

## 向量空间

$\mathbb{R}^n \quad n \in \mathbb{Z}^+$

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}}_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in \mathbb{R}\}$$

$\mathbb{R}^n$  上的加法  $(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$

数乘  $\lambda \in \mathbb{R}, \underline{(a_1, \dots, a_n)} \in \mathbb{R}^n \quad \lambda(a_1, \dots, a_n) = (\lambda a_1, \lambda a_2, \dots, \lambda a_n)$

<b>加法</b>  <b>(加法和)数乘</b>	结合律 $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \quad \forall \alpha, \beta, \gamma \in \mathbb{R}^n$ // 加法: 分量加法, 传承其实数结合律
	零向量 $\vec{0} = (0, 0, \dots, 0) \quad \alpha + \vec{0} = \vec{0} + \alpha = \alpha \quad \forall \alpha \in \mathbb{R}^n$ // 也可由分量证明
	$\forall \alpha \in \mathbb{R}^n$ , 对 $\underline{-\alpha} = (-a_1, -a_2, \dots, -a_n)$ , 有 $\alpha + (-\alpha) = (-\alpha) + \alpha = \vec{0}$
	交换律 $\alpha + \beta = \beta + \alpha, \quad \forall \alpha, \beta \in \mathbb{R}^n$ $\forall \alpha, \beta \in \mathbb{R}, \quad \alpha, \beta \in \mathbb{R}^n$ .
	(1) $(\alpha + \beta)\alpha = \alpha\alpha + \beta\alpha$ (分配律) (2) $\alpha(\alpha + \beta) = \alpha\alpha + \alpha\beta$ (3) $(\alpha\beta)\alpha = \alpha(\beta\alpha)$ (结合律) (4) $1 \cdot \alpha = \alpha$
	满足8条性质, $\mathbb{R}^n$ 是 $\mathbb{R}$ 上的向量空间 $(\mathbb{R}, (\mathbb{R}^n, +), \cdot)$

集合  $A, B$  的笛卡尔积  $A \times B = \{(a, b) \mid a \in A, b \in B\}$

$A_1, A_2, \dots, A_n$   $A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, \dots, a_n \in A_n\}$

二元关系 - 一个  $A \times B$  的子集  $R \subseteq A \times B$  称为  $A$  到  $B$  的一个二元关系.

$\text{dom}(R) = \{a \mid \exists b, \text{s.t. } (a, b) \in R\}$

$\text{ran}(R) = \{b \mid \exists a, \text{s.t. } (a, b) \in R\}$

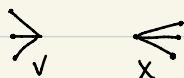
$R^{-1} = \{(x, y) \mid (y, x) \in R\} \quad (x, y) \leftrightarrow (y, x)$

关系的复合运算

$R_1, R_2$  是二元关系

$R_1 \circ R_2 = \{(a, c) \mid \exists b, \text{s.t. } (a, b) \in R_1, (b, c) \in R_2\}$

$R_2 \circ R_1$  记为 与映射保持一致:  $(g \circ f)(x) = g(f(x))$  从右到左



一个二元关系  $T$  称为一个映射:

若  $\forall (a, b) \in T, (a, c) \in T$ , 必有  $b = c$ . // 每个原像只能对应一个像  
对  $(a, b) \in T$ , 记  $b = T(a)$

$X$  是集合  $S(X) = \{f \mid f: X \rightarrow X \text{ 是双射}\}$

$f, g \in S(X) \Rightarrow f \circ g \in S(X)$

$f \in S(X) \Rightarrow f^{-1} \in S(X)$

恒等映射  $I: X \rightarrow X \quad I(x) = x, \forall x \in X. \quad f \circ I = I \circ f = f$

$(S(X), \circ)$  做成群 // "S(X) 做成群": 默认逆真是复合才能这么写

(商群 / 商环)

等价关系  $X$ : 集合,  $\sim$  是  $X$  上的二元关系.

