第五章　复数域和多项式

7.3　单位根

设 $n \in \mathbb{Z}^+$. 方程 $z^n = 1$ 在 $\mathbb{C}$ 中的根称为 n 次单位根.

命题 7.5 方程 $z^n = 1$ 在 $\mathbb{C}$ 中有 n 个互不相同的根

$$\epsilon_k = e^{\frac{2k\pi\mathbf{i}}{n}}, \quad k = 0, 1, \ldots, n-1.$$

证明. 直接计算得

$$\epsilon_k^n = e^{2k\pi\mathbf{i}} = 1.$$

故 $\epsilon_0, \epsilon_1, \ldots, \epsilon_{n-1}$ 都是单位根. 设 $k, m \in \{0, 1, \ldots, n-1\}$ 且 $k \le m$. 如果 $\epsilon_k = \epsilon_m$, 则

$$1 = \epsilon_m \epsilon_k^{-1} = e^{\frac{2(m-k)\pi\mathbf{i}}{n}}.$$

因为 $m-k \in \{0, 1, \ldots, n-1\}$, 所以 $m = k$. 故 $\epsilon_0, \epsilon_1, \ldots, \epsilon_{n-1}$ 两两不同. □

根据第五章第二讲定理 3.19, 方程 $z^n = 1$ 在 $\mathbb{C}$ 中的至多有 n 个根. 于是, $\mathbb{C}$ 中恰有 n 个互不相同的单位根. 记 U_n 是这些单位根的集合.

命题 7.6 三元组 $(U_n, \cdot, 1)$ 是循环群. $U_n = \langle \epsilon_\ell \rangle$ 当且仅当 $\gcd(\ell, n) = 1$.

证明. 设 $\epsilon_k, \epsilon_m \in U_n$. 则 $(\epsilon_k\epsilon_m^{-1})^n = \epsilon_k^n(\epsilon_m^n)^{-1} = 1$. 故 $\epsilon_k\epsilon_m^{-1} \in U_n$. 故 $(U_n, \cdot, 1)$ 是 $(\mathbb{C}^*, \cdot, 1)$ 的子群 (第四章第一讲命题 2.24).

注意到:

$$
\begin{aligned}
U_n = \langle \epsilon_\ell \rangle &\iff \mathrm{ord}(\epsilon_\ell) = n \\
&\iff \frac{n}{\gcd(n,\ell)} = n \text{ (上学期第四章第一讲推论 2.41)} \\
&\iff \gcd(n,\ell) = 1 \quad \square
\end{aligned}
$$

当 $U_n = \langle \epsilon_\ell \rangle$ 时, ϵ_ℓ 称为 n 次本原单位根.

7.4 代数学基本定理

定理 7.7 *(代数学基本定理)* 设 $f \in \mathbb{C}[x] \setminus \mathbb{C}$. 则 f 在 $\mathbb{C}[x]$ 有根.

上述定理的证明要用到超出本课程范围的知识. 这里不给出证明. 但它的两个推论对下学期的学习比较重要.

推论 7.8 设 $f \in \mathbb{C}[x]\setminus\mathbb{C}$. 则存在互不相同的复数 $\alpha_1, \cdots, \alpha_k$ 和非零正整数 $m_1, \ldots, m_k$ 使得

$$f = \mathrm{lc}(f)(x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k}.$$

证明. 设 $n = \deg(f), \ell = \mathrm{lc}(f)$. 我们对 n 归纳.

设 $n>1$ 且结论对 $n-1$ 次复系数多项式都成立. 由代数学基本定理, 存在 $\alpha\in\mathbb{C}$ 使得 $f(\alpha)=0$. 根据余式定理,

$$f(x)=(x-\alpha)g(x),$$

其中 $g\in\mathbb{C}[x]$, $\deg(g)=n-1$ 且 $\mathrm{lc}(g)=\lambda$. 由归纳假设存在互不相同的复数 $\alpha_1,\cdots,\alpha_k$ 和非零正整数 $m_1,\ldots,m_k$ 使得

$$g=\lambda(x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k}.$$

如果 $\alpha\in\{\alpha_1,\ldots,\alpha_k\}$, 则不妨设 $\alpha=\alpha_1$. 由此得出

$$f(x)=\lambda(x-\alpha_1)^{m_1+1}\cdots(x-\alpha_k)^{m_k}.$$

否则

$$f(x)=\lambda(x-\alpha)(x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k}. \quad \square$$

该推论说明 $\mathbb{C}[x]$ 中的不可约元是零次或者一次的多项式, 每个复系数多项式在 $\mathbb{C}$ 中的根的个数(计算重数)与其次数相同.

