感受伽羅瓦：子環與商環

本章主旨是介紹環的內部結構，我們首先從最基本的概念－子環(subring)說起。簡言之，環是一種代數結構，這種代數結構由一個集合 R 連同定義於其上，分別稱為「加」$(+)$ 和「乘」$(\times)$ 的兩種運算組成，而這兩種運算須滿足《感受伽羅瓦：環及其子類》所介紹的一些公理。在抽象代數學上，環一般記作三元組 $(R, +, \times)$，但如「加」和「乘」確定無疑，也可僅記作 R。給定一個環 $(R, +, \times)$，其子環就是代數結構 $(S, +, \times)$，其中 $S \subseteq R$，$+$ 和 $\times$ 則是繼承自 $(R, +, \times)$ 中的同類運算，而 $(S, +, \times)$ 本身必須滿足環的定義。

為證明 $(S, +, \times)$ 是 $(R, +, \times)$ 的子環，必須證明：(i)$+$ 和 $\times$ 運算在 S 上封閉，即任選 S 上元素 a 和 b，$a+b$ 和 $a \times b$ 都是 S 的元素；(ii)$+$ 運算具有結合性和交換性，$\times$ 運算具有結合性，$\times$ 對 $+$ 具有分配性；(iii)S 包含 R 中的加法單位元 (一般記作 0)，並且 S 中每個元素的加法逆元都在 S 中。由於 $(S, +, \times)$ 中的 $+$ 和 $\times$ 是繼承自 $(R, +, \times)$ 中的同類運算，必然繼承了上述 (ii) 所列的性質，因此在進行上述證明時，實際只須證明 (i) 和 (iii)。

容易看到，給定環 R，R 本身和 $\{0\}$ 都是 R 的子環。除了這些「平凡」(trivial) 子環的例子外，也不難找出非平凡子環的例子。舉例說，$6\mathbb{Z}$ (即 6 的倍數組成的集合) 便構成 $\mathbb{Z}$ 的子環，這是因為首先，6 的任意兩個倍數相加和相乘，所得結果都是 6 的倍數，即 $+$ 和 $\times$ 運算在 $6\mathbb{Z}$ 上封閉；其次，0 是 6 的倍數，即 $6\mathbb{Z}$ 包含 $\mathbb{Z}$ 中的加法單位元 0，並且 6 的任意倍數 a 的加法逆元 $-a$ 都是 6 的倍數，即 $6\mathbb{Z}$ 中每個元素的加法逆元都在 $6\mathbb{Z}$ 中。

反之，$1+6\mathbb{Z}$ (即 1 加上 6 的倍數所得整數組成的集合) 卻不構成 $\mathbb{Z}$ 的子環，這是因為 $1+6\mathbb{Z}$ 的任意兩個成員相加 (例如 $1+7$)，所得結果不是 $1+6\mathbb{Z}$ 的成員，即 $+$ 運算在 $1+6\mathbb{Z}$ 上不封閉 (儘管 $\times$ 運算封閉)；而且 0 不是 $1+6\mathbb{Z}$ 的成員，即 $1+6\mathbb{Z}$ 不包含 $\mathbb{Z}$ 中的加法單位元 0。一般地，設 n 為大於 1 的正整數，m 為正整數且 $0 < m < n$，則 $n\mathbb{Z}$ (即 n 的倍數組成的集合) 構成 $\mathbb{Z}$ 的子環，而 $m+n\mathbb{Z}$ (即 m 加上 n 的倍數所得整數組成的集合) 卻不構成 $\mathbb{Z}$ 的子環。

我們在《感受伽羅瓦：等價關係與分數域》中曾介紹模 n 同餘的概念：設 a 和 b 為整數，n 為正整數，則 a 與 b 關於模 n 同餘 (記作 $a \equiv_n b$)，當

