第 17 章

有限體及組合設計

現在是回憶第 14 章環結構的時候，當我們檢視多項式環及多項式環在有限體所扮演的角色時。我們知道對每個質數 p，$(\mathbf{Z}_p, +, \cdot)$ 是一個有限體，但本章我們將發現其它有限體。正如有限布林代數的階數被限制為 2 的冪方，有限體的可能階數為 p^n，其中 p 是質數且 $n \in \mathbf{Z}^+$。這些有限體的應用將包含 Latin 正方形的組合設計之討論。最後，我們將探討一個有限幾何的結構及發掘這些幾何和組合設計間如何的相互影響。

17.1 多項式環

我們記得環 $(R, +, \cdot)$ 是由一個非空集合 R 所組成，其中 $(R, +)$ 是一個交換群，$(R, \cdot)$ 在可結合的運算 $\cdot$ 之下是封閉的，且這兩個運算有分配律的關係：$a(b+c)=ab+ac$ 且 $(b+c)a=ba+ca$，對所有 a，b，$c \in R$ (我們寫 ab 表 $a \cdot b$)。

為介紹具係數在 R 上的多項式之正式概念，我們令 x 表一個未定元——亦即，是一個不是環 R 上元素的一正式符號。我們接著使用這個符號來定義下面。

定義 17.1

給一個環 $(R, +, \cdot)$，一個形如 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0 x^0$ 的表示式，其中 $a_i \in R$ 對所有 $0 \le i \le n$，被稱是一個**係數取自 R 以 x 爲未定元的多項式** (polynomial in the indeterminate x with coefficient from R)。

若 a_n 不是 R 的零元素，則稱 a_n 為 $f(x)$ 的**首項係數** (the leading

coefficient) 且我們稱 $f(x)$ 的次數為 n。因此，一個多項式的次數是多項式的被加項中 x 的最高冪次方。a_0x^0 項被稱為 $f(x)$ 的**常數** (constant) 或**常數項** (constant term)。

若 $g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x^1+b_0x^0$ 亦是一個佈於 R 的 x 之多項式，則 $f(x)=g(x)$ 若 $m=n$ 且 $a_i=b_i$ 對所有 $0\le i\le n$。

最後，我們使用記號 $R[x]$ 表係數取自 R 以 x 為未定元的所有多項式所成的集合。

例題 17.1

a) 佈於環 $R=(\mathbf{Z}_6, +, \cdot)$，表示求 $5x^2+3x^1-2x^0$ 是一個次數為 2 的多項式，具首項係數 5 及常數項 $-2x^0$。如同先前，此處我們使用 a 表 $[a]$ 於 $\mathbf{Z}_6$ 裡。此多項式亦可被寫為 $5x^2+3x^1+4x^0$，因為 $[4]=[-2]$ 於 $\mathbf{Z}_6$ 裡。

b) 若 z 是環 R 的零元素，則零多項式 $zx^0=z$ 亦是 $R[x]$ 的零元素且被稱**沒有次數** (no degree) 及無首項係數。一個是零元素或次數為 0 的佈於 R 之多項式被稱是**常數多項式** (constant polynomial)。例如，佈於 $\mathbf{Z}_7$ 的多項式 $5x^0$ 的次數為 0 且首項係數為 5 且是一個常數多項式。

對一個係數環 $(R, +, \cdot)$，令

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x^1+a_0x^0$$
$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x^1+b_0x^0,$$

其中 $a_i, b_j\in R$ 對所有 $0\le i\le n$，$0\le j\le m$。我們介紹加法及乘法之 (封閉的二元) 運算給這兩個多項式以得一個新環。

假設 $n\ge m$。我們定義

$$f(x)+g(x)=\sum_{i=0}^{n}(a_i+b_i)x^i, \tag{1}$$

其中 $b_i=z$ 對 $i>m$，且

$$f(x)g(x)=(a_nb_m)x^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)x^{n+m-1}$$
$$+\cdots+(a_1b_0+a_0b_1)x^1+(a_0b_0)x^0. \tag{2}$$

在 $f(x)+g(x)$ 的定義中，係數 (a_i+b_i)，對每個 $0\le i\le n$，係由 R 上元素相加而得。對 $f(x)g(x)$，x^t 的係數是 $\sum_{k=0}^{t}a_{t-k}b_k$，其所有的加法及乘法均運算在 R 上，且 $0\le t\le n+m$。此處是一個此類的例子來說明所含括的計算型態。

令 $f(x)=4x^3+2x^2+3x^1+1x^0$ 且 $g(x)=3x^2+x^1+2x^0$ 為取自 $\mathbf{Z}_5[x]$ 的多項式。此處

$$a_3=4,\quad a_2=2,\quad a_1=3,\quad a_0=1,$$

且

$$b_2=3,\quad b_1=1,\quad b_0=2.$$

對所有 $n\ge 4$，我們發現 $a_n=0$。當 $m\ge 3$，我們有 $b_m=0$。使用方程式 (1) 和 (2) 的定義，其中係數的加法及乘法現被以模 5 來執行，我們得

$$\begin{aligned} f(x)+g(x) &= (4+0)x^3+(2+3)x^2+(3+1)x^1+(1+2)x^0 \\ &= 4x^3+0x^2+4x^1+3x^0 = 4x^3+4x^1+3x^0 \end{aligned}$$

且

$$\begin{aligned} f(x)g(x) &= \left(\sum_{k=0}^{5} a_{5-k}b_k\right)x^5+\left(\sum_{k=0}^{4} a_{4-k}b_k\right)x^4+\left(\sum_{k=0}^{3} a_{3-k}b_k\right)x^3 \\ &\quad+\left(\sum_{k=0}^{2} a_{2-k}b_k\right)x^2+\left(\sum_{k=0}^{1} a_{1-k}b_k\right)x^1+\left(\sum_{k=0}^{0} a_{0-k}b_k\right)x^0 \\ &= (0\cdot 2+0\cdot 1+4\cdot 3+2\cdot 0+3\cdot 0+1\cdot 0)x^5 \\ &\quad+(0\cdot 2+4\cdot 1+2\cdot 3+3\cdot 0+1\cdot 0)x^4 \\ &\quad+(4\cdot 2+2\cdot 1+3\cdot 3+1\cdot 0)x^3 \\ &\quad+(2\cdot 2+3\cdot 1+1\cdot 3)x^2+(3\cdot 2+1\cdot 1)x^1+(1\cdot 2)x^0 \\ &= 2x^5+0x^4+4x^3+0x^2+2x^1+2x^0 = 2x^5+4x^3+2x^1+2x^0. \end{aligned}$$

定義在方程式 (1) 及 (2) 的封閉二元運算給我們下面結果。

定理 17.1　若 R 是一個環，則在方程式 (1) 和 (2) 中所給的加法及乘法運算下，$(R[x],+,\cdot)$ 是一個環，稱之為**佈於 R 的多項式環** (polynomial ring or ring of polynomial)。

證明： $R[x]$ 的環性質依 R 的環性質而定。因此，我們將在這裡證明乘法的結合律，作為一個例子，而將剩下的其它性質留給讀者。令 $h(x)=\sum_{k=0}^{p} c_k x^k$，其中 $f(x)$，$g(x)$ 如稍早所定義的。$(f(x)g(x))h(x)$ 中的基本被加項之形式為 Ax^t，其中 $0\le t\le (m+n)+p$ 且 A 是所有形如 $(a_ib_j)c_k$ 的乘積項之和，其中 $0\le i\le n$，$0\le j\le m$，$0\le k\le p$，且 $i+j+k=t$。在 $f(x)(g(x)h(x))$ 中，x^t 的係數是所有形如 $a_i(b_jc_k)$ 的乘積項之和，其中再次是 $0\le i\le n$，$0\le j\le m$，$0\le k\le p$，且 $i+j+k=t$。因為 R 在乘法下是可結合的。$(a_ib_j)c_k=a_i(b_jc_k)$ 對這些項的各個，且所以 $(f(x)g(x))h(x)$ 中 x^t 的係數和

$f(x)(g(x)h(x))$ 中 x^t 的係數相同。因此，$(f(x)g(x))h(x)=f(x)(g(x)h(x))$。

系理 17.1

令 $R[x]$ 是一個多項式環。

a) 若 R 是可交換的，則 $R[x]$ 是可交換的。
b) 若 R 是一個具有單位元素的環，則 $R[x]$ 是一個具有單位元素的環。
c) $R[x]$ 是一個整環若且唯若 R 是一個整環。

證明：此系理之證明留給讀者。

由此刻起，我們以 x 代替 x^1。若 R 有單位元素 u，我們定義 $x^0=u$，且對所有 $r\in R$，我們記 rx^0 為 r。

例題 17.2

令 $f(x)$，$g(x)\in \mathbf{Z}_8[x]$ 且 $f(x)=4x^2+1$ 及 $g(x)=2x+3$。則 $f(x)$ 的次數為 2 且 $g(x)$ 的次數為 1。由我們過去多項式的經驗，我們期待 $f(x)g(x)$ 的次數為 3，即 $f(x)$ 和 $g(x)$ 的次數和。然而，這裡 $f(x)g(x)=(4x^2+1)(2x+3)=8x^3+12x^2+2x+3=4x^2+2x+3$，因為 $[8]=[0]$ 在 $\mathbf{Z}_8$ 裡。所以 degree $f(x)g(x)=2<3=$ degree $f(x)+$ degree $g(x)$。

例題 17.2 現象的原因是環 $\mathbf{Z}_8$ 中零的真因數存在。這個觀察引我們到下面定理。

定理 17.2

令 $(R, +, \cdot)$ 是一個具單位元函數的交換環，則 R 是一個整環若且唯若對所有 $f(x)$，$g(x)\in R[x]$，若 $f(x)$ 及 $g(x)$ 均非零多項式，則

$$\text{degree } f(x)g(x)=\text{degree } f(x)+\text{degree } g(x)$$

證明：令 $f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{j=0}^{m}b_jx^j$，其中 $a_n\neq z$，$b_m\neq z$。若 R 是一個整環，則 $a_nb_m\neq z$，所以 degree $f(x)g(x)=n+m=$ degree $f(x)+$ degree $g(x)$。反之，若 R 不是一個整環，令 a，$b\in R$ 且 $a\neq z$，$b\neq z$，但 $ab=z$。多項式 $f(x)=ax+u$，$g(x)=bx+u$，各個的次數為 1，但 $f(x)g(x)=(a+b)x+u$ 且 degree $f(x)g(x)\leq 1<2=$ degree $f(x)+$ degree $g(x)$。

在我們可繼續之前，我們需回憶在 14.2 節所介紹的一個概念——在習題 21。若 R 是一個具單位元素 u 的環，且 $r\in R$，我們定義 $r^0=u$，$r^1=r$，且 $r^{n+1}=r^nr$ 對所有 $n\in \mathbf{Z}^+$。[由這些定義，吾人可證明，例如，對所有 m，$n\in \mathbf{Z}^+$，$(r^m)(r^n)=r^{m+n}$ 且 $(r^m)^n=r^{mn}$。] 所以現在我們繼續如下。

令 R 是一個具單位元素 u 的環，且令 $f(x)=a_nx^n+\cdots+a_1x+a_0 \in R[x]$。若 $r \in R$，則 $f(r)=a_nr^n+\cdots+a_1r+a_0 \in R$。我們特別對那些滿足 $f(r)=z$ 的 r 感興趣，且這個興起引我們至下面的概念。

定義 17.2

令 R 是一個具單位元素 u 的環，且令 $f(x) \in R[x]$，滿足 degree $f(x) \geq 1$。若 $r \in R$ 且 $f(r)=z$，則稱 r 是多項式 $f(x)$ 的一個**根** (root)。

例題 17.3

a) 若 $f(x)=x^2-2 \in \mathbf{R}[x]$，則 $f(x)$ 有 $\sqrt{2}$ 及 $-\sqrt{2}$ 作為根，因為 $(\sqrt{2})^2-2=0=(-\sqrt{2})^2-2$。而且，我們可寫 $f(x)=(x-\sqrt{2})(x+\sqrt{2})$，且 $x-\sqrt{2}$，$x+\sqrt{2} \in \mathbf{R}[x]$。然而，若我們視 $f(x)$ 為 $\mathbf{Q}[x]$ 的元素，則 $f(x)$ 沒有根，因為 $\sqrt{2}$ 及 $-\sqrt{2}$ 是無理數。因此，多項式根的存在性依賴係數所在的環。

b) 對 $f(x)=x^2+3x+2 \in \mathbf{Z}_6[x]$，我們發現

$$f(0)=(0)^2+3(0)+2=2 \qquad f(3)=(3)^2+3(3)+2=20=2$$
$$f(1)=(1)^2+3(1)+2=6=0 \qquad f(4)=(4)^2+3(4)+2=30=0$$
$$f(2)=(2)^2+3(2)+2=12=0 \qquad f(5)=(5)^2+3(5)+2=42=0$$

因此，$f(x)$ 有四個根：1，2，4 及 5。這超出我們期待的。在我們先前的經驗，次數為 2 的多項式至多有兩個根。

在本章我們將主要考慮多項式環 $F[x]$，其中 F 是一個體 (且 $F[x]$ 是一個整環)。因此，我們將不處在任何更進一步的情況，其中 degree $f(x)g(x)$ $<$ degree $f(x)+$ degree $g(x)$。而且，除非有說明，否則，我們將把體的零元素表為 0 且以 1 表體的單位元素。

由於 17.3(b) 的結果，我們現在將來發展找何時一個次數為 n 的多項式至多有 n 的根所需的概念。

定義 17.3

令 F 是一個體。對 $f(x)$，$g(x) \in F[x]$，其中 $f(x)$ 不是零多項式，我們稱 $f(x)$ 是 $g(x)$ 的一個**因式** (divisor or factor) 若存在 $h(x) \in F[x]$ 滿足 $f(x)h(x)=g(x)$。此時，我們亦稱 $f(x)$ **整除** (divides) $g(x)$ 且稱 $g(x)$ 是 $f(x)$ 的一個**倍式** (multiple)。

此引出多項式的**除法原理** (division algorithm)。然而，在證明一般結果之前，我們將檢視兩個特別的例題。

例題 17.4

在早期代數裡，我們被教如何執行具實係數之多項式的長除法。給兩個多項式 $f(x)$，$g(x)$，其中 degree $f(x) \leq$ degree $g(x)$，我們將我們的工作整

理成

$$\begin{array}{r} q_1(x)+q_2(x)+\cdots+q_t(x)\ (=q(x)) \\ f(x)\overline{)\,g(x)} \\ \underline{f(x)q_1(x)} \\ g(x)-f(x)q_1(x) \\ \underline{\cdots\cdots\cdots\cdots} \\ r(x) \end{array}$$

其中我們繼續除直到我們發現不是

$$r(x)=0 \text{ 就是 degree } r(x) < \text{degree } f(x).$$

且得 $g(x)=q(x)f(x)+r(x)$。

例如，若 $f(x)=x-3$ 且 $g(x)=7x^3-2x^2+5x-2$，則 $f(x)$，$g(x)\in \mathbf{Q}$ (或 $\mathbf{R}[x]$，或 $\mathbf{C}[x]$)，且我們發現

$$\begin{array}{r} 7x^2+19x+62\ \ (=q(x)) \\ x-3\overline{)\,7x^3-2x^2+5x-2} \\ \underline{7x^3-21x^2} \\ 19x^2+5x-2 \\ \underline{19x^2-57x} \\ 62x-2 \\ \underline{62x-186} \\ 184\ (=r(x)) \end{array}$$

檢查這些結果，我們有

$$q(x)f(x)+r(x)=(7x^2+19x+62)(x-3)+184=7x^3-2x^2+5x-2=g(x).$$

例題 17.5

例題 17.4 所展示的技巧亦可使用當多項式的所有係數取自一個**有限體** (finite field) 時。

若 $f(x)=3x^2+4x+2$ 且 $g(x)=6x^4+4x^3+5x^2+3x+1$ 是 $\mathbf{Z}_7[x]$ 上的多項式時，則長除法的過程提供下面計算：

$$\begin{array}{r} 2x^2+x+6\ \ (=q(x)) \\ 3x^2+4x+2\overline{)\,6x^4+4x^3+5x^2+3x+1} \\ \underline{6x^4+x^3+4x^2} \\ 3x^3+x^2+3x+1 \\ \underline{3x^3+4x^2+2x} \\ 4x^2+x+1 \\ \underline{4x^2+3x+5} \\ 5x+3\ \ (=r(x)) \end{array}$$

