感受伽羅瓦：伽羅瓦理論基本定理

本章的主旨是介紹伽羅瓦理論的核心知識－「伽羅瓦理論基本定理」。一言以蔽之，伽羅瓦理論基本定理就是有關「伽羅瓦對應」的定理，上兩章其實已包含伽羅瓦理論基本定理的一些基本內容，本章目的是重溫這些內容，補充前兩章沒有介紹的內容，並提供有關實例。

首先提供伽羅瓦理論基本定理的內容如下 (在以下定理中，$\subseteq$ 代表子域或子群關係，$|\ |$ 代表域擴張的次數或者群的階，$/$ 代表商群關係)：

定理 1 (伽羅瓦理論基本定理Fundamental Theorem of Galois Theory)：設 $E:F$ 為伽羅瓦擴張，K 為 F 與 E 之間的中間域 (包括 F 和 E 這兩者)，H 為 $\mathrm{Gal}(E:F)$ 的子群，則

(i) $\mathrm{Gal}(E:K)$ 是 $\mathrm{Gal}(E:F)$ 的子群，$\mathrm{Fix}_E(H)$ 是 F 與 E 之間的中間域。

(ii) $\mathrm{Gal}(E:\cdot)$(即求伽羅瓦群的函數) 與 Fix_E (即求不動域的函數) 互為逆函數，此一關係可以概括為，中間域 K 與子群 H 存在對應關係當且僅當以下兩等式同時成立：

$$\begin{aligned} \mathrm{Gal}(E:K) &= H \qquad (1) \\ \mathrm{Fix}_E(H) &= K \qquad (2) \end{aligned}$$

(iii) 上述逆函數關係使上述中間域與子群之間形成反向包含的一一對應關係。這即是說，設中間域 K_1 和 K_2 分別與子群 H_1 和 H_2 存在對應關係，若 $K_1 \subseteq K_2$，則 $H_2 \subseteq H_1$；反之，若 $H_1 \subseteq H_2$，則 $K_2 \subseteq K_1$。

(iv) 域擴張的次數與伽羅瓦群的階存在以下對應關係：

(a)
$$|E:K| = |\mathrm{Gal}(E:K)| \qquad (3)$$

(b)
$$|K:F| = \frac{|\mathrm{Gal}(E:F)|}{|\mathrm{Gal}(E:K)|} \qquad (4)$$

(v) $K:F$ 是正規擴張當且僅當 $\mathrm{Gal}(E:K)$ 是 $\mathrm{Gal}(E:F)$ 的正規子群。

(vi) 若 $K:F$ 是正規擴張，則

$$\mathrm{Gal}(K:F) \cong \mathrm{Gal}(E:F)/\mathrm{Gal}(E:K) \qquad (5)$$

請注意在上述公式 (4) 和 (5) 中，如果撇除其中的 | | 和 Gal( ) 符號，把其中的 E、F 和 K 當作非零實數，並且把 : 和 / 符號一律當作除號，那麼該兩式相當於以下實數除法的結果：

$$\frac{K}{F} = \frac{E}{F} \div \frac{E}{K}$$

這是記憶上述兩式的方法。

本章的其餘部分會詳細討論一個實例，在討論過程中，我們會重溫前面各章的已有知識和例示本章引入的新知識，這個例子是四次多項式 $f = x^4 - 2$ 在 $\mathbb{Q}$ 上的分裂域，即包含 $\mathbb{Q}$ 和 f 的所有根的最小的域。容易看到，f 有以下四個根：$\sqrt[4]{2}$、$-\sqrt[4]{2}$、$i\sqrt[4]{2}$ 和 $-i\sqrt[4]{2}$。因此運用我們在《感受伽羅瓦：代數擴張與超越擴張》中分析三次多項式 $x^3 - 2$ 的相同方法，可以得知 f 的分裂域是 $\mathbb{Q}(\sqrt[4]{2}, i)$[1]。

接著考慮域擴張 $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$，它可以看成由兩個簡單擴張－ $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ 和 $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})$ 複合而成。運用我們在《感受伽羅瓦：擴張域》中介紹的方法，可以求得 $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ 的一個基底是 $\{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3\}$，故有 $|\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| = 4$；而 $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})$ 的一個基底是 $\{1, i\}$，故有 $|\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})| = 2$。

由此根據上述網頁的「定理 1」，可知 $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ 的一個基底是

$$\{1, i\} \otimes \{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3\} = \{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3, i, i\sqrt[4]{2}, i\sqrt{2}, i(\sqrt[4]{2})^3\}$$

以及

$$\begin{aligned} |\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}| &= |\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})| \times |\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}| \\ &= 2 \times 4 \\ &= 8 \end{aligned}$$

