證 明 指 南

Q：為什麼碰到證明題常不知如何下手?

A：主要原因通常是不注意定義. 即使是明顯的事實, 只要定義不會寫, 就必定無從下手.

Q：平時如何準備?

A：(1) 每個定義都要動手練習到能自己寫得出來. 這一步若省略掉, 不但自己不會證, 而且連書上的證明都將會讀不懂.

(2) 對書上的各個定理, 由定義先看出"到底要證什麼", 再弄清楚它的推導起點及終點. 簡單的題目到這一步就可以掌握得住怎麼證明了.

(3) 對較大的題目必須先分出段落及推導的中間點. 再把每個段落當做一個小題目像(2)一樣處理. "綜合線性代數"裡的證明段落很明顯, 讀一段時期後就可以體會出證明的模式都差不多. 這時再去看別的書就有能力從一大堆看來好像很亂的文字裡抓出它的結構.

(4) 以上的(2)(3)只是讀法而已, 讀懂之後還要自己動手練習證. 初學者的表達能力通常都是一團糟而不自知, 一定要動手才會發現自己還有很多地方有困難. 這些困難若是留到進考場才發現就太遲了.

(5) 一般人心裡想的和寫出來的往往不一致, 而且自己還不知道. 要請別人檢查才會發現, 也才能注意改正而不致冤枉失分.

Q：這樣準備要花掉太多時間, 有沒有速成的應考法?

A：俗語說"欲速則不達", 其實這是最快的方法, 而且花的時間沒有想像中那麼多. 剛開始確實是很慢, 但這是不可避免的基礎工程. 只要基礎穩固, 學習速度會越來越快. 等練習一段時期把證明模式摸熟後, 就有能力把小題目(及大題目的小段)的證明用心算完成. 一般人心急, 火候還不到就想只用眼睛做題目, 這樣當然是越讀越不懂. 試想, 在連寫出來都還不太對的程度時, 不動手怎麼能學得好? 而線代的前後相關又很重, 前面只是不太清楚, 到後面就一團糟了. 一般同學所以會失敗就是

這樣. 其實學證明不難, 按步就班而已. 越“笨”的人越容易學得好.

Q：這一回講義的主題是什麼?

A：列出一些學證明用得到, 但一般學生卻不太清楚的基本知識. 這些知識在離散數學的代數結構部份尤其常用.

§1．應考邏輯

學習邏輯的目地有二: (1) 對平常使用直覺的證明過程由“知其然”進步到“知其所以然”, (2) 能進一步掌握思緒較複雜的證明(尤其在矛盾証法). 本節所述並未達到數理邏輯(Mathematical Logic)的嚴密度, 但已足夠供數學證明使用. 學習時應該建立直覺, 不要只注重格式. 也就是要“直覺為主, 格式為輔”.

【要點１】**邏輯式與邏輯運算**

① 邏輯式(*formula*): 是一個可以明確判定真(true;Ｔ;正確;成立),假(false;Ｆ;偽;錯誤;不成立) 的式子. 通常邏輯式p一寫出來, 就是在宣告“p成立”. 但這個宣告未必正確. 例如邏輯式“$2\geq 3$”就是錯的.

② 我們可利用邏輯運算(*junction*, 或稱*sentential connective*)$\neg,\wedge,\vee,\rightarrow,\leftrightarrow$, 由簡單的式子逐步建構出複雜的式子:

否定(negation): “$\neg p$”表示“非p”.

連接(conjuntion): “$p\wedge q$”表示“p且q”.

選擇(disjuntion): “$p\vee q$”表示“p或q”.

條件式(conditional): “$p\rightarrow q$”表示“若p則q”, 也就是“由p推得(imply)q”, 又可寫作“$q\leftarrow p$”. 有的書將“$\rightarrow$”記為“$\supset$”.

雙條件式(biconditional,或稱雙如言): “$p\leftrightarrow q$”表示“p等價於(iff; if and only if; be equivalent to) q”.

③ 只使用$\neg,\wedge,\vee,\rightarrow,\leftrightarrow$的邏輯系統稱為命題邏輯(*propositional logic*).

[說明] (1) 邏輯運算的真值表(*truth table*)規定如下:

p	q	$\neg p$	$p\wedge q$	$p\vee q$	$p\to q$	$p\leftrightarrow q$
F	F	T	F	F	T	T
F	T	T	F	T	T	F
T	F	F	F	T	F	F
T	T	F	T	T	T	T

(2) 邏輯式“$p\vee q$”表示“要就p成立, 不然就q成立”, 只要p, q中有一個成立, $p\vee q$就成立. 只有在p和q都不成立時, $p\vee q$才不成立.

(2) 邏輯式“$p\wedge q$”表示“既p成立又q成立”, 它要求p和q都要成立. 只要p, q中有一個不成立, $p\wedge q$就不成立.

(3) 邏輯式“$p\to q$”之中, p稱為前提(*antecedent*), q稱為結語(*consequent*).
注意此式在“結語正確”時成立; 在“前提錯誤”時成立; 只有在“正確的前提推到錯誤的結語”時才不成立.
有許多同學常將$p\to q$的情況誤寫為$p\wedge q$. 應注意分辨.

(4)“且”和“或”常會被簡記為“,”, 這時可由上下文依習慣用法判定是那一個. 例如
$\{\,5x \mid x=1,2,3\,\}$ 的逗點是表示“或”.
$\{\,(x, y) \mid x+y=1\,,\, x-y=4\,\}$ 後面的逗點是表示“且”.

(5) “$p\leftrightarrow q$”相當於“$(p\leftarrow q)\wedge(p\to q)$”.

(6) 一個式子內含許多個連接詞時, 為避免混淆(ambiguous), 應加上括號.
例如 “$(p\wedge q)\vee r$”與“$p\wedge(q\vee r)$”並不相同.

(7) 習慣上規定$\neg$的優先權高於其他符號. 所以“$(\neg p)\to q$”可簡寫為“$\neg p\to q$”.

(8) 由$\wedge$和$\vee$的結合律(見要點4), “$(p\wedge q)\wedge r$”和“$p\wedge(q\wedge r)$”都簡寫為“$p\wedge q\wedge r$”; “$(p\vee q)\vee r$”和“$p\vee(q\vee r)$”都簡寫為 “$p\vee q\vee r$”.
還有, $\wedge$和$\vee$通常也優先於$\to$和$\leftrightarrow$.

[例1.1] 我們考慮這句競選承諾:

"若我當選縣長, 就發放老人年金."

如果這個候選人當選, 而也發了年金, 顯然前述承諾已履行.

如果這個候選人沒當選, 則無論年金是否發放, 都不算違背前述承諾.

只有在這個候選人當選而卻沒發年金的情況下, 前述承諾才變成是謊言.

[習題1.1] 利用真值表驗証"$(p\leftarrow q)\wedge(p\rightarrow q)$"與"$p\leftrightarrow q$"相同.

[習題1.2] 利用真值表驗証"$\neg(\neg p\wedge\neg q)$"與"$p\vee q$"相同.

【要點２】**邏輯量號**

① 量號(*quantifier*) : 用來描述式子內變元(*variable*)的屬性.

(a) "$\forall x\, p(x)$"表示"<u>對每個</u>(for all; for each) x, $p(x)$都成立".

(b) "$\exists x\, p(x)$"表示"存在(there exist) x使$p(x)$成立". 也就是"<u>有某個</u>(there is a) x 使$p(x)$成立". 數學上常說成"$p(x)$中的x具有存在性".

(c) "$!\, x\, p(x)$"表示"滿足$p(x)$的x最多只有一個(unique)", 數學上常說成"$p(x)$中的x具有唯一性".

"$!\, x\, p(x)$"相當於"$\forall u,v,\ ((p(u)\wedge p(v))\ \rightarrow\ (u=v))$".

(d) "$\exists\, !\, x\, p(x)$"相當於"$(\exists x\, p(x))\wedge(!\, x\, p(x))$", 表示"滿足$p(x)$的$x$恰有一個(unique)". 數學上常說成 "$x$具有存在性及唯一性".

②量號縮寫法:

(a) 在數學上常將"$\forall x\, p(x)$"簡寫爲"$p(x)$".

(b) "$\exists x\ (x\in A\ \wedge\ p(x))$"簡寫爲 "$\exists x\in A, p(x)$"

(c) "$\forall x\ (x\in A\rightarrow p(x))$"簡寫爲"$\forall x\in A, p(x)$", 也可簡寫爲"$x\in A\ \rightarrow\ p(x)$"

③使用$\neg,\wedge,\vee,\rightarrow,\leftrightarrow,\forall,\exists$的邏輯系統稱爲述詞邏輯(*predicate logic*).

[說明] (1) 數學書通常不直接使用$\neg,\wedge,\vee,\rightarrow,\leftrightarrow,\forall,\exists,!$這些符號, 而是用文字描述. 符號"!"尤其少見, 應避免使用. 但我們在閱讀時必須特別注意這些邏輯上的關鍵字.

