科學圖書大庫

代數數論

譯者　葉哲志　陳弘毅

徐氏基金會出版

科學圖書大庫

代數數論

譯者　葉哲志　陳弘毅

徐氏基金會出版

美國徐氏基金會科學圖書編譯委員會

科學圖書大庫

監修人 徐銘信 科學圖書編譯委員會主任委員
編輯人 林碧鑾 科學圖書編譯委員會編譯委員

中華民國五十九年十月二十二日初版
中華民國六十二年三月二十五日再版

代數數論

定價 新台幣二十五元 港幣四元
國外訂價 1.30 元

譯者
葉哲志 國立師範大學數學系理學士
陳弘毅 國立師範大學數學系理學士

本出版部經內政部核准登記登記證爲內版台業字第1347號

出版者 財團法人臺北市徐氏基金會出版部 臺北郵政信箱3261號 電話783686號
發行人 財團法人臺北市徐氏基金會出版部 林碧鑾 郵政劃撥帳戶15795號
印刷者 大興圖書印製有限公司 三重市三和路四段151號 電話979739號

我們的工作目標

文明的進步，因素很多，而科學居其首。科學知識與技術的傳播，是提高工業生產、改善生活環境的主動力，在整個社會長期發展上，乃人類對未來世代的投資。從事科學研究與科學教育者，各就專長，竭智盡力，發揮偉大功能，共使科學飛躍進展，同把人類的生活，帶進更幸福、更完善之境界。

近三十年來，科學急遽發展之成就，已超越既往之累積，昔之認爲絕難若幻想者，今多已成爲事實。人類一再親履月球，是各種科學綜合建樹與科學家精誠合作的貢獻，誠令人有無限興奮！時代日新又新，如何推動科學教育，有效造就科學人才，促進科學研究與發展，允爲社會、國家的基本任務。培養人才，起自中學階段，學生對普通科學，如物理、數學、生物、化學，漸作接觸，及至大專院校，便開始專科教育，均仰賴師資與圖書的啓發指導，不斷進行訓練。從事科學研究與科學教育的學者，志在貢獻研究成果與啓導後學。旨趣崇高，至足欽佩！

科學圖書是學人們研究、實驗、教學的精華，明確提供科學知識與技術經驗，本具互相啓發作用，富有國際合作性質，歷經長久的交互影響與演變，遂產生可喜的收穫。我國民中學一年級，便以英語作主科之一，然欲其直接閱讀外文圖書，而能深切瞭解，並非數年所可苛求者。因此，本部編譯出版科學圖書，引進世界科技新知，加速國家建設，實深具積極意義。

本基金會由徐銘信氏捐資創辦，旨在協助國家發展科學知識與技術，促進民生樂利。民國四十五年四月成立於美國紐約。初由旅美學人胡適博士、程其保博士等，甄選國內大學理工科優秀畢業生出國深造，前後達四十人，返國服務者十不得一。另贈國內大學儀器設備，輔助教學頗收成效；然審度衡量，仍嫌未能普及，乃再邀承國內外權威學者，設置科學圖書編譯委員會，主持「科學圖書大庫」編譯事宜。主任委員徐[illegible]氏爲監修人，編譯委員林碧鏗氏爲編輯人，各編譯委員擔任分組審查及校閱。「科學圖書大庫」首期擬定二千册，凡四億言，叢書百種，門分類別，細大不捐；分爲叢書，合則大庫。從事翻譯之學者五百位，於英、德、法、日文中精選最新基本或實

用科技名著，譯成中文，編譯校訂，不憚三復。嚴求深入淺出，務期文圖並茂，供給各級學校在校學生及社會大衆閱讀，有教無類，效果宏大。賢明學人同鑑及此，毅然自公私兩忙中，撥冗贊助，譯校圖書，心誠言善，悉付履行，感人至深。其旅居國外者，亦有感於爲國人譯著，助益青年求知，遠勝於短期返國講學，遂不計稿酬菲薄，費時又多，迢迢乎千萬里，書稿郵航交遞，報國熱忱，思源固本，僑居特切，至足欽慰！

