



抽象代數

Uwni ✉ satanyalin@gmail.com

目录

1 二元運算	1
2 幺元	1
3 逆元	2
4 羣	3
5 置換	4
5.1 輪換	5
6 同構與同態	5

1 二元運算

A, B, C 是集合. 稱映射 $\cdot : A \times B \rightarrow C$ 為定義在 A, B 上的二元映射, 一般使用中綴表示法 $a \cdot b$ 來表示 $\cdot(a, b)$. 特殊地, $A = B = C$ 時, 稱為 A 上的二元算子. 對於二元算子 \cdot 和 \star , $\forall a, b, c \in A$ 如果滿足

- $a \cdot b = b \cdot a$, 則稱 \cdot 可易.
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, 則稱 \cdot 結合.
- $a \star (b \cdot c) = (a \star b) \cdot (a \star c)$, 則稱 \star 對 \cdot 分配.

2 幺元

對於 A 和其上的二元算子 \cdot , 若 $\exists e_r \in A, \forall a \in A, a \cdot e_r = a$ 則稱 e_r 為 \cdot 的右幺元. 同理, $\exists e_l \in A, \forall a \in A, e_l \cdot a = a$, 則稱 e_l 為 \cdot 的左幺元. 注意: 幺元是針對與運算的, 因此一個運算一個幺元

命題 AA1 若左幺元和右幺元同時存在, 則必然相等

證. 由右幺元的定義: $e_l e_r = e_l$ 由左幺元的定義: $e_l e_r = e_r$ 因此 $e_l = e_r$ ■

因此, 若左幺元和右幺元皆存在, 則可稱之為幺元, 記為 e .

> M: 好像左極限右極限, 左導數右導數的那種感覺, 同時存在且相等才有.

命題 AA2 存在唯一性定理 若幺元存在，則唯一

證. 假設存在符合定義的幺元 e_1 和 e_2 因為幺元必然是右幺元, $e_1 e_2 = e_1$ 因為幺元必然是左幺元, $e_1 e_2 = e_2$ 因此 $e_1 = e_2$ ■

> M: 好像極限的存在唯一性, 微分方程 Picard 存在唯一性, 泊松方程的存在唯一性. 而且證明思路類似, 用反證法

3 逆元

A 是集合, 若運算 \cdot 存在幺元 e . 對於 $a \in A$, 若 $\exists t_l \in A$ 使得 $t_l a = e$ 則稱 t_l 為 a 的左逆元. 且可類似地定義右逆元. > 注意: 逆元是針對與元素的, 在存在逆元的條件下, 一個元素對應一個逆元

命題 AA3 若運算可結合, 且 $a \in A$ 的左逆和右逆皆存在, 則左逆等於右逆

證. $t_r = e t_r = (t_l a) t_r = t_l (a t_r) = t_l e = t_l$ ■

若左逆等於右逆, 則稱其為 a 的逆元.

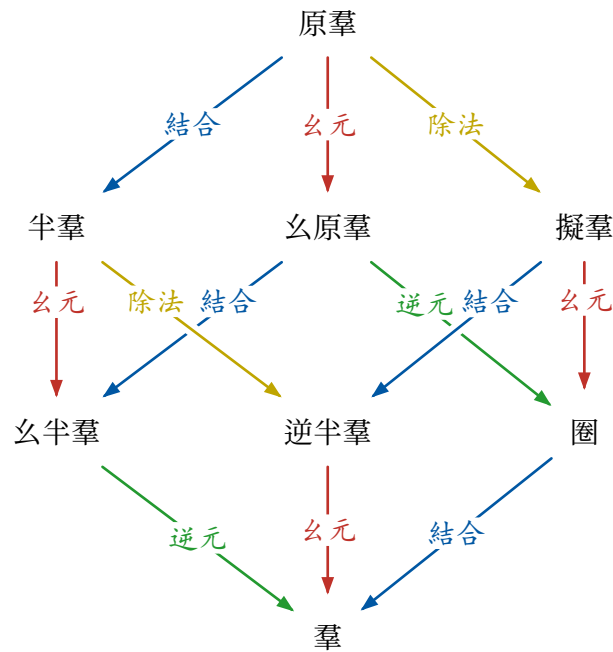
命題 AA4 若可結合運算存在 a 的逆元, 則逆唯一

證. 設 $t_1 t_2$ 都是 a 的逆元

$$t_1 = t_1 (a t_2) = (t_1 a) t_2 = t_2$$
 ■

若對於所有 $a \in A$ 都存在逆元, 則稱運算 \cdot 在 A 上可逆.

4 羣



設集合 G 非空，且在 G 上定義二元算子 \cdot 。則稱 (G, \cdot) 為原羣。 \cdot 謂之運算。如果原羣 (G, \cdot) 上

- 存在 $e \in G$ 為 \cdot 的幺元： $\forall a \in G(a \cdot e = e \cdot a = a)$ ，則稱 (G, \cdot, e) 為幺元羣；
- 運算 \cdot 結合： $\forall a, b, c \in G((a \cdot b) \cdot c = a \cdot (b \cdot c))$ ，則稱 (G, \cdot) 為半羣；
 - 存在幺元 $e \in G$ ，且運算 \cdot 結合，則稱 (G, \cdot, e) 為幺半羣；
 - 若 (幺) 半羣上運算交易： $\forall a, b \in G(a \cdot b = b \cdot a)$ ，則謂之交易 (幺) 半羣。

