感受伽羅瓦：自同構

至此我們介紹了兩個最重要的代數結構－環與群，以及環以下最重要子類－域的基本知識。雖然在抽象代數學下，群、環和域各自形成相對獨立的分支學科「群論」(Group Theory)、「環論」(Ring Theory) 和「域論」(Field Theory)，但在某些研究中，卻要綜合運用這幾個分支學科的知識，伽羅瓦理論正能體現這類研究的特點。在本章，我們將重點介紹一個結合群論與域論知識的概念－域上的「自同構」。

我們在《感受伽羅瓦：環的同態與同構》和《感受伽羅瓦：群的同態與同構》中介紹了環和群的「同構」，指出兩個環 R 和 S (或者兩個群 G 和 H) 之間的同構就是從 R 到 S (或者從 G 到 H) 的一個一一到上函數 θ，並且這個函數保留上述兩個環 (或者群) 中元素之間的運算關係。現在如果在上述定義中，θ 所聯繫的兩個環 (或者群) 是同一個環 (或者群)，那麼這個同構就稱為自同構(automorphism)。

從上述定義可見，自同構是同構的次類。此外，根據 θ 所聯繫的兩個代數結構的類別，可以有「環自同構」(其中包含「域自同構」這個次類) 和「群自同構」。不過，伽羅瓦理論所研究的自同構是「域自同構」，以下所討論的自同構一律都是「域自同構」。更具體地說，設 $(F,+,\times)$ 為域，則 F 上的自同構就是一個從 F 到 F 的一一到上函數 $\theta : F \to F$，使得對任何 $a,b \in F$，均有

$$\begin{aligned} \theta(a+b) &= \theta(a)+\theta(b) \qquad (1) \\ \theta(a\times b) &= \theta(a)\times\theta(b) \qquad (2) \end{aligned}$$

以下把 F 上的自同構組成的集合記作 $\mathrm{Aut}(F)$。以複數域 $\mathbb{C}$ 為例，如用 $^-$ 代表把複數映射為其共軛複數的函數 (即若 $z=x+yi$，則 $\overline{z}=x-yi$)，那麼 $^-\in\mathrm{Aut}(\mathbb{C})$，因為這是一個一一到上函數，並且容易驗證，這個函數滿足上述 (1) 和 (2)，即對任何 $z_1,z_2\in\mathbb{C}$，均有

$$\begin{aligned} \overline{z_1+z_2} &= \overline{z_1}+\overline{z_2} \\ \overline{z_1\times z_2} &= \overline{z_1}\times\overline{z_2} \end{aligned}$$

在一個域上，可以有不只一個自同構。仍以 $\mathbb{C}$ 為例，如用 I 代表 $\mathbb{C}$ 上的恆等函數 (即對任何 $z\in\mathbb{C}$，均有 $I(z)=z$)，則 $I\in\mathrm{Aut}(\mathbb{C})$。

請注意自同構作為函數，可以進行複合，而且所得結果也是一個函數。例如前述的 $^-$ 便可以與自身複合，由於若 $z = x + yi$，則 $\overline{\overline{z}} = \overline{x - yi} = x + yi = z$，可知兩個 $^-$ 進行複合的結果等於恆等映射。如用 $\circ$ 代表複合運算，那麼可以把上述結果記作 $^- \circ {}^- = I$。當然，$\mathbb{C}$ 上的兩個自同構 I 與 $^-$ 還可以進行其他複合，例如 $I \circ I = I$，$I \circ {}^- = {}^-$，等等。

我們在《感受伽羅瓦：群的基本概念》中曾指出，某些函數組成的集合連同這些函數之間的複合運算構成群，由於自同構本質上是函數，因此自同構連同自同構之間的複合運算也可構成群。仍以 $\mathbb{C}$ 為例，容易看到 $(\{I, \neg\}, \circ)$ 構成一個群，因為這個群的兩個元素在 $\circ$ 運算下封閉，其單位元是 I，並且每個元素以自身作為逆元。除了 I 和 $^-$ 外，$\mathbb{C}$ 上還有其他無限多個自同構。可以證明，這些自同構 (即 $\mathrm{Aut}(\mathbb{C})$ 的成員) 也構成一個群，而 $\{I, \neg\}$ 則是 $\mathrm{Aut}(\mathbb{C})$ 的子群。