$(X, \sim) \quad a \sim a \quad (\forall a \in X)$  自反性

$a \sim b \Rightarrow b \sim a$  对称性

$a \sim b, b \sim c \Rightarrow a \sim c$  传递性

类似于相容.

$\forall a \in X, [a] = \{b \mid b \in X, a \sim b\}$  ( $a$  所属的等价类)

$([a] \mid a \in X) \quad X = \bigcup_{a \in X} [a]$ , 并且  $\forall a, b \in X \quad [a] = [b] \Leftrightarrow [a] \cap [b] = \emptyset$

$\forall a \in X \quad a \sim a, \quad a \in [a]$

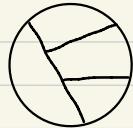
若  $[a] \cap [b] \neq \emptyset$ , 则  $a \sim b$ , 并且  $[a] = [b]$

证: 取  $x \in [a] \cap [b]$

$$a \sim x, \underline{b \sim x} \quad x \sim b \quad \therefore a \sim b$$

$\forall c \in [a], a \sim c, \quad x \sim b \sim a, \quad b \sim c \quad \therefore c \in [b] \quad [a] \subseteq [b]$

同理,  $[b] \subseteq [a], \quad \therefore [a] = [b]$ . #



划分

{1, 2, 3, 4, 5}

$i \sim j \Leftrightarrow (i, j)$  奇偶性一样

{1, 3, 5} {2, 4}

封闭性: \*在 $X \times X$ 上有定义(外面的)  
 $\forall a, b \in X, a * b$ 都在 $X$ 上, 即可.

但不居

### 二元运算

设 $X$ 是集合, 一个 $X \times X \rightarrow X$ 的映射称为 $X$ 上

$(\mathbb{R}^n, +)$

的一个二元运算.

$(\mathbb{Z}, \times)$

若 $*$ 是 $X$ 上的一个二元运算 //不一定有交换律

$(M_2(\mathbb{R}), \cdot)$  矩阵乘法

$2 \times 2$  方阵

$\forall (a, b) \in X \times X, a * b \in X.$

$$a * b = (a * b) * c = a * (b * c)$$

### 半群, 么半群

定义: 称 $(X, *)$ 是一个半群, 是指: //  $X$ 是一个半群, 有略运算非常清楚

(1) \* 是 $X$ 上的二元运算

(2) \* 在 $X$ 上满足结合律, 即  $(a * b) * c = a * (b * c), \forall a, b, c \in X$

eg.  $M_n(\mathbb{R})$   $(AB)C = A(BC)$  // 用矩阵乘法定义验证,  $\Sigma$

$$\text{集合的对称差 } A \Delta B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

$$(A \Delta B) \Delta C = A \Delta (B \Delta C)$$

$$= (A - (B \cup C)) \cup (B - (A \cup C)) \cup (C - (A \cup B)) \cup (A \cap B \cap C)$$

设  $n \in \mathbb{Z}^+$   $\oplus_n$  模  $n$  加  $\otimes_n$  模  $n$  乘

$\forall b \in \mathbb{Z}$   $b = gn + r$ , 其中  $g \in \mathbb{Z}$ ,  $r \in \{0, 1, \dots, n-1\}$   $r = b \% n$ .

$$a \oplus_n b = (a + b) \% n \quad a \otimes_n b = (ab) \% n$$

定义 半群  $(X, *)$  称为么半群, 是指  $\exists |_x \in X$ , 满足  $a * |_x = |_x * a = a, \forall a \in X$

此时  $|_x$  称为  $(X, *)$  的么元/单位元

eg. 全体偶数在乘法下没有么元

但是群(满足封闭性、结合律)



若二元运算有幺元，唯一  
证明中未用结合律，不用是群  
 $e = e * \tilde{e} = \tilde{e} * e = \tilde{e}$

命题. 设  $e_1, e_2$  是半群  $(X, *)$  的幺元，则  $e_1 = e_2$ .

