0.1 互素多项式的应用

命题 0.1

设 $f(x), g(x)$ 是数域 $\mathbb{K}$ 上的互素多项式,A 是 $\mathbb{K}$ 上的 n 阶方阵, 满足 $f(A) = O$, 证明:$g(A)$ 是可逆矩阵.

证明 根据假设, 存在 $\mathbb{K}$ 上的多项式 $u(x), v(x)$, 使得

$$f(x)u(x) + g(x)v(x) = 1.$$

在上述式中代入 $x = A$, 可得恒等式

$$f(A)u(A) + g(A)v(A) = I_n.$$

因为 $f(A) = O$, 故有 $g(A)v(A) = I_n$, 从而 $g(A)$ 是非零矩阵且 $g(A)^{-1} = v(A)$.

□

命题 0.2

设 $f(x), g(x)$ 是数域 $\mathbb{K}$ 上的互素多项式,A 是 $\mathbb{K}$ 上的 n 阶方阵, 证明:$f(A)g(A) = O$ 的充要条件是 $r(f(A)) + r(g(A)) = n$.

证明 根据假设, 存在 $\mathbb{K}$ 上的多项式 $u(x), v(x)$, 使得

$$f(x)u(x) + g(x)v(x) = 1.$$

在上述式中代入 $x = A$, 可得恒等式

$$f(A)u(A) + g(A)v(A) = I_n.$$

考虑如下分块矩阵的初等变换:

$$\begin{pmatrix} f(A) & O \\ O & g(A) \end{pmatrix} \to \begin{pmatrix} f(A) & f(A)u(A) \\ O & g(A) \end{pmatrix} \to \begin{pmatrix} f(A) & I_n \\ O & g(A) \end{pmatrix} \to \begin{pmatrix} f(A) & I_n \\ -f(A)g(A) & O \end{pmatrix} \to \begin{pmatrix} O & I_n \\ -f(A)g(A) & O \end{pmatrix},$$

故有 $r(f(A)) + r(g(A)) = r(f(A)g(A)) + n$, 从而结论得证.

□

命题 0.3

设 $f(x), g(x)$ 是数域 $\mathbb{K}$ 上的互素多项式,φ 是 $\mathbb{K}$ 上 n 维线性空间 V 上的线性变换, 满足 $f(\varphi)g(\varphi) = 0$, 证明:$V = V_1 \oplus V_2$, 其中 $V_1 = \mathrm{Ker} f(\varphi), V_2 = \mathrm{Ker} g(\varphi)$.

笔记 这个命题告诉我们: 多项式的互素因式分解可以诱导出空间的直和分解, 从几何层面上看, 这就是相似标准型理论原始的出发点.

证明 根据假设, 存在 $\mathbb{K}$ 上的多项式 $u(x), v(x)$, 使得

$$f(x)u(x) + g(x)v(x) = 1.$$

在上述式中代入 $x = \varphi$, 可得恒等式

$$f(\varphi)u(\varphi) + g(\varphi)v(\varphi) = I_V.$$

对任意的 $\alpha \in V$, 由上述可得

$$\alpha = f(\varphi)u(\varphi)(\alpha) + g(\varphi)v(\varphi)(\alpha),$$

注意到

$$g(\varphi)(f(\varphi)u(\varphi)(\alpha)) = g(\varphi)f(\varphi)u(\varphi)(\alpha) = u(\varphi)f(\varphi)g(\varphi)(\alpha) = 0,$$
$$f(\varphi)(g(\varphi)u(\varphi)(\alpha)) = f(\varphi)g(\varphi)u(\varphi)(\alpha) = u(\varphi)f(\varphi)g(\varphi)(\alpha) = 0.$$

于是 $f(\varphi)u(\varphi)(\alpha) \in \mathrm{Ker}g(\varphi), g(\varphi)v(\varphi)(\alpha) \in \mathrm{Ker}f(\varphi)$, 故有 $V = V_1 + V_2$. 任取 $\beta \in V_1 \cap V_2$, 由上述可得

$$\beta = u(\varphi)f(\varphi)(\beta) + v(\varphi)g(\varphi)(\beta) = 0,$$

故有 $V_1 \cap V_2 = 0$, 因此 $V = V_1 \oplus V_2$.

□

例题 0.1 设 $\mathbb{Q}(\sqrt[n]{2}) = \{a_0 + a_1\sqrt[n]{2} + a_2\sqrt[4]{4} + \cdots + a_{n-1}\sqrt[n]{2^{n-1}} \mid a_i \in \mathbb{Q}, 0 \leqslant i \leqslant n-1\}$, 证明:$\mathbb{Q}(\sqrt[n]{2})$ 是一个数域, 并求 $\mathbb{Q}(\sqrt[n]{2})$ 作为 $\mathbb{Q}$ 上线性空间的一组基.

