感受伽羅瓦：代數擴張與超越擴張

我們在上一章介紹了域擴張的概念，域擴張的主旨就是把域 F 沒有的一個或多個元素添加到 F 中，從而得到一個較大的域 (即擴張域)。添加這些元素有多種可能目的，其中一個常見目的是讓一些在 F 中沒有解的多項式方程在擴張域中有解 (以下稱為「根」)，正由於這一點，「域擴張」與「方程求根」被拉上關係。

舉例說，在上一章我們指出複數域 $\mathbb{C}$ 是對實數域 $\mathbb{R}$ 的擴張，而數學家進行這種擴張正是為了對某些多項式方程求根。舉例說，x^2+1 這個方程在實數域中沒有根，因為其根等於負數的平方根 $\pm\sqrt{-1}$，而實數域並不包含這樣的數；但在複數域中，這個方程卻變得有根，其根是 $\pm i$，其中 i 正是用來代表 $\sqrt{-1}$。x^2+1 與 $\mathbb{C}$ 的情況不是孤立的現象，而是一個普遍現象，可以概括為一條定理。但在介紹該定理前，須先引入另一條定理。

定理 1：設 F 為域，則 $F[x]$ 中任何非單位非零多項式 f 均可被寫成不可約多項式的乘積，而且上述因式分解結果是唯一的，這裡「唯一」的意思是指，如果 f 可被寫成兩種因式分解結果：$p_1 \dots p_m$ 和 $q_1 \dots q_n$ (其中 p_1、…、p_m、q_1、…、q_n 是 $F[x]$ 中的不可約多項式)，則 $m=n$，並且每個 p_i 都剛好等於某個 q_j，或與某個 q_j 相伴 (即等於某個常數多項式乘以 q_j[1])。

上述定理是對《感受伽羅瓦：因子分解》中的「有理係數多項式唯一分解定理」(即該網頁的「定理 4」) 的推廣，該定理說 $\mathbb{Q}[x]$ 中任何非單位非零多項式均可被唯一地寫成不可約多項式的乘積，而上述定理則說不僅 $\mathbb{Q}[x]$，任何 $F[x]$ 都滿足此一「唯一分解性質」。舉例說，在 $\mathbb{C}[x]$ 中，x^2+1 便可以因式分解為 $(x+i)(x-i)$，這個多項式還可以因式分解為 $(\frac{1}{2}x-\frac{1}{2}i)(2x+2i)$，但這兩個因式分解結果都剛好包含兩個不可約多項式，而且 $2x+2i=2(x+i)$ 和 $\frac{1}{2}x-\frac{1}{2}i=\frac{1}{2}(x-i)$，因此上述因式分解結果確是唯一的。接下來便可引入本章最重要的定理。

定理 2 (克羅內克定理Kronecker's Theorem)(又稱域論基本定理Fundamental Theorem of Field Theory)：設 F 為域，f 為 $F[x]$ 中的非常數多項式，則存

[1]「相伴」概念的定義見於《感受伽羅瓦：因子分解》。

在域 $F[x]/\langle p\rangle$ (其中 p 是 f 的一個不可約因式)，使得 F 與這個域的某個子域同構 (因而可以把 $F[x]/\langle p\rangle$ 看成 F 的擴張域)，並且 f 在這個擴張域中有根，這個根就是 $x+\langle p\rangle$。

請注意由於 F 是域，根據「定理 1」，必能為 f 找到一個不可約因式 p。上述定理則是說，利用這個 p，便可構造一個擴張域 $F[x]/\langle p\rangle$，使得 f 在這個擴張域中有根。

接下來看一些實例，試考慮 $\mathbb{R}[x]$ 中的多項式 x^2+1，如前所述，這個多項式在 $\mathbb{R}[x]$ 中不可約，因此根據上述定理，$\mathbb{R}[x]/\langle x^2+1\rangle$ 就是所需的擴張域，現在讓我們驗證這一點。首先，由於 x^2+1 在 $\mathbb{R}[x]$ 中不可約，根據《感受伽羅瓦：質理想與極大理想》中的「定理 3」, 可知 $\langle x^2+1\rangle$ 是 $\mathbb{R}[x]$ 的極大理想；由此再根據上述網頁的「定理 2」, 可知 $\mathbb{R}[x]/\langle x^2+1\rangle$ 確是一個域。

其次，我們知道 $\mathbb{R}[x]/\langle x^2+1\rangle$ 的元素包括所有形如 $f+\langle x^2+1\rangle$ 的陪集，其中 f 是任意實係數多項式除以 x^2+1 後所得的餘式。由於這樣的餘式必然是次數小於 2 的實係數多項式，即形如 $ax+b$ (其中 $a,b\in\mathbb{R}$) 的多項式，可知

$$\mathbb{R}[x]/\langle x^2+1\rangle=\{ax+b+\langle x^2+1\rangle : a,b\in\mathbb{R}\} \qquad (1)$$

請注意每個實數 a 都對應著一個形如 $a+\langle x^2+1\rangle$ 的陪集，反之亦然，由此有以下同構關係：

$$\mathbb{R}\cong\{a+\langle x^2+1\rangle : a\in\mathbb{R}\}$$

容易看到上式右端的集合構成 $\mathbb{R}[x]/\langle x^2+1\rangle$ 的子域，由此可見 $\mathbb{R}$ 與 $\mathbb{R}[x]/\langle x^2+1\rangle$ 的某個子域同構，因此 $\mathbb{R}[x]/\langle x^2+1\rangle$ 的確可以看成 $\mathbb{R}$ 的擴張域。

最後，讓我們驗證 $x+\langle x^2+1\rangle$ 是 x^2+1 的根。請注意由於現在我們是在討論擴張域 $\mathbb{R}[x]/\langle x^2+1\rangle$，因此多項式方程 x^2+1 中的常數項 1 不應再被理解為實數, 而應被理解為 $\langle x^2+1\rangle$ 的陪集, 即等於 $1+\langle x^2+1\rangle$；該方程中的變項 x 也不應再被視為實數變項，而應被視為以 $\langle x^2+1\rangle$ 的陪集為值的變項，以下把這個變項改寫成大寫 X 以資識別。基於以上的理解，多項式方程 x^2+1 實應具有 $X^2+(1+\langle x^2+1\rangle)$ 的形式。現在把 $x+\langle x^2+1\rangle$ 代入 $X^2+(1+\langle x^2+1\rangle)$ 中的變項 X：

$$\begin{aligned}
& (x+\langle x^2+1\rangle)^2+(1+\langle x^2+1\rangle)\\
= \;& (x^2+\langle x^2+1\rangle)+(1+\langle x^2+1\rangle)\\
= \;& x^2+1+\langle x^2+1\rangle\\
= \;& \langle x^2+1\rangle
\end{aligned}$$

請注意上面最後一行中的 $\langle x^2+1\rangle\,(=0+\langle x^2+1\rangle)$ 是上述擴張域的加法單位元，因此 $x+\langle x^2+1\rangle$ 確是 $X^2+(1+\langle x^2+1\rangle)$ 的根。

看到這裡，有些讀者可能覺得奇怪，本文提過兩個包含 x^2+1 的根的 $\mathbb{R}$ 的擴張域，其中一個是 $\mathbb{C}$，另一個則是 $\mathbb{R}[x]/\langle x^2+1\rangle$ (其元素列於 (1))，這是否兩個不同的擴張域？沒錯，$\mathbb{C}$ 和 $\mathbb{R}[x]/\langle x^2+1\rangle$ 的確各自由不同性質的元素組成，前者由一種特殊定義的數組成，後者則由陪集組成，但這兩個域卻存在同構關係, 因此從抽象代數學的角度看, 可以視為相同的擴張域。

