師大數學

6

台北市和平東路一段

國立台灣師範大學數學系

——弁　言——

時代進步，科學昌明。數學之應用，愈來愈廣泛。非但自然科學、應用科學，不能離開數學，即社會科學理論之研究，亦非應用數學不可。同時，數學本身之領域，亦日益擴展；尤以代數、拓樸等學科，近年來更是發展迅速，一日千里。

本系成立於今二十餘年，畢業同學，數以千計。出國深造者，更各有成就，或繼續研究，或返國服務。而本系班級，年有增加，同學數量，與之俱增。眞乃潛力深遠，前途無量。

本刋爲我師生校友發表心得及創見之園地，年來經負責同學之辛苦耕耘及師生校友大力支援下，業已生根發芽，滋長茁壯。但願大家不吝珠璣，源源賜稿，則本刋將如初生旭日，光芒萬丈。際茲第六期發刋之日，謹贅數語，願與同仁校友暨同學共勉之。

范 傳 坡　民國六十一年四月

——編者的話——

過去的經驗，未來的展望與各位師長，同學熱誠的讚助下，終於使這一份屬於我們的數學刋物——師大數學——順利地誕生了。

由於本校數學研究所的創立，使得本校的數學氣息又再度激起陣陣澎湃的熱潮。一系列的專題演講，同學之間的討論會，不但證明了這種數學氣氛的復甦，更進而爲我們這一份園地添加了一批潛力渾厚的生力軍。

在本期中，我們把舊有的數學系刋提昇到另一個個新的境界——師大數學——；由只是同學的創作拓展到師長、系友的專題論述。雖然僅是十多篇，然而這都是各位師長，同學在百忙中賜稿，我們除了表示最高的謝意外，並且希望各位師長今後能繼續來栽培灌溉這一塊屬於我們的園地。

很幸運的，在本期的編輯工作中，我們有了甫自國外歸來的薛昭雄博士當我們的顧問，對於一切稿件的審核，編輯事務的推展無不全力以赴。值此出刋之際，我們除了向薛老師致最謝外，並且對於其他熱心幫助的師長同學也一併致以由衷的感激。

主 編

目 錄

有關線性常微分方程式與線性代數

湯森客座教授著
張晶助教譯

1. 簡　介

本文係二篇在台北市國立師範大學對數學系學生之講稿。本文之目的在敍述線性常微分方程式與線性代數互相之關係。特別借此兩支數學導致以及應用 e^{At} 的觀念，此A表示一 n 階方陣。

2. 線性常微分方程組

考慮常微分方程式（O.D.E.）$x'=ax$ 。在這兒我們必須要求何式其微分後爲 ax ？利用初微我們就可得到答案是“ $e^{at}c$ 。此 c 爲一常數”。因此每一個常微分方程式 $x=ax$ 之解是 $e(t)=e^{at}c$ 這種形式，此 c 爲一常數。

現在我們考慮一線性常微分方程組如下：

$$x_1'=a_{11}(t)\,x_1+a_{12}(t)\,x_2+\cdots\cdots+a_{1n}(t)\,x_n+b_1(t).$$
$$x_2'=a_{21}(t)\,x_1+a_{22}(t)\,x_2+\cdots\cdots+a_{2n}(t)\,x_n+b_2(t).$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$x_n'=a_{n1}(t)\,x_1+a_{n2}(t)\,x_2+\cdots\cdots+a_{nn}(t)\,x_n+b_n(t).$$

此方程組可以表成矩陣形式：

$$\begin{bmatrix} x_1' \\ x_2' \\ \vdots \\ x_n' \end{bmatrix} = \begin{bmatrix} a_{11}(t) & a_{12}(t) & \cdots & a_{1n}(t) \\ a_{21}(t) & a_{22}(t) & \cdots & a_{2n}(t) \\ \vdots & \vdots & \cdots\cdots & \\ a_{n1}(t) & a_{n2}(t) & \cdots & a_{nn}(t) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} b_1(t) \\ b_2(t) \\ \vdots \\ b_n(t) \end{bmatrix}$$

我們將這縮寫爲：

（L）　$\vec{x}'=A(t)\,\vec{x}+\vec{b}(t).$

當 $\vec{b}(t)\equiv\vec{0}$ 時（L）式成

（LH）　$\vec{x}'=A(t)\,\vec{x}.$

當 $b(t)\equiv 0$ 且 A 爲常數時：

(LHC)　$\vec{x}' = A\vec{x}$.

首先我們考慮上三式中最簡單的（LHC）式。類推此每一個（LHC）之解是 $e^{At}\vec{c}$ 的形式；此 $\vec{c}$ 爲一常數向量。但是當 A 爲一矩陣時 e^{At} 表示什麼呢？而且（L）式之解又是什麼呢？這就是我們要討論的。

定義1. 對一矩陣函數 Φ，定義爲 $\Phi(t)=[\varphi_{ij}(t)]$ 則 $\Phi'(t)=[\varphi'_{ij}(t)]$，若每項導函數皆存在。

定義2. 一向量函數 φ 或一方程式 $\vec{x}=\vec{\varphi}(t)$ 是（L）之解。如果存在 a 及 b 使得對任一 $t\in(a,b)$，$\vec{\varphi}'(t)=A(t)\vec{\varphi}(t)+\vec{b}(t)$.

定義3. 如果當 $i=1,2,\cdots,n$，　$\vec{\varphi}_i(t)=\begin{bmatrix}\varphi_{1i}(t)\\ \varphi_{2i}(t)\\ \vdots\\ \varphi_{ni}(t)\end{bmatrix}$　是

（LH）的一解，則 $\Phi(t)=[\varphi_{ij}(t)]$，是（LH）的一個矩陣解。（M.S.）如果 $\vec{\varphi}_1,\vec{\varphi}_2,\cdots,\vec{\varphi}_n$ 向量函數是線性獨立，則 Φ 是（LH）的一個基本矩陣解。（F.M.S.）（fundamatal matrix solution）.

基本定理1B. 令 Φ 是（LH）的一個M.S. 則 Φ 是（LH）的一個（F.M.S.）若且唯若存在 $t\in(a,b)$ 使得 $\Phi(t)$ 之行列式不爲0；即 $\det(\Phi(t))\neq 0$.

基本定理2B. 如果 A 及 $\vec{b}$ 在 (a,b) 間爲連續，則對任一 $t_0\in(a,b)$ 且 $\vec{x}_0$；存在唯一（L）之解 $\vec{\varphi}$ 使得 $\vec{\varphi}(t_0)=\vec{x}_0$.

基本定理3B. 如 Φ 是（LH）的一個 F.M.S. 且 X 是（LH）的一個 M.S.，則存在一常數矩陣 C 使得 $X=\Phi C$.

摘要1. 令 Φ 是（LH）的一個 F.M.S. 且 $\vec{\varphi}$ 是（LH）的一解，且令 $X=[\vec{\varphi},\vec{0},\cdots,\vec{0}]$，則由3B存在一常數矩陣 C，使得 $X=\Phi C$；即存在一常數向量 $\vec{C}$ 使得 $\vec{\varphi}=\Phi C$。因此，（LH）之解形成一 n 度向量空間。

摘要2. 可以找到所有（L）之解，如果給一個（LH）的 F.M.S.（參考矩陣之應用）。如此我們只要會解（LH）就行了。

定理　令 A 在 (a,b) 內連續，則存在一（LH）的 F.M.S.

證明：當 $i=1,2,\cdots,n$，令 $\vec{e_i}$ 爲單位矩陣 I 中等 i 行之向量，且令 $t_0\in(a,b)$。現在對 $i=1,2,\cdots,n$，由 2B 可存在一個唯一解 $\vec{\varphi_i}$ 使 $\vec{\varphi_i}(t_0)=\vec{e_i}$。則 $\Phi(t)=[\vec{\varphi_1}(t),\vec{\varphi_2}(t)\cdots\phi_n(t)]$ 是（LH）的一個 M.S.。另外 $\det(\Phi(t_0))=\det(I)=1\neq 0$.。由 1B 知 Φ 是（LH）的一個 F.M.S.

定義 1. 當 $i,j=1,2,\cdots,n$，令 s_{ij} 是一級數。則矩陣級數定義爲 S；依 $S(n)=[s_{ij}(n)]$。

定義 2. 一矩陣級數 S 收斂至 $L=[l_{ij}]$，$S\to L$，如果當 $i,j=1,2,\cdots,n$，$s_{ij}\to l_{ij}$.

定義 3. 令 S 是一矩陣級數且 P_s 亦是一矩陣，級數定義爲 $P_s(k)=\sum\limits_0^k S(k)$。則 $\sum\limits_0^\infty S(k)$ 收斂至 L；$\sum\limits_0^\infty S(k)=L$，如 $P_s\to L$。

定義 4. 當給一矩陣 A，$e^{A(t)}$ 是一個矩陣級數等於 $\sum\limits_0^\infty A^k t^k/k!$，此 $A^0=I$；

即 $e^{A(t)}=I+At+A^2t^2/2!+A^3t^3/3!+\cdots\cdots$.

定理　對所有 A 與 t，e^{At} 是收斂。

證明：令 $A=[a_{ij}]$，$a=\max\{|a_{ij}|;i,j=1,2,\cdots,n\}$
$B=[a_{ij}]$（每一在矩陣 B 之項爲 a），$S(k)=A^kt^k/k!=[s_{ij}(k)]$，$T(k)=B^kt^k/k!=[t_{ij}(k)]$
則對任一 k 及所有 $i,j=1,2,\cdots,n$，$|s_{ij}(k)|<t_{ij}(k)$，則我們只須證明 $\sum\limits_{k=0}^\infty T(k)$ 是收斂。
因爲知 $B^0=I$，$B^1=[a]=a[1]$，$B^2=a^2[1]^2=a^2[n]=na^2[1]=na[a]=naB$；可知 $B^k=n^{k-1}a^{k-1}B=[n^{k-1}a^k]$。於是對任一 k 且 $i,j=1,2,\cdots,n$，時 $t_{ij}^{(k)}=n^{k-1}a^kt^k/k!$ 應用"比例試法"（Ratio Test），我們得到 $t_{ij}(k+1)/t_{ij}(k)=n^ka^{k+1}t^{k+1}k!|(k+1)!n^{k-1}a^kt^k=nat/k\to o$ 當 $k\to\infty$。因此 e^{At} 是收斂對所有 A 及 t。

摘要　當 A 和 t 都是複數　前一定理　仍能成立。另外因 e^{At} 中每一項是一乘冪級數；我們可以逐項微分而得下列結果。

即：$d(e^{At})/dt=A+A^2t+A^3t^2/2!+A^4t^3/3!+\cdots$
$$=A(I+At+A^2t^2/2!+A^3t^3/3!+\cdots)=Ae^{At}。$$

定理　（LHC）$\vec{x}'=A\vec{x}$ 的一個 F.M.S. 是 $\Phi(t)=e^{At}$。

證明：顯然 e^{At} 是（LHC）的一 M.S. 而且 $\det(e^{A0})=\det(I)\neq 0$，所以 e^{At} 是一 F.M.S.。

所有（LHC）的解都是 $e^{At}C$ 這種形式。當然這解的每一項都是由A的乘冪級數來決定。因此我們要找一個明顯表示 e^{At} 的方法。

例1　令 $A=\begin{bmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{bmatrix}$　則 $A^0=I$，$A^1=A$，$A^2=\begin{bmatrix} a^2 & 2a & 1 \\ 0 & a^2 & 2a \\ 0 & 0 & a^2 \end{bmatrix}$

$A^3=\begin{bmatrix} a^3 & 3a^2 & 3a \\ 0 & a^3 & 3a^2 \\ 0 & 0 & a^3 \end{bmatrix}$　由數學歸納法知　$A^k=\begin{bmatrix} a^k & ka^{k-1} & k(k-1)a^{k-2} \\ 0 & a^k & ka^{k-1} \\ 0 & 0 & a^k \end{bmatrix}$

於是　$e^{At}=\left[\begin{array}{l} 1+at+a^2t^2/2!+\cdots,\ t+2at^2/2!+3a^2t^3/3!+\cdots,\ t^2/2+3at^3/3!+12a^2t^2/2\cdot4!+\cdots \\ \qquad\qquad\qquad\qquad\text{以此對角線為軸而對稱} \\ \qquad O \end{array}\right]$

$$=\begin{bmatrix} e^{at} & te^{at} & t^2e^{at}/2 \\ 0 & e^{at} & te^{at} \\ 0 & 0 & e^{at} \end{bmatrix}=e^{at}\begin{bmatrix} 1 & t & t^2/2 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{bmatrix},$$

例2　相似地令 $A=\begin{bmatrix} a & 1 & 0 & 0 & \cdots & 0 \\ 0 & a & 1 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots & 0 & a \end{bmatrix}$，同理可得知

$e^{At}=e^{at}\left[\begin{array}{l} 1\quad t\quad t^2/2\ \cdots\cdots\ t^{n-1}/(n-1)! \\ \qquad\text{以此對角線為軸而對稱} \\ \qquad O \end{array}\right]$

定義　像例2形式的矩陣A稱之為爵當圖形矩陣。（Jordan block matrix）。在 對角線（main diagonal）上，一矩陣包含爵當圖形矩陣為一爵當矩陣。（Jordan matrix）.

例示 $A=\left[\begin{array}{ccc|c|ccc} 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 5 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{array}\right]$ 是一爵當矩陣。

如果令 $A=\begin{bmatrix} B & & \\ & C & \\ & & D \end{bmatrix}$，則 $A^k=\begin{bmatrix} B^k & & \\ & C^k & \\ & & D^k \end{bmatrix}$ 且 $e^{At}=\begin{bmatrix} e^{Bt} & & \\ & e^{Ct} & \\ & & e^{Dt} \end{bmatrix}$

從上一例示我們了解，當A是一爵當矩陣時，我們如何明白的表示 e^{At}。 但是如果是其他的情形將如何呢？對這個問題我們就要用到線性代數上一個很重要的方法。

定理 （爵當定理）對任一矩陣A，恒存在一非退化矩陣P（nonsinguler matrix）使得 $P^{-1}AP$ 爲一爵當矩o。（參考〔3〕）

這個定理可以用來找 e^{At}，當A不是一爵當矩陣。

定理 令P爲一非退化矩陣。如 Ψ 是 $\vec{y}'=P^{-1}AP\vec{y}$ 的一個 F.M.S.，則 $P\Psi$ 是 $\vec{x}'=A\vec{x}$ 的一個F.M.S.。

證明 Ψ 是 $\vec{y}'=P^{-1}AP\vec{y}$ 的一個 F.M.S. 則存在t使得 $\det[\Psi(t)]\neq 0$，且 $\Psi'=P^{-1}AP\Psi$，則存在t使得 $\det(P\Psi(t))=\det(P)\det(\Psi(t))\neq 0$，且 $(P\Psi)'=P\Psi'=AP\Psi$，則 $P\Psi$ 是 $\vec{x}'=A\vec{x}$ 的一個 F.M.S.

定理 令P爲一非退化矩陣。則對所有t及A， $e^{At}=Pe^{P^{-1}APt}P^{-1}$。

證明 $e^{P^{-1}APt}$ 是 $\vec{y}'=P^{-1}AP\vec{y}$ 的一 F.M.S.。則 $Pe^{P^{-1}APt}$ 是 $\vec{x}'=A\vec{x}$ 的一個 F.M.S.。則存在一常數矩陣C使得對所有t，$Pe^{P^{-1}APt}=e^{At}C$，則（令 $t=0$），$P=C$；即 $e^{At}=Pe^{P^{-1}APt}P^{-1}$。

摘要 注意在前一個微分方程式定理中我們利用了一個矩陣的結果。另外在最後一定理中證明 $\vec{x}'=A\vec{x}$ 之解很明白地要找一矩陣P（用爵當定理），而P是由A的特徵值（eigenvalue）來決定。

3. 應用於週期系統

令 $P^{-1}AP$ 爲一爵當矩陣，此 P 爲一非退化矩陣。則 $\Phi = P e^{P^{-1}APt} P P^{-1} = P e^{P^{-1}APt}$ 爲（LHC）$\vec{x}' = A\vec{x}$ 的一個 F.M.S.。因 Φ 爲（LHC）之一 F.M.S. 所有（LHC）之解是由 Φ 決定，且其解之性質決定於 Φ。$P^{-1}AP$ 的對角線項目（diogonal member）是 A 的特徵值，且 Φ 的某一行是下列形式。

$$\vec{\varphi} = P e^{\lambda t} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ t^m/m! \\ t^{m-1}/(m-1)! \\ \vdots \\ t \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$ 此 λ 是 A 的一個特徵值。

因此解的特殊性質決定於 λ 及每一個 λ 一爵當圖形矩陣 $P^{-1}AP$ 之序（order）。例示；如 λ 之實部小於 0，即 $Re(\lambda) < 0$ 則 $\vec{\varphi} \to \vec{0}$ 當 $t \to \infty$；如 λ 之實部大於 0，即 $Re(\lambda) > 0$，則 $\vec{\varphi}$ 沒界限（unbounded），當 $t \to \infty$；如 $m = Re(\lambda) = 0$，則 $\vec{\varphi}$ 是一週期函數。

現令 A 是一連續函數以 T 爲週期且考慮某一齊次線性方程系統（lineur homogenous system）之解。

（LHP）$\vec{x}' = A(t)\vec{x}$.

定理（Tloquet）　存在一個矩陣函數 P 以 T 爲週期且以 B 爲爵當矩陣，使得 $\Gamma(t) = P(t) e^{Bt}$ 是（LHP）之一個 F.M.S.（參考〔5〕）。

在這種情況，當 B 知道則（LHP）之性質就知道。找 B 的方法就如解（LHP）的特徵指數（characteristic exponents）的方法。對此種方程組已經有很多被做了而且也正有人正在做。（參考〔2〕），（LHP）的結果常被決定一非線性系統（nonlinear systems）的解的性質。（參考〔1〕）。

4. 參考資料

討論這篇論文最主要的內容的一本書是在〔5〕中。

〔1〕 Burton, T. A. and Townsend, C.G. "Stability Regions of the Forced Lienard Equation" J. London Math. Soc. (2), 3 (1971), 393-402

〔2〕 Cesari, L., Asymptotic Beharior and Stability Problems in Ordinary Differential Equations, Academic Press, 1963.

〔3〕 Hoffman, K. and Kunze R. Linear Algebra Printece-Hall 1965.

〔4〕 Pontryogin, L., Ordinary Differential Equations. Addison-Wesley, 1962

〔5〕 Wilson, H., Ordinary Differential Equations, Addison-Wesley, 1971.

可解群之一特性

常法徽

於 Sylow定理，若G爲一有限群，

$$|G| = p^m a \quad 及 \quad (p^m, a) = 1$$

時，則G中至少有一級爲 b^m 之子群，且級爲 p^m 之任意二子群均共軛。今所討論者爲P.Hall 定理，即若可解群之級爲ab 及（a，b）＝1時，則G中至少有一級爲a之子群，且級爲a之任意二子群共軛。

定義1　於群G，若有一有限子群鏈：

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

而 $G_i \triangle G_{i-1}$ 及 G_{i-1}/G_i 爲亞伯群時，稱G爲可解群（Solvable group）。於此 i＝1，2，…，n，e爲G之么元素。

定義2　設H爲群G之子群，若對於每一同構　$f: G \longrightarrow G$

均有 f(H)⊂H時，稱H爲G之特徵子群（Characteristic subgroup）。

若對於每一同態

$$f: G \longrightarrow G$$

均有 f(H)⊂H時，稱H爲G之全不變子群（Fully invariant subgroup）.

由此定義，知若H爲G之全不變子群，則H爲G之特徵子群。G之每一特徵子群均爲G之正則子群（Normal subgroup）.

引1　若H⊂N△G，且H爲N之特徵子群，則　H△G

因H爲N之特徵子群，故H△N，是以H△N△G，但不能就說　H△G，今就同構

$$f: N \longrightarrow N$$

$$f(n) = g^n g^{-1},\ g \in G,\ (g^n g^{-1} \in N)$$

論之，則對於每h∈H，均有

$$f(h) = g^h g^{-1} \in H \quad (因\ f(H) \subset H)$$

即　$g^H g^{-1} \subset H$

故　H△G

引2　於任意一群G，則Z(G)爲G之特徵子群。

設

$$f: G \longrightarrow G$$

爲任意一同構，Z∈Z(G)，g∈G則

$$f(z) = f(gzg^{-1})$$
$$= f(g) f(z) (f(g))^{-1}$$

因f爲G映成G之同構，故f(z)∈G，是以f(z)∈Z(G)而　f(Z(G))⊂Z(G)。

引3　設G爲有限群，則其每一正則p-Sylow子群均爲G之全不變子群。

設　$f: G \longrightarrow G$

爲任意一同態，P爲G之正則p-Sylow子群。

設x∈P，則對於某整數r（r≧0）x之級爲 p^r，f(x)之級爲 p^r 之約數，令之爲 p^{r_1}，

則G有p^{n}級之子群H，於此H爲p——子群，其必含於某一p-Sylow 子群內。

因　　$P \triangle G$

$\therefore$　　$gPg^{-1}=P$，$g \in G$

因G中所有p-Sylow 子群均共軛，P之共軛群爲gPg^{-1}，故G中之p-Sylow 子群只P一個。

$\therefore$　$f(x) \in P$

即　$f(P) \subset P$，而P爲G之全不變子群。

定義3　設N爲群G之正則子群，若

(1)　$N \neq \{e\}$

(2)　N不包含眞子群爲G之正則子群。

稱N爲G之最小正則子群（Minimal normal subgroup）.

引4　於可解之有限群G中，每一最小正則子群N爲某一p群。

設N′爲N之換位子群（Commutator subgroup），即

$N' \subset N \triangle G$

令　$f: N \longrightarrow N$爲任意一同態，$x \in N'$

$x=a^{-1}b^{-1}ab$.

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

$f(a)f(b) \in N'$

$\therefore$　$f(N') \subset N'$

即N′爲N之全不變子群。由引1，知$N' \triangle G$。

因N爲G之最小正則子群，則抑$N'=N$或$N'=\{e\}$，因N爲可解群G之子群，故N爲可解群，則必

$N' \neq N$。

蓋若$N'=N$，則$(N')'=N$，…，顯知N不爲可解群，此爲矛盾。故必

$N'=\{e\}$

由是，知N爲亞伯群。因每一有限亞伯群可表爲諸Sylow子群P等之直積（Direct product）。

因N爲亞伯群，

故　$P \triangle N$

由引3，P爲N之全不變子群，由引1，知

$P \triangle G$

然以N爲G之最小正則子群，則必N爲-p-Sylow 子群。

故N爲p群。

定理，設G爲可解群，其級爲ab，且$(a, b)=1$。則G至少含有a級之一子群，且級爲a之任意二子群均共軛。

證　於$|G|$上用歸納法證明之。

情形1

設　$H \triangle G$及$|H|=a_1b_1$，$a_1|a$，$b_1|b$，$b_1<b$.

因G爲可解群，$H \triangle G$，則G／H亦爲可解群（於此不加證明）。

$$|G/H|=\frac{ab}{a_1b_1}=\frac{a}{a_1}\frac{b}{b_1} \leq |G|,\ \left(\frac{a}{a_1},\frac{b}{b_1}\right)=1$$

在僅只$|G/H|=|G|$，即$|H|=1$，此定理成立。

若 $|G/H|<|G|$，由歸納法之假設，知 G/H 有級爲 $\frac{a}{a_1}$ 之一子群，令之爲 $\bar{A}/H$ 。因 G/H 爲可解群，故 $\bar{A}/H$ 亦爲可解群。易知 $\bar{A}$ 爲G之可解子群，其級爲

$$\frac{a}{a_1}\, a_1 b_1 = ab_1 < ab\ ,\ (a, b_1) = 1$$

$(\bar{A})$ 再由歸納法假設知 $\bar{A}$ 中有級爲a之子群。然以 $\bar{A}\subset G$ 即G中含有級爲a之子群。

次設A及 A_1 同爲G之a級子群，令

$$k = |AH|$$

則 $k\mid ab$，

又以 $A/H\cap A \quad AH/H$

故 $k\mid |A|\,|H|$，即 $k\mid aa_1b_1$

因 $(a, b)=1$，故 $k\mid ab_1$

由Lagrange定理，知

$[AH:H]=|AH|/|H|$，

$[AH:A]=|AH|/|A|$.

故 $k=|AH|$ 可被a及被 a_1b_1 除盡，即 $a\mid k$，$a_1b_1\mid k$，因 $(a, b)=1$，故 $ab_1\mid k$ 由是

$$k = ab_1\ ,$$

是以 $|AH| = ab_1$，

同理 $|A_1H| = ab_1$。

今 $H\triangle G$，A爲G之子群，故AH爲G之子群，是以

$$AH/H \text{ 及 } A_1H/H$$

均爲 G/H 之子群。於此 $|G/H| = \frac{a}{a_1}\,\frac{b}{b_1}$，$\left(\frac{a}{a_1}, \frac{b}{b_1}\right)=1$，$AH/H$ 及 A_1H/H 之級同爲 $\frac{ab_1}{a_1b_1} = \frac{a}{a_1}$

因 $|G/H|<|G|$，由歸納法之假想，知 AH/H 與 A_1H/H 共軛。

故有 $\bar{x}\in G/H$ （$\bar{x}=xH$）便

$$\bar{x}\, AH/H\, \bar{x}^{-1} = A_1H/H 。$$

設 $a\in A$，某 $a_1\in A$ 有

$$\bar{x}\, aH\bar{x}^{-1} = a_1H 。$$

即 $xax^{-1}H = a_1H$

$xax^{-1} = a_1h_1$ （某 $h_1\in H$）

$xa = a_1h_1x$

設 $h\in H$，則

$$xah = a_1h_1xh$$

$$xahx^{-1} = a_1h_1xhx^{-1} = a_1h_1h_2$$

（$xhx^{-1}=h_2\in H$，此因 $H\triangle G$）

$\therefore\ xAHx^{-1}\subset A_1H$。

次設 $a_1\in A$ 則有某 $a\in A$ 便

$$a_1H = \bar{x}\, aH\, \bar{x}^{-1}$$

則 $a_1H = xax^{-1}H$

$a_1 = xax^{-1}h_1$ （某 $h_1\in H$）

令 $h\in H$ 則 $a_1h = xax^{-1}h_1h = xah_2x^{-1}$

（$h_2x^{-1} = x^{-1}h_1h$，此因 $H\triangle G$）

$\therefore\ A_1H\subset xAHx^{-1}$ 。

是以有

$$xAHx^{-1} = A_1H$$

即AH與A_1H共軛

今由上式，xAx^{-1} 及A_1同爲可解群A_1H之子群其級同爲a，且以 $|A_1H| = ab_1 < |G|$ (a, b_1) = 1。由歸納法之假設知 xAx^{-1} 與 A_1 共軛，然 xAx^{-1}與A共軛，故A與A_1 共軛。故證明了第一種情形。

若H爲G之某一眞正則子群，bXH($|H| = a_1b_1$，$a_1 | a$，$b_1 | b$，$b_1 < b$)時，此即爲第一種情形。玆設附於G之每一眞正則群H均有 $b \nmid |H|$。

若H爲G之一最小正則子群，由引4，知H爲一p群。故對於某質數p，有

$$|H| = p^m。$$

因 $b | |H|$，故 $b | p^m$，則必 $b = p^m$。蓋若 $b \neq p^m$，例如 $b = p^{m-1}$，則

$$|H| = p^m = pp^{m-1}$$
$$= a_1b$$

得 $p = a_1$，即p同爲a，b之公約數，此爲矛盾。

由 $b = p^m$，知

$$|G| = ab = ap^m \quad (a, p) = 1$$

因 $|H| = p^m$ 及 $p^m = b$，故H爲G之p-Sylow子群，因H△G，故H爲G之正則p-Sylow子群，若H_1爲另一p-Sylow子群則H與H_1 共軛，是以某 $x \in G$ 有

$$H_1 = xHx^{-1}$$

因H△G，故H_1=H，即如是之子群爲唯一

情形2　$b | |H|$，H爲G之唯一最小正則子群之情形於此 $|H| = p^m$。

因G爲有限群，G之每一正則子群（除{e}外）必含有G之一最小正則子群，故G之每一眞正則子群均必包含H。

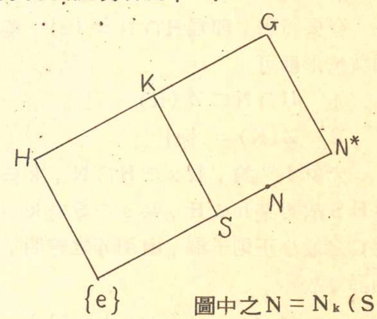
令K／H爲G／H它最小正則子群，由引4，知對於某負數q有

$$|K/H| = q^n$$

故　$|K| = p^mq^n$　（p，q互質）

令S爲K之一q－Sylow子群，$|S| = q^n$，令　$N^* = N_G(S)$

於此，先要證明者爲 $|N^*| = a$.



圖中之 $N = N_K(S)$

因 $H \cap S = \{e\}$，$HS \subset K$

$\therefore |HS| = |H||S| = p^mq^n = K$

故HS＝K

因K／H△G／H，故K△G，然以 $S \subset K$，故對於每 $x \in G$ 均爲

$$xSx^{-1} \subset K$$

$\{xSx^{-1} \mid x\in G\}$ 中，每一 xSx^{-1} 均為 K之子群且共軛於S，令 $C=[G:N^*]$，則

$$C=[G:N^*]$$
$$=[K:N]$$
$$=[HS:N]$$
$$=[HN:N]\ (N=N_k(S)\quad S\subset N)$$
$$=[H:H\cap N]\ (\text{由}\ |HN|=\frac{|H|\,|N|}{|H\cap N|})$$

若能證明 $H\cap N=\{e\}$，則 $C=|H|=p^m=[G:N^*]$，而

$$N^*=\frac{ab}{p^m}=\frac{ab^m}{p^m}=a\ 。$$

今要證者，即為 $H\cap N=\{e\}$，能證明下列兩種情形即可

1° $H\cap N\subset Z(K)$

2° $Z(K)=\{e\}$

先就1° 論，設 $x\in H\cap N$，$k\in K$，因 $K=HS$ 故對某 $h\in H$，某 $s\in S$ 有 $k=hs$。因H為G之最小正則子群，由引4之證明，知其為亞伯群，故

$$xh=hx\qquad(x,\ h\in H)$$

又 $x^{-1}s^{-1}xs=(x^{-1}s^{-1}x)s$

因 $x\in N$，$N=\{x\in K \mid xS=Sx\}$，則 $x^{-1}s^{-1}x\in S$，故

$$x^{-1}s^{-1}xs\in S$$

又 $x^{-1}s^{-1}xs=x^{-1}(s^{-1}xs)\in H$ 因($H\triangle G$)

故 $x^{-1}s^{-1}xs\in S\cap H$

但 $S\cap H=\{e\}$，

故 $x^{-1}s^{-1}xs=e$

$$xs=sx$$

$$xk=x(hs)=(xh)s=(hx)s=h(xs)=h(sx)=kx$$

即 $x\in Z(K)$

即 $H\cap N\subset Z(K)$

就2° 論之，要證明 $Z(K)=\{e\}$。

因 $Z(K)\subset K\triangle G$，由引2，知 $Z(K)$ 為K之特徵子群；由引1，則 $Z(K)\triangle G$。若 $Z(K)\neq\{e\}$，則 $Z(K)$必包含一最小正則子群，故

$H\subset Z(K)$。

由 $K=HS$ 及 $H\subset Z(K)$ 以證明 $S\triangle K$：

設 $s\in S$，$k\in K$ 則

$$ksk^{-1}=(hs_1)s(hs_1)^{-1}\quad(k=hs_1)$$
$$=h(s_1ss_1^{-1})h^{-1}$$
$$=hs_2h^{-1}\quad(s_2=s_1ss_1^{-1})$$

因 $s_2\in K$，$h\in Z(K)$

$\therefore\ hs_2h^{-1}=s_2$

即 $hsk^{-1}\in S$，故 $S\triangle K$，由引3知

即 $S\triangle K\triangle G$，因S為q-Sylow子群，故S為K之全不變子群。由引1，則 $S\triangle G$，故

$H\subset S$

但 $H\cap S=\{e\}$，

此為矛盾，故必 $Z(K)=\{e\}$。

最後，設 A_1為G中級a之另一子群，由此知

$$a\mid |A_1K|,$$

又 $|K|\mid |A_1K|$，

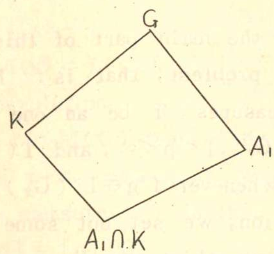
故 $p^m q^n \mid |A_1K|$

然以 $p^m = b$，故

$$\begin{cases} a \mid |A_1K|, \\ b \mid |A_1K|, \quad \text{（於此}(a, b) = 1\text{）} \end{cases}$$

則 $A_1K = G$

由下圖考之：



因 $K \triangle G$，

故 $G/K = A_1K/K \cong A_1/A_1\cap K$

故 $|A_1K|\,|A_1\cap K| = |A_1|\,|K|$

即 $|A_1\cap K| = \dfrac{abq^n}{ab} = q^n$

因S與G之 q－Sylow 子群，其級爲 q^n，故 $A_1\cap K$ 與S共軛。

因之有某 $g\in G$ 使 $A_1\cap K = gSg^{-1}$

$N_G(A_1\cap K) = \{x\in G \mid x(A_1\cap K) = (A_1\cap K)x\} = \{x\in G \mid xgSg^{-1} = gSg^{-1}x\} = \{x\in G \mid g^{-1}xgS = Sg^{-1}xg\}$

∴ $g^{-1}xg \in N_G(S)$ 即 $g^{-1}N_G(A_1\cap K)g \subset N_G(S)$.

