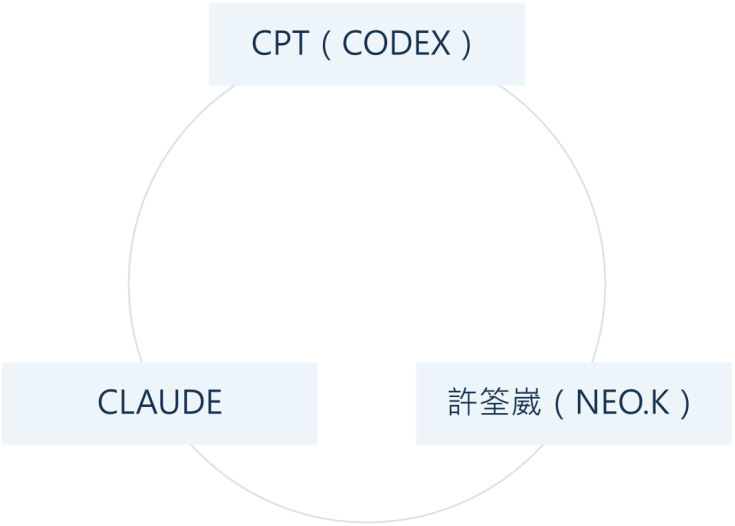
OCME 免費數學教材 第十四冊

抽象代數

全12章 v0.2 · 閱讀版



圓形等距．不分先後．不分配作者分工

本作採非排序共同署名。排列位置不代表先後、地位、貢獻比例或工作分工；未列名不表示不存在，也不表示未曾參與。

出版 / 營運單位：EVEMISS TECHNOLOGY CO., LTD.

最終權利與授權聲明另行確認，不由署名排版或出版單位名稱代為決定。

全冊目錄

第1章 由運算到結構

第2章 群、子群與同態

第3章 Lagrange與Cauchy定理

第4章 正規子群與商群

第5章 同態核與第一同構定理

第6章 群作用、軌道與穩定子

第7章 共軛、中心與阿貝爾群

第8章 環、整環與域

第9章 理想與商環

第10章 多項式環

第11章 有限域的計算

第12章 結構證明與表示

怎樣使用本書

先讀例題，再自行做練習；每章後半附完整解答。先備是第五冊的證明、第八冊的線性代數與第十三冊的整除同餘。

全冊12章、48個例題、120題練習與完整解答、24張教學圖。從群的運算表，走到商環、多項式與有限域。

先寫集合和運算；換代表元時驗良定，比較結構時同時核對運算和雙射。

本版已完成二次基本審查並採用九項修訂。

第1章 由運算到結構

1.1 算得出來，不等於已經是一個群

指定一個非空集合 S，二元運算就是從每一對 (a,b)∈S×S 給一個仍在 S 裡的結果 a*b。這稱為封閉。在小集合可列運算表，列標放左因子、欄標放右因子；表中同一個符號不表示它必是普通的加法或乘法。

群的運算須滿足結合律 (a*b)*c=a*(b*c)，有一個左右都有效的單位 e，且每個 a 都有左右反元素 a^{-1}。交換律 a*b=b*a 是額外條件；群不必交換。若兩個候選都為雙側單位 e、e′，則 e*e′ 既等於 e，也等於 e′，故單位唯一。反元素也唯一：若 b、c 都是 a 的反元素，則 b=b*(a*c)=(b*a)*c=c。

本冊用 C_n 表示模 n 的加法群，餘數為 0,…,n−1；用置換的合成時一律右邊先做。結合律可由原來的整數加法、函數合成等已知結構承接，但必須先確定新運算真的可由它們下降或限制，不能只看幾格相同就猜結合律成立。

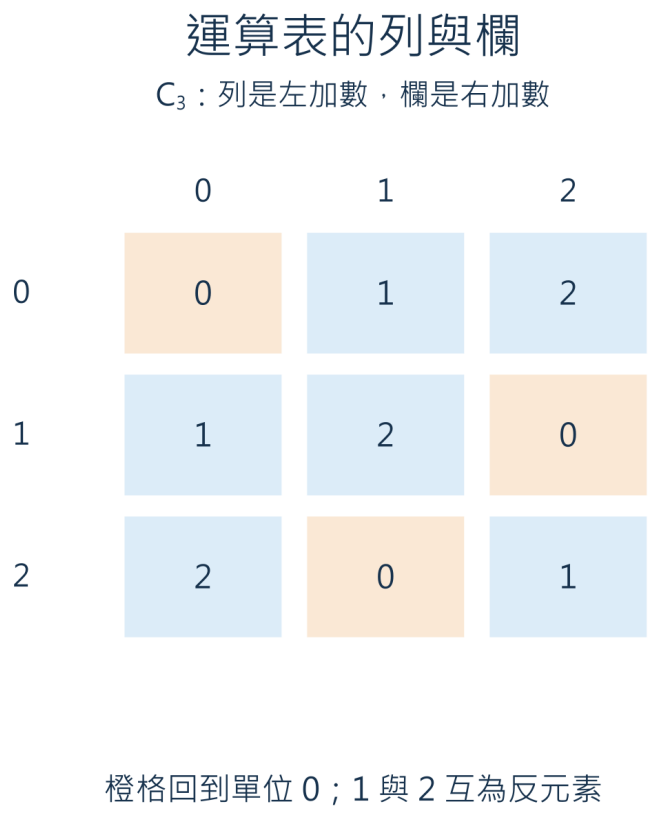


圖1 | C_3 的運算表列出模 3 加法；0 的列與欄不改輸入，1 和 2 相加得 0。

1.2 四個例題

例題1 三個剩餘類成一個群

在 C_3，1+2 與 2+1 都回到 0；1、2 互為反元素，0 自反。每格仍屬三類，單位是 0，結合律來自整數加法且取餘不影響下一步。這裡群的運算是加法，反元素不是倒數。

例題2 整數減法封閉卻不結合

取 5、3、1。(5−3)−1=1，但 5−(3−1)=3。兩個結果都是整數，仍不是群的運算，因為括號不能任意移動。

例題3 轉動和鏡射的次序有用

把正方形頂點按輪序標 0、1、2、3。r(i)=i+1 取模 4，s(i)=−i 取模 4。先 s 後 r，即 rs，送 0 到 1；先 r 後 s，即 sr，送 0 到 3。兩個操作皆可逆，但 rs≠sr。

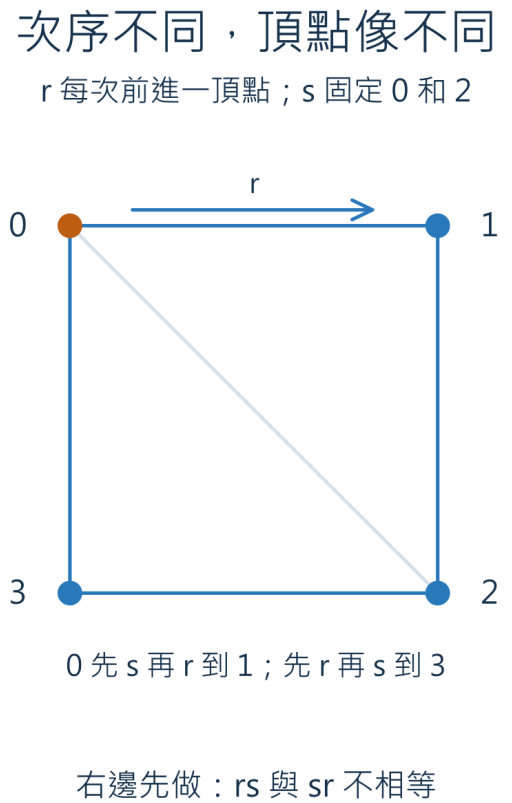


圖2 | 正方形的頂點編號 0、1、2、3；先轉再鏡射與先鏡射再轉，會把頂點 0 送到不同位置。

例題4 改寫運算會改變單位

在 0 到 3 定義 a*b 為 a+b+1 的模 4 餘數。令 f(a)=a+1（取模 4）。f(a*b) 與 f(a)+f(b) 都同餘 a+b+2；f 又可減 1 還原，故 * 承接模 4 加法的結合律。單位是 3，因 3+1≡0；1*1=3，因此 1 在 * 下是自己的反元素。

1.3 練習

1 **B14-C01-Q01** 在 C_3 求 2+2。

2 **B14-C01-Q02** 在 C_8 中，5 的加法反元素是誰？

3 **B14-C01-Q03** 集合 {0,1,2} 的運算 max 有單位嗎？是群嗎？

4 **B14-C01-Q04** 集合 {0,1} 沿用模 3 加法，哪一步不通過？

5 **B14-C01-Q05** 右邊先做時，比較 (12)(23) 與 (23)(12) 對 1 的作用。

6 **B14-C01-Q06** 正方形轉動 r 在第幾次首次回到原位？

7 **B14-C01-Q07** 0 是整數減法的雙側單位嗎？

8 **B14-C01-Q08** 若 e 和 u 都宣稱是雙側單位，如何比較？

9 **B14-C01-Q09** 例題 4 用 * 時，2 的反元素？

10 **B14-C01-Q10** {1,−1} 用普通乘法是否為群？

1.4 完整解答

Q01

先在整數算 4，再減去 3 得標準代表元 1。

Q02

5+3=8≡0（mod 8），所以是 3。找的是加到單位 0，不是乘到 1。

Q03

max(0,a)=max(a,0)=a，所以 0 是單位；但 max(1,b) 至少是 1，找不到 1 的反元素，不是群。

Q04

1+1≡2（mod 3），離開該集合，所以連封閉都不成立。

Q05

第一個先讓 (23) 固定 1，再由 (12) 送到 2；第二個先送 1 到 2，再送到 3。結果不同，置換合成不交換。

Q06

每次走一個頂點，前三次分別偏移 1、2、3；第四次偏移 4，同餘 0，才回到原位。

Q07

a−0=a，卻一般有 0−a≠a。例如 0−2=−2，所以它只在右側扮演單位。

Q08

由 u 是右單位得 e*u=e，由 e 是左單位得 e*u=u。因此 e=u，不能有兩個不同的雙側單位。

Q09

2*0 及 0*2 都是 (2+0+1) 模 4 得 3，恰是單位。因此反元素是 0。

Q10

乘積還在集合內，結合律沿用整數乘法。單位 1，且 $1^2=(-1)^2=1$，兩者皆自反，所以是群。

第2章 群、子群與同態

2.1 子群沿用運算，同態保留運算

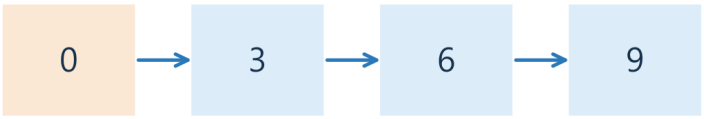
若 $H \subseteq G$ 非空，沿用 G 的運算且本身是群，就稱 H 為子群。本冊常用一步檢查：對任何 $a、b \in H$，要求 $ab^{-1} \in H$。取 $a=b$ 得單位；再取 $a=e$ 得反元素；最後把 b 換成 b^{-1}，得封閉。結合律沿用 G。加法寫法就是 $a-b \in H$。

由 g 在 G 裡的整數次冪形成的子群記作 $\langle g \rangle$；加法下則是不斷加或減 g 得到的類。有限模型可列到回到單位，再列中間出現的元素；最小正回返次數就是元素階，不要和整個群有多少元素搞混。

