Fundamental Abstract Algebra
基礎抽象代數

許胖

2015 年 1 月 15 日

目 錄

第 一 章

代數結構

第一節　簡介

定義 1.1 (二元運算)**.** 一個函數 $\mathcal{R} : A \times B \to C$，對於所有 $a \in A$、$b \in B$，存在**唯一**的 $c \in C$，使得 $\mathcal{R}(a, b) = c$，我們稱 $\mathcal{R}$ 是一個從 $A \times B$ 到 C 的**二元運算 *(Binary Operation)***，此時記爲 $a\mathcal{R}b = c$。

註. 若 $A = B = C = S$，我們稱 $\mathcal{R}$ 是定義在 S 上的二元運算。

範例 1.2. 下列爲二元運算：

1. 整數加法 $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
2. 實數乘法 $\cdot : \mathbb{R}^2 \to \mathbb{R}$
3. 實係數矩陣乘法 $\cdot : \mathbb{M}_{m\times n}(\mathbb{R}) \times \mathbb{M}_{n\times p}(\mathbb{R}) \to \mathbb{M}_{m\times p}(\mathbb{R})$
4. 充要條件 $\Leftrightarrow : \mathcal{L} \times \mathcal{L} \to \{\top, \bot\}$
5. $\mathcal{O}(n^2)$ 的 *LCS* 演算法 $\mathrm{LCS} : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^k$

定義 1.3 (n元運算)**.** 一個函數 $\mathcal{R} : A_1 \times A_2 \times \ldots \times A_n \to B$，對於所有 $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \ldots \times A_n$，存在**唯一**的 $b \in B$，使得 $\mathcal{R}(a_1, a_2, \ldots, a_n) = b$，我們稱 $\mathcal{R}$ 是一個從 $A_1 \times A_2 \times \ldots \times A_n$ 到 B 的 ***n* 元運算 *(n-ary Operation)***。

定義 1.4 (代數結構與代數系統)**. 一代數結構 *(Algebraic Structure)*** $(S, \mathcal{R}_1, \ldots, \mathcal{R}_n)$ 滿足以下條件

1. 有一非空集合 S
2. $\mathcal{R}_1, \ldots, \mathcal{R}_n$ 爲定義在 S 上的二元運算
3. 一系列的公理 $\mathcal{A}$

若 $\mathcal{R}_1, \ldots, \mathcal{R}_n$ 爲定義在 S 上的 n 元運算，則稱 $(S, \mathcal{R}_1, \ldots, \mathcal{R}_n)$ 爲**代數系統 *(Algebraic System)***。

範例 1.5. 下列爲代數結構：

1. 有理數與加法、乘法 $(\mathbb{Q}, +, \cdot)$
2. 複係數矩陣乘法 $(\mathbb{M}_{n\times n}(\mathbb{C}), \cdot)$
3. 正整數與最大公因數 $(\mathbb{Z}^+, \gcd)$，其中最大公因數爲二元運算 $\gcd : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$
4. 函數合成 $(\mathbb{F}(\mathbb{R}, \mathbb{R}), \circ)$

第二節　二元運算的性質

一、 基本性質

定義 1.6 (封閉律)**.** 一個代數結構 $(S, \mathcal{R})$ 中，若對於所有 $a, b \in S$，使得 $a\mathcal{R}b \in S$，則稱二元運算 $\mathcal{R}$ 對 S 滿足**封閉律 *(Closure)***。

範例 1.7. 説明下列代數結構是否滿足封閉律。

1. $(\mathbb{R}, +)$
2. $(\mathbb{N}, /)$
3. $\left(\mathbb{Z}[\sqrt{2}], \cdot\right)$
4. $(\mathbb{M}_{n\times n}(\mathbb{C}), \cdot)$
5. $(\mathbb{Q}_c, +)$
6. $(\mathbb{R}^2, \spadesuit)$，定義 $\spadesuit : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$，規則爲：對所有 $a \in \mathbb{R}$、$(x, y) \in \mathbb{R}^2$，使得 $a\spadesuit(x, y) = (x + a, y - a)$

證明

3. 我們取任意 $a_1, a_2, b_1, b_2 \in \mathbb{Z}$，計算

$$\begin{aligned}&(a_1 + a_2\sqrt{2}) \cdot (b_1 + b_2\sqrt{2})\\=&(a_1b_1 + 2a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{2}\end{aligned}$$

