

2. Proof of Hilbert's zero theorem

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **24 (1978)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **13.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

$S = \bigoplus_{d \geq 0} S_d$, 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, \dots, x_n respectively the cosets of X_0, X_1, \dots, X_n modulo J . Let φ be any k -linear ring homomorphism from R into K , and put $\xi_0 = \varphi(x_0), \dots, \xi_n = \varphi(x_n)$. It is clear that the vector $\xi = (\xi_0, \xi_1, \dots, \xi_n)$ is a common zero of the polynomials in J . Conversely, for any such common zero, there exists a unique k -linear ring homomorphism $\varphi : R \rightarrow K$ such that $\xi_0 = \varphi(x_0), \dots, \xi_n = \varphi(x_n)$. The vector ξ is equal to zero if and only if φ maps $R_1 = kx_0 + \dots + kx_n$ 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 $d \geq d_0$;*
- b) *or for every nonnegative integer d , one has $R_d \neq 0$ and there exists a k -linear ring homomorphism $\varphi : R \rightarrow K$ 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{S} 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{S} , hence \mathfrak{S} 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, \dots, a_r be a linear basis of R_1 over k . There would then exist an integer $N \geq 1$ such that $a_1^N = \dots = a_r^N = 0$, any monomial of degree $> Nr$ in a_1, \dots, 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 $d \geq 0$, and the inverse to $1 - x$ would be congruent to $1 + x + x^2 + \dots + x^d$ modulo the ideal $\sum_{i>d} R_i$ for every

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

$$(1) \quad u = b_1 f_1(x) + \dots + b_N f_N(x)$$

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

$$u \equiv b_1 f_1(1) + \dots + b_N f_N(1) \pmod{M},$$

hence $[L : k] \leq N$ 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{S} . Let $r_0 = 0$,

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

3. ELIMINATION THEORY

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

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

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

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

(E) There exists an integer $N \geq 1$ such that $f X_0^N, f X_1^N, \dots, f X_n^N$ 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 $x = (x_0 : x_1 : \dots : x_n)$ and $y = (y_1, \dots, y_m)$ such that $P_j(x_0, x_1, \dots, x_n; y_1, \dots, y_m) = 0$ for $1 \leq j \leq r$. 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

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

together with its subring $B_0 = k[Y_1, \dots, Y_m]$. Denote by B_d the B_0 -module generated in B by the monomials of degree d in X_0, X_1, \dots, X_n . Then $B = \bigoplus_{d \geq 0} B_d$ 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: