Chapter 5

Function

這一章我們將介紹 function (函數). Function 可以說是要進入高等數學一定要學習的數學工具. 簡單的說函數可以幫助我們了解兩集合之間的關係. 更進一步的, 當我們要探討的集合有更豐富的結構時, 我們有興趣的函數就要求有更多的性質. 比方說在實數上, 由於實數有距離的概念, 我們可以談論所謂的連續函數, 可微函數. 而對於向量空間, 由於有線性組合的性質, 所以我們可以談論所謂的線性映射. 不過在這裡我們僅由集合的概念來探討最基本的函數性質, 也就是說不牽涉任何結構上的問題, 在這裡所談論的函數性質是適用於以後大家會學習的各式各樣函數. 本章中, 我們從最基本的函數定義出發, 介紹一些基本性質. 接著探討一些有特殊性質的函數, 即一對一以及映成函數. 最後我們會將這些概念運用在處理集合的計數問題.

5.1. Basic Definition

給定兩個 nonempty sets X,Y. 它們之間的 function 其實是 X,Y 之間的一種特殊的 relation. 這一種 relation, 給我們一個從 X 到 Y 的對應關係, 由於這種對應關係就如同一個機器經過某一程度的運作將 X 中的元素轉化成 Y 的元素, 所以英文稱之為 "function". 從機器的觀點來看若 $f \subseteq X \times Y$ 是一個從 X 到 Y 的 relation, 怎樣才是一個好機器呢? 首先當然是每個要放入機器的元素都能產生出東西來, 所以我們要求對所有 $x \in X$, 皆存在 $y \in Y$ 使得 $(x,y) \in f$. 另外, 我們當然希望放入機器的元素都能產生固定的東西, 否則每次產生的東西都不相同, 那要這機器何用? 也就是說, 我們要求對所有 $x \in X$, 存在唯一的 $y \in Y$ 使得 $(x,y) \in f$. 這個唯一性用比較好處理的數學寫法就是若 $(x,y) \in f$ 且 $(x,y') \in f$, 則 $y = y'$. 因此 function 的定義如下:

Definition 5.1.1. 假設 X,Y 為 nonempty sets 且 $f \subseteq X \times Y$, 為一個 from X to Y 的 relation. 若 f 滿足以下性質, 則稱 f 為一個 from X to Y 的 *function* (函數). 有時我們也稱 function 為 *mapping* 或 *map* (映射).

(1) 對所有 $x \in X$, 皆存在 $y \in Y$ 使得 $(x,y) \in f$.

(2) 若 $x \in X$, $y,y' \in Y$ 滿足 $(x,y) \in f$ 且 $(x,y') \in f$, 則 $y = y'$.

由於用 relation 的方法來表示 function 不容易感受它是一個有如“機器”的作用, 一般來說我們會用 $f: X \to Y$, 來表示 f 是一個從 X 到 Y 的 function. 而對於任意 $x \in X$, 我們用 $f(x) = y$ 來表示 x 這個元素放入 f 這一個“機器”後產生出 y 來. 也就是說 $f(x) = y$ 就表示 $(x,y) \in f$. 要注意當我們說 f 是一個 function 時必須清楚表達 f 是從哪個集合到哪個集合的 function, 否則無法確定是否會符合 (1), (2) 的性質 (請參考以下 Example 5.1.2). 所以用 $f: X \to Y$ 這樣的符號表示是必要的. 從機器的觀點來說 $f: X \to Y$, 清楚的表達了 f 這個機器是要放那些元素進去且會產生出哪一類的東西, 這樣的機器我們才會覺得是好機器. 因此這裡的 X, Y 特別重要. 這裡 X 就稱為 f 的 *domain* (定義域), 指的是所有可以放入這個機器的元素所成的集合. 而 Y 稱為 f 的 *codomain* (對應域), 就是說這個機器“可能”產生的元素所成的集合. 注意這裡我們用“可能”這個字眼, 是因為在 function 的定義中並沒有要求每個 Y 中的元素都可以找到 X 中的元素代入得到. 當我們拿到或自己設定了一個 function 後就必須說明它是一個 “well-defined function”, 也就是說要檢查它真的符合成為 function 的條件 (用比喻的說法就是說明它是一個好機器). 當然了, 這裡用 “well-defined” 這個字眼只是一種強調的語氣, 所有的 function 都應該是 well-defined.

Example 5.1.2. 我們考慮以下幾種 relations, 看看哪一個是 well-defined function.

(A) 考慮 $X = \{x \in \mathbb{R} : x \geq 0\}$, $Y = \mathbb{R}$ 以及 relation $f \subseteq X \times Y$ 定義為 $f = \{(x,y) \in X \times Y : y^2 = x\}$. 這個 relation f 符合 function 的性質 (1), 因為對於任意 $x \in X$, 表示 $x \geq 0$, 故只要令 $y = \sqrt{x}$, 我們有 $y \in Y = \mathbb{R}$ 且 $y^2 = \sqrt{x}^2 = x$. 得證對於任意 $x \in X$, 存在 $y \in Y$ 使得 $(x,y) \in f$. 不過 f 並不滿足性質 (2). 例如我們有 $1^2 = (-1)^2 = 1$, 故 $(1,1) \in f$ 且 $(1,-1) \in f$. 也因此知 f 不是 function.

(B) 考慮 $X = \{x \in \mathbb{R} : x \geq 0\}$, $Y = \{y \in \mathbb{R} : y \leq 0\}$ 以及 relation $f \subseteq X \times Y$ 定義為 $f = \{(x,y) \in X \times Y : y^2 = x\}$. 這個 relation f 符合 function 定義 (1) 的性質, 因為對於任意 $x \in X$, 表示 $x \geq 0$, 故只要令 $y = -\sqrt{x}$, 我們有 $y \in \mathbb{R}$ 且 $y \leq 0$, 即 $y \in Y$. 又 $y^2 = \sqrt{x}^2 = x$, 故知對於任意 $x \in X$, 存在 $y \in Y$ 使得 $(x,y) \in f$. 另外 f 也滿足性質 (2). 因為若 $x \in X$, $y, y' \in Y$ 滿足 $(x,y) \in f$ 且 $(x,y') \in f$, 表示 $y^2 = x = y'^2$. 因此得 $(y-y')(y+y') = 0$, 亦即 $y = y'$ 或 $y = -y'$. 現若 $x = 0$, 我們有 $y = y' = 0$. 而若 $x \neq 0$, 得 $y \neq 0$ 且 $y' \neq 0$, 此時因 $y, y' \in Y$, 我們有 $y < 0$ 且 $y' < 0$. 故知 $y = -y'$ 不可能成立, 得證 $y = y'$. 依此得證 $f: X \to Y$ 是 function.

(C) 若將 (B) 中的 X 改為 $X = \mathbb{R}$, 則 $f = \{(x,y) \in X \times Y : y^2 = x\}$ 就不是 function. 這是因為 $-1 \in X$, 但我們找不到 $y \in Y \subseteq \mathbb{R}$ 滿足 $y^2 = -1$. 也就是說不存在 $y \in Y$ 滿足 $(-1,y) \in f$. 因此 f 不滿足性質 (1), 所以 f 不是 function. 另一方面, 若我們將 (B) 中的 Y 改為 $Y = \{y \in \mathbb{R} : y < 0\}$, 則 $f = \{(x,y) \in X \times Y : y^2 = x\}$ 也不是 function. 這是因為 $0 \in X$, 但我們找不到 $y \in Y$ 滿足 $y^2 = 0$, 也就是說不存在 $y \in Y$ 滿足 $(0,y) \in f$. 因此 f 不是 function.

(D) 考慮 $X = \mathbb{R}$, $Y = \mathscr{P}(\mathbb{R})$ 以及 function $f: X \to Y$ 其定義為對任意 $x \in X$, 令

$$f(x) = \{y \in \mathbb{R} : y^2 = x\}.$$

我們說明 f 是 well-defined function. 這是因為對任意 $x \in X = \mathbb{R}$, 我們可以將 x 區分為 $x > 0, x = 0, x < 0$ 三種情況. 當 $x > 0$ 時, 我們有 $f(x) = \{\sqrt{x}, -\sqrt{x}\}$ 為 $\mathbb{R}$ 的 subset, 因此確實為 $Y = \mathscr{P}(\mathbb{R})$ 中的元素. 又當 $x = 0$ 時, 我們有 $f(0) = \{0\}$, 仍為 $Y = \mathscr{P}(\mathbb{R})$ 中的元素. 而

當 $x<0$ 時, 我們有 $f(x)=\emptyset$, 亦為 $Y=\mathscr{P}(\mathbb{R})$ 的元素. 因此知對於任意 $x\in X$, 我們確實可找到 $\mathbb{R}$ 的 subset $A\in Y$ 使得 $(x,A)\in f$. 要注意, 在 $x<0$ 的情形, 我們有 $f(x)=\emptyset$, 也就是說在這情況之下, 存在 $\emptyset\in Y$ 使得 $(x,\emptyset)\in f$. 並不是說找不到 $y\in Y$, 使得 $(x,y)\in f$, 所以 f 事實上是符合性質 (1). 另外 f 也符合性質 (2). 這是因為如上面所述, 對任意 $x\in X$, 我們確實找到唯一的 $\mathbb{R}$ 的 subset A 滿足 $f(x)=A$. 要注意, 這裡當 $x>0$, 時 $f(x)$ 是 $\{\sqrt{x},-\sqrt{x}\}$ 這一個 Y 中的元素. 亦即我們有 $(x,\{\sqrt{x},-\sqrt{x}\})\in f$; 而不是 $(x,\sqrt{x})\in f$ 且 $(x,-\sqrt{x})\in f$. 因此 f 確實符合 (2) 的性質.

從 Example 5.1.2 的各個例子, 我們知道即使一樣的映射規則, 會由於定義域或對應域的不同, 影響其是否為一個函數. 也因此, 對於兩個函數 $f:X\to Y$ 和 $f':X'\to Y'$ 只有在 $X=X'$, $Y=Y'$ 且對於所有 $x\in X$, 皆有 $f(x)=f'(x)$ 的情形, 我們才稱 f 和 f' 為同樣的函數. 另外在 Example 5.1.2 (D) 的例子, 其實對應域比實際 f 會產生的元素所成的集合大了許多. 不過這並不影響它是一個函數的事實. 由於一般當我們定義一個函數時, 在實際的情況往往不容易描繪那些元素可以被該函數產生. 所以對應域的用意主要是大致上知道該函數會產生哪一類的東西即可. 以後當我們談論到映成函數時, 會再進一步討論這個問題.

在所有函數中, 有一個簡單但很重要的函數, 稱為 identity function. 簡單來說, 它是一個將定義域中每個元素自己映射到自己的函數. 其正式定義如下:

Definition 5.1.3. 假設 X 為 nonempty set. 定義 $\mathrm{id}_X:X\to X$, 為 $\mathrm{id}_X(x)=x$, $\forall x\in X$. id_X 是一個 function, 我們稱之為 the *identity function* on X.

Question 5.1. *假設 $f:X\to X$ 是一個 function. 將 f 視為 relation on X. 下面哪一個性質可以確保 $f:X\to X$ 是一個 identity function? 若有一項的性質無法推得 f 為 identity function, 試用 $X=\{1,2\}$ 的情況找到例子, 說明該性質無法推得 f 為 identity function.*

(1) *f is reflexive.*

(2) *f is symmetric.*

(3) *f is transitive.*

最後我們介紹幾個由給定的函數, 造出新的函數的方法. 其實給定一個函數 $f:X\to Y$, 我們只要改變定義域 X 或對應域 Y, 就可以得到“新”的函數. 不過在做這些改變時, 要注意仍需遵守函數的規則. 因此最簡單的情形就是, 對任意 X 的 nonempty subset X', 我們考慮 $f|_{X'}:X'\to Y$, 這樣的函數. $f|_{X'}$ 的定義為: 對所有 $x\in X'$, $f|_{X'}(x)=f(x)$. 也就是說 $f|_{X'}$ 只是將 f 的定義域限制縮小在 X' 這一個 subset, 而它的映射規則和 f 是一致的. 因此很容易從 f 為 X 到 Y 的 function 得到 $f|_{X'}$ 為 X' 到 Y 的 function. 我們稱 $f|_{X'}$ 為 the *restriction* of f to X'. 例如在 Example 5.1.2 (B) 中, 我們可以考慮 $X'=\{x\in\mathbb{R}:x>1\}$, 則 $f|_{X'}:X'\to Y$, 仍為一個 function. 我們也可以改變一個 function 的對應域. 當然了, 將對應域擴大沒有甚麼意義. 比較有意思的還是縮小對應域, 讓大家更精確地知道這個函數能產生那些元素. 但要注意不能將對應域縮得太小, 以至於定義域中有元素找不到對應域的元素對應 (例如 Example 5.1.2 (C) 的情況). 例如在 Example 5.1.2 (D) 中, 我們可以將對應域縮小為 $Y'=\{A\in\mathscr{P}(\mathbb{R}):\#(A)\le 2\}$, 仍會使的 $f:X\to Y'$ 為一個 function.

當 $f:X\to Y$ 且 $g:Y\to Z$ 為 functions, 我們可以利用 f,g 造出一個從 X 到 Z 的 function, $g\circ f:X\to Z$. $g\circ f$ 的定義為: 對於任意 $x\in X$, $g\circ f(x)=g(f(x))$. 也就是說 $g\circ f(x)$ 這個 Z 中的元素就是先將 x 代入 f 得到 $f(x)$ 這個 Y 中的元素, 再將 $f(x)$ 代入 g 得到的 Z 中元素 $g(f(x))$. 用圖示就是 $x\xmapsto{f} f(x)\xmapsto{g} g(f(x))$. 我們說明 $g\circ f:X\to Z$ 確實為 function. 首先檢查性質 (1): 對於任意 $x\in X$, 由於 $f:X\to Y$ 為 function 故存在 $y\in Y$ 使得 $f(x)=y$. 此時對此 y, 因 $g:Y\to Z$ 為 function, 故存在 $z\in Z$, 使得 $g(y)=z$. 因此取此 $z\in Z$, 我們有 $g\circ f(x)=g(f(x))=g(y)=z$. 接著檢查性質 (2), 也就是說若 $x\in X$ 則存在唯一的 $z\in Z$ 滿足 $g\circ f(x)=z$. 然而因 $f:X\to Y$ 為 function, 對於任意 $x\in X$, 存在唯一的 $y\in Y$ 使得 $f(x)=y$. 現若有不同的 $z,z'\in Z$ 皆滿足 $g\circ f(x)=z$ 以及 $g\circ f(x)=z'$, 由於 $g\circ f(x)=g(f(x))=g(y)$, 此即表示 $z,z'\in Z$ 皆滿足 $g(y)=z$ 以及 $g(y)=z'$. 此與 $g:Y\to Z$ 為 function 之假設相矛盾, 故知 $z=z'$. 由於 $g\circ f:X\to Z$ 確實為函數, 我們稱此函數為 f 和 g 的 *composite function* (合成函數). 而形成合成函數的這個動作稱為 *composition*.