由此亦可得

$$\begin{aligned} & \mathbb{Q}(\sqrt[4]{2}, i) \\ = \; & \{a + b\sqrt[4]{2} + c\sqrt{2} + d(\sqrt[4]{2})^3 + ei + fi\sqrt[4]{2} + gi\sqrt{2} + hi(\sqrt[4]{2})^3 : \\ & a, b, c, d, e, f, g, h \in \mathbb{Q}\} \qquad (6) \end{aligned}$$

[1]請注意 i 是 1 的主幅角為 $\frac{2\pi}{4}$ 的四次方根，即 $i = \omega_4$。

從以上討論可知，$\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ 是有限擴張，因為它的次數是有限整數 (8)。另外, 由於 $\mathbb{Q}(\sqrt[4]{2}, i)$ 是 f 的分裂域, 根據《感受伽羅瓦：伽羅瓦擴張》中的「定理 1」，可知 $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ 也是正規擴張。再者，由於 $\mathbb{Q}(\sqrt[4]{2}, i)$ 是 $\mathbb{Q}$ 的擴張域，根據我們在上述網頁的討論，可知 $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ 也是可分擴張。至此看到，$\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ 同時具備有限性、正規性和可分性，因此根據上述網頁的定義, 這是伽羅瓦擴張, 因而「伽羅瓦理論基本定理」適用於這個域擴張。

接著考慮伽羅瓦群 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})$，設 $\theta \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})$，運用我們在《感受伽羅瓦：自同構》中介紹的推理，可知為確定 θ，只須確定 $\theta(\sqrt[4]{2})$ 和 $\theta(i)$ 的值，而且這兩個值必須分別滿足 $\theta(\sqrt[4]{2})^4 = 2$ 和 $\theta(i)^2 = -1$ 這兩個條件。根據第一個條件，$\theta(\sqrt[4]{2})$ 有 $\sqrt[4]{2}$、$-\sqrt[4]{2}$、$i\sqrt[4]{2}$ 和 $-i\sqrt[4]{2}$ 這四個可能值；根據第二個條件，$\theta(i)$ 有 i 和 $-i$ 這兩個可能值。

綜合以上討論，可知 θ 共有八個可能值，如用 α 代表把 $\sqrt[4]{2}$ 映射為 $i\sqrt[4]{2}$ 並把 i 映射為 i 的自同構，並且用 β 代表把 $\sqrt[4]{2}$ 映射為 $\sqrt[4]{2}$ 並把 i 映射為 $-i$ 的自同構，便可以把 θ 的八個可能值表達為 α 的冪次 (包括零冪次) 與 β 的乘積，以下列出這八個可能值的表達形式及其對 $\sqrt[4]{2}$ 和 i 的作用：

$$\begin{array}{rclcrcl}
I(\sqrt[4]{2}) &=& \sqrt[4]{2} & \qquad & I(i) &=& i \\
\alpha(\sqrt[4]{2}) &=& i\sqrt[4]{2} & & \alpha(i) &=& i \\
\alpha^2(\sqrt[4]{2}) &=& -\sqrt[4]{2} & & \alpha^2(i) &=& i \\
\alpha^3(\sqrt[4]{2}) &=& -i\sqrt[4]{2} & & \alpha^3(i) &=& i \\
\beta(\sqrt[4]{2}) &=& \sqrt[4]{2} & & \beta(i) &=& -i \\
\alpha\beta(\sqrt[4]{2}) &=& i\sqrt[4]{2} & & \alpha\beta(i) &=& -i \\
\alpha^2\beta(\sqrt[4]{2}) &=& -\sqrt[4]{2} & & \alpha^2\beta(i) &=& -i \\
\alpha^3\beta(\sqrt[4]{2}) &=& -i\sqrt[4]{2} & & \alpha^3\beta(i) &=& -i
\end{array}$$

讀者可自行驗證以上自同構對 $\sqrt[4]{2}$ 和 i 的作用是正確的，而且這些自同構滿足以下等式：

$$\begin{aligned}
\alpha^4 &= I \qquad (7) \\
\beta^2 &= I \qquad (8) \\
\beta\alpha &= \alpha^3\beta \qquad (9)
\end{aligned}$$

至此求得

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}) = \{I, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$$

接下來讓我們驗證「定理 1」，為此先要求 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})$ 的所有子群和 $\mathbb{Q}$ 與 $\mathbb{Q}(\sqrt[4]{2}, i)$ 之間的中間域，如同上一章的做法，我們先從較容易的方面－子群入手。讀者可自行驗證，$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})$ 共有以下十個子群：

