

初等几何判定问题与机械化证明

吴 文 俊

(中国科学院数学研究所)

摘 要

机械化证明定理,目前值得注意的是 Tarski 关于初等几何与初等代数定理的机械证明法. 他以及后来一些研究工作者的方法,大都基于 Sturm 定理的某种推广,这些方法仍极繁复,因之即使使用了计算机,实际上也是难以实现的. 本文的目的,在于把定理限制在不牵涉到“之间”关系的情形,应用完全不同的原理给出初等几何定理的机械化证法. 这种方法仅用手算即可给出不太简单的定理的证明.

一、问题的提出

Tarski 在 1948 年的一篇经典著作^[1]中,解决了实闭域的判定问题,其主要目的之一,是给出初等几何定理的机械化证明. 以后 Seidenberg^[2], Robinson^[3] 与 Cohen^[4] 等人又给出了 Tarski 定理的不同证法. 这些作者还提出了制作某种判定机器以实现这些机械化证明的建议. 但是,这种建议离实现之期似颇遥远^[5,6]. 事实上,只有一些极不足道的初等几何定理,曾在计算机上证明过,例如文献 [7, 8]. 本文的目的是在不考虑点的“之间”关系的情况下,给出初等几何判定问题的另一解法. 我们的解法,依据了与前面那些作者所使用的完全不同的原理,提供了几何定理的机械化证明,即使颇为困难的定理,仅用纸和笔也往往可实现. 依据这种方法编成程序,在计算机上进行计算,也不应发生实质上的困难.

我们考虑的仅限于平面初等几何,虽然所用方法也可应用于其它各种几何. 方法的第一步,在于几何问题的代数化. 平面中的点,将定义为某一固定域,例如有理数域 R 上的有序数偶. 其次是建立一部辞典,把几何关系翻译成为代数形式,不妨把这些看作定义或公理. 例如对于若干个点的 $A_i = (x_i, y_i)$, 不论重合与否,可规定:

A_1A_2 平行于 A_3A_4 , 如果 $(x_1 - x_2)(y_3 - y_4) - (x_3 - x_4)(y_1 - y_2) = 0$,

A_1A_2 垂直于 A_3A_4 , 如果 $(x_1 - x_2)(x_3 - x_4) + (y_1 - y_2)(y_3 - y_4) = 0$,

A_1A_2 的长度平方为 $r^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$,

等等.

如果把基本域 R 易为其它的域,或把点当作其它类型的数组,或改变公理中的代数形式,例如把上面长度平方函数 r^2 改为函数 $r^4 = (x_1 - x_2)^4 + (y_1 - y_2)^4$, 我们即进入别的几何领域,例如非欧几何,实或复的投影几何,有限几何,等等. 但在本文中,将以平面初等几何为限,

因为它可以说是具有代表性的.

作为说明,先举一个简单的例子如下.

试考虑下述语句:

(S_n) 设 $A_0A_1A_2$ 是一直角三角形, 直角在 A_0 , 记直角边 A_0A_1 , A_0A_2 的长为 x_1 , x_2 , 斜边的长为 x_3 , 则有

$$x_1^n + x_2^n = x_3^n.$$

我们的问题是如何判定语句 (S_n) 的真伪. 我们所用以证明或否定 (S_n) 的判定算法, 应对初等几何中的一切类似的语句(不考虑“之间”的关系)都同样适用.

为解决这一问题, 试首先注意在语句中出现的那些点, 在语句假设所含的条件限制之下, 具有普定性质, 因此, 若将这些点用座标表示为 $A_0 = (x_0, v_0)$, $A_1 = (u_1, v_1)$, $A_2 = (u_2, v_2)$, 诸座标 v_0, u_1, v_1, u_2, v_2 可视为不定量, 而其它座标与几何度量 x_0, x_1, x_2, x_3 则代数地依赖于这些不定量, 依据语句 (S_n) 中的假设为以下诸代数方程所制约:

$$f_0 \equiv (u_1 - x_0)(u_2 - x_0) + (v_1 - v_0)(v_2 - v_0) = 0,$$

$$f_1 \equiv x_1^2 - (u_1 - x_0)^2 - (v_1 - v_0)^2 = 0,$$

$$f_2 \equiv x_2^2 - (u_2 - x_0)^2 - (v_2 - v_0)^2 = 0,$$

$$f_3 \equiv x_3^2 - (u_1 - u_2)^2 - (v_1 - v_2)^2 = 0.$$

至于语句 S_n 中的结论则相当于等式

$$g_n \equiv x_3^n - x_1^n - x_2^n = 0,$$

在以后, 将以 R 表示有理数域, 并取之为基本域. 命 A^9 为 R 上的 9 维仿射空间, 以 $(v_0, u_1, v_1, u_2, v_2, x_0, x_1, x_2, x_3)$ 为座标, 并按上述确定次序排列. 于是以上诸方程 $f_i = 0$ 在 A^9 中定义了一个 5 维的代数簇, 在本例中, 在 R 上不可约, 并有普点例如 $(v_0, u_1, v_1, u_2, v_2, \bar{x}_0, \bar{x}_1, \bar{x}_2, \bar{x}_3)$, 其中 v_0, u_1, v_1, u_2, v_2 为独立的不定量. 于是语句 (S_n) 的真伪与否相当于