且僅當 a 和 b 除以 n 所得的餘數相等。此外，我們還指出模 n 同餘關係是等價關係，根據此一等價關係可以確定等價類，設 $a \in \mathbb{Z}$，我們有

$$[a] = \{b \in \mathbb{Z} : a \equiv_n b\} \qquad (1)$$

上述集合包含所有在除以 n 後與 a 有相同餘數的整數。為推廣上述概念，我們首先把模 n 同餘的定義改寫成以下等價形式：

$$a \equiv_n b \text{ iff } b - a \in n\mathbb{Z}$$

接著利用上式把 (1) 中的集合改寫如下：

$$\begin{aligned}
[a] &= \{b \in \mathbb{Z} : a \equiv_n b\} \\
&= \{b \in \mathbb{Z} : b - a \in n\mathbb{Z}\} \\
&= \{b \in \mathbb{Z} : \text{存在 } c \in n\mathbb{Z} \text{ 使得} b - a = c\} \\
&= \{b \in \mathbb{Z} : \text{存在 } c \in n\mathbb{Z} \text{ 使得} b = a + c\} \\
&= \{a + c : c \in n\mathbb{Z}\} \qquad (2)
\end{aligned}$$

上面最後一行的集合包含所有把 a 加上 $n\mathbb{Z}$ 中元素所得的結果，為簡便起見，也可以把上述集合記作 $a + n\mathbb{Z}$，即 $[a] = a + n\mathbb{Z}$。此外，根據《感受伽羅瓦：等價關係與分數域》中的「定理 1」，上述所有相異等價類組成的集合構成 $\mathbb{Z}$ 的一個劃分，而這個等價類集合可以記作 $\mathbb{Z}/{\equiv_n}$。

舉例說，設 $n = 6$ 和 $a = 1$，那麼根據 (1) 或 (2)，均可求得

$$[1] = \{\cdots, -11, -5, 1, 7, 13, \cdots\}$$

上述集合的元素既可看成在除以 6 後餘數為 1 的整數，也可看成 1 加上 $6\mathbb{Z}$ 中的元素 (即 6 的倍數) 所得的結果，根據前面的討論，上述集合也可記作 $1 + 6\mathbb{Z}$。此外，容易看到，在模 6 同餘下，共有六個等價類 (因為任何整數除以 6 均只有六個可能餘數)，可分別記作 [0]、[1]、[2]、[3]、[4] 和 [5]，也可分別記作 $6\mathbb{Z}\,(= 0 + 6\mathbb{Z})$、$1 + 6\mathbb{Z}$、$2 + 6\mathbb{Z}$、$3 + 6\mathbb{Z}$、$4 + 6\mathbb{Z}$ 和 $5 + 6\mathbb{Z}$，即

$$\mathbb{Z}/{\equiv_6} = \{6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z}, 5 + 6\mathbb{Z}\}$$

正如我們在上述網頁所指出，每個等價類都可以用該等價類中的任何元素作為代表，因此模 6 同餘的六個等價類其實也可記作 [108]、[−17]、[56]、[−63]、[40] 和 [−1]，或者記作 $108 + 6\mathbb{Z}$、$-17 + 6\mathbb{Z}$、$56 + 6\mathbb{Z}$、$-63 + 6\mathbb{Z}$、$40 + 6\mathbb{Z}$ 和 $-1 + 6\mathbb{Z}$，因而也有

$$\mathbb{Z}/{\equiv_6} = \{108 + 6\mathbb{Z}, -17 + 6\mathbb{Z}, 56 + 6\mathbb{Z}, -63 + 6\mathbb{Z}, 40 + 6\mathbb{Z}, -1 + 6\mathbb{Z}\}$$

以上是與整數的模 n 同餘有關的概念，有趣的是，我們可以把這些概念推廣到一般的環，設 R 為環，S 為其子環，$a, b \in R$，現定義以下關係：

$$a \sim b \text{ iff } b - a \in S \qquad (3)$$

容易證明上述關係是一個等價關係，根據此一等價關係可以確定等價類，設 $a \in R$，我們有

$$[a] = \{b \in R : a \sim b\}$$

類似同餘的情況，上述集合也可以改寫如下：

$$\begin{aligned} [a] &= \{b \in R : a \sim b\} \\ &= \{b \in R : b - a \in S\} \\ &= \{b \in R : \text{存在 } s \in S \text{ 使得} b - a = s\} \\ &= \{b \in R : \text{存在 } s \in S \text{ 使得} b = a + s\} \\ &= \{a + s : s \in S\} \qquad (4) \end{aligned}$$