推论 7.9 *在 $\mathbb{R}[x]$ 中的不可约元的次数至多是二次.*

证明. 假设 $f(x)=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_0\in\mathbb{R}[x]$ 是不可约的且 $n>2$ 和 $f_n\neq 0$. 因为 f 也是复系数多项式, 所以代数学基本定理蕴含 f 由复根 α. 注意到 $\alpha\notin\mathbb{R}$. 否则

由余式定理 f 会有一次实系数因子 $x-\alpha$, 与 f 的不可约性矛盾. 特别地, $\bar{\alpha} \neq \bar{\alpha}$.

因为实数的共轭是它自身, 所以

$$0 = f(\alpha) = \overline{f(\alpha)} = \sum_{i=0}^{n} \bar{f}_i \bar{\alpha}^i = \sum_{i=0}^{n} f_i \bar{\alpha}^i = f(\bar{\alpha}).$$

故 f 由两个互不相同的复根 α 和 $\bar{\alpha}$. 因为 $\bar{\alpha} \neq \bar{\alpha}$, 所以 $x-\alpha$ 与 $x-\bar{\alpha}$ 不相伴. 由第二讲命题 6.27, $g := (x-\alpha)(x-\bar{\alpha})$ 在 $\mathbb{C}[x]$ 中整除 f. 注意到 $f, g \in \mathbb{R}[x]$, 存在 $h \in \mathbb{R}[x]$ 使得 $f = gh$. 因为 $\deg(f) > 2$ 和 $\deg(g) = 2$, 所以 f 在 $\mathbb{R}[x]$ 中可约. 矛盾. □

该推论说明 $\mathbb{R}[x] \setminus \mathbb{R}$ 中的多项式, 都是 $\mathbb{R}[x]$ 中若干一次或二次不可约多项式的乘积.

7.5 应用举例

例 7.10 设循环矩阵

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-3} & a_{n-2} \\ a_{n-2} & a_{n-1} & \cdots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix} \in \mathrm{M}_n(\mathbb{R}).$$

计算 A 的行列式. 当矩阵 A 可逆时, 求 A^{-1}.

解. 设 $\epsilon_0, \ldots, \epsilon_{n-1}$ 是 n 个 n 次单位根. 令

$$f = a_0 + a_1 x + \cdots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1} \in \mathbb{C}[x].$$

对 $k \in \{0, 1, \ldots, n-1\}$, 利用 $\epsilon_k^n = 1$ 得到

$$f(\epsilon_k) = a_0 + a_1 \epsilon_k + \cdots + a_{n-2} \epsilon_k^{n-2} + a_{n-1} \epsilon_k^{n-1},$$

$$\begin{aligned}
\epsilon_k f(\epsilon_k) &= a_{n-1} + a_0 \epsilon_k + \cdots + a_{n-3} \epsilon_k^{n-2} + a_{n-2} \epsilon_k^{n-1}, \\
\epsilon_k^2 f(\epsilon_k) &= a_{n-2} + a_{n-1} \epsilon_k + \cdots + a_{n-4} \epsilon_k^{n-2} + a_{n-3} \epsilon_k^{n-1}, \\
&\vdots \\
\epsilon_k^{n-1} f(\epsilon_k) &= a_1 + a_2 \epsilon_k + \cdots + a_{n-1} \epsilon_k^{n-2} + a_0 \epsilon_k^{n-1}.
\end{aligned}$$

利用矩阵写成

$$f(\epsilon_k) \begin{pmatrix} 1 \\ \epsilon_k \\ \epsilon_k^2 \\ \vdots \\ \epsilon_k^{n-1} \end{pmatrix} = A \begin{pmatrix} 1 \\ \epsilon_k \\ \epsilon_k^2 \\ \vdots \\ \epsilon_k^{n-1} \end{pmatrix}, \quad k = 0, 1, \ldots, n-1.$$

设

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \epsilon_0 & \epsilon_1 & \cdots & \epsilon_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \epsilon_0^{n-1} & \epsilon_1^{n-1} & \cdots & \epsilon_{n-1}^{n-1} \end{pmatrix}.$$

则 $V\mathrm{diag}(f(\epsilon_0),\ldots,f(\epsilon_{n-1})) = AV$. 由 *Vandermonde* 行列式可知, V 可逆. 故

$$A = V\mathrm{diag}(f(\epsilon_0),\ldots,f(\epsilon_{n-1}))V^{-1}.$$

两边取行列式得

$$\det(A) = f(\epsilon_0)\cdots f(\epsilon_{n-1}).$$

而 A 可逆当且仅当任何 n 次单位根都不是 f 的根. 此时,

$$A^{-1} = V\mathrm{diag}(f(\epsilon_0)^{-1},\ldots,f(\epsilon_{n-1})^{-1})V^{-1}.$$

例 7.11 设

$$H = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \;\middle|\; u, v \in \mathbb{C} \right\}.$$

则 $(H, +, O, \cdot, E)$ 是 $\mathrm{M}_2(\mathbb{C})$ 中的非交换子环, 且 H 中的每个非零元在 H 中有可逆元. 这是数学史上第一个斜域*(skew-field)*, 称为 *Hamilton* 四元数系.

