師大數學

7

MATH·MATH·MATH·MA

國立台灣師範大學數學系

目 錄

分割理論簡介

中央研究院數學研究所
陳明博

我們所知道的，在整數論的研究中，有一支是利用解析的方法來討論的，這就是大家所謂的解析的整數論（Analytic Number Theory）除了素數（Prime numbers）分佈的討論等等之外，分割理論（Partition Theory）的探討也是在解析的整數論中很熱門的一支，本文將就分割理論做一個簡單的介紹，爲了節省篇幅，許多地方我們在此不想做詳儘的討論，對於一些基本的定義定理等等，敬請讀者參考（9 ；第12,13和 14章），（38 ；第12章），（44；第19章），以及（63 ；第10章）。

令N表示爲所有正整數的集合，A爲N的子集合，對於任意一正整數 n，令$P_A(n)$ 表示將n 表爲A中元素之和亦卽形成

$$n = a_1 + a_2 + \cdots\cdots + a_m$$

$$a_i \in A,\quad 1 \leqq i \leqq m,\quad m \in N$$

的表示方法的個數，其中的 a_i 我們稱爲和項（summard），分割理論就是在研究算術函數$P_A(n)$的性質，最簡單的情形也就是說當A＝N時，此種分割函數通常記之爲P(n)，今就 n＝5 舉例說明如下：

5 的所有分割爲5，4＋1，3＋2，3＋1＋1，2＋2＋1，2＋1＋1＋1，以及1＋1＋1＋1＋1，因此P(5)＝7。當然我們可加條件於和項之上，例如我們可以規定a_i均相異，此種分割函數記之爲$q_A(n)$，當A＝N時，簡寫爲q(n)，例如q(5)＝3，我們也可以加條件在和項數m之上，例如 $9_{m=3}(5)=2$，通常我們恒規定$P_A(0)=1$

圖形的表示法以及母函數（generating function）的探討爲研究分割理論的兩種最常用的方法。今首先談談圖形的表示法。

圖形的討論法卽是一般所謂的組合法（Combinatorial method），對於任一正整數n，令　$n = a_1 + a_2 + \cdots\cdots + a_m$　爲n的一個分割（partition）表示法，其中的a_i 是依大小的順序而排列的，卽$a_1 \geqq a_2 \geqq \cdots\cdots \geqq a_m$，我們利用n 個點的圖形來代表此一分割，這n 個點是依水平線由上而下排成m行，每一行的最左邊的一點是排成一縱直線的，第一行有 a_1 個點，第二行有 a_2 個點，………第m行有 a_m 個點，利用這種圖形我們就可以來研究分割函數的一些性質了，擧n＝7 爲例，4＋2＋1爲7 的一個分割表示法，這個分割的圖形爲

$$\begin{array}{llll} \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & & \\ \bullet & & & \end{array}$$

但是我們如果就這圖形由左向右讀，將每一縱直線上的點的個數看成一和項，此時這圖形對應於 7 的另一個分割 3＋2＋1＋1，圖形的研究法即是利用此種一一對應的關係來討論的，今舉一個實際的定理來說明：

定理 1：令 $P_m(n)$ 表將 n 表爲和項數（number of summands）不超過 m 的分割數，$\pi_m(n)$ 表爲和項均不超過 m 之分割數，則 $P_m(n)=\pi_m(n)$

證：　讓我們考慮將 n 表爲和項數 i 不超過 m（$i\leqq m$）的一個分割的圖形，此一圖形由上而下讀一共有 i 行，因爲此一 i 行是最長而短來排列的，因此我們如果由左而右讀的話，有一縱直線也是由長而短來排列的，我們已說過，每一縱線的點數看成一和項，因爲最左一列有 i 點，因此如果把從左至右讀看成 n 的一個分割的話，則此種分割的最大和項爲 i，但 $i\leqq m$，因此此種分割的和項均不超過 m 的，即 $P_m(n)$ 中之一種分割對應於 $\pi_m(n)$ 中之一種分割，逆推也成立，利用這種一一對應的關係，我們就證得 $P_m(n)=\pi_m(n)$。

以 n＝5，m＝3 來說明，$P_3(5)=5$ 即 5，4＋1，3＋2，3＋1＋1，2＋2＋1 等 5 種。$\pi_3(5)=5$ 即 3＋2，3＋1＋1，2＋2＋1，2＋1＋1＋1，1＋1＋1＋1＋1 等五種，他們的一一對應關係爲

$5 \longleftrightarrow 1+1+1+1+1$

• • • • •

$4+1 \longleftrightarrow 2+1+1+1$

• • • •
•

$3+2 \longleftrightarrow 2+2+1$

• • •
• •

$3+1+1 \longleftrightarrow 3+1+1$

• • •
•
•

$2+2+1 \longleftrightarrow 3+2$

• •
• •
•

設 f(n) 爲定義在非負整數上的函數；即數論函數，f(n) 的母函數爲

$$F(x)=\sum_{n=0}^{\infty} f(n)x^n \quad \cdots\cdots\cdots\cdots(1)$$

在組合理論的討論中，我們只關心係數 f(n)，而不必考慮級數(1)的收斂性，即討論形式冪級數（formol power series）就好了，事實上我們如果加上 $|x|<1$ 的條件，常常能使級數(1)滿足收斂性，甚至於絶對收斂性或一致收斂性的。

無限制分割函數 P(n) 的母函數爲

$$\sum_{n=0}^{\infty} P(n)x^n$$

並且不難證得（見 9；第 162 頁定理 13-3）

定理 2：$$\sum_{n=0}^{\infty} P(n)x^n=\prod_{j=1}^{\infty}\frac{1}{1-x^j},\quad |x|<1 \quad \cdots\cdots\cdots\cdots(2)$$

以及

定理3：$\sum_{n=0}^{\infty} q(n)x^n = \prod_{j=1}^{\infty}(1+x^j)$，$|x|<1$ …………(3)

（見9；164頁定理13-5）。

事實上我們可以更進一步得到（見38；220頁定理1）

定理4：$\sum_{n=0}^{\infty} P_A(n)x^n = \prod_{a\in A}(1-x^a)^{-1}$，$|x|<1$ ………(4)

利用 $\sum_{n=0}^{\infty} q(n)x^n = \prod_{j=1}^{\infty}(1+x^j)$

$$= \prod_{j=1}^{\infty}\frac{(1+x^j)(1-x^j)}{(1-x^j)}$$

$$= \prod_{j=1}^{\infty}\frac{(1-x^{2j})}{(1-x^j)}$$

$$= \prod_{j=1}^{\infty}(1-x^{2j})\prod_{j=1}^{\infty}(1-x^j)^{-1}$$

$$= \prod_{j=1}^{\infty}(1-x^{2j})\prod_{j=1}^{\infty}(1-x^{2j})^{-1}(1-x^{2j-1})^{-1}$$

$$= \prod_{j=1}^{\infty}(1-x^{2j-1})^{-1}$$

以及定理4， 設$P_o(n)$表示將n表爲和項均爲奇數的分割數，我們可以得到Euler有名的結果即

定理5：$q(n)=P_o(n)$

此定理的證明方法，開創了利用分析來討論整數論的新紀元。

上一定理的證明，將無限乘積

$$\prod_{n=1}^{\infty}(1-x^n)，\text{ ………………(5)}$$

在分割理論中所佔的重要地位完全展露出來了，因此引起一些數學家對於(5)的推廣無限乘積

$$\prod_{n=0}^{\infty}(1-q^{2n+2})(1+q^{2n+1}z)(1+q^{2n+1}z^{-1})\text{…(6)}$$

的廣泛興趣（以$q=x^{\frac{1}{2}}$，$z=-x^{\frac{1}{2}}$代入(6)中即得(5)）。

Jacobi首先得到下列結果

定理6：（Jacobi triple product identity）

$$\prod_{n=0}^{\infty}(1-q^{2n+2})(1+q^{2n+1}z)(1+q^{2n+1}z^{-1}) = \sum_{n=-\infty}^{\infty} q^{n^2}z^n，$$

$$z\neq 0 \quad |q|<1 \text{ ……………………………(7)}$$

Jacobi原來的證明方法並不簡單，最近Andrews教授（9；169頁定理13-8）（8；333-334），以及Menon教授〔60〕提出了簡單的解析證法）尤其Andrews教授的證明方法只需利用到Euler的兩個等式（9；167頁定理13-7），是一個非常漂亮的

證明方法，故值得在此加以推薦的。

等式(7)是相當有用的，例如L. Carlitz在1962（21；591-592）利用(7)而得

定理7：令$\alpha(n,m)$表示將(n,m)表爲相異和項$(a,a-1)$，$(b-1,b)$（$a,b=1,2,3\cdots\cdots$），的和的分割數，則

$$\alpha(n,m)=P\left(n-\frac{1}{2}(n-m)(n-m+1)\right)$$

在1965年E. M. Wright依據此一結果，將(7)給予一個組合法的證明〔74〕，由此引起了大家對於組合證明法的興趣，在此方面Andrews〔6，和14〕，Cheema〔25〕，Sudler〔70〕均有所貢獻。

我們以$q=x^{\frac{3}{2}}$，$z=-x^{\frac{1}{2}}$代入(7)中就可以得到一個非常重要的Euler's五角數（Pentagonal Number）定理。

定理8：$$\prod_{n=1}^{\infty}(1-x^n)=\sum_{n=-\infty}^{\infty}(-1)^n x^{n(3n-1)/2}\ ,\ |x|<1\cdots\cdots\cdots(8)$$

在這裏值得一提的，就是定理8的組合證明法（38；232-235），（44；286-288）開創了組合證法的始祖。

定理8在分割理論的討論上是相當有用的，例如我們可利用定理2和定理5而得（38）；224定理5）。

定理9：$$P(n)=P(n-1)+P(n-2)-P(n-5)-P(n-7)+\cdots\cdots+(-1)^{j+1}P(n-n_j)+\cdots\cdots,\ n_j=\frac{1}{2}j(3j\pm1)\cdots\cdots\cdots\cdots\cdots(9)$$

利用此公式，我們就可以逐次求出$P(n)$的值來，Ramanujan就是利用此公式來對$P(n)$做研究的，一直到最近（29；125-127）J. A. Ewell利用定理8得

定理10：(i) $$\sum_{k=0}(-1)^{k(k+1)/2}P(2n-k(k+1)/2)=q(n)$$

(ii) $$\sum_{k=0}(-1)^{k(k+1)/2}P(2n+1-k(k+1)/2)=0$$

此處之k是取所有使P（ ）有意義之k。

漸近行爲（Asymptotic behaviors），同餘等式（Congruence identities），以及分割恒等式（Partition identities），爲研究分割理論的主要三大支流，現在首先談談漸近理論的發展。

對於任意正整數n易知$P(n)\geqq n$因此$P(n)\to\infty$，當$n\to\infty$，但是$P(n)$趨於無窮的速度如何呢？這是我們所感興趣的問題。這個問題在1920年左右，首先由Hardy和Ramanujan，以及Uspensky所解決了，他們的結果是這樣的。〔43〕，〔71〕，（19；146-155），（24；178-184），或（49；90-99）。

定理11：$P(n)\sim\dfrac{1}{4n\sqrt{3}}\exp\left(\sqrt{\dfrac{2}{3n}}\,\pi\right)$當$n\to\infty$。Hardy-Ramanujan的證明方法引進了Modular functions，他們的證法並不簡單，因此此後的許多數論專家致力於尋求定理11的簡單證法以及餘項（Remainder）的探求。經過數學家們的努力，最後在1962年，D. J. Newman得到了一個很簡單的證明方法（見61；283-287）。另一個問題就是討論有條件分割函數（Restricted partition function）的漸近行爲

，例如q(n)趨於無窮的速度如何呢？等等，在這一部門。Ingham〔47〕，Iseki〔48〕，Grosswald〔37〕，Petersson〔64〕，Meinardus〔59〕，Rademacher〔65〕，等均有所貢獻，我最近也做了一些結果，例如其中之一爲（見27）。

定理12：令r(n)表將n分割爲和項均爲形式 $8m+1$，$8m+4$，$8m+7$（$m=0,1,2,\cdots\cdots$）的分割數，則

$$r(n)\sim 2^{-11/4}(\sqrt{2}+1)^{1/2}n^{-3/4}\exp\left(\frac{\sqrt{n}}{2}\pi\right),\ n\to\infty$$

欲知這一方面更進一步的發展，請參考〔24〕，〔27〕，以及在〔27〕中所列到的參考資料。

同餘等式的研究起自Ramanujan（1887～1920）。他利用公式(9)將P(n)的值由 $n=1$ 來到 $n=200$，列出一個表來探求P(n)的性質，然後利用Jacobi triple product identity證明出（見44；288-289，或63；243-245）

定理13：(i) $P(5m+4)\equiv 0\pmod 5$

(ii) $P(7m+5)\equiv 0\pmod 7$

(iii) $P(11m+6)\equiv 0\pmod{11}$

在此附帶提一下，(iii)的原來證明並不簡單，在1969年L. Winquist提出了一個相當簡單的證明方法（73；56-59），是值得大家參考的。

Ramanujan更依據P(n)的值（$1\leqq n\leqq 200$）而做了下列的假定；當 $\delta=5^a7^b11^c$ 之形式（a，b，c均爲非負整數）且 $24n\equiv 1\pmod\delta$ 時，則 $P(n)\equiv 0\pmod\delta$ 他本人只證明到當 $\delta=5^2,7^2,11^2$ 時，他的假定是正確的，但是在1934年Chowla和Gupta得到 $n=243$ 滿足 $24n-1=5831\equiv 0\pmod{7^3}$

$P(243)=1339782593448 88\equiv 0\pmod{7^2}$

但是 $\not\equiv 0\pmod{7^3}$ 〔28〕

因此將Ramanujan的假定推翻了，到了1938年，Watson改正Ramanujan的假定，他假定〔72〕

(i)若 $24n\equiv 1\pmod{5^a}$ 則 $P(n)\equiv 0\pmod{5^a}$

(ii)若 $24n\equiv 1\pmod{7^b}$ 則 $P(n)\equiv 0\pmod{7^{[(b+2)/2]}}$

(iii)若 $24n\equiv 1$ (mob 11^c) 則 $P(n)\equiv 0\pmod{11^c}$

他同時也將(i)(ii)給予完整的證明，但是關於(iii)的證明，一直到最近，才由一位英國的數學家A. O. L. Atkin完全將它證明出來〔17〕，到此我們就可以總結一下而得

定理14：若 $24n\equiv 1\pmod{5^a7^b11^c}$，a，b，c均爲非負整數，則得 $P(n)\equiv 0\pmod{5^a7^d11^c}$ $d=[(b+2)/2]$ 在這類問題之上，J. Lehner〔58〕，M. Newman〔62〕以及Zuckerman〔76〕等幾位數學家均有所貢獻，讀者如果欲知這個定理的詳細證明，敬請閱讀M. Knopp的書。

同餘等式的問題就到此結束嗎？不是的，例如Atkin和Brien在1967〔18〕就曾經討論到13的問題，還有17，19………等等無限個的質數呢？問題是做不完的，只是每一個問題恐怕均是很難的。M. Newman也提出假定；對於任一對正整數m和r，同餘方程式 $P(n)\equiv r\pmod m$ 是否有無限多解呢？這也是一個尚未完全解決的問題，還有D. B. Lahiri在最近〔51～56〕也一連串做了類似；「對幾乎所有n，${}^{48}_{14}P(n)\equiv {}^{48}_{2}p(n-4)\pmod 2$，${}^{27}_{3}p(n)\equiv {}^{27}_{6}p(n)\equiv {}^{27}_{12}p(n)\equiv 0\pmod 3$，${}^{121}p(11n+6)$

$\equiv 0 \pmod{11}$。」等諸類的問題，總之對於此類的問題，還有許多的話可以談的，爲了節省篇幅就此擱筆了，有興趣的讀者敬請閱讀〔41〕，以及在它上面所提到的參考文獻。

最後就是要談一談關於分割恒等式的問題，這一個問題最早起自於定理5。但是在十九世紀並沒有任何數學家注意到這問題，到了本世紀初葉，印度數學家Ramanujan重新開始致力於這一方面的研究，他的主要兩個定理（9；第14章）（44；290～295）；開了分割等式的新里程。

定理15：將n分割爲任何兩和項之差至少爲2的分割數恰等於將n分割爲和項均爲形式5m+1，5m+4之分割數。

定理16：將n分割爲任何兩和項之差至少爲2，且任何和項均不小於2的分割數恰等於將n分割爲和項均爲形式5m+2，5m+3的分割數。

Ramanujan爲了證明這兩個定理，引證了兩個非常有名的Rogers-Ramanujan恒等式；

定理17：當$|\chi|<1$，則

$$1+\sum_{n=1}^{\infty}\frac{\chi^{n^2}}{(1-\chi)(1-\chi^2)\cdots\cdots(1-\chi^n)}=\prod_{n=0}^{\infty}\frac{1}{(1-\chi^{5n+1})(1-\chi^{5n+4})}$$

以及

$$1+\sum_{n=1}^{\infty}\frac{\chi^{n^2+n}}{(1-\chi)(1-\chi^2)\cdots\cdots(1-\chi^n)}=\prod_{n=0}^{\infty}\frac{1}{(1-\chi^{5n+3})(1-\chi^{5n+4})}$$

後來很多數論專家們一方面在尋求此二恒等式的組合證法，例如見（11,15,31）以及各論文中所提到的參考資料，和此二等式的簡單證明方法，見（7及13），尤其〔13〕所提到的68篇論文是對於Rogers-Ramanjan恒等式最完整的資料。以及此二恒等式的推廣等式，在這方面請參看〔1〕，〔16〕，以及〔16〕中所列出的參考文獻。

但是在1920～1960年之間，分割等式却死沈了一陣子，到了1966年Andrews教授發表了下列定理（見4，5，和8）重新又把分割等式從墳墓裏挖出來。

定理18：設a和k均爲整數$0<a\leqq k$令$A_{k,a}(n)$表將n分割爲和項並不是形式$(2k+1)m$，$(2k+1)m\pm a$的分割數，令$B_{k,a}(n)$表示將n寫成

$$n=b_1+b_2+\cdots\cdots+b_s$$

$b_i\geqq b_{i+1}$，$b_i-b_{i+k-1}\geqq 2$，且1最多僅能出現a−1次在和項中之分割數，則$A_{k,a}(n)=B_{k,a}(n)$。

實際上這個定理是定理15和定理16的推廣，在最近7年內，關於分割等式的新論文眞是如同雨後春筍不勝枚擧，到了1972年在這方面，Andrews教授更有了輝煌的貢獻，他引白了格子論（Lattice Theory）將分割等式帶到更廣泛且帶有一點點抽象意味的境地了。在此我鄭重介紹有興趣的讀者閱讀〔2〕，〔12〕以及此兩篇論文中所提到的115篇的文獻，則在此方面的研究工作必定會有很大的收穫。

當然的，分割理論的研究並不是僅僅只限於這三方向，一些新的基礎性質的發現（例如39，40和42），已知結果的新的簡單證明方法（例如30）和組合證法（例如66），以及電子計算機在分割理論方面的應用（例如10和26）等，總是人們所感興趣的，除了分割理論的抽象化（見R.P.Stanley在哈佛大學的畢業論文）之外，數學家們又開創了二維，三維，甚至於高維的分割理論了，卽所謂Plane partitions，Solid partitions等等，例如請參考（20,22,32～36，46,67～69，以及75），大家可以發現這些均是非常新的論文，這是因爲多維分割的理論剛剛正在發芽的時期，在這方面將有很多的寶藏等待我們去挖掘

，希望在此能引起拋磚引玉的作用，導致大家對分割理論的興趣，此外在研究分割理論上所需要利用到的特殊函數（Special functions）尤其是超幾何函數（Hypergeometric functions）的發展，以及一些零星的Ramanujan's型的無窮連分數（例如見23和45）也是非常有趣的問題。

最後謝謝母系使我有這個機會向各位介紹分割理論的一些智識。

參考文獻

1. H.L. Alder, Generalizations of the Rogers-Ramanujan identities, Pacific J. Math., 4 (1954), 161-168.
2. H.L. Alder, Partition identities from Euler to the present, Amer. Math. Monthly, 76 (1969), 733-746.
3. G.E. Andrews, A simple proof of Jacobi's triple product identity, proc. Amer. Math. Soc. 16(1965), 333-334.
4. G.E. Andrews, An analytic proof of the Rogoers-Ramanujan Gordon identities, Amer. T. Math., 88(1966) 844-846.
5. G.E. Andrews, Partition thuorems related to the Rogers-Ramanujan identities, J. Combinatorial theory, 2(1967), 422-430.
6. G.E. Andrews, Enumerative proofs of certain q-identities, Glasgow Math. J. 8(1967) 33-40.
7. G.E. Andrews, A polynomial identity which implies the Rogers-Ramanujan identities, Scripta Math. 23(1970) 297-305.
8. G.E. Andrews, A generalization of the classical partition theorem, Trans. Amer. Math. Soc., 145(1969), 205-221.
9. G.E. Andrews, Number Theory, W.B. Saunders company (1971).
10. G.E. Andrews, The use of computers in search of identities of the Rogers-Ramanujan type, computers in Number Theory, Edited by A.O.L. Atkin and B.J. Birch, Academic press (1971), 377-387.
11. G.E. Andrews, Sieves for theorems of Euler, Rogers, and Ramanujan, proceedings of the Kalamazoo conferences on Arithmetic Functions, Springer-Verlag, Lecture Notes in Math., No. 251, 1-20.
12. G.E. Andrews, Partition Identities, Advances in Mathematics, 9(1972), 10-51.
13. G.E. Andrews, on identities implying the Rogers-Ramanujan identities, to appear.
14. G.E. Andrews, Two theorems of Gauss and allied identities proved arithmetically, to appear.
15. G.E. Andrews, Sieves in the theory of partitions, to appear.

16. G. E. Andrews, On the Alder polynomials and a new generalization of the Roges-Ramanujan identities, to appear.
17. A. O. L. Atkin, proof of a conjecture of Ramanujan, Glasgow Math. J. 8, 14-32 (1967).
18. A. O. L. Atkin., and J. N. O'Brien, Some properties of P(n) and c(n) modulo powers of 13, Trans. Amer. Math. Soc. 126, 442-459 (1967).
19. R. Ayoub, An introduction to the analytic theory of numbers, (chapter 3), Amer. Math. Soc., (1963).
20. E. A. Bender and D. B. Kunth, Enumeration of plane partitions, J. of combinatorial Theory (A) 13, 40-54 (1972)
21. L. Carlity, A note on the Jacobi theta formula, Bull. Amer. Math. Soc., 68 (1962), 591-592.
22. L. Carlitz and J. Riodan, Enumeration of some two-line arrays by extent, J. of combinatorial Theory 10, 271-283 (1971)
23. L. carlitz, Some continued fraction formulas, Duke Math. J. 39 (1972), 793-799.
24. K. Chandrasekharan, Arithmetical functions, Springer-Verlag., (1970).
25. M. S. Cheema, Vector partitions and combinatorial identities, Math. comp. 18(1964), 414-420.
26. M. S. Cheema and W. E. Conway, Numerical investigation of certain asymptotic results in the theory of partitions, Math. Comp. 26(1972), 999-1005.
27. M. P. Chen, Asymptotic theorems in partition theory, Ph. D thesis, The Pennsylvania State University, (1972).
28. S. Chowla, congruence properties of partitions, J. London Math. Soc. 9, 247 (1934).
29. J. A. Ewell, partition recurrences, J. of combinatorial Theory (A) 14, 125-127 (1973).
30. J. M. Gandhi, Generalization of Ramanujan congruences $P(5m+4)\equiv 0 \pmod 5$ and $P(7m+5)\equiv 0 \pmod 7$, Monatsh. Math. 69, 389-392 (1965).
31. B. Gordon, A combinatoril generalization of Rogers-Ramanujan identities, Amer. J. Math 83, 393-399 (1961).
32. B. Gordon and L. Houten, Notes on plane partitions I, J. Combinatorial Theory 4, 72-80 (1968).
33. B. Gordon and Houten, Notes on plane partitions II, J. Combinatorial Theory 4, 81-99 (1968).

34. B. Gordon and and L. Houten, Notes on plane partitions Ⅲ, Duke Math. J. 37, 801-824 (1970)

35. B. Gordon, Notes on plane partitions Ⅳ, proc. of Symposia in pure Math. vol XIX, Combinatories (1970) 91-100.

36. B. Gordon, Notes on plane partitions V. J. of Combinatorial Theory 11, 157-168 (1971).

37. E. Grosswald, Elementary proofs in the theory of partitions, Math Z. 81, 52-61 (1963).

38. E. Grosswald, Topics from the theory of Numbers, The Macmillan company, New York, (1966).

39. H. Gupta, partition of j-partite numbers, Math. Student 31 (1963) ; 179-186 (1964).

40. H. Gupta, Highly restricted partitions, J. Res. Nat. Bur. Stand. B 73 (1969) 329-335.

41. H. Gupta, partitions- a survey, J. Res. Nat. Bur. stand. B 74 (1970), 1-29.

42. H. Gupta, On partitions of n into k summands, proc. of the Edinburgh Math. Soc., 17 (1971) 337-339.

43. G. H. Hardy and S. Ramanujan, Asymptotic formula in combinatory analysis, proc. London Math. Soc (2) 17 (1918), 75-115 [=Collected papers of S. Ramanujan, 276-309 (paper 36), = Collected papers of G. H. Hardy, Volume I, 306-339.]

44. G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 4th ed, Oxford Univ. Press, Oxford, (1960).

45. M. D. Hirschhorn, partitions and Ramanujan continued fraction, Duke Math. J. 39 (1972), 789-791.

46. L. Houten, A note on solid partitions, Acta Arithmetica, XV (1968) 71-76.

47. A. E. Ingham, A Tauberian theoum for partitions, Ann. of Math. 42(1941), 1075-1090.

48. S. Iseki, A proof of a functional equation related to the theory of partitions, proc. Amer. Math. Soc., 12 (1961), 502-505.