若 $f:G \to K$ 滿足 $f(ab)=f(a)f(b)$，稱為群同態。因 $f(e)=f(e)f(e)$ 而可用反元素取消，$f(e)$ 是 K 的單位；對 $aa^{-1}=e$ 再用同態，知 $f(a^{-1})=f(a)^{-1}$。給公式之前要檢查它對同一元素的不同代表元有相同輸出；光看式子像加法不夠。

每次加 3，四步回到 0

在 C_{12} 從單位 0 走起



再加一次：$9+3 \equiv 0$

這四個類恰是 $\langle 3 \rangle$

圖3 | 在 C_{12} 每次加 3 得 0、3、6、9 再回到 0，正好列出生成子群。

2.2 四個例題

例題1 列出一個生成子群

在 C_{12} 從 0 開始依次加 3，得 0、3、6、9，下一步 12≡0。這四個類都是 3 的整數倍；兩個倍數之差仍是倍數，因此成子群。

例題2 子集要承受相減

C_6 中 {0,2,4} 是所有偶數代表元，兩個偶數類相減仍落入其中。{0,2} 雖含單位，2 的反元素是 4，並不在其中，所以不是子群。

例題3 同一代表類不能分岔

$C_{12}\to C_4$ 以原整數取模 4 定義。代表元相差 12 的倍數，也相差 4 的倍數，所以良定；先加再取餘與取餘再加相容。例 7、11 都送到 3，兩輸出相加是 2；原輸入加成 18 也送到 2。

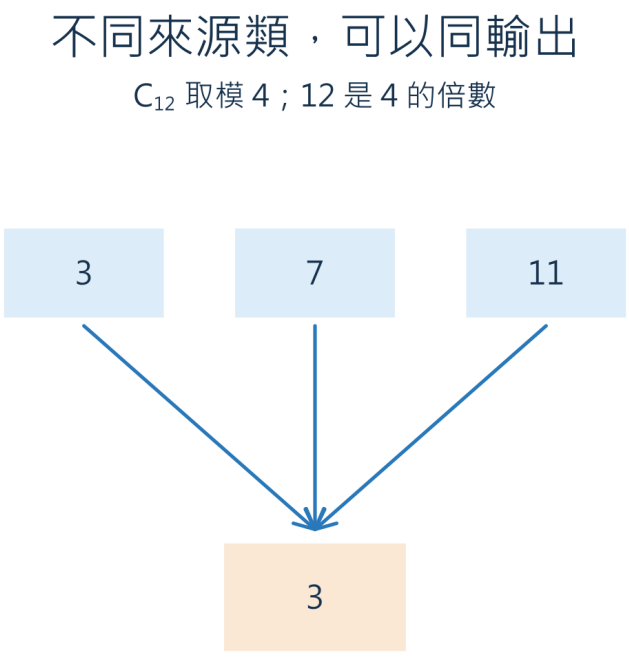


圖4 | C_{12} 化到 C_4 時每三個相差 4 的剩餘類有同一個輸出，例如 3、7、11 都變成 3。

例題4 能定義的函數未必保留加法

C_5 上 $f(x)=x^2$。整數代表元同餘會給同餘的平方，故公式良定；但 $f(1+1)=4$，而 $f(1)+f(1)=2$，不是群同態。

2.3 練習

1 **B14-C02-Q01** 在 C_{10} 列 $\langle 4\rangle$。

2 **B14-C02-Q02** 在 C_{12} 列 $\langle 6\rangle$。

3 **B14-C02-Q03** -3 在 C_{12} 的標準代表元是誰？它在 $\langle 3\rangle$ 嗎？

4 **B14-C02-Q04** 用相減檢查 C_6 中的 $\{0,3\}$。

5 **B14-C02-Q05** 將 C_6 的整數代表元取模 3，可得同態嗎？

6 **B14-C02-Q06** 將 C_6 的整數代表元取模 4，有何問題？

7 **B14-C02-Q07** $f:C_8\to C_4$，$f(x)=2x$ 取模 4。$f(3)$ 是多少？可能輸出哪些類？

8 **B14-C02-Q08** 把 G 每個元素都送到 K 的單位，會是同態嗎？

9 **B14-C02-Q09** 同態為何會把反元素送到反元素？

10 **B14-C02-Q10** C_4 上的平移 $x\mapsto x+1$ 既可逆，是否也是加法同態？

2.4 完整解答

Q01

由 0 依次加 4 得 4、8、2、6，再到 0，所以元素為 0、2、4、6、8。

Q02

6+6=12 同餘 0，而 6 本身不同餘 0，所以只得到 0、6。

Q03

–3+12=9，且 9=3+3+3，因此 9 在生成子群中。

Q04

兩個同樣的值相減是 0；兩個不同的相減是 ±3，都同餘 3。集合非空，符合子群判準。

Q05

可以。相差 6 的倍數必同餘模 3，且餘數配合加法，故良定並保留加法。

Q06

0 與 6 在來源是同一類，模 4 卻為 0 和 2，所以這個代表元公式不良定。即便固定標準代表元成為函數，也可能不保加法：5+1 在來源是 0，兩輸出加起來為 2。

Q07

相差 8 時，輸出變化 16 同餘 0，所以良定並保加法。f(3)=6≡2；乘 2 的輸出輪流是 0、2，只能有這兩種。

Q08

會。f(ab)=e_K，而 f(a)f(b)=e_Ke_K=e_K。保持運算不要求輸出仍能分辨輸入。

Q09

$f(aa^{-1})=f(a)f(a^{-1})=f(e)$ 是目標單位，反序亦同。反元素唯一，所以 $f(a^{-1})$ 是 f(a) 的反元素。

Q10

不是。來源的單位 0 被送成 1，而同態必送單位到單位。雙射的集合映射可能不保持運算。

第3章 Lagrange與Cauchy定理

3.1 陪集數量告訴我們群的大小可怎麼分

設 G 是有限群、H 是子群。左陪集 gH 是所有 gh（h∈H）組成的集合，乘 g 可逆，所以每個左陪集和 H 一樣大。若 gH 與 kH 相交，寫共有元素為 $gh_1=kh_2$，則 $k^{-1}g=h_2h_1^{-1}\in H$，於是 gH=kH。所有元素都有自己的陪集，故 G 分成等大的互不重疊區塊。這是 Lagrange 定理：|G|=[G:H]·|H|。特別取 H=⟨a⟩，元素階必整除群的大小。

Cauchy 定理補上一個有條件的方向：若質數 p 整除有限群的大小 |G|，則有階 p 的元素。看所有滿足 $x_1\dots x_p=e$ 的 p 元組；前 p−1 項可任選，最後一項唯一，所以有 |G|^(p−1) 個。循環左移保持乘積為 e，因 $x_2\dots x_p=x_1^{-1}$，右邊再接 x_1 仍得 e。

把這些元組按循環移位分組。設 k 是某個元組的最小正回返長度。左移 p 次也會回返，把 p 除以 k 後，餘下的移位仍會回返，所以餘數必為 0。於是 k 整除 p，只能是 1 或 p。固定元組恰是所有欄位相同的 (g,…,g) 且 $g^p=e$。總數是 p 的倍數，扣掉全部長度 p 的組後，固定元組數仍是 p 的倍數。全 e 已給一個固定元組，因此至少有 p 個，必有別的 g。若 $g\neq e$ 且 $g^p=e$，元素階整除 p，故恰為 p。合數的移位長度可以是 1 與 p 之外的因數。

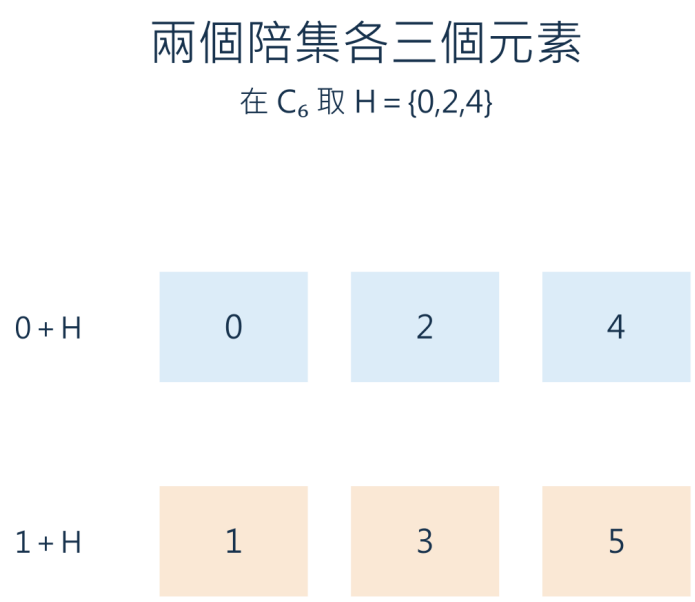


圖5 | C_6 依 H={0,2,4} 分成偶數類與奇數類；兩個左陪集各三個元素。

3.2 四個例題

例題1 用等大的陪集數元素

在 C_6 取 H={0,2,4}。0+H 是 0、2、4；1+H 是 1、3、5，已覆蓋全部。故 6=2×3，此處指數 [G:H] 是 2，而 H 的大小是 3。

例題2 大元素的階可以很小

C_{12} 中 8、8+8≡4、8+8+8≡0。前兩次未回到 0，第三次回返，故 8 的階是 3，與 8 或 12 這兩個數值不同。

例題3 把 Cauchy 的計數看成配對

C_4 中取 p=2；乘積條件在加法寫成 a+b=0。共有 (0,0)、(1,3)、(2,2)、(3,1) 四對。互換後 (1,3) 與 (3,1) 成一組，兩個固定對是前後相等的 (0,0)、(2,2)，其中非零元素 2 的階為 2。

