感受伽羅瓦：質理想與極大理想

我們在《感受伽羅瓦：子環與商環》中介紹了理想的概念，並在該網頁的「定理 1」中指出，如果 R 是交換環並且 I 是其理想，則 R/I 構成一個環 (稱為商環)。我們在《感受伽羅瓦：環及其子類》中也曾指出，環是包含「加」和「乘」這兩種二元運算的基本代數結構，此外，環還有多種子類。有趣的是，當我們選擇 I 的適當子類時，所得的 R/I 便會是商環的某種特殊子類，本章的主旨是介紹理想的兩個特殊子類－「質理想」和「極大理想」以及對應的商環子類，現先把這些對應關係總結成下表 (請注意以下討論的環都是交換環)：

I 的類別	R/I 的類別
理想	環
質理想	整環
極大理想	域

回顧理想的定義，簡言之，I 是 R 的理想當且僅當 I 是 R 的子環，並且 I 是一個「乘法黑洞」。由於 R 是自身的子環，並且 R 必然是一個「乘法黑洞」(因為 R 的任何元素乘以 R 的任何元素必然也是 R 的元素)，所以 R 是自身的理想。如果撇除 R 不計，我們把 R 以外的 R 的理想稱為 R 的真理想(proper ideal)，例如 $6\mathbb{Z}$ 就是 $\mathbb{Z}$ 的一個真理想。

現在介紹質理想(prime ideal) 的概念。設 R 是交換環，I 是其真理想，則 I 是 R 的質理想當且僅當若 $a, b \in R$ 並且 $ab \in I$，則 $a \in I$ 或者 $b \in I$。請注意上述定義跟我們在《感受伽羅瓦：因子分解》中介紹的「質數」的定義很相似：整數 p 是質數當且僅當若 $a, b \in \mathbb{Z}$ 並且 $p \mid ab$，則 $p \mid a$ 或者 $p \mid b$。質理想和質數定義的共同點是：若乘積 ab 具有某性質，則 a 具有該性質或者 b 具有該性質。

舉例說，在 $Z[x]$ 中，主理想 $\langle x \rangle$ 便是一個質理想。回顧上一章，$\langle x \rangle$ 包含所有常數項等於 0 的整係數多項式，例如 0、x、$2x$、x^2 等。從另一角度看，也可把 $\langle x \rangle$ 的成員看成滿足 $f(0) = 0$ 的整係數多項式 f。現在讓我們證明 $\langle x \rangle$ 是質理想，設 $g, h \in \mathbb{Z}[x]$ 並且 $gh \in \langle x \rangle$，那麼 $g(0)h(0) = 0$。由於 $g(0)$ 和 $h(0)$ 是整數，故有 $g(0) = 0$ 或者 $h(0) = 0$，即 $g \in \langle x \rangle$ 或者 $h \in \langle x \rangle$。

以下定理確立質理想與整環的對應關係。

定理 1：設 R 為帶乘法單位元的交換環，I 為其理想，則 R/I 構成一個整環當且僅當 I 是 R 的質理想。

根據前面的討論，$\langle x\rangle$ 是 $Z[x]$ 的質理想，由此根據上述定理，可知 $\mathbb{Z}[x]/\langle x\rangle$ 是一個整環。現在讓我們看看 $\mathbb{Z}[x]/\langle x\rangle$ 究竟包含甚麼元素。為此，我們拿 $\mathbb{Z}[x]/\langle x\rangle$ 跟上一章討論過的 $\mathbb{Z}/6\mathbb{Z}$ 作一對比 (請注意 $6\mathbb{Z}$ 也可寫作 $\langle 6\rangle$)。

我們知道 $\mathbb{Z}/6\mathbb{Z}$ 由陪集組成，這些陪集分別代表把任意整數除以 6 所得的餘數，由於把整數除以 6 共有六種可能餘數，因此

$$\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}\,(=0+6\mathbb{Z}), 1+6\mathbb{Z}, 2+6\mathbb{Z}, 3+6\mathbb{Z}, 4+6\mathbb{Z}, 5+6\mathbb{Z}\}$$

