數學傳播　36卷3期, pp. 24-40

「抽象代數」真的抽象嗎? (下)

沈淵源

5. 多項式的唯一分解性

現在我們轉移焦點至多項式環 $k[x]$; 此處 k 是一個體, 其中加法與乘法的單位元素分別是 0 與 1。若感覺太抽象, 不妨將 k看成是有理數體 $(\mathbb{Q},+,\cdot)$ 、實數體 $(\mathbb{R},+,\cdot)$ 或複數體 $(\mathbb{C},+,\cdot)$。

多項式 $k[x]$ 上的加法與乘法是你所熟悉的。因此你老早就已經知道:

(i) $(k[x],+)$ 形成一個阿貝爾群, 零多項式 0就是加法單位元素。

(ii) 乘法 $\cdot$ 具有結合律、交換律, 常數多項式 1就是乘法單位元素。

(iii) 乘法 $\cdot$ 對加法 $+$ 的分配律成立。

因此, $(k[x],+,\cdot)$ 跟整數環一樣; 也是一個擁有乘法單位元素的交換環, 但可逆元素 (units) 則包含所有的非零常數多項式。

我們可定義多項式環 $k[x]$ 中整除性如同跟整數環一樣; 唯一需要變的就是把「(整) 數」改成「 (多項) 式」。我們說一個多項式 a整除一個多項式 b, 如果有一個多項式 c 使得

$$b = ac\,;$$

而以符號 $a|b$表示之。換句話說, a除 b之後沒有餘式 (remainder) 。a 稱爲 b的一個因式 (divisor), 而 b則稱爲a的一個倍式 (multiple) 。例如: $x+1 \mid x^2-1$, $-x^2+x-1 \mid x^3-1$, 然而 $x^2+1 \nmid x^3+1$ (不整除)。

與整除性相關的是分解性。數 (式) 分解成較小 (低) 數 (式) 的乘積, 其大小就是絕對值 (次數) 的大小。多項式的次數 (degree) 通常用符號 $\deg a$ 來表示, 其中最重要的性質爲

$$\deg ab = \deg a + \deg b\,, \quad \deg a = 0 \Longleftrightarrow a \text{ 爲非零常數多項式 。}$$

前面所列出關乎整除性的11個基本性質在多項式裡頭也都成立; 當然性質 6 中的「±1」得改成多項式裡頭的可逆元素「非零常數多項式」, 而性質 9 及性質10 的絕對值則改爲多項式裡頭的次數。

質數的觀念在多項式裡頭也相仿, 當然稱爲質多項式或簡稱爲質式 (irreducible polynomials) ; 意指不可再分解的多項式。更明確的說, 一個非常數多項式 p 稱之爲質多項式如果 $q \mid p$ 導致 q 爲常數多項式或爲 p 的常數倍。

爲了方便起見, 我們定義首項係數 (即領導係數 leading coefficient) 爲 1 的多項式爲首一多項式 (monic polynomial)。譬如說, 多項式

$$x^2 + 7x - 11 \qquad 及 \qquad x^4 - 3x^2 + 9x - 19$$

都是首一多項式但 $7x^2 - 11$ 及 $3x^4 + 9x - 19$都不是。

令 $a \in k[x]$ 且令 p爲首一質式。則若 $a \neq 0$, 必存在一非負整數 α 使得 (因爲 p 之次冪的次數越來越大)

$$p^{\alpha} \mid a \qquad 但 \quad p^{\alpha+1} \nmid a\,。$$

這個 α 就稱之爲 a 在質式 p 的階數 (the order of a at p), 以符號 $\operatorname{ord}_p a$表示之。粗略言之, $\operatorname{ord}_p a$ 就是 p 整除 a 的次數。若 $a = 0$, 則我們定義 $\operatorname{ord}_p a = \infty$。注意到, 另一個極端爲

$$\operatorname{ord}_p a = 0 \Longleftrightarrow p \nmid a\,。$$

接著我們逐步預備好要證明多項式版本之算術基本定理的工具。首先處理存在性的部分, 同樣地這只是數學歸納法原理的一個簡單練習而已。按慣例, 得勞大駕動動手將這簡單的證明完成; 但需注意的乃是, 要對多項式的次數作數學歸納法。

引理 1. 任何非零多項式都可以寫成質式的乘積。

注意到, 每一個多項式都可以寫成其領導係數跟一個首一多項式的乘積; 而質式經此手續後, 就變成其領導係數跟一個首一質式的乘積。物以類聚, 將同一個首一質式擺在一起; 我們可以將一個多項式 f 寫成 $f = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$, 其中 p_i 爲首一質式且 a_i 爲正整數。我們會採用底下更方便的方式來表達: $f = c \prod_p p^{a(p)}$, 此處 c 爲 f 之領導係數, 而乘積中的 p 是對所有的首一質式。次冪 $a(p)$ 乃是非負整數; 當然, 除了有限多個首一質式外, 此次冪都是零。

算術基本定理 (多項式版本). 對任何非零多項式 f 存在一質式分解式

$$f = c\prod_p p^{a(p)}\,,$$

此處 c 爲 f 之領導係數, 而乘積中的 p 是對所有的首一質式; 其次冪由 f 所唯一決定。實際上, 我們有 $a(p) = \operatorname{ord}_p f$。