(2)“存在”是說“至少有一個”，“唯一”是說“最多只有一個”，“存在唯一”就是“(不多不少)恰有一個”. 雖然唯一性常常和存在性一起討論，但唯一並不保證存在.

(3) “There is a ...”只是說“有至少一個”並不含“唯一”的意思. “There is an unique ...”才是“存在唯一”.

(4)“使得(such that)”常接在“∃-子句”之後作爲文字敘述上的連接詞. 它在邏輯上沒有意義，只用來使語氣通順.
有許多學生把such that誤認爲→. 這是嚴重錯誤，要特別注意.

(5)“$\forall x\, p(x)$”也常說成“對任意(*for any*) x, $p(x)$都成立”.
初學者常把“對任意”誤認成“任意(*arbitrary*)”.
請注意任意只是表示不特定，它常被用在口語的存在性敘述中，但並非邏輯術語. 無論有沒有arbitrary這個字，存在量號所描寫的變元都不是特定的.

(6) ∀是∧的推廣，例如
“ $a>0\wedge b>0\wedge c>0\wedge d>0$ ”可改寫成“ $\forall x\in\{a,b,c,d\},\quad x>0$ ”.

(7) ∃是∨的推廣. 例如
“ $a>0\vee b>0\vee c>0\vee d>0$ ”可改寫成“ $\exists x\in\{a,b,c,d\},\quad x>0$ ”.

◎[例2.1]

數學上被量號所描述的變數常帶著“變動範圍(*universe*)”. 例如

$\exists x\in\mathbb{Z},\quad x+7=6$.

讀做“存在屬於$\mathbb{Z}$的x,(使得)$x+7=6$(成立)”.

帶著變動範圍的敘述方式其實是一種簡寫. 上式相當於

$\exists x, (x\in\mathbb{Z}$ 且 $x+7=6)$.

◎[例2.2]

$\forall x, (\, x\in\mathbb{N} \;\rightarrow\; x\leq 2x\,)$.

可以利用帶著變動範圍(*universe*)的方式簡寫爲

$\forall x\in\mathbb{N}\ , x\leq 2x$.

讀做“對每個屬於$\mathbb{N}$的x, $x\leq 2x$(必成立)”.

◎[例2.3]

字面上的“∀子句”若不帶著變動範圍, 通常就被省略. 　例如

$\forall x\,(\, x\in\mathbb{N} \;\to\; x\leq 2x\,)$

可以簡寫成

$x\in\mathbb{N} \;\to\; x\leq 2x$ 　.

由⑦可以發現 ︰帶著變動範圍的“∀-子句”相當於一個條件句的前提.

[習題2.1] 對函數$f：A\longrightarrow B$, 試將下列敘述改用量號寫出:

“每個B中的元素b都是某個A中元素a的像點”.

[習題2.2] 對函數$f：A\longrightarrow B$, 及B中的元素b, 試將下列敘述改用量號寫出:

“A中最多只能有一個元素對映到b”.

【要點３】**邏輯關係**

爲了證明的需求, 我們還要考慮兩個邏輯式之間的關係:

① 可推得(*logically imply*)

若“$p\to q$”對所有真假值都得出T, 就說p推得q. 這種情況記爲“ $p \Longrightarrow q$ ”, 也常寫成 “ $q \Longleftarrow p$”. 有的書記爲 “ $p \vDash q$ ” .

② 等價(*logically equivalent*)

若邏輯式“$p\leftrightarrow q$”對所有真假值都得出T, 就說p等價於q. 這種情況記爲 “ $p \Longleftrightarrow q$ ” 有的書記爲 “ $p \equiv q$ ”

[說明] (1) “$p\to q$”與“$p \Longrightarrow q$”意思大致相同但用法不同.

這兩句話都是“若p則q”, 但前者是由邏輯式p和q在同一層次造出一個新的邏輯式“$p\to q$”. 這個新式子可能爲真, 也可能爲假, 要依p,q的真假來判定. 至於後者是在描述邏輯式p和邏輯式q之間的關係. 當“$p\to q$”恆爲真時, 才說“$p \Longrightarrow q$”.

“$p \Longrightarrow q$”的層次高過p和q, 它已經不是一個邏輯式了.

(2) “$p\leftrightarrow q$”與“$p \Longleftrightarrow q$”也是意思大致相同但用法不同. 情況和(1)一樣.

(3) 由真值表觀察, “$p \Longleftrightarrow q$”表示p的行和q的行中各列都相同.

“$p \Longrightarrow q$”表示p的行和q的行中, 若某列p是T, 則q也是T.

(4) $\Longrightarrow$ 的用法並不統一. 清大73年資科所的考題曾將→寫成$\Longrightarrow$.

(5) 當 “$p \Longrightarrow q$”和“$q \Longrightarrow r$”都成立時, 常合併寫爲“$p \Longrightarrow q \Longrightarrow r$”.

當“$p \Longleftrightarrow q$”和“$q \Longleftrightarrow r$”都成立時, 常併爲“$p \Longleftrightarrow q \Longleftrightarrow r$”.

(6) 大部份的定理以“$p \Longrightarrow q$”的型態呈現. p稱爲已知, q稱爲求證.

(7) 型如“$p \Longrightarrow q$”的定理. q變強則定理變強, p變強則定理變弱. (見例3.2)

[例3.1] 觀察下列的真值表:

p	q	$p\to q$	$(p\to q)\wedge p$	$((p\to q)\wedge p)\to q$
F	F	T	F	T
F	T	T	F	T
T	F	F	F	T
T	T	T	T	T

因“$((p\to q)\wedge p)\to q$”恆真, 所以說“$((p\to q)\wedge p) \Longrightarrow q$”

再觀察下列的真值表:

p	q	$p\to q$	$(p\to q)\wedge q$	$((p\to q)\wedge q)\to p$
F	F	T	F	T
F	T	T	T	F
T	F	F	F	T
T	T	T	T	T

因“$((p\to q)\wedge q)\to p$”並不恆真, 所以“$((p\to q)\wedge q) \Longrightarrow p$”不成立.

[例3.2] ([說明7]的實例)

考慮下列敘述: “若考上研究所, 則贈送獎金五千元”.

設 p=“考上研究所”, q=“贈送獎金五千元”

設 p'=“考上研究所榜首”, q' =“贈送獎金五千元及音響一套”

p'比p強, q'比q強. 原敘述爲“ $p \Longrightarrow q$ ”.

“ $p \Longrightarrow q'$ ”比原敘述強. (成效變強)

“ $p' \Longrightarrow q$ ”比原敘述弱. (條件變成不容易達成)

[習題3.1]

利用真值表證明 $p\wedge(q\wedge r) \Longleftrightarrow (p\wedge q)\wedge r$.

【要點４】基本運算性質

①交換律： $p\wedge q \Longleftrightarrow q\wedge p$;　$p\vee q \Longleftrightarrow q\vee p$

②結合律： $(p\wedge q)\wedge r \Longleftrightarrow p\wedge(q\wedge r)$;　$(p\vee q)\vee r \Longleftrightarrow p\vee(q\vee r)$

③分配律： $p\wedge(q\vee r) \Longleftrightarrow (p\wedge q)\vee(p\wedge r)$;

$p\vee(q\wedge r) \Longleftrightarrow (p\vee q)\wedge(p\vee r)$

④遞移律： $(p\rightarrow q)\wedge(q\rightarrow r) \Longrightarrow (p\rightarrow r)$

⑤ $\forall x\, \forall y\, p(x, y) \Longleftrightarrow \forall y\, \forall x\, p(x, y)$　　(見例4.1)

此式常簡寫成“ $\forall x, y, p(x, y)$ ”

⑥ $\exists x\, \exists y\, p(x, y) \Longleftrightarrow \exists y\, \exists x\, p(x, y)$

此式常簡寫成“$\exists x, y, p(x, y)$ ”

*⑦ $\forall x, (p(x)\wedge q(x))$

$\Longleftrightarrow (\forall x, p(x))\wedge(\forall x, q(x))$

$\Longleftrightarrow (\forall x, p(x))\wedge(\forall y, q(y))$

*⑧ $\exists x, (p(x)\vee q(x))$

$\Longleftrightarrow (\exists x, p(x))\vee(\exists x, q(x))$

$\Longleftrightarrow (\exists x, p(x))\vee(\exists y, q(y))$

[說明] (1) $p \to q$ 與 $q \to p$ 不同.

(2) $(p \wedge q) \vee r$ 與 $p \wedge (q \vee r)$ 不同 (比較真值表即知)

$(p \vee q) \wedge r$ 與 $p \vee (q \wedge r)$ 不同 (比較真值表即知)

(3) $(p \to q) \to r$ 與 $p \to (q \to r)$ 不同 (比較真值表即知)

(4) 如前所述, "$p \Longrightarrow q \Longrightarrow r$" 只是表示 "$p \Longrightarrow q$" 和 "$q \Longrightarrow r$" 都成立.

"$(p \Longrightarrow q) \Longrightarrow r$" 無意義. "$p \Longrightarrow (q \Longrightarrow r)$" 也無意義.

(5) $\forall x \exists y$與$\exists y \forall x$不同.