验证如下:

(i) 设 $W = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ 和 $Z = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix}$, 其中 $u, v, x, y \in \mathbb{C}$.

我们有

$$W - Z = \begin{pmatrix} u - x & v - y \\ -\bar{v} + \bar{y} & \bar{u} - \bar{x} \end{pmatrix} = \begin{pmatrix} u - x & v - y \\ -\overline{v - y} & \overline{u - x} \end{pmatrix} \in H.$$

故 $(H,+,O)$ 是 $(\mathrm{M}_2(\mathbb{C}),+,O)$ 的子群.

计算

$$WZ=\begin{pmatrix} ux-v\bar{y} & uy+v\bar{x} \\ -\bar{v}x-\bar{u}\bar{y} & -\bar{v}y+\bar{u}\bar{x}\end{pmatrix}=\begin{pmatrix} ux-v\bar{y} & uy+v\bar{x} \\ -\overline{(uy+v\bar{x})} & \overline{ux-v\bar{y}}\end{pmatrix}\in H.$$

注意到

$$E_2=\begin{pmatrix} 1 & 0 \\ -\bar{0} & \bar{1}\end{pmatrix}\in H.$$

故 H 是 $\mathrm{M}_2(\mathbb{C})$ 的子环.

(ii) 设 $A=\begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i}\end{pmatrix}$ 和 $B=\begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0\end{pmatrix}$. 则 $A,B\in H$.

直接计算得

$$AB=\begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix},\quad BA=\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}.$$

因为 $AB\neq BA$, 所以 H 不是交换环.

(iii) 设 $W\neq O$. 则 $\det(W)=|u|^2+|v^2|\neq 0$. 故 W 是可逆矩阵. 在 $\mathrm{M}_n(\mathbb{C})$ 中,

$$W^{-1}=\frac{1}{u\bar{u}+v\bar{v}}\begin{pmatrix} \bar{u} & -v \\ \bar{v} & u\end{pmatrix}\in H.$$

故 W 在 H 中可逆.

例 7.12 设 $\mathbb{Z}[\sqrt{-5}]=\{x+y\sqrt{-5}\,|\,x,y\in\mathbb{Z}\}$.

断言. $\mathbb{Z}[\sqrt{-5}]$ 是整环, 且它的可逆元是 ± 1.

断言的证明. 设 $a, b \in \mathbb{Z}[\sqrt{-5}]$. 则存在整数 k, ℓ, m, n 使得

$$a = k + \ell\sqrt{-5} \quad 和 \quad b = m + n\sqrt{-5}.$$

则

$$a - b = (k - m) + (\ell - n)\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}].$$

故 $(\mathbb{Z}[\sqrt{-5}], +, 0)$ 是交换群. 因为

$$ab = (km - 5\ell n) + (kn + \ell m)\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

且

$$1 = 1 + 0\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}],$$

所以 $(\mathbb{Z}[\sqrt{-5}], +, 0)$ 是交换的含幺半群. 于是, $\mathbb{Z}[\sqrt{-5}]$ 是交换环. 又因为 $\mathbb{Z}[\sqrt{-5}] \in \mathbb{C}$, 所以它是整环.

再设 $ab = 1$. 则 $|a||b| = 1$. 故 $|a| \le 1$ 或 $|b| \le 1$. 不妨设 $|a| \le 1$. 故

$$\sqrt{k^2 + 5\ell^2} \le 1 \implies k^2 = 1 \text{ 且 } \ell = 0 \implies a = \pm 1.$$

从而, $b = \pm 1$. 断言成立.

下面说明 $\mathbb{Z}[\sqrt{-5}]$ 不是唯一因子分解整环. 注意到

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

下面我们证明 3 和 $2 \pm \sqrt{-5}$ 都是 $\mathbb{Z}[\sqrt{-5}]$ 中的不可约元.

