1

實數系的建構與性質

微積分的起源約莫於十七世紀後半期, 由英國物理學家、數學家牛頓 (I. Newton, 1643–1727) 與德國哲學家、數學家萊布尼茲 (G. W. Leibniz, 1646–1716) 各自建立了微積分的計算系統, 而在那個年代的科學家們也已經會用微積分的方式描述並推演, 將很多自然界的現象包括物理、天文等進行深入地探討與認識。

wIBHMjqgbSk

雖然微積分在那時候就已彰顯出強大的威力並回答各式物理與天文上的問題, 但是這當中的數學邏輯論述上存在著很多有待澄清的地方。特別是關於「無窮 — 無窮大或無窮小」的概念總是以一種似懂非懂的方式進行闡述, 這引起了人們長達一個多世紀的爭論, 而這件事在數學上引發了第二次的數學危機。直到十九世紀初, 柯西 (A. L. Cauchy, 1789–1857) 及魏爾斯特拉斯 (K. Weierstrass, 1815–1897) 等人替極限理論做進一步詮釋下才將微積分奠定了更穩固的基礎。又過了半個世紀, 康托 (G. 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, 也就是必須對實數要有一個清楚的認識, 於是當實數的完備性建立之後, 當初有待澄清的問題才得以完全解決。

而實數的完備性 (completeness of the real numbers) 到底是什麼樣的概念呢? 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或是數論的課程中已經學到相關的理論, 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。

這一章的內容編排如下: 單元 1.1 將簡介有理數的系統, 當中會說明體 (field) 還有全序 (totally order) 的概念, 這兩個概念及其運算規則會在單元 1.2 介紹的實數完備性中經常使用, 至於實數的完備性, 這裡採用戴德金切割法 (Dedekind cut method) 進行建構並給予完整論述。單元 1.3 相較於前一單元來說較爲獨立, 我們將用基數 (cardinality) 的方式討論一個集合的元素個數, 並引出可數集 (countable set) 與不可數集 (uncountable set) 這兩個概念。從這個面向出發, 也可以區分有理數集與實數集的差別。

這裡附帶一提的是, 關於實數完備性的理論, 在數學歷史上已經建立非常多互相等價的敘述, 這些敘述都各有特色, 而且也影響著數學分析在不同面向的發展, 而我們會在第 3 章重新回到實數完備性的課題進一步探討這個理論。

1.1 有理數的基本性質

PIQWOW1FpWE

考慮 有理數 (rational numbers) 所成的集合 $\mathbb{Q}=\{\frac{p}{q}|p,q\in\mathbb{Z},q\neq 0\}$, 以下列出有理數集的基本運算規則:

(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:

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

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

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

($\mathrm{F}_{+\mathrm{Iv}}$) *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 $a+(-a)=(-a)+a=0$。

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

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

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

($\mathrm{F}_{\cdot\mathrm{Iv}}$) *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 $a\cdot a^{-1}=a^{-1}\cdot a=1$。

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

z2eq3kK6hUk

(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 $a\leq b$ 或者是 $b\geq a$ 表示 a 小於 b 或 a 等於 b。

這裡註記兩件事: 由於 $\mathbb{Q}$ 是將兩個整數相除且分母非零所形成的數字收集起來, 有些元素是被視爲相同的, 比方說 $\frac{1}{2}=\frac{2}{4}=\frac{3}{6}=\cdots$。一般來說, 若 $p_1,p_2,q_1,q_2\in\mathbb{Z},q_1\neq 0,q_2\neq 0$, 則 $\frac{p_1}{q_1}=\frac{p_2}{q_2}$ 等價於 $p_1q_2=p_2q_1$。此外, 若 $r\in\mathbb{Q},r\neq 0$, 那麼我們可以透過質因數分解的原理, 對於有理數有多種表達之情形, 可以找到 p,q 是非零且 *互質* (coprime) $(p,q)=1$ 的整數使得 $r=\frac{p}{q}$。

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) 課程中應以最自然的方式感受並順勢使用, 不應刻意地去背誦之; 也就是說, 此時我們會把上述規則視爲已知而直接使用, 就像各位在中學階段處理數字的運算時, 除了某些關鍵步驟會仔細解釋其原理外, 我們並不會一直強調每一步到底用到了什麼規則, 而我們所關心的重點將放在其它地方 (例如實數完備性的意義)。但是如果你是在代數學 (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 (structure), 於是就必須花時間逐一理解每一個規則代表的意義, 甚至要對各種規則進行比較, 所以在代數課當中勢必要花時間把每個條文都確實地記起來。

舉例來說, 有一個經常使用的不等式規則是: 若 $a, b, c \in \mathbb{Q}, a < b, 0 < c$, 則 $a \cdot c < b \cdot c$ (這裡由於我們還沒有建構出實數, 故以有理數的層級討論), 若你把這件事和上面的有理數運算規則對照, 並沒有找到這一個結果。然而, 這個結果是將上面的規則進行複合式討論, 經逐步拆解則爲下面論述:

- 因爲 $a < b$, 所以用加法的保序性對於不等式兩邊加上 $-a$ 得到 $a + (-a) < b + (-a)$, 又由加法反元素的性質得知 $0 < b + (-a)$。

- 因爲 $0 < b + (-a)$ 且 $0 < c$, 所以由乘法對正有理數的保序性知 $0 < (b + (-a)) \cdot c$, 再由乘法的交換律還有乘法對加法的分配律得知 $0 < c \cdot (b + (-a)) = c \cdot b + c \cdot (-a)$。

- 根據加法的保序性, 對上述不等式兩邊加上 $c \cdot a$, 再由加法反元素的性質得知 $c \cdot a < c \cdot b$, 最後由乘法的交換律得到 $a \cdot c < b \cdot c$。

上述將每一個步驟都拆解的過程會在代數上必須仔細討論, 但我們現在不需要做這件事, 因爲分析課程的重點在於極限還有其它重要觀念必須認識, 若執意這麼做會沒完沒了, 然後在這個學科中失焦, 無法進入分析課程中最深刻的意涵。所以我們就從習以爲常的運算規則直接拿來使用即可。

在此簡要補充前述規則在代數學上使用的術語: 滿足 **(F)** 所有性質的集合稱爲 *體* (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); 若一個集合同時滿足 **(F)** 與 **(O)** 的所有條件, 則稱之爲 *有序體* (totally-ordered field)。所以有理數是一個有序體, 而我們會把 $(\mathbb{Q}, +, \cdot, <)$ 整體稱爲 *有理數系* (rational number system)。

以下指出一個有理數系 $(\mathbb{Q}, +, \cdot, <)$ 的性質:

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

證明: 若 $x, y \in \mathbb{Q}$, 假設 $x < y$, 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 戴德金切割與實數的完備性

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, 它不像正整數集 $\mathbb{N}$ 就是 $\{1, 2, 3, \ldots\}$、整數集 $\mathbb{Z}$ 就是由正整數集與 0 還有正整數取負號全部收集而成的集合、有理數集 $\mathbb{Q}$ 就是包含了所有兩整數相除的形式之元素那樣, 它們都有很明確的表達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。

-NJQEkDMc40

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解釋清楚。」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, 把正整數與整數的討論完全推卸給數學導論或數論老師), 這就是導致你對很多數學觀念一知半解的原因。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, 前一單元我們只是對有理數系 $(\mathbb{Q},+,\cdot,<)$ 有了初步認識, 關於有理數集 $\mathbb{Q}$, 它不僅僅是那些可以寫成 $\frac{p}{q}$, 其中 $p,q\in\mathbb{Z},q\neq 0$ 的數字所成的集合而已, 實際上有理數集還賦予了加法 $+$、乘法 $\cdot$ 還有全序 $<$ 的結構。現在我們要繼續對有理數系進一步討論以建立實數系。

在歷史上, 有很多理論都可以建立實數系, 比方說一些教科書中會看到作者用十進位小數的方法鋪陳實數系, 而這份講義則是採用 *戴德金切割法* (Dedekind cut method) 建構實數。戴德金切割法的特色是以有理數系爲基礎, 然後只利用集合與邏輯的語言論述, 所以用這種最基礎的語句呈現理論的時候, 想法單純而且清楚, 只是在最後的建構過程中, 由於一直把概念往上堆疊的情況下所以會顯得有一點冗長, 但整體而言, 戴德金的這套理論仍然是最爲人推崇。

戴德金所建構的實數完備性理論, 第一步是引進有理數集的切割, 現給出切割的定義:

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 $\mathbb{Q}$ 當中的一個子集合 Q 並且滿足以下三個條件:

(A) 集合 $Q\neq\emptyset$, 而且 $Q\neq\mathbb{Q}$。

(B) 若 $r\in Q$, 則對所有 $r'\in\mathbb{Q}$ 且 $r'<r$, 都有 $r'\in Q$。

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

因爲有理數集 $\mathbb{Q}$ 具有 $<$ 運算且滿足全序關係, 所以我們會把有理數想成是許許多多的點分佈在一個數軸上, 利用左右類比於兩個有理數誰比較小誰比較大。關於有理數集切割的三個條件, 基本上可以想像成這些散佈在數軸上有理數一刀切 (cut) 成左、右兩半, 條件 (A) 要形容的是必須把有理數集分成兩部份, 條件 (B) 要說的是切割這個集合想要選取的是左邊的集合。至於條件 (C) 就顯得非常微妙, 實際上它就是攸關實數完備性的深刻概念, 各位在看往後的內容時, 應好好體會條件 (C) 的意義。

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

pqS3umc24cM

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

證明:

(A) 因爲 $0\in\mathbb{Q},0<1$, 所以 $0\in Q$, 得到 $Q\neq\emptyset$; 因爲 $2\in\mathbb{Q},2>1$, 所以 $2\notin Q$, 因此 $Q\neq\mathbb{Q}$。

(B) 若 $r\in Q$, 則 $r\in\mathbb{Q}$ 且 $r<1$。對所有 $r'\in\mathbb{Q}$ 滿足 $r'<r$, 因爲 $r'<r<1$, 所以 $r'\in Q$。

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

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

C-lnxeDn_0k

證明:

(A) 因爲 $0\in\mathbb{Q},0\leq 0$, 所以 $0\in Q$, 得到 $Q\neq\emptyset$; 因爲 $2\in\mathbb{Q},2>0$ 且 $2^2=4>2$, 所以 $2\notin Q$, 於是 $Q\neq\mathbb{Q}$。

(B) 若 $r\in Q$, 對所有 $r'\in\mathbb{Q}$ 滿足 $r'<r$, 如果 $r'\leq 0$, 則 $r'\in Q$; 如果 $r'>0$, 因爲 $(r')^2<r^2<2$, 所以 $r'\in Q$。

