Lecture 4
Finite Fields

Jason Lin

學習目標

- 回顧代數結構的概念
- 定義「群」並使用範例解說
- 定義「環」並使用範例解說
- 定義「體」並使用範例解說
- 強調在現代區塊加密法中對 n 位元做加減乘除運算的能力來自於由 $GF(2^n)$ 所構成的有限體 (Finite Field)

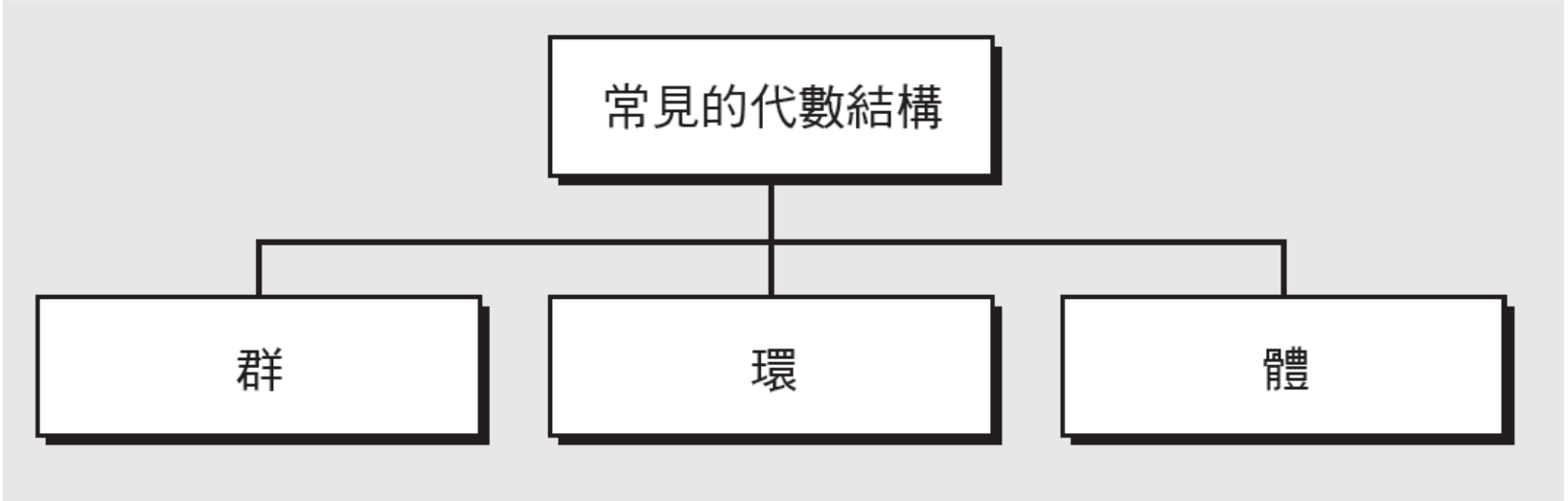
4.1 代數結構

- 密碼學需要整數集以及定義這些集合的特定運算式，這些集合以及對集合元素所進行的運算合稱為代數結構 (Algebraic Structure)
- 本章我們將要定義群 (Group)、環 (Ring)、體 (Field) 等三個常用的代數結構

4.1 代數結構 (續)

- 本節討論主題：
  - 群 (Group)
  - 環 (Ring)
  - 體 (Field)

