A SIMPLE PROOF OF THE MAIN THEOREM OF ELIMINATION THEORY IN ALGEBRAIC GEOMETRY

by P. CARTIER and J. TATE

SUMMARY

The purpose of this note is to provide a simple proof (which we believe to be new) for the weak zero theorem in the case of homogeneous polynomials. From this theorem and Nakayama's lemma, we deduce easily the main theorem of elimination theory. Our version of elimination theory is given in very general terms allowing a straightforward translation into the language of schemes. Our proofs are highly non constructive—the price we pay for simplicity and elegance.

We thank N. Bourbaki for numerous lively discussions about the subject matter of this note.

1. HILBERT'S ZERO THEOREM: A PARTICULAR CASE

We denote by k a field and K an algebraically closed extension of k. The statement of Hilbert's zero theorem, in its weak form for homogeneous polynomials, reads as follows:

THEOREM A. *Let n be a nonnegative integer and J an ideal in the polynomial ring $k[X_0, X_1, ..., X_n]$ generated by homogeneous polynomials. One has the following dichotomy:*

a) *Either there exists a nonnegative integer d_0 such that J contains every homogeneous polynomial of degree $d \geqslant d_0$;*

b) *or there exists a nonzero vector $\xi = (\xi_0, \xi_1, ..., \xi_n)$ with coordinates from K such that $P(\xi) = 0$ holds for any polynomial P in J.*

We begin by reformulating the previous theorem. It is immediate that properties a) and b) are mutually exclusive. For any nonnegative integer d, let S_d be the vector space (over k) consisting of the polynomials in the ring $S = k[X_0, X_1, ..., X_n]$ which are homogeneous of degree d. Then

$S = \bigoplus_{d \geq 0} S_d$, and for the multiplication one gets $S_d \cdot S_e \subset S_{d+e}$. Otherwise stated, *$S$ is a graded algebra over the field k*. Since J is generated by homogeneous polynomials, it is a *graded ideal*, namely $J = \bigoplus_{d \geq 0} (J \cap S_d)$. The factor algebra $R = S/J$ is therefore graded with $R_d = S_d/(J \cap S_d)$ for any nonnegative integer d. It enjoys the following properties:

(i) *As a ring, R is generated by $R_0 \cup R_1$.*

(ii) *For any nonnegative integer d, the vector space R_d is finite-dimensional over k.*

(iii) $R_0 = k$.

Denote by $x_0, x_1, \ldots, x_n$ respectively the cosets of $X_0, X_1, \ldots, X_n$ modulo J. Let φ be any k-linear ring homomorphism from R into K, and put $\xi_0 = \varphi(x_0), \ldots, \xi_n = \varphi(x_n)$. It is clear that the vector $\xi = (\xi_0, \xi_1, \ldots, \xi_n)$ is a common zero of the polynomials in J. Conversely, for any such common zero, there exists a unique k-linear ring homomorphism $\varphi : R \to K$ such that $\xi_0 = \varphi(x_0), \ldots, \xi_n = \varphi(x_n)$. The vector ξ is equal to zero if and only if φ maps $R_1 = kx_0 + \ldots + kx_n$ onto 0, that is if and only if the kernel of φ is equal to the ideal $R^+ = \bigoplus_{d \geq 0} R_d$ in R.

Theorem A is therefore equivalent to the following.

THEOREM B. *Let R be a graded commutative algebra over k, satisfying hypotheses* (i), (ii) *and* (iii) *above. One has the following dichotomy:*

a) *Either there exists a non-negative integer d_0 such that $R_d = 0$ for $d \geqslant d_0$;*

b) *or for every nonnegative integer d, one has $R_d \neq 0$ and there exists a k-linear ring homomorphism $\varphi : R \to K$ whose kernel is different from $R^+ = \bigoplus_{d \geq 1} R_d$.*

Notice that R is a finite-dimensional vector space in case a), infinite-dimensional in case b).

2. PROOF OF HILBERT'S ZERO THEOREM

We proceed to the proof of theorem B.

