

五. 組合設計簡介

在歷史上組合數學對於研究如何設計實驗使得成效更好，有很大的貢獻。研究實驗設計中所隱函的數學 (Combinatorics in Experimental Designs) 一般稱之為組合設計；而研究組合設計就不得不先介紹最具有影響力的拉丁方陣。

1. 拉丁方陣 (Latin Square)

例1. 假如我們要設計一個實驗來研究 5 種藥物， $\alpha, \beta, \gamma, \delta, \epsilon$ ，對人體的影響，(每天可以吃一種)，我們應該如何安排才可以避免所得到的結論過於偏差。顯然，我們找一個人來做實驗，會因為他個人體質的關係，而造成有偏差的結論；如果找太多人，又會造成太多的重複；因此，有一種設計方式是找到 5 個人來實驗，而且在 5 天內完成。表 1(a) 的安排，看起來十分容易，而且似乎達到實驗效果。然而，有些藥可能會對隔日，或以後的身體狀況有很大的影響力，而容易造成在服用該種藥之後，其它的藥效果不彰，譬如催吐藥。於是服用的先後次序也要考量，如此一來，偏差自然減少。因此，表 1(b) 的安排顯然就比較好，一方面每天都可以看到 5 種藥對人體的可能影響，同時每個人每天所服用的藥也都不相同。這樣的設計又稱為是拉丁方陣設計或簡稱為拉丁方陣 (Latin Square)。

人	M	Tu	W	Th	F
甲	α	β	γ	δ	ϵ
乙	α	β	γ	δ	ϵ
丙	α	β	γ	δ	ϵ
丁	α	β	γ	δ	ϵ
戊	α	β	γ	δ	ϵ

表 1(a)

人	M	Tu	W	Th	F
甲	ϵ	δ	γ	β	α
乙	δ	γ	β	α	ϵ
丙	γ	β	α	ϵ	δ
丁	β	α	ϵ	δ	γ
戊	α	ϵ	δ	γ	β

表 1(b)

定義 1.1. 用 $1, 2, \dots, n$ 為元素所安排的 n 階方形陣列 $A = [a_{ij}]_{n \times n}$ ，如果在每一行及每一列中，每個元素都恰好出現一次，則 A 稱為是一個 n 階拉丁方陣。如果對所有的 $1 \leq i, j \leq n$ ， $a_{ij} = a_{ji}$ ，則此拉丁方陣為對稱的拉丁方陣；若是對於每一個 $1 \leq i \leq n$ ， $a_{ii} = i$ ，則為等幂 (Idempotent) 拉丁方陣。

在表 1(b) 中，如果用 1,2,3,4,5 分別代表 $\epsilon, \gamma, \alpha, \delta, \beta$ ，則所得到的陣列 (Array) 為一對稱且等幂的 5 階拉丁方陣。為了便於解釋，以後拉丁方陣中的元素，我們都用 $\{1, 2, \dots, n\}$ 中的元素來表示。(若是經由代數方法製造，則用 $Z_n = \{0, 1, \dots, n-1\}$ 。)

- (性質 1) 各階的拉丁方陣都存在。
- (性質 2) 各階的對稱拉丁方陣都存在。
- (性質 3) 各階的等幂拉丁方陣都存在。
- (性質 4) 只有奇數階的等幂對稱拉丁方陣存在。

我們可以利用 n 階拉丁方陣 $A = [a_{ij}]$ 來定義一個運算 $*$ ， $i * j = a_{ij}$ 。則 $*$ 為一二元運算，而且滿足：對於任何 $a, b \in \{1, 2, \dots, n\}$ ， $a * x = b$ 和 $y * a = b$ 在 $\{1, 2, \dots, n\}$ 中都有唯一解。假如 $*$ 為一二元運算，同時方程式 $a * x = b$ 及 $y * a = b$ 在 S 中都有唯一解，則我們把這一個代數結構 $(S, *)$ 稱為是擬似群 (Quasigroup)。

- (性質 5) 具有結合律的擬似群為一群 (Group)。
- (性質 6) 一個擬似群不一定可結合。

例2.

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

$$2 * (1 * 2) = 2 * 2 = 1$$

$$(2 * 1) * 2 = 3 * 2 = 3$$

接下來我們看一個問題。

問題1. 假設有 16 位軍官要參加國慶閱兵的分列式，他們代表著 4 個兵種的 4 個官階，也就是說由步兵、砲兵、通訊兵、工兵，各派出一位少尉、中尉、上尉、少校參加。分列式將以四列、四行的方形排列前進。如果我們要求每一列（每一行）都要有四個兵種的代表而且是四個不同的官階，問要如何安排？

在回答這個問題之前，我們先來看一個定義。

定義 1.2. 我們稱 $L = [l_{ij}]$ 和 $M = [m_{ij}]$ 為兩個互相垂直的拉丁方陣，如果下列的兩個條件滿足：

- (i) L 和 M 為同階 (n 階) 的拉丁方陣；
- (ii) $\{(l_{ij}, m_{ij}) | 1 \leq i, j \leq n\} = I_n \times I_n, I_n = \{1, 2, \dots, n\}$ 。

例3. 下面的三個拉丁方陣，彼此互相垂直。

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

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

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

由（互相）垂直拉丁方陣的定義，我們可以發現問題 1 是在問：是否存在兩個互相垂直的 4 階拉丁方陣，答案顯然是肯定的。不過同樣的問題對於 6 階拉丁方陣就不同了。在 1900 年左右 Terry 已經用苦力式的方法

發現；根本不存在有這樣的兩個 6 階拉丁方陣，理論上的證明則等了 80 多年才完成。對於垂直拉丁方陣的研究，一直是組合設計的重要課題，我們在第 3 節再仔細討論。

以直觀的方式來看拉丁方陣，我們可以把一個 n 階拉丁方陣 $L = [l_{ij}]$ 的 n 列看成是 n 個排列，其形式如下：第 i 列 $\begin{pmatrix} 1 & 2 & 3 & \cdots & j & \cdots & n \\ a_{i1} & a_{i2} & a_{i3} & \cdots & a_{ij} & \cdots & a_{in} \end{pmatrix}$ ， $i = 1, 2, \dots, n$ 。因此，一個拉丁方陣可以由第一列先選好之後再第二列，第三列， $\dots$ ，只要維持每一個位置，譬如第 j 個，出現的元素都不一樣即可。

例 4. 不同的 4 階拉丁方陣有 576 個。

答. 第一列的選擇有 24 種，第二列的選擇有 $D_4 = 9$ 種。如何找出全部的 4 階拉丁方陣，除了利用電腦外，也可以用分類的方式求出來。

我們比較希望知道的是：一列一列往下找，一定可以找到 n 個來形成一個拉丁方陣嗎？會不會到了哪個位置，譬如 $n - k$ 列之後，就無法繼續找了？在回答這個問題之前，我們先介紹一個定義。(註) 在圖的應用中，我們已經提及它，在此作完整說明。

定義 1.3. 假設 $\{S_1, S_2, \dots, S_n\}$ 為 n 個正整數集的子集合族；如果 $x_i \neq x_j$, $1 \leq i \neq j \leq n$ ，且 $x_i \in S_i$, $i = 1, 2, \dots, n$ ，則我們稱 $(x_1, x_2, \dots, x_n)$ 為 $\{S_1, S_2, \dots, S_n\}$ 的一個相異代表系 (System of Distinct Representatives, SDR)。

例 5. $S_1 = \{1, 2, 3\}$, $S_2 = \{2, 3\}$, $S_3 = \{1, 4, 5\}$, $(3, 2, 1)$ 為 $\{S_1, S_2, S_3\}$ 的一個 SDR。

例 6. $S_1 = \{2, 3\}$, $S_2 = \{2\}$, $S_3 = \{2, 3\}$, $S_4 = \{1, 2, 3, 4\}$ ；則不存在有任何的 SDR。

顯然，若是 $S_1, S_2, \dots, S_n$ 有一相異代表系，則任取 k 個 S'_{ij} , $\left| \bigcup_{j=1}^k S'_{ij} \right| \geq k$ 。此必要條件實際上也是 SDR 存在的充分條件，當然對於集合個數及集合的基數需要略做規範。下面的定理是 P. Hall 所發現，也簡稱為 P. Hall 定理。(註) 組合數學史上有兩位是以 Hall 為姓的數學家，一位是 Marshall, 另一位為 Philip，本定理是在 1935，Philip 所證明的結果，我們也會有機會提到 M. Hall。

定理 1.4. (P. Hall, 1935)

集合族 $F = \{S_1, S_2, \dots, S_n\}$ 有 SDR 的充要條件為任意 k 個 F 中的元素之聯集至少含有 k 個元素, $k = 1, 2, \dots, n$ 。