(C) 對於 $r\in Q$, 若 $r\leq 0$, 取 $r''=1\in\mathbb{Q}$, 則 $r''=1>0\geq r$ 且 $(r'')^2=1<2$, 所以 $r''\in Q$ 且 $r<r''$; 若 $r>0$, 考慮 $r''=r-\frac{r^2-2}{r+2}\in\mathbb{Q}$, 因爲 $r^2-2<0$, 所以 $-\frac{r^2-2}{r+2}>0$, 於是 $r<r''$。此外, 因爲 $r''>r>0$, 計算
$$(r'')^2-2=\left(\frac{2r+2}{r+2}\right)^2-2=\frac{4r^2+8r+4-2(r^2+4r+4)}{(r+2)^2}=\frac{2(r^2-2)}{(r+2)^2},$$
因爲 $r^2<2$, 所以 $(r'')^2-2<0$, 得到 $(r'')^2<2$, 因此 $r''\in Q$。

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

上述兩個例子都是有理數集 $\mathbb{Q}$ 的切割, 但是這兩個切割有什麼主要差異呢? 爲說明這關鍵性的差異, 我們需要引進以下兩組定義。

定義 **4** (上界; 下界)**.** 給定一個有序集 S, 而有另一個集合 $E\subset S$,

zQ99Igzku-4

(A) 若存在 $C\in S$ 使得對所有 $x\in E$ 都滿足 $x\leq C$, 則稱集合 E 是 *有上界的* (bounded above), 此時 C 稱爲集合 E 的一個 *上界* (upper bound)。

(B) 若存在 $c\in S$ 使得對所有 $x\in E$ 都滿足 $c\leq x$, 則稱集合 E 是 *有下界的* (bounded below), 此時 c 稱爲集合 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, 而有另一個集合 $E\subset S$,

(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 $x\in E$ 都有 $x\leq M$。 (M 是 E 的一個上界)

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

一個集合 E 的最小上界我們會用記號 $\sup E$ 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 $x\in E$ 都有 $m\leq x$。 (m 是 E 的一個下界)

(2) 對所有 $m'\in S$ 滿足 $m<m'$, 存在 $x'\in E$ 使得 $x'<m'$。 (任何在 S 中大於 m 的數都不是 E 的下界)

一個集合 E 的最大下界我們會用記號 $\inf E$ 表示。

特別注意的是: 這兩組定義中的 C, c, M, m 都是在有序集 S 內找尋滿足條件的元素。而且有關最小上界與最大下界的第二個條件當中, M' 與 m' 也是有序集 S 當中的元素; 換言之, 各位在認識這兩組定義時, 必須體會到原始的設定一定會有一個大的有序集 S 還有一個它的子集合 E, 然後關於集合 E 的上界、下界、最小上界、最大下界都是在大的有序集 S 上找到滿足條件的元素。

以下先指出最小上界與最大下界的一個性質:

E5pk3UWbQ4I

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 $M_1, M_2 \in S$ 都是集合 E 的最小上界。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 $M_1 < x'$, 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 $M_2 < x'$, 則 M_2 不是 E 的上界, 於是 $M_2 < M_1$ 不對。因此, 由三一律 (trichotomy law) 得知 $M_1 = M_2$。

至於最大下界若存在則唯一的討論也是類似的, 在此也一併說明: 假設 $m_1, m_2 \in S$ 都是集合 E 的最大下界。如果 $m_1 < m_2$, 那麼從 m_1 是最大下界的意義來看, 存在 $x' \in E$ 使得 $x' < m_2$, 則 m_2 不是 E 的下界, 於是 $m_1 < m_2$ 不對。同樣地, 如果 $m_2 < m_1$, 那麼從 m_2 是最大下界的意義來看, 存在 $x' \in E$ 使得 $x' < m_1$, 則 m_1 不是 E 的下界, 於是 $m_2 < m_1$ 不對。因此, 由三一律 (trichotomy law) 得知 $m_1 = m_2$。 □

現在我們要從集合最小上界的觀點說明 例 **2** 與 例 **3** 中關於有理數集的切割在有理數集合中之最主要差異。

padcYBwDdiE

例 **7.**

(A) 考慮有理數集 $\mathbb{Q}$ 的切割 $Q = \{r \in \mathbb{Q} | r < 1\}$, 則 Q 的最小上界在 $\mathbb{Q}$ 中存在。

(B) 考慮有理數集 $\mathbb{Q}$ 的切割 $Q = \{r \in \mathbb{Q} | r \leq 0\} \cup \{r \in \mathbb{Q} | r > 0, r^2 < 2\}$, 則 Q 的最小上界在 $\mathbb{Q}$ 中不存在。

證明:

(A) 證明 $\underline{1 \in \mathbb{Q}\text{ 是 }Q\text{ 的最小上界}}$: 因爲對所有 $r \in Q$ 都滿足 $r < 1$, 所以 1 是 Q 的一個上界。對任何 $M' \in \mathbb{Q}$ 滿足 $M' < 1$, 考慮 $r' = \frac{M'+1}{2} \in \mathbb{Q}$, 則 $r' = \frac{M'+1}{2} < \frac{1+1}{2} = 1$, 所以 $r' \in Q$; 此外, $M' = \frac{M'+M'}{2} < \frac{M'+1}{2} = r'$, 所以 M' 不是 Q 的上界。因此 1 是 Q 的最小上界。

wztQAn8Yfr4

(B) 首先證明$\underline{\text{滿足 }r^2 > 2\text{ 的正有理數都不是 }Q\text{ 的最小上界}}$: 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 $(r')^2 > 2$。上面的討論告知: 對任何滿足 $r^2 > 2$ 的正有理數, 存在正的有理數 r' 使得 $r > r'$ 以及 $(r')^2 > 2$, 所以在 r' 與 r 之間並沒有 Q 的元素, 這件事與 r 是 Q 的最小上界矛盾。故 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 $p=2m,m\in\mathbb{N}$, 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, 因爲 Q 是有理數集的切割, 由切割的條件得知: 集合 Q 內的元素都不是 Q 的最小上界。因此 Q 的最小上界在 $\mathbb{Q}$ 中不存在。

$\square$

經過上面的分析, 我們會說切割 $Q=\{r\in\mathbb{Q}|r<1\}$ 定義了一個有理數 1; 換言之, 我們把切割 $Q=\{r\in\mathbb{Q}|r<1\}$ 與有理數 1 對應; 而對於切割 $Q=\{r\in\mathbb{Q}|r\le 0\}\cup\{r\in\mathbb{Q}|r>0,r^2<2\}$ 而言, 因爲它無法在 $\mathbb{Q}$ 中找到最小上界, 於是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, 就如各位在國中或高中數學課程中學到的概念, 我們將它記成 $\sqrt{2}$。

K4heLbRkn0w

於是我們利用有理數集切割的最小上界之想法定義實數集:

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

這裡再次解釋上述的想法: 現考慮任何一個有理數集 $\mathbb{Q}$ 的切割 Q, 如果 Q 的最小上界可以在 $\mathbb{Q}$ 當中找到, 則切割 Q 定義了一個有理數; 如果 Q 的最小上界無法在 $\mathbb{Q}$ 當中找到, 則切割 Q 定義了一個無理數; 這時我們硬是用一個符號 (數字) 表示這個切割 Q, 然後將所有的有理數與所有新定義的符號 (數字) 全部收集起來, 稱之爲實數集 $\mathbb{R}$。

於是, 當我們把有理數集的切割放到實數集這個更大的框架中, 就得到如下敘述:

任何一個有理數集 $\mathbb{Q}$ 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) 單元 1.1 的 *定理* **1** 是在說明有理數的稠密性: 任兩個不相等的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。而這一單元到目前爲止試圖說明的是: 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, 也就是在探討有理數集的切割之最小上界的概念時在有理數集當中找不到的缺失, 希望將它補足。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, 則會形成一條「完整無縫隙的數線」, 也就可以和各位在中學時學到實數與數線上的點有完全的對應之概念連繫。

x1e_MIPWOqU

(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 $\mathbb{Q}$ 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可以在實數集中找到。

到目前爲止, 我們只對實數集 $\mathbb{R}$ 有了最初步認識; 也就是說, 至此只說明了實數集 $\mathbb{R}$ 裡面的元素有哪些。對於實數集 $\mathbb{R}$ 上的某個元素 α, 我們的認知是把它理解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。接下來要做的事情是: 在實數集 $\mathbb{R}$ 上我們可以定義加法 $+$、乘法 $\cdot$、以及全序 $<$ 的概念, 並且檢視 **(F)** 與 **(O)** 的所有性質。這麼一來, 就能得知實數集搭配加法、乘法、全序關係 $(\mathbb{R},+,\cdot,<)$ 是一個有序體 (totally-ordered field)。

在建立完有序體之後, 我們還要重新定義實數集的切割, 並追問實數集切割的最小上界, 由此引進實數完備性 — 實數集切割的最小上界在實數集中的存在性, 記成公理 (D) — 將它納入實數集合中使得 $(\mathbb{R},+,\cdot,<,(\mathtt{D}))$ 是一個完備的有序體, 這才是實數系 (real number system) 的完整結構。

以下幾頁的篇幅試圖將戴德金切割理論中如何建構出有序體的所有步驟都證明清楚, 有鑑於其它文獻與教科書中雖有介紹但是並沒有把過程都仔細地證明下, 這裡寫出完整的內容, 不僅可以提供學習者一個參考資料, 實際上這些內容中有一些不是那麼顯而易見的討論也值得深思。但這裡也要注意到, 關於實數集是有序體的建構只是爲了理論完整起見而寫下, 它在整個分析的理論中並非最主要的重點, 各位應該多花心思在實數完備性的部份。另一個註記是: 現在要建構的是實數的有序體, 所以下面的篇幅都以 $<$ 表示, 並不把 $>$ 的符號拿來混合使用, 雖然有許多地方改用 $>$ 的方式去體會比較有感覺。

CgyMOHWrZRc

(O) 首先定義兩實數 $\alpha,\beta\in\mathbb{R}$ 的大小關係 $\alpha<\beta$ 爲: $Q_\alpha \subsetneqq Q_\beta$。現證明性質 (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 $b<a$, 因爲 $a\in Q_\alpha$, 所以 $b\in Q_\alpha$, 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 $\alpha<\gamma$。

4zpSqdiUAB8

(F) 給定 $\alpha,\beta\in\mathbb{R}$, 因爲 α 與 β 分別對應到有理數集的一種切割 Q_α 與 Q_β, 現將 $\alpha+\beta$ 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 $a\in Q_\alpha, b\in Q_\beta$, 則 $a+b\in Q_{\alpha+\beta}$, 所以 $Q_{\alpha+\beta}\neq\emptyset$。取 $a'\notin Q_\alpha, b'\notin Q_\beta$, 則 $a'+b'\notin Q_{\alpha+\beta}$, 所以 $Q_{\alpha+\beta}\neq\mathbb{Q}$。

