數學導論

李華介

國立台灣師範大學數學系

前言

大學所學的數學和高中階段所學習數學在層次上有所不同. 簡單來說大學數學著重於理論的基礎. 本講義希望介紹同學如何讀懂定理, 理解證明甚而自己寫下證明. 我們將介紹邏輯 (Logic), 集合 (Set) 以及函數 (Function) 的概念. 要注意, 我們不是要介紹邏輯學以及集合論. 這裡談論的僅著重於將來大家學習數學所需要的邏輯及集合的概念.

本講義雖然主要以中文撰寫, 不過當涉及定義或專有名詞時, 為免翻譯的困擾將以英文取代. 因此將以中英夾雜較不傳統的方式顯現, 若有不便請見諒.

本講義編寫費時, 編寫完後並未經過嚴謹的校對. 疏漏在所難免, 雖不至於有理論性上嚴重的錯誤, 但讀者仍應注意不宜概括全收. 若發現錯誤, 歡迎提出寶貴的意見.

Chapter 1

Basic Logic

其實學習數學就像學習新的語言. 一些名詞的定義就像 "單字" 一樣, 而邏輯 *logic* 就好比是將這些單字組合成一個句子所需的 "文法". 一般同學在學習邏輯時, 會不自覺地將一些邏輯規則以背誦的方式記憶, 這會造成以後學習上許多的障礙. 其實這些規則應該是潛意識內的直覺, 這樣學習數學才能通行無阻.

邏輯學可以是非常抽象的，不只與數學關係密切，也與資訊科學以及哲學發展有著密切的關係。不過這裡，我們僅介紹很基本的與數學論證相關的邏輯。

1.1. Connectives

在數學中能明確知道對或錯的論述我們稱之為 *statement*. 例如 $2>0$ 是一個 statement, $3<2$ 也是一個 statement 但 $x>0$ 就不是一個 statement (除非我們知道 x 是什麼). 注意一個 statement 只能是對或錯其中之一，不能是半對半錯或是有時候對有時候錯。所以我們稱一個 statement 的 *truth value* 為 T 當這個 statement 為對的 (即 true)；反之則以 F 表示，即此 statement 為錯的 (false).

舉例來說 "今天天氣很熱" 不是一個 statement. 為什麼呢？因為大家對熱的標準不一，除非我們明確定義 "很熱" 的標準（例如超過幾度）。再例如 "天空打雷會下雨" 這個論述我們覺得半對半錯，有時候會下有時候不會下，所以它也不是一個 statement. 但如果改為 "天空打雷一定會下雨"，那它便是一個 truth value 為 F 的 statement. 這裡要注意，在數學上的敘述，我們往往會省略 "一定" 這個字眼，所以數學上當一個論述有時候對有時候錯，我們會認定它是**錯**的。例如 "由 $x^2>4$, 可得 $x>2$" 雖沒有加上 "一定" 的字眼，但我們認定它是 truce value 為 F 的 statement.

數個 statements 可以組合成一個 statement, 連接這些 statements 的就是所謂 *connectives*. 我們要探討經由 connectives 連結成的 statement 其對或錯的情形.

1.1.1. And. 首先介紹的便是 "and" 這一個 connective. 這一個 connective 應該是大家最容易理解的一個. 若 P 和 Q 皆為 statement, 我們用 $P\wedge Q$ 表示「P and Q」這一個

statement (邏輯上稱為 the "conjunction" of P, Q). $P\wedge Q$ 什麼時候是對的什麼時候是錯的呢? 按照字面的意義 "and" 就是 "且" 的意思, 就如同習慣用語當 P 而且 Q 都是對時我們才能說 $P\wedge Q$ 是對的, 而只要 P 和 Q 其中有一個是錯的, 我們便會說 $P\wedge Q$ 是錯的. 例如「$2>0$ and $2<7$」是對的, 而「$2>0$ 且 $2>7$」便是錯的.

我們可利用所謂的真值表 *truth table* 來表示用 connectives 連結兩個 statements 後其對錯的情況. 前面提過，我們用 T 表示對 (true), F 表示錯 (false). 所以我們有以下的 truth table.

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

基本上 Truth table 就是將 P,Q 每個可能對錯的情況列出, 然後由 P,Q 所對應的情況, 寫下它們連接後的對錯情況. 例如上表第三橫排為 P 為 T, Q 為 F 故寫下 $P\wedge Q$ 為 F.

很容易發現不管 P,Q 的對錯情況如何 $P\wedge Q$ 和 $Q\wedge P$ 的對錯情形皆相同. 也就是說 $P\wedge Q$ 和 $Q\wedge P$ 在邏輯上是相等的. 我們稱它們為 *logically equivalent.*

對於 logically equivalent, 我們需再釐清一下說法. 當 P,Q 是確定的 statements 時, $P\wedge Q$ 和 $Q\wedge P$ 也會是確定的 statements (也就是說它們對錯的情況已經固定), 所以此時說 $P\wedge Q$ 和 $Q\wedge P$ 是 logically equivalent 並不是很恰當. 事實上我們是將 P,Q 看成變數一樣, 它們可以用任意的 statement 取代, 所以此時 $P\wedge Q$ 的對錯會因為 P,Q 的不同而有所不同, 故此時說 $P\wedge Q$ 是 statement 也不恰當. 在本講義，當 P,Q 是可變動的情況之下, 我們便稱它們利用 connectives 連結起來的結果為 "statement form". 兩個 statement forms 在所有情況之下其 truth tables 皆相同，我們便稱它們為 logical equivalent. 所以我們應該說成 $P\wedge Q$ 和 $Q\wedge P$ 這兩個 statement forms 為 logically equivalent. 不過為了方便起見我們常常會省略 statement form 且用 "$\sim$" 來表示兩個 statement forms 為 logically equivalent, 例如我們有 $(P\wedge Q)\sim(Q\wedge P)$.

Truth table 可以幫助我們判斷許多 statements 用 connectives 連接起來後其對錯的情況, 例如 $(P\wedge Q)\wedge R$ 的 truth table 為

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

Question 1.1. 你會列出 $P\wedge(Q\wedge R)$ 的 *truth table* 嗎?

注意 $(P\wedge Q)\wedge R$ 和 $P\wedge(Q\wedge R)$ 在定義上是不一樣的. $(P\wedge Q)\wedge R$ 是先探討 $P\wedge Q$ 的對錯再和 R 連結; 而 $P\wedge(Q\wedge R)$ 是先探討 $Q\wedge R$ 的對錯再和 P 連結. 不過從它們的 truth table 我們知道 $((P\wedge Q)\wedge R)\sim(P\wedge(Q\wedge R))$. 既然 $(P\wedge Q)\wedge R$ 和 $(P\wedge(Q\wedge R))$ 在邏輯上意義相同，以後我們就可以不必括弧直接用 $P\wedge Q\wedge R$ 表示。

1.1.2. Or. 當 P 和 Q 皆為 statement, 我們用 $P\vee Q$ 表示「P or Q」這一個 statement (邏輯上稱為 the "disjunction" of P, Q). 按照字面的意義 "or" 就是 "或" 的意思. 不過在我們日常用語中 "或" 有兩種用法: 例如在速食店點套餐, 飲料可以選擇「可樂或果汁」. 這裡的 "或" 表示二者擇一, 你不可以兩個都選 (這種 "or" 稱為 *exclusive or*); 而遊樂園購票時規定「六歲以下或身高 105 公分以下」才可購買兒童票. 這裡的 "或" 表示六歲以下和身高 105 公分以下二者有一個成立就可以, 並不排除六歲以下且身高 105 公分以下同時成立的情況 (這種 "or" 稱為 *inclusive or*). 在數學邏輯上, "or" 指的是後面那種 inclusive or 的說法, 也就是說當 P 和 Q 其中有一個是對的 $P\vee Q$ 便是對的 (並不排除 P 和 Q 皆為對的情況). 換言之, 只有當 P 和 Q 都是錯的, $P\vee Q$ 才是錯的.

例如, 「$4<5$ or $4<3$」這個 statement 是對的, 因為 $4<5$ 是對的. 而「$4>5$ or $4>6$」這個 statement 便是錯的, 因為二者皆不成立. 要注意「$4<5$ or $4>3$」這個 statement 依然是對的, 雖然你會認為用 and 比較好, 不過在邏輯上它依然是對的, 千萬別搞錯.

我們有以下關於 $P\vee Q$ 的 truth table.

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

Question 1.2. $P\vee Q$ 和 $Q\vee P$ 是否為 *logically equivalent statement forms?* $(P\vee Q)\vee R$ 和 $P\vee(Q\vee R)$ 是否為 *logically equivalent statement forms?* $P\vee Q\vee R$ 有意義嗎*?*

既然 and, or 皆為 connectives, 我們可以將其混合使用. 例如當 P,Q,R 為 statements 我們可以考慮如 $(P\wedge Q)\vee R$, $(P\vee Q)\wedge R$,... 等形式的 statements. 如何判定它們的對錯呢? 例如 $(P\wedge Q)\vee R$ 是對的就必須 $(P\wedge Q)$ 或 R 其中一個是對的. 所以只要是 R 是對的, $(P\wedge Q)\vee R$ 就一定對, 而若 R 是錯的那就必須 P,Q 皆對, $(P\wedge Q)\vee R$ 才會是對的. 注意, 千萬不要誤以為 $(P\wedge Q)\vee R$ 和 $P\wedge(Q\vee R)$ 這兩個 statement forms 是 logically equivalent. 很顯然的 $P\wedge(Q\vee R)$ 是對的就必須 P 和 $Q\vee R$ 皆為對的. 例如當 R 是對的時, 不管 Q 為對或錯 $Q\vee R$ 皆為對, 但還必須 P 為對才可得到 $P\wedge(Q\vee R)$ 是對的. 這和只要是 R 是對的, $(P\wedge Q)\vee R$ 就一定對不同, 所以 $(P\wedge Q)\vee R$ 和 $P\wedge(Q\vee R)$ 不是 logically equivalent statement forms. 當然我們也可利用以下的 truth table 判定它們不是 logically equivalent.

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

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

另一方面, 考慮 $(P\vee R)\wedge(Q\vee R)$ 的 truth table,

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

不難發現

$$((P\wedge Q)\vee R)\sim((P\vee R)\wedge(Q\vee R)).$$

同樣的我們可利用 truth table 檢查 $(P\vee Q)\wedge R$ 和 $(P\wedge R)\vee(Q\wedge R)$ 亦為 logically equivalent statement forms.

我們可以利用 truth table 檢驗一些 statement forms 是否為 logically equivalent. 在一些有關 logic 的書也會有一些 logical equivalences 的列表讓大家檢驗. 不過這些都是為了讓大家熟悉這些 connectives 以及 truth table 的運用. 除了以後和論證有關的 logical equivalences 我們需要注意且會特別提醒大家要熟悉, 一般來說大家不必花時間於記憶這些 logical equivalences.

最後提醒一下和 "or" 有關的數學符號 $\geq$ 和 $\leq$. 在數學上 $x\geq y$ 表示 $x>y$ or $x=y$, 所以 $4\geq 3$ 這一個 statement 按照 or 的邏輯規則是對的. 同理 $4\leq 5$ 是對的. 當然了 $4\leq 4$ 也是對的。

1.1.3. If - Then. 這是一個數學定理裡常見的 connective 但又是許多同學不甚了解而經常誤解的 connective, 請務必弄清楚. 當 P 和 Q 皆為 statement, 我們用 $P\Rightarrow Q$ 表示「if P then Q」這一個 statement, 即「若 P 則 Q」的意思 (邏輯上稱為 the "conditional" of P, Q). 要注意 $P\Rightarrow Q$ 在數學上的意涵與純粹邏輯上有所不同. 主要的區別是, 數學上 $P\Rightarrow Q$ 較常表達的是 P,Q 之間的因果關係 (也就是說 P,Q 通常是相關的). 這裡 P,Q 通常不是 statement, 而是如「x 為實數」這樣的 "性質". 而邏輯上將 $\Rightarrow$ 看成是一個 connective 可以連結任意的 P,Q (即使它們毫無關係). 例如數學上我們有 "if $x>3$ then $x^2>9$" 這樣的 statement (注意 $x>3$ 和 $x^2>9$ 皆不是 statement, 但用 if-then 連結後, 它是一個 statement). $x>3$ 和 $x^2>9$ 是有關係的. 而在邏輯上在我們有 "if $3>2$ then 2 is even" 這樣的 statement (即使

$3>2$ 和 2 為偶數是沒有關係的). 在探討 $P\Rightarrow Q$ 在邏輯上對錯的情況之前, 我們先強調它在數學理論以及推理與論證上的意涵.

在數學上, 當我們說「if P then Q」意即 "當 P 成立時, Q 一定成立". (注意: 為了區別性質與 statement, 我們說一個性質成不成立, 而不用對錯這樣的說法.) 這裡要強調的是, 當我們說 if P then Q 表示我們僅知道如果 P 成立, 則可確定 Q 一定成立. 如果 P 不成立, 是無法知道 Q 是否成立. 所以在數學上要論述「if P then Q」我們只關心當 P 成立時, Q 是否也成立這樣的 "因果關係", 不必在意 P 不成立的情況. 這一點和邏輯上的「if P then Q」看成 P,Q 這兩個 statements 的 connective 相當的不同, 因為既然要讓「if P then Q」成為一個 statement, 就必須明定 P,Q 在任何的對錯情況時 $P\Rightarrow Q$ 的對錯情況. 另外我們也要強調 $P\Rightarrow Q$ 和 $Q\Rightarrow P$ 在數學上是完全不一樣的. 有許多同學會誤以為可由 $P\Rightarrow Q$ 是對的，推得 $Q\Rightarrow P$ 是對的。這個是不正確的, 事實上 $P\Rightarrow Q$ 僅表示由 P 成立可推得 Q 成立, 但不表示當 P 不成立時不會使得 Q 成立. 例如我們知道 if $x>3$ then $x^2\geq 9$, 但這並不表示當 $x\leq 3$ 時不會使得 $x^2\geq 9$. 也就是說我們無法由 Q 成立得到 P 成立. 總而言之, $P\Rightarrow Q$ 是對的，並不能確保 $Q\Rightarrow P$ 是對的. 等一下我們定義「if P then Q」在邏輯上的對錯情況時, 我們也會發現 $P\Rightarrow Q$ 和 $Q\Rightarrow P$ 在邏輯上也不是 equivalent statement forms.

Question 1.3. 如果我們知道 P 成立則 Q 成立. 那麼當我們發現 Q 不成立時, 是否可以斷言 P 也不成立*?*

現在我們來看在邏輯上如何定義 $P\Rightarrow Q$ 的對錯情況. 從前面數學上的意義來看, 當 P,Q 為 statements 時, 如果 P 是對的且 Q 是對的, 那麼並未違背 $P\Rightarrow Q$ 的說法, 所以在這種情況我們定 $P\Rightarrow Q$ 為對. 但若 P 是對的而 Q 是錯的, 那麼就違背 $P\Rightarrow Q$ 的說法, 所以在這種情況我們定 $P\Rightarrow Q$ 為錯. 但是若 P 是錯的, 如何定 $P\Rightarrow Q$ 的對錯呢? 由於 $P\Rightarrow Q$ 並未論及當 P 是錯時, Q 會如何, 所以當 P 是錯時, 不管 Q 的對錯都未違背前述 $P\Rightarrow Q$ 的說法, 所以此時我們都定義 $P\Rightarrow Q$ 為對. 例如 $2>3$ 是錯的且 $2^2>9$ 是錯的, 但這並不違背前面所提 if $x>3$ then $x^2>9$ 這一個對的 statement. 另一方面, $-4>3$ 是錯的, 但 $(-4)^2>9$ 是對的, 也不違背前述 if $x>3$ then $x^2>9$ 這一個對的 statement. 簡單來說, 在數學上 $x>3\Rightarrow x^2>9$ 這個對的敘述, 由邏輯上 $P\Rightarrow Q$ 的定義便可以解釋成將 x 代入任何的實數, $x>3\Rightarrow x^2>9$ 都是對的. 總而言之, 關於 $P\Rightarrow Q$ 我們有以下的 truth table.

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

Question 1.4. 試利用 *truth table* 判斷 $Q\Rightarrow P$ 和 $P\Rightarrow Q$ 是否為 *logically equivalent statement forms?* $(P\Rightarrow Q)\Rightarrow R$ 是否和 $P\Rightarrow(Q\Rightarrow R)$ 為 *logically equivalent statement forms?* $P\Rightarrow Q\Rightarrow R$ 是否有意義*?*

或許有些同學對 $P\Rightarrow Q$ 的對錯情況為何這麼定義仍有疑慮, 在我們介紹 "if and only if" 這個 connective 時會再進一步說明.

最後我們補充 $P \Rightarrow Q$ 在英文上的幾種說法. 除了「if P then Q」外, 還有

- 「Q if P」
- 「P implies Q」
- 「P is sufficient for Q」(意即 P 成立足以使得 Q 成立)
- 「Q is necessary for P」(意即需要 Q 成立才有可能使得 P 成立)
- 「P only if Q」(意即只有當 Q 成立時 P 才可能成立)
- 「Q whenever P」(意即每當 P 成立時 Q 都會成立)

1.1.4. If and Only If. 當我們將 $P \Rightarrow Q$ 和 $Q \Rightarrow P$ 用 and 連接時, 即 $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$, 我們稱之為 "$P$ if and only if Q", 用 $P \Leftrightarrow Q$ 來表示 (邏輯上稱為 the "biconditional" of P, Q).

$P \Leftrightarrow Q$ 其實是由很多 connectives 組合起來的 (以後我們會知道 $P \Rightarrow Q$ 也是如此), 所以我們可以將它看成是 connectives 組合起來的 "縮寫"。會特別用縮寫，當然是它會經常被用到，特別是在數學上，所以我們依然先探討在數學上 $P \Leftrightarrow Q$ 的意義。依定義在數學上我們說 $P \Leftrightarrow Q$ 表示 $P \Rightarrow Q$ 且 $Q \Rightarrow P$. 也就是說若 P 成立則 Q 一定成立, 另一方面若 Q 成立則 P 一定成立. 因此 P,Q 有一個成立時另一個一定也成立. 換言之, $P \Leftrightarrow Q$ 表示若 Q 成立則 P 一定成立而且只有當 Q 成立時才會使得 P 成立 (否則會造成 P 成立但 Q 不成立的情況). 這也是在中文我們將 $P \Leftrightarrow Q$ 稱之為 "P 若且唯若 Q" (或 P 當且僅當 Q) 的原因.

現在我們來看在邏輯上 $P \Leftrightarrow Q$ 的對錯情況. 從前面數學上的意義來看, 我們可以知道 $P \Leftrightarrow Q$ 表示 P 對則 Q 且 Q 對則 P 對. 不會有一對一錯的情況. 因此若 P,Q 有一個錯則另一個一定也是錯的. 也就是說在邏輯上 $P \Leftrightarrow Q$ 是對的表示 P 和 Q 必須是同時是對的或同時是錯的. 所以我們有以下關於關於 $P \Leftrightarrow Q$ 的 truth table.

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

Question 1.5. 試利用 $P \Rightarrow Q$ 以及 $Q \Rightarrow P$ 的 *truth table* 寫下 $P \Leftrightarrow Q$ 的 *truth table.*

Question 1.6. $P \Leftrightarrow Q$ 和 $Q \Leftrightarrow P$ 是否為 *logically equivalent?* $(P \Leftrightarrow Q) \Leftrightarrow R$ 和 $P \Leftrightarrow (Q \Leftrightarrow R)$ 是否為 *logically equivalent?* $P \Leftrightarrow Q \Leftrightarrow R$ 是否有意義*?*

邏輯上 $P \Leftrightarrow Q$ 對錯的情況, 和數學上的情況很一致, 大家應該覺得較為自然. 現在我們利用 $P \Leftrightarrow Q$ 來解釋為何邏輯上只要 P 是錯的, 不管 Q 的對錯, $P \Rightarrow Q$ 都定義為對的. 當然了, 因為 $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ 就是 $P \Leftrightarrow Q$, 所以當 P,Q 皆為錯時, 為了讓 $P \Leftrightarrow Q$ 為對, 我們當然要定義 $P \Rightarrow Q$ 和 $Q \Rightarrow P$ 為對. 所以當 P,Q 皆為錯時, 我們定義 $P \Rightarrow Q$ 為對. 至於 P 錯 Q 對的情形, 由於此時 $Q \Rightarrow P$ 為錯, 不管 $P \Rightarrow Q$ 怎麼定都可以使得 $P \Leftrightarrow Q$ 為錯. 然而此時若 $P \Rightarrow Q$ 定為錯, 將會導致 $P \Rightarrow Q$, $Q \Rightarrow P$ 和 $P \Leftrightarrow Q$ 皆有相同的 truth table (亦即

equivalent), 此和前述數學上不能由 $P \Rightarrow Q$ 推得 $Q \Rightarrow P$ 相違背, 所以當 P 錯 Q 對的情形, 我們依然定義 $P \Rightarrow Q$ 為對.

最後我們補充 $P \Leftrightarrow Q$ 在英文上的幾種說法. 除了「P if and only if Q」外, 還有

- 「P iff Q」
- 「P is equivalent to Q」
- 「P is necessary and sufficient for Q」

1.2. Logical Equivalence and Tautology

前面我們介紹過 logical equivalence 的概念. 我們可以利用 logical equivalence 的一些規則推導出更多的 logical equivalences. 這樣的好處是不必每次都用 Truth table 來探討有關 logical equivalence 的問題.

第一個常見的 logical equivalence 的使用規則是: 我們可以將 logically equivalent 的兩個 statement forms 其中同一個變數用其他的 statement form 取代, 仍可得到 logical equivalence. 例如已知 $(P \wedge Q) \sim (Q \wedge P)$, 我們可將 P 用 $P \Rightarrow Q$ 取代得

$$((P \Rightarrow Q) \wedge Q) \sim (Q \wedge (P \Rightarrow Q)).$$

這個規則的原因很簡單, 因為既然 logically equivalent 的 statement forms 有相同的 truth table, 我們將其中某個變數任意變換當然最後所得新的 statement forms 仍會有相同的 truth table. 同樣的道理, 我們可以將其中某個變數用兩個 (或好幾個) logically equivalent 的 statement forms 取代, 最後所得新的 statement forms 仍為 logically equivalent. 例如已知 $(P \wedge Q) \sim (Q \wedge P)$ 以及 $(R \vee S) \sim (S \vee R)$, 所以可以將 $(P \wedge Q) \sim (Q \wedge P)$ 左邊的 P 用 $R \vee S$ 取代, 而右邊的 P 用 $S \vee R$ 取代得

$$((R \vee S) \wedge Q) \sim (Q \wedge (S \vee R)).$$

還有一個常用的規則是, 如果兩個 statement forms A, B 是 logically equivalent 而 B 和另一個 statement form C 也是 logically equivalent, 那麼 A 和 C 也是 logically equivalent. 例如我們有 $((P \wedge Q) \vee R) \sim ((Q \wedge P) \vee R)$, 也有 $((Q \wedge P) \vee R) \sim (R \vee (Q \wedge P))$, 故可得

$$((P \wedge Q) \vee R) \sim (R \vee (Q \wedge P)).$$

這個規則會成立的原因仍然由 truth table 的全等可以得到.

利用這些規則我們可以不必藉由 truth table 很容易推得一些 statement forms 為 logically equivalent. 簡單來說我們可以將 logically equivalent 如“等號”一樣運用. 我們前面學過的 logical equivalences, 例如 $\wedge$ 的交換性和 $\vee$ 的交換性, 即

$$(P \wedge Q) \sim (Q \wedge P), \quad (P \vee Q) \sim (Q \vee P) \tag{1.1}$$

以及 $\wedge$ 的結合性和 $\vee$ 的結合性, 即

$$((P \wedge Q) \wedge R) \sim (P \wedge (Q \wedge R)), \quad ((P \vee Q) \vee R) \sim (P \vee (Q \vee R)) \tag{1.2}$$

還有 $\wedge,\vee$ 之間的分配性質, 即

$$((P\wedge Q)\vee R)\sim((P\vee R)\wedge(Q\vee R)),\quad ((P\vee Q)\wedge R)\sim((P\wedge R)\vee(Q\wedge R)) \tag{1.3}$$

都是常用來幫助我們推導許多 logical equivalences 的工具.

Example 1.2.1. 考慮 $(P\wedge Q)\vee(P\vee Q)$ 這一個 statement form. 利用式子 (1.3) 中的 $((P\wedge Q)\vee R)\sim((P\vee R)\wedge(Q\vee R))$, 將 R 用 $P\vee Q$ 取代, 我們有

$$(P\wedge Q)\vee(P\vee Q)\sim((P\vee(P\vee Q))\wedge(Q\vee(P\vee Q))). \tag{1.4}$$

再由 $(P\vee(P\vee Q))\sim((P\vee P)\vee Q)$ 以及 $(Q\vee(P\vee Q))\sim(Q\vee(Q\vee P))\sim((Q\vee Q)\vee P)$ 得

$$((P\vee(P\vee Q))\wedge(Q\vee(P\vee Q))\sim(((P\vee P)\vee Q)\wedge((Q\vee Q)\vee P)). \tag{1.5}$$

很容易檢查 $(P\vee P)\sim P$ 以及 $(Q\wedge Q)\sim Q$, 故知

$$(((P\vee P)\vee Q)\wedge((Q\vee Q)\vee P))\sim((P\vee Q)\wedge(Q\vee P))\sim(P\vee Q). \tag{1.6}$$

最後連結式子 (1.4), (1.5), (1.6), 得

$$((P\wedge Q)\vee(P\vee Q))\sim(P\vee Q).$$

當一個 statement form 其 truth table 在任何情況之下皆為對, 我們稱此 statement form 為 *tautology*. 意即它是重複多餘的. 例如 $P\Leftrightarrow P$ 的 truth table 為

P	$P\Leftrightarrow P$
T	T
F	T

故 $P\Leftrightarrow P$ 為 tautology.

Question 1.7. $P\Rightarrow P$ 是否為 *tautology?* $P\Rightarrow(P\Rightarrow P)$ 是否為 *tautology?*

Tautology 雖然有重複多餘的意思, 但它在邏輯上仍是有意思的. 它可以幫我們用另一種方法來詮釋 logically equivalent. 當兩個 statement forms A,B 為 logically equivalent 時, 因為 A,B 的對錯情況一致, 我們有 $A\Leftrightarrow B$ 恆為對. 意即 $A\Leftrightarrow B$ 為 tautology. 反之, 當 $A\Leftrightarrow B$ 為 tautology 時, 由於 A,B 的對錯情形一致, 它們有相同的 truth table. 意即 $A\sim B$. 我們有以下的性質.

Proposition 1.2.2. 假設 A,B 為兩個 *statement forms.* 則 A 和 B 為 *logically equivalent* 等同於 $A\Leftrightarrow B$ 為 *tautology.*

其實在前面的說明中, 我們先假設 $A\sim B$ 成立推得 $A\Leftrightarrow B$ 為 tautology (即若 $A\sim B$ 則 $A\Leftrightarrow B$ 為 tautology), 後又由 $A\Leftrightarrow B$ 為 tautology 推得 $A\sim B$. 故 Proposition 1.2.2 可以說成 $A\sim B$ 若且唯若 $A\Leftrightarrow B$ 為 tautology.

Question 1.8. 假設 A,B 為兩個 *statement forms.* 若 $A\sim B$ 可否推得 $A\Rightarrow B$ 為 *tautology?* 若 $A\Rightarrow B$ 為 *tautology* 可否推得 $A\sim B$*?*

Question 1.9. 假設 A,B,C 為 *statement forms.* 若 $A \Leftrightarrow B$ 和 $B \Leftrightarrow C$ 皆為 *tautology,* 是否可推得 $A \Leftrightarrow C$ 為 *tautology?*

和 tautology 相反的是所謂的 *contradiction* (矛盾). 它指的是一個 statement form 在任何情況之下皆為錯的. 關於 contradiction, 我們會在下一節介紹 "not" 之後再探討.

Question 1.10. 假設 A,B 為 *statement forms.*

(1) 若 A 為 *tautology,* 試說明 $(A \wedge B) \sim B$ 並說明 $A \vee B$ 為 *tautology.*

(2) 若 A 為 *contradiction,* 試說明 $(A \vee B) \sim B$ 並說明 $A \wedge B$ 為 *contradiction.*

1.3. Not and Contradiction

我們介紹 "not" 以及和 not 有關的 equivalences. 本節內容分量比前面幾節重, 而且許多情形很可能和你的直覺不同. 希望大家能好好熟習, 糾正錯誤的直覺, 而將正確觀念成為你的本能反應而不是盲目地記誦.

Not 有否定和相反的意思, 給定一個 statement P, 我們用 $\neg P$, 來表示 not P, 一般稱為 "非 P". 它的定義就是當 P 為對時, $\neg P$ 就為錯. 反之, 當 P 為錯時, $\neg P$ 就為對. 所以我們有以下 $\neg P$ 的 truth table.

P	$\neg P$
T	F
F	T

.

利用這個定義, 我們馬上有

$$P \sim \neg(\neg P). \tag{1.7}$$

Not P 雖然定義簡單, 但是對於由許多 connectives 連結的 statement 取 not 之後, 其對錯狀況就較複雜了. 例如 $\neg(P \wedge Q)$, 或許很多人會誤以為是 $(\neg P) \wedge (\neg Q)$, 不過檢查一下 truth table 可得

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

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

很明顯看出, 在 P 對 Q 錯或 P 錯 Q 對時, $\neg(P \wedge Q)$ 和 $(\neg P) \wedge (\neg Q)$ 是不同的. 事實上, 利用 truth table, 我們可得

$$\neg(P \wedge Q) \sim (\neg P) \vee (\neg Q). \tag{1.8}$$

我們藉由大家熟知的數學例子來理解這個事實. 考慮 $0 \le x \le 1$, 這表示 $x \le 1$ and $x \ge 0$. 它的相反, 大家都知是 $x > 1$ or $x < 0$. 我們可以任取一個數 x 令 P 為 $x \le 1$ 這一個 statement, 而 Q 為 $x \ge 0$, 則 $\neg P$, $\neg Q$ 分別為 $x > 1$, $x < 0$. 也就是說 $0 \le x \le 1$ 可以用 $P \wedge Q$ 表示而 $x > 1$ or $x < 0$ 就是 $(\neg P) \vee (\neg Q)$. 由此可以看出 $\neg(P \wedge Q)$ 和 $(\neg P) \vee (\neg Q)$ 為 logically equivalent, 而不是 $(\neg P) \wedge (\neg Q)$ (否則會得到 $x > 1$ and $x < 0$ 這個矛盾).

我們可以用上一節有關於 statement form 的 logically equivalent 的規則來處理 not. 例如將式子 (1.8) 中的 P, Q 分別用 $\neg P$ 和 $\neg Q$ 取代, 可得

$$\neg((\neg P)\wedge(\neg Q)) \sim (\neg(\neg P))\vee(\neg(\neg Q)).$$

再利用 $\neg(\neg P) \sim P$, 得

$$\neg((\neg P)\wedge(\neg Q)) \sim (P\vee Q).$$

最後兩邊取 not, 得

$$\neg(P\vee Q) \sim (\neg P)\wedge(\neg Q). \tag{1.9}$$

例如考慮 $x\geq 0$ 的情形, 我們知它的相反為 $x<0$. 若令 P, Q 分別為 $x>0, x=0$, 則 $x\geq 0$ 即為 $P\vee Q$. 此時 $\neg P$ 為 $x\leq 0$, $\neg Q$ 為 $x\neq 0$. 而 $(\neg P)\wedge(\neg Q)$ 為 $x\leq 0$ and $x\neq 0$, 即為 $x<0$ 也就是 $x\geq 0$ 的相反.

式子 (1.7), (1.8), (1.9) 對於推導和 not 有關的 statement forms 之間的 logical equivalence 相當重要. 其中式子 (1.8), (1.9) 稱為 *DeMorgan's laws.*

接下來我們自然會問, 怎樣的 statement form 會和 $\neg(P\Rightarrow Q)$ logically equivalent 呢? 或許大家會認為是 $P\Rightarrow\neg Q$, 不過利用 truth table 檢查一下, 大家會發現在 P 是對的時 $P\Rightarrow Q$ 和 $P\Rightarrow\neg Q$ 確實對錯相反, 但是當 P 為錯時 $P\Rightarrow Q$ 和 $P\Rightarrow\neg Q$ 皆為對. 所以 $\neg(P\Rightarrow Q)$ 和 $P\Rightarrow\neg Q$ 並不是 logically equivalent, 千萬要記住.

Question 1.11. 試寫下會使得 $x\geq 0\Rightarrow x\geq 1$ 為對的所有實數 x, 也寫下會使得 $x\geq 0\Rightarrow x<1$ 為對的所有實數 x. 它們是否相反呢?

大家常忽略的就是 $P\Rightarrow Q$ 中 P 錯的情況, 而造成邏輯的錯誤, 千萬要注意. 不過另一方面, 若 A, B 為 statement form 且 A 為 tautology, 那麼 $\neg(A\Rightarrow B)$ 就和 $A\Rightarrow\neg B$ 為 logically equivalent. 主要的原因是, A 既然全為對, 那麼 $A\Rightarrow B$ 的對錯完全會和 B 的對錯完全一致了.

Question 1.12. 試寫下會使得 $x^2\geq 0\Rightarrow x>0$ 為對的所有實數 x, 也寫下會使得 $x^2\geq 0\Rightarrow x\leq 0$ 為對的所有實數 x. 它們是否相反呢?

要處理 $\neg(P\Rightarrow Q)$ 會和什麼為 logically equivalent, 我們可以換一個角度來看 $P\Rightarrow Q$. 首先回顧一下 $P\Rightarrow Q$ 較通俗的說法是 P 對則 Q 一定對. 所以我們知道 Q 會對, 除非 P 是錯的. 也就是說要不然是 Q 對, 要不然就是 P 錯. 這讓我們想到 $Q\vee\neg P$ 這一個 statement form. 事實上用 truth table 檢驗

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

我們得到

$$(P\Rightarrow Q) \sim (Q\vee\neg P). \tag{1.10}$$

利用 $(Q\vee\neg P)\sim((\neg P)\vee Q)$ 以及 $\neg(\neg Q)\sim Q$, 我們得 $(P\Rightarrow Q)\sim((\neg P)\vee\neg(\neg Q))$, 再利用式子 (1.10) 得 $((\neg P)\vee\neg(\neg Q))\sim((\neg Q)\Rightarrow(\neg P))$, 故知

$$(P\Rightarrow Q)\sim((\neg Q)\Rightarrow(\neg P)). \tag{1.11}$$

這和我們提過 $P\Rightarrow Q$ 為對, 表示若 Q 為錯則 P 一定錯, 相吻合.

利用式子 (1.10), 我們可得 $\neg(P\Rightarrow Q)\sim\neg(Q\vee\neg P)$. 而由 DeMorgan's laws 知

$$\neg(Q\vee\neg P)\sim((\neg Q)\wedge\neg(\neg P))$$

故得

$$\neg(P\Rightarrow Q)\sim(P\wedge(\neg Q)). \tag{1.12}$$

式子 (1.10), (1.11), (1.12) 是我們將來處理 "若 P 則 Q" 這種類型的論述時常用的 logical equivalences.