引理 2. 若 $a, b \in k[x]$ 而且 $\deg b > 0$, 則存在 $q, r \in k[x]$ 使得

$$a = qb + r\,, \qquad \text{其中} \quad \deg r < \deg b \ \text{ 或 } \ r = 0。$$

證明. 因爲零多項式的次數沒有定義, 所以很自然的, 我們必須分成兩種情況來討論。

(i) $b \mid a$: 令 $q = a/b$。則 $a = qb + r\,,\ r = 0$; 故得證。

(ii) $b \nmid a$: 令 $r = a - qb$ 爲形如 $a - ub,\ \ u \in k[x]$的多項式中擁有最低次數者。我們必須證明 $\deg r < \deg b$。若否, 令 r與 b之最高次項分別爲 $r_d x^d$與 $b_m x^m$。則

$$r - r_d b_m^{-1} x^{d-m} b = a - (q + r_d b_m^{-1} x^{d-m})b$$

爲形如 $a - ub,\ \ u \in k[x]$ 的多項式, 卻擁有比 r 還小的次數; 矛盾也, 故得證。

引理 2就是多項式裡頭的長除法, 其證明過程當然也用到了自然數的良序原理。這裡比的是次數的大小, 而上一節比的是絕對值的大小。

定義. 若 $a_1, \cdots, a_n \in k[x]$, 定義多項式集合 $(a_1, \cdots, a_n)$ 爲

$$(a_1, \cdots, a_n) = \{a_1u_1 + \cdots + a_nu_n \mid u_1, \cdots, u_n \in k[x]\}\,。$$

令 $I = (a_1, \cdots, a_n)$。顯而易見, 這個集合在加法與減法之下都具有封閉性; 亦即, 任何 I 裡頭的兩個元素的和或差仍然還是裡頭的元素。不僅如此, 若將裡頭的元素乘上任何的多項式仍然還是裡頭的元素。也就是說, 不管你的整數來源如何; 或在 I 裡頭, 或不在 I 裡頭; 一旦乘上 I 裡頭的元素, 就會被吸入, 成爲裡頭的一份子。在環論的術語, 這就是所謂的理想; 因此 I 是多項式環 $k[x]$ 的一個理想。

引理 3. 若 $a, b \in k[x]$, 則存在 $d \in k[x]$ 使得 $(a, b) = (d)$。

證明. 若 $a = b = 0$, 那麼樣就沒甚好證的; 故假設 a, b不全爲零, 因而 $(a, b) \neq \{0\}$。令 $d \in (a, b)$ 爲當中次數最小的一個多項式。顯而易見, $(d) \subseteq (a, b)$; 我們必須證明, 反方向 $(a, b) \subseteq (d)$ 也對。

假設 $x \in (a,b)$。引理 2告訴我們, 存在 $q, r \in k[x]$ 使得

$$x = qd + r\,, \qquad \text{其中} \quad \deg r < \deg d \ \text{ 或 } \ r = 0\text{。}$$

顯而易見, $r = x - qd \in (a,b)$。若 $r \neq 0$, 則 r 爲 (a,b) 中次數比 d 還小的一個多項式; 此乃一矛盾, 因此 $r = 0$ 是唯一的歸宿。所以得到 $x = qd \in (d)$, 故得證。

定義. 令 $a, b \in k[x]$。d 稱爲 a 與 b 的一個最高公因式; 若

(i) d是 a與 b的公因式,

(ii) 任何其它 a與 b的公因式都整除 d。

特別注意到, 定義中說的是一個最高公因式。那到底有幾個呢? 若 c 是另一個, 那麼我們就必定有

$$c \mid d \qquad \text{且} \qquad d \mid c\,,$$

因而 $\deg c = \deg d$。故兩個多項式的最高公因式, 若存在; 任意兩個都會有相同的次數, 其間就差一個常數倍。其中那個首一最高公因式, 通常我們用符號 $\gcd(a,b)$ 來表示。

引理 4. 令 $a, b \in \mathbb{Z}$。若 $(a,b) = (d)$, 則 d 是 a 與 b 的一個最高公因式。

證明. (i) 因爲 $a, b \in (a,b) = (d)$, 故 d 是 a 與 b 的公因式。

(ii) 假設 c是 a與 b的公因式。因此 c整除任何 a與 b的線性組合, 而 $d \in (d) = (a,b)$就是 a與 b的一個線性組合; 故 $c \mid d$。

這就是最高公因式的存在性定理。在實作中, 我們通常使用輾轉相除法來計算。

定義. 我們說多項式 a 與 b 是互質的; 若其僅有的公因式只有非零常數, 即多項式中的可逆元素。換句話說, $\gcd(a,b) = 1$。

定理 P. 假設 $a \mid bc$ 而且 $\gcd(a,b) = 1$, 則 $a \mid c$。

證明. 因 $\gcd(a,b) = 1$, 存在 $x, y \in k[x]$ 使得

$$xa + yb = 1\text{。}$$

兩邊同時乘上 c, 得到

$$xac + ybc = c\text{。}$$

根據假設 $a \mid bc$, 得知 a 整除上式左側的每一項; 因此

$$a \text{ 整除左側 } = \text{ 右側 } = c\,,$$

故得證。

推論 1. 若 p爲質式且 $p \mid bc$, 則 $p \mid b$ 或 $p \mid c$。

證明. 因 p 爲質式, 故得

$$\gcd(p,b) = p \qquad \text{或} \qquad \gcd(p,b) = 1\text{。}$$

因此我們有

(i) $\gcd(p,b) = p$: 因 $\gcd(p,b) \mid b \Longrightarrow p \mid b$,

(ii) $\gcd(p,b) = 1$: 定理 P $\Longrightarrow p \mid c$;

