感受伽羅瓦：擴張域

本章主旨是介紹擴張域(extension field) 的基本概念。「擴張域」與上一章介紹的「子域」是相對的概念。設有兩個域 $(F,+,\times)$ 和 $(E,+,\times)$，它們有相同的運算 $+$ 和 $\times$，並且 $F\subseteq E$，那麼我們說 F 是 E 的子域，但反過來也可以說 E 是 F 的擴張域，例如 $\mathbb{R}$ 是 $\mathbb{C}$ 的子域，而 $\mathbb{C}$ 則是 $\mathbb{R}$ 的擴張域。在抽象代數學上，域 F 與其擴張域 E 的關係稱為域擴張(field extension)，可用符號 $E:F$ 代表。

設 E 為 F 的擴張域，並且 $a_1,\cdots,a_n\in E$，則 $F(a_1,\ldots,a_n)$ 代表包含 F 和 a_1、...、a_n 的最小的域[1]，這裡「最小」的意思是指，若 K 也是包含 F 和 a_1、...、a_n 的域，則 $F(a_1,\ldots,a_n)\subseteq K$。在上述定義中，若只有一個 a，則 $F(a):F$ 稱為簡單擴張(simple extension)，這是域擴張中最簡單的情況。容易看到如果 $a\in F$，那麼 F 本身就是包含 F 和 a 的最小的域，故有 $F(a)=F$，因此以下只考慮 $a\notin F$ 時 $F(a)$ 的情況。

我們在上一章曾指出，域 E 可以看成其子域 F 上的向量空間，並且可根據這個向量空間的基底確定這個空間的維度。由於域 F 與其擴張域 E 的關係實質上是子域與域的關係，上述概念也可應用於域擴張。設 $E:F$ 為域擴張，那麼可以把 E 看成 F 上的向量空間，我們把這個向量空間的維度稱為 $E:F$ 的擴張次數(degree of extension)，並記作 $|E:F|$[2]。如果 $|E:F|$ 是有限整數，我們便說 $E:F$ 是有限擴張(finite extension)，否則便是無限擴張(infinite extension)，本章只會討論有限擴張。

接下來讓我們看一些簡單擴張的例子，首先考慮 $\mathbb{R}(i):\mathbb{R}$。由於 $\mathbb{R}(i)$ 是包含所有實數和虛數單位 i 的最小的域，它包含實數和 i 自身及互相進行加減乘除的結果，那麼它到底包含哪些數？容易看到它包含所有具有形式 $a+bi$ (其中 $a,b\in\mathbb{R}$) 的數，即所有複數。雖然 $a+bi$ 表面上只涵蓋加減法 (請注意 a 和 b 可以是負數，而減法等於加上一個負數)，而並未涵蓋乘

[1]請注意這裡要用圓括號 ( ) 而非方括號 [ ] 括著 a_1、...、a_n，因為抽象代數學上習慣使用圓括號代表域 (方括號則代表非域的整環)。

[2]我們在《感受伽羅瓦：子群與商群》中使用符號 $|G:H|$ 代表群 H 關於群 G 的「指數」，「指數」的符號雖然與這裡引入的「擴張次數」符號相同，但前者是有關「群」的概念，後者則是有關「域」的概念，根據上下文，應不會引致混淆。

除法，但由於 $i^2 = -1$，$\frac{1}{i} = -i$ 和 $\frac{1}{i^2} = -1$，可知 i 自身進行乘除，只可能得到 i、$-i$、1 和 -1 這四個結果，因此 i 和實數自身及互相進行乘除的結果必然也具有 $a + bi$ 的形式[3]，由此我們有

$$\mathbb{R}(i) = \mathbb{C}$$

根據前面的討論，我們可以把擴張域 $\mathbb{R}(i)$ 看成域 $\mathbb{R}$ 上的向量空間。此外，根據我們在上一章的討論，$\{1, i\}$ 構成 $\mathbb{C}$ 的基底，由於這個基底包含兩個元素，可知這個向量空間的維度是 2，即 $|\mathbb{R}(i) : \mathbb{R}| = 2$。