证:  $e_1$  是幺元  $\therefore e_1 * e_1 = e_1$

$e_2$  是幺元  $\therefore e_1 * e_2 = e_1$

$\therefore e_1 = e_2$  #

$M_2(\mathbb{R}) \Rightarrow$  半群  $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$A$  称为可逆的，若  $\exists B \in M_2(\mathbb{R})$  s.t.  $AB = BA = I_2$ .

$A$  可逆  $\Leftrightarrow \det(A) \neq 0$ .

$GL_2(\mathbb{R}) = \{A \mid A \in M_2(\mathbb{R}), A \text{ 可逆}\}$

群

半群  $(X, *)$  称为群，若  $\forall a \in X, \exists b \in X$ , s.t.  $a * b = b * a = l_x$ . // 有逆元

## 二元运算

### $X$ 集合

一个  $X$  上的二元运算 是一个映射  $\star: X \times X \rightarrow X$  (映射在  $X \times X$  上有定义, 且  $\forall a, b \in X, a \star b \in X$ )

$(X, \star)$  是半群, 是指:

(1)  $\star$  是  $X$  上的二元运算

$$(2) (a \star b) \star c = a \star (b \star c), \forall a, b, c \in X$$

如果还有  $|_x \in X$ , s.t.  $a \star |_x = |_x \star a = a, \forall a \in X$ .

则称  $(X, \star)$  是么半群,  $|_x$  是么元(惟一).  $\| e = e \star \tilde{e} = \tilde{e} \star e = \tilde{e}$

如果么半群  $(X, \star)$  有  $\forall a \in X, \exists b \in X$  s.t.  $a \star b = b \star a = |_x$ , 则称  $(X, \star)$  是一个群.

定义, 称  $(X, \star)$  是一个群, 若下面四个条件成立.

(1)  $\star$  是  $X$  上的二元运算

$$(2) (a \star b) \star c = a \star (b \star c), \forall a, b, c \in X$$

$$(3) \exists |_x \in X, \text{ s.t. } \forall a \in X, |_x \star a = a \star |_x = a$$

$$(4) \forall a \in X, \exists b \in X \text{ s.t. } a \star b = b \star a = |_x \quad (\text{b 称为 a 的逆元})$$

eg. $(\mathbb{Z}, +)$	(1)      (2)      (3)      (4)
	$\checkmark$ $\checkmark$ $\textcircled{O}$ $\checkmark$ $-a \checkmark$

$(\mathbb{Q} - \{0\}, \times)$	$\checkmark$ $\checkmark$ $\textcircled{I}$ $\checkmark$ $\frac{1}{a} \checkmark$
--------------------------------	---

$(\mathbb{Q}, \times)$	-      -      -      -      0 没有逆元
------------------------	------------------------------------

证明逆元唯一.

左逆元 = 右逆元

命题: 设  $(X, \star)$  是么半群,  $a, b, c \in X$ . 若  $a \star b = |_x, b \star c = |_x$ , 则  $a = c$ .

证:  $(a \star b) \star c = |_x \star c = c.$        $\therefore c = a$

$$\text{a} \star (\text{b} \star \text{c}) = \text{a} \star |_x = \text{a} \quad \#$$

推论：若  $a * b_1 = b_1 * a = l_x$ ,  $a * b_2 = b_2 * a = l_x$ , 则  $b_1 = b_2$ .

在群  $(X, *)$  中，对任  $a \in X$ , 用  $a^{-1}$  表示  $a$  的逆元，即  $a^{-1} \in X$  且  $a * a^{-1} = a^{-1} * a = l_x$ .