證明. ($\Rightarrow$) 很容易。

($\Leftarrow$) 用歸納法 (討論集合的個數)。 $n = 1$ 時顯然成立, 假設 $n = 1, 2, \dots, m$ 時成立。令 $\{S_1, S_2, \dots, S_{m+1}\}$ 為一集合族, 而且在此集合族中的任意 k 個集合的聯集至少含有 k 個元素, $k = 1, 2, \dots, m+1$ 。對於任意選定的 k , 假如任意 k 個集合的聯集都含有至少 $k+1$ 個元素, 令 $x_{m+1} \in S_{m+1}$ 。則 $\{S_1 \setminus \{x_{m+1}\}, S_2 \setminus \{x_{m+1}\}, \dots, S_{m+1} \setminus \{x_{m+1}\}\}$ 有 SDR $(x_1, x_2, \dots, x_m)$ (由歸納假設), 因此有一 SDR $(x_1, x_2, \dots, x_m, x_{m+1})$ 。在另一方面, 如果存在有一 k , 及 k 個集合, 它們的聯集恰含 k 個元素, 不失一般性, 令 $\left| \bigcup_{j=1}^k S_i \right| = k$ 且 $S = \bigcup_{j=1}^k S_i$ 。由假設 $S_{k+1} \setminus S, \dots, S_{m+1} \setminus S$ 均不為 ϕ , 且 $\{S_{k+1} \setminus S, S_{k+2} \setminus S, \dots, S_{m+1} \setminus S\}$ 有一 SDR $(x_{k+1}, x_{k+2}, \dots, x_{m+1})$ (?), 而由歸納假設 $\{S_1, S_2, \dots, S_k\}$ 也有一 SDR $(x_1, x_2, \dots, x_k)$; 合併之後 $\{S_1, S_2, \dots, S_{m+1}\}$ 有一 SDR, 所以得證。 ■

在定理 1.4 中的條件 ”任意 k 個集合的聯集至少含有 k 個元素” 又簡稱為 Hall 的條件 (Hall's condition)。於是滿足 Hall 的條件之集合族就存在有一個相異代表系 (SDR), 這樣的特性在應用上有很多, 我們可以用它來證明, 以排列堆積的方式一定可以完成一個拉丁方陣。

定義 1.5. 在一個 $r \times s$ 陣列中如果每個元素皆來自 $S = \{1, 2, \dots, n\}$, 而且每一個元素在每一行每一列中最多只出現一次, 則此長方形陣列又稱為是一個基於 S 的 $r \times s$ 拉丁長方形 (Latin rectangle)。

定理 1.6. (M. Hall, 1945) 任一個基於 $S = \{1, 2, \dots, n\}$ 的 $r \times n$ 拉丁長方形都可以把它繼續伸展成一個 n 階的拉丁方陣。

證明. 令 $r \times n$ 拉丁長方形為 $M = [m_{ij}]_{r \times n}$, $S_j = S \setminus \{m_{1j}, m_{2j}, \dots, m_{rj}\}$, $j = 1, 2, \dots, n$ 利用定理 1.4 $\{S_1, S_2, \dots, S_n\}$ 有一個 SDR (?), 所以第 $r+1$ 列即可填好; 繼續同樣的方法可證明本定理。 ■

如果我們希望打一個基於 $S = \{1, 2, \dots, n\}$ 的 $r \times s$ 拉丁長方形 A 向右且向下伸展成為一個 n 階的拉丁方陣 (圖 1.1), 結果就要比定理 1.6 複雜許多。例 7 中的 A 就無法伸展成 7 階的拉丁方陣。

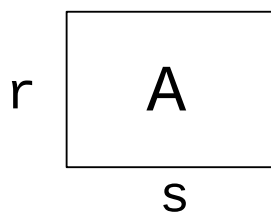


圖 1.1

例 7.

$$A = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 2 & 3 & 4 & 1 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 1 & 2 & 3 \\ \hline \end{array}$$

顯然地那是因為放在 A 中的元素沒有預先規定條件所造成的，下面的定理可以說明這件事。

定理 1.7. (H.J. Ryser, 1951)

令 R 為基於 $S = \{1, 2, \dots, n\}$ 的 $r \times s$ 拉丁長方形， $R(i)$ 代表 i 在 R 中出現的次數；則 R 可以伸展成一個 n 階拉丁方陣的充要條件為對於所有的 $i = 1, 2, \dots, n$ ； $R(i) \geq r + s - n$ 。

證明. 充分條件的證明在此省略。

(必要條件) 如圖 1.2 所示，任一個元素 i 在 $C \cup D$ 中必定出現 $n - r$ 次，而在 B 中至多出現 $n - s$ 次，所以在 R 中， i 至少出現 $n - [(n - r) + (n - s)] = r + s - n$ 次，所以 $R(i) \geq r + s - n$ 。 ■

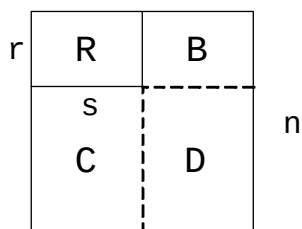


圖 1.2

由定理 1.7, 我們更容易看出例 7 的 A 為何不能伸展成 7 階拉丁方陣。
($R(5) = 0 < 4 + 4 - 7$ 。) 然而, 例 7 的 A 卻可以伸展成 8 階, 9 階, $\dots$, 的
拉丁方陣。

定義 1.8. 如果我們可以將 M 伸展而得到 L , 則我們稱一個拉丁方陣 M
可以嵌入於一個拉丁方陣 L 。

例 8. 例 7 中的 A 可以嵌入於

A	$A+4$
$A+4$	A

, $A+4 = [a_{ij} + 4]$, $A = [a_{ij}]$ 。

推論 1.9. 任一個 m 階拉丁方陣皆可嵌入於一個 $n(\geq 2m)$ 階拉丁方陣中。

證明. 由定理 1.7 可得證。

以代數的角度來看推論 1.9, 嵌入的拉丁方陣實際上是一個子擬似群。
所以我們發現一個現象, 即子擬似群與擬似群的關係和子群與群的關係
不盡相同。

推論 1.10. 若是 $(Q_1, *)$ 為 $(Q, *)$ 的子擬似群, 則 $2|Q_1| \leq |Q|$ 。

證明. 由定理 1.7 可得證。

(註) $|Q_1|$ 不一定是 $|Q|$ 的因數, 這與 Lagrange 定理 (有限群與子群的關係)
不同。



2. 區組設計 (Block Design)

在例 1 中，被實驗的對象 $\alpha, \beta, \gamma, \delta, \epsilon$ 所成的集合又稱為處理元集 (Treatments)，而它的任一個子集合皆稱為是一個區組，而把一個處理元集中的元素用來安排成“元素個數一樣”的許多個區組（可能只有一個），稱為是一個區組設計 (Block Design)。當每個區組實際上是整個處理元集時，此設計又稱為是一個完全區組設計 (Complete Block Design)，若是區組的元素少於處理元集個數，則此設計為不完全區組設計 (Incomplete Block Design)。我們可以把拉丁方陣看成是一個完全區組設計，以行或以列為區組皆可。為了方便表示，我們通常以 $(V, \mathfrak{B})$ 代表一個區組設計， V 為處理元集，而 $\mathfrak{B}$ 為區組族 (collection of blocks)。下面的例子就是一個不完全區組設計。

例 9. $V = \{1, 2, 3, 4, 5, 6, 7\}$ ， $\mathfrak{B} = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{5, 6, 1\}, \{6, 7, 2\}, \{7, 1, 3\}\}$ 。

(註) 在有限幾何的研究中， V 為點集合， $\mathfrak{B}$ 為線集合。

如果我們仔細觀察例 9，還可以發現下列的現象：

- (1) V 中的任兩個元素，剛好共同出現在一個集合。(以幾何觀點而言，即為任兩點決定一線。)
- (2) $\mathfrak{B}$ 中的任兩個區組，恰好有一共同的元素。(兩線交於一點。)

顯然，並非所有的區組設計都會具有上述的兩種性質；滿足 (i) 及 (ii) 的不完全區組設計的確是非常特別，它是一種對稱設計 (Symmetric Design)。滿足 (i) 的現象是研究區組設計的學者最有興趣的一種設計。

定義 2.1. 在一個不完全區組設計中，如果任意兩點所共同出現的區組數為一固定數“ λ ”，則此設計稱為是平衡不完全區組設計 (Balanced Incomplete Block Design)，簡稱 BIBD。

例 9 即為一 BIBD，其中 $\lambda = 1$ 。如果我們假設在一個 BIBD 中， $|V| = v$ ， $|\mathfrak{B}| = b$ ，對於 $\mathfrak{B}$ 中的任一個區組皆有 $K(> 0)$ 個元素，而且 V 中的每個元素都出現在 $r(> 0)$ 個區組中，同時任意兩點所共同出現的區組有 $\lambda(> 0)$ 個，則此 BIBD 又稱為是 (v, b, r, k, λ) -設計，而且滿足下列兩個條件。

- (i) $\lambda(v-1)/(k-1)$ 爲正整數；
- (ii) $\lambda(v-1)v/(k-1)k$ 爲正整數。

証明 (i), (ii) 並不難，實際上 $r = \lambda(v-1)/(k-1)$, $b = \lambda v(v-1)/k(k-1)$ 。除上述兩個性質，我們也可以證明下列定理。

定理 2.2. 在一個 (v, b, r, k, λ) -設計中， $bk = vr$ 且 $\frac{\lambda(v-1)}{k-1}$ 及 $\frac{\lambda v(v-1)}{k(k-1)}$ 皆爲正整數。

證明. 由兩方向計數，(Two-way Counting) 即可證明。 $bk = vr$ (把全部的區組排出來，再計算元素出現的總數。) 另兩部分當成作業。 ■

當 $k = 3$ 時，上述設計又稱爲是三元素系統 (Triple System)。和三元素系統有關的著名問題，是在 1847 年由柯克曼所提出的安排 15 個女學童排路隊上學的問題。

問題 2. (Kirkman's schoolgirl problem)

有一個老師，他班上有 15 位女學生，他希望能把這 15 位女學生排成三人一列的路隊上學；在 7 天中，每天每位女學生都和同列的兩位同學相識；問如何安排才能使她們在七天後，每位女學生都能認識全部其他的 14 位同學，亦即每天和不同的兩位同學一列。

答. 這比一個三元素系統的要求更多；不過，至少要是一個三元素系統。(你能找到答案嗎？)

如果把問題 2 改成九個學生，則它的答案可分成 4 組。下面就是其中的一種安排。

例 10.

