感受伽羅瓦：有限域

在前面各章，我們討論了若干種域：$\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$、$\mathbb{Z}_p$ (其中 p 為正質數) 以及多種擴張域，如 $\mathbb{Q}(\sqrt{2})$、$\mathbb{Q}(\sqrt[3]{2}, \omega_3)$、$\mathbb{Q}(\pi)$ 等。按照這些域所含元素的數目，可以把這些域分為兩大類：包含無限個元素的無限域(infinite field) 和包含有限個元素的有限域(finite field)，前者的例子有 $\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$ 以及這些域上的擴張域，後者的例子有 $\mathbb{Z}_p$。由於有限域包含著人們不太熟悉的數系，對有限域的研究有助加深我們對這些數系的認識。

以下定理概括了有限域的所有可能種類。

定理 1 (伽羅瓦有限域定理Galois' Theorem on Finite Fields)：設 p 為正質數，n 為正整數，那麼存在一個包含 p^n 個元素的有限域，而且所有包含 p^n 個元素的有限域都互相同構。反過來，設 F 為有限域，那麼 F 包含 p^n 個元素，其中 p 是某正質數，n 是某正整數。

抽象代數學把上述定理中包含 p^n 個元素的有限域稱為 p^n 階伽羅瓦域(Galois Field)，並記作 $\mathrm{GF}(p^n)$。根據上述定理，可知不存在 $\mathrm{GF}(6)$，因為 6 不能表示成 p^n 的形式。此外，也可知必定存在 $\mathrm{GF}(529)$，因為 $529 = 23^2$，而 23 是正質數。

我們早在《感受伽羅瓦：環及其子類》中便已指出 $\mathbb{Z}_p$ 是包含 $p\,(= p^1)$ 個元素的有限域，即 $\mathbb{Z}_p = \mathrm{GF}(p)$，這 p 個元素是 0、1、...、$p-1$，而且這些元素的加、減、乘運算就是模 p 同餘下的加、減、乘運算，而對於非零元素的求乘法逆元運算則可用乘法運算反推而得。舉例說，如何求 $\mathbb{Z}_7$ 中 3 的乘法逆元？方法是算出 3 的各個倍數，看看哪一個在模 7 同餘下等於 1。由於 $3 \times 1 = 3$、$3 \times 2 = 6$、...、$3 \times 5 = 15$，由於 15 在模 7 同餘下等於 1，故知 $\mathbb{Z}_7$ 中 3 的乘法逆元是 5。

以上討論了 $\mathrm{GF}(p)$，$\mathrm{GF}(p^n)$ (其中 $n > 1$) 的情況又如何？在討論這些有限域前，須先引入直積(direct product) 的概念[1]。設 $(G_1, \circ_1)$、...、$(G_n, \circ_n)$ 為群，則這些群的直積，記作 $(G_1 \times \cdots \times G_n, \circ)$ 是一個群，這個群的集合

[1]在某些情況下，抽象代數學要區分兩種直積—「外直積」(external direct product) 和「內直積」(internal direct product)。但由於本文只會討論一種直積，所以這裡不作區分，

是 G_1、...、G_n 的笛卡爾積，其元素是由 G_1、...、G_n 的元素組成的有序 n 元組：

$$G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) : g_1 \in G_1, \ldots, g_n \in G_n\}$$

這個群的運算則是有序 n 元組之間的運算,其運算定義如下：設 $(g_1, \ldots, g_n)$, $(h_1, \ldots, h_n) \in G_1 \times \cdots \times G_n$，則

$$(g_1, \ldots, g_n) \circ (h_1, \ldots, h_n) = (g_1 \circ_1 h_1, \ldots, g_n \circ_n h_n)$$

根據上述定義，在計算兩個有序 n 元組的運算結果時，每個坐標各自進行運算。由於組成有序 n 元組的各個群可以各有不同性質的運算 (如加法、乘法或函數複合)，在進行有序 n 元組的運算時，可能要就不同坐標進行不同性質的運算。

