解　答

第 14 章
環和模數算術

14.1 節

1. (例題 14.5): $-a = a, -b = e, -c = d, -d = c, -e = b$
(例題 14.6): $-s = s, -t = y, -v = x, -w = w, -x = v, -y = t$

3. **a)**
$$\begin{aligned}(a+b)+c &= (b+a)+c && +\text{的交換律}\\ &= b+(a+c) && +\text{的結合律}\\ &= b+(c+a) && +\text{的交換律}\end{aligned}$$

b)
$$\begin{aligned}d+a(b+c) &= d+(ab+ac) && \cdot\text{對}+\text{的分配律}\\ &= (d+ab)+ac && +\text{的結合律}\\ &= (ab+d)+ac && +\text{的交換律}\\ &= ab+(d+ac) && +\text{的結合律}\end{aligned}$$

c)
$$\begin{aligned}c(d+b)+ab &= ab+c(d+b) && +\text{的交換律}\\ &= ab+(cd+cb) && \cdot\text{對}+\text{的分配律}\\ &= ab+(cb+cd) && +\text{的交換律}\\ &= (ab+cb)+cd && +\text{的結合律}\\ &= (a+c)b+cd && \cdot\text{對}+\text{的分配律}\end{aligned}$$

5. a) (i) 封閉的二元運算 $\oplus$ 是可結合的。對所有 a，b，$c \in \mathbf{Z}$，我們發現

$$(a \oplus b) \oplus c = (a+b-1) \oplus c = (a+b-1)+c-1 = a+b+c-2.$$

且

$$a \oplus (b \oplus c) = a \oplus (b+c-1) = a+(b+c-1)-1 = a+b+c-2.$$

(ii) 對封閉的二元運算 $\odot$ 及所有 a，b，$c \in \mathbf{Z}$，我們有

$$\begin{aligned}(a \odot b) \odot c &= (a+b-ab) \odot c = (a+b-ab)+c-(a+b-ab)c\\ &= a+b-ab+c-ac-bc+abc = a+b+c-ab-ac-bc+abc,\end{aligned}$$

且

$$\begin{aligned}a \odot (b \odot c) &= a \odot (b+c-bc) = a+(b+c-bc)-a(b+c-bc)\\ &= a+b+c-bc-ab-ac+abc = a+b+c-ab-ac-bc+abc.\end{aligned}$$

因此，封閉的二元運算 $\odot$ 亦是可結合的。

(iii) 對任意整數 a，b，c，我們發現

$$\begin{aligned}(b \oplus c) \odot a &= (b+c-1) \odot a = (b+c-1)+a-(b+c-1)a\\ &= b+c-1+a-ba-ca+a = a+a+b+c-1-ba-ca,\end{aligned}$$

且

$$(b \odot a) \oplus (c \odot a) = (b + a - ba) \oplus (c + a - ca)$$
$$= (b + a - ba) + (c + a - ca) - 1$$
$$= a + a + b + c - 1 - ba - ca.$$

因此，第二個分配律亦成立。

c) 除了 0 之外，唯一另一個可逆元素是 2，因為 $2 \odot 2 = 2 + 2 - (2 \cdot 2) = 0$，$(\mathbf{Z}, \oplus, \odot)$ 的單位元素。

d) 此環是一個整環，但不是一個體。對所有 a，$b \in \mathbf{Z}$，我們看到 $a \odot b = 1$ (零元素) $\Rightarrow a + b - ab = 1 \Rightarrow a(1 - b) = (1 - b) \Rightarrow (a - 1)(1 - b) = 0$ $\Rightarrow a = 1$ 或 $b = 1$，所以沒有零的真因數在 $(\mathbf{Z}, \oplus, \odot)$ 上。

7. 由前面習題，我們知道需決定在 k，m 上的條件以使分配律成立。因 $\odot$ 是可交換的，我們可將焦點集中在這些定律中的一個即可。

若 x，y，$z \in \mathbf{Z}$，則

$$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$$
$$\Rightarrow x \odot (y + z - k) = (x + y - mxy) \oplus (x + z - mxz)$$
$$\Rightarrow x + (y + z - k) - mx(y + z - k) = (x + y - mxy) + (x + z - mxz) - k$$
$$\Rightarrow x + y + z - k - mxy - mxz + mkx = x + y - mxy + x + z - mxz - k$$
$$\Rightarrow mkx = x \Rightarrow mk = 1 \Rightarrow m = k = 1 \text{ 或 } m = k = -1$$，因為 m，$k \in \mathbf{Z}$。

9. a) 我們將證明分配律中的一個。若 a，b，$c \in \mathbf{Q}$，則

$$a \odot (b \oplus c) = a \odot (b + c + 7)$$
$$= a + (b + c + 7) + [a(b + c + 7)]/7$$
$$= a + b + c + 7 + (ab/7) + (ac/7) + a,$$

而

$$(a \odot b) \oplus (a \odot c) = (a \odot b) + (a \odot c) + 7$$
$$= a + b + (ab/7) + a + c + (ac/7) + 7$$
$$= a + b + c + 7 + (ab/7) + (ac/7) + a.$$

而且，有理數 -7 是零元素，且每個有理數 a 的加法反元素是 $-14 - a$。

c) 對每個 $a \in \mathbf{Q}$，$a = a \odot u = a + u + (au/7) \Rightarrow u[1 + (a/7)] = 0 \Rightarrow u = 0$，因為 a 是任意的。因此有理數 0 是這個環的單位元素，現在令 $a \in \mathbf{Q}$，其中 $a \neq -7$，環的零元素。我們能找到 $b \in \mathbf{Q}$ 使得 $a \odot b = 0$，亦即 $a + b + (ab/7) = 0$ 嗎？得 $a + b + (ab/7) = 0 \Rightarrow b = (1 + (a/7)) = -a$

$\Rightarrow b=(-a)/[1+(a/7)]$。因此，每個有理數，除 -7 之外，是一個可逆元。

11. b) $1,\ -1,\ i,\ -i$

13. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = (1/(ad-bc))\begin{bmatrix} d & -b \\ -c & a \end{bmatrix},\quad ad-bc\neq 0$

15. a) $xx=x(t+y)=xt+xy=t+y=x$

$yt=(x+t)t=xt+tt=t+t=s$

$yy=y(t+x)=yt+yx=s+s=s$

$tx=(y+x)x=yx+xx=s+x=x$

$ty=(y+x)y=yy+xy=s+y=y$

b) 因為 $tx=x\neq t=xt$，此環不可交換。

c) 沒有單位元素，因此沒有可逆元。

d) 此環既不是整環也不是體。

14.2 節

1. 定理 14.10(a)。若 $(S,\ +,\ \cdot)$ 是 R 的一個子環，則 $a-b$，$ab\in S$，對所有 a，$b\in S$。反之，因為 $S\neq\emptyset$，令 $a\in S$，則 $a-a=z\in S$，且 $z-a=-a\in S$。而且，若 $b\in S$，則 $-b\in S$，所以 $a-(-b)=a+b\in S$，且由定理 14.9，S 是一個子環。

3. a) $(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aua^{-1}=aa^{-1}=u$ 且 $(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)b=b^{-1}ub=b^{-1}b=u$，所以 ab 是一個可逆元。因為可逆元的乘法反元素唯一，所以 $(ab)^{-1}=b^{-1}a^{-1}$。

b) $A^{-1}=\begin{bmatrix} 2 & -7 \\ -1 & 4 \end{bmatrix}$ $B^{-1}=\begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix}$ $(AB)^{-1}=\begin{bmatrix} 4 & -15 \\ -9 & 34 \end{bmatrix}$

$(BA)^{-1}=\begin{bmatrix} 16 & -39 \\ -9 & 22 \end{bmatrix}$ $B^{-1}A^{-1}=\begin{bmatrix} 4 & -15 \\ -9 & 34 \end{bmatrix}$

5. $(-a)^{-1}=-(a^{-1})$

7. $z\in S$，$T\Rightarrow z\in S\cap T\Rightarrow S\cap T\neq\emptyset$。$a$，$b\in S\cap T\Rightarrow a$，$b\in S$ 且 a，$b\in T\Rightarrow a+b$，$ab\in S$ 且 $a+b$，$ab\in T\Rightarrow a+b$，$ab\in S\cap T$。$a\in S\cap T\Rightarrow a\in S$ 且 $a\in T\Rightarrow -a\in S$ 且 $-a\in T\Rightarrow -a\in S\cap T$。所以 $S\cap T$ 是 R 的子環。

9. 若否，存在 a，$b\in S$ 滿足 $a\in T_1$，$a\notin T_2$ 且 $b\in T_2$，$b\notin T_1$。因為 S 是 R 的一個子環，得 $a+b\in S$。因此，$a+b\in T_1$ 或 $a+b\in T_2$。

不失一般性假設 $a+b\in T_1$，因為 $a\in T_1$，我們有 $-a\in T_1$，所以由 T_1 上加法封閉性，我們發現 $(-a)+(a+b)=(-a+a)+b=b\in T_1$，得一矛盾。因此，$S\subseteq T_1\cup T_2\Rightarrow S\subseteq T_1$ 或 $S\subseteq T_2$。

11. b) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ **c)** $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

d) S 是一個整環，而 R 是一個含單位元素的不可交換環。

13. 因為 $za=z$，得 $z \in N(a)$ 且 $N(a) \neq \emptyset$。若 r_1，$r_2 \in N(a)$，則 $(r_1-r_2)a=r_1a-r_2a=z-z=z$，所以 $r_1-r_2 \in N(a)$。最後 $r \in N(a)$ 且 $s \in R$，則 $(rs)a=(sr)a=s(ra)=sz=z$，所以 rs，$sr \in N(a)$。因此，由定義 14.6，$N(a)$ 是一個理想。

15. 2

17. a) $a=au \in aR$ 因為 $u \in R$，所以 $aR \neq \emptyset$。若 ar_1，$ar_2 \in aR$，則 $ar_1-ar_2=a(r_1-r_2) \in aR$。而且，對 $ar_1 \in aR$ 且 $r \in R$，我們有 $r(ar_1)=(ar_1)^r=a(r_1r) \in aR$。因此 aR 是 R 的一個理想。

b) 令 $a \in R$，$a \neq z$。則 $a=au \in aR$ 所以 $aR=R$。因為 $u \in R=aR$，$u=ar$ 對某些 $r \in R$，且 $r=a^{-1}$。因此，R 是一個體。

19. a) $\binom{4}{2}(49)$ **b)** 7^4 **c)** 是的，元素 (u, u, u, u) **d)** 4^4

21. b) 若 R 有一個單位元素 u，定義 $a^0=u$，對 $a \in R$，$a \neq z$。若 a 是 R 的一個可逆元，定義 a^{-n} 為 $(a^{-1})^n$，對 $n \in \mathbf{Z}^+$。

14.3 節

1. a) (i) 是 (ii) 否 (iii) 是 **b)** (i) 否 (ii) 是 (iii) 是

3. a) −6, 1, 8, 15 **b)** −9, 2, 13, 24 **c)** −7, 10, 27, 44

5. 因為 $a \equiv b \pmod{n}$，我們可記 $a=b+kn$ 對某些 $k \in \mathbf{Z}$，且 $m|n \Rightarrow n=\ell m$ 對某些 $\ell \in \mathbf{Z}$。因此，$a=b+kn=b+(k\ell)m$ 且 $a \equiv b \pmod{m}$。

7. 令 $a=8$，$b=2$，$m=6$，且 $n=2$。則 $\gcd(m, n)=\gcd(6, 2)=2>1$，$a \equiv b \pmod{m}$ 且 $a \equiv b \pmod{n}$。且 $a-b=8-2=6 \neq k(12)=k(mn)$，對任一 $k \in \mathbf{Z}$。因此 $a \not\equiv b \pmod{mn}$。

