

# 初等代数和几何的判定法

A. 塔爾斯基 著  
J. C. C. 麥克鏗賽

科学出版社

# 初等代數和幾何的判定法

A. 塔爾斯基 著  
J.C.C. 麥克鏗賽  
陸 鍾 萬 譯

科 學 出 版 社

1959

A. TARSKI  
J. C. C. MCKINSEY  
A DECISION METHOD FOR  
ELEMENTARY ALGEBRA AND GEOMETRY  
SECOND EDITION, REVISED  
1951

內 容 簡 介

本書說明什麼是判定問題，並且敘述了一些普通數學理論(初等代數和幾何)的判定方法。

本書內容分為緒論和三節。

緒論中說明什麼是判定問題及其重要性，並舉出若干判定問題已經解決的數學理論。

第一節描述初等代數的系統。

第二節詳細地說明了初等代數的判定方法。

第三節討論這個判定法對於初等幾何及其它有關係的推廣，並說明一些未解決的問題。

本書對於數學工作者及數理邏輯工作者有很大意義，它對於中學數學教學亦很有意義。因為用了這個判定方法，對於任何一個初等代數與幾何中的命題，總可以一步步地判定這個命題是否是眞的、因而對於初等代數與幾何的問題作了徹底的解決。

初等代數和幾何的判定法

A. 塔爾斯基 著  
J. C. C. 麥克金賽 著  
陸鍾萬 譯

\*

科學出版社出版 (北京朝陽門大街 117 號)  
北京市書刊出版業營業許可證出字第 061 號

科學出版社上海印刷廠印刷 新華書店總經售

\*

1959年2月第一版 書號: 1635 字數: 55,000  
1959年2月第一次印刷 開本: 787×1092 1/32  
(編) 1-13,840 印張: 2 1/3

定價: (9) 0.30 元

## 目 錄

緒論	1
1. 初等代數系統	9
2. 初等代數的判定法	19
3. 對於有關系統的推廣	52
註解	56
參考文獻	69
補充註解	72

## 緒 論

所謂語句(或其它表達式)類 $K$ 的判定法,是指這樣一個方法,用了它,我們能在有窮多個步驟之內判定一個任意給定的語句 $\Theta$ 是否屬於 $K$ ;類 $K$ 的判定問題就是給 $K$ 找出判定法的問題。判定法必須像藥方一樣,能告訴我們每一步做些什麼,使得在照着它做的時候不再需要任何知識;人們只要能認識並且照着所指出的去做,就能應用判定法。

希爾伯特(D. Hilbert)着重地指出了判定問題對於整個數學(以及對於各個特殊的數學理論)的重要性,他把判定問題看作一個新的數學研究領域中的主要工作,這個新領域他取名為“元數學”(metamathematics)。判定問題中最重要的一種是這樣的,其中的 $K$ 是某個理論中所有真語句的類。如果我們說某個理論是有判定法的,那就是說這個理論的真語句的類是有判定法的<sup>(1)</sup>(所有在右上角圓括號中的數目字是指後面從第56頁開始的註解)。

有些判定法很早就知道了。例如,輾轉相除法在它的功用之中特別給具有“ $p$ 和 $q$ 是互素的”形式的真語句的類提供了判定法,其中的 $p$ 和 $q$ 是整數(或者是有常係數的多項式)。又如史得姆(Sturm)定理使我們能判定一個多項式有幾個根,因而能判定具有“多項式 $p$ 恰好有 $k$ 個根”形式的語句的真確性。

其它的一些判定法是較近才得出的。勒文海姆(L. Löwenheim)在1915年給僅含有一個變項的狹謂詞演算的真確公式類找到了判定法。波斯特(E. L. Post)在1921年為普通語句演算的熟知的判定法,即所謂真值表方法的有效性給

出了嚴格的證明。蘭福特(C. H. Langford)在1927年給出了綫性次序初等理論的判定法。普列斯波格(M. Presburger)在1930年為僅包含加法運算的那部分整數算術找出了判定法。塔爾斯基(A. Tarski)在1940年給布爾代數的初等理論找到了判定法。麥克鏗賽(J. C. C. McKinsey)在1943年給出了初等格論的真確全稱語句類的判定法。史米列芙夫人(Mrs. W. Szmielew)最近得出了交換羣初等理論的判定法<sup>(2)</sup>。