其次考慮 $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$。請注意由於 $\sqrt[3]{2} \in \mathbb{R}$，必有 $\mathbb{R}(\sqrt[3]{2}) = \mathbb{R}$，所以這裡以 $\mathbb{Q}$ 而非 $\mathbb{R}$ 作為子域。$\mathbb{R}$ 雖然是包含所有有理數和 $\sqrt[3]{2}$ 的域，但不是滿足此條件的最小的域，所以 $\mathbb{Q}(\sqrt[3]{2})$ 有別於我們以前討論過的域 (即 $\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$ 和 $\mathbb{Z}_p$，其中 p 是正質數)，那麼它到底包含哪些數？由於

$$\begin{aligned}
(\sqrt[3]{2})^2 &= 2^{\frac{2}{3}} \\
(\sqrt[3]{2})^3 &= 2 \\
\frac{1}{\sqrt[3]{2}} &= \frac{1 \times 2^{\frac{2}{3}}}{\sqrt[3]{2} \times 2^{\frac{2}{3}}} \\
&= \frac{1}{2}\left(2^{\frac{2}{3}}\right) \\
\frac{1}{(\sqrt[3]{2})^2} &= \frac{1 \times \sqrt[3]{2}}{(\sqrt[3]{2})^2 \times \sqrt[3]{2}} \\
&= \frac{1}{2}(\sqrt[3]{2}) \\
\frac{1}{(\sqrt[3]{2})^3} &= \frac{1}{2}
\end{aligned}$$

可知 $\sqrt[3]{2}$ 自身進行乘除，其結果必然具有 a_2、$b_2\sqrt[3]{2}$ 或 $c_2(2^{\frac{2}{3}})$ 的形式 (其中 $a_2, b_2, c_2 \in \mathbb{Q}$)，而 $\mathbb{Q}(\sqrt[3]{2})$ 的元素則是把以上這些結果中的一個或多個乘以有理數後再相加的結果，即

$$\begin{aligned}
\mathbb{Q}(\sqrt[3]{2}) &= \left\{a_1(a_2) + b_1(b_2\sqrt[3]{2}) + c_1\left(c_2\left(2^{\frac{2}{3}}\right)\right) : a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{Q}\right\} \\
&= \left\{a + b\sqrt[3]{2} + c\left(2^{\frac{2}{3}}\right) : a, b, c \in \mathbb{Q}\right\} \qquad (1)
\end{aligned}$$

請注意上述集合是 $\mathbb{R}$ 的真子集，例如 $\sqrt{3}$ 便不屬於上述集合。

[3]事實上，我們在《感受伽羅瓦：二次方程與複數》中曾示範如何進行複數的乘除法，所得結果必然具有 $a + bi$ 的形式。

如果把擴張域 $\mathbb{Q}(\sqrt[3]{2})$ 看成 $\mathbb{Q}$ 上的向量空間，那麼 $\{1, \sqrt[3]{2}, 2^{\frac{2}{3}}\}$ 構成 $\mathbb{Q}(\sqrt[3]{2})$ 的基底，以下讓我們證明這個集合滿足上一章提出的基底所須滿足的兩個條件：(i) 從 (1) 容易看到 $\langle 1, \sqrt[3]{2}, 2^{\frac{2}{3}} \rangle = \mathbb{Q}(\sqrt[3]{2})$；(ii) 設 $a + b\sqrt[3]{2} + c(2^{\frac{2}{3}}) = 0$，則有

$$a = -b\sqrt[3]{2} - c(2^{\frac{2}{3}})$$

上式右端中的無理項 $\sqrt[3]{2}$ 和 $2^{\frac{2}{3}}$ 不可能透過與非零有理數相乘而變成有理項或互相抵銷，這即是說上式中的有理數 b 和 c 若有一個不是 0，上式右端不可能等於有理數 a，因此如要令上式成立，必須有 $b = c = 0$，在此情況下，也必有 $a = 0$，因此 $\{1, \sqrt[3]{2}, 2^{\frac{2}{3}}\}$ 是線性獨立的。由於基底 $\{1, \sqrt[3]{2}, 2^{\frac{2}{3}}\}$ 包含三個元素，可知 $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$。

