回忆: 定理6.1 设 $a, b \in \mathbb{Z}$, $b \neq 0$. 则

(i) a, b 的最大公因子

(ii) $\exists\, u, v \in \mathbb{Z}$, 使得

$$ua + vb = \gcd(a, b)$$

证法2 设 $S = \{xa + yb \mid x, y \in \mathbb{Z}\}$.

因为 $b \neq 0$, 所以 $S \cap \mathbb{Z}^+ \neq \emptyset$.

设 g 是 S 中最小的正整数, 则存在

$u, v \in \mathbb{Z}$ 使得

$$ua + vb = g \qquad (*)$$

下面证: g 是 a 和 b 的最大公因子.

由带余除法 $a = qg + r$,

其中 $q \in \mathbb{Z}$, $r \in \{0, 1, \cdots, g-1\}$

由 $(*)$ $\quad a = q(ua + vb) + r$

$\Rightarrow (1 - qu)a + (-v)b = r$

$\Rightarrow r \in S$

$\Rightarrow r = 0$ $\quad$ ($\because$ $0 \le r < g$ 且 g 是 S 中最小正整数)

$\Rightarrow g \mid a$

同理 $g \mid b$ 于是 g 是 a 和 b 的公因子.

设 d 是 a, b 的另一个公因子.

由 $(*)$ $\quad d \mid g$ $\quad$ (引理4.2).

于是 $g = \gcd(a, b)$ ▨

例: 计算 95 和 57 的最大公因子.

解: $r_0 = 95$, $r_1 = 57$

$$95 = 1 \cdot 57 + 38$$
$$57 = 1 \cdot 38 + 19 \qquad \Rightarrow \gcd(95, 57) = 19$$
$$38 = 2 \cdot 19$$

再求 $u, v \in \mathbb{Z}$ 使得

$$u \cdot 95 + v \cdot 57 = 19$$

$57 - 1 \cdot 38 = 19$

$57 - (95 - 57) = 19$

$\Rightarrow (-1)\,95 + 2 \cdot 57 = 19$

$\Rightarrow u = -1$, $v = 2$.

定义：设 $a, b \in \mathbb{Z}$, $b \neq 0$. 如果 $\gcd(a,b)=1$

则称 a, b 互素

定理 6.2 设 $a, b \in \mathbb{Z}$ 且 $b \neq 0$

则 a, b 互素 $\Leftrightarrow \exists\, u, v \in \mathbb{Z}$, 使得 $ua+vb=1$

证："$\Rightarrow$" 定理 6.1 的直接推论

"$\Leftarrow$" 设 $g = \gcd(a,b)$. 由引理 4.2

$g \mid a, g \mid b \Rightarrow g \mid 1 \Rightarrow g = 1$ ▨

引理 6.1 设 $a, b \in \mathbb{Z} \setminus \{0\}$. ~~如果~~ a, b 互素

则 $\operatorname{lcm}(a, b) = ab$

证：ab 显然是 a 和 b 的公倍式.

设 m 是 a, b 的另一个公倍式

则 $\exists\, s, t \in \mathbb{Z}$ 使得

$m = sa = tb$

因为 a, b 互素，所以存在 $u, v \in \mathbb{Z}$ ②

$ua + vb = 1$ (定理 6.2)

$\Rightarrow uam + vbm = m$

$\Rightarrow uatb + vbsa = m$

$\Rightarrow ab(ut + vs) = m$

$\Rightarrow (ab) \mid m$

$\Rightarrow \operatorname{lcm}(a,b) = ab$ ▨

定理 6.2 设 $a, b \in \mathbb{Z} \setminus \{0\}$.

则 $\operatorname{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$

证：设 $g = \gcd(a,b)$. 则存在 $c, d \in \mathbb{Z}$

使得 $a = cg$, $b = dg$

且 c, d 互素.

