「抽象代數」真的抽象嗎？

沈淵源

February 14, 2011

「抽象代數」一詞是從英文的「abstract algebra」翻譯而來；作爲數學的一門學科，主要研究對象是代數結構，比如群(Groups)、環(Rings)、體(Fields)、模(Modules)、向量空間(Vector Spaces)和代數(Algebras)。這些代數結構，有的在十九世紀就已經有了正式的定義。這裡所謂的抽象(abstract)指的是純理論的，而不是一般所理解[1]「泛指籠統概括，難以想像」或是「具體」的相反詞。其實，「abstract」當成動詞乃是「提煉、萃取」；而當成名詞則爲「萃取物、摘要」。在此文中，我們要從不同的個例如整數集、實係數的多項式集等，萃取其中之所以得到唯一分解性的關鍵性質；進而將這些關鍵性質當成此等代數結構的公設(或公理)，由此建立並發展其上的理論架構。從這個層面上來看，正因爲已經剔除了其他不相關的性質，那麼就很容易會令人感覺到太抽象了(或有點抽象)、不容易理解。然而，這一切的一切都是由耳熟能詳、具體的例子當中所萃取出來的，絕非憑空想像得到；否則的話，整個建造出來的理論就不會有任何的應用價值。

[1]見教育部國語辭典簡編本【網路版】，網址爲
http://140.111.34.46/jdict/main/cover/main.htm

首先，我們利用眾所周知整數系$\mathbb{Z}$的唯一分解性來求出不定方程

$$x^2 + y^2 = z^2$$

所有的整數解；並依樣畫葫蘆地，求出不定方程

$$y^3 = x^2 + 2$$

所有的整數解。然而，若想繼續仿照此法；來算出不定方程

$$y^3 = x^2 + 23$$

的整數解，那可就要碰一鼻子灰了。因此，我們得回頭詳細考察之所以擁有唯一分解性之代數結構的關鍵性質爲何；如此一來，才能理解之所以碰了一鼻子灰的真正緣由。

爲了方便討論起見，我們接著簡要的介紹最簡單也最常見的幾個代數結構群、環、體以及一些常用的術語；然後再回到整數環$(\mathbb{Z}, +, \cdot)$當中討論跟整除性相關的一些性質，並歸結在唯一分解性上。其次，我們轉向一樣耳熟能詳的多項式環並且刻意作了一個平行的考察；同樣地，也歸結在唯一分解性上。顯而易見，這兩者當中有諸多的相似之處。有一股莫名的興奮湧上心頭，讓你無可抗拒地想要抽取當中之所以擁有唯一分解性的關鍵條件；再將這些關鍵性質當成此等代數結構的公設(或公理)，並發展其對應的理論。最後，回歸來時路；也就是前面所碰到的那些個別的實例$\mathbb{Z}[\sqrt{-2}]$以及$\mathbb{Z}[\sqrt{-23}]$，在這個地方看來，那只不過是上面所建立之理論的一個特例或推論而已。至此，大功告成；你說，「抽象代數」真的抽象嗎？

1 從畢達哥拉斯定理說起

打從國中開始，你就對畢達哥拉斯定理[2]瞭若指掌；不僅如此，其實你或快或慢可以脫口說出好幾個邊長爲整數的直角三角形如(3,4,5), (5,12,13), (7,24,25)等。

當然你會問，到底這樣子的直角三角形其個數有多少呢？聰明的你立刻回答說：有無窮多個！因爲對任意的正整數n, $(3n, 4n, 5n)$也是。但心理卻說：笨蛋，這還用問嗎？簡單極了！那麼爲了避開你的嘀嘀咕咕，我們就把這一類的算一個就是了；也就是說，我們假設三邊長爲整數且互質(亦即沒有公共的因子)。或許沉默幾分鐘之後，你會說：對任意的正偶數(爲何不要奇數？)n, 數串 $(n^2-1,\ 2n,\ n^2+1)$就是一個直角三角形彼此互質的三邊長。

其實，我們想知道的不僅僅是個數是否無限的問題而已；我們所要的乃是找出所有邊長爲整數的直角三角形。換句話說，我們要找出不定方程式

$$x^2 + y^2 = z^2$$

所有的整數解(x, y, z)。上面提到的，只不過暗示我們可將所要求的解簡化爲彼此互質的三元數(x, y, z)。當然，我們也只消求出正整數解即可。此等三元數通常稱之爲畢達哥拉斯原始三元數(primitive Pythagorean triples)，簡稱畢氏原始三元數又稱素勾股數。

所以我們現在的任務是求出所有的素勾股數。假設(x, y, z)就是這

[2]畢達哥拉斯定理(簡稱畢氏定理)，又稱勾股弦定理(簡稱勾股定理)；是幾何學上的一個基本定理，傳統上認爲是古希臘的畢達哥拉斯所證明。據說畢達哥拉斯證明了這個定理後，即斬了百頭牛慶祝，因此又稱百牛定理。在中國，《周髀算經》記載了勾股弦定理的一個特例，相傳是商代的商高發現，故又稱之爲商高定理。

樣子的一組素勾股數。首先，考慮奇偶性。對三元數(x,y,z)而言，共有8種不同的組合方式，如下表所顯示；這當中僅第三跟第五兩種組合是可能的素勾股數，而其他六種組合都是不可能發生的，其原因[3]列在最右側一欄(注意：平方之後奇偶性不會改變)。

序號	x或x^2	y或y^2	z或z^2	可能嗎？	原因
1	奇	奇	奇	否	奇＋奇＝偶
2	奇	奇	偶	否	見註解3
3	奇	偶	奇	✓	
4	奇	偶	偶	否	奇＋偶＝奇
5	偶	奇	奇	✓	
6	偶	奇	偶	否	偶＋奇＝奇
7	偶	偶	奇	否	偶＋偶＝偶
8	偶	偶	偶	否	三數不互質

然而，不定方程中的x,y是對稱的；這意味著，第三跟第五兩種組合可當成同一個來看待。因此之故，我們可假設x,z爲奇數而y則爲偶數；所以我們得到下面三個數

$$\alpha=\frac{z+x}{2},\quad \beta=\frac{y}{2},\quad \gamma=\frac{z-x}{2}$$

都是正整數，而且不難證明α,γ兩數彼此互質[4]。將原不定方程寫成

$$y^2=z^2-x^2=(z+x)(z-x)\Longrightarrow\left(\frac{y}{2}\right)^2=\frac{z+x}{2}\cdot\frac{z-x}{2},$$

[3]因爲奇數平方之後被4除餘1，但偶數平方之後被4除盡。

[4]因爲任何這兩個數的質因子p必整除這兩個數的和$(=z)$還有這兩個數的差$(=x)$，但這又導致p整除y($\because p\mid y^2=z^2-x^2\Longrightarrow p\mid y$)；因而$p$爲$x,y,z$的一個公因數，此與假設$(x,y,z)$是一組素勾股數不合。

因而得到這三個正整數的一個關係式如下：

$$\beta^2 = \alpha\gamma$$

根據算術基本定理[5]，不難看出α, γ兩者本身都是完全平方數[6]；也就是說，存在二正整數m, n使得

$$\alpha = m^2\,, \qquad \gamma = n^2\ 。$$

故得原先的畢達哥拉斯三元數爲

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2\ 。$$

至此，我們已經找出所有的素勾股數；不僅僅有無窮多組，更帥的是可用上面很簡單的公式表達出來。而其他的勾股數就是這些素勾股數的常數倍冠上自由選取的正負號，如此這般的我們得到不定方程式$x^2 + y^2 = z^2$所有的整數解。

【定理】　不定方程式$x^2 + y^2 = z^2$的整數解(x, y, z)如下：

$$x = \pm k(m^2 - n^2), \quad y = \pm k(2mn), \quad z = \pm k(m^2 + n^2)\,;$$

其中正負號可自由選取，k爲任意正整數；而m, n則爲一奇一偶彼此互質的兩個正整數。

下面網頁[7]中提供了一個Javascript計算器，用以計算這些數串；不妨試試如何。下表列出當m, n限制在10以內的情況下所有的素勾股數。

---

[5]任何正整數都可以寫成其質因數的乘積且此種表示法是唯一的。

[6]將這兩個數寫成質因數的乘積$\alpha = p_1^{a_1}\cdots p_k^{a_k}$, $\gamma = q_1^{b_1}\cdots q_k^{b_k}$。但$\alpha$與$\gamma$互質，因而得知這些質因數$p_i, q_j$必定兩兩互異，所以$\beta^2 = \alpha\gamma$的質因數乘積表示法就是$p_1^{a_1}\cdots p_k^{a_k} q_1^{b_1}\cdots q_k^{b_k}$;因此這些次冪$a_i, b_j$都是偶數，故得證$\alpha, \gamma$都是完全平方數。

[7]http://www.math.clemson.edu/~simms/neat/math/pyth/

n	m	(x,y,z)	n	m	(x,y,z)
1	2	(3, 4, 5)	3	8	(55, 48, 73)
1	4	(15, 8, 17)	4	5	(9, 40, 41)
1	6	(35, 12, 37)	4	7	(33, 56, 65)
1	8	(63, 16, 65)	4	9	(65, 72, 97)
2	3	(5, 12, 13)	5	6	(11, 60, 61)
2	5	(21, 20, 29)	5	8	(39, 80, 89)
2	7	(45, 28, 53)	6	7	(13, 84, 85)
2	9	(77, 36, 85)	6	9	(45, 108, 117)
3	4	(7, 24, 25)	7	8	(15, 112, 113)
3	6	(27, 36, 45)	8	9	(17, 144, 145)

2 求$y^3 = x^2 + 2$的整數解

在上一節中，我們稍稍的品嚐到算術基本定理的美妙滋味；這裡所用到的，說穿了其實就是整數的唯一分解性。現在讓我們依樣畫葫蘆，試著來找出不定方程

$$y^3 = x^2 + 2$$

所有的整數解。

假設$x, y \in \mathbb{Z}$滿足不定方程式$y^3 = x^2 + 2$, 並將此式寫成

$$y^3 = x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2}) \text{ 。}$$

很自然的，上式引導我們去思考長的像$a + b\sqrt{-2}$, $a, b \in \mathbb{Z}$之類的複數；在代數上，通常以符號$\mathbb{Z}[\sqrt{-2}]$表示之，故

$$\mathbb{Z}[\sqrt{-2}] = \{\, a + b\sqrt{-2} \mid a, b \in \mathbb{Z} \,\} \text{ 。}$$

