平面代數曲線的交點—BEZOUT 定理 (初級版)

臺大數學系 齊震宇

我們從探討以下的問題開始。

> **問題一:** 在平面上畫上兩組雙曲線 H_1 與 H_2，請問 $H_1 \cap H_2$ 最多可以有幾個元素？

這裡一組雙曲線指的是到平面上兩相異定點的距離差為某定值的點構成的集合。眾所周知，這樣的點集有兩個「分支」。請注意即使平面上已經選定了坐標軸與單位，我們也不只限於考慮對稱軸與坐標軸平行的那種雙曲線。稍微嘗試不難發現可以畫出交點數為一、二、三與四的 H_1 與 H_2；如果我們很天真地把一組雙曲線的兩支想像成兩條拋物線，那麼不難發現可以畫出有八個交點的圖形。問題是，雙曲線的兩支跟兩條拋物線是很不同的，例如，前者有兩條漸近線 (何謂漸近線？)，後者卻沒有對應的物件。如果我們很仔細地觀察雙曲線與漸近線的行為，似乎可以感覺到這類有八個交點的情況不可能發生。無論如何，光憑這個觀察要做出結論—即便不是不可能—也似乎不是三言兩語可以辦到的。

接著我們來看一個似乎與此毫無關聯的問題。

> **問題二:** 考慮一個正整數 m 以及由 $\cos\theta$、$\sin\theta$、$\cos 2\theta$、$\sin 2\theta$、$\ldots$、$\cos m\theta$ 與 $\sin m\theta$ 做四則運算構成的等式，也就是它們的有理函數組合，例如
>
> $$\frac{\sin m\theta}{\sin\theta} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \left(\sin^2\theta - \sin^2\frac{2j\pi}{m} \right) 。$$
>
> 是否存在一個正整數 N, 使得「如果可以找到 N 個不同的 (介於 0 至 2π 間的) 角度 θ 讓這個等式成立，則這個等式對所有的角度 θ 都成立」?

這個問題看起來近乎無稽，因為任給兩個以 θ 為變數的函數，就算它們在若干個 θ 彼此取值相同，也不能代表它們在其他的 θ 處會取值相同。不過，它真的像表面上看來那般無聊嗎？

1. 多項式方程組的解的個數

1.1. 多項式的零點集. (多變數多項式的相關定義與性質，請見附錄2.3小節。)

定義 1.1.1. 對任何多項式 $f \in \mathbf{R}[X,Y]$, 我們稱集合

$$\{(x,y) \in \mathbf{R}^2 \mid f(x,y) = 0\}$$

為 f 的「零點集」或「解集」，記作 $V(f)$。

比方說，單位圓即 $V(X^2+Y^2-1)$；僅含原點的集合 $\{(0,0)\}$ 等於 $V(X^2+Y^2) = V(3X^2-2XY+4Y^2)$(為什麼？)。事實上，平面上的一個有限集必定為某個多項式的零點集 (為什麼？)。所有非退化與退化的圓錐曲線都可以看成某個二次多項式的零點集。

1.2. 兩個單變數多項式有無公因式的判別法—結式 (resultant). (關於一些基本的代數概念與性質，請參考附錄。)

給定 f 與 $g \in \mathbf{R}[Y]$，如何判斷兩者有沒有非常數的公因式呢？利用定理2.3.2我們馬上得到以下的結果。

引理 1.2.1. 假設 f 與 $g \in \mathbf{R}[Y]$。那麼，f 與 g 有 (非常數的) 公因式，若且唯若存在不全為零的 h 與 $k \in \mathbf{R}[Y]$ 使得 $\deg(h) < \deg(g)$、$\deg(k) < \deg(f)$ 且 $hf + kg = 0$。

證明. ($\Longrightarrow$) 假設 $d \in \mathbf{R}[Y]$ 是 f 與 g 的一個非常數的公因式 (也久是說 $\deg(d) > 0$)，那麼 $h = f/d$ 與 $k = -g/d$ 即滿足要求的條件。
($\Longleftarrow$) 反之，假設存在那樣的多項式 h 與 k。由 $hf+kg = 0$ 可知 $hf = (-k)g$，假如 f 與 g 沒有非常數的公因式，那麼存在多項式 p 與 $q \in \mathbf{R}[Y]$ 使得 $1 = pf + qg$。(這可由輾轉相除法得到。為什麼？) 按假設不妨設 h 非零。將兩側同乘以 h 得 $h = phf + qhg = (-k+qh)g$。這樣一來便知 g 是 h 的因式，但是由假設又有 $\deg(h) < \deg(g)$，這是個矛盾。因此 f 與 g 有非常數的公因式。證完。

