1

實數系的建構與性質

微積分創始於十七世紀後半期, 由英國物理學家、數學家牛頓 (I. Newton, 1643–1727) 與德國哲學家、數學家萊布尼茨 (G. W. Leibniz, 1646–1716) 各自建立了微積分的計算系統, 將很多自然界的現象包括物理、天文等利用數學的語言描述及推演並得以清楚地認識。

雖然微積分在那時彰顯出強大威力並解決各式物理與天文上的問題, 但是數學的邏輯論述上卻存在著很多有待澄清的地方。特別是「無窮 — 無窮大或無窮小」這個概念總是以一種似懂非懂的方式闡述, 這引起了人們長達一個多世紀的爭論。直到十九世紀初, 柯西 (A. L. Cauchy, 1789–1857) 才以極限理論替微積分奠定了基礎, 又過了半個世紀後, 康托 (Georg Cantor, 1845–1918) 與戴德金 (R. Dedekind, 1831–1916) 等人發現到: 極限理論實際上依賴於更根本的問題, 也就是對實數的完備性要有更深刻的認識。

實數的完備性到底是什麼呢? 我們必須先從數系的建構開始討論起, 然而關於正整數集合 $\mathbb{N}$ (natural numbers) 與整數集合 $\mathbb{Z}$ (integers) 的意義及性質, 這裡預設各位在一年級的數學導論課程與數論的課程中學到相關的理論, 故在此不多做解釋。倘若你完全沒有修過這兩門課, 或是你覺得你修了這兩門課但是沒有學好, 我認爲這不至於對高等微積分的學習有直接的衝擊, 不妨就還是以國小、國中、高中對於自然數與整數的認知繼續往下學習即可。於是以下小節將從有理數的系統開始談起, 然後建立實數的系統, 從中比較兩系統之間的差異, 最後點出實數的完備性這個概念。而實數的完備性除了這一章會詳細說明外, 還會在第 3 章利用其它方式進一步介紹。

1.1 有理數的基本性質

考慮 *有理數* (rational numbers) 所成的集合:

$$\mathbb{Q} = \left\{ \frac{p}{q} \,\middle|\, p \in \mathbb{Z}, q \in \mathbb{N}, (p,q) = 1 \right\},$$

其中最後一個條件 $(p,q) = 1$ 表示 p 與 q *互質* (coprime), 也就是說: p 與 q 的 *最大公因數* (greatest common divisor) 是 1。以下將列出有理數集的基本性質:

(F) 在有理數集 $\mathbb{Q}$ 上可定義加法運算 $+$ 與乘法運算 $\cdot$ 使得對任意 $a, b \in \mathbb{Q}$ 都有 $a + b \in \mathbb{Q}$ 以及 $a \cdot b \in \mathbb{Q}$, 並且有以下的運算規則:

(F$_{+\mathrm{C}}$) *加法交換律* (commutative law): 對所有 $a, b \in \mathbb{Q}$, $a + b = b + a$。

(F$_{+\mathrm{A}}$) *加法結合律* (associative law): 對所有 $a, b, c \in \mathbb{Q}$, $(a + b) + c = a + (b + c)$。

(F$_{+\mathrm{Id}}$) *加法單位元素* (additive identity): 存在元素 $0 \in \mathbb{Q}$ 使得對所有 $a \in \mathbb{Q}$, $a + 0 = 0 + a = a$。

(F$_{+\mathrm{Iv}}$) *加法反元素* (additive inverse): 每個元素 $a \in \mathbb{Q}$ 都存在另一元素 $-a \in \mathbb{Q}$ 使得 $a + (-a) = (-a) + a = 0$。

(F$_{\cdot\mathrm{C}}$) *乘法交換律* (commutative law): 對所有 $a, b \in \mathbb{Q}$, $a \cdot b = b \cdot a$。

(F$_{\cdot\mathrm{A}}$) *乘法結合律* (associative law): 對所有 $a, b, c \in \mathbb{Q}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$。

(F$_{\cdot\mathrm{Id}}$) *乘法單位元素* (multiplicative identity): 存在元素 $1 \in \mathbb{Q}$ 使得對所有 $a \in \mathbb{Q}$, $a \cdot 1 = 1 \cdot a = a$。

(F$_{\cdot\mathrm{Iv}}$) *乘法反元素* (multiplicative inverse): 每個元素 $a \in \mathbb{Q}, a \neq 0$ 都存在另一元素 $a^{-1} \in \mathbb{Q}$ 使得 $a \cdot a^{-1} = a^{-1} \cdot a = 1$。

(F$_{\cdot+\mathrm{D}}$) *乘法對加法的分配律* (distributive law): 對所有 $a, b, c \in \mathbb{Q}$, $a \cdot (b + c) = a \cdot b + a \cdot c$。

(O) 在有理數集 $\mathbb{Q}$ 上可定義 *全序關係* $<$ (total order relation), 並且有以下規則:

(O1) *三一律* (trichotomy law): 對任意 $a, b \in \mathbb{Q}$, 則 $a < b, a = b, b < a$ 三者之一必成立。

(O2) *遞移律* (transitivity): 對於 $a, b, c \in \mathbb{Q}$, 若 $a < b$ 且 $b < c$, 則 $a < c$。

(O3) *加法的保序性* (compatibility of $<$ and $+$): 若 $a, b \in \mathbb{Q}$ 且 $a < b$, 則對任何 $c \in \mathbb{Q}$ 都有 $a + c < b + c$。

(O4) *乘法對正有理數的保序性* (compatibility of $<$ and $\cdot$): 若 $a, b \in \mathbb{Q}, 0 < a$ 且 $0 < b$, 則 $0 < a \cdot b$。

關於全序關係, 我們有時候會用 $>$ 符號, 也就是說 $a < b$ 與 $b > a$ 同義。此外, 再與等號搭配, 會用 $a \leq b$ 或 $b \geq a$ 表示。

根據課程的屬性, 以上所列舉的條文, 在高等微積分 (advanced calculus) 或數學分析 (mathematical analysis) 課程中以自然地方式感受並順勢地使用即可; 但是在代數學 (algebra) 的課程中, 因爲那門課強調的是集合、運算、關係之間的結構性, 所以在代數課中就必須花時間逐一理解甚至比較並且記憶它。在此簡短地補充代數學的術語: 滿足 **(F)** 的所有性質之集合稱爲 *體* 或 *域* (field); 若一個集合滿足 (O1) 與 (O2) 這兩個條件的話, 則稱集合是一個 *有序集* (totally-ordered set); 若一個體又滿足 **(O)** 的所有條件, 則稱之爲 *有序體* (totally-ordered field)。

以下將介紹有理數集 $\mathbb{Q}$ 的性質:

定理 1 (有理數的稠密性, dense property)**.** 任兩個不相等的有理數之間必存在第三個有理數。

證明: 若 $x, y \in \mathbb{Q}, x < y$, 則 $\frac{x+y}{2} \in \mathbb{Q}$, 並且 $x = \frac{x+x}{2} < \frac{x+y}{2} < \frac{y+y}{2} = y$。 □

1.2　戴德金切割

在正式進入這個主題前, 先想一想你對實數集 $\mathbb{R}$ 的了解有多少? 沒一會兒你就會發現你似乎說不清楚這個集合的意思, 它不像自然數集 $\mathbb{N}$ 就是 $\{1,2,3,\ldots\}$、整數集 $\mathbb{Z}$ 就是由自然數集與 0 還有自然數取負號全部收集而成的集合、有理數集 $\mathbb{Q}$ 就是彼此互質的整數與自然數相除所成的集合那樣, 它們都有很明確的表達式告知該集合內的元素組成之方式。或許你還可以再擠出一點點對於實數集的認識, 像是 $\sqrt{2}$ 還有 π 是實數但不是有理數, 也可能想到循環小數與不循環小數可能會和實數集的討論有一些關聯, 或是你依稀記得中學老師曾經告訴你實數集就把它想像成是一條數線, 數線上的每個點就代表一個數, 好像這樣的說詞就可以把你說服並不再追問了。

這裡不妨岔個題, 跟你說一個數學老師們最經典的騙術: 推卸責任法。回想一下你學習數學的經驗就會發現到, 小學數學老師會跟你說:「某某觀念現在對你來說太難了, 等到你讀國中的時候, 數學老師就會把這件事跟你講清楚。」然而上了國中, 國中數學老師就會說:「某某觀念各位在小學的時候就學過了, 這裡不再多述。」這個現象也必然發生在其它求學階段 (甚至像這份講義的一開始一樣, 把自然數與有理數的討論推卸給數導或數論老師), 這就是導致你對實數集一知半解的原因。而這件事你也不需要有什麼過多的怨言, 台灣的數學教育本來就會讓數學老師的騙術一再上演而且成功, 短時間內無法扭轉。

回到正題, 前一節我們只是對有理數集 $\mathbb{Q}$ 有了初步認識, 有理數集 $\mathbb{Q}$ 不僅僅是那些可表示成 $\frac{p}{q}, p\in\mathbb{Z}, q\in\mathbb{N}, (p,q)=1$ 的數字所成的集合而已, 實際上有理數集還賦予加法 $+$、乘法 $\cdot$ 以及全序 $<$ 的結構, 接下來我們要繼續對有理數集進一步地討論以建立實數集。

在歷史上, 有很多種理論都可以建立實數, 一些教科書中將會看到作者用十進位小數的方法鋪陳實數集, 而這份講義則是採用 *戴德金切割法* (Dedekind cut method) 建構實數, 這個方法的特色是利用集合與邏輯的語言論述, 寫法單純且清楚, 所以最爲人推崇。

定義 **1** (有理數集的切割)**.** 有理數集 $\mathbb{Q}$ 的一個 *切割* (cut) 指的是 $\mathbb{Q}$ 的一個子集合 Q 滿足以下三個條件:

(a) 集合 Q 非空, 而且 $Q\neq\mathbb{Q}$。

(b) 若 $r\in Q, r'\in\mathbb{Q}$ 而且 $r'<r$, 則 $r'\in Q$。

(c) 若 $r\in Q$, 則存在 $r''\in Q$ 使得 $r<r''$。

我們先用以下兩個例子說明有理數集 $\mathbb{Q}$ 的切割可能之情況:

例 **2.** 定義 $Q=\{r\in\mathbb{Q}|r<1\}$, 則 Q 是有理數集 $\mathbb{Q}$ 的一個切割。

證明:

(a) 因爲 $0\in\mathbb{Q}, 0<1$, 因此 Q 非空。因爲 $2\in\mathbb{Q}, 2>1$, 所以 $2\notin Q$, 因此 $Q\neq\mathbb{Q}$。

(b) 若 $r\in Q$, 即 $r\in\mathbb{Q}, r<1$。若有 $r'\in\mathbb{Q}$ 而且 $r'<r$, 則 $r'<r<1$, 所以 $r'\in Q$。

(c) 若 $r\in Q$, 取 $r''=\frac{r+1}{2}\in\mathbb{Q}$, 則 $r=\frac{r+r}{2}<r''=\frac{r+1}{2}<\frac{1+1}{2}=1$ 得知 $r''\in Q$。

由上述討論得知 $Q=\{r\in\mathbb{Q}|r<1\}$ 是有理數集 $\mathbb{Q}$ 的一個切割。 □

例 **3.** 定義 $Q=\{r\in\mathbb{Q}|r\le 0\}\cup\{r\in\mathbb{Q}|r>0,r^2<2\}$, 則 Q 是有理數集 $\mathbb{Q}$ 的一個切割。

證明:

(a) 取 $1\in Q$ 所以 Q 非空; 因爲 $2\in\mathbb{Q}, 2\notin Q$, 所以 $Q\neq\mathbb{Q}$。

(b) 若 $r\in Q, r'\in\mathbb{Q}$ 且 $r'<r$, 如果 $r'\le 0$, 則 $r'\in Q$; 如果 $r'>0$, 則 $(r')^2<r^2<2$ 得到 $r'\in Q$。

(c) 對任意 $r\in Q$, 若 $r\le 0$, 取 $r''=1$ 即爲所求; 若 $r>0$, 考慮 $r''=r-\frac{r^2-2}{r+2}=\frac{2r+2}{r+2}\in\mathbb{Q}$, 則

$$(r'')^2-2=\left(\frac{2r+2}{r+2}\right)^2-2=\frac{4r^2+8r+4-2(r^2+4r+4)}{(r+2)^2}=\frac{2(r^2-2)}{(r+2)^2},$$

因爲 $r^2<2$, 所以 $(r'')^2-2<0$, 得到 $(r'')^2<2$, 所以 $r''\in Q$。

由上討論得知 $Q=\{r\in\mathbb{Q}|r\le 0\}\cup\{r\in\mathbb{Q}|r>0,r^2<2\}$ 是有理數集 $\mathbb{Q}$ 的一個切割。 □

這兩個例子分別都代表有理數集的一種切割, 但是這兩者之間的差別在哪裡呢? 爲說明兩者的主要差異, 我們需要引進以下定義。

定義 **4** (上界; 下界)**.** 給定一個有序集 S, 且 $E\subset S$,

(a) 若存在 $C\in S$ 使得對所有 $x\in E$, $x\le C$, 則稱集合 E 是 *有上界的* (bounded above), 而 C 是集合 E 的一個 *上界* (upper bound)。

(b) 若存在 $c\in S$ 使得對所有 $x\in E$, $x\ge c$, 則稱集合 E 是 *有下界的* (bounded below), 而 c 是集合 E 的一個 *下界* (lower bound)。

定義 **5** (最小上界; 最大下界)**.** 給定一個有序集 S, 且 $E\subset S$,

(a) 若存在 $M\in S$ 滿足以下兩個條件, 則稱 M 是集合 E 的 *最小上界* 或 *上確界* (supremum):

  (1) 對所有的 $x\in E$ 都有 $x\le M$。 (M 是 E 的一個上界)

  (2) 對所有 $M'<M$, 存在 $x'\in E$ 使得 $M'<x'$。 (任何小於 M 的數都不是 E 的上界)

  一個集合 E 的最小上界會用記號 $\sup E$ 表示。

(b) 若存在 $m\in S$ 滿足以下兩個條件, 則稱 m 是集合 E 的 *最大下界* 或 *下確界* (infimum):

  (1) 對所有的 $x\in E$ 都有 $x\ge m$。 (m 是 E 的一個下界)

  (2) 對所有 $m'>m$, 存在 $x'\in E$ 使得 $m'>x'$。 (任何大於 m 的數都不是 E 的下界)

  一個集合 E 的最大下界會用記號 $\inf E$ 表示。

注意到這些定義當中的 C,c,M,m 都是在有序集 S 當中找尋滿足條件的元素。

以下先討論最小上界與最大下界的一個性質:

定理 **6.** 記 S 是有序集且 $E \subset S$, 若 E 的最小上界存在, 則唯一; 若 E 的最大下界存在, 則唯一。

證明: 假設 M_1 與 M_2 都是集合 E 的最小上界, 而且如果 $M_1 < M_2$, 那麼從 M_2 是最小上界的意義來看, 存在 $x \in E$ 使得 $x > M_1$, 則 M_1 不是 E 的上界, 於是 $M_1 < M_2$ 不對。同樣地, 如果 $M_2 < M_1$, 那麼從 M_1 是最小上界的意義來看, 存在 $x \in E$ 使得 $x > M_2$, 則 M_2 不是 E 的上界, 於是 $M_2 < M_1$ 不對。所以由三一律得知 $M_1 = M_2$。 □

現在將指出 例 **2** 與 例 **3** 中對於有理數的切割之主要差異。

例 **7.**

(a) 關於有理數集 $\mathbb{Q}$ 的切割 $Q = \{r \in \mathbb{Q} | r < 1\}$, 其最小上界在 $\mathbb{Q}$ 中存在。

(b) 關於有理數集 $\mathbb{Q}$ 的切割 $Q = \{r \in \mathbb{Q} | r \leq 0\} \cup \{r \in \mathbb{Q} | r > 0, r^2 < 2\}$, 其最小上界在 $\mathbb{Q}$ 中不存在。

證明:

(a) 欲證 1 是 Q 的最小上界: 因爲對所有 $r \in Q$ 滿足 $r < 1$, 所以 1 是 Q 的一個上界。對任何 $M' \in \mathbb{Q}, M' < 1$, 取 $r = \frac{M'+1}{2} \in Q$, 則 $M' = \frac{M'+M'}{2} < \frac{M'+1}{2} = r$, 所以 M' 不是 Q 的上界。因此 1 是 Q 的最小上界。

(b) 首先證明滿足 $r^2 > 2$ 的正有理數都不是最小上界: 假設 $r \in \mathbb{Q}$ 滿足 $r > 0, r^2 > 2$, 考慮 $r' = r - \frac{r^2-2}{r+2} = \frac{2r+2}{r+2} \in \mathbb{Q}$, 則 $r' < r$, 並且

$$(r')^2 - 2 = \left(\frac{2r+2}{r+2}\right)^2 - 2 = \frac{4r^2+8r+4-2(r^2+4r+4)}{(r+2)^2} = \frac{2(r^2-2)}{(r+2)^2},$$

因爲 $r^2 > 2$, 所以 $(r')^2 - 2 > 0$, 得到 $(r')^2 > 2$, 所以 r 不是 Q 的最小上界。

再證不存在正有理數滿足 $r^2 = 2$: 假設存在有理數 $r = \frac{p}{q}$, 其中 $p, q \in \mathbb{N}, (p, q) = 1$ 使得 $r^2 = 2$, 那麼 $\frac{p^2}{q^2} = 2$ 得到 $p^2 = 2q^2$, 所以 p^2 是偶數, 得到 p 也是偶數。記 $p = 2m$, 再代回 $p^2 = 2q^2$ 得到 $q^2 = 2m^2$, 於是 q^2 也是偶數, 得到 q 也是偶數, 這與 $(p, q) = 1$ 矛盾。所以不存在正有理數滿足 $r^2 = 2$。

最後, 由 例 **3** 的 (c) 的討論得知, 集合 Q 內的元素也不會是 Q 的最小上界。因此 Q 的最小上界在 $\mathbb{Q}$ 中不存在。

□

由前面的分析, 我們稱切割 $Q = \{r \in \mathbb{Q} | r < 1\}$ 定義了一個有理數 1, 而切割 $Q = \{r \in \mathbb{Q} | r \leq 0\} \cup \{r \in \mathbb{Q} | r > 0, r^2 < 2\}$ 因爲無法在 $\mathbb{Q}$ 中找到最小上界, 因此稱這個切割定義了一個 無理數 (irrational number) α。關於滿足 $r^2 = 2$ 的正無理數, 就如在國中或高中數學課程中學到的概念, 我們將它記成 $\sqrt{2}$。

於是我們利用對於有理數集合的切割之概念定義實數集:

定義 **8.** *實數集* 或 *實數系* (real number system) $\mathbb{R}$ 是將所有的有理數切割之最小上界收集而成的集合。

由上述定義可知: 任何一個有理數的切割之最小上界在實數集 $\mathbb{R}$ 中存在。

這裡必須澄清兩件事:

(1) 在 1.1 節 *定理* **1** 告知的是有理數的稠密性: 任兩個有理數之間必存在第三個有理數, 所以有理數集是一些密密麻麻的點, 無論用放大鏡或是更高倍的顯微鏡觀察有理數, 它都還是密集地分佈。但是上面的討論要說明的是: 有理數集雖然是「密集地分佈」, 但是卻「漏洞百出」。所謂的漏洞就是那些無理數, 將所有無理數收集起來再與有理數集取聯集而成的實數集, 就是一條「完整無縫隙的數線」, 也就是各位在中學時學到對於實數的概念與感覺一致。

(2) 觀察 *定理* **6** 的敘述:「記 S 是有序集且 $E \subset S$, 若 E 的最小上界存在, 則唯一; 若 E 的最大下界存在, 則唯一。」敘述當中是說「若」E 的最小上界「存在」的話, 則這個最小上界是獨一無二的; 而 *例* **7** 說明的是: 如果是在有理數集 $\mathbb{Q}$ 當中想找出有理數切割之最小上界的話, 可能會找不到。而在實數集 $\mathbb{R}$ 的意義下, 我們承認這些有理數的分割之最小上界存在。

另一方面, 對於實數集 $\mathbb{R}$ 上的元素 α, 我們目前必須把它想成有理數集的一種切割 Q_α。而且由前面的例子知道: 有一些實數集的元素並非有理數。以下的討論是要在實數集 $\mathbb{R}$ 上定義加法 $+$、乘法 $\cdot$ 以及全序 $<$ 的概念, 並且檢視 **(F)** 與 **(O)** 的所有性質:

(O) 首先定義兩實數 $\alpha, \beta \in \mathbb{R}$ 的大小關係 $\alpha < \beta$ 爲: $Q_\alpha \subsetneqq Q_\beta$。然後證明性質 (O1) 與 (O2):

(O1) 三一律: 對任意 $\alpha, \beta \in \mathbb{R}$, 則 $\alpha < \beta, \alpha = \beta, \beta < \alpha$ 三者之一必成立。

- 給定 $\alpha, \beta \in \mathbb{R}$, 如果 $\alpha < \beta$ 與 $\alpha = \beta$ 都不對, 則存在 $a \in Q_\alpha$ 使得 $a \notin Q_\beta$。對所有 $b \in Q_\beta$, 則有 $b < a$, 又 $a \in Q_\alpha$ 得到 $b \in Q_\alpha$, 因此 $Q_\beta \subsetneqq Q_\alpha$ 得到 $\beta < \alpha$。