關於 $a'+b'\notin Q_{\alpha+\beta}$, 應該要仔細驗證的是: $a'+b'$ 無法重新分解成 $a+b$ 的形式, 其中 $a\in Q_\alpha, b\in Q_\beta$。理由是: 考慮 $a'+b'=(a'+c)+(b'-c)$, 其中 $c\in\mathbb{Q}$, 這是所有可能的拆解法, 如果 $0<c$, 因爲 $a'\notin Q_\alpha$, 所以 $a'+c\notin Q_\alpha$; 如果 $c=0$, 則 $a'+b'\notin Q_{\alpha+\beta}$; 如果 $c<0$, 因爲 $b'\notin Q_\beta$, 所以 $b'-c\notin Q_\beta$。因此 $a'+b'$ 無論如何都無法分解成 $a+b$ 的形式, 其中 $a\in Q_\alpha, b\in Q_\beta$。

(B) 若 $r\in Q_{\alpha+\beta}$, 則 $r=a+b$, 其中 $a\in Q_\alpha, b\in Q_\beta$, 對所有 $r'\in\mathbb{Q}, r'<r$, 則 $r'-b<a$, 所以 $r'-b\in Q_\alpha$, 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 $Q_{\alpha+\beta}$ 是有理數集的一種切割。

定義完實數集 $\mathbb{R}$ 上的加法之後, 以下要驗證實數集上的加法規則:

mMvOwxGMuP8

($\mathrm{F}_{+\mathrm{C}}$) 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

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

  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 $r \in Q_{\alpha+0}$, 則 $r = a + b$, 其中 $a \in Q_\alpha, b \in Q_0$, 因爲 $a + b < a$, 所以 $a + b \in Q_\alpha$, 得到 $Q_{\alpha+0} \subset Q_\alpha$。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 $\alpha + 0 = 0 + \alpha = \alpha$。

($\mathrm{F}_{+\mathrm{Iv}}$) 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。

l5zcVrPbDsE

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

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

  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 $b = -a' - 1 \in \mathbb{Q}$, 則 $-b - 1 = a' \notin Q_\alpha$ 得到 $b \in Q_\beta$, 因此 $Q_\beta \neq \emptyset$。取 $a \in Q_\alpha$, 因爲所有 $r \in \mathbb{Q}, 0 < r$ 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 $r \in \mathbb{Q}, 0 < r$ 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 $r \in \mathbb{Q}, 0 < r$ 使得 $-b - r \notin Q_\alpha$。取 $b'' = b + \frac{r}{2} \in \mathbb{Q}$, 則 $b < b''$, 而且 $-b'' - \frac{r}{2} = -b - \frac{r}{2} - \frac{r}{2} = -b - r \notin Q_\alpha$, 因此 $b'' \in Q_\beta$。

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

- 再證 $\alpha + \beta = 0$: 若 $r \in Q_{\alpha+\beta}$, 則 $r = a + b$, 其中 $a \in Q_\alpha, b \in Q_\beta$, 因爲存在 $\tilde{r} \in \mathbb{Q}, 0 < \tilde{r}$ 使得 $-b - \tilde{r} \notin Q_\alpha$, 所以 $a < -b - \tilde{r}$, 得到 $r = a + b < -\tilde{r} < 0$, 所以 $r \in Q_0$, 因此 $Q_{\alpha+\beta} \subset Q_0$。另一方面, 若 $r \in Q_0$, 取 $r' = -\frac{r}{2}$, 則 $0 < r'$。存在 $k \in \mathbb{Z}$ 使得 $kr' \in Q_\alpha$ 且 $(k+1)r' \notin Q_\alpha$。令 $b = -(k+2)r'$, 因爲 $-b - r' = (k+1)r' \notin Q_\alpha$, 所以 $b \in Q_\beta$, 於是 $r = kr' + b \in Q_{\alpha+\beta}$, 因此 $Q_0 \subset Q_{\alpha+\beta}$。

  iINNmhu4XH8

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

Ky4YvxZztcg

(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 $Q_\alpha \subsetneqq Q_\beta$, 這意味著兩件事: 對任何 $a \in Q_\alpha$ 都有 $a \in Q_\beta$; 存在 $b \in Q_\beta$ 使得 $b \notin Q_\alpha$。對於 $\gamma \in \mathbb{R}$, 它對應於有理數的切割 Q_γ, 現考慮集合

$$Q_{\alpha+\gamma} = \{a + r | a \in Q_\alpha, r \in Q_\gamma\} \text{ 與 } Q_{\beta+\gamma} = \{b + r | b \in Q_\beta, r \in Q_\gamma\}。$$

證明: $\underline{Q_{\alpha+\gamma} \subset Q_{\beta+\gamma}}$。對所有 $x \in Q_{\alpha+\gamma}$, 則 $x = a + r$, 其中 $a \in Q_\alpha, r \in Q_\gamma$, 因爲 $a \in Q_\alpha$, 所以 $a \in Q_\beta$, 於是 $x = a + r \in Q_{\beta+\gamma}$, 因此 $Q_{\alpha+\gamma} \subset Q_{\beta+\gamma}$。
證明: $\underline{Q_{\alpha+\gamma} \neq Q_{\beta+\gamma}}$。已知存在 $b \in Q_\beta$ 使得 $b \notin Q_\alpha$, 因爲 Q_β 是一個切割, 所以存在 $b' \in Q_\beta$ 且 $b < b'$。記 $d = \frac{b'-b}{2} \in \mathbb{Q}$, 則 $0 < d$。對於 Q_γ, 存在 $k \in \mathbb{Z}$ 使得 $kd \in Q_\gamma$ 而 $(k+1)d \notin Q_\gamma$, 考慮 $y = b' + kd \in Q_{\beta+\gamma}$, 以下欲證明 $y \notin Q_{\alpha+\gamma}$: 考慮對於 y 的各種可能拆解法: $y = b' + kd = (b' - ld) + (k + l)d$, 其中 $l \in \mathbb{Q}$, 如果 $l < 0$, 因爲 $b \notin Q_\alpha$, 而 $b < b' < b' - ld$ 得到 $b' - ld \notin Q_\alpha$, 所以將 y 進行 $l < 0$ 的拆解下不可行; 如果 $0 \leq l < 1$, 因爲

$$b' - ld = b' - l\left(\frac{b' - b}{2}\right) = b + (b' - b)\left(1 - \frac{l}{2}\right),$$

得知 $b < b' - ld$, 因爲 $b \notin Q_\alpha$, 所以 $b' - ld \notin Q_\alpha$, 於是將 y 進行 $0 \leq l < 1$ 的拆解下也不可行; 如果 $1 \leq l$, 因爲 $(k+1)d \notin Q_\gamma$, 所以 $(k+l)d \notin Q_\gamma$。因此將 y 進行 $1 \leq l$ 的拆解下不可行; 由上述討論得知: $y \notin Q_{\alpha+\gamma}$。綜合上述討論, 我們得知 $Q_{\alpha+\gamma} \subsetneqq Q_{\beta+\gamma}$, 故 $\alpha + \gamma < \beta + \gamma$。

g4RdKmuMOBw

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

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

首先驗證 $Q_{\alpha\cdot\beta}$ 是有理數集 $\mathbb{Q}$ 的一個切割:

(A) 取 $q = 0 \in \mathbb{Q}$ 而且 $0 < a \cdot b$, 其中 $a \in Q_\alpha, 0 < a, b \in Q_\beta, 0 < b$, 所以 $q \in Q_{\alpha\cdot\beta}$, 因此 $Q_{\alpha\cdot\beta} \neq \emptyset$。存在 $a' \notin Q_\alpha, b' \notin Q_\beta$, 取 $q' = a' \cdot b' \in \mathbb{Q}$, 則對所有 $a \in Q_\alpha, 0 < a, b \in Q_\beta, 0 < b$, 都有 $0 < a \cdot b < a' \cdot b' = q'$, 所以 $q' \notin Q_{\alpha\cdot\beta}$, 因此 $Q_{\alpha\cdot\beta} \neq \mathbb{Q}$。

(B) 若 $q \in Q_{\alpha\cdot\beta}$, 對任何 $q' \in \mathbb{Q}, q' < q$, 遞移律告知 $q' < q < a \cdot b$, 其中 $a \in Q_\alpha, 0 < a, b \in Q_\beta, 0 < b$, 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 $a \in Q_\alpha, 0 < a, b \in Q_\beta, 0 < b$, 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 $q < q''$, 此外, 因爲 $q'' < a'' \cdot b''$, 其中 $a'' \in Q_\alpha, 0 < a'', b'' \in Q_\beta, 0 < b''$, 因此 $q'' \in Q_{\alpha\cdot\beta}$。

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

(O) 給出正實數集的乘法之後, 這裡可以先把 (O4) 證明完畢。 tVmCj1rp7Xo

(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 $a \in Q_\alpha, 0 < a, b \in Q_\beta, 0 < b$, 則 $r < 0 < a \cdot b$ 得知 $r \in Q_{\alpha\cdot\beta}$ 而且 $0 \notin Q_0$, 因此 $Q_0 \subsetneqq Q_{\alpha\cdot\beta}$, 即 $0 < \alpha \cdot \beta$。

(F) 再證乘法對於正實數集 $\mathbb{R}^+$ 的情況成立: SmkobCHsT_E

(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

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

(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 $c \in Q_{\alpha\cdot\beta}, 0 < c, r \in Q_\gamma, 0 < r$, 由此得到 $q < c \cdot r < a \cdot b \cdot r$, 其中 $a \in Q_\alpha, 0 < a, b \in Q_\beta, 0 < b, r \in Q_\gamma, 0 < r$; 記 $d = b \cdot r$, 因爲存在 $b'' \in Q_\beta$ 使得 $b < b''$ 以及 $r'' \in Q_\gamma$ 使得 $r < r''$, 所以 $d = b \cdot r < b'' \cdot r''$ 得知 $d \in Q_{\beta\cdot\gamma}$, 這麼一來, $q < a \cdot d$, 其中 $a \in Q_\alpha, 0 < a, d \in Q_{\beta\cdot\gamma}, 0 < d$, 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 $a \in Q_\alpha, 0 < a, d \in Q_{\beta\cdot\gamma}, 0 < d$, 由此得到 $q < a \cdot d < a \cdot b \cdot r$, 其中 $a \in Q_\alpha, 0 < a, b \in Q_\beta, 0 < b, r \in Q_\gamma, 0 < r$, 記 $c = a \cdot b$, 因爲存在 $a'' \in Q_\alpha$ 使得 $a < a''$ 以及 $b'' \in Q_\beta$ 使得 $b < b''$, 所以 $c = a \cdot b < a'' \cdot b''$ 得知 $c \in Q_{\alpha\cdot\beta}$, 這麼一來, $q < c \cdot r$, 其中 $c \in Q_{\alpha\cdot\beta}, 0 < c, r \in Q_\gamma, 0 < r$, 即 $q \in Q_{(\alpha\cdot\beta)\cdot\gamma}$。因此 $Q_{\alpha\cdot(\beta\cdot\gamma)} \subset Q_{(\alpha\cdot\beta)\cdot\gamma}$。