將 f 與 g 寫成如下的形式：

$$f(Y) = a_0 + a_1 Y + \cdots + a_{m-1}Y^{m-1} + a_m Y^m + \cdots ,$$

$$g(Y) = b_0 + b_1 Y + \cdots + b_{n-1}Y^{n-1} + b_n Y^n + \cdots 。$$

不妨設 $\deg(f) = m \geqslant \deg(g) = n$。故若 $i > m$ 且 $j > n$ 則 $a_i = 0 = b_j$。

定義 1.2.1. 我們稱以下這個 $m+n$ 階行列式

$$
\begin{vmatrix}
a_0 & 0 & \dots & 0 & b_0 & 0 & 0 & \dots & \dots & 0 & 0 \\
a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & 0 & \ddots & \ddots & \ddots & 0 \\
\vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
a_{n-1} & \ddots & \ddots & a_0 & b_{n-1} & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
a_n & \ddots & \ddots & a_1 & b_n & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
a_{m-1} & \ddots & \ddots & a_{m-n} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & b_0 \\
a_m & \ddots & \ddots & a_{m-n+1} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & b_1 \\
0 & a_m & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & b_n & b_{n-1} \\
0 & \vdots & 0 & a_m & 0 & \dots & \dots & \dots & \dots & 0 & b_n
\end{vmatrix}
\tag{1.1}
$$

為多項式 f 與 g 的結式 (resultant)，記為 $R_{f,g}$。

舉例來說，如果 $f(Y)=6Y^3-7Y^2+9$，$g(Y)=2Y^2-Y+5$，則

$$
R_{f,g}=\begin{vmatrix}
6 & 0 & 2 & 0 & 0 \\
-7 & 6 & -1 & 2 & 0 \\
0 & -7 & 5 & -1 & 2 \\
9 & 0 & 0 & 5 & -1 \\
0 & 9 & 0 & 0 & 5
\end{vmatrix}
$$

我們想知道有沒有多項式 h 與 k 滿足引理1.2.1中的條件，頭兩個條件 $\deg(h)<\deg(g)$ 與 $\deg(k)<\deg(f)$ 允許我們將未知的 h 與 k 寫成如下的形式：

$$h(Y)=u_{n-1}Y^{n-1}+u_{n-2}Y^{n-2}+\cdots+u_1Y+u_0，$$

$$k(Y)=v_{m-1}Y^{m-1}+v_{m-2}Y^{m-2}+\cdots+v_1Y+v_0。$$

關於最後一個條件 $hf+kg=0$，我們將 $hf+kg$ 的項對變數 Y 做升冪排列，Y^k $(k=0,\dots,m+n-1)$ 的係數為

$$(a_0u_k+a_1u_{k-1}+\cdots+a_{k-1}u_1+a_ku_0)+(b_0v_k+b_1v_{k-1}+\cdots+b_{k-1}v_1+b_kv_0)。$$

這樣一來，條件 $hf+kg=0$ 等同於以下的齊次方程組：

$$\left(\begin{array}{cccc|ccccccc} a_0 & 0 & \dots & 0 & b_0 & 0 & 0 & \dots & \dots & \dots & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ a_{n-1} & \ddots & \ddots & a_0 & b_{n-1} & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ a_n & \ddots & \ddots & a_1 & b_n & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ a_{m-1} & \ddots & \ddots & a_{m-n} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & b_0 \\ a_m & \ddots & \ddots & a_{m-n+1} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & b_1 \\ 0 & a_m & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & b_n & b_{n-1} \\ 0 & \vdots & 0 & a_m & 0 & \dots & \dots & \dots & \dots & 0 & b_n \end{array}\right)\left(\begin{array}{c} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \\ v_0 \\ v_1 \\ v_2 \\ \vdots \\ \vdots \\ \vdots \\ v_{m-1} \end{array}\right) = \left(\begin{array}{c} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{array}\right)。$$

最後，「存在有滿足所有上述條件且不全為零的多項式 h 與 k」等價於「這個方程組具有分量不全為零的解」；由定理2.4.1，這又進一步地等價於

$$R_{f,g}=\left|\begin{array}{cccccccccccc} a_0 & 0 & \dots & 0 & b_0 & 0 & 0 & \dots & \dots & 0 & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ a_{n-1} & \ddots & \ddots & a_0 & b_{n-1} & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ a_n & \ddots & \ddots & a_1 & b_n & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ a_{m-1} & \ddots & \ddots & a_{m-n} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & b_0 \\ a_m & \ddots & \ddots & a_{m-n+1} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & b_1 \\ 0 & a_m & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & b_n & b_{n-1} \\ 0 & \vdots & 0 & a_m & 0 & \dots & \dots & \dots & \dots & 0 & b_n \end{array}\right| = 0。$$

綜合以上的討論，我們得到下面的結果。

定理 1.2.2. *f 與 $g\in\mathbf{R}[Y]$ 有非常數的公因式若且為若 $R_{f,g}=0$。*

1.3. **Bezout 定理 (初級版).** 現在起假設給定了兩個<u>沒有非常數公因式</u>的非零多項式 f 與 $g\in\mathbf{R}[X,Y]$。我們要利用前一節探討過的結式來了解 $V(f)\cap V(g)$。假設 $\deg(f)=m$ 且 $\deg(g)=n$。先將 f 與 g 視為 Y 的多項式，其係數則為

X 的多項式，將它們表示如下：

$$f(X,Y) = a_0(X) + a_1(X)Y + \cdots + a_{m-1}(X)Y^{m-1} + a_m(X)Y^m + \cdots ,$$

$$g(X,Y) = b_0(X) + b_1(X)Y + \cdots + b_{n-1}(X)Y^{n-1} + b_n(X)Y^n + \cdots 。$$

若以 $\deg_X(\ )$ 表示「求作為以 X 為變數的多項式的次數」這個操作，我們有 $\deg_X(a_j) \leqslant m-j$ 與 $\deg_X(b_k) \leqslant n-k$(為什麼？)；特別地，當 $i > m$ 與 $j > n$ 時 a_i 與 b_j 都是 X 的零多項式。

考慮集合

$$P_{f,g} := \{y \in \mathbf{R} \,|\, \text{存在某個 } x \in \mathbf{R} \text{ 使得 } f(x,y) = g(x,y) = 0\}。$$

換句話說，$P_{f,g}$ 是 $V(f) \cap V(g)$ 在投影映射 $(X,Y) \in \mathbf{R}^2$ 之下的影像。我們

$$\begin{array}{ccc} (X,Y) & \in & \mathbf{R}^2 \\ \downarrow & & \downarrow \\ X & \in & \mathbf{R} \end{array}$$

首先想了解每個 $x \in \mathbf{R}$ 的「頭上」到底有多少個點 (x,y) 在 $V(f) \cap V(g)$ 中？

引理 1.3.1. 對每個 $x \in P_{f,g}$，滿足 $(x,y) \in V(f) \cap V(g)$ 的 y 只有有限多個。

證明. 採用反證法。如果對某個 $x_0 \in P_{f,g}$ 能找到無限多個 y 滿足 $(x_0,y) \in V(f) \cap V(g)$，那麼以 Y 為變數的多項式 $f(x_0,Y)$ 與 $g(x_0,Y)$ 都有無限多個(公)根，而這說明了它們是零多項式(否則根只能有有限多個)。換句話說，所有的 $a_j(X)$ 與 $b_k(X)$ 都以 x_0 為一根，因此都有 $(X-x_0)$ 這個一次因式。這樣一來，$(X-x_0)$ 也是 f 與 g 的一個(非常數的)公因式，跟最初關於 f 與 g 的假設相違背，矛盾。證完。

現在我們以 $R_{f,g}(X)$ 表示 $R_{f(X,\cdot),g(X,\cdot)}$，也就是以 Y 為變數(X 視為數字)的多項式 $f(X,\cdot)$ 與 $g(X,\cdot)$ 的結式。換句話說，$R_{f,g}(X)$ 就是把所有「係數多項式」$a_j(X)$ 與 $b_k(X)$ 帶入結式的定義1.2.1 $\big($公式 (1.1)$\big)$的結果，因此是一個以 X 為變數的多項式。

引理 1.3.2. $P_{f,g} \subseteq \{x \in \mathbf{R} \,|\, R_{f,g}(x) = 0\}$。

證明. 若 $x \in P_{f,g}$，則存在某個 $y \in \mathbf{R}$ 使得 $(x,y) \in V(f) \cap V(g)$。因此 $Y-y$ 是 $f(x,Y)$ 與 $g(x,Y)$ 的一個非常數的公因式。由定理1.2.2知道 $R_{f,g}(x) = R_{f(x,\cdot),g(x,\cdot)} = 0$。

練習 1.3.1. 請證明 $R_{f,g}(X)$ 不是零多項式。(提示：必須用到 f 與 g 沒有非常數的公因式。你可能會需要先將 f 與 g 想成 $\mathbf{R}(X)[Y]$ 中的元素，這裡 $\mathbf{R}(X)$ 是指所有實係數單變數有理函數構成的體。)

引理 1.3.3. $R_{f,g}(X)$ 的次數不超過 mn。

證明. 先引進一些簡單的概念。(參考定義2.3.1(3)。) 首先，把 $a_j(X)$ 的每個項都乘上一個固定變數 Z 的某次方，使得所有的項作為 X 與 Z 的雙變數多項式時都有次數 $m-j$，並將得到的多項式記為 $\widetilde{a}_j(X,Z)$。類似地，把 $b_k(X)$ 的每個項都乘上 Z 的某次方，使得所有的項作為 X 與 Z 的雙變數多項式時都有次數 $n-k$，並將結果記為 $\widetilde{b}_k(X,Z)$。舉例來說，若 $m=6$ 且 $a_2(X)=4X^3-7X^2+9$，則 $\widetilde{a}_2(X,Z)=4X^3Z-7XZ^3+9Z^4$。對所有的 j 與 k，我們總有 $\widetilde{a}_j(X,1)=a_j(X)$ 與 $\widetilde{b}_k(X,1)=b_k(X)$。

