感受伽羅瓦：整數與多項式

在前面各章，我們介紹了一些求解具體多項式方程的方法。不過，如要對多項式方程的求解問題有更深入的了解，便不能不從「抽象代數學」(Abstract Algebra) 的角度研究多項式。抽象代數學的研究目標就是找出不同數學對象之間的共同性，為讓讀者由淺入深地了解抽象代數學，本章首先從整數(integer) 與多項式(polynomial) 的共同性開始說起。

整數是我們熟悉的數系，它由正整數 (又稱「自然數」natural number)、0 和負整數組成，數學家一般把由整數組成的集合記作 $\mathbb{Z}$。多項式則是指具有以下形式的數式 (其中 n 是正整數或 0)：

$$a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n \qquad (1)$$

上式把多項式的項按冪次從小到大排列，是為了使上式與下列包含求和 (summation) 符號 $\sum$ 的濃縮形式一致：

$$\sum_{i=0}^{n} a_ix^i \qquad (2)$$

但在寫出具體的多項式時，本文會沿用一般人的習慣，把多項式的項按冪次從大到小排列。在中學數學中，上式中的 x 一般稱為「變項」(variable)，這實質上把上述多項式視為函數。但在抽象代數學中，多項式並不總被看成函數，因此這個 x 實際只是一個「佔位符號」(placeholder)，並被稱為不定元(indeterminate)。事實上，(1) 也可寫成以下形式：

$$(a_0, a_1, a_2, \ldots, a_{n-1}, a_n)$$

(1) 中的 a_i 稱為「係數」(但在中學數學中，a_0 一般不稱為係數，而稱為「常數項」)。多項式的係數可以從各種數系中取值。為免過於抽象，本章只討論以有理數作為係數的多項式。以下我們把以有理數作為係數並以 x 作為不定元的多項式的集合記作 $\mathbb{Q}[x]$[1]，其中 $\mathbb{Q}$ 代表有理數集。

[1]這裡必須使用方括號 [ ] 而不可使用圓括號 ( )，這是因為 $\mathbb{Q}(x)$ 另有所指，讀者會在以後的章節看到這一點。

整數與有理係數多項式雖然是兩種很不同的數學對象，但兩者其實有很多共同特性。我們知道對任意兩個整數進行加法、減法和乘法運算，所得結果仍是整數；但如把一個整數除以另一個非零整數，所得結果卻不一定是整數，例如 $\frac{1}{2}$ 便不是整數，數學家把整數的上述特性稱為整數對加法、減法和乘法運算的封閉性(closure)。

對有理係數多項式也可以進行加法、減法和乘法運算，我們在中學時期便已學習多項式的加、減、乘運算，以下我們以較形式化的方式表達這些運算。設 $f = \sum_{i=0}^{m} a_i x^i$ 和 $g = \sum_{i=0}^{n} b_i x^i$ 為有理係數多項式 (即 $\mathbb{Q}[x]$ 的成員)，那麼

$$f \pm g = \sum_{i=0}^{\max(m,n)} (a_i \pm b_i) x^i$$

上式的意思是把兩個多項式相加減，就是把這兩個多項式中有相同冪次的項的係數相加減。上式所包含的 $\max(m,n)$ 代表 m、n 這兩個數中較大的一個，這是為了使上式適用於 $m \neq n$ 的情況。舉例說，設 $f = \frac{3}{4}x^2 - 17x + 3$ 和 $g = \frac{1}{3}x - 5$，那麼由於 $\max(2,1) = 2$ 而 g 可以寫成 $g = 0x^2 + \frac{1}{3}x - 5$，我們有

$$\begin{aligned} f + g &= \left(\frac{3}{4}x^2 - 17x + 3\right) + \left(0x^2 + \frac{1}{3}x - 5\right) \\ &= \left(\frac{3}{4} + 0\right)x^2 + \left(-17 + \frac{1}{3}\right)x + (3 - 5) \\ &= \frac{3}{4}x^2 - \frac{50}{3}x - 2 \end{aligned}$$