圖 4.1 常見的代數結構



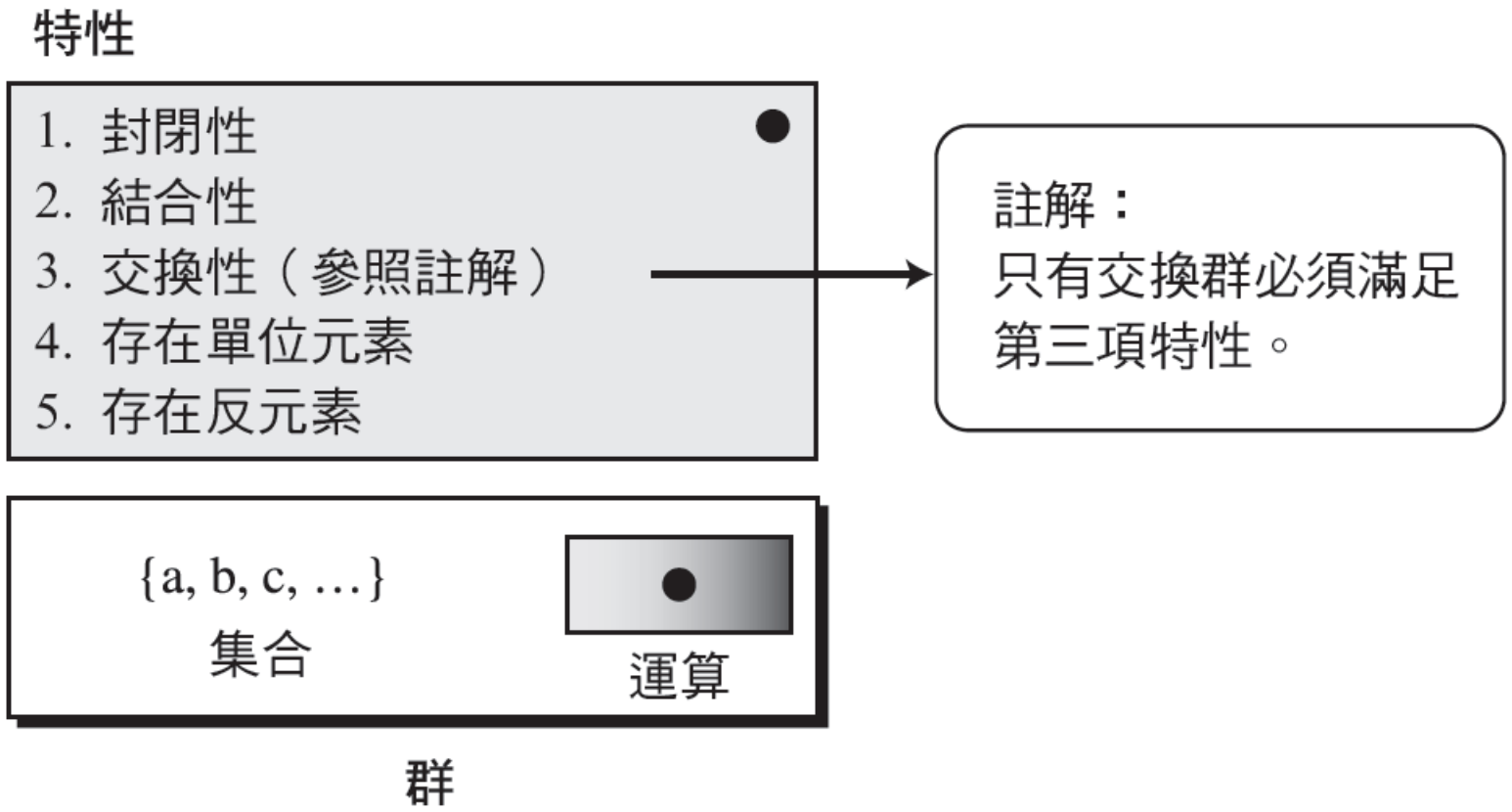
4.1.1 群

- 群（Group）是一個元素的集合和一個二元運算子「$\bullet$」的結合，滿足以下四種特性（或稱公理）。
  - 封閉性 (Closure)：對於所有集合 G 中的元素 a 和 b，運算 $a \bullet b$ 的結果也在 G 中。
  - 結合性 (Associativity)：對於所有集合 G 中的元素 a、b 和 c，等式 $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ 成立。
  - 存在單位元素 (Identity Element)：存在集合 G 中的一個元素 e，使得對於所有 G 中的元素 a，等式 $e \bullet a = a \bullet e = a$ 成立。
  - 存在反元素 (Inverse Element)：對於集合 G 中的每個元素 a，存在一個 G 中的元素 b，使得 $a \bullet b = b \bullet a = e$，其中這裡的 e 是單位元素。

4.1.1 群 (續)

- 一個交換群（Commutative Group，或稱為 Abelian Group），除了滿足群的四個特性之外，還有以下一個額外的特性。
  - 交換性 (Commutative)：對於集合 G 中所有的元素 a 和 b，皆滿足等式 $a \bullet b = b \bullet a$ 。

圖4.2 群


特性
1. 封閉性
2. 結合性
3. 交換性（參照註解）
4. 存在單位元素
5. 存在反元素
註解：
只有交換群必須滿足第三項特性。
{a, b, c, …}
集合
運算
群

應用

- 雖然一個群只有單一的運算子，但是這個運算子受到群的特性影響，使得一個群可以有一對互為逆運算的運算子。

範例 4.1

- 整數餘數集合與加法運算子

$$G = < Z_n, + >$$

為一交換群，我們可以對此集合的元素 執行加法與減法的運算，而結果仍為此集合的元素。

範例 4.2

- 集合 Z_{n^*} 與乘法運算子可構成一交換群

$$G = < Z_{n^*}, \times >$$

範例 4.3

- 以下定義一個群 G = <{*a*, *b*, *c*, *d*}, •>，其運算如表 4.1 所示。

•	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*c*	*d*	*a*
c	*c*	*d*	*a*	*b*
d	*d*	*a*	*b*	*c*

範例 4.4

- 排列群（Permutation Group）是一個很有意思的例子，這個集合是所有排列方式的集合，其運算是可合成（Compositional）的：先進行一種排列，之後再進行另一種排列。