9. 對 n 為奇數，考慮 $n-1$ 個數 1，2，3，…，$n-3$，$n-2$，$n-1$ 為 $(n-1)/2$ 對：1 和 $(n-1)$，2 和 $(n-2)$，3 和 $(n-3)$，…，$n-\left(\frac{n-1}{2}\right)-1$ 和 $n-\left(\frac{n-1}{2}\right)$。每對和是 n，其同餘 0 模 n。因此，$\sum_{i=1}^{n-1} i \equiv 0 \pmod{n}$。當 n 是偶數時，考慮 $n-1$ 個數 1，2，3，…，$(n/2)-1$，$(n/2)$，$(n/2)+1$，…，$n-3$，$n-2$，$n-1$ 為 $(n/2)-1$ 對，即 1 和 $n-1$，2 和 $n-2$，3 和 $n-3$，…，$(n/2)-1$ 和 $(n/2)+1$，及單一數 $(n/2)$。每對和是 n，或 0 模 n，所以 $\sum_{i=1}^{n-1} i \equiv (n/2) \pmod{n}$。

11. b) 否，$2 \mathrel{\mathcal{R}} 3$ 且 $3 \mathrel{\mathcal{R}} 5$，但 $5 \not\mathrel{\mathcal{R}} 8$。而且，$2 \mathrel{\mathcal{R}} 3$ 且 $2 \mathrel{\mathcal{R}} 5$，但 $4 \not\mathrel{\mathcal{R}} 15$。

13. $[17]^{-1}=[831]$ **b)** $[100]^{-1}=[111]$ **c)** $[777]^{-1}=[735]$

15. a) 16 個可逆元，0 個真零約數 **b)** 72 個可逆元，44 個真零約數

c) 1116 個可逆元，0 個真零約數

17. $\left[\binom{334}{3}+2\binom{333}{3}+\binom{334}{1}\binom{333}{1}^2\right] \Big/ \binom{1000}{3}$

19. a) 對 $n=0$，我們有 $10^0=1=1(-1)^0$，所以 $10^0\equiv(-1)^0 \pmod{11}$。[因 $10-(-1)=11$，$10\equiv(-1)\pmod{11}$，或 $10^1\equiv(-1)^1\pmod{11}$。因此，結果對 $n=1$ 亦成立。] 假設結果對 $n=k\geq 1$ 為真，且考慮 $k+1$ 的情形，則因 $10^k\equiv(-1)^k\pmod{11}$ 且 $10\equiv(-1)\pmod{11}$。我們有 $10^{k+1}=10^k\cdot 10\equiv(-1)^k(-1)=(-1)^{k+1}\pmod{11}$。由數學歸納法原理，結果對所有 $n\in\mathbf{N}$ 成立。

b) 若 $x_nx_{n-1}\cdots x_2x_1x_0 = x_n\cdot 10^n + x_{n-1}\cdot 10^{n-1}+\cdots+x_2\cdot 10^2+x_1\cdot 10+x_0$ 表一個 $(n+1)$- 位整數，則

$$x_nx_{n-1}\cdots x_2x_1x_0 \equiv (-1)^n x_n + (-1)^{n-1}x_{n-1}+\cdots+x_2-x_1+x_0 \pmod{11}.$$

證明：

$$\begin{aligned} x_nx_{n-1}\cdots x_2x_1x_0 &= x_n\cdot 10^n + x_{n-1}\cdot 10^{n-1}+\cdots+x_2\cdot 10^2+x_1\cdot 10+x_0 \\ &\equiv x_n(-1)^n + x_{n-1}(-1)^{n-1}+\cdots+x_2(-1)^2+x_1(-1)+x_0 \\ &= (-1)^n x_n + (-1)^{n-1}x_{\bar{n}-1}+\cdots+x_2-x_1+x_0 \pmod{11}. \end{aligned}$$

21. 令 $g=\gcd(a, n)$，$h=\gcd(b, n)$。[$a\equiv b\pmod{n}$] $\Rightarrow$ [$a=b+kn$，對某些 $k\in\mathbf{Z}$] $\Rightarrow$ [$g|b$ 且 $h|a$]。[$g|b$ 且 $g|n$] $\Rightarrow g|h$; [$h|a$ 且 $h|n$] $\Rightarrow h|g$。因為 g，$h>0$，得 $g=h$。

23. (1) 明語

	a	*ℓ*	*ℓ*	*g*	*a*	*u*	*ℓ*	*i*	*s*	*d*	*i*	*v*	*i*	*d*	*e*	*d*
(2)	0	11	11	6	0	20	11	8	18	3	8	21	8	3	4	3
(3)	3	14	14	9	3	23	14	11	21	6	11	24	11	6	7	6
(4) 密語	*D*	*O*	*O*	*J*	*D*	*X*	*O*	*L*	*V*	*G*	*L*	*Y*	*L*	*G*	*H*	*G*

i	*n*	*t*	*o*	*t*	*h*	*r*	*e*	*e*	*p*	*a*	*r*	*t*	*s*
8	13	19	14	19	7	17	4	4	15	0	17	19	18
11	16	22	17	22	10	20	7	7	18	3	20	22	21
L	*Q*	*W*	*R*	*W*	*K*	*U*	*H*	*H*	*S*	*D*	*U*	*W*	*V*

對每個 θ 在列 (2)，在它之下的列 (3) 相對應結果是 $(\theta+3)$ **mod** 26。

25. a) (24)(8)=192 **b)** (25)(20)=500 **c)** (27)(18)=486 **d)** (30)(8)=240

27. a) 9 **b)** 10, 15, 2, 13, 11, 1, 8, 5, 9

29. 證明： (利用數學歸納法)：

[注意對 $n\geq 1$，$(a^n-1)/(a-1)=a^{n-1}+a^{n-2}+\cdots+1$，其可被計算於環 $(\mathbf{Z}, +, \cdot)$ 裡。]

當 $n=0$，$a^0x_0+c[(a^0-1)/(a-1)]\equiv x_0+c[0/(a-1)]\equiv x_0 \pmod{m}$，所以公式在此第一基底 $(n=0)$ 為真。假設結果對 n (≥ 0)，我們有 $x_n\equiv a^nx_0+c[(a^n-1)/(a-1)]\pmod{m}$，$0\leq x_n<m$。繼續至下一個情形，我們學到

$$\begin{aligned} x_{n+1} &\equiv ax_n + c \pmod m \\ &\equiv a[a^n x_0 + c[(a^n - 1)/(a-1)]] + c \pmod m \\ &\equiv a^{n+1}x_0 + ac[(a^n - 1)/(a-1)] + c(a-1)/(a-1) \pmod m \\ &\equiv a^{n+1}x_0 + c[(a^{n+1} - a + a - 1)/(a-1)] \pmod m \\ &\equiv a^{n+1}x_0 + c[(a^{n+1} - 1)/(a-1)] \pmod m \end{aligned}$$

且我們選 x_{n+1} 使得 $0 \le x_{n+1} < m$。現由數學歸納法原理得

$$x_n \equiv a^n x_0 + c[(a^n - 1)/(a-1)] \pmod m, \quad 0 \le x_n < m.$$

31. 證明：令 n，$n+1$，及 $n+2$ 為三個連續整數。則 $n^3+(n+1)^3+(n+2)^3 = n^3+(n^3+3n^2+3n+1)+(n^3+6n^2+12n+8) = (3n^3+15n)+9(n^2+1)$。所以，我們考慮 $3n^3+15n = 3n(n^2+5)$。若 $3|n$，則完成。若否，則 $n \equiv 1 \pmod 3$ 或 $n \equiv 2 \pmod 3$。若 $n \equiv 1 \pmod 3$，則 $n^2+5 \equiv 1+5 \equiv 0 \pmod 3$，所以，$3|(n^2+5)$。若 $n \equiv 2 \pmod 3$，則 $n^2+5 \equiv 9 \equiv 0 \pmod 3$，且 $3|(n^2+5)$。所有情形現均涵蓋，所以我們有 $3|[n(n^2+5)]$。因此，$9|[3n(n^2+5)]$，且因此，9 整除 $(3n^3+15n)+9(n^2+1) = n^3+(n+1)^3+(n+2)^3$。

33. $\displaystyle\sum_{k=0}^{n-1} p(k(n+1), n, n) = \frac{1}{n+1}\binom{2n}{n}$，第 n 個 Catalan 數。

35. a) 112 **b)** 031-43-3464

37. a) 1，28，14，34，2，3(＝2＋1)，15(＝14＋1)，4(＝3＋1) **b)** 1，2，3，4，5

14.4 節

1. $s \to 0$，$t \to 1$，$v \to 2$，$w \to 3$，$x \to 4$，$y \to 5$

3. 令 $(R, +, \cdot)$，$(\mathbf{Z}, \oplus, \odot)$，及 $(T, +', \cdot')$ 為環。對所有 a，$b \in R$，$(g \circ f)(a+b) = g(f(a+b)) = g(f(a) \oplus f(b)) = g(f(a)) +' g(f(b)) = (g \circ f)(a) +' (g \circ f)(b)$。而且，$(g \circ f)(a \cdot b) = g(f(a \cdot b)) = g(f(a) \odot f(b)) = g(f(a) \cdot' g(f(b)) = (g \circ f)(a) \cdot' (g \circ f)(b)$。因此，$g \circ f$ 是一個環同態函數。

5.a) 因為 $f(z_R) = z_S$，得 $z_R \in K$ 且 $K \neq \emptyset$。若 x，$y \in K$，則 $f(x-y) = f(x+(-y)) = f(x) \oplus f(-y) = f(x) \ominus f(y) = z_S \ominus z_S = z_S$，所以 $x-y \in K$。最後，若 $x \in K$ 且 $r \in R$，則 $f(rx) = f(r) \odot f(x) = f(r) \odot z_S = z_S$，且 $f(xr) = f(x) \odot f(r) = z_S \odot f(r) = z_S$，所以 rx，$xr \in K$。因此，K 是 R 的一個理想。

b) 核集是 $\{6n | n \in \mathbf{Z}\}$。

7. a)

x (在$\mathbf{Z}_{20}$)	$f(x)$ (在$\mathbf{Z}_4 \times \mathbf{Z}_5$)	x (在$\mathbf{Z}_{20}$)	$f(x)$ (在$\mathbf{Z}_4 \times \mathbf{Z}_5$)
0	(0, 0)	10	(2, 0)
1	(1, 1)	11	(3, 1)
2	(2, 2)	12	(0, 2)
3	(3, 3)	13	(1, 3)
4	(0, 4)	14	(2, 4)
5	(1, 0)	15	(3, 0)
6	(2, 1)	16	(0, 1)
7	(3, 2)	17	(1, 2)
8	(0, 3)	18	(2, 3)
9	(1, 4)	19	(3, 4)

b) (i) $f(17)(19)+(12)(14)=(1, 2)(3, 4)+(0, 2)(2, 4)=(3, 3)+(0, 3)=(3, 1)$，且 $f^{-1}(3, 1)=11$

9. a) 4 **b)** 1 **c)** 否

11. 否，$\mathbf{Z}_4$ 有兩個可逆元，而例題 14.4 的環僅有一個可逆元。

13. $397+k(648)$，$k \in \mathbf{Z}$ **15.** $173+k(210)$，$k \in \mathbf{Z}$

補充習題

1. a) 錯。令 $R=\mathbf{Z}$ 且 $S=\mathbf{Z}^+$。 **b)** 錯。令 $R=\mathbf{Z}$ 且 $S=\{2x|x \in \mathbf{Z}\}$。

c) 錯。令 $R=M_2(\mathbf{Z})$ 且 $S=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| a \in \mathbf{Z}\right\}$. **d)** 真。

e) 錯。環 $(\mathbf{Z}, +, \cdot)$ 是 $(\mathbf{Q}, +, \cdot)$ 的一個子環 (但不是一個體)。

f) 錯。對任一質數 p，$\{a/(p^n)|a, n \in \mathbf{Z}, n \geq 0\}$ 是 $(\mathbf{Q}, +, \cdot)$ 的一個子環。

g) 錯。考慮表 14.6 的體。 **h)** 真。

3. a) $[a+a=(a+a)^2=a^2+a^2+a^2+a^2=(a+a)+(a+a)] \Rightarrow [a+a=2a=\mathbf{z}]$，因此 $-a=a$。

b) 對每個 $a \in R$，$a+a=z \Rightarrow a=-a$。對 a，$b \in R$，$(a+b)=(a+b)^2=a^2+ab+ba+b^2=a+ab+ba+b \Rightarrow ab+ba=z \Rightarrow ab=-ba=ba$，所以 R 是可交換的。

