

初步數學散雜

林福來 教授譯

九章算術是中國古老、最有系統的算書，
我們以之爲名，冀望爲我國數學教育獻力

離散數學初步

●林福來 譯●

本書譯作權 屬
國立編譯館所有

出版者：九章文化事業有限公司

臺北市羅斯福路三段 297 之 2 號

3940207 . 3940208

(局版臺業字第 1871 號)

發行人：陳碧美

印刷者：九章文化事業有限公司

出版日期：中華民國 69 年 9 月初版

定價：250元（平裝本）

郵政劃撥：112091 孫文先帳戶

(本書如有缺頁、破損、請寄回更換)

版權所有◎翻印必究

(法律顧問：范光順律師事務所)

離散數學初步

本書譯作權屬
國立編譯館所有

(法律顧問：范光順律師事務所)

導 言

本書取材自集合論，組合理論，圖形學及代數書中，個人認為較基本並且對於主修應用數學，電算機科學和工程的同學有幫助的部分，設計的對象是供大二或大三程度的學生當做離散數學的教科書，又因學習本書所需的預備知識很少超越高中的數學程度，所以大一的學生也可以使用，本書的教材，對於程度較好的學生，可以在一學期內，每週四節，教完。對進度比較慢的班級，可以刪掉其中一部分、章節之前，帶有星號*的刪掉後，並不會影響全書的連貫性。

本書是我在伊利諾大學（Urbana — Champaign校區）電算機系開課的講義整理後付梓的。希望本書不僅是紀錄我在課內所談的教材，同時還能反應出我當時在班上是如何講授這份教材的。我所嘗試的是，當我嚴密且直截了當地灌輸數學概念的同時，還要避免複雜的形式化以及符號，原則上，如果我沒有辦法提出具體而有意義的例子來解釋定義或定理，那麼這些定義，定理我就寧可不談。基於此原則，很可能地，本書將遺漏一些重要的定義或定理，不過，我確信當學生們需要這些定義或定理的時候，他們一定很容易可以在其他書上找到並且瞭解它們。我嘗試着以有趣生動的方式教學生們一些有用的數學。希望同學們修過這門課之後，能夠瞭解數學是如何地應用於解決一些實際的日常生活問題，進一步希望我

有效的數學工具

的能力。雖然

不過在許多章

我個人的觀點

只學一些

數學問題

的知識，

希望這些

……以文。

感謝我們 James N. Synd 的鼓勵與支持；同時感謝 Murruy Euelberg, Jane W. S. Lin 和 Andrew H. Sherman 等人將原稿仔細地看過；Donald K. Friesen 幫忙準備教師手冊；

Edward M. Reingold 和 F. Frances Yao 等人許多建設性的建議，都是我衷心感激的。幾年之前，我有幸參與一次由美國數學學會的大學數學課程委員會所主辦，關於數學上的計算的研討會。從該次研討會關於“離散數學的教學”的討論中，我個人真是獲益匪淺，對參與該研究會的成員，我也很感激，同時感謝幫忙打字及編輯的 G. Glenna Gochenour, Connie Nosbisch, Judy Wathins 和 June Winger。最後，還要謝謝 Kathleen D. Lin 的幫忙整理索引。

本書與多年前我所寫的一本“組合數學導論”有一部分雷同，許多例題，跟組合數學導論一書所舉的都一樣。

C. L. Lin

第一章 集合與命題

1•1	引言	1
1•2	集合的運算	5
1•3	有限集合與無限集合	10
1•4	數學歸納法	15
1•5	排容原理	20
1•6	重元素	26
1•7	命題	28
1•8	參考資料	32

第二章 排列與組合

2•1	引言	47
2•2	加法律與乘法律	47
2•3	排列	48
2•4	組合	54
2•5	排列和組合的推廣	60
2•6	參考資料	63

第三章 關係與函數

3•1	引言	71
3•2	圖表中心所用的關係模式	75
3•3	二元的關係性質	78
3•4	等價關係與分割	82
3•5	偏序關係與絡	86
3•6	鏈與散鏈	90
3•7	工程的輪工表問題	92
3•8	函數與鴿籠	97

