談多項式的因子分解與高斯引理

徐正梅
臺北市立建國高級中學

“多項式與整數”在初等理論的內容與方法上有很多相似的地方，如除法、因式與倍式、輾轉相除法……等，而且兩者都討論“因子分解”這一重要問題，但多項式的因子分解與其係數所佈的數系有很密切的關係。

在下面的討論中，爲了便於表達，規定一些常用的記號

Z：整數集　Q：有理數集　R：實數集　C：複數集

給了多項式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_1x+a_0$　$(n\in N, n\geq 1)$，如果 f(x)之各項係數（缺項之係數看做 0）都在 Q 內，我們就說 f(x)佈於 Q，（其餘依此類推）。

例如：四次多項式 $f(x)=x^4-4$ 之因子分解爲

$x^4-4=(x^2-2)(x^2+2)$　（因子佈於 Z）

$=(x-\sqrt{2})(x+\sqrt{2})(x^2+2)$　（因子佈於 R）

$=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}\ i)(x+\sqrt{2}\ i)$　（因子佈於 C）

一、因子分解

給定兩個多項式 f(x)和 g(x)，如果存在多項式 q(x)滿足 $f(x)=q(x)\cdot g(x)$，那麼，我們就說“g(x)整除 f(x)”，用記號表成 $g(x)\mid f(x)$，此時稱 f(x)是 g(x)的倍式，而 g(x)是 f(x)的因式（因子）。

設 K 表 Z,Q,R,C 中任一數系，一個係數分佈於數系 K 的多項式 f(x)，如果可以表成兩個多項式的乘積

$f(x)=p(x)\cdot q(x)$

其中 p(x)與 q(x)之係數亦佈於 K，且它們的次數都比 f(x) 的次數低，那麼我們就說”f(x)在 K 內可分解“（或說 f(x)在 K 內可約），否則就稱 f(x)在 K 內是不可分解或不可約多項式。例如：$x^2-2=(x-\sqrt{2})(x+\sqrt{2})$ 在 R 內可約，在 Q 內不可約。

二、在複數範圍內分解

設 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots\cdots+a_1x+a_0$　$(n\in N, n\geq 1)$ 且 f(x)佈於 C（複數集），代數

基本定理告訴我們：f(x)至少有一個複數根α_1（方程式 f(x)=0 的根也稱爲多項式 f(x)的根，再透過因式定理，f(x)可被$x-\alpha_1$整除，即

$$f(x)=(x-\alpha_1)f_1(x) \quad \cdots\cdots(1)$$

其中$f_1(x)$是佈於 C 的(n-1)次多項式。當$n-1\geq 1$時，$f_1(x)$至少也有一個複數根α_2，同樣的討論得

$$f_1(x)=(x-\alpha_2)f_2(x) \quad \cdots\cdots(2)$$

此處$f_2(x)$是佈於 C 的$(n-2)$次多項式，把(2)代入(1)，得

$$f(x)=(x-\alpha_1)(x-\alpha_2)f_2(x) \quad \cdots\cdots(3)$$

對$f_2(x)$繼續討論下去，最後可得

$$f(x)=a_n(x-\alpha_1)(x-\alpha_2)\cdots\cdots(x-\alpha_n) \quad \cdots\cdots(4)$$

其中a_n是 f(x)的首項係數。故得下面結論：

> (1)每一個佈於 C 的 n 次$(n\geq 2)$多項式 f(x)都是可約的，而且可以分解成 n 個一次因子（係數佈於 C）的乘積。
> (2)若 k 次重根算成 k 個根，則 n 次多項式恰有 n 個複數根（含實根）。

三、在實數範圍內分解

設$f(x)=a_nx^n+\cdots+a_1x+a_0$且 f(x)之係數佈於 R（實數集），f(x)之次數$n\geq 2$，令

$$\alpha=a+bi \qquad (a,b\in R \text{ 且 } b\neq 0)$$

α之共軛複數記作$\overline{\alpha}=a-bi$，經過計算可得到

$$\overline{f(\alpha)}=f(\overline{\alpha}) \quad \cdots\cdots(5)$$

換句話說：實係數 n 次多項式 f(x)保有共軛性，即$\alpha,\overline{\alpha}$共軛，則它們的函數值$f(\alpha)$與$f(\overline{\alpha})$仍保持共軛。由(5)式可以導出實係數 n 次方程式的虛根共軛成雙定理：