消去律 设  $(X, *)$  是群， $a, b, c \in X$ , 则

$$(1) a * b = a * c \Rightarrow b = c.$$

$$(2) b * a = c * a \Rightarrow b = c$$

证：(1) 在等式两边左乘  $a^{-1}$ .

$$a^{-1} * (a * b) = (a^{-1} * a) * b = l_x * b = b, \therefore b = c$$

$$a^{-1} * (a * c) = (a^{-1} * a) * c = l_x * c = c.$$

(2) - - - - 右乘  $a^{-1}$

$$(b * a) * a^{-1} = b * (a * a^{-1}) = b * l_x = b. \quad \text{--- 同} \quad \#$$

(khlb)

集合与图论中也讲过类似任意打括号  
信号，用算二数归。

命题：任意加括号方式都等于

$$(-(a_1 * a_2) * \dots) * a_n$$

证： $n=1$  ✓, 任  $n \leq k$ ,  $n=k+1$  时：

$$\begin{aligned} & \text{任 } (a_1 * \dots * a_s) * (a_m * \dots * a_{s+m}) \\ &= (a_1 * \dots * a_s) * ((a_{s+1} * a_{s+2}) * \dots * a_{s+m}) \\ &= ((\underbrace{(a_1 * \dots * a_s)}_{\text{归纳}}) * (\underbrace{(a_{s+1} * a_{s+2}) * \dots * a_{s+m}}_{\text{归纳}})) * a_{s+1} \\ &= \dots \quad \checkmark \end{aligned}$$

结合律  $\Rightarrow a_1 * a_2 * a_3 * \dots$  可“任意打括号”

设  $(X, *)$  是半群， $a_1, a_2, \dots, a_n \in X$ .

对  $1 \leq k \leq n$ . 定义从  $a_k$  乘到  $g_n$ ,  $a_k * a_{k+1} * a_{k+2} * \dots * a_n$ . (递归定义)

$$\prod_{i=k}^n a_i = a_k, \text{ 对 } k \leq m \leq n-1, \prod_{i=k}^m a_i = \left( \prod_{i=k}^{m+1} a_i \right) * a_{m+1}.$$

命题 设  $1 \leq k \leq n-1$ , 则  $\prod_{i=1}^n a_i = \left( \prod_{i=1}^k a_i \right) * \left( \prod_{i=k+1}^n a_i \right)$  (任意)

证：若  $k=n-1$ , ✓ 由定义.

$$\begin{aligned} & \text{不妨设 } 1 \leq k \leq n-2. \quad \text{结合律} \\ & \text{左} = \left( \prod_{i=1}^n a_i \right) * a_n \stackrel{\text{def}}{=} \left( \left( \prod_{i=1}^k a_i \right) * \left( \prod_{i=k+1}^{n-1} a_i \right) \right) * a_n \stackrel{\text{结合律}}{=} \left( \prod_{i=1}^k a_i \right) * \left( \left( \prod_{i=k+1}^{n-1} a_i \right) * a_n \right) \\ & \text{由归纳假设,} = \left( \prod_{i=1}^k a_i \right) * \left( \prod_{i=k+1}^{n-1} a_i \right) \stackrel{\text{def}}{=} \left( \prod_{i=1}^k a_i \right) * \left( \prod_{i=k+1}^{n-1} a_i \right) \end{aligned}$$