為簡便起見，我們把上面最後一行的集合記作 $a+S$ (若 $a = 0$，通常寫作 S，即 $0+S = S$)。在抽象代數學上，$a+S$ 稱為以 a 為代表的 S 的陪集(coset)[1]，因此陪集實質上是等價類[2]。此外，上述所有相異陪集組成的集合構成 R 的一個劃分，而這個陪集集合可以記作 $R/\sim$。

舉例說，我們知道整係數多項式集合 $\mathbb{Z}[x]$ 構成一個環，容易看到整數集合 $\mathbb{Z}$ 是這個環的一個子環。根據 (3)，可以定義以下等價關係 (在下式中，$a, b \in \mathbb{Z}[x]$)：

$$a \sim_1 b \text{ iff } b - a \in \mathbb{Z}$$

容易驗證

$$\begin{aligned} 2 &\sim_1 -1 \\ x + 2 &\sim_1 x - 1 \\ 20x^3 - 5x + 2 &\sim_1 20x^3 - 5x - 1 \end{aligned}$$

根據 (4)，可以確定以下陪集：

$$\begin{aligned} 0 + \mathbb{Z} &= \mathbb{Z} \\ &= \{0, 1, -1, 2, -2, \cdots\} \\ x + \mathbb{Z} &= \{x + s : s \in \mathbb{Z}\} \end{aligned}$$

[1]某些人把「以 a 為代表的 S 的陪集」記作 $S+a$，由於加法在環 (不論是否交換環) 上具有交換性，$a+S$ 和 $S+a$ 其實沒有分別，都是指同一個集合。

[2]陪集與等價類的關係如下：每一個陪集都是等價類，但並非每一個等價類都是陪集。

$$
\begin{aligned}
&= \{x, x+1, x-1, x+2, x-2, \cdots\} \\
20x^3-5x+\mathbb{Z} &= \{20x^3-5x+s : s \in \mathbb{Z}\} \\
&= \{20x^3-5x, 20x^3-5x+1, 20x^3-5x-1, 20x^3-5x+2, \\
&\quad 20x^3-5x-2, \cdots\}
\end{aligned}
$$

由於陪集實質上是等價類，因此跟等價類一樣，每個陪集都可以用該陪集中的任何元素作為代表，例如上列的 $\mathbb{Z}$、$x+\mathbb{Z}$ 和 $20x^3-5x+\mathbb{Z}$ 也可以分別寫成 $1+\mathbb{Z}$、$x-1+\mathbb{Z}$ 和 $20x^3-5x+2+\mathbb{Z}$。我們也可以這樣來理解上列改寫關係，由於 $1, -1, 2 \in \mathbb{Z}$，1、-1 和 2 都可被「吸收」進 $\mathbb{Z}$，所以 $1+\mathbb{Z}$、$x-1+\mathbb{Z}$ 和 $20x^3-5x+2+\mathbb{Z}$ 分別等同於 $\mathbb{Z}$、$x+\mathbb{Z}$ 和 $20x^3-5x+\mathbb{Z}$。

此外。所有相異陪集組成以下 (無窮) 集合：

$$
\begin{aligned}
&\mathbb{Z}[x]/\sim_1 \\
= \ &\{\mathbb{Z}, x+\mathbb{Z}, -x+\mathbb{Z}, 2x+\mathbb{Z}, -2x+\mathbb{Z}, x^2+\mathbb{Z}, -x^2+\mathbb{Z}, \cdots\} \qquad (5)
\end{aligned}
$$