這個集合$\mathbb{Z}[\sqrt{-2}]$跟整數集$\mathbb{Z}$有許許多多相似的地方。

首先，兩者都是複數集$\mathbb{C}$的子集；所以也都承繼了當中加法與乘法的運算，以及其上的一些代數結構。這兩個耳熟能詳的加、乘運算就是一般所謂的二元運算。更明確的說，集合S上的一個二元運算其實就是一個從$S \times S$到S的函數而已，

$$f : S \times S \to S \text{ 。}$$

所以集合S上面的兩個元素α, β經過f運算之後，得到的結果即函數值$f(\alpha, \beta)$仍然還是在集合S上。因此之故，當我們說這個運算具有封閉性，只不過爲了強調此點而已。習慣上，我們將運算符號寫在兩個元素的中間；所以

$$\alpha f \beta$$

指的就是$f(\alpha, \beta)$，就如同「和」與「積」我們習慣寫成$\alpha + \beta$與$\alpha \cdot \beta$而不是$+(\alpha, \beta)$與$\cdot(\alpha, \beta)$一樣的道理。

顯而易見，複數的加法與乘法運算在集合$\mathbb{Z}[\sqrt{-2}]$之中跟在整數集$\mathbb{Z}$之中一樣都具有封閉性；這是代數結構的第一步，其他的代數性質等下一節再詳細解說。當務之急乃是找出不定方程

$$y^3 = x^2 + 2$$

所有的整數解。如上所說，在集合$\mathbb{Z}[\sqrt{-2}]$中；上式可分解爲

$$y^3 = x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2}) \,,$$

而且也可證明右側的兩個數$x + \sqrt{-2}$與$x - \sqrt{-2}$彼此是互質的。假設$(\mathbb{Z}[\sqrt{-2}], +, \cdot)$跟整數系$(\mathbb{Z}, +, \cdot)$一樣擁有所需要的代數結構。因此唯一

分解性告訴我們，這兩個數本身都是複數集$\mathbb{Z}[\sqrt{-2}]$之中的完全立方數；也就是說，存在$a+b\sqrt{-2}\in\mathbb{Z}[\sqrt{-2}]$使得

$$x+\sqrt{-2}=(a+b\sqrt{-2})^3\ 。$$

將右式展開，整理後得到

$$x+\sqrt{-2}=(a^3-6ab^2)+(3a^2b-2b^3)\sqrt{-2}\,;$$

並比較等號兩側的虛部，得知

$$1=3a^2b-2b^3=(3a^2-2b^2)\,b\in\mathbb{Z}\ 。$$

因而得到

$$b=\pm1\quad 且\quad 3a^2-2b^2=\pm1\,;$$

故得

$$b^2=1\Longrightarrow 3a^2-2=\pm1\Longrightarrow 3a^2=2\pm1=3\,或1\ 。$$

因此，我們一定有

$$a^2=1\Longrightarrow a=\pm1\,;$$

再回到上面的展開式，得知

$$x=a^3-6ab^2=(\pm1)^3-6(\pm1)=\mp5\ 。$$

最後，將$x=\pm5$代回原不定方程

$$y^3=x^2+2\,;$$

故得$y=3$，因而原不定方程之整數解爲

$$x=\pm5\,,\qquad y=3\ 。$$

至此，我們已經成功地找到了兩個不定方程之整數解；第一個在上節，擁有無窮多組解；第二個就在上面，僅有兩組解。因爲是如此的成功，我們得打鐵趁熱一起來找出另一個不定方程式

$$y^3 = x^2 + 23$$

的整數解。如上，假設$x, y \in \mathbb{Z}$滿足不定方程$y^3 = x^2 + 23$;將此式寫成

$$y^3 = x^2 + 23 = (x + \sqrt{-23})(x - \sqrt{-23}) \text{ 。}$$

很自然的，我們工作的地方變成

$$\mathbb{Z}[\sqrt{-23}] = \{\, a + b\sqrt{-23} \,|\, a, b \in \mathbb{Z} \,\} \text{ 。}$$

不難證明右側的兩個數$x + \sqrt{-23}$與$x - \sqrt{-23}$彼此是互質的；因此這兩個數本身都是$\mathbb{Z}[\sqrt{-23}]$中的完全立方數；也就是說，在$\mathbb{Z}[\sqrt{-23}]$當中有某個數$a + b\sqrt{-23}$使得

$$x + \sqrt{-23} = (a + b\sqrt{-23})^3 \text{ 。}$$

將右式展開，整理後得到

$$x + \sqrt{-2} = (a^3 - 69ab^2) + (3a^2b - 23b^3)\sqrt{-23}\,;$$

並比較等號兩側的虛部，得知

$$1 = 3a^2b - 23b^3 = (3a^2 - 23b^2)\, b \in \mathbb{Z} \text{ 。}$$

因而得到

$$b = \pm 1 \quad \text{且} \quad 3a^2 - 23b^2 = \pm 1\,;$$

故得

$$b^2 = 1 \Longrightarrow 3a^2 - 23 = \pm 1 \Longrightarrow 3a^2 = 23 \pm 1 = 24 \text{或} 22 \text{。}$$

因此，我們一定有

$$a^2 = 8 \text{。}$$

顯而易見，沒有這樣子的整數存在；結論是，原不定方程

$$y^3 = x^2 + 23$$

無解。然而，隨便觀察即可得知原不定方程有整數解爲

$$x = \pm 2\,, \qquad y = 3 \text{。}$$

這到底是怎麼一回事呢？幾分鐘前，還悠然自得的沉醉在成功的高山上；怎麼才一下下的功夫而已，卻跌落至深不可測的山坳低谷裡。聰明的你，可告訴我？

3 代數結構簡介

爲了方便介紹所要學的代數結構，難免需要採用一些術語；雖說是單調乏味，在此盡可能用閒話家常的方式爲之，還請忍耐片刻。

我們接著談一個集合上之二元運算的種種性質。一個集合若是沒有任何的二元運算，那當然就沒什麼代數結構可言。這就好比在一個團體裡面，若當中兩兩彼此都沒有任何互動、沒有任何關係；那麼這樣子的一個團體只不過是互不相干的一些個體所成的一個集合體而已，沒有任何的結構可言。當然，這樣子的團體就沒有被研究的價值，因爲不可能具有任何的影響力。

令$*$爲集合S上的一個二元運算。

- 我們說運算$*$是可結合的(associative)；若

$$(a*b)*c = a*(b*c)\,, \qquad \forall a,b,c \in S\ 。$$

- 我們說運算$*$是可交換的(commutative)；若

$$a*b = b*a\,, \qquad \forall a,b \in S\ 。$$

- 元素$e \in S$稱之爲運算$*$的一個單位元素(identity element)；若

$$a*e = e*a = a\,, \qquad \forall a \in S\ 。$$

- 若集合S擁有運算$*$的一個單位元素e；則我們說元素$u \in S$在集合S中具有反元素(inverse)，如果存在$v \in S$使得

$$u*v = v*u = e\ 。$$

現在回到複數集$\mathbb{C}$。在$\mathbb{C}$中有兩個我們熟悉的二元運算加$+$與乘$\cdot$；就是這兩個二元運算使得複數集$\mathbb{C}$擁有豐富無比的代數結構。

(i) 加法運算$(+)$在複數集$\mathbb{C}$上具有封閉性(封)、結合性(結)並擁有單位元素$0+0i$(單)且每一元素$a+bi$都有反元素$(-a)+(-b)i$(反)，這就是所謂的群(group)的代數結構。

一般而言，集合S上的一個二元運算$*$；若滿足上述的封、結、單、反四個性質，我們就說S在運算$*$之下形成一個群或說$(S,*)$是一個群。如果運算$*$是可交換的；那麼理所當然，我們就說$(S,*)$是一個交換群(commutative group)。通常又稱爲阿貝爾群(abelian

group)，爲的是要紀念數學家阿貝爾[8]。複數集 $(\mathbb{C}, +)$ 在加法運算之下當然是一個阿貝爾群。

(ii) 乘法運算 $(\cdot)$ 在複數集 $\mathbb{C}$ 上具有封閉性、結合性並擁有單位元素 $1 + 0i$ 而且每一個非零元素 $a + bi \neq 0$ 都有反元素 $\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} i$，又乘法也有交換性；換句話說，$(\mathbb{C}\backslash\{0\}, \cdot)$ 也是一個阿貝爾群。

(iii) 這兩個運算，並不是獨立存在毫無關連的；其相關性就是所謂的乘法運算 $(\cdot)$ 對加法運算 $(+)$ 的分配律，即

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma\,, \qquad \forall \alpha, \beta, \gamma \in \mathbb{C}\ 。$$

這就是所謂的體 (field) 的代數結構。一般而言，擁有兩個二元運算 $*_1$, $*_2$ 的集合 S；若滿足如上述 $\mathbb{C}$ 之性質者，我們就說 S 在運算 $*_1$, $*_2$ 之下形成一個體或說 $(S, *_1, *_2)$ 是一個體。更明確的說，令 $*_1$, $*_2$ 爲集合 S 的兩個二元運算；我們說 $(S, *_1, *_2)$ 是一個體，若滿足下述三個性質：

(i) $(S, *_1)$ 是一個阿貝爾群。

(ii) $(S \setminus \{e_1\}, *_2)$ 也是阿貝爾群，此處 e_1 爲運算 $*_1$ 的單位元素。

(iii) 運算 $*_2$ 對運算 $*_1$ 的分配律成立：

$$a *_2 (b *_1 c) = (a *_2 b) *_1 (a *_2 c)\,, \qquad \forall a, b, c \in S\ 。$$

[8]尼爾斯·亨利克·阿貝爾（Niels Henrik Abel，1802 年—1829 年），挪威數學家，以證明五次元方程的根式解的不可能性而聞名。1825 年得到政府資助，遊學柏林和巴黎。生前不得志，無法獲得教席俾專心研究，最後因肺結核在挪威的弗魯蘭逝世。死後兩天，來自柏林的聘書才寄到家中。跟同樣早逝的伽羅華一同被奉爲群論的先驅。現代有以他名字命名的阿貝爾獎。