按定義 $R_{f,g}(X)$ 是把所有 $a_j(X)$ 與 $b_k(X)$ 帶入結式的定義1.2.1 (公式 (1.1))的結果。若我們改以 $\widetilde{a}_j(X,Z)$ 與 $\widetilde{b}_k(X,Z)$ 帶入，那麼我們會得到一個以 X 與 Z 為變數的多項式

$$R(X,Z)=\begin{vmatrix}
\widetilde{a}_0 & 0 & \dots & 0 & \widetilde{b}_0 & 0 & 0 & \dots & \dots & 0 & 0\\
\widetilde{a}_1 & \widetilde{a}_0 & \ddots & \vdots & \widetilde{b}_1 & \widetilde{b}_0 & 0 & \ddots & \ddots & \ddots & 0\\
\vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\
\widetilde{a}_{n-1} & \ddots & \ddots & \widetilde{a}_0 & \widetilde{b}_{n-1} & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\
\widetilde{a}_n & \ddots & \ddots & \widetilde{a}_1 & \widetilde{b}_n & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\
\vdots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0\\
\widetilde{a}_{m-1} & \ddots & \ddots & \widetilde{a}_{m-n} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \widetilde{b}_0\\
\widetilde{a}_m & \ddots & \ddots & \widetilde{a}_{m-n+1} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \widetilde{b}_1\\
0 & \widetilde{a}_m & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\
\vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \widetilde{b}_n & \widetilde{b}_{n-1}\\
0 & \vdots & 0 & \widetilde{a}_m & 0 & \dots & \dots & \dots & \dots & 0 & \widetilde{b}_n
\end{vmatrix}。$$

注意到 $R(X,1)=R_{f,g}(X)$。我們將證明 $R(X,Z)$ 是 mn 次齊次多項式，這樣一來便知道 $R_{f,g}(X)$ 的次數不會超過 mn。我們要說明對任一變數 T 總有 $R(TX,TZ)=T^{mn}R(X,Z)$。

由於 $R(TX,TZ)=$

$$\begin{vmatrix}
T^m\widetilde{a}_0 & 0 & \dots & 0 & T^n\widetilde{b}_0 & 0 & 0 & \dots & \dots & 0 & 0 \\
T^{m-1}\widetilde{a}_1 & T^m\widetilde{a}_0 & \ddots & \vdots & T^{n-1}\widetilde{b}_1 & T^n\widetilde{b}_0 & 0 & \ddots & \ddots & \ddots & 0 \\
\vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
T^{m-n+1}\widetilde{a}_{n-1} & \ddots & \ddots & T^m\widetilde{a}_0 & T^1\widetilde{b}_{n-1} & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
T^{m-n}\widetilde{a}_n & \ddots & \ddots & T^{m-1}\widetilde{a}_1 & \widetilde{b}_n & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
T^1\widetilde{a}_{m-1} & \ddots & \ddots & T^n\widetilde{a}_{m-n} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & T^n\widetilde{b}_0 \\
\widetilde{a}_m & \ddots & \ddots & T^{n-1}\widetilde{a}_{m-n+1} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & T^{n-1}\widetilde{b}_1 \\
0 & \widetilde{a}_m & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \widetilde{b}_n & T^1\widetilde{b}_{n-1} \\
0 & \vdots & 0 & \widetilde{a}_m & 0 & \dots & \dots & \dots & \dots & 0 & \widetilde{b}_n
\end{vmatrix},$$

依序將前 n 行乘上 $T^n,\dots,T^2,T^1$，將後 m 行乘上 $T^m,\dots,T^2,T^1$，我們得到

$T^{(n+\cdots+2+1)+(m+\cdots+2+1)}R(TX,TZ)=$

$$\begin{vmatrix}
T^{m+n}\widetilde{a}_0 & 0 & \dots & 0 & T^{n+m}\widetilde{b}_0 & 0 & 0 & \dots & \dots & 0 & 0 \\
T^{m+n-1}\widetilde{a}_1 & T^{m+n-1}\widetilde{a}_0 & \ddots & \vdots & T^{n+m-1}\widetilde{b}_1 & T^{n+m-1}\widetilde{b}_0 & 0 & \ddots & \ddots & \ddots & 0 \\
\vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
T^{m+1}\widetilde{a}_{n-1} & \ddots & \ddots & T^{m+1}\widetilde{a}_0 & T^{m+1}\widetilde{b}_{n-1} & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
T^m\widetilde{a}_n & \ddots & \ddots & T^m\widetilde{a}_1 & T^m\widetilde{b}_n & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
T^{1+n}\widetilde{a}_{m-1} & \ddots & \ddots & T^{n+1}\widetilde{a}_{m-n} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & T^{n+1}\widetilde{b}_0 \\
T^n\widetilde{a}_m & \ddots & \ddots & T^n\widetilde{a}_{m-n+1} & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & T^n\widetilde{b}_1 \\
0 & T^{n-1}\widetilde{a}_m & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & T^2\widetilde{b}_n & T^2\widetilde{b}_{n-1} \\
0 & \vdots & 0 & T\widetilde{a}_m & 0 & \dots & \dots & \dots & \dots & 0 & T\widetilde{b}_n
\end{vmatrix}$$