> **虛根共軛成雙定理**
> 實係數 n 次方程式 f(x)=0 之虛根共軛成雙出現。
> 即 $f(\alpha)=0 \quad \Leftrightarrow \quad f(\overline{\alpha})=0$

於是當 f(x)的次數 n 爲奇數時，由於虛根有偶數個（也許沒有），故 f(x)至少有一個實根。

今假設 f(x)有 n 個根，分別爲：

虛根：$\alpha_1,\overline{\alpha_1},\alpha_2,\overline{\alpha_2},\ldots\ldots,\alpha_k,\overline{\alpha_k}$　　（計 2k 個，此處 $\alpha_j=a_j+b_ji$）

實根：$r_1,r_2,\text{-----},r_s$　　（計 s 個，此處 n＝2k+s）

則 f(x)在複數範圍內可以分解成（f(x)佈於 R，當然也佈 C）

$$f(x)=(x-\alpha_1)(x-\overline{\alpha_1})(x-\alpha_2)(x-\overline{\alpha_2})\ldots\ldots(x-\alpha_k)(x-\overline{\alpha_k})(x-r_1)\ldots(x-r_s)\ldots\ldots\ldots\ldots(6)$$

因共軛因子的乘積：$(x-\alpha_j)(x-\overline{\alpha_j})=(x-a_j)^2+bj^2$ 是一個實係數二次因子，故(6)式可以改寫成：

$$f(x)=\underbrace{[(x-a_1)^2+b_1{}^2][(x-a_2)^2+b_2{}^2]\ldots.[(x-a_k)^2+b_k{}^2]}_{\text{二次因子的乘積}}\underbrace{(x-r_1)\ldots(x-r_s)}_{\text{一次因子之乘積}}\ldots\ldots\ldots(7)$$

(7)式呈現一個重要的結論：

> (1)實係數 n 次多項式 f(x)，當 n≥3 時，f(x)在 R 內可約，且 f(x)可分解成二次因子或一次因子（係數佈於 R）之乘積。
>
> (2)n＝2 時，$f(x)=ax^2+bx+c$，當 $b^2-4ac\geq 0$ 時，f(x)在 R 內可約。當 $b^2-4ac<0$ 時，f(x)在 R 內不可約。

例 1：設 $f(x)=x^4+x^3+x^2+x+1$，試在 C,R 內分解 f(x)。

（解）：因 $x^4+x^3+x^2+x+1=\dfrac{x^5-1}{x-1}$　　（等比級數和）

故 $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$，於是 f(x)之四個複數根爲

$\omega,\omega^2,\omega^3,\omega^4$　　（此處 $\omega=\cos\dfrac{2}{5}\pi+i\sin\dfrac{2}{5}\pi$）

(1)在 C 內分解：

$$x^4+x^3+x^2+x+1=(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4)$$

(2)在 R 內分解：

當 $|\alpha|=1$時，有 $\alpha\cdot\overline{\alpha}=|\alpha|^2=1$，今 $\omega^5=1$，故知

ω與ω^4共軛且ω^2與ω^3共軛

$$x^4+x^3+x^2+x+1=\{(x-\omega)(x-\omega^4)\}\{(x-\omega^2)(x-\omega^3)\}$$

$$=(x^2-2x\cos\frac{2}{5}\pi+1)(x^2-2x\cos\frac{4}{5}\pi+1)$$

(3) $x^4+x^3+x^2+x+1$ 在 Q 內不可約。

四、整係數多項式的分解問題：

我們都知道：Q,R,C 這三個集合中任何一個，都可以進行“加，減，乘，除”四則運算，唯一的限制是除數不可爲 0。但在 Z 中，只能進行“加，減，乘”三種運算（因兩個整數相除它的商數不一定是整數），正因爲這一差別，對整係數多項式的分解問題，高斯(C.F.Gauss 1777～1855)提出了他的看法：