故得證。

若將推論 1 寫成其反逆敍述, 則有

推論1′. 若 p 爲質式滿足 $p \nmid b$ 且 $p \nmid c$, 則 $p \nmid bc$。

推論 2. 假設 p 是首一質式而且 $a, b \in k[x]$。則

$$\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b\text{。}$$

證明. 令 $\alpha = \operatorname{ord}_p a$ 且令 $\beta = \operatorname{ord}_p b$。則

$$a = p^{\alpha}a' \quad \text{且} \quad b = p^{\beta}b'\,; \quad \text{其中 } p \nmid a' \quad \text{且} \quad p \nmid b'\text{。}$$

因此我們有

$$ab = p^{\alpha+\beta}a'b'\,, \quad \text{其中 } p \nmid a'b' \ (\text{推論}1')\,;$$

所以得證

$$\operatorname{ord}_p ab = \alpha + \beta\text{。}$$

至此, 準備工作完成; 回到唯一分解性之證明。

多項式版本的算術基本定理之證明. 引理 1 已經證明, 對任何非零多項式 f 存在一質數分解式 $f = c\prod_p p^{a(p)}$。兩邊同時取 ord_q, 並使用推論 2; 我們有

$$\mathrm{ord}_q\, n = \mathrm{ord}_q(c) + \sum_p a(p)\mathrm{ord}_q(p)\,。 \tag{1}$$

根據 ord_q 之定義, 我們有

$$\mathrm{ord}_q(c) = 0 \qquad \text{且} \quad \mathrm{ord}_q(p) = \begin{cases} 1 \text{ 若 } p = q \\ 0 \text{ 若 } p \neq q \end{cases}。$$

所以實際上, (1) 式的右側僅剩單一的一項 $a(q)$ 沒有陣亡; 我們有

$$\mathrm{ord}_q\, f = a(q)\,,$$

故得證。

6. 歐氏整域的唯一分解性

看完了整數環與多項式環的唯一分解性後, 你一定很訝異這之間存在著如此驚人的相似性。那麼, 這背後是否隱藏著怎麼樣更豐富的結構; 使得活現在你眼前的整數環與多項式環, 只不過是裡頭兩個特殊的例子而已呢?

幾番細思量, 不難發現; 引理 2所帶出來的性質可說是相當的關鍵, 而在引理 3中更是發揮得淋漓盡致。一來, 其間有大小的觀念; 在 $\mathbb{Z}$ 中爲一般的絕對值 (非負整數) , 而在 $k[x]$ 中則爲多項式的次數 (也是非負整數) ; 這提供了良序性可以展現她婀娜多姿神采的舞台, 也成就了最小元素卻是最大公因數 (最高公因式) 的美談。二來, 只要一個集合在減法與倍數 (式) 之下有封閉性; 那麼最小元素搖身一變, 成爲這個集合的生成元素; 也就是說, 所有的元素都是最小元素的倍數 (式) 。

從實作的層面來說, 引理 2乃是計算最大公因數、最高公因式演算法的基石; 那就是所謂的輾轉相除法, 也稱爲歐基里德演算法。因此之故, 引理 2有些人也把它稱爲歐基里德演算法 (Euclid's algorithm)。很自然地, 人們就把具備有引理 2性質的整域 (integral domain) 稱爲歐基里德域簡稱爲歐氏整域。更明確的說, 我們有如下的定義。

定義. 一個歐氏整域 (Euclidean domain) 就是一個整域 R; 其非零元素上定義有一函數 σ 映到非負整數上, 使得對任意 $a, b \in R$, $b \neq 0$ 存在 $q, r \in R$ 滿足

$$a = qb + r \qquad \text{其中} \qquad \sigma(r) < \sigma(b) \quad \text{或} \quad r = 0。$$

除了整數環及多項式環是歐氏整域外, 還有高斯整數環 $\mathbb{Z}[\sqrt{-1}]$ 及前面碰到的複數子集 $\mathbb{Z}[\sqrt{-2}]$ 也是歐氏整域。

例題 1. 高斯整數環 $\mathbb{Z}[\sqrt{-1}]$ 是一個歐氏整域。

證明. 顯而易見, $\mathbb{Z}[\sqrt{-1}] \subseteq \mathbb{C}$ 是一個整域。定義函數

$$\sigma(\alpha+\beta\sqrt{-1}) = \alpha^2+\beta^2, \quad \alpha+\beta\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]。$$

令 $a, b \neq 0$ 爲任意的高斯整數。將 a 除以 b 得到

$$u = a/b = s+t\sqrt{-1}, \qquad s,t \in \mathbb{Q}。$$

選取整數 ξ, ζ 使得

$$|s-\xi| \leq \frac{1}{2} \qquad 且 \qquad |t-\zeta| \leq \frac{1}{2}。$$

令 $q = \xi+\zeta\sqrt{-1}$, 則

$$\sigma(a/b-q) = (s-\xi)^2+(t-\zeta)^2 \leq \frac{1}{4}+\frac{1}{4} = \frac{1}{2}。$$

