**M7210 Lecture 37** Monday, November 19, 2012

**Characteristic and minimum polynomials**

Using the same notation as in the previous lecture, the *characteristic polynomial of* $A$ is

$$f(x) = \det(xI - A) = d_{n-s+1}d_{n-s+2}\cdots d_n(x),$$

and the *minimum polynomial of* $A$ is $d_n(x)$.

Recall that $\mathbb{F}[x]z_i \cong \mathbb{F}[x]/\big(d_i(x)\big)$. Therefore, $d_i(x)z_i = 0$. Since $d_i(x)|d_j(x)$ if $i < j$, $d_n(x)z_i = 0$ for all $i$. It follows that $d_n(x)x^j z_i = 0$ for all $i$ and $j$. Since the every element of $V$ is a linear combination of some $x^j z_i$s for various $i$ and $j$, it follows that $d_n(x)v = 0$ for all $v \in V$. Thus, $d_n(L) = 0$. This is a stronger statement than:

**Theorem.** (Cayley-Hamilton.) *Suppose* $L : V \to V$ *is a linear map,* $A$ *is the matrix for* $L$ *(with respect to a basis) and* $f(x) = \det(xI - A)$. *Then* $f(L) = 0$.

The Cayley-Hamilton theorem can be proved directly, and it is true not just for endomorphisms of a vector space, but for endomorphisms of any finitey-generated module over any commutative ring. *In the following,* $R$ *will be a commutative ring with* 1 *and* $M$ *will be a finitely-generated* $R$*-module.*

**Theorem.** (Generalized Cayley-Hamilton; see Eisenbud, *Commutative Algebra,* p. 120.) *Let* $J \subset R$ *an ideal and let* $\phi : M \to M$ *be an* $R$*-module endomorphism such that* $\phi(M) \subseteq JM$. *Then there is a monic polynomial* $p(x) \in R[x]$,

$$p(x) = x^n + p_1x^{n-1} + \cdots + p_n, \text{ with } p_i \in J^i,$$

*such that* $p(\phi) = 0$.

*Comment.* The theorem is meaningful and informative even in the case that $J = R$, but we get useful additional information when $J$ is a proper ideal. Reminder: $JM$ is the submodule of $M$ generated by $\{\, ym \mid y \in J,\, m \in M \,\}$. It consists of all sums $\sum_{i=1}^k y_i m_i$, where $k \in \mathbb{N}$, $y_i \in J$ and $m_i \in M$.

*Proof.* Let $m_1, \ldots, m_n$ be a finite set of generators for $M$ and let $A$ be a matrix expressing $\phi$ with respect to these generators:

$$\phi(m_i) = \sum_j a_{ij}m_j, \text{ with } a_{ij} \in J.$$

(Note that the $A$ is not unique, nor is every $n \times n$ matrix with entries from $R$ necessarily associated with and endomorphism. These things are true if the $m_i$ form a basis for $M$, but we have not assumed that they do, nor even that $M$ has a basis.) Now, regard $M$ as an $R[x]$-module by letting $x$ act as $\phi$, i.e., $xm := \phi(m)$, for $m \in M$. Let $\mathbf{m}$ be the column vector whose entries are the $m_j$. If $I$ is the $n \times n$ identity matrix, then

$$(xI - A)\mathbf{m} = 0.$$

If we multiply on the left by the matrix of cofactors of $xI - A$, we get

$$\big[\det(xI - A)\big] I \cdot \mathbf{m} = 0.$$

Let $p(x) := \det(xI - A)$. The previous line shows that $p(x)m_j = p(\phi)m_j = 0$ for all $m_j$. Accordingly $p(\phi) = 0$. It is clear from the definition of the determinant that the coefficient in $p$ of $x^i$ is in $J^{n-i}$. /////

**Corollary.** *If $\alpha : M \to M$ is a surjective homomorphism of $R$-modules, then $\alpha$ is an isomorphism. (We are assuming that $M$ is finitely-generated. This is not true otherwise.)*

*Proof*. We will apply Cayley-Hamilton with the ring being $R[t]$. Regard $M$ as an $R[t]$-module by letting $tm = \alpha(m)$. For the ideal $J$ we take $(t) \subset R[t]$. Since $\alpha$ is surjective, $IM = M$. For the endomorphism $\phi$, we take $\mathrm{id}_M$. The theorem gives us a polynomial $q(t, x) \in R[t][x]$ such that $q(t, id_M) = 0$. Now,

$$q(t, x) = x^n + q_1(t)x^{n-1} + \cdots + q_n(t), \text{ with } q_i(t) \in (t^i).$$

This means that each $q_i(t)$ has zero constant term. Thus, $q(t, id_M) = 0$ is of the form $(1 - Q(t)t)$ for some $Q(t) \in R[t]$ and so $Q(t)t = tQ(t) = 1$. Thus $Q(\alpha) = \alpha^{-1}$. Since $\alpha$ has an inverse, it is an isomorphism. /////

**Corollary.** *Any set $\mathcal{F} = \{f_1, \ldots, f_n\} \subseteq R^n$ that generates $R^n$ forms a free basis.*

*Proof*. Define $\beta : R^n \to R^n$ by $\beta(e_i) = f_i$, where $\{e_1, \ldots, e_n\}$ is the standard basis. Then $\beta$ is surjective, hence an isomorphism, so $\mathcal{F}$ is a free basis. /////

**Corollary.** *Any basis of $R^n$ has $n$ elements.*

*Proof*. Suppose $\mathcal{G} = \{g_1, \ldots, g_m\} \subseteq R^n$ generates $R^n$. If $m < n$, then let $g_{m+1} = \cdots = g_n = 0$, and let $\mathcal{G}' = \{g_1, \ldots, g_n\}$. Then by the first part of the corollary, $\mathcal{G}'$ is a free basis—but this is absurd. Thus, any generating set (hence, any free basis) of $R^n$ must have *at least* $n$ elements. If $R^n$ contained a free basis with $s \geq n$ elements, then $R^n \cong R^s$. The same argument shows that $n$ cannot be strictly less than $s$. Thus, any free basis of $R^n$ has $n$ elements. /////