> **商斯引理**
>
> 如果整係數 n 次多項式 f(x)在 Q 內可分解，那麼 f(x)在 Z 內也可分解。

把整係數多項式 f(x)看作一個係數佈於 Q 中的多項式，再來考慮它的分解問題，高斯認爲：“f(x)能否在整數系 Z 範圍內分解，完全取決於 f(x)能否在有理數系 Q 範圍內分解”。爲了證明這一重要結論，先介紹一些相關概念。

（定義）：

設 $f(x)=a_nx^n+a_{n-1}x^{n-1}+.....+a_1x+a_0$ 是整係數多項式，若 f(x)之各項係數的最大公因數等於 1，即 $(a_n,a_{n-1},.....,a_1a_0)=1$，則稱 f(x)爲**模多項式**（簡稱**模式**）。

讓我們先證明下面引理：

（引理 1）設 f(x),g(x),h(x)都是整係數多項式且 $h(x)=f(x)\cdot(x)$，如果質數 p 整除 h(x)的各項係數，則 f(x)與 g(x)中必有一個多項式，它的各項係數也都能被 p 整除。

〔證明〕用反證法

設 $f(x)=a_nx^n+a_{n-1}x^{n-1}+.....+a_1x+a_0$ 中至少有一個係數 a_i 不被 p 整除以及 $g(x)=b_mx^m+b_{m-1}x^{m-1}+.....+b_1x+b_0$ 中至少有一個係數 b_j 不被 p 整除，即 $p\nmid a_i$，$p\nmid b_j$ 且 i 和 j 是滿足此條件的最小指標，則 $p\nmid a_ib_j$，考慮 $h(x)=f(x)\cdot g(x)$之x^{i+j}項係數c_{i+j}：

$$c_{i+j}=a_{i+j}b_0+.....+a_ib_j+.....+a_0b_{i+j}.....(8)$$

$a_k=0,k=n+1,n+2,.....'b_\ell=0,\ell=m+1,m+2,.....)$

(8)這一項外，其餘所有的項，包括

$\alpha_{i+j}b_0,\alpha_{i+j-1}b_1,.....\alpha_{i+1}\ b_{j-1},\alpha_{i-1}b_{j+1},.....\alpha_0b_{i+j}$都是 p 的倍數

（$\because p|\alpha_k,k=0,1,.....,i-1;p|b_\ell,\ell=0,1,.....,j-1$），因而 $p\nmid c_{i+j}$，這與題意不符。#

（推論）兩個樸式 f(x),g(x)之乘積 h(x)＝f(x)・g(x)仍是樸式。

（推論與引理 1 是等價命題）

現在我們可以來證明**高斯引理**：

> 高斯引理：
> 如果整係數 n 次多項式 f(x)在有理數系 Q 內可約，那麼 f(x)在 Z 內也可約解。

（證明）把整係數多項式 f(x)看成佈於 Q 內的多項式，並假設 f(x)可以在 Q 內分解成次數較低的兩多項式乘積：

$$f(x)=p(x)\cdot q(x)$$

因 p(x)是有理係數，先將 p(x)之各項係數（分數）通分，然後將分母提出，其次將通分後的各項分子之最大公因數提出，這樣一來，剩下一個整係數的樸式 $p_1(x)$，即$p(x)=\frac{d_1}{m_1}p_1(x)$，同理，對 q(x)做同樣的處理，得 $q(x)=\frac{d_2}{m_2}q_1(x)$，（$q_1(x)$是樸式），於是有

$$f(x)=p(x)\cdot q(x)=\frac{d_1d_2}{m_1m_2}p_1(x)q_1(x)=\frac{d}{m}p_1(x)q_1(x)\quad\cdots\cdots(9)$$