接著從每列依序提出因子 $T^{m+n},\dots,T^2,T$，我們看到

$$T^{(m+n)+\cdots+2+1}R(Z,W)=T^{(n+\cdots+2+1)+(m+\cdots+2+1)}R(TX,TZ)，$$

由於

$$(m+n)+\cdots+2+1-(n+\cdots+2+1)-(m+\cdots+2+1)=mn，$$

消去 T 的因子可得 $R(TX,TZ)=T^{mn}R(X,Z)$，得證。

現在我們可以介紹下述的主要定理。

定理 1.3.4 (Bezout 定理 (初級版))**.** 給定兩非零多項式 f 與 $g \in \mathbf{R}[X,Y]$。如果 f 與 g 沒有公因式且次數分別為 m 與 n，則 $V(f) \cap V(g)$ 最多有 mn 個元素。

證明. 由引理1.3.2、1.3.3及練習1.3.1可知 $P_{f,g}$ 最多只有 mn 個點。如果每個 $P_{f,g}$ 的點頭上只有一個 $V(f) \cap V(g)$ 的點，那麼便得出 $V(f) \cap V(g)$ 最多只有 mn 個點。無論如何，由1.3.1知 $V(f) \cap V(g)$ 總是由 $P_{f,g}$「頭上」的有限個點構成，因此 $V(f) \cap V(g)$ 是個有限集。這使得我們總是能重新選擇坐標系，使得在新的 $X - Y$ 坐標下每個 $P_{f,g}$ 的點的頭上只有一個 $V(f) \cap V(g)$ 的點 (為什麼可以？跟 $V(f) \cap V(g)$ 的有限性有何關聯？)，這樣便證明了這個定理！

這個定理回答了一開始的問題一。

練習 1.3.2. 能否用上述定理回答問題二？(提示：想到 $\cos\theta$ 與 $\sin\theta$ 你會想到哪個多項式的零點集？三角恆等式跟多項式的零點集有甚麼關係？)

2. 附錄：一些基本的代數概念與性質

2.1. 二元運算、結合律與交換律、單位元、可逆元.

定義 2.1.1 (二元運算)**.** 給定一個集合 S。一個 S 上的二元運算 (binary operation/magma) 指的是一個從 $S \times S$ 映至 S 的映射。換句話說，一個 S 上的二元運算指的是一個「為 S 中兩個依序給定的元素指定一個 S 的元素的規則」。對於一個給定的二元運算，如果依序給定了任意的 $s_1, s_2 \in S$，一般常用如 $s_1 \square s_2$ 或 $s_1 \bullet s_2$ 表示這個規則指定給序對 (s_1, s_2) 的那個元素。$\square$ 與 $\bullet$ 可以換成任何明白指定了的符號，如果不會引起混淆，甚至可以把 $s_1 \square s_2$ 簡記為 $s_1 s_2$。我們也會用符號 $(S, \square)$ 表示一個帶有某個 (被指定了的) 二元運算的集合或說 $\square$ 是 S 上的一個二元運算。

例 2.1.1. (1) 令 $+$ 與 $\cdot$ 為一般數字的加法與乘法，則 $(\mathbf{N}, +)$ 與 $(\mathbf{Z}, \cdot)$ 都是二元運算的例子。
(2) 對任意集合 A 與 B，我們以 B^A 表示由所有從 A 映至 B 的映射構成的集合。給定三集合 A、B 與 C，我們有映射的「合成」(composition) 這個操作：

$$\begin{aligned} C^B \times B^A &\xrightarrow{\circ} C^A \\ (g, f) &\longmapsto g \circ f , \end{aligned}$$

這裡的 $g \circ f$ 表示將每個 $a \in A$ 映至 $g(f(a))(\in C)$ 的這個映射。特別地，$(A^A, \circ)$ 是一個帶有二元運算的集合。

(3) 對任一集合 T，我們令 $\mathcal{P}(T)$ 為以所有 T 的子集合為元素的集合，稱作 T 的冪集 (power set)。那麼 $(\mathcal{P}(T), \cap)$、$(\mathcal{P}(T), \cup)$ 與 $(\mathcal{P}(T), \setminus)$ 都是二元運算的例子，這裡 $\cap$、$\cup$ 與 $\setminus$ 分別表示兩個 T 的子集的交集、聯集與差集。

定義 2.1.2 (結合律、單位元、反元素). 給定一集合 S 上的二元運算 $\square$。

(1) 如果對任何的 $s, s', s'' \in S$ 都有

$$s\square(s'\square s'') = (s\square s')\square s'',$$

我們便說 $\square$ 滿足結合律或說它是結合的(associative)。

(2) 如果一個元素 $e \in S$ 對所有的 $s \in S$ 都滿足

$$s\square e = s = e\square s,$$

我們便稱 e 為二元運算 $\square$ 的一個單位元(identity/unit element)。注意到這樣的 e 若是存在則必定只有一個 (為什麼？)。