前者的y與x有關, 只適用於已固定住的x, 因此常將這種y記爲y_x或$y(x)$.

後者的y獨立於x, 適用於一切未定的x. (見例4.2)

因此後者較強, 亦即 $(\exists y, \forall x, p(x)) \Longrightarrow (\forall x, \exists y, p(x))$.

同理, $\exists x \forall y$與$\forall y \exists x$不同, 前者較強.

(6) 邏輯式 $(\forall x, p(x)) \wedge (\forall x, q(x))$ 中第一個$\forall x$的語意區(*scope*)只到$(\forall x, p(x))$爲止. $(\forall x, q(x))$的x和前面毫不相干.

† (7) $\forall x, (p(x) \vee q(x))$ 與 $(\forall x, p(x)) \vee (\forall x, q(x))$ 不同, 後者較強. (見例4.3)

† (8) $\exists x, (p(x) \wedge q(x))$ 與 $(\exists x, p(x)) \wedge (\exists x, q(x))$ 不同, 前者較強. (見例4.4)

[例4.1] (⑤的實例)

(a) 下列三式在$x, y \in \mathbb{R}$時都成立.

(i) $\forall x, \forall y, xy=yx$

(ii) $\forall y, \forall x, xy=yx$

(iii) $\forall x, y, xy=yx$

(b) 在2×2矩陣考慮時, 這三式都不成立. (見綜線CH2範例5)

例如

$$\begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 4 & 5 \\ 6 & 7 \end{bmatrix} \neq \begin{bmatrix} 4 & 5 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}$$

$\exists x, \exists y, xy=yx$ 當然成立.

$\forall x, \exists y, xy=yx$ 也成立. (y取零矩陣即可)

甚至 $\exists x, \forall y, xy=yx$ 仍成立. (x取零矩陣即可)

[例4.2]

(1) “ $\forall x\in\mathbb{R}, \exists y\in\mathbb{R}, x+y=0$ ” 成立. (取$y=-x$即可)

“ $\exists y\in\mathbb{R}, \forall x\in\mathbb{R}, x+y=0$ ” 不成立.

(2) “ $\exists z\in\mathbb{R}, \forall x\in\mathbb{R}, z+x=x$ ” 成立. (取$z=0$即可)

“ $\forall x\in\mathbb{R}, \exists z\in\mathbb{R}, z+x=x$ ” 當然也成立. (取$z=0$即可)

(3) 設$\mathscr{A}=\{\{1\},\{2\},\{1,2\}\}$,

“ $\exists X\in\mathscr{A}, \forall Y\in\mathscr{A}, Y\subseteq X$ ” 成立. (取$X=\{1,2\}$即可)

“ $\forall Y\in\mathscr{A}, \exists X\in\mathscr{A}, Y\subseteq X$ ” 成立. (取$X=\{1,2\}$即可)

“ $\exists X\in\mathscr{A}, \forall Y\in\mathscr{A}, X\subseteq Y$ ” 不成立.

“ $\forall Y\in\mathscr{A}, \exists X\in\mathscr{A}, X\subseteq Y$ ” 成立. (取$Y=X$即可)

(4) 設$A=\{t\in\mathbb{R} \mid 1\le t<2\}$,

“ $\exists x\in A, \forall y\in A, x\le y$ ” 成立. (取$x=1$即可)

“ $\forall y\in A, \exists x\in A, x\le y$ ” 成立. (取$x=1$即可)

“ $\exists x\in A, \forall y\in A, y\le x$ ” 不成立. (A中沒有最大元素)

“ $\forall y\in A, \exists x\in A, y\le x$ ” 成立. (取$x=y$即可)

“ $\forall y\in A, \exists x\in A, y<x$ ” 仍成立. (取$x=(y+2)/2$即可)

(5) $\lim\limits_{n\to\infty} f(n)=l$ 的定義為: $\forall\varepsilon>0, \exists K\in\mathbb{N}, \quad n>K \Longrightarrow |f(n)-l|<\varepsilon$

† [例4.3]

(1) “每個人都出國或考研究所”和“每個人都出國或每個人都考研究所”並不相同, 後者較強.

(2) 對集合$A=\{-1, 7, 9\}$,

“$\forall x\in A, ((x>0)\vee(x<0))$”成立, 但“$(\forall x\in A, x>0)\vee(\forall x\in A, x<0)$”不成立. 另外,

“$\forall x\in A, ((x>10)\vee(x<10))$”和“$(\forall x\in A, x>10)\vee(\forall x\in A, x<10)$”都成立.

† [例4.4]

(1)“有人既喜歡數學又喜歡英文”和“有人喜歡數學而且有人喜歡英文”並不相同，前者較強.

(2) 在實數系,“$(\exists x, x>0)\wedge(\exists x, x<0)$”成立, 但“$\exists x, (x>0)\wedge(x<0)$”不成立. 另外,“$(\exists x, x\geq 0)\wedge(\exists x, x\leq 0)$”和“$\exists x, (x\geq 0)\wedge(x\leq 0)$”都成立.

[習題4.1] 試由真值表證明分配律

[習題4.2] 試比較 $(p\wedge q)\vee r$ 與 $p\wedge(q\vee r)$

[習題4.3] 試由真值表比較 $(p\rightarrow q)\rightarrow r$ 與 $p\rightarrow(q\rightarrow r)$

◎【要點５】否定法

① $\neg(\neg p) \Longleftrightarrow p$

② $\neg(p\rightarrow q) \Longleftrightarrow p\wedge\neg q$

③ $\neg(p\leftrightarrow q) \Longleftrightarrow p\leftrightarrow\neg q$

④ $\neg(p\wedge q) \Longleftrightarrow \neg p\vee\neg q$

⑤ $\neg(p\vee q) \Longleftrightarrow \neg p\wedge\neg q$

⑥ $\neg(\forall x, p(x)) \Longleftrightarrow \exists x, \neg p(x)$

⑦ $\neg(\exists x, p(x)) \Longleftrightarrow \forall x, \neg p(x)$

[說明] (1) ①–⑤可用真值表驗證. ④–⑦稱為 De Morgan's rule. 其中⑥式是④式的推廣; ⑦式是⑤式的推廣.

(2) ②,⑥是 "舉反例" 的基本原理.

(3) ⑥式含有變動範圍時為:

$$\neg(\forall x\in A, p(x)) \Longleftrightarrow \exists x\in A, \neg p(x)$$

⑦式含有變動範圍時為:

$$\neg(\exists x\in A, p(x)) \Longleftrightarrow \forall x\in A, \neg p(x)$$

特別注意:否定是對同一群對象在做否定, 所以變動範圍不可改變.

或者我們也可以證明如下:

$$\neg(\forall x\in A, p(x))$$
$$\Longleftrightarrow \neg(\forall x, x\in A\to p(x))$$
$$\Longleftrightarrow \exists x,\ \neg(x\in A\to p(x))$$
$$\Longleftrightarrow \exists x, (x\in A \text{ 且 } \neg p(x))$$
$$\Longleftrightarrow \exists x\in A, \neg p(x)$$

[例5.1]

“既考不好又常翹課”的否定是“考得好或不常翹課”　.....④

“每個學生都用功”的否定是“有的學生不用功”　..........⑥

“惡有惡報”的否定是“惡而不受惡報”　...............②

“不是不報”相當於“報”　.............................①

[例5.2] (參閱綜線CH6定義9)

向量x, y, z“線性相關”:

$\exists$不全爲零的a,b,c; $ax+by+cz=o$

否定後變成:

$\forall$不全爲零的a,b,c; $ax+by+cz\neq o$

(注意到“不全爲零”是變動範圍, 做否定時不改)

也就是:

a,b,c不全爲零　$\to$　$ax+by+cz\neq o$

換成逆否命題(見要點6):

$ax+by+cz=o$　$\to$　a,b,c全爲零

這就是“線性獨立”的定義.

[例5.3]

“$\forall x,\exists y, p(x, y)$” 的否定是

“$\exists x,\neg(\exists y, p(x, y))$”, 也就是“$\exists x,\forall y,\neg p(x, y)$”

[習題5.1] Prove or disprove the following statement.

For square matrix A, if $A^2=O$, then $A=O$. (hint:②)

[習題5.2] “$\exists x,\forall y, p(x, y)$”的否定是什麼?

[習題5.3] “ $\forall u\neq o,\exists v$, 使$f(u,v)\neq o$ ”的否定是什麼? (參閱綜線CH10定理22)

◎【要點６】若**p**則**q**的變形

① $p\rightarrow q$ (也就是$q\leftarrow p$) 有下列重要的等價變形:

$p\rightarrow q \iff \neg q\rightarrow\neg p$

$p\rightarrow q \iff \neg p\vee q \iff \neg(p\wedge\neg q)$

② 下列各敘述是同一回事 :

(ⅰ) $p \Longrightarrow q$ (p implies q.)

(ⅱ) $q \Longleftarrow p$ (q is implied by p.)