<u>123</u>	<u>159</u>	<u>168</u>	<u>147</u>
<u>456</u>	<u>267</u>	<u>249</u>	<u>258</u>
<u>789</u>	<u>348</u>	<u>357</u>	<u>369</u>

現在再以幾何的觀點來看上面的結構，則平行線存在 (交集爲空集合的兩線)。同時過直線外一點必定存在唯一的一線包含此點且與給定的直線平行，這也就是平行公設啊！我們將分別以投影平面 (Projective Plane)，仿射平面 (Affine Plane) 來稱呼例 9，例 10 兩種具有特殊性質的 BIBD。

以下我們分成三部分來分別介紹互相垂直的拉丁方陣，投影平面及仿射平面。

3. 彼此互相垂直的拉丁方陣 MOELS(Mutually Orthogonal Latin Squares)

由於我們需要用到有限體 (Finite Field) 的觀念，因此先介紹這個代數結構。

定義 3.1. 一個集合 F 及兩個運算 $+, \cdot$ ，構成一個代數結構 $(F, +, \cdot)$ 為一體 (Field) 假如下列的條件成立：

- (i) $(F, +)$ 為一交換群，
- (ii) $(F, \cdot)$ 為一交換群，其中 F^* 為 F 扣除加法單位元素 0，及
- (iii) 分配律成立， $a \cdot (b + c) = a \cdot b + a \cdot c$ ， $a, b, c \in F$ 。

如果 F 為一有限集合，則此體稱為一有限體。

定理 3.2. 一個有限體 $(F, +, \cdot)$ 存在的充分必要條件為 $|F| = p^k$ ， p 為質數， k 為正整數。

證明. 請參考代數課本。

對於上述定理的證明，在此略述綱要。在必要條件方面， F 可以看成是佈於 Z_p 的一個向量空間，如果是 k 維，則 $|F| = p^k$ 。另一方向，我們需要證明存在有一個在 Z_p 上不可分解 (Irreducible) 的 k 次多項式，例如 $x^2 + x + 1$ 在 Z_2 上不可分解，因此存在一個有限體它的元素個數為 2^2 。

有了定理 3.2，就可以得到垂直拉丁方陣的研究上最重要的定理。

定理 3.3. 對於所有的質數 p 及正整數 k ，都存在有 $p^k - 1$ 個彼此互相垂直的 p^k 階拉丁方陣。

證明. 由定理 3.2，我們知道對於任意的質數方 p^k ，都存在有一個體 $(F, +, \cdot)$ ，其中 $|F| = p^k$ 。因此 $|F^*| = p^k - 1$ 。對於 F^* 中的任意一個元素 h ，定義一個 $p^k \times p^k$ 的陣列 $L^{(h)} = [l_{ij}^{(h)}]$ 使得 $l_{ij}^{(h)} = i \cdot h + j$ ， $i, j \in F$ 。首先，我們核對 $L^{(h)}$ 為一拉丁方陣 (?) 然後再判斷任給 $h, h' \in F^*$ 與 $L^{(h')}$ 是否垂直。假設 $l_{ij}^{(h)} = l_{i'j'}^{(h')}$ ，且 $l_{ij}^{(h')} = l_{i'j'}^{(h')}$ 則 $i \cdot h + j = i' \cdot h + j'$ ，且 $i \cdot h' + j = i' \cdot h' + j'$ ，所以 $(i - i')h = (j' - j)$ ，且 $(i - i')h' = (j' - j)$ 因為 $h \neq h'$ ，所以 $i = i'$ ，於是 $j = j'$ 。因此我們證明了 $L^{(h)}$ 與 $L^{(h')}$ 垂直。 ■

這個定理也說明存在有三個互相垂直的 4 階拉丁方陣 (例 3)，然而對於不是質數方階的情況，是否存在有互相垂直的拉丁方陣，就沒有這麼容易了。譬如 6, 10, 12, ...。首先，我們可以回答 12 階的情況。

定義 3.4. 令 $A = [a_{ij}]$ 及 $B = [b_{ij}]$ 分別為 l 階及 m 階之拉丁方陣，則 $A \times B$ 稱為是 A 與 B 的卡迪遜積 (Cartesian Product)，可以定義成 $[(A, b_{ij})]_{m \times m}$ ，其中 (A, b_{ij}) 為一 l 階拉丁方陣，它的 (i', j') 位置之元素為 $(a_{i'j'}, b_{ij})$ 。

因此 $A \times B$ 為一 $l \cdot m$ 階拉丁方陣，下面例子是由 3 階拉丁方陣與 4 階拉丁方陣的乘積所得到的 12 階拉丁方陣。

例 11.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 4 & 3 & 2 \\ 4 & 1 & 2 & 3 \\ 3 & 2 & 1 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

$(1,1) (2,1) (3,1)$ $(2,1) (3,1) (1,1)$ $(3,1) (1,1) (2,1)$	$(1,4) (2,4) (3,4)$ $(2,4) (3,4) (1,4)$ $(3,4) (1,4) (2,4)$	$(1,3) (2,3) (3,3)$ $(2,3) (3,3) (1,3)$ $(3,3) (1,3) (2,3)$	$(1,2) (2,2) (3,2)$ $(2,2) (3,2) (1,2)$ $(3,2) (1,2) (2,2)$
$(A, 4)$	$(A, 1)$	$(A, 2)$	$(A, 3)$
$(A, 3)$	$(A, 2)$	$(A, 1)$	$(A, 4)$
$(A, 2)$	$(A, 3)$	$(A, 4)$	$(A, 1)$

我們不難把上面的拉丁方陣轉變成以 $1, 2, \dots, 12$ 所填出來的拉丁方陣 (?)。

定理 3.5. 若是 A_1 與 A_2 為互相垂直的 l 階拉丁方陣, B_1 與 B_2 為互相垂直的 m 階拉丁方陣, 則 $A_1 \times B_1$ 與 $A_2 \times B_2$ 為互相垂直的 $l \cdot m$ 階拉丁方陣。

証明. 由乘積的定義可以直接核對。

推論 3.6. 當 $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$ 時, 存在有 $\min_{i=1}^s \{p_i^{k_i} - 1\}$ 個互相垂直的 n 階拉丁方陣。

証明. 由定理 3.2 及 3.5 可得證。

(註) 存在有多少個並不代表一共就只有這麼多, 譬如推論 3.6, 存在有兩個互相垂直的 12 階拉丁方陣; 但是目前已經可以找到 3 個。

由推論 3.6, 我們不難看出真正有問題的是那些是 2 的倍數, 但是它不是 4 的倍數, 即所有的 $n \equiv 2 \pmod{4}$ 。第一個面對的數 2, 很容易看出沒有兩個互相垂直的拉丁方陣; 那麼 6 呢? 於是尤拉在看到這個現象, 在努力尋找 6 階互相垂直的拉丁方陣失敗之後, 他猜測 (很久以前); 對於所有 $n \equiv 2 \pmod{4}$, 皆不存在有任何互相垂直的 n 階拉丁方陣。

到了 1900 年, Terry 他證實了尤拉的第一個猜測數字 $n = 6$ 是對的。據說, 他是把所有的 6 階方陣都 "適當" 地列出之後, 兩兩比較而得到證明的。然而, 尤拉也只有猜對這個數而已, 在 1960 的兩篇論文中, 三位作者證明了下列結果。(証明省略)。

定理 3.7. (Parker, Bose, Shrikhande, 1960)

對於所有的正整數 $n \neq 2, 6$, 都存在有兩個互相垂直的 n 階拉丁方陣。

可是 MOLS 的研究並未因此而大功告成, 對於不是質數方的數, 究竟有多少個 MOLS's 目前仍然是個謎。值得一提的是 MOLS 也是非常有用的工具, 我們將會再提到它。

4. 投影平面 (Projective Plane)

實驗設計可以應用的幾何上是一個非常有趣而且重要的發展。投影平面就是其中的一個重要例子。再第二節的例 9，我們曾提及，在一個設計中（不一定是區組設計），可以把 V 的元素當作點， $\mathfrak{B}$ 中的區組當作線，如此一來有了點線及點線關係，就有幾何的存在。例 9 有下列兩個特性：

(P_1) 任兩點決定唯一的線。

(P_2) 任兩線交於唯一的點。

定義 4.1. 滿足 (P_1) 及 (P_2) 的設計 $(V, \mathfrak{B})$ 稱為投影平面。若是 $|V| < +\infty$ ，則稱為是有限投影平面 (Finite Projective Plane)。如果 V 中存在有 4 個點且任 3 點皆不在同一線上 (P_3)，則 $(V, \mathfrak{B})$ 為非退化 (Nondegenerate) 投影平面，反之則為退化投影平面。

在本節討論的都是非退化的有限投影平面，也就是滿足 (P_1)，(P_2) 及 (P_3)。例 9，可以用下圖來表示出來。

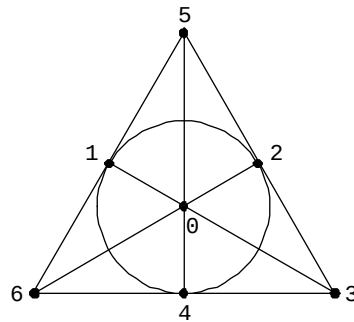


圖 4.1 : The Fano Plane.

