感受伽羅瓦：等價關係與分數域

我們在《感受伽羅瓦：環及其子類》中介紹了環及其各種子類，如域、整環等，其中域可以說是最「完美」的代數結構，因為它滿足上述網頁列出的全部十條公理，因而可在其上進行加、減、乘和整除這四種運算，而在我們熟悉的數系中，$\mathbb{Z}_p$ (其中 p 是正質數)、$\mathbb{Q}$、$\mathbb{R}$ 和 $\mathbb{C}$ 都構成域。

跟域比較，整環卻沒有那麼「完美」，因為整環只滿足上述網頁中的九條公理，在其上可以進行加、減、乘運算，但不能進行整除運算。根據上述網頁，我們也知道 $\mathbb{Z}$、$\mathbb{Z}[x]$、$\mathbb{Z}_p[x]$(其中 p 是正質數)、$\mathbb{Q}[x]$、$\mathbb{R}[x]$ 和 $\mathbb{C}[x]$ 都構成整環[1]。可喜的是，數學家發現了一些方法，可以使整環「完美化」，將之擴充為域，其中一種方法的靈感來自把 $\mathbb{Z}$ 擴充為 $\mathbb{Q}$ 的過程。但在詳細介紹這種方法前，須先引入等價關係(equivalence relation) 及其相關概念。

等價關係是一種特殊的二元關係 (即存在於兩件事物之間的關係)，以下用 $\sim$ 來代表。設 S 為集合，S 上二元關係 $\sim$ 是等價關係當且僅當對 S 中任何元素 a、b、c，均有

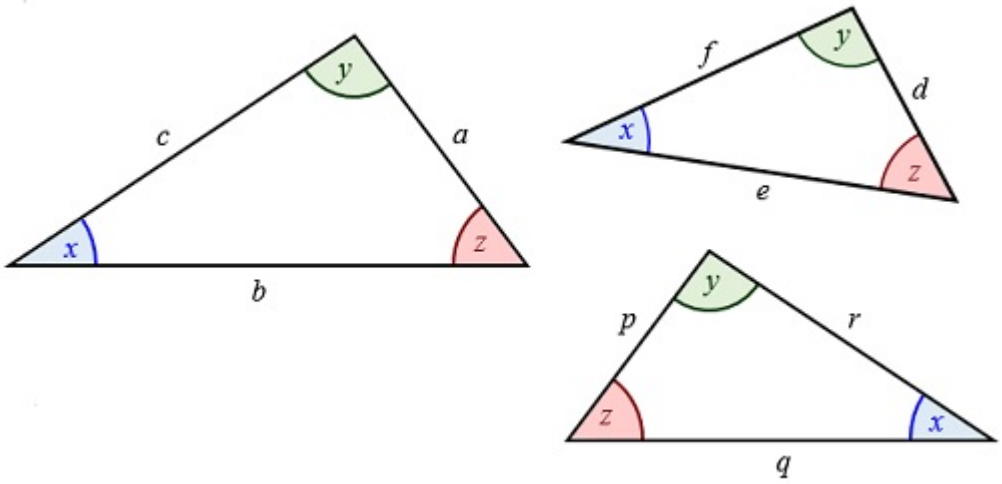
(i) $a \sim a$，即 $\sim$ 具有自反性(reflexivity)

(ii) 若 $a \sim b$，則 $b \sim a$，即 $\sim$ 具有對稱性(symmetry)

(iii) 若 $a \sim b$ 並且 $b \sim c$，則 $a \sim c$，即 $\sim$ 具有傳遞性(transitivity)

等價關係其實是對「相等關係」(equality，通常用等號 $=$ 表示) 的抽象，容易驗證我們通常理解的「相等關係」具有上述三種性質，因此是一種等價關係 (也可以說相等關係是等價關係的「原型」)。但除了相等關係外，數學上還存在其他等價關係，這些等價關係雖然並不表示兩件事物之間的相等關係，但在某程度上是相等關係的推廣，可被看成在某方面隱含著相等關係。以下介紹兩種等價關係，第一種是三角形之間的「相似關係」(similarity)。根據基礎幾何學，如果兩個三角形的所有對應角相等，則該兩個三角形是相似三角形，下圖展示三個相似三角形：

