基礎集合論

仙女國公主

最後編輯: 2026 年 11 月 20 日

目錄

1 邏輯與命題 **5**
- 1.1 邏輯的基本觀念 . . . 5
- 1.2 複合命題與邏輯連結詞 . . . 6
- 1.3 邏輯等價 . . . 9
- 1.4 邏輯量詞 . . . 12
- 1.5 推理 . . . 13
- 1.6 基本的證明方法 . . . 16

2 集合的基本概念 **19**
- 2.1 集合的公理 . . . 19
- 2.2 集合的運算律 . . . 24
- 2.3 指標族 . . . 29

3 映射 **31**
- 3.1 映射的定義與性質 . . . 31
- 3.2 映射的運算 . . . 33
- 3.3 像與原像 . . . 36
- 3.4 一般積集 . . . 38
- 3.5 運算 . . . 41
- 3.6 交換圖 . . . 43

4 關係 **45**
- 4.1 關係的定義 . . . 45
- 4.2 關係的閉包 . . . 47
- 4.3 等價關係 . . . 48
- 4.4 序關係 . . . 51
- 4.5 良序與數學歸納原理 . . . 53

5 集合的基數 **59**
- 5.1 基數 . . . 59
- 5.2 可數集 . . . 62
- 5.3 基數算術 . . . 64

單元 1

邏輯與命題

1.1 邏輯的基本觀念

定義 1.1.1 在我們所應用的語句中, 用來描述事實或表達看法的語句稱爲**陳述句**, 而可以判斷眞僞的陳述句稱爲**命題**. 通常以**眞值**表示命題的眞僞, 記**眞命題**的眞值爲 1, **僞命題** (或稱**假命題**) 的眞值爲 0. 一般上, 可用大寫字母 $P, Q, R, \ldots$ 來代表**任意**的命題, 這些字母稱爲**命題變數**, 由命題變數與基本**邏輯連接詞** (見下一節) 以及括號所組成的合法語句, 稱爲**命題公式**. 若 $P_1, \ldots, P_n$ 爲 n 個命題變數, 則可記它們組成的命題公式爲 $P(P_1, \ldots, P_n)$.

注意 1.1.2 命題公式本身並不具有特定的眞值. 只有當把公式中的所有命題變數, 都代入具體的特定命題 (或賦予具體的眞值 1 或 0) 時, 該公式才會成爲一個確定的**複合命題** (見定義 1.1.6), 並具有對應的眞值.

例 1.1.3 以下句子皆爲命題:

(1) $1 + 2 = 3$.

(2) 在平面上, 任意四邊形的內角和爲 $360°$.

(3) 37 是合數.

(4) 大阪是日本的首都.

其中, (1) 和 (2) 爲**眞命題**, (3) 和 (4) 爲**假命題**.

例 1.1.4 以下句子或者不是陳述句, 或者爲無法判斷眞僞的陳述句, 故不爲命題:

(1) 我美嗎? (疑問句)

(2) 男僕好像應該在下午的時候幫女王洗脚. (無法判斷眞僞)

(3) 參見女王陛下! (無法判斷眞僞)

(4) 跪下! (祈使句; 這是命令, 不是命題)

(5) 你的男友人眞好! (感歎句)

(6) $x \geq 0$. (在不確定 x 的取值的情況下, 無法判斷對錯, 不能算是直接的命題)

(7) 這句話不是眞話. (悖論, 不管認爲對還是錯都會導致矛盾)

注意 1.1.5 上例的第 (6) 點中, 如果加上量詞, 比如「 對任意實數 x, 都有 $x^2 \geq 0$. 」即爲一個命題, 其眞值爲 1; 或者如果上下文已經爲 x 賦值, 比如「 令 $x = 5$, 則 $x \geq 0$. 」也是一個命題. 單獨一句「 $x \geq 0$ 」只能算是「 命題函數 」.

定義 1.1.6 若一個命題不包含更小的命題, 則稱其爲**原子命題**或**簡單命題**, 否則稱爲**複合命題**.

例 1.1.7 (1) 不定方程式 $x^3+y^3=z^3$ 沒有非平凡整數解. (簡單命題)

(2) 你只有年滿十歲, 你才有資格出去抓寵物. (複合命題; 由「你年滿十歲」和「你有資格出去抓寵物」兩個命題組成)

1.2 複合命題與邏輯連結詞

定義 1.2.1 設 P 表示一命題, 所謂 P 的**否命題**或**否言**, 記作 $\neg P$, 是滿足如下性質的命題: 若 P 爲眞命題, 則 $\neg P$ 爲僞命題; 若 P 爲僞命題, 則 $\neg P$ 爲眞命題. 「$\neg$」稱爲**否定連結詞**, $\neg P$ 讀作「非 P」.

註記 1.2.2 一般上, 常以如下**眞值表**來表示 P 與 $\neg P$ 之間的關係:

P	$\neg P$
0	1
1	0

例 1.2.3 考慮如下三個命題:

(1) $1+2=4$.

(2) $1+2\neq 4$.

(3) $1+2=4$ 不成立.

這裡, (2) 及 (3) 都是 (1) 的否命題.

定義 1.2.4 設 P,Q 爲兩命題, 所謂 P 和 Q 的**合取**或**連言**, 記作 $P\wedge Q$, 是指滿足如下性質的命題: 當 P 和 Q 同時爲眞時, $P\wedge Q$ 爲眞; 只要 P 和 Q 至少有一者爲假, $P\wedge Q$ 便爲假. 「$P\wedge Q$」讀作「P 且 Q」, 「$\wedge$」稱爲**合取連結詞**.

註記 1.2.5 一般上, 常以如下眞值表來表示 $P\wedge Q$ 的眞值:

P	Q	$P\wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

註記 1.2.6 $\wedge$ 相當於自然語言中的「並且」、「與」、「和」、「以及」、「不但……而且……」、「雖然……但是……」、「儘管……仍然……」等. 但應注意, 命題「小明和小華是情侶」中的「和」沒有合取之意.

例 1.2.7 考慮如下四個命題:

(1) 鯨魚是哺乳類且 $2+2>2$.

(2) 鯨魚是魚類且 $2+2>2$.

(3) 鯨魚是哺乳類且 $2+2>5$.

(4) 鯨魚是魚類且 $2+2>5$.

只有命題 (1) 爲眞, 餘者皆爲假.

定義 1.2.8 設 P, Q 爲兩命題, 所謂 P 和 Q 的**析取** (**相容析取**) 或**選言** (**相容選言**), 記作 $P \vee Q$, 是指滿足如下性質的命題: 只要 P 和 Q 至少有一者爲眞, $P \vee Q$ 便爲眞; 當 P 和 Q 同時爲假時, $P \vee Q$ 爲假. 「$P \vee Q$」讀作「P 或 Q」, 「$\vee$」稱爲**析取連結詞**.

註記 1.2.9 一般上, 常以如下眞值表來表示 $P \vee Q$ 的眞值:

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

例 1.2.10 考慮如下四個命題:

(1) 鯨魚是哺乳類或 $2 + 2 > 2$.

(2) 鯨魚是魚類或 $2 + 2 > 2$.

(3) 鯨魚是哺乳類或 $2 + 2 > 5$.

(4) 鯨魚是魚類或 $2 + 2 > 5$.

只有命題 (4) 爲假, 餘者皆爲眞.

定義 1.2.11 設 P, Q 爲兩命題, 所謂 P 和 Q 的**排他析取**或**不相容選言**, 記作 $P \oplus Q$ 或 $P \veebar Q$, 是指滿足如下性質的命題: 當 P 和 Q 兩者的眞值相異時, $P \veebar Q$ 便爲眞; 當 P 和 Q 兩者的眞值相同時, $P \veebar Q$ 爲假. 「$P \veebar Q$」讀作「P 異或 Q」, 「$\oplus$ 及 $\veebar$」稱爲**異或連結詞**.

註記 1.2.12 一般上, 常以如下眞值表來表示 $P \veebar Q$ 的眞值:

P	Q	$P \veebar Q$
0	0	0
0	1	1
1	0	1
1	1	0

註記 1.2.13 自然語言中的「或」是指「可兼或 ($\vee$)」還是「不可兼或 ($\veebar$)」需要仔細分析. 一般來說, 只要不是非常明顯的不可兼或, 就使用 $\vee$. 另外, $\veebar$ 相當於自然語言中的「或者……或者……」、「要麼……要麼……」等.

例 1.2.14 (1)「一個整數是奇數或是偶數」中的「或」顯然是不可兼或, 因爲一個整數不可能同時爲奇數和偶數.

(2)「二次方程式 $x^2 - 5x + 6 = 0$ 的解爲 $x = 2$ 或 $x = 3$」中的「或」也是不可兼或, 因爲如果 $x = 2$、$x = 3$ 同時成立, 即 x 同時是 2 及 3, 那麼就表示 $2 = 3$, 這不可能成立. 不過常常在解具有多解的方程式或方程組時, 還是會有人用符號「$\vee$」來連接各解.

(3) 不等式 $x \leq y$ 表示「$x < y$ 或 $x = y$」, 這裡的「或」也是不可兼或, 因爲根據三一律, 可知這兩者不可能同時成立.

(4)「有兩條對稱軸的四邊形是菱形或矩形」中的「或」則是可兼或, 因爲一個四邊形可以同時是菱形和矩形, 即正方形.

定義 1.2.15 設 P, Q 爲兩命題, 所謂**蘊含**或**條件命題**或**假言**, 記作 $P \to Q$, 是指滿足如下性質的命題: 只有當 P 爲眞且 Q 爲假時, $P \to Q$ 便爲假, 其餘三種情形之下 $P \to Q$ 爲眞. 「$P \to Q$」讀作「P 蘊含 Q」或「若 P 則 Q」, 「$\to$」稱爲**條件連結詞**或**蘊含連結詞**, P 稱爲**前件**或**前因**, Q 稱爲**後件**或**後果**.

註記 1.2.16 一般上, 常以如下眞值表來表示 $P \to Q$ 的眞值:

P	Q	$P \to Q$
0	0	1
0	1	1
1	0	0
1	1	1

註記 1.2.17 $\to$ 相當於自然語言中的「若⋯⋯則⋯⋯」、「當⋯⋯時, ⋯⋯」、「如果⋯⋯那麼⋯⋯」.

注意 1.2.18 命題「$P \to Q$」中, P 和 Q 之間不一定要有因果關係. 數學上的蘊含爲**實質蘊含**, 與日常語言中必須具有因果關聯的條件句有所不同.

例 1.2.19 (1)「若 $1+1=2$, 則雞是鳥類」是眞命題, 即使「$1+1=2$」和「雞是鳥類」之間沒有因果關係.

(2)「若氫氣是稀有氣體, 則人類用鰓呼吸」是眞命題, 即使「氫氣是稀有氣體」和「人類用鰓呼吸」都是假命題.

註記 1.2.20 只要 P 爲眞能保證 Q 爲眞, $P \to Q$ 便是眞命題. 比如說, 以 P 表示 $x=1$, Q 表示 $x^2=1$. 當 $x=1$ 時, 即 P 爲眞, 此時必有 $x^2=1$, 即 Q 爲眞. 但是, 當 $x^2=1$ 時, 即 Q 爲眞, 卻無法保證 P 爲眞, 因爲有可能 $x=-1$, 此時 P 命題爲假.

定義 1.2.21 設 P, Q 爲兩命題, 則稱 $Q \to P$ 爲 $P \to Q$ 的**逆命題**, $\neg Q \to \neg P$ 爲 $P \to Q$ 的**逆否命題**.

註記 1.2.22 「當 P 時, Q」及「若 P, 則 Q」是指「$P \to Q$」, 而「僅當 P 時, Q」及「唯若 P, 則 Q」是指「$Q \to P$」.

註記 1.2.23 「$P \to Q$」的常見英文句型爲「If P, then Q」或「Q if P」. 在有的中文教材或文章中, 也會用很生硬的語句將之直翻作「Q 若 P」、「Q 如果 P」、「Q 當 P」、「P 僅當 Q」等, 此類句型對中文來說更像倒裝句(不算錯誤句型), 帶有強烈的「翻譯腔」. 本講義會盡量避免使用此類句型, 因爲和常用的邏輯語句「$P \to Q$」的結構剛好相反.

註記 1.2.24 觀察 $P \to Q$ 及其逆命題、逆否命題的眞值表之間的關係:

P	Q	$P \to Q$	$Q \to P$	$\neg Q \to \neg P$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	1
1	1	1	1	1

容易看出, $\neg Q \to \neg P$ 與 $P \to Q$ 的眞值對應相同.

定義 1.2.25 設 P, Q 爲兩命題, 所謂**雙蘊含**、「等價」、**雙條件命題**或**雙假言**, 記作 $P \leftrightarrow Q$, 是指滿足如下性質的命題: 當 P 和 Q 的眞值相同時, $P \leftrightarrow Q$ 的眞值爲 1; 當 P 和 Q 的眞值相異時, $P \leftrightarrow Q$ 的眞值爲 0.「$P \leftrightarrow Q$」讀作「P 等價於 Q」, 「$\leftrightarrow$」稱爲**雙條件連結詞**或**雙蘊含連結詞**.

註記 1.2.26 一般上, 常以如下眞值表來表示 $P \leftrightarrow Q$ 的眞值:

P	Q	$P \leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

注意到, $P \leftrightarrow Q$ 和 $Q \leftrightarrow P$ 及 $\neg(P \veebar Q)$ 的眞值對應相同.

註記 1.2.27 「$P \leftrightarrow Q$」相當於自然語言中的「若且唯若 P, 則 Q」、「當且僅當 P 時, Q」、「P 的充分必要條件爲 Q」. 在數位邏輯中, 等價連結詞 $\leftrightarrow$ 也稱爲「同」.

在英文中, 「$P \leftrightarrow Q$」常用「Q if and only if P」或「Q iff P」來敍述, 故部分中文教材或文章也使用「Q 若且唯若 P」或「Q 當且僅當 P」等此類句型, 頻率甚至比「若且唯若 P, 則 Q」還高, 因此有人認爲「Q 若且唯若 P」聽起來更自然. 不過, 如果還是堅持要配合邏輯符號「$P \leftrightarrow Q$」的順序結構的話, 建議使用「P 的充要條件爲 Q」(見註記 1.3.17) 會更自然且不違背中文的標準文法.

例 1.2.28 (1) 四邊形的兩雙對邊平行的充要條件爲該四邊形是平行四邊形.

(2) 平面上三點共線的充要條件爲以它們爲頂點的三角形的面積爲 0.

註記 1.2.29 除了上述連結詞外, 還有「與非」、「或非」、「條件否定」等連結詞, 本講義不作進一步的介紹, 感興趣的讀者可自行參考數位邏輯的參考書.

1.3 邏輯等價

定義 1.3.1 設 $P = P(P_1, \ldots, P_n)$ 爲一命題公式. 若在任何指派 (即代入特定的命題) 之下, 命題 P 的眞值均爲 1, 則稱命題公式 P 爲**重言式**或**恆眞言**. 若在任何指派 (即代入特定的命題) 之下, 命題 P 的眞值均爲 0, 則稱命題公式 P 爲**矛盾式**或**恆假言**.

定理 1.3.2 如下命題公式均爲重言式:

(1) $P \vee \neg P$;

(2) $(P \vee Q) \leftrightarrow (\neg P \to Q)$;

(3) $(\neg(P \to Q)) \leftrightarrow (P \wedge \neg Q)$;

(4) $(\neg(P \vee Q)) \leftrightarrow (\neg P \wedge \neg Q)$ (狄摩根律);

(5) $(\neg(P \wedge Q)) \leftrightarrow (\neg P \vee \neg Q)$ (狄摩根律);

(6) $(\neg(\neg P)) \leftrightarrow P$ (雙否定律).

證明 僅證明 (3), 餘者請讀者自行給出證明.

P	Q	$\neg Q$	$P \to Q$	$\neg(P \to Q)$	$P \wedge \neg Q$	$(\neg(P \to Q)) \leftrightarrow (P \wedge \neg Q)$
0	0	1	1	0	0	1
0	1	0	1	0	0	1
1	0	1	0	1	1	1
1	1	0	1	0	0	1

由上述眞值表可知, 不論 P 和 Q 的眞值爲何, $(\neg(P \to Q)) \leftrightarrow (P \wedge \neg Q)$ 的眞值恆爲 1, 即爲重言式. □

定理 1.3.3 如下命題公式均爲重言式:

(1) $(P \leftrightarrow Q) \to (Q \leftrightarrow P)$;

(2) $(P \leftrightarrow Q) \leftrightarrow (\neg P \leftrightarrow \neg Q)$;

(3) $(\neg P \to (Q \wedge \neg Q)) \to P$;

(4) $(P \leftrightarrow Q) \to ((R \wedge P) \leftrightarrow (R \wedge Q))$;

(5) $(P \leftrightarrow Q) \to ((R \vee P) \leftrightarrow (R \vee Q))$.

證明 留給讀者自行檢驗. □

定理 1.3.4 如下命題公式均爲重言式:

(1) $((P \to Q) \wedge (Q \to R)) \to (P \to R)$ (遞移律);

(2) $((P \leftrightarrow Q) \wedge (Q \leftrightarrow R)) \to (P \leftrightarrow R)$ (遞移律);

(3) $(P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R))$ (分配律);

(4) $(P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R))$ (分配律);

(5) $(P \vee (Q \vee R)) \leftrightarrow ((P \vee Q) \vee R)$ (分配律);

(6) $(P \wedge (Q \wedge R)) \leftrightarrow ((P \wedge Q) \wedge R)$ (分配律).

證明 請讀者自行驗證. □

定理 1.3.5 如下命題公式均爲矛盾式:

(1) $P \wedge \neg P$;

(2) $(P \to Q) \wedge (P \wedge \neg Q)$;

(3) $((P \vee Q) \wedge \neg P) \wedge \neg Q$;

(4) $(P \wedge Q) \wedge \neg P$.

證明 僅證明 (2), 餘者留給讀者作爲練習.

P	Q	$\neg Q$	$P \to Q$	$P \wedge \neg Q$	$(P \to Q) \wedge (P \wedge \neg Q)$
0	0	1	1	0	0
0	1	0	1	0	0
1	0	1	0	1	0
1	1	0	1	0	0

由上述眞值表可知, 不論 P 和 Q 的眞值爲何, $(P \to Q) \wedge (P \wedge \neg Q)$ 的眞值恆爲 0, 即爲矛盾式. □

定義 1.3.6 若兩命題公式 $P(P_1, \ldots, P_n)$ 和 $Q(P_1, \ldots, P_n)$ 的眞值恆對應相等, 則稱它們**邏輯等價**, 記作

$$P(P_1, \ldots, P_n) \equiv Q(P_1, \ldots, P_n) \quad 或 \quad P(P_1, \ldots, P_n) \iff Q(P_1, \ldots, P_n).$$

命題 1.3.7 上述定義中的「$\Leftrightarrow$」是「等價關係」, 即

(1) 對於一切命題公式 P, 有 $P \Leftrightarrow P$ (自反性);

(2) 若 $P \Leftrightarrow Q$, 則 $Q \Leftrightarrow P$ (對稱性);

(3) 若 $P \Leftrightarrow Q$ 且 $Q \Leftrightarrow R$, 則 $P \Leftrightarrow R$ (傳遞性).

命題 1.3.8 $P \Leftrightarrow Q$ 成立的充要條件爲命題公式 $P \leftrightarrow Q$ 是重言式.

命題 1.3.9 若命題 P 和 Q 同爲重言式或同爲矛盾式, 則 $P \Leftrightarrow Q$.

命題 1.3.10 若 $P(P_1, \ldots, P_n) \Leftrightarrow Q(P_1, \ldots, P_n)$, 其中 $P_1, \ldots, P_n$ 是命題變數, 則對任何特定的命題 $Q_1, \ldots, Q_n$, 有 $P(Q_1, \ldots, Q_n) \Leftrightarrow Q(Q_1, \ldots, Q_n)$.

定理 1.3.11 $P \to Q \Leftrightarrow \neg Q \to \neg P$.

證明 見註記 1.2.24. □

例 1.3.12 若以命題 P 表示「在 $\triangle ABC$ 中, $|\overline{AB}| = |\overline{AC}|$」, 以命題 Q 表示「在 $\triangle ABC$ 中, $\angle B = \angle C$」, 則 $P \Leftrightarrow Q$.

定理 1.3.13 設 P 和 Q 爲兩命題公式, 則如下三個條件等價:

(1) $P \to Q$ 爲重言式;

(2) $\neg P \vee Q$ 爲重言式;

(3) $P \wedge \neg Q$ 爲矛盾式.

證明 見定理 1.3.2 之 (2) 和 (3). □

註記 1.3.14 上述定理經常用於對假言的否定.

定義 1.3.15 設 P 和 Q 爲兩命題公式, 若 $P \to Q$ 爲重言式, 則稱 P **邏輯地蘊含** Q, 記作 $P \Rightarrow Q$. 當 $P \Rightarrow Q$ 成立時, 稱 P 爲 Q 的**充分條件**, Q 爲 P 的**必要條件**.

命題 1.3.16 上述定義中的「$\Rightarrow$」滿足:

(1) 對於一切命題公式 P, 有 $P \Rightarrow P$ (自反性);

(2) 若 $P \Rightarrow Q$ 且 $Q \Rightarrow P$, 則 $P \Leftrightarrow Q$ (反對稱性);

(3) 若 $P \Rightarrow Q$ 且 $Q \Rightarrow R$, 則 $P \Rightarrow R$ (傳遞性).

包括此命題及接下來幾道命題, 只需要依「$P \Rightarrow Q$」的定義列出眞值表檢驗 $P \to Q$ 爲重言式即可, 故此部分的證明都給讀者留作練習.

註記 1.3.17 由上述命題的 (2), 當 Q 既是 P 的必要條件, 也是 P 的充分條件時, 稱 Q 和 P 互爲**充分必要條件**, 簡稱**充要條件**.

命題 1.3.18 若 $P(P_1, \ldots, P_n) \Rightarrow Q(P_1, \ldots, P_n)$, 其中 $P_1, \ldots, P_n$ 是命題變數, 則對任意特定的命題 $Q_1, \ldots, Q_n$, 有 $P(Q_1, \ldots, Q_n) \Rightarrow Q(Q_1, \ldots, Q_n)$.

命題 1.3.19 設 P 和 Q 爲兩命題公式, 則

(1) $P \Rightarrow P \vee Q$, $Q \Rightarrow P \vee Q$;

(2) $P \wedge Q \Rightarrow P$, $P \wedge Q \Rightarrow Q$;

(3) $P \wedge Q \Rightarrow P \vee Q$.

注意 1.3.20 許多數學推導步驟都有「若且唯若」的意涵, 比如在解多項式方程式時,

$$x^2 + 4x + 4 = 0 \iff (x+2)^2 = 0 \iff x = -2,$$

這保證了最終答案能夠滿足原方程式. 一般上在解方程式的過程中, 常省略「$\Leftrightarrow$」.

注意 1.3.21 在解無理方程式時, 比如說:

$$\sqrt{x} = x - 2 \implies x = (x-2)^2 \iff x^2 - 5x + 4 = 0 \iff (x-4)(x-1) = 0 \iff x = 1 \text{ 或 } x = 4.$$

其中, 可由 $\sqrt{x} = x - 2$ 推得 $x = (x-2)^2$, 但卻不能由 $x = (x-2)^2$ 推得 $\sqrt{x} = x - 2$. 因此, 無法保證最終的解都能滿足原方程式, 故才需要檢驗. 這也是產生增根的原因.

雖然此處未介紹集合和映射的概念, 但這裡稍微說明一下: 「 $\Rightarrow$ 」的動作「 相當於 」集合的包含關係, $P \Rightarrow Q$ 即 $\{x : P(x)\} \subseteq \{x : Q(x)\}$, 而 $\{x : P(x)\}$「 相當於 」函數的定義域. 當 Q 無法回推 P 時, 意味著 $\{x : P(x)\} \subsetneq \{x : Q(x)\}$, 看起來就像是「 定義域被擴大 」(因而產生增根), 這表示解方程時得到的 x 可能落在 $\{x : Q(x)\} \setminus \{x : P(x)\}$ 中.

同理, 解方程時也有可能產生遺根, 原理與增根的成因相似, 只是蘊含方向相反而已, 也可以理解成「 定義域縮小 」導致原方程的根被排除在外. 比如說, 在不確定方程兩邊某含未知數的因子是否不爲零時擅自約分消去就有可能產生遺根; 或者在解三角方程式時, 比如說解 $\sin x - \cos x = 1$, 通常使用三角疊合, 但如果選擇用萬能公式 (即正切半角代換, $t = \tan \frac{x}{2}$), 也可能會產生遺根, 因爲正切函數的定義域嚴格包含於正弦函數及餘弦函數的定義域中, 方程的解就有可能落在 $\tan \frac{x}{2}$ 的定義域外. 如果堅持要使用萬能公式將超越方程轉化爲代數方程求解, 應特別討論 $x/2$ 爲 $\pi/2$ 的奇數倍的情形是否滿足原方程.

1.4 邏輯量詞

例 1.4.1 考慮如下兩命題:

- P: 任何實數的平方都不小於 0.
- Q: 對所有的實數 x, 都有 $3x + 1 > x$.

命題 P 中有一個量詞「 任何 」, 稱之爲**全稱量詞**, 以符號「 $\forall$ 」表示. 命題 P 可以寫成「 $\forall\, x \in \mathbb{R}, x^2$ 不小於 0 」(將在第 2 章中說明「 $\in$、$\mathbb{R}$ 」等符號的意義.), 或完全以數學符號表示, 即「 $\forall\, x \in \mathbb{R}, x^2 \geq 0$ 」(因爲 x^2 不小於 0 即 $x^2 < 0$ 的否命題). 顯然命題 P 爲眞.

命題 Q 中的「 對所有的 」亦爲全稱量詞, 可把命題 Q 寫成「 $\forall\, x \in \mathbb{R}, 3x + 1 > x$ 」. 如果考慮實數 $x = -1$, 那麼 $3x + 1 > x$ 便不成立, 從而命題 Q 爲假.

其他全稱量詞還有「 對一切 」、「 每個 」、「 對任意 」等.

例 1.4.2 考慮如下兩命題:

- R: 有的整數不是 1 的倍數.
- S: 存在質量數超過 40 的元素.

命題 R 中有一個量詞「 有的 」, 稱之爲**存在量詞**, 以符號「 $\exists$ 」表示. 命題 R 可以寫成「 $\exists\, n \in \mathbb{Z}, n$ 不是 1 的倍數 」, 或完全以數學符號表示, 即「 $\exists\, n \in \mathbb{Z}, 1 \nmid n$ 」(因爲 n 不是 1 的倍數即 1 不是 n 的因數). 顯然命題 R 爲假.

命題 S 中的「 存在 」也是存在量詞. 由於可找到滿足該條件的元素 (如鈧, 其相對原子質量大約爲 45), 因此命題 S 爲眞.

例 1.4.3 考慮命題 P: 所有人都會飛.

若 P 是假命題, 則表示「 不是所有人都會飛 」, 亦即「 有的人不會飛 」, 因此 P 的否命題 $\neg P$ 爲「 有的人不會飛 」.

再考慮命題 Q: 有的人不會閃身步.

