4.4

2018年11月9日 13:18

§4.4 域上的代数

例: 1) $P[X] := \{\sum_{i=0}^{l} a_i x^i \mid l \geq 0, a_i \in P\}$

$(P[X], +, \cdot)$ 为环, 同时 $P[X]$ 为 P-向量空间且,

$\forall f, g \in P[X]$, $\lambda \in P$, $\lambda(fg) = f(\lambda g) = (\lambda f)g$

2) $M_n(P) := \{(a_{ij})_{n\times n} \mid a_{ij} \in P\}$

$(M_n(P), +, \cdot)$ 为环, $M_n(P)$ 为 P-向量空间.

$\forall a, b \in M_n(P)$, $\lambda \in P$

$\lambda(ab) = (\lambda a)b = a(\lambda b)$.

定义: P 为域, 集合 A 称为 P 上的代数 (或 P-代数), 若 A 为 P-向量空间且

$\exists$ 运算 $\cdot$: $A \times A \longrightarrow A$ 满足

$(a, b) \longrightarrow a\cdot b$

1) $\forall a, b, c \in A$

$(a+b)\cdot c = a\cdot c + b\cdot c$ $c(a+b) = ca + c\cdot b$ (分配律)

2) $\forall a, b \in A$, $\lambda \in P$

$\lambda(a\cdot b) = (\lambda a)\cdot b = a\cdot(\lambda b)$. (双线性性)

3) $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ (结合律) (有些书中定义不要求3)).

进一步满足: 4) $\exists 1 \in A$, s.t. $1\cdot a = a\cdot 1 = a$, 称 A 为含幺代数.

A 为 P 上的代数, 则 $(A, +, \cdot)$ 为环.

定义': 集合 A 称为 P-代数, 若 A 具有环与 P-向量空间的结构且满足:

1) 环中的加法与 P-向量空间中的加法是相同的

2) 环的乘法运算是 P-双线性映射, i.e. $(\lambda a)b = a(\lambda b) = \lambda(ab)$.

$B \subseteq A$ 称为子代数, 若 B 为子环同时为子空间.

$\{B_\lambda \mid \lambda \in I\}$ 为 A 的子代数的集合则 $\bigcap_{\lambda\in I} B_\lambda$ 依然为子代数.

$T \subseteq A$ 为子集. $P[T] :=$ 由 T 生成的子代数

$$= \bigcap_{T\subseteq B\subseteq A \text{ 子代数}} B$$

A, B 为 P 上的代数.

映射 $\varphi: A \longrightarrow B$ 为代数同态, 若 φ 为环同态且为 P-线性映射.

类似地，可定义代数同构.

$B \subseteq A$ 称为 A 的理想 若 B 为 $(A,+,\cdot)$ 的理想且为子空间.

B 为 A 的理想. 则 A/B 为商空间 A/B 作为商环的乘法满足代数公理

$$\left(\begin{aligned}\lambda[(a_1+B)(a_2+B)] &= \lambda a_1 a_2 + B = (\lambda a_1 + B)(a_2+B)\\ &= (a_1+B)(\lambda a_2 + B)\end{aligned}\right)$$

$\therefore A/B$ 为 P 上的代数称为商代数.

例: Γ 为含幺群. $P[\Gamma] := \left\{ \sum_{\gamma\in\Gamma} a_\gamma \gamma \;\middle|\; \begin{array}{l} a_\gamma \in P \\ \text{仅有限个 } a_\gamma \neq 0 \end{array} \right\}$ (形式和)

· $\sum a_\gamma \gamma = \sum b_\gamma \gamma \Leftrightarrow \forall \gamma\in\Gamma,\ a_\gamma = b_\gamma$

· $\sum a_\gamma \gamma + \sum b_\gamma \gamma := \sum (a_\gamma + b_\gamma)\gamma$

· $(\sum a_\gamma \gamma)(\sum b_{\gamma'}\gamma') := \sum_{\gamma}\sum_{\gamma'} a_\gamma a_{\gamma'} \gamma\gamma'$

可验证: $P[\Gamma]$ 为 P-代数.

· 令 $\Gamma = \{1, X, X^2, \cdots\}$. 则 $P[\Gamma] = P[X]$.

· 当 Γ 为群时. $P[\Gamma]$ 称为群代数.

$\dim_P(A)$ 称为 P-代数 A 的维数.

命题1: n 维 P-代数同构于 $M_k(P)$ 的一个子代数, $k \le n+1$.

证: 设 $1\in A$, 且 $u_1=1, u_2, \cdots u_n$ 为 A 的一组基作为 P-向量空间.

$\forall a\in A.\ \exists!\ L_a \in M_n(P)$ s.t $a(u_1,\cdots u_n) = (u_1,\cdots u_n)L_a$

定映射 φ: $\begin{array}{ccc} A & \longrightarrow & M_n(P) \\ a & \longrightarrow & L_a \end{array}$

$$(a+b)(u_1,\cdots u_n) = a(u_1,\cdots u_n)+b(u_1,\cdots u_n) = (L_a+L_b)(u_1,\cdots u_n)$$

$$\Rightarrow \varphi(a+b) = \varphi(a)+\varphi(b)$$

$$ab(u_1,\cdots u_n) = a(u_1,\cdots u_n)L_b = (u_1,\cdots u_n)L_aL_b$$

$$\Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$$

$$\lambda a(u_1,\cdots u_n) = (u_1,\cdots u_n)\lambda L_a \Rightarrow \varphi(\lambda a) = \lambda\varphi(a)$$

$\therefore \varphi$ 是 P-代数同态.

设 $L_a = 0$. 则 $a(u_1,\cdots u_n) = 0 \Rightarrow au_1 = 0 \Rightarrow a = 0$

$\Rightarrow \varphi$ 为单射

设 A 不含幺元. 令 $\overline{A} = P\oplus A$ 且定乘法:

$$(\lambda, a)\cdot(\lambda', a') = (\lambda\lambda', aa' + \lambda a' + \lambda' a)$$

则 $\overline{A}$ 为 P-代数且含幺元 $(1, 0)$.

$\because \dim_P \overline{A} = \dim_P A + 1 = n+1$. 由已证结果知 $\overline{A}$ 同构于 $M_{n+1}(P)$ 之子代数. □

中心 $Z(A) := \{a \in A \mid ab = ba \ \forall\, b \in A\}$.

$Z(A)$ 为 A 之子代数.

例: $Z(M_n(P)) = \{\lambda I_n \mid \lambda \in P\} \cong P$.

设 A 为含幺 P-代数. 定义 $\varphi: P \to A$

$$\lambda \longrightarrow \lambda \cdot 1$$

乘法双线性 $\Rightarrow \varphi(P) \subseteq Z(A)$, $1 \cdot 1 = 1 \neq 0 \Rightarrow \varphi(P) \neq \{0\}$

$\Rightarrow \varphi$ 是单同态

定义': 含幺环 A 称为 P-代数如果存在单同态 $\varphi: P \to Z(A)$.

P-代数 A 称为单的, 如果 $\{0\}$ 与 A 是其所有的(双边)理想.

A 称为中心单的, 如果 A 是单代数且 $Z(A) \cong P$.

命题2: $M_n(P)$ 是中心单代数.

证: 设 $I \subseteq M_n(P)$ 为理想且 $I \neq \{0\}$. 设 $0 \neq a = \sum_{i,j} a_{ij} E_{ij} \in I$,

其中 $E_{ij} = \begin{pmatrix} & & \\ & 1 & \\ & & \end{pmatrix}$ (i 行, j 列). 设 $a_{kl} \neq 0$. 则 $\forall\, 1 \le s, t \le n$, $E_{st} = a_{kl}^{-1} E_{sk}\, a\, E_{lt} \in I$

$\Rightarrow M_n(P) = I$.

可除代数: A 为 P-代数且 $(A, +, \cdot)$ 为除环则称 A 为可除代数.

注: 设 D 为可除代数则 $M_n(D)$ 是单代数.

Wedderburn-Artin 定理: P 上有限维单代数 A 同构于 $M_n(D)$, 其中 D 为

可除代数且 n 与 D 由 A 唯一确定.

例: · P 本身是可除代数.

· $\mathbb{C}$ 是可除 $\mathbb{R}$-代数

· $\mathbb{H}$ 是可除 $\mathbb{R}$-代数. (而且是中心单的)

设 A 为有限维可除 P-代数.

· P 为有限域 $\Rightarrow A$ 为域 (Frobenius)

· $P = \mathbb{R}$ $\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$ 为所有的有限维可除 $\mathbb{R}$-代数.

设A为含幺P-代数.

A含幺 $\Rightarrow P \hookrightarrow Z(A) \Rightarrow$ 将P看作A的子环.

此时 向量空间的数乘 $\longrightarrow$ 环的乘法

$\lambda \cdot a \longrightarrow (\lambda \cdot 1) \cdot a$.

$a \in A$ 称为P上代数的, 如果 $1, a, a^2, \cdots$ P-线性相关.

即 $\exists f(X) \in P[X], f(X) \neq 0$, s.t $f(a) = 0$.

称使得 $f(a)=0$ 的次数最小的多项式 $f(X)$ 为 a 的极小多项式. 记作 $\mu_a(X)$.

命题3: 设A为n维含幺P-代数.

1) a在P上代数且 $\deg(\mu_a(X)) \leq n$.

2) a为可逆元 $\Leftrightarrow \mu_a(0) \neq 0$.

3) 若A中无零因子, 则A是可除代数, 进一步若P是代数闭域

则 $n=1$, $A = P \cdot 1$

证: 1) $\dim_P A = n \Rightarrow 1, a, \cdots, a^n$ 在P上线性相关.

即 $\exists \lambda_0, \lambda_1, \cdots \lambda_n \in P$ 不全为0 s.t $\sum_{i=0}^{n} \lambda_i a^i = 0$

$\therefore$ a在P上代数且 $\deg(\mu_a(X)) \leq n$.

2) ($\Rightarrow$) 若 $\mu_a(0)=0$. 则 $\mu_a(X) = X \cdot f(X)$, $f(X) \in P[X]$ 且 $\deg f(X) < \deg \mu_a(X)$

$\mu_a(a) = 0 \Rightarrow a f(a) = 0 \Rightarrow f(a) = 0$ 与 $\mu_a(X)$ 次数极小矛盾.

($\Leftarrow$) 注意到 $\mu_a(0) \in P \cdot 1$, $\mu_a(0) \neq 0 \Rightarrow \mu_a(0) = \lambda \cdot 1$, $\lambda \neq 0$.

$(-\lambda^{-1})\mu_a(X) = (-\lambda^{-1}) X f(X) - 1 \Rightarrow (-\lambda^{-1}) a f(a) - 1 = 0$

$\Rightarrow$ a 可逆.

3) $\forall a \in A \setminus 0$. 断言 $\mu_a(0) \neq 0$ (从命题2 a可逆 $\Rightarrow$ A是可除代数)

设 $\mu_a(0)=0$. 则 $\mu_a(X) = X f(X)$, $f(X) \in P[X]$ 且 $\deg f(X) < \deg \mu_a(X)$

$\left.\begin{array}{l} 0 = \mu_a(0) = a f(a) \\ f(a) \neq 0 \end{array}\right\} \Rightarrow$ a是零因子 矛盾.

设P为代数闭域. 则 $\mu_a(X) = \prod_{i=1}^{l} (X - c_i)$ $c_i \in P$.

$\because \prod_{i=2}^{l} (a - c_i) \neq 0 \quad \therefore \prod_{i=2}^{l} (a - c_i)$ 可逆

$\therefore a - c_1 = \mu_a(X) \cdot \left(\prod_{i=2}^{l} (a - c_i)\right)^{-1} = 0 \Rightarrow a = c_1 \in P$.

设 $P = \mathbb{R}$. A为有限维P-可除代数.

命题3 $\Rightarrow \mu_a(X)$ 是不可约的，且 $\deg \mu_a(X) \le 2$. □

推论：设 A 为有限维可除 $\mathbb{R}$-代数，$a \in A \setminus \mathbb{R}$. 则 $\mathbb{R}[a] \cong \mathbb{C}$

证：由命题3：$\mu_a(X)$ 是不可约的且 $\deg \mu_a(X) = 2$.

设 $\mu_a(X) = X^2 + \alpha X + \beta$, $\alpha, \beta \in \mathbb{R}$ 且 $\alpha^2 - 4\beta < 0$

令 $x = \frac{2}{\sqrt{4\beta - \alpha^2}}(a + \frac{\alpha}{2})$. 则 $\mu_a(a) = 0 \Rightarrow x^2 + 1 = 0$.

易知：$\mathbb{R}[a] = \mathbb{R}[x] := \left\{ \sum_{i=0}^{n} c_i x^i \;\middle|\; \begin{matrix} n \ge 0 \\ c_i \in \mathbb{R} \end{matrix} \right\}$

$= \{ c_0 + c_1 x \mid c_0, c_1 \in \mathbb{R} \}$.

考虑：$\varphi: \mathbb{R}[X] \longrightarrow \mathbb{R}[x]$, $f(X) \longrightarrow f(x)$ 易验证 φ 为 $\mathbb{R}$-代数满同态.

$\ker \varphi = \langle X^2 + 1 \rangle \Rightarrow \mathbb{R}[x] \cong \mathbb{R}[X] / \langle X^2 + 1 \rangle$.

同理可证：$\mathbb{C} = \mathbb{R}[\sqrt{-1}] \cong \mathbb{R}[X] / \langle X^2 + 1 \rangle$.

$\therefore \mathbb{R}[x] \cong \mathbb{C}$ □

定理1（Frobenius）$\mathbb{R}$ 上的有限维可除代数只有 $\mathbb{R}$, $\mathbb{C}$ 及 $\mathbb{H}$.

证：设 A 为 $\mathbb{R}$ 上的有限维可除代数.

· 若 $\dim_{\mathbb{R}} A = 1$. 则 $A = \mathbb{R}$

· 设 $\dim_{\mathbb{R}} A \ge 2$. 取 $a \in A \setminus \mathbb{R}$. 则由推论知 $\mathbb{R}[a] \cong \mathbb{C}$.

即 $\exists$ 单同态 $\varphi: \mathbb{C} \longrightarrow A$. 将 $\mathbb{C}$ 看作 A 的 $\mathbb{R}$-子代数.

考虑左乘：$\mathbb{C} \times A \longrightarrow A$, $(\lambda, a) \longrightarrow \lambda a$ 赋予 A $\mathbb{C}$-向量空间结构.

令 $A^+ := \{ a \in A \mid ia = ai \}$. $i = \sqrt{-1}$

$A^- := \{ a \in A \mid ia = -ai \}$

1) A^+, A^- 为 $\mathbb{R}$-向量空间. 且 $A = A^+ \oplus A^-$ (向量空间内直和)

$\forall a \in A$, $a = \underbrace{\frac{a + iai}{2}}_{\in A^-} + \underbrace{\frac{a - iai}{2}}_{\in A^+} \in A^+ + A^-$

$a \in A^+ \cap A^- \Rightarrow ai = -ai \Rightarrow a = 0 \Rightarrow A^+ \cap A^- = \{0\}$.

2) $\forall a \in A \setminus \{0\}$, $a \in A^-$ (或 A^+) $\Rightarrow a^{-1} \in A^-$ (或 A^+)

3) A^+, A^- 为 $\mathbb{C}$-向量空间.