要注意, 合成函數在合成時, 必需開始的第一個函數所產生的元素要落在第二個函數的定義域中才能合成. 也就是說若第一個函數的對應域包含於第二個函數的定義域, 我們就可以將它們合成. 不過由於擴大對應域, 並不影響函數的取值, 所以在這裡為了方便起見, 我們設定第一個函數的對應域等於第二個函數的定義域. 另外要注意的是合成函數的寫法. 雖然我們寫字是從左至右, 但是寫函數代入的過程是從右到左. 例如將 x 代入 f 得 $f(x)$, 而將 $f(x)$ 代入 g 得 $g(f(x))$. 因此在書寫合成函數時是先動作的函數寫在右邊, 而後動作的寫在左邊, 不要弄錯了.

Example 5.1.4. 假設 $X=\{1,2,3\}$, $Y=\{a,b,c,d\}$, $Z=\{\alpha,\beta,\gamma\}$. 若 $f:X\to Y$ 的定義為: $f(1)=a,f(2)=a,f(3)=c$ 且 $g:Y\to Z$ 的定義為: $g(a)=\gamma,g(b)=\beta,g(c)=\gamma,g(d)=\alpha$, 則 $g\circ f:X\to Z$ 的定義為: $g\circ f(1)=g(f(1))=g(a)=\gamma$, $g\circ f(2)=g(f(2))=g(a)=\gamma$, $g\circ f(3)=g(f(3))=g(c)=\gamma$.

回顧一下 identity function 就是將每個元素固定不變的函數, 所以它和其他的函數合成, 有個“特殊的效果”, 就是保持原函數不變. 我們有以下的性質.

Lemma 5.1.5. 假設 $f:X\to Y$ 是一個 *function.* 對於 X 上的 *identity function* $\mathrm{id}_X:X\to X$ 以及 Y 上的 *identity function* $\mathrm{id}_Y:Y\to Y$, 我們有以下性質*:*

$$f\circ\mathrm{id}_X=f,\quad \mathrm{id}_Y\circ f=f.$$

Proof. 首先檢查 $f\circ\mathrm{id}_X$ 和 f 有相同的定義域以及相同的對應域. 由於 $\mathrm{id}_X:X\to X$ 而 $f:X\to Y$, 所以依合成函數的定義, 我們有 $f\circ\mathrm{id}_X:X\to Y$. 現對任意 $x\in X$, 我們有 $f\circ\mathrm{id}_X(x)=f(\mathrm{id}_X(x))=f(x)$. 得證 $f\circ\mathrm{id}_X=f$.

$\mathrm{id}_Y\circ f$ 和 f 也有相同的定義域以及相同的對應域. 這是因為 $f:X\to Y$ 而 $\mathrm{id}_Y:Y\to Y$, 所以依合成函數的定義, 我們有 $\mathrm{id}_Y\circ f:X\to Y$. 現對任意 $x\in X$, 我們有 $\mathrm{id}_Y\circ f(x)=\mathrm{id}_Y(f(x))$. 因為 $f(x)\in Y$, 故有 $\mathrm{id}_Y(f(x))=f(x)$. 得證 $\mathrm{id}_Y\circ f=f$. □

要注意 composition 並沒有交換性. 也就是說若 $f:X\to Y$ 且 $g:Y\to Z$ 為 functions, 則 $g\circ f$ 並不一定會等於 $f\circ g$. 當然了, 當 $Z\neq X$ 時, $f\circ g$ 根本就沒有定義 (不能合成), 所以它們不相等. 不過即使在 $Z=X$ 情形 $g\circ f$ 和 $f\circ g$ 仍有可能不相等.

Question 5.2. 考慮 $X=\{1,2\}$, 試舉例 $f:X\to X$, $g:X\to X$ 會使得 $g\circ f\neq f\circ g$.

雖然 composition 沒有交換律, 不過重要的是 composition 有所謂的結合律. 我們有以下的性質.

Proposition 5.1.6. 假設 X,Y,Z,W 皆為 *nonempty sets.* 若 $f:X\to Y$, $g:Y\to Z$ 以及 $h:Z\to W$ 為 *functions,* 則
$$h\circ(g\circ f)=(h\circ g)\circ f.$$

Proof. 首先檢查 $h\circ(g\circ f)$ 和 $(h\circ g)\circ f$ 是否有相同的定義域和相同的對應域. 依定義 $g\circ f:X\to Z$, 所以 $h\circ(g\circ f):X\to W$. 得知 $h\circ(g\circ f)$ 的定義域為 X, 對應域為 W. 而 $h\circ g:Y\to W$, 所以 $(h\circ g)\circ f:X\to W$. 得知 $(h\circ g)\circ f$ 的定義域為 X, 對應域為 W.

接著就是說明, 對所有 $x\in X$ 皆有 $h\circ(g\circ f)(x)=(h\circ g)\circ f(x)$. 依定義 $h\circ(g\circ f)(x)$ 為將 $g\circ f(x)$ 代入 h 所得的元素 $h((g\circ f)(x))$. 然而 $g\circ f(x)=g(f(x))$, 故有
$$h\circ(g\circ f)(x)=h((g\circ f)(x))=h(g(f(x))).$$
也就是說 $h\circ(g\circ f)(x)$ 就是將 x 代入 f 所得的元素 $f(x)$, 再代入 g 後所得的元素 $g(f(x))$, 最後再代入 h 得 $h(g(f(x)))$. 同理 $(h\circ g)\circ f(x)$ 為將 $f(x)$ 代入 $h\circ g$ 所得的元素 $(h\circ g)(f(x))$. 然而 $(h\circ g)(f(x))$ 為將 $f(x)$ 代入 g 後所得的元素 $g(f(x))$ 再代入 h, 故有
$$(h\circ g)\circ f(x)=(h\circ g)(f(x))=h(g(f(x))).$$
得證 $h\circ(g\circ f)$ 和 $(h\circ g)\circ f$ 為相同的函數. □

合成函數有結合律, 這在我們以後處理函數的合成問題時相當重要, 大家千萬要記住.

5.2. Image and Inverse Image

前面提過一個函數的對應域並沒有明確的指出該函數所能產生的元素有哪些, 所以我們有興趣知道該函數所產生的元素有哪些. 同樣的我們也有興趣知道函數限制在某個非空子集所能產生的元素, 所以引進了 image 的概念. 反過來說, 對於對應域的非空子集, 我們也對於定義域裡有哪些元素可以產生此子集的元素有興趣, 因此引進了 inverse image 的概念. 在以後的數學課程裡, image 和 inverse image 都是用來了解一個函數經常討論的課題.

簡單來說, 給定一個 function $f:X\to Y$ 以及 X 的 subset A, 所謂 A 在 f 的作用之下所得 image 就是收集 A 中的元素代入 f 後所得元素的集合. 我們有以下的定義.

Definition 5.2.1. 假設 $f:X\to Y$ 為 function 且 $A\subseteq X$. 定義 $f(A)=\{f(a):a\in A\}$, 且稱 $f(A)$ 為 the *image* of A under f. 特別的, the image of X under f, 即 $f(X)$ 稱為 f 的 *range* (值域).

從 $f(A)$ 的定義, 我們知道 $f(A)$ 是對應域 Y 的 subset. 這個定義很直接, 很容易讓人理解這個元素的組成元素. 不過它卻不容易掌握, 主要是很難描繪其元素 (請參閱以下 Example 5.2.2). 另外要注意的是, 有的同學可能會誤解 $f(a) \in f(A)$ 表示 $a \in A$. 其實這在邏輯上是錯誤的, 因為有可能有元素 $b \not\in A$ 但是 $f(b) \in f(A)$. 一個比較好的寫法是, 直接將 $f(A)$ 裡的元素看成是 Y 中的元素. 也就是考慮 $y \in f(A)$, 表示存在 $a \in A$ 使得 $y = f(a)$. 反之, 若 $y \in A$ 且存在 $a \in A$ 使得 $y = f(a)$ 依定義就表示 $y \in f(A)$. 所以 $f(A)$ 有另一個等價的定義是

$$f(A) = \{y \in Y : \exists a \in A, y = f(a)\}.$$

這個定義感覺較不自然, 不過反而比較容易讓我們掌握 $f(A)$ 的元素. 我們看以下的例子.

Example 5.2.2. 令 $X = \mathbb{R} \setminus \{3\}$, 且 $f : X \to \mathbb{R}$ 定義為 $f(x) = (x+1)/(x-3)$, $\forall x \in X$. 很容易檢查, f 為 well-defined function. 我們要找出 f 的 range, 即 $f(X)$. 若直接用定義, 我們有 $f(X) = \{(x+1)/(x-3) : x \in X\}$, 很難讓我們知道 $f(X)$ 中到底有那些元素. 不過若用另一個等價定義, 對於任意 $y \in f(X)$, 表示 $y \in \mathbb{R}$ 且存在 $x \in X$ 使得 $y = f(x) = (x+1)/(x-3)$. 也就是說 y 這個實數, 會使得方程式 $y = (x+1)/(x-3)$ 在 X 中有解. 注意此時 y 是實數, x 是未知數, 所以利用 $y(x-3) = x+1$ 可得 $(y-1)x = 3y+1$, 解得 $x = (3y+1)/(y-1)$. 要注意, 這個推演過程告訴我們的是, 若 $y \in \mathbb{R}$ 且存在 $x \in X$ 使得 $y = (x+1)/(x-3)$, 則 $x = (3y+1)/(y-1)$. 所以它僅告訴我們 x 可能的值, 並不保證 x 必定存在. 因此我們須代回驗證這樣的 x 確實可得 $f(x) = y$.

首先由 $x = (3y+1)/(y-1)$, 我們可知 $y \neq 1$. 事實上如果 $y = 1$, 則由假設存在 $x \in X$ 滿足 $1 = (x+1)/(x-3)$, 會得到 $x+1 = x-3$, 即 $1 = -3$ 之矛盾. 現假設 $y \neq 1$, 則當 $x = (3y+1)/(y-1)$, 我們有

$$\frac{x+1}{x-3} = \frac{\frac{3y+1}{y-1}+1}{\frac{3y+1}{y-1}-3} = \frac{\frac{4y}{y-1}}{\frac{4}{y-1}} = \frac{4y}{4} = y.$$

也就是說, 當 $y \neq 1$ 時, 確實存在 $x = (3y+1)/(y-1) \in \mathbb{R}$ 使得 $(x+1)/(x-3) = y$. 我們要確認此時 $x \neq 3$, 才能確定 $x \in X$. 然而若 $x = (3y+1)/(y-1) = 3$, 表示 $3y+1 = 3y-3$, 即得 $1 = -3$ 之矛盾, 故知 $x \in X$. 我們證得了, 當 $y \neq 1$ 時, 存在 $x \in X$ 使得 $y = f(x)$. 又知當 $y = 1$ 時不可能找到 $x \in X$ 使得 $y = f(x)$. 因此得 $f(X) = \mathbb{R} \setminus \{1\}$.

接下來, 我們探討有關 image 的性質.

Lemma 5.2.3. 假設 $f : X \to Y$ 為 *function* 且 A, B 為 X 的 *subsets.* 若 $A \subseteq B$, 則 $f(A) \subseteq f(B)$.

Proof. 依定義, 若 $y \in f(A)$, 表示存在 $a \in A$, 使得 $y = f(a)$. 此時因 $A \subseteq B$, 我們有 $a \in B$. 也就是此時考慮 $a \in B$ 會使得 $y = f(a)$, 故 $y \in f(B)$. 得證 $f(A) \subseteq f(B)$. □

現若考慮 X 任意兩個 subsets A, B, 我們有 $A \subseteq A \cup B$ 且 $B \subseteq A \cup B$. 故利用 Lemma 5.2.3, 可得 $f(A) \subseteq f(A \cup B)$ 且 $f(B) \subseteq f(A \cup B)$. 因此由 Corollary 3.2.4, 得 $f(A) \cup f(B) \subseteq f(A \cup B)$. 反之, 若 $y \in f(A \cup B)$, 表示存在 $x \in A \cup B$, 使得 $y = f(x)$. 此時, 若 $x \in A$, 則得 $y = f(x) \in f(A)$,

而若 $x \in B$, 則得 $y = f(x) \in f(B)$. 因此得 $y \in f(A)$ 或 $y \in f(B)$. 此即表示 $y \in f(A) \cup f(B)$, 得證 $f(A \cup B) \subseteq f(A) \cup f(B)$. 因此我們推得了以下性質.

Proposition 5.2.4. *假設 $f : X \to Y$ 為 function 且 A, B 為 X 的 subsets. 則*

$$f(A) \cup f(B) = f(A \cup B).$$

至於交集, 由於 $A \cap B \subseteq A$ 以及 $A \cap B \subseteq B$, 因此由 Lemma 5.2.3, 可得 $f(A \cap B) \subseteq f(A)$ 以及 $f(A \cap B) \subseteq f(B)$. 故由 Corollary 3.2.4, 得 $f(A \cap B) \subseteq f(A) \cap f(B)$. 不過要注意 $f(A) \cap f(B)$ 並不一定包含於 $f(A \cap B)$. 因為若 $y \in f(A) \cap f(B)$, 表示 $y \in f(A)$ 且 $y \in f(B)$, 亦即存在 $a \in A$ 以及 $b \in B$ 滿足 $y = f(a)$ 及 $y = f(b)$. 但這並不表示 $a = b$, 因此我們無法推得 $a \in A \cap B$. 例如考慮函數 $f : \{1, 2\} \to \{0\}$ 定義為 $f(1) = f(2) = 0$. 若令 $A = \{1\}$, $B = \{2\}$, 我們有 $A \cap B = \emptyset$, 故 $f(A \cap B) = \emptyset$. 但 $f(A) = f(B) = \{0\}$ 因此 $f(A) \cap f(B) = \{0\}$. 由此例知 $f(A) \cap f(B)$ 有可能不包含於 $f(A \cap B)$. 不過 $f(A \cap B) \subseteq f(A) \cap f(B)$ 永遠是對的.

對於差集, 我們要考慮的是 $f(A \setminus B)$ 和 $f(A) \setminus f(B)$ 的關係. 首先若 $y \in f(A) \setminus f(B)$, 表示存在 $a \in A$ 使得 $y = f(a)$ 但 $y \notin f(B)$. 現若 $a \in B$, 會造成 $y = f(a) \in f(B)$ 之矛盾. 故知 $a \in A \setminus B$, 即 $y = f(a) \in f(A \setminus B)$. 得證 $f(A) \setminus f(B) \subseteq f(A \setminus B)$. 不過反過來並不成立, 因為若 $y \in f(A \setminus B)$, 表示存在 $a \in A \setminus B$. 因為 $(A \setminus B) \subseteq A$, 我們當然有 $f(a) \in f(A)$. 但 $a \notin B$, 並不表示 $y = f(a) \notin f(B)$, 因為很有可能存在 $b \in B$ 滿足 $f(a) = f(b)$. 例如前面 $f : \{1, 2\} \to \{0\}$ 定義為 $f(1) = f(2) = 0$ 的例子. 若令 $A = \{1\}, B = \{2\}$, 我們有 $A \setminus B = A$, 因此有 $f(A \setminus B) = f(A) = \{0\}$. 但 $f(A) = f(B) = \{0\}$, 所以 $f(A) \setminus f(B) = \emptyset$. 由此例知 $f(A \setminus B)$ 有可能不包含於 $f(A) \setminus f(B)$. 不過 $f(A) \setminus f(B) \subseteq f(A \setminus B)$ 永遠是對的.