可以證明上面定義的直積滿足群的定義，即其運算具有結合性，有單位元 $(e_1, \ldots, e_n)$,其中 e_1、...、e_n 分別代表 G_1、...、G_n 中的單位元,而且每個元素都有逆元。設 $(g_1, \ldots, g_n) \in G_1 \times \cdots \times G_n$, 則 $(g_1, \ldots, g_n)^{-1} = ({g_1}^{-1}, \ldots, {g_n}^{-1})$, 其中 ${g_i}^{-1}\,(1 \leq i \leq n)$ 代表 g_i 在 G_i 中的逆元。

舉例說, 從 $(\mathbb{Z}_2, +_2)$ 和 $(\mathbb{Z}_3, +_3)$, 可以構造直積 $(\mathbb{Z}_2 \times \mathbb{Z}_3, +')$, 這個直積由以下六個有序對組成：$(0,0)$、$(0,1)$、$(0,2)$、$(1,0)$、$(1,1)$、$(1,2)$，這些有序對在相加時，各個坐標各自進行不同性質的加法，其中第一坐標進行模 2 同餘下的加法 (記作 $+_2$), 第二坐標則進行模 3 同餘下的加法 (記作 $+_3$), 例如 $(1,2)+'(1,1) = (1+_2 1, 2+_3 1) = (0,0)$。容易看到,$(0,0)$ 是這個直積的單位元, 而且每個元素都有其逆元, 例如根據前面的計算, 可知 $(1,2)$ 的逆元是 $(1,1)$。

某些直積的元素雖然具有有序 n 元組的形式，但在實質上與一個單純的群 (即並非由兩個或以上的群組成的直積) 同構。以前述的 $\mathbb{Z}_2 \times \mathbb{Z}_3$ 為例, 這個直積是一個循環群，$(1,1)$ 是它的一個生成元。為證明這一點，可以列出 $(1,1)$ 的各個倍數如下 (以下用 $n \times' (1,1)$ 代表把 n 個 $(1,1)$ 進行 $+'$ 運算)：

$$\begin{aligned}
1 \times' (1,1) &= (1,1) \\
2 \times' (1,1) &= (0,2) \\
3 \times' (1,1) &= (1,0) \\
4 \times' (1,1) &= (0,1) \\
5 \times' (1,1) &= (1,2) \\
6 \times' (1,1) &= (0,0)
\end{aligned}$$

僅稱為「直積」。此外，抽象代數學上有時也使用「直和」(direct sum) 一名以指稱「直積」, 尤其當組成「直積」的群是交換群時。

上述計算顯示，$\mathbb{Z}_2 \times \mathbb{Z}_3$ 實際是一個六階循環群，由於 $\mathbb{Z}_6$ 是六階循環群的典型代表，我們有以下同構關係：

$$(\mathbb{Z}_2 \times \mathbb{Z}_3, +') \cong (\mathbb{Z}_6, +_6)$$

具備直積的概念後，便可以寫出 $\mathrm{GF}(p^n)$ 的加法部分的結構，而 $\mathrm{GF}(p^n)$ 的乘法部分則可以表述為一個循環群，如以下定理所示。

定理 2：$\mathrm{GF}(p^n)$ 的元素在加法上組成一個群，同構於直積 $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (這個直積由 n 個 $\mathbb{Z}_p$ 組成)。$\mathrm{GF}(p^n)$ 的非零元素在乘法上組成一個循環群 $\langle r \rangle$，其中 r 是這個循環群的生成元。

由於上述定理把 $\mathrm{GF}(p^n)$ 的加法和乘法結構分開處理，單憑上述定理，很難構造出 $\mathrm{GF}(p^n)$ (其中 $n > 1$) 的實例。舉例說，假設我們想構造 $\mathrm{GF}(9)$。由於 $9 = 3^2$，根據上述定理，我們知道這個域的元素在加法上組成一個群，同構於直積 $\mathbb{Z}_3 \times \mathbb{Z}_3$，現把這個直積的元素列出如下：

$$\begin{aligned} & \mathbb{Z}_3 \times \mathbb{Z}_3 \\ = \ & \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\} \end{aligned} \tag{1}$$