(ⅲ) $\neg q \Longrightarrow \neg p$

(ⅳ) $\neg p$或q(至少)有一個成立

(ⅴ) p和$\neg q$不能都成立

(ⅵ)若p則q (If p, then q.) (q if p.)

(ⅶ) p只在q成立時才可能成立. (p only if q.)

(換句話說: q不成立時p必定也不成立)

(ⅷ) p是q的充份條件 (p is a *sufficient condition* of q.)

(ⅸ) q是p的必要條件 (q is a *necessary condition* of p.)

[說明] (1) “$p\rightarrow q$”與“$\neg q\rightarrow\neg p$”互稱爲逆否命題(contraposition), 或對偶命題.

(2) 助憶口訣:

充份條件是“理由”, 必要條件是“結論”.

“if-子句”是“理由”, “only-if-子句”是“結論”.

(3) $p \Longrightarrow q$ 是說p成立時q一定要成立.

我們對p加以討論:

在p不成立的情況下，$\neg p$成立; 在p成立的情況下, q成立.
所以$\neg p,q$兩個中至少有一個成立, 也就是$(\neg p$或$q)$成立.

[例6.1]

下列各敘述是同一回事 :

(ⅰ) $x>1 \Longrightarrow x^2>1$　($x>1$ implies $x^2>1$.)

(ⅱ) $x^2>1 \Longleftarrow x>1$　($x^2>1$ is implied by $x>1$.)

(ⅲ) $\neg(x^2>1) \Longrightarrow \neg(x>1)$

(ⅳ) $\neg(x>1)$或$x^2>1$ (至少)有一個成立

(ⅴ) $x>1$和$\neg(x^2>1)$不能都成立

(ⅵ)若$x>1$則$x^2>1$　(If $x>1$, then $x^2>1$.) ($x^2>1$ if $x>1$.)

(ⅶ) $x>1$只在$x^2>1$成立時才可能成立.　($x>1$ only if $x^2>1$.)

(換句話說: $x^2>1$不成立時$x>1$必定也不成立)

(ⅷ) $x>1$是$x^2>1$的充份條件　($x>1$ is a *sufficient condition* of $x^2>1$.)

(ⅸ) $x^2>1$是$x>1$的必要條件　($x^2>1$ is a *necessary condition* of $x>1$.)

[例6.2]

下列各敘述是同一回事 :

(ⅰ) 下雨 $\Longrightarrow$ 路溼　(下雨 implies 路溼.)

(ⅱ) 路溼 $\Longleftarrow$ 下雨　(路溼 is implied by 下雨.)

(ⅲ) 路沒溼 $\Longrightarrow$ 沒下雨

(ⅳ) 沒下雨或路溼(至少)有一個成立

(ⅴ) 下雨和路沒溼不能都成立

(ⅵ) 若下雨則路溼 (If 下雨, then 路溼.) (路溼 if 下雨.)

(ⅶ) 只在路溼的情況下才可能有下雨.　(下雨 only if 路溼.)

(換句話說: 路沒溼時必定沒下雨)

(ⅷ) 下雨是路溼的充份條件　(下雨 is a *sufficient condition* of 路溼.)

(ⅸ) 路溼是下雨的必要條件　(路溼 is a *necessary condition* of 下雨.)

[習題6.1] 證明①

[習題6.2] 仿①寫出 $\neg p \to q$ 的各種等價變形:

【要點７】證明格式

證明 $p \Longrightarrow q$ (已知p, 求證q) 的方法：

①順向證法：由 p 逐步推導出 q

②逆向證法：由 $\neg q$ 逐步推導出 $\neg p$

③夾攻證法：由 p且$\neg q$ 逐步推導出矛盾

[說明] (1) 順向證法通稱為直接證法, 夾攻證法和逆向證法都叫做間接證法, 或矛盾證法. 遇到題目通常是用順向證法開始想, 若不行再試逆向證法. 若還是不行才試夾攻證法.

(2) 逆向證法由要點6②(ⅲ)產生.

(3) 夾攻證法由要點6②(ⅴ)產生.

[例7.1] 若方陣A, B都是對稱矩陣, 求證$A+B$也是對稱矩陣.

證法一：(參看綜合線性代數CH2定義25①)

$(A+B)^{\mathrm{T}}=A^{\mathrm{T}}+B^{\mathrm{T}}$ (綜線CH2定理23)

$=A+B$ ($\because$ $A=A^{\mathrm{T}}$, $B=B^{\mathrm{T}}$)

$\therefore$ $A+B$ 是對稱矩陣.

證法二：(參看綜合線性代數CH2定義22①)

設 $A=[\,a_{\mathrm{ij}}\,]$, $B=[\,b_{\mathrm{ij}}\,]$, $A+B=[\,c_{\mathrm{ij}}\,]$.

則 $\forall i, j$, $c_{\mathrm{ij}}=a_{\mathrm{ij}}+b_{\mathrm{ij}}$. (綜線CH2定義3)

$\forall\, i, j$ $c_{\mathrm{ji}}=a_{\mathrm{ji}}+b_{\mathrm{ji}}$

$=a_{\mathrm{ij}}+b_{\mathrm{ij}}$ ($\because$ A, B都對稱)

$=c_{\mathrm{ij}}$

$\therefore$ $A+B$ 是對稱矩陣.

[例7.2] 對方陣A, 若A正定, 求證A可逆. 　(參閱綜線CH10定理23)

證: (用逆向證法)

若 A不可逆,

則 存在向量$v\neq o$, 使 $Av=o$ 　(綜線CH8定理17)

$\therefore$ $v^{\mathrm{H}}Av=0$

$\therefore$ A 不爲正定 　(綜線CH10定義19)

[例7.3] 對方陣A, 設 adj$A$ 可逆, 求證A可逆. 　(參閱綜線CH4定理17)

證: (用夾攻證法)

若adj$A$可逆,但A不可逆,

則 $A\,\mathrm{adj}A = (\det A)I$ 　(綜線CH4定理17①)

$= 0\,I = O$ 　(綜線CH4定理17②)

$\therefore$ $A = O\,(\mathrm{adj}A)^{-1} = O$ 　(上式兩邊同乘$(\mathrm{adj}A)^{-1}$)

$\therefore$ $\mathrm{adj}A = O$ 　(綜線CH4定義16)

$\therefore$ adj$A$ 不可逆, 此爲矛盾.

◎【要點８】等價的變形

下列各敘述是同一回事 :

(ⅰ) $p \Longleftrightarrow q$ 　(p,q等價)

(ⅱ) "$p \Longrightarrow q$" 而且 " $p \Longleftarrow q$"

(ⅲ) $q \Longleftrightarrow p$

(ⅳ) p is equivalent to q. 　(p等價於q)

(ⅴ) p if and only if q. 　(p若且唯若q)

(ⅵ) p is a necessary and sufficient condition of q. 　(p是q的充份必要條件)

[說明] (1) "充份必要條件" 簡稱爲 "充要條件" .

(2) “if and only if”簡記爲“iff”.

中文裏沒有對應的詞，勉強譯做“若且唯若”.

(3) 要證明 “$p \Longleftrightarrow q$” 就是要分兩段證明“$p \Longrightarrow q$” 以及“$p \Longleftarrow q$”.

這兩段再各別利用要點7選則合適的證法. 有時候這兩段還可以合併起來.

【要點９】多式等價的意義

下列各敘述是同一回事：

(ⅰ) p, q, r 等價(equivalent)

(ⅱ) “$p \Longleftrightarrow q$” 且 “$q \Longleftrightarrow r$” 且 “$r \Longleftrightarrow p$”

(ⅲ) “$p \Longrightarrow q$” 且 “$p \Longrightarrow r$” 且 “$q \Longrightarrow p$”

且“$q \Longrightarrow r$” 且 “$r \Longrightarrow p$” 且 “$r \Longrightarrow q$”

[習題9.1] 寫出 “p, q, r, s等價”的各種同義的說法.

【要點１０】多式等價的證明格式

以下列出多種證明“p, q, r等價”的方法：

“直線型1”：分別證明 ① $p \Longleftrightarrow q$, ② $q \Longleftrightarrow r$,

“直線型2”：分別證明 ① $p \Longleftrightarrow r$, ② $r \Longleftrightarrow q$

“直線型3”：分別證明 ① $q \Longleftrightarrow p$, ② $p \Longleftrightarrow r$

“繞圈型1”：分別證明 ① $p \Longrightarrow q$, ② $q \Longrightarrow r$, ③ $r \Longrightarrow p$

“繞圈型2”：分別證明 ① $p \Longrightarrow r$, ② $r \Longrightarrow q$, ③ $q \Longrightarrow p$

[說明] (1) 把 p,q,r 看成點，把→看成單行道，證明等價就是要把交通網建好，

讓每一點都能直接或間接通到任何其他點.

(2) 解題時依各點之間的"天然距離"來決定採用那一型.

(3) 直線型1常再變成分別證明 ① $p \Longrightarrow q$, ② $q \Longrightarrow p$,
③ $q \Longrightarrow r$,　$r \Longrightarrow p$.　但①②有時可合併, ③④有時可合併.