若 Q 是假命題, 則表示「 沒有人不會閃身步 」, 亦即「 所有人都會閃身步 」, 因此 Q 的否命題 $\neg Q$ 爲「 所有人都會閃身步 」.

註記 1.4.4 由上述例子, 可知若 $P(x)$ 是命題函數, 且命題 Q 表示 $\forall\, x, P(x)$, 則命題 Q 的否定爲 $\exists\, x, \neg P(x)$, 即

$$\neg\, [\forall\, x, P(x)] \iff \exists\, x, \neg P(x);$$

若命題 Q 表示 $\exists\, x, P(x)$, 則命題 Q 的否定爲 $\forall\, x, \neg P(x)$, 即

$$\neg [\exists\, x, P(x)] \iff \forall\, x, \neg P(x).$$

註記 1.4.5 有時會聽到「對的請證明, 錯的舉反例」, 其實這句話不完全精確. 常常在習題或考試時, 題目都會給一個「全稱命題」, 要求判斷眞僞並提出論證. 比如說, 問「對於所有四邊形, 只要對角線互相平分, 該四邊形必爲菱形」是否正確, 如果認爲是僞命題, 那麼只要給出「一個」對角線互相平分但不爲菱形的四邊形 (如相鄰兩邊不等長的平行四邊形) 即可, 這是在舉反例. 其實我們在做的事情是: 爲了說明原命題 P 是僞命題 (即原命題不成立), 我們可以找一個矛盾式 (通常都考慮 $P \wedge \neg P$), 只要說明 $\neg P$ 是眞命題, 那麼根據「P 和 $\neg P$ 不可能同時成立」的邏輯, 便可說明 P 不成立. 此時, 由於 P 是全稱命題, $\neg P$ 就是存在命題, 因此爲了證明 $\neg P$ 是眞命題, 就要說明「存在性」, 而說明「存在性」最直接的方法就是給出一個例子. 這就是人們常說的「錯的舉反例」背後的數學邏輯. 事實上, 若能用其他定理來保證反例的存在性, 則當然可以不用具體構造反例就能說明原命題爲假.

如果原命題是存在命題, 且認爲原命題爲假, 那麼「錯的舉反例」就不再正確, 因爲此時的否命題是全稱命題, 不宜用特定例子來以偏概全, 而需要抽象地論證.

注意 1.4.6 當遇到連續兩個相異的邏輯量詞時, 不可隨意對調其順序, 即 $\forall\, x, \exists\, y, P(x,y)$ 未必等價於 $\exists\, y, \forall\, x, P(x,y)$. 例如, 考慮實數 x, y 與命題 $P(x,y) : x + y = 0$. 「$\forall\, x, \exists\, y, P(x,y)$」爲眞 (對於任意實數 x, 皆可取 $y = -x$); 但「$\exists\, y, \forall\, x, P(x,y)$」爲假 (不存在一個固定的 y, 能夠與所有實數相加皆爲 0).

命題 1.4.7 以下命題爲重言式:

(1) $\big[\forall\, x, [P(x) \wedge Q(x)]\big] \leftrightarrow \big[[\forall\, x, P(x)] \wedge [\forall\, x, Q(x)]\big]$;

(2) $\big[\exists\, x, [P(x) \vee Q(x)]\big] \leftrightarrow \big[[\exists\, x, P(x)] \vee [\exists\, x, Q(x)]\big]$;

(3) $\big[[\forall\, x, P(x)] \vee [\forall\, x, Q(x)]\big] \rightarrow \big[\forall\, x, [P(x) \vee Q(x)]\big]$;

(4) $\big[\exists\, x, [P(x) \wedge Q(x)]\big] \rightarrow \big[[\exists\, x, P(x)] \wedge [\exists\, x, Q(x)]\big]$.

證明 (1) 設 $\forall\, x, [P(x) \wedge Q(x)]$ 爲眞, 則對於論域中 (即所討論的 x 可取值的範圍) 的任意元素 c, $P(c) \wedge Q(c)$ 都成立. 既然 $P(c) \wedge Q(c)$ 爲眞, 於是 $P(c)$ 爲眞, 且 $Q(c)$ 也爲眞. 因爲 c 是任意選取的, 所以可得「對所有 x, $P(x)$ 爲眞」且「對所有 x, $Q(x)$ 爲眞」. 因此, $[\forall\, x, P(x)] \wedge [\forall\, x, Q(x)]$ 爲眞.

反之, 設 $[\forall\, x, P(x)] \wedge [\forall\, x, Q(x)]$ 爲眞, 則 $\forall\, x, P(x)$ 爲眞, 且 $\forall\, x, Q(x)$ 也爲眞. 對於論域中的任意元素 c, 由前半部分可知 $P(c)$ 爲眞, 由後半部分可知 $Q(c)$ 爲眞. 因此, $P(c) \wedge Q(c)$ 必然爲眞. 因爲 c 是任取的, 所以 $\forall\, x, [P(x) \wedge Q(x)]$ 爲眞.

餘者的證明與 (1) 類似, 請讀者自行給出. □

注意 1.4.8 全稱量詞對析取連結詞沒有分配律, 存在量詞對合取連結詞沒有分配律.

例 1.4.9 考慮整數 x, 以 $P(x)$ 表示「x 是偶數」, $Q(x)$ 表示「x 是奇數」.

因爲的確有整數是奇數, 也有整數是偶數, 所以 $[\exists\, x, P(x)] \wedge [\exists\, x, Q(x)]$ 爲眞. 但沒有任何一個整數同時是偶數和奇數, 故 $\exists\, x, P(x) \wedge Q(x)$ 爲假. 因此, $[\exists\, x, P(x)] \wedge [\exists\, x, Q(x)]$ 並不邏輯等價於 $\exists\, x, P(x) \wedge Q(x)$.

另一方面, 因爲一個整數必爲奇數或偶數, 所以 $\forall\, x, P(x) \vee Q(x)$ 爲眞. 但不是所有整數都是奇數, 也不是所有整數都是偶數, 故 $\forall\, x, P(x)$ 及 $\forall\, x, Q(x)$ 爲假, 從而 $[\forall\, x, P(x)] \vee [\forall\, x, Q(x)]$ 爲假. 因此, $[\forall\, x, P(x)] \vee [\forall\, x, Q(x)]$ 並不邏輯等價於 $\forall\, x, P(x) \vee Q(x)$.

1.5 推理

說明 所謂**推理**, 是從一些已有的判斷 (已經確定成立的命題)$P_1, \ldots, P_n$ 去推導出一個新的命題 C 的過程. 這些已有的判斷或已經成立的命題稱爲**前提**, 新的判斷稱爲**結論**.

例 1.5.1 考慮如下命題:

- P_1: 若四邊形的各角相等, 則此四邊形爲矩形.
- P_2: 四邊形 $ABCD$ 的各角相等.

- C: $ABCD$ 是矩形.

在這種推理形式下, 若 P_1, P_2 爲眞命題, 則所得到的結論也必定爲眞. 可將上述的推理形式寫成

$$\begin{array}{lll} & P \to Q & (P_1) \\ & P & (P_2) \\ \hline \therefore & Q & (C) \end{array}$$

例 1.5.2 考慮如下前提:

- P_1: 所有大於 1 的整數或者爲質數, 或者爲合數.
- P_2: 整數 n $(n > 1)$ 不是合數.

根據前提 P_1, 可知一個大於 1 的整數必爲奇數或合數的其中一者, 且不可能同時爲兩者. 根據前提 P_2, 既然已知 n 不是合數, 那麼根據前提 P_1, 可推斷出 n 必然爲質數. 因此, 「n 爲質數」即爲推理的結論.

此例表現了推理的如下形式:

$$\begin{array}{lll} & P \vee Q & (P_1) \\ & \neg Q & (P_2) \\ \hline \therefore & P & (C) \end{array}$$

例 1.5.3 考慮如下前提:

- P_1: 如果男友聽到命令, 就會反射性地做出反應.
- P_2: 男友沒有做出反應.

結合這兩個前提, 可作結論: 男友沒有聽到命令. 因爲如果男友有聽到命令, 根據 P_1 就會做出反應, 這與 P_2 互相矛盾.

此例表現了推理的另一種形式, 即

$$\begin{array}{lll} & P \to Q & (P_1) \\ & \neg Q & (P_2) \\ \hline \therefore & \neg P & (C) \end{array}$$

注意 1.5.4 不是給定任何的前提都能作出有效的推理. 在前提都爲眞的情況下, 有效的推理才能給出眞的結論. 看看如下例子.

例 1.5.5 判斷以下的推理是否有效:

- P_1: 星期六去臺北或臺中.
- P_2: 星期六去臺北.
- C: 星期六不去臺中.

解 令 P: 星期六去臺北, Q: 星期六去臺中. 若 P, Q 皆爲眞命題, 則兩個前提

$$P_1\text{: } P \vee Q \text{ 爲眞},$$
$$P_2\text{: } P \text{ 爲眞}.$$

但是, 結論 $C : \neg Q$ 卻是僞命題 (因爲 Q 爲眞命題). 因此, 題目所給的推理無效.

註記 1.5.6 其實還可以透過眞值表來判斷推理是否有效. 以例 1.5.5 說明之:

P	Q	$P \vee Q$	$\neg Q$
0	0	0	1
0	1	1	0
1	0	1	1
1	1	1	0

其中第三、四列中, 兩個前提 $P \vee Q$ 及 P 的眞值皆爲 1, 但第四列中結論 $\neg Q$ 的眞值爲 0, 所以推理無效.

再看例 1.5.1 的有效性.

P	Q	$P \to Q$
0	0	1
0	1	1
1	0	0
1	1	1

其中第四列中, 兩個前提 $P \to Q$ 和 P 都爲眞, 此時結論 Q 也爲眞, 所以這個推理有效.

例 1.5.7 (三段論定律) 檢驗 $P_1 : P \to Q$, $P_2 : Q \to R$; $C : P \to R$ 的有效性.

證明 觀察如下眞值表:

P	Q	R	$P \to Q$	$Q \to R$	$P \to R$
0	0	0	1	1	1
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	1	1	1
1	0	0	0	1	0
1	0	1	0	1	1
1	1	0	1	0	0
1	1	1	1	1	1

其中第一、二、四、八列中, 兩個前提 $P \to Q$ 和 $Q \to R$ 爲眞, 此時結論 $P \to R$ 也爲眞, 所以這個推理有效. □

註記 1.5.8 對於上述例子, 也可以檢驗「 $[(P \to Q) \wedge (Q \to R)] \to (P \to R)$ 」是重言式 (即 $(P \to Q) \wedge (Q \to R) \implies P \to R$) 來說明推理的有效性.

注意 1.5.9 看看如下例子:

- P_1: 如果人有翅膀, 那麼人會飛.
- P_2: 人有翅膀.
- C: 人會飛.

其推理形式是: $P \to Q, P; \therefore Q$, 是有效推理, 但其前提「 人有翅膀 」和結論「 人會飛 」都是錯的. 由此可見, 有效推理並不能保證結論爲眞. 能保證結論爲眞的推理必須具備兩個條件:

(1) 它是有效推理, 即推理的前提和結論間的關係符合邏輯規則;

(2) 它的前提都爲眞.

考慮到前提的眞實性需要靠其他學科解決, 因而傳統的邏輯和現代的邏輯都把自己限於研究推理的有效性.

1.6 基本的證明方法

說明 大致上在數學中, 想要證明的命題常爲假言 (或等價), 即證明「若 P, 則 Q」. 根據先前的討論, 若 P 爲假命題, 則 $P \to Q$ 自動爲眞命題, 所以眞正待證明的部分是「若 P 爲眞, 則 Q 爲眞」.

基於先前的小節的論述, 原則上可經由如下幾種基本方法來達成論證的目的.

(1) 直接證明法: 如果認爲「$P \to Q$」爲眞, 那麼可假設 P 成立, 經由一番有效的邏輯論證, 直接推得結論 Q.

(2) 逆否命題法: 如果認爲「$P \to Q$」爲眞, 那麼可假設 $\neg Q$ 成立, 經由一番有效的邏輯論證, 推得結論 $\neg P$, 由此可知「$\neg Q \to \neg P$」成立, 間接說明了「$P \to Q$」成立.

(3) 矛盾法: 如果認爲給定命題爲眞, 那麼可假設原命題爲假 (比如如果認爲 $P \to Q$ 爲眞, 那麼可假設 $P \to Q$ 爲假, 即 $P \wedge \neg Q$ 爲眞), 經由一番有效的邏輯論證, 得到一個矛盾式 $R \wedge \neg R$.

(4) 舉反例法: 基於全稱量詞的否定, 比如

$$\neg(\forall\, x, [P(x) \to Q(x)]) \iff \exists\, x, \neg[P(x) \to Q(x)] \iff \exists\, x, P(x) \wedge \neg Q(x),$$

那麼可給出滿足 $P(x)$ 但不滿足 $Q(x)$ 的例子來說明 $\forall\, x, [P(x) \to Q(x)]$ 不成立.

例 1.6.1 (直接證明法) 已知當 $a > 0$ 時, 對於 $b > 1$, 有 $b^a > 1$. 設 x, y 均爲實數, 證明: 若 $x < y$, 則 $2^x < 2^y$.

證明 因 $x < y$, 故存在滿足 $y = x + a$ 的正實數 a. 於是,

$$2^y = 2^{x+a} = 2^a \cdot 2^x.$$

又由 $a > 0$ 可得 $2^a > 1$, 故 $2^y > 2^x$, 即 $2^x < 2^y$. □

例 1.6.2 (逆否命題法) 設 a, b, x, y 均爲實數, 其中 $a \neq 0$, 證明: 若 $x \neq y$, 則 $ax + b \neq ay + b$.

證明 設 $ax + b = ay + b$, 依等量公理, 等式兩邊減去 b 再同除以 a, 可得 $a = b$. 也就是說「$(ax + b = ay + b) \to (x = y)$」成立, 於是其原命題「$(x \neq y) \to (ax + b \neq ay + b)$」成立. □

例 1.6.3 (矛盾法) 證明 $\sqrt{2}$ 不是有理數.

證明 設 $\sqrt{2}$ 是有理數, 則存在兩互質的正整數 p, q, 使得 $\sqrt{2} = p/q$. 兩邊同乘以 q 並取平方, 得 $2q^2 = p^2$. 於是, p^2 是偶數, 即存在滿足 $p = 2k$ 的正整數 k, 此時 $2q^2 = (2k)^2$, 即 $q^2 = 2k^2$, 從而 q 也是偶數. 但如此一來, p 和 q 至少有公因數 2, 這使得 p, q 不互質, 與假設矛盾. 因此, $\sqrt{2}$ 不是有理數. □

例 1.6.4 (矛盾法) 證明有無窮多個除以 4 餘 3 的質數.

證明 假設只有有限多個除以 4 餘 3 的質數, 不妨設爲 $p_1, \ldots, p_k$. 令 $L = 2p_1 \cdots p_k + 1$, 則

$$L \equiv 2 \cdot 3^k + 1 \equiv 2 \cdot (-1)^k + 1 \equiv 3 \pmod 4.$$

若 L 是質數, 則 L 是除以 4 餘 3 且異於先前假設的 $p_1, \ldots, p_k$ 的質數, 矛盾. 若 L 是合數, 則可將 L 作因數分解, 即 $L = q_1 \cdots q_\ell$, 其中各 q_i 皆爲奇質數. 若一切 q_i 除以 4 都餘 1, 則 $L \equiv 1^\ell \equiv 1 \pmod 4$, 與 $L \equiv 3 \pmod 4$ 矛盾. 所以, 至少有一個除以 4 餘 3 的 q_i, 不妨設之爲 q_1, 於是 q_1 必爲 $p_1, \ldots, p_k$ 之中的一者, 不妨設 $q_1 = p_1$, 從而

$$p_1 q_2 \cdots q_\ell = L = 2p_1 p_2 \cdots p_k + 1 \implies 0 \equiv 1 \pmod{p_1},$$

這也是一個矛盾.

因此, 必有無窮多個除以 4 餘 3 的質數. □

例 1.6.5 (舉反例) 給定實數 x, y, 證僞: 若 x 爲有理數, 而 y 爲無理數, 則 xy 亦爲無理數.

證明 要說明命題

$$\forall\, x, \forall\, y, [(x \text{ 爲有理數} \wedge y \text{ 爲無理數}) \to xy \text{ 爲無理數}]$$

爲假, 可說明命題

$$\exists\, x, \exists\, y, [(x \text{ 爲有理數} \wedge y \text{ 爲無理數}) \wedge xy \text{ 不爲無理數}]$$

爲眞. 取 $x = 0$ (有理數), $y = \sqrt{2}$ (無理數), 則 $xy = 0$ 不爲無理數. □

例 1.6.6 (*存在性的證明——直接構造法*) 若整數 m, n 均可表成四個平方數之和, 則 mn 亦可表成四個平方數之和.

證明 設 $m = a^2 + b^2 + c^2 + d^2$, $n = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$, 其中 $a, b, c, d, \alpha, \beta, \gamma, \delta$ 皆爲整數, 則不難注意到

$$\begin{aligned} &a\alpha + b\beta + c\gamma + d\delta, \quad a\beta - \alpha b + c\delta - \gamma d, \\ &a\gamma - \alpha c - b\delta + d\beta, \quad a\delta - d\alpha + b\gamma - c\beta \end{aligned}$$

皆爲整數, 並且

$$\begin{aligned} mn = (a\alpha + b\beta + c\gamma + d\delta)^2 + (a\beta - \alpha b + c\delta - \gamma d)^2 \\ + (a\gamma - \alpha c - b\delta + d\beta)^2 + (a\delta - d\alpha + b\gamma - c\beta)^2. \end{aligned}$$

此過程的構造極其顯而易見. (這條華麗的等式稱爲**歐拉四平方和恆等式**. 雖然直接展開就能驗證其正確性, 但它的構造對初學者而言通常一點都不「顯而易見」, 其背後蘊含著四元數的優美代數結構.) □

單元 2

集合的基本概念

2.1 集合的公理

一般來說, 數學是一門建立在邏輯學上的形式科學, 其與自然科學的不同點在於: 數學最多允許使用演繹推理, 而自然科學則允許使用演繹及歸納推理. 演繹推理是透過正確的前提來推得正確的結果的過程, 而依照演繹推理, 正確的前提亦爲其他正確的前提所推理而來, 這樣便會沒有盡頭、沒完沒了. 於是, 人們很自然會希望如此的演繹過程有個起點. 那麼, 人們就設定了某些前提, 使這些前提不需要其他前提來支撐, 亦即, 大家預設這些前提是正確、不證自明的, 這些前提稱爲**公理**.

一切公理體系中總會從一些「未定義概念」開始. 比如在幾何學中, 所謂的「點」和「直線」一般上沒有具體的定義, 但儘管在腦海中可以自由地爲這些概念賦予某種具象化的「意義」, 在數學處理上, 必須表現得像是「完全不知道它們代表什麼」一樣. 一個「未定義概念」除了被明確賦予的性質之外, 不具備任何其他屬性; 因此, 必須將所期望這些未定義概念所具有的所有基本性質, 全數以公理的形式描述出來.

公理化集合論系統僅僅建立在兩個未定義概念之上:「類」以及「屬於關係『$\in$』」. 在這套理論中, 所有的探討對象都被稱爲**類**. 爲了避免產生邏輯上的悖論, 必須區分兩種不同的類: 一種稱爲**集合**, 另一種則稱爲**眞類**. 關於這兩者的區別, 暫且按下不表, 稍後會再深入探討. 不過, 在接下來的公理建構與絕大多數的數學討論中, 本文將把焦點放在「集合」上.

若 x 與 A 皆爲探討的對象, 則表達式 $x \in A$ 讀作「x 是 A 的**元素**」, 或是「x 屬於 A」. 爲了方便起見, 通常將「x 不屬於 A」記作 $x \notin A$.

註記 2.1.1 在這樣的公理化系統中, 屬於關係必須具有**確定性**: 對於任意的 x 與 A, 命題「$x \in A$」或者爲眞, 或者爲假, 兩者必居其一且絕無模稜兩可的空間. 這是後續利用性質或邏輯語句來建構新集合的基石.

定義 2.1.2 設 x 爲一個探討的對象. 若 x 是某個類 (或集合)A 的元素, 則稱 x 爲一**集合**. 若 x 不爲任合類的元素, 則稱 x 爲一**眞類**.

作爲一套以集合爲核心的公理化系統, 本文仰賴十條公理來規範集合的行爲與性質. 下文將先逐條說明, 再進行統整.

公理 2.1.3 (外延公理) 兩個集合 X, Y 相同 (記作 $X = Y$) 的充要條件爲它們具有完全相同的元素, 即

$$\forall\, X, \forall\, Y, [X = Y \iff \forall\, z, (z \in X \leftrightarrow z \in Y)].$$

公理 2.1.4 (空集公理) 沒有任何元素的集合 (稱爲**空集**) 存在, 即 $\exists\, A, \forall\, x, x \notin A$.

命題 2.1.5 空集是唯一的.

證明 假如 A 和 B 都是空集. 任予 x, 依空集的定義, 必有 $x \notin A$. 於是, 依假言的定義 (定義 1.2.15), 命題 $x \in A \to x \in B$ 爲眞. 同理, 命題 $x \in B \to x \in A$ 亦爲眞. 因此,

$$\forall\, x, [x \in A \leftrightarrow x \in B]$$

成立. 依外延公理, 有 $A = B$, 即此二空集相同. 既然任兩個空集均相同, 這迫使空集是唯一的. □

註記 2.1.6 既然空集是唯一的, 那麼就賦予其專屬符號, 以 $\varnothing$ 恆 $\{\}$ 表示空集.

公理 2.1.7 (分離公理) 給定任意集合 A 與任意性質 P, 皆存在一個集合 B, 使得對所有 x 而言, $x \in B$ 的充要條件爲 $x \in A$ 且 x 滿足性質 P, 即

$$\forall\, A, \forall\, P, \exists\, B, \forall\, x, [x \in B \iff (x \in A) \land P(x)].$$

註記 2.1.8 如同空集, 依外延公理, 對於給定的集合 A 與性質 P, 滿足上述條件的集合 B 必定是唯一的. 事實上, 給定集合 A 與性質 P, 假設有兩個集合 B 與 C 皆滿足上述條件, 則對於任意 x, 有

$$x \in B \iff (x \in A \land P(x)) \iff x \in C.$$

這意味著對於任意 x, $x \in B \Leftrightarrow x \in C$ 皆成立. 依外延公理, 必有 $B = C$, 即如此分離出來的集合是唯一的. 於是, 同樣可賦予其專屬記號, 將此集合 B 記作

$$\{x \in A \mid P(x)\} \quad 或 \quad \{x \in A : P(x)\}.$$

分離公理的核心精神在於: 不能毫無限制地用任意性質來宣告一個集合的存在, 而是必須立基於一個「已經存在的集合 A」, 再藉由性質 $P(x)$ 將 A 中符合條件的元素「分離」出來構成新的集合. 這個限制有效避免了早期素樸集合論中的「羅素悖論」.

公理 2.1.9 (配對公理/無序對公理) 對於任兩個元素, 都存在同時僅僅包含它們的集合, 即

$$\forall\, x, \forall\, y, \exists\, Z, \forall\, a, [a \in Z \iff a = x \lor a = y].$$

註記 2.1.10 同理可證, 此僅包含 x 和 y 的集合是唯一的, 故可記作 $\{x, y\}$, 稱爲 x 和 y 的**雙元集**. 特別地, 將 x 和 x 的雙元集稱爲 x 的**單元集**, 記作 $\{x\}$.

藉由邏輯連結詞的性質, 可觀察到集合的兩大基本特徵:

(1) **無序性**: 由於「$\lor$」具有交換性 ($a = x \lor a = y \Leftrightarrow a = y \lor a = x$), 依外延公理可知 $\{x, y\} = \{y, x\}$. 這表示集合內的元素沒有順序之分.

(2) **互異性**: 由於「$\lor$」具有冪等性 ($a = x \lor a = x \Leftrightarrow a = x$), 依外延公理可知 $\{x, x\} = \{x\}$. 這表示集合內的元素不計重複, 相同的元素在集合中只算作一個.

定義 2.1.11 設 A 與 X 爲集合. 若 X 的所有元素皆爲 A 的元素, 即

$$\forall\, y, [y \in X \to y \in A],$$

則稱 X 爲 A 的**子集**, A 爲 X 的**父集**, 記作 $X \subseteq A$ 或 $A \supseteq X$, 讀作 X **包含**於 A, 或 A 包含 X. 若在此之上, 還有 $A \neq X$, 則可記 $A \subsetneq X$ 或 $A \supsetneq X$, 稱 X 爲 A 的**眞子集**, 讀作 X **眞包含**於 A, 或 A 眞包含 X.

命題 2.1.12 空集 $\varnothing$ 是任合集合的一個子集.

證明 給定集合 A. 若 $x \notin A$, 則因 $\varnothing$ 不含任何元素, 故 $x \notin \varnothing$. 依邏輯性質「$(P \to Q) \leftrightarrow (\neg Q \to \neg P)$ 是重言式」, 即得 $\varnothing \subseteq A$. □

公理 2.1.13 (冪集公理) 對於任意集合 A, 皆存在一個集合 P, 其元素恰好爲 A 的所有子集, 即

$$\forall\, A, \exists\, P, \forall\, X, [X \in P \iff X \subseteq A],$$

將子集的定義展開, 即爲

$$\forall\, A, \exists\, P, \forall\, X, \big[X \in P \iff [\forall\, y, (y \in X \to y \in A)]\big].$$

註記 2.1.14 同理可證, 依據外延公理, 對於給定的集合 A, 其所有子集所構成的集合 P 是唯一的, 故將此唯一的集合稱爲 A 的**冪集**, 並賦予其專屬記號, 記作 $\mathcal{P}(A)$ 或 2^A. 以後會說明 2^A 的另一個含義 (見註記 3.3.10).

例 2.1.15 設 $A=\{x,y\}$, 則 $\mathcal{P}(A)=\{\varnothing,\{x\},\{y\},\{x,y\}\}$.

公理 2.1.16 (聯集公理) 對於任意集合 A, 皆存在一個集合 U, 其元素恰好爲 A 中所有元素的元素, 即

$$\forall A,\exists U,\forall x,\big[x\in U \iff \exists Y,[Y\in A\wedge x\in Y]\big].$$

註記 2.1.17 同理可證, 依外延公理, 對於給定的集合 A, 滿足上述條件的集合 U 是唯一的, 故將此唯一的集合稱爲 A 的**聯集**或**並集**, 有時也簡稱**聯**或**並**, 並賦予其專屬記號, 記作 $\bigcup A$.

特別地, 當 A 爲一個配對集合 $\{X,Y\}$ 時, 其聯集 $\bigcup\{X,Y\}$, 即包含了 X 與 Y 中所有元素的集合, 通常將此情形簡記作 $X\cup Y$.

註記 2.1.18 讀者可能會好奇, 既然有聯集公理, 那是否也需要一條「交集公理」? 事實上是不需要的. 藉由剛剛介紹的分離公理, 就能保證交集的存在性.