~~由定理 6.2 $\exists\, u, v \in \mathbb{Z}$ 使得~~

$uc + vd = 1$

~~设 m 是 a, b 的另一个公倍数~~

$\frac{ab}{g} = \frac{cg \cdot dg}{g} = cdg$. 只要证明

$lcm(a,b) = cdg$ 即可

首先 $cdg = cb = da \Rightarrow cdg$ 是 a,b 的公倍数

再设 m 是 a,b 的公倍数. 则存在 $s,t \in \mathbb{Z}$

使得 $m = sa = tb$

$= scg = tdg$

于是 $sc = td =: w$. 由此可知

w 是 c, d 的公倍数.

由引理 6.1. $w = rcd$ 其中 $r \in \mathbb{Z}$

$m = wg = rcdg \Rightarrow (cdg) \mid m$

$\Rightarrow lcm(a,b) = cdg$ ▨

定义: 设 $p \in \mathbb{Z}^+ \setminus \{1\}$, 如果 p 不能写成两个小于 p 的正整数之积, 则称 p 是素数 (prime).

例: 2, 3, 5, 7, 11, 13, 17, 19 …

定理 6.4 设 $m \in \mathbb{Z}^+ \setminus \{1\}$, 则 m 是若干素数之积

证: ~~且~~ $m = 2$ ✓

设 $m > 2$ 且定理对小于 m 大于等 2 的正整数成立. 如果 m 是素数, 则定理成立

否则 $m = kl$, 其中 $1 < k < m$, $1 < l < m$

由归纳假设, k, l 是若干素数之积, 则 m 也是 ▨

例: $24 = 2^3 \times 3$

$829348951 = 104729 \times 1299709$

例: 证明素数有无穷多个

证：假设只~~有~~有限多个素数

$p_1, \dots, p_k$

令 $m = p_1 \cdots p_k + 1 > p_i, \ i=1,\dots k$

于是 m 不是素数. 由定理 6.3

$\exists i \in \{1,\dots,k\}$ 使得 $p_i \mid m$

$\Rightarrow p_i \mid 1$ （定理 4.2）

$\rightarrow\leftarrow$ ▨

引理6.2. 设 $a, b \in \mathbb{Z}$, p 是素数

~~则~~ 如果 $p \mid (ab)$, 则 $p \mid a$ 或 $p \mid b$

<u>证:</u> 设 $p \nmid a$. 则 $\gcd(a,p)=1$.

由定理 6.2, $\exists\, u, v \in \mathbb{Z}$ 使得

$$ua + vp = 1$$

$$uab + vpb = b$$

$\because p \mid (ab)$, $p \mid (pb)$ $\therefore p \mid b$ （引理4.2） ▨

例：设 p 是素数, $1<k<p$.

则 $p \mid \binom{p}{k}$

证：$\binom{p}{k} = \dfrac{p!}{k!\,(p-k)!}$

$\Rightarrow \quad p! = k!\,(p-k)!\,\binom{p}{k}$

$\because p \mid p! \quad \therefore p \mid \left[(k!)\,(p-k)!\,\binom{p}{k}\right]$

如果 $p \mid k!$, 则 $p \mid i$, $1 < i \le k$. （引理6.2）

不可能

同理 $p \nmid (p-k)!$

$\Rightarrow p \mid \binom{p}{k}$. ▨

第二章 矩阵

§1 向量

行向量 $(\alpha_1, \cdots, \alpha_n)$, $\alpha_i \in \mathbb{R}$

列向量 $\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix}$ $\beta_j \in \mathbb{R}$

