Contents

1 前言：關於證明和邏輯

自然科學觀察的對象是大自然. 科學家發展的學說, 無論多麼有天才巧思, 最後的判斷標準來自外在的大自然, 而不是人的心靈.

但是數學很特別, 數學透過科學理論間接與大自然有關. 當科學家以數學語言建構理論時, 如果遇到與預測不符, 並沒有人懷疑是其中的數學有問題, 這表示數學理論的成立, 另有特殊的來源, 和科學非常不同.

一般人視數學為真理, 其理論的成立來自嚴格的證明, 現代數學的領域雖然博雜, 有些異常深刻, 但這個原則始終不變. 數學家和科學家都需要高超的想像與洞識, 發明玄妙的概念, 解決難纏的問題, 但是作為最後裁判依據的, 前者依靠證明、後者仰賴現實世界（實驗）. 這個倚賴嚴格推理的原則是數學的基本特徵. 換句話說, 學數學首先要知道如何證明你手中的命題.

數學證明和邏輯有重要的關係, 但兩者並不相等. 證明就像寫論理的文章, 內容可以關乎各式各樣大家關心的議題, 而邏輯在其中只占有是否符合文法、論證是否成立的部分, 和文章實質內容完全無關. 這個角色看似側面, 卻異常關鍵：因為論理的文章如果論證有問題就沒有價值了.

邏輯就好像每天跑步、體操或健身, 是為了鍛鍊身體, 協助我們完成人生的重要目標. 學習邏輯的目的, 是協助我們順利學習和研究數學[1]. 尤其, 邏輯來自日常語言的思想結構, 如果你思想一向條理清楚, 或許沒有必要特意學習邏輯, 就能寫出嚴格的數學證明. 另一方面, 邏輯的某些論證規律, 有時也相當困擾人, 否則就不會出現許多夾纏不清的論戰.

因此, 接下來兩節邏輯的介紹, 是一種輔助性的材料, 說明在數學中常見的論證方式、規則、應用, 甚至來龍去脈. 如果你已經很熟悉, 盡可以跳過去. 但如果你比較陌生或常常有疑惑, 希望其中一些說明, 能夠對你有幫助.

值得提醒的是, 證明如同寫論理文章, 除了確認自己想法的正確性之外, 同時也是寫給其他關心相同論題的人閱讀的. 既然書寫證明本身帶有與同行溝通的目, 因此即使邏輯相同, 如何書寫一個證明或經營一系列證明, 讓其他人能很快看懂證明的本質與意義, 也是各位學習數學時應該著墨的地方.

總之, 研究數學不等於書寫邏輯正確的證明, 這只是一個必要條件. 如果你學習數學時, 能夠深入思考證明背後的意義, 積極學習和同學溝通你的看法, 很快就能理解這層意思了.

---

[1]當然, 有人可能把健身當作人生目標, 但這是少數人. 在數學中有一個專攻邏輯的領域, 稱為數理邏輯, 但是絕大部分數學家, 都只理解數理邏輯到某種程度, 而不是數理邏輯家.

1.1 一個例子

示例. a 是偶數且 b 是奇數, 則 $a+b$ 是奇數.

證明.

a 是偶數, 表示 $a=2k$; 而 b 是奇數, 表示 $b=2l+1$, 因此 $a+b=2k+2l+1=2(k+l)+1$, 證完.

□

這是一個直接的證明, 各位在高中做的證明基本上都是直接計算證明. 但是底下類似的敘述, 可以這樣來證明嗎？

示例. 若 a 是有理數, b 是無理數, 則 $a+b$ 是無理數.

a 是有理數, 表示 $a=\frac{p}{q}$, 其中 p, q 是非零整數, 且不妨假設 p,q 互質 (不是重點). 但是無理數呢？「b 是無理數」只能透過「b 不是有理數」來定義, 缺乏正面可計算的表示法. 如此一來, 上面的直接計算證明法就毫無用武之地. 怎麼辦呢？注意: 在這個脈絡裡, 能算的只有有理數, 有可能透過這一點來證明嗎？

底下有四個「證明」, 哪一個是正確的？已知 a 是有理數, 寫成 $a=\frac{p}{q}$.

1. 「如果 b 不是無理數而是有理數，由計算知道 $a+b$ 是有理數，所以如果 b 是無理數，那 $a+b$ 必是無理數。」
2. 「已知 b 是無理數。若 $a+b$ 不是無理數而是有理數，由計算知 $b=(a+b)-a$ 是有理數，與前提矛盾，因此 $a+b$ 必為無理數。
3. 原來的敘述相當於「若 a 是有理數, $a+b$ 是有理數, 則 b 是有理數」，但由計算這顯然正確，因此原來的敘述是正確的。
4. 原來的敘述相當於「若 a 是有理數, $a+b$ 是有理數, 則 b 是有理數」, 但因為由計算知「b 是有理數且 $a+b$ 是有理數, 則 a 是有理數」，因此原來的敘述是正確的。

討論. 那個論證是對的？

注意到上面四個「證明」裡的計算都是對的, 因此問題完全不在計算, 而是論證的方式是否合理. 我們要如何判斷自己做了一個合理或不合理的論證呢？底下先介紹一般數學敘述常用的語句形式。

2 命題演算

可以判斷真 (T) 或假 (F) 的句子, 稱為命題 (proposition) . 數學敍述的基礎即是命題. 例如「7 是質數」、「$\sqrt{5} > 3$」、「四邊形的四邊平方和等於兩對角線平方和」、「任何一個自然數都有另一個自然數比它小」等都是數學的命題。

P
T
F

2.1 複合命題

從某些「原子」命題開始, 依靠五種邏輯連接詞, 可以得到更長更複雜的複合命題:

2.1.1 命題的否定: 非 P

命題 P 的否定「非 P」記為 $\neg P$，$\neg P$ 和 P 的真假關係如下：

P	$\neg P$
T	F
F	T

例如真命題「7 是質數」的否定「7 不是質數」就是假命題；假命題「$\sqrt{5} > 3$」的否定命題「$\sqrt{5} \ngtr 3$」(或寫成「$\sqrt{5} \leqslant 3$」) 為真。有趣的是「四邊形的四邊平方和等於兩對角線平方和」的否定命題是什麼？是「四邊形的四邊平方和不等於兩對角線平方和」嗎？「任何一個自然數都有另一個自然數比它小」的否定命題是什麼？是「任何一個自然數都有另一個自然數不小於它」嗎？(後面我們會再回到這個問題)

2.1.2 P 且 Q

像「5 是質數且 5+2 也是質數」這類命題，牽涉到邏輯連接詞「且」(and)。「P 且 Q」記為 $P \wedge Q$, 其複合命題的真假如下:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

換句話說，只要 P 或 Q 其中有一個為假，則 $P \wedge Q$ 就是假命題。或者說，複合命題 $P \wedge Q$ 想要為真，就必須子命題 P 和 Q 同時皆為真。

例如「5 是質數且 $5+2$ 是質數」是真命題，但是「7 是質數且 $7+2$ 是質數」是假命題。另外，雖然看起來有點怪，不過「13 是質數且對頂角相等」是真命題。

2.1.3 P 或 Q

「1 是質數或 1 是合成數」這類命題牽涉到邏輯連接詞「或」(or)。「P 或 Q」記為 $P \vee Q$, 其複合命題的真假如下:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

換句話說，只要 P 或 Q 其中有一個為真，則 $P \vee Q$ 就是真命題。或者說，複合命題 $P \vee Q$ 要為假，就必須子命題 P 和 Q 同時皆為假。

例如「1 是質數或 1 是合成數」是假命題，但是「3764323 是質數或 3764323 是合成數」則是真命題。另外，怪怪的「13 是質數或對頂角相等」是真命題。

2.1.4 若 P 則 Q

由命題 P「推理」出 Q 是證明的根本，像「13 是整數則 13 是有理數」這類命題牽涉到邏輯連接詞「則」。「若 P 則 Q」記為「$P \Rightarrow Q$」, 其複合命題的真假

如下:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

「若 P 則 Q」英文寫成 If P then Q, 不過也可寫成 Q if P 或 P only if Q。其中 P 稱為 Q 的充分條件（sufficient condition），Q 稱為 P 的必要條件（necessary condition）。所以「13 是整數則 13 是有理數」是真命題，「-2 是整數則 -2 是自然數」則是假命題。如果用日常的例子：「天雨則地濕」是真命題，「天雨則地不濕」是假命題。至於「天不雨」，則「地濕」「地不濕」都有可能，因此都算真命題！

其實 $P \Rightarrow Q$ 的真假值安排經常讓人感到疑惑，例如按照這個規則「13 是質數則對頂角相等」是一個真命題。但是我們怎麼從「13 是質數」推導到「對頂角相等」呢？! 更糟的是，如果以「4 是質數」為前提，則「4 是質數則 $\sqrt{2}$ 不是有理數」和「4 是質數則 $\sqrt{2}$ 是有理數」都是真命題。

簡而言之，$\Rightarrow$ 真假值規則只保證：前提為真時「推出」真命題的整個命題為真；前提為真時「推出」假命題的整個命題為假。我們通常認為的推理，牽涉到命題內容之間的因果關係，這時如果真命題 P 的確能推理出 Q（因此 Q 也是真命題），則至少前述規則保證 $P \Rightarrow Q$ 為真。另外真命題 P 竟然推理出假命題 Q，這是不可能的，那麼至少前述規則保證 $P \Rightarrow Q$ 為假。換句話說，$\Rightarrow$ 的真假值規則至少相容於真正的推理。至於，假命題前提既然為假，那結論是真是假都有可能，因此都給 $P \Rightarrow Q$ 真值。

總之，就像學語文時要學文法，正確的句子必須遵守文法，但遵守文法的句子並不見得有意義。命題演算 $P \Rightarrow Q$ 是一種文法式的規則，和牽涉到語意內容的推理並不相同，只是相容罷了 [2]。但是後面我們會看到它的用處。

2.1.5 P 和 Q 等價

「P 等價於 Q」意思是 P 和 Q 的真假值相同，記為 $P \Leftrightarrow Q$，其真值表

[2] 請參考
https://highscope.ch.ntu.edu.tw/wordpress/?p=32474 (〈奇怪的若 P 則 Q (一)〉)
https://highscope.ch.ntu.edu.tw/wordpress/?p=32530 (〈奇怪的若 P 則 Q (二)〉)
https://highscope.ch.ntu.edu.tw/wordpress/?p=12492 (李國偉〈真值蘊涵〉)

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

其意義我們後面再來說明。

2.1.6 複合命題的真假值

所有複合命題都是由「原子」命題以連接詞組成的, 因此其真假值由各原子命題的真假值, 透過上述真值表來決定.

示例. 討論 $P \wedge (Q \vee R)$ 的真假. 共有八種情況, 依序取值如下:

P	$\wedge$	$(Q$	$\vee$	$R)$
T		T		T
T		F		T
F		T		T
F		F		T
T		T		F
T		F		F
F		T		F
F		F		F

$\longrightarrow$

P	$\wedge$	$(Q$	$\vee$	$R)$
T		T	T	T
T		F	T	T
F		T	T	T
F		F	T	T
T		T	T	F
T		F	F	F
F		T	T	F
F		F	F	F

$\longrightarrow$

P	$\wedge$	$(Q$	$\vee$	$R)$
T	T	T	T	T
T	T	F	T	T
F	F	T	T	T
F	F	F	T	T
T	T	T	T	F
T	F	F	F	F
F	F	T	T	F
F	F	F	F	F

□

示例. $(P \ \Leftrightarrow\ Q) \ \Leftrightarrow\ ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$.

$(P$	$\Leftrightarrow$	$Q)$	$\Leftrightarrow$	$((P$	$\Rightarrow$	$Q)$	$\wedge$	$(Q$	$\Rightarrow$	$P))$
T	T	T	T	T	T	T	T	T	T	T
T	F	F	T	T	F	F	F	F	T	T
F	F	T	T	F	T	T	F	T	F	F
F	T	F	T	F	T	F	T	F	T	F

這可以解釋成 $P \Leftrightarrow Q$ 相當於 $((P \Rightarrow Q)$ 而且 $(Q \Rightarrow P))$ 的意思, 很多人根本用這個敘述當作「 $\Leftrightarrow$ 」的定義. □

2.1.7 恆真命題和恆假命題

有一類特別的複合命題稱為「恆真」命題 (tautology)．這類命題和各原子命題的真假取值毫無關係, 是和具體內容無關, 絕對為真的邏輯命題, 因此可以當作命題系統內的定理, 性質或公設. 後面將會大量討論.

