JP Journal of Algebra, Number Theory and Applications
© 2013 Pushpa Publishing House, Allahabad, India
Published Online: February 2014
Available online at http://pphmj.com/journals/jpanta.htm
Volume 31, Number 2, 2013, Pages 75-90

REPRESENTATION OF ENDOMORPHISMS OF A MODULE OVER A VALUATION DOMAIN

Hiroyuki Ishibashi

Department of Mathematics
Josai University
Sakado, Saitama 350-02
Japan
e-mail: hishi@math.josai.ac.jp

Abstract

We study a representation of an arbitrary endomorphism σ on a free module M of a finite rank n over a valuation domain R, that is, factorize M into a direct sum of some free submodules determined by σ, give a sufficient condition for σ to have the rational canonical form, find a basis for M over R relative to which the matrix of σ is a sum of a lower triangular matrix and a super diagonal matrix, and show that for some simple ring extension of R the natural prolongation of σ has the rational canonical form.

1. Introduction

A matrix representation of a linear transformation of a free module over a commutative ring depends on the choice of a basis for the module.

So, it will be natural to seek a nice basis relative to which the matrix of the transformation is expressed in a simple form. On this demand, many

Received: October 24, 2013; Accepted: November 23, 2013

2010 Mathematics Subject Classification: 15A04, 15A23, 15A33.

Keywords and phrases: rational canonical form, system of invariants, Jordan normal form, minimal polynomial, characteristic polynomial, endomorphism ring of a module, classical groups.

excellent forms of linear transformations were devised, say, diagonal forms, triangular forms, rational canonical forms, Jordan normal forms, etc., and the conditions for them under which linear transformations have such simple forms were investigated.

In the present paper, among those forms, we will be especially attracted our attention to the rational canonical forms of endomorphisms of modules.

It was first introduced by Frobenius in the late 1800s. Since then much of the results concerning it appeared and have been expanded in various directions.

For instance Matthews [16] showed that a square matrix A over fields is similar to a block diagonal H of hyper companion matrices and gave an algorithm to get P satisfying that $H = PAP^{-1}$. Also, Huang [9], Beard [3] and others pursued the study of the rational canonical forms in various situation and obtained many important and useful results.

However, the methods they contrived were applicable only when the scalars form a field or a skew field.

In this note we will try to deal with the theory of the rational canonical forms in some more general setting for the underlying rings, that is, we will take a valuation domain instead of a field, and obtain the results stated in the abstract. The details of the theorem will be stated in the next section after providing necessary preparation.

On the other hand it is well known that the classical groups have various generating systems. Let σ be an arbitrary element of a group. If we fix a set S of generators of the group, then the minimal number of factors expressing σ as a product of elements of $S \cup S^{-1}$ is called the *length* of σ and denoted by $\ell(\sigma)$.

Dieudonné [5] determined $\ell(\sigma)$ for σ in the various classical groups with its generating sets. The generalization of this length problem to valuation rings or to semi local semi hereditary rings was achieved by the author in 1970s to 1980s (see Ishibashi [10, 11, 12]).

One can see in Hahn and O'Meara [7], Knus [13], McDonald [15] and Baeza [2], how the theory of classical groups over fields has been developed to the theory over rings.

As for the fundamental results in basic algebra and the rational canonical forms are seen in any of Herestein [8], Cohn [4] and Lang [14].

2. Statements of the Theorem and the Corollary

Let R be an integral domain and M be a free module of rank n over R with a basis $X = \{x_1, x_2, ..., x_n\}$. We write $\operatorname{End}_R M$ to denote the algebra over R of all endomorphisms of M over R, and σ denotes an arbitrary element in $\operatorname{End}_R M$. We consider the quotient field F of R to be a ring extension of R. In other words, we will regard R as a subring of F, and thus F is a module over R.

This allows us to define a coefficient extension $\hat{M}$ of M by

$$\hat{M} = F \otimes_R M = \bigoplus_{i=1}^{n} F(1 \otimes x_i),$$

which is an n-dimensional vector space over F with a basis

$$\hat{X} = \{1 \otimes x_i \,|\, 1 \leq i \leq n\}.$$

Therefore, identifying x_i with $1 \otimes x_i$ for $i = 1, 2, ..., n,$ we take $X = \hat{X}$ as a basis for $\hat{M}$ over F. Further, since R is a subring of F, $\hat{M}$ the module over F is also a module over R, consequently M is a submodule of $\hat{M}$ over R.