以上介紹的都是簡單擴張的例子，在這些擴張中，域 F 外的一個元素 a 被添加到 F 中並構成擴張域 $F(a)$。但域擴張也可以是把多個元素 a_1、...、a_n 添加到 F 中並構成擴張域 $F(a_1, \ldots, a_n)$。這種擴張雖然不是簡單擴張，但我們可以把它看成逐次添加一個元素的過程，即簡單擴張的複合，例如 $F(a_1, a_2)$ 便可以看成先把 a_1 添加到 F，得到 $F(a_1)$，這是第一重簡單擴張 $F(a_1) : F$；然後再把 a_2 添加到 $F(a_1)$，從而得到 $F(a_1)(a_2)$，這是第二重簡單擴張 $F(a_1)(a_2) : F(a_1)$。上述兩重簡單擴張的複合結果就是 $F(a_1)(a_2) : F$，也就是 $F(a_1, a_2) : F$。

把域擴張看成簡單擴張的複合，有助我們了解某些複雜擴張域所包含的元素和基底。試考慮 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$，如前所述，可以把這個域擴張看成兩個簡單擴張的複合，即把它看成 $\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}$。為了解這個複合域擴張，首先考慮第一重簡單擴張 $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$。由於 $(\sqrt{2})^2 = 2$，$\frac{1}{\sqrt{2}} = \frac{1}{2}(\sqrt{2})$ 和 $\frac{1}{(\sqrt{2})^2} = \frac{1}{2}$，可知 $\sqrt{2}$ 自身進行乘除，其結果必然具有 a_2 或 $b_2\sqrt{2}$ 的形式 (其中 $a_2, b_2 \in \mathbb{Q}$)，而 $\mathbb{Q}(\sqrt{2})$ 的元素則是把以上這些結果中的一個或多個乘以有理數後再相加的結果，即

$$\begin{aligned} \mathbb{Q}(\sqrt{2}) &= \{a_1(a_2) + b_1(b_2\sqrt{2}) : a_1, b_1, a_2, b_2 \in \mathbb{Q}\} \\ &= \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \qquad (2) \end{aligned}$$

如果把擴張域 $\mathbb{Q}(\sqrt{2})$ 看成 $\mathbb{Q}$ 上的向量空間，那麼 $\{1, \sqrt{2}\}$ 構成 $\mathbb{Q}(\sqrt{2})$ 的基底，以下讓我們證明這個集合滿足基底所須滿足的兩個條件：(i) 從 (2) 容易看到 $\langle 1, \sqrt{2} \rangle = \mathbb{Q}(\sqrt{2})$；(ii) 設 $a + b\sqrt{2} = 0$，則有

$$a = -b\sqrt{2}$$

上式右端中的無理項 $\sqrt{2}$ 不可能透過與非零有理數相乘而變成有理項並從而等於有理數 a，因此如要令上式成立，必須有 $b = 0$，在此情況下，也必有 $a = 0$，因此 $\{1, \sqrt{2}\}$ 是線性獨立的。由於基底 $\{1, \sqrt{2}\}$ 包含兩個元素，可知 $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$。

接著考慮第二重簡單擴張 $\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})$，由於 $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$，我們知道 $\mathbb{Q}(\sqrt{2})(\sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$。類似 $\sqrt{2}$ 的情況，$\sqrt{3}$ 自身進行乘除，其結果必然具有 u_2 或 $v_2\sqrt{3}$ 的形式 (其中 $u_2, v_2 \in \mathbb{Q}$)，而 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ 的元素則是把以上這些結果中的一個或多個乘以 $\mathbb{Q}(\sqrt{2})$ 的元素後再相加的結果，即

$$\begin{aligned} \mathbb{Q}(\sqrt{2})(\sqrt{3}) &= \{u_1(u_2) + v_1(v_2\sqrt{3}) : u_1, v_1 \in \mathbb{Q}(\sqrt{2}); u_2, v_2 \in \mathbb{Q}\} \\ &= \{u + v\sqrt{3} : u, v \in \mathbb{Q}(\sqrt{2})\} \qquad (3) \end{aligned}$$