判定問題亦有一些重要的否定性的結果。從戈德爾(K. Gödel)在1930年所得出的基本結果以及後來由邱吉(A. Church)在1936年和羅塞(J. B. Rosser)在1936年所得出的關於這些基本結果的改進，可以得到下面的結論：任何包括所有初等數論(即用到加法和乘法運算的整數算術)語句的理論都是沒有判定法的——因此整個數學的判定法是不可能有的。羅賓遜夫人(Mrs. J. Robinson)最近給包括所有有理數算術語句的理論得出了類似的結果。我們亦知道，近世代數中的某些部分理論——環的初等理論(由莫斯托夫斯基(A. Mostowski)和塔爾斯基所給出)；羣和格的初等理論(由塔爾斯基所給出)以及域的初等理論(由羅賓遜夫人所給出)是沒有判定法的<sup>(3)</sup>。

在本書中我們要介紹一個方法(這個方法在1930年就已經獲得，但一直沒有發表)<sup>(4)</sup>，它用來判定實數的初等代數中的語句的真確性，因而亦能用來判定初等幾何語句的真確性。

所謂初等代數，是指實數的一般理論中的這樣一個部分，其中我們僅用到表示實數的變量，表示個別數目的常數，例如“0”和“1”；表示施用於實數的初等運算和實數之間的初等關係的符號，例如“+”，“·”，“-”，“<”，“>”和“=”等；還

有初等的邏輯詞項，例如“並且”，“或”，“非”，“有些  $x$ ”和“所有  $x$ ”。在初等代數的公式中有代數方程和不等式；然後，用上面所列舉的邏輯詞項把方程、不等式連結起來，就得到初等代數的語句。例如，下面就是初等代數的兩個語句：

$$0 > (1 + 1) + (1 + 1);$$

對於任意的  $a, b, c$  和  $d$ ，其中  $a \neq 0$ ，存在着  $x$  使得

$$ax^3 + bx^2 + cx + d = 0.$$

上面第一個語句是假的，第二個是真的。

另一方面，在初等代數中我們沒有用變量去代表任意實數的集合或者實數的序列，實數的函數等等。（在本書中，當我們把形容詞“初等的”加到某個理論時，就是指不能用到集合論的概念。）因此，如果當用上面所列舉的基本概念來定義某種代數概念的時候需要用到集合論的工具，那麼這種代數概念是不可能我們的初等代數系統中得到表示的。例如，多項式的一般概念；方程可解性（利用根式）的概念以及其它類似的概念，都是如此。因此，例如下面這個語句就不能算作初等代數的語句：

每個多項式至少有一個根。

相反地，我們可以在初等代數中表述下列各個語句：

每個一次多項式有一個根；

每個二次多項式有一個根；

每個三次多項式有一個根；

等等。因為我們所處理的是實數的代數，而不是複數的代數，所以上述各個語句在奇次數的情形是真的，在偶次數的情形是假的。

應當着重說明，整數（有理數，代數數亦一樣）的一般概念也是不可能在我們的初等代數系統中表示出來的，雖然每個個別的整數很容易表示出來（例如，2 可以表示為  $1 + 1$ ，3 表

示為  $1 + 1 + 1$ , 等等)<sup>(9)</sup>。在初等代數中，變量是代表任意實數的，我們不能設想變量只取整數值。因為如果這樣設想，那就會得到結論：初等代數語句的類包括初等數論的全部語句；而由上面所提到的結果，判定這樣一個類的語句的真假是沒有普遍方法的。因此，下面的語句不是初等代數的語句：

