Today: What does Jordan form mean, and how does it lead to proof?

Def: $F$ is algebraically closed if every polynomial with coeffs in $F$ has a root in $F$.

$\Rightarrow p(\lambda) = (\lambda - \alpha_1)^{m_1} \cdots (\lambda - \alpha_r)^{m_r} \Rightarrow$ hypothesis of JF thm.

How to guarantee all $\lambda \in F$

Fundamental Thm of Algebra: $C$ is algebraically closed.

What block diagonal means:

Def (direct sum): $V = V_1 \oplus V_2$ means $V = V_1 + V_2$ and $V_1 \cap V_2 = 0$.

Prop: $\iff V$ has basis $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ with $V_i = \text{span} \mathcal{B}_i$ for $i = 1, 2$.

Ex: $F^n = F^m \oplus F^{n-m} = \text{span}(e_1, \ldots, e_m) \oplus \text{span}(e_{m+1}, \ldots, e_n)$.

Def: $V = V_1 \oplus \cdots \oplus V_r$ if $V = V_1 + \cdots + V_r$ and $V_i \cap \bigoplus_{j \neq i} V_j = 0 \; \forall \; i$.

Prop: $\iff V$ has basis $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_r$ with $V_i = \text{span} \mathcal{B}_i \; \forall \; i$.

Ex: $V$ has basis $v_1, \ldots, v_n \iff V = \text{span}(v_1) \oplus \cdots \oplus \text{span}(v_n)$.

Prop: $\phi$ block diagonal $\iff V = V_1 \oplus \cdots \oplus V_r$ with $\phi(V_i) \subseteq V_i \; \forall \; i$.

What Jordan blocks mean; needs:

Def: $V_i$ is $\phi$-invariant.

Cayley-Hamilton Thm: $p_\phi(\phi) = 0$.

Pf: Fix basis $e_i, \ldots, e_n$ of $V$, so $\phi e_i = a_{i1} e_1 + \cdots + a_{in} e_n = A_i e_i$.

By def, $p_\phi(t) = \det(A - tI)$. Need $p_\phi(\phi) e_i = 0 \; \forall \; i$.

Equivalently, $\begin{bmatrix} p_\phi(t) & \vdots & e_i \\ \vdots & \vdots & \vdots \\ p_\phi(t) e_n \\ \end{bmatrix}$ becomes $\begin{bmatrix} \ast \\ \vdots \\ 0 \\ \end{bmatrix}$ when evaluated at $t = \phi$.

$\det(A - tI) = C^T(A - tI)$, where $C =$ cofactor matrix of $A - tI$.

But $(A - \phi I) \begin{bmatrix} e_i \\ \vdots \\ e_n \\ \end{bmatrix} = A \begin{bmatrix} e_i \\ \vdots \\ e_n \\ \end{bmatrix} - \begin{bmatrix} \phi e_i \\ \vdots \\ \phi e_n \\ \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \end{bmatrix}$ by $(\times)$. Now multiply by $C^T \bigg|_{t = \phi}$ on the left.

Def: A minimal polynomial of $\phi$ (or $A$) is a monic polynomial $m(t)$
of minimal degree satisfying $m(\phi) = 0$ (or $m(A) = 0$).

Prop: 1. $\exists! m(t)$.

2. $f(\phi) = 0 \Rightarrow m | f$.

Pf: 1. follows from 2: $m | f$ and $\deg m = \deg f \Rightarrow f = \omega m \Rightarrow f = m$.

2. Assume $f(\phi) = 0$. Write $f = qm + r$ with $\deg r < \deg m$. $(\ast)$

Then $0 = f(\phi) - q(\phi)m(\phi) = r(\phi) \Rightarrow r = 0$.
Jordan block: $A \in \mathbb{F}^{d \times d}$ or $\Phi: V \to V$ with $\dim V = d$ whose minimal polynomial is $(t - \lambda)^d$

$d = 1$: $(\Phi - \lambda)v = 0 \iff v \in E(\lambda) \Rightarrow \mathcal{B} = \{v\} \Rightarrow [\Phi]_\mathcal{B} = [\lambda]

$d = 2$: $(\Phi - \lambda)V \neq V$ or else $(\Phi - \lambda)^2 V = (\Phi - \lambda)((\Phi - \lambda)V) = (\Phi - \lambda)V = V$, but $(\Phi - \lambda)V \neq 0$ by def of minimal polynomial

$\Rightarrow \dim (\Phi - \lambda)V = 1 \Rightarrow (\Phi - \lambda)V$ is in the $d = 1$ case.

$d$ arbitrary (prove by easy induction): $(\Phi - \lambda)V$ has $\dim d - 1$

$(\Phi - \lambda)^{d - 2} V = (\Phi - \lambda)^{d - 1} V = (\Phi - \lambda)^{d - 2} V = (\Phi - \lambda)^{d - 3} V = \cdots = (\Phi - \lambda) V = 0$

$V_{d - k} = (\Phi - \lambda)^{d - k} V$

Choose $v = v_d \in V \setminus V_{d - 1}$. Then $(\Phi - \lambda)^d v_d = 0$ but $(\Phi - \lambda)^{d - 1} v_d \neq 0$, so

$(\Phi - \lambda)^{d - k} v = v_{d - k} \in V_{d - k} \setminus V_{d - k - 1}$

$(\Phi - \lambda)^{d - k} v = v_k \in V_k \setminus V_{k - 1}$

$\Rightarrow (\Phi - \lambda)^{d - k} v_k = v_k - v_{k - 1}$

$\Rightarrow \Phi v_k = \lambda v_k + v_{k - 1}$ when $k \geq 2$, and

$\Phi v_1 = \lambda v_1$.

So $\mathcal{B} = \{v_d, v_{d - 1}, \ldots, v_1\} \Rightarrow [\Phi]_\mathcal{B} = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_d \end{bmatrix}$.

Pf of Jordan form thm: Need $V = V_1 \oplus \cdots \oplus V_r$ with $V_i$ $\Phi$-invariant for all $i$. 

Not so hard to do directly, but best done using rings and modules.

Def: A commutative ring satisfies all field axioms except * multiplicative inverses need not exist

E.g. field, $\mathbb{Z}$, $\mathbb{F}^{n \times n}$, $\mathbb{Z}^{n \times n}$, $\mathbb{R}^{n \times n}$ for any commutative ring $R$

$F[t], \mathbb{Z}[t], \mathbb{R}[t]$ for any ring $R$ and any set $t$ of variables

Def: A module over a ring $R$ satisfies the same axioms as a vector space over $F$ but with scalars $R$.

E.g. vector space $V/F$ with $\Phi: V \to V$ is a module $/F[t]$ with $tv = \Phi(v)$.

JF thm follows by classifying all $F[t]$-modules of $\dim F < \infty$:

all are $\oplus$-invariant submodules $\langle v \rangle$ with $p^d(v) = 0$ for some irreducible $p$.

Look up "module over PID"

Note: same classification describes all finitely generated abelian groups: $\mathbb{Z}$ and $F[t]$ are both PIDs