilon^{-1} \cdots D_\varepsilon^{-1} (N_+T) \cdots (N_+T)
\]
\[
= D_\varepsilon^{-k} N_+^k T^k.
\]
This proves a). Next we shall prove b). We suppose that there exists $s_0$ such that $r(s_0) = n-1$. Then by Lemma 1, 2 and the fact that any diagonal matrices commute each other, we have
\[
VU^{r(s_0)}V = (D_\varepsilon^{-1}(N_+^{-1}T^{m+1}))(D_\varepsilon^{-1}(N_+T))^r(s_0)(D_\varepsilon^{-1}(N_+^{-1}T^{m+1}))
\]
\[
= D_\varepsilon^{-1}(N_+^{-1}T^{m+1})D_\varepsilon^{-r(s_0)+1}(N_+T)^r(s_0) N_+^{-1}T^{m+1}
\]
\[
= D_\varepsilon^{-1}D_\varepsilon^{-r(s_0)+1}r(s_0)N_+^{-1}T^{m+1} = D_\varepsilon^{-1}(r(s_0)+1)r(s_0)N_+^{-1}T^{m+1} = 0,
\]
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). Similary if $r(s) = n-1$ for any $s$, we have the following by the first part of this theorem.
\[
U^iVU^{n-1}V^{\lambda-1}U^j
\]
\[
= (D_\varepsilon^{-i}N_+T^i)(D_\varepsilon^{-n}(N_+^{-1}T^{n+1}))(D_\varepsilon^{-n}N_+^{-1}N_+^{-n-1}T^{m+1})^{\lambda-1}(D_\varepsilon^{-j}N_+^jT^j)
\]
\[
= D_\varepsilon^{-(i+1)}D_\varepsilon^{-n} \sum_{l=0}^{\lambda-1} \sum_{m=0}^{\lambda-1} \sum_{n=0}^{\lambda-1} \sum_{l=0}^{\lambda-1} T^{(m+n)(\lambda-1)+m+1+i+j}
\]
\[
= D_\varepsilon^{(1-\lambda)-n} \sum_{l=0}^{\lambda-1} \sum_{m=0}^{\lambda-1} \sum_{n=0}^{\lambda-1} \sum_{l=0}^{\lambda-1} T^{(m+n)\lambda+k}.
\]
Now the theorem is proved.

In Theorem 1 we have defined $U$ and $V$. We shall define here $W^{(\lambda)}_k$ as follows and these notation will be fixed throughout this paper.
for $0 \leq k < n$, and
\[ W_{-k}^{(0)} = U_k \]
for $\lambda \geq 1$, $|k| < n$. Then we have the following.

**Lemma 3.**

a) $W_{-k}^{(0)}$ is a monomial of degree $(m+n)\lambda + k$ in $T$.

b) $u^{-1} \pi = \sum_{|k| < n, (m+n)\lambda + k \geq 0} W_{-k}^{(\lambda)}$.

**Proof.** The first assertion is an immediate consequence of Theorem 1. Now we have
\[ u^{-1} \pi = (I_n - (U + V))^{-1} = \sum_{r \geq 0} (U + V)^r \]
\[ = I_n + U + V + U^2 + UV + VU + V^2 + \ldots \]

From Theorem 1 it follows easily that
\[ u^{-1} \pi = \sum_{k=0}^{n} U_k + \sum_{j \geq 0, \lambda \geq 1} U_j V(U^{m-1} V)^{\lambda-1} U_j \]
\[ = \sum_{k=0}^{n} U_k + \sum_{\lambda, k} \sum_{j = n-1+k} U_j V(U^{m-1} V)^{\lambda-1} U_j \]
\[ = \sum W_{-k}^{(\lambda)}. \]

**Corollary.** If $\pi^\tau = \pi$ we have
\[ u^{-1} \pi = \sum D_{\tau}^{-((m+n)\lambda + k)} N_k T^{(m+n)\lambda + k} \]
where $N_k$ denotes $N_{+, k}$ for $k > 0$, $I_n$ for $k = 0$ and $N_{-, k}$ for $k < 0$.