由 $A_1\cap K = gSg^{-1}$ 知 $S = g^{-1}(A_1\cap K)g$

$N_G(S) = \{y\in G \mid y(g^{-1}(A_1\cap K)g) = (g^{-1}(A_1\cap K)g)y\} = \{y\in G \mid gyg^{-1}(A_1\cap K) = (A_1\cap K)gyg^{-1}\}$

∴ $gyg^{-1} \in N_G(A_1\cap K)$

$y \in g^{-1}(N_G(A_1\cap K))g$，故

$N_G(S) \subset g^{-1}(N_G(A_1\cap K)g$

故 $N_G(S) = g^{-1}(N_G(A_1K))g$

今 $N_G(S) = N^*$，$N_G(A_1\cap K) = A_1$

（因 $A_1\cap K \triangle A_1$）

故 N^* 與 A_1 共軛，

故G中級爲a之任意二子群共軛。

證明完。

Multipliers on Some Topological Linear Spaces

Prepared by Lien Ming-Chiao （連明嬌）

1. Introduction and preliminaries

This paper contains three sections. Section 2 is the main part of this paper, in which we prove a theorem related to isomorphism problem; that is: Let G_1 and G_2 be locally compact groups with left Haar measures, T be an one to one, bipositive linear transformation from $L^p(G_1)$ onto $L^p(G_2)$, $1<p<\infty$, and $T(f*g)=Tf*Tg$ whenever $f*g\in L^p(G_1)$, $T^{-1}(f*g)=T^{-1}f*T^{-1}g$ whenever $f*g\in L^p(G_2)$. Then G_1 and G_2 are topologically isomorphic. In this section, we set out some notations and definitions which remain standard throughout this paper.

1.2 L^p Spaces ($1\leq p\leq\infty$)

Let G be a locally compact group with left Haar measure dx. If G is compact, dx is assumed to be normalized so that $\int_G dx=1$. If G is locally compact Abelian, we denote $\hat{G}$ the dual group of G.

Let $L^p(G)$, $1\leq p<\infty$, be the Banach space of all p-th power absolute integrable functions with respect to dx, the norm of $L^p(G)$ is given by

$$\|f\|_{L^p}=\|f\|_p=\left[\int_G |f(x)|^p\,dx\right]^{\frac{1}{p}},$$

and $L^\infty(G)$ denotes the Banach space of all essential bounded functions and normed by

$$\|f\|_{L^\infty}=\|f\|_\infty=\text{loc. ess. sup}\,|f(x)|.$$

Denote by $C_0=C_0(G)$ the space of all continuous functions which vanich at infinity and by $C_c=C_c(G)$ tha space of all continuous functions with compact supports. The topology of C_0 is the topology of uniform convergence defined by restricting to C_0 with the norm $\|\cdot\|_\infty$. The topology of C_c is the topology obtained by regarding C_c as the internal inductive limit of its subspace

$$C_{c,K} = \{ f \in C_c \ ; \ \mathrm{supp}\ f \subset K \},$$

where K ranges over all the compact subsets of G and each of $C_{c,K}$ being regarded as a Banach space with the supremum norm.

We define the left and right translations by

$$\tau_a f(x) = f(a^{-1}x),$$

$$\rho_a f(x) = f(xa^{-1}).$$

1.3 Convolutions

Let $M = M(G)$ denote the space of all complex regular Borel measures on G with the weak topology $\sigma(M, C_c)$, and $M_{bd} = M_{bd}(G)$ be the subspace of M formed of those measures μ such that

$$\|\mu\| = |\mu|(G) < \infty .$$

For the space M_{bd}, together with this norm, is the dual of C_0. M_L^p [resp. M_R^p] denotes the measures $\mu \in M$ such that $\|\mu * f\|_p \leq$ const. $\|f\|_p$ [resp. $\|f*\mu\|_p \leq$ const. $\|f\|_p$], for all $f \in C_c$. If $\lambda, \mu \in M(G)$ and for any Borel subset E of G, we define

$$\lambda * \mu(E) \underset{\leftarrow}{=} \int_G \mu(s^{-1}E)\, d\lambda(s)$$

Convolution of function f and measure μ by

$$f*\mu(x) \underset{\leftarrow}{=} \int_G \Delta(y) f(xy^{-1})\, d\mu(y)$$

and

$$\mu * f(x) \underset{\leftarrow}{=} \int_G f(y^{-1}x)\, d\mu(y),$$

where $\Delta(y)$ denote the modular function.

If f, g are functions, we define

$$f*g(x) = \int_G g(y^{-1}x) f(y)\, dy.$$

clearly,

$\tau_a(f*g) = \tau_a f*g$,

$\rho_a(f*g) = f*\rho_a g$.

1.4 Positive mappings

A mapping T from a function space into a function space is called positive, if $Tf \geq 0$ almost everywhere whenever $f \geq 0$ almost everywhere. If T is an one-one onto mapping, T and T^{-1} are positive, we call T bipositive.

1.5 Multipliers

Let G be a locally compact group, X, Y be topological linear spaces of functions defined on G, then a continuous linear transformation T from X to Y is called a left (right) multiplier for the pair (X, Y) whenever $T\tau_s = \tau_s T$ ($T\rho_s = \rho_s T$) for each $s \in G$. If T is both a left and a right multiplier, then we call simply T a multiplier.

We denote the set of all left (right) multipliers for $(L^p(G), L^p(G))$ by $M_l(L^p)$ [resp. $M_R(L^p)$] and the set of all multipliers for $(L^p(G), L^p(G))$ by $M(L^p)$, $1 \leq p \leq \infty$.

Denote by $M_l(L^p, L^q)$, $M(L^p, L^q)$ the set of all left (right) multipliers for (L^p, L^q), $M(L^p, L^q)$ the set of all multipliers for (L^p, L^q), $1 \leq p, q \leq \infty$.

2. Isomorphism theorems relate to multipliers

2.1 Introduction

Let G_1 and G_2 be locally compact (Hausdorff) groups, and $E(G_i)$ denote the function space over the group G_i.

The isomorphism problem consists of that at what conditions on the mapping of $E(G_1)$ onto $E(G_2)$ can deduce to the isomorphic topological groups G_1 and G_2. First kawada [5] proved that if there exists a bipositive isomorphism of $L^1(G_1)$ onto $L^1(G_2)$, then G_1 and G_2 are topologically isomorphic.

Wendel [10][11] proved the isomorphic groups from the hypothesis that if there is a norm nonincreasing isomorphism of $L^1(G_1)$ onto $L^1(G_2)$. Later Edwards [2] consider the situation where the groups G_i ($i=1, 2$) are compact and there exists a bipositive isomorphism of $L^p(G_1)$ onto $L^p(G_2)$ ($1\leq p<\infty$) and proved under these conditions, the groups are topologically isomorphic. In Edwards [2], he asked whether the compact groups G_1 and G_2 are necessarily isomorphic if the bipositive is replace by isometry. The affirmative answer to this questien was given by Strichartz [9]. Further, Parrott [7] proved the question for general locally compact groups G_1 and G_2 under the isometric tranformation of $L^p(G_1)$ onto $L^p(G_2)$ ($1\leq p<\infty$, $p\neq 2$) and some additional conditions which are necessary for the Lebesgue space L^p (Indeed, $L^p(G)$ needs not be an algebra if G is not compact). We ask that whether the Parrott's result holds if the isometry is replaced by bipositive. That is the same question that in Edwards [2], whether the locally compact groups G_1 and G_2 are necessarily isomorphic if we assume that there is an injective bipositive linear mapping from the Banach space $L^p(G_1)$ onto the Banach space $L^p(G_2)$. For this purpose we give the affirmative answer in this paper.

Some another isomorphic problems were given by Johnson [4], Gaudry [3] and Strichartz [8].

Johnson [4] showed on the bounded regular measure algebra under the isometric isomorphism. Gaudry [3] proved on the multiplier algebra $M(L^p)$ $1\leq p<\infty$ under the condition of isometric isomorphism and bipositive isomorphism.

2.2 The main theorem

For convenient, we state the following

Lemma A: If T is a positive linear transformation of $L^p(G_1)$ into $L^p(G_2)$ ($1\leq p\leq\infty$), then T is continuous.

Proof: we give the alternative proof of Brainerd and Edwards [1] as following: If T were not bounded, these would exist $\{f_n\}$ in $L^p(G_1)$ such that

$$\| f_n \|_{L^p(G_1)} \leq 1 \quad \text{and} \quad \| Tf_n \|_{L^p(G_2)} \geq n^3$$

Since T is positive, $| Tf_n | < T | f_n |$, and so we may assume that $f_n \geq 0$. The series $f = \sum_{n=1}^{\infty} n^{-2}\ Tf$ converges in $L^p(G_1)$ and $f_n < n^2 f$, we have $0 \leq Tf_n \leq n^2\ Tf$ and

$$n^2 \| Tf \|_{L^p(G_2)} \geq \| Tf_n \|_{L^p(G_2)} \geq n^3$$

implies $\| Tf \|_{L^p(G_2)} \geq n$ which is a contradiction for n may be large enough.

We shall need the result of Brainerd and Edwards [1 ; Theorem 3.5] later, thus we state as following.

Theorem B: If T is a positive linear map of L^p into L^p ($1 \leq p \leq \infty$) which commute with ρ_a [resp. τ_a], then there exists a positive $\mu \in M_L{}^p$ [resp. $M_R{}^p$] such that

$Tf = \mu * f$ [resp. $f * \mu$]

for $f \in C_c$; if $p < \infty$, the above identity holds for $f \in L^p(G)$. And conversely.

Now we are going to give our main theorem as following.

Theorem: Let G_1 and G_2 be locally compact groups with left Haar measures, Let T be an one to one, bipositive linear transformation from $L^p(G_1)$ onto $L^p(G_2)$, where $1 < p < \infty$, and satisfying $T(f*g) = Tf*Tg$ whenever $f*g \in L^p(G_1)$ and $T^{-1}(f*g) = T^{-1}f*T^{-1}g$ whenever $f*g \in L^p(G_2)$. Then G_1 and G_2 are topologically isomorphic.

Proof of the theorem:

As T is an one to one linear mapping of $L^p(G_1)$ onto $L^p(G_2)$, it is immediately that $T\rho_a T^{-1}$ is a linear operator on $L^p(G_2)$ for every $a \in G_1$.

If $f, g \in L^p(G_2)$ and $f*g \in L^p(G_2)$, we have $(T\rho_a T^{-1})(f*g) = T\rho_a(T^{-1}f*T^{-1}g)$ $= T(T^{-1}f*\rho_a T^{-1}g) = f*T\rho_a T^{-1}g$.

And for $b \in G_2$,

$$\tau_b(T\rho_a T^{-1})(f*g) = \tau_b f * T\rho_a T^{-1} g,$$

and

$$(T\rho_a T^{-1})\tau_b(f*g) = (T\rho_a T^{-1})(\tau_b f*g) = \tau_b f*(T\rho_a T^{-1})g.$$

Therefore,

$$\tau_b(T\rho_a T^{-1})(f*g) = (T\rho_a T^{-1})\tau_b(f*g)$$

whenever $f*g \in L^p(G_2)$, where $a \in G_1$, $b \in G_2$.

Since C_c*C_c is norm dense in L^p, we see that $T\rho_a T^{-1}$ commutes with left translation for each $a \in G_1$.

As T and T^{-1} are positive linear transformation, we see that T and T^{-1} are bounded by Lemma A. Hence $T\rho_a T^{-1}$ is a bounded positive linear operator on $L^p(G_2)$ which commutes with τ_b, $b \in G_2$. Then there exist positive measures μ, $v \in M_R^p(G_2)$ such that

$$(T\rho_a T^{-1})f = f*\mu \qquad \text{for } f \in L^p(G_2),$$

and

$$(T\rho_{a^{-1}} T^{-1})f = f*v \qquad \text{for } f \in L^p(G_2).$$

(by Theorem B)

Since

$$(T\rho_{a^{-1}}T^{-1})(T\rho_a T^{-1})f = f*\mu*v \qquad \text{for } f \in L^p(G_2),$$

and

$$(T\rho_{a^{-1}}T^{-1})(T\rho_a T^{-1})f = f = f*\delta_0 \qquad \text{for } f \in L^p(G_2),$$

We have

$$\mu*v = \delta_0 .$$

Next, we prove μ, v are Dirac measures.

Suppose that b_1 and b_2 are two distinct points of the support of μ, c is a point of the support of v ($b_1, b_2, c \in G_2$). Since G_2 is Hausdorff, we can choose a neighborhood U of the identity $e_2 \in G_2$ such that $b_1 U c U \cap b_2 U c U = \phi$. choose a function $\phi \in C_c(G_2)$ with $0 \leq \phi \leq 1$ such that $\phi(e_2) = 1$ and support $\subset$ U (by Urysohn lemma). Define.

$$\mu_1 = (\tau_{b_1}\phi) + (\tau_{b_2}\phi)\mu ,$$
$$v_1 = (\tau_c \phi) v$$

then μ_1, v_1 are positive, nonzero measures, and it is obvious that $v_1 \leq v$, $\mu_1 \leq \mu$, and

$$\mu_1 * v_1 \leq \mu * v = \delta_0 .$$

But $\mu_1 * v_1$ is a positive measure with at least two distinct points b_1c, b_2c in its support. We can show this by the following:

$$\begin{aligned} \mu_1 * v_1 (b_1 c) &= \int_{G_2} v_1(y^{-1} b_1 c)\, d\mu_1(y) \\ &\geq v_1(b_1^{-1} b_1 c)\mu_1(b_1) \\ &\geq \mu(b_1) v(c) \\ &> 0 \end{aligned}$$

Similarly, $\mu_1 * v_1 (b_2 c) \geq \mu(b_2) v(c) > 0$.

Since δ_0 has only one point support, it deduce a contradiction.

Therefore μ, v are Dirac measures.

$$\text{Let } \delta_a(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{otherwise} \end{cases},$$

then $\quad f * \delta_a = \rho_a f$.

Since μ depends on a, we denote the support of μ by $\Lambda(a)$ and the mass of μ by $\lambda(a)$, then $\Lambda(a) \in G_2$, and

$$f * \mu = f * \lambda(a) \delta \Lambda(a) = \lambda(a) \quad \rho \Lambda(a) f .$$

Hence we obtain

$$(T \rho_a T^{-1}) f = \lambda(a) \quad \rho \Lambda(a) f, \text{for } f \in L^p(G_2) .$$

Since $T\rho_a T^{-1}$ is a positive linear operator, $\lambda(a) \geq 0$ and Λ is a mapping from G_1 to G_2.

It remains to prove that Λ is an algebra isomorphism and a bicontinuous mapping from G_1 onto G_2.

It is obvious that Λ and λ are homomorphisms. Indeed,

$$\lambda(ab)\,\rho_{\Lambda(ab)} f = T\rho_{ab} T^{-1} f = (T\rho_a T^{-1})(T\rho_b T^{-1}) f$$

$$= \lambda(a)\,\rho_{\Lambda(a)}\,\lambda(b)\,\rho_{\Lambda(b)} f = \lambda(a)\,\lambda(b)\,\rho_{\Lambda(a)}\,\rho_{\Lambda(b)} f$$

for every $a, b \in G_1$ and any $f \in L^p(G_2)$

If we take the norm $\|\cdot\|_p$ on both sides, we obtain

$$\lambda(ab) = \lambda(a)\,\lambda(b)$$

and so

$$\rho_{\Lambda(ab)} = \rho_{\Lambda(a)}\,\rho_{\Lambda(b)}$$

We want to show that Λ is one to one and bicontinuous.

Let e_1 and e_2 be the identity of G_1 and G_2 respectively, and I_1, I_2 be the identity operators of $L^p(G_1)$ and $L^p(G_2)$ respectively.

Suppose that $\Lambda(a) = e_2$, $a \in G_1$, then

$$T\rho_a T^{-1} = \lambda(a)\,\rho_{\Lambda(a)} = \lambda(a)\, I_2$$

and $\rho_a = \lambda(a)\, I_1$, $\lambda(a) = 1$, $a = e_1$, $\lambda(e_1) = 1$.

This shows that Λ is an injective mapping. Actually $\lambda(a) = 1$ for all $a \in G_1$. In fact, if $\lambda(a) > 1$ for some $a \in G_1$, then by the reason of homomorphism λ, we can find a sequence $\{a_n\}$ in G_1 such that $\lambda(a_n) > n$, and since

$$\|T\|\,\|\rho_{a_n}\|\,\|T^{-1}\| \geq \|T\rho_{a_n} T^{-1}\| \geq \|n\,\rho_{\Lambda(a_n)}\| = n,$$

We get

$$\|T\|\,\|T^{-1}\| \geq n.$$

This is a contradiction for sufficiently large n, since T and T^{-1} are bounded linear transformation. Therefore, $\lambda(a) \leq 1$ for any $a \in G_1$. On the other hand, if $\lambda(a) < 1$, then $\lambda(a^{-1}) > 1$, for $a \in G_1$. This shows $\lambda(a) = 1$ for all $a \in G_1$.

Now we show that Λ is bicontinuous. For conveneient, we give an alternative proof for the continuity as Wendel [1].

We observe that Λ is the product of the following mappings :

M_1 : $a \to \rho_a$, $a \in G_1$.

M_2 : $\rho_a \to T\rho_a T^{-1} = \rho_{\Lambda(a)}$, $a \in G_1$,

$= \rho_a'$ (set $\Lambda(a) = a'$, then $a' \in G_2$)

$M_3: \rho_a' \to a'$, $a' \in G_2$.

Evidently M_1 is continuous in the strong operator topology in $L^p(G_1)\, 1<p<\infty$. We now prove that M_2 is continuous.

Since T is bounded, If $\rho_a \to \rho_b$ in the strong operator topology, then

$$\| T\rho_a T^{-1} f - T\rho_b T^{-1} f \|_p \leq \| T \| \, \| \rho_a T^{-1} f - \rho_b T^{-1} f \|_p \to 0 \text{ , for } f \in L^p(G_2).$$

Hence $T\rho_a T^{-1} \to T\rho_b T^{-1}$ in the strong operator topology, and M_2 is continuous.

Finally, we prove that M_3 is continuous. It is clear that M_3 is a homomorphism of groups of operators $\{\rho_a'\}$ onto G_2. Let V' be an arbitrary neighborhood of $e_2 \in G_2$, we shall construct a strong neighborhood of I_2 whose image under M_3 is contained in V'. If we can do this, then M_3 is continuous, since M_3 is a homomorphism.

Let W' be a neighborhood of e_2 having finite measure δ and satisfying $W' W'^{-1} \subseteq V$. Let $\chi' \in L^p(G_2)$ be the characteristic function of W', we shall show that if $\| \rho_a' \chi' - \chi' \|_p < \delta$, then $a' \in V$. In fact, if $a' \notin V'$, then $W' \cap W' a' = \phi$ and $W' \cap W' a'^{-1} = \phi$, since for otherwise $W' a' \cap W' \neq \phi$ implies that there exists x such that $x \in W' a'$ and $x \in W'$, $xa'^{-1} \in W'$, and so

$$(xa'^{-1})^{-1} x \in W'^{-1} W' \subset V \Rightarrow a' \in V',$$

this is a contradiction, similarly, $W' a'^{-1} \cap W' = \phi$.

In this case

$$\| \rho_a \chi' - \chi' \|_p = \{ \int_{G_2} | \chi'(xa'^{-1}) - \chi'(x) |^p \, dx \}^{\frac{1}{p}} = (\| \rho_{a'} \chi' \|_p^p + \| \chi' \|_p^p)^{\frac{1}{p}} = 2^{\frac{1}{p}} \delta,$$

deduce a contradiction.

If $\| \rho_a f - f \|_p < 2^{\frac{1}{p}} \delta$, $f \in L^p(G_2)$, then $\| \rho_{a'} \chi' - \chi' \|_p < 2^{\frac{1}{p}} \delta$, where χ' is constructed as above. So if $\| \rho_{a'} f - f \|_p < 2^{\frac{1}{p}} \delta$ for every $f \in L^p(G_2)$, we get $a' \in V'$ from the above discussion.

This shows that for every neighborhood V' of e_2 in G_2, there is a neighborhood V of I_2 in the strong operator topology such that the image of V under the mapping M_3 is contained in V'. Hence M_3 is continuous. Therefore $\Lambda = M_3$

$M_2 M_1$ is continuous.

At last, we prove Λ is an onto mapping. If $a' \in G_2$, evidently, $T^{-1} \rho_a T$ is a positive linear operator on $L^p(G_1)$ which commute with left translations by the same argument as done above, So there exist $a \in G_1$ such that

$$T^{-1} \rho_{a'} T = \rho_a ,$$

and

$$T \rho_a T^{-1} = \rho_{a'} = \rho_{\Lambda(a)} .$$

That is,

$$a' = \Lambda(a) .$$

This shows that Λ is an onto mapping. Hence the inverse Λ^{-1} of Λ from G_2 onto G_1 exists and continuous.

From the above argument, we prove that Λ is an algebra isomorphism and a bicontinuous mapping from G_1 onto G_2. Therefore, G_1 and G_2 are Topologically isomorphic. Q.E.D.

3. Additional remarks

Remark 1. Whether the isomorphism problem holds for the space $L^\infty(G)$ for general locally compact Group G is still open. Note that if G is compact, the problem was given by Strichartz [9].

Remark 2. The problem for isomorphism that are neither isometric nor bipositive would appear to remain largely open.

Remark 3. Assume that G_1 and G_2 are locally compact Abelian. $M(L^p(G_i))$ and $M(L^q(G_i))$, $i=1,2$, have isometric and bipositive isomorphism between them, where $\frac{1}{p}+\frac{1}{q}=1$. Use this property, we can extend the result of Gaudry [3] such that if there is an isometric or bipositive isomorphism from $M(L^p(G_1))$ onto $M(L^q(G_2))$, $\frac{1}{p}+\frac{1}{q}=1$, ($p.q \neq 2$ for isometric case), then G_1 and G_2 are topologically isomorphic.

Remark 4. Assume that G_1 and G_2 are locally compact Abelian groups. $M(C_0(G_i))$ and $M(G_i)$, $i=1.2$, have isometric and bipositive isomorphism between them. If there exists an isometric or bipositive isomorphism from $M(C_0(G_1))$ onto $M(C_0(G_2))$, then G_1 and G_2 are topologically isomorphic.

Remark 5. Assume that G_1 and G_2 are locally compact groups. $M(L^1(G_i), L^p(G_i))$, $M(L^q(G_i), L^\infty(G_i))$ and $L^p(G_i)$, $i=1.2$, have isometric and bipositive isomorphism one another. We can extend the result of Parrott [7] and the theorem we just proved such that if T is an isometric [resp. bipositive] isomorphism from $M(L^1(G_1), L^p(G_1))$ onto $M(L^1(G_2), L^p(G_2))$ or from $M(L^q(G_1), L^\infty(G_1))$ onto $M(L^q(G_2), L^\infty(G_2))$, $p.q \neq 2$, $1 \leq p.q < \infty$ [resp. $1 \leq p < \infty$], then G_1 and G_2 are topologically isometric.

References

1. B. Brainerd and R. E. Edwards, Linear operators which commute with translations, I, J. Austr. Math. Soc. VI (1966), 289-350.
2. R. E. Edwards, Bipositive and isometric isomorphism of some convolution algebras, Canad. J. Math. 17 (1965), 839-846.
3. G. I. Gaudry, Isomorphisms of multiplier algebras, Canad. J. Math. 20(1968), 1165-1172.
4. B. E. Johnson, Isometric isomorphisms of measure algebras, Proc. Amer. Math. Soc. 15(1964), 186-189.
5. Y. Kawada, On the group ring of a topological group, Math. Japonicae 1(1948), 1-5.
6. R. Larsen, Lecture Notes in Mathematics (105), The multiplier problem, Edited by A. Dold, Heidelberg and B. Eckmann, Zurich, 1970.
7. S. K. Parrott: Isomorphism multipliers, Pacific J. Math. 25 (1968), 159-166.

8. R. Strichartz, Isometric isomorphisms of measure algebras, Pacific J. Math. 15(1965),315-317.

9. R. Strichartz, Isomorphisms of group algebras, Proc. Amer. Math. Soc. 17(1966),858-862.

10. J. G. Wendel, On isometric isomorphism of group algebra, Pacific, J. Math. 1(1951),305-311.

11. J. G. Wendel, Left centralizers and isomorphisms of group algebra, Pacific J. Math. 2(1952),251-261.

馬可夫過程與微分積分的一些關係

林大風　台大

1. 設（Ω，β，P）爲機率空間，S爲狀態空間，$\{X_t, t\geq 0\}$是S上的markov process（時間上一致的）

(1-1)　X_t的推移函數（transition function）$P(t, a; E)$，定義爲

$$P(t, a; E) = P\{X_t \in E \mid x_0 = a\}$$

$t\geq 0$，$a\in S$，$E\in F(s)$，　則對固定的E，$P(t, a; E)$是(t, a)的可測函數，對固定的(t, a)，$P(t, a; E)$是S上的機率測度。$P(t, a; E)$也滿足Chapmam-Kolmogorov方程式

(1-1-a)　$$\int_S P(t, a; dy) P(s, y; E) = P(t+s, a; E)$$

(1-2)　設$\widetilde{B}$是S上的有界可測函數族所成的Banach空間，在$\widetilde{B}$定義H_t，$t\geq 0$，如下，

(1-2-a)　$$H_t f(x) = \int_S f(y) P(t, x; dy), \qquad f\in\widetilde{B}$$

則　$$\| H_t f \| = \sup_{x\in s} | H_t f(x) | \leq \sup_{x\in s} \int | f(y) | P(t, x; dy)$$

$$\leq \| f \| \sup_{x\in s} \int_s P(t, x; dy) = \| f \|$$

(1-2-b)　$$\| H_t \| \leq 1, \qquad t\geq 0$$

又由（1-1-a）及（1-2-a）⇨

$$[H_t(H_s f)](x) = \int_s (H_s f)(y) P(t, x; dy) = \int_y \int_z f(z) \cdot P(s, y; dz) \cdot P(t, x; dy)$$

$$= \int_s f(z) \cdot P(t+s, x; dz) = H_{t+s} f(x)$$

因此有

(1-2-c) $$H_t H_s f = H_{t+s} f, \qquad f \in \widetilde{B}$$

即 $\{H_t, t \geq 0\}$ 是 $\widetilde{B}$ 上的線性算子半群。

(1-3) 對於 $f \in \widetilde{B}$，$H_t f$，$t \geq 0$，不一定是 $\widetilde{B}$ 的連續函數。於是令

$$B = \{ f \in \widetilde{B} : \lim_{t \downarrow 0} H_t f = f \}$$

則 B 是 $\widetilde{B}$ 的 Banach subspace，而且由於（1-2-b），$H_t B \subset B$，因此可把 $\{H_t, t \geq 0\}$ 看作是 B 上的線性算子半群。這時定義

$$D(A) = \{ f \in B : \lim_{h \downarrow 0} \frac{1}{h} (H_h f - f) \text{存在} \}$$

$$Af = \lim_{h \downarrow 0} \frac{1}{h} \{ H_h f - f \}$$

稱 A 是 H_t，$t \geq 0$〔或 $P(t, x; E)$，X_t〕的（強）衍生算子。

這時有：

(1-3-a) $$\lim \frac{H_{t+h} f - H_t f}{h} = A H_t f = H_t A f \qquad f \in D(A)$$

對 $\lambda > 0$，定義 B 上的算子（resolvent of A）.

$$R_\lambda f = \int_0^\infty e^{-\lambda t} H_t f dt \qquad f \in B$$

則 $$\| R_\lambda f \| \leq \int_0^\infty e^{-\lambda t} \| H_t f \| dt \leq \int_0^\infty e^{-\lambda t} dt \cdot \| f \| = \frac{\| f \|}{\lambda}$$

(1-3-a) 故 $\| R_\lambda \| < \frac{1}{\lambda}$, $\quad R_\lambda B \subset B$ 其實

R_λ 與 A 的關係式是，（對任意的 $\lambda > 0$）

(1-3-b) $R_\lambda = (\lambda I - A)^{-1}$, $\quad (\lambda I - A) = R_\lambda^{-1}$

$$D(A) \underset{R_\lambda}{\overset{\lambda I - A}{\rightleftarrows}} B \qquad 1-1 \text{, onto.}$$

(1-4) 考慮方程式

(1-4-a)
$$\begin{cases} \dfrac{\partial}{\partial t}F(t,x)=AF(t,x) \\ \lim\limits_{t\downarrow 0} F(t,x)=f(x), \quad (\text{uniformly in } x) \quad f\in B \end{cases}$$

如果令

(1-4-b) $$F(t,x)=(H_t f)(x)$$

則由 (1-3-a)及B的定義知

$$\begin{cases} \dfrac{\partial}{\partial t}F(t,x)=\dfrac{\partial}{\partial t}H_t f(x)=AH_t f(x)=AF(t,x) \\ \lim\limits_{t\downarrow 0} F(t,x)=\lim\limits_{t\downarrow 0} H_t f(x)=f(x) \quad (\text{uniformly in } x) \end{cases}$$

因此(1-4-b)是(1-4-a)的解。

2. 設$K(x,dy)$是積分核， 滿足

$$0\leq K(x,E)\leq 1 \qquad x\in S,\ E\in g(s),$$

$$Kf(x)=\int_S K(x,dy)f(y)\in B, \qquad \forall\ f\in B$$

$$\|Kf\|\leq\|f\|$$

我們希望找出下列方程的和率解：

$$\begin{cases} \dfrac{\partial}{\partial t}F(t,x)=AF(t,x)-\alpha F(t,x)+\alpha\int_S K(x,dy)F(t,y), \quad \alpha>0 \\ \lim\limits_{t\downarrow 0} F(t,x)=f(x) \qquad (\text{uniformly in } x), \qquad f\in B \end{cases}$$

(2-1) 令Y_t，$t\geq 0$，是由X_t，$t\geq 0$，再加上跳躍的馬可夫過程，跳躍的等待時刻是$\alpha e^{-\alpha t}\alpha_t$，跳躍分佈是$K(x,dy)$，這時令$P^*$，$H_t^*$，$A^*$及$R_\lambda^*$，各爲$Y_t$的推移函數，綫性算子半群，衍生算子及 resolvent

(2-1-a) 則
$$\begin{cases} P_0^*(t,x;E)=e^{-\alpha t}P(t,x;E) \\ P_{n+1}^*(t,x;E)=\int_0^t e^{-\alpha(t-s)}\alpha ds\int_S P(t-s,x;dy) \\ \qquad\qquad \int_S K(y,dz)P_n^*(s,z;E) \end{cases}$$

其中 $P_n^*(t, x; E) = P\{Y_t \in E \mid Y_0 = x$，經過 n 次跳躍 $\}$

(2-1-b) $$P^*(t, x; E) = \sum_{n=0}^{\infty} P_n^*(t, x; E)$$

設 $B' = \{h(t, x) : \|h\|_t = \sup_{0 \le s \le t,\, x \in S} |h(s, x)| < \infty \ \forall t \ge 0\}$

(2-2) 定義

$$(Lh)(t, x) = \int_0^t e^{-\alpha(t-s)} \alpha ds \int_S P(t-s, x; dy) \int_S K(y, dz) h(s, z)$$

則 $L(B') \subset B'$，而且

$$\|L^n h\|_t \le (1 - e^{-\alpha t})^n \|h\|_t$$

令 $T = \sum_{n=0}^{\infty} L^n$， 則由於 (2-2-b)，$TB' \subset B'$，

$$\|Th\|_t \le e^{\alpha t} \|h\|_t , \qquad t \ge 0$$

故 由 (2-1)

$$P^*(t, x; E) = \sum_{n=0}^{\infty} P_n^*(t, x; E) = \sum_{n=0}^{\infty} L^n P_0(t, x; E) = T\, P_0(t, x; E)$$

即得

(2-2-a) $$H_t^* f(x) = \int_S P^*(t, x; dy) f(y)$$

$$= \sum_{n=0}^{\infty} L^n \int_S P_0(t, x; dy) f(y)$$

$$= \sum_{n=0}^{\infty} L^n \int_S e^{-\alpha t} P(t, x; dy) f(y)$$

$$= \sum_{n=0}^{\infty} L^n (e^{-\alpha t} H_t f(x)) = T(e^{-\alpha t} H_t f(x))$$

(2-3) $$R_\lambda^* f(x) = \int_0^{\infty} e^{-\lambda t} H_t^* f(x)\, dt \qquad f \in B$$

由 induction 可證出

$$(2\text{-}3\text{-}a)\qquad \int_0^\infty e^{-\lambda t}\,(e^{-\alpha t}H_t f)\,dt = \int_0^\infty e^{-(\lambda+\alpha)t}H_t f(x)\,dt = R_{\lambda+\alpha} f$$

$$\int_0^\infty e^{-\lambda t} L^n(e^{-\alpha t}H_t f)\,dt = \alpha^n (R_{\lambda+\alpha}K)_0^n R_{\lambda+\alpha} f \qquad n \geq 0$$

因此由(2-3-a)得

$$R_\lambda^* f = \int_0^\infty e^{-\lambda t}\sum_{n=0}^\infty L^n(e^{-\alpha t}H_t f)\,dt$$

$$= \sum_{n=0}^\infty \int_0^\infty e^{-\lambda t} L^n(e^{-\alpha t}H_t f)\,dt$$

$$= \sum_{n=0}^\infty \alpha^n (R_{\lambda+\alpha}\circ K)^n \bullet R_{\lambda+\alpha} f = \sum_{n=0}^\infty R_{\lambda+\alpha}\bullet\alpha^n (R_{\lambda+\alpha}\circ K)^n f$$

因爲由(1-3-a)

$$\|\alpha R_{\lambda+\alpha}\circ K\| \leq \alpha\bullet\|R_{\lambda+\alpha}\|\bullet\|K\| \leq \frac{\alpha}{\lambda+\alpha} < 1$$

故 $\sum_{n=0}^\infty \alpha^n (R_{\lambda+\alpha}\circ K)^n = (I-\alpha R_{\lambda+\alpha}\circ K)^{-1}$。

$\Longrightarrow$

$$(2\text{-}3\text{-}b)\qquad R_\lambda^* f = (I-\alpha R_{\lambda+\alpha}\circ K)^{-1} R_{\lambda+\alpha} f$$

$$= R_{\lambda+\alpha}(I-\alpha R_{\lambda+\alpha}\circ K)^{-1} f$$

$$(2\text{-}4)\qquad \lambda f - A^* f = (R_\lambda^*)^{-1} f = (R_{\lambda+\alpha})^{-1}(I-\alpha R_{\lambda+\alpha}\circ K) f$$

$$= G_{\lambda+\alpha}^{-1} f - \alpha K f = (\lambda+\alpha) f - Af - \alpha K f$$

$$A^*\bullet f = Af - \alpha f - \alpha K f$$

$$= Af - \alpha f - \alpha\int K(x,dy) f(y)$$

$$\therefore\quad \lim_{t\downarrow 0}\frac{H_t^* f(x)\bullet f(x)}{t} = Af(x) - \alpha f(x) - \alpha\int_S K(x,dy) f(y) \qquad (\text{uniformly in } x)$$

令 $F(t,x) = H_t^* f(x)$ 即爲

$$\frac{\partial F}{\partial f} = AF - \partial F + \int KF$$

$$\lim_{t \downarrow 0} F = f$$

之解。

Some Remarks on Teaching Linear Algebra and Matrix Theory

By

Yueh-er Kuo （郭月娥）

The University of Tennessee

Study of linear algebra and matrix theory become popular in recent years. Mathematics students are required to take the course and students in applied and social sciences are taking this course as an important tool in their fields. As you know linear algebra is being taught from freshman or sophomore year on. Here we only discuss teaching of the course to upper division college students and graduate students in three different groups: (1) mathematics major, (2) major in applied and social sciences, (3) high school mathematics teachers.