多項式乘法的定義如下：

$$\begin{aligned} fg &= \sum_{k=0}^{m+n} c_k x^k, \\ \text{其中 } c_k &= \sum_{i+j=k} a_i b_j \\ &= a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 \end{aligned}$$

上式看似很複雜，其實只是把我們在中學時代學習的多項式乘法以形式化方式表達的結果。舉例說，設 $f = \frac{3}{4}x^2 - 17x + 3$ 和 $g = \frac{1}{3}x - 5$，那麼

$$\begin{aligned} fg &= \left(\frac{3}{4}x^2 - 17x + 3\right)\left(\frac{1}{3}x - 5\right) \\ &= \left(\left(\frac{3}{4}\right)\left(\frac{1}{3}\right)\right)x^3 + \left((-17)\left(\frac{1}{3}\right) + \left(\frac{3}{4}\right)(-5)\right)x^2 \end{aligned}$$

$$
\begin{aligned}
&+\left((3)\left(\frac{1}{3}\right)+(-17)(-5)\right)x+(3)(-5)\\
=\;&\frac{1}{4}x^3-\frac{113}{12}x^2+86x-15
\end{aligned}
$$

根據以上公式，對 $\mathbb{Q}[x]$ 的成員 f 和 g 進行加法、減法和乘法運算，所得多項式的係數是 f 和 g 的係數相加、相減和相乘的結果，所以也是有理數，由此可知有理係數多項式對加法、減法和乘法運算也滿足封閉性。跟整數一樣，把一多項式除以另一非零多項式 (即並非所有係數都等於 0 的多項式)，所得結果不一定是多項式。舉例說，設 $f=\frac{3}{4}x^2-17x+3$ 和 $g=\frac{1}{3}x-5$，那麼 $\frac{f}{g}$ 不是多項式。

整數的運算具有一系列特性，設 a、b 和 c 為任意整數，那麼

(i) $(a+b)+c=a+(b+c)$，即加法具有結合性(associativity)

(ii) $(ab)(c)=(a)(bc)$，即乘法具有結合性

(iii) $a+b=b+a$，即加法具有交換性(commutativity)

(iv) $ab=ba$，即乘法具有交換性

(v) 存在整數 0 (稱為加法單位元(identity)) 使得 $a+0=0+a=a$

(vi) 存在整數 1 (稱為乘法單位元) 使得 $(a)(1)=(1)(a)=a$

(vii) 對於每個整數 a，存在整數 $-a$ (稱為其加法逆元(inverse))，使得 $a+(-a)=(-a)+a=0$

(viii) $a(b+c)=ab+ac$，即乘法對加法具有分配性(distributivity)

請注意減去某個整數實質上是加上該整數的加法逆元，即 $a-b=a+(-b)$，所以整數的減法實質上也是一種加法；而且由於每個整數都有另一個整數作為其加法逆元，所以整數的減法也滿足封閉性。至於除法，容易看到對於任意非零整數 a，其乘法逆元就是 $\frac{1}{a}$ (因為 $(a)(\frac{1}{a})=(\frac{1}{a})(a)=1$)，但由於 $\frac{1}{a}$ 不一定是整數，並非每個整數都有乘法逆元，所以整數的除法運算並不滿足封閉性。

如果把上述特性中的 a、b 和 c 看成 $\mathbb{Q}[x]$ 的成員，那麼上述特性仍然成立。舉例說，在 $\mathbb{Q}[x]$ 中，0 (即 $0+0x+0x^2+\cdots$) 和 1 (即 $1+0x+0x^2+\cdots$) 分別起著加法單位元和乘法單位元的作用；而若 $f=\sum_{i=0}^{m}a_ix^i$ 為有理係數多項式，則 $-f=\sum_{i=0}^{m}-a_ix^i$ 就是其加法逆元。跟整數相同，對於任意非零多項式 f，其乘法逆元就是 $\frac{1}{f}$，但由於 $\frac{1}{f}$ 不一定是多項式，並非每個多項式都有乘法逆元，所以多項式的除法運算並不滿足封閉性。