事實上，我們在《感受伽羅瓦：環的同態與同構》中證明了 $\mathbb{R}[x]/\langle x^2+1\rangle$ 的確與 $\mathbb{C}$ 同構，其中 $x+\langle x^2+1\rangle$ 對應著 i。直觀地看，如果把 (1) 中等號右端的 $\langle x^2+1\rangle$ 略去，並把 x 改為 i，那麼該集合便變成 $\mathbb{C}$ 的定義：

$$\mathbb{C}=\{ai+b : a,b\in\mathbb{R}\} \qquad (2)$$

此外，我們在上面也已證明了 $x+\langle x^2+1\rangle$ 是 $X^2+(1+\langle x^2+1\rangle)$ 的根，而這正好對應著 i 是 x^2+1 的根此一事實。

看到這裡，有些讀者又可能發現 (2) 中有關 $\mathbb{C}$ 的定義跟上一章介紹的簡單擴張域 $\mathbb{R}(i)$ 的以下定義是一模一樣的：

$$\mathbb{R}(i)=\{ai+b : a,b\in\mathbb{R}\} \qquad (3)$$

根據以上的討論，可知 (1) 和 (3) 中的兩個擴張域是同構的，這不是孤立現象，而是一個普遍現象，可以概括為以下定理。

定理 3：設 F 為域，p 為 $F[x]$ 中的不可約多項式，r 為 p 的根，則 $F(r)\cong F[x]/\langle p\rangle$。若 $\deg(p)=n$，則

$$F(r)=\{a_{n-1}r^{n-1}+a_{n-2}r^{n-2}+\cdots+a_1r+a_0 : a_{n-1},a_{n-2},\ldots,a_1,a_0\in F\} \qquad (4)$$

根據上述定理，可知 $\mathbb{R}[x]/\langle x^2+1\rangle\cong\mathbb{R}(i)$，而且 (3) 中集合的定義正就是 (4) 中集合的定義。由於存在上述同構關係，(1) 和 (3) 實質上表達同一個擴張域，但由於 (3) 較為簡潔，而且簡單擴張的概念比陪集概念較為直觀，以下將主要採用 (3) 這類表示法。

以上介紹了包含 $F[x]$ 中非常數多項式方程 f 的至少一個根的擴張域，但很多 f 不只一個根。事實上，根據《感受伽羅瓦：因子分解》中的「代數基本定理」(即該網頁的「定理 6」)，若 $\deg(f)=n$，則 f 共有 n 個不一定兩兩相異的根 r_1、...、r_n。現設 F 的某個擴張域 E 包含這全部 n 個根，那麼 f 在 E 中可以因式分解為一個常數多項式 a 與 n 個一次首一多項式的乘積，即

$$f=a(x-r_1)\cdots(x-r_n) \qquad (5)$$

我們把包含 F 和 f 全部 n 個根的最小的域稱為 f 在 F 上的分裂域(splitting field)。根據擴張域的定義，上述分裂域也就是 $F(r_1, \ldots, r_n)$。從上述定義也可看到，f 在 F 上的分裂域也就是能使 f 達致如 (5) 所示的因式分解結果的 F 的最小擴張域。

仍以 $\mathbb{R}[x]$ 中的二次多項式方程 x^2+1 為例，如前所述，$\mathbb{R}(i)$ 是包含這個方程的根 i 的擴張域。這個方程還有另一個根 $-i$，但由於 $-i=(-1)(i)$，可見 $-i \in \mathbb{R}(i)$，因此 $\mathbb{R}(i,-i)=\mathbb{R}(i)$，由此可知 x^2+1 在 $\mathbb{R}$ 上的分裂域就是 $\mathbb{R}(i)\,(=\mathbb{C})$。事實上，$\mathbb{C}$ 上確有以下因式分解結果：

$$x^2+1=(x-i)(x+i)$$

上例中的分裂域頗為簡單，接下來讓我們看一個較為複雜的例子。試考慮 $\mathbb{Q}[x]$ 中的三次多項式方程 x^3-2，這是 $\mathbb{Q}[x]$ 中的不可約多項式，根據我們在《感受伽羅瓦：二次方程與複數》中的討論，這個方程有三個根：$\sqrt[3]{2}$、$\omega_3(\sqrt[3]{2})$ 和 ${\omega_3}^2(\sqrt[3]{2})$，其中 ω_3 代表 1 的主幅角為 $\frac{2\pi}{3}$ 的立方根 (即 $-\frac{1}{2}+\frac{\sqrt{3}}{2}i$)。首先考慮第一個根 $\sqrt[3]{2}$，根據「定理 3」，可知包含這個根的 $\mathbb{Q}$ 的擴張域是