進一步，若在幺半羣 (G, \cdot, e) 上 \cdot 可逆，即如果 $\forall a \in G, \exists a^{-1} \in G(a \cdot a^{-1} = a^{-1} \cdot a = e)$ ，則稱 (G, \cdot, e) 為羣。並且定義映射

$$G \ni a \mapsto a^{-1} \in G$$

為 \cdot 逆映射，如果羣 $(G, +, e)$ 是加法羣，則記 $+$ 逆映射為

$$G \ni a \mapsto -a \in G$$

由命題 AA4 可知，羣中每個元素都存在唯一的逆。

如果羣上的運算交易，則稱之為交易羣。

□ 例 AA1 映射幺半羣

$$(X^X, \circ, \text{id}_X)$$

□

□ 例 AA2 二元乘法羣

設 $G = \{1, -1\}$ 是為有兩個不同元素的集合. 用乘法表定義其上的二元運算

·	1	-1
1	1	-1
-1	-1	1

表 3

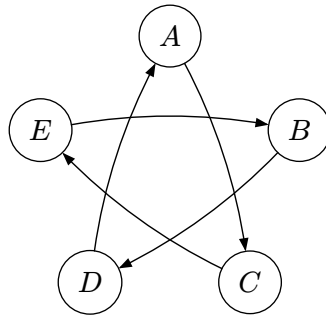
可以看出, $(G, \cdot, 1)$ 是一個交易羣. 其幺元為 1, 且每個元素都是其自身的逆元. 從對稱性可以看出, 乘法是可易的.

5 置換

設集合 X 非空, 令

$$S_X = \{f \in X^X \mid f \text{ 雙映也}\},$$

稱 S_X 中的元素為 X 上的置換. 置換在定義上是同一個集合上的雙映. 直觀上, 置換是對元素的重排列, 然而置換卻不必依賴於任何序或者指標. 想象一個班的學生換座位, 換座位後, 之前某人的位置上都坐上了新同學 (當然可能是自己). 且每個座位都只能座一人. 因此是「換座位」的過程是在學生集合上的雙映. 其中自變量是同學, 因變量是換到之前誰的座位上. 舉例來說, 我們可以用置換圖來表示這個過程.



圖示 10 $\{A, B, C, D, E\}$ 上的置換.

對於有限勢 N 的集合 X 上的置換 $\sigma \in S_X$, 我們可以用一個 $2 \times N$ 的矩陣表示映射規則. 比如對於上面的例子, 設 $X = \{A, B, C, D, E\}$ $\sigma(A) = C, \sigma(B) = D, \sigma(C) = E, \sigma(D) = A, \sigma(E) = B$ 可以使用如下的矩陣來表示

$$\begin{bmatrix} A & B & C & D & E \\ C & D & E & A & B \end{bmatrix}$$

兩類表示法的置換與列的順序無關.

進一步. 如果 $\sigma \in S_{\{1, \dots, n\}}$, 則可使用一列表示法. 我們約定第一列為自然數順序, 則只需要寫出第二列, 就能表示整個置換. 比如

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix}$$

可記作

$$[2 \ 4 \ 1 \ 3]$$

命題 AA5 X 設為非空集合, $(S_X, \circ, \text{id}_X)$ 是羣, 稱為 X 上的置換羣. 其中 \circ 是映射的複合, id_X 是 X 上的恒等映射.

證.

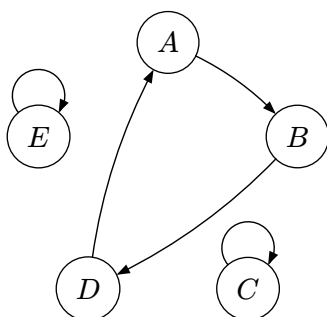
- **封閉性:** 任何雙射的複合仍然是雙射, 因此 S_X 在 \circ 下封閉.
- **結合性:** 映射複合天然滿足結合律, $(f \circ g) \circ h = f \circ (g \circ h)$.
- **幺元:** id_X 是雙射, 且對任意 $f \in S_X$ 有 $\text{id}_X \circ f = f \circ \text{id}_X = f$, 故 $\text{id}_X \in S_X$ 為幺元.
- **逆元:** 每個雙射 $f \in S_X$ 都存在反函數 f^{-1} , 且 f^{-1} 亦為雙射, $f \circ f^{-1} = f^{-1} \circ f = \text{id}_X$. ■

5.1 輪換

輪換是一類特殊的置換. 設 $\sigma \in S_X$. 如果 $\exists A = \{x_1, \dots, x_l\} \subset S$,

$$\sigma(x_1) = x_2, \sigma(x_2) = x_3, \dots, \sigma(x_l) = x_1,$$

且 $\forall x \in S \setminus A, \sigma(x) = x$ 則稱其 l -輪換. 其中 l 稱作輪換長度.



圖示 11 $\{A, B, C, D, E\}$ 上的輪換. 其中 $A \rightarrow B \rightarrow D \rightarrow A$ 輪換長度為 3

6 同構與同態

設 (G, \circ) 和 (H, \cdot) 是兩個原羣. 映射 $f \in H^G$, 如果對於所有 $a, b \in G$ 有

$$f(a \circ b) = f(a) \cdot f(b)$$

稱 f 為從 (G, \circ) 到 (H, \cdot) 的**同態映射**. 簡稱**同態**. 如果是從 (G, \circ) 到其自身的同態, 則稱為其上的**自同態**.

如果同態 f 是雙射, 則稱 f 為**同構映射**, 簡曰**同構**. f 是自同態則相應稱之為**自同構**. 若存在同構 f , 則稱兩個原羣**同構**. 記作 $G \cong H$.

“ 自同構和置換有什麼關係? 自同構不僅是置換, 還要保持運算結構. 但不是所有置換都是自同構. 置換且同態 \Leftrightarrow 自同構