$$g_n \text{ 在 } V \text{ 上 } \equiv 0$$

或

$$g_n \text{ 在 } V \text{ 上 } \not\equiv 0.$$

由以上分析可知, 一般的判定问题可依下面的形式表达.

问题. 在一 R 上以 $(u_1, \dots, u_d, x_1, \dots, x_n)$ 为座标的 $n = r + d$ 维仿射空间 A^n 中, 设有一代数簇 V , 其定义方程是 $(u_1, \dots, u_d$ 是独立的不定量):

$$\left. \begin{aligned} f_1(u_1, \dots, u_d, x_1) &= 0, \\ f_2(u_1, \dots, u_d, x_1, x_2) &= 0, \\ \dots & \\ f_r(u_1, \dots, u_d, x_1, x_2, \dots, x_r) &= 0. \end{aligned} \right\} \quad (I)$$

这一代数簇 V 分裂成若干不可约成份, 其维数假定都 $\leq d$, 其中 d 维成份的总和为 V^* , 通常与 V 相合. V^* 的每一成份具有形如 $(u_1, \dots, u_d, \bar{x}_1, \dots, \bar{x}_r)$ 的普点, 其中 $\bar{x}_i$ 都是域

$$K = R(u_1, \dots, u_d)$$

上的代数量. 另设有一多项式 $g(u_1, \dots, u_d, x_1, \dots, x_r)$ 或多项式组 $g_k \in R[u_1, \dots, u_d, x_1, \dots, x_r]$. 问题是要依据一种算法来判定在 V^* 上是否

$$g \equiv 0 \text{ (或 } g_k \equiv 0).$$

在上述问题的提法中,代数簇 V 或 V^* 反映了几何语句中的假设部份. V 或 V^* 将称为该语句的相关簇.若视簇 V^* 为定义于域 $K = R(u_1, \dots, u_d)$ 上时,其维数为0.方程组(I)的形式说明代数依赖的变量 $x_1, \dots, x_r$ 应依次地逐一添入域 K .这反映了这样的几何事实:在某些普定的直线或圆上取某些普定的点,又应用作联线,平行线,垂直线或圆,并取直线或圆的交点等等几何手续,依次代数地添入新的点.这些几何作法产生含有 x 与 u 的代数方程,只须用简单的消去法即可化成方程组(I)的形式.因为事实上 x 与 u 间的原始方程很少会是超过2次的.我们将称变量 u 为参量而 x 为依量.其次注意 V 的诸不可约成份在 R 上的维数都 $\leq d$ 这一条件,无非反映了我们所考虑的几何语句都具有确定性质,而把考虑限制于 V^* ,则指退化情形将排除在外.这两者事实上都是通常几何定理中隐含,而不加明述的假设.至于多项式 g 或 g_k 在 V^* 上 $\equiv 0$,则是所需证明或否决的语句中结论部份的代数等价式.在以下,我们将称 g 或 g_k 为相应几何语句的判定多项式(组).

在理论上, Hermann^[9]所用的方法,早就足以给出上述判定问题的算法的解答.但是,他的方法如此繁复,不可避免地要引起诸算式的天文数字般的膨胀,以致即使是最简单不过的几何定理,也无法加以证明.相反,我们在下面所用的判定方法,利用了方程组(I)的特殊形式,只需用纸笔即可给出很不简单的定理以机械化的证明.

我们的判定方法依据了以下三个定理,证明见第四节.

定理1. 有一算法,据此可将任一确定性几何语句由(I)式定义的相关簇 V^* ,分裂成 R 上的不可约成份,使每一 d 维成份 V' 视作定义于域 $K = R(u_1, \dots, u_d)$ 上时,有一形如 $(p_1, \dots, p_r)$ 的基(即相应素理想的基),具有以下诸性质:

(T1)₁ 每一 p_i 是一 $R[u_1, \dots, u_d, x_1, \dots, x_r]$ 中的多项式,对 x_i 的次数 $m_i > 0$.

(T1)₂ 视 p_i 为 x_i 的多项式时,其系数都是 $R[u_1, \dots, u_d, x_1, \dots, x_{i-1}]$ 中的多项式,设有公共因子,且对每一 $j = 1, \dots, i-1$, x_j 的次数都小于 m_j .

