1. A, B可分别对角化，$AB=BA \Rightarrow$ 可同时对角化

proof: (1)（矩阵方法） 参见6.8，例4

(2)（几何证法）. 引理：A的特征子空间V_{λ_0}是B的不变子空间. $(\lambda_0\neq 0)$

$$\left(\begin{array}{l}\forall x\in V_{\lambda_0},\quad AX=\lambda_0 X. \qquad BX=\frac{1}{\lambda_0}BAX=\frac{1}{\lambda_0}ABX \\ \Rightarrow A(BX)=\lambda_0 BX \Rightarrow BX\in V_{\lambda_0}\end{array}\right)$$

A可对角化 $\Rightarrow A=\bigoplus_{i=1}^{t} V_{\lambda_i}$ B可对角化 $\Rightarrow B|_{V_{\lambda_i}}$ 也可对角化.

只需（分别在V_{λ_i}）找一组基. s.t $B|_{V_{\lambda_i}}$ 为对角矩阵，则 $B\sim \mathrm{diag}(B|_{V_{\lambda_1}},\cdots,B|_{V_{\lambda_n}})$

也为对角阵.

$AB=0$，$\mathrm{rank}A+\mathrm{rank}B\le n$?

$B=(X_1,\cdots,X_n)$. $AX_i=0 \Rightarrow$ B列向量均为 $AX=0$ 解.

$\Rightarrow$. ~~rank B~~ ~~dim~~ $U_B\subseteq \mathrm{Ker}A$ i.e. $\mathrm{rank}B\le n-\mathrm{rank}A$.

$\mathrm{rank}AB \geqslant \mathrm{rank}A+\mathrm{rank}B-n.$, $A,B\in M_{n\times n}(\mathbb{F})$.

$\Leftrightarrow n-\mathrm{rank}AB\le (n-\mathrm{rank}A)+(n-\mathrm{rank}B)$.

$BX=0 \Rightarrow ABX=0$. $\eta_1,\cdots,\eta_k$为 $BX=0$ 解空间一组基.

扩充为 $\eta_1,\dots,\eta_k,\eta_{k+1},\dots,\eta_r$ 为 $ABX=0$ 的解.

则 $B\eta_{k+1},B\eta_{k+2},\dots,B\eta_r$ 为 $AX=0$ 中线性无关的解.

即 $V=\langle B\eta_{k+1},\dots,B\eta_r\rangle\subseteq \ker A$.

$\dim V=\dim\ker AB-\dim\ker B$

$\Rightarrow \dim\ker AB=\dim\ker B+\dim V\le \dim\ker B+\dim\ker A$.

7.3.6. α,β 相对 A 的最小多项式 $d_\alpha(\lambda),d_\beta(\lambda)$ 互素，求证:

$F[\mathscr{A}]\alpha\oplus F[\mathscr{A}]\beta=F[\mathscr{A}][\alpha+\beta]$

proof: $\exists u,v$ $u(\lambda)d_\alpha(\lambda)+v(\lambda)d_\beta(\lambda)=1\Rightarrow u(\lambda)d_\alpha(\lambda)=1-v(\lambda)d_\beta(\lambda)$

若 $\gamma\in F[\mathscr{A}]\alpha\cap F[\mathscr{A}]\beta$. $\exists f,g\in F[x]$, s.t.

$\gamma=f(\mathscr{A})\alpha=g(\mathscr{A})\beta\Rightarrow u(\mathscr{A})d_\alpha(\mathscr{A})f(\mathscr{A})\alpha=(I-v(\mathscr{A})d_\beta(\mathscr{A}))g(\mathscr{A})\beta$.

$\Rightarrow g(\mathscr{A})\beta=0\Rightarrow\gamma=0$. $\alpha+\beta\in F[\mathscr{A}]\alpha\oplus F[\mathscr{A}]\beta\Rightarrow$ "$\supseteq$"

而 $u(\mathscr{A})d_\alpha(\mathscr{A})(\alpha+\beta)=u(\mathscr{A})d_\alpha(\mathscr{A})\alpha+(I-v(\mathscr{A})d_\beta(\mathscr{A}))\beta$.

