感受伽羅瓦：伽羅瓦擴張

我們在上一章介紹了伽羅瓦群和不動域的概念, 如把求伽羅瓦群 $\mathrm{Gal}(E:F)$ 的過程看成把函數 $\mathrm{Gal}(E:\cdot)$ 作用於 E 的子域 F (這裡用 $\cdot$ 代表函數的輸入部分)，並把求不動域 $\mathrm{Fix}_E(G)$ 的過程看成把函數 Fix_E 作用於 E 上某些自同構組成的群 G，那麼在某些情況下，函數 $\mathrm{Gal}(E:\cdot)$ 和 Fix_E 互為逆函數，即對任何 G 和 F，都有

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

可是上述 (1) 和 (2) 所示的關係只有在域擴張 $E:F$ 滿足三個條件時才能同時成立，本章主旨就是介紹這三個條件。

第一個條件是 $E:F$ 必須是「有限擴張」，根據《感受伽羅瓦：代數擴張與超越擴張》中的「定理 6」，所有超越擴張都是無限擴張。由此可知超越擴張不能同時滿足 (1) 和 (2)，以下讓我們看一個例子。考慮 $\mathbb{Q}(\pi):\mathbb{Q}$, 由於 π 是超越數，這是一個超越擴張。由於 $\mathbb{Q}(\pi)$ 的元素全是實數，而我們在《感受伽羅瓦：自同構》中曾指出，實數域上只有一個自同構，即恆等函數 I，我們有

$$\mathrm{Gal}(\mathbb{Q}(\pi):\mathbb{Q}) = \{I\}$$

另一方面，由於 I 的不動點必然包含整個域 (不論是甚麼域)，我們亦有

$$\mathrm{Fix}_{\mathbb{Q}(\pi)}(\{I\}) = \mathbb{Q}(\pi)$$

綜合以上結果，我們有[1]

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\pi):\mathrm{Fix}_{\mathbb{Q}(\pi)}(\{I\})) &= \{I\} \\ \mathrm{Fix}_{\mathbb{Q}(\pi)}(\mathrm{Gal}(\mathbb{Q}(\pi):\mathbb{Q})) &= \mathbb{Q}(\pi) \end{aligned}$$

上述結果顯示，對於 $\mathbb{Q}(\pi):\mathbb{Q}$ 而言，(2) 並不成立。

[1]以下第一個結果的理據如下：對任何域 E 而言，只有恆等函數 I 才能以 E 的所有元素作為不動點，即 $\mathrm{Gal}(E:E)=\{I\}$，故有 $\mathrm{Gal}(\mathbb{Q}(\pi):\mathbb{Q}(\pi))=\{I\}$。

第二個條件是 $E:F$ 必須是正規擴張(normal extension)，我們說 $E:F$ 是正規擴張，當且僅當若 f 是 $F[x]$ 中的不可約多項式，並且 E 包含 f 的一個根，則 E 包含 f 的所有根。舉例說，$\mathbb{C}:\mathbb{R}$ 和 $\mathbb{C}:\mathbb{Q}$ 都是正規擴張，因為複數域包含任何實係數不可約多項式和有理係數不可約多項式的所有根。但 $\mathbb{R}:\mathbb{Q}$ 卻不是正規擴張，這是因為存在有理係數不可約多項式 f，使得 f 有某些根在 $\mathbb{R}$ 上，某些卻不在 $\mathbb{R}$ 上，例如根據「艾森斯坦判別法」(即《感受伽羅瓦：因子分解》中的「定理 8」)，x^3-2 是有理係數不可約多項式，這個多項式有一個根 (即 $\sqrt[3]{2}$) 是實數，其餘兩個 (以下記作 $\omega_3(\sqrt[3]{2})$ 和 ${\omega_3}^2(\sqrt[3]{2})$) 卻不是實數。