(4) 求證“p,q,r,s等價 ”的證明型態變化更多, 例如：
“直線型”：分別證明 ①$p \Longleftrightarrow q$, ②$q \Longleftrightarrow r$, ③$r \Longleftrightarrow s$
“放射型”：分別證明 ①$p \Longleftrightarrow q$, ②$p \Longleftrightarrow r$, ③ $p \Longleftrightarrow s$
“繞圈型”：分別證明 ①$p \Longrightarrow q$, ② $q \Longrightarrow r$, ③ $r \Longrightarrow s$, ④$s \Longrightarrow p$.
“混合型”：分別證明 ① $p \Longrightarrow q$, ② $q \Longrightarrow r$, ③ $r \Longrightarrow p$, ④ $s \Longleftrightarrow p$.

【要點１１】

① $p\to(q\wedge r) \Longleftrightarrow (p\to q)\wedge(p\to r)$

② 證明 $p \Longrightarrow (q\wedge r)$ 的方法：
順向證法：分別證明“$p \Longrightarrow q$”以及“$p \Longrightarrow r$”即可.
逆向證法：證明“$(\neg q\vee\neg r) \Longrightarrow \neg p$”(見要點12)

[說明] (1) 由要點7可知還有別種證明型態, 但不太有用.
(2) $p \Longrightarrow q$ 以及 $p \Longrightarrow r$ 有時可以合併一起證.

[習題11.1] 證明 $p\to(q\wedge r)$ 與 $(p\to q)\wedge(p\to r)$ 等價

【要點１２】

① $(p\vee q)\to r \Longleftrightarrow (p\to r)\wedge(q\to r)$

② 證明 “ $(p\vee q) \Longrightarrow r$ ” 的方法：
基本證法：分別證明 “$p \Longrightarrow r$” 以及 “$q \Longrightarrow r$”

逆向證法：證明 “$\neg r \Longrightarrow (\neg p \wedge \neg q)$”

[說明] (1) 由要點7可知還有別種證明型態，但不太有用.

[習題12.1] 證明 $(p \vee q) \to r$ 與 $(p \to r) \wedge (q \to r)$ 等價

【要點１３】

證明 $(p \to q) \Longrightarrow r$ 的方法：

順向證法：r是求證的主體，在推導r的過程中適當地套用所給的已知條件“$p \to q$”來完成證明.

逆向證法：假設$\neg r$，推導出 $\neg(p \to q)$

這時通常 $(p \to q)$是$(\forall x, p(x) \to q(x))$的省略型.

所以$\neg(p \to q)$不能只解釋爲$p \wedge \neg q$. 而應該是$(\exists x, p(x) \wedge \neg q(x))$

這要靠$\neg r$來找$(p \to q)$的反例，也就是找使$p(x) \wedge \neg q(x)$成立的x.

(不能拆成證明“$\neg r \Longrightarrow p$” 以及 “$\neg r \Longrightarrow \neg q$”)

[例13.1] 已知實數向量u,v滿足下列條件

“ $au + bv = cu + dv \ \to\ a = c, b = d$ ”

求證“ u,v線性獨立 ” (參閱綜合線性代數CH6定義9)

證: (已知條件其實是“$\forall a,b \in \mathbb{R}, (au + bv = cu + dv \to (a = c \wedge b = d))$ ”的簡寫)

利用已知條件推導出“向量u,v線性獨立”：

若 $xu + yv = o$

則 $xu + yv = 0u + 0v$,

由已知條件即得 $x = 0, y = 0$.

故得證.

[習題13.1] 試用逆向證法證明例13.1.

【要點１４】

① $p\to(q\to r) \Longleftrightarrow (p\wedge q)\to r$

② 證明 $p \Longrightarrow (q\to r)$ 的方法：

由 $p\wedge q$ 推導出 r (就是證明 $(p\wedge q) \Longrightarrow r$)

[說明] (1) 由真值表可驗證 “$p\to(q\to r)$” $\Longleftrightarrow$ “$(p\wedge q)\to r$”

[例14.1]

下列各敘述是同一回事：

(ｉ) 若下雨又頭痛則翹課

(ii) 若下雨, 那麼若頭痛則翹課

[例14.2]

C語言的程式片斷:

```
if( x > 0    &&    y > 5 ) {
      z = x + y ;
}
```

相當於是

```
if( x >0 ) {
    if ( y > 5 ) { z = x+ y ; }
}
```

[例14.3] 證明 $p\vee q \Longrightarrow \neg p\to q$

$$
\begin{aligned}
& (p\vee q)\wedge(\neg p) \\
\Longleftrightarrow\ & (p\wedge\neg p)\vee(q\wedge\neg p) \\
\Longleftrightarrow\ & \mathsf{F}\vee(q\wedge\neg p) \quad \Longleftrightarrow \quad (q\wedge\neg p)
\end{aligned}
$$

$\Longrightarrow \quad q$

$\therefore \quad p \vee q \Longrightarrow \neg p \to q$

[例14.4] 已知向量u,v線性獨立, 求證

$$au+bv=cu+dv \ \to \ a=c, b=d$$

證: 用順向證法, 由“向量u,v線性獨立”和“$au+bv=cu+dv$”

推導出 " $a=c, b=d$ " :

設 $au+bv=cu+dv$

則 $(a-c)u+(b-d)v=o$

而 u,v線性獨立,

$\therefore \quad a-c=0$, $b-d=0$. (綜線CH6定義9)

$\therefore \quad a=c, b=d$.

故得證.

[例14.5] 對方陣A, B, 已知A可逆, B不可逆, 求證AB不可逆.

證: 本題欲證 “A可逆$\wedge B$不可逆$\to AB$不可逆”

即“A可逆$\to$(B不可逆$\to AB$不可逆)”

即“A可逆$\to$(AB可逆$\to B$可逆)”

即“(A可逆$\wedge AB$可逆)$\to B$可逆)”

若A可逆,且AB可逆,

則 A^{-1}可逆

$\therefore \quad A^{-1}AB$可逆

$\therefore \quad B$可逆

[習題14.1] 證明①

[習題14.2] 已知 $p\to q$ 求證 $(p\wedge r)\to q$

[習題14.3] 已知線性映射T滿足 $\mathrm{Ker}T=\{o\}$ 的條件,

求證:　$T(u)=T(v) \rightarrow u=v$

【要點１５】

下列各邏輯式等價 :

(ⅰ) $p \vee q$

(ⅱ) $\neg p \rightarrow q$

(ⅲ) $\neg q \rightarrow p$

(ⅳ) $\neg(\neg p \wedge \neg q)$

[說明] (1) 由(ⅰ)(ⅱ)可發現: “或” 就是 “否則”

[例15.1] 下列四敘述等價:

(ⅰ) “你要用功還是要落榜?”

(ⅱ) “你若不用功就會落榜.”

(ⅲ) “你若不願落榜就必須用功.”

(ⅳ) “你不用功又不落榜是不可能的.”

[例15.2] 人類在說話時並不一定遵守邏輯規則, 我們經常還要參照上下文或當時的情境來判定意義.

例如有強盜問 : “要錢還是要命” , 這在字面上好像是 “或” 的結構, 但實質上並不允許 “都要” 的答覆. 由常理可知這話是 “若要錢就不要命” , 也就是 “若要命就不要錢” , 邏輯上其實是 “不要錢還是不要命” 才對.

假如被問的人是正準備自殺的人, 那他可能會回答 “都不要” , 這在邏輯上是允許的. 因此原先的問句並不是exclusive-or.

[習題15.1] 試證要點15

【要點１６】

① 下列各邏輯式等價:

(ｉ) $p \to (q \vee r)$　　(ⅱ) $(p \wedge \neg q) \to r$

(ⅲ) $(p \wedge \neg r) \to q$　　(ⅳ) $(\neg q \wedge \neg r) \to \neg p$

(ｖ) $\neg(p \wedge \neg q \wedge \neg r)$

② 證明 $p \Longrightarrow (q \vee r)$ 的方法：

第一型： 由p推導出$q \vee r$　(即 $p \Longrightarrow q \vee r$)

第二型： 由$p \wedge \neg q$推導出r　(即 $p \wedge \neg q \Longrightarrow r$)

第三型： 由$p \wedge \neg r$推導出q　(即 $p \wedge \neg r \Longrightarrow q$)

第四型： 由$\neg q \wedge \neg r$推導出$\neg p$　(即 $\neg q \wedge \neg r \Longrightarrow \neg p$)

第五型： 由$p \wedge \neg q \wedge \neg r$推導出矛盾

[習題16.1] 證明①

[習題16.2] 設U, V是向量空間W的子空間, 若$U \cup V$也是W的子空間,
求證　$U \subseteq V$ 或 $V \subseteq U$　　(參閱綜線CH5定理24)
(hint: 用第五型. 先研讀好第二回講義再做.)

§2. 特種證明技巧

【要點17】Σ的記號

爲了表達及運算的需要, $a_1+a_2+....+a_k$常記爲 $\sum_{i=1}^{k} a_i$

上式中 i是求和程序中的控制變數. 它從下限1每次加一, 逐步變到上限k, 過程中的每一項都拿來加, 而得出總和. 上限等於下限時只有一項. 上限小於下限時全式

爲0.