至此我們看到域與群概念的一個奇妙結合，本章所介紹的自同構是域上的自同構，但由於自同構是函數，這些自同構本身又構成一個群。請注意在這裡，群這個概念被提升到一個更抽象的層次，因為這不是由普通函數組成的群，而是由自同構這種把域映射到域的抽象函數組成的群。

我們在《感受伽羅瓦：排列與對稱多項式》中曾介紹「排列」的概念，排列就是從集合 X 到 X 的一一到上函數。根據此定義，可見自同構也可看成一種排列，但自同構不是普通的排列，因為它必須滿足條件 (1) 和 (2)，上述條件大大限制了自同構的範圍。以有理數域 $\mathbb{Q}$ 為例，如定義以下函數 ϕ：對任何 $n \in \mathbb{Q}$，均有 $\phi(n) = n + 1$，那麼容易看到 ϕ 是 $\mathbb{Q}$ 上的一個排列。但 ϕ 卻不是 $\mathbb{Q}$ 上的自同構，因為它不滿足條件 (1) 和 (2)，例如一方面我們有 $\phi(0 + 1) = \phi(1) = 2$，另一方面我們亦有 $\phi(0) + \phi(1) = 1 + 2 = 3$，因此 $\phi(0 + 1) \neq \phi(0) + \phi(1)$。

事實上，$\mathbb{Q}$ 上只有一個自同構－恆等函數，現證明如下。設 θ_1 為 $\mathbb{Q}$ 上的自同構，那麼由於 $1 \times 1 = 1$，根據條件 (2)，必有 $\theta_1(1) = \theta_1(1) \times \theta_1(1)$，即 $\theta_1(1) = 0$ 或 $\theta_1(1) = 1$。但根據《感受伽羅瓦：環的同態與同構》中的「定理 1(i)」，對任何域 (域是環的次類) 上的自同構 (同構是同態的次類) θ_1 而言，必有 $\theta_1(0) = 0$，因此不可能有 $\theta_1(1) = 0$ (因為如果同時有 $\theta_1(0) = 0$ 和 $\theta_1(1) = 0$，θ_1 便不是一一函數)，故只可能有 $\theta_1(1) = 1$。

由此根據條件 (1)，必有 $\theta_1(2) = \theta_1(1 + 1) = \theta_1(1) + \theta_1(1) = 2$。由此再根據數學歸納法，可知對任何正整數 n，必有 $\theta_1(n) = n$。設 n 為正整數，那麼 $0 = \theta_1(0) = \theta_1(n + (-n)) = \theta_1(n) + \theta_1(-n) = n + \theta_1(-n)$，故必有 $\theta_1(-n) = -n$。至此證得對任何 $n \in \mathbb{Z}$，都有 $\theta_1(n) = n$。

接著考慮任意有理數 $r = \frac{a}{b}$，其中 $a, b \in \mathbb{Z}$ 並且 $b \neq 0$。由於 $a = r \times b$，根據條件 (2)，必有 $\theta_1(a) = \theta_1(r) \times \theta_1(b)$，由此得 $\theta_1(r) = \frac{\theta_1(a)}{\theta_1(b)} = \frac{a}{b} = r$。至此證得對任何 $r \in \mathbb{Q}$，都有 $\theta_1(r) = r$，即 θ_1 是 $\mathbb{Q}$ 上的恆等函數。如沿用 I 代表恆等函數，那麼我們有 $\mathrm{Aut}(\mathbb{Q}) = \{I\}$。實數的情況類似有理數，即我們有 $\mathrm{Aut}(\mathbb{R}) = \{I\}$，但證明較繁複，這裡從略。