上述集合構成 $\mathbb{Z}[x]$ 的一個劃分。

總括以上的討論，給定一個環及其子環，我們可以根據 (3) 定義一個等價關係，並且根據 (4) 確定該子環的陪集，並從而得到該環的一個劃分。上述結果適用於任何環的任意子環，可是如果我們希望得到更豐富的內容，便要選取特定的子環，這種子環稱為理想(ideal)[3]。為方便討論，以下把討論範圍限於交換環，即乘法具有交換性的環。給定一個交換環 R，其子環 I 稱為 R 的理想當且僅當對任何 $i \in I$ 和 $r \in R$，均有 $ir \in I$[4]。

根據上述定義，要證明 I 是交換環 R 的理想，首先要證明 I 是子環，並且 I 要像一個「乘法黑洞」，即 R 的任何元素一旦與 I 的元素相乘，所得結果都被「吸進」I 中。

舉例說，$6\mathbb{Z}$ 便是交換環 $\mathbb{Z}$ 的理想。在前面我們已指出 $6\mathbb{Z}$ 是 $\mathbb{Z}$ 的子環，容易看到，$6\mathbb{Z}$ 也是一個「乘法黑洞」，這是因為任何整數乘以 6 的倍數，必然也是 6 的倍數。另一方面，$\mathbb{Z}$ 雖然是 $\mathbb{Z}[x]$ 的子環，但卻不是 $\mathbb{Z}[x]$ 的理想，例如把 $\mathbb{Z}$ 的成員 5 乘以 $\mathbb{Z}[x]$ 的成員 x，所得結果 $5x$ 不是 $\mathbb{Z}$ 的成員，由此可見 $\mathbb{Z}$ 不是「乘法黑洞」。

[3]有些讀者可能感到奇怪，為何數學家要選用「理想」這個古怪詞語來指稱某一類子環？這是因為 19 世紀數學家庫默爾 (Kummer) 最初把某一類數稱為「理想數」(ideal number)，後來其他數學家把理想數的某些性質推廣至其他情況，並逐漸演變為把某一類子環稱為「理想」。

[4]如果討論的環是非交換環，便要區分「左理想」和「右理想」，這會令以下的討論頗為複雜，這就是我們把討論範圍限於交換環的原因。

接下來介紹一種有特殊結構的理想。設 R 為交換環，並設 $i_1, \cdots, i_n \in R$，那麼可以證明

$$\langle i_1, \cdots, i_n \rangle = \{i_1 r_1 + \cdots + i_n r_n : r_1, \cdots, r_n \in R\} \qquad (6)$$

是一個理想，稱為由 $i_1, \cdots, i_n$ 生成的理想(ideal generated by $i_1, \cdots, i_n$)。特別地，當 $n = 1$，上述定義變成

$$\langle i \rangle = \{ir : r \in R\} \qquad (7)$$

上述理想稱為由 i 生成的主理想(principal ideal generated by i)。

舉例說，容易看到 $6\mathbb{Z}$ 等於以下集合：

$$6\mathbb{Z} = \{6r : r \in \mathbb{Z}\} = \langle 6 \rangle$$

因此 $6\mathbb{Z}$ 可被看成由 6 生成的主理想。

接著看一些較複雜的例子，試考慮以下根據 (6) 定義的理想：

$$\langle -18, 42 \rangle = \{-18r_1 + 42r_2 : r_1, r_2 \in \mathbb{Z}\}$$

上式雖然看似由 -18 和 42 生成的理想，但由於 -18 和 42 的最大公因數是 6，運用我們在《感受伽羅瓦：整數與多項式》中介紹的「歐幾里得算法」，可以求得

$$6 = (-18)(2) + 42$$

因此 6 的任何倍數都可寫成 $-18r_1 + 42r_2$ 的形式，例如由於 $102 = 6 \times 17$，利用上式，可馬上求得

$$\begin{aligned} 102 &= 6 \times 17 \\ &= ((-18)(2) + 42) \times 17 \\ &= (-18)(34) + (42)(17) \end{aligned}$$