设 $3=(m+n\sqrt{-5})(k+\ell\sqrt{-5})$, 其中 $m,n,k,\ell\in\mathbb{Z}$. 两边取共轭得 $3=(m-n\sqrt{-5})(k-\ell\sqrt{-5})$. 于是

$$9=(m^2+5n^2)(k^2+5\ell^2).$$

但 $m^2+5n^2=3$ 无整数解. 故 $m^2+5n^2=1$ 或 $m^2+5n^2=9$. 前者意味着 $m=\pm1$, $n=0$, 即 $m+n\sqrt{-5}=\pm1$ 是可逆元. 而后者意味着 $k+\ell\sqrt{-5}$ 是可逆元. 故 3 不可约.

类似地, 设 $2+\sqrt{-5}=(m+n\sqrt{-5})(k+\ell\sqrt{-5})$, 其中 $m,n,k,\ell\in\mathbb{Z}$. 两边取共轭得

$$2-\sqrt{-5}=(m-n\sqrt{-5})(k-\ell\sqrt{-5}).$$

于是, $9=(m^2+5n^2)(k^2+5\ell^2)$. 同样的推理可知 $2+\sqrt{-5}$ 不可约. 同理 $2-\sqrt{-5}$ 也不可约. 显然 3 与 $2\pm\sqrt{-5}$ 都不相伴. 故 $\mathbb{Z}[\sqrt{-5}]$ 不是唯一因子分解整环.

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:

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

满足以下规律

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

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

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

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

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, $F[x_1,\ldots,x_n]$ 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 $\mathrm{Map}(S,V)$ 是从 S 到 V 的所有映射的集合. 对任意 $f,g\in\mathrm{Map}(S,V)$, $\alpha\in F$ 定义*:*

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

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

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

是线性空间. 实例 $\mathrm{Map}(\mathbb{R},\mathbb{R})$ 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) $\lambda\mathbf{0}=\mathbf{0}$;

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

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

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

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

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

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

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:

$$\begin{aligned} & 2 = 1 + 1 = (1_F 1 + 1_F 1) = (1_F + 1_F)1 = \lambda 1 \\ \Longrightarrow\ & \lambda^{-1}2 = 1 \\ \Longrightarrow\ & \lambda^{-1}(1+1) = 1 \\ \Longrightarrow\ & \lambda^{-1}1 + \lambda^{-1}1 = 1. \end{aligned}$$

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

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 $\{1,x,x^2,\ldots\}$ 是一个线性无关集.

例 1.11 在 $\mathrm{Map}(\mathbb{R},\mathbb{R})$ 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 $e^{\alpha_1x},\ldots,e^{\alpha_nx}\in\mathrm{Map}(\mathbb{R},\mathbb{R})$, 其中 $\alpha_1,\ldots,\alpha_n\in\mathbb{R}$ 两两不同. 证明: $e^{\alpha_1x},\ldots,e^{\alpha_nx}$ 在 $\mathbb{R}$ 上线性无关.

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

$$\beta_1e^{\alpha_1x}+\cdots+\beta_ne^{\alpha_nx}=0.$$

对上式求 k 阶导数得

$$\beta_1\alpha_1^ke^{\alpha_1x}+\cdots+\beta_n\alpha_n^ke^{\alpha_nx}=0.$$

取 $k=0,1,\ldots,n-1$, 我们有

$$\underbrace{\begin{pmatrix}1&1&1&\cdots&1\\ \alpha_1&\alpha_2&\alpha_3&\cdots&\alpha_n\\ \vdots&\vdots&\vdots&\ddots&\vdots\\ \alpha_1^{n-1}&\alpha_2^{n-1}&\alpha_3^{n-1}&\cdots&\alpha_n^{n-1}\end{pmatrix}}_{A}\begin{pmatrix}\beta_1e^{\alpha_1x}\\ \beta_2e^{\alpha_2x}\\ \vdots\\ \beta_ne^{\alpha_nx}\end{pmatrix}=\begin{pmatrix}0\\0\\ \vdots\\0\end{pmatrix}.$$

因为 $\det(A) \neq 0$, 所以 A 可逆. 故

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

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

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 $x \in (a, b)$,

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

(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. □

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 $\phi : F^n \longrightarrow F^m$ 是线性映射. 则 $\ker(\phi)$ 是 F^n 的子空间, $\mathrm{im}(\phi)$ 是 F^m 的子空间.

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

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

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

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 $\mathrm{Map}([a,b],\mathbb{R})$ 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 $V_1,\ldots,V_k$ 是 V 的子空间, 定义

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

则 $V_1+V_2+\cdots+V_k$ 是子空间. 称之为 $V_1,\ldots,V_k$ 的和. 验证见上学期第二章第一讲命题 1.23.