[1]嚴格地說，上述這些整環都屬於整環中的某個子類，稱為「歐幾里得整環」(Euclidean domain)，在「歐幾里得整環」中雖然不能進行整除運算，但可進行帶有餘數的除運算。不過由於歐幾里得整環涉及一些複雜定義，這裡不予介紹。



在上圖中，三角形 abc 與 def 的三對對應角 (即標示為 x、y 和 z 的角) 相等，所以是相似三角形。同樣，也可看到 def 與 pqr 以及 abc 與 pqr 也是相似三角形。請注意上述三個三角形儘管各不相等 (它們處於不同的位置，各有不同的邊長)，但卻隱含著「對應角相等」此一相等關係，因此三角形的相似關係可被看成相等關係的推廣。事實上，借助上圖，容易驗證相似關係具有等價關係的上述三種性質：(i) 自反性，例如三角形 abc 與自身相似；(ii) 對稱性，例如三角形 abc 與 def 相似，而 def 也與 abc 相似；(iii) 傳遞性，例如三角形 abc 與 def 相似，並且 def 與 pqr 相似，而 abc 也與 pqr 相似。

第二種等價關係是整數之間的同餘(congruence modulo) 關係。給定正整數 n 和兩個整數 a 和 b，我們說 a 與 b 關於模 n 同餘 (記作 $a \equiv_n b$)[2]，當且僅當 a 和 b 除以 n 所得的餘數相等。為方便驗算，上述定義也可以表述為以下等價形式：a 與 b 關於模 n 同餘當且僅當 $b-a$ 是 n 的倍數。舉例說，我們有

$$4 \equiv_3 -11$$

這是因為 4 和 -11 除以 3 所得的餘數都是 1，或者等價地，$-11-4\,(=-15)$ 是 3 的倍數。請注意 4 和 -11 儘管並不相等，但卻隱含著「除以 3 所得的餘數相等」此一相等關係，因此同餘關係可被看成相等關係的另一種推廣。事實上，不難證明同餘關係具有等價關係的上述三種性質。

確定集合 S 上的等價關係 $\sim$ 後，便可以就 S 中的任一元素 a 找出所有與 a 等價的元素，這些元素所組成的集合稱為以 a 為代表的等價類(equivalence

[2]數學上通常把「a 與 b 關於模 n 同餘」記作 $a \equiv b \pmod{n}$，但由於這種記法頗為累贅，本文採用較簡單的記法。另外，由於同餘關係有專用的符號 $\equiv_n$，所以這裡不用 $\sim$ 這個符號代表這個等價關係。

class)，記作 $[a]$，即

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

以前述的相似三角形為例，假設把圖中三個三角形歸入一個集合 $\text{Tri} = \{abc, def, pqr\}$，並用 $\sim_1$ 代表三角形之間的相似關係，那麼由於這三個三角形互相相似，容易看到

$$\begin{aligned} [abc] &= \{\Delta \in \text{Tri} : abc \sim_1 \Delta\} \\ &= \{abc, def, pqr\} \end{aligned}$$

同樣也有

$$\begin{aligned} [def] &= \{abc, def, pqr\} \\ [pqr] &= \{abc, def, pqr\} \end{aligned}$$

另外又如根據前述的模 3 同餘關係，可以在 $\mathbb{Z}$ 上確定等價類如下：

$$\begin{aligned} [0] &= \{b \in \mathbb{Z} : 0 \equiv_3 b\} \\ &= \{...-6, -3, 0, 3, 6, ...\} \\ [1] &= \{b \in \mathbb{Z} : 1 \equiv_3 b\} \\ &= \{...-5, -2, 1, 4, 7, ...\} \\ [2] &= \{b \in \mathbb{Z} : 2 \equiv_3 b\} \\ &= \{...-4, -1, 2, 5, 8, ...\} \\ [3] &= \{b \in \mathbb{Z} : 3 \equiv_3 b\} \\ &= \{...-6, -3, 0, 3, 6, ...\} \\ [4] &= \{b \in \mathbb{Z} : 4 \equiv_3 b\} \\ &= \{...-5, -2, 1, 4, 7, ...\} \\ [5] &= \{b \in \mathbb{Z} : 5 \equiv_3 b\} \\ &= \{...-4, -1, 2, 5, 8, ...\} \\ &\vdots \end{aligned}$$