$\mathbb{C}$ 的情況則較複雜，如前所述，$\mathrm{Aut}(\mathbb{C})$ 包含無限多個成員。但我們可以只考慮這個集合中具有某種特別性質的成員，即把任何實數 (實數域是複數域的子域，亦即複數域是實數域的擴張域) 都映射為自身的自同構。數學上把被函數 θ 映射為自身的元素稱為 θ 的不動點(fixed point)，因此上述自同構也就是以實數作為不動點的自同構。現在讓我們看 $\mathrm{Aut}(\mathbb{C})$ 中哪些成員以實數作為不動點，設 θ_2 為具有這種性質的自同構，由於複數具有 $x + yi$ 的形式，其中 x 和 y 是實數，而 θ_2 以實數為不動點，故必有 $\theta_2(x) = x$ 和 $\theta_2(y) = y$。由此根據自同構的性質 (1) 和 (2)，我們有

$$\begin{aligned} \theta_2(x + yi) &= \theta_2(x) + \theta_2(y) \times \theta_2(i) \\ &= x + y \times \theta_2(i) \end{aligned}$$

由此可知，為確定 θ_2 對任何複數 $x + yi$ 的作用，只需確定 $\theta_2(i)$ 的值。另一方面，根據 $-1 = i \times i$ 此一事實和自同構的性質 (2)，我們又有 (請注意 -1 是實數)：

$$-1 = \theta_2(-1) = \theta_2(i \times i) = \theta_2(i) \times \theta_2(i)$$

從上式可得到二次方程 $(\theta_2(i))^2 = -1$，並解得 $\theta_2(i) = \pm i$。至此我們看到，$\mathrm{Aut}(\mathbb{C})$ 中只有兩個成員以實數作為不動點，其中一個把 i 映射為 i，此即恆等函數 I；另一個則把 i 映射為 $-i$，此即把複數映射為共軛複數的函數 $^-$。

我們可以把上述 $\mathbb{C}$ 與 $\mathbb{R}$ 的關係推廣到一般情況。給定域 F 及其擴張域 E，我們把 E 上以 F 的全體元素作為不動點的自同構組成一個集合，可以證明，這個集合的成員構成 $\mathrm{Aut}(E)$ 的一個子群，這個群稱為 F 上 E 的伽羅瓦群(Galois group)，記作 $\mathrm{Gal}(E : F)$，即

$$\mathrm{Gal}(E : F) = \{\theta \in \mathrm{Aut}(E) : \text{對任何 } a \in F, \text{ 都有} \theta(a) = a\} \qquad (3)$$

反過來，給定 $\mathrm{Aut}(E)$ 的某個子群 G，我們把 E 中同時作為 G 中每一個成員的不動點的元素組成一個集合，可以證明，這個集合的成員構成 E 的一個子域，稱為 G 的不動域(fixed field)，記作 $\mathrm{Fix}_E(G)$，即

$$\mathrm{Fix}_E(G) = \{a \in E : \text{對任何 } \theta \in G, \text{ 都有} \theta(a) = a\} \qquad (4)$$

請注意根據上述定義，$\mathrm{Gal}(E : F)$ 的成員是 E 上的自同構，而 $\mathrm{Fix}_E(G)$ 的成員則是 E 的元素，請不要將兩者混淆。

