Introduction to Rings and Modules

Lecture 16, Wednesday June 14 2023
Ari Feiglin

16.1 Cannonical Forms

Theorem 16.1.1:

Let A be a matrix of size $d \times d$ over the field F. Then there exists monic polynomials (polynomials with a leading coefficient of 1) $d_1, \dots, d_n \in F[x]$ such that $d_i | d_{i+1}$ and

$$A \sim \bigoplus_{i=1}^{n} C_{d_i}$$

ie. A is similar to the direct sum of the companion matrices of d_i.

Proof:

Let V be an n-dimensional vector space over F, and let B be a basis of V. Further let φ be the linear transformation represented by A under the basis B. Together V and φ define an $F[x]$-module M.
We claim that M is finitely generated. Suppose $B = (b_1, \dots, b_n)$, and since $M = V$ (as sets), every element $m \in M$ can be written as

$$m = a_1 b_1 + \cdots + a_n b_n$$

where $a_i \in F$. Since a_i is also a constant polynomial and $B \subseteq M$, we have that B generates M. Thus M is a finitely-generated module.
Since M is an $F[x]$-module, and since F is a field, $F[x]$ is a PID, we have that

$$M \cong F[x]^r \times {}^{F[x]}\big/_{(d_1)} \times \cdots \times {}^{F[x]}\big/_{(d_t)}$$

such that $d_i | d_{i+1}$, and d_i are unique up to friends. Note that $r = 0$ since $F[x]$ is an infinite-dimension vector space over F, as we can take the infinite basis $(1, x, x^2, \dots)$. And since $\dim M = n < \infty$, this means $r = 0$.
Since F is a field, the units of $F[x]$ are those of F, which is $F \setminus \{0\}$. Thus every polynomial is friends with a unique monic polynomial, so we can assume d_i are monic polynomials.
For every component ${}^{F[x]}\big/_{(d_i)}$ we will choose the basis $B_i = (1 + (d_i), x + (d_i), \dots, x^{\deg d_i - 1} + (d_i))$. Relative to this basis, the scalar multiplication mapping of x is represented by C_{d_i}. We can take a basis of M as the set

$$B' = \bigcup_{i=1}^{t} \{0\}^{i-1} \times B_i \times \{0\}^{t-i}$$

essentially we take all elements of B_i and place them in a tuple which is 0 except for at the index i. Relative to this basis, the scalar multiplication mapping of x is represented by

$$\bigoplus_{i=1}^{t} C_{d_i}$$

But by definition, the scalar multiplication mapping is represented by A (under the original basis B), and thus we have

$$A \sim \bigoplus_{i=1}^{t} C_{d_i}$$

as required. ■

Theorem 16.1.2 (Cayley-Hamilton Theorem):

Suppose F is a field and $A \in M_n(F)$. Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be A's characteristic polynomial, then

$$p(A) = A^n + a_{n-1}A^{n-1} + \cdots + a_0 I_n = 0$$

Proof:

We know that A is similar to a matrix of the form

$$A \sim \bigoplus_{i=1}^{t} C_{d_i}$$

and it can be shown that the characteristic polynomial of C_{d_i} is d_i, and so

$$p(x) = d_1 \cdots d_t$$

Let M be the module defined above to show this similarity, then A represents scalar multiplication by x. This means that $p(A)$ represents scalar multiplication by $p(x)$. Let us represent scalar multiplication by x by φ_x, and so $A = [\varphi_x]_B^B$ and thus

$$p(A) = p\big([\varphi_x]_B^B\big) = \big[p(\varphi_x)\big]_B^B$$

and $p(\varphi_x)$ is precisely $\varphi_{p(x)}$ as required.
So

$$M \cong F[x]\big/(d_1) \times \cdots \times F[x]\big/(d_t)$$

And since $p(x)$ is the product of d_is, it is divisible by every d_i. But since multiplying by d_i equals zero on the component $F[x]/(d_i)$, we have that multiplication by $p(x)$ is zero on every component and thus is zero on M. So we have that $\varphi_{p(x)} = 0$ and since $p(A)$ represents it, we have that $p(A) = 0$ as required. ■

Theorem 16.1.3 (Jordan Cannonical Form):

Let F be a field, and $A \in M_d(F)$ then suppose F contains every eigenvalue of A, then A is similar to the direct sum of Jordan blocks

$$A \sim \bigoplus_{i=1}^{n} J_{n_i}(\lambda_i)$$

where the $\lambda_i \in F$s are not necessarily distinct, and this form is unique up to the order of the Jordan blocks.

Proof:

Since $F[x]$ is a PID, it is a UFD. By assumption, the characteristic polynomial $p(x)$ can be factorized into linear terms (otherwise there would exist an irreducible term of degree $> n$ which would not have a root in F). We know that if M is the module defined by a finite dimensional vector space V and A for the linear transform defining scalar multiplication by x, we have

$$M \cong F[x]\big/(p_1^{n_1}) \times \cdots \times F[x]\big/(p_t^{n_t})$$

For p_i irreducible, not necessarily distinct, and unique up to friends.
For the same reason as above (using the companion matrices), we have that the characteristic polynomial of the scalar multiplication mapping of x is equal to the product of $p_i^{n_i}$, and since scalar multiplication of x is represented by A we have

$$p(x) = p_1(x)^{n_1} \cdots p_t(x)^{n_t}$$

where $p(x)$ is the characteristic polynomial of A. Since p can be factored into linear terms $x - \lambda_i$, and $F[x]$ is a UFD, this means that $p_i(x) = x - \lambda_i$.
Thus

$$M \cong F[x]\big/((x-\lambda_1)^{n_1}) \times \cdots \times F[x]\big/((x-\lambda_t)^{n_t})$$

and taking the basis $B_i = \big((x-\lambda_i)^{n_i-1} + \big((x-\lambda_i)^{n_i}\big), \dots, 1 + \big((x-\lambda_i)^{n_i}\big)\big)$ gives a representation of scalar multiplication of x as $J_{n_i}(\lambda_i)$ on the ith component, as shown previously. Thus scalar multiplication by x is represented by

$$\bigoplus_{i=1}^{t} J_{n_i}(\lambda_i)$$

and since A represents scalar multiplication of x, we have

$$A \sim \bigoplus_{i=1}^{t} J_{n_i}(\lambda_i)$$

as required. ■

Note that A is diagonalizable if and only if every Jordan block is of size 1×1 if and only if

$$M \cong {}^{F[x]}\big/_{(x-\lambda_1)} \times \cdots \times {}^{F[x]}\big/_{(x-\lambda_t)}$$

16.2 Completeness

Definition 16.2.1:

Let $R \subseteq S$ commutative rings. An element $s \in S$ is **algebraic** over R if it is the root of a polynomial over R. If s is the root of a monic polynomial over R, then it is called **integral** over R.

If R is a field, s is algebraic if and only if it is integral.

Definition 16.2.2:

If R is an integral domain, let $F = \operatorname{Frac} R$. R is called an **integrally closed domain** if for every $s \in F$ if s is integral over R, then $s \in R$.

Proposition 16.2.3:

Every UFD is completely closed.

Proof:

Let R be a UFD. Let $\alpha \in \operatorname{Frac} R$ integral over R, suppose $\alpha = \frac{r}{s}$ is a reduced fraction. By definition α is the root of some monic polynomial

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

and by proposition 11.0.9, $s|1$ and $r|a_0$. In particular this means that s is invertible, and so $\alpha = rs^{-1} \in R$, as required.