求和式中的a_i可以是任何式子(向量, 矩陣, 函數, 向量空間, ...), 不一定要是數.

若將上式內的每個 i 都改名爲z, 所得的求和式 $\sum_{z=1}^{k} a_z$ 並無不同. 所以i又稱爲啞變數(dummy variable).

前述符號可靈活運用, 產生許多變化. 例如

$$\sum_{i=-2}^{2} a_i = a_{-2}+a_{-1}+a_0+a_1+a_2 .$$

$$\sum_{k=1}^{6} b_k = b_1+b_2+b_3+b_4+b_5+b_6 .$$

Σ的求和記號在線性代數中很常用, 它的運算性質常用在某些證明之中, 請參閱綜線CH2, CH7, CH10.

[例17.1]

$$\sum_{k=1}^{t} b_k = b_1+b_2+\dots+b_t .$$

$$\sum_{i=1}^{4} a_i^3 = a_1^3+a_2^3+a_3^3+a_4^3 .$$

$$\sum_{k=1}^{100} 3^k = 3^1+3^2+\dots+3^{100} .$$

$$\sum_{k=1}^{\infty} 3^k = 3^1+3^2+\dots .$$ (此爲無限級數)

[習題17.1]

① 將 $\sum_{i=1}^{5} 4i$ 展開

② 將 $\sum_{i=1}^{50} i^2$ 展開

③ 將 $\sum_{i=1}^{5} a_i^{i+2}$ 展開

④ 將 $\sum_{i=1}^{5} a$ 展開

[習題17.2]

將 1・2・3 + 2・3・4 + 3・4・5 + ... + 56・57・58 改用Σ表示

【要點18】Σ的基本性質

① $\sum_{j=1}^{n}\alpha = n\alpha$.

② $\beta\sum_{j=1}^{n}\alpha_j = \sum_{j=1}^{n}\beta\alpha_j$. (分配律)

③ $\sum_{j=1}^{n}(\alpha_j+\beta_j) = \sum_{j=1}^{n}\alpha_j + \sum_{j=1}^{n}\beta_j$. (改變求和順序)

④ 若 $1\le s\le n$, 則 $\sum_{j=1}^{n}\alpha_j = \sum_{j=1}^{s}\alpha_j + \sum_{j=s+1}^{n}\alpha_j$. (分段求和)

⑤ $\sum_{j=1}^{n} \alpha_{j+k} = \sum_{j=1+k}^{n+k} \alpha_j$　　(改變足標)

[說明] 綜線CH2定理28, CH7定理15的證明須用到這些公式.

[例18.1] 證明②如下:

$$\beta\sum_{j=1}^{n}\alpha_j = \beta(\alpha_1+\alpha_2+....+\alpha_n) = \beta\alpha_1+\beta\alpha_2+....+\beta\alpha_n = \sum_{j=1}^{n}\beta\alpha_j$$

[例18.2] 分項對消法:

$$\sum_{p=1}^{100}\frac{1}{p(p+1)(p+2)} = \sum_{p=1}^{100}\frac{1}{2}\left(\frac{1}{p(p+1)} - \frac{1}{(p+1)(p+2)}\right)$$

$$= \frac{1}{2}\left(\sum_{p=1}^{100}\frac{1}{p(p+1)} - \sum_{p=1}^{100}\frac{1}{(p+1)(p+2)}\right) \qquad \text{(由②,③)}$$

$$= \frac{1}{2}\left(\sum_{p=1}^{100}\frac{1}{p(p+1)} - \sum_{p=2}^{101}\frac{1}{p(p+1)}\right) \qquad \text{(由⑤)}$$

$$= \frac{1}{2}\left(\frac{1}{1\cdot 2} - \frac{1}{101\cdot 102}\right)$$

本題是套用公式逐步求解, 其實可用分項對消法直接由第一行跳到第四行.

[例18.3] 應用實例

$$\sum_{p=1}^{n}(p+1)^3 = \sum_{p=1}^{n}(p^3+3p^2+3p+1) = \sum_{p=1}^{n}p^3+3\sum_{p=1}^{n}p^2+3\sum_{p=1}^{n}p+n$$

$$3\sum_{p=1}^{n}p^2 = \sum_{p=1}^{n}(p+1)^3 - \sum_{p=1}^{n}p^3 - 3\sum_{p=1}^{n}p - n = (n+1)^3 - 1 - 3\cdot\frac{n(n+1)}{2} - n$$

化簡即得 $\sum_{p=1}^{n}p^2 = \dfrac{n(n+1)(2n+1)}{6}$

依同法對$(p+1)^4$展開求和可導出 $\sum\limits_{p=1}^{n} p^3$ 的公式.

[習題18.1]

證明③, ④, ⑤

【要點19】多維Σ記號

“二維”求和式

$a_{32}+a_{33}+a_{34}+a_{35}$

$+a_{42}+a_{43}+a_{44}+a_{45}$

$+a_{52}+a_{53}+a_{54}+a_{55}$

可記爲

$$\sum_{3\le i\le 5,\ 2\le j\le 5} a_{ij}$$

依此方式可靈活運用Σ符號，產生許多變化．例如

$$\sum_{3\le i\le j\le 5} a_{ij} = a_{33}+a_{34}+a_{35}+a_{44}+a_{45}+a_{55}$$

$$\sum_{3\le i<j\le 5} a_{ij} = a_{34}+a_{35}+a_{45}$$

$$\sum_{1\le i\le 2,\ 3\le j\le 4,\ 5\le k\le 7} a_{ijk} = a_{135}+a_{136}+a_{137}+a_{145}+a_{146}+a_{147}+a_{235}+a_{236}+a_{237}+a_{245}+a_{246}+a_{247}$$

多維和可用多層的一維和逐層求算.

[例19.1]

① $\sum\limits_{j=1}^{i} a(i, j) = a(i, 1)+a(i, 2)+....+a(i, i)$

② $\sum_{i=1}^{5}\sum_{j=1}^{i} a(i,j) = \sum_{j=1}^{1} a(1,j) + \sum_{j=1}^{2} a(2,j) + \sum_{j=1}^{3} a(3,j) + \sum_{j=1}^{4} a(4,j) + \sum_{j=1}^{5} a(5,j)$

$=a(1, 1)$
$+ a(2, 1)+a(2, 2)$
$+ a(3, 1)+a(3, 2)+a(3,3)$
$+ a(4, 1)+a(4, 2)+a(4,3)+a(4,4)$
$+ a(5, 1)+a(5, 2)+a(5,3)+a(5,4)+a(5,5)$

$= \sum_{1\le j\le i\le 5} a(i,j)$

[習題19.1]

展開 $\sum_{1\le j\le k\le 5} \alpha_{jk}$

[習題19.2]

① 將 $\sum_{j=1}^{3} a(i,j)$ 展開

② 將 $\sum_{i=1}^{5}\sum_{j=1}^{3} a(i,j)$ 展開

【要點20】多維Σ與多層Σ的性質

① $\sum_{1\le j\le n,\ 1\le k\le s} \alpha_{jk} = \sum_{j=1}^{n}\sum_{k=1}^{s} \alpha_{jk} = \sum_{k=1}^{s}\sum_{j=1}^{n} \alpha_{jk}$.　(改變求和順序)

② $\sum_{\substack{1\le j\le n \\ 1\le k\le n}} \alpha_{jk} = \sum_{j=1}^{n} \alpha_{jj} + \sum_{1\le j<k\le n} \alpha_{jk} + \sum_{1\le k<j\le n} \alpha_{jk}$.　(分區求和)

[說明] 綜線CH2定理28③的證明用到①的性質. 綜線CH10範例2a的證明須用到②的性質.

[例20.1] 證明①如下:

$$\sum_{j=1}^{n}\sum_{k=1}^{s}\alpha_{jk}=\sum_{j=1}^{n}(\alpha_{j1}+\alpha_{j2}+\ldots+\alpha_{js})$$

$$\begin{aligned}
&= (\alpha_{11}+\alpha_{12}+\ldots+\alpha_{1s}) \\
&\quad + (\alpha_{21}+\alpha_{22}+\ldots+\alpha_{2s}) \\
&\quad + \ \ldots\ldots \\
&\quad + (\alpha_{n1}+\alpha_{n2}+\ldots+\alpha_{ns}) \\
&= (\alpha_{11}+\alpha_{21}+\ldots+\alpha_{n1}) \\
&\quad + (\alpha_{12}+\alpha_{22}+\ldots+\alpha_{n2}) \\
&\quad + \ \ldots\ldots \\
&\quad + (\alpha_{1s}+\alpha_{2s}+\ldots+\alpha_{ns}) \qquad \text{(改變求和順序)}
\end{aligned}$$

$$=\sum_{k=1}^{s}(\alpha_{1k}+\alpha_{2k}+\ldots+\alpha_{nk})=\sum_{k=1}^{s}\sum_{j=1}^{n}\alpha_{jk}$$

[習題20.1]

已知 $\forall p,q,\ a_{pq}=a_{qp}$， 求證

$$\sum_{\substack{1\le p\le n\\ 1\le q\le n}} a_{pq}=\sum_{p=1}^{n}a_{pp}+2\sum_{1\le p<q\le n}a_{pq}$$

∗[習題20.2]

證明

(a) $\displaystyle\sum_{i=1}^{5}\sum_{j=1}^{i}a(i,j)=\sum_{j=1}^{5}\sum_{i=j}^{5}a(i,j)$

(b) $\displaystyle\sum_{i=3}^{5}\sum_{j=1}^{i}a(i,j)=\sum_{j=1}^{2}\sum_{i=3}^{5}a(i,j)+\sum_{j=3}^{5}\sum_{i=j}^{5}a(i,j)$

【要點21】數學歸納法(有限型) (*finite induction*)

$p(n)$是一個與整數n有關的敘述, 若滿足下述二條件

$$\begin{cases} (\text{i})\ p(1) \text{ 成立} \\ (\text{ii})\ \text{“}\ \forall k, p(k)\to p(k+1)\ \text{”} \quad \text{成立,} \end{cases}$$

則 $p(n)$對任意正整數n都成立.