圖 4.3 排列運算的合成（範例 4.4）

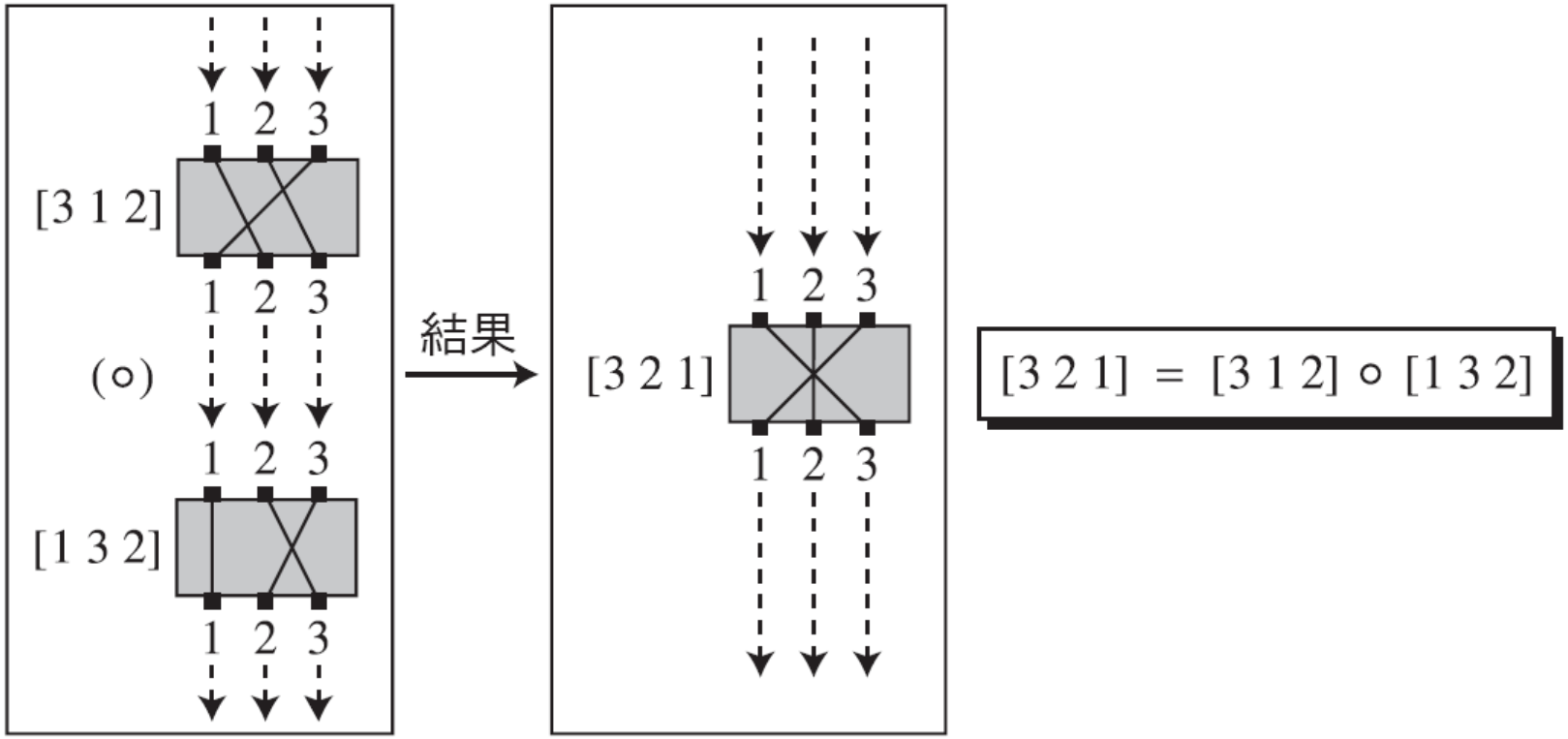


表 4.2 排列群的運算表

		1st					
	∘	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
	[1 2 3]	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
	[1 3 2]	[1 3 2]	[1 2 3]	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
2nd	[2 1 3]	[2 1 3]	[3 1 2]	[1 2 3]	[3 2 1]	[1 3 2]	[2 3 1]
	[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	[1 2 3]	[2 1 3]
	[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	[1 2 3]	[2 3 1]	[1 3 2]
	[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 1 3]	[1 2 3]

範例 4.5

- 在前一個範例中，我們將一組排列方式加上合成運算就成為一個群。這裡隱含的意思是使用兩個連續的排列方式並不能提升加密法的安全度，我們必定可以找到一個排列方式，其效果相當於兩個排列方式的合成，因為這是群的封閉性。

4.1.1 群 (續)

- 有限群 (Finite Group)
- 群的秩 (Rank of a Group)
- 子群 (Subgroup)

範例 4.6

- 群 $H = < Z_{10}, + >$ 是否為 $G = < Z_{12}, + >$ 的子群？
- 解法：答案是否定的。雖然 H 是 G 的子集合，但是這兩個群所定義的運算子並不相同。H 的運算子是模數為 10 的加法，而 G 的運算子是模數為 12 的加法。

循環子群

- 若一個子群的每一個元素都是另一個群中某一個元素的乘冪，則此子群稱為循環子群（Cyclic Subgroup），這裡乘冪的意思是重複對這個元素引用群運算：

$$a^n \rightarrow a \bullet a \bullet \cdots \bullet a\ (n\ 次)$$

範例 4.7

- 群 $G = < Z_6, + >$ 可以產生四個循環子群，分別是 $H_1 = < \{0\}, + >$、$H_2 = < \{0, 2, 4\}, + >$、$H_3 = < \{0, 3\}, + >$ 和 $H_4 = G$。

$0^0 \bmod 6 = 0$

$1^0 \bmod 6 = 0$
$1^1 \bmod 6 = 1$
$1^2 \bmod 6 = (1 + 1) \bmod 6 = 2$
$1^3 \bmod 6 = (1 + 1 + 1) \bmod 6 = 3$
$1^4 \bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4$
$1^5 \bmod 6 = (1 + 1 + 1 + 1 + 1) \bmod 6 = 5$

$2^0 \bmod 6 = 0$
$2^1 \bmod 6 = 2$
$2^2 \bmod 6 = (2 + 2) \bmod 6 = 4$

$3^0 \bmod 6 = 0$
$3^1 \bmod 6 = 3$

$4^0 \bmod 6 = 0$
$4^1 \bmod 6 = 4$
$4^2 \bmod 6 = (4 + 4) \bmod 6 = 2$

$5^0 \bmod 6 = 0$
$5^1 \bmod 6 = 5$
$5^2 \bmod 6 = 4$
$5^3 \bmod 6 = 3$
$5^4 \bmod 6 = 2$
$5^5 \bmod 6 = 1$

範例 4.8

- 從群 $G = <Z_{10^*}, \times>$ 中產生的三個循環子群只有四個元素：1、3、7 和 9。這些循環子 群分別是 $H_1 = <\{1\}, \times>$、$H_2 = <\{1, 9\}, \times>$ 和 $H_3 = G$。

$1^0 \bmod 10 = 1$

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$
$3^2 \bmod 10 = 9$
$3^3 \bmod 10 = 7$

$7^0 \bmod 10 = 1$
$7^1 \bmod 10 = 7$
$7^2 \bmod 10 = 9$
$7^3 \bmod 10 = 3$

$9^0 \bmod 10 = 1$
$9^1 \bmod 10 = 9$

循環群

- 若一個群為本身的循環子群，或者說本身能由其單個元素所生成，則稱為循環群（Cyclic Group）。
  - 令 g 為一個循環群 G 的生成子（Generator），則 $G = \{e, g, g^2, \ldots, g^{n-1}\}$，其中 $g^n = e$。
- 每個循環群都是 Abelian Group，滿足運算的交換性。

範例 4.9

- 群 $\boldsymbol{G} = < \boldsymbol{Z}_6, + >$ 為一個含兩個生成子 $g = 1$ 和 $g = 5$ 的循環群。
- 群 $\boldsymbol{G} = < \boldsymbol{Z}_{10^*}, \times >$ 為一個含兩個生成子 $g = 3$ 和 $g = 7$ 的循環群。

元素的階

- 所謂元素的階 (Order) 就是這個元素所生成之循環群的基數 (Cardinality)，也就是其元素的個數。
- 一個群 G 的秩 (Rank)，是 G 的各個生成集合中最小的基數，也就是 $rank(G) = \min\{|H| : H \subseteq G, \langle H \rangle = G\}$。
- $rank(G) = 1$ if and only if G 是一個循環群。