發現 $a_1b_1 + 2a_2b_2 \in \mathbb{Z}$ 且 $a_1b_2 + a_2b_1 \in \mathbb{Z}$，因此 $(a_1b_1 + 2a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$，因此 $\cdot$ 在 $\mathbb{Z}[\sqrt{2}]$ 中滿足封閉律。

5. 令 $1 + \sqrt{2}, 1 - \sqrt{2} \in \mathbb{Q}_c$，我們發現 $(1 + \sqrt{2}) + (1 - \sqrt{2}) = 2 \notin \mathbb{Q}_c$，因此 $(\mathbb{Q}_c, +)$ 不具封閉律。

□

定義 1.8 (結合律). 一個封閉的代數結構 $(S, \mathcal{R})$ 中，若對於所有 $a, b, c \in S$，使得 $(a\mathcal{R}b)\mathcal{R}c = a\mathcal{R}(b\mathcal{R}c)$，則稱二元運算 $\mathcal{R}$ 對 S 具有**結合律 *(Associativity, Associative property)***。

定義 1.9 (交換律). 一個封閉的代數結構 $(S, \mathcal{R})$ 中，若對於所有 $a, b \in S$，使得 $a\mathcal{R}b = b\mathcal{R}a$，則稱二元運算 $\mathcal{R}$ 對 S 具有**交換律 *(Commutativity, Commutative property)***。

範例 1.10. 說明下列代數結構是否有交換律。

1. $(\mathbb{N}, \mathcal{R})$，$\forall a, b \in \mathbb{N}$，$a\mathcal{R}b = a^b$

證明

1. 計算 $3\mathcal{R}2 = 3^2 = 9$、$2\mathcal{R}3 = 2^3 = 8$，因爲 $9 \neq 8$，因此 $3\mathcal{R}2 \neq 2\mathcal{R}3$，$\mathcal{R}$ 不具交換律。

□

定義 1.11 (吸收律). 一個封閉的代數結構 $(S, \mathcal{R}_1, \mathcal{R}_2)$ 中，若對於所有 $a, b \in S$，使得

$$a\mathcal{R}_1(a\mathcal{R}_2 b) = a$$
$$a\mathcal{R}_2(a\mathcal{R}_1 b) = a$$

，則稱二元運算 $\mathcal{R}_1, \mathcal{R}_2$ 在 S 上滿足**吸收律 *(Absorption law)***。

註. 吸收律是定義在**一對**二元運算上，因此不能單獨定義一個運算子具有吸收律。

定義 1.12 (分配律). 一個封閉的代數結構 $(S, \mathcal{R}_1, \mathcal{R}_2)$ 中，若對於所有 $a, b, c \in S$，使得

$$a\mathcal{R}_1(b\mathcal{R}_2 c) = (a\mathcal{R}_1 b)\mathcal{R}_2(a\mathcal{R}_1 c)$$
$$(b\mathcal{R}_2 c)\mathcal{R}_1 a = (b\mathcal{R}_1 a)\mathcal{R}_2(c\mathcal{R}_1 a)$$

，則稱二元運算 $\mathcal{R}_1$ 在 S 上對 $\mathcal{R}_2$ 具有**分配律 *(Distributivity, Distributive property)***。

註. 儘管 $\mathcal{R}_1$ 對 $\mathcal{R}_2$ 有分配律，但 $\mathcal{R}_2$ **未必**對 $\mathcal{R}_1$ 有分配律。

二、 單位元素

定義 1.13 (單位元素). 一個封閉的代數結構 $(S, \mathcal{R})$ 中，若

- 存在 $e_l \in S$，對所有 $a \in S$，$e_l \mathcal{R} a = a$，則 e_l 爲**左單位元素** ***(Left identity)***
- 存在 $e_r \in S$，對所有 $a \in S$，$a \mathcal{R} e_r = a$，則 e_r 爲**右單位元素** ***(Right identity)***
- 存在 $e \in S$，對所有 $a \in S$，$e \mathcal{R} a = a \mathcal{R} e = a$，則 e 爲**單位元素** ***(Identity)***