前面說過整數的除法運算並不滿足封閉性，這是就「整除」(即不容許出現餘數) 的情況來說的。但我們在小學學到的除法是容許出現餘數的，只要除數不是 0，這種除法總是能夠進行，而且所得商數和餘數都是整數。不過，如果對餘數不加限制，這種除法的結果可以並不唯一。舉例說，$(-13)\div(-3)$ 的結果，可以說成商數是 4，餘數是 -1；也可說成商數是 5，餘數是 2。為避免這種情況，可以規定餘數必須是 0 或者正整數，而且其數值小於除數的絕對值。根據此一規定，$(-13)\div(-3)$ 應以 5 為商數，2 為餘數，因為 $0\le 2<|-3|$ (其中 $|-3|$ 代表 -3 的絕對值，即 3)。我們有以下定理保證進行上述除法必能取得所需結果。

定理 1 (整數的除法算法Division Algorithm)：給定整數 a (稱為被除數 dividend) 和 b (稱為除數 divisor)，其中 $b\neq 0$，存在唯一的一對整數 q (稱為商數 quotient) 和 r (稱為餘數 remainder)，使得 $a=bq+r$ 並且 $0\le r<|b|$。

有趣的是，可以把上述這種除法推廣至 $\mathbb{Q}[x]$ 的成員，但這裡存在一個困難，我們沒有「多項式絕對值」的概念。不過，「絕對值」(absolute value) 其實只是對整數的一種度量，如果可以為多項式定義一種度量，便可把這個度量當作多項式的「絕對值」。數學家定義了一個度量，稱為多項式的次數(degree)。設 f 為多項式，以下把 f 的次數記作 $\deg(f)$。若 $f\neq 0$，則 $\deg(f)$ 等於 f 中具有非零係數的最高冪次項的冪次；若 $f=0$，則 $\deg(f)=-\infty$[2]。舉例說，設 $f=7x^8-5x^3+3$，則 $\deg(f)=8$。把次數視為多項式的絕對值，便可把「定理 1」推廣到 $\mathbb{Q}[x]$ 的成員，即有以下定理。

定理 2 (多項式的除法算法)：給定 $\mathbb{Q}[x]$ 的成員 f (稱為被除式) 和 g (稱為除式)，其中 $g\neq 0$，存在唯一的一對 $\mathbb{Q}[x]$ 的成員 q (稱為商式) 和 r (稱為餘式)，使得 $f=gq+r$ 並且 $0\le\deg(r)<\deg(g)$。

舉例說，設 $f=\frac{3}{4}x^2-17x+3$ 和 $g=\frac{1}{3}x-5$，那麼由於 $\deg(g)=1<2=\deg(f)$，容易看到 $g\div f$ 的結果是：商式為 0，餘式為 $\frac{1}{3}x-5$。如要求 $f\div g$，可以進行長除法如下：

$$
\begin{array}{r}
\frac{4}{9}x \quad -\frac{69}{4} \\
\hline
\frac{1}{3}x-5\ \big)\ \frac{3}{4}x^2 \quad -17x \quad +3 \\
\frac{3}{4}x^2 \quad -\frac{45}{4}x \\
\hline
\qquad\quad -\frac{23}{4}x \quad +3 \\
\qquad\quad -\frac{23}{4}x \quad +\frac{345}{4} \\
\hline
\qquad\qquad\quad -\frac{333}{4}
\end{array}
$$

由此可知 $f\div g$ 的結果是：商式為 $\frac{4}{9}x-\frac{69}{4}$，餘式為 $-\frac{333}{4}$，這個餘式的次數是 0，小於除式的次數 1。