如果你懷疑怎麼可能有這樣的命題, 最簡單的例子只用到一個原子命題 P:

示例. $P \vee \neg P$.

P 和 $\neg P$ 兩者必有一為真, 依 $\vee$ 的規則, 此複合命題必為真. □

如果 a 是一個整數，那「a 是偶數或 a 是奇數」必為真，因為 $\neg$「a 是偶數」就是「a 是奇數」。日常生活也有很多這類例子：「天空要嘛下雨要嘛不下雨」,「眼前的人要嘛是新一, 不然就不是新一」, 了無意義是這類恆真句的特徵. 但是 $P \vee \neg P$ 在古典邏輯稱為「排中律」, 説明除 P 和非 P 之外再無其他可能, 因此兩者必有一成立. 這的確是和命題內容無關的定律.

反過來, 還有一類命題稱為恆假命題, 也可稱為矛盾命題, 解釋起來就是不可能發生的事情.

示例. $P \wedge \neg P$.

P 和 $\neg P$ 兩者必有一為假, 依 $\wedge$ 的規則, 此複合命題必為假. □

注意到這也是和命題具體內容毫無關係絕對為假的命題。例如若 a 滿足 $a^7 - a^4 + a + 1 = 0$（也就是方程式 $x^7 - x^4 + x + 1 = 0$ 的根）, 那「$a > 0$ 而且 $a \leqslant 0$」顯然是完全不需要計算就知道為假的命題. .

2.2 等價的命題

前面提到的「$(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$」就是恆真句。這類句子的特徵是 $A \Leftrightarrow B$, 中間的連接詞是 $\Leftrightarrow$, 而 $\Leftrightarrow$ 下方的真假值都是 T, 因此是恆真句. 由於 $\Leftrightarrow$ 兩邊的真假值必須完全相同才會是 T, 因此可把兩邊的命題當作同義，或稱為等價的命題, 有時直接寫成 $A = B$. 例如 $(P \Leftrightarrow Q) = ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$.

底下這些等價的命題有些很直觀, 有些可能得多想想才能領會.

示例.

1. (De Morgan's law)

$\neg(P \vee Q) \;\Leftrightarrow\; \neg P \wedge \neg Q$ (或 $\neg(P \vee Q) = \neg P \wedge \neg Q$)

$\neg(P \wedge Q) \;\Leftrightarrow\; \neg P \vee \neg Q$ (或 $\neg(P \wedge Q) = \neg P \vee \neg Q$) .

2. (分配律)

   $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$;

   $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$

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

□

討論. 舉些例子討論這些等價命題是否有道理. 特別留意 3. 中對於 $P \Rightarrow Q$ 的重新「詮釋」.

習題 2.1. 模仿前例, 證明下面的敍述.

1. $P = \neg\neg P$
2. (交換律) $P \wedge Q = Q \wedge P$, $P \vee Q = Q \vee P$
3. (結合律) $P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$, $P \vee (Q \vee R) = (P \vee Q) \vee R$
4. $(P \;\Leftrightarrow\; Q) = (P \wedge Q) \vee (\neg P \wedge \neg Q)$
5. $(P \Rightarrow Q) = (\neg Q \Rightarrow \neg P)$
6. $((P \wedge Q) \Rightarrow R) = (P \Rightarrow (Q \Rightarrow R))$

習題 2.2. 證明 $P \vee \neg P$, $\neg(P \wedge \neg P)$, $P \Rightarrow P$ 都是恆真式. 它們和 $P \Rightarrow \neg\neg P$ 或 $\neg\neg P \Rightarrow P$ 有何關係 ?

由以上的證明過程, 你可能已經發現:

習題 2.3. 形式上來說, 證明所有複合命題的連接詞其實只需要用到 $\neg$ 和 $\vee$ 就夠了. 如果用 $\neg$ 和 $\Rightarrow$ 可以嗎 ?

2.3 命題演算與邏輯推理律

底下説明有一些恆真句, 最後牽涉到 $\Rightarrow$. 如果把這當成「推得」, 其實就是「證明」或「推理」時, 經常用到的推理法則.

示例.

1. $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$. 已知 P 為真, 且 $P \Rightarrow Q$, 可以推得 Q. 這是最基本的推理律, 稱為「肯定前件」(Modus Ponens) .

$((P$	$\Rightarrow$	$Q)$	$\wedge$	$P)$	$\Rightarrow$	Q
T	T	T	T	T	T	T
T	F	F	F	T	T	F
F	T	T	T	F	T	T
F	T	F	T	F	T	F

2. $((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$. 已知 $P \Rightarrow Q$, 但 Q 為假, 則可推得 P 為假, 稱為「否定後件」(Modus tollens) .

3. $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$. 若可從 P 推得 Q, 而且從 Q 推得 R, 則從 P 可以推得 R. 這是推論的遞移律, 稱為「假言三段論」(hypothetical syllogism) . 這是構成證明的基本結構.

4. $\neg(\neg P) \Rightarrow P$. 想要證明 P, 可以證明 $\neg P$ 是錯的. 稱為「反證法」(proof by contradiction).

5. $(\neg P \Rightarrow (Q \wedge \neg Q)) \Rightarrow P$. 想證明 P, 若能從 $\neg P$ 推出矛盾, 則 P 就為真. 這就是知名的歸謬法 (reductio ad absurdum) .

6. $(\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q)$. 想要證明 $P \Rightarrow Q$, 可以證明 $\neg Q \Rightarrow \neg P$. 稱為原來命題的逆反命題 (transposition) .

7. $\neg(P \wedge \neg Q) \Rightarrow (P \Rightarrow Q)$. 若能證明 P 和 $\neg Q$ 不可能同時成立, 則證明 $P \Rightarrow Q$, 這其實是將反證法用到 $P \Rightarrow Q$ 的結果.

□

注意. 想想 2., 6., 7. 是不是一樣的. 4. 和 5. 呢？

特別提醒, 如果善用等價的命題 $(A = B)$, 就不見得要靠繁瑣的真值表來證明所有恆真句. 例如

$$(P \Rightarrow Q) = (\neg P \vee Q) = (Q \vee \neg P) = (\neg\neg Q \vee \neg P) = (\neg Q \Rightarrow \neg P)$$

就簡單證明 $(P \Rightarrow Q) = (\neg Q \Rightarrow \neg P)$. [3]

[3]命題演算的一種表示法, 可以完全不用真值表, 只依靠一些恆真命題稱為公設以及推理法則, 而得到所有系統中的定理 (或恆真命題) . 如果你擔心這樣的系統只關心恆真命題, 似乎跟現實世界無關, 那你得先想想, 其實數學命題也都是恆真命題, 只是系統比命題演算複雜. 利用公設來推導真命題, 從古希臘歐基里德的《原本》就已經開始了.

$\boxed{\textbf{習題}}$ **2.4.** 用上述想法, 盡量重新證明前面的邏輯推論規則, 我們是不是總要先假設些什麼?

$\boxed{\textbf{習題}}$ **2.5.** 證明下列歸謬法的不同形式:

1. $(\neg P \Rightarrow Q) \Rightarrow ((\neg P \Rightarrow \neg Q) \Rightarrow P)$;
2. $((\neg P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q)) \Rightarrow P$.

$\boxed{\textbf{習題}}$ **2.6.** 證明下列邏輯推理規則, 哪些你本來就認為是對的?

1. $(P \Rightarrow (Q \Rightarrow R)) \Rightarrow ((P \Rightarrow Q) \Rightarrow (P \Rightarrow R))$
2. $\neg P \Rightarrow (P \Rightarrow Q)$
3. $((P \vee Q) \wedge \neg P) \Rightarrow Q$
4. $(P \wedge Q) \Rightarrow P$
5. $P \Rightarrow (P \vee Q)$
6. $((P \Rightarrow Q) \wedge (P \Rightarrow R)) \Rightarrow (P \Rightarrow (Q \wedge R))$ (反過來, 也對嗎？)
7. $((P \Rightarrow Q) \vee (P \Rightarrow R)) \Rightarrow (P \Rightarrow (Q \vee R))$ (反過來, 也對嗎？)
8. $((P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow R)) \Rightarrow R$
9. $((P \Rightarrow Q) \wedge (R \Rightarrow S)) \Rightarrow ((P \wedge R) \Rightarrow (Q \wedge S))$
10. $((P \Rightarrow Q) \wedge (R \Rightarrow S)) \Rightarrow ((P \vee R) \Rightarrow (Q \vee S))$

2.3.1 反例

證明時偶而會碰到看似正確但其實錯誤的「推理規律」或命題. 當然運用真值表去檢查是一個基本的方法, 但有時練習找出反例可能更靈活.

例如從下面的真值表, 已看出 $P \Rightarrow Q$ 和 $Q \Rightarrow P$ 並非等價.

$(P$	$\Rightarrow$	$Q)$	$\Leftrightarrow$	$(Q$	$\Rightarrow$	$P)$
T	T	T	T	T	T	T
T	F	F	F	F	T	T
F	T	T	F	T	F	F
F	T	F	T	F	T	F

這是最常見的推理錯誤. 反例可以簡單的舉如:「天雨則地濕」是對的, 但「地濕則天雨」是錯的, 因為可能還有別的原因造成地濕. 通常也可舉數學簡易的例子, 例如「$a = 2$ 則 $a^2 = 4$」是對的, 但反過來「若 $a^2 = 4$ 則 $a = 2$」當然是錯的. 尋找反例可以針對真假值不一致的地方.

$\boxed{\textbf{習題}}$ **2.7.** 下面的「規律」是對的嗎？如果不對, 請找出反例.

1. $((P \vee Q) \Rightarrow R) \Rightarrow ((P \Rightarrow R) \vee (Q \Rightarrow R))$
2. $((P \wedge Q) \Rightarrow R) \Rightarrow ((P \Rightarrow R) \wedge (Q \Rightarrow R))$
3. $((P \vee Q) \Rightarrow R) \Rightarrow ((P \Rightarrow R) \wedge (Q \Rightarrow R))$
4. $((P \wedge Q) \Rightarrow R) \Rightarrow ((P \Rightarrow R) \vee (Q \Rightarrow R))$

2.4 回到最前面的例子

回顧第3頁的四個證明. 令 P 是「a 是有理數」, Q 是「b 是有理數」, R 是「$a+b$ 是有理數」, 原來要證明的敘述是

$$(P \wedge \neg Q) \Rightarrow \neg R$$

第三個證明

我們知道只有在 P（a 是有理數）、Q（b 是有理數）和 R（$a+b$ 是有理數）時才能計算, 因此可以嘗試從命題演算, 去得到跟上式等價但只用到 P、Q、R 的命題。例如

$$\begin{aligned}(P \wedge \neg Q) \Rightarrow \neg R &= P \Rightarrow (\neg Q \Rightarrow \neg R) \\ &= P \Rightarrow (R \Rightarrow Q) \\ &= (P \wedge R) \Rightarrow Q\end{aligned}$$

最後命題 $(P \wedge R) \Rightarrow Q$ 就是第三個證明中所謂的等價命題「若 a 是有理數, $a+b$ 是有理數, 則 b 是有理數」. 因此第三個證明是正確的。

第二個證明

第二個證明也是正確的。說明方式如下:

本已假設「a 是有理數」（P）與「b 是無理數」（$\neg Q$）。由計算知
「若 a 是有理數, $a+b$ 是有理數, 則 b 是有理數」 （$(P \wedge R) \Rightarrow Q$）

由逆反命題這相當於

「若 b 是無理數則 a 是無理數或 $a+b$ 是無理數」($\neg Q \Rightarrow (\neg P \vee \neg R)$)

但「b 是無理數」，因此

「a 是無理數或 $a+b$ 是無理數」　（已假設 $\neg Q$, 肯定前件）

但「a 是有理數」, 又因 $\neg P \vee \neg R$ 相當於 $P \Rightarrow \neg R$, 所以

「$a+b$ 是無理數」(已假設 P, 肯定前件)

因此由假設「a 是有理數」與「b 是無理數」，推得「$a+b$ 是無理數」，證完[4]。除了假設與用計算直接證明的簡單敘述，其他就是邏輯推理法則：逆反命題和肯定前件。

以第二個證明的精神，還可以用反證法（或歸謬法）來證明：

因為「若 a 是有理數, b 是無理數, 則 $a+b$ 是無理數」的反命題是「a 是有理數, b 是無理數, 且 $a+b$ 是有理數」。使用反証法，假設此反命題為真，但已知「若 a 是有理數, $a+b$ 是有理數, 則 b 是有理數」，因此若反命題為真, 則 b 同時為有理數和無理數，得到矛盾，因此該反命題必須為假，故原命題為真.