定理 1.14 (單位元素存在性). 一個封閉的代數結構 $(S, \mathcal{R})$ 中，若存在左單位元素 e_l、右單位元素 e_r，則 $e_l = e_r$，即單位元素存在。

證明 根據定義 1.13，我們知道對於所有元素 $a \in S$，$e_l \mathcal{R} a = a$ 且 $a \mathcal{R} e_r = a$，我們嘗試去計算 $e_l \mathcal{R} e_r$，因爲 e_l 是左單位元素，因此

$$e_l \mathcal{R} e_r = e_r$$

又因爲 e_r 是右單位元素，因此

$$e_l \mathcal{R} e_r = e_l$$

我們得到

$$e_l = e_l \mathcal{R} e_r = e_r$$

根據定義 1.13，我們知道有一個單位元素即是 $e = e_l = e_r$ (因爲左單位元素和右單位元素是同一個)。 □

定理 1.15 (單位元素唯一性). 一個封閉的代數結構 $(S, \mathcal{R})$ 中，若存在單位元素，則單位元素唯一。

證明 不失一般性假設有兩個單位元素 e_1 和 e_2，我們同樣下去計算 $e_1 \mathcal{R} e_2$，因爲 e_1 是單位元素，所以

$$e_1 \mathcal{R} e_2 = e_2$$

同時，e_2 也是單位元素，因此

$$e_1 \mathcal{R} e_2 = e_1$$

我們得到

$$e_1 = e_1 \mathcal{R} e_2 = e_2$$

□

三、 反元素

定義 1.16 (反元素)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 存在單位元素 $e \in S$，若對 $a \in S$，

- 存在 $b_l \in S$，$b_l\mathcal{R}a = e$，則 b_l 稱爲 a 的**左反元素** ***(Left inverse)***
- 存在 $b_r \in S$，$a\mathcal{R}b_r = e$，則 b_r 稱爲 a 的**右反元素** ***(Right inverse)***
- 存在 $b \in S$，$b\mathcal{R}a = a\mathcal{R}b = e$，則 b 稱爲 a 的**反元素** ***(Inverse)***，a 又稱**可逆元素** ***(Invertible element)***

若對所有 $a \in S$ 都有反元素，則稱 $\mathcal{R}$ 在 S 上有**反元素** ***(Inverse property)***。

性質 1.17. 一個封閉的代數結構 $(S,\mathcal{R})$ 存在單位元素 e，則 e 的反元素爲 e。

證明 根據定義 1.13，我們知道 $e\mathcal{R}e = e$，同時也符合反元素的定義。 □

定理 1.18 (反元素存在性)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 存在單位元素 e，且 $\mathcal{R}$ 具有結合律，若 $a \in S$ 存在左反元素 b_l，右反元素 b_r，則 $b_l = b_r$，即反元素存在。

證明 做爲習題。 □

定理 1.19 (反元素唯一性)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 存在單位元素 e，且 $\mathcal{R}$ 具有結合律，若 $a \in S$ 存在反元素，則反元素唯一。

證明 做爲習題。 □

定理 1.20. 一個封閉的代數結構 $(S,\mathcal{R})$ 若滿足結合律，則以下兩個敘述是等價的：

1. *(a)* 有左單位元素 e_l
   (b) 對所有 $a \in S$，存在左反元素
2. *(a)* e_l 是單位元素
   (b) 對所有 $a \in S$，存在反元素

證明 我們要證明第 1 項和第 2 項等價，因此我們有兩部分要證明：第一、證明第 1 項可以推到第 2 項；第二、證明第 2 項可以推到第 1 項。

1. 我們先證第 2 項推到第 1 項 $(\Leftarrow)$：
   (a) 根據定義 1.13，我們有單位元素 e_l，換句話說 e_l 也是左單位元素。
   (b) 同樣地，根據定義 1.16，我們馬上就可以得到對於所有 $a \in S$，存在左反元素。
2. 再證第 1 項可以推到第 2 項 $(\Rightarrow)$：