以下用一些例子說明上述概念，前面說過 $\mathrm{Aut}(\mathbb{C})$ 中只有 I 和 $^-$ 這兩個成員以實數作為不動點，故有

$$\mathrm{Gal}(\mathbb{C}:\mathbb{R}) = \{I, ^-\} \qquad (5)$$

反過來，考慮自同構群 $\{I, ^-\}$。一方面，這個群中的兩個成員的不動點都包含全體實數；另一方面，雖然 I 的不動點還包含全體複數，但 $^-$ 的不動點卻不包含實數以外的數，這是因為如果 $x+yi$ 是 $^-$ 的不動點，則有 $x-yi = x+yi$，由此必有 $y=0$，這即是說 $^-$ 的不動點只能是實數。根據以上討論，只有實數才能同時作為 I 和 $^-$ 的不動點，故有

$$\mathrm{Fix}_{\mathbb{C}}(\{I, ^-\}) = \mathbb{R} \qquad (6)$$

接著考慮另一個跟上述例子很相似的例子，試考慮 $\mathbb{Q}$ 及其擴張域 $\mathbb{Q}(\sqrt{2})$。由於 $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$ 在形式上跟 $\mathbb{C} = \{x+yi : x,y \in \mathbb{R}\}$ 很相似，而且 $\sqrt{2}$ 跟 i 一樣也是某個實數的平方根，運用跟上面相似的推理，容易求得 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}):\mathbb{Q})$ 只有兩個成員，其中一個把 $\sqrt{2}$ 映射為 $\sqrt{2}$，即恆等函數 (以下記作 I)；另一個則把 $\sqrt{2}$ 映射為 $-\sqrt{2}$ (以下記作 α)，即

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}):\mathbb{Q}) = \{I, \alpha\} \qquad (7)$$

反過來，考慮自同構群 $\{I, \alpha\}$，同樣運用跟上面相似的推理，容易求得

$$\mathrm{Fix}_{\mathbb{Q}(\sqrt{2})}(\{I, \alpha\}) = \mathbb{Q} \qquad (8)$$

接下來考慮一些較複雜的擴張域，首先考慮 $\mathbb{Q}(\sqrt{3},\sqrt{5})$。設 θ_3 為伽羅瓦群 $\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q})$ 的成員，由於 $\mathbb{Q}(\sqrt{3},\sqrt{5}) = \{a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15} : a,b,c,d \in \mathbb{Q}\}$，根據自同構的性質，我們有

$$\begin{aligned} & \theta_3(a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15}) \\ = \;& \theta_3(a) + \theta_3(b)\times\theta_3(\sqrt{3}) + \theta_3(c)\times\theta_3(\sqrt{5}) + \theta_3(d)\times\theta_3(\sqrt{15}) \\ = \;& a + b\times\theta_3(\sqrt{3}) + c\times\theta_3(\sqrt{5}) + d\times\theta_3(\sqrt{3})\times\theta_3(\sqrt{5}) \end{aligned}$$

由此可知，為確定 θ_3，只需確定 $\theta_3(\sqrt{3})$ 和 $\theta_3(\sqrt{5})$ 的值。另一方面，我們又有

$$3 = \theta_3(3) = \theta_3((\sqrt{3})^2) = (\theta_3(\sqrt{3}))^2$$

$$5 = \theta_3(5) = \theta_3((\sqrt{5})^2) = (\theta_3(\sqrt{5}))^2$$

從以上兩個二次方程可解得 $\theta_3(\sqrt{3}) = \pm\sqrt{3}$ 和 $\theta_3(\sqrt{5}) = \pm\sqrt{5}$。

至此我們看到，$\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q})$ 共有四個成員 (以下稱為 θ_{31} 至 θ_{34})，以下列出這四個成員對 $\sqrt{3}$ 和 $\sqrt{5}$ 的作用：

$$\begin{array}{lcllcl}
\theta_{31}(\sqrt{3}) &=& \sqrt{3} & \theta_{31}(\sqrt{5}) &=& \sqrt{5} \\
\theta_{32}(\sqrt{3}) &=& -\sqrt{3} & \theta_{32}(\sqrt{5}) &=& \sqrt{5} \\
\theta_{33}(\sqrt{3}) &=& \sqrt{3} & \theta_{33}(\sqrt{5}) &=& -\sqrt{5} \\
\theta_{34}(\sqrt{3}) &=& -\sqrt{3} & \theta_{34}(\sqrt{5}) &=& -\sqrt{5}
\end{array}$$