由上述討論可知 $Q_{(\alpha\cdot\beta)\cdot\gamma} = Q_{\alpha\cdot(\beta\cdot\gamma)}$, 即 $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$, 其中 $\alpha, \beta, \gamma \in \mathbb{R}^+$。

(F.$_\mathrm{Id}$) 乘法單位元素: 定義 $1 \in \mathbb{R}^+$ 是切割 $Q_1 = \{r \in \mathbb{Q} | r < 1\}$, 則對所有 $\alpha \in \mathbb{R}^+$, $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$。 gG4PUyDkpfY

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

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

得到 $q \in Q_{\alpha\cdot 1}$, 因此 $Q_\alpha \subset Q_{\alpha\cdot 1}$。

由上討論可知 $Q_{\alpha\cdot 1} = Q_{1\cdot\alpha} = Q_\alpha$。因此 $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$。

FABTBn-g3ho

GwkbRLobKUU

(F.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:

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

在這個記號下, 首先觀察集合 $A = \left\{ b \in \mathbb{Q} \,\middle|\, \text{存在 } r \in \mathbb{Q}, 0 < r \text{ 使得 } \frac{1}{b} - r \notin Q_\alpha \right\}$, 證明 $A \neq \emptyset$: 因爲 $\alpha \in \mathbb{R}^+$, 所以存在 $r' \in \mathbb{Q}$ 使得 $r' \notin Q_\alpha$, 由此得知 $0 < r'$, 任取 $r'' \in \mathbb{Q}$ 使得 $r' < r''$, 則 $r'' \notin Q_\alpha$。取 $\tilde{r} = r'' - r'$, 則 $\tilde{r} \in \mathbb{Q}$ 且 $0 < \tilde{r}$。因爲

$$\frac{1}{\frac{1}{r''}} - \tilde{r} = r'' - (r'' - r') = r' \notin Q_\alpha,$$

所以 $\frac{1}{r''} \in A$。因此 $A \neq \emptyset$。

接著要證明 Q_β 是有理數集 $\mathbb{Q}$ 的一個切割:

(A) 因爲 $0 \in \mathbb{Q}$ 且 $0 \in Q_\beta$, 所以 $Q_\beta \neq \emptyset$。取 $a \in Q_\alpha$ 且 $0 < a$, 則任何 $0 < r$ 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 $0 < b$ 的情況即可。因爲存在 $r \in \mathbb{Q}, 0 < r$ 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。此外, 因爲 $A \neq \emptyset$, 所以 $\beta \in \mathbb{R}^+$。

wWPtDHOKmpO

- 欲證明 $\alpha \cdot \beta = \beta \cdot \alpha = 1$: 若 $q \in Q_{\alpha\cdot\beta}$, 則 $q < a \cdot b$, 其中 $a \in Q_\alpha, 0 < a, b \in Q_\beta, 0 < b$, 因爲存在 $r \in \mathbb{Q}, 0 < r$ 使得 $\frac{1}{b} - r \notin Q_\alpha$, 而 $a \in Q_\alpha$, 得到 $a < \frac{1}{b} - r$, 於是 $q < a \cdot b < 1 - r \cdot b < 1$, 所以 $q \in Q_1$。因此 $Q_{\alpha\cdot\beta} \subset Q_1$。

另一方面, 欲證 $Q_1 \subset Q_{\alpha\cdot\beta}$, 先看 $Q_\alpha \subset Q_1$ 的情況, 而且以下的討論只需要看正有理數的情形即可。若 $0 < q < 1$, 則存在 $n \in \mathbb{N}$ 使得 $q^n \in Q_\alpha$ 而 $q^{n-1} \notin Q_\alpha$。

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

若 $\frac{1}{q^{n-1}} \notin Q_\beta$, 則對任何 $r \in \mathbb{Q}, 0 < r$, $q^{n-1} - r \in Q_\alpha$。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:

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

則

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

一方面 $q^n + q \cdot r''' = q'' \in Q_\alpha$; 至於 $\frac{1}{q^{n-1}+r'''}$, 取 $\frac{r'''}{2} \in \mathbb{Q}$, 則 $0 < \frac{r'''}{2}$, 且

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

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

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 $\frac{1}{q^n} \notin Q_\alpha$。

jyMcZCKAM9A

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

若 $q^n \notin Q_\beta$, 則對任何 $r \in \mathbb{Q}, 0 < r$ 都有 $\frac{1}{q^n} - r \in Q_\alpha$。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:

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

則

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

一方面,$q\left(\frac{1}{q^n} + r'''\right) = q'' \in Q_\alpha$。另一方面, 對於 $\frac{1}{\frac{1}{q^n}+r'''}$ 而言, 取 $\frac{r'''}{2} \in \mathbb{Q}$, 則 $0 < \frac{r'''}{2}$, 且

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

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

綜合所有討論得知 $Q_{\alpha\cdot\beta} = Q_{\beta\cdot\alpha} = Q_1$, 因此每個元素 $\alpha \in \mathbb{R}^+$ 都存在另一元素 $\beta \in \mathbb{R}^+$ 使得 $\alpha \cdot \beta = \beta \cdot \alpha = 1$。

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

Cr0sr8QZmRA

- 若 $q \in Q_{\alpha\cdot(\beta+\gamma)}$, 則 $q < a \cdot d$ 其中 $a \in Q_\alpha, 0 < a, d \in Q_{\beta+\gamma}, 0 < d$, 得到 $q < a \cdot (b + r) = a \cdot b + a \cdot r$ 其中 $a \in Q_\alpha, 0 < a, b \in Q_\beta, r \in Q_\gamma, 0 < b + r$。因爲 $0 < \beta, 0 < \gamma$, 所以可取到 $0 < b'', 0 < d''$ 使得 $b'' \in Q_\beta, d'' \in Q_\gamma$ 且 $q < a \cdot b'' + a \cdot r''$, 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 $q \in Q_{\alpha\cdot\beta+\alpha\cdot\gamma}$。於是 $Q_{\alpha\cdot(\beta+\gamma)} \subset Q_{\alpha\cdot\beta+\alpha\cdot\gamma}$。

  另一方面, 若 $q \in Q_{\alpha\cdot\beta+\alpha\cdot\gamma}$, 則 $q < c + d$ 其中 $c \in Q_{\alpha\cdot\beta}, 0 < c, d \in Q_{\alpha\cdot\gamma}, 0 < d$, 得到 $q < a' \cdot b + a'' \cdot r$ 其中 $a', a'' \in Q_\alpha, 0 < a', a'', b \in Q_\beta, 0 < b, r \in Q_\gamma, 0 < r$。取 $a = \max(a', a'')$, 則 $q < a \cdot b + a \cdot r = a \cdot (b + r)$ 其中 $a \in Q_\alpha, 0 < a, b + r \in Q_{\beta+\gamma}, 0 < b + r$, 所以 $q \in Q_{\alpha\cdot(\beta+\gamma)}$。於是 $Q_{\alpha\cdot\beta+\alpha\cdot\gamma} \subset Q_{\alpha\cdot(\beta+\gamma)}$。

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

現在要探討一般實數的乘法。首先, 對於 $\alpha \in \mathbb{R}$, 定義 $\alpha \cdot 0 = 0 \cdot \alpha = 0$; 至於其它情況, 記 $\mathbb{R}^- = \{\alpha \in \mathbb{R} | \alpha < 0\}$ 表示所有負實數所成的集合, 定義乘法如下:

L5oKOOMMeKO

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

現在要逐一驗證乘法規則在 $\mathbb{R}$ 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 $\alpha \cdot \beta = (-\alpha) \cdot (-\beta) = (-\beta) \cdot (-\alpha) = \beta \cdot \alpha$。

-EDotUKsaJI

($\mathrm{F}_{\cdot\mathrm{A}}$) 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 $(\alpha \cdot \beta) \cdot \gamma = ((-\alpha) \cdot (-\beta)) \cdot \gamma = -(((-\alpha) \cdot (-\beta)) \cdot (-\gamma)) = -((-\alpha) \cdot (-\beta) \cdot (-\gamma)) = -((-\alpha) \cdot ((-\beta) \cdot (-\gamma))) = -((-\alpha) \cdot (\beta \cdot \gamma)) = \alpha \cdot (\beta \cdot \gamma)$。

LYNQvrzGx74

($\mathrm{F}_{\cdot\mathrm{Id}}$) 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 $\alpha \cdot 1 = -((-\alpha) \cdot 1) = -(-\alpha) = \alpha$, 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

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

所以 $\alpha \cdot \beta = \beta \cdot \alpha = 1$。

($\mathrm{F}_{\cdot+\mathrm{D}}$) 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 $\alpha = 0$, 則 $\alpha \cdot (\beta + \gamma) = 0 = \alpha \cdot \beta + \alpha \cdot \gamma$。
若 $\beta = 0$, 則 $\alpha \cdot (\beta + \gamma) = \alpha \cdot \gamma = \alpha \cdot \beta + \alpha \cdot \gamma$。
至於 $\gamma = 0$ 的情況則可由前述 $\beta = 0$ 的證明過程搭配加法交換律可得。
- 若 $\beta + \gamma = 0$, 則 $\alpha \cdot (\beta + \gamma) = 0$。如果 $\alpha, \beta \in \mathbb{R}^+, \gamma \in \mathbb{R}^-$, 則 $\beta = -\gamma$, 而 $\alpha \cdot \beta + \alpha \cdot \gamma = \alpha \cdot \beta + (-(\alpha \cdot (-\gamma))) = \alpha \cdot \beta + (-(\alpha \cdot \beta)) = 0$。同理可得 $\alpha, \gamma \in \mathbb{R}^+, \beta \in \mathbb{R}^-$ 的情形。如果 $\alpha, \beta \in \mathbb{R}^-, \gamma \in \mathbb{R}^+$, 則 $\gamma = -\beta$, 而 $\alpha \cdot \beta + \alpha \cdot \gamma = (-\alpha) \cdot (-\beta) + (-((-\alpha) \cdot \gamma)) = (-\alpha) \cdot (-\beta) + (-((-\alpha) \cdot (-\beta))) = 0$。同理可得 $\alpha, \gamma \in \mathbb{R}^-, \beta \in \mathbb{R}^+$ 的情形。