$\{I, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$、$\{I, \alpha, \alpha^2, \alpha^3\}$、$\{I, \alpha^2, \beta, \alpha^2\beta\}$、$\{I, \alpha^2, \alpha\beta, \alpha^3\beta\}$、$\{I, \alpha^2\}$、$\{I, \beta\}$、$\{I, \alpha\beta\}$、$\{I, \alpha^2\beta\}$、$\{I, \alpha^3\beta\}$ 和 $\{I\}$。

接著計算上述十個子群的不動域，首先提供以下較容易得到的結果：

$$\begin{aligned}
\mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}) &= \mathbb{Q} \\
\mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I, \alpha, \alpha^2, \alpha^3\}) &= \mathbb{Q}(i) \\
\mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I, \alpha^2, \beta, \alpha^2\beta\}) &= \mathbb{Q}(\sqrt{2}) \\
\mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I, \alpha^2, \alpha\beta, \alpha^3\beta\}) &= \mathbb{Q}(i\sqrt{2}) \\
\mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I\}) &= \mathbb{Q}(\sqrt[4]{2}, i)
\end{aligned}$$

其餘的不動域可用解聯立方程的方法求得，以下是計算 $\{I, \alpha^2\}$ 的不動域的步驟。為求這個不動域的元素，要找出 $\mathbb{Q}(\sqrt[4]{2}, i)$ 中所有同時滿足等式 $I(x) = x$ 和 $\alpha^2(x) = x$ 的元素 x。由於對任何元素而言，前一等式必然成立，我們只需找出滿足後一等式的元素。為此首先根據 (6) 寫出 $\mathbb{Q}(\sqrt[4]{2}, i)$ 的任意元素

$$x = a + b\sqrt[4]{2} + c\sqrt{2} + d(\sqrt[4]{2})^3 + ei + fi\sqrt[4]{2} + gi\sqrt{2} + hi(\sqrt[4]{2})^3 \qquad (10)$$

其中 $a, b, c, d, e, f, g, h \in \mathbb{Q}$。接著計算

$$\begin{aligned}
& \alpha^2(x) \\
= \; & \alpha^2(a + b\sqrt[4]{2} + c\sqrt{2} + d(\sqrt[4]{2})^3 + ei + fi\sqrt[4]{2} + gi\sqrt{2} + hi(\sqrt[4]{2})^3) \\
= \; & a + b\alpha^2(\sqrt[4]{2}) + c(\alpha^2(\sqrt[4]{2}))^2 + d(\alpha^2(\sqrt[4]{2}))^3 + e\alpha^2(i) + f\alpha^2(i)\alpha^2(\sqrt[4]{2}) \\
& + g\alpha^2(i)(\alpha^2(\sqrt[4]{2}))^2 + h\alpha^2(i)(\alpha^2(\sqrt[4]{2}))^3 \\
= \; & a + b(-\sqrt[4]{2}) + c(-\sqrt[4]{2})^2 + d(-\sqrt[4]{2})^3 + ei + fi(-\sqrt[4]{2}) + gi(-\sqrt[4]{2})^2 \\
& + hi(-\sqrt[4]{2})^3 \\
= \; & a - b\sqrt[4]{2} + c\sqrt{2} - d(\sqrt[4]{2})^3 + ei - fi\sqrt[4]{2} + gi\sqrt{2} - hi(\sqrt[4]{2})^3 \qquad (11)
\end{aligned}$$

如要令 x 滿足等式 $\alpha^2(x) = x$，必須使 (10) 和 (11) 中等號右端各項的係數相等，即要解以下聯立方程：

$$\begin{cases}
a = a \\
b = -b \\
c = c \\
d = -d \\
e = e \\
f = -f \\
g = g \\
h = -h
\end{cases}$$

根據上述聯立方程，我們必須有 $b=d=f=h=0$，由此可知 x 是具有以下形式的數：

$$x = a + c\sqrt{2} + ei + gi\sqrt{2}$$

其中 $a,c,e,g \in \mathbb{Q}$。容易看到，具有上述形式的數構成中間域 $\mathbb{Q}(\sqrt{2},i)$，至此求得

$$\mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I,\alpha^2\}) = \mathbb{Q}(\sqrt{2},i)$$

上述計算尚算簡單，接下來看一個較複雜的例子，讓我們用上述方法求 $\{I,\alpha\beta\}$ 的不動域。運用類似上面的推理，為求這個不動域，只需找出所有滿足等式 $\alpha\beta(x)=x$ 的元素 x。讀者可自行驗證，我們有

$$\alpha\beta(x) = a + f\sqrt[4]{2} - c\sqrt{2} - h(\sqrt[4]{2})^3 - ei + bi\sqrt[4]{2} + gi\sqrt{2} - di(\sqrt[4]{2})^3$$

由此可得以下聯立方程：

$$\begin{cases} a = a \\ b = f \\ c = -c \\ d = -h \\ e = -e \\ f = b \\ g = g \\ h = -d \end{cases}$$