[2]有些人把 $\deg(0)$ 定義為 -1。

請注意即使被除式和除式都是以整數作為係數的多項式 (這類多項式組成的集合可記作 $\mathbb{Z}[x]$)，進行上述除法運算所得的商式和餘式也不一定是 $\mathbb{Z}[x]$ 的成員。舉例說，若 $f = x^2 + 1$ 和 $g = 2x$，則 $f \div g$ 的結果是：商式為 $\frac{1}{2}x$，餘式為 1，其中商式不是 $\mathbb{Z}[x]$ 的成員。換句話說，如把「定理 2」中的 $\mathbb{Q}[x]$ 改為 $\mathbb{Z}[x]$，該定理不成立。這就是本文採用 $\mathbb{Q}[x]$ 而非 $\mathbb{Z}[x]$ 作為 $\mathbb{Z}$ 的對應概念的原因。

與整數除法相關的概念還有整除和因數等。設有整數 a 和 b，我們說 b 整除(divide) a (記作 $b \mid a$) 當且僅當存在整數 n 使得 $a = bn$，在此情況下，b 和 n 稱為 a 的因數(factor)。設有兩個整數 a 和 b，其中至少有一個不是 0，它們各自有一系列因數，其中如果有某個整數 c 同時是 a 和 b 的因數，則 c 稱為 a 和 b 的公因數(common factor)。由於 1 和 -1 能整除任何整數，所以 a 和 b 至少有兩個公因數：1 和 -1。在 a 和 b 的公因數中最大的正整數稱為 a 和 b 的最大公因數(highest common factor)，記作 $\gcd(a, b)$[3]。由於對任何整數 n，都有 $0 = n \times 0$，所以任何整數都是 0 的因數，因此當 a 和 b 都是 0 時，任何整數都是它們的公因數，$\gcd(0, 0)$ 沒有定義。如果 $\gcd(a, b) = 1$，則稱 a 和 b 互質(coprime 或 relatively prime)。

整數 a 和 b 的最大公因數具有以下性質：它能被 a 和 b 的任何公因數整除。事實上，有些人採用以下最大公因數的定義：整數 d 是 a 和 b 的最大公因數，當且僅當 (i) d 是正整數；(ii) $d \mid a$ 並且 $d \mid b$；(iii) 若有 $c \mid a$ 並且 $c \mid b$，則 $c \mid d$。

為求 $\gcd(a, b)$，可以先求 a 和 b 的所有因數，然後再從中找出最大的公因數，但當 a 和 b 的絕對值很大時，這種方法很費時。幸好古人早已找出一種求 $\gcd(a, b)$ 的簡單方法，稱為歐幾里得算法(Euclidean Algorithm)(亦即我國的「輾轉相除法」)，其步驟如下。首先取 a 和 b 的絕對值，比較兩者的大小，並運用前述的除法算法，求較大數除以較小數的餘數 r_1。如果 $r_1 = 0$，那麼 $\gcd(a, b)$ 等於上述運算中的除數；否則比較上述運算中的除數與 r_1 的大小，並運用除法算法，求較大數除以較小數的餘數 r_2。如果 $r_2 = 0$，那麼 $\gcd(a, b)$ 等於上述運算中的除數；否則比較上述運算中的除數與 r_2 的大小，並運用除法算法，求較大數除以較小數的餘數 r_3，如是者繼續下去，直至出現一次除法運算的餘數是 0，那麼 $\gcd(a, b)$ 等於最後一次除法運算中的除數。

[3]gcd 是 greatest common divisor 的縮寫，請注意「因數」有兩個英文名稱：factor 和 divisor (亦可譯作「約數」)。由於 factor 一詞在多項式中較通用 (例如有 factorization、Factor Theorem 等概念)，本網頁採用 factor 作為「因數」的英文名稱。按照此一約定，本應使用 hcf 作為「最大公因數」的縮寫，但因數學界習用 gcd 此一縮寫，這裡惟有從俗。