上述結果顯示 $102 \in \langle -18, 42 \rangle$，由此容易看到 6 的任何倍數都屬於 $\langle -18, 42 \rangle$。反過來，也容易看到 $\langle -18, 42 \rangle$ 的任何成員都是 6 的倍數，由此我們有

$$\langle -18, 42 \rangle = \langle 6 \rangle$$

上述結果顯示 $\langle -18, 42 \rangle$ 可以化約為由 6 生成的主理想。事實上，可以證明 $\mathbb{Z}$ 下的所有理想都是主理想，因此之故，$\mathbb{Z}$ 這類環可稱為主理想環(principal ideal ring)，即所有理想都是主理想的環。

接著看一個非主理想環的例子，考慮交換環 $\mathbb{Z}[x]$，這個環當然有主理想，例如根據 (7)，可以定義以下由 x 生成的主理想：

$$\begin{aligned}\langle x\rangle &= \{xr : r\in\mathbb{Z}[x]\}\\ &= \{0, x, -x, 2x, -2x, x^2, -x^2, \cdots\}\end{aligned}$$

上述集合包含所有常數項等於 0 的整係數多項式。可是，並非 $\mathbb{Z}[x]$ 的所有理想都是主理想，試考慮以下由 2 和 x 生成的理想：

$$\langle 2, x\rangle = \{2r_1 + xr_2 : r_1, r_2 \in \mathbb{Z}[x]\}$$

上述集合包含所有常數項為偶數的整係數多項式，例如 $6\,(=(2)(3)+(x)(0))$、$20x^3-5x-144\,(=(2)(-72)+(x)(20x^2-5))$ 等等。

以下讓我們驗證上述集合確是 $\mathbb{Z}[x]$ 的一個理想。首先驗證它是 $\mathbb{Z}[x]$ 的子環，任選 $\langle 2, x\rangle$ 中的兩個元素 i_1 和 i_2，那麼這兩個元素可以寫成 $i_1 = 2r_1 + xr_2$ 和 $i_2 = 2r_3 + xr_4$ 的形式，其中 $r_1, r_2, r_3, r_4 \in \mathbb{Z}[x]$，以下計算這兩個元素相加和相乘的結果：

$$\begin{aligned}i_1 + i_2 &= 2r_1 + xr_2 + 2r_3 + xr_4\\ &= 2(r_1 + r_3) + x(r_2 + r_4)\\ i_1 i_2 &= (2r_1 + xr_2)(2r_3 + xr_4)\\ &= 4r_1r_3 + 2xr_1r_4 + 2xr_2r_3 + x^2r_2r_4\\ &= 2(2r_1r_3 + xr_1r_4 + xr_2r_3) + x(xr_2r_4)\end{aligned}$$

上述結果顯示 $i_1 + i_2$ 和 i_1i_2 都是 $\langle 2, x\rangle$ 的元素，即 $+$ 和 $\times$ 運算在 $\langle 2, x\rangle$ 上封閉。此外，容易看到 $\mathbb{Z}[x]$ 中的加法單位元 $0 = 2(0) + x(0)$，所以 $0 \in \langle 2, x\rangle$；而 $\langle 2, x\rangle$ 中任意元素 $i_1 = 2r_1 + xr_2$ 的加法逆元是 $-i_1 = -2r_1 - xr_2 = 2(-r_1) + x(-r_2)$，所以 $-i_1 \in \langle 2, x\rangle$。至此驗證了 $\langle 2, x\rangle$ 是 $\mathbb{Z}[x]$ 的子環。其次驗證 $\langle 2, x\rangle$ 是「乘法黑洞」，任選 $\langle 2, x\rangle$ 中元素 $i_1 = 2r_1+xr_2$ 和 $\mathbb{Z}[x]$ 中元素 r_3，那麼 $i_1r_3 = (2r_1+xr_2)r_3 = 2(r_1r_3)+x(r_2r_3)$，即 $i_1r_3 \in \langle 2, x\rangle$，由此可見 $\langle 2, x\rangle$ 確是「乘法黑洞」。至此驗證了 $\langle 2, x\rangle$ 確是 $\mathbb{Z}[x]$ 的理想。

