3.11 THE RING OF ENDOMORPHISMS OF A FINITELY GENERATED MODULE OVER A P.I.D.

An interesting problem is that of determining the $n \times n$ matrices $B$ with entries in a field $F$ which commute with a given matrix $A \in M_n(F)$. This translates to the geometric problem of determining the linear transformations $U$ in an $n$-dimensional vector space $V$ over $F$ which commute with a given linear transformation $T$ of $V$ over $F$. Then $U$ is an endomorphism of the additive group of $V$ such that $U(ax) = a(Ux), a \in F,$ and $U(Tx) = T(Ux)$. Regarding $V$ as an $F[x]$-module, as before, the last condition becomes $U(ax) = a(Ux)$, which implies that $U(ax) = a(Ux)$ for any polynomial $f(x) \in F[x]$ and so $U$ is an endomorphism of $V$ regarded as an $F[x]$-module. Conversely, this condition is sufficient to insure that $U$ is a linear transformation in $V$ over $F$ which commutes with $T$, since it includes the facts that $U$ is a group endomorphism, that $U(ax) = a(Ux), a \in F,$ and $U(Tx) = U(ax) = a(Ux) = T(Ux)$.

More generally, we now consider the problem of explicitly determining the ring $D$ of endomorphisms (that is, $\text{Hom}(M, M)$) of a finitely generated module $M$ over a p.i.d. $D$. We begin with a decomposition $M = Dz_1 \oplus Dz_2 \oplus \cdots \oplus Dz_s$, where $ann z_i \supseteq ann z_{i+1} \supseteq \cdots \supseteq ann z_s$, and $ann z_i = (\alpha_i)$ for $i \leq r$ but $ann z_i = 0$ if $i > r$. Let $\eta \in D^r$ and suppose $\eta z_i = \sum a_i \alpha_i$, where $a_i \in D$. Then $\eta = \sum a_i \eta z_i = \sum a_i \eta z_i = \sum a_i \eta z_i = \sum a_i w_i$.

This shows (as we know already) that $\eta$ is determined by its effect on the generators $z_i$ of $M$. Moreover, $\eta w_i = \eta (z_i \alpha_i) = \eta (\alpha_i z_i) = 0$, which shows that $ann w_i \supseteq ann z_i$, so if $ann w_i = (\alpha_i)$, then $\eta z_i = (\alpha_i)$ if $i \leq r$, and $\eta z_i = 0$ if $i > r$.

Conversely, suppose that for each $i$ we pick an element $w_i \in M$ such that $ann w_i = ann z_i$. Suppose $x \in M$ and $x = \sum a_i \alpha_i = \sum b_i \beta_i$. Two representations of $x$. Then we have $a_i = b_i \varepsilon_{ann} \alpha_i$. Hence $a_i = b_i \varepsilon_{ann} \alpha_i$, and consequently $\sum a_i \alpha_i = \sum b_i \beta_i$. This shows that $\eta: \sum a_i \alpha_i = \sum a_i \eta \alpha_i$ is a map of $M$ into $M$. Direct verification shows also that $\eta \in D$.

Our result is the following. We have a bijection $\eta \rightarrow (w_1, w_2, \ldots, w_r)$ of the ring $D^r = \text{Hom}(M, M)$ onto the set of $r$-tuples of elements of $M$ satisfying $ann w_i \supseteq ann z_i$. We now write $w_i = \sum b_i \beta_i$, $b_i \in D$, and we associate with the ordered set $(w_1, w_2, \ldots, w_r)$ the matrix

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1r} \\ b_{21} & b_{22} & \cdots & b_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \cdots & b_{rr} \end{pmatrix}$$

(45)

in the ring $M(D)$ of $r \times r$ matrices with entries in $D$. This matrix may not be uniquely determined since any $b_{ij}$ may be replaced by $b_{ij} + b_{ij} (mod D)$ if $i \neq j$. This is the only alteration which can be made without changing the $w_i$. The condition that $ann w_i \supseteq ann z_i$ is equivalent to

$$d_i b_{ij} = 0 (mod D)$$

(46)

This, of course, means that there exist $c_{ij} \in D$ such that $d_i b_{ij} = c_{ij} d_j$. Hence (46) is equivalent to the following condition on the matrix $B$ of (45): there exists a $C \in M(D)$ such that

$$\text{diag}(d_1, d_2, \ldots, d_r) B = C \text{diag}(d_1, d_2, \ldots, d_r)$$

(47)