(1) For students in mathematics major.

These students need solid foundation in linear algebra and matrix theory. Text books should be chosen with emphasis in theoretical aspects with richness of exercises in proofs. When teaching these students it would be helpful to explain the importance of the course at the beginning, and also at the times when there are some important statements or formulas. Let students know how to prove in order to let them modify the proofs to prove more complicated statements and develop new statements and formulas in the future.

For undergraduate students, we can use linear algebra and matrix theory as a tool to the general abstract algebra. For graduate students, we can do this in a reverse way, starting from general abstract algebra and considering linear algebra and matrix theory as particular cases or examples.

(2) For students in applied and social sciences.

Text books which contain many numerical examples and exercises, and also contain many up to date different methods for numerical problems would be useful. It is also appreciated, if the bibliography in the text book contains different types of many references. When teaching the course to the students let us give numerical examples and explain some applications. It might be good not to use theoretical approach, but we still need to give the students the techniques of proofs. Sometimes students are only interested in how to solve the problems, but if the students have some degree of the techniques of proofs, sometimes they can check formulas or statements very easily and create new methods in the future.

If the students are from different types of majors, we need to concentrate on general concepts and general applications. We need not let them study too many methods, but we can explain some typical types of methods, and let students study by themselves for applications to their own fields. To the certain types of students, for example, teaching physics and engineering students, you may need to give more details on eigenvalue problems, norms, and orthogonalities. For social sciences students, you may give geometric concepts and concepts of mathematical programming and game theory.

It may give you a good opportunity to know how the students apply the course, if you let the students write a report on applications of the course to their fields or other applications.

(3) For the training of high school mathematics teachers.

It may be said these students are on the half way between (1) and (2), therefore we may combine the above mentioned techniques of (1) and (2) to these students. We need to concentrate on fundamental concepts. It is also desired to give examples. In case there are some high school teachers who are out of schools for many years, you may start from the beginning concept of the course.

If the students in the class are of mixed types, you may find out the distributions of the students and use appropriate approach accordingly. If the distributions of the students are about the same for (1), (2) and (3), you may use the technique for type (3) and assign the appropriate different readings to them.

It is hoped the above remarks can give the teachers in the course some thought to improve the teaching and give more effective applications to the course.

References

1. Committee on Undergraduate Programs in Mathematics, Preparation for Graduate Study in Mathematics, Mathematical Association of America, 1965.
2. ________, A Beginning Graduate Program in Mathematics for Prospective Teachers of Undergraduates, Mathematical Association of America, 1969.
3. ________, Pregraduate Preparation of Research Mathematicians, Mathematical Association of America, 1963.
4. ________, Recommendations of the Undergraduate Mathematics Program for engineers and Physicists, Mathematical Association of America, 1967.
5. ________, Recommendations on the Undergraduate Mathematics Program for Work in Computing, Mathematical Association of America, 1964.
6. ________, Tentative Recommendations for the Undergraduate Mathematics Program of Students in the Biological Management and Social Sciences, Mathematical Association of America, 1964.
7. ________, Course Guides for the Training of Teachers of Junior High and High School Mathematics, Mathematical Association of America, 1961.

A Partition Theorem for the Modulus 15

by

Yu Ching-Shu

(游 靜 淑)

In (2) § 5 Professor G. E. Andrews discovered a partition theorem for the modulus 7. In this paper, I follow his technique to get a partition theorem for the modulus 15. First I have to introduce several definitions which were defined by professor G.E. Andrews in (2).

Let S denote the set of all sequences $\{f_i\}_{i=1}^{\infty}$ (more briefly $\{f_i\}$) where each f_i is a non-negative integer and where only finitely many f_i are nonzero. Then S forms a distributive lattice under the partial ordering $\{f_i\} \leqq \{g_i\}$ provided $f_i \leqq g_i$ for each i (2, Lemma 2.1.). Next let us define a function σ on S such that

$\sigma(\pi) = \sum_{i=1}^{\infty} f_i \cdot i$ for any $\pi = \{f_i\}_{i=1}^{\infty} \in S$, then σ is a positive valuation on S.

Definition 1. A semi-ideal in the lattice S is called a partition ideal. (2, Lemma 2. 2.).

Definition 2. If C is a partition ideal in S, we say that $p(C;n)$ is the C-partition function if for each n, $p(C;n)$ denotes the cardinality of the set $\{\pi \mid \pi \in C,\ \sigma(\pi)=n\}$.

Definition 3. We say that two partition ideals C_1 and C_2 of S are partition-theoretically equivalent (more briefly PT-equivalent) if for each non-negative integer $p(C_1;n) = p(C_2;n)$, and we shall write $C_1 PT C_2$.

Definition 4. Let $C(a_1, a_2, \cdots, a_r; m)$ denote $\{\pi \mid \pi = \{f_i\} \in S$ and if $f_i \neq 0$, then $i \equiv a_1, a_2, \cdots$, or $a_r \pmod m\}$. Let $C_d(a_1, a_2, \cdots, a_r; m)$ denote $\{\pi \mid \pi = \{f_i\} \in S,\ 0 \leqq f_i \leqq 1$, and if $f_i \neq 0$, then $i \equiv a_1, a_2, \cdots$, or $a_r \pmod m\}$.

Definition 5. Let $D(r;b_1,b_2,\cdots,b_m;m)$ denote $\{\pi \mid \pi=\{f_i\}\in S,\ f_j=0$ when $j<r,\ 0\leqq f_j\leqq 1$, and if $f_j=1$ with $j\equiv k \pmod m$, then $f_{j+1}=f_{j+2}=\cdots=f_{j+b_k-1}=0\}$.

Now I can state the teheorem in the following:

Theorem: $C(1,17,19,23;30)$ PT $C_d(1,2,4,8;15)$ PT $D(1;15,15,28,15,26,26,39,15,22,22,35,22,33,31,46;15)$.

Remark: To simplify notation we shall write D for $D(1;15,15,28,15,26,26,39,15,22,22,35,22,33,31,46;15)$.

Proof: The equivalence

$C(1,17,19,23;30)$ PT $C_d(1,2,4,8;15)$ appears in (1, Theorem 2.). It also can follow directly from Theorem 4 in (2).

To prove the second equivalence we start by defining $p_a(m,n)$ to be the cardinalty of the following set:

$\{\{f_i\}\mid\{f_i\}\in D,\ \sum_{i=1}^{\infty} f_i\cdot i=n,\ \sum_{i=1}^{\infty} f_i=m$, and $f_i=0$ if $i\leqq a\}$ we must now establish the following identities.

(1) $p_0(m,n)=p_1(m,n)+p_0(m-1,n-15m+14)$

(2) $p_1(m,n)=p_2(m,n)+p_1(m-1,n-15m+13)$

(3) $p_2(m,n)=p_3(m,n)+p_0(m-1,n-30m+27)$

(4) $p_3(m,n)=p_4(m,n)+p_3(m-1,n-15m+11)$

(5) $p_4(m,n)=p_5(m,n)+p_0(m-1,n-30m+25)$

(6) $p_5(m,n)=p_6(m,n)+p_1(m-1,n-30m+24)$

(7) $p_6(m,n)=p_7(m,n)+p_0(m-1,n-45m+38)$

(8) $p_7(m,n)=p_8(m,n)+p_7(m-1,n-15m+7)$

(9) $p_8(m,n)=p_9(m,n)+p_0(m-1,n-30m+21)$

(10) $p_9(m,n)=p_{10}(m,n)+p_1(m-1,n-30m+20)$

(11) $p_{10}(m,n)=p_{11}(m,n)+p_0(m-1,n-45m+34)$

(12) $p_{11}(m,n)=p_{12}(m,n)+p_3(m-1,n-30m+18)$

(13) $p_{12}(m,n)=p_{13}(m,n)+p_0(m-1,n-45m+32)$

(14) $p_{13}(m, n) = p_{14}(m, n) + p_1(m-1, n-45m+31)$

(15) $p_{14}(m, n) = p_{15}(m, n) + p_0(m-1, n-60m+45)$

(16) $p_{15}(m, n) = p_0(m, n-15m)$.

The proofs of these sixteen identities all resemble one another. We therefore choose (8) to present in detail. First we see that $p_7(m, n) - p_8(m, n)$ is exactly the number of partitions π of n with m parts such that $\pi \in D$ and 8 is a summand of π. By the requirements on D we see that all other summands besides the 8 must be at least as large as 23. We now transform these partitions by deleting the 8 and subtracting 15 from every other part.

This leaves us with a partition of the type enumerated by $p_7(m-1, n-15m+7)$. Clearly the above process is reversible, and so we have established a one-to-one correspondence between the partitions enumerated by $p_7(m, n) - p_8(m, n)$ and those enumerated by $p_7(m-1, n-15m+7)$. Thus (8) is established.

We now define

$$f_a(x) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} p_a(m, n)\, x^m q^n$$

Then directly from our sixteen identities, we deduce that

(17) $f_0(x) = f_1(x) + xq f_0(xq^{15})$

(18) $f_1(x) = f_2(x) + xq^2 f_1(xq^{15})$

(19) $f_2(x) = f_3(x) + xq^3 f_0(xq^{30})$

(20) $f_3(x) = f_4(x) + xq^4 f_3(xq^{15})$

(21) $f_4(x) = f_5(x) + xq^5 f_0(xq^{30})$

(22) $f_5(x) = f_6(x) + xq^6 f_1(xq^{30})$

(23) $f_6(x) = f_7(x) + xq^7 f_0(xq^{45})$

(24) $f_7(x) = f_8(x) + xq^8 f_7(xq^{15})$

(25) $f_8(x) = f_9(x) + xq^9 f_0(xq^{30})$

(26) $f_9(x) = f_{10}(x) + xq^{10} f_1(xq^{30})$

(27) $f_{10}(x) = f_{11}(x) + xq^{11} f_0(xq^{45})$

(28) $f_{11}(x) = f_{12}(x) + xq^{12} f_3(xq^{30})$

(29) $f_{12}(x) = f_{13}(x) + xq^{13} f_0(xq^{45})$

(30) $f_{13}(x) = f_{14}(x) + xq^{14} f_1(xq^{45})$

(31) $f_{14}(x) = f_{15}(x) + xq^{15} f_0(xq^{60})$

(32) $f_{15}(x) = f_0(xq^{15})$.

We wish now to solve these equations to obtain an identity in $f_0(x), f_0(xq^{15})$, $f_0(xq^{30}), \cdots$. To do this we note that adding all these equations produces an identity $f_0(x) = E_1$ where E_1 involves only f_0, f_1, f_3 and f_7 (with various arguments). Adding the first seven equations produces an identity $f_7(x) = E_2$, where E_2 involves only f_0, f_1 and f_3. Adding the first three equations produces an identity $f_3(x) = E_3$, where E_3 involves only f_0 and f_1. Furthermore (17) may be transformed to produce an identity $f_1(x) = f_0(x) - xqf_0(xq^{15}) = E_4$, an expression involving only f_0. Thus we may use E_4 for substitutions into E_3 to produce an identity $f_3(x) = E_5$ where E_5 involves only f_0. Then we use E_4 and E_5 for substitutions into E_2 to produce an identity $f_7(x) = E_6$, where E_6 involves only f_0. Finally we may use E_4, E_5 and E_6 for substitutions into E_1 to produce an identity involving only f_0 with various arguments. The final result is

(33) $$f_0(x) = (1 + xq + xq^2 + xq^4 + xq^8)\, f_0(xq^{15}) + x\,(q^3 + q^5 + q^6 + q^9 + q^{10} + q^{12})(1 - xq^{15})\, f_0(xq^{30}) + x\,(q^7 + q^{11} + q^{13} + q^{14})(1 - xq^{15})(1 - xq^{30})\, f_0(xq^{45}) + xq^{15}(1 - xq^{15})(1 - xq^{30})(1 - xq^{45})\, f_0(xq^{60})$$

If we define $g(x) = f_0(x) / (x\,;q^{15})_\infty$,

(where $(x\,;q^{15})_\infty = \prod_{n=0}^{\infty} (1 - xq^{15n})$)

then by dividing (33) by $(xq^{15}\,; q^{15})_\infty$ we obtain

(34) $$(1 - x)\,g(x) = (1 + xq + xq^2 + xq^4 + xq^8)\, g(xq^{15}) + x\,(q^3 + q^5 + q^6 + q^9 + q^{10} + q^{12})\, g(xq^{30}) + x\,(q^7 + q^{11} + q^{13} + q^{14})\, g(xq^{45}) = xq^{15} g(xq^{60}).$$

We now consider the Maclaurin series for $g(x)$, namely

$g(x)=\sum_{n=0}^{\infty} A_n x^n$, and we substitute into (34). Thus from the coefficients of x^n after the substitution we see that

$$(35)\quad \begin{aligned} A_n - A_{n-1} &= q^{15n} A_n + q^{15n-14} A_{n-1} + q^{15n-13} A_{n-1} + q^{15n-11} A_{n-1} \\ &+ q^{15n-7} A_{n-1} + q^{30n-27} A_{n-1} + q^{30n-25} A_{n-1} + q^{30n-24} A_{n-1} \\ &+ q^{30n-21} A_{n-1} + q^{30n-20} A_{n-1} + q^{30n-18} A_{n-1} + q^{45n-38} A_{n-1} \\ &+ q^{45n-34} A_{n-1} + q^{45n-32} A_{n-1} + q^{45n-31} A_{n-1} + q^{60n-45} A_{n-1} \end{aligned}$$

Therefore

$$(36)\quad (1-q^{15n})A_n = (1+q^{15n-14})(1+q^{15n-13})(1+q^{15-11})(1+q^{15n-7})A_{n-1}$$

Since $A_0 = g(0) = f_0(0) = 1$, we may easily solve the recurrence (36) bv iteration. Therefore

$$(37)\quad A_n = \frac{(-q;q^{15})_n(-q^2;q^{15})_n(-q^4;q^{15})_n(-q^8;q^{15})_n}{(q^{15};q^{15})_n}$$

Hence

$$\begin{aligned} f_0(x) &= (x;q^{15})_\infty g(x) \\ &= (x;q^{15})_\infty \sum_{n=0}^{\infty} \frac{(-q;q^{15})_n(-q^2;q^{15})_n(-q^4;q^{15})_n(-q^8;q^{15})_n x^n}{(q^{15};q^{15})_n} \end{aligned}$$

Letting $x \longrightarrow 1^-$, we deduce using Appell Comparison theorem (3; page 108) that

$$(38)\quad \begin{aligned} \sum_{n=0}^{\infty} p_0(D;n)q^n &= f_0(1) = \lim_{x\to 1^-} f_0(x) \\ &= (q^{15};q^{15})_\infty \lim_{x\to 1^-} (1-x) \sum_{n=0}^{\infty} \frac{(-q;q^{15})_n(-q^2;q^{15})_n(-q^4;q^{15})_n(-q^8;q^{15})_n x^n}{(q^{15};q^{15})_n} \\ &= (-q;q^{15})_\infty(-q^2;q^{15})_\infty(-q^4;q^{15})_\infty(-q^8;q^{15})_\infty \\ &= \sum_{n=0}^{\infty} p(C_d(1,2,4,8;15);n)q^n \end{aligned}$$

Thus D PT $C_d(1,2,4,8;15)$ and the theorem is established.

References

1. G. E. Andrews, A general theorem on partition with difference conditions, Amer. J. Math. 91 (1969), 18-24.
2. G. E. Andrews, Partition Identities (to appear).
3. G. E. Hardy, Divergent Series (Oxford 1963).

A TOPOLOGICAL PROPERTY BETWEEN T_0 AND T_1

Yean-ming Huang (黃允明)
University of Minnesota

In a general topological space $(X, \mathfrak{J})$, the set of accumulation points of each subset of X is not necessary closed. It is well-known, however, that in T1-space the set of accumulation points of each subset is closed. Furthermore, Mr. C. T. Yang ([1], pg 56, problem D) proved that if $(X, \mathfrak{J})$ is a topological space, then A' is closed for every $A \subset X$ if only if for each $x \in X$, $\{x\}'$ is closed. Here we use A' to denote the set of all accumulation points of A, i.e. A' is so-called derived set of A.

The present discussion was motivated, in the first place, by the desire to find an example of a To-space which contains a subset whose derived set is not closed. In attacking this problem one is inclined to look, first of all, at topologies on a finite set. It turns out, however, that this approach is doomed to failure and, in fact, we have the following curious result.

Theoreml. If $(X, \mathfrak{J})$ is a finite To-space, then for each $A \subset X$, A' is closed.

Proof: By Yang's result, mentioned above, it suffices to prove that $\{x\}'$ is closed for each $x \in X$.

For each $x \in X$, consider the neighborhood system η_x of x. Since X is finite set, so is η_x. Let $G = \cap \{N \mid N \text{ is an open nbhd of } x\}$. Then G is open for a finite intersection of open sets is open. If $y \in G$, $y \neq x$, then $y \in N$ for each open nbhd N of x, and so by the To-property there is an open nbhd $V \in \eta_y$ such that $x \notin V$. Thus y is not an accumulation point of x. Let $F = \cap \{C \mid x \in C, C \text{ is a closed subset of } X\}$. Then F is the closure of x, i.e. $F = \{x\} \cup \{x\}'$. We observe that $(X \setminus G) \cap F$ is closed. We claim that $\{x\}' = (X \setminus G) \cap F$. For if $y \in \{x\}$, then $y \notin G$ and $y \in F$, thus $y \in (X \setminus G) \cap F$. Conversely, if $y \in (X \setminus G) \cap F$ then $y \in F$ and $y \neq x$ so $y \in \{x\}'$. Hence $\{x\}' = (X \setminus G) \cap F$ is closed.

In regard to the original question, now that one knows where to not look it is rather easy to produce an example of a T_0-space in which derived sets are not always closed.

Example 1. Let X be the set of real numbers, and let $\mathcal{J} = \{\phi, X\} \cup \{(-\infty, a) \mid a \in X\}$. It is clear that $(X, \mathcal{J})$ is a T_0-space but not T_1-space. Furthermore, for each $x \in X$, $\{x\}' = (x, \infty)$ is not a $\mathcal{J}$-closed set.

The considerations above suggest a further investigation of topological spaces X which have the property that $\{x\}'$ is closed for every $x \in X$. We begin with the following observation.

Theorem 2. If $(X, \mathcal{J})$ is a topological space, and for each $x \in X$, $\{x\}'$ is closed, then $(X, \mathcal{J})$ is a T_0-space.

Proof: Let $x, y \in X$, $x \neq y$. Then we consider the following cases: (a) $y \in \{x\}'$. By definition of accumulation points of a set, we have $x \notin \{x\}'$ that is $x \in X \setminus \{x\}'$. Thus if $y \in \{x\}'$ then $X \setminus \{x\}'$ is a neighborhood of x that does not contain y. (b) $y \in \{x\}'$. Then there is an open $M \in \eta_y$ such that $M \cap (\{x\} \setminus \{y\}) = M \cap \{x\} = \phi$; thus $x \notin M$. Hence there is $M \in \eta_y$ such that $x \notin M$. By (a), (b) we have proved that $(X, \mathcal{J})$ is a T_0-space.

Corollary: If $(X, \mathcal{J})$ is a finite topological space then $(X, \mathcal{J})$ is a T_0-space iff $\{x\}'$ is closed for all $x \in X$.

Proof: This is immediate from Theorem 1 and Theorem 2.

Let us now agree to call a topological space $(X, \mathcal{J})$ a $T_{1/2}$-space if it has the property that $\{x\}'$ is closed for every $x \in X$. This choice of terminology is motivated by the fact that any T_1-space is a $T_{1/2}$-space and any $T_{1/2}$-space is a T_0-space (Theorem 2). Furthermore, it is possible to characterize the $T_{1/2}$-property so that, like the classical "T"-axioms, it appears as a separation-type property. This is the content of the following theorem.

Theorem 3. X is a $T_{1/2}$-space iff it has the property that, for each $x \in X$, there is a neighborhood U of x such that if $y \in U$, $y \neq x$, then there is a neighborhood V of y such that $x \notin V$.

Proof: Necessity. Take $U = X \setminus \{x\}'$. Then U is an open neighborhood of x. If $y \in U$, $y \neq x$, then since $y \notin \{x\}'$ there is a neighborhood V of y such that $x \notin V$.

Sufficiency. We show that the set $X \setminus \{x\}'$ is open by showing that it is a neighborhood of each of its points. Let $y \in X \setminus \{x\}'$. If $y \neq x$ then there is a neighborhood N of y such that $N \cap \{x\} = \phi$. Clearly $N \subseteq X \setminus \{x\}'$; thus $X \setminus \{x\}'$ is a neighborhood of y. Now consider the point $x \in X \setminus \{x\}'$. By hypothesis, there is a neighborhood U of x such that if $z \in U$, $z \neq x$, then there is a neighborhood V_z of z such that $x \notin V_z$. From this it is clear that $U \subseteq X \setminus \{x\}'$; thus $X \setminus \{x\}'$ is a neighborhood of x.

The space of Example 1 is a T_0-space but not a $T_{1/2}$-space. We now offer an example of a $T_{1/2}$-space which is not T_1-space; thus we see that the $T_{1/2}$-property fits strictly between T_0 and T_1.

Example 2. Let X be the set of real numbers, and let $\mathcal{T} = \{\phi, X\} \cup \{(-\infty, a) \mid a \in X\} \cup \{(-\infty, b) \mid b \in X\}$. Clearly $(X, \mathcal{T})$ is topological space. Furthermore, if $x \in X$ then $\{x\}' = (x, \infty)$ is $\mathcal{T}$-closed; thus X is a $T_{1/2}$-space. On the other hand, $\{x\}$ is not $\mathcal{T}$-closed and so X is not a T_1-space.

The rest of our discussion is concerned with the question of whether or not the $T_{1/2}$-property is preserved under the standard topological constructions.

Theorem 4. Any subspace of $T_{1/2}$-space is $T_{1/2}$-space.

Proof: Suppose X is a $T_{1/2}$-space and Y is a subspace of X. If $x \in Y$ then the set of accumulation points of $\{x\}$ in Y is $\{x\}' \cap Y$, and hence is a a closed set in Y. Thus Y is a $T_{1/2}$-space.

Theorem 5. The finite product of $T_{1/2}$-spaces is a $T_{1/2}$-space.

Proof: Let $X=\prod_{i=1}^{n} X_i$, where X_i $i=1,2,\cdots,n$ are $T_{1/2}$-spaces. If $x\in X$, let $x=(x_1,x_2,\cdots,x_n)$ where $x_i\in X_i$. Since each X_i is a $T_{1/2}$-space, by Theorem 3, there exists an open neighborhood U_i of x_i such that $U_i\setminus\{x_i\}$ is open in X_i. For each fixed i, let $\widetilde{U}_i=\{(y_1,y_2,\cdots,y_n)\mid y_j\in U_j \text{ if } j\neq i,\ y_i\in U_i\setminus\{x_i\}\}$. Then $\widetilde{U}_i$ is open, for it is a finite product of open sets. Furthermore, $\bigcup_{i=1}^{n}\widetilde{U}_i=(\prod_{i=1}^{n} U_i)\setminus\{x\}$ is also open in X. Let $U=\prod_{i=1}^{n} U_i$. Then U is an open neighborhood of x such that $U\setminus\{x\}$ is open. Hence for all $y\in U$, $y\neq x$, then exists V a neighborhood of y st. $x\notin V$. By Theorem 3, X is a $T_{1/2}$-space.

Unfortunately, the product of infinitely many $T_{1/2}$-spaces is not in gereneral a $T_{1/2}$-space. In fact, quite the opposite is true.

Theorem 6. Any infinite product of $T_{1/2}$ but not T_1 spaces is not $T_{1/2}$.

Proof: Let $X=\prod_{i\in I} X_i$ where X_i, $i\in I$ are $T_{1/2}$-spaces but not T_1. Since X_i is $T_{1/2}$ not T_1, there exists, for each $i\in I$, a point $x^i\in X_i$ such that $\{x^i\}'$ is nonvoid and closed. Now let $x=(x^i)_{i\in I}$. We will show that $\{x\}'$ is not closed by showing there exists a net in $\{x\}'$ which converges to x. Let $\mathfrak{F}=\{F\mid F \text{ is a finite subset of } I\}$, then $\mathfrak{F}$ is directed upward by "$\subseteq$", so is a directed set. Define a net $\{y_F\}_{F\in\mathfrak{F}}$ as follows:

$$y_F^i=x^i \quad \text{if} \quad i\in F$$
$$y_F^i\in\{x^i\}' \quad \text{if} \quad i\notin F,\ i\in I$$

We claim that $\{y_F\}_{F\in\mathfrak{F}}$ is a net in $\{x\}'$ and $\{y_F\}_{F\in\mathfrak{F}}$ converges to x.

To see that each y_F is an accumulation point of x, consider each basic neighborhood G of y_F. Then $G=\prod_{i\in I} G_i$ where $G_i=X_i$ except for finitely many i. Then if $G_i=X_i$, we clearly have $x^i\in G_i$; if $G_i\neq X_i$ and $i\in F$, then $x^i=y_F^i\in G_i$ automatically; if $G_i\neq X_i$ and $i\notin F$, then $x^i\in G_i$ because $y_F^i\in\{x^i\}$. Hence each basic open neighborhood G of y_F contains x, and so $y_F \in \{x\}'$. That x is the limit of $\{y_F\}_{F\in\mathfrak{F}}$ is clear.

Remark: In general, the quotient space of a $T_{1/2}$-space is not $T_{1/2}$. For example: Let $(X,\mathfrak{J})$ be the space of Example 2. Let Z be the set of integers and consider X/Z with the quotient topology $\eta\#(\mathfrak{J})$ induced by the natural map η of X onto X/Z. Then $(X/Z, \eta\#(\mathfrak{J}))$ is the indiscrete topological space, hence $(X/Z, \eta\#(\mathfrak{J}))$ is not $T_{1/2}$.

Reference

1. J. L. Kelley, General Topology, Van Nostrand, Princeton, 1955.

A survey in Summability Theory

張紹騫清大

We limitourselvesto matrix methods in this discussion . Consider the C_1 -methods , if we write $C_1 : s \to s$, with s the set of all complex sequence , then we ean write .

$$C_1 = \begin{matrix} 1 & & \\ \frac{1}{2} & \frac{1}{2} & \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \cdots\cdots & & \end{matrix} \qquad \text{clearly } C_1 x = \left(x_1, \frac{x_1+x_2}{2}, \frac{x_1+x_2+x_3}{3}, \cdots\cdots\right)$$

i.e. some summability methods can be represented by infinite matrices. On the other hand , a matrix $A = (a_{nk})$, n , k = 1 , 2, ..., can define a summability method. viz.

$$A_x = \begin{pmatrix} a_{11} & a_{21} & a_{13} & \cdots\cdots \\ a_{21} & a_{22} & a_{23} & \cdots\cdots \\ a_{31} & a_{32} & a_{33} & \cdots\cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \cdots \end{pmatrix} = \left(\sum_k a_{nk} x_k\right)$$

to treat x as a colunm. vectors . Let, $(Ax)_n = \sum_k a_{nk} x_k$, we denote $\lim_n (Ax)_n$ by $\lim_A x$. Degine $C_A = \{ x \in s \mid A_x \in c \}$ — the summability domain (some call it — field) . A method A is said to be regular , if $\lim_A x = \lim x$, $Ax \in c$, c the space of conv. seqs.

Toeplitz(1911) proved that A is regular →

(N) $\|A\| = \sup_n \{ \sum |a_{nk}| < \infty$,

(R) $\lim_{n} \sum_{k} a_{nk} = 1$,

(C) $\lim_{n} a_{nk} = 0$

e.g. C_1 , Lototsky ete are regular.