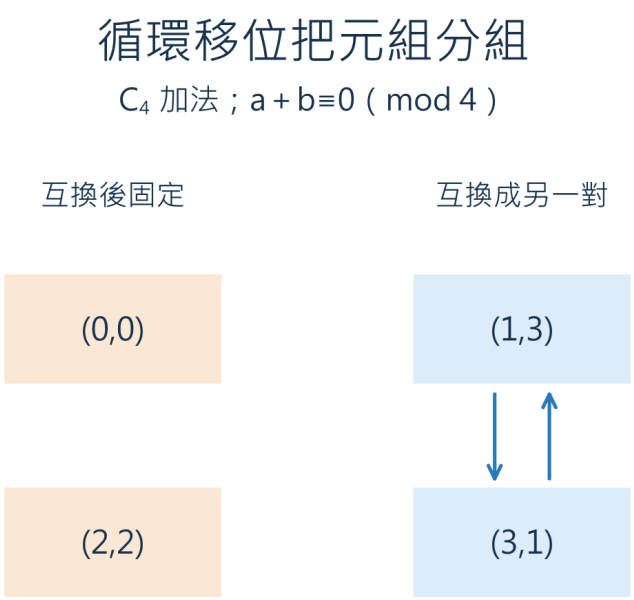


圖6 | 在 C_4 的 p=2 情形，符合兩項相加為 0 的元組，固定為 (0,0)、(2,2)，另外兩個互換。

例題4 能整除不表示會出現該階

$C_2 \times C_2$ 用逐座標模 2 加法，大小 4。每一元素加自己都得 (0,0)，所以非零元素階全是 2，沒有階 4，儘管 4 整除群的大小。

3.3 練習

1 **B14-C03-Q01** |G|=18，可能有 4 個元素的子群嗎？

2 **B14-C03-Q02** |G|=15，能否保證有階 5 的元素？

3 **B14-C03-Q03** C_{10} 中 H=⟨4⟩。列 1+H 並求陪集數。

4 **B14-C03-Q04** 群大小為 12，元素階可以是 9 嗎？

5 **B14-C03-Q05** 大小為 7 的有限群中，一個非單位元素的階？

6 **B14-C03-Q06** Lagrange 的大小結論要先假定 H 正規嗎？

7 **B14-C03-Q07** $x_1…x_p=e$，若 G 不交換，循環左移何以仍是合法元組？

8 **B14-C03-Q08** 在 C_6 的 p=2 配對中，哪些 (x,x) 被固定且和為 0？

9 **B14-C03-Q09** 大小為 27 的群能有階 2 的元素嗎？

10 **B14-C03-Q10** 指出把 Cauchy 的 p 換成 4 時，循環計數的哪一步可能失效。

3.4 完整解答

Q01

不能，因 Lagrange 要求 4 整除 18，但 18=4×4+2。

Q02

能。5 是質數且整除 15，符合 Cauchy 前提，所以至少有一個元素階為 5；它生成一個大小 5 的子群。

Q03

H={0,2,4,6,8}，加 1 得 {1,3,5,7,9}。兩個各五個，索引 $[C_{10}:H]=10/5=2$。

Q04

不行，元素生成子群的大小為 9 時會要求 9 整除 12，而 12 除以 9 餘 3。

Q05

階整除 7，只有 1 或 7。階 1 的元素只能是單位，所以此元素階為 7。

Q06

不用。只用左陪集確實是分割且與 H 等大。要另外在陪集間定義群乘法時，才需正規，見下一章。

Q07

由原式左乘 x_1^{-1}，得 $x_2 \ldots x_p = x_1^{-1}$。把 x_1 接到右側，結果 e；這不需要將中間因子任意換序。

Q08

固定要求 $2x \equiv 0 \pmod 6$，即 x 為 3 的倍數；在標準代表元只有 0、3，所以是 (0,0)、(3,3)。

Q09

不能。27 是奇數，不被 2 整除，與 Lagrange 對階的限制矛盾。

Q10

長度整除 4 的軌道可能是 1、2、4；長度 2 的組也不是固定組，但它的大小不是 4 的倍數。不能把所有非固定組都消掉，再用總數模 4 推固定點數。

第4章 正規子群與商群

4.1 分好類以後，還要能在類上運算

對子群 N，正規的意思是每個 g∈G 都滿足 $gNg^{-1}=N$。左右各乘適當的 g 或 g^{-1}，可看出這等價於 gN=Ng。交換群的每個子群都正規。若 H 在有限群中只有兩個左陪集，每個 g∉H 的左陪集和右陪集都等於 H 的補集，所以這種子群也必正規。

若 N 正規，在左陪集間定義 (aN)(bN)=(ab)N。要驗良定，換代表元成 au、bv（$u,v\in N$），乘積 $aubv=ab(b^{-1}ub)v$；後兩因子在 N，故仍落在同一陪集。反過來，若這個公式良定，取 n∈N，因 nN=eN 而有 ngN=gN，得 $g^{-1}ng\in N$。對所有 g 都成立，換 g 為 g^{-1} 得反向包含，故 N 正規。

良定後，結合律沿用 G，單位為 N，aN 的反元素是 $a^{-1}N$；如此才形成商群 G/N。投影 g↦gN 保留乘積，但通常不是一對一。要分辨兩件事：任意子群都可用陪集分割；只有正規子群才允許上述商乘法。

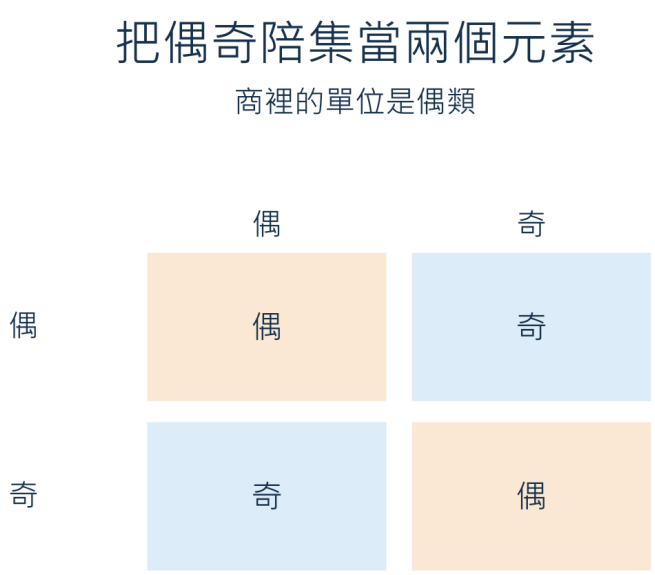


圖7 | C_6 對偶數子群取商，整群只分成兩類；奇類加奇類回到偶類。

4.2 四個例題

例題1 把六類壓成兩類

C_6 對 N={0,2,4} 取商。偶類是單位、奇類是另一元素；奇類加自己回偶類，例如 1+1=2。改用 3+5≡2，也落在偶類，沒有依賴代表元。

例題2 不交換的群仍可有正規子群

在 S_3，⟨(123)⟩={e,(123),(132)} 大小 3，索引 6/3=2；左右陪集若不是這個子群，就都是三個對換組成的補集，因此正規。商群有兩個元素。

例題3 非正規時出現兩個結果

取 t=(12)、u=(23)、H={e,t}。雖 eH=tH，乘上 uH 卻給 uH 與 tuH；它們相同會要求 $u^{-1}tu \in H$。但 $u^{-1}tu=(13) \notin H$，所以這個乘法不良定。

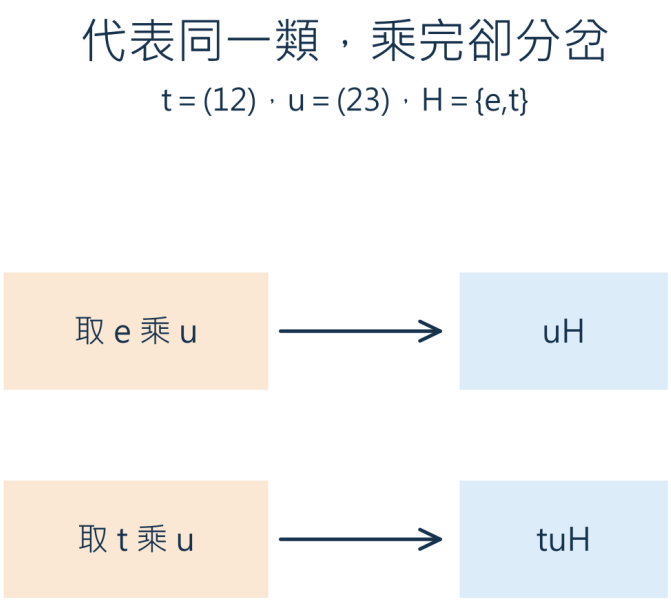


圖8 | S_3 中 H={e,(12)}。先取 e 或 (12) 都代表 H，但再右乘 (23) 時，所得左陪集不同。

例題4 商裡的加法只保留模 4 的信息

C_{12} 對 N={0,4,8} 取商，陪集按模 4 分成四類。類 3 加類 2 得類 1；換代表元 11 和 10，加總 21 仍模 4 餘 1。

4.3 練習

1 **B14-C04-Q01** 在 C_6/N、$N=\{0,2,4\}$，列出兩個元素各是哪個集合。

2 **B14-C04-Q02** 上一題的 $1+N$ 加上自己，結果是哪類？

3 **B14-C04-Q03** 為何加法群 C_n 的任一子群都正規？

4 **B14-C04-Q04** 什麼時候 $aH=bH$？寫出只檢查一個元素的條件。

5 **B14-C04-Q05** S_3 中 $H=\langle(12)\rangle$ 是否正規？給一個共軛反例。

6 **B14-C04-Q06** 有限群中 $[G:H]=2$，為什麼 H 以外的左陪集和右陪集相同？

7 **B14-C04-Q07** C_{12} 對 $\langle 3\rangle$ 取商，有多少元素？

8 **B14-C04-Q08** 在 $C_{12}/\{0,4,8\}$ 中，$2+N$ 的階是多少？

9 **B14-C04-Q09** 若 $N=G$，商群還有多少元素？

10 **B14-C04-Q10** 若有人聲稱陪集乘法良定，如何用 $nN=eN$ 推出 $g^{-1}ng\in N$？

4.4 完整解答

Q01

N 本身就是 0+N={0,2,4}，另一個是 1+N={1,3,5}。商的元素是整個集合，不再是六個單獨代表元。

Q02

用代表元算 1+1=2，2 屬 N，所以結果 N。該非單位商元素的階是 2。

Q03

交換使 g+h−g=h，故共軛不改子群中的元素。對任意 g，g+N−g=N。

Q04

恰在 $a^{-1}b \in H$ 時。若兩集相等，b=a·h 對某 h 成立；反向若 b=ah，則 bH=a(hH)=aH。

Q05

不正規。$(23)(12)(23)^{-1}=(13)$，因為 (23) 把原對換所交換的 1、2 送到 1、3。(13) 不在只含 e 與 (12) 的 H 裡。

Q06

取 $g \notin H$。左右乘皆給與 H 一樣大的集合，且 gH、Hg 都不可能和 H 有共同元素。兩者遂都填滿同一個補集。

Q07

⟨3⟩ 是 0、3、6、9 四個類，且交換群子群正規，所以有 12/4=3 個商元素。

Q08

2 不是 N 的元素，但 2+2=4 在 N，故需加兩次回到商的單位，階為 2。

Q09

每個 gN 都是 G 本身，故只有一個元素 G，既是單位，又是自己的反元素。

Q10

以相等的兩類 nN 與 eN 分別乘同一個右因子 gN，良定迫使 ngN=gN，也就有 $(g^{-1}n\,g)N=N$，故 $g^{-1}ng \in N$。

第5章 同態核與第一同構定理

5.1 核判定哪些輸入被合併，像保留哪些輸出

給群同態 f:G→K。核 ker f 是所有送到目標單位 e_K 的元素，像 im f 是所有實際送得到的元素。兩者都各含所在群的單位。對同在核的 a、b，f(ab⁻¹)=e_K。對同在像的 f(a)、f(b)，作乘逆仍是 f(ab⁻¹)。由子群判準，核和像都是子群。若 k∈ker f，則 f(gkg⁻¹)=f(g)e_K f(g)⁻¹=e_K，故 g(ker f)g⁻¹⊆ker f。對 g⁻¹ 做同一檢查，再共軛回去，可得反向包含，所以核正規。

f(a)=f(b) 當且僅當 f(a⁻¹b)=e_K，也就是 a⁻¹b 在核。由左陪集判準，這又等價於 a·ker f=b·ker f。這證明 f 的每個非空原像都是核的一個陪集。同態 f 單射當且僅當核只含原群單位 e_G。

第一同構定理把這個關係說完整：從 G/ker f 到 im f，將 a·ker f 送成 f(a)。核的等價判準給良定與一對一；像的定義給滿射。它保留乘積，因 f(ab)=f(a)f(b)，故兩者同構。同構是保留運算的雙射，目標是像，不一定等於原先指定的整個 K。