給定兩個集合 X 與 Y, 可將 X 視爲分離公理中的「母集合」, 並將性質 $P(x)$ 設爲「$x\in Y$」. 藉由分離公理, 可直接建構出一個新集合, 稱爲 X 與 Y 的**交集**, 或簡稱**交**, 記作 $X\cap Y$, 即

$$X\cap Y=\{x\in X:x\in Y\}.$$

定義 2.1.19 更一般地, 給定一個**非空**集合 A, 可以定義 A 中所有元素的**交集**, 記作 $\bigcap A$.

因 A 是非空的, 故可取定 A 的某個元素 E(即 $E\in A$). 接著以 E 爲母集合, 利用分離公理將「同時屬於 A 中所有集合」的元素分離出來:

$$\bigcap A=\{x\in E:\forall Y,(Y\in A\to x\in Y)\}.$$

註記 2.1.20 在上述一般交集的定義中, 必須特別強調 A 爲「非空集合」. 若 $A=\varnothing$, 則條件 $Y\in A\to x\in Y$ 對於所有 x 皆爲「空洞的眞理」(即**虛眞命題**). 如此一來, 「$\bigcap\varnothing$」將會包含宇宙中所有的對象, 形成一個「包含所有集合的集合」, 這將引發羅素悖論. 因此, 在標準集合論中 $\bigcap\varnothing$ 是無意義的 (或說它是一個眞類, 而不是集合).

定義 2.1.21 給定任意集合 x, 定義 x 的**後繼**爲 $x\cup\{x\}$, 暫時將其簡記爲 x^+.

公理 2.1.22 (無窮公理) 存在一個集合 A, 其包含空集 $\varnothing$ 作爲元素, 且對於 A 中的任意元素 x, x 的後繼 x^+ 亦爲 A 的元素, 即

$$\exists A,\big[\varnothing\in A\wedge\forall x(x\in A\to x\cup\{x\}\in A)\big].$$

註記 2.1.23 滿足無窮公理條件 (即包含空集, 且對「取後繼」的操作封閉) 的集合, 稱爲**歸納集**. 因此, 無窮公理的本質也就是在宣告「宇宙中至少存在一個歸納集」.

這條公理是極爲關鍵的里程碑. 藉由它, 才得以在沒有任何實體數字的集合論世界中, 「無中生有」地建構出**自然數**[1]: 若將 0 定義爲 $\varnothing$, 那麼 1 就是 $0^+=\varnothing\cup\{\varnothing\}=\{\varnothing\}$, 而 2 就是 $1^+=1\cup\{1\}=\{\varnothing,\{\varnothing\}\}$, 依此類推. 無窮公理保證了, 那個能把所有自然數都裝進去的「無窮集合」是確實存在的.

註記 2.1.24 藉由配對公理與聯集公理, 可以進一步建構出包含任意有限多個元素的集合.

例如, 給定三個對象 x,y,z, 可先利用配對公理造出雙元集 $\{x,y\}$ 與單元集 $\{z\}$, 再利用聯集公理取此二者的聯集 $\{x,y\}\cup\{z\}$. 依據外延公理, 這樣構造出來的集合是唯一的, 其元素恰好爲 x,y 與 z, 將其稱爲這三個元素的**三元集**, 記作 $\{x,y,z\}$.

依此類推, 透過反覆使用配對公理與聯集公理, 可以建構出包含四個對象的**四元集** $\{w,x,y,z\}$, 乃至於包含任意 n 個對象的集合 $\{x_1,x_2,\ldots,x_n\}$.

注意 2.1.25 在標準的「ZFC 集合論」中, 實際上還有**替代公理**及**選擇公理**. 然而, 這兩條公理的表述與應用高度牽涉到「映射」的概念. 爲了避免過早引入複雜的敍述, 本文將待後文正式定義了映射之後, 再行補上這兩條公理.

[1] 此處是爲了配合皮亞諾公理才暫時使用「自然數」這個詞, 實際上筆者更傾向於把自然數這個名稱留給**正整數**, 而非負整數則稱爲**完整數**.

公理 2.1.26 (正則公理) 每一個非空的集合 A, 都至少包含一個元素 x, 使得 x 與 A 沒有共同元素 (即交爲空集), 即

$$\forall A, \big[A \neq \varnothing \implies \exists x, (x \in A \wedge x \cap A = \varnothing)\big].$$

若不使用交集符號, 則可寫作

$$\forall A, \big[A \neq \varnothing \implies \exists x, [x \in A \wedge \forall y, \neg(y \in x \wedge y \in A)]\big].$$

註記 2.1.27 正則公理 (又稱爲**基礎公理**) 的主要目的, 是爲了將那些「病態」的集合從所討論範圍中排除.

例如, 假設存在一個集合 X 滿足 $X \in X$. 若利用配對公理造出單元素集合 $A = \{X\}$, 則這顯然是一個非空集合. 根據正則公理, A 中必須存在一個與 A 不相交的元素. 但 A 唯一的元素就是 X, 而 X 與 A 的交集 $X \cap A = X \cap \{X\} = \{X\} \neq \varnothing$(因爲前提假設了 $X \in X$). 這就違反了正則公理.

因此, 正則公理保證了「沒有任何集合可以包含自己作爲元素」($X \notin X$), 同時也排除了無窮遞降的屬於關係 ($\cdots \in x_3 \in x_2 \in x_1$), 這使得所有的集合都可以從空集開始, 透過井然有序的層次一步步建構出來.

有了上述公理, 便可定義如下集合:

定義 2.1.28 設 A, B 是兩個集合.

(1) 如定義 2.1.19, A 與 B 的**交集**爲 $A \cap B = \{x : x \in A \text{ 且 } x \in B\}$.

(2) 如公理 2.1.16, A 與 B 的**聯集**爲 $A \cup B = \{x : x \in A \text{ 或 } x \in B\}$.

(3) 若 $A \cap B = \varnothing$, 則稱 A 和 B **相離**或**互斥**.

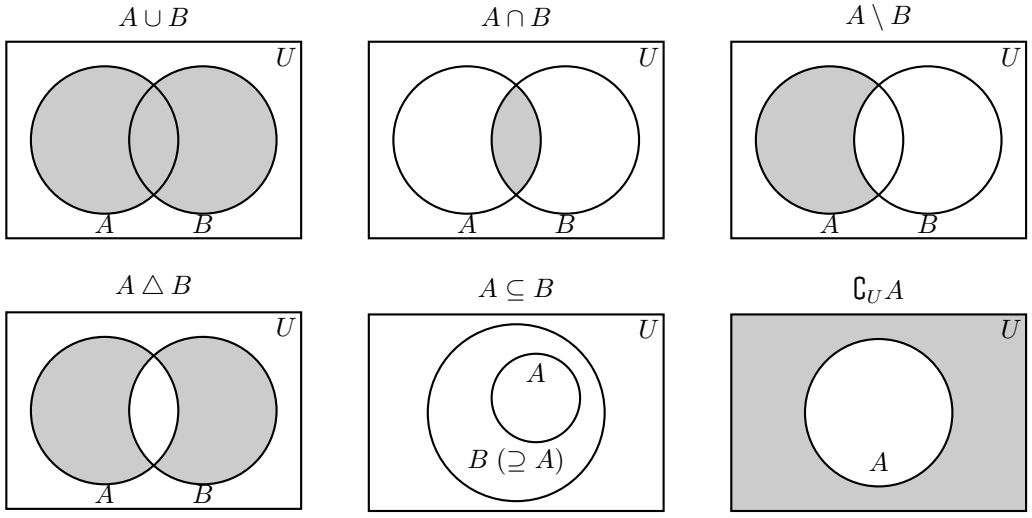
(4) 當 A, B 相離時, 它們的聯集也可記作 $A \sqcup B$, 稱爲 A 和 B 的**無交聯集**.

(5) 依分理公理, 可定義 A 與 B 的**差集**爲 $A \setminus B = \{x : x \in A \text{ 且 } x \notin B\}$.

(6) 若所討論的問題在某個集合 (稱爲**全集**, 此處記作 U) 中進行, 且 $A \subseteq U$, 則稱 $U \setminus A$ 是 A 關於 U 的**補集**或**餘集**, 記作 $\complement_U A$. 如果全集很明確, 那麼也可以將 A 的補集簡記作 $A^{\complement}$.

(7) A 和 B 的**對稱差集**爲 $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

以下用**文氏圖**來幫助直觀理解上述集合的定義:



前面已探討過集合的無序性, 即 $a, b = b, a$. 然而, 在諸多數學討論中 (例如解析幾何或映射), 元素的先後順序往往是至關重要的. 爲了在純粹的公理化集合論框架下精確刻畫「順序」的概念, 必須設法利用集合來編碼元素的先後次序. 爲此, 先給出以下關於雙元集的預備命題.

命題 2.1.29 若 $\{a,b\}=\{c,d\}$, 則

$$\begin{cases} a=c, \\ b=d, \end{cases} \quad \text{或} \quad \begin{cases} a=d, \\ b=c. \end{cases}$$

證明 a 與 b 必滿足 $a=b$ 或 $a\neq b$ 之中的一條且僅一條, 故分成此二情形討論.

(1) 情況一: 若 $a=b$, 則對於 $c\in\{c,d\}$, 因 $\{c,d\}=\{a,b\}$, 故依外延公理, 有 $c\in\{a,b\}$. 於是, $c=a$ 或 $c=b$. 無論 $c=a$ 還是 $c=b$, 均有 $c=a=b$. 同理可證 $d=a=b$, 因此 $a=b=c=d$, 即結論爲眞.

(2) 若 $a\neq b$, 則對於 $a\in\{a,b\}$, 因 $\{a,b\}=\{c,d\}$, 故 $a=c$ 或 $a=d$.

- 若 $a=c$, 則由 $b\in\{a,b\}$ 得 $b\in\{c,d\}$, 從而 $b=c$ 或 $b=d$. 但 $a=c$, 所以如果 $b=c$, 則 $a=b$, 違反設定. 於是 $b=d$, 故得結論.
- 若 $a=d$, 則由 $b\in\{a,b\}$ 得 $b\in\{c,d\}$, 從而 $b=c$ 或 $b=d$. 但 $a=d$, 所以如果 $b=d$, 則 $a=b$, 違反設定. 於是 $b=c$, 故得結論.

□

定義 2.1.30 設 a,b 爲元素, 將**序偶** (亦稱爲**有序對**或**二元組**)(a,b) 定義成集合

$$(a,b)=\{\{a\},\{a,b\}\}.$$

命題 2.1.31 $(a,b)=(c,d)$ 的充要條件爲 $a=c$ 且 $b=d$.

證明 依序偶的定義, $(a,b)=(c,d)$ 等價於

$$\{\{a\},\{a,b\}\}=\{\{c\},\{c,d\}\}.$$

將 $\{a\},\{a,b\}$ 以及 $\{c\},\{c,d\}$ 視爲元素, 依命題 2.1.29, 可得以下兩種情形:

(1) 情形一: $\{a\}=\{c\}$ 且 $\{a,b\}=\{c,d\}$. 由 $\{a\}=\{c\}$ 即得 $a=c$. 將 $a=c$ 代入 $\{a,b\}=\{c,d\}$ 可得 $\{c,b\}=\{c,d\}$. 再依命題 2.1.29, 有 $[(c=c)\wedge(b=d)]\vee[(c=d)\wedge(b=c)]$.

- 若爲前者, 則 $b=d$, 故 $a=c$ 且 $b=d$.
- 若爲後者, 則 $b=c=d$, 從而亦有 $a=c$ 且 $b=d$.

(2) 情形二: $\{a\}=\{c,d\}$ 且 $\{a,b\}=\{c\}$. 由 $\{a\}=\{c,d\}$ 可知 $c\in\{a\}$ 且 $d\in\{a\}$, 故 $c=a$ 且 $d=a$, 得到 $a=c=d$. 另一方面, 由 $\{a,b\}=\{c\}$ 可知 $a\in\{c\}$ 且 $b\in\{c\}$, 故 $a=c$ 且 $b=c$, 得到 $a=b=c$. 綜合得 $a=b=c=d$, 故在此情形下 $a=c$ 且 $b=d$ 亦成立.

綜上所述, 無論何種情形, 皆有 $a=c$ 且 $b=d$. 反之顯而易見. □

定義 2.1.32 設 A,B 爲兩集合. A 與 B 的**積集** (亦稱**笛卡兒積**或**卡氏積**) 爲所有首項屬於 A、末項屬於 B 的序偶所構成的集合, 記作 $A\times B$, 即

$$A\times B=\{(a,b):a\in A\text{ 且 }b\in B\}.$$

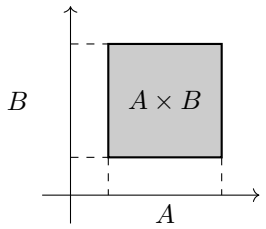
注意 2.1.33 依分離公理, $A\times B$ 的確是一個集合, 其嚴格構造如下: 對於任意 $a\in A$ 與 $b\in B$, 皆有 $\{a\}\subseteq A\cup B$ 及 $\{a,b\}\subseteq A\cup B$, 從而 $\{a\},\{a,b\}\in\mathcal{P}(A\cup B)$. 於是

$$(a,b)=\{\{a\},\{a,b\}\}\in\mathcal{P}(\mathcal{P}(A\cup B)),$$

故積集可藉由分離公理嚴格保證其存在性:

$$A\times B=\{x\in\mathcal{P}(\mathcal{P}(A\cup B)):\exists\,a\in A,\exists\,b\in B,x=(a,b)\}.$$

註記 2.1.34 $A \times B$ 的示意圖如下:



有了序偶與兩個集合的積集作爲基礎, 便可藉由遞迴的方式, 將此概念推廣至有限多個元素與集合的情形.

定義 2.1.35 給定 n 個元素 $a_1, a_2, \ldots, a_n$(其中整數 $n \geq 3$), 可以遞迴地定義**有序 n 元組** (簡稱 n **元組**) 如下:

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

即將前 $n-1$ 個元素構成的有序 $n-1$ 元組視爲序偶的首項, 而將 a_n 視爲序偶的末項, 藉此化爲 $n-1$ 的情況.

定義 2.1.36 已知 n 個集合 $A_1, A_2, \ldots, A_n$(其中整數 $n \geq 3$), 可以遞迴地定義此 n 個集合的**積集**如下:

$$A_1 \times A_2 \times \cdots \times A_n = (A_1 \times A_2 \times \cdots \times A_{n-1}) \times A_n,$$

即同樣化爲 $n-1$ 的情況, 也記作

$$\prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_1 \in A_1, \ldots, a_n \in A_n\}.$$

註記 2.1.37 特別地, 若參與積集運算的 n 個集合皆相同, 即 $A_1 = A_2 = \cdots = A_n = A$, 則其積集 $\underbrace{A \times A \times \cdots \times A}_{n次}$ 通常簡記爲 A^n.

2.2 集合的運算律

命題 2.2.1 (交換律) 設 A, B 爲兩集合, 則

(1) $A \cup B = B \cup A$;

(2) $A \cap B = B \cap A$;

(3) $A \triangle B = B \triangle A$;

(4) 若 $A \neq B$, 則 $A \times B \neq B \times A$;

(5) 若 $A = B$, 則 $A \times B = B \times A$;

(6) 若 $A = \varnothing$ 或 $B = \varnothing$, 則 $A \times B = B \times A = \varnothing$.

證明 僅證明 (1), 餘者由讀者自行給出. 依 $\vee$ 的交換性 (即 $P \vee Q \leftrightarrow Q \vee P$ 是重言式), 有

$$x \in A \cup B \iff (x \in A) \vee (x \in B) \iff (x \in B) \vee (x \in A) \iff x \in B \cup A,$$

依外延公理, 即得 $A \cup B = B \cup A$. □

注意 2.2.2 一般上, $A \setminus B \neq B \setminus A$.

命題 2.2.3 (結合律) 設 A, B, C 爲三集合, 則

(1) $A \cup (B \cup C) = (A \cup B) \cup C$;

(2) $A \cap (B \cap C) = (A \cap B) \cap C$;

(3) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$.

證明 僅證明 (1), 餘者由讀者自行給出. 依 $\vee$ 的結合性 (即 $((P \vee Q) \vee R) \leftrightarrow (P \vee (Q \vee R))$ 是重言式), 有

$$x \in (A \cup B) \cup C \iff (x \in A \cup B) \vee (x \in C) \iff [(x \in A) \vee (x \in B)] \vee (x \in C)$$
$$\iff (x \in A) \vee [(x \in B) \vee (x \in C)] \iff (x \in A) \vee (x \in B \cup C) \iff x \in A \cup (B \cup C).$$

依外延公理, 即得 $A \cup (B \cup C) = (A \cup B) \cup C$. □

注意 2.2.4 一般上, $A \setminus (B \setminus C) \neq (A \setminus B) \setminus C$.

定義 2.2.5 有了結合律的保證, 多個集合在進行相同的交、聯或對稱差運算時, 括號的添加順序不會影響最終結果. 於是, 對於任意 n 個集合 $A_1, A_2, \ldots, A_n$ (其中整數 $n \geq 3$), 可明確定義其**有限聯**、**有限交**及**有限對稱差** (並省略括號) 如下:

(1) 有限聯: $\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$;

(2) 有限交: $\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$;

(3) 有限對稱差: $\bigtriangleup_{i=1}^{n} A_i = A_1 \triangle A_2 \triangle \cdots \triangle A_n$.

註記 2.2.6 有限對稱差 $A_1 \triangle A_2 \triangle \cdots \triangle A_n$ 中的元素, 恰好是那些「屬於奇數個 A_i」的元素.

命題 2.2.7 (分配律) 設 A, B, C 爲三集合, 則

(1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;

(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

(3) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$;

(4) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;

(5) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;

(6) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

證明 僅證明 (1) 及 (6), 餘者由讀者自行給出.

對於 (1), 依 $\wedge$ 對 $\vee$ 的分配性 (即 $(P \wedge (Q \vee R)) \leftrightarrow ((P \wedge R) \vee (Q \wedge R))$ 是重言式), 有

$$x \in A \cap (B \cup C) \iff (x \in A) \wedge (x \in B \cup C) \iff (x \in A) \wedge [(x \in B) \vee (x \in C)]$$
$$\iff [(x \in A) \wedge (x \in B)] \vee [(x \in A) \wedge (x \in C)] \iff (x \in A \cap B) \vee (x \in A \cap C)$$
$$\iff x \in (A \cap B) \cup (A \cap C).$$

依外延公理, 即得 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

對於 (6), 依 $\wedge$ 的結合性及分配性, 有

$$(x, y) \in (A \times B) \cap (C \times D) \iff (x, y) \in A \times B \wedge (x, y) \in C \times D)$$

$$\begin{aligned}
&\iff [(x \in A) \wedge (y \in B)] \wedge [(x \in C) \wedge (y \in D)] \\
&\iff [(x \in A) \wedge (x \in C)] \wedge [(y \in B) \wedge (y \in D)] \\
&\iff [x \in A \cap C] \wedge [y \in B \cap D] \\
&\iff (x, y) \in (A \cap C) \times (B \cap D).
\end{aligned}$$

依外延公理, 即得 $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$. □

注意 2.2.8 一般上, $A \cup (B \triangle C) \neq (A \cup B) \triangle (A \cup C)$.

命題 2.2.9 (差集律) 設 A, B, C 爲三集合, 則

(1) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;

(2) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;

(3) $(B \cup C) \setminus A = (B \setminus A) \cup (C \setminus A)$;

(4) $(B \cap C) \setminus A = (B \setminus A) \cap (C \setminus A)$.

證明 僅證明 (1), 餘者由讀者自行給出.

$$\begin{aligned}
&x \in A \setminus (B \cup C) \iff (x \in A) \wedge (x \notin B \cup C) \iff (x \in A) \wedge \neg(x \in B \cup C) \\
&\iff (x \in A) \wedge \neg[(x \in B) \vee (x \in C)] \iff (x \in A) \wedge [\neg(x \in B) \wedge \neg(x \in C)] \\
&\iff (x \in A) \wedge [(x \notin B) \wedge (x \notin C)] \iff [(x \in A) \wedge (x \notin B)] \wedge [(x \in A) \wedge (x \notin C)] \\
&\iff (x \in A \setminus B) \wedge (x \in A \setminus C) \iff x \in (A \setminus B) \cap (x \in A \setminus C).
\end{aligned}$$

依外延公理, 即得 $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$. □

命題 2.2.10 (冪等律) 設 A 爲一集合, 則

(1) $A \cup A = A$;

(2) $A \cap A = A$.

證明 僅證明 (1), 餘者由讀者自行給出. 依 $\vee$ 的吸收性 (即 $(P \vee P) \leftrightarrow P$ 是重言式), 有

$$x \in A \cup A \iff (x \in A) \vee (x \in A) \iff x \in A.$$

依外延公理, 即得 $A \cup A = A$. □

命題 2.2.11 (零律) 設 A 爲一集合, 則

(1) $A \cup \varnothing = A$;

(2) $A \cap \varnothing = \varnothing$;

(3) $A \setminus A = \varnothing$;

(4) $A \setminus \varnothing = A$.

證明 依空集的定義, 對任意 x 而言, 命題 $x \in \varnothing$ 皆爲矛盾式.

對於 (1), 依邏輯性質「若 Q 是矛盾式, 則 $P \vee Q \leftrightarrow P$ 是重言式」, 有

$$x \in A \cup \varnothing \iff (x \in A) \vee \underbrace{(x \in \varnothing)}_{\text{矛盾式}} \iff x \in A.$$

依外延公理, 即得 $A \cup \varnothing = A$.

對於 (2), 依邏輯性質「若 Q, R 是矛盾式, 則 $P \vee Q \leftrightarrow R$ 是重言式」, 有

$$x \in A \cap \varnothing \iff (x \in A) \wedge \underbrace{(x \in \varnothing)}_{\text{矛盾式}} \iff x \in \varnothing.$$

依外延公理, 即得 $A \cap \varnothing = \varnothing$.

對於 (3), 依邏輯性質「$P \wedge \neg P$ 是矛盾式」, 有

$$x \in A \setminus A \iff (x \in A) \wedge (x \notin A) \iff \underbrace{(x \in A) \wedge \neg(x \in A)}_{\text{矛盾式}} \iff \underbrace{x \in \varnothing}_{\text{矛盾式}}.$$

依外延公理, 即得 $A \setminus A = \varnothing$.

對於 (4), 因 $x \in \varnothing$ 是矛盾式, 故其否定 $x \notin \varnothing$ 爲重言式. 依邏輯性質「若 Q 是重言式, 則 $P \wedge Q \leftrightarrow P$ 是重言式」, 有

$$x \in A \setminus \varnothing \iff (x \in A) \wedge \underbrace{(x \notin \varnothing)}_{\text{重言式}} \iff x \in A.$$

依外延公理, 即得 $A \setminus \varnothing = A$. □

命題 2.2.12 (么律) 設 U 爲全集, A 爲 U 的子集, 則

(1) $A \cup U = U$;

(2) $A \cap U = A$.

證明 因 $A \subseteq U$, 對任意 x 而言, 若 $x \in A$, 則必然 $x \in U$. 對於 (2), 依邏輯性質「若 Q 是重言式, 則 $P \wedge Q \leftrightarrow P$ 是重言式」, 有

$$x \in A \cap U \iff (x \in A) \wedge (x \in U) \iff x \in A.$$

依外延公理, 即得 $A \cap U = A$. (1) 的證明同理, 留給讀者作爲練習. □

命題 2.2.13 (餘補律) 設 U 爲全集, A 爲 U 的子集, 則

(1) $A \cup A^{\complement} = U$;

(2) $A \cap A^{\complement} = \varnothing$.

證明 依邏輯性質 ($P \vee \neg P$ 是重言式、$P \wedge \neg P$ 是矛盾式) 即得證. □

命題 2.2.14 (逆律) 設 U 爲全集, A 爲 U 的子集, 則

(1) $(A^{\complement})^{\complement} = A$;

(2) $U^{\complement} = \varnothing$;

(3) $\varnothing^{\complement} = U$.

證明 對於 (1), 只需要應用雙否定律 (即 $\neg(\neg P) \leftrightarrow P$ 是重言式) 即可. (2) 即命題 2.2.11(3) 中取 $A = U$. (3) 即命題 2.2.11(4) 中取 $A = U$. □

命題 2.2.15 (狄摩根律) 設 U 爲全集, A, B 爲 U 的子集, 則

(1) $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$;

(2) $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$.

證明 僅證明 (1), 餘者由讀者自行給出. 依補集的定義及邏輯的狄摩根律 (即 $\neg(P \vee Q) \leftrightarrow \neg P \wedge \neg Q$ 是重言式), 得

$$\begin{aligned} x \in (A \cup B)^{\complement} &\iff (x \in U) \wedge (x \notin A \cup B) \\ &\iff (x \in U) \wedge \neg[(x \in A) \vee (x \in B)] \\ &\iff (x \in U) \wedge [\neg(x \in A) \wedge \neg(x \in B)] \\ &\iff (x \in U) \wedge [(x \notin A) \wedge (x \notin B)] \\ &\iff [(x \in U) \wedge (x \notin A)] \wedge [(x \in U) \wedge (x \notin B)] \\ &\iff (x \in A^{\complement}) \wedge (x \in B^{\complement}) \\ &\iff x \in A^{\complement} \cap B^{\complement}. \end{aligned}$$

依外延公理, 即得 $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$. □

命題 2.2.16 (子集的關係式) 設 A, B, C 爲三集合, 則

(1) $A \cap B \subseteq A \subseteq A \cup B$ 且 $A \cap B \subseteq B \subseteq A \cup B$;

(2) $A \setminus B \subseteq A$;

(3) $A \triangle B \subseteq A \cup B$;

(4) 對稱律: $A \subseteq B$ 且 $B \subseteq A$ 的充要條件爲 $A = B$;

(5) 遞移律: 若 $A \subseteq B$ 且 $B \subseteq C$, 則 $A \subseteq C$;

(6) 吸收律: $A \subseteq B$ 等價於 $A \cap B = A$, 又等價於 $A \cup B = B$ (由此可得 $(A \cap B) \cup A = A$, $(A \cup B) \cap A = A$);

(7) 設 U 爲全集, 則 $A \subseteq B$ 的充要條件爲 $B^{\complement} \subseteq A^{\complement}$.

證明 (1) 任予 x, 依邏輯性質「$(P \wedge Q) \to P$ 及 $P \to (P \vee Q)$ 是重言式」, 有

$$x \in A \cap B \implies (x \in A) \wedge (x \in B) \implies x \in A$$

及

$$x \in A \implies (x \in A) \vee (x \in B) \implies x \in A \cup B,$$

依子集的定義, 即有 $A \cap B \subseteq A \subseteq A \cup B$. 同理可證 $A \cap B \subseteq B \subseteq A \cup B$.

(2) 任予 x, 依邏輯性質「$(P \wedge Q) \to P$ 是重言式」, 有

$$x \in A \setminus B \iff (x \in A) \wedge (x \notin B) \implies x \in A.$$

(3) 任予 x, 依邏輯性質「$(P \veebar Q) \to (P \vee Q)$ 是重言式 (讀者可自行透過眞值表檢驗)」, 有

$$x \in A \triangle B \iff (x \in A) \veebar (x \in B) \implies (x \in A) \vee (x \in B) \iff x \in A \cup B.$$

(4) 依邏輯性質「$\big[\forall x, [P(x) \wedge Q(x)]\big] \leftrightarrow \big[[\forall x, P(x)] \wedge [\forall x, Q(x)]\big]$ 是重言式」, 有

$$\begin{aligned} (A \subseteq B) \wedge (B \subseteq A) &\iff [\forall x, (x \in A \to x \in B)] \wedge [\forall x, (x \in B \to x \in A)] \\ &\iff \forall x, [(x \in A \to x \in B) \wedge (x \in B \to x \in A)] \\ &\iff \forall x, [x \in A \leftrightarrow x \in B] \\ &\iff A = B. \end{aligned}$$

(5) 依邏輯性質「$[(P \to Q) \wedge (Q \to R)] \to (P \to R)$ 是重言式」即得證.