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

接著考慮第二個根 $\omega_3(\sqrt[3]{2})$，由於這個根是複數而上述集合僅包含實數，這個根顯然不屬於上述集合，因此現在要對上述域作進一步擴張。理論上，固然可以把上述第二個根直接添加到上述域中，從而得到 $\mathbb{Q}(\sqrt[3]{2},\omega_3(\sqrt[3]{2}))$，但此一結果頗為累贅，因為兩重簡單擴張的「主角」都包含 $\sqrt[3]{2}$ 這個因數。為使擴張域的形式較為簡潔，可以把 ω_3 添加到上述域中，從而得到 $\mathbb{Q}(\sqrt[3]{2},\omega_3)$。由於 ω_3 是二次多項式 x^2+x+1 的一個根，而 x^2+x+1 是 $\mathbb{Q}(\sqrt[3]{2})[x]$ 中的不可約多項式[2]，根據「定理 3」，可得所需擴張域如下：

$$\begin{aligned}
\mathbb{Q}(\sqrt[3]{2},\omega_3) &= \{u\omega_3+v : u,v\in\mathbb{Q}(\sqrt[3]{2})\}\\
&= \{(a(\sqrt[3]{2})^2+b\sqrt[3]{2}+c)\omega_3+(d(\sqrt[3]{2})^2+e\sqrt[3]{2}+f) :\\
&\quad a,b,c,d,e,f\in\mathbb{Q}\}\\
&= \{a\omega_3(\sqrt[3]{2})^2+b\omega_3(\sqrt[3]{2})+c\omega_3+d(\sqrt[3]{2})^2+e\sqrt[3]{2}+f :\\
&\quad a,b,c,d,e,f\in\mathbb{Q}\} \qquad (6)
\end{aligned}$$

容易看到，$\omega_3(\sqrt[3]{2})$ 的確屬於上述集合。

最後考慮第三個根 ${\omega_3}^2(\sqrt[3]{2})$，表面上看這個根似乎不屬於上述集合，但根據《感受伽羅瓦：二次方程與複數》中的「定理 2」，我們有 $1+\omega_3+{\omega_3}^2=0$，

[2]請注意雖然 ω_3 是 1 的立方根，但這裡不能使用 x^3-1 這個三次多項式，因為這個多項式在 $\mathbb{Q}[x]$ (以及 $\mathbb{Q}(\sqrt[3]{2})[x]$) 中是可約的，它可以因式分解為 $(x-1)(x^2+x+1)$。

由此有

$$\begin{aligned} {\omega_3}^2(\sqrt[3]{2}) &= (-1-\omega_3)(\sqrt[3]{2}) \\ &= -\sqrt[3]{2}-\omega_3(\sqrt[3]{2}) \end{aligned}$$

因此第三個根實際也屬於 (6)。至此可以確定，$\mathbb{Q}(\sqrt[3]{2},\omega_3)$ 就是 x^3-2 在 $\mathbb{Q}$ 上的分裂域。事實上，$\mathbb{Q}(\sqrt[3]{2},\omega_3)$ 上確有以下因式分解結果：

$$x^3-2=(x-\sqrt[3]{2})(x-\omega_3(\sqrt[3]{2}))(x-{\omega_3}^2(\sqrt[3]{2}))$$

在以上的例子中，我們對有關多項式方程的根都有一定了解，接下來讓我們看另一個較複雜的例子。考慮 $\mathbb{Q}[x]$ 中的方程 x^5-6x+3，這是一個沒有根式解的五次多項式方程。我們先用《感受伽羅瓦：因子分解》中的「艾森斯坦判別法」(即該網頁的「定理 8」) 證明這個多項式在 $\mathbb{Q}[x]$ 中不可約。為此，要找質數 p 使得 $p\nmid 1$，$p\mid -6$，$p\mid 3$ 和 $p^2\nmid 3$，容易看到 3 滿足上述要求，因此上述多項式不可約。

