

第五章 复数域和多项式

6.3 重数

定义 6.19 设 D 是唯一因子分解整环, $a \in D^*$ 和 $p \in D^*$ 是不可约元. 如果非负整数 m 使得 $p^m | a$ 但 $p^{m+1} \nmid a$, 则称 m 是 p 在 a 中的重数 (*multiplicity*), 记为 $\text{mult}_p(a)$.

因为 D 是唯一因子分解整环, 所以定义中的非负整数 m 一定存在. 换言之, $\text{mult}_p(a)$ 是良定义的, 且 $p \nmid a$ 当且仅当 $\text{mult}_p(a) = 0$.

对于相伴的不可约元, 它们的重数是一样的. 这是因为对不可约元而言相伴等价与相互整除. 这一事实在本节的推理中经常用到.

引理 6.20 设 D 是唯一因子分解整环, $a, b \in D^*$, $p \in D$ 不可约. 则 $\text{mult}_p(ab) = \text{mult}_p(a) + \text{mult}_p(b)$.

证明. 设 $m = \text{mult}_p(a)$ 和 $n = \text{mult}_p(b)$. 则 $p^m | a$ 和 $p^n | b$. 故 $p^{m+n} | ab$. 注意到存在 $c, d \in D^*$ 使得 $a = cp^m$ 和 $b = dp^n$. 从而, $ab = cdp^{m+n}$.

假设 $p^{m+n+1} | ab$. $p | cd$. 因为 p 是素元, 所以 $p | c$ 或 $p | d$. 由此得出, $\text{mult}_p(a) > m$ 或 $\text{mult}_p(b) > n$, 矛盾. 故 $\text{mult}_p(ab) = m + n$. \square

定理 6.21 (标准不可约分解) 在唯一因子分解整环中, 每个非零非可逆元 a 可表示为

$$a \approx p_1^{m_1} \cdots p_k^{m_k},$$

其中 p_1, \dots, p_k 是两两互不相伴的不可约元, $m_i = \text{mult}_{p_i}(a) > 0$, $i = 1, \dots, k$.

证明. 设 a 有不可约分解 $a = q_1 \cdots q_l$. 令 $p_1 = q_1$.

我们对 l 归纳. 如果 $l = 1$, 则结论显然成立. 设 $l > 1$ 且当元素是小于 l 个不可约元之积时结论成立.

再设 $p_1 \approx q_i$, $i = 1, 2, \dots, m_1$ 且 p_1 与 q_{m_1+1}, \dots, q_l 都不相伴. 则 $a \approx p_1^{m_1} q_{m_1+1} \cdots q_l$. 如果 $m_1 = l$, 则结论成立. 否则对 $b = q_{m_1+1} \cdots q_l$ 应用归纳假设得

$$b \approx p_2^{m_2} \cdots p_k^{m_k},$$

其中 p_2, \dots, p_k 是两两互不相伴的不可约元, $m_i = \text{mult}_{p_i}(b)$ 为正, $i = 2, \dots, k$.

假设 $p_1^{m_1+1} | a$. 则 $p_1 | b$. 故存在 $i \in \{m_1 + 1, \dots, l\}$ 使得 $p_1 | q_j$. 故 $p_1 \approx q_j$ (因为 p_1 和 q_j 都不可约), 矛盾. 从而我们有 $m_1 = \text{mult}_{p_1}(a)$. 特别地, $p_1 \nmid b$. 故 p_1 与 p_2, \dots, p_k 都不相伴. 对任意 $i \in \{2, \dots, k\}$, 上述引理蕴含

$$\text{mult}_{p_i}(a) = \text{mult}_{p_i}(p_1^{m_1}) + \text{mult}_{p_i}(b) = \text{mult}_{p_i}(b). \quad \square$$

因为 \mathbb{Z} 和 $F[x]$ 是唯一因子分解整环, 我们有:

定理 6.22 (算术学基本定理) 设 $n \in \mathbb{Z} \setminus \{0, 1, -1\}$. 则存在唯一的两两不同的素数 p_1, p_2, \dots, p_m 和正整数 i_1, i_2, \dots, i_m 使得

$$n = \pm p_1^{i_1} p_2^{i_2} \cdots p_m^{i_m}.$$

定理 6.23 设 $f \in F[x]$. 则存在唯一的两两不相等的不可约且首一的多项式 $p_1, p_2, \dots, p_m \in F[x]$, $i_1, i_2, \dots, i_m \in \mathbb{Z}^+$, $u \in F^*$ 使得

$$f = \text{lc}(f) p_1^{i_1} p_2^{i_2} \cdots p_m^{i_m}.$$

定义 6.24 设 $f \in F[x]^*$ 和 $x - \alpha \in F[x]$. 设 $x - \alpha$ 在 f 中的重数 m 为正. 则称为 α 是 f 中的 m 重根. 当 $m = 1$ 时, α 称为 f 的单根 (*simple root*); 当 $m > 1$ 时, α 称为 f 的重根 (*multiple root*).

例 6.25 $44 = 2^2 \cdot 11 = -(-2)^2 \cdot (-11)$.

$$242340461377689532 = 41 \cdot (11 \cdot 2^2 \cdot 13) \cdot 3214571^2.$$

例 6.26 设

$$f = \underbrace{(2x - 1)}_{q_1} \underbrace{(10x - 5)}_{q_2} \underbrace{\left(\frac{1}{2}x^2 - \frac{1}{3}x + 2\right)}_{q_3} \in \mathbb{Q}[x].$$

一次多项式 q_1 和 q_2 是 $\mathbb{Q}[x]$ 中的不可约多项式. 二次多项式 q_3 的判别式小于零. 故 q_3 也是 $\mathbb{Q}[x]$ 中的不可约多项

式. 计算每个因子的首一部分得到

$$f = 10 \underbrace{\left(x - \frac{1}{2}\right)}_{p_1}^2 \underbrace{\left(x^2 - \frac{2}{3}x + 4\right)}_{p_2}.$$

6.4 Gauss 引理

在本节中, 为简介起见, 我们令 $D = \mathbb{Z}$. 当 D 是唯一因子分解整环时结论都成立且证明类似. 我们进一步规定最大公因子都是正整数.

定义 6.27 设

$$f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0, \quad f_i \in \mathbb{Z}, f_n \neq 0.$$

则

$$\gcd(f_n, f_{n-1}, \dots, f_0)$$

称为 f 的容度 (*content*), 记为 $\text{cont}(f)$. 设 $f = \text{cont}(f)g$, 其中 $g \in \mathbb{Z}[x]^*$ 满足 $\text{cont}(g) = 1$. 称 g 是 f 的本原部分 (*primitive part*), 记为 $\text{pp}(f)$.

设 $h \in \mathbb{Z}[x]^*$. 如果 $\text{cont}(h) = 1$, 则称 h 是本原多项式.

引理 6.28 设 $a_1, \dots, a_n \in \mathbb{Z}$ 不全为零, $c \in \mathbb{Z}^*$. 则

$$\gcd(ca_1, \dots, ca_n) = |c| \gcd(a_1, \dots, a_n).$$

证明. 设 $g = \gcd(a_1, \dots, a_n)$. 则 cg 是 ca_1, \dots, ca_n 的公因子. 故存在 $b_i \in \mathbb{Z}$, 使得 $a_i = b_i g$, $i = 1, 2, \dots, k$. 设 $d = \gcd(b_1, \dots, b_n)$. 则 dg 是 a_1, \dots, a_n 公因子. 故 $(dg)|g$. 由此得 $d = 1$.

再设 $h = \gcd(ca_1, \dots, ca_n)$. 则存在 $k_i \in \mathbb{Z}$, 使得

$$ca_i = k_i h,$$

$i = 1, \dots, n$, 和存在 $u \in \mathbb{Z}$ 使得 $h = ucg$. 由以上等式得

$$cb_i g = k_i ucg \implies b_i = k_i u,$$

$i = 1, \dots, n$. 则 u 是 b_1, \dots, b_n 的公因子. 于是, $u|d$. 从而 $u = \pm 1$. 于是 $h = \pm cg$. \square

注解 6.29 上述引理蕴含: 如果 $f = ch$, 其中 $c \in \mathbb{Z}$ 和 $h \in \mathbb{Z}[x]$ 是本原的. 则

$$c > 0 \implies \text{cont}(f) = c \quad \text{且} \quad \text{pp}(f) = h,$$

$$c < 0 \implies \text{cont}(f) = -c \quad \text{且} \quad \text{pp}(f) = -h.$$

上述引理蕴含 $\text{cont}(f) = |c|$. 从而,

$$\text{cont}(f) \approx c \quad \text{和} \quad \text{pp}(f) \approx h.$$

引理 6.30 (Gauss) 设 $f, g \in \mathbb{Z}[x]^*$ 都是本原多项式. 则 fg 也是本原多项式.

证明. 设

$$f = f_m x^m + f_{m-1} x^{m-1} + \cdots + f_0$$

和

$$g = g_n x^n + g_{n-1} x^{n-1} + \cdots + g_0,$$

其中 $f_m, f_{m-1}, \dots, f_0, g_n, g_{n-1}, \dots, g_0 \in \mathbb{Z}$ 且 f_m, g_n 都非零. 假设 fg 不是本原的. 则存在素数 p 使得 $p | \text{cont}(fg)$. 因为 $\text{cont}(f) = 1$, 所以存在 $i \in \{0, 1, \dots, m\}$ 使得

$$p | f_m, p | f_{m-1}, \dots, p | f_{i+1}, \text{ 但 } p \nmid f_i.$$

同理存在 $j \in \{0, 1, \dots, n\}$ 使得

$$p | g_n, p | g_{n-1}, \dots, p | g_{j+1}, \text{ 但 } p \nmid g_j.$$

注意到在 fg 在中 x^{i+j} 的系数是

$$c = \sum_{k+l=i+j} f_k g_l \quad \text{且} \quad p | c.$$

如果 $l < j$, 则 $k > i$. 故 $p | f_k \implies p | f_k g_l$. 如果 $l > j$, 则 $p | g_l$. 故 $p | f_k g_l$. 于是, $p | f_i g_j$. 故 $p | f_i$ 或 $p | g_j$. 矛盾. \square

定理 6.31 设 $f \in \mathbb{Z}[x]$ 且 $\deg(f) > 0$. 如果 f 不能写成两个 $\mathbb{Z}[x]$ 中正次数的多项式之积. 则 f 在 $\mathbb{Q}[x]$ 不可约.

证明. 假设 $f = gh$, 其中 $g, h \in \mathbb{Q}[x] \setminus \mathbb{Q}$. 则存在 $\alpha, \beta \in \mathbb{Z}$ 使得

$$\alpha f = \beta \tilde{g}\tilde{h},$$

其中 $\alpha, \beta \in \mathbb{Z}^*$, $\tilde{g}, \tilde{h} \in \mathbb{Z}[x]$ 是本原多项式, $\deg \tilde{g} = \deg(g)$, $\deg(\tilde{h}) = \deg(h)$. 根据注释 6.29, $\alpha \text{cont}(f) \text{pp}(f) = \beta(\tilde{g}\tilde{h})$. 我们得到 $\text{pp}(f) = u\tilde{g}\tilde{h}$, 其中 $u \in \{1, -1\}$. 故

$$f = \text{cont}(f) \text{pp}(f) = (\text{cont}(f)u\tilde{g})\tilde{h}.$$

矛盾. \square

定理 6.32 (*Eisenstein* 不可约性判别法) 设

$$f = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0,$$

其中 $n > 0$, $f_n, f_{n-1}, \dots, f_0 \in \mathbb{Z}$ 且 $f_n \neq 0$. 设 p 是素数. 如果

$$p \nmid f_n, p \mid f_{n-1}, \dots, p \mid f_0, p^2 \nmid f_0,$$

则 f 在 $\mathbb{Q}[x]$ 中不可约.