证明 设 $f(x) = x^n - 2$, 由 Eisenstein 判别法可知 $f(x)$ 在 $\mathbb{Q}$ 上不可约, 从而 $f(x)$ 是 $\sqrt[n]{2}$ 的极小多项式. 我们先证明:$a_0 + a_1\sqrt[n]{2} + \cdots + a_{n-1}\sqrt[n]{2^{n-1}} = 0$ 的充要条件是 $a_0 = a_1 = \cdots = a_{n-1} = 0$. 充分性是显然的, 现证必要性: 令 $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, 则 $g(\sqrt[n]{2}) = 0$, 由极小多项式的基本性质可得 $f(x) \mid g(x)$. 因为 $g(x)$ 的次数小于 n, 故只能是 $g(x) = 0$, 即 $a_0 = a_1 = \cdots = a_{n-1} = 0$.

利用 $\sqrt[n]{2} = 2$ 容易验证,$\mathbb{Q}(\sqrt[n]{2})$ 中任意两个数的加法、减法和乘法都是封闭的. 要证明 $\mathbb{Q}(\sqrt[n]{2})$ 是数域, 只要证明除法或者取倒数封闭即可. 任取 $\mathbb{Q}(\sqrt[n]{2})$ 中的非零数 $\alpha = a_0 + a_1\sqrt[2]{2} + \cdots + a_{n-1}\sqrt[n]{2^{n-1}} \neq 0$, 由上面的讨论可知 $a_0, a_1, \cdots, a_{n-1}$ 不全为零. 令 $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, 则 $g(\sqrt[n]{2}) \neq 0$. 因为 $f(x)$ 不可约且 $g(x) \neq 0$ 的次数小于 n, 故 $f(x)$ 与 $g(x)$ 互素, 由多项式互素的充要条件可知, 存在有理系数多项式 $u(x), v(x)$, 使得

$$f(x)u(x) + g(x)v(x) = 1,$$

在上述中代入 $x = \sqrt[n]{2}$, 可得 $\sqrt[n]{2}v(\sqrt[n]{2}) = 1$, 于是 $\alpha^{-1} = v(\sqrt[n]{2}) \in \mathbb{Q}(\sqrt[n]{2})$. 因此,$\mathbb{Q}(\sqrt[n]{2})$ 是数域.

由 $\mathbb{Q}(\sqrt[n]{2})$ 的定义可知,$\mathbb{Q}(\sqrt[n]{2})$ 中任一元都是 $1, \sqrt[2]{2}, \cdots, \sqrt[n]{2^{n-1}}$ 的 $\mathbb{Q}$-线性组合; 又由开始的讨论可知,$1, \sqrt[2]{2}, \cdots, \sqrt[n]{2^{n-1}}$ 是 $\mathbb{Q}$-线性无关的, 因此它们构成了 $\mathbb{Q}(\sqrt[n]{2})$ 作为 $\mathbb{Q}$ 上线性空间的一组基. 特别地,$\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[n]{2}) = n$.

□

命题 0.4

设 $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ 是数域 $\mathbb{K}$ 上的不可约多项式,φ 是 $\mathbb{K}$ 上 $m(\geqslant n)$ 维线性空间 V 上的线性变换,$\alpha_1 \neq 0, \alpha_2, \cdots, \alpha_n$ 是 V 中的向量, 满足

$$\varphi(\alpha_1) = \alpha_2, \varphi(\alpha_2) = \alpha_3, \cdots, \varphi(\alpha_{n-1}) = \alpha_n, \varphi(\alpha_n) = -a_n\alpha_1 - a_{n-1}\alpha_2 - \cdots - a_1\alpha_n.$$

证明:$\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ 线性无关.

证明 用反证法, 设存在不全为零的 n 个数 $c_1, c_2, \cdots, c_n$, 使得

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = 0,$$

则有

$$(c_1I_V + c_2\varphi + \cdots + c_n\varphi^{n-1})(\alpha_1) = 0.$$

令 $g(x) = c_1 + c_2x + \cdots + c_nx^{n-1}$, 则 $g(x) \neq 0$ 且 $g(\varphi)(\alpha_1) = 0$. 另一方面, 由条件容易验证 $f(\varphi)(\alpha_1) = 0$. 因为 $f(x)$ 不可约且 $g(x)$ 的次数小于 n, 故 $f(x)$ 与 $g(x)$ 互素, 从而存在 $\mathbb{K}$ 上的多项式 $u(x), v(x)$, 使得

$$f(x)u(x) + g(x)v(x) = 1.$$

在上述中代入 $x = \varphi$, 可得恒等式

$$f(\varphi)u(\varphi) + g(\varphi)v(\varphi) = I_V.$$

上式两边同时作用 α_1 可得

$$\alpha_1 = u(\varphi)f(\varphi)(\alpha_1) + v(\varphi)g(\varphi)(\alpha_1) = 0,$$

这与 $\alpha_1 \neq 0$ 矛盾!

□

例题 0.2 设 $\alpha, \beta, \gamma \in \mathbb{Q}^3$ 且 $\alpha \neq 0$. 若 $A \in \mathbb{Q}^{3\times3}$ 满足

$$A\alpha = \beta, A\beta = -\gamma, A\gamma = \alpha - \beta \Longleftrightarrow A\alpha = \beta, A\beta = \gamma, A\gamma = \alpha + \beta.$$

证明:α,β,γ 在 $\mathbb{Q}$ 上线性无关.

