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 trans- formation 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 $F[\lambda]$-module, as before, the last condition becomes $U(\lambda x) = \lambda(Ux)$, which implies that $U(\lambda^k x) = \lambda^k(Ux)$. Then we have $U(f(\lambda)x) = f(\lambda)(Ux)$ for any poly- nomial $f(\lambda) \in F[\lambda]$ and so U is an endomorphism of V regarded as an $F[\lambda]$-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 $U(Tx) = U(\lambda x) = \lambda(Ux) = T(Ux)$.

More generally, we now consider the problem of explicitly determining the ring D' of endomorphisms (that is, $\mathrm{Hom}(M, M)$) 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 $\mathrm{ann}\, z_1 \supset \mathrm{ann}\, z_2 \supset \cdots \supset \mathrm{ann}\, z_s$ and $\mathrm{ann}\, z_i = (d_i) \neq 0$ for $i \leq r$ but $\mathrm{ann}\, z_i = 0$ if $i > r$. Let $\eta \in D'$ and suppose $\eta z_i \ (=\eta(z_i)) = w_i \in M$, $1 \leq i \leq s$. Then if $x \in M$, $x = \sum_1^s a_i z_i$, $a_i \in D$, and hence

$$\eta x = \eta\left(\sum a_i z_i\right) = \sum \eta(a_i z_i) = \sum a_i(\eta z_i) = \sum a_i w_i.$$

This shows (as we know already) that η is determined by its effect on the gener- ators z_i of M. Moreover, $d_i w_i = d_i(\eta z_i) = \eta(d_i z_i) = 0$, which shows that $\mathrm{ann}\, w_i \supset \mathrm{ann}\, z_i$ so if $\mathrm{ann}\, w_i = (g_i)$, then g_i is arbitrary if $i > r$, and $g_i | d_i$ if $i \leq r$.

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

Our result is the following. We have a bijection $\eta \to (w_1, w_2, \ldots, w_s)$ of the ring $D' = \mathrm{Hom}(M, M)$ onto the set of s-tuples of elements of M satisfying $\mathrm{ann}\, w_i \supset \mathrm{ann}\, z_i$. We now write $w_i = \sum b_{ij} z_j$, $b_{ij} \in D$, and we associate with the ordered set $(w_1, w_2, \ldots, w_s)$ the matrix

(45)
$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \cdots & \cdots & \cdots & \cdots \\ b_{s1} & b_{s2} & \cdots & b_{ss} \end{pmatrix}$$

in the ring $M_s(D)$ of $s \times s$ matrices with entries in D. This matrix may not be uniquely determined since any b_{ij} may be replaced by b'_{ij} such that $b'_{ij} \equiv b_{ij} \pmod{d_j}$ if $j \leq r$. This is the only alteration which can be made without changing the w_i. The condition that $\mathrm{ann}\, w_i \supset \mathrm{ann}\, z_i$ is equivalent to

(46)
$$d_i b_{ij} \equiv 0 \pmod{d_j}.$$

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 $C \in M_s(D)$ such that

(47)
$$\mathrm{diag}\{d_1, d_2, \ldots, d_s\} B = C\, \mathrm{diag}\{d_1, d_2, \ldots, d_s\}.$$

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

(48)
$$B = Q\, \mathrm{diag}\{d_1, d_2, \ldots, d_s\}$$

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

THEOREM 3.15. *Let $M = Dz_1 \oplus Dz_2 \oplus \cdots \oplus Dz_s$ where the order ideals* $\mathrm{ann}\, z_i = (d_i)$ *satisfy* $\mathrm{ann}\, z_1 \supset \mathrm{ann}\, z_2 \supset \cdots \supset \mathrm{ann}\, z_s$. *Then the ring D' of endomorphisms of the D-module M is anti-isomorphic to R/K where R is the ring of matrices $B \in M_s(D)$ for which there exists a $C \in M_s(D)$ such that* $\mathrm{diag}\{d_1, \ldots, d_s\} B = C\, \mathrm{diag}\{d_1, \ldots, d_s\}$ *and K is the ideal of matrices of the form Q diag$\{d_1, \ldots, d_s\}$, $Q \in M_s(D)$.*

If M is a free module, all the $d_i = 0$. Then $R = M_s(D)$ 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 $B = (b)$ is trivially satisfied by the commutativity of D. Then $D' \cong D/(d)$ 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 $d_i \equiv 0 \pmod{d_j}$;
2. $b_{ij} = 0$ if $i \leq r$ and $j > r$ since in this case $d_i \neq 0$ and $d_j = 0$;
3. b_{ij} is arbitrary if $i, j > r$ since $d_i = d_j = 0$ in this case;
4. $b_{ij} \equiv 0 \pmod{d_i^{-1} d_j}$ if $i < j \leq r$.