- 若 $\alpha \in \mathbb{R}^+, \beta+\gamma \in \mathbb{R}^+$ 但是 $\beta \in \mathbb{R}^-$, 考慮 $\gamma = (\beta+\gamma)+(-\beta)$, 則 $\alpha\cdot\gamma = \alpha\cdot((\beta+\gamma)+(-\beta)) = \alpha\cdot(\beta+\gamma)+\alpha\cdot(-\beta) = \alpha\cdot(\beta+\gamma)+(-(\alpha\cdot\beta))$, 因此 $\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma$。
  至於 $\alpha \in \mathbb{R}^+, \beta+\gamma \in \mathbb{R}^+$ 但是 $\gamma \in \mathbb{R}^-$ 的情況同理。

STI6fT3-yaM

- 若 $\alpha \in \mathbb{R}^+, \beta+\gamma \in \mathbb{R}^-$ 但是 $\beta \in \mathbb{R}^+$, 則 $\alpha\cdot(\beta+\gamma) = -(\alpha\cdot(-(\beta+\gamma))) = -(\alpha\cdot((-\beta)+(-\gamma))) = -(\alpha\cdot(-\beta))+(-(\alpha\cdot(-\gamma))) = -(-(\alpha\cdot(-(-\beta))))+\alpha\cdot\gamma = \alpha\cdot\beta+\alpha\cdot\gamma$。
  上述的討論用到一件事: 對所有 $x, y \in \mathbb{R}$ 都有 $-(x+y) = (-x)+(-y)$, 這個結果的理由在於: 因爲 $(x+y)+(-y)+(-x) = x+(y+(-y))+(-x) = x+(-x) = 0$, 所以 $(-y)+(-x) = (-x)+(-y)$ 是 $x+y$ 的加法反元素。
  至於 $\alpha \in \mathbb{R}^+, \beta+\gamma \in \mathbb{R}^-$ 但是 $\gamma \in \mathbb{R}^+$ 的情況同理。
- 若 $\alpha \in \mathbb{R}^-, \beta+\gamma \in \mathbb{R}^+$ 但是 $\beta \in \mathbb{R}^-$, 則 $\alpha\cdot(\beta+\gamma) = -((-\alpha)\cdot(\beta+\gamma)) = -((-\alpha)\cdot\beta+(-\alpha)\cdot\gamma) = -((-\alpha)\cdot\beta)+(-((-\alpha)\cdot\gamma)) = -(-((-\alpha)\cdot(-\beta)))+\alpha\cdot\gamma = \alpha\cdot\beta+\alpha\cdot\gamma$。
  至於 $\alpha \in \mathbb{R}^-, \beta+\gamma \in \mathbb{R}^+$ 但是 $\gamma \in \mathbb{R}^-$ 的情況同理。
- 若 $\alpha \in \mathbb{R}^-, \beta+\gamma \in \mathbb{R}^-$ 但是 $\beta \in \mathbb{R}^+$, 則 $\alpha\cdot(\beta+\gamma) = (-\alpha)\cdot(-(\beta+\gamma)) = (-\alpha)\cdot((-\beta)+(-\gamma)) = (-\alpha)\cdot(-\beta)+(-\alpha)\cdot(-\gamma) = -((-\alpha)\cdot(-(-\beta)))+\alpha\cdot\gamma = -((-\alpha)\cdot\beta)+\alpha\cdot\gamma = \alpha\cdot\beta+\alpha\cdot\gamma$。
  至於 $\alpha \in \mathbb{R}^-, \beta+\gamma \in \mathbb{R}^-$ 但是 $\gamma \in \mathbb{R}^+$ 的情況同理。
- 若 $\alpha, \beta, \gamma \in \mathbb{R}^-$, 則 $\alpha\cdot(\beta+\gamma) = (-\alpha)\cdot(-(\beta+\gamma)) = (-\alpha)\cdot((-\beta)+(-\gamma)) = (-\alpha)\cdot(-\beta)+(-\alpha)\cdot(-\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma$。

綜合所有討論, 我們得到對所有 $\alpha, \beta, \gamma \in \mathbb{R}$, 都有 $\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma$。

至此我們已全部證明完實數集 $\mathbb{R}$ 關於有序體 **(F)** 與 **(O)** 的所有性質; 也就是說, 我們現在知道 $(\mathbb{R}, +, \cdot, <)$ 形成一個有序體, 但是目前依舊看不出有理數集 $\mathbb{Q}$ 與實數集 $\mathbb{R}$ 有什麼顯著的差異, 只知道實數集比有理數集來說多了許多叫做無理數的元素而已。爲了道出有理數集與實數集的差異, 我們想要再走一次類似於之前的過程, 以實數集合爲主體定義其切割還有它的最小上界並進行觀察。不過, 這裡需要先證明實數集的另一個性質, 也就是實數的稠密性。

定理 9 (實數的稠密性)**.** *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。*

eYP6iUJvk_U

證明: 給定 $\alpha, \beta \in \mathbb{R}$ 而且 $\alpha < \beta$, 因爲 α 與 β 分別對應於有理數的切割 Q_α 與 Q_β, 並且 $Q_\alpha \subsetneqq Q_\beta$, 所以存在有理數 $q \in Q_\beta$ 使得 $q \notin Q_\alpha$, 於是 $\alpha \le q < \beta$。注意到: 若 α 是有理數的話, $q = \alpha$ 等號可能成立, 但是 q 一定與 β 不相等, 否則它將違反有理數切割的定義。

如果 $q = \alpha$, 因爲 Q_β 是有理數集的切割, 所以存在 $q'' \in Q_\beta$ 且 $q < q''$, 於是 $\alpha = q < q'' < \beta$, 這時 q'' 即爲所求。 □

現在我們從實數集 $\mathbb{R}$ 出發, 定義實數集的切割。

定義 **10.** 實數集 $\mathbb{R}$ 的一個 *切割* (cut) 指的是實數集 $\mathbb{R}$ 的一個子集合 R 滿足以下三個條件:

(A) 集合 $R \neq \emptyset$, 而且 $R \neq \mathbb{R}$。

(B) 若 $x \in R$, 則對所有 $x' \in \mathbb{R}$ 且 $x' < x$, 都有 $x' \in R$。

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

Gg01cE3k-co

因爲實數集 $\mathbb{R}$ 上具有 $<$ 的運算因而形成有序集, 對於實數集合的切割 $R \subset \mathbb{R}$, 我們想要問 R 在 $\mathbb{R}$ 中的最小上界, 這時, 它還會像是有理數集切割的情況類似, 有時候實數集切割的最小上界在實數集中存在, 然後有時候實數集切割的最小上界在實數集中不存在呢? 假如這件事情發生的話, 那麼我們就還要再把集合擴充一次, 再證一次擴充後的集合是有序體, 然後再給出新的有序體之切割並討論其最小上界, 倘偌這件事持續發生的話, 會不會沒完沒了呢?

令人驚奇的是, 數學上可以證明: 實數集切割的最小上界在實數集合中必存在; 也就是說, 一定可以在實數集中找到對應的元素滿足實數集切割之最小上界的兩個條件, 此外, 根據 *定理* **6** 得知最小上界必唯一。如此關於最小上界的操作在實數集合中具有封閉性之意義下, 我們就不用再次擴充了。而這件事情稱爲 (D) 戴德金切割原理, 現陳述如下:

(D) *戴德金切割原理* (Dedekind Cut Principle)**.** 實數集 $\mathbb{R}$ 的任何一個切割 R 之最小上界在 $\mathbb{R}$ 中存在。此時, $\sup R = \sup(R \cap \mathbb{Q})$。

在證明戴德金切割原理之前, 先簡述整個證明的想法: 首先, 給定實數集的一個切割 R, 考慮集合 $Q = R \cap \mathbb{Q}$, 則可以證明集合 Q 是有理數集 $\mathbb{Q}$ 的切割, 所以根據之前討論, 關於 $\sup Q = \sup(R \cap \mathbb{Q})$ 在實數集 $\mathbb{R}$ 中存在。然後再證明關於實數集的切割 R 之最小上界 $\sup R$ 與 $\sup Q = \sup(R \cap \mathbb{Q})$ 兩者一致。

證明: 給定實數集的一個切割 R, 考慮集合 $Q = R \cap \mathbb{Q}$, 首先證明集合 Q 是有理數集 $\mathbb{Q}$ 的一個切割:

- 因爲 $R \neq \emptyset$, 所以存在 $x \in R$, 而且存在 $x'' \in R$ 使得 $x < x''$, 由實數的稠密性, 存在 $q \in \mathbb{Q}$ 使得 $x < q < x''$, 因爲 $x'' \in R$, 所以 $q \in R$, 於是 $q \in R \cap \mathbb{Q} = Q$, 因此 $Q \neq \emptyset$。存在 $x \notin R$, 對所有 $x' \in \mathbb{R}$ 滿足 $x < x'$, 都有 $x' \notin R$, 由實數的稠密性, 存在 $q \in \mathbb{Q}$ 使得 $x < q < x'$, 因爲 $x \notin R$, 所以 $q \notin R$, 於是 $q \notin R \cap \mathbb{Q} = Q$, 因此 $Q \neq \mathbb{Q}$。

- 若 $r \in Q$, 對所有 $r' \in \mathbb{Q}$ 且 $r' < r$, 因爲 $r \in R$, 而 $r' \in \mathbb{R}$ 且 $r' < r$, 得到 $r' \in R$, 因此 $r' \in R \cap \mathbb{Q} = Q$。

- 對所有 $r \in Q$, 因爲 $r \in R$, 所以存在 $x'' \in R$ 使得 $r < x''$, 由實數的稠密性, 存在 $r'' \in \mathbb{Q}$ 使得 $r < r'' < x''$。因爲 $x'' \in R$, 所以 $r'' \in R$, 因此 $r'' \in R \cap \mathbb{Q} = Q$, 於是存在 $r'' \in Q$ 滿足 $r < r''$。

由上述討論, 我們知道 $Q = R \cap \mathbb{Q}$ 是有理數集 $\mathbb{Q}$ 的一個切割, 所以 $\sup Q = \sup(R \cap \mathbb{Q}) = \alpha \in \mathbb{R}$ 存在。

接下來要證明的是: $\sup R = \alpha$。

- 證明: α 是集合 R 的一個上界: 假設存在 $x' \in R$ 使得 $\alpha < x'$, 由實數的稠密性, 存在 $q \in \mathbb{Q}$ 使得 $\alpha < q < x'$, 因為 $x' \in R$, 所以 $q \in R$, 於是 $q \in R \cap \mathbb{Q} = Q$, 得到 α 不是集合 Q 的一個上界, 這與 $\alpha = \sup Q$ 矛盾。因此 α 是集合 R 的一個上界。