3.9	參考資料	
-----	------	-------

第四章 圖形與平面圖形

4.1	引言	 113
4.2	基本術語	 115
4.3	多邊圖和加權圖	 119
4.4	路徑與廻路	 122
4.5	加權圖中最短的路徑	 124
4.6	尤拉路徑與尤拉環路	 128
4.7	漢米爾頓路徑與漢米爾頓環路	 135
4.8	推銷員的旅程問題	 140
4.9	圖形的 k 次子圖	 146
4.10	平面圖形	 151
4.11	參考資料	 157

第五章 數與切集

5.1	樹	 174
5.2	帶根樹	 178
5.3	帶根樹中的路徑長	 182
5.4	字首密碼	 185
5.5	二元尋查樹	 190
5.6	衍生樹與切集	 194
5.7	最小衍生樹	 199
5.8	運輸網路	 203
5.9	參考資料	 210

第六章 離散數值函數與生成函數

6.1	引言	 221
-----	----	-----------

6.2	數值函數間的運算	222
6.3	生成函數	228
6.4	組合問題	235
6.5	摘要及參考資料	240

第七章 遞迴關係數

7.1	引言	248
7.2	常係數線性遞迴律	249
7.3	利用生成函數求解	257
7.4	數字編列	262
7.5	附注及參考資料	271

第八章 群與環

8.1	引言	280
8.2	群	282
8.3	子群	288
8.4	生成元素與乘冪計算	289
8.5	陪集及 Lagrange 定理	293
8.6	置換群	295
8.7	密碼與群密碼	303
8.8	同構與自同構	307
8.9	同態與正規子群	310
8.10	環、整域和體	316
8.11	環的同態	320
8.12	多項式環與循環密碼	323
8.13	參考資料	326

第九章 布爾(Boole)代數

9•1	絡與代數系	339
9•2	對偶原理	342
9•3	絡所定義的代數系的基本性質	344
9•4	分配性與具補絡	347
9•5	布爾絡與布個代數	351
9•6	有限布爾代數的唯一性	352
9•7	布爾函數與布爾式	358
9•8	命題的運算	359
9•9	設計與數字的網路機器	363
9•10	開關電路	366
9•11	參考資料	373

第一章

集合與命題

1.1 引言

本書的主要內容是要研究離散事物 (discrete objects) 以及它們之間的關係。離散事物這術語是一個普通名詞。它所包含的事物非常地多，例如人，書，電算機，收音機，電算機程式……等等。在我們的日常生活以及技術性的工作中，常會碰到這些事物，同時也會涉及一些敘述，像“這教室內的人都是電算系二年級的學生”，“我買的所有書都是 A. B. Charles 所著的偵探小說”，以及“我希望選購一部同時可作學術與商業用的電算機，並且價格不能超過 200,000 元”，我們希望將涉及的許多種不同的離散事物的一些基本概念，加以抽象化，同時定義一些關於它們的共用術語。

仔細觀察上面這三個敘述，我們發現它們有一些共同的地方，因此將其抽象化的可能性是相當明顯的。說得明白一點，在第一個敘述中，我們涉及的是具有兩種特性的人——電算系並且是二年級生；在第二個敘述中，我們談的是具有兩種特性的書——一種偵探小說且是 A. B. Charles 所著的；在第三個敘述中，我們涉及的是具三種特性的電算機——適用於學術研究，適用於商業用途及價錢不能夠超過 200,000 元。讓我們從另外一個角度，來描述上面這些人、書和電算機，如果考慮電算系的所有學生群，以及大學二年級的所有學生群，那麼在我們上面第一個敘述中所涉及的就是同時屬於這兩群的學生。

如果考慮所有的偵探小說類及 A. B. Charles 所著的所有小說，那麼第二個敘述中所涉及的就是屬於這兩類的小說。最後，如果我們考慮所有適合學術研究用的電算機、所有適合商業用的電算機以及價錢少於 200,000 元的電算機，那麼第三個敘述所涉及的就是同時屬於這三個範疇的電算機。

上面的例子，說明了我們時常會碰到許多類的事物，又希望考慮那些同時屬於每一類的事物。同樣地，我們也時常考慮那些屬於好幾類的事物中的某一類的事物，例如，下面的敘述，“我要會談所有會講德語或者法語的學生”。這敘述中，我們所涉及的學生，是屬於講德語的學生群，或者屬於講法語的學生群。