以上集合包含六個陪集，分別代表上述可能餘數 0、1、2、3、4 和 5，而每個陪集所包含的整數都在除以 6 後有相同的餘數，例如

$$1+6\mathbb{Z} = \{\cdots, -11, -5, 1, 7, 13, \cdots\}$$

上述陪集所包含的整數都在除以 6 後得餘數 1。

同理，$\mathbb{Z}[x]/\langle x\rangle$ 也由陪集組成，這些陪集分別代表把任意整係數多項式除以 x 所得的餘式。由於整係數多項式可以被分成兩部分：包含 x 的部分和常數項部分，而包含 x 的部分總能被 x 整除，因此把任意整係數多項式除以 x，所得餘式必然是該多項式的常數項部分，即一個整數。以 $37x^{20}+13x^7-111$ 為例,由於 $37x^{20}+13x^7$ 能被 x 整除,$(37x^{20}+13x^7-111)\div x$ 的餘式是整數 -111。反過來看，任何整數都可作為某個整係數多項式的常數項。綜合以上討論，把任意整係數多項式除以 x 所得的餘式包括而且僅包括所有整數，即

$$\mathbb{Z}[x]/\langle x\rangle = \{\langle x\rangle\,(=0+\langle x\rangle), 1+\langle x\rangle, -1+\langle x\rangle, 2+\langle x\rangle, -2+\langle x\rangle, \cdots\}$$

以上集合包含無窮多個陪集，分別代表上述可能餘式 0、1、-1、2、-2 等等，而每個陪集所包含的整係數多項式都在除以 x 後有相同的餘式，例如

$$1+\langle x\rangle = \{1, x+1, -x+1, 2x+1, -2x+1, x^2+1, -x^2+1, \cdots\}$$

上述陪集所包含的整係數多項式都在除以 x 後得餘式 1。從以上討論可見，$\mathbb{Z}[x]/\langle x\rangle$ 的成員對應著全體整數，事實上，在下一章，我們將證明 $\mathbb{Z}[x]/\langle x\rangle$ 實質上等同於 $\mathbb{Z}$。由於我們在《感受伽羅瓦：環及其子類》中指出了 $\mathbb{Z}$ 是整環，由此可知 $\mathbb{Z}[x]/\langle x\rangle$ 確是一個整環。

接下來介紹極大理想(maximal ideal) 的概念。首先必須指出，由於理想

是一種集合，一個交換環 R 的某個理想可以包含於另一個理想中 (即作為另一個理想的子集)，而極大理想就是指除了 R 外並不包含於其他理想的真理想。形式化地說，設 R 是交換環，I 是其真理想，則 I 是 R 的極大理想當且僅當對任何 J 而言，若 J 也是 R 的理想，並且 $I \subseteq J \subseteq R$，則必有 $J = I$ 或者 $J = R$。

舉例說，$6\mathbb{Z}$ 便不是 $\mathbb{Z}$ 的極大理想，這是因為 $6\mathbb{Z}$ 被包含於 $\mathbb{Z}$ 的另一個理想中，這個理想是 $3\mathbb{Z}$，即由 3 的倍數組成的集合。容易證明 $3\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想，並且 $6\mathbb{Z} \subseteq 3\mathbb{Z}$ (因為 6 的任何倍數也是 3 的倍數)。此外，也容易證明 $3\mathbb{Z}$ 是 $\mathbb{Z}$ 的極大理想。以下定理確立極大理想與域的對應關係。