接下來讓我們用上述方法求 $\gcd(1071, 462)$。首先計算 $1071 \div 462$，由於

$$1071 = 462 \times 2 + 147 \qquad (3)$$

第一次除法運算的除數是 462，餘數是 147。接著計算 $462 \div 147$，由於

$$462 = 147 \times 3 + 21 \qquad (4)$$

第二次除法運算的除數是 147，餘數是 21。接著計算 $147 \div 21$，由於

$$147 = 21 \times 7 + 0 \qquad (5)$$

第三次除法運算的除數是 21，餘數是 0，由此可知 $\gcd(1071, 462) = 21$。

某兩個整數的最大公因數有一個有趣特性：它可以表達為該兩個整數的「線性組合」(linear combination)，此即以下定理的內容。

定理 3：設 a 和 b 為整數，其中至少有一個不是 0，則存在兩個整數 c 和 d，使得 $\gcd(a, b) = ac + bd$。

利用歐幾里得算法的中間計算結果，可容易求得上述定理中的整數 c 和 d。以上述的 $\gcd(1071, 462) = 21$ 為例，先後利用 (4) 和 (3)，可以計算出：

$$\begin{aligned} \gcd(1071, 462) &= 462 - 147 \times 3 \\ &= 462 - (1071 - 462 \times 2) \times 3 \\ &= 1071 \times (-3) + 462 \times 7 \end{aligned}$$

上述概念也適用於 $\mathbb{Q}[x]$ 的成員。舉例說,我們有 $(2x-1) \mid \left(20x^3 - 2x^2 - 5x + \frac{1}{2}\right)$，因為 $20x^3 - 2x^2 - 5x + \frac{1}{2} = (2x - 1)\left(10x^2 + 4x - \frac{1}{2}\right)$。接著討論多項式的最大公因式，前面我們規定整數的最大公因數必須是正整數，這是為了使最大公因數具有唯一性。對於多項式，如要確保唯一性，可以規定最大公因式必須是首一多項式(monic polynomial)，即最高冪次項的係數為 1 的多項式，例如 $x^3 - 100x + \frac{4}{7}$ 便是首一多項式，1 也是首一多項式。

以下是最大公因式的定義：設有 $\mathbb{Q}[x]$ 的成員 f 和 g，其中至少有一個不是 0，則 $\mathbb{Q}[x]$ 的成員 d 是 f 和 g 的最大公因式，當且僅當 (i) d 是首一多項式；(ii) $d \mid f$ 並且 $d \mid g$；(iii) 若有 $h \mid f$ 並且 $h \mid g$，則 $h \mid d$。前述的歐幾里得算法也可用來求最大公因式，不過跟整數的情況不同，開始時我們並不先將給定的多項式轉化為首一多項式，因為運用歐幾里得算法的過程並不保證每一中間計算結果都是首一多項式，所以我們留至最後才把所得結果轉化為首一多項式。

接下來讓我們用歐幾里得算法求 $\gcd\left(20x^3-2x^2-5x+\frac{1}{2},4x^3-x\right)$。由於給定的兩個多項式的次數都是 3，可以任選其中一個除以另一個，例如 $\left(20x^3-2x^2-5x+\frac{1}{2}\right)\div(4x^3-x)$，由於

$$20x^3-2x^2-5x+\frac{1}{2}=(4x^3-x)(5)+\left(-2x^2+\frac{1}{2}\right)\qquad(6)$$

第一次除法運算的除式是 $4x^3-x$，餘式是 $-2x^2+\frac{1}{2}$。接著計算 $(4x^3-x)\div\left(-2x^2+\frac{1}{2}\right)$，由於

$$4x^3-x=\left(-2x^2+\frac{1}{2}\right)(-2x)+0\qquad(7)$$

第二次除法運算的除式是 $-2x^2+\frac{1}{2}$，餘式是 0。為把 $-2x^2+\frac{1}{2}$ 轉化為首一多項式，可把該多項式乘以 $-\frac{1}{2}$，得

$$\left(-2x^2+\frac{1}{2}\right)\left(-\frac{1}{2}\right)=x^2-\frac{1}{4}\qquad(8)$$