49. M. I. Knopp, Modular functions in analytic number theory, Markham, (1970).

50. D. Knuth, A note on solid partitions, Math. of comp. 24 (1970), 955-961.

51. D. B. Lahiri, Some restricted partition functions: Congruences modulo 7, Trans. Amer. Math. Soc. 140 (1969), 475-484.

52. D. B. Lahiri, Some restricted partition functions, congruences

mod 5, J. Austr. Math. Soc 9(1969), 424-432.

53 D.B. Lahiri, Some restricted partition functions: congruences modulo 3, Pacific J., Math., 28 (1969) 575-581.

54 D.B.Lahiri, Some restricted partition functions: congruences modulo 3, J. Austr. Math. Soc 10(1970) 82-90.

55 D.B.Lahiri, Some restricted partition functions: congruences modulo 2, Trans. of the Amer. Math. Soc., 147 (1970), 271-278.

56 D.B.Lahiri, Some restricted partition functions: congruences modulo 11, pacific J. of Math. 38 (1971), 103-116.

57 D.H.Lehmer, On the Hardy-Ramanujan series for the partitions function, J. London Math. Soc. 12, 171-176(1937).

58 J. Lehner, proof of Ramanujan's partition congruence for the modulus 11³, proc. Amec. Math. Soc. 1, 172-181(1950).

59 G. Meinardus, Über Partition mit Differengenbedingungen, Math. Z. 61(1954), 289-302.

60 P.K. Menon, On Ramanujan's continued fraction and related identities, J. London Math. Soc. 40 (1965), 49-54.

61 D. J.Newman, A simplified proof of the partition formula, Michigan Math. J. 9, 283-287(1962).

62 M. Newman, congruence for the partition functions to composite moduli, Illinois J. Math. 6, 59-63 (1962).

63 Niven and Zuckerman, An introduction to the theory of Numbers, Second Edition, John Wiley & Sons, Inc., (1966).

64 H. Petersson, Über Modulfunktionen und partition-probleme, Abh. Deutsch Akad Berlin kl. Math. Allg. Nat.1954. No. 2, p.59.

65 H. Rademacher, A convergent series for the partition function. proc. Nat. Acad. Sci. (V.S.A.)

66 V. Ramamani and k. Venkatachaliengar, On a partition theorem of Sylvester, Michigan Math. J. 19(1972) 137-140.

67 R.P. Stanley, Theory and application of plane partition : part 1, Studies in App. Math. Vol L (1971), 167-188.

68 R.P.Stanley, Theory and application of plane partition: part 2, Studies in App. Math. vol L (1971), 259-279.

69 R.P. Stanley, The conjugate trace and trace of a plane partition, J. of combinatorial Theory (A) 14, 53-65 (1973).

70 C. Sudler, Two enumerative proofs of an identity of Jacobi, proc. Edinburgh Math. Soc. 15 (Series II, 1966-1967), 67-71.

71 J.V.Vspensky, Asymptotic expressions of numerical functions occuring in problems of partition of numblers (in Russian), Bull.

Acad. Sci deRussie (6), 199-218.

72. G.N. Watson, Ramanujan's Vermutung über Zerfallungszahlen, J. Reine Angew. Math. 179, 97-128 (1938).

73. L. Winquist, An elementary proof of $P(11m+6)\equiv 0 \pmod{11}$, J. of combinatorial Theory 6, 56-59 (1969).

74. E.M. Wright, An enumerative proof of an identity of Jacobi, J. London Math. Soc. 40 (1965), 55-57.

75. E.M. Wright, Stacks (III), ouart. J. of Math. (Oxford) (2) 23 (1972), 153-158.

76. H. S. Zackerman, Identities analogous to Ramanujan's identities involving the partition function. Duke Math. J. 5, 88-110 (1939).

Network Flows In Scheduling School Courses

Yueh-Er Kuo
University of Tennessee

From [1] we know the following: A capacitated network (N,K) consists of a finite set N of nodes which will be denoted by x, y, etc. An ordered pair of nodes (x, y) is called an edge of the network. The capacity function k attaches to each edge (x, y) a nonnegative integer k(x, y).

A flow in the network (N, k) is a function f which attaches an integer f(x, y) to each edge (x, y) of the network and satisfies $f(x, y)=-f(y, x)$ and $f(x, y)\leqq k(x, y)$.

The theory of network flows can be applied to make class-teacher timetables.

Example 1. There is a high school which contains three classes C_1, C_2 and C_3. One teacher teaches one course. We want to make class-teacher timetables for a week under the following conditions:

1. Every class must take 5 hours of English, 4 hours of Mathematics, 4 hours of Natural Science, and 2 hours of Social Science a week.
2. Every class takes at most 2 hours of lessons for one course every day.
3. Every class must take 3 hours of lessons for these courses every day from 8 a.m. to 11 a.m.

We denote the teachers of English, Mathematics, Natural Science, and Social Science by T_1, T_2, T_3 and T_4 respectively. We put Monday, wednesday, Friday, Tuesday, and Thursday as an order in the table to avoid C_1 taking the same course serially (see Table 1). In Table 1 we put 1 at the positions which are assigned C_i to T_j, and 0 at the positions which cannot be assigned.

Let S_1 be any subset of $S=\{C_1, C_2, C_3\}$, and $T(S_1)$ be all T_j for which at least one member of S_1 is qualified. It is possible to make this class-teacher timetable if for any S_1, $T(S_1)$ contains at least as many elements as S_i in every subtable (an application of Theorem 5.2 in [1]). The rule of assignment in evey subtable is :

1. Assign C_i to the T_j for which he was qualified having the lowest subscript (e.g. $(C_1, T_1) = 1$ in the first subtable). Having assigned the first k C_i, we assign the (k + 1)st to the T_j for which he qualifies which has not been previously assigned, having the lowest subscript (e.g. $(C_2, T_2) = 1$ in the first subtable).

2. Put 0 at the position which already satisfied the conditions 1 or 2 of the problem in the previous table (e.g. $(C_1, T_1) = 0$ in the third subtable).

3. In the case we cannot assign, find a path form an unassigned C_i to an unassigned T_j (e.g. Friday 10-11 a.m. ; $(C_1, T_2) = 1$, $(C_2, T_1) = 1$. $C_3 \to T_1 \to C_2 \to T_4$; remove (C_2, T_1) to $C_2, T_4) = 1$ and assign $(C_3, T_1) = 1$).

		Mondy				Wednesday				Friday				Tuesday				Thursday			
		T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4
8-9	C_1	1				1				1				0	0	1		0	0	1	
	C_2		1				1				0	1		1	0			1	0		
	C_3			1				1			1	0	0		1	0	0		1	0	0
9-10	C_1	1				1				0*	1			0	0	1		0	0	1	
	C_2		1				1				0	1		1	0			0*	0		1
	C_3			1				1		1		0	0		1	0	0	1	0*	0	0
10-11	C_1	0*	1			0*	1			0*	1			0	0	0*	1	0	0		1
	C_2	1	0*			1	0*			1^{a}	0	0	$\to 1^{b}$	0*	0	1		0*	0	1	
	C_3			0*	1			0*	1	1		0	0	1	0*	0	0	1	0*	0	0
Total hours a day	C_1	2	1			2	1			1	2					2	1			2	1
	C_2	1	2			1	2					2	1	2		1		1		1	1
	C_3			2	1			2	1	2	1			1	2			2	1		
Positions that can-not be assigned any more	C_1									0	0			0	0			0	0	0	0
	C_2						0				0				0			0	0	0	0
	C_3							0	0			0	0			0	0	0	0	0	0

TABLE 1

0 : indicates the positions which cannot be assigned any more after this table

0*: indicates the positions which cannot be assigned any more in this day.

1^a: becomes 0 at the same time 1^b becomes 1

Therefore we can get the following timetables.

Date	T_1			T_2			T_3			T_4		
	1	2	3	1	2	3	1	2	3	1	2	3
M	C_1	C_1	C_2	C_2	C_2	C_1	C_3	C_3				C_3
T	C_2	C_2	C_3	C_3	C_3		C_1	C_1	C_2			C_1
W	C_1	C_1	C_2	C_2	C_2	C_1	C_3	C_3				C_3
Th	C_2	C_3	C_3	C_3			C_1	C_1	C_2		C_2	C_1
F	C_1	C_3	C_3	C_3	C_1	C_1	C_2	C_2			C_2	

TABLE 2

TIMETABLE FOR TEACHERS

Date	C_1			C_2			C_3		
	1	2	3	1	2	3	1	2	3
M	E	E	M	M	M	E	N	N	S
T	N	N	S	E	E	N	M	M	E
W	E	E	M	M	M	E	N	N	S
Th	N	N	S	E	S	N	M	E	E
F	E	M	M	N	N	S	M	E	E

TABLE 3

TIMETABLE FOR STUDENTS

E : English

M : Mathematics

N : Natural Science

S : Social Science

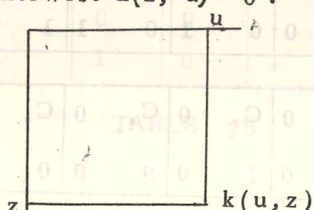
Form [1] we also know the following : In a transhipment problem, some of the nodes are plants and others are markets: The set of plants is denoted by p and the set of markets is denoted by M. The supply at the plant x in p is denoted by σ (x) and the demand at the node x in M is denoted by δ (x). A transhipment problem is called feasible if there is a flow f such that $f(N,x) \geqq \delta(x)$ for $x \varepsilon M$, and $f(x, N) \leqq \delta(x)$ for $x \varepsilon p$.

Another example of an application of network flows is the scheduling of students to courses in a college.

Exmple 2. A college offers courses C_1, C_2, C_3, C_4, and C_5. The opening of these courses are 2, 1, 2, 2, and 3 classes respectively. There are three different groups S_1, S_2, and S_3 of students; they must take 4, 3, and 3 courses respectively. S_2 cannot take C_2, and S_3 cannot take C_4 (for exmple, C_2 is Calculus II; and S_2 did not take Calculus I before). We want to make a schedule which sati satisfies these conditions.

We make Table 4 and put 1 if S_i can take C_j; put 0 if S_i cannot take C_j.

Let $S=\{S_1, S_2, S_3\}$, $C=\{C_1, C_2, C_3, C_4, C_5\}$, $N=\{S_1, S_2, S_3, C_1, C_2, C_3, C_4, C_5\}$, M be any subset of N and $M'=N-M$. The number of courses which a group of students y in S must take is noted by $\sigma(y)$, and the number of classes of opening course x in C is denoted by $\sigma(x)$. $k(z, u)$ is an entry in the table below if $z \varepsilon S$, $u \varepsilon C$, otherwise $k(z, u)=0$.



The scheduling is possible if for every set M,

$$\sum_{x \varepsilon M' \cap C} \delta(x) - \sum_{y \varepsilon M' \cap S} \sigma(y) \leqq \sum_{z \varepsilon M,\, u \varepsilon M} k(z, u)$$

(an application of Theorem 5.3 in [1]).

		C_1	C_2	C_3	C_4	C_5
		Number of Classes				
		2	1	2	2	3
	No. of Courses					
S_1	4	1	1	1	1	1
S_2	3	1	0	1	1	1
S_3	3	1	1	1	0	1

TABLE 4

We make an expanded table :

	C_1 2	C_2 1	C_3 2	C_4 2	C_5 3
S_1 4	1 : 0	1 : 0	1 : 0	1 : 0	1 : 0
S_2 3	1 : 0	0 : 0	1 : 0	1 : 0	1 : 0
S_3 3	1 : 0	1 : 0	1 : 0	0 : 0	1 : 0

TABLE 5

We start by moving as many as possible from S_1 to C_1 without exceeding number of classes or entries in the table. Then,

	C_1 1	C_2 0	C_3 1	C_4 1	C_5 3
S_1 0	0 : 1	0 : 1	0 : 1	0 : 1	0 : 0

We do the same way for S_2 and S_3.

	C_1 0	C_2 0	C_3 0	C_4 0	C_5 3
S_2 0	0 1	0 0	0 1	0 1	1 0

	C_1 0	C_2 0	C_3 0	C_4 0	C_5 2
S_3 2	1 0	1 0	1 0	0 0	0 1

The full table is :

		C_1	0	C_2	0	C_3	0	C_4	0	C_5	2
S_1	0	0	1	0	1	0	1	0	1	1	0
S_2	0	0	1	0	0	0	1	0	1	1	0
S_3	2	1	0	1	0	1	0	0	0	0	1

TABLE 6

We seek paths from S_3 to C_5.

$$S_3 \to C_1 \to S_2 \to C_5$$
$$S_3 \to C_3 \to S_1 \to C_5$$

Having added the flows in the usual manner, we get the new table:

		C_1	0	C_2	0	C_3	0	C_4	0	C_5	0
S_1	0	0	1	0	1	1	0	0	1	0	1
S_2	0	1	0	0	0	0	1	0	1	0	1
S_3	0	0	1	1	0	0	1	0	0	0	1

TABLE 7a

i.e.:

	C_1	C_2	C_3	C_4	C_5
S_1	1	1	0	1	1
S_2	0	0	1	1	1
S_3	1	0	1	0	1

TABLE 7b

Therefore

S_1 takes C_1, C_2, C_4, C_5

S_2 takes C_3, C_4, C_5, and

S_3 takes C_1, C_3, C_5,

REFERENCE

〔1〕 D. Gale: The Theory of Linear Economic Models. New York: McGraw-Hill Book Company, 1960.

冪零群

Nilpotent Group

•教授•常法徽

本文多取材於 Jeseph J. Rotman 所著之群論第六章，今述之於后，以供參考：

記號：

1. $H \triangleleft G$ 表 H 爲群 G 之正規子群（Normal subgroup）.
2. 若 H，K 爲群 G 之子群，令

$$(H, K) = \{ h^{-1}k^{-1}hk \mid h \in H, k \in K \}$$

(H, K) 表由 $h^{-1}k^{-1}hk$ 形式之元素形成之子群。

引1　設 H 爲群 G 之子群，若且唯若 $(H, G) \subset H$，則 $H \triangleleft G$.

證：若 $(H, G) \subset H$，則對於每 $h \in H$，$g \in G$ 有

$$h^{-1}g^{-1}hg \in H$$

$$\therefore \quad g^{-1}gh \in H$$

故　$H \triangleleft G$.

反之，設 $H \triangleleft G$，則對於每 $h \in H$，$g \in G$，有

$$g^{-1}hg \in H$$

$$\therefore \quad h^{-1}g^{-1}gh \in H$$

故　$(H, G) \subset H$

引2　設 H，K 爲群 G 之子群及 $K \triangleleft G$，$K \subset H$. 若且唯若 $(H, G) \subset K$ 時，則 $H/K \subset Z(G/K)$.

證：設 $(H, G) \subset K$，則對於每 $h \in H$，$g \in G$ 有

$$h^{-1}g^{-1}hg \in K$$

即　$(gh)^{-1}hg \in K$

$$\therefore \quad ghK = hgK$$

$$gK\ hK = hK\,gK$$

$$hK \in Z(G/K)$$

故　$H/K \in Z(G/K)$

反之，若 $H/K \subset Z(G/K)$，則對於每 $hK \in H/K$ 及 $gK \in G/K$ 有

$$hK\,gK = gK\,hK$$

$$\therefore \quad hgK = ghK$$

$$h^{-1}g^{-1}hg \in K$$

故 $(H, G) \subset K$

引3　設 $f \cdot G \longrightarrow L$ 爲群G映成群L之同態寫像，若 $A \subset Z(G)$，則 $f(A) \subset Z(L)$.

證：設 $A \subset Z(G)$ 及 $x \in A$，則對於每 $g \in G$，均有 $xg = gx$

故　$f(xg) = f(gx)$

即　$f(x)f(g) = f(g)f(x)$

故　$f(x) \in Z(L)$

　　$f(A) \subset Z(L)$

定義1　設G爲群，定

$$\gamma(G) = G$$

$$\gamma_{i+1}(G) = (\gamma_i(G), G)$$

於此 i 爲正整數。

於正整數 i 上，可用歸納法證明 $(\gamma_i(G), G) \subset \gamma_i(G)$.

$i = 1$ 時，　$(G, G) \subset G$

故　$(\gamma_1(G), G) \subset \gamma_1(G)$

次設　$(\gamma_1(G), G) \subset \gamma_1(G)$，則

$$(\gamma_{i+1}(G), G) = ((\gamma_i(G), (G), G) \subset (\gamma_i(G), G) = \gamma_{i+1}(G)$$

即　$(\gamma_{i+1}(G), G) \subset \gamma_{i+1}(G)$

故對於每一正整數 i 均有

$$(\gamma_i(G), G) \subset \gamma_i(G)$$

故　$\gamma_i(G) \triangleleft G$　　　(引1)

且然以　$\gamma_{i+1}(G) \subset \gamma_i(G)$　故 $\gamma_{i+1}(G) \triangleleft \gamma_i(G)$

定義2　下列正規級數

$$G = \gamma_1(G) \supset \gamma_2(G) \supset \cdots\cdots$$

稱爲群G之降中心級數 (Desending central series)

定義3　設G爲群，定 $Z^{\circ}(G) = \{e\}$，於此 e 爲G之么元素。於自然同態寫像 $f_i : G \longrightarrow G/Z^i(G)$ 下，定 $Z^{iH}(G)$ 爲G中與 $G/Z^i(G)$ 之核心 $Z(G/Z^i(G))$ 相對應之子群。即 $Z^{i+1}(G) = f_i^{-1}(Z(G/Z^i(G)))$。

於 $i = 0$，顯見 $Z^1(G)$ 即爲G之核心 $Z(G)$，證之如下：

設　$x \in Z^1(G)$，則

$$f_{\circ}(x) = xZ^{\circ}(G) = x\{e\} \in Z(G/\{e\})$$

對於每 $g \in G$，有 $g\{e\}\chi\{e\} = \chi\{e\}g\{e\}$，故 $gx = xg$，即 $x \in Z(G)$

故 $Z'(G) \subset Z(G)$，反之，設 $y \in Z(G)$，則對於每 $g \in G$，有 $gy = yg$，

故 $f_{\circ}(g)f_{\circ}(y) = f_{\circ}(y)f_{\circ}(g)$ 而 $f_{\circ}(y) \in Z(G/\{e\})$ 矣，

$y \in f_{\circ}^{-1}\left(Z\left(G/\{e\}\right)\right)$　　$Z'(G)$，由此知 $Z(G) \subset Z'(G)$ 故

$Z(G) = Z'(G)$.

次者可證明 $Z^i(G) \subset Z^{i+1}(G)$，$Z^{i+1}(G) \lhd G$，證之如下：

設　$x \in Z^i(G)$，則

$$f_i(x) = xZ^i(G) = Z^i(G) \in Z\left(G/Z^i(G)\right)$$

故　$x \in Z^{i+1}(G)$，即 $Z^i(G) \subset Z^{i+1}(G)$

因　$Z\left(G/Z^i(G)\right) \lhd G/Z^i(G)$，由同構之對應定理，知 $Z^{i+1}(G) \lhd G$

上述定義，可簡示之如下：

$$G \longrightarrow G/Z^i(G)$$

$$Z^{i+1}(G) \longrightarrow Z\left(G/Z^i(G)\right) = Z^{i+1}(G)/Z^i(G)$$

$$Z^i(G) \longrightarrow \{Z^i(G)\} = \{(G/Z^i(G)\text{之么元素})\}$$

定義 4．下列級數稱之爲升中心級數（Ascending central series）：

$$\{e\} = Z^0(G) \subset Z'(G) \subset Z^2(G) \subset \cdots\cdots\text{。}$$

爲方便計，可用 Z^i 表 $Z^i(G)$，γ_i 表 $\gamma_i(G)$

定理 1．設 G 爲任意一群。

(1) 若 $Z^m(G) = G$；則對於所有非負之整數 i 有 $\gamma_{i+1}(G) \subset Z^{m-i}(G)$

(2) 若且唯若 $r_{m+1}(G) = \{e\}$，則 $Z^m(G) = G$。於此 e 爲 G 之么元素。

證　(1) 設 $Z^m(G) = G$ 於 i 上可用歸納法證明 $\gamma_{i+1}(G) \subset Z^{m-i}$.

當 $i = 0$ 時，　$\gamma_1 = G$

故 $\gamma_1 \subset Z^m$

次設　　$\gamma_{i+1} \subset Z^{m-i}$

則　　$\gamma_{i+2} = (\gamma_{i+1}, G) \subset (Z^{m-i}, G)$

由　　$Z^{m-i-1} \lhd G$ 及 $Z^{m-i-1} \subset Z^{m-i}$，故 Z^{m-i}/Z^{m-i-1} 爲

商群，今　$Z^{m-i}/Z^{m-i-1} = Z\left(G/Z^{m-i-1}\right)$

即

$$Z^{m-i}/Z^{m-i-1} \subset Z\left(G/Z^{m-i-1}\right)$$

由引 2　$(Z^{m-i}, G) \subset Z^{m-i-1}$，再由 $\gamma_{i+2} \subset (Z^{m-i}, G)$

故　　$\gamma_{i+2} \subset Z^{m-i-1}$

即　　$\gamma_{i+2} \subset Z^{m-(i+1)}$

即對於 $i = 0, 1, 2, \cdots\cdots m$ 均有 $\gamma_{i+1} \subset Z^{m-i}$

(2) 由 $\gamma_{i+1} \subset Z^{m-i}$，令 $i=m$

得 $\gamma_{m+1} \subset Z^0 = \{e\}$

故 $\gamma_{m+1} = \{e\}$

反之，設 $\gamma_{m+1} = \{e\}$，於 j 上先用歸納法證明 $\gamma_{m+1-j} \subset Z^j$

$j=0$ 時，由 $\gamma_{m+1} = \{e\} = Z^0$

故 $\gamma_{m+1} \subset Z^0$

次者，設 $\gamma_{m+1-j} \subset Z^j$，先定一寫像如下：

$$f : G/\gamma_{m+1-j} \longrightarrow G/Z^j$$

$$f(g\gamma_{m+1-j}) = gZ^j$$

若 $g_1\gamma_{m+1-j} = g_2\gamma_{m+1-j}$，則

$g_1^{-1}g_2 \in \gamma_{m+1-j} \subset Z^j$

即 $g_1^{-1}g_2 \in Z^j$

故 $g_1Z^j = g_2Z^j$

即此寫像為完備且為映成寫像，又

$$\begin{aligned} f((g_1\gamma_{m+1-j})(g_2\gamma_{m+1-g})) &= f(g_1g_2\gamma_{m+1-j}) \\ &= g_1g_2Z^j \\ &= g_1Z^jg_2Z^j \\ &= f(g_1\gamma_{m+1-j})f(g_2\gamma_{m+1-j}) \end{aligned}$$

故 f 為 G/γ_{m+1-j} 映成 G/Z^i 之同態寫像

由 $\gamma_{m+1-j} = \gamma_{m-j+1} = (\gamma_{m-j}, G)$ 自然有

$(\gamma_{m-j}, G) \subset \gamma_{m-j+1}$

由引2得

$$\gamma_{m-j}/\gamma_{m-j+1} \subset Z(G/\gamma_{m-j+1})$$

今 f 為映成同態寫像，由引3，知 $f(\gamma_{m-j}/\gamma^{m+1-j}) \subset Z(G/Z^j)$

因 $f(\gamma_{m-j}/\gamma_{m+1-j}) = \{xZ^j \mid x \in \gamma_{m-j}\} = \gamma_{m-j}Z^j/Z^j$

故

$$\gamma_{m-j}Z^j/Z^j \subset Z(G/Z^j) = Z^{j+1}/Z^j$$

即 $Z^{j+1}/Z^j \supset \gamma_{m-j}Z^j/Z^j$

故 $Z^{j+1} \supset \gamma_{m-j}Z^j \supset \gamma_{m-j}$

故 $\gamma_{m-j} \subset Z^{j+1}$

$\gamma_{m+1-(j+1)} \subset Z^{j+1}$

因此對於所有 j （$j=0, 1, \cdots m$）均有

$$\gamma_{m+1-j} \subset Z^{j}$$

令　$j=m$，　得

$$\gamma_1 \subset Z^m$$

即　　$G \subset Z^m$

故　　$G = Z^m$

定義5　設G爲群，若有某正整數m使 $\gamma_m(G)=\{e\}$ 稱G爲冪零群，於此 e 爲G之么元素。

若G之降中心級數 $G=\gamma_1 \supset \gamma_2 \supset \cdots\cdots$ 趨於 $\{e\}$ 或G之升中心級數　$\{e\}=Z^0 \subset Z' \subset Z^2 \subset \cdots\cdots$ 趨於G，則G爲冪零群。

若G爲交換群，則 $\gamma_1=G$，$\gamma_2=(G, G)=\{e\}$，故G爲冪零群。

若G爲冪零群，可證明G爲可解群（Solvable group）用歸納法先證明G之高階換位子群（commutator subgroup）$G^{(i)}$ 有 $G^{(i)} \subset \gamma_i(G)$