$$mf(x)=d\cdot p_1(x)q_1(x)\quad\cdots\cdots(10)$$

根據上面引理的推論知：$p_1(x)q_1(x)$也同樣是樸式。再由(10)式可知，整數 m 可以除盡 $d\cdot p_1(x)q_1(x)$各項係數（但樸式 $p_1(x)q_1(x)$之所有係數互質），因而 $m\mid d$，即$\frac{d}{m}$是一個整數，(9)式變成：

$$f(x)=\frac{d}{m}p_1(x)q_1(x)=\text{（整數）}\cdot\text{（樸式）}\cdot\text{（樸式）}$$

故知：f(x)在 Z 內亦可分解。#

高斯引理也可用等價命題來描述：

> 如果整係數多項式 f(x)在 Z 內不可約，則 f(x)在 Q 內亦不可約。

艾森斯坦(Eisenstein)對一個整係數多項式 f(x)在 Z 內是否可約，提出了一個有用的判別法：

艾森斯坦判別法：

設 $f(x)=c_nx^n+c_{n-1}x^{n-1}+.....+c_1x+c_0$ 是整係數多項式，並且存在一質數 p 滿足

(1) $p|c_j$　$(j=0,1,2,.....,n-1)$　　(2) $p\nmid c_n$　　(3) $p^2\nmid c_0$

則 f(x)在 Z 內不可約。

（證明）利用反證法

設 f(x)在 Z 內可分解成兩個次數較低的整係數多項式的乘積

$$f(x)=p(x)\cdot q(x)$$

其中 $p(x)=a_rx^r+a_{r-1}x^{r-1}+.....+a_1x+a_0$

$q(x)=b_sx^s+b_{s-1}x^{s-1}+.....+b_1x+b_0$

$r+s=n,\quad 1\le r\le n-1,\quad 1\le s\le n-1$

由於 $p\mid c_0$ 且 $p^2\nmid c_0$ 得 $p|a_0b_0$ 且 $p^2\nmid a_0b_0$

不妨設 $p|a_0$ 且 $p\nmid b_0$

由條件 $p\nmid c_n$ 得 $p\nmid \alpha_rb_s$，故 $p\nmid \alpha_r$　$(p\nmid b_s)$

不妨設 a_k 是 $a_0,a_1,a_2,.....,a_r$ 中，第一個不被 p 整除者，則

$$1\le k\le r\le n-1$$

現在考慮 $c_k=a_kb_0+a_{k-1}b_1+.....+a_0b_k$ 該式右端除了第一項 a_kb_0 之外，其餘各項都能被 p 整除，因而 $p\nmid c_k$，此與定理中的所予條件矛盾。#

例 2：$f(x)=x^{p-1}+x^{p-2}+.....+x^2+x+1$ 其中 p 是一個質數，則 f(x)在 Z 內不可約。

（解）：$f(x)=\dfrac{x^p-1}{x-1}$ 考慮 $g(y)=f(y+1)=\dfrac{(y+1)^p-1}{y}$

則 $g(y)=y^{p-1}+C_1^py^{p-2}+C_2^py^{p-3}+.....+C_{p-2}^py+C_{p-1}^p$

因 $p|C_j^p\ (j=1,2,.....,p-1)$　但 $p^2\nmid c_{p-1}^p$　$(C_{p-1}^p=C_1^p=p)$，$p^2\nmid 1$

故 g(y)不可約，從而 f(x)也不可約。

例 3：整係數多項式之有理根檢驗法

設 $f(x)=\alpha_nx^n+\alpha_{n-1}x^{n-1}+.....+\alpha_1x+\alpha_0$ 是整係數樸式，p 與 q 是互質的兩整數。

如果 $\dfrac{q}{p}$ 爲 f(x)之一個有理根，則

(1) $p|\alpha_n$ 且 $q|\alpha_0$

(2) $p-q \mid f(1)$且$(p+q) \mid f(-1)$

（證明）(1)因 $f(\frac{q}{p})=0 \quad \Rightarrow \quad \alpha_n(\frac{q}{p})^n+\alpha_{n-1}(\frac{q}{p})^{n-1}+\ldots\ldots+\alpha_1(\frac{q}{p})+\alpha_0=0$