現在就開始來介紹一些基礎集合論中的一些基本的術語和概念。

一集合是一群相異的事物。因此，所有大學二年級的學生形成一集合，所有電算系的學生也是一集合。當時，所有電算系二年級的學生也形成一集合。將以符號 $\{a, b, c\}$ 代表包含 a, b, c 三件事物的集合。在一集合中的事物稱為這集合的元素 (elements) 或分子 (members)。通常也給整個集合命名，例如， $S = \{a, b, c\}$ 意思就是說一個名為 S 的集合，包含有 a, b, c 三個元素。此時，我們稱集合 S 與稱集合 $\{a, b, c\}$ 指的對象都一樣。另外一個例子：

電算系二年級學生 $= \{ \text{陳建中, 李明光, 王中生, 胡又明, 林小思} \}$

(這裡集合 $\{ \text{陳建中, 李明光, 王中生, 胡又明, 林小思} \}$ 的名字是電算系二年級學生，相當地長。讀者可能會建議何不改變個簡捷的名字，例如 S 或 CS 。不過我們在此強調長的集合名字也沒有錯。) 符號 $a \in S$ 代表 a 是集合 S 的一個元素。此時，亦稱 S 包含元素 a 。符號 $d \notin S$ 代表 d 不是集合 S 中的元素，此時，稱 S 不包含元素 d 。例如上面的例子中，林小思 $\in$ 電算系二年級學生，但是，林小品 $\notin$ 電算系二年級學生。

我們還需注意集合中包含的元素都是相異的。像集合 $\{a, a, b, c\}$ 應該寫成 $\{a, b, c\}$ ；同樣地， $\{\text{午夜訪客, 午夜訪客}$

，失蹤的證人，114 大街}也是一種不當的表示 A. B. Charles 所著的偵探小說的方法。或許有人會問：如果圖書館藏有 A. B. Charles 所著的偵探小說“午夜訪客”兩本，“失蹤的證人”及“114 大街”各一本，那麼如何表示這 4 本書呢？這種情況下，集合{午夜訪客，失蹤的證人，114 大街}是指圖書館中所藏 A. B. Charles 的偵探小說的書名，而集合{午夜訪客—1，午夜訪客—2，失蹤的證人，114 大街}則是指圖書館中所藏 A. B. Charles 所著的偵探小說，其中午夜訪客—1 指第一本午夜訪客，午夜訪客—2 指第二本午夜訪客。要注意的是，在後面這集合中，午夜訪客—1 及午夜訪客—2 是兩件不同的事物。

集合中的元素並沒有次序關係。因此， $\{a, b, c\}$ 和 $\{b, a, c\}$ 代表同樣的集合。稍後，我們還會介紹有序集 (ordered sets) 的概念。

如上所述，將所有這些元素都列出來是描述一個集合中的元素的方法之一。不過，有很多情形，當一個集合的元素共有某些特性時，我們可以敘述能夠明確決定這集合元素的特徵；所描述這些元素。例如，令 $S = \{2, 4, 6, 8, 10\}$ ，我們可以說 S 的元素是所有不大於 10 的正偶數。這也可以用符號來表示：

$$S = \{x \mid x \text{ 是不大於 } 10 \text{ 的正偶數}\}$$

一般而言，我們將以符號

$$\{x \mid x \text{ 具有某些性質}\}$$

來描述具有某些共同性質的集合中的元素，因此，

$$S = \{\text{陳建中, 李明光, 王中生, 胡又明, 林小思}\}$$

$$\text{和 } S = \{x \mid x \text{ 是一電算系二年級學生}\}$$

是兩種不同描述同一集合的元素的方法。

一個集合中如果不包含任何的元素，稱之為空集合 (empty set)，以符號 ϕ 表之。(如果利用兩個大括號來表示集合，那麼空集合也可以用 $\{\}$ 來表示)。例如，設 S 代表 A. B. Charles 在 1924 年出版的所有偵探小說所成的集合。顯然地，因為 A. B. Charles 生於 1925 年，所以 S 是一空集合。