- 證明: 對所有 $M' \in \mathbb{R}$ 滿足 $M' < \alpha$, 則 M' 不是集合 R 的上界: 給定 $M' \in \mathbb{R}$ 滿足 $M' < \alpha$, 由實數的稠密性得知: 存在 $q \in \mathbb{Q}$ 使得 $M' < q < \alpha$, 則 q 不是集合 Q 的上界, 所以存在 $q' \in Q = R \cap \mathbb{Q}$ 使得 $M' < q < q'$, 因為 $q' \in R$ 且 $M' < q'$, 這麼一來, M' 不是集合 R 的上界。

□

由上面的討論, 我們終於可以把實數系說明清楚並突顯它與有理數集的差異, 那就是:

_yUjc8twFxU

> *實數系* $(\mathbb{R}, +, \cdot, <, (\mathtt{D}))$ (real number system) 是一個滿足 (D) 戴德金切割原理的有序體。

為了後續的討論, 我們將 (D) 戴德金切割原理稱為 *實數的完備性公理* (the completeness axiom in real number system), 並且在這份講義中使用符號 (D) 表示。回顧這一個單元的討論, 我們利用戴德金提出的切割法將實數系建構完畢, 並且認識到對於實數集切割之最小上界一定可以在實數集合中找到唯一的元素滿足最小上界的條件。然而在往後數學分析的討論, 若是想要了解最小上界的問題, 然後就得將每一件事情都用戴德金切割原理的方式進行論述將會變得非常複雜, 這是因為光是要驗證一個集合是實數的切割就必須花時間仔細討論切割的三個條件, 在過往的經驗中便能體會到它並非易事; 又或者說, 當初在定義最小上界時, 只要對於一個有序集的子集合就可以問最小上界這個概念了, 所以由戴德金切割法得到的結果只是在那些實數集當中非常特殊的子集合(切割) 之情況下知道其最小上界存在, 對於一般的集合最小上界的存在性目前來說並不清楚。

所以我們現在想要了解的是: 一般集合的最小上界是否存在? 又該怎麼確定? 這會是一個很重要的問題, 因為這件事情若能解決的話, 則可以將理論化為實際, 也就是找到一個比戴德金切割原理還要容易操作的替代方案幫助我們進行各種運算及邏輯推演。而這個問題的答案是正面的, 以下要介紹的 (S) 確界原理 (Supremum Principle) 可對於任何非空有界集 (nonempty and bounded set) 討論最小上界與最大下界的概念, 甚至可以證明 (S) 確界原理與 (D) 戴德金切割原理兩者等價, 這麼一來, 我們可以把實數系 $(\mathbb{R}, +, \cdot, <, (\mathtt{D}))$ 替換成 $(\mathbb{R}, +, \cdot, <, (\mathtt{S}))$, 而在實數系統上利用確界原理的方式探討問題會更為實用及便利。

為闡述確界原理以及它和戴德金切割原理之間的關係, 我們需要先提出另一個觀念, 稱為最大元素與最小元素。

OMR64EINhZU

定義 **11** (最大元素; 最小元素)**.** 給定一個有序集合 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 *最大元素* (maximum element), 記為 $\max E = x$; 若有一個元素 $x' \in E$ 滿足對所有 $y \in E$ 都有 $y \geq x'$, 則稱 x' 是 E 的 *最小元素* (minimum element), 記為 $\min E = x'$。

這裡應注意的是: 若將上面的定義與 *定義* **4** 還有 *定義* **5** 相比, 最大元素或最小元素是在有序集合 E 當中尋找滿足條件的元素, 我們並沒有把它放到一個更大的有序集 S 尋找元素; 而最小上界或最大下界的概念, 必須要有 $E \subset S$ 的關係, 而且我們是在大的有序集 S 當中去檢查哪個元素滿足最小上界或最大下界的條件。

另一方面, 一個有序集合 E 的最大元素或最小元素不見得存在, 例如正整數集 $\mathbb{N}$ 並沒有最大元素, 但它有最小元素 1。這裡再舉一個例子: 考慮集合 $E = \{\frac{1}{n} | n \in \mathbb{N}\}$, 欲求 $\max E$ 與 $\min E$, 討論如下:

- 取 $n = 1$, 則 $\frac{1}{1} = 1$。對所有 $n \in \mathbb{N}$, 因爲 $n \geq 1$, 所以 $\frac{1}{n} \leq \frac{1}{1} = 1$, 所以 $\max E = 1$。
- 假設 $\min E = m$ 存在, 則存在 $n_0 \in \mathbb{N}$ 使得 $\frac{1}{n_0} = m$, 考慮 $n_0 + 1 \in \mathbb{N}$, 因爲 $n_0 + 1 > n_0$, 所以 $\frac{1}{n_0+1} < \frac{1}{n_0} = m$, 這與 m 是集合 E 的最小元素矛盾。故 $\min E$ 不存在。

0VdfKbbp0rs

現在我們要給出確界原理的敘述。

(S) *確界原理* (Supremum Principle)**.** *若一個非空的集合* $E \subset \mathbb{R}$ *有上界, 則有最小上界。*

以下兩個定理將闡明戴德金切割原理與確界原理互相等價。

定理 **12.** *實數集合中, 已知* (D) *戴德金切割原理, 則可推得* (S) *確界原理。*

證明: 若一個非空的集合 $E \subset \mathbb{R}$ 有上界, 現分兩種情形討論其最小上界的存在性:

(A) <u>若 E 有最大元素 M</u>, 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 $M' \in \mathbb{R}$ 必有 $M' < M$, 得到 M' 不是 E 的上界。因此 M 是 E 的最小上界。

(B) <u>若 E 沒有最大元素</u>, 以下將實數集 $\mathbb{R}$ 按照以下方法建立一種切割 R: 首先, 考慮集合

$$R' = \{M \in \mathbb{R} | \, M \text{ 是集合 } E \text{ 的上界}\},$$

然後記 $R = \mathbb{R} - R'$。

首先要驗證的是集合 R 是實數集 $\mathbb{R}$ 的一個切割:

- 任取 $x \in E$, 則 $x \in R$, 得到 $R \neq \emptyset$; 因爲 E 有上界, 所以 R' 非空, 得到 $R \neq \mathbb{R}$。
- 若 $x \in R$, 而 $x' \in \mathbb{R}$ 滿足 $x' < x$, 則 x' 不是 E 的上界, 因此 $x' \in R$。
- 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 中沒有最大元素告知 $x'' \notin R'$, 得到 $x'' \in R$。

由戴德金切割原理 (Dedekind Cut Principle) 知: 分割 R 確定了一個實數 α, 它是 R 的最小上界。以下證明 α 也是 E 的最小上界: 一來, 因爲 $E \subset R$, 而分割的意義得知 α 是 E 的上界。二來, 對所有 $M' \in \mathbb{R}$ 滿足 $M' < \alpha$, 存在 $x' \in R$ 使得 $M' < x'$, 而 x' 不是 E 的上界告知存在 $x'' \in E$ 使得 $x' < x''$, 得到 $M' < x''$ 其中 $x'' \in E$, 於是 α 是 E 的最小上界。

□

定理 13. 實數集合中, 已知 (S) 確界原理, 則可推得 (D) 戴德金切割原理。

vnV1WYK8Ihw

證明: 若 R 是實數集 $\mathbb{R}$ 的一個切割, 因爲 $R \neq \mathbb{R}$, 即存在 $y \in \mathbb{R}$ 使得對所有 $x \in R$ 都有 $x < y$, 所以 y 是集合 R 的一個上界, 由確界原理 (Supremum Principle) 得知: $\alpha = \sup R$ 在 $\mathbb{R}$ 中存在, 於是戴德金切割原理 (Dedekind Cut Principle) 成立。 □

由上面討論, 我們可將實數系改寫成以下敘述:

實數系 $(\mathbb{R}, +, \cdot, <, (\mathtt{S}))$ (real number system) 是一個滿足確界原理的有序體。

確界原理在此稱爲 (S) 實數的完備性公理。至此, 我們已完成「(D) 實數的完備性公理 $\Leftrightarrow$ (S) 實數的完備性公理」的論證。關於實數完備性的故事其實並沒有結束, 當我們進入第 2 章討論數列的極限後, 還會再引進更多的術語及觀念, 然後到第 3 章的時候, 我們會回過頭來重新認識實數的完備性公理, 屆時還會再引進幾個看似不同樣貌卻彼此等價的敘述並給予證明, 最後得知這些敘述都是實數的完備性公理的一個表述。

關於確界原理, 還有一件事情必須說明, 就是最小上界與最大下界其實是對等的觀念, 現說明如下:

定理 14. (S) 確界原理的敘述等價於「若一個非空的集合 $E \subset \mathbb{R}$ 有下界, 則有最大下界。」

EAUhLKkb-3c

證明: $(\Rightarrow)$ 給定非空集合 E, 考慮集合 $-E \overset{\text{定義}}{=\!=} \{-x | x \in E\}$, 因爲集合 E 非空, 所以集合 $-E$ 非空。因爲集合 E 有下界, 即存在 $m \in \mathbb{R}$ 使得對所有 $x \in E$ 都有 $x \geq m$; 得到對所有 $-x \in -E$ 都有 $-x \leq -m$, 所以集合 $-E$ 有一個上界 $-m$。由確界原理 (Supremum Principle) 得知 $\alpha \overset{\text{記}}{=} \sup(-E) \in \mathbb{R}$ 存在。以下證明: 實數 $-\alpha$ 是集合 E 的最大下界。

- 對所有 $x \in E$, 則 $-x \in -E$, 得到 $-x \leq \alpha$, 於是 $x \geq -\alpha$, 因此 $-\alpha$ 是集合 E 的下界。
- 對任意 $m' \in \mathbb{R}$ 滿足 $m' > -\alpha$, 則 $-m' < \alpha$, 所以 $-m'$ 不是集合 $-E$ 的上界, 故存在 $-x' \in -E$ 使得 $-m' < -x'$, 得到 $m' > x'$, 於是 m' 不是集合 E 的下界。

由上述討論得知 $-\alpha$ 是集合 E 的最大下界。

$(\Leftarrow)$ 給定非空集合 E, 考慮集合 $-E \overset{\text{定義}}{=\!=} \{-x | x \in E\}$, 因爲集合 E 非空, 所以集合 $-E$ 非空。因爲集合 E 有上界, 即存在 $M \in \mathbb{R}$ 使得對所有 $x \in E$ 都有 $x \leq M$; 得到對所有 $-x \in -E$ 都有 $-x \geq -M$, 所以集合 $-E$ 有一個下界 $-M$, 所以 $\beta \overset{\text{記}}{=} \inf(-E) \in \mathbb{R}$ 存在。以下證明: 實數 $-\beta$ 是集合 E 的最小上界。