S. Mazur & W. Orlicz , Sur les niébhodes liveeives de sommation C.R. Acad. Sci 196 , 32 - 34 (1933) ob'serves that C_A in general is not a Banach space, unless A is reversable , they said that C_A is a B_0 -space in general . Since the World war II breakes out . a detail study on this was discontinues. Till after the war . a member of school of Tubrugen , Germany . K. Zeller define the structure FK-sp (B_0 - sp as Matur, Orlicz mentioned) in (AELV) Allgemeine Eigenschaften von Liuritieruvgsvergahrean M.Z. (1951). which gives the proper topology for C_A . (FK-top is unique !).

Kojima proved (in 1913) that A is onservative (i.e. simply $C \subset C_A$) $\rightarrow$

(N) — ditto —

(R) ......= exists

(C) ......– exists.

(See Rogosinski , Fourier series .)

Both proofs in Topitz & Kojuna were difficult in nec cond'n for (N) —— a samewhat compliectio reductio ad absrudum argument (Some call it gliding hump argument). But S. Bauach. Th'eorie des op'eration lin'earires . Warsaw (1932). pvovided easier mechinary, i.e. by using U.B.P. A. Wilansky , An app $\frac{n}{}$ of Banach linear functionals to summability TAMS (1949)

A. Wil. classified the conservative matrices :

1 – 1

1 – 1

1 – 1

conull

....

C_1

coregular

emeguler

(i) $x(A) = \lim_n \sum_{k} a_{nk} - \sum_k \lim_n a_{nk} \neq 0$, A co-regular

(ii) $x(A) = 0$, A conull .

In 1950 s there are many collabvations of Wil. & Zeller , which enrichs the theory greatly in this direction .

Note that, in Zellgs' AELV, there are two faets so fundamentally important.

(i) FK-top is unique, hence counllity (so is eoregularity) is essentially invariant.

(ii) For any conservative matrix A, $f \in C_A$, there is a matrix $B \ni f = \lim_B$ with $C_B \supset C_A$, This justify the reason to develope matrix methods.

Much studis have been doneon coregularity , but very little has been done on conullity (thou , it has been shown that a conull matrix sums a bounded divergent sequence and also a unbounded one.) There are, however , some general facts m conservative matrices that suggests further study an conullity. (m is space of bounded sequence with sup-norm.

Wil & Zeller , TAMS (1955) showed that $C \supset m \cap C_A$, if A conegular .

Mazur Orlicz , Stu. M (1954) proved that, if A is eoregular , than $\forall$ B with $C_B \supset m \cap C_A$, $\lim_A mC \to \lim_A = \lim_B mm \cap C_A$. Jurimae , E Tartu U (1965) defined that

(i) $A \in J$ (Chang et al say), if $C \supset m \cap C_A$ in C_A .

(ii) $A \in O$, if $\forall B$, with $C_B \supset m \cap C_A$ and $\lim_A = \lim_B mC \to \lim_A = \lim_B$ an $m \cap C_A$.

Clearly , if A is coregula , then $A \in J$ & $A \in O$. He further remarked that $A \in J \to A \in O$, Unfortunately , this is false in general , by considering .

$$P = \begin{pmatrix} \frac{1}{2} & & & & & \\ 1 & -1 & & & & \\ 1 & -1 & \frac{1}{2^3} & & & \\ 1 & -1 & \frac{1}{2^3} & \frac{1}{2^4} & & \\ \frac{1}{2} & \frac{1}{2^2} & \frac{1}{2^3} & 1 & -1 & \end{pmatrix}$$

P : conull

$P \in J$ & $P \in O$

(Chang , Macphail , Snyder & Wil , M.Z. (1968)

In the article of Wil , Distinguished subsets & summability invariants . J.d'Anal. Math (1964), says that for $f \in C_A'$.

$$f(x) = \sum_k f(\delta^k) x_k + \alpha(\lim_A x - \sum_k \lim_A \delta^k x_k), \forall x \in m \cap C_A$$

Define that

$$W_1 = \{ x \in C_A \mid f(x) = \sum_k f(\delta^k) x_k , \forall f \in C_A' \}$$

A.K. Snyder . counll FK- space . M.Z (1965) proved that A is conull $\Leftrightarrow 1 \in W_1$

In Chang et al say that if A conull , $A \in O \rightarrow W_1 \supset m \cap C_A$. These facts suggests a generalization of conullity ($A \in O$ as well).

With an aid of two-norm theory (Suggested by polish school), much work has been done recently .

① (Snyder, 1965) X is conull FK-sp $\Leftrightarrow 1 \in 2$ - norm cl. of E^∞ with respect $\| \|_\infty$.

② (Chang 1970) $X \in O$, & conull $\Leftrightarrow m \cap X \subset 2$ - norm cl. of E^∞ for semi-cons.(Snyder - Wil)

③ (Sember to appear) X is conull $\Leftrightarrow 1 \in 2$-n.l. cl of E^∞ w.r.t. $\| \|_{bv}$.

④ (Sember) X is v - FK, X conull $\Rightarrow 1 \in E$ (v), and $\Leftarrow$ is false in general .

Mathematatic logic : its methods and some results

數理邏輯的方法及結果

在證明定理的過程中，我們需用推理的方法。現在我們便以它們爲對象，以數學方法研究思考過程中的特徵，結果，並以符號表示。其中與數學有關的即稱數理邏輯。

這門學問是於1899年，由Frege和Hilbert開始研究，他們將亞里斯多德的方法，以符號表之。他們的目的在證明上以符號化推理過程，將兩千多年前的logic系統化、符號化。

到1900年，Peano將Frege的符號改造，將數學中所需要的東西符號化，並建立Peano公設（即自然數五公設），其中數學歸納法（即對任何條件 $\varphi(x)$, if $\varphi(0)$, and $\forall n[\varphi(n)\rightarrow\varphi(n+1)]$ 則 $\forall n\,\varphi(n)$）即無法以Frege的方法表示出。所以Peano與Frege的符號，有語言與層次之差。

Frege之語：

基本符號：x, y, z, ………

P(predlicate)：P_1, P_2, ……

→, V, &, ¬, ∀, ∃.

但其中∀，∃爲量化符，僅對x，y，z起量化，對述詞不發生量化作用，是爲初階語言。

1930至1935年發現，set theory及algebra均可以初階語言表示。這些符號便成爲研究logic（Object language）的語言（Mata language）。二者不同，前者較嚴密。但爲了研究Object language，我們除了用Mate language外，常常還要用第三種語言。如考慮對於P（述詞）的量化，則有二階語言。這在討論代數以外的東西時，常常需要的。對於各階語言，必須層次分明；否則便常會發生像“我的話是謊言”這類的Paradox。

從1900至1920，邏輯分成許多體系，如二次邏輯，採用對分法。古典邏輯即屬此類，以 $A\vee\neg A$ 爲公設之一。但有人反對這條公設，他們認爲，當所考慮的對象有無限多時，這條公設就不適用了。例如：令 $x\in N$，$\varphi(x)$爲“x爲質數”，則對很大的數，就不易判定 $\varphi(x)$ 或者 $\neg\varphi(x)$。試觀察存在定理中的證明，可發現它們多半只告訴我們某種東西存在，但却不能幫我們找出那東西。（例如：f在[a, b]中存在有max and min）。這類證明多半利用排中律（

$A \vee \neg A$ ）及選擇公設。所以關於存在證明，就發生兩派觀點。一即所謂的 Constructive proof ，就是要以有限的步驟找出所要的；另一為 nonconstructive proof ，只利用選擇公設證明存在而已。於是在數學中就劃分出 constructive mathematics 及 nonconstructive mathematics 而 Constructive Logic 與 Classical Logic 最大的不同處就是在於 $A \vee \neg A$ 被一腳踢開。

Classical logic 的公設如下：令 A、B、C、……表 statements A(x) 表示一個 statement containing x.

I. Axiom Schemata

1. $A \to (B \to A)$
2. $[A \to (B \to C)] \to [(A \to B) \to (A \to C)]$
3. $A \& B \to A$
4. $A \& B \to B$
5. $A \to (B \to A \& B)$
6. $A \to A \vee B$
7. $B \to A \vee B$
8. $(A \to C) \to [(B \to C) \to [A \vee B \to C]]$
9. $(A \to B) \to [(A \to \neg B) \to \neg A]$
10. $\neg A \to (A \to B)$
11. $A \vee \neg A$ （或 $\neg\neg A \to A$ ）

II.

12. $A(x) \to \exists x A(x)$
13. $\forall x A(x) \to A(x)$

III. Rules of Inference

R_1 ： A ， $A \to B$ 　則 B

R_2 ： $A(x) \to C$ ， C 與 x 無關，則 $\exists x A(x) \to C$

R_3 ： $C \to A(x)$ ， $\therefore C \to \forall x A(x)$

把第 11 條的排中律從古典邏輯中除去，便是 Constructive Logic 中的 Intuitonistic Logic（ I L ）。IL 還不敢排除第 1 條，因為沒有它的話，麻煩就大了。這種邏輯雖然很 Constructive ，但不很成功。像向量空間的基底存在問題，就得費很大的功夫才得證明，以荷蘭一帶的新潮派最樂衷此道了。

古典邏輯採用二值，所以可以用眞值表來研究。但在 I L 中，則眞值有 Countable many ，沒有眞值表可供研究．這眞是天壤之別。理論上，I L 比古典的強，但是古典的二值却簡化了許多證明。

I L 之眞值有 Countable many 是 Godel 在 1930 年提出的。Godel 在 1931 年又證出 Completeness theorem ，即“如果一句話 A 是眞的，那麼 A（在系統內）可以得到證明。”所謂證明，也就是一串公式 S_1 ， S_2 ，…， S_n ，其中 S_i 或為公理，或為 S_j （ $j < i$ ）的結論。Completeness 定理給當時一個很大的鼓舞。早在 1904 年，德國的數學家 Hilbert 就想造出一種機械，能夠證出所有的數學定理來。但是 Godel 在 1934 年證出，如果建立一個系統 A，包

含Peano公設如/A無矛盾，則 /A 不可能完備；如果/A內種種有限方法證明/A 本身是沒有矛盾的。因此一個系統的一致性無法由其自身證明，除非再找來一些比此系本身更有力的方法。這個發現使Hilbert的希望完全成了泡影，數學的眞理原來不是公理化所能窮盡的。

1935年至1936年，Church,Turing證出，“若φ爲CL（古典邏輯，下同）的一個敍述，則無法以有限步驟證出「CL is not decidable」”如果這個定理不對，我們就可以着手建造一個計算機，讓它建立全部數學。但是這個定理却告訴我們，數學的建立還須要一種超特、獨創的概念，“Mathematics needs creative idea as well as logic”所以光靠邏輯是不夠的，數學家的頭腦還是不能缺少。

求全雖然無法實現，但是我們却從Church Turing 的這條定理獲得啓示。通常我們以爲任何問題均可解決，判定爲眞、假，或許一時不能解決，但終有解決的一天。今後我們的數學問題將分成三類：

1. Can be solvable：根據有限步驟，可決定對；
2. unsolvable ：根據有限步驟，可決定不對；
3. undecidable：有限步驟不能決定。

1936 年以後，一群邏輯學家開始對幾個古老的問題加以探索，判定它們到底是屬於那一類的問題。所以邏輯家的工作其實就是和交通警察一樣，指出數學家的方向，不要走向那些 undecidable 的問題。至於解決問題，則交給數學家，這是需要創造性的思考。

1908至1968 這段時間，公設化的集合論漸漸被建立起來，如Zermelo ，Frankel，Jon Neumann ，G[illegible]l 等人均從事此工作。ZF+AC 即爲前二者建立之公設化理論；N－G－B＋AC 則爲後二者和瑞士的Bernays所建立，其中AC表Axiom of Choice ，即

若$F=\{A_i \mid i \in I, i \neq j \quad A_i \cap A_j = \phi, A_i \neq \phi\}$，

則 $\exists x_i \,[\, C \cap A_i = \{x_i\} \,]$

這兩個系統均包含AC，AC 是否會使兩者引起矛盾呢？1939年，Godel 證明，如果ZF（NGB）是沒有矛盾的話，那ZF+AC（NGB+AC）還是沒有矛盾的。至此，數學家獲得邏輯上的保證，可以放心地去使用AC。但是Axiom of Choice 是不是眞實的呢？

在1924年，Banch和Tarski同時發現，應用set theory 中的公理及AC，可將一個半徑爲r的球分成兩個半徑均爲γ的球；同樣地應用AC，若將橘子分成α片，地球分成α片，則地球的每一片均可放入橘子中。這種驚人的結果，使大家希望AC爲假，即希望ZF＋¬AC 也能成立。這就引起一個問題，即AC是否和ZF獨立呢？史丹福大學的Paul J. Cohen解決了這個問題，在1963 年，他證明出AC獨立於ZF，N－G－B，爲此他獲得 field smedal。因此，

以ZF＋＞AC建立新系統是可以的，但是這件工作至今尚在研究。

至此，set theory 與math漸漸分離，(1936 年以後，發展出全新數學)，希望能發展出不建於 set theory 之數學。

參考書 Math logic

Schoenfield : Mathematical logic

1967 Addison-Wesley

Field extension

We have field Q and its subset J(integers) in which we have addition, multiplication. The division in J is not closed. Now we want to enlarge the field Q. How do we it ?

Let J be the set of integers, Q the set of rationals,

$$Q(I) = \{ \frac{f(I)}{g(I)} \mid f, g \text{ be polynomials on } J \}$$

If I be a root of some $f(x) \varepsilon Q[x]$, then I is algebraic. Q(I) is called an extension field of Q. What shall we mean by an "integer" in this field? An element $\xi \varepsilon Q(I)$ is called an "algebraic integer" if ξ is a root of some $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$, $a_i \varepsilon J$.

If I be an algebraic integer; let it satisfy the equation $x^2 + 2ax + b = 0$, where a, b are rational numbers. Then I is of the form $\gamma + s\sqrt{m}$, where γ, $s \in Q$, and m is a square free integer. Clearly

$$Q(I) = Q(\sqrt{m}) = \{ \frac{a + b\sqrt{m}}{c} \mid a, b, c \in J, (a, b, c) = 1, c > 0 \}$$

If $\xi = \dfrac{a + b\sqrt{m}}{c}$, then since $(\dfrac{a + b\sqrt{m}}{c})(\dfrac{a - b\sqrt{m}}{c}) = \dfrac{a^2 - b^2 m}{c^2}$,

and $\dfrac{a + b\sqrt{m}}{c} + \dfrac{a - b\sqrt{m}}{c} = \dfrac{2a}{c}$, ξ is a root of

$$x^2 - \frac{2a}{c} x + \frac{a^2 - b^2 m}{c^2} = 0 .$$

Hence, if $\dfrac{2a}{c}$ and $\dfrac{a^2 - b^2 m}{c^2}$ are integers, then ξ will be an algebraic integer of Q(g). Now we want to know what does an integer in Q(I) look like.

Let $(a, c) = d$

Since $\frac{a^2 - b^2 m}{c^2} \varepsilon J$, and $d^2 | a^2$, $d^2 | c^2$, we have $d^2 | b^2 m$. But $(a, b, c) = 1$, hence $d = 1$.

Since $\frac{2a}{c} \varepsilon J$, $c | 2$, thus $c = 1$, or 2.

If $c = 1$, $\xi = a + b\sqrt{m}$ is an integer in Q(I).

If $c = 2$, then $a \equiv 1 \pmod 2$ since $(a, c) = 1$.

and $a^2 - b^2 m \equiv 0 \pmod 4$ since $c = 2$.

$\therefore\ b^2 m \equiv a^2 \equiv 1 \pmod 4$

$\therefore\ b \equiv 1 \pmod 2$

$\therefore\ m \equiv 1 \pmod 4$

Therefore if $Q(I) = Q(\sqrt{m}) = \{\frac{a + b\sqrt{m}}{c} | a, b, c \varepsilon J,\ c > 0,\ (a, b, c) = 1\}$, integers of Q(I) is of the form

(i) $m \equiv 1 \pmod 4$, then $\frac{a + b\sqrt{m}}{2}$ are integers in Q(g), where $a \equiv b \equiv 1 \pmod 2$.

(ii) $m \not\equiv 1 \pmod 4$, the integers are $a + b\sqrt{m}$.

Note that the above proog stilled needs fulfilled Example. In $Q(\sqrt{-1}) = Q(i)$, integers are called Gaussian integers. This is an excellent example of Euclidean ring. In a Euclidean ring, we have divisiblity, Common divisor, etc.

Now we consider a property of J in Q: J has unique factorization property, i.e., factorization of integers into primes is " essentially unique, up to association. For example,

$$12 = 2^2 \cdot 3 \cdot 1 = 3 \cdot 2^2 \cdot 1 = 2 \cdot (-3) \cdot (-2)$$

Whether $Q(\sqrt{m})$ has unique factorization or not ? We still have many problem in this part.

For each $\xi \varepsilon Q(\sqrt{m})$, if $\xi = \gamma + s\sqrt{m}$, where $\gamma, s \varepsilon Q$, we define $N(\xi) = \gamma^2 - s^2m$ to be the norm of ξ. A little computation shows that $N(\alpha\beta) = N(\alpha)N(\beta)$. Thus, if $\alpha \mid \gamma$, then $N(\alpha) \mid N(\gamma)$. Also, if ξ is an integer in $Q(\sqrt{m})$, then $N(\xi) \varepsilon J$.

With the help of the above, we may find units of a quadratic domain. For example, let us find all the units in the quadratic domain $Q(\sqrt{-1})$:

if $\alpha \mid 1 \qquad N(\alpha) \mid 1$,

let $\alpha = a + b\sqrt{-1}$, $N(\alpha) = a^2 + b^2 \mid 1$

$\therefore \; N(\alpha) = a^2 + b^2 = 1$

$\therefore \; \alpha = \pm 1, \; b = 0$; or

$a = 0, \; b = \pm 1$

Therefore $1, -1, +i, -i$ are the only units of $Q(i)$.

The next example shows that we may have inginitely many units, and the unit can occur to be arbitrarily large.

Example. In $Q(\sqrt{2})$, if $\alpha = a + b\sqrt{2}$, $a, b \varepsilon J$ is to be a unit, then

$N(\alpha) = a^2 - 2b^2 \mid 1 \rightarrow a^2 - 2b^2 = \pm 1 \rightarrow a = \pm 1, \; b = 0$; or $a = \pm 1, b = \pm 1$

Since $(1+\sqrt{2})(-1+\sqrt{2}) = 1 \qquad (1+\sqrt{2})^n(-1+\sqrt{2})^n = 1$

All these elements $(1+\sqrt{2})^n$ are units of $Q(\sqrt{2})$.

An element of a quadratic domain is called prime if the only divisors of it are units and itself.

Example. $Q(\sqrt{-5})$ has ± 1 as its units. 3 is a prime in $Q(\sqrt{-5})$. We show this as follows :

Since $N(3) = 9$, $\therefore \; \alpha \neq \pm 1, 9 \quad \alpha \mid 3 \Longrightarrow N(\alpha) \mid 9 \Longrightarrow N(\alpha) = 3$

$-5 \not\equiv 1 \pmod{4}$

$\therefore\quad \alpha = a + b\sqrt{-5}$, $a^2 + 5b^2 = 3$ has no integer root.

$\therefore\quad$ 3 is a prime.

Similarly , 2 , $1+\sqrt{-5}$, $1-\sqrt{-5}$ are primes in $Q(\sqrt{-5})$, but $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ shows that there are two distinct factorizations of 6. Hence $Q(\sqrt{-5})$ has no unique factorization property.

Example. In $Q(\sqrt{-6})$, $6 = 2\cdot 3 = (\sqrt{-6})(\sqrt{-6})$

In $Q(\sqrt{10})$, $10 = 2\cdot 5 = \sqrt{10}\cdot\sqrt{10}$

In $Q(\sqrt{82})$, $-713 = (-23)(31) = (5+3\sqrt{82})(5-3\sqrt{82})$.

We conclude that there are fields which do not have unique factorization.

But we can not ouspect that all fields do not have unique factorization. For instance , Gaussian integers in $Q(i)$ do have unique factorization. Although the unique factorization is not generally true for any algebraic integer , the mathematicians still hope that unique factorization in other sense may be found.

Example. In $Q(\sqrt{-5})$, factorizing 21 , we find

$$3\cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5}) = (4+\sqrt{-5})(4-\sqrt{-5})$$

are all possible factorization of 21.

We hope to use prime ideal to get a property of (21) , which may be called unique factorization.

Consider $P_1 = (3, 1+2\sqrt{-5}) = \{3\alpha + (1+2\sqrt{-5})\beta \mid \alpha, \beta$ integers in $Q(\sqrt{-5})\}$

$P_2 = (3, 1-2\sqrt{-5})$,

$Q_1 = (7, 1+2\sqrt{-5})$,

$Q_2 = (7, 1-2\sqrt{-5})$.

P_1 , P_2 , Q_1 and Q_2 are prime ideals of $Q(\sqrt{-5})$,

$P_1P_2 = (9, 3-6\sqrt{-5}, 3+6\sqrt{-5}, 21) = (3)$

(since $3 = 21\cdot 1 + 9\cdot(-2)$, $3 \in P_1P_2$)

$Q_1Q_2 = (7)$, $P_1Q_2 = (4-\sqrt{-5})$, $P_1Q_1 = (1+2\sqrt{-5})$,

$P_2Q_1 = (4+\sqrt{-5})$, $P_2Q_2 = (1-2\sqrt{-5})$

$\therefore$ $(21)=P_1P_2Q_1Q_2$. We have factorized the ideal (21) into prime ideals. We may suspect that the ideal generated by an algebraic integer can have unique factorization , although the integer may not have unique factorization.

參考書：

Hardy and Wright : Number theory

Harry Pollard : The theory of algebraic numbers

分解性質

王懷權

一個代數（algebra）（A，＋，・）一定具有$A+A=A$及$A^2\subset A$的基本性質。我們現在問一個有趣的問題：是否任一代數A皆有$A^2=A$的性質？此處$A^2=A$意義乃指A之每一個x皆為A中y與z之乘積。當$A^2=A$時我們稱A可分解。否則稱A不可分解。我們知道如果A中有單位元素的話，A一定為可分解。

分解乃純代數性質，但據我們所知，還沒有純代數學家來惹她。為什麼？我們的看法有二：第一是不好惹，就如同代數基本定理（Fundameutal theorem of algebra）的證明。第二是沒時間惹，所謂美景不能盡收。

如果A為一巴氏代數（Banach algebra），則A已經被關心到了。Cohen〔1〕找到一個使A可分解的充分條件。我個人Wang〔4〕也找到一個使A不可分解的充分條件，讀君若有興趣，不妨由Referreuas找出Papers看看。

我們願意在此舉出並加以證明兩個例子，其一為可分解，另一為不可分解。這兩個都是群代數（group algebra）一個群代數是在同一個給定的局部緊緻群上的函數集，此函數集用普通加，矢乘法及用Convolution當乘法而形成一個巴氏代數。

I. 可分解代數的例子：若R為實數拓樸群，R上有一Lebesgue measure，令$L^1(R)$為R上可積分函數集。若f，$g\in L^1(R)$，而α為一複素集，定義 $(f+g)(x)=f(x)+g(x)$，$(\alpha f)(x)=\alpha f(x)$，$(f*g)(x)=\int f(x-y)g(y)dy$，$\|f\|=\int|f(x)|dx$，則$L^1(R)$形成一個群代數。

定理：$L^1(R)$為一可分解代數。

證明：此證明乃摘自Rudin〔2，3〕。在此證明中我們假設讀君對於調和分析的一些基本性質已經知道。

若$f\in L^1(R)$。令$(K_t)_{t>0}$為Fejér Rernel。令$\in(t)=\|K_t*f-f\|$。則$\in(t)\to 0$ as $t\to\infty$。可找到$(0,\infty)$上的一個正且連續的函數x滿足$\int_0^\infty\{\in(t)+\frac{1}{t}\}\propto(t)dt<\infty$但$\int_0^\infty\alpha(t)dt=\infty$。定義$\phi(t)=1+\int_0^t\propto(s)ds+t\int_t^\infty\frac{\propto(s)}{s}ds$ $(t\geq 0)$，則$\phi(t)<\infty$且$\phi(t)\to\infty$ as $t\to\infty$. 並且ϕ為凸集合。

定義$g(x)=f(x)+\int_0^\infty\{f(x)-(f*K_t)(x)\}\propto(t)dt$. 由Fubini定理以及調和分析的基本性質知道 $g\in L^1(R)$且

$\hat{g}(y)=\hat{f}(y)\{1+\int_0^\infty[1-\hat{K}t(y)]\propto$

$(t)\,dt\}=f(y)\,\phi(|y|)$。故 $\hat{f}(y)=\hat{g}(y)\,\lambda(|y|)$，此處 $\lambda(|y|)=\dfrac{1}{\phi(|y|)}$．若令 $h(x)=\int_0^\infty K_t(x)\,t\,\lambda''(t)\,dt$，則 $h\in L^1(R)$ 且 $\hat{h}(y)=\lambda(|y|)$．故 $\hat{f}(y)=\hat{g}(\mu)\,\hat{h}(\mu)$，即 $f=g*h$．故得證

Ⅱ．不可分解代數的例子：令T爲圓群（the circle group）即此緊致群 $\{z : z$ comple with $|z|=1\}$，亦即實數軸上的 $(0,2\pi)$ 令 $L^1(T)$ 爲T上可積分函數集。仿Ⅰ之定義，$L^1(T)$ 爲一群代數。若 $f\in L^1(T)$，用 $\hat{f}(n)$ 表 f 在 n 之富氏係數。

引理：若A爲 $L^1(T)$ 之一子代數，存在一 p_0，$0<p_0<\infty$，使得A中每一 f 有 $(\hat{f}(n))\in l^{p_0}$。若 $A^2=A$，則對所有 p，$0<p\leq\infty$ 及A中每一 f 有 $(\hat{f}(n))\in l^p$．

證明：由調和分析基本性質知道任一 $f\in A$ 有 $(\hat{f}(n))\in l^\infty$ 的性質，因此對任一 $f\in A$，$(\hat{f}(n))\in l^p$，$p_0\leq p\leq\infty$。

其次令 $f\in A$，則有 g，$h\in A$ 使得 $f=g*h$，亦即 $\hat{f}=\hat{g}\hat{h}$。因 $\Sigma|\hat{f}(n)|^{\frac{p_0}{2}}=\Sigma|\hat{g}(n)|^{\frac{p_0}{2}}|\hat{h}(n)|^{\frac{p_0}{2}}\leq(\Sigma|\hat{g}(n)|^{p_0})^{\frac{1}{2}}(\Sigma|\hat{h}(n)|^{p_0})^{\frac{1}{2}}<\infty$，所以 $(\hat{f}(n))\in l^{\frac{p_0}{2}}$。繼續這類似的步驟，我們得到 $(\hat{f}(n))\in l^{\frac{p_0}{2^m}}$，，$m=1,2,\cdots\cdots$，現在對任一 p，$0<p\leq p_0$，一定可以找到一個m使得 $\frac{p_0}{2^m}<p\leq p_0$。因此 $(\hat{f}(n))\in l^p$。此引理得證。

若 $C(T)$ 表在T上之連續函數集。定義 $C(T)$ 上的代數運算如Ⅰ及模爲 $\|f\|=\max\limits_{x\in T}|f(x)|$，則 $C(T)$ 爲一群代數。

定理：$C(T)$ 爲一不可分解代數。

證明：我們知道 $C(T)\subset L^2(T)\subset L^1(T)$ 以及每一 $f\in L^2(T)$ 有 $(\hat{f}(n))\in l^2$ 的性質，此處 $L^2(T)$ 表T上平方可積分函數集。因此每一 $f\in C(T)$ 均有 $(\hat{f}(n))\in l^2$ 的性質，假設 $C(T)$ 爲一可分解代數，由引理知道 $(\hat{f}(n))\in l^p$，$0<p\leq\infty$，爲了要證明 $C(T)$ 爲不可分，我們只要在 $C(T)$ 中找到一個 f 使得 $(\hat{f}(n))\notin l^r$，對某一 r，$0<r<\infty$。我們知道對任一整數 n，$e^{int}\in C(T)$。因爲 $\sum\limits_{n=1}^{\infty}\dfrac{\|e^{int}\|}{n^2}=\sum\limits_{n=1}^{\infty}\dfrac{1}{n^2}<\infty$，又 $C(T)$ 爲一巴氏空間，所以存在一個 $f\in C(T)$ 使得 $f(t)=\sum\limits_{n=1}^{\infty}\dfrac{e^{int}}{n^2}$。

因爲 $\sum\limits_{m=-\infty}^{\infty}|\hat{f}(m)|^{\frac{1}{2}}=\sum\limits_{m-1}^{\infty}|\hat{f}(m)|^{\frac{1}{2}}=\sum\limits_{m=1}^{\infty}\left|\dfrac{1}{m^2}\right|^{\frac{1}{2}}=\sum\limits_{m=1}^{\infty}\dfrac{1}{m}=\infty$，故 $(\hat{f}(m))\notin l^{\frac{1}{2}}$。

Peferrences

〔1〕P. J. Cohen, Factorization in group algebras , Dake Math. J. 26(1954) 199-250).

〔 2 〕W. Rudin , Fectorization in the group algebra of the real line, proc Nat. Acad. Sci. 43(1957), 339-340

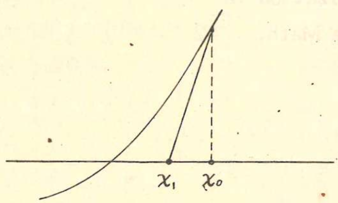
〔 3 〕W. Rudin , Representation of fanct- ious by convolutions , J. Math. 7(1958), 103-116.

〔 4 〕H.C. Wang , Nonfactorization in group algebras , Studia Math. , 42 (1972), 231-241.

Some Application of the Implicit Function Theorem to Differential Equations

Jan W. Nienhuys

If we want to find a zero of a function f (a nice function) we can do as



follows : Start at x_0 let the slope of f be about equal to the number p. Define

$$x_1 = x_0 - p^{-1} f(x_0)$$

$$x_2 = x_1 - p^{-1} f(x_1)$$

If this converges , then the ceft hand converges to some point x_{lim} . By continuity of f, the right hand converges to $x_{lim} - p^{-1} f(x_{lim})$. So $p^{-1} f(x_{lim}) = 0$ hence $f(x_{lim}) = 0$.

Now, can we find out whether it converges ?

Let us look to

$$x_{i+1} - x_i = x_i - x_{i-1} - p^{-1} (f(x_i) - f(x_{i-1}))$$

If we suppose that

$$g(x) = x - p^{-1} f(x)$$

has the property .

(1) $| g(x) - g(x^1) | \leq C \, | x - x^1 |$ for some $C < 1$ then.

(2) $| x_{i+1} - x_i | \leq C \, | x_i - x_{i-1} | \leq \cdots \leq C^i \, | x_1 - x_0 | = C^i | p^{-1} f(x_0) |$ So we

can condude.

(3) $|x_{i+1} - x_0| \leq |x_{i+1} - x_i| + |x_i - x_{i-1}| + \cdots\cdots + |x_1 - x_1| \leq$

$$(C^i + C^{i-1} + \cdots\cdots + 1)\,|p^{-1}f(x_0)| = \frac{1 - C^{i+1}}{1 - C}\,|p^{-1}f(x_0)$$

and likewise.

(4) $$|x_{i+1} - x_{j+1}| \leq \frac{|C^{j+1} - C^{i+1}|}{1 - C}\,|p^{-1}f(x_0)|$$

Both (3) and (4) follow from the formula for a partial sum of a geometric series with common ratio C.

The inequality (4) is just what we are looking for: it tells us that the sequence $\{x_i\}$ is a Cauchy sequence (remember, $C < 1$) :

The diffi cult points are not cleaved up yet, for we cannot be sure, in general, that (1) holds for all x ,and x^1.

So we make an assumption, namely that it holds whenever x and x^1 are in the set $B = \{x \mid |x - x_0| \leq A\}$.

In that case estimates (2) can only be made when x_i, x_{i-1}, ⋯ etc are all in B. But for x_i, x_{i-1}, ⋯⋯ etc it follows than that inequalities (3) hold (with i, $i-1$, etc. instead of $i+1$)

If $\dfrac{|p^{-1}f(x_0)|}{1 - C} \leq A$ then x_i, x_{i-1}, ⋯⋯ etc are all in B. This means

$|p^{-1}f(x_0)| \leq A(1 - C)$.

Is there any way to tell whether (1) is true in a set like B ? Sure we have the meanvalue theorem :

Theorem 1. Let' $f : V \rightarrow W$ be differentiable Suppose for all x in a convex set B we have

$$\| f'(x) \| \leq M$$

(We suppose V, W are vectorspaces with norm and the above inequality means that $\| f'(x)\,h \| \leq M \| h \|$ for all $x \in B$ and $h \in V$.

f' is a linear map.)