一個集合中的元素，並沒有任何限制，因此 $S = \{ \text{林小思}, \text{午夜訪客}, \text{CDC} - 6600 \}$ 也是一個有意義的集合。其中的元素，林小思（一個人），午夜訪客（一本書的書名），和 $\text{CDC} - 6600$ （一種電算機）看起來似乎沒有任何關係，並不需要將其同時放在一個集合裡，不過並不影響它們形成一個集合的事實。另外，還得指出，一個集合的元素也可以是集合。因此，例如，集合 $\{ \{ a, b, c \}, d \}$ 就是一個集合，包含兩個元素 $\{ a, b, c \}$ 和 d ，其中的一個元素 $\{ a, b, c \}$ 本身也是一個集合，再如 $\{ \{ a, b, c \}, a, b, c \}$ 是一個集合，包含 4 個元素 $\{ a, b, c \}$ ， a ， b 和 c 。又如美國參議院的所有委員會可以用集合 $\{ \{ a, b, c \}, \{ a, d, e, f \}, \{ b, e, g \} \}$ 來表示，這集合中的每一個元素代表一個委員會，這些委員會也是集合，以參加該委員會的參議員為其元素。同樣地， $\{ a, \{ a \}, \{ \{ a \} \} \}$ 也是一集合，包含三個相異的元素 a ， $\{ a \}$ 及 $\{ \{ a \} \}$ 。集合 $\{ \phi \}$ 包含一個元素——空集合，而集合 $\{ \phi, \{ \phi \} \}$ 則含有兩個元素，一個是空集合，另一個是恰含空集合一個元素的集合。

給定兩個集合 P 和 Q ，如果 P 中的每一個元素都是 Q 中的元素，就稱 P 是 Q 的子集（subset）。將以符號： $P \subseteq Q$ ，代表 P 為 Q 的一子集。例如，集合 $\{ a, b \}$ 是集合 $\{ x, y, b, c, a \}$ 的一子集，但 $\{ a, b \}$ 不是集合 $\{ a, c, d, e \}$ 的子集。電算系二年級學生的集合是大二學生的子集；同時也是電算系學生的子集。反過來，電算機系的學生集並不是大二學生集的子集，而大二學生集也不是電算機系學生集的子集。設 $A = \{ a, b, c \}$ ， $B = \{ \{ a, b, c \}, a, b, c \}$ ，此時， $A \in B$ 且 $A \subseteq B$ 。以下的一些簡單性質，請讀者自行驗證：

對任意集合 P ， P 為 P 的一子集

空集合是每一個集合的一子集

集合 $\{ \phi \}$ 不是集合 $\{ \{ \phi \} \}$ 的子集

設 P 和 Q 為兩集合，如果 P 和 Q 包含相同的元素，就稱 P 和 Q 兩集合相等。例如，令

$$P = \{ x \mid x \text{ 是不大於 } 10 \text{ 的正偶數} \}$$

$$Q = \{ x \mid x = y + z, \text{ 其中 } y \in \{ 1, 3, 5 \}, \\ z \in \{ 1, 3, 5 \} \}$$

則 $P = Q$ 。設 P 和 Q 為二集合，若 P 為 Q 的一子集且 Q 亦為 P 的一子集，則 $P = Q$ 。有時候，以這敘述當做兩集合相等的定義，非常方便，稍後就會遇上這種例子。

設集合 P 為集合 Q 的一子集，如果 P 不等於 Q ，就稱 P 為 Q 的真子集 (Proper subset)。也就是說，至少有一個 Q 中的元素不在 P 中。例如，集合 $\{ a, b \}$ 是集合 $\{ x, y, b, c, a \}$ 的一真子集。將以符號 $P \subset Q$ 代表 P 是 Q 的真子集。