值得在此說明的是 (P_2) 基本上和歐幾里德的平行公設是相違背的，因為，過線外一點找不到不和此線相交的線。因此我們可以定義出一套不同的幾何，即投影幾何。投影幾何的發展可以追溯到西元第四世紀 Pappas 的研究，然後才導至十九世紀 Boole, Cayley 及 Sylvester 不變量代數理論的產生，接下來有 Tensor Calculus (張量微積分) 的成果，最後才會有愛因斯坦的萬有引力 (Gravitation) 理論。

接下來我們探討一下投影平面的基本性質。

定理 4.2. 在投影平面中，存在有四條線，其中任三條皆不含有共同的交點 (P_4) 。

証明. 由 (P_3) ，存再有四個點 x, y, z, w 任三點皆不在同一線上。令 l_1, l_2, l_3, l_4 ，分別為由 x 與 y ， y 與 z ， z 與 w 及 w 與 x 所決定的線。由於任三點皆不在同一線上，所以此四條線皆不相同。不失一般性，假設 l_1, l_2 與 l_3 有一共同交點 u ，因為 y 不在 l_3 上， $u \neq y$ ，如此一來 l_1 與 l_2 交於 y 及 u 不同的兩點，此與 (P_2) 矛盾，故得證。 ■

仔細觀察定理 4.2 中的 (P_4) 及 (P_3) 之間的關係，及 (P_1) 與 (P_2) 的關係，我們不難發現，它們只是點、線的角色互換而已。這種點、線互換的特性，也稱為是對偶性 (Duality)。由於證明投影平面的特性時都要用到 (P_1) ， (P_2) 及 (P_3) ，所以加 (P_4) ，對偶的結果也都會成立，所以下面的定理自然成立。

定理 4.3. (對偶性原則)

投影平面的任何敘述如果是一個定理，則它的對偶敘述也是一個定理。

接下來是投影平面的一些特性。

定理 4.4. 在投影平面中，每一點都會落在一樣多的線上，每一線也會有一樣多的點。

証明. 我們只要證明每一線都含有一樣多的點即可。(對偶性原則)。令 L, L' 為任意兩線；則存在有一點 x ， x 不在 L 及 L' 上。(?) 於是對於 L 上的任一點 a ，通 a, x 的線必交 L' 於一點 a' ，我們 a' 為 a 經過 x 在 L' 上的投影，所以 L 上的點與 L' 上的點有 1-1 的對應，故得證。 ■

定理 4.5. 在投影平面中，通過一點的線數等於每一線上的點數。

証明. 任選一線 L 及不在 L 上的一點 x ，對於 L 上的任一點 y 定義 $L(y)$ 為通過 y, x 的線，於是 y 與 $L(y)$ 有 1-1 的對應故得證。 ■

推論 4.6. 在一個投影平面中，如果每條線上有 $m+1$ 個點，則此平面共用 m^2+m+1 個點及 m^2+m+1 條線。

證明. 令 x 為任一點，由對偶性，通過 x 的線有 $m + 1$ 條，因此總點數為 $(m + 1) \cdot m + 1$ ，故得證。 ■

讀了這麼多投影平面的特性，究竟有投影平面存在嗎？例 9 就是一個 2 階的投影平面 (Order 2)，每一線有 $m + 1$ 個點的投影平面是 m 階投影平面。下面是 3 階的例子。

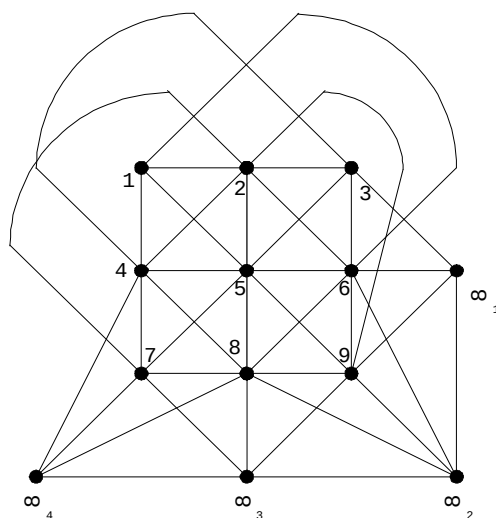


圖 4.2

定理 4.7. 對於 $m \geq 2$ ，一個 m 階投影平面存在的充要條件為一個 $(m^2 + m + 1, m^2 + m + 1, m + 1, m + 1, 1)$ -設計存在。

要證明這個定理，我們需要知道對稱設計的一些特性。

定義 4.8. 一個 (b, v, r, k, λ) -設計在 $b = v$ 的情況下稱為是對稱設計，簡記為 (v, k, λ) -設計。

對稱設計有很多特性，其中最重要的一個性質是下面的定理所敘述的特性。

定理 4.9. 在一個 (v, k, λ) -設計中，任意兩個區組的交集恰含有 λ 個元素。

證明. 省略。

現在，定理 4.7 也就不難證明（作業）。然而，定理 4.7 卻留下了一個同樣困難解決的問題，即“($m^2 + m + 1, m + 1, 1$) – 設計何時存在？”。這方面的研究，一直到今天，仍然是組合數學最想知道答案的一個問題。儘管一般而言，沒有明確的答案，不過在一些特殊情況已經有了結果。

定理 4.10. (Bose, 1938)

在 $m \geq 2$ 的情況下， m 階投影平面存在的充要條件為 $m - 1$ 個 m 階彼此互相垂直的拉丁方陣存在。

證明. 省略。

因此由定理 3.3，當 m 為質數方的形式，都存在有一個 m 階的投影平面。另一個定理則是把一些不可有投影平面的階數找出來，証明省略。

定理 4.11. (Bruck, Ryser 1949)

在 $m \equiv 1$ or $2 \pmod{4}$ 時，令 d 為 m 的最大平方因數，如果 $\frac{m}{d}$ 可以被 $4k + 3$ 形式的質數整除，則不存在有 m 階的投影平面。

例如 $m = 6$ ， $m = 54$ ， $m = 3t^2, 6t^2$ 等都是例子。下面的定理則是更明確地把投影平面存在的必要條件找出來。它的證明也在此省略。

定理 4.12. (Bruck-Ryser-Chowlam, 1950)

(v, k, λ) – 設計存在的必要條件是：

- (1) 假如 v 是偶數，則 $k - \lambda$ 為一平方數。
- (2) 假如 v 是奇數，則 $x^2 = (k - \lambda)y^2 + (-1)^{(v-1)/2} \lambda z^2$ 有不全為 0 的整數解， x, y, z 。

投影平面存在的必要條件，由定理 4.7 的角度來看，即為此定理的特別情況。

(註) n 階投影平面的研究，對於 $n \leq 10$ ，目前已全部解決，即 $n = 6, 10$ 不存在， $n = 1$ 退化，其它階數階存在。

5. 仿射平面 (Affine Plane)

一個 BIBD $(V, \mathfrak{B})$ 如果它的 b 個區組可以分解成 t 個部分，使得在每一個部分每一個 V 中的元素都恰好出現一次，即此設計為可分解的 BIBD (Resolvable BIBD)。一個可分解的 BIBD 又稱為是仿射可分解的 BIBD，如果來自不同部分的區組都會交於固定個數的元素。例 10 就是一個例子，例 11 則是一個可分解但不是仿射的 BIBD。

例 11.