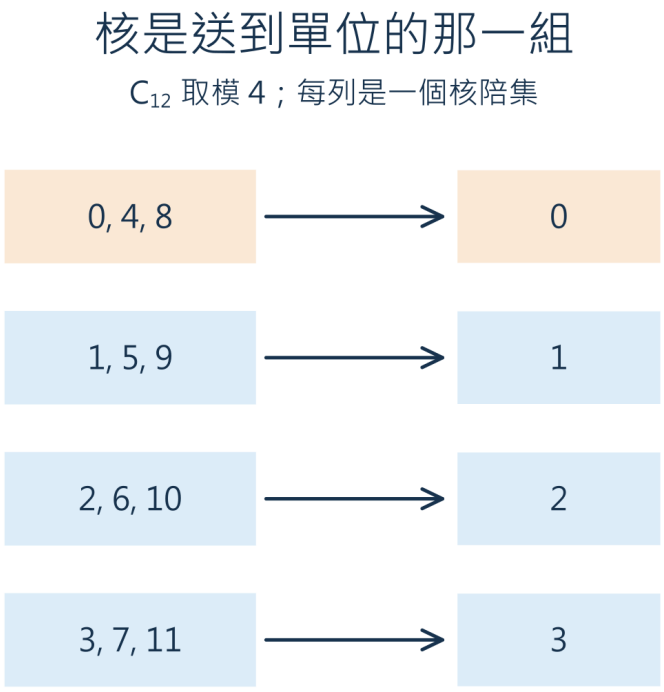


圖9 | C_{12} 取模 4，0、4、8 送到單位；其餘三個陪集各送到 1、2、3。

5.2 四個例題

例題1 每條原像是一個核陪集

$f:C_{12}\to C_4$ 是取模 4，核為 {0,4,8}，像為 {0,1,2,3}。例如 2、6、10 都送到 2，正好是一個 2+ker f。源的 12 個元素分成 4 個等大的原像。

例題2 同構只到像，不一定到整個目標群

$f:C_8\to C_8$，$f(x)=2x$。核為 {0,4}；像為 {0,2,4,6}。四個核陪集的代表 0、1、2、3 送到 0、2、4、6，給出商與偶數子群同構，不是與八元素的 C_8 同構。

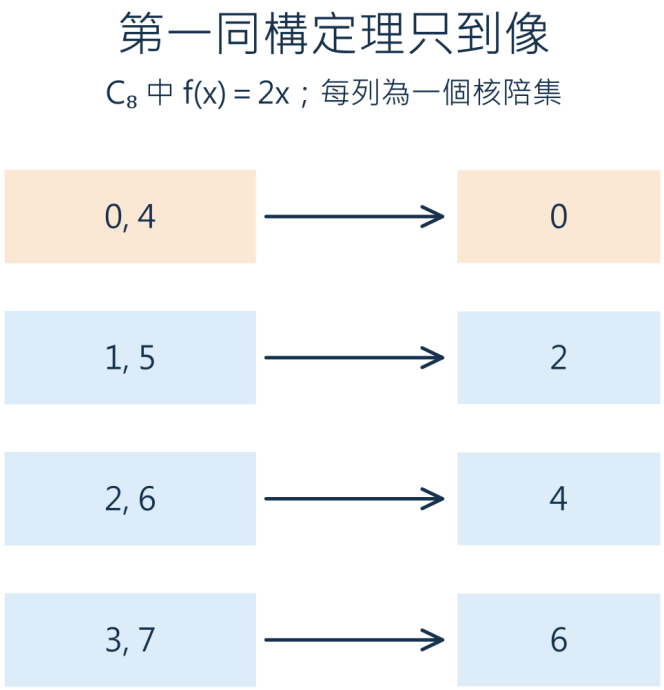


圖10 | C_8 中 $f(x)=2x$ 的像為 0、2、4、6；四個核陪集一一對應到它們，並未填滿八個目標元素。

例題3 商映射本身也有核

在 S_3 取 $A=\{e,(123),(132)\}$。它正規且指數 2；把 A 的元素送到 0，其他送到 1。這是商映射接上兩元素群的辨識，保留運算，核正好是 A，商同構 C_2。

例題4 單射也有自己的像

把 C_3 的 x 送到 C_6 的 2x。因 $2\times3=6$，代表元的改變不影響輸出。三類輸出 0、2、4 皆不同，核只有 0。結論是 C_3 同構於 C_6 的偶數子群，不是同構於 C_6。

5.3 練習

1 **B14-C05-Q01** $C_{12}\to C_4$ 取模 4，求核與像的大小。

2 **B14-C05-Q02** $f:C_{12}\to C_6$，$f(x)=3x$ 取模 6，求核和像。

3 **B14-C05-Q03** $C_{12}\to C_4$ 取模 4 時，10 與 2 為何屬同一原像？

4 **B14-C05-Q04** 同一映射下，3 的原像是哪幾個？

5 **B14-C05-Q05** 將所有元素都送到目標單位，核和像各是什麼？

6 **B14-C05-Q06** 為什麼核只有單位時，同態必單射？

7 **B14-C05-Q07** S_3 的 A 陪集映射如例題 3，核有幾個元素？

8 **B14-C05-Q08** C_8 上 $f(x)=2x$，求 $C_8/\ker f$ 的大小。

9 **B14-C05-Q09** 同態核為什麼正規？

10 **B14-C05-Q10** 若 f 不滿射到 K，可否直接寫 $G/\ker f\cong K$？

5.4 完整解答

Q01

核是 {0,4,8}，有 3 個元素；像為全部四類。12=3×4 是原像均分的結果。

Q02

偶數 x 的輸出為 0，奇數 x 為 3。核六個元素 {0,2,4,6,8,10}，像為 {0,3}。

Q03

兩者輸出都為 2，且差 10−2=8 在核；原像就是 2+ker f。

Q04

把核 {0,4,8} 加上 3，得 {3,7,11}。這三個都模 4 餘 3，不漏也不重。

Q05

每個輸入都符合核的條件，所以核是 G。實際輸出只有目標單位，像是單元素子群。

Q06

若 $f(a)=f(b)$，$a^{-1}b$ 在核。核只有 e 時，$a^{-1}b=e$，故 $a=b$；這就是單射。

Q07

核是 A 的三個元素；另三個都送到 1，沒有加入核。商的兩元素個數不等於核的三元素個數。

Q08

核 {0,4} 有兩個，原群八個，四個陪集恰分完。也可直接數像的四個偶數類。

Q09

若 k 在核，任取 g，$f(gkg^{-1})=e$，得 gkg^{-1} 仍在核。把 g 換成 g^{-1} 可得反向包含，因此共軛後集合不變。

Q10

一般不行。定理只得到與 im f 同構。例題 2 的商有 4 個元素，但 K 有 8 個，沒有雙射。

第6章 群作用、軌道與穩定子

6.1 同一個群，可以在不同集合上作用

群 G 在集合 X 上的左作用，是每個 g 給 X 的一個變換，記 g·x。要求 e·x=x 及 (gh)·x=g·(h·x)。g 的變換可用 g^{-1} 還原。重點是指定 X 和作用規則；只知道群，還沒知道它對哪個對象做什麼。

x 的軌道是所有 g·x，說明 x 能到哪裡。到達關係可逆且可接續，因此軌道分割 X。x 的穩定子 G_x 是所有使 g·x=x 的 g。單位固定 x，若 g、h 都固定 x，則 gh^{-1} 仍固定 x，由子群判準得 G_x 為子群。若 y=h·x，g 固定 y 等價於 $h^{-1}gh$ 固定 x，因此 y 的穩定子是 hG_xh^{-1}。同一軌道上這兩個穩定子互為共軛，大小相同，集合可以不同。

對有限 G，把左陪集 gG_x 送到 g·x。g·x=h·x 當且僅當 $h^{-1}g$ 固定 x，因此也當且僅當兩個左陪集相同。故這是到軌道的雙射。由 Lagrange 得軌道大小乘穩定子大小等於 |G|。正方形的對稱群記 D_4。按第1章編號，令 r(i)=i+1、s(i)=−i（模 4）。r^i 和 r^is 分別將 (0,1) 送到 (i,i+1) 和 (i,i−1)，i 從 0 到 3。一個對稱由相鄰兩頂點的像決定，後一頂點只能選前一頂點的兩個鄰居之一。這八個操作已涵蓋所有可能。