- 對所有 $x \in E$, 則 $-x \in -E$, 得到 $-x \geq \beta$, 於是 $x \leq -\beta$, 因此 $-\beta$ 是集合 E 的上界。
- 對任意 $M' \in \mathbb{R}$ 滿足 $M' < -\beta$, 則 $-M' > \beta$, 所以 $-M'$ 不是集合 $-E$ 的下界, 故存在 $-x' \in -E$ 使得 $-x' < -M'$, 得到 $M' < x'$, 於是 M' 不是集合 E 的上界。

由上述討論得知 $-\beta$ 是集合 E 的最小上界。 □

一般來說, 當我們想用確界原理的等價敘述進行討論時, 此時仍然會把這個等價敘述稱爲確界原理 (Supremum Principle), 因爲它和原敘述在概念上是一樣的, 數學上有時就不會再給它新的名稱。當然, 如果你想要把這個等價敘述稱爲下確界原理 (Infimum Principle) 也是可以的。

經過上面討論, 各位可以看到的是: 一方面我們順利將實數完備性的敘述轉換成確界原理的敘述, 這樣可爲日後的分析帶來很大的便利, 因爲它告知任何非空有界的集合都可以得到其最小上界與最大下界。另一方面, 雖然戴德金切割原理日後就很少使用, 但它的功勞是不可抹滅的, 因爲由戴德金切割原理的建構, 我們可以看出實數關於有序體的代數結構, 還有實數與有理數之間的緊密關聯。

這個單元的最後想要介紹一個日後在技術層面上有時會用到的阿基米德性質。

c8XF0SPYjHU

定理 **15** (阿基米德性質, Archimedean 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 $\alpha = \sup E \in \mathbb{R}$。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 是 E 的最小上界這個性質矛盾。因此, 存在 $n \in \mathbb{N}$ 使得 $nx > y$。 □

關於阿基米德性質最常見的應用有以下兩個:

(A) $y \in \mathbb{R}$ 給定, 然後取 $x = 1$, 則存在 $n \in \mathbb{N}$ 使得 $nx > y \Rightarrow n > y$; 也就是說, 任給一個實數 y, 一定會有比 y 還要大的正整數 n。

(B) $x > 0$ 給定, 然後取 $y = 1$, 則存在 $n \in \mathbb{N}$ 使得 $nx > y \Rightarrow nx > 1 \Rightarrow 0 < \frac{1}{n} < x$; 也就是說, 任給一個正數 x, 在 0 和 x 之間一定會有一個長相是 $\frac{1}{n}$ 的有理數, 這個有理數的分子是 1, 分母是某個正整數 n。這裡要注意的是, 實數的稠密性本來就可以得知 0 和 x 之間必存在有理數, 而這裡可以得到是一個更特別的有理數。

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。

N1QwjOzLYOk

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多少的一個常用方法, 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手邊, 自己的鬥片盒放在右手邊, 然後左、右手同時抓取一個鬥片出來, 在不斷地抓取下, 結果會在某個狀態, 左手還可以再抓出一個鬥片但是右手無法再取出一個鬥片, 這時就知道左邊盒子的鬥片數是比較多的。

回到數學層面, 這個單元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」, 這裡特別注意, 我故意把迷思二字加上引號, 代表著若是根據之後所給出的數學定義進行判斷, 那麼以下的三個解釋有的結論錯誤, 有的結論雖然正確但是推論有誤。

(A) 因爲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) 因爲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) 因爲 $[0,2]$ 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。

如果想清楚上面三個論述, 就會知道這三個論述的觀點都是利用兩個集合之間的包含 $\subset$ 關係看待事情。透過集合的包含關係在某些情況的確可以描述元素個數多寡的關係, 但也不難發現有的時候兩個集合不見得會有包含的關係, 例如 $A=\{1,2\}$ 與 $B=\{2,3\}$ 彼此沒有包含的關係, 甚至集合 A 與集合 $C=\{4,5\}$ 的交集是空集合。在代數上, 我們會說集合搭配包含的關係 $\subset$ 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, 雖然兩集合並沒有一個包含於另一個的關係, 卻可以清楚地「計數」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 的元素個數「一樣多」。於是在數學上我們想要提出一個可以比較任兩個集合元素個數多寡之方法。

不曉得各位有沒有意識到剛才的三個問題比起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都沒有辦法好好地「算」個數, 就以正整數集合來說, 讓 $1,2,3,\ldots$ 依序地排列之下, 你是看不到正整數的盡頭, 而正整數看不到盡頭這件事若用數學的術語來說, 則是指正整數有 *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加困難。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 (先各別計算個數, 再說出數字比較大小) 處理之, 但是第二種方法產生了契機說明清楚。

這裡或許先提一件事情: 上述用集合包含的關係所得的論述與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:

(1) 因爲正偶數集包含於正整數集, 所以「正偶數集的個數沒有比正整數集來得多」。

(2) 因爲有理數集包含於實數集, 所以「有理數集的個數沒有比實數集來得多」。

(3) 因爲 $[0,1]$ 區間包含於 $[0,2]$ 區間, 所以「$[0,1]$ 中的實數個數沒有比 $[0,2]$ 中的實數多」。

換言之, 若要從集合包含的關係看上述這三組集合的元素個數時, 只能知道小集合的元素個數不會比大集合的元素個數來得多, 至於它們會被歸類成一樣多, 還是說小集合的元素個數會比大集合的元素個數少很多呢? 這時就要再繼續深究。

以下篇幅就要試圖好好地回答這三個問題。爲了解釋完整起見, 我們有必要把集合與映射相關的術語重新介紹一次。

hSAq3DhfHmU

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 都指定到集合 Y 當中一個元素 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)。

各位有時候會在某些文獻或書籍中看到作者把 $f : X \to Y$ 稱爲 *函數* (function)。一般來說, 若對應域 Y 並非實數集或複數集的時候, 通常會採用映射一詞形容 f, 而函數這個詞在多數情況會特別用來描述 $f : X \to \mathbb{R}$ 或是 $f : X \to \mathbb{C}$ 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)。

若要檢查一個映射是否爲一對一, 我們也可以用它的否逆命題檢查之; 也就是說, 假設 $f(x_1) = f(x_2)$, 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。

現在我們用能否在兩個集合之間建立一對一且映成的映射來定義兩個集合內的元素個數之多寡。

定義 **3.** 如果兩個非空集合 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)。

rcYu5W_zRHU

如果可以從 X 到 Y 建立一個映射, 因爲映射只是要求 X 中每一個的元素都必須指定 Y 裡面其中一個元素, 它並沒有給出這種指定有什麼額外的要求, 所以一個映射有可能產生在 X 中的兩個不同的元素都指定到 Y 當中的同一個元素。而這樣的映射對於目前想了解兩集合元素多寡的問題並沒有幫助, 因爲這種映射會把 X 中的「兩個」元素對應到 Y 中的「一個」元素, 就會產生在個數上無法對等的現象。

回想前面比較兩盒鬥片多少時使用的方法, 它是一個特別的映射, 因爲每一次動作都是左、右手各抓取一個鬥片, 一旦抓出來之後就擺在一起並放在一旁, 然後再用左、右手於盒中同時抓取一個鬥片, 所以不同的兩次動作所抓取到的鬥片也會不同, 這個現象將類推到我們想要建立的不僅是映射的關係, 而且還要是一對一的映射。

另一方面, 若我們只是建立了 $f : X \to Y$ 是一對一的映射之下, 得到的會是定義域中的元素都可以逐一對應到對應域中的元素; 也就是說, 我們完成了定義域 X 與其值域 $f(X) = R$ 之間的完全對應, 然而這時有可能 $R \subsetneq Y$, 透過 f 是映成的性質, 才可以把 Y 中的每個元素都與 X 中的元素建立對應關係。

當兩個集合有相同的基數時, 則可以驗證這是一種 等價關係 (equivalence relation), 此時會用記號 $X \sim Y$ 表示。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 $X \sim Z$。

現在花一點時間討論爲什麼「兩個集合有相同的基數」這件事是一種等價關係。

(A) 考慮 $f : X \to X$, 其中 $f(x) = x$。若 $x_1 \neq x_2$, 則 $f(x_1) = x_1 \neq x_2 = f(x_2)$, 所以 f 是一對一。對所有 $x \in X$, 取 $x \in X$, 則 $f(x) = x$, 所以 f 是映成的。因此, $X \sim X$。

(B) 若 $X \sim Y$, 即存在一對一且映成的映射 $f : X \to Y$, 因爲 f 是映成的, 所以對任何 $y \in Y$, 存在 $x \in X$ 使得 $f(x) = y$。因爲 f 是一對一的, 如果 $f(x_1) = y$ 又 $f(x_2) = y$ 的話, 因爲 $f(x_1) = y = f(x_2)$, 所以 $x_1 = x_2$。由上討論得知: 對任何 $y \in Y$, 存在唯一 $x \in X$ 使得 $f(x) = y$。於是我們可以建立一個映射 $g : Y \to X$, 其中 $g(y) = x$, 而 x 和 y 之間的關係是由 $f(x) = y$ 確定。

若 $y_1 \neq y_2$, 因爲分別存在 x_1, x_2 使得 $f(x_1) = y_1, f(x_2) = y_2$, 則 $g(y_1) = x_1, g(y_2) = x_2$, 如果 $x_1 = x_2$, 則 $f(x_1) = f(x_2)$, 得到 $y_1 = y_2$ 矛盾, 故 $x_1 \neq x_2$。因此映射 g 是一對一。

因爲對任意 $x \in X$ 都有 $f(x) = y$, 所以就有 $g(y) = x$, 於是 g 是映成的。

由上討論得知: 若 $X \sim Y$, 則 $Y \sim X$。

(C) 因爲 $X \sim Y$, 所以存在一對一且映成的映射 $f : X \to Y$, 因爲 $Y \sim Z$, 所以存在一對一且映成的映射 $g : Y \to Z$。考慮映射 $h = g \circ f : X \to Z$。

VmqTj9ZujQY

若 $x_1 \neq x_2$, 則 $f(x_1) \neq f(x_2)$, 得到 $g(f(x_1)) \neq g(f(x_2))$, 於是 $h(x_1) \neq h(x_2)$, 因此 h 是一對一。

對任意 $z \in Z$, 存在 $y \in Y$ 使得 $g(y) = z$, 對於 $y \in Y$, 存在 $x \in X$ 使得 $f(x) = y$, 所以 $h(x) = g(f(x)) = g(y) = z$, 因此 h 是映成的。