(6) 設 $A \subseteq B$. 由 (1), 顯然有 $A \cap B \subseteq A$. 另一方面, 任予 $x \in A$, 因 $A \subseteq B$, 故 $x \in B$, 即 $x \in A \cap B$, 於是 $A \subseteq A \cap B$, 從而 $A \cap B = A$. 反之, 設 $A \cap B = A$, 則由 (1) 得 $A \cap B \subseteq B$, 即 $A \subseteq B$. 同理可證 $A \subseteq B$ 等價於 $A \cup B = B$.

(7) 設 $A \subseteq B$, 則任予 $x \in B^{\complement}$, 有 $x \notin B$. 若 $x \notin A^{\complement}$, 則 $x \in A$, 再由 $A \subseteq B$ 可得 $x \in B$, 這是一個矛盾. 因此, $x \in A^{\complement}$. 依 x 的任意性, 即得 $B^{\complement} \subseteq A^{\complement}$. 充分性的證明留給讀者作爲練習. □

2.3 指標族

先前已經定義了有限多個集合的交集與聯集. 對於更一般的情況, 爲了標明不同的集合, 遂引入指標集的工具.

考慮一個非空集合 I, 若其中的元素 $i, j, k, \ldots$ 被用作指標來指定某個集族中的各個集合, 則此整體便稱爲一個**指標族**或**帶指標的集族**, 簡稱**集族**, 而 I 稱爲**指標集**, 其元素即爲**指標**. 爲了簡潔, 通常將這個族記作 $\{A_i\}_{i\in I}$ 或 $\{A_i : i \in I\}$.

有了指標族的概念, 便可將交集與聯集推廣至任意族的情形:

定義 2.3.1 已知一族集合 $\{A_i\}_{i\in I}$, 其中 I 爲指標集.

(1) 此族集合的**一般聯集**或**廣義聯集**由所有至少屬於族中某一個 A_i 的元素所構成, 記作

$$\bigcup_{i\in I} A_i = \{x : \exists\, i \in I, x \in A_i\}.$$

(2) 此族集合的**一般交集**或**廣義交集**由屬於族中每一個 A_i 的元素所構成, 記作

$$\bigcap_{i\in I} A_i = \{x : \forall\, i \in I, x \in A_i\}.$$

註記 2.3.2 特別地, 若對任意 $i, j \in I$, 當 $i \neq j$ 時, 都有 $A_i \cap A_j = \varnothing$, 則可將其一般聯記作

$$\bigsqcup_{i\in I} A_i,$$

並稱爲**一般無交聯集** (或**一般無交並集**).

命題 2.3.3 設 $\{A_i\}_{i\in I}$ 爲一集族, B 爲一集合.

(1) 若 $\forall\, i \in I$, $A_i \subseteq B$, 則

$$\bigcup_{i\in I} A_i \subseteq B.$$

(2) 若 $\forall\, i \in I$, $B \subseteq A_i$, 則

$$B \subseteq \bigcap_{i\in I} A_i.$$

證明 僅證明 (1), 餘者留給讀者作爲習題. 任予 $x \in \bigcup_{i\in I} A_i$, 則有 $\exists\, i \in I, x \in A_i$. 由 $A_i \subseteq B$, 可得 $x \in B$. 依 x 的任意性, 即得 $\bigcup_{i\in I} A_i \subseteq B$. □

命題 2.3.4 (廣義狄摩根定律) 設 $\{A_i\}_{i\in I}$ 爲一集族, U 爲全集, 則

(1) $\left(\bigcup_{i\in I} A_i\right)^{\complement} = \bigcap_{i\in I} A_i^{\complement}$;

(2) $\left(\bigcap_{i\in I} A_i\right)^{\complement} = \bigcup_{i\in I} A_i^{\complement}$.

證明 僅證明 (1), 餘者留給讀者作爲習題. 任予 x,

$$\begin{aligned} x \in \left(\bigcup_{i\in I} A_i\right)^{\complement} &\iff (x \in U) \wedge \neg \left(x \in \bigcup_{i\in I} A_i\right) \\ &\iff (x \in U) \wedge \neg (\exists\, i \in I, x \in A_i) \\ &\iff (x \in U) \wedge (\forall\, i \in I, x \notin A_i) \\ &\iff \forall\, i \in I, (x \in U) \wedge (x \notin A_i) \\ &\iff \forall\, i \in I, x \in A_i^{\complement} \\ &\iff x \in \bigcap_{i\in I} A_i^{\complement}. \end{aligned}$$

依外延公理, 即得 $\left(\bigcup_{i\in I} A_i\right)^{\complement} = \bigcap_{i\in I} A_i^{\complement}$. □

命題 2.3.5 (廣義分配律) 設 $\{A_i\}_{i\in I}$ 及 $\{B_j\}_{j\in J}$ 爲兩集族, 則

(1) $\left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) = \bigcup_{(i,j)\in I\times J} (A_i \cap B_j)$;

(2) $\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right) = \bigcap_{(i,j)\in I\times J} (A_i \cup B_j)$.

證明 僅證明 (1), 餘者留給讀者作爲習題. 任予 x,

$$\begin{aligned} x \in \left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) &\iff \left(x \in \bigcup_{i\in I} A_i\right) \wedge \left(x \in \bigcup_{j\in J} B_j\right) \\ &\iff (\exists\, i \in I, x \in A_i) \wedge (\exists\, j \in J, x \in B_j) \\ &\iff \exists\, i \in I, \exists\, j \in J, (x \in A_i) \wedge (x \in B_j) \\ &\iff \exists\, (i,j) \in I \times J, x \in A_i \cap B_j \\ &\iff x \in \bigcup_{(i,j)\in I\times J} (A_i \cap B_j). \end{aligned}$$

依外延公理, 即得 $\left(\bigcup_{i\in I} A_i\right) \cap \left(\bigcup_{j\in J} B_j\right) = \bigcup_{(i,j)\in I\times J} (A_i \cap B_j)$. □

單元 3

映射

3.1 映射的定義與性質

定義 3.1.1 設有兩個集合 A, B. 如果 $A \times B$ 的某個子集 f 滿足條件:

(1) 對一切 $x \in A$, 均存在 $y \in B$ 滿足 $(x, y) \in f$;

(2) 若 $(x, y_1) \in f$ 且 $(x, y_2) \in f$, 則 $y_1 = y_2$,

則稱 f 爲自 A 至 B 的**映射**, 一般寫成 $f : A \to B$. 若 $(x, y) \in f$, 則記之爲 $y = f(x)$, 並且稱 x 爲 y 的**原像**, 稱 y 爲 x 的**像**. 以上兩個條件也可以寫成:

(1) 對一切 $x \in A$, 均存在 $y \in B$ 滿足 $y = f(x)$;

(2) 若 $y_1 = f(x)$ 且 $y_x = f(x)$, 則 $y_1 = y_2$,

或者直接簡化成一個條件: $\forall\, x \in A, \exists\,! \, y \in B, (x, y) \in f$ (即 $y = f(x)$). 當 A、B 爲數集 (如 $\mathbb{R}$ 或 $\mathbb{C}$) 時, 也稱映射爲**單變數函數**, 且當 $B \subseteq \mathbb{R}$ 時, 稱映射爲**實函數**. 當 A 爲 $\mathbb{R}^n$ 或其子集時, 稱映射爲**多變數函數**, 且當 $B \subseteq \mathbb{R}^m$ 時, 稱映射爲**向量函數**. 當 A、B 爲幾何對象所成的全體時, 也稱 f 爲**變換**.

定義 3.1.2 設 $f : A \to B$ 爲一映射,

(1) 稱 A 爲 f 的**定義域**, 記作 D_f 或 $\mathrm{dom}(f)$, 從映射的定義不難看出 $D_f = \{x : \exists\, y \in B, f(x) = y\}$;

(2) 稱 B 爲 f 的**對應域**或**陪域**;

(3) 稱 B 的子集 $\{y \in B : \exists\, x \in A, f(x) = y\}$ 爲 f 的**值域**, 記作 $f(D_f)$ (即 $f(A)$) 或 $\mathrm{im}(f)$[1]或 R_f.

另外, 本文也以符號 $\mathcal{F}(A, B)$ 或 B^A 表示以 A 爲定義域、以 B 爲對應域的全體映射, 即 $f \in \mathcal{F}(A, B)$ 或 $f \in B^A$.

註記 3.1.3 (1) (定義域的限制) 若 $f \in B^A$, 且 $C \subseteq A$, 則

$$f|_C : C \longrightarrow B, \quad x \longmapsto f(x)$$

是一個映射. 注意到 $f|_C \subseteq f$.

(2) (對應域的調整) 若 $f \in B^A$, 且集合 C 滿足 $f(A) \subseteq C$, 則 $f \in C^A$.

(3) (函數的延拓) 設 $f \in B^{A_1}$, $g \in B^{A_2}$. 若 $A_1 \subseteq A_2$, 且對所有 $x \in A_1$, 有 $f(x) = g(x)$, 則 $g|_{A_1} = f$, 且稱 g 是 f 在 A_2 上的**延拓**.

[1]這種記號在遇到複變函數時可能會與虛部造成混淆.

命題 3.1.4 設 $f, g \in B^A$, 則 $f = g$ 的充要條件爲: 對一切 $x \in A$, 均有 $f(x) = g(x)$.

證明 必要性: 設 $f = g$. 予 $x \in A$, 依映射的定義, 存在 $y \in B$ 使得 $y = f(x)$. 又因 $f = g$, 所以由 $(x, y) \in f = g$ 可推得 $y = g(x)$, 即 $f(x) = g(x)$.

充分性: 設對一切 $x \in A$, 均有 $f(x) = g(x)$. 若 $(x, y) \in f$, 則 $y = f(x) = g(x)$, 亦即 $(x, y) \in g$, 所以 $f \subseteq g$. 同理可推得 $g \subseteq f$, 故 $f = g$. □

注意 3.1.5 對於兩個映射而言, 只有當它們的定義域以及對應關係完全一樣時, 才能說它們是相等的. 如 $f(x) = |x|$ $(x \in \mathbb{R})$ 及 $g(x) = x\,\mathrm{sgn}(x)$ $(x \in \mathbb{R})$[2], 雖然它們形式上不同, 但它們具有同樣的定義域和對應關係, 故爲同一個函數. 而函數 $\varphi(x) = x^3$ $(x \in \mathbb{R})$ 及 $\psi(x) = x^3$ $(x \geq 0)$ 是不同的函數.

例 3.1.6 證明定義成 $f(x) = \sqrt{x^2 + 2x + 5}$ $(x \in \mathbb{R})$ 的函數 f 的值域爲 $B = \{y \in \mathbb{R} : y \geq 2\}$.

證明 要證明兩集合 $f(\mathbb{R})$ 及 B 相等, 需要證明它們互相包含於對方. 任取 $y \in f(\mathbb{R})$, 根據值域的定義, 存在 $x \in \mathbb{R}$ 使得 $y = f(x) = \sqrt{x^2 + 2x + 5} = \sqrt{(x+1)^2 + 4}$. 因爲

$$(x+1)^2 \geq 0 \implies (x+1)^2 + 4 \geq 4 \implies y^2 \geq 4 \implies y \leq -2 \text{ 或 } y \geq 2,$$

並且 $y \geq 0$, 所以 $y \in B$, 因此 $f(\mathbb{R}) \subseteq B$. 另一方面, 給定 $y \in B$, 那麼 $y \geq 2$ 可推得 $y^2 - 4 \geq 0$, 故可取 $x = -1 \pm \sqrt{y^2 - 4} \in \mathbb{R}$, 得

$$f(x) = \sqrt{x^2 + 2x + 5} = \sqrt{(x+1)^2 + 4} = \sqrt{\left(-1 \pm \sqrt{y^2 - 4} + 1\right)^2 + 4} = \sqrt{y^2 - 4 + 4} = \sqrt{y^2} = |y| = y,$$

即 $y \in f(\mathbb{R})$, 因此 $B \subseteq f(\mathbb{R})$. □

定義 3.1.7 設映射 $f \in B^A$.

(1) 若 $f(x_1) = f(x_2)$ 可推得 $x_1 = x_2$, 則稱 f 爲**單射**或**嵌射**, 且當 f 爲函數時也稱爲**一對一函數**, 有時記作 $f : A \hookrightarrow B$;

(2) 若 $f(A) = B$, 即對一切 $y \in B$, 均存在 $x \in A$ 滿足 $y = f(x)$, 則稱 f 爲**滿射**或**蓋射**, 且當 f 爲函數時也稱爲**映成函數**, 有時記作 $f : A \twoheadrightarrow B$;

(3) 若 f 爲單射且爲滿射, 則稱 f 爲**雙射**或**對射**, 且當 f 爲函數時也稱爲**一一映成函數**.

例 3.1.8 設 A, B 爲兩集合.

(1) 映射

$$\mathrm{id}_A : A \longrightarrow A, \quad x \longmapsto x$$

稱爲**恆等映射**. 不難看出 id_A 是雙射.

(2) 設 $A \subseteq B$, 映射

$$\iota : A \hookrightarrow B, \quad x \longmapsto x$$

稱爲**包含映射**. 不難看出 ι 是單射, 且當 $A \subsetneq B$ 時, ι 不是滿射.

(3) 設 $A = \prod_{i=1}^n A_i$, 其中 A_i $(i = 1, \ldots, n)$ 爲一族集合. 固定 $j \in \{1, \ldots, n\}$, 映射

$$\pi_j : A \twoheadrightarrow A_j, \quad (x_1, \ldots, x_n) \longmapsto x_j$$

稱爲**投影映射**. 不難看出 π_j 是滿射.

[2] sgn 是**符號函數**, 定義爲: 當 $x > 0$ 時, $\mathrm{sgn}(x) = 1$; 當 $x < 0$ 時, $\mathrm{sgn}(x) = -1$; 當 $x = 0$ 時, $\mathrm{sgn}(x) = 0$.

(4) 設 $A=\bigsqcup_{i\in I}A_i$, 其中 A_i $(i\in I)$ 爲一族非空集合, 映射

$$\pi : A \longrightarrow\!\!\!\!\!\rightarrow I, \quad x \longmapsto i \quad (x\in A_i)$$

也稱爲**投影映射**, 其指出無交聯集中元素所在集合的指標.

(5) 設 $b\in B$, 映射

$$C_b : A \longrightarrow B, \quad x \longmapsto b$$

稱爲**常值映射**. 顯然, 當 A 及 B 的元素個數各都超過 1 個時, C_b 不是單射, 也不是滿射.

(6) 設 $B\subseteq A$, $C=\{0,1\}$, 映射

$$\chi_B : A \longrightarrow C, \quad x \longmapsto \begin{cases} 1, & x\in B, \\ 0, & x\notin B \end{cases}$$

稱爲 B 在 A 上的**特徵映射**.

(7) 設 $B=\{x_n : n\in\mathbb{R}\}$, 序列 $\{x_n\}_{n\in\mathbb{N}}$ 相當於映射

$$f : \mathbb{N} \longrightarrow B, \quad n \longmapsto x_n$$

的值域. 也就是說, 序列可以看作以 $\mathbb{N}$ 爲定義域的映射.

3.2 映射的運算

定理 3.2.1 設 A,B,C 爲三個集合, 且 $f\in B^A$ 和 $g\in C^B$, 定義

$$g\circ f=\{(x,y)\in A\times C : \exists\, z\in B, (x,z)\in f, (z,y)\in g\},$$

則 $g\circ f$ 是一個映射, 且 $g\circ f\in C^A$.

證明 對一切 $x\in A$, 因爲 $f\in B^A$, 所以存在 $z\in B$ 使得 $(x,z)\in f$. 又 $g\in C^B$, 所以對於上述 $z\in B$, 存在 $y\in C$ 使得 $(z,y)\in g$. 根據 $g\circ f$ 的定義可知 $(x,y)\in g\circ f$, 故滿足定義 3.1.1(1).

若 $(x,y_1),(x,y_2)\in g\circ f$, 則存在 $z_1,z_2\in B$ 使得 $(x,z_1),(x,z_2)\in f$ 且 $(z_1,y_1),(z_2,y_2)\in g$. 因爲 $f\in B^A$ 是映射, 所以 $z_1=z_2$. 又 $g\in C^B$ 是映射, 所以 $y_1=g(z_1)=g(z_2)=y_2$, 故滿足定義 3.1.1(2).

綜上所述, $g\circ f\in C^A$. □

定義 3.2.2 定理 3.2.1 中的 $g\circ f$ 稱爲**合成映射**或**複合映射**, 且當 f、g 爲函數時稱 $g\circ f$ 爲**合成函數**或**複合函數**.

註記 3.2.3 (1) 對於 $x\in A$, 有 $(g\circ f)(x)=g\,(f(x))$.

(2) 若 $f\in B^A$, $g\in D^C$ 均爲映射, 則必須要有 $f(B)\subseteq C$, $g\circ f$ 才有意義.

命題 3.2.4 設 $f\in B^A$, $g\in C^B$, $h\in D^C$, 則

(1) $(h\circ g)\circ f=h\circ(g\circ f)$ (結合律);

(2) $f\circ \mathrm{id}_X=f$ (右單位律);

(3) $\mathrm{id}_Y\circ f=f$ (左單位律);

(4) 對於 $c\in C$, 若 C_c 是自 B 至 $\{c\}$ 的常值映射, 則 $C_c\circ f$ 是自 A 至 $\{c\}$ 的常值映射 (左零律);

(5) 對於 $b\in B$, 若 C_b 是自 A 至 $\{b\}$ 的常值映射, 則 $g\circ C_b$ 是 X 到 $\{g(y)\}$ 的常值映射 (右零律).

證明 僅證明 (1), 餘者留給讀者作爲練習.

$$\begin{aligned}
&(x,y)\in(h\circ g)\circ f\\
\Longleftrightarrow\ &\exists\, z\in B,(x,z)\in f,(z,y)\in h\circ g\\
\Longleftrightarrow\ &\exists\, z\in B,\exists\, w\in C,(x,z)\in f,(z,w)\in g,(w,y)\in h\\
\Longleftrightarrow\ &\exists\, w\in C,(x,w)\in g\circ f,(w,y)\in h\\
\Longleftrightarrow\ &(x,y)\in h\circ(g\circ f).
\end{aligned}$$

□

命題 3.2.5 設 $f\in B^A$ 及 $g\in C^B$,

(1) 若 f,g 均爲單射, 則 $g\circ f$ 爲單射;

(2) 若 f,g 均爲滿射, 則 $g\circ f$ 爲滿射;

(3) 若 f,g 均爲雙射, 則 $g\circ f$ 爲雙射.

證明 (1) 設 $x_1,x_2\in A$ 滿足 $(g\circ f)(x_1)=(g\circ f)(x_2)$, 由 g 是單射可得 $f(x_1)=f(x_2)$, 再由 f 是單射可得 $x_1=x_2$.

(2) 予 $z\in C$, 因 g 是滿射, 所以存在 $y\in B$, $g(y)=z$; 又因 f 是滿射, 所以存在 $x\in A$, $f(x)=y$, 從而 $(g\circ f)(x)=g(f(x))=g(y)=z$.

(3) 由 (1) 和 (2) 即得結論.

□

命題 3.2.6 設 $f\in B^A$,

(1) 若且唯若 f 是單射, 則存在滿足 $g\circ f=\mathrm{id}_A$ 的映射 $g\in A^B$ (即存在左逆);

(2) 若且唯若 f 是滿射, 則存在滿足 $f\circ g=\mathrm{id}_B$ 的映射 $g\in A^B$ (即存在右逆);

(3) 若且唯若 f 是滿射, 則存在滿足 $g\circ f=\mathrm{id}_A$ 且 $f\circ g=\mathrm{id}_B$ 的唯一映射 $g\in A^B$ (即存在雙邊逆).

證明 (1) 充分性:

$$f(x)=f(y)\implies g(f(x))=g(f(y))\implies(g\circ f)(x)=(g\circ f)(y)\implies \mathrm{id}_A(x)=\mathrm{id}_A(y)\implies x=y,$$

即 f 是單射.

必要性: 對於 $f(A)$, 定義 $g:f(x)\mapsto x$. 因 f 是單射, 故 g 良定義. 對於 $B\setminus f(A)$, 因 $A\neq\varnothing$, 故可取 $a\in A$, 定義 $g(y)=a$ $(y\notin f(A))$. 也就是說, 定義

$$g:B\longrightarrow A,\quad y\longmapsto\begin{cases}x, & y=f(x)\in f(A),\\ a, & y\notin f(A).\end{cases}$$

不難驗證 $g\circ f=\mathrm{id}_A$, 即 $\forall\, x\in A,(g\circ f)(x)=x$.

(2) 充分性: 任取 $y\in B$, 因 $f(g(y))=y$ 且 $g(y)\in A$, 故取 $x=g(y)\in A$, 於是 $y=f(x)\in f(A)$, 即 $B=f(A)$.

必要性: 任取 $y\in B$, 由 f 是滿射, 可得存在 $x_y\in A$ 使得 $f(x_y)=y$. 定義

$$g:B\longrightarrow A,\quad y\longmapsto x_y,$$

則 $\forall\, y\in B$, $(f\circ g)(y)=f(g(y))=f(x_y)=y=\mathrm{id}_B(y)$.

(3) 充分性: 由 (1) 及 (2) 即得.

必要性: 定義

$$g : B \longrightarrow A, \quad y = f(x) \longmapsto x.$$

因 $B = f(A)$, 且 f 是單射, 故 g 良定義. 若 $h \in A^B$ 也滿足 $h \circ f = \mathrm{id}_A$ 及 $f \circ h = \mathrm{id}_B$, 則

$$g \circ f = \mathrm{id}_A = h \circ f \implies g \circ (f \circ g) = h \circ (f \circ g) \implies g \circ \mathrm{id}_B = h \circ \mathrm{id}_B \implies g = h.$$

□

命題 3.2.7 設 $f \in B^A$ 及 $g \in C^B$,

(1) 若 $f \circ g$ 是單射, 則 g 是單射;

(2) 若 $f \circ g$ 是滿射, 則 f 是滿射;

(3) 若 $f \circ g$ 是雙射, 則 f 是滿射, 且 g 是單射.

證明 直接透過定義檢驗即可. □

定義 3.2.8 設 $f \in B^A$, 定義

$$f^{-1} = \{(x, y) : (y, x) \in f\},$$

若 $f^{-1} \in A^B$ [3], 則稱 f 是**可逆的**, 且稱 f^{-1} 爲 f 的**逆映射**或**反映射**, 且當 f 爲函數時, 也稱 f^{-1} 爲**反函數**.

註記 3.2.9 $f \in B^A$ 可逆 $\iff \mathrm{dom}(f^{-1}) = B \iff f(A) = B$, 同時, $\forall\, x \in A,\ y = f(x) \iff x = f^{-1}(y)$.

命題 3.2.10 設 $f \in B^A$, $g \in C^B$ 爲兩可逆的函數, 則

(1) $\mathrm{id}^{-1} = \mathrm{id}$; (2) $\left(f^{-1}\right)^{-1} = f$; (3) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

證明 (1)、(2) 顯而易見. (3) $(x, y) = (g \circ f)^{-1} \iff (y, x) \in g \circ f \iff \exists\, z \in B, (y, z) \in f, (z, x) \in g$
$\iff \exists\, z \in B, (x, z) \in f^{-1}, (z, y) \in g^{-1} \iff (x, y) \in f^{-1} \circ g^{-1}$. □

命題 3.2.11 [4] 設 $f \in B^A$ 爲可逆的函數, 則

(1) $\mathrm{dom}(f) = \mathrm{im}(f^{-1})$; (2) $\mathrm{dom}(f^{-1}) = \mathrm{im}(f)$.

證明 (1) $x \in \mathrm{dom}(f) \iff \exists\, y \in B, (x, y) \in f \iff \exists\, y \in B, (y, x) \in f^{-1} \iff x \in \mathrm{im}(f^{-1})$.

(2) $x \in \mathrm{dom}(f^{-1}) \iff \exists\, y \in A, (x, y) \in f^{-1} \iff \exists\, y \in A, (y, x) \in f \iff x \in \mathrm{im}(f)$.

□

命題 3.2.12 設 A, B 爲兩個集合.

(1) 若 $f \in B^A$ 爲雙射, 則 $f^{-1} \in A^B$ 且爲雙射.

(2) 若 $f \in B^A$ 可逆, 則 f 是雙射.

證明 (1) (a) 先證明 f^{-1} 是映射: 對一切 $y \in B$, 因爲 f 是滿射, 所以存在 $x \in A$ 使得 $(x, y) \in f$, 即 $(y, x) \in f^{-1}$. 給定 $(y, x_1), (y, x_2) \in f^{-1}$, 有 $(x_1, y), (x_2, y) \in f$. 因爲 f 是單射, 所以 $x_1 = x_2$. 因此, $f^{-1} \in A^B$.

[3] 注意, f^{-1} 未必是映射.

[4] 爲了避免混淆, 本命題暫不使用 $f^{-1}(B)$ 來表示 f^{-1} 的值域.

(b) 證明 f^{-1} 是單射: 若 $(y_1,x),(y_2,x)\in f^{-1}$, 則 $(x,y_1),(x,y_2)\in f$, 再由 $f:A\to B$ 是函數可知 $y_1=y_2$, 故 f^{-1} 是單射.

(c) 證明 f^{-1} 是滿射: 予 $x\in A$, 因爲 f 是函數, 所以存在 $y\in B$ 使得 $(x,y)\in f$, 即 $(y,x)\in f^{-1}$, 因此 f^{-1} 是滿射.

(2) 根據註記 3.2.9, 可知 $f(A)=B$, 所以 f 是滿射. 若 $(x_1,y),(x_2,y)\in f$, 則 $(y,x_1),(y,x_2)\in f^{-1}$. 由於 f^{-1} 是函數, 因此 $x_1=x_2$, 即 f 是單射, 故 f 是雙射.

□

命題 3.2.13 設 $f\in B^A$ 可逆, 則

(1) $f^{-1}\circ f=\mathrm{id}_A$; (2) $f\circ f^{-1}=\mathrm{id}_B$.

證明 顯而易見. □

命題 3.2.14 設 $f\in B^A$, $g\in A^B$ 爲兩映射. 若 $g\circ f=\mathrm{id}_A$ 且 $f\circ g=\mathrm{id}_B$, 則 f 爲雙射且 $g=f^{-1}$.