執行所有算術於 $\mathbf{Z}_7$ 裡，我們發現 (如在例題 17.4 裡)

$$\begin{aligned} q(x)f(x)+r(x) &= (2x^2+x+6)(3x^2+4x+2)+(5x+3) \\ &= 6x^4+4x^3+5x^2+3x+1 = g(x) \end{aligned}$$

我們現在轉向一般情形。

定理 17.3

除法演算法 (Division Algorithm)。令 $f(x)$，$g(x) \in F[x]$ 且 $f(x)$ 不是零多項式，則存在唯一的多項式 $q(x)$，$r(x) \in F[x]$ 滿足 $g(x)=q(x)f(x)+r(x)$，其中 $r(x)=0$ 或 degree $r(x)<$dregree $f(x)$。

證明：令 $S=\{g(x)-t(x)f(x)|t(x) \in F[x]\}$。

若 $0 \in S$，則 $0=g(x)-t(x)f(x)$ 對某些 $t(x) \in F[x]$。則以 $q(x)=t(x)$ 且 $r(x)=0$，我們有 $g(x)=q(x)f(x)+r(x)$。

若 $0 \notin S$，考慮 S 的所有元素之次數，且令 $r(x)=g(x)-q(x)f(x)$ 為 S 中次數最小的元素。因為 $r(x) \neq 0$，若 degree $r(x)<$degree $f(x)$，則結果成立。若否，令

$$\begin{aligned} r(x) &= a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0, \qquad a_n \neq 0, \\ f(x) &= b_mx^m+b_{m-1}x^{m-1}+\cdots+b_2x^2+b_1x+b_0, \qquad b_m \neq 0, \end{aligned}$$

且 $n \geq m$。定義

$$\begin{aligned} h(x) = r(x)-[a_nb_m^{-1}x^{n-m}]f(x) &= (a_n-a_nb_m^{-1}b_m)x^n+(a_{n-1}-a_nb_m^{-1}b_{m-1})x^{n-1} \\ &+\cdots+(a_{n-m}-a_nb_m^{-1}b_0)x^{n-m}+a_{n-m-1}x^{n-m-1}+\cdots+a_1x+a_0. \end{aligned}$$

則 $h(x)$ 的次數小於 n、$r(x)$ 的次數。更重要的，$h(x)=[g(x)-q(x)f(x)]-[a_nb_m^{-1}x^{n-m}]f(x)=g(x)-[q(x)+a_nb_m^{-1}x^{n-m}]f(x)$，所以 $h(x) \in S$ 且這和 $r(x)$ 被選為次數最小的條件矛盾。因此，degree $r(x)<$degree $f(x)$ 且我們有了定理的存在部份。

至於唯一性，令 $g(x)=q_1(x)f(x)+r_1(x)=q_2(x)f(x)+r_2(x)$，其中 $r_1(x)=0$ 或 degree $r_1(x)<$degree $f(x)$，且 $r_2(x)=0$ 或 degree $r_2(x)<$degree $f(x)$。則 $[q_2(x)-q_1(x)]f(x)=r_1(x)-r_2(x)$，且若 $q_2(x)-q_1(x) \neq 0$ 則 degree $([q_2(x)-q_1(x)]f(x) \geq$ degree $f(x)$，而其中 $r_1(x)-r_2(x)=0$ 或 degree $[r_1(x)-r_2(x)] \leq$ max {degree $r_1(x)$, degree $r_2(x)$}$<$degree $f(x)$。因此，$q_1(x)=q_2(x)$，且 $r_1(x)=r_2(x)$。

除法演算法提供下面有關根和因式的結果。

定理 17.4 **餘式定理** (The Remainder Theorem)。對 $f(x) \in F[x]$ 且 $a \in F$，則 $f(x)$ 除以 $(x-a)$ 的餘式是 $f(a)$。

證明： 由除法演算法，$f(x)=q(x)(x-a)+r(x)$，其中 $r(x)=0$ 或 degree $r(x)$ $<$degree $(x-a)=1$。因此，$r(x)=r$ 是 F 的元素。以 a 代 x，我們發現 $f(a)$ $=q(a)(a-a)+r=0+r=r$。

定理 17.5 **因式定理** (The Factor Theorem)。若 $f(x) \in F[x]$ 且 $a \in F$，則 $x-a$ 是 $f(x)$ 的一個因式若且唯若 a 是 $f(x)$ 的一個根。

證明： 若 $x-a$ 是 $f(x)$ 的一個因式，則 $f(x)=q(x)(x-a)$。因 $f(a)=q(a)(a-a)=0$，得 a 是 $f(x)$ 的一根。反之，假設 a 是 $f(x)$ 的一根。由除法演算法，$f(x)=q(x)(x-a)+r$，其中 $r \in F$。因為 $f(a)=0$，我們有 $r=0$，所以 $f(x)=q(x)(x-a)$，且 $x-a$ 是 $f(x)$ 的一個因式。

例題 17.6

a) 令 $f(x)=x^7-6x^5+4x^4-x^2+3x-7 \in \mathbf{Q}[x]$。由餘式定理，當 $f(x)$ 被 $x-2$ 除時，餘式是

$$f(2)=2^7-6(2^5)+4(2^4)-2^2+3(2)-7=-5.$$

若 $f(x)$ 除以 $x+1$，則餘式為 $f(-1)=-2$。

b) 若 $g(x)=x^5+3x^4+x^3+x^2+2x+2 \in \mathbf{Z}_5[x]$ 除以 $x-1$，則餘式是 $g(1)=1+3+1+1+2+2=0$ (於 $\mathbf{Z}_5$)。因此，$x-1$ 整除 $g(x)$，且由餘式定理，

$$g(x)：q(x)(x-1) \quad (\text{其中 degree } q(x)=4)。$$

使用定理 17.4 及 17.5 的結果，我們現在建立本節的最後主要概念。

定理 17.6 若 $f(x) \in F[x]$ 的次數 $n \geq 1$，則 $f(x)$ 至多有 n 個根於 F 裡。

證明： 對 $f(x)$ 的次數做數學歸納法。若 $f(x)$ 的次數為 1，則 $f(x)=ax+b$，其中 a，$b \in F$，$a \neq 0$。因為 $f(-a^{-1}b)=0$，$f(x)$ 至少有一個根於 F 上。若 c_1 和 c_2 均為根，則 $f(c_1)=ac_1+b=0=ac_2+b=f(c_2)$。由環消去律，$ac_1+b$ $=ac_2+b \Rightarrow ac_1=ac_2$。因為 F 是一個體，且 $a \neq 0$，我們有 $ac_1=ac_2 \Rightarrow c_1$ $=c_2$，所以 $f(x)$ 僅有一根於 F 上。

現在假設定理結果對所有 $F[x]$ 上次數 k (≥ 1) 的多項式成立。考慮一個次數為 $k+1$ 的多項式 $f(x)$。若 $f(x)$ 沒有根於 F 上，定理成立。否則，令 $r \in F$ 滿足 $f(r)=0$。由因式定理，$f(x)=(x-r)g(x)$，其中 $g(x)$ 的次數為

k。因此，由歸納法假設，$g(x)$ 至多有 k 個根於 F 上，且 $f(x)$ 至多有 $k+1$ 個根於 F 上。

例題 17.7

a) 令 $f(x)=x^2-6x+9 \in \mathbf{R}[x]$，則 $f(x)$ 至多有兩根於 $\mathbf{R}$ 上——即根 3，3。所以我們稱 3 是一個**重根數** (multiplicity) 為 2 的根。而且，$f(x)=(x-3)(x-3)$，兩個一次，或線性，因式的分解。

b) 對 $g(x)=x^2+4 \in \mathbf{R}[x]$，$g(x)$ 無實根，但和定理 17.6 不矛盾 (為何？) 在 $\mathbf{C}[x]$ 上，$g(x)$ 的根為 $2i$，$-2i$，且可被因式分解為 $g(x)=(x-2i)(x+2i)$。

c) 若 $h(x)=x^2+2x+6 \in \mathbf{Z}_7[x]$，則 $h(2)=0$，$h(3)=0$，且這些是唯有的根。而且，$h(x)=(x-2)(x-3)=x^2-5x+6=x^2+2x+6$，因為 $[-5]=[2]$ 於 $\mathbf{Z}_7$ 上。

d) 如我們在例題 17.3(b) 所見的，多項式 x^2+3x+2 有四個根。這和定理 17.6 不矛盾，因為 $\mathbf{Z}_6$ 不是一個體。而且 $x^2+3x+2=(x+1)(x+2)=(x+4)(x+5)$，兩個不同的因式分解。

我們以一個 $F[x]$ 上因式分解概念的最後註解來結束本節，但不給證明。若 $f(x) \in F[x]$ 的次數為 n 且 r_1，r_2，$\cdots$，r_n 為 $f(x)$ 在 F 上的根 (有可能是重根——即 $r_i=r_j$ 對某些 $1 \le i<j \le n$)，則 $f(x)=a_n(x-r_1)(x-r_2)\cdots(x-r_n)$，其中 a_n 是 $f(x)$ 的首項係數。不考慮一次因式的順位。$f(x)$ 的這個表示式是唯一的。

習題 17.1

1. 令 $f(x)$，$g(x) \in \mathbf{Z}_7[x]$，其中 $f(x)=2x^4+2x^3+3x^2+x+4$，且 $g(x)=3x^3+5x^2+6x+1$。求 $f(x)+g(x)$，$f(x)-g(x)$，及 $f(x)g(x)$。
2. 求 $\mathbf{Z}_2[x]$ 上所有次數為 2 的多項式。
3. $\mathbf{Z}_{11}[x]$ 上有多少個次數為 2 的多項式？有多少個次數為 3 的多項式？有多少個次數為 4 的多項式？有多少個次數為 n 的多項式，其中 $n \in \mathbf{N}$？
4. a) 在 $\mathbf{Z}_{12}[x]$ 上找兩個非零多項式 $f(x)$，$g(x)$ 滿足 $f(x)g(x)=0$。
   b) 在 $\mathbf{Z}_{12}[x]$ 上找多項式 $h(x)$，$k(x)$ 滿足 degree $h(x)=5$，degree $k(x)=2$，且 degree $h(x)k(x)=3$。
5. 完成定理 17.1 及系理 17.1 的證明。
6. 對下面各雙 $f(x)$，$g(x)$，求 $q(x)$，$r(x)$ 使得 $g(x)=g(x)f(x)+r(x)$，其中 $r(x)=0$ 或 degree $r(x)<$ degree $f(x)$。
   a) $f(x), g(x) \in \mathbf{Q}[x],\quad f(x)=x^4-5x^3+7x,\ g(x)=x^5-2x^2+5x-3$
   b) $f(x), g(x) \in \mathbf{Z}_2[x], f(x)=x^2+1, g(x)=x^4+x^3+x^2+x+1$

c) $f(x), g(x) \in \mathbf{Z}_5[x], f(x) = x^2 + 3x + 1, g(x) = x^4 + 2x^3 + x + 4$

7. a) 若 $f(x) = x^4 - 16$，求其根及其在 $\mathbf{Q}[x]$ 上的分解。
   b) 對 $f(x) \in \mathbf{R}[x]$ 回答 (a)。
   c) 對 $f(x) \in \mathbf{C}[x]$ 回答 (a)。
   d) 對 $f(x) = x^4 - 25$ 回答 (a)，(b)，及 (c)。
8. a) 求 $f(x) = x^2 + 4x$ 的所有根若 $f(x) \in \mathbf{Z}_{12}[x]$。
   b) 找四個相異的線性多項式 $g(x)$，$h(x)$，$s(x)$，$t(x) \in \mathbf{Z}_{12}[x]$，使得 $f(x) = g(x)h(x) = s(x)t(x)$。
   c) (b) 之結果和例題 17.7 之後的敘述有矛盾嗎？
9. 對下面各題求 $f(x)$ 除以 $g(x)$ 的餘式。
   a) $f(x), g(x) \in \mathbf{Q}[x], f(x) = x^8 + 7x^5 - 4x^4 + 3x^3 + 5x^2 - 4, g(x) = x - 3$
   b) $f(x), g(x) \in \mathbf{Z}_2[x], f(x) = x^{100} + x^{90} + x^{80} + x^{50} + 1, g(x) = x - 1$
   c) $f(x), g(x) \in \mathbf{Z}_{11}[x], f(x) = 3x^5 - 8x^4 + x^3 - x^2 + 4x - 7, g(x) = x + 9$
10. 對下面各題多項式 $f(x) \in \mathbf{Z}_7[x]$，求其在 $\mathbf{Z}_7$ 上的所有根並將 $f(x)$ 寫為一次多項式的乘積。
    a) $f(x) = x^3 + 5x^2 + 2x + 6$
    b) $f(x) = x^7 - x$
11. 環 $\mathbf{Z}_5[x]$ 上有多少個可逆元素？$\mathbf{Z}_7[x]$ 有多少個可逆元素？p 為質數，$\mathbf{Z}_p[x]$ 上有多少個可逆元素？
12. 給一個體 F，令 $f(x) \in F[x]$，其中 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$。證明 $x - 1$ 是 $f(x)$ 的因式若且唯若 $a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 = 0$。
13. 令 R，S 為環，且令 $g: R \to S$ 是一個環同態函數。證明函數 $G: R[x] \to S[x]$ 定義為
$$G\left(\sum_{i=0}^{n} r_i x^i\right) = \sum_{i=0}^{n} g(r_i)x^i$$
是一個環同態函數。
14. 若 R 是一個整環，證明若 $f(x)$ 是 $R[x]$ 上的一個可逆元素，則 $f(x)$ 是一個常數且是 R 上的一個可逆元素。
15. 證明 $f(x) = 2x + 1$ 是 $\mathbf{Z}_4[x]$ 上的一個可逆元素。此和習題 14 的結果矛盾嗎？
16. 對 $n \in \mathbf{Z}^+$，$n \geq 2$，令 $f(x) \in \mathbf{Z}_n[x]$。證明若 a，$b \in \mathbf{Z}$ 且 $a \equiv b \pmod n$，則 $f(a) \equiv f(b) \pmod n$。
17. 若 F 是一個體，令 $S \subseteq F[x]$，其中 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \in S$ 若且唯若 $a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 = 0$。證明 S 是 $F[x]$ 上的一個理想。
18. 令 $(R, +, \cdot)$ 是一個環。若 I 是 R 上的一個理想，證明 $I[x]$，係數在 I 上以 x 為未定元的所有多項式所成的集合，是 $R[x]$ 上的一個理想。

17.2 不可約多項式：有限體

我們現在想建構 $(\mathbf{Z}_p, +, \cdot)$ 型態之外的有限體，其中 p 為一質數。此建構將使用下面特殊的多項式。

定義 17.4

令 $f(x) \in F[x]$，其中 F 是一個體且 degree $f(x) \geq 2$。我們稱 $f(x)$ **可約的** (reducible)(在 F 上) 若存在 $g(x)$，$h(x) \in F[x]$，滿足 $f(x)=g(x)h(x)$ 且 $g(x)$，$h(x)$ 各個的次數 ≥ 1。若 $f(x)$ 不是可約的，則稱它是**不可約的** (irreducible) 或為**質式** (prime)。

定理 17.7 包含一些關於不可約多項式的有用觀察。

定理 17.7

對 $F[x]$ 上的多項式。

a) 每一個次數 ≤ 1 的非零多項式是不可約的。
b) 對 $f(x) \in F[x]$ 且 degree $f(x)=2$ 或 3，則 $f(x)$ 是可約的若且唯若 $f(x)$ 有一根在體 F 上。

證明：證明留給讀者。

例題 17.8

a) 多項式 x^2+1 在 $\mathbf{Q}[x]$ 及 $\mathbf{R}[x]$ 上是不可約的，但在 $\mathbf{C}[x]$ 上，我們發現 $x^2+1=(x+i)(x-i)$。
b) 令 $f(x)=x^4+2x^2+1 \in \mathbf{R}[x]$。雖然 $f(x)$ 沒有實根，但它是可約的，因為 $(x^2+1)^2=x^4+2x^2+1$。因此，定理 17.7(b) 不可應用於次數 >3 的多項式。
c) 在 $\mathbf{Z}_2[x]$ 上，$f(x)=x^3+x^2+x+1$ 是可約的，因為 $f(1)=0$。但 $g(x)=x^3+x+1$ 是不可約的，因為 $g(0)=g(1)=1$。
d) 令 $h(x)=x^4+x^3+x^2+x+1 \in \mathbf{Z}_2[x]$。$h(x)$ 在 $\mathbf{Z}_2[x]$ 上可約嗎？因為 $h(0)=h(1)=1$，$h(x)$ 沒有一次因式，但或許我們可找到 a，b，c，$d \in \mathbf{Z}_2$ 滿足 $(x^2+ax+b)(x^2+cx+d)=x^4+x^3+x^2+x+1$。