Lagrange 定理

- 假設有一群 G，H 為其子群 $(H \subseteq G)$，令 G 和 H 的秩分別為 $|G|$ 和 $|H|$。根據 Lagrange 定理，$|H|$ 會整除 $|G|$，見範例 4.10。

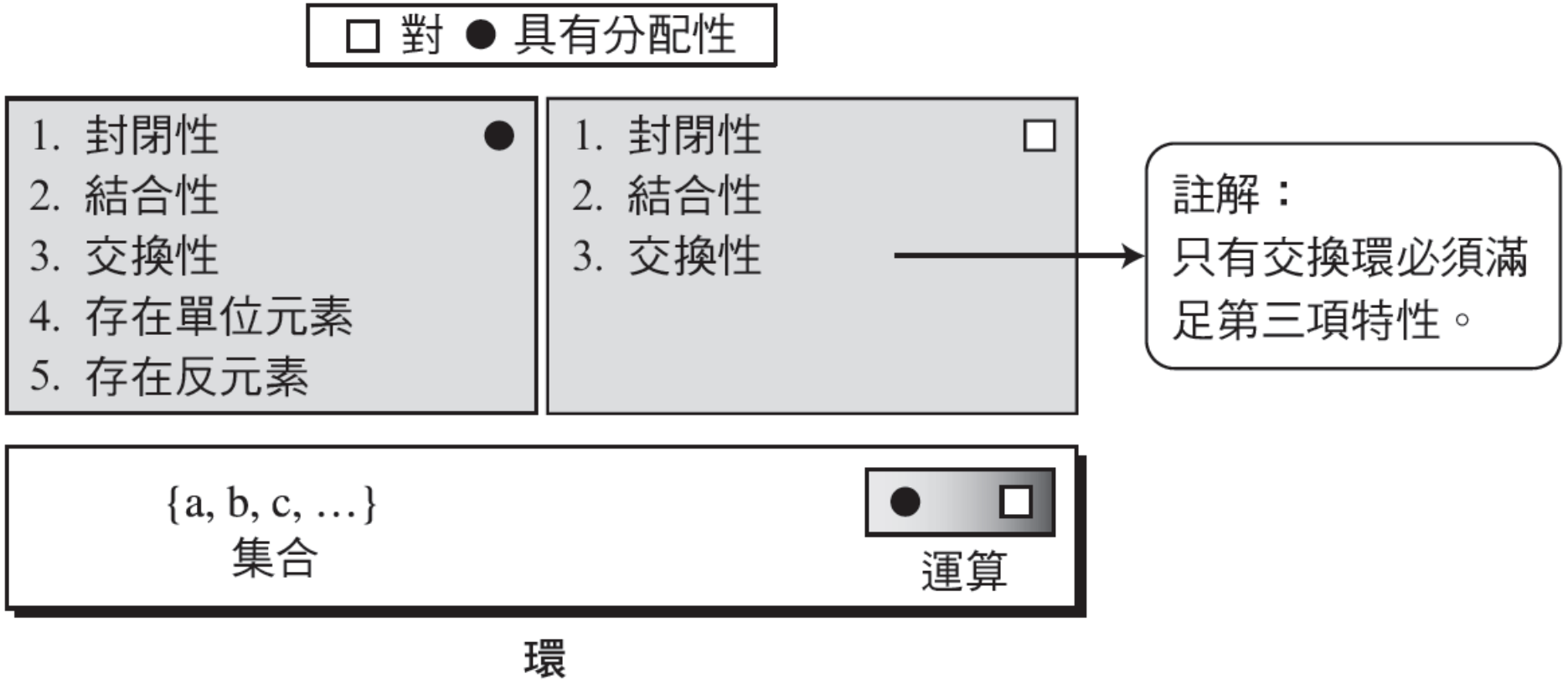
範例 4.10

- 在群 $G = < Z_6, + >$ 中，個別元素的階 (Order) 為：$ord(0) = 1$，$ord(1) = 6$，$ord(2) = 3$，$ord(3) = 2$，$ord(4) = 3$，$ord(5) = 6$。
- 在群 $G = < Z_{10^*}, \times >$ 中，個別元素的階為：$ord(1) = 1$，$ord(3) = 4$，$ord(7) = 4$，$ord(9) = 2$。

4.1.2 環

- 環（Ring）是由一個集合和兩種二元運算所構成的代數結構，記作 **R** = <{…}, •, □>

圖 4.4 環


□ 對 ● 具有分配性
1. 封閉性 ●
2. 結合性
3. 交換性
4. 存在單位元素
5. 存在反元素
1. 封閉性 □
2. 結合性
3. 交換性
註解：
只有交換環必須滿足第三項特性。
{a, b, c, …}
集合
● □
運算
環