5. 因為 $az=z=za$，對所有 $a \in R$，我們有 $z \in C$ 且 $C \neq \emptyset$。若 x，$y \in C$，則 $(x+y)a=xa+ya=ax+ay=a(x+y)$，$(xy)a=x(ya)=x(ay)=(xa)y=(ax)y=a(xy)$，且 $(-x)a=-(xa)=-(ax)=a(-x)$，對所有 $a \in R$，所以 $x+y$，xy，$-x \in C$。因此，C 是 R 的一個子環。

7. b) 因 m，n 互質，我們可記 $1=ms+nt$，其中 s，$t \in \mathbf{Z}$。由於 m，$n>0$，得 s，t 中必有一個為正，且另一個為負。假設 (不失一般性) s 是負的使得 $1-ms=nt>0$。

則 $a^n=b^n \Rightarrow (a^n)^t=(b^n)^t \Rightarrow a^{nt}=b^{nt} \Rightarrow a^{1-ms}=b^{1-ms} \Rightarrow a(a^m)^{(-s)}=b(b^m)^{(-s)}$。

但以 $-s>0$ 且 $a^m=b^m$，我們有 $(a^m)^{(-s)}=(b^m)^{(-s)}$。因此，

$$([(a^m)^{(-s)} = (b^m)^{(-s)} \neq z] \wedge [a(a^m)^{(-s)} = b(b^m)^{(-s)}]) \Rightarrow a = b,$$

因為我們可使用乘法消去律於整環裡。

9. 令 $x=a_1+b_1$，$y=a_2+b_2$，對 a_1，$a_2 \in A$ 且 b_1，$b_2 \in B$。則 $x-y=(a_1-a_2)+(b_1-b_2) \in A+B$。若 $r \in R$ 且 $a+b \in A+B$，以 $a \in A$ 及 $b \in B$，則 $ra \in A$，$rb \in B$，且 $r(a+b) \in A+B$。同理，$(a+b)r \in A+B$，且 $A+B$ 是 R 的一個理想。

11. 考慮 x_1，x_1+x_2，$x_1+x_2+x_3$，$\cdots$，$x_1+x_2+x_3+\cdots+x_n$ 等數。若這些數中有一個是同餘 0 模 n，則結果成立。若否，則存在 $1 \le i<j \le n$ 滿足 $(x_1+x_2+\cdots+x_i) \equiv (x_1+\cdots+x_i+x_{i+1}+\cdots+x_j) \pmod{n}$。因此，$n$ 整除 $(x_{i+1}+\cdots+x_j)$。

13. a) 1875 **b)** 2914 **c)** 3/16

15. 證明：對所有 $n \in \mathbf{Z}$，我們發現 $n^2 \equiv 0 \pmod 5$，當 $5|n$ 或 $n^2 \equiv 1 \pmod 5$ 或 $n^2 \equiv 4 \pmod 5$。假設 5 不整除 a，b 或 c 中的任何一個，則

(i) $a^2+b^2+c^2 \equiv 3 \pmod 5$ ——當 $a^2 \equiv b^2 \equiv c^2 \equiv 1 \pmod 5$;

(ii) $a^2+b^2+c^2 \equiv 1 \pmod 5$ ——當 a^2，b^2，c^2 中的兩個各個是同餘 1 模 5 且另一個平方是同餘 4 模 5。

(iii) $a^2+b^2+c^2 \equiv 4 \pmod 5$ ——當 a^2，b^2，c^2 中有一個是同餘 1 模 5 且另兩個平方的每一個是同餘 4 模 5；或

(iv) $a^2+b^2+c^2 \equiv 2 \pmod 5$ ——當 $a^2 \equiv b^2 \equiv c^2 \equiv 4 \pmod 5$。

17. $(e_1+1)(e_2+1)\cdots(e_k+1)-1$

第 15 章
布林代數和轉換函數

15.1 節

1. a) 1 **b)** 1 **c)** 1 **d)** 1 **3. a)** 2^n **b)** $2^{(2^n)}$

5. a) d.n.f. $xyz+x\bar{y}z+x\bar{y}\bar{z}+xy\bar{z}+\bar{x}y\bar{z}$

c.n.f. $(x+y+z)(x+y+\bar{z})(x+\bar{y}+\bar{z})$

b) $f=\Sigma m(2, 4, 5, 6, 7)=\prod M(0, 1, 3)$

7. a) 2^{64} **b)** 2^6 **c)** 2^6

9. $m+k=2^n$ **11. a)** $y+x\bar{z}$ **b)** $x+y$ **c)** $wx+z$

13. a)

f	g	h	fg	$\overline{f}h$	gh	$fg+\overline{f}h+gh$	$fg+\overline{f}h$
0	0	0	0	0	0	0	0
0	0	1	0	1	0	1	1
0	1	0	0	0	0	0	0
0	1	1	0	1	1	1	1
1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	0	1	0	0	1	1
1	1	1	1	0	1	1	1

或者 $fg+\overline{f}h=(fg+\overline{f})(fg+h)=(f+\overline{f})(g+\overline{f})(fg+h)=$

$\mathbf{1}(g+\overline{f})(fg+h)=fgg+gh+\overline{f}fg+\overline{f}h=fg+gh+\mathbf{0}g+\overline{f}h=fg+gh+\overline{f}h.$

(ii) $fg+f\overline{g}+\overline{f}g+\overline{f}\,\overline{g}=f(g+\overline{g})+\overline{f}(g+\overline{g})=f\cdot\mathbf{1}+\overline{f}\cdot\mathbf{1}=f+\overline{f}=\mathbf{1}$

b) (i) $(f+g)(\overline{f}+h)(g+h)=(f+g)(\overline{f}+h)$

(ii) $(f+g)(f+\overline{g})(\overline{f}+g)(\overline{f}+\overline{g})=\mathbf{0}$

15. a) $f\oplus f=\mathbf{0}$; $f\oplus\overline{f}=\mathbf{1}$; $f\oplus\mathbf{1}=\overline{f}$; $f\oplus\mathbf{0}=f$

b) (i) $f\oplus g=\mathbf{0}\Leftrightarrow f\overline{g}+\overline{f}g=\mathbf{0}\Rightarrow f\overline{g}=\overline{f}g=\mathbf{0}$。[$f=1$ 且 $f\overline{g}=\mathbf{0}$] $\Rightarrow g=1$。

[$f=0$ 且 $\overline{f}g=\mathbf{0}$] $\Rightarrow g=0$。因此 $f=g$。

(iii) $\overline{f}\oplus\overline{g}=\overline{f}\,\overline{\overline{g}}+\overline{f}\overline{g}=\overline{f}g+f\overline{g}=f\overline{g}+\overline{f}g=f\oplus g$

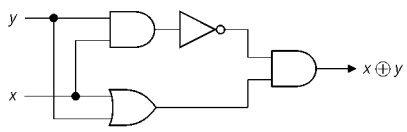
(iv) 這是唯一不為真的結果。當 f 有值 1，g 有值 0 且 h 有值 1 (或 g 有值 1 且 h 有值 0)，則 $f\oplus gh$ 有值 1 但 $(f\oplus g)(f\oplus h)$ 有值 0。

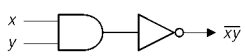
(v) $f\overline{g}\oplus fh=\overline{f\overline{g}}\,fh+f\overline{g}\,\overline{fh}=(\overline{f}+\overline{g})fh+fg(\overline{f}+\overline{h})=$
$\overline{f}fh+f\overline{g}h+f\overline{f}g+fg\overline{h}=f\overline{g}h+fg\overline{h}=f(\overline{g}h+g\overline{h})=f(g\oplus h)$

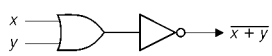
(vi) $\overline{f}\oplus g=\overline{f\overline{g}+fg}=fg+\overline{f}\,\overline{g}=f\oplus\overline{g}$
$\overline{f\oplus g}=f\overline{g}+\overline{f}g=(\overline{f}+g)(f+\overline{g})=\overline{f}\,\overline{g}+fg=\overline{f}\oplus g$

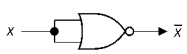
15.2 節

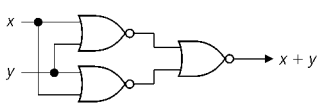
1. a) $x\oplus y=(x+y)(\overline{xy})$

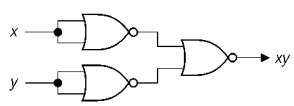


b) $\overline{xy}$ 

c) $\overline{x+y}$ 

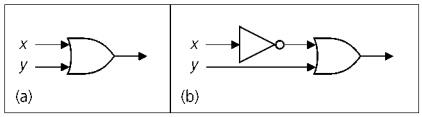
3. a) 



b) 

5. $f(w,x,y,z)=\overline{w}\,\overline{x}y\overline{z}+(w+x+\overline{y})z$

7.



a) 輸出是 $(x+\overline{y})(x+y)+y$。此簡化為 $x+(\overline{y}y)+y=x+0+y=x+y$，且提供我們較簡單的等價網路於圖 (a)。

b) 此處輸出是 $\overline{(x+\overline{y})}+(\overline{x}\,\overline{y}+y)$，其簡化為 $\overline{x}\,\overline{\overline{y}}+\overline{x}\,\overline{y}+y=\overline{x}y+\overline{x}\,\overline{y}+y=\overline{x}(y+\overline{y})+y=\overline{x}(1)+y=\overline{x}+y$。此說明圖 (b) 中的等價網路。

9. **a)** $f(w,x,y)=\overline{x}y+x\overline{y}$ **b)** $f(w,x,y)=x$ **c)** $f(w,x,y,z)=xz+\overline{x}\,\overline{z}$

d) $f(w,x,y,z)=w\overline{y}\,\overline{z}+x\overline{y}z+wyz+xy\overline{z}$ **e)** $f(w,x,y,z)=wy+w\overline{x}z+xyz$

f) $f(v,w,x,y,z)=\overline{v}\,\overline{w}x\overline{y}\,\overline{z}+vwx\overline{z}+\overline{v}\,\overline{x}y\overline{z}+\overline{w}\,\overline{x}z+v\overline{w}y+vyz$

11. a) 2 **b)** 3 **c)** 4 **d)** $k+1$

13. a) $|f^{-1}(0)|=|f^{-1}(1)|=8$ **b)** $|f^{-1}(0)|=12, |f^{-1}(1)|=4$

c) $|f^{-1}(0)|=14, |f^{-1}(1)|=2$ **d)** $|f^{-1}(0)|=4, |f^{-1}(1)|=12$

15.3 節

1. $uv+wvy+uxz+uyz+wz$

3. a) $f(w,x,y,z)=z$ **b)** $f(w,x,y,z)=\overline{x}\,\overline{y}\,\overline{z}+x\overline{y}z+xy\overline{z}$

c) $f(v,w,x,y,z)=v\overline{y}\,\overline{z}+\overline{w}\,\overline{x}yz+\overline{v}\,\overline{w}\,\overline{z}+\overline{v}x\overline{y}$

5. $\{b,d\}, \{c,d\}, \{d,f\}, \{a,g\}, \{e,f\}, \{b,e\}, \{c,e\}, \{a,f\}, \{b,g\}, \{c,g\}$

15.4 節

3. a) 30 **b)** 30 **c)** 1 **d)** 21 **e)** 30 **f)** 70

5. a) $w\le 0 \Rightarrow w\cdot 0=w$。但由定理 15.3(a)，$w\cdot 0=0$。

c) $y\le z \Rightarrow yz=y$，且 $y\le\overline{z}\Rightarrow y\overline{z}=y$。因此 $y=yz=(y\overline{z})z=y(\overline{z}z)=y\cdot 0=0$。