根據上述聯立方程，我們必須有 $c=e=0$、$b=f$ 和 $d=-h$，由此可知 x 是具有以下形式的數：

$$\begin{aligned} x &= a + b\sqrt[4]{2} + d(\sqrt[4]{2})^3 + bi\sqrt[4]{2} + gi\sqrt{2} - di(\sqrt[4]{2})^3 \\ &= a + b(1+i)\sqrt[4]{2} + gi\sqrt{2} + d(1-i)(\sqrt[4]{2})^3 \\ &= a + b(1+i)\sqrt[4]{2} + \frac{g}{2}(1+2i-1)\sqrt{2} - \frac{d}{2}(1+3i-3-i)(\sqrt[4]{2})^3 \\ &= a + b(1+i)\sqrt[4]{2} + \frac{g}{2}((1+i)\sqrt[4]{2})^2 - \frac{d}{2}((1+i)\sqrt[4]{2})^3 \end{aligned}$$

其中 $a,b,d,g \in \mathbb{Q}$。容易看到，具有上述形式的數構成中間域 $\mathbb{Q}((1+i)\sqrt[4]{2})$，至此求得

$$\mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I,\alpha\beta\}) = \mathbb{Q}((1+i)\sqrt[4]{2})$$

利用上述方法，還可求得其餘三個不動域如下：

$$\begin{aligned} \mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I,\beta\}) &= \mathbb{Q}(\sqrt[4]{2}) \\ \mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I,\alpha^2\beta\}) &= \mathbb{Q}(i\sqrt[4]{2}) \\ \mathrm{Fix}_{\mathbb{Q}(\sqrt[4]{2},i)}(\{I,\alpha^3\beta\}) &= \mathbb{Q}((1-i)\sqrt[4]{2}) \end{aligned}$$

上述計算所得的十個不動域都是 $\mathbb{Q}$ 與 $\mathbb{Q}(\sqrt[4]{2},i)$ 之間的中間域，這十個中間域是 $\mathbb{Q}$、$\mathbb{Q}(i)$、$\mathbb{Q}(\sqrt{2})$、$\mathbb{Q}(i\sqrt{2})$、$\mathbb{Q}(\sqrt[4]{2},i)$、$\mathbb{Q}(\sqrt{2},i)$、$\mathbb{Q}((1+i)\sqrt[4]{2})$、$\mathbb{Q}(\sqrt[4]{2})$、$\mathbb{Q}(i\sqrt[4]{2})$ 和 $\mathbb{Q}((1-i)\sqrt[4]{2})$。原則上我們可以逐一就這十個中間域計算相關的伽羅瓦群，但基於「定理 1(ii)」中的公式 (1) 和 (2)，我們可以省卻這些計算。舉例說，根據上面最後一個有關不動域的計算結果，我們可即時得到

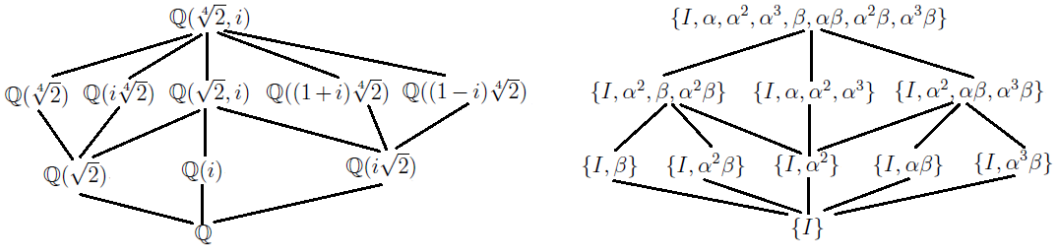
$$\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}((1-i)\sqrt[4]{2}) = \{I,\alpha^3\beta\}$$

為證實上述結果，可以進行以下計算：

$$\begin{aligned}\alpha^3\beta((1-i)\sqrt[4]{2}) &= (\alpha^3\beta(1)-\alpha^3\beta(i))\times\alpha^3\beta(\sqrt[4]{2})\\ &= (1-(-i))\times(-i\sqrt[4]{2})\\ &= -i\sqrt[4]{2}+\sqrt[4]{2}\\ &= (1-i)\sqrt[4]{2}\end{aligned}$$

由此可見，$\alpha^3\beta$ (以及 I) 是以全體有理數和 $(1-i)\sqrt[4]{2}$ 為不動點的自同構，當然我們還要驗證其他自同構不具上述性質，經以上驗證後，便能證實上述結果。其餘九個伽羅瓦群的計算和證實方法類此。

