質數！質式！

黃呈明

壹、動機

國中時代我們說“3 是質數”似無不妥，但在高中課程來講卻必須指明是在所有整數所成的集合 Z 中而言，而對於所有有理數所成的集合 Q 中而言“3”卻非質數又國中的課程中並無負質數而高中的課程中增加了負質式何謂質式如何判別諸多問題耐人尋味，一般同學在此節中較不易清晰，遂寫本文以幫助同學澄清一些概念。

貳、內容

㈠可逆元

1. 定義：

設 S 表一數集合（S 表 N, Z, Q, R, C 或 $Z[x]$）若 $a \in S$ 且 $\frac{1}{a} \in S$ 則謂 a 爲 S 中之一可逆元。

2. 例子：

(1) $1 \in N$，$\frac{1}{1} \in N$ 故 1 爲 中之一可逆元。

(2) $0 \in Z$ 但 $\frac{1}{0} \notin Z$ ∴ 0 不爲 Z 中之可逆元。

(3) $x \in Q$，$x \neq 0$ ∴ $x = \frac{n}{m} (m, n \in Z$ 且 $mn \neq 0)$

$\frac{1}{x} = \frac{m}{n} \in Q$ 故 x 爲 Q 中之可逆元。

3. 性質：

(1) N 中之可逆元只有一個

(2) Z 中之可逆元只有 ± 1

(3) Q 中之可逆元有無限多個。

即除了 0 之外任何有理數均爲 Q 中之可逆元。

(4) R 中之可逆元有無限多個。

即除了 0 之外任意實數均爲 R 中之可逆元。

(5) C 中之可逆元有無限多個。

即除了 0 外任何複數均爲 C 中之可逆元。

(6) $Z(x)$ 中之可逆元 $= Z$ 中之可逆元。

常數多項式$=Z$

一次多項式 $ax+b\Longrightarrow$

$\frac{1}{ax+b}\notin Z[x]$非可逆元。

二次多項式。

(7)$Q[x]$ 中之可逆元$=Q$中之可逆元。

(8)$R[x]$ 中之可逆元$=R$中之可逆元。

(9)$C[x]$ 中之可逆元$=C$中之可逆元。

(二)質數（式）之定義

1. 定義:

設S表一數集合

$a\in S$ 且每當a寫成 $b\cdot c$ 之乘積 $(b,c\in S)$ b,c 中恰有一個爲S中之可逆元則a爲質數。

2. 性質:

(1)N中質數 2, 3, 5, 7, 11……（無限多個）。

$1=1\cdot 1$

1, 1 均爲可逆元 $\therefore$ 1 不爲N中之質數。

$3=3\cdot 1$

恰有一個爲可逆元 $\therefore$ 3 爲N中之質數。

(2)Z中之質數 $\pm 2,\pm 3,\pm 5,\pm 7$……（無限多個）

(3)Q, R, C 中均無質數

說明:

若$a\in Q$, $a\neq 0$, $b\cdot c$ 表示法（任一）$\because a\neq 0$ $\therefore b$, c 均不爲 0

則 b,c 均爲Q中之可逆元。

故a不爲Q中之質數同理 R, C 亦沒有質數。

(4)$Z[x]$ 中之質式

①常數多項式 $f(x)=a_0$, $f(x)$ 爲質式$\longleftrightarrow a$ 爲Z中的質數。

②$f(x)=ax+b(a\neq 0)$, $f(x)$ 爲質式$\longleftrightarrow(a,b)=1$

③$f(x)=ax^2+bx+c(a\neq 0)f(x)$ 爲質式$\longleftrightarrow(a,b,c)=1$，且 $f(x)$ 無一次因式

(5)$Q[x]$ 中之質式 $(f(x)\in Q[x])$

①常數多項式恒不爲質式

證明: $f(x)\in Q[x]$, $f(x)=a_0, a_0\neq 0$ $a_0=bc$ 表示法（任一）$\therefore b,c$ 不爲 $0_0 b,c$ 爲 $Q[x]$ 中之可逆元，故 $f(x)=a_0$ 不爲 $Q[x]$ 中之質式。

若$f(x)=0$, $\because 0=0\cdot 0$, 0, 0 均不爲可逆元故 0 亦不爲 $Q[x]$ 中之質式，

$\therefore$常數多項式恒不爲質式。

②$f(x)=ax+b(a\neq 0)$, $f(x)$恒爲質式（即一次均爲質式）

證明:

設 $f(x)=r\cdot f'(x), (r\in Q, f'(x)\in Q[x])$

其每一表法均因r不爲 0, $\therefore r$ 爲$Q[x]$中之可逆元。

$f'(x)$ 不爲 $Q[x]$ 中之可逆元（ $f'(x)$ 爲一次式），

故 $f(x)$ 爲質式。

③$f(x)=ax^2+bx+c, (a\neq 0) a,b,c\in Q$

$f(x)$ 爲 $Q[x]$ 中之質式$\Longleftrightarrow\triangle=b^3-4ac\neq$有理數之完全平方。

證明:

$$f(x)=ax^2+bx+c$$

$$=a\left(x+\frac{b+\sqrt{b^2-4ac}}{2a}\right)$$

$$\left(x+\frac{b-\sqrt{b^2-4ac}}{2a}\right)$$

若且唯若 $b^2-4ac=$有理數之完全平方則此二多項式

$$x+\frac{b+\sqrt{b^2-4ac}}{2a}$$

$$x+\frac{b-\sqrt{b^2-4ac}}{2a}$$

均爲 $Q[x]$ 中一次式，均不是可逆元。

$\therefore f(x)=ax^2+bx+c$ 不爲質式$\Longleftrightarrow\triangle=b^2-4ac$ 有理數之完全平方

故 $f(x)$ 爲 $Q[x]$ 中之質式$\Longleftrightarrow\triangle=b^2-4ac\neq$有理數之完全平方。

(6)$R[x]$ 中之質式

①常數多項式均不爲質式

證明:

其道理和 $Q[x]$ 證明方法同

②$f(x)=ax+b(a\neq 0, a, b\ni R)\Longrightarrow f(x)$ 恒爲質式

證明: 同(5)

③$f(x)=ax^2+bx+c(a\neq 0, a, b, c\in R)$

$f(x)$ 爲 $R[x]$ 中之質式$\Longleftrightarrow\triangle=b^2-4ac\leq 0$

(7) $C[x]$ 中之質式

①常數多項式均不爲質式

②一次式均爲質式

③二次以上均不爲質式

㈢質式之定理

定理一：兩整係數樸式 $f(x)$，$g(x)$ 其乘積亦是樸式。

已知:

$f(x)=a_nx^n+\cdots\cdots+a_1x+a_0\in Z[x]$

$g(x)=b_mx^m+\cdots\cdots+b_1x+b_0\in Z[x]$

$(a_n,a_{n-1},\cdots\cdots,a_0)$

$=(b_m,b_{m-1},\cdots\cdots b_0)=1$

$f(x)\cdot g(x)=c_{n+m}x^{n+m}+\cdots+c_1x+c_0$

求證:

$\because (a_0,a_1,\cdots\cdots,a_n)=1$，對任一正質數 P 有些 a_c 不能被 P 整除設最小足碼爲 a_j。

$\because (b_0,b_1,\cdots\cdots,b_m=1$ 對任一正質數 P 有些 b_c 不能被 p 整除設最小足碼爲 b_i。

則 $f(x)\cdot g(x)$ 中 x^{i+j} 項係數

$c_{i+j}=(a_{i+j}b_0+a_{i+j-1}b_1+\cdots\cdots+a_{j+1}b_{i-1})$

$+a_jb_i+(a_{j-1}b_{i+1}+\cdots\cdots+a_0b_{i+j})$

右式中除 a_jb_i 這一項，其餘均爲 p 之倍數

$\therefore c_{i+j}$ 不爲 p 之倍數

$\therefore \exists\ c_{i+j}$ 使 $p\nmid c_{i+j}$

$\therefore (c_0,c_1,\cdots\cdots,c_{m+n})=1$

定理二：設 $P(x)$ 爲 $Z(x)$ 中之質式

$\deg P(x)>0$，則

①$P(x)$ 爲樸式

②$P(x)$ 爲 $Q[x]$ 中之質式

證明:

①先證 $p(x)$ 爲樸式

若 $p(x)$ 不爲一樸式則可寫成 $p(x)=d\cdot p'(x)$ 其 $p'(x)$ 爲一樸式，d 爲 $p(x)$ 係數的最大公因數。且 $d>1$

$\therefore p(x)$ 不爲 $Z[x]$ 中之質式，矛盾。

$\therefore p(x)$ 爲一樸式

②再證 $p(x)$ 在 $Q[x]$ 中的質式

若 $p(x)$ 不爲 $Q[x]$ 中的質式設 $p(x)=g(x)\cdot h(x)$

$g(x),h(x)\in Q[x]$ 設 $g(x)=r\cdot g'(x),h(x)=s\cdot h'(x),r,s\in Q^+$.