上面最後一行的理據是 u_2 和 v_2 作為 $\mathbb{Q}$ 的元素，自然也是 $\mathbb{Q}(\sqrt{2})$ 的元素，因此 $u_1u_2, v_1v_2 \in \mathbb{Q}(\sqrt{2})$，可以分別被 u 和 v 取代。

如果把擴張域 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ 看成 $\mathbb{Q}(\sqrt{2})$ 上的向量空間，那麼 $\{1, \sqrt{3}\}$ 構成 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ 的基底，以下讓我們證明這個集合滿足基底所須滿足的兩個條件：(i) 從 (3) 容易看到 $\langle 1, \sqrt{3}\rangle = \mathbb{Q}(\sqrt{2})(\sqrt{3})$；(ii) 設 $u + v\sqrt{3} = 0$，由於 $u, v \in \mathbb{Q}(\sqrt{2})$，此一等式可以寫成 $a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3} = 0$ (其中 $a, b, c, d \in \mathbb{Q}$)，則有

$$a = -b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

上式右端中的無理項 $\sqrt{2}$、$\sqrt{3}$ 和 $\sqrt{6}$ 不可能透過與非零有理數相乘而變成有理項或互相抵銷，這即是說上式中的有理數 b、c 和 d 若有一個不是 0，上式右端不可能等於有理數 a，因此如要令上式成立，必須有 $b = c = d = 0$，在此情況下，也必有 $a = 0$，因此 $\{1, \sqrt{3}\}$ 是線性獨立的。由於基底 $\{1, \sqrt{3}\}$ 包含兩個元素，可知 $|\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})| = 2$。

至此我們討論了兩重簡單擴張 $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ 和 $\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})$，接著討論這兩者的複合 $\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}$，也就是 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$。為此，先把 (2) 應用於 (3)，得到以下結果：

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \{u + v\sqrt{3} : u, v \in \mathbb{Q}(\sqrt{2})\} \\ &= \{(a + b\sqrt{2}) + (c + d\sqrt{2})(\sqrt{3}) : a, b, c, d \in \mathbb{Q}\} \\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\} \qquad (4) \end{aligned}$$

此外，根據前面的討論，不難看到如果把擴張域 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 看成 $\mathbb{Q}$ 上的向量空間，那麼 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ 構成 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 的基底，以下讓我們證明這個集合滿足基底所須滿足的兩個條件：(i) 從 (4) 容易看到 $\langle 1, \sqrt{2}, \sqrt{3}, \sqrt{6}\rangle = \mathbb{Q}(\sqrt{2}, \sqrt{3})$；(ii) 設 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$，則有

$$a = -b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

但剛才我們已證明若要令上式成立，必須有 $a = b = c = d = 0$，因此 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ 是線性獨立的。由於基底 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ 包含四個元素，

可知 $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}|=4$。

現在讓我們回顧上述複合擴張 $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$ 與兩個簡單擴張 $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$ 和 $\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})$ 的關係。在基底方面,複合擴張的基底 $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ 是兩個簡單擴張的基底 $\{1,\sqrt{2}\}$ 和 $\{1,\sqrt{3}\}$ 的元素逐一相乘的結果，即 $1=1\times1$，$\sqrt{2}=\sqrt{2}\times1$，$\sqrt{3}=1\times\sqrt{3}$ 和 $\sqrt{6}=\sqrt{2}\times\sqrt{3}$。在擴張的次數方面，複合擴張的次數 (即 $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}|=4$) 是兩個簡單擴張的次數 (即 $|\mathbb{Q}(\sqrt{2}):\mathbb{Q}|=2$ 和 $|\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})|=2$) 相乘的結果。

上述關係並非偶然，而是域擴張之間的普遍關係，而且這種關係並不限於兩重域擴張，現把這種關係概括為以下定理。為方便表述以下定理，先定義域元素集合的乘積。設 $V=\{v_1,\ldots,v_n\}$ 和 $W=\{w_1,\ldots,w_m\}$ 為兩個由域元素組成的有限集合，則它們的乘積就是把兩個集合中的元素逐一相乘的結果，即 $V\otimes W=\{v_1w_1,\ldots,v_1w_m,\ldots,v_nw_1,\ldots,v_nw_m\}$[4]，容易把此一定義推廣到多個向量集合的乘積。