1 2 3	1 4 5	1 6 7	1 8 9	1 10 11	1 12 13	1 14 15
4 8 12	2 8 10	2 9 11	2 12 15	2 13 14	2 4 6	2 5 7
5 10 14	3 13 15	3 12 14	3 5 6	3 4 7	3 9 10	3 8 11
6 11 13	6 9 14	4 10 15	4 11 14	5 9 12	5 11 15	4 9 13
7 9 15	7 11 12	5 8 13	7 10 13	6 8 15	7 8 14	6 10 12

例 11 同時也是問題 2 的一組答案。

定理 5.1. 任意的 $(k^2, k^2 + k, k + 1, k, 1)$ -設計皆為仿射可分解的 BIBD。

證明. 令 B_0 為設計 $(V, \mathfrak{B})$ 中的任一個區組。因為 $\lambda = 1$ ，所以 B_0 和其它區組的交集最多只有一元素。由 $r = k + 1$ ，所以對於 B_0 中的任一個元素尚有 k 個不同於 B_0 的區組包含此元素，因此在 $(V, \mathfrak{B})$ 中有 $(k^2 + k) - k \cdot k - 1 = k - 1$ 個區組和 B_0 的交集為空集合，現在考慮這些區組中任一個元素，它和 B_0 中的任一個元素共同出現於一個區組，一共有 k 個，所以，還有一個區組 B' 含有此一元素，但是 $B' \cap B_0 = \emptyset$ ；因為對於不在 B_0 的 $k^2 - k$ 個元素而言，每個元素都要出現在一個不與 B_0 相交的區組中，而且一共只有 $k - 1$ 這樣的區組，所以 $k^2 - k$ 個元素必定是分配在彼此不相交的 $k - 1$ 個區組上，於是和 B_0 形成一個分解族 (Resolution class)，即 V 中的每一個元素都恰好出現一次。由於 B_0 為對任意選擇的區組，所以每一區組都是在某一個分解族中，這證明了 $(V, \mathfrak{B})$ 是可分解的 BIBD。由上面的證明也不難看出來自不同分解族的兩個區組必定會交於一點，所以 $(V, \mathfrak{B})$ 是仿射可分解的 BIBD，故得證。 ■

我們可以利用定理 5.1 的設計來建構一個對稱的 $(k^2 + k + 1, k + 1, 1)$ -設計，也就是 k 階的投影平面。它的方法如下：令上述設計的 $k + 1$ 個分解族分別為 $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{k+1}$ ，現在令 $V' = V \cup \{\infty_1, \infty_2, \dots, \infty_k\}$ ， $\mathfrak{B}' = \{B' \mid B' = B \cup \{\infty_i\}, B \in \varepsilon_i, i = 1, 2, \dots, k + 1\} \cup \{\infty_1, \infty_2, \dots, \infty_{k+1}\}$ 。於是

$(V', \mathfrak{B})$ 爲所求。圖 4.2 就是利用例 10 的仿射可分解設計所建構出來的 3 階投影平面。

定義 5.2. 一個 $(k^2, k^2 + k, k + 1, k, 1)$ -設計又稱爲是 k 階的仿射平面 (Affine Plane)。

現在我們可以把上面建構的方式反過來，也就是利用 k 階的投影平面來建構 k 階的仿射平面 (?)。於是就得下面的定理。

定理 5.3. k 階的投影平面存在若且唯若 k 階的仿射平面存在。

定理 5.4. 一個 k 階仿射平面存在的充要條件爲 $k - 1$ 個彼此互相垂直的 k 階拉丁方陣存在。

證明.

($\Leftarrow$) 令 $L_3, L_4, \dots, L_{k+1}$ 爲 $k - 1$ 個彼此互相垂直的 k 階拉丁方陣，同時 R 爲第 i 列全部填 i 的 k 階陣列。現在考慮 $k + 1$ 個陣列 $L_1 (= R)$, $L_2 (= R^*)$, $L_3, L_4, \dots, L_{k+1}$ 及 $A = [a_{ij}]_{k \times k}$, $a_{ij} = (i - 1)k + j$ 。我們利用 $k + 1$ 個拉丁方陣來定義 $k + 1$ 個分解族：第 i 個分解族的第 j 個區組 $B_{ij} = \{x \mid L_i(i', j') = j \text{ 且 } a_{i'j'} = x\}$ 。由垂直拉丁方陣的定義可以證明這些區組所成的集合形成一個 k 階的仿射平面。 (?)

($\Rightarrow$) 反過來，我們要利用 $k + 1$ 個分解族來建構 $k - 1$ 個彼此互相垂直的 k 階拉丁方陣。令 $R_l, R_c, R_1, R_2, \dots, R_{k-1}$ 爲仿射平面的 $k + 1$ 個分解族；首先，我們將每個分解族的區組給定順序，即第一個區組至第 k 個區組；然後第 t 個拉丁方陣可以用下列方式填入：若是 R_l 的第 i 個區組與 R_c 的第 j 個區組的交集 $\{ak + b\}$, $0 \leq a \leq k - 1, 1 \leq b \leq k$ ；則在 L_t 的 (a, b) 位置上填入 y ，其中 y 來自 R_l 第 i 個區組與 R_t 的第 j 個區組之交集 $\{xk + y\}$, $0 \leq x \leq k - 1, 1 \leq y \leq k$ 。此種填法可以得到 $k - 1$ 個彼此互相垂直的 k 階拉丁方陣。故得證。 ■

由定理 5.3 及 5.4，我們可以得知 k 階投影平面， k 階仿射平面及 $k - 1$ 個 $\text{MOLS}(k)$ 的存在是等價的關係。

作業.

41. 我們以 $GF(q)$ 代表一個具有 q 個元素的有限體。先建構一個有限體 $GF(4)$ ，再利用它來產生三個互相垂直的 4 階拉丁方陣。
42. 令 N_m 代表不同 m 階拉丁方陣的個數。已知 $N_1 = 1, N_2 = 2, N_3 = 12$ ，求 N_4 。
43. 證明定理 1.6。
44. 試證在一個 (v, b, r, k, λ) -設計中， $\lambda(v-1)/(k-1)$ 及 $\lambda v(v-1)/k(k-1)$ 皆為整數。
45. 證明定理 3.5。
46. 試證在一個 (v, b, r, k, λ) -設計中， $b \geq v$ 。

提示：

- (a) 定義一個設計 $(V, \mathfrak{B})$ 的相接矩陣 $A = [a_{ij}]_{v \times b}$ ，其中 $a_{ij} = 1$ 假如 $x_i \in B_j$ ， $1 \leq i \leq v$ ， $1 \leq j \leq b$ ， $V = \{x_1, x_2, \dots, x_v\}$ 且 $\mathfrak{B} = \{B_1, B_2, \dots, B_b\}$ ，另外的位置 $a_{ij} = 0$ 。
 - (b) 證明 $\det(AA^T) = [r + (v-1)\lambda](r - \lambda)^{v-1}$ 。
47. 證明定理 4.7。
 48. 證明定理 4.9。提示：令 J 為 v 階全部為 1 的方形矩陣，則 $AJ = KJ$ ， $AA^T = (k - \lambda)I + \lambda J$ ， $A^{-1}J = K^{-1}J$ ， $A^T A = (k - \lambda)I + \lambda k^{-1}JA$ ，且 $JA = kJ$ 。
 49. 利用 m 階互相垂直拉丁方陣存在的理由，證明一個 l 階的拉丁方陣， $l \leq m$ ，一定可以伸展成一個 $(l+m)$ 階的拉丁方陣。



六. 計數 (Counting)

1. 等價類 (Equivalence classes)

在圖 1.1 中 (四個格子的正方形) 每個格子可以選擇塗黑或是不塗黑, 方法有 16 種。如果我們把經過旋轉後會是一樣的型式當成”相同”, 則不相同型式只有 6 種 $C_1; C_2, C_3, C_4, C_5; C_6, C_7, C_8, C_9; C_{10}, C_{11}; C_{12}, C_{13}, C_{14}, C_{15}; C_{16}$ 。更進一步, 加上黑白可以互換的條件之後, 不相同的型式就剩下 4 種而已, 因為 C_1 和 C_{16} , C_2 和 C_{12} 算是相同。由此我們可以發現, 經過不同的規定, 所得到的”相同”型式之個數也隨著改變。這些規定即為所謂的等價關係 (Equivalence Relation)。

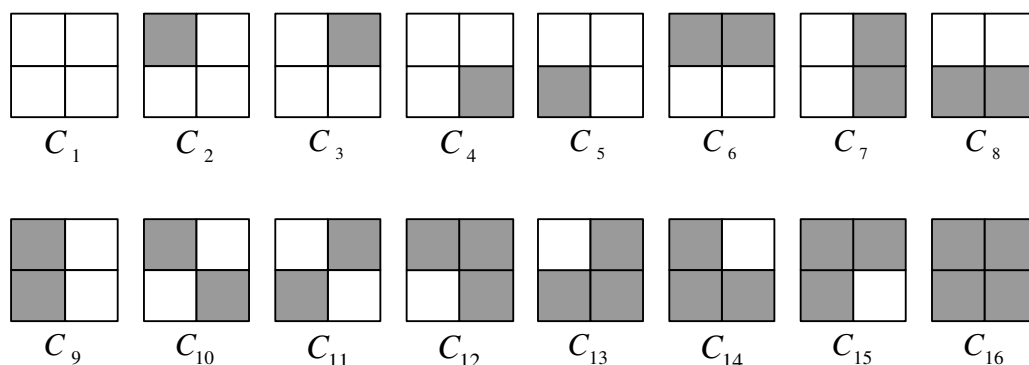


圖 1.1

假設 S 和 T 為兩個非空的集合, 如果 $\sim$ 為 $S \times T$ 的子集合, 我們稱” $\sim$ ”為集合 S 和 T 的一個二元關係。舉例來說, 令 $S = \{1, 2, 3\}$, $T = \{a, b, c, d\}$, 則 $\sim = \{(1, a), (1, c), (2, b), (2, c), (3, b), (3, d)\}$ 為一二元關係。在 $S = T$ 的情況下, 我們稱 $\sim$ 為 S 的一個二元關係。為了方便表示, 如果 $(a, b) \in \sim$, 我們有用 $a \sim b$ 來表示。這裡要注意 $a \sim b$ 不一定能得到 $b \sim a$ 。也就是 (a, b) 和 (b, a) 不一定要同時在 $\sim$ 中。下面我們定義一種特殊關係。

