感受伽羅瓦：環及其子類

我們在《感受伽羅瓦：整數與多項式》中介紹了整數 ($\mathbb{Z}$) 和有理係數多項式 ($\mathbb{Q}[x]$) 的一些共有性質，$\mathbb{Z}$ 和 $\mathbb{Q}[x]$ 之所以具有共通性，是因為這兩者屬於同一類代數結構。本章主旨是介紹當今抽象代數學所研究的一些代數結構－環及其子類。

簡言之，代數結構是一個集合 S 加上一些封閉「運算」(operation) 所組成的結構，這裡的集合是指由某些數學對象 (例如整數、多項式、矩陣等) 所組成的集合，封閉運算則是指以 S 中一個或多個元素作為「論元」(argument，亦稱函數的「輸入項」input) 並以 S 中的一個元素作為「值」(value，亦稱函數的「輸出項」output) 的函數。在本章，我們只考慮包含兩個二元運算(binary operation，即以兩個元素作為論元的運算) 的數學結構，並把這兩個二元運算稱為「加法」(用 $+$ 表示) 和「乘法」(用 $\times$ 表示，或用兩個元素並排放在一起，例如 ab，表示)。為了清晰表明這是一個包含兩個二元運算的數學結構，我們把這種數學結構寫成有序三元組 $(S, +, \times)$ 的形式。引入 $+$ 和 $\times$ 這兩個運算符號後，便可以把運算封閉性簡潔地定義為：設 a 和 b 為 S 中任意兩個元素，$a+b$ 和 ab 都是 S 的元素。

除了運算封閉性外，S 中的元素還可能具有其他性質，根據 S 中元素所具有的性質，可以把 S 界定為某種數學結構，以下首先列出各種可能性質 (在抽象代數學上這些性質又稱為公理(axiom))，在以下公理中，a、b 和 c 為 S 中任意元素：

(i) $(a+b)+c = a+(b+c)$，即加法具有結合性

(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

(iv) 存在加法單位元 (記作 0) 使得 $a+0 = 0+a = a$

(v) 對於每個元素 a，存在其加法逆元 (記作 $-a$)，使得 $a+(-a) = (-a)+a = 0$

(vi) $a(b+c) = ab+ac$，即乘法對加法具有分配性

(vii) $ab = ba$，即乘法具有交換性

(viii) 存在乘法單位元 (記作 1) 使得 $(a)(1) = (1)(a) = a$

(ix) 若 $ab = 0$，則 $a = 0$ 或 $b = 0$

(x) 對於每個元素 a，若 $a \neq 0$，則存在其乘法逆元 (記作 a^{-1})，使得 $(a)(a^{-1}) = (a^{-1})(a) = 1$

請注意上列公理跟《感受伽羅瓦：整數與多項式》中列舉的整數性質在次序上不盡相同，而且該網頁沒有 (x) 這個性質，(ix) 則是作為「定理 5」出現於該網頁中。

我們在《感受伽羅瓦：整數與多項式》和《感受伽羅瓦：因子分解》中分別介紹了「零因子」和「單位」的概念，把這兩個概念推廣應用於上述集合 S，那麼「零因子」是指存在另一個非零元素 b 使得 $ab = 0$ 的非零元素 a，「單位」則是指有乘法逆元的非零元素。根據上述定義，上述公理 (ix) 等價於「S 中所有元素都不是零因子」，公理 (x) 則等價於「S 中所有非零元素都是單位」。

在抽象代數學上，對滿足某些公理組合的代數結構給予一些特殊名稱，現把這些代數結構的名稱以及它們所滿足的公理列於下表：

名稱	所滿足的公理
環(ring)	(i)-(vi)
交換環(commutative ring)	(i)-(vii)
帶乘法單位元的環(ring with unity)	(i)-(vi), (viii)
不含零因子的環(ring with no zero divisors)	(i)-(vi), (ix)
整環(integral domain)	(i)-(ix)
除環(division ring，又稱「反對稱域」skew field)	(i)-(vi), (viii)-(x)
域(field)	(i)-(x)

從以上定義可以看到，環是包含「加」和「乘」這兩種二元運算的最基本的代數結構，上述其他代數結構都是在環之上再加上一條或多條公理而得的代數結構，因此都可看成環的子類。

根據環所滿足的公理，我們可以證明環中的元素滿足某些基本性質，現把這些性質總結為以下定理。

定理 1：設 $(R, +, \times)$ 為環，並且 $a, b, c \in R$，則

(i) $(a)(0) = (0)(a) = 0$

(ii) $(a)(-b) = (-a)(b) = -(ab)$

(iii) $(-a)(-b) = ab$

上述定理所陳述的事實似乎是我們從小學起便已熟悉的實數乘法運算的事實，但請注意在上述定理中，R 並不限於實數集，而可以是任何滿足上述公理 (i)-(vi) 的數學對象的集合。因此上述定理揭示了一個重要現象：某些適用於實數 (或有理數、整數) 運算的事實也適用於一般的環。

上述某些公理之間存在邏輯依存關係，例如公理 (iv) 是 (v) 的必要條件，而公理 (viii) 則是 (x) 的必要條件，這些都是顯而易見的 (如果沒有加／乘法單位元，根本無法定義加／乘法逆元)。此外，還有一個不太明顯的依存關係：如果集合 S 滿足公理 (x)，則 S 也必滿足公理 (ix)，這是因為若 S 滿足公理 (x)，則 S 的所有非零元素都有乘法逆元，現在設 $ab = 0$ 並且 $a \neq 0$，那麼 a 有乘法逆元 a^{-1}，由此必有

$$\begin{array}{rcll} (a^{-1})(ab) & = & (a^{-1})(0) & (\text{根據 } ab = 0 \text{ 此一假設}) \\ (a^{-1}a)(b) & = & (a^{-1})(0) & (\text{根據乘法的結合性}) \\ (1)(b) & = & (a^{-1})(0) & (\text{根據乘法逆元的定義}) \\ b & = & (a^{-1})(0) & (\text{根據乘法單位元的定義}) \\ b & = & 0 & (\text{根據定理 1(i)}) \end{array}$$

即若 $ab = 0$，則 $a = 0$ 或 $b = 0$。正由於存在上述依存關係，上述公理的某些組合是不合邏輯的，因而也不可能產生相應的代數結構，例如不可能出現滿足公理 (i) — (viii) 和 (x) 而不滿足公理 (ix) 的代數結構。

接下來讓我們看上述各種代數結構的例子。根據上述定義和上兩章的討論，可知 $(\mathbb{Z}, +, \times)$ 是整環，但卻並非域 (因為絕大多數整數在 $\mathbb{Z}$ 中沒有乘法逆元，所以 $(\mathbb{Z}, +, \times)$ 不滿足公理 (x))。跟 $(\mathbb{Z}, +, \times)$ 不同，$(\mathbb{Z}_p, +, \times)$ (其中 p 是質數)、$(\mathbb{Q}, +, \times)$、$(\mathbb{R}, +, \times)$ 和 $(\mathbb{C}, +, \times)$ 則都是域，這是因為這些數系中的每個非零成員都有乘法逆元，例如 2 在 $\mathbb{Z}_5$ 中的乘法逆元是 3，在 $\mathbb{Q}$、$\mathbb{R}$ 和 $\mathbb{C}$ 中的乘法逆元則都是 $\frac{1}{2}$。

多項式的情況又如何？我們有以下定理。

定理 2：設 $(F, +, \times)$ 為域，則 $(F[x], +, \times)$(即以 F 的成員作為係數的多項式組成的代數結構) 是整環。

根據上述定理和以上的討論，可知 $(\mathbb{Z}_p[x], +, \times)$(其中 p 是質數)、$(\mathbb{Q}[x], +, \times)$、$(\mathbb{R}[x], +, \times)$ 和 $(\mathbb{C}[x], +, \times)$ 都是整環。除此以外，雖然 $(\mathbb{Z}, +, \times)$ 並非域，但不難驗證 $(\mathbb{Z}[x], +, \times)$ 滿足上列公理 (i) — (ix)，所以 $(\mathbb{Z}[x], +, \times)$ 也是整環。至此我們看到，整數與有理係數多項式的共通點是兩者都構成整環。

請注意雖然 $(\mathbb{Z}_p, +, \times)$ (其中 p 是質數)、$(\mathbb{Q}, +, \times)$、$(\mathbb{R}, +, \times)$ 和 $(\mathbb{C}, +, \times)$ 是域，但相對應的 $(\mathbb{Z}_p[x], +, \times)$、$(\mathbb{Q}[x], +, \times)$、$(\mathbb{R}[x], +, \times)$ 和 $(\mathbb{C}[x], +, \times)$ 卻是整環而非域，這是因為一般非零多項式的乘法逆元不是多項式。舉例說，容易看到多項式 x 的乘法逆元是 $\frac{1}{x}$ (因為 $x \times \frac{1}{x} = \frac{1}{x} \times x = 1$)，但 $\frac{1}{x}$ 卻不是多項式 (因為 $\frac{1}{x} = x^{-1}$，而多項式不容許負冪次項)。

我們也可以從以下角度看上述數系與多項式集合的區別：在 $\mathbb{Z}_p$ (其中 p 是質數)、$\mathbb{Q}$、$\mathbb{R}$ 和 $\mathbb{C}$ 中，所有非零元素都是單位，所以這些數系都構成域。由於這些數系的每個成員都可看成 (常數) 多項式 (例如 2 既可看成一個數，也可看成一個 (常數) 多項式)，這些數系都可被看成其相應多項式集合的子集 (例如 $\mathbb{Q}$ 可被看成 $\mathbb{Q}[x]$ 的子集)，因此在 $\mathbb{Z}_p[x]$、$\mathbb{Q}[x]$、$\mathbb{R}[x]$ 和 $\mathbb{C}[x]$ 中，除了非零常數多項式外，還有很多其他非零多項式 (例如 x)，而這些多出來的多項式都不是單位，正是由於存在這些多出來的多項式，這些多項式集合不構成域。

至此我們討論了整環和域這兩個最重要的代數結構，現把這兩者的關係總結成以下定理。

定理 3：所有域都是整環，但有整環不是域。

上述定理的第一句可從上表中整環和域的定義推得 (由於域滿足公理 (i)-(x)，任何域都必然滿足公理 (i)-(ix)，所以必然是整環)；第二句則可以從上述那些不是域的整環實例 (例如 $(\mathbb{Z}, +, \times)$、$(\mathbb{Q}[x], +, \times)$ 等) 推得。

整環和域涵蓋了最常用的數系和多項式集合，但除此以外，還有一些特殊數學對象組成的集合，它們既不構成整環又不構成域，而是構成其他代數結構，以下提供一些例子。首先考慮 $(\mathbb{Z}_4, +, \times)$，容易驗證這是一個交換環，而且帶有乘法單位元 1。但 $(\mathbb{Z}_4, +, \times)$ 並不滿足公理 (ix)，這是因為在 $\mathbb{Z}_4$ 中，我們有 $2 \times 2 = 0$，而 $2 \neq 0$；$(\mathbb{Z}_4, +, \times)$ 也不滿足公理 (x)，這是因為在 $\mathbb{Z}_4$ 中，2 沒有乘法逆元。總上所述，$(\mathbb{Z}_4, +, \times)$ 是帶乘法單位元的交換環。

其次考慮由所有偶數組成的集合，以下把這個集合記作 $2\mathbb{Z}$，容易驗證這是一個交換環，而且滿足公理 (ix)。但 $(2\mathbb{Z}, +, \times)$ 並不滿足公理 (viii)，這是因為 $1 \notin 2\mathbb{Z}$；$(2\mathbb{Z}, +, \times)$ 也不滿足公理 (x)，這是因為在 $2\mathbb{Z}$ 中，所有非零成員都沒有乘法逆元。總上所述，$(2\mathbb{Z}, +, \times)$ 是不含零因子的交換環。

接著考慮由包含整數項的 2×2方陣(square matrix) 組成的集合，這是

指具有以下形式的矩陣的集合：

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

其中 a、b、c 和 d 都是整數，以下把這個集合記作 $M_2(\mathbb{Z})$，其中 M_2 代表 2×2 方陣 (又稱「二階方陣」)，$\mathbb{Z}$ 則代表這是包含整數項的矩陣。對於 $M_2(\mathbb{Z})$ 的成員，可以定義加法和乘法如下。設有以下方陣：