In the same way we define a linear transformation $\hat{\sigma}$ by

$$\hat{\sigma} = 1_F \otimes \sigma \in \operatorname{End}_F \hat{M},$$

where 1_F denotes the identity linear transformation of the R-module F. The endomorphism $\hat{\sigma}$ is frequently called a *prolongation* of σ on M to $\hat{M}$. Clearly $\sigma = \hat{\sigma}|_M$, the restriction of $\hat{\sigma}$ to M. We may use σ for $\hat{\sigma}$ if their matrices are the same.

The polynomial ring in *t* over *R* is denoted by $R[t]$. Similarly, $F[t]$ is the one in *t* over *F*. The module $\hat{M}$ will be given a module structure over $F[t]$ if we define the scalar multiplication by $f(t)x = f(\hat{\sigma})x$ for $f(t) \in F(t)$ and $x \in \hat{M}$.

An integral domain *R* is called a *valuation domain* if for any nonzero *a* and *b* in *R* either *a* divides *b*, or *b* divides *a*, i.e., $a|b$ or $b|a$. We know that a valuation domain *R* is a local ring of which unique maximal ideal $\mathfrak{m}$ is the set of all non-units in *R*.

For σ in $\mathrm{End}_R M$ if *P* is the matrix of σ relative to a basis *X* for *M*, i.e., $\sigma^t X = P^t X$, we write

$$\sigma \simeq_X P,$$

where ${}^t X$ denotes the transpose of *X*.

For a monic polynomial

$$f(t) = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + t^n, \quad a_i \in F$$

in $F[t]$, the matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \cdots & \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix}$$

is called the *companion matrix* of $f(t)$ and denoted by $C(f(t))$ or $C(f)$.

With these preparations we now describe our theorem and the corollary. The theorem consists of three results (a), (b) and (c). In (a) we will factorize *M* into a direct sum and compose some σ-invariants direct summands of *M*, and in (b) and (c) we will give some matrix representations of σ relative to some bases for M over R. In the corollary, for a simple ring extension R° of R we will show that the natural prolongation σ° of σ has its rational canonical form.

To save symbols we will use a letter X to denote various bases for M over R if there is no confusion. Also we will say the rational canonical form of σ for saying that of the matrix of σ.

Theorem. *Let R be a valuation domain, M be a free module of rank n over R, and σ be an element in $End_R M$. For the quotient field F of R let $\hat{M} = F \otimes_R M$ and $\hat{\sigma} = 1_F \otimes \sigma \in End_F \hat{M}$, and for the polynomial ring $F[t]$ in t over F let $\mathcal{F} = \{f_1(t), f_2(t), ..., f_m(t)\}$ in $F[t]$ be the system of invariants of $\hat{\sigma}$. Further write $n_j = \deg f_j(t)$ for $j = 1, 2, ..., m$.*

Then, there exist $y_1, y_2, ..., y_m$ in M which are generators of cyclic factors of $\hat{M}$ as a $F[t]$-module, i.e.,

$$\hat{M} = F[t]y_1 \oplus F[t]y_2 \oplus \cdots \oplus F[t]y_m, \quad y_j \in M, \quad j = 1, 2, ..., m,$$

and for which we have the following (a), (b) *and* (c):

(a) *There are free submodules $M_1, M_2, ..., M_m$ of M over R such that*

(i) $M = M_1 \oplus M_2 \oplus \cdots \oplus M_m$ *with* $n_j = \operatorname{rank} M_j = \deg f_j$ *for* $j =$ $1, 2, ..., m,$ *and if we set* $L_j = M_1 \oplus M_2 \oplus \cdots \oplus M_j,$ *we have*

(ii) $\sigma L_j \subseteq L_j$ *for* $j = 1, 2, ..., m.$

(b) *For* $j = 1, 2, ..., m$ *set*

$$Y_j = \{y_j, \sigma y_j, ..., \sigma^{n_j - 1} y_j\}$$

and

$$Y = Y_1 \cup Y_2 \cup \ldots \cup Y_m.$$

Then, we have a basis X for M over R such that

$$^tY = A^tX,$$

where $A = (a_{pq}) \in M_n(R)$ *is lower triangular with* $a_{pp} \neq 0$ *for* $p =$ $1, 2, ..., n.$