展開 $(x^2+ax+b)(x^2+cx+d)$ 且比較 x 冪次方的同項係數，我們發現 $a+c=1$，$ac+b+d=1$，$ad+bc=1$，且 $bd=1$。以 $bd=1$，得 $b=1$ 且 $d=1$，所以 $ac+b+d=1 \Rightarrow ac=1 \Rightarrow a=c=1 \Rightarrow a+c=0$。此和 $a+c=1$ 矛盾。因此 $h(x)$ 在 $\mathbf{Z}_2[x]$ 上不可約。

例題 17.8 的所有多項式享有一共同性質，我們將現在定義之。

定義 17.5

稱多項式 $f(x) \in F[x]$ 是**首項一** (monic) 若其首項係數是 1，即 F 的單位元素。

下面某些結果 (包含例題 17.11 中的討論) 喚醒第 4 及 14 章的記憶。

定義 17.6 若 $f(x)$，$g(x) \in F[x]$，則 $h(x) \in F[x]$ 是 $f(x)$ 和 $g(x)$ 的一個**最大公因式** (greatest common divisor)，

a) 若 $h(x)$ 整除 $f(x)$ 和 $g(x)$ 各個，且
b) 若 $k(x) \in F[x]$ 且 $k(x)$ 整除 $f(x)$，$g(x)$ 兩者，則 $k(x)$ 整除 $h(x)$。

我們現在敘述所謂的最大公因式之存在性和唯一性於下面結果，我們將其縮寫為 gcd。更而，有個方法來求這個 gcd，且稱這個方法為多項式的歐幾里得演算法。第一個結果的證明被概述於本節習題裡。

定理 17.8 令 $f(x)$，$g(x) \in F[x]$，且 $f(x)$，$g(x)$ 中至少有一個不是零多項式。則每一個可被表為 $f(x)$ 和 $g(x)$ 之線性組合——亦即形如 $s(x)f(x)+t(x)g(x)$，其中 $s(x)$，$t(x) \in F[x]$ ——的最小次數多項式將是 $f(x)$，$g(x)$ 的一個最大公因式。若我們要求 gcd 要為首項一，則它將是唯一的。

定理 17.9 **多項式的歐幾里得演算法** (Euclidean Algorithm for Polynomials)。令 $f(x)$，$g(x) \in F[x]$ 滿足 degree $f(x) \le$ degree $g(x)$ 且 $f(x) \neq 0$。應用除法演算法，我們寫

$$\begin{aligned}
g(x) &= q(x)f(x) + r(x), && \text{degree } r(x) < \text{degree } f(x)\\
f(x) &= q_1(x)r(x) + r_1(x), && \text{degree } r_1(x) < \text{degree } r(x)\\
r(x) &= q_2(x)r_1(x) + r_2(x), && \text{degree } r_2(x) < \text{degree } r_1(x)\\
&\vdots && \vdots\\
r_{k-2}(x) &= q_k(x)r_{k-1}(x) + r_k(x), && \text{degree } r_k(x) < \text{degree } r_{k-1}(x)\\
r_{k-1}(x) &= q_{k+1}(x)r_k(x) + r_{k+1}(x), && r_{k+1}(x) = 0.
\end{aligned}$$

則 $r_k(x)$，即最後的非零餘式，是 $f(x)$，$g(x)$ 的一個最大公因式且是 $f(x)$，$g(x)$ 的首項一最大公因式的某常數倍數。[將 $r_k(x)$ 乘上其首項係數的倒數將得唯一的首項一多項式，我們稱它為最大公因式。]

定義 17.7 若 $f(x)$，$g(x) \in F[x]$ 且它們的 gcd 是 1，則稱 $f(x)$ 和 $g(x)$ 為**互質** (relatively prime)。

我們用來建構我們的新有限體的最後結果，提供我們在 14.3 節所發展的構造一個類比。

定理 17.10

令 $s(x) \in F[x]$，$s(x) \neq 0$。定義 $F[x]$ 上的關係 $\mathcal{R}$ 為 $f(x)\ \mathcal{R}\ g(x)$ 若 $f(x) - g(x) = t(x)s(x)$，對某些 $t(x) \in F[x]$ ——亦即，$s(x)$ 整除 $f(x) - g(x)$。則 $\mathcal{R}$ 是 $F[x]$ 上的一個等價關係。

證明：$\mathcal{R}$ 的反身、對稱，及遞移性質之證明留給讀者。

當定理 17.10 的情形發生，我們稱 **$f(x)$ 和 $g(x)$ 同餘模 $s(x)$** ($f(x)$ is congruent to $g(x)$ modulo $s(x)$) 且記 $f(x) \equiv g(x) \pmod{s(x)}$。稱關係 $\mathcal{R}$ 為**同餘模 $s(x)$** (congruence modulo $s(x)$)。

讓我們檢視一個此類關係的等價類。

例題 17.9

令 $s(x) = x^2 + x + 1 \in \mathbf{Z}_2[x]$。則

a) $[0] = [x^2 + x + 1] = \{0, x^2 + x + 1, x^3 + x^2 + x, (x + 1)(x^2 + x + 1), \ldots\}$
$= \{t(x)(x^2 + x + 1) | t(x) \in \mathbf{Z}_2[x]\}$

b) $[1] = \{1, x^2 + x, x(x^2 + x + 1) + 1, (x + 1)(x^2 + x + 1) + 1, \ldots\}$
$= \{t(x)(x^2 + x + 1) + 1 | t(x) \in \mathbf{Z}_2[x]\}$

c) $[x] = \{x, x^2 + 1, x(x^2 + x + 1) + x, (x + 1)(x^2 + x + 1) + x, \ldots\}$
$= \{t(x)(x^2 + x + 1) + x | t(x) \in \mathbf{Z}_2[x]\}$

d) $[x + 1] = \{x + 1, x^2, x(x^2 + x + 1) + (x + 1), (x + 1)(x^2 + x + 1)$
$+ (x + 1), \ldots\} = \{t(x)(x^2 + x + 1) + (x + 1) | t(x) \in \mathbf{Z}_2[x]\}$

這些是全部等價類嗎？若 $f(x) \in \mathbf{Z}_2[x]$，則由除法演算法 $f(x) = q(x)s(x) + r(x)$，其中 $r(x) = 0$ 或 degree $r(x) <$ degree $s(x)$。因為 $f(x) - r(x) = q(x)s(x)$，得 $f(x) \equiv r(x) \pmod{s(x)}$，所以 $f(x) \in [r(x)]$。因此，欲決定所有等價類，我們考慮 $r(x)$ 的所有可能性。此處 $r(x) = 0$ 或 degree $r(x) < 2$，所以 $r(x) = ax + b$，其中 $a, b \in \mathbf{Z}_2$。因為對 a，b 各個僅有兩個選擇，所以有四個選擇給 $r(x)$：即 0，1，x，$x+1$。

我們現在擺一個環結構在例題 17.9 的等價類上。記得在第 14 章這個是如何被完成給 $\mathbf{Z}_n$ 的，我們定義加法為 $[f(x)] + [g(x)] = [f(x) + g(x)]$。因為 degree $(f(x) + g(x)) \leq \max\{\text{degree } f(x), \text{ degree } g(x)\}$，我們可找到等價類給 $[f(x) + g(x)]$ 而不會太麻煩。此處，例如，$[x] + [x + 1] = [x + (x + 1)] = [2x + 1] = [1]$，因為 $2 = 0$ 於 $\mathbf{Z}_2$ 上。

在定義這些等價類的乘法方面，我們稍有困難。例如，例題 17.9 中，$[x][x]$ 是什麼？假若，一般上，我們定義 $[f(x)][g(x)] = [f(x)g(x)]$，則可能會有 degree $f(x)g(x) \geq$ degree $s(x)$，所以我們可能無法在等價類表中發現 $[f(x)g(x)]$。然而，若 degree $f(x)g(x) \geq$ degree $s(x)$，則使用除法演算法，我

們可記 $f(x)g(x)=q(x)s(x)+r(x)$，其中 $r(x)=0$ 或 degree $r(x)<$degree $s(x)$。由於 $f(x)g(x)=q(x)s(x)+r(x)$，得 $f(x)g(x)\equiv r(x)(\text{mod } s(x))$，且我們定義 $[f(x)g(x)]=[r(x)]$，其中 $[r(x)]$ *確實*出現在等價表中。

由這些觀察，我們分別對 $\{[0], [1], [x], [x+1]\}$ 的加法及乘法建構表 17.1 及 17.2。(在這些表中，我們以 a 表 $[a]$。)

表 17.1

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

表 17.2

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

由乘法表 (表 17.2)，我們發現這些等價類不僅形成一個環且形成一個體，其中 $[1]^{-1}=[1]$，$[x]^{-1}=[x+1]$，且 $[x+1]^{-1}=[x]$。這個階數為 4 的體被表為 $\mathbf{Z}_2[x]/(x^2+x+1)$，且我們發現它包含**子體** (subfield) $\mathbf{Z}_2$ (的一個同構影本)。[一般上，體 $(F, +, \cdot)$ 的子環 $(R, +, \cdot)$ 是一個子體，當 $(R, +, \cdot)$ 是一個體時。] 而且，對這個體的所有非零元素，我們發現 $[x]^1=[x]$，$[x]^2=[x+1]$，$[x]^3=[1]$，所以我們有一個階數為 3 的循環群。但任一體的所有非零元素在乘法之下形成一個群，且任一階數為 3 的群是循環的，所以為何困擾這個觀察呢？一般來講，任一有限體的所有非零元素在乘法之下形成一個循環群。(證明可被發現於參考資料 [10] 的第 12 章。)

前面所建構的被整理於下面定理裡。證明大綱被給在本節習題裡。

定理 17.11　令 $s(x)$ 為 $F[x]$ 上的一個非零多項式。

a) $F[x]$ 對同餘模 $s(x)$ 之關係的所有等價類在封閉二元運算

$$[f(x)]+[g(x)]=[f(x)+g(x)], \quad [f(x)][g(x)]=[f(x)g(x)]=[r(x)],$$

下形成一個具單位元素的交換環，其中 $r(x)$ 是 $f(x)g(x)$ 除以 $s(x)$ 的餘式。這個環被表為 $F[x]/(s(x))$。

b) 若 $s(x)$ 在 $F[x]$ 上是不可約的，則 $F[x]/(s(x))$ 是一個體。

c) 若 $|F|=q$ 且 degree $s(x)=n$，則 $F[x]/(s(x))$ 包含 q^n 個元素。

在繼續之前，我們將強調體 $F[x]/(s(x))$ 中的所有元素**不是**單純的 (x 之) 多項式，其中 $s(x)$ 在 $F[x]$ 上是不可約的。但這如何可為如此？考慮在例題 17.9 體 $\mathbf{Z}_2[x]/(x^2+x+1)$ 中元素 $[x]$ 及 $[x+1]$ 各個的符號 x 之出現。

為使我們的觀點更明朗，考慮一個無限的例題，其對我們有點熟悉。

例題 17.10

此處我們令 $F=(\mathbf{R}, +, \cdot)$，即實數體，且我們考慮 $\mathbf{R}[x]$ 上的不可約多項式 $s(x)=x^2+1$。由定理 17.11(b)，我們知道 $\mathbf{R}[x]/(s(x))=\mathbf{R}[x]/(x^2+1)$ 是一個體。

對所有 $f(x)\in\mathbf{R}[x]$，由除法演算法，得

$$f(x)=q(x)(x^2+1)+r(x), \quad \text{其中 } r(x)=0 \text{ 或 } 0\le \deg r(x)\le 1.$$

因此，

$$\mathbf{R}[x]/(x^2+1)=\{[a+bx]|a, b\in\mathbf{R}\},$$

其中可證明 $[a+bx]=[a]+[bx]=[a]+[b][x]$。

$\mathbf{R}[x]/(x^2+1)$ 的所有元素 (有無限多個) 是下面：

1) $[1]=\{1+t(x)(x^2+1)|t(x)\in\mathbf{R}[x]\}$，其中我們發現元素 x^2+2 及 $3x^3+3x+1$ (取自 $\mathbf{R}[x]$)；
2) $[r]=\{r+t(x)(x^2+1)|t(x)\in\mathbf{R}[x]\}$，其中 r 是任一(固定的) 實數；
3) $[-1]=\{-1+t(x)(x^2+1)|t(x)\in\mathbf{R}[x]\}$，其中我們發現多項式 $-1+(1)(x^2+1)=x^2$ ——所以，$[x][x]=[x^2]=[-1]$；且
4) $[\sqrt{2}x-3]=\{(\sqrt{2}x-3)+t(x)(x^2+1)|t(x)\in\mathbf{R}[x]\}$。

現在讓我們考慮複數體 $(\mathbf{C}, +, \cdot)$ 及對應

$$h: \mathbf{R}[x]/(x^2+1)\to\mathbf{C},$$

其中 $h([a+bx])=a+bi$。

對所有 $[a+bx], [c+dx]\in\mathbf{R}[x]/(x^2+1)$，我們有 $[a+bx]=[c+dx]\Leftrightarrow (a+bx)-(c+dx)=t(x)(x^2+1)$，對某些 $t(x)\in\mathbf{R}[x]\Leftrightarrow (a-c)+(b-d)x=t(x)(x^2+1)$。若 $t(x)$ 不是零多項式，則我們有 $(a-c)+(b-d)x$，一個次數小於 2 的多項式，等於 $t(x)(x^2+1)$，一個次數至少 2 的多項式。因此，$t(x)=0$，所以 $a+bx=c+dx$ 且 $a=c$，$b=d$。此保證 h 所給的對應確實是一個函數。事實上，h 是一個體的同構函數。(見本節習題 24) 欲建立 h 保留乘法運算，例如，我們觀察

$$\begin{aligned} h([a+bx][c+dx]) &= h([ac+adx+bcx+bdx^2]) \\ &= h([ac+(ad+bc)x]+[bd][x^2]) \\ &= h([ac+(ad+bc)x]+[bd][-1]) \\ &= h([ac-bd)+(ad+bc)x]) \end{aligned}$$

$$= (ac - bd) + (ad + bc)i = (a + bi)(c + di)$$
$$= h([a + bx])h([c + dx]).$$

因為 $\mathbf{R}[x]/(x^2+1)$ 同構於 $\mathbf{C}$，對應 $h([x])=i$ 令我們認為 $[x]$ 為 $\mathbf{R}[x]/(x^2+1)$ 上的一個**數** (number) 而非 ($\mathbf{R}[x]$ 上) x 的多項式。數 $[x]$ 表 $\mathbf{R}[x]$ 上多項式的一個等價類，且此數 $[x]$ 之行為像體 $(\mathbf{C}, +, \cdot)$ 中的複數 i。我們應亦注意到對每個實數 r，$h([r])=r$，且 $\{[r] | r \in \mathbf{R}\}$ 是 $\mathbf{R}[x]/(x^2+1)$ 的一個子體，其同構於 $\mathbf{C}$ 的子體 $\mathbf{R}$。

最後，若我們將體 $\mathbf{R}[x]/(x^2+1)$ 和體 $(\mathbf{C}, +, \cdot)$ 視為相同，我們可將上面所發生的整理如下：我們以 $\mathbf{R}[x]$ 上的不可約多項式 $s(x)=x^2+1$ 開始，其沒有根於體 $(\mathbf{R}, +, \cdot)$ 中。接著我們將 $(\mathbf{R}, +, \cdot)$ 擴大至 $(\mathbf{C}, +, \cdot)$，且在 $\mathbf{C}$ 中我們發現根 i (及一根 $-i$) 給 $s(x)$，其現可被因式分解為 $(x+i)(x-i)$ 於 $\mathbf{C}[x]$ 上。

