Vol. XXI No. 2 SCIENTIA SINICA March - April 1978

ON THE DECISION PROBLEM AND THE MECHANIZATION OF THEOREM-PROVING IN ELEMENTARY GEOMETRY

Wu Wen-tsün (吴文俊)

(*Institute of Mathematics, Academia Sinica*)

Received May 14, 1977.

Abstract

The idea of proving theorems mechanically may be dated back to Leibniz in the 17th century and has been formulated in precise mathematical forms in this century through the school of Hilbert as well as his followers on mathematical logic. The problem consists in essence in replacing qualitative difficulties inherited in usual mathematical proofs by quantitative complexities of calculations on standardizing the proof procedures in an algorithmic manner. Such quantitative complexities of calculations, formerly far beyond the reach of human abilities, have become more and more trivial owing to the occurrence and rapid development of computers. In spite of vigorous efforts, however, researches in this direction give rise quite often to negative results in the form of undecidable mathematical theories. To cite a notable positive result, we may mention Tarski's method of proving theorems mechanically in elementary geometry and elementary algebra. The methods of Tarski as well as later ones are largely based on a generalization of Sturm theorem and are still too complicated to be feasible, even with the use of computers. The present paper, restricted to theorems with betweenness out of consideration and based on an entirely different principle, aims at giving a mechanical procedure which permits to prove quite non-trivial theorems in elementary geometry even by hands.

1. Formulation of the Problem

A. Tarski in a classic paper[14] of 1948 has settled the decision problem of real closed field with one of its main aims to give mechanical proofs of theorems in elementary geometry. Alternative proofs of Tarski's result have later been given by Seidenberg, A. Robinson and P. J. Cohen, cf [12, 9, 2]. These authors have even suggested construction of certain decision machine to carry out such mechanical proofs. However, such a procedure seems to be far from being realized. In fact, only proofs of very trivial theorems in elementary geometry have actually been carried out on computers, cf. e.g. [6, 7]. The purpose of the present paper is, leaving aside questions involving betweenness of points, to give an alternative solution of the decision problem of elementary geometry based on a principle entirely different from those employed by the authors above-mentioned. Our method permits to furnish mechanical proofs of quite difficult geometrical theorems which can be practised even by hands, i.e., by means of papers and pencils only. The programming on a computer, based on such a method, though has not yet been done, will present no actual difficulties at all.

We shall restrict our considerations wholly to plane elementary geometry, though our method may be applied to the consideration of various other kinds of geometry. The first step of our method consists in the algebraic formalization of the geometrical problems involved. Points in the plane are to be defined as ordered pairs of numbers in a fixed field, say the field of rational numbers R. A dictionary is then set up turning geometrical relations into algebraic expressions which may be considered as either definitions or axioms. For example, for points $A_i = (x_i, y_i)$, distinct or not, we shall say:

A_1A_2 is parallel to A_3A_4 if $(x_1 - x_2)(y_3 - y_4) - (x_3 - x_4)(y_1 - y_2) = 0$,
A_1A_2 is orthogonal to A_3A_4 if $(x_1 - x_2)(x_3 - x_4) + (y_1 - y_2)(y_3 - y_4) = 0$,
the length-square of A_1A_2 is $r^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$, etc.

We may replace the basic field R by other fields, make correspondence the points to other kinds of number-sets, or modify the algebraic expressions in the axioms, e.g., instead of the length-square function r^2 given above, we consider the function $r^4 = (x_1 - x_2)^4 + (y_1 - y_2)^4$. We then go to other realms of geometry, non-euclidean geometry, real or complex projective geometry, finite geometry, etc. We shall however stick ourselves in what follows to plane elementary geometry only which has some representative character.

To illustrate our method of treatment, let us cite first a simple example. Consider the following statement:

(S_n) Let $A_0A_1A_2$ be a right-angled triangle with right angle at A_0. If x_1, x_2 denote the lengths of sides A_0A_1, A_0A_2 and x_3 is the length of the hypotenuse, then

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

The problem is to decide whether the statement (S_n) is true or not and to give an algorithmic procedure of proving or disproving (S_n) which holds good for all statements alike in elementary geometry (with betweenness out of consideration).