Question 5.3. *假設 X 為宇集, $A \subseteq X$ 且 $f : X \to X$ 為 function. 試問 $f(A^c) \subseteq f(A)^c$ 是否成立? 又 $f(A)^c \subseteq f(A^c)$ 是否成立?*

接下來, 我們來探討所謂的 inverse image. 簡單來說, 給定一個 function $f : X \to Y$ 以及 Y 的 subset C, 所謂 C 在 f 的作用之下所得 inverse image 就是收集那些經由 f 會落在 C 中的元素所成的集合. 我們有以下的定義.

Definition 5.2.5. 假設 $f : X \to Y$ 為 function 且 $C \subseteq Y$. 定義 $f^{-1}(C) = \{x \in X : f(x) \in C\}$, 且稱 $f^{-1}(C)$ 為 the *inverse image* of C under f.

從 $f^{-1}(C)$ 的定義, 我們知道 $f^{-1}(C)$ 是定義域 X 的 subset. 這個 inverse image 的定義已充分描繪其元素, 所以我們可以直接利用這個定義處理 inverse image 的性質. 以下的定理, 我們會發現, inverse image 比起 image 更能保持集合之間的運算關係.

Proposition 5.2.6. *假設 $f : X \to Y$ 為 function 且 C, D 為 Y 的 subsets.*

(1) 若 $C \subseteq D$, 則 $f^{-1}(C) \subseteq f^{-1}(D)$.

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

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

(4) $f^{-1}(C\setminus D)=f^{-1}(C)\setminus f^{-1}(D)$.

Proof. (1) 假設 $x\in f^{-1}(C)$, 表示 $f(x)\in C$. 故由 $C\subseteq D$, 得 $f(x)\in D$, 亦即 $x\in f^{-1}(D)$. 得證 $f^{-1}(C)\subseteq f^{-1}(D)$.

(2) 由於 $C\subseteq C\cup D$ 且 $D\subseteq C\cup D$, 故由 (1) 知 $f^{-1}(C)\subseteq f^{-1}(C\cup D)$ 且 $f^{-1}(D)\subseteq f^{-1}(C\cup D)$. 因此由 Corollary 3.2.4 可得 $f^{-1}(C)\cup f^{-1}(D)\subseteq f^{-1}(C\cup D)$. 反之, 假設 $x\in f^{-1}(C\cup D)$, 表示 $f(x)\in C\cup D$, 亦即 $f(x)\in C$ 或 $f(x)\in D$. 依定義得 $x\in f^{-1}(C)$ 或 $x\in f^{-1}(D)$, 也就是說 $x\in f^{-1}(C)\cup f^{-1}(D)$. 證明了 $f^{-1}(C\cup D)\subseteq f^{-1}(C)\cup f^{-1}(D)$, 也因此證得 $f^{-1}(C\cup D)=f^{-1}(C)\cup f^{-1}(D)$.

(3) 由於 $C\cap D\subseteq C$ 且 $C\cap D\subseteq D$, 故由 (1) 知 $f^{-1}(C\cap D)\subseteq f^{-1}(C)$ 且 $f^{-1}(C\cap D)\subseteq f^{-1}(D)$. 因此由 Corollary 3.2.4 可得 $f^{-1}(C\cap D)\subseteq f^{-1}(C)\cap f^{-1}(D)$. 反之, 假設 $x\in f^{-1}(C)\cap f^{-1}(D)$, 表示 $x\in f^{-1}(C)$ 且 $x\in f^{-1}(D)$, 亦即 $f(x)\in C$ 且 $f(x)\in D$. 因此得 $f(x)\in C\cap D$, 依定義即為 $x\in f^{-1}(C\cap D)$. 證明了 $f^{-1}(C)\cap f^{-1}(D)\subseteq f^{-1}(C\cap D)$, 也因此證得 $f^{-1}(C\cap D)=f^{-1}(C)\cap f^{-1}(D)$.

(4) 假設 $x\in f^{-1}(C\setminus D)$, 表示 $f(x)\in C\setminus D$, 亦即 $f(x)\in C$ 且 $f(x)\not\in D$. 得知 $x\in f^{-1}(C)$. 現若又 $x\in f^{-1}(D)$, 表示 $f(x)\in D$, 此與前面 $f(x)\not\in D$ 相矛盾, 故知 $x\not\in f^{-1}(D)$. 由 $x\in f^{-1}(C)$ 且 $x\not\in f^{-1}(D)$, 我們得 $x\in f^{-1}(C)\setminus f^{-1}(D)$. 得證 $f^{-1}(C\setminus D)\subseteq f^{-1}(C)\setminus f^{-1}(D)$. 反之, 假設 $x\in f^{-1}(C)\setminus f^{-1}(D)$, 表示 $x\in f^{-1}(C)$ 且 $x\not\in f^{-1}(D)$. 得知 $f(x)\in C$. 現若又 $f(x)\in D$, 表示 $x\in f^{-1}(D)$, 此與前面 $x\not\in f^{-1}(D)$ 相矛盾, 故知 $f(x)\not\in D$. 由 $f(x)\in C$ 且 $f(x)\not\in D$, 我們得 $f(x)\in C\setminus D$, 即 $x\in f^{-1}(C\setminus D)$. 得證 $f^{-1}(C)\setminus f^{-1}(D)\subseteq f^{-1}(C\setminus D)$, 也因此證明了 $f^{-1}(C\setminus D)=f^{-1}(C)\setminus f^{-1}(D)$. □

Question 5.4. *假設 X 為宇集, $A\subseteq X$ 且 $f:X\to X$ 為 function. 試問 $f^{-1}(A^c)\subseteq(f^{-1}(A))^c$ 是否成立? 又 $(f^{-1}(A))^c\subseteq f^{-1}(A^c)$ 是否成立?*

當 $f:X\to Y$ 為 function 且 A 為 X 的 subset 時, 既然 $f(A)$ 為 Y 的 subset, 我們當然可以考慮 $f^{-1}(f(A))$. 現假設 $a\in A$, 我們有 $f(a)\in f(A)$, 故依 inverse image 的定義得 $a\in f^{-1}(f(A))$, 得證 $A\subseteq f^{-1}(f(A))$. 反之, 若 $x\in f^{-1}(f(A))$, 表示 $f(x)\in f(A)$, 但這並不表示 $x\in A$. 例如前面 $f:\{1,2\}\to\{0\}$ 定義為 $f(1)=f(2)=0$ 的例子. 若令 $A=\{1\}$, 我們有 $f(A)=\{0\}$, 但 $f^{-1}(f(A))=f^{-1}(\{0\})=\{1,2\}\neq A$. 由此例知 $f^{-1}(f(A))$ 有可能不包含於 A. 不過 $A\subseteq f^{-1}(f(A))$ 永遠是對的.

Question 5.5. *假設 $f:X\to Y$ 為 function. 試證明 $f^{-1}(f(X))=X$.*

同樣的當 C 為 Y 的 subset 時, 既然 $f^{-1}(C)$ 為 X 的 subset, 我們當然可以考慮 $f(f^{-1}(C))$. 現假設 $y\in f(f^{-1}(C))$, 表示存在 $x\in f^{-1}(C)$ 使得 $y=f(x)$. 然而依 inverse image 的定義 $x\in f^{-1}(C)$ 表示 $f(x)\in C$, 故得 $y=f(x)\in C$. 得證 $f(f^{-1}(C))\subseteq C$. 反之, 若 $y\in C$, 不見得會有 $y\in f(f^{-1}(C))$, 這是因為不一定存在 $x\in X$ 使得 $y=f(x)$. 例如考慮函數 $f:\{1,2\}\to\{3,4\}$ 定義為 $f(1)=f(2)=3$. 若令 $C=\{3,4\}$, 我們有 $f^{-1}(C)=\{1,2\}$, 但 $f(f^{-1}(C))=f(\{1,2\})=\{3\}\neq C$. 由此例知 C 有可能不包含於 $f(f^{-1}(C))$. 不過若 $y\in C$ 且存在 $x\in X$ 使得 $y=f(x)$, 則情況就不一樣了. 我們有下面的結果.

Proposition 5.2.7. 假設 $f:X\to Y$ 為 *function* 且 C 為 Y 的 *subset*, 則

$$f(f^{-1}(C))=C\cap f(X).$$

Proof. 前面已證得 $f(f^{-1}(C))\subseteq C$, 又因 $f^{-1}(C)\subseteq X$, 故有 $f(f^{-1}(C))\subseteq f(X)$, 因此得 $f(f^{-1}(C))\subseteq C\cap f(X)$. 另一方面若 $y\in C\cap f(X)$, 表示 $y\in C$ 且存在 $x\in X$ 使得 $y=f(x)$. 因此知, 此 x 滿足 $f(x)=y\in C$, 亦即 $x\in f^{-1}(C)$. 所以 $y=f(x)\in f(f^{-1}(C))$, 得證 $C\cap f(X)\subseteq f(f^{-1}(C))$. 因此證明了 $f(f^{-1}(C))=C\cap f(X)$. □

Proposition 5.2.7, 有許多應用. 例如給定函數 $f:X\to Y$ 以及 X 的 subset A. 我們有 $f(A)$ 為 Y 的 subset, 且 $f(A)\subseteq f(X)$. 故套用 Proposition 5.2.7 ($C=f(A)$ 的情況), 可得

$$f(f^{-1}(f(A)))=f(A)\cap f(X)=f(A).$$

Question 5.6. 假設 $f:X\to Y$ 為 *function* 且 C 為 Y 的 *subset.* 試利用 *Proposition 5.2.7, Proposition 5.2.6* 以及 *Question 5.5* 證明

$$f^{-1}(f(f^{-1}(C)))=f^{-1}(C).$$

5.3. Onto, One-to-One and Inverse

Onto 和 one-to-one 是函數中兩種特殊的性質. 有這兩種特殊性質的函數就會有所謂的反函數. 這些都是將來在進階數學課程中會遇到的性質. 我們將學習如何辨認 onto 及 one-to-one 的函數, 以及它們基本的性質.

所謂 onto (映成) 的函數, 簡單來說就是對應域裡每個元素, 都可由定義域裡的元素映射而得. 也就是說一個函數的 range (值域) 恰為 codomain (對應域) 就是 onto 的函數. 其正式定義如下:

Definition 5.3.1. 假設 $f:X\to Y$ 為 function. 若 $f(X)=Y$, 則我們稱 f 為 *onto*. 也就是說對任意 $y\in Y$ 皆存在 $x\in X$ 使得 $f(x)=y$. 有時也稱 onto 的函數為 *surjective function.*

用 inverse image 的觀點來看 $f:X\to Y$ 為 onto 也等同於對於任意 $y\in Y$, $f^{-1}(\{y\})\neq\emptyset$. 不過當要證明一個函數為 onto, 一般常用的方法還是如前一節找 image 的方法處理. 我們看以下的例子.

Example 5.3.2. (A) 在 Example 5.2.2 中我們考慮函數 $f:\mathbb{R}\setminus\{3\}\to\mathbb{R}$ 定義為 $f(x)=(x+1)/(x-3)$, $\forall x\in X$. 我們找出 f 的 range 為 $\mathbb{R}\setminus\{1\}$. 因此 f 不是 onto. 但若考慮 “新” 的函數 $g:\mathbb{R}\setminus\{3\}\to\mathbb{R}\setminus\{1\}$ 定義為 $g(x)=(x+1)/(x-3)$, $\forall x\in X$, 則 $g(x)$ 為 onto.

(B) 考慮函數 $f:\mathbb{Z}\to\mathbb{N}\cup\{0\}$ 定義為

$$f(n)=\begin{cases}2n, & \text{if } n\geq 0;\\ -2n-1, & \text{if } n<0.\end{cases}$$

我們說明 f 為 onto. 首先由 f 的映射規則我們大致知道可以將 f 的對應域元素分成偶數與奇數. 現若 $k\in\mathbb{N}\cup\{0\}$ 為偶數, 表示 $k/2\in\mathbb{Z}$ 且 $k/2\geq 0$. 故此時取 $n=k/2$, 我們有 $f(n)=2n=k$. 而若 $k\in\mathbb{N}\cup\{0\}$ 為奇數, 表示 $k+1\in\mathbb{Z}$ 為偶數且 $k+1>0$. 此時取

$n=-(k+1)/2$, 我們有 $n\in\mathbb{Z}$ 且 $n<0$, 故依定義有 $f(n)=-2n-1=(-2(-(k+1)/2)-1=k$. 得證 f 為 onto.

當遇到抽象的函數 (即函數沒有具體的形式) 時, 有時用定義證明它是 onto 有點麻煩. 接下來我們介紹一個很好用來證明一個抽象函數為 onto 的方法.

Theorem 5.3.3. 假設 $f:X\to Y$ 為 *function*. 則 f 為 *onto* 若且唯若存在 $g:Y\to X$ 為 *function* 滿足 $f\circ g=\mathrm{id}_Y$.

Proof. $(\Rightarrow)$ 當 $f:X\to Y$ 為 onto 時, 我們要利用 f 找到一個函數 $g:Y\to X$ 滿足 $f\circ g=\mathrm{id}_Y$. 這一個證明其實嚴格來說是要用 *Axiom of Choice* 來處理, 不過由於我們尚未介紹過它, 所以這裡的證明嚴格來說並不是很完善. 希望大家知道它的證明大致上的意思即可. 首先由 f 為 onto, 我們知道對任意 $y\in Y$, $f^{-1}(\{y\})\neq\emptyset$. 因此對於任意 $y\in Y$, 我們定義 $g(y)$ 為非空集合 $f^{-1}(\{y\})$ 中的某一個特定元素. 由此我們定義了一個從 Y 到 X 的函數 g. 依此定義我們有 $f\circ g:Y\to Y$ 且對於任意 $y\in Y$, 若 $g(y)=x$, 則因 $x\in f^{-1}(\{y\})$, 知 $f(x)=y$. 也就是說 $f\circ g(y)=f(g(y))=f(x)=y$. 得證 $f\circ g=\mathrm{id}_Y$.

$(\Leftarrow)$ 現假設 $g:Y\to X$ 為 function 且滿足 $f\circ g=\mathrm{id}_Y$, 我們要證明 $f:X\to Y$ 為 onto, 也就是說對任意 $y\in Y$, 要找到 $x\in X$ 使得 $y=f(x)$. 然而因 $y\in Y$, 我們有 $g(y)\in X$. 因此若考慮 $x=g(y)\in X$, 則 $f(x)=f(g(y))=f\circ g(y)=\mathrm{id}_Y(y)=y$. 得證確實存在 $x\in X$ 使得 $y=f(x)$, 故知 $f:X\to Y$ 為 onto. □

Example 5.3.4. 考慮 $X=\{1,2,3\}$, $Y=\{a,b\}$ 以及 $f:X\to Y$, 定義為 $f(1)=f(2)=a$, $f(3)=b$. 依此定義 $f:X\to Y$ 為 onto. 我們要找到 $g:Y\to X$ 使得 $f\circ g=\mathrm{id}_Y$. 由於要定義從 Y 到 X 的函數, 所以每個 Y 中的元素都要定義其如何映射. 現由於 $f^{-1}(\{a\})=\{1,2\}$, 我們任取 $f^{-1}(\{a\})$ 中的一個元素, 比方說取 2, 因此定義 $g(a)=2$. 又由於 $f^{-1}(\{b\})=\{3\}$ 僅有一個元素, 所以我們定義 $g(b)=3$. 依此定義我們有 $g:Y\to X$ 為一個 function 且滿足 $f\circ g(a)=f(g(a))=f(2)=a$ 以及 $f\circ g(b)=f(g(b))=f(3)=b$. 故得 $f\circ g=\mathrm{id}_Y$.