請注意 $\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q})$ 不可能包含一個成員 θ_{35}，使得 $\theta_{35}(\sqrt{5})=\sqrt{3}$，這是因為根據 θ_{35} 的此一性質，我們必有 $\theta_{35}(5)=\theta_{35}(\sqrt{5}\times\sqrt{5})=\theta_{35}(\sqrt{5})\times\theta_{35}(\sqrt{5})=\sqrt{3}\times\sqrt{3}=3\neq 5$。但這麼一來，5 便不是 θ_{35} 的不動點，因此 θ_{35} 不可能是 $\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q})$ 的成員。

在上述四個自同構中，θ_{31} 顯然就是恆等函數，故以下將之改寫為 I；而 θ_{34} 則等於 θ_{32} 與 θ_{33} 的複合，故以下將之改寫為 $\theta_{32}\theta_{33}$。經改寫後，我們有

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q})=\{I,\theta_{32},\theta_{33},\theta_{32}\theta_{33}\} \qquad (9)$$

容易驗證，這個集合的確構成一個群。

反過來，考慮自同構群 $\{I,\theta_{32},\theta_{33},\theta_{32}\theta_{33}\}$。一方面，這個群中的四個成員的不動點都包含全體有理數；另一方面，除了 I 外，其餘三個自同構都有一些 $\mathbb{Q}$ 以外的元素並非其不動點，例如對 θ_{32} 來說，$\sqrt{3}$ 並非其不動點；對 θ_{33} 來說，$\sqrt{5}$ 並非其不動點；對 $\theta_{32}\theta_{33}$ 來說，$\sqrt{3}$ 和 $\sqrt{5}$ 都並非其不動點，因此只有 $\mathbb{Q}$ 的元素才同時作為這四個自同構的不動點，故有

$$\mathrm{Fix}_{\mathbb{Q}(\sqrt{3},\sqrt{5})}(\{I,\theta_{32},\theta_{33},\theta_{32}\theta_{33}\})=\mathbb{Q} \qquad (10)$$

接著考慮 $\mathbb{Q}(\sqrt[3]{2})$。設 θ_4 為伽羅瓦群 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})$ 的成員，由於 $\mathbb{Q}(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2 : a,b,c\in\mathbb{Q}\}$，根據自同構的性質，我們有

$$\begin{array}{rcl}
\theta_4(a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2) &=& \theta_4(a)+\theta_4(b)\times\theta_4(\sqrt[3]{2})+\theta_4(c)\times\theta_4((\sqrt[3]{2})^2) \\
&=& a+b\times\theta_4(\sqrt[3]{2})+c\times(\theta_4(\sqrt[3]{2}))^2
\end{array}$$

由此可知，為確定 θ_4，只需確定 $\theta_4(\sqrt[3]{2})$ 的值。另一方面，我們又有

$$2=\theta_4(2)=\theta_4((\sqrt[3]{2})^3)=(\theta_4(\sqrt[3]{2}))^3$$

雖然三次方程 $(\theta_4(\sqrt[3]{2}))^3=2$ 有三個解，但根據我們在《感受伽羅瓦：二次方程與複數》中介紹的求根方法，在這三個解中，只有 $\sqrt[3]{2}$ 才是實數，由於 $\mathbb{Q}(\sqrt[3]{2})$ 的元素全是實數，我們在這裡只能取 $\theta_4(\sqrt[3]{2})=\sqrt[3]{2}$ 這個解。因此 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})$ 只有一個成員，這就是把 $\sqrt[3]{2}$ 映射為 $\sqrt[3]{2}$ 的恆等函數 I，即

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})=\{I\} \qquad (11)$$

反過來，考慮自同構群 $\{I\}$，由於任何元素都是恆等函數 I 的不動點，故有

$$\mathrm{Fix}_{\mathbb{Q}(\sqrt[3]{2})}(\{I\}) = \mathbb{Q}(\sqrt[3]{2}) \qquad (12)$$