因本章主要關心的是有限體，我們現在檢視有限體的另一個例子，其產生自定理 17.11。

例題 17.11

在 $\mathbf{Z}_3[x]$ 上，多項式 $s(x)=x^2+x+2$ 是不可約的，因為 $s(0)=2$，$s(1)=1$，且 $s(2)=2$。因此，$\mathbf{Z}_3[x]/(s(x))$ 是一個體，其包含形如 $[ax+b]$ 的所有等價類，其中 $a, b \in \mathbf{Z}$。這些來自多項式 $f(x) \in \mathbf{Z}_3[x]$ 被 $s(x)$ 除後可能的餘式。九個等價類為：$[0]$，$[1]$，$[2]$，$[x]$，$[x+1]$，$[x+2]$，$[2x]$，$[2x+1]$，及 $[2x+2]$。

不建構一個完整的乘法表，我們檢視四個樣本乘法及做兩個觀察。

a) $[2x][x]=[2x^2]=[2x^2+0]=[2x^2+(x^2+x+2)]=[3x^2+x+2]=[x+2]$，因 $3=0$ 於 $\mathbf{Z}_3$ 上。

b) $[x+1][x+2]=[x^2+3x+2]=[x^2+2]=[x^2+2+2(x^2+x+2)]=[2x]$。

c) $[2x+2]^2=[4x^2+8x+4]=[x^2+2x+1]=[(-x-2)+(2x+1)]$，因為 $x^2 \equiv (-x-2) \pmod{s(x)}$。因此，$[2x+2]^2=[x-1]=[x+2]$。

d) 我們經常不使用中括號來記等價類且集中在 x 的冪次方之係數。例如，11 表 $[x+1]$ 且 21 表 $[2x+1]$。因此，$(21)\cdot(12)=[2x+1][x+2]=[2x^2+5x+2]=[2x^2+2x+2]=[2(-x-2)+2x+2]=[-4+2]=[-2]=[1]$，所以，$(21)^{-1}=(12)$。

e) 我們亦觀察

$[x]^1=[x]$	$[x]^3=[2x+2]$	$[x]^5=[2x]$	$[x]^7=[x+1]$
$[x]^2=[2x+1]$	$[x]^4=[2]$	$[x]^6=[x+2]$	$[x]^8=[1]$

因此，$\mathbf{Z}_3[x]/(s(x))$ 的所有非零元素在乘法之下形成一個循環群。

f) 最後，當我們考慮等價類 [0]，[1]，[2] 時，我們明白它們提供我們 $\mathbf{Z}_3[x]/(s(x))$ 的一個子體——一個我們視同 $(\mathbf{Z}_3, +, \cdot)$ 的子體。

在例題 17.9 (及在其後之討論) 及在例題 17.11，我們分別建構了階數為 4 $(=2^2)$ 及階數為 9 $(=3^2)$ 的有限體。現在我們將以探討有限體階數的其它可能性作為本節的結束。欲達成這個，我們需下面概念。

定義 17.8

令 $(R, +, \cdot)$ 為一個環。若存在一個最小的正整數 n 滿足 $nr=z$ (R 的零) 對所有 $r \in R$，則我們稱 R 有**特徵數 *n*** (characteristic n) 且記 $\text{char}(R)=n$。當無此類整數存在時，稱 R 有特徵數 0。

例題 17.12

a) 環 $(\mathbf{Z}_3, +, \cdot)$ 有特徵數 3；$(\mathbf{Z}_4, +, \cdot)$ 有特徵數 4；一般來講，$(\mathbf{Z}_n, +, \cdot)$ 有特徵數 n。

b) 環 $(\mathbf{Z}, +, \cdot)$ 及 $(\mathbf{Q}, +, \cdot)$ 兩者均有特徵數 0。

c) 一個環可為無限的且仍然有正特徵數。例如，$\mathbf{Z}_3[x]$ 是一個無限環但它有特徵數 3。

d) 例題 17.9 的環有特徵數 2。例題 17.11 之環的特徵數是 3。不像 (a) 之例子，一個有限環的階數可不同於其特徵數。

然而，例題 17.9 及 17.11 不僅是環。它們是具有質特徵數的體。這個性質對所有的有限體可為真嗎？

定理 17.12

令 $(F, +, \cdot)$ 是一個體。若 $\text{char}(F)>0$，則 $\text{char}(F)$ 必為質數。

證明：在這個證明裡，我們記 F 的單位元素為 u 使得它不同於正整數 1。令 $\text{char}(F)=n>0$。若 n 不是質數，我們記 $n=mk$，其中 m，$k \in \mathbf{Z}^+$ 且 $1<m<n$，$1<k<n$。由特徵數的定義，$nu=z$，即 F 的零。因此 $(mk)u=z$。但

$$(mk)(u) = \underbrace{(u+u+\cdots+u)}_{mk\text{ 個被加項}} = \underbrace{(u+u+\cdots+u)}_{m\text{ 個被加項}}\underbrace{(u+u+\cdots+u)}_{k\text{ 個被加項}} = (mu)(ku).$$

由於 F 是一個體，$(mu)(ku)=z \Rightarrow (mu)=z$ 或 $(ku)=z$。不失一般性假設 $ku=z$。則對每個 $r \in F$，$kr=k(ur)=(ku)r=zr=z$，和 n 為 F 的特徵數矛盾。因此，$\text{char}(F)$ 是質數。

(定理 17.12 的證明事實上僅需 F 是一個整環。)

若 F 是一個有限體且 $m=|F|$，則 $ma=z$ 對所有 $a \in F$，因為 $(F, +)$ 是一個階數為 m 的加法群。(見 16.3 節習題 8)。因此，F 有正特徵數且由定理 17.12，此特徵數為質數。此引我們至下面定理。

定理 17.13 一個有限體 F 有階數 p^t，其中 p 為質數且 $t \in \mathbf{Z}^+$。

證明：因 F 是一個有限體，令 $\text{char}(F)=p$，是一個質數，且令 u 表單位元素及 z 為零元素。則 $S_0=\{u, 2u, 3u, \cdots, pu=z\}$ 是 F 上 p 個相異元素所成的集合。若否，$mu=nu$ 對 $1 \le m<n \le p$ 且 $(n-m)u=z$，其中 $0<n-m<p$。所以對所有 $x \in F$，我們發現 $(n-m)x=(n-m)(ux)=[(n-m)u]x=zx=z$，且這和 $\text{char}(F)=p$ 矛盾。若 $F=S_0$，則 $|F|=p^1$ 且結果成立。若否，令 $a \in F-S_0$，則 $S_1=\{ma+nu|0<m, n \le p\}$ 是 F 的子集合滿足 $|S_1| \le p^2$。若 $|S_1|<p^2$，則 $m_1a+n_1u=m_2a+n_2u$，其中 $0<m_1$，m_2，n_1，$n_2 \le p$ 且 m_1-m_2，n_2-n_1 中至少有一個不等於 0。若 $m_1-m_2=0$，則 $(m_1-m_2)a=z=(n_2-n_1)u$，其中 $0<|n_2-n_1|<p$。因此，對所有 $x \in F$，$|n_2-n_1|x=|n_2-n_1|(ux)=(|n_2-n_1|u)x=zx=z$，其中 $0<|n_2-n_1|<p=\text{char}(F)$，得另一個矛盾。若 $n_1-n_2=0$，則 $(m_1-m_2)a=z$，其中 $0<|m_1-m_2|<p$。因 F 是一個體且 $a \neq z$，我們知道 $a^{-1} \in F$，所以 $|m_1-m_2|u=|m_1-m_2|aa^{-1}=za^{-1}=z$，其中 $0<|m_1-m_2|<p$ ——還是另一個矛盾。因此，m_1-m_2 及 n_1-n_2 兩者均非 0。因此，$(m_1-m_2)a=(n_2-n_1)u \neq z$。選取 $k \in \mathbf{Z}^+$，使得 $0<k<p$ 且 $k(m_1-m_2) \equiv 1 (\text{mod } p)$。則 $a=k(m_1-m_2)a=k(n_2-n_1)u$，且 $a \in S_0$，又多一個矛盾。因此，$|S_1|=p^2$，且若 $F=S_1$，定理得證。若否，以 $b \in F-S_1$，繼續此法，則 $S_2=\{\ell b+ma+nu|0<\ell, m, n \le p\}$ 將有階數 p^3。(證之) 因為 F 是有限，我們可達 $F=S_{t-1}$ 對某些 $t \in \mathbf{Z}^+$，且 $|F|=|S_{t-1}|=p^t$。

由此定理，我們將沒有階數為 6，10，12，14，15，… 的有限體。此外，對每個質數 p 及每個 $t \in \mathbf{Z}^+$，確實是僅有一個階數為 p^t 的體。任兩個相同階數的有限體是同構的。這些體被發現於法國數學家 Evariste Galois (1811-1832) 在解次數 ≥ 5 佈於 $\mathbf{Q}$ 的一般多項式方程公式不存在的作品裡。因此，階數為 p^t 的有限體被表為 $GF(p^t)$，其中字母 GF 代表 Galois **體** (Galois field)。

習題 17.2

1. 試決定下面各個多項式在所給的體是否為不可約的。若它是可約的，將其分解成不可約的因式。
   a) x^2+3x-1 佈於 $\mathbf{Q}$，$\mathbf{R}$，$\mathbf{C}$。

b) x^4-2 佈於 $\mathbf{Q}$，$\mathbf{R}$，$\mathbf{C}$。

c) x^2+x+1 佈於 $\mathbf{Z}_3$，$\mathbf{Z}_5$，$\mathbf{Z}_7$。

d) x^4+x^3+1 佈於 $\mathbf{Z}_2$。

e) x^3+3x^2-x+1 佈於 $\mathbf{Z}^5$。

2. 給一個多項式 $f(x) \in \mathbf{R}[x]$，使其為次數 6，可約的，但沒有實根。
3. 求所有多項式 $f(x) \in \mathbf{Z}_2[x]$ 滿足 $1 \le$ degree $f(x) \le 3$ 且 $f(x)$ (在 $\mathbf{Z}_2$ 上) 是不可約的。
4. 令 $f(x)=(2x^2+1)(5x^3-5x+3)(4x-3) \in \mathbf{Z}_7[x]$。將 $f(x)$ 寫為一個可逆多項式及三個首項一多項式的乘積。
5. $\mathbf{Z}_7[x]$ 上有多少個次數為 5 的首項一多項式。
6. 證明定理 17.7。
7. 定理 17.8 的證明大綱如下：

   a) 令 $S=\{s(x)f(x)+t(x)g(x) | s(x), t(x) \in F[x]\}$。在 S 中選一個最小次數的元素 $m(x)$。(記得零多項式沒有次數，所以不選它。) 我們能保證 $m(x)$ 是首項一的嗎？

   b) 證明若 $h(x) \in F[x]$ 且 $h(x)$ 同時整除 $f(x)$ 及 $g(x)$，則 $h(x)$ 整除 $m(x)$。

   c) 證明 $m(x)$ 整除 $f(x)$。若否，使用除法演算法且記 $f(x)=g(x)m(x)+r(x)$，其中 $r(x) \ne 0$ 且 degree $r(x) <$ degree $m(x)$。接著證明 $r(x) \in S$ 且得一矛盾。

   d) 重複 (c) 的理論證明 $m(x)$ 整除 $g(x)$。
8. 證明定理 17.9 及 17.10。
9. 使用多項式的歐幾里得演算法，求下面各對多項式的 gcd，佈於指定的體 F。接著將 gcd 寫為 $s(x)f(x)+t(x)g(x)$，其中 $s(x)$，$t(x) \in F[x]$。

   a) $f(x)=x^2+x-2, g(x)=x^5-x^4+x^3+x^2-x-1$ 在 $\mathbf{Q}[x]$。

   b) $f(x)=x^4+x^3+1, g(x)=x^2+x+1$ 在 $\mathbf{Z}_2[x]$。

   c) $f(x)=x^4+2x^2+2x+2, g(x)=2x^3+2x^2+x+1$ 在 $\mathbf{Z}_3[x]$。
10. 若 F 是任一體，令 $f(x)$，$g(x) \in F[x]$。若 $f(x)$，$g(x)$ 互質，證明沒有 $a \in F$ 滿足 $f(a)=0$ 及 $g(a)=0$。
11. 令 $f(x)$，$g(x) \in \mathbf{R}[x]$ 且 $f(x)=x^3+2x^2+ax-b$，$g(x)=x^3+x^2-bx+a$。試決定 a，b 之值使得 $f(x)$，$g(x)$ 的 gcd 是次數為 2 的多項式。
12. 對例題 17.9，決定那一個等價類包含下面各題：

   a) x^4+x^3+x+1

   b) x^3+x^2+1

   c) $x^4+x^3+x^2+1$
13. 定理 17.11 證明的大綱如下。

   a) 證明若 $f(x) \equiv f_1(x) \pmod{s(x)}$ 且 $g(x) \equiv g_1(x) \pmod{s(x)}$，則 $f(x)+g(x) \equiv f_1(x)+g_1(x) \pmod{s(x)}$ 且 $f(x)g(x) \equiv f_1(x)\,g_1(x) \pmod{s(x)}$。來證明定理 17.11(a) 所定義的運算是有意義的。

   b) 證明 $F[x]/(s(x))$ 中所有等價的環性質。

   c) 令 $f(x) \in F[x]$，滿足 $f(x) \ne 0$ 且 degree $f(x) <$ degree $s(x)$。若 $s(x)$ 在 $F[x]$ 上不可約，為何可得 $f(x)$ 和 $s(x)$ 的 gcd 是 1？

   d) 使用 (c) 來證明若 $s(x)$ 在 $F[x]$ 上是不可約的，則 $F[x]/(s(x1))$ 是一個體。

   e) 若 $|F|=q$ 且 degree $s(x)=n$，求 $F[x]/(s(x))$ 的階數。
14. a) 證明 $s(x)=x^2+1$ 在 $\mathbf{Z}_2[x]$ 上不可約。

   b) 求環 $\mathbf{Z}_2[x]/(s(x))$ 的所有等價類。

   c) $\mathbf{Z}_2[x]/(s(x))$ 是一個整環嗎？
15. 對例題 17.11 的體求下面各題：

a) $[x+2][2x+2]+[x+1]$

b) $[2x+1]^2[x+2]$

c) $(22)^{-1}=[2x+2]^{-1}$

16. 令 $s(x)=x^4+x^3+1\in \mathbf{Z}_2[x]$。

a) 證明 $s(x)$ 是不可約的。

b) 體 $\mathbf{Z}_2[x]/(s(x))$ 的階數是多少？

c) 於 $\mathbf{Z}_2[x]/(s(x))$ 上求 $[x^2+x+1]^{-1}$。(提示：求 a，b，c，$d\in \mathbf{Z}_2$ 使得 $[x^2+x+1][ax^3+bx^2+cx+d]=[1]$。)

d) 決定 $[x^3+x+1][x^2+1]$ 於 $\mathbf{Z}_2[x]/(s(x))$。

17. p 為一質數，令 $s(x)$ 為 $\mathbf{Z}_p[x]$ 上次數為 n 的不可約多項式。

a) 體 $\mathbf{Z}_p[x]/(s(x))$ 中有多少個元素？

b) $\mathbf{Z}_p[x]/(s(x))$ 中有多少個元素生成這個體的非零元素所成的乘法群？

18. 給下面各個環的特徵數：

a) $\mathbf{Z}_{11}$　　b) $\mathbf{Z}_{11}[x]$　　c) $\mathbf{Q}[x]$

d) $\mathbf{Z}[\sqrt{5}]=\{a+b\sqrt{5}|a, b\in \mathbf{Z}\}$，在實數尋常的加法及乘法二元運算下。

19. 下面各個環，其運算是各分量相加及相乘，如 14.2 節習題 18。求各情形的特徵數。

a) $\mathbf{Z}_2\times\mathbf{Z}_3$　　b) $\mathbf{Z}_3\times\mathbf{Z}_4$　　c) $\mathbf{Z}_4\times\mathbf{Z}_6$

d) $\mathbf{Z}_m\times\mathbf{Z}_n$，對 m，$n\in \mathbf{Z}^+$，m，$n\geq 2$

e) $\mathbf{Z}_3\times\mathbf{Z}$

20. 對定理 17.13，證明 $|S_2|=p^3$。

21. 求階數 n 給所有體 $GF(n)$，其中 $100\leq n\leq 150$。

22. 建構一個 25 個元素的有限體。

23. 建構一個 27 個元素的有限體。

24. a) 證明例題 17.10 的函數 h 是一對一且映成且保留加法運算。

b) 令 $(F, +, \cdot)$ 及 $(K, \oplus, \odot)$ 為兩個體，若 $g: F\to K$ 是一個環同構函數且 a 是 F 的非零元素 (亦即，a 是 F 上的一個可逆元素)，證明 $g(a^{-1})=[g(a)]^{-1}$。(因此，函數 g 建立一個體的同構函數。特別地，例題 17.10 的函數 h 是一個這樣的函數。)