定理 1：設有有限擴張 $F_1:F_2$、$F_2:F_3$、...、$F_{n-1}:F_n$，其中 V_1、V_2、...、V_{n-1} 分別是 $F_1:F_2$、$F_2:F_3$、...、$F_{n-1}:F_n$ 的基底，則 $F_1:F_n$ 也是有限擴張，$V_1\otimes V_2\otimes\ldots\otimes V_{n-1}$ 是其基底，並且

$$|F_1:F_n|=|F_1:F_2|\times|F_2:F_3|\times\ldots\times|F_{n-1}:F_n| \qquad (5)$$

上列公式在抽象代數學上一般稱為塔式法則(Tower Law)。請注意在上述定理中，$F_1:F_2$ 等不一定是簡單擴張，也可以是複合擴張。另請注意如把上式中的 : 當作除號，那麼上式類似以下分數乘法法則：

$$\frac{a_1}{a_n}=\frac{a_1}{a_2}\times\frac{a_2}{a_3}\times\ldots\times\frac{a_{n-1}}{a_n}$$

接下來讓我們看上述定理的一個應用，考慮 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}$。如前所述，可以把這個域擴張處理成多重擴張的複合，例如複合擴張 $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$ 與簡單擴張 $\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}):\mathbb{Q}(\sqrt{2},\sqrt{3})$ 的複合。由於在前面我們已處理了上述複合擴張，現在只需處理簡單擴張 $\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}):\mathbb{Q}(\sqrt{2},\sqrt{3})$。由於 $\sqrt{5}\notin\mathbb{Q}(\sqrt{2},\sqrt{3})$，我們知道 $\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5})\neq\mathbb{Q}(\sqrt{2},\sqrt{3})$。利用類似前面的推理方法，可以得到

$$\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5})=\{u+v\sqrt{5}:u,v\in\mathbb{Q}(\sqrt{2},\sqrt{3})\} \qquad (6)$$

此外，還可求得 $\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}):\mathbb{Q}(\sqrt{2})(\sqrt{3})$ 的一個基底 $\{1,\sqrt{5}\}$ 以及 $|\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}):\mathbb{Q}(\sqrt{2},\sqrt{3})|=2$。

[4]這裡使用符號 $\otimes$，以區別於兩個集合的笛卡爾積 (通常用符號 $\times$ 表示)。

接著討論 $\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}) : \mathbb{Q}$，也就是 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}$。為此，先把 (4) 應用於 (6)，得到以下結果：

$$\begin{aligned} & \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) \\ = \; & \{u+v\sqrt{5} : u,v \in \mathbb{Q}(\sqrt{2},\sqrt{3})\} \\ = \; & \{(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})+(e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6})\sqrt{5} : \\ & a,b,c,d,e,f,g,h \in \mathbb{Q}\} \\ = \; & \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}+e\sqrt{5}+f\sqrt{10}+g\sqrt{15}+h\sqrt{30} : \\ & a,b,c,d,e,f,g,h \in \mathbb{Q}\} \qquad (7) \end{aligned}$$

根據「定理 1」，$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}$ 的基底等於 $\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{2},\sqrt{3})$ 的基底與 $\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}$ 的基底的乘積，即

$$\{1,\sqrt{5}\} \otimes \{1,\sqrt{2},\sqrt{3},\sqrt{6}\} = \{1,\sqrt{2},\sqrt{3},\sqrt{6},\sqrt{5},\sqrt{10},\sqrt{15},\sqrt{30}\}$$

而根據公式 (5)，$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}$ 的擴張次數則可以計算如下：

$$\begin{aligned} & |\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}| \\ = \; & |\mathbb{Q}(\sqrt{2},\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{2},\sqrt{3})| \times |\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}| \\ = \; & 2 \times 4 \\ = \; & 8 \end{aligned}$$