容易看到

$$[a] = \begin{cases} \{...-6, -3, 0, 3, 6, ...\}, & \text{若 } a \text{ 可被 3 整除} \\ \{...-5, -2, 1, 4, 7, ...\}, & \text{若 } a \text{ 除以 3 所得的餘數是 1} \\ \{...-4, -1, 2, 5, 8, ...\}, & \text{若 } a \text{ 除以 3 所得的餘數是 2} \end{cases}$$

從上述例子可以看到，一個等價類可以取該等價類中的任何元素作為代表，例如在模 3 同餘關係下，$\{...-6, -3, 0, 3, 6, ...\}$ 這個等價類可以取 0、3 以

至 -369 作為代表，即 $[0]=[3]=[-369]$；相異等價類沒有相同的元素，即相異等價類之間的交集是空集，例如在模 3 同餘關係下，我們有

$$[0]\cap[1]=\emptyset,\ \ [0]\cap[2]=\emptyset,\ \ [1]\cap[2]=\emptyset$$

所有相異等價類的元素窮盡集合 S 的所有元素，即所有相異等價類的并集等於 S，例如在模 3 同餘關係下，我們有

$$[0]\cup[1]\cup[2]=\mathbb{Z}$$

事實上，根據集合論，我們有以下定理。

定理 1：設 $\sim$ 為集合 S 上的一個等價關係，則 S 的所有相異等價類組成的集合構成 S 的一個劃分(partition)，即 S 的相異等價類之間的交集是空集，並且 S 的所有相異等價類的并集等於 S。

以下把 S 在等價關係 $\sim$ 下的相異等價類組成的集合記作 $S/\sim$，這個集合稱為 S 關於 $\sim$ 的商集(quotient set)。請注意由於 S 的等價類是集合，所以 $S/\sim$ 是由集合組成的集合 (亦稱「集合族」collection of sets)。以 $\mathbb{Z}$ 為例，這個集合在模 3 同餘關係下有三個相異等價類：$[0]$、$[1]$ 和 $[2]$，前面我們已論證了這三個等價類兩兩之間的交集是空集，並且它們的并集等於 $\mathbb{Z}$，因此這三個等價類構成 $\mathbb{Z}$ 的一個劃分，而且我們有

$$\begin{aligned}&\mathbb{Z}/\equiv_3\\ =\ &\{[0],[1],[2]\}\\ =\ &\{\{...-6,-3,0,3,6,...\},\{...-5,-2,1,4,7,...\},\{...-4,-1,2,5,8,...\}\}\end{aligned}$$

另外又如前述的三角形集合 Tri，在相似關係 $\sim_1$ 下這個集合只有一個等價類 $[abc]$，這個等價類自然構成 Tri 的一個劃分，而且我們有

$$\begin{aligned}&\mathrm{Tri}/\sim_1\\ =\ &\{[abc]\}\\ =\ &\{\{abc,def,pqr\}\}\end{aligned}$$

請注意上列集合族僅由一個集合組成。

有了等價關係的概念，便可討論如何把 $\mathbb{Z}$ 擴充為 $\mathbb{Q}$，有理數是指具有形式 $\frac{a}{b}$ 的數，其中 a 是整數，b 是非零整數。如果撇除分數線，我們也可以把有理數抽象地看成「有序對」(a,b)，其中第一坐標 a 由整數組成，代表分子；第二坐標 b 由非零整數組成，代表分母。為方便以下的討論，我們把由這些有序對組成的集合記作 $\mathbb{Z}\times(\mathbb{Z}-\{0\})$，即

$$\mathbb{Z}\times(\mathbb{Z}-\{0\})=\{(a,b):a\in\mathbb{Z}\wedge b\in\mathbb{Z}-\{0\}\}$$