$=\beta\in F[\mathscr{A}][\alpha+\beta]$ 同理 $\alpha\in F[\mathscr{A}][\alpha+\beta]$. $\Rightarrow$ "$\subseteq$"

理想：I 称为环 R 的理想，若 $\forall a\in R$，$aI\subseteq I$，$Ia\subseteq I$.

$aI=\{ax \mid x\in I\}$. 若 R 除 0 和 R 外没有其他理想 $\Rightarrow$ R 为单环.

Thm: $M_{n\times n}(\mathbb{F})$ 是单环.（最典型的单环，非交换环）.

Pf: $A\in M_{n\times n}(\mathbb{F})$ $A\neq 0$，若 $A\in I$，~~若非和~~ 若 $I\neq 0$.

初等变换 $A\sim\begin{pmatrix} I_r & 0 \\ 0 & 0\end{pmatrix}$，$r=\operatorname{rank} A$.

可将 A 初等变换为 $\begin{pmatrix} 0 & & \\ & 0\ I_r & \\ & & 0 \\ & & & 0\end{pmatrix}$，将 $A_i=\begin{pmatrix} O_{ir} & & \\ & I_r & \\ & & O_{n-(i+1)r}\end{pmatrix}$ 求和，$A_i\in I$.

($(i+1)r<n$) 再与 $\begin{pmatrix} O_{n-r} & 0 \\ 0 & I_r\end{pmatrix}\in I$ 求和，得对角线全为1或2，

其他为0. 将2的行乘 $1/2$（初等变换）. 得 $I_n\in I$ $\Rightarrow$ $\forall A\in M_{n\times n}(\mathbb{F})$.

$A=AI_n\in AI\subseteq I$ $\Rightarrow$ $I=R$.

正合列 $\to M_{i-1}\xrightarrow{f_{i-1}} M_i\xrightarrow{f_i} M_{i+1}\to\cdots$ (exact).

M_i 为 R-mod（或看成线性空间），f_i 为 R-mod 同态（或看成线性映射）

称为正合列，若 $\operatorname{Im} f_{i-1}=\ker f_i$

$0\to A\xrightarrow{f} B$ exact. $\Rightarrow f$ 单射.

$A\xrightarrow{f} B\to 0$ exact. $\Rightarrow f$ 满射.

$0\to A\xrightarrow{f} B\xrightarrow{g} C\to 0$. 短正合列. $C\simeq B/A$.

~~$(C=\operatorname{Im} f\simeq B/\ker f$~~.（B处正合）

$(C=\operatorname{Im} g\simeq B/\ker g=B/\operatorname{Im} f$

$=B/A)$.

(五引理).

$$\begin{tikzcd}
A_1 \arrow[r, "f_1"] \arrow[d, "h_1"] & A_2 \arrow[r, "f_2"] \arrow[d, "h_2"] & A_3 \arrow[r, "f_3"] \arrow[d, "h_3"] & A_4 \arrow[r, "f_4"] \arrow[d, "h_4"] & A_5 \arrow[d, "h_5"] \\
B_1 \arrow[r, "g_1"] & B_2 \arrow[r, "g_2"] & B_3 \arrow[r, "g_3"] & B_4 \arrow[r, "g_4"] & B_5
\end{tikzcd}$$

(3x3引理).

交换图

行正合，h_2，h_4 单，h_1 满 $\Rightarrow$ h_3 单.

h_2，h_4 满，h_5 单 $\Rightarrow$ h_3 满.

整性相关. R 为交换环(含幺). α 为 R 上整元素，若 $\exists f(x)\in R[x]$，

s.t $f(\alpha)=0$. (f 首一).

TFAE: (1) α 为 R 上整元素.

(2). $R[\alpha]$ 有限生成 R-模.

i.e. $R[\alpha]=\{\sum_{i=0}^{\infty} a_i\alpha^i, a_i\in R\} = Rx_1+\cdots+Rx_n$. (有限维向量空间).

(3) $\exists$. $T\supseteq R$，T 作为 R-模有限生成，$\alpha\in T$.

(1) $\Rightarrow$ (2). $1,\alpha,\ldots,\alpha^d$ 线性相关. $d=\deg f$.