上述擴張次數剛好等於上述基底所含元素的個數。

利用上述方法把元素添加到一個域前，必須先檢查該元素是否屬於將要添加的域。如果不作檢查而盲目地沿用上述方法，將會得到不正確的結果，以下提供這方面的例子。試考慮 $\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}) : \mathbb{Q}$，由於這個域擴張跟剛才討論的例子頗相似，有些讀者可能以為這個域擴張的次數也是 8，但這是不正確的。為了解這個域擴張，我們把它處理成三重簡單擴張的複合。首先考慮第一重簡單擴張 $\mathbb{Q}(\sqrt{6}) : \mathbb{Q}$，利用類似前面的推理方法，可以得到

$$\mathbb{Q}(\sqrt{6}) = \{a+b\sqrt{6} : a,b \in \mathbb{Q}\} \qquad (8)$$

此外，還可求得 $\mathbb{Q}(\sqrt{6}) : \mathbb{Q}$ 的一個基底 $\{1,\sqrt{6}\}$ 以及 $|\mathbb{Q}(\sqrt{6}) : \mathbb{Q}| = 2$。

接著考慮第二重簡單擴張 $\mathbb{Q}(\sqrt{6})(\sqrt{10}) : \mathbb{Q}(\sqrt{6})$，由於 $\sqrt{10} \notin \mathbb{Q}(\sqrt{6})$ (這是因為 $\sqrt{10} = \sqrt{2} \times \sqrt{5}$ 包含著 $\sqrt{5}$ 這個因子，而 $\mathbb{Q}(\sqrt{6})$ 卻不包含 $\sqrt{5}$)，我們知道 $\mathbb{Q}(\sqrt{6})(\sqrt{10}) \neq \mathbb{Q}(\sqrt{6})$。利用類似前面的推理方法，可以得到

$$\mathbb{Q}(\sqrt{6})(\sqrt{10}) = \{u+v\sqrt{10} : u,v \in \mathbb{Q}(\sqrt{6})\} \qquad (9)$$

此外,還可求得 $\mathbb{Q}(\sqrt{6})(\sqrt{10}) : \mathbb{Q}(\sqrt{6})$ 的一個基底 $\{1,\sqrt{10}\}$ 以及 $|\mathbb{Q}(\sqrt{6})(\sqrt{10}) : \mathbb{Q}(\sqrt{6})| = 2$。

接著討論 $\mathbb{Q}(\sqrt{6})(\sqrt{10}) : \mathbb{Q}$，也就是 $\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}$。為此，先把 (8) 應用於 (9)，得到以下結果：

$$\begin{aligned}\mathbb{Q}(\sqrt{6}, \sqrt{10}) &= \{u + v\sqrt{10} : u, v \in \mathbb{Q}(\sqrt{6})\} \\ &= \{(a + b\sqrt{6}) + (c + d\sqrt{6})\sqrt{10} : a, b, c, d \in \mathbb{Q}\} \\ &= \{a + b\sqrt{6} + c\sqrt{10} + d\sqrt{60} : a, b, c, d \in \mathbb{Q}\}\end{aligned}$$

根據「定理 1」，可以求得 $\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}$ 的一個基底如下：

$$\{1, \sqrt{6}\} \otimes \{1, \sqrt{10}\} = \{1, \sqrt{6}, \sqrt{10}, \sqrt{60}\}$$

而根據公式 (5)，可以求得

$$|\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}| = 2 \times 2 = 4$$

接著考慮第三重簡單擴張 $\mathbb{Q}(\sqrt{6}, \sqrt{10})(\sqrt{15}) : \mathbb{Q}(\sqrt{6}, \sqrt{10})$，這次我們發現 $\sqrt{15} \in \mathbb{Q}(\sqrt{6}, \sqrt{10})$(這是因為 $\sqrt{15} = \frac{1}{2}(\sqrt{60})$)，因此不能沿用前面的方法，但我們可以即時得出以下結論：$\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10})$，由此可知域擴張 $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) : \mathbb{Q}$ 的次數應等於 $\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}$ 的次數，即是 4 而非 8。