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \qquad (1)$$

則有

$$A + B = \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{pmatrix}$$

$$AB = \begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix}$$

可以證明 $(M_2(\mathbb{Z}), +, \times)$ 是一個環，其加法單位元 (一般記作 O 而非 0) 是

$$O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

這是因為對 $M_2(\mathbb{Z})$ 中任何成員 A，均有 $A + O = O + A = A$。$M_2(\mathbb{Z})$ 的每一個成員都有加法逆元，設 A 為如 (1) 所定義的方陣，則

$$-A = \begin{pmatrix} -a_1 & -a_2 \\ -a_3 & -a_4 \end{pmatrix}$$

讀者可自行驗證，根據上述定義，$A + (-A) = (-A) + A = O$。此外，$M_2(\mathbb{Z})$ 還有乘法單位元 (一般記作 I 而非 1)：

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

這是因為對 $M_2(\mathbb{Z})$ 中任何成員 A，均有 $AI = IA = A$。此外，還可證明 $M_2(\mathbb{Z})$ 滿足公理 (i)、(ii)、(iii) 和 (vi)，但這涉及繁冗的運算，茲從略。

可是，$(M_2(\mathbb{Z}), +, \times)$ 並不滿足公理 (vii)，這是因為矩陣乘法一般不具有交換性。舉例說，設

$$C = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, D = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}$$

則

$$CD = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}$$

$$DC = \begin{pmatrix} 23 & 34 \\ 31 & 46 \end{pmatrix}$$

在上例中，$CD \neq DC$。$(M_2(\mathbb{Z}), +, \times)$ 也不滿足公理 (ix)，舉例說，設

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, F = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

那麼

$$EF = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O$$

但 $E \neq O$ 並且 $F \neq O$。$(M_2(\mathbb{Z}), +, \times)$ 也不滿足公理 (x)，根據線性代數，一個 2×2 方陣 A 有乘法逆元當且僅當 $\det(A) \neq 0$，其中 $\det(A)$ 代表 A 的「行列式」(determinant)。設 A 為如 (1) 所定義的方陣，則

$$\det(A) = a_1 a_4 - a_2 a_3$$

當 $\det(A) \neq 0$ 時，我們有

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{pmatrix}$$

因此當 $\det(A) = 0$ 時，A^{-1} 不存在；但即使 $\det(A) \neq 0$，A^{-1} 也可能不屬於 $M_2(\mathbb{Z})$。舉例說，設

$$G = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, H = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

那麼 $\det(G) = -2$ 並且 $\det(H) = 0$，由此得

$$G^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \notin M_2(\mathbb{Z})$$

而 H^{-1} 不存在，上述結果顯示 $M_2(\mathbb{Z})$ 中並非所有非零成員都有乘法逆元。總上所述，$(M_2(\mathbb{Z}), +, \times)$ 是一個帶乘法單位元的 (非交換) 環。

接著考慮由包含偶數項的 2×2 方陣組成的集合，以下把這個集合記作 $M_2(2\mathbb{Z})$，這個集合包含以下矩陣 J (因為其中所有項都是偶數)，但不包含以下矩陣 K (因為至少有一個項 1 是奇數)：

$$J = \begin{pmatrix} 0 & 2 \\ 4 & 6 \end{pmatrix}, K = \begin{pmatrix} 1 & 2 \\ 4 & 6 \end{pmatrix}$$

容易看到跟 $(M_2(\mathbb{Z}), +, \times)$ 一樣，$(M_2(2\mathbb{Z}), +, \times)$ 也滿足公理 (i) — (vi) 但不滿足公理 (vii)、(ix) 和 (x)。跟 $(M_2(\mathbb{Z}), +, \times)$ 不同，$(M_2(2\mathbb{Z}), +, \times)$ 並不滿足公理 (viii)，這是因為 2×2 方陣的乘法單位元 I 的項中包含 1 這個奇數，所以 I 不屬於 $M_2(2\mathbb{Z})$，即 $M_2(2\mathbb{Z})$ 不包含乘法單位元。總上所述，$(M_2(2\mathbb{Z}), +, \times)$ 是一個 (非交換) 環。