由此得 $\gcd\left(20x^3-2x^2-5x+\frac{1}{2},4x^3-x\right)=x^2-\frac{1}{4}$。

類似整數的情況，某兩個多項式的最大公因式也可以表達為該兩個多項式的線性組合，此即以下定理的內容。

定理 4：設 f 和 g 為 $\mathbb{Q}[x]$ 的成員，其中至少有一個不是 0，則存在兩個 $\mathbb{Q}[x]$ 的成員 h 和 i，使得 $\gcd(f,g)=fh+gi$。

利用歐幾里得算法的中間計算結果，同樣可以求得上述定理中的多項式 h 和 i。以上述的 $\gcd\left(20x^3-2x^2-5x+\frac{1}{2},4x^3-x\right)=x^2-\frac{1}{4}$ 為例，先後利用 (8) 和 (6)，可以計算出：

$$\begin{aligned}
&\gcd\left(20x^3-2x^2-5x+\frac{1}{2},4x^3-x\right)\\
=\;&\left(-2x^2+\frac{1}{2}\right)\left(-\frac{1}{2}\right)\\
=\;&\left(\left(20x^3-2x^2-5x+\frac{1}{2}\right)-(4x^3-x)(5)\right)\left(-\frac{1}{2}\right)\\
=\;&\left(20x^3-2x^2-5x+\frac{1}{2}\right)\left(-\frac{1}{2}\right)+(4x^3-x)\left(\frac{5}{2}\right)
\end{aligned}$$

最後要介紹整數的另一種特性，為此先要引入零因子(zero divisor) 的概念。零因子是指符合以下條件的非零整數 a：存在非零整數 b 使得 $ab=0$，我

們有以下定理。

定理 5：設 a、b 和 c 為整數，那麼以下三個等價命題成立。

(i) 任何非零整數都不是零因子

(ii) 若 $ab = 0$，則 $a = 0$ 或 $b = 0$

(iii) 若 $ca = cb$ 並且 $c \neq 0$，則 $a = b$

有些人可能覺得上述定理所提的都是一些顯而易見的事實，沒有必要以定理的形式表述出來，例如 (iii)(又稱約簡律cancellation law) 在中學不是已經學過了嗎？假設 (iii) 的前提成立，把等號左右兩端的非零整數 c 同時約去，不就得到所需結論嗎？可是這裡的所謂「約去 c」，其實是指「除以 c」，亦即「乘以 c 的乘法逆元」，但如前所述，並非每個整數都有乘法逆元，因此若僅從整數的前述性質 (i) — (viii) 考慮，上述「約簡律」其實並非顯而易見。

事實上，上述定理的 (iii) 可以從 (ii) 推導出來，這是因為如果 $ca = cb$，那麼 $ca - cb = 0$，根據整數乘法對加法的分配性，這等於 $c(a - b) = 0$，由此根據 (ii)，必有 $c = 0$ 或 $a - b = 0$，但因假設了 $c \neq 0$，故必有 $a - b = 0$，即 $a = b$。由此可見，雖然並非每個整數都有乘法逆元，但因整數滿足上述定理的 (ii)，所以上述約簡律成立。

上述零因子的概念也適用於 $\mathbb{Q}[x]$ 的成員。事實上，如把「定理 5」中的「整數」改為「$\mathbb{Q}[x]$ 的成員」，定理仍然成立。由此我們有以下定理。

定理 6：設 f、g 和 h 為 $\mathbb{Q}[x]$ 的成員，那麼以下三個等價命題成立。

(i) $\mathbb{Q}[x]$ 中的任何非零成員都不是零因子

(ii) 若 $fg = 0$，則 $f = 0$ 或 $g = 0$

(iii) 若 $hf = hg$ 並且 $h \neq 0$，則 $f = g$

$\mathbb{Z}$ 與 $\mathbb{Q}[x]$ 的成員在整除性和因數／式方面尚有其他共同性，這將留待下章介紹。

連結至數學專題
連結至周家發網頁