7. $y\le x$

9. 由定理 15.5(a)，且 x_1，x_2 為相異原子，若 $x_1x_2\neq 0$，則 $x_1=x_1x_2=x_2x_1=x_2$，得一矛盾。

11. a) $f(0)=f(x\overline{x})$ 對每個 $x\in\mathcal{B}_1$。$f(x\overline{x})=f(x)f(\overline{x})=f(x)\overline{f(x)}=0$。

b) 由 (a)，利用對偶性，成立。

c) $x\le y\iff xy=x\Rightarrow f(xy)=f(x)\Rightarrow f(x)f(y)=f(x)\iff f(x)\le f(y)$

13. a) $f(xy)=f\overline{(\overline{x}+\overline{y})}=\overline{f(\overline{x}+\overline{y})}=\overline{f(\overline{x})+f(\overline{y})}=\overline{f(\overline{x})}\cdot\overline{f(\overline{y})}=f(\overline{\overline{x}})\cdot f(\overline{\overline{y}})=f(x)\cdot f(y)$

b) 令 $\mathcal{B}_1$，$\mathcal{B}_2$ 為布林代數滿足 $f:\mathcal{B}_1\to\mathcal{B}_2$ 是一對一且映成，則 f 是一個同構函數若 $f(\overline{x})=\overline{f(x)}$ 且 $f(xy)=f(x)f(y)$ 對所有 $x, y\in\mathcal{B}_1$。[由 (a)，利用對偶性，成立。]

15. 對所有 $1\le i\le n$，$(x_1+x_2+\cdots+x_n)x_i=x_1x_i+x_2x_i+\cdots+x_{i-1}x_i+x_ix_i+x_{i+1}x_i+\cdots x_nx_i=0+0+\cdots+0+x_i+0+0\cdots+0=x_i$，由定理 15.5(b)。因

此，由定理 15.7 得 $(x_1+x_2+\cdots+x_n)x=x$ 對所有 $x\in\mathcal{B}$。因為 1 是唯一的 (由習題 10) ，我們得 $1=x_1+x_2+\cdots+x_n$。

補充習題

1. a) 當 $n=2$，x_1+x_2 表 x_1 和 x_2 的布林和。對 $n\geq 2$，我們以 $(x_1+x_2+\cdots+x_n)+x_{n+1}$ 遞迴定義 $x_1+x_2+\cdots+x_n+x_{n+1}$。 (類似定義可被給布林乘積)。對 $n=2$，$\overline{x_1+x_2}=\overline{x}_1\overline{x}_2$ 為真；這是 DeMorgan 定律之一。假設結果對 $n=k$ (≥ 2) 為真且考慮 $n=k+1$ 的情形。

$$\begin{aligned}\overline{(x_1+x_2+\cdots+x_k+x_{k+1})} &= \overline{(x_1+x_2+\cdots+x_k)+x_{k+1}}\\ &= \overline{(x_1+x_2+\cdots+x_k)}\,\overline{x_{k+1}}\\ &= \overline{x_1}\,\overline{x_2}\cdots\overline{x_k}\,\overline{x_{k+1}}\end{aligned}$$

因此，由數學歸納法原理，結果對所有 $n\geq 2$ 成立。

b) 由 (a)，利用對偶性，成立。

3. 她僅能邀請 Nettie 和 Cathy。

5. 若 $x\leq z$ 且 $y\leq z$，則由 15.4 節習題 6(b)，我們 $x+y\leq z+z$。且由冪等定律，我們有 $z+z=z$。反之，假設 $x+y\leq z$。我們發現 $x\leq x+y$，因為 $x(x+y)=x+xy$ (由冪等定律) $=x$ (由吸收定律) 。因 $x\leq x+y$ 且 $x+y\leq z$，我們有 $x\leq z$，因為偏序是可遞移的。 (同理可證 $y\leq z$。)

7. a) $x\leq y\Rightarrow x+\overline{x}\leq y+\overline{x}\Rightarrow 1\leq y+\overline{x}\Rightarrow y+\overline{x}=\overline{x}+y=1.$ 反之

$\overline{x}+y=1\Rightarrow x(\overline{x}+y)=x\cdot 1\Rightarrow x\overline{x}\,(=0)+xy=x\Rightarrow xy=x\Rightarrow x\leq y.$

b) $x\leq\overline{y}\Rightarrow x\overline{y}=x\Rightarrow xy=(x\overline{y})y=x(\overline{y}y)=x\cdot 0=0.$ 反之

$xy=0\Rightarrow x=x\cdot 1=x(y+\overline{y})=xy+x\overline{y}=x\overline{y}$ 及 $x=x\overline{y}\Rightarrow x\leq\overline{y}.$

9. a) $f(w,x,y,z)=\overline{w}\,\overline{x}+xy$ **b)** $g(v,w,x,y,z)=\overline{v}\,\overline{w}yz+xz+w\overline{y}\,\overline{z}+\overline{x}\,\overline{y}\,\overline{z}$

11. a) $2^{(2^n-1)}$ **b)** 2^4；2^{n+1}

13. a) 若 $n=60$，有 12 個因數，且無布林代數有 12 個元素，因 12 不是 2 的冪次方。

b) 若 $n=120$，有 16 個因數。然而，若 $x=4$，則 $\overline{x}=30$ 且 $x\cdot\overline{x}=\gcd(x,\overline{x})=\gcd(4,30)=2$，其不是零元素，所以逆定律不滿足。

第 16 章
群、編碼理論，及 Polya 枚舉法

16.1 節

1. a) 是。單位元數是 1 且每個元素是它自己的反元素。

b) 否。集合在加法下不是封閉的且沒有單位元素。

c) 否。集合在加法下不是封閉的。

d) 是。單位元素是 0；$10n$ 的反元素是 $10(-n)$ 或 $-10n$。

e) 是。單位元素是 1_A 且 $g : A \to A$ 的反元素是 $g^{-1}: A \to A$。

f) 是。單位元素是 0；$a/(2^n)$ 的反元素是 $(-a)/(2^n)$。

3. 減法不是 $\mathbf{Z}$ 的結合 (封閉) 二元運算。例如，$(3-2)-4=-3\neq5=3-(2-4)$。

5. 因 $x, y \in \mathbf{Z} \Rightarrow x+y+1 \in \mathbf{Z}$，運算是一個封閉二元運算 (或 $\mathbf{Z}$ 在 $\circ$ 之下是封閉的)。對 $w, x, y \in \mathbf{Z}$，$w \circ (x \circ y)=w \circ (x+y+1)=w+(x+y+1)+1=(w+x+1)+y+1=(w \circ x) \circ y$，所以二元運算是可結合的。更而，$x \circ y=x+y+1=y+x+1=y \circ x$，對所有 $x, y \in \mathbf{Z}$，所以 $\circ$ 亦是可交換的。若 $x \in \mathbf{Z}$，則 $x \circ (-1)=x+(-1)+1=x$ [$=(-1) \circ x$]，所以 -1 是 $\circ$ 的單位元素。且最後，對每個 $x \in \mathbf{Z}$，我們有 $-x-2 \in \mathbf{Z}$ 且 $x \circ (-x-2)=x+(-x-2)+1=-1$ [$=(-x-2) \circ x$]，所以 $-x-2$ 是 x 在 $\circ$ 下的反元素。因此，$(\mathbf{Z}, \circ)$ 是一個交換群。

7. $U_{20}=\{1, 3, 7, 9, 11, 13, 17, 19\}$　$U_{24}=\{1, 5, 7, 11, 13, 17, 19, 23\}$

9. a) 由定理 16.1(b) 結果成立，因為 $(a^{-1})^{-1}$ 及 a 均是 a^{-1} 的反元素。

b) $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(e)b = b^{-1}b = e$ 且

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = aa^{-1} = e$

所以 $b^{-1}a^{-1}$ 是 ab 的反元素，且由定理 16.1(b)，$(ab)^{-1}=b^{-1}a^{-1}$。

11. a) {0}; {0, 6}; {0, 4, 8}; {0, 3, 6, 9}; {0, 2, 4, 6, 8, 10}; $\mathbf{Z}_{12}$

b) {1}; {1, 10}; {1, 3, 4, 5, 9}; $\mathbf{Z}_{11}^*$

c) $\{\pi_0\}$; $\{\pi_0, \pi_1, \pi_2\}$; $\{\pi_0, r_1\}$; $\{\pi_0, r_2\}$; $\{\pi_0, r_3\}$; S_3

13. a) 共有 10 個；五個轉 i (72°) 的旋轉，$0 \le i \le 4$，及五個對通過一頂點及對邊中點之直線的鏡射。

b) 對一正 n 邊形 ($n \ge 3$)，共有 $2n$ 個剛體運動。有 n 個轉 i (360°/n) 的旋轉，$0 \le i \le n-1$。有 n 個鏡射。對 n 為奇數，共有 $n/2$ 個對通過相對頂點之直線的鏡射及 $n/2$ 個對通過兩對邊中點的直線之鏡射。

15. 因 $eg=ge$ 對所有 $g \in G$，得 $e \in H$ 且 $H \neq \emptyset$。若 $x, y \in H$，則 $xg=gx$ 且 $yg=gy$ 對所有 $g \in G$。反之 $(xy)g=x(yg)=x(gy)=(xg)y=(gx)y=g(xy)$ 對所有 $g \in G$，且我們有 $xy \in H$。最後，對每個 $x \in H$，$g \in G$，$xg^{-1}=g^{-1}x$。所以，$(xg^{-1})^{-1}=(g^{-1}x)^{-1}$，或 $gx^{-1}=x^{-1}g$，且 $x^{-1} \in H$。因此，H 是 G 的一個子群。

17. b) (i) 216

(ii) $H_1=\{(x, 0, 0) | x \in \mathbf{Z}_6\}$ 是一個階數為 6 的子群

$H_2=\{(x, y, 0) | x, y \in \mathbf{Z}_6, y=0, 3\}$ 是一個階數為 12 的子群

$H_3 = \{(x, y, 0) | x, y \in \mathbf{Z}_6\}$ 有階數 36

(iii) $-(2, 3, 4) = (4, 3, 2); -(4, 0, 2) = (2, 0, 4); -(5, 1, 2) = (1, 5, 4)$

19. a) $x = 1$，$x = 4$ **b)** $x = 1$，$x = 10$

c) $x = x^{-1} \Rightarrow x^2 \equiv 1 \pmod{p} \Rightarrow x^2 - 1 \equiv 0 \pmod{p} \Rightarrow (x-1)(x+1) \equiv 0 \pmod{p} \Rightarrow$ $x - 1 \equiv 0 \pmod{p}$ 或 $x + 1 \equiv 0 \pmod{p} \Rightarrow x \equiv 1 \pmod{p}$ 或 $x \equiv -1 \equiv p - 1 \pmod{p}$.

d) 結果對 $p = 2$ 為真，因為 $(2-1)! = 1! \equiv -1! \pmod{2}$。對 $p \geq 3$，考慮 $(\mathbf{Z}_p^*, \cdot)$ 上的元素 1，2，…，$p-1$。元素 2，3，…，$p-2$ 產生 $(p-3)/2$ 對的形如 x，x^{-1} 的數對。 (例如，當 $p = 11$，我們發現 2，3，4，…，9 產生 2, 6; 3, 4; 5, 9; 7, 8 等四對。) 因此 $(p-1)! \equiv (1)(1)^{(p-3)/2}(p-1) \equiv p - 1 \equiv -1 \pmod{p}$。

16.2 節

1. $f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(e_G) = eH$ 且 $f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H$，所以 $f(a^{-1})$ 是 $f(a)$ 的一個反元素。由反元素的唯一性 (定理 16.1b)，得 $f(a^{-1}) = [f(a)]^{-1}$。

3. $f(0) = (0, 0)$ $f(1) = (1, 1)$ $f(2) = (2, 0)$
$f(3) = (0, 1)$ $f(4) = (1, 0)$ $f(5) = (2, 1)$

