# 第五章　复数域和多项式

## 5.7　$\mathbb{Z}[x]$ 中的 Gauss 引理

**定义 5.29** 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

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

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

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

**引理 5.30** 设 $a_1, \ldots, a_n \in \mathbb{Z}$ 不全为零, $c \in \mathbb{Z}^*$. 则

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

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

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

$$ca_i = k_i h,$$

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

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

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

**引理 5.31** *(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 $f_m, f_{m-1}, \ldots, f_0, g_n, g_{n-1}, \ldots, g_0 \in \mathbb{Z}$ 且 $f_m$, $g_n$ 都非零. 假设 $fg$ 不是本原的. 则存在素数 $p$ 使得 $p|\mathrm{cont}(fg)$. 因为 $\mathrm{cont}(f) = 1$, 所以存在 $i \in \{0, 1, \ldots, m\}$ 使得

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

同理存在 $j \in \{0, 1, \ldots, n\}$ 使得

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

注意到在 $fg$ 在中 $x^{i+j}$ 的系数是

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

如果 $\ell<j$, 则 $k>i$. 故 $p|f_k \Longrightarrow p|f_k g_\ell$. 如果 $\ell>j$, 则 $p|g_\ell$. 故 $p|f_k g_\ell$. 于是, $p|f_i g_j$. 故 $p|f_i$ 或 $p|g_j$. 矛盾. □

**定理 5.32** 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, $\deg \tilde{g} = \deg(g)$, $\deg(\tilde{h}) = \deg(h)$. 因为, $\alpha \mathrm{cont}(f)\mathrm{pp}(f) = \beta(\tilde{g}\tilde{h})$. 我们得到 $\mathrm{pp}(f) = u\tilde{g}\tilde{h}$, 其中 $u \in \{1, -1\}$. 故

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

矛盾. □

**定理 5.33** *(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 $n > 0$, $f_n, f_{n-1}, \ldots, f_0 \in \mathbb{Z}$ 且 $f_n \neq 0$. 设 $p$ 是素数. 如果

$$p \nmid f_n,\ p|f_{n-1},\ \ldots,\ p|f_0,\ p^2 \nmid f_0,$$

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 $k, \ell \in \mathbb{Z}^+$, $g_k, \ldots, g_1, g_0, h_\ell, \ldots, h_1, h_0 \in D$ 且 $g_k, h_\ell$ 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 $p | f_0$, 所以 $p | g_0$ 或 $p | h_0$. 不妨设 $p | g_0$. 又因为 $p^2 \nmid f_0$, 所以 $p \nmid h_0$. 因为 $p \nmid g_k$ 和 $p | g_0$, 所以存在 $i \in \{0, 1, \ldots, k\}$ 使得

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

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

**例 5.34** 证明: 对于 $n > 1$, $x^n - 2x + 2$ 在 $\mathbb{Q}[x]$ 中不可约.

证明. 注意到 $2 \nmid 1$, $2 | -2$, $2 | 2$ 但 $2^2 \nmid 2$. 根据定理 *5.33*, 该多项式不可约.

**例 5.35** 设 $p$ 是素数. 证明: $x^{p-1} + x^{p-2} + \cdots + x + 1$ 在 $\mathbb{Q}[x]$ 中不可约.

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

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

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

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

也是环同态. 因为 $\phi \circ \psi = \psi \circ \phi = \mathrm{id}_{\mathbb{Z}[x]}$, 所以 $\phi$ 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 5.32)*. 由于 $\phi$ 是同构, 只要证明 $f(x+1)$ 在 $\mathbb{Z}[x]$ 中不可约即可. 注意到

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

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 *5.33* 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:

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

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 $(V,+,\mathbf{0},$ 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*:*

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

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 $\lambda^{-1}$ 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 1.12).

**引理 1.8** 设 $\mathbf{v}_1, \ldots, \mathbf{v}_k$; $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ 是 $V$ 中两组向量. 如果 $k > \ell$ 且 $\mathbf{v}_i$ 是 $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ 的线性组合, $i = 1, \ldots, k$. 则 $\mathbf{v}_1, \ldots, \mathbf{v}_k$ 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 $A = (a_{i,j}) \in F^{m\times n}$, $\mathbf{x}_1, \ldots, \mathbf{x}_m \in V$. 记

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

可直接验证, 对任意 $B \in F^{n\times s}$,

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

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

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

因为 $k > \ell$, 所以存在 $\alpha_1, \ldots, \alpha_k \in F$ 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,

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

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

证明. 设 $\beta_1,\ldots,\beta_n\in\mathbb{R}$ 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 $k=0,1,\ldots,n-1$, 我们有

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

因为 $\det(A) \neq 0$, 所以 $A$ 可逆. 故

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

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 $F[x]^{(d)} = \{p \in F[x] | \deg(p) < d\}$. 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

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

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.