方程

$$x^3 + y^3 = z^3$$

沒有  $x, y, z$  的整數解。

我們希望已經給初等代數語句這個概念作了充分的說明。現在轉向幾何，我們可以粗略地說，所謂初等幾何的語句，就是指能夠通過一個固定的坐標系把它變成初等代數語句的語句。大家知道，大部分在傳統意義下的初等幾何語句是屬於這一類的。然而亦有例外。例如明顯地或者隱含地牽涉到整數一般概念的語句，就是例外。又如關於有任意邊數的多邊形的語句，例如：在任意多邊形中，每一邊小於其餘各邊的和，亦是例外。但這並不是說，涉及點集——任意幾何圖形——的一般概念的語句在我們意義之下亦不是初等的；然而這類語句按照通常的了解却很難算是初等的了。

另一方面，亦有這樣的語句，它們在我們定義之下是初等的，然而普通却不這麼了解。解析幾何中關於任意固定次數的代數曲綫的大部分語句就是這樣的，例如這個定理：任意兩個橢圓最多交於四點。

認識下面這一點是很重要的：當決定一個幾何定理是否初等幾何語句的時候，所用到的僅僅是定理中所包含的概念的性質，而不是證明方法的性質。例如，“每個角能被三等分”這個語句在我們意義之下是初等語句，並且當然是一個真的初等語句，雖然在證明這個語句時一般都主要要用到連續性公理。相反地，用直尺和圓規作圖的一般概念不能在初等幾



何中定義，因此“一個角一般地不能用直尺和圓規被三等分”不是初等語句，雖然我們能够在初等幾何中表達下列事實：一個  $30^\circ$  的角不能經過一次，二次，…或一般地，經過任意固定的  $n$  次應用直尺和圓規而被三等分。

假如把本書所要處理的初等代數和幾何的理論同上面提到的已經找出判定方法的其它理論比較一下，我們可以立刻看出，雖然雙方的邏輯結構同樣是初等的，但本書所研究的理論有着更豐富的數學內容，可以舉出許多能在這些理論中表述的問題，這些問題過去曾在數學的發展中起過重要的作用。在解決這些問題的過程中，一般地在我們所考慮的理論的發展過程中，各種各樣的推理方式都曾被採用過，其中有些是比較複雜的（僅舉一例：像定理“如果三角形中兩個角的平分綫相等，則三角形是等腰的”的證明）。因此，存在着關於初等代數和幾何的普遍適用的判定方法這個事實不能被認為是必然的結論。

由上面這些說明，我們不應期望，即將討論的判定法的數學基礎有着很顯然而不足道的性質。事實上，如果對這個判定法進行分析，讀者會很容易發現，它在數學內容上和一個古典的代數結果——即前面提到過的史得姆定理——有着很密切的連系，它甚至還把這個定理推廣到多個未知數的任意方程和不等式系的情形。

因此從本質上看，應用判定法的時候不需要任何知識，所以很清楚，當人們能够給出語句類  $K$  的判定法時，也就能設計出一架機器來判定一個任意給定的語句是否屬於  $K$ 。不論在純粹的或者應用的數學研究中，都可能發生關於初等代數或幾何中複雜語句的真假問題。本書中所介紹的判定方法保證數學家能够解決每一個這樣的問題，只要照着它進行足夠多的步驟。一旦這樣的機器設計出來，數學家的工作就成為把

問題向機器或者向它的運算者，作出說明。假如能用例子來具體說明判定機器確實有助於未解決的問題的研究，可能是很有益處的。

大家知道，任意兩個面積相等的多邊形  $P$  和  $Q$  能夠各被分解成相等的有窮  $n$  個不相重疊的三角形，使得  $P$  中的每個三角形和  $Q$  中的某個對應的三角形全等。在各種可能的分解中決定所分成的三角形的最小數目，這是一個有趣的問題。在下面我們假設  $P$  是單位正方形， $Q$  是有單位面積的，底邊長  $x$  個單位的矩形。於是，最小數目  $n$  將僅僅依賴於  $x$ ，設以  $d(x)$  代表它；我們的問題就成為對  $x$  的一切正值來描述函數  $d$  的性質。