证明. 由上述定理可知, 我们只要证明 f 不能写成 $\mathbb{Z}[x]$ 中两个正次数的多项式之积即可. 假设

$$f(x) = (g_k x^k + \cdots + g_1 x + g_0)(h_\ell x^\ell + \cdots + h_1 x + h_0),$$

其中 $k, \ell \in \mathbb{Z}^+$, $g_k, \dots, g_1, g_0, h_\ell, \dots, h_1, h_0 \in D$ 且 g_k, h_ℓ 都不等于零.

因为 $f_n = g_k h_\ell$ 且 $p \nmid g_k h_\ell$, 所以 $p \nmid g_k$ 和 $p \nmid h_\ell$. 因为 $f_0 = g_0 h_0$ 和 $p \mid f_0$, 所以 $p \mid g_0$ 或 $p \mid h_0$. 不妨设 $p \mid g_0$. 又因为 $p^2 \nmid f_0$, 所以 $p \nmid h_0$. 因为 $p \nmid g_k$ 和 $p \mid g_0$, 所以存在 $i \in \{0, 1, \dots, k\}$ 使得

$$p \mid g_0, \dots, p \mid g_{i-1} \quad \text{但} \quad p \nmid g_i.$$

则 $f_i = h_0 g_i + h_1 g_{i-1} + \dots + h_i g_0$. 因为 $i \leq k < n$, 所以 $p \nmid f_i$. 由此可知, $p \nmid h_0 g_i$. 故 $p \nmid h_0$ 或 $p \nmid g_i$. 矛盾. \square

例 6.33 证明: 对于 $n > 1$, $x^n - 2x + 2$ 在 $\mathbb{Q}[x]$ 中不可约. 证明. 注意到 $2 \nmid 1$, $2 \mid -2$, $2 \mid 2$ 但 $2^2 \nmid 2$. 根据定理 6.32, 该多项式不可约.

例 6.34 设 p 是素数. 证明: $x^{p-1} + x^{p-2} + \dots + x + 1$ 在 $\mathbb{Q}[x]$ 中不可约.

证明. 设 $f(x) = x^{p-1} + x^{p-2} + \dots + x + 1$. 考虑映射

$$\begin{aligned} \phi: \mathbb{Z}[x] &\longrightarrow \mathbb{Z}[x] \\ g(x) &\longmapsto g(x+1). \end{aligned}$$

则 ϕ 是由 $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]$ 和 $x \mapsto x+1$ 诱导的环同态. 同理

$$\begin{aligned} \psi: \mathbb{Z}[x] &\longrightarrow \mathbb{Z}[x] \\ g(x) &\longmapsto g(x-1) \end{aligned}$$

也是环同态. 因为 $\phi \circ \psi = \psi \circ \phi = \text{id}_{\mathbb{Z}[x]}$, 所以 ϕ 是环同构.

要证明 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约. 只要证明 $f(x+1)$ 在 $\mathbb{Z}[x]$ 中不可约 (定理 6.31). 由于 ϕ 是同构, 只要证明 $f(x+1)$ 在 $\mathbb{Z}[x]$ 中不可约即可. 注意到

$$f(x) = \frac{x^p - 1}{x - 1} \implies f(x+1) = \frac{(x+1)^p - 1}{x}.$$

故

$$f(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{2}x + p.$$

由第二章第一讲例 7.17 和定理 6.32 可知, $f(x+1)$ 不可约. 故 $f(x)$ 也不可约.