在我們所熟悉的例子當中，除了有理數體 $(\mathbb{Q},+,\cdot)$、實數體 $(\mathbb{R},+,\cdot)$ 以及複數體 $(\mathbb{C},+,\cdot)$ 之外；

$$(\mathbb{Q},+,\cdot)\subset(\mathbb{R},+,\cdot)\subset(\mathbb{C},+,\cdot)$$

還有那些介於有理數體及複數體之間許許多多的數體[9] (number fields)，更有那數也數不清擁有質數個數的有限體[10] $\mathbb{Z}_p$ (prime finite fields) 。

那我們前面的老朋友整數系 $(\mathbb{Z},+,\cdot)$ 又是怎麼樣的一付德性呢？萬事俱備，只欠東風；不過這個缺陷乃是先天的，無法補救。所缺的就是非零元素的乘法反元素除了 ±1 之外，都不存在。這就是所謂的環 (ring) 的代數結構。更明確的說，擁有兩個二元運算 $*_1$, $*_2$ 的集合 S；若滿足下述三個性質者，我們就說 S 在運算 $*_1$, $*_2$ 之下形成一個環或說 $(S,*_1,*_2)$ 是一個環。

(i) $(S,*_1)$ 是一個阿貝爾群。

(ii) 運算 $*_2$ 是可結合的。

(iii) 運算 $*_2$ 對運算 $*_1$ 的左、右分配律都成立：

$$a*_2(b*_1c)=(a*_2b)*_1(a*_2c)\,,\qquad\forall a,b,c\in S\,,$$

$$(b*_1c)*_2a=(b*_2a)*_1(c*_2a)\,,\qquad\forall a,b,c\in S\,。$$

習慣上，我們把環裡面的第一個運算稱之爲加法，用符號「$+$」來表示；而第二個運算則稱之爲乘法，用符號「$\cdot$」來表示。因此，我們也習慣將第一個運算的單位元素稱之爲加法單位元素且用「0」來表示；

[9]這些體可看成是佈於有理數體的向量空間，若其維數是有限的就稱之爲數體。

[10]當然也有非質數個數的有限體，但其個數必定是某一質數的次冪。

而第二個運算的單位元素，若存在則稱之爲乘法單位元素且用「1」來表示。記住，這只是一個習慣用法；所以當你看到在一個環或體裡面的0(或1)，那指的就是加法單位元素0(或乘法單位元素1)，而跟整數裡的0(或1)一點關係也沒有。

當然啦，整數環$(\mathbb{Z},+,\cdot)$遠比一般的環還好很多；那就是第二個運算不僅有單位元素而且還是可交換的，這一種環通常稱之爲具乘法單位元素的交換環(commutative ring with unit)。與此相對的有佈於實數體的n階方陣環$(\mathrm{M}_n(\mathbb{R}),+,\cdot)$，這是一個擁有乘法單位元素的非交換環(noncommutative ring with unit)；還有那偶整數環$(2\mathbb{Z},+,\cdot)$則是不具乘法單位元素的交換環(commutative ring without unit)。

其實，整數環還有更細膩的性質；譬如說，任何兩個非零元素相乘還是非零元素。這就是所謂的整域(integral domain)[11]的代數結構。一般的環，如$\mathbb{Z}_6$就包含有非零元素2及3相乘之後等於零；還有矩陣環中，

$$\begin{pmatrix} 7 & 11 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 11 \\ 0 & -7 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

也有類似的現象發生(這樣子的非零元素就是所謂的零因子)。

總而言之，整數環既然擁有如此多采多姿的面貌；那就值得我們打著燈籠，再一次聚精會神的來把這位交往多年的老朋友瞧個仔細。

4 整數的唯一分解性

現在回到小學生所學的整數$\mathbb{Z}$，包括正整數、負整數及零；當然對負數的理解得等到高年級的時候才比較成熟，因此讓我們先停留在自然

[11]沒有零因子的交換環就稱爲整域。

數(即正整數)上且做一回的小小學生。數學家克羅內克L. Kronecker[12]曾說：「上帝創造了自然數，其餘都是人的工作。」其實他對上帝的認識，不僅太膚淺而且層次不高。上帝的創造，除了大自然外還有許許多多的活物；而其創造的最高峰乃是按著祂自己形像、樣式所造的人，所以人只不過是上帝的傑作而已。

這裡實在是有太多的東西好講，在此只能談談與代數結構相關的部分。先從整除性說起。我們說一個數a整除一個數b，如果有一個數c使得

$$b = ac\,;$$

而以符號$a \mid b$表示之。換句話說，a除b之後沒有餘數。a稱爲b的一個因子，而b則稱爲a的一個倍數。例如：$6 \mid 12,\ (-14) \mid 98,\quad$然而$7 \nmid 11$。

若給你一個數，你就試著要把這個數分解成兩個數的乘積；還不夠，那就再分解，一直到沒辦法再分解爲止。此乃基於小數容易掌控的心理罷！如

$$360 = 36 \times 10 = 6 \times 6 \times 2 \times 5 = 2 \times 3 \times 2 \times 3 \times 2 \times 5\,。$$

不能再分解的數就是所謂的質數(prime numbers)。更明確的說，一個數$p > 1$稱之爲質數；若此數僅有的因子爲1及p。質數是非常的重要，如下面主要定理所顯示的；對乘法而言，質數乃是建造整數的磚塊，是整數當中最基本的元素。

[12]利奧波德·克羅內克(Leopold Kronecker，1823年12月7日－1891年12月29日)，德國數學家與邏輯學家，出生於利格尼茨(現屬波蘭的萊格尼察)，卒于柏林。他認爲算術與數學分析都必須以自然數爲基礎。這與數學家喬治·康脫(Georg Cantor)的觀點相互對立。克羅內克是恩斯特·庫默爾(Ernst Kummer)的學生和終身摯友。

也許你會說，所有這些東東我老早就知道了；沒什麼新奇的，簡直無聊透頂。那麼，我請問你；你雖然知道質數有無窮多個，但你可知道

「目前已知最大的質數是多少嗎？」

答案當然不是「要有多大就有多大」，爲什麼呢？想想看，隨便給你一個整數，你能馬上回答此數就是質數嗎？也許你說：給我些許時間我就可以給你答案。好吧！那你就隨便挑一個一百位數，再試試看如何？其實，你的知道只是理論上的知道，而不是實作上的知道。判斷一個整數是否爲質數乃是一個大挑戰，但已被證實存在有演算法，可在多項式時間內完成 [1]。在此先介紹兩類有趣的質數：梅仙質數 (Mersenne Primes) 及費馬質數 (Fermat Primes)。

- 梅仙質數：形如 $M_p = 2^p - 1$ 的質數稱之爲梅仙質數。此類質數與完全數有關，目前已知最大的質數就是這一類的質數爲

  $$2^{43112609} - 1。$$

  這是已被發現的第四十五個 (按時間順序) 梅仙質數，是一個擁有約一千三百萬 12,978,189 位數的龐然大數；由 GIMPS[13] 團隊於 2008

[13] 乃 The Great Internet Mersenne Prime Search 的縮寫，這是此大搜索團隊所發現的第 11 個。巧的是，無獨有偶；才隔了兩個禮拜 (2008 年 9 月 6 日)，在德國科隆 (Cologne) 附近 Langenfeld 的 Hans-Michael Elvenich 又發現第四十六個。不過，比上面那一個小；爲 $2^{37156667} - 1$。七個月後，2009 年 4 月 12 日又發現第四十七個，還是比上面那一個小；爲 $2^{42643801} - 1$。最大梅仙質數發現之前的三個是 $2^{32582657} - 1$, $2^{30402457} - 1$ 與 $2^{25964951} - 1$ 分別在 2006 年 9 月 4 日，2005 年 12 月 15 日與 2005 年 2 月 18 日發現。詳情請進入其網站，網址爲 http://www.mersenne.org。

年8月23日在美國洛杉磯UCLA數學系的一部電腦發現，Edson Smith是負責安裝及維護GIMPS軟體於其上的人。在此特別推薦克瑞斯·迦爾德威爾(Chris K. Caldwell)所精心設計的質數網頁[7]，值得進去遨遊一番。

- 費馬質數：形如$F_n = 2^{2^n} + 1$的質數稱之爲費馬質數。前面五個費馬質數爲

$$F_0 = 3\,,\ F_1 = 5\,,\ F_2 = 17\,,\ F_3 = 257 \text{ 與 } F_4 = 65537\,。$$

當年費馬因此推斷所有這一類型的數都是質數，但奇怪的是，這五個數是目前僅有的費馬質數。於是有人猜測說：僅存在有限多個費馬質數。你認爲呢？

與質數相關的趣事，還有一籮筐；值得提的，至少有底下兩個響叮噹的猜測：孿生質數猜測(Twin Prime Conjecture)及哥德巴赫猜測(Goldbach Conjecture)。

- 孿生質數猜測：即使從小質數表觀察，不難察覺有如下的質數對出現

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ \cdots;$$

稱之爲孿生質數。此種孿生質數是否有無窮多呢？答案是，不知道。等你來解決！

- 哥德巴赫猜測：是否每一個大於2的偶數都可以寫成兩個奇質數的和呢？這就是名滿天下哥德巴赫猜測；即使有電腦侍候在旁的今天，至今尚未找到反例，是數論中存在最久的未解問題之一。目

前，這方面的進展還是停留在1937年維諾格拉朵夫(Vinogradov)所證明的結果[14]還有陳景潤在1966年的結果[15]。

這裡我們要專注在數的乘法結構上，此間最主要定理可追溯到歐幾里得的年代；這就是唯一分解性定理，通常稱之爲算術基本定理。因有甚多與整數相關的重要結果，都是由它推論而來；故冠此頭銜，也是理所當然，更是實至名歸。這定理簡單說就是，每一個數可唯一寫成其質因子的乘積。譬如說，$360 = 2 \times 3 \times 2 \times 3 \times 2 \times 5 = 2^3 \times 3^2 \times 5$。唯一指的是，其質因子爲2, 3及5而其次冪分別是3, 2及1；這些數乃是由360所唯一決定的。

必須一提的是所謂的良序原理(Well-Ordering Principle)，此原理乃是自然數最基本的假設；跟數學歸納法原理(Principle of Mathematical Induction)是等價的，在很多的場合我們需要此二老的幫忙。