(T1)₃ 视 p_i 为 x_i 的多项式时,其主系数是 $R[u_1, \dots, u_d]$ 中的多项式且 $\neq 0$.

(T1)₄ 作为 x_1 的多项式 p_1 ,在域 $K = R(u_1, \dots, u_d)$ 中不可约.又对每一 $i > 1$,视作 x_i 的多项式 p_i ,在依方程 $p_1 = 0, \dots, p_{i-1} = 0$ 将 $x_1, \dots, x_{i-1}$ 添入 K 中所得的扩充域上不可约.

显然多项式 $p_1, \dots, p_r$ 为 V' 所唯一确定到 R 中的因子,我们将称之为构成 V' 的一个优选基(更正确地说是 V' 在 K 上的素理想的一个优选基).但须注意,诸依量 $x_1, \dots, x_r$ 依照所给定的次序排列,又注意这一概念事实上为 Gröbner 所引入,被称为素基,如参阅文献[10],又可参阅文献[11]中与此密切相关的一个概念: Characteristic sets.

定理2. 设 $(p_1, \dots, p_r)$ 是相关簇 V 的任一不可约成份 V' 的优选基.有一算法,据此足以对任一 $R[u_1, \dots, u_d, x_1, \dots, x_r]$ 中的多项式 h ,确定一等式形如

$$Dh = \sum_{i,j=0}^{m_j-1} h_{i_1 \dots i_r} x^{i_1} \dots x^{i_r} + \sum_{i=1}^r A_i p_i,$$

使满足以下诸条件:

(T2)₁ $D, h_{i_1 \dots i_r}$ 都是 $R[u_1, \dots, u_d]$ 中的多项式,且 $D \neq 0$.

(T2)₂ A_i 都是 $R[u_1, \dots, u_d, x_1, \dots, x_r]$ 中的多项式.

诸多项式 $h_{i_1 \dots i_r}$ 由算法所唯一确定至 R 中的因子,将称为多项式 h 相应于 V' 的优选基

$(p_1, \dots, p_r)$ 的余系式, 或简称为相应于 V' 的余系式.

定理 3. 相关簇是 V 而判定多项式(组)是 g (或 g_k) 的一个几何语句, 其成立的充要条件是: 任意取定依量 $x_1, \dots, x_r$ 的一个固定次序后, g (或 g_k) 对 V^* 的任一不可约成份 V' 的一切余系式都恒等于 0.

二、举 例

在给出这些定理的证明之前(见第四节), 先举例说明其应用如下:

例 1. 对于本文开始所举直角三角形的语句 (S_n) , 可见相关簇 V 的参量与依量各取为 v_0, u_1, u_2, v_1, v_2 与 x_0, x_1, x_2, x_3 时, 在 R 中不可约且有一优选基 (p_1, p_2, p_3, p_4) 如下:

$$\begin{aligned} p_1 &= x_0^2 - (u_1 + u_2)x_0 + u_1u_2 + (v_1 - v_0)(v_2 - v_0), \\ p_2 &= x_1^2 + (u_1 - u_2)x_0 - u_1^2 + u_1u_2 - (v_1 - v_0)(v_1 - v_2), \\ p_3 &= x_2^2 - (u_1 - u_2)x_0 - u_2^2 + u_1u_2 + (v_2 - v_0)(v_1 - v_2), \\ p_4 &= x_3^2 - (u_1 - u_2)^2 - (v_1 - v_2)^2, \end{aligned}$$

由此得

$$g_2 = p_4 - p_2 - p_3,$$

而在 $n > 2$ 时, 有

$$g_n \not\equiv 0 \pmod{(p_1, p_2, p_3, p_4)}.$$

因此语句 (S_n) 只在 $n = 2$ 时成立, 即所谓勾股定理.

例 2. 我们的判定方法可用以给出三角恒等式的机械化证明. 例如试考虑下述语句:

(S) 若 $A_1 + A_2 + A_3 = 180^\circ$, 则

$$\sin 2A_1 + \sin 2A_2 + \sin 2A_3 = 4 \sin A_1 \sin A_2 \sin A_3.$$

(C) 若 $A_1 + A_2 + A_3 = 180^\circ$, 则

$$\cos 2A_1 + \cos 2A_2 + \cos 2A_3 + 4 \cos A_1 \cos A_2 \cos A_3 = 0.$$

为判定 (S) 或 (C) 的真实性, 先置

$$\begin{aligned} \sin A_i &= s_i, \quad \cos A_i = c_i \quad (i = 1, 2), \\ \sin 2A_i &= x_i, \quad \cos 2A_i = y_i \quad (i = 1, 2, 3), \\ \sin A_3 &= z_1, \quad \cos A_3 = z_2. \end{aligned}$$

取 c_1 与 c_2 为参量, 而

$$s_1, s_2, z_1, z_2, x_1, x_2, x_3, y_1, y_2, y_3$$

为依量(依上述次序), 则 (S) 与 (C) 的相关簇已在 R 中不可约, 且有一优选基 $(p_1, \dots, p_{10})$ 如下:

$$\begin{aligned} p_1 &= s_1^2 + c_1^2 - 1, & p_2 &= s_2^2 + c_2^2 - 1, \\ p_3 &= z_1 - c_2s_1 - c_1s_2, & p_4 &= z_2 - s_1s_2 + c_1c_2, \\ p_5 &= x_1 - 2c_1s_1, & p_6 &= x_2 - 2c_2s_2, \\ p_7 &= x_3 - 2z_1z_2, & p_8 &= y_1 - 2c_1^2 + 1, \\ p_9 &= y_2 - 2c_2^2 + 1, & p_{10} &= y_3 + 4c_1c_2s_1s_2 - 4c_1^2c_2^2 + 2c_1^2 + 2c_2^2 - 1. \end{aligned}$$

语句 (S) 与 (C) 的判定多项式各为:

$$g_S = x_1 + x_2 + x_3 - 4s_1s_2z_1,$$

$$g_C = y_1 + y_2 + y_3 + 4c_1c_2z_2.$$

验算得

$$\begin{aligned} g_S &= p_7 + p_6 + p_5 + 2z_1p_4 - 2p_3(s_1s_2 + c_1c_2) - 2c_1s_1p_2 - 2c_2s_2p_1 \\ &\equiv 0 \pmod{(p_1, \dots, p_{10})}. \end{aligned}$$

$$\begin{aligned} g_C &= -1 + p_{10} + p_9 + p_8 + 4c_1c_2p_4 \\ &\not\equiv 0 \pmod{(p_1, \dots, p_{10})}. \end{aligned}$$

由此知 (S) 给出一真恒等式而 (C) 则不然.

例 3. 试考虑 Simson 线定理, 其相应语句为:

(S_i). 从 $\triangle A_1A_2A_3$ 外接圆上一点 A_4 , 向三角形三边作垂线, 其垂足必同在一直线上.

为证此, 可简化取外接圆心为 $(0, 0)$, 而半径为 r . 记 $A_i (i = 1, 2, 3, 4)$ 为 (x_i, u_i) , 而垂足 A_j 为 (x_j, y_j) , $j = 5, 6, 7$. 以 r, u_1, u_2, u_3, u_4 作为参量, 而

$$x_1, x_2, x_3, x_4, y_5, y_6, y_7, x_5, x_6, x_7$$

为依量, 其次序即如上述.

相关 Simpson 簇不可约, 且有优选基 $(p_1, \dots, p_{10})$ 如下:

$$\begin{aligned} p_1 &= x_1^2 + u_1^2 - r^2, & p_2 &= x_2^2 + u_2^2 - r^2, \\ p_3 &= x_3^2 + u_3^2 - r^2, & p_4 &= x_4^2 + u_4^2 - r^2, \\ p_5 &= 2r^2y_5 - h_5, & p_6 &= 2r^2y_6 - h_6, \\ p_7 &= 2r^2y_7 - h_7, & p_8 &= u_{23}x_5 - x_{23}y_5 + u_3x_2 - u_2x_3, \\ p_9 &= u_{31}x_6 - x_{31}y_6 + u_1x_3 - u_3x_1, & p_{10} &= u_{12}x_7 - x_{12}y_7 + u_2x_1 - u_1x_2, \end{aligned}$$

在上面的方程中, 已采用了下述简化符号:

$$\left. \begin{aligned} u_{ij} &= u_i - u_j \\ x_{ij} &= x_i - x_j \end{aligned} \right\} (i, j = 1, 2, 3).$$

$$h_5 = u_4x_2x_3 - (u_2x_3 + u_3x_2)u_4 + r^2(u_2 + u_3 + u_4) - u_2u_3u_4.$$

h_6 与 h_7 式与此类似.

判定多项式为:

$$g = x_5(y_6 - y_7) + x_6(y_7 - y_5) + x_7(y_5 - y_6).$$

直截的计算给出

$$g \equiv 0 \pmod{(p_1, \dots, p_{10})},$$

这证明了 Simson 语句 (S_i) 的真确性.

例 4. 作为一个比较非不足道的例子, 试考虑 Feuerbach 定理, 它的相应语句为:

(S_F). 三角形的九点圆与四个内切傍切圆相切.