(O2) 遞移律: 對於 $\alpha, \beta, \gamma \in \mathbb{R}$, 若 $\alpha < \beta$ 且 $\beta < \gamma$, 則 $\alpha < \gamma$。

- 若 $\alpha < \beta$ 且 $\beta < \gamma$, 則 $Q_\alpha \subsetneqq Q_\beta \subsetneqq Q_\gamma$, 得到 $\alpha < \gamma$。

(F) 給定 $\alpha, \beta \in \mathbb{R}$, 因爲 α 對應於有理數集的一種切割 Q_α, 而 β 對應於有理數集的一種切割 Q_β, 將 $\alpha + \beta$ 對應到集合 $Q_{\alpha+\beta} = \{a + b | a \in Q_\alpha, b \in Q_\beta\}$, 首先檢視 $Q_{\alpha+\beta}$ 是有理數集的一種切割:

(a) 存在 $a \in Q_\alpha, b \in Q_\beta$, 所以 $a + b \in Q_{\alpha+\beta}$。取 $a' \in \mathbb{Q} - Q_\alpha, b' \in \mathbb{Q} - Q_\beta$, 則 $a' + b' \in \mathbb{Q} - Q_{\alpha+\beta}$, 所以 $Q_{\alpha+\beta} \neq \mathbb{Q}$。

(b) 若 $r \in Q_{\alpha+\beta}$, 則 $r = a + b$, 其中 $a \in Q_\alpha, b \in Q_\beta$, 若有 $r' < r$, 則 $r' - b < a$, 所以 $r' - b \in Q_a$, 於是 $r' = (r' - b) + b \in Q_{\alpha+\beta}$。

(c) 若 $r \in Q_{\alpha+\beta}$, 則 $r = a + b$, 其中 $a \in Q_\alpha, b \in Q_\beta$, 因爲存在 $a'' \in Q_\alpha$ 使得 $a < a''$, 令 $r'' = a'' + b$, 則 $r < r''$ 且 $r'' \in Q_{\alpha+\beta}$。

由上討論得知 $Q_{\alpha+\beta}$ 是有理數集的一個切割。

定義完實數集 $\mathbb{R}$ 上的加法後, 現在要檢視實數集上的加法規則:

($\mathrm{F}_{+\mathrm{C}}$) 加法交換律: 對所有 $\alpha, \beta \in \mathbb{R}$, $\alpha+\beta=\beta+\alpha$。

- 因爲 $Q_{\alpha+\beta}=\{a+b|a \in Q_\alpha, b \in Q_\beta\}=\{b+a|b \in Q_\beta, a \in Q_\alpha\}=Q_{\beta+\alpha}$, 所以 $\alpha+\beta=\beta+\alpha$。

($\mathrm{F}_{+\mathrm{A}}$) 加法結合律: 對所有 $\alpha, \beta, \gamma \in \mathbb{R}$, $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$。

- 因爲

$$\begin{aligned} Q_{(\alpha+\beta)+\gamma} &= \{(a+b)+r|a \in Q_\alpha, b \in Q_\beta, r \in Q_\gamma\} \\ &= \{a+b+r|a \in Q_\alpha, b \in Q_\beta, r \in Q_\gamma\} \\ &= \{a+(b+r)|a \in Q_\alpha, b \in Q_\beta, r \in Q_\gamma\} = Q_{\alpha+(\beta+\gamma)}, \end{aligned}$$

  所以 $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$。

($\mathrm{F}_{+\mathrm{Id}}$) 加法單位元素: 存在元素 $0 \in \mathbb{R}$ 使得對所有 $\alpha \in \mathbb{R}$, $\alpha+0=0+\alpha=\alpha$。

- 定義 0 是切割 $Q_0=\{r \in \mathbb{Q}|r<0\}$。若 $a \in Q_\alpha, b \in Q_0$, 則 $a+b<a$ 得到 $a+b \in Q_\alpha$, 所以 $Q_{\alpha+0} \subset Q_\alpha$。另一方面, 若 $a \in Q_\alpha$, 則存在 $a'' \in Q_\alpha$ 使得 $a<a''$, 得到 $a-a''<0$, 於是 $a=a''+(a-a'') \in Q_{\alpha+0}$, 所以 $Q_\alpha \subset Q_{\alpha+0}$。因此 $Q_{\alpha+0}=Q_{0+\alpha}=Q_\alpha$, 即 $0+\alpha=\alpha+0=\alpha$。

($\mathrm{F}_{+\mathrm{Iv}}$) 加法反元素: 每個元素 $\alpha \in \mathbb{R}$ 都存在另一元素 $\beta \in \mathbb{R}$ 使得 $\alpha+\beta=\beta+\alpha=0$。建構完畢後會用 $-\alpha$ 表示 α 的加法反元素。

- 給定 $\alpha \in \mathbb{R}$, 它對應於一個切割 Q_α, 令 Q_β 是滿足以下條件的有理數所成的集合:

$$Q_\beta=\{b \in \mathbb{Q}|\text{ 存在 } r>0 \text{ 使得 } -b-r \notin Q_\alpha\},$$

  首先證明 Q_β 是有理數集 $\mathbb{Q}$ 的一個切割:

  (a) 取 $a' \notin Q_\alpha$, 令 $b=-a'-1$, 則 $-b-1 \notin Q_\alpha$ 得到 $b \in Q_\beta$, 因此 Q_β 非空。取 $a \in Q_\alpha$, 因爲所有 $r>0$ 都滿足 $a-r=-(-a)-r \in Q_\alpha$, 所以 $-a \notin Q_\beta$, 因此 $Q_\beta \neq \mathbb{Q}$。

  (b) 取 $b \in Q_\beta$, 則存在 $r>0$ 使得 $-b-r \notin Q_\alpha$。對所有 $b'<b$, 則 $-b'-r>-b-r$, 於是 $-b'-r \notin Q_\alpha$, 因此 $b' \in Q_\beta$。

  (c) 若 $b \in Q_\beta$, 則存在 $r>0$ 使得 $-b-r \notin Q_\alpha$。取 $b''=b+\frac{r}{2}>b$, 則 $-b''-\frac{r}{2}=-b-r \notin Q_\alpha$, 因此 $b'' \in Q_\beta$。

  由上討論得到 Q_β 是有理數集 $\mathbb{Q}$ 的一個切割。

- 再證 $\alpha+\beta=0$: 若 $a \in Q_\alpha, b \in Q_\beta$, 則存在 $r>0$ 使得 $-b-r \notin Q_\alpha$, 所以 $a<-b-r$, 得到 $a+b<-r<0$, 也就是說, $Q_{\alpha+\beta} \subset Q_0$。另一方面, 若 $r \in Q_0$, 取 $r'=-\frac{r}{2}$, 則 $r'>0$。取整數 $k \in \mathbb{Z}$ 使得 $kr' \in Q_\alpha$ 但 $(k+1)r' \notin Q_\alpha$。令 $b=-(k+2)r'$, 因爲 $-b-r'=(k+1)r' \notin Q_\alpha$, 所以 $b \in Q_\beta$ 得到 $r=kr'+b \in Q_{\alpha+\beta}$, 因此 $Q_0 \subset Q_{\alpha+\beta}$。

  由上述討論得知 $Q_{\alpha+\beta}=Q_0$, 即 $\alpha+\beta=0$。

(O) 討論完實數集 $\mathbb{R}$ 上的加法後, 可以先證明 (O3) 的性質:

(O3) 加法的保序性: 若 $\alpha, \beta \in \mathbb{R}, \alpha < \beta$, 則對任何 $\gamma \in \mathbb{R}$ 都有 $\alpha + \gamma < \beta + \gamma$。

- 由 $\alpha < \beta$ 得到 $Q_\alpha \subsetneqq Q_\beta$, 所以對任何 $\gamma \in \mathbb{R}$ 都有 $Q_{\alpha+\gamma} \subsetneqq Q_{\beta+\gamma}$, 所以 $\alpha + \gamma < \beta + \gamma$。

至於實數上的乘法運算 $\cdot$, 首先定義正實數集 $\mathbb{R}^+ = \{\alpha \in \mathbb{R} | \alpha > 0\}$ 的乘法規則: 若 $\alpha, \beta \in \mathbb{R}^+$, 將 $\alpha \cdot \beta$ 對應到集合

$$Q_{\alpha\cdot\beta} = \{q \in \mathbb{Q} | q < a \cdot b, a \in Q_\alpha, b \in Q_\beta, a, b > 0\},$$

同樣地, 要先檢視 $Q_{\alpha\cdot\beta}$ 是 $\mathbb{Q}$ 的一個切割:

(a) 取 $q = 0 \in \mathbb{Q}$ 得到 $q \in Q$, 因爲存在 $a' \notin Q_\alpha, b' \notin Q_\beta$, 取 $q' = a' \cdot b'$, 則 $q' \notin Q_{\alpha\cdot\beta}$, 於是 $Q_{\alpha\cdot\beta} \neq \mathbb{Q}$。

(b) 給定 $q \in Q_{\alpha\cdot\beta}$, 對任何 $q' \in \mathbb{Q}, q' < q$, 遞移律告知 $q' < q < a \cdot b$, 其中 $a \in Q_\alpha, b \in Q_\beta, a, b > 0$, 所以 $q' \in Q_{\alpha\cdot\beta}$。

(c) 對任何 $q \in Q_{\alpha\cdot\beta}$, 則 $q < a \cdot b$, 其中 $a \in Q_\alpha, b \in Q_\beta, a, b > 0$, 因爲存在 $a'' \in Q_\alpha$ 與 $b'' \in Q_\beta$ 滿足 $0 < a < a'', 0 < b < b''$, 記 $q'' = a'' \cdot b''$, 則 $q'' > q$ 且 $q'' \in Q_{\alpha\cdot\beta}$。

由上討論得知 $Q_{\alpha\cdot\beta}$ 是 $\mathbb{Q}$ 的一個切割。

接著我們可以把 (O4) 證明完畢。

(O4) 乘法對正實數的保序性: 若 $\alpha, \beta \in \mathbb{R}^+$, 則 $0 < \alpha \cdot \beta$。

- 對於 $r \in Q_0$, 以及 $a \in Q_\alpha, b \in Q_\beta, a, b > 0$, 則 $r < 0 < a \cdot b$ 得知 $r \in Q_{\alpha\cdot\beta}$, 因此 $Q_0 \subsetneqq Q_{\alpha\cdot\beta}$ 得到 $0 < \alpha \cdot \beta$。

(F) 再證乘法對於正實數集 $\mathbb{R}^+$ 的情況成立:

($\mathrm{F}._\mathrm{C}$) 乘法交換律: 對所有 $\alpha, \beta \in \mathbb{R}^+$, $\alpha \cdot \beta = \beta \cdot \alpha$。

- 這是因爲

$$\begin{aligned} Q_{\alpha\cdot\beta} &= \{q \in \mathbb{Q} | q < a \cdot b, a \in Q_\alpha, b \in Q_\beta, a, b > 0\} \\ &= \{q \in \mathbb{Q} | q < b \cdot a, b \in Q_\beta, a \in Q_\alpha, b, a > 0\} = Q_{\beta\cdot\alpha}。\end{aligned}$$

($\mathrm{F}._\mathrm{A}$) 乘法結合律: 對所有 $\alpha, \beta, \gamma \in \mathbb{R}^+$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$。

- 若 $q \in Q_{(\alpha\cdot\beta)\cdot\gamma}$, 則 $q < c \cdot r$, 其中 $c \in Q_{\alpha\cdot\beta}, r \in Q_\gamma, c, r > 0$, 得到 $q < c \cdot r < a \cdot b \cdot r$, 其中 $a \in Q_\alpha, b \in Q_\beta, r \in Q_\gamma, a, b, r > 0$, 記 $d = b \cdot r$, 則 $q < a \cdot d$, 其中 $a \in Q_\alpha, d \in Q_{\beta\cdot\gamma}, a, d > 0$, 即 $q \in Q_{\alpha\cdot(\beta\cdot\gamma)}$。因此 $Q_{(\alpha\cdot\beta)\cdot\gamma} \subset Q_{\alpha\cdot(\beta\cdot\gamma)}$。

- 若 $q \in Q_{\alpha\cdot(\beta\cdot\gamma)}$, 則 $q < a \cdot d$, 其中 $a \in Q_\alpha, d \in Q_{\beta\cdot\gamma}, a, d > 0$, 得到 $q < a \cdot d < a \cdot b \cdot r$, 其中 $a \in Q_\alpha, b \in Q_\beta, r \in Q_\gamma, a, b, r > 0$, 記 $c = a \cdot b$, 則 $q < c \cdot r$, 其中 $c \in Q_{\alpha\cdot\beta}, r \in Q_\gamma, c, r > 0$, 即 $q \in Q_{(\alpha\cdot\beta)\cdot\gamma}$。因此 $Q_{\alpha\cdot(\beta\cdot\gamma)} \subset Q_{(\alpha\cdot\beta)\cdot\gamma}$。
  由上討論則有 $Q_{(\alpha\cdot\beta)\cdot\gamma} = Q_{\alpha\cdot(\beta\cdot\gamma)}$, 即 $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$。

($\mathrm{F}_{\cdot\,\mathrm{Id}}$) 乘法單位元素: 存在元素 $1 \in \mathbb{R}^+$ 使得對所有 $\alpha \in \mathbb{R}^+$, $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$。

- 對任何 $q \in Q_{\alpha\cdot 1}$, 則 $q < a \cdot b$, 其中 $a \in Q_\alpha, b \in Q_1, a, b > 0$, 得到 $q < a$, 其中 $a \in Q_\alpha, a > 0$, 所以 $q \in Q_\alpha$。因此 $Q_{\alpha\cdot 1} \subset Q_\alpha$。
- 給定 $q \in Q_\alpha$, 存在 $a \in Q_\alpha, a > 0$ 使得 $q < a$, 又存在 $a'' \in Q_\alpha$ 使得 $q < a < a''$, 所以

$$q < a = a'' \cdot \frac{a}{a''}, \quad \text{其中 } a'' \in Q_\alpha,\ \frac{a}{a''} \in Q_1, a'', \frac{a}{a''} > 0$$

  因此 $q \in Q_{\alpha\cdot 1}$, 得到 $Q_\alpha \subset Q_{\alpha\cdot 1}$。
  由上討論可知 $Q_{\alpha\cdot 1} = Q_{1\cdot\alpha} = Q_\alpha$。因此 $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$。

($\mathrm{F}_{\cdot\,\mathrm{Iv}}$) 乘法反元素: 每個元素 $\alpha \in \mathbb{R}^+$ 都存在另一元素 $\beta \in \mathbb{R}^+$ 使得 $\alpha \cdot \beta = \beta \cdot \alpha = 1$。建構完畢後會用 α^{-1} 表示 α 的乘法反元素。

- 給定 $\alpha \in \mathbb{R}^+$, 它對應於一個切割 Q_α, 令 Q_β 是滿足以下條件的有理數所成的集合:

$$Q_\beta = \{b \in \mathbb{Q} | b \leq 0\} \cup \left\{ b \in \mathbb{Q} \,\middle|\, \text{存在 } r > 0 \text{ 使得 } \frac{1}{b} - r \notin Q_\alpha \right\},$$

  首先證明 <u>Q_β 是有理數集 $\mathbb{Q}$ 的一個切割</u>:

  (a) 首先, $0 \in Q_\beta$; 取 $a \in Q_\alpha, a > 0$, 則任何的 $r > 0$ 都滿足 $\frac{1}{(\frac{1}{a})} - r = a - r \in Q_\alpha$, 所以 $\frac{1}{a} \notin Q_\beta$, 因此 $Q_\beta \neq \mathbb{Q}$。

  (b) 若 $b \in Q_\beta$, 對於 $b' \in \mathbb{Q}, b' < b$, 這裡只需討論 $0 < b' < b$ 的情況即可。因爲存在 $r > 0$ 使得 $\frac{1}{b} - r \notin Q_\alpha$, 而 $\frac{1}{b'} - r > \frac{1}{b} - r$, 所以 $\frac{1}{b'} - r \notin Q_\alpha$, 因此 $b' \in Q_\beta$。

  (c) 若 $b \in Q_\beta$, 這裡只需討論 $b > 0$ 的情況即可。因爲存在 $r > 0$ 使得 $\frac{1}{b} - r \notin Q_\alpha$, 令 b'' 滿足 $\frac{1}{b''} = \frac{1}{b} - \frac{r}{2}$, 則 $\frac{1}{b''} - \frac{r}{2} = \frac{1}{b} - \frac{r}{2} - \frac{r}{2} = \frac{1}{b} - r \notin Q_\alpha$, 而且 $\frac{1}{b''} = \frac{1}{b} - \frac{r}{2} < \frac{1}{b}$ 得知 $b'' > b$, 所以 $b'' \in Q_\beta$。

  由上述討論得知 Q_β 是有理數集 $\mathbb{Q}$ 的一個切割。

- 欲證明 <u>$\alpha \cdot \beta = \beta \cdot \alpha = 1$</u>: 若 $q \in Q_{\alpha\cdot\beta}$, 則 $q < a \cdot b$, 其中 $a \in Q_\alpha, b \in Q_\beta, a, b > 0$, 因爲存在 $r > 0$ 使得 $\frac{1}{b} - r \notin Q_\alpha$, 而 $a \in Q_\alpha$ 得到 $a < \frac{1}{b} - r$, 於是 $q < a \cdot b < 1 - r \cdot b < 1$, 因此 $Q_{\alpha\cdot\beta} \subset Q_1$。
  另一方面, 欲證 $Q_1 \subset Q_{\alpha\cdot\beta}$, <u>先看 $Q_\alpha \subset Q_1$ 的情況</u>, 而且以下的討論只需要看正有理數的情形即可。若 $0 < q < 1$, 取 $n \in \mathbb{N}$ 使得 $q^n \in Q_\alpha$ 而 $q^{n-1} \notin Q_\alpha$。
  <u>若 $\frac{1}{q^{n-1}} \in Q_\beta$</u>, 則 $q = q^n \cdot \frac{1}{q^{n-1}}$, 其中 $q^n \in Q_\alpha, \frac{1}{q^{n-1}} \in Q_\beta$ 就告知 $q \in Q_{\alpha\cdot\beta}$。

若 $\frac{1}{q^{n-1}} \notin Q_\beta$, 則對任何有理數 $r > 0$, $q^{n-1} - r \in Q_\alpha$。由有理數的稠密性, 存在 $q'' \in \mathbb{Q}$ 使得 $q^n < q'' < q^{n-1}$, 現將 q'' 重新表示如下:

$$q'' = q^{n-1} - r' = q^n + r'' = q^n + q \cdot r''', \quad 其中 \quad r', r'', r''' > 0,$$

則

$$q = q \cdot (q^{n-1} + r''') \cdot \frac{1}{q^{n-1} + r'''} = (q^n + q \cdot r''') \cdot \frac{1}{q^{n-1} + r'''},$$

得到 $q^n + q \cdot r''' = q'' \in Q_\alpha$; 關於 $\frac{1}{q^{n-1}+r'''}$, 取有理數 $\frac{r'''}{2} > 0$, 則

$$\frac{1}{\frac{1}{q^{n-1}+r'''}} - \frac{r'''}{2} = q^{n-1} + r''' - \frac{r'''}{2} = q^{n-1} + \frac{r'''}{2} \notin Q_\alpha,$$

所以 $\frac{1}{q^{n-1}+r'''} \in Q_\beta$, 因此 $Q_1 \subset Q_{\alpha\cdot\beta}$。

再看 $Q_1 \subset Q_\alpha$ 的情況, 給定 q 滿足 $0 < q < 1$, 取 $n \in \mathbb{N}$ 使得 $\frac{1}{q^{n-1}} \in Q_\alpha$ 而 $\frac{1}{q^n} \notin Q_\alpha$。

若 $q^n \in Q_\beta$, 則 $q = \frac{1}{q^{n-1}} \cdot q^n$, 其中 $\frac{1}{q^{n-1}} \in Q_\alpha, q^n \in Q_\beta$ 就告知 $q \in Q_{\alpha\cdot\beta}$。

若 $q^n \notin Q_\beta$, 則對任何有理數 $r > 0$, $\frac{1}{q^n} - r \in Q_\alpha$。由有理數的稠密性, 存在 $q'' \in \mathbb{Q}$ 使得 $\frac{1}{q^{n-1}} < q'' < \frac{1}{q^n}$, 現將 q'' 重新表示如下:

$$q'' = \frac{1}{q^n} - r' = \frac{1}{q^{n-1}} + r'' = q\left(\frac{1}{q^n} + r'''\right), \quad 其中 \quad r', r'', r''' > 0,$$

則

$$q = q\left(\frac{1}{q^n} + r'''\right) \cdot \frac{1}{\frac{1}{q^n} + r'''}$$

因爲 $q\left(\frac{1}{q^n} + r'''\right) = q'' \in Q_\alpha$, 對於 $\frac{1}{\frac{1}{q^n}+r'''}$ 而言, 因爲 $\frac{1}{q^n} + r''' - \frac{r'''}{2} = \frac{1}{q^n} + \frac{r'''}{2} \notin Q_\alpha$, 所以 $\frac{1}{\frac{1}{q^n}+r'''} \in Q_\beta$, 於是 $Q_1 \subset Q_{\alpha\cdot\beta}$。