定理 2：設 R 為帶乘法單位元的交換環，I 為其理想，則 R/I 構成一個域當且僅當 I 是 R 的極大理想[1]。

根據前面的討論，$6\mathbb{Z}$ 並非極大理想，由此根據上述定理，可知 $\mathbb{Z}/6\mathbb{Z}$ 並不構成域 (但構成環)。換句話說，$6\mathbb{Z}$ 中並非所有非零元素都有乘法逆元。容易驗證，$2+6\mathbb{Z}$、$3+6\mathbb{Z}$ 和 $4+6\mathbb{Z}$ 都沒有乘法逆元，例如由於

$$\begin{aligned}
(2+6\mathbb{Z})(6\mathbb{Z}) &= 6\mathbb{Z} \\
(2+6\mathbb{Z})(1+6\mathbb{Z}) &= 2+6\mathbb{Z} \\
(2+6\mathbb{Z})(2+6\mathbb{Z}) &= 4+6\mathbb{Z} \\
(2+6\mathbb{Z})(3+6\mathbb{Z}) &= 6\mathbb{Z} \\
(2+6\mathbb{Z})(4+6\mathbb{Z}) &= 2+6\mathbb{Z} \\
(2+6\mathbb{Z})(5+6\mathbb{Z}) &= 4+6\mathbb{Z}
\end{aligned}$$

可知 $2+6\mathbb{Z}$ 與 $\mathbb{Z}/6\mathbb{Z}$ 中任何元素相乘的結果, 都不會等於乘法單位元 $1+6\mathbb{Z}$, 因此 $2+6\mathbb{Z}$ 沒有乘法逆元。

另一方面，前面說過 $3\mathbb{Z}$ 是 $\mathbb{Z}$ 的極大理想，由此根據上述定理，可知 $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$ 構成一個域，這個域中的所有非零元素 (即 $3\mathbb{Z}$ 以外的元素) 都有乘法逆元，其中 $1+3\mathbb{Z}$ 作為乘法單位元，是自身的乘法逆元；另外由於 $(2+3\mathbb{Z})(2+3\mathbb{Z}) = 1+3\mathbb{Z}$, 可知 $2+3\mathbb{Z}$ 也是自身的乘法逆元。

接下來讓我們看看多項式的例子，設 F 為域，根據《感受伽羅瓦：環及其子類》中的「定理 2」，$F[x]$ 是環 (更準確地說，是整環)。現考慮多項式 $f \in F[x]$，我們知道由 f 生成的主理想 (記作 $\langle f \rangle$) 是一個理想，因此根據「定理 2」，$F[x]/\langle f \rangle$ 構成一個域當且僅當 $\langle f \rangle$ 是 $F[x]$ 的極大理想，那

[1]我們在《感受伽羅瓦：等價關係與分數域》中介紹了一種從整環構造域的方法，這種方法使用「分數域」的概念；本定理則提供一種從帶乘法單位元的交換環構造域的方法, 這種方法使用「極大理想」的概念。

麼在甚麼情況下 $\langle f\rangle$ 是極大理想？這個問題有一個簡單解答,請看以下定理。

定理 3：設 F 為域，並且多項式 $f \in F[x]$，則主理想 $\langle f\rangle$ 是 $F[x]$ 的極大理想當且僅當 f 在 $F[x]$ 上不可約。

舉例說，由於 $\mathbb{R}$ 是域，並且 x^2+1 是 $\mathbb{R}[x]$ 上的不可約多項式，從上述定理可知主理想 $\langle x^2+1\rangle$ 是 $\mathbb{R}[x]$ 的極大理想，再由此根據「定理 2」，可知 $\mathbb{R}[x]/\langle x^2+1\rangle$ 是一個域。現在讓我們看看 $\mathbb{R}[x]/\langle x^2+1\rangle$ 究竟包含甚麼元素。

跟前面的相類例子一樣，$\mathbb{R}[x]/\langle x^2+1\rangle$ 由陪集組成，這些陪集分別代表把任意實係數多項式除以 x^2+1 所得的餘式。根據《感受伽羅瓦：整數與多項式》中的「多項式的除法算法」(即該網頁的「定理 2」)[2]，把任意實係數多項式除以二次多項式 x^2+1，所得的餘式要麼是 0，要麼是次數小於 2 的實係數多項式，即實係數一次多項式或實常數多項式。反過來看，任何實係數一次多項式或實常數多項式都可作為某個實係數多項式除以 x^2+1 的餘式，例如 $-\frac{2}{3}x+\sqrt{5}$ 便可作為 $x^3+\frac{1}{3}x+\sqrt{5}$ 除以 x^2+1 的餘式 (因為 $x^3+\frac{1}{3}x+\sqrt{5}=(x^2+1)(x)+(-\frac{2}{3}x+\sqrt{5})$)。綜合以上討論，把任意實係數多項式除以 x^2+1 所得的餘式包括而且僅包括所有實係數一次多項式和實常數多項式，即