取 $x_i=\alpha^i$，$R[\alpha]=Rx_0+\cdots+Rx_{n-1}$.

(2) $\Rightarrow$ (3). $T=R[\alpha]$

(3) $\Rightarrow$ (1). $T=Ry_1+\cdots+Ry_m$. $\alpha\in T \Rightarrow \alpha y_i\in T$

$\alpha y_i=\sum_{j=1}^{m} a_{ij}y_j$. $\Rightarrow$ $\cancel{\alpha I(y_1, \ldots, y_j)}$.

$$\alpha I\begin{pmatrix} y_1\\ \vdots \\ y_j\end{pmatrix} = A\begin{pmatrix} y_1\\ \vdots \\ y_j\end{pmatrix} \Rightarrow (\alpha I-A)\begin{pmatrix} y_1\\ \vdots \\ y_j\end{pmatrix}=0.$$

$y_1,\ldots,y_j$ 为基 $\Rightarrow$ $\det(\alpha I-A)=0$. $f(t)=\det(tI-A)$.

Jordan 标准形算矩阵指数 $\quad A\in M_{n\times n}(\mathbb{R})$

$$e^{xA} = I + xA + \frac{(xA)^2}{2!} + \cdots + \frac{(xA)^k}{k!} + \cdots \qquad \left(e^A = \sum_{n=0}^{\infty}\frac{A^n}{n!}\right)$$

$$\frac{d}{dx}e^{xA} = A + xA^2 + \frac{x^2A^3}{2!} + \cdots$$

$$= A(I + xA + \cdots) = Ae^{xA}$$

$\Rightarrow e^{xA}$ 满足 $\frac{d\Phi(x)}{dx} = A\Phi(x)$.

$e^{P^{-1}AP} = e^{A}$ $\Rightarrow$ 可将 A 化为 Jordan 标准形计算

$A \sim diag(J_1,\dots,J_s)$, J_i n_i阶.

$$e^{xA} = diag(e^{xJ_1},\dots,e^{xJ_s})$$

$$e^{xJ_i} = e^{x\left(\lambda_i I_{n_i} + \underbrace{\begin{pmatrix}0 & 1 & & \\ & \ddots & \ddots & \\ & & & 1\\ & & & 0\end{pmatrix}_{n_i\times n_i}}_{=N_{n_i}}\right)}$$

$$= e^{\lambda_i x}\left(I_{n_i} + xN_{n_i} + \frac{(xN_{n_i})^2}{2!} + \cdots + \frac{(xN_{n_i})^{n_i-1}}{(n_i-1)!}\right)$$

$$= e^{\lambda_i x}\begin{pmatrix}1 & x & \cdots & \frac{x^{n_i-1}}{(n_i-1)!}\\ & \ddots & \ddots & \vdots\\ & & \ddots & x\\ & & & 1\end{pmatrix}$$

$\frac{d\vec{y}}{dx}=A(x)\vec{y}$ n-dim 线性空间 (具体参考常微分方程相关教材)

密码学: 明文 P 密文 $\mathcal{C}$ 密钥 K

$\forall k\in K$, $\exists\ e_k\in\mathcal{E}$ $d_k\in\mathcal{D}$
(加密空间) (解密空间)

$e_k: P\to\mathcal{C}$, $d_k\to\mathcal{C}\to P$ $d_k(e_k(x))=x$

(互逆) e.g. $P=(\mathbb{Z}_{29})^n=\mathcal{C}$

$\mathcal{E},\mathcal{D}\in GL_n(\mathbb{F}_{29})$ 可逆矩阵

$e_k=k$, $d_k=k^{-1}$ (私钥, 较为简单)

(不知道密钥无法破解)

公钥 (公开加密体制和一部分信息

e.g. $p\in G$. G. 循环群, $a\in\mathbb{Z}$.

$p+a\to p^a$ ✓ $p^a+p\to a$ ✗

$a=\log_p p^a$ (离散对数)

(密钥交换) fixed G, A. 选 a, B 选 b. ($G=\langle p\rangle$)

A 算 p^a 给 B. B 算 p^b 给 a p, p^a, p^b ✓

无法得出 a,b!

p^{ab} 即为公共密钥.