例：设 $A = (a_{ij})_{m\times n}$

$\vec{A_i} = (a_{i1}, \cdots, a_{in})$, $i=1,2,\cdots m$

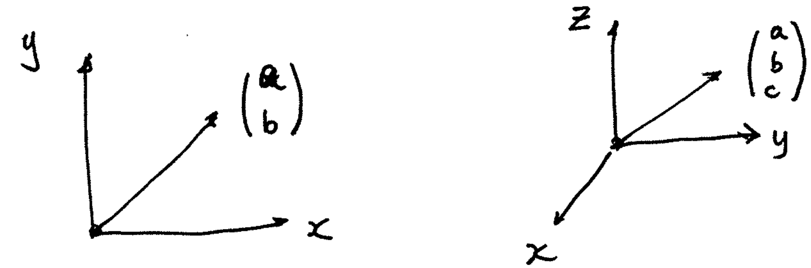
$\vec{A^{(j)}} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$, $j=1,2,\cdots n$

§1.1 坐标空间

$\mathbb{R}^{1\times n} = \{ (\alpha_1, \cdots, \alpha_n) \mid \alpha_1, \cdots \alpha_n \in \mathbb{R} \}$

$\mathbb{R}^{n\times 1} = \{ \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \mid \beta_1, \cdots \beta_n \in \mathbb{R} \}$

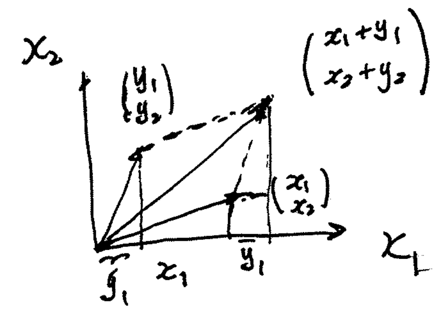
把 $\mathbb{R}^{n\times 1}$ 简记为 $\mathbb{R}^n$



设 $\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $\vec{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ $\in \mathbb{R}^n$

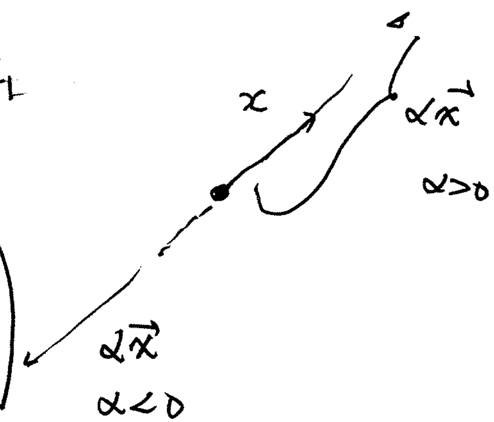
$\vec{x} + \vec{y} := \begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix}$

$\vec{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ $\vec{x} + \vec{0} = \vec{x}$



设 $\alpha \in \mathbb{R}$

$\alpha \vec{x} := \begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{pmatrix}$



加法与数乘的运算规律.

$\forall \vec{x}, \vec{y}, \vec{z} \in \mathbb{R}^n$

$\vec{x}+\vec{y} = \vec{y}+\vec{x}$ （加法交换律）

$(\vec{x}+\vec{y})+\vec{z} = \vec{x}+(\vec{y}+\vec{z})$ （…结合律）

$\vec{x}+\vec{0} = \vec{x}$ （加法单位元）

$\exists!\ \vec{u} \in \mathbb{R}^n$

$\vec{x}+\vec{u} = \vec{0}$ （加法逆）

注：$\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. 则 $\vec{u} = \begin{pmatrix} -x_1 \\ \vdots \\ -x_n \end{pmatrix}$

$\forall \alpha, \beta \in \mathbb{R}$

$(\alpha\beta)\vec{x} = \alpha(\beta\vec{x})$. （数乘结合律）

$1\vec{x} = \vec{x}$ （数乘单位）

注：$\vec{x}$ 是加法逆.是 $(-1)\vec{x}$

$\vec{x}+(-1)\vec{y}$ 记为 $\vec{x}-\vec{y}$

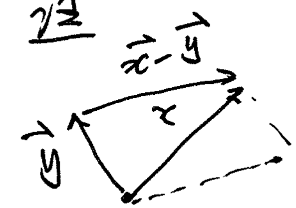
分配律

$\alpha(\vec{x}+\vec{y}) = \alpha\vec{x}+\alpha\vec{y}$

$(\alpha+\beta)\vec{x} = \alpha\vec{x}+\beta\vec{y}$

注：所有的验证都是平凡的

注



$\vec{x} = (\vec{x}-\vec{y})+\vec{y}$

例：设

$$(L)\ \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

$A = (a_{ij})_{m\times n}$, $\vec{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$