试记三角形的三顶点为 $(2u_i, 2v_i)$, 九点圆的中心为 (x_1, y_1) , 半径为 r_1 , 而任一内切或傍切圆的中心为 (x_2, y_2) , 半径为 r_2 , 又引入变量 z_1, z_2, z_3 各与三角形三边之长相当, 于是以 $u_1, v_1, u_2, v_2, u_3, v_3$ 为参量, 而 $z_1, z_2, z_3, x_1, y_1, x_2, y_2, r_1, r_2$ 为依量 (次序如上) 时, 相关 Feuerbach 簇 V_F 分裂成四个不可约簇, 具有以下形式的优选基 $(p_1, \dots, p_9)$:

$$\begin{aligned} p_1 &= z_1^2 - u_{23}^2 - v_{23}^2, & p_2 &= z_2^2 - u_{31}^2 - v_{31}^2, \\ p_3 &= z_3^2 - u_{12}^2 - v_{12}^2, & p_4 &= 4\Delta x_1 - \alpha_1, \\ p_5 &= 4\Delta y_1 - \beta_1, & p_6 &= 4\Delta x_2 - \alpha_2, \end{aligned}$$

$$\begin{aligned} p_7 &= 4\Delta y_2 - \beta_2, & p_8 &= 4\Delta r_1 - z_1 z_2 z_3, \\ p_9 &= 2\Delta r_2 + \gamma. \end{aligned}$$

在以上诸公式中,我们采用了下面的简记符号($\varepsilon_i = \pm 1$):

$$u_{ii} = u_i - u_j, \quad v_{ij} = v_i - v_j \quad (i, j = 1, 2, 3),$$

$$\Delta = \begin{vmatrix} u_1 & v_1 & 1 \\ u_2 & v_2 & 1 \\ u_3 & v_3 & 1 \end{vmatrix},$$

$$\alpha_1 = v_{23}v_{31}v_{12} + u_1^2v_{23} + u_2^2v_{31} + u_3^2v_{12} - 2(u_2u_3v_{23} + u_3u_1v_{31} + u_1u_2v_{12}),$$

$$\beta_1 = u_{23}u_{31}u_{12} - v_1^2u_{23} - v_2^2u_{31} - v_3^2u_{12} + 2(v_2v_3u_{23} + v_3v_1u_{31} + v_1v_2u_{12}),$$

$$\alpha_2 = -[v_{23}v_{31}v_{12} + v_1(u_2^2 - u_3^2) + v_2(u_3^2 - u_1^2) + v_3(u_1^2 - u_2^2)$$

$$+ \varepsilon_2\varepsilon_3v_{23}z_2z_3 + \varepsilon_3\varepsilon_1v_{31}z_3z_1 + \varepsilon_1\varepsilon_2v_{12}z_1z_2],$$

$$\beta_2 = u_{23}u_{31}u_{12} + u_1(v_2^2 - v_3^2) + u_2(v_3^2 - v_1^2) + u_3(u_1^2 - u_2^2)$$

$$+ \varepsilon_2\varepsilon_3u_{23}z_2z_3 + \varepsilon_3\varepsilon_1u_{31}z_3z_1 + \varepsilon_1\varepsilon_2u_{12}z_1z_2,$$

$$\gamma = \varepsilon_1(u_{31}u_{12} + v_{31}v_{12})z_1 + \varepsilon_2(u_{12}u_{23} + v_{12}v_{23})z_2$$

$$+ \varepsilon_3(u_{23}u_{31} + v_{23}v_{31})z_3 + \varepsilon_1\varepsilon_2\varepsilon_3z_1z_2z_3.$$

注意 $\varepsilon_i = +1$ 或 -1 的选择相应于四个内切或傍切圆,并反映了 Feuerbach 簇的分裂.

语句(S_F)的判定多项式形如

$$g_\eta = (\eta r_1 - r_2)^2 - (x_1 - x_2)^2 - (y_1 - y_2)^2,$$

其中 $\eta = +1$ 或 -1 . 通过冗长繁复,但直截了当的计算,验得在 $\eta = +\varepsilon_1\varepsilon_2\varepsilon_3$ 时, g_η 为 $p_1, \dots, p_9$ 的线性组合,而在 $\eta = -\varepsilon_1\varepsilon_2\varepsilon_3$ 时则不然. 由此知 Feuerbach 语句(S_F)为一真实定理,而 $\eta = +\varepsilon_1\varepsilon_2\varepsilon_3$ 则反映了九点圆与相应内切或傍切圆之间的相切方式. 注意:在我们问题的提法下“之间”关系并不考虑在内,因而圆的相切方式我们并不重视. 因此,我们可以取 $g = g_{+1} \cdot g_{-1}$ 为判定多项式,同样也可不引入 z_1, z_2, z_3 , 而在 u_i, v_i, x_i, y_i, r_i 的仿射空间中取定 Feuerbach 簇,这样它在一开始就将是不可约的.