By property (i) above, one gets $R_1 \cdot R_d = R_{d+1}$ hence $R_d = 0$ implies $R_{d+1} = 0$. Hence either R_d is 0 for all sufficiently large d's, or $R_d \neq 0$

for every d. From now on, assume we are in the second case. Since R is generated over the field k by a finite number of elements, the maximum condition holds for the ideals in R. We can therefore select a maximal element in the set $\mathfrak{I}$ of graded ideals I in R such that $R_d \neq I \cap R_d$ for every nonnegative integer d (notice (0) belongs to $\mathfrak{I}$, hence $\mathfrak{I}$ is nonempty). Replacing R by R/I, we may assume that R enjoys the following property:

(M) *For every nonnegative integer d, one has $R_d \neq 0$. Every graded ideal $I \neq (0)$ in R contains R_d for all sufficiently large d's.*

We claim that R_1 *contains a non-nilpotent element.* Assume the converse and let $a_1, \ldots, a_r$ be a linear basis of R_1 over k. There would then exist an integer $N \geqslant 1$ such that $a_1^N = \ldots = a_r^N = 0$, any monomial of degree $> Nr$ in $a_1, \ldots, a_r$ would be equal to zero, and we would have $R_d = 0$ for any integer $d > Nr$, contrary to assumption (M).

Pick a non-nilpotent element x in R_1. *The element $1 - x$ has no inverse in R.* Indeed x^d belongs to R_d for any $d \geqslant 0$, and the inverse to $1 - x$ would be congruent to $1 + x + x^2 + \ldots + x^d$ modulo the ideal $\sum_{i>d} R_i$ for every $d \geqslant 1$, contrary to the assumption that R is the direct sumof the R_d's. By Krull's theorem, we may select a maximal ideal M in R containing $1 - x$. Then $L = R/M$ is a field extension of k, and the element x of R_1 satisfies $x \equiv 1 \bmod M$. Since K is an algebraically closed extension of k, it remains to show that L is of finite degree over k, hence isomorphic to a subextension of K.

Since $x \,.\, R = \bigoplus_{d \geqslant 0} x \,.\, R_d$ is a graded ideal in R, one gets from (M) the existence of an integer $d_0 \geqslant 0$ such that $x \,.\, R_d = R_{d+1}$ for $d \geqslant d_0$. Hence, as a module over its subring $k[x]$, R is generated by $R_0 + R_1 + \ldots + R_{d_0}$ hence by a (finite) basis $b_1, \ldots, b_N$ of this vector space over k. That is, any element u in R is of the form

$$u = b_1 f_1(x) + \ldots + b_N f_N(x) \tag{1}$$

where $f_1, \ldots, f_N$ are polynomials in one indeterminate with coefficients in k. From (1) one gets

$$u \equiv b_1 f_1(1) + \ldots + b_N f_N(1) \mod M,$$

hence $[L : k] \leqslant N$ is finite.

Q.E.D.

For the reader who doesn't want to appeal to Hilbert's basis theorem, here is a direct construction of a maximal element in $\mathfrak{I}$. Let $r_0 = 0$,

$I_0 = (0)$ and $\mathfrak{I}_0 = \mathfrak{I}$ and define inductively r_d, I_d and $\mathfrak{I}_d$ as follows. For $d \geqslant 0$, let r_{d+1} be equal to the maximum of the dimensions of $I \cap R_{d+1}$ for I running over $\mathfrak{I}_d$, let I_{d+1} be any ideal in $\mathfrak{I}_d$ such that $\dim (I_{d+1} \cap R_{d+1}) = r_{d+1}$ and let $\mathfrak{I}_{d+1}$ be the set of ideals I in $\mathfrak{I}_d$ such that $I \cap R_{d+1} = I_{d+1} \cap R_{d+1}$. Then the ideal $\bigoplus_{d \geqslant 1} (I_d \cap R_d)$ is a maximal element in $\mathfrak{I}$, as it is easily checked.

3. Elimination theory

The main theorem of elimination theory may be formulated as follows. Let $P_1, \ldots, P_r$ be polynomials in $k[X_0, X_1, \ldots, X_n; Y_1, \ldots, Y_m]$ with P_j homogeneous of degree d_j in the variables $X_0, X_1, \ldots, X_n$ alone, i.e. of the form

$$P_j = \sum_{\alpha_0 + \ldots + \alpha_n = d_j} X_0^{\alpha_0} X_1^{\alpha_1} \ldots X_n^{\alpha_n} f_{\alpha, j}(Y_1, \ldots, Y_m)$$

where the $f_{\alpha, j}$'s are polynomials in $k[Y_1, \ldots, Y_m]$.