證明 f 爲雙射是命題 3.2.6(3) 的結論.
設 $(y,x)\in g$, 即 $x=g(y)$, 則

$$f(x)=f(g(y))=(f\circ g)(y)=\mathrm{id}_B(y)=y,$$

所以 $(x,y)\in f$, 即 $(y,x)\in f^{-1}$. 另一方面, 設 $(y,x)\in f^{-1}$, 即 $x=f^{-1}(y)$ 或 $y=f(x)$, 則

$$g(y)=g(f(x))=(g\circ f)(x)=\mathrm{id}_A(x)=x,$$

所以 $(y,x)\in g$. 因此, $g=f^{-1}$. □

3.3 像與原像

定義 3.3.1 設 $f\in B^A$, $C\subseteq A$, $D\subseteq B$,

(1) 定義 C 在 f 之下的**像集**爲

$$f(C)=\{f(x)\in B:x\in C\};$$

(2) 定義 D 在 f 之下的**原像集**爲

$$f^{-1}(D)=\{x\in A:f(x)\in D\}.$$

註記 3.3.2 (1) 先前已經用 $f(A)$ 這個記號來表示值域了.

(2) 就算函數 f 不可逆, $f^{-1}(D)$ 仍有意義; 而當 f 可逆時, $f^{-1}(D)$ 恰爲 f^{-1} 的值域.

例 3.3.3 (1) 將 f 定義成 $f(x)=2x+1$ $(x\in\mathbb{R})$, 則 $f([1,2])=[3,5]$, $f^{-1}([3,5])=[1,2]$.

(2) 將 g 定義成 $g(x)=x^2$ $(x\in\mathbb{R})$, 則 $g([-1,2])=[0,4]$, $g([-2,1))=[0,4]$, $g^{-1}([0,4])=[-2,2]$.

注意 3.3.4 上例 (2) 意味著, 若 X,Y,Z 爲三個集合, 則 $g(X)=Y$ 未必能推得 $X=g^{-1}(Y)$, 反之亦然; $g(X)=g(Z)$ 也無法保證 $X=Z$. 而顯然地, 只要 f 可逆, $f(X)=Y$ 就能推出 $X=f^{-1}(Y)$; $f(X)=f(Z)$ 也可推得 $X=Z$.

命題 3.3.5 設 A, B 爲兩集合, $f \in B^A$ 爲一映射, 則

$$\bar{f} : \mathcal{P}(A) \longrightarrow \mathcal{P}(B), \quad C \longmapsto f(C)$$

及

$$\hat{f} : \mathcal{P}(B) \longrightarrow \mathcal{P}(A), \quad D \longmapsto f(D)$$

均爲映射.

證明 僅證明 (1), 而 (2) 的證明也類似. 設 $C, D \subseteq A$ 且 $C = D$, 則根據像集的定義, 有 $f(C) = f(D)$. 另外, 對於一切 $C \subseteq A$, 因爲 $f \in B^A$, 所以對所有 $x \in C$, 均有 $y \in B$ 滿足 $y = f(x)$, 設 E 由這些 y 組成, 則 $f(C) = E$ 且 $E \in \mathcal{P}(B)$, 即 $(C, E) \in f$. 因此, $\bar{f} \in (\mathcal{P}(B))^{\mathcal{P}(A)}$. □

命題 3.3.6 設 A, B 爲兩集合, $f \in B^A$ 是一映射, $\{C_i : i \in I\}$ 爲 A 的一族子集, $\{D_j : j \in J\}$ 爲 B 的一族子集, 則

(1) $f^{-1}\left(\bigcup\limits_{j\in J} D_j\right) = \bigcup\limits_{j\in J} f^{-1}(D_j)$;

(2) $f^{-1}\left(\bigcap\limits_{j\in J} D_j\right) = \bigcap\limits_{j\in J} f^{-1}(D_j)$;

(3) $f\left(\bigcup\limits_{i\in I} C_i\right) = \bigcup\limits_{i\in I} f(C_i)$;

(4) $f\left(\bigcap\limits_{i\in I} C_i\right) \subseteq \bigcap\limits_{i\in I} f(C_i)$.

證明 (1) $x \in f^{-1}\left(\bigcup_{j\in J} D_j\right) \iff f(x) \in \bigcup_{j\in J} D_j \iff \exists\, j \in J, f(x) \in D_j$
$\iff \exists\, j \in J, x \in f^{-1}(D_j) \iff x \in \bigcup_{j\in J} f^{-1}(D_j)$.

(2) $x \in f^{-1}\left(\bigcap_{j\in J} D_j\right) \iff f(x) \in \bigcap_{j\in J} D_j \iff \forall\, j \in J, f(x) \in D_j \iff \forall\, j \in J, x \in f^{-1}(D_j)$
$\iff x \in \bigcap_{j\in J} f^{-1}(D_j)$.

(3) $y \in f\left(\bigcup_{i\in I} C_i\right) \iff \exists\, x \in \bigcup_{i\in I} C_i, y = f(x) \iff \exists\, i \in I, \exists\, x \in C_i, y = f(x)$
$\iff \exists\, i \in I, y \in f(C_i) \iff y \in \bigcup_{i\in I} f(C_i)$.

(4) $y \in f\left(\bigcap_{i\in I} C_i\right) \iff \exists\, x, x \in \bigcap_{i\in I} C_i, y = f(x) \iff \exists\, x, \forall\, i \in I, x \in C_i, y = f(x)$
$\implies \forall\, i \in I, y \in f(C_i) \iff y \in \bigcap_{i\in I} f(C_i)$.

□

注意 3.3.7 (4) 中的等號未必成立. 例如, 令 $A = B = \{1, 2\}$, $C = \{1\}$, $D = \{2\}$, 定義 $f \in B^A$, $f(1) = f(2) = 1$, 則

$$f(C \cap D) = f(\varnothing) = \varnothing \subsetneq \{1\} = f(C) \cap f(D).$$

命題 3.3.8 設 A, B 爲兩集合, $f \in B^A$ 是一映射, $C, E \subseteq A$, $D, G \subseteq B$, 則

(1) $C \subseteq f^{-1}(f(C))$, 而當 f 是單射時, 等號成立;

(2) $f\left(f^{-1}(D)\right) \subseteq D$, 而當 f 是滿射時, 等號成立;

(3) $f^{-1}(G \setminus D) = f^{-1}(G) \setminus f^{-1}(D)$;

(4) $f(C) \setminus f(E) \subseteq f(C \setminus E)$, 且等號對所有 $C, E \subseteq A$ 成立的充要條件爲 f 是單射.

證明 (1) 設 $x \in C$, 則 $f(x) \in f(C)$. 依像集的定義, 有 $x \in f^{-1}(f(C))$, 因此 $C \subseteq f^{-1}(f(C))$. 當 f 是單射時, 設 $x \in f^{-1}(f(C))$, 則 $f(x) \in f(D)$, 於是存在 $x' \in D$ 使得 $f(x') = f(x)$, 從而由 f 是單射, 得 $x = x' \in D$, 因此 $f^{-1}(f(C)) = C$.

(2)、(3)、(4) 的證明也不難, 留給讀者自行練習. □

例 3.3.9 (1) 取 $A=\{1,2\}$, $B=\{3\}$, $C=\{1\}\subseteq A$, 定義 $f(1)=3, f(2)=3$, 則

$$f^{-1}(f(C))=f^{-1}(\{3\})=\{1,2\}\supsetneq C.$$

(2) 取 $A=\{1\}$, $B=\{2,3\}$, $D=\{2,3\}\subseteq B$, 定義 $f(1)=2$, 則

$$f(f^{-1}(D))=f(\{1\})=\{2\}\subsetneq D.$$

(3) 取 $A=\{1,2\}$, $B=\{3\}$, $C=\{1\}\subseteq A$, $E=\{2\}\subseteq A$, 定義 $f(1)=3, f(2)=3$, 則

$$f(C)\setminus f(E)=\{3\}\setminus\{3\}=\varnothing\subsetneq\{3\}=f(\{1\})=f(C\setminus E).$$

註記 3.3.10 先前在註記 2.1.14 有提到 2^A 這個記號, 現在說明其意義. 依無窮公理 (公理 2.1.22) 中的符號約定, $2=\{\varnothing,\{\varnothing\}\}=\{0,1\}$, 則 2^A 是以 A 爲定義域、2 爲對應域的所有映射的集合. 定義

$$f:\mathcal{P}(A)\longrightarrow 2^A,\quad B\longmapsto\chi_B,$$

其中 $B\subseteq A$, 且 χ_B 爲 B 在 A 上的特徵映射. 顯然 f 是一個映射.

若 $B,C\subseteq A$ 滿足 $f(B)=f(C)$, 即 $\chi_B=\chi_C$, 則

$$B=\{x\in A:\chi_B(x)=1\}=\{x\in A:\chi_C(x)=1\}=C,$$

這表示 f 是單射.

若 $g\in 2^A$, 則取 $B=g^{-1}(\{1\})$, 於是 $B\subseteq A$, 且 $f(B)=\chi_B=g$, 這意味著 f 是滿射.

綜上, f 是雙射, 即 A 的一切子集合與自 A 映至 $\{0,1\}$ 的所有映射之間具有一一對應的關係.

3.4 一般積集

前文曾提及, 替代公理與選擇公理須待映射的概念確立後方能引入. 現已具備映射及 B^A(即以 A 爲定義域、B 爲對應域的映射全體) 之基礎, 故於此可將此二公理補齊, 並順勢引入一般積集的嚴格定義.

公理 3.4.1 (替代公理) 給定任意命題公式 $P(x,y)$, 若 P 給出了一個單值的對應規則 (即對任意 x, 最多存在一個 y 使得 $P(x,y)$ 爲眞), 則對於任意集合 A, 必存在一個集合 B, 其元素恰爲 A 中元素透過 P 所對應出的對象, 即

$$\forall\, A,\forall\, P,[\forall\, x,\exists\,!\, y,[P(x,y)]],\exists\, B,\big[\forall\, y,[(y\in B)\iff\exists\, x,[(x\in A)\wedge P(x,y)]]\big].$$

註記 3.4.2 替代公理確保了前面所提的「指標族」$\{A_i\}_{i\in I}$ 確實是一個合法的集合. 這是因爲可以將指標集 I 視爲定義域, 透過命題公式 (而非預先存在的映射集合) 將每個指標 $i\in I$ 對應到集合 A_i. 替代公理便保證了這一切 A_i 所聚集而成的族必定是一個集合, 而非引發悖論的眞類.

注意 3.4.3 直觀而言, 替代公理的核心精神可以通俗地理解爲:「一個集合的像必然也是一個集合」. 初學者常會試圖將其表述爲:「若 A 爲集合, 且存在滿射 $f:A\to B$, 則 B 也是集合」. 雖然此說法在精神上完全正確, 但在嚴格的公理化體系中卻存在語病. 因爲當寫出映射 $f:A\to B$(或 $f\in B^A$) 時, 在定義上便已預設了對應域 B 是一個合法存在的集合. 替代公理的眞正價值在於: 當只有一個已知集合 A, 且對應規則是由「命題公式」給出 (此時目標範圍大到是整個眞類, 而非某個已知集合) 時, 該公理保證了被 A 中元素對應到的所有對象, 能夠被安全地「圈」起來, 成爲一個合法的集合.

既然確立了指標族的集合地位, 接著便可將有限積集推廣至任意指標集 I 的情形. 在有限積集中, n 元組實質上可視爲以指標集 $\{1,2,\dots,n\}$ 爲定義域的映射; 同理, 任意指標族的一般積集亦可透過映射來嚴密刻畫.

定義 3.4.4 已知一族集合 $\{A_i\}_{i\in I}$, 令 $A=\bigcup_{i\in I}A_i$. 定義此族集合的**一般積集** (或**一般卡氏積**) 爲

$$\prod_{i\in I}A_i=\{f\in A^I:\forall\, i\in I, f(i)\in A_i\}.$$

注意 3.4.5 在文獻與實際的數學書寫中, 對於積集中的映射 $f \in \prod_{i\in I} A_i$, 非常習慣將 $f(i)$ 記作 x_i, 並將整個映射 f 簡記爲 $(x_i)_{i\in I}$. 此記號的優勢在於: 它直觀地將映射 f 視爲一組由指標集 I 所索引的「廣義元組」, 完美呼應了有限情形中 $(a_1, a_2, \ldots, a_n)$ 的形式. 採用此記號, 一般積集即可表爲

$$\prod_{i\in I} A_i = \{(x_i)_{i\in I} : \forall\, i \in I, x_i \in A_i\}.$$

註記 3.4.6 已知集合 A, 可遞迴地定義其有限次積集爲 $A^{n+1} = A^n \times A$, 其中整數 $n \geq 1$. 而對於一般的指標集 I, 若參與積集運算的每一項皆爲相同的集合 A, 則定義

$$A^{|I|} = \prod_{i\in I} A,$$

這直觀上表示了「I 那麼多」個 A 自身的積集.

註記 3.4.7 需特別留意的是, 依據前文對一般積集的嚴格定義, 當族中所有集合皆爲 A 時, 其積集 $\prod_{i\in I} A$ 實質上即爲所有從 I 映射至 A 的映射全體. 因此, 這裡引入的符號 $A^{|I|}$, 與前文所定義的映射空間 A^I 在集合論的本質上是完全一致的.

觀察一般積集的定義, 若集族中存在某個 $k \in I$ 使得 $A_k = \varnothing$, 則顯然不可能存在映射 f 能滿足 $f(k) \in A_k$, 故此時必然有 $\prod_{i\in I} A_i = \varnothing$. 然而, 反過來說, 若對於所有的 $i \in I$, 皆有 $A_i \neq \varnothing$, 其積集 $\prod_{i\in I} A_i$ 是否必定非空? 這在指標集 I 爲無窮集時, 並非其他公理所能保證, 必須仰賴最後一條核心公理來確立.

公理 3.4.8 (選擇公理) 對於任意由非空集合構成的族 $\{A_i\}_{i\in I}$(即對所有 $i \in I$, 皆有 $A_i \neq \varnothing$), 必存在至少一個滿足對所有 $i \in I$, 皆有 $f(i) \in A_i$ 的映射 $f \in (\bigcup_{i\in I} A_i)^I$. 換言之, 其一般積集非空:

$$\prod_{i\in I} A_i \neq \varnothing,$$

或

$$\forall\, I, \left[\varnothing \notin I \implies \exists\, f, \left[\left(f \in \left(\bigcup I\right)^I\right) \wedge (\forall\, X, [X \in I \implies f(X) \in X])\right]\right].$$

註記 3.4.9 在此表述中, 由於映射 f 能從每一個非空集合 $X \in I$ 中確實「選擇」出一個代表元素 $f(X)$, 故 f 被稱爲集族 I 上的**選擇函數**. 選擇公理保證了, 即便集族 I 包含無窮多個集合, 這樣的選擇函數依然存在.

註記 3.4.10 選擇公理直觀上相當於宣稱: 即使面臨無窮多個非空集合, 依然可以同時從每個集合 A_i 中「選擇」出一個元素 x_i, 並將這些被選出的元素組裝成一個廣義元組 $(x_i)_{i\in I}$. 它是現代數學中證明存在性 (如線性空間必有基、任何集合皆可良序化等) 不可或缺的基石.

定義 3.4.11 設 $\{A_i\}_{i\in I}$ 是一族集合, 固定 $i \in I$, 映射

$$\pi_i : \prod_{j\in I} A_j \longrightarrow A_i \quad (x_j)_{j\in I} \longmapsto x_i$$

稱爲 $\prod_{i\in I} A_i$ 在 A_i 上的**投影映射**.

注意 3.4.12 在定義映射時 (見定義 3.1.2), 並沒有保證 B^A 是一個集合, 實際上這是需要證明的.

命題 3.4.13 若 A 和 B 均爲集合, 則 B^A 亦爲集合.

證明 留給讀者作爲練習. 提示: B^A 的一切元素均爲 $A \times B$ 的子集. □

命題 3.4.14 設 $\{A_i\}_{i\in I}$ 及 $\{B_i\}_{i\in I}$ 爲指標集相同的兩族集合, 則

$$\left(\prod_{i\in I} A_i\right) \cap \left(\prod_{i\in I} B_i\right) = \prod_{i\in I} (A_i \cap B_i).$$

證明 任予 x,

$$\begin{aligned}(x_i)_{i\in I}\in\left(\prod_{i\in I}A_i\right)\cap\left(\prod_{i\in I}B_i\right) &\iff \left((x_i)_{i\in I}\in\prod_{i\in I}A_i\right)\wedge\left((x_i)_{i\in I}\in\prod_{i\in I}B_i\right)\\ &\iff (\forall\, i\in I, x_i\in A_i)\wedge(\forall\, i\in I, x_i\in B_i)\\ &\iff \forall\, i\in I, ((x_i\in A_i)\wedge(x_i\in B_i))\\ &\iff \forall\, i\in I, x_i\in A_i\cap B_i\\ &\iff (x_i)_{i\in I}\in\prod_{i\in I}(A_i\cap B_i)\,.\end{aligned}$$

因此, 等式得證. □

命題 3.4.15 設 $\{A_i\}_{i\in I}$ 及 $\{B_i\}_{i\in I}$ 爲指標集相同的兩族集合, 則

$$\left(\prod_{i\in I}A_i\right)\cup\left(\prod_{i\in I}B_i\right)\subseteq\prod_{i\in I}(A_i\cup B_i).$$

證明 任予 $x=(x_i)_{i\in I}\in\left(\prod_{i\in I}A_i\right)\cup\left(\prod_{i\in I}B_i\right)$, 依聯集的定義, 有

$$(x_i)_{i\in I}\in\prod_{i\in I}A_i\quad\text{或}\quad(x_i)_{i\in I}\in\prod_{i\in I}B_i.$$

分成以下兩種情形討論:

- 若 $(x_i)_{i\in I}\in\prod_{i\in I}A_i$, 則對所有的 $i\in I$, 皆有 $x_i\in A_i$. 依聯集的定義, 必然有 $x_i\in A_i\cup B_i$, 從而 $(x_i)_{i\in I}\in\prod_{i\in I}(A_i\cup B_i)$.
- 若 $(x_i)_{i\in I}\in\prod_{i\in I}B_i$, 則對所有的 $i\in I$, 皆有 $x_i\in B_i$. 依聯集的定義, 亦有 $x_i\in A_i\cup B_i$, 從而 $(x_i)_{i\in I}\in\prod_{i\in I}(A_i\cup B_i)$.

綜上所述, 無論何種情形皆有 $x\in\prod_{i\in I}(A_i\cup B_i)$, 故包含關係得證. □

注意 3.4.16 一般而言, 上述命題中的包含關係是嚴格的 (即通常不相等). 例如取 $A_1=\{0\}, A_2=\{0\}$ 與 $B_1=\{1\}, B_2=\{1\}$, 則 $(0,1)$ 屬於右式, 但不屬於左式. 讀者切勿將交集的性質錯誤類推至聯集.

命題 3.4.17 設 $\{A_i\}_{i\in I}$ 及 $\{B_i\}_{i\in I}$ 爲指標集相同的兩族集合. 若 $\prod_{i\in I}A_i\neq\varnothing$, 則

$$\prod_{i\in I}A_i\subseteq\prod_{i\in I}B_i\iff\forall\, i\in I, A_i\subseteq B_i.$$

證明 充分性: 任予 $x=(x_i)_{i\in I}\in\prod_{i\in I}A_i$. 依積集的定義, 對所有的 $i\in I$ 皆有 $x_i\in A_i$. 因已知 $\forall i\in I, A_i\subseteq B_i$, 故 $\forall\, i\in I$, $x_i\in B_i$. 再次依積集的定義, 可得 $(x_i)_{i\in I}\in\prod_{i\in I}B_i$.

必要性: 設 $\prod_{i\in I}A_i\subseteq\prod_{i\in I}B_i$. 因 $\prod_{i\in I}A_i\neq\varnothing$, 故存在至少一個元素 $a=(a_i)_{i\in I}\in\prod_{i\in I}A_i$. 任予 $k\in I$ 及任予 $y\in A_k$, 構造一個新的族元素 $x=(x_i)_{i\in I}$ 如下:

$$x_i=\begin{cases}y, & i=k,\\ a_i, & i\neq k.\end{cases}$$

顯然, 對於所有 $i\in I$, 皆有 $x_i\in A_i$, 故 $x\in\prod_{i\in I}A_i$. 依前提 $\prod_{i\in I}A_i\subseteq\prod_{i\in I}B_i$, 必然有 $x\in\prod_{i\in I}B_i$. 這意味著 x 的每一個分量皆屬於相應的 B 集合, 特別地, 第 k 個分量 $x_k\in B_k$. 由於 $x_k=y$, 即得 $y\in B_k$. 依 y 的任意性, 可得 $A_k\subseteq B_k$. 再依 k 的任意性, 即得 $\forall\, i\in I, A_i\subseteq B_i$. □

注意 3.4.18 若不加上 $\prod_{i\in I}A_i\neq\varnothing$ 的前提, 則原等價關係將未必成立. 例如令 $I=\{1,2\}$, $A_1=\varnothing, A_2=\{0\}$ 及 $B_1=\{1\}, B_2=\varnothing$. 此時, $\prod_{i\in I}A_i=\varnothing\subseteq\varnothing=\prod_{i\in I}B_i$ 爲眞命題, 但 $A_2\subseteq B_2$ 爲假命題.

3.5 運算

定義 3.5.1 設有集合 X,Y,Z. 若 $*\in Z^{X\times Y}$, 則稱 $*$ 是自 X 和 Y 至 Z 的**二元運算**, 簡稱**運算**. 對於 $*(x,y)=z$, 記 $x*y=z$.

定義 3.5.2 若 $*$ 是自 X 和 Y 至 Z 的二元運算, 定義

$$\bullet : Y\times X\longrightarrow Z,\quad (y,x)\longmapsto \bullet(y,x)=y\bullet x:=x*y,$$

稱爲 $*$ 的**反運算**.

註記 3.5.3 雖然二元運算 $X\times Y\to Z$ 是用映射來定義的, 但是比起映射常用的字母, 如 f,g,h 等, 習慣上更常用符號「$+,\times,\cdot,*,\oplus,\otimes,\odot,\boxplus,\boxtimes,\boxdot,\wedge,\vee$」等來表示運算, 並寫在 X 和 Y 的元素之間.

定義 3.5.4 若 $*\in X^{X\times X}$, 則稱 $*$ 爲 X 上的**封閉二元運算**, 簡稱**封閉運算**. 若 $*\in X^{(X^n)}$, 則稱 $*$ 爲 X 上的 n **元封閉運算**.

註記 3.5.5 所謂封閉性, 是指無論如何運算, 所得元素皆不會脫離給定的集合. 例如 $\mathbb{R}$ 上傳統的加法及、減法、乘法及除法是其上的封閉運算, 集合的交、聯、補也是封閉運算, 而 $\mathbb{Z}$ 上的除法不是其上的封閉運算. 另外, 對複數取共軛是一元運算, 對三個點求重心是三元運算, 對矩陣取轉置也是一元運算.

定義 3.5.6 運算 $*\in Z^{X\times Y}$ 也稱爲 X 在 Y 上至 Z 的一個**左作用**, 亦稱爲 Y 在 X 上至 Z 的一個**右作用**, 同樣記作 $*(x,y)=x*y$.

例 3.5.7 (1) 線性空間或模的數乘是一個作用. 詳言之, 若 R 是環, M 是 R 模, 則

$$\cdot : R\times M\longrightarrow M,\quad (r,m)\longmapsto r\cdot m$$

是 R 在 M 上的左作用.

(2) $m\times n$ 階矩陣的全體在 n 維行向量上有左作用, 在 m 維列向量上有右作用.

(3) {旋轉, 平移, 反射} 在平面上有作用.

(4) Y^X 在 X 上至 Y 有作用, 其作用即爲「代入」, 即對於 $f\in Y^X$, $x\in X$, 有

$$*(f,x)=f*x:=f(x).$$

註記 3.5.8 任何 X 在 Y 至 Z 上的作用可視爲自 X 至 Z^Y 的映射. 比如說, 對於 $*\in Z^{X\times Y}$, 有

$$F:X\longrightarrow Z^Y,\quad x\longmapsto F(x):=[x*-:y\longmapsto x*y],$$

即 $\forall\, y\in Y$, $F(x)(y):=x*y$. 反過來, 對於映射 $g\in (Z^Y)^X$, 其對應於作用

$$\star : X\times Y\longrightarrow Z,\quad (x,y)\longmapsto x\star y:=(g(x))\,(y).$$

一般上, 任何作用 $\star\in Z^{X\times Y}$ 都自動對應於映射 $f_\star\in (Z^Y)^X$. 詳言之, 兩映射族 $Z^{X\times Y}$ 及 $(Z^Y)^X$ 之間可建立雙射.

定義 3.5.9 設 $*$ 是 X 上的封閉運算, 若

$$\forall\, x,y,z\in X, (x\cdot y)\cdot z=x\cdot(y\cdot z),$$

則稱 $*$ 滿足或具有**結合律**.

註記 3.5.10 結合律給出爲 X 中的一串元素作 $*$ 運算略去括號的權利. 不具有結合律的一串算式應寫作如 $(a\cdot(b\cdot c))\cdot d$ 的形式, 例如 $\mathbb{R}^3$ 中的叉積.

例 3.5.11 $\mathbb{R}$ 上的加運算及乘運算、映射的合成運算具有結合律.

定義 3.5.12 設 $*$ 是 X 上的封閉運算, 若

$$\forall\, x, y \in X, x \cdot y = y \cdot x,$$

則稱 $*$ 滿足或具有**交換律**.

註記 3.5.13 交換律給出爲 X 中一串元素作 $*$ 運算忽略順序的權利. 即使 $*$ 不具有結合律, 亦能對一串算式略作化簡, 比如

$$(a \cdot (b \cdot c)) \cdot d = ((b \cdot c) \cdot a) \cdot d).$$

定義 3.5.14 (單位律; 么律) 設 $*$ 是 X 上的封閉運算, 若

$$\exists\, \varepsilon \in X, \forall\, x \in X, x * \varepsilon = \varepsilon * x = x,$$

則稱 X 有 $*$ 的**單位元**或**么元** ε.

例 3.5.15 $\mathbb{R}$ 中的 0 和 1 分別爲加法和乘法的單位元. 恆等映射爲映射族中合成運算的單位元. 零矩陣是矩陣加法的單位元 (故也有人稱之爲加法單位矩陣), 單位矩陣是矩陣乘法的單位元. 零向量是向量空間中加法的單位元.

命題 3.5.16 單位元若存在則必唯一.

證明 若 $\varepsilon, \varepsilon'$ 均爲 $*$ 的單位元, 則 $\varepsilon' = \varepsilon' * \varepsilon = \varepsilon$. □

定義 3.5.17 (零律) 設 $*$ 是 X 上的封閉運算, 若

$$\exists\, o \in X, \forall\, x \in X, x * o = o * x = o,$$

則稱 X 有 $*$ 的**零元** o.

例 3.5.18 $\mathbb{R}$ 中的 0 是乘法的零元, 零矩陣是矩陣乘法的零元.

定義 3.5.19 設 X 上有兩封閉運算 $\oplus, \otimes$, 若

$$\forall\, x, y, z \in X, x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z),$$

則稱 $\otimes$ 對 $\oplus$ 有**左分配律**; 若

$$\forall\, x, y, z \in X, (y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x),$$

則稱 $\otimes$ 對 $\oplus$ 有**右分配律**. 對於同時滿足左右兩種分配律的運算, 稱其滿足對於同時滿足左右兩種分配律的運算, 稱其滿足分配律.