Theorem 5.3.3 可以幫我們不必用 onto 的定義處理有關 onto 的證明. 例如我們有以下的性質.

Proposition 5.3.5. 若 $f_1:X\to Y$, $f_2:Y\to Z$ 皆為 *onto function*, 則 $f_2\circ f_1:X\to Z$ 亦為 *onto*.

Proof. (方法一) 我們可以用 onto 的定義處理, 對於任意 $z\in Z$, 要找到 $x\in X$ 使得 $f_2\circ f_1(x)=z$. 然而 $f_2:Y\to Z$ 為 onto, 故對此 $z\in Z$, 存在 $y\in Y$ 使得 $f_2(y)=z$. 又因 $f_1:X\to Y$ 為 onto, 所以對此 $y\in Y$, 存在 $x\in X$ 使得 $f_1(x)=y$. 現利用此 x, 我們有 $f_2\circ f_1(x)=f_2(f_1(x))=f_2(y)=z$. 因此得證 $f_2\circ f_1:X\to Z$ 為 onto.

(方法二) 利用 Theorem 5.3.3, 要證明 $f_2\circ f_1:X\to Z$ 為 onto, 我們僅要找到 $g:Z\to X$ 使得 $(f_2\circ f_1)\circ g=\mathrm{id}_Z$ 即可. 然而已知 $f_1:X\to Y$, $f_2:Y\to Z$ 皆為 onto, 故由 Theorem 5.3.3 知存在 $g_1:Y\to X$, $g_2:Z\to Y$ 滿足 $f_1\circ g_1=\mathrm{id}_Y$ 以及 $f_2\circ g_2=\mathrm{id}_Z$. 現令 $g=g_1\circ g_2:Z\to X$,

我們有 $(f_2\circ f_1)\circ g=(f_2\circ f_1)\circ(g_1\circ g_2)$. 利用合成函數的結合律 (Proposition 5.1.6) 以及 Lemma 5.1.5, 我們有 $(f_2\circ f_1)\circ(g_1\circ g_2)=f_2\circ(f_1\circ g_1)\circ g_2=f_2\circ(\mathrm{id}_Y\circ g_2)=f_2\circ g_2=\mathrm{id}_Z$. 得證 $(f_2\circ f_1)\circ g=\mathrm{id}_Z$. □

要注意 Proposition 5.3.5 的反向不一定成立, 也就是說 $f_2\circ f_1$ 為 onto 並不表示 f_1,f_2 皆為 onto. 例如在 Example 5.3.4 中 $g:\{a,b\}\to\{1,2,3\}$ 定義為 $g(a)=2,g(b)=3$, 不是 onto. 但 $f\circ g=\mathrm{id}_{\{a,b\}}$ 為 onto. 不過我們有以下之結果.

Corollary 5.3.6. *若 $f_1:X\to Y$, $f_2:Y\to Z$ 皆為 function 且 $f_2\circ f_1:X\to Z$ 為 onto, 則 f_2 為 onto.*

Proof. 由 $f_2\circ f_1:X\to Z$ 為 onto, 利用 Theorem 5.3.3 知存在 $g:Z\to X$ 滿足 $(f_2\circ f_1)\circ g=\mathrm{id}_Z$. 因此利用合成函數結合律得 $f_2\circ(f_1\circ g)=\mathrm{id}_Z$. 現令 $g_2=f_1\circ g$, 我們有 $g_2:Z\to Y$ 且滿足 $f_2\circ g_2=f_2\circ(f_1\circ g)=\mathrm{id}_Z$. 所以再次利用 Theorem 5.3.3 得證 $f_2:Y\to Z$ 為 onto. □

Question 5.7. *試利用 onto 的定義證明 Corollary 5.3.6.*

要注意 Corollary 5.3.6 的反向也不一定成立, 也就是說單僅假設 f_2 為 onto 並不能保證 $f_2\circ f_1$ 為 onto.

Question 5.8. *考慮 $X=\{a,b\}$, $Y=\{1,2,3\}$, 試找到例子 $f_1:X\to Y$, $f_2:Y\to X$ 為 functions 其中 f_2 為 onto, 但是 $f_2\circ f_1$ 不是 onto.*

接下來我們探討所謂 one-to-one (一對一) 的函數, 簡單來說就是定義域裡相異的的元素都會被映射對應域裡相異的元素. 其正式定義如下:

Definition 5.3.7. 假設 $f:X\to Y$ 為 function. 若對於 X 中任兩相異元素 $x_1\neq x_2$, 皆有 $f(x_1)\neq f(x_2)$, 則我們稱 f 為 *one-to-one*. 有時也稱 one-to-one 的函數為 *injective function*.

用 inverse image 的觀點來看 $f:X\to Y$ 為 one-to-one 也等同於對於任意 $y\in Y$, $\#(f^{-1}(\{y\}))\leq 1$ (有可能 $f^{-1}(\{y\}))=\emptyset$). 另外一般來說要處理不等號較為困難, 所以當要證明 one-to-one 時, 我們大都用 Definition 5.3.7 的 contrapositive 處理. 也就是說證明對任意 $x_1,x_2\in X$ 滿足 $f(x_1)=f(x_2)$, 則 $x_1=x_2$. 我們看以下的例子.

Example 5.3.8. 我們探討 Example 5.3.2 中的函數是否為 one-to-one.

(A) 考慮函數 $f:\mathbb{R}\setminus\{3\}\to\mathbb{R}$ 定義為 $f(x)=(x+1)/(x-3), \forall x\in X$. 現若 $x_1,x_2\in\mathbb{R}\setminus\{3\}$ 滿足 $f(x_1)=f(x_2)$, 表示 $(x_1+1)/(x_1-3)=(x_2+1)/(x_2-3)$, 即 $(x_1+1)(x_2-3)=(x_2+1)(x_1-3)$. 化簡得 $x_2-3x_1=x_1-3x_2$, 即 $x_1=x_2$. 因此得證 f 為 one-to-one.

(B) 考慮函數 $f:\mathbb{Z}\to\mathbb{N}\cup\{0\}$ 定義為

$$f(n)=\begin{cases}2n, & \text{if } n\geq 0;\\ -2n-1, & \text{if } n<0.\end{cases}$$

現假設 $n_1,n_2\in\mathbb{Z}$ 滿足 $f(n_1)=f(n_2)$. 由於若 n_1,n_2 其中有一個為大於等於 0 另一個為小於 0, 則依 f 的定義 $f(n_1)$ 和 $f(n_2)$ 必為一奇一偶, 此與 $f(n_1)=f(n_2)$ 相矛盾. 因此我們

有 $n_1 \geq 0, n_2 \geq 0$ 或 $n_1 < 0, n_2 < 0$. 當 $n_1 \geq 0, n_2 \geq 0$, 我們有 $f(n_1) = 2n_1, f(n_2) = 2n_2$, 故由 $f(n_1) = f(n_2)$ 之假設得 $n_1 = n_2$. 同理, 當 $n_1 < 0, n_2 < 0$, 我們有 $f(n_1) = -2n_1 - 1, f(n_2) = -2n_2 - 1$, 故由 $f(n_1) = f(n_2)$ 之假設得 $n_1 = n_2$. 因此得證 f 為 one-to-one.

和 onto 的情況一樣, 我們有一個不必由定義證明一個抽象函數為 one-to-one 的方法.

Theorem 5.3.9. 假設 $f : X \to Y$ 為 *function.* 則 f 為 *one-to-one* 若且唯若存在 $h : Y \to X$ 為 *function* 滿足 $h \circ f = \mathrm{id}_X$.

Proof. $(\Rightarrow)$ 當 $f : X \to Y$ 為 one-to-one 時, 我們要利用 f 找到一個函數 $h : Y \to X$ 滿足 $h \circ f = \mathrm{id}_Y$. 首先由 f 為 one-to-one, 我們知道對任意 $y \in Y$, $\#(f^{-1}(\{y\})) \leq 1$. 因此對於任意 $y \in Y$, 若 $f^{-1}(\{y\}) = \emptyset$ 我們定義 $h(y)$ 為 X 中某一個固定元素. 而若 $f^{-1}(\{y\}) \neq \emptyset$, 則 $f^{-1}(\{y\})$ 僅有一個元素. 因此若 $f^{-1}(\{y\}) = \{x\}$ 我們便定義 $h(y) = x$. 依此我們便定義了一個從 Y 到 X 的函數 h. 依此定義我們有 $h \circ f : X \to X$ 且對於任意 $x \in X$, 若 $f(x) = y$, 則因 $x \in f^{-1}(\{y\})$, 知 $h(y) = x$. 也就是說 $h \circ f(x) = h(f(x)) = h(y) = x$. 得證 $h \circ f = \mathrm{id}_X$.

$(\Leftarrow)$ 現假設 $h : Y \to X$ 為 function 且滿足 $h \circ f = \mathrm{id}_X$, 我們要證明 $f : X \to Y$ 為 one-to-one, 也就是說若 $x_1, x_2 \in X$ 滿足 $f(x_1) = f(x_2)$, 我們要證明 $x_1 = x_2$. 然而因 $x_1 \in X$, 我們有 $x_1 = \mathrm{id}_X(x_1) = h \circ f(x_1) = h(f(x_1))$. 同理因 $x_2 \in X$, 我們有 $x_2 = h(f(x_2))$. 現由假設 $f(x_1) = f(x_2) \in Y$ 以及 $h : Y \to X$ 為 function 知 $h(f(x_1)) = h(f(x_2))$. 因此得證

$$x_1 = h(f(x_1)) = h(f(x_2)) = x_2.$$

□

Example 5.3.10. 考慮 $X = \{a, b\}$, $Y = \{1, 2, 3\}$ 以及 $f : X \to Y$, 定義為 $f(a) = 3$, $f(b) = 1$. 依此定義 $f : X \to Y$ 為 one-to-one. 我們要找到 $h : Y \to X$ 使得 $h \circ f = \mathrm{id}_X$. 由於要定義從 Y 到 X 的函數, 所以每個 Y 中的元素都要定義其如何映射. 現由於 $f^{-1}(\{2\}) = \emptyset$, 我們任取 X 中的一個元素, 比方說取 a, 因此定義 $h(2) = a$. 又由於 $f^{-1}(\{1\}) = \{b\}$ 所以我們定義 $h(1) = b$. 而 $f^{-1}(\{3\}) = \{a\}$ 所以我們定義 $h(3) = a$ 依此定義我們有 $h : Y \to X$ 為一個 function 且滿足 $h \circ f(a) = h(f(a)) = h(3) = a$ 以及 $h \circ f(b) = h(f(b)) = h(1) = b$. 故得 $h \circ f = \mathrm{id}_X$.

Theorem 5.3.9 可以幫我們不必用 one-to-one 的定義處理有關 one-to-one 的證明. 例如我們有以下的性質.

Proposition 5.3.11. 若 $f_1 : X \to Y$, $f_2 : Y \to Z$ 皆為 *one-to-one function,* 則 $f_2 \circ f_1 : X \to Z$ 亦為 *one-to-one.*

Proof. (方法一) 我們可以用 one-to-one 的定義處理. 假設 $x_1, x_2 \in X$ 符合 $f_2 \circ f_1(x_1) = f_2 \circ f_1(x_2)$. 也就是說 $f_2(f_1(x_1)) = f_2(f_1(x_2))$, 然而 $f_2 : Y \to Z$ 為 one-to-one, 因此知 $f_1(x_1) = f_1(x_2)$. 再由 $f_1 : X \to Y$ 為 one-to-one, 得證 $x_1 = x_2$

(方法二) 利用 Theorem 5.3.9, 要證明 $f_2 \circ f_1 : X \to Z$ 為 one-to-one, 我們僅要找到 $h : Z \to X$ 使得 $h \circ (f_2 \circ f_1) = \mathrm{id}_X$ 即可. 然而已知 $f_1 : X \to Y$, $f_2 : Y \to Z$ 皆為 one-to-one,

故由 Theorem 5.3.9 知存在 $h_1 : Y \to X$, $h_2 : Z \to Y$ 滿足 $h_1 \circ f_1 = \mathrm{id}_X$ 以及 $h_2 \circ f_2 = \mathrm{id}_Y$. 現令 $h = h_1 \circ h_2 : Z \to X$, 我們有 $h \circ (f_2 \circ f_1) = (h_1 \circ h_2) \circ (f_2 \circ f_1)$. 利用合成函數的結合律 (Proposition 5.1.6) 以及 Lemma 5.1.5, 我們有 $(h_1 \circ h_2) \circ (f_2 \circ f_1) = h_1 \circ (h_2 \circ f_2) \circ f_1 = h_1 \circ (\mathrm{id}_Y \circ f_1) = h_1 \circ f_1 = \mathrm{id}_X$. 得證 $h \circ (f_2 \circ f_1) = \mathrm{id}_X$. □

要注意 Proposition 5.3.11 的反向不一定成立, 也就是說 $f_2 \circ f_1$ 為 one-to-one 並不表示 f_1, f_2 皆為 one-to-one. 例如在 Example 5.3.10 中 $h : \{1,2,3\} \to \{a,b\}$ 定義為 $h(1) = b, h(2) = a, h(3) = a$, 不是 one-to-one. 但 $h \circ f = \mathrm{id}_{\{a,b\}}$ 為 one-to-one. 不過我們有以下之結果.

Corollary 5.3.12. 若 $f_1 : X \to Y$, $f_2 : Y \to Z$ 皆為 *function* 且 $f_2 \circ f_1 : X \to Z$ 為 *one-to-one,* 則 f_1 為 *one-to-one.*

Proof. 由 $f_2 \circ f_1 : X \to Z$ 為 one-to-one, 利用 Theorem 5.3.9 知存在 $h : Z \to X$ 滿足 $h \circ (f_2 \circ f_1) = \mathrm{id}_X$. 因此利用合成函數結合律得 $(h \circ f_2) \circ f_1 = \mathrm{id}_X$. 現令 $h_1 = h \circ f_2$, 我們有 $h_1 : Y \to X$ 且滿足 $h_1 \circ f_1 = (h \circ f_2) \circ f_1 = \mathrm{id}_X$. 所以再次利用 Theorem 5.3.9 得證 $f_1 : X \to Y$ 為 one-to-one. □

Question 5.9. 試利用 *one-to-one* 的定義證明 *Corollary 5.3.12.*

要注意 Corollary 5.3.12 的反向也不一定成立, 也就是說單僅假設 f_1 為 one-to-one 並不能保證 $f_2 \circ f_1$ 為 one-to-one.