由上述討論可知 $Q_{\alpha\cdot\beta} = Q_{\beta\cdot\alpha} = Q_1$, 因此每個元素 $\alpha \in \mathbb{R}^+$ 都存在另一元素 $\beta \in \mathbb{R}^+$ 使得 $\alpha \cdot \beta = \beta \cdot \alpha = 1$。

($\mathrm{F}_{\cdot+\mathrm{D}}$) 乘法對加法的分配律: 對所有 $\alpha, \beta, \gamma \in \mathbb{R}^+$, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$。

- 若 $q \in Q_{\alpha\cdot(\beta+\gamma)}$, 則 $q < a\cdot d$ 其中 $a \in Q_\alpha, d \in Q_{\beta+\gamma}, a, d > 0$, 得到 $q < a\cdot(b+r) = a \cdot b + a \cdot r$ 其中 $a \in Q_\alpha, b \in Q_\beta, r \in Q_\gamma, a, b+r > 0$。因爲 $\beta > 0, \gamma > 0$, 所以可取到 $b'' > 0, d'' > 0$ 使得 $q < a \cdot b'' + a \cdot r''$, 令 $c = a \cdot b'', d = a \cdot r''$, 所以 $q < c + d$ 其中 $c \in Q_{\alpha\cdot\beta}, d \in Q_{\alpha\cdot\gamma}$, 因此 $q \in Q_{\alpha\cdot\beta+\alpha\cdot\gamma}$, 也就是說, $Q_{\alpha\cdot(\beta+\gamma)} \subset Q_{\alpha\cdot\beta+\alpha\cdot\gamma}$。
  另一方面, 若 $q \in Q_{\alpha\cdot\beta+\alpha\cdot\gamma}$, 則 $q < c + d$ 其中 $c \in Q_{\alpha\cdot\beta}, d \in Q_{\alpha\cdot\gamma}, c, d > 0$, 得到 $q < a' \cdot b + a'' \cdot r$ 其中 $a', a'' \in Q_\alpha, b \in Q_\beta, r \in Q_\gamma, a', a'', b, r > 0$。取 $a = \max(a', a'')$, 則 $q < a\cdot b + a \cdot r = a\cdot(b+r)$ 其中 $a \in Q_\alpha, b+r \in Q_{\beta+\gamma}, a, b+r > 0$, 所以 $q \in Q_{\alpha\cdot(\beta+\gamma)}$, 於是 $Q_{\alpha\cdot\beta+\alpha\cdot\gamma} \subset Q_{\alpha\cdot(\beta+\gamma)}$。

由上討論, 得到對所有 $\alpha, \beta, \gamma \in \mathbb{R}^+$, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$。

接著, 對於 $\alpha \in \mathbb{R}$, 定義 $\alpha \cdot 0 = 0 \cdot \alpha = 0$。至於其它情況, 則用以下方式定義乘法:

$$\alpha \cdot \beta = \begin{cases} -(\alpha \cdot (-\beta)) & \text{若 } \alpha \in \mathbb{R}^+, \beta \in \mathbb{R}^- \\ -((-\alpha) \cdot \beta) & \text{若 } \alpha \in \mathbb{R}^-, \beta \in \mathbb{R}^+ \\ (-\alpha) \cdot (-\beta) & \text{若 } \alpha \in \mathbb{R}^-, \beta \in \mathbb{R}^-, \end{cases}$$

其中 $\mathbb{R}^- = \{\alpha \in \mathbb{R} | \alpha < 0\}$。現在要逐一驗證乘法的規則在 $\mathbb{R}$ 上都成立。

($\mathrm{F}_{\cdot \mathrm{C}}$) 乘法交換律: 對所有 $\alpha, \beta \in \mathbb{R}$, $\alpha \cdot \beta = \beta \cdot \alpha$。

- 若 $\alpha = 0$ 或 $\beta = 0$, 則 $\alpha \cdot \beta = 0 = \beta \cdot \alpha$。
- 若 $\alpha \in \mathbb{R}^+, \beta \in \mathbb{R}^-$, 則 $\alpha \cdot \beta = -(\alpha \cdot (-\beta)) = -((-\beta) \cdot \alpha) = \beta \cdot \alpha$。
- 若 $\alpha \in \mathbb{R}^-, \beta \in \mathbb{R}^+$, 則 $\alpha \cdot \beta = -((-\alpha) \cdot \beta) = -(\beta \cdot (-\alpha)) = \beta \cdot \alpha$。
- 若 $\alpha \in \mathbb{R}^-, \beta \in \mathbb{R}^-$, 則 $\alpha \cdot \beta = (-\alpha) \cdot (-\beta) = (-\beta) \cdot (-\alpha) = \beta \cdot \alpha$。

($\mathrm{F}_{\cdot \mathrm{A}}$) 乘法結合律: 對所有 $\alpha, \beta, \gamma \in \mathbb{R}$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$。

- 若 $\alpha = 0$ 或 $\beta = 0$ 或 $\gamma = 0$, 則 $(\alpha \cdot \beta) \cdot \gamma = 0 = \alpha \cdot (\beta \cdot \gamma)$。
- 若 $\alpha, \beta \in \mathbb{R}^+, \gamma \in \mathbb{R}^-$, 則 $(\alpha \cdot \beta) \cdot \gamma = -((\alpha \cdot \beta) \cdot (-\gamma)) = -(\alpha \cdot \beta \cdot (-\gamma))$, 而 $\alpha \cdot (\beta \cdot \gamma) = \alpha \cdot (-(\beta \cdot (-\gamma))) = -(\alpha \cdot (-(-(\beta \cdot (-\gamma))))) = -(\alpha \cdot (\beta \cdot (-\gamma))) = -(\alpha \cdot \beta \cdot (-\gamma))$, 所以 $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$。反覆利用乘法交換律也可得知其它兩正一負的三實數乘法結合律也成立。
- 若 $\alpha \in \mathbb{R}^+, \beta, \gamma \in \mathbb{R}^-$, 則 $(\alpha \cdot \beta) \cdot \gamma = -(\alpha \cdot (-\beta)) \cdot \gamma = (-(-(\alpha \cdot (-\beta)))) \cdot (-\gamma) = (\alpha \cdot (-\beta)) \cdot (-\gamma) = \alpha \cdot (-\beta) \cdot (-\gamma) = \alpha \cdot ((-\beta) \cdot (-\gamma)) = \alpha \cdot (\beta \cdot \gamma)$。反覆利用乘法交換律也可得知兩負一正的三實數乘法結合律也成立。
- 若 $\alpha, \beta, \gamma \in \mathbb{R}^-$, 則 $(\alpha \cdot \beta) \cdot \gamma = ((-\alpha) \cdot (-\beta)) \cdot \gamma = -(((-\alpha) \cdot (-\beta)) \cdot (-\gamma)) = -((-\alpha) \cdot (-\beta) \cdot (-\gamma)) = -((-\alpha) \cdot ((-\beta) \cdot (-\gamma))) = -((-\alpha) \cdot (\beta \cdot \gamma)) = \alpha \cdot (\beta \cdot \gamma)$。

($\mathrm{F}_{\cdot \mathrm{Id}}$) 乘法單位元素: 存在元素 $1 \in \mathbb{R}$ 使得對所有 $\alpha \in \mathbb{R}$, $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$。

- 若 $\alpha = 0$, 則 $\alpha \cdot 1 = 0 = 1 \cdot \alpha = \alpha$。
- 若 $\alpha \in \mathbb{R}^-$, 則 $\alpha \cdot 1 = -((-\alpha) \cdot 1) = -(1 \cdot (-\alpha)) = 1 \cdot \alpha$, 而 $-((-\alpha) \cdot 1) = -(-\alpha) = \alpha$, 所以 $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$。

($\mathrm{F}_{\cdot \mathrm{Iv}}$) 乘法反元素: 每個元素 $\alpha \in \mathbb{R} - \{0\}$ 都存在另一元素 $\beta \in \mathbb{R} - \{0\}$ 使得 $\alpha \cdot \beta = \beta \cdot \alpha = 1$。建構完畢後會用 α^{-1} 表示 α 的乘法反元素。

- 對於 $\alpha \in \mathbb{R}^-$, 取 $\beta = -(-\alpha)^{-1} \in \mathbb{R}^-$, 則

$$\alpha \cdot (-(-\alpha)^{-1}) = (-(-\alpha)^{-1}) \cdot \alpha = (-(-(-\alpha)^{-1})) \cdot (-\alpha) = (-\alpha)^{-1} \cdot (-\alpha) = 1。$$

($\mathrm{F}_{\cdot +\mathrm{D}}$) 乘法對加法的分配律: 對所有 $\alpha, \beta, \gamma \in \mathbb{R}$, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$。

- 若 $\alpha = 0$, 則 $\alpha \cdot (\beta + \gamma) = 0 = \alpha \cdot \beta + \alpha \cdot \gamma$; 若 $\beta = 0$, 則 $\alpha \cdot (\beta + \gamma) = \alpha \cdot \gamma = \alpha \cdot \beta + \alpha \cdot \gamma$; $\gamma = 0$ 的情況與 $\beta = 0$ 的情況一樣地討論。