此外，由於 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q})$ 只有前述十個子群，而根據「定理 1(iii)」，這些子群與中間域存在一一對應關係，因此 $\mathbb{Q}$ 與 $\mathbb{Q}(\sqrt[4]{2},i)$ 之間只有前述十個中間域。現把上述十個中間域和十個子群的包含關係繪成以下哈斯圖：



上面左圖中的包含關係並不難證明 (右圖中的包含關係則顯而易見，無須證明)。舉例說，以下讓我們證明 $\mathbb{Q}(i\sqrt{2})\subseteq\mathbb{Q}((1-i)\sqrt[4]{2})$。一方面，$\mathbb{Q}(i\sqrt{2})$ 中的任意元素 x 具有 $a+bi\sqrt{2}$ (其中 $a,b\in\mathbb{Q}$) 的形式；另一方面，x 又可以表達為 $a-\frac{b}{2}((1-i)\sqrt[4]{2})^2$，可見是 $\mathbb{Q}((1-i)\sqrt[4]{2})$ 的元素。至此證得 $\mathbb{Q}(i\sqrt{2})$ 中任何元素都是 $\mathbb{Q}((1-i)\sqrt[4]{2})$ 中的元素，即 $\mathbb{Q}(i\sqrt{2})\subseteq\mathbb{Q}((1-i)\sqrt[4]{2})$。

現在我們可以用上圖驗證「定理 1(iii)」中的反向包含一一對應 (即上一章介紹的「伽羅瓦對應」) 關係。舉例說，$\mathbb{Q}(\sqrt{2})$ 與 $\{I,\alpha^2,\beta,\alpha^2\beta\}$ 存在對應關係，$\mathbb{Q}(\sqrt[4]{2})$ 也與 $\{I,\beta\}$ 存在對應關係。一方面，我們有 $\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt[4]{2})$；另一方面，我們也有 $\{I,\beta\}\subseteq\{I,\alpha^2,\beta,\alpha^2\beta\}$。

接下來驗證公式 (3)，為此要先就每個中間域 K 計算擴張次數 $|\mathbb{Q}(\sqrt[4]{2}, i) : K|$，而為進行這種計算，可以先求相關域擴張的基底。舉例說，$\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt{2}, i)$ 的一個基底是 $\{1, \sqrt[4]{2}\}$。為證明這一點，我們要證明這個集合滿足《感受伽羅瓦：向量空間與子域》所述的基底的兩個條件。首先，我們有

$$\begin{aligned} & \{u + v\sqrt[4]{2} : u, v \in \mathbb{Q}(\sqrt{2}, i)\} \\ = \ & \{(a + b\sqrt{2} + ci + di\sqrt{2}) + (e + f\sqrt{2} + gi + hi\sqrt{2})\sqrt[4]{2} : \\ & a, b, c, d, e, f, g, h \in \mathbb{Q}\} \\ = \ & \{a + e\sqrt[4]{2} + b\sqrt{2} + f(\sqrt[4]{2})^3 + ci + gi\sqrt[4]{2} + di\sqrt{2} + hi(\sqrt[4]{2})^3 : \\ & a, b, c, d, e, f, g, h \in \mathbb{Q}\} \\ = \ & \mathbb{Q}(\sqrt[4]{2}, i) \end{aligned}$$

由此證得 $\langle 1, \sqrt[4]{2}\rangle = \mathbb{Q}(\sqrt[4]{2}, i)$。

其次，我們要證明 $\{1, \sqrt[4]{2}\}$ 在 $\mathbb{Q}(\sqrt{2}, i)$ 上是線性獨立的，為此，我們求解以下方程：

$$a + b\sqrt[4]{2} = 0$$

其中 $a, b \in \mathbb{Q}(\sqrt{2}, i)$，把 $a = a_1 + a_2\sqrt{2} + a_3 i + a_4 i\sqrt{2}$ 和 $b = b_1 + b_2\sqrt{2} + b_3 i + b_4 i\sqrt{2}$ (其中 $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{Q}$) 代入上式，可得

$$\begin{aligned} (a_1 + a_2\sqrt{2} + a_3 i + a_4 i\sqrt{2}) + (b_1 + b_2\sqrt{2} + b_3 i + b_4 i\sqrt{2})\sqrt[4]{2} &= 0 \\ a_1 + b_1\sqrt[4]{2} + a_2\sqrt{2} + b_2(\sqrt[4]{2})^3 + a_3 i + b_3 i\sqrt[4]{2} + a_4 i\sqrt{2} + b_4 i(\sqrt[4]{2})^3 &= 0 \end{aligned}$$

從上式可以得到 $a_1 = a_2 = a_3 = a_4 = b_1 = b_2 = b_3 = b_4 = 0$，即 $a = b = 0$，至此證得 $\{1, \sqrt[4]{2}\}$ 在 $\mathbb{Q}(\sqrt{2}, i)$ 上是線性獨立的。