令 $r = a-qb$, 則 $r \in \mathbb{Z}[\sqrt{-1}]$ 且 $a = qb+r$; 其中 $r = 0$ 或

$$\sigma(r) = \sigma(b(a/b-q)) = \sigma(b)\sigma(a/b-q) \leq \frac{1}{2}\sigma(b) < \sigma(b)。$$

故得證高斯整數環 $\mathbb{Z}[\sqrt{-1}]$ 是一個歐氏整域。

例題 2. 複數子集 $R = \mathbb{Z}[\sqrt{-2}]$ 也是一個歐氏整域。

證明. 如上顯而易見, $R \subseteq \mathbb{C}$ 是一個整域。定義函數

$$\sigma(\alpha+\beta\sqrt{-2}) = \alpha^2+2\beta^2, \quad \alpha+\beta\sqrt{-2} \in R。$$

令 $a, b \neq 0$ 爲 R 中任意的元素。將 a 除以 b 得到

$$u = a/b = s+t\sqrt{-2}, \qquad s,t \in \mathbb{Q}。$$

選取整數 ξ, ζ 使得 $|s-\xi| \leq \frac{1}{2}$ 且 $|t-\zeta| \leq \frac{1}{2}$。
令 $q = \xi+\zeta\sqrt{-2}$, 則

$$\sigma(a/b-q) = (s-\xi)^2+2(t-\zeta)^2 \leq \frac{1}{4}+2\cdot\frac{1}{4} = \frac{3}{4}。$$

令 $r = a - qb$, 則 $r \in R$ 且 $a = qb + r$; 其中 $r = 0$ 或

$$\sigma(r) = \sigma(b(a/b - q)) = \sigma(b)\sigma(a/b - q) \leq \frac{3}{4}\sigma(b) < \sigma(b)。$$

故得證 R 是一個歐氏整域。

定義. 一個環 $(R, +, \cdot)$ 的非空子集 I 稱之爲理想; 若

(i) $a, b \in I \Longrightarrow a - b \in I$

(ii) $a \in I, r \in R \Longrightarrow ra \in I, ar \in I$

定理 ED. 若 I 爲歐氏整域 R 中的一個理想, 則存在一元素 $a \in R$ 使得

$$I = Ra = \{ra \mid r \in R\}。$$

證明. 若 $I = 0$, 那麼樣就沒甚好證的; 故假設 $I \neq 0$。令 $a \in I$ 爲當中 σ 值最小的一個元素。顯而易見, $Ra \subseteq I$; 我們必須證明, 反方向 $I \subseteq Ra$也對。

假設 $x \in I$。因 R 是歐氏整域, 故存在 $q, r \in R$ 使得

$$x = qa + r\,, \qquad \text{其中} \quad \sigma(r) < \sigma(a) \ \text{ 或 } \ r = 0。$$

顯而易見, $r = x - qa \in I$。若 $r \neq 0$, 則 r 爲 I 中 σ 值比 a之 σ 值還小的一個元素; 此乃一矛盾, 因此 $r = 0$是唯一的歸宿。所以得到 $x = qa \in Ra$, 故得證。

習慣上, 我們將 Ra 寫成 (a); 同樣地, $(a_1, \cdots, a_n)$ 表示

$$Ra_1 + \cdots + Ra_n = \{r_1a_1 + \cdots + r_na_n \mid r_i \in R, i = 1, \cdots, n\}。$$

顯而易見, 若 R 是一交換環, 則 $(a_1, \cdots, a_n)$ 爲 R 中的一個理想。若 I 是環 R 中的一個理想且 $I = (a_1, \cdots, a_n)$, 那麼我們就說 I 是有限生成 (finitely generated) 的一個理想; 當 $n = 1$ 時, 則稱 I 爲 R 中的一個主理想 (principal ideal)。

定義. 我們稱呼整域 $(R, +, \cdot)$ 是一個主理想域 (principal ideal domain, 縮寫 PID); 若 R 中的每一個理想都是主理想。

所以定理 ED 說, 歐氏整域都是 PID; 因而整數環, 多項式環, 高斯整數環及 $(\mathbb{Z}[\sqrt{-2}], +, \cdot)$ 都是 PID。引進歐氏整域的觀念是相當有用的; 因爲在實作上, 要證明某些環是 PID; 往往我們先証明此環是一歐氏整域, 然後再透過定理 ED 得到 PID 的結論。

底下我們將整除性的觀念推廣到擁有乘法單位元素 1的 PID 當中, 然後討論唯一分解性的問題; 當然這些觀念可在一般的環當中來討論, 但那不是我們所要的。因此從現在開始, 我們活動的空間就侷限在擁有乘法單位元素 1 的 PID 裡頭。

令 R爲擁有乘法單位元素 1的 PID。先定義跟整除性相關的術語如下:

- 我們說 R 裡頭的一個元素 $a \neq 0$ 整除一個元素 $b \in R$, 若存在另一個元素 $c \in R$ 使得 $b = ac$; 而以符號 $a|b$ 表示之。
- 一個元素 $u \in R$ 稱之爲可逆元素 (unit), 若 u 整除 R 裡頭的乘法單位元素 1。
- 兩個元素 $a, b \in R$ 稱之爲夥伴 (associate) , 若存在一可逆元素 u 使得 $a = bu$。
- 一個元素 $p \in R$ 稱爲不可約的 (irreducible) , 若 $a \mid p$ 則 a 是可逆元素或是 p 的夥伴。
- 一個不可逆元素 $p \in R$ 稱爲質的 (prime) , 若 $p \neq 0$ 且

$$p \mid ab \Longrightarrow p \mid a \quad \text{或} \quad p \mid b。$$

不可約元素 (irreducible elements) 跟質元素 (prime elements) 的區分是過去沒有的; 因爲在整數環與多項式環中, 這兩個觀念是合而爲一的。在上面定義質數 (式) 時, 所採用的乃是不可約的觀念; 而質性的觀念, 則彰顯在推論 2裡面。對我們而言, 其實也不需要如此區分; 因爲在 PID 中, 這兩個觀念也是合而爲一的, 我們等一下就會證明。

上面那些觀念都可轉換成 '理想' 的術語如下:

- $a \mid b \Longleftrightarrow (b) \subseteq (a)$。
- $u \in R$ 爲可逆元素 $\Longleftrightarrow (u) = R$。
- $a, b \in R$爲夥伴 $\Longleftrightarrow (a) = (b)$。
- $p \in R$ 爲不可約的, 若$(p) \subseteq (a)$ 則 $(a) = R$ 或 $(a) = (p)$。
- $p \in R$ 爲質的, 若且唯若 $ab \in (p) \Longrightarrow a \in (p)$ 或 $b \in (p)$。

定義. 令 $a, b \in R$。d 稱之爲 a 與 b 的一個最大公因子; 若

(i) $d \mid a$ 且 $d \mid b$,

(ii) $d' \mid a$ 且 $d' \mid b \Longrightarrow d' \mid d$。

特別注意到下面兩件事情:

(i) 定義中說的是一個最大公因子。那到底有幾個呢? 若 c 是另一個, 那麼我們就必定有 $c \mid d$ 且 $d \mid c$, 因而 c 與 d 是夥伴; 亦即, 存在一可逆元素 u 使得 $c = ud$。因此最大公因子的個數就是其可逆元素的個數。

(ii) 兩個元素的最大公因子不見得一定會存在; 然而對 PID 來說, 我們有下面的定理。

定理. 令 R是一個具有單位元素 1 的 PID 且令 $a, b \in R$。則 a 與 b 有一個最大公因子 d, 而且 $(a, b) = (d)$。

證明. 考慮由 a, b 所生成的理想 $(a, b) = Ra + Rb$。因爲 R 是一個 PID, 所以有一元素 d 使得

$$(a, b) = (d)\,。$$

(i) $a \in (a, b) = (d) \Longrightarrow d \mid a$ 且 $a \in (a, b) = (d) \Longrightarrow d \mid b$,

(ii) $d' \mid a$ 且 $d' \mid b \Longrightarrow (a) \subseteq (d')$ 且 $(b) \subseteq (d')$
$\Longrightarrow (d) = (a, b) \subseteq (d')$
$\Longrightarrow d' \mid d$。

故得證 d 爲 a 與 b 的一個最大公因子。

定義. 我們說 R 中兩個元素 a 與 b 是互質的; 若其僅有的公因子是可逆元素。換句話說, $(a, b) = R$。

推論 1. 若 R 爲一 PID 且 p 是不可約的 (irreducible), 則 p 是質元素 (prime element)。

證明. 假設 $p \mid ab$。上述定理允許我們考慮 a 與 p 的最大公因子。因 p是不可約的, 故僅有的因子爲可逆元素或 p 的夥伴; 所以有 $(a, p) = R$ 或 $(a, p) = (p)$ 兩種情況需要討論。

(i) $(a, p) = (p)$: 顯而易見 $(a) \subseteq (a, p) = (p) \Longrightarrow p \mid a$。

(ii) $(a, p) = R$: 此種情況我們得到 $(ab, pb) = (b)$。假設告訴我們 $p \mid ab \Longleftrightarrow ab \in (p)$且 $pb \in (p)$, 因而得知

$$(b) = (ab, pb) \subseteq (p) \Longrightarrow p \mid b\,。$$

所以我們已經證明了

$$p \mid ab \Longrightarrow p \mid a \quad \text{或} \quad p \mid b\,,$$

故得證, p是質元素。

問題. 反過來說, 若 p 是質元素, p 是否不可約呢? 換句話說, 推論 1的逆敍述是否成立?