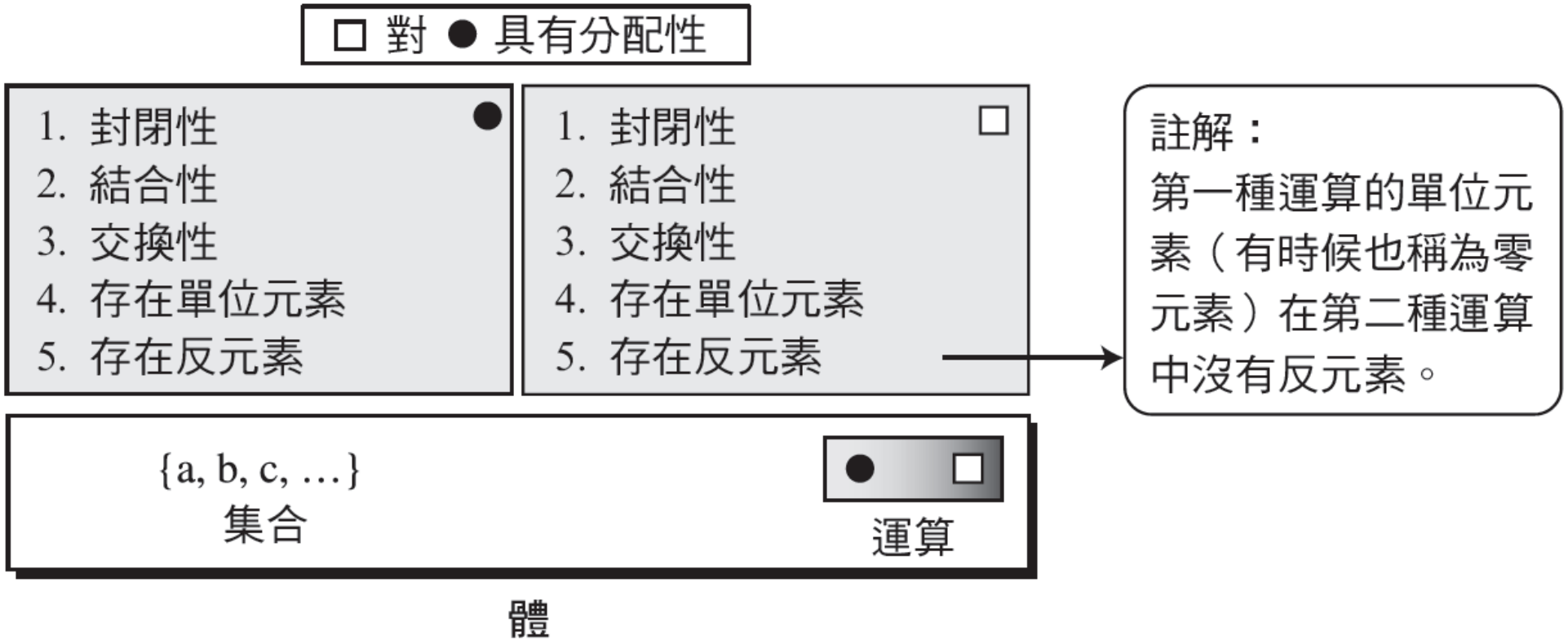
範例 4.11

- 集合 Z 內含加法與乘法兩種運算，為一交換環（Commutative Ring）。
- 我們可以證明 $R = < Z, +, \times >$，其中加法滿足全部五項特性，而乘法僅滿足三項特性。

4.1.3 體

- 體（Field），記為 **F** = <{…}, •, □ >，為一交換環，其中第二種運算能夠滿足和第一種運算一樣的五項特性，唯一的例外是第一種運算的單位元素（有時候也稱為零元素）在第二種運算中沒有反元素。

圖4.5 體


□ 對 ● 具有分配性
1. 封閉性
2. 結合性
3. 交換性
4. 存在單位元素
5. 存在反元素
●
1. 封閉性
2. 結合性
3. 交換性
4. 存在單位元素
5. 存在反元素
□
註解：
第一種運算的單位元素（有時候也稱為零元素）在第二種運算中沒有反元素。
{a, b, c, …}
集合
● □
運算
體

有限體

- 蓋洛瓦（Galois）證明，如果一個體為有限體（Finite Field），則其元素個數為 p^n，其中 p 為質數且 n 為正整數。

注意

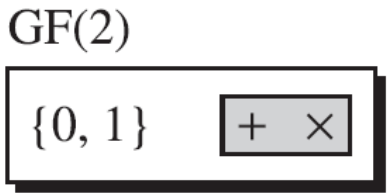
蓋洛瓦體 $GF(p^n)$ 是一個有限體，內含有限 p^n 個元素，亦稱為其 Order。

$GF(p)$ 體

- 當 $n = 1$ 時，我們得到 $\boldsymbol{GF}(p)$ 體。這個體可以是集合 $\boldsymbol{Z}_p = \{0, 1, \ldots, p-1\}$，內含兩種算術運算（加法與乘法）。

範例 4.12

- 在這一類中很常用到的體是 $\boldsymbol{GF}(2)$，集合為 $\{0, 1\}$，內含加法與乘法兩種運算，參考圖 4.6。



+	0	1
0	0	1
1	1	0

加法

×	0	1
0	0	0
1	0	1

乘法

a	0	1
$-a$	0	1

a	0	1
a^{-1}	—	1

反元素

範例 4.13

- 我們從集合 $\boldsymbol{Z_5}$（5 是質數）可以定義出內含加法與乘法運算子的 $\boldsymbol{GF}(5)$，見圖 4.7。

GF(5)

{0, 1, 2, 3, 4} + ×

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

加法

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

乘法

加法反元素

a	0	1	2	3	4
$-a$	0	4	3	2	1

a	0	1	2	3	4
a^{-1}	—	1	3	2	4

乘法反元素

表 4.3 代數結構總整理

代數結構	所支援的典型運算	所支援的典型整數集合
群	$(+\ -)$ 或 $(\times\ \div)$	$\mathbf{Z}_n$ 或 $\mathbf{Z}_n{}^*$
環	$(+\ -)$ 與 $(\times)$	$\mathbf{Z}$
體	$(+\ -)$ 與 $(\times\ \div)$	$\mathbf{Z}_p$

4.2 $GF(2^n)$ 體

- 在密碼學中，我們常常要用到加減乘除等四則運算。也就是說，我們需要用到體的概念，然而在電腦中正整數是以 n 位元字組的型態儲存。

4.2 $GF(2^n)$ 體 (續)

- 本節討論主題
  - 多項式 (Polynomial)
  - 使用生成子 (Generator)
  - 結語

範例 4.14

- 我們來定義 $\boldsymbol{GF}(2^2)$ 這個體，其集合由 2 位元字組所組成：{00, 01, 10, 11}。我們為這個體重新定義加法和乘法，使得這些特性都能滿足，見圖 4.8 為例。