請注意雖然我們也有 $\langle 1, \sqrt[4]{2}, \sqrt{2}\rangle = \mathbb{Q}(\sqrt[4]{2}, i)$，但 $\{1, \sqrt[4]{2}, \sqrt{2}\}$ 在 $\mathbb{Q}(\sqrt{2}, i)$ 上不是線性獨立的[2]，這是因為我們有

$$(\sqrt{2})(1) + (0)(\sqrt[4]{2}) + (-1)(\sqrt{2}) = 0$$

其中 $\sqrt{2}, 0, -1 \in \mathbb{Q}(\sqrt{2}, i)$，且不全為 0，由此可見 $\{1, \sqrt[4]{2}, \sqrt{2}\}$ 不是所需的基底。

至此證得 $\{1, \sqrt[4]{2}\}$ 確是 $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt{2}, i)$ 的基底，因此 $|\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt{2}, i)| = 2$，並且由 (3) 可知 $|\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt{2}, i))| = 2$，而這是正確的，因為根據前面的討論，可知 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt{2}, i)) = \{I, \alpha^2\}$。

[2]惟請注意，$\{1, \sqrt[4]{2}, \sqrt{2}\}$ 在域 $\mathbb{Q}$ 上卻是線性獨立的。這個例子顯示要判斷一個集合是否線性獨立，不僅要看該集合包含甚麼成員，還要看這個集合是相對於哪個域而言。

另外又如 $\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2})$ 的一個基底是 $\{1,i,(1+i)\sqrt[4]{2},(1-i)\sqrt[4]{2}\}$，其證明方法跟前面的例子相同，只不過計算較為繁複。因此我們有 $|\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2})|=4$，並且由 (3) 可知 $|\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2}))|=4$，而這是正確的，因為根據前面的討論，可知 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2}))=\{I,\alpha^2,\alpha\beta,\alpha^3\beta\}$。運用上面介紹的方法，可以就每個中間域 K 驗證公式 (3)。

「定理 1(i) — (iii)(a)」是有關域擴張 $E:K$，「定理 1(iii)(b) — (vi)」則是有關域擴張 $K:F$。現在我們驗證公式 (4)，為此要先就每個中間域 K 計算擴張次數 $|K:\mathbb{Q}|$。由於這些中間域都寫成簡單代數擴張 $\mathbb{Q}(a)$ 或複合代數擴張 $\mathbb{Q}(a,b)$ 的形式，我們可以透過「最小多項式」求 $|K:\mathbb{Q}|$。

舉例說，$\mathbb{Q}((1+i)\sqrt[4]{2}):\mathbb{Q}$ 是簡單代數擴張，為求相關的擴張次數，可以先求 $(1+i)\sqrt[4]{2}$ 在 $\mathbb{Q}$ 上的最小多項式，這個最小多項式是 x^4+8，以下讓我們證明這一點。首先，容易證明 $(1+i)\sqrt[4]{2}$ 是 x^4+8 的一個根。其次，要證明 x^4+8 在 $\mathbb{Q}$ 上不可約。由於這是一個四次方程，如果它可約，它的因式分解形式必然包含一次因式或二次因式。根據我們在《感受伽羅瓦：二次方程與複數》中介紹的方法，不難求得 x^4+8 的四個根為 $(1+i)\sqrt[4]{2}$、$(-1+i)\sqrt[4]{2}$、$(-1-i)\sqrt[4]{2}$ 和 $(1-i)\sqrt[4]{2}$。因此如果 x^4+8 可約，它的因式分解形式必然包含 $x-(1+i)\sqrt[4]{2}$、$x-(-1+i)\sqrt[4]{2}$、$x-(-1-i)\sqrt[4]{2}$ 和 $x-(1-i)\sqrt[4]{2}$ 這些一次因式，或者由這些一次因式相乘而得的二次因式。但上述這些一次因式全都不是有理係數一次多項式，而且把它們如何相乘都不可能得到有理係數二次多項式，由此可見 x^4+8 在 $\mathbb{Q}$ 上不可約。

以上證明了四次多項式 x^4+8 是 $(1+i)\sqrt[4]{2}$ 在 $\mathbb{Q}$ 上的最小多項式，由此根據《感受伽羅瓦：代數擴張與超越擴張》中的「定理 6」，可知 $|\mathbb{Q}((1+i)\sqrt[4]{2}):\mathbb{Q}|=4$。另一方面，根據公式 (4)，應有

$$\begin{aligned}|\mathbb{Q}((1+i)\sqrt[4]{2}):\mathbb{Q}| &= \frac{|\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q})|}{|\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}((1+i)\sqrt[4]{2}))|}\\ &= \frac{8}{2}\\ &= 4\end{aligned}$$

