感受伽羅瓦：群的基本概念

在前面各章，我們討論了包含加、乘這兩種運算的代數結構—環的特點。但在某些應用中，我們需要考慮只包含一種運算的代數結構。在這類結構中，群(group) 是最重要的一種，本章主旨是介紹與群有關的一些基本概念。

群是指一個集合 G 加上其上的一個二元封閉運算 (以下記作 $\circ$) 且滿足以下公理的代數結構 (以下把這個代數結構記作 $(G,\circ)$)，在以下公理中，a、b 和 c 是 S 中任意元素：

(i) $(a\circ b)\circ c = a\circ(b\circ c)$

(ii) 存在單位元 (記作 e) 使得 $a\circ e = e\circ a = a$

(iii) 對於每個元素 a，存在其逆元 (記作 a')，使得 $a\circ a' = a'\circ a = e$

如果群 $(G,\circ)$ 還滿足以下公理：

(iv) $a\circ b = b\circ a$

則稱 $(G,\circ)$ 為交換群(commutative group)，亦稱阿貝爾群(Abelian group)。

把以上定義跟環和域的定義 (見《感受伽羅瓦：環及其子類》) 加以比較，容易看到給定一個環 $(R,+,\times)$，那麼 $(R,+)$ 構成一個交換群；而如果 $(R,+,\times)$ 是一個域，那麼 $(R-\{0\},\times)$ 也構成一個交換群。舉例說，由於 $(\mathbb{Q},+,\times)$ 是域，可知 $(\mathbb{Q},+)$ 和 $(\mathbb{Q}-\{0\},\times)$ 都是交換群，即所有有理數在加法下以及所有非零有理數在乘法下構成交換群。另一方面，由於 $(\mathbb{Z},+,\times)$ 是非域環，可知 $(\mathbb{Z},+)$ 是交換群，但 $(\mathbb{Z}-\{0\},\times)$ 卻不是群 (因為並非所有非零整數都有乘法逆元)。

請注意 $(\mathbb{Q}-\{0\},\times)$ 與 $(\mathbb{Z}-\{0\},\times)$ 的上述差異 (前者是群，後者卻不是) 也可以作如下解釋：在 $\mathbb{Q}$ 中，所有非零元素都是「單位」(即有乘法逆元的元素，詳見《感受伽羅瓦：因子分解》中的介紹)，但在 $\mathbb{Z}$ 中，並非所有非零元素都是「單位」，但如果僅考慮 $\mathbb{Z}$ 中的兩個單位 1 和 -1，那麼 $(\{1,-1\},\times)$ 卻構成群。由此可以作出推論，如果從一個帶乘法單位元的環中抽出所有單位，那麼由這些單位組成的集合連同該環的乘法運算便會構

成一個群，此一推論有助我們從帶乘法單位元的環中找出群。

接下來讓我們考慮以下特殊數系 $\mathbb{Z}_n$ (其中 n 是任意正整數，不一定是正質數)，即由 0、1、...、$n-1$ 組成的數系，其中的加法和乘法是模 n 同餘下的加法和乘法運算。容易看到 $\mathbb{Z}_n$ 的元素在加法下構成群，即 $(\mathbb{Z}_n, +)$ 是群。乘法的情況又如何？根據上段的討論，如果從 $\mathbb{Z}_n$ 中抽出所有單位並組成集合，記作 $U(n)$，那麼 $(U(n), \times)$ 是群，這種群稱為單位群(group of units)。

根據我們在《感受伽羅瓦：因子分解》中的討論 (見該網頁註 4)，$\mathbb{Z}_n$ 中的元素 a 是單位當且僅當 a 與 n 互質，因此 $U(n)$ 包含所有小於 n 且與 n 互質的正整數。舉例說，由於小於 10 且與 10 互質的正整數共有 1、3、7 和 9 這四個，所以 $U(10) = \{1, 3, 7, 9\}$。讀者可自行驗證，這四個元素在模 10 同餘下都有乘法逆元，分別是 1、7、3 和 9。此外，當 n 是正質數時，所有小於 n 的正整數都與 n 互質，$U(n)$ 因而包含 $\mathbb{Z}_n$ 中的所有非零成員，即 $U(n) = \mathbb{Z}_n - \{0\}$。舉例說，由於 11 是正質數，故知 $U(11) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$。讀者可自行驗證，這十個元素在模 11 同餘下都有乘法逆元，分別是 1、6、4、3、9、2、8、7、5 和 10。