5. $f(4, 6) = -5g_1 + 3g_2$

7. a) $\mathbb{O}(\pi_0) = 1, \mathbb{O}(\pi_1) = \mathbb{O}(\pi_2) = 3, \mathbb{O}(r_1) = \mathbb{O}(r_2) = \mathbb{O}(r_3) = 2$

b) (見圖 16.6) $\mathbb{O}(\pi_0) = 1, \mathbb{O}(\pi_1) = \mathbb{O}(\pi_3) = 4, \mathbb{O}(\pi_2) = \mathbb{O}(r_1) = \mathbb{O}(r_2) = \mathbb{O}(r_3) = \mathbb{O}(r_4) = 2$

9. a) 階數為 10 的元素是 4，12，28，及 36。

11. $\mathbf{Z}_5^* = \langle 2 \rangle = \langle 3 \rangle$; $\mathbf{Z}_7^* = \langle 3 \rangle = \langle 5 \rangle$; $\mathbf{Z}_{11}^* = \langle 2 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle$

13. 令 $(G, +)$，$(H, *)$，$(K, \cdot)$ 為所給群。對所有 $x, y \in G$，$(g \circ f)(x+y) = g(f(x+y)) = g(f(x) * f(y)) = (g(f(x))) \cdot (g(f(y))) = ((g \circ f)(x)) \cdot ((g \circ f)(y))$，因為 f，g 為同態函數。因此，$g \circ f : G \to K$ 是一個群同態函數。

15. a) $(\mathbf{Z}_{12}, +) = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$
$(\mathbf{Z}_{16}, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 15 \rangle$
$(\mathbf{Z}_{24}, +) = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle = \langle 23 \rangle$

b) 令 $G = \langle a^k \rangle$。因為 $G = \langle a \rangle$，我們有 $a = (a^k)^s$ 對某些 $s \in \mathbf{Z}$。則 $a^{1-ks} = e$，所以 $1 - ks = tn$ 因為 $\mathbb{O}(a) = n$。$1 - ks = tn \Rightarrow 1 = ks + tn \Rightarrow \gcd(k, n) = 1$。反之，令 $G = \langle a \rangle$，其中 $a^k \in G$ 且 $\gcd(k, n) = 1$。則 $\langle a^k \rangle \subseteq G$。$\gcd(k, n) = 1 \Rightarrow 1 = ks + tn$，對某些 s，$t \in \mathbf{Z} \Rightarrow a = a^1 = a^{ks+nt} = (a^k)^s (a^n)^t = (a^k)^s (e)^t = (a^k)^s \in \langle a^k \rangle$。因此，$G \subseteq \langle a^k \rangle$。所以 $G = \langle a^k \rangle$，或 a^k 生成 G。

c) $\phi(n)$

16.3 節

1. a) $\{\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\}$

b) $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}H = \{\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\}$

$\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}H = \{\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}\}$

$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}H = \{\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\}$

$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}H = \{\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}\}$

$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}H = \{\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\}$

$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}H = H$

3. 12

5. 由 Lagrange 定理，我們知道 $|K|=66$ ($=2\cdot 3\cdot 11$) 整除 $|H|$ 且 $|H|$ 整除 $|G|=660$ ($=2^2\cdot 3\cdot 5\cdot 11$)。因此，因 $K\neq H$ 且 $H\neq G$，得 $|H|$ 是 $2(2\cdot 3\cdot 11)=132$ 或 $5(2\cdot 3\cdot 11)=330$。

7. a) 令 $\epsilon = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \alpha = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \beta = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$, 且 $\delta = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$.

$\cdot$	ϵ	α	β	δ
ϵ	ϵ	α	β	δ
α	α	ϵ	δ	β
β	β	δ	ϵ	α
δ	δ	β	α	ϵ

由定理 16.3 得 H 是 G 的一個子群，且因伴隨矩陣中的元素和其上到右下的對角線成對稱，我們有 H 是 G 的一個交換子群。

b) 因為 $|G|=4!=24$ 且 $|4|=4$，有 $24/4=6$ 個 H 的左傍集在 G 上。

c) 考慮函數 $f: H \to \mathbf{Z}_2\times\mathbf{Z}_2$ 被定義為

$$f(\epsilon) = (0, 0), \qquad f(\alpha) = (1, 0), \qquad f(\beta) = (0, 1), \qquad f(\delta) = (1, 1).$$

此函數 f 是一對一且映成，且對所有 $x, y \in H$，我們發現

$$f(x \cdot y) = f(x) \oplus f(y).$$

因此，f 是一個同構函數。

(注意：這裡可能有其它答案。事實上，吾人在這裡可定義 6 種可能的同構函數。)

9. a) 若 H 是 G 的一個真子群，則由 Lagrange 定理，$|H|$ 是 2 或是 p。若 $|H|=2$，則 $H=\{e, x\}$，其中 $x^2=e$，所以 $H=\langle x\rangle$。若 $|H|=p$，令 $y\in H$，$y\neq e$。則 $\mathbb{O}(y)=p$，所以 $H=\langle y\rangle$。

b) 令 $x\in G$，$x\neq e$。則 $\mathbb{O}(x)=p$ 或 $\mathbb{O}(x)=p^2$。若 $\mathbb{O}(x)=p$，則 $|\langle x\rangle|=p$。若 $\mathbb{O}((x)=p^2$，則 $G=\langle x\rangle$ 且 $\langle x^p\rangle$ 是 G 的一個階數為 p 的子群。

11. b) 令 $x\in H\cap K$。若 x 的階數是 r，則 r 必定同時整除 m 和 n。因為 $\gcd(m, n)=1$，得 $r=1$，所以 $x=e$ 且 $H\cap K=\{e\}$。

13. a) $(\mathbf{Z}_p^*, \cdot)$ 有 $p-1$ 個元素，所以由習題 8，對每個 $[x] \in (\mathbf{Z}_p^*, \cdot)$，$[x]^{p-1} = [1]$，或 $x^{p-1} \equiv 1 \pmod{p}$。或 $x^p \equiv x \pmod{p}$。對所有 $a \in \mathbf{Z}$，若 $p|a$，則 $a \equiv 0 \pmod{p}$ 且 $a^p \equiv 0 \equiv a \pmod{p}$。若 $p \nmid a$，則 $a \equiv b \pmod{p}$ 其中 $1 \le b \le p-1$，且 $a^p \equiv b^p \equiv b \equiv a \pmod{p}$。

b) $\mathbf{Z}_n$ 的可逆元所形成的群 G，共有 $\phi(n)$ 個元素，若 $a \in \mathbf{Z}$ 且 $\gcd(a, n) = 1$，則 $[a] \in G$ 且 $[a]^{\phi(n)} = [1]$ 或 $a^{\phi(n)} \equiv 1 \pmod{n}$。

c) 和 **d)** 由習題 6 及 8，結果成立。它們是習題 8 的特殊情形。

16.4 節

1. 0462 0170 1809 0462 1809 1981 0305

3. DRIVESAFELYX **5.** $p = 157$，$q = 773$

16.5 節

1. a) $e = 0001001$ **b)** $r = 1111011$ **c)** $c = 0101000$

3. a) (i) $D(111101100) = 101$ (ii) $D(000100011) = 000$
(iii) $D(010011111) = 011$

b) 000000000，000000001，100000000 **c)** 64

16.6 及 16.7 節

1. $S(101010, 1) = \{101010, 001010, 111010, 100010, 101110, 101000, 101011\}$

$S(111111, 1) = \{111111, 011111, 101111, 110111, 111011, 111101, 111110\}$

3. a) $|S(x, 1)| = 11$; $|S(x, 2)| = 56$; $|S(x, 3)| = 176$

b) $|S(x, k)| = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{k} = \sum_{i=0}^{k} \binom{n}{i}$

5. a) 碼字間的最小距離是 3。這個碼可偵測所有權數 ≤ 2 的錯誤或修正所有單一錯誤。

b) 碼字間的最小距離是 5。這個碼可偵測所有權數 ≤ 4 的錯誤或修正所有權數 ≤ 2 的錯誤。

c) 最小距離是 2。這個碼偵測所有單一錯誤但沒有修正能力。

7. a) $C = \{00000, 10110, 01011, 11101\}$。碼字間的最小距離是 3，所以這個碼可偵測所有權數 ≤ 2 的錯誤或修正所有單一錯誤。

b) $H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

c) (i) 01 (ii) 11 (v) 11 (vi) 10

對 (iii) 和 (iv)，特徵是 $(111)^{tr}$，其不是 H 的一行。假設一個雙重錯誤，若 $(111)^{tr} = (110)^{tr} + (001)^{tr}$，則解碼的接收字是 01 [給 (iii)] 及 10 [給 (iv)]。若 $(111)^{tr} = (011)^{tr} + (100)^{tr}$，我們得到 10 [給 (iii)] 及 01 [給

(iv)]。

9. $G=[I_8|A]$，其中 I_8 是 8×8 乘法單位矩陣且 A 是一個八個 1 的行。$H=[A^{tr}|1]=[11111111|1]$。

11. 將習題 9 的生成 (奇偶性-校驗) 矩陣和習題 10 的奇偶性-校驗 (生成器) 矩陣做比較。

16.8 及 16.9 節

1. $\binom{256}{2}$; 255

3. a)

特徵	傍集首項			
000	00000	10110	01011	11101
110	10000	00110	11011	01101
011	01000	11110	00011	10101
100	00100	10010	01111	11001
010	00010	10100	01001	11111
001	00001	10111	01010	11100
101	11000	01110	10011	00101
111	01100	11010	00111	10001

(最後兩列不唯一。)

b)

接收字	碼字	已解碼的訊息
11110	10110	10
11101	11101	11
11011	01011	01
10100	10110	10
10011	01011	01
10101	11101	11
11111	11101	11
01100	00000	00

5. a) G 是 57×63; H 是 6×63 **b)** 速率是 $\frac{57}{63}$。

7. a) $(0.99)^7+\binom{7}{1}(0.99)^6(0.01)$ **b)** $[(0.99)^7+\binom{7}{1}(0.99)^6(0.01)]^5$

16.10 節

1. a)

$$\pi_2^*=\begin{pmatrix}C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16}\\ C_1 & C_4 & C_5 & C_2 & C_3 & C_8 & C_9 & C_6 & C_7 & C_{10} & C_{11} & C_{14} & C_{15} & C_{12} & C_{13} & C_{16}\end{pmatrix}$$

$$r_4^*=\begin{pmatrix}C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16}\\ C_1 & C_4 & C_3 & C_2 & C_5 & C_9 & C_8 & C_7 & C_6 & C_{10} & C_{11} & C_{12} & C_{15} & C_{14} & C_{13} & C_{16}\end{pmatrix}$$

b)

$$(\pi_1^{-1})^* = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} \\ C_1 & C_5 & C_2 & C_3 & C_4 & C_9 & C_6 & C_7 & C_8 & C_{11} & C_{10} & C_{15} & C_{12} & C_{13} & C_{14} & C_{16} \end{pmatrix}$$

$$= (\pi_1^*)^{-1}$$

c)

$$\pi_3^* r_4^* = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} \\ C_1 & C_5 & C_4 & C_3 & C_2 & C_6 & C_9 & C_8 & C_7 & C_{11} & C_{10} & C_{13} & C_{12} & C_{15} & C_{14} & C_{16} \end{pmatrix}$$

$$= (\pi_3 r_4)^*$$

3. a) $\mathcal{O}(\alpha) = 7; \quad \mathcal{O}(\beta) = 12; \quad \mathcal{O}(\gamma) = 3; \quad \mathcal{O}(\delta) = 6$

b) 令 $\alpha \in S_n$，以 $\alpha = c_1 c_2 \cdots c_k$，一個互斥循環的乘積，則 $\mathcal{O}(\alpha)$ 是 $\mathcal{l}(c_1)$，$\mathcal{l}(c_2)$，…，$\mathcal{l}(c_k)$ 的 1cm，其中 $\mathcal{l}(c_i) = c_i$ 的長度，其中 $1 \le i \le k$。