由式子 (1.10) 我們知道, 所有的 statement form 都可以利用 logical equivalence 寫成 $\neg,\wedge,\vee$ 的組合. 例如由 $P\Leftrightarrow Q$ 的定義, 我們可得

$$(P\Leftrightarrow Q)\sim(Q\vee(\neg P))\wedge(P\vee(\neg Q)). \tag{1.13}$$

再利用 $\wedge,\vee$ 的分配性 (即式子 (1.3)) 推得

$$(P\Leftrightarrow Q)\sim(P\wedge Q)\vee((\neg P)\wedge(\neg Q)). \tag{1.14}$$

因此我們可以用 DeMorgan's laws, 式子 (1.7), 以及 $\wedge,\vee$ 之間的關係式 (式子 (1.1),(1.2), (1.3)), 推導出一個 statement form 取 not 之後的 logical equivalence. 例如式子 (1.13) 取 not 可得

$$\neg(P\Leftrightarrow Q)\sim((\neg Q)\wedge P)\vee((\neg P)\wedge Q).$$

有趣的是, 若比較式子 (1.14) 中的 Q 用 $\neg Q$ 取代後的結果, 我們得到

$$\neg(P\Leftrightarrow Q)\sim(P\Leftrightarrow\neg Q).$$

以上差不多就是我們需要了解有關 "not" 的性質。為了方便起見，我們將比較常用的再列出如下：

(1) $P\sim\neg(\neg P)$
(2) 若已知 $P\sim Q$ 則 $\neg P\sim\neg Q$
(3) $\neg(P\wedge Q)\sim(\neg P)\vee(\neg Q)$
(4) $\neg(P\vee Q)\sim(\neg P)\wedge(\neg Q)$
(5) $(P\Rightarrow Q)\sim((\neg Q)\Rightarrow(\neg P))\sim(Q\vee\neg P)$
(6) $\neg(P\Rightarrow Q)\sim(P\wedge(\neg Q))$
(7) $(P\Leftrightarrow Q)\sim(P\wedge Q)\vee((\neg P)\wedge(\neg Q))$
(8) $\neg(P\Leftrightarrow Q)\sim(P\Leftrightarrow\neg Q)\sim(\neg P\Leftrightarrow Q)$

最後我們再談一下 contradiction, 回顧一下這表示一個 statement form 在任何情況之下皆為錯的。當 A 為 statement form 時, $\neg A$ 的對錯完全和 A 的對錯相反, 所以 $A\Leftrightarrow\neg A$ 的 truth table 在任何情況之下皆為錯, 可知 $A\Leftrightarrow\neg A$ 為 contradiction. 反之, 若 B 為 statement form 且 $A\Leftrightarrow B$ 為 contradiction, 表示在任何情況下 A 和 B 的對錯情況相反, 可知 $B\sim\neg A$. 因此我們有以下和 Proposition 1.2.2 相對應的性質.

Proposition 1.3.1. 假設 A,B 為兩個 *statement forms.* 則 $\neg A$ 和 B 為 *logically equivalent* 等同於 $A\Leftrightarrow B$ 為 *contradiction.*

1.4. Quantifiers

我們已經了解在已知各 statement 的對錯情況之下它們用 connective 以及 not 連接之後其對錯的狀況, 我們也知道一個 statement form 的否定為何. 不過一個單一的 statement, 很可能就很複雜, 不容易判斷對錯. 例如在數學上一個 statement 常常會有一些 quantifier (量詞) 出現, 而增加了判斷對錯的困難度. 在本節中我們將介紹常見的 quantifiers, 並探討它們取否定的情形.

數學上常見的 quantifiers 有以下幾種:

- "for all", "for every" (即對所有的), 常用 $\forall$ 表示.
- "there exists", "there is" (即存在, 可以找到), 常用 $\exists$ 表示.
- "there is a unique" (即存在唯一的), 常用 $\exists!$ 表示.

$\exists!$ 牽涉到唯一性的問題, 以後我們在談論證明方法時會提到它, 這裡我們先探討 $\forall$ 和 $\exists$. 首先要說明的是, 在談論這些 quantifiers 時必須說明清楚是在怎樣的集合內. 比方說對所有的整數和對所有的有理數就是完全不同的兩回事, 而存在一個自然數和存在一個偶數也不同. 不過由於我們僅介紹這些 quantifiers 的概念, 而不觸及證明. 所以這裡為了簡單起見我們說明的例子考慮的都是整個實數. 例如我們說 $\forall x$ 或 $\exists x$, 它們分別表示的就是 for all x in $\mathbb{R}$ 或 there exists an x in $\mathbb{R}$, 以後就不再聲明指的是實數了.

我們先看簡單的例子: $\forall x, x^2 \geq 0$. 指的就是所有的實數 x 皆會滿足 $x^2 \geq 0$. 我們知道這個 statement 是對的, 因為每一個實數 x 都對, 沒有例外. 這類的 statement 我們可以用以下的形式表示 "$\forall x, P(x)$". 這裡 $P(x)$ 指的是和 x 有關的性質 (例如上例中 $P(x)$ 就是 $x^2 \geq 0$). 它指的就是所有的 x 皆會滿足 $P(x)$ 這個性質. 這個 statement 要對就必須所有的 x 都對, 一個都不能錯. 例如 $\forall x, x^2 > 0$ 便是錯的 ($x = 0$ 就不成立).

類似的, 我們可以用 "$\exists x, P(x)$" 來表示, 存在 x 使得 $P(x)$ 成立. 這個 statement 要對, 只要能找到一個 x 使得 $P(x)$ 成立即可. 注意它並沒有說有多少個會對, 有可能很多, 有可能只有一個, 所以只要找到一個對即可 (這就是英文用 there exists 的原因). 上面提過 $\forall x, x^2 > 0$ 是錯的, 但若改為 $\exists x, x^2 > 0$ 便是對的 (取 $x = 1$, 即可). $\exists x, x^2 = 0$ 也是對的; 但 $\exists x, x^2 < 0$ 便是錯的 (因為我們僅考慮實數)。

$\forall$ 和 $\exists$ 有著有趣的關係, 例如 "$\forall x, P(x)$" 是對的話, 那麼 "$\exists x, P(x)$" 就一定對 (只要挑隨便一個 x 即可). 不過反過來就不對. 你不能隨便挑幾個 x 符合 $P(x)$, 就聲稱對所有的 x 都會符合 $P(x)$. 另外 $\forall$ 和 $\exists$ 在取否定時關係就更密切了. 當你發現 "$\forall x, P(x)$" 有可能錯時, 如何說明它是錯的呢? 前面說過 "$\forall x, P(x)$" 只要有一個 x 不符合 $P(x)$ 就是錯的, 所以要否定它, 我們只要找到一個 x 讓 $P(x)$ 不成立即可. 用符號表示就是 $\exists x, \neg P(x)$. 例如前面提過 $\forall x, x^2 > 0$ 是錯的, 因為我們發現 $\exists x, x^2 \leq 0$.

再次提醒，很多同學會誤以為 "$\forall x, P(x)$" 的否定是 "$\forall x, \neg P(x)$". 雖然若 "$\forall x, \neg P(x)$" 是對的可以知道 "$\forall x, P(x)$" 是錯的. 但是 "$\forall x, P(x)$" 是錯的, 並不表示 "$\forall x, \neg P(x)$" 是對的. 所以不能說 "$\forall x, P(x)$" 的否定是 "$\forall x, \neg P(x)$". 例如 $\forall x, x^2 > 0$ 是錯的, 但 $\forall x, x^2 \leq 0$ 也是錯的, 唯有 $\exists x, x^2 \leq 0$ 才會對. 大家千萬注意, 不要弄錯. 總而言之我們有以下的 logical

equivalence

$$\neg(\forall x, P(x)) \sim (\exists x, \neg P(x)). \tag{1.15}$$

同理要否定 "$\exists x,\ P(x)$", 表示找不到 x 使得 $P(x)$ 成立. 所以我們便需說明所有的 x 皆不滿足 $P(x)$, 也就是說 $\forall x,\ \neg P(x)$. 同樣的, 很多同學會誤以為 "$\exists x,\ P(x)$" 的否定是 "$\exists x,\ \neg P(x)$". 這是錯的, 因為找到 x 不滿足 $P(x)$ 還是有可能找到另一個 x 會滿足 $P(x)$. 因此光由 "$\exists x,\ \neg P(x)$" 並不能否定 "$\exists x,\ P(x)$". 總而言之我們有以下的 logical equivalence

$$\neg(\exists x, P(x)) \sim (\forall x, \neg P(x)). \tag{1.16}$$

Question 1.13. 試利用式子 *(1.15)* 以及 *logical equivalence* 的規則推導出式子 *(1.16).*

Quantifier 有時會發生在兩個或更多變數的情形, 這裡我們僅探討兩個變數的情形, 更多變數的情況可以依兩個變數的情況類推下去. 所謂兩個變數的情況, 是形如 "$\forall x, \exists y, P(x,y)$" 的 statement, 這裡 $P(x,y)$ 指的是和 x,y 有關的性質. 例如微積分中, 函數 $f(x)$ 在 $x=a$ 的極限為 l (即 $\lim_{x\to a} f(x) = l$) 的定義 "$\forall \varepsilon > 0, \exists \delta > 0$, 滿足 $0 < |x-a| < \delta \Rightarrow |f(x)-l| < \varepsilon$" 就是兩個變數的情況. 大致上我們會有下面四種類型的 statement.

$$(1)\forall x, \exists y, P(x,y) \quad (2)\exists x, \forall y, P(x,y) \quad (3)\forall x, \forall y, P(x,y) \quad (4)\exists x, \exists y, P(x,y).$$

(1) 指的是: 對於所有的 x 皆可找到 y 使得 $P(x,y)$ 成立. 注意這裡 x 的部分先講, 再提存在 y, 所以這個存在的 y 並不是固定的, 它可能會隨著 x 的選取而變動. 例如 $\forall x, \exists y, x+y=0$ 這個 statement 是對的. 它說任意選取 x, 皆可找到 y 滿足 $x+y=0$. 這裡 y 會隨著 x 而變動, 即 $y=-x$. 例如 $x=1$ 時 $y=-1$, 而 $x=2$ 時 $y=-2$. 這裡 x,y 的先後順序很重要, 千萬要注意.

(2) 指的是: 存在 x 使得對所有的 y 都會滿足 $P(x,y)$. 注意這裡存在的 x 先講, 再提所有的 y, 所以這個存在的 x 並是固定的, 它不可以隨著 y 而變動. 例如 $\exists x, \forall y, x+y=y$ 這個 statement 是對的. 它是說可以找到 x 讓任意的 y 皆滿足 $x+y=y$. 這裡 x 找到後便固定下來了, 即 $x=0$. 不過例如在 (1) 的情形我們知道 $\forall x, \exists y, x+y=0$ 這個 statement 是對的, 但若將 $\forall x$ 和 $\exists y$ 的順序交換得 $\exists y, \forall x, x+y=0$ 這個 statement 便是錯的. 因為我們無法找到一個固定的 y 使的所有的 x 都會滿足 $x+y=0$. 再次強調, 這裡先後順序很重要, "$\forall x, \exists y, P(x,y)$" 和 "$\exists y, \forall x, P(x,y)$" 雖然只是 $\forall x$ 和 $\exists y$ 先後順序調動, 但意義完全不同千萬要注意.

Question 1.14. $\exists x, \forall y, x+y=y$ 這個 *statement* 是對的, 但若換成 $\forall y, \exists x, x+y=y$, 是否為對呢? 又換成 $\forall x, \exists y, x+y=y$ 及 $\exists y, \forall x, x+y=y$, 哪一個對呢?

Question 1.15. 假設 $f(x,y), g(x,y)$ 皆為兩個變數的多項式. 已知 "$\forall x, \exists y, f(x,y)=0$" 和 "$\exists y, \forall x, g(x,y)=0$" 皆為對. 試問 $f(x,y)=0$ 和 $g(x,y)=0$ 在坐標平面上的圖形哪一個一定會包含一條水平直線, 哪一個一定會和鉛直線 $x=101$ 相交?

(3) 和 (4) 的情況較為單純. (3) 指的是任取一個 x, 對於任意的 y 都會使得 $P(x,y)$ 成立. 利用坐標平面的看法, 我們可以說平面上任一點 (x,y) 都會使得 $P(x,y)$ 成立, 所以此時

$\forall x$ 和 $\forall y$ 變換順序並不會改變整個 statement. 而 (4) 指的是可以找到 x 使得有一個 y 滿足 $P(x,y)$. 利用坐標平面的看法, 我們可以說平面上存在一點 (x,y) 使得 $P(x,y)$ 成立. 因此此時 $\exists x$ 和 $\exists y$ 變換順序並不會改變整個 statement. 例如若我們在 $x=3$ 時, 可找到 $y=7$ 使得 $P(3,7)$ 是正確的, 此時我們也可以說 $y=7$ 時, 可找到 $x=3$ 使得 $P(x,y)$ 為對. 總而言之 (3), (4) 因兩個變數的 quantifier 皆相同, 所以 x,y 的先後不重要. (3) 一般會簡化成 $\forall x,y$, $P(x,y)$, 而 (4) 簡化成 $\exists x,y$, $P(x,y)$.

接下來我們來看有兩個變數的 statement 取否定時 quantifier 的變化情形. 在 (1) 的情形, 即 "$\forall x,\exists y,P(x,y)$". 此時, 我們可以把 "$\exists y,P(x,y)$" 看成是 $H(x)$ 這樣的條件. 所以原 statement 可看成 $\forall x,H(x)$. 利用式子 (1.15), 我們知道它的否定為 $\exists x,\neg H(x)$. 然而式子 (1.16) 告訴我們 $\neg H(x)\sim(\forall y,\neg P(x,y))$, 所以我們得

$$\neg(\forall x,\exists y,P(x,y)) \quad\sim\quad (\exists x,\forall y,\neg P(x,y)).$$

同理我們可得

$$\begin{aligned}
\neg(\exists x,\forall y,P(x,y)) &\sim (\forall x,\exists y,\neg P(x,y))\\
\neg(\forall x,\forall y,P(x,y)) &\sim (\exists x,\exists y,\neg P(x,y))\\
\neg(\exists x,\exists y,P(x,y)) &\sim (\forall x,\forall y,\neg P(x,y)).
\end{aligned}$$

例如前面所提, 函數 $f(x)$ 滿足 $\lim_{x\to a}f(x)=l$ 的否定應為

$$\exists\varepsilon>0,\forall\delta>0,\neg(0<|x-a|<\delta\Rightarrow|f(x)-l|<\varepsilon).$$

利用式子 (1.12) 我們知

$$\neg(0<|x-a|<\delta\Rightarrow|f(x)-l|<\varepsilon) \quad\sim\quad ((0<|x-a|<\delta)\wedge(|f(x)-l|\geq\varepsilon)).$$

所以 $\lim_{x\to a}f(x)=l$ 的否定應為

$$\exists\varepsilon>0,\forall\delta>0,(0<|x-a|<\delta)\wedge(|f(x)-l|\geq\varepsilon).$$

最後, 我們說明一下 $\forall$ 和 $\exists$ 在習慣上用法的差異. 在習慣上的用語, 我們常會省略 $\forall x$. 例如 $x\geq3\Rightarrow x^2\geq9$, 這一個 statement 嚴格來說應寫成 $\forall x,(x\geq3\Rightarrow x^2\geq9)$. 也就是說, 在邏輯上我們說這個 statement 是對的應該是對所有的實數 x 都是對的. 給定一實數 x, 當 $x\geq3$, 當然可得 $x^2\geq9$. 而當 $x<3$, 因為它已不符合 $x\geq3$ 的前提, 我們知道此時 $x\geq3\Rightarrow x^2\geq9$ 也是對的. 所以我們可以認定 $\forall x,(x\geq3\Rightarrow x^2\geq9)$ 是對的 (這也是邏輯上定義 P 錯時 $P\Rightarrow Q$ 為對的用意, 希望同學能體會). 要注意的是 $\exists x$ 就絕不能省略, 否則就弄不清楚是 $\forall x$ 或 $\exists x$ 了.

總而言之, 當我們看到「$P(x)\Rightarrow Q(x)$」這樣的說法，可以看成「$\forall x,P(x)\Rightarrow Q(x)$」。也就是說，對所有的 x, 皆會使得 $P(x)\Rightarrow Q(x)$ 成立。由於邏輯上當 x 會使得 $P(x)$ 不成立時，$P(x)\Rightarrow Q(x)$ 依然成立，所以僅剩下那些使得 $P(x)$ 成立的 x 需要探討。也因此"對所有的 x, 皆會使得 $P(x)\Rightarrow Q(x)$ 成立"就表示那些剩下的 x (即 $P(x)$ 成立) 皆會使得 $P(x)\Rightarrow Q(x)$ 成立 (即 $Q(x)$ 成立)。因此在數學上對於「$P(x)\Rightarrow Q(x)$」, 我們可以將之解讀為「只要 x 符合 $P(x)$ 也會符合 $Q(x)$」這種 statement.

至於 $\exists$ 的用法, 就要注意了。在數學上，我們幾乎不會有「$\exists x, P(x) \Rightarrow Q(x)$」這樣的用法。這個 statement 當然在邏輯上是說得通的，也就是說存在 x 使得 "$P(x) \Rightarrow Q(x)$" 成立。讓我們分兩種情況來探討這個 statement 在邏輯上的意義。

(1) 存在 x 使得 $P(x)$ 不成立：此時利用此 x 知 $P(x)$ 不成立，也因此不管 $Q(x)$ 是否成立, $P(x) \Rightarrow Q(x)$ 是成立的。所以「$\exists x, P(x) \Rightarrow Q(x)$」這個 statement 當然是對的。也就是說，在此情況 $Q(x)$ 這個性質根本沒意義。

(2) 不存在 x 使得 $P(x)$ 不成立：此時表示對所有 x, 皆會使得 $P(x)$ 成立，所以「$\exists x, P(x) \Rightarrow Q(x)$」就等同於存在 x 使得 $Q(x)$ 成立。也就是說，在此情況 $P(x)$ 這個性質根本沒意義。

由此可知，數學上應該看不到「$\exists x, P(x) \Rightarrow Q(x)$」這樣的 statement. 那我們如何表達「存在一個 x 滿足由 $P(x)$ 成立可得 $Q(x)$」成立呢？因為這個 x 使得 $P(x)$ 成立，所以要 $P(x) \Rightarrow Q(x)$ 成立就表示 $Q(x)$ 也成立。因此這個說法真的很奇怪，我們應該說「存在一個 x 滿足 $P(x)$ 成立且 $Q(x)$ 成立」，即用「$\exists x, P(x) \wedge Q(x)$」來表達. 例如當我們要表達 $\sqrt{10}$ 是存在的，我們可以說「存在一個大於 0 的實數 x, 滿足 $x^2 = 10$」，因此應寫成「$\exists x, (x > 0) \wedge (x^2 = 10)$」, 而不能寫成「$\exists x, (x > 0) \Rightarrow (x^2 = 10)$」; 否則找到任意小於等於 0 的 x 都會使得「$\exists x, (x > 0) \Rightarrow (x^2 = 10)$」為對，就無法讓人知道此和 $\sqrt{10}$ 有什麼關係了。

Question 1.16. 假設 $f(x,y)$ 是一個兩個變數的多項式.「存在一實數 $a > 0$ 使得 $f(a,y) = 0$ 無解」這一個 *statement,* 數學的表示法為何*?* 並寫出這 *statement* 的否定.

Chapter 2

Methods of Proof

學會了簡單的邏輯後, 接下來便是學習如何證明. 在本章中我們將介紹一些證明的方法. 這裡我們只談有關證明的一些基本原則, 而不談證明的技巧, 所以給的例子將會挑選淺顯易懂的證明.

2.1. IF-Then 的證明

在數學中最常看到的就是這種 $P \Rightarrow Q$ 的 statement. 要證明這種 statement, 我們大致上有 **direct method**, **contrapositive method** 和 **contradiction method** 三種方法.

2.1.1. Direct Method. 所謂 direct method 指的就是直接證明, 也就是直接利用 P 成立的假設得到 Q 成立. (再次強調, 我們不必管 P 不成立時, Q 會如何). 當我們要證明 $P \Rightarrow Q$ 時, 若覺得 P 的條件已經足夠, 便可以考慮使用直接證明. 例如以下的例子.

Example 2.1.1. 令 p,a,b 為整數. 證明 if $p \mid a$ and $p \mid b$, then $p \mid a+b$.

Proof. 由假設 $p \mid a, p \mid b$, 知存在整數 m,n 使得 $a = pm, b = pn$. 故得

$$a+b = pm+pn = p(m+n).$$

因 $m+n$ 為整數, 得證 $p \mid a+b$. □

有時用直接證明的方法並不能一次到位, 需要借助其他的結果幫忙才能完成. 也就是說或許我們不能直接證出 $P \Rightarrow Q$, 但若證得 $P \Rightarrow R$ 又證得 $R \Rightarrow Q$, 此時便證得 $P \Rightarrow Q$ 了. 這是因為若證得 $P \Rightarrow R$, 表示 P 對的話 R 一定對, 再由 $R \Rightarrow Q$ 知 R 對的話 Q 一定對, 故連結而知 P 對則 Q 一定對, 得證 $P \Rightarrow Q$. 這種利用遞移性的證明通常有一部分是一些常用的性質或是一些 (輔助) 定理。例如以下的例子.

Example 2.1.2. 設 a 為正實數且 $a \neq 1$. 已知若 $a^z = 1$, 則 $z = 0$. 證明若 x,y 為實數滿足 $a^x = a^y$, 則 $x = y$.

Proof. 由於 $a \neq 0$, 對於任何實數 y, 我們知 $a^y \neq 0$, 故由 $a^x = a^y$, 等號兩邊除以 a^y 得 $a^{x-y} = 1$. 又因 $a \neq 1$, 我們知道若 $a^z = 1$, 則 $z = 0$. 故由 $a^{x-y} = 1$ 可得 $x - y = 0$, 得證 $x = y$. □

這個證明的例子中, 我們其實是先證得 $(a^x = a^y) \Rightarrow (a^{x-y} = 1)$, 再由 $(a^{x-y} = 1) \Rightarrow (x = y)$ 得證 $(a^x = a^y) \Rightarrow (x = y)$. 其中我們用了一個大家都知道的事實, 即當 a 為正實數且 $a \neq 1$, 若 $a^z = 1$, 則 $z = 0$. 這個事實是需要證明的，不過不容易用 direct method 證明，等一下我們會利用 contradiction method 來證明.

有時在 direct method 中我們可以分成好幾種情況, 看看哪些情況符合 P 的條件, 然後證得 Q. 這樣的證明方法有時稱為 *proof in cases.* 例如以下的例子.

Example 2.1.3. 假設 x 為實數. 證明 if $x^2 - 3x + 2 < 0$, then $1 < x < 2$.

Proof. 由 $x^2 - 3x + 2 = (x-1)(x-2) < 0$, 我們知可分成 2 種情況, 即

(1) $(x-1) < 0$ and $(x-2) > 0$;

(2) $(x-1) > 0$ and $(x-2) < 0$.

(1) 的情況表示 $x < 1$ 且 $x > 2$. 由於沒有實數 x 會同時滿足 $x < 1$ 以及 $x > 2$, 我們知 (1) 不可能成立, 故推得 (2), 即 $x > 1$ 且 $x < 2$. 證得 $1 < x < 2$. □

注意, 在這個證明中, 有些同學或許會疑惑為什麼是排除 (1), 而不直接驗證 (2) 可得 $x^2 - 3x + 2 < 0$ 呢? 這是錯誤的. 在我們的證明中明明白白表示: 若 x 滿足 $x^2 - 3x + 2 < 0$, 那麼 x 一定會滿足 (1) 或是 (2). 排除 (1) 表示只有 (2) 會對, 所以確定若 x 滿足 $x^2 - 3x + 2 < 0$, 那麼 x 一定滿足 (2). 若僅說 x 滿足 (2) 可得 $x^2 - 3x + 2 < 0$, 而沒有排除 (1), 那麼這是證明 if $1 < x < 2$, then $x^2 - 3x + 2 < 0$, 而不是證 if $x^2 - 3x + 2 < 0$, then $1 < x < 2$. 千萬別搞錯.

Question 2.1. 假設 x 為實數.

(1) *"If* $x^2 - 3x + 2 < 0$, *then* $0 < x < 3$*."* 和 *"If* $x^2 - 3x + 2 < 0$, *then* $1.3 < x < 1.7$*."* 這兩個 *statements* 哪一個是對的*?*

(2) *"If* $0 < x < 3$, *then* $x^2 - 3x + 2 < 0$*."* 和 *"If* $1.3 < x < 1.7$, *then* $x^2 - 3x + 2 < 0$*."* 這兩個 *statements* 哪一個是對的*?*

有時在論證的問題有多種結論例如要論證 $P \Rightarrow Q \wedge R$ 或是 $P \Rightarrow Q \vee R$. 當要論證 $P \Rightarrow Q \wedge R$，我們當然就是證明 P 對則 Q 和 R 都會對。但要證明 $P \Rightarrow Q \vee R$, 就會有點麻煩。因為 $Q \vee R$ 會對表示有可能 Q 對 R 錯；Q 錯 R 對，甚至 Q,R 都對。也因此要推得 $Q \vee R$ 會對，感覺有點麻煩。接下來這個技巧就很好用。我們可以直接僅考慮已知 P 對且 Q 錯的情況，因為如果 Q 對那自然 $Q \vee R$ 是對的。因此，此時我們就只要證明由 P 對 Q 錯可推得 R 對即可。從邏輯來看，因為 $(P \Rightarrow (Q \vee R)) \sim (\neg P \vee (Q \vee R))$, 而 $((P \wedge \neg Q) \Rightarrow R) \sim (\neg(P \wedge \neg Q) \vee R) \sim ((\neg P \vee Q) \vee R))$ 所以 $(P \Rightarrow (Q \vee R)) \sim ((P \wedge \neg Q) \Rightarrow R)$. 我們看以下的例子。

Example 2.1.4. 證明若 $xy=0$, 則 $x=0$ 或 $y=0$.

Proof. 我們可假設 $xy=0$ 且 $x\neq 0$, 此時因 $x\neq 0$, 可將等式 $xy=0$ 的兩邊除以 x (或說乘以 $1/x$), 得 $y=0$. □

當然了，在證明 $P\Rightarrow(Q\vee R)$ 時，若覺得 $\neg R$ 比較好用，當然可改成證 $(P\wedge\neg R)\Rightarrow Q$.

2.1.2. Contrapositive Method. 我們稱 $(\neg Q)\Rightarrow(\neg P)$ 為 $P\Rightarrow Q$ 這個 statement 的 *contrapositive statement.* 回顧一下, 我們知道 $P\Rightarrow Q$ 和 $(\neg Q)\Rightarrow(\neg P)$ 是 logically equivalent (參見式子 (1.11)). 也就是說 $P\Rightarrow Q$ 和 $(\neg Q)\Rightarrow(\neg P)$ 的對錯是一致的. 因此, 若我們能證明 $(\neg Q)\Rightarrow(\neg P)$ 便證得 $P\Rightarrow Q$ 了.

當要證明 $P\Rightarrow Q$ 時, 若發現 P 的條件似乎不容易幫助我們證明, 而 $\neg Q$ 較容易處理時便可以考慮使用 contrapositive method. 也就是說證明 $(\neg Q)\Rightarrow(\neg P)$. 最常發生的情況就是有不等式的情形. 因為不等式不如等式使用方便, 很多不等式的使用規則其實都是用等式推導的, 所以如果一個 statement 牽涉到不等式, 而它的 contrapositive statement 是等式. 那麼自然用 contrapositive method 會比較容易證明. 我們有以下的例子.

Example 2.1.5. 設 x,y 為實數. 證明 if $x\neq y$, then $x^3\neq y^3$.

當然了, 若你了解 $f(x)=x^3$ 的圖形或利用微積分, 可以知道這一定對的. 不過我們想要用比較基礎的方法處理. 若用 contrapositive method 來證明, 就是先假設 $\neg(x^3\neq y^3)$ (即 $x^3=y^3$), 要證得 $\neg(x\neq y)$ (即 $x=y$).

Proof. 利用 contrapositive method, 首先假設 $x^3=y^3$, 即 $0=x^3-y^3=(x-y)(x^2+xy+y^2)$. 由 Example 2.1.4 可得 $x-y=0$ 或 $x^2+xy+y^2=0$. 因此可用 proof in cases 處理。

(1) $x-y=0$：此時即 $x=y$.

(2) $x^2+xy+y^2=0$: 此時由

$$x^2+xy+y^2=(x+\frac{1}{2}y)^2+\frac{3}{4}y^2.$$

可得 $x+\frac{1}{2}y=0$ 且 $y=0$. 因此得 $x=y=0$.

由於所有情況皆得 $x=y$, 故得證 if $x^3=y^3$ then $x=y$, 也因此得證 if $x\neq y$, then $x^3\neq y^3$. □

當我們利用 contrapositive method 把要證明的 $P\Rightarrow Q$ 改為證明 $\neg Q\Rightarrow\neg P$ 後，就可以用前面所提的 direct method 的方法證明 $\neg Q\Rightarrow\neg P$. 在上例中，我們就是利用遞移性以及 proof in case 處理。

若一個 statement 是由包含 x 的式子的性質, 來推得 x 本身的性質, 由於通常是反過來將 x 代入式子比較容易，此時也是用 contrapositive method 的好時機. 例如以下的簡單例子.

Example 2.1.6. 設 x 為整數. 證明 if x^2 is even (偶數), then x is even.

Proof. 用 contrapositive method, 即證明若 x 為奇數, 則 x^2 為奇數. 然而 x 為奇數, 表示 x 可以寫成 $x=2n+1$, 其中 n 為整數. 故得證 $x^2=(2n+1)^2=4n^2+4n+1=2(2n^2+2n)+1$ 為奇數. □

Question 2.2. 假設 x,y 為整數. 試用 *contrapositive method* 證明 *if $x+y$ is even, then x and y are both even or odd.*

有時用 proof in cases 處理的情況, 也可用 contrapositive method 來證明. 例如 Example 2.1.3 就可以用 contrapositive method 證明. 也就是說, 先假設 $\neg(1<x<2)$ (即 $x\geq 2$ or $x\leq 1$) 求得 $\neg(x^2-3x+2<0)$ (即 $x^2-3x+2\geq 0$). 我們看另外的例子.

Example 2.1.7. 設 x,y,a 為正實數. 證明 if $xy=a$, then $x\leq\sqrt{a}$ or $y\leq\sqrt{a}$.

用 proof in cases 證明，需考慮 x,y 所有可能與 $\sqrt{a}$ 的大小關係，要分成好幾種情況。而用 contrapositive method, 我們只要考慮一種情況。

Proof. 用 contrapositive method, 先假設 $\neg((x\leq\sqrt{a})\vee(y\leq\sqrt{a}))$ (即 $x>\sqrt{a}$ and $y>\sqrt{a}$) 要證得 $\neg(xy=a)$ (即 $xy\neq a$). 然而 x,y,a 為正, 故由 $x>\sqrt{a}$ and $y>\sqrt{a}$ 可得 $xy>(\sqrt{a})^2=a$, 得證 $xy\neq a$. □

Question 2.3. 利用類似 *Example* 2.1.4 中證明 $P\Rightarrow(Q\vee R)$ 的方法，證明 *Example* 2.1.7.

Question 2.4. 設 x,y,a 為正實數. 請問 *if $xy=a$, then $x\geq\sqrt{a}$ or $y\geq\sqrt{a}$* 是否為對*?* 若為對, 此和 *Example 2.1.7,* 是否有矛盾*?*

2.1.3. Contradiction Method. 回顧式子 (1.10) 告訴我們 $P\Rightarrow Q$ 和 $Q\vee\neg P$ 是 logically equivalent. 也就是說, 若我們能證明 $Q\vee\neg P$ 就等同證明了 $P\Rightarrow Q$. 然而 $Q\vee\neg P$ 是“或”的情況, 處理起來有點像前面提過的 proof in cases, 沒有太多的優勢. 不過若考慮 $\neg(P\Rightarrow Q)$, 此時和 $(\neg Q)\wedge P$ 為 logically equivalent (參見式子 (1.12)). 因此若能證明 $(\neg Q)\wedge P$ 一定是錯的, 便證得 $P\Rightarrow Q$ 為對. 這就是所謂的 contradiction method.

Contradiction method 的處理方法就是, 先假設 $(\neg Q)$ 和 P 皆為對, 再從中推導出與我們知道一定對的 statement 相矛盾. 如此一來便表示 $(\neg Q)$ 和 P 是錯的, 而得證 $P\Rightarrow Q$. 這個方法的最大優點就是它一次便同時假設 P 和 $\neg Q$ 為對, 給我們較多的資訊去推導, 而不像 direct method 僅假設 P 為對, 或 contrapositive method 僅假設 $\neg Q$ 為對. 它的缺點就是, 不像 direct method 或 contrapositive method 明確地知道要推導甚麼 (即由 P 推導出 Q 或由 $\neg Q$ 推導出 $\neg P$), 而是要推導出一個“未知”的矛盾.

當要證明 $P\Rightarrow Q$ 時, 若發現單獨 P 的條件或是單獨 $\neg Q$ 的條件似乎不容易幫助我們證明, 這時便可以考慮 P 和 $\neg Q$ 的條件可同時使用的 contradiction method. 我們看以下的例子.

Example 2.1.8. 設 r 為實數, 證明 if $r^2=2$, then r is irrational (無理數).

我們幾乎沒有直接的方法證明一個數是無理數, 所以不可能用 direct method. 而若用 contrapositive method 雖可先假設 r 為有理數, 但要推得 $r^2 \neq 2$ 這個不等式. 前面已提過不等式的推導並不容易, 所以我們用 contradiction method 來證明.

Proof. 用 contradiction method, 即假設 r 為有理數且滿足 $r^2 = r$, 希望能得到矛盾. 依假設 r 為有理數, 表示 r 可以寫成 $r = (m/n)$, 其中 m,n 為整數. 現若 m,n 皆為偶數, 我們可以約掉 2, 如此一直下去, 我們可假設 m,n 為一奇一偶或皆為奇數. 然而 $r^2 = 2$, 即 $m^2 = 2n^2$ 為偶數, 故由 Example 2.1.6 知 m 必為偶數. 也就是說 m 可寫成 $m = 2m'$, 其中 m' 為整數. 此時得 $4m'^2 = 2n^2$, 即 $n^2 = 2m'^2$ 為偶數. 故再由 Example 2.1.6 知 n 亦為偶數. 此與當初假設 m,n 為一奇一偶或皆為奇數相矛盾. 故得證 if $r^2 = 2$, then r is irrational. □

從 Example 2.1.8 中我們應可體會, 當初若沒有想到將 $r = (m/n)$ 中分子分母的 2 約乾淨, 就無法推出矛盾了. 所以用 contradiction method 證明的困難處就是要 "製造矛盾".

回顧在 Example 2.1.2 的證明中, 我們用了一個事實, 即當 $a \neq 1$ 且為正實數時, 若 z 為實數 $a^z = 1$, 則 $z = 0$. 我們可以用 contradiction method 來證明這個 statement.

Example 2.1.9. 設 $a \neq 1$ 且為正實數. 證明若 z 為實數滿足 $a^z = 1$, 則 $z = 0$.

若要用 contradiction method, 我們必須假設 $z \neq 0$ 且 $a^z = 1$ 而得到矛盾. 要如何製造矛盾呢? 我們知道這個 statement $a \neq 1$ 是重要的前提 (否則它會錯), 所以矛盾的關鍵是 $a \neq 1$.

Proof. 我們利用 contradiction method, 先假設 $z \neq 0$ 且 $a^z = 1$. 此時由於 $z \neq 0$, 我們知 $1/z$ 是存在的, 故利用 $(a^z)^{1/z} = a$ 以及 $a^z = 1$, 得

$$a = (a^z)^{1/z} = 1^{1/z} = 1.$$

此與已知 $a \neq 1$ 相矛盾, 得證若 $a^z = 1$, 則 $z = 0$. □

Remark 2.1.10. 在證明 $P \Rightarrow Q$ 時，其實用 contrapositive method 或 contradiction method 它們第一步是一樣的，也就是先假設 $\neg Q$. 接著我們就可以判斷是否條件夠我們推導出 $\neg P$. 若條件夠，那就用 contrapositive method. 若條件不夠，則可以加上 P 的條件，看看是否可推得矛盾，這就是 contradiction method. 這兩種方法，各有很多種中文名稱，甚至兩種分別都有人稱之為 "反證法"。為了方便起見，以後我不太想去區分這兩種方法，我都一律稱之為反證法。也就說只要是要用 $\neg Q$ 這樣的條件來證明，我都一律稱之為「反證法」。

2.1.4. If and Only If 的證明. $P \Leftrightarrow Q$ 的證明基本上就是要證明 $P \Rightarrow Q$ 和 $Q \Rightarrow P$. 大家或許看過有些證明由於每一個步驟逆推回去也是對的, 所以在推導完 $P \Rightarrow Q$ 後便說反向亦然, 而得證 $P \Leftrightarrow Q$. 在這裡特別提醒大家, 除非你確認每一個步驟逆推回去也是對的, 千萬不要隨便認定反向亦然, 就說得證 $P \Leftrightarrow Q$. 尤其在以後許多進階一點的定理, 很可能兩邊的推導方式是用到完全不同的概念或原理. 所以證明 $P \Leftrightarrow Q$ 還是要分別證明 $P \Rightarrow Q$ 和 $Q \Rightarrow P$ 為宜.