從以上例子可見，一個群的運算在不同數學對象中可以體現為加法，也可以體現為乘法，這就是我們在上述定義中使用「中立」符號 $\circ$ 以代表群的運算的原因。事實上，由於群只包含一個運算，這個概念的應用範圍比環廣闊得多，其中一個應用範疇是函數(function)，即把函數看作一種數學對象，而複合(composition) 則可看作函數之間的二元運算，以下介紹一些例子。

我們在《感受伽羅瓦：排列與對稱多項式》中介紹了「排列」的概念，並指出給定集合 X，X 的排列就是 X 上的「一一到上」函數。舉例說，設 $X = \{A, B, C\}$，若沿用上述網頁介紹的「循環式」表示排列，那麼 $f = (AC)$ 和 $g = (BC)$ 便是 X 的兩個不同排列，這兩個排列是 X 上的函數，因為它們把 X 中的每個元素映射為另一元素，例如我們有 $f(A) = C$ 和 $g(A) = A$ 等。

由於排列本質上是函數，因而可以進行複合。複合的意思就是把某函數 f 先作用於定義域中某元素 x，得到中間結果 $f(x)$，然後再用函數 g 作用於此一中間結果，從而得到上述兩個函數複合的結果 $g(f(x))$。此一結果也可以看成把一個複合函數作用於 x 所得的結果，這個複合函數可稱為「先 f 後 g」，以下記作 $g \circ f$，即

$$g \circ f(x) = g(f(x))$$

請注意這裡把「先 f 後 g」記作 $g \circ f$，是為了使上式左右兩端 f 和 g 的出現次序一致。請記著在上式中由於 f 比 g 更靠近 x，所以是先用 f 作用於

x，然後再用 g 作用於 $f(x)$，這就是「先 f 後 g」的意思[1]。

以前述的排列 $f = (AC)$ 和 $g = (BC)$ 為例，考慮複合函數 $g \circ f$，我們可以求出這個複合函數作用於 X 中每個元素的結果。舉例說，由於有 $g(f(A)) = g(C) = B$，故有 $g \circ f(A) = B$。同樣也容易求得 $g \circ f(B) = C$ 和 $g \circ f(C) = A$，由此我們看到 $g \circ f$ 是一個排列，即 X 上的一一到上函數，把這個函數以循環式寫出來，便得到 $g \circ f = (ABC)$，撇除 f、g 等符號，也可以把以上結果寫成[2]

$$(BC) \circ (AC) = (ABC) \qquad (1)$$

現在如果把 $X = \{A, B, C\}$ 上的所有排列組成一個集合，並記作 S_3，那麼 S_3 包含以下 $3! = 6$ 個元素 (其中 (A) 代表「恆等排列」，即把 X 中每個元素映射為自身的函數)：

$$S_3 = \{(A), (AB), (AC), (BC), (ABC), (ACB)\}$$

介紹完上述這個由排列組成的集合以及排列之間的複合運算後，一個很自然的問題是，$(S_3, \circ)$ 是否構成一個群？現在讓我們解答這個問題。由於 S_3 包含 X 上所有可能排列，而 X 上任何兩個排列的複合必然也是 X 上的排列，因此 $\circ$ 是 S_3 上的封閉運算。接著看 $(S_3, \circ)$ 是否滿足前述的公理。