In particular, if a_{pp} *'s are all units in R for* $p = 1, 2, ..., n,$ *then* σ *has its rational canonical form*

$$\sigma \simeq_Y C = \begin{pmatrix} C(f_1) & & & 0 \\ & C(f_2) & & \\ & & \ddots & \\ 0 & & & C(f_m) \end{pmatrix},$$

where $\mathcal{F} = \{f_1, f_2, ..., f_m\}$ *in* $R[t]$ *is the system of invariants of* $\hat{\sigma}$*.*

(c) *Relative to X in* (b) *let B be the matrix of* σ, *i.e.,* $\sigma^tX = B^tX.$ *Then, B admits a partition into blocks such that*

$$B = \begin{pmatrix} B_{11} & 0 & 0 & \cdots & 0 \\ B_{21} & B_{22} & 0 & \cdots & 0 \\ & & & \cdots & \\ B_{m1} & B_{m2} & B_{m3} & \cdots & B_{mm} \end{pmatrix} \in M_n(R),$$

where B_{jk} *is in* $M_{n_jn_k}(R)$ *for* $j = 1, 2, ..., m$ *and* $k = 1, 2, ..., j$ *and* B_{jj} *is a sum of a lower triangular matrix and an upper diagonal matrix, i.e., in a form*

$$B_{jj} = \begin{pmatrix} * & * & 0 & 0 & \cdots & 0 \\ * & * & * & 0 & \cdots & 0 \\ & & & & \cdots & \\ * & * & * & * & \cdots & 0 \\ * & * & * & * & \cdots & * \\ * & * & * & * & \cdots & * \end{pmatrix}.$$

Corollary. *In* (b) *of the Theorem there exists a diagonal element a of A such that if we set*

$$R^{\circ} = R[a^{-1}], \quad a^{-1} \in F,$$

a simple ring extension of R in F and

$$M^{\circ} = R^{\circ} \otimes_R M \simeq \oplus_{i=1}^{n} R^{\circ} x_i^{\circ} \ \text{ for } \ x_i^{\circ} = 1 \otimes x_i,$$

then

$$X^{\circ} = \{x_i^{\circ} = 1 \otimes x_i \,|\, i = 1, 2, ..., n\}$$

is a basis for M° *over* R° *and*

$$\sigma^{\circ} = 1_{R^{\circ}} \otimes \sigma \in \mathrm{End}_{R^{\circ}} M^{\circ}$$

has the rational canonical form

$$\sigma^{\circ} \simeq_{X^{\circ}} A^{\circ} = \begin{pmatrix} C(f_1) & & & 0 \\ & C(f_2) & & \\ & & \ddots & \\ 0 & & & C(f_m) \end{pmatrix} \in M_n(R^{\circ}),$$

where $\mathcal{F} = \{f_1, f_2, ..., f_m\}$ *in* $R^{\circ}[t]$ *is the system of invariants of* σ°.

3. Proofs for the Theorem and the Corollary

3.1. Proof for the Theorem

Since F is a field and $\hat{M} = F \otimes_R M$ is a vector space of dimension n over F, there exists a system of invariants $\mathcal{F} = \{f_1, f_2, ..., f_m\}$ of $\hat{\sigma} = 1_F \otimes \sigma$ with f_j's monic for $j = 1, 2, ..., m$ and $f_1 \,|\, f_2 | \cdots | f_m$ in $F[t]$ (see Lang [11, p. 151, Theorem 7.7]).

More precisely for $f(t) \in F(t)$ and $x \in M$ if we define a scalar multiplication by

$$f(t)x = f(\sigma)x,$$

$\hat{M}$ is endowed with a structure of a module over $F[t]$. Hence by the structure theorem of a finitely generated torsion module over a PID $\hat{M}$ is factorized into a direct sum of m cyclic submodules $M'_1, M'_2, ..., M'_m$ of $\hat{M}$ over $F[t]$.

Therefore, if we denote those generators of $M'_1, M'_2, ..., M'_m$ in $\hat{M}$ by $\{y_1, y_2, ..., y_m\}$, respectively, we have an expression

$$\hat{M} = M'_1 \oplus M'_2 \oplus \cdots \oplus M'_m \tag{3.1}$$

with

(i) $M'_j = F[t]y_j = Fy_j \oplus F\sigma y_j \oplus \cdots \oplus F\sigma^{n_j-1}y_j$,

(ii) $n_j = \deg f_j = \dim M'_j$,

(iii) $f_j(\hat{\sigma}) = 0$ for $j = 1, 2, ..., m$ and

(iv) $n = n_1 + n_2 + \cdots + n_m$.