用命題符號寫起來就是

假設 $\neg((P \wedge \neg Q) \Rightarrow \neg R) = P \wedge \neg Q \wedge R$ 為真。但由計算知 $(P \wedge R) \Rightarrow Q$

由推理法則 $((P_1 \Rightarrow Q_1) \wedge (P_2 \Rightarrow Q_2)) \Rightarrow ((P_1 \wedge P_2) \Rightarrow (Q_1 \wedge Q_2))$

因此 $((P \wedge R) \wedge \neg Q) \Rightarrow (Q \wedge \neg Q)$

矛盾. 由歸謬法知前提為假，但前提 $(P \wedge R) \wedge \neg Q$ 是 $\neg((P \wedge \neg Q) \Rightarrow \neg R)$

故知 $(P \wedge \neg Q) \Rightarrow \neg R$ 為真，故證完.

錯誤的證明

第一個證明是錯的, 因為用了常見錯誤的推理律: $(P \Rightarrow Q) \Rightarrow (Q \Rightarrow P)$.

第四個證明重述於下:

原來的敍述相當於「若 a 是有理數, $a+b$ 是有理數, 則 b 是有理數」, 但因為由計算知「b 是有理數且 $a+b$ 是有理數, 則 a 是有理數」，因此原來的敍述是正確的。

形式上相當於 $((Q \wedge R) \Rightarrow P) \Rightarrow ((P \wedge R) \Rightarrow Q)$. 這顯然不成立 (可以舉反例知道) . 因此嚴格的說，第四個證明是錯的。

不過有些人看這個證明，會覺得似乎有幾分道理。這是因為在我們的問題脈絡裡, 命題「a 是有理數且 $a+b$ 是有理數, 則 b 是有理數」看起來有對稱性,

[4]這只是一種證明的寫法, 平常寫證明只要交代了來龍去脈就可以了.

a 在前面或 b 在前面感覺似乎沒什麼差別。這個錯誤或混淆有一個意義，說明如下:

- 「b 是有理數且 $a+b$ 是有理數, 則 a 是有理數」和前一句的 a, b 攪在一起, 造成混淆.
- 覺得有道理的人，心裡把這個敍述解釋成一個性質：「對任意 x, y, y 是有理數且 $x+y$ 是有理數, 則 x 是有理數」。如果不和 a,b 混淆，這樣寫十分清楚, 就算只寫成「y 是有理數且 $x+y$ 是有理數, 則 x 是有理數」大家也可以理解。如果這樣寫，證明其實是對的.
- 如果執意要用 a 和 b，就要寫成「對任意 a, b, b 是有理數且 $a+b$ 是有理數, 則 a 是有理數」這種一般規則的敍述方式, 雖然還是有混淆的危險，但至少清楚呈現這樣寫的意思.

如果答者的真正意思是第三個敍述, 其證明是對的. 問題是他的敍述方式不夠完善，和前面的敍述混淆. 這告訴我們有沒有加上前面的「對任意 a, b」有很大的差別, 這帶我們進入下個課題.

3 述詞演算; 一階邏輯

在數學中看到的命題, 通常是針對某一個「集合」裡面的元素, 表明這些元素是不是有某個性質. 例如「所有的自然數都大於 0」, 「某些自然數是質數」, 「對任意自然數 p, a, b, 如果 p 整除 ab, 且 p 是質數, 則 p 整除 a 或 p 整除 b. 」

3.1 量詞的必要性

常見的性質如「a 是偶數且 b 是奇數, 則 $a+b$ 是奇數」嚴格的說, 應該寫成「對任意整數 a, b, 若 a 是偶數且 b 是奇數, 則 $a+b$ 是奇數」. 用符號來寫, 可以記成

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z} \;\; P(a,b)$$

其中 $\forall$ 是一種量詞 (quantifier) 表示「對所有」或「對任意」, 而 $P(a,b)$ 就像帶著變數 a, b 的函數, 定義成

$$P(a,b) \;=\; ((E(a) \wedge \neg E(b)) \Rightarrow \neg E(a+b))$$

其中 $E(a)$ 表示 a 是偶數, 而在整數中 $\neg E(a)$ 表示 a 不是偶數, 亦即 a 是奇數. 所以原式也可以寫成

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z} \;\; (E(a) \wedge \neg E(b) \Rightarrow \neg E(a+b))$$

這樣的「語言」系統稱為「述詞演算」(predicate calculus) 或一階邏輯 (first order logic) . 底下是邏輯書中常舉的例子, 從上節命題演算並無法「證明」:

凡人皆有死, 蘇格拉底是人, 所以蘇格拉底會死.

$$(\forall p(M(p) \Rightarrow D(p)) \wedge M(\text{蘇格拉底})) \Rightarrow D(\text{蘇格拉底})$$

其中 $M(p)$ 表示「p 是人」, $D(p)$ 表示「p 會死」.

因此述詞演算是一個以命題演算為基礎, 更細緻的「語言」系統. 另外, 在邏輯系統中, 量詞的使用預設某個討論的範圍 (例如上述的自然數, 人類) , 這個「範圍」在數學裡通常運用集合的概念, 但如果只是討論述詞演算的邏輯性質與推理, 這個「範圍」並不重要, 「集合」的概念將在後面介紹.

3.2 量詞與其性質

我們先介紹量詞, 再討論量詞的性質與含量詞的推理. 常用的量詞有兩種:

1. $\forall x$: 表示「對所有 x」(對任意 x). 命題 $\forall x\, P(x)$ 為真的條件是對所有可能的 a, $p(a)$ 皆為真. 例如實數中 $\forall x\ \ x^2 \geqslant 0$ 為真; $\forall x\ \ x^2 > 0$ 為假.

2. $\exists x$: 表示「存在 x」(有某個 x). 命題 $\exists x\, P(x)$ 為真的條件是可以找到某個 a 使得 $P(a)$ 為真. 例如 $\exists x\ \ x^2 \leqslant 0$ 為真; $\exists x\ \ x^2 < 0$ 為假.

再以 $x+3>0$ 為例. 在自然數中, 用常數 7, -10, 代入上面的公式得 $7+3>0$ 為真; $-10+3>0$ 為假. 因為 $7+3>0$ 為真, 因此 $\exists x\ \ x+3>0$ 為真. 而因為 $-10+3>0$ 為假, 所以 $\forall x\ \ x+3>0$ 為假. 至於 $x+3>0$ 這樣的句子, 則因為 x 是 (自由) 變數, 沒有真假值, 所以不是命題. 因此,

> 一個有變數 $x_1, \cdots, x_n$ 的公式 $Q(x_1, \cdots, x_n)$, 只有在前方針對每一變數都加上量詞如 $\forall x_1 \cdots \forall x_n\ \ Q(x_1, \cdots, x_n)$, 才能夠判斷真假, 也才是命題.

述詞演算中的命題可由前節的「連接詞」再加上量詞得到新型的複合命題, 因此需要一些新的性質, 來辨認同義的命題. 說明這些性質時，把 $\forall x\, P(x)$ 想成 $P(a_1) \wedge P(a_2) ... \wedge P(a_N)$, $\exists x\, P(x)$ 想成 $P(a_1) \vee P(a_2) ... \vee P(a_N)$ 特別有用:

1. $\neg(\forall x\, P(x)) \Leftrightarrow \exists x\ \neg P(x)$. 例如 $\neg(\forall x\ \ x^2 \geqslant 0) \Leftrightarrow (\exists x\ \ x^2 < 0)$;

   $\neg$「所有人皆會死」 $\Leftrightarrow$「有人不會死」.

   $\neg(\exists x\, P(x)) \Leftrightarrow \forall x\ \neg P(x)$. 例如 $\neg(\exists x\ \ x^2 \leqslant 0) \Leftrightarrow (\forall x\ \ x^2 > 0)$.

   $\neg$「有人不喜歡數學」 $\Leftrightarrow$「所有人都喜歡數學」

2. $(\forall x\, P(x)) \wedge (\forall x\, Q(x)) \Leftrightarrow \forall x\, (P(x) \wedge Q(x))$.

   「所有人皆會死」$\wedge$ 「所有人都是動物」 $\Leftrightarrow$ 「所有人都是會死的動物」

   $(\exists x\, P(x)) \vee (\exists x\, Q(x)) \Leftrightarrow \exists x\, (P(x) \vee Q(x))$.

   「有些數是奇數」$\vee$ 「有些數是質數」 $\Leftrightarrow$ 「有些數是奇數或質數」

3. $(\forall x\, P(x)) \vee (\forall x\, Q(x)) \Leftrightarrow \forall x \forall y\, (P(x) \vee Q(y))$.

   $(\exists x\, P(x)) \wedge (\exists x\, Q(x)) \Leftrightarrow \exists x \exists y\, (P(x) \wedge Q(y))$.

4. $(\forall x\, P(x)) \Rightarrow Q \Leftrightarrow \exists x\, (P(x) \Rightarrow Q)$, 其中 x 不是 Q 的自由變數.

   $P \Rightarrow (\forall x\, Q(x)) \Leftrightarrow \forall x\, (P \Rightarrow Q(x))$, 其中 x 不是 P 的自由變數.

習題 3.1. 仔細想想, 為什麼「所有人皆會死」的否定不是「所有人皆不會死」? 為什麼「有人喜歡數學」的否定不是「有人不喜歡數學」?「有人喜歡數學」和「有人不喜歡數學」意思一不一樣？

習題 3.2. 說明下式成立. 其中 x 不是 P, Q 的自由變數.

1. $(\forall x\, P(x)) \wedge Q \Leftrightarrow \forall x\, (P(x) \wedge Q)$; $(\forall x\, P(x)) \vee Q \Leftrightarrow \forall x\, (P(x) \vee Q)$.

2. $(\exists x\, P(x)) \vee Q \Leftrightarrow \exists x\, (P(x) \vee Q)$; $(\exists x\, P(x)) \wedge Q \Leftrightarrow \exists x\, (P(x) \wedge Q)$.

3. $(\exists x\, P(x)) \Rightarrow Q \Leftrightarrow \forall x\, (P(x) \Rightarrow Q)$; $P \Rightarrow (\exists x\, Q(x)) \Leftrightarrow \exists x\, (P \Rightarrow Q(x))$.

習題 3.3. 找出反例.

1. 為什麼 $(\forall x\, P(x)) \vee (\forall x\, Q(x))$ 和 $\forall x\, (P(x) \vee Q(x))$ 不一樣？

2. 為什麼 $(\exists x\, P(x)) \wedge (\exists x\, Q(x))$ 和 $\exists x\, (P(x) \wedge Q(x))$ 不一樣？

3. 為什麼 $(\forall x\, (P(x) \Rightarrow Q(x))$ 和 $(\forall x\, P(x)) \Rightarrow (\forall x\, Q(x))$ 不一樣？

特別提醒: 一般來說, 命題「x 是質數 $\Rightarrow x$ 是奇數」感覺似乎有真假, 而且我們認為是錯的. 這是因為我們自動加上量詞「$\forall x$」, 變成「$\forall x$ (x 是質數 $\Rightarrow x$ 是奇數)」, 也就是考慮了整體敘述的真假. 如果只是個別來看, 其實只有 $x = 2$ 時是假, 其他質數都是真. 這個暗中加上 $\forall x$ 的約定, 經常出現在數學敘述裡.

3.3 雙量詞的性質

數學的敍述中經常會用到兩個以上的量詞, 底下就以兩個量詞為例, 其他類推. 首先, 雙量詞是這樣定義的:

$$\forall x \forall y P(x,y) = \forall x(\forall y P(x,y))$$

$$\forall x \exists y P(x,y) = \forall x(\exists y P(x,y))$$

以此類推. 當量詞如第二個式子有參差時, 必須要小心順序.

示例. 量詞相同可以交換順序.

1. $\forall x \forall y P(x,y) = \forall y \forall x P(x,y)$. 例如前述奇偶數的例子.

$$\forall a, \forall b\ ((E(a) \wedge \neg E(b)) \Rightarrow \neg E(a+b))$$

2. $\exists x \exists y P(x,y) = \exists y \exists x P(x,y)$. 例如

$$\exists a \exists b\ (E(a) \wedge \neg E(b) \wedge E(a+b))$$

□

示例. 量詞不同, 變數或順序不同的意義可能不同. 檢視底下的敍述, 其中前兩句是量詞順序調換, 後兩句也是. 假設討論的是自然數.