如要驗證公理 (i)，要進行繁重的計算，但幸好我們知道任何函數的複合運算都滿足結合性，因此無需計算也可斷定 $(S_3, \circ)$ 滿足公理 (i)。對於公理 (ii)，容易看到恆等排列 (A) 就是 $(S_3, \circ)$ 中的單位元。至於公理 (iii)，容易看到，每個排列的逆元的循環式就是把該排列的循環式中的字母顛倒次序寫出來所得的結果，例如 (AC) 的逆元就是 (CA)(這個排列也可寫作 (AC)，換句話說，(AC) 以自身作為逆元)。至此我們看到 $(S_3, \circ)$ 滿足公理 (i)-(iii)，所以是群。

$(S_3, \circ)$ 是否滿足公理 (iv)？為解答此問題，我們進行以下計算：

$$(AC) \circ (BC) = (ACB) \qquad (2)$$

綜合 (1) 和 (2) 中的計算結果，得 $(BC) \circ (AC) \neq (AC) \circ (BC)$，由此可知 $(S_3, \circ)$ 不滿足公理 (iv)，即 $(S_3, \circ)$ 不是交換群。

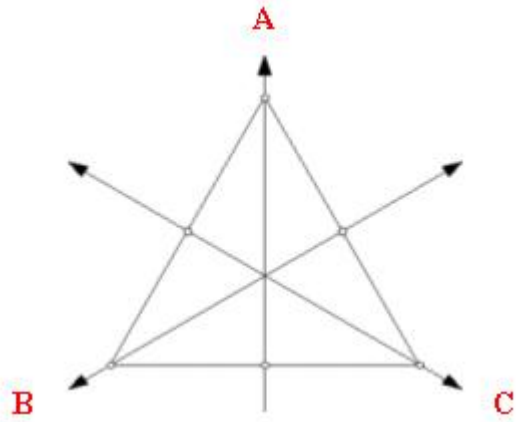
---

[1]有些學者覺得把「先 f 後 g」記作 $g \circ f$，似乎把 f 和 g 的次序顛倒了，因此主張把「把函數 f 作用於元素 x」記作 xf (而不是 $f(x)$)，這樣「先 f 後 g」便可以記作 $f \circ g$，但由於這種新記法與我們習慣的函數寫法大異，本文不予採納。

[2]請注意數學界對於用循環式表示排列的複合，有兩種截然相反的做法。以 (1) 為例，有些人把 (1) 理解為「先 (AC) 後 (BC)」，有些人則把 (1) 理解為「先 (BC) 後 (AC)」。本文採取前一種觀點，此一觀點跟我們把排列看成函數的觀點一致。

我們可以把上述例子推廣到一般情況，設 X 包含 n 個元素，我們把這 n 個元素的 $n!$ 種排列組成一個集合 S_n，那麼容易看到這個集合連同複合運算 $\circ$ 構成一個群 $(S_n, \circ)$。在抽象代數學上，這種群稱為n 次對稱群(symmetric group of degree n)[3]。

幾何圖形的變換在本質上也是函數，因而也可構成群。由於幾何變換種類繁多，這裡只介紹最簡單的正 n 邊形的幾何變換，即在變換後正 n 邊形形狀、大小不變且留於原位的變換，以下圖為例：



上圖顯示一個等邊三角形以及三條對稱軸，共有以下六種可使原圖形狀、大小不變且留於原位的變換，包括三種「旋轉」(rotation)：恆等變換 (identity transformation，記作 I，即不作任何變換，亦等同於逆時針旋轉 0°)、逆時針旋轉 120°(記作 R_{120})、逆時針旋轉 240°(記作 R_{240})，以及三種「反射」(reflection)：以通過三角形中上方頂點的軸為對稱軸的反射 (記作 R_{middle})、以通過三角形左下方頂點的軸為對稱軸的反射 (記作 R_{left})、以通過三角形右下方頂點的軸為對稱軸的反射 (記作 R_{right})。