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

**Proposition 1.** If $m = 0$ we have
\[ u^{-1} \pi = \sum_{\tau = 0}^\infty (D_{\tau}^{-1} CT)^\tau = \sum_{\tau = 0}^\infty D^{(\tau)} C^\tau T^\tau \]
where $C = N_{+, n-1} + N_{-, n-1}$ and $D^{(\tau)}$ is a diagonal matrix whose $(i, i)$-th entry $\delta_{i}^{(\tau)}$ satisfies the condition:
\[ \nu(\delta_{i}^{(\tau)}) = -s \]
for any $i$.

**Proof.** We have
\[ u^{-1} \pi = (I_n - D_{\tau}^{-1} CT)^{-1} = \sum_{\tau = 0}^\infty (D_{\tau}^{-1} CT)^\tau \]
and
\[ (D_{\tau}^{-1} CT)^\tau = (D_{\tau}^{-1} C)(D_{\tau}^{-1} C)^{\tau-1}(D_{\tau}^{-1} C)^{\tau-1} T^\tau. \]

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

$$(D^{-1}_s CT)^0 = I_n C^0 T^s.$$  

Next we assume

$$(D^{-1}_s CT)^s = D^{(s)} C^s T^s = \begin{bmatrix} \delta^{(s)}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \delta^{(s)}_n \end{bmatrix} C^s T^s$$

with $\nu(\delta^{(s)}_i) = -i$ for any $i$. Then we have

$$(D^{-1}_s CT)^{s+1} = (D^{-1}_s CT)D^{(s)} C^s T^s = D^{-1}_s C D^{(s)} C^s T^{s+1}$$

$$= D^{-1}_s \begin{bmatrix} 0 & 1 & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \delta^{(s)}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \delta^{(s)}_n \end{bmatrix} C^s T^{s+1}$$

$$= D^{-1}_s \begin{bmatrix} \delta^{(s)}_1 \delta^{(s)}_2 \cdots \delta^{(s)}_n \\ \vdots \ddots \vdots \\ \delta^{(s)}_n \delta^{(s)}_n \cdots \delta^{(s)}_2 \delta^{(s)}_1 \end{bmatrix} C^{s+1} T^{s+1}.$$  

We shall set

$$D^{(s+1)} = \begin{bmatrix} \delta^{(s+1)}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \delta^{(s+1)}_n \end{bmatrix} = D^{-1}_s \begin{bmatrix} \delta^{(s)}_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \delta^{(s)}_n \end{bmatrix}.$$  

It is easy to see that

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

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

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

This completes the induction process.

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

**Lemma 4.**  

a) $W^{(\lambda)}_k = W^{(\lambda)}_{k-1} U + U^{n-1+k} V(U^{n-1})^{\lambda-1} = UW^{(\lambda)}_{k-1} + (VU^{n-1})^{\lambda-1} V U^{n-1+k}$

for $\lambda \geq 1$.

b) $W^{(\lambda)}_{k+1} = UW^{(\lambda)}_k U$

for $k \geq 0, \lambda \geq 1$. 
Proof. From the defining equation of $W_{1}^{(\lambda)}$ we have
\[ W_{1}^{(\lambda)} = \sum_{i \geq 0, m - 1 + k - i \geq 0} U^i V(U^{m - 1} V)^{\lambda - 1} U_{n - 1 + k - i} \]
\[ = (\sum_{i \geq 0, m - 2 + k - i \geq 0} U^i V(U^{m - 1} V)^{\lambda - 1} U_{n - 2 + k - i}) U \]
\[ + U^{n - 1 + k} V(U^{m - 1} V)^{\lambda - 1} \]
\[ = W_{1}^{(\lambda)} U + U^{n - 1 + k} V(U^{m - 1} V)^{\lambda - 1}. \]

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 $k \geq 0$ (cf. Theorem 1).