例如設 a 為整數要證明 "a^2 為偶數 $\Leftrightarrow$ a 為偶數", 大家可能會先證 $\Leftarrow$ 這個方向. 此時可令 $a=2n$, 其中 n 為整數, 便得 $a^2=(2n)^2=4n^2$ 為偶數. 但這個推導方式, 逆推就有問題了. 因為知道 a^2 為偶數, 為何 a^2 一定可以寫成 $4n^2$ 這個樣子呢? 所以 $\Rightarrow$ 這個方向還是要推導的 (我們在 Example 2.1.6 已證明過了).

由於 $(P\Rightarrow Q)\sim((\neg Q)\Rightarrow(\neg P))$ 且 $(Q\Rightarrow P)\sim((\neg P)\Rightarrow(\neg Q))$ 我們知 $P\Leftrightarrow Q$ 和 $(\neg P)\Leftrightarrow(\neg Q)$ 為 logically equivalent. 有的同學會覺得若證明 $P\Leftrightarrow Q$ 較麻煩, 可考慮證明 $(\neg P)\Leftrightarrow(\neg Q)$. 其實這是沒必要的, 不管證明哪一個都需要經過一樣的過程. 例如假設 a,b 為整數, 證明 "ab is even $\Leftrightarrow$ a is even or b is even" 和證明 "ab is odd $\Leftrightarrow$ a and b are odd" 其實是一樣的. 即使後面那一個看起來比較簡潔, 但是不管證明哪一個, 證明的過程都是一樣的. 反倒是有的同學可能會證明了 $(\neg Q)\Rightarrow(\neg P)$ 後又去證 $P\Rightarrow Q$. 重複證明了同一件事而不自知, 誤以為證得了兩個方向, 千萬要注意. 所以基本上在證明若且唯若的 statement 時, 最好表明目前在證明哪一個方向. 這樣自己較不會弄錯, 看證明的人也較清楚整個證明過程. 兩全其美, 何樂而不為呢?

數學上也經常會有類似這樣的 statement:

$$\text{The following are equivalent.}\quad (1)\,P;\quad (2)\,Q;\quad (3)\,R.$$

(有時不只會有 P,Q,R 三項, 可能會有更多項). 這個意思就是說

$$P\Leftrightarrow Q,\quad Q\Leftrightarrow R\quad\text{and}\quad R\Leftrightarrow P.$$

雖是如此, 我們不必 "六" 個 $\Rightarrow$ 都證. 事實上僅要證明

$$P\Rightarrow Q,\quad Q\Rightarrow R\quad\text{and}\quad R\Rightarrow P$$

即可. 這是因為 $Q\Rightarrow P$ 的部分, 可由 $Q\Rightarrow R$ 以及 $R\Rightarrow P$ 得到, 而 $R\Rightarrow Q$ 的部分, 可由 $R\Rightarrow P$ 以及 $P\Rightarrow Q$ 得到. 最後 $P\Rightarrow R$ 的部分, 可由 $P\Rightarrow Q$ 以及 $Q\Rightarrow R$ 得到. 當然了, 有時不一定這個順序好證, 也可考慮倒過來證明

$$R\Rightarrow Q,\quad Q\Rightarrow P\quad\text{and}\quad P\Rightarrow R.$$

甚至有時候會發生不管哪一邊都不好證, 例如 $P\Leftrightarrow R$ 兩邊都不好證, 這時證明

$$P\Leftrightarrow Q\quad\text{and}\quad Q\Leftrightarrow R$$

也可. 因為 $P\Rightarrow R$ 的部分, 可由 $P\Rightarrow Q$ 以及 $Q\Rightarrow R$ 得到, 而 $R\Rightarrow P$ 的部分, 可由 $R\Rightarrow Q$ 以及 $Q\Rightarrow P$ 得到. 總之, 在證明這一類的問題, 要注意推導的方向, 確保任兩個 statement 都可通行無阻. 時時標明目前是從哪一個 statement 推導到哪一個 statement, 是必要的.

2.2. Existence and Uniqueness 的證明

Existence 指的是存在性, 而 uniqueness 指的是唯一性. 這兩個性質的探討也經常在數學定理中出現. 要注意, existence 和 uniqueness 是兩個互相獨立的性質. 也就是說存在未必會唯一. 而這裡的唯一指的是若存在則會唯一, 所以證得唯一也未必會存在. 所以這裡, 我們分開討論 existence 和 uniqueness 的證明.

2.2.1. Existence. 有關 existence 的證明方法大致上有兩類. 一類是所謂的 *constructive method* 指的是確實告知存在的是什麼. 另一類是 *nonconstructive method* 指的是利用已知的理論或邏輯的推導得知一定存在, 但未必知道有哪些.

例如證明存在實數 x 滿足 $6x^2-x-1=0$. 我們可以將 $6x^2-x-1$ 分解得 $(2x-1)(3x+1)$ 故明確找出 $x=1/2$ (或 $x=-1/3$) 這個實數會滿足 $6x^2-x-1=0$. 這就是一個 construct method. 我們也可考慮多項式函數 $f(x)=6x^2-x-1$, 發現 $f(0)=-1<0$ 且 $f(1)=4>0$. 故由多項式函數為連續函數以及連續函數的中間值定理, 證得 $f(x)=0$ 在 $0<x<1$ 之間必有一根, 而證得了存在性. 這個方法雖證出存在性, 但因無法明確指出哪一個 x 會滿足 $6x^2-x-1=0$, 所以是 nonconstructive method. 我們再看以下的例子.

Example 2.2.1. 證明 there exists irrational numbers a,b such that a^b is rational.

Proof. Constructive Method: 考慮 $a=\sqrt{2}$ 且 $b=\log_2 9$. 我們已知 a 為無理數. 同樣的利用反證法可證明 b 亦為無理數. 事實上若存在 m,n 為整數滿足 $\log_2 3=n/m$. 表示 $2^n=3^m$, 我們知道 3 的任何整數次方都不會是偶數, 得到矛盾. 故知 $b=\log_2 9$ 為無理數. 此時

$$a^b=2^{\frac{1}{2}\log_2 9}=2^{\log_2 3}=3,$$

得證存在無理數 a,b 使得 a^b 為有理數.

Nonconstructive Method: 考慮 $a'=\sqrt{2}$ 且 $b'=\sqrt{2}$. 我們知道 a',b' 為無理數. 令 $c=(a')^{b'}$. 若 c 為有理數, 則 $a=\sqrt{2},b=\sqrt{2}$ 為所求. 而若 c 為無理數, 此時令 $a=c,b=\sqrt{2}$, 則

$$a^b=(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}=\sqrt{2}^2=2.$$

得證存在無理數 a,b 使得 a^b 為有理數. □

這裡這個 nonconstructive method 由於沒有證明 $\sqrt{2}^{\sqrt{2}}$ 是否為有理數. 因此無法確定 $a=b=\sqrt{2}$ 和 $a=\sqrt{2}^{\sqrt{2}},b=\sqrt{2}$ 中哪一個會是符合存在性的要求, 但確定它們兩個其中有一個會符合, 所以是 nonconstructive method. 事實上只要知道 $\sqrt{2}^{\sqrt{2}}$ 是無理數, 令 $a=\sqrt{2}^{\sqrt{2}},b=\sqrt{2}$ 這便是 constructive method. 不過 $\sqrt{2}^{\sqrt{2}}$ 是無理數的證明非常困難 (遠遠超過本講義的範圍). 所以我們避開它的證明, 而仍能證明存在性, 這就是 nonconstructive method 的精神.

Question 2.5. 試找到其他的例子或更一般的方法, 利用 *construct method* 證明 *there exists irrational numbers a,b such that a^b is rational.*

大家可以發現利用 constructive method 得到存在性, 證明的重點並不是在於如何找到這些存在的東西, 而是要確實驗證並說明為何它們符合存在的條件. 例如在證明一個方程式的解存在時, 同學們常常利用等式推導出解的可能值, 而沒有代回驗證是否為解就誤以為證得存在性. 這是同學們常弄錯的, 所以我們特別說明一下. 在求解的推導過程, 往往是假設解存在, 再利用一些等式推導出解的 "可能值". 也就是說, 除非你的推導過程是 "雙向" 皆成立的, 否則你推出的結果是,「若解存在的話, 則它們可能的值」, 未必這些真的是解 (這再次

說明若 P 則 Q 方向性的重要). 這些推出的值只是讓我們縮小要驗證的範圍而已, 此時唯有將這些值代回驗證, 才能確保解的存在. 我們看下面的例子.

Example 2.2.2. 是否存在實數 x 滿足 $\sqrt{3-2x}=x-2$?

若直接假設有解, 則兩邊平方得 $3-2x=x^2-4x+4$, 即 $x^2-2x+1=0$. 得 $x=1$. 這表示若有解, 其解必為 $x=1$. 也就是除了 $x=1$ 可能會是此方程式之解外, 其他實數都不可能是解. 但將 $x=1$ 代回原式, 得 $1=-1$ 不合. 故知不存在實數 x 滿足 $\sqrt{3-2x}=x-2$.

其實使用 nonconstructive method 證明存在性, 一般或多或少會用到反證法. 例如前面提過利用連續函數的中間值定理證明存在實數 x 滿足 $6x^2-x-1=0$. 雖然看似沒用到反證法, 不過中間值定理本身的證明一般來說都會用到反證法. 還有一個常用來證明存在性的方法, 就是 *pigeonhole principle* (鴿籠原理). 它原本是 "Dirichlet's drawer principle", 不過現在許多人習慣用 pigeonhole principle 稱之.

Theorem 2.2.3 (Pigeonhole Principle)**.** 令 n 為正整數. 假設有 n 個鴿籠以及多於 n 隻的鴿子. 若要所有的鴿子住進鴿籠裡, 則一定會有一個鴿籠會有兩隻以上的鴿子.

Proof. 很明顯的, 這個存在性無法用 constructive method. 利用反證法, 原本 statement 是說「存在一個鴿籠會有兩隻以上的鴿子」, 它的否定便是「所有的鴿籠都只有一隻或沒有鴿子」但如此一來表示所有 n 個鴿籠裡的鴿子最多只有 n 隻, 與原本假設有多於 n 隻的鴿子矛盾. 得證必有一個鴿籠會有兩隻以上的鴿子. □

將來我們會碰到利用 pigeonhole principle 證明存在性的問題. 大致上, 只要弄清楚甚麼拿來當鴿子, 甚麼拿來當鴿籠就好. 例如證明任取 6 個整數, 其中一定有兩個整數其除以 5 的餘數相同. 這裡我們可以將 6 個整數當成 6 隻鴿子, 將鴿籠從 0 到 4 編號. 若除以 5 的餘數為 0 就放到 0 號鴿籠, 餘數為 1 就放 1 號鴿籠, 依此類推. 因鴿子個數 6 多於鴿籠的個數 5, 利用鴿籠原理, 我們知必有一個鴿籠裡有兩隻以上的鴿子. 也就是說會有兩個整數除以 5 的餘數相同.

我們可以將這個結果稍微推廣一下. 例如任取 16 個整數, 可以證明其中可找到 4 個整數除以 5 有同樣餘數. 這是因為若這些整數除以 5 餘數為 0,1,2,3,4 的都不超過 3 個, 那麼這些整數總共最多不會超過 15 個, 就和原本假設有 16 個整數相矛盾了. 我們有以下 Theorem 2.2.3 的推廣, 證明就不再贅述了.

Theorem 2.2.4. 令 k,n 為正整數. 假設有 n 個鴿籠以及多於 kn 隻的鴿子. 若要所有的鴿子住進鴿籠裡, 則一定會有一個鴿籠會有 k 隻以上的鴿子.

Question 2.6. 試證明 *Theorem 2.2.4*

最後提醒一下, 鴿籠原理不能處理鴿子數少於或等於鴿籠數的情況 (除非另有特殊條件). 它並沒有說在鴿子數少於或等於鴿籠數的情況下不會有鴿籠有兩隻以上的鴿子. 另外它也沒有說在鴿子數多於鴿籠數的情況之下不會有空籠子. 這些都很容易找到反例, 請不要自己過度解讀這個原理.

2.2.2. Uniqueness. 基本上唯一性的證明是在假設存在的前提之下去證明唯一. 所以唯一性的證明一般和存在性的證明是無關的. 當然了, 如果已知不存在了, 就不必去證明唯一性了. 例如在 Example 2.2.2 中當我們假設 x 為解而推得 $x=1$ 時, 便證明了此方程式若有解則解唯一. 不過後來知道方程式無解, 所以這唯一性就不重要了.

大致上唯一性的證明也分成直接證明與反證法兩種. 直接證明就如前述, 直接說明若東西存在應該是什麼. 而反證法一般用的方法是假設有兩個不同的東西滿足條件, 進而推得矛盾. 我們簡單的用 $\mathbb{R}^2$ 上向量的性質來說明.

Example 2.2.5. 證明 $\mathbb{R}^2$ 中若存在一個向量 $\overrightarrow{O}$ 滿足對任意 $\mathbb{R}^2$ 上的向量 $\overrightarrow{V}$ 皆符合 $\overrightarrow{V}+\overrightarrow{O}=\overrightarrow{V}$, 則 $\overrightarrow{O}$ 是唯一的.

(1) 直接證明: 假設 $\overrightarrow{O}=(x,y)$, 對任意 $\overrightarrow{V}=(a,b)\in\mathbb{R}^2$. 由於 $\overrightarrow{O}$ 須符合 $\overrightarrow{V}+\overrightarrow{O}=\overrightarrow{V}$, 得 $(a,b)+(x,y)=(a+x,b+y)=(a,b)$. 利用向量相等的定義得 $a+x=a, b+y=b$, 即 $x=0, y=0$. 得證 $\overrightarrow{O}$ 若存在, 則必須等於 $(0,0)$.

(2) 反證法: 假設 $\overrightarrow{O},\overrightarrow{Q}\in\mathbb{R}^2$ 且 $\overrightarrow{O}\neq\overrightarrow{Q}$ 皆滿足對任意 $\overrightarrow{V}\in\mathbb{R}^2$,

$$\overrightarrow{V}+\overrightarrow{O}=\overrightarrow{V} \tag{2.1}$$

以及

$$\overrightarrow{V}+\overrightarrow{Q}=\overrightarrow{V} \tag{2.2}$$

考慮 $\overrightarrow{Q}=\overrightarrow{V}$ 的情形代入式子 (2.1) 得 $\overrightarrow{Q}+\overrightarrow{O}=\overrightarrow{Q}$. 同理將 $\overrightarrow{O}=\overrightarrow{V}$ 代入式子 (2.2) 得 $\overrightarrow{O}+\overrightarrow{Q}=\overrightarrow{O}$. 由於 $\overrightarrow{Q}+\overrightarrow{O}=\overrightarrow{O}+\overrightarrow{Q}$, 得 $\overrightarrow{Q}=\overrightarrow{O}$. 此與當初假設 $\overrightarrow{O}\neq\overrightarrow{Q}$ 相矛盾, 得證唯一性.

Question 2.7. 給定 $\overrightarrow{V}\in\mathbb{R}^2$ 試利用直接證法以及反證法證明: $\mathbb{R}^2$ 中若存在一個向量 $\overrightarrow{W}$ 滿足 $\overrightarrow{V}+\overrightarrow{W}=\overrightarrow{O}$, 則 $\overrightarrow{W}$ 是唯一的.

注意在 Example 2.2.5 中的直接證法中, 我們求出 $\overrightarrow{O}$ 若存在, 則 $\overrightarrow{O}=(0,0)$. 如再帶回驗證, 確認 $\overrightarrow{O}=(0,0)$ 確實符合, 我們便也證得存在性了. 這是直接證法的好處. 而反證法就沒辦法推得存在性了. 所以一般不是用直接證明時, 存在性及唯一性的證明是要分開來處理的. 然而將來我們會碰到較抽象的數學問題時, 大多直接證明是行不通的. 此時只好仰賴反證法了.

Example 2.2.6. 證明若存在一個實數 r 滿足, $r^3=3$, 則此實數 r 是唯一的.

Proof. 回顧一下在 Example 2.1.5 中我們證明了, 若 x,y 為實數且 $x\neq y$, 則 $x^3\neq y^3$. 假設 $r\in\mathbb{R}$ 滿足, $r^3=3$ 且 $s\neq r$ 是另一個實數滿足 $s^3=3$, 則利用 Example 2.1.5 的結果得 $3=s^3\neq r^3=3$. 由此矛盾知不可能有另一個實數 s 會滿足 $s^3=3$. □

在 Example 2.2.6 中我們是先證明 $x\neq y$ 時, x,y 不可能都符合某性質, 再利用反證法推得唯一性. 這是我們一般證明唯一性常用的方法. 再強調一次, Example 2.2.6 的證明中我們無法得知是否存在實數 r 滿足 $r^3=3$, 我們只知道若存在的話必唯一. 至於此存在性的證明, 是需要另外利用實數的完備性 (或利用多項式函數 $f(x)=x^3$ 的連續性) 來證明的. 這樣有了存在性和唯一性我們才進一步用符號 $3^{1/3}$ 來表示這個唯一滿足 $r^3=3$ 的實數 r.

2.3. Mathematical Induction

另一個常見的證明方法就是所謂的 "數學歸納法". 其實數學歸納法牽涉到建立整數系的 axiom (公設), 不過這裡我們不去談論這些公設邏輯的問題. 而著重於理解並正確使用數學歸納法. 我們將介紹三種數學歸納法, 雖然它們看起來不大一樣, 不過背後的原理是相同的, 事實上它們是等價的.

數學的理論證明其實根源是一些大家都能接受但無法證明的 axiom (公設). 介紹數學歸納法之前, 我們先了解所謂 *well-ordering principle*. 它是可以用其他的公設來證明的, 不過由於我們目前不想牽涉到這方面的課題. 所以我們直接把 well-ordering principle 當成是一個公設. 也就是說它和我們的直觀吻合, 所以我們相信它而不去證明.

所謂 well-ordering 字面上的解釋是 "好的排序" 的意思, 這個排序原理簡單來說是:「將一些正整數收集起來所成的非空集合中, 一定有一個最小的元素」. 相信大家應該不會覺得這個 principle (原則) 不對吧! 直觀上, 自然數是有最小元素 1 的, 所以有下界. 因此大家應不會懷疑這集合裡會有最小的元素. 問題是這集合可能有無窮多的元素, 我們可能無法真正找出這最小元素來, 不過我們相信它一定存在.

接下來我們來看, 最基本的第一種數學歸納法.

Theorem 2.3.1 (Mathematical Induction)**.** 假設以下兩個 *statement* 是對的

I1: $P(1)$ 成立

I2: 若 $k \in \mathbb{N}$ 且 $P(k)$ 成立, 則 $P(k+1)$ 成立

那麼對任意正整數 n, $P(n)$ 皆成立.

Proof. 由於我們不可能直接證明所有的正整數 n 都會使得 $P(n)$ 成立, 所以我們用反證法. 也就是說假設 (1), (2) 是對的以及「對任意正整數 n, $P(n)$ 皆成立」是錯的來得到矛盾.「對任意正整數 n, $P(n)$ 皆成立」是錯的, 亦即「存在正整數 n, 使得 $P(n)$ 不成立」. 因此我們可以將使得 $P(n)$ 不成立的這些正整數 n 收集起來. 因為它不是空集合, 故由 well-ordering principle 知, 必存在最小的正整數 m 使得 $P(m)$ 不成立. 由 (1) 我們知 $P(1)$ 成立, 故得 $m \neq 1$. 也就是說 m 為大於 1 的正整數. 現由於 $m-1$ 為正整數且 $m-1 < m$, 故由 m 為使得 $P(m)$ 不成立的最小正整數之假設知 $P(m-1)$ 成立. 然而由 (2) 知, 當 $P(m-1)$ 成立時, $P((m-1)+1) = P(m)$ 必成立. 此與 $P(m)$ 不成立之假設相矛盾. 故知不可能存在正整數 n, 使得 $P(n)$ 不成立, 也就是說對任意正整數 n, $P(n)$ 皆成立. □

數學歸納法是很好理解的, 它是說由 (I1) 知 P(1) 是對的, 將 (I2) 代 $k = 1$ 的情況, 故由 $P(1)$ 對可推得 $P(2)$ 是對的. 接著代 $k = 2$ 的情況, 由 $P(2)$ 是對的推得 $P(3)$ 是對的. 這樣一直下去. 所以 $P(1)$ 的起頭非常重要. 另外要強調的是 (I2) 指的是假設 $P(k)$ 對推得 $P(k+1)$ 是對的. 所以它並不是要證明 $P(k)$ 是對的, 你也不必擔心 $P(k)$ 到底對不對, 只要想法子利用 $P(k)$ 是對的假設證出 $P(k+1)$ 是對的. 若你沒辦法單純由 $P(k)$ 是對的推得 $P(k+1)$ 是對的, 那基本上就無法用數學歸納法證明了. 例如考慮多項式 $f(x) = x^2 + x + 41$. 當我們代 $x = 1$ 時 $f(1) = 43$ 為質數. 代 $x = 2$, 得 $f(2) = 47$ 仍為質數. $f(3) = 53$, $f(4) = 61$,

$f(5)=71$ 也都是質數. 或許你會有一股衝動認為 x 代任何的整數 n 都會使 $f(n)$ 為質數. 事實上一直代到 $x=39$ 它都會是質數. 但是光由代的動作, 而不去考慮如何由 $f(k)$ 是質數得到 $f(k+1)$ 是質數, 是沒有辦法用數學歸納法的. 事實上我們可以看出, 當 $x=40$ 時, $f(40)=40^2+40+41=40(40+1)+41$ 是可以被 41 整除的, 所以不是質數.

我們看下一個可以用數學歸納法證明的例子.

Example 2.3.2. 設 a,b 為相異的整數, 利用數學歸納法證明: 對任意的正整數 n 皆有 a^n-b^n 為 $a-b$ 的倍數.

Proof. 我們可以將 a^n-b^n 分解成 $(a-b)(a^{n-1}+a^{n-2}b+\cdots+b^{n-1})$, 得證 a^n-b^n 為 $a-b$ 的倍數. 不過這裡想介紹如何用數學歸納法證明. 首先我們第一步代入 $n=1$ 得 $a-b$. 當然是 $a-b$ 的倍數, 故成立. 第二步是直接假設 a^k-b^k 為 $a-b$ 的倍數, 要推得 $a^{k+1}-b^{k+1}$ 為 $a-b$ 的倍數. 所以我們要想辦法看看 $a^{k+1}-b^{k+1}$ 和 a^k-b^k 的關係. 為了要讓 $a^{k+1}-b^{k+1}$ 和 a^k-b^k 扯上關係, 我們自然將之寫成

$$a^{k+1}-b^{k+1}=aa^k-bb^k=aa^k-ab^k+ab^k-bb^k=a(a^k-b^k)+(a-b)b^k.$$

此時由假設 a^k-b^k 為 $a-b$ 的倍數, 我們可將 a^k-b^k 寫成 $(a-b)m$, 其中 m 為整數. 所以 $a^{k+1}-b^{k+1}=a(a-b)m+(a-b)b^k=(a-b)(am+b^k)$. 得證 $a^{k+1}-b^{k+1}$ 為 $a-b$ 的倍數. 故由數學歸納法知, 對任意的正整數 n, a^n-b^n 為 $a-b$ 的倍數 □

一般來說, 數學歸納法的第一步只是代值驗證, 應該沒問題. 而第二步就是一個若 P 則 Q 的證明, 可以利用前面 2.1 節介紹的方法證明. 在證明過程中若無法馬上看出 $P(k)$ 和 $P(k+1)$ 的關係, 可以嘗試先找出 $P(1),P(2)$ 的關係, $P(2),P(3)$ 的關係, 等. 再推敲出 $P(k)$ 和 $P(k+1)$ 的關係. 另外要謹記, 要單純從 $P(k)$ 成立推出 $P(k+1)$, 在這的過程中不能加入其他的假設. 我們看一個錯誤的例子.

Example 2.3.3. 以下的數學歸納法是要證明任意取 n 個數都會相等. 這個結論當然是錯的, 我們必須找出推論錯誤之處.

第一步: 任取一個數, 因為只有一個當然成立.

第二步: 假設任取 k 個數都會相等, 要證明任取 $k+1$ 個數也都會相等. 現任取 $k+1$ 個數, 將這些數留下一個設其值為 a, 而其他 k 個數放入袋中. 依假設袋中 k 個數都會相等設為 b. 現將袋中取出一個數, 再將當初留下的那個數 a 放入袋中. 依假設此時袋中這 k 個數都應相等, 故得 $a=b$. 因此依數學歸納法, 得證任意取 n 個數都會相等.

這個證明出錯的當然是在第二步. 它假設在袋中取出一個數後仍有 $k-1$ 個數在袋中. 然而當 $k=1$ 時, 此時袋中沒有東西, 最後放入袋中的數 a 無其他的數與之比較, 故無法得知 $a=b$. 所以雖然上面的論述當 $k\geq 2$ 時, 確實由假設 $P(k)$ 證得 $P(k+1)$ 對, 但在 $k=1$ 時就無法由 $P(k)$ 對推得 $P(k+1)$ 對. 這不符合數學歸納法要求對所有的正整數 k, 都要滿足若 $P(k)$ 對, 則 $P(k+1)$ 對. 所以論證是錯誤的。由這個例子我們建議，若要用數學歸納法，通常在驗證 $P(1)$ 對之後，不要馬上去證明 $P(k)\Rightarrow P(k+1)$, 而是想看看如何能單純由 $P(1)$ 是

對的推得 $P(2)$ 是對的。這樣不只能讓我們比較有想法知道如何去證明 $P(k) \Rightarrow P(k+1)$，也可避免如上述的錯誤。

有時有的性質並不會從 $n=1$ 開始就對, 例如當 $n \geq 5$ 時, 證明 $2^n > n^2$. 這裡數學歸納法若只能從 1 開始, 就無法處理了. 事實上, 依照 Theorem 2.3.1 的推論, 我們有以下更一般化的數學歸納法.

Corollary 2.3.4 (Extended Mathematical Induction)**.** 設 m 為整數. 假設以下兩個 *statement* 是對的

EI1: $P(m)$ 成立

EI2: 若 $k \geq m$ 為整數且 $P(k)$ 成立, 則 $P(k+1)$ 成立

那麼對任意大於等於 m 的整數 n 皆會使得 $P(n)$ 成立.

Proof. 事實上，可以學 Theorem 2.3.1 用 well-ordering principle 來證明，不過這裡我們想用 Theorem 2.3.1 來證明。首先令 $Q(n) = P(m+n-1)$. 因已知 $P(m)$ 成立, 故知 $Q(1) = P(m)$ 成立. 亦即 Q 滿足 Theorem 2.3.1 的條件 (I1). 接著我們檢查 Q 是否符合 Theorem 2.3.1 的條件 (I2), 也就是假設 $k \geq 1$ 為整數且 $Q(k)$ 成立, 是否可推得 $Q(k+1)$ 成立。現假設 $k \in \mathbb{N}$ 且 $Q(k)$ 成立, 此時 $m+k-1 \geq m$ 為整數, 且 $P(m+k-1) = Q(k)$ 成立, 故由 (EI2) 的假設得 $P(m+k) = Q(k+1)$ 成立. 我們證得, 若 $k \in \mathbb{N}$ 且 $Q(k)$ 成立, 則 $Q(k+1)$ 成立. 故由 Theorem 2.3.1 知對所有的 $n' \in \mathbb{N}$, $Q(n') = P(m+n'-1)$ 成立. 因此當 n 為大於等於 m 的整數時, 令 $n = m+n'-1$, 此時 $n' \in \mathbb{N}$, 故得 $P(n) = P(m+n'-1) = Q(n')$ 成立. □

這個 "extended mathematical induction" 我們用 Corollary 稱之, 是因為它可由 Theorem 2.3.1 直接推得. 事實上在 $m=1$ 的情況 Corollary 2.3.4 就是 Theorem 2.3.1, 所以我們知道 Theorem 2.3.1 和 Corollary 2.3.4 是 equivalent 的.

Example 2.3.5. 證明對任意正整數 n, 當 $n \geq 5$ 時, $2^n > n^2$.

Proof. 我們用 extended mathematical induction $m=5$ 且 $P(n)$ 為 $2^n > n^2$ 的情況證明. 當 $n=5$ 時, $2^5 = 32 > 25 = 5^2$, 故 $P(5)$ 成立. 假設 $k \geq 5$ 為整數且 $2^k > k^2$. 因 $2^{k+1} = 2 \times 2^k$, 故由 $2^k > k^2$ 之假設得 $2^{k+1} > 2k^2$. 而 $(k+1)^2 = k^2 + 2k + 1$ 若能證得 $2k^2 > k^2 + 2k + 1$, 則得證 $2^{k+1} > (k+1)^2$, 即 $P(k+1)$ 成立. 然而 $2k^2 > k^2 + 2k + 1$ 等同於 $k^2 - 2k > 1$, 又 $k^2 - 2k = k(k-2)$, 故由 $k \geq 5$ 得知 $k^2 - 2k > 1$. 我們證得了若 $k \geq 5$ 為整數且 $P(k)$ 成立, 則 $P(k+1)$ 成立, 故由 extended mathematical induction (Corollary 2.3.4) 得證對任意大於等於 5 的整數 n 皆會使得 $P(n)$, 即 $2^n > n^2$ 成立. □

Question 2.8. 在 *Example 2.3.5* 的證明中要用到 $k(k-2) > 1$. 不過此式在 $k=3$ 就會成立, 為何 $2^n > n^2$ 需要到 $n \geq 5$ 時才都會成立呢*?*

數學的理論推導，常常是由許多論證利用邏輯堆砌起來。因此在每一步驟，都應清楚這個步驟是在論證什麼。常見的錯誤就是不明究理，盲目的推導，最後連自己的論證對錯

都不知，甚至證出什麼都不曉得。若你能回答 Question 2.8 這樣的問題，那非常的好，表示你能注意到每一步驟在論證什麼。在 Example 2.3.5 我們是證明了當 $k \geq 3$ 時可由 $P(k)$ 成立推得 $P(k+1)$ 成立。它只告訴我們 $P(3)$ 成立的話 $P(4)$ 就會成立，並不表示 $P(3)$ 成立。事實上 $P(3)$, $P(4)$ 都不成立。然而我們知道 $P(5)$ 成立，而又 $5 > 3$, 所以可推得 $P(6)$ 成立，以至於對整個大於等於 5 的整數皆成立。同樣的道理，假如 $P(5)$ 成立，而在推導 $P(k) \Rightarrow P(k+1)$ 的過程中發現只有在 $k \geq 10$ 的情況成立。此時無法推得 $P(6)$ 成立，所以也就無法馬上下結論說 $P(n)$ 會對 $n \geq 5$ 都會成立了。但因為這裡僅剩幾個情況 (即 $6 \leq k \leq 10$) 需檢驗，若驗證它們都成立，當然就能下結論說 $P(n)$ 會對 $n \geq 5$ 都會成立。

Question 2.9. 假設當 $k \geq 10$ 皆會滿足 $P(k) \Rightarrow P(k+1)$. 試寫下在以下情況當 n 大於等於多少時，$P(n)$ 會成立（有可能無法確定）。

(1) $P(9)$ 成立。

(2) $P(11)$ 成立。

(3) $P(8), P(9), P(10)$ 成立。

(4) 當 n 是 3 的倍數時 $P(n)$ 皆成立。

在數學歸納法的證明中有時 $P(k)$ 對的條件不足以直接證明 $P(k+1)$ 對. 例如一些遞迴數列的問題, 有時需要之前更多項才能決定下一項的性質. 事實上當我們由 $P(1)$ 對證得 $P(2)$ 對, 再由 $P(2)$ 對要證 $P(3)$ 時, 其實 $P(1)$ 已經知道是對的, 所以我們不只有 $P(2)$ 對的前提, 我們還有 $P(1)$ 對. 同理在證得 $P(3)$ 對要證明 $P(4)$ 時, 其實 $P(1), P(2)$ 為對的條件也可以用上, 所以我們有以下條件更強的數學歸納法.

Corollary 2.3.6 (Strong Mathematical Induction)**.** 設 m 為整數. 假設以下兩個 *statement* 是對的

SI1: $P(m)$ 成立

SI2: 若 $k \geq m$ 為整數且 $P(m), P(m+1), \ldots, P(k-1), P(k)$ 皆成立, 則 $P(k+1)$ 成立

那麼對任意大於等於 m 的整數 n 皆會使得 $P(n)$ 成立.

Proof. 對於大於等於 m 的整數 n, 令 $Q(n) = P(m) \wedge P(m+1) \wedge \cdots \wedge P(n-1) \wedge P(n)$. 因假設 $P(m)$ 成立, 故知 $Q(m) = P(m)$ 成立，亦即 Q 滿足 Corollary 2.3.4 的條件 (EI1). 接著我們檢查 Q 是否符合 Corollary 2.3.4 的條件 (EI2), 也就是假設 $k \geq m$ 為整數且 $Q(k)$ 成立, 是否可推得 $Q(k+1)$ 成立。然而 $Q(k)$ 成立表示 $P(m), \ldots, P(k-1), P(k)$ 皆成立, 故由 (SI2) 的假設得 $P(k+1)$ 成立. 然而已知 $P(m), P(m+1), \ldots, P(k-1), P(k)$ 皆成立, 故知 $Q(k+1) = P(m) \wedge P(m+1) \wedge \cdots \wedge P(k) \wedge P(k+1)$ 成立. 我們證得, 若 $k \geq m$ 為整數且 $Q(k)$ 成立, 則 $Q(k+1)$ 成立. 故由 Corollary 2.3.4 知對任意大於等於 m 的整數 n 皆會使得 $Q(n)$ 成立. 然而 $Q(n)$ 成立表示 $P(m), P(m+1), \ldots, P(n-1), P(n)$ 皆成立, 自然 $P(n)$ 成立, 故得證當 n 為大於等於 m 的整數時, $P(n)$ 皆成立. □

Remark 2.3.7. Strong Mathematical Induction 的 (SI2) 一般我們可以改寫為：若 $k \geq m$ 為整數且對於滿足 $m \leq i \leq k$ 的整數 i, $P(i)$ 皆成立, 則 $P(k+1)$ 成立。

我們稱 Corollary 2.3.6 為 strong mathematical induction 意即它比 Theorem 2.3.1 強。在數學上，我們稱一個定理比另一個定理強，大致上的意思是它可以在更廣泛的情況使用。例如 Corollary 2.3.4 就比 Theorem 2.3.1 強，因為它可以應用在任意整數 m 起頭的情況，而不只是 1. 通常比較強的定理很容易就可推導出比較弱的。例如 Corollary 2.3.4 只要考慮 $m=1$ 的情況就可得 Theorem 2.3.1. 不過感覺上比較弱的定理，未必就真的比較弱。例如我們是用 Theorem 2.3.1 證得 Corollary 2.3.4, 所以邏輯上來說他們是等價的，沒有誰強誰弱之分。不過在使用上當然 Corollary 2.3.4 比較方便。

同樣的 Corollary 2.3.6 直觀上也比 Corollary 2.3.4 強（因為 (SI2) 的條件比較多比較好使用）。我們可以很容易用 Corollary 2.3.6 來證明 Corollary 2.3.4. 事實上當 P 符合 Corollary 2.3.4 的 (EI1), (EI2), 我們希望證明 P 也會符合 Corollary 2.3.6 的 (SI1), (SI2) 因此由 Corollary 2.3.6 的結論得到 $P(n)$ 對所有 $n \geq m$ 都成立。其實 (EI1) 和 (SI1) 是一樣的，所以只要探討 P 若符合 (EI2) 是否會符合 (SI2), 也就是假設 $P(m),\ldots,P(k-1),P(k)$ 成立是否可得 $P(k+1)$ 成立。然而由這個假設當然表示 $P(k)$ 成立，而又已知 P 符合 (EI2), 也就是 $P(k)$ 成立的話 $P(k+1)$ 一定成立，也因此推得 P 確實符合 (SI2)。另一方面 Corollary 2.3.6的證明是利用 Corollary 2.3.4 證得的，也因此知它們是等價的。最後由等價的遞移性，我們知這裡介紹的三個數學歸納法都是等價的。這是從邏輯的觀點來看（它們沒有強弱之分），實際在證明時當然是挑最適合的來證明。下一個例子我們可以看出，應該用 strong mathematical induction 來證明較合適。

Example 2.3.8. 證明所有大於 1 的整數都可以寫成有限多個質數的乘積.