<p>*群最早被提出: <math>\{1, \dots, n\}</math></p> <p><math>S_n = \{\sigma   \sigma \text{是} [1, \dots, n] \text{到自身的双射}\}</math></p> <p><math>(S_n, \circ)</math> 复合: <math>(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)</math></p>	<p><math>(a_1, a_2, a_3), (b_1, b_2, b_3) \in \mathbb{R}^3</math> 叉乘</p> <p><math>(a_1, a_2, a_3) \times (b_1, b_2, b_3) = (a_2 b_3 - a_3 b_2, a_3 b_1 - a_1 b_3, a_1 b_2 - a_2 b_1)</math> 没有结合律!</p> <p><math>a, b, r \in \mathbb{R}^3</math>. <math>a \times b \times r</math> 无意义! <math>(a \times b) \times r \neq a \times (b \times r)</math></p>
<p>目的: 研究多项式方程是否有根. 重 <math>\geq 5</math> 次, 无一般的求解公式.</p> <p><math>S_n</math> 是不可解群</p>	<p>定义. 设 <math>*</math> 是集合 <math>X</math> 上的二元运算, 称 <math>(X, *)</math> 满足交换律是指 <math>a * b = b * a, \forall a, b \in X</math>.</p> <p>若 <math>(X, *)</math> 是群且满足交换律, 则称 <math>(X, *)</math> 是交换群 / Abel 群.</p> <p>e.g. <math>GL_1(\mathbb{R}) = \{2 \times 2 \text{阶可逆实矩阵}\}</math>. 在矩阵乘法下做成群, 但无交换律.</p> <p><math>\begin{pmatrix} 1 &amp; 0 \\ 0 &amp; 1 \end{pmatrix} \quad \begin{pmatrix} 0 &amp; 1 \\ 1 &amp; 0 \end{pmatrix}</math> 验证</p> <h3>带余除法</h3> <p>设 <math>a \in \mathbb{Z}^+</math>, <math>b \in \mathbb{Z}</math>, 则 <math>\exists q, r \in \mathbb{Z}^+, r \in \{0, 1, \dots, a-1\}</math>, s.t. <math>b = qa + r</math></p> <p><math>\{q   q \in \mathbb{Z}, qa \leq b\}</math> 找到 <math>q \in \mathbb{Z}</math>, s.t. <math>qa \leq b</math>, <math>(q+1)a &gt; b</math>. <math>q = \lfloor \frac{b}{a} \rfloor</math>, <math>r = b \% a</math>.</p> <p>设 <math>a, b \in \mathbb{Z}</math>, 不全为 0</p> <p><math>\gcd(a, b) = d</math>. <math>d   a, d   b</math>, 且 <math>\forall c \in \mathbb{Z}, c   a, c   b \Rightarrow c   d</math></p> <p>事实: 每在 <math>x, y \in \mathbb{Z}</math>, s.t. <math>(ax+by)   a</math>, <math>(ax+by)   b</math>.</p> <p>(接受) 若 <math>c   a</math>, <math>c   b</math>, 则 <math>c   (ax+by)</math>, <math>\forall x, y \in \mathbb{Z}</math> 则此 <math>ax+by</math> 是 <math>\gcd</math></p> <p>证: 不妨设 <math>a \in \mathbb{Z}^+</math>, 对 <math>a</math> 归纳</p> <p><math>a=1 \vee</math></p> <p>设 <math>a \geq 2</math>, <math>b = qa + r</math> 带余除法</p> <p><math>r=0 \vee</math></p> <p><math>(\leq r \leq a-1)</math>, 由归纳假设, <math>\exists x, y \in \mathbb{Z}</math>, 使 <math>(rx+by)   b</math>, <math>(rx+by)   r</math>.</p> <p>.....</p>

证:  $T = \{ax+by \mid x, y \in \mathbb{Z}\}$

$\forall u, v \in T, u \neq v \in T$

$a, b$ 不全为0.  $\therefore T$ 中有正整数

而d是T中最小的正整数

任取  $w \in T$ , 来证  $d \mid w$ .

$w = qd + r, 0 \leq r < d$  (带余除法)

$d \in T, qd \in T$  又  $w \in T \therefore r = w - qd \in T$ . 且  $r < d$ .

而d是T中最小的正整数  $\therefore r$  不是正整数.  $\therefore r=0$ . 即  $d \mid w$ .

$\because a, b \in T$ .

$\therefore d \mid a, d \mid b$ .

又  $d \in T$ , 则  $d = ax + by$ , 对某  $x, y \in \mathbb{Z}$ . #

同余. 设  $n \in \mathbb{Z}^+$

对  $a, b \in \mathbb{Z}$ , 若  $a \equiv b \pmod{n}$  若  $n \mid (b-a)$

$a = q_1n + r_1, b = q_2n + r_2, a \equiv b \pmod{n} \Leftrightarrow r_1 = r_2$ .

$\equiv \pmod{n}$  是  $\mathbb{Z}$  上的等价关系. //自反, 对称, 传递 ✓

$a \equiv b \pmod{n} \Rightarrow a+c \equiv b+d \pmod{n}$

$c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$