最後考慮由四元數(quaternion) 組成的集合，以下記作 $\mathbb{H}$ (以紀念創造四元數的愛爾蘭數學家漢密爾頓 Hamilton)。四元數是複數的推廣，是指具有以下形式的數：

$$a + bi + cj + dk \qquad (2)$$

其中 a、b、c 和 d 是實數，i、j 和 k 則是四元數單位，且滿足以下運算關係：

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij = k \qquad ji &= -k \\ jk = i \qquad kj &= -i \\ ki = j \qquad ik &= -j \end{aligned}$$

跟複數一樣，四元數也可進行加、乘運算，其計算方法跟普通代數的同類運算很相似，只需把 i、j 和 k 當作變項處理，並加上上述運算關係。以下提供一個計算示例：

$$\begin{aligned} & (1 + 2i - 3j - 4k)(5 + 6i - 7j + 8k) \\ = \; & (1)(5) + (1)(6i) + (1)(-7j) + (1)(8k) \\ & + (2i)(5) + (2i)(6i) + (2i)(-7j) + (2i)(8k) \\ & + (-3j)(5) + (-3j)(6i) + (-3j)(-7j) + (-3j)(8k) \\ & + (-4k)(5) + (-4k)(6i) + (-4k)(-7j) + (-4k)(8k) \\ = \; & 5 + 6i - 7j + 8k + 10i - 12 - 14k - 16j \\ & - 15j + 18k - 21 - 24i - 20k - 24j - 28i + 32 \\ = \; & 4 - 36i - 62j - 8k \qquad (3) \end{aligned}$$

可以證明 $(\mathbb{H}, +, \times)$ 是一個除環，其加法單位元是 $0\,(= 0 + 0i + 0j + 0k)$，其乘法單位元則是 $1\,(= 1 + 0i + 0j + 0k)$。$\mathbb{H}$ 的每一個成員都有加法逆元，容易看到，給定如 (2) 所定義的四元數，其加法逆元為

$$-a - bi - cj - dk$$

$\mathbb{H}$ 的每一個非零成員也有乘法逆元，可以證明，給定如 (2) 所定義的四元數，其乘法逆元為

$$\frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk)$$

舉例說，根據上式，四元數 $1+2i-3j-4k$ 的乘法逆元是

$$\begin{aligned} & \frac{1}{1^2+2^2+(-3)^2+(-4)^2}(1-2i+3j+4k) \\ = \quad & \frac{1}{30}-\frac{1}{15}i+\frac{1}{10}j+\frac{2}{15}k \end{aligned}$$

讀者可自行驗證 $(1+2i-3j-4k)\left(\frac{1}{30}-\frac{1}{15}i+\frac{1}{10}j+\frac{2}{15}k\right)=\left(\frac{1}{30}-\frac{1}{15}i+\frac{1}{10}j+\frac{2}{15}k\right)(1+2i-3j-4k)=1$。此外，還可證明 $(\mathbb{H},+,\times)$ 滿足公理 (i)、(ii)、(iii) 和 (vi)，但這涉及繁冗的運算，茲從略。另外，由於 $(\mathbb{H},+,\times)$ 滿足公理 (x)，根據公理 (ix) 與 (x) 的依存關係，可知 $\mathbb{H}$ 也滿足公理 (ix)。

可是，$(\mathbb{H},+,\times)$ 並不滿足公理 (vii)，為證明這一點，我們先計算

$$\begin{aligned} & (5+6i-7j+8k)(1+2i-3j-4k) \\ = \quad & 4+68i+18j-16k \qquad (4) \end{aligned}$$

比較 (3) 和 (4)，可以看到 $(1+2i-3j-4k)(5+6i-7j+8k)\neq(5+6i-7j+8k)(1+2i-3j-4k)$。總上所述，$(\mathbb{H},+,\times)$ 是一個 (非交換) 除環。

連結至數學專題
連結至周家發網頁