定義 1.1. 我們稱 $\sim$ 為 S 的一個等價關係 (Equivalence Relation), 如果 $\sim$ 為 S 的一個二元關係, 同時滿足下列三個條件:

- (i) 反身性：對於所有的元素 $a \in S$, $a \sim a$ 。
- (ii) 對稱性：對於任意兩個在 S 的元素 a 和 b , 如果 $a \sim b$ 則 $b \sim a$ 。
- (iii) 遞移性：對於任意三個在 S 的元素 a, b 和 c , 若 $a \sim b$ 且 $b \sim c$, 則 $a \sim c$ 。

如果利用等價關係把集合 S 中的元素分類, 即當 $a \sim b$ 時, a, b 在同一類, 則我們可以把集合 S 分成互斥的子集合, 每個子集合為一個等價類 (Equivalence class)。

定理 1.2. 假設 $\sim$ 為集合 S 的一個等價關係, 則 S 可以被分割成等價類。

證明. 在 S 中先任取一個元素 a , 定義 $S_a = \{x | a \sim x, x \in S\}$; 因為當 $y, z \in S_a$ 時, 則 $a \sim y, a \sim z$; 因此 $y \sim a, a \sim z$, 所以 $y \sim z$ 。如果 $S_a = S$, 則 S 中只有一個等價類; 不然令 $b \in S/S_a$, 同理定義 $S_b, S_c, \dots$ 。接下來我們證明任意兩個不同的等價類必定互斥。假設 $S_a \cap S_b \neq \emptyset$ 則令 $d \in S_a \cap S_b$, 因此 $a \sim d$ 且 $b \sim d$, 所以 $a \sim b$, 此為矛盾。因此定理得證。 ■

定義 1.3. S 上的一個二元運算 “ $*$ ”, 為由 $S \times S$ 映至 S 的一個函數。

定義 1.4. (群, Group)

一個集合 S 及在 S 上的一個二元運算 $*$ 稱為是一個群, 如果下列三個條件滿足:

- (i) 結合律, 即對於 S 中任意三個元素 a, b, c , $a * (b * c) = (a * b) * c$ 。
- (ii) 有單位元素, 即存在有一個元素 e , 使得對於 S 中任意元素 a , $a * e = e * a = a$ 。
- (iii) 有反元素, 即對於 S 中任意元素 a , 都可以找到一個元素 $a^{-1} \in S$, 使得 $a * a^{-1} = a^{-1} * a = e$ 。

(註) 定義中的單位元素及反元素都是唯一的。

定義 1.5. (排列, Permutation)

一個集合 S 的排列為一個由 S 映至 S 的一對一, 映成函數。

定義 1.6. (排列群, Permutation Group)

由一個集合 S 的一些排列及合成運算所形成的群, 稱為是 S 的排列群。

例. 令 $S = \{1, 2, 3\}$, 則 $G = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\}$ 為一排列群。

(如果運算不會被弄錯, 就可以不必再提是什麼樣的運算。)

令 $S = \{1, 2, 3, 4\}$, $G\{e, (12), (34), (12)(34)\}$ 則 G 為一排列群。

(註) 這裡的 $(12)(34)$ 代表 $\begin{pmatrix} 1234 \\ 2143 \end{pmatrix}$ 。

我們可以用排列群來導出 S 的一個二元關係 (Induced Binary Relation)。假設 G 為 S 上的一個排列群, 令 $a \sim b$, 若且唯若存在一個 G 中的排列 π , 使得 $\pi(a) = b$ (或是 $a_\pi = b$)。我們可以得到下面的結果。

定理 1.7. 由排列群所導出的二元關係為一個等價關係。

證明. 令 G 為集合 S 上的一個排列群, 由於 G 中有單位元素 e , 所以對於 S 中的任一元素 a , $e(a) = a$, 因此 $a \sim a$ 。接下來, 如果 $a \sim b$, 即有一 G 中的元素 π 使得 $\pi(a) = b$, 於是 $\pi^{-1}(\pi(a)) = \pi^{-1}(b)$, $\pi^{-1}(b) = a$ 。因為 π^{-1} 在 G 中, 所以 $b \sim a$ 。最後, 假設 $a \sim b$ 且 $b \sim c$, 於是, 存在有 $\pi_1, \pi_2 \in G$, 使得 $\pi_1(a) = b$, $\pi_2(b) = c$ 。利用合成關係, $\pi_2(\pi_1(a)) = c$, 即 $(\pi_2 \circ \pi_1)(a) = c$, 因此 $a \sim c$, 所以定理得證。 ■

由於排列群可以導出等價關係, 我們就可以計算等價類的個數, 以下是前面所提到的例子。(圖 1.1) 假如我們定義 4 個排列如下:

$$\pi_1 = (C_2 C_3 C_4 C_5) (C_6 C_7 C_8 C_9) (C_{10} C_{11}) (C_{12} C_{13} C_{14} C_{15}) \text{ (順時針轉 } 90^\circ)$$

$$\pi_2 = (C_2 C_4) (C_3 C_5) (C_6 C_8) (C_7 C_9) (C_{12} C_{14}) (C_{13} C_{15}) \text{ (順時針轉 } 180^\circ)$$

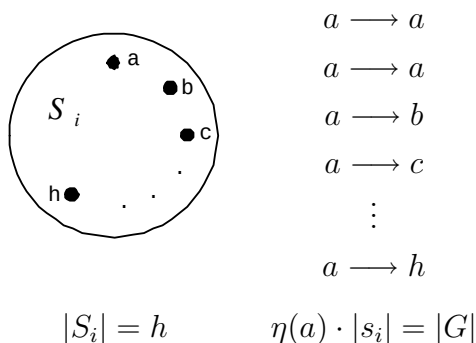
$$\pi_3: \text{順時針轉 } 270^\circ, \pi_4 \text{ 不轉。}$$

則我們可以求出 6 個等價類, 基本上每一類中的正方形圖樣和其它類的圖樣是無法用旋轉來使它們成為相同的圖樣。這 6 個等價類分別為 $\{C_1\}$, $\{C_2, C_3, C_4, C_5\}$, $\{C_6, C_7, C_8, C_9\}$, $\{C_{10}, C_{11}\}$, $\{C_{12}, C_{13}, C_{14}, C_{15}\}$, $\{C_{16}\}$ 。現在我們來觀察在同一個等價類中, 元素之間的關係。譬如在 $\{C_{10}, C_{11}\}$ 這個集合中, 究竟有多少個 G 中的排列會把 C_{10} 對應到 C_{11} 呢? 假設 π_x 為其中一個, 則對於所有的 $\pi_i \in G$, $\pi_i(C_{10}) = C_{10}$, $(\pi_x \circ \pi_i)$ 也是這樣的排列, 所以在 G 中能把 C_{10} 對應到 C_{11} 的排列數, 至少為把 C_{10} 固定的排列數。(?) 是否還令更多呢? 假設 π_y 為另一個這種排列, 且 $\pi_y(a) = b$, $a = C_{10}$, $b = C_{11}$, 所以 $(\pi_x^{-1} \circ \pi_y)(a) = a$, 於是 $(\pi_x^{-1} \circ \pi_y)$ 固定 a , 且 $\pi_x \circ (\pi_x^{-1} \circ \pi_y) = \pi_y$, 因此 π_y 必為上述的形式。也就是說不會有更多的了。現在, 我們假設 G 為

S 上的一個排列群，對於 S 中的任意元素， $\eta(a)$ 代表在 G 的元素中，可以把 a 對應到 a 的排列數。則下面的定理就可以成立。

定理 1.8. 令 G 為 S 上的一個排列群，則用 G 所導出的等價關係可以把 S 分成 $\frac{\sum_{s \in S} \eta(s)}{|G|}$ 個等價類。

證明. 假設 a, b 為同一等價類 S_i 中之元素， a 可能等於 b ，由上面的說明，我們求得 G 中能把 a 對應到 b 的排列恰有 $\eta(a)$ 個，由於 $\eta(a)$ 這個量獨立於 b ，所以 $\eta(a) \cdot |S_i| = |G|$ (?)，



又 $\eta(a) = \eta(b)$ ，所以 $\sum_{s \in S_i} \eta(s) = |G|$ 。如此一來 $\sum_{s \in S} \eta(s) = \sum_{i=1}^t \left(\sum_{s \in S_i} \eta(s) \right) = t \cdot |G|$ ，其中 t 為等價類的個數。因此得證。 ■