今科學圖書大庫已出版七百餘册，都一億八千餘萬言；排印中者，二百餘册，四千餘萬字。依循編譯、校訂、印刷、發行一貫作業方式進行。就全部複雜過程，精密分析，設計進階，各有工時標準。排版印製之衞星工廠十餘家，直接督導，逐月考評。以專業負責，切求進步。校對人員既重素質，審愼從事，復經譯者最後反覆精校，力求正確無訛。封面設計，納入規範，裝訂注意技術改善。藉技術與分工合作，建立高效率系統，縮短印製期限。節節緊扣，擴大譯校複核機會，不斷改進，日新又新。在翻譯中，亦三百餘册，七千餘萬字。譯校方式分爲：(1)個別者：譯者具有豐富專門知識，外文能力強，國文造詣深厚，所譯圖書，以較具專門性而可從容出書者屬之。(2)集體分工者：再分爲譯、校二階次，或譯、編、校三階次，譯者各具該科豐富專門之知識，編者除有外文及專門知識外，尙需編輯學驗與我國文字高度修養，校訂者當爲該學門權威學者，因人、時、地諸因素而定。所譯圖書，較大部頭、叢書、或較有時間性者，人事譯務，適切配合，各得其宜。除重質量外，並爭取速度，凡美、德科學名著初版發行半年內，本會譯印之中文本，賡即出書，欲實現此目標，端賴譯校者之大力贊助也。

謹特掬誠呼籲：

自由中國大專院校教授，研究機構專家、學者，與從事科學建設之工程師；

旅居海外從事教育與研究學人、留學生；

大專院校及研究機構退休教授、專家、學者。

主動地精選最新、最佳外文科學名著，或個別參與譯校，或聯袂而來譯校叢書，或就多年研究成果，撰著成書，公之於世。本基金會樂於運用基金，並藉優良出版系統，善任傳播科學種子之媒介。祈學人們，共襄盛舉是禱！

原　序

本專論的目的是在古典代數數的主要部分作一明確的介紹，康乃爾（Cornell）大學在 1947～48的春季班中曾以複印本來講授本專論，經幾位讀者的批評指教後，再加以修改才成本書。在此特別感謝Leila R. Raines 小姐對原稿的整理與校對。

Harry Pollard

目　錄

第一章　除法

1.唯一因數分解法

初步的數論是在研討有關整數 $0, \pm 1, \pm 2, \cdots$ 之問題，這些數中，**質數**佔很重要的地位；異於 $0, \pm 1$ 之整數 m 除了 ± 1 和 $\pm m$ 外無其他因數，則稱此數為質數，例如 $2, 3, -5$ 皆為質數，而 $6 = 2\cdot 3$, $9 = 3^2$ 則否。因除 0 和 ± 1 外之所有整數皆可由質數造成，故質數甚為重要，在算術基本定理中闡明：**每一大於 1 之整數恰有一方法將其分解為正質數之積，但不考慮其因數排列之次序**，於是

$$12 = 2^2\cdot 3 = 2\cdot 3\cdot 2 = 3\cdot 2^2$$

為將 12 分解成正質數乘積之所有分解法，但此三種方法皆得相同之因數，其差別僅在於因數出現之次序而已。

吾人將證明算術基本定理，在此過程中，先觀察下述一重要結果：每一非負整數所成之集合（有限或無限）必包含一最小元素，此項結果直覺上顯然成立，讀者可視其為整數所定義之性質，以下為幾個預備的定理。

定理1-1. 設 a, b 為整數，$b > 0$，則在整數中恰有二元素 q, r 使

$$a = bq + r \qquad 其中\ 0 \leq r < b$$

考慮有理數 $\frac{a}{b}$，並令 q 為不大於 $\frac{a}{b}$ 之所有整數中最大者。因此，$q \leq \frac{a}{b}$，且 $q+1 > \frac{a}{b}$. 令 $r = a - bq$，因 $\frac{r}{b} = \frac{a}{b} - q \geq 0$，且 $b > 0$ 故 $r \geq 0$ 同時 $1 > (\frac{a}{b} - q) = \frac{a-bq}{b} = \frac{r}{b}$，即 $1 > \frac{r}{b}$，故 $r < b$