Then also, for all $x, y \in B$

$$\| f(y) - f(x) \| \leq M \| y - x \|$$

We omit the proof. It is based on the idea that this inequality is " almost true " if y and x are very dose together. Then one goes along a straight line in small steps from x to y.

If we apply this theorem to the function

$$g(x) = x - p^{-1} f(x)$$

we find $g'(x) = 1 - p^{-1} \dfrac{df}{dx}(x)$

we can now formulate a theorem.

Theorem 2. Suppose f differentiable in the set. $B = \{x \mid |x - x_0| \leq A\}$.

Suppose there exists a $C < 1$ and a number $p \neq 0$ such that

(i) $\left| 1 - p^{-1} \dfrac{df}{dx}(x) \right| \leq C$ for $x \in B$

(ii) $| p^{-1} f(x_0) | \leq A(1 - C)$.

Then f has a unique zero in B.

Proof: we have almost everything proved, except the uniqueness of the root. But if $f(x) = f(y) = 0$ then

$$|x - y| = |x - p^{-1}f(x) - y + p^{-1}f(y)| = |g(x) - g(y)| \leq C|x - y|$$

As $C < 1$ uniqueness follows.

Now we suppose f depends on an extra parameter t: $f(x, t)$

For every t we can do the constructions above. We get functions $x_i(t)$ of t. All the x_i are continuous. Put $x_0(t) \equiv x_0$

(4) will change into $|x_{i+1}(t) - x_{j+1}(t)| \leq \dfrac{|C^{j+1} - C^{i+1}|}{1 - C} |p^{-1} f(x_0, t)|$

If we suppose that (i) and (ii) of the above theorem hold uniform in t for t in some set D, we can conclude from (4) that the $x_i(t)$ form a uniform convergent sequence of functions in D. Hence the limit is a continuous function.

So we can formulate another theorem.

Theorem 3. Suppose $\frac{\partial f}{\partial x}(x,t)$ exists throughout $B \times D$; $B = \{x \mid |x - x_0| \leq A\}$. Suppose there exists a constant $C < 1$ and a number $p \neq 0$ such that

(i) $\left| 1 - p^{-1} \frac{\partial f}{\partial x}(x,t) \right| \leq C$ in $B \times D$

(ii) $| p^{-1} f(x_0, t) | \leq A(1-C)$ for $t \in D$.

Then there exists a unique continuous function

$$x : D \to B : t \to x(t)$$

such that

$$f(x(t), t) = 0$$

From this follows immedidtely another theorem Implicit Function Theorem

Theorem 4. Let $f(x,t)$ and $\frac{\partial f}{\partial x}(x,t)$ be continuous throughout $B \times D$

Suppose for $(x_0, t_0) \in B \times D$.

(i) $\frac{\partial f}{\partial x}(x_0, t_0) = p \neq 0$

(ii) $f(x_0, t_0) = 0$

Then there exists a unique function defined on a heighborhood D' of t_0, values in B such that

$$f(x(t), t) = 0$$

Proof $\left| 1 - p^{-1} \frac{\partial f}{\partial x}(x_0, t_0) \right| = 0$ so

$$|1-p^{-1}\frac{\partial f}{\partial x}(x,t)| \leq 1/2$$ in some neighborhood $B' \times D'$ of (x_0, t_0) (By continuity of $\frac{\partial f}{\partial x}$)

$|p^{-1} f(x_0, t_0)| = 0$ so

$|p^{-1} f(x_0, t)| \leq A' \cdot \frac{1}{2}$ for A' = radius of B' and t in some neighborhood $D'' \subset D'$ of t_0. (By continuity of f).

Remark 1. We have done everything in $R \times R$, 1-dimensional vector spaces. However we may do the same thing in a so-called Banach space. A Banach space is a vector space V with a norm $\| \cdot \| : V \to R^+$: $x \to \|x\|$ such that

(i) $\|x\| = 0$ $x = 0$

(ii) $\|\alpha x\| = |\alpha| \, \|x\|$

(iii) $\|x+y\| \leq \|x\| + \|y\|$ triangle inequality

(iv) Cauchy sequences in V have a limit in V.

The standard example of a Banach space is the space of continuous functions on some set T, with norm $\|x\| = \sup\limits_{t \in T} |x(t)|$. Condition (iv) is fulfilled because a Cauchy sequence neaus here a uniformly convergent sequence of continuous functions.

Because of (iv) we make "Fake" any limit of a Cauchy sequence.

We can repeat the proof of Theorem 3 word by word, if we write $\| \;\|$ instead of $| \;|$ everywhere, in the care $B \times D$ is in some Banach space $V_1 \times V_2$.

The expression $1-p^{-1}\frac{\partial f}{\partial x}$ has to be changed into $I - p^{-1}\frac{\partial f}{\partial x}$; I = identity map. p should now be a linear continuous map with continuous inverse . (Students of Banach spaces know that continuity and boundedness are equivalent for linear maps ; in finite dimensional spaces a linear map is always bounded on the unit - ball , but in general Banach spaces this need not be true.)

Remark 2. If $f(x,t)$ continuously differentiable then the implicit function is also continuously differentiable (when $\frac{\partial f}{\partial x}$ is invertible) and the devivative x' can be found by differentiating

$$f(x(t), t) = 0$$

with respect to t :

$$f_x x' + f_t = 0$$

Remark 3. Instead of f differentiable with respect to x one may take other conditions to substitute the use of the Mean Value Theorem. We will not do that here .

Applications to differential equations. First we apply Theorem 3 to prove existence and uniqueness for differential equations . We will at the same time find that the solutions depend continuously (differentiably) on the initial conditions.

Let us consider the problem

$$x'(t) = f(x,t) \qquad \tau,\ t \in T_a = \{ t \mid |t - t_0| \leq a \} .$$

$$x(\tau) = \S \qquad x, x^1, \S \in X , \text{ finite dimensional vector space}$$

We suppose f is continuously differentiable with respect to x in $T_a \times X_b$; $X_b = \{ x \mid \| x - x_0 \| \leq b \}$. Suppose $\| \frac{\partial f}{\partial x} \| \leq M^1$ and $\| f(x) \| < M$ throughout $T_a \times X_b$ if $a \leq a_0$. We write the problem as an integral equation :

$$x(t) - \S - \int_{\tau}^{t} f(x(s), \S, s)\, ds = 0 \qquad (*)$$

Now observe that for any function x on T_a with values in X_b, the left hand mernber is defined. So we introduce the Banach space V of continuous functions $T_a \to X$ with norm $\|x\|_v = \sup_{t\in T_a} \|x(t)\|$. We take a special point $x_0 \in V$, which is the function $x_0(t) \equiv x_0$.

(One should in the above distinguish between functions $x : T_a \to X$ and vecfors $x \in X$. The former are elements of **V**. Unfortunately the notation is a little confusing).

We can now write for the left hand member of (*).

$F(x, \S, \tau)$, which is in V again ; defined for $x \in B = \{x \mid \|x - x_0\| \leq b\}$, $\S \in X_b$, $\tau \in T_a$, we take $p = I$.

$\frac{\partial F}{\partial x}$ is computed from :

$$F(x+h, \S, \tau) - F(x, \S, \tau) = h(t) - \int_\tau^t f(x(s)+h(s), s) - f(x(s), s)\, ds =$$

$$h(t) - \int_\tau^t \frac{\partial f}{\partial x}(x(s), s)\, h(s)\, ds + o\,(h).$$

(The expressions in which t occurs should be interpreted as functions of the variable t, and not as vectors in X).

So $(I - \frac{\partial f}{\partial x})\, h = \int_\tau^t \frac{\partial f}{\partial x}(x(s),s) \quad h(s)\, ds$

We can estimate:

$$\|(I - \frac{\partial f}{\partial x})\, h\| \leq \int_{t_0-a}^{t_0+a} \|\frac{\partial f}{\partial x}\|\, \|h\|\, ds \leq 2a\, M' \|h\|.$$

So $\|I - \frac{\partial f}{\partial x}\| \leq 2a\, M'$.

Further more

$$\| F(x_0, \tau, \S) \| = \| x_0 - \S + \int_{\tau}^{t} f(x_0, s)\, ds \| \leq \| x_0 - \S \| + 2aM$$

Now we have not made any assumption on the range of $\S$: Let us assume that we only consider $\S$ s.t $\| \S - x_0 \| \leq b'$. ($b' \leq b$)

Then $\| F(x_0, \tau, \S) \| \leq b' + 2aM$.

Condition (i) and (ii) of Theorem 3 reced now

$$2aM' < 1$$

$$b' + 2aM \leq b(1 - 2aM')$$

These conditions can be satisfied by taking a and b' small enough.

So we obtain

Theorem : Let $f(x,t)$ be continuously differentiable with respect to x and bounded with respect to both variables on $T_{a_0} \times X_b$

Let the solction of

$$x'(t) = f(x_1 t)$$

$$x(\tau) = \S$$

be denoted by $x(t, \S, \tau)$

Let $\| \frac{\partial f}{\partial x} \| \leq M'$ and $\| f \| \leq M$ on $T_{a_0} \times X_b$.

Then, for $\S \in X_b'$ there exists a unique sountion

$$x(t, \S, \tau)$$

defined for τ, $t \in T_a$, $x(t, \S, \tau) \in X_b$, which depends continuously on $\S$ and τ (in the sense of being an element of V depending on $\S$ and τ)

if $\quad 2aM' < 1$ and $\quad b' + 2aM \leq b(1 - 2aM')$

Actually, because we assumed f differentiable with respect to x, we have also.

Theorem 5. $x(t, \S, \tau)$ is differentiable with respect to § and satisfies,

if $\frac{\partial x(t)}{\partial \S} = y(t)$, the equation

$$y' = \frac{\partial f(t)}{\partial x} y$$

$$y(t) = I$$

Proof y(t) is a linear map $X \rightarrow X$ and from the .

Remark 2. following Theorem 4 we have

$$\frac{\partial F}{\partial x} y + \frac{\partial F}{\partial \S} = 0$$

But $\frac{\partial F}{\partial \S} = -I$ (the function $T_a \rightarrow I$, $I : X \rightarrow X$ identity)

and so we obtain

$$y(t) - \int_{\tau}^{t} \frac{\partial f(x,s)}{\partial x} y(s)\, ds - I = 0$$

But this is just the integral form of the equation of the statement is know as the of the theorem.

Remark . This equation is known as the variation equation . One may derive one for $\frac{\partial x}{\partial \tau}$ too , if f is assumed continuous.

Now we prove as a second application a stability theorem..

Suppose we have an equation

$$x' = f(x) \quad , \quad f \text{ differentiable } X \rightarrow X$$

and 0 is a singular point : $f(0) = 0$

Then the equation can be written

$$x' = A\,x + g(x) \qquad (**)$$

in which $A = \frac{\partial f(0)}{\partial x}$ and $\frac{\| g(x) \|}{\| x \|} \to 0$

We hope that the solutions of this equation " behave " very much like the solutions of

$$x' = A_x$$

Suppose that $X = X_1 + X_2$, both X_1, X_2 invariant under A , $X_1 \cap X_2 = \{0\}$ and $A | X_1$ has only eigenvalves whose real part is negative and $A | X_2$ has only eigenvalves whose real part is positive. Put $A_1 = A | X_1$, $A_2 = A | X_2$.

Any vector v in X will be written as $v = v_1 + v_2$, $v_1 \in X_1$, $v_2 \in X_2$, v_1 and v_2 are unique.

Then $\| e^{A_1 t} v_1 \| \leq C e^{\mu_1 t} \| v_1 \| \qquad t \geq 0$

$\| e^{-A_2 t} v_2 \| \leq C e^{+\mu_1 t} \| v_2 \| \qquad t \geq 0$

for some $\mu_1 < 0$ and some $C > 0$.

We want to prove that X has a subspace S (not linear) which in a way looks like X_1, and such that any solution starting on S will stay on S and will approach 0 as quick as $e^{\mu_1 t}$.

To do this, first choose a μ , $\mu_1 < \mu < 0$. Introduce the Banach space V_μ of functions $[0, \infty) \to X$ such that $\| e^{-\mu t} x(t) \|$ is bounded. We give it the norm $\| x \|_\mu = \sup_{t\ 0} \| e^{-\mu t} x(t) \|$.

We convert (*x) into an integral equation. Then we must adapt the integral equation so it can be written as $F(x, \cdots) = 0$, $F(x_1 \cdots) \in V_\mu$ if $x \in V_\mu$.

The dots represent a variable whose nature we still must discuss.

$$x' = A_x + g(x)$$

We interpret this as an inhomogeneous linear equation, with inhomogeneous term $g(x(t))$.

Solution is

$$x(t) = e^{At}\, x(0) + \int_0^t e^{A\,t-s}\, g(x(s))\, ds$$

$$= e^{A_1 t}\, x_1(0) + e^{A_2 t}\, x_2(0) + \int_0^t e^{A_1(t-s)}\, g_1(x(s))\, ds + \int_0^t e^{A_2(t-s)} g_2(x(s))\, ds$$

Now, because $\lim\limits_{x\ 0} \dfrac{\|g(x)\|}{\|x\|} = 0$, we can state: for $\|x\|_\mu$ small enough

$$\|g_i(x(s))\| \leq \varepsilon \|x(s)\|$$

so $$\|g_i(x(s))\| \leq \varepsilon\, e^{\mu s}\, \|x\|_\mu \qquad i = 1, 2$$

We first use this for proving that

$$\int_0^\infty e^{-A_2 s}\, g_2(x(s))\, ds$$

converges, if $x \in V_\mu$, and $\|x\|_\mu$ small enough.

Indeed $\|e^{-A_2 s}\, g_2(x(s))\| \leq \varepsilon\, e^{+\mu_1 s}\, e^{\mu s}\, \|x\|_\mu$ for $\|x\|_\mu$ small enough

$$= \varepsilon \|x\|_\mu\, e^{s(\mu+\mu_1)} \qquad \mu + \mu_1 < 0, \text{ so}$$

convergence is established.

If we write $v_2(x) = \int_0^\infty e^{A_2(t-s)}\, g_2(x(s))\, ds$ then

our equation becomes

$$x(t) = e^{A_1 t}\, x_1(0) + e^{A_2 t}(x_2(0) + v_2(x))$$

$$+ \int_0^t e^{A_1(t-s)}\, g_1(x(s))\, ds - \int_t^\infty e^{A_2(t-s)}\, g_2(x(s))\, ds$$

We prove now that if $x \in V_\mu$ the first and the second integral represent functions of t that are in V_μ again. This is a little tedious computation:

$$\| e^{-\mu t} \int_0^t e^{A_1(t-s)} g_1(x(s))\, ds \| \leq$$

$$e^{-\mu t} \int_0^t e^{\mu_1(t-s)} \varepsilon e^{\mu s} \|x\|_\mu \, ds = \varepsilon \|x\|_\mu \int_0^t e^{(\mu_1-\mu)(t-s)} ds = \varepsilon \|x\|_\mu \int_0^t e^{(\mu_1-\mu)s'} ds'$$

which is bounded as $\mu_1 - \mu < 0$

$$\| e^{-\mu t} \int_t^\infty e^{A_2(t-s)} g_2(x(s))\, ds \| \leq \int_t^\infty e^{-\mu t} e^{\mu_1(s-t)} e^{\mu s} \varepsilon \|x\|_\mu \, ds =$$

$$\varepsilon \|x\|_\mu \int_\epsilon^\infty e^{(\mu_1+\mu)(s-t)} ds = \varepsilon \| x_\mu \| \int_0^\infty e^{(\mu_1+\mu)s'} ds' ,$$

this integral converges as $\mu_1 + \mu < 0$.

Now if $x(t)$ is solution of

$$x' = A_x + g(x) \qquad (**)$$

and $x \in V_\mu$, then

$$e^{A_2 t} (x_2(0) + v_2(x))$$

must be a function in V_μ . So $x_2(0) + v_2(x) = 0$. So we can write

$$(1) \quad 0 = x(t) - e^{A_1 t} a - \int_0^\epsilon e^{A_1(t-s)} g_1(x(s))\, ds + \int_t^\infty e^{A_2(t-s)} g_2(x(s))\, ds , \quad a \in X_1 .$$

(onversely , if this equation holds for $x \in V_\mu$, then x is a solution of (**) and $x_1(0) = a$.

So let $F(x,a)$ be the right hand member of (1), for $x \in V_\mu$, $a \in X_1$

$F(0,0) = 0$ so condition (ii) of Thm 3 can be easily satisfied.

Take $p = I : V_\mu \to V_\mu$.

$$\frac{\partial F}{\partial x}\,h = h(t) - \int_0^t e^{A_1(t-s)}\frac{\partial g_1(x(s))}{\partial x}\,h(s)\,ds + \int_t^\infty e^{A_2(t-s)}\frac{\partial g_2(x(s))}{\partial x}\,h(s)\,ds$$

As $\frac{\partial g(0)}{\partial x} = 0$, $\frac{\partial g_1}{\partial x}$ and $\frac{\partial g_2}{\partial x}$ are arbitravily small if $\|x\|_\mu$ is small enough.

So we get a unique continuous function

$$X_1 \to V_\mu : a \to x(t,a)$$

such that $x_1(0,a) = a$ and $x(t,a)$ is a solution of $(**)$

$$\frac{\partial F}{\partial a} \div H \to -e^{A_1 t} H$$

If we apply

$$\frac{\partial F}{\partial x}\frac{\partial x}{\partial a} + \frac{\partial F}{\partial a} = 0$$

and compute the derivative for $a = 0$ $(\to x(t_1 a) = 0)$

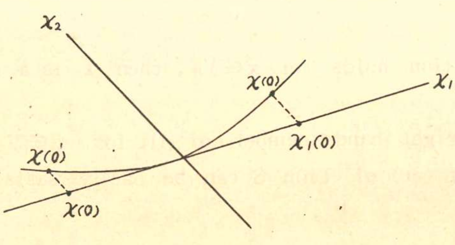
we find

$$\frac{\partial x(t,0)}{\partial a} H = e^{A_1 t} H$$

putting $t = 0$ we find

$$\frac{\partial x(0,0)}{\partial a} H = H$$

$x \in V_\mu$ depends differentiably on a depends differentiably on x. So $x(0,a)$ is a differentiable mauifold S for a small enough , which is tangent to X_1 in 0.



Historical remarks and veferences.

Historically the use of successive approximations for obtaining solutions to differential equations was practised by astronomers for a long time. The first general convergence proof is due to Picard (1891, Bull. Soc. Math. France). Only in 1903, Gowrsat used this method for proving the implicit function theorem (Bull. Soc. Math) but the theorem was already proved by other methods in more reotricted cases (fanalytic orso) by Cauchy and Dim, and in the special case of roots of a polynomial depending on the coefficients, using successive approximations, by Weierstrass (1859, Werke I).

Gencralizations to Banach spaces were developed by Hilde brandt and Graves (1929, Trans. Am. Math. Soc.), and the first appearance of Banach spaces, in this kind of theorems go even back to 1916 (Bermett, Proc. Acad. Sci. U.S.A.).

Basically, everything we have done is contained in the articles of Hildebrandt and Graves. The stability theorem of the second application is also very old. A good reference for theorems of this kind is ., Mc Graw Hill (1953) A good reference for Theorem 4 (The usual implicit function theorem) is Diecidonne', Foundations of modern analysis. Ac. Press 1960 Robbin (Proc. Am. Math. Soc, 1968) proves existence & uniqueness using the usual implicit function theorem plus a trick to get the " starting zero " $F(x_0, t_0) = 0$.

The idea to use the implicit function theorem for proving stability theorems is due to Dr J.J. Duister maat.

The advantage of this method is, that one obtains the dependence on ' initial) parameters in a more explicit way.

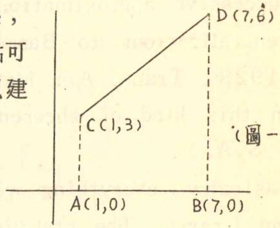
The above litterature references can all be found in the library of the Mathematics Department of National Taiwan Unversity.

An article in which the above is worked out more and with a few more examples will appear in the Taita Mathematics Journal.

無限大

每次遇到要算帳，算錢的場合，朋友們總說“你是數學系的，你來吧！”。可是只有我們這些沾了數學邊的，才知道自己與數字是那麼少接觸，有時連加加減減都錯誤百出。可是有一種數法却是我們感興趣的，那就是數錢時永遠用不着的無限大。

對於無限大，歷代數學家持着幾種不同的態度；有人認爲無限是不可想像的，就如同早期人們只承認自然數，認爲負數和有理數是“不自然的”。到笛卡兒利用坐標系，發現解析幾何，進而討論直綫圖形時，便產生了直綫與另一直綫上的點可以一一對應，雖然二者長度不同。如（圖一）綫段CD與綫段AB可以建立函數 $g: AB \to CD$，$g[(x,0)] = (x, f(x))$，



（圖一）

$f(x) = \frac{1}{2}(x+5)$，$1 \leq x \leq 7$。很明顯的 f 是1對1，因爲

若 $\frac{1}{2}(x_1+5) = \frac{1}{2}(x_2+5)$ 則 $x_1 = x_2$；$\therefore$ g是1－1而且g是 onto，因爲對任何一點 (x, y)

在 CD上，則 $\frac{y-3}{x-1} = \frac{6-3}{7-1} = \frac{1}{2}$ $\therefore$ $f(x) = y = \frac{1}{2}(x+5)$ 所以g是1對1，映成函數。

這是個大問題，因爲明明兩綫段長度不同，怎麼可以有相同多的點呢！這問題現在已經成了我們常遇見的題目：“作一函數使Q與N成一對一對應”。到了十九世紀初，Cantor 對無限大所持的態度是“決定來數一數有理數和所有實數”。他的數法就是利用一對一函數。Cantor 認爲“如果二集合中元素個數相等，則二集合可以一對，一對的去數，應該剛好數完”。結果他發現自然數和有理數呈一一對應；自然數和正偶數呈一一對應；而有理數和實數不能呈一一對應，於是無限大有了等級之分。有理數和實數顯然不在同一級。這就是我們要討論的 cardinal number。

我們分十個問題來認識一下無窮大和 cardinal number：

一、人們爲什麼要研究無限大？

這個問題或許你覺得沒什麼意思，不過 Georg Cautor 開始研究時，這問題却是需要考慮的。

儘管人們認爲無限大是玄虛的，不自然的，但是却得天天接觸一些含有無限多元素的集合：自然

數集，偶數集，有理數，實數，平面上的三角形等等都是無限集合，所以面對着它們不斷的挑釁，數學家們自然把這問題看成了研究的目標。

二、我們應該考慮“如果二集合成一對一對應則其元素個數相同”是否正確？

在一般個數有很的集合間，這是話是對的。可是如果元素有無限多，那麼我們考慮 $A=\{n \mid n$是整數$\}$，$B=\{2n \mid n$是整數$\}$，則 $f: A\to B$ 定義爲 $f(n)=2n$ 則 A，B成一對一對應，而B却是A的部分集合，似乎個數該比A少。這就是有限集合和無限集合的不同，無限集合可以和自己的部分集合對應，而有限集合不可以。

而對無限集合，元素的個數如何數，我們還不知道，所以要解決“問題二，便引起了我個的第三個問題：”我們是否能定義無限集合的個數，使問題二的答案成爲“是”。

三、如何定義無限集合，“使二集合個數相等 $\Longleftrightarrow$ 二集合成一對一？事實上我想你已經知道這種無限集合的個數，最好的定義就是”二集合個數相等 $\Longleftrightarrow$ 二集合呈一對一對應”。於是 Cautor 的 cardinal number 就由此應運而生。

定義如下：定義 $A\cong B$，當 $\exists f: A\to B$，f 爲 1－1 映成函數，所有集合所成的集合，因此而分成許多 equivaleut classes，在同一個的 equivaleut class 中之集合有相同的 cardinal number，（如果稱這 cardinal number 就是集合元素的個數亦可）

所以“二集合有相同的 cardinal number $\Longleftrightarrow$ 二者呈一對一對應”。

我們不妨看幾個例子：

(a) 若A有 k 個元素，k 爲有限數，則我們定 card $A=k$，如 card $\{1,2,3\}=3$.

(b) N爲自然數集，則給 card N 一個特別記號 card $N=S_0$ 我們知道正有理數 Q^+ 和自然數呈一一對應，對應方法如右圖，刪去重覆的，則成 1，2，1/2，1/3，3，4，3/2，2/3，1/4，1/5，5，6，…… 一數列，與自然數成 1－1 對應。∴ card $Q^+=S_0$，事實上 card $Q=S_0$，你不妨試試。

$1\to 2$，$3\to 4$，$5\to 6$，…

1/2，2/2，3/2，4/2，5/2，6/2，…

1/3，2/3，3/3，4/3，5/3，6/3，…

1/4，2/4，3/4，4/4，5/4，6/4

(c) $E=\{2n \mid n$ 爲自然數$\}$，我們前面已經提及 $N\cong E$（即N與E呈一對一對應），∴ card $E=S_0$，同樣 $O=\{2n+1 \mid n\in N\}\cong N$.

(d) R爲所有實數所成的集合，我們也給 card R 一個特殊記號 card $R=c$.

首先我們看看 c 是否等於 S_0，前面我們知道 cantor 已經發現 $c\neq S_0$，我們不妨就直接用

他的方法：我們假設所有實數個數 $c=S_0$，那麼便可以將實數列成一數列，而每一個實數均以小數形式表出，於是現在的工作是要找出一個 $x\varepsilon R$，而不在數列中。圖二是表示數列中前四個數字，我們取 $x=N.abcd\cdots\cdots$ 其中N爲任意整數，$a=1$ 如果 $a_1\neq 1$；$a=2$ 如果 $a_1=1$。$b=1$ 或2也是一樣取決於 b_2，c 決定於 $c_3\cdots\cdots$ 這樣x不等於數列中任何數，而 $x\varepsilon R$，

$\therefore$ card $R=c\neq S_0=$ card N。

第一個數字	N_1, $a_1\ a_2\ a_3\cdots\cdots$
二	N_2, $b_1\ b_2\ b_3\ b_4\cdots$
三	N_3, $c_1\ c_2\ c_3\ c_4\cdots$
四	N_4, $d_1\ d_2\ d_3\cdots\cdots$

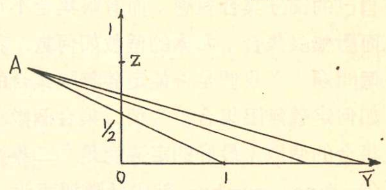
圖二

(e) card $(-1,1)=$ card $R=c$.

我們定義 $f:(-1,1)\to R$ 如圖三

$x\varepsilon(0,1)$　$f(x)$ 即爲A與x連綫與 $\overrightarrow{OY}$ 之交點（$\overrightarrow{Ax}\cap\overrightarrow{OY}$）

若 $x\varepsilon(-1,0)$　　$f(x)=-f(-x)$



圖三

f是1對1，而且 R^+ 中任一元素x可以在 $\overleftrightarrow{OY}$ 綫上找一點P與之對應，∴可以在 $(0,1)$ 中找到一點 $\overleftrightarrow{AP}\cap\overline{OZ}=y$ 使 $f(y)=x$ 對 R^- 中也是一樣 $\therefore(-1,1)\cong R$.

(f) card $(0^{-1},1)=$ card $(0^{-1},1)=$ card $[0^{-1},+1]=c$

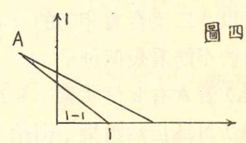
我們知道由圖四 $[-1,1)\cong[0,\infty)$ $(-1,1)\cong(0,\infty)$

可是 $(0,\infty)\cong[0,\infty)$ ∵ ∃ $f:[0,\infty)\to(0,\infty)$

$f(x)=x$ 若 $x\varepsilon[0,\infty)-N-\{0\}$，$f(x)=x+1$

若 $x\varepsilon N\cup\{0\}$，f 爲 1－1，映成

$\therefore[-1,1)\cong(-1,1)$ card $[-1,1)=$ card $(-1,1)=c$



圖四

你不妨試試 $[-1,1]$ 與 $[-1,1)$ 之關係。

四、現在我們既然把 cardinal number 看成“個數”，那是否能像自然數一樣，定義一種加法運算？

我們知道自然數既然是 cardinal number，所以我們希望對 cardinal number 定的加法能合乎自然數中之加法。

所以我們先考慮一個例子：$A=\{1,2,3\}$，$B=\{7,4,5,6\}$

card $A=3$，card $B=4$.

$3+4=7$ ． ∴ 我們希望 card A + card $B=7$ ．

所以最明顯的方法是定 card A + card B = card $A\cup B$ ，不過有一點要注意的是 $A\cap B=\phi$ 是個充要條件。

cardinal number 加法定義：

S_1，S_2 爲＝cardinal number ；我們可以選兩個集合

A，B， $A\cap B=\phi$，card $A=S_1$ ， card $B=S_2$

則 S_1+S_2 = card A + card B = card $A\cup B$

這種定義很合乎將自然數的加法運算擴展至 cardinal number ，不過我們必須先驗證一下這定義是否" well-defined " ，也就是" 如果 $A\cap B=A'\cap B'=\phi$ 而 $A\cong A'$，$B\cong B'$，那 $A\cup B\cong A'\cup B'$ 是否成立？" 因爲 card ($A\cup B$) = card A + card B = card A' + card B'

= card ($A'\cup B'$)

所以如 $A\cup B\ncong A'\cup B'$ 那麼這加法就有問題了！

讓 $f: A\cup B\to A'\cup B'$ 而 $f(x)=f_1(x)$，如果 $x\varepsilon A$ $f_1: A\to A'$ 1－1，onto

$f(x)=f_2(x)$，如 $x\varepsilon B$ $f_2: B\to B'$ 1－1，onto

∴ f 爲由 $A\cup B$ 映至 $A'\cup B'$ 的一對一對應。

∴ $A\cup B\cong A'\cup B'$ card ($A\cup B$) = card ($A'\cup B'$) 無誤。

現在 cardinal number 中 S_1+S_2 已經定義，而無限多 cardinal number 一樣可依此法定義他們的加法：

$$\sum_{\mu} S_\mu = \text{card}\,(\cup_\mu A_\mu)\ \mu\,\varepsilon\, s \qquad S_\mu = \text{card}\ A_\mu \text{ 而且 } A_\mu\cap A_{\mu'}=\phi \quad \mu\ ,\ \mu'\,\varepsilon\, s\ .$$

五、有了加法，我們又希望知道一些加法的性質。

(a) $S_0+S_0=S_0$ S_0 = card N

card $\{1,3,5,7,\cdots\cdots\}$ = card $\{2,4,6,8,\cdots\cdots\}$ = card $N=S_0$

而 $\{1,3,5,7,\cdots\cdots\}\cap\{2,4,6,8,\cdots\cdots\}=\phi$

$\{1,3,5,7,\cdots\cdots\}\cup\{2,4,6,8,\cdots\cdots\}=N$

∴ S_0+S_0 = card $\{1,3,5,7,\cdots\cdots\}$ + card $\{2,4,6,8,\cdots\cdots\}$

= card $\{1,2,3,4,5,6,7,8\cdots\cdots\}$

$=S_0$.

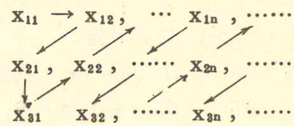
(b) $\underbrace{S_0 + S_0 + \cdots\cdots}_{S_0 \text{個}} = S_0$

card $\{x_{11}, x_{12}, x_{13}, \cdots x_{1n}, \cdots\} = S_0$

card $\{x_{21}, x_{22}, x_{23}, \cdots x_{2n}, \cdots\} = S_0$

card $\{x_{31}, x_{32}, x_{33}, \cdots\cdots x_{3n}, \cdots\} = S_0$

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$



圖五（x_{ij} 符號而已不表數字）

故 $x_{ij} \neq x_{kl}$，$i \neq k$ 或 $j \neq l$

如圖五各集合聯集中元素可列成一數列，所以 $S_0 + S_0 + \cdots\cdots = S_0$

這就是大家熟悉的" countable union of countable sets is countable ".