To solve this problem, let us remark first that the points, etc., occurring in the statement have a generic character subjected to the conditions implied in the hypothesis of the statement. Thus, if we represent the points in question in coordinates with $A_0 = (x_0, v_0)$, $A_1 = (u_1, v_1)$, $A_2 = (u_2, v_2)$, the coordinates v_0, u_1, v_1, u_2, v_2 can be considered as indeterminates. On the other hand, the other coordinates and geometric entities x_0, x_1, x_2, x_3 are then algebraically dependent on these indeterminates, being restricted by following algebraic equations according to hypothesis of the statement (S_n):

$$f_0 \equiv (u_1 - x_0)(u_2 - x_0) + (v_1 - v_0)(v_2 - v_0) = 0,$$
$$f_1 \equiv x_1^2 - (u_1 - x_0)^2 - (v_1 - v_0)^2 = 0,$$
$$f_2 \equiv x_2^2 - (u_2 - x_0)^2 - (v_2 - v_0)^2 = 0,$$
$$f_3 \equiv x_3^2 - (u_1 - u_2)^2 - (v_1 - v_2)^2 = 0.$$

The conclusion in the statement (S_n) is equivalent to

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

Let us now take once for all the rational number field R as the base field. Let A^9 be the affine space on R with coordinates $(v_0, u_1, v_1, u_2, v_2, x_0, x_1\ x_2, x_3)$ arranged in that definite order. Then the above equations $f_i = 0$ define an algebraic variety V of dimension 5, in the present case irreducible over R, with some generic point $(v_0, u_1, v_1, u_2, v_2, \bar{x}_0, \bar{x}_1, \bar{x}_2, \bar{x}_3)$ of which v_0, u_1, v_1, u_2, v_2 are indeterminates. The truth or untruth of the statement (S_n) amounts to $g_n \equiv 0$ or $\not\equiv 0$ on V respectively.

It turns out that the general decision problem can be formulated in the following manner.

Problem. In a certain affine space A^n of dimension $n = r + d$ over R with coordinates $(u_1, \ldots, u_d, x_1, \ldots, x_r)$, consider an algebraic variety V with defining equations (u_i being independent indeterminates)

$$\text{(I)} \qquad \begin{cases} f_1(u_1, \cdots, u_d, x_1) = 0, \\ f_2(u_1, \cdots, u_d, x_1, x_2) = 0, \\ \qquad \cdots\cdots \\ f_r(u_1, \cdots, u_d, x_1, x_2, \cdots, x_r) = 0. \end{cases}$$

The variety V may eventually split into irreducible components, all of (real) dimension $\leqslant d$. Those of dimension $= d$, with generic points of the form $(u_1, \ldots, u_d, \bar{x}_1, \ldots\ \bar{x}_r)$ for which $\bar{x}_j$ are algebraic over the field $K = R(u_1, \ldots, u_d)$ will have a union V^* usually coincident with V. Let a polynomial $g(u_1, \ldots, u_d, x_1, \ldots, x_r)$ (or a set of such polynomials g_k) in $R[u_1 \ldots, u_d, x_1, \ldots, x_r]$ be given. It is to decide in an algorithmic manner whether

$$g \equiv 0$$

(or all $g_k \equiv 0$) on V^* or not.

In the above formulation the algebraic variety V, or preferably V^* reflects the hypothesis of the geometric statement considered. Either V or V^* will be called the *associated variety* of the statement in question. The variety V^* considered as one defined on the field $K = R(u_1, \ldots, u_d)$ is of dimension 0. The form of equations (I) shows that the algebraically dependent variables $x_1, \ldots, x_r$ are to be adjoined to K *successively* which reflects the geometrical fact that, starting from some generic points on certain generic lines, circles, etc., new points are to be *successively* adjoined in an algebraic manner by various geometric operations of joining points, drawing parallels, perpendiculars or circles, forming intersections of lines and circles, etc. These geometrical constructions give rise to algebraic equations involving x and u which can easily be turned into the form (I) by simple elimination procedure. In fact, the starting equations in x and u are rarely higher than 2. We shall call the variables u as the *parameters* and x as the *dependents*. It is also to be remarked that the condition for all components of V to be of dimension $\leqslant d$ over R reflects just the *determinate* character of the geometric statements to be considered, and the restriction to V^* reflects the depriving of degeneracies in our consideration. Both of these are, in reality, implicitly implied in the hypothesis of ordinary geometrical theorems. On the other hand, the equation $g \equiv 0$ on V^* (or set of $g_k \equiv 0$ on V^*) is the algebraic

equivalent of the conclusion of the statement to be proved or disproved. We shall call g or set of g_k in what follows the *deciding polynomial(s)* of the geometrical statement in question.