由於上述變換是函數，它們可以進行複合。舉例說，容易看到逆時針旋轉 120°，然後再逆時針旋轉 240°，所得結果等同於沒有進行任何變換，此一結果可以寫成 $R_{240} \circ R_{120} = I$)。讀者可自行驗證，以通過中上方頂點的軸為對稱軸進行反射，然後再逆時針旋轉 120°，所得結果等同於以通過右下方頂點的軸為對稱軸進行反射，此一結果可以寫成 $R_{120} \circ R_{middle} = R_{right}$。

[3]請注意「對稱群」一名雖有「對稱」二字，但跟幾何圖形的對稱無關。事實上，在抽象代數學上，有一個稱為 symmetry group 的概念，才跟幾何圖形的對稱性有直接關係。為區別這兩者，有些人把 symmetry group 譯作「空間對稱群」。本文下文只會介紹「空間對稱群」的一個次類－「二面體群」，因此不會產生「對稱群」與「空間對稱群」相混淆的問題。

現在如果把上述六種變換組成一個集合，並記作 D_3，即

$$D_3 = \{I, R_{120}, R_{240}, R_{middle}, R_{left}, R_{right}\}$$

那麼不難看到 $(D_3, \circ)$ 構成一個群，這是因為這些變換中任何兩個的複合結果都是這六個變換中的一個 (即 $\circ$ 在 D_3 上封閉)，而且如前所述，函數的複合滿足公理 (i)。此外，也容易看到 I 是 D_3 中的單位元，而且 I、R_{middle}、R_{left} 和 R_{right} 都以自身作為逆元，而 R_{120} 與 R_{240} 則互為對方的逆元。另一方面，$(D_3, \circ)$ 不是交換群，這是因為我們有 $R_{120} \circ R_{middle} = R_{right}$ 和 $R_{middle} \circ R_{120} = R_{left}$，由此得 $R_{120} \circ R_{middle} \neq R_{middle} \circ R_{120}$，即 $(D_3, \circ)$ 不滿足公理 (iv)。

如果我們如上圖所示把等邊三角形的三個頂點位置命名為 A、B 和 C，那麼可以把上述變換看成把 $X = \{A, B, C\}$ 映射為 X 中另一成員的函數，即前述 S_3 的某個成員。請注意這裡的 A、B 和 C 是固定不變的位置標籤，變換記錄著三角形的三個頂點在變換前後的所在位置。舉例說，由於 R_{120} 的結果是把原在 A 的頂點送到 B，把原在 B 的頂點送到 C，並把原在 C 的頂點送到 A，R_{120} 相當於 S_3 中的成員 (ABC)，D_3 中的其他成員也各與 S_3 中的某個成員存在對應關係。事實上，由於 D_3 和 S_3 各有六個成員，這是一個一一對應關係，下表列出此一對應：

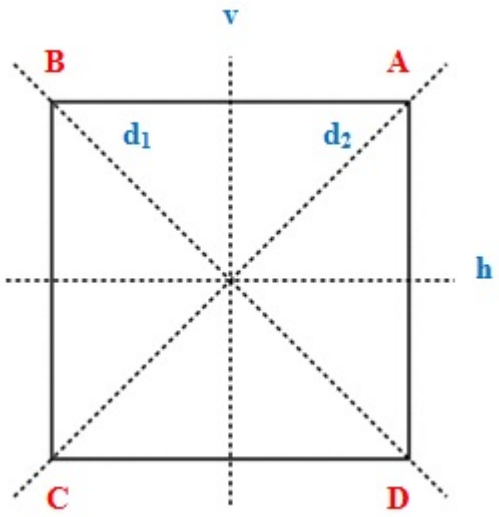
D_3 的成員	S_3 的成員
I	(A)
R_{120}	(ABC)
R_{240}	(ACB)
R_{middle}	(BC)
R_{left}	(AC)
R_{right}	(AB)