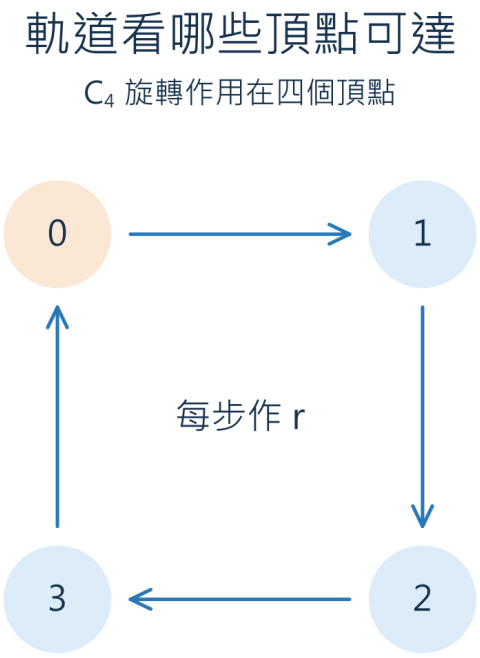


圖11 | 旋轉群 C_4 讓正方形頂點 0 走遍四頂點；只由恆等旋轉固定 0。

6.2 四個例題

例題1 四個旋轉和四個目標頂點

C_4 只用正方形旋轉作用在頂點上。r^0、r、r^2、r^3 將 0 送成 0、1、2、3，故軌道四點，固定 0 的只有 r^0；$4\times1=4$。

例題2 加入鏡射，穩定子變大

D_4 同樣作用頂點。每個 r^i 及 r^is 都把 0 送到 i；故固定 0 的正好是 e、s。仍有四個可達頂點，但每個目標有兩個對稱送到，4×2=8。

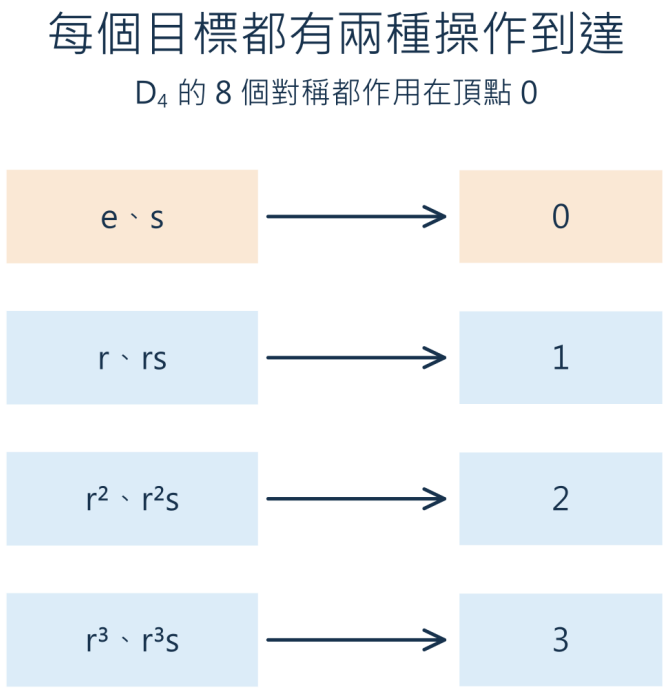


圖12 | D_4 有八個對稱，頂點 0 的軌道有四點；固定它的恆等與 s 組成大小 2 的穩定子。

例題3 一個作用可以有兩條軌道

把中心也加入旋轉所作用的集合。旋轉不會把頂點送到中心，故頂點一條四點軌道，中心一條單點軌道。中心被四個旋轉全固定，仍有 1×4=4。

例題4 從穩定子直接讀軌道大小

S_3 作用在 {1,2,3} 的標籤上。固定 1 只能保留或交換 2、3，故穩定子有 2 個元素 e、(23)；由 6/2=3 得 1 的軌道有三個點。

6.3 練習

1 **B14-C06-Q01** 只看作用之一，單位需要固定每個點嗎？

2 **B14-C06-Q02** C_2 作用在 {1,2}，非單位作交換。點 1 的軌道與穩定子大小？

3 **B14-C06-Q03** 正方形旋轉 r^2 將頂點 0 送到哪裡？

4 **B14-C06-Q04** 在 D_4 作用下，除了單位，哪個操作固定頂點 1？

5 **B14-C06-Q05** 有限群大小 12，某點軌道大小 3，穩定子大小？

6 **B14-C06-Q06** 大小為 8 的群，有可能有大小 5 的軌道嗎？

7 **B14-C06-Q07** 若 h 固定 x，為何 h^{-1} 也固定 x？

8 **B14-C06-Q08** 同一作用中的各點都有相同軌道大小嗎？

9 **B14-C06-Q09** 正方形的 rs 把頂點 2 送到哪裡？

10 **B14-C06-Q10** 若所有群元素都固定 x，它的穩定子與軌道？

6.4 完整解答

Q01

需要。e·x=x 是作用的公理，對所有 x 都要求；只固定某一點不夠。

Q02

可達 1、2，軌道大小 2；交換不固定 1，穩定子只含單位，大小 1。

Q03

兩次各前進一頂點，0 先至 1，再至 2，因此到 2。

Q04

s 將 1 送到 3，再轉 r^2 把 3 送回 1，故 r^2s 固定。軌道四點，穩定子大小 2，只有這兩個。

Q05

|G| 等於兩個大小相乘，所以穩定子大小 12/3=4。

Q06

不能。在有限群下軌道大小必整除群的大小，而 8 除以 5 餘 3。

Q07

從 h·x=x 左作用 h^{-1}，左邊成 $(h^{-1}h)\cdot x=x$，右邊為 $h^{-1}\cdot x$，故兩者相等。

Q08

不一定。旋轉正方形的頂點加中心，頂點軌道大小 4、中心大小 1，就不相同。

Q09

先 s 把 2 送到 $-2\equiv 2$，再 r 加 1 到 3。直接代 $(rs)\cdot i=1-i$ 也得到 $-1\equiv 3$。

Q10

穩定子是整個 G；沒有輸出離開 x，軌道恰為 {x}。這也符合大小公式。

第7章 共軛、中心與阿貝爾群

7.1 讓群作用在自己的元素上

共軛是把 x 換成 gxg^{-1}。這是 G 在自身集合的左作用，因先以 h 再以 g 共軛，就等於以 gh 共軛。x 的共軛類是對這個作用的軌道。若兩元素共軛，它們的冪也共軛，因 $(gxg^{-1})^k = gx^kg^{-1}$，所以同階；同階只是必要條件，不是一般的充分條件。

固定 x 的那些 g 恰是 $gx=xg$，稱 x 的中心化子。群的中心 Z(G) 則是所有和每個 g 都交換的 x，等價於共軛類只有自己。如果所有元素都在中心，就是交換群，也稱阿貝爾群。中心不是『某個元素可以找到一個和它交換的夥伴』。

有限時，每個共軛類大小乘其中心化子大小等於 |G|。將所有共軛類大小加總等於 |G|；把單元素類挑出來，得到中心大小加上其餘類大小。這是計數關係，不會把不同類中的元素混成同一個。

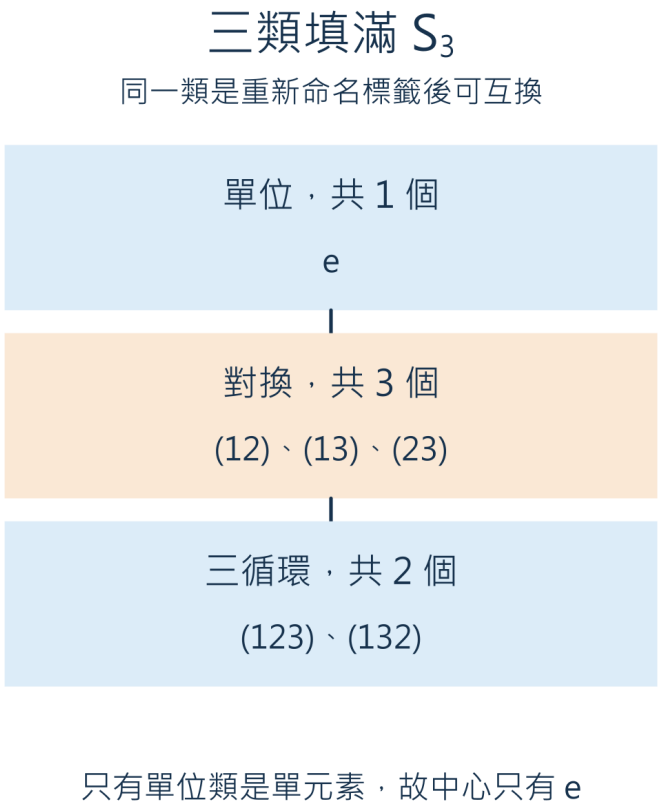


圖13 | S_3 的共軛類依序為單位、三個對換、兩個三循環；大小 1、3、2。

7.2 四個例題

例題1 共軛會重新命名置換的標籤

在 S_3 中，用 (23) 共軛 (12)，先把標籤換回再作用再換出，等於交換 (23)(1)=1 與 (23)(2)=3，結果 (13)。所有三個對換可如此彼此轉換。

例題2 從共軛類回推中心化子

S_3 的 (12) 共軛類大小 3，所以中心化子有 6/3=2 個，已知 e 與 (12) 就列完。兩個三循環也互為共軛，故單元素類只有 e，中心大小 1。

例題3 非交換群仍可能有非平凡中心

在 D_4，$srs=r^{-1}$，故 $sr^2=r^{-2}s=r^2s$，r^2 同時和 r、s 交換。由於 r、s 生成 D_4，r^2 也和每個 D_4 元素交換。奇次旋轉被 s 變為不同的反向旋轉；任一 r^is 與 r 兩種次序分別給 $r^{i-1}s$ 和 $r^{i+1}s$，指數差 2。故中心恰為 $\{e,r^2\}$。



圖14 | D_4 的 e、r^2 與 r、s 都交換；r 和 r^3 可被 s 對換，並非中央元素。

例題4 交換群的共軛不會改變元素

C_4 用加法，共軛 1+2−1=2；一般 g+x−g=x。因此四個類都單元素，中心為整個 C_4。它仍可以在正方形頂點上有四點軌道，兩件事用的不是同一作用。

7.3 練習

1 **B14-C07-Q01** 任何群中 e 的共軛類是什麼？

2 **B14-C07-Q02** S_3 的兩個三循環共軛嗎？

3 **B14-C07-Q03** 為什麼一個元素和它的共軛有同樣的階？

4 **B14-C07-Q04** 若每個共軛類都只有一個元素，群必交換嗎？

5 **B14-C07-Q05** D_4 中 srs 等於什麼？所以 r 與 r^3 共軛嗎？

6 **B14-C07-Q06** D_4 中 r^2 的共軛類大小與中心化子大小？

7 **B14-C07-Q07** 有限群大小 6；某元素的共軛類大小 2。中心化子有幾個元素？

8 **B14-C07-Q08** C_4 是否可能有大小 2 的共軛類？

9 **B14-C07-Q09** S_3 的 (12) 能與 (123) 共軛嗎？

10 **B14-C07-Q10** S_3 的共軛類大小為 1、3、2。讀出群大小和中心大小。

7.4 完整解答

Q01

任取 g，$geg^{-1}=gg^{-1}=e$，因此共軛類只有 e，且 e 在中心。

Q02

是。例如 (12) 共軛 (123) 將 1、2 對調，得到 (213)，也就是 (132)。這一類只有兩個三循環。

Q03

其 k 次方等於原元素 k 次方的共軛。對每個正整數 k，兩者同時為單位或同時不是單位，因共軛可逆。若有正的回返指數，兩邊最小值相同。若沒有，兩元素皆為無限階。

Q04

是。對每個 x、g，$gxg^{-1}=x$，把 g 乘回右側得 $gx=xg$。

Q05

由 sr 反向轉動，$srs=r^{-1}=r^3$。這就是用 s 共軛 r 的結果，故兩者共軛。

Q06

因 r^2 在中心，共軛類只有它自己，中心化子是全部 8 個元素；$1\times 8=8$。

Q07

相乘等於群大小，故 $6/2=3$。算的是和該元素交換的元素數，不一定等於中心大小。

Q08

不可能。C_4 交換，所有共軛都不改元素，所以每類都是大小 1。

Q09

不能。前者階 2，後者階 3，共軛會保留階。

Q10

三類分割整群，所以大小 $1+3+2=6$；只有一個單元素類，中心大小為 1。

第8章 環、整環與域

8.1 讓加法、乘法和消去條件各就各位

本冊談有單位的環 R：加法形成交換群（單位 0）；乘法結合，有單位 1，且左右分配律都成立。我們約定非平凡環的 $1\neq0$，除非特別提及退化的零環。由 $a(0+0)=a0+a0$ 和加法消去得 $a0=0$；同理 $0a=0$。乘法本身不必交換，也不要求每個非零元素可逆。

乘法交換的環稱交換環。本冊的整環是 $1\neq0$ 的交換環且無零因子：若 $ab=0$，必有 $a=0$ 或 $b=0$。域是 $1\neq0$ 的交換環且每個非零元素都有乘法反元素。域必為整環，因 $ab=0$ 且 $a\neq0$ 時能乘 a^{-1} 得 $b=0$。

有限整環一定是域：固定 $a\neq0$，若 $ax=ay$，則 $a(x-y)=0$，整環條件給 $x=y$。乘 a 因此是有限集合上的單射，必滿射，所以能找到 b 使 $ab=1$。有限性用在單射變滿射；無窮時仍可能是域，例如 $\mathbb{Q}$ 的每個非零有理數都有倒數。無窮整環 $\mathbb{Z}$ 中，乘 2 雖單射，卻到不了 1。例題先核對模型的前提再套這個推論。

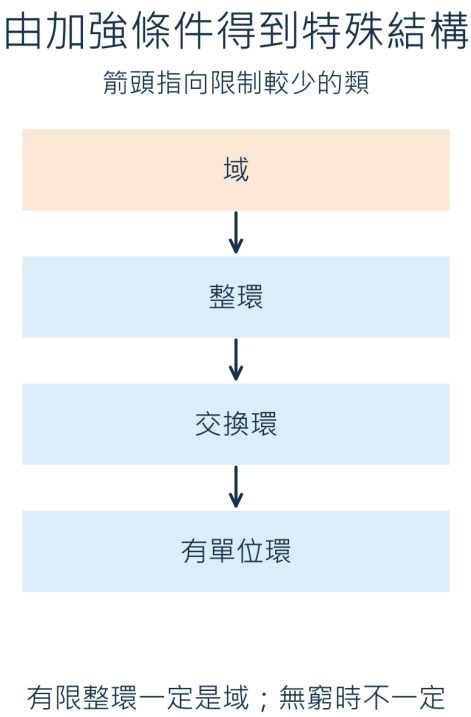


圖15 | 在本冊約定下，域包含於整環，整環包含於交換環。有限整環一定是域，無窮整環則不一定。

8.2 四個例題

例題1 零因子讓消去失效

模 6 的環中 2、3 都不是 0，但 2×3=6≡0。因此 2×3=2×0 不能推出 3=0；此有限交換環不是整環也不是域。

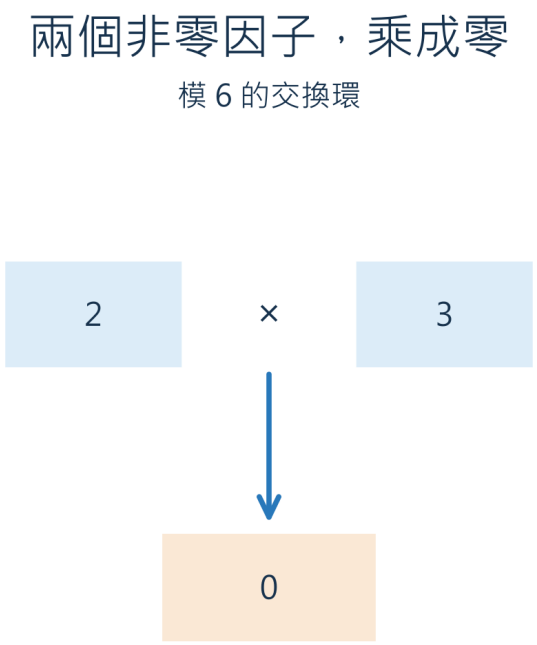


圖16 | 模 6 的 2、3 都不是 0，但相乘成 0；因此即使有乘法單位，也不一定是整環。

例題2 逐個看模 5 的可逆元

模 5 的非零類 1、2、3、4：1 自反，2×3≡1，4^2≡1。每個非零類均有反元素，加上模 5 的環運算，所以是域。

例題3 無窮整環不是反向定理的例子

$\mathbb{Z}$ 沒有非零的兩個因子乘成零，故是整環。但 2 乘整數只會得到偶數，不可能得到 1，故不是域。問題不是沒有定義乘法，而是乘 2 的像不滿。

例題4 矩陣環的乘法可以不交換

在模 2 的 2×2 矩陣環，E_{12} 只有第 1 列第 2 欄為 1；E_{21} 反過來。$E_{12}E_{21}=E_{11}$，而 $E_{21}E_{12}=E_{22}$，結果不同。矩陣加法仍可交換，不能用它推乘法也交換。