[說明] (1) 數學歸納法本身的證明可不管, 會使用就可以了.

(2) 由(ⅰ)先得知 $p(1)$ 成立. 經由(ⅱ)可知 $p(2)$ 成立(取$k=1$). 再由(ⅱ)可知 $p(3)$ 成立(取$k=2$). 再由(ⅱ)可知 $p(4)$ 成立(取$k=3$). 再由(ⅱ)可知 $p(5)$ 成立........

依此類推可知 $p(n)$對每個正整數n都成立.

(3) 若把(ⅰ)改爲 "$p(-2)$成立", 則定理的結論變成

"$p(n)$對$n=-2,-1,0,1,2,3,\ldots..$都成立".

其他情形的變化依此類推.

(4) 數學歸納法本身是一個“法律程序”. 許多定理雖然用它證明, 但並不是靠它想出來的.

[例21.1] 用數學歸納法證明

$$\sum_{m=1}^{n} m^2 = \frac{n(n+1)(2n+1)}{6}$$

[證] $n=1$ 時,

$$\frac{1(1+1)(2\cdot 1+1)}{6} = 1 = 1^2$$

∴ 原式成立.

設 $n=k$ 時原式成立, 則

$$\sum_{m=1}^{k+1} m^2 = \sum_{m=1}^{k} m^2 + (k+1)^2$$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= \frac{(k+1)}{6}\,[k(2k+1) + 6(k+1)]$$

$$= \frac{(k+1)}{6}\,(2k^2+7k+6)$$

$$= \frac{(k+1)}{6}\,(k+2)(2k+3)$$

$$= \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6}$$

∴ 原式在$n=k+1$ 時成立.

故得證.

[習題21.1] 證明

$$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & \sin n\theta \\ -\sin n\theta & \cos n\theta \end{bmatrix}$$

【要點22】數學歸納法(有限推廣型)

設r為正整數, $p(n)$是一個與整數n有關的敘述，若下述二條件成立

$$\begin{cases} (\text{i}) & p(1)\wedge p(2)\wedge \dots \wedge p(r) \\ (\text{ii}) & \forall k, ((p(k)\wedge p(k+1)\wedge \dots \wedge p(k+r-1)) \rightarrow p(k+r)) \end{cases}$$

則 $p(n)$對任意正整數n都成立.

[說明] (1) 若把(ⅰ)改為 "$p(0)\wedge p(1)\wedge\ldots\wedge p(r-1)$", 則定理的結論變成 "$p(n)$對$n=0,1,2,3,\ldots\ldots$都成立".
其他情形的變化依此類推.

[例22.1] (清大69資科)

$T_n(x)=\cos(n\arccos x)$ 求證 $T_n(x)$ 為 n 次多項式

令 $\theta=\arccos(x)$, 則

$T_0(x)=\cos(0)=1$, $\deg(T_0(x))=0$

$T_1(x)=\cos(\arccos x)=x$, $\deg(T_1(x))=1$

設 $T_k(x)$是k次多項式, 且$T_{k+1}(x)$是$k+1$次多項式.

$$
\begin{aligned}
T_{k+2}(x) &= \cos((k+2)\theta) = \cos((k+1)\theta+\theta) \\
&= \cos((k+1)\theta)\cos\theta-\sin((k+1)\theta)\sin\theta \\
&= 2\cos((k+1)\theta)\cos\theta - (\cos((k+1)\theta)\cos\theta+\sin((k+1)\theta)\sin\theta) \\
&= 2\cos((k+1)\theta)\cos\theta - (\cos((k+1)\theta-\theta)) \\
&= 2\cos((k+1)\theta)\cos\theta - \cos(k\theta) \\
&= 2T_{k+1}(x)T_1(x) - T_k(x) \\
&= 2xT_{k+1}(x)-T_k(x) \quad \text{為}k+2\text{次多項式.}
\end{aligned}
$$

故得證.

【要點23】**數學歸納法(超限型)** (*transfinite induction*)

$p(n)$是一個與整數n有關的敘述, 若滿足下述二條件

$$
\begin{cases}
(\text{i})\ p(1) \\
(\text{ii})\ \forall m, ((\forall k<m, p(k))\rightarrow p(m))
\end{cases}
$$

則 $p(n)$對任意正整數n都成立.

[說明] (1) 超限型的威力是表現在證明 well-ordered set 上的敘述. 這件事對一般同學來說超出範圍, 可不理會. 在此只列出在正整數系上的情形.

(2) 超限型的(ⅱ)相當於

“ $p(1), p(2),...., p(m-1)$ 成立→$p(m)$ 成立 ”,

比有限型好證(因為前提部份較強). 但一般習慣上都儘可能使用有限型, 遇到困難時才考慮用超限型.

(3) 有的書在證明時會把(ⅰ)的部份省略掉, 但考卷上還是要寫(以策安全). 為了與(ⅱ)銜接, 有時在(ⅰ)中還要多證幾個特殊的$p(n)$.

習 題 解 答

[習題1.1解]

p	q	$p\rightarrow q$	$p\leftarrow q$	$(p\leftarrow q)\wedge(p\rightarrow q)$	$p\leftrightarrow q$
F	F	T	T	T	T
F	T	T	F	F	F
T	F	F	T	F	F
T	T	T	T	T	T

[習題1.2解]

p	q	$\neg p$	$\neg q$	$\neg p\wedge\neg q$	$\neg(\neg p\wedge\neg q)$	$p\vee q$
F	F	T	T	T	F	F
F	T	T	F	F	T	T
T	F	F	T	F	T	T
T	T	F	F	F	T	T

[習題2.1解]　"$\forall b\in B, \exists a\in A, b=f(a)$"

[習題2.2解] $\forall x, y\in A, ((f(x)=b\wedge f(y)=b) \rightarrow x=y)$

[習題3.1解]

證明　$p\wedge(q\wedge r) \Longleftrightarrow (p\wedge q)\wedge r)$;

將$p\wedge(q\wedge r)$記爲X, 將$(p\wedge q)\wedge r)$ 記爲Y,

p	q	r	$p\wedge q$	$q\wedge r$	X	Y	$X\leftrightarrow Y$
F	F	F	F	F	F	F	T
F	F	T	F	F	F	F	T
F	T	F	F	F	F	F	T
F	T	T	F	T	F	F	T
T	F	F	F	F	F	F	T
T	F	T	F	F	F	F	T
T	T	F	T	F	F	F	T
T	T	T	T	T	T	T	T

因 $X\leftrightarrow Y$ 恆真, 所以 $X \Longleftrightarrow Y$

[習題4.1解]

p	q	r	$q\vee r$	$p\wedge(q\vee r)$	$p\wedge q$	$p\wedge r$	$(p\wedge q)\vee(p\wedge r)$
F	F	F	F	F	F	F	F
F	F	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	T	T	T	F	F	F	F
T	F	F	F	F	F	F	F
T	F	T	T	T	F	T	T
T	T	F	T	T	T	F	T
T	T	T	T	T	T	T	T

比較得知 $p\wedge(q\vee r)$ 與 $(p\wedge q)\vee(p\wedge r)$ 等價. 另一式讀者自證.

[習題4.2解]

$$p\wedge(q\vee r)$$
$$=(p\wedge q)\vee(p\wedge r)$$
$$\rightarrow(p\wedge q)\vee r \qquad (\because\ \ p\wedge r\rightarrow r)$$

由真值表也可發現凡是$p\wedge(q\vee r)$爲T的列, $(p\wedge q)\vee r$都是T.

[習題4.3解]

p	q	r	$p\rightarrow q$	$(p\rightarrow q)\rightarrow r$	$q\rightarrow r$	$p\rightarrow(q\rightarrow r)$
F	F	F	T	F	T	T
F	F	T	T	T	T	T
F	T	F	T	F	F	T
F	T	T	T	T	T	T
T	F	F	F	T	T	T
T	F	T	F	T	T	T
T	T	F	T	F	F	F
T	T	T	T	T	T	T

由真值表發現凡是$(p\rightarrow q)\rightarrow r$爲T的列, $p\rightarrow(q\rightarrow r)$都是T.