- 若 $\beta+\gamma=0, \beta>0$, 則 $\gamma<0$, 考慮 $\beta=(\beta+\gamma)+(-\gamma)$, 則 $\alpha\cdot\beta=\alpha\cdot((\beta+\gamma)+(-\gamma))=\alpha\cdot(\beta+\gamma)+\alpha\cdot(-\gamma)$, 得到 $\alpha\cdot(\beta+\gamma)=\alpha\cdot\beta-\alpha\cdot(-\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma$。
- 若 $\alpha\in\mathbb{R}^-, \beta+\gamma\in\mathbb{R}^+$, 則 $\alpha\cdot(\beta+\gamma)=-((-\alpha)\cdot(\beta+\gamma))=-((-\alpha)\cdot\beta+(-\alpha)\cdot\gamma)=-(-\alpha)\cdot\beta-(-\alpha)\cdot\gamma=\alpha\cdot\beta+\alpha\cdot\gamma$。
- 若 $\alpha\in\mathbb{R}^+, \beta\in\mathbb{R}^-, \beta+\gamma\in\mathbb{R}^+$, 考慮 $\gamma=(\beta+\gamma)+(-\beta)$, 則 $\alpha\cdot\gamma=\alpha\cdot((\beta+\gamma)+(-\beta))=\alpha\cdot(\beta+\gamma)+\alpha\cdot(-\beta)=\alpha\cdot(\beta+\gamma)-\alpha\cdot\beta$, 所以 $\alpha\cdot(\beta+\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma$。
- 若 $\alpha\in\mathbb{R}^+, \beta\in\mathbb{R}^-, \beta+\gamma\in\mathbb{R}^-$, 則 $\alpha\cdot(\beta+\gamma)=-(\alpha\cdot(-(\beta+\gamma)))=-(\alpha\cdot(-\beta+(-\gamma)))=-(\alpha\cdot(-\beta)+\alpha\cdot(-\gamma))=-\alpha\cdot(-\beta)-\alpha\cdot(-\gamma)=\alpha\cdot\beta-(-(\alpha\cdot(-(-\gamma)))))=\alpha\cdot\beta+\alpha\cdot\gamma$。
- 若 $\alpha,\beta,\gamma\in\mathbb{R}^-$, 則 $\alpha\cdot(\beta+\gamma)=(-\alpha)\cdot(-(\beta+\gamma))=(-\alpha)\cdot(-\beta+(-\gamma))=(-\alpha)\cdot(-\beta)+(-\alpha)\cdot(-\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma$。
- 若 $\alpha,\beta,\beta+\gamma\in\mathbb{R}^-, \gamma\in\mathbb{R}^+$, 考慮 $\beta=(\beta+\gamma)+(-\gamma)$, 則 $\alpha\cdot\beta=\alpha\cdot((\beta+\gamma)+(-\gamma))=\alpha\cdot(\beta+\gamma)+\alpha\cdot(-\gamma)=\alpha\cdot(\beta+\gamma)-\alpha\cdot\gamma$, 因此 $\alpha\cdot(\beta+\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma$。
- 若 $\alpha,\beta\in\mathbb{R}^-, \gamma,\beta+\gamma\in\mathbb{R}^+$, 則 $\alpha\cdot(\beta+\gamma)=-((-\alpha)\cdot(\beta+\gamma))=-((-\alpha)\cdot\beta+(-\alpha)\cdot\gamma)=-(-\alpha)\cdot\beta+(-(-\alpha)\cdot\gamma)=-(\alpha\cdot(-\beta))-(-\alpha)\cdot\gamma=\alpha\cdot\beta+\alpha\cdot\gamma$。

至此我們已全部證明完實數系 $\mathbb{R}$ 關於有序體的所有性質 **(F)** 與 **(O)**, 最後我們要引進實數集的切割以及戴德金切割原理與確界原理。

定義 **9.** 實數集 $\mathbb{R}$ 的一個 *切割* (cut) 指的是實數集 $\mathbb{R}$ 的一個的一個子集合 R 滿足以下三個條件:

(a) 集合 R 非空, 而且 $R\neq\mathbb{R}$。

(b) 若 $x\in R, x'\in\mathbb{R}$ 而且 $x'<x$, 則 $x'\in R$。

(c) 若 $x\in R$, 則存在 $x''\in R$ 使得 $x<x''$。

公理 (戴德金切割原理)**.** 對於實數集 $\mathbb{R}$ 的任何一個切割 R 之最小上界存在。

換言之, 我們可以說

實數集 $\mathbb{R}$ 是滿足戴德金切割原理的有序體。

為了後續的討論, 我們將戴德金切割原理稱為 *實數的完備性公理* (D)。利用戴德金提出的切割原理可以將實數集 $\mathbb{R}$ 建構完畢而得以有清楚的認識, 然而在往後數學分析的討論, 若要將所有事物利用戴德金的切割原理進行論述將會變得非常複雜, 於是我們需要一個比戴德金的切割原理還要容易操作的方式進行各種運算及邏輯推演, 以下要介紹的確界原理日後便取代了戴德金切割原理, 這是因為確界原理描述實數完備性的方式是以一般的有界集合為主角, 而非以切割為主體。

定義 10 (最大數與最小數)**.** 一個有序集合 E, 若有一個元素 $x \in E$ 滿足對所有 $y \in E$ 都有 $y \leq x$, 則稱 x 是 E 的 最大數 (maximum element); 若有一個元素 $x' \in E$ 滿足對所有 $y \in E$ 都有 $x' \leq y$, 則稱 x' 是 E 的 最小數 (minimum element)。

這裡應注意的是: 與 定義 **4** 與 定義 **5** 相比, 最大數與最小數是直接在有序集合 E 當中尋找滿足條件的元素。

定理 11 (確界原理)**.** 若一個非空的集合 $E \subset \mathbb{R}$ 有上界, 則有最小上界。若一個非空的集合 $E \subset \mathbb{R}$ 有下界, 則有最大下界。

證明:

(A) 若 E 中有最大數 M, 則 M 就是 E 的一個上界。另一方面, 因爲 $M \in E$, 所以任何小於 M 的實數 M' 必有 $M' < M$, 得到 M' 不再是 E 的上界, 所以 M 是 E 的最小上界。

(B) 若 E 中沒有最大數, 則將實數集 $\mathbb{R}$ 按照以下方法建立一種切割 R: 令 R' 是將所有 E 的上界收集而成的集合, 記 $R = \mathbb{R} - R'$。

首先要驗證的是 R 形成實數集 $\mathbb{R}$ 的一個切割:

(a) 取 $x \in E$, 則 $x \in R$; 因爲 E 有上界, 所以 R' 非空, 得到 $R \neq \mathbb{R}$。

(b) 對於 $x \in R$, $x' \in \mathbb{R}$ 而且 $x' < x$, 則 x' 不是 E 的上界, 因此 $x' \in R$。

(c) 若 $x \in R$, 則 x 不是 E 的上界, 所以存在 $x'' \in E$ 使得 $x < x''$, 而 E 中沒有最大數告知 $x'' \notin R'$, 得到 $x'' \in R$。

由戴德金切割原理: 分割 R 確定了一個實數 α, 它是 R 的最小上界。欲說明 α 也是 E 的最小上界, 這是因爲由 (c) 得知 $E \subset R$, 而分割的意義得知 α 是 E 的上界。另一方面, 任何 $\beta < \alpha$, 存在 $x' \in R$ 使得 $\beta < x'$, 而 x' 不是 E 的上界告知存在 $x'' \in E$ 使得 $x' < x''$, 得到 $\beta < x''$ 其中 $x'' \in E$, 於是 α 是 E 的最小上界。

同理可證: 有下界的非空實數集必有最大下界。請同學自行推演一次。 □

到目前爲止, 我們把實數集改寫成以下敘述:

實數集 $\mathbb{R}$ 是一個滿足確界原理的有序體。

確界原理在這裡把它稱爲 `實數的完備性公理 (S)`。上面的討論其實只證明了一半, 也就是說, 我們只完成了「`實數的完備性公理 (D)` $\Rightarrow$ `實數的完備性公理 (S)`」這一部份的論證。實際上它們是等價的敘述, 從確界原理出發推得戴德金切割原理的證明, 我們必須引進其它術語才能證明, 因此留到第 3 章再討論。

至此我們定義完實數並檢視有序體的所有性質後, 先接受了戴德金切割原理與確界原理等價的情況下, 現在我們要證明的是實數集也具有稠密性:

定理 12 (實數的稠密性, dense property)**.** 任兩個不相等的實數間必存在第三個實數, 並且這個實數可以取到有理數。

證明: 若 $\alpha < \beta, \beta \notin \mathbb{Q}$ 因爲 α 是由 Q_α 決定, 而 β 是由 Q_β 決定, 並且 $Q_\alpha \subset Q_\beta, Q_\alpha \neq Q_\beta$, 所以存在有理數 $q \in Q_\beta$ 使得 $q \notin Q_\alpha$, 於是 $\alpha \leq q < \beta$ (注意到若 α 是有理數時, 等號可能成立)。因爲 Q_β 沒有最大數, 所以如果 $q = \alpha$ 的話, 那麼就重新找一個更大的有理數 $\alpha = q < q' < \beta$, 則 q' 即爲所求。 □

這一節的最後還要介紹一個之後會用到的阿基米德性質:

定理 13 (阿基米德性質, Archimedes property)**.** 若 $x, y \in \mathbb{R}, x > 0$, 則存在 $n \in \mathbb{N}$ 使得 $nx > y$。

證明: 考慮集合 $E = \{nx\}_{n\in\mathbb{N}}$, 假設結論不對, 則 y 是集合 E 的一個上界, 所以 E 會有最小上界 $\alpha = \sup E$。因爲 α 爲最小上界, 而且 $x > 0$, 所以 $\alpha - x$ 不是 E 的上界, 所以存在 $m \in \mathbb{N}$ 使得 $\alpha - x < mx$, 即 $\alpha < (m+1)x \in E$, 這與 α 爲最小上界這個性質矛盾。因此, 存在 $n \in \mathbb{N}$ 使得 $nx > y$。 □

1.3 可數集與不可數集

各位在小學的時候是否有跟同學玩過「鬥片」或「翹牌」? 它是一種五顏六色的塑膠片, 通常都是卡通造形的圖案, 兩人各取一個鬥片放在桌上, 用手輪流推送自己的鬥片, 只要自己的鬥片壓在對方的鬥片上就算贏, 即可獲得對方的鬥片。

鬥片在我那個年代風行一時, 文具店賣著各式各樣的鬥片, 常常放學後就會去文具店挑選購買喜歡的鬥片, 隔天期待著下課時間和同學對戰。我小時候手腦很不協調, 每玩必輸, 所以一度手上有幾十個鬥片不一會兒就輸得精光, 卻見強者我同學有個專門放鬥片的盒子而且愈裝愈滿。而我印象很深刻的一件事情是有一次我用一個很不起眼的小小鬥片贏到同學的一個夜光鬥片, 那個夜光鬥片真的是太漂亮了, 之後就被我收藏起來。

講這個故事是要提出一個大家在比較數量時的一個常用方法, 那就是先分別計數自己手上的鬥片, 數完之後再分別報數, 得到強者我同學 94 狂, 而我只有 87 個沒辦法再多了, 所以強者我同學的鬥片比較多。如果我們不在意 $94, 87$ 這兩個數, 只是想要知道「誰的鬥片多或少」的情況下, 這時有另外一個方法, 那就是把同學的鬥片盒放在左邊, 自己的鬥片盒放在右邊, 然後左手右手同時抓取一個鬥片出來, 在不斷地抓取之下, 結果會在某個時刻, 左手可以再抓出一個鬥片而右手無法再抓出一個鬥片, 這時就知道左邊盒子的鬥片數是比較多的。

回到數學層面, 這一節想要回答以下三個數學問題:

(1) 正整數的個數與正偶數的個數哪個比較多?

(2) 有理數的個數與實數的個數哪個比較多?

(3) $[0, 1]$ 區間中的實數與 $[0, 2]$ 區間中的實數哪個比較多?