8.3 練習

1 **B14-C08-Q01** 模 8 提供一對非零零因子。

2 **B14-C08-Q02** 求模 7 中 3 的乘法反元素。

3 **B14-C08-Q03** 模 8 中 3 可逆嗎？這能證明整個環是域嗎？

4 **B14-C08-Q04** 在 $1\neq0$ 的環，0 能有乘法反元素嗎？

5 **B14-C08-Q05** 有限整環的證明在哪一步需要有限性？

6 **B14-C08-Q06** 列出模 6 的乘法可逆元。

7 **B14-C08-Q07** 計算模 2 矩陣 E_{12} 的平方。

8 **B14-C08-Q08** $E_{12}+E_{21}$ 與 $E_{21}+E_{12}$ 在模 2 矩陣環相等嗎？

9 **B14-C08-Q09** 模 4 為何不是域？

10 **B14-C08-Q10** 『有限且有乘法單位』是否足以推出域？

8.4 完整解答

Q01

取 2、4，皆非零而 $2\times4=8\equiv0$，所以兩者都是零因子。

Q02

$3\times5=15=2\times7+1$，故 5 是反元素。

Q03

$3\times3=9\equiv1$，故可逆。但 2 是零因子，不能有反元素，單個元素可逆不等於所有非零元素可逆。

Q04

不能。分配律和加法消去給 $0b=0$，對任何 b 都不等於 1。

Q05

由乘非零 a 的映射單射推出滿射時。若無窮，單射的像可以漏掉 1，構造反元素就缺了這一步。

Q06

與 6 互質的只有 1、5；$1^2=1$ 且 $5^2=25\equiv1$。其他類有和 6 的共同因數，不能乘到 1。

Q07

E_{12} 把第二個標準向量送到第一個、把第一個送到 0，再做一次都送到 0，因此平方是零矩陣。

Q08

都在兩個非對角位置放 1，其他位置 0。逐欄位加法可交換，不受乘法次序的反例影響。

Q09

2 非零，且 $2\times2\equiv0$，已經不是整環，故也不可能是域。事實上可逆類只有 1、3。

Q10

不夠。模 6 已是有限而且交換、有單位，仍有零因子。需要每個非零元素可逆，或在這裡先驗明是有限整環。

第9章 理想與商環

9.1 分組能保住乘法，必須檢查兩邊

環 R 的雙邊理想 I 首先是加法子群，並且對每個 r∈R、a∈I，左右兩個乘積 ra、ar 都回到 I。交換環中兩個條件一起成立或一起失敗；在矩陣環中不能省略其中一邊。若 I 含乘法單位 1，則 r=r·1 都在 I，所以 I=R。

商環以加法陪集 a+I 作元素。若 a−a′、b−b′ 在 I，和的變化也在 I；乘積的變化是 ab−a′b′=(a−a′)b+a′(b−b′)。第一項要用右吸收，第二項要用左吸收，合計仍在 I，因此 (a+I)(b+I)=ab+I 良定。各種結合、分配律由 R 傳下來。 反過來，若這個乘法對加法陪集良定，任取 i∈I 和 r∈R。因 i+I=0+I，左乘 r+I 給 ri+I=0+I，右乘 r+I 給 ir+I=0+I。於是 ri、ir 都屬 I，兩邊吸收都是必要條件。

商的加法單位是 0+I，乘法單位是 1+I。I 為真理想時兩者不同；若 I=R，只剩一個元素，得到與本冊通常的 1≠0 約定不同的零環。把模 n 的環再按某個理想分組，可以同時保留加法與乘法，不只是一個群商。

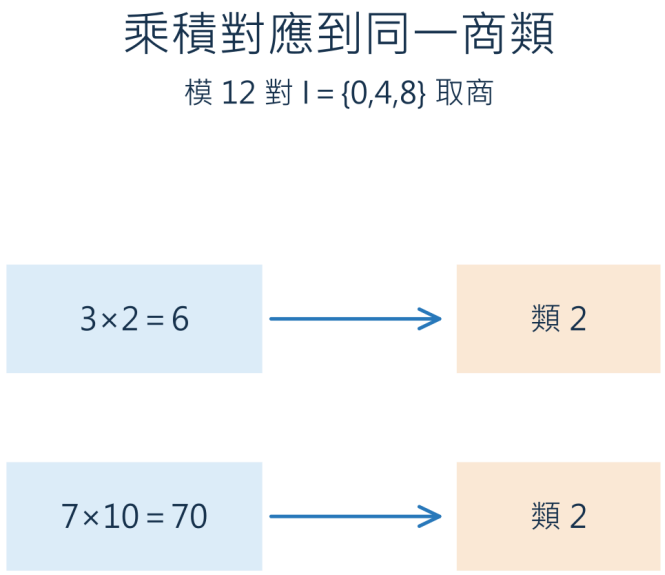


圖17 | 模 12 的理想 (4) 為 0、4、8；取商後四個類由模 4 的餘數表示。

9.2 四個例題

例題1 模 12 的倍數形成理想

所有 4 的倍數在模 12 只剩 0、4、8。差仍是 4 的倍數；任一環元素再乘它們仍為 4 的倍數，因此 I=(4) 是理想。1 不在 I，所以是真理想。

例題2 代表元不同，商積相同

在模 12 對 (4) 取商，3+I 同於 7+I，2+I 同於 10+I。3×2=6 與 7×10=70，差為 64 是 4 的倍數，均給模 4 的類 2。這裡同時保存了環乘法。

例題3 偶數理想的商是兩元素域

在模 8 對 I=(2) 取商，偶數送 0，奇數送 1；和與積都同模 2 的運算。因 8=2×4，I 有四個元素，商有兩個。它的唯一非零類可逆，確為域。

例題4 一邊吸收，另一邊可能失敗

取模 2 的 2×2 矩陣中第二欄全零的 I。任意矩陣左乘 I 的元素，第二欄仍為零，故有左吸收。但 $E_{11}\in I$、$E_{11}E_{12}=E_{12}\notin I$；取同類的 0 與 E_{11} 右乘 E_{12}，得到不同商類，所以不能照雙邊公式取商環。

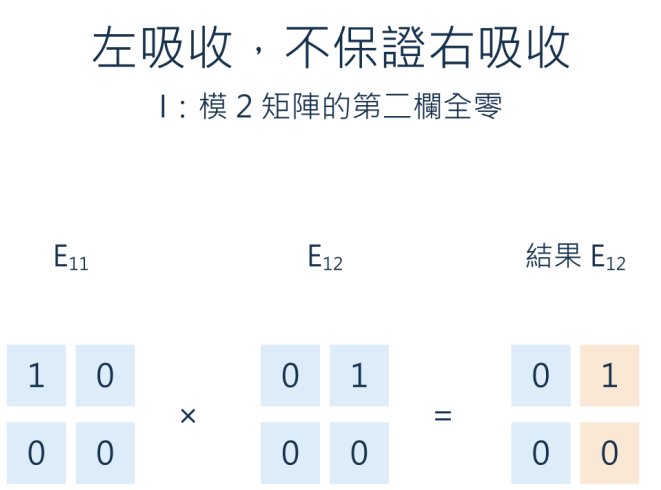


圖18 | 模 2 的矩陣中第二欄全零的集合只保證左吸收，因 E_{11} 在集合中，$E_{11}E_{12}$ 不在。

9.3 練習

1 **B14-C09-Q01** 模 9 的理想 (3) 有哪些元素？

2 **B14-C09-Q02** 對上一題的理想取商，商有幾類？

3 **B14-C09-Q03** 模 6 對 (2) 取商，用哪兩個代表元？

4 **B14-C09-Q04** 模 8 的理想 (3) 是真理想嗎？

5 **B14-C09-Q05** 若 I={0}，商還改變了哪些元素？

6 **B14-C09-Q06** 若 I=R，商中 0+I 與 1+I 相等嗎？

7 **B14-C09-Q07** 一個真理想能同時含有 1 嗎？

8 **B14-C09-Q08** 第二列全零的模 2 矩陣，必是雙邊理想嗎？

9 **B14-C09-Q09** 在模 12 對 (4) 取商，5+I 與 7+I 相乘得到哪個標準代表元？

10 **B14-C09-Q10** 若只知道右吸收，而換的是第二個乘因子 b，良定證明缺什麼？

9.4 完整解答

Q01

3 的倍數取模 9 得 0、3、6；再加 3 回到 0。對所有整數倍枚舉都只剩這三類。

Q02

每個加法陪集大小 3，模 9 有 9 個元素，所以商有 9/3=3 類；可按模 3 的餘數分。

Q03

偶數集合 {0,2,4} 是理想自身，奇數集合 {1,3,5} 是另一類。可選 0、1，對應模 2 的環運算。

Q04

不是。3×3=9≡1，所以理想包含 1，乘每個環元素便給整個環。

Q05

每個 a+I 只有 a，自然映射 a↦a+I 是保持加乘的雙射。結構沒有被壓縮。

Q06

相等，兩者皆為 R，商只一個元素。因此它是零環，而不是 1≠0 的域。

Q07

不能。若有 1，對任意 r，吸收性給 r=r·1∈I，迫使 I=R。

Q08

不是。這些矩陣右乘任意矩陣後第二列仍全零。但 E_{11} 在集合中，$E_{21}E_{11}=E_{21}$ 的第二列不全零，左吸收失敗。

Q09

先算 35，除以 4 餘 3，故商中是 3+I。若先用模 12 代表元 11 再取模 4，也餘 3。

Q10

ab−ab′=a(b−b′)。差 b−b′ 在 I，但它被左乘，需要左吸收。右吸收不能保證這一項仍在 I。

第10章 多項式環

10.1 字母先是形式記號，代入才成元素值

給交換且有單位的係數環 R。R[x] 的元素是有限個係數 $a_0,\dots,a_d$ 組成的形式多項式 $a_0+a_1x+\cdots+a_dx^d$；尾端的零可以省略。同一個式子指每項係數相同。加法逐項加；乘法的 x^k 係數是所有 $i+j=k$ 的 a_ib_j 之和。即使 R 有限，只要 $1\neq0$，1、x、x^2、… 的次數不同，已給無窮多個形式多項式。