三、一些引理

为了证明定理作些准备,本节中将考虑一个在基本域 R 上的扩充域 $R(u_1, \dots, u_d, x_1, \dots, x_r)$, 其中 $u_1, \dots, u_d$ 在 R 上超越,而 $x_1, \dots, x_r$ 在 R 上是代数的,后者的代数扩充则由以下诸方程所确定:

$$\left. \begin{aligned} p_1(x_1) &\equiv p_{10}x_1^{m_1} + p_{11}x_1^{m_1-1} + \dots + p_{1m_1} = 0, \\ p_2(x_1, x_2) &\equiv p_{20}x_2^{m_2} + p_{21}x_2^{m_2-1} + \dots + p_{2m_2} = 0, \\ &\dots \\ p_r(x_1, \dots, x_r) &\equiv p_{r0}x_r^{m_r} + p_{r1}x_r^{m_r-1} + \dots + p_{rm_r} = 0, \end{aligned} \right\} \quad (\text{II})$$

我们假定对 $1 \leq i \leq r$, 诸 p_{ij} 都是环

$$P_{i-1} = R[u_1, \dots, u_d, x_1, \dots, x_{i-1}]$$

中的多项式, p_{i0} 都是

$$P_0 = R[u_1, \dots, u_d]$$

中 $\neq 0$ 的多项式,而将 p_i 视为 x_i 的多项式时, p_i 在由

$$p_1(x_1) = 0, \cdots, p_{i-1}(x_1, \cdots, x_{i-1}) = 0$$

等方程所定的域

$$K_{i-1} = R(u_1, \cdots, u_d, x_1, \cdots, x_{i-1})$$

上不可约. 这里 K_0 指域 $K_0 = K = R(u_1, \cdots, u_d)$.

以 $\mathcal{J}$ 表示一切指数组 $I = (i_1, \cdots, i_r)$ 的集体, 其中 $0 \leq i_j \leq m_j - 1$. 对这些 I 将采用形式记号

$$x^I = x_1^{i_1} \cdots x_r^{i_r},$$

任一形如

$$A = \sum a_I x^I$$

的多项式, 其中 a_I 为某一环或域 F 中的元素时, 将称为 $F[x_1, \cdots, x_r]$ 中的一个规范多项式.

引理 1. 有一算法, 足以对任一 P_r 中的多项式 A , 唯一地确定一组整数 $s_1, \cdots, s_r \geq 0$ 与一组 P_0 中的多项式 $A_I, I \in \mathcal{J}$, 使满足以下诸条件:

(L1)₁ 除去 P_r 上 p_i 间的一个线性组合外, 有

$$p_{r0}^{s_1} \cdots p_{r1}^{s_r} A \equiv \sum A_I x^I.$$

(L1)₂ A_I 都是 P_0 中的多项式, 其系数对 A 作为 P_r 中多项式的系数说来是线性的.

(L1)₃ $s_1, \cdots, s_r \geq 0$ 是使 (L1)₁ 与 (L1)₂ 成立的最小整数.

证. 视 A 与 p_r 为系数在 P_{r-1} 中的 x_r 的多项式, 应用除法即可得一最小整数 $s_r \geq 0$, 使下式成立:

$$p_{r0}^{s_r} A = Q_r p_r + R_{r-1},$$

其中 Q_r, R_{r-1} 为 P_r 中的多项式, 而 R_{r-1} 对 x_r 的次数 $< m_r$. 今视 p_r 与 R_{r-1} 为系数在 $R[u_1, \cdots, u_d, x_1, \cdots, x_{r-2}, x_r]$ 中的 x_{r-1} 的多项式, 仍用除法可得一最小整数 $s_{r-1} \geq 0$, 使下式成立:

$$p_{r-1,0}^{s_{r-1}} R_{r-1} = Q_{r-1} p_{r-1} + R_{r-2}.$$

其中 Q_{r-1}, R_{r-1} 都是 P_r 中的多项式, 而 R_{r-2} 对 x_r 与 x_{r-1} 的次数各 $< m_r$ 与 m_{r-1} . 依次进行, 可相继得:

$$p_{r-2,0}^{s_{r-2}} R_{r-2} = Q_{r-2} p_{r-2} + R_{r-3},$$

...

$$p_{10}^{s_1} R_1 = Q_1 p_1 + R_0,$$

其中 R_0 为一 P_r 中的多项式, 对 x_i 的次数 $< m_i, 1 \leq i \leq r_1$ 于是可将 R_0 写成 $\sum A_I x^I$, 而得引理所需符合诸条件的多项式.

引理 2. 有一算法足以对任一以 y 为不定量的多项式

$$A = A_0 y^m + A_1 y^{m-1} + \cdots + A_m,$$

其中 $A_i \in P_r$, 而 A_0 在 K_r 中 $\neq 0$, 确定以下两式:

$$HA = B + C_1 p_1 + \cdots + C_r p_r,$$

$$B = B_0 y^m + B_1 y^{m-1} + \cdots + B_m,$$

使满足以下诸条件:

(L2)₁ 诸 B_i 都是 P_r 中的规范多项式, 且 B_0 是 P_0 中 $\neq 0$ 的多项式.