接著讓我們用反證法證明 $\langle 2, x\rangle$ 不是主理想。為此，假設 $\langle 2, x\rangle = \langle f\rangle$，其中 $f \in \mathbb{Z}[x]$，那麼由於 $2, x \in \langle 2, x\rangle$，必有

$$\begin{aligned}2 &= fr_1 \qquad (8)\\ x &= fr_2 \qquad (9)\end{aligned}$$

其中 $r_1, r_2 \in \mathbb{Z}[x]$。根據 (8)，$f$ 不可能是次數大於或等於 1 的多項式，因為把這樣的多項式乘以另一個多項式 r_1，不可能得到常數多項式 2。因此

f 必然是整數，而且只可能是 ± 1 或 ± 2。但由於 $\pm 1 \notin \langle 2, x\rangle$，故 $f = \pm 2$。把這一點代入 (9)，會得到 $x = \pm 2r_2$，由此便會得到 $r_2 = \pm\frac{1}{2}x$，但這違反了 $r_2 \in \mathbb{Z}[x]$ 的假設。由此證得 $\langle 2, x\rangle$ 不能化約為 $\langle f\rangle$，即它不是主理想。

給定一個交換環 R 及其理想 I，由於 I 是 R 的子環，我們也可應用前述的 (3) 和 (4) 就 I 定義一個等價關係 $\sim$ 和 I 的陪集 $a + I$ (只須把 (3) 和 (4) 中的 S 改為 I 即可)，從而得到一個陪集集合 $R/\sim$。有趣的是，這個陪集集合不僅是一個集合,而且是一個代數結構。事實上,我們有以下定理。

定理 1：設 R 為交換環，I 為其子環，則 I 的陪集構成一個環，當且僅當 I 是 R 的理想。上述由陪集組成的環的加法和乘法定義如下。設 $a+I$ 和 $b+I$ 為 I 的兩個陪集，則

$$(a+I)+(b+I) = a+b+I \qquad (10)$$
$$(a+I)\times(b+I) = ab+I \qquad (11)$$

這個環的加法單位元是 $I\,(= 0+I)$，$a+I$ 的加法逆元是 $-a+I$。

以下把上述定理中的環記作 R/I，這個環稱為 R 關於 I 的商環(quotient ring)[5]。有些讀者可能覺得 (10) 和 (11) 中的等式違背一般的代數法則，他們可能覺得 $(a+I)+(b+I)$ 似乎應該等於 $a+b+2I$，這是對上式的誤解。在上式中，$a+I$ 不是代表兩個變項相加，而是代表一個陪集，由於陪集實質上是等價類，所以 $a+I$ 其實也可寫成 $[a]$。如果採用這種寫法，上式便變得合理了：

$$[a]+[b] = [a+b]$$
$$[a]\times[b] = [ab]$$

接下來讓我們看商環的具體例子。前面曾指出 $6\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想，因此根據「定理 1」，

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

構成一個商環。根據 (10) 和 (11)，可以計算以下結果 (請注意 $7+6\mathbb{Z}$ 和 $12+6\mathbb{Z}$ 分別等於 $1+6\mathbb{Z}$ 和 $6\mathbb{Z}$)：

$$(3+6\mathbb{Z})+(4+6\mathbb{Z}) = 1+6\mathbb{Z} \qquad (12)$$
$$(3+6\mathbb{Z})\times(4+6\mathbb{Z}) = 6\mathbb{Z} \qquad (13)$$