5. a) 8 **b)** 39 **7. a)** 70 **b)** 55

9. 三角形圖：**a)** 8 **b)** 8 正方形圖：**a)** 12 **b)** 12

11. a) 140 **b)** 102 **13.** 315

16.11 節

1. a) 165 **b)** 120

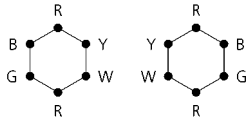
3. 三角形圖：**a)** 96 **b)** 80

正方形圖：**a)** 280 **b)** 220

六邊形圖：**a)** 131,584 **b)** 70,144

5. a) 2635 **b)** 1505

c)



7. a) 21 **b)** 954

c) 否：$k = 21$ 及 $m = 21$，所以 $km = 441 \ne 954 = n$。此處某邊的位置必被考慮和所有頂點的位置有關。例如  不等價於  ，甚至  等價於  且  等價於  。

16.12 節

1. a) (i) 及 (ii) $r^4 + w^4 + r^3 w + 2r^2 w^2 + r w^3$

b) (i) $(1/4)[(r+b+w)^4 + 2(r^4 + b^4 + w^4) + (r^2 + b^2 + w^2)^2]$

(ii) $(1/8)[(r+b+w)^4 + 2(r^4 + b^4 + w^4) + 3(r^2 + b^2 + w^2)^2 + 2(r+b+w)^2(r^2 + b^2 + w^2)]$

3. a) 10

b) $(1/24)[(r+w)^6+6(r+w)^2(r^4+w^4)+3(r+w)^2(r^2+w^2)^2+6(r^2+w^2)^3+8(r^3+w^3)^2]$

c) 2

5. 令 g＝綠色且 y＝金色

三角形圖：$(1/6)[(g+y)^4+2(g+y)(g^3+y^3)+3(g+y)^2(g^2+y^2)]$

正方形圖：$(1/8)[(g+y)^5+2(g+y)(g^4+y^4)+3(g+y)(g^2+y^2)^2+2(g+y)^3(g^2+y^2)]$

六邊形圖：$(1/4)[(g+y)^9+2(g+y)(g^2+y^2)^4+(g+y)^5(g^2+y^2)^2]$

7. a) 136 **b)** $(1/2)[(r+w)^8+(r^2+w^2)^4]$ **c)** 38; 16 **9.** $\binom{m+n-1}{n}$

補充習題

1. a) 因為 $f(e_G)=e_H$，得 $e_G \in K$ 且 $K \neq \emptyset$。若 $x, y \in K$，則 $f(x)=f(y)=e_H$ 且 $f(xy)=f(x)f(y)=e_He_H=e_H$，所以 $xy \in K$。而且，對 $x \in K$，$f(x^{-1})=[f(x)]^{-1}=e_H^{-1}=e_H$，所以 $x^{-1} \in K$。因此，K 是 G 的子群。

b) 若 $x \in K$，則 $f(x)=e_H$。對所有 $g \in G$。

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)e_H f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H.$$

因此，對所有 $x \in K$，$g \in G$，我們發現 $gxg^{-1} \in K$。

3. 令 $a, b \in G$，則 $a^2b^2=ee=e=(ab)^2=abab$。但 $a^2b^2=abab \Rightarrow aabb=abab \Rightarrow ab=ba$，所以 G 是可交換的。

5. 令 $G=\langle g\rangle$，且令 $h=f(g)$。若 $h_1 \in H$，則 $h_1=f(g^n)$ 對某些 $n \in \mathbf{Z}$，因為 f 是映成且 G 是循環的。因此，$h_1=f(g^n)=[f(g)]^n=h^n$，且 $H=\langle h\rangle$。

7. 對所有 $a, b \in G$，

$$(a \circ a^{-1}) \circ b^{-1} \circ b = b \circ b^{-1} \circ (a^{-1} \circ a) \Rightarrow$$
$$a \circ a^{-1} \circ b = b \circ a^{-1} \circ a \Rightarrow a \circ b = b \circ a,$$

所以 $(G, \circ)$ 是一個交換群。

9. a) 考慮一個排列 σ，其被計數在 $P(n+1, k)$。若 $(n+1)$ 是一個 σ 上 (長度為 1 的) 循環，則 σ (被限制至 $\{1, 2, 3, \cdots, n\}$) 被計數在 $P(n, k-1)$。否則，考慮每個排列 τ，其被計數在 $P(n, k)$。對 τ 的每個循環，稱 $(a_1a_2\cdots a_r)$，有 r 個位置來擺 $n+1$ —— (1) 介於 a_1 和 a_2 之間；(2) 介於 a_2 和 a_3 之間；…；$(r-1)$ 介於 a_{r-1} 和 a_r 之間；及 (r) 介於 a_r 和 a_1 之間。因此，共有 n 個位置來擺 $n+1$ 於 τ 上。因此，$P(n+1, k)=P(n, k-1)+nP(n, k)$。

b) $\sum_{k=1}^{n} P(n, k)$ 計數 S_n 上的所有排列，其有 $n!$ 個元素。

11. a) 假設 n 是合成數。我們考慮兩種情形。

(1) $n=m\cdot r$，其中 $1<m<r<n$：此處 $(n-1)!=1\cdot 2\cdots\cdot(m-1)\cdot m\cdot(m+1)\cdot\cdots\cdot(r-1)\cdot r\cdot(r+1)\cdot\cdots\cdot(n-1)\equiv 0 \pmod n$。因此 $(n-1)!\not\equiv -1 \pmod n$。

(2) $n=q^2$，其中 q 是一質數：若 $(n-1)!\equiv -1 \pmod n$ 則 $0\equiv q(n-1)!\equiv q(-1)\equiv n-q\not\equiv 0 \pmod n$。所以在這個情形，我們亦有 $(n-1)!\not\equiv -1 \pmod n$。

b) 由 Wilson 定理，當 p 是一個奇質數，我們發現

$$-1\equiv (p-1)!\equiv (p-3)!(p-2)(p-1)\equiv (p-3)!(p^2-3p+2)\equiv 2(p-3)! \pmod p.$$

第 17 章
有限體及組合設計

17.1 節

1. $f(x)+g(x)=2x^4+5x^3+x^2+5$

$f(x)g(x)=6x^7+2x^6+3x^5+4x^4+2x^3+x^2+4x+4$

3. $(10)(11)^2$; $(10)(11)^3$; $(10)(11)^4$; $(10)(11)^n$

7. a) 和 **b)** $f(x)=(x^2+4)(x-2)(x+2)$; 根為 ± 2。

c) $f(x)=(x+2i)(x-2i)(x-2)(x+2)$; 根為 $\pm 2, \pm 2i$。

d) (a) $f(x)=(x^2-5)(x^2+5)$; 沒有有理根。

(b) $f(x)=(x-\sqrt{5})(x+\sqrt{5})(x^2+5)$; 根為 $\pm\sqrt{5}$。

(c) $f(x)=(x-\sqrt{5})(x+\sqrt{5})(x-\sqrt{5}i)(x+\sqrt{5}i)$; 根為 $\pm\sqrt{5}, \pm i\sqrt{5}$。

9. a) $f(3)=8060$ **b)** $f(1)=1$ **c)** $f(-9)=f(2)=6$

11. 4; 6; $p-1$

13. 令 $f(x)=\sum_{i=0}^{m} a_i x^i$ 且 $h(x)=\sum_{i=0}^{k} b_i x^i$，其中 $a_i\in R$ 對 $0\le i\le m$，$b_i\in R$ 對 $0\le i\le k$，且 $m\le k$。則 $f(x)+h(x)=\sum_{i=0}^{k}(a_i+b_i)x^i$，其中 $a_{m+1}=a_{m+2}=\cdots=a_k=z,$，$R$ 的零，所以 $G(f(x)+h(x))=G\left(\sum_{i=0}^{k}(a_i+b_i)x^i\right)=\sum_{i=0}^{k} g(a_i+b_i)x^i=\sum_{i=0}^{k}[g(a_i)+g(b_i)]x^i=\sum_{i=0}^{k} g(a_i)x^i+\sum_{i=0}^{k} g(b_i)x^i=G(f(x))+G(h(x))$。而且，$f(x)h(x)=\sum_{i=0}^{m+k} c_i x^i$，其中 $c_i=a_ib_0+a_{i-1}b_1+\cdots+a_1b_{i-1}+a_0b_i$，且

$$G(f(x)h(x))=G\left(\sum_{i=0}^{m+k} c_i x^i\right)=\sum_{i=0}^{m+k} g(c_i)x^i.$$

因為 $g(c_i)=g(a_i)g(b_0)+g(a_{i-1})g(b_1)+\cdots+g(a_1)g(b_{i-1})+g(a_0)g(b_i)$，得

$$\sum_{i=0}^{m+k} g(c_i)x^i=\left(\sum_{i=0}^{m} g(a_i)x^i\right)\left(\sum_{i=0}^{k} g(b_i)x^i\right)=G(f(x))\cdot G(h(x)).$$

因此，$G: R[x]\to S[x]$ 是一個環同態函數。

15. 在 $\mathbf{Z}_4[x]$ 上，$(2x+1)(2x+1)=1$，所以 $(2x+1)$ 是一個可逆元。此和習

題 14 不矛盾，因為 $(\mathbf{Z}_4, +, \cdot)$ 不是一個整環。

17. $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ ，我們有 $a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 = 0$ 若且唯若 $f(1)=0$。因為零多項式是在 S 上，集合 S 是非空。以 $f(x)$ 如這裡所給的，令 $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2x^2 + b_1x + b_0 \in S$ 。(這裡 $m \le n$ 且對 $m<n$，我們有 $b_{m+1}=b_{m+2}=\cdots=b_n=0$。) 則 $f(1)-g(1)=0-0=0$，所以 $f(x)-g(x) \in S$。

現考慮 $h(x) = \sum_{i=0}^{k} r_i x^i \in F[x]$。這裡 $h(x)f(x) \in F[x]$ 且 $h(1)f(1)=h(1)\cdot 0=0$，所以 $h(x)f(x) \in S$。

因此，S 是 $F[x]$ 的一個理想。

17.2 節

1. a) x^2+3x-1 在 $\mathbf{Q}$ 上不可約。佈於 $\mathbf{R}$，$\mathbf{C}$，

$$x^2 + 3x - 1 = [x - ((-3+\sqrt{13})/2)][x - ((-3-\sqrt{13})/2)].$$

b) x^4-2 在 $\mathbf{Q}$ 上不可約。

佈於 $\mathbf{R}$，$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$;

$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)$ 佈於 $\mathbf{C}$。

c) $x^2+x+1=(x+2)(x+2)$ 佈於 $\mathbf{Z}_3$。佈於 $\mathbf{Z}_5$，x^2+x+1 不可約；$x^2+x+1=(x+5)(x+3)$ 佈於 $\mathbf{Z}_7$。

d) x^4+x^3+1 在 $\mathbf{Z}_2$ 上不可約。

e) x^3+3x^2-x+1 在 $\mathbf{Z}_5$ 上不可約。

3. 次數 1 : x; $x+1$　次數 2 : x^2+x+1　次數 3 : x^3+x^2+1; x^3+x+1　**5.** 7^5

7. a) 是，因為多項式的所有係數取自一個體。

b) $h(x) | f(x), g(x) \Rightarrow f(x) = h(x)u(x), g(x) = h(x)v(x)$ ，對某些 $u(x), v(x) \in F[x]$ 。

$m(x) = s(x)f(x) + t(x)g(x)$ 對某些 $s(x), t(x) \in F[x]$ ，所以

$m(x) = h(x)[s(x)u(x) + t(x)v(x)]$ 且 $h(x) | m(x)$ 。

c) 若 $m(x) \nmid f(x)$ ，則 $f(x) = q(x)m(x) + r(x)$ ，其中 $0 < \deg r(x) < \deg m(x)$ 。