Denote by J the ideal in $k[X_0, X_1, \ldots, X_n; Y_1, \ldots, Y_m]$ generated by $P_1, \ldots, P_r$ and by $\mathfrak{A}$ the ideal of polynomials f in $k[Y_1, \ldots, Y_m]$ with the following property (the so-called Hurwitz' Trägheitsformen):

(E) There exists an integer $N \geqslant 1$ such that $f X_0^N, f X_1^N, \ldots, f X_n^N$ all belong to J.

As usual we denote by $\mathbf{P}^n(K)$ the n-dimensional projective space over K.

Theorem C. *Let V be the subset of $\mathbf{P}^n(K) \times K^m$ consisting of the pairs (x, y) with $x = (x_0 : x_1 : \ldots : x_n)$ and $y = (y_1, \ldots, y_m)$ such that $P_j(x_0, x_1, \ldots, x_n; y_1, \ldots, y_m) = 0$ for $1 \leqslant j \leqslant r$. Let W be the subset of K^m consisting of the vectors y such that $Q(y) = 0$ for every Q in $\mathfrak{A}$. Then the projection of $V \subset \mathbf{P}^n(K) \times K^m$ onto the second factor K^m is equal to W.*

To reformulate theorem C, let us consider the ring

$$B = k[X_0, X_1, \ldots, X_n; Y_1, \ldots, Y_m]$$

together with its subring $B_0 = k[Y_1, \ldots, Y_m]$. Denote by B_d the B_0-module generated in B by the monomials of degree d in $X_0, X_1, \ldots, X_n$. Then $B = \bigoplus_{d \geqslant 0} B_d$ is a graded ring with J a graded ideal. Define the *graded ring* $A = B/J$ with $A_d = B_d/(B_d \cap J)$. We have the following properties:

(i) *As a ring,* A *is generated by* $A_0 \cup A_1$.

(ii) *For any nonnegative integer* d, A_d *is a finitely generated module over* A_0.

Furthermore, let $\mathfrak{S}$ be the ideal in A_0 consisting of all a's such that $aA_d = 0$ for all sufficiently large d's, i.e. the union of the annihilators of the A_0-modules $A_0, A_1, A_2, \ldots$.

THEOREM D. *Let* $A = \bigoplus_{d \geq 0} A_d$ *be a graded commutative ring obeying hypotheses* (i) *and* (ii) *above. Let* K *be an algebraically closed field and* $\varphi : A_0 \to K$ *be a ring homomorphism. In order that* φ *extend to a ring homomorphism* $\Psi : A \to K$ *which does not annihilate the ideal* $A^+ = \bigoplus_{d \geq 1} A_d$ *in* A, *it is necessary and sufficient that* φ *annihilate the ideal* $\mathfrak{S}$ *defined above.*

We leave to the reader the simple proof of the necessity in theorem D as well as the derivation of theorem C from theorem D.

4. PROOF OF THEOREM D

Let $\mathfrak{P}$ be the kernel of φ, a prime ideal in A_0. Assume $\mathfrak{S} \subset \mathfrak{P}$. We subject the ring A to a number of transformations. At each step, the properties (i) and (ii) enunciated before the statement of theorem D will be preserved, as well as property $A_d \neq 0$ for every $d \geqslant 0$. We shall mention what has been achieved after each step.

a) Factor A through the following graded ideal J: an element a in A belongs to J if and only if there exists an element s in A_0 such $s \notin \mathfrak{P}$ and $sa = 0$. For every $d \geqslant 0$, the annihilator $\mathfrak{S}_d$ of the A_0-module A_d is contained in $\mathfrak{S}$ hence in $\mathfrak{P}$ and this implies $J \cap A_d \neq A_d$. Put $A' = A/J$, $\mathfrak{P}' = (\mathfrak{P} + J)/J$ and $\Sigma = A_0' - \mathfrak{P}'$. Then *any element in* Σ *is regular in* A'.

b) Enlarge A' by replacing it by the subring A'' of the total quotient ring of A' consisting of the fractions with denominators in Σ. Let A_d'' be the set of fractions with numerator in A_d' and denominator in Σ; then $A'' = \bigoplus_{d \geq 0} A_d''$. Then A_0'' *is a local ring with maximal ideal* $\mathfrak{P}'' = \mathfrak{P}' \cdot A_0'$.

c) Factor A'' through the graded ideal $\mathfrak{P}'' \cdot A''$. Since A_d'' is a finitely generated module over the local ring A_0'', one gets $A_d'' \neq \mathfrak{P}'' A_d''$ by Nakayama's lemma. Put $k = A_0'' \backslash \mathfrak{P}''$, and $R = A''/\mathfrak{P}''A''$.