上述結果與前面的計算結果吻合。

另外又如 $\mathbb{Q}(\sqrt{2},i):\mathbb{Q}$ 可以看成兩重簡單代數擴張複合而成的結果。首先考慮第一重簡單代數擴張 $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$，$\sqrt{2}$ 在 $\mathbb{Q}$ 上的最小多項式是二次多項式 x^2-2，為證明這一點，應看到 $\sqrt{2}$ 是這個多項式方程的根，而且這個多項式只能因式分解為 $(x-\sqrt{2})(x+\sqrt{2})$，其中兩個因式都不是 $\mathbb{Q}[x]$ 中的成員，因此這個多項式在 $\mathbb{Q}$ 上不可約，故為所需的最小多項式。由此根

據上述網頁的「定理 6」，可知 $|\mathbb{Q}(\sqrt{2}):\mathbb{Q}|=2$。

其次考慮第二重簡單代數擴張 $\mathbb{Q}(\sqrt{2})(i):\mathbb{Q}(\sqrt{2})$，$i$ 在 $\mathbb{Q}(\sqrt{2})$ 上的最小多項式是二次多項式 x^2+1，為證明這一點，應看到 i 是這個多項式方程的根，而且這個多項式只能因式分解為 $(x-i)(x+i)$，其中兩個因式都不是 $\mathbb{Q}(\sqrt{2})[x]$ 中的成員，因此這個多項式在 $\mathbb{Q}(\sqrt{2})$ 上不可約，故為所需的最小多項式。由此根據上述網頁的「定理 6」, 可知 $|\mathbb{Q}(\sqrt{2})(i):\mathbb{Q}(\sqrt{2})|=2$。

至此求得 $|\mathbb{Q}(\sqrt{2})(i):\mathbb{Q}(\sqrt{2})|$ 和 $|\mathbb{Q}(\sqrt{2}):\mathbb{Q}|$，由此根據《感受伽羅瓦：擴張域》中的「定理 1」，可知

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

另一方面，根據公式 (4)，應有

$$\begin{aligned}|\mathbb{Q}(\sqrt{2},i):\mathbb{Q}| &= \frac{|\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q})|}{|\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(\sqrt{2},i))|}\\ &= \frac{8}{2}\\ &= 4\end{aligned}$$

上述結果與前面的計算結果吻合。

接著驗證「定理 1(v)」，這部分定理是有關「正規擴張」與「正規子群」的對應關係。根據《感受伽羅瓦：伽羅瓦擴張》中的「定理 1」，有限擴張 $E:F$ 是正規擴張當且僅當 E 是 F 上某個多項式的分裂域。另外根據《感受伽羅瓦：子群與商群》中的「定理 2」，N 是 G 的正規子群當且僅當對任何 $n\in N$ 和 $g\in G$，均有 $g\circ n\circ g^{-1}\in N$。正是由於「定理 1(v)」所示的對應關係，才使以上兩個相去甚遠的概念共同使用「正規」這個名稱。

在 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q})$ 的十個子群中，$\{I,\alpha,\alpha^2,\alpha^3,\beta,\alpha\beta,\alpha^2\beta,\alpha^3\beta\}$、$\{I,\alpha,\alpha^2,\alpha^3\}$、$\{I,\alpha^2,\beta,\alpha^2\beta\}$、$\{I,\alpha^2,\alpha\beta,\alpha^3\beta\}$、$\{I,\alpha^2\}$ 和 $\{I\}$ 是正規子群，而 $\{I,\beta\}$、$\{I,\alpha\beta\}$、$\{I,\alpha^2\beta\}$ 和 $\{I,\alpha^3\beta\}$ 則不是正規子群。為證明這一點，我們要利用前面的 (7) — (9) 進行計算。舉例說，由於

$$\begin{aligned}\alpha\circ\beta\circ\alpha^{-1} &= \alpha\circ\beta\circ\alpha^3\\ &= \alpha\circ(\beta\circ\alpha)\circ\alpha^2\\ &= \alpha\circ(\alpha^3\beta)\circ\alpha^2\\ &= \alpha^4\circ(\beta\circ\alpha)\circ\alpha\end{aligned}$$

$$\begin{aligned} &= \alpha^3\beta \circ \alpha \\ &= \alpha^3 \circ (\beta \circ \alpha) \\ &= \alpha^3 \circ \alpha^3\beta \\ &= \alpha^2\beta \end{aligned}$$

我們有 $\alpha \circ \beta \circ \alpha^{-1} \notin \{I, \beta\}$，因此 $\{I, \beta\}$ 不是正規子群。