In (3.1), since F is the quotient field of R, by a suitable scalar multiplication we may choose y_j an element in M for $j = 1, 2, ..., m$, that is, we may assume that

$$\{y_1, y_2, ..., y_m\} \subseteq M, \tag{3.2}$$

in particular,

$$\hat{\sigma}y_j = \sigma y_j \text{ for } j = 1, 2, ..., m.$$

As we have mentioned in the previous section we have a basis

$$X = \{x_1, x_2, ..., x_n\}$$

for M over R. Also for $\{y_1, y_2, ..., y_m\}$ above we will set

$$Y = Y_1 \cup Y_2 \cup \ldots \cup Y_m \tag{3.3}$$

with

$$Y_j = \{y_j, \sigma y_j, \ldots, \sigma^{n_j - 1} y_j\},$$

i.e.,

$$Y = \{y_1, \sigma y_1, \ldots, \sigma^{n_1 - 1} y_1, \ldots, y_m, \sigma y_m, \ldots, \sigma^{n_m - 1} y_m\}.$$

Therefore, by (3.1)

$$Y \text{ is a basis for } \hat{M} \text{ over } F. \tag{3.4}$$

Further we have

$${}^tY = A^tX \text{ for some } A = (a_{pq}) \in M_n(R). \tag{3.5}$$

The following is the key lemma for the proof of the Theorem.

Lemma 3.1. *There exists a basis X for M over R such that A in* (3.5) *is lower triangular with non-zero diagonal elements.*

Proof. For A in (3.5) suppose that there exists r in $\{1, 2, \ldots, n\}$ such that the top left corner of A is an $(r-1) \times (r-1)$ lower triangular matrix, that is,

$$A = \begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ & & & \cdots & & & \cdots & \\ a_{(r-1)1} & a_{(r-1)2} & a_{(r-1)3} & \cdots & a_{(r-1)(r-1)} & 0 & \cdots & 0 \\ a_{r1} & a_{r2} & a_{r3} & \cdots & a_{r(r-1)} & a_{rr} & \cdots & a_{rn} \\ & & & \cdots & & & \cdots & \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{n(r-1)} & a_{nr} & \cdots & a_{nn} \end{pmatrix}.$$

Since by (3.4) Y is a basis for $\hat{M}$ over F, it is linearly independent over F, and so at least one a_{rq} in $\{a_{rr}, a_{r(r+1)}, \ldots, a_{rn}\}$ is not zero, $r \leq q \leq n$. Here, since R is a valuation domain, there is k in $\{r, r+1, \ldots, n\}$ such that $a_{rk} \mid a_{rk'}$ in R for any $k' = r, r+1, \ldots, n$.

Therefore, by a suitable renumbering of the basis elements

$\{x_r, x_{r+1}, ..., x_n\}$ in X we may assume that $k = r$, i.e.,

$$a_{rr} \mid a_{rk'} \text{ in } R$$

for any $k' = r, r+1, ..., n$.

From this if we set

$$x'_r = x_r + a_{rr}^{-1} a_{r(r+1)} x_{r+1} + \cdots + a_{rr}^{-1} a_{rn} x_n,$$

we find that

$$X' = \{x_1, ..., x_{r-1}, x'_r, x_{r+1}, ..., x_n\}$$

is still a basis for M over R and relative to which A is expressed as

$$A = \begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ & & & \cdots & & & \cdots & \\ a_{r1} & a_{r2} & a_{r3} & \cdots & a_{rr} & 0 & \cdots & 0 \\ a_{(r+1)1} & a_{(r+1)2} & a_{(r+1)3} & \cdots & a_{(r+1)r} & a_{(r+1)(r+1)} & \cdots & a_{rn} \\ & & & \cdots & & & \cdots & \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{n(r+1)} & a_{n(r+1)} & \cdots & a_{nn} \end{pmatrix}.$$