(c) $a + S_0 = a$，如果 a 是無限的 cardinal number（也就是 $a = \text{card } A$，A 中必有一部分集合 A'，$A' \cong N$）

$\therefore$ card $A = a$，card $N = S_0$

而 $A' \cong N$，$\therefore$ A' 中元素可成一數列 $\{a_1, a_2, \cdots\cdots\cdots\}$

定 $f : A \cup N \to A$　$f(x) = a_{2n-1}$　若 $x \varepsilon \{a_1, a_2, \cdots\cdots\}$

$f(x) = a_{2n}$　若 $x \varepsilon \{1, 2, 3, 4, \cdots\cdots\}$

$f(x) = x$　若 $x \varepsilon A - \{a_1, a_2, \cdots\cdots\}$

$\therefore$ $a + S_0 = a$，若 $a = \text{card } A$，A 中有 $A' \subseteq A$，$A' \cong N$.

$\therefore$ $C + S_0 = C$ 爲一特例，$\because$ $N \subseteq R$，$N \cong N$.

(d) $C + C = C$

card $(-1, 1) = $ card $(1, 3) = C$

而 $(-1, 3)$ 與 $(-1, 1)$ 呈一對一對應，對應如圖

定 $f : (-1, 1) \to (-1, 3)$　　$f(x) = 2x + 1$

$\because$ $\dfrac{x+1}{y+1} = \dfrac{2}{4} = \dfrac{1}{2}$ 見圖六

$\therefore$ card $(-1, 3) = $ card $(-1, 1) = C$

$\therefore$ card $(-1, 1) + $ card $(1, 3) = C + C = $ card $(-1, 3) = C$

(e) $\underbrace{C + C + C + \cdots\cdots}_{S_0 \text{個}} = C$

$\because$ card $[n, n+1) = C$

而 $\bigcup_{n=1}^{\infty} [n, n+1) = \{x \mid x \geq 1\}$

$\therefore$ card $[1, 2) +$ card $[2, 3) + \cdots = C + C + \cdots + C + \cdots = C$

六、對 cardinal number 中減法是否成立？

這是很明顯的，-2，-3 都不是 cardinal number，而且由問題五的答案更告訴我們 $C + C = C$，$C + C + C = C + C = C$，$C + S = C$，所以 S，C 都是 C 的加法反元素，所以減法不是 cardinal number 中的運算。

七、至於乘法運算，我們是否也可以利用自然數的乘法，加以擴展到 cardinal number 呢？

我們也先看一下如果 card $A = 3_1$, card $B = 4_2$

$3 \times 4 = 12 =$ card $A \times B$

所以對任二 cardinal number 乘法運算定義如下：

$S_1 =$ card A_1, $S_2 =$ card A_2，則 $S_1 \cdot S_2 =$ card $A_1 \times A_2$

要檢查這定義是否 " well-defiued " ？就是要檢查每一對 cardinal number (S_1, S_2) 是否有而且唯一對應元素？

" 有 " 的部分，我們已找到 (S_1, S_2) 對應 card $A_1 \times A_2$

而 " 唯一 " 的部分，如果 card $A_1 =$ card $B_1 = S_1$, card $A_2 =$ card $B_2 = S_2$

則 $S_1 \cdot S_2 =$ card $A_1 \times A_2$　　　$S_1 \cdot S_2 =$ card $B_1 \times B_2$

所以問題在 $A_1 \times A_2 \cong B_1 \times B_2$ 是否成立？

$\because A_2 \cong B_1$，$A_2 \cong A_2$　　　$\therefore$　$f_1 : A_1 \to B_1$, $f_2 : A_2 \to B_2$ 均爲 1－1 映成。

$\therefore$　$g : M \times N \to M' \times N'$　$g(m, n) = (f_1(m), f_2(m))$

g 是 1－1 映成。

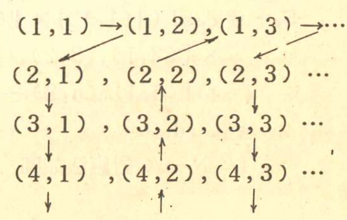
八、cardinal number 的乘法是否也有些與自然數不同的性質？

(a) $S_0 \cdot S_0 = S_0$

$S_0 \cdot S_0 =$ card $\{(x, y) \mid x, y \in N\}$

$\{(x, y) \mid x, y \in N\}$ 可與N中元素以右圖方式呈一一對應。

$\therefore$ $S_0 \cdot S_0 = S_0$



(b) $S_0 \cdot C = C$

$S_0 \cdot C = \text{card}\,\{(x,y) \mid x \in N,\ y \in [0,1)\}$

我們定義 $f:\{(x,y) \mid x \in N,\ y \in [0,1)\} \to R \quad f(x,y) = x+y$

f 是1－1 ∵若 $x_1+y_1 = x_2+y_2$，則 $x_1-x_2 = y_2-y_1$ $|x_1-x_2| \geq 1$ 而 $|y_2-y_1| < 1$

∴ $x_1-x_2 \neq y_1-y_2$，除非 $x_1=x_2$，$y_1=y_2$

∴ $(x_1, y_1) = (x_2, y_2)$

但 f 不是映成，所以 $\{(x,y) \mid x \in N,\ y \in [0,1)\} \cong R' \subseteq R$

∴ card $\{(x,y) \mid x \in N,\ y \in [0,1)\}$ 該比C小或相等，但是

如果定義 $g: R \to \{(x,y) \mid x \in N,\ y \in [0,1)\} \quad g(y) = (1, y)$

那麼C反而要小於 card $\{(x,y) \mid x \in N,\ y \in [0,1)\}$ 了。

∴ $C = S_0 \cdot C$

由上面的證明中，我們看得出已經用了 cardinal number 中的次序關係。定義是這樣的：$S_1 \leq S_2$ 若 A_1, A_2 $S_1 = \text{card } A_1$，$S_2 = \text{card } A_2$，而 $A_1 \subseteq A_2$。這次序關係也和自然數一樣合乎三一律，我們剛才用的就是這性質。

(c) $C \cdot C = C$

$C \cdot C = \text{card } A = \text{card } A\{(x,y) \mid x, y \in (0,1)\}$

∵ 每一 $x \in (0,1)$ 都可表成 $0.x_1x_2x_3\cdots\cdots$ 凡遇1均以 $0.999\cdots\cdots$ 表

∴ $f: A \to (0,1)$，$f(0.x_1x_2\cdots,\ 0.y_1y_2y_3\cdots) = 0.x_1y_1x_2y_2x_3y_3\cdots\cdots$

則 f 是 1－1 ∵若 $0.a_1a_2a_3\cdots\cdots = 0.b_1b_2b_3\cdots\cdots \neq 1$

則 $a_1 = b_1$ ∴ $0.a_2a_4\cdots\cdots = 0.b_2b_4\cdots\cdots$

$0.a_1a_3\cdots\cdots = 0.b_1b_3\cdots\cdots$

而且 outo.

(d) $S_0! = 1 \cdot 2 \cdot 3 \cdots\cdots n \cdots\cdots S_0 = S_0$

$S_0! = \text{card}(\{(1,1)\} \times \{(2,1),(2,2)\}$
$\times \{(2,1),(3,2),(3,3)\} \times \cdots\cdots\cdots$
$\times \{(n,1),(n,2)\cdots(n,n)\} \times \cdots\cdots)$
$= \text{card } A$

$f: N \to A$ 對應法如圖

(1,1)
↓
(2,1) ↗ (2,2)
↓ ↓
(3,1) (3,2) ↗ (3,3)
↙ ↓
(4,1) (4,2) ↗ (4,3) (4,4)
↓ ↗ ↗
(5,1) (5,2)

$\therefore S_0 ! = S_0$

九、我們一直考慮有限數；S_0；以及C，那麼是否還有其他的cardinal number？

我們不妨試着找找，第一我們先定義 cardinal number 的指數關係 card $\{ f : A \to B \mid$ card $\{ f : A \to B \mid \text{card } A = a , \text{card } B = b \} = 0^a$

所以 $2^a = \text{card } \{ f : A \to \{0,1\} \mid \text{card } A = a \}$

而 $\{ f : A \to \{0,1\} \mid \text{card } A = a \} \cong \{ B \mid B \subset A \}$ $\because \exists g(f) = f^{-1}(1)$

$\therefore 2^a = \text{card } P(A)$

好，現在我們可以比一比 a 和 2^a，（即 Cantor theorm）

(1)若 card $A = a$， card $P(A) = 2^a$

定義 $f : A \to P(A)$ $f(x) = \{x\} \varepsilon P(A)$ $\therefore a \leq 2^a$

(2)但是 $a = 2^a$ 會不會成立呢？

我們假設 $f : A \to P(A)$，f 是 1－1，映成，

於是 $\forall x \varepsilon A$，$\exists f(x) \subseteq A_1$。可是 $A' = \{ x \mid x \varepsilon f(x) \} \subseteq A$． $\therefore A' \varepsilon P(A)$

$\because$ f 是映成，$\therefore \exists x_0$，$f(x_0) = A'$ 那麼 $x_0 \varepsilon A'$，還 $x_0 \varepsilon A'$ 呢？

如果 $x_0 \varepsilon A'$ 則 $x_0 \varepsilon f(x_0)$ $\therefore x_0 \varepsilon A'$（由 A' 之定義）

如 $x_0 \varepsilon A'$ 則 $x_0 \varepsilon f(x_0)$ $\therefore x_0 \varepsilon A'$（由 A' 之定義）

$\therefore$ 無法找到這種 f，$\therefore 2^a > a$．

所以每一個 cardinal number a 都可以找到 $2^a > a$，所以 cardinal number 也有無限多，而且在有限數，S_0，C之外還有多。

十、或許你要問我為什麼要寫這篇東西，一篇毫不深入的東西（因為許多更進一步的性質被犧牲不少）？

答案是這樣的，我希望利用這連續的十個問題，把你已有的 cardinal number 的概念引成一系統，如果你看了，覺得我並沒做到這目標，麻煩你告訴我一下，我將想一下能否換個方法，以求最適合思考途徑，至於這方面深入些的資料下面幾本書中均可找到。

註：參考書： theory and problem of set theory（by Seymour Lipschutz）

Topology (Dugundji) fundatias of general top（William j Peroin）

Interoduction to algebraic topology

～前　　言～

拓樸學是研究幾何圖形經過拓樸變換而不改變的性質。一般可分爲點集拓樸與組合（或代數）拓樸。以點集中的鄰域概念作基礎，視空間爲幾何學中的連續點集，只要一集合能滿足某些鄰域公理，就把此集合看成最廣義的空間，如此許多有意義的概念與定理都與距離、平直性，甚至空間的維數無關。拓樸中最重要的概念即同胚（homeomorphism.，即兩點集間有一正逆兩方都單值且連續的變換）此概念與點集有關，而和包含他們的空間無關。在拓樸學中，扭結（knot）和圓周是相同的圖形，若將之放在三維中就有區別了，可是若把包含他的三維空間當作四維空間的子空間，因而可引用四維空間的變狀，此種區別又消失了。如此說來，拓樸有兩種性質，一是內在的（經過此圖形所有的拓樸變換都不改變的）；一是依賴於包含此圖形的空間即 imbedding（浸沒到空間）的，經過整個空間的所有拓樸變換都不改變的性質。此種區別，正好像微分幾何中度量性質間的區別一樣，一種是內在的，不依曲面在空間中的位置，由第一基本式斷定；另一種是由曲面和空間所組成的圖形的度量性質，由第二基本式斷定。拓樸中主要的問題就是要判定兩圖形是否同胚，並且可能的話列舉不同胚的圖形。爲了避免集合論中的困難起見，我們不用很廣義的圖形概念，而只限制在 Brouwer 所創始的 complex（複合形）上，甚或只討論條件更強的流形（manifold）。爲此，我們引出同調（homology），上同調（Cohomology）、同倫（homotopy）理論（同調、上同調的理論距今已有 70 年歷史）。事實上，組合（代數）拓樸是討論空間的連通性（connectedness）的理論，創始者是 Poincar'e（Poincar'e 在 1895 提出基本群的概念。Hurwicz 在 1935～36 提出同倫的概念），這理論可說是藉重代數中的群論（及環論）來區別圖形的同胚與否。譬如說同調群可做二維流形的分類標準，而高維的複合形可能有相同（指同構）的同調群而不同胚，故需基本群（fundamental group，或稱一維同倫群），或上同調環（Cohomology ring）來區別。說句老實話，要學會同調、同倫理論並無捷徑可循

，只有步步為營，穩紮穩打。本文標明“notes”旨在將一些代拓的概念、重要結果（應用）介紹給讀者，至於冗長的證明就請讀者翻閱文後所列參考書了。用同倫、同調的理論可證 Brouwer's 定點定理，Jordan-Brouwer Separation 定理（任何 n 維球面 S^n 恰可被 S^{n-1} 分割成兩連通部分）及代數基本定理（任一 n 次複係數多項式至少有一零根）。代拓的理論大部分都是抽象化了的範疇（Category）理論的較具體實例。在深入了解代拓後，你會驚異何以那些數學家會創出像“exact sequence”，“excision theorem”這樣好的工具來解決問題。

～一些定義及概念～

0-1 設此 P＋1 個點 $u_0, u_1 \cdots u_m$ 在 n 維歐式空間線性獨立，則此集合

$$S=\{\sum_{i=0}^{m} x_i u_i \mid \sum_{i=0}^{m} x_i=1,\ x_i\geq 0\}$$

叫作以 $u_0,\cdots u_m$ 為頂點的歐式 m 維單純形（m-simplex），以 $[u_0, u_1, \cdots u_m]$ 表之。令 $e_i=(0,0,\cdots,0,1,\cdots 0)$ 其中 1 是在第 i＋1 坐標軸上的坐標，則 $[e_0,\cdots e_n]$ 叫作標準 n 維單純形，以 $\triangle_n$ 表之，例如 $\triangle_0$ 是一點，$\triangle_1$ 是一線段，$\triangle_2$ 是一三角形，$\triangle_3$ 是一四面體。

0-2 一個廣義的 n-simplex 是一個從 $\triangle_n$ 到拓樸空間 X 的連續函數（或其寫像）$\sigma_n:\triangle_n\to X$，如 n＝1，則 σ_1 是一“道路”（path），如 n＝0 則 σ_0 可看成一點。

0-3 設 G 是交換群（通常為整數集 Z），X：任一拓樸空間。則鍊群（Chain group）$C_P(X;G)=\{\Sigma a_i\sigma_i \mid a_i\in G,\ \sigma_i:\triangle_P\to X$ 是連續函數$\}$，表所有係數在 G 中的廣義 P- 鍊所成的群，其中 Σ 是形式和，$C_P(X;G)$ 可縮寫成 $C_P(X)$。另外表所有從 $C_P(X;Z)$ 到 G 的同態所成的廣義餘鍊群（Cochain group）

$C^P(X;G)=\mathrm{Hom}_Z(C_P(X;G),G)$

$=\{f \mid f(\sigma)\in G,\ \sigma$ 是廣義 P simplex$\}$

0-4 若 $f: x\to Y$ 連續，且 $f_1: C_P(X,G)\to C_P(Y,G)$ 被定義為 $f_1(\Sigma a_i\sigma_i)=\Sigma a_i f(\sigma_i)$ 則 f_1 是被 f 所引導出的同態。

0-5 若 $u_0,\cdots,u_P$ 在 E_n 中線性獨立，定義函數 $(u_0, u_1, \cdots, u_P):\triangle_P\to[u_0, u_1,\cdots,u_P]$ 如 $\Sigma x_i e_i\to\Sigma x_i u_i$ 則 $(u_0, u, \cdots, u_P)$ 和 u_i 之次序有關，且 $(e_0, e_1, \cdots, e_P)$ 為同一函數（identity map）.

0-6 設 σ 為 X 的廣義 P simplex．則 σ 的界函子 d（boundary operator）被定義成 $d\sigma=\sigma d(e_0\cdots e_P)=\sigma[\Sigma(-1)^i(e_0\cdots e_i\cdots e_P)]=\Sigma(-1)^i\sigma_0(e_0,\cdots\hat{e}_i\cdots e_P)$

$\in C_{P-1}(X, G)$

其中 $(e_0, \cdots \hat{e}_i \cdots e_P) : \triangle_{P-1} \to \triangle_P$

（$\hat{e}_i$ 表去掉 e_i 這一項）

更進一步，若 $\Sigma a_i \sigma_i \in C_P(X, G)$，

則定義 $d(\Sigma a_i \sigma_i) = \Sigma a_i d(\sigma_i)$

0-7 $d^2 = d \circ d = 0 : C_P(X,G) \to C_{P-2}(X,G)$

（或更確切一些說 $d_{P-1} d_P = 0$）

0-8 一個鍊複合形 Chain complex C 包含一序列的交換群 C_n 和同態界函子 $d : C_n \to C_{n-1}$，且 $dd = d^2 = 0$

一個餘鍊複合形 Cochain complex C 包含一序列的交換群 C^n 和同態（餘界函子）$\delta : C^n \to C^{n+1}$ 且 $\delta\delta = \delta^2 = 0$

0-9 若 $d_n : C_n \to C_{n-1}$

則① $\mathrm{Ker}\ d_n = Z_n(C) = C$ 的 n-cycle（n 閉鍊）所成之群

② $I_m\ d_{n+1} = B_n(C) = C$ 的 n-bdy（n 邊界）所成之群

③ $H_n(C) = Z_n(C)/B_n(C) = C$ 的 n 維同調群（$Z_n(C)/B_n(C)$ 表商群）

0-10 ①若 $X = \{x\}$，則只有一廣義 P simplex

$\sigma_P : \triangle_P \to \{x\}$

所以 $d(\sigma_P) = \begin{cases} \sigma_{P-1} & 若 P > 0 且偶數 \\ 0 & 若 P 爲奇數 \end{cases}$

$\Rightarrow \quad Z_P = B_P = \begin{cases} 0 & P > 0 \ 偶數, \\ C_P & P 爲奇數 \end{cases}$

且 $\{a\sigma_P \mid a \in G\} = C_P(X;G) \cong G$

$H_P(X;G) = 0 \qquad P > 0$

②若 $P = 0$，則 $H_0(X;G) \cong G$

蓋 $H_0(X;G) = Z_0 = C_0 \cong G$.

0-11 若 $X \neq \phi$ 且是 path-connected 則 $H_0(X;G) \cong G$.

0-12 若 A 是 X 的非空子空間，且 X 是 path connected，則 $H_0(X, A; G) = 0$（零維相對同調群），如 $A = \phi$，則 $H_0(X, \phi; G) = H_0(X; G) = G$

故 $A = \phi$ 時相對（relative）同調群卽爲前述的（絕對）同調群。

0-13 $H_P(X, X; G) = 0 \quad \forall\ P$.

0-14 兩連續函數 $f, g : (X, A) \to (X^1, A^1)$ 是同倫（homotopic）若且唯若存在一連續函數 $F : (X \times I, A \times I) \to (X^1, A^1)$ 使得 $F(x, 0) = f(x)$，

$F(x, 1) = g(x) \quad \forall\ x$

並且我們寫作：

$F : f \simeq g\ (X, A) \to (X^1, A^1)$

更進一步對任一 P，它們所引導的同態 f_{*P}，g_{*P} 相等。

0-15 若 $0 \to A \xrightarrow{g} B \to 0$ 是一 exact sequence 則同態 g 是一同構．

0-16 若 $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ 是一 exact sequence 則 h 是一對一同態 $\Longleftrightarrow$ f 是映成同態 $\Longleftrightarrow$ g 是零同態。

0-17 X，Y 兩拓樸空間有相同的 homotopy

type 若且唯若存在連續函數 $f: X \to Y$, $g: Y \to X$，使得 $fg \simeq$ identity map of X，$gf \simeq$ identity map of Y，此時 f, g 叫 homotopically equivalent.

0-18 若 $f: (X, A) \to (X^1, A^1)$ 是一同胚，則 $H_P(X, A) \xrightarrow{f_{*P}} H_P(X^1, A^1)$ 是一同構。

0-19 設 $E^n = \{(x_0, \cdots, x_{n-1}) \mid \Sigma x_i^2 \leq 1\}$

$S^n = \{(x_0, \cdots, x_n) \mid \Sigma x_i^2 = 1\}$

$E_n^+ = \{(x_0 \cdots x_n) \in S^n \mid x_n \geq 0\}$

$E_n^- = \{(x_0, \cdots, x_n) \in S^n \mid x_n \leq 0\}$

$E_n^+ \cap E_n^- = S^{n-1}$

則 $H_P(E_n^+, S^{n-1}) \cong H_P(S^n, E_n^-)$

$\cong H_P(S^n) \cong H_P(E^n, S^{n-1})$

$\cong H_{P-1}(S^{n-1})$ ($P \geq 2$，$n \geq 1$)

所以 $H_P(S^n) \cong \begin{cases} G & (p = n \geq 1) \\ 0 & (p \neq n, p, n \geq 1) \\ 0 & (n = 0, p \geq 1) \\ G \otimes G & (n = p = 0) \end{cases}$

0-20 $A \subset X$ 是 X 的 deformation retract 若且唯若存在一 retraction $r: X \to A$ (即 $r(a) = a$，$\forall a \in A$) 和一同倫 $f: X \times I \to X$，使得對所有 $x \in X$，$f(x, 0) = x$，$f(x, 1) = r(x)$，對 $a \in A$，$t \in I$，$f(a, t) = a$。在此情況況下，inclusion map $i: A \to X$ 引導出一從基本群 $\pi_1(A, a)$ 至 $\pi_1(X, a)$ 之同構。

如果 $\{x\}$ 是 X 的 deformation retract 則 X 叫作可緊縮至一點 (contractible to a porint)，此時 X 必是單連通 (simply connected) (即基本群只包含一元素，且 X 爲 arcwise connected) 例如 $[0, 1)$, $(-1, 1)$ 均可緊縮至一點，故他們有相同的 homotopy type.

附帶提一下，用"S^{n-1} 不是 E^n 的 retract"這一定理，可證 Brouwer 定點定理。

0-21 ①若 f, g 是 X 中之兩道路，且 $f(1) = g(0)$

則 f 和 g 之乘積 $f \cdot g: I \to X$ 被定義爲

$$(f \cdot g)(t) = \begin{cases} f(2t) & (0 \leq t \leq \frac{1}{2}) \\ g(2t-1) & (\frac{1}{2} \leq t \leq 1) \end{cases}$$

②有同始點，同終點兩道路是 equivalent ($f \simeq g$) 若且唯若存在一連續函數 $F: I \times I \to X$，使得

$F(s, 0) = f(s)$
$F(s, 1) = g(s)$ $\quad \forall s \in I$

$F(0, t) = f(0) = g(0)$
$F(1, t) = g(1) = f(1)$ $\quad \forall t \in I$

在此情形下，"$\simeq$"是一 equivalence relation 我們取其 homotopy

class $[f]=\{g \mid g\simeq f\}$.
並設 $\pi_1(X,x)=\{[f] \mid f$ 是在 x點的一閉道路，$f(0)=x=f(1)\}$
則 $\pi_1(X,x)$ 在①中所述的乘積下成群，吾人稱之爲X在x點之基本群（或一維同倫群）。

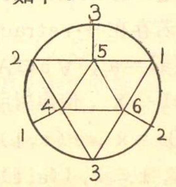
0-22 lifting lemma：若f是 s^1 之一道路．（即 $f:[0,1]\to s^1$ 連續）且 $f(0)=0$ $\phi:R\to s^1$ 定義爲 $\phi(x)=e^{2\pi ix}$（連續同態），則在R中存在唯一的道路 f' 使得 $\varphi^0 f^1=f$.

0-23 $\pi_1(X\times Y,(x_0,y_0))\cong\pi_1(X,x)\otimes\pi_1(Y,y_0)$.

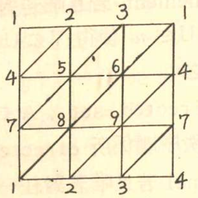
0-24 X：path connected
$\varphi:\pi_1(X,x_0)\to H_1(X,Z)$ 是一同態其 kernel 是 $\pi_1(X,x_0)$ 之一 commutator subgroup，$\pi_1(X,x_0)$ 不一定是 abelian，若是的話，則 $\pi_1(X,x_0)\cong H_1(X,Z)$.

0-25 一個（paracompact）Hausdorff 空間之每一點均有一鄰域和n維 disk 同胚，則此空間叫做 n-manifold。若 $n=2$，且此空間是連通的則此二維流形叫做一個“surface”，任一緊緻單連通曲面和 S^2 同胚。任一非緊緻二維流形和 R^3 之一子集同胚，若此流形爲單連通之曲面，則其和 R^2 同胚。Porincar'e 臆測任一緊緻單連通之三維流形和 S^3 同胚，這問題到現在仍未解決。對四維而言，很易找到緊緻單連通的四維流形（$S^2\times S^2$）和 S^4 不同胚。球式十二面體空間和 S^3 有相同的同調群，但不同胚，這種流形叫做 Poincar'e 空間。我們所知的 Poincar'e 空間有無窮多，但其中基本群是有限的，似乎只有球氏十二面體空間這一個。所謂的透鏡空間（緊緻三維流形）都是“同倫一致”而不同胚。一個更廣義的 Poincar'e conjectuce 是任一緊緻n維流形若和 S^n“同倫一致”（homotopically equivalent）則必同胚。此問題當 $n>4$ 時被 S.Smale 在1960年解決了，但 $n=4$ 仍未解決。

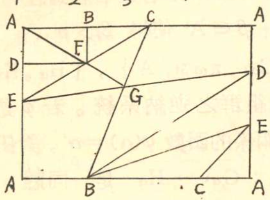
0-26 一個緊緻曲面S的 triangulation（三角形剖分）包含一組有限多個覆蓋S的閉子集 $\{T_1,T_2\cdots T_n\}$，和一組同胚函數 $\varphi_i:T_i'\to T_i\ (i=1,\cdots m)$，其中 T_i' 是 R^2 的三角形。
例如 projective plane P^2 的 triangulation 如下：



torus 可 triangulated 如下二圖：



9 個頂點
18 個三角形
27 邊



7 個頂點
14 個三角形
21 邊

像流形 P^2，torus，S^2 的 triangulation 的頂點個數的最小數可以 Euler 示性數計算出來（參考4．頁41）．如 $h(P^2)=6$ $h(\text{torus})=7$，$h(S^2)=4$．

關於二維曲面之可以三角形剖分，是因爲在此曲面上存在一非恒常數的調和函數，故此曲面有一個 countable basis 。至於三維流形的三角形可剖分性由 E. Moise 證出（1952）而 $n\geq 4$ 時則未知 。可三角形剖分的流形當維數 n 小於 8 時可以有"可微結構"（differential structure），而 $n\geq 8$ 時則否（如此的第一個例子是由M. Kervaire 造出來的）。Kervaire 及 Milnor 證出在 S^n 上不同可微結構的個數如下：$S^5:1$；$S^6:1$；$S^7:28$；$S^8:2$；$S^9=8$；$S^{10}:6$；$S^{11}:992$；$S^{12}:1$；$S^{13}:3$；$S^{14}:2$；$S^{15}:16256$；$S^{16}:16\times10^6$.（他們又證出對任一整數 n，這些個數均有限）

0-27 任一有限複合形K的廣義同調群 $H_P(k)$是一"有限衍生"（finitely generated）的交換群，因而和一自由群與數個有限循環群的"直和"（direct sum）同構，此一自由群的衍生子個數叫做K的第 p 個 Betti 數記作 $b_P(K)$,剩下的有限循環群的直和叫 k 的"撓群"，每一有限循環群的秩叫做 k 的第 p 個撓係數 。若令 $a_P(K)$ 表 k 的 p-sumplexes 的個數，則 Euler示性數 $X(K)\equiv\Sigma(-1)^P a_P(K)=\Sigma(-1)^P b_P(K)$，此即 Euler Poincar'e formula 由此公式對低維的複合形可以很快計算出其同調群 。例如一"井"字，其示性數爲 0（$=12-12$），其本身是連通的故 $H_0(K,Z)\cong Z$，所以 $b_1(K)=1-0=1$，故 $H_1(K,Z)\cong Z$．

0-28 一個閉曲面的虧格 p（genus）是可畫在此曲面上的而又不分離此曲面的不自相交的閉曲線的最大個數，我們有一公式 $V-E+F=2-2P$（V：頂點數，E：邊數，F：面數）。若 k 是一 simple polyhedron（即和 S^2同胚），其虧格爲 0 故 $V-E+F=2$．對環面（torus）來

說，p＝1，故 V－E＋F＝0

0-29 一個 directed 集合就是一個 partially ordered 集合A，其秩序關係滿足：對任二元素 $\alpha,\beta\in A$，存在 $\gamma\in A$ 使得 $\gamma>\alpha$，$\gamma>\beta$．

0-30 一組群的逆納系統 inverse system 就是 $\{G_\alpha\}_{\alpha\in A}$，其中 G_α 是群，A是－directed set，且對任二 α,β 而言，若 $\beta>\alpha$ 則存在一同態 $\pi_{\alpha\beta}: G_\beta\to G_\alpha$ 滿足

①對所有 $\alpha\in A$，$\pi_{\alpha\alpha}$ 是 identity

②當 $\gamma>\beta>\alpha$ 時，$\pi_{\alpha\beta}\pi_{\beta\gamma}=\pi_{\alpha\gamma}$

此系統以 $\{G_\alpha,\pi_{\alpha\beta},A\}$ 或 $\{G_\alpha,\pi_{\alpha\beta}\}$ 或 $\{G_\alpha\}$ 表之．

0-31 令 $G\subset\Pi G_\alpha$，且G中元素的坐標當 $\beta>\alpha$ 時滿足 $g_\alpha=\pi_{\alpha\beta}\,g_\beta$，則G是 ΠG_α（無限積）的子群，我們稱他是此系統 $\{G_\alpha\}$ 的逆納極限，以 $\lim_A G_\alpha$ 或 $\lim G_\alpha$ 表之．

0-32 如同 0-30，一組群的直導系統 direct system 是 $\{G_\alpha,\pi^{\alpha\beta},A\}$，且對 $\alpha>\beta$，$\pi^{\alpha\beta}: G_\beta\to G_\alpha$ 滿足

① $\pi^{\alpha\alpha}$：identity　$(\forall\alpha)$

② $\pi^{\alpha\beta}\pi^{\beta\gamma}=\pi^{\alpha\gamma}$　$(\alpha>\beta>\gamma)$

0-33 如同 0-31，令R表由 ΣG_α 中所有 $x_\alpha-\pi^{\beta\alpha}x_\alpha$ $(\beta>\alpha)$ 的形式的元素所衍生出的子群，則此系統的直導極限 $\lim_A G_\alpha$ 或 $\lim G_\alpha$ 被定義成商群 $\Sigma G_\alpha/R$（Σ 表直和）．

0-34 設 u，v 均是空間E的有限開覆蓋，則 v 是 u 的 refinement 若且唯若對任一 $V\in v$，$\exists U\in u$ 使得 $V\subset U$，此關係以 $v>u$ 表之。

0-35 若A是一 directed set，$A^1\subset A$，A^1 也被A中之秩序關係所 directed，則 A^1 在A中 cofinal 若且唯若對任一 $\alpha\in A$，存在一 $\beta\in A^1$ 使得 $\beta>\alpha$．

0-36 設 $\{G_{\alpha^1},\pi_{\alpha^1\beta^1},A\}$，$\{H_\alpha,K_{\alpha\beta},B\}$ 爲兩組群之逆納系統。若 ϕ 是一保持秩序關係的函數 $\varphi(\alpha)=\alpha'$，對任一 $\alpha\in\beta$ 令 $f_\alpha: G_{\alpha^1}\to H_\alpha$ 是一同態，且對任一 $\beta>\alpha$，$K_{\alpha\beta}f_\beta=f_\alpha\pi_{\alpha^1\beta^1}$

則 $\{f_\alpha\}_{\alpha\in\beta}$ 是對應於 ϕ 的一組同態的逆系統，此逆納系統的極限 f 以 $\lim_B f_\alpha$ 或 $\lim f_\alpha$ 表之。

～The Eilenberg-Steenrod Axioms for homology～

Ax.1. Identity axiom：若 $i:(X,A)\to(X,A)$ 是從拓樸對 (X,A) 到 (X,A) 的 identity map，那對所有整數 q，它所引導出來的同態。$i_*: H_q(X,A)\to H_q(X,A)$ 是同調群 $H_q(X,A)$ 的一個 identity 自同構。

Ax.2. Composition axiom：

若 $f:(X,A)\to(Y,B)$，

$g:(Y,B)\to(Z,C)$ 都是 maps（即連續函數）那對任一整數 q，均有

$(g\circ f)_{*q}=g_{*q}\circ f_{*q}$

Ax．3. Commutativity Axciom：

若 $f:(X,A)\to(Y,B)$ 是連續函數，$g:A\to B$ 是連續函數，且對 $x\in A$，定義 $g(x)=f(x)$，那下列圖表對任意 q 均可交換：（即 $\partial\circ f_*=g_*\circ\partial$）

$$\begin{array}{ccc} H_q(X,A) & \xrightarrow{f_*} & H_q(Y,B) \\ \downarrow{\scriptstyle\partial} & & \downarrow{\scriptstyle\partial} \\ H_{q-1}(A) & \xrightarrow{g_*} & H_{q-1}(B) \end{array}$$

Ax．4. Exactness axiom：

若 (X,A) 是一拓樸對，且 $i:A\to X$，$j:X\to(X,A)$ 均是 inclusion maps 那下面這無限序列（(X,A) 的同調序列）$\cdots\to H_q(A)\xrightarrow{i_*}H_q(X)\xrightarrow{j_*}H_q(X,A)\xrightarrow{\partial}H_{q-1}(A)\to\cdots$（其中 i_*，j^*，∂ 均是同態），是 exact 序列。亦即說對此序列中任一同調群而言，其輸入同態像和輸出同態函數的 kernel 相同。

Ax．5. Excision axiom：若 U 是拓樸空間 X 的開子集，且其閉包 $\bar{U}$ 包含於 X 的子空間 A 的內部，則對任意 q，此 inclusion map $e(X-U,A-U)\to(X,A)$ 引導出的同態。$e_{*q}:H_q(X-U,A-U)\to H_q(X,A)$ 是一同構。

〔註：在廣義的同調理論中，U 不必是 X 的開子集，但在 Čech 所造的同理論中，U 必是開集〕

Ax．6. Homotopy axiom：

若 $f,g:(X,A)\to(Y,B)$ 同倫，則對任意 q，$f_{*q}=g_{*q}$.