例 3.5.20 集合的交運算對聯運算有分配律, 聯運算對交運算也有分配律.

定義 3.5.21 設 $* \in Z^{X \times Y}$ 爲一運算, 若

$$\forall\, x \in X, \forall\, y, y' \in Y, x * y = x * y' \iff y = y',$$

則稱 $*$ 滿足**左消去律**; 若

$$\forall\, x, x' \in X, \forall\, y \in Y, x * y = x' * y \iff x = x',$$

則稱 $*$ 滿足**右消去律**. 對於同時滿足左右兩種消去律的運算, 稱其滿足**消去律**.

例 3.5.22 矩陣環不滿足消去律, 例如

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

但

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}.$$

3.6 交換圖

所謂**交換圖**, 是以集合爲頂點、有向邊爲映射, 且複合連接任意兩集合的不同路徑上的映射所得的結果均相等的圖.

例 3.6.1 設有集合 A, B, C 及映射 f, g, h, 如下圖:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow^{h} & \downarrow{\scriptstyle g} \\ & & C \end{array}$$

當 $h = g \circ f$ 時, 上圖可交換.

例 3.6.2 設有集合 A, B, C, D 及映射 f, g, φ, ψ, 如下圖:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle g} \\ D & \xrightarrow[\psi]{} & C \end{array}$$

當 $g \circ f = \psi \circ \varphi$ 時, 上圖可交換.

例 3.6.3 設有若干個集合及映射, 如下圖:

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{h} & C \\ {\scriptstyle \varphi}\downarrow & \searrow^{\rho} & \downarrow{\scriptstyle g} & \nearrow_{\sigma} & \\ D & \xrightarrow[\psi]{} & E & & \end{array}$$

當 $g \circ f = \rho = \psi \circ \varphi$ 且 $h \circ f = \sigma \circ g \circ f = \sigma \circ \rho = \sigma \circ \psi \circ \varphi$ 且 $h = \sigma \circ g$ 時, 上圖可交換.

命題 3.6.4 (積集的泛性質) 給定一族集合 $\{A_i\}_{i \in I}$, 設 $A = \prod_{i \in I} A_i$, $\pi_i \in (A_i)^A$ 爲映至 A_i 上的投影映射, 則對一切集合 X 及任一族映射 $\{\psi_i \in (A_i)^X : i \in I\}$, 皆存在唯一的一個映射 $\rho \in A^X$, 對所有 $i \in I$, 都有 $\pi_i \circ \rho = \psi_i$, 即下圖可交換.

$$\begin{array}{ccc} X & & \\ {\scriptstyle \rho}\vdots & \searrow^{\psi_i} & \\ A & \xrightarrow[\pi_i]{} & A_i \end{array}$$

證明 定義映射

$$\rho : X \longrightarrow \prod_{i \in I} A_i, \quad x \longmapsto (\psi_i(x))_{i \in I},$$

則對一切 $i \in I$, 任予 $x \in X$, 都有

$$\pi_i \circ \rho(x) = \pi_i \left((\psi_i(x))_{i \in I} \right) = \psi_i(x).$$

若有映射 $\sigma \in A^X$ 亦滿足 $\forall\, i \in I, \pi_i \circ \sigma = \psi_i$, 則對所有 $x \in X$, 記 $\sigma(x) = (y_j)_{j \in I}$, 都有

$$y_i = \pi_i \circ \sigma(x) = \psi_i(x).$$

因此, 對所有 $x \in X$, 皆有

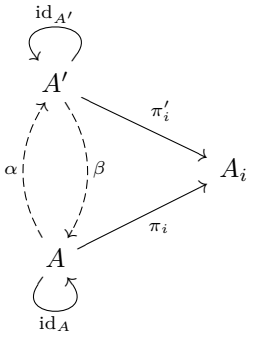
$$\sigma(x) = (y_j)_{j \in I} = (\psi_j(x))_{j \in I} = \rho(x),$$

故 $\sigma = \rho$, 唯一性得證. □

系理 3.6.5 滿足命題 3.6.4 的任兩對 $(A,\{\pi_i\}_{i\in I})$ 之間可建立雙射. 換言之, 若 $(A,\{\pi_i\}_{i\in I})$ 及 $(A',\{\pi_i\}_{i\in I})$ 都滿足命題 3.6.4 所述之泛性質, 則存在映射 $\alpha\in(A')^A$ 及 $\beta\in A^{A'}$, 使得對一切 $i\in I$, 均有

$$\alpha\circ\beta=\mathrm{id}_{A'},\quad \beta\circ\alpha=\mathrm{id}_A,\quad \pi_i\circ\beta=\pi'_i,\quad \pi'_i\circ\alpha=\pi_i,$$

即下圖爲交換圖:

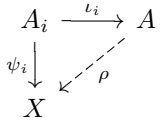


證明 對於 $X=A'$ 及 $\psi_i=\pi'_i$ $(i\in I)$, 依命題 3.6.4, 存在對一切 $i\in I$ 都滿足 $\pi_i\circ\beta=\pi'_i$ 的 $\beta\in A^{A'}$. 同理, 交換 A 與 A', 可知存在對一切 $i\in I$ 都滿足 $\pi'_i\circ\alpha=\pi_i$ 的 $\alpha\in(A')^A$. 再取 $X=A$ 及 $\psi_i=\pi_i$ $(i\in I)$, 顯然 id_A 是滿足條件的一個映射, 而 $\rho=\beta\circ\alpha$ 也滿足

$$\pi_i\circ\rho=\pi_i\circ\beta\circ\alpha=\pi'_i\circ\alpha=\pi_i=\psi_i.$$

依唯一性, 得 $\mathrm{id}_A=\beta\circ\alpha$. 同理可證 $\mathrm{id}_{A'}=\alpha\circ\beta$. □

命題 3.6.6 (無交聯集的泛性質) 給定一族互不相交的集合 $\{A_i\}_{i\in I}$, 設 $A=\coprod_{i\in I}A_i$, $\iota_i\in A^{A_i}$ 爲包含映射, 則對一切集合 X 及任一族映射 $\{\psi_i\in X^{A_i}:i\in I\}$, 皆存在唯一的一個映射 $\rho\in X^A$, 對所有 $i\in I$, 都有 $\rho\circ\iota_i=\psi_i$, 即下圖可交換.



證明 定義映射

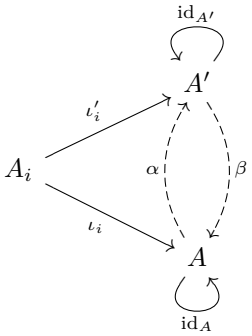
$$\rho:\coprod_{i\in I}A_i\longrightarrow X,\quad A_i\ni a_i\longmapsto\psi_i(a).$$

如同命題 3.6.4, 同樣可以證明 ρ 是唯一滿足條件的映射. □

系理 3.6.7 滿足命題 3.6.6 的任兩對 $(A,\{\iota_i\}_{i\in I})$ 之間可建立雙射. 換言之, 若 $(A,\{\iota_i\}_{i\in I})$ 及 $(A'.\{\iota'_i\}_{i\in I})$ 都滿足命題 3.6.6 所述之泛性質, 則存在映射 $\alpha\in(A')^A$ 及 $\beta\in A^{A'}$, 使得對一切 $i\in I$, 均有

$$\alpha\circ\beta=\mathrm{id}_{A'},\quad \beta\circ\alpha=\mathrm{id}_A,\quad \beta\circ\iota_i=\iota'_i,\quad \alpha\circ\iota'_i=\iota_i,$$

即下圖爲交換圖:



證明 請讀者自行練習. □

單元 4

關係

4.1 關係的定義

定義 4.1.1 給定兩集合 X, Y, 若 $R \subseteq X \times Y$, 則稱 R 爲 X 和 Y 上的**二元關係**, 簡稱**關係**. 若 $(x, y) \in R$, 則記 xRy, 否則記作 $x \not R y$. 若 $X = Y$, 則稱 R 爲 X 上的**二元關係**或**關係**.

註記 4.1.2 不難看出, 映射 $f \in Y^X$ 是 X 和 Y 上的關係, 但反過來, 關係未必是一個映射.

註記 4.1.3 關係 $R \subseteq X \times Y$ 可看成 R 的特徵映射:

$$\chi_R : X \times Y \longrightarrow \{0, 1\} \qquad (x, y) \longmapsto \begin{cases} 1, & (x, y) \in R \text{ (即} xRy), \\ 0, & (x, y) \notin R \text{ (即} x \not R y), \end{cases}$$

也就是把 $\{0, 1\}$ 視爲 {有關係, 無關係}, 再以一個映射來指定.

定義 4.1.4 設 X, Y, Z 爲三個集合, $S \subseteq X \times Y$, $R \subseteq Y \times Z$, 則稱

$$R \circ S := \{(x, z) \in X \times Z : \exists\, y \in Y, (x, y) \in S, (y, z) \in R\}$$

爲 R 與 S 上的**合成關係**.

定義 4.1.5 設 $R \subseteq X \times Y$, 則稱

$$R^{-1} := \{(y, x) : (x, y) \in X \times Y\}$$

爲 R 的**反關係**.

例 4.1.6 (1) $\mathbb{R}$ 上的 $=, <, \leq, >, \geq, \neq$ 均可視爲 $\mathbb{R}$ 上的某些指定的子集對 (即關係).

(2) 平面幾何中, 直線相交、平行, 曲線相交、相切、相離, 也可看作對平面上的子集對的指定. 同理, 空間中的曲線、曲面等幾何對象亦有類似的刻畫.

定義 4.1.7 設 $R \subseteq X \times Y$. 若 $R = \varnothing$, 則稱 R 爲**空關係**; 若 $R = X \times Y$, 則稱 R 爲**全關係**. 當 $Y = X$, 且 $R = \{(x, x) : x \in X\} = \{(x, y) \in X \times X : x = y\}$ 時, 稱 R 爲 X 上的**恆等關係**或**單位關係**.

定義 4.1.8 設 R 爲 X 上的二元關係.

(1) 若 $\forall\, x \in X$, xRx, 則稱 R **自反**或**反身**.

(2) 若 $\forall\, x \in X$, $x \not R x$, 則稱 R **反自反**或**反反身**.

(3) 若 $\forall\, x, y \in X$, $xRy \iff yRx$, 則稱 R **對稱**.

(4) 若 $\forall\, x, y \in X$, $xRy, yRx \implies x = y$, 則稱 R **反對稱**.

(5) 若 $\forall\, x, y \in X$, $xRy \implies x \not R y$, 則稱 R **不對稱**.

(6) 若 $\forall\, x, y, z \in X$, $xRy, yRz \implies xRz$, 則稱 R **傳遞**或**遞移**.

例 4.1.9 (1) 恆等關係、$\mathbb{R}$ 上的 $=, \leq, \geq$ 都是自反的.

(2) $\mathbb{R}$ 上的 $\neq, <, >$ 都是反自反的.

(3) $\mathbb{R}$ 上的 $=, \neq$, 以及 $\mathbb{Z}$ 上的同餘運算 $\equiv$ 都是對稱的.

(4) $\mathbb{R}$ 上的 $=, \leq, \geq$ 都是反對稱的、傳遞的.

(5) 空關係具有對稱性、反對稱性、傳遞性.

(6) 全關係具有自反性、對稱性、傳遞性.

(7) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2 + 4\}$ 給出了 $\mathbb{R}$ 上的一個反自反關係.

註記 4.1.10 設 X 的對角集爲 $D_X = \{(x, x) : x \in X\}$. 不難看出:

(1) R 是自反的的充要條件爲 $D_X \subseteq R$;

(2) R 是恆等關係的充要條件爲 $D_X = R$.

定理 4.1.11 設 $R \subseteq X \times X$.

(1) R 是對稱的的充要條件爲 $R = R^{-1}$.

(2) R 是反對稱的的充要條件爲 $R \cap R^{-1} \subseteq D_X$.

(3) R 是傳遞的的充要條件爲 $R \circ R \subseteq R$.

證明 (1) 設 R 具有對稱性, 則

$$(x, y) \in R \iff (y, x) \in R \iff (x, y) \in R^{-1},$$

因此 $R = R^{-1}$.

反過來, 設 $R = R^{-1}$, 則 $(x, y) \in R \iff (x, y) \in R^{-1} \iff (y, x) \in R$, 因此 R 具有對稱性.

(2) 設 R 反對稱, 則

$$\begin{aligned}(x, y) \in R \cap R^{-1} &\implies (x, y) \in R \quad \text{且} \quad (x, y) \in R^{-1} \\ &\implies (x, y) \in R \quad \text{且} \quad (y, x) \in R \\ &\implies x = y \quad (\text{根據 } R \text{ 的反對稱性}) \\ &\implies (x, y) = (x, x) \in D_X.\end{aligned}$$

因此, $R \cap R^{-1} \subseteq D_X$.

反過來, 設 $R \cap R^{-1} \subseteq D_X$. 若 $(x, y) \in R$ 且 $(y, x) \in R$, 則 $(x, y) \in R \cap R^{-1} \subseteq D_X$, 由此得 $x = y$, 從而 R 是反對稱的.

(3) 設 R 具有傳遞性. 若 $(x,y)\in R\circ R$, 則存在滿足 $(x,z)\in R$ 且 $(z,y)\in R$ 的 $z\in X$, 依 R 的傳遞性, 得 $(x,y)\in R$. 因此, $R\circ R\subseteq R$.

反過來, 設 $(x,z),(z,y)\in R$, 則依合成關係的定義, 有 $(x,y)\in R\circ R\subseteq R$, 故 R 具有遞移性.

□

命題 4.1.12 設 R,S 爲 X 上的關係, 那麼:

(1) $(R^{-1})^{-1}=R$;

(2) $R\subseteq S$ 的充要條件爲 $R^{-1}\subseteq S^{-1}$;

(3) $(R\cup S)^{-1}=R^{-1}\cup S^{-1}$, $(R\cap S)^{-1}=R^{-1}\cap S^{-1}$;

(4) $R\cup R^{-1}$ 及 $R\cap R^{-1}$ 均有對稱性.

證明 證明給讀者留作習題. □

註記 4.1.13 事實上, 一個集合 X 上的關係 R 可用**關係圖**或**關係矩陣**來刻畫, 但本文不討論, 感興趣的讀者可參考 [5].

4.2 關係的閉包

定義 4.2.1 設 R 爲 X 上的關係. 若自反 (相應地, 對稱, 傳遞) 關係 S 滿足: 對任何自反 (相應地, 對稱, 傳遞) 關係 T,

$$R\subseteq T\iff S\subseteq T,$$

則稱 S 爲 R 的**自反閉包** (相應地, **對稱閉包**, **傳遞閉包**).

命題 4.2.2 設 R 爲 X 上的關係, 則其自反 (相應地, 對稱, 傳遞) 閉包 S 存在且唯一, 並滿足

$$S=\bigcap_{T\supseteq R}T\supseteq R,$$

其中 T 遍及一切自反 (相應地, 對稱, 傳遞) 關係. 將 R 的自反 (相應地, 對稱, 傳遞) 閉包記作 $r(R)$(相應地, $s(R),t(R)$).

證明 不難驗證, 自反 (相應地, 對稱, 傳遞) 關係的任意交仍是自反 (相應地, 對稱, 傳遞) 關係, 故對於關係 R,

$$S=\bigcap_{T\supseteq R}T\supseteq R$$

是一個自反 (相應地, 對稱, 傳遞) 關係, 從而對任何自反 (相應地, 對稱, 傳遞) 關係 T,

$$R\subseteq T\iff S\subseteq T.$$

因此, 自反 (相應地, 對稱, 傳遞) 閉包存在.

若有兩個自反 (相應地, 對稱, 傳遞) 閉包 S_1 及 S_2, 則

$$R\subseteq S_2\iff S_1\subseteq S_2,\quad R\subseteq S_1\iff S_2\subseteq S_1,$$

從而 $S_1=S_2$. □

命題 4.2.3 設 R 爲 X 上的關係, 則 $R\subseteq\langle R\rangle$, 此處 $\langle R\rangle$ 表示 $r(R),s(R)$ 或 $t(R)$.

證明 依定義, 有

$$R \subseteq \langle R\rangle \iff \langle R\rangle \subseteq \langle R\rangle.$$

顯而易見, 右邊爲眞. □

命題 4.2.4 (單調性) 若 S,T 爲 X 上的關係, 且 $S \subseteq T$, 則 $\langle S\rangle \subseteq \langle T\rangle$, 此處 $\langle R\rangle$ 表示 $r(R), s(R)$ 或 $t(R)$ $(R = S$ 或 $T)$.

證明 依命題 4.2.3,

$$S \subseteq T \implies S \subseteq \langle T\rangle \iff \langle S\rangle \subseteq \langle T\rangle.$$

□

命題 4.2.5 (冪等性) 若 S 爲 X 上的關係, 則 $\langle\langle S\rangle\rangle = \langle S\rangle$, 此處 $\langle S\rangle$ 表示 $r(S), s(S)$ 或 $t(S)$.

證明 不難看出,

$$\langle S\rangle \subseteq \langle S\rangle \iff \langle\langle S\rangle\rangle \subseteq \langle S\rangle.$$

另一方向由命題 4.2.3 即得. □

命題 4.2.6 設 R 爲 X 上的關係, 則 R 爲自反 (或對稱, 或傳遞) 關係的充要條件爲 $R = r(R)$ (或 $s(R), t(R)$).

證明 充分性: $r(R)$ (或 $s(R), t(R)$) 已經是自反關係 (或對稱關係, 傳遞關係), 故 $R = r(R)$ (或 $s(R), t(R)$) 表示 R 即爲自反關係 (或對稱關係, 傳遞關係).

必要性: 若 R 爲自反關係 (或對稱關係, 傳遞關係), 則依定義, 即有 $R = r(R)$ (或 $s(R), t(R)$). □

命題 4.2.7 設 R 爲 X 上的關係, 記 id 爲 X 上的恆等關係, 定義 $R^{n+1} = R^n \circ R$ $(n \in \mathbb{N})$, 則

(1) $r(R) = R \cup \mathrm{id}$;

(2) $s(R) = R \cup R^{-1}$;

(3) $t(R) = \bigcup\limits_{k=1}^{+\infty} R^k$.

命題 4.2.8 僅證明 (3), 餘者留給讀者作爲練習. 設 T 爲包含 R 的傳遞關係. 由於

$$(x,y) \in R, (y,z) \in R \implies (x,z) \in T,$$

因此 $R^2 \subseteq T$, 依此類推, 可得 $R^k \subseteq T$. 考慮 $R' := \bigcup_{k=1}^{+\infty} R^k$, 令 $(x,y), (y,z) \in R'$, 則存在 i,j 使得 $(x,y) \in R^i$, $(y,z) \in R^j$, 於是存在 $a_1, \ldots, a_i, b_1, \ldots, b_j$, 使得

$$xRa_1Ra_2R \cdots Ra_iRyRb_1Rb_2R \cdots Rb_jRz,$$

從而 $(x,z) \in R^{i+j}$, 得 $(x,z) \in R'$.

4.3 等價關係

定義 4.3.1 設 $\sim$ 爲 X 上的關係. 若 $\sim$ 具有自反性、對稱性、傳遞性, 則稱 $\sim$ 是 X 上的**等價關係**. 對於 $x \in X$, 記

$$[x] := \{y \in X : x \sim y\},$$

稱爲 x 所在的**等價類**.

例 4.3.2 (1) 數論中的同餘是 $\mathbb{Z}$ 上的等價關係.

(2) 線性代數中, 相抵、合同、相似是 F 矩陣空間 $F^{m\times n}$ 上的等價關係.

命題 4.3.3 設 $\sim$ 爲 X 上的等價關係, $x,y\in X$, 則有

(1) $x\sim y \iff [x]=[y]$;

(2) $x\not\sim y \iff [x]\cap[y]=\varnothing$;

(3) $X=\bigcup_{x\in X}[x]$.

也就是說, 等價類或者相離, 或者相等.

證明 (1) 設 $x\sim y$, 則依 $\sim$ 的定義, 有

$$z\in[x] \iff x\sim z \iff y\sim z \iff z\in[y],$$

故 $[x]=[y]$.

(2) 設存在 $z\in[x]\cap[y]$, 則 $z\sim x$ 且 $z\sim y$, 故 $x\sim y$. 反過來看, 只要 $x\not\sim y$, 便有 $[x]\cap[y]=\varnothing$.
另一方面, 根據 (1), 有

$$x\sim y \iff [x]=[y] \implies [x]\cap[y]\neq\varnothing,$$

故反過來看, 只要 $[x]\cap[y]=\varnothing$, 便有 $x\not\sim y$.

(3) 顯而易見.

□

定義 4.3.4 設 $\mathcal{X}=\{X_\alpha\}_{\alpha\in I}$ 是集合 X 的一族子集. 若

(1) 對一切 $\alpha,\beta\in I$, 或者 $X_\alpha=X_\beta$, 或 $X_\alpha\cap X_\beta=\varnothing$;

(2) $X=\bigcup_{\alpha\in I}X_\alpha$,

則稱 $\mathcal{X}$ 爲 X 的**劃分**, 記作

$$X=\bigsqcup_{\alpha\in I}X_\alpha=\bigsqcup_{Y\in\mathcal{X}}Y.$$

命題 4.3.5 集合 X 上的等價關係和 X 的一個分劃相*互互逆*確定. 詳言之,

(1) 對於等價關係 $\sim$, 確定的劃分爲

$$\{[x]:x\in X\};$$

(2) 對於分劃 $\mathcal{X}$, 確定的等價關係爲

$$x\sim y \iff x,y \text{ 屬於 } \mathcal{F} \text{ 中的同一個元素},$$

且兩者*互逆*.

證明 依命題 4.3.3, 可知 $\{[x]:x\in X\}$ 是 X 的一個劃分, 故 (1) 成立.
設 X 有劃分 $\mathcal{X}$, 定義關係

$$xRy \iff \exists\, X_\alpha\in\mathcal{X},(x,y)\in X_\alpha.$$

顯然若 $x\in X_\alpha$, 則 $(x,x)\in X_\alpha$. 若 $(x,y)\in X_\alpha$, 則 $(y,x)\in X_\alpha$. 若 $(x,y)\in X_\alpha$, $(y,z)\in X_\beta$, 則 $\alpha=\beta$ 且 $(x,z)\in X_\alpha$. 因此, R 是 X 上的等價關係.

等價關係 $\sim$ 確定的劃分所決定的等價關係爲

$$x \sim' y \iff x, y \text{ 在同一等價類},$$

而 x 已經在 $[x]$ 之中了, 故等價於 $y \in [x]$, 等價於 $x \sim y$. 而劃分 $\mathcal{X}$ 確定的等價關係所決定的等價類爲

$$[x] = \{y \in X : y \text{ 和 } x \text{ 在同一類}\} = x \text{ 所在的那一類},$$

故 $\{[x] : x \in X\} = \mathcal{X}$. □

定義 4.3.6 設集合 X 上有等價關係 R, 定義

$$X/R = \{[x] : x \in X\},$$

稱爲 X 的**商集**.

若 $\{x_i\}_{i\in I} \subseteq X$ 滿足 $\{[x_i] : i \in I\} = X/R$, 且當 $i \neq j$ 時, $[x_i] \cap [x_j] = \varnothing$, 則稱 $\{x_i\}_{i\in I}$ 爲等價關係 R 的一組**代表元**. 對於 $y \in [x]$, 也稱 y 爲等價類 $[x]$ 的**代表元**.

例 4.3.7 設 $n \in \mathbb{N}$, $X = \mathbb{R}^{n+1} \setminus \{\mathbf{0}\}$, 定義關係 $\sim$: $\forall\, \mathbf{x}, \mathbf{y} \in X$

$$\mathbf{x} \sim \mathbf{y} \iff \exists\, \lambda \in \mathbb{R} \setminus \{0\}, \mathbf{x} = \lambda \mathbf{y}.$$

不難驗證 $\sim$ 是 $\mathbb{R}^{n+1} \setminus \{\mathbf{0}\}$ 上的等價關係, 並且對所有 $\mathbf{x} \in X$, 其等價類爲

$$[\mathbf{x}] = \{t\mathbf{x} : t \in \mathbb{R} \setminus \{0\}\}.$$

例 4.3.8 設 $X = \mathbb{S}^2 := \left\{\mathbf{x} \in \mathbb{R}^3 : \|\mathbf{x}\| = 1\right\}$ 爲幾何空間中的球面, 定義關係 $\sim$: $\forall\, \mathbf{x}, \mathbf{y} \in X$,

$$\mathbf{x} \sim \mathbf{y} \iff \mathbf{x} = \pm \mathbf{y},$$

即把對徑點 $\mathbf{x}, \mathbf{y}$ 以 $\mathbf{x} \sim \mathbf{y}$ 表示. 不難驗證 $\sim$ 是 $\mathbb{S}^2$ 上的等價關係, 並且對所有 $\mathbf{x} \in X$, 其等價類爲

$$[\mathbf{x}] = \{\mathbf{x}, -\mathbf{x}\}.$$

例 4.3.9 設 $n \in \mathbb{N} \cap [2, +\infty)$, 定義關係 $\sim$ 如下: $\forall\, m, m' \in \mathbb{Z}$,

$$m \sim m' \iff m \equiv m' \pmod{n} \iff \exists\, k \in \mathbb{N}, m = m' + nk.$$

顯然 $\sim$ 是 $\mathbb{Z}$ 上的等價關係, 並且對所有 $m \in \mathbb{Z}$, 其等價類爲

$$[m] = \{m + nk : k\mathbb{Z}\} = m + n\mathbb{Z}.$$

將 $[0], [1], [2], \ldots, [n-1]$ 稱爲 n 的**剩餘類**. 若 $m_0, m_1, \ldots, m_{n-1}$ 是 n 個整數, 並且其中任兩數都不在同一個剩餘類裡, 則稱此 n 數爲模 n 的一個**完全剩餘系**. 不難看出, n 個整數組成模 n 的一個完全剩餘系的充要條件爲兩兩對模 n 不同餘. 若一個模 n 的剩餘類中的數與 n 互質, 則稱之爲一個**與模 n 互質的剩餘類**. 在與模 n 互質的全部剩餘類中, 從每一類中各取一數所組成的數集稱爲模 n 的一個**簡化剩餘系**.

定義 4.3.10 設 $f \in Y^X$, 定義 X 上的關係

$$R = \{(x, y) \in X \times X : f(x) = f(y)\},$$

則 R 是 X 上的一個等價關係, 稱之爲 f 在 X 上誘導出的等價關係, 或 f 的**等價核**.

定義 4.3.11 設 $\sim$ 是 X 上的等價關係, 定義映射

$$\pi : X \to X/\sim, \quad x \longmapsto [x],$$

稱 π 爲由 X 至商空間 $X/\sim$ 的**自然映射**或**典範映射**.

命題 4.3.12 設 $\sim$ 是集合 X 上的等價關係, π 爲由 X 至 $X/\sim$ 的自然映射, 則 $\sim$ 爲 π 在 X 上誘導出的等價關係.