惟請注意 $\mathbb{Q} \neq \mathbb{Z} \times (\mathbb{Z} - \{0\})$，這是因為即使 (a, b) 和 (c, d) 是兩個不同的有序對，但它們卻可能對應著同一個有理數。運用簡單的算術運算，我們有

$$\frac{a}{b} = \frac{c}{d} \text{ iff } ad = bc$$

由此可以定義以下等價關係 $\sim_2$：設 (a, b) 和 (c, d) 為 $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ 的成員，則

$$(a, b) \sim_2 (c, d) \text{ iff } ad = bc \qquad (1)$$

容易證明 (1) 所定義的 $\sim_2$ 確是等價關係。舉例說，由於 $(1)(-6) = (2)(-3)$，我們有 $(1, 2) \sim_2 (-3, -6)$，換句話說，$(1, 2)$ 和 $(-3, -6)$ 雖然是不同的有序對，但其實隱含著 $\frac{1}{2} = \frac{-3}{-6}$ 此一相等關係。

我們可以把前述的等價類概念推廣到 $\sim_2$，舉例說，我們有

$$\begin{aligned} [(1, 2)] &= \{(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) : (1, 2) \sim_2 (a, b)\} \\ &= \{(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) : b = 2a\} \\ &= \{(1, 2), (2, 4), (-3, -6), ...\} \end{aligned}$$

容易看到上述等價類對應著 $\frac{1}{2}$ 這個有理數。以下是另一個等價類：

$$\begin{aligned} [(-7, 4)] &= \{(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) : (-7, 4) \sim_2 (a, b)\} \\ &= \{(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) : -7b = 4a\} \\ &= \{(-7, 4), (-14, 8), (21, -12), ...\} \end{aligned}$$

容易看到上述等價類對應著 $-\frac{7}{4}$ 這個有理數，而且等價類 $[(-7, 4)]$ 與 $[(1, 2)]$ 沒有共同元素，因為它們各自對應著不同的有理數。

至此我們看到，有理數所對應的不是 $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ 的成員，而是 $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ 的等價類。根據前面的討論，我們把這些等價類組成的 (無窮) 集合記作

$$\begin{aligned} & (\mathbb{Z} \times (\mathbb{Z} - \{0\}))/\sim_2 \\ = \ & \{[(0, 1)], [(1, 1)], [(-1, 1)], [(1, 2)], [(-1, 2)], [(2, 1)], [(-2, 1)], \cdots\} \end{aligned}$$

根據「定理 1」，我們知道上述集合構成 $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ 的一個劃分，即上述集合中的元素對應著各不相同的有理數，而且窮盡了全體有理數。

以上我們確立了 $\mathbb{Q}$ 與 $(\mathbb{Z} \times (\mathbb{Z} - \{0\}))/\sim_2$ 這兩個集合的成員的對應關係，還未確立這兩個集合的運算的對應關係。但這並不困難，給定 $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$，我們有

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd} \\ \frac{a}{b} \times \frac{c}{d} &= \frac{ac}{bd} \end{aligned}$$

據此，可以定義 $(\mathbb{Z}\times(\mathbb{Z}-\{0\}))/\sim_2$ 上的加法和乘法運算如下：給定 $[(a,b)],[(c,d)]\in(\mathbb{Z}\times(\mathbb{Z}-\{0\}))/\sim_2$，我們有

$$\begin{aligned}[(a,b)]+[(c,d)] &= [(ad+bc,bd)] \qquad (2)\\ [(a,b)]\times[(c,d)] &= [(ac,bd)] \qquad (3)\end{aligned}$$