上列集合中的元素雖然滿足上述定理中的第一句，但卻不滿足第二句。這是因為 $\mathbb{Z}_3 \times \mathbb{Z}_3$ 只能理解為加法群，如要構造乘法群，首先要從 $\mathbb{Z}_3$ 剔除 0 這個元素，得到 $U(3) = \{1, 2\}$ (請參閱《感受伽羅瓦：群的基本概念》中有關「單位群」的介紹)，從而構造出乘法群 $U(3) \times U(3)$ (但 $U(3) \times U(3)$ 只有四個元素)，因此上列集合中的元素根本無法構成乘法群。

上述例子顯示 $\mathrm{GF}(p^n)$ 的元素雖然在加法上同構於直積 $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$，但並不等於這個直積，因此在構造 $\mathrm{GF}(p^n)$ 的實例時，我們必須另闢蹊徑，其中一個方法是借用《感受伽羅瓦：代數擴張與超越擴張》中的「定理 2」、「定理 3」和「定理 4」。根據該三個定理，若 $F(r) : F$ 是簡單代數擴張，f 是 r 的最小多項式 (即以 r 為根的次數最小的不可約首一多項式)，則 $F(a)$ 同構於擴張域 $F[x]/\langle f \rangle$，而若 $\deg(f) = n$，則

$$F(r) = \{a_{n-1}r^{n-1} + a_{n-2}r^{n-2} + \cdots + a_1 r + a_0 : a_{n-1}, a_{n-2}, \ldots, a_1, a_0 \in F\} \tag{2}$$

請注意如果 F 有 p 個元素，上述集合便有 p^n 個元素。因此如要構造 $\mathrm{GF}(p^n)$，可以先選擇一個包含 p 個元素的域 F，並在 $F[x]$ 中找出適當的不可約 n 次首一多項式 f 及其一個根 r，然後構造 $F(r)$，這個 $F(r)$ 就是所需的 $\mathrm{GF}(p^n)$。

仍以 $\mathrm{GF}(9)$ 為例，由於 $9 = 3^2$，按照上段所述方法，我們先選擇域 $\mathbb{Z}_3$，並設 f 為 $\mathbb{Z}_3[x]$ 中的不可約二次首一多項式，r 為 f 的一個根，那麼根據

(2)，我們有

$$\begin{aligned}\mathbb{Z}_3(r) &= \{ar+b : a,b \in \mathbb{Z}_3\} \\ &= \{0,1,2,r,r+1,r+2,2r,2r+1,2r+2\} \qquad (3)\end{aligned}$$

上列集合共有九個成員，正符合我們的要求。容易看到上列集合同構於 $\mathbb{Z}_3 \times \mathbb{Z}_3$ (同構函數為 $\theta_1(ar+b) = (a,b)$)，滿足上面「定理 2」的第一句。

可是並非任何不可約二次首一多項式的根都能作為上面「定理 2」第二句所提及的生成元。為找出這個生成元，我們可以先列出 $\mathbb{Z}_3[x]$ 中所有不可約二次首一多項式 f，然後就每個 f 的根 r 檢查 r 能否生成 (3) 中的八個非零成員。

為列出 $\mathbb{Z}_3[x]$ 中所有不可約二次首一多項式，可以首先寫出所有形如 $(x+a)(x+b)$ (其中 $a,b \in \mathbb{Z}_3$) 的多項式，這些多項式都是可約二次首一多項式，例如由於在 $\mathbb{Z}_3[x]$ 下，$x^2+2 = (x+1)(x+2)$，可知 x^2+2 在 $\mathbb{Z}_3[x]$ 中是可約二次首一多項式。用上述方法剔除所有可約二次首一多項式後，便可得到 $\mathbb{Z}_3[x]$ 中所有不可約二次首一多項式如下：x^2+1、x^2+x+2 和 x^2+2x+2。