Theoretically, the methods given by Hermann in [4] permit already to solve the above decision problem in an algorithmic manner. However, his methods are so complicated to give rise to astronomical expansions that even the simplest geometrical theorems can hardly be proved. On the contrary the decision procedure given below takes advantages of the particular character of the equations (I) and permits to prove mechanically quite non-trivial theorems even by hands, i.e. by means of pencils and papers only.

Our method of decision procedure is based on the following three theorems:

Theorem 1. *There is an algorithmic procedure permitting us to split the associated variety V^* of any determinative geometric statement defined by (I) into subvarieties V' irreducible over R each of which, considered as defined over the field $K = R(u_1, \ldots, u_d)$ has a representative basis (i.e. basis of the associated prime ideal) of the form*

$$(p_1, \cdots, p_r),$$

having the following properties:

(T1)$_1$. Each p_i is a polynomial in $R[u_1, \ldots, u_d, x_1, \ldots, x_i]$ of some degree $m_i > 0$ in x_i.

(T1)$_2$. The coefficients of p_i, considered as a polynomial in x_i, are polynomials in $R[u_1, \ldots, u_d, x_1, \ldots, x_{i-1}]$ having no common factor and with degree in x_j less than m_j for $j = 1, \ldots, i-1$.

(T1)$_3$. The leading coefficient of p_i, considered as a polynomial in x_i, is a polynomial $\neq 0$ in $R[u_1, \ldots, u_d]$ free of all x.

(T1)$_4$. p_1, as a polynomial in x_1, is irreducible in the field $K = R(u_1, \ldots, u_d)$, and for each $i > 1$, p_i, as a polynomial in x_i, is irreducible in the field obtained by adjoining $x_1, \ldots, x_{i-1}$ to K by the algebraic equations $p_1 = 0, \ldots, p_{i-1} = 0$.

It is clear that the polynomials $p_1, \ldots p_r$ are uniquely determined by V' up to multipliers in R and will be said to form a *privileged basis* of V' (more exactly, of the prime ideal associated to V' over K), with respect to the given order $x_1, \ldots, x_r$ of the dependents. Remark that the notion is in reality due to Gröbner under the name of prime basis, cf. e.g. [3] and cf. also [8] for the intimately related concept of characteristic sets introduced by R. F. Ritt.

Theorem 2. *Let $(p_1, \ldots, p_r)$ be a privileged basis of any irreducible component V' of the associated variety V^*. There is an algorithmic procedure which permits to determine, for any polynomial h in $R[u_1, \ldots, u_d, x_1, \ldots, x_r]$, an equation of the form*

$$Dh = \sum_{i_s=0}^{m_s-1} h_{i_1 \cdots i_r} x^{i_1} \cdots x^{i_r} + \sum_{i=1}^{r} A_i p_i,$$

verifying the following conditions:

$(T2)_1$. *D, $h_{i_1 \cdots i_r}$ are all polynomials in $R[u_1, \ldots, u_d]$ and $D \neq 0$,*

$(T2)_2$. *A_i are all polynomials in $R[u_1, \ldots, u_d, x_1, \ldots, x_r]$.*

The polynomials $h_{i_1}, \ldots, i_r$ which are uniquely determined up to multipliers in R by the algorithmic procedure, will be called the *remainder constituents* of the polynomial h with respect to the privileged basis $(p_1, \ldots, p_r)$ of V', or, by abuse of language, simply the remainder constituents of h with respect to V'.

Theorem 3. *For a geometrical statement with associated variety V^* and deciding polynomial g (or a set g_k of deciding polynomials) to be true, it is necessary and sufficient that for any irreducible component V' of V^*, all remainder constituents of g (or of all g_k) should be identically zero.*

II. Examples

Before giving proofs of these theorems in IV, we shall illustrate their use by some examples below.

Ex. 1. For the geometrical statement (S_n) about right-angled triangle as cited in the beginning of the present paper, we see readily that the associated variety V in parameters v_0, u_1, v_1, u_2, v_2 and dependents x_0, x_1, x_2, x_3, is already irreducible over R and possesses a privileged basis (p_1, p_2, p_3, p_4), where

$$p_1 = x_0^2 - (u_1 + u_2)x_0 + u_1u_2 + (v_1 - v_0)(v_2 - v_0),$$
$$p_2 = x_1^2 + (u_1 - u_2)x_0 - u_1^2 + u_1u_2 - (v_1 - v_0)(v_1 - v_2),$$
$$p_3 = x_2^2 - (u_1 - u_2)x_0 - u_2^2 + u_1u_2 + (v_2 - v_0)(v_1 - v_2),$$
$$p_4 = x_3^2 - (u_1 - u_2)^2 - (v_1 - v_2)^2.$$

It is readily verified that

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

while for $n > 2$, we have

$$g_n \not\equiv 0 \mod (p_1, p_2, p_3, p_4).$$

It follows that (S_n) is true only for $n = 2$ which corresponds to the Keu-Kou Theorem.