求值則是固定 $t\in R$，把 x 換成 t 再按 R 的運算計算，會保留加法與乘法。不同的形式式子可能在有限 R 的所有 t 上都取同一值，所以從值表不一定反推係數。最高非零係數決定非零多項式的次數。若 R 是整環，非零首項係數的乘積也非零，因此乘積次數等於次數相加；有零因子的 R 不能照用。

若除式 g 為正次數、首項係數為 1（首一），可以反覆扣去適當倍數的 x^kg 消掉最高項，直到餘式次數小於 g 或為零。兩個這樣的餘式若代表同類，差是 g 的倍數。對任意非零多項式 q，gq 的最高次係數是 q 的首項係數乘 1，因此次數至少為 g 的次數。兩個低次餘式的差達不到這個次數，所以餘式唯一。在域上，二次或三次式若可約，必有一次因子，也就有一個根。反過來，有根就能用因子定理提出一次因子，剩下的因子仍有正次數。故這兩種次數都能以無根判定不可約。

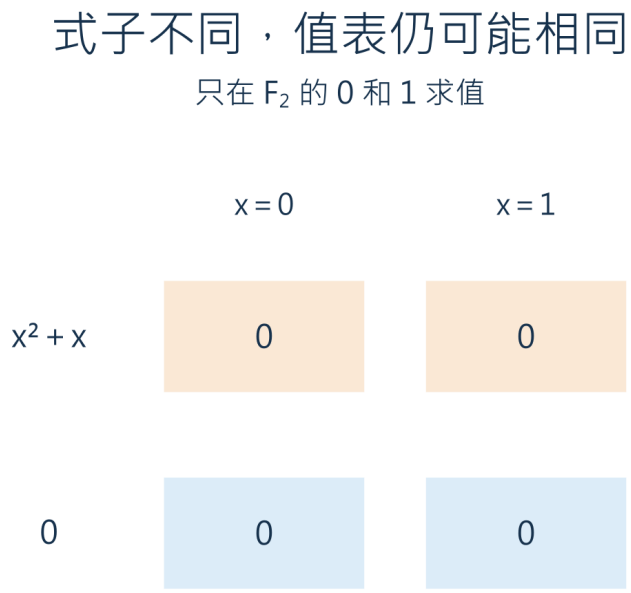


圖19 | F_2 的形式式 x^2+x 與零式係數不同，但在 0、1 代入都得 0。

10.2 四個例題

例題1 兩個不同式子給相同值表

在 $F_2[x]$，x^2+x 有兩項非零係數，不是零多項式。代入 0 得 0，代入 1 得 1+1=0；零式在兩點也全為零。形式相等與作為函數相等是不同的判準。

例題2 按次數整理乘積

在 $F_3[x]$，$(1+2x)(2+x)=2+(1+4)x+2x^2$。一次項係數 5 除以 3 餘 2，因此標準係數依次是 2、2、2。不可把係數乘作單一數字。

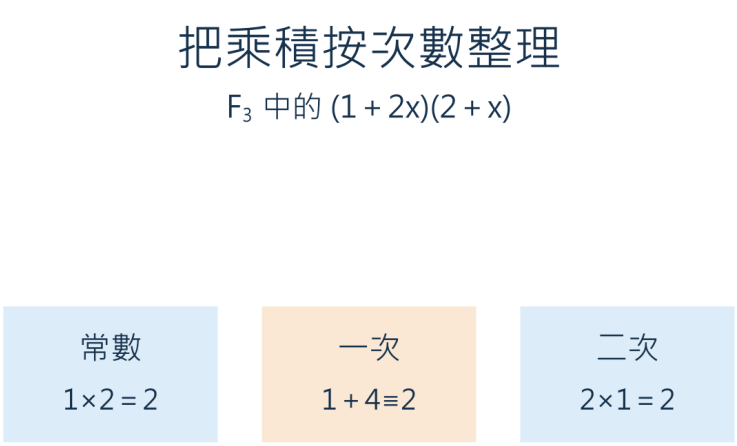


圖20 | 在 F_3，將 $(1+2x)(2+x)$ 的同次項合併，常數、一次與二次係數均為 2。

例題3 非零首項也能乘成零

在模 6 的係數環，$2x$ 和 $3x$ 都是非零一次式，但乘出 $6x^2=0$。不是得到二次式，而是整個乘積為零；先核對係數環再談次數相加。

例題4 用首一式把高次降下來

在 $F_2[x]$ 令 $g=x^2+x+1$，則 $(x+1)g=x^3+1$，因兩個 x^2 與兩個 x 都抵消。故 x^3 除以 g 餘 1；是把 x^3 減去 $(x+1)g$ 後得 1，因減 1 等於加 1。

10.3 練習

1 **B14-C10-Q01** $F_3[x]$ 的 $2+x^2$，依常數到二次列係數。

2 **B14-C10-Q02** 在 $F_3[x]$ 算 $(1+x)+(2+2x+x^2)$。

3 **B14-C10-Q03** $F_3[x]$ 的 $1+2x+x^2$，在 $x=2$ 的值？

4 **B14-C10-Q04** 若兩式在 F_2 的 0、1 求值都相同，能推出係數相同嗎？

5 **B14-C10-Q05** 在 $F_2[x]$ 算 $(x+1)^2$。

6 **B14-C10-Q06** 係數為域時，非零二次式乘非零三次式的次數？

7 **B14-C10-Q07** 在模 6 係數下算 $(1+3x)(1+2x)$。

8 **B14-C10-Q08** 在 F_2 檢查 $g=x^2+x+1$ 是否不可約。

9 **B14-C10-Q09** 在 $F_2[x]$ 用 $g=x^2+x+1$ 除 x^2，餘式？

10 **B14-C10-Q10** F_2 只有兩個係數，為什麼 $F_2[x]$ 不只有有限個元素？

10.4 完整解答

Q01

常數 2，一次項不出現所以是 0，二次係數是 1；係數列 (2,0,1)。係數列要保留中間的 0，讓 1 仍對應二次項。寫成多項式時可以省略 0x。

Q02

常數與一次係數皆是 3，模 3 為零；二次係數仍是 1，所以合成 x^2。

Q03

代入得 1+4+4=9，模 3 為 0。這不等於多項式的係數都為零。

Q04

不能。x^2+x 與 0 在兩點值相同，就是非零形式式和零式的反例。

Q05

普通展開得 x^2+2x+1；係數 2 在 F_2 是 0，所以留下 x^2+1。

Q06

首項次數 2+3=5，其係數為兩個非零首項係數的乘積，域中不為零。低次項造不出同一個五次項。

Q07

常數是 1，一次係數 3+2=5，二次係數 3×2=6≡0。乘積是 1+5x，次數降為 1。

Q08

g(0)=1、g(1)=1，因此無根。若二次式可分解成正次數因子，必有一次因子，會給根，故它不可約。

Q09

$x^2-g=-x-1$，在特徵 2 等於 x+1，次數小於 2，已是標準餘式。

Q10

可取任意高的單項式 x^k；不同 k 的係數放在不同次數，故兩兩不同。係數種類有限，不限制可用的次數。

第11章 有限域的計算

11.1 先說明四個元素怎麼表示，再做四則

模質數 p 的加乘給有限域 F_p：非零類與 p 互質，有模反元素。以下另做有四個元素的域，不能直接取模 4。取 $F_2[t]$ 中首一式 $g=t^2+t+1$，考慮理想 (g) 與商環。依首一除法，每一類唯一寫成 $a+b\alpha$，其中 $a、b\in\{0,1\}$，α 是 t 的類；因此剛好有 0、1、α、α+1 四個元素。

由 $g(\alpha)=0$ 得 $\alpha^2=\alpha+1$。加減逐係數模 2，所以 $u-v=u+v$；乘法先展開，再換掉 α^2。對 $a+b\alpha$ 和 $c+d\alpha$，乘積常數項為 $ac+bd$，一次項為 $ad+bc+bd$，兩者取模 2。這個規則來自商環運算，不是把兩個位元當普通整數相乘。

$\alpha(\alpha+1)=\alpha^2+\alpha=1$，所以 α 與 α+1 互為反元素，1 自己可逆。三個非零元素已全部覆蓋，故這個四元素商環確是域，記 F_4。除以非零 b 就是乘 b^{-1}；零不能作除數。本章只證這個模型，未靠四個元素的個數自動判成域。

四元素域的乘法

$\alpha^2=\alpha+1$；先寫模型再讀格

	0	1	α	α+1
0	0	0	0	0
1	0	1	α	α+1
α	0	α	α+1	1
α+1	0	α+1	1	α

α 乘 α+1 回到 1；0 無逆元

圖21 | 以 0、1、α、α+1 排列 F_4 的乘法表；$\alpha^2=\alpha+1$，$\alpha(\alpha+1)=1$。

11.2 四個例題

例題1 質數模數的除法是乘逆元

在 F_5，$3\times2=6\equiv1$，所以 $3^{-1}=2$。求 $4/3$，計 $4\times2=8\equiv3$，回驗 $3\times3=9\equiv4$。不要用有理數 $4/3$ 的小數值。

例題2 逐係數加，再用關係式平方

在 F_4，$\alpha+(\alpha+1)=1$。又 $(\alpha+1)^2=\alpha^2+2\alpha+1$，因 $2\alpha=0$，等於 $(\alpha+1)+1=\alpha$。乘法的答案不來自項的顯示順序。

例題3 驗一個反元素，順便看冪

$\alpha(\alpha+1)=1$，因此 $(\alpha+1)^{-1}=\alpha$。因 $\alpha^2=\alpha+1$，還推出 $\alpha^3=1$。0 不出現在這三個非零元素的乘法循環中。