接著根據「定理 2」，可知 $\mathbb{Q}[x]/\langle x^5-6x+3\rangle$ 就是包含 x^5-6x+3 的一個根的 $\mathbb{Q}$ 的擴張域，而這個根就是 $x+\langle x^5-6x+3\rangle$。上述擴張域的元素包括所有形如 $f+\langle x^5-6x+3\rangle$ 的陪集，其中 f 是任意有理係數多項式除以 x^5-6x+3 後所得的餘式。由於這樣的餘式必然是次數小於 5 的有理係數多項式，可知

$$\mathbb{Q}[x]/\langle x^5-6x+3\rangle=\{ax^4+bx^3+cx^2+dx+e+\langle x^5-6x+3\rangle : a,b,c,d,e\in\mathbb{Q}\} \qquad (7)$$

但上述表達式頗為累贅，為此，不妨引入一個符號 α_1，用來代表 x^5-6x+3 的某個根。接著便可以應用公式 (4)，寫出簡單擴張域 $\mathbb{Q}(\alpha_1)$ 的元素如下：

$$\mathbb{Q}(\alpha_1)=\{a{\alpha_1}^4+b{\alpha_1}^3+c{\alpha_1}^2+d\alpha_1+e : a,b,c,d,e\in\mathbb{Q}\} \qquad (8)$$

根據「定理 3」，(7) 和 (8) 中的擴張域是同構的。

由於 $\mathbb{Q}(\alpha_1)$ 是域，可以在其上進行四則運算，其運算法則跟一般有理數的運算法則基本相同，惟須加入一個附加條件 ${\alpha_1}^5-6\alpha_1+3=0$，這是因為我們設定了 α_1 是 x^5-6x+3 的根，以下用一個除法例子示範如何進行這些運算，試求 $\frac{1}{\alpha_1}$，進行這個除法實質等於求 $\mathbb{Q}(\alpha_1)$ 中的一個數 $a{\alpha_1}^4+b{\alpha_1}^3+c{\alpha_1}^2+d\alpha_1+e$，使得這個數與 α_1 相乘所得結果為 1，即

$$\begin{aligned} (a{\alpha_1}^4+b{\alpha_1}^3+c{\alpha_1}^2+d\alpha_1+e)(\alpha_1) &= 1 \\ a{\alpha_1}^5+b{\alpha_1}^4+c{\alpha_1}^3+d{\alpha_1}^2+e\alpha_1 &= 0{\alpha_1}^4+0{\alpha_1}^3+0{\alpha_1}^2+0\alpha_1+1 \end{aligned}$$

由於 ${\alpha_1}^5-6\alpha_1+3=0$，可以把 $6\alpha_1-3$ 代入上式中的 ${\alpha_1}^5$，從而得到

$$\begin{aligned} a(6\alpha_1-3)+b{\alpha_1}^4+c{\alpha_1}^3+d{\alpha_1}^2+e\alpha_1 &= 0{\alpha_1}^4+0{\alpha_1}^3+0{\alpha_1}^2+0\alpha_1+1 \\ b{\alpha_1}^4+c{\alpha_1}^3+d{\alpha_1}^2+(6a+e)\alpha_1-3a &= 0{\alpha_1}^4+0{\alpha_1}^3+0{\alpha_1}^2+0\alpha_1+1 \end{aligned}$$

接下來求解以下聯立方程：

$$\begin{cases} b=0 \\ c=0 \\ d=0 \\ 6a+e=0 \\ -3a=1 \end{cases}$$

容易解得 $a=-\frac{1}{3}, b=c=d=0, e=2$，由此得 $\frac{1}{\alpha_1}=-\frac{1}{3}{\alpha_1}^4+2$。