$m(x) = s(x)f(x) + t(x)g(x)$ 故 $r(x) = f(x) - q(x)[s(x)f(x) + t(x)g(x)]$

$= (1 - q(x)s(x))f(x) - q(x)t(x)g(x)$ ，所以 $r(x) \in S$ 。

由於 $\deg r(x) < \deg m(x)$，這和 $m(x)$ 的選擇矛盾。因此，$r(x)=0$ 且 $m(x) | f(x)$。

9. a) gcd 是 $(x-1) = (1/17)(x^5 - x^4 + x^3 + x^2 - x - 1)$

$- (1/17)(x^2 + x - 2)(x^3 - 2x^2 + 5x - 8).$

b) gcd 是 $1 = (x+1)(x^4 + x^3 + 1) + (x^3 + x^2 + x)(x^2 + x + 1).$

c) gcd 是 $x^2 + 2x + 1 = (x^4 + 2x^2 + 2x + 2) + (x + 2)(2x^3 + 2x^2 + x + 1).$

11. $a=0$，$b=0$; $a=0$，$b=1$

13. a) $f(x) \equiv f_1(x) \pmod{s(x)} \Rightarrow f(x) = f_1(x) + h(x)s(x)$，對某些 $h(x) \in F[x]$，且 $g(x) \equiv g_1(x) \pmod{s(x)} \Rightarrow g(x) = g_1(x) + k(x)s(x)$，對某些 $k(x) \in F[x]$。因此 $f(x) + g(x) = f_1(x) + g_1(x) + (h(x) + k(x))s(x)$，所以 $f(x) + g(x) \equiv f_1(x) + g_1(x) \pmod{s(x)}$，且 $f(x)g(x) = f_1(x)g_1(x) + (f_1(x)k(x) + g_1(x)h(x) + h(x)k(x)s(x))s(x)$，故 $f(x)g(x) \equiv f_1(x)g_1(x) \pmod{s(x)}$.

b) 由 $F[x]$ 的相對應性質，這些性質成立。例如，對分配律

$$\begin{aligned}[f(x)]([g(x)] + [h(x)]) &= [f(x)][g(x) + h(x)] = [f(x)(g(x) + h(x))] \\ &= [f(x)g(x) + f(x)h(x)] = [f(x)g(x)] + [f(x)h(x)] \\ &= [f(x)][g(x)] + [f(x)][h(x)].\end{aligned}$$

d) $F[x]/(s(x))$ 的非零元素之形式為 $[f(x)]$，其中 $f(x) \neq 0$ 且 $\deg f(x) < \deg s(x)$。因 $f(x)$，$s(x)$ 互質，存在 $r(x)$，$t(x)$ 滿足 $1 = f(x)r(x) + s(x)t(x)$，所以 $1 \equiv f(x)r(x) \pmod{s(x)}$ 或 $[1] = [f(x)][r(x)]$。因此 $[r(x)] = [f(x)]^{-1}$。

15. a) $[2x + 1]$ **b)** $[2x + 1]$ **c)** $[2x]$ **17. a)** p^n **b)** $\phi(p^n - 1)$

19. a) 6 **b)** 12 **c)** 12 **d)** lcm(m, n) **e)** 0

21. 101, 103, 107, 109, 113, 121, 125, 127, 128, 131, 137, 139, 149

23. 對 $s(x) = x^3 + x^2 + x + 2 \in \mathbf{Z}_3[x]$，吾人發現 $s(0) = 2$，$s(1) = 2$，且 $s(2) = 1$。則由定理 17.7(b) 及定理 17.11 的 (b) 和 (c)，得 $\mathbf{Z}_3[x]/(s(x))$ 是一個有限體且含 $3^3 = 27$ 個元素。

25. a) 因為 $0 = 0 + 0\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$，集合 $\mathbf{Q}[2]$ 是非空的。對 $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$，我們有

$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$，其中 $(a - c), (b - d) \in \mathbf{Q}$; 且

$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$，其中 $ac + 2bd, ad + bc \in \mathbf{Q}$.

因此，由定理 14.10(a) 得 $\mathbf{Q}[\sqrt{2}]$ 是 $\mathbf{R}$ 的一個子環。

b) 欲證明 $\mathbf{Q}[\sqrt{2}]$ 是 $\mathbf{R}$ 的一個子體，我們須在 $\mathbf{Q}[\sqrt{2}]$ 裡找一個乘法反元素給 $\mathbf{Q}[\sqrt{2}]$ 上的每個非零元素。令 $a + b\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$，且 $a + b\sqrt{2} \neq 0$。若 $b = 0$，$a \neq 0$ 且 $a^{-1} \in \mathbf{Q}$，且 $a^{-1} + 0 \cdot \sqrt{2} \in \mathbf{Q}[\sqrt{2}]$。對 $b \neq 0$，我們須找 $c + d\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$，使得

$$(a + b\sqrt{2})(c + d\sqrt{2}) = 1.$$

現在 $(a + b\sqrt{2})(c + d\sqrt{2}) = 1 \Rightarrow (ac + 2bd) + (ad + bc)\sqrt{2} = 1 \Rightarrow ac + 2bd = 1$ 且 $ad + bc = 0 \Rightarrow c = -ad/b$ 且 $a(-ad/b) + 2bd = 1 \Rightarrow -a^2d + 2b^2d = b \Rightarrow d = b/(2b^2 - a^2)$ 且 $c = -a/(2b^2 - a^2)$。(注意：$2b^2 - a^2 \neq 0$，因為 $\sqrt{2}$ 是無理數。) 因此，$(a + b\sqrt{2})^{-1} = [-a/(2b^2 - a^2)] + [b/(2b^2 - a^2)]\sqrt{2}$，且 $[-a/(2b^2 - a^2)]$，$[b/(2b^2 - a^2)] \in \mathbf{Q}$。所以 $\mathbf{Q}[\sqrt{2}]$ 是 $\mathbf{R}$ 的一個子體。

因為 $s(x)=x^2-2$ 在 **Q** 上不可約，由定理 17.11(b)，得 $\mathbf{Q}[x]/(x^2-2)$ 是一個體。定義對應

$$f: \mathbf{Q}[x]/(x^2-2) \to \mathbf{Q}[2] \quad 為 \quad f([a+bx]) = a+b\sqrt{2}.$$

例題 17.10 及習題 24(a) 類似的理論，得 f 是一個同構函數。

17.3 節

1. a)
$$\begin{matrix}1&2&3&4\\2&1&4&3\\4&3&2&1\\3&4&1&2\end{matrix}$$
b)
$$\begin{matrix}1&2&3&4\\3&4&1&2\\2&1&4&3\\4&3&2&1\end{matrix}$$
c)
$$\begin{matrix}1&3&4&2\\4&2&1&3\\3&1&2&4\\2&4&3&1\end{matrix}$$

3. $a_{ri}^{(k)} = a_{rj}^{(k)} \Rightarrow f_k f_r + f_i = f_k f_r + f_j \Rightarrow f_i = f_j \Rightarrow i = j$

5. L_3:
$$\begin{matrix}4&5&1&2&3\\2&3&4&5&1\\5&1&2&3&4\\3&4&5&1&2\\1&2&3&4&5\end{matrix}$$
L_4:
$$\begin{matrix}5&1&2&3&4\\4&5&1&2&3\\3&4&5&1&2\\2&3&4&5&1\\1&2&3&4&5\end{matrix}$$

具標準型，Latin 方形 Li，$1 \le i \le 4$，變為

L_1':
$$\begin{matrix}1&2&3&4&5\\2&3&4&5&1\\3&4&5&1&2\\4&5&1&2&3\\5&1&2&3&4\end{matrix}$$
L_2':
$$\begin{matrix}1&2&3&4&5\\3&4&5&1&2\\5&1&2&3&4\\2&3&4&5&1\\4&5&1&2&3\end{matrix}$$
L_3':
$$\begin{matrix}1&2&3&4&5\\4&5&1&2&3\\2&3&4&5&1\\5&1&2&3&4\\3&4&5&1&2\end{matrix}$$
L_4':
$$\begin{matrix}1&2&3&4&5\\5&1&2&3&4\\4&5&1&2&3\\3&4&5&1&2\\2&3&4&5&1\end{matrix}$$

7. 引進一個第三因子，諸如 4 個傳送流體型態或 4 個輪胎型態。

17.4 節

1.

體	點數	直線數	一直線上的點數	過一點的直線數
$GF(5)$	25	30	5	6
$GF(3^2)$	81	90	9	10
$GF(7)$	49	56	7	8
$GF(2^4)$	256	272	16	17
$GF(31)$	961	992	31	32

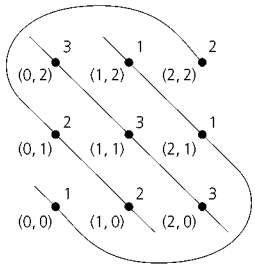
3. 有 9 個點及 12 條直線。這些直線分成四個平行類。

(i) 0 斜率：$y=0; y=1; y=2$

(ii) 無限斜率：$x=0; x=1; x=2$

(iii) 斜率 1 : $y=x; y=x+1; y=x+2$

(iv) 斜率 2 (如圖所示)：(1) $y=2x$ (2) $y=2x+1$ (3) $y=2x+2$



對應到第四個平行類的 Latin 方形是

$$\begin{matrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{matrix}$$

5. a) $y=4x+1$ **b)** $y=3x+10$ 或 $2x+3y+3=0$

c) $y=10x$ 或 $10y=11x$

7. a) 垂直線：$x=c$。直線 $y=mx+b$ 和這個垂直線相交於唯一的點 $(c, mc+b)$。當 b 取 F 上的值時，沒有兩行元素 (在直線 $x=c$ 上) 是相同的。

水平線：$y=c$。直線 $y=mx+b$ 和這個水平線相交於唯一的點 $(m^{-1}(c-b), c)$。當 b 取 F 上的值時，沒有兩列元素 (在直線 $y=c$ 上) 是相同的。

17.5 節

1. $v=9$，$b=12$，$r=4$，$k=3$，$\lambda=1$

3. $\lambda=2$

1 2 3 4	1 3 5 7	2 3 6 7
1 2 5 6	1 4 6 7	2 4 5 7
		3 4 5 6

5. a) 否 **b)** 否

7. a) $\lambda(v-1)=r(k-1)=2r \Rightarrow \lambda(v-1)$ 為偶數。

$\lambda v(v-1)=vr(k-1)=bk(k-1)=b(3)(2) \Rightarrow 6|\lambda v(v-1)$

b) ($\lambda=1$) $6|\lambda v(v-1) \Rightarrow 6|v(v-1) \Rightarrow 3|v(v-1) \Rightarrow 3|v$ 或 $3|(v-1)$

$\lambda(v-1)$ 偶數 $\Rightarrow (v-1)$ 偶數 $\Rightarrow v$ 奇數

$3|v \Rightarrow v=3t$，t 奇數 $\Rightarrow v=3(2s+1)=6s+3$ 且 $v\equiv 3 \pmod 6$

$3|(v-1) \Rightarrow v-1=3t$，$t$ 偶數 $\Rightarrow v-1=6x \Rightarrow v=6x+1$ 且 $v\equiv 1 \pmod 6$

9. $v=9$，$r=4$ **11. a)** $b=21$ **b)** $r=7$

13. 有 λ 個區組包含 x 和 y。且因 r 是設計的複製數，得 $r-\lambda$ 個區組含 x，但不含 y。同樣的，有 $r-\lambda$ 個區組含 y 但不含 x。因此，設計中包

含 x 或 y 的區組個數是 $(r-\lambda)+(r-\lambda)+r=2r-\lambda$。

15. a) 31 **b)** 8

17. a) $v=b=31$; $r=k=6$; $\lambda=1$ **b)** $v=b=57$; $r=k=8$; $\lambda=1$

c) $v=b=73$; $r=k=9$; $\lambda=1$

補充習題

1. $n=9$ **3. a)** 31 **b)** 30 **c)** 29 **d)** $k=1000$

5. 對所有 $a \in \mathbf{Z}_p$，$a^p=a$ [見 16.3 節末的習題 13(a)]，所以 a 是 x^p-x 的一根且 $x-a$ 是 x^p-x 的一個因式。因 $(\mathbf{Z}_p, +, \cdot)$ 是一個體，多項式 x^p-x 至多有 p 個根。因此，$x^p - x = \prod_{a\in\mathbf{Z}_p}(x-a)$。