25. a) 令 $\mathbf{Q}[\sqrt{2}]=\{a+b\sqrt{2}|a, b\in \mathbf{Q}\}$。證明 $(\mathbf{Q}[\sqrt{2}], +, \cdot)$ 是體 $(\mathbf{R}, +, \cdot)$ 的一個子環。(此處 $\mathbf{R}$ 及 $\mathbf{Q}[\sqrt{2}]$ 的二元運算是實數尋常加法及乘法的二元運算。)

b) 證明 $\mathbf{Q}[\sqrt{2}]$ 是一個體且 $\mathbf{Q}[x]/(x^2-2)$ 同構於 $\mathbf{Q}[\sqrt{2}]$。

26. 令 p 為一質數。(a) $\mathbf{Z}_p[x]$ 上有多少個首項一之二次 (次數 2) 多項式 x^2+bx+c，我們可將它因式分解成 $\mathbf{Z}_p[x]$ 上的線性因式？(例如，若 $p=5$，則多項式 x^2+2x+2 在 $\mathbf{Z}_5[x]$ 上，將是一個我們將處理的二次多項式，在這些條件下。) (b) $\mathbf{Z}_p[x]$ 上有多少個二次多項式 ax^2+bx+c，我們可將它因式分解成 $\mathbf{Z}_p[x]$ 上的線性因式？(c) $\mathbf{Z}_p[x]$ 上有多少個首項一之二次多項式 ax^2+bx+c 在 $\mathbf{Z}_p$ 上是不可約的？(d) $\mathbf{Z}_p[x]$ 上有多少個二次多項式在 $\mathbf{Z}_p$ 上是不可約的？

17.3　Latin 方形

本章第一個應用處理一個所謂的 Latin 方形的結構。此類圖形出現在組合設計的研究上，且在統計學上扮演一個角色——在實驗的設計上。我們介紹這個結構於下面例題裡。

例題 17.13

某石油公司有興趣測試四種汽油添加劑來決定它們對里程的影響。欲如此做，研究團隊設計一個實驗，其中四種不同汽車，被表為 A，B，C，及 D，在實驗室的一個固定車道上跑。每次跑時使用同量的汽油及一種添加劑。欲瞭解每一種添加劑是如何影響各種型態的汽車，團隊依循表 17.3 的程序，其中添加劑被編碼為 1，2，3，及 4。此程序表提供以各種汽車測試每種添加劑的方法。假若某個添加劑於所有四種添加劑中產生最佳結果，則實驗顯示其優越的才能。

同一公司亦有興趣測試其它四種用來清理引擎的添加劑。這些測試的相同程序被示於表 17.4，其中這些清引擎的添加劑被表為 1，2，3，及 4。

表 17.3

汽車	日期			
	星期一	星期二	星期三	星期四
A	1	2	3	4
B	2	1	4	3
C	3	4	1	2
D	4	3	2	1

表 17.4

汽車	日期			
	星期一	星期二	星期三	星期四
A	1	2	3	4
B	3	4	1	2
C	4	3	2	1
D	2	1	4	3

更而，研究團隊有趣於結合這兩種型態添加劑的影響。需要 16 天來測試 16 對可能的添加劑 (一個用來改進里程，另一個用來清理引擎) 於每輛汽車。若結果需要 4 天，研究團隊必須設計程序使得每對添加劑被某輛汽車測試一次。{1, 2, 3, 4}×{1, 2, 3, 4} 中共有 16 個有序對，所以這可在打算的時間內完成若表 17.3 及 17.4 的程序重疊而得表 17.5 的程序。例如，元素 (4, 3) 說明在星期二，汽車 C 被用來測試用來改進里程的第四種添加劑及用來保養清理引擎的第三種添加劑。

表 17.5

汽車	日期			
	星期一	星期二	星期三	星期四
A	(1, 1)	(2, 2)	(3, 3)	(4, 4)
B	(2, 3)	(1, 4)	(4, 1)	(3, 2)
C	(3, 4)	(4, 3)	(1, 2)	(2, 1)
D	(4, 2)	(3, 1)	(2, 4)	(1, 3)

這裡所發生的引我們至下面概念。

定義 17.9

一個 $n \times n$ 的 Latin **方形** (Latin square) 是一個符號的方形陣列，通常符號為 1，2，3，…，n，其中每個符號在陣列的各列及各行恰出現一次。

例題 17.14

a) 表 17.3 及 17.4 是 4×4 Latin 方形的例子。

b) 對所有 $n \geq 2$，我們可由群 $(\mathbf{Z}_n, +)$ 的表中得一個 $n \times n$ Latin 方形若我們將所有的 0 改為 n。

由例題 17.13 的 Latin 方形，我們可以產生 $S \times S$ 中所有的序對，對 $S = \{1, 2, 3, 4\}$。我們來問是否可對一般的 $n \times n$ Latin 方形來做這個。

定義 17.10

令 $L_1 = (a_{ij})$，$L_2 = (b_{ij})$ 為兩個 $n \times n$ Latin 方形，其中 $1 \leq i, j \leq n$ 且每個 a_{ij}，$b_{ij} \in \{1, 2, 3, \cdots, n\}$。若所有 n^2 個序對 (a_{ij}, b_{ij})，$1 \leq i, j \leq n$，為相異，則 L_1，L_2 被稱是**一個正交的 Latin 方形對** (a pair of orthogonal Latin squares)。

例題 17.15

a) 沒有 2×2 正交的 Latin 方形對，因為唯一的可能性是

$$L_1: \begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix} \quad \text{及} \quad L_2: \begin{matrix} 2 & 1 \\ 1 & 2 \end{matrix}$$

b) 在 3×3 的情形，我們發現正交對為

$$L_1: \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix} \quad \text{及} \quad L_2: \begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix}$$

c) 例題 17.13 的兩個 4×4 Latin 方形形成一個正交對。表 17.6 所示的 4×4 Latin 方形正交於例題 17.13 的各個 Latin 方形。

表 17.6

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

我們可繼續列一些更大的 Latin 方形，但我們此刻已看夠它們，可來問下面問題：

1) 是否存在 $n>2$，其中沒有正交的 $n\times n$ Latin 方形對？若有，則此類 n 的最小值為何？
2) 對 $n>1$，可被建構每對均正交的 $n\times n$ Latin 方形有多少個？
3) 是否有方法幫我們來建構一個正交的 $n\times n$ Latin 方形對某個 $n>2$？

在我們可檢視這些問題之前，我們需將一些結果標準化。

定義 17.11

若 L 是一個 $n\times n$ Latin 方形，則稱 L 具**標準型** (standard form) 若其第一列是 $1, 2, 3, \cdots, n$。

除了例題 17.15(a) 的 Latin 方形 L_2 之外，我們在本節已見到的所有 Latin 方形均具標準型。若一個 Latin 方形不是標準型，則可藉著交換一些符號將它改為標準型。

例題 17.16

(a) 中的 5×5 Latin 方形不是標準型。然而，若我們將各個 4 改為 1，各個 5 改為 4，且各個 1 改為 5，則所得的結果是 (b) 中的 (標準) 5×5 Latin 方形。

4	2	3	5	1
1	3	5	4	2
3	4	2	1	5
2	5	1	3	4
5	1	4	2	3

(a)

1	2	3	4	5
5	3	4	1	2
3	1	2	5	4
2	4	5	3	1
4	5	1	2	3

(b)

處理具標準型的 Latin 方形是較方便的。但此會以任何方式影響正交對的結果嗎？

定理 17.14 令 L_1，L_2 是一個 $n\times n$ Latin 方形的正交對。若 L_1，L_2 被標準化為 L_1^*，L_2^*, 則 L_1^*，L_2^* 是正交的。

證明：此結果之證明留給讀者。

我們需要這些概念來給本節的主要結果。

定理 17.15 在 $n\in \mathbf{Z}^+$，$n>2$，雙雙正交的 $n\times n$ Latin 方形的可能最大數為 $n-1$。

證明：令 L_1，L_2，…，L_k 為 k 個相異的 $n\times n$ Latin 方形，且均具標準型及雙雙正交，我們以 $a_{ij}^{(m)}$ 表 L_m 的第 i 列及第 j 行的元素，其中 $1\le i, j\le n$，$1\le m\le k$。因為這些 Latin 方形均具標準型，我們有 $a_{11}^{(m)}=1$，$a_{12}^{(m)}=2$，…且 $a_{1n}^{(m)}=n$，對所有 $1\le m\le k$。現在考慮 $a_{21}^{(m)}$，對所有 $1\le m\le k$。這些位在第二列及第一行的元素是在 $a_{11}^{(m)}=1$ 之下。因此 $a_{21}^{(m)}\ne 1$，對所有 $1\le m\le k$，或圖形不是一個 Latin 方形。更而，若存在 $1\le \ell<m\le k$ 滿足 $a_{21}^{(\ell)}=a_{21}^{(m)}$，則 L_ℓ，L_m 這一對不可能是一個正交對。(為何不是？) 因此，存在 $n-1$ 個最佳選法給 a_{21} 元素於我們的 $n\times n$ Latin 方形中的任何一個，且由此觀察，結果成立。

此定理提供雙雙正交的 $n\times n$ Latin 方形個數的一個上界。我們將發現對某些 n，這個上界可得。此外，下一個定理提供一個方法來建構這些 Latin 方形，雖然一開始不具標準型。此建構使用有限體。然而，在證明這個定理一般情形之前，我們將檢視一個特殊情形。

例題 17.17 令 $F=\{f_i|1\le i\le 5\}=\mathbf{Z}_5$ 其中 $f_1=1$，$f_2=2$，$f_3=3$，$f_4=4$，且 $f_5=5$，為 $\mathbf{Z}_5$ 的零元素。

對 $1\le k\le 4$，令 L_k 為 5×5 陣列 $(a_{ij}^{(k)})$，其中 $1\le i, j\le 5$ 且

$$a_{ij}^{(k)}=f_kf_i+f_j.$$

當 $k=1$ 時，我們建構 $L_1=(a_{ij}^{(1)})$ 如下。此處 $a_{ij}^{(1)}=f_1f_i+f_j=f_i+f_j$，對 $1\le i, j\le 5$。以 $i=1$，L_1 的第一列被計算如下：

$$a_{11}^{(1)}=f_1+f_1=2 \qquad a_{12}^{(1)}=f_1+f_2=3 \qquad a_{13}^{(1)}=f_1+f_3=4$$
$$a_{14}^{(1)}=f_1+f_4=5 \qquad a_{15}^{(1)}=f_1+f_5=1$$

L_1 第二列的元素被計算當 $i=2$ 時。此處我們發現

$$a_{21}^{(1)}=f_2+f_1=3 \qquad a_{22}^{(1)}=f_2+f_2=4 \qquad a_{23}^{(1)}=f_2+f_3=5$$
$$a_{24}^{(1)}=f_2+f_4=1 \qquad a_{25}^{(1)}=f_2+f_5=2$$

繼續這些計算，我們得 Latin 方形 L_1 為

$$\begin{array}{ccccc} 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{array}$$

對 $k=2$，L_2 的所有元素以公式 $a_{ij}^{(2)}=f_2f_i+f_j=2f_i+f_j$ 給之。欲得 L_2 的第一列，我們設 $i=1$ 且計算

$$a_{11}^{(2)}=2f_1+f_1=3 \qquad a_{12}^{(2)}=2f_1+f_2=4 \qquad a_{13}^{(2)}=2f_1+f_3=5$$
$$a_{14}^{(2)}=2f_1+f_4=1 \qquad a_{15}^{(2)}=2f_1+f_5=2$$

當設定 $i=2$ 時，L_2 第二列的所有元素被計算如下：

$$a_{21}^{(2)}=2f_2+f_1=5 \qquad a_{22}^{(2)}=2f_2+f_2=1 \qquad a_{23}^{(2)}=2f_2+f_3=2$$
$$a_{24}^{(2)}=2f_2+f_4=3 \qquad a_{25}^{(2)}=2f_2+f_5=4$$

對 $i=3$，4，及 5 做相似計算得 Latin 方形 L_2 為

$$\begin{array}{ccccc} 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{array}$$

直接檢驗可得兩 Latin 方形 L_1 和 L_2 是正交的。在 (本節末的) 習題 5，讀者將被要求計算 L_3 及 L_4。下一個結果將證明 4 個陣列 L_1，L_2，L_3 和 L_4 為 Latin 方形且它們是雙雙正交的。

定理 17.16　令 $n\in\mathbf{Z}^+$，$n>2$。若 p 是一質數且 $n=p^t$，其中 $t\in\mathbf{Z}^+$，則存在 $n-1$ 個 $n\times n$ Latin 方形且雙雙正交。

證明：令 $F=GF(p^t)$，階數為 $p^t=n$ 的 Galois 體。考慮 $F=\{f_1, f_2, \cdots, f_n\}$，其中 f_1 是單位元素且 f_n 是零元素。

我們建構 $n-1$ 個 Latin 方形如下。

對每個 $1\le k\le n-1$，令 L_k 是 $n\times n$ 陣列 $(a_{ij}^{(k)})$，$1\le i, j\le n$，其中 $a_{ij}^{(k)}=f_kf_i+f_j$。

首先我們證明每個 L_k 是一個 Latin 方形。若否，有兩個相等的 F 元

素位在 L_k 的同一列或同一行。假設在某行有重複的值出現——亦即，$a_{rj}^{(k)} = a_{sj}^{(k)}$，其中 $1 \le r, s \le n$。則 $a_{rj}^{(k)} = f_k f_r + f_j = f_k f_s + f_j = a_{sj}^{(k)}$。此蘊涵 $f_k f_r = f_k f_s$，由於 F 之加法消去律。因為 $k \ne n$，得 $f_k \ne f_n$，F 的零元素。因此，f_k 是可逆的，所以 $f_r = f_s$ 且 $r = s$。同理可證明無重複值出現在 L_k 的任何一列。

此刻我們有 $n-1$ 個 Latin 方形，L_1，L_2，…，L_{n-1}。現在我們將證明它們是雙雙正交。若否，令 $1 \le k < m < n-1$ 滿足

$$a_{ij}^{(k)} = a_{rs}^{(k)}, \qquad a_{ij}^{(m)} = a_{rs}^{(m)}, \qquad 1 \le i, j, r, s \le n, \qquad \text{且} \qquad (i, j) \ne (r, s).$$

(則相同序對發生兩次當我們將 L_k 和 L_m 重疊時。) 但

$$a_{ij}^{(k)} = a_{rs}^{(k)} \Leftrightarrow f_k f_i + f_j = f_k f_r + f_s, \quad \text{且}$$
$$a_{ij}^{(m)} = a_{rs}^{(m)} \Leftrightarrow f_m f_i + f_j = f_m f_r + f_s.$$

將這兩方程式相減，我們發現 $(f_k - f_m)f_i = (f_k - f_m)f_r$。因 $k \ne m$，$(f_k - f_m)$ 不是 F 的零元素，所以它是可逆的且我們有 $f_i = f_r$。將這個代回前面兩方程式中的任何一個，我們發現 $f_j = f_s$。因此，$i = r$ 且 $j = s$。因此，對 $k \ne m$，Latin 方形 L_k 和 L_m 形成一個正交對。