以下定理提供一個判別正規擴張的方法。

定理 1：設 $E:F$ 為有限擴張，則 $E:F$ 是正規擴張當且僅當 E 是 F 上某個多項式的分裂域。

上述定理須用到分裂域的概念，我們在《感受伽羅瓦：代數擴張與超越擴張》中引入了這個概念，F 上多項式 f 的分裂域是指包含 F 和 f 所有根的最小的域。請注意由於 $\mathbb{R}$ 包含超越數，$\mathbb{R}:\mathbb{Q}$ 是無限擴張，因此上述定理不適用於這個域擴張。儘管 $\mathbb{R}$ 是 $\mathbb{Q}$ 上某個 (事實上是無限多個) 多項式的分裂域，但 $\mathbb{R}:\mathbb{Q}$ 不是正規擴張。

接下來讓我們以前述的有理係數多項式 x^3-2 為例說明上述定理，我們在《感受伽羅瓦：代數擴張與超越擴張》中曾指出，$\mathbb{Q}(\sqrt[3]{2},\omega_3)$ 是這個多項式的分裂域，由於 $\mathbb{Q}(\sqrt[3]{2},\omega_3):\mathbb{Q}$ 是有限代數擴張，故可應用上述定理。由此根據上述定理，可知 $\mathbb{Q}(\sqrt[3]{2},\omega_3):\mathbb{Q}$ 是正規擴張。

另一方面，$\mathbb{Q}(\sqrt[3]{2})$ 卻不是 x^3-2 的分裂域，而且對其他有理係數多項式 f 而言，如果 f 的根包括一個不是 $\sqrt[3]{2}$ 的無理數，則 $\mathbb{Q}(\sqrt[3]{2})$ 更不可能是 f 的分裂域；如果 f 的根全部都是有理數，則 $\mathbb{Q}(\sqrt[3]{2})$ 也不可能是 f 的分裂域[2]。以上討論顯示，$\mathbb{Q}(\sqrt[3]{2})$ 不是任何有理係數多項式的分裂域，因此根據上述定理，$\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ 不是正規擴張。

根據上述討論，如果 $E:F$ 不是正規擴張，它就不能同時滿足 (1) 和 (2)，現在讓我們看一些例子。首先，如前所述，$\mathbb{R}:\mathbb{Q}$ 不是正規擴張，所以我們預期 $\mathbb{R}:\mathbb{Q}$ 不能同時滿足 (1) 和 (2)[3]，事實正是如此。運用與前面類似

[2]以 x^2-1 為例，$\mathbb{Q}(\sqrt[3]{2})$ 雖然包含著 $\mathbb{Q}$ 和這個多項式的所有根 (即 1 和 -1)，但卻不是包含 $\mathbb{Q}$ 和這個多項式所有根的「最小」的域 (因為 $\mathbb{Q}$ 才是包含 $\mathbb{Q}$ 和 x^2-1 所有根的最小的域)，所以 $\mathbb{Q}(\sqrt[3]{2})$ 不是 x^2-1 的分裂域。

[3]事實上，如前所述，$\mathbb{R}:\mathbb{Q}$ 不是有限擴張，因此單憑這一點，已可推斷 $\mathbb{R}:\mathbb{Q}$ 不能同時滿足 (1) 和 (2)。

的推理，我們有

$$\begin{aligned} \mathrm{Gal}(\mathbb{R}:\mathbb{Q}) &= \{I\} \\ \mathrm{Fix}_{\mathbb{R}}(\{I\}) &= \mathbb{R} \end{aligned}$$

由此我們有

$$\begin{aligned} \mathrm{Gal}(\mathbb{R}:\mathrm{Fix}_{\mathbb{R}}(\{I\})) &= \{I\} \\ \mathrm{Fix}_{\mathbb{R}}(\mathrm{Gal}(\mathbb{R}:\mathbb{Q})) &= \mathbb{R} \end{aligned}$$

上述結果顯示，對於 $\mathbb{R}:\mathbb{Q}$ 而言，(2) 並不成立。

其次，如前所述，$\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ 也不是正規擴張，所以我們預期 $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ 不能同時滿足 (1) 和 (2)，事實也正是如此。根據我們在《感受伽羅瓦：自同構》中的討論，我們知道

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

由此我們有

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

上述結果顯示，對於 $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ 而言，(2) 並不成立。

第三個條件是 $E:F$ 必須是可分擴張(separable extension)，在介紹可分擴張的定義前，須先引入多項式的「導函數」(或簡稱導數) 和「可分不可約多項式」的概念。導函數此一概念本來自數學分析，但為免引入數學分析的背景知識，以下僅從多項式的形式定義導函數，並不涉及「極限」等概念。設 f 為具有以下形式的多項式：