Ex. 2. Our decision procedure can also be applied to give mechanical proofs of trigonometric identities. Consider, e.g. the following statements:

(S) If $A_1 + A_2 + A_3 = 180^\circ$, then

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

(C) If $A_1 + A_2 + A_3 = 180^\circ$, then

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

To decide whether (S) or (C) is true, let us set

$$\sin A_i = s_i, \quad \cos A_i = c_i, \quad (i = 1, 2),$$
$$\sin 2A_i = x_i, \quad \cos 2A_i = y_i, \quad (i = 1, 2, 3),$$
$$\sin A_3 = z_1, \quad \cos A_3 = z_2.$$

Take c_1 and c_2 as parameters and

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

as dependents (in this order), then the associated variety of (S) or (C) is already irreducible in R and possesses a privileged basis $(p_1, \ldots, p_{10})$ given by

$$p_1 = s_1^2 + c_1^2 - 1,$$
$$p_2 = s_2^2 + c_2^2 - 1,$$
$$p_3 = z_1 - c_2 s_1 - c_1 s_2,$$
$$p_4 = z_2 - s_1 s_2 + c_1 c_2,$$
$$p_5 = x_1 - 2c_1 s_1,$$
$$p_6 = x_2 - 2c_2 s_2,$$
$$p_7 = x_3 - 2z_1 z_2,$$
$$p_8 = y_1 - 2c_1^2 + 1,$$
$$p_9 = y_2 - 2c_2^2 + 1,$$
$$p_{10} = y_3 + 4c_1 c_2 s_1 s_2 - 4c_1^2 c_2^2 + 2c_1^2 + 2c_2^2 - 1.$$

The deciding polynomials of the statements (S) and (C) are given respectively by

$$g_s = x_1 + x_2 + x_3 - 4s_1 s_2 z_1,$$
$$g_c = y_1 + y_2 + y_3 + 4c_1 c_2 z_2.$$

We verify readily that

$$g_s = -2c_2 s_2 p_1 - 2c_1 s_1 p_2 - 2p_3(s_1 s_2 + c_1 c_2) + 2z_1 p_4 + p_5 + p_6 + p_7$$
$$\equiv 0 \mod (p_1, \cdots, p_{10}),$$
$$g_c = -1 + 4c_1 c_2 p_4 + p_8 + p_9 + p_{10} \not\equiv 0 \mod (p_1, \cdots, p_{10}).$$

Hence (S) gives a true identity while (C) not.

Ex. 3. Let us consider the Simson-Line Theorem which corresponds to the following statement:

(S_s). From a point A_4 on the circumscribed circle of a triangle $A_1A_2A_3$, perpendiculars are drawn to the sides of the triangle. Then the feet of the perpendiculars are in a line.

To prove this, let us take for simplicity the center of the circumscribed circle as the point (0, 0), while the radius is r. Let the points A_i $(i = 1, 2, 3, 4)$ be (x_i, u_i) and the feet of perpendiculars A_j be (x_j, y_j), $j = 5, 6, 7$. Consider r, u_1,

u_2, u_3, u_4 as parameters and

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

as the dependents in the order indicated.

A prime basis $(p_1, \ldots, p_{10})$ of the associated Simson variety which is irreducible is readily given as follows:

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

In the above equations we have set for simplicity:

$$u_{ij} = u_i - u_j, \quad x_{ij} = x_i - x_j, \qquad (i, j = 1, 2, 3),$$
$$h_5 = u_4x_2x_3 - (u_2x_3 + u_3x_2)u_4 + r^2(u_2 + u_3 + u_4) - u_2u_3u_4.$$

Similarly for h_6 and h_7.

The deciding polynomial is given by

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

Straightforward calculation shows again

$$g \equiv 0 \mod (p_1, \cdots, p_{10}),$$

which proves the truth of Simson statement (S_s).

Ex. 4. For a less trivial example, let us consider the Feuerbach theorem which corresponds to the following statement:

(S_F) The 9-point circle of a triangle is tangent to the four incribed and the escribed circles of the triangle.