欲證 q, r 為唯一，可設 q', r' 為任二整數且

$$a = bq' + r', \qquad 0 \leq r' < b.$$

若 $q'>$ 則 $q'\geq q+1$，故

$$r'=a-bq'\leq a-b(q+1)=(r-b)<0$$

與 $r'\geq 0$ 矛盾。

若 $q'<q$，則 $q'\leq q-1$，故

$$r'=(a-bq')\geq a-b(q-1)=r+b\geq b$$

與 $r'<b$ 矛盾故 $q'>q$ 與 $q'<q$ 二者皆不成立，故 $q=q'$ 成立。且 $r=r'$ 故定理 1.1 即得證。

二整數 a,b 除 ± 1 外無其他公因數，則謂 a,b **互質**。例如：5與9互質，而6與9則不互質。

定理1-2. <u>設 a,b 互質，則存在二整數 s,t 使 $as+bt=1$.</u>

注意此定理中之 s,t 並無"唯一"之限制，事實上若取 $a=3$, $b=5$，則

$$2\cdot 3-1\cdot 5=1, \qquad -3\cdot 3+2\cdot 5=1,$$

其中 $s=2$, $t=-1$, 或 $s=-3$, $t=2$.

欲證此定理，須注意 a,b 均不爲零。考慮所有具 $ax+by$ 形式之數所成之集合，其中 x,y 均爲整數，令此集合爲 S，若取 $x=1,y=0$ 和 $x=-1$, $y=0$ 則知 a 與 $-a$ 均在 S 中。因 $a\neq 0$ 故 a 與 $-a$ 必有一爲正數，故 S 必包含某一正數，令 d 爲 S 中最小之正數，故書 $d=as+bt$，其中 s,t 爲整數。

由定理 1.1 吾人可找到 q,r 使

$$b=dq+r, \qquad 0\leq r<d.$$

則

$$r=b-dq=b-(as+bt)q=a(-sq)+b(1-qt)\in S,$$

故 $r\in S$. 故 r 爲 S 中最小正數，但 $0<r<d$ 爲不可能，故 $r=0$. 於是 $b=dq$. 同樣，若

$$a=dq'+r',$$

而 q',r' 爲整數，　　$0\leq r<b.$

可得證 $r'=0$，故 $a=dq'$.

由以上結果，我們證得：d 爲 a, b 之公因數，但 a, b 互質，故 $d=\pm 1$；而 d 爲正數，所以 $d=1$，因此 $1=as+bt$.

吾人可用記號"$m|n$"表示"m 整除 n"或"m 爲 n 之因數"。若 m 非爲 n 之因數時，則記爲 $m \nmid n$。由下面的定理可得到唯一因數分解法之關鍵。

定理 1-3. 設 p 爲質數，且 $p|ab$，則 $p|a$ 或 $p|b$.

此定理中 $p|a$，$p|b$ 並非互斥的。（亦即可能同時 $p|a$，$p|b$.）

若 $p|a$，則此定理成立。

設 $p \nmid a$，因 p, a 互質，故有二整數 l, m 使

$$lp+ma=1, \qquad lpb+mab=b.$$

因 $p|ab$，故 $ab=pq$，q 爲整數，所以 $lpb+mpq=b$，即 $p(lb+mq)=b$，故 $p|b$.

推論 1-4. 若 p 爲一質數且 $p|a_1 a_2 \cdots a_n$，其中 $a_1, \cdots a_n$ 皆爲整數，則 $a_1, a_2 \cdots a_n$ 中至少有一 a_i，使 $p|a_i$.

因對每一個數 a_i，$1 \leq i \leq n$，若 $p \nmid a_i$，則由定理 1.3 知

$$p \nmid a_1 a_2, \ p \nmid (a_1 a_2) a_3, \ \cdots p \nmid (a_1 a_2 \cdots a_{n-1}) a_n.$$

現在吾人欲證此章剛開始時所提到之"基本定理"。令 m 爲不等於 1 的正整數。若 m 爲非質數，設其可分解爲 $m=m_1 m_2$，而 $m_1>1$，$m_2>1$．若 m_1，m_2 皆爲質數，則即爲得證；反之則對 m_1，m_2 二數反覆進行此種步驟，繼續找其新因數。最後分解至某一有限次，則所有之因數定無法再分解。否則 m 雖爲一有限整數，但 m 可寫成任意大於 1 之因數乘積，如此便會產生矛盾結果。

