Séminaire Dubreil.
Algèbre et théorie
des nombres

Paulo Ribenboim

Le théorème des zéros pour les corps ordonnés

Séminaire Dubreil. Algèbre et théorie des nombres, tome 24, n° 2 (1970-1971), exp. n° 17, p. 1-32

<http://www.numdam.org/item?id=SD_1970-1971__24_2_A6_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
24e année, 1970/71, n° 17, 32 p.

28 juin 1971

LE THÉORÈME DES ZÉROS POUR LES CORPS ORDONNÉS

par Paulo RIBENBOIM

Cet exposé est basé sur les travaux de D. W. DUBOIS et G. EFROYMSON ([1] et [2]).

TABLE DES MATIÈRES

-:-:-:-

1. Introduction.

Soient $k \subseteq K$ des corps, et $n \geq 1$ un entier,

$$k[X] = k[X_1 , \dots , X_n] , \quad k(X) = k(X_1 , \dots , X_n) .$$

Pour tout sous-ensemble T de $k[X]$, soit

$$V_K(T) = \{x = (x_1 , \dots , x_n) \in K^n \mid f(x) = 0 \text{ pour tout } f \in T\} .$$

Pour tout sous-ensemble S de K^n, soit

$$Id_k(S) = \{f \in k[X] \mid f(x) = 0 \text{ pour tout } x \in S\} .$$

On a les propriétés évidentes suivantes :

1° $T \subseteq Id_k(V_K(T))$, $S \subseteq V_K(Id_k(S))$;

2° Si $S \subseteq S'$, alors $Id_k(S) \supseteq Id_k(S')$, si $T \subseteq T'$, alors $V_K(T) \supseteq V_K(T')$;

3° $V_K(Id_k(V_K(T))) = V_K(T)$;

4° Si I est l'idéal de $k[X]$, engendré par T, alors $V_K(I) = V_K(T)$;

5° Si $S = \{x\}$, où $x = (x_1 , \dots , x_n)$, $x_i \in k$, alors $Id_k(S)$ est un idéal maximal, à savoir celui engendré par les polynômes $X_1 - x_1 , \dots , X_n - x_n$.

Tout ensemble non vide de la forme $V_K(I)$, où I est un idéal de $k[X]$, s'appelle un k-ensemble algébrique de K^n.

Un problème fondamental est la détermination des idéaux I du type $I = Id_k(S)$, où S est un k-ensemble algébrique de K^n.

Le résultat suivant est bien connu.

THÉORÈME.des zéros de Hilbert. - Si K est la clôture algébrique de k, alors, pour tout idéal I de $k[X]$, on a $Id_k(V_K(I)) = \sqrt{I} = \{f \in k[X] \mid$ il existe $m \geqslant 1$ tel que $f^m \in I\}$.

$\sqrt{I}$ est le radical de I ; c'est un idéal contenant I, et égal à l'intersection des idéaux premiers contenant I. En fait, $\sqrt{I}$ est égal à l'intersection des idéaux premiers minimaux contenant I, et ceux-ci sont en nombre fini.

Il en résulte que, si $I \neq k[X]$, alors $\sqrt{I} \neq k[X]$ et $V_K(I) \neq \emptyset$. En outre, si $V_K(I)$ est un ensemble réduit à un point, alors $\sqrt{I}$ est un idéal maximal de $k[X]$; réciproquement, si $k = K$ et si $\sqrt{I}$ est un idéal maximal de $K[X]$, alors $V_K(I)$ est réduit à un point.

Que se passe-t-il lorsque K n'est pas algébriquement clos ?

Soit par exemple $k = K = \underset{\sim}{R}$. Dans ce cas, le théorème des zéros de Hilbert n'est plus valide. En effet, soit $f = X_1^2 + X_2^2 + 1$, f est irréductible en $\underset{\sim}{R}[X_1, X_2]$, l'idéal principal (f) est premier, donc $\sqrt{(f)} = (f)$. On a $V_{\underset{\sim}{R}}((f)) = \emptyset$, car $x_1^2 + x_2^2 + 1 \neq 0$ pour tout élément $x = (x_1, x_2) \in \underset{\sim}{R}^2$. Donc

$$Id_{\underset{\sim}{R}}(V_{\underset{\sim}{R}}((f))) = \underset{\sim}{R}[X_1, X_2] \neq (f) .$$

Dans cet exposé, il sera indiqué un théorème, analogue au théorème des zéros de Hilbert, pour le cas des corps ordonnés.

2. Rappel de quelques résultats sur les corps ordonnés.

La théorie des corps ordonnés a été développée par ARTIN et SCHREIER. Les quelques résultats cités ou démontrés ci-dessous seront importants dans la suite de cet exposé. Le lecteur pourra consulter les articles originaux de ARTIN et SCHREIER (parus en 1927 et 1928 aux Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg). Des présentations plus modernes se trouvent dans [3], [4] et [5].

(A) [ARTIN et SCHREIER]. - Soient k un corps ordonné, et $K|k$ une extension. Il existe un ordre total compatible sur le corps K, qui prolonge l'ordre donné sur k si, et seulement si, la condition suivante est vérifiée.

Si $\sum_i p_i x_i^2 = 0$, $1 \leqslant i \leqslant m$, $0 < p_i \in k$, $x_i \in K$, alors $x_1 = \ldots = x_m = 0$. On dit alors que $K|k$ est une extension ordonnable. Dans ce cas, $x \in K$ est positif pour tout ordre de K prolongeant l'ordre de k si, et seulement si,

$$x \in \{\textstyle\sum_{i=1}^m p_i x_i^2 \mid 0 < p_i \in k, \ x_i \in K\} .$$

Soient $K|k$ et $L|k$ des extensions. Soit A un sous-anneau de K contenant k. Tout k-homomorphisme $\sigma : A \to L$ s'appelle une L-spécialisation de $K|k$; A est le domaine de σ.

Soit $E \subseteq K$, et soit σ une L-spécialisation de $K|k$ dont le domaine contient E. Si $K|k$ et $L|k$ sont des extensions ordonnées, on dit que σ préserve E lorsque :

1° Si $x \in E$, $0 < x$, alors $0 < \sigma(x)$;
2° Si $x \in E$, $x < 0$, alors $\sigma(x) < 0$.

(B) [ARTIN]. - Soient $K|k$ et $L|k$ des extensions ordonnées. Soit

$$f = Y^m + a_1 Y^{m-1} + \ldots + a_m \in K[Y]$$

un polynôme ayant exactement $t \geqslant 0$ racines distinctes dans $\overline{K}$ (clôture réelle de K). Alors il existe un ensemble fini $E \subset K$, contenant les coefficients de f et tel que, si σ est une L-spécialisation de $K|k$ qui préserve E, alors

$$f^\sigma = Y^m + \sigma(a_1) Y^{m-1} + \ldots + \sigma(a_m)$$

a exactement t racines distinctes dans $\overline{L}$ (clôture réelle de L).

Démonstration. - Soit $(f_0, f_1, \ldots, f_s)$ la suite canonique de f. On rappelle que $f_0 = f$, $f_1 = f'$ (dérivée de f), $f_{j-1} = q_{j-1} f_j - f_{j+1}$ (pour $j = 1, \ldots, s-1$) et $f_{s-1} = q_{s-1} f_s$ avec $\deg(f_{j+1}) < \deg(f_j)$.

Soit $\eta = 1 + m + \sum_{i=1}^m a_i^2 \in K$. Soit E le sous-ensemble de K formé de tous les coefficients des polynômes f_j, q_j, ainsi que des éléments $f_j(-\eta)$, $f_j(\eta)$.

Soit σ une L-spécialisation de $K|k$ qui préserve E, donc son domaine contient E. La suite canonique de $f^\sigma \in L[X]$ est $(f_0^\sigma, f_1^\sigma, \ldots, f_s^\sigma)$.

