Beginning of Sept.26, 2022

We say $f(x), g(x)$ are **relative prime** if $\gcd(f(x), g(x))$ is degree 1.

Definition: Irreducible Polynomials

We say $0 \neq f(x)$ is **irreducible** if $f(x) \neq \alpha(x)\beta(x)$ for α, β with strictly lower degrees.

Facts, all of which should ring a bell to the prime number analogue:

- Every nonconstant polynomial is a product of irreducible polynomials.
- If $f(x)$ is irreducible, and $g(x)$ is a polynomial, then either $\gcd(f(x), g(x)) = 1$ [degree-wise] or $f(x)$ divides $g(x)$.
- If $f(x)$ is irreducible and $f(x)$ divides $\alpha(x)\beta(x)$ then $f(x)$ divides either $\alpha(x)$ or $\beta(x)$.

  Proof. Suppose $f(x)$ does not divide $\alpha(x)$. Then $1 = \gcd(f(x), \alpha(x))$ so $1 = \gamma(x)f(x) + \delta(x)\alpha(x)$. Hence

  $$\beta(x) = \gamma(x)\beta(x)f(x) + \alpha(x)\beta(x)\delta(x)$$

  where $\alpha(x)\beta(x)$ is a multiple of $f(x)$ by assumption. □
- Any nonconstant polynomial is uniquely (up to order) a product of irreducibles.

0.1 Canonical Forms under Similarity

Fact: if $A \in M_n(F)$ and $m(x)$ is the min poly of A then there exists a column vector v such that $h(A)v \neq 0$ for any polynomial $h(x)$ of degree < deg $m(x)$.

Proof for infinite fields. Note that $m(x)$ has only finitely many proper divisors $h_1(x), ..., h_r(x)$. Let V be the space of column vectors and let V_i be the set of all vectors $\{v : h_i(A)v = 0\} = \ker h_i(A)$, a proper space of V, for each i. If the result fails, $V = V_1 \cup ... \cup V_r$. Then there exists $\ell_i : V \to F$ with $\ell_i(V_i) = 0$. Let $v_1, ..., v_n$ be a basis for V. Then any linear $\ell : V \to F$ with $\ell(v_i) = \delta_i$, $\ell(\sum x_i v_i) = \sum \delta_i x_i$, so ℓ can be interpreted as a polynomial of $x_1, x_2, ..., x_n$. Now we define $g = \ell_1 \ell_2 ... \ell_r$, a nonzero polynomial of $x_1, x_2, ..., x_n$ of degree $r > 0$. □

Theorem: Rational Canonical Form

Suppose $A \in M_n(F)$. Then A is similar to a matrix of form

$$\text{block diagonal}(C_{f_1}, C_{f_2}, ..., C_{f_r})$$

were C_{f_i} is the companion matrix of a monic polynomial $f_i(x)$. Moreover, $f_r(x) \mid f_{r-1}(x) \mid ... \mid f_1(x)$.

Idea of proof: if f_1 is the min poly then $f_i(C_{f_i}) = 0$ since each f_i divides f_1. If so, $f_1(A) = 0$, i.e., the char poly of A is just $f_1 f_2 ... f_r$.

Invariance: let $B \in M_n(F[(x)])$, i.e., polynomial entries. Let $\gamma_1(B) :=$ gcd of all entries. To define $\gamma_2(B)$, take all 2×2 minors and take the gcd of all their determinants. Similarly, $\gamma_k(B)$ is the gcd of the determinants of all $k \times k$ minors, and in particular $\gamma_n(B) = \det B$.

In particular, if B is a companion matrix C_{f_1}, we have $\gamma_i(xI - C_{f_1}) = 1$ for all i except $i = n$, where $\gamma_n(xI - C_{f_1}) = f_1(x)$.