$g'(x),h'(x)$ 爲樸式，$\therefore p(x)=r\cdot s\cdot g'(x)\cdot h'(x)$

因 $p(x)$ 爲 $Z[x]$ 中之質式，故 $p(x)$ 爲一樸式。

而 $g'(x),h'(x)$ 均爲樸式，故由高斯引理知 $g'(x),h'(x)$ 亦爲一樸式，但因任意有理係數多項式都可唯一寫成一個正有理數與一樸式的乘積。

故由 $p(x)=r\cdot s\cdot g'(x)\cdot h'(x)$ 知 $r\cdot s=1$，且 $p(x)=g'(x)\cdot h'(x)$

$\therefore P(x)$ 不爲 $Z[x]$ 中之質式，矛盾！

$\therefore P(x)$ 在 $Q[x]$ 中爲一質式

定理三

設 $f(x)=a_0+a_1x+\cdots\cdots+a_nx^n\in Z[x]$

若存在一正質數 p 使

$p\mid a_i,\ i=0,1,2,3,\cdots,n-1$

$p\nmid a_n$

$p^2\nmid a_0$

則 $f(x)$ 爲 $Z[x]$ 中之質式

證明:

設 $f(x)$ 不爲 $Z[x]$ 中之質式，

$f(x)=g(x)\cdot h(x)$

①令 $h(x)=c_0+c_1x\cdots\cdots+c_sx^s$

$g(x)=b_0+b_1x+\cdots\cdots+b_rx^r$

$(r<n,r+s=n,g(x),h(x)\in Z[x])$

比較兩邊 x^0 項係數 $a_0=b_0c_0$

x^n 項係數 $a_n=b_rc_s$

②$\because p\mid a_0$ 即 $p\mid b_0c_0\Longrightarrow p\mid b_0$ 或 $p\mid c_0$

若 $p\mid b_0$ 且 $p\mid c_0$ 則 $p^2\mid a_0$ 不合

$\therefore p\mid b_0,p\mid c_0$ 恰有一成立，設 $p\mid b$ 且 $p\nmid c_0$

③$\because p\nmid a_n\quad\therefore p\nmid b_r$

$\therefore b_0,b_1\cdots\cdots b_r$ 至少有一個不爲 p 之倍數。

設足碼最小者爲 b_i 即 $p\nmid b_i$ 而 p 可整除 $b_0,b_1\cdots\cdots,b_{i-1}$

而 $a_i=b_ic_0+b_{i-1}c_1+b_{i-2}c_2+\cdots\cdots+b_0c_i$

$p\mid b_ic_0,b_{i-1}c_1+b_{i-2}c_2+\cdots\cdots+b_0c_i$ 爲 p 之倍數

$\Longrightarrow a_i$ 爲 p 之倍數 $\therefore p\mid c_0$ 不合

$\therefore f(x)$ 爲 $Z[x]$ 中之質式

定理四：$f(x)$ 爲 $Q[x]$ 中之質式$\Longleftrightarrow$ $h\in Q,f(x+h)$ 是質式

證明:

$f(x)$ 不是質式$\Longleftrightarrow f(x)=A(x)B(x)$

$\Longleftrightarrow f(x+h)=A(x+h)B(x+h)$

$\Longleftrightarrow f(x+h)$ 不是質式

由邏輯推理知 $A\longleftrightarrow B$ 與 $\sim A\longleftrightarrow\sim B$ 同義故

$f(x)$ 爲 $Q[x]$ 之質式$\Longleftrightarrow f(x+h)$爲 $Q[x]$ 之質式, $h\in Q$

定理五: P 爲正質數, 則$f(x)=x^{P-1}+x^{P-2}\cdots+x+1$ 爲 $Z[x]$ 中之質式

證明:

$$
\begin{aligned}
&f(x+1)\\
&=(x+1)^{p-1}+(x+1)^{p-2}+\cdots\cdots+(x+1)+1\\
&=[x^{p-1}+(p-1)x^{p-2}+\cdots\cdots+(p-1)x+1]\\
&\quad+[x^{p-2}+(p-2)x^{p-3}+\cdots\cdots+(p-2)x+1]\\
&\quad+[x^{p-3}+(p-3)x^{p-4}+\cdots\cdots+(p-3)x+1]\\
&\quad+\cdots\cdots+(x+1)+1\\
&=x^{p-1}+px^{p-2}+\frac{p(p-1)}{2}x^{p-3}\\
&\quad+\cdots\cdots+\frac{p(p-1)}{2}x+p
\end{aligned}
$$

p 爲質數且不等於 2 則 $p-1$ 爲偶數則$\frac{p-1}{2}$爲整數

若 p 爲2, $f(x+1)=x+2$

因 x^{p-2}, x^{p-3}, $\cdots\cdots x$ 項係數及常數項之係數存在一質數 p 整除它們且 $p\nmid 1$, (x^{p-1} 項係數) $p^2\nmid p$(常數項)則依定理三知$f(x+1)$爲 $Q[x]$ 中質式, 又依定理四知 $f(x)$ 爲 $Q[x]$ 中之質式。