## 1.4 子空间的直和

**定义 1.17** 设 $V_1,\ldots,V_k$ 是 $V$ 的子空间, $W = V_1+\cdots+V_k$. 如果对于任意 $\mathbf{w} \in W$ 存在唯一的 $\mathbf{v}_1 \in V_1,\ldots,\mathbf{v}_k \in V_k$ 使得

$$\mathbf{w} = \mathbf{v}_1 + \cdots + \mathbf{v}_k.$$

则称 $W$ 是 $V_1, \ldots, V_k$ 的直和, 并记为

$$W = V_1 \oplus \cdots \oplus V_k.$$

**定理 1.18** 设 $V$ 是线性空间, $V_1, \ldots, V_k$ 是 $V$ 的子空间, 且 $W = V_1 + \cdots + V_k$. 则以下结论等价.

*(i)* $W$ 是 $V_1, \ldots, V_k$ 的直和;

*(ii)* 如果 $\mathbf{0} = \mathbf{v}_1 + \cdots + \mathbf{v}_k$, $\mathbf{v}_1 \in V_1, \ldots, \mathbf{v}_k \in V_k$, 则 $\mathbf{v}_1 = \cdots = \mathbf{v}_k = \mathbf{0}$.

*(iii)* 对任意 $i \in \{1, 2, \ldots, k\}$,

$$V_i \cap (V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_k) = \{\mathbf{0}\}.$$

**证明.** (i) $\Longrightarrow$ (ii). 显然.

(ii) $\Longrightarrow$ (iii). 不妨设 $i = 1$. 设 $\mathbf{w} \in V_1 \cap (V_2 + \cdots + V_k)$. 则存在 $\mathbf{v}_2 \in V_2, \ldots, \mathbf{v}_k \in V_k$ 使得 $\mathbf{w} = \mathbf{v}_2 + \cdots + \mathbf{v}_k$. 于是

$$\mathbf{0} = -\mathbf{w} + \mathbf{v}_2 + \cdots + \mathbf{v}_k.$$

由 $-\mathbf{w} \in V_1$ 和 (ii) 可知, $\mathbf{w} = \mathbf{0}$.

(iii) $\Longrightarrow$ (i). 设 $\mathbf{w} \in W$, 且

$$\mathbf{w} = \mathbf{u}_1 + \cdots + \mathbf{u}_k = \mathbf{v}_1 + \cdots + \mathbf{v}_k,$$

其中 $\mathbf{u}_1, \mathbf{v}_1 \in V_1, \ldots, \mathbf{u}_k, \mathbf{v}_k \in V_k$. 则 $\mathbf{0} = (\mathbf{u}_1 - \mathbf{v}_1) + \cdots + (\mathbf{u}_k - \mathbf{v}_k)$. 于是

$$(\mathbf{v}_1 - \mathbf{u}_1) = (\mathbf{u}_2 - \mathbf{v}_2) + \cdots + (\mathbf{u}_k - \mathbf{v}_k).$$

由此得出, $\mathbf{v}_1 - \mathbf{u}_1 \in V_1 \cap (V_2 + \cdots + V_k)$. 根据 (iii), $\mathbf{v}_1 = \mathbf{u}_1$. 类似地可得 $\mathbf{v}_i = \mathbf{u}_i$, $i = 2, \ldots, k$. □

**例 1.19** 设 $\mathbf{v}_1, \ldots, \mathbf{v}_n$ 是 $\mathbb{R}^n$ 的一组基. 则

$$\mathbb{R}^n = \langle \mathbf{v}_1 \rangle \oplus \cdots \oplus \langle \mathbf{v}_n \rangle.$$

这是因为 $\mathbb{R}^n$ 中的元素都是 $\mathbf{v}_1, \ldots, \mathbf{v}_n$ 的线性组合而且 $\mathbf{v}_1, \ldots, \mathbf{v}_n$ 线性无关.

**例 1.20** 设 $F$ 是特征不等于 $2$ 的域. 证明:

$$\mathrm{M}_n(F) = \mathrm{SM}_n(F) \oplus \mathrm{SSM}_n(F).$$

**证明.** 设 $A \in \mathrm{M}_n(F)$. 令

$$B = \frac{1}{2}(A + A^t) \quad \text{和} \quad C = \frac{1}{2}(A - A^t).$$

因为 $2 \neq 0$, 所以 $B$ 和 $C$ 是良定义的. 可直接验证

$$B \in \mathrm{SM}_n(F),\ C \in \mathrm{SSM}_n(F), \text{ 且 } A = B + C.$$

于是, $\mathrm{M}_n(F) = \mathrm{SM}_n(F) + \mathrm{SSM}_n(F)$. 若 $A \in \mathrm{SM}_n(F) \cap \mathrm{SSM}_n(F)$, 则 $A = A^t = -A^t$. 于是, $2A^t = O$. 因为 $2$ 可逆, 所以 $A = O$, 即这两个子空间交平凡. 由定理 *1.18 (iii)*, $\mathrm{M}_n(F) = \mathrm{SM}_n(F) \oplus \mathrm{SSM}_n(F)$. □