Let us take the three vertices of the triangle as $(2u_i, 2v_i)$, the center and radius of the 9-point circle as (x_1, y_1) and r_1, and the center and radius of either the incribed or any of the escribed circles as (x_2, y_2) and r_2. Introduce also variables z_1, z_2, z_3 corresponding to lengths of the sides of the triangle. Then with u_1, v_1, u_2, v_2, u_3,v_3 as the parameters and z_1, z_2, z_3, x_1, y_1, x_2, y_2, r_1, r_2 as dependents in this order, the associated Feuerbach variety V_F splits into irreducible ones having privileged basis

$(p_1, \ldots, p_9)$ given by:

$$
\begin{aligned}
p_1 &= z_1^2 - u_{23}^2 - v_{23}^2, \\
p_2 &= z_2^2 - u_{31}^2 - v_{31}^2, \\
p_3 &= z_3^2 - u_{12}^2 - v_{12}^2, \\
p_4 &= 4\Delta x_1 - \alpha_1, \\
p_5 &= 4\Delta y_1 - \beta_1, \\
p_6 &= 4\Delta x_2 - \alpha_2, \\
p_7 &= 4\Delta y_2 - \beta_2, \\
p_8 &= 4\Delta r_1 - z_1 z_2 z_3, \\
p_9 &= 2\Delta r_2 + \gamma.
\end{aligned}
$$

In the above formulas we have put for simplicity

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

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

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

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

$$\begin{aligned}
\alpha_2 = &- [v_{23}v_{31}v_{12} + v_1(u_2^2 - u_3^2) + v_2(u_3^2 - u_1^2) + v_3(u_1^2 - u_2^2) \\
&+ \varepsilon_2\varepsilon_3 v_{23} z_2 z_3 + \varepsilon_3\varepsilon_1 v_{31} z_3 z_1 + \varepsilon_1\varepsilon_2 v_{12} z_1 z_2],
\end{aligned}$$

$$\begin{aligned}
\beta_2 = &\, u_{23}u_{31}u_{12} + u_1(v_2^2 - v_3^2) + u_2(v_3^2 - v_1^2) + u_3(v_1^2 - v_2^2) \\
&+ \varepsilon_2\varepsilon_3 u_{23} z_2 z_3 + \varepsilon_3\varepsilon_1 u_{31} z_3 z_1 + \varepsilon_1\varepsilon_2 u_{12} z_1 z_2,
\end{aligned}$$

$$\begin{aligned}
\gamma = &\, \varepsilon_1(u_{31}u_{12} + v_{31}v_{12}) z_1 + \varepsilon_2(u_{12}u_{23} + v_{12}v_{23}) z_2 \\
&+ \varepsilon_3(u_{23}u_{31} + v_{23}v_{31}) z_3 + \varepsilon_1\varepsilon_2\varepsilon_3 z_1 z_2 z_3.
\end{aligned}$$

Remark that the choice of $\varepsilon_i = +1$ or -1 corresponds to the 4 inscribed or escribed circles and reflects the reducibility of the Feuerbach variety.

Now the deciding polynomial of statement (S_F) is of the form

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

in which $\eta = +1$ or -1. By a straightforward calculation, however lengthy and tedious, we verify that g_η will be a linear combination of $p_1, \ldots, p_9$ for $\eta = +\varepsilon_1\varepsilon_2\varepsilon_3$ but not so for $\eta = -\varepsilon_1\varepsilon_2\varepsilon_3$. Thus the Feuerbach statement is a true theorem and $\eta = +\varepsilon_1\varepsilon_2\varepsilon_3$ reflects the manner of contact between the 9-point circle and the respective in- or es-cribed circle. Remark that in our formulation we have left aside the question of betweenness and the manner of contact of circles is not of interest to us. In this way we can take $g = g_{+1} \cdot g_{-1}$ as the deciding polynomial if we like. We may also take the Feuerbach variety in the affine space of u_i, v_i, x_j, y_j only without the introduction of z_1, z_2, z_3 so that it is irreducible at the outset.