(11) 中所示結果很簡單，這是因為 $\mathbb{Q}(\sqrt[3]{2})$ 並不包含三次方程 $(\theta_3(\sqrt[3]{2}))^3 = 2$ 的所有解。現在如果考慮一個比 $\mathbb{Q}(\sqrt[3]{2})$ 更大的擴張域 $\mathbb{Q}(\sqrt[3]{2}, \omega_3)$ (其中 ω_3 代表 1 的主幅角為 $\frac{2\pi}{3}$ 的立方根)[1]，情況將大為不同。

設 θ_5 為伽羅瓦群 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega_3) : \mathbb{Q})$ 的成員，由於 $\mathbb{Q}(\sqrt[3]{2}, \omega_3) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 + d\omega_3 + e\omega_3(\sqrt[3]{2}) + f\omega_3(\sqrt[3]{2})^2 : a, b, c, d, e, f \in \mathbb{Q}\}$，根據與前面類似的推理，我們知道如要確定 θ_5，只需確定 $\theta_5(\sqrt[3]{2})$ 和 $\theta_5(\omega_3)$ 的值。一方面，根據前面的討論，我們知道 $\theta_5(\sqrt[3]{2})$ 必然是三次方程 $(\theta_5(\sqrt[3]{2}))^3 = 2$ 的三個解，即 $\sqrt[3]{2}$、$\omega_3(\sqrt[3]{2})$ 和 ${\omega_3}^2(\sqrt[3]{2})$。另一方面，根據我們在《感受伽羅瓦：二次方程與複數》中介紹的知識，ω_3 滿足 ${\omega_3}^3 = 1$ 和 $1 + \omega_3 + {\omega_3}^2 = 0$，因此根據自同構的性質，$\theta_5(\omega_3)$ 必須滿足以下兩條方程：

$$\begin{cases} (\theta_5(\omega_3))^3 = 1 \\ 1 + \theta_5(\omega_3) + (\theta_5(\omega_3))^2 = 0 \end{cases}$$

從上面第一條方程我們知道 $\theta_5(\omega_3)$ 必須是 1 的立方根，但在 1 的三個立方根，即 1、ω_3 和 ${\omega_3}^2$ 中，只有 ω_3 和 ${\omega_3}^2$ 滿足上面第二條方程，因此 $\theta_5(\omega_3)$ 等於 ω_3 或 ${\omega_3}^2$。

至此我們看到，$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega_3) : \mathbb{Q})$ 共有六個成員 (以下稱為 θ_{51} 至 θ_{56})，以下列出這六個成員對 $\sqrt[3]{2}$ 和 ω_3 的作用：

$$\begin{array}{rclrcl}
\theta_{51}(\sqrt[3]{2}) &=& \sqrt[3]{2} & \theta_{51}(\omega_3) &=& \omega_3 \\
\theta_{52}(\sqrt[3]{2}) &=& \omega_3(\sqrt[3]{2}) & \theta_{52}(\omega_3) &=& {\omega_3}^2 \\
\theta_{53}(\sqrt[3]{2}) &=& {\omega_3}^2(\sqrt[3]{2}) & \theta_{53}(\omega_3) &=& \omega_3 \\
\theta_{54}(\sqrt[3]{2}) &=& \sqrt[3]{2} & \theta_{54}(\omega_3) &=& {\omega_3}^2 \\
\theta_{55}(\sqrt[3]{2}) &=& \omega_3(\sqrt[3]{2}) & \theta_{55}(\omega_3) &=& \omega_3 \\
\theta_{56}(\sqrt[3]{2}) &=& {\omega_3}^2(\sqrt[3]{2}) & \theta_{56}(\omega_3) &=& {\omega_3}^2
\end{array}$$