(a) 根據定義 1.13，我們證明 e_l 是單位元素，只要證明對所有 $a \in S$，都符合 $a\mathcal{R}e_l = a$ 即可。根據定義 1.16，假設 b_l 是 a 的左反元素，我們有

$$b_l\mathcal{R}a = e_l$$

假設 d_l 是 b_l 的左反元素，我們也可得到：

$$d_l\mathcal{R}b_l = e_l$$

接著我們計算 $a\mathcal{R}e_l$：

$$\begin{aligned}
a\mathcal{R}e_l &= e_l\mathcal{R}(a\mathcal{R}e_l) && e_l \text{ 是 } (a\mathcal{R}e_l) \text{ 的左單位元素} \\
&= (d_l\mathcal{R}b_l)\mathcal{R}(a\mathcal{R}e_l) && \text{因爲 } d_l\mathcal{R}b_l = e_l \\
&= d_l\mathcal{R}(b_l\mathcal{R}(a\mathcal{R}e_l)) && \text{結合律} \\
&= d_l\mathcal{R}((b_l\mathcal{R}a)\mathcal{R}e_l) && \text{結合律} \\
&= d_l\mathcal{R}(e_l\mathcal{R}e_l) && \text{因爲 } b_l\mathcal{R}a = e_l \\
&= d_l\mathcal{R}e_l && e_l \text{ 是 } e_l \text{ 的左單位元素} \\
&= d_l\mathcal{R}(b_l\mathcal{R}a) && \text{因爲 } b_l\mathcal{R}a = e_l \\
&= (d_l\mathcal{R}b_l)\mathcal{R}a && \text{結合律} \\
&= e_l\mathcal{R}a && \text{因爲 } d_l\mathcal{R}b_l = e_l \\
&= a && e_l \text{ 是 } a \text{ 的左單位元素}
\end{aligned}$$

得出對所有 $a \in S$，使得 $e_l\mathcal{R}a = a\mathcal{R}e_l = e_l$，因此 e_l 是單位元素。

(b) 做爲習題。

□

註. 若是只有右單位元素 e_r，以及對所有 $a \in S$ 有右反元素 b_r 的時候，也會有類似的性質。

四、 零元素與零因子

定義 1.21 (零元素)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 中，若

- 存在 $z_l \in S$，對所有 $a \in S$，$z_l\mathcal{R}a = z_l$，則 z_l 爲***左零元素 (Left zero element)***
- 存在 $z_r \in S$，對所有 $a \in S$，$a\mathcal{R}z_r = z_r$，則 z_r 爲***右零元素 (Right zero element)***

- 存在 $z \in S$，對所有 $a \in S$，$z\mathcal{R}a = a\mathcal{R}z = z$，則 z 爲**零元素 *(Zero element)***

註. 零元素又稱**吸收元素 *(Absorbing element)***。

定理 1.22 (零元素存在性)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 具有結合律，若存在左零元素 z_l，右零元素 z_r，則 $z_l = z_r$，即零元素存在。

證明 做爲習題。 □

定理 1.23 (零元素唯一性)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 具有結合律，若存在零元素，則零元素唯一。

證明 做爲習題。 □

定理 1.24. 一個封閉的代數結構 $(S, \mathcal{R})$ 有單位元素 e、零元素 z，若 $|S| \geq 2$，則 $e \neq z$。

證明 我們用反證法證明，假設 $e = z$，則對於所有 $a \in S$，我們發現

$$
\begin{aligned}
a &= a\mathcal{R}e && e \text{ 是單位元素} \\
&= a\mathcal{R}z && e = z \\
&= z && z \text{ 是零元素} \\
&= e && e = z
\end{aligned}
$$

我們求出所有的 $a = e = z$ 都是相同的元素，因此 $|S| = 1$，與 $|S| \geq 2$ 矛盾。 □

性質 1.25. 一個封閉的代數結構 $(S, \mathcal{R})$ 存在單位元素 e，若 $\mathcal{R}$ 在 S 上有零元素 z 且 $z \neq e$，則 z 沒有反元素。

證明 做爲習題。 □

定義 1.26 (零因子)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 中存在零元素 z，若 $a, b \in S$ 且 $a, b \neq z$，使得 $a\mathcal{R}b = z$，則 a, b 稱爲**零因子 *(Zero divisor)***。

定理 1.27 (零因子性質)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 滿足以下條件：

- 有結合律
- 存在單位元素 e
- 存在零元素 z

若 $a, b \in S$ 是零因子，則 a, b 沒有反元素。

證明 因為 a, b 是零因子，所以 $a\mathcal{R}b = z$ 且 $a, b \neq z$。先假設 a 有反元素 $c \in S$，也就是 $a\mathcal{R}c = c\mathcal{R}a = e$，我們知道

$$
\begin{aligned}
z &= c\mathcal{R}z && z \text{ 是零元素，因此 } c\mathcal{R}z = z \\
&= c\mathcal{R}(a\mathcal{R}b) && a\mathcal{R}b = z \\
&= (c\mathcal{R}a)\mathcal{R}b && \text{結合律} \\
&= e\mathcal{R}b && c \text{ 是 } a \text{ 的反元素，因此 } c\mathcal{R}a = e \\
&= b && e \text{ 是單位元素}
\end{aligned}
$$

我們求出 $z = b$，與原來的前提 $(a, b \neq z)$ 矛盾。同理，b 也沒有反元素。 □

定義 1.28 (消去律)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 中，對所有 $a, b, c \in S$，若

- $a\mathcal{R}b = a\mathcal{R}c$ 可得到 $b = c$，則 $\mathcal{R}$ 在 S 上有**左消去律** ***(Left cancellation law)***。
- $b\mathcal{R}a = c\mathcal{R}a$ 可得到 $b = c$，則 $\mathcal{R}$ 在 S 上有**右消去律** ***(Right cancellation law)***。
- $\mathcal{R}$ 滿足左消去律和右消去律，則 $\mathcal{R}$ 在 S 上有**消去律** ***(Cancellation law)***。

定理 1.29 (消去律性質)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 滿足以下條件：

- 有結合律
- 有單位元素 e
- 對所有 $a \in S$ 都有反元素

則 $\mathcal{R}$ 在 S 上有消去律。

證明 根據定義 1.28，我們要驗證 $\mathcal{R}$ 有左消去律和右消去律。

左消去律 對於所有 $a, b, c \in S$，驗證 $a\mathcal{R}b = a\mathcal{R}c$ 是否能推導出 $b = c$。假設 a 有反元素 $d \in S$，使得 $d\mathcal{R}a = a\mathcal{R}d = e$，則

$$
\begin{aligned}
a\mathcal{R}b = a\mathcal{R}c &\Rightarrow d\mathcal{R}(a\mathcal{R}b) = d\mathcal{R}(a\mathcal{R}c) && \text{等式兩邊同時與 } d \text{ 做運算} \\
&\Rightarrow (d\mathcal{R}a)\mathcal{R}b = (d\mathcal{R}a)\mathcal{R}c && \text{結合律} \\
&\Rightarrow e\mathcal{R}b = e\mathcal{R}c && d \text{ 是 } a \text{ 的反元素} \\
&\Rightarrow b = c && e \text{ 是單位元素}
\end{aligned}
$$

右消去律 做爲習題。 □

定理 1.30. 一個封閉的代數結構 $(S,\mathcal{R})$ 若滿足結合律，則以下兩個敘述是等價的：

1. (a) e 是單位元素
   (b) 對所有 $a\in S$，存在反元素
2. 對於任意 $a,b\in S$，x,y 是未知數，方程式 $a\mathcal{R}x=b$ 和 $y\mathcal{R}a=b$ 存在唯一解。

證明

1. $(\Rightarrow)$ 方向：已知有單位元素 e 和反元素，我們要證存在性和唯一性。
   (a) 先證存在性，我們只要找出一組解酒可以證明存在性。假設 $c\in S$ 是 a 的反元素，我們可以找出當 $x=c\mathcal{R}b$ 時，

$$\begin{aligned} a\mathcal{R}x &= a\mathcal{R}(c\mathcal{R}b) && x=c\mathcal{R}b \\ &= (a\mathcal{R}c)\mathcal{R}b && \text{結合律} \\ &= e\mathcal{R}b && c\text{ 是 }a\text{ 的反元素} \\ &= b && e\text{ 是單位元素} \end{aligned}$$