1. $\exists x \forall y\ \ x \leqslant y$. 「有一數小於或等於所有數」, 1 就是這樣的數, 命題為真.
2. $\forall y \exists x\ \ x \leqslant y$. 「任意一數必有一數比它小或相等」為真, 選這個數即可.
3. $\exists y \forall x\ \ x \leqslant y$. 「有一個數大於或等於所有數」, 因為自然數每一個數後面都還有個數 (所以有無限多數) , 這是不可能的.
4. $\forall x \exists y\ \ x \leqslant y$. 「任意一數必有一數比它大或相等」, 同 2., 這當然是對的.

□

習題 3.4. 將上例中的「$\leqslant$」改成「$<$」. 重新討論這個例子

習題 3.5. 在人的範圍內, 用 $L(a,b)$ 表示「a 喜歡 b」, 確認這些話的意思:

1. $\forall a \exists b\ L(a,b)$.
2. $\exists b \forall a\ L(a,b)$.

3. $\forall b \exists a\ L(a,b)$.

4. $\exists a \forall b\ L(a,b)$.

習題 **3.6.** 若 a 是女性, b 是人. $B(a,b)$ 表示「a 生 b」(a 是 b 的生物母親) , 下面哪句話表示「人皆有母」.

1. $\forall a \exists b\ B(a,b)$.

2. $\exists b \forall a\ B(a,b)$.

3. $\forall b \exists a\ B(a,b)$.

4. $\exists a \forall b\ B(a,b)$.

在前面的例子, 知道 $\exists y \forall x\ x \leqslant y$ 是錯的, 這表示它的否定是正確的, 問題是它的否定是什麼？依照定義得

$$\neg\,(\exists y\,(\forall x\, x \leqslant y)) = \forall y\ \ \neg\,(\forall x\ \ x \leqslant y) = \forall y \exists x\ \ x > y$$

這句話的意思是「任一數都 (至少) 有一數比它還大」, 這正是自然數的性質.

習題 **3.7.** 否定前面習題中你認為錯誤的敍述, 並確認其正確性.

3.4 述詞演算的推理

和命題演算相同, 恆真命題在述詞演算中也扮演重要的角色: 公設, 定理, 邏輯律. 底下是有量詞情況下, 顯而易見的推理律

1. $(\forall x\ P(x)) \Rightarrow P(a)$, a 表示某常數. 也可寫成 $\forall y\ ((\forall x\ P(x)) \Rightarrow P(y))$.

2. $P(a) \Rightarrow (\exists x\ P(x))$.

3. $(\forall x\ P(x)) \vee (\forall x\ Q(x)) \Rightarrow \forall x\ (P(x) \vee Q(x))$

4. $\exists x\ (P(x) \wedge Q(x)) \Rightarrow (\exists x\ P(x)) \wedge (\exists x\ Q(x))$

5. $\forall x\ (P(x) \Rightarrow Q(x)) \Rightarrow ((\forall x\ P(x)) \Rightarrow (\forall x\ Q(x)))$

6. $\exists x \forall y\ P(x,y) \Rightarrow \forall y \exists x\ P(x,y)$

注意. 注意這些式子都不是等價, 後面四個式子我們曾經討論過.

習題 **3.8.** 說明下列規則是正確的.

1. $\forall x\ P(x) \Rightarrow \exists x\ P(x)$.
2. $\forall x\ (P(x) \Rightarrow Q(x)) \Rightarrow ((\exists x\ P(x)) \Rightarrow (\exists x\ Q(x)))$

注意. 如果這個習題的第一小題你認為沒有任何問題, 可能要小心. 「袋子裡的球都是藍色的」推得「袋子裡有藍色的球」需要一個前提: 「袋子裡有球」。然而，第二小題則沒有這個問題。

4 應用：關於輾轉相除法之二三事

4.1 基本定義

本節討論的「範圍」基本上都是非負整數 (有時也容許是整數) . 先回顧除法, 若 $m > n > 0$ 則 m 除以 n 得

$$m = n \cdot q + r, \quad 0 \leqslant r < n$$

q 是商, r 是餘數.

定義 4.1. (整除, 因數) 若 $m = n \cdot k$ 則 n 整除 m, 記為 $n \,|\, m$, 這時也說 n 是 m 的因數.

$$(n \,|\, m \iff \exists k\ (m = n \cdot k))$$

定義 4.2. (質數) 若 $p \neq 1$ 且其因數只有 1 和 p 本身, 則稱 p 是質數.

$$\mathrm{Pr}(p) \iff p \neq 1 \wedge \forall a(a \,|\, p \Rightarrow (a = 1 \vee a = p))$$

若 m 不是質數也不是 1, 則稱 m 是合數.

注意. 依此約定 1 不是質數也不是合數.

定義 4.3. (質因數) $\iff$ 若 p 是質數且 $p \,|\, m$, 則稱 p 是 m 的質因數.

$$\mathrm{Pr}(p) \wedge p \,|\, m$$

定義 4.4. (公因數) 若 k 同時是 m 與 n 的因數, 稱 k 是 m 與 n 的公因數.

$$\mathrm{cd}(k, m, n) \iff k \,|\, m \wedge k \,|\, n$$

注意. 若使用集合符號, 定義 m 與 n 公因數的集合 $\mathrm{cd}(m, n) = \{k \mid (k \,|\, m \wedge k \,|\, n)\}$, 用 $k \in \mathrm{cd}(m, n)$ 可能比 $\mathrm{cd}(k, m, n)$ 更易理解.

定義 4.5. (最大公因數) 若 d 是 m 與 n 公因數中最大的數, 則稱 d 是 m 與 n 的最大公因數 (gcd) .

$$d = \mathrm{gcd}(m, n) \ \Leftrightarrow \ \mathrm{cd}(d, m, n) \wedge \forall k \, (\mathrm{cd}(k, m, n) \Rightarrow k \leqslant d)$$

定義 4.6. (互質) 若 $\mathrm{gcd}(m, n) = 1$ 則稱 m 與 n 互質.

4.2 輾轉相除法

一般的短除法只能求簡單數字的最大公因數, 想求一般兩數的最大公因數, 需要知名而基本的歐基里德算則——輾轉相除法. 這個算則附帶贈送了一個很好用的定理, 解決了一些基礎的算術問題.

(輾轉相除法介紹)

將輾轉相除法的步驟寫清楚:

$$\begin{aligned}
m &= n \cdot q_0 + r_1 && (0 < r_1 < n) \\
n &= r_1 \cdot q_1 + r_2 && (0 < r_2 < r_1) \\
r_1 &= r_2 \cdot q_2 + r_3 && (0 < r_3 < r_2) \\
&\cdots && \cdots \\
r_{N-3} &= r_{N-2} \cdot q_{N-1} + r_{N-1} && (0 < r_{N-1} < r_{N-2}) \\
r_{N-2} &= r_{N-1} \cdot q_{N-1} + r_N && (0 < r_N < r_{N-1}) \\
r_{N-1} &= r_N \cdot q_N
\end{aligned}$$

從餘數的性質得 $n > r_1 > r_2 > \cdots \geqslant 0$, 因此知道必有 N, 使得 $r_{N+1} = 0$. 令 $d = r_N$.

性質 4.1. $d = \mathrm{gcd}(m, n)$

證明.

由最後一式知 $d \,|\, r_{N-1}$, 再由倒數第二式知 $d \,|\, r_{N-2}$, 依此類推得 $d \,|\, n$ 且 $d \,|\, m$, 即 d 是 m 與 n 的公因數.

若 k 是 m 與 n 的公因數, 由第一式 $k \,|\, r_1$, 再由第二式知 $k \,|\, r_2$, 依此類推, 一直到倒數第二式, 可得 $k \,|\, r_N$.

d 是 m 與 n 的公因數, 且所有公因數都整除 d, 因此 d 是 m 與 n 的最大公因數.

□

從輾轉相除法可得到下面的基礎性質:

性質 4.2. 若 $d = \gcd(m, n)$, 則必可找到整數 s, t, 使得 $sm + tn = d$.

證明.

從倒數第二式知

$$d = r_N = r_{N-2} - r_{N-1} \cdot q_{N-1}$$

從倒數第二式則知

$$r_{N-1} = r_{N-3} - r_{N-2} \cdot q_{N-1}$$

代入前式得

$$d = r_N = r_{N-2} - (r_{N-3} - r_{N-2} \cdot q_{N-1}) \cdot q_{N-1}$$

等號右邊消除 r_{N-1}, 將 d 寫成 r_{N-2} 和 r_{N-3} 的整係數組合; 接著再由上一個等式, 又可以消除 r_{N-2}, 將 d 改寫成 r_{N-3} 和 r_{N-4} 的整係數組合; 以此類推, 最後可將 d 寫成 m 和 n 的整係數組合.

□

注意. s 和 t 必互質 (為什麼？) .

習題 4.1. 有什麼好方法可以解出一組解？

4.3 重要應用

底下似乎是一個顯然正確的性質, 問題是怎麼證明呢？

性質 4.3. 若 p 為質數且 $p \mid mn$, 則 $p \mid m$ 或 $p \mid n$.

證明.

要證明上式, 只要證明若 $p \nmid m$, 則 $p \mid n$ 即可 (why?) .

假設 $p \nmid m$, 且 p 是質數, 因此 p 和 m 互質, 由**性質 4.2** 知, 存在 s 和 t, 使得 $sp + tm = 1$, 將等號兩邊同乘以 n 得

$$n = spn + tmn.$$

又因為 $p \mid mn$, 故 $p \mid n$, 得證.

□

習題 **4.2.** 用命題演算, 檢查證明第一行的 (why?) 正不正確？

習題 **4.3.** 若 p 為質數且 $p \mid m_1 m_2 \cdots m_n$, 則 $\exists i \;\; p \mid m_i$.

習題 **4.4.** 若 $k \mid mn$, 且 k 和 m 互質, 則 $k \mid n$. (注意未假設 k 是質數)

4.3.1 算術基本定理

由此性質可證明算術基本定理, 亦即質因數分解之唯一性.

定理 4.1. (算術基本定理) 若不計質因數分解乘積的順序, 一數的質因數分解是唯一的.

證明.

若該數有兩種質因數分解

$$A = p_1 p_2 \cdots p_N = q_1 q_2 \cdots q_M, \quad p_i, q_j \text{ 都是質數}$$

因為 p_1 是質數, 所以必有某 i, $p_1 \mid q_j$, 但因為 q_j 是質數, 所以 $p_1 = q_j$. 將兩邊同除以此數, 依此步驟, p_i 將與 q_j 一一配對, 證完.

□

習題 **4.5.** 為什麼任何一個自然數都有質因數分解？

4.3.2 丟番圖線性不定方程

示例. (Diophantine equation, 丟番圖線性不定方程)

給定非零整數 m 和 n, 求 $mx + ny = k$ 的所有整數解.

首先, 取 $d = \gcd(m, n)$. 若 $d \nmid k$, 則此方程組無解; 若 $d \mid k$, 在等號兩邊同除以 d, 得

$$m'x + n'y = k', \quad \text{此時 } m' \text{ 和 } n' \text{ 互質.}$$

1. ($k' = 0$) 由於要求的是整數解, 於是 $n' \mid m'x$, 但是因為 m' 和 n' 互質, 由**習題 4.4** 知 $n' \mid x$, 亦即 $x = n't$, 代入原式得 $y = -m't$, 因此一般解為 $(n't, -m't)$, $t \in \mathbb{Z}$.

2. ($k' \neq 0$) 因為 m' 和 n' 互質, 由**性質 4.2**知, 有整數 x_0 和 y_0 滿足 $m'x_0 + n'y_0 = 1$, 因此 $m'(k'x_0) + n'(k'y_0) = k'$ 是一組解. 若還有其他解, 由

$$\begin{cases} m'x + n'y &= k' \\ m'(k'x_0) + n'(k'y_0) &= k' \end{cases}$$

相減得

$$m'(x - k'x_0) + n'(y - k'y_0) = 0.$$

但這回到 1. 的情況, 因此得到一般解為

$$(k'x_0 + n't, k'y_0 - m't), \quad t \in \mathbb{Z}.$$

□

4.3.3 質數無限多個

歷史上, 想發明質數生成公式的嘗試都失敗了, 沒有辦法用正面的方式證明質數有無限多個. 但是歐基里德在古希臘時期, 就已經證明質數有無限多個, 他用的法寶就是歸謬法.

定理 4.2. 質數無限多個.

證明.

假設質數只有有限多個, 全部編號為 $p_1, p_2, \cdots, p_N$. 現考慮一數

$$A = p_1 \cdot p_2 \cdots p_N + 1$$

顯然 $A \neq 1$ 且 $\forall i \;\; A \neq p_i$, 因此 A 是合數. 但因為 p_i 除 A 都有餘數 1, 因此所有質數都不是 A 的因數, 從質因數分解知 A 本身必為質數. A 是合數也是質數, 矛盾！故原假設有誤, 即質數有無限多個.