Changing the notation slightly we see that B has the form

$$
(49)\qquad \left(\begin{array}{ccccccc}
b_{11} & b_{12}d_1^{-1}d_2 & \cdots & b_{1r}d_1^{-1}d_r & 0 & \cdots & 0 \\
b_{21} & b_{22} & \cdots & b_{2r}d_2^{-1}d_r & 0 & \cdots & 0 \\
\hdashline
b_{r1} & b_{r2} & \cdots & b_{rr} & 0 & \cdots & 0 \\
b_{r+1,1} & b_{r+1,2} & \cdots & b_{r+1,r} & b_{r+1,r+1} & \cdots & b_{r+1,s} \\
\hdashline
b_{s,1} & b_{s,2} & \cdots & b_{s,r} & b_{s,r+1} & \cdots & b_{ss}
\end{array}\right)
$$

Here the upper right-hand corner consists of 0's, all the indicated b_{ij} are arbitrary, and the (i, j)-entry for $i < j \le r$ is $b_{ij}d_i^{-1}d_j$. The conditions that the matrix is in K are that the $b_{ij} = 0$ if $j > r$, that b_{ij} is divisible by d_j if $i \ge j$ and $j \le r$, and that b_{ij} is divisible by d_i if $i < j \le r$. 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 $b_{ij}, i \ge j$, can be replaced by b'_{ij} in the same coset mod d_j. Hence we may assume $\deg b_{ij} < n_j = \deg d_j$ if $i \ge j$. Similarly, we may assume $\deg b_{ij} < n_i$ if $i < j$. Matrices $B \in R$ satisfying these conditions will be called *normalized*. It is clear that the map $B \to \eta$ 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 $a \in F$. For D' we define $a\eta$, $a \in F$, $\eta \in D'$, by $(a\eta)x = a(\eta x) = \eta(ax)$ (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 $B \to \eta$ is an F-linear isomorphism of S into D'. We are interested in calculating the dimensionality of D' over F, in matrix terms, the dimensionality 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}, $1 \le i, j \le s$, 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 $i \ge j$, and $\dim S_{ij} = n_i$ if $i < j$. Since S is the direct sum of the subspaces S_{ij} we have

$$
\begin{aligned}
\dim S &= \sum_{j=1}^{s} (s - j + 1)n_j + \sum_{i=1}^{s-1} (s - i)n_i \\
&= \sum_{j=1}^{s} (2s - 2j + 1)n_j.
\end{aligned}
$$

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 $d_1(\lambda)$, $d_2(\lambda)$, $\ldots$, $d_s(\lambda)$ be the invariant factors $\neq 1$ of $\lambda 1 - A$. 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*

$$
(50)\qquad N = \sum_{j=1}^{s} (2s - 2j + 1)n_j.
$$

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 $d_s(\lambda)$ is the minimum polynomial $m(\lambda)$ of T and hence n_s 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 $N > \sum_1^s n_j > n_s$. Hence there exist linear transformations commuting with T which are not polynomials in T. □

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 via T then $V = \mathbb{Q}[\lambda]f_1 \oplus \mathbb{Q}[\lambda]f_2$. The invariant factors are $\lambda - 1$ and $(\lambda - 1)^2$. The normalized matrices of R have the form

$$
(51)\qquad \begin{pmatrix} b_{11} & b_{12}(\lambda - 1) \\ b_{21} & b_{22} + b'_{22}\lambda \end{pmatrix}, \qquad b_{ij} \in \mathbb{Q}.
$$

Since $\lambda f_1 = f_1$, $\lambda^2 f_2 = (2\lambda - 1)f_2 = -f_2 + 2(\lambda f_2)$, the linear transformation U corresponding to (51) satisfies

$$
\begin{aligned}
Uf_1 &= b_{11}f_1 - b_{12}f_2 + b_{12}(\lambda f_2) \\
Uf_2 &= b_{21}f_1 + b_{22}f_2 + b'_{22}(\lambda f_2) \\
U(\lambda f_2) &= b_{21}f_1 - b'_{22}f_2 + (b_{22} + 2b'_{22})(\lambda f_2).
\end{aligned}
$$