【良序原理】 任何正整數的非空集合必擁有一最小的元素。

【數學歸納法原理】 令$P(n)$是一個與整數有關的敘述使得$P(n_0)$成立且[16]對所有整數$n_0 \le j \le k$, $P(j)$成立$\Longrightarrow P(k+1)$也成立。則對所有的整數$n \ge n_0$, $P(n)$都成立。

現在回到整數環$\mathbb{Z}$來，因爲在這兒工作比較方便一些。整除的觀念暢行無阻，甚至於連文字都不需修改；只消把那邊的「數」，理解成整

[14]他證明了：「每一個足夠大的奇數可以寫成三個奇質數的和。」

[15]他證明了：「任何一個足夠大的偶數，都可以寫成兩個數的和；其一爲奇質數，另一則爲奇質數的乘積其個數不超過2。」(簡稱「1+2」)此乃哥德巴赫猜想研究上的里程碑，而他所發表的成果也被稱之爲陳氏定理。

[16]這是比較一般化的版本；通常的版本，我們取$n_0 = 1$而此處的條件也可取代爲：對某一整數$k \ge n_0$, $P(k)$成立$\Longrightarrow P(k+1)$也成立。

數即可。質數的觀念也是一樣，變成多出來負質數而已。底下我們列出來一些整除性的基本性質，得勞駕動動手將這些簡單的證明完成。

1. $a \mid a\,, \quad \forall a \neq 0$ （反身律）
2. $a \mid b$ 且 $b \mid c \Longrightarrow a \mid c$ （遞移律）
3. $a \mid b$ 且 $a \mid c \Longrightarrow a \mid mb + nc$ （線性律）
4. $a \mid b \Longrightarrow ma \mid mb$ （乘法律）
5. $ma \mid mb$ 且 $m \neq 0 \Longrightarrow a \mid b$ （消去律）
6. $\pm 1 \mid a$ （± 1 整除每一個數）
7. $a \mid 0$ （每個數都整除零）
8. $0 \mid a \Longrightarrow a = 0$ （唯零整除零）
9. $a \mid b$ 且 $b \neq 0 \Longrightarrow |a| \leq |b|$ （比較律）
10. $a \mid b$ 且 $b \mid a \Longrightarrow |a| = |b|$
11. $a \mid b$ 且 $a \neq 0 \Longrightarrow (b/a) \mid b$

令 $n \in \mathbb{Z}$ 且令 p 爲一質數。則若 $n \neq 0$，必存在一非負整數 a 使得

$$p^a \mid n \qquad \text{但} \quad p^{a+1} \nmid n \,。$$

這個 a 就稱之爲 n 在質數 p 的階數 (the order of n at p), 以符號 $\mathrm{ord}_p n$ 表示之。粗略言之，$\mathrm{ord}_p n$ 就是 p 整除 n 的次數。若 $n = 0$，則我們定義 $\mathrm{ord}_p n = \infty$。注意到，另一個極端爲

$$\mathrm{ord}_p n = 0 \Longleftrightarrow p \nmid n \,。$$

因此對一個非零整數n而言，只有在其質因子的階數會是正的；而在其他不整除n的質數，其階數則全部都是0。

接著我們逐步預備好要證明算術基本定理(Fundamental Theorem of Arithmetic)的工具。首先處理存在性的部分，這只是良序原理或數學歸納法原理的一個簡單練習而已。按慣例，應該勞駕您動動手將這簡單的證明完成才是；然而爲了完全起見，特別附上兩個不同的論證方式提供初學者參考。

【引理1】　任何非零整數都可以寫成質數的乘積。

【證明一】　若否，則下列集合爲非空集合

$$S = \{x \in \mathbb{N} \mid x\text{不是質數的乘積}\} \neq \varnothing。$$

良序性告訴我們，S擁有一最小的正整數s；故s本身不是質數，因此我們有$s = mn$,　此處　$1 < m, n < s$。然而，m, n都是比s小的正整數；因而都是質數的乘積，所以s也是質數的乘積。矛盾出現，故得證。

【證明二】　僅需證明≥ 2的正整數可寫成質數的乘積。

(i) 2是一個質數。

(ii) 假設$2 < N$且假設對所有介於2與N的整數都可寫成質數的乘積。若N是質數，則證明完畢；否則我們有

$$N = mn, \quad \text{此處} \quad 2 \leq m, n < N。$$

然而，假設告訴我們；m, n都是質數的乘積，所以N也是質數的乘積。據數學歸納法原理，故得證。

物以類聚，將同一質數擺在一起；我們可以將一個整數n寫成$n = p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$,其中$p_i$爲質數且$a_i$爲正整數。我們會採用底下更方便的方式來表達：

$$n = (-1)^{\mathrm{sgn}(n)}\prod_p p^{a(p)}\,,$$

此處$\mathrm{sgn}(n) = 0$或1隨著n的正、負來決定，而乘積中的p是對所有的質數。次冪$a(p)$乃是非負整數；當然，除了有限多個質數外，此次冪都是零。譬如說，前面所看到過的那個數$n = 360$；我們有$\mathrm{sgn}(n) = 0\,,\ a(2) = 3\,,\ a(3) = 2\,,\ a(5) = 1\,$,而其餘的$a(p) = 0$。

【算術基本定理】對任何非零整數n存在一質數分解式

$$n = (-1)^{\mathrm{sgn}(n)}\prod_p p^{a(p)}\,,$$

其次冪由n所唯一決定。實際上，我們有$a(p) = \mathrm{ord}_p\, n$。

【引理2】若$a, b \in \mathbb{Z}$且$b > 0$，則$\exists q, r \in \mathbb{Z}$使得

$$a = qb + r\,, \qquad \text{其中} \quad 0 \le r < b。$$

【證明】　考慮集合S如下：$S = \{a - xb \mid x \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$。顯而易見，$S$爲非空集合；良序性告訴我們，$S$擁有一最小的非負整數$r$，故有一整數$q$使得$0 \le r = a - qb$。我們必須證明$r < b$。若否，則

$$r = a - qb \ge b \Longrightarrow 0 \le r - b = a - (q+1)b < r\,;$$

因而得到在S中比r還小的非負整數$r - b$, 這跟r的身分不合，故得證。

引理2就是所謂的長除法(long division)，又稱爲歐幾里德演算法(Euclid's Algorithm)；雖然不醒眼，卻是相當關鍵的性質。多項式環也

具有這個性質。所以談完多項式環的唯一分解性後，我們會將此性質抽象化；而滿足此等性質的整域，理所當然就稱爲歐幾里德整域(Euclidean Domains)。歐幾里德整域也同樣會具有唯一分解性。

【定義】　若$a_1, \cdots, a_n \in \mathbb{Z}$，定義集合$(a_1, \cdots, a_n)$爲

$$(a_1, \cdots, a_n) = \{a_1x_1 + \cdots + a_nx_n \mid x_1, \cdots, x_n \in \mathbb{Z}\}\ 。$$

令$I = (a_1, \cdots, a_n)$。顯而易見，這個集合在加法與減法之下都具有封閉性；亦即，任何I裡頭的兩個元素的和或差仍然還是裡頭的元素。不僅如此，若將裡頭的元素乘上任何的整數仍然還是裡頭的元素。也就是說，不管你的整數來源如何；或在I裡頭，或不在I裡頭；一旦乘上I裡頭的元素，就會被吸入，成爲裡頭的一份子。在環論的術語，這就是所謂的理想；因此I是整數環$\mathbb{Z}$中的一個理想。

【引理3】　若$a, b \in \mathbb{Z}$，則存在$d \in \mathbb{Z}$使得$(a, b) = (d)$。

【證明】　若$a = b = 0$，那麼樣就沒甚好證的；故假設a, b不全爲零，因而$S = (a, b) \cap \mathbb{N} \neq \varnothing$。良序性告訴我們，$S$擁有一最小的正整數$d$。顯而易見，$(d) \subseteq (a, b)$；我們必須證明，反方向$(a, b) \subseteq (d)$也對。

假設$x \in (a, b)$。引理2告訴我們，存在$q, r \in \mathbb{Z}$使得

$$x = qd + r\,, \qquad \text{其中} \quad 0 \leq r < d\,。$$

顯而易見，$r = x - qd \in (a, b)$；因此$0 \leq r < d$及d是(a, b)裡最小的正整數，讓我們看見$r = 0$是唯一的歸宿。所以得到$x = qd \in (d)$, 故得證。

【定義】 令$a, b \in \mathbb{Z}$。d稱之爲a與b的一個最大公因數；若

(i) d是a與b的公因數，

(ii) 任何其它a與b的公因數都整除d。

特別注意到，定義中說的是一個最大公因數。那到底有幾個呢？若c是另一個，那麼我們就必定有

$$c \mid d \qquad \text{且} \qquad d \mid c,$$

因而$c = \pm d$。故兩個整數的最大公因數，若存在，就剛剛好有兩個，其間只差一個符號。通常用符號$\gcd(a,b)$來表示那個正的最大公因數。

【引理4】 令$a, b \in \mathbb{Z}$。若$(a,b) = (d)$，則d是a與b的一個最大公因數。
【證明】(i) 因爲$a, b \in (a,b) = (d)$，故d是a與b的公因數。
(ii) 假設c是a與b的公因數。因此c整除任何a與b的線性組合，而$d \in (d) = (a,b)$就是a與b的一個線性組合；故$c \mid d$。

這就是最大公因數的存在性定理。有兩點值得一提：

(i) 上面的證明方法，雖說是簡潔漂亮，但美中不足的是；在整個證明的過程當中，我們看不到怎麼去找x與y的蛛絲馬跡。請參閱密碼學之旅[8]第二章數論輕鬆遊中所提出的三個計算最大公因數的演算法。