(L2)₂ C_i 都是 $P_r[y]$, 而 H 是 P_r 中的多项式.

(L2)₃ $H \not\equiv 0 \pmod{(p_1, \cdots, p_r)},$

任意这样满足 $(L2)_i$ 的多项式 B , 将称为 P_r 上以 y 为不定量的规范多项式.

证. 由引理 1 可得整数 $s_1, \dots, s_r \geq 0$ 与下式:

$$p_{10}^{s_1} \cdots p_{r0}^{s_r} A = A'_0 y^m + A'_1 y^{m-1} + \cdots + A'_m \bmod (p_1, \dots, p_r),$$

其中 A'_i 都是 P_r 中的规范多项式, 且 A'_0 在 K_r 中 $\neq 0$. 设 A'_0 与 $x_{i+1}, \dots, x_r$ 无关, 但确实含有 x_i , 因 A'_0 对 x_i 的次数 $< m_i$, p_i 对 x_i 的次数为 m_i , 且在 K_{i-1} 中不可约, 故由通常的除法程序算法可得 P_i 中的多项式 h, k 以及 P_{i-1} 中的多项式 A'_{00} , 使

$$hA'_0 + kp_i = A'_{00},$$

其中 h 在 K_i 中 $\neq 0$, 而 A'_{00} 在 K_{i-1} 中 $\neq 0$. 由此得下式:

$$hp_{10}^{s_1} \cdots p_{r0}^{s_r} A + kp_i y^m = A'_{00} y^m + hA'_1 y^{m-1} + \cdots + hA'_m \bmod (p_1, \dots, p_r).$$

应用引理 1 于 A'_i 与 A'_{00} , 可得下式:

$$h''A = A''_0 y^m + A''_1 y^{m-1} + \cdots + A''_m \bmod (p_1, \dots, p_r),$$

其中 A''_i 都是 P_r 中的规范多项式, A''_0 在 K_r 中 $\neq 0$, 且不含有任一 $x_i, i \geq i$. 又 h'' 为 P_r 中的多项式, 且在 K_r 中 $\neq 0$. 若 A''_0 中不再含有任一 $x_1, \dots, x_r$, 即可取 $A''_0 y^m + A''_1 y^{m-1} + \cdots + A''_m$ 为引理所需的多项式 B , 否则如前进行即得证明.

引理 3. 有一算法足以对 $P_r[y]$ 中的任一多项式

$$A = A_0 y^m + A_1 y^{m-1} + \cdots + A_m,$$

在 K_r 中作因子分解(诸 A_i 都 $\in P_r$, 且 A_0 在 K_r 中 $\neq 0$, 又 $m \geq 2$). 详言之, 即可确定形式

$$\begin{aligned} HA &= A' + \sum C_i p_i, \\ A' &= \bar{A}_1 \cdots \bar{A}_t. \end{aligned}$$

使以下诸条件满足:

$(L3)_1$ 诸 $\bar{A}_i$ 都是 $P_r[y]$ 中的规范多项式, 且在 K_r 中不可约.

$(L3)_2$ H 是 P_r 中的多项式, 且在 K_r 中 $\neq 0$.

$(L3)_3$ C_i 都是 $P_r[y]$ 中的多项式.

证. Hermann 在文献 [9] 中的方法给出了 A 在 K_r 中的因子分解. 在通分后即得形式

$$DA = B_1 \cdots B_t + \sum B'_i p_i,$$

其中 B_i, B'_i 都是 $P_r[y]$ 中的多项式, B_i 在 K_r 中不可约, D 是 P_r 中的多项式, 而在 K_r 中 $\neq 0$. 对每一 B_i 应用引理 2 即得所需的形式. 又可参阅文献 [12, p. 130].

四、定理的证明

至此定理 1—3 可容易地证明如下.

定理 1 的证明.

对于相关簇 V 的定义方程组 (I) 试视 $f_1(u_1, \dots, u_d, x_1)$ 为一 x_1 的多项式, 以 $R[u_1, \dots, u_d]$ 中的多项式为系数, 依据引理 3 的算法, 而以 x_1 作为 y , 0 作为 r , 可将 f_1 分解为 K 中的不可约规范因子. 任取其一为 $p_1(x_1)$, 命 K_1 为将 x_1 依方程

$$p_1(x_1) = 0$$

添加于域 $K = R(u_1, \dots, u_d)$ 所得的扩充域. 今视 f_2 为不定量 x_2 的多项式时, 必不能在域 K_1 中恒等于 0, 否则簇 V 的维数将 $> d$, 这与原来几何语句的确定性假设相违. 今将 x_2 作为 y , 1 作为 r , 而应用引理 3 于 f_2 , 即得一 $R[u_1, \dots, u_d, x_1, x_2]$ 中的多项式 f'_2 与一式如