Lemma 5. Suppose $\lambda \geq 1$. Let $X^{(\lambda)} = [x_{i,j}^{(\lambda)}], Y^{(\lambda)} = [y_{i,j}^{(\lambda)}]$ and $Z^{(\lambda)} = [z_{i,j}^{(\lambda)}]$ be matrices in $M_n(K)$ satisfying the following equations (cf. Theorem 1) respectively:
\[ X^{(\lambda)} T^{(m + n)} = (U^{m - 1} V)^\lambda \]
\[ Y^{(\lambda)} T^{(m + n)} = (V U^{n - 1})^\lambda \]
\[ Z^{(\lambda)} T^{(m + n)} = W_{1}^{(\lambda)}. \]

Then we have the followings:

a) $x_{i,j}^{(\lambda)} = 0$ for $(i, j) \neq (1, 1)$, and $\nu(x_{i,j}^{(\lambda)}) = -n \lambda$.

b) $y_{i,j}^{(\lambda)} = 0$ for $(i, j) \neq (n, n)$, and $\nu(y_{i,j}^{(\lambda)}) = -n \lambda$.

c) $z_{i,j}^{(\lambda)} = 0$ for $i \neq 1$, and $\nu(z_{i,j}^{(\lambda)}) = -n \lambda + 1$ for $i \neq j$ with $j < n$.

Proof. This lemma is an immediate consequence of Theorem 1 and the fact that $\pi^{s'}$ is a prime element of $p$ for any $s$. We shall set $x_{i,j}^{(\lambda)} = x_{i,j}^{(\lambda)}$, $y_{i,j}^{(\lambda)} = y_{i,j}^{(\lambda)}$ and $z_{i,j}^{(\lambda)} = z_{i,j}^{(\lambda)}$ for any $j < n$. These notation will be fixed throughout the rest of this paper.

Lemma 6. $\text{End}_0(H) = M_{n}(0) \cap u^{-1} \mathfrak{A}_n u$.

We owe this lemma to Honda [3] (Corollary of Theorem 3). We shall identify $\text{End}_0(H)$ with $M_{n}(0) \cap u^{-1} \mathfrak{A}_n u$ by the above isomorphism.

3. The ring $\text{End}_0(H)$ in case $m > 0$

In this section we shall determine the structure of $\text{End}_0(H)$ more explicitly, in case $m > 0$. We shall set $o' = \{\alpha \in o \mid \alpha^* = \alpha\}$ and shall see the following theorem.
Theorem 2. If $m > 0$, then $\text{End}_0(H) = \mathfrak{a}'$.

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

1. $A \in \text{End}_0(H)$.
2. $uAu^{-1} \in \mathfrak{U}_n$.
3. $\pi^{-1}uAu^{-1} \pi \in \mathfrak{U}_n$.

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

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

We shall denote by $m_i(s)$ the $i$-th row vector of $M(s)$.

First we shall prove that

$$\text{End}_0(H) \subset \{ D_\alpha \in M_n(\mathfrak{a}) | \alpha^r = \alpha \}.$$ 

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

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

We shall denote by $a_i = (\alpha_{1i}, \ldots, \alpha_{in})$ the $i$-th row vector of $A$.

Then we have

$$\pi^{-1}uA = (I_n - D_\alpha^{-1}N_+ T - D_\alpha^{-1}N_- A^{m+1})A$$
$$= A - D_\alpha^{-1}N_+ A^{s+1} T - D_\alpha^{-1}N_- A^{m+1}$$
$$= \begin{bmatrix}
\alpha_i - \pi^{-1}a_i \sigma T \\
\alpha_{n-1} - \pi^{-1}a_n \sigma T \\
\vdots \\
\alpha_n - \pi^{-1}a_n \sigma T
\end{bmatrix}$$

which imply

$$\pi^{-1}uAu^{-1} \pi = \pi^{-1}uA \sum W^{(\alpha)} = \begin{bmatrix}
(\alpha_i - \pi^{-1}a_i \sigma T) \sum W^{(\alpha)} \\
(\alpha_{n-1} - \pi^{-1}a_n \sigma T) \sum W^{(\alpha)} \\
(\alpha_n - \pi^{-1}a_n \sigma T) \sum W^{(\alpha)}
\end{bmatrix}.$$ 

Thus we have

$$(\alpha_i - \pi^{-1}a_i \sigma T) \sum W^{(\alpha)} = \sum_{s=0}^{\infty} m_i(s)T^s = 0 \quad \text{mod } \mathfrak{a}$$

for any $i$ with $i < n$ and

$$(\alpha_n - \pi^{-1}a_n \sigma T) \sum W^{(\alpha)} = \sum_{s=0}^{\infty} m_n(s)T^s = 0 \quad \text{mod } \mathfrak{a}.$$
We shall look for the condition for \( a_1, \ldots, a_n \) so that the coefficient vectors \( m_i(s) \) of \( T^s \) have integral entries.