沿用我們在《感受伽羅瓦：環的同態與同構》) 中引入的術語，我們有 $D_3 \cong S_3$，即 D_3 與 S_3 同構。

我們可以把上述例子推廣到一般情況，設有正 n 邊形 (其中 $n \geq 3$)，我們把使這個平面圖形的形狀、大小不變且留於原位的變換，連同這些變換之間的複合運算 $\circ$ 組成一個群 $(D_n, \circ)$，這種群稱為$2n$ 階二面體群(dihedral group of order $2n$)。D_n 的每個成員由 $2n$ 種變換組成，其中包括 n 種旋轉和 n 種反射。正 n 邊形的 n 種旋轉包括逆時針旋轉 $\frac{360^\circ}{n}$ 的 0 倍、1 倍、...、$n-1$ 倍，其中的 0 倍旋轉相等於恆等變換 I。

若 n 是奇數，正 n 邊形的反射包括以該圖形的某個頂點與對邊中點的連線作為對稱軸的反射，由於正 n 邊形共有 n 個頂點，故共有 n 種反射。

若 n 是偶數，正 n 邊形的反射分為兩種，其中一半 (即共有 $\frac{n}{2}$ 種) 是以該圖形的某條邊的中點與對邊中點的連線作為對稱軸的反射，另外一半 (也共有 $\frac{n}{2}$ 種) 則是以該圖形的某個頂點與對角頂點的連線作為對稱軸的反射，以下圖為例：



上圖顯示一個正方形及其四條對稱軸：豎向的 v、橫向的 h 以及斜向的 d_1 和 d_2。類似上述等邊三角形的情況，容易看到 D_4 包含以下八個成員：

$$D_4 = \{I, R_{90}, R_{180}, R_{270}, R_v, R_h, R_{d_1}, R_{d_2}\}$$

現在如果如上圖所示把正方形的四個頂點位置命名為 A、B、C 和 D，那麼可以把上述變換看成把 $X = \{A, B, C, D\}$ 映射為 X 中另一成員的函數，即 S_4 的某個成員，例如 R_{90} 便相當於 S_4 中的成員 $(ABCD)$。但跟前述等邊三角形的情況不同，D_4 並不與 S_4 同構，這是因為 D_4 只有 $2 \times 4 = 8$ 個成員，而 S_4 卻有 $4! = 24$ 個成員。換句話說，S_4 中有很多成員並不對應正方形上的對稱變換，例如 (AB) 便並不對應任何對稱變換 (我們無法找到一個對稱變換可以只對調 A 和 B 而使 C 和 D 留於原位)。這個例子顯示儘管 $D_3 \cong S_3$，但當 $n > 3$ 時，D_n 與 S_n 是各不相同的群。

接下來介紹與群有關的一些重要概念，首先介紹階(order) 的概念。給定群 $(G, \circ)$，G 所含元素的個數稱為這個群的階，記作 $|G|$。回顧前面的例子，我們有 $|Z_n| = n$、$|U(n)| = \phi(n)$、$|S_n| = n!$ 和 $|D_n| = 2n$[4]，其中 $\phi(n)$ 是數論上的「歐拉總計函數」(Euler's totient function)，這個函數就每個正整數 n 提供小於 n 且與 n 互質的正整數的數目，例如 $\phi(10) = 4$、$\phi(11) = 10$

[4]這就是 $(D_n, \circ)$ 稱為「$2n$ 階二面體群」的原因。

等[5]。此外，我們也知道 $(\mathbb{Z},+)$、$(\mathbb{Q}-\{0\},\times)$ 等是無限階群。

「階」的概念除適用於整個群外，也適用於群的元素。為方便以下定義，現先引入群的「(抽象) 冪次」的概念及其簡記法，設 a 為群 $(G,\circ)$ 的元素，我們把 $a\circ a$ 簡記作 a^2，並且一般地，把 $a\circ\cdots\circ a$ (這裡共有 n 個 a，其中 n 是正整數) 簡記作 a^n。這裡借用了一般乘法的「冪次」概念及其「指數」記法，照此類推，我們也可以把群 $(G,\circ)$ 的單位元 e 記作 a^0，並把 a 的逆元記作 a^{-1}，而 a^{-n} (其中 n 是正整數) 既可以理解為 a^n 的逆元，即 $(a^n)^{-1}$；又可理解為 $a^{-1}\circ\cdots\circ a^{-1}$ (共有 n 個 a^{-1})，即 $(a^{-1})^n$。