或許很多同學會用以下的方法證明. 設 n 為大於 1 的整數, 若 n 為質數, 則 n 符合可寫成有限多個質數乘積. 若 n 不是質數, 依定義 n 可以寫成兩個比 n 小但大於 1 的整數相乘, 這樣一直下去可證得可以寫成有限多個質數的乘積. 相信大家都能接受這樣的說法來解釋這個性質是對的. 但它並不是好的證明, 比方說如何“一直下去”且為何這個程序經有限多次後會停止 (這樣才能說是有限多個質數的乘積) 也要說明清楚. 有了數學歸納法, 就是能幫我們解決這些不容易說清楚的地方. 在這個例子, 若我們僅假設 k 可以寫成有限多個質數乘積, 是無法證得 $k+1$ 可以寫成有限多個質數乘積, 所以我們必須用 strong mathematical induction 來證明.

Proof. 當 $n=2$ 時, 因 2 為質數, 故成立. 假設當 $k \geq 2$ 時對所有滿足 $2 \leq i \leq k$ 的整數 i 都可以寫成有限多個質數的乘積. 現考慮 $k+1$ 的情形. 因為 $k+1$ 是質數時自然成立, 所以我們僅需考慮 $k+1$ 不為質數的情形. 此時 $k+1=ab$, 其中 $1<a,b\leq k$. 故由前歸納之假設知 a,b 皆為有限多個質數的乘積, 因此 $k+1=ab$ 自然可以寫成有限多個質數的乘積. 故由 strong mathematical induction 知所有大於 1 的整數都可以寫成有限多個質數的乘積. □

在利用數學歸納法證明的過程中, 最重要且最難的部分就是第二步驟由假設 $P(k)$ 成立 (或 $P(m),P(m+1),\ldots,P(k)$ 成立) 證得 $P(k+1)$ 成立. 這裡常常在推導的過程中發現 k 要在某些範圍內才會對. 例如在 Example 2.3.3 的錯誤示範中, 其實“任取 k 個數相等推得任取 $k+1$ 個數會相等”的證明在 $k \geq 2$ 時是對的. 所以此時若能再補上 $k=1$ 的情況也對, 整個

證明就完成了 (當然在 Example 2.3.3 這個例子這是不可能做到的). 前面提過，當我們在處理第二步驟時, 若發現 k 要有所限制才能對, 此時我們可以多檢查那些 k 無法涵蓋的情況, 若這些情況也都對, 就完成歸納法的證明了. 總之, 在數學歸納法的證明中, 有時並不是僅檢查初始的情況就好, 我們再多看一些例子。

Example 2.3.9. 考慮所謂的 *Fibonacci sequence* $\{F_0, F_1, F_2, \dots\}$, 即 $F_0 = 0, F_1 = 1$ 且對任意 $i \geq 2$, F_i 滿足 $F_i = F_{i-1} + F_{i-2}$. 證明 $F_n < 2^{n-2}$, for $n \geq 4$.

很顯然地, 因 F_{k+1} 的值由 F_k 和 F_{k-1} 所決定, 我們無法僅由 F_k 來推得 F_{k+1}. 所以這裡我們用 strong mathematical induction 來處理. 依定義 $F_2 = F_1 + F_0 = 1, F_3 = F_2 + F_1 = 1 + 1 = 2$, 故當 $n = 4$ 時, $F_4 = F_3 + F_2 = 2 + 1 = 3$, 所以 $F_4 = 3 < 2^{4-2} = 4$ 成立. 現假設 $k \geq 4$ 且對所有 $4 \leq i \leq k$, 皆有 $F_i < 2^{i-2}$. 此時 $F_{k+1} = F_k + F_{k-1}$. 我們希望用到 $F_k < 2^{k-2}$ 和 $F_{k-1} < 2^{(k-1)-2} = 2^{k-3}$ 的假設推得 $F_{k+1} < 2^{(k+1)-2} = 2^{k-1}$. 不過當 $k = 4$ 時, $i = k - 1$ 並不符合 $4 \leq i \leq k$, 所以此時無法使用 $F_{k-1} < 2^{k-3}$ 的假設 (事實上此時 $F_{k-1} = F_3 = 2 = 2^{4-3}$). 所以我們再補上 $k = 4$ 的情況, 即直接驗證 $F_{k+1} = F_5 = F_4 + F_3 = 5 < 2^{5-2} = 8$, 才可完成證明.

Proof. 首先直接驗證得 $F_4 = 3 < 2^{4-2}, F_5 = 5 < 2^{5-2}$.

現假設 $k \geq 5$ 且對任意 $i = 4, 5, \dots, k$ 皆有 $F_i < 2^{i-2}$. 因為 $4 \leq k - 1 \leq k$ 且 $4 \leq k \leq k$, 我們有 $F_k < 2^{k-2}, F_{k-1} < 2^{(k-1)-1} = 2^{k-3}$, 故得

$$F_{k+1} = F_k + F_{k-1} < 2^{k-2} + 2^{k-3} = 2^{k-3}(2+1) < 4 \times 2^{k-3} = 2^{k-1} = 2^{(k+1)-2}.$$

依數學歸納法得證 $F_n < 2^{n-2}$, for $n \geq 4$. □

在下一個例子中, 我們想證明所有大於 20 的整數都可以寫成 4 和 5 的正整數倍之和. 也就是證明若 $n > 20$, 則存在正整數 l, m 使得 $n = 4l + 5m$. 或許同學會想到 $1 = 5 - 4$, 所以若 $k = 4l + 5m$, 則 $k + 1 = 4l + 5m + (5 - 4) = 4(l - 1) + 5(m + 1)$. 不錯, 用這個方法可以證明所有的整數皆可以寫成 4 的倍數和 5 的倍數之和, 但我們要求的是寫成 4 和 5 的正整數倍之和. 因此無法用這方法證明。不過觀察一下發現若 $k = 4l + 5m$, 則 $k + 4n = 4(l + n) + 5m$, 所以我們可以先驗證 $21, 22, 23, 24$ 都可以寫成 4 和 5 的正整數倍之和, 就可利用 proof by cases 將所有大於 20 的正整數分成 $21 + 4n, 22 + 4n, 23 + 4n, 24 + 4n$ 來探討，而得證。根據這個想法，我們用 strong mathematical induction 來證明。

Example 2.3.10. 證明若 n 為整數且 $n > 20$, 則存在 l, m 為正整數滿足 $n = 4l + 5m$.

Proof. 由於 $21 = 4 \times 4 + 5 \times 1$, $22 = 4 \times 3 + 5 \times 2$, $23 = 4 \times 2 + 5 \times 3$ 和 $24 = 4 \times 1 + 5 \times 4$ 故知當 $n = 21, 22, 23, 24$ 時成立. 現假設 $k \geq 24$ 時對於所有滿足 $21 \leq i \leq k$ 的整數 i, 皆存在正整數 l, m 使得 $i = 4l + 5m$. 考慮 $k + 1$ 的情形, 由於 $k + 1 = (k - 3) + 4$, 且 $i = k - 3$ 滿足 $21 \leq i \leq k$, 故存在正整數 l, m 使得 $k - 3 = 4l + 5m$, 得 $k + 1 = 4l + 5m + 4 = 4(l + 1) + 5m$. 由數學歸納法知, 當 n 為大於 20 的整數, 存在 l, m 為正整數滿足 $n = 4l + 5m$. □

數學歸納法是一個很好使用的數學工具. 它不只可以拿來處理整數的問題, 其實很多可以用整數分類的問題都可以用數學歸納法處理. 例如代數中許多有關於多項式的問題, 我們

Chapter 3

Set

集合的理論是所有數學理論的基礎系統. 在這一章中我們將簡單的介紹集合的一些基本理論. 我們採用較自然及直覺的方式介紹集合論, 而不涉及抽象的公設結構.

3.1. Basic Definition

首先我們介紹有關集合的基本定義, 並了解集合之間的關係.

集合和元素是數學最基本的名詞, 嚴格說起來它是無法定義清楚的. 這裡我們就不去定義集合, 而採用較直觀的說法. 所謂一個集合 (英文稱之為 *set*) 就是一些事物收集起來的結果, 而組成這個集合的事物, 我們稱為此集合的元素 (英文稱之為 *element*). 通常我們會用英文大寫來表示一個 set, 例如 A,B,S 等, 而用小寫字母來表示 set 裡的元素. 不過有些數學常用的集合大家都習慣用特定的符號表示. 例如: $\mathbb{N}$ 表示所有自然數所成的集合, $\mathbb{Z}$ 為整數所成的集合, $\mathbb{Q}$ 表示有理數所成的集合, 而所有實數所成的集合我們用 $\mathbb{R}$ 來表示. 若 x 為集合 S 裡的一個元素, 我們就用 $x \in S$ 來表示, 稱之為 x *belongs to* S (即 x 屬於 S). 若 x 不在 S 中, 我們就用 $x \notin S$ 來表示.

在數學上, 我們希望一個 set 是要明確的知道哪些是它的 element 哪些不是它的 element. 也就是說給定一集合 S, 對於任意的 x, 我們必須明確知道 $x \in S$ 是對的還是錯的. 一般來說, 一個集合若僅有有限多個元素, 我們便可以一一將它們列舉出來. 例如 $S = \{1,2,3\}$ 表示的就是有 3 個元素的集合, 其元素為 1,2 和 3. 這裡 S 是一個集合, 例如我們知道 $1 \in S$, 而 $4 \notin S$. 有時一個集合我們無法一一列舉出它的元素, 此時我們便用所謂 *set-builder notation* 來表示其元素. 它的表示法通常為 $\{x : P(x)\}$ 這樣的形式, 其中冒號 : 左邊的 x 表示我們要用 x 來表示此集合的元素, 而冒號 : 右邊的 $P(x)$ 指的是這個集合裡的元素 x 需滿足 $P(x)$. 也就是說 $\{x : P(x)\}$ 這個集合便是收集所有滿足 $P(x)$ 的 x 所成的集合.

在探討集合相關性質之前, 首先我們必須定義何謂集合的相等, 以及集合間的包含關係.

Definition 3.1.1. 設 A,B 為集合. 如果 B 中的 element 皆為 A 的 element, 我們稱 B 為 A 的 *subset* (子集合), 也稱 B is *contained* in (包含於) A, 記為 $B \subseteq A$. 若 $B \subseteq A$ 且 $A \subseteq B$, 則稱 A,B 為 *equal*, 記為 $A = B$. 另外若 $B \subseteq A$ 但 $B \neq A$, 則稱 B 為 A 的 *proper subset*, 記為 $B \subset A$.

注意 subset 和 proper set 的符號 "$\subseteq$" 和 "$\subset$", 許多參考書籍的符號並不一致, 請在閱讀時注意.

依定義若要證明 $B \subseteq A$, 我們必須說明任意 B 中的元素 x, 皆會是 A 的元素, 所以用數學的表示法就是要證明 "$x \in B \Rightarrow x \in A$". 而要證明 $A = B$ 的話就是等同於證明 "$x \in B \Leftrightarrow x \in A$". 從這裡得知, 兩集合的包含關係以及相等, 只與元素是否屬於該集合有關, 和集合的表示法無關. 例如以下的例子:

Example 3.1.2. 令 $A = \{1,2,2\}$, $B = \{1,2,3\}$, $C = \{3,3,1,2\}$, $D = \{n \in \mathbb{N} : 1 \leq n \leq 3\}$, $E = \{2,4\}$.

由於 A 僅有 1,2 兩個元素, 而 $1 \in B$ 且 $2 \in B$, 故知 $A \subseteq B$. 又 $3 \in B$ 但 $3 \notin A$, 知 B 不包含於 A, 故得 $A \subset B$. 同理我們知 $B = C$.

現若 $x \in B$, 則知 $x \in \mathbb{N}$ 且 $1 \leq x \leq 3$, 故得 $x \in D$. 得證 $B \subseteq D$. 另一方面, 若 $x \in D$ 表示 $x \in \mathbb{N}$ 且 $1 \leq x \leq 3$, 所以 $x = 1,2,3$ 皆在 B 中, 得證 $D \subseteq B$, 由此知 $B = D$.

最後因 $1 \in B$ 但 $1 \notin E$, 我們知 B 不是 E 的 subset. 同樣的, 因 $4 \in E$ 但 $4 \notin B$, 我們知 E 也不是 B 的 subset.

當 A,B 為 sets, 但 B 不是 A 的 subset 時, 我們也用 $B \nsubseteq A$ 來表示. 所以如果 $B \subseteq A$ 但 $A \nsubseteq B$, 依定義我們得 $B \subset A$.

Question 3.1. 假設 $P(x)$, $Q(x)$ 皆為 *statement form.* 令 $P = \{x : P(x)\}$ 且 $Q = \{x : Q(x)\}$ 試證明以下性質:

(1) $P \subseteq Q$ 若且唯若 $P(x) \Rightarrow Q(x)$.

(2) $P = Q$ 若且唯若 $P(x) \Leftrightarrow Q(x)$.

為了將來探討集合間的關係方便, 我們定義兩個特殊的集合. 首先, 當我們所探討的問題都是某個特定集合的元素或其 subset 時, 為了方便我們定此特定集合為 *universal set* (宇集). 例如當我們談論的是有關於實數, 我們就可以說 $\mathbb{R}$ 為我們的 universal set. 如此便可以不必每次都要去提類似如 $x \in \mathbb{R}$ 這樣的事. 不過 universal set 可以因所探討的問題不同而改變, 例如在 a,b 為整數時, 我們可以在 universal set 為 $\mathbb{Q}$ 時談論 $ax + b = 0$ 的解. 但談論 $ax^2 + b = 0$, 就可能要令 universal set 為 $\mathbb{R}$ 或複數 $\mathbb{C}$ 才有意思. 不管如何, 當我們發現要探討的集合都是某一個特定集合的子集合時, 明確的將之訂定為 universal set 確有其方便性. 不過當我們訂定 universal set 之後, 所有談論的 set 就必須是此 universal set 的 subset.

另一個我們需要定義的是所謂 *empty set* (空集合). 它是一個沒有任何元素的集合, 我們用 $\emptyset$ 來表示. 或許大家會疑惑 $\emptyset$ 有符合集合的要求嗎? 其實由於我們可以明確的知道所有的元素皆不屬於空集合, 所以它並未違背當初我們說的 "明確知道 $x \in \emptyset$ 是對或錯" 的要求. 由於我們將來要探討集合的一些如交集等的 operations, 因此將 $\emptyset$ 視為一集合確有其必要性. 關於 universal set 和 empty set, 我們有以下的性質.

Proposition 3.1.3. 假設 X 為 *universal set* 且 A 為 *set.* 則 $A \subseteq X$ 且 $\emptyset \subseteq A$.

Proof. 依定義 X 為 universal set, 故 A 為 X 的 subset, 得 $A \subseteq X$. 另一方面, 要證明 $\emptyset \subseteq A$ 等同於要證明若 $x \in \emptyset$ 則 $x \in A$. 但不可能會有 $x \in \emptyset$ 的情形發生, 故由當 P 錯時 $P \Rightarrow Q$ 恆對的邏輯規則知 "$x \in \emptyset \Rightarrow x \in A$" 為正確故知 $\emptyset \subseteq A$. □

Question 3.2. 在此 *Question* 中令 X 為 *universal set.* 試問 *universal set* 是否唯一? 又 *empty set* 是否唯一?

一般數學上定義了一些名詞後, 接著便是要探討這些名詞相關的性質, 接下來我們便是要談論有關 subset 的基本性質.

Proposition 3.1.4. 假設 A,B,C 為 *sets,* 我們有以下的性質.

(1) $A \subseteq A$.

(2) 若 $A \subseteq B$ 且 $B \subseteq C$, 則 $A \subseteq C$.

Proof. (1) 假設 $x \in A$, 自然有 $x \in A$, 故得 $A \subseteq A$.

(2) 設 $x \in A$, 由 $A \subseteq B$ 得 $x \in B$. 又由 $B \subseteq C$ 得 $x \in C$. 綜言之, 對於任意 $x \in A$ 必有 $x \in C$, 得證 $A \subseteq C$. □

Question 3.3. 試利用 *Proposition 3.1.4* 證明若 $A = B$ 且 $B = C$, 則 $A = C$.

Question 3.4. 假設 A,B,C 為 *sets,* 下列哪些是對的?

(1) 若 $A \subset B$ 且 $B \subseteq C$, 則 $A \subseteq C$.

(2) 若 $A \subseteq B$ 且 $B \subseteq C$, 則 $A \subset C$.

(3) 若 $A \subset B$ 且 $B \subset C$, 則 $A \subseteq C$.

(4) 若 $A \subset B$ 且 $B \subseteq C$, 則 $A \subset C$.

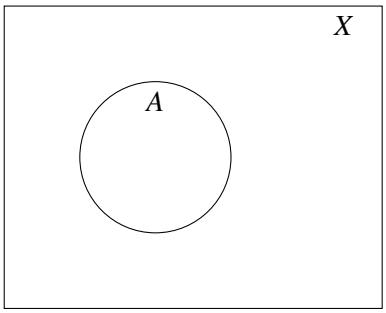
再強調一次, 當要證明 $A = B$ 時必須 $A \subseteq B$ 以及 $B \subseteq A$ 兩個方向都證明才行. 尤其在處理解方程式的情形, 我們都會設未知數為解然後解方程式, 同學常常弄不清楚是處理哪一邊的包含關係或常常忘了處理另一邊的包含關係. 我們看以下的例子.

Example 3.1.5. 令 $A = \{(x,y) \in \mathbb{R}^2 : x^2 - x = y = 2\}$ 且 $B = \{(2,2),(-1,2)\}$. 證明 $A = B$.

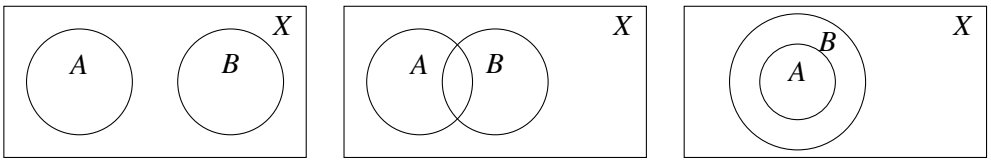
Proof. 設 $(x,y) \in A$, 表示 $x^2 - x = 2$ 且 $y = 2$, 故得 $x = 2$ 或 $x = -1$ 且 $y = 2$. 此表示若 $(x,y) \in A$, 則 $(x,y) = (2,2)$ 或 $(x,y) = (-1,2)$. 故知 $(x,y) \in B$, 亦即得證 $A \subseteq B$. 接著設 $(x,y) \in B$, 知 $(x,y) = (2,2)$ 或 $(x,y) = (-1,2)$ 代入皆符合 $x^2 - x = y = 2$, 故知 $(x,y) \in A$. 得證 $B \subseteq A$, 故知 $A = B$ □

Question 3.5. 令 $A = \{x \in \mathbb{R} : \sqrt{x} = x - 2\}$, $B = \{1\}$, $C = \{4\}$, $D = \{1,4\}$. 試寫下 A,B,C,D 相互間的包含關係.

我們可以利用所謂的 *Venn diagrams* 來幫助我們了解集合間的關係. 大致上, 我們先畫一個框框表示 universal set, 然後在此框框內畫一個封閉區域 (一般是畫一個圓) 表示一個 set. 例如下圖就是表示在宇集 X 中的一個 set A.

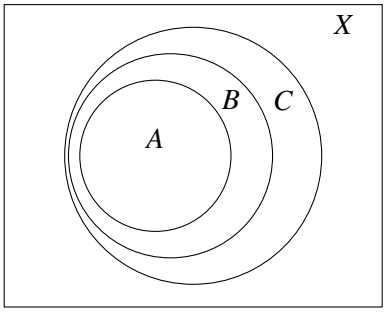


我們可以用 Venn diagrams 來表示兩個集合 A,B 之間三種可能的關係如下.



最左邊圖示表示的是 A,B 沒有共同的元素, 中間圖示表示的是 A,B 有共同元素但互相沒有包含關係, 而最右邊表示的是 $A \subseteq B$.

有時 Venn diagrams 可以幫助我們了解一些集合的性質, 甚至給我們證明這些性質的提示. 例如以下的圖示便可以幫助我們理解 Proposition 3.1.4 (2) 若 $A \subseteq B$ 且 $B \subseteq C$, 則 $A \subseteq C$ 這個性質.



當然了 Venn diagrams 只是讓我們參考用, 絕不能只是畫個圖就以為證明完成.

Question 3.6. 假設 A,B,C 為 *sets.* 已知 $A \subseteq B$. 若 B 和 C 沒有共同的元素, 畫出可能的 *Venn diagrams.* 是否可以確定 A 和 C 沒有共同元素? 又若 B 和 C 有共同的元素, 畫出可能的 *Venn diagrams,* 是否可確定 A 和 C 有共同元素? 同樣的, 從 A,C 有沒有共同元素的情況畫出可能的 *Venn diagrams,* 並探討是否依此可確定 B,C 有沒有共同元素.

最後提醒大家千萬不要把 "$\in$" (屬於) 和 "$\subseteq$" (包含於) 弄混淆. "$\in$" 指的是元素和集合之間的關係, 而 "$\subseteq$" 指的是兩集合間的關係. 對於集合我們有 $A \subseteq B$ 且 $B \subseteq C$ 則 $A \subseteq C$ 的性質, 但對於元素 $A \in B$ 且 $B \in C$ 未必可得 $A \in C$. 例如

$$A = \{1\}, \quad B = \{\{1\}\}, \quad C = \Big\{\{\{1\}\}\Big\}.$$

我們有 $A \in B$ 且 $B \in C$, 但很明顯的 $A \notin C$.

3.2. Set Operations

所謂 set operation, 就是利用兩個已知的集合得到另一個集合的方法. 我們將介紹集合間幾種重要的 operations, 即 intersection, union 和 set difference, 並探討這幾種 set operations 之間重要的性質.

3.2.1. Intersection and Union. 首先我們定義 intersection 與 union.

Definition 3.2.1. 設 A,B 為 sets. 我們令 $A\cap B=\{x:x\in A \text{ and } x\in B\}$ 稱之為 the *intersection* of A and B (A 和 B 的交集). 令 $A\cup B=\{x:x\in A \text{ or } x\in B\}$ 稱之為 the *union* of A and B (A 和 B 的聯集).

簡單的說 $A\cap B$ 就是將 A,B 共同的元素收集起來所得的集合, 而 $A\cup B$ 是將 A,B 所有的元素收集起來而得的元素. 例如以下的例子.

Example 3.2.2. 令 $A=\{1,2,3\}$, $B=\{2,4,6\}$. 由於只有 2 是同時屬於 A 且屬於 B, 所以得 $A\cap B=\{2\}$. 而 1,3 雖沒有在 B 但都屬於 A, 符合屬於 A 或屬於 B 的條件故知 1,3 皆屬於 $A\cup B$. 同理 4,6 亦屬於 $A\cup B$. 至於 2 既然同時屬於 A 和 B 當然符合屬於 A 或屬於 B 的條件, 故知 2 也屬於 $A\cup B$. 又由於沒有其他的數在 A 中或 B 中, 我們可以確定 $A\cup B=\{1,2,3,4,6\}$.

聯集和交集與原來的集合是有關係的. 例如在上面的例子中我們有 $A\cap B=\{2\}\subseteq A=\{1,2,3\}$ 以及 $B=\{2,4,6\}\subseteq A\cup B=\{1,2,3,4,6\}$. 事實上, 若 $x\in A\cap B$, 表示 $x\in A$ 且 $x\in B$, 故知 x 一定屬於 A 且 x 一定屬於 B, 所以我們有

$$(A\cap B)\subseteq A \quad \text{and} \quad (A\cap B)\subseteq B. \tag{3.1}$$

注意 $A\cap B$ 有可能是空集合, 此時我們稱 A,B 為 *disjoint*. 不過空集合包含於任意的集合, 所以當 A,B 為 disjoint 時上式仍然成立. 另一方面若 $x\in A$, 則 x 必屬於 A 或 B, 所以 $x\in A\cup B$ 成立. 我們有

$$A\subseteq(A\cup B) \quad \text{and} \quad B\subseteq(A\cup B) \tag{3.2}$$

Question 3.7. 試證明 $(A\cap A)=A$ 以及 $(A\cup A)=A$.

交集和聯集在某種程度上可以說是保持包含關係的, 事實上我們有以下的性質.

Proposition 3.2.3. 設 A,B,C,D 皆為 *sets* 滿足 $A\subseteq B$ 且 $C\subseteq D$. 則

$$(A\cap C)\subseteq(B\cap D) \quad \text{and} \quad (A\cup C)\subseteq(B\cup D).$$

Proof. 因 $A\subseteq B$, 可由 $x\in A$ 得 $x\in B$. 同理因 $C\subseteq D$, 可由 $x\in C$ 得 $x\in D$. 現若 $x\in A\cap C$, 表示 $x\in A$ 且 $x\in C$. 故可得 $x\in B$ 且 $x\in D$. 得證 $(A\cap C)\subseteq(B\cap D)$. 同理, 若 $x\in A\cup C$, 表示 $x\in A$ 或 $x\in C$. 當 $x\in A$ 時可得 $x\in B$, 而當 $x\in C$ 時可得 $x\in D$. 故由 $x\in A\cup C$ 可得 $x\in B\cup D$. 得證 $(A\cup C)\subseteq(B\cup D)$. □

特別的, 當 $A \subseteq B$ 且 $A \subseteq D$ 時, 我們可以考慮 $C = A$ 的情形套用 Proposition 3.2.3 得 $(A \cap A) \subseteq (B \cap D)$. 又由於 $(A \cap A) = A$, 得知 $A \subseteq (B \cap D)$. 同理, 當 $A \subseteq B$ 且 $C \subseteq B$ 時, 我們有 $(A \cup C) \subseteq (B \cup B)$. 又由於 $(B \cup B) = B$, 得知 $(A \cup C) \subseteq B$. 我們證得以下性質. 由於這個結果是由 Proposition 3.2.3 簡單推導而得, 我們就用 *corollary* (引理) 稱之.

Corollary 3.2.4. 假設 A, B, C, D, E 為 *sets.*

(1) 若 $A \subseteq B$ 且 $A \subseteq C$, 則 $A \subseteq (B \cap C)$.

(2) 若 $D \subseteq A$ 且 $E \subseteq A$, 則 $(D \cup E) \subseteq A$.

Question 3.8. 試直接證明 *Corollary 3.2.4,* 並用此結果推導出 *Proposition 3.2.3.*

我們也可利用交集或聯集來判斷兩集合的包含關係. 我們有以下的結果.

Proposition 3.2.5. 假設 A, B 為 *sets.* 則以下是 *equivalent.*

(1) $A \subseteq B$.

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

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

Proof. 我們證明 (1) $\Leftrightarrow$ (2) 以及 (1) $\Leftrightarrow$ (3).

(1) $\Leftrightarrow$ (2): 假設 $A \subseteq B$, 我們要證明 $(A \cap B) = A$. 事實上由式子 (3.1) 我們知 $(A \cap B) \subseteq A$, 故僅要證明 $A \subseteq (A \cap B)$. 然而已知 $A \subseteq A$ 以及 $A \subseteq B$, 故由 Corollary 3.2.4 得 $A \subseteq (A \cap B)$. 因此證明了 (1) $\Rightarrow$ (2). 另一方面, 由式子 (3.1) 我們知 $(A \cap B) \subseteq B$. 故由 $A = (A \cap B)$ 可得 $A \subseteq B$, 證明了 (2) $\Rightarrow$ (1).

(1) $\Leftrightarrow$ (3): 假設 $A \subseteq B$, 我們要證明 $(A \cup B) = B$. 事實上由式子 (3.2) 我們知 $B \subseteq (A \cup B)$, 故僅要證明 $(A \cup B) \subseteq B$. 然而已知 $A \subseteq B$ 以及 $B \subseteq B$, 故由 Corollary 3.2.4, 得 $(A \cup B) \subseteq B$. 因此證明了 (1) $\Rightarrow$ (3). 另一方面, 由式子 (3.2) 我們知 $A \subseteq (A \cup B)$. 故由 $(A \cup B) = B$ 可得 $A \subseteq B$, 證明了 (3) $\Rightarrow$ (1). □

由 Definition 3.2.1 我們知道 "交集" 和邏輯的 "and" 有關, 而 "聯集" 和 "or" 有關. 所以我們很容易推得以下的關係:

(1) $A \cap B = B \cap A$.

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

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

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

由於 (3) 的關係, 以後多個集合的交集我們便省略括弧不必去強調哪幾個先作交集, 例如直接寫成 $A \cap B \cap C$. 同理由於 (4), 以後多個集合的聯集我們也省略括弧, 例如直接寫成 $A \cup B \cup C$.

利用邏輯 $\wedge,\vee$ 之間的分配性質, 即

$$((P\wedge Q)\vee R)\sim((P\vee R)\wedge(Q\vee R)),\quad ((P\vee Q)\wedge R)\sim((P\wedge R)\vee(Q\wedge R)),$$

我們有以下的性質.

Proposition 3.2.6. 假設 A,B,C 為 *sets,* 則

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

Proof. 首先由 $(A\cap B)\subseteq A$ 以及 $C\subseteq C$ 利用 Proposition 3.2.3 得 $((A\cap B)\cup C)\subseteq(A\cup C)$. 同理知 $((A\cap B)\cup C)\subseteq(B\cup C)$. 再利用 Corollary 3.2.4 得 $((A\cap B)\cup C)\subseteq(A\cup C)\cap(B\cup C)$. 另一方面假設 $x\in(A\cup C)\cap(B\cup C)$ 表示 $x\in A\cup C$ 且 $x\in B\cup C$. 我們利用 proof in cases, 考慮 $x\in C$ 和 $x\notin C$ 這兩種情況. 若 $x\in C$, 則當然 $x\in(A\cap B)\cup C$. 而若 $x\notin C$, 則由 $x\in A\cup C$ 且 $x\in B\cup C$, 知 $x\in A$ 且 $x\in B$, 亦即 $x\in A\cap B$. 故此時仍有 $x\in(A\cap B)\cup C$. 也就是說不管哪種情況, 我們都可以由 $x\in(A\cup C)\cap(B\cup C)$ 推得 $x\in(A\cap B)\cup C$, 得證 $((A\cup C)\cap(B\cup C))\subseteq(A\cap B)\cup C$. 故知 $((A\cap B)\cup C)=(A\cup C)\cap(B\cup C)$.

至於 $((A\cup B)\cap C)=(A\cap C)\cup(B\cap C)$ 的證明, 首先由 $A\subseteq(A\cup B)$ 以及 $C\subseteq C$ 利用 Proposition 3.2.3 得 $(A\cap C)\subseteq((A\cup B)\cap C)$, 同理我們有 $(B\cap C)\subseteq((A\cup B)\cap C)$. 故由 Corollary 3.2.4 知 $(A\cap C)\cup(B\cap C)\subseteq((A\cup B)\cap C)$. 另一方面, 若 $x\in(A\cup B)\cap C$, 表示 $x\in A\cup B$ 且 $x\in C$. 由 $x\in A\cup B$, 我們知 $x\in A$ 或 $x\in B$. 當 $x\in A$ 時, 由於已知 $x\in C$, 故得 $x\in A\cap C$. 此時自然有 $x\in(A\cap C)\cup(B\cap C)$. 同理, 當 $x\in B$ 時, 可得 $x\in B\cap C$. 因此也有 $x\in(A\cap C)\cup(B\cap C)$, 得證 $((A\cup B)\cap C)\subseteq(A\cap C)\cup(B\cap C)$. 故知 $((A\cup B)\cap C)=(A\cap C)\cup(B\cap C)$ □

Question 3.9. 試利用 *Proposition 3.2.5* 中 $(1)\Rightarrow(2)$ 的結果以及 *Proposition 3.2.6* 證明 *Proposition 3.2.5* 中 $(2)\Rightarrow(3)$.

3.2.2. Set Difference. 我們定義何謂 set difference.

Definition 3.2.7. 假設 A,B 為 sets, 定義 $A\setminus B=\{x:x\in A\text{ and }x\notin B\}$, 稱之為 the *set difference* of B in A (B 在 A 中的差集). 若 X 為 universal set, 則令 $A^c=X\setminus A=\{x:x\notin A\}$ 稱之為 the *complement* of A (A 的補集).

注意 A^c 的定義原本應為 $\{x:x\in X\text{ and }x\notin A\}$, 但因 X 為 universal set, 我們知道所有元素皆在 X 中, 故省略 $x\in X$ 直接寫 $x\notin A$. 所以在使用補集時要特別注意是否已明確說明了什麼是宇集, 否則會有符號不唯一的問題. 例如若 $\mathbb{Q}$ 為宇集, 則 $\mathbb{Q}^c=\emptyset$, 而當宇集為 $\mathbb{R}$ 時, $\mathbb{Q}^c$ 就是所有無理數所成的集合了.

利用補集的符號, 依定義我們有 $A\setminus B=A\cap B^c$, 從這裡我們知道一般的情況 $A\setminus B$ 和 $B\setminus A$ 是不相同的. 事實上我們有 $(A\setminus B)\cap(B\setminus A)=\emptyset$. 這是因為很明顯的 $A\cap A^c=\emptyset$ 且 $B\cap B^c=\emptyset$, 故知

$$(A\setminus B)\cap(B\setminus A)=(A\cap B^c)\cap(B\cap A^c)=(A\cap A^c)\cap(B\cap B^c)=\emptyset.$$

Example 3.2.8. 假設 $X=\{1,2,3,4,5,6\},A=\{1,2,3\},B=\{2,4,6\}$. 因 $1,3\in A$ 且 $1\notin B$ 且 $3\notin B$, 知 $1,3\in A\setminus B$. 雖然 $2\in A$ 但是 $2\in B$, 故 $2\notin A\setminus B$. 得 $A\setminus B=\{1,3\}$. 同理可得

$B\setminus A=\{4,6\}$. 我們有 $(A\setminus B)\cap(B\setminus A)=\{1,3\}\cap\{4,6\}=\emptyset$. 又 $1,3,5\in X$ 且 $1,3,5$ 皆不在 B 中, 故知 $1,3,5\in B^c$. 而 $2,4,6\in B$ 故 $2,4,6$ 皆不屬於 B^c, 得 $B^c=\{1,3,5\}$. 最後考慮 $A\cap B^c$ 得 $A\cap B^c=\{1,2,3\}\cap\{1,3,5\}=\{1,3\}=A\setminus B$.

接下來我們看 set difference 的一些性質，其實這些性質我們可以用元素的方式證明，不過在證明時由於常出現否定的問題所以經常要用反證法，如此反反覆覆，容易搞混。但如使用補集符號，就可以化繁為簡。所以我們先介紹有關於補集的一些性質，再處理差集的問題。

Proposition 3.2.9. 假設 A,B 為 *sets,* 我們有以下的性質.

(1) $(A^c)^c=A$.

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

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

(4) $A\subseteq B$ 若且唯若 $B^c\subseteq A^c$.

Proof. 這些性質都可以利用前面邏輯相關的 equivalence 推導. 我們主要使用的方式就是 $x\notin A$ 是 $x\in A$ 的否定，所以

$$(x\in A^c)\sim(x\notin A)\sim\neg(x\in A).$$

(1) $x\in(A^c)^c$ 表示 $x\notin A^c$, 即 $\neg(x\in A^c)$. 等同於 $\neg(x\notin A)$, 亦即 $\neg(\neg(x\in A))$. 因此由式子 (1.7), 知此與 $x\in A$ 等價，故得證。

(2) $x\in(A\cap B)^c\sim\neg(x\in(A\cap B))\sim\neg((x\in A)\wedge(x\in B))$. 由式子 (1.8) 知此與 $\neg(x\in A)\vee\neg(x\in B)$ 等價，亦即 $(x\in A^c)\vee(x\in B^c)$, 故得證等同於 $x\in(A^c\cup B^c)$.

(3) $x\in(A\cup B)^c\sim\neg(x\in(A\cup B))\sim\neg((x\in A)\vee(x\in B))$. 由式子 (1.9) 知此與 $\neg(x\in A)\wedge\neg(x\in B)$ 等價，亦即 $(x\in A^c)\wedge(x\in B^c)$, 故得證等同於 $x\in(A^c\cap B^c)$.

(4) 由於 $A\subseteq B$ 等價於 $(x\in A)\Rightarrow(x\in B)$ 且 $B^c\subseteq A^c$ 等價於 $\neg(x\in B)\Rightarrow\neg(x\in A)$. 由式子 (1.11) 我們有 $((x\in A)\Rightarrow(x\in B))\sim(\neg(x\in B)\Rightarrow\neg(x\in A))$, 故得證。 □

利用 Proposition 3.2.9, 我們立即可得以下的定理。

Corollary 3.2.10. 假設 A,B,C 為 *sets,* 我們有以下的性質.

(1) $(C\setminus(C\setminus A))=(C\cap A)$.

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

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

(4) 若 $A\subseteq B$ 則 $(C\setminus B)\subseteq(C\setminus A)$.

Proof. 我們使用補集、交集、聯集之間的關係證明。

(1) 依定義 $(C\setminus(C\setminus A))=C\cap(C\setminus A)^c=C\cap(C\cap A^c)^c$. 由 Proposition 3.2.9 (1)(2), $(C\cap A^c)^c=C^c\cup(A^c)^c=C^c\cup A$, 故得 $(C\setminus(C\setminus A))=C\cap(C^c\cup A)$. 再由分配率

$$C\cap(C^c\cup A)=(C\cap C^c)\cup(C\cap A)=\emptyset\cup(C\cap A)$$

得證 $(C\setminus(C\setminus A))=(C\cap A)$.

(2) 依定義 $C\setminus(A\cap B)=C\cap(A\cap B)^c$. 由 Proposition 3.2.9 (2), $(A\cap B)^c=(A^c\cup B^c)$, 故得 $C\setminus(A\cap B)=C\cap(A^c\cup B^c)$. 再由分配率 $C\cap(A^c\cup B^c)=(C\cap A^c)\cup(C\cap B^c)$. 得證 $C\setminus(A\cap B)=(C\setminus A)\cup(C\setminus B)$.

(3) 依定義 $C\setminus(A\cup B)=C\cap(A\cup B)^c$. 由 Proposition 3.2.9 (3), $(A\cup B)^c=(A^c\cap B^c)$, 故得 $C\setminus(A\cup B)=C\cap(A^c\cap B^c)$. 再由 $C\cap(A^c\cap B^c)=(C\cap A^c)\cap(C\cap B^c)$. 得證 $C\setminus(A\cup B)=(C\setminus A)\cap(C\setminus B)$.

(4) 依定義 $C\setminus B=C\cap B^c$. 現若 $A\subseteq B$ 由 Proposition 3.2.9 (4) 可得 $B^c\subseteq A^c$, 故得 $C\cap B^c\subseteq C\cap A^c$, 得證 $(C\setminus B)\subseteq(C\setminus A)$. □

Corollary 3.2.10 (4) 的反向是不正確的, 不過我們有以下之結果.

Proposition 3.2.11. 假設 A,B,C 為 *sets.* $(C\cap A)\subseteq(C\cap B)$ 若且唯若 $(C\setminus B)\subseteq(C\setminus A)$.

特別的，若已知 $A\subseteq C$, 則 $A\subseteq B$ 若且唯若 $(C\setminus B)\subseteq(C\setminus A)$.

Proof. 首先注意 $C\setminus A=C\setminus(C\cap A)$ 這是因為由 Corollary 3.2.10 (2),

$$C\setminus(C\cap A)=(C\setminus C)\cup(C\setminus A)=\emptyset\cup(C\setminus A)=C\setminus A.$$

同理 $C\setminus B=C\setminus(C\cap B)$.

現若 $(C\cap A)\subseteq(C\cap B)$, 利用 Corollary 3.2.10 (4) 可得 $C\setminus(C\cap B)\subseteq C\setminus(C\cap A)$, 得證 $(C\setminus B)\subseteq(C\setminus A)$. 反之，若 $(C\setminus B)\subseteq(C\setminus A)$, 則同樣由 Corollary 3.2.10 (4) 得 $C\setminus(C\setminus A)\subseteq C\setminus(C\setminus B)$. 再由 Proposition 3.2.10 (1) 得證 $(C\cap A)\subseteq(C\cap B)$.

由 Corollary 3.2.10 (4) 已知若 $A\subseteq B$ 則 $(C\setminus B)\subseteq(C\setminus A)$. 故當已知 $A\subseteq C$, 我們僅要證明：若 $(C\setminus B)\subseteq(C\setminus A)$ 則 $A\subseteq B$. 此時由前知 $(C\setminus B)\subseteq(C\setminus A)$ 可得 $(C\cap A)\subseteq(C\cap B)$. 故由 $A\subseteq C$ 的假設得 $A=(C\cap A)\subseteq(C\cap B)$. 但 $(C\cap B)\subseteq B$, 故得證 $A\subseteq B$. □

Question 3.10. $C\setminus(B\setminus A)$ 會等於 $(C\setminus B)\setminus A$ 嗎? 試證明 $C\setminus(B\setminus A)=(C\setminus B)\cup(C\cap A)$ 以及 $(C\setminus B)\setminus A=C\setminus(B\cup A)$.

其實這些集合 operations 之間的關係與性質, 都可以直接各邊取一元素, 利用第一章介紹邏輯的 connectives 的性質得到集合包含關係, 最後證得兩邊集合相等. 另一方面我們也可套用這一章中所介紹各集合的 operations 的性質推導. 這兩種方法並無好壞之分, 雖然有時直接套用集合 operations 的性質推導很快速, 但它並非萬能. 在這裡我們並不是鼓勵大家用背誦的方式記憶這麼多的性質, 而是希望大家能夠學習如何利用一些已知的性質推導出新的定理. 最後我們再看一個例子.

Example 3.2.12. 假設 A,B,C 為集合且 $B^c \subseteq A$, 我們要證明 $((C\setminus A)\cup B) = B$.

方法一: 我們用元素的方法處理. 首先已知 $B \subseteq ((C\setminus A)\cup B)$, 故要證明等式成立只要證明 $((C\setminus A)\cup B) \subseteq B$. 現假設 $x \in ((C\setminus A)\cup B)$, 我們要證明 $x \in B$. 然而 $x \in ((C\setminus A)\cup B)$ 表示 $x \in C\setminus A$ 或 $x \in B$. 如果 $x \in B$, 則證明結束, 所以我們僅要討論 $x \in C\setminus A$ 的情形, 即 $x \in C$ 且 $x \notin A$. 因為無法直接證明 $x \in B$, 所以我們可以考慮反證法, 即假設 $x \notin B$ 而得到矛盾. 現若 $x \notin B$, 表示 $x \in B^c$, 故由 $B^c \subseteq A$ 的假設得 $x \in A$. 此與 $x \notin A$ 相矛盾, 故知 $x \in B$. 得證 $((C\setminus A)\cup B) \subseteq B$.

方法二: 我們也可完全用前面證得的性質處理. 首先看到等式左右兩邊都有 B, 所以我們可以利用 Proposition 3.2.5. 也就是說若能證明 $(C\setminus A) \subseteq B$, 則可得證 $((C\setminus A)\cup B) = B$. 如何證明 $(C\setminus A) \subseteq B$ 呢? 由於 $(C\setminus A) \subseteq C$, 利用 Proposition 3.2.11, 我們只要驗證 $(C\setminus B) \subseteq (C\setminus (C\setminus A))$. 然而左邊 $C\setminus B = C\cap B^c$, 右邊 $C\setminus (C\setminus A) = C\cap A$, 所以由 $B^c \subseteq A$ 得證 $(C\setminus B) \subseteq (C\setminus (C\setminus A))$, 因而得 $(C\setminus A) \subseteq B$.

3.3. Indexed Family

在前一節中, 我們談的交集或聯集, 是將其視為兩個集合間的 operation. 不過當我們知道交集和聯集有所謂的結合律後, 我們便可以談論多個集合的聯集與交集了. 這一節中, 我們藉由適當的符號與定義的推廣, 將探討任意多個集合的聯集與交集問題. 大致上之前談的兩個集合的交集與聯集的性質, 都可以推廣到更一般的情形. 不過處理無限多個集合的情況, 有些地方可能和有限的情況稍有不同, 要特別留意.

當我們談論有限多個集合的交集和聯集時, 如果集合個數不多, 例如 5 個集合 A,B,C,D,E 的交集, 我們直接用 $A\cap B\cap C\cap D\cap E$ 來表示. 這裡我們都可以不用括弧區分到底哪兩個集合先交集後再和其他的集合做交集, 因為交集有結合律. 我們也不必擔心交集的順序, 因為交集有交換性. 同樣的對於聯集也是如此. 當集合的個數太多時, 像前面這樣一一列出就不切實際了. 遇到這種情形, 我們可以把要處理的集合一一編號, 例如有 100 個集合, 我們就編成 $A_1,A_2,\ldots,A_{100}$ (當然了, 這些 A_i 是甚麼應說明清楚). 然後這些集合的交集與聯集我們便像處理加法的 "summation" 符號, 將這些集合的交集與聯集分別用 $\bigcap_{i=1}^{100} A_i$, $\bigcup_{i=1}^{100} A_i$ 來表示. 例如若 $A_i = [i-1,i]$ (即介於 $i-1$ 和 i 之間的實數), 則 $\bigcap_{i=1}^{100} A_i = \emptyset$, $\bigcup_{i=1}^{100} A_i = [0,100]$. 如果有無窮多集合怎麼辦? 像前面的例子, 如果對所有的自然數 $i \in \mathbb{N}$, A_i 皆有定義, 我們可以考慮對所有的 A_i 的交集和聯集. 這時候我們一般可以學無窮級數的方法, 將這些交集和聯集分別表示成 $\bigcap_{i=1}^{\infty} A_i$, $\bigcup_{i=1}^{\infty} A_i$. 當然了, 這樣的符號底下表示的是 i 從哪一個數開始, 上面表示的是到哪一個為止, 所以我們要考慮 A_5, A_6, A_7, A_8 的交集和聯集就可以分別用 $\bigcap_{i=5}^{8} A_i$, $\bigcup_{i=5}^{8} A_i$ 來表示. 因此一般若要談 i 從 m 到 n 的 A_i 之交集與聯集, 我們便分別用 $\bigcap_{i=m}^{n} A_i$, $\bigcup_{i=m}^{n} A_i$ 來表示. 而要表達所有 i 大於等於 m 的 A_i 之交集與聯集, 我們便分

別用 $\bigcap_{i=m}^{\infty} A_i$, $\bigcup_{i=m}^{\infty} A_i$ 來表示. 這裡要注意, 很多同學會誤以為 $\bigcap_{i=m}^{\infty} A_i$, $\bigcup_{i=m}^{\infty} A_i$ 是 $\bigcap_{i=m}^{n} A_i$, $\bigcup_{i=m}^{n} A_i$ 當 n 趨近於 ∞ 的極限. 這個說法是有問題的, 因為我們從未定義過 "集合的極限".

不過這些符號仍不夠我們的需求. 有時我們要探討的集合, 它們的個數是不能像整數一樣一個一個數的. 例如實數, 就無法一個一個數. 所以若我們談的集合和實數有關, 如 $(-r,r)$ 其中 $r>0$, 這樣的區間, 要如何表達所有這樣的區間的交集與聯集呢? 於是乎, 我們引進了 index set 的概念. 所謂 *index set* 就是你要用來 "編足碼" 的東西所成的集合. 例如前面 $A_i=[i-1,i]$ 的例子, 我們考慮的 i 是所有的自然數 $\mathbb{N}$, 所以此時 $\mathbb{N}$ 便是我們的 index set. 而若要探討 $[-r,r]$ 的情形, 我們可以用正實數 $\mathbb{R}^+$ 為我們的 index set, 將要考慮的區間編碼成 $A_r=[-r,r]$. 這樣將所有被編碼好的集合 $A_r, r\in\mathbb{R}^+$ 收集在一起, 便是所謂的 *indexed family* 了. 所以一般來說, 我們要先說好 index set 為何. 接下來要說明要探討的集合如何用 index set 裡的元素編碼, 這樣才能形成一個 indexed family. 也就是說若 I 為 index set, 我們必須說明 A_i 是甚麼, 這樣 $\{A_i, i\in I\}$ 便會是一個 indexed family.

接下來, 我們便是要定義一個 indexed family 裡的集合其交集與聯集. 注意, 即使只有有限個集合, 我們仍可將其視為 indexed family. 例如兩個集合 A,B, 我們仍可將其是為 index set 為 $I=\{1,2\}$ 的 indexed family, 其中 $A_1=A$, $A_2=B$. 所以我們定義 index family 的交集與聯集需與有限集合的交集與聯集一致. 當我們有兩個集合 A,B 時, 要求交集的元素必須在每一個集合中; 而聯集裡的元素需在 A,B 某一個中. 所以我們有以下的定義.

Definition 3.3.1. 假設 I 為 index set, 而 $\{A_i, i\in I\}$, 為以 I 為 index set 的 indexed family. 定義此 indexed family 的 intersection 為

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

定義此 indexed family 的 union 為

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

利用此定義, 我們看以下的例子.

Example 3.3.2. 考慮 index set I 為大於 1 的整數. 對任意 $i\in I$, 令 $A_i=\{m/i : m\in\mathbb{Z}\}$. 我們要證明

$$\bigcap_{i\in I} A_i = \mathbb{Z},\quad \bigcup_{i\in I} A_i = \mathbb{Q}.$$

首先, 任意 $n\in\mathbb{Z}$, 我們都可以寫成 $n=ni/i$. 由於 $ni\in\mathbb{Z}$, 故得 $n\in A_i, \forall i\in I$. 證得了 $\mathbb{Z}\subseteq\bigcap_{i\in I} A_i$. 另一方面, 若 $x\in\bigcap_{i\in I} A_i$, 表示對任意 $i\in I$ 皆有 $x\in A_i$. 現由於 $x\in A_2$ 以及 $x\in A_3$, 我們有 $x=m/2$ 且 $x=m'/3$, 其中 $m,m'\in\mathbb{Z}$. 然而此即表示 $3m=2m'$, 故知 $3m$ 必為偶數. 因而得知 m 為偶數 $2n$, 其中 $n\in\mathbb{Z}$. 代回得 $x=m/2=n\in\mathbb{Z}$. 得證 $\bigcap_{i\in I} A_i\subseteq\mathbb{Z}$, 故 $\bigcap_{i\in I} A_i=\mathbb{Z}$.

現若 $x\in\mathbb{Q}$, 依有理數之定義, x 可寫成 m/n, 其中 $m\in\mathbb{Z}$, $n\in\mathbb{N}$. 現若 $n=1$, 即 $x=m\in\mathbb{Z}$. 我們可以將 x 寫成 $x=2m/2$, 知此時 $x\in A_2$. 而若 $n\geq 2$, 表示 $n\in I$, 故此時 $x\in A_n$. 得證

$\mathbb{Q} \subseteq \bigcup_{i\in I} A_i$. 另一方面, 若 $x \in \bigcup_{i\in I} A_i$, 表示存在 $n \in I$, 使得 $x \in A_n$. 故依定義得 $x = m/n$, 其中 $m \in \mathbb{Z}$. 此即表示 $x \in \mathbb{Q}$, 得證 $\bigcup\limits_{i\in I} A_i \subseteq \mathbb{Q}$, 故 $\bigcup\limits_{i\in I} A_i = \mathbb{Q}$.

Question 3.11. 令 A_i 如 *Example 3.3.2* 所設. 利用當 $m \in \mathbb{Z}$ 時, 若 p,q 為兩互質整數且 p 整除 mq, 則 p 整除 m 之事實, 證明若 p,q 為兩互質整數, 則 $A_p \cap A_q = \mathbb{Z}$. 依此證明當 $m \in \mathbb{N}$, $\bigcap\limits_{i=m}^{\infty} A_i = \mathbb{Z}$.

現在我們探討一些有關兩集合的交集與聯集的性質, 是否可以推廣到更一般 indexed family 的情形. 首先 Proposition 3.2.3 是可以推廣的.

Proposition 3.3.3. 假設 $\{A_i, i \in I\}$, $\{B_i, i \in I\}$ 是以 I 為 *index set* 的兩組 *indexed family.* 若對於所有 $i \in I$ 皆有 $A_i \subseteq B_i$, 則

$$\bigcap_{i\in I} A_i \subseteq \bigcap_{i\in I} B_i \quad \text{and} \quad \bigcup_{i\in I} A_i \subseteq \bigcup_{i\in I} B_i.$$

Proof. 設 $x \in \bigcap\limits_{i\in I} A_i$, 表示對所有 $i \in I$, 皆有 $x \in A_i$, 故由 $A_i \subseteq B_i$, 得 $x \in B_i$. 因為這是對任意的 $i \in I$ 皆成立, 故得 $x \in \bigcap\limits_{i\in I} B_i$. 得證 $\bigcap\limits_{i\in I} A_i \subseteq \bigcap\limits_{i\in I} B_i$.

現若 $x \in \bigcup\limits_{i\in I} A_i$, 表示存在 $i \in I$ 使得 $x \in A_i$, 故由 $A_i \subseteq B_i$, 得 $x \in B_i$. 此即表示 $x \in \bigcup\limits_{i\in I} B_i$, 得證 $\bigcup\limits_{i\in I} A_i \subseteq \bigcup\limits_{i\in I} B_i$. □

很容易知道, 若對於任意 $i \in I$, 皆有 $A_i = A$, 則 $\bigcap\limits_{i\in I} A_i = A$ 且 $\bigcup\limits_{i\in I} A_i = A$. 所以我們套用 Proposition 3.3.3 有以下 Corollary 3.2.4 的推廣.

Corollary 3.3.4. 假設 A,B 為 *set* 且 $\{A_i, i \in I\}$, $\{B_i, i \in I\}$ 是以 I 為 *index set* 的 *indexed family.*

(1) 若對於所有 $i \in I$ 皆有 $A \subseteq A_i$, 則 $A \subseteq \bigcap\limits_{i\in I} A_i$.

(2) 若對於所有 $i \in I$ 皆有 $B_i \subseteq B$, 則 $\bigcup\limits_{i\in I} B_i \subseteq B$.

雖然前面幾個結果顯示一些關於有限多個集合的交集或聯集的性質可以推廣到無窮多個集合的交集或聯集, 不過這並不是完全對的. 例如有可能有一些集合當你在它們中任意取有限多個做交集時都不是空集合, 但是取無窮多個做交集時有可能會是空集合. 我們有以下的例子.

Example 3.3.5. 我們要舉例說明有可能一個以自然數 $\mathbb{N}$ 為 index set 的 indexed family $\{A_i, i \in I\}$, 滿足對所有 $n \in \mathbb{N}$ 皆有 $\bigcap\limits_{i=1}^{n} A_i$ 不是空集合 (甚至會有無窮多個元素), 但 $\bigcap\limits_{i=1}^{\infty} A_i$ 是空集合.

事實上對所有 $i\in\mathbb{N}$ 考慮 A_i 為開區間 (i,∞). 此時 A_i 滿足 $A_i\neq\emptyset$ 且當 $j\geq i$ 時, $A_j\subseteq A_i$. 因此得 $\bigcap_{i=1}^{n}A_i=A_n=(n,\infty)\neq\emptyset$. 但 $\bigcap_{i=1}^{\infty}A_i=\emptyset$. 這是因為若 $x\in\bigcap_{i=1}^{\infty}A_i$, 則因 $x\in\mathbb{R}$ 必存在 $n\in\mathbb{N}$ 滿足 $n>x$. 我們得 $x\notin A_n=(n,\infty)$. 此與 $x\in\bigcap_{i=1}^{\infty}A_i$ 相矛盾, 得證 $\bigcap_{i=1}^{\infty}A_i=\emptyset$.

從上面這個例子我們知道, 一些在有限多個集合的交集或聯集會對的情形, 在無窮多個集合的時候有可能是錯的, 所以還是要多加留意.

Question 3.12. 假設 A_i 為 *Example 3.3.5* 中的開區間 (i,∞), 為何不是 $\bigcap_{i=1}^{\infty}A_i=\{\infty\}$?

關於交集與聯集分配律的性質, 我們有以下 Proposition 3.2.6 的推廣.

Proposition 3.3.6. 假設 B 為 *set,* 且 $\{A_i, i\in I\}$ 是以 I 為 *index set* 的 *indexed family.* 則

$$(\bigcap_{i\in I}A_i)\cup B=\bigcap_{i\in I}(A_i\cup B)\quad\text{and}\quad(\bigcup_{i\in I}A_i)\cap B=\bigcup_{i\in I}(A_i\cap B).$$

Proof. 由於對所有 $k\in I$ 皆有 $(\bigcap_{i\in I}A_i)\subseteq(A_k\cup B)$ 且 $B\subseteq(A_k\cup B)$, 由 Corollary 3.2.4 (2) 知 $((\bigcap_{i\in I}A_i)\cup B)\subseteq(A_k\cup B)$. 因為這是對任意 $k\in I$ 皆對, 故由 Corollary 3.3.4 (1) 知

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

另一方面, 若 $x\in\bigcap_{i\in I}(A_i\cup B)$, 則對所有 $i\in I$, 皆有 $x\in A_i$ 或 $x\in B$. 我們分 $x\in B$ 以及 $x\notin B$ 兩種情況來討論. 若 $x\in B$, 則自然有 $x\in(\bigcap_{i\in I}A_i)\cup B$. 而若 $x\notin B$, 則知 $x\in A_i$ 且由於這是對所有 $i\in I$ 皆成立, 故得 $x\in\bigcap_{i\in I}A_i$, 因此 $x\in(\bigcap_{i\in I}A_i)\cup B$. 得證 $\bigcap_{i\in I}(A_i\cup B)\subseteq((\bigcap_{i\in I}A_i)\cup B)$, 故

$$(\bigcap_{i\in I}A_i)\cup B=\bigcap_{i\in I}(A_i\cup B).$$

同理, 對所有 $k\in I$ 皆有 $(A_k\cap B)\subseteq(\bigcup_{i\in I}A_i)$ 且 $(A_k\cap B)\subseteq B$, 由 Corollary 3.2.4 (1) 知 $(A_k\cap B)\subseteq(\bigcup_{i\in I}A_i)\cap B$. 因為這是對任意 $k\in I$ 皆對, 故由 Corollary 3.3.4 (2) 知

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

另一方面, 若 $x\in(\bigcup_{i\in I}A_i)\cap B$, 表示 $x\in\bigcup_{i\in I}A_i$ 且 $x\in B$. 因此存在 $i\in I$, 使得 $x\in A_i$ 且 $x\in B$. 亦即存在 $i\in I$ 使得 $x\in A_i\cap B$. 故知此時 $x\in\bigcup_{i\in I}(A_i\cap B)$, 得證 $((\bigcup_{i\in I}A_i)\cap B)\subseteq\bigcup_{i\in I}(A_i\cap B)$, 故

$$(\bigcup_{i\in I}A_i)\cap B=\bigcup_{i\in I}(A_i\cap B).$$

□

最後我們推廣有關於有限集合差集的 DeMorgan's laws (Proposition 3.2.9 (2)(3)).

Proposition 3.3.7. 假設 C 為 *sets* 且 $\{A_i, i\in I\}$ 是以 I 為 *index set* 的 *indexed family*, 我們有以下的性質.

(1) $C\setminus(\bigcap_{i\in I}A_i)=\bigcup_{i\in I}(C\setminus A_i)$. 特別的, 我們有 $(\bigcap_{i\in I}A_i)^c=\bigcup_{i\in I}A_i^c$.

(2) $C\setminus(\bigcup_{i\in I}A_i)=\bigcap_{i\in I}(C\setminus A_i)$. 特別的, 我們有 $(\bigcup_{i\in I}A_i)^c=\bigcap_{i\in I}A_i^c$.

Proof. (1): 我們先證 $(\bigcap_{i\in I}A_i)^c=\bigcup_{i\in I}A_i^c$. 為了方便我們直接用 logical equivalence 來證明。因 $x\in(\bigcap_{i\in I}A_i)^c$ 表示 $x\notin(\bigcap_{i\in I}A_i)$, 亦即 $\neg(x\in\bigcap_{i\in I}A_i)$ 然而 $x\in\bigcap_{i\in I}A_i$ 表示 $\forall i\in I, x\in A_i$, 故 $\neg(x\in\bigcap_{i\in I}A_i)$ 等同於 $\exists i\in I, x\notin A_i$, 即 $\exists i\in I, x\in A_i^c$, 故得證此等同於 $x\in\bigcup_{i\in I}A_i^c$. 得證 $(\bigcap_{i\in I}A_i)^c=\bigcup_{i\in I}A_i^c$.

現因 $C\setminus(\bigcap_{i\in I}A_i)=C\cap(\bigcap_{i\in I}A_i)^c=C\cap(\bigcup_{i\in I}A_i^c)$ 由交集和聯集的分配律 (Proposition 3.3.6) 知 $C\cap(\bigcup_{i\in I}A_i^c)=\bigcup_{i\in I}(C\cap A_i^c)$, 故得證

$$C\setminus(\bigcap_{i\in I}A_i)=\bigcup_{i\in I}(C\setminus A_i).$$

(2): 利用 (1) 的結果我們有 $(\bigcap_{i\in I}A_i^c)^c=\bigcup_{i\in I}(A_i^c)^c$, 再利用 Proposition 3.2.9 (1), 得 $(\bigcap_{i\in I}A_i^c)^c=\bigcup_{i\in I}A_i$. 取 complement 並再次利用 Proposition 3.2.9 (1) 得證 $(\bigcup_{i\in I}A_i)^c=\bigcap_{i\in I}A_i^c$. 現因

$$C\setminus(\bigcup_{i\in I}A_i)=C\cap(\bigcup_{i\in I}A_i)^c=C\cap(\bigcap_{i\in I}A_i^c)\quad\text{and}\quad\bigcap_{i\in I}(C\setminus A_i)=\bigcap_{i\in I}(C\cap A_i^c),$$

由交集本身的結合律與交換律知 $C\cap(\bigcap_{i\in I}A_i^c)=\bigcap_{i\in I}(C\cap A_i^c)$, 故得證

$$C\setminus(\bigcup_{i\in I}A_i)=\bigcap_{i\in I}(C\setminus A_i).$$

□

Question 3.13. 假設 C 為 *sets* 且 $\{A_i, i\in I\}$ 是以 I 為 *index set* 的 *indexed family*. 試問 $(\bigcap_{i\in I}A_i)\setminus C$ 會等於 $\bigcap_{i\in I}(A_i\setminus C)$ 或是 $\bigcup_{i\in I}(A_i\setminus C)$, 還是都不對? 而 $(\bigcup_{i\in I}A_i)\setminus C$ 會等於甚麼?

3.4. Power Set and Cartesian Product

前面介紹的幾個集合的運算 (交集, 聯集和差集) 在作用後所得的集合仍在宇集中, 接著要介紹的這兩種運算在作用後所得的集合很可能會不在原先的宇集中 (當然此時要擴大我們的宇集), 這一點要特別留意.

3.4.1. Power Set.

首先我們定義 power set.

Definition 3.4.1. 假設 A 為 set. 我們定義 A 的 *power set* 為 A 的 subsets 所成的集合, 用 $\mathscr{P}(A)$ 來表示. 依定義我們有

$$\mathscr{P}(A)=\{S : S\subseteq A\}.$$

由於對任意的 set A, 皆有 $\emptyset \subseteq A$ 以及 $A \subseteq A$, 我們得 $\emptyset \in \mathscr{P}(A)$ 且 $A \in \mathscr{P}(A)$. 最特別的是, 因 $\emptyset$ 包含於任何的集合, 故我們仍有 $\emptyset \subseteq \mathscr{P}(A)$. 也就是我們會同時有 $\emptyset \in \mathscr{P}(A)$ 且 $\emptyset \subseteq \mathscr{P}(A)$ 的情形發生. 另外若 $a \in A$, 表示 $\{a\} \subseteq A$, 故知 $\{a\} \in \mathscr{P}(A)$. 原來的 set 和其 power set 中 "屬於" 和 "包含於" 關係的轉變, 千萬不要混淆. 我們看以下的例子.

Example 3.4.2. 由於 $\emptyset$ 只有自己一個子集合, 故得 $\mathscr{P}(\emptyset) = \{\emptyset\}$.

考慮 $A = \{1,2,3\}$, 由前已知 $\emptyset, A, \{1\}, \{2\}, \{3\}$ 皆在 $\mathscr{P}(A)$ 中. 又因 $\{1,2\}, \{1,3\}, \{2,3\}$ 皆包含於 A, 故得

$$\mathscr{P}(A) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\big\}.$$

當一個集合 A 僅有有限多個元素時, 我們稱之為 *finite set*. 此時我們用 $\#(A)$ 來表示 A 的元素個數. 例如在上面 Example 3.4.2 中 $\#(A) = 3$, 此時我們發現 $\#(\mathscr{P}(A)) = 2^3 = 8$. 一般的 finite set, 我們都可以由其元素個數, 得到知道它的 power set 的元素個數.

Proposition 3.4.3. 假設 A 為 *finite set* 且 $\#(A) = n$. 則 $\#(\mathscr{P}(A)) = 2^n$.

Proof. 我們可以用排列組合的方法得到 $\#(\mathscr{P}(A)) = 2^n$. 不過這不是本門課所要談論的技巧, 我們用數學歸納法證明. 我們對 A 的元素個數 $\#(A)$ 做數學歸納法. 當 $\#(A) = 0$ 時, 表示 A 沒有任何元素, 即 $A = \emptyset$. 由 Example 3.4.2, 我們知此時 $\#(A) = 1 = 2^0$. 而當 $\#(A) = 1$ 時, 表示 A 僅有一元素, 設其為 a, 即 $A = \{a\}$. 此時我們有 $\mathscr{P}(A) = \{\emptyset, \{a\}\}$, 故得 $\#(A) = 2 = a^1$. 證得 $n = 0,1$ 時成立.

現假設當集合的個數為 k 時成立. 考慮 $\#(A) = k+1$ 的情形, 假設 $A = \{a_1, \ldots, a_k, a_{k+1}\}$. 此時令 $A' = A \setminus \{a_{k+1}\}$. 我們有 $\#(A') = k$, 故由歸納法之假設得 $\mathscr{P}(A') = 2^k$, 亦即 A' 共有 2^k 個元素. 現因 $A' \subset A$, A' 的 subset 必為 A 的 subset. 故知 $\mathscr{P}(A)$ 至少有 2^k 個元素. 然而 A 中有 subset 是不包含於 A' 的, 就是那些含有 a_{k+1} 的 subset. 若 S 為這樣的 subset, 即 $a_{k+1} \in S$. 此時令 $S' = S \setminus \{a_{k+1}\}$, 則 $S' \subseteq A'$. 反之, 若 $S' \subseteq A'$, 則令 $S = S' \cup \{a_{k+1}\}$, 我們會得到 S 是 A 的 subset, 但不是 A' 的 subset. 換言之, A 的 subset, 要不然就是 A' 的 subset, 要不然就是將某個 A' 的 subset 聯集 $\{a_{k+1}\}$ 而得. 故得 A 的 subset 的個數為 $2^k + 2^k = 2^{k+1}$, 證得 $\#(\mathscr{P}(A)) = 2^{k+1}$. 故由數學歸納法知, 若 $\#(A) = n$, 則 $\#(\mathscr{P}(A)) = 2^n$. □

接下來我們要談論 power set 和原來的 set 之間的關係. 由於這些關係仍和集合的包含關係有關, 我們只要能掌握 power set 的元素即可. 依 power set 的定義, 若 A 為 set, 則 $S \in \mathscr{P}(A)$ 若且唯若 $S \subseteq A$. 利用這個看法, 我們可以很容易地得到一些有關 power set 的性質. 首先我們來看, power set 事實上是會保持包含關係的.

Proposition 3.4.4. 假設 A, B 為 *sets*. 則 $A \subseteq B$ 若且唯若 $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

Proof. ($\Rightarrow$): 假設 $A \subseteq B$. 若 $S \in \mathscr{P}(A)$, 表示 $S \subseteq A$. 故由 $A \subseteq B$ 得 $S \subseteq B$, 亦即 $S \in \mathscr{P}(B)$. 得證 $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

($\Leftarrow$): 假設 $\mathscr{P}(A) \subseteq \mathscr{P}(B)$. 由於 $A \in \mathscr{P}(A)$, 故由 $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, 得 $A \in \mathscr{P}(B)$. 依 power set 之定義, 此即表示 $A \subseteq B$. □

Question 3.14. 假設 A,B 為 *sets.* 試問 $A\subset B$ 若且唯若 $\mathscr{P}(A)\subset\mathscr{P}(B)$ 是否正確?

Power set 也保持交集的運算, 也就是說我們有以下的性質.

Proposition 3.4.5. 假設 A,B 為 *sets.* 則 $\mathscr{P}(A\cap B)=\mathscr{P}(A)\cap\mathscr{P}(B)$.

Proof. 因 $(A\cap B)\subseteq A$ 且 $(A\cap B)\subseteq B$ 由 Proposition 3.4.4 我們有 $\mathscr{P}(A\cap B)\subseteq\mathscr{P}(A)$ 且 $\mathscr{P}(A\cap B)\subseteq\mathscr{P}(B)$. 故由 Corollary 3.2.4 知 $\mathscr{P}(A\cap B)\subseteq\mathscr{P}(A)\cap\mathscr{P}(B)$.

另一方面, 若 $S\in\mathscr{P}(A)\cap\mathscr{P}(B)$ 表示 $S\in\mathscr{P}(A)$ 且 $S\in\mathscr{P}(B)$, 亦即 $S\subseteq A$ 且 $S\subseteq B$. 故再由 Corollary 3.2.4 知 $S\subseteq(A\cap B)$, 也就是說 $S\in\mathscr{P}(A\cap B)$. 得證 $\mathscr{P}(A)\cap\mathscr{P}(B)\subseteq\mathscr{P}(A\cap B)$, 故 $\mathscr{P}(A\cap B)=\mathscr{P}(A)\cap\mathscr{P}(B)$. □

Question 3.15. 假設 $\{A_i, i\in I\}$ 是以 I 為 *index set* 的 *indexed family.* 試問 $\mathscr{P}(\bigcap_{i\in I}A_i)$ 是否等於 $\bigcap_{i\in I}\mathscr{P}(A_i)$?

Power set 是否會保持聯集呢? 雖然我們有 $A\subseteq(A\cup B)$ 且 $B\subseteq(A\cup B)$ 所以由 Proposition 3.4.4 可得 $\mathscr{P}(A)\subseteq\mathscr{P}(A\cup B)$ 且 $\mathscr{P}(B)\subseteq\mathscr{P}(A\cup B)$, 再由 Corollary 3.2.4 得

$$(\mathscr{P}(A)\cup\mathscr{P}(B))\subseteq\mathscr{P}(A\cup B). \tag{3.3}$$

不過一般來說 $\mathscr{P}(A\cup B)\subseteq\mathscr{P}(A)\cup\mathscr{P}(B)$ 卻是不正確的. 這是因為若 $S\in\mathscr{P}(A\cup B)$ 表示 $S\subseteq(A\cup B)$, 但這並不一定保證 $S\subseteq A$ 或 $S\subseteq B$. 例如當 $A=\{1\}$, $B=\{2\}$, 我們有 $S=\{1,2\}\subseteq A\cup B$, 但 $S\nsubseteq A$ 且 $S\nsubseteq B$. 事實上此時 $\mathscr{P}(A)=\{\emptyset,\{1\}\},\mathscr{P}(B)=\{\emptyset,\{2\}\}$, 故有 $\mathscr{P}(A)\cup\mathscr{P}(B)=\{\emptyset,\{1\},\{2\}\}$. 但是 $\mathscr{P}(A\cup B)=\{\emptyset,\{1\},\{2\},\{1,2\}\}$. 故此時 $\mathscr{P}(A\cup B)\neq\mathscr{P}(A)\cup\mathscr{P}(B)$, 即 $\mathscr{P}(A)\cup\mathscr{P}(B)\subset\mathscr{P}(A\cup B)$.