Question 5.10. 考慮 $X = \{a,b\}$, $Y = \{1,2,3\}$, 試找到例子 $f_1 : X \to Y$, $f_2 : Y \to X$ 為 *functions* 其中 f_1 為 *one-to-one,* 但是 $f_2 \circ f_1$ 不是 *one-to-one.*

最後我們來探討 one-to-one and onto 的函數. 這樣的函數一般我們稱之為 *bijective function* 或 *bijection.* 假設 $f : X \to Y$ 是 bijective, 由 f 為 onto 知存在 $g : Y \to X$ 滿足 $f \circ g = \mathrm{id}_Y$ (Theorem 5.3.3). 又由 f 為 one-to-one 知存在 $h : Y \to X$ 使得 $h \circ f = \mathrm{id}_X$ (Theorem 5.3.9). 因此由結合律以及 Lemma 5.1.5, 我們有

$$h = h \circ \mathrm{id}_Y = h \circ (f \circ g) = (h \circ f) \circ g = \mathrm{id}_X \circ g = g.$$

也就是說當 $f : X \to Y$ 為 bijective 時, 我們可以找到 $g : Y \to X$, 同時滿足 $f \circ g = \mathrm{id}_Y$ 且 $g \circ f = \mathrm{id}_X$. 事實上這樣的函數 g 是唯一的. 這是因為假設 $g : Y \to X$ 和 $g' : Y \to X$ 皆滿足 $f \circ g = f \circ g' = \mathrm{id}_Y$ 以及 $g \circ f = g' \circ f = \mathrm{id}_X$, 利用剛才相同的理由我們有

$$g' = g' \circ \mathrm{id}_Y = g' \circ (f \circ g) = (g' \circ f) \circ g = \mathrm{id}_X \circ g = g.$$

就因為這樣的函數 g 是唯一的且又和 f 有關, 我們給它一個特殊的符號 f^{-1}, 且稱之為 f 的 inverse. 由於這個原因, 我們也稱 bijective function 為 *invertible function.*

Question 5.11. 假設 $f : X \to Y$ 為 *injective.* 試證明若 $g : Y \to X$ 滿足 $f \circ g = \mathrm{id}_Y$, 則 $g = f^{-1}$. 且證明此時若 $h : Y \to X$ 滿足 $h \circ f = \mathrm{id}_X$, 則 $h = f^{-1}$.

要注意, 千萬不要將 f^{-1} 和 inverse image 搞混了. 一般的函數都可以定 inverse image, 也就是說不管 $f:X\to Y$ 是不是 bijective, 對任意 Y 的 subset C, inverse image $f^{-1}(C)$ 都是有定義的. 但對於 Y 元素 y, 就只有當 f 為 bijective 時 $f^{-1}(y)$ 才有定義. 所有要留意, 對任意 $y\in Y$, $f^{-1}(\{y\})$ 都有定義, 但 $f^{-1}(y)$ 就只有當 f 為 bijective 時才有定義.

當 $f:X\to Y$ 為 bijective 時, 我們可以利用 inverse image 將 $f^{-1}:Y\to X$ 寫下. 事實上, 對任意 $y\in Y$, 由 f 為 onto 以及 one-to-one, 我們有 $\#(f^{-1}(\{y\}))=1$. 也就是說 $f^{-1}(\{y\})$ 恰有一個元素. 因此若 $f^{-1}(\{y\})=\{x\}$, 則我們定義 $f^{-1}(y)=x$. 依此定義, 我們有 $f(x)=y$ 若且唯若 $f^{-1}(y)=x$, 因此確實得 $f\circ f^{-1}=\mathrm{id}_Y$ 且 $f^{-1}\circ f=\mathrm{id}_X$.

Example 5.3.13. 我們探討 Example 5.3.2 中的 bijective function 其 inverse 為何.

(A) 考慮函數 $g:\mathbb{R}\setminus\{3\}\to\mathbb{R}\setminus\{1\}$ 定義為 $g(x)=(x+1)/(x-3)$, $\forall x\in X$, 則 $g(x)$ 為 onto. 在 Example 5.2.2 中我們知道對任意 $y\in\mathbb{R}\setminus\{1\}$, $g^{-1}(\{y\})=\{(3y+1)/(y-1)\}$. 因此知 $g^{-1}:\mathbb{R}\setminus\{1\}\to\mathbb{R}\setminus\{3\}$ 定義為 $g^{-1}(x)=(3x+1)/(x-1)$, $\forall x\in\mathbb{R}\setminus\{1\}$.

(B) 考慮函數 $f:\mathbb{Z}\to\mathbb{N}\cup\{0\}$ 定義為

$$f(n)=\begin{cases}2n, & \text{if } n\geq 0;\\ -2n-1, & \text{if } n<0.\end{cases}$$

在 Example 5.3.2 中我們知若 $k\in\mathbb{N}\cup\{0\}$ 為偶數, 則 $f^{-1}(\{k\})=\{k/2\}$. 而若 $k\in\mathbb{N}\cup\{0\}$ 為奇數, 則 $f^{-1}(\{k\})=\{-(k+1)/2\}$. 因此得 $f^{-1}:\mathbb{N}\cup\{0\}\to\mathbb{Z}$ 定義為

$$f^{-1}(n)=\begin{cases}n/2, & \text{if } n \text{ is even};\\ -(n+1)/2, & \text{if } n \text{ is odd}.\end{cases}$$

我們知道當 $f:X\to Y$ 為 bijective 時, f 的 inverse 存在. 反之, 若 f 的 inverse 存在, 即存在 $f^{-1}:Y\to X$ 使得 $f\circ f^{-1}=\mathrm{id}_Y$ 且 $f^{-1}\circ f=\mathrm{id}_X$, 則由 Theorem 5.3.3 和 Theorem 5.3.9 知 f 為 bijective. 因此我們有以下之結果.

Theorem 5.3.14. 假設 $f:X\to Y$ 為 *function*. 則 f 為 *bijection* 若且唯若存在 $f^{-1}:Y\to X$ 使得 $f\circ f^{-1}=\mathrm{id}_Y$ 且 $f^{-1}\circ f=\mathrm{id}_X$.

Question 5.12. 假設 $f:X\to Y$ 為 *bijective function*. 試證明 $f^{-1}:Y\to X$ 亦為 *bijective* 且 $(f^{-1})^{-1}=f$.

利用 Proposition 5.3.5 和 Proposition 5.3.11 我們馬上有以下的性質:

Proposition 5.3.15. 若 $f_1:X\to Y$, $f_2:Y\to Z$ 皆為 *bijective function*, 則 $f_2\circ f_1:X\to Z$ 亦為 *bijective function*. 且此時

$$(f_2\circ f_1)^{-1}=f_1^{-1}\circ f_2^{-1}.$$

Proof. 其實我們只要證明 $(f_2\circ f_1)\circ(f_1^{-1}\circ f_2^{-1})=\mathrm{id}_Z$ 以及 $(f_1^{-1}\circ f_2^{-1})\circ(f_2\circ f_1)=\mathrm{id}_X$. 再利用 Theorem 5.3.14 就可得 $f_2\circ f_1:X\to Z$ 為 bijective. 又因 inverse function 的唯一性, 也證得了 $(f_2\circ f_1)^{-1}=f_1^{-1}\circ f_2^{-1}$. 然而

$$(f_2\circ f_1)\circ(f_1^{-1}\circ f_2^{-1})=f_2\circ(f_1\circ f_1^{-1})\circ f_2^{-1}=(f_2\circ\mathrm{id}_Y)\circ f_2^{-1}=f_2\circ f_2^{-1}=\mathrm{id}_Z,$$

$$(f_1^{-1}\circ f_2^{-1})\circ(f_2\circ f_1)=f_1^{-1}\circ(f_2^{-1}\circ f_2)\circ f_1=f_1^{-1}\circ(\mathrm{id}_Y\circ f_1)=f_1^{-1}\circ f_1=\mathrm{id}_X.$$

得證本定理. □

Question 5.13. 假設 $f_1:X\to Y$, $f_2:Y\to Z$ 皆為 *function* 且 $f_2\circ f_1:X\to Z$ 為 *bijective.* 是否 $f_1:X\to Y$, $f_2:Y\to Z$ 皆為 *bijective?* 又若 f_1,f_2 其中有一個是 *bijective,* 則另一個是否為 *bijective?*

5.4. Equivalent Sets and Cardinal Number

當我們在計算一個集合裡元素的個數時, 其實是給了此集合和正整數的子集合之間的一個一對一且映成的函數關係. 例如假設集合 A 有 n 個元素, 當我們一個一個的數 A 的元素時, 事實上就給了一個 $\{1,\ldots,n\}$ 到 A 的 bijective function. 所以我們很自然的有以下的定義.

Definition 5.4.1. 假設 A,B 為 set, 若存在一個 bijection $f:A\to B$, 則稱 A is *equivalent* to B, 且用 $|A|=|B|$ 表示.

要注意當 A 為 finite set, 可以說 $|A|$ 就是指 A 的元素個數 $\#(A)$. 不過由於我們不只探討 A 為 finite set 情況, 所以我們用 $|A|$ 這樣的符號, 且稱之為 A 的 *cardinal number.* 因此我們可以說 A is equivalent to B 若且唯若 A 和 B 有一樣的 cardinal number.

Equivalent set 之間的關係事實上是一個 equivalence relation.

Proposition 5.4.2. 對於任意的 *sets* A,B,C, 我們有以下的性質.

(1) $|A|=|A|$.

(2) 若 $|A|=|B|$ 則 $|B|=|A|$.

(3) 若 $|A|=|B|$ 且 $|B|=|C|$, 則 $|A|=|C|$.

Proof. (1) 對任意的集合 A, 考慮 $\mathrm{id}_A:A\to A$. 很明顯的 id_A 為 bijective, 故得 $|A|=|A|$.

(2) 若 $|A|=|B|$, 表示存在 $f:A\to B$ 為 bijective. 故考慮 $f^{-1}:B\to A$, 亦為 bijective (參見 Question 5.12), 得證 $|B|=|A|$.

(3) 若 $|A|=|B|$ 且 $|B|=|C|$, 表示存在 $f:A\to B$, $g:B\to C$ 皆為 bijective, 故由 Proposition 5.3.15 知 $g\circ f:A\to C$ 亦為 bijective. 得證 $|A|=|C|$. □

以下, 為了方便起見, 對於任意正整數 n, 我們用 I_n 表示 1 到 n 之間所有的正整數所成的集合, 亦即 $I_1=\{1\}$, $I_2=\{1,2\}$,..., $I_n=\{1,\ldots,n\}$. 現若 A 是有 n 個元素的 finite set, 我們很容易知道 $|A|=|I_n|$. 因此若 A 和 B 皆有 n 個元素, 我們有 $|A|=|I_n|$ 以及 $|B|=|I_n|$, 因此由 Proposition 5.4.2 知 $|A|=|B|$.

另外若 A, B 皆為 finite set 但 A 的元素個數 n 不等於 B 的元素個數 m, 那麼有可能 $|A|=|B|$ 嗎? 我們可以先考慮 $|I_n|$ 和 $|I_m|$ 是否相等. 首先由於 $n\neq m$, 不失一般性, 我們假設 $m>n$. 現若 $|I_m|=|I_n|$, 表示存在 bijection $f:I_m\to I_n$. 然而由鴿籠原理 Theorem 2.2.3 (想像定義域的 I_m 表示有 m 隻鴿子, 對應域 I_n 表示 n 個籠子), 知 $f:I_m\to I_n$ 不可能為 one-to-one

(鴿子數大於籠子數, 所以一定有一個籠子住了多於 1 隻的鴿子), 此與 f 為 bijective 的假設相矛盾, 得證 $|I_n| \neq |I_m|$. 現若 $|A| = |B|$, 則由 $|A| = |I_n|$, $|B| = |I_m|$ 以及 Proposition 5.4.2 推得 $|I_n| = |I_m|$ 之矛盾, 故知 $|A| \neq |B|$.

到目前為止, 在 finite set 的情況, 我們知道 cardinal number 頗符合我們對集合元素個數的計數原則. 我們也可利用 cardinal number 來定義 infinite set. 也就是說, 因為有無窮多個元素的集合, 其元素無法一個一個數完, 所以對一個 nonempty set A, 如果對任意 $n \in \mathbb{N}$, 皆有 $|A| \neq |I_n|$, 我們稱 A 為 *infinite set*.

其實 cardinal number 還符合許多其他計數的原則, 例如若 $A \cap B = \emptyset$, $C \cap D = \emptyset$, 且 $|A| = |C|$, $|B| = |D|$, 則由計數的原則, 我們會預期 $|A \cup B| = |C \cup D|$. 事實上這是對的, 我們有以下的定理.

Lemma 5.4.3. *假設 I 為 index set, $\{A_i, i \in I\}$, $\{B_i, i \in I\}$ 分別為 A, B 的 partition. 若對所有 $i \in I$, 皆有 $|A_i| = |B_i|$, 則 $|A| = |B|$.*

Proof. 回顧一下, $\{A_i, i \in I\}$ 為 A 的 partition 表示 $A = \bigcup_{i \in I} A_i$ 且對於 $i, j \in I$, 若 $i \neq j$, 則 $A_i \cap A_j = \emptyset$. 現依假設, 對所有 $i \in I$, 皆有 $|A_i| = |B_i|$, 此即表示存在 $f_i : A_i \to B_i$ 為 bijective function. 我們想利用這些 f_i, 建構出一個 bijective function $f : A \to B$. 依此便得證 $|A| = |B|$.

定義 $f : A \to B$ 如下: 對於任意 $a \in A$, 由於 $\{A_i, i \in I\}$ 為 A 的 partition, 我們知有唯一的 $i \in I$ 使得 $a \in A_i$, 此時定義 $f(a) = f_i(a) \in B_i$. 由於 $\{A_i, i \in I\}$ 為 A 的 partition, 在 f 的定義中每一個 A 的元素皆有定義其映射規則且 $B_i \subseteq B$. 所以這確實定義出了一個從 A 到 B 的 function. 我們要證明 $f : A \to B$ 為 one-to-one and onto.

現對任意 $b \in B$, 由於 $\{B_i, i \in I\}$ 為 B 的 partition, 故存在唯一的 $i \in I$, 使得 $b \in B_i$. 又因為 $f_i : A_i \to B_i$ 為 onto, 故知存在 $a \in A_i$ 滿足 $f_i(a) = b$. 現依 f 的定義, 對於這個 b, 我們只要取此 $a \in A$, 因為 $a \in A_i$, 由 f 的定義得 $f(a) = f_i(a) = b$. 得證 $f : A \to B$ 為 onto.

現若 $a, a' \in A$ 滿足 $f(a) = f(a')$. 由 $f(a) \in B$, 知存在唯一的 $i \in I$ 使得 $f(a) = f(a') \in B_i$. 再由 f 的定義, 我們知若 $a \in A_j$, 則 $f(a) = f_j(a) \in B_j$. 因此由 $f(a) \in B_i \cap B_j$ 得 $i = j$, 亦即 $a \in A_i$. 同理我們有 $a' \in A_i$. 所以由 f 的定義我們有 $f(a) = f_i(a)$ 且 $f(a') = f_i(a')$. 因此由 $f(a) = f(a')$ 之假設得 $f_i(a) = f_i(a')$, 再由 f_i 為 one-to-one 得證 $a = a'$. 因此得證 f 為 one-to-one. □

既然 cardinal number 和集合的元素個數有關, 我們當然希望它能比較大小. 在 finite set 的情況, 我們都知道元素比較少的集合可以 one-to-one 的映射到元素比較多的集合. 因此我們有以下的定義.

Definition 5.4.4. 假設 A, B 為 set, 我們用 $|A| \leq |B|$ 表示存在一個 one-to-one function $f : A \to B$.

這個定義也很符合我們的直覺. 例如若 $A \subseteq B$, 則考慮 $f : A \to B$, 定義為 $f(a) = a$, $\forall a \in A$. 很容易驗證 f 為 one-to-one function, 所以在這情況之下我們有 $|A| \leq |B|$. 特別的,

當 $m,n \in \mathbb{N}$ 且 $m > n$, 則由於 $I_n \subseteq I_m$, 所以我們有 $|I_n| \leq |I_m|$. 而前面我們利用鴿籠原理知道不可能有 one-to-one function $f : I_m \to I_n$, 所以我們也知道 $|I_m| \leq |I_n|$ 不成立.

另外直覺上元素比較多的元素可以找到映成的函數對應到元素比較少的集合, 對 cardinal number 這也是對的. 我們有以下的結果.

Proposition 5.4.5. 假設 A,B 為 *set*. 則 $|A| \leq |B|$ 若且唯若存在 *onto function* $h : B \to A$.

Proof. ($\Rightarrow$) 由 $|A| \leq |B|$, 我們知存在一個 one-to-one function $: A \to B$. 由 Theorem 5.3.9 知存在 $h : B \to A$ 滿足 $h \circ f = \mathrm{id}_A$. 然而 $\mathrm{id}_A : A \to A$ 是 onto function, 故由 Corollary 5.3.6 知 $h : B \to A$ 為 onto.

($\Leftarrow$) 由 $h : B \to A$ 為 onto 知, 存在 $g : A \to B$ 滿足 $h \circ g = \mathrm{id}_A$ (Theorem 5.3.3). 故由 id_A 為 one-to-one 得知 $g : A \to B$ 為 one-to-one (Corollary 5.3.12). 因此得證 $|A| \leq |B|$. □

接下來我們要說明 Definition 5.4.4 定義出 cardinal number 之間的 partial order. (事實上它可定義出 cardinal number 之間的 total order, 不過這需用到 Axiom of Choice 而且我們之後也不會用到, 所以這裡略過不談.) 首先對於 reflexive 的性質, 對於任意的集合 A, 我們僅要考慮 $\mathrm{id}_A : A \to A$, 由於 id_A 是 one-to-one, 故得證 $|A| \leq |A|$. 至於 transitive 的性質, 若 $|A| \leq |B|$ 且 $|B| \leq |C|$, 則由存在 $f : A \to B$ 以及 $g : B \to C$ 皆為 one-to-one, 可得 $g \circ f : A \to C$ 為 one-to-one (Proposition 5.3.11). 故證得 $|A| \leq |C|$. 至於 anti-symmetric 性質, 就比較複雜, 這是所謂 Cantor–Schröder–Bernstein Theorem.

Theorem 5.4.6 (Cantor–Schröder–Bernstein)**.** 假設 A,B 為 *sets* 滿足 $|A| \leq |B|$ 且 $|B| \leq |A|$, 則 $|A| = |B|$.

Proof. 由假設 $|A| \leq |B|$ 知存在 $f : A \to B$ 為 one-to-one function. 又由 $|B| \leq |A|$, 知存在 $g : B \to A$ 為 one-to-one function. 我們要利用 f,g 得到 A,B 的 partition, 再利用 Lemma 5.4.3 得到 $|A| = |B|$.

首先對於任意 $a \in A$, 我們建構出一個由 $A \cup B$ 的元素所組成的數列. 其建構方式如下: 首先令第一項 $x_1 = a$, 考慮 inverse image $g^{-1}(\{a\})$. 由於 g 是 one-to-one, 我們知 $g^{-1}(\{a\})$ 最多僅有一個元素. 若 $g^{-1}(\{a\}) = \emptyset$, 則這個數列僅有 x_1 這個元素. 而若 $g^{-1}(\{a\}) = \{b\}$, 則令 $x_2 = b$. 由於 $b \in B$, 接著考慮 $f^{-1}(\{b\})$. 同樣的, 因為 f 為 one-to-one, 我們知 $f^{-1}(\{b\})$ 最多僅有一個元素. 若 $f^{-1}(\{b\}) = \emptyset$, 則這個數列僅有 x_1, x_2 兩個元素. 而若 $f^{-1}(\{b\}) = \{a'\}$, 則令 $x_3 = a'$. 又由於 $a' \in A$, 我們又可考慮 $g^{-1}(\{a'\})$, 然後依前面規則這樣一直下去. 令 $\langle a \rangle$ 表示利用這個規則由 a 所建構出的數列 (若對如何建構這樣的數列仍不清楚, 請參考底下 Example 5.4.7). 這樣由所有 $a \in A$ 而得的數列 $\langle a \rangle = x_1, x_2, \ldots$, 我們可以分成三類. 第一類是有奇數項的有限數列. 例如若 $a \in A$ 且 $g^{-1}(\{a\}) = \emptyset$, 此時 $\langle a \rangle$ 僅有一項, 故屬於這一類的數列. 第二類是有偶數項的有限數列. 例如 $a \in A$ 且 $g^{-1}(\{a\}) = \{b\}$ 但 $f^{-1}(\{b\}) = \emptyset$, 此時 $\langle a \rangle$ 有 a,b 兩項, 故屬於這一類的數列. 第三類是有無窮多項的數列, 也就是說 $a \in A$ 所建構的數列每一項的 inverse image 皆不是空集合. 現令

$$A_o = \{a \in A : \langle a \rangle \text{有奇數項}\}, \quad A_e = \{a \in A : \langle a \rangle \text{有偶數項}\}, \quad A_\infty = \{a \in A : \langle a \rangle \text{有無窮多項}\}.$$

由於每一個 $a \in A$, 都可依這個規則建構出一組唯一數列 $\langle a \rangle$, 因此 a 一定會是 A_o, A_e, A_∞ 其中之一的元素, 且任兩個不會有交集. 所以 A_o, A_e, A_∞ 是 A 的一個 partition.

要注意這樣做出的數列, 其奇數項一定是 A 中的元素, 而偶數項一定是 B 中的元素. 也就是說若 $\langle a \rangle = x_1, x_2, \ldots$, 則當 i 為奇數時 $x_i \in A$. 又此時因 $x_i \in f^{-1}(\{x_{i-1}\})$, 故有 $f(x_i) = x_{i-1}$. 而當 i 為偶數時 $x_i \in B$. 又此時因 $x_i \in g^{-1}(\{x_{i-1}\})$, 故有 $g(x_i) = x_{i-1}$.

同樣的對任意 $b \in B$, 我們也用相同規則做出一個由 b 起始的數列, 亦即 $y_1 = b$, 然後考慮 $f^{-1}(\{b\})$ 來決定下一項, 這樣一直下去. 令 $\langle b \rangle$ 表示 b 利用這個規則所建構出的數列. 同樣的, 我們得到 B 的一個 partition B_o, B_e, B_∞, 其中

$$B_o = \{b \in B : \langle b \rangle \text{有奇數項}\}, \quad B_e = \{b \in B : \langle b \rangle \text{有偶數項}\}, \quad B_\infty = \{b \in B : \langle b \rangle \text{有無窮多項}\}.$$

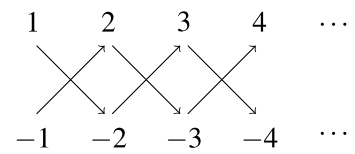
現考慮 restriction map $f|_{A_o} : A_o \to B$, 也就是對任意 $a \in A_o$, $f|_{A_o}(a) = f(a)$. 由於 f 為 one-to-one, 很自然的 $f|_{A_o}$ 仍為 one-to-one. 我們要說明 $f|_{A_o}$ 的 range $f|_{A_o}(A_o)$ 為 B_e. 對任意 $a \in A_o$, 我們有 $f|_{A_o}(a) = f(a) \in B$. 此時考慮 $f(a)$ 所建構的 sequence, 首項為 $y_1 = f(a)$, 而因 $f^{-1}(\{f(a)\}) = \{a\}$ (因 $f(a) \in \{f(a)\}$), 依 $\langle f(a) \rangle$ 的建構方式我們有 $y_2 = a$. 換言之, 數列 $\langle f(a) \rangle$ 前兩項為 $y_1 = f(a), y_2 = a$, 又由於下一項 (即第三項) y_3 完全由 $g^{-1}(\{a\})$ 所決定. 這和考慮 a 所建構的數列 $\langle a \rangle$ 第二項 x_2 是一樣的. 換言之, 數列 $\langle f(a) \rangle$ 只是將數列 $\langle a \rangle$ 的第一項之前再多加一項 $f(a)$ 而已. 現 $a \in A_o$, 表示 $\langle a \rangle$ 有奇數項, 所以 $\langle f(a) \rangle$ 會有偶數項, 故由 $f(a) \in B$ 知 $f(a) \in B_e$. 得證 $f|_{A_o}(A_o) \subseteq B_e$. 反之, 若 $b \in B_e$, 表示 b 所建構的數列 $\langle b \rangle$ 有偶數項. 因此 $\langle b \rangle$ 的第二項一定存在 (否則僅有一項, 造成矛盾). 所以由 $\langle b \rangle$ 的建構方法知 $f^{-1}(\{b\})$ 不是空集合, 也就是說存在 $a \in A$ 使得 $f(a) = b$. 事實上 a 就是 $\langle b \rangle$ 的第二項, 因此如前所述, $\langle a \rangle$ 是將 $\langle b \rangle = \langle f(a) \rangle$ 的第一項除去所得, 也就是說 $\langle a \rangle$ 有奇數項, 因此得 $a \in A_o$. 我們證得了對任意 $b \in B_e$, 皆存在 $a \in A_o$ 使得 $f(a) = f|_{A_o}(a) = b$. 因此知 $B_e \subseteq f|_{A_o}(A_o)$, 也得證了 $f|_{A_o}$ 的 range $f|_{A_o}(A_o)$ 就是 B_e. 換言之, $f|_{A_o}$ 可以視為是一個從 A_o 到 B_e 的 one-to-one and onto function. 我們證得了 $|A_o| = |B_e|$.

同理, 考慮 $g : B \to A$ 在 B_o 的 restriction $g|_{B_o} : B_o \to A$, 我們可以得到 $|B_o| = |A_e|$ (只是將上面的證明 f, g 互換即可). 最後我們考慮 g 在 B_∞ 上的 restriction $g|_{B_\infty}$ (也可考慮 f 在 A_∞ 上的 restriction). 此時 $g|_{B_\infty}$ 依然為 one-to-one. 而對於任意 $b \in B_\infty$, 我們考慮 $g(b)$ 所產生的數列 $\langle g(b) \rangle$. 由於 $g(b) \in A$, 而 $g^{-1}(\{g(b)\}) = \{b\}$, 故 $\langle g(b) \rangle$ 的第一項為 $g(b)$, 第二項為 b, 之後依序就是 $\langle b \rangle$ 的其他各項. 因此由 $b \in B_\infty$ 即 $\langle b \rangle$ 有無窮多項得 $\langle g(b) \rangle$ 亦有無窮多項. 得證 $g(b) \in A_\infty$, 亦即證得 $g|_{B_\infty}$ 的 range $g|_{B_\infty}(B_\infty)$ 包含於 A_∞. 反之, 若 $a \in A_\infty$, 表示 a 所建構的數列 $\langle a \rangle$ 有無窮多項. 因此 $\langle a \rangle$ 的第二項一定存在. 所以由 $\langle a \rangle$ 的建構方法知 $g^{-1}(\{a\})$ 不是空集合, 也就是說存在 $b \in B$ 使得 $g(b) = a$. 事實上 b 就是 $\langle a \rangle$ 的第二項, 因此如前所述, $\langle b \rangle$ 是將 $\langle a \rangle$ 的第一項除去所得, 也就是說 $\langle b \rangle$ 仍有無窮多項, 因此得 $b \in B_\infty$. 我們證得了對任意 $a \in A_\infty$, 皆存在 $b \in B_\infty$ 使得 $g(b) = g|_{B_\infty}(b) = a$. 因此知 $A_\infty \subseteq g|_{B_\infty}(B_\infty)$, 也得證了 $g|_{B_\infty}$ 的 range $g|_{B_\infty}(B_\infty)$ 就是 A_∞. 換言之, $g|_{B_\infty}$ 可以視為是一個從 B_∞ 到 A_∞ 的 one-to-one and onto function. 我們證得了 $|B_\infty| = |A_\infty|$.

最後因 A_o, A_e, A_∞ 為 A 的 partition 以及 B_o, B_e, B_∞ 為 B 的 partition, 又因 $|A_o| = |B_e|$, $|A_e| = |B_o|$ 以及 $|A_\infty| = |B_\infty|$, 利用 Lemma 5.4.3 得證 $|A| = |B|$. $\square$

Question 5.14. *Theorem 5.4.6* 的證明中, $|A_e| = |B_o|$ 的證明為何是考慮 g 在 B_o 的 *restriction* 而不是考慮 f 在 A_e 的 *restriction*? 若考慮 f 在 A_e 的 *restriction* $f|_{A_e} : A_e \to B$, 其 *range* 為何? 又 $|A_\infty| = |B_\infty|$ 的證明可以考慮 f 在 A_∞ 上的 *restriction* $f|_{A_\infty} : A_\infty \to B$ 嗎?

Example 5.4.7. 考慮 $A = \{1,2,\ldots\}$ 為正整數所成的集合, $B = \{-1,-2,\ldots\}$ 為負整數所成的集合. 考慮 $f : A \to B$ 定義為 $f(a) = -1-a$, $\forall a \in A$ 以及 $g : B \to A$ 定義為 $g(b) = 1-b$, $\forall b \in B$. 我們利用這個例子說明 Theorem 5.4.6 中建構數列的方法. 首先我們用以下圖示來表示這兩個函數的映射關係:



注意上圖中由上往下的映射是 f, 而由下往上的是 g.

現考慮 $3 \in A$, 由 $g^{-1}(\{3\}) = \{-2\}$, $f^{-1}(\{-2\}) = \{1\}$ 以及 $g^{-1}(\{1\}) = \emptyset$, 我們知道利用 3 所建構的數列 $\langle 3 \rangle$ 為 $3,-2,1$. 因為此數列有 3 項, 所以知 $3 \in A_o$. 同理, 由上圖很快看出利用 4 所建構的數列 $\langle 4 \rangle$ 為 $4,-3,2,-1$, 得 $4 \in A_e$. 很快的我們可以歸納出, 當 $a \in A$ 為奇數時 $a \in A_o$, 而當 $a \in A$ 為偶數時 $a \in A_e$. 也因此知 $A_\infty = \emptyset$. 事實上此時 A_o, A_e 就是 A 的一個 partition (恰好就是奇數與偶數的 partition).

而對於 $-3 \in B$, 由 $f^{-1}(\{-3\}) = \{2\}$, $g^{-1}(\{2\}) = \{-1\}$ 以及 $f^{-1}(\{-1\}) = \emptyset$, 我們知道利用 -3 所建構的數列 $\langle -3 \rangle$ 為 $-3,2,-1$. 因為此數列有 3 項, 所以知 $-3 \in B_o$. 同理, 由上圖很快看出利用 -4 所建構的數列 $\langle -4 \rangle$ 為 $-4,3,-2,1$, 得 $-4 \in B_e$. 很快的我們可以歸納出, 當 $b \in B$ 為奇數時 $b \in B_o$, 而當 $b \in B$ 為偶數時 $b \in B_e$. 也因此知 $B_\infty = \emptyset$. 事實上此時 B_o, B_e 就是 B 的一個 partition.