但請注意就特定的群 $(G,\circ)$ 而言，有關運算 $\circ$ 可能是我們習用的加法，這時便要小心理解上述簡記法。舉例說，對 $(\mathbb{Z},+)$ 而言，設 $a\in\mathbb{Z}$ 並且 n 是正整數，那麼 $a\circ\cdots\circ a$ 實際等於 $a+\cdots+a$，因此 a^n 實際等於 na，a^0 實際等於 0，a^{-n} 實際等於 $-na$ 等等。

利用上述簡記法，我們可以作如下定義。設 a 為群 $(G,\circ)$ 中的元素，則 a 的階就是使 a^n 等於 $(G,\circ)$ 中單位元的最小正整數 n，如不存在這樣的正整數，便說 a 有無限階，以下把 a 的階記作 $\mathrm{Ord}(a)$。以前述的二面體群 $(D_4,\circ)$ 中的元素 R_{90} 為例，容易看到 ${R_{90}}^1=R_{90}$，${R_{90}}^2=R_{180}$，${R_{90}}^3=R_{270}$，${R_{90}}^4=I$，因此使 ${R_{90}}^n=I$ 的最小正整數是 4，故有 $\mathrm{Ord}(R_{90})=4$。另外又如在 $(\mathbb{Q}-\{0\},\times)$ 中，由於 $1^1=1$，所以 $\mathrm{Ord}(1)=1$；又由於 $(-1)^2=1$，所以 $\mathrm{Ord}(-1)=2$；對於其他非零有理數 a，由於沒有正整數 n 可以使 $a^n=1$，所以這些非零有理數都有無限階。

由此還可以定義一種特殊的群—循環群(cyclic group)。設 $(G,\circ)$ 為群，如果存在一個 $a\in G$，使 $G=\{a^n:n\in\mathbb{Z}\}$，即 G 中每個元素都是 a 的某個冪次 (包括正冪次、零冪次和負冪次)，則稱 $(G,\circ)$ 為循環群，而 a 則是這個群的生成元(generator)。為了突出 a 生成整個循環群的作用，也可以把 $\{a^n:n\in\mathbb{Z}\}$ 寫成 $\langle a\rangle$ 的形式，即 $(G,\circ)$ 是循環群，當且僅當存在 a 使得 $G=\langle a\rangle$[6]。

以下提供循環群的一些例子。我們知道 $(\mathbb{Z},+)$ 是循環群，它有兩個生成元：1 和 -1，這是因為任何整數都可表示為 1 或 -1 的整數倍 (請注意群的 (抽象) 冪次在 $(\mathbb{Z},+)$ 中體現為倍數)，即 $\mathbb{Z}=\langle 1\rangle=\langle -1\rangle$。請注意上述結果也適用於 $(\mathbb{Z}_n,+)$，即對任何正整數 n 而言，$(\mathbb{Z}_n,+)$ 都是循環群，其生成元至少有 1 和 -1，這裡的 -1 是指 $\mathbb{Z}_n$ 中與 -1 同餘的元素。

[5]數論上有一條求歐拉總計函數的值的公式，由於此公式與本文的討論沒有直接關係，這裡不作介紹。

[6]「循環群」與「主理想」(見《感受伽羅瓦：子環與商環》的介紹) 一樣，都用角括號 $\langle\rangle$ 表示。這兩個概念的定義雖然有很大差異，但有一個共同點，就是都由一個元素生成。在抽象代數學中，角括號 $\langle\rangle$ 常用來表示由某些元素「生成」的集合。