特別，給定  $x_0$ ，我們能向  $d(x_0)$  的值是多少。在大部分的情形，甚至回答這個簡單的問題亦會有困難；例如，是否  $d(7/2) = 8$  是不很容易看得出來的。然而，我們很容易用直接的幾何論證來確定  $d(x_0)$  的上界；事實上，假如  $1 \leq x_0 \leq n$ ，其中  $n$  是整數，那麼就有  $d(x_0) \leq 2n$ 。因此，在“ $d(x_0) = 1$ ”，“ $d(x_0) = 2$ ”， $\dots$ ，“ $d(x_0) = 2n$ ”這些語句中，恰好有一個是真的。更進一步，假如  $x_0$  是代數數，那麼所有這些語句將都能在初等幾何中表達。所以，只要讓機器開動至多  $2n$  次，我們就能檢查出哪一個語句是真的，從而找出  $d(x_0)$  的值。

我們可以逐一考慮關於函數  $d$  在某些區間內的性質的猜測。隨便舉個例說，下述語句似乎是可以成立的：當  $2 < x \leq 3$  時， $5 \leq d(x) \leq 6$ 。這個猜測在初等幾何中是可以表達的，因此可以用機器來肯定或否定它。但是，當我們考慮更一般的，關於函數  $d$  在它的整個定義域內的性質的猜測，例如這樣的猜測：對於任意的實數  $x$  和整數  $n$ ，假如  $x > n$ ，則  $d(x) > 2n$  的時候，情況就變了。這個猜測甚至對於  $n$  的很小的值都尚未得到證實。這個猜測一般是不能在初等幾何中表達

的，因此也就不能用這裏所設想的機器來試驗。然而，機器却容許我們就  $n$  的任意特定的值來試驗這個猜測，我們能夠對一系列的連續的值， $n = 2, 3, \dots$ ，比方一直到  $n = 100$ ，進行試驗。假如至少有一個試驗得出否定的結果，那就說明猜測是假的；否則，我們對於猜測的信心將會增加，我們將會更敢於去建立它（用通常的數學證明的方法），而不是試圖找出一個反例。

從上面最後的說明可以看出，這個機器對於某些不能在初等代數（或幾何）中表述的問題也可能是有用的。這類問題中最典型的是那種具有“條件  $C_n$  是否對於每一個整數  $n$  都成立？”形式的問題，其中  $C_n$ ，對於  $n$  的每個固定的值來說，是能在初等代數中表達的。這個機器能夠對於  $n$  的一系列連續的值機械地解決這類的問題；其結果，或者是問題不可能在一般的情形得到解決；否則就是解決的可能性似乎有所增加。許多重要而困難的問題都屬於這一類，機器之能夠應用於這類問題可以大大增加它對於數學研究的價值（本書的結果，對於上面所討論的這類問題來說，還有着和機器的應用無關的更多的含義；見補充註解 7）。

從後面關於判定法的詳細描述可以看到，機器能夠服務於更多的目的。我們所遇到的往往不是初等代數的語句，而是某個含有參變量  $a, b, c, \dots$  的，以初等代數的語句來表述的條件；這個條件可能是很複雜的，我們想把它簡化——事實上，是要把它轉化為由代數方程和不等式（以  $a, b, c, \dots$  為未知數的）組成的標準形式。舉例來說，試考慮：要使方程

$$ax^2 + bx + c = 0$$

恰好有兩個實根， $a, b$ ，和  $c$  應滿足什麼樣的必要而且充分的條件。在這個情形，把條件轉化為標準形式是很簡單的；從高中代數教科書就可以知道條件的標準形式是：

$$c \neq 0, \text{ 並且 } b^2 - 4ac > 0.$$

下面所要展開的判定法將保證這種轉化總是可能的；判定機器能機械地完成它。

本書分爲三節。第一節描述作爲判定法作用對象的代數系統。在第二節中，判定法本身將得到詳細的發展。第三節討論已獲得結果的某些推廣和一些有關的未解決的問題。本書最後的註解，除了歷史的和文獻的參考之外，還包括對一些有理論興趣的論點的討論，這些論點和構造判定機器的問題是沒有直接連系的。註解後面的簡短的參考文獻列舉了本書中所援引的著作<sup>(6)</sup>。