爲了回答這個問題, 我們得看看: 當 p 是質元素的時候, 元素 p 有那些因子呢? 假設 a 是 p 的一個因子, 那麼就存在 b 使得 $p = ab$; 因此 $p \mid ab$, 但 p 是質元素導致 $p \mid a$ 或 $p \mid b$。

(i) $p \mid a$: 假設是 $a \mid p$, 故得知 a是 p的夥伴。

(ii) $p \mid b$: 存在 c使得 $b = pc$。但 $p = ab$, 故得

$$p = ab = a(pc) = p(ac) \Longrightarrow p(ac-1) = 0 \overset{R\text{是整域}}{\Longrightarrow} ac = 1\,;$$

因而 a爲可逆元素。

所以我們已經證明了, p 的因子裡頭; 不是 p 的夥伴, 就是可逆元素。故得證, p 是不可約的 (irreducible)。

因此, 在一個擁有乘法單位元素 1 的 PID 裡頭; 不可約元素跟質元素這兩個觀念是合而爲一、不分彼此的。我們把這個性質稱爲 PID 的基本性質, 敍述如下。

PID **的基本性質**. 若 R爲一擁有乘法單位元素 1的 PID, 則

$$p\text{是不可約(irreducible) 元素} \iff p\text{是質(prime) 元素。}$$

接著, 我們要逐步預備好證明 PID 版本的算術基本定理。首先當然得處理存在性的部分, 這一次良序原理或數學歸納法原理根本使不上力; 因爲一個擁有乘法單位元素 1的 PID 跟自然數或非負整數根本扯不上任何的關係。

你若要將一個元素分解、再分解, 直到不能再分解爲止; 問題在這分解的過程是不是停得下來呢? 如果停不下來的話, 那麼連不可約元素存在與否都是個問題; 因爲前面定義過的不可約元素就是那不能再分解的元素。職是之故, 我們得回頭看看; 整數環與多項式環那邊, 分解因數 (式) 的時候是怎麼個停下來的呢?

在整數那邊, 分解之後的數變小了; 這大小指的是絕對值的大小, 分解一次就降一次; 頂多降到 1就必須停止。在多項式那邊, 分解之後多項式的次數變小了; 頂多降到 0就必須停止。整

數裡頭絕對值是 1的就只有 ± 1, 而多項式裡頭次數是 0的就是非零常數多項式; 這些元素分別是整數及多項式裡頭的可逆元素。所以, 在這兩個環裡頭的元素; 都有大小的觀念, 可供分解的依據; 降到最小就是可逆元素, 最小之前的那個元素當然就有可能是不可約元素。

然而, 我們現在工作的場所僅僅是一個擁有乘法單位元素 1 的 PID 而已, 當然就沒那麼美那麼帥囉。這可怎麼辦呢? 一方面我們當然要善用 PID 特有的代數結構, 每一個理想子環都是一個主理想子環; 亦即, 每一個理想子環都是其中某一個元素的倍數。另一方面, 你可還記得嗎? 前面將兩個元素之間的整除關係轉化成兩個主理想子環之間的包含關係; 亦即, $a \mid b \iff (b) \subseteq (a)$。因此之故, 整除性就跟 PID 特有的代數結構掛上勾了。而主理想子環之間的包含關係就變成其生成元素之間的大小關係, 主理想子環愈大其生成元素愈小。因此, 分解到最後的那個最小元素; 當然就是一個可逆元素, 而此時其對應的主理想子環就是你所看到的這個 PID 本身。

現在, 我們要證明在一個擁有乘法單位元素 1的 PID 中; 非零不可逆元素都是不可約元素的乘積。這個證明可分成兩個步驟:

(i) 首先證明每一個非零不可逆元素 a都存在有不可約的因子,

(ii) 然後再證明 a就是這些不可約因子的乘積。

這兩個步驟當中, 我們都會用到底下的「停下來原理」。因爲停下來, 所以不可約因子存在; 因爲停下來, 所以乘積中只包含有限多個不可約的因子。眞是妙不可言!

停下來原理. 令 R 爲一擁有乘法單位元素 1 的 PID 且令

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

爲一向上攀升的主理想鏈。則存在一正整數 n 使得

$$(a_n) = (a_{n+m}) \qquad \forall\, m = 0, 1, 2, \cdots 。$$

換句話說, 此鏈在有限步之後就停下來。

證明. 令 $I = \bigcup_{i=1}^{\infty} (a_i)$。顯而易見, I 是主理想域 R 中的一個理想。故存在 $a \in R$ 使得 $I = (a)$。但

$$a \in \bigcup_{i=1}^{\infty} (a_i) \Longrightarrow a \in (a_n) \quad \text{對某一個 } n\,,$$

因此我們有 $I=(a)\subseteq(a_n)$; 又 $(a_n)\subseteq\bigcup_{i=1}^{\infty}(a_i)=I$, 故得證

$$I=(a_n)=(a_{n+1})=\cdots。$$

引理 1. 令 R 爲一擁有乘法單位元素 1 的 PID。則每一個非零不可逆元素都是不可約元素的乘積。

證明. 令 $a\in R$ 爲非零不可逆元素。

(i) 首先證明 a存在有不可約的因子。若 a是不可約的, 則得證; 否則 $a=a_1b_1$, 其中 a_1 及 b_1 皆爲不可逆元素。若 a_1 是不可約的, 則得證; 否則 $a_1=a_2b_2$, 其中 a_2 及 b_2 皆爲不可逆元素。若 a_2 是不可約的, 則得證; 否則繼續如上之論證。顯而易見, 我們有

$$(a)\subseteq(a_1)\subseteq(a_2)\subseteq\cdots。$$

停下來原理告訴我們, 此鏈必斷。故存在某個 n, a_n 是不可約的。

(ii) 其次證明 a 是不可約元素的乘積。若 a 是不可約的, 則得證; 否則令 p_1爲其不可約之因子, 因此 $a=p_1c_1$。若 c_1 是可逆元素, 則得證; 否則令 p_2 爲其不可約之因子, 因此 $a=p_1p_2c_2$。若 c_2 是可逆元素, 則得證; 否則繼續如上之論證。顯而易見, 我們有

$$(a)\subseteq(c_1)\subseteq(c_2)\subseteq\cdots。$$

停下來原理告訴我們, 此鏈必斷。故存在某個 n, c_n是可逆元素且 $a=p_1p_2\cdots p_nc_n$; 又 p_nc_n ,是不可約的, 故得證。