This, by induction in r, implies that there exists a basis X for M over R relative to which A is lower triangular with non-zero diagonal elements i.e., we obtain

$$A = \begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ & & & \cdots & \\ a_{(n-1)1} & a_{(n-1)2} & a_{(n-1)3} & \cdots & 0 \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix} \tag{3.6}$$

where $a_{11}, a_{22}, ..., a_{nn} \neq 0$. □

For X in Lemma 3.1 we define a partition of X as

$$X = X_1 \cup X_2 \cup \ldots \cup X_m$$

where for $j = 1, 2, ..., m$ the set $X_1 \cup X_2 \cup \ldots \cup X_j$ is the first $n_1 + n_2 + \cdots + n_j$ elements of X. Therefore, if we write

$$x_k^{(j)} = x_{n_1+n_2+\cdots+n_{j-1}+k}$$

for $j = 1, 2, ..., m$ and $k = 1, 2, ..., n_j$, we have

$$X_j = \{x_1^{(j)}, x_2^{(j)}, ..., x_{n_j}^{(j)}\}$$

for $j = 1, 2, ..., m$.

For a subset S of M, we write $\langle S \rangle_R$ for the submodule spaned by S over R, i.e.,

$$\langle S \rangle_R = \left\{ \sum^{finite} as \,|\, a \in R,\ s \in S \right\}.$$

Similar notation $\langle S \rangle_F$ is adopted to denote the same object over F for R.

(I) Proof for (a) of the Theorem

We write

$$M_j = \langle X_j \rangle_R \tag{3.7}$$

for the submodule M_j spanned by X_j over R. Then, since $X = X_1 \cup X_2 \cup \ldots \cup X_m$ is a basis for M over R, we have

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_m \tag{3.8}$$

with

$$\text{rank}\, M_j = n_j = \deg f_j$$

for $j = 1, 2, ..., m$. This is the first half of (a).

To show the last half of (a) we use Lemma 3.1, so we have

$${}^tY = A^tX, \quad A \in M_n(R), \tag{3.9}$$

where A is lower triangular with all the diagonal elements non-zero. This implies that A is invertible in $M_n(F)$ and so

$$\langle Y_1 \cup Y_2 \cup \ldots \cup Y_j \rangle_F = \langle X_1 \cup X_2 \cup \ldots \cup X_j \rangle_F$$

for $j = 1, 2, \ldots m.$ Hence,

$$\langle Y_1 \cup Y_2 \cup \ldots \cup Y_j \rangle_F \cap M = \langle X_1 \cup X_2 \cup \ldots \cup X_j \rangle_F \cap M. \quad (3.10)$$

Since X is a basis for M over R and simultaneously it is a basis for $\hat{M}$ over $\hat{F},$ we find that the right hand side of (3.10) coincides with

$$\langle X_1, X_2, \ldots, X_j \rangle_R = M_1 \oplus M_2 \oplus \cdots \oplus M_j = L_j, \quad (3.11)$$

i.e.,

$$L_j = \langle Y_1 \cup Y_2 \cup \ldots \cup Y_j \rangle_F \cap M.$$

Since both $\langle Y_1 \cup Y_2 \cup \ldots \cup Y_j \rangle_F$ and M are σ-invariant, so is L_j, that is,

$$\sigma L_j \subseteq L_j \text{ for } j = 1, 2, \ldots, m \quad (3.12)$$

as was to be shown.

(II) Proof for (b) of the Theorem

Since Lemma 3.1 is the first half of (b), the rest to be shown is the last half. Since the triangular matrix A is in $M_n(R),$ if the diagonal elements of A are all units in R, Y becomes a basis for M over R. Consequently, we get the last half of (*b*).

(III) Proof for (c) of the Theorem

Put $l_0 = 0$ and $l_j = n_1 + n_2 + \cdots + n_j$ for $j = 1, 2, \ldots, m,$ so $l_j = \operatorname{rank} L_j$ for $j = 1, 2, \ldots, m.$ Then, observing the form of B_{jj} in the statement of (c) in the previous section, we find that (c) is equivalent to

$$\text{(i) } \sigma x_i \in \sum_{\lambda=1}^{i+1} R x_\lambda \text{ if } l_{j-1} < i < l_j \text{ for } j = 1, 2, \ldots, m \quad (3.13)$$

and

(ii) $\sigma x_i \in \sum_{\lambda=1}^{i} Rx_\lambda$ if $i = l_j$ for $j = 1, 2, ..., m.$