III. Some Lemmas

To make some preparations we shall consider a field $R(u_1,\ldots,u_d,\ x_1,\ldots,x_r)$ in which $u_1,\ldots,u_d$ are transcendental while $x_1,\ldots,x_r$ are algebraic over the base field R. The algebraic extensions to $x_1,\ldots,x_r$ are defined successively by the following equations

$$(\mathrm{II})\qquad \begin{cases} p_1(x_1) \equiv p_{10}x_1^{m_1} + p_{11}x_1^{m_1-1} + \cdots + p_{1m_1} = 0, \\ p_2(x_1,x_2) \equiv p_{20}x_2^{m_2} + p_{21}x_2^{m_2-1} + \cdots + p_{2m_2} = 0, \\ \cdots\cdots\cdots\cdots \\ p_r(x_1,\cdots,x_r) \equiv p_{r0}x_r^{m_r} + p_{r1}x_r^{m_r-1} + \cdots + p_{rm_r} = 0. \end{cases}$$

It is assumed that for $1 \leqslant i \leqslant r$, the p_{ij}'s are polynomials in the ring $P_{i-1} = R[u_1,\ldots,u_d,\ x_1,\ldots,x_{i-1}]$, that p_{i0} are polynomials $\neq 0$ in $P_0 = R[u_1,\ldots,u_d]$, and that p_i considered as polynomials in x_i are irreducible over the field $K_{i-1} = R(u_1,\ldots,u_d,\ x_1,\ldots,x_{i-1})$ defined by the equations $p_1(x_1) = 0,\ldots,\ p_{i-1}(x_1,\ldots x_{i-1}) = 0$. We put here

$$K_0 = K = R(u_1,\cdots,u_d).$$

Let $\mathcal{I}$ be the collection of sets of indices $I = (i_1,\ldots,i_r)$ with $0 \leqslant i_j \leqslant m_j - 1$. For such an I we shall write symbolically

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

Any polynomial of the form

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

with coefficients a_I in a certain ring or field F will be called then a *normalized* one in $F[x_1,\ldots,x_r]$.

Lemma 1. *There is an algorithmic procedure which permits to determine uniquely for any polynomial A in P_r a set of integers $s_1,\ldots,s_r \geqslant 0$ and a set of polynomials A_I in P_0 for $I \in \mathcal{I}$ verifying the following conditions:*

$(L1)_1$. *Modulo some linear combination of p_i over P_r, we have*

$$p_{10}^{s_1}\cdots p_{r0}^{s_r}A \equiv \Sigma A_I x^I.$$

$(L1)_2$. *A_I are polynomials in P_0 with coefficients linear in those of A, considered as polynomial in P_r.*

$(L1)_3$. *$s_1,\ldots,s_r$ are the least integers $\geqslant 0$ to make $(L1)_1$ and $(L1)_2$ possible.*

Proof. Considering both A and p_r as polynomials in x_r with coefficient in p_{r-1}, we get by division for some integer $s_r \geqslant 0$ taken to be least possible

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

with Q_r, R_{r-1} polynomials in P_r for which the degree of R_{r-1} in x_r is $< m_r$. Considering now p_{r-1} and R_{r-1} as polynomials in x_{r-1} with coefficients in $R[u_1,\ldots,u_d,\ x_1,\ldots,\ x_{r-2},x_r]$, we get by division for some integer $s_{r-1} \geqslant 0$ taken to be least

possible

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

with Q_{r-1}, R_{r-2} polynomials in P_r for which the degrees of R_{r-2} in x_r and x_{r-1} are $< m_r$ and $< m_{r-1}$ respectively. Proceeding in this manner, we get successively

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

$$\cdots\cdots$$

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

with R_0 as a polynomial in P_r for which the degree in x_i is $< m_i$, $1 \leqslant i \leqslant r$. We may then write R_0 as $\Sigma A_I x^I$ and get the expression verifying all the conditions in the Lemma as required.

Lemma 2. *There is an algorithmic procedure which permits to determine for any polynomial in some indeterminate y of the form*

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

with each A_i in P_r and $A_0 \neq 0$ in K_r expressions of the form

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

with

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

verifying the following conditions:

$(L2)_1$. *All B_i are normalized polynomials in P_r and B_0 is a polynomial $\neq 0$ in P_0.*

$(L2)_2$. *C_i are all polynomials in $P_r\,[y]$ and H is one in P_r.*

$(L2)_3$. *$H \not\equiv 0 \mod (p_1, \ldots, p_r)$.*

Any such polynomial B satisfying $(L2)_1$ will then be said to be a normalized polynomial over P_r in the indeterminate y.