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

以上集合包含無窮多個陪集，分別代表上述可能餘式，而每個陪集所包含的實係數多項式都在除以 x^2+1 後有相同的餘式，例如

$$-\frac{2}{3}x+\sqrt{5}+\langle x^2+1\rangle = \{-\frac{2}{3}x+\sqrt{5}, x^2-\frac{2}{3}x+1+\sqrt{5}, x^3+\frac{1}{3}x+\sqrt{5},\cdots\} \qquad (2)$$

上述陪集所包含的實係數多項式都在除以 x^2+1 後得餘式 $-\frac{2}{3}x+\sqrt{5}$。

由於 $\mathbb{R}[x]/\langle x^2+1\rangle$ 是域，它的每個非零成員都應有乘法逆元，以下用一個實例說明如何就某特定非零成員求其乘法逆元。設要求 $x+1+\langle x^2+1\rangle$ 的乘法逆元，我們假設這個乘法逆元具有 $ax+b+\langle x^2+1\rangle$ 的形式，其中 $a,b\in\mathbb{R}$。根據乘法逆元和商環中乘法的定義，我們有

$$\begin{aligned}(x+1+\langle x^2+1\rangle)\times(ax+b+\langle x^2+1\rangle) &= 1+\langle x^2+1\rangle\\ ax^2+(a+b)x+b+\langle x^2+1\rangle &= 1+\langle x^2+1\rangle\end{aligned}$$

上式的意思是 $ax^2+(a+b)x+b$ 除以 x^2+1 的餘式應等於 1，即

$$ax^2+(a+b)x+b = f\times(x^2+1)+1$$

[2]該定理雖然是就 $\mathbb{Q}[x]$ 提出的，但其實適用於所有 $F[x]$，其中 F 是域。特別地，該定理適用於 $\mathbb{R}[x]$。

其中 f 代表某實係數多項式，接著我們要解出 f、a 和 b。首先必須觀察到，f 不可能包含帶 x 的項，例如如果 $f = cx + d$，那麼上式右端便變成 $cx^3 + dx^2 + cx + d + 1$，接著比較等號兩端，勢必得到 $c = 0$。因此在上式中，f 只可能是一個實常數項。把上式右端展開，得到

$$ax^2 + (a + b)x + b = fx^2 + f + 1$$

比較上式兩端，可得到以下聯立方程：

$$\begin{cases} a &= f \\ a + b &= 0 \\ b &= f + 1 \end{cases}$$

解此方程，可得到 $a = -\frac{1}{2}, b = \frac{1}{2}$，由此可知 $x + 1 + \langle x^2 + 1\rangle$ 的乘法逆元是 $-\frac{1}{2}x + \frac{1}{2} + \langle x^2 + 1\rangle$。上述方法可以推廣為求乘法逆元的一般方法，但由於這涉及線性代數的某些知識，這裡不作討論，我們會在下一章介紹求乘法逆元的另一種方法。

(1) 中集合的成員還滿足以下特殊乘法結果：

$$\begin{aligned} (x + \langle x^2 + 1\rangle) \times (x + \langle x^2 + 1\rangle) &= x^2 + \langle x^2 + 1\rangle \\ &= -1 + \langle x^2 + 1\rangle \qquad (3) \end{aligned}$$