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

則 f 的導函數(derivative)(記作 f') 是指具有以下形式的多項式：

$$f' = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

利用導函數，可以判別某多項式是否具有重根，這是以下定理的內容。

定理 2：設 f 為域 F 上的多項式，則 f 在 F 的擴張域 E 上有重根當且僅當 f 與其導函數 f' 在 F 上有次數大於 0 的共同因式。

以 $\mathbb{Q}$ 上的多項式 $f_1 = x^2 + 2x + 1$ 為例，一方面，這個多項式可以因式分解為 $(x+1)^2$，故有二重根 -1；另一方面，這個多項式的導函數是 $f_1' = 2x + 2$，容易看到 f_1 和 f_1' 有共同因式 $x+1$，而且這個共同因式的次數是 1。另外又如 $\mathbb{Q}$ 上的多項式 $f_2 = x^2 - 1$，一方面，這個多項式沒有重根 (它的兩個根是 1 和 -1)；另一方面，這個多項式的導函數是 $f_2' = 2x$，容易看到 f_2 和 f_2' 沒有次數大於 0 的共同因式 (但它們有次數等於 0 的共同因式,因為任何非零有理數都是它們的共同因式),以上兩例驗證了上述定理。

接著引入可分不可約多項式的定義，設 f 為 F 上的不可約多項式，我們說 f 是可分的當且僅當 f 不存在重根。請注意在上述定義中，「可分性」是僅就不可約多項式而言的[4]。以上面的 f_1 為例，由於 f_1 是可約多項式，它無所謂可分不可分。不過，f_1 的因式 $x+1$ 是不可約多項式，而這個多項式沒有重根，所以是可分的。事實上，我們最常接觸的不可約多項式全都是可分的，這是以下定理的內容。

定理 3：設 F 為特徵為 0 的域或者特徵大於 0 的有限域，則 F 上的所有不可約多項式都是可分的。

上述定理用到域的「特徵」的概念，我們在《感受伽羅瓦：擴張域》中曾經介紹這個概念，這是指使得 $n \times 1 = 0$ 成立 (這裡 $n \times 1$ 代表把 n 個 1 相加的結果) 的最小正整數 n，如無這樣的正整數，則規定域的特徵為 0。根據此一定義，無限域 $\mathbb{Q}$、$\mathbb{R}$ 和 $\mathbb{C}$ 以及這些域的擴張域都是特徵為 0 的域。特徵大於 0 的有限域則包括 $\mathbb{Z}_p$ (其中 p 是正質數) 以及 $\mathbb{Z}_p$ 的有限擴張域 (例如 $\mathbb{Z}_2(s_1)$ (其中 s_1 代表 $x^3 + x^2 + 1$ 的根，我們在《感受伽羅瓦：有限域》中曾討論這個有限擴張域)。由此根據「定理 3」，可知上述這些域上的所有不可約多項式都是可分的。

根據上述討論，如要尋找不可分的不可約多項式，只能從特徵大於 0 的無限擴張域中尋找，其中一個例子是

$$\mathbb{Z}_2(\pi) = \{0, 1, \pi, \frac{1}{\pi}, 1+\pi, \frac{1}{1+\pi}, \frac{\pi}{1+\pi}, \frac{1+\pi}{\pi}, \pi^2, \frac{1}{\pi^2}, \ldots\}$$

這是一個由 π 的有理式組成的域，這個域具有特徵 2，因為在這個域中，$2 \times 1 = 0$。此外，這個域是 $\mathbb{Z}_2$ 的無限擴張域，因為 π 在 $\mathbb{Z}_2$ 上是超越元，而前面已指出所有超越擴張都是無限擴張。

[4]理論上也可以為可約多項式定義可分性，即一個可約多項式是可分的當且僅當它的每個不可約因式都是可分的，但我們不會用到這個定義。

現在我們證明[5]

$$f_3 = x^2 + \pi \qquad (3)$$

是 $\mathbb{Z}_2(\pi)$ 上的不可分不可約多項式。首先證明 (3) 在 $\mathbb{Z}_2(\pi)$ 上不可約，由於 (3) 是二次多項式，如果它可約，只可能分解為 $(x+a)(x+b)$ (其中 $a, b \in \mathbb{Z}_2(\pi)$) 的形式，由此便會得到 a 和 b 是 (3) 的根。因此為證明 (3) 在 $\mathbb{Z}_2(\pi)$ 上不可約，只需證明它在 $\mathbb{Z}_2(\pi)$ 上沒有根。以下我們用反證法來證明這一點，故設 (3) 在 $\mathbb{Z}_2(\pi)$ 上有根，那麼這個根必然是 π 的某個有理式，即具有以下形式：

$$\frac{a_n\pi^n + \cdots + a_0}{b_m\pi^m + \cdots + b_0}$$

其中 $a_n, \ldots, a_0, b_m, \ldots, b_0 \in \mathbb{Z}_2$，由此必有

$$\begin{aligned}
\left(\frac{a_n\pi^n + \cdots + a_0}{b_m\pi^m + \cdots + b_0}\right)^2 + \pi &= 0 \\
\frac{(a_n\pi^n + \cdots + a_0)^2}{(b_m\pi^m + \cdots + b_0)^2} + \pi &= 0 \\
(a_n\pi^n + \cdots + a_0)^2 + \pi(b_m\pi^m + \cdots + b_0)^2 &= 0 \\
{a_n}^2\pi^{2n} + {a_0}^2 + {b_m}^2\pi^{2m+1} + {b_0}^2\pi &= 0
\end{aligned}$$

上面最後一行的理據是，把 $(a_n\pi^n + \cdots + a_0)^2$ 和 $(b_m\pi^m + \cdots + b_0)^2$ 展開後，會分別得到 ${a_n}^2\pi^{2n} + {a_0}^2 + 2 \times$ (其他項) 和 ${b_m}^2\pi^{2m} + {b_0}^2 + 2 \times$ (其他項)，但對 $\mathbb{Z}_2(\pi)$ 中任何元素 a，均有 $2a = 0$，因此這裡的 $2 \times$ (其他項) 必然等於 0。上面最後一行可看成把 π 代入以下多項式中的 x 的結果：

$${a_n}^2x^{2n} + {a_0}^2 + {b_m}^2x^{2m+1} + {b_0}^2x$$

但這麼一來，我們便得到 π 是上述多項式的根，但由於 π 是 $\mathbb{Z}_2$ 上的超越元，它不可能是這個多項式的根，至此證明了 (3) 在 $\mathbb{Z}_2(\pi)$ 上沒有根，也就是 (3) 在 $\mathbb{Z}_2(\pi)$ 上不可約。

其次證明 (3) 在 $\mathbb{Z}_2(\pi)$ 上是不可分的，即它在 $\mathbb{Z}_2(\pi)$ 的某個擴張域上有重根。為證明這一點，可以先計算 f_3 的導函數如下：

$$\begin{aligned}
{f_3}' &= 2x \\
&= 0
\end{aligned}$$

由此可得 f_3 與 f_3' 有共同因式 $x^2 + \pi^6$，而且這個共同因式的次數大於 0，由此根據上面的「定理 2」，可知 (3) 有重根。

---

[5]請注意在 $\mathbb{Z}_2(\pi)$ 中, $-1 = 1$, 而且基於乘法對加法的分配性, 有 $\pi+\pi = \pi\times1+\pi\times1 = \pi\times(1+1) = \pi\times0 = 0$，故有 $-\pi = \pi$，因此在 $\mathbb{Z}_2(\pi)$ 中所有負號都變成正號。