圖 4.8 $GF(2^2)$ 體的例子

加法

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

單位元素：00

乘法

⊗	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

單位元素：01

4.2.1 多項式

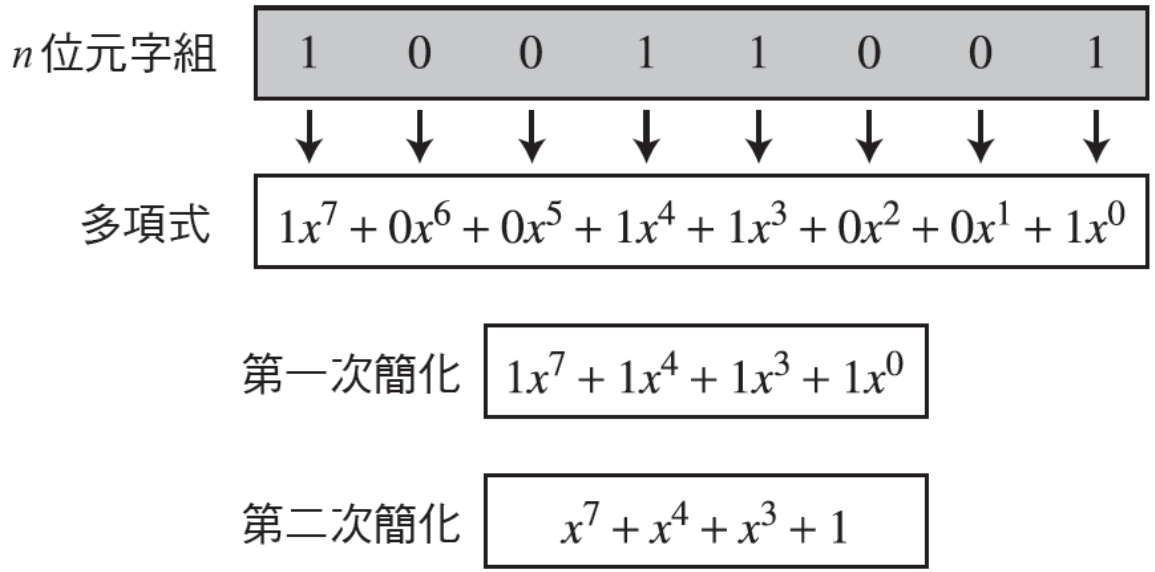
- 一個 $n-1$ 階的多項式通常寫成

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

其中，x^i 稱為第 i 項，而 a_i 則稱為第 i 項的係數。

範例 4.15

- 圖 4.9 說明如何使用多項式來表示一個 8 位元的字組 (10011001)。



範例 4.16

- 要找出多項式 $x^5 + x^2 + x$ 所代表的 8 位元字組，首先要將省略的項加以還原。因為 $n = 8$，所以多項式的階數為 7。還原後的多項式為

$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0$$

所以這個 8 位元字組為 00100110。

運算

注意

用來表示 n 位元字組的多項式使用兩個體：$GF(2)$ 和 $GF(2^n)$ 。

模多項式

- 對於在 $\boldsymbol{GF}(2^n)$ 的多項式，我們定義了一組 n 階的模多項式（Modulo Polynomial）。這些模多項式在這裡被當作質多項式（Prime Polynomial），意思就是集合中沒有任何一個多項式可以將之整除。質多項式不能被分解成 n 階以下的多項式，所以又稱為不可分解多項式（Irreducible Polynomial）。

表 4.4 不可分解多項式列表

階數	不可分解多項式
1	$(x+1)$, (x)
2	(x^2+x+1)
3	(x^3+x^2+1), (x^3+x+1)
4	$(x^4+x^3+x^2+x+1)$, (x^4+x^3+1), (x^4+x+1)
5	(x^5+x^2+1), $(x^5+x^3+x^2+x+1)$, $(x^5+x^4+x^3+x+1)$, $(x^5+x^4+x^3+x^2+1)$, $(x^5+x^4+x^2+x+1)$

加法

注意

對多項式而言，加法和減法是完全相等的運算。

範例 4.17

- 現在我們在 $\boldsymbol{GF}(2^8)$ 下執行 $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$。我們在這裡使用⊕符號來代表多項式的加法。加法程序如下：

$$
\begin{array}{l}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 \quad \oplus \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 \\
\hline
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 \quad \rightarrow \quad x^5 + x^3 + x + 1
\end{array}
$$

範例 4.18

- 還有另外一種速解。因為在 $\boldsymbol{GF}(2)$ 下的加法相當於 XOR 運算，所以可以直接將兩個字組做位元的 XOR 運算而得到相同的結果。以上一個範例來說，$x^5 + x^2 + x$ 相當於 00100110，而 $x^3 + x^2 + 1$ 相當於 00001101。

乘法

- 係數是在 $\boldsymbol{GF}(2)$ 下執行乘法。
- x^i 乘以 x^j 就得到 x^{i+j} 。
- 相乘的結果階數可能會超過 $n-1$，所以必須除以模多項式取其餘式。

範例 4.19

- 計算在 $\boldsymbol{GF}(2^8)$ 下 $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ 的結果，不可分解多項式為 $(x^8 + x^4 + x^3 + x + 1)$。這裡我們用 $\otimes$ 符號來代表兩個多項式相乘。
- 解法

$$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$
$$P_1 \otimes P_2 = x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2$$
$$P_1 \otimes P_2 = (x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1$$

要得到最後的結果，必須將相乘後的 12 階多項式除以 8 階的模多項式，然後得到餘式。這個 過程也和代數的作法相同，但是要記住現在加法和減法的結果相同。圖 4.10 是除法的過程。

圖 4.10 係數在 $GF(2)$ 之下的多項式除法

$$
\begin{array}{r}
 & x^4 + 1 \\
\hline
x^8 + x^4 + x^3 + x + 1 \;\big| & x^{12} + x^7 + x^2 \\
 & x^{12} + x^8 + x^7 + x^5 + x^4 \\
\hline
 & x^8 + x^5 + x^4 + x^2 \\
 & x^8 + x^4 + x^3 + x + 1 \\
\hline
\text{餘式} & \boxed{x^5 + x^3 + x^2 + x + 1}
\end{array}
$$