設 $i=1$，　則

$$G^{(1)}=(G, G) \subset G=\gamma_1$$

∴　　$G^{(1)} \subset \gamma_1$

次設　　$G^{(i)} \subset \gamma_i$

則　　$G^{(i+1)}=\left(G^{(i)}, G^{(i)}\right) \subset (\gamma_i, G)=\gamma_{i+1}$

即　　$G^{(i+1)} \subset \gamma_{i+1}$

因G爲冪零群，故對於某正整數m有 $\gamma_m=\{e\}$

∴　　$G^{(m)} \subset \{e\}$

即　　$G^{(m)}=\{e\}$

故G爲可解群。

〔註〕於群G，若有 k 有 $G^{(k)}=\{e\}$ 時，則G爲可解群。

反之，並不一定爲眞，例如對稱群 S_3 爲可解群，然其並不爲冪零群，說明於次：

若G爲冪零性，其必有非顯明之核心，即 $Z(G) \neq \{e\}$，今設m爲使 $\gamma_{m+1}=\{e\}$ 之第一整數，則

$$\gamma_m \neq \{e\}$$

即　　$\{e\} \neq \gamma_m \subset Z'$　（於 $\gamma_{m+1} \subset Z^{m-i}$，令 $m=i+1$）

故　　$Z'=Z(G) \neq \{e\}$

於 S_3 中，$Z(S_3)=\{e\}$，故 S_3 不爲冪零群。

定理2　冪零群之子群爲冪零群。

證　設G爲冪零群，H爲G之子群，則對於每一正整數 i 均有

$$\gamma_i(H) \subset \gamma_i(G)$$

因G爲冪零群，故有某正整數m使

$$\gamma_m(G)=\{e\} \quad (e\text{爲G之么元素})$$

由　　$\gamma_m(H) \subset \gamma_m(G)$

故必　　$\gamma_m(H)=\{e\}$

即H爲冪零群。

定理 3　設G爲冪零群及$H \triangleleft G$，則 G/H 爲冪零群。

證　設　$f: G \longrightarrow L$

爲群G映成群L之同態寫像，於 i 上可用歸納法證明

$$\gamma_i(L) \subset f(\gamma_i(G))$$

$i=1$時，　$f(\gamma_1(G)) = f(G) = L \supset \gamma_1(L) = L$

故　$\gamma_1(L) \subset f(\gamma_1(G))$

次設　$\gamma_i(L) \subset f(\gamma_i(G))$，則

$$\begin{aligned}\gamma_{i+1}(L) &= (\gamma_i(L), L) \subset (f(\gamma_i(G)), L) \\ &= (f(\gamma_i(G)), f(G)) \subset f(\gamma_i(G), G) \\ &= f(\gamma_{i+1}(G))\end{aligned}$$

即　$\gamma_{i+1}(L) \subset f(\gamma_{i+1}(G))$

今設自然映成同態之寫像爲

$$\phi: G \longrightarrow G/H$$

則　$\gamma_i(G/H) \subset \phi(\gamma_i(G))$

因G爲冪零群故有某m使 $r_m(G) = \{e\}$

由　$\gamma_m(G/H) \subset \phi(\gamma_m(G))$

故　$\gamma_m(G/H) \subset \phi(\{e\}) = \{H\}$

即　$\gamma_m(G/H) = \{H\}$

故　G/H 爲冪零群

今已證明冪零群之子群爲冪零群，及若G爲冪零群，$H \triangleleft G$時，則 G/H 亦爲冪零群。然若$H \triangleleft G$及H，G/H 均爲冪零群時，則G不一定爲冪零群，例如A_3 及 S_3/A_3 均爲亞伯群，故A_3 及 S_3/A_3 均爲冪零群，但S_3不爲冪零群。

定理 4　設G爲有限個冪零群之直積，則G爲冪零群

證　設H，K爲二冪零群，用歸納法先證明

$$\gamma_i(H \times K) \subset \gamma_i(H) \times \gamma_i(K)$$

$i=1$，　$\gamma_1(H \times K) = H \times K = \gamma_1(H) \times \gamma_1(K)$

$\therefore$　$\gamma_1(H \times K) \subset \gamma_1(H) \times \gamma_1(K)$

次設　$\gamma_i(H \times K) \subset \gamma_i(H) \times \gamma_i(K)$，則

$$\begin{aligned}\gamma_{i+1}(H \times K) &= (\gamma_i(H \times K), H \times K) \\ &\subset (\gamma_i(H) \times \gamma_i(K), H \times K)\end{aligned}$$

可證明　$(\gamma_i(H) \times \gamma_i(K), H \times K) \subset \gamma_{i+1}(H) \times \gamma_{i+1}(K)$　如下

設　$x \in (\gamma_i(H) \times \gamma_i(K), H \times K)$　爲簡便計，令

$$x = (a, b)^{-1}(c, d)^{-1}(a, b)(c, d)$$

$$= (a^{-1}c^{-1}ac ,\ b^{-1}d^{-1}bd)$$

於此　$a\in\gamma_i(H)$，　$b\in\gamma_i(K)$，　$c\in H$，　$d\in K$

故　$x\in(\gamma_i(H),H)\times(\gamma_i(K),K)=\gamma_{i+1}(H)\times\gamma_{i+1}(K)$

故　$(\gamma_i(H)\times\gamma_i(K),H\times K)\subset\gamma_{i+1}(H)\times\gamma_{i+1}(K)$

由此得

$$\gamma_{i+1}(H\times K)\subset\gamma_{i+1}(H)\times\gamma_{i+1}(K)$$

故對於一切正整數 i 均有

$$\gamma_i(H\times K)\subset\gamma_i(H)\times\gamma_i(K)$$

因H，K均爲冪零群，是以對於某m_1，m_2有

$$\gamma_{m_1}(H)=\{e_H\}$$
$$\gamma_{m_2}(K)=\{e_K\}$$

於此e_H，e_K分別表H及K之么元素

令　　$m=\max\{m_1,m_2\}$，則

$$\gamma_m(H)=\{e_H\}$$
$$\gamma_m(K)=\{e_K\}$$
$$\gamma_m(H\times K)\subset\{(e_H,e_K)\}$$
$$\gamma_m(H\times K)=\{\text{么元素}\}$$

故H×K爲冪零群。

於一般，可用歸納法證明有限個冪零群之直積仍爲冪零群。

引4　設P是質數，每一有限P群均爲冪零群。

證　設G爲一有限P群，若G只含有一元素，G當然爲冪零群，今設G中元素之個數多於一，則

$$Z(G)\neq\{e\}\qquad(e\text{爲么元素})$$

即　$Z'(G)\neq\{e\}$

故　$Z^2(G)\neq\{e\}$　　(因$Z'\subset Z^2$)

由升中心級數

$$Z^0\subset Z'\subset Z^2\subset\cdots\cdots$$

觀之，若某 i 使$Z^i\neq G$　則

$$Z_{i+1}\quad Z^i\text{及}Z^{i+1}\neq Z^i$$

因G爲有限群，不能對所有 i 均有此不等式，故必有某 i 使$Z^i=G$故G爲冪零群。

引5　設H爲群G之子群，設

$$N=N_G(H)$$
$$=\{x\in G\mid xH=Hx\}$$

則N爲使(H，N)⊂H之最大子群

證　設M爲G之子群，並設H⊂M及(H，M)⊂H

由引1，H◁M，故對於每m∈M有

$$mH=Hm$$

∴　　$m\in N$

故　　$M\subset N$

引6　設P為有限群G之P－sylow 子群，H 為G之子群，且$N_G(P)\subset H\subset G$，則 $N_G(H)=H$ 於此"(⊂)"不一定為「真含於」。

證　設　$x\in N_G(H)$　則

$xH=Hx$

即　$xHx^{-1}=H$

因　$P\subset N_G(P)\subset H$

∴　$P\subset H$

是　$xPx^{-1}\subset H$

因P與xPx^{-1}均含於H中，均為H之P－sylow子群，故必共軛，故有$h\in H$

使　$hPh^{-1}=xPx^{-1}$

∴　$P=h^{-1}\chi P\chi^{-1}h=h^{-1}xP(h^{-1}x)^{-1}$

$h^{-1}x\in N_G(P)\subset H$

故　$x\in H$

即　$N_G(H)\subset H$

但　$H\subset N_G(H)$

故　$H=N_G(H)$

定理5　設G為有限群，若且僅若G為其諸Sylow子群之直積時，則G為冪零群。

證　設　$G=P_1\times P_2\times\cdots\cdots\times P_K$

為諸sylow子群之直積，故每一P_i $(i=1,2,\cdots\cdots k)$均為某P群由引4，知P_i為冪零群，再由定理4，知G為冪零群。

反之，設G為冪零群，並設H為G之真子群，$N=N_G(H)$，首先證明$H\neq N$

因H為G之真子群，則必有某i使

$H\supset\gamma_{i+1}$

$H\not\supset\gamma_i$

例如　$\gamma_1=G$　$H\not\supset G$

今　$(\gamma_i,H)\subset(\gamma_i,G)=\gamma_{i+1}\subset H$

即　$(\gamma_i,H)\subset H$

因　$(H,\gamma_i)=(\gamma_i,H)$

故　$(H,\gamma_i)\subset H$

由引5，　$\gamma_i\subset N$

由　$H\not\supset\gamma_i$ 及 $\gamma_i\subset N$

故　$H\neq N$

次者，設P為G之任意一P－sylow 子群，令

$N_1=N_G(P)$　故有

$N_G(P)\subset N_1\subset G$

由引6，知 $N_G(N_1)=N_1$

由前段之敍述，若N_1為G之真子群，則必

$N_G(N_1)\neq N_1$

故N_1不為G之真子群，又以$P\subset N_G(P)=N$，故$N_1\neq\{e\}$

是以　$N_1=G$

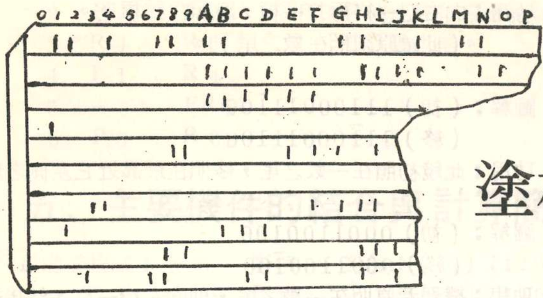
由　　　　$P \lhd N_G(P) = N_1$

故　　　　$P \lhd N_1$

即　　　　$P \lhd G$

由此知G之每一 sylow子群均爲G之正規子群，故G爲此等 sylow子群之直積

〔註〕設G爲有限群，若G之每一 sylow子群P_i有$P_i \lhd G$時，則G爲此等P_i之直積。



簡 塗林計算機 介

助教▲張晶

一、沿革與功用

塗林氏（Turing）1936 年所造的計算機（Machine ）。以此機器來計算所有的遞迴函數（Recursive Functions）又根據Church Thesis 所有有效可計算的函數均爲遞迴函數。（All effectively calculable functions are recursive functions.）。則此機器可計算所有有效可計算的函數。

二、構造

㈠向兩方向無限延伸之紙帶 . 紙帶分成間格相等的空格。

㈡可以認識簡單符號的玻鏡。此鏡恒照在紙帶的格子上。它可以沿紙帶左右移動或不動，每次只移一格。

㈢儲備無窮多個單元機件，多數的雷同，而不同的只有幾種。每一個單元當與玻鏡連絡時被稱爲活躍狀態。它能因玻鏡所照格子上所顯的形像而有不同之行動。

三、行動

㈠加印一豎槓，或擦掉。（如已有一槓，再加一槓視爲重合）。或不印也不擦。

㈡左，右或不動。（每次只移一格）

在㈠㈡兩動作完畢後，此單元自動打斷與玻鏡的連絡而進入「靜止狀態」。此後須看使用者要用什麽單元進入「活躍狀態」接替工作下去。

程式中以P（Print）	表示「印」	圖示中 0011$\bar{1}$000	以三槓表數「2」
E（Erase）	表示「擦」		以n+1槓表數「n」
R（Right）	表示「右移一格」		以0表空白時的空格
L（Left）	表示「左移一格」		以－表鏡照的格子
O	表示結束	稱 0011$\bar{1}$00 爲鏡照在一數（2）之尾。	

四、九個主要機件

㈠引：程式：

程式	空白	豎槓
1	—	R 2
2	RP 3	—
3	0	—

圖解：（初）$111\bar{1}00$

（終）$11110\bar{1}$

功用：向右空一格再打一槓，鏡照在該槓上。

（此鏡原須照在數之尾）。

㈡退：程式：

程式	空白	豎槓
1	L 2	L 1
2	L 2	0

圖解：（初）$1110001\bar{1}00$

（終）$11\bar{1}00011100$

功用：此鏡初照在一數之尾，終照在最靠近它左側之數之尾。

㈢試：程式：

程式	空白	豎槓
1	—	L 2
2	R 3	R 4

圖解：（初）$0001100\bar{1}00$

（終）$0001100\bar{1}00$

功用：機器若原照在一數之尾，則向左行一格，然後返回照在原數之尾，視左邊一格之爲空白或豎槓而令不同單元3或單元4進入活躍狀態。

㈣減：程式：

程式	空白	豎槓
1	—	ELO

圖解：（初）$00111\bar{1}0$

（終）$0011\bar{1}00$

功用：鏡初照在一數（n）之尾，現照在該數減一（n—1）之尾。

㈤進：程式：

程式	空白	豎槓
1	—	R 2
2	R 2	R 3
3	LO	R 3

圖解：（初）$11\bar{1}001100$

（終）$111001\bar{1}00$

功用：爲㈡退之相反。

㈥加：程式：

程式	空白	豎槓
1	P 0	R 1

圖解：（初）$0011\bar{1}00$

（終）$00111\bar{1}0$

功用：爲㈣進之相反。

㈦補：程式：

程式	空白	豎槓
1	—	R 2
2	PR 2	L 3
3	-	ELO

圖解：（初）$1\bar{1}0001110$

（終）$111\bar{1}01110$

功用：鏡初照在一數之尾，終將此數與右邊下一數之間空白補加豎槓，最後只剩下一個空白，介乎兩數之間，鏡再退回原數加n豎槓之尾。

㈧擦：程式：

程式	空白	豎槓
1	L 2	L 1
2	3	4
3	R 3	R 5
4	L 2	EL 4
5	L 0	R 5

圖解（初）$10010110111\bar{1}0$

（終）$10000000111\bar{1}0$

功用：鏡初照在一數之尾，終將該數與左邊有連續兩空白之間的數全部擦去。再退回原數之尾。

(九)緊：程式：

	空白	豎槓
1	—	EL2
2	PL3	L2
3	R4	R5
4	L1	R4
5	—	ER6
6	P0	R6

圖解：（初）$110000111\bar{1}0$

（終）$11011\bar{1}0000$

功用：終使此數和左邊最近一數之間只有一個空白。而仍照在該數之尾。

五、主要機件的結合與計算簡單初級遞迴函數

(一)進^3 進進進程式：

	空白	豎槓
1	—	R2
2	R2	R3
3	L4	R3
4	—	R5
5	R5	R6
6	L7	R6
7	—	R8
8	R8	R9
9	L0	R9

圖解：（初）$11\bar{1}00110101110$

（終）$1110011010111\bar{1}0$

功用：（略）如上圖。

(二)抄$_n$　引退^{n}試　補進^n。　（若為空白）

　　　　　　　　減進^n $\dot{加}$　（若為豎槓）

功用：把照在該數之尾的前面第 n 個數抄在後面而照在此數之尾。

註：退^{n}及$\dot{加}$上面之點表示循環的做。

(三)（抄$_n$）^{n}　功用：把前 n 個數依次抄在後。

(四)（特抄）$_m$ ＝加（抄$_m$）減退^{m}減進^{m}減。

功用：空二格再抄一組 m 個數。

(五)加函數：$\varphi(X)=X+1$

則算 φ ＝抄$_1$加。

(六)投影函數：$\varphi(X_1,\cdots\cdots,X_n)=X_i \quad 1\leq i\leq n$

則算 φ ＝抄$_{n-i+1}$。

(七)常函數：$\varphi(X_1,\cdots\cdots,X_n)=P$　P為常數

則算 φ ＝引加^P。

(八)$\varphi(X_1,\cdots\cdots X_n)=\Psi(X_1(X_1,\cdots\cdots,X_n),\cdots\cdots,X_r(X_1,\cdots\cdots X_n))$

在此 Ψ 及 $X_1,\cdots\cdots,X_r$ 均為已知函數

則算 φ ＝（特抄）$_n$ 算 X_1（抄$_{n+1}$）^{n} 算 X_2（抄$_{n+1}$）^{n} ……算 X_r 抄$_{(r-1)(n+1)+1}$ 抄$_{(r-2)(n+1)+2}$ ……抄$_r$ 算 ψ 緊擦。（在此 ψ，X_1，……，X_r 皆已製好的計劃）

(九)設 $\Psi(X_1,\cdots\cdots,X_n)$ 之定義為

$\varphi(0,X_2,\cdots\cdots,X_n)=\psi(X_2,\cdots\cdots,X_n)$

$\varphi(Y+1,X_2,\cdots\cdots,X_n)=X(Y,\varphi(Y,X_2,\cdots\cdots X_n),X_2,\cdots\cdots,X_n)$

在此 X，ψ 為已知函數。

則算φ =（特抄$)_n$　算Ψ抄n+1試　$\begin{matrix}\text{抄}_2\text{擦緊。} \\ \text{引抄}_2(\text{抄}_{n+3})^{n-1}\end{matrix}$ 算X抄$_{n+3}$減試　$\begin{matrix}\text{抄}_2\text{擦緊。} \\ \text{抄}_{n+3}\text{加。}\end{matrix}$

在此算Ψ算X皆已製好之計算，當n=1時Ψ表一常數。

(十)設$\varphi(x_1,\cdots\cdots,x_n)$之定義爲

$\varphi(x_1,\cdots\cdots,x_n)=\mu y\,[X(x_1,\cdots\cdots,x_n,y)=0]$。

卽函數$\varphi(x_1,\cdots\cdots,x_n)$之值使$X(x_1,\cdots\cdots x_n,Y)=0$之最小之y。在此X爲一已知函數，且對於任一組n個數$x_1,\cdots\cdots,x_n$皆至少有一個y存在合於$X(x_1,\cdots x_n,y)=0$

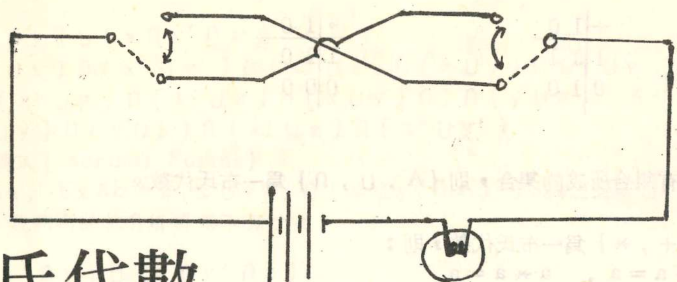
則算φ =（特抄$)_n$　引算X試　$\begin{matrix}\text{抄}_2\text{擦緊。} \\ (\text{抄}_{n+2})^{n+1}\text{加}\end{matrix}$

六、參考資料

(一)劉世超教授61年11月11日至12月2日每週在中研院之專題演講。

(二)S.C.Kleene：Introduction to Mathematics 1952.

(三)S.C.Kleene：General Recursive functions of Natual numbers 1936.



布氏代數與交換電路

·數三甲·
═王正宗═

近廿年來，科學上有三大成就(1)物理的研究導致原子彈的發明而結束了第二次世界大戰。(2)通貨膨脹的研究解決了經濟危機。(3)數學的應用導出了電子計算機，其中以電子計算機（或稱電腦），使人類完成了從前以為不可能的事——登陸月球。布氏代數其應用為交換電路。交換電路為計算機的基本設計原理，故布氏代數實為學習計算機邏輯設計的不二法門。本文僅就布氏代數的基本性質及簡單交換電路應用加以介紹。

{布氏代數}〔Boolean Algebras〕

定義1：

集合B＝{a，b，c……}，若{B，+，×}滿足下列六個條件，則B稱為布氏代數（詳細點則稱{B＋·}為一布氏代數）。

①封閉性：

$a, b \in B \quad a+b \in B, \ a \times b \in B$。

②交換律：

$a, b \in B \quad a+b=b+a, \ a \cdot b=b \cdot a$。

③結合律：

$a, b, c \in B \quad (a+b)+c=a+(b+c),$
$(a \cdot b) \cdot c=a \cdot (b \cdot c)$

④分配律：

$a \cdot b \cdot c \in B \quad a+(b \cdot c)=(a+b) \cdot (a+c)$
$a \cdot (b+c)=(a \cdot b)+(a \cdot c)$

⑤單位元素：

$\exists\, 0, 1 \ni, \forall a \in B \quad a+0=a, \ a \cdot 1=a$

⑥補元律：

$\forall a \in B, \quad \exists\, a' \ni a+a'=1, \quad a \cdot a'=0$

以上＋，∘，1，0分別以∪，∩，$\mho$（宇集合），ϕ之眼光看待極為方便。

〔Ex 1〕

B＝{1，0}，+，·定義如下，則B或{B，+，·}為一布氏代數。

+	1	0
1	1	1
0	1	0

·	1	0
1	1	0
0	0	0

〔Ex 2〕

A爲所有集合所成的集合，則 $\{A, \cup, \cap\}$ 爲一布氏代數。

〔性質1〕

$\{B, +, *\}$ 爲一布氏代數，則：

(i) $a+a=a$, $a*a=a$

(ii) $a+1=1$, $a*0=0$

(iii) $(a')'=a$

(IV) $1'=0$, $0'=1$

(V) $(a+b)'=a'\cdot b'$, $(a\cdot b)'=a'+b'$。此二項卽爲狄摩根定律。

定義2：

布氏代數的對偶：一敍述的對偶敍述卽爲將原敍述的＋，∗互換，1及0互換，例如 $(1+a)\cdot(b+0)=b$，其對偶敍述卽爲 $(0\cdot a)+(b\cdot 1)=b$

對偶原理：在布氏代數中的任何定理，其對偶命題仍爲眞。

布氏函數：

§(二)，布氏函數（Boolean functions）

布氏代數 $B=\{a, b, c, \ldots\ldots\}$，$a'\cup(b\cap c)$，若改用＋，，，・，則爲 $a'+b\cdot c$，如此很自然的我們可以視 a' 及 $b\cdot c$ 爲單項，而 $a'+b\cdot c$ 爲多項。

定義3：

任何敍述 $x\cup x'$，$a\cap b$，$[a\cap(b\cup c')]\cup(a'\cap b'\cap c)$，包含有限個B中之元素，而以∪，∩結合起來的，我們則稱爲Boolean function，而在Boolean function之變數個數卽爲出現在敍述中不同字母的個數。（註：a a′視爲同一變數）。

〔Ex 3〕

$x\cup x'$ 是單一變數的Boolean function.

〔Ex 4〕

$a\cap b'$ 爲二變數的Boolean function.

〔性質2〕

在一般代數中任一個integral function of several variables，常可用多項式（包含0）表示出。但不經常的可以用若干個linear factor的乘積（product）表示出，然而在Boolean Algebra中却兩者皆可用，也就是任何一Boolean function可用下列兩種表示出：

① a union of distinct intersections.

② an intersection of distinct unions.

〔Ex 5a〕

$$[(x\cup y')\cap(x\cap y'\cap z)']'=(x\cup y')'\cup[(x\cap y'\cap z)']'$$
$$=(x'\cap y)\cup(x\cap y'\cap z)$$

〔Ex 5b〕

$$[(x\cup y')\cap(x\cap y'\cap z)']'$$

$= (x' \cap y) \cup (x \cap y' \cap z)$

$= (x' \cup x) \cap (x' \cup y') \cap (x' \cup z) \cap (x \cup y) \cap (y \cup y') \cap (y \cup z)$

$= 1 \cap (x' \cup y') \cap (x' \cup z) \cap (x \cup y) \cap 1 \cap (y \cup z)$

$= (x \cup y) \cap (y \cup z) \cap (x' \cup z) \cap (x' \cup y')$

§(三)：模式 (Normal Forms)

在Ex 5a， Ex 5b中$[(x \cup y') \cap (x \cap y' \cap z)']'$為三變數的Boolean function，我們再將其分析可得下列二式：

① $(x' \cap y) \cup (x \cap y' \cap z)$

$= (x' \cap y \cap 1) \cup (x \cap y' \cap z) = [(x' \cap y) \cap (z \cup z')]$
$\cup (x \cap y' \cap z)$

$= (x' \cap y \cap z) \cup (x' \cap y \cap z') \cup (x \cap y' \cap z)$

② $(x \cup y) \cap (y \cup z) \cap (x' \cup z) \cap (x' \cup y')$

$= [(x \cup y) \cup (z \cap z')] \cap [(y \cup z) \cup (x \cap x')]$
$\cap [(x' \cup z) \cup (y \cap y')] \cap [(x' \cup y') \cup (z \cap z')]$

$= (x \cup y \cup z) \cap (x \cup y \cup z') \cap (x' \cup y \cup z) \cap$
$(x' \cup y' \cup z) \cap (x' \cup y' \cup z')$

在第一式裡我們發現每項均有三個變數，在第二式裡每一聯集裡亦含三變數，這裡我們要注意的是任一含n變數的Boolean function皆可以用性質2的兩種表示法表示出，且各項或(每一聯集)皆含n變數，如此第一式我們稱之Candnicol form 或disjunctive normal form ，第二式稱：dual canonical form或 conjunctive normal form. (Not dual of canonical form)。含n變數之Boolean function其canonical form至少含 2^n 項 (若含 2^n 項則稱complete canonical form)。其dual canonical form亦至多有 2^n 個distinct factors，若含 2^n 個稱complete dual canonical form.

Theorem 1 :

Complete canonical form其值為1

Theorem 2:

Complete dual canonical form其值為0。

Theorem 3:

dual canonical form is the dual of complement of canonical form.

§(四)：布氏函數形式的轉換 (changing the form of a Boolean function).

