Fundamental Abstract Algebra
基礎抽象代數

許胖

2015 年 1 月 23 日

目 錄

第 一 章

基礎知識

第一節　數系

定義 1.1 (常見數系定義)**.** 對於一般數字，我們定義以下集合：

1. **非負整數**表示爲 $\mathbb{N} = \{0, 1, 2, \cdots\}$
2. **整數**表示爲 $\mathbb{Z} = \{\cdots, -1, 0, 1, \cdots\}$
3. **正整數**表示爲 $\mathbb{Z}^+ = \{1, 2, \cdots\}$
4. **負整數**表示爲 $\mathbb{Z}^- = \{-1, -2, \cdots\}$
5. **有理數**表示爲 $\mathbb{Q}$
6. **無理數**表示爲 $\mathbb{Q}_c$
7. **實數**表示爲 $\mathbb{R}$
8. **正數**表示爲 $\mathbb{R}^+$
9. **負數**表示爲 $\mathbb{R}^-$
10. **複數**表示爲 $\mathbb{C}$

定義 1.2 (雙複數)**.** 定義**雙複數** ***(Bicomplex number)*** $a+bi+cj+dk$，其中 $a, b, c, d \in \mathbb{R}$，並滿足以下運算法則：

1. $ij = ji = k$
2. $i^2 = k^2 = -1$
3. $j^2 = 1$

定義 1.3 (四元數)**.** 定義**四元數** ***(Quaternion)*** $a + bi + cj + dk$，其中 $a, b, c, d \in \mathbb{R}$，並滿足運算法則 $i^2 = j^2 = k^2 = ijk = -1$。

第二節　函數

定義 1.4 (函數)**.** 有兩個集合 A、B，若 A 和 B 之間存在對應關係 f，使得所有 $a \in A$ 皆可對應到**唯一的** $b \in B$，則 f 稱為**函數 *(Function)***，記為 $f : A \to B$，此時 a 對應到 b 記為 $f(a) = b$。

註. 對所有 $a \in A$ 不會對應到兩個以上的 b，或是沒有 b 值。

定義 1.5 (定義域、對應域與值域)**.** 有兩個集合 A、B，若有一函數 $f : A \to B$，則

1. A 稱為**定義域 *(Domain)***
2. B 稱為**對應域 *(Codomain)***
3. 對於所有 $a \in A$，$f(a)$ 形成的集合稱為**值域 *(Range)***，記為 $f(A)$ 或是 $R(f)$。

定義 1.6 (函數的合成運算)**.** 有三個集合 A、B 和 C，若有兩個函數 f、g

$$\begin{aligned} f &: A \to B \\ g &: B \to C \end{aligned}$$

定義函數的合成運算 $h = g \circ f$ (簡寫為 gf)，其中 $h : A \to C$，使得對所有 $a \in A$

$$h(a) = (gf)(a) = (g \circ f)(a) = g(f(a))$$

定理 1.7 (函數合成結合律)**.** 有四個集合 A_1、A_2、A_3 和 A_4，若有三個函數 f、g、h

$$\begin{aligned} f &: A_1 \to A_2 \\ g &: A_2 \to A_3 \\ h &: A_3 \to A_4 \end{aligned}$$

則函數合成符合 $(hg)f = h(gf)$。

證明 對所有 $a_1 \in A_1$，則

$$\begin{aligned} ((hg)f)(a_1) &= (hg)(f(a_1)) && \text{根據定義 1.6} \\ &= h(g(f(a_1))) && \text{根據定義 1.6} \\ &= h((gf)(a_1)) && \text{根據定義 1.6} \\ &= (h(gf))(a_1) && \text{根據定義 1.6} \end{aligned}$$

□

定義 1.8 (單位函數)**.** 集合 A 上有一函數 $I_A : A \to A$，若對於所有 $a \in A$ 使得 $I_A(a) = a$，則 I_A 稱爲在 A 上的**單位函數** ***(Identity function)***。