範例 4.20

- 在 $\boldsymbol{GF}(2^4)$ 下，找出多項式 (x^2+1) 對模多項式 (x^4+x+1) 的乘法反元素。
- 解法：答案為 (x^3+x+1)，如下表所示。

q	r_1	r_2	r	t_1	t_2	t
(x^2+1)	(x^4+x+1)	(x^2+1)	(x)	(0)	(1)	(x^2+1)
(x)	(x^2+1)	(x)	(1)	(1)	(x^2+1)	(x^3+x+1)
(x)	(x)	(1)	(0)	(x^2+1)	(x^3+x+1)	(0)
	(1)	(0)		(x^3+x+1)	(0)	

範例 4.21

- 在 $\boldsymbol{GF}(2^8)$ 下，找出 (x^5) 模 $(x^8 + x^4 + x^3 + x + 1)$ 的反元素。
- 解法：答案為 $(x^5 + x^4 + x^3 + x)$，如下表所示。

q	r_1	r_2	r	t_1	t_2	t
(x^3)	$(x^8 + x^4 + x^3 + x + 1)$	(x^5)	$(x^4 + x^3 + x + 1)$	(0)	(1)	(x^3)
$(x + 1)$	(x^5)	$(x^4 + x^3 + x + 1)$	$(x^3 + x^2 + 1)$	(1)	(x^3)	$(x^4 + x^3 + 1)$
(x)	$(x^4 + x^3 + x + 1)$	$(x^3 + x^2 + 1)$	(1)	(x^3)	$(x^4 + x^3 + 1)$	$(x^5 + x^4 + x^3 + x)$
$(x^3 + x^2 + 1)$	$(x^3 + x^2 + 1)$	(1)	(0)	$(x^4 + x^3 + 1)$	$(x^5 + x^4 + x^3 + x)$	(0)
	(1)	(0)		$(x^5 + x^4 + x^3 + x)$	(0)	

使用電腦執行乘法運算

- 在電腦上實作時會使用另一個較好的演算法，它將一個已經分解的多項式重複乘上 x。

範例 4.22

- 計算在 $\boldsymbol{GF}(2^8)$ 下，$P_1 = (x^5 + x^2 + x)$ 乘以 $P_2 = (x^7 + x^4 + x^3 + x^2 + x)$ 的結果，使用不可分解多項式 $(x^8 + x^4 + x^3 + x + 1)$。
- 解法：計算的過程列在表 4.7，我們先分別算出 x^0、x^1、x^2、x^3、x^4 以及 x^5 乘以 P_2 的結果。可以在表中看到，雖然只需要三項，我們還是把 $x^m \otimes P_2$ 的乘積從 $m = 0$ 算到 $m = 5$，這是因為每一項乘積計算都要用到前一項的結果。

表 4.7　一個較有效率的多項式乘法演算法（範例 4.22）

階數	運算	新的結果	是否化約
$x^0 \otimes P_2$		$x^7 + x^4 + x^3 + x^2 + x$	否
$x^1 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x^5 + x^2 + x + 1$	**是**
$x^2 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x^2 + x + 1)$	$x^6 + x^3 + x^2 + x$	否
$x^3 \otimes P_2$	$\boldsymbol{x} \otimes (x^6 + x^3 + x^2 + x)$	$x^7 + x^4 + x^3 + x^2$	否
$x^4 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2)$	$x^5 + x + 1$	**是**
$x^5 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x + 1)$	$x^6 + x^2 + x$	否
$\mathbf{P_1 \times P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			

範例 4.23

- 將範例 4.22 的計算用 8 位元的字組重做一次。
- 解法：現在，令 $P_1 = 00100110$，$P_2 = 10011110$，模數為 100011011（9 個位元）。符號 $\oplus$ 代表 XOR 的運算，見表 4.8。

表 4.8 用 n 位元字組做乘法運算的快速演算法

階數	位元左移	XOR 運算
$x^0 \otimes P_2$		10011110
$x^1 \otimes P_2$	00111100	(00111100) $\oplus$ (00011011) = **00100111**
$x^2 \otimes P_2$	01001110	**01001110**
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	00111000	(00111000) $\oplus$ (00011011) = 00100011
$x^5 \otimes P_2$	01000110	**01000110**
$P_1 \otimes P_2$ = (00100111) $\oplus$ (01001110) $\oplus$ (01000110) = 00101111		

範例 4.24

- $\boldsymbol{GF}(2^3)$ 的體共有 8 個元素。
- 以下我們用不可分解多項式 $(x^3 + x^2 + 1)$ 列出這個體的加法和乘法表。該表同時列出 3 位元字組以及多項式的表示法。
- 要注意的是，3 階多項式一共有兩個 不可分解多項式，另一個式子 $(x^3 + x + 1)$ 會得到完全不同的乘法表。
- 表 4.9 列出所有的加法運算。

表 4.9 $GF(2^3)$下的加法表

⊕	000 (0)	001 (1)	010 (x)	011 ($x+1$)	100 (x^2)	101 x^2+1	110 (x^2+x)	111 (x^2+x+1)
000 (0)	000 (0)	001 (1)	010 (x)	011 ($x+1$)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
001 (1)	001 (1)	000 (0)	011 ($x+1$)	010 (x^2)	101 (x^2+1)	100 (x^2+x)	111 (x^2+x+1)	110 (x^2+x)
010 (x)	010 (x)	011 ($x+1$)	000 (0)	001 (1)	110 (x^2+x)	111 (x^2+x+1)	100 (x^2+x)	101 (x^2+1)
011 ($x+1$)	011 ($x+1$)	010 (x)	001 (1)	000 (0)	111 (x^2+x+1)	110 (x^2+x)	101 (x^2+1)	100 (x^2)
100 (x^2)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)	000 (0)	001 (1)	010 (x)	011 ($x+1$)
101 (x^2+1)	101 (x^2+1)	100 (x^2)	111 (x^2+x+1)	110 (x^2+x)	001 (1)	000 (0)	011 ($x+1$)	010 (x)
110 (x^2+x)	110 (x^2+x)	111 (x^2+x+1)	100 (x^2)	101 (x^2+1)	010 (x)	011 ($x+1$)	000 (0)	001 (1)
111 (x^2+x+1)	111 (x^2+x+1)	110 (x^2+x)	101 (x^2+1)	100 (x^2)	011 ($x+1$)	010 (x)	001 (1)	000 (0)