[6]由於 0 可被任何非零多項式整除，所以任何非零多項式都是 0 的因式。

事實上，如果把 (3) 的一個根寫成 $\sqrt{\pi}$ 的形式，那麼 (3) 可以因式分解如下：

$$f_3 = (x + \sqrt{\pi})^2$$

由此可知 (3) 確有一個二重根 $\sqrt{\pi}$，這個根不在 $\mathbb{Z}_2(\pi)$ 上 (前面我們已證明了 (3) 在 $\mathbb{Z}_2(\pi)$ 上沒有根)，而是在 $\mathbb{Z}_2(\pi)$ 的擴張域 $\mathbb{Z}_2(\pi)(\sqrt{\pi})$ 上。請注意這是一個頗特殊的擴張域，其特殊之處在於它包含著兩類型域擴張[7]，其中從 $\mathbb{Z}_2$ 擴張到 $\mathbb{Z}_2(\pi)$ 是超越擴張，因為 π 是 $\mathbb{Z}_2$ 上的超越元，它不滿足 $\mathbb{Z}_2$ 上的任何多項式；而從 $\mathbb{Z}_2(\pi)$ 擴張到 $\mathbb{Z}_2(\pi)(\sqrt{\pi})$ 卻是代數擴張，因為 $\sqrt{\pi}$ 滿足 $\mathbb{Z}_2(\pi)$ 上的多項式 (3)。我們以下還會對 $\mathbb{Z}_2(\pi)(\sqrt{\pi})$ 作更多討論。

至此我們詳細討論了導函數和可分不可約多項式的概念，現在終於可以引入可分擴張的定義，我們說域擴張 $E : F$ 是可分擴張，當且僅當對 F 上的每個代數元 a 而言，a 的最小多項式都是可分的。由於我們在前面已指出，$\mathbb{Q}$、$\mathbb{R}$ 和 $\mathbb{C}$ 的擴張域，以及 $\mathbb{Z}_p$ 的有限擴張域上的所有不可約多項式都是可分的，而最小多項式按定義必然是不可約多項式，所以上述這些域擴張全都是可分擴張。

基於以上討論，如要尋找不可分擴張，只能從 $\mathbb{Z}_p$ 的無限擴張域中尋找，而前面討論的 $\mathbb{Z}_2(\pi)(\sqrt{\pi})$ 正符合我們的要求。以下證明 $\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi)$ 是不可分擴張，為此要找出 $\mathbb{Z}_2(\pi)$ 上的一個代數元，使得這個代數元的最小多項式不可分。$\sqrt{\pi}$ 就是所需的代數元，為證明這一點，首先證明 $\sqrt{\pi}$ 是 $\mathbb{Z}_2(\pi)$ 上的代數元。$\sqrt{\pi}$ 雖然不是代數數，但它卻是 $\mathbb{Z}_2(\pi)$ 上的代數元，因為它滿足 $\mathbb{Z}_2(\pi)$ 上的多項式 (3)。這也就是我們分兩步把 $\mathbb{Z}_2$ 擴張為 $\mathbb{Z}_2(\pi)(\sqrt{\pi})$ 的原因，如果直接把 $\mathbb{Z}_2$ 擴張為 $\mathbb{Z}_2(\sqrt{\pi})$ (請注意這個擴張域也包含 π 這個元素)，$\sqrt{\pi}$ 就不會是 $\mathbb{Z}_2$ 上的代數元。

其次證明 $\sqrt{\pi}$ 的最小多項式是不可分的。我們看到 $\sqrt{\pi}$ 是 $\mathbb{Z}_2(\pi)$ 上的不可約二次多項式 (3) 的根，而且 $\sqrt{\pi}$ 不可能是 $\mathbb{Z}_2(\pi)$ 上任何一次多項式的根 (請注意雖然 $\sqrt{\pi}$ 是一次多項式 $x + \sqrt{\pi}$ 的根，但 $x + \sqrt{\pi}$ 不是 $\mathbb{Z}_2(\pi)$ 上的多項式，因為它的常數項 $\sqrt{\pi}$ 不是 $\mathbb{Z}_2(\pi)$ 中的元素)，因此 (3) 就是 $\sqrt{\pi}$ 的最小多項式，而前面已證明了這個多項式是不可分的。

根據上述討論，我們預期不可分擴張 $\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi)$ 不能同時滿足上面的 (1) 和 (2)，為證明這一點，我們首先求 $\mathrm{Gal}(\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi))$，設 θ 是這個群的成員，由於 $\mathbb{Z}_2(\pi)(\sqrt{\pi}) = \{a + b\sqrt{\pi} : a, b \in \mathbb{Z}_2(\pi)\}$，根據自同構的性質，我們有

$$\theta(a + b\sqrt{\pi}) \;\; = \;\; \theta(a) + \theta(b) \times \theta(\sqrt{\pi})$$