定義 1.9 (反函數)**.** 兩集合 A、B 上有一函數 $f : A \to B$，若存在 $g : B \to A$ 使得

$$gf = I_A$$
$$fg = I_B$$

則 g 稱爲 f 的反函數，此時 g 可記爲 f^{-1}。

定義 1.10 (可逆函數)**.** 兩集合 A、B 上有一函數 $f : A \to B$，若 f 存在反函數，則 f 稱爲**可逆函數** ***(Invertible function)***。

定義 1.11 (單射函數)**.** 兩集合 A、B 上有一函數 $f : A \to B$，若對於所有 $a_1, a_2 \in A$，$f(a_1) = f(a_2)$ 可以得到 $a_1 = a_2$，我們稱函數 f 爲**一對一函數** ***(One-to-one function)*** 或是**單射函數** ***(Injective function)***。

定義 1.12 (滿射函數)**.** 兩集合 A、B 上有一函數 $f : A \to B$，若對於所有 $b \in B$ 皆可找到 $a \in A$ 使得 $f(a) = b$，我們稱函數 f 爲**映成函數** ***(Onto function)*** 或是**滿射函數** ***(Surjective function)***。

定義 1.13 (雙射函數)**.** 兩集合 A、B 上有一函數 $f : A \to B$，若 f 是單射函數且爲滿射函數，則 f 稱爲**雙射函數** ***(Bijective function)***。

定理 1.14. 兩集合 A、B 上有一函數 $f : A \to B$，則 f 是可逆函數若且唯若 f 是雙射函數。

證明 做爲習題。 □

定理 1.15 (反函數唯一性)**.** 兩集合 A、B 上有一函數 $f : A \to B$，若 f 是可逆函數，則 f 的反函數是唯一的。

證明 做爲習題。 □

定理 1.16. 兩集合 A、B 上有一函數 $f : A \to B$，若 f 是可逆函數，則反函數 $f^{-1} : B \to A$ 也是可逆函數。

證明 做爲習題。 □

習題

1. 證明定理 1.14。
2. 證明定理 1.15。
3. 證明定理 1.16。

第 二 章

代數結構

第一節 簡介

定義 2.1 (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 2.2. 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 2.3 (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 2.4 (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 2.5. 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 2.6 (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)***。

定義 2.7 (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 2.8 (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 2.9. 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。

□

範例 2.10. 說明下列代數結構是否滿足封閉律。

1. $(\mathbb{R}, +)$

2. $(\mathbb{N}, /)$
3. $\big(\mathbb{Z}[\sqrt{2}], \cdot\big)$
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 2.11 (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

$$\begin{aligned}a\mathcal{R}_1(a\mathcal{R}_2b) = a\\ a\mathcal{R}_2(a\mathcal{R}_1b) = a\end{aligned}$$

，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。

範例 2.12. 一個邏輯語句與 *or* 運算、*and* 運算 $(\mathcal{L}, \vee, \wedge)$ 有吸收律，因爲對於 a

定義 2.13 (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

$$\begin{aligned}a\mathcal{R}_1(b\mathcal{R}_2c) = (a\mathcal{R}_1b)\mathcal{R}_2(a\mathcal{R}_1c)\\ (b\mathcal{R}_2c)\mathcal{R}_1a = (b\mathcal{R}_1a)\mathcal{R}_2(c\mathcal{R}_1a)\end{aligned}$$

，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。

範例 2.14. 整數加法與乘法 $(\mathbb{Z}, +, \cdot)$ 中乘法對加法有分配律，加法對乘法則無。

$$2 \cdot (3 + 4) = (2 \cdot 3) + (2 \cdot 4)$$
$$2 + (3 \cdot 4) \neq (2 + 3) \cdot (2 + 4)$$

二、 單位元素

定義 2.15 (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 2.16 (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 2.15，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 2.15，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 2.17 (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 2.18 (反元素)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 中，若

- 存在左單位元素 $e_l \in S$，使得 $a, b_l \in S$，$b_l \mathcal{R} a = e_l$，則 b_l 稱爲 a 的**左反元素 *(Left inverse)***
- 存在右單位元素 $e_r \in S$，使得 $a, b_r \in S$，$a \mathcal{R} b_r = e_r$，則 b_r 稱爲 a 的**右反元素 *(Right inverse)***
- 存在單位元素 $e \in S$，使得 $a, b \in S$，$b \mathcal{R} a = a \mathcal{R} b = e$，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 2.19. 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 2.15，我們知道 $e \mathcal{R} e = e$，同時也符合反元素的定義。 □