Proof. By Lemma 1, we have for some integers $s_1, \ldots, s_r \geqslant 0$ an expression of the form

$$p_{10}^{s_1} \cdots p_{r0}^{s_r} A = A_0' y^m + A_1' y^{m-1} + \cdots + A_m' \mod (p_1, \cdots, p_r)$$

with all A_i' normalized in P_r and $A_0' \neq 0$ in K_r. Suppose that A_0' is free of $x_{i+1}, \ldots, x_r$ but not so for x_i. As A_0' has a degree $< m_i$ in x_i while p_i is irreducible in K_{i-1} and of degree m_i in x_i, we find by the usual division algorithm polynomials h, k in P_i and A_{00}' in P_{i-1} such that

$$hA_0' + kp_i = A_{00}',$$

in which h is $\neq 0$ in K_i and $A_{00}' \neq 0$ in K_{i-1}. We have then an expression of the form

$$hp_{10}^{s_1} \cdots p_{r0}^{s_r} A + kp_i y^m = A_{00}' y^m + hA_1' y^{m-1} + \cdots + hA_m' \mod (p_1, \cdots, p_r).$$

Applying Lemma 1 again to hA_i' and A_{00}', we get then some expression

$$h''A = A_0''y^m + A_1''y^{m-1} + \cdots + A_m'' \mod (p_1, \cdots, p_r),$$

for which all A_i'' are normalized in P_r with $A_0'' \neq 0$ in K_r and not containing any x_j for $j \geqq i$, and h'' is some polynomial in P_r which is $\neq 0$ in K_r. If A_0'' is free of all $x_1, \ldots, x_r$, we may take

$$B = A_0''y^m + A_1''y^{m-1} + \cdots + A_m''$$

as the polynomial B required or otherwise we proceed as before.

Lemma 3. *There is an algorithmic procedure which permits to factorize in K_r any polynomial in $P_r[y]$*

$$A = A_0y^m + A_1y^{m-1} + \cdots + A_m$$

with A_i in P_r and $A_0 \neq 0$ in K_r, $m \geqq 2$. More precisely, it permits to find expression of the form

$$HA = A' + \Sigma C_ip_i,$$

with

$$A' = \bar{A}_1 \cdots \bar{A}_t,$$

verifying the following conditions:

$(L3)_1$. *Each $\bar{A}_j$ is a normalized polynomial in $P_r[y]$ and is irreducible in K_r.*

$(L3)_2$. *H is a polynomial in P_r which is $\neq 0$ in K_r.*

$(L3)_3$ *C_i are polynomials in P_r $[y]$.*

Proof. The method of Hermann in [4] permits to give, in an algorithmic manner, a factorization of A into irreducible ones in K_r so that after clearing of fractions we have an expression of the form

$$DA = B_1 \cdots B_t + \Sigma B_i'p_i,$$

with B_i, B_i' polynomials in $P_r[y]$, B_i irreducible in K_r and D a polynomial in P_r which is $\neq 0$ in K_r. Applying now Lemma 2 to each B_i, we get then the expression required. Consider also the reference [15], p. 130.

IV. Proofs of the Theorems

We are now in a position to give proofs of Theorems 1—3 quite simply as follows:

Proof of Theorem 1. For the defining system of equations (I) of the associated variety V, let us consider $f_1(u_1, \ldots, u_d, x_1)$ as a polynomial in x_1 with coefficients in $R[u_1, \ldots, u_d]$ and factorize f_1 into ones irreducible in $K = R(u_1, \ldots, u_d)$ by applying the algorithm in Lemma 3, with x_1 as y and 0 as r there. Take any such irreducible factor as $p_1(x_1)$. Let K_1 be the field obtained from K by adjoining x_1 defined by the equation

$$p_1(x_1) = 0.$$

Now f_2, considered as a polynomial in the indeterminate x_2, cannot be identical with 0 in the field K_1, for otherwise the variety V would be of dimension $> d$, contrary to the determinancy hypothesis of our geometric statement. Applying Lemma 3 to f_2 with x_2 as y and 1 as r there, we get a certain polynomial f_2' in $P_2 = R[u_1, \ldots, u_d, x_1, x_2]$ with an expression of the form

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

in which f_2', as a polynomial in the indeterminate x_2, is a product of normalized factors irreducible and $\neq 0$ in the field K_1. Take any such factor as $p_2(x_1, x_2)$. Let K_2 be the field obtained from K_1 by adjoining x_2 defined by the equation

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

Then f_3 is a polynomial in the indeterminate x_3 over P_2 which cannot be identical with 0. Applying Lemma 3, we get an expression of the form

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

in which the polynomial f_3' in x_3 is a product of normalized factors irreducible and $\neq 0$ in K_2. Take any factor as $p_3(x_1, x_2, x_3)$, adjoin x_3 to K_2 by the equation

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

and proceed further as before. In this manner, we get finally system of subvarieties V' irreducible over R, each defined on K by systems of equations of the type

(III)
$$\begin{cases} p_1(x_1) = 0, \\ p_2(x_1, x_2) = 0, \\ \cdots\cdots \\ p_r(x_1, x_2, \cdots, x_r) = 0, \end{cases}$$

verifying some obvious conditions as described in III.