笔记 由命题 0.4可立得.

证明 若 α,β 在 $\mathbb{Q}$ 上线性相关, 则存在 $k\in\mathbb{Q}$, 使得 $\beta=k\alpha$. 从而由条件可得

$$A\alpha=\beta=k\alpha \Longrightarrow A\beta=kA\alpha=k^2\alpha=-\gamma \Longrightarrow A\gamma=\alpha-\beta=(1-k)\alpha=-k^2A\alpha=-k^3\alpha.$$

于是就有 $\left(k^3-k+1\right)\alpha=0$. 又 $\alpha\neq 0$, 故 $k^3-k+1=0$. 但这个方程没有有理根, 矛盾! 故 α,β 在 $\mathbb{Q}$ 上线性无关.

若 α,β,γ 在 $\mathbb{Q}$ 上线性相关, 则存在 $a,b\in\mathbb{Q}$, 使得 $\gamma=a\alpha+b\beta$. 由条件可得

$$A\gamma=\alpha-\beta=aA\alpha+bA\beta=a\beta-b\gamma=a\beta-b\left(a\alpha+b\beta\right)=-ab\alpha+\left(a+b^2\right)\beta.$$

因此

$$ab=1,\quad a+b^2=-1\Longrightarrow a+\frac{1}{a^2}=-1\Longrightarrow a^3-a^2+1=0,$$

而上式无有理根, 矛盾! 故 α,β,γ 在 $\mathbb{Q}$ 上线性无关.

□

例题 0.3 设 V 是 $\mathbb{Q}$ 上 4 维空间,φ 是 V 上的线性变换. 若

$$\alpha_i\in V, i=1,2,3,4,5.$$

且满足

$$\alpha_1\neq 0,\quad \alpha_4\neq\alpha_1+\alpha_2,\quad \varphi(\alpha_1)=\alpha_2,\quad \varphi\alpha_2=\alpha_3,$$
$$\varphi(\alpha_3)=\alpha_1+\alpha_2,\quad \varphi(\alpha_4)=\alpha_5,\quad \varphi(\alpha_5)=\alpha_3+\alpha_4.$$

求 $\det\varphi$.

证明 由命题 0.4可知 $\alpha_1,\alpha_2,\alpha_3$ 线性无关. 若 $\alpha_4\in\operatorname{span}\{\alpha_1,\alpha_2,\alpha_3\}$, 设

$$\alpha_4=a\alpha_1+b\alpha_2+c\alpha_3,\quad a,b,c\in\mathbb{Q}.$$

由条件可得

$$\varphi(\alpha_4)=\alpha_5\Longrightarrow\varphi^2(\alpha_4)=\varphi(\alpha_5)=\alpha_3+\alpha_4=a\alpha_1+b\alpha_2+(c+1)\alpha_3,$$

$$\varphi^2(\alpha_4)=\varphi^2(a\alpha_1+b\alpha_2+c\alpha_3)=\varphi\left(c\alpha_1+(a+c)\alpha_2+b\alpha_3\right)=b\alpha_1+(b+c)\alpha_2+(a+c)\alpha_3.$$

从而

$$a=b\quad,b=b+c,\quad c+1=a+c\Longrightarrow a=b=1,\quad c=0.$$

故 $\alpha_4=\alpha_1+\alpha_2$ 与条件矛盾! 因此 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ 线性无关. 又因为 V 是 $\mathbb{Q}$ 上 4 维空间, 所以 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ 就是 V 的一组基. 从而

$$\varphi\left(\alpha_1,\alpha_2,\alpha_3,\alpha_4\right)=(\alpha_1,\alpha_2,\alpha_3,\alpha_4)\begin{pmatrix}0&0&1&x\\1&0&1&y\\0&1&0&z\\0&0&0&m\end{pmatrix},$$

其中 $x,y,z,m\in\mathbb{Q}$. 由条件可知

$$\varphi^2(\alpha_4)=\varphi(\alpha_5)=\alpha_3+\alpha_4.$$

于是 $\varphi^2(\alpha_4)$ 的在基 $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ 下的坐标就是

$$\begin{pmatrix}0&0&1&x\\1&0&1&y\\0&1&0&z\\0&0&0&m\end{pmatrix}^2\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\1\\1\end{pmatrix}\Longleftrightarrow\begin{pmatrix}z+xm\\x+z+ym\\y+zm\\m^2\end{pmatrix}=\begin{pmatrix}0\\0\\1\\1\end{pmatrix}.$$

解得 $(x, y, z, m)^T = (-1, 0, 1, 1)^T$ 或 $(1, 2, 1, -1)^T$. 故

$$\det\varphi = \begin{vmatrix} 0 & 0 & 1 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix} = -1 \text{或} \begin{vmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & -1 \end{vmatrix} = 1.$$

□