1.2 集合的運算

這小節將介紹，集合與集合經過不同的方法組合可以產生新的集合。例如，設 P 代表所有選修計算理論的學生所成的集合， Q 代表所有選修音樂欣賞的學生所成的集合，如果在計算理論課及音樂欣賞課，教授都宣佈了某一新聞，試問聽到這兩位教授宣佈該新聞的學生所成的集合是什麼？顯然地，這集合的元素是選了計算理論課或音樂欣賞課的學生。再說，如果這兩門課的期末考時間相同，那麼這兩門課期末考衝堂的學生所成的集合是什麼？當然，這集合的元素就是同時選了計算理論與音樂欣賞的學生。爲了將這些概念形式化，我們將定義集合的聯集和交集。集合 P 和 Q 的聯集 (union) 是一集合，恰含 P 中或 Q 中的所有元素，以符號 $P \cup Q$ 表之。例如，

$$\{ a, b \} \cup \{ c, d \} = \{ a, b, c, d \}$$

$$\{ a, b \} \cup \{ a, c \} = \{ a, b, c \}$$

$$\{ a, b \} \cup \phi = \{ a, b \}$$

$$\{ a, b \} \cup \{ \{ a, b \} \} = \{ a, b, \{ a, b \} \}$$

集合 P 和 Q 的交集 (intersection) 是一集合，恰含同時在 P 及 Q 中的所有元素，以符號 $P \cap Q$ 表之。例如，

$$\{ a, b \} \cap \{ a, c \} = \{ a \}$$

$$\{ a, b \} \cap \{ c, d \} = \phi^*$$

$$\{ a, b \} \cap \phi = \phi$$

如果集合 P 中的元素是以其所具有的某一共同性質所指出，集合 Q 中的元素則是以其所具有的另一個共同性質所指出，則 P 和 Q 的聯集，是具有這兩種共同性質之一的所有元素所成的集合，而 P 和 Q 的交集，則是同時具有這兩種共同性質的所有元素所成的集合。根據聯集的定義， $P \cup Q$ 與 $Q \cup P$ 為相等的集合。同時 $P \cap Q$ 與 $Q \cap P$ 也是相等的集合。

一般而言，如果有 k 個集合， $P_1, P_2, \dots, P_k$ ，則其聯集

$$P_1 \cup P_2 \cup \dots \cup P_k \text{ 是一集合，恰含 } P_1, P_2, \dots, P_k$$

中的所有元素。而其交集

$$P_1 \cap P_2 \cap \dots \cap P_k \text{ 則是一集合，恰含同時在 } P_1, P_2, \dots$$

$, P_k$ 中的所有元素。例如，某一大學中大學部的所有學生集是大大一學生集、大二學生集、大三學生集和大四學生集的聯集。四年級畢業生集是大四學生集，修滿 144 學分以上的學生集和平均成績在 C 等以上的學生集的交集。

設 P 代表選修計算理論的學生集， Q 代表選修音樂欣賞的學生集， R 代表血型是 AB 型的學生集。假設在計算理論課及音樂欣賞課，作了一緊急宣佈，急需血型 AB 的志願捐血者。現在希望知道聽到這緊急宣佈後有資格捐血者的名單。因為聽到緊急宣佈的學生所成的集合是 $S = P \cup Q$ 。因此希望知道的名單就是 $R \cap S$ 中的所有元素。如果不預先將 $P \cup Q$ 的另一名字 S 表示，那麼所求的名單為 $R \cap (P \cup Q)$ 中的元素，其中的括號是為避免混淆加進去的。再從另一個角度看，有資格捐血者是那些學生？這些聽到緊急宣佈而有資格捐血的學生，有些是在計算理論課上聽到而有資格者，另一些是在音樂欣賞

* 兩個集合如果交集是空集合，就稱此二集合不相交 (disjoint)

課上聽到而有資格捐血者。因此，所有聽到緊急宣佈又夠資格捐血的學生集是 $(R \cap P) \cup (R \cap Q)$ 。這個例子指出，對任意的集合 $P, Q, R, R \cap (P \cup Q)$ 和 $(R \cap P) \cup (R \cap Q)$ 應該是相等的兩集合。以下就來證明這事實。

首先證明： $R \cap (P \cup Q) \subseteq (R \cap P) \cup (R \cap Q)$ ，亦即欲證 $R \cap (P \cup Q)$ 中的每一個元素，都在 $(R \cap P) \cup (R \cap Q)$ 中。設 x 為 $R \cap (P \cup Q)$ 中的一元素。