有些人會覺得這三個問題都很簡單, 比方說會有以下的「迷思」(代表以下推論是有些狀況的):

(A) 正整數比正偶數來說多了正奇數, 所以正整數個數比正偶數多。

(B) 實數比有理數來說多了無理數 (比方說 $\sqrt{2}$ 還有 π 等), 所以實數個數比有理數多。

(C) $[0,2]$ 區間比 $[0,1]$ 區間多了 $(1,2]$ 這一段, 所以 $[0,2]$ 中的實數個數比 $[0,1]$ 中的實數多。

如果看清楚上面三個論述, 就會知道這三個論述的觀點是以兩個集合之間利用包含 $\subset$ 的關係看待事情。利用集合的包含關係 $\subset$ 在某些情況是可以描述所謂的大小關係, 但也不難發現有的時候兩個集合在包含的意義下是沒有辦法比較的, 例如 $A=\{1,2\}$ 與 $B=\{2,3\}$ 彼此沒有包含的關係。在代數學上, 我們會說集合搭配包含的關係 $\subset$ 會形成 *偏序集* (partially ordered set)。

但是就以 $A=\{1,2\}$ 與 $B=\{2,3\}$ 這兩個集合來說, 雖然兩集合並沒有包含的關係, 卻可以淸楚地「數」集合中的元素個數, 因爲集合 A 與集合 B 的元素個數都是兩個, 所以我們會說集合 A 與集合 B「一樣多」。於是我們希望在數學上提出一個可以「數個數」的概念, 進而比較任兩個集合的元素個數的多寡。

不曉得現在各位有沒有意識到剛才的三個問題比數門片數量的問題來說困難得多, 這是因爲基本上這三個問題是沒有辦法好好地算個數, 就以正整數集來說, 讓 $1,2,3,\ldots$ 好好地排列之下, 你是看不到自然數的盡頭, 若用數學的術語來說, 自然數有 *後繼元素* (successor), 而有理數、實數、或是區間的元素怎麼計算個數又更爲困難。這告訴我們在面對這些問題時, 我們無法利用第一種數門片的方法 (先各別算個數, 再說出數字的大小比較) 處理現在遇到的問題, 但第二種方法產生了契機說明清楚。

另一個要提的是: 上述用集合包含的關係而得的論述和現在所謂的數個數之間又有什麼樣的關聯呢? 雖然正式的數學術語還沒有介紹, 但是這裡想先給各位一點點感覺, 若兩個集合之間有包含的關係時, 對於集合中的元素個數來說, 將以相對「保守」的方式下結論, 比方說:

(A) 因爲偶數集包含於整數集, 所以可以下的結論是「偶數集的個數不會比整數集來得多」;

(B) 因爲有理數集包含於實數集, 所以「有理數集的個數不會比實數集來得多」;

(C) 因爲 $[0,1]$ 區間包含於 $[0,2]$ 區間, 所以「$[0,1]$ 中的實數個數不會比 $[0,2]$ 中的實數多」。

在確實討論這三個問題前, 爲了解釋完整起見, 我們必須把集合與映射的相關術語重新介紹一次。

定義 **1** (映射; 定義域; 對應域; 值域)**.** 給定兩個集合 X,Y, 若有一種規則 f 將集合 X 中的每個元素 x, 都對應到集合 Y 中的唯一元素 y, 則稱 f 是集合 X 到 Y 的一個 *映射* (mapping)。其中 y 稱爲 x 在映射 f 之下的 *像* (image); 而 X 稱爲 f 的 *定義域* (domain), Y 稱爲 f 的 *對應域* (codomain), 而集合 $R=\{f(x)|x\in X\}$ 稱爲 f 的 *值域* (range)。

各位在一些文獻或書籍中會看到 $f:X\to Y$ 有時候會稱爲 *函數* (function)。而一般來說, 若 Y 並非實數集的時候, 通常會採用映射一詞形容 f, 而函數這個詞會比較常特別用來形容 $f:X\to\mathbb{R}$ 的關係。

定義 **2** (一對一; 映成)**.**

(a) 若映射 $f : X \to Y$ 滿足以下性質:「對任何 $x_1, x_2 \in X, x_1 \neq x_2$ 都有 $f(x_1) \neq f(x_2)$」, 則稱 $f : X \to Y$ 是 一對一 (one-to-one, injective)。

(b) 若映射 $f : X \to Y$ 滿足以下性質:「對任何 $y \in Y$, 都存在 $x \in X$ 使得 $f(x) = y$。」, 則稱 $f : X \to Y$ 是 映成的 (onto, surjective)。

在檢查一個映射是否爲一對一的時候, 我們也可以用它的否逆命題檢查之。也就是說, 從 $f(x_1) = f(x_2)$ 出發, 若能推得 $x_1 = x_2$ 的話, 那麼也可以得知 $f : X \to Y$ 是一對一。

定義 **3.** 如果兩個集合 X 和 Y 之間存在一對一且映成的映射, 則稱集合 X 和 Y 有相同的基數 (have the same cardinality)。當兩個集合有相同的基數時, 我們會用記號 $X \sim Y$ 表示。

在代數上, 我們說 $X \sim Y$ 會形成一個 等價關係 (equivalence relation), 所謂等價關係, 指的是滿足以下三個條件的關係:

(a) 對任何集合 X 都有 $X \sim X$。

(b) 給定 X 與 Y 爲兩集合, 若 $X \sim Y$, 則 $Y \sim X$。

(c) 給定 X, Y, Z 爲三個集合, 若 $X \sim Y$ 且 $Y \sim Z$, 則 $X \sim Z$。

定義 **4.** 給定一個集合 S,

(a) 若 S 是空集合 (empty set), 或是存在 $n \in \mathbb{N}$ 使得 S 與 $\{1, 2, \ldots, n\}$ 有一樣的基數, 則稱集合 S 是 有限集 (finite set)。

(b) 若 S 不是有限集, 則稱集合 S 是 無限集 (infinite set)。

(c) 若 S 與正整數集 $\mathbb{N}$ 有相同的基數, 則稱集合 S 是 可數集 (countable set)。

(d) 若 S 不是有限集也不是可數集, 則稱集合 S 是 不可數集 (uncountable set)。

注意到這份講義的定義, 可數集並不包括有限集, 這個詞就專指與正整數集有相同基數的集合, 所以有的時候會特地強調成 無窮可數集 (infinite countable set)。然而有些書籍或文獻會把可數集也包括有限集, 這種見仁見智的定義方式, 只要前後文自成系統就好了, 不需要對這件事有過多的困擾。

探討一個集合可數與不可數是有一套深刻的理論, 這裡並不打算完整地介紹那個理論, 因爲它並不是高等微積分課程的主軸。這裡的重點只是要用最精簡且最快速的方法回答前面三個問題, 從中讓大家了解自然數、整數、有理數與實數在可數或不可數的意義下之關係。

例 **5.** 正整數 $\mathbb{N}$ 與正偶數 $2\mathbb{N}$ 有一樣的基數。

證明: 建立映射 $f : \mathbb{N} \to 2\mathbb{N}$ 爲 $f(n) = 2n$。

(a) 對於 $m, n \in \mathbb{N}, m \neq n$, 則 $f(m) = 2m \neq 2n = f(n)$, 所以 $f : \mathbb{N} \to 2\mathbb{N}$ 是一對一映射。

(b) 對於 $y \in 2\mathbb{N}$, 則 $y = 2m$ 其中 $m \in \mathbb{N}$, 所以 $f(m) = 2m = y$ 得到 $f : \mathbb{N} \to 2\mathbb{N}$ 是映成的。

由上得知 $\mathbb{N} \sim 2\mathbb{N}$。 $\square$

例 **6.** 可數集 A 的子集合 E, 若 E 不是有限集, 則 E 是可數集。

證明: 因爲 A 是可數集, 則存在 $f:\mathbb{N}\to A$ 是一對一且映成的映射。換言之, 我們可以將 A 中的元素給予標號 $f(1)=a_1, f(2)=a_2,\ldots,f(n)=a_n,\ldots$, 於是 $A=\{a_1,a_2,\ldots,a_n,\ldots\}$。

對於 $E\subset A$ 且 E 不是有限集, 從 $a_1,a_2,a_3,\ldots$ 開始尋找, 將第一個落在 E 中的元素記爲 a_{n_1}, 再從 a_{n_1} 之後找到下一個落在 E 中的元素記爲 a_{n_2}, 由此得到 a_{n_k} 是在 $a_{n_{k-1}}$ 之後尋找下一個落在 E 中的元素。如此建立了映射 $\overline{f}:\mathbb{N}\to E$, 其中 $\overline{f}(k)=a_{n_k}$。以下將證明 $\mathbb{N}$ 與 E 有相同的基數。

(a) <u>$\overline{f}$ 是一對一映射</u>: 若 $k'\neq k''$ 得到 $\overline{f}(k')=a_{n_{k'}}, \overline{f}(k'')=a_{n_{k''}}$, 因爲 $n_{k'}\neq n_{k''}$, 而 $f:\mathbb{N}\to A$ 是一對一映射, 所以 $a_{n_{k'}}\neq a_{n_{k''}}$, 因此 $\overline{f}$ 是一對一。

(b) <u>$\overline{f}$ 是映成的</u>: 對於 $a\in E\subset A$, 因爲 $f:\mathbb{N}\to A$ 是映成的, 所以存在 $n\in\mathbb{N}$ 使得 $f(n)=a$, 按照記號的約定, 會記成 $a=a_n$, 而對於 $\bar{f}$ 來說, 依序從 $\overline{f}(1),\overline{f}(2),\ldots,\overline{f}(n)$ 開始找起, 一定會在 $\{1,2,\ldots,n\}$ 當中找到某個數 k 使得 $\overline{f}(k)=a_n=a$, 所以 $\overline{f}$ 是映成的。

□

例 **7.** $(0,1)$ 開區間中的有理數集 $(0,1)\cap\mathbb{Q}$ 是可數集。

證明: 按照以下方式將 $(0,1)\cap\mathbb{Q}$ 的元素排列:

$$\frac{1}{2},\frac{1}{3},\frac{2}{3},\frac{1}{4},\frac{3}{4},\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5},\ldots,$$

也就是說, $(0,1)$ 中的有理數可表示成 $\frac{p}{q}, p,q\in\mathbb{N}, p<q, (p,q)=1$, 排列的方式是先按照分母 q 由小到大排列, 若 q 相同時, 再按照分子 p 由小到大排列。

注意到上述的有理數排列必須把 p,q 不互質的情況刪除。現在我們把上述的有理數排列補回當初不互質的元素:

$$\frac{1}{2},\frac{1}{3},\frac{2}{3},\frac{1}{4},\frac{2}{4},\frac{3}{4},\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5},\ldots,\frac{1}{k},\frac{2}{k},\ldots,\frac{k-1}{k},\frac{1}{k+1},\frac{2}{k+1},\ldots,\frac{k}{k+1},\ldots,$$