接著要逐一考慮上述三個多項式，首先考慮 x^2+1，並把其根記作 r_1，因此 r_1 滿足等式 ${r_1}^2+1=0$，即 ${r_1}^2 = 2$ (請注意在 $\mathbb{Z}_3$ 下，$-1=2$)。以下列出 r_1 的各個冪次，看看它能否生成 (3) 中的八個非零成員：

$$\begin{aligned}{r_1}^1 &= r_1 \\ {r_1}^2 &= 2 \\ {r_1}^3 &= ({r_1}^2)(r_1) = 2r_1 \\ {r_1}^4 &= ({r_1}^3)(r_1) = 2({r_1}^2) = (2)(2) = 1\end{aligned}$$

根據上述結果，可以預見接下來的 r_1 冪次只會重覆出現 r_1、2、$2r_1$ 和 1 這四個結果，因此 r_1 不能生成 (3) 中的八個非零成員。

其次考慮 x^2+x+2，並把其根記作 r_2，因此 r_2 滿足等式 ${r_2}^2+r_2+2=0$，即 ${r_2}^2 = 2r_2+1$ (請注意在 $\mathbb{Z}_3$ 下，$-1=2, -2=1$)。以下列出 r_2 的各個冪次：

$$\begin{aligned}{r_2}^1 &= r_2 \\ {r_2}^2 &= 2r_2+1 \\ {r_2}^3 &= (2r_2+1)(r_2) = 2{r_2}^2+r_2 = 2(2r_2+1)+r_2 = 2r_2+2 \\ {r_2}^4 &= (2r_2+2)(r_2) = 2{r_2}^2+2r_2 = 2(2r_2+1)+2r_2 = 2 \\ {r_2}^5 &= (2)(r_2) = 2r_2 \\ {r_2}^6 &= (2r_2)(r_2) = 2{r_2}^2 = 2(2r_2+1) = r_2+2 \\ {r_2}^7 &= (r_2+2)(r_2) = {r_2}^2+2r_2 = 2r_2+1+2r_2 = r_2+1 \\ {r_2}^8 &= (r_2+1)(r_2) = {r_2}^2+r_2 = 2r_2+1+r_2 = 1\end{aligned}$$

上述結果顯示 r_2 能夠生成 (3) 中的八個非零成員，由此可知以下集合是我們要求的 GF(9)：

$$\mathbb{Z}_3(r_2) = \{ar_2 + b : a, b \in \mathbb{Z}_3; {r_2}^2 = 2r_2 + 1\}$$

請注意上述集合的元素實質上就是 (3) 所列的元素，只不過上述集合標明 r_2 須滿足等式 ${r_2}^2 = 2r_2 + 1$，正是這個性質使得 r_2 可以成為「定理 2」中第二句所提及的生成元。

由於 $\mathbb{Z}_3(r_2)$ 是域，它的元素可以進行四則運算，其中加減法須滿足 $\mathbb{Z}_3$ 上的加減法法則，而上面列出的 r_2 的冪次則可以用來把乘除法轉化為 r_2 冪次的加減法，而這個冪次上的加減法須滿足 $\mathbb{Z}_8$ 上的加減法法則 (因為 ${r_2}^8 = 1$)，以下是一個計算實例：

$$\begin{aligned} \frac{(1) + (2r_2 + 2)}{r_2 + 2} &= \frac{2r_2}{r_2 + 2} \\ &= \frac{{r_2}^5}{{r_2}^6} \\ &= {r_2}^{5-6} \\ &= {r_2}^7 \\ &= r_2 + 1 \qquad (4) \end{aligned}$$