Further, for $f_j(t)$ in $\mathcal{F}$ if we express

$$f_j(t) = c_{j0} + c_{j1}t + \cdots + c_{j(n_j-1)}t^{n_j-1} + t^{n_j}, \quad c_{jh} \in F$$

for $j = 1, 2, ..., m$ and $h = 0, 1, ..., n_j - 1,$ we have

$$\sigma^{n_j} y_j = -c_{j0}y_j - c_{j1}\sigma y_j - \cdots - c_{j(n_j-1)}\sigma^{n_j-1}y_j, \quad c_{jh} \in F \quad (3.14)$$

for $j = 1, 2, ..., m$ and $h = 0, 1, ..., n_j - 1.$

On the other hand, by (3.9) we have ${}^tY = A^tX$ with A lower triangular, hence

$$\sigma^{k-1}y_j = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{ii}x_i \text{ with } i = l_{j-1} + k \quad (3.15)$$

for $j = 1, 2, ..., m$ and $k = 1, 2, ..., n_j.$

Substituting the right hand side of (3.15) for $\sigma^h y_j$ in (3.14) for $h = k - 1 = 0, 1, ..., n_j - 1,$ we have

$$\sigma^{n_j} y_j \in \sum_{i=1}^{l_j} Rx_i \text{ for } j = 1, 2, ..., m. \quad (3.16)$$

Now we start our proof for (c). Since (c) is equivalent to (3.13), we prove (3.13) by induction in i for $i = 1, 2, ..., n.$ Let us assume that (c) holds for $i = 0$ and so $i \geq 1.$

First we treat the case (i) in (3.13), i.e., we are in case where $l_{j-1} < i < l_j.$ So we have $k = 1, 2, ..., n_j - 1,$ if we set $i = l_{j-1} + k.$ This enable us to apply (3.15) to $(i + 1, k + 1)$ for (i, k) and we get

$$\sigma^k y_j = a_{(i+1)1}x_1 + a_{(i+1)2}x_2 + \cdots + a_{(i+1)(i+1)}x_{i+1}, \tag{3.17}$$

where $i + 1 = l_{j-1} + k + 1$ for $j = 1, 2, ..., m$ and $k = 1, 2, ..., n_j - 1.$

Multiplying the both sides of (3.15) by σ, we have

$$\sigma^k y_j = a_{i1}\sigma x_1 + a_{i2}\sigma x_2 + \cdots + a_{ii}\sigma x_i \text{ with } i = l_{j-1} + k$$

for $i = 1, 2, ..., n,$ $j = 1, 2, ..., m$ and $k = 1, 2, ..., n_j.$

Since by Lemma 3.1 $a_{ii} \neq 0$ for $i = 1, 2, ..., n,$ this gives us

$$\sigma x_i = a_{ii}^{-1}(\sigma^k y_j - a_{i1}\sigma x_1 - a_{i2}\sigma x_2 - \cdots - a_{i(i-1)}\sigma x_{i-1}). \tag{3.18}$$

Substituting the right hand side of (3.17) for $\sigma^k y_j$ in (3.18), we have

$$\sigma x_i = a_{ii}^{-1}\left(\sum_{\lambda=1}^{i+1} a_{(i+1)\lambda}x_\lambda - \sum_{\mu=1}^{i-1} a_{i\mu}\sigma x_\mu\right). \tag{3.19}$$

Therefore applying our inductive hypothesis in *i* to $\sum_{\mu=1}^{i-1} a_{i\mu}\sigma x_\mu$ in (3.19), we have

$$\sum_{\mu=1}^{i-1} a_{i\mu}\sigma x_\mu \in \bigoplus_{\mu=1}^{i} Rx_\mu,$$

hence (3.19) yields

$$\sigma x_i = a_{ii}^{-1}\left(\sum_{\lambda=1}^{i+1} b_{i\lambda}x_\lambda\right) \tag{3.20}$$

for some $b_{i\lambda} \in R.$

Here since σx_i in (3.20) is in *M*, so is the right hand side of (3.20). Further, since $X = \{x_1, x_2, ..., x_n\}$ is a basis for *M* over *R* and simultaneously a basis for $\hat{M}$ over *F*, we conclude that $a_{ii}^{-1}b_{i\lambda}$ in (3.20) belongs to *R* for $l_{j-1} < i < l_j,$ $j = 1, 2, ..., m$ and $\lambda = 1, 2, ..., i + 1.$ Thus we have proved (i) of (3.13).