$\therefore$ "$(p\rightarrow q)\rightarrow r$" $\rightarrow$ "$p\rightarrow(q\rightarrow r)$"

也就是說$(p\rightarrow q)\rightarrow r$較強.

[習題5.1解]　(disprove)

Let $A=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$, than $A^2=O$ and $A\neq O$.

[習題5.2解]　$\forall x,\exists y,\neg p(x,y)$

[習題5.3解] $\exists u\neq o$, 使$\forall v, f(u,v)=o$

[習題6.1解] 讀者利用真值表自證.

[習題6.2解]

$$\neg p\rightarrow q \quad\Longleftrightarrow\quad \neg q\rightarrow p$$

$$\neg p\rightarrow q \quad\Longleftrightarrow\quad p\vee q \quad\Longleftrightarrow\quad \neg(\neg p\wedge\neg q)$$

[習題8.1解]　下列各敘述是同一回事：

(ｉ) p, q, r, s等價(equivalent)

(ⅱ) “$p\Longleftrightarrow q$” 且 “$p\Longleftrightarrow r$” 且 “$p\Longleftrightarrow s$” 且 “$q\Longleftrightarrow r$” 且 “$q\Longleftrightarrow s$” 且 “$r\Longleftrightarrow s$”

(ⅲ) “$p\Longrightarrow q$” 且 “$p\Longrightarrow r$” 且 “$p\Longrightarrow s$” 且 “$q\Longrightarrow p$” 且 “$q\Longrightarrow r$” 且 “$q\Longrightarrow s$” 且 “$r\Longrightarrow p$” 且 “$r\Longrightarrow q$” 且 “$r\Longrightarrow s$” 且 “$s\Longrightarrow p$” 且 “$s\Longrightarrow q$” 且 “$s\Longrightarrow r$”

[習題11.1解]

$$\begin{aligned} & p\rightarrow(q\wedge r) \\ \Longleftrightarrow\quad & \neg p\vee(q\wedge r) \\ \Longleftrightarrow\quad & (\neg p\vee q)\wedge(\neg p\vee r) \\ \Longleftrightarrow\quad & (p\rightarrow q)\wedge(p\rightarrow r) \end{aligned}$$

也可利用真值表證明.

[習題12.1解]

$$\begin{aligned} & (p\vee q)\rightarrow r \\ \Longleftrightarrow\quad & \neg(p\vee q)\ \vee r \\ \Longleftrightarrow\quad & (\neg p\wedge\neg q)\ \vee r \\ \Longleftrightarrow\quad & (\neg p\vee r)\wedge(\neg q\vee r) \\ \Longleftrightarrow\quad & (p\rightarrow r)\wedge(q\rightarrow r) \end{aligned}$$

也可利用真值表證明.

[習題13.1解]

[證] 假設u,v不爲線性獨立, 則

存在不全爲零的純量α,β, 使得 $\alpha u+\beta v=o$.

此時 $\alpha u+\beta v=0u+0v$, 但“$\alpha=0$ 且 $\beta=0$”不成立,

與以知條件矛盾.

[習題14.1解]

可利用真值表證明. 也可利用公式推導如下:

$$
\begin{aligned}
& p\to(q\to r) \\
\Longleftrightarrow\quad & \neg p\vee(q\to r) \\
\Longleftrightarrow\quad & \neg p\vee(\neg q\vee r) \\
\Longleftrightarrow\quad & (\neg p\vee\neg q)\vee r \\
\Longleftrightarrow\quad & \neg(p\wedge q)\vee r \\
\Longleftrightarrow\quad & (p\wedge q)\to r
\end{aligned}
$$

$$
\begin{aligned}
& p\to(q\to r) \\
\Longleftrightarrow\quad & \neg(q\to r)\to\neg p \\
\Longleftrightarrow\quad & (q\wedge\neg r)\to\neg p
\end{aligned}
$$

[習題14.2解]

$$
\begin{aligned}
& (p\to q)\wedge(p\wedge r) \\
\Longleftrightarrow\quad & (\neg p\vee q)\wedge(p\wedge r) \\
\Longleftrightarrow\quad & (\neg p\wedge(p\wedge r))\ \vee\ (q\wedge(p\wedge r)) \\
\Longleftrightarrow\quad & ((\neg p\wedge p)\wedge r)\ \vee\ (q\wedge(p\wedge r)) \\
\Longleftrightarrow\quad & (\mathrm{F}\wedge r)\ \vee\ (q\wedge(p\wedge r)) \\
\Longleftrightarrow\quad & \mathrm{F}\ \vee\ (q\wedge(p\wedge r)) \\
\Longleftrightarrow\quad & q\wedge(p\wedge r) \\
\Longrightarrow\quad & q
\end{aligned}
$$

$\therefore\quad p\to q\ \Longrightarrow\ (p\wedge r)\to q$

[習題14.3解]

若 $\operatorname{Ker}T=\{o\}$ 且 $T(u)=T(v)$

則 $T(u-v)=T(u)-T(v)=o$

$\therefore$ $u-v\in \operatorname{Ker}T$

$\therefore$ $u-v=o$

$\therefore$ $u=v$

[習題15.1解]

可利用真值表證明.

[習題16.1解]

(i) $\Longleftrightarrow$ (ii) ：

$p\to(q\vee r)$

$\Longleftrightarrow$ $p\to(\neg q\to r)$

$\Longleftrightarrow$ $(p\wedge\neg q)\to r$,

(i) $\Longleftrightarrow$ (ii) ：

讀者自證

(i) $\Longleftrightarrow$ (iv) ：

$p\to(q\vee r)$

$\Longleftrightarrow$ $\neg(q\vee r)\to p$

$\Longleftrightarrow$ $(\neg q\wedge\neg r)\to\neg p$

(i) $\Longleftrightarrow$ (v) ：

$p\to(q\vee r)$

$\Longleftrightarrow$ $\neg(p\wedge\neg(q\vee r))$

$\Longleftrightarrow$ $\neg(p\wedge\neg q\wedge\neg r)$

[習題16.2解]

參看綜合線性代數CH5定理24

[習題17.1解]

① 4+8+12+16+20

② $1^2+2^2+3^2+...+50^2$

③ $a_1^{\,3}+a_2^{\,4}+a_3^{\,5}+a_4^{\,6}+a_5^{\,7}$

④ $a+a+a+a+a=5a$

[習題17.2解]

$$\sum_{k=1}^{56} k(k+1)(k+2)$$

[習題18.1解]

③ $$\sum_{j=1}^{n}(\alpha_j+\beta_j) = (\alpha_1+\beta_1)+(\alpha_2+\beta_2)+ ... + (\alpha_n+\beta_n)$$

$$= (\alpha_1+\alpha_2+ ... +\alpha_n) + (\beta_1+\beta_2+ ... +\beta_n)$$ (改變求和順序)

$$= \sum_{j=1}^{n}\alpha_j + \sum_{j=1}^{n}\beta_j \quad .$$

[習題19.2解]

① $$\sum_{j=1}^{3} a(i, j) = a(i, 1)+a(i, 2)+a(i, 3)$$

② $$\sum_{i=1}^{5}\sum_{j=1}^{3} a(i,j) = \sum_{j=1}^{3} a(1,j) + \sum_{j=1}^{3} a(2,j) + \sum_{j=1}^{3} a(3,j) + \sum_{j=1}^{3} a(4,j) + \sum_{j=1}^{3} a(5,j)$$

$$\begin{aligned} &= a(1, 1)+a(1, 2)+a(1, 3) \\ &+ a(2, 1)+a(2, 2)+a(2, 3) \\ &+ a(3, 1)+a(3, 2)+a(3, 3) \\ &+ a(4, 1)+a(4, 2)+a(4, 3) \\ &+ a(5, 1)+a(5, 2)+a(5, 3) \end{aligned}$$

[習題21.1解]

$n=1$ 時顯然成立.

設在$n=k$時成立, 則在$n=k+1$時：

$$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}^{k+1} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}^{k} \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$$

$$= \begin{bmatrix} \cos k\theta & \sin k\theta \\ -\sin k\theta & \cos k\theta \end{bmatrix} \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(k\theta+\theta) & \sin(k\theta+\theta) \\ -\sin(k\theta+\theta) & \cos(k\theta+\theta) \end{bmatrix}$$

故得證

==
=== 何謂證明?

以公理(Axiom,或稱公設)爲基礎, 由定義(Definition)及已知的定理推出新的結果
定理(Theorem), 引理(預備定理)(Lemma), 推論(系)(Corollary), 命題(Proposition)

source of ambigous in literal.:
   example:
前提錯誤或結語正確時成立.
前提錯誤成立且結語正確成立.
前提錯誤以及結語正確時成立.
前提錯誤和結語正確時成立. (此句的和在英文是and,但在中文不應寫成且)