则 (L) 可表示为

$$x_1\vec{A}^{(1)} + \cdots + x_n\vec{A}^{(n)} = \vec{b}$$

其中 $\vec{A}^{(1)}, \ldots, \vec{A}^{(n)}, \vec{b} \in \mathbb{R}^m$

§1.2 线性相关性

设 $\vec{v}_1, \cdots, \vec{v}_k \in \mathbb{R}^n$, $\alpha_1, \cdots \alpha_k \in \mathbb{R}$

则 $\alpha_1\vec{v}_1 + \cdots + \alpha_k\vec{v}_k$ 称为 $\vec{v}_1, \cdots, \vec{v}_k$ 的一个线性组合. $\alpha_1 \cdots \alpha_k$ 称为该线性组合的系数.

例. (L) 相容 $\Longleftrightarrow$ $\vec{b}$ 是 $\vec{A}^{(1)}, \cdots \vec{A}^{(n)}$ 的线性组合.

例: 设 $\vec{u} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$, $\vec{v}_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$, $\vec{v}_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

问 $\vec{u}$ 是不是 $\vec{v}_1, \vec{v}_2$ 的线性组合?

解: 设

$$\vec{u} = \alpha_1\vec{v}_1 + \alpha_2\vec{v}_2$$

则 $\begin{pmatrix} \alpha_1+\alpha_2 \\ 2\alpha_1 \\ 3\alpha_1 \\ 4\alpha_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ 即 $\begin{cases} \alpha_1+\alpha_2=1 \\ 2\alpha_1=1 \\ 3\alpha_1=1 \\ 4\alpha_1=1 \end{cases}$ 不相容

于是 $\vec{u}$ 不是 $\vec{v}_1$ 和 $\vec{v}_2$ 的线性组合

定义: 设 $\vec{v}_1, \cdots, \vec{v}_k \in \mathbb{R}^n$. 如果存在 $\alpha_1, \cdots \alpha_k \in \mathbb{R}$ 不全为零, 使得

$$\alpha_1\vec{v}_1 + \cdots + \alpha_k\vec{v}_k = \vec{0}$$

则称 $\vec{v}_1, \cdots, \vec{v}_k$ 线性相关. 否则称 $\vec{v}_1, \cdots, \vec{v}_k$ 线性无关.

例:

$$(H) \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ \cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

设 $A = (a_{ij})_{m\times n}$

则 (H) 有非零解

$\Longleftrightarrow \vec{A}^{(1)}, \cdots, \vec{A}^{(n)} \in \mathbb{R}^m$ 线性相关

例：判断 $\vec{v_1}=\begin{pmatrix}1\\0\\1\\1\end{pmatrix}$，$\vec{v_2}=\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$，$\vec{v_3}=\begin{pmatrix}1\\1\\0\\0\end{pmatrix}$

是否线性相关

解：设 $\alpha_1,\alpha_2,\alpha_3\in\mathbb{R}$ 使得

$$\alpha_1\vec{v_1}+\alpha_2\vec{v_2}+\alpha_3\vec{v_3}=\vec{0}$$

即 $$\begin{pmatrix}\alpha_1+\alpha_2+\alpha_3\\ \alpha_2+\alpha_3\\ \alpha_1+\alpha_2\\ \alpha_1+\alpha_2\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$$\Rightarrow\begin{cases}\alpha_1+\alpha_2+\alpha_3=0\\ \alpha_2+\alpha_3=0\\ \alpha_1+\alpha_2=0\end{cases}\Rightarrow\begin{cases}\alpha_1=0\\ \alpha_2=0\\ \alpha_3=0\end{cases}$$

于是 $\vec{v_1},\vec{v_2},\vec{v_3}$ 线性无关

关于线性相关性的几何意义

设 $\vec{u}\in\mathbb{R}^n$. $\vec{u}$ 线性相关

$\Longleftrightarrow\ \vec{u}=\vec{0}$.