(ii) 注意到，此d在(a,b)中是最小的正整數；但卻是a與b的最大公因數，值得回味。

【定義】 我們說整數a與b是互質的；若其僅有的公因數只有± 1，整數中的可逆元素。

【定理Z】 假設$a \mid bc$而且$\gcd(a,b) = 1$, 則$a \mid c$。

【證明】　因$\gcd(a,b)=1$，存在$x,y\in\mathbb{Z}$使得

$$xa+yb=1\text{。}$$

兩邊同時乘上c，得到

$$xac+ybc=c\text{。}$$

根據假設$a\mid bc$，得知a整除上式左側的每一項；因此

$$a\text{整除左側}=\text{右側}=c\,,$$

故得證。

【推論1】　若p爲質數且$p\mid bc$，則 $p\mid b$ 或 $p\mid c$。

【證明】　因p爲質數，僅有的因數爲$\pm1,\pm p$；故得

$$\gcd(p,b)=p\qquad\text{或}\qquad\gcd(p,b)=1\text{。}$$

因此我們有

(i) $\gcd(p,b)=p$ ：　因$\gcd(p,b)\mid b\Longrightarrow p\mid b\,,$

(ii) $\gcd(p,b)=1$ ：　定理$\mathrm{Z}\Longrightarrow p\mid c\,;$

故得證。若將推論1寫成其反逆敘述，則有

【推論1′】　若p爲質數滿足$p\nmid b$ 且 $p\nmid c$，則$p\nmid bc$。

【推論2】　假設p是一個質數而且$a,b\in\mathbb{Z}$。則

$$\operatorname{ord}_p ab=\operatorname{ord}_p a+\operatorname{ord}_p b\text{。}$$

【證明】　令 $\alpha = \mathrm{ord}_p\, a$ 且令 $\beta = \mathrm{ord}_p\, b$。則

$$a = p^{\alpha}a' \quad \text{且} \quad b = p^{\beta}b'\,; \quad \text{其中 } p \nmid a' \quad \text{且} \quad p \nmid b'。$$

因此我們有

$$ab = p^{\alpha+\beta}a'b'\,, \quad \text{其中 } p \nmid a'b' \ (\text{推論 } 1')\,;$$

所以　$\mathrm{ord}_p\, ab = \alpha + \beta,$　故得證。

至此，準備工作完成；回到唯一分解性之證明。

【算術基本定理之證明】　引理 1 已經證明，對任何非零整數 n 存在一質數分解式

$$n = (-1)^{\mathrm{sgn}(n)} \prod_p p^{a(p)} \ 。$$

兩邊同時取 ord_q，並使用推論 2；我們有

$$\mathrm{ord}_q\, n = \mathrm{sgn}(n)\mathrm{ord}_q(-1) + \sum_p a(p)\mathrm{ord}_q(p) \ 。 \tag{1}$$

根據 ord_q 之定義，我們有

$$\mathrm{ord}_q(-1) = 0 \qquad \text{且} \quad \mathrm{ord}_q(p) = \begin{cases} 1 & \text{若} p = q \\ 0 & \text{若} p \neq q \end{cases} 。$$

所以實際上，(1) 式的右側僅剩單一的一項 $a(q)$ 沒有陣亡；我們有 $\mathrm{ord}_q\, n = a(q)$，故得證。

5　多項式的唯一分解性

現在我們轉移焦點至多項式環 $k[x]$；此處 k 是一個體，其中加法與乘法的單位元素分別是 0 與 1。若感覺太抽象，不妨將 k 看成是有理數體

$(\mathbb{Q},+,\cdot)$、實數體$(\mathbb{R},+,\cdot)$或複數體$(\mathbb{C},+,\cdot)$。

多項式$k[x]$上的加法與乘法是你所熟悉的。因此你老早就已經知道：

(i) $(k[x],+)$形成一個阿貝爾群，零多項式0就是加法單位元素。

(ii) 乘法$\cdot$具有結合律、交換律，常數多項式1就是乘法單位元素。

(iii) 乘法$\cdot$對加法$+$的分配律成立。

因此，$(k[x],+,\cdot)$跟整數環一樣；也是一個擁有乘法單位元素的交換環，但可逆元素(units)則包含所有的非零常數多項式。

我們可定義多項式環$k[x]$中整除性如同跟整數環一樣；唯一需要變的就是把「(整)數」改成「(多項)式」。我們說一個多項式a整除一個多項式b，如果有一個多項式c使得

$$b = ac\,;$$

而以符號$a|b$表示之。換句話說，a除b之後沒有餘式(remainder)。a稱爲b的一個因式(divisor)，而b則稱爲a的一個倍式(multiple)。例如：$x+1 \mid x^2-1,\ -x^2+x-1 \mid x^3-1$，然而$x^2+1 \nmid x^3+1$(不整除)。

與整除性相關的是分解性。數(式)分解成較小(低)數(式)的乘積，其大小就是絕對值(次數)的大小。多項式的次數(degree)通常用符號$\deg a$來表示，其中最重要的性質爲

$$\deg ab = \deg a + \deg b\,,\quad \deg a = 0 \Longleftrightarrow a \text{爲非零常數多項式}\ 。$$

前面所列出關乎整除性的11個基本性質在多項式裡頭也都成立；當然性質6中的「±1」得改成多項式裡頭的可逆元素「非零常數多項式」，而性質9及性質10的絕對值則改爲多項式裡頭的次數。

質數的觀念在多項式裡頭也相仿，當然稱爲質多項式或簡稱爲質式(irreducible polynomials)；意指不可再分解的多項式。更明確的說，一個非常數多項式p稱之爲質多項式如果$q \mid p$導致q爲常數多項式或爲p的常數倍。

爲了方便起見，我們定義首項係數(即領導係數leading coefficient)爲1的多項式爲首一多項式(monic polynomial)。譬如說，多項式

$$x^2 + 7x - 11 \qquad 及 \qquad x^4 - 3x^2 + 9x - 19$$

都是首一多項式但$7x^2 - 11$ 及 $3x^4 + 9x - 19$都不是。

令$a \in k[x]$且令p爲首一質式。則若$a \neq 0$，必存在一非負整數α使得(因爲p之次冪的次數越來越大)

$$p^\alpha \mid a \qquad 但 \quad p^{\alpha+1} \nmid a \text{。}$$

這個α就稱之爲a在質式p的階數(the order of a at p), 以符號$\operatorname{ord}_p a$表示之。粗略言之，$\operatorname{ord}_p a$就是p整除a的次數。若$a = 0$，則我們定義$\operatorname{ord}_p a = \infty$。注意到，另一個極端爲

$$\operatorname{ord}_p a = 0 \Longleftrightarrow p \nmid a \text{。}$$

接著我們逐步預備好要證明多項式版本之算術基本定理的工具。首先處理存在性的部分，同樣地這只是數學歸納法原理的一個簡單練習而已。按慣例，得勞大駕動動手將這簡單的證明完成；但需注意的乃是，要對多項式的次數作數學歸納法。

【引理1】　任何非零多項式都可以寫成質式的乘積。

注意到，每一個多項式都可以寫成其領導係數跟一個首一多項式的乘積；而質式經此手續後，就變成其領導係數跟一個首一質式的乘積。物以類聚，將同一個首一質式擺在一起；我們可以將一個多項式 f 寫成 $f = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$,其中 p_i 爲首一質式且 a_i 爲正整數。我們會採用底下更方便的方式來表達： $f = c\prod_p p^{a(p)}$， 此處 c 爲 f 之領導係數，而乘積中的 p 是對所有的首一質式。次冪 $a(p)$ 乃是非負整數；當然，除了有限多個首一質式外，此次冪都是零。

【算術基本定理(多項式版本)】 對任何非零多項式 f 存在一質式分解式

$$f = c\prod_p p^{a(p)},$$

此處 c 爲 f 之領導係數，而乘積中的 p 是對所有的首一質式；其次冪由 f 所唯一決定。實際上，我們有 $a(p) = \operatorname{ord}_p f$。

【引理2】 若 $a, b \in k[x]$ 而且 $\deg b > 0$，則存在 $q, r \in k[x]$ 使得

$$a = qb + r, \qquad \text{其中} \quad \deg r < \deg b \ \text{ 或 } \ r = 0。$$

【證明】 因爲零多項式的次數沒有定義，所以很自然的，我們必須分成兩種情況來討論。

(i) $b \mid a$: 令 $q = a/b$。則 $a = qb + r$, $r = 0$ ；故得證。

(ii) $b \nmid a$: 令 $r = a - qb$ 爲形如 $a - ub$, $u \in k[x]$ 的多項式中擁有最低次數者。我們必須證明 $\deg r < \deg b$。若否，令 r 與 b 之最高次項分別爲 $r_d x^d$ 與 $b_m x^m$ 。則

$$r - r_d b_m^{-1} x^{d-m} b = a - (q + r_d b_m^{-1} x^{d-m}) b$$

爲形如$a-ub,\ \ u\in k[x]$的多項式，卻擁有比r還小的次數；矛盾也，故得證。

引理2就是多項式裡頭的長除法，其證明過程當然也用到了自然數的良序原理。這裡比的是次數的大小，而上一節比的是絕對值的大小。

【定義】若$a_1,\cdots,a_n\in k[x]$，定義多項式集合$(a_1,\cdots,a_n)$爲

$$(a_1,\cdots,a_n)=\{a_1u_1+\cdots+a_nu_n\mid u_1,\cdots,u_n\in k[x]\}\ 。$$

令$I=(a_1,\cdots,a_n)$。顯而易見，這個集合在加法與減法之下都具有封閉性；亦即，任何I裡頭的兩個元素的和或差仍然還是裡頭的元素。不僅如此，若將裡頭的元素乘上任何的多項式仍然還是裡頭的元素。也就是說，不管你的整數來源如何；或在I裡頭，或不在I裡頭；一旦乘上I裡頭的元素，就會被吸入，成爲裡頭的一份子。在環論的術語，這就是所謂的理想；因此I是多項式環$k[x]$的一個理想。

【引理3】若$a,b\in k[x]$，則存在$d\in k[x]$使得$(a,b)=(d)$。

【證明】　若$a=b=0$，那麼樣就沒甚好證的；故假設a,b不全爲零，因而$(a,b)\neq\{0\}$。令$d\in(a,b)$爲當中次數最小的一個多項式。顯而易見，$(d)\subseteq(a,b)$；我們必須證明，反方向$(a,b)\subseteq(d)$也對。

假設$x\in(a,b)$。引理2告訴我們，存在$q,r\in k[x]$使得

$$x=qd+r\,,\qquad \text{其中}\quad \deg r<\deg d\ \text{ 或 }\ r=0。$$

顯而易見，$r=x-qd\in(a,b)$。若$r\neq0$，則r爲(a,b)中次數比d還小的一個多項式；此乃一矛盾，因此$r=0$是唯一的歸宿。所以得到$x=qd\in(d)$, 故得證。