在上述六個自同構中，$\theta_{51} = I$。此外，還有 $\theta_{54} = \theta_{52}{\theta_{53}}^2$、$\theta_{55} = {\theta_{53}}^2$ 以及 $\theta_{56} = \theta_{52}\theta_{53}$，讀者可自行證明這一點。舉例說，如要證明 $\theta_{54} = \theta_{52}{\theta_{53}}^2$，可以作如下計算：

$$\begin{array}{rcl}
\theta_{52}{\theta_{53}}^2(\sqrt[3]{2}) &=& \theta_{52}(\theta_{53}(\theta_{53}(\sqrt[3]{2}))) \\
&=& \theta_{52}(\theta_{53}({\omega_3}^2(\sqrt[3]{2}))) \\
&=& \theta_{52}((\theta_{53}(\omega_3))^2 \times \theta_{53}(\sqrt[3]{2}))
\end{array}$$

[1]我們曾在《感受伽羅瓦：代數擴張與超越擴張》中討論這個擴張域。

$$
\begin{aligned}
&= \theta_{52}({\omega_3}^2 \times {\omega_3}^2(\sqrt[3]{2})) \\
&= (\theta_{52}(\omega_3))^2 \times (\theta_{52}(\omega_3))^2 \times \theta_{52}(\sqrt[3]{2}) \\
&= ({\omega_3}^2)^2 \times ({\omega_3}^2)^2 \times \omega_3(\sqrt[3]{2}) \\
&= \sqrt[3]{2} \\
&= \theta_{54}(\sqrt[3]{2}) \\
\theta_{52}{\theta_{53}}^2(\omega_3) &= \theta_{52}(\theta_{53}(\theta_{53}(\omega_3))) \\
&= \theta_{52}(\theta_{53}(\omega_3)) \\
&= \theta_{52}(\omega_3) \\
&= {\omega_3}^2 \\
&= \theta_{54}(\omega_3)
\end{aligned}
$$

經上述改寫後，我們有

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega_3):\mathbb{Q}) = \{I, \theta_{52}, \theta_{53}, {\theta_{53}}^2, \theta_{52}\theta_{53}, \theta_{52}{\theta_{53}}^2\} \qquad (13)$$

容易驗證，這個集合的確構成一個群。把上述結果跟 (11) 比較，可以看到,採用一個比 $\mathbb{Q}(\sqrt[3]{2})$ 更大的擴張域後,所得到的伽羅瓦群增添了很多成員。

反過來，考慮自同構群 $\{I, \theta_{52}, \theta_{53}, {\theta_{53}}^2, \theta_{52}\theta_{53}, \theta_{52}{\theta_{53}}^2\}$。一方面，這個群中的六個成員的不動點都包含全體有理數；另一方面，除了 I 外，其餘五個自同構都有一些 $\mathbb{Q}$ 以外的元素並非其不動點，例如對 θ_{53} 和 ${\theta_{53}}^2$ 來說，$\sqrt[3]{2}$ 並非其不動點；對 $\theta_{52}{\theta_{53}}^2$ 來說，ω_3 並非其不動點；對 θ_{52} 和 $\theta_{52}\theta_{53}$ 來說，$\sqrt[3]{2}$ 和 ω_3 都並非其不動點，因此只有 $\mathbb{Q}$ 的元素才同時作為這六個自同構的不動點，故有

$$\mathrm{Fix}_{\mathbb{Q}(\sqrt[3]{2},\omega_3)}(\{I, \theta_{52}, \theta_{53}, {\theta_{53}}^2, \theta_{52}\theta_{53}, \theta_{52}{\theta_{53}}^2\}) = \mathbb{Q} \qquad (14)$$

從上述例子，讀者應可看到伽羅瓦群和不動域是互相相對的概念：給定 E 的某個子域 F，我們可以求 E 上的自同構群 $\mathrm{Gal}(E:F)$；給定 E 上某個自同構群 G，我們可以求 E 的子域 $\mathrm{Fix}_E(G)$。現在如果把 $\mathrm{Fix}_E(G)$ 代入 $\mathrm{Gal}(E:F)$ 中的 F，所得結果 $\mathrm{Gal}(E:\mathrm{Fix}_E(G))$ 是甚麼？反過來，如果把 $\mathrm{Gal}(E:F)$ 代入 $\mathrm{Fix}_E(G)$ 中的 G,所得結果 $\mathrm{Fix}_E(\mathrm{Gal}(E:F))$ 又是甚麼？