再设 $\vec{u},\vec{v}\in\mathbb{R}^n$

$\vec{u},\vec{v}$ 线性相关. $\Longleftrightarrow\ \exists\,\alpha,\beta\in\mathbb{R}$，不全为零

$$\alpha\vec{u}+\beta\vec{v}=\vec{0}$$

不妨设 $\alpha\neq0$ $\quad\vec{u}=-\left(\frac{\beta}{\alpha}\right)\vec{v}$

于是 $\vec{u},\vec{v}$ "同向"或"反向". 即平行

设 $\vec{v_1},\cdots,\vec{v_k}\in\mathbb{R}^n$.

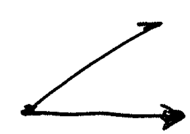
则 $\vec{v_1},\cdots,\vec{v_k},\vec{0}$ 线性相关

证：$0\cdot\vec{v_1}+\cdots+0\cdot\vec{v_k}+1\cdot\vec{0}=\vec{0}$

$\Rightarrow\ \vec{v_1},\cdots,\vec{v_k},\vec{0}$ 线性相关

由此可知 $\vec{0}$ 与任何向量都"同向"（"反向"）. 称 $\vec{0}$ 是迷向的.

两个向量线性无关 $\Longleftrightarrow$ 它们不共线



⑨

例：设 $\vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^3$

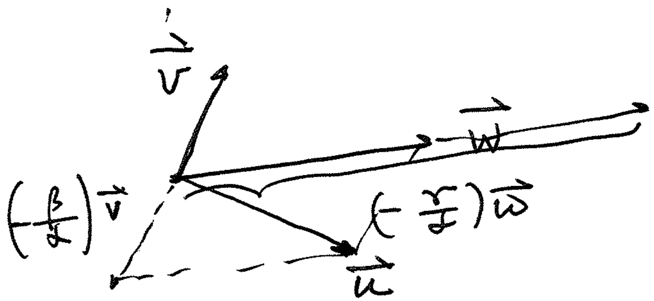
$\vec{u}, \vec{v}, \vec{w}$ 線性相关

$\Leftrightarrow \vec{u}, \vec{v}, \vec{w}$ 在一張平面上

证："⇒" 设 $\alpha, \beta, \gamma \in \mathbb{R}$，不~~相~~全為零

使得 $\alpha\vec{u} + \beta\vec{v} + \gamma\vec{w} = \vec{0}$

$$\vec{u} = \left(-\frac{\beta}{\alpha}\right)\vec{v} + \left(-\frac{\gamma}{\alpha}\right)\vec{w}$$



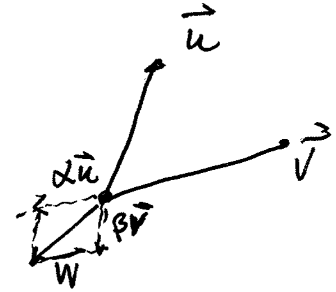
"⇐" 设 $\vec{u} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}, \vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}, \vec{w} = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}$ 共面

~~设平面為 $ax_1 + bx_2 + cx_3 = 0$~~

~~$a, b, c \in \mathbb{R}$，不全為零~~

~~$\alpha u_1 + b u_2$~~

不妨设 $\vec{u}, \vec{v}, \vec{w}$ 兩兩不平行



$\vec{w} = \alpha\vec{u} + \beta\vec{v}$ ▯