F (x , y , z ……) 表Boolean function ，因計算機邏輯只含二元素 1 及 0 (關及閉)，故我們在此僅討論$B = \{0, 1\}$ 含二元素的Booleam algebra，首先討論如何從一眞值表裡寫出F (x , y , z ……)

〔Ex 6〕　眞值表如下。〔Table1, 1〕

x	y	z	F(x, y, z)
1	1	1	1
1	1	0	0
1	0	1	1
0	1	1	0
1	0	0	0
0	1	0	0
0	0	1	1
0	0	0	1

則$F(x,y,z)$之canonical form為在complete canonical form中值為1的所有項，其dual canonical form即為在Complete dual canonical form中，值為0的所有項(但寫出時各元素須a與a′互換，∩與∪互換)。

〔Canonical form〕

$$F(x,y,z)=(x\cap y\cap z)\cup(x\cap y'\cap z)\cup(x'\cap y'\cap z)\cup(x'\cap y'\cap z')$$
$$=(x\cap z)\cup(x'\cap y')$$

〔dual canonical form〕

$$F(x,y,z)=(x'\cup y'\cup z)\cap(x\cup y'\cup z')\cap(x'\cup y\cup z)\cap(x\cup y'\cup z)=(x'\cup z)\cap(x\cup y')$$

〔Ex 7〕 Find the dual canonical form for

$$F=(x\cap y\cap z')\cup(x\cap y'\cap z')\cup(x\cap y'\cap z')\cup(x'\cap y\cap z)\cup(x'\cap y'\cap z')$$

Since $F'=(x\cap y\cap z)\cup(x'\cap y'\cap z)\cup(x'\cap y\cap z')$

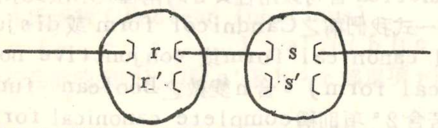
So that gain: $F=(F')'=(x'\cup y'\cup z')\cap(x\cup y\cup z')\cap(x\cup y'\cup z)$

§(五)：布氏交換電路(Algebra of Electrical Networks)

在Boolean algebra, $B=\{0,1\}$中電路網的代數式是一很有趣且在近廿年來廣泛的被運用在計算機中。Boolean algebra中之∪，∩在交換電路中分別為並聯與串聯。

〔Ex 8a〕(r，s兩開關)

〔串聯〕——r——s——



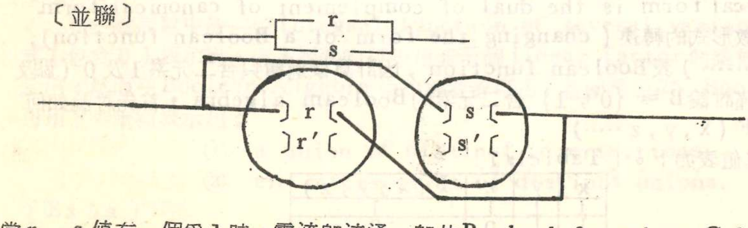
當r及s值為1時，電流方可流通，即其Boolean function $F(r,s)=1$。

r	s	F(r,s)
1	1	1
1	0	0
0	1	0
0	0	0

$F(r,s)=r\cap s$

〔Ex 8b〕

〔並聯〕



當r，s值有一個為1時，電流即流通，即其Booleal function. $G(r,s)=1$

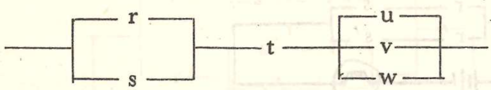
r	s	G(r, s)
1	1	1
1	0	1
0	1	1
0	0	0

$G(r, s) = r \cup s$

or $G(r, s) = (r \cap s) \cup (r \cap s') \cup (r' \cap s)$

〔Ex 9〕

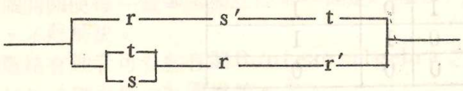
寫出下列交換電路的Boolean function（不必寫成canonical form）



Ans：$F(r, s, t, u) = (r \cup s) \cap t \cap (u \cup v \cup w)$

〔Ex 10〕

寫出下面交換電路的Boolean function及眞值表：



Ans：$F(r,s,t) = (r \cap s' \cap t) \cup [(t \cup s)] \cap r'$

r	s	t	$r \cap s' \cap t$	$(r \cup s) \cap r'$	F(r s t)
1	1	1	0	0	0
1	1	0	0	0	0
1	0	1	1	0	1
0	1	1	0	1	1
1	0	0	0	0	0
0	1	0	0	1	1
0	0	1	0	1	1
0	0	0	0	0	0

§㈥ 後述

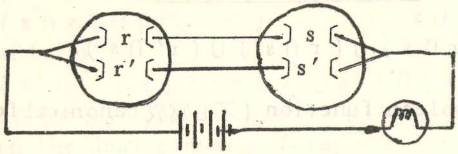
隨著科學的發達，商業也繁榮起來了，百貨公司大廈一間間的蓋了起來，晚間大量的男男女女湧進了百貨公司，五花八門的電子自動遊樂場所如雨後春筍的在百貨公司裡做起生意了，其基本原理全在布氏代數之交換電路應用，現就提出幾個有趣的實例供大家欣賞：

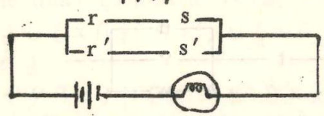
〔Ex 11〕

今有一樓梯中間置一電燈，如何設計電路使在樓上或樓下皆可控制此電燈，（此相同於如何設計自動電梯使在兩端皆可控制其開或關）

Ans：爲此，吾人先考慮兩變數的眞相，設法使下值爲r，s值相同時爲1，不同時爲0，就是$F = (r \cap s) \cup (r' \cap s')$。

r	s	F (r , s)
1	1	1
1	0	0
0	1	0
0	0	1

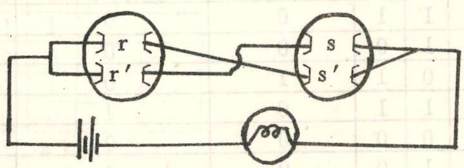




相同的亦可設計：F (r , s) = (r ∩ s′) ∪ (r′ ∩ s)，亦卽當 r s 値不同時 F (r,s) 爲1。

r	s	F (r , s)
1	1	0
1	0	1
0	1	1
0	0	0

r　　　s′
r′　　　s



〔Ex　12〕：有一間車房置一電燈，車房兩房有兩間臥室，試設計如何在每間房子設置一個開關，可分別控制車房的電燈。

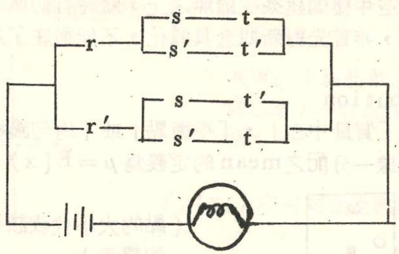
設計一Boolean function, F或G卽可，同學可自行試驗。

r	s	t	F (x y z)	G (x y z)
1	1	1	1	0
1	1	0	0	1
1	0	1	0	1
0	1	1	0	1
1	0	0	1	0
0	1	0	1	0
0	0	1	1	0
0	0	0	0	1

$$G(xyz) = (r\cap s\cap t') \cup (r\cap s'\cap t) \cup (r'\cap s\cap t) \cup (r'\cap s'\cap t')$$

$$F(xyz) = (r\cap s\cap t) \cup (r\cap s'\cap t') \cup (r'\cap s\cap t') \cup (r'\cap s'\cap t)$$
$$= \{r\cap[(s\cap t)\cup(s'\cap t')]\} \cup \{r'\cap[(s\cap t')\cup(s'\cap t)]\}$$

Consider : $F(xyz) = \{r\cap[(s\cap t)\cup(s'\cap t')]\} \cup \{r'\cap[(s\cap t')\cup(s'\cap t)]\}$



〔Ex　13〕

如何設置4個開關使每一個都能獨立控制一固定的電燈，n個開關時又如何？有趣者可就其眞值思考之，不難解決。

對有關交換電路有趣者可看些有關Boolean algebra之應用方面的書，市面上也有這方面的譯本如布林氏代數與數位計算機等。

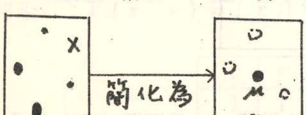
機率與統計
機個最基本之圖解

－數四乙－
～師岱濤～

我覺得Hogg那本Introduction to Mathematical Statics某些地方寫得的確簡單流暢，讀來膾炙人口，令人有勢如破竹，一瀉千里不可收拾之感，但往往由於這些地方過份「快速」閱讀反而導致所學只重表面記憶却忽略了所代表之某些事項眞實意義——這也是我們學數學的常犯的毛病（空中樓閣建築在虛無之上，隨時有幻滅的可能）；有幾個非常基本而極其重要的觀念及性質，非首先對新觀念具體化，不能徹底了解機率與統計之眞實內涵：

①Mean of a distribution

一個分配的mean可視爲「質量中心」，「平衡點」或「均勻濃縮點」。下圖中圖(1)表一隨機變數X之分配情況，根據一分配之mean的定義爲 $\mu = E(x)$，作圖(2)



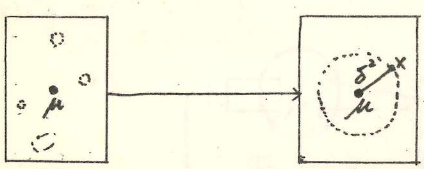
(1)　　(2)

（點的大小代表該點所分配到之頻率——即機率）

(1)圖中點×之位置及大小分佈得並不均勻，不方便觀察，故取一具有代表性之一點 μ（即mean）作爲(1)圖之初步代表，如圖(2)所示。

②Variance of a distribution

根據一分配之variance的定義 $\delta^2 = Var(x) = E(x-\mu)^2$，卽方差平均值，作圖(3)：



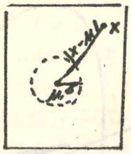
(2)　　(3)

圖(3)可視爲各點x距 μ 之平方差均爲 δ^2（當然是假想的）。如此合①②兩項，mean及variance便構成一分配（資料）之兩個基本代表量。圖(3)卽代表圖(1)之大約內涵（統計學應爲一「大約」之學），不但表明了(1)圖之「中心」位置及大小，且更說明了各實際點x距 μ 之方差平均值（卽此一分配之分散情況）。

③Chebyshev's inequality

此不等式說：$Pr(|x-\mu| \geqq k\delta) \leqq \frac{1}{k^2}$　（條件簡略）

我認爲如將其改寫爲 $Pr\left(\frac{|x-\mu|}{\delta} \geqq k\right) \leqq \frac{1}{k^2}$ 較爲具體易懂，易記，其謂：任何一點x與 μ 之差的絕對值與 δ 之比大于或等於k之機率恒小于或等于 $\frac{1}{k^2}$。

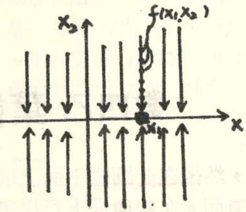


（有些書上稱 $\dfrac{x-\mu}{\delta}$ 爲 Z－score）

④ Marginal p.d.f.

設 $f(x_1,x_2)$ 爲隨機變數 x_1 與 x_2 之聯合 p.d.f.

則 $f_1(x_1)=\int_{-\infty}^{\infty} f(x_1,x_2)\,dx_2$ （or $f_1(x_1)=\sum\limits_{x_2^a} f(x_1,x_2)$）稱爲 x_1 之 marginal p.d.f. ，以離散型圖解之：

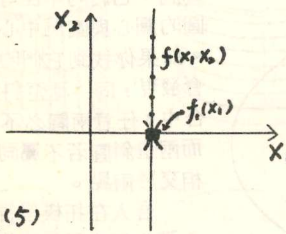


其實此爲極簡單之微積分結果，但我們往往不假思索，一昧記憶公式而忽略了了解其眞實內涵。

$f_2(x_2)$ 亦可同樣定義繪圖。

⑤ Conditional p.d.f.

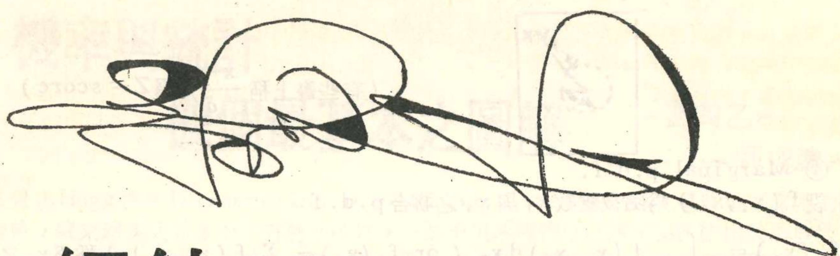
條件同④，則 $f(x_2|x_1)=\dfrac{f(x_1,x_2)}{f_1(x_1)}$ 稱爲 x_1 與 x_2 在 $x_1=x_1$ 時之 Conditional p.d.f. ：



由此圖即很容易了解 $\dfrac{f(x_1,x_2)}{f_1(x_1)}$ 之眞實代表意義了。

$f(x_1|x_2)$ 亦可同樣定義繪圖。

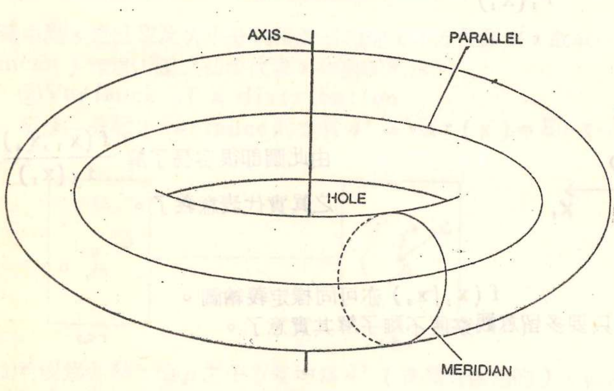
以上所舉的爲極簡單之例子，只要多留意觀察便不難了解其實意了。



繩結的數學

數四乙 葉樹華

輪環面是一種狀似油煎圈餅的曲面，我們可以任取一圓，然後在此圓的平面上取一與圓不相交的直線，以此直線為軸，將圓繞此軸轉一周，即得輪環面。在輪環面上可以畫一些圓：有的稱之為經線（meridians），有的稱為緯線（parallels）〔如圖一〕。經線和緯線的數目皆為無限。除此之外，輪環面上還有兩種歪斜的圓。它們的半徑等於經線圓的圓心與圓洞中心的距離。如果你找到它們的話，你會發現，同一種歪斜圓的集合中，任意兩圓必不相交，而兩歪斜圓若不屬同類，則相交於兩點。



The torus

圖 一

吾人在拓樸學裡，只關心那些經由彈性變形後依然保持的性質。這種變形是假設物質有很好的彈性，可以任意伸張或壓縮而不至於斷裂。所以從拓樸的眼光來看，單孔的鈕扣、咖啡杯、橡皮圈、有一個把手的球，有一個洞穿過中間的立方體等都被視為同等。因為我們可以把這些曲面想成可以任意壓縮或伸展的薄膜，而它們經過壓縮或伸展後，都可變成完整的輪環面。以下，我們就以輪環面表示一切與它同等的曲面。

如果已知兩個曲面同等，那麼在三度空間中，有沒有辦法使其中一種經過彈性變形而變成另外一種呢？事實上，這常無法辦到，在三度空間中，möbius帶分左手式和右手式兩種。我們無法把一個左手式的möbius帶扭成右手式的，雖然它們的拓樸性質完全相等。左右手性並不是一種內在性質（intrinsic property），möbius帶只有嵌在三度空間中才

顯出這種性質。四度空間的人可以將我們手上的左手式 möbius 帶取去，扭轉之後再丢回來，變成了一個右手式的möbius 帶。

封閉曲線上的結也有這種二分法，在一條繩上打一個結，然後將繩的兩端聯接起來，每種結都有兩種打法，一種稱爲左手式的，一種稱爲右手式的。不管你怎樣播弄這根繩子，你永遠也無法將左手式的結變成右手式的結。繩結不是內在性質，更何況左右手性。四度空間的人可以將我們手上一條未打結的繩環取去，扭弄一下，再丢給我們。我們所接到的繩環很可能是打了左手式或是右手式的繩結。對四度空間的人而言，繩子打不打結都一樣，繩結的所有性質都是因爲嵌在三度空間中顯出來的附加性質（extrinsic property）

如果已知兩個曲面在拓樸上完全同等，如何判斷它們可以經由彈性變形而互變常是非常困難。在輪胎面上挖一個洞，能不能把輪胎的內面翻出來而形成一個相同的輪胎呢？答案是可以。只是一個橡皮製的輪胎無法做到，但一個羊毛製的則可以很輕易的翻過來。你可以取一塊方布，對折之後，將相反的兩個邊緣縫合而形成一個管狀物，然後把管狀物的兩端縫合而形成一個輪環面。做成後把它壓平，它的形狀是一個方形。在外面切一個口〔見圖二〕，然後你可以把它翻過來，一個布製的輪環面被翻過來之後，它的形狀完全與原來一樣，只是原來的經線變成了緯線，原來的緯線變成了經線。爲了便於看見這種轉變，可在原來的模型上，用有顏色的線綉上經線和緯線。

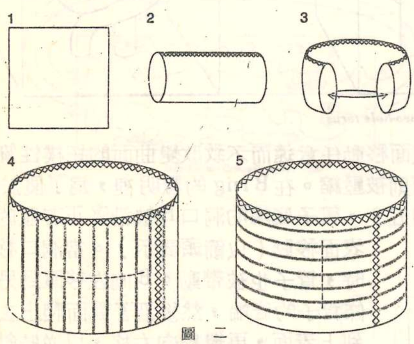


圖 二

Reversible cloth torus

現在我們要進入稍微複雜的情況。我們可以把打了結的繩環想成打了結的輪環面。在三度空間中，若不考慮在右性，這種打了結的輪環面只有兩種：一種是打內結的，一種是打外結的〔如圖三（a）（b）。把一個打外結的輪環面取來，在遠離結的一處沿著經線把它切斷，然後把其中一端像翻襪子一樣翻過來，把結套在裡面，然後與另一端聯合。這就形成一個打內結的輪環面。或者取一塊立方體的木頭，從上面鑽一個洞到相反的一面，這個洞在立方體裡頭打了一個結。這樣也形成了一個打內結的輪環面。你可能會猜想，會不會有一種輪環面，同時打了一個外結又打了一個內結。但此爲不可能。有一種輪環面看來好像又有外結又有內結〔如圖三（c）〕。其實這兩個結只是唬唬人而已。只要將外結解開，內結也就解開了。它同一個沒有打結的輪環面是同等的，或者你可以把它想成一條花園裡噴水用的橡皮管。

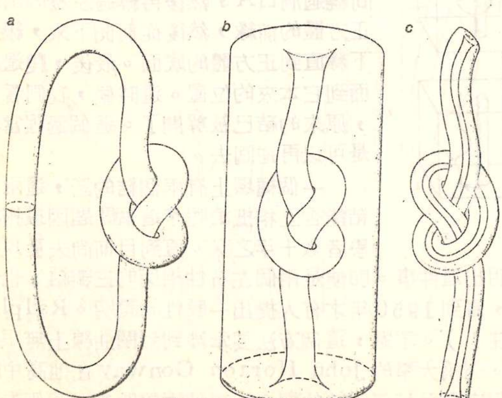


圖 三

Torus with outside knot (a), inside knot (b) and pseudoknots (c)

雖然外結與內結的輪環面內在性完

全相同，然而在三度空間中，它們無法經由彈性變形而互變。打外結的輪環面上若挖了一個洞，那麼在三度空間中能否把它翻過來而成爲打內結的輪環面呢？Wisconsin大學的R. H. Bing已經給了一個很簡潔的答案。Bing在他的論文「Mapping a 3-Sphere onto a Homotopy 3-Sphere」裡還解決了一個與這類似但比這更難的問題，假定現在有三個正立方體，第一個有兩條直管穿過其中；第二個也是有兩條管穿過，一條直的，一條在裡頭打了結；第三個中間也有兩條管，一條直的，另一條則繞著直管打了一個結〔如圖四〕。令人驚奇的是，第三種曲面竟可經由彈性變形而變成第一種曲面。Bing的證明非常

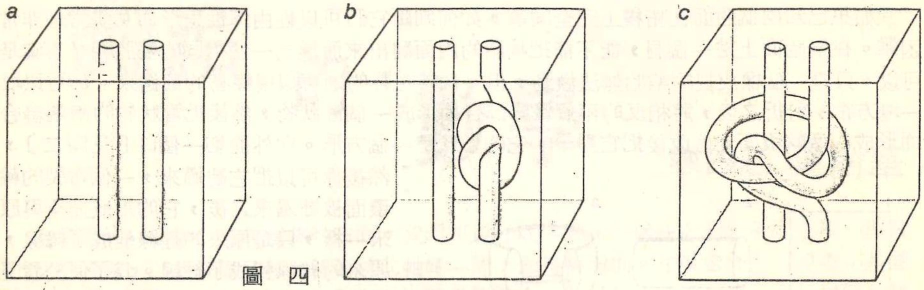


圖　四

Three varieties of a two-hole torus

簡潔易懂。在彈性變形中，吾人可將洞口沿著表面移動任意遠而不致改變曲面的拓樸性質。當洞口向前移動時，它的後面被伸展，它的前面則被壓縮。在Bing的證明裡，爲了便於說明，所以打了結的那條管子被畫成一條線〔如圖五〕。管子底端的洞口B被沿著正方體的下表面移動（以箭頭表示）。當洞口移動時，管子也被帶動。B向左移直到另一條管子的底端，然後沿著管面爬上去直到上表面，再繼續向右移，以逆時針方向繞過洞口A，然後再繞過左邊的洞到正方體的前緣，然後從前側下來，繞過下緣直到正方體的底面。最後，爬過底面到它本來的位置。這時候，我們看見，原來的結已被解開了。這個過程當然是可以再逆回去。

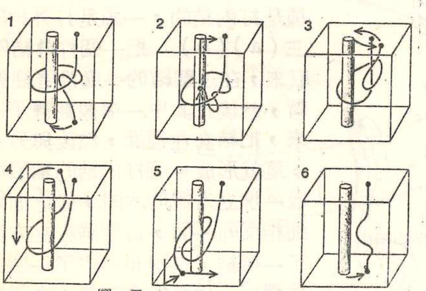
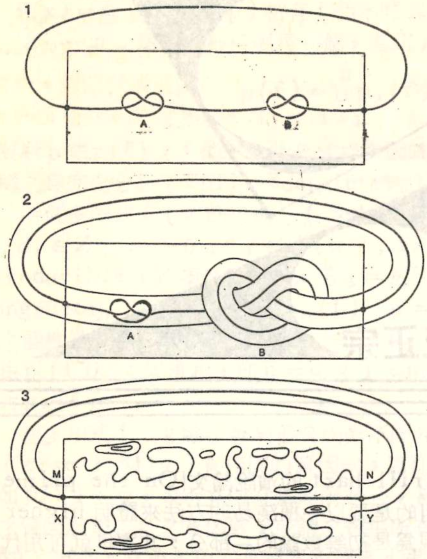
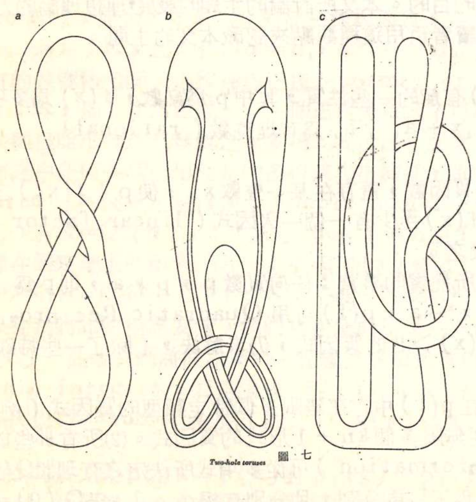


圖　五　　*R. H. Bing's proof*

一個繩環上有兩個結的話，這兩個結能否互相抵消呢？這個問題困擾拓樸學者數十年之久。直到目前尚未發現一對可以互相抵消的結，不過並沒有人證明出這件事。即使是兩個左右性相反的三瓣結，也無人證明其無法相互抵消。關於這種問題，直到1950年才有人提出一般性的證明。Ralph H. Fox於1963年提出了一種方法（註１）。不過，這個方法要牽涉到封閉曲線上無限多繩結的概念，而這個概念是相當繁瑣的。劍橋大學的John Horton Conway在他高中時，無意間發現一個簡單的證明，這種證明完全免掉無限結的觀念。從他的證明裡，我們看見，一個打結的輪環面在近代繩結的理論上扮演著相當重要的角色。Conway是用歸謬法證明，首先我們想像一條穿過房間的封閉繩子。因爲我們只關心房間裡發生的事，那外面的部分我們可以不去管它。〔如圖六(1)〕繩上有A結和B結，這些結若單一的在繩上時，均不能



John Horton Conway's proof. 圖 六



Two-hole toruses 圖 七

被解開。假設A結和B結可以互抵消，在這繩上，我們加上一個輪環面〔如圖六(2)〕。這個輪環面呑下了A結而環繞著B結。因此，管面上任何一條緯線，在兩牆中間的一段必定與B結打一樣的結。事實上，管面上從牆到牆的任何一條線（只要不與自己相交）都與B結有相同的結。現在，開始在繩上進行操作，這個操作可以解開A結和B結。因爲在操作的過程中，不允許繩子自己與自己相交，所以可以不慮打破管壁。如果管壁有攔阻的話，可以推開它，圖六(3)表示最後的結果，繩子的結解開了，管子的形狀變得相當複雜。讓一個垂直的面沿著直繩切下去，我們可以看出管子的橫截面來，就如圖上所示，有一些「島嶼」出現。還有兩條從牆到牆的線XY與MN，這兩條線自己不與自己相交，而且無結。因爲這兩條線都在管面上，而已知所有這種線都與B結有相同的的結，上面的變形等於從一個單有B結的繩上解開了B結。這與假設相反。所以一個繩環上若有可互相抵消的兩結，則每一個都是假結（pseudoknots）。

雖然單洞的輪環面僅以三種方式嵌在三度空間中：外結、內結、無結。雙洞的輪環面却有許多古怪的形式，其數目相信至今還無人能知。我們僅能把某些模型變形成較簡單的形式。例如圖七(a)中的管穿洞式的輪環面是與普通雙洞輪環面同等。圖七(b)中，一個內結從一個外結穿過。圖七(c)中，一個外結穿過一個洞。像這類怪異的形狀，尙有數打之多。

註1：「A Quick Trip Through Knot Theory」in Topology of 3-Manifolds and Related Topics, edited by M.K. Fort Jr. (Prentice Hall, 1963).