Question 3.16. 假設 $\{A_i, i\in I\}$ 是以 I 為 *index set* 的 *indexed family.* 試問 $\bigcup_{i\in I}\mathscr{P}(A_i)\subseteq\mathscr{P}(\bigcup_{i\in I}A_i)$ 是否成立?

Question 3.17. 試證明 $\mathscr{P}(A)\cup\mathscr{P}(B)\neq\mathscr{P}(A\cup B)$ 若且唯若 $A\nsubseteq B$ 且 $B\nsubseteq A$.

在任何情況之下, Power set 都無法保持差集. 這是因為當 A,B 為 sets 時, 在任何情況之下皆有 $\emptyset\in\mathscr{P}(A)$, $\emptyset\in\mathscr{P}(B)$. 因此會得到 $\emptyset\notin\mathscr{P}(A)\setminus\mathscr{P}(B)$. 然而 $\emptyset\in\mathscr{P}(A\setminus B)$, 故知 $(\mathscr{P}(A)\setminus\mathscr{P}(B))\neq\mathscr{P}(A\setminus B)$. 不過當 $S\neq\emptyset$ 時, 若 $S\in\mathscr{P}(A\setminus B)$, 表示 $S\subseteq(A\setminus B)$. 此時因 $(A\setminus B)\subseteq A$, 故得 $S\subseteq A$ (即 $S\in\mathscr{P}(A)$). 這時我們也會有 $S\nsubseteq B$ (即 $S\notin\mathscr{P}(B)$). 否則由 $S\subseteq(A\setminus B)$ 以及 $S\subseteq B$, 得 $S\subseteq(A\setminus B)\cap B=\emptyset$ 此與 $S\neq\emptyset$ 相矛盾。故由 $S\in\mathscr{P}(A)$ 且 $S\notin\mathscr{P}(B)$ 得 $S\in\mathscr{P}(A)\setminus\mathscr{P}(B)$. 我們證明了 $\mathscr{P}(A\setminus B)$ 中除了空集合以外, 其他的元素都會在 $\mathscr{P}(A)\setminus\mathscr{P}(B)$ 中, 故得

$$(\mathscr{P}(A\setminus B)\setminus\{\emptyset\})\subseteq(\mathscr{P}(A)\setminus\mathscr{P}(B)). \tag{3.4}$$

不過上面的包含關係的反向並不成立. 因為若 $S\in\mathscr{P}(A)\setminus\mathscr{P}(B)$ 表示 $S\subseteq A$ 且 $S\nsubseteq B$. 但這不表示 $S\subseteq(A\setminus B)$. 例如若 $A=\{1,2\}$, $B=\{2\}$, 此時考慮 $S=\{1,2\}$. 則 $S\subseteq A$ 且

$S \not\subseteq B$ (即 $S \in \mathscr{P}(A) \setminus \mathscr{P}(B)$), 但 $S = \{1,2\} \not\subseteq (A \setminus B) = \{1\}$. (即 $S \notin \mathscr{P}(A \setminus B) \setminus \{\emptyset\}$). 故此時 $(\mathscr{P}(A) \setminus \mathscr{P}(B)) \not\subseteq (\mathscr{P}(A \setminus B) \setminus \{\emptyset\})$.

Question 3.18. 假設 A, B 為 *sets.*

(1) 證明若 $A \setminus B = \emptyset$ 則 $(\mathscr{P}(A) \setminus \mathscr{P}(B)) = \emptyset$.

(2) 證明若 $A \cap B = \emptyset$ 則 $(\mathscr{P}(A) \setminus \mathscr{P}(B)) = (\mathscr{P}(A) \setminus \{\emptyset\})$.

(3) 證明 $(\mathscr{P}(A \setminus B) \setminus \{\emptyset\}) \neq (\mathscr{P}(A) \setminus \mathscr{P}(B))$ 若且唯若 $A \setminus B \neq \emptyset$ 且 $A \cap B \neq \emptyset$

3.4.2. Cartesian Product. 我們曾強調對於集合我們是不考慮其元素的排列順序, 例如 $\{1,2\}$ 和 $\{2,1\}$ 是相同的集合. 不過若考慮集合 $S_1 = \{\{1\},\{1,2\}\}$ 和 $S_2\{\{2\},\{1,2\}\}$, 很容易知道 $\{1\} \in S_1$ 且 $\{1\} \notin S_2$, 所以我們知道 $S_1 \neq S_2$. 這個方法, 幫助我們將 1, 2 這兩個元素做了排序. 因此我們定義以下的符號.

Definition 3.4.6. 假設 A, B 為 sets. 若 $a \in A, b \in B$, 我們定義 *ordered pair*

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

且令

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

稱之為 the *Cartesian product* of A and B.

所謂 ordered pair, 意指有序的數對, 也就是這裡的元素都是成對出現, 而且順序是有關的. 例如前面的例子, 我們有 $(1,2) = \{\{1\},\{1,2\}\}$, 而 $(2,1) = \{\{2\},\{1,2\}\}$, 故 $(1,2) \neq (2,1)$. 一般來說設 $a, a' \in A$, $b, b' \in B$. 若 $a = a'$, $b = b'$, 則依集合相等的定義, 我們有

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

另一方面若 $(a,b) = (a',b')$ 表示 $\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\}$. 現若 $a \neq b$, 表示 $\{a,b\}$ 中有兩個元素, 故若 $(a,b) = (a',b')$, 表示 $\{a',b'\}$ 必須亦為有兩個元素的集合 (否則 $\{\{a'\},\{a',b'\}\}$ 中沒有一個有兩元素的集合, 不可能等於 $\{\{a\},\{a,b\}\}$). 既然如此, 由集合相等之定義, 我們必有 $\{a\} = \{a'\}$ 以及 $\{a,b\} = \{a',b'\}$. 這告訴我們 $a = a'$ 且 $b = b'$. 而若 $\{a,b\}$ 中僅有一元素, 即 $a = b$. 此時依集合定義 $\{a,b\} = \{a\}$, 故

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

因此, 這時候要 $(a,b) = (a',b')$ 非得 $b' = a' = a$, 故此時依然有 $a = a'$ 且 $b = b'$. 我們證得了以下的結果.

Proposition 3.4.7. 假設 A, B 為 *sets,* 又設 $a, a' \in A$ 且 $b, b' \in B$ 則 $(a,b) = (a',b')$ 若且唯若 $a = a'$ 且 $b = b'$.

我們觀察一下, 當 $a \in A$, $b \in B$, $\{\{a\},\{a,b\}\}$ 會是哪一個集合的元素. 首先由 $\{a,b\}$ 我們可以看出, 此集合應該和 $A \cup B$ 有關. 又 $\{a\}$, $\{a,b\}$ 為 $A \cup B$ 的 subset, 我們有 $\{a\}$ 和 $\{a,b\}$ 皆為 $\mathscr{P}(A \cup B)$ 的元素. 故 $\{\{a\},\{a,b\}\}$ 為 $\mathscr{P}(A \cup B)$ 的子集合, 得 $\{\{a\},\{a,b\}\} \in \mathscr{P}(\mathscr{P}(A \cup B))$.

也就是說 (a,b) 為 $\mathscr{P}(\mathscr{P}(A\cup B))$ 中的元素. 從這裡知道將 (a,b) 考慮成 $\{\{a\},\{a,b\}\}$ 這樣複雜的集合, 以後處理問題很不方便. 不過 Proposition 3.4.7 告訴我們, 以後可以不去管 (a,b) 的原始定義. 直接將 (a,b) 看成是 $A\times B$ 中的一個元素, 我們可以直接利用 $(a,b)=(a',b')$ 來探討 $A\times B$ 這樣的集合的相關性質.

Example 3.4.8. (1) 假設 $A=\{a,b\}$, $B=\{1,2,3\}$. 則依定義我們可以將 $A\times B$ 寫成

$$A\times B=\{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3)\}.$$

另外依定義我們有 $A\times\{\emptyset\}=\{(a,\emptyset),(b,\emptyset)\}$.

(2) 考慮 $S=\{(x,y)\in\mathbb{R}\times\mathbb{R}:x^2+y^2\leq 1\}$. 雖然 S 為 $\mathbb{R}\times\mathbb{R}$ 的 subset, 但不存在 $A\subseteq\mathbb{R}$, $B\subseteq\mathbb{R}$ 使得 $S=A\times B$. 事實上, 若 $S=A\times B$, 由 $(1,0)\in S$, 我們得 $1\in A$. 另外 $(0,1)\in S$, 我們得 $1\in B$. 因此得 $(1,1)\in A\times B$. 然而 $1^2+1^2=2>1$, 得 $(1,1)\notin S$. 此與 $S=A\times B$ 的假設矛盾, 故得證不存在 $A\subseteq\mathbb{R}$, $B\subseteq\mathbb{R}$ 使得 $S=A\times B$.

要注意區分 $A\times\emptyset$ 和 $A\times\{\emptyset\}$ 之不同. 依定義 $(x,y)\in A\times\{\emptyset\}$ 表示 $x\in A$ 以及 $y\in\{\emptyset\}$, 故此時因 $\{\emptyset\}$ 是一個僅有一個元素 $\emptyset$ 的集合, 故 $y=\emptyset$. 然而 $(x,y)\in A\times\emptyset$ 表示 $x\in A$ 以及 $y\in\emptyset$, 不過不可能會有元素屬於 $\emptyset$, 故此處 y 並不存在. 所以依定義 $A\times\emptyset$ 中沒有任何元素, 故得 $A\times\emptyset=\emptyset$. 同理我們會有 $\emptyset\times B=\emptyset$. 事實上我們有以下的結果.

Proposition 3.4.9. 假設 A,B 為 *sets,* 則 $A\times B=\emptyset$ 若且唯若 $A=\emptyset$ 或 $B=\emptyset$.

Proof. 我們僅剩下證明若 $A\times B=\emptyset$, 則 $A=\emptyset$ 或 $B=\emptyset$. 利用 contrapositive method, 假設 $A\neq\emptyset$ 且 $B\neq\emptyset$. 此時存在 $a\in A$ 且 $b\in B$, 故存在 $(a,b)\in A\times B$. 得證 $A\times B\neq\emptyset$. □

當 A,B 為 finite sets 時, 我們可以如 Example 3.4.8 一一列出 $A\times B$ 中的元素. 當我們選定 $a\in A$ 後, 考慮 $(a,y)\in A\times B$. 由 Proposition 3.4.7 我們知, 當我們選 y 為 B 中的相異元素時, 所得的 (a,y) 就會不同. 也就是說此時 $A\times B$ 中為 (a,y) 這樣形式的元素共有 $\#(B)$ 個. 然而當 a 不同時這些元素亦皆不同, 故由排列組合中的乘法原理我們知 $A\times B$ 共會有 $\#(A)\times\#(B)$ 個元素, 因此有以下之定理.

Proposition 3.4.10. 假設 A,B 為 *finite sets.* 則 $\#(A\times B)=\#(A)\times\#(B)$.

因為 $\#(\emptyset)=0$, 故由 Proposition 3.4.10 得 $\#(A\times\emptyset)=\#(A)\times\#(\emptyset)=0$. 此結論和 Proposition 3.4.9 中 $A\times\emptyset=\emptyset$ 的結論一致.

接下來我們探討 Cartesian product 對集合包含關係的影響. 首先注意, 對於任意的 set A, 當 $B=\emptyset$ 時, 我們有 $A\times B=\emptyset$ 所以我們無法由 $A\times B$ 和 $A'\times B$ 來判斷 A,A' 之間的關係. 因此我們必須排除 $A\times B$ 其中 A,B 任一個是 $\emptyset$ 的情形. 我們有以下的結果.

Proposition 3.4.11. 假設 A,B,C,D 為 *sets* 且 $A\neq\emptyset$ 以及 $B\neq\emptyset$. 則 $A\subseteq C$ 且 $B\subseteq D$ 若且唯若 $(A\times B)\subseteq(C\times D)$.

Proof. $(\Rightarrow)$: 假設 $A\subseteq C$ 且 $B\subseteq D$. 現任取 $(x,y)\in A\times B$, 表示 $x\in A$ 且 $y\in B$, 故由 $A\subseteq C$ 且 $B\subseteq D$ 得 $x\in C$ 且 $y\in D$. 因此依定義知 $(x,y)\in C\times D$, 得證 $(A\times B)\subseteq(C\times D)$.

($\Leftarrow$): 假設 $(A\times B)\subseteq(C\times D)$. 現任取 $x\in A$, 由於 $B\neq\emptyset$, 故存在 $b\in B$. 此時考慮 $(x,b)\in A\times B$. 利用 $(A\times B)\subseteq(C\times D)$, 得 $(x,b)\in C\times D$. 因此依定義知 $x\in C$, 得證 $A\subseteq C$. 同理, 任取 $y\in B$, 由於 $A\neq\emptyset$, 故存在 $a\in A$. 此時考慮 $(a,y)\in A\times B$. 利用 $(A\times B)\subseteq(C\times D)$, 得 $(a,y)\in C\times D$. 因此依定義知 $y\in D$, 得證 $B\subseteq D$. □

Question 3.19. *Proposition 3.4.11* 的證明中, 哪一部分需要 $A\neq\emptyset$ 以及 $B\neq\emptyset$ 的假設? 又為何將 $A\subseteq C$ 和 $B\subseteq D$ 分開來證明?

接下來我們看 Cartesian product 和 intersection 的關係.

Proposition 3.4.12. 假設 A,B,C,D 為 *sets.* 則

$$(A\cap C)\times B=(A\times B)\cap(C\times B)\quad\text{and}\quad A\times(B\cap D)=(A\times B)\cap(A\times D).$$

Proof. 因 $(A\cap C)\subseteq A$ 且 $(A\cap C)\subseteq C$ 由 Proposition 3.4.11 知 $((A\cap C)\times B)\subseteq(A\times B)$ 且 $((A\cap C)\times B)\subseteq(C\times B)$ (注意 Proposition 3.4.11 此部分不需非空集合的假設). 故由 Corollary 3.2.4(1) 得 $((A\cap C)\times B)\subseteq(A\times B)\cap(C\times B)$.

另一方面, 對任意 $(x,y)\in(A\times B)\cap(C\times B)$, 我們有 $(x,y)\in A\times B$ 且 $(x,y)\in C\times B$. 因此 $x\in A$ 且 $x\in C$ 以及 $y\in B$, 得 $x\in A\cap C$ 且 $y\in B$, 故知 $(x,y)\in(A\cap C)\times B$. 得證 $(A\times B)\cap(C\times B)\subseteq(A\cap C)\times B$, 因此證明了 $(A\cap C)\times B=(A\times B)\cap(C\times B)$. 同理可證 $A\times(B\cap D)=(A\times B)\cap(A\times D)$. □

利用 Proposition 3.4.12 我們可以求 $(A\cap C)\times(B\cap D)$. 首先將 Proposition 3.4.12 中的 B 以 $B\cap D$ 取代, 得 $(A\cap C)\times(B\cap D)=(A\times(B\cap D))\cap(C\times(B\cap D))$. 再由 $A\times(B\cap D)=(A\times B)\cap(A\times D)$ 以及 $C\times(B\cap D)=(C\times B)\cap(C\times D)$, 我們得

$$(A\cap C)\times(B\cap D)=(A\times B)\cap(A\times D)\cap(C\times B)\cap(C\times D).\tag{3.5}$$

現若 $(x,y)\in(A\times B)\cap(C\times D)$ 表示 $(x,y)\in A\times B$ (知 $x\in A$, $y\in B$) 且 $(x,y)\in C\times D$ (知 $x\in C$, $y\in D$), 故得 $(x,y)\in A\times D$ (因 $x\in A$, $y\in D$) 且 $(x,y)\in C\times B$ (因 $x\in C$, $y\in B$). 因此得 $(x,y)\in(A\times D)\cap(C\times B)$, 得證 $((A\times B)\cap(C\times D))\subseteq((A\times D)\cap(C\times B))$. 故由 Proposition 3.2.5 知式子 (3.5) 可化簡成

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

我們有以下之結果.

Corollary 3.4.13. 假設 A,B,C,D 為 *sets.* 則

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

Question 3.20. 你能利用 *Corollary 3.4.13* 證明 $(A\cap C)\times(B\cap D)=(A\times D)\cap(C\times B)$ 嗎? 試不套用 *Corollary 3.4.13* 直接證明之.

Question 3.21. 試證明 $(A\times B)\cap(C\times D)=(A\times D)\cap(C\times B)$.

一般來說, 我們會想知道一些集合的 Cartesian products 在經過 operations 後是否仍為 Cartesian product. 例如在交集的情形, 我們會想知道兩對集合的 Cartesian products 的交集是否可寫成一對集合的 Cartesian product. 也就是說 $(A\times B)\cap(C\times D)$ 是否仍可寫成一個 Cartesian product $S\times T$ 的形式. 由 Corollary 3.4.13 我們知道這個答案是肯定的. 只要令 $S=A\cap C$, $T=B\cap D$, 則 $(A\times B)\cap(C\times D)=S\times T$. 由此我們也知, 任意多對集合的 Cartesian products 的交集仍為 Cartesian product.

Question 3.22. 假設 $\{A_i, i\in I\}$, $\{B_i, i\in I\}$ 是以 I 為 *index set* 的 *indexed family.* 試證明

$$\bigcap_{i\in I}(A_i\times B_i)=(\bigcap_{i\in I}A_i)\times(\bigcap_{i\in I}B_i).$$

對於 Cartesian product 和 union 也有和 Proposition 3.4.12 類似的關係.

Proposition 3.4.14. 假設 A,B,C,D 為 *sets.* 則

$$(A\cup C)\times B=(A\times B)\cup(C\times B)\quad\text{and}\quad A\times(B\cup D)=(A\times B)\cup(A\times D).$$

Proof. 因 $A\subseteq(A\cup C)$ 且 $C\subseteq(A\cup C)$ 由 Proposition 3.4.11 知 $(A\times B)\subseteq((A\cup C)\times B)$ 且 $(C\times B)\subseteq((A\cup C)\times B)$. 故由 Corollary 3.2.4(2) 得 $(A\times B)\cup(C\times B)\subseteq((A\cup C)\times B)$.

另一方面, 對任意 $(x,y)\in(A\cup C)\times B$, 我們有 $x\in A\cup C$ 以及 $y\in B$, 得 $x\in A$ 或 $x\in C$ 且 $y\in B$. 若 $x\in A$, 則由 $y\in B$ 得 $(x,y)\in A\times B$, 而若 $x\in C$, 則由 $y\in B$ 得 $(x,y)\in C\times B$. 故知 $(x,y)\in A\times B$ 或 $(x,y)\in C\times B$, 亦即 $(x,y)\in(A\times B)\cup(C\times B)$. 得證 $((A\cup C)\times B)\subseteq(A\times B)\cup(C\times B)$, 因此證明了 $(A\cup C)\times B=(A\times B)\cup(C\times B)$. 同理可證 $A\times(B\cup D)=(A\times B)\cup(A\times D)$ □

Question 3.23. 試利用數學歸納法證明當 A,B 為 *finite sets* 時 $\#(A\times B)=\#(A)\times\#(B)$ *(Proposition* 3.4.10*). (Hint:* 固定集合 A 的個數再對集合 B 的個數使用數學歸納法. 需用到 *Proposition* 3.4.14*.)*

利用 Proposition 3.4.14 我們可以求 $(A\cup C)\times(B\cup D)$. 首先將 Proposition 3.4.14 中的 B 以 $B\cup D$ 取代, 得 $(A\cup C)\times(B\cup D)=(A\times(B\cup D))\cup(C\times(B\cup D))$. 再由 $A\times(B\cup D)=(A\times B)\cup(A\times D)$ 以及 $C\times(B\cup D)=(C\times B)\cup(C\times D)$, 我們得以下的結果.

Corollary 3.4.15. 假設 A,B,C,D 為 *sets.* 則

$$(A\cup C)\times(B\cup D)=(A\times B)\cup(A\times D)\cup(C\times B)\cup(C\times D).$$

注意 $(A\cup C)\times(B\cup D)$ 一般來說不會有類似 Corollary 3.4.13 中的性質. 也就是說一般的情形 $(A\cup C)\times(B\cup D)$ 是不會等於 $(A\times B)\cup(C\times D)$ 的. 這是因為一般來說 $A\times D$ 是不會包含於 $(A\times B)\cup(C\times D)$ (除非 $A\subseteq C$ 或 $D\subseteq B$). 所以我們只要考慮 $A\nsubseteq C$ 且 $D\nsubseteq B$, 就能找出反例. 例如當 A,D 皆不是 $\emptyset$ 但 $B=C=\emptyset$, 則 $(A\cup C)\times(B\cup D)=A\times D$ 不為 $\emptyset$ (參見 Proposition 3.4.9), 但 $(A\times B)\cup(C\times D)=\emptyset\cup\emptyset=\emptyset$. 故此時 $(A\cup C)\times(B\cup D)\neq(A\times B)\cup(C\times D)$.

Question 3.24. 試找另外的例子使得 $(A\cup C)\times(B\cup D)\neq(A\times B)\cup(C\times D)$.

從前面的探討, 我們特別強調一下, 除了一些特殊的情況 (例如 $A \subseteq C$ 且 $B \subseteq D$), 在一般的情況 Cartesian product 的聯集 $(A \times B) \cup (C \times D)$ 無法寫成一個 Cartesian product $S \times T$ 的形式.

最後我們看 Cartesian product 和 set difference 之關係.

Proposition 3.4.16. 假設 A, B, C, D 為 *sets.* 則

$$(C \setminus A) \times B = (C \times B) \setminus (A \times B) \quad \text{and} \quad A \times (D \setminus B) = (A \times D) \setminus (A \times B).$$

Proof. 對任意 $(x,y) \in (C \setminus A) \times B$, 我們有 $x \in C \setminus A$ 以及 $y \in B$. 亦即 $x \in C$ 且 $x \notin A$ 以及 $y \in B$. 此時我們知 $(x,y) \in C \times B$ 且 $(x,y) \notin A \times B$ (否則 $(x,y) \in A \times B$ 會導致 $x \in A$ 之矛盾). 故得 $(x,y) \in (C \times B) \setminus (A \times B)$, 證明了 $(C \setminus A) \times B \subseteq (C \times B) \setminus (A \times B)$.

另一方面, 對任意 $(x,y) \in (C \times B) \setminus (A \times B)$, 我們有 $(x,y) \in C \times B$ (得 $x \in C$, $y \in B$) 且 $(x,y) \notin A \times B$ (得 $x \notin A$ 或 $y \notin B$). 但由 $(x,y) \in C \times B$ 我們知 $y \in B$, 故由 $(x,y) \notin A \times B$ 知 $x \notin A$ (否則 $x \in A$ 加上 $y \in B$ 會造成 $(x,y) \in A \times B$ 之矛盾). 因此由 $x \in C$ 且 $x \notin A$ 以及 $y \in B$, 推得 $(x,y) \in (C \setminus A) \times B$, 證明了 $(C \times B) \setminus (A \times B) \subseteq (C \setminus A) \times B$. 得證 $(C \setminus A) \times B = (C \times B) \setminus (A \times B)$. 同理可得 $A \times (D \setminus B) = (A \times D) \setminus (A \times B)$. □

我們也順便討論一下 Cartesian product 和 complement 的關係. 這裡要特別說明, 其實 Cartesian product 很重要的地方是它可以幫我們連結兩個不同宇集中的集合. 也就是說若集合 A 所在的宇集為 X, 而集合 B 所在的宇集為 Y, 我們仍可談論 $A \times B$. 不過此時 $A \times B$ 所在的宇集應為 $X \times Y$. 而這裡我們談 A 的 complement A^c 是指在 X 裡的 complement, 亦即 $A^c = X \setminus A$. 同理 B^c 指的是 B 在 Y 的 complement, 即 $B^c = Y \setminus B$. 而 $A \times B$ 的 complement $(A \times B)^c$, 指的是 $A \times B$ 在 $X \times Y$ 的 complement, 即 $(A \times B)^c = (X \times Y) \setminus (A \times B)$. 所以要特別注意, 這裡三個 complement 分指在三個不同 universal sets 上的 complement.

現將 X, Y 分別寫成 $X = A \cup A^c$, $Y = B \cup B^c$, 考慮 $X \times Y = (A \cup A^c) \times (B \cup B^c)$, 由 Corollary 3.4.15, 得

$$X \times Y = (A \times B) \cup (A \times B^c) \cup (A^c \times B) \cup (A^c \times B^c). \tag{3.6}$$

再由 Corollary 3.4.13, 我們知

$$(A \times B) \cap (A \times B^c) = A \times (B \cap B^c) = \emptyset,$$
$$(A \times B) \cap (A^c \times B) = (A \cap A^c) \times B = \emptyset,$$
$$(A \times B) \cap (A^c \times B^c) = (A \cap A^c) \times (B \cap B^c) = \emptyset.$$

故得

$$(A \times B) \cap ((A \times B^c) \cup (A^c \times B^c) \cup (A^c \times B)) = \emptyset. \tag{3.7}$$

因此連結式子 (3.6), (3.7) 得證以下定理.

Proposition 3.4.17. 假設 A, B 為 *sets.* 則 $(A \times B)^c = (A \times B^c) \cup (A^c \times B^c) \cup (A^c \times B)$.

最後說明一下, 其實我們可以談論三個或更多集合的 Cartesian product. 不過因為我們之後不需用到, 就不探討這方面的問題了.

Chapter 4

Relation and Order

在這一章我們將介紹 relation. Relation 一般有分不同集合之間其元素的 relation 以及同一個集合其元素相互的 relation. 我們將會專注於同一個 set 自身的 relation. 我們會介紹幾種特殊性質的 relation, 其中最重要的是所謂的 equivalence relation. Equivalence relation 可以幫助我們在一個集合之間做分類, 有時定出一個好的 equivalence relation 可以幫助我們更加了解一個 set 的特性. 所以學習 relation 是一個重要的課題. 我們還會介紹另一種 relation, 就是所謂的 order. Order 的意義就是所謂的排序 (比較大小), 所以它是另一個幫助我們了解一個 set 的重要工具.

4.1. Relation

給定兩個 sets X,Y. 若 S 是 $X\times Y$ 的一個 nonempty subset, 我們就稱 S 是一個 *relation* from X to Y. 特別地, 一個 $X\times X$ 的 nonempty subset S 就稱為一個 *relation* on X.

給定一個 relation S 之後, 我們一般會用 $x\sim y$ 來表示 (x,y) 是 S 裡的元素. 這個符號 $x\sim y$ 的好處是容易讓人感受 x 和 y 是有關係的, 比較貼切 relation 字面上的意思. 不過當我們要回歸到利用集合的性質處理 relation 的問題時, 回歸到 $(x,y)\in S$ 的定義, 會比較方便.

Example 4.1.1. (1) 考慮 $X=\{1,0,-1\}$, $Y=\{0,1,2\}$. 定義 $S=\{(x,y)\in X\times Y : y=x^2+1\}$. 則 S 是一個 X 到 Y 的 relation. 在此 relation 之下我們有 $1\sim 2$, $0\sim 1$ 以及 $-1\sim 2$.

(2) 考慮 $X=\{1,0,-1\}$. 定義 $S=\{(x,x')\in X\times X : x>x'\}$. 則 S 是 X 上的一個 relation. 在此 relation 之下我們有 $1\sim 0$, $1\sim -1$ 以及 $0\sim -1$.

Question 4.1. 假設 X 為 *nonempty set.* 考慮 X 上的 *relation* S. 試證明 $S=X\times X$ 若且唯若對任意 $x,y\in X$ 皆有 $x\sim y$.

一般來說一個兩個不同集合的 relation 主要是用來探討兩集合之間的關係, 例如 Example 4.1.1(1) 就是有關 X,Y 兩集合間的函數 $f(x)=x^2+1$ 所產生的 relation. 另一方面同一集合的 relation, 主要用來探討這個集合元素之間的關係, 例如 Example 4.1.1(2) 就是有關集合 X 元素之間的大小關係所產生的 relation.

雖然一開始我們的 relation 是由一個 $X \times Y$ 的子集合開始定起, 然後我們利用 S 來描繪 X,Y 裡的元素之間的關係. 不過我們也可由一個已知 X,Y 裡的元素之間的關係, 來得到 S 這樣的 $X \times Y$ 的子集合. 這樣我們便可利用集合的性質來談論這個 relation 的性質. Example 4.1.1 中的例子事實上就是由已知的關係 (函數, 大小關係) 來描繪 S 這一個集合. 我們看下一個較抽象的例子.

Example 4.1.2. 給定一集合 X 我們要如何定一個 relation 來描繪 X 的子集合間 "包含於" 的關係呢?

首先這個 relation 所關係的元素應該是 X 的子集合, 所以我們應該建立的是 X 的 power set $\mathscr{P}(X)$ 上的 relation. 也就是說我們要找到 $S \subseteq \mathscr{P}(X) \times \mathscr{P}(X)$ 滿足 $A \subseteq B$ 若且唯若 $(A,B) \in S$. 所以我們可以定 $S = \{(A,B) \in \mathscr{P}(X) \times \mathscr{P}(X) : A \subseteq B\}$. 在這個 relation 之下我們就會有 $A \sim B$ 若且唯若 $A \subseteq B$ 了.

接下來在本章中, 我們專注於談論一個集合上的 relation. 也就是假設 S 是一個 relation on X, 在這情況之下, 我們特別有興趣於有以下三種特性的 relation.

Reflexive: 當 S 滿足對所有 $x \in X$ 皆有 $x \sim x$, 即

$$(x,x) \in S, \forall x \in X,$$

我們稱此 relation 是 *reflexive*.

Symmetric: 當 S 滿足對於 $x,y \in X$ 若 $x \sim y$, 則 $y \sim x$, 即

$$(x,y) \in S \Rightarrow (y,x) \in S,$$

我們稱此 relation 是 *symmetric*.

Transitive: 當 S 滿足對於 $x,y,z \in X$ 若 $x \sim y$ 且 $y \sim z$, 則 $x \sim z$, 即

$$((x,y) \in S) \wedge ((y,z) \in S) \Rightarrow (x,z) \in S,$$

我們稱此 relation 是 *transitive*.

對於這三種性質, 我們特別針對幾種大家可能誤解的情況說明一下.

(1) S 為 reflexive 指的是對任意的 $x \in X$ 皆必須有 (x,x) 一定在 S. 並不是說只要存在 $x \in X$ 使得 $(x,x) \in S$ 就是 reflexive. 另外它也沒有說如果 $(x,y) \in S$ 則 $x = y$. 總而言之, 要檢查 S 是否為 reflexive, 我們僅要檢查是否對於 X 中的元素 x, (x,x) 皆會在 S 中, 而不必管其他 (x,y) 其中 $x \neq y$ 的情況.

(2) S 為 symmetric 指的是對任意的 $(x,y) \in S$ 皆必須有 (y,x) 一定也在 S. 並不是說只要存在一組 (x,y) 以及 (y,x) 在 S 中就是 symmetric. 總而言之, 要檢查 S 是否為 symmetric, 我們僅要檢查是否有 $(x,y) \in S$ 但 $(y,x) \notin S$ 的情況發生. 如果沒有才會是 symmetric, 否則就不是 symmetric.

(3) S 為 transitive 指的是只要 (x,y) 和 (y,z) 在 S 中, 則 (x,z) 一定也在 S. 並不是說只要存在一組 $(x,y),(y,z)$ 和 (x,z) 在 S 中就是 transitive. 另外這裡也沒有說只要 $(x,y) \in S$ 則會有一個 $z \in X$ 使得 $(y,z) \in S$. 所以即使 S 僅有一個元素 (x,y) 那麼 S 也是 transitive. 總而言

之, 要檢查 S 是否為 transitive, 我們僅要檢查是否有 $(x,y),(y,z)\in S$ 但 $(x,z)\notin S$ 的情況發生. 如果沒有才會是 transitive, 否則就不是 transitive.

Example 4.1.3. 令 $X=\{1,2,3\}$, 我們探討那些 relation $S\subseteq X\times X$ 是 reflexive, symmetric 或 transitive.

(1) 如果 $S=\{(1,1),(2,2)\}$, 那麼 S 不是 reflexive, 因為 $3\in X$ 但是 $(3,3)\notin S$. 如果 $S=\{(1,1),(2,2),(3,3),(1,2)\}$, 那麼 S 是 reflexive. 注意在此例中雖然 S 中存在 (x,y) 但 $x\neq y$ 這樣的元素 (即 $(1,2)\in S$) 但不影響其為 reflexive 的事實.

(2) 當 $S=\{(1,1),(2,2)\}$, 我們知 S 不是 reflexive, 不過 S 是 symmetric. 但若加入 $(1,2)$, 即 $S=\{(1,1),(2,2),(1,2)\}$, 此時因 $(1,2)\in S$ 但 $(2,1)\notin S$, 故 S 不是 symmetric. 此時 S 還要加入 $(2,1)$ (即 $S=\{(1,1),(2,2),(1,2),(2,1)\}$) 才會變成 symmetric.

(3) 當 $S=\{(1,1),(2,2),(1,2)\}$, 我們知 S 不是 reflexive, 也不是 symmetric, 但它是 transitive. 但若加入 $(2,3)$, 即 $S=\{(1,1),(2,2),(1,2),(2,3)\}$, 此時因 $(1,2),(2,3)\in S$ 但 $(1,3)\notin S$, 故 S 不是 transitive. 此時 S 還要加入 $(1,3)$ (即 $S=\{(1,1),(2,2),(1,2),(2,3),(1,3)\}$) 才會變成 transitive.

從上一個 Example 我們可以看出 reflexive, symmetric 以及 transitive 是相互獨立的. 也就是說這三個性質相互之間沒有關係. 有可能一個 relation 符合其中一個性質, 但不符合另外兩個性質. 例如有可能一個 relation 是 reflexive 但不是 symmetric 也不是 transitive. 另一方面, 也有可能一個 relation 符合其中兩個性質, 但不符合另外一個性質. 例如有可能一個 relation 是 reflexive 以及 symmetric 但不是 transitive. 這裡最常發現的是以下錯誤的論述誤以為 symmetric 和 transitive 可推得 reflexive.

Example 4.1.4. 假設 X 為一個 set, 而 S 為 X 上的一個 relation. 假設 S 為 symmetric 以及 transitive, 是否可推得 S 為 reflexive? 以下的論述哪裡有錯?

假設 $x\sim y$, 由於 S 為 symmetric, 因此知 $y\sim x$. 也就是說, 我們有 $x\sim y$ 且 $y\sim x$, 故利用 transitive 的性質, 推得 $x\sim x$.

這個論述沒有錯, 錯的是它並沒有證得 S 是 reflexive. 它僅證得了, 對於 $x\in X$, 如果存在 $y\in X$ 滿足 $x\sim y$, 則 $x\sim x$. 但 reflexive 的性質, 最重要的關鍵在於對每一個 $x\in X$, 皆有 $x\sim x$. 現若在 X 中存在一元素 x 根本沒有任何元素和它有關, 也就是說找不到 $y\in X$ 滿足 $x\sim y$, 那麼我們就沒辦法得到 $x\sim x$ 了. 例如 $X=\{1,2,3\}$ 的情形, 若 $S=\{(1,1),(2,2),(1,2),(2,1)\}$, 很容易驗證 S 為 symmetric 以及 transitive. 由於 1 找得到元素和它有關 (例如我們有 $1\sim 2$), 而 2 也找得 1 和它有關 (即 $2\sim 1$), 所以由 S 為 symmetric 以及 transitive 知 $(1,1)$, $(2,2)$ 皆在 S 中. 然而, 沒有任何和 3 有關的元素, 所以 $(3,3)$ 未必會出現在 S 中. 在此例中 $(3,3)\notin S$, 所以 S 雖為 symmetric 以及 transitive, 但 S 不是 reflexive.