證明 設 $\sim'$ 爲 π 在 X 上誘導出的等價關係, 則

$$x \sim y \iff [x]=[y] \iff \pi(x)=\pi(y) \iff x \sim' y,$$

因此 $\sim=\sim'$. □

4.4 序關係

定義 4.4.1 設 $\leq$ 爲 X 上的關係. 若 $\leq$ 具有自反性及遞移性, 則稱其爲**預序關係**. 若預序 $\leq$ 還反對稱性, 則稱 $\leq$ 是 X 上的**偏序關係**, 稱 $(X,\leq)$ 爲**偏序集**.

定義 4.4.2 設集合 X 上有偏序關係 $\leq$. 若 X 中任兩元素**可比**. 即對所有 $x,y\in X$, 或者 $x\leq y$, 或者 $y\leq x$, 則稱 $\leq$ 爲 X 上的**全序關係**或**線性序關係**, $(X,\leq)$ 是**全序集**或**線性序集**.

例 4.4.3 (1) $\mathbb{R}$ 上的 $\leq$ 是全序關係.

(2) $\mathbb{N}$ 上的整除關係是偏序關係.

(3) 集合的包含關係是偏序關係.

註記 4.4.4 設 $(X,\leq)$ 爲偏序集, 約定符號如下:

$$\begin{aligned} a\geq b &\iff b\leq a,\\ a<b &\iff \begin{cases} a\leq b,\\ a\neq b,\end{cases}\\ a>b &\iff \begin{cases} a\geq b,\\ a\neq b.\end{cases}\end{aligned}$$

以及區間

$$\begin{aligned} [a,b] &:= \{x\in X : a\leq x\leq b\},\\ (a,b] &:= \{x\in X : a< x\leq b\},\\ [a,b) &:= \{x\in X : a\leq x< b\},\\ (a,b) &:= \{x\in X : a< x< b\}.\end{aligned}$$

註記 4.4.5 設 $(X,\leq)$ 是偏序集, 則 $<$ 是 X 上具有反自反性、不對稱性及遞移性, 稱之爲**嚴格偏序關序**.

定義 4.4.6 設 X,Y 爲兩偏序集, 定義積集 $X\times Y$ 上的**字典序**如下: 令 $(x_1,y_1),(x_2,y_2)\in X\times Y$,

$$(x_1,y_1)\leq(x_2,y_2) \iff x_1<x_2, \text{ 或 } [x_1=x_2 \text{ 且 } y_1\leq y_2].$$

注意 4.4.7 $\mathbb{C}$ 上可以定義字典序, 但無法從 $(\mathbb{R},\leq)$ 延伸定義、在與原本的實數系相容的情況下, 對所有複數定義全序. 事實上, 假如 $\mathbb{C}$ 上可定義全序, 則依虛數單位的定義, 有 $\mathrm{i}\neq 0$. 依可比性, 或者 $\mathrm{i}>0$, 或者 $\mathrm{i}<0$. 若 $\mathrm{i}>0$, 則當不等式兩邊同乘以 i 時, 不等號方向不變, 得 $-1>0$, 這與原本的 $(\mathbb{R},\leq)$ 不相容, 即矛盾. 若 $\mathrm{i}<0$, 則當不等式兩邊同乘以 i 時, 不等號方向改變, 得 $-1>0$, 同樣是矛盾.

定義 4.4.8 設 X, Y 爲兩偏序集, $f \in Y^X$. 若對任意 $x, y \in X$, 只要 $x \leq y$, 便有 $f(x) \leq f(y)$, 則稱 f **遞增**或**保序**. 若上述兩個「$\leq$」替換成「$<$」, 則稱 f **嚴格遞增**. 若 f 是雙射, 且對所有 $x, y \in X$,

$$x \leq y \iff f(x) \leq f(y),$$

則稱 f 是**同構映射**.

命題 4.4.9 設 X, Y 爲兩偏序集, $f \in Y^X$ 是同構映射, 則

$$x < y \iff f(x) < f(y).$$

證明 設 $x < y$, 則 $x \leq y$, 於是 $f(x) \leq f(y)$. 若 $f(x) = f(y)$, 則 $f(y) \leq f(x)$, 推得 $y \leq x$, 矛盾, 於是 $f(x) < f(y)$. 反之亦然. □

命題 4.4.10 設 X, Y 爲兩偏序集, $f \in Y^X$ 是雙射, 則 f 是同構映射的充要條件爲 f, f^{-1} 皆遞增.

證明 注意到, 對一切 $x \in X$, 都有 $x = f^{-1}(f(x))$. 因此, 依同構映射的定義, 可直接推得此結論. □

定義 4.4.11 設 $(X, \leq)$ 是偏序集.

(1) 若 $g \in X$, 且 $\forall\, x \in X$, $x \leq g$, 則稱 g 是 X 的**最大元**.

(2) 若 $l \in X$, 且 $\forall\, x \in X$, $l \leq x$, 則稱 l 是 X 的**最小元**.

(3) 若 $M \in X$ 滿足 $M \leq x \iff M = x$, 則稱 M 是 X 的**極大元**.

(4) 若 $m \in X$ 滿足 $x \leq m \iff m = x$, 則稱 m 是 X 的**極小元**.

註記 4.4.12 當最大元、最小元存在時, 必唯一.

例 4.4.13 設 $X = [1, 12] \cap \mathbb{N}$, 整除關係在 X 上是偏序關係, 則 1 是極小元, $7, 8, 9, 10, 11, 12$ 是極大元.

定義 4.4.14 設 X 爲偏序集, $A \subseteq X$, $A \neq \varnothing$.

(1) 若 $u \in X$ 滿足 $\forall\, a \in A, a \leq u$, 則稱 u 是 A 在 X 中的一個**上界**.

(2) 若 $l \in X$ 滿足 $\forall\, a \in A, m \leq a$, 則稱 l 是 A 在 X 中的一個**下界**.

(3) 若 A 的上界 $s \in X$ 滿足 $\forall\, u \in \{u \in X : u \text{ 是} A \text{ 的上界}\}$, $s \leq u$, 則稱 s 是 A 在 X 中的**上確界**, 記作 $\sup_X A$.

(4) 若 A 的下界 $i \in X$ 滿足 $\forall\, l \in \{l \in X : l \text{ 是} A \text{ 的下界}\}$, $l \leq i$, 則稱 i 是 A 在 X 中的**下確界**, 記作 $\inf_X A$.

注意 4.4.15 這裡不要求上界、下界一定要屬於 A, 只要求要屬於 X.

例 4.4.16 設 $X = [1, 12] \cap \mathbb{N}$, 整除關係在 X 上是偏序關係, 則 6 是子集 $\{2, 3\}$ 在 X 中的上界, 1 是下界; $4, 8, 12$ 都是 $\{2, 4\}$ 的上界, $1, 2$ 都是下界; $\{3, 7\}$ 無上界, 只有下界 1; $\{4, 6\}$ 的上確界爲 12, 下確界爲 2; $\{4, 3\}$ 的上確界爲 12, 下確界爲 1.

命題 4.4.17 設 X 是全序集, $\varnothing \neq A \subseteq X$, 則

(1) $u = \sup_X A$ 的充要條件爲 $\forall\, x < u$, $(x, u] \cap A \neq \varnothing$.

(2) $l = \inf_X A$ 的充要條件爲 $\forall\, x > l$, $[l, x) \cap A \neq \varnothing$.

證明 (1) 和 (2) 是對偶的敍述, 此處僅證明 (2).

必要性: 假設存在滿足 $[l,x)\cap A=\varnothing$ 的 $x>l$. 因

$$\forall\, a\in A, a\geq l \iff a\geq x \text{ 或 } l\leq a<x,$$

故所有 $a\in A$ 都滿足 $a\geq x$, 此時 x 是比下確界 l 更大的下界, 矛盾.

充分性: 對於 A 的任一個下界 l', 若 $l<l'$, 則 $[l,l')\cap A\neq\varnothing$, 故存在滿足 $l\leq a<l'$ 的 $a\in A$, 這與 l' 是 A 的下界矛盾. □

註記 4.4.18 依命題 4.4.17, 有時也稱上確界及下確界爲**最小上界**及**最大下界**. 它們存在時必唯一.

命題 4.4.19 設 X 是全序集, $\varnothing\neq A\subseteq X$.

(1) 若 A 有最大元, 則最大元即上確界.

(2) 若 A 有最小元, 則最小元即下確界.

證明 僅證明 (2). 設 A 的最小元爲 m, 顯然 m 是 A 的一個下界, 且只要 l 是 A 的下界, 便有 $l\leq m$. □

4.5 良序與數學歸納原理

定義 4.5.1 設 X 爲偏序集. 若 X 的所有非空子集都有最小元, 則稱 X 爲**良序集**.

例 4.5.2 在通常的偏序關係 $\leq$ 之下, $\mathbb{N}$ 是良序集 (稍後會用數學歸納原理說明), $\mathbb{Q},\mathbb{R}$ 不是良序集.

定理 4.5.3 良序集必爲全序集.

證明 設 X 爲良序集, 任取 $x,y\in X$, 則 $\{x,y\}$ 是 X 的非空子集. 依良序關係的定義, $\{x,y\}$ 必有最小元. 若 x 是最小元, 則 $x\leq y$; 若 y 是最小元, 則 $y\leq x$. 由 $x,y\in X$ 的任意性, 可知 X 是全序集. □

定理 4.5.4 (超限歸納原理) 設 X 是非空良序集. 若 X 的子集 Y 滿足:

(1) Y 含 X 的最小元 x_0;

(2) 對於 $x\in X$, $S_x:=\{y\in X:y<x\}$, $S_x\subseteq Y$ 可推得 $x\in Y$,

則 $Y=X$.

證明 假設 $X\setminus Y\neq\varnothing$, 則依 X 的良序性, $X\setminus Y$ 必有最小元 m. 因 X 的最小元 $x_0\in Y$, 故 $m\neq x_0$, 即 $x_0<m$. 於是, $x_0\in S_m$, 即 $S_m\neq\varnothing$. 另外, 對所有 $x\in S_m$, $x<m$, 故 x 不可能是 $X\setminus Y$ 的元素, 否則便會違背 m 是 $X\setminus Y$ 是最小元的事實, 於是 $x\in Y$, 即 $S_m\subseteq Y$. 依條件 (2), 可得 $m\in Y$, 矛盾. 因此, $X\setminus Y=\varnothing$, 即 $Y=X$. □

定義 4.5.5 設 S 爲 $\mathbb{N}$ 的非空子集. 所謂 S 具有**歸納性**, 是指只要 $n\in S$, 便有 $n+1\in S$.

公理 4.5.6 (數學歸納原理) 若 $S\subseteq\mathbb{N}$ 具有歸納性, 且 $1\in S$, 則 $S=\mathbb{N}$.

定理 4.5.7 (廣義數學歸納原理) 設 $k\in\mathbb{N}$, S 爲 $\mathbb{N}$ 的非空子集. 若

(1) $k\in S$;

(2) 只要 $n\geq k$ 且 $n\in S$, 便有 $n+1\in S$,

則 $\{n\in\mathbb{N}:n\geq k\}\subseteq S$.

證明 設 $k\geq 2$ ($k=1$ 即數學歸納原理), 令 $T=S\cup\{n\in\mathbb{N}:n<k\}$, 則 $\mathbb{N}\supseteq T\neq\varnothing$, T 具有歸納性, 且 $1\in T$. 依數學歸納原理, 有 $T=\mathbb{N}$, 故 $\{n\in\mathbb{N}:n\geq k\}\subseteq S$. □

定理 4.5.8 (強數學歸納原理) 設 S 是 $\mathbb{N}$ 的非空子集. 若

(1) $1 \in S$;

(2) $\forall\, n \in \mathbb{N}$, 只要 $\{1, \ldots, n\} \subseteq S$, 便有 $n+1 \in S$,

則 $S = \mathbb{N}$.

定理 4.5.9 (廣義強數學歸納原理) 設 $k \in \mathbb{N}$, S 爲 $\mathbb{N}$ 的非空子集. 若

(1) $k \in S$;

(2) $\forall\, n \in \mathbb{N}$, 只要 $n \geq k$ 且 $\{k, k+1, \ldots, n\} \in S$, 便有 $n+1 \in S$,

則 $\{n \in \mathbb{N} : n \geq k\} \subseteq S$.

定理 4.5.10 (良序原理) $\mathbb{N}$ 是良序集.

命題 4.5.11 以下三個敍述等價:

(1) 數學歸納原理;

(2) 強數學歸納原理;

(3) 良序原理.

證明 (1)⇒(3): 假設 $\mathbb{N}$ 有一個不具有最小元的非空子集 S, 則 $1 \notin S$ (否則 1 是 S 的最小元), 於是 $1 \in \mathbb{N} \setminus S$. 令 $T = \{n \in \mathbb{N} : \{1, \ldots, n\} \subseteq \mathbb{N} \setminus S\}$. 首先, 因爲 $1 \in \mathbb{N} \setminus S$, 所以 $1 \in T$. 接著, 設 $n \in T$, 亦即 $\{1, \ldots, n\} \subseteq \mathbb{N} \setminus S$ (1 到 n 皆不屬於 S). 若 $n+1 \in S$, 則 $n+1$ 將會是 S 中的最小元, 這與 S 不具有最小元的假設矛盾. 因此必有 $n+1 \notin S$, 即 $n+1 \in \mathbb{N} \setminus S$. 這意味著 $\{1, \ldots, n, n+1\} \subseteq \mathbb{N} \setminus S$, 故 $n+1 \in T$. 依數學歸納原理, $T = \mathbb{N}$. 這代表對於所有正整數 n, 皆有 $n \notin S$, 也就是 $S = \varnothing$, 這與 S 是非空子集的假設矛盾. 因此, $\mathbb{N}$ 的任何非空子集都必有最小元, 即 $\mathbb{N}$ 是良序集.

(3)⇒(2): 設 S 是 $\mathbb{N}$ 的非空子集, 且滿足 $1 \in S$, 以及 $\forall\, n \in \mathbb{N}$, 只要 $\{1, \ldots, n\} \subseteq S$, 便有 $n+1 \in S$. 欲證 $S = \mathbb{N}$. 假設 $S \neq \mathbb{N}$, 令 $U = \mathbb{N} \setminus S$, 則 U 非空. 依良序原理, U 中必存在最小元, 設之爲 m. 因爲 $1 \in S$, 所以 $1 \notin U$, 故 $m > 1$, 這保證了 $m - 1 \in \mathbb{N}$. 由於 m 是 U 中的最小元, 所以所有小於 m 的正整數都不屬於 U, 即皆屬於 S. 這表示 $\{1, \ldots, m-1\} \subseteq S$. 根據強數學歸納原理的前提假設 (將原假設中的 n 代換爲 $m-1$), 只要 $\{1, \ldots, m-1\} \subseteq S$, 便有 $(m-1)+1 = m \in S$. 但這與 $m \in U = \mathbb{N} \setminus S$ 矛盾. 因此假設錯誤, 必有 $S = \mathbb{N}$.

(2)⇒(1): 設 S 爲 $\mathbb{N}$ 的非空子集, 且滿足 $1 \in S$, 以及只要 $n \in S$, 便有 $n+1 \in S$. 欲證 $S = \mathbb{N}$. 已知 $1 \in S$. 假設對某個 $n \in \mathbb{N}$, 有 $\{1, \ldots, n\} \subseteq S$. 由於 $\{1, \ldots, n\} \subseteq S$, 特別地, 有 $n \in S$. 根據數學歸納原理的前提假設「只要 $n \in S$, 便有 $n+1 \in S$」, 可以直接推得 $n+1 \in S$. 也就是說, 只要 $\{1, \ldots, n\} \subseteq S$, 便有 $n+1 \in S$. 依強數學歸納原理, $S = \mathbb{N}$. □

註記 4.5.12 既然談到序, 這裡不加證明地給出一些和序有關的敍述. 下列敍述皆等價, 但目前仍無法由其他已知的工具推得:

(1) 策梅羅良序定理: 任何非空的集合皆可良序化, 即只要集合 $S \neq \varnothing$, 便存在 S 上的二元關係 R, 使得 (S, R) 是良序集.

(2) 選擇公理: 設 $\mathcal{X}$ 是一集族, 則存在定義於 $\mathcal{X}$ 上的選擇函數. (參考公理 3.4.8)

(3) 豪斯多夫極大定理: 任意非空的偏序集, 總存在極大的全序子集.

(4) 佐恩引理: 設 X 是非空偏序集, 若 X 的每個全序子集在 X 中均有上界, 則 X 有極大元.

例 4.5.13 (旋轉矩陣) 證明: 對所有 $n \in \mathbb{N}$, 均有

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^n = \begin{pmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{pmatrix}.$$

證明 當 $n = 1$ 時, 等式顯然成立. 假設當 $n = k$ 時, 等式成立, 則當 $n = k + 1$ 時,

$$\begin{aligned} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{k+1} &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^k \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \\ &= \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \\ &= \begin{pmatrix} \cos k\theta\cos\theta - \sin k\theta\sin\theta & -\sin\theta\cos k\theta - \cos\theta\sin k\theta \\ \sin k\theta\cos\theta + \cos k\theta\sin\theta & \cos k\theta\cos\theta - \sin k\theta\sin\theta \end{pmatrix} \\ &= \begin{pmatrix} \cos(k+1)\theta & -\sin(k+1)\theta \\ \sin(k+1)\theta & \cos(k+1)\theta \end{pmatrix}. \end{aligned}$$

□

例 4.5.14 證明: 對所有 $n \in \mathbb{N}$, 3 整除 $n^3 + 2n$.

證明 考慮集合

$$A = \{n \in \mathbb{N} : 3 \text{ 不能整除 } n^3 + 2n\}.$$

假設 $A \neq \varnothing$, 則依良序原理, A 必有最小元, 記作 m. 因當 $n = 1$ 時, $1^3 + 2 \cdot 1 = 3$, 故 $1 \notin A$, 於是 $m > 1$, 從而 $m - 1 \in \mathbb{N}$. 因 m 是 A 的最小元, 且 $m - 1 < m$, 故 $m - 1 \notin A$, 這意味著 $(m-1)^3 + 2(m-1)$ 是 3 的倍數. 稍作計算, 可得

$$(m^3 + 2m) - \big((m-1)^3 + 2(m-1)\big) = 3(m^2 - m + 1),$$

移項得

$$m^3 + 2m = 3(m^2 - m + 1) + \big((m-1)^3 + 2(m-1)\big).$$

因爲 $3(m^2 - m + 1)$ 及 $(m-1)^3 + 2(m-1)$ 均爲 3 的倍數, 所以它們的和 $m^3 + 2m$ 當然也是 3 的倍數, 這導致 $m \in A$, 與假設矛盾. 因此, $A = \varnothing$, 即一切正整數 n 均爲 $n^3 + 2n$ 的因數.

此例亦可用數學歸納法的「標準流程」來論證, 請讀者嘗試用數學歸納法給出證明. □

例 4.5.15 給定數列 $\{x_n\}_{n=0}^{+\infty}$, 其滿足

$$\begin{cases} x_0 = 1, \\ x_1 = 2, \\ x_n = 3x_{n-1} - 2x_{n-2}, \end{cases}$$

證明: 對一切非負整數 n, 都有 $x_n = 2^n$.

證明 (方法一: 強數學歸納法) 當 $n = 0$ 時, $x_0 = 1 = 2^0$. 當 $n = 1$ 時, $x_1 = 2 = 2^1$. 當 $n = 2$ 時, $x_2 = 3x_1 - 2x_0 = 3 \cdot 2 - 2 \cdot 1 = 4 = 2^2$. 假設當 $n < k$ $(k \in \mathbb{N})$ 時, 都有 $x_n = 2^n$, 則當 $n = k$ 時,

$$x_k = 3x_{k-1} - 2x_{k-2} = 3 \cdot 2^{k-1} - 2 \cdot 2^{k-2} = (3-1) \cdot 2^{k-1} = 2 \cdot 2^{k-1} = 2^k.$$

因此, 命題得證. □

注意 4.5.16 即使此例是在 $\mathbb{N} \cup \{0\}$ 上操作, 而不是在 $\mathbb{N}$ 上, 但 $\mathbb{N} \cup \{0\}$ 亦爲歸納集, 故仍可使用數學歸納法.

以下提供針對這種遞迴式的其他四種常見的處理方法給讀者參考, 它們的原理超出了本文所討論的內容, 感興趣的讀者可參考線性代數或組合數學的教材.

證明 (方法二: 線性組合法) 若數列 $\{a_n\}_{n=0}^{+\infty}$ 及 $\{b_n\}_{n=0}^{+\infty}$ 均滿足遞迴式 $x_n = 3x_{n-1} - 2x_{n-2}$ $(n \geq 2)$, 則它們的線性組合 $\{\alpha a_n + \beta b_n\}_{n=0}^{+\infty}$ 亦滿足該遞迴式. 事實上, 對一切實數 α, β 及大於 1 的整數,

$$\alpha a_n + \beta b_n = \alpha(3a_{n-1} - 2a_{n-2}) + \beta(3b_{n-1} - 2b_{n-2}) = 3(\alpha a_{n-1} + \beta b_{n-1}) - 2(\alpha a_{n-2} + \beta b_{n-2}).$$

於是,

$$V := \left\{\{a_n\}_{n=0}^{+\infty} : \forall\, n \geq 2, a_n = 3a_{n-1} - 2a_{n-2}\right\}$$

是 $\mathbb{R}$ 線性空間, 且 $\{x_n\}_{n=0}^{+\infty} \in V$.

現, 設等比數列[1] $\{r^n\}_{n=0}^{+\infty} \in V$, 則

$$r^n = 3r^{n-1} - 2r^{n-2} \iff (r-1)(r-2) = 0 \iff r = 1 \text{ 或 } r = 2,$$

這意味著 $\{1^n\}_{n=0}^{+\infty}$ 及 $\{2^n\}_{n=0}^{+\infty}$ 都是 V 的元素. 顯然這兩個元素是 $\mathbb{R}$ 線性獨立的, 且 $\dim_{\mathbb{R}} V = 2$, 故該兩元素組成 V 的一組基. 既然 $\{x_n\}_{n=0}^{+\infty}$, 可設

$$x_n = \alpha + \beta 2^n \quad (n \in \mathbb{N} \cup \{0\}).$$

將 $x_0 = 1$ 及 $x_1 = 2$ 代入, 得方程組

$$\begin{cases} \alpha + \beta = 1, \\ \alpha + 2\beta = 2, \end{cases}$$

解得 $\alpha = 0$, $\beta = 1$, 從而 $x_n = 2^n$ $(n \in \mathbb{N} \cup \{0\})$. □

註記 4.5.17 讀者可將方法二中待定係數的操作與常係數線性微分方程的解法對比.

證明 (方法三: 對角化法) 當 $n \geq 2$ 時,

$$\mathbf{x}_n := \begin{pmatrix} x_n \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} 3x_{n-1} - 2x_{n-2} \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} 3 & -2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_{n-2} \end{pmatrix} := A\mathbf{x}_{n-1}.$$

當 $n > 2$ 時, 將上式的 $\mathbf{x}_{n-1}$ 用 $A\mathbf{x}_{n-2}$ 替換, 重複此操作直到 $\mathbf{x}$ 的下標不再滿足上式爲止, 得

$$\mathbf{x}_n = A^{n-1}\mathbf{x}_1. \tag{4.1}$$

將 A 對角化, 讀者可嘗試用常規計算特徵多項式的方法, 此處用循環子空間來處理. 注意到

$$A\mathbf{e}_2 = \begin{pmatrix} 3 & -2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \end{pmatrix} = -2\mathbf{e}_1,$$

兩邊同左乘 A, 得

$$A^2\mathbf{e}_2 = -2A\mathbf{e}_1 = -2\begin{pmatrix} 3 \\ 1 \end{pmatrix} = -2(3\mathbf{e}_1 + \mathbf{e}_2) = 3 \cdot (-2\mathbf{e}_1) - 2\mathbf{e}_2 = 3A\mathbf{e}_2 - 2\mathbf{e}_2,$$

即

$$(A^2 - 3A + 2I_2)\mathbf{e}_2 = \mathbf{0}.$$

於是, $\lambda^2 - 3\lambda + 2$ 爲 A 的特徵多項式, 且 A 的特徵值爲 $1, 2$. 又

$$\ker(A - I_2) = \ker\begin{pmatrix} 2 & -2 \\ 1 & -1 \end{pmatrix} = \operatorname{span}_{\mathbb{R}}\left\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\},$$

[1] 此數列公比爲 r, 而公比的定義爲連續兩項中的後項與前項的比, 因此設 $r \neq 0$, 公比才有意義.

$$\ker(A-2I_2)=\ker\begin{pmatrix}1&-2\\1&-2\end{pmatrix}=\operatorname{span}_{\mathbb{R}}\left\{\begin{pmatrix}2\\1\end{pmatrix}\right\},$$

於是記特徵向量 $\mathbf{v}_1=(1,1)^\top$, $\mathbf{v}_2=(2,1)^\top$, 就有

$$A(\mathbf{v}_1,\mathbf{v}_2)=(A\mathbf{v}_1,A\mathbf{v}_2)=(\mathbf{v}_1,2\mathbf{v}_2)=(\mathbf{v}_1,\mathbf{v}_2)\begin{pmatrix}1&0\\0&2\end{pmatrix},\quad \text{即}\quad A=(\mathbf{v}_1,\mathbf{v}_2)\begin{pmatrix}1&0\\0&2\end{pmatrix}(\mathbf{v}_1,\mathbf{v}_2)^{-1}.$$

將此結果代回式 (4.1), 得

$$\begin{aligned}\begin{pmatrix}x_n\\x_{n-1}\end{pmatrix}&=\begin{pmatrix}1&2\\1&1\end{pmatrix}\begin{pmatrix}1^{n-1}&0\\0&2^{n-1}\end{pmatrix}\begin{pmatrix}1&2\\1&1\end{pmatrix}^{-1}\begin{pmatrix}x_1\\x_0\end{pmatrix}\\&=\begin{pmatrix}1&2\\1&1\end{pmatrix}\begin{pmatrix}1^{n-1}&0\\0&2^{n-1}\end{pmatrix}\begin{pmatrix}-1&2\\1&-1\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}=\begin{pmatrix}2^n\\2^{n-1}\end{pmatrix},\end{aligned}$$

即 $x_n=2^n$ $(n\geq 2)$. 經檢驗, 當 $n=0$ 或 1 時, 仍滿足 $x_n=2^n$. □

證明 (方法四: 生成函數法) 將數列 $\{x_n\}_{n=0}^{+\infty}$ 的生成函數定義作形式冪級數

$$f(t)=\sum_{n=0}^{+\infty}x_nt^n=x_0+x_1t+x_2t^2+x_3t^3+\cdots.$$

已知當 $n\geq 2$ 時, 有 $x_n=3x_{n-1}-2x_{n-2}$, 將之兩邊同乘以 t^n, 並且對一切 $n\in\mathbb{N}\cap[2,+\infty)$ 求和, 即

$$\sum_{n=2}^{+\infty}x_nt^n=3\sum_{n=2}^{+\infty}x_{n-1}t^n-2\sum_{n=2}^{+\infty}x_{n-2}t^n.\tag{4.2}$$

分別用 $f(t)$ 表示這三個無窮和:

- $\displaystyle\sum_{n=2}^{+\infty}x_nt^n=\sum_{n=0}^{+\infty}x_nt^n-x_0-x_1t=f(t)-x_0-x_1t;$
- $\displaystyle\sum_{n=2}^{+\infty}x_{n-1}t^n=t\sum_{n=2}^{+\infty}x_{n-1}t^{n-1}=t\left(\sum_{n=0}^{+\infty}x_nt^n-x_0\right)t(f(t)-x_0);$
- $\displaystyle\sum_{n=2}^{+\infty}x_{n-2}t^n=t^2\sum_{n=2}^{+\infty}x_{n-2}t^{n-2}=t^2f(t).$

於是, 式 (4.2) 化爲

$$f(t)-1-2t=3t(f(t)-1)-2t^2f(t),$$

整理可得

$$f(t)=\frac{1-t}{1-3t+2t^2}=\frac{1-t}{(1-t)(1-2t)}=\frac{1}{1-2t}.$$

利用等比級數公式將上式展開, 得

$$\sum_{n=0}^{+\infty}x_nt^n=f(t)=\sum_{n=0}^{+\infty}(2t)^n=\sum_{n=0}^{+\infty}2^nt^n,$$

比較 t^n 的係數, 即得 $t_n=2^n$ $(n\in\mathbb{N}\cup\{0\})$. □

證明 (*方法五: 差分法*)　將遞迴式 $x_n = 3x_{n-1} - 2x_{n-2}$ $(n \geq 2)$ 的右側項拆解並移項, 可得

$$x_n - x_{n-1} = 2x_{n-1} - 2x_{n-2} = 2(x_{n-1} - x_{n-2}).$$

若令 $d_n = x_n - x_{n-1}$ $(n \geq 1)$, 則上式可化爲一階遞迴式

$$d_n = 2d_{n-1} \qquad (n \geq 2).$$

這表示數列 $\{d_n\}_{n=1}^{+\infty}$ 是公比爲 2 的等比數列. 由初始條件可知, 首項爲 $d_1 = x_1 - x_0 = 2 - 1 = 1$, 從而可得其通項公式爲

$$d_n = d_1 \cdot 2^{n-1} = 2^{n-1} \qquad (n \geq 1).$$

接著利用累加法求 x_n. 當 $n \geq 1$ 時,

$$x_n = x_0 + \sum_{k=1}^{n}(x_k - x_{k-1}) = x_0 + \sum_{k=1}^{n} d_k = 1 + \sum_{k=1}^{n} 2^{k-1} = 1 + \frac{1 \cdot (2^n - 1)}{2 - 1} = 1 + 2^n - 1 = 2^n.$$

經檢驗, 當 $n = 0$ 時, $x_0 = 1 = 2^0$ 亦滿足此結果. 因此, 對一切非負整數 n, 都有 $x_n = 2^n$. □

單元 5

集合的基數

5.1 基數

定義 5.1.1 若集合 X 的元素個數爲有限個, 則稱 X 爲**有限集**, 稱 X 的元素個數爲 X 的**基數**、**勢**, 或**階**, 通常記作 $|X|, \mathrm{card}(A)$ 或 $\#A$. 另外, 約定 $\#\varnothing = 0$. 對於**無窮集** X (即 X 有爲無窮多個元素), 形式上地記 $|X| = +\infty$.