可以證明上述兩個運算是「良定義」(well defined) 的，即運算結果並不依賴於等價類的代表。舉例說，$[(1,2)]$ 與 $[(-3,-6)]$ 是同一個等價類 (兩者都對應著有理數 $\frac{1}{2}$)，$[(-7,4)]$ 與 $[(21,-12)]$ 也是同一個等價類 (兩者都對應著有理數 $-\frac{7}{4}$)。根據 (2)，我們有

$$\begin{aligned}[(1,2)]+[(-7,4)] &= [((1)(4)+(2)(-7),(2)(4))]\\ &= [(-10,8)]\\ [(-3,-6)]+[(21,-12)] &= [(-3)(-12)+(-6)(21),(-6)(-12)]\\ &= [(-90,72)]\end{aligned}$$

請注意以上兩個計算結果 $[(-10,8)]$ 和 $[(-90,72)]$ 是同一個等價類 (兩者都對應著有理數 $-\frac{5}{4}$)，這即是說不論取哪一個代表 $\frac{1}{2}$ 的有序對與哪一個代表 $-\frac{7}{4}$ 的有序對相加，所得結果都是某個代表 $-\frac{5}{4}$ 的有序對，而 $\frac{1}{2}+(-\frac{7}{4})=-\frac{5}{4}$。

不僅如此，還可以證明 (2) 和 (3) 所定義的加法和乘法滿足《感受伽羅瓦：環及其子類》中介紹的十條公理，例如 $[(0,1)]$ 和 $[(1,1)]$ 分別是加法和乘法單位元；給定 $[(a,b)]\in\mathbb{Z}\times(\mathbb{Z}-\{0\})$，其加法逆元是 $[(-a,b)]$，而且若 $a\neq 0$，則其乘法逆元是 $[(b,a)]$。

總上所述，$(\mathbb{Z}\times(\mathbb{Z}-\{0\}))/\sim_2$ 加上上述兩個運算是一個域。此外，容易看到，每個整數 a 都與 $(\mathbb{Z}\times(\mathbb{Z}-\{0\}))/\sim_2$ 的成員 $[(a,1)]$ 存在對應關係 (因為任何整數 a 都等於有理數 $\frac{a}{1}$)，因此整數集 $\mathbb{Z}$ 可被看成 $(\mathbb{Z}\times(\mathbb{Z}-\{0\}))/\sim_2$ 的子集。至此我們證明了，通過引入有序對和等價類的概念，可以把 $(\mathbb{Z},+,\times)$ 這個整環擴充為 $((\mathbb{Z}\times(\mathbb{Z}-\{0\}))/\sim_2,+,\times)$ 這個域。由於 $(\mathbb{Z}\times(\mathbb{Z}-\{0\}))/\sim_2$ 中的成員對應著分數 (即有理數)，有些人把 $((\mathbb{Z}\times(\mathbb{Z}-\{0\}))/\sim_2,+,\times)$ 稱為 $(\mathbb{Z},+,\times)$ 的分數域(field of fractions)。

有趣的是，我們可以把上述方法應用於其他整環，從而推導出相應的分數域，以下以 $\mathbb{Z}[x]$ 為例說明這一點。如前所述，$\mathbb{Z}[x]$ 是一個整環而非域，這是因為 $\mathbb{Z}[x]$ 中並非每個非零成員都有乘法逆元。可是，如果我們把眼光從「多項式」擴展到有理式(rational expression)，情況便有所不同。有理式是指具有 $\frac{a}{b}$ 形式的數式，其中 a、b 是多項式，並且 $b\neq 0$，例如 $\frac{1}{x^2+x+1}$ 便是有理式，請注意任何多項式都是分母為 1 的有理式。以下把分子分母皆為整係數多項式的有理式稱為「整係數有理式」，並把這些有理式組成的集

合記作 $\mathbb{Z}(x)$ 以區別於整係數多項式集合 $\mathbb{Z}[x]$[3]，這樣 x^2+x+1 在 $\mathbb{Z}[x]$ 中沒有乘法逆元，但在 $\mathbb{Z}(x)$ 中卻有乘法逆元 $\frac{1}{x^2+x+1}$。