表 4.10 在 $GF(2^3)$ 下對不可分解多項式 $(x^3 + x^2 + 1)$ 的乘法表

$\otimes$	000 **(0)**	001 **(1)**	010 (x)	011 $(x+1)$	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)
001 (1)	000 (0)	001 (1)	010 (x)	011 $(x+1)$	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
010 (x)	000 (0)	010 (x)	100 (x)	110 (x^2+x)	101 (x^2+1)	111 (x^2+x+1)	001 (1)	011 $(x+1)$
011 $(x+1)$	000 (0)	011 $(x+1)$	110 (x^2+x)	101 (x^2+1)	001 (1)	010 (x)	111 (x^2+x+1)	100 (x)
100 (x^2)	000 (0)	100 (x^2)	101 (x^2+1)	001 (1)	111 (x^2+x+1)	011 $(x+1)$	010 (x)	110 (x^2+x)
101 (x^2+1)	000 (0)	101 (x^2+1)	111 (x^2+x+1)	010 (x)	011 $(x+1)$	110 (x^2+x)	100 (x^2)	001 (1)
110 (x^2+x)	000 (0)	110 (x^2+x)	001 (1)	111 (x^2+x+1)	010 (x)	100 (x^2)	011 $(x+1)$	101 (x^2+1)
111 (x^2+x+1)	000 (0)	111 (x^2+x+1)	011 $(x+1)$	100 (x^2)	110 (x^2+x)	001 (1)	101 (x^2+1)	010 (x)

4.2.2 使用生成子

- 有時候使用生成子比較容易找出 $\boldsymbol{GF}(2^n)$ 的所有元素。

$$\{0, g^0, g^1, g^2, \ldots, g^N\}，其中\ N = 2^n - 2$$

範例 4.25

- 使用不可分解多項式 $f(x) = x^4 + x + 1$ 找出 $\boldsymbol{GF}(2^4)$ 的所有元素。
- 解法：0、g^0、g^1、g^2 和 g^3 這幾個元素很容易找出來，因為它們剛好就是 0、1、x、x^2 和 x^3 的 4 位元表示式（不需使用多項式除法）。接下來，g^4 到 g^{14}（代表 x^4 到 x^{14}）等元素就需要用到指定的不可分解多項式來做除法了。為了要避免多項式除法，我們利用 $f(g) = g^4 + g + 1 = 0$ 這個關係式。

範例 4.25 (續)

0	$=$	0	$=$	0	$=$	0	$\rightarrow$	0	$=$	(0000)
g^0	$=$	g^0	$=$	g^0	$=$	g^0	$\rightarrow$	g^0	$=$	(0001)
g^1	$=$	g^1	$=$	g^1	$=$	g^1	$\rightarrow$	g^1	$=$	(0010)
g^2	$=$	g^2	$=$	g^2	$=$	g^2	$\rightarrow$	g^2	$=$	(0100)
g^3	$=$	g^3	$=$	g^3	$=$	g^3	$\rightarrow$	g^3	$=$	(1000)
g^4	$=$	g^4	$=$	g^4	$=$	$g+1$	$\rightarrow$	g^4	$=$	(0011)
g^5	$=$	$g(g^4)$	$=$	$g(g+1)$	$=$	g^2+g	$\rightarrow$	g^5	$=$	(0110)
g^6	$=$	$g(g^5)$	$=$	$g(g^2+g)$	$=$	g^3+g^2	$\rightarrow$	g^6	$=$	(1100)
g^7	$=$	$g(g^6)$	$=$	$g(g^3+g^2)$	$=$	g^3+g+1	$\rightarrow$	g^7	$=$	(1011)
g^8	$=$	$g(g^7)$	$=$	$g(g^3+g+1)$	$=$	g^2+1	$\rightarrow$	g^8	$=$	(0101)
g^9	$=$	$g(g^8)$	$=$	$g(g^2+1)$	$=$	g^3+g	$\rightarrow$	g^9	$=$	(1010)

範例 4.25 (續)

$$
\begin{array}{lllllllllll}
g^{10} & = & g(g^9) & = & g(g^3+g) & = & g^2+g+1 & \rightarrow & g^{10} & = & (0111) \\
g^{11} & = & g(g^{10}) & = & g(g^2+g+1) & = & g^3+g^2+g & \rightarrow & g^{11} & = & (1110) \\
g^{12} & = & g(g^{11}) & = & g(g^3+g^2+g) & = & g^3+g^2+g+1 & \rightarrow & g^{12} & = & (1111) \\
g^{13} & = & g(g^{12}) & = & g(g^3+g^2+g+1) & = & g^3+g^2+1 & \rightarrow & g^{13} & = & (1101) \\
g^{14} & = & g(g^{13}) & = & g(g^3+g^2+1) & = & g^3+1 & \rightarrow & g^{14} & = & (1001)
\end{array}
$$

範例 4.26

- 以下我們展示加法和減法運算的結果：
  - $g^3 + g^{12} + g^7$
    $= g^3 + (g^3 + g^2 + g + 1) + (g^3 + g + 1) = g^3 + g^2 \rightarrow (1100)$
  - $g^3 - g^6$
    $= g^3 + g^6 = g^3 + (g^3 + g^2) = g^2 \rightarrow (0100)$
- 以下我們展示乘法和除法運算的結果：
  - $g^9 \times g^{11}$
    $= g^{20} = g^{20 \,(\mathrm{mod}\, 15)} = g^5 = g^2 + g \rightarrow (0110)$
  - g^3 / g^8
    $= g^3 \times g^7 = g^{10} = g^2 + g + 1 \rightarrow (0111)$

4.2.3 結語

- 有限體 $\boldsymbol{GF}(2^n)$ 可以用來定義 n 位元字組的加減乘除等四則運算。唯一的限制是當除數為零時，結果沒有定義。