   (b) 再證唯一性，假設 x 有兩個解 d 和 $d^{'}$，亦即 $a\mathcal{R}d=b=a\mathcal{R}d^{'}$，則

$$\begin{aligned} d &= e\mathcal{R}d && e\text{ 是單位元素} \\ &= (c\mathcal{R}a)\mathcal{R}d && c\mathcal{R}a=e \\ &= c\mathcal{R}(a\mathcal{R}d) && \text{結合律} \\ &= c\mathcal{R}(a\mathcal{R}d^{'}) && a\mathcal{R}d=b=a\mathcal{R}d^{'} \\ &= (c\mathcal{R}a)\mathcal{R}d^{'} && \text{結合律} \\ &= e\mathcal{R}d^{'} && c\mathcal{R}a=e \\ &= d^{'} && e\text{ 是單位元素} \end{aligned}$$

   (c) 同理，也可證明 y 存在唯一解 $b\mathcal{R}c$。
2. $(\Leftarrow)$ 方向：做爲習題。

□

五、 符號簡化

定義 1.31 (單位元素記號)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 存在單位元素 e，若

- $\mathcal{R}$ 爲加法 $+_S$，則 e 爲**加法單位元素 *(Additive identity)***，此時 e 記爲 0_S。
- $\mathcal{R}$ 爲乘法 $\cdot_S$，則 e 爲**乘法單位元素 *(Multiplicative identity)***，e 記爲 1_S。

註. *1.* $+_S$ 不是眞的代表實數或複數的加法運算，而是代表他在 S 上有類似我們常見的加法性質，因此用這個符號容易聯想；$\cdot_S$ 亦然。

2. 使用 0 和 1 做爲記號只是方便我們去聯想他的性質，事實上並不是實數的「0」和「1」，只是單純的**符號**。

定義 1.32 (反元素記號)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 存在單位元素 e，且所有 $a\in S$ 均有反元素 $b\in S$，若

- $\mathcal{R}$ 爲加法 $+_S$，則 b 爲**加法反元素 *(Additive inverse)***，此時 b 記爲 $-a$。
- $\mathcal{R}$ 爲乘法 $\cdot_S$，則 b 爲**乘法反元素 *(Multiplicative inverse)***，此時 b 記爲 a^{-1}。

註. 同樣地，$-a$ 和 a^{-1} 只是單純的符號，不要和減法與倒數搞混。

定義 1.33 (連加記號)**.** 若一個封閉的代數結構 $(S,+_S)$ 的二元運算爲加法 $+_S$，且滿足以下條件：

- 有單位元素 0_S
- 對所有 $a\in S$ 有反元素 $-a$

，則定義連加記號 ka，$k\in\mathbb{Z}$：

1. $k=0$ 時，$0a=0_S$

2. $k>0$ 時，$ka=a+_S(k-1)a$

3. $k<0$ 時，

六、 其他性質

定義 1.34 (連乘)**.** 在一個封閉的代數結構 $(S,\mathcal{R})$ 中，對所有 $a\in S$ 定義 a^k，$k\in\mathbb{Z}^+$：

1. 若 $k=1$，則 $a^k=a^1=a$

2. 若 $k>1$，則 $a^k=a\mathcal{R}a^{k-1}$

定義 1.35 (冪等元素與冪等律)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 中，若有 $a\in S$，使得 $a\mathcal{R}a=a$，則 a 稱爲**冪等元素 *(Idempotent element)***。若所有 $a\in S$ 都是冪等元素，則稱二元運算 $\mathcal{R}$ 在 S 上滿足**冪等律 *(Idempotent)***。

定義 1.36 (冪零律)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 中，若對於所有 $a\in S$，使得 $a\mathcal{R}a=a$，則稱二元運算 $\mathcal{R}$ 對 S 滿足**冪等律 *(Idempotent)***。

第三節　同態與同構

習題

1. 定義一個在 $\mathbb{Z}$ 上二元運算 $\diamondsuit$，對所有 $x, y \in \mathbb{Z}$，使得 $x \diamondsuit y = 3x + y - 4$。問 $((7 \diamondsuit 5) \diamondsuit 3) - 7 \diamondsuit (5 \diamondsuit 3)$？
2. 證明定理 1.18。
3. 證明定理 1.19。
4. 證明定理 1.20 第 2b 項。
5. 證明定理 1.22。
6. 證明定理 1.23。
7. 證明性質 1.25。
8. 證明定理 1.29 右消去律部分。
9. 證明定理 1.30 $(\Leftarrow)$ 部分。
10. 一封閉的代數結構 $(S, \mathcal{R})$ 有交換律，試證明：
    (a) 若 $\mathcal{R}$ 有左單位元素 e_l，則單位元素存在
    (b) 對所有 $a \in S$ 都有左反元素 b_l，則反元素存在
11. 一個封閉的代數結構 $(S, \mathcal{R})$ 滿足以下條件：
    - 有結合律
    - 有左單位元素 e_l
    - 對所有 $a \in S$ 都有左反元素