根據以上的討論結果和「定理 1(v)」，可知 $\mathbb{Q} : \mathbb{Q}$、$\mathbb{Q}(i) : \mathbb{Q}$、$\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$、$\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}$、$\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$ 和 $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ 是正規擴張，而 $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$、$\mathbb{Q}((1+i)\sqrt[4]{2}) : \mathbb{Q}$、$\mathbb{Q}(i\sqrt[4]{2}) : \mathbb{Q}$ 和 $\mathbb{Q}((1-i)\sqrt[4]{2}) : \mathbb{Q}$ 則不是正規擴張。舉例說，容易看到 $\mathbb{Q}(i\sqrt{2})$ 是 $\mathbb{Q}$ 上多項式 x^2+2 的分裂域，因為 $\mathbb{Q}(i\sqrt{2})$ 顯然是包含 $\mathbb{Q}$ 和這個多項式所有根 (即 $i\sqrt{2}$ 和 $-i\sqrt{2}$) 的最小的域，由此根據前述《感受伽羅瓦：伽羅瓦擴張》中的「定理 1」，可知 $\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}$ 是正規擴張。另外又如 $x^4 - 2$ 是 $\mathbb{Q}$ 上的不可約多項式 (這一點可用《感受伽羅瓦：因子分解》中的「定理 8」來證明)，而 $\mathbb{Q}(\sqrt[4]{2})$ 包含這個多項式的一個根 (即 $\sqrt[4]{2}$)，但不包含所有根 (例如複數 $i\sqrt[4]{2}$)，因此根據正規擴張的定義[3]，$\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ 不是正規擴張。

最後我們用 $\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}$ 來驗證「定理 1(vi)」。容易看到 $\mathbb{Q}(i\sqrt{2}) = \{a+bi\sqrt{2} : a, b \in \mathbb{Q}\}$，而 $\mathrm{Gal}(\mathbb{Q}(i\sqrt{2}) : \mathbb{Q})$ 僅包含兩個成員，其中一個把 $i\sqrt{2}$ 映射為 $i\sqrt{2}$，此即恆等函數 I；另一個則把 $i\sqrt{2}$ 映射為 $-i\sqrt{2}$，以下記作 γ，即我們有

$$\mathrm{Gal}(\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}) = \{I, \gamma\} \qquad (12)$$

此外，γ 顯然滿足以下等式：

$$\gamma^2 = I \qquad (13)$$

另一方面，由於 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i\sqrt{2}))$ 是 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})$ 的正規子群，可知存在以下商群 (請參閱《感受伽羅瓦：子群與商群》中的「定理 3」)：

$$\begin{aligned} &\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i\sqrt{2})) \\ = \ &\{I, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}/\{I, \alpha^2, \alpha\beta, \alpha^3\beta\} \end{aligned}$$

回顧商群的定義，上述商群由兩個陪集組成，其中一個是 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i\sqrt{2})) = \{I, \alpha^2, \alpha\beta, \alpha^3\beta\}$，另一個則是 $\alpha \circ \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i\sqrt{2})) = \{\alpha, \alpha^3, \alpha^2\beta, \beta\}$，即我們有

$$\begin{aligned} &\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i\sqrt{2})) \\ = \ &\{\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i\sqrt{2})), \alpha \circ \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i\sqrt{2}))\} \qquad (14) \end{aligned}$$

[3]我們在《感受伽羅瓦：伽羅瓦擴張》中指出，$E : F$ 是正規擴張，當且僅當若 f 是 F 上的不可約多項式，並且 E 包含 f 的一個根，則 E 包含 f 的所有根。

根據上述結果，可知 (12) 和 (14) 中的兩個群同構，這是因為 I 和 γ 分別對應著陪集 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2}))$ 和 $\alpha\circ\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2}))$，其中陪集 $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2}))$ 扮演著前述商群中單位元的角色 (正如 I 扮演著 $\{I,\gamma\}$ 中單位元的角色那樣)。此外，我們還有

$$\begin{aligned}(\alpha\circ\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2})))^2 &= \alpha^2\circ\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2}))\\ &= \{\alpha^2\circ I,\alpha^2\circ\alpha^2,\alpha^2\circ\alpha\beta,\alpha^2\circ\alpha^3\beta\}\\ &= \{\alpha^2,I,\alpha^3\beta,\alpha\beta\}\\ &= \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2}))\end{aligned}$$

上述結果正好對應著 (13) 中的等式。至此證得

$$\begin{aligned}&\mathrm{Gal}(\mathbb{Q}(i\sqrt{2}):\mathbb{Q})\\ \cong\ &\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i):\mathbb{Q}(i\sqrt{2}))\end{aligned}$$

由此驗證了「定理 1(vi)」。

連結至數學專題
連結至周家發網頁