補完之後, 我們不要把這些元素想成是兩數的除法, 而是純粹以指標 $a_{pq}=\frac{p}{q}$ 的眼光看待之, 其中 $p,q\in\mathbb{N}, p<q, q\geq 2$。如果你把這些元素寫成表格的話, 則 a_{pq} 在表格中是位在上三角的地方。

記 $A=\{a_{pq}\}$, 此時建立 $f:A\to\mathbb{N}$ 爲 $f(a_{pq})=(0+1+2+\cdots+(q-2))+p$。

(a) $f:A\to\mathbb{N}$ 是一對一: 若 $a_{pq}\neq a_{p'q'}$, 則 $p\neq p'$ 或 $q\neq q'$。

- 若 $q\neq q'$, 比方說 $q<q'$, 則 $q'\geq q+1$ 得到 $q'-2\geq q-1$, 所以

$$\begin{aligned} f(a_{pq})&=(0+1+2+\cdots+(q-2))+p\leq 0+1+2+\cdots+(q-2)+(q-1)\\ &\leq 0+1+2+\cdots+(q'-2)<0+1+2+\cdots+(q'-2)+p'=f(a_{p'q'}) \end{aligned}$$

- 若 $q=q', p\neq p'$, 比方說 $p<p'$, 則

$$\begin{aligned} f(a_{pq})&=(0+1+2+\cdots+(q-2))+p=(0+1+2+\cdots+(q'-2))+p\\ &<(0+1+2+\cdots+(q'-2))+p'=f(a_{p'q'})。 \end{aligned}$$

(b) $f: A \to \mathbb{N}$ 是映成的: 給定 $n \in \mathbb{N}$, 存在一數 $q' \in \mathbb{N} \cup \{0\}$ 使得 $0+1+2+\cdots+q' < n$ 但是 $0+1+2+\cdots+q'+(q'+1) \geq n$, 令 $q = q'+2$, 記 $p = n-(0+1+2+\cdots+q')$, 則 $f(a_{pq}) = n$。

由上討論可知 A 是可數集; 最後再用 例 **6** 的結果得知 $(0,1)\cap\mathbb{Q}$ 是可數集。 □

例 **8.** $[0,1]$ 閉區間中的有理數集 $[0,1]\cap\mathbb{Q}$ 是可數集。

解. 因爲存在一對一且映成的映射 $f: \mathbb{N} \to (0,1)\cap\mathbb{Q}$, 現建立映射 $\overline{f}: \mathbb{N} \to [0,1]\cap\mathbb{Q}$ 如下:

$$\overline{f}(1) = 0, \quad \overline{f}(2) = 1, \quad \overline{f}(n) = f(n-2),\ n \in \mathbb{N},\ n \geq 3。$$

(a) $\overline{f}: \mathbb{N} \to [0,1]\cap\mathbb{Q}$ 是一對一: 對於 $m \neq n$, 若 $m,n \geq 3$, 因爲 f 是一對一得知 $\overline{f}$ 是一對一; 若 $m = 1, n \neq 1$, 則 $\overline{f}(1) = 0, \overline{f}(n) > 0$ 得知 $\overline{f}(1) \neq \overline{f}(n)$; 若 $m = 2, n \neq 2$, 則 $\overline{f}(2) = 1, \overline{f}(n) < 1$ 得知 $\overline{f}(2) \neq \overline{f}(n)$。因此 $\overline{f}$ 是一對一。

(b) $\overline{f}: \mathbb{N} \to [0,1]\cap\mathbb{Q}$ 是映成的: 給定 $a \in [0,1]\cap\mathbb{Q}$, 若 $a = 0$, 則取 $n = 1$ 使得 $\overline{f}(n) = a$; 若 $a = 1$, 則取 $n = 2$ 使得 $\overline{f}(2) = 1$, 若 $a \in (0,1)\cap\mathbb{Q}$, 因爲 f 映成, 則存在 k 使得 $f(k) = a$, 於是取 $n = k+2$ 則得 $\overline{f}(k+2) = f(k) = a$。因此 $\overline{f}$ 是映成的。

由上討論得知:$[0,1]$ 閉區間中的有理數集 $[0,1]\cap\mathbb{Q}$ 是可數集。

例 **9.** 若 $A_1, A_2, \ldots, A_n, \ldots$ 是可數集, 則 $\cup_{n=1}^{\infty} A_n$ 也是可數集。

證明: 因爲對所有 $n \in \mathbb{N}$, A_n 是可數集, 所以將每個集合的元素用以下方式列出來:

$$\begin{aligned}
A_1 &= \{a_{11}, a_{12}, a_{13}, \ldots, a_{1n}, \ldots\} \\
A_2 &= \{a_{21}, a_{22}, a_{23}, \ldots, a_{2n}, \ldots\} \\
A_3 &= \{a_{31}, a_{32}, a_{33}, \ldots, a_{3n}, \ldots\} \\
&\vdots \\
A_n &= \{a_{n1}, a_{n2}, a_{n3}, \ldots, a_{nn}, \ldots\} \\
&\vdots
\end{aligned}$$

注意到 a_{ij} 的第一個指標代表 a_{ij} 屬於集合 A_i, 而第二個指標代表元素 a_{ij} 在 A_i 中與正整數之間的對應。

現在要將這些元素做以下的重排 (這種排列方法稱爲斜線排列法):

$$\begin{aligned}
f: \cup_{n=1}^{\infty} A_n &\longrightarrow \qquad \mathbb{N} \\
a_{ij} \quad &\longmapsto (0+1+2+\cdots+(i+j-2))+i
\end{aligned}$$

這種排列的方式可仿照 例 **7** 的討論可證明 f 是一對一且映成的映射。而且當 A_n 之間有共同的元素時, 則聯集之後那些重覆的元素只能算一個元素, 所以用 例 **6** 的結果得知 $\cup_{n=1}^{\infty} A_n$ 是可數集。 □

例 **10.** 有理數集是可數集。

證明: 因爲對所有 $k \in \mathbb{Z}$, $[k, k+1] \cap \mathbb{Q}$ 是可數集, 所以由 例 **9** 知有理數集可表示成

$$\cup_{k=1}^{\infty}([k-1, k] \cup [-k, -k+1] \cap \mathbb{Q})$$

是可數集。 □

最後要討論的是實數的基數。首先花一點時間解釋實數的小數表示法。現以 $(0,1)$ 爲例, 給定 $(0,1)$ 中的實數 a, 記 $N = \{0,1,2,3,4,5,6,7,8,9\}$, 現在想要將 a 改用小數點的方式註記, 方法如下:

(1) 將 $(0,1)$ 分成十等份, 由三一律告知 $\frac{a_1}{10} \le a < \frac{a_1}{10} + \frac{1}{10}$, 其中 $a_1 \in N$, 則 a_1 是 a 的小數點第一位。

(2) 將 $[\frac{a_1}{10}, \frac{a_1}{10} + \frac{1}{10})$ 再分成十等份, 則三一律告知 $\frac{a_1}{10} + \frac{a_2}{10^2} \le a < \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{1}{10^2}$, 其中 $a_2 \in N$, 則 a_2 是 a 的小數點第二位。

(3) 依上述原則, 將 $\left[\sum\limits_{k=1}^{n} \frac{a_k}{10^k}, \sum\limits_{k=1}^{n} \frac{a_k}{10^k} + \frac{1}{10^n}\right)$ 再分成十等份, 由三一律告知

$$\sum_{k=1}^{n} \frac{a_k}{10^k} + \frac{a_{n+1}}{10^{n+1}} \le a < \sum_{k=1}^{n} \frac{a_k}{10^k} + \frac{a_{n+1}}{10^{n+1}} + \frac{1}{10^{n+1}},$$

其中 $a_{n+1} \in N$, 則 a_{n+1} 是 a 的小數點第 $n+1$ 位。

(4) 由上述原則可將 $a \in (0,1)$ 對應到一個小數表示法: $0.a_1\, a_2\, a_3\, \ldots\, a_n\, a_{n+1}, \ldots$。

對於微積分課學得還不錯的同學, 可能會突然想到一件事: 印象中有好像有多個小數表示法代表同一個實數, 比方說從 $0.\bar{9} = 1$ 的經驗可推知 $0.4\bar{9} = 0.5\bar{0}$。但是上述將實數指定至一種小數表示法與這個無關。此外, 會有多種表示法的情形是出現在那個小數在某一位之後全部都是 9 的情況才會發生, 等一下的討論我們會避免使用 9 這個數字。

例 **11.** $(0,1)$ 區間中的實數集不可數。

證明: 利用反證法。假設 $(0,1)$ 區間中的實數集是可數的, 也就是存在一對一且映成的映射 $f : \mathbb{N} \to (0,1)$, 我們把這個對應關係寫出來:

$$\begin{aligned}
f(1) &= 0.\, a_{11}\, a_{12}\, a_{13} \ldots a_{1n} \ldots \\
f(2) &= 0.\, a_{21}\, a_{22}\, a_{23} \ldots a_{2n} \ldots \\
f(3) &= 0.\, a_{31}\, a_{32}\, a_{33} \ldots a_{3n} \ldots \\
\vdots & \qquad\quad \vdots \\
f(n) &= 0.\, a_{n1}\, a_{n2}\, a_{n3} \ldots a_{nn} \ldots \\
\vdots & \qquad\quad \vdots
\end{aligned}$$

其中 $a_{ij} \in N = \{0,1,2,3,4,5,6,7,8,9\}$ 間的數字。

考慮以下小數: $r = 0.r_1\,r_2\,r_3\ldots r_n\ldots$, 其中

$$r_i = \begin{cases} 4 & \text{如果 } a_{ii} \neq 4 \\ 7 & \text{如果 } a_{ii} = 4, \end{cases}$$

則 r 爲 $(0,1)$ 中的一個實數, 而對所有 $i \in \mathbb{N}$, $r \neq f(i)$, 得到 r 無法和自然數有一對一的對應關係。所以 $(0,1)$ 區間中的實數集是不可數的。 □

例 **12.** $[0,1]$ 中的實數與 $[0,2]$ 中的實數有一樣多的基數。

解**.** 考慮 $f:[0,1]\to[0,2]$ 爲 $f(x) = 2-2x$。

(a) 若 $x_1, x_2 \in [0,1], x_1 \neq x_2$, 則 $(2-2x_1)-(2-2x_2) = -2(x_1-x_2) \neq 0$, 所以 f 是一對一映射。

(b) 對所有 $y \in [0,2]$, 取 $x = \frac{2-y}{2} \in \mathbb{R}$, 而且 $0 \leq \frac{2-y}{2} \leq 1$, 所以 f 是映成的。

因此 $[0,1] \sim [0,2]$。