Step 1. Here we are looking for the condition

\[
m_i(s) = 0 \quad \text{mod } o
\]

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

\[
a_i W^{(k)}_k - \pi^{-\sigma^{n-i}} a_{i+1}^\sigma T W^{(k)}_k = 0 \quad \text{mod } o
\]

and

\[
a_i W^{(k)}_k - \pi^{-\sigma^{n-i}} a_{i+1}^\sigma T W^{(k+1)}_k = 0 \quad \text{mod } o,
\]

which imply by Lemma 4

\[
a_i (VU^{n-1})^\lambda + (a_i U - \pi^{-\sigma^{n-i}} a_{i+1}^\sigma T) W^{(k+1)}_k = 0 \quad \text{mod } o
\]

and

\[
-\pi^{-\sigma^{n-i}} a_{i+1}^\sigma T(U^{n-1}V^\lambda) + (a_i U - \pi^{-\sigma^{n-i}} a_{i+1}^\sigma T) W^{(k+1)}_k = 0 \quad \text{mod } o.
\]

By Lemma 5 we shall see that \( a_i (VU^{n-1})^\lambda, (a_i U - \pi^{-\sigma^{n-i}} a_{i+1}^\sigma T) W^{(k+1)}_k, (a_i U - \pi^{-\sigma^{n-i}} a_{i+1}^\sigma T) W^{(k)}_k U \) and \( \pi^{-\sigma^{n-i}} a_{i+1}^\sigma T(U^{n-1}V)^\lambda \) are vectors of the following forms:

\[
\begin{align*}
& a_i (VU^{n-1})^\lambda = (0, \ldots, 0, *) , \\
& (a_i U - \pi^{-\sigma^{n-i}} a_{i+1}^\sigma T) W^{(k+1)}_k = (*, \ldots, *, *), \\
& (a_i U - \pi^{-\sigma^{n-i}} a_{i+1}^\sigma T) W^{(k)}_k U = (0, *, \ldots, *), \\
& -\pi^{-\sigma^{n-i}} a_{i+1}^\sigma T(U^{n-1}V)^\lambda = (*, 0, \ldots, 0).
\end{align*}
\]

Therefore each of the above four vectors is congruent to 0 mod o from the congruence \( (C_i) \). 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:

\[
\begin{align*}
& \alpha_{i n} T^{(m+n)\lambda} \equiv 0 \quad \text{mod } o, \\
& (\pi^{-\sigma^{n-i}} a_{i+1}^\sigma T)^{\lambda} T^{(m+n)\lambda} \equiv 0 \quad \text{mod } o
\end{align*}
\]

for \( j \leq n \), and

\[
-\pi^{-\sigma^{n-i}} \alpha_{i+1}^\sigma T^{(m+n)\lambda+1} \equiv 0 \quad \text{mod } o.
\]

Thus we have

\[
\begin{align*}
& \alpha_{i n} \equiv 0 \quad \text{mod } p^{n\lambda}, \\
& \pi^{-\sigma^{n-i}} \alpha_{i+1}^\sigma \equiv 0 \quad \text{mod } p^{n\lambda}, \\
& \pi^{-\sigma^{n-i}} \alpha_{i+1} \equiv 0 \quad \text{mod } p^{n\lambda+1}.
\end{align*}
\]
Let $\lambda$ increase. Then we have

$$\alpha_{in} = 0,$$

$$\pi^{-j} \alpha_{ij} - \pi^{-i} \alpha_{i+1 j+1} = 0$$

for $j < n$, and

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

respectively. Now by these equations, we have seen that

$$A = D_{\alpha}$$

where $\alpha = \alpha_{n, n}$.