於是吾人得一因數分解：

$$m=p_1 p_2 \cdots p_r$$

其中 p_i 爲正質數。

假設
$$m=q_1 q_2 \cdots q_s$$

爲 m 之另一分解法，其中 q_i 爲正質數。吾人欲證此二分解法所不同者只在於因數出現次序不同而已。因

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

由推論 1.4 知 $p_1, \cdots p_r$ 中至少有一數 p_i 使 $q_1 \mid p_i$。可設此數為 p_1 以應吾人所須，於是 $q_1 \mid p_1$。因 p_1, q_1 皆為正質數，故 $p_1 = q_1$。消去 p_1, q_1 後，得

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

此步驟重覆進行，直至上式中一邊之所有質因數除完為止。在此過程中另一邊之所有因數亦必除盡。否則將會產生一種矛盾情形：若干個質數乘積會等於 1。因此 $r=s$ 必成立。故此定理得證。

假設吾人欲將"因數分解之唯一性"用到負整數上，則由於因數中會有負號"$-$"出現，會遭遇到困難。例如：

$$-12 = 2^2(-3) = (-2)(-3)(-2)$$

觀察此式，可知將 -12 分解成質數乘積有二方法，而此兩種分解法不僅在因數次序上有所不同，而且因數本身亦有所差異，在第一種情形下，其因數為 $2, 2, -3$，但在第二種情況中，其因數為 $-2, -3, -2$. 不過我們若將基本定理略加改述，使其包含負整數，則此種困難便能補救。今稱 1 和 -1 為**單位**(units). 則定理可另述如下：

定理 1-5. (基本定理)每一不為零或單位之整數，可被分解為質數之乘積，若不考慮其因數排列之次序，亦不考慮其因數以單位乘之，則其分解法為唯一。

此定理之證明與前述者略有改變，讀者試證之。

2.一般問題

今觀察一代數數論中之基本問題：假若吾人將"整數"之意義擴充，使其包含比 $0, \pm 1, \pm 2, \cdots$ 較廣之集合。如此類似於定理 1.5 之敍述是否仍為眞確？關於此問題，讀者試觀察數個例子，便會很淺顯地看出來。

首先提到**高斯整數**(Gaussian integers)，吾人定義此種整數為具 $a+bi$ 形式之數，其中 a, b 為平常所謂之整數，而 $i=\sqrt{-1}$. 為避免混淆，以後吾人將稱平常整數為**有理整數**(rational integers). 令 G 表所有高斯整數所成之集合。J 表所有有理整數所成之集合。注意：在每一集合中，整數之和，差，積仍為整數。

設 $\beta \in G$, 若存在一數 $\gamma \in G$ 使 $\beta = \alpha\gamma$，則稱 α 整除 β，記為 $\alpha \mid \beta$. G 中

之元素若能整除 1，則稱此元素爲 **單位**(unit)．由此定義可知，單位可整除 G 中每一元素。若一數 π 能滿足二條件：①不爲單位；②若 $\pi=\alpha\beta$，則 α 或 β 爲單位，則稱 π 爲**質數**。

由於定義這些名詞，因此定理 1.5 對集合 G 而言便有意義，但定理 1.5 對 G 是否仍爲眞確呢？吾人不久將即給予證明。但在證明此結果以前，先舉一簡單之整數集合以證明定理 1.5 對此集合而言雖有意義，但不爲眞確。

吾人定義一種整數爲具 $a+b\sqrt{-5}$ 之形式之數，其中 a，b 爲有理整數。令此種形式之數所成之集合爲 H，顯然 H 中任二元素之和，差，積仍在 H 中，定義 H 中之單位和質數與 G 中之定義相仿，只要把 G 代以 H 便可。稍後吾人將予證明 ± 1 爲 H 中僅有之單位；$3, 7, 1+2\sqrt{-5}, 1-2\sqrt{-5}$ 在 H 中皆爲質數。但

$$21=3\cdot 7=(1+2\sqrt{-5})(1-2\sqrt{-5}).$$

觀察上式雖不計其因數排列次序或其因數與單位乘積，但其因數分解法並非唯一。

因此，基本定理在何種整數集合下成立？何種集合下不成立？又 J, G 和 H 之間有何不同？如何予以圓滿解釋？這些問題以後將予答覆。

3.高斯整數

設 $\alpha=(a+bi)\in G$，則 $\alpha\bar{\alpha}$ 稱爲 α 之**模**(norm)，記爲 $N(\alpha)$ 或 $N\alpha$，而 $\alpha\bar{\alpha}=|\alpha|^2=a^2+b^2$.（ $\bar{\alpha}$ 爲 α 之共軛複數 ），模之基本性質可列之如下：

(1) 若 $\alpha\in G$ 且 $\alpha\in J$，則 $N\alpha=\alpha^2$.