$\forall a_1, a_2 \in A^+, \lambda_1, \lambda_2 \in \mathbb{C}$

$$\begin{aligned} i(\lambda_1 a_1 + \lambda_2 a_2) &= i\lambda_1 a_1 + i\lambda_2 a_2 = (i\lambda_1)a_1 + (i\lambda_2)a_2 \\ &= (\lambda_1 i)a_1 + (\lambda_2 i)a_2 = \lambda_1 i a_1 + \lambda_2 i a_2 \\ &= \lambda_1 a_1 i + \lambda_2 a_2 i = (\lambda_1 a_1 + \lambda_2 a_2) i \end{aligned}$$

$\Rightarrow \lambda_1 a_1 + \lambda_2 a_2 \in A^+$

同理 A^- 为 $\mathbb{C}$-向量空间.

4) A^+ 是 $\mathbb{C}$-代数.

$\forall a, b \in A^+ \quad \lambda \in \mathbb{C}, \quad \lambda = \lambda_1 + \lambda_2 i \quad \sqrt{-1}\, ab = a\sqrt{-1}\, b = ab\sqrt{-1} \Rightarrow ab \in A^+$

$\Rightarrow (A^+, +, \cdot)$ 为环.

$$\begin{aligned} a(\lambda b) &= a[(\lambda_1 + \lambda_2 i)b] = a[\lambda_1 b + \lambda_2 (ib)] = a(\lambda_1 b) + a[\lambda_2 (ib)] \\ &= \lambda_1 (ab) + \lambda_2 (aib) = \lambda_1 (ab) + \lambda_2 (aib) = \lambda_1 (ab) + \lambda_2 i (ab) \\ &= (\lambda_1 + \lambda_2 i)(ab) = \lambda (ab) \end{aligned}$$

由结合律知: $(\lambda a) b = \lambda (ab)$.

$\because \mathbb{C}$ 是代数闭域 $\therefore$ 由命题3, $\Rightarrow A^+ = \mathbb{C}$.

i) 若 $A^- = \{0\}$. 则 $A = A^+ = \mathbb{C}$.

ii) 设 $A^- \neq \{0\}$. 令 $b \in A^- \setminus \{0\}$.

$\forall a \in A^-, \quad iab = -aib = abi \Rightarrow ab \in A^+$

定义 $\varphi_b : A^- \longrightarrow A^+$, $a \longrightarrow ab$ 为 $\mathbb{C}$-线性映射 且 $\ker \varphi_b = \{0\}$

$\therefore 1 \leq \dim_{\mathbb{C}} A^{-1} \leq \dim_{\mathbb{C}} A^+ = 1 \Rightarrow \dim_{\mathbb{C}} A^- = 1$.

$\Rightarrow \varphi_b$ 为同构.

$\therefore A = \mathbb{C} \oplus \mathbb{C} b^{-1} = (\mathbb{R} \oplus \mathbb{R} i) \oplus (\mathbb{R} \oplus \mathbb{R} i) b^{-1}$

$b^{-1} \notin \mathbb{R} \Rightarrow \deg \mu_{b^{-1}}(X) = 2 \Rightarrow (b^{-1})^2 = \alpha b^{-1} + \beta, \ \alpha, \beta \in \mathbb{R}$ 且 $\alpha^2 + 4\beta < 0$

又 $\because (b^{-1})^2 \in A^+ = \mathbb{C} \quad \therefore \alpha = 0$ (否则 $b^{-1} \in \mathbb{C} = A^+$ 矛盾) $\Rightarrow \beta < 0$.

令 $j = \frac{b^{-1}}{\sqrt{-\beta}}$. 则 $j^2 = -1$. 且 $A = \mathbb{R} \oplus \mathbb{R} i \oplus \mathbb{R} j \oplus \mathbb{R} ij$

其中 $i^2 = -1, \ j^2 = -1, \ ij = -ji \ (\because j \in A^-)$

由 $\mathbb{H}$ 构造知 $A = \mathbb{H}$.

□