再來, 我們定義非零元素 a 在不可約元素 p 的階數爲下面引理 2中的那個唯一的正整數 n , 以符號 $\operatorname{ord}_p a$ 表示之。

引理 2. 令 R 爲一擁有乘法單位元素 1 的 PID 且令 $p\in R$ 爲不可約元素及 $a\neq0$。則存在一正整數 n 使得

$$p^n\mid a\text{ 但 }p^{n+1}\nmid a。$$

證明. 若否, 則對每一個正整數 m 就存在一元素 $b_m\in R$ 使得 $a=p^mb_m$。因此 $pb_{m+1}=b_m$。顯而易見, 我們有無限向上攀升的主理想鏈

$$(b_1)\subseteq(b_2)\subseteq(b_3)\subseteq\cdots;$$

這與停下來原理背道而馳, 故得證。

引理 3. 若 $p \in R$ 是一個質 (=不可約) 元素且 $a, b \in R$ 爲非零二元素。則

$$\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b \quad 。$$

證明. 令 $\alpha = \operatorname{ord}_p a$ 且令 $\beta = \operatorname{ord}_p b$。則

$$a = p^\alpha a' \quad 且 \quad b = p^\beta b' ; \quad 其中 \ p \nmid a' \quad 且 \quad p \nmid b' 。$$

因此我們有

$$ab = p^{\alpha+\beta} a'b' , \quad 其中 \ p \nmid a'b' \ (質元素定義) ;$$

所以 $\operatorname{ord}_p ab = \alpha + \beta$, 故得證。

至此, 準備工作幾近完成; 底下先敍述唯一分解性, 然後證明之。令 S 爲 R 中具備下列二性質的質元素集:

(i) 每一個 R 中的質元素跟 S 中某個質元素是夥伴。

(ii) S 中任意兩個質元素都不是夥伴。

想要得到這樣子的質元素集, 簡單至極; 僅需從每一個夥伴類中選取一個質元素, 即可組成。這選擇的自由度當然非常大, 但在整數環及多項式環卻有著極其自然的選擇法。在整數環中, 我們選的是正質數; 而多項式環中, 我們則選首一質多項式。

算術基本定理 (PID **版本**). 令 R 爲一擁有乘法單位元素 1 的 PID 且令 S 爲如上選取的質元素集。則任何非零元素 a 存在一質元素分解式

$$a = u \prod_p p^{e(p)} ,$$

此處 u 爲可逆元素, 而乘積中的 p 是對所有 S 中質元素; 可逆元素 u 以及次冪 $e(p)$ 由 a 所唯一決定。實際上, 我們有 $e(p) = \operatorname{ord}_p a$。

證明. 引理 1 已經證明, 任何非零元素 a 存在一質元素分解式

$$a = u \prod_p p^{e(p)} 。$$

兩邊同時取 ord_q, 並使用引理 3; 我們有

$$\mathrm{ord}_q\, a = \mathrm{ord}_q(u) + \sum_p e(p)\mathrm{ord}_q(p)\,。 \tag{2}$$

根據 ord_q之定義, 我們有

$$\mathrm{ord}_q(u) = 0 \qquad 且 \quad \mathrm{ord}_q(p) = \begin{cases} 1 & 若\ p = q \\ 0 & 若\ p \neq q \end{cases}。$$

所以實際上, (2) 式的右側僅剩單一的一項 $e(q)$ 沒有陣亡; 我們有

$$\mathrm{ord}_q\, a = e(q)\,,$$

故得證。

7. 另一個唯一分解性之應用

凡具備有算術基本定理之性質的整域就稱之爲唯一分解整域 (Unique Factorization Domain 縮寫 UFD)。早在歐基里德的年代就隱約知道, 整數環是一個 UFD 的事實; 但第一個將此結果清楚明白的寫下來, 似乎得等到高斯的著作《算術研究》[17]中才出現。

上面我們已經證明了每一個 PID 都是一個 UFD; 反之則否。在例題 1 及例題 2 中, 我們證明了二次數體 (quadratic number fields) $\mathbb{Q}(\sqrt{-1})$ 及 $\mathbb{Q}(\sqrt{-2})$ 所對應的整數環 (rings of integers)

$$\mathbb{Z}[\sqrt{-1}] \quad 及 \quad \mathbb{Z}[\sqrt{-2}]$$

都是 UFD。值的一提的是, 在1966 年史達克 (Stark, H.M.) 完成了一個數論中懸宕未解決的問題; 他證明了二次數體 $\mathbb{Q}(\sqrt{d})$, 其中 $d < 0$ 所對應的整數環是一個 UFD 只有當

$$d = -1, -2, -3, -7, -11, , -19, -43, -67, \text{ 及 } -163$$

時, 而且再也沒有其他的值了。

在第一、二節, 我們已經看過了兩個簡單的應用; 分別用到了整數環以及 $(\mathbb{Z}[\sqrt{-2}], +, \cdot)$ 是 UFD 的事實。底下我們一起來看看另一個唯一分解性的應用; 包括用來證明有無限多個質數、質多項式。