多項式的質因式

譯・王正宗

簡介 這篇是譯自 Irving Gerst 和 John Brill hart 的演說論文「On the prime divisors of polynomial」這篇論文其目的是要以一種淺易的方法來證明 higher congruence 理論的某些結果。這些結果可視爲是初等數論的一部分，其實早就可用代數數體的理想（ideal）理論之應用來建立。這篇文章它限制使用體論與等式理論之基礎觀念來說明；以便使更廣大的讀者能接受有趣的數論。本文要討論的定理，純粹是一些淺顯易明的，定理 11 的第一部分是唯一的例外。其他部分，諸如材料（material）的安排證明以及各種應用，都達到了盡可能使讀者感到興趣的目的。本文所討論的主題的發展，理想理論的方法是相當有力而且有深遠理想的，所以建議讀者也用這種觀點來認識本文的主題。

§1 我們將討論 $f(x)\equiv 0 \pmod{p}$ 有解的一些性質，其中 p 爲質數，$f(x)$ 爲多項式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_1x+a_0$，$a_i$ 爲有理整數（rational integral），且 $a_i \not\equiv 0 \pmod{p}$.
若 $f(x)\equiv 0 \pmod{p}$ 有解，則稱 p 爲 f 的質因數，蓋存在某一整數 x_0，使 $p \mid f(x_0)$ 之故，用 $p \mid f(x)$ 表之。在這種情形之下，$f(x)$ 至少有一個一次因式（linear factor $\pmod{p}$）。所有 f 的質因數用 $p(f)$ 表之。

為了解釋這些觀念，我們重溫一個大家所熟習的事實：任何質數 p，$p \nmid a$，則 p 爲 $f(x)=ax+b$ 之質因式；同樣的 $f(x)=x^2-a$，$p(f)$ 可用 Quadratic Reciprocity 定理求得，但在一般情況下，$\deg f(x)>2$ 的質因式，仍未解決，（除了一些特殊情形）。

關於 $p(f)$ 的性質，可歸類成兩種：(1)在 $p(f)$ 中存在無限多個特定類型的質因式（例如在（定理 9）對每一自然數；在 $p(f)$ 中存在無限多個 $kn+1$ 形式的質因式。(2)所有那些能整除某些多項式的質式所成集合的知識（Information）可從多項式所決定之有理體 Q 的擴張間的關係中求得。例如 f，g 在 Q 中皆爲不可再分割，且分別有根 α，β，若 $Q(\alpha)=Q(\beta)$，則 f，g 除了有限個質因數外，其餘質因數皆相同。

§2 基本性質

(A) 以下我們將用 f，g，h 表示只含有一變數的非常數多項式，且此多項式佈於整數系，也就是說 $f(x)\in Z[x]$，記號 p 表示有理質數（rational prime）。如 $\deg f(x)=$

n. $f(x)\equiv 0$ (mod p)恰有 i 個不同解時，其質因式所成集合用 $p_i(f)$ 表之，i=1，2，3……n，這裡重根只視爲一個，若此，顯然的

$$p(f)=\bigcup_{i=1}^{n} p_i(f)$$

在質數 $p\in p(f)$，f 能完全的化成一次因式（linear factors）的乘積，對這些 p，f 稱之爲完全分裂（Split completely）

一個多項式 f（或許可再分（reducible）），表爲 $a\pi f_i^{\alpha_i}$ 之法爲唯一，〔式子中 $a,\alpha_i\in Z$，$\alpha_i>0$，$f_i\in Z[x]$，$fi\neq fj$ if $i\neq j$〕且 $\{fi\}$ 爲 primitive irreducible，首項係數爲正。若 $g=\pi f_i$ 而 g 與幾個不同的一次因式的乘積同餘(congruent)，〔ie. $p\in p_m(f)$ $m=\deg g$〕顯然的，f（mod p）之不同一次因式之個數最大爲m，則稱 f 對於 $p\in p(f)$ 可完全分裂。（Splits completely for $p\in p(f)$）。f 無重根，即 $n=\deg f=m$ 爲一重要之特例，此時 f 完全分裂的條件爲 $p\in p_n(f)$

當多項式 f，g 除了有限個質因素不同外，其餘的質因數皆相同時，則謂 f，g 本質的的（essentially）有相同的質因式，寫作 $p(f)=p(g)$，這裡特別注意「=」之含意，如 $p(f)\neq\phi$，表示 $p(f)$ 爲無限集合，當用 $p(f)\leq p(g)$ 時表除了有限個質因數外，f 之質因數皆爲 g 之質因數，或謂之幾乎所有 f 之質因數皆爲 g 之質因數。

(B) 其次，重溫多項式及體間的關係。我們將討論的體爲有理數體Q中之有限擴張（finite extension），以K，L，M表示體K等可定義爲有理數Q添加一不可分的多項式的根所擴張之體），如此的根稱爲擴張的原元素（primitive element）。當 f 不可分，以K中之原元素（Primitive element）爲根，則稱爲多項式 f 屬於K（f belongs to K），記做 f：K．，對任一體K而言，存在無限多個多項式 f 使 f：K。

若 f：K，且 f 有根 $\alpha=\alpha_1,\alpha^2,\cdots\cdots\alpha_n$，$K=Q(\alpha)$ 則 $Q(\alpha_i)$ 稱爲共軛體，若所有的共軛體相同，則K稱爲正規（normal or Golois）在這情形下，任一多項式 f，若 f：K，則 f 亦爲正規。（一個正規多項式不可再分解，顯然的，當 f 爲正規，一個根 α 的共軛根能用佈於有理數之 α 多項式表示出；反之，若一個不可再分割之多項式 f 之根，與它們之中任何一個可用如此的多項式表出關係，則 f 屬於Q，Q爲由這些根所組成（generated）的簡單正規擴張（Simple nomal extension）。

若 $K=Q(\alpha)$，f：K，$\deg f=n$ 且 $f(\alpha)=0$，我們的證明將基於主要的下列兩種在體定理上的結果①若一多項式 $\phi(x)\in Q[x]$ α 爲其根，則 $\phi(x)$ 爲 $f(x)$ 在 $Q[x]$ 中之倍數。②每一元素 $\gamma\in K$ 有一唯一的表示法 $\gamma=\sum_{j=1}^{n}\gamma_j\alpha^{j-1}$ $\gamma_j\in Q$。其他體論之結果在我們證明中需要者，我們將在後面再逐一介紹。

〔C〕 此後我們將假設屬於一個體之多項式首項係數爲1（monic），設其根是 algebraic integers。若多項式 $f(x)=a_0x^n+\cdots\cdots+a_n$ $a_0\neq 0$，不是monic，我們能代以另一momic 多項式 g，$g(x)=a_0^{n-1}f(x/a_0)$

顯然的依定義 $p(g)=p(f)$ 且 $p_i(g)=p_i(f)$ $i=1,2\cdots\cdots n$。因爲唯一的不同，在此二質數集合至多有有限個質數能整除 a_0；同樣顯然的，若 f：K則 g：K，這些觀察足以推得在這篇裡所證明的monic 多項式的定理適用於非monic 多項式。

在這一節裡，我們複習幾個在有理數（modp）的代數上基本的事實，一分數 a／b（mod p）被定義成 $bx\equiv a$（mod p）而 $p\nmid b$ 之唯一解 x（mod p）。一般化簡

congruence 的法則適用在分數裡；甚而當 $p \nmid b$ $f(a/b) = A/B$ $A, B \in Z$，且 $p \nmid B$ 則 $f(a/b) \equiv A/B \pmod p$ a/b 和 A/B 釋爲分數 $(\bmod p)$，特別的若 $p \mid A$，則 $f(a/b) \equiv 0 \pmod p$ 且 $p \in p(f)$

這特別的論據將在這篇裡許多證明中出現。

§3 基本定理

〔定理1〕 每一不爲常數的多項式 f，均有無限多個質因式（Prime divisors），也就是說 $p(f) \neq \phi$．

證明 假設 $f(0) = C \neq 0$，（因若 $f(0) = C = 0$ 則任一質數皆能整 $f(x)$）。因一個多項式至多有限次值爲 ± 1，故 $f(x)$ 至少存在一質因數。假設 $p_1 p_2, \cdots\cdots p_n$，爲 f 僅有的質因數，令 $a = p_1 p_2 \cdots\cdots p_n$ 則 $f(acx) = cg(x)$

$g(x) = 1 + c_1 x + c_2 x^2 + \cdots\cdots$，且 $a \mid c_i$ $g(x)$ 之質因數 p，也可整除 $f(x)$，因而必爲某一 p_i，但 $p \mid c_i$，推得 $p \mid 1$，因此 $g(x)$ 沒有質因式，即 $g(x) = \pm 1$ 對任一整數 x，這是不可能的。

〔定理2〕 若 $K \leq L$，$f : K$ $g : L$，則 $p(f) \geqq p(g)$

證明 我們必須證幾乎所有 g 的質因式，亦爲 f 之質因式。令 $f(\alpha) = g(\beta) = 0$，$\alpha \in K$，$\beta \in L$ 則因 $K \leq L$，我們寫爲 $\alpha = \phi(\beta)$，$\phi(x) \in Q〔x〕$，則 $f(\phi(x))$ 和 $g(x)$ 有共同根 β，因而 $g(x)$ 之不可再分割，推得

(1) $$f(\phi(x)) = g(x) g_1(x), \quad g_1(x) \in Q〔x〕$$

假設 $p \in p(g)$ 不能整除在 ϕ 中任一係數之分母，（ϕ assumed to be lowest terms），（因 $g(x)$ 爲 monic，相同的 $g_1(x)$ 之係數亦成立），因此從(1)式，若 $g(b) \equiv 0 \pmod p$，$b \in Z$，$\phi(b)$ 將爲 $f(x) \equiv 0 \pmod p$ 之一根，因而 $p \mid f(x)$。

〔定理2〕 亦可用來證明由 f 所定義之體 K，不能包含在由 g 所定義的體 L 中，$\deg f \leq \deg g$，〔若 $\deg f \nmid \deg g$ 則 $K \not\subset L$〕因爲若 $g(\beta) = 0$，考慮多項式 $\phi(x)$ 之所有根（$\phi(\beta)$ 可表爲某一 f 之根 α），若一符合下列三種情況的質數 p 能被找到，則 $K \not\subset L$：①$p \mid g(x)$ ②$p \notin p(f)$ ③p 不能整除 $\phi(x)$ 中的任一分母。

從計算的觀點上，顯然的，可看出如何企圖找質數 p 滿足①和②，（見定理3後之例題），證明如此的 p，是否滿足③，我們必須驗證這些質數可能的發生在 $\phi(x)$ 之分母中，這件事被完成在下面補充定理。

預備定理1〕 設 $L = \phi(\beta)$，β 爲佈於有理數 Q 的 n 次 algebraic integer，定義一項式 g，設任何 algebraic integer $\alpha \in L$ 的 Canonical field 表示法爲 $\alpha =$

$\phi(\beta) = \sum_{j=1}^{n} \gamma_j \beta^{j-1}$，$(\forall_j . \gamma_j \in Q$, are in lowest terms)，若 p 整除任一 γ_j 的分母，則它必定整除 g 的判別式 $D(g)$。

證明 存在 algebraic integers $\gamma_i \in L$，$i = 1, 2 \cdots\cdots n$，使得若 $\alpha \in L$ 是一個 algebraic integer，則 α 有唯一的表示法。

(2) $$\alpha = \sum_{i=1}^{n} d_i \gamma_i \qquad d_i \in Z$$

因 β 的冪級數亦爲 L 中之整數

(3) $$\beta^{j-1} = \sum_{i=1}^{n} C_{ji} \gamma_i \qquad C_{ji} \in Z \qquad j = 1, 2 \cdots\cdots n$$

表β，γ_i 的體共軛(field conjugate)爲$\beta=\beta_1\beta_2\cdots\cdots\beta_n$

$\gamma_i=\gamma_i^{(1)},\gamma_i^{(2)},\cdots\cdots,\gamma_i^{(n)}$　$i=1,2,\cdots\cdots n$，用(3)式我們得一矩陣關係式。

$$(\beta_j^{\,i-1})=(C_{ij})(\gamma_i^{\,j})\quad i.j.=1,2,\cdots\cdots n$$

取每一邊的行列式，並平方，在上式左邊得Vandermonde行列式的平方，這是大家所熟悉的g的判別式，因此

(4)　　$D(g)=J^2\cdot\triangle\quad J=\det(C_{ij})\quad \triangle=[\det(\gamma_i(j))]^2$　等式中J和$D(g)\neq 0$爲有理整數，因△爲 algebrai integer　等於一個有理數，故它必定也是一個有理整數。這裡要提醒的是｜J｜與△，(習慣上稱β的指標和L的判別式)可被證明得與基底$\{\gamma_i\}$之選取無關。

其次，用(3)在$\alpha=\sum\limits_{i=1}^{n}\gamma_j\beta^{j-1}$中我們得

$$\alpha=\sum_{i=1}^{n}\left(\sum_{j=1}^{n}\gamma_j C_{ji}\right)\gamma_i$$

此等式與(2)式比較，γ_i 的對應係數相等，得$d_i=\sum\limits_{j=1}^{n}\gamma_j C_{ji}$，$i=1,2\cdots\cdots n$

得解γ_j(最低項)，$\gamma_j=S_j/J$，$J=1,2,\cdots\cdots n$，有理整數S_j和分子在cramer's rule中，因此，任一質數P，整除γ_j的分母必須整除J，在(4)中得予$P\mid D(g)$

〔附註〕①預備定理1之證明能用指標｜J｜代替D(g)，無論如何，因爲D(g)比指標更易去計算(mod p)，它充分的在numberical應用中，去應用這補充定理。

②在ideal theoretic terms中，$P\nmid D(g)$之條件，推得P在L中是「unramified」，也就是說P分成不同prime ideals在L中。

在這一節的最後一定理，給予有關能整除同屬於一個體的兩個不同多項式的質數所成集合的一些資料。

〔定理3〕　若$f:K$，$g:K$，則$p(f)=p(g)$，且$p_i(f)=p_i(g)$　$i=1,2\cdots n$　$\deg f=\deg g=n$

證明　由定理2知$p(f)\subset p(g)$，且$p(f)\supset p(g)$，因此$p(f)=p(g)$，爲了證明第二部分，我們首先定一個1－1函數，從$g(x)\equiv 0\pmod p$的所有incongruent根所成集合至$f(x)\equiv 0\pmod p$的所有incongruent根所集合。

假設$f(\alpha)=g(\beta)=0$　$\alpha,\beta\in K$，則存在多項式$\phi(x)$　$\phi(x)\in Q[x]$，$\beta=\phi(\alpha)$，$\alpha=\phi(\beta)$，用這個ϕ定一函數：$bi\longrightarrow\phi(bi)$，$bi$爲$g(x)\equiv 0\pmod p$之incongruent根，同定理2之證明，我們能驗證(1)，若P不能整除在ϕ中之分母，則從(1)式中得$\phi(bi)$也是$f(x)\equiv 0\pmod p$之一根。

其次證$\phi(bi)\equiv\phi(b_j)\pmod p$，$i\neq j$，從等式$\phi(\phi(\beta))=\beta$，我們得等式

(5)　　$\phi(\phi(x))-x=g(x)g_2(x)$，　$g_2(x)\in Q[x]$

假設$\phi(bi)\equiv\phi(b_j)\pmod p$，則定$x=bi$，及bi在(5)中，若P不能整除$\phi$中之分母，我們找到

$$bi\equiv\phi(\phi(bi))\equiv\phi(\phi(bj))\equiv bj\pmod p$$

這是一個矛盾。若我們現倒置f，g之角色，在上面論證中，我們可得一個1－1函數，在incongruent根所成的兩個集合中。

〔附註〕顯然從預備定理1及定理3的證明，若$P\nmid D(f)D(g)$ 則$P\mid f(x)$，若且唯若$P\mid g(x)$，因此由它的應用去證明兩個不可再分割的等式多項式，不能決定相同的體，我們僅找一個質數P，使$P\nmid D(f)D(g)$ ，$P\nmid f(x)$，及$P\nmid g(x)$，或若$P\mid g(x)$則f和g沒有相同的incongruent根(mod p)的個數。

〔例題〕：考慮兩個不可再分割的多項式

$$f_1(x)=x^4+4x^3-4x^2-40x-56$$

和 $$f_2(x)=x^4-8x^2-24x-20$$

其判別式$D=-2^{12}\cdot 3^2\cdot 31$ （不可再分割性，可用未定係數及simple pavity方法證明得），$13\mid f_1(2)=-2^6\cdot 13$

但 $13\nmid f_2(x)$ $\forall x=0,1,2,\cdots\cdots 12$

同樣 $13\nmid D$ ，因此這二多項式屬於不同的體。

§4 屬於一個正規體（normal field）的多項式

其次我們研究一個正規（normal）多項式有關於它的質因式（Prime divi-9 sors）的性質。

〔定理4〕：一個正規多項式，對所有它的質因式幾乎可完全分裂。

證明 令$f(x)=x^n+a_1x^{n-1}+\cdots\cdots+a_n$為正規（normal），因 $P_n(f)\subset p(f)$，我們僅要證明$p(f)\subset P_n(f)$即可。 從f的正規性，知：它的根可寫為 $\alpha_1=\alpha$，$\alpha_2=\phi_2(\alpha)$，……，$\alpha_n=\phi_n(\alpha)$， $\phi_i(x)\in Q[x]$

用這些ϕ_i一個有用的二變數恒等式，可從下列乘積的展開式中得到

(6) $$(y-x)(y-\phi_2(x))\cdots\cdots(y-\phi_n(x))=y^n+\gamma_1(x)y^{n-1}+\cdots\cdots+\gamma_n(x)$$

若我們定$x=\alpha$在(6)式，則左邊變成$f(y)$，右邊的係數變為a_i，因此$\gamma_i(x)-a_i$和$f(x)$有共同根α，從f的不可分割性質，推得

$$\gamma_i(x)-a_i=f(x)g_i(x)，i=1,2,\cdots\cdots n \quad g_i(x)\in Q[x]$$

用這些結果代替(6)式中之γ_i，可得吾人所需要的恒等式

(7) $$(y-x)(y-\phi_2(x))\cdots\cdots(y-\phi_n(x))=f(y)+f(x)g_1(x,y)$$
$$g_1(x,y)\in Q[x,y]$$

現在假設P不能整除在ϕ_i中的任一分母；（因此也在g中），同樣，讓$P\in P(f)$；即$P\mid f(a)$，則在(7)中代$x=a$，並考慮(7)式為一congruence（mod p），我們得

(8) $$(y-a)(y-\phi_2(a))\cdots\cdots(y-\phi_n(a))\equiv f(y)\pmod p$$

若$P\nmid D(f)$，也一樣(8)式左邊的根各個不同，而推得$P\in P_n(f)$

〔附註〕要證明一個不可再分割之多項式f不是正規，只要找到一個質數$P\in P(f)$ $P\nmid D(f)$而f不能完全分裂。

〔例題1〕 $$f(x)=x^4-2x^3-2x^2+3x+1$$

則$f(x)$為不可再分割，因它是不可再分割（mod 2），現在$f(5)=11\cdot 31$且$11\nmid D(f)=5^2\cdot 29$，若$P=11$ 則

$f(x)\equiv(x-5)(x-7)(x^2-x-5)\pmod{11}$，這裡的二次因子，不可再分割(mod 11)，因此f不是正規(normal)。

〔例題2〕 多項式$f(x)=x^3-3x+1$ 為正規，其根α，$\phi_2(\alpha)=\alpha^2-2$，且$\phi_3(\alpha)=-\alpha^2-\alpha+2$， （$\alpha$為$f(x)$之任一根，同樣$D(f)$ 3^4，現在$f(8)=3.163$，因此我們能選$P=163$，因$163\nmid D(f)$，$f(x)$（mod 163）所餘留的兩個根能在ϕ_2，ϕ_3中以$a=8$代入而得，所給予的完全因子分解

$$x^3-3x+1\equiv(x-8)(x-62)(x-93) \quad (\text{mod } 163)$$

〔附註〕①若 $f(x)$ 對每一個所試的質因式皆可完全分裂，我們有一很好的指示，f 爲正規，因爲定理4的逆定理亦成立。

②定理4爲下面定理的特殊情形。

〔定理〕　若 f 爲一正規多項式，且 $P\nmid D(f)$，則 f 可化成相同次數的幾個不同再分割的因子 (mod p)，次數依 P 而定

〔推論〕　若 f 爲一正規多項式，其次數爲質數，且 $P\nmid D(f)$　則 f 爲不可再分割 (mod p)，或完全分裂 (mod p)

下面我們考慮定理2的特殊情形，在定理2中定2爲正規，在此我們可得 g 之質因式之更精密的資料。

〔定理5〕　若 $K\leq L$，而 L 正規，f：K，且 g：L，

則　$P_n(f)\geqq p(g)$，$\deg f=n$

證明　我們必須證 f 幾乎對所有 g 的質因式可完全分裂，由假設，f 之根能寫爲 $\alpha_1=\phi(\beta)$，$\alpha_2=\phi_2(\beta)$……　$\alpha_n=\phi_n(\beta)$　β 爲 g 的任一根，$\phi_i(x)\in Q[x]$，利用定理4相同證明方法，可得恒等式。

$$(9)\quad \prod_{i=1}^{n}[y-\phi_i(x)]=f(y)+g(x)g_1(x,y)\quad,\quad g_1(x,y)\in Q[x,y]$$

和以前一樣，若 $g(b)\equiv 0$ (mod p)，$b\in Z$，但 p 不能整除在 ϕ_i 中的任何分母，則

$$f(y)\equiv\prod_{i=1}^{n}[y-\phi_i(b)] \quad (\text{mod } p)$$

若 $p\nmid D(f)$，則右邊的根皆不相等。

〔推論〕：每一不爲常數的多項式，有無限個質因式，而使其完全分裂 (split completely)

證明　考慮正規擴張 $L=Q(\alpha_1,\cdots\cdots\alpha_n)$，$\alpha_i$ 爲多項式 f 之根，若 g：L，佈於 Z 之 f，其每一不可再分割之因子 f_i 定義一 Q 之簡單擴張 (Q 爲 L 之子體)，從定理5中，應用到這些子體，每一個 f_i 將完全分裂，對幾乎所有的 g 的質因式，由定理1，g 有無限多個質因式，因此，從 P(g) 中略去有限個能整除 D(h) $(\neq 0)$ 之 P，〔h(x) 爲所有 f_i 之乘積〕，則推論便證明了。

〔定理6〕　讓 $K\leq L$ (L 爲 K 最小的正規擴張)，若 f：K，g：L，則 $P_n(f)=P(g)$，$\deg f=n$

〔附註〕體 L 可改換以 f 的分裂域 (splitting field)。

證明　由定理5，我們僅需證明 $P_n(f)\leq P(g)$，假設 $\alpha_1,\cdots\cdots\alpha_n$ 爲 f 的根，且 $p\in P_n(f)$，由假設

$$(10)\quad f(x)=\prod_{i=1}^{n}(x-\alpha_i)\equiv\prod_{i=1}^{n}(x-a_i)(\text{mod } p)$$

$$a_i\in Z \quad a_i\neq a_j \quad (i\neq j)$$

從(10)我們得到一結論

$$(11)\quad G_j(\alpha_i)\equiv G_j(a_i) \quad (\text{mod } p),\quad j=1,2,\cdots\cdots n$$

G_j 表第 j 個基本的對稱函數。

其次，我們考慮從 K 擴張到 L，大家所熟悉的是對 K 的最小的正規擴張，存在一個本原

元素$\beta\in L$，$\beta=\sum_{i=1}^{n} C_i\alpha_i$，$C_i\in Z$不失一般性下，我們可假設$\beta$為g的一根，因為由定理3，任何兩個多項式屬於同一個體，本質的有相同的質因式，現在由二個多項式

$$h(x)=\prod_{Sj\in Sn}\left[x-Sj\left(\sum_i C_i\alpha_i\right)\right]$$
$$=\sum_k d_k x^k,\qquad d_{n!}=1$$

和 $$h^*(x)=\prod_{Sj\in Sn}\left[x-S_j\left(\sum_i c_i a_i\right)\right]$$
$$=\sum d_k^* x^k\qquad d_{n!}^*=1$$

在這兩個乘積裡，S_j在對稱群S_n中變動（n個元素的所有排列），例如：$S_j\left(\Sigma_i C_i\alpha_i\right)$，我們表示其為$\Sigma_i C_i\alpha_{1l}$ $l=S_i(i)$

係數d_k（為α_i的對稱函數），顯然的是整數，它可以寫為$d_k=F_k(G_1(\alpha_i),G_2(\alpha_i),\cdots\cdots)$，$F_k$為佈於整數系的多項式，$h^*(x)$的係數$d_k^*$，確切的由相同的多項式$F_k$所決定。將$G_j(a_i)$代替$G_j(\alpha_i)$，然後從(11)式得$d_k^*\equiv d_k\pmod p$因此

(12) $$h(x)\equiv h^*(x)\pmod p$$

因$h^*(x)$為一次因式（linear factors (mod p)）的乘積，故對$h(x)\pmod p$亦成立。但$g(x)$與$h(x)$有共根β，因此$g(x)$可整除$h(x)$，故$P\mid g(x)$

〔附註〕①從上證明最後一句話，可得

$$g(x)\equiv\prod_{j=1}^{n}\left[x-S_j\left(\sum_i C_i a_i\right)\right]\pmod p\qquad m=\deg g$$

在這個乘積裡，S_j變動於S_n的排列中，且$\beta_j=S_j\left(\sum_i C_i\alpha_i\right)$，為$\beta$的m個共軛（conjugates），（這些$S_j$組成了f的Galois group），$g(x)\pmod p$的根。

例題 $f(x)=x^3-2$，其根$\alpha_1=\theta$，$\alpha_2=W\theta$，$\alpha_3=w^2\theta$，$\theta=2^{\frac{1}{3}}$ $w=[-1+(-3)^{\frac{1}{2}}]/2$ 包含α_1的Q的最小正規擴張，其deg為6，因f不為正規，適當的選取

$$\xi=\alpha_1+a\alpha_2+b\alpha_3=a^{\theta}(1+aw+bw^2),\quad a,b\in Z$$，使ξ在α_1的六個排列下有六個不同的值。例如$a=2$，$b=-1$，則$\xi=\theta(1+2w-w^2)$為方程式

$$g(x)=x^6+40x^3+1372=0$$

的根，現在 $31\in P_s(f)$，因

$$f(x)\equiv(x-4)(x-7)(x-20)\pmod{31}$$

現在 $g(x)\equiv 0\pmod{31}$的6個根b_i能由將$a_1\equiv 4$ $a_2\equiv 7$ $a_3\equiv 20\pmod{31}$的6個排列(a_{i1},a_{i2},a_{i3})代入

$a_{i1}+2a_{i2}-a_{i3}$中得bi，如$(a_{i1},a_{i2},a_{i3})=(4,20,7)$

則 $b_2\equiv 6\pmod{31}$，etc 最後

$$g(x)\equiv(x-6)(x-12)(x-21)(x-26)(x-29)(x-30)\pmod{31}$$

②在定理6中，若體k已知為正規，則$K:L$，且定理6導出定理4。

§7 應用

〔定理7〕 對任二不為常數多項式f和g，存在無限多個質因數，能使f和g split completely。

證明　添加 f 和 g 的所有根到Q擴張成正規體 L。設 h：L，則每一佈於 Z 的 f 或 g 之不可再分因子（irreducible factor）定義一個Q的簡單擴張，此爲 L 之一解。就如同在定理 5 的補充定理的證明中，推得 f 和 g 分別幾乎對所有 h 的質因式可完全分裂。但因而存在無限個質數，同時使 f 和 g 對此質數完全分裂。

〔補充定理〕　對有限個不爲常數的多項式，定理 7 亦成立。

〔定理8〕　若 $P \nmid n$，則 $P \mid Q_n(x)$，若且唯若 $P \equiv 1 \pmod{n}$

在定理 7 的補充定理中，我們若考慮 m+1 個函數，$f_1, f_2, \cdots\cdots f_m, Q_n$ 所成的集合，並利用定理 8 可得定理 9。

〔定理9〕　若 $f_1, f_2, \cdots\cdots f_m$，$m \geqq 1$，爲任何不爲常數之多項式，則對每一個固定 n，$n \geqq 1$，存在無限多個 $kn+1$ 形式的質數，使每一 f_i 皆能完全分裂（Splits completely）.