## 1. 初等代數系統

在這一節中我們要描述一個初等代數的形式系統，特別是要用嚴格的方法來定義出這個系統的語句的類<sup>(1)</sup>。

所謂變項，我們指下列符號中的任意一個：

$$x, x_1, x_2, \dots; y, y_1, y_2, \dots; z, z_1, z_2, \dots.$$

我們假設有無窮多個變項，它們排成一個序列，使得我們能說某某變項是在這個序列中的第一個，第二個， $\dots$ ，第  $n$  個位置上。我們可以在直覺上設想這些變項的範圍是實數集。

所謂代數常項，我們指以下三個符號之一：

$$1, 0, -1.$$

所謂代數運算符號，我們指以下兩個符號之一：

$$+, \cdot.$$

第一個稱為加號，第二個稱為乘號。

所謂代數項，是指由變項和代數常項用初等運算符號構造起來的任何有意義的表達式。例如

$$x, x_1 + y, -1 \cdot x, [(x_1 \cdot -1) \cdot x_1] + x_2$$

都是代數項。但是

$$x +, \sqrt{2} + x$$

都不是代數項：第一個不是代數項，因為它是無意義的；第二個不是代數項，因為其中含有“ $\sqrt{2}$ ”這樣一個既不是變項也不是代數常項的符號（代數常項當然是限於我們上面所說的意義）。

如果需要作出代數項的嚴格的定義，則可以遞歸地定義如下：第一階的代數項就是變項或者是三個代數常項中的一個。如果  $\alpha$  和  $\beta$  最多是第  $k$  階的代數項，並且  $\alpha$  和  $\beta$  的階數

的最大值是  $k$ ，則  $(\alpha \cdot \beta)$  和  $(\alpha + \beta)$  是第  $k + 1$  階的代數項。一個表達式稱為代數項，如果它是某  $k$  階的代數項。

按照上述定義，我們就應當把對於項施加運算的結果放進括號之中。例如，我們應當寫

$$(x + y) \text{ 和 } (x \cdot y),$$

而不是簡單地寫

$$x + y \text{ 和 } x \cdot y.$$

然而，在不至於引起混淆的情形，我們又常常省略這些括號。一般地，我們將使用通常的約定來省略代數項中的括號。這樣，我們就寫

$$x + y \cdot z$$

來代替

$$[x + (y \cdot z)].$$

減法運算可以像下面這樣引進<sup>(3)</sup>：如果  $\alpha$  和  $\beta$  是任意的項，則令

$$(\alpha - \beta) \equiv [\alpha + (-1 \cdot \beta)].$$

這裏我們用符號“ $\equiv$ ”表示兩個公式的完全相同，而在方才的情形，則是用它來作定義。我們將在整個這一報告中使用這個符號。當我們寫

$$\alpha \equiv \beta$$

時，這就是說， $\alpha$  和  $\beta$  是由完全相同的符號組成的，並且符號的排列次序亦完全相同。例如

$$0 \equiv 0$$

和

$$(0 = 1) \equiv (0 = 1)$$

都是真的；然而

$$(0 + 0) \equiv 0$$

和

$$(0 = 1) \equiv (1 = 0)$$

都不是真的。

引進任意有窮和與積的符號亦是很便利的。設  $\alpha_1, \alpha_2, \dots$  是項的序列，則我們令

$$\sum_{i=1}^1 \alpha_i \equiv \alpha_1,$$

$$\sum_{i=1}^{k+1} \alpha_i \equiv \left( \sum_{i=1}^k \alpha_i + \alpha_{k+1} \right),$$

類似地

$$\prod_{i=1}^1 \alpha_i \equiv \alpha_1,$$

$$\prod_{i=1}^{k+1} \alpha_i \equiv \left( \prod_{i=1}^k \alpha_i \cdot \alpha_{k+1} \right).$$