(2) $N(\alpha\beta)=N\alpha\, N\beta$.

(3) 若且唯若 $N\alpha=1$，則 α 爲一單位。

(4)

$$N\alpha=\begin{cases}=0 & 若\ \alpha=0,\\ =1 & 若\ \alpha=\pm 1\ 或\ \pm i,\\ >1 & 其他。\end{cases}$$

(5)若 $N\alpha$ 爲 J 中的質數，則 α 爲 G 中的質數。

於(1)中因 $b=0$，故顯然成立。欲證(2)，若 $\alpha=a+bi$，$\beta=c+di$，則

$$(\alpha\beta)(\overline{\alpha\beta})=(\alpha\overline{\alpha})(\beta\overline{\beta}).$$

至於(3)，設α爲一單位，於是$\alpha \mid 1$，故$\alpha\beta=1$，其中$\beta\in G$．由(2)$N\alpha\ N\beta=N1=1$，且$N\alpha \mid 1$，因$N\alpha$必須爲非負整數，所以$N\alpha=1$．反之，若$N\alpha=1$，則$a^2+b^2=1$，因此$a=0$或$b=0$，於是$\alpha=1$，-1，i，或$-i$，而這些數顯然爲單位。以上之討論可證明(4)中大部分，其餘留給讀者自行爲之。最後證明(5)，假設$N\alpha$爲質數且$\alpha=\beta\gamma$，則$N\alpha=N\beta\ N\gamma$在J中爲質數，故$N\beta$或$N\gamma$必有一數等於1．由(3)知β或γ爲一單位，因此α在G中爲質數。

(5)之逆敍述不成立，吾人只須證明3在G中爲質數，便足以了解。因$N3=3^2=9$，設$3=\alpha\beta$，於是$9=N\alpha\ N\beta$。若α，β皆非單位，$N\alpha\neq 1$，$N\beta\neq 1$，故$N\alpha=N\beta=3$，亦即：若$\alpha=a+bi$則$a^2+b^2=3$．但對J中任意二元素a，b而言，此事爲不可能。（何故？）

欲證明定理1.5對於G仍成立，吾人將儘量模倣在J中之證明。

定理1-6. 設$\alpha,\beta\in G$，$\beta\neq 0$，則存在二整數π,β使

$$\alpha=\pi\beta+\rho,\qquad 其中N\rho<N\beta.$$

觀察此數$\frac{\alpha}{\beta}=A+Bi$，而$A$，$B\in J$．可適當選擇$s$，$t\in J$使

$$|A-s|\leq\frac{1}{2},\qquad |B-t|\leq\frac{1}{2}.$$

吾人可分別選取最接近A,B之s，t．令$\pi=s+ti$，$\rho=\alpha-\pi\beta$．

欲證$N\rho<N\beta$，觀察下式：

$$\begin{aligned}|\rho|&=|\alpha-\pi\beta|=|\alpha-(s+ti)\beta|=|\beta|\left|\frac{\alpha}{\beta}-s-ti\right|\\&=|\beta|\,|(A-s)+(B-t)i|=|\beta|\{(A-s)^2+(B-t)^2\}^{1/2}\\&\leq|\beta|\left\{\frac{1}{2^2}+\frac{1}{2^2}\right\}^{1/2}<|\beta|.\end{aligned}$$

因$N\rho=|\rho|^2<|\beta|^2=N\beta$，故此不等式成立。

例如：令$\alpha=5-i$，$\beta=1+2i$，則

$$\frac{\alpha}{\beta}=\frac{(5-i)(1-2i)}{(1+2i)(1-2i)}=\frac{3}{5}-\frac{11}{5}i$$

故 $A=\frac{3}{5}$, $B=\frac{-11}{5}$, 取 $\gamma=1$, $t=-2$, $\pi=1-2i$, $\rho=(5-i)-(1-2i)(1+2i)$ $=5-i-5=-i$,於是

$$5-i=(1-2i)(1+2i)-i,$$

且 $N(-i)<N(1+2i)$.

讀者試舉一例子，對照定理 1.1 ，證明 π 和 ρ 均非唯一。

定理1-7. 設 π 爲質數，且 $\pi\mid\alpha\beta$, 則 $\pi\mid\alpha$ 或 $\pi\mid\beta$.

若 $\pi\mid\alpha$ 則此定理成立。

設 $\pi\nmid\alpha$, 吾人欲證 $\pi\mid\beta$. 由定理 1.6, 可選取 δ,ρ 使

$$\alpha=\delta\pi+\rho,\qquad N\rho<N\pi.$$

且 $N\rho\neq 0$, (若 $N\rho=0$, 則 $\rho=0$, $\therefore\pi\mid\alpha$ 與假設矛盾)。故 $0<N\rho<N\pi$.

令 T 爲一切在 G 中具 $\alpha\xi+\pi\eta$ 形式且不爲零之數所成之集合。 $\rho=\alpha-\pi\delta\in T$。由 G 中模之性質(4)知: T 中每一元素皆有其模，且至少等於 1 。故 T 中必有一元素 $\gamma=\alpha\xi_0+\pi\eta_0$ 其模爲最小正數。今 $\rho=\alpha-\pi\delta\in T$ ，且其模小於 $N\pi$, 因 γ 之模爲最小，故 $N\gamma<N\pi$ 。下面吾人欲證 γ 爲一單位。

取 θ,ζ 使

$$\pi=\theta\gamma+\zeta;\qquad N\zeta<N\gamma.$$

因 $\zeta=\pi-\theta\gamma=\pi-\theta(\alpha\xi_0+\pi\eta_0)=\alpha(-\theta\xi_0)+\pi(1-\theta\eta_0)$, 假設 $N\zeta\neq 0$, 則 $\zeta\in T$ 且 $N\zeta<N\gamma$, 如此與前述“ $N\gamma$ 爲最小”產生矛盾，故 $N\zeta=0$ 且 $\pi=\theta\gamma$, $N\pi=N\theta\cdot N\gamma$ 。因 π 爲質數，故 θ 與 γ 必有一爲單位。但若 $N\theta=1$, 則 $N\pi=N\gamma$, 如此與 $N\pi>N\gamma$ 矛盾，故 θ 非單位，所以 γ 爲一單位。

因此 $\gamma=\alpha\xi_0+\pi\eta_0$ 爲一單位。於是

$$\alpha\beta\xi_0+\pi\beta\eta_0=\gamma\beta.$$

因由假設 $\pi\mid\alpha\beta$ 和 $\pi\mid\pi\beta\eta_0$, 故 $\pi\mid\gamma\beta$. 可寫成 $\gamma\beta=\pi\tau$, 而 $\tau\in G$. 於是 $\beta=\pi(\tau/\gamma)$. 因 $\tau/\gamma\in G$, 故 $\pi\mid\beta$.

欲證定理 1.5 對整數 G 仍爲眞確，吾人之討論方法與在 J 中是類似的。設 α 不爲整數，且不爲單位，令 $\alpha=\alpha_1\alpha_2$, 其中 $N\alpha_1>1$, $N\alpha_2>1$. 對 α_1 , α_2 重覆進行此步驟，而此過程必須在某個時候停止，否則， $N\alpha$ 便可寫成任意大於 1 之因數之乘積。故 $\alpha=\pi_1\cdots\pi_r$, 而 π_i 皆爲質數。若 α 亦可寫成 $\alpha=\sigma_1\cdots\sigma_t$ 而 σ_i 皆爲質數，於是由定理 1.7 知 $\pi_1\cdots\pi_r$ 中必有一數 π_i ,令其爲 π_1 ,