Question 4.2. 令 $X=\{1,2,3\}$ 舉例說明存在 *relation on* X 滿足 *reflexive* 以及 *symmetric* 的性質, 但不滿足 *transitive* 的性質. 並舉例說明存在 *relation on* X 滿足 *reflexive* 以及 *transitive* 的性質, 但不滿足 *symmetric* 的性質.

最後我們再看 Example 4.1.2 中的 relation 符合哪些性質.

Example 4.1.5. 假設 X 為 nonempty set. 考慮 $S=\{(A,B)\in\mathscr{P}(X)\times\mathscr{P}(X):A\subseteq B\}$ 為 $\mathscr{P}(X)$ 上的 relation. 首先我們說明 S 為 reflexive. 這是因為對於任意 $A\in\mathscr{P}(X)$, 我們有 $A\subseteq A$ (參見 Proposition 3.1.4(1)), 故 $(A,A)\in S$. 得知 S 為 reflexive. 我們也可得 S 為 transitive. 這是因為若 $(A,B)\in S$ 且 $(B,C)\in S$, 表示 $A\subseteq B$ 且 $B\subseteq C$, 故可得 $A\subseteq C$ (參見 Proposition 3.1.4(2)). 亦即 $(A,C)\in S$, 得證 S 為 transitive. 不過 S 不是 symmetric. 要說明這點, 我們只要找到 $A,B\in\mathscr{P}(X)$ 滿足 $(A,B)\in S$ 但 $(B,A)\notin S$ 即可. 考慮 $A=\emptyset$ 以及 $B=X$ 即可. 這是因為 $\emptyset\in\mathscr{P}(X)$ 且 $X\in\mathscr{P}(X)$ 且 $\emptyset\subseteq X$, 故知 $(\emptyset,X)\in S$. 但已知 $X\neq\emptyset$, 故 $X\nsubseteq\emptyset$, 也就是說 $(X,\emptyset)\notin S$. 得證 S 不是 symmetric.

Question 4.3. 假設 X 為 *nonempty set.* 考慮 $S=\{(A,B)\in\mathscr{P}(X)\times\mathscr{P}(X):A\cup B=X\}$ 為 $\mathscr{P}(X)$ 上的 *relation.*

(1) 試問 S 一定為 *reflexive* 嗎? 若答案是否定的, 那 S 一定不是 *reflexive* 嗎?

(2) 試問 S 一定為 *symmetric* 嗎? 若答案是否定的, 那 S 一定不是 *symmetric* 嗎?

(3) 試問 S 一定為 *transitive* 嗎? 若答案是否定的, 那 S 一定不是 *transitive* 嗎?

4.2. Equivalence Relation

在所有的 relation 中, 最重要的便是所謂 equivalence relation. 它可以幫我們將一個很複雜的集合做分類, 亦即分成所謂的 equivalence classes, 以便讓我們更容易掌握這個集合. 將來在許多數學課程裡, 大家會發現它是一個很方便的工具.

家裡有許多書或是 cd, 要如何找到你想要的書或 cd 呢? 當然最好的方法就是將它們分類. 同樣的, 在數學, 對於一個有很多元素的的集合, 我們也可藉由分類的方法來處理這一個集合的相關問題. 一般來說一個好的分類方式必須符合以下三個要素. 第一個就是, 要被分類的東西, 自己和自己必須是是同類的; 另一要素是若甲和乙是同類的則乙也必須和甲是同類的; 最後一個要素是如果甲和乙同類且乙和丙同類, 則甲必須和丙同類. 如果我們將一個集合 X 的元素利用這個三個原則分類, 然後將同類的東西視為相關, 例如若 x,y 同類, 則用 $x\sim y$ 來表示. 在這個符號之下, 前面所說的分類的第一個要素: 自己和自己是同類的, 就可表示為對所有 $x\in X$ 皆有 $x\sim x$. 也就是這樣定出的 relation 必為 reflexive. 而第二個要素: 若甲和乙是同類的則乙也必須和甲是同類的, 就可表示為若 $x\sim y$ 則 $y\sim x$. 也就是這樣定出的 relation 必為 symmetric. 最後一個要素: 若甲和乙同類且乙和丙同類, 則甲必須和丙同類, 就可表示為若 $x\sim y$ 且 $y\sim z$ 則 $x\sim z$. 也就是這樣定出的 relation 必為 transitive. 反之, 現如果有一個在 X 上的 relation S 具有 reflexive, symmetric 以及 transitive 這三項性質, 而且我們將符合這個 relation 的元素視為同類 (即若 $x\sim y$, 則是為 x,y 為同類), 那麼這樣的分類方式也會符合好的分類方式的三個要素. 因此我們給符合 reflexive, symmetric 以及 transitive 這三項性質的 relation 一個特殊的名稱. 由於在本節中我們不需要將一個在 X 上的 relation 視為 $X\times X$ 的 subset 來處理問題, 為了方便起見, 我們直接用 $\sim$ 是 X 上的一個 relation 這樣的說法.

Definition 4.2.1. 假設 $\sim$ 是集合 X 上的 relation, 若符合以下三個性質, 則稱此 relation 為 *equivalence relation*

Reflexive: 對所有 $x \in X$, 皆有 $x \sim x$.

Symmetric: 若 $x, y \in X$ 滿足 $x \sim y$, 則 $y \sim x$.

Transitive: 若 $x, y, z \in X$ 滿足 $x \sim y$ 且 $y \sim z$, 則 $x \sim z$.

到底用 equivalence relation 來分類有什麼好處呢? 首先由 reflexive 的性質可得每一個元素都會被分到某一類. 另外由 symmetric 和 transitive 的性質知不會有一個元素會同時分屬於不同的類別, 也就是說兩個不同類的元素所成的集合不會有交集; 這是因為如果 A, B 為不同類, 但 x 在 A 類且在 B 類中. 則在 A 類中的任一元素 a 因和 x 是同類的故 $a \sim x$ 而 B 類中的任一元素 b 因也和 x 同類故 $b \sim x$. 故由 symmetric 和 transitive 的性質知 $a \sim b$. 也就是說 A 中的所有元素和 B 中的所有元素都同類. 這和 A 與 B 是不同類的假設相矛盾。

現假設 $\sim$ 是一個在集合 X 上的 equivalence relation. 對於 $x \in X$, 我們考慮集合 $\{y \in X : y \sim x\}$, 即我們將所有 X 中和 x 相關的元素收集起來. 這樣的集合, 我們稱為 x 的 *equivalence class*, 用 $[x]$ 來表示. 用分類的角度來說, $[x]$ 就是所有和 x 同類的元素所成的集合. 依 reflexive 的定義, 我們知道 $[x]$ 絕對不是空集合, 因為至少 $x \sim x$, 也就是說我們有 $x \in [x]$. 另一方面依定義若 $y \sim x$, 則 $[x] = [y]$. 這是因為, 對任意 $z \in [x]$, 表示 $z \sim x$. 然而又假設 $y \sim x$, 故由 symmetric 及 transitive 得 $z \sim y$, 即 $z \in [y]$. 得證 $[x] \subseteq [y]$. 同理可得 $[y] \subseteq [x]$, 故知 $[y] = [x]$. 另外一方面如果 $y \not\sim x$ (即表示 $(y, x) \notin S$), 則如同前面不同類的集合交集為 $\emptyset$ 的解釋, 我們知 $[y] \cap [x] = \emptyset$. 換言之, 利用 X 上的 equivalence relation $\sim$, 我們可將 X 分成一些互不相交的 equivalence classes 的聯集. 通常我們會用 $X/\sim$ 這個符號表示將 X 利用此 equivalence relation 所分出的 equivalence classes. 簡單來說 $X/\sim$ 就是告訴我們用 $\sim$ 這個關係將 X 分成了哪幾類. 由於這樣的分類將 X 分割成好幾個不相交的 subsets 的聯集, 我們稱此為 X 上的一個 partition, 其正式定義如下.

Definition 4.2.2. 假設 X 為 set, I 為 index set. 若對於任意 $i \in I$, C_i 為 X 的 nonempty subset 且 $X = \bigcup_{i \in I} C_i$ 以及 $C_i \cap C_j = \emptyset$, for $i \neq j$, 則稱此 $\{C_i : i \in I\}$ 為 X 的一個 *partition*.

簡單來說給定一個 X 上的 partition, 就是將 X 上的元素分類. 前面已知道, 給定一個 X 上的 equivalence relation, 考慮此 equivalence relation 所成的 equivalence classes (也就是說將同類的收集起來) 就會是 X 的一個 partition. 現在我們考慮反過來, 若給定 X 上的 partition $X = \bigcup_{i \in I} C_i$, 對於任意 $x, y \in X$, 我們定義 $x \sim y$ 若且唯若 $x, y \in C_i$, for some $i \in I$ (亦即同類的元素視為相關), 則在此定義之下, 我們可得 $\sim$ 是一個 equivalence relation. 這是因為依定義 $X = \bigcup_{i \in I} C_i$, 因此對於任意 $x \in X$, 皆存在 $i \in I$, 使得 $x \in C_i$, 因此得 $x \sim x$ (證得 reflexive). 另外若 $x \sim y$, 表示 $x, y \in C_i$, for some $i \in I$, 當然也有 $y, x \in C_i$, 故得 $y \sim x$ (證得 symmetric). 最後若 $x \sim y$, $y \sim z$, 知存在 $i, j \in I$ 使得 $x, y \in C_i$, $y, z \in C_j$. 由於 $y \in C_i \cap C_j$, 利用若 $i \neq j$ 則 $C_i \cap C_j = \emptyset$ 得知 $i = j$. 亦即 $x, z \in C_i$, 因此得 $x \sim z$ (證得 transitive). 我們得到以下的定理.

Theorem 4.2.3. 假設 X 為 *set.*

(1) 若 $\sim$ 為 X 上的一個 *equivalence relation,* 則 $\{[x] : [x] \in X/\sim\}$ 是 X 的一個 *partition.*

(2) 若 I 為 *index set* 且 $\{C_i : i \in I\}$ 為 X 的一個 *partition,* 對於任意 $x,y \in X$, 定義 $x \sim y$ 若且唯若 $x,y \in C_i$, *for some* $i \in I$, 則 $\sim$ 為 X 上的一個 *equivalence relation.*

Example 4.2.4. 若我們將整數 $\mathbb{Z}$ 分為 2 的倍數所成的集合 $C_1 = \{2n : n \in \mathbb{Z}\}$, 3 的倍數所成的集合 $C_2 = \{3n : n \in \mathbb{Z}\}$ 以及 5 的倍數所成的集合 $C_3 = \{5n : n \in \mathbb{Z}\}$, 則 $\{C_1, C_2, C_3\}$ 不是一個 $\mathbb{Z}$ 的 partition. 因為 7 就不是 2, 3 或是 5 的倍數 (亦即 $7 \notin C_1 \cup C_2 \cup C_3$), 故知 $\mathbb{Z} \neq C_1 \cup C_2 \cup C_3$. 另外 $C_1 \cap C_2 \neq \emptyset$, 例如我們有 $6 \in C_1 \cap C_2$. 同理 $C_1 \cap C_3 \neq \emptyset$, $C_2 \cap C_3 \neq \emptyset$.

若考慮 $\mathbb{Z}$ 的 3 個 subset $C_1 = \{n : n = 3m, m \in \mathbb{Z}\}, C_2 = \{n : n = 3m+1, m \in \mathbb{Z}\}$ 以及 $C_3 = \{n : n = 3m+2, m \in \mathbb{Z}\}$, 則 $\{C_1, C_2, C_3\}$ 是一個 $\mathbb{Z}$ 的 partition. 事實上, 我們可以將 C_1, C_2, C_3 分別看成除以 3 餘數分別為 0, 1 以及 2 的元素所成的集合. 很容易看出 $\mathbb{Z} = C_1 \cup C_2 \cup C_3$, 而且 $C_1 \cap C_2 = C_1 \cap C_3 = C_2 \cap C_3 = \emptyset$. 利用這個 partition, 我們可以定出 $\mathbb{Z}$ 中的一個 equivalence relation 為 $x \sim y$ 若且唯若 $x,y \in C_i$, for some $i \in \{1,2,3\}$. 若 $x,y \in C_1$ 表示 $x = 3m, y = 3m'$ for some $m, m' \in \mathbb{Z}$ 所以 $x - y = 3(m - m')$, 亦即 $3 \mid x-y$ (表示 3 可以整除 $x-y$). 同理當 $x,y \in C_2$ 或 $x,y \in C_3$, 皆有 $3 \mid x-y$. 所以我們知此 equivalence relation 可定義為 $x \sim y$ 若且唯若 $3 \mid x-y$. 很容易檢查 $\sim$ 是 equivalence relation. 首先對所有 $x \in \mathbb{Z}$, 我們有 $3 \mid x-x$, 所以 $x \sim x$. 另外若 $x \sim y$, 表示 $3 \mid x-y$, 故有 $3 \mid -(x-y)$. 因此得 $3 \mid y-x$, 即 $y \sim x$. 最後若 $x \sim y$ 且 $y \sim x$, 表示 $3 \mid x-y$ 且 $3 \mid y-z$. 因此得 $3 \mid (x-y)+(y-z)$, 即 $3 \mid x-z$. 得證 $x \sim z$. 在這裡我們有 $C_1 = [0] = [4]$, $C_2 = [1] = [-3]$ 以及 $C_3 = [2] = [11]$... 等. 我們有 $\mathbb{Z}/\sim = \{[0], [1], [2]\}$.

Question 4.4. 對於任意正整數 m, 令 $I = \{0, 1, \ldots, m-1\}$ 為 *index set.* 考慮 Z 的 *partition,* $C_i = \{mk + i : k \in \mathbb{Z}\}$, $i \in I$. 試問此 *partition* 所對應的 *equivalence relation* 為何?

利用 equivalence relation 將集合分類成 partition 後再利用此分類來探討此集合, 這樣的方法將來大家學習一些數學的理論時會用到. 目前我們僅介紹一個簡單的應用. 就是它可以幫我們計算一個有限集合的個數. 我們有以下的定理.

Proposition 4.2.5. 假設 X 是一個 *finite set,* 且用一個 *equivalence relation* 將其分成 *equivalence classes* $C_1, \ldots, C_n$. 若 $\#(X)$ 及 $\#(C_i)$ 表示這些集合的元素的個數, 則

$$\#(X) = \sum_{i=1}^{n} \#(C_i).$$

Proof. 由前面說明已知當 $i \neq j$ 時, $C_i \cap C_j = \emptyset$. 也就是說這些 C_i 是兩兩不相交的. 再加上每個 X 中的元素都會落在某個 C_i 中, 所以 X 的元素的個數剛好是這些 $C_1, \ldots, C_n$ 的元素個數之和. □

Example 4.2.6. 令 $A = \{1,2,3\}$ 且令 $X = \mathscr{P}(A)$. 考慮 X 上的 relation, 其定義為對任意 $B, C \in X$, $B \sim C$ 若且唯若 $\#(B) = \#(C)$. 很容易看出 $\sim$ 為 X 上的 equivalence relation. 這是因為, 對任意 $B \in X$, 我們有 $\#(B) = \#(B)$, 故知 $B \sim B$. 又若 $B \sim C$, 表示 $\#(B) = \#(C)$, 故

由 $\#(C)=\#(B)$, 得 $C\sim B$. 最後若 $B\sim C$ 且 $C\sim D$, 則由 $\#(B)=\#(C)$ 以及 $\#(C)=\#(D)$ 得 $\#(B)=\#(D)$. 故得 $B\sim D$.

利用這個 equivalence relation 所得的 equivalence classes 形成 $X=\mathscr{P}(A)$ 的一個 partition. 我們有以下的 partition:

沒有元素: $\{\emptyset\}$

一個元素: $\{\{1\},\{2\},\{3\}\}$.

二個元素: $\{\{1,2\},\{1,3\},\{2,3\}\}$.

三個元素: $\{\{1,2,3\}\}$.

注意這幾個 equivalence classes 的元素個數分別為 $\binom{3}{0}$, $\binom{3}{1}$, $\binom{3}{2}$, $\binom{3}{3}$. 所以由 Proposition 4.2.5 知

$$\binom{3}{0}+\binom{3}{1}+\binom{3}{2}+\binom{3}{3}=\#(X)=\#(\mathscr{P}(A))=2^3=8.$$

Question 4.5. 令 n 為正整數, $A=\{1,2,\ldots,n\}$ 且令 $X=\mathscr{P}(A)$. 考慮 X 上的 *relation,* 其定義為對任意 $B,C\in X$, $B\sim C$ 若且唯若 $\#(B)=\#(C)$. 若 $m\in\mathbb{N}$ 且 $0<m<n$, 試問 $\{1,2,\ldots,m\}$ 所在的 *equivalence class* 其元素個數為何? 試證明

$$\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n-1}+\binom{n}{n}=2^n.$$

4.3. Order Relation

在數學上另一種常見的 relation 就是所謂 order relation, 亦即排序的關係. 它是一種符合三種性質的 relation, 這類的 relation 和我們習慣的比較大小關係有一致的性質, 因此稱為 order relation.

以下介紹的 relation 由於和比較大小有類似的性質, 大家可以將之視為 "小於等於" 這樣的關係. 為了讓大家習慣它的性質, 我們不用 $\sim$ 這個符號, 不過不希望誤以為它就是一般的 "小於等於", 所以我們選用 "$\preceq$" 這個符號.

Definition 4.3.1. 假設 X 為 nonempty set 且 $\preceq$ 為 X 上的 relation. 若 $\preceq$ 符合以下三種性質, 我們便稱 $\preceq$ 為 X 上的 *partial order.*

(1) 對所有 $x\in X$, 皆有 $x\preceq x$.

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

(3) 若 $x,y,z\in X$ 滿足 $x\preceq y$ 且 $y\preceq z$, 則 $x\preceq z$.

在 Definition 4.3.1 的性質 (1) 我們知道就是 reflexive 性質, 而性質 (3) 就是 transitive 性質. 不過性質 (2) 和 symmetric 性質就差很多了. 它指的是若 $x\neq y$, 則不可能同時會有 $x\preceq y$ 且 $y\preceq x$. 若我們仍用 $S\subseteq X\times X$ 來表示這個 relation, 由於這個性質說的是當 $x\neq y$ 時, (x,y) 和 (y,x) 不可能同時在 S 中, 故我們稱這個性質為 *anti-symmetric.* 當 $\preceq$ 為 X 上的一個 partial order, 一般我們就簡稱 $(X,\preceq)$ 為一個 *poset.*

Example 4.3.2. 假設 A 為 nonempty set, 令 $X=\mathscr{P}(A)$. 考慮 X 上一般集合包含於的 relation $\subseteq$, 則 $(X,\subseteq)$ 就是一個 poset.

Question 4.6. 假設 A 為 *nonempty set,* 令 $X=\mathscr{P}(A)$. 考慮 X 上一般集合的 *relation* $\supseteq$, 則 $(X,\supseteq)$ 是否是一個 *poset?*

Question 4.7. 考慮實數 $\mathbb{R}$ 一般的小於等於關係 $\leq$, 是否 $(\mathbb{R},\leq)$ 為 *poset?* 又 $(\mathbb{R},\geq)$ 是否為 *poset?*

在一個 poset $(X,\preceq)$ 中, 若 $x,y\in X$ 滿足 $x\preceq y$ 或 $y\preceq x$, 則稱 x,y 這兩個元素為 *comparable* (意指可以比較). Definition 4.3.1 之所以會稱為 "partial" order, 就是因為它並沒有要求任兩個 X 中的元素都是 comparable. 例如考慮 $A=\{1,2\}$ 的情形, 我們知 $\subseteq$ 是 $\mathscr{P}(A)$ 上的 partial order. 然而 $\{1\},\{2\}\in\mathscr{P}(A)$ 並不是 comparable, 因為 $\{1\}\subseteq\{2\}$ 和 $\{2\}\subseteq\{1\}$ 皆不成立. 不過實數 $(\mathbb{R},\leq)$ 這個 poset 就有任兩個元素皆為 comparable 的性質. 因此我們又特別考慮以下的 order relation.

Definition 4.3.3. 假設 X 為 nonempty set 且 $\preceq$ 為 X 上的 relation. 若 $\preceq$ 符合以下三種性質, 我們便稱 $\preceq$ 為 X 上的 *total order.*

(1) 若 $x,y\in X$ 滿足 $x\preceq y$ 且 $y\preceq x$, 則 $x=y$.

(2) 若 $x,y,z\in X$ 滿足 $x\preceq y$ 且 $y\preceq z$, 則 $x\preceq z$.

(3) 對所有 $x,y\in X$, 皆有 $x\preceq y$ 或 $y\preceq x$.

Definition 4.3.3 的性質 (3) 便是要求任兩個元素皆要 comparable, 這個性質就是 *total* 的性質. 要注意由 (3) 的性質, 便可得到 reflexive, 因為這裡 x,y 沒有要求要相異, 所以依定義, 我們會有 $x\preceq x$. 也因此我們知一個 total order 一定是 partial order (反過來就不一定對). 當 $\preceq$ 為 X 上的 total order, 一般我們就稱 $(X,\preceq)$ 為一個 *total ordered set.* 另外有的書會稱 total order 為 *linear order* 或是 *simple order.*

Question 4.8. 考慮實數 $\mathbb{R}$ 一般的小於關係 $<$, 是否 $(\mathbb{R},<)$ 為 *total ordered set?*

或許大家會好奇前面談的 order $\preceq$ 都有一個 "等號", 也就是說 $x\preceq x$ 成立的原因是 $x=x$. 那麼是否可以像實數的 $\leq$ 去掉等號得到 $<$ 這樣的 order 呢? 事實上, 如果 $(X,\preceq)$ 是一個 total ordered set, 我們可以定義 $x\prec y$ 若且唯若 $x\preceq y$ 且 $x\neq y$. 在這情況之下, 我們便稱 $\prec$ 為 X 的一個 *strict total order.* 我們有以下的定義.

Definition 4.3.4. 假設 X 為 nonempty set 且 $\prec$ 為 X 上的 relation. 若 $\prec$ 符合以下二種性質, 我們便稱 $\prec$ 為 X 上的 *strict total order.*

(1) 若 $x,y,z\in X$ 滿足 $x\prec y$ 且 $y\prec z$, 則 $x\prec z$.

(2) 對所有 $x,y\in X$, 皆會滿足 $x=y$, $x\prec y$ 或 $y\prec x$ 其中之一, 且其中僅有一個會成立.

在 Definition 4.3.4 中, 性質 (2) 稱為 *trichotomy* (三一律).

Example 4.3.5. 我們可以對所有複數所成的集合 $\mathbb{C}$ 定義一個 strict order. 對任意 $a+bi, c+di \in \mathbb{C}$, 其中 $a,b,c,d \in \mathbb{R}$ 且 $i^2=-1$. 我們定義 $(a+bi) \prec (c+di)$ 若且唯若 (1) $a<c$ 或 (2) $a=c$ 且 $b<d$. 此時 $(\mathbb{C}, \prec)$ 便是 strict total ordered set. 首先檢查 transitive 性質. 假設 $a+bi, c+di, e+fi \in \mathbb{C}$ 其中 $a,b,c,d,e,f \in \mathbb{R}$ 滿足 $(a+bi) \prec (c+di)$ 且 $(c+di) \prec (e+fi)$. 依 $\prec$ 的定義, 我們知此時 $a \leq c$ 且 $c \leq e$, 因此得 $a \leq e$. 我們可以分成兩種情況討論: (一) 若 $a<e$, 則由 $\prec$ 的定義得 $(a+bi) \prec (e+fi)$; (二) 若 $a=e$, 則可得 $a=c=e$. 此時由 $(a+bi) \prec (c+di)$ 知 $b<d$, 再由 $(c+di) \prec (e+fi)$ 知 $d<f$. 故得 $b<f$, 因此依 $\prec$ 的定義得 $(a+bi) \prec (e+fi)$. 證明了 $\prec$ 符合 transitive 性質. 至於三一律, 若 $a+bi \neq c+di$, 依複數相等的定義知 $a \neq c$ 或 $b \neq c$. 若 $a \neq c$, 依實數的三一律知 $a<c$ 或 $c<a$, 也就是說此時 $(a+bi) \prec (c+di)$ 或 $(c+di) \prec (a+bi)$. 而若 $a=c$, 此時必有 $b \neq d$, 故依然由實數的三一律可得 $(a+bi) \prec (c+di)$ 或 $(c+di) \prec (a+bi)$. 我們證明了任兩複數在 $\prec$ 之下皆為 comparable, 證得了 $\prec$ 有 trichotomy 的性質.

在此定義之下 $(\mathbb{C}, \prec)$ 為 strict total ordered set 且它保持了原本實數上 $<$ 這個 order. 不過為甚麼常聽說複數不能比大小呢? 其實這是簡略的說法. 事實上, 實數和複數它們不只是 sets, 它們的元素之間還有加法及乘法運算. 所以我們在談其上的 order 時其實還多要求了兩個性質. 即在實數的情形我們多了和加法與乘法有關的兩個性質:

A: 若 $a<b$, 則對任意 c 皆有 $a+c<b+c$.

M: 若 $a<b$, 則對任意 $0<c$ 皆有 $ac<bc$.

很容易驗證剛才定義複數上的 $\prec$ 符合性質 A. 但是它不符合性質 M. 這是因為依定義我們有 $0 \prec i$, 但若性質 M 成立, 則有 $0 \times i \prec i \times i$, 即 $0 \prec -1$. 此與 $\prec$ 之定義不符, 故知 $\prec$ 不符合性質 M.

事實上, 我們可以證明在 $\mathbb{C}$ 上面不可能定義出一個 strict total order $\prec$ 會保持原本實數的大小關係且符合性質 A 和 M. 這是因為若 $(\mathbb{C}, \prec)$ 符合這些要求, 則依三一律, 我們有 $0 \prec i$ 或 $i \prec 0$ 兩種情況會發生. 若 $0 \prec i$, 則由性質 M 會推得 $0 \prec -1$, 不符合原本實數的大小關係. 而若 $i \prec 0$, 則由性質 A 可推得 $i+(-i) \prec 0+(-i)$, 即 $0 \prec -i$. 此時再由性質 M, 可推得 $0 \times (-i) \prec (-i) \times (-i)$, 即 $0 \prec -1$, 同樣的不符合原本實數的大小關係. 因為在 $\mathbb{C}$ 上是不可能存在 strict total order 符合這些性質, 所以我們才簡略的說複數是不能比大小的.

要注意 strict total order 並不是 total order. 但如前面所述, 每一個 total ordered set $(X, \preceq)$, 都可定義一個 strict total order.

Proposition 4.3.6. 假設 $(X, \preceq)$ 是一個 *total ordered set.* 若定義 $x \prec y$ 若且唯若 $x \preceq y$ 且 $x \neq y$, 則在此定義之下, $\prec$ 為 X 的一個 *strict total order.*

Proof. 首先我們證明 transitive 性質, 即若 $x,y,z \in X$ 滿足 $x \prec y$ 且 $y \prec z$, 則要證明 $x \prec z$. 由於 $x \prec y$ 表示 $x \preceq y$ 且 $x \neq y$, 而 $y \prec z$ 表示 $y \preceq z$ 且 $y \neq z$. 故由 $\preceq$ 為 total order 有 transitive 性質, 得 $x \preceq z$. 我們必須證明 $x \neq z$. 利用反證法, 假設 $x=z$, 由 $x \preceq y$ 得 $z \preceq y$. 但又已知 $y \preceq z$, 故由 $\preceq$ 為 total order 有 anti-symmetric 性質, 得 $y=z$. 此與當初假設 $y \prec z$ (即 $y \neq z$) 相矛盾, 故知 $x \neq z$. 得證 $x \prec z$.

接著我們證明 trichotomy 性質. 因 $\preceq$ 為 total order 有 total 性質, 亦即對任意 $x,y\in X$, 我們有 $x\preceq y$ 或 $y\preceq x$. 現若 $x=y$, 我們得 x,y 滿足 $x=y$. 而若 $x\neq y$, 則由 $x\preceq y$ 或 $y\preceq x$, 得 $x\prec y$ 或 $y\prec x$. 得證 x,y 滿足 $x=y$, $x\prec y$ 或 $y\prec x$. 現要說明 x,y 僅能滿足 $x=y$, $x\prec y$ 或 $y\prec x$ 其中之一. 首先若 $x=y$, 依 $\prec$ 之定義我們知不可能 $x\prec y$ 或 $y\prec x$ 成立. 而若 $x\neq y$ 我們用反證法證明不可能 $x\prec y$, $y\prec x$ 兩者皆成立. 假設 $x\prec y$, $y\prec x$ 兩者皆成立, 由 $\prec$ 之定義知 $x\preceq y$ 且 $y\preceq x$. 再次由 anti-symmetric 性質, 得 $x=y$. 此與 $x\neq y$ 之假設相矛盾. 得證不可能 $x\prec y$, $y\prec x$ 兩者皆成立. □

同樣的, 若已知 $\prec$ 為 X 上的 strict total order, 對任意 $x,y\in X$, 我們定義 $x\preceq y$ 若且唯若 $x=y$ 或 $x\prec y$, 則 $\preceq$ 會是 X 上的 total order.

Question 4.9. 假設 X 為 *nonempty set* 且 $\prec$ 為 X 上的 *strict total order.* 若對任意 $x,y\in X$, 我們定義 $x\preceq y$ 若且唯若 $x=y$ 或 $x\prec y$, 試證明 $\preceq$ 會是 X 上的 *total order.*

從這裡, 我們知道給了 X 上一個 total order 就等同於給了一個 strict total order, 反之亦然. 所以當談論到 total order 的性質, 我們都可以轉換成 strict total order 的性質. 為了方便起見, 當我們用 $\preceq$ 表示一個 total order, 則會用 $\prec$ 表示其對應的 strict total order, 反之亦然.

有了 order 的關係後, 我們就可以定義所謂的上下界, 最大最小元素. 假設 $(X,\preceq)$ 為 poset. 對於 X 中的非空子集 T, 我們說 $u\in X$ 是 T 的一個 *upper bound*, 表示對於任意 T 中的元素 t 皆滿足 $t\preceq u$. 假設 $u\in X$ 是 T 的 upper bound 且對任意 T 的 upper bound u', 皆滿足 $u\preceq u'$, 則稱 u 為 T 的 *least upper bound* (或 *supremum*). 相對應的, 我們稱 $l\in X$ 為 T 的一個 *lower bound*, 表示對於任意 T 中的元素 t 皆滿足 $l\preceq t$. 假設 $l\in X$ 是 T 的 lower bound 且對任意 T 的 lower bound l', 皆滿足 $l'\preceq l$, 則稱 l 為 T 的 *greatest lower bound* (或 *infimum*).

要注意, 一般來說 poset $(X,\preceq)$ 的 nonempty subset 未必會有 upper bound 或 lower bound. 而即使有 upper bound 或 lower bound, 仍有可能 least upper bound 或 greatest lower bound 會不存在. 我們看以下的例子:

Example 4.3.7. (A) 考慮 $(\mathbb{R},\leq)$ 這個 total ordered set. 令 $T=\{x\in\mathbb{R}:0<x<1\}$. 所有大於等於 1 的實數都是 T 的 upper bound, 而 1 是 T 的 least upper bound. 所有小於等於 0 的實數都是 T 的 lower bound, 而 0 是 T 的 greatest lower bound. 至於 $\{x\in\mathbb{R}:x\geq 0\}$, 則無 upper bound. 而 $\{x\in\mathbb{R}:x<1\}$, 則無 lower bound.

(B) 考慮 $(\mathbb{Q},\leq)$ 這個 total ordered set. 令 $T=\{x\in\mathbb{Q}:\sqrt{2}<x<\sqrt{3}\}$. 所有大於 $\sqrt{3}$ 的有理數都是 T 的 upper bound, 而所有小於 $\sqrt{2}$ 的有理數都是 T 的 lower bound. 但是 T 沒有 least upper bound. 這是因為若 $u\in\mathbb{Q}$ 為 T 的 least upper bound, 表示 $\sqrt{3}<u$, 但 $\sqrt{3}$ 和 u 之間仍存在著有理數 (這是有理述的稠密性), 也就是說存在 $u'\in\mathbb{Q}$ 滿足 $\sqrt{3}<u'<u$. 既然 u' 為 T 的 upper bound 但又小於 u, 此與 u 為 T 的 least upper bound 相矛盾, 故知 T 沒有 least upper bound. 同理我們知 T 沒有 greatest lower bound.

(C) 給定 nonempty set A, 考慮 $(\mathscr{P}(A),\subseteq)$ 這個 poset. 對於任意 $\mathscr{P}(A)$ 的 nonempty subset $\mathscr{T}$, A 是 $\mathscr{T}$ 的 upper bound, 因為對任何 $B\in\mathscr{T}$, 皆有 $B\subseteq A$. 同理 $\emptyset$ 為 $\mathscr{T}$ 的 lower bound. 此時 $\mathscr{T}$ 的 least upper bound 一定存在, 事實上 $U=\bigcup_{B\in\mathscr{T}} B$ 會是 $\mathscr{T}$ 的 least upper bound. 這是因為對任意 $B\in\mathscr{T}$, 皆有 $B\subseteq U$, 所以 U 是 $\mathscr{T}$ 的 upper bound. 而若 $U'\in\mathscr{P}(A)$ 是 $\mathscr{T}$ 的 upper bound, 表示對任意 $B\in\mathscr{T}$, 皆有 $B\subseteq U'$, 故由 Corollary 3.3.4, 知 $U=\bigcup_{B\in\mathscr{T}} B\subseteq U'$. 得證 $U=\bigcup_{B\in\mathscr{T}} B$ 會是 $\mathscr{T}$ 的 least upper bound. 例如 $A=\{1,2,3,4\}$ 的情形, 考慮 $\mathscr{T}=\{\{1,2\},\{1,3\}\}$. 則 $\{1,2\}\cup\{1,3\}=\{1,2,3\}$ 就是 $\mathscr{T}$ 的 least upper bound.

Question 4.10. 給定 *nonempty set* A, 考慮 $(\mathscr{P}(A),\subseteq)$ 這個 *poset.* 對於任意 $\mathscr{P}(A)$ 的 *nonempty subset* $\mathscr{T}$, 試證明 $\mathscr{T}$ 的 *greatest lower bound* 存在.

要注意, 一般來說對於 poset $(X,\preceq)$ 的 nonempty subset T, 雖然其 least upper bound 可能不存在, 不過若存在的話它會是唯一的. 這是因為如果 $u,u'\in X$ 皆為 T 的 least upper bound, 則由 u 為 least upper bound 且 u' 為 upper bound, 得 $u\preceq u'$. 同理可得 $u'\preceq u$, 故由 partial order 的 anti-symmetric 性質得 $u=u'$. 同樣的 T 的 greatest lower bound 若存在的話, 也會是唯一的. 所以我們有以下性質.

Proposition 4.3.8. 假設 $(X,\preceq)$ 是 *partial ordered set* 且 T 是 X 的 *nonempty subset.* 若 T 的 *least upper bound* 存在, 則唯一. 而若 T 的 *greatest lower bound* 存在, 也會是唯一的.

當 T 的 least upper bound 存在時，由於是唯一的，我們就用 $\sup(T)$ 表示之。同理，我們會用 $\inf(T)$ 表示 T 的 greatest lower bound.

當 $(X,\preceq)$ 是 total ordered set 時, least upper bound 和 greatest lower bound 除了唯一性外還有一個重要的性質. 依定義若 $u\in X$ 是 T 的 least upper bound, 表示如果 $x\prec u$, 則 x 不可能是 T 的 upper bound. 這是因為若 x 是 T 的 upper bound 則會得到 $u\preceq x$ 之矛盾 (注意 $\prec$ 是 strict total order, 所以依三一律, $x\prec u$ 和 $u\preceq x$ 不可能同時成立). 我們有以下之結論.

Proposition 4.3.9. 假設 $(X,\preceq)$ 是 *total ordered set,* T 是 X 的 *nonempty subset* 且 $u\in X$ 是 T 的 *least upper bound.* 若 $x\in X$ 滿足 $x\prec u$, 則存在 $t\in T$ 滿足 $x\prec t$.