□

4.3.4 $\sqrt{2}$ 是無理數

另一個和質數性質有關的知名歸謬法應用如下

性質 4.4. $\sqrt{2}$ 是無理數.

證明.

假設 $\sqrt{2}$ 是有理數, 則 $\sqrt{2}=\frac{p}{q}$, 且可以假設 p 和 q 互質. 由此得

$$2q^2=p^2$$

但由**性質 4.3**, $2\,|\,p^2 \Rightarrow 2\,|\,p$, 所以 $p=2k$, 再代入上式

$$2q^2=(2k)^2 \Rightarrow q^2=2k^2$$

於是 q 也是偶數, 和假設 p 和 q 互質矛盾, 所以 $\sqrt{2}$ 是無理數.

□

5 集合的概念

現代數學是以集合論為基礎而發展的 (尤其自從法國 Bourbaki 學派的工作之後) . 但是數學和集合論不同, 數學家對於集合論必須有基本的知識, 但是不見得要對集合論的公設系統, 最新發展或猜想感興趣.

數學的命題與證明基於前兩節的架構, 許多數學命題必須至少用一階邏輯來表述, 但一階邏輯的量詞預設某個「範圍」, 在數學中因此需要「集合」的概念. 20 世紀之前 Cantor 發展的「素樸」集合論, 在形式化後碰到很大的困難[5], 於是由數學家開始重建整個集合論. 目前數學家所採用的集合論稱為 ZFC 集合論, 這是基於 Zermelo 和 Fraenkel 在 20 世紀初發展出來的 ZF 集合論, 再加上 C 所代表「選擇公設」(axiom of choice) . 但是就初學者來說, 並不需要那麼形式化的集合論, 原來的素樸集合論已經很夠用.

回顧高中學過的集合, 集合就是一個組合, 其中有一些元素. 符號上記為

$$A=\{a_1,a_2,\cdots,a_N\},\ a_i\in A \quad (a_i \text{ 屬於 } A)$$

其中重複的元素只能算成一個元素. 萬一集合空無一物, 則這個集合稱為空集合 (empty set) , 記成 $\emptyset$. 我們熟知下列的集合: 自然數 ($\mathbb{N}$) , 整數 ($\mathbb{Z}$) , 有理數 ($\mathbb{Q}$) , 實數 ($\mathbb{R}$) , 複數 ($\mathbb{C}$). 為了方便起見, 我們約定用 $\overline{n}$ 表示 $\{1,2,\cdots,n\}$.

設 A, B 為兩集合, 如果 $\forall a\ (a\in B \Rightarrow a\in A)$, 則稱 B 為 A 的子集合 (subset), B 包含於 A, 或 A 包含 B, 記為 $B\subseteq A$. 當 $B\subseteq A$ 且 $B\neq A$ 時, 稱 B 是 A

[5]如羅素悖論, 通常所有困難都來自「無限」與自我指涉.

的真子集 (proper subset), 記為 $B \subset A$. (記號類似 $\leqslant$ 和 $<$ 的差別) . 另外依照 $\Rightarrow$ 的真假值約定, $\emptyset \subseteq A$, 對任何集合 A 都正確.

條列集合表示太侷限, 更常使用的是集合的性質表示法: $A = \{a \mid P(a)\}$, 表示滿足性質 $P(x)$ 的所有元素, 於是可以和述詞演算的語言結合起來. 通常這樣定義集合時, 需要一個已知的集合當作背景.

1. 在自然數中, $\{n \mid \forall m\ (m \,|\, n \Rightarrow (m = 1 \vee m = n))\} \subset \mathbb{N}$. 表示質數所成的子集合.

2. 在實數中, $\left\{a \mid a^2 = 2\right\} \subset \mathbb{R}$. $x^2 - 2 = 0$ 的解集合是實數的子集合.

3. $\left\{x \mid x^2 + 1 = 0\right\}$. 若在 $\mathbb{R}$ 中討論, 這個集合是 $\emptyset$. 但在 $\mathbb{C}$ 中, 這個集合是 $\{i, -i\}$.

4. $\{a \mid a \in A\} \subseteq A$. 這是以「是否屬於 A」作為條件所定義的集合, 當然就是 A 本身.

上面用到集合相等的符號, 兩集合 A 和 B 相等 $(A = B)$ 的合理定義為

$$\forall x\ \ (x \in A \ \Leftrightarrow\ x \in B)$$

由前節知這相當於

$$\forall x\ \ (x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)$$

再檢視定義可知

$$A = B \quad \Leftrightarrow \quad (A \subseteq B) \wedge (B \subseteq A)$$

在數學中經常要檢視兩個用不同方式得到的集合是否相等, 這是基本的檢查法.

習題 5.1. 檢視下列兩集合相等

1. $A = \{a \mid a \in A\}$.

2. 在實數中定義 B 為 $\left\{a \mid \exists b\ \ a = b^3\right\}$, 說明 $\mathbb{R} = B$

3. $\{a \mid a = 2m + 3n, m, n \in \mathbb{Z}\} = \{b \mid b = -m + 4n, m, n \in \mathbb{Z}\}$

假設一背景集合 U (稱為宇集，表示討論脈絡下所有元素所成的集合) , 若 $A, B \subseteq U$. 定義幾種集合運算如下:

1. 餘集 (complement set) : $A^c = \{a \mid \neg (a \in A)\}$. $\neg (a \in A)$ 可記為 $a \notin A$.

2. 交集 (intersection set) : $A \cap B = \{a \mid a \in A \wedge a \in B\}$.

3. 聯集 (union set) : $A \cup B = \{a \mid a \in A \vee a \in B\}$.

習題 5.2. $A, B, C \subseteq U$, 用前節結果證明下列性質.

1. (De Morgan's law)

   $(A \cup B)^c = A^c \cap B^c$

   $(A \cap B)^c = A^c \cup B^c$

2. $A \cup A^c = U$; $A \cap A^c = \emptyset$; $A = (A^c)^c$.

3. (交換律) $A \cap B = B \cap A$; $A \cup B = B \cup A$.

4. (結合律) $A \cap (B \cap C) = (A \cap B) \cap C$; $A \cup (B \cup C) = (A \cup B) \cup C$.

5. (分配律)

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

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

習題 5.3. 定義 A 和 B 的差集 $A \setminus B$ 為 $\{a \mid a \in A \wedge a \notin B\}$. 證明下列敍述.

1. $A \setminus B = A \cap B^c$.

2. (De Morgan's law)

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

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

習題 5.4. 前節的連結詞 $\neg P$, $P \wedge Q$, $P \vee Q$ 在集合論中有相對應的 A^c, $A \cap B$, $A \cup B$. 我們似乎可定義與 $P \Rightarrow Q$ 對應的概念. 但 $\Rightarrow$ 已經用於 $\subseteq$ 的定義中, 這兩種概念中間的差異是什麼？

習題 5.5. 證明 $A \cap B = \emptyset \Leftrightarrow A \subseteq B^c$

定義 5.1. (冪集合, power set) 給定一集合 A, 定義 A 的冪集合 2^A 為

$$2^A = \{B \mid B \subseteq A\}$$

也就是由 A 的所有子集合所成的集合.

$\boxed{\text{習題}}$ **5.6.** 若 A 有 N 個元素 (譬如 $\overline{N}$) , 說明 2^A 有 2^N 個元素.

定義 5.2. (笛卡兒乘積, Cartesian product) 給定兩集合 A, B, 可定義 A 和 B 的笛卡兒乘積 $A \times B$ 為

$$A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$$

我們見過的例子是平面 $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, 空間 $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.

注意. 其實 $\mathbb{R}^3$ 的這個定義, 目前有點不清楚, 你能看出來嗎？

5.1 關係與函數

給定兩集合 A, B, $R \subseteq A \times B$ 定義了 A 和 B 間的關係 (relation) .

示例. F 是女人的集合, P 是人的集合, 考慮集合 $\{(a,b) \mid B(a,b)\} \subseteq F \times P$, 其中性質 $B(a,b)$ 表示 a 生 b. 此子集合定義一關係, 可稱為母子關係. $\square$

示例. P 是人的集合, 考慮集合 $\{(a,b) \mid L(a,b)\} \subseteq P \times P$, 其中性質 $L(a,b)$ 表示 a 喜歡 b, 此子集合定義一關係, 或可稱為喜愛關係. $\square$

示例. 考慮集合 $\big\{(x,y) \mid x^2 - y^2 = 0\big\} \subseteq \mathbb{R} \times \mathbb{R}$, 此子集合定義了 $\mathbb{R}^2$ 中 x 和 y 之間的一個關係. $\square$

由這些例子可以看出抽象的「關係」非常寬鬆. 底下介紹兩個在數學中很重要的關係.

5.1.1 等價關係

若 $D \subseteq A \times A$, 用 $a \sim b$ 表示 $(a,b) \in D$.

定義 5.3. 若對所有 a, b, $c \in A$, $\sim$ 滿足下列三條件, 稱關係 $\sim$ 為等價關係 (equivalence relation) , 這是數學中所謂分類的基礎.

1. (反身性, Reflexivity) $a \sim a$
2. (對稱性, Symmetry) $a \sim b \ \Rightarrow b \sim a$
3. (遞移性, Transitivity) $(a \sim b \wedge b \sim c) \Rightarrow a \sim c$

注意. 如果把 $a \sim b$ 想成同類, 依日常理解, 「同類」的確滿足這三個條件.

$\boxed{\text{習題}}$ **5.7.** 人與人之間的喜愛關係顯然不是等價關係, 它違反了哪些條件？

示例. 我們來看看一些數學中的範例.

1. $a \sim b$ 表示 $a = b$. 「相等」顯然是等價關係.

2. 在 $\mathbb{R}$ 中, $a \sim b$ 表示 $a > b$. 這顯然不是等價關係 (違反了 1., 2.) .

3. 在 $\mathbb{R}$ 中, $a \sim b$ 定義成 $\exists \lambda > 0, a = \lambda b$. 這是等價關係, 略證如下:

   (a) $a = 1 \cdot a$;

   (b) 若 $a = \lambda b$, 則 $b = \frac{1}{\lambda} a$;

   (c) $a = \lambda b$, $b = \mu c$ 則 $a = (\lambda\mu)c$.

   這個等價關係對應的分類是正數, 負數和零.

4. 在 $\mathbb{Z}$ 中, $m \sim n$ 定義成 $2 \,|\, m - n$. 這是等價關係:

   (a) $2 \,|\, m - m$;

   (b) 若 $2 \,|\, m - n$, 則 $2 \,|\, n - m$;

   (c) 若 $2 \,|\, m - n$ 且 $2 \,|\, n - k$, 則 $2 \,|\, (m - n) + (n - k)$, 即 $2 \,|\, m - k$.

   這個等價關係對應的分類是奇數和偶數.

5. 在平面直線中, $L \sim M$ 表示 L 平行於 M. 若容許一直線和本身平行, 則這是等價關係. 其分類要素是「斜率」.

6. 在平面圖形中, $\Gamma \sim \Sigma$ 表示 Γ 和 Σ 全等. 這顯然是等價關係. 它的分類是什麼呢？

$\square$

$\boxed{\textbf{習題}}$ **5.8.** 底下這些關係是不是等價關係. 若不是, 它違反那個條件. 若是, 請討論它對應的分類.

1. $a \sim b$ 表示 $a \neq b$.

2. $a \sim b$ 表示 $a \leqslant b$.

3. 在自然數中, $m \sim n$ 定義成 m 和 n 有共同大於 1 的因數.

4. 在平面直線中, $a \sim b$ 表示 a 垂直於 b.

5. 在平面圖形中, $a \sim b$ 表示 a 和 b 相似.

6. 在人所成的集合中, $a \sim b$ 表示 a 和 b 同一天生.
7. 在人所成的集合中, $a \sim b$ 表示 a 和 b 有共同的生物母親.

對於 $a \in A$, 定義 a 的等價類 (equivalence class) A_a 為:

$$A_a = \{b \mid a \sim b\}$$

也就是與 a「同類」的元素所成的集合.

性質 5.1. 下面是關於等價類的基本性質:

1. 若 $b, c \in A_a$, 則 $b \sim c$.
2. $a \sim b \Leftrightarrow A_a = A_b$.
3. 若 $A_a \cap A_b \neq \emptyset$, 則 $A_a = A_b$.
4. $a \not\sim b \Leftrightarrow A_a \cap A_b = \emptyset$

證明.