(3) 假設 $\square$ 的單位元存在 (記作 e)。如果兩個元素 $s, \tilde{s} \in S$ 滿足

$$s\square\tilde{s} = e = \tilde{s}\square s,$$

我們便說 $\tilde{s}$ 是 s 的一個反元素或逆元(inverse)。注意到如果 $\square$ 是結合的，那麼這樣的 $\tilde{s}$ 若是存在則必定只有一個 (為什麼？)，這時我們常將它寫成 s^{-1}。有逆元的元素稱作可逆的 (invertible)。

定義 2.1.3 (交換律). 給定一集合 S 上的二元運算 $\square$。如果對任何的 $s, s' \in S$ 都有

$$s\square s' = s'\square s,$$

我們便說 $\square$ 滿足交換律或說它是可換的(commutative)。

練習 2.1.1. 以下哪些二元運算滿足結合律、交換律或具有單位元？那些滿足結合律且有單位元的情況中的可逆元素分別是甚麼？

(1)$(\mathbf{N}, +)$；(2)$(\mathbf{N}, \cdot)$；(3)$(\mathbf{Z}, +)$；(4)$(\mathbf{Z}, \cdot)$；(5)$(\mathbf{R}\backslash\{0\}, \cdot)$；(6)$(A^A, \circ)$ 與 $(\mathrm{Perm}(A), \circ)$ (這裡 A 是任意集合而 $\mathrm{Perm}(A)$ 是所有由 A 映至 A 的對射 (bijection))；(7)$(\mathcal{P}(T), \cap)$、$(\mathcal{P}(T), \cup)$ 與 $(\mathcal{P}(T), \setminus)$ (這裡 T 是任意集合)。

2.2. **群、可換環、體、唯一分解整環.**

定義 2.2.1 (群/可換群)**.** 我們說一個帶有二元運算的集合 $(G,\cdot)$ 是一個群 (group) 的意思是二元運算 $\cdot$ 滿足結合律、具有單位元且所有元素均可逆。如果 $\cdot$ 還滿足了交換律，我們便稱 $(G,\cdot)$ 為一個可換群或 Abel 群 (abelian group)。

練習 2.2.1. 在上個習題中哪幾個是群？哪些是可換群？

定義 2.2.2. (1) 一個可換環(commutative ring)$(A,+,\cdot)$ 由以下資訊組成：
一個集合 A 與兩個 A 上的二元運算 $+$ 與 $\cdot$，習慣上會依序稱作「加法」(addition) 與「乘法」(multiplication)，它們滿足以下條件：

(A) $(A,+)$ 是個可換群。我們將它的單位元記作 0，並將 $a\in A$ 的 (加法) 反元素記為 $-a$；

(M) $(A,\cdot)$ 滿足結合律與交換律且具有單位元。我們將它的單位元記作 1; 若某元素 $a\in A$(對乘法) 可逆，那它的 (乘法) 反元素記為 a^{-1}；

(D) (分配律) 對任意的 $a,a',a''\in A$，總有

$$(a+a')\cdot a''=(a\cdot a'')+(a'\cdot a'')$$

與

$$a''\cdot(a+a')=(a''\cdot a)+(a''\cdot a')。$$

有時為了簡便，我們會從符號 $(A,+,\cdot)$ 中省略 $+$ 與 $\cdot$ 而將之簡記為 A。
(2) 給定一可換環 A。如果對任何的 $a,a'\in A\setminus\{0\}$ 總有 $a\cdot a'\neq 0$，我們便說 A 是一個整環(integral domain)。
(3) 給定一可換環 K。如果所有 $K\setminus\{0\}$ 的元素都對 $\cdot$ 可逆，那麼我們稱 K 為一個體(field)。

定義 2.2.3. 給定一可換環 A。
(1) 對於 f 與 $g\in A$，如果存在 $h\in A$ 使得 $f=gh$，我們便說 g 是 f 的一個因子。
(2) 如果一個非零元素 $f\in A$ 無法寫成兩個不可逆元素的乘積，我們便說 f 是 A 中的一個不可約的 (irreducible) 元素。
(3) 我們說 A 是個唯一分解整環 (unique factorization ring/UFD)，如果給定任何非零元素 $f\in A$，必存在不可約元 $g_1,\ldots,g_t\in A$ 使得 $f=g_1\cdots g_t$。此外，如果有另一組不可約元 $h_1,\ldots,h_u\in A$ 也使得 $f=h_1\cdots h_u$，則必有

$t = u$，且存在可逆元 $c_1, \ldots, c_t \in \mathbf{R}$ 以及一個 $1, \ldots, t$ 的排列 $k_1, \ldots, k_t$ 使得 $g_1 = c_1 h_{k_1}, \ldots, g_t = c_t h_{k_t}$。換句話說，任一非零元素都可以表示成不可約元的乘積，且這樣的表達法 (最多差了乘上可逆元素與重排順序) 是唯一的。