不是質數冪次方的第一個 n 值是 6。一對 6×6 正交 Latin 方形的存在首先由 Leonhard Euler (1707-1783) 所探討的，當他在找一個解給“36 位軍官問題”時。這個問題處理 6 個不同兵團，其中有 6 位軍官，每個的官階均不同，被由各個兵團中選出。(僅有 6 種可能的官階。) 這個問題的目標是以一個 6×6 陣列安排 36 位軍官使得在陣列的各列或各行，每個階級及每個兵團恰被表示一次。因此，方形陣列中的每位軍官對應到一個序對 (i, j)，其中 $1 \le i, j \le 6$，i 表他的兵團且 j 表他的官階。1782 年，Euler 猜測這個問題不可能被解——沒有一對 6×6 正交 Latin 方形。他更進一步猜測對所有 $n \in \mathbf{Z}^+$，若 $n \equiv 2 \pmod 4$，則沒有一對 $n \times n$ 正交 Latin 方形。1900 年，G. Tarry 以分類枚舉所有可能的 6×6 Latin 方形，證明了 Euler 的猜測在 $n = 6$ 的結果。然而，直到 1960年，才由 R. C. Bose，S. S. Shrikhande，及 E. T. Parker 的共同努力，證明 Euler 剩餘的猜測是錯的。他們證明若 $n \in \mathbf{Z}^+$ 滿足 $n \equiv 2 \pmod 4$ 且 $n > 6$，則存在一對 $n \times n$ 正交 Latin 方形。

欲多知這個結果及一般的 Latin 方形，讀者應參訪本章參考資料。

習題 17.3

1. a) 將下面的 4×4 Latin 方形改為具標準型。

$$\begin{matrix} 1 & 3 & 4 & 2 \\ 3 & 1 & 2 & 4 \\ 2 & 4 & 3 & 1 \\ 4 & 2 & 1 & 3 \end{matrix}$$

   b) 找一個具標準型的 4×4 Latin 方形使其和 (a) 之結果正交。

   c) 應用 (a) 中方法的反方法至 (b) 之結果。證明您的答案正交於所給的 4×4 Latin 方形。
2. 證明定理 17.14。
3. 完成定理 17.16 第一部份的證明。
4. 表 17.3，17.4 及 17.6 的三個 4×4 Latin 方形是雙雙正交的。您可以再找另一個 4×4 Latin 方形使其和這三個 Latin 方形中的每一個正交嗎？
5. 完成例題 17.17 的計算以得二個 5×5 Latin 方形 L_3 及 L_4。將每個 Latin 方形 L_i，其中 $1 \le i \le 4$，改寫為具標準型。
6. 找三個雙雙正交的 7×7 Latin 方形。將這些結果改寫為具標準型。
7. 將例題 17.13 的實驗擴大使得研究團隊需三個雙雙正交的 4×4 Latin 方形。
8. Latin 方形 L 被稱是**自我-正交** (self-orthogonal) 若 L 和其轉置 L^{tr} 形成一正交對。

   a) 證明沒有 3×3 自我-正交 Latin 方形。

   b) 給一個自我-正交的 4×4 Latin 方形。

   c) 若 $L=(a_{ij})$ 是一個 $n \times n$ 自我-正交 Latin 方形，證明所有元素 a_{ii}，$1 \le i \le n$，必全相異。

17.4　有限幾何及仿射平面

在實數平面的歐幾里得幾何裡，我們發現 (a) 相異兩點決定一條唯一直線且 (b) 若 ℓ 是平面上的一直線，且 P 是不在 ℓ 上的一點，則存在一條唯一直線 ℓ' 包含 P 且與 ℓ 平行。在 18 及 19 世紀間，非歐幾何被發展當條件 (b) 的替代型被探討時。所有這些幾何包含無限多點及無限多直線。有限幾何的觀念並未出現直到 19 世紀末才出現在 Gino Fano (*Giornale di Matematiche*, 1892) 的作品裡。

我們如何可建構此一幾何？欲如此做，我們回到更熟悉的歐氏幾何。欲以代數方式描述這個平面上的點及直線，我們介紹坐標軸集合並以一個實數序對 (c, d) 來辨識各點 P。此描述建立了平面上點及集合 $\mathbf{R} \times \mathbf{R}$ 間的

一個一對一對應。藉由使用斜率的概念，我們可將此平面上的各直線唯一的表為不是 (1) $x=a$，其中斜率是無限大，就是 (2) $y=mx+b$，其中 m 是斜率；a，m，及 b 是實數。我們亦發現兩相異直線平行若且唯若它們有相同斜率。當它們的斜率是相異的，兩直線相交於一唯一點。

不使用實數 a，b，c，d，m 表點 (c, d) 及直線 $x=a$，$y=mx+b$，我們現在回到一個類比的**有限結構**，即有限體。我們的目標是建構一個所謂的 (有限) 仿射平面。

定義 17.12

令 $\mathcal{P}$ 是一個有限的點集合，且令 $\mathcal{L}$ 是 $\mathcal{P}$ 的子集合所成的集合，稱為直線。一個在集合 $\mathcal{P}$ 及 $\mathcal{L}$ 上的 **(有限) 仿射平面** (affine plane) 是一個有限結構滿足下面條件。

A1) $\mathcal{P}$ 上的兩相異點 (同時) 位在 $\mathcal{L}$ 上的唯一元素；亦即它們位在唯一的一直線上。

A2) 對每個 $\ell \in \mathcal{L}$，及每個 $P \in \mathcal{P}$ 滿足 $P \notin \ell$，存在一個唯一的元素 $\ell' \in \mathcal{L}$，其中 $P \in \ell'$ 及 ℓ，ℓ' 沒有共同點。

A3) 有 4 個點在 $\mathcal{P}$ 上，這 4 點中無 3 點共線 (亦即，這 4 點中無 3 點位在 $\mathcal{L}$ 的任一子集合 ℓ 上。)

條件 (A3) 的理由是避免圖 17.1 所示的不感興趣的情形。若僅有條件 (A1) 及 (A2) 被考慮，則這個系統將是一個仿射平面。

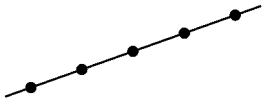

圖 17.1

我們現在回到我們的建構。令 $F=GF(n)$，其中 $n=p^t$ 對某些質數 p 及 $t \in \mathbf{Z}^+$。在建構仿射平面時，被表為 $AP(F)$，我們令 $\mathcal{P}=\{(c, d)|c, d \in F\}$。因此，我們有 n^2 個點。

我們應有多少條直線給集合 $\mathcal{L}$ 呢？

所有直線分成兩個範疇。無限大斜率的直線方程式是 $x=a$，其中 $a \in F$。因此，我們有 n 條此類“垂直線”。其它直線的代數式被給為 $y=mx+b$，其中 m，$b \in F$。因對 m 和 b 各有 n 個選擇，得有 n^2 條直線是非“垂直的”。因此，$|\mathcal{L}|=n^2+n$。

在我們證明 $AP(F)$，以所建構的 $\mathcal{P}$ 和 $\mathcal{L}$，是一個仿射平面之前，我們給另兩個觀察。

首先，對每條直線 $\ell \in \mathscr{L}$，若 ℓ 被給為 $x=a$，則有 n 個選擇給 y 在 $\ell=\{(a, y)|y \in F\}$。因此，ℓ 恰含 n 個點。若 ℓ 被給為 $y=mx+b$，其中 $m, b \in F$，則對每個 x 的選擇，y 唯一被決定，且再次 ℓ 有 n 個點。

現在考慮任一點 $(c, d) \in \mathscr{P}$。此點是位在直線 $x=c$ 上。更而，在有限斜率為 m 的各條直線 $y=mx+b$，$d-mc$ 唯一決定 b。以 n 個選擇給 m，我們看到點 (c, d) 位在 n 條形式為 $y=mx+(d-mc)$ 的直線上。所以，(c, d) 是在 $n+1$ 條直線上。

因此，在建構 $AP(F)$ 時，我們有一個點集合 $\mathscr{P}$ 及一個直線集合 $\mathscr{L}$，其中 (a) $|\mathscr{P}|=n^2$；(b) $|\mathscr{L}|=n^2+n$；(c) 每條 $\ell \in \mathscr{L}$ 包含 n 個點；及 (d) $\mathscr{P}$ 上各點恰位在 $n+1$ 條直線上。我們現在將證明 $AP(F)$ 滿足成為仿射平面的三個條件。

A1) 令 (c, d)，$(e, f) \in \mathscr{P}$。使用直線方程式的兩點公式，我們有

$$(e-c)(y-d)=(f-d)(x-c)$$

我們發現 (c, d) 及 (e, f) 均在直線上。這些點的各個均位在 $n+1$ 條直線上。可有第二條直線包含這兩點嗎？

點 (c, d) 是位在直線 $x=c$ 上。若 (e, f) 亦位在這條直線上，則 $e=c$，但 $f \neq d$，因這兩點相異。以 $e=c$，方程式 (1) 簡化為 $0=(f-d)(x-c)$，或 $x=c$，因為 $f-d \neq 0$，且所以我們沒有第二條直線。

以 $c \neq e$，若 (c, d)，(e, f) 位在形如 $y=mx+b$ 的第二條直線上，則 $d=mc+b$，$f=me+b$，且 $(f-d)=m(e-c)$。我們的係數是取自一個體且 $e \neq c$，所以 $m=(f-d)(e-c)^{-1}$ 且 $b=d-mc=d-(f-d)(e-c)^{-1}$。因此，這條含 (c, d) 及 (e, f) 的第二條直線是

$$y=(f-d)(e-c)^{-1}x+[d-(f-d)(e-c)^{-1}c]$$

或因為 F 上的乘法是可交換的，$(e-c)(y-d)=(f-d)(x-c)$ 即為方程式 (1)。因此，$\mathscr{P}$ 上兩點僅位在一直線上，則條件 (A1) 被滿足。

A2) 欲證明這個條件，考慮圖 17.2 所示的點 P 及直線 ℓ。因為在任一直線上有 n 個點，令 P_1，P_2，…，P_n 為 ℓ 上的所有點。(這些是 ℓ 上唯有的點，雖然圖上可能建議有其它點。) 點 P 不在 ℓ 上，所以 P 和 P_i 決定一唯一直線 ℓ_i，對每個 $1 \leq i \leq n$。我們稍早證明各點位在 $n+1$ 條直線上，所以現在有一條額外直線 ℓ' 使得 P 在 ℓ' 上且 ℓ' 和 ℓ 不相交。

A3) 最後條件使用體 F。因為 $|F| \geq 2$，F 上有單位元素 1 及零元素 0。考慮點 (0, 0)，(1, 0)，(0, 1)，(1, 1) 若直線 ℓ 包含這些點中的任何

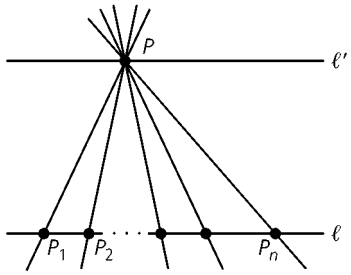

圖 17.2

三點，則之中的兩點之形式為 (c, c)，(c, d)。因此，ℓ 之方程式被給為 $x=c$，其不被 (d, c) 或 (d, d) 滿足。因此，這些點中無 3 點共線。

我們現在已證明了下面定理。

定理 17.17 若 F 是一個有限體，則基於點集合 $\mathcal{P}$ 及線集合 $\mathcal{L}$ 的系統，如上面所描述的，是一個仿射平面且被表為 $AP(F)$。

一些特殊例題將說明有限幾何，或仿射平面，及前節的 Latin 方形之間的聯結。

例題 17.18 對 $F=(\mathbf{Z}_2, +, \cdot)$，我們有 $n=|F|=2$。圖 17.3 的仿射平面有 $n^2=4$ 個點及 $n^2+n=6$ 條直線。例如，直線 $\ell_4=\{(1, 0), (1, 1)\}$，且 ℓ_4 沒包含圖可建議的其它點。更而，ℓ_5 和 ℓ_6 在這個有限幾何上是平行線，因為它們不相交。

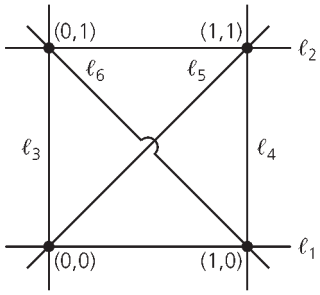

圖 17.3

例題 17.19 令 $F=GF(2^2)$ ——為例題 17.9 的體。回憶例題 17.11(d) 的記號且記 $F=\{00, 01, 10, 11\}$，具表 17.7 所給的加法及乘法。我們使用這個體來建構一個含 $n^2=16$ 個點及 $n^2+n=20$ 條直線的有限幾何。這 20 條直線可被分

表 17.7

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

·	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

割成五個**平行類** (parallel classes)，每個平行類有 4 條直線。

類 1：此處我們有無限大斜率的直線。這 4 條“垂直”線被給為方程式 $x=00$，$x=01$，$x=10$ 及 $x=11$。

類 2：對“水平”類，或斜率為 0 的類，我們有 4 條直線 $y=00$，$y=01$，$y=10$，及 $y=1$。

類 3：具斜率 01 的直線之方程式為 $y=01x+00$，$y=01x+01$，$y=01x+10$，及 $y=01x+11$。

類 4：這個類由方程式為 $y=10x+00$，$y=10x+01$，$y=10x+10$，及 $y=10x+11$ 的直線所組成。

類 5：最後一類的 4 條直線為 $y=11x+00$，$y=11x+01$，$y=11x+10$，及 $y=11x+11$。

因為在 $AP(F)$ 上的每條直線包含 4 點及每個平行類含有 4 條直線，我們現在將看看這些平行類中的 3 個如何分割 $AP(F)$ 上的所有 16 個點。

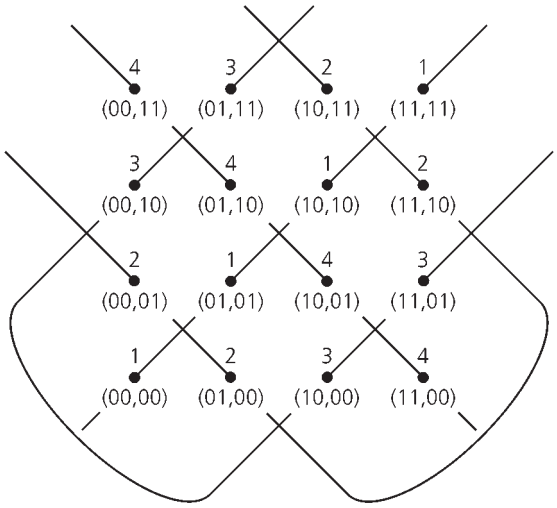

圖 17.4

對含 $m=01$ 的這一類，有 4 條直線：(1) $y=01x+00$; (2) $y=01x+01$; (3) $y=01x+10$; 及 (4) $y=01x+11$。上面在 $AP(F)$ 上的各點，我們寫下對應到它所在的直線碼。(見圖 17.4)。這個圖可由下面的 Latin 方形

$$\begin{array}{cccc} 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{array}$$

給之。

若我們重複這個方法給類 4及類 5，我們分別得到圖 17.5 及 17.6 所示的分割。在各類中，直線被列出，對所給的斜率，和圖 17.4 相同的順位。各圖中含有其對應的 Latin 方形。

這些圖給我們 3 個雙雙正交的 4×4 Latin 方形。

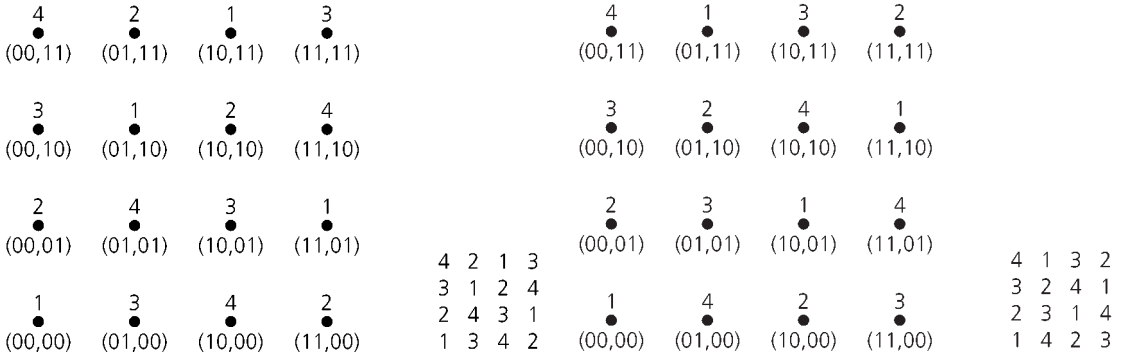

圖 17.5　　圖 17.6

此例題之結果並不意外，如下面定理所描述的。

定理 17.18　令 $F=GF(n)$，其中 $n \geq 3$ 且 $n=p^t$，p 為一質數，$t \in \mathbf{Z}^+$。來自有 $n-1$ 個平行類，其中斜率既不是 0 也不是無限大的 $AP(F)$ 之 Latin 方形，是雙雙正交的。