接著我們看 f 確實一對一的將 A_o 映成至 B_e (英文稱之為 one-to-one correspondence). 首先當 $a \in A_o$ 表示 a 為正奇數, 利用 $f(a) = -(1+a)$ 知 $f(a)$ 為負偶數, 即 $f(a) \in B_e$. 因此 f 確實一對一將 A_o 映射至 B_e. 而對於 $b \in B_e$, 我們知 b 為負偶數. 今考慮 $a = -b-1$, 我們有 $a > 0$ (因 $b \leq -2$) 且 a 為奇數, 即 $a \in A_o$. 將 $a = -b-1 \in A_o$ 代入 f 得 $f(a) = -(1+a) = b$. 故知 f 確實一對一將 A_o 映成至 B_e. 注意 f 無法將 A_e 映成至 B_o. 主要原因是 B_o 中有可能有元素其 inverse image 是空集合. 例如這裡我們有 $-1 \in B_o$ 且 $f^{-1}(\{-1\}) = \emptyset$. 所以這裡我們是用 g 來得到 B_o 至 A_e 之間的 one-to-one correspondence. 事實上對任意 $b \in B_o$, 我們有 b 為負奇數, 因此 $g(b) = 1-b$ 為正偶數, 即 $g(b) \in A_e$. 反之, 對任意 $a \in A_e$, 我們有 $b = 1-a < 0$ (因 $a \geq 2$) 且為奇數. 此時將 $b = 1-a \in B_o$ 代入 g, 得 $g(b) = 1-b = 1-(1-a) = a$, 故得證 g 確實一對一將 B_o 映成至 A_e.

Question 5.15. 試利用 *Example 5.4.7* 中的 f 和 g 寫下一個 A 到 B 的 *bijective function* $h : A \to B$ 滿足 $h|_{A_o} = f|_{A_o}$.

最後, 我們想定義 cardinal number 之間的 "strict order". 當 A, B 為 sets, 滿足 $|A| \leq |B|$ 且 $|A| \neq |B|$ 時, 我們就用 $|A| < |B|$ 來表示. 前面已知當 m,n 為正整數且 $m > n$ 時, 我們有

$|I_n| \leq |I_m|$ 且 $|I_n| \neq |I_m|$, 所以我們有 $|I_n| < |I_m|$. 另外當 A 為 infinite set, 依定義對任意 $n \in \mathbb{N}$ 皆有 $|I_n| \leq |A|$ 但 $|I_n| \neq |A|$, 因此我們有 $|I_n| < A$. 現若 B 為 finite set, 我們知存在 $n \in \mathbb{N}$ 使得 $|B| = |I_n|$, 所以得 $|B| < |A|$. 因此這樣的 strict order 頗符合我們直觀對集合計數的想法.

5.5. Countable and Uncountable Sets

一個 finite set 的 cardinal number, 我們知道就是其元素的個數, 但對於 infinite set, 其 cardinal number 並不是只有一種 "無窮大" 而已. 事實上會有無窮多個 infinite set 它們的 cardinal number 都相異, 也就是說利用 cardinal number, 我們有可以把 "無窮大" 區分成好幾種. 不過在本講義中, 我們不會深入的討論這個問題. 我們僅談論最簡單的區分方法, 即分成 countable set 和 uncountable set 兩種.

Definition 5.5.1. 假如 S 是一個 set 滿足 $|S| \leq |\mathbb{N}|$, 則稱 S 為 *countable* set. 反之則稱為 *uncountable* set.

Question 5.16. 假設 S, T 為 *sets* 且 $|S| \leq |T|$. 若 T 為 *countable,* 是否可知 S 為 *countable?*

簡單來說, 若存在一個 one-to-one function $f : S \to \mathbb{N}$, 則 S 就是一個 countable set. 由此定義我們知道若 S 是 finite set, 那一定是 countable. 不過有可能一個 infinite set 也是 countable, 例如 $\mathbb{N}$ 本身, 或是如 $2\mathbb{N}$ (正的偶數所成的集合), 都是 infinite set 且為 countable. 不過 uncountable set 就一定會是 infinite set. 所以當一個 infinite set 是 countable 時, 我們會將之稱為 *countably infinite* 特別將這種 infinite set 和 uncountable set 區分出來.

首先我們要關注的是, 在 finite set 和 $\mathbb{N}$ 之間是否還有其他的 cardinal number? 答案是否定的. 也就是說對於 infinite set 來說 $|\mathbb{N}|$ 就是最小的 cardinal number. 現假設 S 是一個 infinite set 且 $|S| \leq |\mathbb{N}|$. 依定義存在一個 one-to-one function $f : S \to \mathbb{N}$. 考慮 $T = f(S)$, 我們可以將 f 視為是一個由 S 到 T 的 one-to-one 且 onto 的函數, 所以 $|S| = |T|$. 由於 T 是 $\mathbb{N}$ 的 infinite subset, 所以我們若能證明此時 $|T| = |\mathbb{N}|$, 那麼就有 $|S| = |T| = |\mathbb{N}|$, 也就是說所有的 countably infinite set 其 cardinal number 皆等於 $|\mathbb{N}|$.

Lemma 5.5.2. 假設 $T \subseteq \mathbb{N}$ 且為 *infinite set,* 則 $|T| = |\mathbb{N}|$.

Proof. 由於 $T \subseteq \mathbb{N}$, 我們知 $|T| \leq |\mathbb{N}|$. 現只要證明存在 $f : \mathbb{N} \to T$ 為 one-to-one function, 則由此知 $|\mathbb{N}| \leq |T|$, 故由 Theorem 5.4.6 (Cantor–Schröder–Bernstein) 得證 $|T| = |\mathbb{N}|$.

這裡我們要利用 $\mathbb{N}$ 在一般的 order $\leq$ 之下是一個 well-ordered set (Well-ordering Principle) 來證明. 回顧一下, 這表示每一個 $\mathbb{N}$ 的 nonempty subset 都有 least element (或 minimum element). 若 S 為 nonempty subset of $\mathbb{N}$, 我們用 $\min(S)$ 表示 S 的 least element, 也就是說, 若 $a = \min(S)$, 表示 $a \in S$ 且對於任意 S 中的元素 s, 若 $s \neq a$, 則 $a < s$.

首先令 $f(1) = \min(T)$, 我們有 $f(1) \in T$. 如何定 $f(2)$ 呢? 很自然的我們考慮 $T_2 = T \setminus \{f(1)\}$, 然後令 $f(2) = \min(T_2)$. 注意此時 $T_2 \neq \emptyset$, 否則會有 $T \subseteq \{f(1)\}$ 此和 T 為 infinite set 之前題相矛盾, 所以我們得到 $f(2) \in T$. 如此一直下去, 我們令 $T_{n+1} = T \setminus \{f(1), \ldots, f(n)\}$ 且令 $f(n+1) = \min(T_{n+1})$, 這樣 "大致" 就定義出一個由 $\mathbb{N}$ 到 T 的 function $f : \mathbb{N} \to T$ 了.

當然我們要說明這樣定出的真的是一個 “well-defined” function, 且要證明其為 one-to-one. 首先檢查 well-defined. 也就是我們要說明對於任意 $n \in \mathbb{N}$ 皆存在唯一的 $t_n \in T$ 滿足 $f(n) = t_n$. 由於當初我們定義 f 的方法是類似用歸納法的手法定義的, 所以這裡的證明很自然的是要用到數學歸納法. 我們要用數學歸納法證明對所有 $n \in \mathbb{N}$, 皆存在唯一的 $t_n \in T$ 滿足 $f(n) = t_n$. 當 $k = 1$ 時, 我們知 $t_1 = \min(T)$ 是 T 中唯一滿足 $t_1 \leq t, \forall t \in T$ 的元素, 所以確實 $f(1) = t_1 \in T$ 而且是唯一的. 現假設對於任意 $k = 1, \ldots, n$ 皆有唯一的 $t_k \in T$ 使得 $f(k) = t_k$. 現考慮 $f(n+1)$, 依定義 $T_{n+1} = T \setminus \{f(1), \ldots, f(n)\} = T \setminus \{t_1, \ldots, t_n\}$ 且 $f(n+1) = \min(T_{n+1})$. 由於 T 為 infinite set, 我們知 $T_{n+1} \neq \emptyset$, 否則會造成 $T \subseteq \{t_1, \ldots, t_n\}$ 此與 T 為 infinite set 相矛盾. 又因前面歸納法假設 T_{n+1} 是一個可以被唯一確定的集合 (因 $t_1, \ldots, t_n$ 皆已被唯一確定), 所以利用 $\mathbb{N}$ 的 well-ordering principle, 我們知 $t_{n+1} = \min(T_{n+1})$ 必屬於 T 且唯一. 因此由 Strong Mathematical Induction (Corollary 2.3.6) 得證對所有 $n \in \mathbb{N}$, 皆存在唯一的 $t_n \in T$ 滿足 $f(n) = t_n$.

我們已知 $f : \mathbb{N} \to T$ 是一個 function, 接著要證明 $f : \mathbb{N} \to T$ 是 one-to-one. 也就是說任取 $n_1, n_2 \in \mathbb{N}$ 且 $n_1 \neq n_2$, 我們要說明 $f(n_1) \neq f(n_2)$. 不失一般性, 我們假設 $n_1 < n_2$. 此時由於 $T_{n_2} = T \setminus \{f(1), \ldots, f(n_1), \ldots, f(n_2 - 1)\}$, 亦即 $f(n_1) \notin T_{n_2}$, 當然由 $f(n_2) = \min(T_{n_2}) \in T_{n_2}$ 得知 $f(n_2) \neq f(n_1)$. 得證 $f : \mathbb{N} \to T$ 是 one-to-one. $\square$

如前所述, 由 Lemma 5.5.2 我們證得了以下定理.

Theorem 5.5.3. 假設 S 為一個 *set.* 則 S 為 *countably infinite* 若且唯若 $|S| = |\mathbb{N}|$.

Question 5.17. 假設 S 為 *infinite set.* 試證明 S 為 *uncountable* 若且唯若 $|S| \neq |\mathbb{N}|$.

依照 countable set 的定義, 我們知道任意一個 countable set 的 subset 仍為 countable. 這是因為若 S 為 countable, 則依定義我們有 $|S| \leq |\mathbb{N}|$, 也因此若 $S' \subseteq S$, 則由 $|S'| \leq |S|$ 以及 $|S| \leq |\mathbb{N}|$, 可得 $|S'| \leq |\mathbb{N}|$. 不過要注意的是比 countable set 大的集合, 仍有可能是 countable. 我們有以下的情形.

Proposition 5.5.4. 有限多個 *countable set* 的聯集仍為 *countable set.* 亦即若 $S_1, \ldots, S_n$ 為 *countable set,* 則 $\bigcup_{i=1}^{n} S_i$ 仍為 *countable set.*

Proof. 我們用數學歸納法證明. 首先證明若 S_1, S_2 為 countable, 則 $S_1 \cup S_2$ 為 countable.

依定義 S_1, S_2 是 countable, 故存在 $f_1 : S_1 \to \mathbb{N}$ 以及 $f_2 : S_2 \to \mathbb{N}$ 皆為 one-to-one functions. 現定義新的 function $f : S_1 \cup S_2 \to \mathbb{N}$, 其定義為

$$f(s) = \begin{cases} 2f_1(s), & \text{if } s \in S_1; \\ 2f_2(s) + 1, & \text{if } s \in S_2 \setminus S_1. \end{cases}$$

很清楚的, f 是 well-defined function, 因為 $S_1 \cup S_2 = S_1 \cup (S_2 \setminus S_1)$ 以及 $S_1 \cap (S_2 \setminus S_1) = \emptyset$, 因此對任意 $s \in S_1 \cup S_2$, s 一定會在 S_1 和 $S_2 \setminus S_1$ 其中一個, 且不會同時皆在其中. 而當 $s \in S_1$, $f_1(s)$ 的取值是明確確定的 (因 $f_1 : S_1 \to \mathbb{N}$ 是一個 function), 所以此時 $f(s)$ 取值 $2f_1(s)$ 亦確定. 同理當 $s \in S_2 \setminus S_1$, 因 $s \in S_2$, $f_2(s)$ 的取值是明確確定的, 所以此時 $f(s)$ 取值 $2f_2(s) + 1$ 亦確定. 我們剩下要證明 $f : S_1 \cup S_2 \to \mathbb{N}$ 是 one-to-one, 也就是要證明任取 $s, t \in S_1 \cup S_2$ 其

中 $s \neq t$, 皆會有 $f(s) \neq f(t)$. 我們分成兩種 cases. 第一種情形就是 s,t 同屬於 S_1 或是同屬於 $S_2 \setminus S_1$. 此時我們分別有 $f(s) = 2f_1(s) \neq 2f_1(t) = f(t)$ (因 f_1 為 one-to-one), 以及 $f(s) = 2f_2(s)+1 \neq 2f_2(t)+1 = f(t)$ (因 f_2 為 one-to-one). 第二種情況是 $s \in S_1$ 但 $t \in S_2 \setminus S_1$ 或是 $t \in S_1$ 但 $s \in S_2 \setminus S_1$. 此時由於 $f(s), f(t)$ 必為一奇一偶, 故亦得 $f(s) \neq f(t)$. 我們證得了 $f : S_1 \cup S_2 \to \mathbb{N}$ 為 one-to-one, 故證得 $S_1 \cup S_2$ 為 countable.

接著我們要用數學歸納法證明, 對於任意 $n \in \mathbb{N}$ 且 $n \geq 2$, 若 $S_1, \ldots, S_n$ 為 countable set, 則 $\bigcup_{i=1}^{n} S_i$ 仍為 countable set. 我們考慮 $n = k+1$ 的情形. 利用歸納假設, $S_1, \ldots, S_k$ 為 countable set, 所以 $\bigcup_{i=1}^{k} S_i$ 為 countable set. 現又若 S_{k+1} 為 countable set, 利用上面證過 $k = 2$ 的情形, 我們知 $(\bigcup_{i=1}^{k} S_i) \cup S_{k+1}$ 為 countable set. 故由 $\bigcup_{i=1}^{k+1} S_i = (\bigcup_{i=1}^{k} S_i) \cup S_{k+1}$ 得證 $\bigcup_{i=1}^{k+1} S_i$ 為 countable set. □

Proposition 5.5.4 有許多應用, 最簡單的一種就是證得所有整數所成的集合為 countable. 這是因為所有的整數可視為正整數, 負整數以及 0 所成的集合的聯集. 然而負整數所成的集合和正整數所成的集合 $\mathbb{N}$ 有一個一對一的對應關係 (即 $-n \mapsto n$), 所以是 countable. 而 $\{0\}$ 是 finite set, 亦為 countable, 因此得證

Corollary 5.5.5. *$\mathbb{Z}$ is countable.*

其實有理數所成的集合 $\mathbb{Q}$ 也是 countable, 我們首先看一個簡單的定理.