2.3. **多項式環.**

定義 2.3.1. (多項式環)(1) 給定一個可換環 A 我們以 $A[X_1, \ldots, X_s]$ 表示由所有以 $X_1, \ldots, X_s$ 為變數、以 A 的元素為係數的多項式構成的集合。多項式間有自然的加法與乘法，不難直接看出 $(A[X_1, \ldots, X_s], +, \cdot)$ 是個可換環，一般稱作 A 上的 (s 變數) 多項式環。
(2) 任一 $f \in A[X_1, \ldots, X_s]$ 可以唯一地表示成

$$f(X_1, \ldots, X_s) = \sum_{j_1, \ldots, j_s} a_{j_1 \ldots j_s} X_1^{j_1} \cdots X_s^{j_s},$$

這裡的 $j_1, \ldots, j_s$ 跑遍所有非負整數，而 $a_{j_1 \ldots j_s}$ 為某些 A 的元素，且只有有限多組 $(j_1, \ldots, j_s)$ 可以讓 $a_{j_1 \ldots j_s} \neq 0$。當變數個數 s 不大時，我們常用不帶足碼的英文字母如 $X, Y, Z, \ldots$ 表示 $X_1, X_2, X_3, \ldots$。對於非零的 f，我們稱 $\{j_1 + \cdots + j_s \,|\, a_{j_1 \ldots j_s} \neq 0\}$ 中的最大數為 f 的次數，記作 $\deg(f)$。例如，如果 $f(X, Y) = 4X^3Y + 2X^4Y - X^2Y^3 + 7X^2Y + 2X - 4$，則 $\deg(f) = 5$。
(3) 令 d 為一正整數。如果 $f \in A[X_1, \ldots, X_s]$ 的係數 $a_{j_1 \ldots j_s}$ 只有當 $j_1 + \cdots + j_s = d$ 時才可能非零，我們就稱 f 為一個 d 次齊次 (homogeneous) 多項式。注意到「f 是一個 d 次齊次多項式」等價於「對變數 T 總有 $f(TX_1, \ldots, TX_s) = T^d f(X_1, \ldots, X_s)$」。

對於一個體 K，單變數多項式環 $K[X]$ 與整數全體構成的集合 $\mathbf{Z}$ 有些相似處。(可以想像 $K = \mathbf{R}$ 或 $\mathbf{C}$ 的情況。) 比方說，兩者都有帶餘除法，這時不可約多項式的角色相當於質數 (與質數加負號)。一般的多項式環 $A[X_1, \ldots, X_s]$ 雖然沒有一個好的帶餘除法操作，但仍舊有某些與 $\mathbf{Z}$ 類似的性質，其中最基本的是以下的結果。

定理 2.3.1. 如果 A 是一個 UFD，則 $A[X_1, \ldots, X_s]$ 亦然。

這個定理的證明可以在許多標準的近世代數 (抽象代數) 教材中找到。注意到對於任何的整環 A，多項式環 $A[X_1, \ldots, X_s]$ 的可逆元即為 A 的可逆元 (為什麼？)。以 $A =$ 某個體 K(例如 $\mathbf{R}$) 為例，K 的可逆元即為非零元素。由於 K 是個 UFD(所有的體都是 UFD，為什麼？)，上述定理告訴我們以下的推論。

定理 2.3.2. 假設 K 是一個體。給定任何非零元素 $f \in K[X_1, \ldots, X_s]$，必存在不可約多項式 $g_1, \ldots, g_t \in K[X_1, \ldots, X_s]$ 使得 $f = g_1 \cdots g_t$。此外，如果有另一組不可約元 $h_1, \ldots, h_u \in K[X_1, \ldots, X_s]$ 也使得 $f = h_1 \cdots h_u$，則必有 $t = u$，且存在非零元素 $c_1, \ldots, c_t \in K$ 以及一個 $1, \ldots, t$ 的排列 $k_1, \ldots, k_t$ 使得 $g_1 = c_1 h_{k_1}, \ldots, g_t = c_t h_{k_t}$。也就是說，任一係數在一體 K 內的非零多項式都可以表示成不可約多項式的乘積，且這樣的表達法 (最多差了乘上非零元素與重排順序) 是唯一的。

2.4. **齊次線性方程組、矩陣與行列式.** 以下令 A 是一個可換環。

定義 2.4.1. (1) 對於任兩個正整數 m 與 n，一個 A 上的 $m \times n$ 矩陣指的是一個形如

$$C = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}$$

的陣列，這裡 c_{jk} 是某些 A 的元素，稱作矩陣 C 的第 i 列第 j 行的分量，簡稱為 C 的 (i, j)-分量。m 與 n 分別稱作矩陣 C 的列數與行數。我們以 $M_{m,n}(A)$ 表示以所有 A 上的 $m \times n$ 矩陣為元素的集合。
(2) 給定兩個 A 上的 $m \times n$ 矩陣

$$C = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix} \quad \text{與} \quad C' = \begin{pmatrix} c'_{11} & c'_{12} & \cdots & c'_{1n} \\ c'_{21} & c'_{22} & \cdots & c'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c'_{m1} & c'_{m2} & \cdots & c'_{mn} \end{pmatrix},$$