[7]為突出這個域擴張乃由兩類擴張構成這一點，以下把這個擴張域寫成 $\mathbb{Z}_2(\pi)(\sqrt{\pi})$，而不寫成 $\mathbb{Z}_2(\pi, \sqrt{\pi})$。

$$= \quad a + b \times \theta(\sqrt{\pi})$$

由此可知，為確定 θ，只需確定 $\theta(\sqrt{\pi})$ 的值。另一方面，我們又有

$$\pi = \theta(\pi) = \theta((\sqrt{\pi})^2) = (\theta(\sqrt{\pi}))^2$$

從上式可得二次方程 $(\theta(\sqrt{\pi}))^2 = \pi$，由此解得 $\theta(\sqrt{\pi}) = \sqrt{\pi}$ (請注意在 $\mathbb{Z}_2(\pi)(\sqrt{\pi})$ 中，$-\sqrt{\pi} = \sqrt{\pi}$，其理據跟註 5 中 $-\pi = \pi$ 的理據相同)，因此 θ 是恆等函數 I，至此求得

$$\mathrm{Gal}(\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi)) = \{I\}$$

另一方面，我們亦有

$$\mathrm{Fix}_{\mathbb{Z}_2(\pi)(\sqrt{\pi})}(\{I\}) = \mathbb{Z}_2(\pi)(\sqrt{\pi})$$

綜合以上結果，我們有

$$\begin{aligned} \mathrm{Gal}(\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathrm{Fix}_{\mathbb{Z}_2(\pi)(\sqrt{\pi})}(\{I\})) &= \{I\} \\ \mathrm{Fix}_{\mathbb{Z}_2(\pi)(\sqrt{\pi})}(\mathrm{Gal}(\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi))) &= \mathbb{Z}_2(\pi)(\sqrt{\pi}) \end{aligned}$$

上述結果顯示，對於 $\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi)$ 而言，(2) 並不成立。

請注意由於 $\sqrt{\pi}$ 在 $\mathbb{Z}_2(\pi)$ 上的最小多項式是 (3)，而 (3) 是二次多項式，因此根據《感受伽羅瓦：代數擴張與超越擴張》中的「定理 6」，$|\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi)| = 2$，即 $\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi)$ 是有限擴張。此外，由於 (3) 是 $\mathbb{Z}_2(\pi)$ 上的多項式，而 (3) 的所有根 (即 $\sqrt{\pi}$) 都在 $\mathbb{Z}_2(\pi)(\sqrt{\pi})$ 內，即 $\mathbb{Z}_2(\pi)(\sqrt{\pi})$ 是 (3) 的分裂域，由此根據上述「定理 1」，可知 $\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi)$ 也是正規擴張。至此我們看到，雖然 $\mathbb{Z}_2(\pi)(\sqrt{\pi}) : \mathbb{Z}_2(\pi)$ 既是有限擴張，又是正規擴張，但由於它是不可分擴張，它不能同時滿足 (1) 和 (2)。由此可見，上面討論的有限性、正規性和可分性各自是使 (1) 和 (2) 同時成立的必要條件，三者缺一不可。此外，可以證明上述三個條件也是 (1) 和 (2) 同時成立的充分條件，即如果某域擴張同時具備上述三個條件，它必然同時滿足 (1) 和 (2)。

抽象代數學上把同時具備有限性、正規性和可分性的域擴張稱為伽羅瓦擴張(Galois extension)。根據上述討論，我們可以作出以下總結：一個域擴張是伽羅瓦擴張，當且僅當它使 (1) 和 (2) 同時成立。換句話說，一個域擴張是伽羅瓦擴張，當且僅當它使 $\mathrm{Gal}(E : \cdot)$ 和 Fix_E 互為逆函數。因此之故，伽羅瓦擴張在伽羅瓦理論中起著非常重要的作用，讀者將在後面各章中看到這一點。

連結至數學專題
連結至周家發網頁