在上面我們介紹了簡單擴張和複合擴張這兩個對立概念，有趣的是，在某些情況下，同一個擴張域既可以用複合擴張得到，又可以用簡單擴張得到。試考慮 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$，在前面我們指出這個擴張域可以通過進行複合擴張而得到，其元素見於公式 (4)。現在我們證明這個擴張域其實等於 $\mathbb{Q}(\sqrt{2} + \sqrt{3})$，即可以通過進行簡單擴張 (把 $\sqrt{2} + \sqrt{3}$ 添加到 $\mathbb{Q}$ 中) 而得到。

首先證明 $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$，由於 $\sqrt{2} + \sqrt{3}$ 是 $\sqrt{2}$ 與 $\sqrt{3}$ 相加的結果，顯然有 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 包含 $\sqrt{2} + \sqrt{3}$，而 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 當然也包含 $\mathbb{Q}$，但 $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ 是包含 $\mathbb{Q}$ 和 $\sqrt{2} + \sqrt{3}$ 的最小的域，根據前面有關「最小」的定義，我們有 $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$。

其次證明 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$，由於 $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$，不難計算

$$\begin{aligned}\sqrt{2} &= \frac{1}{2}(\sqrt{2} + \sqrt{3})^3 - \frac{9}{2}(\sqrt{2} + \sqrt{3}) \\ \sqrt{3} &= \frac{11}{2}(\sqrt{2} + \sqrt{3}) - \frac{1}{2}(\sqrt{2} + \sqrt{3})^3\end{aligned}$$

這即是說 $\sqrt{2}$ 和 $\sqrt{3}$ 都是 $\sqrt{2}+\sqrt{3}$ 的冪次乘以有理數後相加的結果, 由此有 $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ 包含 $\sqrt{2}$ 和 $\sqrt{3}$，而 $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ 當然也包含 $\mathbb{Q}$，但 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

是包含 $\mathbb{Q}$、$\sqrt{2}$ 和 $\sqrt{3}$ 的最小的域，根據前面有關「最小」的定義，我們有 $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$。綜合以上兩段，我們有 $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$。

根據上段的結果，我們知道 $|\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}| = 4$，現在的問題是，能否為 $\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}$ 找出一個由 $\sqrt{2}+\sqrt{3}$ 的冪次組成的基底？由於這個基底應包含 4 個元素，其中兩個是 1 和 $\sqrt{2}+\sqrt{3}$，可以猜想其餘兩個元素應是 $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$ 和 $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$。事實上，$\{1, \sqrt{2}+\sqrt{3}, 5+2\sqrt{6}, 11\sqrt{2}+9\sqrt{3}\}$ 確是 $\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}$ 的基底，以下讓我們證明這一點。

為此，要證明上述集合滿足基底所需滿足的兩個條件，即 (i) $\langle 1, \sqrt{2}+\sqrt{3}, 5+2\sqrt{6}, 11\sqrt{2}+9\sqrt{3}\rangle = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ 和 (ii) 上述集合中的元素是線性獨立的。由於 $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$，上述 (i) 實際上等於要證明以下兩個集合相等[5]：

$$\begin{aligned} X &= \{x + y(\sqrt{2}+\sqrt{3}) + z(5+2\sqrt{6}) + w(11\sqrt{2}+9\sqrt{3}) : x,y,z,w \in \mathbb{Q}\} \\ A &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a,b,c,d \in \mathbb{Q}\} \end{aligned}$$

為證明 $X = A$，可以分別證明 $X \subseteq A$ 和 $A \subseteq X$。前者很容易證明，因為給定 X 的任意元素，只要把該元素展開並化簡，便可證明它也是 A 的元素，例如給定 $\frac{1}{2} + (-7)(\sqrt{2}+\sqrt{3}) + (0)(5+2\sqrt{6}) + (1)(11\sqrt{2}+9\sqrt{3})$，把它展開並化簡為 $\frac{1}{2} + 4\sqrt{2} + 2\sqrt{3}$，即可看到這個元素屬於 A。