1. $b, c \in A_a$, 則 $a \sim b$ 且 $a \sim c$. 由對稱性 $b \sim a$, 再由遞移性 $b \sim c$.
2. ($\Rightarrow$) 因為 $a \sim b$, 對任意 $x \in A_a$, 則 $a \sim x$, 同上 $b \sim x$, 則 $x \in A_b$. 這證明 $A_a \subseteq A_b$. 同理因為 $b \sim a$ (對稱性) 得 $A_b \subseteq A_a$, 故 $A_a = A_b$

   ($\Leftarrow$) $b \in A_b = A_a$, 則 $a \sim b$.
3. 由假設, 令 $c \in A_a \cap A_b$. 因為 $c \in A_a$, 所以 $a \sim c$, 同理 $b \sim c$, 因此 $a \sim b$, 由 2. 得 $A_a = A_b$.
4. ($\Rightarrow$) 本命題相當於 $A_a \cap A_b \neq \emptyset \Rightarrow a \sim b$. 由 3. 若 $A_a \cap A_b \neq \emptyset$, 則 $A_a \sim A_b$, 再由 2. 即得 $a \sim b$.

   ($\Leftarrow$) 本命題相當於 $a \sim b \Rightarrow A_a \cap A_b \neq \emptyset$. 由 2. 若 $a \sim b$ 則 $A_a = A_b$, 當然 $A_a \cap A_b \neq \emptyset$.

$\square$

由此可以得到下面的性質.

性質 5.2. $A = \coprod_i A_{a_i}$, 其中 $a_i \in A$, 且當 $i \neq j$ 時, $a_i \not\sim a_j$.

注意. 符號 $\coprod$ 表示互不相交的聯集.

這個性質表示, A 可以依等價關係 $\sim$ 被完整分類, 每類彼此無重複, 每個元素隸屬某個類別.

5.1.2 函數

函數是大家熟悉的概念, 但這裡著重的是最基本的函數意義, 有人可能不習慣把它視為一種特殊的關係, 也許更無法接受不用代數算式來定義函數.

函數 f 是一種關係 $\Gamma_f \subseteq A \times B$, 在這種情況, Γ_f 常被稱為函數的「圖形」(graph) . [6]

[6]更抽象一點, 可以說 $f \in 2^{A \times B}$

函數 f 或 Γ_f 有兩個基本條件: (順便練習多量詞命題)

1. $\forall a \in A \ \exists b \in B \ \ (a,b) \in \Gamma_f$.
2. $\forall a \in A \ \forall b_1, b_2 \in B \ \ ((a,b_1) \in \Gamma_f \wedge (a,b_2) \in \Gamma_f \Rightarrow b_1 = b_2)$

這兩者結合在一起, 意思就是 A 中<u>每一</u>元素 a, 都有<u>唯一</u>元素 $b \in B$, 使得 $(a,b) \in \Gamma_f$. 因此通常把 b 記為 $f(a)$, 稱為 a 所對應的的函數值, 並把函數關係, 重新寫為 $f : A \to B$. A 稱為 f 的定義域 (domain) , B 稱為 f 的對應域 (codomain 或 range) , $f(A) = \{f(a) \mid a \in A\}$ 稱為像集 (image) .

注意. 函數有可能多對一, 而且 B 中不見得每一點都會被對應到.

若 $f : A \to B$, $g : B \to C$, 定義合成函數 (composite function) $g \circ f : A \to C$ 如下[7]:

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

底下討論有特別性質的函數:

定義 5.4. 函數 $f : A \to B$

1. (單射, injection, 也稱為嵌射或 1 對 1) 記為 $f : A \rightarrowtail B$,

$$\forall a_1, a_2 \in A \ \ (f(a_1) = f(a_2) \ \Rightarrow \ a_1 = a_2)$$

2. (滿射, surjection, 也稱為蓋射或映成) 記為 $f : A \twoheadrightarrow B$,

$$\forall b \in B \, \exists a \in A \ \ f(a) = b$$

   即 $f(A) = B$ 的意思.

3. (對射, bijection) 若 f 同時為嵌射與滿射, 則稱為對射. 記為 $f : A \leftrightarrow B$.

$\boxed{\textbf{習題}}$ **5.9.** 證明下列敘述

1. 若 $f : A \rightarrowtail B$, $g : B \rightarrowtail C$, 則 $g \circ f : A \rightarrowtail C$
2. 若 $f : A \twoheadrightarrow B$, $g : B \twoheadrightarrow C$, 則 $g \circ f : A \twoheadrightarrow C$
3. 若 $f : A \leftrightarrow B$, $g : B \leftrightarrow C$, 則 $g \circ f : A \leftrightarrow C$

[7]「$\circ$」念作 of. 「$(g \circ f)(a)$」念作 g of f of a.

如果將 f 對映的方向倒轉, 便是「反函數」$f^{-1}: B \to A$ 的概念. 這相當於考慮 $\Gamma_{f^{-1}} \subseteq B \times A$, 其中

$$(b,a) \in \Gamma_{f^{-1}} \subseteq B \times A \;\Leftrightarrow\; (a,b) \in \Gamma_f \subseteq A \times B$$

問題是倒過來的關係不見得真是一個函數, 必須檢查是否符合基本條件:

1. B 中每一元素皆有對應:

   $$\forall b \in B \,\exists a \in A \;\; (b,a) \in \Gamma_{f^{-1}} \;\Leftrightarrow\; \forall b \in B \,\exists a \in A \;\; (a,b) \in \Gamma_f$$

   這相當於 f 是滿射的條件.

2. 不容許有一對多的情況:

   $$\begin{aligned} & \forall b \in B \,\forall a_1, a_2 \in A \;\; ((b,a_1) \in \Gamma_{f^{-1}} \wedge (b,a_2) \in \Gamma_{f^{-1}} \Rightarrow a_1 = a_2) \\ \Leftrightarrow \;\; & \forall b \in B \,\forall a_1, a_2 \in A \;\; ((a_1,b) \in \Gamma_f \wedge (a_2,b) \in \Gamma_f \Rightarrow a_1 = a_2) \end{aligned}$$

   這正是單射的條件.

這表示如果 $f: A \to B$ 同是單射與滿射 (也就是對射) , 那麼 $\Gamma_{f^{-1}} \subseteq B \times A$ 將定義一個函數 $f^{-1}: B \to A$. 此函數 f^{-1} 稱為 f 的反函數, 滿足

$$f^{-1}(f(a)) = a, \quad f(f^{-1}(b)) = b.$$

如果用合成函數的符號可以記成

$$f^{-1} \circ f = \mathbf{1}_A, \quad f \circ f^{-1} = \mathbf{1}_B$$

其中函數 $\mathbf{1}_A : A \to A$ 定義為 $\mathbf{1}_A(a) = a$, 同理 $\mathbf{1}_B : B \to B$ 定義為 $\mathbf{1}_B(b) = b$.

$\boxed{\textbf{習題}}$ **5.10.** 若 $f: A \rightarrowtail B$, 考慮

$$g: A \to f(A), \quad g(a) = f(a)$$

則 g 有反函數.

$\boxed{\textbf{習題}}$ **5.11.** 假設 $f: A \to B$, $g: B \to A$. 證明下面敘述

1. 若 $g \circ f = \mathbf{1}_A$ (亦即 $\forall a \in A \;\; g(f(a)) = a$) , 證明 f 必為單射.

2. 若 $f \circ g = \mathbf{1}_B$ (亦即 $\forall b \in B \;\; f(g(b)) = b$) , 證明 f 必為滿射.

3. 由此證明若 g 滿足

$$g \circ f = \mathbf{1}_A, \quad f \circ g = \mathbf{1}_B$$

則 f 必為對射, 且 g 為 f 的反函數.

習題 5.12. 假設 $f : A \to B$ 和 $g : B \to C$ 分別有反函數 $f^{-1} : B \to A$ 和 $g^{-1} : C \to B$. 證明 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

若 $f : A \to B$, 且 $C \subseteq B$. 記號 f^{-1} 也常用來定義下列集合:

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\} \subseteq A.$$

習題 5.13. 假設 $f : A \to B$, 且 $C \subseteq A$, $D \subseteq B$. 下列敍述是否正確？

1. $f^{-1}(B) = A$.
2. $f(f^{-1}(C)) = C$.
3. $f^{-1}(f(D)) = D$.

習題 5.14. 假設 $f : A \to B$, 且 $C, D \subseteq B$, 證明下列各敍述:

1. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.
2. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
3. $f^{-1}(D \setminus C) = f^{-1}(D) \setminus f^{-1}(C)$.

習題 5.15. 在上個習題中, 若把問題換成 f, 結果會如何？

5.2 無限集合有多大

人類對於無限很好奇, 但通常僅止於想像, 反映出這個概念並非現實世界的實體. 直到數學家 Cantor 在 19 世紀開始探討「無限」, 才開始以理性的方式探討這個迷人的課題. 更因為無限的概念看似推廣有限的生活經驗, 造成許多違反直覺的爭議, 在 20 世紀初期爆發數學哲學的論戰. 現在數學家已經理解, 推廣日常經驗到牽涉無限的概念都必須小心, 必須思考清楚自己推理的論據.

5.2.1 有限集合

定義 5.5. (有限, finite) 若存在對射 $f : A \leftrightarrow \overline{n}$, $n \in \mathbb{N}$, 則稱集合 A 是有限的.

這個定義源自熟悉的點數經驗, 因此如果以 $|A|$ 表示集合的基數 (cardinality, cardinal number, 集合的大小, 集合元素的多寡) , 當 $f : A \leftrightarrow \overline{n}$ 時, 則 $|A| = n$. 但嚴格來講, 我們並沒有真正證明基數的概念是良好定義的 (well defined) . 也就是說, 尚未證明「若 $n \neq m$, 則 $\overline{n}$ 和 $\overline{m}$ 之間不存在對射」. (你可能覺得很荒唐！)

後續將假設下面基於經驗, 「顯然正確」的事實:

性質 5.3. 假設 $f : A \leftrightarrow \overline{n}$, 如果 $\varnothing \neq B \subset A$, 則

1. 不可能有 $B \leftrightarrow \overline{n}$.
2. 可找到 $0 < m < n$, 使得 $B \leftrightarrow \overline{m}$.

從這個性質可以很容易推出底下性質:

性質 5.4.

1. A 有限, 且 $B \subset A$, 則不存在 $B \leftrightarrow A$.
2. A 有限, 且 $B \subseteq A$, 則 B 有限且 $|B| \leqslant |A|$, 尤其若 $B \subset A$, 則 $|B| < |A|$.

習題 5.16. 證明這個性質.

習題 5.17. (基數概念是良好定義的) 若 $A \leftrightarrow \overline{n}$ 且 $A \leftrightarrow \overline{m} \Rightarrow n = m$.

在數學中, 等價的命題 (這些命題經常有不同的用途) 常用底下的方式來敍述與證明, 這時安排一個比較簡單的證明順序是很有意思的.

性質 5.5. 底下三個敍述是等價的:

1. A 有限.
2. $\exists n > 0$, 可找到 $f : \overline{n} \twoheadrightarrow A$.
3. $\exists n > 0$, 可找到 $g : A \rightarrowtail \overline{n}$.

證明.

(1. $\Rightarrow$ 2.) 對射是一種滿射, 顯然正確.
(2. $\Rightarrow$ 3.) $\forall a \in A$, 令 $g(a) = f^{-1}(\{a\})$ 的最小元素. $g : A \to \overline{n}$ 顯然是單射.

(3. $\Rightarrow$ 1.) $g(A) \subseteq \overline{n}$, 所以 $g(A)$ 有限, 亦即存在 $m \leqslant n$, 使得 $g(A) \leftrightarrow \overline{m}$. 又

$$((A \leftrightarrow g(A)) \wedge (g(A) \leftrightarrow \overline{m})) \Rightarrow (A \leftrightarrow \overline{m})$$

即 1.

$\square$

性質 5.6. 若 A 和 B 是有限集合, 則 $A \cup B$ 是有限集合.

證明.
用 $A \leftrightarrow \overline{n}$, $B \leftrightarrow \overline{m}$, 可造出 $\overline{m+n} \twoheadrightarrow A \cup B$. (how?)

$\square$

$\boxed{\text{習題}}$ **5.18.** 若 $A_1, A_2, \cdots, A_n$ 都是有限集合, 則 $A_1 \cup A_2 \cup \cdots \cup A_n$ 有限.

性質 5.7. 若 A 和 B 是有限集合, 則 $A \times B$ 是有限集合.