請注意上例跟引入複數的過程很相似，如前所述，為了使 $\mathbb{R}[x]$ 中的不可約多項式方程 x^2+1 有根，數學家引入符號 i 代表這個方程的一個根，從而構造出一個可以在其上進行四則運算的數域，而這些運算須滿足附加條件 $i^2+1=0$。同樣，在上例中，我們為了使 $\mathbb{Q}[x]$ 中的不可約多項式方程 x^5-6x+3 有根，引入符號 α_1 代表這個方程的一個根，從而構造出一個可以在其上進行四則運算的數域，而這些運算須滿足附加條件 ${\alpha_1}^5-6\alpha_1+3=0$。這樣，從抽象代數學的角度看，複數只不過是眾多可能擴張域之一。

接下來的問題是，能否找到 x^5-6x+3 在 $\mathbb{Q}$ 上的分裂域？這涉及頗為複雜的問題，以下讓我們看看其複雜性。由於前面設定 α_1 是這個多項式方程的根，這個多項式應可被 $x-\alpha_1$ 整除，從而得到一個四次方程，以下用長除法進行這個除法：

$$\begin{array}{rl|llllll}
 & & x^4 & +\alpha_1 x^3 & +{\alpha_1}^2 x^2 & +{\alpha_1}^3 x & +{\alpha_1}^4-6 & \\
\hline
x-\alpha_1 &)\,x^5 & & & & & -6x & +3 \\
 & x^5 & -\alpha_1 x^4 & & & & & \\
\hline
 & & \alpha_1 x^4 & & & & -6x & +3 \\
 & & \alpha_1 x^4 & -{\alpha_1}^2 x^3 & & & & \\
\hline
 & & & {\alpha_1}^2 x^3 & & & -6x & +3 \\
 & & & {\alpha_1}^2 x^3 & -{\alpha_1}^3 x^2 & & & \\
\hline
 & & & & {\alpha_1}^3 x^2 & & -6x & +3 \\
 & & & & {\alpha_1}^3 x^2 & -{\alpha_1}^4 x & & \\
\hline
 & & & & & & (\alpha_1^4-6)x & +3 \\
 & & & & & & (\alpha_1^4-6)x & -{\alpha_1}^5+6\alpha_1 \\
\hline
 & & & & & & & 0
\end{array}$$

上面最後一行的理據如下：

$$\begin{aligned} 3-(-{\alpha_1}^5+6\alpha_1) &= 3+{\alpha_1}^5-6\alpha_1 \\ &= 3+6\alpha_1-3-6\alpha_1 \\ &= 0 \end{aligned}$$

從以上計算結果可知 $x^5-6x+3=(x-\alpha_1)(x^4+\alpha_1x^3+{\alpha_1}^2x^2+{\alpha_1}^3x+{\alpha_1}^4-6)$, 接下來要求四次多項式方程 $x^4+\alpha_1x^3+{\alpha_1}^2x^2+{\alpha_1}^3x+{\alpha_1}^4-6$ 的一個根, 當然我們可以再引入另一符號 α_2, 用來代表這個根, 並把包含 x^5-6x+3 的兩個根 α_1 和 α_2 的 $\mathbb{Q}$ 的擴張域記作 $\mathbb{Q}(\alpha_1,\alpha_2)$, 但現在的問題是, 我們不知 α_2 是否屬於 $\mathbb{Q}(\alpha_1)$, 因而不能斷定 $\mathbb{Q}(\alpha_1,\alpha_2)$ 是一個較大的擴張域, 還是等於 $\mathbb{Q}(\alpha_1)$。造成上述困難的原因是我們對五次多項式方程的各個根之間的關係了解不多,因而也無法深入討論 x^5-6x+3 在 $\mathbb{Q}$ 上的分裂域。