§6　屬於合成體的多項式

在這一節，我們考慮比前面更複雜的情形。在此，我們研究有關屬於合成體的多項式的質因式。

再回想關於此等體的事實；若 $K = Q(\alpha)$，且 $L = Q(\beta)$，爲Q之二有限簡單擴張，合成體 $M = KL$ 定義爲 $Q(\alpha, \beta)$ M爲Q的有限簡單擴張，M存在一原元素具 $\gamma = \alpha + a\beta$ 的形式，a 爲適當選取的有理整數，γ 定義的多項式 h(y) 爲 v(y) 的不可再分割因式（factor）.

$$v(y) = \prod_{i=1}^{n} \prod_{j=1}^{m} \left[y - (\alpha_i + a\beta_j) \right] \qquad v(y) \in Q[y] \tag{13}$$

有根 γ，在這個定義 α_i 和 β_j 爲 $\alpha_1 = \alpha$，$\beta_1 = \beta$ 的共軛（conjugates），且 a 爲適當的選取，使 v(y) 沒有重根。

特例的，若 K 和 L 爲正規，則 $M = KL$ 亦爲正規。爲明白這個觀察，γ 的任一共軛（conjugate）γ_k，將存在一 i 和 j 使 $\gamma_k = \alpha_i + a\beta_j$，K 和 L 的正規性（normality），推得特別根 αi 和 β_j，必定分別落在 K 和 L 中；但 K 和 L 爲M的子體，因此 α_i，β_j 可用 r 的有理式表示 $\gamma_k = \alpha_i + a\beta_j$，故 γ_k 亦可用 γ 的有理式表示，故M爲正規（normal）

〔定理10〕　K，L 爲正規，$M = KL$，若 f：K，g：L，h：M，

則　$P(h) = P(f) \cap P(g)$

證明：因爲 $K \subset M$，　$L \subset M$，由定理 2 得

$$P(f) \supset P(h)$$

且

$$P(g) \supset P(h)$$

因此

$$P(f) \cap P(g) \supset P(h)$$

留下要證明爲

$$P(f) \cap P(g) \subset P(h)$$

若　$\alpha_1 = \alpha$，$\alpha_2, \cdots\cdots \alpha_n$　　且 $\beta_1 = \beta$，$\beta_2, \cdots\cdots \beta_m$

分別爲 f 和 g 的根，則 f 和 g 的正規性（normality），推得存在多項式 $\phi_i(x)$，$\psi_j(x) \in Q[x]$，使得

$$\alpha_i = \phi_i(\alpha) \qquad i = 1, 2, \cdots\cdots n。$$

$$\beta_j = \psi_j(\beta) \qquad j = 1, 2, \cdots\cdots m。$$

這裡我們取 $\phi_1(x) = \psi_1(x) = x$，就如前假設 $\gamma = \alpha + a\beta$，已經是 h 的一根，a 爲適當的選取的整數。

其次，我們建立一類似(9)的恒等式，牽涉到 f 和 g，若恒等式(7)，y 以 $y - a\psi_j(z)$， （z為一新的未定數 indeterminate）代替，可得

$$\prod_{i=1}^{n}\left[y-a\phi_j(z)-\phi_i(x)\right]=f\left(y-a\phi_j(z)\right)+f(x)q_j(x,y,z)$$

$$q_j(x,y,z)\in Q\left[x,y,z\right]$$

若 j 變動於 1，2，……m，則

(14) $$\prod_{j=1}^{n}\prod_{i=1}^{n}\left[y-a\phi_j(z)-\phi_i(x)\right]=\prod_{j=1}^{n}f\left(y-a\phi_j(z)\right)+f(x)$$

$$\gamma(x,y,z),\ \gamma(x,y),z\in Q\left[x,y,z\right]$$

展開乘積的右邊，得

$$\prod_{j=1}^{m}f\left(y-a\phi_j(z)\right)=y^{mn}+\gamma_1(z)y^{mn-1}+\cdots+\gamma_{mn}(z)$$

$$\gamma_i(z)\in Q\left[z\right]$$

代 $z=\beta$ 於上式左邊得下式

$$\prod_{j=1}^{m}f\left(y-a\beta_j\right)=\prod_{j=1}^{m}\prod_{i=1}^{n}\left[\left(y-a\beta_j\right)-\alpha_i\right]$$

$$=v(y)$$

由(13)繼續建立於(7)式之過程，我們得

$$\prod_{j=1}^{m}f\left(y-a\phi_j(z)\right)=v(y)+g(z)s(y,z)$$

$S(y,z)\in Q\left[y,z\right]$

將這結果代入(14)，得所須的恒等式

(15) $$\prod_{j=1}^{m}\prod_{i=1}^{n}\left[y-\phi_i(x)-a\phi_j(z)\right]=v(y)+f(x)\gamma(x,y,z)+g(z)S(y,z)$$

現假設 $P\in P(f)\cap P(g)$，P不能整除(15)式中任何分母，也就是說：存在 b，c $\in Z$，

$$f(b)\equiv g(c)\equiv 0 \pmod p$$

則顯然的，$v(y)$，splits into （不一要相異）linear factors (mod p)，當我們在(15)式中，以 $x=b$，$z=c$，代替並考慮(15)式（mod p），因爲 $h(y)$ 爲 $v(y)$ 的一個因子（factor），故得到 $P\in P(h)$

〔補充定理〕 若 $f:K$，$g:L$，且 $h:M$，log $f=n$，$\deg g=m$ $\deg h=k$，$M=KL$，則

$$P_k(h)=P_n(f)\cap P_m(g)$$

證明 設 K_1，L_1，M_1 分別爲K，L，M的最小正規擴張，並設 $f_1:k_1$，$g_1:L_1$，$h_1:M_1$，則由定理 6

$$P_n(f)=P(f_1)$$
$$P_m(g)=P(g_1)$$
$$P_k(h)=p(h_1)$$

因它可證明得 $M_1=K_1L_1$，由定理 10，馬上可導出此補充定理。

我們現在研究定理 10 的一般情形，K，L 僅有一爲正規。

〔定理 11〕 設 $M=KL$，K爲正規，並設 $f:K$，$g:L$，$h:M$，$\deg g=m$；又若

$\alpha\in K$，為 f 的一根，則設 α 相對於 L 的 degree 為 S，則 deg $h=ms$，且對每一 i $1\leq i\leq ms$，我們記得 $P_i(h)=\phi$，若 $S\nmid i$

$$P_i(h)=P(f)\cap P\gamma(g)\ 。$$

若 $i=rs$ $1\leq r\leq m$ 且

$$P(h)=P(f)\cap P(g)$$

證明 設 $\alpha_1=\alpha$，α_2，……α_n，$\beta_1=\beta$，β_2，……β_m 分別為 f 和 g 的根，並設 $\alpha+a\beta$，$a\in Z$ 為 h 的一根，及 $L=Q(\beta)$

考慮：

(16) $$f(x)=\prod_{k=1}^{t} f_k(x:\beta)$$

f_k 為佈於 L 不可再分割之 monic，若 f_1 有根 α，則由假設 deg $f_1=S$。因此 $M=L(\alpha)$，故 deg $h=ms$，由 f 的正規性推得對每一 i $M=L(\alpha_i)$；故所有相關於 L 之 α_i 的次數為 S；因此，所有 f_k 的次數為 s，比較(16)式，兩邊的次數可得 $n=st$。

因體 $Q(\beta_j)$ 互為 isomorhic，故如 β 代以其任一共軛數，亦可像(16)式予於分解，故以 β_j 代替 β，$x-a\beta_i$ 代替 x，在(16)式中得

$$f(x-a\beta_j)=\prod_{k=1}^{t} f_k(x-a\beta_j;\beta_j),\ j=1,2,\cdots\cdots m$$

將這 m 個等式乘在一起，並用(13)式得

$$v(x)=\prod_{j=1}^{m} f(x-a\beta_j)$$

$$=\prod_{k=1}^{t} h_k(x)$$

$$h_k(x)=\prod_{j=1}^{m} f_k(x-a\beta_j\ ;\ \beta_j)$$

因後項乘積對 β_j 言為對稱，$h_k(x)\in Z[x]$ deg $h_k=ms$，顯然 $h_1(x)=h(x)$，故所有 $h_k(x)$ 屬於 M，因為存在某一 i，使得 $\alpha_i+a\beta$ 為 $h_k(x)$ 的一根，因此由 f 的正規性，

$$Q(\alpha_i+a\beta)=Q(\alpha+a\beta)=M$$

結果，對每一個 k，$h_k(x)$ 為不可再分割，(佈於 Q)

其次分別考慮佈於 Z_p 的 f 和 g 的根

$$\alpha_i^*,\quad i=1,2,\cdots\cdots n \qquad 和 \qquad \beta_j^*,\quad j=1,2\cdots\cdots m$$

組成多項式

$$v^*(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i^*-a\beta_j^*)$$

我們得 $v^*(x)\in Z_p[x]$，然後同在建立(12)的討論，我們得到

(17) $$v(x)\equiv v^*(x)\pmod p$$

同樣，若 $P\nmid D(f)D(g)$，∃ 某一 γ，$1\leq\gamma\leq M$ 使得

$$P\in P(f)\cap P\gamma(g)$$

則，確切的 γ 個相異 β_j^*，將落在 Z_p 中。由定理 4，所有 α_i^* 在 Z_p 中為相異的，因此，若 $P\nmid D(v)$，v^* 將至少有 nr 個相異一次因式（linear factors (mod p)），但 v^* 不能有比 nr 更多，一次因式可推得存在某一 i 和 j，使

$$\alpha_1{}^* + a\beta_j{}^* \in Z_p$$

也因為 $\alpha_1{}^* \in Z_p$，$P \nmid a$，而使 $\beta_j{}^* \in Z_p$，（實際上，$P \nmid D(v)$ 直接導出了 $P \nmid a$）

現在由(17)式 $P \mid v(x)$ 得知P能整除至少有一個 $v(x)$ 的 factors $h_k(x)$，就讓其為 $P \in P_1(h_k)$，則由定理3，幾乎所有能整除這個因子的質數，也將能整除 $v(x)$ 的其他因式（factor），在這些的每一個的 incongruent 解（mod p）的個數，將相同，因此 $v(x)$ 相異的一次因式（linear factor）的個數，將為 t_1，這數目與 $v^*(x)$ 的因式相等，而得 $t_1 = nr$，推得 $i = rs$，（用 $n = st$）故

(18) $$P_1(h) \supset P(f) \cap Pr(g) \qquad i = rs \quad r = 1, 2, \cdots\cdots m$$

其次，我們證明(18)式中的包含，能夠被倒轉，及 $P_1(h) = \phi$。當 $S \nmid i$，假設有某一 i，$1 \leq i \leq ms$，$P \in P_1(h)$，因為K和L為M之子體，由定理2，

$$P_1(h) \subset P(f) \cap P(g)$$

同樣，每一 $P \in P_1(h)$（除了有限個例外），皆屬於某一 $Pr(g)$ $1 \leq rm$，若 $P \in P\gamma(g)$，則因f完全分裂（mod p），我們再S發現，當v有 t_1 個一次因式，則 v^* 有nr個相異一次因式。因此 $\gamma = i/s$。這證明了 γ 由i唯一決定，且 $s \mid i$，至少有有限個質數屬於 $P_1(h)$，同樣當i為s的倍數時，這個倍數將為 γ，故

$$P_1(h) \subset P(f) \cap P\gamma(g)$$

最後

$$P(h) = \bigcup_{i=1}^{ms} P_i(h)$$

$$= \bigcup_{r=1}^{m} \left[P(f) \cap P\gamma(g) \right]$$

$$= P(f) \cap \left[\bigcup_{r=1}^{m} P\gamma(g) \right]$$

$$= P(f) \cap P(g)$$

驚人的九章算術

SWETZ 著.

數四乙— 謝南瑞・譯 ——

十九世紀中葉，中國自兩千年來的排外安眠中，被外洋訪問者的鐵艦與大炮所猛然震醒。突然地，中華帝國的存續不再是依仗儒家的道德倫理，而是要仰賴工藝專技的求取。改革派人士在慈禧皇太后御前擁論他們的見解。他們上奏，另促以教育革新爲工業化的基礎，主要的是，他們欲研究「洋鬼子」的語言與科學，以圖知曉西洋各國卓越工藝專技的秘密。在科學之研究中，最優先的是數學，因爲數學一般均認爲是其它各門科學的基礎。

主管總理各國事務衙門的恭親王，在他于1860年代主倡教育改革時，曾上奏皇上謂：

西洋科學實借根于中國數學，西洋人仍視其數學爲來自東方。只因爲西洋人審愼與尋知的心靈，而使其擅於由老舊中推衍出新穎……中國人發明了方法，西洋人採用了它……（註2；此譯文中之註，概爲原註）。

這種態度廣傳於許多老派的中國學者官吏中，是否恭親王的話僅是一種心理宣傳，想使人們對西洋知識較願接受；或僅是民族優越感的作祟？他的這番話有否可能是眞的？

在本世紀的起頭十年中，各學術雜誌曾出刊了大量有關在當時仍屬新興之漢學(Sinology)的論文。中國的數學成就亦爲前所未悉，而被察考的中華各類文化之一。對於此一論題，有些作者認爲早期中國有高深的數學發展；但有些學者則認爲中國數學成就乃完全受西洋的影響（註3）。綜結此爭論的是史密斯（David Eugene Smith）所作的一篇標題爲「有關中國數學的未決問題」（Unsettled Questions concerning the Mathematics of China）的論文；文中他條列了從事此探討的諸種困難（註4）。這位美國僅有的深研東方數學的史密斯，建議欲建立中國數學眞正的歷史價值，尙須對漢學作更進一步的研究。但自史氏的論文發表後，此種研究就因戰爭與中國內部動亂而中止。這段中斷時期裏，數學史家不是根本忽略早期中國人的貢獻，就是認爲它們不值得作愼重的注意（註5）。

目前漢學研究的復蘇——由於李約瑟（Joseph Needham）的鉅著「中國的科學與文化」（Science and civilization in China）而掀起高潮——必然會使學者對此懸案重行研討（註6）。爲使我們能較瞭解古了中國數學的內涵，本文簡介中國數學古籍中最引起爭論也最具影響力的九章算術。這本許多世紀以來均爲東方數學之主要簿籍的作品，首先由魏利（Alexander Wylie）譯成英文。魏利是滿淸政府所聘用的一位學者兼數學家，他曾爲自己的發現而大感驚奇（註7）。

九章算術的起源與形式

欲判斷古代中國作品成於何時是極爲困難的。殘暴秦始皇在公元前213年首次焚書；因

而漢朝的學者不得不靠著記憶與殘存的斷簡重寫下中國文學與科學的傳統作品。他們常將某一作品歸功於古代某一聖人以求增加此作品的威望，也常常僞造一些作品。因此，九章究竟成於何人何時就混淆不明了。目前，我們認爲它是一本晚秦與漢初之際的作品，可能是一個名叫張蒼的人所寫，他綜合流傳當時的諸古籍而成此書。（譯者按，據傅溥老師謂，九章之作者實尚無定論）。留存至今的版本則是西元 250年時劉徽所著的註本。是以，此書可說是一本截至西元三世紀中葉中國所有數學知識的綜錄；而其核心在耶穌紀元之二百年前即已集備。

九章算術由九個章節所組成。每個章節討論一個與當時中國社會有關的數學論題；其內容爲提出某一問題而後敍述解題規則。中國學者並沒有一套代數符號系統；因此所有的說明均是文學式的。書中並無多少提及解題規則如何地導得；但書文整體而言是代數與算數底，且顯示出是一種經驗方法論。

九章算術的內容：

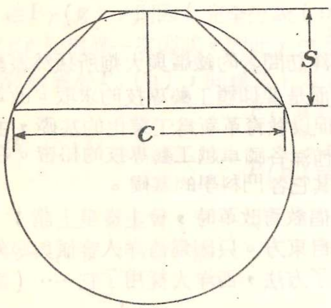


圖　一

一、方田（田地之測量）（註８）。此章中有各種基本土木工程所需的算式。他們包括求矩形，三角形，梯形，與圓形（π 之近似值取爲３）之面積的正確計算規則。一圓弓形面積的梯形近似解爲 $\frac{S}{2}$（c＋s）；c 表弓形的弦，s 表弓形的矢（見圖１）。討論此近似解適當與否，可作爲現今一個有趣的課堂練習。

此章中也提出一種利用最小公分母與最大公因數來演算分數的規則（此與現代所用者相同）。這種分數演算法在歐洲直至十五、六世紀才被人所利用。

π 的近似值取爲３在古代數學書中極通用。魏利在翻譯九章時曾與中國同事討論 π 取３是否適當，他認爲古代學者是有意採用此近似值，而不用另外雖較精確但不便應用的數值。若我們憶起此書本是爲日常經濟應用而作，且古埃及人與巴比倫人類似的作品中也均採用「３」爲近似值，則我們得承認魏利的說法是可信的。李約瑟的研究似乎也採同一觀點。

二、粟米：此章討論簡易的百分率與比例問題。

三、衰分（利用級數來分配）。包括捐稅，合股，算術與幾何級數等的問題於此提出，它們的解是利用比例法與「三律」（rule of three）而求得。

雖然三律一般均認爲起源於印度，但九章算術對此方法之說明却早於梵文本中者（ca 628）。這個在中古歐洲的商業社會中甚受重視的規則，實際上僅是由三個已知量求出一未知量的比例式。有關此規則之一中國例題如下所敍（譯者按，爲閱讀方便起見，本文中所有原載九章的例題概用白話譯出；九章之原題則列於附錄中）。

七分之三兩銀子可買二又二分之一擔的稻子，問九兩銀子可買幾擔稻子？

利用現代數學符號與三律，我們輕易得出其解：

$$\frac{2\frac{1}{2}}{\frac{3}{7}}=\frac{x}{9} \qquad \frac{35}{6}=\frac{x}{9} \qquad x=\frac{(35)(9)}{6} \qquad x=52\frac{1}{2}\ \text{（擔）}$$

此章中有關級數的典型例題是個紡織問題：

一個精於織布的女孩子每天可織出她先一天所織的布的兩倍量。她在五天內織了五尺布，問她第一天與其後諸天每天各織多少布？

今天，一個具少許代數知識的學生，就能將此問題符號化，而得出其解：

$$a+2a+4a+8a+16a = 5$$

因而得 a 爲三十一分之五。九章亦得此答，但中國學者是利用假位律（Rule of False position）而得此解（假位律見七所述）。

四、少廣。此章包含二十四個土地測量問題，其中所列有的若干例子顯出中國人在求平方根與立方根方面的進步。魏利曾注意到本章中所述的解題規則與當時（西元1876 ）英國學校中所講授者極相似。

本章中求一數的平方與立方根是利用一個稱爲天元法（Celestial Element Method）的計算程式。此程式所隱有的概念相當於W. G. Horner在十九世紀時所設計的方法。在Horner 之前二千年，中國人已在敲著算盤，利用他的方法，在解諸如 $x^3 = 1,860,867$ 與 $x^2+34x = 71,000$ 之類的方程式了！雖然後來的數學史家均欲肯定魏利此種看法，但是直到 1955 年王鈴與李約瑟所發表的論文中，纔詳細分析比較Horner 法，而大家方承認這兩種方法在基本原則上完全一致。

天元法（中國人慣以天表未知，故有此名），是由關係式 $(a+b)^2 = a^2+2ab+b^2$（此式乃由幾何學而得）所推出的。Theon of Alexandria (ca 390) 曾運用相類似的程式而得到一求平方根法（註１２）。雖然九章僅是討論整數方根，但有證據示當時的學者確能開方至小數點後若干位。本章中的問題九與十之解顯示出中國人有時將 $\sqrt[n]{m}$ 變形爲 $\sqrt[n]{\dfrac{mp}{p}}$ 以便開方。若取 p 爲 10 的乘　則得

$$\sqrt[n]{m} = \frac{\sqrt[n]{m10^{KN}}}{10^K}$$

此變形首助於根的小數化且可使開方有較大的精確度，漢代數學家在解諸如 $\sqrt{0.35}$ 的問題時，常將它改成 $\sqrt{\dfrac{350}{1000}}$，而得 $\dfrac{\sqrt{350000}}{1000}$，由是就可利用算盤與天元法以求 350,000 的平方根。這種計算技巧，經過印度與伊斯蘭商人推廣後西傳入歐洲，於中世紀末期曾被用來制定平方根表。

此章中有若干關於單位分數（Unit fraction）的問題曾引起爭論，這些問題使早期的研究者誤以爲中國人曾使用一套與埃及人相類似的單位分數系統。

五、商功（土木工程的諸商）。此章中我們可見到建造堤防或堡壘時所需用到的體積計算公式，如稜柱，圓柱，四面體，角錐，圓錐台與楔形等。書中較特異的公式之一爲正三角稜柱楔形的體積，$\dfrac{b_1+b_2+b_3}{6}DL$，其中 b_1，b_2，b_3 爲此楔形的三個寬，D爲高，L爲長（見圖二）。通常我們均以爲Legendre於 1794 年在其書Elements de Gëometrie 中所設計出的（註１３）。另一值得注意的公式是：一四面體若有二對邊 a，b成直角，且公垂線之長

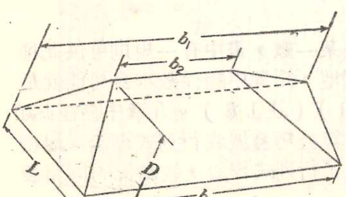


圖　二

爲h，則此四面體積是 $\frac{1}{6}$ 。諸如此類的公式很可能是利用實體模型實測後所得者。

六、均輸（公平課稅）。此章所討論的是稅捐的分配與如何將人民所納的糧運送到京師（追捕問題pursuit problem）。追捕問題——一個令許多學生頭大的問題——引起歐洲人的注意爲時頗晚。史密斯曾將Alcuin of york的propositions of Acundas Jnrenes can 7751一書列爲此問題的西方源始，該書中曾提到獵犬追捕野兔的問題（註14）。九章中對此問題的列例爲：

兔在犬前50步，犬在後追了250步；當二者相距30步時，犬再追幾步即可趕上兔？

七、盈不足（過多與過少）。本章中的代數技巧在西方通常稱爲假位律，用來解形如 $ax-b=0$ 的方程式。這對我們而言是極簡單的，但在採用代數符號以前的年代裏，它的解却是頗爲困難。我們試以中國人的方法來解 $6x-12=0$ 先假定二數 g_1，g_2 爲x的值，$g_1=3$（盈），$g_2=1$（不足）。此二數代入式中得 f_1 與 f_2：

$$(6)(3)-12=\ 6=f_1$$
$$(6)(1)-12=-6=f_2$$

自十三世紀以來，此方法之變形曾廣泛應用於歐洲，其名稱爲Regula Falsae positions。一般均以爲此法是阿拉伯數學家自印度傳入歐洲；對Brahmagupta時代（ca 628）的梵文教本作一查察，即可發現對此方法的提示。埃及的Rhind papyrus亦曾提出另一個假位律，但它與中國和歐洲者均不同。

八、方程。此章中有十八個問題，討論一次聯立方程組的解。

使用算盤的人必須先將一所予的方程組的係數以一矩陣表出纔能遂行其技術。與現代相同的基本行列運算被運用於此矩陣以求解。研究此章中的一例題可能有所啓廸：

有三種等級的米。單拿二簍一等米，或三簍二等米，或四簍三等米均不能湊足某一所需量。但若一等米中加入一簍二等米，二等米中加入一簍三等米，三等米中加入一簍一等米，則都可湊足此所需量。問，在每個混裝簍中此三種米各有多少？

此亦即

$$\begin{aligned} 2x+\ y\qquad &=1\\ 3y+z\ &=1\\ x\qquad +4z\ &=1 \end{aligned}$$

所形成的矩陣爲

1		2	一等米（x）
	3	1	二等米（y）
4	1		三等米（z）
1	1	1	所需量

「零」在矩陣中以空白表之。此問題需要求解人自無中減去某一數，書中有一規則可供此種運算——這表示中國人是首先發展出負數運算的民族。同樣地，矩陣中的係數本身可能就是負數。先前所認爲首先使用負數的是印度數學家（ca 630）（註16）。九章中存在此類問題，這否定了此一看法。然而，中國人却沒有將他們的計算技巧發展成行列式理論。繼續研究者之一的月本數學家saki kowa最後在1683年形成了行列式理論，較歐洲的同類發展早了十年。

本章中最後所討論的一個具有四個方程式五個未知數的方程組顯示早期中國人對不定方程式的探討。後期中國數學家改進不定分析，且將此研究定名爲太元九數。中國學者所研究

的典型問題是「百隻家畜」。

一隻公鷄值五分錢，一隻母鷄值三分錢，小鷄三隻值一分錢，問一百分錢可買總數爲一百隻的公鷄，母鷄，小鷄各幾隻？（ca 475）

九、勾股（直角）。此章中有二十四個有關直角三角形之性質的問題。必須精確測量土地，這使得早期中國人民就不能不對畢氏定理有所瞭解且能應用。

在我們錄下此章中若干較有趣的問題，以使諸者能欣賞欣賞，且可作爲課堂上的練習題，它們可供爲想像力與數學推理訓練的題目。在已予解答的例題中，可令學生討論究竟如何推得此解答。

有根繩子懸於桿上。此繩有三尺閑置地面，拉直繩子使它的末端恰觸於地面，則接觸點離基點八尺。問繩長若干？

有個圓柱體恰埋在一堵牆面之後。當牆被鑿開 $\frac{1}{10}$ 尺後，見到此圓柱體露出一尺之寬。問圓柱體的直徑若干？（圖三）

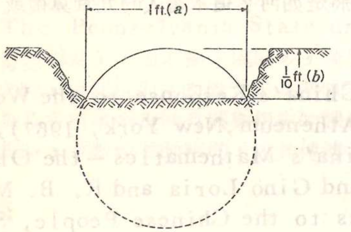


圖　三

解法：$a + \left[\frac{b}{2}\right]^2 / a = d$

在一棵二十尺高，周長三尺的樹下長有葛藤，此藤繞樹幹七圈而恰達到樹頂。問繞長若干？

在十平方尺的池塘中央長有一葦，它突出水面一尺。將此葦拉向岸邊，則其頂端恰與岸齊。問水熱與葦長各若干？

解法：

$$\text{水深} = \frac{\left[\frac{\text{池塘邊長}}{2}\right]^2 - \left[\text{蘆葦突出水面部分的長}\right]^2}{2\,(\text{蘆葦突出水面部分的長})}$$

有根十尺高的竹子，折斷其上端而使其彎觸地面，按觸點離根三尺。問折斷處離地若干？（見圖四）

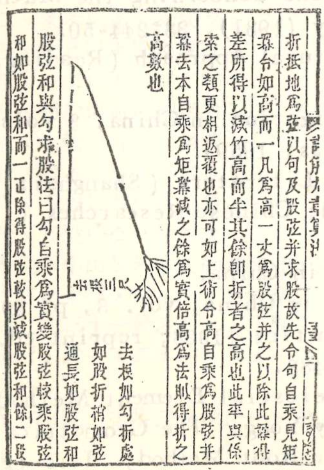


Fig. 4. The controversial "bent bamboo problem." From *Science and Civilization in China*, by Joseph Needham; volume III, courtesy of Cambridge University Press.