当 $F$ 的特征等于 $2$ 时, $1 = -1$. 于是,

$$\mathrm{SM}_n(F) = \mathrm{SSM}_n(F).$$

故 $\mathrm{SM}_n(F) \cap \mathrm{SSM}_n(F) \neq \{O\}$. 这两个子空间之和不是直和.

**例 1.21** 设 $V$ 是线性空间, $V_1, \ldots, V_k$ 是 $V$ 的子空间. 如果 $V_1 + \cdots + V_k$ 是直和, 则对任意的 $\ell \in \{1, 2, \ldots, k\}$, $V_1 + \cdots + V_\ell$ 也是直和.

**证明.** 设 $\mathbf{v}_1 \in V_1, \ldots, \mathbf{v}_\ell \in V_\ell$ 使得 $\mathbf{v}_1 + \cdots + \mathbf{v}_\ell = \mathbf{0}$. 则

$$\mathbf{v}_1 + \cdots + \mathbf{v}_\ell + \underbrace{\mathbf{0} + \cdots + \mathbf{0}}_{k-\ell} = \mathbf{0}.$$

将定理 *1.18 (ii)* 用于 $V_1, \ldots, V_\ell, \ldots, V_k$ 可知, $\mathbf{v}_1 = \cdots = \mathbf{v}_\ell = \mathbf{0}$. 再将定理 *1.18 (ii)* 用于 $V_1, \ldots, V_\ell$ 得到, $V_1 + \cdots + V_\ell$ 也是直和. □

**例 1.22** 设

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ \mathbf{v}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \ \mathbf{v}_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{R}^2.$$

则 $\langle \mathbf{v}_1 \rangle \cap \langle \mathbf{v}_2 \rangle = \{\mathbf{0}\}$, $\langle \mathbf{v}_1 \rangle \cap \langle \mathbf{v}_3 \rangle = \{\mathbf{0}\}$ 且 $\langle \mathbf{v}_3 \rangle \cap \langle \mathbf{v}_1 \rangle = \{\mathbf{0}\}$. 但 $\langle \mathbf{v}_3 \rangle \cap (\langle \mathbf{v}_1 \rangle + \langle \mathbf{v}_2 \rangle) = \langle \mathbf{v}_3 \rangle$. 于是 $\langle \mathbf{v}_1 \rangle + \langle \mathbf{v}_2 \rangle + \langle \mathbf{v}_3 \rangle$ 不是直和.

**例 1.23** 设 $P^{(d)} := \{f \in F[x_1, \ldots, x_n] | \deg(f) \leq d\}$ 和 $H_i = \{h \in F[x_1, \ldots, x_n] | h \text{ 齐 } i \text{ 次}\}$. 根据多元多项式的齐次加法分解,

$$P^{(d)} := \bigoplus_{i=0}^{d} H_i.$$

## 1.5 子空间的生成元

设 $S$ 是 $V$ 的非空子集. 令 $\langle S\rangle$ 是 $S$ 中的元素的所有在 $F$ 上的线性组合的集合, 即

$$\langle S\rangle := \left\{ \sum_{i=1}^{k} \alpha_i \mathbf{v}_i \,|\, k \in \mathbb{Z}^+, \alpha_i \in F, \mathbf{v}_i \in S \right\}.$$

可验证 $\langle S\rangle$ 是一个子空间(上学期第二章第二讲命题 1.26). 称 $\langle S\rangle$ 为由 $S$ 生成的子空间, $S$ 称为 $\langle S\rangle$ 的一组生成元.

设 $U$ 是 $V$ 的子空间. 如果存在有限集 $S \subset V$ 使得 $U = \langle S\rangle$, 则称 $U$ 是 在 $F$ 上有限生成的子空间.

**例 1.24** 设 $V = F[x]$. 则 $V$ 不是有限生成的.

**证明.** 假设 $F[x]$ 可以由 $p_1, \ldots, p_\ell \in F[x]$ 生成. 则 $1, x, \ldots, x^\ell$ 都是 $p_1, \ldots, p_\ell$ 在 $F$ 上的线性组合. 由线性组合引理可知, $1, x, \ldots, x^\ell$ 在 $F$ 上线性相关. 矛盾.