以 $\mathbb{Z}_{10}$ 為例, 由於 9 在模 10 下與 -1 同餘, 我們知道 9 是 $\mathbb{Z}_{10}$ 的生成元之一。

不過，$(\mathbb{Z}_n, +)$ 在很多情況不只有兩個生成元，因為我們有以下定理。

定理 1：整數 k 是 $(\mathbb{Z}_n, +)$ 中的生成元當且僅當 n 與 k 互質, 即 $\gcd(n, k) = 1$。

以 $\mathbb{Z}_{10}$ 為例, 由於 $\mathbb{Z}_{10}$ 中與 10 互質的元素共有 1、3、7 和 9 這四個, 根據上述定理, 可知這四個元素都是 $\mathbb{Z}_{10}$ 的生成元, 即 $\mathbb{Z}_{10} = \langle 1\rangle = \langle 3\rangle = \langle 7\rangle = \langle 9\rangle$。為驗證上述結果, 以下列出上述四個整數在 $\mathbb{Z}_{10}$ 中的各個倍數 (請注意群的 (抽象) 冪次在 $(\mathbb{Z}_n, +)$ 中體現為倍數)：

k	1	3	7	9
$2k$	2	6	4	8
$3k$	3	9	1	7
$4k$	4	2	8	6
$5k$	5	5	5	5
$6k$	6	8	2	4
$7k$	7	1	9	3
$8k$	8	4	6	2
$9k$	9	7	3	1
$10k$	0	0	0	0

上表的第二至第五欄都齊備 $\mathbb{Z}_{10}$ 中的十個元素：0、1、2、3、4、5、6、7、8 和 9，由此可見 1、3、7 和 9 的確能各自生成 $\mathbb{Z}_{10}$ 中的所有元素。

與有限階循環群相關的還有以下定理。

定理 2：設 $(G, \circ) = \langle a\rangle$ 並且 $|G| = n$, 則 $\langle a\rangle = \langle a^k\rangle$ 當且僅當 $\gcd(n, k) = 1$。

利用上述定理，我們可以從某循環群的某一個生成元推導出其他生成元。以 $\mathbb{Z}_{10}$ 為例，我們知道 1 是這個循環群的生成元，由於 $|\mathbb{Z}_{10}| = 10$，而小於 10 且與 10 互質的正整數共有 1、3、7 和 9 這四個，根據上述定理，可知 3、7 和 9 也是 $\mathbb{Z}_{10}$ 的生成元，此一結果與前面的討論完全吻合。

在上例中，我們不一定要從 1 推導出其他生成元，也可以從 3、7 和 9 中任何一個推導出其他生成元。舉例說，若給定 9 是 $\mathbb{Z}_{10}$ 的生成元之一，那麼由於 1、3、7 和 9 與 10 互質，根據上述定理 (請注意群的 (抽象) 冪次在 $(\mathbb{Z}_n, +)$ 中體現為倍數)，可知 $3 \times 9 \equiv_{10} 7$、$7 \times 9 \equiv_{10} 3$ 和 $9 \times 9 \equiv_{10} 1$ 也是 $\mathbb{Z}_{10}$ 的生成元，同樣可得出上述結果。

最後考慮 $(U(10), \times)$，其中 $U(10) = \{1, 3, 7, 9\}$，並且 $|U(10)| = 4$。不難證明 $(U(10), \times)$ 是循環群，其中一個生成元是 3。由於當 $k = 1$ 或 3 時，$\gcd(4, k) = 1$，但當 $k = 2$ 或 4 時，$\gcd(4, k) \neq 1$，根據上述定理，我們知道在 $U(10)$ 中，$3^1 \equiv_{10} 3$ 和 $3^3 \equiv_{10} 7$ 是生成元，而 $3^2 \equiv_{10} 9$ 和 $3^4 \equiv_{10} 1$ 則不是生成元。為驗證上述結果，以下列出上述四個整數在模 10 下的各個冪次：

k	3	7	9	1
k^2	9	9	1	1
k^3	7	3	9	1
k^4	1	1	1	1

在上表中，只有第二和第三欄齊備 $U(10)$ 的四個元素：1、3、7 和 9，由此可見的確只有 3 和 7 能生成 $U(10)$ 的所有元素。

連結至數學專題
連結至周家發網頁