利用定理 1.8，我們不難算出上面例子中正方形格子的形式有

$$\frac{1}{4} (4 + 1 + \cdots + 1 + \overset{\uparrow}{2} + \overset{\uparrow}{2} + 1 + \cdots + 1 + 4) = 6$$

$\eta(C_1) \qquad \eta(C_{10}) \quad \eta(C_{11}) \qquad \eta(C_{16})$

但是有些問題，集合 S 太大，如此一一計算 $\eta(a)$ 值比較費力，因此另一形式的公式可供計算。

定理 1.9. $\sum_{s \in S} \eta(s) = \sum_{\pi \in G} \psi(G)$ ， $\psi(G) = |\{a \in S \mid \pi(a) = a\}|$ 。

證明. 這可以用兩方向的計算來證明。左式和右式都是在計算不變性 ($\pi(x) = x$) 的總數，左式依元素一一累加，而右式則依排列一一累加，故得證。 ■

有了定理 1.9，等價類的個數就可以依另一式子來計算，這也是聞名的朋塞輔助定理 (Burnside's Lemma)。

定理 1.10. (Burnside)

令 G 為 S 上的一個排列群，則用 G 所導出的等價關係可以把 S 分成 t 個等價類， $t = \frac{\sum_{\pi \in G} \psi(\pi)}{|G|}$ 。

若以正方形格子的著色 (上例)， $t = \frac{\psi(\pi_1) + \psi(\pi_2) + \psi(\pi_3) + \psi(\pi_4)}{|G|} = \frac{2+4+2+16}{4} = 6$ 。由於 G 中的元素較少，計算似乎較容易。接下來再看一個問題。

問題 1. 用三顆紅色、六顆藍色寶石所串起來的項鍊，共有多少種不同型式？(轉動或翻面後一樣，即算是相同的型式。)

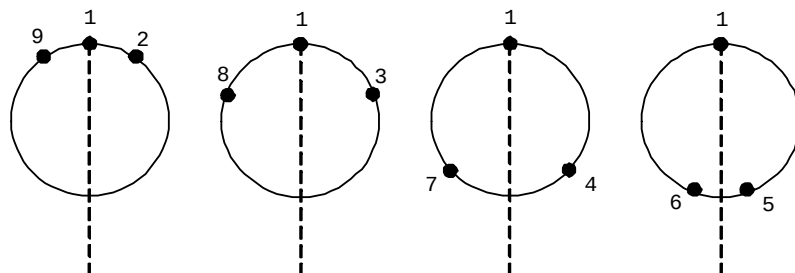
答. 首先由組合我們得知 $|S| = \binom{9}{3} = 84$ ，接著因為旋轉與鏡射後的型式和原來的型式看成一樣，所以 G 中的元素為 $r_1, r_2, \dots, r_9, \delta_1, \delta_2, \dots, \delta_9$ 。其中 r_i 為順時針旋轉 $i \cdot \frac{360^\circ}{9} = (40i)^\circ$ ， $\delta_j = \begin{pmatrix} \cdots & j-2 & j-1 & j & j+1 & j+2 & \cdots \\ \cdots & j+2 & j+1 & j & j-1 & j-2 & \cdots \end{pmatrix}$ (鏡射)。現在，我們需要計算 $\psi(r_i)$ 及 $\psi(\delta_j)$ ， $i, j = 1, 2, \dots, 9$ 。然後，

$$t = \frac{\sum_{i=1}^9 \psi(r_i) + \sum_{j=1}^9 \psi(\delta_j)}{18}$$

$$= (0 + 0 + 3 + 0 + 0 + 3 + 0 + 0 + 84 + \underset{\substack{\uparrow \\ \psi(\delta_1)}}{4} + \underset{\substack{\uparrow \\ \psi(\delta_9)}}{4} + 4 + 4 + 4 + \cdots + 4) / 18$$

$$= \frac{126}{18} = 7$$

(註 1.) $\psi(\delta_1) = 4$ 的理由可以由下圖看出。



(註 2.) 至於是哪七種，我們把它當成作業。

2. 等價函數 (Pólya's Counting Theorem)

前面計算等價類的概念可以作適當的推廣，現在把計算的對象轉換成函數，亦即探討等價的函數。

令 F 代表由 $D = \{a, b, c, d\}$ 映至 $R = \{0, 1\}$ 的所有函數所成的集合， $F = R^D$ 於是 $|F| = |R|^{|D|} = 2^4 = 16$ 。再令 $G = \{e, (abcd), (ac)(bd), (adcb)\}$ 為 D 的一個排列群；於是我們可以定義 F 的一個等價關係： $f_1 \sim f_2$ 若且唯若存在一個 $\pi \in G$ ，使得 $f_1 = f_2 \circ \pi$ 。所以，上述的 16 個函數就可以分成數個等價類：如下圖所示

函數 \ 函數值	$f(a)$	$f(b)$	$f(c)$	$f(d)$
f_1	0	0	0	0
f_2	1	0	0	0
f_3	0	1	0	0
f_4	0	0	1	0
f_5	0	0	0	1
f_6	1	1	0	0
f_7	0	1	1	0
f_8	0	0	1	1
f_9	1	0	0	1
f_{10}	1	0	1	0
f_{11}	0	1	0	1
f_{12}	1	1	1	0
f_{13}	0	1	1	1
f_{14}	1	0	1	1
f_{15}	1	1	0	1
f_{16}	1	1	1	1

a	b
d	c

再來我們介紹函數的加權 (Weight of Function)。首先，對於由 D 對應到 R 的函數 f ，定義 R 的儲存算子 (Store Enumerator) φ ，與 f 無關， $\varphi = \sum_{r \in R} w(r)$ ，其中 $w(r)$ 為 r 的加權。

(註) 這裡 $w(r)$ 可以是數也可以是符號。

例. $D = \{d_1, d_2, d_3\}$, $R = \{r_1, r_2, r_3\}$, $w(r_1) = u$, $w(r_2) = v$, $w(r_3) = u$, 則儲存算子為 $2u + v$ 。

有了儲存算子，再看函數的加權 $w(f) = \prod_{d \in D} w(f(d))$ ，於是，不同的

函數可能有相同的加權；例如，

	r_1	r_2	r_3
d_1	✓		
d_2		✓	
d_3	✓		

,

	r_1	r_2	r_3
d_1		✓	
d_2	✓		
d_3			✓

所代表

的兩個函數它們的加權都是 u^2v 。

從函數的加權，我們可以看出 D 中元素的分配情形 (f)，例如 u^2v ，代表有兩個 u -type，一個 v -type，而當我們有很多個分配放在一起的時候，這些加權的總和就可以反應出整體元素分配的情形。我們為了方便起見，把這些函數的加權之總和以 I_s 代表，其中 S 代表所有一起討論的函數所成的集合。 I_s 一般稱為 S 的儲存和 (Inventory)。

接著，我們來看等價關係對上述加權概念的影響。

定理 2.1. (輔助定理)

等價函數的加權值相等。

證明. 由前面定義 $f_1 \sim f_2$ ，若且唯若存在一個排列 $\pi \in G$ ，滿足 $f_1(d) = f_2(\pi(d))$, $\forall d \in D$ 。所以， $\prod_{d \in D} w[f_1(d)] = \prod_{d \in D} w[f_2(\pi(d))]$ ，但是 $\prod_{d \in D} w[f_2(\pi(d))] = \prod_{d \in D} w[f_2(d)]$ ，所以 $W(f_1) = W(f_2)$ 。 ■

因此，在同一等價類的函數都具有相等的加權，這個加權也稱為是這個等價類 (或型式, Pattern) 的加權。不過，值得一提的是具有相同加權的函數，不一定會來自同一等價類。

例. (函數加權的概念)

有 8 個人，其中 3 個來自一個家庭，另 2 個來自一個家庭；他們準備去拜訪 3 個城市，而且同一家庭的人要一起去，試問不同的訪問方法有多少種？

利用上述的概念，令 $D = \{a, b, c, d, e, f, g, h\}$, $R = \{c_1, c_2, c_3\}$ ，其中 $\{a, b, c\}$, $\{d, e\}$ 分別為兩家庭的成員；同時 c_1, c_2, c_3 的加權分別為 α, β, γ ，則由 $(\alpha^3 + \beta^3 + \gamma^3)(\alpha^2 + \beta^2 + \gamma^2)(\alpha + \beta + \gamma)^3$ (?) 可以求出不同的訪問方式。(很像生成函數的概念，不是嗎？)

要求出函數的等價需要多一些的工具。

在上一節，我們已經發現排列群，或排列子群在計數上所扮演的角色；同時，如何把一個排列以適當的方式表示出來也很重要。所以，首先介紹圈分解 (Cycle Factorization) 的概念。

例.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 1 & 7 & 3 & 6 & 5 & 8 & 2 \end{pmatrix} = (14753) \circ (29) \circ (6) \circ (8)。$$

(14753) 代表 $1 \rightarrow 4, 4 \rightarrow 7, 7 \rightarrow 5, 5 \rightarrow 3, 3 \rightarrow 1$ 。