由上討論得知: 若 $X \sim Y$ 且 $Y \sim Z$, 則 $X \sim Z$。

現在將給出集合元素個數的分類。

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 與集合 $\{1, 2, \ldots, n\}$ 有相同的基數, 則稱集合 S 是 有限集 (finite set)。

P4cyb0oHGCU

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

定義 5. 給定一個集合 S,

(A) 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)。

(B) 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, 我們並不把有限集歸類成可數集; 也就是說,「可數集」這個詞在此專指與正整數集有相同基數的集合, 所以有時候會特別強調它是一個 *無窮可數集* (infinite countable set)。然而有些書籍或文獻會把有限集也視爲可數集 (因爲有限集明明就可以計數)。在數學上有時會出現定義上的落差, 面對這樣的現象, 只要確定前後文能夠自成一個系統不互相混用即可, 不需要對於定義這件事有過多的爭辯。

探討一個集合是可數集或是不可數集其實已經發展出一套十分深刻的理論, 但是這裡並不打算完整介紹那個理論, 因爲它並不是高等微積分課程的主軸。這個單元的重點只是要用簡要的方式回答前面三個問題, 讓各位從中了解自然數集 $\mathbb{N}$、整數集 $\mathbb{Z}$、有理數集 $\mathbb{Q}$ 與實數集 $\mathbb{R}$ 在可數與不可數的意義下之關係。

根據上面集合基數的定義, 現在想要回答第一個問題: 正整數集與正偶數集的基數比較。

例 **6.** 正整數集 $\mathbb{N}$ 與正偶數集 $2\mathbb{N}$ 有相同的基數。

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

由上討論得知 $\mathbb{N}\sim 2\mathbb{N}$。 □

至於第二個問題的答案則需要慢慢建構。這裡先下結論, 我們要證明: 有理數集是可數集, 而實數集是不可數集。所以實數集的元素個數比有理數集的元素個數還要多很多。

ew5Nzo3xyQ0

引理 **7.** 假設集合 A 是可數集, 而集合 $E\subset A$。若 E 不是有限集, 則 E 是可數集。

證明: 因爲 A 是可數集, 所以存在 $f:\mathbb{N}\to A$ 是一對一且映成的映射; 換言之, 我們可以將 A 中的元素給予編號 $f(1)=a_1, f(2)=a_2,\ldots,f(n)=a_n,\ldots$, 於是對集合 A 裡面的元素來說, 我們可以給出一個排序的關係: $A=\{a_1,a_2,\ldots,a_n,\ldots\}$。

若 $E\subset A$ 且 E 不是有限集, 現在從 $a_1,a_2,a_3,\ldots$ 依序詢問該元素是否也在集合 E 裡面, 將第一個落在 E 裡面的元素重新標記成 a_{n_1}, 再從 a_{n_1} 之後找到下一個落在 E 中的元素, 將它記爲 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 $F:\mathbb{N}\to E$, 其中 $F(k)=a_{n_k}$。這裡注意到: 在集合 E 當中的元素編號與集合 A 當中的元素編號形成一對一的映射 $g:\mathbb{N}\to\mathbb{N}$, 其中 $g(k)=n_k$。

以下將證明 $\mathbb{N}$ 與 E 有相同的基數。

(A) <u>F 是一對一映射</u>: 對任何 $k',k''\in\mathbb{N}$ 且 $k'\neq k''$, 則 $F(k')=a_{n_{k'}}, F(k'')=a_{n_{k''}}$, 因爲由 k' 與 k'' 對應到 A 中的元素編號不同, 即 $g(k')\neq g(k'')$, 或是說 $n_{k'}\neq n_{k''}$, 而 $f:\mathbb{N}\to A$ 是一對一映射, 所以 $a_{n_{k'}}\neq a_{n_{k''}}$, 即 $F(k')\neq F(k'')$, 因此 F 是一對一。

(B) <u>F 是映成的映射</u>: 對任何 $a\in E\subset A$, 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, 則有 $a=a_n$。對於 F 來說, 現在依序從 $F(1),F(2),\ldots,F(n)$ 開始找起, 一定會在 $\{1,2,\ldots,n\}$ 當中找到某個數 k 使得 $F(k)=a_n=a$, 所以 F 是映成的。

□

E9034w5sFRI

例 **8.** 證明: $(0,1)$ 中的有理數所成的集合 $(0,1)\cap\mathbb{Q}$ 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 $\frac{p}{q}$, 其中 $p,q\in\mathbb{N}, p<q, (p,q)=1$, 而上述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。現在我們把這個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, 純粹以指標 $a_{pq}=\frac{p}{q}$ 的眼光看待之, 其中 $p,q\in\mathbb{N}, p<q, q\geq 2$。若將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 $A=\{a_{pq}\}$, 此時建立映射 $f:A\to\mathbb{N}$ 爲 $f(a_{pq})=(0+1+2+\cdots+(q-2))+p$。

(A) $f:A\to\mathbb{N}$ 是一對一映射: 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) $f:A\to\mathbb{N}$ 是映成的映射: 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 引理 **7** 的結果得知 $(0,1)\cap\mathbb{Q}$ 是可數集。 □

這裡我們回顧 例 **8** 的建構方式, 因爲在 $(0,1)$ 內的有理數比較不好直接寫出它與正整數 $\mathbb{N}$ 之間的對應關係, 所以將那些分子、分母不互質的表達法全部補回去, 甚至把它們理解爲不同的元素時, 因爲這樣子可以很清楚寫下規律, 也就是給定分母是 $q\in\mathbb{N}, q\geq 2$ 之下, 分子就從 $1,2,\ldots,q-1$ 依序排列, 這麼一來就也可以用定義的方式證明這個映射具有一對一且映成的性質。而 $(0,1)\cap\mathbb{Q}$ 在集合的意義下是包含於上述所討論的集合, 而且它又不是有限集, 於是由 引理 **7** 得知 $(0,1)\cap\mathbb{Q}$ 是可數集。

下一個例題是要驗證: 比 $(0,1)\cap\mathbb{Q}$ 再多 0 還有 1 這兩個元素所成的集合仍然是可數集。以下呈現論述的方式, 在數學上與希爾伯特旅館悖論 (Hilbert's Paradox of the Grand Hotel) 有關。

wF2IgdXOKp4

例 **9.** $[0,1]$ 中的有理數集 $[0,1]\cap\mathbb{Q}$ 是可數集。

解. 已知: 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 $F:\mathbb{N}\to[0,1]\cap\mathbb{Q}$ 如下:

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

(A) $\underline{F:\mathbb{N}\to[0,1]\cap\mathbb{Q}\text{ 是一對一映射}}$: 對於 $m\neq n$, 若 $m,n\geq 3$, 因爲 f 是一對一得知 F 是一對一; 若 $m=1,n\neq 1$, 則 $F(1)=0,F(n)>0$ 得知 $F(1)\neq F(n)$; 若 $m=2,n\neq 2$, 則 $F(2)=1,F(n)<1$ 得知 $F(2)\neq F(n)$。因此 F 是一對一。

(B) $\underline{F:\mathbb{N}\to[0,1]\cap\mathbb{Q}\text{ 是映成的}}$: 給定 $a\in[0,1]\cap\mathbb{Q}$, 若 $a=0$, 則取 $n=1$ 使得 $F(n)=a$; 若 $a=1$, 則取 $n=2$ 使得 $F(2)=1$, 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 $F(n)=F(k+2)=f(k)=a$。因此 F 是映成的。

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

ZqjWNtqSSzc

例 **10.** 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, 第二個指標代表 a_{ij} 在 A_i 中與正整數之間的對應。

現在要將這些元素進行以下的重排(這種排列方法稱爲斜線排列法):

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

注意到定義域中我們寫 $\sqcup_{n=1}^{\infty}A_n$ 表示不自交的聯集 (disjoint union); 也就是說, 我們把所有元素都視爲不一樣。仿照 例 **8** 的討論可證明 f 是一對一且映成的映射。又因爲 $\cup_{n=1}^{\infty}A_n\subset\sqcup_{n=1}^{\infty}A_n$ 而且 $\sqcup_{n=1}^{\infty}A_n$ 是可數集, 所以由 例 **7** 的結果得知 $\cup_{n=1}^{\infty}A_n$ 是可數集。 □

將上述結果綜合起來就可以證明有理數集是可數集。

例 **11.** 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 **10** 知有理數集可表示成

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

所以有理數集是可數集。 □

現在要討論的是實數集的基數。首先我們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:

r2VB33Lq-AQ

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

(2) 將 $[\frac{a_1}{10},\frac{a_1}{10}+\frac{1}{10})$ 再分成十等分, 則三一律 (trichotomy law) 告知 $\frac{a_1}{10}+\frac{a_2}{10^2}\leq a<\frac{a_1}{10}+\frac{a_2}{10^2}+\frac{1}{10^2}$, 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 $\left[\sum\limits_{k=1}^{n}\frac{a_k}{10^k},\sum\limits_{k=1}^{n}\frac{a_k}{10^k}+\frac{1}{10^n}\right)$ 再分成十等分, 由三一律告知

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

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

(4) 由此可將 $a\in(0,1)$ 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 $0.4\bar{9}=0.5$。但是上述將實數指定至一種小數表示法與這件事無關。此外, 一個實數會有多種小數表示法的情形是出現在那個小數的某一位之後全部都是 9 的情況才會發生, 所以等一下的討論我們會避免使用 9 這個數字。

例 **12.** 證明: $(0,1)$ 中的實數集是不可數集。

tI58gjy7Xbc

證明: 利用反證法。假設 $(0,1)$ 中的實數集是可數集, 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:

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

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

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。由上述規定得知: 對所有 $i\in\mathbb{N}$, $f(i)\neq r$, 得到 f 並非映成, 矛盾。所以 $(0,1)$ 中的實數集是不可數集。 □

MBavOPTOBGA

這個單元的最後要回答 $[0,1]$ 區間與 $[0,2]$ 區間的基數比較。

例 **13.** 證明: $[0,1]$ 中的實數與 $[0,2]$ 中的實數有相同的基數。

證明: 考慮映射 $f:[0,1]\to[0,2]$ 為 $f(x)=2-2x$。

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

(B) 對所有 $y\in[0,2]$, 考慮 $x=\frac{2-y}{2}\in\mathbb{R}$, 則 $0\leq\frac{2-y}{2}\leq 1$, 而且

$$f(x)=f\left(\frac{2-y}{2}\right)=2-2\left(\frac{2-y}{2}\right)=2-(2-y)=2-2+y=y,$$

所以 f 是映成的。

由上討論得知: $[0,1]\sim[0,2]$。 □