圖　四

此問題是中國數學西傳的指示者。Aryabhata 時代（ca 510）之後的梵文作品中包含有此例題（註17）。再後，它就出現於歐洲作品之中。

本章中第二十個例題顯示出中國人對二次方程式的知識。

有個未知邊長的方形鄉村，它被一條連結南北西邊之中心的道路貫通。在北門之北20步之處有棵樹，自南門南行14步再西行1775後，可見到此樹。問此鄉村每邊長度若干？

此問題可簡化成求方程式 $x^2+(20+14)x-(2)(20)(1775)=0$ 的正根。答案是250步。雖然書中並沒提到如何解出，但告訴讀者利用參法（譯音）。參法是天元法所使用的計算表法的一部分；因此，顯然天元法的變形

可用來解二次方程式。

結　論：

九章算術雖然不是一本有關數學演繹的書籍，但我們應該記得，除希臘之外，早期的數學作品可說沒有討論推理演繹的。甚至許多年後，中世紀歐洲學者仍用類似的型式寫作數學書。九章中所顯示的各種數學「第一」，似可作為恭親王所謂中國學者在早期已在實用數學方面發展到一高水準的部分證明。這種數學知識有多少會傳入歐洲目前尚無定論。早在第三世紀時，中國的絲綢與鐵器已在羅馬帝國的市場上高價買賣；如此，為何我們不能認為中國的智慧產品，包括數學知識，亦於早期就傳到西方。

雖然中國在早期有這麼一段強勁的數學活動，如九章之內容所表露的，持續的社會壓力却窒礙了數學由僅是一種經驗技巧的階段作更進一步的發展，中國人所擁有的這一大塊赤地，必須藉著工藝專技或社會教條的發展，纔能維持衆多人口的生存。中國人選擇了後者，他們寧可限制自身與群體的自由以求與自然妥協，而不願改變自然以適應社會。因此，演繹科學——包括數學在內——就作了儒家人文思想的犧牲品，以保證社會的和諧。我們眞不能不疑惑，若是中國人不採取此種策略，則歷史的路線將是如何？這本驚人的九章算術或可予我們部分的解答！

原文註：

2. John Fairbank and Teng Ssu-Yu, China's Response to the West : A Documentary Survey 1839-1923 (Atheneum, New York, 1967), p.74
3. For example Albion Fellows, China's Mathematics — the Oldest, China Review (1921), 1:214-15; and Gino Loria and R. B. Mc-Clenon, The Debt of Mathematics to the Chinese People, Scientific Monthly (1921), 12:517-21.
4. David E. Smith, Unsettled Questions Concerning the Mathematics of China, Scientific Monthly (1931), 33:244-50.
5. Morris Kline, Mathematics: A Cultural Approach (Reading. Miss : Addison-Wesley, 1962), p. 12.
6. Joseph Needham, Science and Civilization in China, 3 vols. (London: Cambridge University Press, 1959).
7. Alexander Wylie, Notes on Chinese Literature (Shanghai: American Presbyterian Press, 1901); Chinese Researches (Shanghai, 1897).
8. Needham, Science and Civilization in China.
9. Needham, Science and Civilization in China, vol. 3, p. 99.
10. David E. Smith, History of Mathematics (1923; reprint ed., New York: Dover Publications), 2:483.
12. For a detailed discussion of the Celestial Element Method and its Greek counterpart, see Lam Lay Yong, The Geometrical Basis of the Ancient Chinese Square-Root Method, Isis (Fall, 1970), pp. 92-101; and Wang Ling and Joseph Needham, Horner's Method in Chinese Mathematics: Its Origins in the Root Extraction Procedures of the Han Dynasty (Toung pao, Leiden, 1955), 43:345-88.

13. J. L. Coolidge, A History of Geometrical Methods (Oxford: Clarendon Press, 1940), p. 21.
14. Smith, History of Mathematics, vol. 2, p. 546.
15. For more details on Chinese matrix problems see D. J. Struik, On Ancient Chinese Mathematics, MATHEMATICS TEACHER 56 Mathematics (New York: John Wiley & Sons, 1968).
16. Kline, Mathematics: A Cultural Approach, p. 19.
17. Yoshio Mikami, The Development of Mathematics in China and Japan (1913; reprint ed., New York: Chelsea publishing Co.), p. 23. Needham indicates much duplication of Chiu Chang material in later Jodlan texts.

譯後的話：

一、本文原載於1972年五月份的Mathematics Teacher，作者爲Frank Swetz; The Pennsylvania State university.
二、匆匆譯就，不通不暢之處頗多，請鑒諒！
三、譯時，對列祖列宗的偉大成就感佩不已，更爲自已對祖宗成就的茫無所知慚愧不已。
四、誠心希望本系重開有關數學史的課程。
五、譯時，承數位老師相助，尤其傅溥老師更以其稿本相借，感激不已。

附錄：

九章算術分爲九卷，其目爲：
卷一、方田以御田疇界域。
卷二、粟米以御交質變易。
卷三、衰分以御貴賤稟稅。
卷四、少廣以御積冪方圓。
卷五、商功以御功程積實。
卷六、均輸以御遠近勞費。
卷七、盈不足以御隱藏互見。
卷八、方程以御錯糅正負。
卷九、句股以御高深廣遠。

玆摘錄九章中出現於本文的各問題，以供參考：

今有女善織，目百倍，五日織五尺，問日織幾何？答曰，初日織一寸三十分寸之十九，次日織三寸三十一分之七。（下略）

術曰，置一，二，四，八，十六爲列衰，副幷，爲法，以五尺乘未幷者，各自爲實，實如法得一。

今有田廣一步半三分步之一，求田一畝，問從幾何？答曰，一百三十步一十一分步之一十。

術曰，下有三分，以一爲六，半爲三，三分之一爲二，幷之，得一十一，爲法，置田二百四十步，亦以一爲六，乘之，爲實，實如法，得從步。

今有兔先走一百步，犬追之二百五十步，不及三十步而止，問犬不止，復行幾何步及之？答曰，一百七步七分步之一。

術曰：置兔先走一百步，以犬走不及三十步減之，餘爲法，以不及三十步，乘犬追步數，爲實，實如法，得一。

今有上禾二秉，中禾三秉，下禾四秉，實皆不滿斗，上取中，中取下，下取上，各一秉，而實滿斗。問上中下禾實一秉各幾何？答曰，上禾一秉，實二十五分斗之九，中禾一秉，實二十五分斗之七，下禾一實，實二十五分斗之四。

今有木長二丈，圍之三尺，葛生其下，纏木七圈，上與木齊，問葛長幾何？答曰，二丈九尺。

術曰，以七周乘三尺，爲股，木長爲句，爲之求弦，弦者葛之長。（下略）

今有池，方一丈，葭生其中，出水一尺，引葭赴岸，適與岸齊，問水深葭長各幾何？答曰，水深一丈二尺，葭長一丈三尺。

術曰，半池方，自乘，（中略），以出水一尺自乘，減之，（中略），餘，倍出水，除之，卽得水深，（中略），加出水數，得葭長。

今有立木，繫索其末，委地三尺，引索卽行，去本八尺而索盡，問索長幾何？答曰，一丈二尺六分之一。

術曰，以去本自乘，（中略），令如委數而一，（中略），所得，加委地數而半之，卽索長。（下略）

今有圓材，埋在壁中，不知大小，以　　之，深一寸，　道長一尺，問徑幾何？答曰，材徑二尺六寸。

術曰，半　道自乘，（中略），如深寸而一，以深寸增之，卽材徑（下略）。

今有竹高一丈，末析抵地，去本三尺，問折者高幾何？答曰，四尺二十分尺之一。

術曰，以去本自乘，（中略），令如高而一，（中略），所得，以減竹高而半，餘卽折者之高也，（下略）。

今有邑方，不知大小，各中開門，出北門二十步有木，出南門一十四步，折而西行一千七百七十五步見木，問邑方幾何？答曰，二百五十步。

術曰，以出北門步數，乘西行步數，倍之，爲實，（中略），拜出南門步數，爲從法，開方除之，卽邑方。（上略）。

註：此附錄乃摘自：商務印書館王雲五主編之「叢書集成初編」第二一一册，爲本校圖書館閱覽室所藏。

拓樸與分析

數二乙
施友仁·譯·

1.導言

本文我所要談的是站在分析學而非拓樸學的立場，尤其我並不討論拓樸上公理系統的結構，也不是引導年輕的心靈對於生命的試驗，更不是一些定理的組織體系。而是，我將大部份地限制我的論題於拓樸在分析上所扮演的角色，以及提供一個更幾何化的觀點。以下，我將給予一連串不相關連的說明。

2.基本的分析

我們假定對於拓樸最簡單的解剖背景為熟悉開放（open），封閉（closed）連通（connected），緊緻（compact）等概念，所有這些名詞將用於歐氏空間中的集合觀念上。

於此，我們先看看二則關於集合與連續函數的敘述：

(1)所有滿足 $x^2-xy+y^3\leq 1$ 的點所成的集合為閉集合。

(2)假設 f 為定義於〔a，b〕上之實值連續函數，則 f 為有界的，且 f 在〔a，b〕中有極大值和極小值。

(3)假設 f 為定義於〔a，b〕上之實值連續函數，而且 $f(a)<0$, $f(b)>0$ 則在 a 與 b 間存在一 t，$a<t<b$ 使得 $f(t)=0$

另外讓我們再考慮三則有關拓樸性質更一般化之敘述：

(1)′設 E 為一閉集合，F 是一連續函數，則其逆像 $F^{-1}(E)$ 是閉集合。

(2)′緊緻集合經連續函映之映像仍為緊緻集合。

(3)′連通集合經連續函映之映像仍為連通集合。

後三則與前三者之關係是非常明顯的，每一敘述(A)′可以推得敘述(A)，而且提供了更清楚的內容。

3.中等的分析

有時，分析可以幫助拓樸觀念的了解，當一位老師第一次介紹拓樸觀念時，一般的方法是顯示學生在一個空間中若干不同的拓樸，並且使他們比較其性質，如果所選的集合是平面或平面的部分集合，則這許多不同的拓樸會像有計劃的打擊學生，他們可能會留下這種感覺，關於拓樸及其性質的討論是沒有永久不變的意義，這是非常真確的，如果他已經學得歐氏拓樸（Euclidem topology）是平面上（或幾維空間）唯一有模的拓樸。（See〔2〕p.p. 191-192）

或許在同一集合的若干拓樸上比較其性質，在中級分析課程會做得更好，假設我們選取 F 為所有定義於 $x=(-\infty,\infty)$ 上的實值函數所成的集合，則我們將可以看出在分析上許多標準的論題都和比較以下兩個定義於 F 上的極限拓樸有關：(i) 點態收斂（pontwise convergence）：$\{f_n\}\to f$ iff $f_n(x)\to f(x)$ $\forall\in X$
(ii) 均勻收斂（uniform convergence）：$\{f_n\}\to f$ iff $f_n(x)\to f(x)$ uniformy $\forall\in X$ 以上這兩條都非常重要，並且在分析中扮演著很主要的角色，因此要問這些拓樸性質的差異不是一般人所能解決。

舉個例子來說明，令C爲包含F中所有連續函數所成的子集合，則我們要問：在每一種情況下，C是否爲一封閉集合？注意其答案是不同的，更甚的定義函數數列的收斂中語言的不同而產生不同的結果。

其他的問題如：一個緊緻集合（compact set）像什麼呢？是否$F(\phi)=\int_0^{x}\phi$，$\phi\in C$爲一定義於C上或F上之連續函數，所有多項式所成的集合P是否爲C中的綢密集合（dense set）。

在每一種情況下，一個普通的拓樸問題產生一個重要的分析結果。

4.高等的分析：

其他拓樸方面非常重要的概念也可以如下來討論（我們藉此修正前節中所可能產生的錯誤影響）。

由點態收斂（i）的觀念產生定義於F上的「點態」拓樸，在F中一函數f_0之鄰域N爲特定有限個點$x_1 x_2 \cdots\cdots x_n$連結函數$\delta_1 \delta_2 \cdots\cdots \delta_n$使得$N=N(x_1,x_2\cdots\cdots x_n;\delta_1,\delta_2,\cdots\cdots\delta_n)$包含所有函數$f\in F$滿足$|f(x_j)-f_0(x_j)|<\delta_j$ for $j=1,2,\cdots\cdots N$.

雖然「點態」拓樸爲一很自然的形態，但它表示一個不可量度（not metrizable）的拓樸。在此拓樸中，一個集合的閉包（closure）不能只由收斂數列的極限來獲得。（因此，點態收斂（i）不能在F上定義一眞正拓樸，而均勻收斂（ii）可以）。

欲證明此情況：令S爲包含F中所有連續函數滿足以下條件(4)所成的子集合。

(4) $\int_0^1 f(x)dx=1$ and $0\leqq f(x)\leqq 2$ for all $x,-\infty<x<\infty$

顯而易見的，常數函數0屬於S的點態閉包（pointwise closure），卽每一0函數的鄰域$N(x_1,x_2,\cdots\cdots x_n;\delta_1,\delta_2,\cdots\cdots\delta_n)$均包含S中的函數。然而在S中並不存在一系列$f_n$點點收斂於0函數。因爲，假設存在$f_n(x)\to 0$ $\forall x\in[0,1]$，則由Lebesgue Bounded Convergence Thorem（參考〔1〕）我們得到

(5) $\int_0^1 f_n\to\int_0^1 0=0$

此和(4)產生矛盾。（當然，S中存在一net $\{f_\lambda\}$ 點點收斂於0（參考〔2〕pp 143-146.）

從不同的方面，有很多例子使拓樸的觀念導致更多的啓發，在基本分析上一個最標準的定理是說在有界區間中，單調連續函數的反函數爲連續。於此有一簡單類似的性質。我們首先研究函數的連續性與其圖形之關係。

定理：令A和B爲度量空間（metric space）且A是緊緻的並令$f:A\to B$爲一函數，$G=\{(a,f(a))|a\in A\}$爲在$A\times B$中的圖形則f爲連續函數若且唯若G是緊緻集合。

證明：($\Longrightarrow$) 此方向非常明顯，假設f爲連續則此函映$x\xrightarrow{T}(x,f(x))$連續，而且$G=T(A)$緊緻。

($\Longleftarrow$) 相反的，假設G是緊緻，但是f不連續，則在A中將存在一數列$\{x_n\}$收斂於$x_0\in A$，但是$d(f(x_n),f(x_0))\geqq\delta>0$ 對所有n。此數列$P_n=(x_n,f(x_n))$屬於G中，則必存在一子數列$\{P_{n_j}\}$收斂於點$(a,b)\in G$，顯然的$a=x_0$所以$b=f(x_0)$，故$f(x_{n_j})\to f(x_0)$，此與假設中$\{x_n\}$的性質矛盾。

由此定理我們可以明顯的推論到下面重要的結果：

推論：令A與B爲度量空間（metric space）A是緊緻的，$f:A\to B$連續且一對一，則f^{-1}連續。

證明：令$B_0=f(A)$；爲B中之一緊緻集合，則函數$f^{-1}:B_0\to A$其圖形與f之圖形同構。因f爲連續，故$B_0=f(A)$緊緻，且f^{-1}連續。

從這點來看，我們可以指出條件A是緊緻的重要性，令C爲可度量空間，包含所有定義在〔0,1〕之連續實値函數加上均勻收斂拓樸。定義一函數$F:C\to C$爲$F(\phi)=\phi$其中$\phi(x)=\int_0^x\phi$, $0\leqq x\leqq 1$,我們易於證明F爲連續，而且F爲一對一，因若$F(\phi_1)=F(\phi_2)$，則$\int_0^x\phi_1-\phi_2=0$ $\forall x\in[0,1]$則$\phi_1=\phi_2$，然而F^{-1}

(此函數存在)不連續。我們可以看出 F^{-1} 就是D,微分運算,假使 $\psi_n \to \psi_0$ uniformly,則 ψ_n' 並不一定收斂於 ψ'。

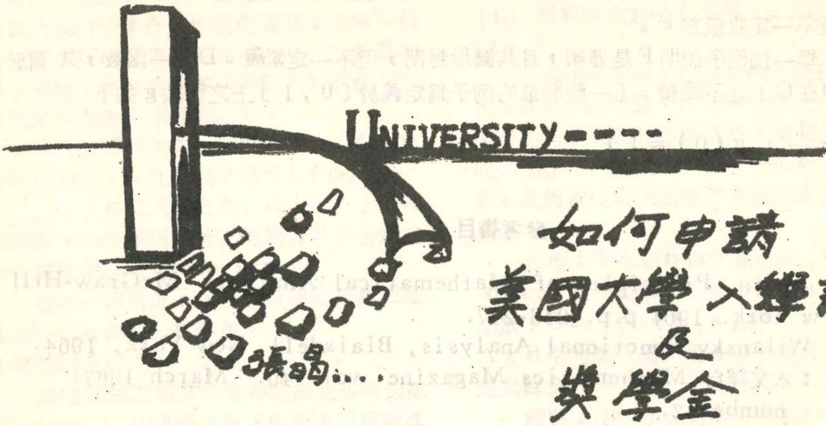
最後,舉一個例子說明F是連續,且其圖形封閉,但不一定緊緻。D為一函數,其圖形封閉,但D在C上並不連續。(一較簡單的例子為定義於〔0,1〕上之函數g如下:$g(x)=\frac{1}{x}$,$g(0)=1$)

參考書目

〔1〕 W. Rudin, Principles of Mathematical Analysis McGraw-Hill New York. 1964 p.p. 246-247.

〔2〕 A. Wilansky Functional Analysis, Blaisdell. New York, 1964.

〔譯者註〕:本文譯自 Mathematics Magazine vol. 40. March 1967. number 2.



如何申請美國大學入學許可及獎學金

一、前言

本文的目的是要指引有志赴美深造的同學，申請美國大學之入學許可及獎學金所需要的大致步驟，以及本人所知道的處理方法。雖然赴美留學近數年來在國內各大學幾乎已經是一種盲目的風氣。但是眞正有志出國深造，回國後能對國家有所貢獻也是目前很需要的。尤其我們讀數學的，在國內只有教書一途，如果志不在此，實在浪費了所學的知識，如能到國外吸收些應用的知識，發揮自己另一方面的潛能，對國家人群就有更大的貢獻。本校是公費學校，結業後實習及服務各一年期滿後，才能辦理展緩服務出國深造，男同學又要服兵役兩年，所以出國風氣在大學內很不盛行。不過本系同學所學程度很高，且在國外之系友很多都表現得很好，如果申請出國深造，應該比其他學校的畢業生容易得多。

二、預備工作

1.托福考試（TOEFL）

每年四次（1月，3月，6月，10月）內容爲聽力，生字，構造，閱讀，寫作五部份。在語言中心報名，需要報名費US＄10，照片三張（1吋光面）帶學歷證件（大專最高年級以上）。均在週日下午考連續3－4小時，所以體力也很要緊。500分以上可簽證，550分以上爲佳。這是不留記錄的，考不好可以再考。因爲每一個學校都要這考試的成績最好在申請前考到一個高分，又因它只保留二年，過時就無效，太早考也沒用。

2.G.R.E.考試

每年四次（1月，3月，6月，10月），須先到濟南路三段美國在華教育基金會拿報名表格（免費），內容①性向測驗—語文能力（Verbal ）及計算能力（quantitive），

②專門測驗（Advanced Test），我們是考數學（Mathematics）大部分是大學學過的，從初微，高微，微方整數論，代數，拓樸，或然率統計甚至計算機及應用數學，一般不甚難，要做些考古題，總會考過900 以上。有些學校要性向成績總分起超過一千分，所以平時宜多背些古怪英文單字，增加閱讀能力，在計算能力多考些高中數學，及一些統計圖表的題目，對我們眞太輕鬆不過，要快要準才能爭取高分。此項考試報名須寄到E.T.S.比考試早一個月，每項US＄9.5。另外它留有記錄且保留五年。所以沒充分準備不可冒然嘗試。均在週末考，上午考性向。下午考專門科。在同一試場內，試題有些是不一樣的，抄別人的答案，如果試題是不一樣的，那就慘了。

3.申請表格：這是向美國大學要正式表格的要求表格，可到濟南路的基金會去拿，每人每次十張。不妨多拿點。此表後面有一空白處可以打些自己的經歷，及想到他校讀什麽之類的。一般都是用這種表，有些人直接用郵簡可以省點錢。

4.結滙：

到台灣銀行總行國外部（總統府左邊）拿一種申請學校及考試滙出外幣的申請表及四聯單辦理。若申請的多，不妨把幾個學校都塡在一張表上，可省點滙費。一般銀行辦事都很慢，不妨上午送進去，下午才去拿滙票省得等。另外寄滙票一定要掛號（赴美為新台幣22元）。

5.英文成績單：

本校成績單要自己先打底稿，送成績股校對後。每一個月最多不可超過申請6份（80元），所以要多準備些，先申請些存在成績股。另外有些學校只要有等第（grade），有些要分數的。所以兩種都要有準備。每份要一吋，二吋光面相片各一張。寄成績單的信封貼掛號郵票（22元）。

6.學校參考資料：

在本系系館有下列二書供參考用。

(一) 1970 Guide Book to Tlepartment in the Mathematical Sciences in the United States and Canada. The Mathematical Associate of America.（系友卜浩熊捐贈）。

(二) Notices of the American Mathematical society：Special issal assistant'shipoand fellowships in Mathematics in 1972—73.

或在美新處及基金會找到其他資料。一般可以看出下列幾個要點。

(一)學校大否：可看它學生的多寡，獎學金名額金費的多不多，及教材陣容判斷出。一般的大學校比較難申請，且有些第一年不給獎學金。

(二)系名、地址及系主任的姓名：資料要愈新愈正確，否則系主任早就換了，您寄錯了信，很可能被退回來，擔誤時間。

(三)該系那一門最強；一方面可由教授陣容中查出，或由它三年內所給的博士中看出。這可看出該系與你往後進修的興趣是否相合，非常重要。

(四)第一年外國學生給獎學金否：可以比較資料(一)中該校總共的研究生及獎學金的差的人數是否比一年級新生多而判斷出。

(五)截止日期：一切的申請表格（正式），成績及介紹信務必要在截止前寄達。

諸位查出以上資料後，根據個人的興趣及程度選擇適當的學校寄出，申請表格向該校要正式表格及簡介。如果申請秋季班入學，最好在八月多就寄出（航空）。

三、申請學校

1. 正式表格的填寫

(一)姓名：Last Name (Family Name)是姓。
First Name是名。

(二)生日：如October 1, 1949 。(有些月份也用阿拉伯字)

(三)Citizen of Taipei, R.O.C.

(四)地址：照郵政局標準翻譯。

(五)要求入學年月：如Fall, 1973 。

(六)攻的學位：M.A., M.S.,及Ph.D.