7. {1, 2, 4}，{2, 3, 5}，{4, 5, 7} **9. a)** 9 **b)** 91

11. b) $A \cdot J_b$ 是一個 $v\times b$ 矩陣，其第 (i, j) 元素是 r，因為 A 的每列有 r 個 1 且 J_b 上的每個元素是 1。因此，$A \cdot J_b = rJ_{v\times b}$。同樣的，$J_v \cdot A$ 是一個 $v\times b$ 矩陣，其第 (i, j) 元素是 k，因為 A 的各行有 k 個 1 且 J_v 上的每個元素是 1。因此，$J_v \cdot A = k \cdot J_{v\times b}$。

c) $A \cdot A^{\text{tr}}$ 的第 (i, j) 元素是 A 的第 i 列和第 j 行各分量乘積和。若 $i=j$，此得列 i 的 1 的個數是 r。對 $i\neq j$，1 的個數是 x_i 和 x_j 出現在同一區組的次數，其被給為 λ。因此，$A \cdot A^{\text{tr}} = (r-\lambda)I_v + \lambda_v$。

d)

$$\begin{vmatrix} r & \lambda & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & \lambda & r & \cdots & \lambda \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda & \lambda & \lambda & \lambda & \cdots & r \end{vmatrix}$$

$$\overset{(1)}{=} \begin{vmatrix} r & \lambda-r & \lambda-r & \lambda-r & \cdots & \lambda-r \\ \lambda & r-\lambda & 0 & 0 & \cdots & 0 \\ \lambda & 0 & r-\lambda & 0 & \cdots & 0 \\ \lambda & 0 & 0 & r-\lambda & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda & 0 & 0 & 0 & \cdots & r-\lambda \end{vmatrix}$$

$$\overset{(2)}{=} \begin{vmatrix} r+(v-1)\lambda & 0 & 0 & 0 & \cdots & 0 \\ \lambda & r-\lambda & 0 & 0 & \cdots & 0 \\ \lambda & 0 & r-\lambda & 0 & \cdots & 0 \\ \lambda & 0 & 0 & r-\lambda & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda & 0 & 0 & 0 & \cdots & r-\lambda \end{vmatrix}$$

關鍵：(1) 將行 1 乘上 -1 並將它加到其它 $v-1$ 個行。

(2) 將列 2 至列 v 各列加到列 1。

附錄 1
指數及對數函數

1. a) $\sqrt{xy^3} = x^{1/2}y^{3/2}$ **b)** $\sqrt[4]{81x^{-5}y^3} = 3x^{-5/4}y^{3/4} = \dfrac{3y^{3/4}}{x^{5/4}}$

c) $5\sqrt[3]{8x^9y^{-5}} = 5(8^{1/3}x^{9/3}y^{-5/3}) = 5(2x^3y^{-5/3}) = \dfrac{10x^3}{y^{5/3}}$

3. a) 625 **b)** 1/343 **c)** 10

5. a) $\log_2 128 = 7$ **b)** $\log_{125} 5 = 1/3$ **c)** $\log_{10} 1/10,000 = -4$ **d)** $\log_2 b = a$

7. a) 3 **c)** 3

9. a) 證明 (利用數學歸納法)：

對 $n = 1$，敘述是 $\log_b r^1 = 1 \cdot \log_b r$，所以結果對這第一個情形成立。假設結果對 $n = k$ (≥ 1) 為真，我們有 $\log_b r^k = k \log_b r$。現對 $n = k+1$ 的情形，我們發現 $\log_b r^{k+1} = \log_b (r \cdot r^k) = \log_b r + \log_b r^k$ [利用定理 A1.2] $= \log_b r + k \log_b r$ (利用歸納法假設) $= (1+k) \log_b r = (k+1) \log_b r$。因此，由數學歸納法原理，對所有 $n \in \mathbf{Z}^+$，結果成立。

b) 對所有 $n \in \mathbf{Z}^+$，$\log_b r^{-n} = \log_b (1/r^n) = \log_b 1 - \log_b r^n$ [利用定理 A1.2 (2)] $= 0 - n \log_b r$ [定理 (a)] $= (-n) \log_b r$。

11. a) 1.5851 **b)** 0.4307 **c)** 1.4650

13. a) 5/3 **b)** 3/2 **c)** 4

15. 令 $x = a^{\log_b c}$ 且 $y = c^{\log_a b}$，則

$$x = a^{\log_b c} \Rightarrow \log_b x = \log_b [a^{\log_b c}] = (\log_b c)(\log_b a), \quad \text{且}$$
$$y = c^{\log_a b} \Rightarrow \log_b y = \log_b [c^{\log_b a}] = (\log_b a)(\log_b c).$$

因此，我們發現 $\log_b x = \log_b y$，且由此得 $x = y$。

附錄 2
矩陣、矩陣運算，及行列式

1. a) $A + B = \begin{bmatrix} 3 & 2 & 5 \\ 0 & 2 & 7 \end{bmatrix}$ **b)** $(A + B) + C = \begin{bmatrix} 3 & 3 & 7 \\ 5 & 6 & 4 \end{bmatrix}$

c) $B + C = \begin{bmatrix} 1 & 2 & 3 \\ 6 & 6 & 1 \end{bmatrix}$ **d)** $A + (B + C) = \begin{bmatrix} 3 & 3 & 7 \\ 5 & 6 & 4 \end{bmatrix}$

e) $2A = \begin{bmatrix} 4 & 2 & 8 \\ -2 & 0 & 6 \end{bmatrix}$ **f)** $2A + 3B = \begin{bmatrix} 7 & 5 & 11 \\ 1 & 6 & 18 \end{bmatrix}$

g) $2C + 3C = \begin{bmatrix} 0 & 5 & 10 \\ 25 & 20 & -15 \end{bmatrix}$ **h)** $5C = \begin{bmatrix} 0 & 5 & 10 \\ 25 & 20 & -15 \end{bmatrix}$

i) $2B - 4C = \begin{bmatrix} 2 & -2 & -6 \\ -18 & -12 & 20 \end{bmatrix}$ **j)** $A + 2B - 3C = \begin{bmatrix} 4 & 0 & 0 \\ -14 & -8 & 20 \end{bmatrix}$

k) $2(3B) = \begin{bmatrix} 6 & 6 & 6 \\ 6 & 12 & 24 \end{bmatrix}$ **l)** $(2 \cdot 3)B = \begin{bmatrix} 6 & 6 & 6 \\ 6 & 12 & 24 \end{bmatrix}$

3. **a)** [12], 或 $\begin{bmatrix}1\\2\end{bmatrix}$ **b)** $\begin{bmatrix}9 & 21\\12 & 27\end{bmatrix}$ **c)** $\begin{bmatrix}-10 & -10\\18 & 24\end{bmatrix}$

d) $\begin{bmatrix}-5 & -7 & 8\\29 & 21 & 2\\-23 & -35 & 6\end{bmatrix}$ **e)** $\begin{bmatrix}a & b & c\\d & e & f\\3g & 3h & 3i\end{bmatrix}$ **f)** $\begin{bmatrix}a & b & c\\3g & 3h & 3i\\d & e & f\end{bmatrix}$

5. **a)** $(-1/5)\begin{bmatrix}1 & -2\\-3 & 1\end{bmatrix}$ **b)** $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$ **c)** 反矩陣不存在 **d)** $\begin{bmatrix}1 & 3\\2 & 7\end{bmatrix}$

7. **a)** $A^{-1}=(1/2)\begin{bmatrix}2 & -1\\0 & 1\end{bmatrix}$ **b)** $B^{-1}=(1/5)\begin{bmatrix}1 & -2\\3 & -1\end{bmatrix}$ **c)** $AB=\begin{bmatrix}-4 & 3\\-6 & 2\end{bmatrix}$

d) $(AB)^{-1}=(1/10)\begin{bmatrix}2 & -3\\6 & -4\end{bmatrix}$ **e)** $B^{-1}A^{-1}=(1/10)\begin{bmatrix}2 & -3\\6 & -4\end{bmatrix}$

9. **b)** $\begin{bmatrix}5 & 3\\3 & -2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}35\\2\end{bmatrix}$

$$\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}5 & 3\\3 & -2\end{bmatrix}^{-1}\begin{bmatrix}35\\2\end{bmatrix}=(-1/19)\begin{bmatrix}-2 & -3\\-3 & 5\end{bmatrix}\begin{bmatrix}35\\2\end{bmatrix}=\begin{bmatrix}4\\5\end{bmatrix}$$

11. $\det(2A)=2^2(31)=124$，$\det(5A)=5^2(31)=775$

13. **a)** 45 **b)** −40 **c)** 14

15. **a)** (i) $\begin{vmatrix}1 & 2 & 1\\0 & -1 & -1\\2 & 3 & 0\end{vmatrix}=2(-1)^{3+1}\begin{vmatrix}2 & 1\\-1 & -1\end{vmatrix}+3(-1)^{3+2}\begin{vmatrix}1 & 1\\0 & -1\end{vmatrix}$

$$=2(-2-(-1))-3(-1)=2(-1)+3=1.$$

(ii) 5 (iii) 25

b) (i) 51 (ii) 306 (iii) 510

附錄 3
可數及不可數集

1. **a)** 真 **b)** 假 **c)** 真 **d)** 真

e) 假：令 $A=\mathbf{Z}\cup(0, 1]$ 且 $B=\mathbf{Z}\cup(1, 2]$，則 A，B 均為不可數，但 $A\cap B=2$ 是可數的。

f) 真

g) 假：令 $A=\mathbf{Z}^+\cup(0, 1]$ 且 $B=(0, 1]$，則 A，B 均為不可數，但 $A-B=\{2, 3, 4, \cdots\}$ 是可數的。

3. 若 B 是可數的，則由定理 A3.3，A 是可數的。此引給我們一個矛盾，因為已知 A 是不可數的。

5. 因為 S，T 均是可數無限，我們知道由定理 A3.2，我們可寫 $S=\{s_1, s_2, s_3, \cdots\}$ 及 $T=\{t_1, t_2, t_3, \cdots\}$ ——兩個相異項 (無限) 數列。定義函數

$$f: S\times T\to\mathbf{Z}^+$$

為 $f(s_i, t_j)=2^i3^j$，對所有 i，$j \in \mathbf{Z}^+$。若 i，j，k，$l \in \mathbf{Z}^+$ 滿足 $f(s_i, t_j)=f(s_k, t_l)$，則 $f(s_i, t_j)=f(s_k, t_l) \Rightarrow 2^i3^j=2^k3^l \Rightarrow i=k$， $j=l$ (由算術基本定理) $\Rightarrow s_i=s_k$ 且 $t_j=t_l \Rightarrow (s_i, t_j)=(s_k, t_l)$。因此，$f$ 是一個一對一函數且 $S\times T \sim f(S\times T) \subset \mathbf{Z}^+$。所以由定理 A3.3，我們知道 $S\times T$ 是可數的。

7. 函數 $f: (\mathbf{Z}-\{0\})\times\mathbf{Z}\times\mathbf{Z} \to \mathbf{Q}$ 被給為 $f(a, b, c)=2^a3^b5^c$ 是一對一 (證明之！) 所以由定理 A3.3 及 A3.8，$(\mathbf{Z}-\{0\})\times\mathbf{Z}\times\mathbf{Z}$ 是可數的。現在對所有 $(a, b, c) \in (\mathbf{Z}-\{0\})\times\mathbf{Z}\times\mathbf{Z}$，二次方程式 $ax^2+bx+c=0$ 至多有兩個 (相異) 實根。由定理 A3.9，二次方程式 $ax^2+bx+c=0$，其中 a，b，$c \in \mathbf{Z}$ 且 $a\neq 0$ 的所有實根所成的集合是可數的。