    則 $\mathcal{R}$ 在 S 上有左消去律。

第一部分

群論

第二章

群

第一節　定義與性質

定義 2.1 (群). 一個代數結構 $(G, \cdot_G)$ 被稱爲***群 (Group)***，滿足以下條件：

(G1) 有封閉律，對於所有 $a, b \in G$，$a \cdot_G b \in G$
(G2) 有結合律，對於所有 $a, b, c \in G$，$(a \cdot_G b) \cdot_G c = a \cdot_G (b \cdot_G c)$
(G3) 有單位元素 $e \in G$，使得所有 $a \in G$，$e \cdot_G a = a \cdot_G e = a$
(G4) 對於每個元素 $a \in G$ 都有反元素 $b \in G$，使得 $a \cdot_G b = b \cdot_G a = e$

此時 $\cdot_G$ 稱爲**群乘法**。

性質 2.2 (群的性質). 若 $(G, \cdot_G)$ 爲一個群，則有以下性質：

1. 單位元素唯一。
2. 對於所有 $a \in G$，其反元素唯一。

證明

1. 根據定理 1.15 得證。
2. 根據定理 1.19 得證。

□

定義 2.3 (符號簡化). 若一個群 G 的二元運算爲群乘法 $\cdot_G$，則我們可對符號簡化：

1. 對於所有 $a, b \in G$，$a \cdot_G b \Leftrightarrow ab$。
2. 對於所有 $a \in G$，其反元素記爲 a^{-1}。

3. 定義群連乘 a^k，$k \in \mathbb{Z}$：
   (a) $k = 0$ 時，$a^k = a^0 = e$
   (b) $k > 0$ 時，$a^k = a \cdot_G a^{k-1} = aa^{k-1}$
   (c) $k < 0$ 時，$a^k = a^{-1} \cdot_G a^{k+1} = a^{-1}a^{k+1}$

性質 2.4. 若 $(G, \cdot_G)$ 爲一個群，對於所有 $a, b \in G$，則有以下性質：

1. $(a^{-1})^{-1} = a$
2. $(ab)^{-1} = b^{-1}a^{-1}$

註. $(a^{-1})^{-1}$ 應理解爲「a^{-1} 的反元素」。

證明

1. 我們知道 a^{-1} 是 a 的反元素，且 $(a^{-1})^{-1}$ 也是 a^{-1} 的反元素，根據群的定義 (G4)，我們知道

$$a^{-1}a = aa^{-1} = e$$
$$\left(a^{-1}\right)^{-1}a^{-1} = a^{-1}\left(a^{-1}\right)^{-1} = e$$

因此

$$\begin{aligned}
a &= ea && \text{群的定義 (G3)} \\
&= (\left(a^{-1}\right)^{-1}a^{-1})a && \left(a^{-1}\right)^{-1}a^{-1} = e \\
&= \left(a^{-1}\right)^{-1}(a^{-1}a) && \text{群的定義 (G2)} \\
&= \left(a^{-1}\right)^{-1}e && a^{-1}a = e \\
&= \left(a^{-1}\right)^{-1} && \text{群的定義 (G3)}
\end{aligned}$$

2. 做爲習題。

$\square$

性質 2.5 (群的消去律)**.** 若 $(G, \cdot_G)$ 爲一個群，則 G 滿足消去律。即對於所有 $a, b, c \in G$，若

1. $ab = ac$，則 $b = c$
2. $ba = ca$，則 $b = c$

證明 根據定理 1.29 得證。 $\square$

定理 2.6. 若 $(G, \cdot_G)$ 爲一個群，則對於任意 $a, b \in G$，x, y 是未知數，$ax = b$ 和 $ya = b$ 存在唯一解。

證明 由定理 1.30 可知唯一解爲 $x = a^{-1}b$ 且 $y = ba^{-1}$。 $\square$

第二節　子群