The set $R$ of matrices $B$ satisfying (47) is a subring of $M(D)$. Any $B \in R$ determines an $\eta \in D^r$ such that $\eta z_i = \sum b_i \alpha_i$. It is easy to verify (as in the special case of a free module treated in section 3.4) that the map $B \rightarrow \eta$ is an epimorphism of $R$ onto $D$. It is clear that $\eta = 0$ if and only if $b_{ij} = 0 (mod D)$ for $B = (b_{ij})$. Hence the kernel $K$ of our homomorphism is the set of matrices $B$ such that,

$$\eta \in D$$

(48)

Where $Q = M(D)$. We remark that matrices of this form automatically satisfy (47). This implies

THEOREM 3.15. Let $M = D \oplus D \oplus \cdots \oplus D s$ where the order ideals $ann z_i = (\alpha_i)$ satisfy $\alpha_i \supseteq \alpha_{i+1} \supseteq \cdots \supseteq \alpha_s$. Then the ring $D^r$ of endomorphisms of the $D$-module $M$ is anti-isomorphic to $R[K]$ where $K$ is the ring of matrices $B \in M(D)$ for which there exists a $C \in M(D)$ such that $\text{diag}(d_1, d_2, \ldots, d_r) = B \rightarrow C \text{diag}(d_1, d_2, \ldots, d_r)$. If $M$ is a free module, all the $d_i = 0$. Then $R = M(D)$ and $K = 0$. In this case we have the result of section 3.4. If $s = 1$, so that $M$ is cyclic, the condition for $B \in R$ is trivially satisfied by the commutativity of $D$. Then $D^r = D^s(d)$ where $d = d_1$.

A more explicit determination of the ring of matrices $R$ can be made if we make use of the conditions on the $d_i$ that $d_i d_j$ if $i \leq j \leq r$, and $d_i = 0$ if $i > r$.

The conditions (46) then imply:

1. $b_{ij}$ is arbitrary if $i \geq j$ since in this case $d_i = 0 (mod d_j)$;
2. $b_{ij} = 0$ if $i \leq r$ and $j > r$ since in this case $d_i = 0$ and $d_j = 0$;
3. $b_{ij}$ is arbitrary if $i < j > r$ since $d_i = d_j = 0$ in this case;
4. $b_{ij} = 0 (mod d_i d_j)$ if $i < j \leq r$. 

(49)
Changing the notation slightly we see that $B$ has the form

$$
\begin{bmatrix}
  b_{11} & b_{12}d_1^{-1} & \cdots & b_{1p}d_1^{-1} & 0 & \cdots & 0 \\
  b_{21} & b_{22}d_2^{-1} & \cdots & b_{2p}d_2^{-1} & 0 & \cdots & 0 \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
  b_{r1} & b_{r2} & \cdots & b_{rp} & 0 & \cdots & 0 \\
  b_{r+1,1} & b_{r+1,2} & \cdots & b_{r+1,p} & \cdots & b_{r+1,r} & 0 \\
  \vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \vdots \\
  b_{r+s,1} & b_{r+s,2} & \cdots & b_{r+s,p} & \cdots & b_{r+s,r} & b_{r+s,s}
\end{bmatrix}
$$

(49)

Here the upper right-hand corner consists of $0$'s, all the indicated $b_{ij}$ are arbitrary, and the $(i,j)$-entry for $i < j \leq r$ is $b_{ij}d_i^{-1}d_j$. The conditions that the matrix $K$ are that the $b_{ij} = 0$ if $j > r$, that $b_{ij}$ is divisible by $d_j$ if $i \geq j$ and $j \leq r$, and that $b_{ij}$ is divisible by $d_i$ if $i < j \leq r$. If the module is a torsion module, $r = s$ and (49) reduces to the block of matrix in the upper left-hand corner.