Proof. 利用反證法, 假設存在 $t\in T$ 滿足 $x\prec t$ 是錯的, 表示所有的 $t\in T$ 都不滿足 $x\prec t$. 然而 $\prec$ 是 X 的 strict total order, 依三一律知, $x\prec t$, $t\prec x$ 和 $x=t$ 必有一項是對的. 因此對所有 $t\in T$ 都不滿足 $x\prec t$ 表示對所有 $t\in T$ 都滿足 $t\preceq x$. 也就是說 x 會是 T 的 upper bound. 但依假設 u 是 T 的 least upper bound, 我們得 $u\preceq x$. 由三一律知此與 $x\prec u$ 之前提相矛盾. 故得證存在 $t\in T$ 滿足 $x\prec t$. □

Question 4.11. 假設 $(X,\preceq)$ 是 *total ordered set,* T 是 X 的 *nonempty subset* 且 $l\in X$ 是 T 的 *greatest lower bound.* 試證明若 $x\in X$ 滿足 $l\prec x$, 則存在 $t\in T$ 滿足 $t\prec x$.

接下來我們介紹 poset $(X,\preceq)$ 中的 nonempty subset T 的最大最小元素. 要注意, 在 poset 中的最大最小元素其實有分兩種. 由於 poset 中未必任兩個元素是 comparable, 所以

一種 T 的最大元素, 稱為 *maximal element* of T, 指的是在 T 中沒有其他元素比它大的元素. 也就是說若 $\mu \in T$ 且不存在 $t \in T$ 滿足 $\mu \prec t$, 則稱 μ 為 T 的 maximal element. 這也等同於說如果 $t \in T$ 滿足 $\mu \preceq t$, 則 $\mu = t$. 另一種最大元素, 稱為 *greatest element* of T (或稱 *maximum element*), 指的是所有 T 中的元素都比它小. 也就是說若 $g \in T$ 且對所有 $t \in T$ 皆滿足 $t \preceq g$, 則稱 g 為 T 的 greatest element. 至於最小元素也有相對的定義. 若 $m \in T$ 且不存在 $t \in T$ 滿足 $t \prec m$, 則稱 m 為 T 的 *minimal element*. 而若 $l \in T$ 且對所有 $t \in T$ 皆滿足 $l \preceq t$, 則稱 l 為 T 的 *least element* (或稱 *minimum element*). 要特別注意的是, T 的 upper bound 和 lower bound 不需要是 T 的元素, 但 T 的 maximal element, greatest element 以及 minimal element, least element 皆要求是 T 的元素. 如同 upper bound 和 lower bound, 上述這幾種最大最小元素, 並不一定會存在. 我們看以下的例子.

Example 4.3.10. (A) 考慮 $(\mathbb{R}, \leq)$ 這個 total ordered set. 令 $T = \{x \in \mathbb{R} : 0 < x < 1\}$. 很容易看出 T 沒有 maximal element. 這是因為對任意 $\mu \in T$ 皆有 $0 < \mu < 1$, 所以若令 $t = (\mu + 1)/2$, 則有 $0 < t < 1$, 亦即 $t \in T$ 且 $\mu < t$. 得證 T 沒有 maximal element. 同理 T 也沒有 minimal element. 另一方面若考慮 $T' = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$. 很容易看出 1 是 T' 的 maximal element 也是 greatest element, 而 0 是 T' 的 minimal element 也是 least element.

(B) 考慮 $A = \{1,2,3\}$ 以及 $(\mathscr{P}(A), \subseteq)$ 這個 poset. 考慮 $\mathscr{T} = \{\{1\}, \{1,2\}, \{2,3\}, \{1,2,3\}\}$. 則 $\{1,2,3\}$ 是 $\mathscr{T}$ 的 maximal element 也是 greatest element. 而 $\{1\}$ 是 $\mathscr{T}$ 的 minimal element 因為找不到 $B \in \mathscr{T}$ 會滿足 $B \subset \{1\}$. 不過 $\{1\}$ 不是 $\mathscr{T}$ 的 least element, 因為 $\{2,3\} \in \mathscr{T}$ 但是 $\{1\}$ 不滿足 $\{1\} \subseteq \{2,3\}$. 另外 $\{2,3\}$ 也是 $\mathscr{T}$ 的 minimal element, 因為我們也找不到 $B \in \mathscr{T}$ 會滿足 $B \subset \{2,3\}$. 另外若考慮 $\mathscr{T}' = \{\{1\}, \{1,2\}, \{2,3\}\}$. 則 $\mathscr{T}'$ 就沒有 greatest element, 而 $\{1,2\}$ 和 $\{2,3\}$ 都是 $\mathscr{T}'$ 的 maximal element. 要注意的是在這情況之下 $\{2,3\}$ 同時是 $\mathscr{T}'$ 的 maximal element 以及 minimal element.

從 Example 4.3.10 我們知道 maximal element 和 minimal element 有可能不唯一. 不過 greatest element 和 least element 若存在的話, 會是唯一的. 事實上我們有以下之結果.

Proposition 4.3.11. 假設 $(X, \preceq)$ 為 *poset*, T 為其 *nonempty subset* 且假設 T 的 *greatest element* 存在. 則 T 的 *greatest element* 為唯一. 又此時 T 的 *maximal element* 會存在且唯一, 事實上 T 的 *maximal element* 就是 T 的 *greatest element*, 也是 T 的 *least upper bound*.

Proof. 首先利用反證法, 證明 greatest element 的唯一性. 假設 $g, g' \in T$ 皆為 T 的 greatest element 且 $g \neq g'$. 由於 $g' \in T$ 且 g 為 T 的 greatest element, 依定義我們有 $g' \preceq g$. 同理知 $g \preceq g'$. 由於 $\preceq$ 為 partial order 具有 anti-symmetric 性質, 由 $g' \preceq g$ 以及 $g \preceq g'$ 得 $g = g'$ 之矛盾. 得證唯一性.

現假設 $g \in T$ 為 T 的 greatest element. 若 $t \in T$ 滿足 $g \preceq t$, 則由 reflexive 性質得 $g = t$. 換言之, 不可能存在 $t \in T$ 滿足 $g \prec t$. 得知 g 為 T 的 maximal element. 證得 T 的 maximal element 是存在的. 現若 $\mu \in T$ 為 T 的 maximal element. 由 $\mu \in T$, 知 $\mu \preceq g$. 然而依 maximal element 的定義以及 $g \in T$ 知不可能有 $\mu \prec g$ 的情形發生, 故得 $\mu = g$. 我們證明

了 T 的 maximal element 一定就是 T 的 greatest element g, 也同時證得了 T 的 maximal element 的唯一性.

依 greatest element 的定義, 對所有 $t \in T$ 皆有 $t \preceq g$, 因此 g 是 T 的 upper bound. 現對任意 T 的 upper bound u, 由於 $g \in T$, 依 upper bound 的定義, 我們有 $g \preceq u$, 得證 g 是 T 的 least upper bound. □

Question 4.12. 假設 $(X, \preceq)$ 為 *poset,* T 為其 *nonempty subset* 且假設 T 的 *least element* 存在. 試證明 T 的 *least element* 為唯一, 且此時 T 的 *minimal element* 會存在且唯一. 並證明 T 的 *minimal element* 就是 T 的 *least element,* 也是 T 的 *greatest lower bound.*

Question 4.13. 假設 $(X, \preceq)$ 為 *poset* 且 T 為其 *nonempty subset.* 試證明 T 的 *least upper bound* u 存在且 $u \in T$ 若且唯若 T 的 *greatest element* 存在. 同樣的, 試證明 T 的 *greatest lower bound* l 存在且 $l \in T$ 若且唯若 T 的 *least element* 存在.

假設 $(X, \preceq)$ 為 poset, T 為其 nonempty subset, 從 Proposition 4.3.11 以及 Question 4.12 我們知道當 T 有 greatest element 時 T 的 maximal element 就是 greatest element, 而當 T 有 least element 時 T 的 minimal element 就是 least element. 其實只有當 $(X, \preceq)$ 是 partial ordered set 不是 total ordered set 時, 因為並不是任兩元素是 comparable 才需區分 maximal element 和 greatest element 以及區分 minimal element 和 least element. 事實上當 $(X, \preceq)$ 是 total ordered set 時 maximal element 和 greatest element 是一致的, 同樣的 minimal element 和 least element 也是一致的.

Proposition 4.3.12. 假設 $(X, \preceq)$ 為 *total ordered set,* T 為其 *nonempty subset.* 若 T 的 *maximal element* 存在, 則 T 的 *maximal element* 就是 T 的 *greatest element.*

Proof. 假設 $\mu \in T$ 為 T 的 maximal element. 由於對任意 $t \in T$, $\mu \prec t$ 皆不成立, 故由三一律知 $t \preceq \mu$. 得證 μ 為 T 的 greatest element. □

Question 4.14. 假設 $(X, \preceq)$ 為 *total ordered set,* T 為其 *nonempty subset.* 試證明若 T 的 *minimal element* 存在, 則 T 的 *minimal element* 就是 T 的 *least element.*

我們利用下表讓大家更清楚這些定義：

名稱	需要在 T	性質	附註
$g =$ greatest element of T	yes	$\forall t \in T,\ t \preceq g$	g 存在則 $g = \mu$
$\mu =$ maximal element of T	yes	$(\lambda \in T) \wedge (\mu \preceq \lambda) \Rightarrow \lambda = \mu$	μ 存在且為 total order 則 $\mu = g$
$u =$ upper bound of T	no	$\forall t \in T,\ t \preceq u$	g 存在則 $g = \sup(T)$
$\ell =$ least element of T	yes	$\forall t \in T,\ \ell \preceq t$	ℓ 存在則 $\ell = m$
$m =$ minimal element of T	yes	$(\lambda \in T) \wedge (\lambda \preceq m) \Rightarrow \lambda = m$	m 存在且為 total order 則 $m = \ell$
$l =$ lower bound of T	no	$\forall t \in T,\ l \preceq t$	ℓ 存在則 $\ell = \inf(T)$

最後我們再定義一個重要的名詞, 就是所謂的 well order, 其定義如下.

Definition 4.3.13. 假設 $(X,\preceq)$ 為 total ordered set. 若對任意 X 的 nonempty subset T 其 least element 皆存在, 則稱 $(X,\preceq)$ 為 *well-ordered set.*

例如對於所有正整數所成的集合, 在一般的大小關係之下就是 well-ordered set. 但所有整數所成的集合, 在一般的大小關係之下就不是 well-ordered set. 因為例如所有的負整數所成的集合就沒有 least element.

在數學上當我們要處理有無窮多元素的集合時, 我們常會用所謂的 *Well-ordering Theorem* 來處理. 這個定理是說對每一個 nonempty set X, 我們都可以找到一個 total order $\preceq$ 使得 $(X,\preceq)$ 為 well-ordered set.

Example 4.3.14. 對於所有整數所成的集合 $\mathbb{Z}$, 雖然在一般的大小關係之下不是 well-ordered set. 我們可以找到一個 total order $\preceq$ 使得 $(\mathbb{Z},\preceq)$ 為 well-ordered set. 考慮以下的 relation: 當 $a,b\in\mathbb{Z}$, 定義 $a\preceq b$ 若且唯若 (1) $|a|<|b|$ 或 (2) $|a|=|b|$ 且 $a\leq b$. 在此定義之下 $(\mathbb{Z},\preceq)$ 為 total ordered set. 因為若 $a\preceq b$ 且 $b\preceq a$, 表示 $|a|=|b|$ (因 $|a|<|b|$ 和 $|b|<|a|$ 不可能同時成立) 以及 $a\leq b$ 且 $b\leq a$, 得證 $a=b$, 即 $\preceq$ 具有 anti-symmetric 性質. 又若 $a\preceq b$ 且 $b\preceq c$, 表示 $|a|\leq|b|$ 且 $|b|\leq|c|$, 故得 $|a|\leq|c|$. 現若 $|a|<|c|$ 可得 $a\preceq c$. 而若 $|a|=|c|$, 我們當然有 $|a|=|b|$, 故由 $a\preceq b$ 之假設得 $a\leq b$. 又因 $|b|=|c|$, 故由 $b\preceq c$ 之假設得 $b\leq c$. 依此得證當 $|a|=|c|$ 時可得 $a\leq c$, 也就是說 $a\preceq c$. 證得了 $\preceq$ 具有 transitive 性質. 至於 total 性質, 任意 $a,b\in\mathbb{Z}$ 我們可以比較 $|a|,|b|$ 的大小, 而若 $|a|=|b|$, 我們都可比較 a,b 的大小, 所以任意 $a,b\in\mathbb{Z}$ 皆為 comparable, 故 $\preceq$ 具有 total 性質. 事實上依此定義, 我們所得的整數排序方法為

$$0\prec -1\prec 1\prec -2\prec 2\cdots.$$

我們要說明 $(\mathbb{Z},\preceq)$ 此 total ordered set 為 well-ordered set. 對於任意 $\mathbb{Z}$ 的 nonempty subset T, 我們先選取 T 中絕對值最小的元素. 若絕對值最小的元素僅有一個, 則依 $\preceq$ 的定義此為 T 的 least element. 而若絕對值最小的元素有兩個, 則取原本為負的那一個便是 T 的 least element. 即在 $\preceq$ 這個 order 之下, T 有 least element. 得證 $(\mathbb{Z},\preceq)$ 為 well-ordered set.

Question 4.15. 考慮 $\mathbb{Z}$ 中以下的 *relation:* 對於任意 $a,b\in\mathbb{Z}$ 定義 $a\preceq b$ 若且唯若 *(1)* $ab\geq 0$ 且 $|a|\leq|b|$ 或 *(2)* $ab<0$ 且 $a\leq b$. 也就是說依此定義所得的整數排序方法為

$$0\prec -1\prec -2\prec -3\cdots\prec 1\prec 2\prec 3\cdots.$$

試證明在此定義之下 $(\mathbb{Z},\preceq)$ 為 *total ordered set.* 是否此時 $(\mathbb{Z},\preceq)$ 為 *well-ordered set?*

Well-ordering Theorem 和所謂 *Zorn's Lemma* 以及 *Axiom of Choice* 是等價的, 等以後我們介紹完 function 的概念後會詳細討論.

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 $x\overset{f}{\longmapsto}f(x)\overset{g}{\longmapsto}g(f(x))$. 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 $b\notin A$ 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 $f(x)\notin D$. 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 $f(x)\notin D$ 相矛盾, 故知 $x\notin f^{-1}(D)$. 由 $x\in f^{-1}(C)$ 且 $x\notin f^{-1}(D)$, 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 $x\notin f^{-1}(D)$. 得知 $f(x)\in C$. 現若又 $f(x)\in D$, 表示 $x\in f^{-1}(D)$, 此與前面 $x\notin f^{-1}(D)$ 相矛盾, 故知 $f(x)\notin D$. 由 $f(x)\in C$ 且 $f(x)\notin D$, 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 $\{1,\dots,n\}$ 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 $I_1=\{1\}$, $I_2=\{1,2\}$,..., $I_n=\{1,\dots,n\}$. 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

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

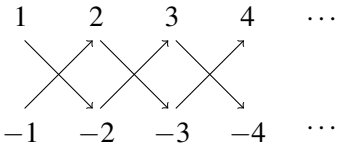
現考慮 restriction map $f|_{A_o}:A_o\to B$, 也就是對任意 $a\in A_o$, $f|_{A_o}(a)=f(a)$. 由於 f 為 one-to-one, 很自然的 $f|_{A_o}$ 仍為 one-to-one. 我們要說明 $f|_{A_o}$ 的 range $f|_{A_o}(A_o)$ 為 B_e. 對任意 $a\in A_o$, 我們有 $f|_{A_o}(a)=f(a)\in B$. 此時考慮 $f(a)$ 所建構的 sequence, 首項為 $y_1=f(a)$, 而因 $f^{-1}(\{f(a)\})=\{a\}$ (因 $f(a)\in\{f(a)\}$), 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 $|A|=|B|$. □

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 $A = \{1, 2, \dots\}$ 為正整數所成的集合, $B = \{-1, -2, \dots\}$ 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 $b \le -2$) 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 $a \ge 2$) 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 $|A| \le |B|$ 且 $|A| \ne |B|$ 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 $t_1\le t,\forall t\in T$ 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 $k=1,\dots,n$ 皆有唯一的 $t_k\in T$ 使得 $f(k)=t_k$. 現考慮 $f(n+1)$, 依定義 $T_{n+1}=T\setminus\{f(1),\dots,f(n)\}=T\setminus\{t_1,\dots,t_n\}$ 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 $T\subseteq\{t_1,\dots,t_n\}$ 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 $t_1,\dots,t_n$ 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 $T_{n_2}=T\setminus\{f(1),\dots,f(n_1),\dots,f(n_2-1)\}$, 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. □

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 $|S|\le|\mathbb{N}|$, 也因此若 $S'\subseteq S$, 則由 $|S'|\le|S|$ 以及 $|S|\le|\mathbb{N}|$, 可得 $|S'|\le|\mathbb{N}|$. 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 $S_1,\dots,S_n$ 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 $q \in \mathbb{Q}$, $q \neq 0$ 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 $0.10110\overline{1}$ 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.

Chapter 6

Axiom of Choice, Well-ordering Theorem and Zorn's Lemma

Axiom of choice 對於大部分數學家都認為直覺是對的, 不過卻可以用它推導出一些令人覺得深奧較不合乎直覺的定理或性質, 例如 Well-ordering Theorem 和 Zorn's Lemma (事實上這三個性質是等價的). 對於 axiom of choice 的使用, 有些數學家並不一定那麼釋懷，不過由於過去一些數學的證明常不自知的用到 axiom of choice, 而且這個 axiom 的使用並沒有和數學的理論造成任何的矛盾, 所以目前絕大部分的數學家是接受 axiom of choice 以及與其等價的 Well-ordering Theorem 和 Zorn's Lemma. 也因此將來大家在學習進階的一些數學課程時會遇到需要用這三個性質其中之一所得到的定理, 所以我們特別介紹這三個性質. 要注意, 我們並不是要證明這三個性質是等價的 (有興趣的同學可參考集合論相關的書籍), 而是著重於瞭解這三個性質以及如何運用.

6.1. Axiom of Choice

Axiom of choice 指的是對於任意的非空集合 S, 我們都可以定義一個 "方法" 在 S 的任意非空子集中挑出一個代表元素. 這個性質在 S 是 finite set 時不會有問題, 因為此時 S 的非空子集只有有限多個, 我們可以用列舉的方法告訴大家如何挑選每個非空子集的代表元素. 另外對於一些特別的 infinite set, 也可能沒問題. 例如當 S 為 $\mathbb{N}$ 時, 我們可以對於 $\mathbb{N}$ 的每個非空子集利用 well-ordering principle, 使用選 least element 的方法挑出代表元素. 不過對於更一般的 infinite set, 就可能會有問題了, 因為我們可能無法明確地造出 "挑選" 的方法. 不過換一個角度來說, 既然是非空子集, 我們可以任意挑選一個元素當代表元素啊! 所以雖然無法像 finite set 的情況用列舉法, 不過至少應該還是一種 "挑選" 的方法. 因此一般的數學家認為這個性質只是對於 finite set 的情形延伸而來, 頗符合直覺, 也應此公認它是對的.

要注意, 前述在非空子集中任意挑選一個元素當代表元素的說法其實是有限制的. 既然要挑代表元素, 便要有一致性. 也就是說對於同一個非空子集, 不能一下子挑一個元素, 一下

子又挑另一個元素. 這種一致性利用 function 來表達便最合適了. 回顧一下集合 S 的子集合所成的集合, 即所謂 S 的 power set, 我們用 $\mathscr{P}(S)$ 來表示. 我們想將 $\mathscr{P}(S)$ 中任一個非空子集 A 對應到 A 的某一個元素, 所以用函數的觀點來看就是找到一個 function f 使得對任意 S 的非空子集 A 皆有 $f(A)\in A$. 這一個 function f, 由於是挑選 S 中每一個非空子集的代表元素, 所以一般我們也稱之為 *choice function*. 接下來, 我們寫下 axiom of choice 的正確敘述.

Axiom of Choice: *For any nonempty set S, there exists a choice function $f:\mathscr{P}(S)\setminus\emptyset\to S$ such that for every nonempty subset A of S* (即 $A\in\mathscr{P}(S)\setminus\emptyset$), *we have $f(A)\in A$.*

要注意, 這裡 A 雖然是一個集合, 但 choice function 對其作用後所得的是 A 中的一個元素, 而不是集合. 也就是說 choice function f 的定義域是 S 的非空子集合, 而不是 S, 千萬不要誤以為 $f(A)$ 是前一章 Section 5.2 所提的 "image of A under f". 另外要說明的是 axiom of choice 中僅談到 choice function 的存在性, 並未論及如何找到此 choice function. 所以一般利用 axiom of choice 所得的結果, 它的存在性都不會是 constructive.

前面提及, 我們常不經意地用到 axiom of choice. 例如在 Proposition 5.5.9 的證明中, 我們事實上用到了 axiom of choice. 也就是在 $S_1,\dots,S_n,\dots$ 皆為 countable set 的假設上, 對於每一個 $i\in\mathbb{N}$, 由於 $|S_i|\le|\mathbb{N}|$, 我們就在可能很多 $S_i\to\mathbb{N}$ 的 one-to-one function 中挑選了一個 $f_i:S_i\to\mathbb{N}$, 為代表. 所以嚴格來說 Proposition 5.5.9 是要用到 axiom of choice 才能成立的. 最後, 我們再看一個利用 axiom of choice 所得的結果.

Proposition 6.1.1. 假設 S 為 *infinite set,* 則 S 中存在 *subset* 是 *countably infinite.*

Proof. 假設 $f:\mathscr{P}(S)\setminus\emptyset\to S$ 為 choice function. 考慮 $g:\mathbb{N}\to S$, 定義為 $g(1)=f(S)$. 令 $S_2=S\setminus\{f(S)\}$, 由於 S 為 infinite set, 我們有 $S_2\neq\emptyset$, 也就是說 $S_2\in\mathscr{P}(S)\setminus\emptyset$, 所以 $f(S_2)$ 是有定義的, 現令 $g(2)=f(S_2)$. 現利用數學歸納法對於 $k\ge2$ 令 $S_{k+1}=S\setminus\{f(S),f(S_2),\dots,f(S_k)\}$. 由 S 為 infinite set, 我們知 $S_{k+1}\in\mathscr{P}(S)\setminus\emptyset$, 故定義 $g(k+1)=f(S_{k+1})$. 依此, 我們定義了一個 $g:\mathbb{N}\to S$ 這樣的一個 one-to-one function, 也因此 g 的 image, 即 $g(\mathbb{N})$ 就是 S 的一個 countably infinite 的 subset. □

一般來說，在處理有無窮多個集合的問題時，就有可能用到 axiom of choice, 但也未必一定要用到。英國哲學家 Russell（也是數學家和邏輯學家）提出了一個簡單區分是否要用到 axiom of choice 的例子。當在無窮多雙的襪子中（一般來說每雙襪子都是同色且不分左右腳），若要從每雙襪子中都挑出一隻襪子，便需用到 axiom of choice；但在無窮多雙的鞋子中（一般來說每雙鞋子都有分左右腳），若要從每雙鞋子中都挑出一隻鞋子，便不需用到 axiom of choice，因為我們可以簡單的都挑左鞋。簡單來說，是否用到 axiom of choice 取決於函數是否為 constructive。

6.2. Well-ordering Theorem

回顧一個 partial ordered set $(X,\preceq)$, 為 total ordered 表示 X 中任意兩個元素都可以比較大小, 亦即若 $a,b\in X$, 則 $a\preceq b$ 或 $b\preceq a$, 其中之一必成立. 而一個 poset (partial ordered set)

$(X,\preceq)$, 稱為 well-ordered 表示每一個 X 的非空子集 T 都會有 least element, 也就是說存在 $t_0 \in T$ 滿足 $t_0 \preceq t$, $\forall t \in T$. 為了方便起見我們用 $\min(T)$ 表示 T 的 least element. 所謂 Well-ordering Theorem, 就是說對於一個非空的集合 X, 我們都可以找到一個 order $\preceq$, 使得 $(X,\preceq)$ 是一個 well-ordered set.

不要將 Well-ordering Theorem 和 Well-ordering Principle 混淆. Well-ordering Principle, 簡單來說指的是用我們一般的 order $\leq$ 會使得 $(\mathbb{N},\leq)$ 是 well-ordered set. 而 Well-ordering Theorem, 指的是任意的非空集合 X, 另外它並無指出哪一種 order $\preceq$ 會使得 $(X,\preceq)$ 是一個 well-ordered set. 例如有理數 $\mathbb{Q}$ 利用一般的 $\leq$, 並不會是 well-ordered (我們無法在 $\{r \in \mathbb{Q} \mid 0 < r < 1\}$ 這個集合中找到最小的有理數). 不過利用 $\mathbb{Q}$ 是 countable (Corollary 5.5.8), 我們可以利用 $\mathbb{N}$ 和 $\mathbb{Q}$ 的一對一的對應, 將 $\mathbb{Q}$ 從新排序, 而利用此新的排序得到 $\mathbb{Q}$ 為 well-ordered. 所以說 Well-ordering Theorem, 對於 countable set, 我們知道可由 $\mathbb{N}$ 的 Well-ordering Principle 推得. 不過對於 uncountable set, Well-ordering Theorem 就較難令人理解. 事實上到目前為止, 我們仍無法具體舉出實數 $\mathbb{R}$ 上的 order $\preceq$ 使得 $(\mathbb{R},\preceq)$ 是 well-ordered.

Well-ordering Theorem 又稱為 Zermelo's Theorem, 它是 Zermelo 利用 Axiom of Choice 證出的. 我們可以很快地利用 Well-ordering Theorem 證出 Axiom of Choice. 所以邏輯上, 它們是等價的. 因此我們也可以將 Well-ordering Theorem 視為是一種 axiom (公設). 不過如前所說, 一般人直覺上較能覺得 Axiom of Choice 是對的, 而直覺上較無法理解 Well-ordering Theorem, 所以一般我們不稱它為公設, 覺得它是由 Axiom of Choice 所推出的定理. 我們正式寫下其定理形式.

Theorem 6.2.1 (Well-ordering Theorem)**.** *Let X be a nonempty set. Then there exists an order relation $\preceq$ on X such that $(X,\preceq)$ is well-ordered.*

Well-ordered Theorem 強調的是可以找到 order $\preceq$, 使得 $(X,\preceq)$ 為 well-ordered. 不過由於這個存在性是利用 Axiom of Choice 所得到, 前面強調過用 Axiom of Choice 所得的存在性不是 constructive, 所以 Well-ordered Theorem 並無法提出使得 $(X,\preceq)$ 為 well-ordered set 的 order $\preceq$ 為何.

在這裡我們不去探討如何由 Axiom of Choice 得到 Well-ordering Theorem. 不過反向是容易的, 即利用 Well-ordering Theorem 推得 Axiom of Choice. 對於任意的 nonempty set S, 利用 Well-ordering Theorem, 考慮 order $\preceq$ 使得 $(S,\preceq)$ 為 well-ordered. 此時對任意 $A \in \mathscr{P}(S) \setminus \emptyset$, 令 $f(A) = \min(A)$. 則 $f : \mathscr{P}(S) \setminus \emptyset \to S$, 滿足 choice function 的要求, 即 $f(A) \in A$. 故推得 Axiom of Choice.

有了 Well-ordering Theorem 這個強大的工具, 就如同 $\mathbb{N}$ 有 Well-ordering principle 一樣, 我們可以有類似 mathematical induction 的方法稱之為 *transfinite induction*. 回顧一下 Corollary 2.3.6, 要使用 mathematical induction 證明 $P(n)$ 對所有 $n \in \mathbb{N}$ 皆成立, 我們先證明 (i) $P(1)$ 是對的; 然後再證明 (ii) 若對任意 $i < k$, $P(i)$ 皆成立, 則 $P(k)$ 亦成立. 證明了 (i), (ii) 便證得 $P(n)$ 對所有 $n \in \mathbb{N}$ 皆成立. 而 transfinite induction 是利用 $(X,\preceq)$ 為

well-ordered, 先證明 (1) $P(\min(X))$ 成立; 再證明 (ii) 若對任意 $\alpha \prec \beta$, $P(\alpha)$ 皆成立, 則 $P(\beta)$ 亦成立. 如此便證得了 $P(x)$, 對所有 $x \in X$ 皆成立. 我們將此定理敘述如下:

Theorem 6.2.2 (Transfinite Induction)**.** 假設 $(X, \preceq)$ 為 *well-ordered set* 且令 $x_1 = \min(X)$. 假設以下兩個 *statement* 是對的, 那麼對任意 $x \in X$, $P(x)$ 皆會成立.

(1) $P(x_1)$ 成立.

(2) 假設 $\beta \in X$. 若對任意 $\alpha \in X$ 滿足 $\alpha \prec \beta$, $P(\alpha)$ 皆成立, 則 $P(\beta)$ 成立.

Proof. 利用反證法, 假設存在 $x \in X$ 使得 $P(x)$ 不成立. 考慮 $S = \{x \in X \mid P(x) \text{ 不成立 }\}$. 依假設 $S \neq \emptyset$. 故由 $(X, \preceq)$ 為 well-ordered, 知存在 $\beta \in S$ 使得 $\beta = \min(S)$. 由 (1) 知 $\beta \neq x_0$. 又因 $\beta = \min(S)$, 我們知對任意 $\alpha \in X$ 滿足 $\alpha \prec \beta$, 皆有 $\alpha \notin S$, 亦即 $P(\alpha)$ 皆成立. 故由 (2) 知 $P(\beta)$ 成立. 此與 $\beta \in S$ 之假設相矛盾, 故知 $S = \emptyset$, 亦即對任意 $x \in X$, $P(x)$ 皆成立. □

Well-ordering Theorem 的好處就是可以讓我們如同處理 $\mathbb{N}$ 一樣地處理一般的集合. 不過這反而會造成同學的誤解. 許多同學會誤以為一個集合是 well-ordered, 表示可以由最小的元素開始排序. 若將最小的元素對應到 1, 第二小的元素對應到 2, 這樣一直下去不就表示所有 infinite set 都可以和 $\mathbb{N}$ 形成一對一對應, 而造成所有的集合都是 countable 這樣的奇怪現象? 這樣的看法其實是錯的, 主要的原因是我們確實可以利用 well-order 的性質將集合中的元素從小排到大, 但這並不代表可以將每一個元素都排到. 例如對於 $\mathbb{N}$ 我們可以有以下的 order $\preceq$: 若 $a, b \in \mathbb{N}$ 且同奇同偶, 則定 $a \preceq b$ 若且唯若 $a \leq b$; 而若 a 為奇數 b 為偶數, 則定 $a \preceq b$. 在此定義之下我們仍可得 $(\mathbb{N}, \preceq)$ 為 well-ordered set, 但是若從小到大排序, 則 2 (或任何的偶數) 永遠都無法被排到 (因為必須將奇數先排完才能排偶數).

6.3. Zorn's Lemma

Zorn's Lemma 和 Axiom of Choice 也是等價的. 由於它的前題對一般的 partial ordered set 都可使用, 所以較易拿來應用. 也因此有許多數學上的定理是用它推得的, 故一般稱之為 Lemma. 事實上, 以後大家在遇到符合 Zorn's Lemma 的前題時, 可以如使用 Axiom 一樣直接套用. 所以我們不去論證 Zorn's Lemma 和 Axiom of Choice (或 Well-ordering Theorem) 之間的等價關係, 而專注於了解這個 Lemma.

首先我們在回顧一些有關於 order 的定義. 在一個 partial ordered set $(S, \preceq)$ 中, 假設 T 是 S 的 subset 且 T 在 $\preceq$ 之下 $(T, \preceq)$ 是一個 total ordered set (意即對任意 $t, t' \in T$ 皆有 $t \preceq t'$ 或 $t' \preceq T$), 我們稱 T 為 $(S, \preceq)$ 的一個 *chain*. 對於 S 的一個 nonempty subset S', 我們說 $u \in S$ 是 S' 的一個 upper bound, 表示對任意 $s' \in S'$ 皆有 $s' \preceq u$. 而我們說 $\mu \in S$ 是 S 的 maximal element, 表示 $\mu \in S$ 且 S 中沒有任何元素 s 會滿足 $\mu \preceq s$ (也就是說 S 中的元素 s, 要不是滿足 $s \preceq \mu$ 就是和 μ 不能比較大小). 現在我們可以敘述 Zorn's Lemma.

Lemma 6.3.1 (Zorn's Lemma)**.** 假設 $(S, \preceq)$ 是一個 *partial ordered set.* 若 S 中每一個 *chain* 皆在 S 中有 *upper bound,* 則 S 有 *maximal element.*

從 Zorn's Lemma 的敘述可知, 當我們要證明一個特定的 partial ordered set 有 maximal element, 可以考慮使用 Zorn's Lemma. 也就是說, 若要證明一個 poset $(S, \preceq)$ 有 maximal element, 我們可以考慮 S 中任意的一組 chain, 然後試著在 S 中找到此組 chain 的 upper bound. 如果能證明所有的 chain 皆在 S 中可找到 upper bound, 那麼 poset $(S, \preceq)$ 會有 maximal element. 要注意, 這裡我們特別強調, 每一個 chain 的 upper bound 必須在 S 中找到, 否則不能確保 S 有 maximal element.

可以看出 Zorn's Lemma 仍然是談論存在性的問題. 由於它和 Axiom of Choice 以及 Well-ordering Theorem 是等價的, 所以它所得的存在性也不是 constructive. 也就是說, 我們可證得 maximal element 的存在性, 但無從得知這些 maximal element 有哪些. Zorn's Lemma 會在將來許多數學課程中用到. 例如代數中, 要證明每個 ring 皆存在著 maximal ideal; 線性代數中, 要證明所有的 (infinite dimensional) vector space 皆存在一組 basis, 都要用到 Zorn's Lemma. 這裡我們特別舉出一個常常使用 Zorn's Lemma 的情況, 事實上前面所舉的這兩種例子就是在這種情況之下得證的.

Proposition 6.3.2. 假設 $\mathscr{S}$ 是由一些具有某特定性質的 *sets* 所成的集合. 考慮一般集合的包含關係 $\subseteq$ 所形成的 *partial ordered set* $(\mathscr{S}, \subseteq)$. 若 $\mathscr{S}$ 中任意的一組 *chain* 的聯集仍在 $\mathscr{S}$ 中, 則在 $\mathscr{S}$ 中必存在一集合 M 使得 $\mathscr{S}$ 中任一集合 S 皆不會滿足 $M \subset S$.

Proof. 注意 $\mathscr{S}$ 這一個集合裡的元素仍為集合. 很明顯的 $\mathscr{S}$ 中任一組 chain 的聯集必包含此 chain 中任一集合, 故由 $\mathscr{S}$ 中任意的一組 chain 的聯集仍在 $\mathscr{S}$ 中之假設知此聯集便是此 chain 的一個 upper bound. 因此由 Zorn's Lemma 知 $(\mathscr{S}, \subseteq)$ 有 maximal element M, 亦即 M 是 $\mathscr{S}$ 中的一個集合, 而且 $\mathscr{S}$ 中沒有其他的集合會比 M "大" (也就是說沒有其他的集合會包含 M), 故得證本定理. □

這裡我們要特別說明的是, 任意的一組集合的聯集當然包含其中任一集合, 所以或許同學會疑問為何 Proposition 6.3.2 中要假設任意的一組 chain 的聯集仍在 $\mathscr{S}$ 中? 這就是我們前面強調的要利用 Zorn's Lemma 的重點在於每一個 chain 的 upper bound 要在 $\mathscr{S}$ 中. 所以光取聯集雖可符合 upper bound 的要求, 但可能不符合在 $\mathscr{S}$ 中的要求. 因此一般使用 Proposition 6.3.2 的重點在於如何利用 "chain" 的特性, 證明將它們取聯集後仍會在 $\mathscr{S}$ 中. 這一點將來遇到用 Zorn's Lemma 證明問題時, 務必留意.