第一章 空间与形式

1 线性空间

1.1 抽象的线性空间

定义 1.1 设 $(V, +, \mathbf{0})$ 是交换群, $(F, +, 0, \cdot, 1)$ 域. 设数乘是映射:

$$\begin{aligned} \text{数乘: } F \times V &\longrightarrow V \\ (\alpha, \mathbf{v}) &\longmapsto \alpha\mathbf{v} \end{aligned}$$

满足以下规律

$$(i) \quad \forall \alpha, \beta \in F, \mathbf{v} \in V, (\alpha\beta)\mathbf{v} = \alpha(\beta\mathbf{v});$$

$$(ii) \quad \forall \mathbf{v} \in V, 1\mathbf{v} = \mathbf{v};$$

$$(iii) \quad \forall \alpha, \beta \in F, \mathbf{v} \in V, (\alpha + \beta)\mathbf{v} = \alpha\mathbf{v} + \beta\mathbf{v};$$

$$(iv) \quad \forall \alpha \in F, \mathbf{u}, \mathbf{v} \in V, \alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}.$$

我们称 $(V, +, \mathbf{0}, \text{数乘}, 1)$ 是域 F 上的线性空间或向量空间. 域 F 称为 V 的基域.

例 1.2 (坐标空间). 设 F 是域, F^n 是 n 维坐标空间. 具体实例 $\mathbb{R}^n, \mathbb{Q}^n, \mathbb{C}^n, \mathbb{Z}_p^n$, 其中 p 是素数. 值得注意的是 \mathbb{Z}_p^n 共有 p^n 个元素.

例 1.3 (矩阵空间). 设 F 是域, $F^{m \times n}$ 是 F 上 m 行 n 列的矩阵的集合. 关于矩阵的加法和数乘, $F^{m \times n}$ 是 F 上的线性空间.

例 1.4 (代数空间). 设 R 是环(不一定交换). 再设 $F \subset R$ 是 R 的子域. 则 R 是 F 上的线性空间. 验证如下: 首先, $(R, +, 0)$ 是交换群. 由 R 中的乘法结合律可知

$$\forall \alpha, \beta \in F, r \in R, (\alpha\beta)r = \alpha(\beta r).$$

因为 1 是 R 的也是 F 的乘法单位, 所以 $1r = r$. R 的分配律蕴含着空间的分配律. 验证完毕.

具体实例: \mathbb{C} 是 \mathbb{R} 上的线性空间, \mathbb{R} 是 \mathbb{Q} 上的线性空间, $F[x_1, \dots, x_n]$ 是域 F 上的线性空间. *Hamilton* 四元数环是 \mathbb{C} 上的线性空间. 设 K 是 F 的子域. 则 F 上的线性空间也是 K 上的线性空间.

例 1.5 (映射空间) 设 S 是非空集合, V 是域 F 上的线性空间. 令 $\text{Map}(S, V)$ 是从 S 到 V 的所有映射的集合. 对任意 $f, g \in \text{Map}(S, V)$, $\alpha \in F$ 定义:

$$\begin{array}{ccc} f + g: S \longrightarrow V & & \alpha f: S \longrightarrow V \\ x \mapsto f(x) + g(x) & \text{和} & x \mapsto \alpha f(x). \end{array}$$

令 $\tilde{\mathbf{0}}: S \longrightarrow V$ 是把 S 中的元素都映成 $\mathbf{0}$ 的映射. 则

$$(\text{Map}(S, V), +, \tilde{\mathbf{0}}, \text{数乘}, 1)$$

是线性空间. 实例 $\text{Map}(\mathbb{R}, \mathbb{R})$ 是线性空间.