【定義】令$a,b\in k[x]$。d稱爲a與b的一個最高公因式；若

(i) d是a與b的公因式，

(ii) 任何其它a與b的公因式都整除d。

特別注意到，定義中說的是一個最高公因式。那到底有幾個呢？若c是另一個，那麼我們就必定有

$$c \mid d \qquad \text{且} \qquad d \mid c,$$

因而$\deg c = \deg d$。故兩個多項式的最高公因式，若存在；任意兩個都會有相同的次數，其間就差一個常數倍。其中那個首一最高公因式，通常我們用符號$\gcd(a,b)$來表示。

【引理4】 令$a, b \in \mathbb{Z}$。若$(a,b) = (d)$，則d是a與b的一個最高公因式。

【證明】(i)因爲$a, b \in (a,b) = (d)$，故d是a與b的公因式。
(ii)假設c是a與b的公因式。因此c整除任何a與b的線性組合，而$d \in (d) = (a,b)$就是a與b的一個線性組合；故$c \mid d$。

這就是最高公因式的存在性定理。在實作中，我們通常使用輾轉相除法來計算。

【定義】 我們說多項式a與b是互質的；若其僅有的公因式只有非零常數，即多項式中的可逆元素。換句話說，$\gcd(a,b) = 1$。

【定理P】 假設$a \mid bc$而且$\gcd(a,b) = 1$，則$a \mid c$。

【證明】 因$\gcd(a,b) = 1$，存在$x, y \in k[x]$使得

$$xa + yb = 1\ 。$$

兩邊同時乘上c，得到

$$xac + ybc = c \text{ 。}$$

根據假設$a \mid bc$，得知a整除上式左側的每一項；因此

$$a \text{ 整除左側 } = \text{ 右側 } = c \text{ ，}$$

故得證。

【推論1】　若p爲質式且$p \mid bc$，則$p \mid b$或$p \mid c$。

【證明】　因p爲質式，故得

$$\gcd(p, b) = p \qquad \text{或} \qquad \gcd(p, b) = 1 \text{。}$$

因此我們有

(i) $\gcd(p, b) = p$ ：　因$\gcd(p, b) \mid b \Longrightarrow p \mid b$,

(ii) $\gcd(p, b) = 1$ ：　定理P $\Longrightarrow p \mid c$;

故得證。

若將推論1寫成其反逆敘述，則有

【推論1′】　若p爲質式滿足$p \nmid b$ 且 $p \nmid c$，則$p \nmid bc$。

【推論2】　假設p是首一質式而且$a, b \in k[x]$。則

$$\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b \text{。}$$

【證明】　令 $\alpha = \operatorname{ord}_p a$ 且令 $\beta = \operatorname{ord}_p b$。則

$$a = p^{\alpha} a' \quad \text{且} \quad b = p^{\beta} b' ; \quad \text{其中 } p \nmid a' \quad \text{且} \quad p \nmid b' \text{。}$$

因此我們有

$$ab = p^{\alpha+\beta}a'b', \quad \text{其中 } p \nmid a'b' \ (\text{推論 } 1');$$

所以得證

$$\operatorname{ord}_p ab = \alpha + \beta \ 。$$

至此，準備工作完成；回到唯一分解性之證明。

【多項式版本的算術基本定理之證明】 引理 1 已經證明，對任何非零多項式 f 存在一質數分解式 $f = c\prod_p p^{a(p)}$。兩邊同時取 ord_q，並使用推論 2；我們有

$$\operatorname{ord}_q n = \operatorname{ord}_q(c) + \sum_p a(p)\operatorname{ord}_q(p) \ 。 \tag{2}$$

根據 ord_q 之定義，我們有

$$\operatorname{ord}_q(c) = 0 \qquad \text{且} \quad \operatorname{ord}_q(p) = \begin{cases} 1 & \text{若} p = q \\ 0 & \text{若} p \neq q \end{cases} \ 。$$

所以實際上，(2) 式的右側僅剩單一的一項 $a(q)$ 沒有陣亡；我們有

$$\operatorname{ord}_q f = a(q)\,,$$

故得證。

6 歐氏整域的唯一分解性

看完了整數環與多項式環的唯一分解性後，你一定很訝異這之間存在著如此驚人的相似性。那麼，這背後是否隱藏著怎麼樣更豐富的結

構；使得活現在你眼前的整數環與多項式環，只不過是裡頭兩個特殊的例子而已呢？

幾番細思量，不難發現；引理2所帶出來的性質可說是相當的關鍵，而在引理3中更是發揮得淋漓盡致。一來，其間有大小的觀念；在$\mathbb{Z}$中爲一般的絕對值(非負整數)，而在$k[x]$中則爲多項式的次數(也是非負整數)；這提供了良序性可以展現她婀娜多姿神采的舞台，也成就了最小元素卻是最大公因數(最高公因式)的美談。二來，只要一個集合在減法與倍數(式)之下有封閉性；那麼最小元素搖身一變，成爲這個集合的生成元素；也就是說，所有的元素都是最小元素的倍數(式)。

從實作的層面來說，引理2乃是計算最大公因數、最高公因式演算法的基石；那就是所謂的輾轉相除法，也稱爲歐基里德演算法。因此之故，引理2有些人也把它稱爲歐基里德演算法(Euclid's algorithm)。很自然地，人們就把具備有引理2性質的整域(integral domain)稱爲歐基里德域簡稱爲歐氏整域。更明確的說，我們有如下的定義。

【定義】　一個歐氏整域(Euclidean domain)就是一個整域R；其非零元素上定義有一函數σ映到非負整數上，使得對任意$a, b \in R,\ b \neq 0$存在$q, r \in R$滿足

$$a = qb + r \qquad \text{其中} \qquad \sigma(r) < \sigma(b) \quad \text{或} \quad r = 0。$$

除了整數環及多項式環是歐氏整域外，還有高斯整數環$\mathbb{Z}[\sqrt{-1}]$及前面碰到的複數子集$\mathbb{Z}[\sqrt{-2}]$也是歐氏整域。

【例題1】　高斯整數環$\mathbb{Z}[\sqrt{-1}]$是一個歐氏整域。

【證明】　顯而易見，$\mathbb{Z}[\sqrt{-1}] \subseteq \mathbb{C}$是一個整域。定義函數

$$\sigma(\alpha+\beta\sqrt{-1}) = \alpha^2+\beta^2, \quad \alpha+\beta\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]。$$

令$a, b \neq 0$爲任意的高斯整數。將a除以b得到

$$u = a/b = s+t\sqrt{-1}, \qquad s,t \in \mathbb{Q}。$$

選取整數ξ, ζ使得

$$|s-\xi| \leq \frac{1}{2} \qquad 且 \qquad |t-\zeta| \leq \frac{1}{2}。$$

令$q = \xi+\zeta\sqrt{-1}$, 則

$$\sigma(a/b-q) = (s-\xi)^2+(t-\zeta)^2 \leq \frac{1}{4}+\frac{1}{4} = \frac{1}{2}。$$

令$r = a-qb$，則$r \in \mathbb{Z}[\sqrt{-1}]$且$a = qb+r$;其中$r = 0$或

$$\sigma(r) = \sigma(b(a/b-q)) = \sigma(b)\sigma(a/b-q) \leq \frac{1}{2}\sigma(b) < \sigma(b)。$$

故得證高斯整數環$\mathbb{Z}[\sqrt{-1}]$是一個歐氏整域。

【例題2】　複數子集$R = \mathbb{Z}[\sqrt{-2}]$也是一個歐氏整域。

【證明】　如上顯而易見，$R \subseteq \mathbb{C}$是一個整域。定義函數

$$\sigma(\alpha+\beta\sqrt{-2}) = \alpha^2+2\beta^2, \quad \alpha+\beta\sqrt{-2} \in R。$$

令$a, b \neq 0$爲R中任意的元素。將a除以b得到

$$u = a/b = s+t\sqrt{-2}, \qquad s,t \in \mathbb{Q}。$$

選取整數ξ, ζ使得　$|s-\xi| \leq \frac{1}{2}$　且　$|t-\zeta| \leq \frac{1}{2}$。

令$q=\xi+\zeta\sqrt{-2}$，則

$$\sigma(a/b-q)=(s-\xi)^2+2(t-\zeta)^2\le\frac{1}{4}+2\cdot\frac{1}{4}=\frac{3}{4}。$$

令$r=a-qb$，則$r\in R$且$a=qb+r$;其中$r=0$或

$$\sigma(r)=\sigma(b(a/b-q))=\sigma(b)\sigma(a/b-q)\le\frac{3}{4}\sigma(b)<\sigma(b)。$$

故得證R是一個歐氏整域。

【定義】　一個環$(R,+,\cdot)$的非空子集I稱之爲理想；若

(i) $a,b\in I\Longrightarrow a-b\in I$

(ii) $a\in I,r\in R\Longrightarrow ra\in I,ar\in I$

【定理ED】 若I爲歐氏整域R中的一個理想，則存在一元素$a\in R$使得

$$I=Ra=\{ra\mid r\in R\}。$$

【證明】　若$I=0$，那麼樣就沒甚好證的；故假設$I\neq 0$。令$a\in I$爲當中σ值最小的一個元素。顯而易見，$Ra\subseteq I$；我們必須證明，反方向$I\subseteq Ra$也對。

假設$x\in I$。因R是歐氏整域，故存在$q,r\in R$使得

$$x=qa+r\,,\qquad \text{其中}\quad \sigma(r)<\sigma(a)\ \text{ 或 }\ r=0。$$

顯而易見，$r=x-qa\in I$。若$r\neq 0$，則r爲I中σ值比a之σ值還小的一個元素；此乃一矛盾，因此$r=0$是唯一的歸宿。所以得到$x=qa\in Ra$, 故得證。

習慣上，我們將Ra寫成(a)；同樣地，$(a_1, \cdots, a_n)$表示

$$Ra_1 + \cdots + Ra_n = \{r_1a_1 + \cdots + r_na_n \mid r_i \in R, i = 1, \cdots, n\}。$$

顯而易見，若R是一交換環，則$(a_1, \cdots, a_n)$爲R中的一個理想。若I是環R中的一個理想且$I = (a_1, \cdots, a_n)$，那麼我們就說I是有限生成(finitely generated)的一個理想；當$n = 1$時，則稱I爲R中的一個主理想(principal ideal)。