跟有理數的情況相似, 我們可以把整係數有理式抽象地看成有序對 (a,b), 其中第一坐標 a 由整係數多項式組成, 代表分子；第二坐標 b 由非零整係數多項式組成, 代表分母, 並把由這些有序對組成的集合記作 $\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\})$, 即

$$\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\})=\{(a,b):a\in\mathbb{Z}[x]\wedge b\in\mathbb{Z}[x]-\{0\}\}$$

但 $\mathbb{Z}(x)\neq\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\})$，這是因為即使 (a,b) 和 (c,d) 是兩個不同的有序對，但它們卻可能對應著同一個整係數有理式。為此，我們可以沿用上面 (1) 定義的等價關係 $\sim_2$，只需把 (1) 中的 a、b、c、d 看成整係數多項式 (而非整數) 便可。有了上述等價關係，便可定義相應的等價類。舉例說，我們有

$$\begin{aligned}
& [(1,x^2+x+1)]\\
= \;& \{(a,b)\in\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\}):(1,x^2+x+1)\sim_2(a,b)\}\\
= \;& \{(a,b)\in\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\}):b=a(x^2+x+1)\}\\
= \;& \{(1,x^2+x+1),(-x,-x^3-x^2-x),(\frac{1}{2},\frac{1}{2}x^2+\frac{1}{2}x+\frac{1}{2}),\cdots\}
\end{aligned}$$

容易看到上述等價類對應著 $\frac{1}{x^2+x+1}$ 這個整係數有理式，並由此看到整係數有理式所對應的不是 $\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\})$ 的成員，而是 $\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\})$ 的等價類。我們把這些等價類組成的 (無窮) 集合記作

$$\begin{aligned}
& (\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\}))/\sim_2\\
= \;& \{[(0,1)],[(1,1)],[(-1,1)],[(1,2)],[(-1,2)],[(1,x)],[(-1,x)],[(2,1)],[(-2,1)],\\
& [(x,1)],[(-x,1)],[(1,3)],[(-1,3)],[(1,2x)],[(-1,2x)],[(1,x^2)],[(-1,x^2)],\cdots\}
\end{aligned}$$

根據「定理 1」，我們知道上述集合構成 $\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\})$ 的一個劃分，由此確立了 $\mathbb{Z}(x)$ 與 $(\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\}))/\sim_2$ 這兩個集合的成員的對應關係。此外，我們還可以沿用上面的 (2) 和 (3) 定義 $(\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\}))/\sim_2$ 上的加法和乘法運算 (只需把 (2) 和 (3) 中的 a、b、c、d 看成整係數多項式)。舉例說，我們有

$$\begin{aligned}
& [(2x,3x+7)]+\big[(1,x^2+x+1)\big]\\
= \;& \big[((2x)(x^2+x+1)+(3x+7)(1),(3x+7)(x^2+x+1))\big]\\
= \;& \big[(2x^3+2x^2+5x+7,3x^3+10x^2+10x+7)\big]
\end{aligned}$$

[3]在抽象代數學中，方括號和圓括號分別代表 (非域) 環和域。整係數多項式的集合是整環 (非域環的一種)，所以記作 $\mathbb{Z}[x]$；整係數有理式的集合是域，所以記作 $\mathbb{Z}(x)$。

上述結果反映了以下計算結果：

$$\frac{2x}{3x+7}+\frac{1}{x^2+x+1}=\frac{2x^3+2x^2+5x+7}{3x^3+10x^2+10x+7}$$

正如有理數的情況，可以證明上述加法和乘法運算是良定義的，並且 $(\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\}))/\sim_2$ 連同上述兩種運算構成一個域。由於 $\mathbb{Z}[x]$ 的每個成員 a 都與 $(\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\}))/\sim_2$ 的成員 $[(a,1)]$ 存在對應關係，可以把 $\mathbb{Z}[x]$ 看成 $(\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\}))/\sim_2$ 的子集，因此 $((\mathbb{Z}[x]\times(\mathbb{Z}[x]-\{0\}))/\sim_2,+,\times)$ 是 $(\mathbb{Z}[x],+,\times)$ 的分數域。

連結至數學專題
連結至周家發網頁