At this point, k is a field (the quotient field of $A_0/\mathfrak{P}$) and R is a graded algebra over the field k, so all assumptions of theorem B are fulfilled. Moreover let ε the composition of the natural maps

$$A \to A' \to A'' \to R\,.$$

In degree 0, ε_0 is nothing else than the natural map from A_0 into k with kernel $\mathfrak{P}$. Since φ has the same kernel $\mathfrak{P}$, it factors through ε_0, making K an algebraically closed extension of k.

We quote now theorem B. There exists a k-linear ring homomorphism $f : R \to K$ such that $f(R^+) \neq 0$. The composite map $\Psi = f\varepsilon$ has all the required properties.

5. Application to schemes

We keep the notation of theorem D. Recall that the spectrum S = **Spec** (A_0) of A_0 is the set of all prime ideals in A_0; the projective spectrum X = **Proj** (A) of A is the set of all *graded* prime ideals in A, which do not contain the ideal $A^+ = \bigoplus_{d \geq 1} A_d$. We have a natural map $\pi : X \to S$ associating to every graded prime ideal $\mathfrak{P}$ in A the prime ideal $\mathfrak{P} \cap A_0$ in A_0.

Moreover S and X are endowed with their respective Zariski topologies. A set F in S (resp. X) is closed if and only if there exists an ideal $\mathfrak{A}$ in A_0 (resp. A) such that F is the set of ideals $\mathfrak{P}$ of S (resp. X) containing $\mathfrak{A}$. It is obvious that π is continuous.

The following theorem is Grothendieck's version of the elimination theorem. Using his language, it is the main step in the proof that X = **Proj** (A) is a proper scheme over S = **Spec** (A_0).

Theorem E. *The map $\pi : X \to S$ is closed, that is the image of a closed set is closed.*

Let $F \subset X$ be closed and let $\mathfrak{A}$ be an ideal in A such that F consists of the graded prime ideals $\mathfrak{P}$ of X containing $\mathfrak{A}$. Replacing if necessary $\mathfrak{A}$ by the ideal generated by the homogeneous components of its elements, we may and shall assume that $\mathfrak{A}$ is a graded ideal. Let $\mathfrak{B}$ be the set of elements a in A_0 such that $a \,.\, A_d \subset \mathfrak{A}$ for large d, and let G be the set of prime ideals in A_0 containing $\mathfrak{B}$. It is obvious that π maps F into G.

Let $\mathfrak{P}_0$ be a prime ideal in G, hence $\mathfrak{P}_0 \supset \mathfrak{A}_0$ (where $\mathfrak{A}_0 = \mathfrak{A} \cap A_0$). Denote by k the quotient field of $A_0/\mathfrak{P}_0$ and by K an algebraically closed

overfield of k. Let φ be the natural composite map $A_0/\mathfrak{A}_0 \to A_0/\mathfrak{P}_0 \to k \to K$. We are now in a position to apply theorem D to the graded ring $A/\mathfrak{A}$, and we get a ring homomorphism $\Psi : A/\mathfrak{A} \to K$ extending φ and such that $\Psi((A^+ + \mathfrak{A})/\mathfrak{A}) \neq 0$. Let $\mathfrak{P}_d$ (for $d \geqslant 1$) be the set of elements a in A_d such that $\Psi(a + \mathfrak{A}) = 0$. Then $\mathfrak{P} = \bigoplus_{d \geqslant 0} \mathfrak{P}_d$ is a graded prime ideal in A containing $\mathfrak{A}$ with $\mathfrak{P} \neq A^+$ and $\mathfrak{P} \cap A_0 = \mathfrak{P}_0$. That is, $\mathfrak{P}$ belongs to F and π maps $\mathfrak{P}$ onto $\mathfrak{P}_0$.

(Reçu le 18 mars 1978)

P. Cartier

Institut des Hautes Etudes Scientifiques
F-91440 — Bures-sur-Yvette

J. Tate

Harvard University
Cambridge, Mass. 02138