使$\sigma_1=\pi_1\epsilon_1$，其中ϵ_1爲一單位，於是

$$\pi_2\cdots\pi_r=\epsilon_1\sigma_2\cdots\sigma_t.$$

以上仿照在J中之證法，吾人可完成此證明。

最後討論到前一節提過而未證明的幾項敍述：H中僅有的單位爲1和-1，至於3，7，$1+2\sqrt{-5}$皆爲H中之質數。

若$\alpha=a+b\sqrt{-5}$，定義$N\alpha$爲$N\alpha=\alpha\bar{\alpha}=a^2+5b^2$，和前面一樣$N(\alpha\beta)=N\alpha N\beta$. 若且唯若$\alpha$爲一單位，則$N\alpha=1$；此證明和高斯整數之情形是一樣的。但$a^2+5b^2=1$只在$b=0$，$a=\pm1$時成立，故$H$中僅含二單位$\alpha=\pm1$.

欲證3爲一質數，假設$3=\alpha\beta$，而α，β皆非單位，亦即$N\alpha\neq1$，$N\beta\neq1$。因$9=N3=N\alpha\cdot N\beta$，則$N\alpha=N\beta=3$，故$a^2+5b^2=3$. 若$b\neq0$，則$a^2+5b^2>3$，故$b=0$. 但對任一J中元素a而言，$a^2=3$均無法成立，故3爲一質數。同理設$7=\alpha\beta$，$N\alpha\neq1$，$N\beta\neq1$，則$a^2+5b^2=7$. 若$b^2\neq0$，$b^2\neq1$，則$a^2+5b^2>7$. 故$b=0$，$a^2=7$或$b=\pm1$，$a^2=2$；但兩種情況皆不可能發生。

$1\pm2\sqrt{-5}$爲質數，因若$1\pm2\sqrt{-5}=\alpha\beta$，則$N(1\pm2\sqrt{-5})=N\alpha N\beta$於是$\alpha$或$\beta$爲單位，或$N\alpha=3$，或$N\beta=3$，但$N\alpha=3$與$N\beta=3$由前之討論知其爲不可能。

另有一整數集合之例，可滿足唯一因數分解，即具形式$a+b\omega$形式之數所成之集合，其中$\omega=\frac{1}{2}(-1+\sqrt{-3})$. 有興趣之讀者想了解其中細節的話，可參考Hardy和Wright合著之一本書之第七章內容，此章中有詳細之說明。

第二章 高斯質數

1.有理質數與高斯質數

對於有理質數（即 J 中之質數）之個數，吾人可建立一事實：有理質數之個數為無限。最簡單之證明，是由 Euclid所發現，如下所述：設 p_1，p_2，⋯ p_n 為已知質數。令 $N=1+p_1p_2\cdots p_n$，則對 p_1，p_2，⋯ p_n 而言，任一 p_i 皆不為 N 之因數，若非如此，則至少有一 p_i 使 $p_i \mid 1$ 成立，但此為不可能。故 N 之任何質因數皆不等於 p_1，p_2，⋯ p_n．因此吾人可得一結論：若已知有限個質數，則必存在一異於已知質數之質數。因此，若存在一已知質數，則其個數必為無限。但吾人既知 2 為質數，故上結論成立。

至於高斯質數，只要吾人能找到一質數，則上述之證明亦能適用於此。而前已證明 3為高斯質數，故 G 亦包含無限多質數。並且，吾人將明確地利用 J 中的質數來表示 G 中的質數，為達此目的，需要基本數論中的一些理論，為此吾人將探討比目前所需還多的理論，這些附加上的理論爾後將應用到，

2.同餘式（Congruences）

此節中吾人將就有理整數以討論。

令 m 為非零整數，a，b 為二整數，若 $m \mid (a-b)$，則稱 a,b 為**同餘模m**（congruent modulo m），記為

$$a \equiv b \pmod{m} \quad \text{或} \quad a \equiv b\ (m).$$

若 a，b 非同餘模 m，則記為 $a \not\equiv b\ (m)$．

由定理 1.1 知，每一整數 a 被 $|m|$ 除之，餘數為 r，$0 \le r < |m|$．吾人欲證：若且唯若 $a \equiv b\ (m)$，則 a，b 被 $|m|$ 除之，有相同之餘數。先設

$$a = q\,|m| + r, \quad b = q'\,|m| + r, \quad 0 \le r < |m|.$$