Step 2. Here we are looking for the condition for $A = D_{\alpha}$ so that the coefficient vector $m_\alpha(s)$ has integral entries. We shall easily see that there exists at most two monomials $W^{(\lambda+1)}_1$ and $W^{(\lambda)}_{m+1}$ whose degrees are $(m+n)\lambda + m + 1$ and unique monomial $W^{(\lambda)}_0$ whose degree is $(m+n)\lambda$ in the expansion $(E)$ (cf. Lemma 3). We shall consider the congruence

$$m_\alpha((m+n)\lambda + m + 1)$$

$$= a_n W^{(\lambda+1)}_1 + a_m W^{(\lambda)}_{m+1} - \pi^{-1} a_i \sigma^{m+1} T^{m+1} W^{(\lambda)}_0$$

$$= 0 \mod \varphi.$$  \hspace{1cm} (C_n)

Here we have

$$a_n W^{(\lambda+1)}_1 = (0, \cdots, 0, \alpha)(V U^{m-1}) V,$$

$$a_m W^{(\lambda)}_{m+1} = 0$$

and

$$\pi^{-1} a_i \sigma^{m+1} T^{m+1} W^{(\lambda)}_0$$

$$= \pi^{-1} (\alpha, 0, \cdots, 0) T^{m+1}((U^{m-1} V)^\lambda + W^{(\lambda)}_1 U).$$

Therefore we have

$$m_\alpha((m+n)\lambda + m + 1)$$

$$= (0, \cdots, 0, \alpha)(V U^{m-1}) V$$

$$- \pi^{-1} (\alpha, 0, \cdots, 0) T^{m+1}((U^{m-1} V)^\lambda + W^{(\lambda)}_1 U)$$

$$= ((0, \cdots, 0, \alpha) V - \pi^{-1} (\alpha, 0, \cdots, 0) T^{m+1}((U^{m-1} V)^\lambda)$$

$$= ((\alpha, 0, \cdots, 0) \pi^{-1} T^{m+1} - \pi^{-1} (\alpha, 0, \cdots, 0) T^{m+1}((U^{m-1} V)^\lambda).$$

Hence by the congruence $(C_n)$ we have

$$(\alpha, 0, \cdots, 0) - (\alpha, 0, \cdots, 0) \pi^{-1} T^{m+1}((U^{m-1} V)^\lambda) = 0 \mod \varphi.$$
Let $\lambda$ increase. Then we have
\[(\alpha, 0, \cdots, 0) = (\alpha', 0, \cdots, 0)\]
namely
\[\alpha' = \alpha.\]

Now we have proved that any matrix $A$ in $M_n(o)$ such that
\[\pi^{-1}uAu^{-1}\pi \in \mathfrak{A}_n\]
must be of the form
\[A = D_\alpha\]
with $\alpha' = \alpha$.

Conversely if a matrix $A$ in $M_n(o)$ satisfies
\[A = D_\alpha\]
with $\alpha' = \alpha$, then $A$ commutes with $N_i^{-1}T^{m+1}, N_j T$ and $D_{\pi}^{-1}$. So $A$ commutes with $\pi^{-1}u = I_n - D_{\pi}^{-1}N_j T - D_{\pi}^{-1}N_j^{-1}T^{m+1}$. 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 $o'$ of $a$ in $o$ with $\alpha' = \alpha$. Now Theorem 2 is proved.

4. The ring $\text{End}_0(H)$ in case $m = 0$

In this section we shall determine $\text{End}_0(H)$ more explicitly in case $m = 0$. First we shall prove the following proposition.

**Proposition 2.** If $m = 0$, then
\[\text{End}_0(H) = \{A \in M_n(o)| D_\pi AD_\pi^{-1} = CA^oC^{-1}\}.\]

**Proof.** As in Theorem 2 we shall identify $\text{End}_0(H)$ with $M_n(o) \cap u^{-1}\mathfrak{A}_n u^{-1}$. We have seen in Proposition 1 that
\[u^{-1}\pi = \sum_{i=0}^n (D_{\pi}^{-1}CT)^i = \sum_{i=0}^n D^{(i)}C^iT^i.\]
where $C$ and $D^{(i)}$ are defined as in Proposition 1. Then for any $A$ in $M_n(o)$ we have
\[(I_n - D_{\pi}^{-1}CT)A \sum_{i=0}^n (D_{\pi}^{-1}CT)^i \]
\[= I_n + \sum_{i=0}^n (AD_{\pi}^{-1}CT - D_{\pi}^{-1}CTA)(D_{\pi}^{-1}CT)^i \]
\[= I_n + \sum_{i=0}^n (AD_{\pi}^{-1}C - AD_{\pi}^{-1}CA^o)TD^{(i)}C^iT^i \]
\[= I_n + \sum_{i=0}^n (AD_{\pi}^{-1}C - AD_{\pi}^{-1}CA^o)D^{(i)}C^iT^{i+1}.\]
Since $C$ and $D^{-s}D_\sigma^{-s}$ are invertible matrices in $M_n(\mathfrak{o})$, we have