最後考慮 $x^2 + 2x + 2$，並把其根記作 r_3，因此 r_3 滿足等式 ${r_3}^2 + 2r_3 + 2 = 0$，即 ${r_3}^2 = r_3 + 1$。以下列出 r_3 的各個冪次：

$$\begin{aligned} {r_3}^1 &= r_3 \\ {r_3}^2 &= r_3 + 1 \\ {r_3}^3 &= (r_3 + 1)(r_3) = {r_3}^2 + r_3 = r_3 + 1 + r_3 = 2r_3 + 1 \\ {r_3}^4 &= (2r_3 + 1)(r_3) = 2{r_3}^2 + r_3 = 2(r_3 + 1) + r_3 = 2 \\ {r_3}^5 &= (2)(r_3) = 2r_3 \\ {r_3}^6 &= (2r_3)(r_3) = 2{r_3}^2 = 2(r_3 + 1) = 2r_3 + 2 \\ {r_3}^7 &= (2r_3 + 2)(r_3) = 2{r_3}^2 + 2r_3 = 2r_3 + 2 + 2r_3 = r_3 + 2 \\ {r_3}^8 &= (r_3 + 2)(r_3) = {r_3}^2 + 2r_3 = r_3 + 1 + 2r_3 = 1 \end{aligned}$$

上述結果顯示 r_3 也能夠生成 (3) 中的八個非零成員，由此可知以下集合也是我們要求的 GF(9)：

$$\mathbb{Z}_3(r_3) = \{ar_3 + b : a, b \in \mathbb{Z}_3; {r_3}^2 = r_3 + 1\}$$

我們同樣可以運用前述方法對這個域上的元素進行四則運算。

至此我們發現了兩個可以充當 GF(9) 的域：$\mathbb{Z}_3(r_2)$ 和 $\mathbb{Z}_3(r_3)$，根據「定理 1」，這兩個域同構，這個同構關係可以用以下函數表示：

$$\theta_2(ar_2 + b) = 2ar_3 + b \qquad (5)$$

接下來讓我們用 (4) 的計算結果驗證上述同構關係，根據同構的定義，應該有

$$\frac{\theta_2(1) + \theta_2(2r_2 + 2)}{\theta_2(r_2 + 2)} = \theta_2\left(\frac{(1) + (2r_2 + 2)}{r_2 + 2}\right)$$

由於 $\theta_2(1) = 1$，$\theta_2(2r_2 + 2) = (2)(2)(r_3) + 2 = r_3 + 2$，$\theta_2(r_2 + 2) = 2r_3 + 2$ 和 $\theta_2(r_2 + 1) = 2r_3 + 1$，根據 (4) 的計算結果，應有

$$\frac{(1) + (r_3 + 2)}{2r_3 + 2} = 2r_3 + 1 \qquad (6)$$

現在進行以下計算：

$$\begin{aligned} \frac{(1) + (r_3 + 2)}{2r_3 + 2} &= \frac{r_3}{2r_3 + 2} \\ &= \frac{r_3}{{r_3}^6} \\ &= {r_3}^{1-6} \\ &= {r_3}^3 \\ &= 2r_3 + 1 \end{aligned}$$

上述計算結果與 (6) 一致。

為加深讀者對伽羅瓦域的構造方法的了解，以下再舉一個例子，試考慮 GF(8)。由於 $8 = 2^3$，我們先選擇域 $\mathbb{Z}_2$，並設 f 為 $\mathbb{Z}_2[x]$ 中的不可約三次首一多項式，s 為 f 的一個根，那麼根據 (2)，我們有

$$\begin{aligned} \mathbb{Z}_2(s) &= \{as^2 + bs + c : a, b, c \in \mathbb{Z}_2\} \\ &= \{0, 1, s, s + 1, s^2, s^2 + 1, s^2 + s, s^2 + s + 1\} \qquad (7) \end{aligned}$$

上列集合共有八個成員，而且同構於 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (同構函數為 $\theta_3(as^2 + bs + c) = (a, b, c)$)，滿足上面「定理 2」的第一句。