證明.
$f : A \leftrightarrow \overline{n}$, 則

$$A \times B = \bigcup_{i=1}^{|A|} B_i, \quad B_i = \{(f(i), b) \mid b \in B\}$$

$\square$

由證明可知 $|A \times B| = |A| \times |B|$.

$\boxed{\text{習題}}$ **5.19.** 若 $A_1, A_2, \cdots, A_n$ 都是有限集合, 則 $A_1 \times A_2 \times \cdots \times A_n$ 有限.

5.2.2 可數的無限

若一集合不是有限集合, 則稱為無限 (infinite, 無窮) 集合. 由**性質 5.4** 知, 一個有限集合, 不會跟它的真子集有對射關係, 這給出檢測一集合是否無限的方法: 若一集合與其真子集有對射關係, 則該集合為無限集合.

性質 5.8. $\mathbb{N}$ 是無限集合.

證明.
定義對射 $f : \mathbb{N} \to \mathbb{N} \setminus \{1\}$: $f(n) = n + 1$, 得證.

$\square$

習題 **5.20.** 若 $B \subseteq A$ 且 $B \leftrightarrow \mathbb{N}$, 則 A 為無限集合.

習題 **5.21.** 若 A 無限, 而 $B \subset A$ 是有限集合, 則 $A \setminus B \neq \emptyset$

後面將說明 $\mathbb{N}$ 是「最小」的無限集合, 扮演類似 $\overline{n}$ 典型集合的角色. Cantor 的貢獻就在於用對射來刻畫集合的大小, 並發現無限的不同等級.[8]

定義 5.6. 若 $A \leftrightarrow \mathbb{N}$, 則稱 A 為可數無限集合 (countable infinity) , 可數無限集合的基數記為 ω. 一無限集合若非可數, 則稱為不可數無限 (uncountable infinity) . 另有限集合和可數無限集合稱為可數集合 (countable) .

習題 **5.22.** 若 A, B 為兩集合，定義 $A \sim B$ 為存在 $A \leftrightarrow B$。證明這是一個集合之間的等價關係。

注意. 這個等價關係定義了一般集合的基數，亦即 $A \leftrightarrow B \Leftrightarrow |A| = |B|$.

示例. 所有正偶數所成的集合是可數無限. $\mathbb{Z}$ 是可數無限. $\mathbb{N} \times \mathbb{N}$ 是可數無限.

每種特殊情況都要找特殊方法來證明存在對射顯然太麻煩. 底下證明一些好用的性質. 和**性質 5.5** 類似, 我們也有刻畫可數集合的方法.

性質 5.9. 底下三個敍述是等價的,

1. A 可數.
2. 可找到 $f : \mathbb{N} \twoheadrightarrow A$
3. 可找到 $g : A \rightarrowtail \mathbb{N}$

證明和**性質 5.5** 很類似, 但是在 3. ⇒ 1. 時, 需要證明下面的性質:

性質 5.10. 若 $A \subset \mathbb{N}$ 且 A 無限, 則 A 是可數無限.

證明.

我們想要造出函數 $f : \mathbb{N} \leftrightarrow A$, 造法是用歸納法遞迴的造出來.

$i = 1$: $f(1) = \min(A)$.

$i = 2$: $f(2) = \min(A \setminus \{f(1)\})$. 因為由**習題 5.21** , $A \setminus \{f(1)\} \neq \emptyset$.

$\cdots\cdots$ 依此類推.

$i = k$: 假設 $f(1), f(2), \cdots, f(k)$ 皆已定義.

[8] 提醒讀者, 在有限集合時點數和對射是同一個概念, 也就是從 1 數到 n 與和 $\overline{n}$ 存在對射是同一件事, 但是在無限時, 這兩種想法就分道揚鑣了: 分別稱為序數 (ordinal number) 和基數.

$i = k+1$: $f(k+1) = \min(A \setminus \{f(1), f(2), \cdots, f(k)\})$.

注意到 f 是一個遞增函數 (習題) , 也就是 $m > n \Rightarrow f(m) > f(n)$. 因此 $f : \mathbb{N} \rightarrowtail A$, 於是只需要證明 $f : \mathbb{N} \twoheadrightarrow A$.

任取 $a \in A \subset \mathbb{N}$, 令 $D = A \cap \overline{a}$ 則 D 為一有限集合, 令 $d = |D|$. 由於 D 的元素是 A 最小的 d 個元素. 由 f 的構造方式知 $f(d) = a$, 證完.

□

習題 5.23. 證明上述 f 是遞增函數.

示例. $\mathbb{N} \times \mathbb{N}$ 和 $\mathbb{Z}$ 是可數無限 (重訪) . 正有理數 $\mathbb{Q}^+$ 也是可數無限.

$\mathbb{N} \times \mathbb{N}$: 利用 $(m,n) \mapsto 2^m \cdot 3^n$ 可得到 $\mathbb{N} \times \mathbb{N} \rightarrowtail \mathbb{N}$.

$\mathbb{Z}$: 利用 $(m,n) \mapsto m-n$ 可得到 $\mathbb{N} \leftrightarrow \mathbb{N} \times \mathbb{N} \twoheadrightarrow \mathbb{Z}$.

$\mathbb{Q}^+$: 利用 $(m,n) \mapsto \frac{m}{n}$ 可得到 $\mathbb{N} \leftrightarrow \mathbb{N} \times \mathbb{N} \twoheadrightarrow \mathbb{Q}^+$.

□

性質 5.11. 若 $A_1, A_2, \cdots, A_n$ 都是可數集合, 則 $A_1 \times A_2 \times \cdots \times A_n$ 可數.

證明.

利用映射 $(m_1, m_2, \cdots, m_k) \mapsto 2^{m_1} \cdot 3^{m_2} \cdots p_k^{m_k}$ 可得到 $\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N} \rightarrowtail \mathbb{N}$. 由此知 $\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}$ 為可數無限. 其中 p_k 為第 k 個質數.

現令 $f_i : \mathbb{N} \twoheadrightarrow A_i$. 利用 $(m_1, m_2, \cdots, m_k) \mapsto (f_1(m_1), f_2(m_2), \cdots, f_k(m_k))$ 可得到 $\mathbb{N} \leftrightarrow \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N} \twoheadrightarrow A_1 \times A_2 \times \cdots \times A_n$.

□

習題 5.24. 可以用類似方法證明 $\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N} \times \cdots$ 可數嗎 ?

性質 5.12. 若 $A_1, A_2, \cdots, A_n \cdots$ 都是可數集合, 則 $A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots$ 也是可數集合.

證明.

令 $f_i : \mathbb{N} \twoheadrightarrow A_i$, 利用 $(i,j) \mapsto f_i(j)$ 可證得

$$\mathbb{N} \leftrightarrow \mathbb{N} \times \mathbb{N} \twoheadrightarrow A_1 \cup A_2 \cup \cdots \cup A_n \cdots$$

□

習題 **5.25.** $\mathbb{Q}$ 是可數無限.

習題 **5.26.** I 可數. 若 $A_\alpha, \alpha \in I$ 皆可數, 則 $\bigcup_{\alpha\in I} A_\alpha$ 也是可數集合.

定義 5.7. (代數數, algebraic number) 令 $m_0, m_1, m_2, \cdots, m_n \in \mathbb{Z}$, $m_n \neq 0$, 則整係數多項式

$$m_n x^n + m_{n-1}x^{n-1} + \cdots + m_1 x + m_0 = 0$$

的根稱為**代數數**.

定義 5.8. (超越數, transcendental number) 非代數數的數稱為**超越數**.

$n = 1$ 時的代數數就是有理數 $\mathbb{Q}$, 這是一個可數無限集合. 高中生所學過的無理數大部分是代數數, 如平方根數、立方根數（why?）, 但 π 是超越數（見後續課程）.

示例. 代數數所成的集合是可數無限.

1. 將多項式 $m_n x^n + m_{n-1}x^{n-1} + \cdots + m_1 x + m_0 = 0$ 的根所成的集合記為 $A_{(m_n,\cdots,m_1,m_0)}$, 其中 $m_0, m_1, \cdots, m_n \in \mathbb{Z}$, $m_n \neq 0$, 這當然是可數集合. 注意 $A_{(m_n,\cdots,m_1,m_0)}$ 的足碼 $(m_n, \cdots, m_1, m_0) \in (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z} \times \cdots \times \mathbb{Z}$. 令 $I = (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, 則 I 可數.

2. 令 A_n 為 1. 中之代數數所成的集合. 因為

$$A_n = \bigcup_{(m_n,\cdots,m_1,m_0)\in I} A_{(m_n,\cdots,m_1,m_0)}$$

由**習題 5.26** 知 A_n 為可數集合.

3. 令 A 為代數數所成的集合. 因為 $A = \bigcup_{n\in\mathbb{N}} A_n$, 故 A 是可數無限.

□

習題 **5.27.** 定義 $\mathbb{N}_0^{\mathbb{N}} = \{(m_1, \cdots, m_n, 0, 0, \cdots) \mid m_i \in \mathbb{N}\}$. 證明 $\mathbb{N}_0^{\mathbb{N}}$ 可數.
(提示: 證明 $\mathbb{N}_0^{\mathbb{N}} = \bigcup_{n\in\mathbb{N}} \{(m_1, \cdots, m_n, 0, 0, \cdots) \mid m_i \in \mathbb{N}\}$.)

注意. $\mathbb{N}_0^{\mathbb{N}} \subset \mathbb{N}^{\mathbb{N}} = \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N} \times \cdots$.

5.2.3 不可數的無限

令 $\{0,1\}^A = \{f \mid f : A \to \{0,1\}\}$. 則對任一集合 A, $\{0,1\}^A$ 和冪集合 2^A 之間有自然的對射:

$$(f : A \to \{0,1\}) \ \mapsto \ \{a \mid f(a) = 1\} \subseteq A$$

習題 5.28. 證明這個對映是對射.

性質 5.13. $\{0,1\}^{\mathbb{N}}$ 是不可數無限.

證明.

運用歸謬法, 假設 $\{0,1\}^{\mathbb{N}}$ 是可數無限, 因此 $\{0,1\}^{\mathbb{N}}$ 的元素可列成 $f_1, f_2, \cdots, f_n \cdots$. 將 f_i 記為 $(f_{i1}, f_{i2}, f_{i3}, \cdots)$, 其中 $f_{ik} = f_i(k) = 0$ 或 1. 於是所有 f_i 可列成:

$$\begin{array}{c||cccccc}
f_1 & f_{11} & f_{12} & f_{13} & \cdots & f_{1k} & \cdots \\
f_2 & f_{21} & f_{22} & f_{23} & \cdots & f_{2k} & \cdots \\
f_3 & f_{31} & f_{32} & f_{33} & \cdots & f_{3k} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots \\
f_k & f_{k1} & f_{k2} & f_{k3} & \cdots & f_{kk} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots
\end{array}$$

現定義 $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_k \cdots)$, 其中 $\alpha_k = 1 - f_{kk}$, 亦即

$$\alpha_k = \begin{cases} 1, & f_{kk} = 0 \\ 0, & f_{kk} = 1 \end{cases}$$

α 定義了一個 $\mathbb{N} \to \{0,1\}$ 的函數 $\alpha(k) = \alpha_k$, 因此 $\exists j \ f_j = \alpha$, 但這是不可能的, 因為 $f_j(j) = f_{jj} = \alpha_j \neq f_{jj}$, 矛盾. 原來的假設 $\{0,1\}^{\mathbb{N}}$ 可數無限有誤, 故 $\{0,1\}^{\mathbb{N}}$ 為不可數無限.

□

這個證明方法稱為「對角論證」(Cantor's diagonal argument) , 是數理邏輯運用歸謬證法非常知名而有用的論證方式. 例如重要的 Gödel 不完備定理和 Turing 不可計算定理, 都是巧妙應用對角論證的結果.

習題 5.29. 用對角論證證明 $[0,1]$ 是不可數無限集合. (假設 $0.5 = 0.4999\cdots$ 只取第一種表示法)

值得注意的是, 如果用 $2^{\mathbb{N}}$ 的角度來思考, $f_i : \mathbb{N} \to \{0,1\}$ 表示一個 $A_i \subseteq \mathbb{N}$, 其中

$$j \in A_i \ \Leftrightarrow \ f_i(j) = 1 \quad \text{或是} \quad A_i = \{j \mid f_i(j) = 1\}.$$

因此 $\alpha:\mathbb{N}\to\{0,1\}$ 所對映的子集合 B 滿足

$$k\in B \;\Leftrightarrow\; \alpha(k)=\alpha_k=1 \;\Leftrightarrow\; f_{kk}=f_k(k)=0 \;\Leftrightarrow\; k\notin A_k$$

亦即

$$B=\{k\mid k\notin A_k\}$$

這個想法脫離了 $\mathbb{N}$ 的限制, 得以證明下列基本定理.