上述例子中的擴張域都是包含某個多項式方程的根的擴張域, 但擴張域還可以有其他可能性, 為此我們引入以下定義。設 $E:F$ 為域擴張, $a\in E$, 若 a 是 $F[x]$ 中某個非零多項式方程的根, 我們便說 a 是 F 上的代數元(algebraic element), 否則是 F 上的超越元(transcendental element)。若 E 中所有元素都是 F 上的代數元, 我們便說 $E:F$ 是代數擴張(algebraic extension), 否則是超越擴張(transcendental extension)。此外, 數學家習慣把 $\mathbb{Q}$ 上的代數元和超越元分別稱為代數數(algebraic number) 和超越數(transcendental number)。

根據上述定義, 任何有理數都是代數數, 這是因為任何有理數 a 都是有理係數一次多項式 $x-a$ 的根。此外, 很多以根式或三角函數值的形式出現的無理數也都是代數數, 因為對這些根式或三角函數值進行適當次數的乘方及其他四則運算後, 便可得到有理係數多項式。舉例說, $\sqrt[3]{2}$ 是代數數, 因為它是 x^3-2 的根, $\cos\frac{\pi}{4}$ 也是代數數, 因為它等於 $\frac{1}{\sqrt{2}}$, 是 $2x^2-1$ 的根。

較複雜的例子如 $\sqrt{2+i}$ 和 $\cos\frac{\pi}{9}$, 也是代數數。為證明前者, 先求 $(\sqrt{2+i})^2=2+i$, 由此得 $(\sqrt{2+i})^2-2=i$。對等號兩端同時取平方並化簡, 得 $(\sqrt{2+i})^4-4(\sqrt{2+i})^2+5=0$, 由此可知 $\sqrt{2+i}$ 是四次多項式 x^4-4x^2+5 的根。為證明後者, 我們可以運用三角恆等式

$$\cos 3\theta=4\cos^3\theta-3\cos\theta$$

把 $\frac{\pi}{9}$ 代入上式中的 θ, 得

$$\begin{aligned}4\left(\cos\frac{\pi}{9}\right)^3-3\cos\frac{\pi}{9} &= \cos\frac{\pi}{3}\\ &= \frac{1}{2}\end{aligned}$$

由此可知 $\frac{\pi}{9}$ 是三次多項式 $4x^3-3x-\frac{1}{2}$ 的根。

但有很多無理數和複數不是代數數, 例如數學家證明了圓周率 π 和自然對數底 e 是超越數。雖然 π 和 e 可以分別看成一次多項式 $x-\pi$ 和 $x-e$ 的根, 但這兩個多項式不是有理係數多項式, 因為它們的常數項不是有理

數，因此只能說 π 和 e 是 $\mathbb{R}$ 上的代數元[3]而非代數數。

根據上述定義，上面討論的域擴張例子全部都是代數擴張。以下是有關簡單代數擴張的定理。

定理 4：設 $F(a) : F$ 為簡單代數擴張，則 $F(a) \cong F[x]/\langle p\rangle$，其中 p 是 $F[x]$ 中的不可約首一多項式，使得 a 是 p 的根，並且 p 是以 a 為根的多項式中次數最小的一個，它可以整除所有以 a 為根的多項式。

根據上述定理，每個簡單代數擴張 $F(a) : F$ 對應著一個以 a 為根的次數最小的首一多項式 p。可以證明給定 F 和 a，這個 p 是唯一確定的，稱為 a 的最小多項式(minimal polynomial)。舉例說，$\mathbb{R}(i) : \mathbb{R}$ 是簡單代數擴張，而 i 的最小多項式是 x^2+1。根據上述定理，可知 $\mathbb{R}(i)$ 同構於 $\mathbb{R}[x]/\langle x^2+1\rangle$ (而後者又同構於 $\mathbb{C}$), 與前面的討論一致。此外, 由於 $i^4-1=0$, 可知 i 也是多項式 x^4-1 的根，而 i 的最小多項式 x^2+1 整除 x^4-1 (因為 $x^4-1=(x^2+1)(x^2-1)$)，驗證了上述定理。