根據交集的定義， x 同時為 R 及 $P \cup Q$ 的元素。根據聯集的定義， $x \in R$ 並且 ($x \in P$ 或者 $x \in Q$)。即 x 一定在 R 中，並且 x 在 P 或 Q 之中。如果 $x \in P$ ，那麼 $x \in R \cap P$ ；如果 $x \in Q$ ，那麼 $x \in R \cap Q$ 。因此， $x \in (R \cap P) \cup (R \cap Q)$ 。故得： $R \cap (P \cup Q) \subseteq (R \cap P) \cup (R \cap Q)$ 。

接着再證明： $(R \cap P) \cup (R \cap Q) \subseteq R \cap (P \cup Q)$ 。設 x 為 $(R \cap P) \cup (R \cap Q)$ 中的一元素，則由聯集的定義， x 為 $R \cap P$ 或者 $R \cap Q$ 中的一元素；即 x 必同時為 R 和 P 中的元素，或者同時為 R 和 Q 中的元素。換句話說， x 必為 R 的一元素，並且為 P 或者 Q 中的一元素。因此， $x \in R \cap (P \cup Q)$ 。故， $(R \cap P) \cup (R \cap Q) \subseteq R \cap (P \cup Q)$ 。

綜合上述證明，即得： $R \cap (P \cup Q) = (R \cap P) \cup (R \cap Q)$ 。

利用相同的方法，可以證明：對任意的三個集合 P, Q 和 R ，

$$R \cup (P \cap Q) = (R \cup P) \cap (R \cup Q)。$$

進一步，還可證明下列二等式；設 $P_1, P_2, \dots, P_k, R$ 為任意的集合，則

$$R \cap (P_1 \cup P_2 \cup \dots \cup P_k) = (R \cap P_1) \cup (R \cap P_2) \dots \cup (R \cap P_k)$$

$$R \cup (P_1 \cap P_2 \cap \dots \cap P_k) = (R \cup P_1) \cap (R \cup P_2) \dots \cap (R \cup P_k)$$

這兩個等式的證明細節，由讀者自證。^{*}

設 P 和 Q 為兩個集合， P 和 Q 的差集是一集合，恰含在 P 但不在 Q 的所有元素，將以符號 $P - Q$ 表之。例如，

$$\{a, b, c\} - \{a\} = \{b, c\}$$

$$\{a, b, c\} - \{a, d\} = \{b, c\}$$

$$\{a, b, c\} - \{d, e\} = \{a, b, c\}$$

設 P 為擁有某一場球賽門票的人所成的集合， Q 是該球賽當天生病的人所成的集合，則 $P - Q$ 為將去參觀該場球賽的人所成的集合。當然， Q 可能包含一些 P 中的元素，也可能不包含任何 P 中的元素，不管有沒有，這些人都不在 $P - Q$ 中。至於生病，又沒有參觀球賽的門票的人不管怎樣，都不會去參觀球賽。如果 Q 中的元素是由某些共有的性質所指出，則 $P - Q$ 中的元素為在 P 中，但不具有那些性質的元素。如果 Q 是 P 的子集，那集合 $P - Q$ 就稱為是 Q 對 P 的餘集 (

Complement of Q with respect to P)。例如，令 P 為選修計算理論的學生所成的集合，而 Q 為選修計算理論課且成績及格的學生所成的集合。則 $P - Q$ 就是該科成績不及格的學生所成的集合。討論餘集時，如果集合 P 從內容中很容易看出，且又不致於混淆，我們可將“ Q 對於 P 的餘集”簡稱為“ Q 的餘集” (the complement of Q)， Q 的餘集將以符號 $\overline{Q}$ 表示。例如，令 P 代表所有選修計算理論課的學生所成的集合， Q 為選修計算理論課的電算機系的學生所成的集合， R 是選修計算理論課的大二學生所成的集合。則 Q 的餘集代表選修計算理論課的非電算機系的學生所成的集合； R 的餘集是計算理論班上非大二的學生集，也就是在討論這些集合時，我們總把對象限制在選修計算理論課的學生。一般而言，當我們作某種討論時，恒將討論的對象限制為某一集合 P 的子集上，就稱 P 為宇集合 (the universe)。

* 目前還不準備介紹代數運算的結合性及分配性；這些將在第八章中介紹。因為 $P \cap Q$ ， $P \cup Q$ ， $P_1 \cup P_2 \cup \dots \cup P_k$ ，根據定義，都只是代表集合的名字，所以並不真正需要結合性和分配性的概念。