命题 1.6 设 V 是域 F 上的线性空间. 设 $\lambda \in F, \mathbf{v} \in V$. 则

$$(i) \quad \lambda \mathbf{0} = \mathbf{0};$$

$$(ii) \quad \lambda \mathbf{v} = \mathbf{0} \text{ 当且仅当 } \lambda = 0 \text{ 或 } \mathbf{v} = \mathbf{0};$$

$$(iii) \quad (-1)\mathbf{v} = -\mathbf{v}.$$

证明. (i) 直接计算得

$$\lambda \mathbf{0} = \lambda(\mathbf{0} + \mathbf{0}) = \lambda \mathbf{0} + \lambda \mathbf{0} \implies \lambda \mathbf{0} = \mathbf{0}.$$

(ii) 设 $\lambda \mathbf{v} = \mathbf{0}$ 且 $\lambda \neq 0$. 则

$$\mathbf{v} = 1\mathbf{v} = (\lambda^{-1}\lambda)\mathbf{v} = \lambda^{-1}(\lambda\mathbf{v}) = \lambda^{-1}\mathbf{0} \stackrel{(i)}{=} \mathbf{0}.$$

当 $\lambda = 0$ 时, 反之, 由 (i) 只要证明 $0\mathbf{v} = \mathbf{0}$. 直接计算得

$$0\mathbf{v} = (0 + 0)\mathbf{v} = 0\mathbf{v} + 0\mathbf{v} \implies 0\mathbf{v} = \mathbf{0}.$$

(iii) 直接计算得

$$\begin{aligned} \mathbf{0} &\stackrel{(ii)}{=} 0\mathbf{v} = (1 + (-1))\mathbf{v} \\ &= 1\mathbf{v} + (-1)\mathbf{v} = \mathbf{v} + (-1)\mathbf{v} \\ &\implies (-1)\mathbf{v} = -\mathbf{v}. \quad \square \end{aligned}$$

例 1.7 证明: $(\mathbb{Z}, +, 0)$ 不可能是任何域 F 上的线性空间.

证明. 设结论不成立. 再设 0_F 和 1_F 分别是 F 中的加法和乘法单位. 先考虑 F 的特征不等于 2 的情形. 此时, $\lambda := 1_F + 1_F \neq 0_F$. 于是 λ^{-1} 存在. 通过直接计算得:

$$2 = 1 + 1 = (1_F 1 + 1_F 1) = (1_F + 1_F)1 = \lambda 1$$

$$\implies \lambda^{-1} 2 = 1$$

$$\implies \lambda^{-1}(1 + 1) = 1$$

$$\implies \lambda^{-1} 1 + \lambda^{-1} 1 = 1.$$

矛盾, 因为两个相同整数之和不可能等于 1.

再设 F 的特征等于 2 的情形. 则

$$2 = 1 + 1 = (1_F 1 + 1_F 1) = (1_F + 1_F)1 = 0_F 1 = 0.$$

矛盾.

1.2 线性相关性

设 $\alpha_1, \dots, \alpha_k \in F$ 和 $\mathbf{v}_1, \dots, \mathbf{v}_k \in V$. 则 $\alpha_1 \mathbf{v}_1 + \dots + \alpha_k \mathbf{v}_k$ 称为 $\mathbf{v}_1, \dots, \mathbf{v}_k$ 在 F 上的一个线性组合. 如果存在不全为零的 $\alpha_1, \dots, \alpha_k$ 使得上述线性组合等于 $\mathbf{0}$, 则称 $\mathbf{v}_1, \dots, \mathbf{v}_k$ 在 F 上线性相关. 否则, 称 $\mathbf{v}_1, \dots, \mathbf{v}_k$ 是在 F 上线性无关.

上学期讲的关于线性组合, 线性相关和无关的结论在抽象线性空间中都成立. 我们回忆线性组合引理 (上学期第五周讲义引理 1.13).

引理 1.8 设 $\mathbf{v}_1, \dots, \mathbf{v}_k; \mathbf{w}_1, \dots, \mathbf{w}_\ell$ 是 V 中两组向量. 如果 $k > \ell$ 且 \mathbf{v}_i 是 $\mathbf{w}_1, \dots, \mathbf{w}_\ell$ 的线性组合, $i = 1, \dots, k$. 则 $\mathbf{v}_1, \dots, \mathbf{v}_k$ 线性相关.

该定理的另一个证明见席南华《基础代数》定理 1.18.