【定義】 我們稱呼整域$(R, +, \cdot)$是一個主理想域(principal ideal domain, 縮寫PID)；若R中的每一個理想都是主理想。

所以定理ED說，歐氏整域都是PID；因而整數環，多項式環，高斯整數環及$(\mathbb{Z}[\sqrt{-2}], +, \cdot)$都是PID。引進歐氏整域的觀念是相當有用的；因爲在實作上，要證明某些環是PID；往往我們先証明此環是一歐氏整域，然後再透過定理ED得到PID的結論。

底下我們將整除性的觀念推廣到擁有乘法單位元素1的PID當中，然後討論唯一分解性的問題；當然這些觀念可在一般的環當中來討論，但那不是我們所要的。因此從現在開始，我們活動的空間就侷限在擁有乘法單位元素1的PID裡頭。

令R爲擁有乘法單位元素1的PID。先定義跟整除性相關的術語如下：

- 我們說R裡頭的一個元素$a \neq 0$整除一個元素$b \in R$，若存在另一個元素$c \in R$使得$b = ac$;而以符號$a|b$表示之。
- 一個元素$u \in R$稱之爲可逆元素(unit)，若u整除R裡頭的乘法單位元素1。

- 兩個元素 $a, b \in R$ 稱之爲夥伴 (associate)，若存在一可逆元素 u 使得 $a = bu$。
- 一個元素 $p \in R$ 稱爲不可約的 (irreducible)，若 $a \mid p$ 則 a 是可逆元素或是 p 的夥伴。
- 一個不可逆元素 $p \in R$ 稱爲質的 (prime)，若 $p \neq 0$ 且

$$p \mid ab \Longrightarrow p \mid a \quad \text{或} \quad p \mid b。$$

不可約元素 (irreducible elements) 跟質元素 (prime elements) 的區分是過去沒有的；因爲在整數環與多項式環中，這兩個觀念是合而爲一的。在上面定義質數 (式) 時，所採用的乃是不可約的觀念；而質性的觀念，則彰顯在推論 2 裡面。對我們而言，其實也不需要如此區分；因爲在 PID 中，這兩個觀念也是合而爲一的，我們等一下就會證明。

上面那些觀念都可轉換成 '理想' 的術語如下：

- $a \mid b \Longleftrightarrow (b) \subseteq (a)$。
- $u \in R$ 爲可逆元素 $\Longleftrightarrow (u) = R$。
- $a, b \in R$ 爲夥伴 $\Longleftrightarrow (a) = (b)$。
- $p \in R$ 爲不可約的，若 $(p) \subseteq (a)$ 則 $(a) = R$ 或 $(a) = (p)$。
- $p \in R$ 爲質的，若且唯若 $ab \in (p) \Longrightarrow a \in (p)$ 或 $b \in (p)$。

【定義】 令 $a, b \in R$。d 稱之爲 a 與 b 的一個最大公因子；若

(i) $d \mid a$ 且 $d \mid b$，

(ii) $d' \mid a$ 且 $d' \mid b \Longrightarrow d' \mid d$。

特別注意到下面兩件事情：

(i) 定義中說的是一個最大公因子。那到底有幾個呢？若c是另一個，那麼我們就必定有$c \mid d$ 且 $d \mid c$,因而c與d是夥伴；亦即，存在一可逆元素u使得$c = ud$。因此最大公因子的個數就是其可逆元素的個數。

(ii) 兩個元素的最大公因子不見得一定會存在；然而對PID來說，我們有下面的定理。

【定理】 令R是一個具有單位元素1的PID且令$a, b \in R$。則a與b有一個最大公因子d，而且$(a, b) = (d)$。

【證明】 考慮由a, b所生成的理想$(a, b) = Ra + Rb$。因爲R是一個PID，所以有一元素d使得

$$(a, b) = (d) \text{ 。}$$

(i) $a \in (a, b) = (d) \Longrightarrow d \mid a$ 且 $a \in (a, b) = (d) \Longrightarrow d \mid b$，

(ii) $d' \mid a$ 且 $d' \mid b \Longrightarrow (a) \subseteq (d')$ 且 $(b) \subseteq (d')$

$$\Longrightarrow (d) = (a, b) \subseteq (d')$$

$$\Longrightarrow d' \mid d \text{。}$$

故得證d爲a與b的一個最大公因子。

【定義】　我們說R中兩個元素a與b是互質的；若其僅有的公因子是可逆元素。換句話說，$(a,b)=R$。

【推論1】若R爲一PID且p是不可約的(irreducible)，則p是質元素(prime element)。

【證明】　假設$p \mid ab$。上述定理允許我們考慮a與p的最大公因子。因p是不可約的，故僅有的因子爲可逆元素或p的夥伴；所以有$(a,p)=R$或$(a,p)=(p)$兩種情況需要討論。

(i) $(a,p)=(p)$ ： 顯而易見$(a)\subseteq(a,p)=(p)\Longrightarrow p\mid a$。

(ii) $(a,p)=R$ ： 此種情況我們得到$(ab,pb)=(b)$。假設告訴我們$p\mid ab\Longleftrightarrow ab\in(p)$且$pb\in(p)$，因而得知

$$(b)=(ab,pb)\subseteq(p)\Longrightarrow p\mid b\,。$$

所以我們已經證明了

$$p\mid ab\Longrightarrow p\mid a\quad 或\quad p\mid b\,,$$

故得證，p是質元素。

【問題】　反過來說，若p是質元素，p是否不可約呢？換句話說，推論1的逆敘述是否成立？

爲了回答這個問題，我們得看看：當p是質元素的時候，元素p有那些因子呢？假設a是p的一個因子，那麼就存在b使得$p=ab$；因此$p\mid ab$，但p是質元素導致$p\mid a$或$p\mid b$。

(i) $p\mid a$ ： 假設是$a\mid p$，故得知a是p的夥伴。

(ii) $p \mid b$ ： 存在c使得$b = pc$。但$p = ab$ ，故得

$$p = ab = a(pc) = p(ac) \Longrightarrow p(ac-1) = 0 \overset{R\text{是整域}}{\Longrightarrow} ac = 1\,;$$

因而a爲可逆元素。

所以我們已經證明了， p的因子裡頭；不是p的夥伴，就是可逆元素。故得證， p是不可約的(irreducible)。

因此，在一個擁有乘法單位元素1的PID裡頭；不可約元素跟質元素這兩個觀念是合而爲一、不分彼此的。我們把這個性質稱爲PID的基本性質，敘述如下。

【PID的基本性質】若R爲一擁有乘法單位元素1的PID，則

$$p\text{是不可約(irreducible)元素} \iff p\text{是質(prime)元素。}$$

接著，我們要逐步預備好證明PID版本的算術基本定理。首先當然得處理存在性的部分，這一次良序原理或數學歸納法原理根本使不上力；因爲一個擁有乘法單位元素1的PID跟自然數或非負整數根本扯不上任何的關係。

你若要將一個元素分解、再分解，直到不能再分解爲止；問題在這分解的過程是不是停得下來呢？如果停不下來的話，那麼連不可約元素存在與否都是個問題；因爲前面定義過的不可約元素就是那不能再分解的元素。職是之故，我們得回頭看看；整數環與多項式環那邊，分解因數(式)的時候是怎麼個停下來的呢？

在整數那邊，分解之後的數變小了；這大小指的是絕對值的大小，分解一次就降一次；頂多降到1就必須停止。在多項式那邊，分解之後

多項式的次數變小了；頂多降到0就必須停止。整數裡頭絕對值是1的就只有± 1，而多項式裡頭次數是0的就是非零常數多項式；這些元素分別是整數及多項式裡頭的可逆元素。所以，在這兩個環裡頭的元素；都有大小的觀念，可供分解的依據；降到最小就是可逆元素，最小之前的那個元素當然就有可能是不可約元素。

然而，我們現在工作的場所僅僅是一個擁有乘法單位元素1的PID而已，當然就沒那麼美那麼帥囉。這可怎麼辦呢？一方面我們當然要善用PID特有的代數結構，每一個理想子環都是一個主理想子環；亦即，每一個理想子環都是其中某一個元素的倍數。另一方面，你可還記得嗎？前面將兩個元素之間的整除關係轉化成兩個主理想子環之間的包含關係；亦即，$a \mid b \iff (b) \subseteq (a)$。因此之故，整除性就跟PID特有的代數結構掛上勾了。而主理想子環之間的包含關係就變成其生成元素之間的大小關係，主理想子環愈大其生成元素愈小。因此，分解到最後的那個最小元素；當然就是一個可逆元素，而此時其對應的主理想子環就是你所看到的這個PID本身。

現在，我們要證明在一個擁有乘法單位元素1的PID中；非零不可逆元素都是不可約元素的乘積。這個證明可分成兩個步驟：

(i) 首先證明每一個非零不可逆元素a都存在有不可約的因子，

(ii) 然後再證明a就是這些不可約因子的乘積。

這兩個步驟當中，我們都會用到底下的「停下來原理」。因爲停下來，所以不可約因子存在；因爲停下來，所以乘積中只包含有限多個不可約的因子。真是妙不可言！

【停下來原理】　令R爲一擁有乘法單位元素1的PID且令

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

爲一向上攀升的主理想鏈。則存在一正整數n使得

$$(a_n) = (a_{n+m}) \qquad \forall\, m = 0, 1, 2, \cdots \text{。}$$

換句話說，此鏈在有限步之後就停下來。

【證明】　令 $I = \bigcup_{i=1}^{\infty} (a_i)$。顯而易見，$I$是主理想域$R$中的一個理想。故存在$a \in R$使得$I = (a)$。但

$$a \in \bigcup_{i=1}^{\infty} (a_i) \Longrightarrow\ a \in (a_n) \quad \text{對某一個} n\,,$$

因此我們有$I = (a) \subseteq (a_n)$;　又 $(a_n) \subseteq \bigcup_{i=1}^{\infty} (a_i) = I$, 故得證

$$I = (a_n) = (a_{n+1}) = \cdots \text{。}$$

【引理1】　令R爲一擁有乘法單位元素1的PID。則每一個非零不可逆元素都是不可約元素的乘積。

【證明】　令 $a \in R$爲非零不可逆元素。

(i) 首先證明a存在有不可約的因子。若a是不可約的，則得證；否則 $a = a_1 b_1$ ，其中a_1及b_1皆爲不可逆元素。若a_1是不可約的，則得證；否則$a_1 = a_2 b_2$ ，其中a_2及b_2皆爲不可逆元素。若a_2是不可約的，則得證；否則繼續如上之論證。顯而易見，我們有