$$h_2 f_2 = f_2' + C_{21} p_1.$$

这里 f_2' 视为不定量 x_2 的多项式时, 在 K_1 中 $\neq 0$, 且已分解成 K_1 中不可约的规范多项式的乘积. 任取一因子为 $p_2(x_1, x_2)$, 命 K_2 为将 x_2 依方程

$$p_2(x_1, x_2) = 0,$$

添入 K_1 后所得的扩充域. 于是 f_3 为 K_2 上不定量 x_3 的多项式, 且不恒等于 0. 今再依引理 3 以得一式

$$h_3 f_3 = f_3' + C_{31} p_1 + C_{32} p_2,$$

其中 x_3 的多项式 f_3' 已分解为规范多项式的乘积, 且每一因子在 K_2 中不可约. 任取一因子为 $p_3(x_1, x_2, x_3)$, 并依方程

$$p_3(x_1, x_2, x_3) = 0,$$

将 x_3 添入 K_2 以得 K_3 . 如此依法进行, 即可得一组子簇 V' , 每一 V' 都在 R 上不可约, 且在 K 上有一如下类型的定义方程组:

$$\left. \begin{aligned} p_1(x_1) &= 0, \\ p_2(x_1, x_2) &= 0, \\ \dots \\ p_r(x_1, \dots, x_r) &= 0. \end{aligned} \right\} \quad (\text{III})$$

它满足若干明显的条件如第三节所述.

易见, 这些子簇构成了整个所给的相关簇 V^* . 盖考虑 V^* 在 R 中的任一不可约成份, 并设 $(u_1, \dots, u_d, \bar{x}_1, \dots, \bar{x}_r)$ 是它的一个普点, 其中 $u_1, \dots, u_d$ 是独立的不定量, 而 $\bar{x}_1, \dots, \bar{x}_r$ 代数地依赖于这些 u . 因 $(u_1, \dots, u_d, \bar{x}_1)$ 必须满足方程组 (I), 特别应满足 f_1 , 故至少需满足 f_1 的一个不可约因子, 不妨设即为前面的 $p_1(x_1)$. 因 $(u_1, \dots, u_d, \bar{x}_1, \bar{x}_2)$ 必须满足方程组 (I) 中的其它诸方程以及方程 $p_1(x_1) = 0$, 故由前面关于 f_2 的等式知, 这一点也将满足方程 $f_2 = 0$, 因而至少须满足 f_2 的某一不可约因子, 设即为前面的 $p_2(x_1, x_2)$. 依次进行可知, $(u_1, \dots, u_d, \bar{x}_1, \dots, \bar{x}_r)$ 应满足类型如 (III) 式的一组方程, 而为前面所得不可约子簇组中某一个的普点. 这就证明了定理 1.

定理 2 与 3 的证明.

定理 2 从引理 1 立即可以得出. 定理 3 则从定理 1 与定理 2 得出.

附注.

我们关于初等几何定理机械化证明所用的算法, 主要牵涉到一些多项式的运用技术, 例如算术运算与简单消元法之类. 应该指出, 这些都是十二至十四世纪宋元时期中国数学家的创造, 在那时已有相当高度的发展. 详细介绍可参阅钱宝琮的著作^[13]. 事实上, 几何问题的代数化与用代数方法系统求解, 乃是当时中国数学家主要成就之一, 其时间远在十七世纪出现解析几何之前.

参 考 文 献

- [1] Tarski, A. & McKinsey, J. C. C., *A Decision Method for Elementary Algebra and Geometry*, 2nd ed., Berkeley and Los Angeles, 1948—1951 (中译本: 初等代数和几何的判定法, 科学出版社, 1959).
- [2] Seidenberg, A., *Annals of Math.*, **60** (1954), 365—374.
- [3] Robinsin, A., *Introduction to model Thory and to the Metamathematics of Algebra*, Amsterdam,

1963.

- [4] Cohen, P. J., *Comm. Pure Appl. Math.*, **22** (1969), 131—152.
- [5] Robinson, A., *Leet. Notes in Math.*, 1975, 498, 14—40.
- [6] ———, in *Proc. of Tarski Symposium*, 1974, 139—152.
- [7] Mehareem, J. D. et al., *IEEE Trans. on Computers*, **C-25** (1976), 773—782.
- [8] Keiter, K., *IEEE Trans. on Computers*, **C-25** (1976), 328—334.
- [9] Hermann, G., *Math. Ann.*, **95** (1926), 736—788.
- [10] Gröbner, W., *Moderne Algebraische Geometrie*, Wien, 1949.
- [11] Ritt, R. F., *Differential Algebra*, 1950.
- [12] Waerden, Van der, *Moderne Algebra*, Bd. 1, 1930.
- [13] 钱宝琮, 中国数学史, 科学出版社, 1964.