Ax．7. Dimension axiom：對任一包含一點 0 的空間 $\{0\}$ 而言，對任意 $q\neq0$，其 q 維同調群必只包含一元素，

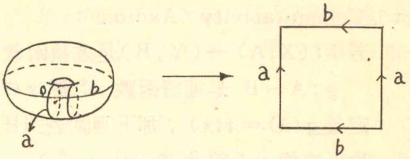
即 $H_q(0)=0$．

〔註：上述公設在廣義（singular）的複合形中均可證，為簡便起見，我們承認它們爲公設而加以應用。又上述同調理論公設均可改爲“對偶”的上同調理論公設，只要把同調群 $H_q(X,A)$ 的下標 q 改爲上同調群 $H^q(X,A)$ 的上標 q，且引導同態 i_* 改爲 i^*；f^* 改爲 f^* 下行的同態；$H_q(X,A)\xrightarrow{\partial}H_{q-1}(A)$ 改爲上行的同態

$H^{q-1}(A)\xrightarrow{\partial}H^q(X,A)$……等等即可。〕

～Singular（廣義）and Simplicial（單純）homology theory～

一個單純複合形 k 是歐氏空間的子空間，且包含有限個歐氏單純形並使其中任兩個的交集是他們的共面。若 k 中每一點至少屬於一單純形，而每一單純形的面單純形仍屬於此一組，則這組單純形叫做 k 的一個單純剖分（Simplicial decomposition）。一個拓樸空間若和一單純複合形同胚，則稱它可三角形剖分。若L是K的子複合形，則對單純複合形對（simplicial pair）（K，L）而言，廣義的同調理論均可適用（如此造出的同調群甚至和 Čech 用 nerve of covering 所造出的同構）。若K－L的維數是n則對任一 q＞n，$H_q(K,L)$ 均等於0。一個概念若和單純剖分無關，即爲拓樸不變量（如Euler示性數）。我們知道一環面和一在球面上一點有兩切圓的二維球雖有相同的同調群但不同胚，這個例子也許較難領會（環面無切割點，另一則有），我們看另一簡單的例子，如何區分環面與S^2？他們都緊緻、連通、局部連通。S^2 的基本群只包含一元素，而環面的基本群則爲 $Z\otimes Z$，如此當然不同胚。從同調的觀點看，他們的零維、二維同調群均是Z，而 $H_1(S^2)=0$，H_1（環面）$=Z\otimes Z$，故不同胚（根據0-18）他們一維同調群何以不同？從虧格看，S^2 上任一閉曲線（閉鍊）都可將 S^2 一分爲二，而環面的虧格是1，即有一"經圓"（閉鍊）不將環面分割爲二實際上我們也只對這"nonbounding"的一維閉鍊感興趣，經圓在環體中可縮成一點，而緯圓則否，事實上這只是環面浸沒在空間的拓樸性質，而非內在性質。我們可將此環面沿經圓(a)、緯圓(b)割開，彎扭成一正方形（這相當於環面的胞腔複合形（cell complex），使得衍生子個數減少，以便於同調群的計算）。



我們說了一大堆，似乎該回到原來的題目上來，爲什麼定義同調群爲 $Z_q(X,G)$ 和 $B_q(X,G)$ 的商群？（當然此商群是複合形的拓樸不變性，不依賴單純剖分）那些閉鍊和同調類的幾何意義是什麼？以上述環面爲例，若有兩條垂直方向的閉鍊，則 a_1 加上 a_2 是環面的一部分的邊界，也就是說 a_1+a_2 是個"bounding"一維閉鍊或說 a_1 和 a_2 同調；關於水平方向的閉鍊，要嗎本身是邊界，不然就和任一垂直閉鍊同調。所以在環面上只須討論兩種不同的閉鍊，所以它的一維 Betti number 是2，（這和我們的直觀說環面有兩個洞相對應）。把幾何圖形變成代數問題，就是把閉曲面（cycles）變成界爲零的鍊，把幾何上的邊界換成代數上的邊界函子，而此曲面上的最大數目的一維閉鍊的個數就和（邊界函子 d_1 的 kernel 模 d_2 的寫像）集合中的衍生子個數一樣。故研究閉曲面及其邊界就可改成研究：d_q 的 kernel 模 d_{P+1} 的寫像所成的商群。

～胞腔剖分（Cellular decomposition）～

一個複合形K可表爲胞腔複合形，只要符合下列四個條件：

①K的任一個P維開胞腔可表爲K中維數≤P的

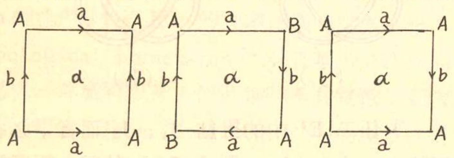
開單純形的聯集，且此P維開胞腔和開的實心P維球 S^P 同胚。

②K的任一P維開胞腔可表成X－Y，其中X,Y均是K的子複合形，且Y是K中維數小於P的胞腔的聯集。

③若X－Y是一P維胞腔，則此有序對（X，Y）和P維胞腔（閉的實心P維球）模P維胞腔邊界有相同的同調群 $H_P(X, Y)$ 的一個衍生子（generator）可以相對閉鍊 α' 表之，則 α 叫做在K中和X－Y有關的能定向P維胞腔。

④若 α 是K的一個能定向P維胞腔，則 $d\alpha$ 是K中P－1維胞腔的線性組合的和。

我們知道由一個空間的胞腔剖分和單純剖分做出來的同調群同構，而胞腔是把一些單純形湊在一起，使得此胞腔的邊界是更低維的胞腔，如此一來計算過程可減化不少。下列三圖分別表環



（一）　　（二）　　（三）

面,P^2（實投射平面），Klein bottle的胞腔剖分。我們要計算環面的同調群。（餘下的讀者自證，或參考21:頁121～123）如第一圖，有一個二維胞腔 α 他的邊界是 $a-b-a+b=0$，所以 α 是一個二維閉鍊，但此圖無三維閉鍊，故 α 是一“nonbounding”二維閉鍊若k是任一非零的正整數，則 $k\alpha$ 是“nonbounding”二維閉鍊，所以他不和其他如此形式的二維閉鍊同調而這兒只有這樣的二維閉鍊，所以它的二維同調群是一無限循環群Z，且其 Betti number $b_2=1$。此圖中有兩個一維閉鍊a和b，他們都不“bound”.（因爲唯一的二維胞腔的邊界是0），所以它的一維同調群是兩個無限循環群的直和（卽 $Z \otimes Z$），其 Betti number $b_1=2$ 最後，唯一的零維胞腔A是“nonbounding”的零維閉鍊

故 H_0（環面）$=Z$，且 $b_0=1$

對實投射平面 P^2 來說，若係數群沒有秩爲二的元素（如Z）

則 $H_2(P^2)=Z$，$H_1(P^2)=Z_2$，$H_0(P^2)=0$

但 $H_0(P^2;Z_2)=H_1(P^2;Z_2)$

$=H_2(P^2;Z_2)=Z_2$

$H_0(P^2;Q)=Q$，$H_1(P^2;Q)=0$（何故?）

$H_2(P^2;Q)=0$

對klein bottle來說，$H_0(K)=Z$，

$H_1(K)=Z\otimes Z_2$，$H_2(K)=0$．

～同倫與基本群～

在前面提到要區別環面和 S^2 時可以一維同調群之不同區別之，也可以基本群的不同區別之。我們設想在環面上挖去一開的“disc”D，則就同調的觀點，可以無視此洞之被挖，蓋仍存

在兩個一維閉鍊的同調鍊；但從同倫的觀點看，D的邊界Z是一閉鍊，且不可能緊縮至一點而不離此環面，所以此洞之被挖就不是無關痛癢的了。我們可以倣造基本群（一維同倫群）的造法造高維同倫群 $\pi_n(k, x_0)$，而他們都是交換群（$n \geq 2$）。

～ Covering Spaces～

若X是arcwise和locally arcwise-connected，則一個連續映成函數 P：B→X叫一個covering map，若對X中任一點x，有一個arcwise-connected 開集U包含x，使得 $P^{-1}(U)$ 的每一個component都是B中的開集，而這些component 又被P同胚映成地映至U。此時B叫做X的covering space，從下面的例子可看出 E^1 是 S^1 的covering space.

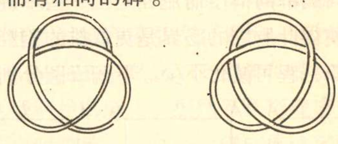
定義 $p: E^1 \to S^1$ 爲 $p(t) = (\cos 2\pi t, \sin 2\pi t)$ 對任一 $(x, y) \in S^1$，令

$U = S^1 - (-x, -y)$，則 $p^{-1}(u)$ 是所有以 $\frac{1}{2\pi}\arccos x$ 爲中點，單位長的開區間的聯集，每一如此的開區間又被P同胚映成到U，故 E^1 是 S^1 的covering space.

如上述定義中P：B→X是一 covering map，若P(b)＝x，則它引導出的同胚 $P_*: \pi_n(B, b) \to \pi_n(X, x)$，$n \geq 2$ 是一個映成同構。

～扭結（knot）及浸沒（imbedding）～

E^3 中的兩個單純閉曲線是同一的（equi-valent）若且唯若他們之間存在一"保持定向的"同胚將一曲線映至另一曲線。一個單純閉曲線是"未扭結的"如果他和 E^3 中的圓（$x_1^2 + x_2^2 = 1$，$x_3 = 0$）是同一的話，否則就是扭結的。事實上任一扭結均是 E^3 的子空間，所以他們自身都是同胚的，要區別他們只有看他們浸沒在 E^3 中的方式如何了。對所有 E^3 中的扭結J，他們在 E^3 的補集的同調群都相同，但 $E^3 - J$ 的基本群（叫做扭結J的群）則不盡相同，且非交換群。但如下的兩個三叉扭結（trefoil knots）非同一而有相同的群。



(J_1)　　(J_2)

對任二 E^3 中的扭結 J_1，J_2 而言，必有一同胚 $h: J_1 \to J_2$，則 J_1 和 J_2 的同一問題變成"是否存在從 E^3 到 E^3 的同胚 $\bar{h}$，使得 $\bar{h}|J_1 = h$？"1908年 Schoenflies 證了如下的定理（即在平面上沒有扭結）："設J是 E^2 上單純閉曲線，h把J同胚地映成至 E^2 的單位圓 S^1，則h可擴張成從 E^2 到 E^2 的同胚 $\bar{h}$。"把此定理中的 E^2 改成 E^3 則不成立。設S是 E^3 中的單純閉曲面（即S和 S^2 同胚）令 $\bar{h}$ 表映至S至 S^2

的同胚，那是否存在 E^3 中的同胚 $\bar{h}$ 使得 $\bar{h}|s=h$？Alexander 證明若 S 是 E^3 中的“finite polytope”，則此定理成立。在一般的情形下，此定理不對，Alexander horned sphere 就是一個有名的反例，因爲此 horned sphere 的補集非單連通，而 E^3-S^2 是單連通（在 horned sphere 上有 Cantor set 這樣的“壞”點）。

Brouwer 在 1912 年證出 E^n 中沒有閉子集和不能定向的 $n-1$ 維流形同胚，這結果很嚴重地阻礙我們對緊緻、不能定向曲面的幾何直觀發展，蓋這種曲面不能同胚地浸沒在 E^3 中。當然若我們允許“singularities”或“自相交”的話，我們也能造出在 E^3 中的這種曲面的模型。我們如果考慮流形的“immersion”這概念的話，也能造出這種模型的數學理論。一個從緊緻 n 維流形 M^n 至 R^m 的連續函數 f 叫做一個“topological immersion”若且唯若 M^n 中每一點有一鄰域可以被 f 同胚地映至其寫像。通常我們所用的 Klein Bottle 在 R^3 中的模型就是 Klein Bottle 在 R^3 中的 immersion。Werner Boy 在 1901 年造出 P^2 在 R^3 中的“immersions”（這些 immersions 相當複雜）。1958 年 Markov 得證說對緊緻、可三角形剖分的四維流形的分類（Classification）的證明都是不存在的。

曲面的分類：曲面中能定向的都能表爲一有 h 個 handles 和 k 個 contours 的球（$h,k\geq 0$）；不能定向的可表成有 q 個 crosscaps 和 k 個 contours 的球（$q,k\geq 0$）。（參考 5，頁 33）

～從 S^k 到 S^n 的連續函數（同調群理論的應用）～

①所有從 S^k 到 S^1 的連續函數必和常數函數同倫（$k>1$）。所有從 S^k 到 S^n（$k<n$）的連續函數必和常數函數同倫。任二從 S^n 到 S^n 的連續函數的“degree”必相等。任兩不同維數的球 S^m, S^n 不同胚。

②徑點函數（antipodal map）$r: S^n\to S^n$ 的 degree 是 $(-1)^{n+1}$。

③ $f,g: S^n\to S^n$ 且對任一 $x\in S^n$，

$$f(x)\neq g(x)$$

則 $\deg(f)+(-1)^n\deg(g)=0$.

④若 $f: S^n\to S^n$ 是一無定點的連續函數（對任何 $x\in S^n$，$f(x)\neq x$），則 $\deg(f)=(-1)^{n+1}$。（所以若 $\deg(f)\neq(-1)^{n+1}$ 則 f 有定點）。

⑤若 $f: S^n\to S^n$ 且 $\deg(f)\neq 1$，則存在一 $P\in S^n$ 使得 $f(P)=-P$.

⑥若 $f: S^{2m}\to S^{2m}$，則存在 $P\in S^{2m}$ 使得 $f(P)=P$ 或 $f(P)=-P$.

⑦ $f: S^n\to S^n$ 若非映成，則必與常數函數同倫蓋 $S^n-\{x\}$ 和 R^n 同胚，而任何連續函數 $f: S^n\to R^n$ 必與常數函數同胚。

⑧若 n 是奇數，則在 S^n 上必存在一連續單位切向量場。

⑨若 n 是偶數，（ $n>0$ ）則在 S^n 上沒有連續的單位切向量場。

〔註：在 S^n 上的連續單位切向量場是指一組 R^{n+1} 中的單位向量所成的集合，這每一單位向量在 S^n 上和 S^n 相切，且使在點 $x\in S^n$ 的向量的方向隨著點 x 連續地改變。〕（參考10，第四章）

～上同調環（Cohomology ring）～

一般說來，同調理論和上同調理論可說是對偶的（dual），即在同調中能發現什麼，在上同調中也能發現相似的。同調中的鍊群 $C_p(X,G)$ 和上同調中的餘鍊群 $C^p(X,G)$ 的關係，就好像泛函分析中的｛所有在X上連續的函數｝和｛在X上的線性泛函數（或函子）｝的關係。可惜的是我們現在要討論的上同調環，在同調理論中竟找不到類似的理論。一個空間的上同調環也是一個拓樸不變量。上同調環是由上同調群再加上上同調類的所謂 cup product 的乘法而成環的，所以可能有兩空間有相同的上同調群而有不同的上同調環，同時也就是用這個來區分出這兩個空間。如 $(P^2\vee S^3)\times P^2$ 和 $P^3\times P^2$ 這兩個空間就是有相同的上同調群而上同調環則不同的例子，還有一個例子是 $S^1\times S^1$（環面）和 $S^1\vee S^1\vee S^2$。他們有相同的同調群和上同調群，而上同調環却不同，（不過這兩個空間有不同的基本群，所以這例子還不太令人滿意。）

設 C^p, C^q 是複合形K中的餘鍊，C^p 和 C^q 的 cup product 被定義成爲一個 P+q 維餘鍊 $C^p\cup C^q$，而 $C^p\cup C^q(<\nu_0\cdots\nu_p,\nu_{p+1}\cdots\nu_{p+q}>)$ $=C^p(<\nu_0\cdots\nu_p>)\cdot C^q(<\nu_p\cdots\nu_{p+q}>)$

且 cup product 滿足下列五性質：

①$C^p\cup C^q$ 是一個 bilinear 函數

②$(C^p\cup C^q)\cup C^r=C^p\cup(C^q\cup C^r)$

③$C^p\cup e^0=e^p$（e^0 是上同調環單位元素，而在K中 e^0 是個餘閉鍊，使得對任何K之頂點 ν，$e^0(\nu)=1$）。

④$e^0\cup C^p=C^p$

⑤$\delta(C^p\cup C^q)=\delta C^p\cup C^q+(-1)^p$ $C^p\cup\delta C^q$

上同調環不一定是交換環（即使其係數環是交換環），但它有如下的交換規則：

$a^p\cup b^q=(-1)^{pq}\ b^q\cup a^p$

其中 $a^p\in H^p(k)$，$b^q\in H^q(k)$。

關於張量積的上同調和積空間的上同調群等理論過於複雜，請讀者自己參考（25，第四章）。像環面可看成拓樸積 $S^1\times S^1$，故其上同調環就要積空間上同調環的理論了。又關於鍊和餘鍊之間的乘積 cap product 請參考（26，頁310）。

～Čech 同調和上同調理論～

Čech 是捷克偉大的拓樸學家，爲紀念他，他所造出的同調與上同調群上都有“ $\vee$ ”這一符號。對單純複合形而言，他的理論和廣義同調，

上同調理論是一樣的。在未說明他的理論是如何造的以前，先看它的一些性質。在 Čech 的理論中，同倫公設中的空間要限制成緊緻的才行。Excision 公設中集合U要是開集；exactness axiom 不存在，或是說以非常弱的形式存在。可是在 Čech 的理論中多了一個 Continuity 公設，說明對同調的逆納系統（或上同調的直導系統）中的緊緻拓樸空間對（E_α，F_α）而言，先取極限再造的 Čech 同調群（或上同調群）和先造 Čech 同調群（或上同調群），再取極限所得之群同構。

我們現在看 Čech同調理論的造法。他的動機是看到用單純複合形去逼近一個拓樸空間，所以他倣造此，對一空間E的有限開覆蓋（open covering）u，造出對應的複合形 K_u（即 u 的 nerve）如下：K_u 中的頂點是 πR_u 中的點U，且U屬於 u。單純形〔$U_0,\cdots,U_P$〕包含於 K_u 若且唯若 $U_0,\cdots,U_P$，被視為E中之開集時，其交集非空。若我們的 covering 愈來愈好的話，則他的 nerve 也就愈來愈逼近原來的複合形了。Čech 同調群被定義為一個空間的 nerve of coverings 的單純同調群的逆納極限。從定義可以很快得知若E只包含一點，則 $H_P(E)=0$（$P>0$），$H_0(E)=G$（係數群）。當 (E,F) 是單純複合形對時，我們可證得 Čech 同調群和能定向的單純同調群同構。又從 Continuity axiom 可證對緊緻空間E上的 Čech 同調群（或上同調群）是唯一的。又（19：Massey 的 lecture notes 上對 Čech cohomology 的造法中以 nerve of covering 造複合形時和函數的 support 有關，有一些說明）。

我們提出一個例子說明 Čech 同調群不一定和廣義同調群同構，令E表平面的子空間，包含線段 $(0,y)$，$(\frac{2}{\pi},y)$ 其中 $1\geq y>-2$ 和線段 $(x,-2)$，其中 $0\leq x\leq\frac{2}{\pi}$ 及圖形 $y=\sin\frac{1}{x}$（$0<x\leq\frac{2}{\pi}$），則 $H_1(E)=0$，而 $\check{H}_1(E)=Z$（無限循環群）（參考25，頁194）。

～ 對偶定理（duality）～

最後我們介紹三個對偶定理（Alexander，Poincar'e，Lefschetz）我們只提及其定理內容及應用而不證明，讀者若有興趣的話，可參考胡世楨的書（上同調理論）。

1. Alexander：

引理 1. 若 $x_0\in A$，A是 R^n 的子空間且和一單純形同胚。則對任一整數 q，$H_q(R^n-\{x_0\}, R^n-A;G)=0$

引理 2. 若A是 R^n 的子空間，且A和一單純形同胚，則同態 $h_u: H_q(R^n, R^n-A;G) \to H^{n-q}(A;G)$ 是一同構。

定理 3. 對 R^n 的任一定向 u，及任一 R^n 的

有限可三角形剖分的子空間A，則對任一整數q。此同態

$h_u: H_q(R^n, R^n - A; G)$

$\to H^{n-q}(A; G)$ 是一同構。

定理4. （R^n 的有限可剖分子空間的對偶定理）.

若A是 R^n 的有限可剖分子空間，則對任一整數q.

$\widetilde{H}_q(R^n - A; G) \cong H^{n-q-1}(A; G)$

（其中 $\widetilde{H}_q(R^n - A; G)$ 表 reduced 廣義同調群）。

結論5. 如定理4且A和 S^m 同胚，則

$H_q(R^n - A; G) \approx H_q(S^{n-m-1}; G)$

結論6. 如定理4且A和 S^{n-1} 同胚，則 $R^n - A$ 包含兩個 components，其中有且僅有一 component 是有界的（bounded）.

結論7. （Jordan Curve 定理）

若A是 R^2 的一單純閉曲線，則 $R^2 - A$ 包含兩個 components，其中有且僅有一 component 是 bounded.

引理8. 若A是 R^n 中緊緻子空間，則對任一整數q，$H_q(R^n, R^n - A; G) \cong H^{n-q}_{R^n}(A; G)$.

引理9. $H^{n-q}_{R^n}(A; G) \cong H^{n-q}(A, G)$

（其中 $H^{n-q}(A, G)$ 表 n－q 維，Alexander 上同調群）。

定理10. （R^n 的緊緻子空間的對偶定理）

對任一 R^n 中的緊緻子空間A，及任一整數q

$H_q(R^n - A; G) \cong H^{n-q-1}(A; G)$

（其中 $H_q(R^n - A; G)$ 表 reduced 廣義同調群，$H^{n-q-1}(A; G)$ 表 n－q－1 Alexander 上同調群）。

2. Poincar'e：

引理1. 令 $X = R^n$，在此系統中，X表n流形，A是X中的緊緻子空間，則對任一整數q. 此同態（homomorphism）

$b_u: H_q(X, X - A; G)$

$\to H_X^{n-q}(A; G)$

是一同構（isomorphism）。

引理2. 若A包含於X的坐標鄰域中，則對任一整數q. 此同態

$b_u: H_q(X, X - A; G)$

$\to H_X^{n-q}(A; G)$ 是一同構。

定理3. 對能定向的n維流形X的任一定向 u 及X的任一緊緻子空間A，此同態

$b_u: H_q(X, X - u, G)$

$\to H_X^{n-q}(A; G)$ 是一同構。

結論4. （Poincar'e 對偶定理）

若X是緊緻的，能定向的n維流形，則對任意整數q.

$H_q(X; G) \cong H^{n-q}(X; G)$

結論5. 若X是緊緻能定向的n維流形，則

$H_q(X; G) = 0 = H^q(X; G)$（其中

$q > n$）.

結論 6. 若 X 是連通緊緻，能定向的 n 維流形則 $H_n(X;G) \cong G \cong H^n(X,G)$（此後 X 表緊緻，能定向的 n 維流形，且 X 和有限胞腔 polytope 同倫一致）。

定理 7. 對任一整數 q，X 的 q 維 Betti number 和 n－q 維的 Betti number 相等。

結論 8. 若 n 是奇數，則 X 的 Euler 示性數是 0.

定理 9. 對任一整數 q，X 的 q 維撓係數（torsion coefficients）和（n－q－1）維的撓係數相等。

結論 10. X 在 0 維，n－1 維，n 維時，都是 torsion free.

3. Lefschetz 對偶定理：

令（X，A）表緊緻，能定向的，有邊界的（with boundary）的 n 維流形，則對任一整數 q.

$$H_q(X;G) \cong H_q(X-A;G) \cong H^{n-q}(X,A;G)$$

$$H^q(X;G) \cong H^q(X-A;G) \cong H_{n-q}(X,A;G)$$

～緒語～

拉拉雜雜地寫了一大堆，又是英文中文夾雜著，很多英文名詞沒有適當的中譯，只好以英文出現了。儘管已經介紹了許多概念，仍有許多未能介紹，如 orientation，incidence number Mayer-Vietoris sequence，acyclic，C－W complex 等等。我們不敢期望看完本文就對代拓有深入的了解，但希望有些點集拓樸及群論知識的讀者能對代拓有些認識，而去找有關代拓的書翻翻（可能的話能提出問題互相討論）。文中本想多做一些同調群的例子，並對 Brouwer 定理加以詳細說明，奈何文章寫下來就不知該在什麼地方補充了。文中曾多次提到用同調群、上同調群、基本群、上同調環等的拓樸不變性來區別拓樸空間，對一些特殊的空間要造上述的群和環除了用 exactness axciom 和 excision axiom，simplicial decomposition，Euler 示性數等有力工具外，還可以 cellular decomposition 使造群的過程減化。文中曾對同調群的閉鍊、邊界等加以幾何直觀的說明，否則代數工具用了太多、太過抽象化後，簡直就不知我們在做什麼了。最後謝謝讀者能耐心地看完本文。

參考資料：

1. Alexandroff： Combinatorial Topology（3 volumes）（1960）
2. Ahlfors：Riemann Surfaces（1953）
3. Brown：Elements of morden topology（1968）
4. Cooke and Finney：Homology of cell complexes（1967）

5. Cairns : Introductory topology (1961)
6. Dugundji : Topology (1960)
7. Eilenberg and Steenrod : Foundations of algebraic topology (1952)
8. Greenberg : lectures on algebraic topology (1968)
9. Hilton : Homology Theory (1966); Homotopy Theory (1953) Homotopy
10. Hu : Homology Theory (1966); Homotopy Theory (1959)
11. Hu : Homological Algebra (1968)
12. Hu : Cohomalogy Theory (1971)
13. Hurewicz and Wallman : Dimension Theory (1941)
14. Lefschetz : Introduction to topology (1949)
15. Lefschetz : Algebraic topology (1942)
16. Markushevich : Theory of functions of a complex variable (Vol. Ⅲ)(1970)
17. May : Simplicial Objects in algebraic topology (1971)
18. Massey : Algebraic topology (1967)
19. Massey : Notes on homology and cohomlogy theory (1971)
20. Pontrjagin : Foundations of Combinatorial topology (1952)
21. Patterson : Topology (1956)
22. Seifert and Threlfall : Lehrbuch der Topologie (1934)(商務印書館有中譯本)江澤涵譯
23. Steenrod : The topology of fibre bundles. (1951)
24. Wallace : An introduction to algebraic topology (1957)
25. Wallace : Algebraic topology (1970)
26. Hocking and Young : Topology (1961)
27. Maclane : Homology (1963)
28. Spanier : algebraic topology (1966)
29. Williard : General topology (1970)
30. Blackett : Elementary topology (1967)

Two Problems on Prime Pairs

謝南瑞三乙

O. Introduction

In the note, we will first find the primes between a given prime P_n and its square; then consider a sufficient-necessary condition for prime pairs . At last, we like to discuss some cenjecture and restriction on our result. This note is developed according to a paper by R. D. larsson [1].

The well-known Butrancl's Cmjecture tells us that there cxists a prime between P_n and $2P_n$, consqueutly P_n and P_n^2. It becomes interesting to find all primes between them.

We exclude the cuse $P_n = 2$.

I. Primes between a prime and its square .

Let $P_1 \cdots\cdots P_n$ be the set of primes with natural order , i.e. $P_1 = 2 \quad P_2 = 3 \quad P_3 = 5 \quad \cdots$

Computing r_i for $P_n \equiv r_i \pmod{P_i}$ $i = 2 \cdots\cdots n-1$, where r_i is least positive residue, we have two sets.

$$E = \{\text{even integers}\} \quad \{ RP_i - r_i \mid i = 2 \cdots\cdots n-1 , R = 1,2,3 \cdots \}$$

and $E' = \{ \text{positive even integers} \} - E$.

Lemma 1.1 E' isn't empty

pf. Assume that $E' = \phi$, then each even integer can be expressed as $RP_i - r_i$ for some R_i and i .

Thus, each of $P_i + 2$, $P_i + 4 \cdots\cdots$ is of the form $P_i + RP_i - r_i$

Sinse $P_i \mid (P_n + RP_i - r_i)$, each of $P_n + 2$, $P_n + 4 \cdots\cdots$ isn't prime.

This contradicts to Burtrand's Cinjecture.

Therefore $E' \neq \emptyset$. QED

Lemma 1.1 assures that $\exists\ b_1 \in E'$: least element of E'

We claim that $P_n + b_1$ is a prime next to P_n.

Lemma 1.2 $0 < b_1 < P_n^2 - P_n$.

pf. Clearly $b_1 > 0$.

$P_n^2 - P_n$ is a positive even integer; hence either $P_n^2 - P_n \in E$ or $P_n^2 - P_n \in E'$

However, $P_n^2 - P_n \in E \rightarrow P_n^2 - P_n = RP_i - r_i$ for some R and i.

$\rightarrow P_n^2 = P_n + RP_i - r_i \rightarrow P_i \mid P_n^2$ Contradicting to $(P_i, P_n) = 1$.

Thus. $P_n^2 - P_n \in E'$ and $b_1 \leq P_n^2 - P_n$.

The assumption $b_1 = P_n^2 - P_n$ will imply that P_n^2 is the least element of $P_n + E'$

It's easy to see that each prime greater than P_n is in $P_n + E'$.

Now this yields a contradiction to Bertrand's cenjecture.

Therefore $b_1 < P_n^2 - P_n$. QED

Now, we may have.

Theorem 1.3 $P_n^2 + b_1$ is a prime next to P_n.

pf. Suppose that $P_i \mid P_n^2 + b_1$ fur some $i = 2, 3, \cdots\cdots n-1$.

Then $P_n \equiv -b_i \pmod{P_i}$, and thus. $r_i \equiv -b_1 \pmod{P_i}$

$\exists\ k \in Z : -b_1 - r_i = RP_i$ Hence. $b_1 = (-k)P_i - r_i$.

Since both b_1 and r_i are positive. k is less than 0.

$-k > 0$, and $b_1 \in E$. A contradiction.

If $P_n \mid P_n + b_1$ then $\exists\ k \in Z : RP_n = P_n + b_1$.

Since. $0 < b_1 < P_n^2 - P_n$, $P_n < RP_n < P_n^2$

$1 < k < P_n$ there exists a P_i smch that $P_i \mid k$. i is one of $1, 2, \cdots\cdots n-1$.

Thus. $P_i \mid P_n + b_1$ A contradiction.

This proves the theorem. QED.

Corollory 1.4 Let $S = \{P_n + b_i \mid b_i \in E' \quad i = 1, 2, \cdots\cdots b_i < P_n^2 - P_n\}$.

then S consists of all primes between P_n and P_n^2.

pf. By theoem 1.3 each element of S is a prme between P_n and P_n^2.

Conversely. consider that each odd integer m greater than.

P_n is either in $P_n + E$ or $P_n + E'$.

However $m \in P_n + E \rightarrow m = P_n + kP_i - r_i$ fun some k and i .

$\rightarrow P_i \mid m$,Thus m isn't a prime . QED .

II. Necessary and Sufficient conditions for prime pairs .

for discussion in this Section is based in the following lemma.