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots \text{。}$$

停下來原理告訴我們，此鏈必斷。故存在某個n， a_n是不可約的。

(ii) 其次證明a是不可約元素的乘積。若a是不可約的，則得證；否則令p_1爲其不可約之因子，因此$a = p_1c_1$。若c_1是可逆元素，則得證；否則令p_2爲其不可約之因子，因此$a = p_1p_2c_2$。若c_2是可逆元素，則得證；否則繼續如上之論證。顯而易見，我們有

$$(a) \subseteq (c_1) \subseteq (c_2) \subseteq \cdots \text{。}$$

停下來原理告訴我們，此鏈必斷。故存在某個n，c_n是可逆元素且$a = p_1p_2 \cdots p_nc_n$；　又p_nc_n,是不可約的，故得證。

再來，我們定義非零元素a在不可約元素p的階數爲下面引理2中的那個唯一的正整數n,以符號$\operatorname{ord}_p a$表示之。

【引理2】　令R爲一擁有乘法單位元素1的PID且令$p \in R$爲不可約元素及$a \neq 0$。則存在一正整數n使得

$$p^n \mid a \text{但} p^{n+1} \nmid a \text{。}$$

【證明】　若否，則對每一個正整數m就存在一元素$b_m \in R$使得$a = p^m b_m$。因此$pb_{m+1} = b_m$。顯而易見，我們有無限向上攀升的主理想鏈

$$(b_1) \subseteq (b_2) \subseteq (b_3) \subseteq \cdots ;$$

這與停下來原理背道而馳，故得證。

【引理3】若$p \in R$是一個質(=不可約)元素且$a, b \in R$爲非零二元素。則

$$\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b \quad \text{。}$$

【證明】　令 $\alpha = \mathrm{ord}_p\, a$ 且令 $\beta = \mathrm{ord}_p\, b$。則

$$a = p^{\alpha}a' \quad \text{且} \quad b = p^{\beta}b'; \quad \text{其中 } p \nmid a' \quad \text{且} \quad p \nmid b'。$$

因此我們有

$$ab = p^{\alpha+\beta}a'b', \quad \text{其中 } p \nmid a'b' \text{ (質元素定義)};$$

所以　$\mathrm{ord}_p\, ab = \alpha + \beta$,　故得證。

至此，準備工作幾近完成；底下先敘述唯一分解性，然後證明之。令 S 爲 R 中具備下列二性質的質元素集：
(i) 每一個 R 中的質元素跟 S 中某個質元素是夥伴。
(ii) S 中任意兩個質元素都不是夥伴。

想要得到這樣子的質元素集，簡單至極；僅需從每一個夥伴類中選取一個質元素，即可組成。這選擇的自由度當然非常大，但在整數環及多項式環卻有著極其自然的選擇法。在整數環中，我們選的是正質數；而多項式環中，我們則選首一質多項式。

【算術基本定理(PID 版本)】　令 R 爲一擁有乘法單位元素 1 的 PID 且令 S 爲如上選取的質元素集。則任何非零元素 a 存在一質元素分解式

$$a = u\prod_p p^{e(p)},$$

此處 u 爲可逆元素，而乘積中的 p 是對所有 S 中質元素；可逆元素 u 以及次冪 $e(p)$ 由 a 所唯一決定。實際上，我們有 $e(p) = \mathrm{ord}_p\, a$。

【證明】　引理 1 已經證明，任何非零元素 a 存在一質元素分解式

$$a = u\prod_p p^{e(p)} \ 。$$

兩邊同時取ord_q，並使用引理3；我們有

$$\mathrm{ord}_q\, a = \mathrm{ord}_q(u) + \sum_p e(p)\mathrm{ord}_q(p)\ 。 \tag{3}$$

根據ord_q之定義，我們有

$$\mathrm{ord}_q(u) = 0 \qquad 且 \quad \mathrm{ord}_q(p) = \begin{cases} 1 & 若 p = q \\ 0 & 若 p \neq q \end{cases}\ 。$$

所以實際上，(3)式的右側僅剩單一的一項$e(q)$沒有陣亡；我們有

$$\mathrm{ord}_q\, a = e(q)\,,$$

故得證。

7 另一個唯一分解性之應用

凡具備有算術基本定理之性質的整域就稱之爲唯一分解整域(Unique Factorization Domain縮寫UFD)。早在歐基里德的年代就隱約知道，整數環是一個UFD的事實；但第一個將此結果清楚明白的寫下來，似乎得等到高斯的著作《算術研究》[17]中才出現。

上面我們已經證明了每一個PID都是一個UFD；反之則否。在例題1及例題2中，我們證明了二次數體(quadratic number fields) $\mathbb{Q}(\sqrt{-1})$ 及 $\mathbb{Q}(\sqrt{-2})$所對應的整數環(rings of integers)

$$\mathbb{Z}[\sqrt{-1}] \quad 及 \quad \mathbb{Z}[\sqrt{-2}]$$

[17]《算術研究》(Disquisitiones Arithmeticae)是德國數學家卡爾·弗里德里希·高斯於1798年寫成的一本數論教材，在1801年他24歲時首次出版。全書用拉丁文寫成。在這本書中高斯整理彙集了費馬、歐拉、拉格朗日和勒讓德等數學家在數論方面的研究結果，並加入了許多他自己的重要成果。

都是UFD。值的一提的是，在1966年史達克(Stark, H.M.)完成了一個數論中懸宕未解決的問題；他證明了二次數體$\mathbb{Q}(\sqrt{d})$，其中$d<0$所對應的整數環是一個UFD只有當

$$d=-1,-2,-3,-7,-11,,-19,-43,-67,\text{及 } -163$$

時，而且再也沒有其他的值了。

在第一、二節，我們已經看過了兩個簡單的應用；分別用到了整數環以及$(\mathbb{Z}[\sqrt{-2}],+,\cdot)$是UFD的事實。底下我們一起來看看更多其他唯一分解性的應用；包括用來證明有無限多個質數、質多項式，還有應用到一些算術函數(arithmetic functions)上。

【質數無限定理(歐幾里德)】　在整數環$\mathbb{Z}$中，存在有無限多個質數。

【證明】　若否，則僅存在有限多個正質數；說是

$$p_1\,,\quad p_2\,,\quad p_3\,,\quad \cdots\quad ,\quad p_n\ 。$$

考慮整數

$$N=p_1\,p_2\,p_3\,\cdots\,p_n+1\ 。$$

顯而易見，$N>1$；根據唯一分解性，N可寫成

$$N=p_1^{a_1}\,p_2^{a_2}\,p_3^{a_3}\,\cdots\,p_n^{a_n}\ 。$$

然而，$p_i\nmid N\ \ \forall i=1,2,3,\cdots,n$；我們有

$$a_i=\mathrm{ord}_{p_i}\,N=0\ \ \forall i=1,2,3,\cdots,n\,,$$

因此$N=p_1^0\,p_2^0\,p_3^0\,\cdots\,p_n^0=1$。與$N>1$矛盾，故得證。

在多項式環$k[x]$中，若k爲無限體；那麼$x-a\ \ (\forall\, a\in k)$都是質多項式，因此$k[x]$當然擁有無限多個不互爲夥伴的質多項式。如果$k$爲有限體；那麼歐幾里德的論證就得出場行禮如儀，如此這般地證明$k[x]$擁有無限多個質多項式。

與此相對且值得一提的另一個極端是；有的環僅擁有一個質元素，茲舉例如下。令$p\in\mathbb{Z}$爲一質數且令

$$\mathbb{Z}_{(p)}=\left\{\frac{a}{b}\mid a,b\in\mathbb{Z}\,,p\nmid b\right\}\ 。$$

則利用p之質性，不難看出$\mathbb{Z}_{(p)}$形成一個環。這個環僅擁有一個質元素，那就是p；爲什麼呢？只要看看這裡頭的可逆元素長的模樣，就可了然於心。請看!

(i) 假設$\dfrac{a}{b}\in\mathbb{Z}_{(p)}$是一個可逆元素，那麼就存在$\dfrac{c}{d}\in\mathbb{Z}_{(p)}$使得$\dfrac{a}{b}\cdot\dfrac{c}{d}=1$。所以$ac=bd$，因而得到$p\nmid a$；這是因爲$p\nmid b$以及$p\nmid d$，再加上$p$之質性所致。

(ii) 反過來，若$\dfrac{a}{b}\in\mathbb{Z}_{(p)}$且$p\nmid a$；那麼我們馬上有$\dfrac{b}{a}\in\mathbb{Z}_{(p)}$且$\dfrac{a}{b}\cdot\dfrac{b}{a}=1$，故得證$\dfrac{a}{b}$是一個可逆元素。

所以$\mathbb{Z}_{(p)}$的可逆元素集就是

$$\mathbb{Z}_{(p)}^{\times}=\left\{\frac{a}{b}\mid a,b\in\mathbb{Z},\ \ p\nmid a\ \ \text{且}\ \ p\nmid b\right\}\ 。$$

參考文獻

[1] Agrawal, Manindra/Kayal, Neeraj/Saxena, Nitin: “PRIMES is in P,” *Annals of Math* 160 (2004), 781-793.
http://www.cse.iitk.ac.in/news/primality.html

[2] Apostol, Tom M.: *Introduction to Analytic Number Theory*, UTM, Springer-Verlag, New York, First Edition, 1976, Corr. Fifth Printing, 1998.

[3] Hardy, G./ Wright E.: *An Introduction to the Theory of Numbers*, Fifth edition, Oxford University Press, 1979.

[4] Hardy, G.H.: *A Course of Pure Mathematics*, Cambridge Mathematical Library, 1993 (First published in 1908).

[5] Hardy, G.H.: *A Mathematician's Apology*, Cambridge University Press, London, 1940. 摘要見網頁

`http://en.wikipedia.org/wiki/A_Mathematician%27s_Apology`

[6] Ireland, Kenneth F./Rosen, Michael I.: *A Classical Introduction to Modern Number Theory*, Volume 84 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, Second Edition, 1990, Corr. Fifth Printing, 1998.

[7] 質數網頁 http://www.utm.edu/research/primes/largest.html

[8] 沈淵源：密碼學之旅 全華圖書有限公司, 2006.