It is easy to see that the collection of all such subvarieties exhausts the given variety V^*. In fact, consider an irreducible component in R of V^* with a generic point, say $(u_1, \ldots, u_d, \bar{x}_1, \ldots, \bar{x}_r)$, in which $u_1, \ldots, u_d$, are independent indeterminates while $\bar{x}_1, \ldots, \bar{x}_r$ depend algebraically on them. As $(u_1, \ldots, u_d, \bar{x}_1)$ should satisfy the system of equations (I), in particular the equation $f_1 = 0$, they should annul some one of the irreducible factors of f_1, say p_1 before. Now, $(u_1, \ldots, u_d, \bar{x}_1, \bar{x}_2)$ should satisfy the other equations in the system (I) as well as the equation $p_1(x_1) = 0$. It follows from expression about f_2' given above that they should also satisfy the equation $f_2' = 0$ and hence should annul one of the irreducible factors of f_2', say $p_2(x_1, x_2)$ above. Proceeding in the same manner we see that $(u_1, \ldots, u_d, \bar{x}_1, \ldots, \bar{x}_r)$ should satisfy a system of equations of the type (III) and hence is a generic point of an irreducible subvariety among the collection found above. This completes the proof of the theorem.

Proofs of Theorems 2 and 3.

Theorem 2 follows immediately from the algorithm in Lemma 1. The truth of Theorem 3 is quite clear from Theorems 1 and 2.

Final Remark. Our algorithm for the mechanization of theorem-proving in elementary geometry involves mainly such polynomial manipulations as arithmetic operations and simple eliminations, which were all originated and quite developed in 12—14 c. Chinese mathematics, cf. e.g. the book of late Chien[1] for the explanations. In fact, the algebrization of geometrical problems and systematic method of their solutions by algebraic tools were some of the main achievements of Chinese mathematicians at that time, much earlier than the appearance of analytic geometry in 17 c.

Added in Proof. (Dec. 1977).

The same principle has been applied to the mechanization of theorem-proving in elementary differential geometry with the aid of Ritt's theory of differential algebra, of which the details will be given later.

References

[1] 钱宝琮，中国数学史，科学出版社，1964.

[2] Cohen, P. J.: Decision procedures for real and p-adic fields, *Comm. Pure Appl. Math.*, **22**(1969), 131—152.

[3] Gröbner, W.: *Moderne algebraische Geometrie*, (1949), Wien.

[4] Hermann, G.: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.*, **95**(1926), 736—788.

[5] Hilbert, D.: *Grundlagen der Geometrie.*

[6] McCharen, J. D. *et al.*: Problems and experiments for and with automated theorem-proving programs, *IEEE Trnas. on Computers*, **C-25**(1976), 773—782.

[7] Reiter, R.: A semantically guided deductive system for automatic theorem proving, *IEEE Trans. on Computers*, **C-25** (1976), 328—334.

[8] Ritt, R. F.: *Differential Algebra*, (1950).

[9] Robinson, A.: *Introduction to Model Theory and to the Metamathematics of Algebra*, (1963), Amsterdam.

[10] ————: Algorithms in algebra, in model theory and algebra, *Lect. Notes in Math.*, No. 498 (1975), 14—40.

[11] Robinson, A.: A decision method for elementary algebra and geometry-revisited, *Proc. of Tarski Symposium*, (1974), 139—152.

[12] Seidenberg, A.: A new decision method for elementary algebra, *Annals of Math.*, **60**(1954), 365—374.

[13] Tarski, A.: What is elementary geometry? *The Axiomatic Method with Special Reference to Geometry and Physics*, (1959), 16—29, Amsterdam.

[14] Tarski, A. & McKinsey, J. C. C.: *A Decision Method for Elementary Algebra and Geometry*, 2nd ed., Berkeley and Los Angeles, (1948—1951).

[15] Waerden, Van der: *Moderne Algebra*, Bd. 1, (1930).

[16] ————: *Einführung in die algebraischen Geometrie*, (1945).