上式最後一行的理據是：x^2 除以 $x^2 + 1$ 的餘式是 -1。

總結以上的討論，根據 (1)，$\mathbb{R}[x]/\langle x^2 + 1\rangle$ 相當於一個由二維實數組成的集合 (因為在 (1) 中，只有 a 和 b 是可變化的部分)，這些二維實數可進行加、減、乘、除運算，並且滿足 (3) 所示的特殊乘法結果。現在如果把 (1) 中等號右端集合中的 $\langle x^2 + 1\rangle$ 刪去，並把 x 改為虛數單位 i，那麼該集合便變成以下複數集合：

$$\{ai + b : a, b \in \mathbb{R}\}$$

而我們知道複數相當於二維實數，可進行加、減、乘、除運算，並且滿足下列特殊乘法結果：

$$i \times i = -1$$

請注意由於 $x + \langle x^2 + 1\rangle$ 和 $-1 + \langle x^2 + 1\rangle$ 分別與 i 和 -1 對應，上述乘法結果與 (3) 存在對應關係。至此我們看到，$\mathbb{R}[x]/\langle x^2 + 1\rangle$ 的成員對應著全體複數，事實上，在下一章，我們將證明 $\mathbb{R}[x]/\langle x^2 + 1\rangle$ 實質上等同於 $\mathbb{C}$。由於我們在《感受伽羅瓦：環及其子類》中指出了 $\mathbb{C}$ 是域，由此可知 $\mathbb{R}[x]/\langle x^2 + 1\rangle$ 確是一個域。

接下來讓我們看「定理 2」和「定理 3」的一個反例。在 $\mathbb{R}[x]$ 中，x^2-1 是可約多項式，由此根據「定理 3」，$\langle x^2-1\rangle$ 不是 $\mathbb{R}[x]$ 的極大理想，再由此根據「定理 2」，可知 $\mathbb{R}[x]/\langle x^2-1\rangle$ 並不構成域 (但構成環)。可是，跟前面討論過的 $\mathbb{R}[x]/\langle x^2+1\rangle$ 相似，$\mathbb{R}[x]/\langle x^2-1\rangle$ 也是由陪集組成，而且運用前面的推理，不難推出跟上面 (1) 相似的結果：

$$\mathbb{R}[x]/\langle x^2-1\rangle = \{ax+b+\langle x^2-1\rangle : a,b\in\mathbb{R}\} \qquad (4)$$

(1) 和 (4) 所列的集合雖然很相似，而且兩者所含的陪集對應著同一批餘式，但兩者的陪集有不同的內容。以餘式 $-\frac{2}{3}x+\sqrt{5}$ 為例，這個餘式在 $\mathbb{R}[x]/\langle x^2+1\rangle$ 下所對應的陪集已列於上面的 (2)，這同一個餘式在 $\mathbb{R}[x]/\langle x^2-1\rangle$ 下則對應著以下陪集：

$$-\frac{2}{3}x+\sqrt{5}+\langle x^2-1\rangle = \{-\frac{2}{3}x+\sqrt{5}, x^2-\frac{2}{3}x-1+\sqrt{5}, x^3-\frac{5}{3}x+\sqrt{5},\cdots\} \qquad (5)$$

上述陪集所包含的實係數多項式都在除以 x^2-1 後得餘式 $-\frac{2}{3}x+\sqrt{5}$。細心比較 (2) 和 (5)，可以發現兩者所含的元素是不同的。

儘管 (1) 和 (4) 所列的集合在形式上只有少許差異，但差之毫釐，謬之千里，這兩個集合有很不同的代數結構。如前所述，(1) 中的集合構成域，它的每個成員都有乘法逆元；(4) 中的集合卻不構成域，並非每個成員都有乘法逆元。事實上，可以證明每個形如 $ax+a+\langle x^2-1\rangle$ 和 $ax-a+\langle x^2-1\rangle$ (其中 $a\in\mathbb{R}$) 的陪集都沒有乘法逆元。