定理 2.20 (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 2.21 (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。 □

定義 2.22 (反元素通用記號)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 中，若對 $a \in S$ 有反元素，則此反元素記爲 a'。

性質 2.23 (反元素性質)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 若滿足以下條件：

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

則對所有 $a, b \in S$ 有以下特性：

1. $(a')' = a$
2. $(a\mathcal{R}b)' = b'\mathcal{R}a'$

證明

1. 依照定義，我們知道 a' 是 a 的反元素、$(a')'$ 是 a' 的反元素，因此

$$a'\mathcal{R}a = a\mathcal{R}a' = e$$
$$(a')'\mathcal{R}a' = a'\mathcal{R}(a')' = e$$

則我們可以推導出：

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

2. 做爲習題。

□

定理 2.24. 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 2.15，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 2.18，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 2.15，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 2.18，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 2.25 (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 2.26 (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 2.27 (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 2.28. 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 2.29. 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 2.30 (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 2.31 (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 $a' \in S$，我們知道

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

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 2.32 (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 2.33 (消去律性質)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 若滿足以下條件：

- 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 2.32，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 $a' \in S$，則

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

右消去律 做爲習題。 □

定理 2.34. 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 是在 S 的未知數，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就可以證明存在性。假設 a 有反元素 $a' \in S$，我們可以找出當 $x = a'\mathcal{R}b$ 時，

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

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

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

   (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 2.35 (連運算記號)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 中，對於任意 $a_1,\cdots,a_n\in S$，定義運算 $\mathfrak{R}_{i=1}^n a_i$，其中 $n\in\mathbb{Z}^+$：

1. 當 $n=1$ 時，$\mathfrak{R}_{i=1}^n a_i = a_1$
2. 當 $n>1$ 時，$\mathfrak{R}_{i=1}^n a_i = a_1\mathcal{R}(a_2\mathcal{R}(\cdots\mathcal{R}a_n)) = a_1\mathcal{R}(\mathfrak{R}_{i=2}^n a_i)$

性質 2.36 (連運算性質)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 中若滿足結合律，則對於 $n,m\in\mathbb{Z}^+$、$n<m$ 且 $a_1,\cdots,a_{n+m}\in S$ 滿足

$$(\mathop{\mathfrak{R}}_{i=1}^{n} a_i)\mathcal{R}(\mathop{\mathfrak{R}}_{j=n+1}^{n+m} a_j) = \mathop{\mathfrak{R}}_{k=1}^{n+m} a_k$$

證明 做爲習題。 □

定義 2.37. 一個封閉的代數結構 $(S,\mathcal{R})$ 中，對於任意 $a_1,\cdots,a_n\in S$ 做運算，且這 n 個元素不得改變次序，所有以某個順序運算 $a_1,\cdots,a_n$ 的集合，我們記爲 $\Phi(a_1,\cdots,a_n)$。

範例 2.38. 假設 $a_1,a_2,a_3,a_4\in S$，則 $\Phi(a_1,a_2,a_3,a_4)$ 有 5 個元素：

1. $a_1\mathcal{R}(a_2\mathcal{R}(a_3\mathcal{R}a_4))$
2. $a_1\mathcal{R}((a_2\mathcal{R}a_3)\mathcal{R}a_4)$
3. $(a_1\mathcal{R}a_2)\mathcal{R}(a_3\mathcal{R}a_4)$
4. $(a_1\mathcal{R}(a_2\mathcal{R}a_3))\mathcal{R}a_4$
5. $((a_1\mathcal{R}a_2)\mathcal{R}a_3)\mathcal{R}a_4$

定理 2.39 (廣義結合律)**.** 一個封閉的代數結構 $(S,\mathcal{R})$ 中若滿足結合律，對於任意 $a_1,\cdots,a_n\in S$，則所有 $\phi\in\Phi(a_1,\cdots,a_n)$，$\phi=\mathfrak{R}_{i=1}^n a_i$。