Next we show (ii) of (3.13), i.e., $\sigma x_i \in \sum_{\lambda=1}^{i} Rx_\lambda$ for $i = l_j$. Since $i = l_{j-1} + k$ in (3.15) we have $k = n_j$, hence (3.15) implies that

$$\sigma^{n_j - 1} y_j = a_{l_j 1} x_1 + a_{l_j 2} x_2 + \cdots + a_{l_j l_j} x_{l_j},$$

and so multiplying the both sides of the equation above by σ and rearranging the terms we have

$$\sigma x_{l_j} = a_{l_j l_j}^{-1} \left(\sigma^{n_j} y_j - \sum_{\mu=1}^{l_j - 1} a_{l_j \mu} \sigma x_\mu \right).$$

Hence by (3.16), (i) of (3.13) and the inductive hypothesis for (ii) of (3.13) we obtain

$$\sigma x_{l_j} = a_{l_j l_j}^{-1} \left(\sum\nolimits_{\mu=1}^{l_j} c_{l_j \mu} x_\mu \right).$$

Now in the same way as the proof for (i) of (3.13) we find that $a_{l_j l_j}^{-1} c_{l_j \mu}$ is in R for $j = 1, 2, \ldots, m,$ which verifies that (ii) of (3.13) holds.

Thus, we have proved (c), and completed the proof for the Theorem.

3.2. Proof for the Corollary

Let S be the set of diagonal elements of A in (b) of the Theorem, i.e.,

$$S = \{a_{ii} \in A \,|\, i = 1, 2, \ldots, n\}.$$

Since $a_{ii} \neq 0$ for $i = 1, 2, \ldots, n$ and R is a valuation domain, we have an element a in S such that a is a multiple for all a_{ii} in S, i.e.,

$$a_{ii} \,|\, a \text{ in } R \text{ for } i = 1, 2, \ldots, n.$$

Then, if we set $R^\circ = R[a^{-1}]$, then $|A|$ is a unit in R° and thus the last half of (b) of the Theorem gives us the corollary.

References

[1] S. N. Afriat, On the rational canonical form of a matrix, J. Linear and Multilinear Algebra 1 (1973), 185-186.

[2] R. Baeza, Quadratic forms over semi-local rings, Lecture Note in Math. 655, Springer, Berlin, Heidelberg, New York, 1978.

[3] J. T. B. Beard, Jr., A rational canonical form for matrix fields, Acta Arith. 25 (1973/74), 331-335.

[4] P. M. Cohn, Algebra, 2nd ed., Vol. 1, John Wiley and Sons, New York, 1982.

[5] J. Dieudonné, Sur les générateurs des groupes classiques, Summa Brasil Math. 3 (1955), 149-178.

[6] E. W. Ellers and H. Ishibashi, Factorization of transformations over a valuation ring, Linear Algebra Appl. 85 (1987), 17-27.

[7] A. J. Hahn and O. T. O'Meara, The Classical Groups and *K*-theory, Grundlehren der Mathematischen Wissenschaften, Vol. 291, Springer-Verlag, Berlin, New York, Tokyo, 1989.

[8] I. N. Herstein, Topics in Algebra, 2nd ed., Vol. 1, John Wiley and Sons, 1982.

[9] L. P. Huang, The primary rational canonical form and eigenvalues of algebraic matrices over a skew field, Acta Math. Sinica (Chin. Ser.) 41 (4) (1998), 871-880.

[10] H. Ishibashi, Generators of $U_n(V)$ over a quasi semilocal semihereditary domain, J. Algebra 60 (1) (1979), 199-203.

[11] H. Ishibashi, Generators of orthogonal groups over valuation rings, Canad. J. Math. 33 (1981), 116-128.

[12] H. Ishibashi, Generators of $U_n(V)$ over a quasi-semilocal semihereditary ring, Canad. J. Math. 33 (1981), 1232-1244.

[13] M. A. Knus, Quadratic and Hermitian Forms over Rings, Grundlehren der Mathematischen Wissenschaften, Vol. 294, Springer-Verlag, Berlin, New York, Tokyo, 1991.

[14] S. Lang, Algebra, 3rd ed., Addison Wesley, Tokyo, 1999.

[15] B. R. McDonald, Geometric Algebra over Local Rings, Dekker, New York, 1976.

[16] K. R. Matthews, A rational canonical form algorithm (English), Math. Bohem. 117(3) (1992), 315-324.