Lemma 2.1 $P_n + 2 = P_{n+1}$ iff $P_i - r_i \neq 2$, $\forall_i = 2 \cdots\cdots n-1$, where P_i , r_i are difined as in Section I . As before we exclude the case $n = 1$.

pf. Assime that $P_n + 2 = P_{n+1}$ and $P_i - r_i = 2$ fur some $i = 2, 3, \cdots\cdots n-1$.

Then $P_{n+1} = P_n + (P_i - r_i)$, which implies that $P_i \mid P_{n+1}$.

A contradict. This proves the sufficient part.

Conversely suppose that $A = P_n + 2$ isn't prime .

then $P_i \mid A$ for some $i = 2, \cdots\cdots n-1$.

$A = kP_i \rightarrow kPi - 2 = P_n$.

Since r_i is least positive residue this forces $2 = P_i - r_i$

Hence the necessary condition nolds QED .

By definition of r_i, we have .

$$P_n - r_i = k_i P_i \quad k_i = [P_n / P_i] \geq 1.$$

Thus. $P_i - r_i = (k_i + 1) P_i - P_n$.

If. $P_i - r_i = 2$, then $k_i + 1$ is odd. Hence , $k_i = 2m_i$, an eveninteger and $k_i + 1 \geq 3$.

By Bertrand's cenjecture, $P_{n+1} < 2P_n$.

It is well-known that to see whether an positive integer n is a prime, one needs only to divide n by there primes which are less than $\sqrt{n}$.

Combining our remark above , we have , by the virtue of lemma 21.

Thm 2.2 For a given n. $P_n + 2$ is a prime iff the following condition holds .

For each P_i such that

$$[P_n / P_i] = 2m_i \text{ and } 3 \leq P_i < \sqrt{2P_n} .$$

Corollary 2.3 If $[P_n/P_i] = 2m_i + 1$, for all $3 \leq P_i < \sqrt{2P_n}$.

then. P_n+2 is a prime .

Remark . Suppose that P_n+2 is a prime .

$P_n = k_i p_i + r_i$ k_i is odd iff r_i is even .

The probalility of r_i being even is $\frac{\frac{P_i-1}{2}}{P_i-2} = \frac{P_i-1}{2(P_i-2)}$

(Note that $P_n \not\equiv 0$, $P_i-2 \pmod{P_i}$)

Hence , the probability of the success of the hypothesis in corollary 2.3 is

$\prod_{2}^{m} \frac{P_i-1}{2(P_i-2)}$ where . P_n is the largest prime such that $P_n < \sqrt{2P_n}$.

As one can see, the value becomes less when n becmes larger.

In fact . by computation, we see that the hypothesis holds.

fon $P_n = 3,5,11,17$, and fails for all prime pairs within 10,000 , beyond. $\{17,19\}$ < see Appendix> .

Therefore , we may cenjecture that the hypothesis of corollary 2.3. fails for all prime pairs beyond $\{17 , 19\}$.

III.A restriction to the necessary condition of Theorem 2.3.

Using congruence,we may restrict the necessaery condition of prime pairs to the following basic one .

Theorem 31 If P_n+2 is a prime then. $P_n = 6r+5$, for all $P_n > 3$.

whue $r \pm 5k, 7k, 5k+3, 7k+5$, $k = 0,1,2,\cdots\cdots$.

pf. Either $P_n \equiv 1 \pmod 3$ on $P_n \equiv 2 \pmod 3$, for all $P_n > 3$.

The fact P_n+2 is a prime implies that $P_n \equiv 2 \pmod 3$

Thns $P_n = 3m+2$, $m \in Z$, $m > 0$

Since P_n is odd , m is odd too $m = 2r+1$, $r = 0,1,2,\cdots\cdots$

$\therefore$ $P_n = 6r+5$

Both $P_n = 6r+5$, and $P_n+2 = 6r+7$ are primes; we see that.

$r \neq 5k, 7k, 5k+3, 7k+5, k = 0, 1, 2, \cdots\cdots$ QED

Remark By thm 31, there is no " Prime trio " $\{P_n, P_n+2, P_n+3\}$ except.

$\{2,3,5\}$, $\{3,5,7\}$, For $P_n > 3$.

$\{P_n+2, P_n+4\}$ is a prime pair, hence $P_n+2 \equiv 2 \pmod 3$.

However, we thus have that $P_n \equiv 0 \pmod 3$, Contradicting to P_n being a prine.

Similar reasming holds fon modulus 5.

If $P_n > 5$ out P_n+2 is a prime, then exact one of $P_n \equiv 1 \pmod 5$, $P_n \equiv 2 \pmod 5$, $P_n \equiv 4 \pmod 5$. holds, we discuss them one by one.

(i) $P_n \equiv 1 \pmod 5$, $P_n = 5m+1 = 10r+1$, Since m is even and can be expressed as $m = 2r$. $r = 1, 2, \cdots\cdots$, $r \neq 3k, 3k+2$, $k = 0, 1, 2, \cdots\cdots$

(ii) $P_n \equiv 2 \pmod 5$. $P_n = 5m+2 = 10r+7$, $(m = 2r+1)$.

$r = 1, 2, \cdots\cdots$ $r \neq 7k, 7k+4, 9k, 9k+2, 9k+3, 9k+5, 9k+6, 9k+8$,

$k = 0, 1, 2, \cdots\cdots$

(iii) $P_n \equiv 4 \pmod 5$ $P_n = 5m+4 = 10r+9$ $(m = 2r+1)$.

$r = 1, 2, \cdots\cdots$ $r \neq 9k, 9k+1, 9k+3, 9k+4, 9k+6, 9k+7, 11k, 11k+9$

$k = 0, 1, 2, \cdots\cdots\cdots\cdots$—

Reference:

〔1〕 Robert. D. Larsson : Necessary and Sufficient conditions for prime pairs. American Math. Jour. 1961.

〔2〕 Calvin. T. Long : Elementary Introduction to Number Theory.

Appendix : (We drop the prime pairs from a table of prime numbers. listed in Calrin T. Long's " Elementary Introtuction to Number Theory ".

$[\frac{41}{5}] = 8$	$[\frac{419}{11}] = 38$	$[\frac{1019}{11}] = 92$	$[\frac{1619}{13}] = 124$
$[\frac{71}{5}] = 14$	$[\frac{431}{5}] = 86$	$[\frac{1031}{5}] = 206$	$[\frac{1667}{7}] = 238$
$[\frac{101}{5}] = 20$	$[\frac{461}{5}] = 92$	$[\frac{1049}{13}] = 80$	$[\frac{1697}{7}] = 242$

$\left[\frac{107}{13}\right]=8$	$\left[\frac{521}{5}\right]=104$	$\left[\frac{1061}{5}\right]=212$	$\left[\frac{1721}{5}\right]=344$
$\left[\frac{137}{11}\right]=12$	$\left[\frac{569}{23}\right]=24$	$\left[\frac{1091}{5}\right]=218$	$\left[\frac{1787}{11}\right]=162$
$\left[\frac{149}{17}\right]=8$	$\left[\frac{599}{11}\right]=54$	$\left[\frac{1151}{5}\right]=230$	$\left[\frac{1871}{5}\right]=374$
$\left[\frac{179}{11}\right]=16$	$\left[\frac{617}{7}\right]=88$	$\left[\frac{1229}{13}\right]=94$	$\left[\frac{1877}{7}\right]=268$
$\left[\frac{191}{5}\right]=38$	$\left[\frac{641}{5}\right]=128$	$\left[\frac{1277}{7}\right]=182$	$\left[\frac{1931}{5}\right]=386$
$\left[\frac{197}{7}\right]=28$	$\left[\frac{659}{7}\right]=94$	$\left[\frac{1289}{7}\right]=184$	$\left[\frac{1949}{7}\right]=278$
$\left[\frac{227}{7}\right]=32$	$\left[\frac{809}{19}\right]=42$	$\left[\frac{1301}{5}\right]=260$	$\left[\frac{1997}{23}\right]=86$
$\left[\frac{239}{7}\right]=34$	$\left[\frac{821}{5}\right]=164$	$\left[\frac{1314}{7}\right]=188$	
$\left[\frac{269}{7}\right]=38$	$\left[\frac{827}{7}\right]=118$	$\left[\frac{1427}{23}\right]=62$	
$\left[\frac{281}{5}\right]=56$	$\left[\frac{857}{7}\right]=122$	$\left[\frac{1481}{5}\right]=296$	
$\left[\frac{311}{5}\right]=62$	$\left[\frac{881}{5}\right]=176$	$\left[\frac{1487}{13}\right]=114$	
$\left[\frac{347}{13}\right]=26$		$\left[\frac{1607}{11}\right]=146$	
$\left[\frac{2027}{11}\right]=184$	$\left[\frac{2729}{11}\right]=248$	$\left[\frac{3119}{19}\right]=164$	$\left[\frac{3671}{5}\right]=734$
$\left[\frac{2081}{5}\right]=416$	$\left[\frac{2789}{7}\right]=398$	$\left[\frac{3167}{7}\right]=452$	$\left[\frac{3767}{7}\right]=538$
$\left[\frac{2111}{5}\right]=422$	$\left[\frac{2801}{5}\right]=560$	$\left[\frac{3251}{5}\right]=650$	$\left[\frac{3821}{5}\right]=764$

$\left[\frac{2129}{7}\right]=304$

$\left[\frac{2141}{5}\right]=428$

$\left[\frac{2237}{13}\right]=172$

$\left[\frac{2267}{11}\right]=106$

$\left[\frac{2309}{23}\right]=100$

$\left[\frac{2339}{7}\right]=334$

$\left[\frac{2381}{5}\right]=476$

$\left[\frac{2549}{7}\right]=364$

$\left[\frac{2591}{5}\right]=518$

$\left[\frac{2657}{13}\right]=204$

$\left[\frac{2687}{11}\right]=244$

$\left[\frac{2771}{5}\right]=542$

$\left[\frac{2969}{7}\right]=424$

$\left[\frac{2999}{7}\right]=428$

$\left[\frac{3257}{11}\right]=296$

$\left[\frac{3299}{17}\right]=194$

$\left[\frac{3329}{11}\right]=302$

$\left[\frac{3359}{13}\right]=258$

$\left[\frac{3371}{5}\right]=674$

$\left[\frac{3389}{7}\right]=484$

$\left[\frac{3461}{5}\right]=692$

$\left[\frac{3467}{13}\right]=266$

$\left[\frac{3527}{11}\right]=320$

$\left[\frac{3539}{13}\right]=272$

$\left[\frac{3557}{7}\right]=508$

$\left[\frac{3581}{5}\right]=716$

$\left[\frac{3851}{5}\right]=770$

$\left[\frac{3917}{11}\right]=356$

$\left[\frac{3929}{13}\right]=302.$

$\left[\frac{4001}{5}\right]=800$

$\left[\frac{4019}{7}\right]=374$

$\left[\frac{4091}{5}\right]=818$

$\left[\frac{4649}{7}\right]=664$

$\left[\frac{4721}{5}\right]=944$

$\left[\frac{4787}{13}\right]=368$

$\left[\frac{5009}{17}\right]=294$

$\left[\frac{5021}{5}\right]=1004$

$\left[\frac{5099}{7}\right]=728$

$\left[\frac{5879}{11}\right]=534$

$\left[\frac{4127}{17}\right]=242$

$\left[\frac{4157}{19}\right]=218$

$\left[\frac{4217}{7}\right]=602$

$\left[\frac{4229}{7}\right]=604$

$\left[\frac{4241}{5}\right]=848$

$\left[\frac{4259}{7}\right]=608$

$\left[\frac{4271}{5}\right]=854$

$\left[\frac{4421}{5}\right]=884$

$\left[\frac{4481}{5}\right]=896$

$\left[\frac{4517}{11}\right]=410$

$\left[\frac{4547}{27}\right]=168$

$\left[\frac{4637}{7}\right]=662$

$\left[\frac{8009}{7}\right]=1144$

$\left[\frac{8087}{13}\right]=622$

$\left[\frac{8219}{7}\right]=1174$

$\left[\frac{4799}{11}\right]=436$

$\left[\frac{4931}{5}\right]=986$

$\left[\frac{4967}{13}\right]=382$

$\left[\frac{5231}{5}\right]=1046$

$\left[\frac{5279}{7}\right]=754$

$\left[\frac{5417}{11}\right]=492$

$\left[\frac{5441}{5}\right]=1088$

$\left[\frac{5501}{5}\right]=1100$

$\left[\frac{5519}{7}\right]=788$

$\left[\frac{5639}{11}\right]=512$

$\left[\frac{5651}{5}\right]=1130$

$\left[\frac{5657}{7}\right]=808$

$\left[\frac{5741}{5}\right]=1148$

$\left[\frac{5849}{17}\right]=344$

$\left[\frac{5867}{7}\right]=838$

$\left[\frac{9011}{5}\right]=1802$

$\left[\frac{9041}{5}\right]=1808$

$\left[\frac{9238}{13}\right]=710$

$\left[\frac{9927}{7}\right]=1418$

$$\left[\frac{8231}{5}\right] = 1646$$

$$\left[\frac{8291}{5}\right] = 1658$$

$$\left[\frac{8387}{7}\right] = 1198$$

$$\left[\frac{8429}{7}\right] = 1204$$

$$\left[\frac{8537}{11}\right] = 776$$

$$\left[\frac{8597}{19}\right] = 452$$

$$\left[\frac{8819}{13}\right] = 678$$

$$\left[\frac{8837}{7}\right] = 1262$$

$$\left[\frac{8861}{5}\right] = 1772$$

$$\left[\frac{8969}{19}\right] = 492$$

$$\left[\frac{8999}{11}\right] = 818$$

$$\left[\frac{9281}{5}\right] = 1856$$

$$\left[\frac{9341}{5}\right] = 1868$$

$$\left[\frac{9419}{11}\right] = 856$$

$$\left[\frac{9431}{5}\right] = 1886$$

$$\left[\frac{9437}{7}\right] = 1348$$

$$\left[\frac{9461}{5}\right] = 1892$$

$$\left[\frac{9629}{13}\right] = 740$$

$$\left[\frac{9677}{7}\right] = 1382$$

$$\left[\frac{9719}{7}\right] = 1388$$

$$\left[\frac{9767}{17}\right] = 574$$

$$\left[\frac{9857}{7}\right] = 1408$$

On Pseudoprime which are Product of Distinct Primes

三乙 高金美

Definition: A composite number n is called a pseudoprime if $n \mid 2^n - 2$.

We denote P(x) to be the number of pseudoprimes $\leqq x$ and let $P_k(x)$ denote the number of square-free pseudoprimes $\leqq x$ having k distinct prime factors.

Follow this definition, we shall prove the inequality $P_2(x) > \frac{1}{4} \log x$, and also estimations of $P_k(x)$ and P(x) from below. Finally, we prove that the series $\Sigma 1/P_n$, where P_n is the nth pseudoprime, is convergent.

Now we prove the following lemma

Lemma : If R is a natural number ≥ 2 and x is sufficiently large, then

$$P_{k+1}(x) \geqq P_k(\log x).$$

proof : Let n be a pseudoprime which is a product of $k \geq 2$ distinct odd primes. By a theorem of Zsigmondy[3], there exists a prime $P > n$ such that $P/2^{n-1}-1$ and $n-1/P-1$. Since n is an odd pseudoprime. By definition of pseudoprime, $n/2^n-2$ and n is odd, $n/2^{n-1}-1$, Thus $np/2^{n-1}-1$, …………(1)

On the other hand, np−1 divisible by n−1, since $n-1/p-1$ and $np-1 = n(p-1)+(n-1)$ Hence $n-1/np-1$ and since $2^{n-1}/2^{np-1}$ Thus by(1) we get $np/2^{np-1}-1$ ie, np is a pseudoprime which is a product of k+1 distinct odd primes. Next, we observe that if n and m are natural numbers $n \neq m$, and p,q are primes such that $p > n$, $q > m$, then $np \neq mq$. Suppose $np = mq$ and $p > n$ then p/m, hend $m \geq p$ and we get $m > n$. Similarly, if $q > m$ we also get $n > m$ this is a contradiction. Therefore $np \neq mq$ Thus, if n,m are distinct pseudoprimes having $k \geq 2$ distinct prime factors, np and mq are distinct, too.

From(1) $\quad p/2^{n-1}-1 \quad$ and $\quad 2^{n-1}-1 = (2^{\frac{n-1}{2}}-1)(2^{\frac{n-1}{2}}+1)$

Since $\quad 2^{\frac{n-1}{2}}-1 < 2^{\frac{n-1}{2}}+1$ and $p/2^{\frac{n-1}{2}}-1$ or $p/2^{\frac{n-1}{2}}+1$ Thus $p \leq 2^{\frac{n-1}{2}}-1$

or $p \leq 2^{\frac{n-1}{2}}+1$ Therefore $p \leq 2^{\frac{n-1}{2}}+1 < 2^{\frac{n}{2}} < e^{\frac{n}{2}}$, since $2^{\frac{n}{2}}-2^{\frac{n-1}{2}} = 2^{\frac{n-1}{2}}(2^{\frac{1}{2}}-1)$, n is a pseudoprime which is a product of $k \geq 2$ distinct odd primes, then $n > 5$, $\frac{n-1}{2} > 2$ Thus $2^{\frac{n-1}{2}} > 4$ Therefore $2^{\frac{n}{2}}-2^{\frac{n-1}{2}} > 1$ i,e, $2^{\frac{n}{2}} > 2^{\frac{n-1}{2}}+1$,

This, if $n \leqq \log x$ then $np < e^{\frac{n}{2}}\, n < e^{\frac{1}{2}\log x} \bullet \log x = x^{\frac{1}{2}} \log x < x$

$$\text{since} \quad \lim_{x \to \infty} \frac{\log x}{x^{\frac{1}{2}}} = \lim_{x \to \infty} \frac{\frac{1}{x}}{\frac{1}{2}x^{-\frac{1}{2}}} = \lim_{x \to \infty} \frac{1}{\frac{1}{2}x^{\frac{1}{2}}} = 0 \quad \text{so} \quad \log x < x^{\frac{1}{2}}$$

Hence, for every pseudoprime $n = P_1 \cdots\cdots P_k \leqq \log x$ there exists at least one pseudoprime $np = P_1 P_2 \cdots\cdots P_k P < x$ and for each pseudoprime $n, m, n \neq m$, the adequate pseudoprimes np and mq then $np = mq$, Therefore , the number of pseudoprimes $\leq x$ having k+1 distinct prime factors is more than the number of pseudoprimes $\leq \log x$ having R distinct prime factors ie,

$$P_{k+1}(x) \geqq P_k(\log x)$$

Theorem 1 : If $x \geqq 2^{22}-1$, then

$$P_2(x) > \frac{1}{4} \log x$$

proof : Let m be an odd number > 3, By Zsigmondy's Theorem [3] there exist prime numbers p and q such that

$$P/2^m-1 \text{ , } q/2^m+1 \text{ , } m/p-1 \text{ , } 2m/q-1 \cdots\cdots\cdots\cdots(2)$$

since p, q and m are odd, $p-1$ is even, $2m/p-1$. Further

$p/2^m-1$ and $2^m-1/2^{q-1}-1$ then $p/2^{q-1}-1$

$q/2^{2m}-1$ and $2^{2m}-1/2^{q-1}-1$ then $q/2^{q-1}-1$

Hence, by a theorem of J.H. Jeans [2], pq is a pseudoprime.

From above we get $pq/2^{2m}-1$ ie, $pq < 2^{2m}-1$

Thus, for every odd number $m > 3$ there exists a pseudoprime of the form pq and

$pq < 2^{2m} - 1$.

Let x be sufficiently large and m be the greatest odd number for which $2^{2m}-1 \leq x$, since for every $m > 3$ and m is an odd number, there exists, p, q such that pq is a pseudoprime.

Therefore if $2^{2m}-1 \leq x$ there are at least $(m-3)/2$ of pseudoprimes of the form pq less than x i,e, $P_2(x) \geq \frac{m-3}{2}$

We see that there are at least $(m-3)/2$ pseudoprimes pq, where p, q are primes satisfying (2), whereas there exist pseudoprimes pq not satisfying (2), for example :

$$17 \cdot 257 \ (17/2^8-1, 257/2^8+1)$$

$$23 \cdot 89 \ (23 \cdot 89 = 2^{11}-1)$$

At the same time for $m=11$, there are two pseudoprimes satisfying (2) namely 23.683 and 89.683. Thus if $x \geq 2^{22}-1$, we may write

$$P_2(x) \geq \frac{n-3}{2} + 3 > \frac{m+2}{2}$$

From above we know that m is the greatest odd number such that $2^{2m}-1 \leqq x$

Now $m+2 > m$ then

$$x < 2^{2(m+2)}-1 < 2^{2(m+2)} < e^{2(m+2)}$$

whence $2(m+2) > \log x$ i.e. $m+2 > \frac{1}{2} \log x$

then $P_2(x) > \frac{m+2}{2} > \frac{1}{4} \log x$

Hence the theorem is proved.

Remark : It may be shown that the inequalty,

$$P_2(x) > \frac{1}{4} \log x$$

holds for $x \geqq 1387$ but not for another x

$1 < x < 1387$

proof : Since $1387 = 19 \times 73$ and

$$73/2^9-1 \qquad 19/2^9-1, \qquad 9/73-1, \qquad 2\times 9/19-1$$

By Zsigmondy's theorem[3] and a theorem of J.H. Jeans[2] we know 1387 is a pseudoprime, now we want to find a pseudoprime which is less than 1387. In Theorem I if we choose $m=5$, $p=31$, $q=11$ then, we get

$$31/2^5-1 \qquad 11/2^5+1 \qquad 5/31-1 \qquad 2\times 5/11-1$$

Therefore $pq=31\times 11$ is a pseudoprime. And when $m=7$, $m=8$, we can't find a pseudoprime which is a product of two, distinct prime and less than 1387. Hence

$$P_2(x)\geq 2 \qquad \text{if } x\geq 1387$$

$$P_2(x)\geq 1 \qquad \text{if } x\geq 341$$

But when $x=341$ $\quad \frac{1}{4}\log x=\frac{1}{4}\log 341=\frac{1}{4}\times 5.832>1.4$

then $\quad P_2(x)>\frac{1}{4}\log x$ is not true gor $341\leq x<1387$

and since $\quad P_2(x)=0$ when $x<341$ such that

$$P_2(x)>\frac{1}{4}\log x \text{ is not true for } 1<x<341$$

Now we get a consequence if $1<x<1387$

$$P_2(x)>\frac{1}{4}\log x \quad \text{is not true}$$

Since $\quad x=1387 \qquad \frac{1}{4}\log x=\frac{1}{4}\times 7.236>1.8$

and $\quad P_2(x)\geq 2 \quad$ for $\quad x\geq 1387$

Hence $\quad P_2(x)>\frac{1}{4}\log x \quad$ holds for $\quad x\geq 1387$

Theorem 2 : If k is a natural number ≥ 2 and x is sufficiently large, then

$$P_k(x)>\frac{1}{4}\log_{k-1}x, \text{ where by}_k x \text{ denote the k times iteratd logarithm.}$$

proof : By Mathematical Induction the statement can be shown. From

Theorem I we know if $k=2$ then .

$P_2(x) > \frac{1}{4}\log x$ Therefore the statement is true for $k=2$, Now if the statement is true for $k=n$ ie

$$P_n(x) > \frac{1}{4}\log_{n-1} x \quad \text{then}$$

$$P_{n+1} \geq P_n(\log x) \quad (\text{by lemma})$$

$$> \frac{1}{4}\log_{n-1}(\log x) = \frac{1}{4}\log_n(x)$$

Hence if $k=n+1$ the statement is also true

Therefore the theorem is proved.

Theorem 3 : If k is a natural number and x is sufficiently large, then

$$P(x) > \frac{1}{4}\log\left\{x \prod_{n=1}^{k} \log_n x\right\}$$

proof : For sufficiently large x

$$P(x) > P_2(x) + P_3(x) + \cdots\cdots + P_{k+2}(x) \quad \text{whence}$$

by Theorem L $\quad P(x) > \frac{1}{4}\log x + \frac{1}{4}\log_2 x + \cdots\cdots + \frac{1}{4}\log_{k+1} x$

$$= \frac{1}{4}[\log x + \log_2 x + \cdots\cdots + \log_{k+1} x]$$

$$= \frac{1}{4}\log[x \cdot \log x \cdot \log_2 x \cdots\cdots \log_k x]$$

$$= \frac{1}{4}\log\left\{x \cdot \prod_{n=1}^{k} \log_n x\right\}$$

Finally we prove another result.

Theorem 4 : The series $\Sigma 1/P_n$, where P_n is the n-th pseudoprime, is convergent.

proof : Since P.Erdos [1] proved that for x sufficiently large,

$$P(x) < 2x \exp\{-\frac{1}{3}(\log x)^{\frac{1}{4}}\}$$

Now we let $x = P_n$, then $P(x) = n$ and

$$n < 2P_n \exp\{-\frac{1}{3}(\log P_n)^{\frac{1}{4}}\}$$

Since, $n < P_n$, we have

$$2P_n > n \exp\{\frac{1}{3}(\log P_n)^{\frac{1}{4}}\} > n \exp\{\frac{1}{3}(\log_n)^{\frac{1}{4}}\}$$

$$\frac{1}{P_n} < \frac{2}{n \exp\{\frac{1}{3}(\log_n)^{\frac{1}{4}}\}}$$

On the other hand, for large m $m^{\frac{1}{4}} > 4 \log m$

Since $\lim\limits_{m \to \infty} \dfrac{4 \log m}{m^{\frac{1}{4}}} = \lim\limits_{m \to \infty} \dfrac{4}{\frac{1}{4} m^{\frac{1}{4}}} = 0$

and thus for sufficiently large n, $(\log n)^{\frac{1}{4}} > 4 \log \log n$

Hence $\exp\{\frac{1}{3}(\log n)^{\frac{1}{4}}\} > \exp\{\frac{4}{3} \log \log n\}$

$$= (\log n)^{\frac{2}{3}}$$

Then $$\frac{1}{P_n} < \frac{2}{n(\log n)^{\frac{4}{3}}}$$

Since $\Sigma 2 / \{n(\log n)^{\frac{4}{3}}\}$ is convergent then $\Sigma \frac{1}{P_n}$ is convergent too.

該是卸下担子的時候了

陳清瑛

同樣的五月天氣，同樣的選擧熱潮，然而三百六十餘日已成過往雲煙了，多少令人緬懷的往事，興奮的日子，驕傲的時刻，焦急的期待，委屈的悲傷都悄悄地走了，正如它們悄悄地來。

學會是一個綜合性的社團，是一系的靈魂，對於它，我們共同有著太多的理想，太多的期許，太多的感情，所以，我們太願意爲它說幾句眞心話，做些眞心事，或許，因此招來若干人的不滿，但是，爲了它的成長茁壯，我們願意忍受著各種打擊，以那種苦行僧的精神。

負責一年的學會工作，它帶給我一些認識，或許是個人的偏見，但期望來者能儘量避免。

一、組織鬆散，行政效率低：理監事人數衆多，原可發揮極大之力量，我們也曾依各人興趣加以分組，期能分層負責，然而未臻理想，致一切工作大多由各股股長獨自奔勞，工作自然無法迅速達成預期目標。

二、學會爲該系各分子之當然社團，非全體組成分子均係志願加入者，因此，有部分同學不關心學會活動，缺乏整體合作精神。

三、陋規頗多，積習太深：學會中有若干「傳統性」不合理的規矩，經多年相襲，已成習慣，一時改之不易，阻礙工作之進展甚鉅。

四、學會工作無正式記錄可供參考，在有限之經費束縛下，一切活動之擧辦進行難免顧此而失彼，竟或捉襟見肘，我們相信一本完整的帳簿是最好的指南，所以，我們很願意，也很高興地將一年來的帳目細節移交下去，期能有助於來年的行政工作。

一年來的學會活動是多采的，是輝煌的，雖然，我們的播種並不夠多，但所結之實是令人驚訝的豐盛，這是數學系的榮耀，更是大家的光榮，讓我們將之獻予所有已畢業的系友和在校的各位。

康樂方面，上、下學期分別在劉宏泰、陳智信兩位同學負責下，頗有出色的表現，像一破傳統的「節目比賽」方式的迎新晚會；氣氛熱烈的象棋，橋牌班際賽；獲獎的全校聯合登山活動；浩蕩的系郊遊一獅頭山之旅，均是康樂股的心血結晶。音樂比賽和日前擧辦的送舊舞會與雞尾酒會，也在康樂股努力下一如往日地圓滿完成。

學術股由葉樹華同學擔當大任，另由蔡高太同學負責系刊編輯工作，在這兒，您們將會發現學術股不再是沉默的一個單位；演講會的擧辦，雖然參加人數不踴躍，但總算爲沙漠中開創一片綠洲，我們希望有人繼續給予苦心灌溉。系刊的革新偏勞薛昭雄老師不少。您可看到它以一副更新的面目出現—成熟且有深度，惟一可惜的是同

學們的習作太少，可謂美中不足。

體育方面是屬於豐收的，序幕的籃球賽，女子組打破多年來均敗於國文系隊之紀錄，最後雖仍屈居第三，但她們的表現却令人吐氣揚眉。排球賽在驚濤下賽完，男子組的蟬聯冠軍，得之不易，期望大家能繼續努力。校運成績是輝煌的，陳素換同學的標槍，黃滿足，莊榮恭、傅銘輝、蕭振才同學的四百接力均改寫校運紀錄，最爲燦爛。另陳素換、傅恒霖、張清約、莊榮恭同學的鐵餅、跳遠、跳高、百米、二百米冠軍。千六接力冠軍、大隊接力的亞軍，男子徑賽囊括冠軍，男、女田賽分奪亞軍等等，這一連串令人驚異的收穫與榮譽，使得他系黯然失色；男桌球隊以全勝的姿態奪得團體冠軍，隊員丁右松同學榮登單打鰲頭；棒球隊勇奪第四名，均屬不易，此外橄欖球、足球、游泳等比賽都有輝煌的成績，股長計恒敬同學的熱心負責是成功的一大要素。

最後，讓我們感謝前、後兩位系主任一康老師與范老師的大力支持，提供每次演講會所需的車馬費，與范主任答應給予的系刊付梓費用，更感謝薛老師不辭辛勞地、義務地爲我們聘請專家演講，暨負責系刊之革新與編輯，爲的是希望他所熱愛的母系能出人頭地，作爲一位系友的他，爲我們年輕的一代，所付出的心血，是我們所難以忘懷的。謝謝各位一年來對我的信任、期許與不變的支持，雖然，這菲薄的成績很難令各位滿意，也謝謝一年來幫忙推動工作的所有助教，同學與股長，尤其是那些默默爲學會貢獻力量者，假如這一年的學會工作尚有一、二可取之處，我們願意將這份榮譽獻予他們，那是他們應得的。

六十年度數學學會組織概況

常務理事：陳清瑛（三甲）

常務監事：紀嶸崧（四乙）

系刋主編：蔡高太（三乙）

康樂股長：劉宏泰（三甲）　陳智信（二甲）

體育股長：計恒敬（三甲）

文教股長：葉樹華（三乙）

總務股長：施學義（三乙）　江清宮（二甲）

衞生股長：周聯貞（三甲）

系館管理：周慶龍（三甲）　蔡子良（三乙）

　　　　　張盛林（二甲）　方忠和（二乙）

顧　問：薛昭雄博士

主　編：蔡高太

編　輯：吳家怡　葉樹華

　　　　戈文正　謝南端

　　　　高金美　林雲壽

理事：

李政貴　陳達增　季大明　（四甲）

許建志　陳文瑛　陳清瑛　（三甲）

黃和玲　賴惠花　蕭　月　（夜三）

施學義　羅振雄　黃光彩　（二乙）

黃堅志　林一民　張明洲　（一甲）

朱正宇　林茂仁　朱正康　（一丙）

劉旭東　吳家怡　沈堯培　（四乙）

蕭振才　陳丁進　師岱濤　（三乙）

蔡福富　張忠恕　蕭泰和　（二甲）

黃美華　張良才　吳佩霞　（夜二）

林　發　林進春　莊得財　（一乙）

程蓬生　施鵬程　王淑敏　（夜一）

監事：

鄒超塵（四甲）　紀嶸崧（四乙）

楊　揚（夜三）　張文忠（二甲）

蕭守正（一甲）　高芳振（一乙）

楊維邦（三甲）　蔡子良（三乙）

陳得發（二乙）　王堯世（夜二）

賴明聰（一丙）　章修璞（夜一）