接著提供一個與簡單超越擴張有關的定理。

定理 5：設 $F(a) : F$ 為簡單超越擴張，則 $F(a) \cong F(x)$，其中 $F(x)$ 代表以 F 的元素作為係數的有理式構成的域。

請注意 $F[x]$ 與 $F(x)$ 的區別，前者的成員是「多項式」，後者的成員則是「有理式」(即分子是多項式而分母是非零多項式的分式)，例如 x 是「整係數多項式」(也是「整係數有理式」)，而 $\frac{1}{x}$ 則是「整係數有理式」。

以下用 $\mathbb{Q}(\pi)$ 為例闡明上述定理的合理性，如前所述，π 是超越數，所以 $\mathbb{Q}(\pi) : \mathbb{Q}$ 是簡單超越擴張，因此根據上述定理，應有 $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$。我們知道 $\mathbb{Q}(\pi)$ 是包含 $\mathbb{Q}$ 和 π 的最小的域，這個域包含 π 與自身以及有理數進行四則運算的所有可能結果，例如

$$2\pi, \frac{1}{4}\pi^2+3\pi, -\frac{7}{4\pi}, \frac{3\pi^3}{\pi^5-\frac{5}{2}\pi^2}$$

容易看到，上列各元素都對應著某個有理係數有理式 (只要把上面的 π 改為 x 便可)，例如

$$2x, \frac{1}{4}x^2+3x, -\frac{7}{4x}, \frac{3x^3}{x^5-\frac{5}{2}x^2}$$

請把以上結果與 $\mathbb{Q}(\sqrt{2})$ 作一比較，雖然我們也可寫出分子分母皆包含 $\sqrt{2}$ 的式子，但由於 $(\sqrt{2})^2=2$ 並且 $\frac{1}{\sqrt{2}}=\frac{1}{2}\sqrt{2}$，我們總能把這些式子化簡成只

[3]事實上，任何實數都是 $\mathbb{R}$ 上的代數元。

有分子才包含 $\sqrt{2}$ 的式子，例如

$$\begin{aligned}\frac{3(\sqrt{2})^3}{(\sqrt{2})^5-\frac{5}{2}(\sqrt{2})^2} &= \frac{6\sqrt{2}}{4\sqrt{2}-5}\\ &= \frac{(6\sqrt{2})(4\sqrt{2}+5)}{(4\sqrt{2}-5)(4\sqrt{2}+5)}\\ &= \frac{48+30\sqrt{2}}{7}\\ &= \frac{30}{7}\sqrt{2}+\frac{48}{7}\end{aligned}$$

反觀包含 π 的式子，卻不能像上面那樣化簡，這就是作為代數數的 $\sqrt{2}$ 與作為超越數的 π 的根本區別。

以下定理提供代數擴張和超越擴張的次數。

定理 6：設 $F(a):F$ 為簡單擴張。若 $F(a):F$ 是代數擴張並且 p 是 a 的最小多項式，則 $|F(a):F| = \deg(p)$；若 $F(a):F$ 是超越擴張，則 $|F(a):F| = \infty$。

舉例說，$\mathbb{R}(i):\mathbb{R}$ 是簡單代數擴張，而 i 的最小多項式是二次多項式 x^2+1，因此根據上述定理，$|\mathbb{R}(i):\mathbb{R}| = 2$。事實上，我們知道 $\{1, i\}$ 構成這個擴張的基底，而這個基底所含元素的個數正好等於這個擴張的次數。另外如前所述，$\mathbb{Q}(\pi):\mathbb{Q}$ 是簡單超越擴張，因此根據上述定理，$|\mathbb{Q}(\pi):\mathbb{Q}| = \infty$。

從「定理 6」，我們知道所有超越擴張都是無限擴張。反過來，可以推知所有有限擴張都不是超越擴張，即都是代數擴張[4]。但這並不代表所有代數擴張都是有限擴張，例如可以證明，$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots):\mathbb{Q}$ 是無限代數擴張。

連結至數學專題
連結至周家發網頁

[4]根據我們在《感受伽羅瓦：擴張域》中提供的定義，有限擴張和無限擴張分別是指擴張次數為有限數和無限大的域擴張。