$$A \in \text{End}_\mathfrak{o}(H)$$

if and only if

$$AD_\sigma^{-1}C-D_\sigma^{-1}CA^\sigma\equiv 0 \pmod{\mathfrak{p}^s}$$

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

$$A \in \text{End}_\mathfrak{o}(H)$$

if and only if

$$AD_\sigma^{-1}C=D_\sigma^{-1}CA^\sigma.$$ i.e.

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

This is the desired result.

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

$$\text{End}_\mathfrak{o}(H) \cong \{\alpha \in \mathfrak{o} | \alpha^\sigma = \alpha\} = \mathfrak{o}'.$$

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 $\alpha$ in $\mathfrak{o}'$ and $X$ in $M_n(\mathfrak{o})$.

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

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

$$D_\sigma(\alpha \circ A)D_\sigma^{-1} = D_\sigma D_\alpha AD_\sigma^{-1} = D_\alpha D_\sigma AD_\sigma^{-1}$$

$$= D_\alpha CA^\sigma C^{-1} = C(D_\alpha A)^\sigma C^{-1} = C(\alpha \circ A)^\sigma C^{-1}.$$  

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 $\text{End}_\mathfrak{o}(H)$. This is what we desire.

For any rational integer $s$ we shall define a $\mathfrak{o}'$-submodule $\mathfrak{M}^{(s)}$ of $\text{End}_\mathfrak{o}(H)$ consisting of matrices $A$'s in $\text{End}_\mathfrak{o}(H)$ such that $X^{(s)} = AC^{-s}$ is a diagonal matrix. Since $C^n = I_\sigma$ 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 $C^s = C^z$ and $\mathfrak{M}^{s} = \mathfrak{M}^{z}$ for any $s$ in $\mathbb{Z}/n\mathbb{Z}$ which is the reduction of a rational integer $s \mod n$. We shall denote by $\overline{S}$ the subset of $\mathbb{Z}/n\mathbb{Z}$ consisting of $s$'s such that

$$\mathfrak{M}^{s} = 0.$$ 

It is easy to see that $\overline{S}$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$.

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

a) $\operatorname{End}_o (H)$ is isomorphic to $\bigoplus_{s \in S} \mathfrak{M}^{(s)}$ as a left $o'$-module.

b) $\mathfrak{M}^{(s)}$ is a free left module of rank one for any $s$ in $\overline{S}$.

**Proof.** Any matrix $X$ in $M_d(o)$ is uniquely expressed as

$$X = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} X^{(s)} C^s$$

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

$$D_s XD_s^{-1} = CX^s C^{-1}$$

if and only if

$$D_s (X^{(s)} C^s) D_s^{-1} = C (X^{(s)} C^s) C^{-1}$$

for any $s$. Therefore we have

$$\operatorname{End}_o (H) \cong \bigoplus_{s \in \overline{S}} \mathfrak{M}^{(s)}$$

as a left $o'$-module. Now we have proved a). Let $X^{(s)}_1 C^s$ and $X^{(s)}_2 C^s$ be non-zero elements of $\mathfrak{M}^{(s)}$. Then we have

$$D_s (X^{(s)}_1 C^s) D_s^{-1} = C (X^{(s)}_1 C^s) C^{-1}$$

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

$$D_s (X^{(s)}_1 C^s) D_s^{-1} (D_s (X^{(s)}_2 C^s) D_s^{-1})^{-1} = (C (X^{(s)}_1 C^s) C^{-1}) (C (X^{(s)}_2 C^s) C^{-1})^{-1}.$$ 

This equation is equivalent to

$$X^{(s)}_1 X^{(s)}_2^{-1} = D_s (X^{(s)}_1 X^{(s)}_2^{-1}) D_s^{-1} = C (X^{(s)}_1 X^{(s)}_2^{-1}) C^{-1}.$$ 

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

$$X^{(s)}_1 X^{(s)}_2^{-1} = D_x.$$ 

Since $\mathfrak{M}^{(s)} \subset M_d(o)$ and on the other hand $o$ is a discrete valuation ring, there exists an element $B^{(s)} C^s$ of $\mathfrak{M}^{(s)}$ such that
Now we have also proved b).