性質 5.14. 在 A 和 2^A 之間不存在對射. 這表示 $|A|\neq\left|2^A\right|$.

證明.

用歸謬證法, 假設有對射 $f:A\leftrightarrow 2^A$. 定義 $B\subseteq A$ 如下

$$B=\{a\mid a\notin f(a)\}$$

令 $\alpha=f^{-1}(B)$, 則 α 可能在 $B=f(\alpha)$ 中, 也可能不在 B 中, 但

$$\alpha\in f(\alpha)\;\Leftrightarrow\;\alpha\in B\;\Leftrightarrow\;\alpha\notin f(\alpha)$$

這當然不可能, 因此原假設不成立, 即 A 和 2^A 之間不存在對射.

□

這個基本性質告訴我們無限有很多層級, 例如 $|\mathbb{N}|=\omega$ 和 $\left|2^{\mathbb{N}}\right|$ 是不一樣的. 底下就來證明 $|\mathbb{R}|=\left|2^{\mathbb{N}}\right|$

性質 5.15. $|\mathbb{R}|=\left|2^{\mathbb{N}}\right|$.

證明.

將證明分成兩個步驟

1. $|\mathbb{R}|=|(0,1)|$: 由 $x\mapsto\frac{1}{2}+\frac{1}{\pi}\tan^{-1}x$ 得 $\mathbb{R}\leftrightarrow(0,1)$.
2. $\{0,1\}^{\mathbb{N}}\leftrightarrow(0,1)$: 主要用到純小數的二進位表示法. 定義由 $\{0,1\}^{\mathbb{N}}$ 到 $[0,1]$ 的函數如下:

$$(a_1,a_2,\cdots,a_n,\cdots)\;\mapsto\;\frac{a_1}{2}+\frac{a_2}{2^2}+\cdots+\frac{a_n}{2^n}+\cdots$$

右邊表示成二進位小數就是 $0.a_1a_2\cdots a_n\cdots$. 例如

$$0.0000000\cdots=0$$
$$0.11111111\cdots=1$$
$$0.0101010\cdots=\frac{1}{3}$$

問題是有一些數如 $\frac{1}{2}$ 有兩種表示法：$0.10000\cdots$ 和 $0.01111\cdots$. 必須把有問題的部分從兩邊移除才會得到對射

$$g:\{0,1\}^{\mathbb{N}}\setminus A \;\leftrightarrow\; [0,1]\setminus B$$

其中

$$\begin{aligned}A=&\{(0,0,0,0,0,\cdots),(1,1,1,1,1,\cdots), \qquad \text{(對到 0 和 1 的部分)}\\ &(\underline{0},1,1,1,1,\cdots),(\underline{1},0,0,0,0,\cdots),\\ &(\underline{0,0},1,1,1,\cdots),(\underline{0,1},0,0,0,\cdots),(\underline{1,0},1,1,1,\cdots),(\underline{1,1},0,0,0,\cdots),\cdots\}\\ B=&\left\{\frac{n}{2^k}\mid n,k\in\mathbb{N}, n<2^k\wedge n\text{ 是奇數}\right\}=\left\{\frac{1}{2},\frac{1}{4},\frac{3}{4},\frac{1}{8},\frac{3}{8},\frac{5}{8},\frac{7}{8},\cdots\right\}\end{aligned}$$

A 和 B 是兩個可數集合，因此存在 $h:A\;\leftrightarrow\;B$. 結合兩者可得

$$f:\{0,1\}^{\mathbb{N}}\;\leftrightarrow\;[0,1],\quad \text{其定義為 } f(\alpha)=\begin{cases}g(\alpha), & \alpha\in\{0,1\}^{\mathbb{N}}-A\\ h(\alpha), & \alpha\in A\end{cases}$$

承上, 再由**習題 5.28**, 即得

$$|\mathbb{R}|=|(0,1)|=\left|\{0,1\}^{\mathbb{N}}\right|=\left|2^{\mathbb{N}}\right|$$

□

習題 5.30. 說明 A 和 B 是可數無限集合。

底下我們想要比較基數的大小。假設一個事實:[9]

性質 5.16. (Bernstein) 如果有 $A\rightarrowtail B$ 且 $B\rightarrowtail A$ 則 $|A|=|B|$.

習題 5.31. 若 $C\subset B\subset A$ 且 $|A|=|C|$, 則 $|A|=|B|=|C|$.

由 Bernstein 性質, 可以定義一個比大小的方式: 若有 $A\rightarrowtail B$, 但沒有 $B\rightarrowtail A$ 則記成 $|A|\prec|B|$, 表示 A 的基數比 B 小. 由於 A 有一顯然的單射到 2^A: $a\in A\mapsto\{a\}\in 2^A$, 由**性質 5.14** 可得 $|A|\prec\left|2^A\right|$. 因此

$$|\mathbb{N}|\prec\left|2^{\mathbb{N}}\right|\prec\left|2^{2^{\mathbb{N}}}\right|\prec\cdots$$

有時也直接寫成

$$\omega\prec 2^{\omega}\prec 2^{2^{\omega}}\prec\cdots$$

[9] 可參考楊維哲《何謂實數》或 Munkres, James R. "Topology", 2nd ed.(2000)

$\boxed{\text{習題}}$ **5.32.** 討論所有無限集合的基數中最小的是不是 ω.（見**性質 5.17**）

實數的基數 $\left|2^{\mathbb{N}}\right|$ 通常記為 c，表示連續統（continuum）的意思. Cantor 曾提出知名的連續統假設 (continuum hypothesis) ，他認為：

$$\text{沒有任何集合的基數介於 } |\mathbb{N}| \text{ 和 } |\mathbb{R}| \text{ 之間.}$$

也就是說「若 $\mathbb{N} \subset A \subset \mathbb{R}$, 則 $|A| = \omega$ 或 $|A| = c$」. 連續統假設後來被 Cohen 證明獨立於 ZFC 集合論的公設, 也就是說無論是連續統假設或其否定, 都無法從從 ZFC 公設推導出來 (如果這些公設之間沒有矛盾) .

$\boxed{\text{習題}}$ **5.33.** 利用下列敍述證明 $\left|\mathbb{R}^2\right| = |\mathbb{R}|$.

1. $\left|\mathbb{R}^2\right| = |[0,1] \times [0,1]|$.

2. 找出對射 $[0,1] \leftrightarrow [0,1] \times [0,1]$. (Hint: 運用前述小數表示法)

3. 這個方法可以推廣到 $\mathbb{R}^3$ 以上嗎？

$\boxed{\text{習題}}$ **5.34.** 利用**性質 5.16** 證明超越數的基數 $= |\mathbb{R}|$

5.2.4 反省無限：選擇公設

「有限」的定義是清楚的, 而「無限」則是透過有限的否定來定義. 因此透過討論有限集合的性質, 可發現兩個證明集合 A 是無限集合的方法. 一是若有 $\mathbb{N} \rightarrowtail A$ 則 A 無限; 二是若 A 和某真子集有對射關係, 則 A 無限. 但是反之是否為真呢？

性質 5.17. 底下三敍述等價

1. A 無限.

2. 有 $\mathbb{N} \rightarrowtail A$.

3. 有 $B \subset A$ 且 $A \leftrightarrow B$.

證明.

由前知 2. $\Rightarrow$ 1., 3. $\Rightarrow$ 1. .

a. (2. $\Rightarrow$ 3.): 因為 $\mathbb{N}$ 和某真子集 (如偶數 $2\mathbb{N}$) 有對射關係. 現假設 $f : \mathbb{N} \rightarrowtail A$, 並令

$$B = (A \setminus f(\mathbb{N})) \cup f(2\mathbb{N}), \quad \text{顯然 } B \subset A$$

定義下列映射 $g : A \to B$

$$f(a) = \begin{cases} a & a \in A \setminus f(\mathbb{N}) \\ f(2n) & a = f(n) \in f(\mathbb{N}) \end{cases}$$

易證此為對射.

b. $(1. \Rightarrow 2.)$: 用前述遞迴定義函數的方式造出 $f : \mathbb{N} \rightarrowtail A$.

$i = 1$: 因為 $A \neq \emptyset$, 取 $a_1 \in A$, 令 $f(1) = a_1$.

$i = 2$: 因為 A 無限, $A \setminus \{a_1\} \neq \emptyset$ 取 $a_2 \in A \setminus \{a_1\}$, 令 $f(2) = a_2$.

$\cdots$ 依此類推.

$i = k$: 假設 $f(1), f(2), \cdots, f(k)$ 皆已定義.

$i = k+1$: 因為 A 無限, $A \setminus \{a_1, a_2, \cdots, a_k\} \neq \emptyset$ 取 $a_{k+1} \in A \setminus \{a_1, a_2, \cdots, a_k\}$, 令 $f(k+1) = a_{k+1}$.

此函數顯然是單射, 證完.

□

許多人定義無限時, 喜歡用出人意料的 3. 做定義, 但真要證明存在這樣的對射時, 則經常用到 2., 也就是這裡提到的證明.

令人意外的是, $(1. \Rightarrow 2.)$ 的證明是「錯」的. 這個證明和**性質 5.10**明明一樣, 到底有什麼錯？兩者的差別在於**性質 5.10**中, $f(1), f(2), \cdots$ 的選法非常明確, 但是在現在的證明裡並沒有清楚有效的選擇方式, 這樣的證明有效嗎？

在日常生活的「有限」環境中, 這樣做沒有問題, 但是對於各式各樣可能的 $A \setminus \{a_1, a_2, \cdots, a_k\}$, 我們到底如何選, 其實毫無頭緒. 我們覺得安心只是把平常有限的策略搬到無限罷了. 數學家在集合論早期已經因為無限, 遇過嚴重的悖論, 因此在 ZF 集合論中對「如何構成集合」給了嚴格的限定. 而現在碰到的情況卻不在 ZF 集合論容許的公設裡, 於是數學家加入一條新公設, 稱為選擇公設 (axiom of choice, 也就是 ZFC 的 C) .

選擇公設: 對於一組集合 $\{A_\alpha\}_{\alpha \in I}$, 其中 $A_\alpha \neq \emptyset$, I 是足碼所成的集合 (可能是不可數無限) . 存在一個選擇集合 C 使得 $C \cap A_\alpha = \{a_\alpha\}$.

注意. 接受選擇公設, 相當於接受一條新的建立集合的規則. 有時 C 被寫為選擇函數 $c : I \to \coprod_{\alpha \in I} A_\alpha$, 滿足 $c(\alpha) = a_\alpha \in A_\alpha$.

在上述證明裡, 我們需先定義選擇函數 $c : 2^A \setminus \{\emptyset\} \to A$, 使得所有 $\emptyset \neq B \subseteq A$, 滿足 $c(B) \in B$. 然後重寫建構函數的步驟如下:

$i=1$: 因為 $A \neq \emptyset$, 令 $f(1)=c(A)$.

$i=2$: 因為 A 無限, $A \setminus \{f(1)\} \neq \emptyset$, 令 $f(2)=c(A \setminus \{f(1)\})$.

$\cdots$ 依此類推.

$i=k$: 假設 $f(1), f(2), \cdots, f(k)$ 皆已定義.

$i=k+1$: 因為 A 無限, $A \setminus \{a_1, a_2, \cdots, a_k\} \neq \emptyset$, 令 $f(k+1) = c(A \setminus \{a_1, a_2, \cdots, a_k\})$.

$\square$

對於選擇公設的取捨, 幾乎重演當初歐氏幾何「平行公設」的爭議. 有人希望證明 ZF 公設能夠推導出選擇公設. 有人希望把選擇公設的否定加入 ZF 公設, 然後導出矛盾. 但最後 Gödel 和 Cohen 分別證明選擇公設的反或正都無法由 ZF 公設推導出來, 也就是選擇公設是獨立於 ZF 公設的命題. 現代數學家一般都接受 ZFC 公設, 作為數學研究的基礎.[10]

[10]但也有人覺得選擇公設太強大, 可能從選擇公設推導出令人難以接受的結果, 其中最知名的就是 Banach–Tarski 悖論:

> 一個三維實心球, 在分割成有限塊後, 經過旋轉和平移, 可以重新組合成兩個「一樣」的球.

如果你覺得選擇公設顯而易見，這是一個警惕。也因此，有些數學家會盡量減弱自己運用選擇公設的強度或盡量迴避.