Lemma 5.5.6. *The Cartesian product $\mathbb{N} \times \mathbb{N}$ is countable.*

Proof. 回顧一下 $\mathbb{N} \times \mathbb{N}$ 的元素為任意的數對 (n_1, n_2), 其中 $n_1, n_2 \in \mathbb{N}$, 而且 $(n_1, n_2) = (n_1', n_2')$ 若且唯若 $n_1 = n_1'$ 且 $n_2 = n_2'$. 現考慮函數 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, 其定義為

$$f(n_1, n_2) = 2^{n_1} 3^{n_2}, \quad \forall n_1, n_2 \in \mathbb{N}.$$

很容易知道 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 為 function, 我們僅要檢驗 f 為 one-to-one. 現若 $(n_1, n_2) \neq (n_1', n_2')$, 由整數的唯一分解性質我們知

$$f(n_1, n_2) = 2^{n_1} 3^{n_2} \neq 2^{n_1'} 3^{n_2'} = f(n_1', n_2').$$

得證 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 為 one-to-one, 故 $\mathbb{N} \times \mathbb{N}$ 是 countable. □

Lemma 5.5.6 證明了 $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$, 不過我們很容易理解 $\mathbb{N} \times \mathbb{N}$ 為 infinite set, 所以 $\mathbb{N} \times \mathbb{N}$ 為 countably infinite, 亦即 $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Proposition 5.5.6, 最常見的應用是可以推得有限多個 countable set 的 Cartesian product 仍為 countable.

Proposition 5.5.7. 若 *$S_1, \ldots, S_n$ 為 countable set,* 則 *$S_1 \times S_2 \times \cdots \times S_n$ 仍為 countable set.*

Proof. 首先我們證明 $S_1 \times S_2$ 為 countable. 利用 S_1, S_2 為 countable 的假設, 我們知道存在 $f_1 : S \to \mathbb{N}$, $f_2 : S_2 \to \mathbb{N}$ 皆為 one-to-one function. 現考慮 $f : S_1 \times S_2 \to \mathbb{N} \times \mathbb{N}$ 其定義為

$$f(s_1, s_2) = (f_1(s_1), f_2(s_2)), \quad \forall s_1 \in S_1, s_2 \in S_2.$$

很容易知道 $f: S_1 \times S_2 \to \mathbb{N}\times\mathbb{N}$ 為 function, 我們僅要檢驗 f 為 one-to-one. 對於任意 $(s_1,s_2),(s_1',s_2') \in S_1\times S_2$ 且 $(s_1,s_2)\neq(s_1',s_2')$, 我們知 $s_1\neq s_1'$ 或 $s_2\neq s_2'$. 現若 $s_1\neq s_1'$, 由 $f_1: S_1\to\mathbb{N}$ 為 one-to-one, 知 $f_1(s_1)\neq f_1(s_1')$, 故此時

$$f(s_1,s_2) = (f_1(s_1),f_2(s_2)) \neq (f_1(s_1'),f_2(s_2')) = f(s_1',s_2').$$

同理當 $s_2\neq s_2'$ 時, 亦可得 $f(s_1,s_2)\neq f(s_1',s_2')$. 得證 $f: S_1\times S_2\to\mathbb{N}\times\mathbb{N}$ 為 one-to-one. 亦即 $|S_1\times S_2|\leq|\mathbb{N}\times\mathbb{N}|=|\mathbb{N}|$, 因此證明了 $S_1\times S_2$ 為 countable.

至於當 $S_1,\ldots,S_n$ 為 countable set, 則利用 $S_1\times S_2\times\cdots\times S_n=(S_1\times S_2\times\cdots\times S_{n-1})\times S_n$ 以及數學歸納法可證明 $S_1\times S_2\times\cdots\times S_n$ 為 countable set, 我們就不多做說明了. □

我們可以利用 Proposition 5.5.7 證明有理數所成的集合 $\mathbb{Q}$ 為 countable. 這是因為有理數除了 0 以外都可以唯一寫成 a/b 其中 $a\in\mathbb{Z}$, $b\in\mathbb{N}$ 且 $\gcd(a,b)=1$ 的形式 (我們稱此為最簡分數). 所以考慮 $f:\mathbb{Q}\to\mathbb{Z}\times\mathbb{N}$, 定義為 $f(0)=(0,1)$; 而當 $q\in\mathbb{Q}$, $q\neq0$ 且 a/b 為 q 的最簡分數時, 則定義 $f(q)=(a,b)$. 由非零有理數最簡分數表法的唯一性, 我們知 $f:\mathbb{Q}\to\mathbb{Z}\times\mathbb{N}$ 為 function. 而若 $q\neq q'$, 當 q,q' 其中有一個為 0 時, 我們知道另一個不為 0, 故其最簡分數不可能寫成 0/1, 因此此時 $f(q)\neq f(q')$. 而若 q,q' 皆不為 0 時, 設其最簡分數分別為 $q=a/b, q'=a'/b'$. 由於 $a/b\neq a'/b'$, 我們知 $f(q)=(a,b)\neq(a',b')=f(q')$. 因此知 $f:\mathbb{Q}\to\mathbb{Z}\times\mathbb{N}$ 為 one-to-one, 得證 $|\mathbb{Q}|\leq|\mathbb{Z}\times\mathbb{N}|$. 由 $\mathbb{Z}$ 為 countable 以及 Proposition 5.5.7 知 $\mathbb{Z}\times\mathbb{N}$ 為 countable, 又 $\mathbb{Z}\times\mathbb{N}$ 為 infinite set, 故 $|\mathbb{Z}\times\mathbb{N}|=|\mathbb{N}|$. 因此 $|\mathbb{Q}|\leq|\mathbb{N}|$, 得證以下的定理.

Corollary 5.5.8. $\mathbb{Q}$ *is countable.*

利用 Lemma 5.5.6, 我們也可將 Proposition 5.5.4 推廣到更一般情況.

Proposition 5.5.9. 若對任意 $i\in\mathbb{N}$, S_i 皆為 *countable set,* 則 $\bigcup_{i=1}^{\infty}S_i$ 仍為 *countable set.*

Proof. 依假設, 對任意 $i\in\mathbb{N}$, 皆存在 $f_i: S_i\to\mathbb{N}$ 為 one-to-one function. 現考慮 $f:\bigcup_{i=1}^{\infty}S_i\to\mathbb{N}\times\mathbb{N}$ 定義為, 對任意 $s\in\bigcup_{i=1}^{\infty}S_i$, 若 i 為最小的正整數滿足 $s\in S_i$, 則令 $f(s)=(i,f_i(s))$. 很容易驗證 $f:\bigcup_{i=1}^{\infty}S_i\to\mathbb{N}\times\mathbb{N}$ 為 function. 現對任意 $s,s'\in\bigcup_{i=1}^{\infty}S_i$, 假設 i,i' 分別為最小的正整數滿足 $s\in S_i, s'\in S_{i'}$. 若 $i\neq i'$, 自然得 $f(s)=(i,f_i(s))\neq(i',f_{i'}(s'))=f(s')$. 而若 $i=i'$, 則因 $s,s'\in S_i$ 且 $f_i: S_i\to\mathbb{N}$ 為 one-to-one, 我們有 $f_i(s)\neq f_i(s')$, 故 $f(s)=(i,f_i(s))\neq(i,f_i(s'))=f(s')$. 得證 $f:\bigcup_{i=1}^{\infty}S_i\to\mathbb{N}\times\mathbb{N}$ 為 one-to-one, 即 $|\bigcup_{i=1}^{\infty}S_i|\leq|\mathbb{N}\times\mathbb{N}|=|\mathbb{N}|$. 證得 $\bigcup_{i=1}^{\infty}S_i$ 為 countable set. □

目前我們處理的都是 countable sets, 是否存在著 uncountable set 呢? 答案是肯定的. 例如 Proposition 5.5.7 中 Cartesian product 並不能如聯集一樣推廣到無窮多個集合的情形. 也就是說有可能 $S_1,\ldots,S_n,\ldots$ 為 countable 但是 $S_1\times\cdots\times S_n\times\cdots$ 為 uncountable. 還有 $\mathbb{N}$ 的 power set $\mathscr{P}(\mathbb{N})$ 也是 uncountable. 回顧一下, 一個集合 A 的 power set $\mathscr{P}(A)$, 即為 A 的所有 subsets 所成的集合. 首先我們有以下的結果.

Theorem 5.5.10. 假設 A 為一個 *set,* $\mathscr{P}(A)$ 為 A 的 *power set,* 則 $|A|<|\mathscr{P}(A)|$.

Proof. 考慮函數 $\iota : A \to \mathscr{P}(A)$ 定義為 $\iota(a) = \{a\}, \forall a \in A$. 我們很容易看出 $\iota : A \to \mathscr{P}(A)$ 為 one-to-one function, 因此得 $|A| \leq |\mathscr{P}(A)|$. 所以要證明 $|A| < |\mathscr{P}(A)|$, 就是要證明 $|A| \neq |\mathscr{P}(A)|$.

我們要證明對於任何 function $f : A \to \mathscr{P}(A)$ 都不可能是 onto. 若證得這個結果就表示不可能存在 function $f : A \to \mathscr{P}(A)$ 是 one-to-one 且 onto 的, 因此得證 $|A| \neq |\mathscr{P}(A)|$. 現對於任何 function $f : A \to \mathscr{P}(A)$, 考慮 A 的一個子集合 $S = \{s \in A \mid s \notin f(s)\}$. 注意 S 是有可能為空集合, 不過不管怎樣我們都有 $S \in \mathscr{P}(A)$. 我們要說明不可能存在一個元素 $a \in A$ 使得 $f(a) = S$. 也就是說 S 不會在函數 $f : A \to \mathscr{P}(A)$ 的 image 中, 因此得到 $f : A \to \mathscr{P}(A)$ 不可能是 onto. 利用反證法, 假設 $a \in A$ 使得 $f(a) = S$. 我們檢查是否 $a \in S$. 假設 $a \in S$, 表示 $a \in f(a)$ (因 $f(a) = S$), 但依 S 的定義若 $a \in S$ 表示 $a \notin f(a)$, 因此得到矛盾, 故知 $a \notin S$. 不過由 $a \notin S$, 得 $a \notin f(a)$, 又依 S 的定義得 $a \in S$ 之矛盾. 也就是說若存在 $a \in A$ 使得 $f(a) = S$, 會造成 $a \in S$ 和 $a \notin S$ 都不可能發生的矛盾 (注意即使 S 為空集合, 這依然不成立). 所以證得 $S \in \mathscr{P}(A)$ 不在 $f : A \to \mathscr{P}(A)$ 的 image 中, 得證 $f : A \to \mathscr{P}(A)$ 不是 onto. □

Question 5.18. 令 $A = \{1,2,3\}$, 考慮 $f : A \to \mathscr{P}(A)$ 定義為

$$f(1) = \{1,2\}, \quad f(2) = \{1,3\}, \quad f(3) = \{2\}.$$

令 $S = \{s \in A \mid s \notin f(s)\}$. 試寫下 S 為何? 並檢驗 S 不在 $f : A \to \mathscr{P}(A)$ 的 *image* 中.

Corollary 5.5.11. $\mathbb{N}$ 的 *power set* $\mathscr{P}(\mathbb{N})$ 是 *uncountable.*

Proof. 由 Theorem 5.5.10 知 $|\mathbb{N}| < |\mathscr{P}(\mathbb{N})|$, 所以因 cardinal number 之間是一個 partial order, $|\mathscr{P}(\mathbb{N})| \leq |\mathbb{N}|$ 不可能成立. 得證 $\mathscr{P}(\mathbb{N})$ 為 uncountable. □

我們知道有限多個 countable set 的 Cartesian product 仍為 countable (Proposition 5.5.7), 不過這對於無窮多個 countable set 的 Cartesian product 並不成立. 事實上我們有以下之結果.

Proposition 5.5.12. 對於任意 $n \in \mathbb{N}$, 令 $S_n = \{0,1\}$. 則無窮的 *Cartesian product*

$$S_1 \times S_2 \times \cdots \times S_n \times \cdots$$

為 *uncountable.*

Proof. 為了符號方便起見, 令 $\mathscr{S} = S_1 \times S_2 \times \cdots \times S_n \times \cdots$. 我們要證明 $|\mathscr{S}| = |\mathscr{P}(\mathbb{N})|$ (亦即存在一對一且映成的函數 $f : \mathscr{S} \to \mathscr{P}(\mathbb{N})$), 因此由 Corollary 5.5.11 得證 $\mathscr{S}$ 為 uncountable.

對於任意 $s = (s_1, s_2, \ldots, s_n, \ldots) \in \mathscr{S}$, 我們令 $f(s) = \{n \in \mathbb{N} \mid s_n = 1\} \in \mathscr{P}(\mathbb{N})$. 依此定義我們得 $f : \mathscr{S} \to \mathscr{P}(\mathbb{N})$ 是一個 (well-defined) function. 我們要證明 f 是一對一且映成的函數. 首先若 $s = (s_1, \ldots, s_n, \ldots) \neq s' = (s'_1, \ldots, s'_n, \ldots)$, 表示存在 $n \in \mathbb{N}$ 使得 $s_n \neq s'_n$. 也就是說如果 $s_n = 1$, 則 $s'_n = 0$, 此時依定義, 我們有 $n \in f(s)$ 但 $n \notin f(s')$, 因此得 $f(s) \neq f(s')$. 同理若 $s_n = 0$, 亦可得 $f(s) \neq f(s')$, 得證 f 為一對一. 至於映成部分, 給定 $S \in \mathscr{P}(\mathbb{N})$ (亦即 $S \subseteq \mathbb{N}$), 若對於任意 $n \in \mathbb{N}$, 若 $n \in S$, 則令 $s_n = 1$; 反之, 則令 $s_n = 0$. 此時考慮 $s = (s_1, \ldots, s_n, \ldots) \in \mathscr{S}$, 可得 $f(s) = S$, 因此得證 f 為映成. □

接下來我們用 Proposition 5.5.12 來證明實數所成的集合 $\mathbb{R}$ 是 uncountable.

Proposition 5.5.13. $\mathbb{R}$ *is uncountable.*

Proof. 考慮 S 為所有整數部分為 0, 而小數點後各位數是 0 或 1 所組成的實數所成的集合. 例如 $0.1011010\overline{0}$ 和 $0.101101\overline{1}$ 都是 S 中的元素. 要注意我們將 S 中的元素都寫成無限小數 (若是有限小數, 我們將之寫成最後皆為 0 的無限循環小數. 例如 $0.101101 = 0.1011010\overline{0}$). 也要注意 S 中不只有無限循環小數, 也有無限不循環小數 (其實無限不循環小數佔了大多數). 由 Proposition 5.5.12 我們知道 S 是 uncountable, 所以利用 $S \subseteq \mathbb{R}$, 可得 $|S| \leq |\mathbb{R}|$, 因此 $|\mathbb{R}| \leq |\mathbb{N}|$ 不可能成立 (否則會造成 $|S| \leq |\mathbb{N}|$ 的矛盾). 得證 $\mathbb{R}$ 為 uncountable. □

Theorem 5.5.10 的證明方法是數學家 Cantor 所提出的. 他利用類似的想法也證出實數所成的集合 $\mathbb{R}$ 為 uncountable, 這個證明方法就留做習題.

最後我們要強調, 一般來說要探討一個 infinite set S 是 countable 或是 uncountable 並不容易. 首先我們必須先用一些資訊來判斷它為 countable 或是 uncountable. 若判斷是 countable, 就必須證明它, 也就是找到一個 $S \to \mathbb{N}$ 的 one-to-one function. 而若判斷為 uncountable, 要證明其為 uncountable, 一般都是用反證法, 也就是說假設其為 countable, 然後得到矛盾. 其中最常用的方法就是如前面的證明, 說明所有 $S \to \mathbb{N}$ 的 function 都不會是 onto.