Beginning of Sept. 21, 2022

Properties of the companion matrix:

- The minimal polynomial of C_f is f; so is the char poly.
- C_f is cyclic (see below).
- If A commutes with C_f then A is a polynomial of C_f. Also, the dimension of the centralizer of A, $\{B \in M_n(F) : AB = BA\}$, is n.

We say a matrix is **cyclic** iff there exists a column vector v so that $v, Av, A^2v, ..., A^{n-1}v$ is a basis.

Proposition

Let A be $n \times n$. TFAE:

(1) A is cyclic.

(2) min poly of A has degree n (and equivalently min poly = char poly).

Proof. If A is cyclic then there exists v with $v, Av, ..., A^{n-1}v$ forming a basis. If $0 \neq h(x)$ for a polynomial of degree $< n$, then $h(A)v \neq 0$:

$$h(x) = h_0 + h_1x + ... + h_{n-1}x^{n-1}$$
$$h(A) = h_0I + h_1A + ... + h_{n-1}A^{n-1}$$
$$h(A)v = h_0v + h_1Av + ... + h_{n-1}A^{n-1}v,$$

and since the A^kv's form a basis, the last quantity is 0 only when $h(x) = 0$. Hence the min poly must be of degree n. Converse omitted. □

For the last claim, suppose $BA = AB$. It suffices to show that it is in the span of $I, A, ..., A^{n-1}$. If $Bv = w$, then $BAv = ABv = Aw$ and $BA^iv = A^iBv = A^iw$. Consider $\theta : B \to Bv$ from the centralizer to V. Furthermore it is linear. By rank nullity $\dim(C(A)) \leqslant n$ since $\ker\theta = 0$. On the other hand, $\dim(C(A)) \geqslant n$ since it at least contains $I, A, ..., A^{n-1}$ and no polynomial of degree n can kill them. Thus $\dim(C(A)) = n$ and $I, A, ..., A^{n-1}$ spans the centralizer.

Remark. If A is cyclic then A is similar to its companion matrix. To see this, we take the basis $v, Av, ..., A^{n-1}v$. Then the matrix w.r.t this matrix is just

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & \cdots & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -b_{n-1} \end{bmatrix}.$$

Claim: the char poly is $x^nb(n-1)x^{n-1} + ... + b_0$. It is enough to show that the min poly $f(x) = x^x + b_{n-1}x^{n-1} + ... + b_0$. Note that

$$f(A)v = b_0v + b_1Av + ... + b_{n-1}A^{n-1}v + A^nv$$

where $A^n v$, by the design of the matrix, kills everything before. Hence $f(A)v = 0$ and it is the lowest degree polynomial killing v.

Corollary

If A is cyclic then A is similar to A^T.

Proof. A and A^T have the same char poly (and the same min poly). □

0.1 Polynomials over Fields

Facts about polynomials over fields:

- There exists a division algorithm for $f(x)/g(x)$ if $g(x) \neq 0$.
- There exists $q(x), r(x)$ such that $f(x) = q(x)g(x) + r(x)$ with $\deg r(x) < \deg g(x)$.

Corollary: PID

$\mathbb{F}[x]$ is a **principal ideal domain (PID)**, i.e., if I is an ideal of $\mathbb{F}[x]$ (I is closed under addition and pointwise multiplication), then $I = h(x)\mathbb{F}(x)$ for some $h(x)$.

Proof. If $I = 0$ the claim is true. Otherwise we choose $h(x) \in I$ nonzero with the lowest possible degree with $h(x)$ monic. Then if $0 \neq f(x) \in I$, $\deg(f) \geq \deg(h)$. By division algorithm $f(x) = h(x)q(x) + r(x)$. Since $r(x) \in I$ it must be 0. □

GCDs of polynomials: if $h(x)$ divides $f(x)$ and $g(x)$, then $h(x)$ divides everything in the ideal

$$f(x)\mathbb{F}[x] + g(x)\mathbb{F}[x] = \ell(x)\mathbb{F}[x] \qquad \text{for some } \ell(x).$$

But then $h = l$ up to a scalar multiple. Therefore, indeed we have

$$\gcd(f, g) = a(x)f(x) + b(x)g(x) \qquad \text{for some } a(x), b(x).$$

The Euclidean algoritm works almost identically in the polynomial case.