以下讓我們用反證法證明 $x-1+\langle x^2-1\rangle$ 沒有乘法逆元，為此，假設它有一個形式為 $ax+b+\langle x^2-1\rangle$ (其中 $a,b\in\mathbb{R}$) 的乘法逆元。根據乘法逆元和商環中乘法的定義，我們有

$$\begin{aligned}(x-1+\langle x^2-1\rangle)\times(ax+b+\langle x^2-1\rangle) &= 1+\langle x^2-1\rangle\\ ax^2+(-a+b)x-b+\langle x^2-1\rangle &= 1+\langle x^2-1\rangle\end{aligned}$$

上式的意思是 $ax^2+(-a+b)x-b$ 除以 x^2-1 的餘式應等於 1，即

$$ax^2+(-a+b)x-b = f\times(x^2-1)+1$$

其中 f 代表某實係數多項式，接著我們要解出 f、a 和 b。如同前面討論過的例子，在上式中，f 只可能是一個實常數項。把上式右端展開，得到

$$ax^2+(-a+b)x-b = fx^2-f+1$$

比較上式兩端，可得到以下聯立方程：

$$\begin{cases} a &= f\\ -a+b &= 0\\ -b &= -f+1\end{cases}$$

把上列第一式代入第三式，可把以上聯立方程化簡為

$$\begin{cases} -a+b &= 0 \\ -a+b &= -1 \end{cases}$$

但以上兩式互相矛盾，不可能解出 a 和 b，由此證得 $x-1+\langle x^2-1\rangle$ 沒有乘法逆元。

至此我們討論了質理想和極大理想，這兩類理想之間有何關係？這個問題的解答可從以下定理得到。

定理 4：所有極大理想都是質理想，但有質理想不是極大理想。

請注意我們在《感受伽羅瓦：環及其子類》中的「定理 3」中曾指出，所有域都是整環，但有整環不是域，而在上面我們又指出了質理想與整環以及極大理想與域之間的密切關係，由此可見上述網頁的「定理 3」與本網頁的「定理 4」陳述了一致和相關的事實。根據「定理 4」，本章討論過的多個極大理想，包括 $3\mathbb{Z}$ 和 $\langle x^2+1\rangle$，也是質理想，因此質理想並不僅僅包括本章所曾討論的 $\langle x\rangle$ 這個例子。

接下來讓我們看看「定理 4」的一些例證，首先看「所有極大理想都是質理想」的例證。如前所述，$3\mathbb{Z}$ 是 $\mathbb{Z}$ 的極大理想，由此可知 $3\mathbb{Z}$ 也應是 $\mathbb{Z}$ 的質理想，即若有整數 a 和 b 使得 $ab\in 3\mathbb{Z}$，則必有 $a\in 3\mathbb{Z}$ 或 $b\in 3\mathbb{Z}$。根據 $3\mathbb{Z}$ 的定義，這等於說若 $3\mid ab$，則必有 $3\mid a$ 或 $3\mid b$，但這等於說 3 是質數[3]。由於 3 確是質數，這證明了 $3\mathbb{Z}$ 確是質理想。

最後看「有質理想不是極大理想」的例證。前面說過，$\langle x\rangle$ 是 $\mathbb{Z}[x]$ 的質理想，請注意這個質理想不是 $\mathbb{Z}[x]$ 的極大理想，這是因為 $\langle x\rangle$ 是 $\langle 2,x\rangle$ 的真子集。如前所述，$\langle x\rangle$ 包含所有常數項等於 0 的整係數多項式，而我們在《感受伽羅瓦：子環與商環》中又曾指出，$\langle 2,x\rangle$ 包含所有常數項為偶數的整係數多項式。由於對任何整係數多項式的常數項而言，若該常數項等於 0,則必然是偶數,但有偶數不等於 0,由此可見 $\langle x\rangle$ 確是 $\langle 2,x\rangle$ 的真子集。

連結至數學專題
連結至周家發網頁

[3]我們在《感受伽羅瓦：因子分解》中曾指出質數可定義如下：設 p 為非單位非零整數，則 p 是質數當且僅當若 $p\mid ab$，則 $p\mid a$ 或 $p\mid b$。