證明 我們用強數學歸納法證明：

1. 先證明 $k=1$，對所有 $\phi\in\Phi(a_1)=\{a_1\}$，$\phi=a_1=\mathfrak{R}_{i=1}^k a_i$
2. 假設對所有 $1\le k\le n$ 都滿足此性質，接著證明當 $k=n+1$ 時，對於所有 $\phi\in\Phi(a_1,\cdots,a_n)$，因爲 $\mathcal{R}$ 是二元運算，最後必有 $\phi_l\in\Phi(a_1,\cdots,a_x)$ 且

$\phi_r \in \Phi(a_{x+1}, \cdots, a_{n+1})$，$1 \leq x \leq n+1$，使得

$$
\begin{aligned}
\phi &= \phi_l \mathcal{R} \phi_r \\
&= (\mathop{\mathfrak{R}}_{i=1}^{x} a_i) \mathcal{R} (\mathop{\mathfrak{R}}_{j=x+1}^{n+1} a_j) && \text{強數學歸納法假設} \\
&= \mathop{\mathfrak{R}}_{i=1}^{n+1} a_i && \text{根據性質 2.36}
\end{aligned}
$$

□

註. 也就是說，一封閉的代數結構 $(S, \mathcal{R})$ 有結合律，則 $a_1, \cdots, a_n \in S$ 只要前後次序不變，則結果相同。

定義 2.40 (倍運算記號). 一個封閉的代數結構 $(S, \mathcal{R})$ 中若滿足以下條件：

- 結合律
- 有單位元素 e

則對於任意 $a \in S$，定義運算 $\mathfrak{R}^n a$，其中 $n \in \mathbb{Z}^+$：

1. 當 $n = 1$，$\mathfrak{R}^n a = \mathfrak{R}^1 a = a$
2. 當 $n > 1$，$\mathfrak{R}^n a = a\mathcal{R}(\mathfrak{R}^{n-1} a)$

註. 根據廣義結合律的性質 *2.36*，無論這幾個 a 以何種順序運算，結果皆相同。

定義 2.41 (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 2.42 (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 $a' \in S$，若

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

六、 其他性質

定義 2.43 (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 2.44 (冪零元素與冪零律)**.** 一個封閉的代數結構 $(S, \mathcal{R})$ 中存在零元素 z，若 $a \in S$，使得 $\mathfrak{R}^k a = z$，$k \in \mathbb{Z}^+$，則 a 稱爲**冪零元素** ***(Nilpotent element)***。則稱二元運算 $\mathcal{R}$ 對 S 滿足**冪零律** ***(Nilpotent)***。

第三節　同態與同構

定義 2.45 (代數結構分類)**.** 兩個代數結構 $(S, \mathcal{R}_{S,1}, \ldots, \mathcal{R}_{S,n})$、$(T, \mathcal{R}_{T,1}, \ldots, \mathcal{R}_{T,n})$，若有相同的公理 $\mathcal{A}$，則我們稱 S 和 T 是同類代數結構。

定義 2.46 (同態)**.** 兩個同類的代數結構 $(S, \mathcal{R}_{S,1}, \ldots, \mathcal{R}_{S,n})$、$(T, \mathcal{R}_{T,1}, \ldots, \mathcal{R}_{T,n})$ 若能找到一函數 $f : S \to T$，使得對所有 $a, b \in S$、$1 \leq i \leq n$ 都遵守

$$f(a\mathcal{R}_{S,i}b) = f(a)\mathcal{R}_{T,i}f(b)$$

則稱 S 和 T **同態** ***(Homomorphism)***。

定義 2.47 (同構)**.** 兩個同類的代數結構 $(S, \mathcal{R}_{S,1}, \ldots, \mathcal{R}_{S,n})$、$(T, \mathcal{R}_{T,1}, \ldots, \mathcal{R}_{T,n})$ 若能找到一函數 $f : S \to T$ 滿足以下條件

1. S 和 T 同態
2. f 是雙射函數

則稱 S 和 T **同構** ***(Isomorphism)***，記爲 $S \cong T$，f 稱爲同構函數。

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 2.20。
3. 證明定理 2.21。
4. 證明定理 2.24 第 2b 項。
5. 證明性質 2.23 第 2 項。