We now specialize $M = V$, where $V$ is the $F[\lambda]$-module determined by a linear transformation $T$ in a finite dimensional vector space $V$ over $F$. This is a torsion module. Any $b_{ij}, i \geq j$, can be replaced by $b_{ij}$ in the same coset mod $d_j$. Hence we may assume $b_{ij}, i < j$, are $b_{ij} < d_j = \deg d_j$ if $i \geq j$. Similarly, we may assume $b_{ij} < d_i$ if $i < j$. Matrices $B \in R$ satisfying these conditions will be called normalized. It is clear that the map $B \rightarrow \eta$ restricted to normalized matrices of $R$ is a bijection into $D$. There is a natural way of regarding $D$ and $R$ as vector spaces over $F$. For $R$ we obtain a module structure over $F$ simply by multiplying all the entries of $B \in R$ by a $F \in F$. For $D$ we define $a \gamma = \gamma(\alpha x)$ (cf. exercise 5, p. 175). Using these vector space structures it is immediate that the set $S$ of normalized matrices contained in $R$ is a subspace and $B \rightarrow \eta$ is an $F[\lambda]$-linear isomorphism of $S$ onto $D$. We are interested in calculating the dimension of $D$ over $F$. In matrix terms, the dimension over $F$ of the vector space of matrices which commute with a given matrix. The isomorphism just established gives us a way of doing this, namely, we may calculate dim $S$. Let $S_{ij}, 1 \leq i, j \leq s$, denote the subspaces of $S$ of normalized matrices having $0$ entries in all places except the $(i,j)$-position. Then dim $S_{ij} = n_j$ if $i \geq j$, and dim $S_{ij} = n_i$ if $i < j$. Since $S$ is the direct sum of the subspaces $S_{ij}$ we have

$$
\text{dim } S = \frac{1}{s} \left( s(s-1)n_1 + \sum_{i=1}^{s-1} (s-i)n_i \right) = \frac{1}{s} \left( 2s^2 - 2s + 1 \right) n_1.
$$

We can state this result in terms of matrices in the following way:

**Theorem 3.16 (Frobenius)** Let $A \in M_n(F)$, $F$ a field, and let $d_1(\lambda), d_2(\lambda), \ldots, d_n(\lambda)$ be the invariant factors $\neq 1$ of $\lambda I - A$. Let $n_i = \deg d_i(\lambda)$. Then the dimensionality of the vector space over $F$ of matrices commutative with $A$ is given by the formula

$$
N = \frac{s}{s-1} \left( 2s - 2 + 1 \right) n_1.
$$

(50)

Of course, this can also be stated in terms of linear transformations. In this form it gives the following

**Corollary.** A linear transformation $T$ is cyclic (that is the corresponding $F[\lambda]$-module is cyclic) if and only if the only linear transformations commuting with $T$ are polynomials in $T$.

**Proof.** $T$ is cyclic if and only if $s = 1$. We also know that $d_1(\lambda)$ is the minimum polynomial $m(\lambda)$ of $T$ and hence if $n_i$ is the dimensionality over $F$ of the ring $F[T]$ of polynomials in $T$ with coefficients in $F$ (see exercise 1, p. 133). If $s = 1$ then (50) gives $N = n_1 = \dim F[T]$. Hence the space of linear transformations commuting with $T$, which, of course, contains $F[T]$, coincides with $F[T]$. If $s > 1$, (50) implies that $N > \sum_{i=1}^{s} n_i > n_1$. Hence there exist linear transformations commuting with $T$ which are not polynomials in $T$. $\square$

**Example**

Let $F = \mathbb{Q}$ and

$$
A = \begin{pmatrix}
1 & 0 & 0 \\
0 & 0 & 1 \\
0 & -1 & 2
\end{pmatrix}
$$

If $T$ is the corresponding linear transformation and the vector space is $\mathbb{Q}[\lambda]$-module over $T$ then $V = \mathbb{Q}[\lambda]e_1 \oplus \mathbb{Q}[\lambda]e_2$. The invariant factors are $\lambda - 1$ and $(\lambda - 1)^2$. The normalized matrices of $R$ have the form

$$
\begin{pmatrix}
 b_{11} & b_{12}(\lambda - 1) \\
 b_{21} & b_{22} + b_{23}(\lambda - 1) \\
 b_{31} & b_{32} + b_{33}(\lambda - 1)
\end{pmatrix}
$$

(51)

Since $I_T = e_1, \lambda I_T = (\lambda - 1)f_2 = -f_2 + 2(\lambda - 1)f_3$, the linear transformation $U$ corresponding to (51) satisfies

$$
Uf_1 = b_{11}f_1 - b_{12}f_2 + b_{13}(\lambda - 1)f_3 \\
Uf_2 = b_{21}f_1 + b_{22}f_2 + b_{23}(\lambda - 1)f_3 \\
U(\lambda f_2 - f_1) = b_{31}f_1 - b_{32}f_2 + b_{33}(\lambda - 1)f_3.
$$