M7210 Lecture 36 Friday, November 16, 2012

$\mathbb{F}[x]$-modules: Analysis of single linear map (continued)

Theorem. *If A is any $m \times n$ matrix with entries from a PID R, then there is an $m \times m$ matrix P with entries from R having an inverse with enteries from R and an $n \times n$ matrix Q with entries from R having an inverse with enteries from R such that PAQ is diagonal. Moreover, we may find P and Q such that*

$$PAQ = \operatorname{diag}\{1, \ldots, 1, d_{n-s+1}, \ldots, d_n(x)\},$$

where d_{n-s+1} is not a unit, $d_i(x)|d_j(x)$ if $i < j$.

Remarks concerning proof. The proof of this is similar to the proof of the diagonalization procedure for integer matrices which we described in Lecture 23. If $R = \mathbb{F}[x]$, the proof is even closer to what we have seen before, since we are able to use the Euclidean algorithm. But it turns out that even when the Euclidean Algorithm is not available for R, the PID condition is enough. A complete proof of this is given in Jacobson, *Basic Algebra I*, Chapter 3, section 7.

As in Lecture 35, let V be an $\mathbb{F}$-vector-space with basis $\mathcal{V} = \{v_1, \ldots, v_n\}$, and let $L : V \to V$ be a linear map, with $(L; \mathcal{V}\mathcal{V}) = (a_{ij})$. Let $\mathcal{E} = \{e_1, \ldots, e_n\}$ be the standard basis for $\mathbb{F}[x]^n$. We studied the $\mathbb{F}[x]$-modules and $\mathbb{F}[x]$-module homomorphisms:

$$\ker \Phi \xrightarrow{\iota} \mathbb{F}[x]^n \xrightarrow{\Phi} (V, L),$$

where $\Phi(e_i) = v_i$. We defined $\widehat{L} : \mathbb{F}[x]^n \to \mathbb{F}[x]^n$ by $\widehat{L}(e_i) = \sum_{j=1}^n a_{ij} e_j$ and we proved that $\ker \Phi$ has an $\mathbb{F}[x]$-module basis $\mathcal{K} = \{\mathbf{k}_1, \ldots, \mathbf{k}_n\}$, where $\mathbf{k}_i = xe_i - \widehat{L}(e_i)$. Thus,

$$(\iota; \mathcal{K}\mathcal{E}) = \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1,n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{n,n} \end{pmatrix} = xI - A.$$

If we apply the theorem above to the matrix $xI - A$, we get $n \times n$ matrices P and Q with entries from $\mathbb{F}[x]$, having inverses with enteries from $\mathbb{F}[x]$, such that $P(xI - A)Q$ is diagonal. Note that there will be no zeros on the diagonal of $P(xI - A)Q$, since the product of the diagonal entries is equal to a unit times the determinant of $xI - A$, and the determinant is a monic polynomial of degree n. Indeed, we may find P and Q such that

$$P(xI - A)Q = \operatorname{diag}\{1, \ldots, 1, d_{n-s+1}, \ldots, d_n(x)\},$$

where d_{n-s+1} is not a unit, $d_i(x)|d_j(x)$ if $i < j$ and all the $d_i(x)$ are monic.

We are representing vectors as rows and are allowing our matrices to act on the right. We can view P, therefore, as a change of basis matrix on $\ker \Phi$. Letting $\mathcal{K}'$ denote the new

basis, we have $P = (\mathrm{id}_{\ker \Phi}; \mathcal{K}'\mathcal{K})$, and the elements of $\mathcal{K}'$ are represented with respect to $\mathcal{K}$ by the rows of P.

Similarly, Q can be viewed a change of basis matrix on $\mathbb{F}[x]^n$. If $\mathcal{E}'$ denotes the new basis, then $Q = (\mathrm{id}_{\mathbb{F}[x]^n}; \mathcal{E}\mathcal{E}')$. The rows of $Q^{-1} = (\mathrm{id}_{\mathbb{F}[x]^n}; \mathcal{E}'\mathcal{E})$ represent the elements of $\mathcal{E}'$ with respect to $\mathcal{E}$. Each element of $\mathcal{E}'$ generates a free cyclic summand of $\mathbb{F}[x]^n$. The last s elements of $\mathcal{E}'$—i.e., the elements of $\mathbb{F}[x]^n$ represented with respect to $\mathcal{E}$ by the last s rows of Q^{-1}—map via Φ to generators of cyclic summands of the $\mathbb{F}[x]$-module (V, L). Thus, if $(q_{i1}^* \ \cdots \ q_{in}^*)$ is the i^{th} row of Q^{-1} and $d_i(x) \neq 1$, then $z_i = \sum_{j=1}^n q_{ij}^* v_j \in (V, L)$ is a generator of a cyclic summand of (V, L), and

$$\mathbb{F}[x]z_i \cong \mathbb{F}[x]/(d_i(x)),\ i = 1, \ldots, n.$$

Moreover,

$$(V, L) \cong \bigoplus_{z_i \neq 1} F[x]z_i. \tag{2}$$

Exercise. In the discussion above, we used the following fact implicitly:

Lemma. *Let A be a ring and for each $i \in I$, let M_i be an A-module and $K_i \subseteq M_i$ be a sub-A-module. Then $\bigoplus_{i\in I} K_i$ is a sub-A-module of $\bigoplus_{i\in I} M_i$ and*

$$\bigoplus_{i\in I} M_i/K_i \cong \bigoplus_{i\in I} M_i \Big/ \bigoplus_{i\in I} K_i. \tag{1}$$

Where and how was this used? Prove (2).

Observe that $\dim_F F[x]z_i = \deg z_i$. The images of z_i under L,

$$\{z_i, L(z_i), L^2(z_i), \ldots, L^{n-1}(z_i)\},$$

form an $\mathbb{F}$-vector-space basis for $F[x]z_i$. Note that $\sum_{i=1}^n \deg z_i = n$, so if any of the $d_i(x)$ is not linear, then $d_1(x) = 1$. Now we can see that as an $\mathbb{F}$-vector space, V can be written as a sum of subspaces V_i, each of which is the underlying $\mathbb{F}$-vector-space of $\mathbb{F}[x]z_i$. Each V_i is invariant under L, in the sense that $L(V_i) \subseteq V_i$. The action of L on each V_i can be understood using the ideas in Lecture 34.

Example. See the example from Jacobson, Basic Algebra I, pages 198-9.