我們定義它們的「和」為

$$C + C' = \begin{pmatrix} c_{11} + c'_{11} & c_{12} + c'_{12} & \cdots & c_{1n} + c'_{1n} \\ c_{21} + c'_{21} & c_{22} + c'_{22} & \cdots & c_{2n} + c'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} + c'_{m1} & c_{m2} + c'_{m2} & \cdots & c_{mn} + c'_{mn} \end{pmatrix}。$$

這樣的加法定義了一個映射 $M_{m,n}(A)\times M_{m,n}(A)\longrightarrow M_{m,n}(A)$。(2) 給定 A 上的 $m\times n$ 矩陣 C 與 $l\times m$ 矩陣 D：

$$D=\begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1m}\\ d_{21} & d_{22} & \cdots & d_{2m}\\ \cdots & \cdots & \cdots & \cdots\\ d_{m1} & d_{m2} & \cdots & d_{lm}\end{pmatrix} \quad 與 \quad C=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n}\\ c_{21} & c_{22} & \cdots & c_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ c_{m1} & c_{m2} & \cdots & c_{mn}\end{pmatrix},$$

我們定義乘積 DC 為以 $d_{i1}c_{1j}+d_{i2}c_{2j}+\cdots+d_{im}c_{mj}$ 為其 (i,j)-分量 $(i=1,\ldots,l,\ j=1,\ldots,n)$ 的 $l\times n$ 矩陣。換言之，DC 的第 (i,j) 分量等於把 D 的第 i 列與 C 的第 j 行的各分量依序相乘後加總得到的結果。這樣的乘法定義了一個映射 $M_{l,m}(A)\times M_{m,n}(A)\longrightarrow M_{l,n}(A)$。

從定義不難驗證，如果 $C,C'\in M_{m,n}(A)$、$D,D'\in M_{l,m}(A)$ 與 $E\in M_{k,l}(A)$，則 $D(C+C')=(DC)+(DC')$、$(D+D')C=(DC)+(D'C)$ 且 $(ED)C=E(DC)$。

定義 2.4.2 (行列式)**.** 令 $C=(c_{jk})$ 為 A 上的一個 $n\times n$ 矩陣。我們定義 C 的行列式

$$\det C=|C|:=\sum_{\sigma\in S_n}(-1)^{\mathrm{sgn}(\sigma)}a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)},$$

這裡 S_n 為全體由 $\{1,2,\ldots,n\}$ 映至自身的所有對射 (一一對應)，而任一個這樣的對射稱作一個 $\{1,2,\ldots,n\}$ 的排列。可以證明任何排列可以分解為一連串的對換 (把某兩元素映為對方，其它元素映至本身)，而且這樣的對換個數的奇偶性只與 σ 有關；我們分別以 $\mathrm{sgn}(\sigma)=\pm1$ 表示 σ 是一個奇排列或偶排列。注意到在上式面的和式中共有 $n!$ 個項。

行列式最基本的性質之一是與線性方程組有關。以下的定理在標準的線性代數教材中都會提到。

定理 2.4.1. 令 K 為一體，考慮線性方程組

$$\begin{cases} c_{11}x_1+c_{12}x_2+\cdots+c_{1n}x_n=0\\ c_{21}x_1+c_{22}x_2+\cdots+c_{2n}x_n=0\\ \quad\cdots\cdots\cdots\cdots\cdots\cdots\\ c_{n1}x_1+c_{n2}x_2+\cdots+c_{nn}x_n=0\end{cases},$$

這裡所有的 c_{jk} 都是 K 中的元素。那麼，這個方程組有一組坐標不全為零的解的充分與必要條件為 $\det C=0$。

證明. 能最簡單地看出這個定理成立的方法是利用 Gauss 消去法。首先，這個方程組可以簡記成 $CX = 0$，這裡 X 為以 $x_1, \ldots, x_n$ 為分量的行向量。進行 Gauss 消去法的過程相當於連續地對 C 施做兩種初等列運算 (elementary row operations)，一種是將矩陣的某兩列互換，另一種為將某特定列加上另一特定列的某倍。不斷進行列運算，最後可以將係數矩陣的非零位置變成特定的階梯狀，從這個形狀可以看出定理的結論成立。另一方面，從行列式的定義可以看出，初等列運算對行列式的影響最多只是加上一個負號，不影響是否為零。另一方面，這些列運算對矩陣 C 的影響為左乘了某些可逆矩陣，故亦不影響「是否有一組坐標不全為零的解」這個問題的答案。因此定理對原始的方程組亦成立。