6. 證明定理 2.26。
7. 證明定理 2.27。
8. 證明性質 2.29。
9. 證明定理 2.33 右消去律部分。
10. 證明定理 2.34 ($\Leftarrow$) 部分。
11. 證明性質 2.36。
12. 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
13. 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 三 章

群

第一節　定義與性質

定義 3.1 (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 $a' \in G$，使得 $a \cdot_G a' = a' \cdot_G a = e$

此時 $\cdot_G$ 稱爲**群乘法**。

性質 3.2 (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 2.17 得證。
2. 根據定理 2.21 得證。

□

定義 3.3 (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 $a, b \in G$，$a \cdot_G b$ 可寫爲 ab。
2. 對於所有 $a \in G$，其反元素記爲 a^{-1}。

性質 3.4. 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。

□

定義 3.5 (群連乘). 若一個群 G 的二元運算爲群乘法 $\cdot_G$，則定義群連乘 a^k，$k \in \mathbb{Z}$：

1. $k = 0$ 時，$a^k = a^0 = e$
2. $k > 0$ 時，$a^k = a \cdot_G a^{k-1} = aa^{k-1}$；$a^{-k} = (a^{-1})^k$

推論 3.6 (群連乘性質). 一個群 G 中，對所有 $a \in G$，$m, n \in \mathbb{Z}$，則

1. $a^m a^n = a^{m+n} = a^n a^m$
2. $(a^m)^n = a^{mn}$
3. $(a^m)^{-1} = a^{-m}$

性質 3.7 (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 2.33 得證。 □

定理 3.8. 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 2.34 可知唯一解爲 $x = a^{-1}b$ 且 $y = ba^{-1}$。 □

定義 3.9 (阿貝爾群)**.** 一個群 $(G, \cdot_G)$，若對所有 $a, b \in G$ 都滿足 $ab = ba$，則 G 稱爲**阿貝爾群 *(Abelian group)***，又稱**交換群**。

範例 3.10. $(\mathbb{Z}, +)$ 是一個交換群，$(\mathbb{M}_{n\times n}(\mathbb{R}), \cdot)$ 就不是，反例：

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
$$AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = BA$$

定義 3.11 (半群和單半群)**.** 一個代數結構 $(G, \cdot_G)$ 若滿足 *(G1)* 和 *(G2)*，則 G 稱爲**半群 *(Semigroup)***。若 $(G, \cdot_G)$ 滿足 *(G1)*、*(G2)*、*(G3)*，則 G 稱爲**單半群 *(Monoid)***。

定義 3.12 (有限群)**.** 一個群 $(G, \cdot_G)$ 若 $|G| < \infty$，則 G 稱爲**有限群 *(Finite group)***。

第二節 子群

定義 3.13 (子群)**.** 一個群 $(G, \cdot_G)$ 上，若 $(H, \cdot_H)$ 是一個群且 $H \subseteq G$、$H \neq \emptyset$，則 $(H, \cdot_H)$ 被稱爲 G 的**子群 *(Subgroup)***。

註. $\cdot_G$ 和 $\cdot_H$ 要是相同的。

引理 3.14 (實用版子群)**.** 一個群 $(G, \cdot_G)$ 上有一個非空子集 H，H 滿足以下條件

1. 對於任意 $a, b \in H$，$ab \in H$
2. 對於任意 $a \in H$，存在 $a^{-1} \in H$

若且唯若 $(H, \cdot_H)$ 是一個子群。

註. 事實上這兩個規則就是驗證 *(G1)* 和 *(G4)*。

引理 3.15 (精簡版子群)**.** 一個群 $(G, \cdot_G)$ 上有一個非空子集 H，對於任意 $a, b \in H$，$ab^{-1} \in H$ 若且唯若 $(H, \cdot_H)$ 是一個子群。

性質 3.16. 一個群 $(G, \cdot_G)$ 上若有兩個子群 H_1、H_2，則 $H_1 \cap H_2$ 是 G 的子群。

定理 3.17 (有限子群)**.** 一個有限群 $(G, \cdot_G)$ 上有一個非空子集 H，對於任意 $a, b \in H$，$ab \in H$ 若且唯若 $(H, \cdot_H)$ 是一個子群。