我們有時亦用

$$\alpha_1 + \alpha_2 + \dots + \alpha_n,$$

或者簡單地用

$$\alpha_1 + \dots + \alpha_n$$

來代替

$$\sum_{i=1}^n \alpha_i;$$

同樣，用

$$\alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_n,$$

或者

$$\alpha_1 \cdot \dots \cdot \alpha_n$$

來代替

$$\prod_{i=1}^n \alpha_i.$$

如果  $\alpha_1, \dots, \alpha_n$  都相同，或者說，都等於  $\alpha$ ，則我們簡單地寫

$$\alpha^n$$

來代替

$$\prod_{i=1}^n \alpha_i.$$

例如

$$\xi^2$$

和

$$[(\xi \cdot \xi) \cdot \xi]$$

有相同的意義。此外，我們有時亦以  $\alpha^0$  代表 1。

所謂代數關係符號，我們指以下兩個符號之一：

$$=, >$$

它們分別稱為等號和大於號<sup>(8)</sup>。

所謂原子公式，我們指具有以下兩種形式之一的表達式：

$$(\alpha = \beta), (\alpha > \beta),$$

其中的  $\alpha$  和  $\beta$  是任意的代數項；按照前面的說明，其中的括號有時是可以省略的。上面的第一種表達式稱為等式，第二種稱為不等式。這樣，例如下面的表達式都是原子公式：

$$1 = 1 + 1,$$

$$0 + x = x,$$

$$x \cdot (y + z) = 0,$$

$$[x \cdot (1 + 1)] + (y \cdot y) > 0,$$

$$x > (y \cdot y) + x.$$

所謂語句連結詞，我們指以下三個符號之一：

$$\sim, \wedge, \vee.$$

第一個稱為否定詞（讀作“非”），第二個稱為合取詞（讀作“並且”），第三個稱為析取詞（讀作“或”——可兼意義下的“或”）。

所謂（存在）量詞，我們指“ $E$ ”這個符號。如果  $\xi$  是任意的變項，則  $(E\xi)$  稱為量詞表達式。表達式  $(E\xi)$  讀作“有  $\xi$  …”。

所謂公式，我們指由原子公式用語句連結詞和量詞構造起來的表達式。例如以下的都是公式：

$$0 = 0,$$

$$(Ex)(x = 0),$$

$$(x = 0) \vee (Ey)(x > y),$$



$$(Ex) \sim (Ey) \sim [(x = y) \vee (x > 1 + y)], \\ \sim (x > 1) \wedge (Ey)(x = y \cdot y).$$

如果需要作出公式的嚴格定義，則可以遞歸地定義公式如下：第一階的公式就是原子公式。如果  $\theta$  是第  $k$  階的公式，則  $\sim\theta$  是第  $k + 1$  階的公式。如果  $\theta$  是第  $k$  階的公式，並且  $\xi$  是變項，則  $(E\xi)\theta$  是第  $k + 1$  階的公式。如果  $\theta$  和  $\phi$  最多是第  $k$  階的公式，並且其中有一個是第  $k$  階的公式，則  $(\theta \wedge \phi)$  和  $(\theta \vee \phi)$  是第  $k + 1$  階的公式。一個表達式是公式，如果它是某  $n$  階的公式。

爲了某種目的，我們要在出現於公式中的變項之中區別所謂“自由”變項。這個概念可以遞歸地定義如下：如果  $\phi$  是原子公式，則  $\xi$  在  $\phi$  中是自由的，必須並且只須  $\xi$  在  $\phi$  中出現； $\xi$  在  $(E\eta)\theta$  中是自由的，必須並且只須  $\eta$  和  $\xi$  是不同的變項，並且  $\xi$  在  $\theta$  中是自由的； $\xi$  在  $\sim\theta$  中是自由的，必須並且只須  $\xi$  在  $\theta$  中是自由的； $\xi$  在  $(\theta \wedge \phi)$  中（在  $(\theta \vee \phi)$  中亦相同）是自由的，必須並且只須  $\xi$  至少在  $\theta$  和  $\phi$  的一個之中是自由的。例如， $x$  在以下各公式中是自由的：

$$x = 1, \\ x = x, \\ (Ey)(y = x), \\ (x = 1) \vee (Ex)(x = 2);$$

但在以下各公式中是不自由的：

$$y = 1, \\ (Ex)(x = x), \\ (Ex)(Ey)(y = x).$$

（爲了某種目的，我們需要一個更爲微妙的概念，即一個變項在一公式中在某個出現的地方是否自由的概念。例如，在公式