證明：本結果之證明被概述於本節習題裡。

習題 17.4

1. 完成下面處理仿射平面的表。

體	點數	直線數	在直線上的點數	過一點的直線數
	25			
$GF(3^2)$				
		56		
				17
			31	

2. 習題 1 的各個仿射平面決定多少個平行類？每個平行類有多少條直線。
3. 建構仿射平面 $AP(\mathbf{Z}_3)$。決定其平行類並對有限非零斜率的平行類決定其對應的 Latin 方形。
4. 以 $\mathbf{Z}_5$ 取代 $\mathbf{Z}_3$，重做習題 3。
5. 決定下面各條直線。
   a) $AP(\mathbf{Z}_7)$ 上的直線平行 $y=4x+2$ 且含點 (3, 6)。
   b) $AP(\mathbf{Z}_{11})$ 上的直線平行 $2x+3y+4=0$ 且含點 (10, 7)。
   c) $AP(F)$ 上的直線，其中 $F=GF(2^2)$，平行 $10y=11x+01$ 且含 (11, 01)(見表 17.7)。
6. 假設我們試著來建構一個仿射平面 $AP(\mathbf{Z}_6)$ 如我們在本節所做的。
   a) 試決定條件 (A1)，(A2)，及 (A3) 在此時那一個不滿足。
   b) 對這個“幾何”，有多少條線包含一已知點 P 及有多少個點位在一已知直線 l上。
7. 下面提供定理 17.18 證明之概述。
   a) 考慮直線 $y=mx+b$ 的一平行類，其中 $m \in F$，$m \neq 0$。證明此類的每條線和每條“垂直”線及每條“水平”線恰相交於 $AP(F)$ 上的一點。因此，利用標示 $AP(F)$ 的所有點所得的圖形，如圖 17.4，17.5 及 17.6，是一個 Latin 方形。
   b) 欲證明對應到兩個不同類的 Latin 方形，斜率 0 或無限斜率類除外，是正交的，假設序對 (i, j) 出現超過一次，當一個方形重疊在另一個方形之上時。此會引至一個矛盾嗎？

17.5 區組設計及投影平面

在這個末節，我們檢視一種組合設計型態，並看看它和有限幾何結構有何關係。下面例題將展示這個設計。

例題 17.20

Dick (d) 和他的夫人 Mary (m) 帶著他們的五個小孩—— Richard (r)，Peter (p)，Christopher (c)，Brain (b)，及 Julie (j)，一起去紐約市。在他們停留紐約市期間，他們每天得到 3 張通行證，共一星期，訪問帝國大廈。我們能夠做一張行程表給這家庭，使得每個人訪問這迷人的地方相同次數嗎？

下面行程表是一種可行性。

1) b, c, d	2) b, j, r	3) b, m, p	4) c, j, m
5) c, p, r	6) d, j, p	7) d, m, r	

此處之結果是由試驗和錯誤而得。對一個這個大小的問題，此一技巧是可行的。然而，一般上，一個更有效率的技巧是需要的。更而，在要求某一個行程表時，我們可要求一些不存在的東西。例如，在這個問題裡，每對家庭成員僅一起訪問一次。若這個家庭每天收到 4 張通行證，我們將無法建構一個保留這個性質的行程表。

上例之情形，將如下來一般化。

定義 17.13

令 V 是一個含 v 個元素的集合。一個由 V 的子集合所成的集族 $\{B_1, B_2, \cdots, B_b\}$ 被稱是一個**平衡的不完全區組設計** (balanced incomplete block design)，或被稱為 (v, b, r, k, λ)- 設計，假若下面條件被滿足：

a) 對每個 $1 \le i \le b$，子集合 B_i 包含 k 個元素，其中 k 是一個固定常數且 $k < v$。
b) 每個元素 $x \in V$ 位在所有子集 B_i，$1 \le i \le b$，r ($\le b$) 次。
c) 每對 V 的元素 x，y 一起出現在所有子集合 B_i，$1 \le i \le b$，λ ($\le b$) 次。

V 的元素經常被稱為**變種** (varieties)，因為早期在實驗設計的應用是在測試肥料及植物。V 的 b 個子集合 B_1，B_2，$\cdots$，B_b 被稱為**區組**

(blocks)，其中每個區組含有 k 個變種。r 被述為設計的**複製數** (replication number)。最後，λ 被稱是設計的**共價數** (covalency)。這個參數以下面意義使設計平衡。對一般的區組設計，我們有一個數 λ_{xy} 給每對 $x, y \in V$；若 λ_{xy} 對 V 的各對元素均相同，則以 λ 表示這個共同量度且稱這個設計是**平衡的** (balanced)。本書將僅處理平衡設計。

例題 17.21

a) 例題 17.20 的行程表是一個 (7, 7, 3, 3, 1) -設計的例子。

b) 對 $V=\{1, 2, 3, 4, 5, 6\}$，十個區組。

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

組成一個 (6, 10, 5, 3, 2)- 設計。

c) 若 F 是一個有限體，且 $|F|=n$，則仿射平面 $AP(F)$ 產生一個 $(n^2, n^2+n, n+1, n, 1)$- 設計。此處之變種是 $AP(F)$ 上的 n^2 個點；所有 n^2+n 條直線是設計的所有區組。

目前有五個參數決定我們的設計。我們現在來檢視這些參數的相關性。

定理 17.19

對一個 (v, b, r, k, λ)- 設計，(1) $vr=bk$ 且 (2) $\lambda(v-1)=r(k-1)$。

證明：

1) 因設計中有 b 個區組及每個區組有 k 個元素，將所有區組的所有元素列出，我們得 bk 個符號。此符號集由 V 的所有元素組成且每個元素出現 r 次，故共有 vr 個符號。因此，$vr=bk$。

2) 對此性質，我們介紹**雙雙投引矩陣** (pairwise incidence matrix) A 給這個設計。因 $|V|=v$，令 $t=\binom{v}{2}$，為 V 的元素對對數。我們建構 $t\times b$ 矩陣 $A=(a_{ij})$ 為定義 $a_{ij}=1$ 若 V 的第 i 對元素位在設計的第 j 個區組；若否，則定義 $a_{ij}=0$。

$$
\begin{array}{c} \\ x_1x_2 \\ x_1x_3 \\ \vdots \\ x_1x_v \\ x_2x_3 \\ \vdots \\ x_{v-1}x_v \end{array}
\begin{array}{c}
\begin{array}{cccc} B_1 & B_2 & \cdots & B_b \end{array} \\
\begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1b} \\
a_{21} & a_{22} & \cdots & a_{2b} \\
\vdots & \vdots & \vdots & \vdots \\
a_{v-1\,1} & a_{v-1\,2} & \cdots & a_{v-1\,b} \\
a_{v\,1} & a_{v\,2} & \cdots & a_{v\,b} \\
\vdots & \vdots & \vdots & \vdots \\
a_{t\,1} & a_{t\,2} & \cdots & a_{t\,b}
\end{bmatrix}
\end{array}
$$

我們現在以兩種方法計數矩陣 A 中 1 的個數。

a) 考慮所有列。因為每對 x_i，x_j，其中 $1 \le i < j \le v$，出現在 λ 個區組，得每列包含 λ 個 1。矩陣有 t 列，所以 1 的個數是 $\lambda t = \lambda v(v-1)/2$。

b) 現在考慮所有行。因每個區組有 k 個元素，此決定 $\binom{k}{2} = k(k-1)/2$ 對，且這是矩陣 A 各行的 1 之個數。因共有 b 行，所以 1 的總個數是 $bk(k-1)/2$。

接著，$\lambda v(v-1)/2 = bk(k-1)/2 = vr(k-1)/2$，所以 $\lambda(v-1) = r(k-1)$。

如我們稍早所提的，當 n 是某質數的一個冪次方時，可由仿射平面 $AP(F)$ 得到一個 $(n^2, n^2+n, n+1, n, 1)$- 設計，其中 $F = GF(n)$。這裡的點是變種且直線是區組。我們現在將介紹一個建構，其將 $AP(F)$ 擴大至一個所謂的有限投影平面。由這個投影平面我們可建構一個 $(n^2+n+1, n^2+n+1, n+1, n+1, 1)$- 設計。首先讓我們看看如何比較這兩種平面。

定義 17.14

若 $\mathcal{P}'$ 是一個有限點集合且 $\mathcal{L}'$ 是一個直線集合，$\mathcal{L}'$ 中的各個元素是 $\mathcal{P}'$ 的非空子集合，則基於 $\mathcal{P}'$ 和 $\mathcal{L}'$ 的 (有限) 平面被稱是一個**投影平面** (projective plane) 若滿足下面條件。

P1) $\mathcal{P}'$ 上的兩相異點僅位在一直線上。
P2) $\mathcal{L}'$ 上的任兩條直線僅相支於一點。
P3) $\mathcal{P}'$ 上有 4 點，其中無 3 點共線。

仿射平面和投影平面間的差異在於處理平行直線的存在條件。基於 $\mathcal{P}$ 和 $\mathcal{L}$ 的仿射平面之平行直線將相交，當已知系統被擴大至基於 $\mathcal{P}'$ 和 $\mathcal{L}'$ 的投影平面時。

建構將如下進行。

例題 17.22

以一個仿射平面 $AP(F)$ 開始，其中 $F = GF(n)$。對每個點 $(x, y) \in \mathcal{P}$，改寫此點為 $(x, y, 1)$。接著我們將所有點考慮為三元序對 (x, y, z)，其中 $z = 1$。將 $AP(F)$ 中的直線 $x = c$ 及 $y = mx + b$ 之方程式改寫為 $x = cz$ 及 $y = mx + bz$，其中 $z = 1$。我們仍然有原始的仿射平面 $AP(F)$，但記法改變。

將點集合 $\{(1, 0, 0)\} \cup \{(x, 1, 0) | x \in F\}$ 加至 $\mathcal{P}$，以得集合 $\mathcal{P}'$。則 $|\mathcal{P}'| = n^2+n+1$。令 ℓ_∞ 為 $\mathcal{P}'$ 的子集合，其由這些新點組成。這條新直線可被給為方程式 $z = 0$，依規定，我們從未有 $x = y = z = 0$。因此，$(0, 0, 0) \notin \mathcal{P}'$。

現在讓我們對仿射平面 $AP(\mathbf{Z}_2)$ 檢視這些概念。此時 $\mathcal{P}=\{(0,0),(1,0),(0,1),(1,1)\}$，所以

$$\mathcal{P}'=\{(0,0,1),(1,0,1),(0,1,1),(1,1,1)\}\cup\{(1,0,0),(0,1,0),(1,1,0)\}.$$

$\mathcal{L}$ 上這 6 條直線原先是

$x=0$: $\{(0,0),(0,1)\}$　　$y=0$: $\{(0,0),(1,0)\}$　　$y=x$: $\{(0,0),(1,1)\}$
$x=1$: $\{(1,0),(1,1)\}$　　$y=1$: $\{(0,1),(1,1)\}$　　$y=x+1$: $\{(0,1),(1,0)\}$

我們將它們改寫為

$$x=0\quad y=0\quad y=x\quad x=z\quad y=z\quad y=x+z$$

並加一條定義為 $z=0$ 的新直線 ℓ_∞。這些組成直線集合 $\mathcal{L}$ 給投影平面。且目前我們考慮 z 為一個**變數** (variable)。因此，直線 $x=z$ 由點 (0, 1, 0)，(1, 0, 1) 及 (1, 1, 1) 所組成。事實上，$\mathcal{L}$ 上包含兩點的每一條直線，現在將包含 3 個點當其被考慮在 $\mathcal{L}'$ 上時。集合 $\mathcal{L}'$ 由下面 7 條直線組成。

$x=0$: $\{(0,0,1),(0,1,0),(0,1,1)\}$　　$y=z$: $\{(1,0,0),(0,1,1),(1,1,1)\}$
$y=0$: $\{(0,0,1),(1,0,0),(1,0,1)\}$　　$y=x$: $\{(0,0,1),(1,1,0),(1,1,1)\}$
$x=z$: $\{(0,1,0),(1,0,1),(1,1,1)\}$　　$y=x+z$: $\{(0,1,1),(1,1,0),(1,0,1)\}$
$z=0$ (ℓ_∞): $\{(1,0,0),(0,1,0),(1,1,0)\}$

在原先的仿射平面，直線 $x=0$ 及 $x=1$ 是平行的，因為這平面上沒有點可同時滿足這兩個方程式。但在這個新系統裡，$x=0$ 和 $x=z$ 相交於點 (0, 1, 0)，所以它們不再是 $AP(\mathbf{Z}_2)$ 上的平行。同樣的，$y=x$ 及 $y=x+1$ 在 $AP(\mathbf{Z}_2)$ 上是平行的，而直線 $y=x$ 和 $y=x+z$ 相交於點 (1, 1, 0)。我們描繪這個基於 $\mathcal{P}'$ 和 $\mathcal{L}'$ 的投影平面於圖 17.7。這裡通過 (1, 0, 1)，(1, 1, 0) 及

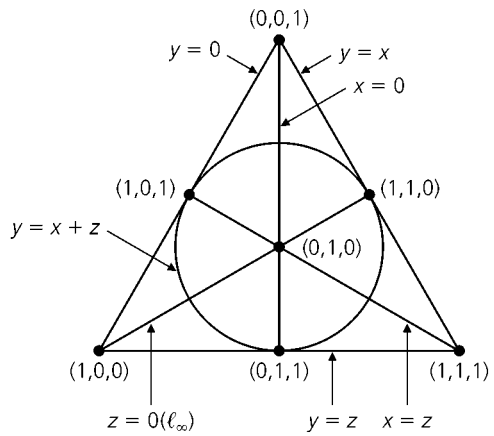

圖 17.7

(0, 1, 1) 的“圓”即是直線 $y=x+z$。注意每條直線與 ℓ_∞ 相交，ℓ_∞ 經常被稱是**直線在無窮** (line at infinity)。這條直線由 3 個**點在無窮** (points at infinity) 組成。我們定義投影平面上的兩條直線為平行當它們相交於一點在無窮 (或在 ℓ_∞ 上)。

此投影平面提供我們一個 (7, 7, 3, 3, 1) -設計，就像我們在例題 17.20 以試驗及錯誤所發展的那一個設計。

我們將例題 17.22 的結果一般化如下：令 n 為某質數的一個冪次方。仿射平面 $AP(F)$，其中 $F=GF(n)$，提供一個 $(n^2, n^2+n, n+1, n, 1)$ -設計的例子。在 $AP(F)$ 上，n^2+n 條直線分成 $n+1$ 個平行類。對每個平行類，我們加一點在無窮至 $AP(F)$。點 (0, 1, 0) 被加給直線 $x=cz$ 的類，$c \in F$；點 (1, 0, 0) 給直線 $y=bz$ 的類，$b \in F$。當 $m \in F$ 及 $m \neq 0$，則我們將點 $(m^{-1}, 1, 0)$ 加給直線 $y=mx+bz$ 的類，$b \in F$。直線在無窮，ℓ_∞，則被定義為 $n+1$ 個點在無窮的集合。依此法，我們得到佈於 $GF(n)$ 的投影平面，其有 n^2+n+1 個點及 n^2+n+1 條直線。這裡每個點在 $n+1$ 條直線上，且每條直線有 $n+1$ 個點。更而，此平面上的任兩點僅位在一條直線上。因此，我們有一個 $(n^2+n+1, n+1, n^2+n+1, n+1, 1)$ - 設計的例子。

習題 17.5

1. 令 $V=\{1, 2, \cdots, 9\}$。決定 v，b，r，k 及 λ 值給由下面區組所給的設計。

126 147 234 279 378 468
135 189 258 369 459 567

2. 找一個 (4, 4, 3, 3, λ) -設計的例子。
3. 找一個 (7, 7, 4, 4, λ) -設計的例子。
4. 完成右表使得在任一列中的參數 v，b，r，k，λ 是可能的對一個平衡不完全區組設計。

v	b	r	k	λ
4			3	2
9	12		3	
10		9		2
13		4	4	
	30	10		3

5. 可能有一個 (v, b, r, k, λ) -設計嗎？其中 (a) $b=28$，$r=4$，$k=3$; (b) $v=17$，$r=8$，$k=5$。
6. 給一個具 $b=v$ 的 (v, b, r, k, λ) -設計，證明若 v 是偶數，則 λ 是偶數。
7. 一個 (v, b, r, k, λ) -設計被稱是**三維系統** (triple system) 若 $k=3$。當 $k=3$ 且 $\lambda=1$，我們稱這個設計為一個 **Steiner 三維**