命題 5.1.2 對於有限集 X, Y, 有 $\#(X \times Y) = \#X \times \#Y$. 又若 $X \subseteq Y$, 則 $\#X \leq \#Y$.

命題 5.1.3 設 X, Y 爲有限集, 則自 X 至 Y 的映射個數爲 $\#(Y^X) = (\#Y)^{\#X}$.

命題 5.1.4 設 X 爲有限集, 則其冪集 2^X 的基數爲 $\#2^X = 2^{\#X}$.

註記 5.1.5 集合中的元素無序且不允許重複 (即重複者只算作一個元素, 如 $\{a, a\} = \{a\}$, 且 $\#\{a, a\} = 1$). 若允許重複, 則稱之爲**多重集**.

命題 5.1.6 設 A_i $(i = 1, \ldots, n)$ 爲有限集, 則有如下基數公式:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \sum_{1\leq i<j<k\leq n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

證明 對 n 做數學歸納法. 當 $n = 2$ 時, $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ 顯然成立. 假設當 $n = k$ 時, 等式成立, 即

$$\left|\bigcup_{i=1}^{k} A_i\right| = \sum_{j=1}^{k} (-1)^{j-1} \sum_{1\leq i_1<\cdots<i_j\leq k} |A_{i_1} \cap \cdots \cap A_{i_j}|,$$

則當 $n = k + 1$ 時, 令 $B = \bigcup_{i=1}^{k} A_i$. 此時, 由 $n = 2$ 的情形, 可得

$$|B \cup A_{k+1}| = |B| + |A_{k+1}| - |B \cap A_{k+1}|.$$

其中, 依歸納假設即得第一項 $|B|$, 而依集合運算的分配律, 第二項可化爲

$$\left|\left(\bigcup_{i=1}^{k} A_i\right) \cap A_{k+1}\right| = \left|\bigcup_{i=1}^{k} (A_i \cap A_{k+1})\right|,$$

這恰好也是 k 個集合 $A_1 \cap A_{k+1}, \ldots, A_k \cap A_{k+1}$ 的聯集, 同樣可套用歸納假設. 將 $|B|$ 與 $|B \cap A_{k+1}|$ 的展開式代入合併後, 所有不包含 A_{k+1} 的交集項來自 $|B|$, 而所有包含 A_{k+1} 的交集項來自於 $-|B \cap A_{k+1}|$ (前面的負號恰好讓原本的 $(-1)^{j-1}$ 變成 $(-1)^j$, 符合增加一個集合後的正負號規律). 兩者合併後, 剛好構成了 $n = k + 1$ 時的完整公式. 由數學歸納法得證. □

註記 5.1.7 (鴿籠原理) 設 A, B 爲非空有限集. 若 $\#A > \#B$, 則對任意映射 $f \in B^A$, f 必不爲單射, 即存在 $y \in B$, 使得原像集 $\{x \in A : f(x) = y\}$ 至少有 2 個元素.

例 5.1.8 設 $\triangle ABC$ 爲邊長爲 1 單位的等邊三角形, 在此三角形的內部任取五點, 則必有兩點之間的距離小於 $1/2$.

證明 將 $\triangle ABC$ 各邊上的中點兩兩相連, 形成四個邊長爲 $1/2$ 的小等邊三角形. 在其中任取五點, 則依鴿籠原理, 至少有兩點落在同一區域 (允許落在小三角形的邊上), 該兩點的距離小於 $1/2$. □

例 5.1.9 證明不超過 $2n$ 的 $n+1$ 個正整數整之中, 必有兩者互質.

證明 將 $1, 2, \ldots, 2n$ 分成 n 組: $\{1, 2\}, \{3, 4\}, \ldots, \{2n-1, 2n\}$. 依鴿籠原理, $1, 2 \ldots, 2n$ 中取 $n+1$ 數必有兩數 a, b 在同一組中. 因爲相鄰兩數必互質, 所以 a, b 必互質. □

命題 5.1.10 設 A, B 爲兩非空有限集.

(1) 單射 $f \in B^A$ 存在的充要條件爲 $\#A \leq \#B$.

(2) 滿射 $g \in B^A$ 存在的充要條件爲 $\#A \geq \#B$.

(3) 雙射 $h \in B^A$ 存在的充要條件爲 $\#A = \#B$.

證明 (1) 根據單射的定義, 可知 B 中至少有 $\#A$ 個不同的元素.

(2) 依鴿籠原理, 視 B 中的各個元素爲「籠子」, 視 A 中各個元素爲「鴿子」, 則每個「籠子」都至少有一隻鴿子.

(3) 依基本的計數原理即得.

□

定義 5.1.11 對於集合 X, 將自 X 至 X 的所有映射稱爲 X 上的**自映射**.

命題 5.1.12 對於有限集 X 上的自映射 f, 有

$$f \text{ 是單射} \iff f \text{ 是滿射}.$$

證明 採計數原理. □

注意 5.1.13 命題 5.1.12 對於無窮集未必成立, 例如 $f(x) = 2^x$ 是 $\mathbb{R}$ 映至 $\mathbb{R}$ 的單射而不是滿射, $g(x) = x^3 - x$ 是 $\mathbb{R}$ 映至 $\mathbb{R}$ 的滿射而不是單射.

定義 5.1.14 設 X, Y 爲兩集合. 若存在雙射 $f \in Y^X$, 則稱 X, Y **等勢**或**有相同的基數**, 記作 $|X| = |Y|$ 或 $\operatorname{card}(X) = \operatorname{card}(Y)$ 或 $\#X = \#Y$.

註記 5.1.15 因爲只要 $f \in Y^X, g \in Z^Y$ 皆爲雙射, $g \circ f \in Z^X$ 便也是雙射, 所以等勢關係具有傳遞性, 即 $|X| = |Y|, |Y| = |Z| \implies |X| = |Z|$.

例 5.1.16 (希爾伯特旅館) $|\mathbb{N}| = |\mathbb{Z}|$.

證明 只需考慮映射

$$f : \mathbb{N} \longrightarrow \mathbb{Z}, \quad n \longmapsto \begin{cases} \dfrac{n}{2}, & n \in 2\mathbb{Z} := \{2k : k \in \mathbb{Z}\}, \\ \dfrac{n+1}{2}, & n \in 2\mathbb{Z} - 1 := \{2k-1 : k \in \mathbb{Z}\}, \end{cases}$$

說明 f 是雙射即可. □

例 5.1.17 $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

證明 定義

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \quad (m, n) \longmapsto 2^{m-1}(2n-1).$$

設 $f(m,n) = f(\mu,\nu)$, 即

$$2^{m-1}(2n-1) = 2^{\mu-1}(2\nu-1).$$

因 $2n-1, 2\nu-1$ 均爲奇數, 都不能被 2 整除, 故依質因數分解的唯一性, 等式兩邊的質因數 2 的個數必相等, 即

$$m-1 = \mu-1 \implies m = \mu.$$

將此結果代回原式並消去偶因數, 得

$$2n-1 = 2\nu-1 \implies n = \mu.$$

因此, $(m,n) = (\mu,\nu)$, 即 f 是單射.

給定 $k \in \mathbb{N}$, 將其不斷除以 2, 直到剩下的數是奇數爲止, 即 k 必可寫作 $k = 2^a b$, 其中 $a \in \mathbb{N} \cup \{0\}$, $b \in 2\mathbb{N}-1$. 因 $a \in \mathbb{N} \cup \{0\}$, 故取 $m = a+1$, 則 $m \in \mathbb{N}$. 因 $b \in 2\mathbb{N}-1$, 故存在 $n \in \mathbb{N}$ 使 $b = 2n-1$, 即 $n = (b+1)/2$. 於是,

$$f(m,n) = 2^{m-1}(2n-1) = 2^a b = k,$$

即 f 是滿射. □

註記 5.1.18 另一種常見的方法是考慮函數

$$g : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \quad g(m,n) = \frac{(m+n-2)(m+n-1)}{2} + n,$$

稱爲**康托爾配對函數**, 也可證明此函數亦爲雙射. 這會給出數列 $(1,1) \mapsto 1$, $(2,1) \mapsto 2$, $(1,2) \mapsto 3$, $(3,1) \mapsto 4$, ... 把這些序偶標在座標平面上, 並將各對應的像標在相應的點旁邊, 作爲該點的編號. 不難看出這些點依次沿對角線排列.

例 5.1.19 $|[0,1)| = |[0,1]| = |[0,+\infty)| = |(0,+\infty)| = |\mathbb{R}|$.

證明 作

$$f : [0,1] \longrightarrow [0,1), \quad x \longmapsto \begin{cases} \dfrac{x}{2}, & \exists\, n \in \mathbb{N}, x = 2^{-n}, \\ x, & \text{其餘情形.} \end{cases}$$

作

$$g : [0,1) \longrightarrow [0,+\infty), \quad x \longmapsto \frac{1}{1-x} - 1.$$

作

$$h : [0,+\infty) \longrightarrow (0,+\infty), \quad x \longmapsto \begin{cases} x+1, & x \in \mathbb{N} \cup \{0\}, \\ x, & \text{其餘情形.} \end{cases}$$

作

$$k : (0,+\infty) \longrightarrow \mathbb{R}, \quad x \longmapsto \log x.$$

由於上述 f, g, h, k 皆爲雙射, 因此得證這五個集合的基數相等. □

例 5.1.20 (康托爾對角線法) $|\mathbb{N}| \neq |\mathbb{R}|$.

證明 假設不然, 則存在自 $\mathbb{N}$ 映至 $\mathbb{R}$ 的雙射 f. 因一切實數皆可寫成十進位小數的形式, 故對所有 $n, m \in \mathbb{N}$, 存在 $a_{n,m} \in \{0,1,\ldots,9\}$ 使得 $f(n) = a_{n,1}.a_{n,2}a_{n,3}a_{n,4}\cdots$, 即

$$f(1) = a_{1,1}.a_{1,2}a_{1,3}a_{1,4}\cdots,$$
$$f(2) = a_{2,1}.a_{2,2}a_{2,3}a_{2,4}\cdots,$$

$$\begin{aligned} f(3) &= a_{3,1}.a_{3,2}a_{3,3}a_{3,4}\cdots, \\ &\vdots \\ f(n) &= a_{n,1}.a_{n,2}a_{n,3}a_{n,4}\cdots, \\ &\vdots \end{aligned}$$

考慮對角線所成的數列 $\{a_{n,n}\}_{n=1}^{+\infty}$, 作數列 $\{b_n\}_{n=1}^{+\infty}$ 如下:

$$b_n = \begin{cases} 2, & a_{n,n} = 3, \\ 3, & a_{n,n} \neq 3, \end{cases}$$

則因爲實數 $b := b_1.b_2b_3b_4\cdots$ 與每一個 $f(n)$ 至少有一位不同, 所以不同於任一個 $f(n)$, 即不存在 $n \in \mathbb{N}$ 使 $f(n) = b$, 這與 f 是雙射矛盾. □

5.2 可數集

定義 5.2.1 設 X 爲一集合. 若 $|X| = |\mathbb{N}|$, 則稱 X 爲**可數集**或**可列集**, 記作 $|X| = \aleph_0$. 有限集和可數集統稱爲**至多可數集**. 若 X 不是至多可數集, 則稱 X **不可數**.

註記 5.2.2 不難看出: 若且唯若非空集 X 至多可數, 則存在自 X 至 $\mathbb{N}$ 的單射.

定義 5.2.3 設 X 爲一集合. 若 $|X| = |\mathbb{R}|$, 則稱 X 爲**連續統**, 記作 $\mathfrak{c}$.

例 5.2.4 $\mathbb{Z}, \mathbb{N}\times\mathbb{N}, \mathbb{N}\cup\{0\}$ 是可數集. $[0,1], (-\infty, 0]$ 是連續統.

定理 5.2.5 至多可數集的子集是至多可數集.

證明 設 X 至多可數, $Y \subseteq X$. 若 $Y = \varnothing$, 則 Y 是有限集, 當然至多可數. 若 $Y \neq \varnothing$, 則因 X 至多可數, 故存在自 X 映至 $\mathbb{N}$ 的單射 f. 考慮 f 在 Y 上的限制 $g = f|_Y$, 則 g 顯然也是單射, 因此 Y 也至多可數. □

定理 5.2.6 至多可數個至多可數集的聯集是至多可數集.

證明 設 I 爲至多可數的指標集, $\{A_i\}_{i\in I}$ 爲一族至多可數集. 若 $I = \varnothing$, 則 $\bigcup_{i\in I} A_i = \varnothing$ 是有限集, 當然至多可數. 若 $I \neq \varnothing$, 則因 I 至多可數, 不失一般性可設 $I = \mathbb{N}$.

同理, 對每個 $n \in \mathbb{N}$, 因 A_n 至多可數, 故可將 A_n 的所有元素排成數列 $a_{n,1}, a_{n,2}, a_{n,3}, a_{n,4}, \ldots$ (若 A_n 爲有限集, 則將其最後一個元素不斷重複即可). 於是聯集 $\bigcup_{n=1}^{+\infty} A_n$ 中的所有元素可排成如下陣列:

$$\begin{aligned} A_1 &= \{a_{1,1}, a_{1,2}, a_{1,3}, a_{1,4}, \ldots\}, \\ A_2 &= \{a_{2,1}, a_{2,2}, a_{2,3}, a_{2,4}, \ldots\}, \\ A_3 &= \{a_{3,1}, a_{3,2}, a_{3,3}, a_{3,4}, \ldots\}, \\ &\vdots \\ A_n &= \{a_{n,1}, a_{n,,2}, a_{n,3}, a_{n,4}, \ldots\}, \\ &\vdots \end{aligned}$$

按照對角線順序 (即下標和 $n+m$ 由小到大) 依序走訪上述陣列, 可得一數列:

$$a_{1,1}, a_{1,2}, a_{2,1}, a_{1,3}, a_{2,2}, a_{3,1}, a_{1,4}, \ldots$$

從此數列中依序取出元素, 若遇到已取過的元素則跳過, 如此即可將 $\bigcup_{n=1}^{+\infty} A_n$ 中的所有不重複元素排成一個新的數列 $\{b_k\}_{k=1}^{+\infty}$. 這等價於存在單射 $g \in (\mathbb{N})^{\bigcup_{n=1}^{+\infty} A_n}$, 因此聯集也至多可數. □

系理 5.2.7 $|\mathbb{Q}| = |\mathbb{N}|$.

證明 注意到

$$\mathbb{Q} = \bigcup_{n\in\mathbb{N}} \left\{ \frac{m}{n} : m \in \mathbb{Z} \right\},$$

故 $\mathbb{Q}$ 可數. □

系理 5.2.8 無理數集不可數, 即 $|\mathbb{R} \setminus \mathbb{Q}| \neq |\mathbb{N}|$.

證明 若 $\mathbb{R} \setminus \mathbb{Q}$ 可數, 則依定理 5.2.6 及系理 5.2.7, 可得 $\mathbb{R} = (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}$ 可數, 但這與例 5.1.20 矛盾. □

定義 5.2.9 設 X, Y 爲兩集合. 若存在單射 $f \in Y^X$, 則記 $|X| \leq |Y|$.

註記 5.2.10 (1) 上述「$\leq$」具有傳遞性.

(2) 存在單射 $f \in Y^X$ 等價於存在滿射 $g \in X^Y$.

命題 5.2.11 設集合 X, Y 滿足 $Y \subseteq X$, 則 $|Y| \leq |X|$.

證明 因包含映射 $i \in X^Y$ 是單射, 故 $|Y| \leq |X|$. □

定理 5.2.12 (康托爾-伯恩斯坦-施洛德定理) 若兩集合 X, Y 滿足 $|X| \leq |Y|$ 且 $|Y| \leq |X|$, 則 $|X| = |Y|$.

證明 設 $f \in Y^X$, $g \in X^Y$ 爲單射. 令

$$\begin{aligned}
&\{A_i\}: \quad A_1 = X, \qquad A_{i+1} = (g \circ f)(A_i),\\
&\{B_i\}: \quad B_1 = g(Y), \qquad B_{i+1} = (g \circ f)(B_i),\\
&\{C_i\}: \quad C_1 = Y, \qquad C_{i+1} = (f \circ g)(C_i),\\
&\{D_i\}: \quad D_1 = f(X), \qquad D_{i+1} = (f \circ g)(D_i),
\end{aligned}$$

則有如下子集列:

$$\begin{aligned}
X = A_1 \supseteq B_1 \supseteq A_2 \supseteq B_2 \supseteq \cdots,\\
Y = C_1 \supseteq D_1 \supseteq C_2 \supseteq D_2 \supseteq \cdots.
\end{aligned}$$

定義映射

$$h : X \longrightarrow Y, \quad h(x) = \begin{cases} f(x), & \exists\, n \in \mathbb{N}, x \in A_n \setminus B_n,\\ g^{-1}(x), & \text{其餘情形}, \end{cases}$$

其中 g^{-1} 是雙射 $g|_{f(X)}$ 的逆映射, 則顯然 h 是單射. 不難推得:

$$h(A_n \setminus B_n) = D_n \setminus C_{n+1}, \quad h(B_n \setminus A_{n+1}) = C_n \setminus D_n, \quad h\left(\bigcap_{i=1}^{+\infty} A_i\right) = \bigcap_{i=1}^{+\infty} C_i,$$

從而 $h(X) = Y$, 即 h 是滿射. 因此, $h \in Y^X$ 是雙射, 即 $|X| = |Y|$. □

命題 5.2.13 $\left|2^{\mathbb{N}}\right| = |\mathbb{R}|$.

證明 利用康托爾-伯恩斯坦-施洛德定理來證明此結論, 即分別構造單射 $f \in (\mathbb{R})^{2^{\mathbb{N}}}$ 與 $g \in (2^{\mathbb{N}})^{\mathbb{R}}$.

首先構造 f. 視 $2^{\mathbb{N}}$ 爲 $\mathbb{N}$ 的冪集, 對任意 $A \in 2^{\mathbb{N}}$, 作數列 $\{a_n\}_{n=1}^{+\infty}$ 如下:

$$a_n = \begin{cases} 1, & n \in A,\\ 0, & n \notin A. \end{cases}$$

並定義 $f \in (\mathbb{R})^{2^{\mathbb{N}}}$ 爲

$$f(A) = \sum_{n=1}^{+\infty} \frac{a_n}{3^n}.$$

因實數的三進位小數展開在不包含數字 2 時是唯一的, 故若 $A \neq B$, 其對應的指標數列必然不同, 展成的三進位小數亦不相等, 即 $f(A) \neq f(B)$. 因此 f 是單射, 得 $\left|2^{\mathbb{N}}\right| \leq |\mathbb{R}|$.

接著構造 g. 考慮有理數集 $\mathbb{Q}$, 因 $|\mathbb{Q}| = |\mathbb{N}|$, 故存在雙射 $h \in (\mathbb{N})^{\mathbb{Q}}$. 對每個 $x \in \mathbb{R}$, 定義 $g \in (2^{\mathbb{N}})^{\mathbb{R}}$ 如下:

$$g(x) = \{h(q) : q \in \mathbb{Q},\ q < x\}.$$

設 $x, y \in \mathbb{R}$ 且 $x < y$. 因有理數在實數中稠密, 存在 $r \in \mathbb{Q}$ 使得 $x < r < y$. 此時因 $r < y$ 故 $h(r) \in g(y)$, 且因 $r > x$ 故 $h(r) \notin g(x)$, 推得 $g(x) \neq g(y)$, 則 g 顯然也是單射, 因此 $|\mathbb{R}| \leq \left|2^{\mathbb{N}}\right|$.

綜合上述兩結論, 根據康托爾-伯恩斯坦-施洛德定理即證得 $\left|2^{\mathbb{N}}\right| = |\mathbb{R}|$. □

命題 5.2.14 設 X 爲任一個無限集, 則 $|\mathbb{N}| \leq |X|$.

證明 取 $x_1 \in X$, 再取 $x_2 \in X \setminus \{x_1\}$, 再取 $x_3 \in X \setminus \{x_1, x_2\}$, 以此類推, 得 X 的一可數子集 $\{x_n \in X : n \in \mathbb{N}\}$. 依命題 5.2.11, 即得結論. □

系理 5.2.15 $|\mathbb{N}| < |\mathbb{R}|$, 即 $\aleph_0 < \mathfrak{c}$.

5.3 基數算術

定義 5.3.1 設集合 X, Y 相離, 它們的基數爲 $|X| = \alpha$, $|Y| = \beta$, 則定義 $\alpha + \beta := |X \cup Y|$.

註記 5.3.2 定義 5.3.1 中的集合 X、Y 可任意選取, 僅需確保 $|X| = \alpha$、$|Y| = \beta$、$X \cap Y = \varnothing$ 即可.

命題 5.3.3 設 α, β, γ 爲三個集合的基數, 則

(1) $\alpha + \beta = \beta + \alpha$ (交換律);

(2) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ (結合律);

(3) $\alpha + 0 = \alpha$ (單位律).

證明 由集合的基本運算性質即得. □

定義 5.3.4 若存在有限集 X 使得 $|X| = \alpha$, 則稱 α 是**有限基數**.

命題 5.3.5 (1) $\aleph_0 + n = \aleph_0$, 其中 n 是有限基數;

(2) $\aleph_0 + \aleph_0 = \aleph_0$;

(3) $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$.

證明 (1) 顯而易見. (2) 依定理 5.2.6 即得. (3) 考慮 $A = [0, 1]$, $B = (1, 2]$, 則 $|A| = |B| = \mathfrak{c}$ 且 $A \cap B = \varnothing$, 因此得 $\mathfrak{c} + \mathfrak{c} = |A \cup B| = \mathfrak{c}$. □

定義 5.3.6 設 α, β 爲兩個集合的基數, 若存在滿足 $\beta = \alpha + \gamma$ 的基數 γ, 則記 $\alpha \leq \beta$.

命題 5.3.7 基數的「$\leq$」是偏序關係, 即:

(1) $\alpha \leq \alpha$ (自反性);

(2) 若 $\alpha \leq \beta$ 且 $\beta \leq \gamma$, 則 $\alpha \leq \gamma$ (傳遞性);

(3) 若 $\alpha \leq \beta$ 且 $\beta \leq \alpha$, 則 $\alpha = \beta$ (對稱性; 康托爾-伯恩斯坦-施洛德定理, 即定理 5.2.12).

定義 5.3.8 設集合 X 和 Y 的基數分別爲 α 及 β, 定義 $\alpha\beta = |A \times B|$.

命題 5.3.9 設 α, β, γ 爲三個集合的基數, 則有

(1) $\alpha\beta = \beta\alpha$ (交換律);

(2) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ (結合律);

(3) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ (分配律);

(4) $\alpha\beta = 0 \implies \alpha = 0$ 或 $\beta = 0$ (零積律);

(5) $\alpha \leq \beta \implies \alpha\gamma \leq \beta\gamma$ (單調律);

(6) $0\alpha = 0$ (零律);

(7) $1\alpha = 1$ (單位律).

證明 證明留給讀者自行練習. □

命題 5.3.10 設 n 爲有限基數, 則

(1) $n\aleph_0 = \aleph_0$;

(2) $\aleph_0\aleph_0 = \aleph_0$;

(3) $n\mathfrak{c} = \mathfrak{c}$;

(4) $\mathfrak{c}\mathfrak{c} = \mathfrak{c}$;

(5) $\aleph_0\mathfrak{c} = \mathfrak{c}$.

證明 依命題 5.2.6 即得 (1). (2) 爲例 5.1.17 的等價敍述. (3)、(4)、(5) 留給讀者自行思考. □

注意 5.3.11 命題 5.3.10 指出, 基數乘積並無消去律.

參考資料

[1] Charles C. Pinter. *A Book of Set Theory*. Dover Publications, Inc., 2014.

[2] 邓辉文. 离散数学. 第 3 版. 清华大学出版社, 2014.

[3] 董教总华文独中工委会统一课程委员会. 高级数学（高一上册）. 马来西亚华校董事联合会总会（董总）, 2023.

[4] 董教总华文独中工委会统一课程委员会. 高级数学（高二下册）. 马来西亚华校董事联合会总会（董总）, 1996.

[5] 刘守民, 熊锐. 集合论、拓扑与代数初步. 第 1 版. 清华大学出版社, 2019.

[6] 程守慶. 數學導論. 華藝數位股份有限公司, 2023.