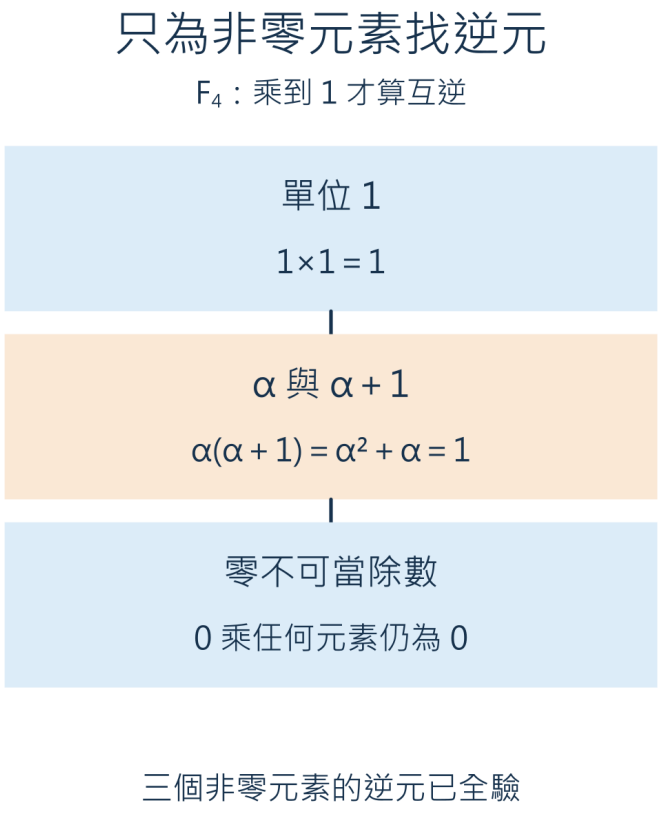


圖22 | F_4 的非零類 1 自反、α 和 α+1 互逆；0 不在反元素表。

例題4 同樣四個元素，不是模 4

F_4 有 1+1=0；在模 4，有 1+1=2≠0，又有非零的 2×2=0。域無這種零因子，因此不能將 F_4 認作模 4 的環。

11.3 練習

1 **B14-C11-Q01** 在 F_4 算 α+α。

2 **B14-C11-Q02** 在 F_4 算 1−α。

3 **B14-C11-Q03** 在 F_4 算 α^2。

4 **B14-C11-Q04** 用關係式算 (α+1)α。

5 **B14-C11-Q05** 1、α、α+1 各有何乘法反元素？

6 **B14-C11-Q06** 在 F_4 算 (α+1)/α。

7 **B14-C11-Q07** 在 F_4 可否計算 α/0？

8 **B14-C11-Q08** 算 $(\alpha+1)^3$，為何不等於 0？

9 **B14-C11-Q09** 在 F_7 算 6/2。

10 **B14-C11-Q10** F_4 和模 4 的加法群也會不同構嗎？

11.4 完整解答

Q01
兩係數各模 2 相加，一次係數 1+1=0，常數仍 0，故為 0。

Q02
特徵 2 意味 α+α=0，所以 −α=α，結果為 1+α。

Q03
關係 t^2+t+1 在商裡為 0，且負號等於正號，因此 $\alpha^2=\alpha+1$。

Q04
展開為 $\alpha^2+\alpha=(\alpha+1)+\alpha=1$。這也驗出兩者互為反元素。

Q05
1 乘自己得 1；α 和 α+1 相乘得 1，且乘法交換。故對應為 1、α+1、α。

Q06
α 的逆元是 α+1，故求 $(\alpha+1)^2$。平方後得到 $\alpha^2+1=\alpha$，回驗 $\alpha\cdot\alpha=\alpha+1$。

Q07
不能。0 乘任何元素還是 0，不會成 1，沒有可乘的逆元；也不存在 $0\cdot x=\alpha$ 的解。

Q08
平方等於 α，再乘 α+1 得 1。非零元素的乘積在域中不能變成 0。

Q09
2 的逆元是 4（$2\times4=8\equiv1$）。$6\times4=24$，模 7 餘 3，且 $2\times3=6$。

Q10
會不同構。F_4 的所有非零元素加自己都得 0，階 2；模 4 的 1 需加四次才回 0，階 4。群同構會保留階。

第12章 結構證明與表示

12.1 找一個保持運算的翻譯，而不只排列符號

比較兩個結構，先說清比較的是群、環還是域。群同構須是保持群運算的雙射；環同構也是雙射，並且同時保加法與乘法。對有限運算表，若能同時換列名、欄名和格內元素名而得到另一張表，該換名正是同構。只數表格大小、只保其中一種運算或只找到一個雙射，均不足夠。

證明同構可分成四個檢查：映射良定、保運算、單射、滿射。證明不同構時，可比較結構本身的不變量，例如元素階、交換性或零因子。只要同構應保留的量不同，就足以排除同構。幾個不變量相同，只表示這幾關沒有排除。核則屬於指定的同態，可用來判斷該映射是否單射。例如同是 C_4 到 C_4，恆等映射的核是 $\{0\}$，倍加映射的核是 $\{0,2\}$。

表示是把抽象操作實現為可算的變換。在三維 F_2 向量空間取標準基底 e_1、e_2、e_3。對 $\sigma \in S_3$，$P(\sigma)$ 將 e_i 送到第 $\sigma(i)$ 個標準基向量，這個向量就是矩陣的第 i 欄。先做 τ 再做 σ，對每個基向量都得到 $P(\sigma)P(\tau)e_i = P(\sigma\tau)e_i$，故保運算。$P(\sigma^{-1})$ 是反矩陣，因此 P 是到可逆矩陣群 $GL_3(F_2)$ 的同態。可從各欄讀回 $\sigma(i)$，故 P 單射，稱為忠實。像是目標群的真子群。例如三階矩陣 $I + E_{12}$ 的平方為 I，但第二欄是 $e_1 + e_2$，不是任一基向量，故它不在像中。

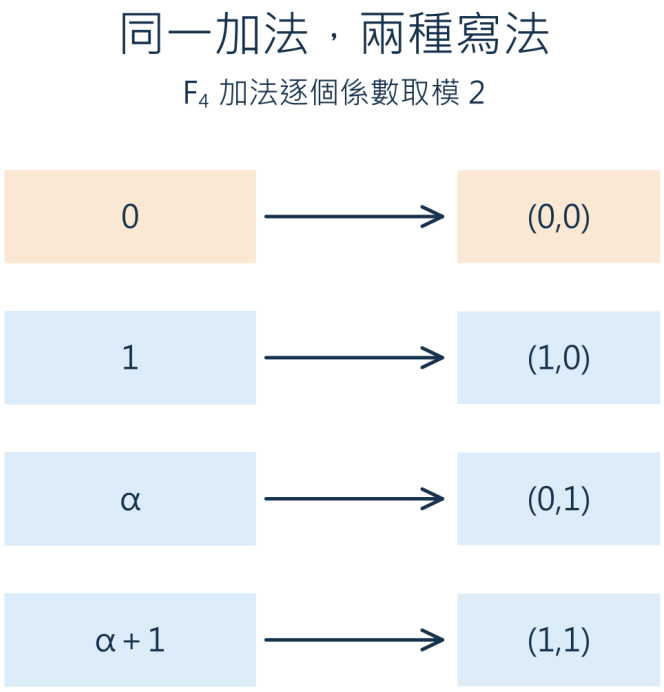


圖23 | F_4 的四個元素依係數對應到 (0,0)、(1,0)、(0,1)、(1,1)；兩邊加法逐位模 2。

12.2 四個例題

例題1 同一加法用兩種符號寫

把 $a+b\alpha$ 送成 (a,b)。兩個係數各有兩值，所以配對有 $2\times2=4$ 個且唯一；F_4 的加法逐係數模 2，因此與 $C_2\times C_2$ 的加法同構。例如 $\alpha+(\alpha+1)=1$，對應 $(0,1)+(1,1)=(1,0)$。

例題2 同一有限域還有另一個群

只取 F_4 的非零元素，有 $4-1=3$ 個，以乘法構成群。α 的冪依序是 1、α、$\alpha+1$ 再回 1，故 $k\mapsto\alpha^k$ 定義 C_3 到非零乘法群的同構。與例題 1 的四元素加法群不同，兩者先選的運算不同。

例題3 相同大小仍不能擁有不同的階

C_4 的 1 有階 4，$C_2 \times C_2$ 的每個非單位元素都只有階 2。群同構必保最小正回返次數，找不到 1 的對應，故不同構。

例題4 用基底像做出置換的矩陣

P((12)) 的三欄是 e_2、e_1、e_3。因此平方會把兩基向量交換兩次，得單位矩陣。如對所有置換取這種矩陣，逐欄可讀回被換到哪個標籤，故 S_3 的 3×2×1 個操作都不同。

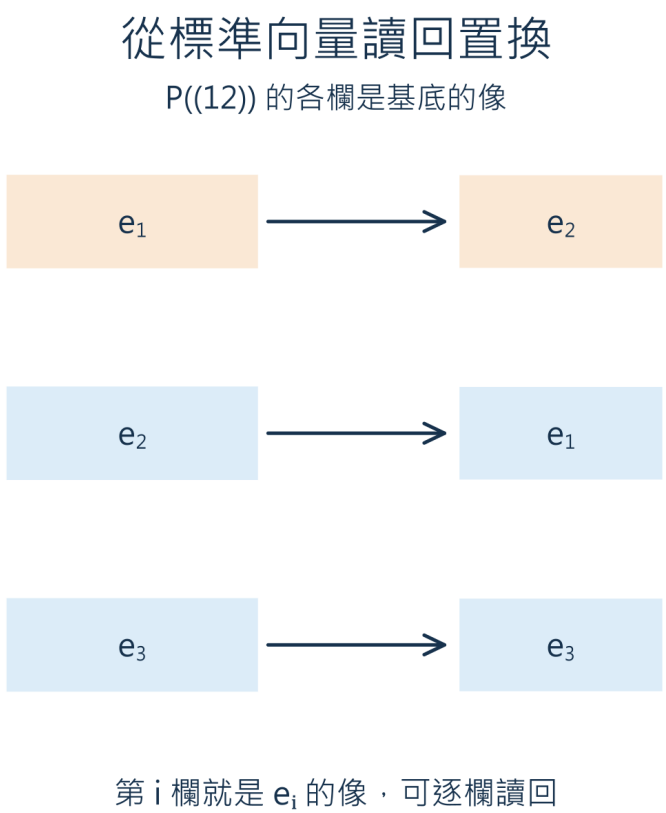


圖24 | 置換 (12) 送 e_1 到 e_2、e_2 到 e_1、e_3 不動；從像即可讀回這個操作。

12.3 練習

1 **B14-C12-Q01** C_4 的平移 $x \mapsto x+1$ 是雙射，為什麼不算同構？

2 **B14-C12-Q02** C_4 的倍加 $x \mapsto 2x$ 是同態，為何不是同構？

3 **B14-C12-Q03** 在 C_5，$x \mapsto -x$ 是加法同構嗎？

4 **B14-C12-Q04** 已知 f 是雙射且保乘法，為什麼 f^{-1} 也保乘法？

5 **B14-C12-Q05** 證明群同構會保留有限的元素階。

6 **B14-C12-Q06** 為什麼 F_4 的乘法群不放入 0？

7 **B14-C12-Q07** P((23)) 的第 2 欄是什麼？

8 **B14-C12-Q08** 這個置換矩陣表示的反矩陣為何存在？

9 **B14-C12-Q09** 只交換運算表的兩列，不換欄或結果標籤，能宣稱看見同構嗎？

10 **B14-C12-Q10** $C_6 \to C_3$ 取餘數。如何由核與像讀出一個商同構？

12.4 完整解答

Q01

單位 0 被送到 1，沒有保持加法的單位。雙射只是集合上的要求，仍要保運算。

Q02

倍加保加法、公式良定，但 0 與 2 都送到 0，非單射。其像只有 0、2，也未滿射到 C_4。

Q03

是。負號與加法相容，且再取一次負號回到原值，故有反函數、是雙射。

Q04

對任意目標 u、v，取 $a=f^{-1}(u)$、$b=f^{-1}(v)$。因 $f(ab)=uv$，再取 f^{-1} 得 $f^{-1}(uv)=ab=f^{-1}(u)f^{-1}(v)$。

Q05

對每個正整數 k，有 $f(g^k)=f(g)^k$。又 f 單射且保單位，$g^k=e$ 恰當 $f(g)^k=e$；最小正指數因此相同。

Q06

若放入 0，0 乘任意元都等於 0，找不到乘到 1 的反元素，無法成群。非零乘積則在域裡仍非零。

Q07

第 2 欄代表 e_2 的像；(23) 將 2 送到 3，所以第 2 欄是 e_3，即從上到下 0、0、1。

Q08

矩陣乘法對應置換合成，$P(\sigma)P(\sigma^{-1})=P(e)$ 且反序也成立；$P(e)$ 是單位矩陣，所以 $P(\sigma^{-1})$ 就是逆。

Q09

不能。要用同一個換名同步處理兩個輸入與輸出，才檢查到 $f(ab)=f(a)f(b)$；只換列並不知道三個位置用了同一映射。

Q10

核為 $\{0,3\}$，像為全部 C_3，故 $C_6/\{0,3\}\cong C_3$。源的六個類先按每兩個一組壓縮，商只有 $6/2=3$ 個。