系統 (Steiner triple system)。

a) 證明在每個三維系統，$\lambda(v-1)$ 是偶數且 $\lambda v(v-1)$ 可被 6 整除。

b) 證明在每個三維系統，v 是同餘 1 或 3 模 6。

8. 證明下面區組組成一個有 9 種變種的 Steiner 三維系統。

1 2 8	1 4 7	2 3 4	2 7 9	3 8 9	4 6 8
1 3 5	1 6 9	2 5 6	3 6 7	4 5 9	5 7 8

9. 對一個具 $b=12$ 的 Steiner 三維系統，求 v 和 r 值。

10. 下面各小題，$\mathcal{P}'$ 是一個點集合且 $\mathcal{L}'$ 是一個直線集合，每條直線是 $\mathcal{P}'$ 的非空子集。定義 17.14 的條件 (P1)，(P2)，及 (P3) 中有那些條件對所給的 $\mathcal{P}'$ 及 $\mathcal{L}'$ 成立。

a) $\mathcal{P}'=\{a, b, c\}$

$\mathcal{L}'=\{\{a, b\}, \{a, c\}, \{b, c\}\}$

b) $\mathcal{P}'=\{(x, y, z)|x, y, z \in \mathbf{R}\}=\mathbf{R}^3$

$\mathcal{L}'$ 是 $\mathbf{R}^3$ 上所有直線所成的集合。

c) $\mathcal{P}'$ 是 $\mathbf{R}^3$ 上通過 (0, 0, 0) 的所有直線所成的集合。

$\mathcal{L}'$ 是 $\mathbf{R}^3$ 上通過 (0, 0, 0) 的所有平面所成的集合。

11. 五位學生組成的保齡隊，每隊由有 15 位大一新生的班級來組成。每位學生參加的隊數相同；每兩位學生一起參加兩隊。(a) 共有多少隊？(b) 每位學生參加多少隊相異的球隊？

12. Mackey 太太給她的電腦課 28 個問題且指導每位學生寫程式來恰解這些問題中的 7 個問題。若每位學生按照指示來做且若每兩個問題恰有一對學生寫程式解它們，試問 Mackey 太太班上有多少位學生？

13. 考慮一個在變種集 V 上的 (v, b, r, k, λ)-設計，其中 $|V|=n \geq 2$。若 $x, y \in V$，在這個設計裡有多少個區組不是包含 x 就是包含 y？

14. 在 Madge 教授的程式設計課共有 n 位學生，且她想指派由 m 位學生所組成的團隊 p 個電腦設計中的每個。若每位學生必被指派的設計個數相同。(a) 每位學生獨自做多少個設計？(b) 每對學生負責多少個設計？

15. a) 若某投影平面有 6 條直線通過每一點，則這個投影平面共有多少個點？

b) 若投影平面有 57 個點，則有多少個點位在這個平面的每條直線上？

16. 在例題 17.22 中，在由 $AP(\mathbf{Z}_2)$ 建構投影平面時，為何我們不想將點 (0, 0, 0) 包含至集合 $\mathcal{P}'$ 中呢？

17. 對由 $AP(F)$ 所得之投影平面所結合的平衡不完全區組設計，求其 v，b，r，k，及 λ 值，其中 F 為下面之選擇：(a) $\mathbf{Z}_5$，(b) $\mathbf{Z}_7$，(c) $GF(8)$。

18. a) 列出 $AP(\mathbf{Z}_3)$ 上的所有點及直線。這個有限幾何有多少個平行類？其所結合的平衡不完全區組設計的參數是什麼？

b) 列出由 $AP(\mathbf{Z}_3)$ 所產生的投影平面之所有點及直線。決定 ℓ_∞ 上的所有點，並使用它們來決定這個幾何的“平行”類。其所結合的平衡不完全區組設計的參數是什麼？

17.6 總結及歷史回顧

體的結構首先發展於第 14 章。本章我們檢視多項式環及其在有限體結構中的角色，引導我們的注意力至有限幾何及組合設計方面的應用。

在第 15 章，我們見到有限布林代數的階數僅能為 2 的某個冪次方。現在我們發現有限體的階數僅能是某質數的一個冪次方，且發現對每個質數 p 及每個 $n \in \mathbf{Z}^+$，僅存在一個，至多同構，階數為 p^n 的體。此體被表為 $GF(p^n)$，以紀念法國數學家 Evariste Galois (1811-1832)。

Evariste Galois (1811-1832)

有限體 $(\mathbf{Z}_p, +, \cdot)$，p 為一質數，被獲得於第 14 章，其係以定義在 $\mathbf{Z}$ 上，同餘模 p 的等價關係而得。使用這些有限體，我們發展了整環 $\mathbf{Z}_p[x]$。接著，以 $\mathbf{Z}_p[x]$ 上一個次數為 n 的不可約多項式 $s(x)$，一個類似等價關係，即同餘模 $s(x)$，給我們一個有 p^n 個等價類的集合，表為 $\mathbf{Z}_p[x]/(s(x))$。這 p^n 個等價類成為體 $GF(p^n)$ 的所有元素。(雖然我們不證明每一個可能的一般結果，但可證明佈於體 $\mathbf{Z}_p$ 上，存在一個次數為 n 的不可約多項式，對每個 $n \in \mathbf{Z}^+$。)

有限體理論被 Galois 發展於他的多項式方程式解問題之作品裡。如我們在第 16 章總結所提的，多項式方程的研究是許多數學家由 16 世紀至 19 世紀的研究領域之一。在 19 世紀，Niels Henrik Abel (1802-1829) 首先證明一般的五次方程的解不能為有理根。Galois 證明對任一個佈於體 F 次數為 n 的多項式，存在一個對應群 G 和 S_n 的子群同構，S_n 是 $\{1, 2, 3, \cdots, n\}$ 的排列群。Galois 作品的本質是這樣的多項式可被以 (加法，減法，乘

法，乘法，及) 根號來解若其對應群是**可解的** (solvable)。現在什麼可使一個有限群可解呢？我們說一個有限群 G 是可解的若它有一個子群鏈 $G = K_1 \supset K_2 \supset K_3 \supset \cdots\cdots \supset K_t = \{e\}$，其中對所有 $2 \le i \le t$，K_i 是 K_{i-1} 的正規子群 (即 $xyx^{-1} \in K_i$ 對所有 $y \in K_i$ 及對所有 $x \in K_{i-1}$)，及商群 K_{i-1}/K_i 是可交換的。吾人發現 S_i 的所有子群，$1 \le i \le 4$，是可解的，但對 $n \ge 5$，則存在 S_n 的子群是不可解的。

雖然 Galois 理論看起來似乎是顯著的考慮群，但它包含更多我們未提到的體之理論。

欲知更多的 Galois 理論，讀者將發現 V. H. Larney [8] 的第 6 章及 N. H. McCoy 和 T. R. Berger [10] 的第 12 章是開始的好章節。I. N. Herstein [6] 的第 5 章有更多的題材，而詳細的呈現可被發現於 S. Roman [11] 及 O. Zariski 和 P. Samuel [17] 的古典作品裡。V. H. Larney [8] 的附錄 E 有簡短有趣的 Galois 一生介紹；更多他的一生可被發現於有點虛構的 L. Infeld [7] 書裡。T. Rothman [12] 的文章提供一個他的一生中不正確及傳奇的當代討論，尤其是 Galois 的死因。J. Stillwell [14] 之 p.p.287-291 所記的傳記中提到更多有關他的一生及這個偉大天才的作品。

本章較後幾節的 Latin 方形、組合設計，及有限幾何說明有限體結構是如何進入設計的問題，可追朔到 Leonhard Euler (1707-1783) 的時代及“36 位軍官”的問題。正交 Latin 方形的研究自 1900 年已被廣泛的發展，且尤其是自 1960 年 R. C. Bose，S. S. Shrikhandle，及 E. T. Parker 的研究。H. J. Ryser [13] 專題論文的第 7 章提供他們的作品細節。C. L. Liu [9] 將編碼理論融入 Latin 方形的討論裡。

有限幾何的研究可追溯回 Gino Fano 的作品，他於 1892 年，考慮一個由 15 點、35 條直線，及 15 個平面所構成的有限三維幾何。然而，直到 1906 年，這些幾何才獲得注意，當 O. Veblen 及 W. Bussey 開始他們的有限投影幾何研究時。欲知更多這個主題，讀者將發現 A. A. Albert 和 R. Sandler [1] 及 H. L. Dorwart [4] 的書是非常有趣的。P. Dombowski [3] 提供更多的材料給那些想尋求更高階的人。

最後，設計的觀念首先由統計學家研究於所謂的實驗設計領域裡。經由 R. A. Fisher 及他的後繼者的努力，這個領域已在近代統計分析理論扮演一個重要的角色。在我們的發展裡，我們檢視 (v, b, r, k, λ) -設計可存在的條件及這些設計和仿射平面及有限投影平面之間有何關係。M. Hall, Jr. [5] 提供更多的這個主題，如同 A. P. Street 和 W. D. Wallis [15] 的作品。參考資料 [15] 的第 13 章包含和設計及編碼理論有關的教材，一個頗完整的設計題材被給於 W. D. Wallis [16] 的作品裡，且 J. H. Dinitz 和 D. R.

Stinson [2] 提供讀者更多這領域的收集。

參考資料

1. Albert, A. Adrian, and Sandler, R. *An Introduction to Finite Projective Planes*. New York: Holt, 1968.
2. Dinitz, Jeffrey H., and Stinson, Douglas R., eds. *Contemporary Design Theory*. New York: Wiley, 1992.
3. Dombowski, Peter. *Finite Geometries*. New York: Springer-Verlag, 1968.
4. Dorwart, Harold L. *The Geometry of Incidence*. Englewood Cliffs, N.J.: Prentice-Hall, 1966.
5. Hall, Marshall, Jr. *Combinatorial Theory*. Waltham, Mass.: Blaisdell, 1967.
6. Herstein, Israel Nathan. *Topics in Algebra*, 2nd ed. Lexington, Mass.: Xerox College Publishing, 1975.
7. Infeld, Leopold. *Whom the Gods Love*. New York: McGraw-Hill, 1948.
8. Larney, Violet H. *Abstract Algebra: A First Course*. Boston: Prindle, Weber & Schmidt, 1975.
9. Liu, C. L. *Topics in Combinatorial Mathematics*. Mathematical Association of America, 1972.
10. McCoy, Neal H., and Berger, Thomas R. *Algebra: Groups, Rings, and Other Topics*. Boston: Allyn and Bacon, 1977.
11. Roman, Steven. *Field Theory*. New York: Springer-Verlag, 1995.
12. Rothman, Tony. "Genius and Biographers: The Fictionalization of Evariste Galois." *The American Mathematical Monthly* 89, no. 2 (1982): pp. 84–106.
13. Ryser, Herbert J. *Combinatorial Mathematics*. Carus Mathematical Monographs, Number 14, Mathematical Association of America, 1963.
14. Stillwell, John. *Mathematics and Its History*. New York: Springer-Verlag, 1989.
15. Street, Anne Penfold, and Wallis, W. D. *Combinatorial Theory: An Introduction*. Winnipeg, Canada: The Charles Babbage Research Center, 1977.
16. Wallis, W. D. *Combinatorial Designs*. New York: Marcel Dekker, Inc., 1988.
17. Zariski, Oscar, and Samuel, Pierre. *Commutative Algebra*, Vol. I. New York: Van Nostrand, 1958.

補充習題

1. 若 $GF(n)$ 有 6561 個不含常數項次數為 5 的首項一多項式，試求 n 值。
2. a) 令 $f(x)=a_nx^n+\cdots+a_1x+a_0 \in \mathbf{Z}[x]$。若 $r/s \in \mathbf{Q}$，滿足 $\gcd(r, s)=1$ 且 $f(r/s)=0$，證明 $s|a_n$ 且 $r|a_0$。

   b) 找下面佈於 $\mathbf{Q}$ 的多項式之所有有理根，若存在。分解 $f(x)$ 於 $\mathbf{Q}[x]$。

   i) $f(x)=2x^3+3x^2-2x-3$

   ii) $f(x)=x^4+x^3-x^2-2x-2$

   c) 證明多項式 $f(x)=x^{100}-x^{50}+x^{20}+x^3+1$ 沒有有理根。
3. a) 有多少個整數 n，其中 $1 \le n \le 1000$，我們可將 $f(x)=x^2+x-n$ 分解成 $\mathbf{Z}[x]$ 上的兩個一次因式的乘積？

   b) 回答 (a) 對 $f(x)=x^2+2x-n$。

   c) 回答 (a) 對 $f(x)=x^2+5x-n$。

   d) 令 $g(x)=x^2+kx-n \in \mathbf{Z}[x]$，其中 $1 \le n \le 1000$。求最小的正整數 k 使得 $g(x)$ 不可被分解成 $\mathbf{Z}[x]$ 上的兩個一次因式，對所有 $1 \le n \le 1000$。
4. 證明多項式 $f(x)=x^4+x^3+x+1$ 是可約的佈於每個體 F (有限或無限)。

5. 若 p 是一個質數，證明在 $\mathbf{Z}_p[x]$ 中，

$$x^p - x = \prod_{a \in \mathbf{Z}_p} (x - a).$$

6. 對任意體 F，令 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x]$。若 r_1，r_2，$\cdots$，r_n 是 $f(x)$ 的所有根，且 $r_i \in F$ 對所有 $1 \le i \le n$，證明

a) $-a_{n-1} = r_1 + r_2 + \cdots + r_n$.

b) $(-1)^n a_0 = r_1 r_2 \cdots r_n$.

7. 在 (7, 7, 3, 3, 1) -設計裡七個區組中的四個為 {1, 3, 7}，{1, 5, 6}，{2, 6, 7} 及 {3, 4, 6}，試求另三個區組。

8. 求所有的 b 及 r 值給一個 Steiner 三維系統，其中 $v = 63$。

9. a) 若某投影平面有 73 個點，則每條直線有多少個點？

b) 若某投影平面上的每條直線通過 10 個點，則此投影平面有多少條直線？

10. 某投影平面以體 F 的所有元素作坐標。若這個平面有 91 條直線，則 $|F|$ 及 char(F) 的值為何？

11. 令 $V = \{x_1, x_2, \cdots, x_n\}$ 為變種集合且 $\{B_1, B_2, \cdots, B_b\}$ 為區組集給 $(v, b, r, k,)$ - 設計。我們定義設計的**投引矩陣** (incidence matrix) A 為

$A = (a_{ij})_{v \times b}$，其中 $a_{ij} = \begin{cases} 1，若 x_i \in B_j \\ 0，否則 \end{cases}$

a) A 的每一列及每一行有多少個 1？

b) 令 $J_{m \times n}$ 為 $m \times n$ 矩陣，其每個元素是 1。我們寫 $J_{n \times n}$。證明對投引矩陣 A，$A \cdot J_b = r \cdot J_{v \times b}$ 且 $J_v \cdot A = k \cdot J_{v \times b}$。

c) 證明

$$A \cdot A^{\mathrm{tr}} = \begin{bmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda & \lambda & \lambda & \cdots & r \end{bmatrix} = (r - \lambda) I_v + \lambda J_v,$$

其中 I_v 是 $v \times v$ (乘法) 單位矩陣。

d) 證明

$\det(A \cdot A^{\mathrm{tr}}) = (r - \lambda)^{v-1}[r + (v-1)\lambda]$

$= (r - \lambda)^{v-1} rk$.

12. 給一個基於 V 的 n 個變種的 (v, b, r, k, λ) -設計，將每個區組 B_i，$1 \le i \le b$，以它的餘集 $\overline{B_i} = V - B_i$ 取代。則集合 $\{\overline{B_1}, \overline{B_2}, \cdots, \overline{B_b}\}$ 提供所有區組給 (v, b, r', k', λ') - 設計，亦基於集合 V。

a) 求這個對應的餘 (v, b, r', k', λ') -設計給 17.5 節習題 1 所給的設計。

b) 一般上，餘設計的所有參數 r', k', λ' 和原設計的所有參數 v，b，r，k，λ 間有何關係？