回顧上面的 (5)、(6)、(7)、(8)、(9)、(10)、(13)、(14)，我們發現以下有趣的結果 (為免使以下結果過於冗長，以下用 G_1 代替 $\{I, \theta_{32}, \theta_{33}, \theta_{32}\theta_{33}\}$，用 G_2 代替 $\{I, \theta_{52}, \theta_{53}, {\theta_{53}}^2, \theta_{52}\theta_{53}, \theta_{52}{\theta_{53}}^2\}$)：

$$
\begin{aligned}
\mathrm{Gal}(\mathbb{C}:\mathrm{Fix}_{\mathbb{C}}(\{I,\bar{}\})) &= \{I,\bar{}\} \\
\mathrm{Gal}(\mathbb{Q}(\sqrt{2}):\mathrm{Fix}_{\mathbb{Q}(\sqrt{2})}(\{I,\alpha\})) &= \{I,\alpha\} \\
\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathrm{Fix}_{\mathbb{Q}(\sqrt{3},\sqrt{5})}(G_1)) &= G_1 \\
\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega_3):\mathrm{Fix}_{\mathbb{Q}(\sqrt[3]{2},\omega_3)}(G_2)) &= G_2
\end{aligned}
$$

$$\begin{aligned}
\mathrm{Fix}_{\mathbb{C}}(\mathrm{Gal}(\mathbb{C}:\mathbb{R})) &= \mathbb{R} \\
\mathrm{Fix}_{\mathbb{Q}(\sqrt{2})}(\mathrm{Gal}(\mathbb{Q}(\sqrt{2}):\mathbb{Q})) &= \mathbb{Q} \\
\mathrm{Fix}_{\mathbb{Q}(\sqrt{3},\sqrt{5})}(\mathrm{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q})) &= \mathbb{Q} \\
\mathrm{Fix}_{\mathbb{Q}(\sqrt[3]{2},\omega_3)}(\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega_3):\mathbb{Q})) &= \mathbb{Q}
\end{aligned}$$

從上述結果我們似乎可以得到以下結論：

$$\mathrm{Gal}(E:\mathrm{Fix}_E(G)) = G \qquad (15)$$

$$\mathrm{Fix}_E(\mathrm{Gal}(E:F)) = F \qquad (16)$$

以上是十分理想的結論，因為如果我們把求 $\mathrm{Gal}(E:F)$ 和 $\mathrm{Fix}_E(G)$ 的過程分別看成作用於域 F 和群 G 上的函數 (請注意 E 在這裡是固定不變的，只有 F 和 G 才是可變的)，那麼 (15) 和 (16) 是說，這兩個函數互為逆函數。

可是，上述結論並不總是成立，回顧上面的 (11) 和 (12)，可以發現

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathrm{Fix}_{\mathbb{Q}(\sqrt[3]{2})}(\{I\})) = \{I\}^2$$

$$\mathrm{Fix}_{\mathbb{Q}(\sqrt[3]{2})}(\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}:\mathbb{Q})) = \mathbb{Q}(\sqrt[3]{2})$$

上面第一個結果符合 (15)，但第二個結果卻不符合 (16)，這顯示 (15) 和 (16) 這兩個理想結果依賴於某些條件，伽羅瓦理論的一個主要內容就是對這些條件的總結，這將是接下來的章節的內容。

連結至數學專題
連結至周家發網頁

[2]為得到此一結果，要先求得 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}(\sqrt[3]{2})) = \{I\}$，但此一結果不難得到，因為以整個域的全體元素作為不動點的自同構顯然只有恆等函數 I。