我们通过(推广的)矩阵乘法的记号再次证明线性组合引理. 设 $A = (a_{i,j}) \in F^{m \times n}$, $\mathbf{x}_1, \dots, \mathbf{x}_m \in V$. 记

$$(\mathbf{x}_1, \dots, \mathbf{x}_m)A = \left(\sum_{i=1}^m a_{i,1}\mathbf{x}_i, \dots, \sum_{i=1}^m a_{i,n}\mathbf{x}_i \right).$$

可直接验证, 对任意 $B \in F^{n \times s}$,

$$((\mathbf{x}_1, \dots, \mathbf{x}_m)A)B = (\mathbf{x}_1, \dots, \mathbf{x}_m)(AB).$$

根据线性组合引理的条件, 存在 $A \in F^{\ell \times k}$ 使得

$$(\mathbf{v}_1, \dots, \mathbf{v}_k) = (\mathbf{w}_1, \dots, \mathbf{w}_\ell)A.$$

因为 $k > \ell$, 所以存在 $\alpha_1, \dots, \alpha_k \in F$ 不全为零, 使得

$$A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} =: \mathbf{0}_\ell.$$

由此得出,

$$(\mathbf{v}_1, \dots, \mathbf{v}_k) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix} = (\mathbf{w}_1, \dots, \mathbf{w}_\ell)A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix} = (\mathbf{w}_1, \dots, \mathbf{w}_\ell)\mathbf{0}_\ell.$$

故 $\alpha_1 \mathbf{v}_1 + \cdots + \alpha_k \mathbf{v}_k = \mathbf{0}$, 即 $\mathbf{v}_1, \dots, \mathbf{v}_k$ 线性相关. \square

定义 1.9 设 S 是 V 的一个非空子集. 如果 S 中存在一个有限子集是线性相关的, 则称 S 是一个线性相关集. 否则, 称 S 是线性无关集.

例 1.10 令 $V = F[x]$. 则 $\{1, x, x^2, \dots\}$ 是一个线性无关集.

例 1.11 在 $\text{Map}(\mathbb{R}, \mathbb{R})$ 中, $\sin(x)^2, \cos(x)^2, 1$ 是线性相关的 ($\because \sin(x)^2 + \cos(x)^2 = 1$).

例 1.12 设 $e^{\alpha_1 x}, \dots, e^{\alpha_n x} \in \text{Map}(\mathbb{R}, \mathbb{R})$, 其中 $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ 两两不同. 证明: $e^{\alpha_1 x}, \dots, e^{\alpha_n x}$ 在 \mathbb{R} 上线性无关.

证明. 设 $\beta_1, \dots, \beta_n \in \mathbb{R}$ 使得

$$\beta_1 e^{\alpha_1 x} + \cdots + \beta_n e^{\alpha_n x} = 0.$$

对上式求 k 阶导数得

$$\beta_1 \alpha_1^k e^{\alpha_1 x} + \cdots + \beta_n \alpha_n^k e^{\alpha_n x} = 0.$$

取 $k = 0, 1, \dots, n-1$, 我们有

$$\underbrace{\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_3^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}}_A \begin{pmatrix} \beta_1 e^{\alpha_1 x} \\ \beta_2 e^{\alpha_2 x} \\ \vdots \\ \beta_n e^{\alpha_n x} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

因为 $\det(A) \neq 0$, 所以 A 可逆. 故

$$\beta_1 e^{\alpha_1 x} = \beta_2 e^{\alpha_2 x} = \cdots = \beta_n e^{\alpha_n x} = 0 \implies \beta_1 = \beta_2 = \cdots = \beta_n = 0.$$

故, $e^{\alpha_1 x}, \dots, e^{\alpha_n x}$ 在 \mathbb{R} 上线性无关. \square

例 1.13 设 $a = \sqrt{-1}$ 和 $b = \sqrt{-2}$. 则 a, b 在 \mathbb{R} 上线性相关. 这是因为 $\sqrt{2}a - b = 0$. 但它们在 \mathbb{Q} 上线性无关. 否则, 存在 $q \in \mathbb{Q}$ 使得 $b = qa$. 于是, $q = \sqrt{2}$. 矛盾.