要證明 $A \subseteq X$，就等於證明給定 A 的任意元素，總能把它寫成 X 的元素的形式，這就等於給定 $a,b,c,d \in \mathbb{Q}$，總能解出以下方程中的變項 x、y、z 和 w，而且其解必須是有理數：

$$x+y(\sqrt{2}+\sqrt{3})+z(5+2\sqrt{6})+w(11\sqrt{2}+9\sqrt{3}) = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \qquad (10)$$

此即

$$(x+5z) + (y+11w)\sqrt{2} + (y+9w)\sqrt{3} + 2z\sqrt{6} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

這等於求解以下聯立方程：

$$\begin{cases} x + 5z = a \\ y + 11w = b \\ y + 9w = c \\ 2z = d \end{cases}$$

[5]下列的 X 是根據上一章有關「生成空間」的定義把 $\langle 1, \sqrt{2}+\sqrt{3}, 5+2\sqrt{6}, 11\sqrt{2}+9\sqrt{3}\rangle$ 改寫成的結果，下列的 A 則是前面的公式 (4)。

上述聯立方程可以寫成以下矩陣形式：

$$\begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \qquad (11)$$

為證實上述方程確有有理數解，可以借用線性代數的知識，首先進行以下計算：

$$\det \begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 2 & 0 \end{pmatrix} = 4$$

在上式中，$\det(M)$ 代表矩陣 M 的「行列式」(determinant)。根據線性代數的知識，由於上述行列式不等於 0，可知 (11) 必有解，即 (10) 必有解。這個解可以透過「高斯消元法」(Gaussian elimination) 求得，而且由於上述係數矩陣中的元素和 a、b、c、d 全是有理數，這個解必全是有理數，至此證得 $A \subseteq X$，亦即完成了上面 (i) 的證明。

我們還要證明上面的 (ii)，但這並不困難，因為這等於要證明以下方程有唯一平凡解 $x = y = z = w = 0$：

$$x + y(\sqrt{2} + \sqrt{3}) + z(5 + 2\sqrt{6}) + w(11\sqrt{2} + 9\sqrt{3}) = 0 \qquad (12)$$

利用類似前面的推理方法，上述方程可以寫成以下矩陣形式：

$$\begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad (13)$$

由於在前面我們已求得上述係數矩陣的行列式不等於 0，根據線性代數的知識，上述方程有唯一平凡解，由此可知 (12) 也有唯一平凡解，(ii) 證畢。根據上述結果，可以把 $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ 寫成以下形式：

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \{a+b(\sqrt{2}+\sqrt{3})+c(\sqrt{2}+\sqrt{3})^2+d(\sqrt{2}+\sqrt{3})^3 : a,b,c,d \in \mathbb{Q}\}$$

簡單擴張與複合擴張的關係可以總結為一條定理，為方便表述此定理，須先引入域的特徵(characteristic) 的概念。設 F 為域，1 為 F 的乘法單位元，則 F 的特徵是指使得 $n \times 1 = 0$ 成立的最小正整數 n，這裡 $n \times 1$ 代表把 n 個 1 相加的結果；如果不存在這樣的正整數 n,則把 F 的特徵定為 0。

根據上述定義，有限域 $\mathbb{Z}_p$ (其中 p 是正質數) 的特徵是 p，因為在 $\mathbb{Z}_p$ 中，$1\,(=1\times 1)$、$2\,(=2\times 1)$、...、$p-1\,(=(p-1)\times 1)$ 都不等於 0，而 $p\times 1=0$，而無限域 $\mathbb{Q}$、$\mathbb{R}$ 和 $\mathbb{C}$ 的特徵都是 0，因為在這些域中，$n\times 1=0$ 對任何正整數 n 都不成立。具備上述概念，便可以提出以下定理。

定理 2：設 F 是特徵為 0 的域，則 F 的任何有限擴張都可表示為簡單擴張。

由於 $\mathbb{Q}$ 是特徵為 0 的域，而複合擴張 $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$ 是有限擴張 (這個擴張的次數是 4)，根據上述定理，可知這個複合擴張可以表示成簡單擴張，而在上面我們把這個複合擴張表示成簡單擴張 $\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}$，驗證了上述定理。

連結至數學專題
連結至周家發網頁