接下來要列出 $\mathbb{Z}_2[x]$ 中所有不可約三次首一多項式 f，然後就每個 f 的根 s 檢查 s 能否生成 (7) 中的七個非零成員。為此，可以首先寫出所有形如 $(x + a)(x^2 + bx + c)$ (其中 $a, b, c \in \mathbb{Z}_2$) 的多項式，這些多項式都是可約三次首一多項式，例如由於在 $\mathbb{Z}_2[x]$ 下，$x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$，可知 $x^3 + x^2 + x + 1$ 在 $\mathbb{Z}_2[x]$ 中是可約三次首一多項式。用上述方法剔除所

有可約三次首一多項式後，便可得到 $\mathbb{Z}_2[x]$ 中所有不可約三次首一多項式如下：x^3+x^2+1 和 x^3+x+1。

接著要逐一考慮上述兩個多項式，首先考慮 x^3+x^2+1，並把其根記作 s_1，因此 s_1 滿足等式 ${s_1}^3+{s_1}^2+1=0$，即 ${s_1}^3={s_1}^2+1$ (請注意在 $\mathbb{Z}_2$ 下，$-1=1$)。以下列出 s_1 的各個冪次，看看它能否生成 (7) 中的七個非零成員：

$$\begin{aligned}
{s_1}^1 &= s_1\\
{s_1}^2 &= {s_1}^2\\
{s_1}^3 &= {s_1}^2+1\\
{s_1}^4 &= ({s_1}^2+1)(s_1)={s_1}^3+s_1={s_1}^2+1+s_1={s_1}^2+s_1+1\\
{s_1}^5 &= ({s_1}^2+s_1+1)(s_1)={s_1}^3+{s_1}^2+s_1={s_1}^2+1+{s_1}^2+s_1=s_1+1\\
{s_1}^6 &= (s_1+1)(s_1)={s_1}^2+s_1\\
{s_1}^7 &= ({s_1}^2+s_1)(s_1)={s_1}^3+{s_1}^2={s_1}^2+1+{s_1}^2=1
\end{aligned}$$

上述結果顯示 s_1 能夠生成 (7) 中的七個非零成員，由此可知以下集合是我們要求的 GF(8)：

$$\mathbb{Z}_2(s_1)=\{a{s_1}^2+bs_1+c : a,b,c\in\mathbb{Z}_2; {s_1}^3={s_1}^2+1\}$$

讀者可自行驗證，上列另一個多項式 x^3+x+1 的根 (設為 s_2) 也能生成 (7) 中的七個非零成員，因此以下集合也是我們要求的 GF(8)：

$$\mathbb{Z}_2(s_2)=\{a{s_2}^2+bs_2+c : a,b,c\in\mathbb{Z}_2; {s_2}^3=s_2+1\}$$

根據「定理 1」，上面求得的 $\mathbb{Z}_2(s_1)$ 與 $\mathbb{Z}_2(s_2)$ 同構，而有關同構關係可以用以下函數表示：

$$\theta_4(a{s_1}^2+bs_1+c)=b{s_2}^2+(a+b)s_2+(a+b+c)$$

為驗證上述同構函數，以下讓我們證明 $\theta_4({s_1}^2)=(\theta_4(s_1))^2$，一方面，我們有

$$\begin{aligned}
\theta_4({s_1}^2) &= \theta_4(1{s_1}^2+0s_1+0)\\
&= 0{s_2}^2+(1+0)s_2+(1+0+0)\\
&= s_2+1
\end{aligned}$$

另一方面，我們又有

$$\begin{aligned}
(\theta_4(s_1))^2 &= (\theta_4(0{s_1}^2+1s_1+0))^2\\
&= ({s_2}^2+s_2+1)^2\\
&= ({s_2}^2+s_2+1)({s_2}^2+s_2+1)\\
&= {s_2}^4+{s_2}^2+1\\
&= ({s_2}^3)(s_2)+{s_2}^2+1\\
&= (s_2+1)(s_2)+{s_2}^2+1\\
&= s_2+1
\end{aligned}$$

至此證得 $\theta_4({s_1}^2) = (\theta_4(s_1))^2$。

連結至數學專題
連結至周家發網頁