例 1.14 设 $f, g \in C^1(a, b)$. 证明:

(i) 如果 f, g 在 \mathbb{R} 上线性相关, 则对任意 $x \in (a, b)$,

$$W_2 = \det \begin{pmatrix} f(x) & g(x) \\ f'(x) & g'(x) \end{pmatrix} = 0. \quad W_2 \text{ 称为二阶 Wronskian.}$$

(ii) 设 f 在 (a, b) 上恒正. 则 (i) 的逆命题成立.

证明. (i) 设 $\lambda, \mu \in \mathbb{R}$, 不全为零, 使得对任意 $x \in (a, b)$ 使得 $\lambda f(x) + \mu g(x) = 0$. 则 $\lambda f'(x) + \mu g'(x) = 0$. 于是

$$\begin{pmatrix} f(x) & g(x) \\ f'(x) & g'(x) \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

对任意 $x \in (a, b)$ 成立. 于是, $W_2 = 0$.

(ii) 注意到 f 在 (a, b) 上恒正蕴含 $1/f(x) \in C^1(a, b)$. 因为 W_2 在 (a, b) 上恒为零, 所以在 (a, b) 上

$$\left(\frac{g}{f}\right)' = 0.$$

故存在 $c \in \mathbb{R}$ 使得 $g/f = c$, 即 $g - cf = 0$ 在 (a, b) 上成立. 由此得出 f, g 在 \mathbb{R} 上线性相关. \square

1.3 子空间

符号约定. 在本小节和以后的各小节中 V 是域 F 上的线性空间.

定义 1.15 设 W 是 V 的非空子集. 如果对于任意的 $\alpha, \beta \in F$, $\mathbf{x}, \mathbf{y} \in W$, 我们有 $\alpha\mathbf{x} + \beta\mathbf{y} \in W$, 则称 W 是 V 的子空间.

每个子空间都是线性空间.

例 1.16 (i) 设 $\phi: F^n \rightarrow F^m$ 是线性映射. 则 $\ker(\phi)$ 是 F^n 的子空间, $\text{im}(\phi)$ 是 F^m 的子空间.

(ii) 设 $\text{SM}_n(F)$ 是 F 上所有 n 阶对称方阵的集合, $\text{SSM}_n(F)$ 是 F 上所有 n 阶斜对称方阵的集合. 则它们都是 $\text{M}_n(F)$ 上的子空间.

验证如下: 设 $A, B \in \text{SM}_n(F)$, $\alpha, \beta \in F$. 我们有

$$(\alpha A + \beta B)^t = \alpha A^t + \beta B^t = \alpha A + \beta B \implies \alpha A + \beta B \in \text{SM}_n(F).$$

斜对称情形类似.

(iii) 设 $F[x]^{(d)} = \{p \in F[x] \mid \deg(p) < d\}$. 则 $F[x]^{(d)}$ 是 $F[x]$ 的子空间.

(iv) 闭区间 $[a, b]$ 上的连续函数的集合 $C[a, b]$ 和连续可微函数的集合 $C^1[a, b]$ 是 $\text{Map}([a, b], \mathbb{R})$ 的子空间.

线性空间 V 中的任意个子空间的交仍是子空间, 其证明与上学期第二章第一讲命题 1.19 类似. 设 V_1, \dots, V_k 是 V 的子空间, 定义

$$V_1 + V_2 + \dots + V_k = \{\mathbf{v}_1 + \mathbf{v}_2 + \dots + \mathbf{v}_k \mid \mathbf{v}_1 \in V_1, \mathbf{v}_2 \in V_2, \dots, \mathbf{v}_k \in V_k\}.$$

则 $V_1 + V_2 + \dots + V_k$ 是子空间. 称之为 V_1, \dots, V_k 的和. 验证见上学期第二章.