[17]《算術研究》(Disquisitiones Arithmeticae) 是德國數學家卡爾·弗里德里希·高斯於1798年寫成的一本數論教材, 在1801年他24歲時首次出版。全書用拉丁文寫成。在這本書中高斯整理彙集了費馬、歐拉、拉格朗日和勒讓德等數學家在數論方面的研究結果, 並加入了許多他自己的重要成果。

質數無限定理 (歐幾里德). 在整數環 $\mathbb{Z}$ 中, 存在有無限多個質數。

證明. 若否, 則僅存在有限多個正質數; 說是

$$p_1\,,\quad p_2\,,\quad p_3\,,\quad \cdots\quad ,\quad p_n\,。$$

考慮整數

$$N = p_1\,p_2\,p_3\,\cdots\,p_n + 1\,。$$

顯而易見, $N > 1$; 根據唯一分解性, N可寫成

$$N = p_1^{a_1}\,p_2^{a_2}\,p_3^{a_3}\,\cdots\,p_n^{a_n}\,。$$

然而, $p_i \nmid N\ \ \forall i = 1, 2, 3, \cdots, n$; 我們有

$$a_i = \mathrm{ord}_{p_i}\,N = 0\ \ \forall i = 1, 2, 3, \cdots, n\,,$$

因此 $N = p_1^0\,p_2^0\,p_3^0\,\cdots\,p_n^0 = 1$。與 $N > 1$矛盾, 故得證。

在多項式環 $k[x]$ 中, 若 k爲無限體; 那麼 $x-a\ \ (\forall\, a\in k)$ 都是質多項式, 因此 $k[x]$ 當然擁有無限多個不互爲夥伴的質多項式。如果 k爲有限體; 那麼歐幾里德的論證就得出場行禮如儀, 如此這般地證明 $k[x]$ 擁有無限多個質多項式。

與此相對且值得一提的另一個極端是; 有的環僅擁有一個質元素, 茲舉例如下。令 $p \in \mathbb{Z}$爲一質數且令

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}\,, p \nmid b \right\}\,。$$

則利用 p之質性, 不難看出 $\mathbb{Z}_{(p)}$ 形成一個環。這個環僅擁有一個質元素, 那就是 p; 爲什麼呢? 只要看看這裡頭的可逆元素長的模樣, 就可了然於心。請看!

(i) 假設 $\dfrac{a}{b} \in \mathbb{Z}_{(p)}$ 是一個可逆元素, 那麼就存在 $\dfrac{c}{d} \in \mathbb{Z}_{(p)}$ 使得 $\dfrac{a}{b}\cdot\dfrac{c}{d} = 1$。所以 $ac = bd$, 因而得到 $p \nmid a$; 這是因爲 $p \nmid b$ 以及 $p \nmid d$, 再加上 p 之質性所致。

(ii) 反過來, 若 $\dfrac{a}{b} \in \mathbb{Z}_{(p)}$且 $p \nmid a$; 那麼我們馬上有 $\dfrac{b}{a} \in \mathbb{Z}_{(p)}$ 且 $\dfrac{a}{b}\cdot\dfrac{b}{a} = 1$, 故得證 $\dfrac{a}{b}$ 是一個可逆元素。

所以 $\mathbb{Z}_{(p)}$ 的可逆元素集就是

$$\mathbb{Z}_{(p)}^{\times} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}\,,\ \ p \nmid a\ \ \text{且}\ \ p \nmid b \right\}\,。$$

參考文獻

1. Agrawal, Manindra/Kayal, Neeraj/Saxena, Nitin: "PRIMES is in P," *Annals of Math* 160 (2004), 781-793.
http://www.cse.iitk.ac.in/news/primality.html
2. Apostol, Tom M.: *Introduction to Analytic Number Theory*, UTM, Springer-Verlag, New York, First Edition, 1976, Corr. Fifth Printing, 1998.
3. Hardy, G./ Wright E.: *An Introduction to the Theory of Numbers*, Fifth edition, Oxford University Press, 1979.
4. Hardy, G.H.: *A Course of Pure Mathematics*, Cambridge Mathematical Library, 1993 (First published in 1908).
5. Hardy, G.H.: *A Mathematician's Apology*, Cambridge University Press, London, 1940. 摘要見網頁 `http://en.wikipedia.org/wiki/A_Mathematician%27s_Apology`
6. Ireland, Kenneth F./Rosen, Michael I.: *A Classical Introduction to Modern Number Theory*, Volume 84 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, Second Edition, 1990, Corr. Fifth Printing, 1998.
7. 質數網頁 `http://www.utm.edu/research/primes/largest.html`
8. 沈淵源: 密碼學之旅 全華圖書有限公司, 2006.

—本文作者任教私立東海大學數學系—