[5]請注意「商集」和「商環」所用的不同符號，「商集」符號 $R/\sim$ 使用代表等價關係的 $\sim$，「商環」符號 R/I 則使用代表理想的 I。

請注意 (10) 和 (11) 是良定義的，這即是說在把兩個陪集相加或相乘時，不論採用陪集中的哪個元素作為代表，都會得到相同的結果。舉例說，$3+6\mathbb{Z}$ 和 $4+6\mathbb{Z}$ 可分別改寫成 $-63+6\mathbb{Z}$ 和 $40+6\mathbb{Z}$，而根據 (10) 和 (11)，

$$\begin{aligned}(-63+6\mathbb{Z})+(40+6\mathbb{Z}) &= -23+6\mathbb{Z}\\(-63+6\mathbb{Z})\times(40+6\mathbb{Z}) &= -2520+6\mathbb{Z}\end{aligned}$$

但 $-23+6\mathbb{Z}$ 和 $-2520+6\mathbb{Z}$ 分別等於 $1+6\mathbb{Z}$ 和 $6\mathbb{Z}$，所以上述計算實質上分別等同於 (12) 和 (13)。

前面也曾指出 $\langle 2,x\rangle$ 是 $\mathbb{Z}[x]$ 的理想，因此根據「定理 1」，

$$\mathbb{Z}[x]/\langle 2,x\rangle=\{\langle 2,x\rangle, 1+\langle 2,x\rangle\}$$

也構成一個商環，這個商環僅有兩個陪集，其中 $\langle 2,x\rangle$ 包含所有常數項為偶數的整係數多項式，$1+\langle 2,x\rangle$ 則包含所有常數項為奇數的整係數多項式。根據 (10) 和 (11)，可以計算以下結果 (請注意 $2+\langle 2,x\rangle$ 等於 $\langle 2,x\rangle$)：

$$\begin{aligned}(1+\langle 2,x\rangle)+(1+\langle 2,x\rangle) &= \langle 2,x\rangle \qquad (14)\\\langle 2,x\rangle\times(1+\langle 2,x\rangle) &= \langle 2,x\rangle \qquad (15)\end{aligned}$$

為驗證 (10) 和 (11) 是良定義的，我們首先把 $1+\langle 2,x\rangle$ 和 $\langle 2,x\rangle$ 分別改寫成 $-8x^9+11+\langle 2,x\rangle$ 和 $6+\langle 2,x\rangle$，然後根據 (10) 和 (11)，

$$\begin{aligned}(-8x^9+11+\langle 2,x\rangle)+(-8x^9+11+\langle 2,x\rangle) &= -16x^9+22+\langle 2,x\rangle\\(6+\langle 2,x\rangle)\times(-8x^9+11+\langle 2,x\rangle) &= -48x^9+66+\langle 2,x\rangle\end{aligned}$$

但 $-16x^9+22+\langle 2,x\rangle$ 和 $-48x^9+66+\langle 2,x\rangle$ 兩者都等於 $\langle 2,x\rangle$，所以上述計算實質上分別等同於 (14) 和 (15)。

請注意根據「定理 1」，只有當 I 是 R 的理想 (而非僅普通子環) 時，I 的陪集才構成商環。前面曾指出 $\mathbb{Z}$ 不是 $\mathbb{Z}[x]$ 的理想，現在讓我們來看 $\mathbb{Z}$ 的陪集 (這些陪集的例子見 (5)) 並不構成商環，為證明這一點，只須證明 (11) 所定義的乘法對於這些陪集來說不是良定義的。為此，首先根據 (11) 計算：

$$\mathbb{Z}\times(x+\mathbb{Z})=\mathbb{Z}$$

其次，把 $\mathbb{Z}$ 改寫成 $5+\mathbb{Z}$，並再次根據 (11) 計算

$$(5+\mathbb{Z})\times(x+\mathbb{Z})=5x+\mathbb{Z}$$

可是，$\mathbb{Z}\neq 5x+\mathbb{Z}$(因為 $5x\notin\mathbb{Z}$)，因此上述兩個乘法結果不相等，由此可見 (11) 所定義的乘法對於 (5) 中的陪集來說不是良定義的，即 (5) 中的陪集並不構成商環。

連結至數學專題
連結至周家發網頁