$\Rightarrow \quad \alpha_n q^n+\alpha_{n-1}pq^{n-1}+\ldots\ldots+\alpha_1 p^{n-1}q+\alpha_0 p^n=0\ldots\ldots\ldots\ldots(A)$

由(A)式得 $p(\alpha_{n-1}q^{n-1}+\ldots\ldots+\alpha_1 p^{n-1}q+.\alpha_0 p^{n-1})=-\alpha_n q^n$

$p \mid \alpha_n q^n \quad \Rightarrow \quad p \mid \alpha_n \quad (\because (p,q)=1)$

同理由(A)式得 $q(\alpha_n q^{n-1}+\alpha_{n-1}pq^{n-2}+\ldots\ldots+.\alpha_1 p^{n-1}=-\alpha_0 p^n$

$q \mid \alpha_0 p^n \quad \Rightarrow \quad q \mid a_0 \quad (\because (p,q)=1)$

(2)因 $f(\frac{q}{p})=0 \quad \Rightarrow f(x)$含因式$px-q$

令 $f(x)$除以$px-q$之商式爲$g(x)$，則$f(x)=(px-q)g(x)$

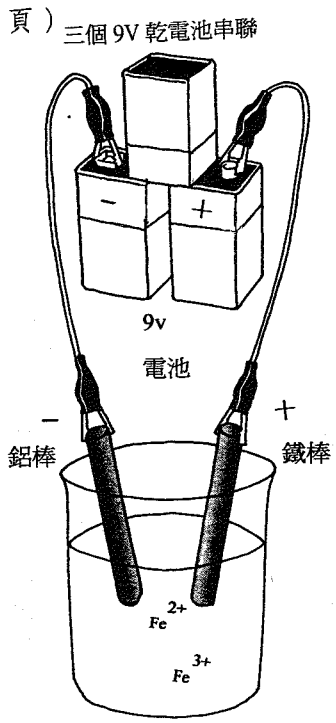
則 $f(x)$在 Q 內可分解，由高斯引理知 $f(x)$在 Z 內亦可分解，於是 $g(x)$必爲整係數多項式。今取

$x=1$代入$f(x)$，得$f(1)=(p-q)g(1)$　　$g(1)$是整數

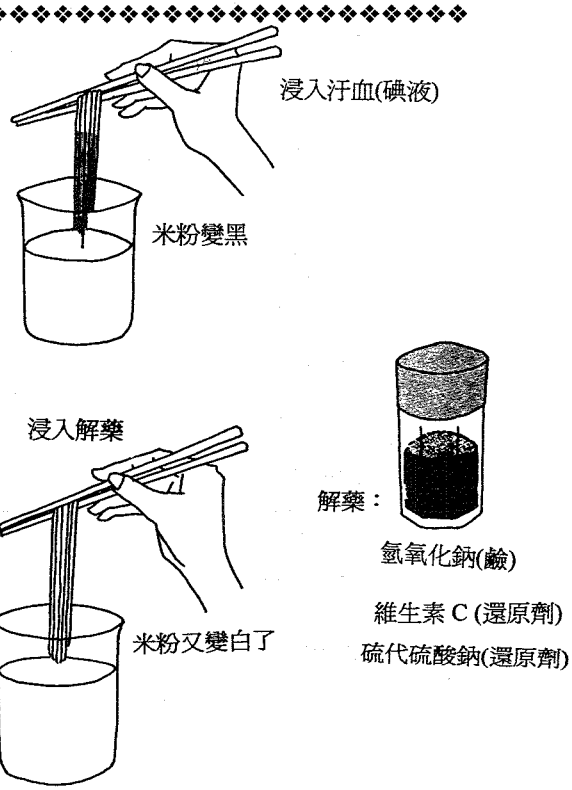
$x=-1$代入$f(x)$，得$f(-1)=(p+q)[-g(-1)]$　　$g(-1)$是整數

$\therefore \quad (p-q) \mid f(1)$且$(p+q) \mid f(-1)$

（上接 45 頁）



圖一



圖二