(七)所讀過的學校：包括小學各級學校的英譯名。

(八)家長及在美聯絡人的姓名及地址。

(九)健康檢查書：可到師大健康中心去檢查。或公私立醫院。

(十)曾得過的獎學金：如中國人文自然科學獎學金(Chinese Culture and Natural Science Scholarship by The Ministry of Education)

(士)介紹信人姓名及地址。

(主)G.P.A.(Grade Point Average)：以成績A爲4，B爲3，C爲2，D爲1，所乘學分之和除整個學分所得之平均數。

(圭)自傳。　(击)讀書計劃。

(去)申請費：有些可以免，一般十元，十五元，廿元不等。

(夫)有些是寄到Admisson office,有些是寄到系裡或Graduate school，要分清楚。

(乞)附一張信告訴他：您寄了什麽給他，以及其他介紹信及托福各項成績是否寄去，請他有事或缺什麽，一定要儘速通知。

(大)簽名年月日。

2. 介紹信：(Letters of Recommandation)

先要取得你請他爲你寫介紹信教授的同意。是他自己寫或要你自己先擬一個稿子，由他修改後再打字簽字。須注意：

(一)在截止前寄達，太厚要多貼點郵票，一定要用系裏的信封，信紙。

(二)不可同時寄不同的介紹信到同一學校。

(三)如同申請一個系，請同一位教授，用的打字機該是一樣的。

(四)不同教授寄到同一個系的打字機要不同才好。

(五)介紹信內容不可把自己太吹噓。要實話實說。否則把本系的招牌砸了，絶了往後系友申請該校之路，就太不該了。

(六)見附(二)系內部份老師中英文名。

3. 自傳及讀書計劃：

這是省不得的，一定要先寫好，請專人修改，才不會像十足的中國英文。內容包括個人興趣，求學過程、經歷、嗜好，以及對將來的打算，希望讀什麽，怎麽讀它，讀出後的打算等等，也可以介紹自己的家庭及經濟情況等。一般學校都很注重這份計劃，所以草率不得。大約在五百到一千字左右。

四、靜候佳音辦理出國手續

一般要到3月中才有消息，常有些學校會沒收到E.T.S.的托福及G.R.E.成績，那你就得再寄(當然又得花錢)，有些消息來得很早，有些要到六、七月才有消息，不過來

得太晚，辦理出國就常會來不及。又有些學校Admission Office 說不給獎學金，而系裏可能會給。所以挑選、拒絕不宜過早。出國前須參加留學生講習，辦理展緩服務，體格檢查，役男服完役辦理自費或甄試留學生出國。應在該校開學前抵達才好。

五、寫在篇後

在師大第六上半時，幾乎都忙著申請學校，承系裏面幾位老助教及老師的指點，使我沒花太多寃枉時間在這方面。眼看著我們系裏學生素質在老師的嚴勵教導下，日漸提高，以後想到國外深造的同學一定不少，希望這篇文章能對諸位有所幫助。

附一、數學系中英文成績對照表

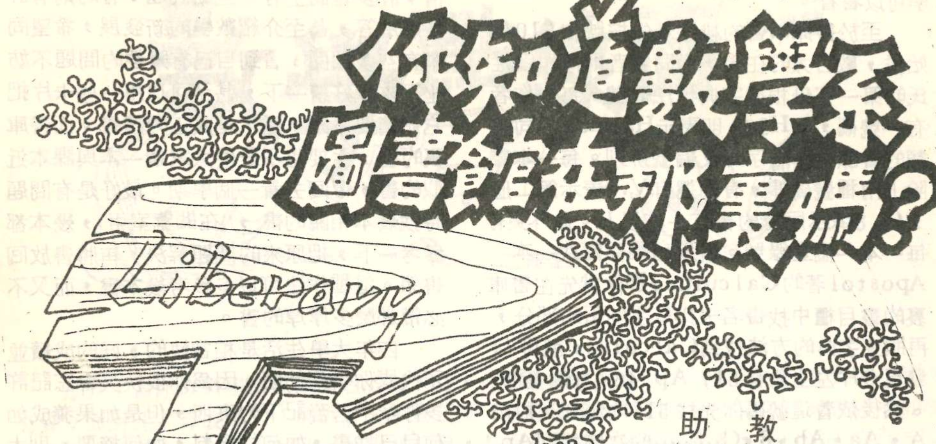
Freshman(Sept 1967–July 1968)	大一
Dr. Sun Yat-Sen's Toughts	國父思想
Chinese	國　文
English	英　文
Introduction to Education	教育概論
Differential and Integral Calcnlus	微積分
Physics	物　理
Physics Laboratory	物理實驗
Solid Analytical Geometry	立體解析幾何
Synthetic Projective Geometry	綜合射影幾何
Physical Education	體　育
Mandarin (WriHen Examination)	國音（筆試）
Mandarin (Oral Examination)	國音（口試）
Four Books	四　書
Military Training	軍　訓
Total & Average	
Sophomore (Sept 1968–July 1969)	大　二
Psychology	心理學
General Method of Teaching	普通教學法
Introduction to Philosoply.	哲學概論
Advanced Calcnlus	高等微積分
Differenticl Equation	微分方程
Theory of Numbers	整數論
Modern History of China	中國近代史
An Introduction to Theory of Sets	集合導論
Theory of Series	級數論
Physical Edncation	體　育
Military Training	軍　訓
Vector and Tenror	向量與張量

Sophomore English	大二英文
Total & Average	
Junior (Sept 1969—July 1970)	大　三
Higher Algelra	高等代數
Differtial Geometry	微分幾何
German (I)	大一德文
Logic	理則學
Theory of Functions of a Complex Variable	複變數函數論
Introduction to Topology	拓樸學導論
Physical Edncation	體　育
Theoretical Mechanics	理論力學
Measure Theory	測度學
Audio-Visual Education	視聽教育
Total & Average	
Senior (Sept 1970—July 1971)	大　四
Teaching Practice	教育實習
Teaching of Mathematics	數學教材教法
Modern Algebra	近世代數
Physical Education	體　育
Linear Algebra	線性代數
German (II)	大二德文
Mathematical Statistics	數理統計
Numerical Analysis	數值分析
Partical Differntial Eqnation	偏微分方程
Integral Equation	積分方程式
Total & Average	
Fifth Year (Aug 1971—July)	教學實習
Teaching Practice	

附二、本系部份老師中英文名

范傳坡：Chuan-Po Fan	李巡伯：Shun-Po Lee
康洪元：Hoong-Yuan Kong	富沙諾：B.A. Fusaro
常法微：Fa-Hvei Chang	湯　森：Carl G. Townsend
蔡英藩：Ying-Fun Tsai	陳銘德：Ming-Teb Chen
劉季植：Gee-Tze Liu	李嘉淦：Chia-Gann Li
陶　濤：Tao Tao	羅芳樺：Fang-Hua Lo
王詩頌：Shih-Sung Wang	郭汾派：Fun-Pay Kuo
邱日盛：Jih-Shen Chiu	傅　溥：P. Fu

你知道數學系(註)圖書館在那裏嗎？



助　教
—吳家怡—

畢業後第一次進我的辦公室—系圖書館—辦第一件工作（註册時負責清點圖書辦理還書手續），就聽到一句令人遺憾的話。一位數三的同學說：「噢，原來這裡是系圖書館呀！」。我呆呆的看着他，無言以對。第二天我們趕快去配了一個「數學系圖書館」的牌子掛在牆上。

唯恐有的同學還不知道系圖書館所在地，我特地在此再提一次：系辦公室三樓兩間房間均為系圖書館，其中一間為書庫，採用開架式，以便同學自由選書，翻閱和借用。另一間為閱覽室，（是由會議室移用，所以仍兼會議室）。閱覽室是為閱覽不可出借的雜誌和期刊而設，也可以閱覽由書庫中取出而不準備借出的書。室中備有桌椅沙發及書架、報架，歡迎同學多多利用。但為方便管理並鼓勵同學多看雜誌，參考書，這間閱覽入和一樓的閱覽室不同，不可攜帶私人書籍內，私人書籍請置於門口桌上。

可是只知道系圖書館在那裏，却不知道你需要的書在那裏還是沒用的。所以我們來談談書庫裏的書。書庫中存書約九千多册，有原版的，也有翻版的。所有的書均採用杜氏編目法，由總館分類編號，系館即依此種分類排列。所有的數約分成十一部份，其中510為數學總論，511為算數，512為代數，513為幾何和拓樸，514是三角，515為投影幾何學，516是歐氏幾何，517微積分，518特殊函數，而519則為機率，統計方面的書，其他的如630的電腦知識，793的數學遊戲，530為應用數學。而其中最常用的有512.8的抽象代數，512.81為數論，512.86群論；幾何方面513.83是拓樸，513.8是非歐幾何；517.38是微分方程，517是高微、初微，517.8則都是複變方面的書。160有邏輯的書。

其中510的總類中有一些是數學概論之類的介紹性書籍，可以對數學各方面的分支有一點了解。而510.9是數學史的部份，雖然藏書不夠新，但多少可以使大家對數學史有較詳盡的認識，對這方面有興趣的同學可以稍為涉獵一下。793那一部分書極少，却是些數學遊戲之類的書，是個有趣却很冷門的部份。此外還有一部分日文書籍，其中以

數學史，數學教育佔多數，看得懂日文的同學可以看看。

至於書庫中書的排法是先按號由510開始排，數目大的在後，而同號者則按作者姓氏的第一字母根據字典排法編號，每一作者有一號碼，如H162 卽表示Halmos 。同一類的書卽依作者字母及編號排列。每一本書除上兩種號碼外，有的還有V. 2表示第二册，C. 3表示同樣的書有一本以上。此外更有每一本一個登錄號。所以如果你要找一本Apostol著的Calculus，那你就先在書庫裏的書目櫃中找書名卡以C字開頭的部分，再照查字典的方法找到Calculus，就可以發現卡片左上角有 517 Ap 46 crp的編號。然後依着這號碼你先找 517的部分，再按A，Aa，Ab，B，C………的次序找到Ap，再按號碼找到46。不過要注意46是表示460而非046 。

如果你只知道作者是Apostol ，則可以由作者卡着手，依查字典法找出Apostol，也可以得到書號。如果你只知道要那一方面的書，就只有靠分類卡，從你要的那一類中選出你要的書。

至於雜誌期刊，都放在閱覽室，約有廿多種却乏人問津。其實雜誌一向是許多新知識的最好來源，系館中的雜誌有的較淺，如Mathematical teacher就是一本相當淺的書，其中有許多簡單而有趣的小問題，和一些問題的教法。另一本The American Mathematical mouthly 則包括較廣也不深，並有一些新書介紹。Mathematical Magezin 是本黃黑色的小本雜誌，談的是純數學的。此外尙有(1)Acta Mathematics (2)Annals of Mathematics (3)Bulletin of the Ameriean Mathematical Society (4)Canaclian Journal of Mathematics (5)Mathematics Reviews (6)Notes of the Amerccan Mathematical Society (7)Topology (8)Transactious of the American Mathematical Society

雜誌很少有同學來翻閱，我們一直覺得很可惜。許多雜誌上有一些新問題，有的則有許多新解答，甚至介紹數學的新發展，希望同學有空多翻閱，看到自己有興趣的問題不妨坐下來好好讀一下，甚至可以用一些卡片把它們摘要下來，這才是眞正的讀書。而書庫裏的書，主要也不是供大家選一本與課本近似的書，帶回去看一個學期。最好是有問題時找幾本相關的書， 在閱覽室中 ，幾本都參考一下，把原來的問題解決，再將書放回書架。這種作法可以多參考幾本書，而又不必帶那麽多厚厚的書。

四年大學生活是相當快的，好的成績並不代表你學到什麽，因爲你很快又會忘記許多你辛辛苦苦記下的東西，但是如果養成如何自己找書，如何找資料，如何摘要，則大學四年所得的一些知識，可以永遠幫助你學到更多新東西，則永遠受用無盡。

圖書館每天定時開放，歡迎大家多多利用。

數二乙
·薛光豐·

數學點線面

朋友！當你以數學系為榮而沾沾自喜時，你可會聽過別系同學對我們的評價？其中有毀有譽，面對此不算成熟的「解析」，不覺莞爾。或許他（她）們的看法很客觀，却是片面的，如同瞎人摸象。但每一句話，其來必有自，甚而有段曲折堪聞的趣事，那只待諸位去旁徵博引，多加考證了！

「我所認識的數學系學生，很多都是『舞棍』，但我所參加的舞會，却以數學系所辦的最破。」

「數學系對理想往往比較欠缺一些。」

「數學系的教室最破。」

「數學系多才女少美女。」

「有一天，我遇見數學系一位新鮮人和一名去年的新鮮人同行，他們自稱是師大『數一數二』的。

「學數學最具有生意眼。」

「數學系的女生總是裂著嘴，露齒大笑。」

「數學系有『深度』的奇多，有『份量』的奇少。」

「家教中心應設在數學系。」

「數學系的舞棍不打領帶，打領帶的，都不會跳舞。」

「物、化系有『誤差』，數學系却標榜『恒等』『精確值』。」

「數學系者，不學無『數』。」

「數學系的男生總愛用『方程式』來描寫女孩子。」

「數學系是大系，故『數』見不鮮。」

「數學系的學生泰半具有雙重身份：『亦師亦生』。」

「數學系的女孩子少『外銷』，因外系不易追之故也。」

「數學系有跟我們（國文系）『人才交流』的必要。」

「數學系最小氣，整天談微『分』、積『分』、三角、一元二次、二元一次……總談不高價錢。」

「在我的印象中，數學系的學生該是戴著厚厚的『樑架』，眼珠無神，欲閉還休，整天抱著洋書，走起路來彎腰駝背，腦中只有X，Y。」

還有許多我不知道我知道，及我知道我不知道的，尚祈望諸位多多挖掘。

某些人談數學

Math ? Math Math

數四甲

—鄭美琪—

生意好：法老！您好啊！來來來！這杯敬您！近來事務所的事業忙吧？有您這般好口才，加上豐富的學識，定是場場勝訴，業務興隆囉！

法超情：哪裡！哪裡！不敢當！不過最近我幫人打了一場有趣的官司，不妨說給您聽聽：有兄弟倆爭遺產，他們的父親遺言以賽跑的勝負分配遺產的多少。哥哥是跑步健將，爲了體諒弟弟的速度只有他的六分之一，就讓弟弟先跑十公尺，然後開始跑，但他跑得快，當然是他先到達終點囉！可是弟弟不服氣，來找我幫忙，他認爲以賽跑來決定得遺產的多少是不公平的。我說：「既然你先跑十公尺，當然是你贏囉！」結果，我幫弟弟打贏這場官司！

生意好：哦！怎麽說呢？

法超情：是這樣的，假設哥哥和弟弟起步的位置分別是A_0和A_1的話，那麽A_1不就在A_0前十公尺嗎？等到哥哥跑到A_1時，弟弟已在A_1前六分之一公尺的A_2點了，等到哥哥跑到A_2時，弟弟又已在A_2前三六分之一公尺的A_3點了……這樣繼續下去，儘管弟兄倆的距離不斷縮短，但是哥哥永遠追不上弟弟。

生意好：啊！您眞是太聰明，太了不起了！能把事情分析得那麽仔細，眞是佩服！佩服！

先掛號：不對！不對！我雖然學的是醫，可是對簡單的算學也還不陌生，很明顯的，如果哥哥的速度是每分六百公尺，那麽他將在出發後$\frac{1}{50}$分追到弟弟，怎麽會追不上呢？

數國人：剛才法先生的論點沒考慮時間的問題。他所涉及的時刻永遠在追上的時刻以前，所以看不到哥哥追上弟弟的可能。法先生引用了希臘詭辯家齊諾的奇論

，眞是聰明。

法超情：我們這一行啊！替別人辯護時，只能採取對己方有利的條件，絶對不能在自己的辯論中加進任何使自己失敗的條件。這不像科學家追求眞理時不放鬆任何情況啊！

生意好：唉呀！在今天這個鷄尾酒會中，還是別談這麽深奧的問題吧！嗨！數國人！今天能遇到您可眞是幸運！我啊！常常迷糊的連帳都弄不清楚，您能吃數學這行飯，對數字一定非常有辦法，請指敎指敎吧！

數國人：大概您以爲咱們學數學的，成天幹的不外是解解方程式，變換大小次序或者利用三角求山高，用代數算複利，是吧！您這就想偏了！其實啊！數學家幾乎和數字絶緣，他們不一定算得好加減乘除呢！

世界通：嗯！聽說啊！數學是一種語言，是將思維用符號表現出來，就好像某一國的語言和文字一樣呢！

數國人：可以這麽說，但其中要加更多的邏輯推理。語言和文字有時是習慣成自然，也有時是積非成是，沒有什麽理由，但數學就不容許這種情形的發生。所以，數學應該是一組精要中肯的假設和另一組結論，經由完美的證明所兜成的邏輯式吻合。

先掛號：既然如此，學數學有什麽用？不就是在假設和結論間打轉，一昧的自我陶醉嗎？

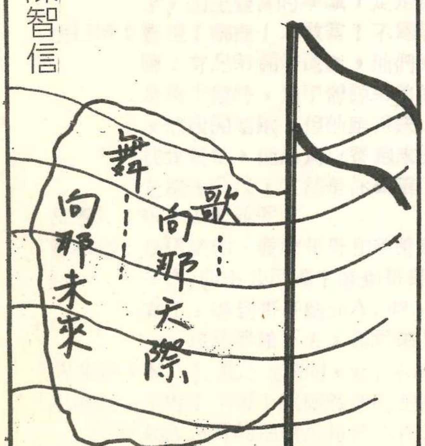
數國人：一個邏輯式數學家是該抱著無所爲而爲的態度的。如果你去接觸它，會發現數學本身蘊藏著很多趣味，很能引人入勝的。不過這好像唱高調，尤其在今天的酒會談論起來更覺不妥。如果各位想和數學王國裡的人交通思想，還是先去學學他們的語言吧！來！預祝各位收益良多！乾一杯！

您是否還記得？

彎彎的小河
　　盛開的花朵
你是否還記得……
金色的沙灘
　　銀白的海浪
你是否還記得……

康樂一年

數三甲
陳智信



匆匆的一年，您可知道，它包含了多少的唏噓、歡樂、惋惜、興奮……？或許，還有那絲絲的安慰。……

對一個數學系的學生來說，如果他能久處於高微、拓樸……之中，那麼，其非瘋子則爲天才。當然，你我都不是。因此，康樂活動對於本系的同學來說，實佔一個很重要的地位。可是，限於環境、經費以及本身的力量，康樂股未能提供更多的活動，這一點，我們感到抱歉。但，畢竟我們已盡了力。

一年來的康樂活動，我們儘量朝著「求新」的目標去做——迎新的健行、系露營以及未來的送舊聚餐，都是新的嘗試，也正因爲如此，活動的成效，未能達到我們預期的目標。但你我也不必過於苛責，畢竟，從舉辦過的活動中，我們獲得了許多的經驗，這對於未來學會的工作，或多或少總是有所稗益的。………

系迎新的健行活動，從清幽的河濱公園，走到富麗的故宮，近兩百人的學子，時而高歌，時而狂嘯，縱心神遨遊天地、任想像超越時空—只是，那盒精緻的野餐，尚沒有被遺忘。

班際橋藝賽的舉辦，爲每個班級掀起了風潮。而且，這股風潮似乎愈湧愈密，君不見學生活動中心、美術系的教室，甚至系舘的角落裡，都成了牌友們的天下？也正因爲如此，在全校的系際橋藝賽中，本系能過關斬將，獨佔鰲頭。

金山的露營活動，又爲學會的活動，掀起了一陣高潮。濛濛的細雨，使這屬於青年的育樂中心，增添了幾許的詩意；凜凜的海風，融合了我們這一群的歡笑，更爲大地帶來了一股新的衝撞力。忘不了海灘上深嵌的足跡；忘不了那滲雜著沙和雨水的飯菜，也忘不了那晚來風寒、相擁而眠的景象；更忘不了那大夥兒促膝長談的夜語，突然，我們之間不再有任何的隔閡。「苦悶的象徵」裡，曾說到——人只有在遊玩的時候，才是一個完全的人——誠如是，那麼，在短短的三天裡，大地已蘊育了一百多個新的「完全人」了。或許，有一天當你老了而我也不再年輕的時候，又重逢在這令人留

戀的沙灘時，我們將道出久藏的心語——呵！往事難忘。

記者之家的舞會，爲那些舞君子帶來了一夜的狂歡，或許還有那藕藕甜美的回憶。寄望不久的迭舊舞會，能使你們再度享受一種心靈的昇華。

負責了一年的康樂股，很遺憾的看到許多學會工作未能順利發展的癥結，我們很願意將它毫無保留的說出。畢竟，我們更期望你我能同心協力除去這病根。或許，這將遭來許多的不滿，但原諒我們無暇顧及這些，只因爲我們如此迫切的希望數學系能很快的茁壯。

一、同學們「自我」的觀念過重：此次系合唱團的組成，我們遭受了極大的阻礙，以五百多人組成的學會，居然湊不到一個四十人的合唱團，這並不意著我們的人才過少，但却看出了同學們還不肯走出自限的領域。且從每次練唱的情形看來，同學們愛系護系的精神還不夠——或許由於先天不足、後天失調，合唱團的水準，始終不能達到一定的目標。然而，也正因爲如此，我們就有權利，也負有這種意務使它紮根、使它成長，畢竟，學會是屬於大家的。可是，有些同學，却在合唱團最迫切需要他的時候，悄悄的走了。我們不願多說什麽，只是，我們將誠懇的希望各位同學，能將自己融合在學會這個大家族裡。別忘了，你是他組成的一份子。

二、同學們責任感的缺乏：班際棋藝賽的舉辦，報名的隊數有八班，但比賽當日却只有兩隊到場，這給予我們極大的困擾，也看出了有些同學尙不能具有對自己負責的信心。對於將爲人師的我們，這實在是一值得警惕之事。

一年來，康樂活動的舉辦，承蒙各位師長、各股幹事以及許多同學精神的支持，使我們在失望、灰心之際，有了再生的勇氣。這些人，都是推動學會工作的無名英雄，盼望有一天，每位同學都能如是，此乃學會之幸啊！深盼著，深盼著………

……打開您的心房，打開心房的窗門，讓春風吹進，那和暖的春風，溶化冬天的冰雪，將冷枯的心溫暖活躍起來……朋友，莫再猶豫。

—五月十八日于師大—

本年度的主要活動概要

六十一年度

本系系旗迎新紀念章圖案設計優勝：夜二、江大昕同學

十月十六日：參加系際籃球賽本系男子組獲冠軍

十月廿十日：迎新健行故宮、雙溪公園

十一月一日：參加系際拔河賽本系表現優良

十一月十一日、十二日：第廿六屆校運本系成績斐然榮獲

男子：田賽——冠軍　　女子：田賽——亞軍

徑賽——冠軍　　徑賽——第五名

大隊接力——亞軍　　大隊接力——亞軍

十二月四日：參加系際桌球賽男子組蟬聯男子組冠軍

十二月四日：參加系際足球賽獲第四名

六十二年度

三月十五日：籃球隊系隊與中原作友誼賽

三月十八日：本系在記者之家學行舞會

三月二十日：邀請中央研究院數研所陳明博博士演講

三月廿三日：參加系際排球賽男子組獲冠軍

四月一、二、三日：全系在金山育樂中心大露營

五月八日：參加系際羽球賽女子組獲冠軍

五月十四日：參加系際棒壘球賽男子組獲第三名

五月十八日：鄒袞偉、辛美月、蔡勝煌同學獲全校時事測驗第一、第二、第四名。

五月十九日：在大利餐館送舊與畢業聚餐

五月二十日：在樂群堂送舊。

五月廿三日：參加系際合唱比賽

六月三日：參加系際水上運動本系獲男子組第四名及大隊接力第五名。

※徵　　稿※

我們盼望第八期的系刊能早日與諸位師長、系友、同學見面；當然，這需要看您的投稿。

第八期中，我們需要的稿子是：

(1)數學的哲學觀。（The philosophy of Mathematics）
(2)讀書心得報告。（包括個人的讀書方法、慘痛經驗、書籍介紹、教本中艱深教材的說明）
(3)專題研究。（尤其歡迎師長、系友們的研究心得）
(4)國內外各大學數學系課程介紹。（並予以適當的說明）
(5)數學研究的新趨勢。（如此，可以給大家方向，方不致於迷惑徘徊）

最後，我們不希望系刊太過於形式化，抽象得令多數人望而生厭。我們期待它是一本「親切的」「可愛的」讀物。

截稿日期：六十二年十二月卅一日。

有任何意見、建議、稿件，請寄至：$\boxed{106}$ 台北郵箱22之104號　系刊編輯收

六十一學年度學會組織概況

常務理事：江清宮（三甲）
刊主編：王正宗（三甲）
康樂股長：陳智信（三甲）
文教股長：黃光彩（三乙）
衛生股長：李和淑（二乙）
系館管理：劉瑞崇（二乙）

常務監事：宋廷申（夜三）
編輯：黃光彩、曾文宏、許燦煌、薛光豐
體育股長：劉茂雄（二乙）
總務股長：黃傳紘（三甲）
交通股長：陳秋錦（二丙）

理監事：

許建志、蔡坤龍、劉宏泰（四甲）
金世淼、卓至臻、莊國輝（夜四）
李善文、曹博盛、李春得（三乙）
蕭漢卿、張炳森、蔡佳容（二甲）
康燕文、柯賢忠、朱錦福（二丙）
洪有情、蔡聰達、梁慈玲（一甲）
林樹頭、李錫南、陳炳煌（一丙）

郭伯嘉、師岱濤、鄭耀洲（四乙）
張盛林、江清宮、張西村（三甲）
黃美華、張良才、宋廷申（夜三）
薛光豐、蔡總湖、楊吉三（二乙）
李健瑛、章修璞、許秀貞（夜二）
吳安生、李金樹、莊萬富（一乙）
詹勝世、李玉芳、顏秀錦（夜一）