定理 2.2. 任一個排列皆有唯一的圈分解。

(註). 沒有共同元素的圈可以交換，這裡的運算 "o" 為函數的合成。

定義 2.3. 令 f 為一集合 X 的排列， $|X| = n$ 。我們用 $\#(f)$ 代表 f 的圈分解中圈的個數。而 $t(f)$ 則代表一個 n -維向量 $(e_1, e_2, \dots, e_n)$ ，其中 e_i 代表圈的大小為 i 的個數， $i = 1, 2, \dots, n$ 。

例. 上例中， $\#(f) = 4$ ， $t(f) = (2, 1, 0, 0, 1, 0, 0)$ 。

為了計數的方便性，令 $mon(f) = z_1^{e_1} z_2^{e_2} \cdots z_n^{e_n}$ ，所以當 G 為一排列群時，我們可以得到 (根據 $t(f)$) 一個生成函數 $\sum_{f \in G} mon(f) = \sum_{f \in G} z_1^{e_1} z_2^{e_2} \cdots z_n^{e_n}$ 。

定義 2.4. (圈指標數, Cycle Index)

一個 n 元集合 X 的排列群 G 的圈指標數為 $P_G(z_1, z_2, \dots, z_n) = \frac{1}{|G|} \sum_{f \in G} z_1^{e_1} z_2^{e_2} \cdots z_n^{e_n}$ 。

例. $P_{D_4}(z_1, z_2, z_3, z_4) = \frac{1}{8} (z_1^4 + 2z_4 + 3z_2^2 + 2z_1^2 z_2)$ 。

(註) D_4 有 8 個元素， $P_{D_4}(z_1, z_2, z_3, z_4)$ 說明了這 8 個元素的圈分解形式分別有一個單位元素，兩個 4-圈，三個形為 $(ab)(cd)$ 的圈，以及兩個形式為 $(x)(y)(zw)$ 的圈。

現在，我們可以證明 Pólya 定理。

定理 2.5. 令 S 代表所有由 D 映至 R 的函數所成的集合，則 S 中等價類 (對應於 G) 的儲存和 (Inventory) 等於 $P_G(z_1, z_2, \dots, z_n)$ ，其中 $z_i = \sum_{r \in R} [w(r)]^i$ ， $i = 1, 2, \dots, n$ 。

證明. 省略。(有興趣的同學可參考 C. L. Liu, Introduction to Combinatorial Mathematics.)

推論 2.6. 由 D 映至 R 的函數之等價類 (對應於 G) 等於 $P_G(|R|, |R|, \dots, |R|)$ 。

証明. 令 R 中每一個元素的加權都是 1。 ■

從上面的推論可以知道：要計算等價類的個數，首先得求出排列群 G ，再利用圈指標數 $P_G(z_1, z_2, \dots, z_n)$ 以 $|R|$ 代入 $z_i, i = 1, 2, \dots, n$ ，即可求出所要的答案。另外，如果 R 中的元素有不同的加權，還是得利用定理 2.5。

問題 2. 利用兩個顏色 x 與 y 來塗一個正四面體的四面，試求不同的著色形式 (等價類)。

解. $P_G(z_1, z_2, z_3, z_n) = \frac{1}{3}(z_1^4 + 2z_1z_3)$ (?)。

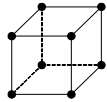
所以方法數為 $P_G(2, 2, 2, 2) = \frac{1}{3}(2^4 + 8) = 8$ 。著色方法的所有形式則為 $\frac{1}{3}[(x+y)^4 + 2(x+y)(x^3+y^3)]$ 。

(註) $z_1 = x + y, z_3 = x^3 + y^3$ 。(定理 2.5. $w(x)=x, w(y)=y$ 。)

作業.

50. 試畫出問題 1 的七個不同型式之項鍊。

51. 如果項鍊型式只考慮旋轉之後相同才算同型，問用紅、黃、藍三種顏色一共 5 個寶石，所串成的項鍊有多少種型式。

52. 試求用 n 個顏色去圖一個正六面體的八角落，，用不同的方法 (經各種方向轉動後仍不同)。

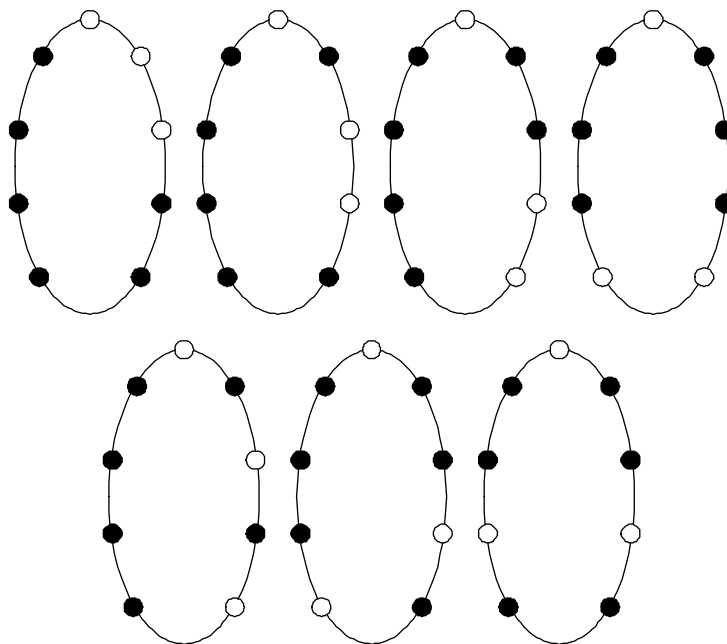
同時證明 $n^8 + 17n^4 + 6n^2$ 為 24 的倍數。

53. 如果我們用 6 種顏色來塗正六面體的每一面，而且每面各一種不同顏色，問方法有多少種？

解答.

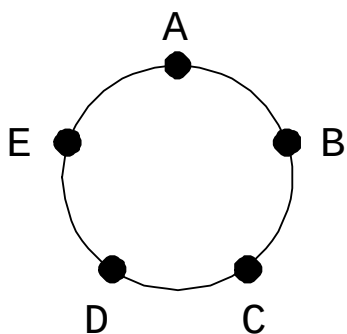
50. 試畫出問題 1 的七個不同型式之項鍊。

答.



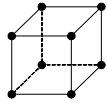
51. 如果項鍊型式只考慮旋轉之後相同才算同型，問用紅、黃、藍三種顏色一共 5 個寶石，所串成的項鍊有多少種型式。

答.



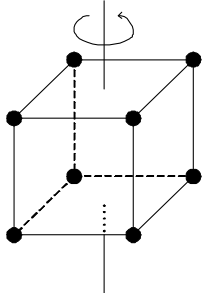
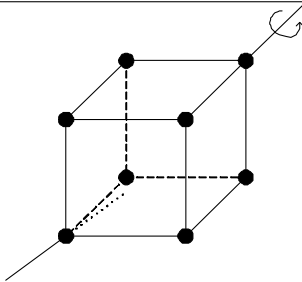
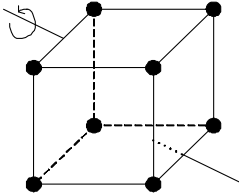
旋轉	0°	3°
	72°	3
	144°	3
	216°	3
	288°	3
共 5 種		255

所以 $\frac{255}{5} = 51$

52. 試求用 n 個顏色去圖一個正六面體的八角落，，用不同的方法（經各種方向轉動後仍不同）。

同時證明 $n^8 + 17n^4 + 6n^2$ 為 24 的倍數。

答.

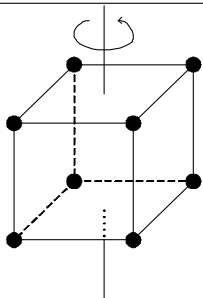
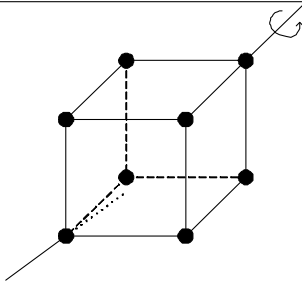
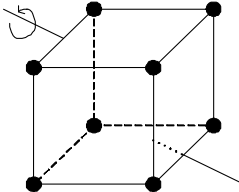
	0°	n^8	
		n^8	
	90° 180° 270°	n^2 n^4 n^2	$\times 3$
	9	$3n^4 + 6n^2$	
	120° 240°	n^4 n^4	$\times 4$
	8	$8n^4$	
	180°	n^4	$\times 6$
	6	$6n^4$	
Total	24	$n^8 + 17n^4 + 6n^2$	

所以 $24 \mid (n^8 + 17n^4 + 6n^2)$ 。

53. 如果我們用 6 種顏色來塗正六面體的每一面，而且每面各一種不同顏色，問方法有多少種？

答.

令六個顏色為 a, b, c, d, e, f ，則

旋轉	0°	$(a + b + c + d + e + f)^6$ (找 abcdef 項的係數)	
因為每面顏色都不同，所以以下不需考慮			
			
			
			
Total	24		

因為每面顏色不同，故所有方法數為 $\frac{6!}{24} = 30$
(另解：先固定一面，則 $1 \times 5 \times \left(\frac{4!}{4}\right) = 30$)