**Corollary.** If \( m = 0 \) and \( \pi^s = \pi \), then we have

\[
\text{Endo} (H) = \{ \sum_{s \in \mathbb{Z}/m} D_s C_s \in M_d (O) \mid \alpha ^s = \alpha \text{ for any } s \}.
\]

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

5. The ring \( o' \)

From now on we shall determine the ring \( o' \) more explicitly. In this section we suppose that \( o \) is complete. Let \( \phi \) be the natural map from \( o \) to \( k \). For any element \( a \) of \( o \) such that \( \alpha ^s = \alpha \), we have

\[
\phi (\alpha) a ^m = \phi (\alpha).
\]

Therefore we shall regard \( o(0') \) as \( GF(q ^{m+n}) \) \( \otimes k \).

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

\[
\begin{array}{ccc}
o & \xrightarrow{\phi} & k \\
\uparrow \phi_{W(k_0)} & & \uparrow \phi_{k_0} \\
W(k_0) & \xrightarrow{\phi} & k_0
\end{array}
\]

where \( \phi_{W(k_0)} \) is the desired embedding and \( \phi_{k_0} \) is the natural embedding of \( k_0 \) into \( k \).

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

\[
\phi_{W(k_0)}: \sum \psi_0 (x_i) p^i \mapsto \sum \psi(x_i) p^i
\]

where \( \psi \) (resp. \( \psi_0 \)) denotes the unique multiplicative representation of \( k_0 \) to \( o \) (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 \( n = 1 \), \( m = 0 \) we have the followings:

a) Endo \((H) - o' = \mathbb{Z}_p [w', \pi']\)

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

b) \( \pi' \) is a root of an Eisenstein polynomial of degree \( e' = e/d \) over \( \mathbb{Z}_p [w'] \).
Proof. We shall set \( k_0 = GF(q^{m+n}) \cap k \). Then we easily obtain

\[ W(k_0) \subset o' , \]

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

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

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

\[ dx + ey = (d, e) , \]

therefore we have

\[ \nu(p^y a^x) = (d, e) \]

and

\[ p^y a^x \in o' . \]

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

\[ \nu(\pi') | e . \]

From now on we shall denote \( d = \nu(\pi') \). For any element \( \beta \) of \( o' \) we have

\[ \psi \circ \phi(\beta) \in W(k_0) \]

and

\[ \psi \circ \phi(\beta) = \beta \mod p . \]

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

\[ \beta - \psi \circ \phi(\beta) = 0 \mod \pi' o . \]

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

\[ \alpha_{-1} = 0 \]

\[ \alpha_i = \psi \circ \phi((\alpha - \alpha_{i-1})/\pi^i) \]

and

\[ \alpha_i = \alpha_{i-1} + x_i \pi^i \]

for \( i \geq 0 \). Then we have

\[ \alpha = \sum_{i=0}^{\infty} x_i \pi^i . \]

As is easily seen \( o' \) is complete as a subring of \( o \). Therefore we have
\[ o' = W(k_0)[[\pi']] \]
as a subring of \( o \). Since \( \nu(\pi'^e) = \nu(p) \) and other hand \( W(k_0) \) is complete, there exists an Eisenstein polynomial \( f \) of degree \( e' = \ell/d \) over \( W(k_0) \) such that \( f(\pi') = 0 \).

Thus we have
\[ o' = W(k_0)[\pi'] \]
as a subring of \( o \), by approximation. Since \( f \) is irreducible over \( W(k_0) \) we can regard \( W(k_0)[\pi'] \) as \( W(k_0)[x]/(f(x)) \). Therefore we have
\[ o' = \mathbb{Z}_p[\omega', \pi'] \]

Now our proof is complete.

**Corollary.** If \( m > 0 \) or \( m = 0, n = 1 \) and moreover \( e = 1 \), then we have
\[ \text{End}_o(H) = \mathbb{Z}_p[\omega'] \]

OSAKA UNIVERSITY

---

**References**