Il est connu que toute racine de f dans la clôture réelle $\overline{K}$ est dans l'intervalle ouvert $(-\eta, \eta)$. Par le théorème de Sturm, le nombre de racines distinctes de f dans l'intervalle ouvert $(-\eta, \eta)$ de $\overline{K}$ est égal à la différence $V_{f,-\eta} - V_{f,\eta}$ où $V_{f,-\eta}$ est le nombre de changements de signe de la suite

$$(f_0(-\eta), f_1(-\eta), \ldots, f_s(-\eta)),$$

et $V_{f,\eta}$ celui de la suite

$$(f_0(\eta), f_1(\eta), \ldots, f_s(\eta)).$$

Ainsi $t = V_{f,-\eta} - V_{f,\eta}$.

Puisque $\sigma(\eta) = 1 + m + \sum_{i=1}^m \sigma(a_i)^2$, alors toute racine de f^σ dans $\overline{L}$ est dans l'intervalle $(-\sigma(\eta), \sigma(\eta))$. Leur nombre est égal à $V_{f^\sigma,-\sigma(\eta)} - V_{f^\sigma,\sigma(\eta)}$.

Or, la suite canonique de f^σ est $(f_0^\sigma , f_1^\sigma , \dots , f_s^\sigma)$, car le domaine de σ contient E , donc il contient les coefficients des polynômes f_j , q_j . D'autre part, $(f_j(-\eta))^\sigma = f_j^\sigma(-\sigma(\eta))$ et $f_j(-\eta) \in E$; ainsi $V_{f^\sigma,-\sigma(\eta)} = V_{f,-\eta}$. De même $V_{f^\sigma,\sigma(\eta)} = V_{f,\eta}$ et ainsi

$$t = V_{f,-\eta} - V_{f,\eta} = V_{f^\sigma,\sigma(\eta)} - V_{f^\sigma,-\sigma(\eta)} .$$

(C) [ARTIN]. - Soient $K|k$ et $L|k$ des extensions ordonnées. Soient

$$f_1 , \dots , f_t \in K[Y]$$

des polynômes (non nécessairement distincts) et

$$r_1 < r_2 < \dots < r_t$$

des éléments de $\overline{K}$ tels que r_i soit une racine de f_i . Alors il existe un ensemble fini $E \subset K$, contenant les coefficients de chaque f_i , tel que, si σ est une L-spécialisation de $K|k$ qui préserve E , il existe des éléments

$$b_1 , \dots , b_t \in \overline{L} ,$$

tels que $b_1 < b_2 < \dots < b_t$, et b_i est une racine de f_i^σ .

Démonstration. - De $r_j < r_{j+1}$ résulte $\sqrt{r_{j+1} - r_j} \in \overline{K}$. Soit

$$K' = K(r_1 , \dots , r_t , \sqrt{r_2 - r_1} , \dots , \sqrt{r_t - r_{t-1}}) ,$$

donc $K'|K$ est une extension algébrique finie, et alors il existe un élément primitif $K' = K(u)$; soit $g \in K[X]$ le polynôme minimal de u sur K . D'après (B), il existe un ensemble fini $E' \subset K$, contenant les coefficients de g et tel que si σ est une L-spécialisation de $K|k$ préservant E' , alors g^σ a une racine dans $\overline{L}$.

Soient p_i , $q_j \in K[Y]$ tels que $r_i = p_i(u)$ et $\sqrt{r_{j+1} - r_j} = q_j(u)$.

Soit $v_i = f_i(p_i) \in K[Y]$, donc $v_i(u) = f_i(p_i(u)) = f_i(r_i) = 0$ et alors $v_i = g v_i'$, avec $v_i' \in K[Y]$ (car g est le polynôme minimal de u). De même, si $\ell_j = p_{j+1} - p_j - q_j^2$, alors $\ell_j(u) = 0$, donc $\ell_j = g\ell_j'$ avec $\ell_j' \in K[Y]$. En outre, $q_j(u) \neq 0$, donc $1/q_j(u) \in K'$, et ainsi il existe $m_j \in K[Y]$ tel que $m_j(u) = \frac{1}{q_j(u)}$; si $z_j = m_j q_j - 1 \in K[Y]$, alors $z_j(u) = 0$, donc $z_j = g z_j'$, avec $z_j' \in K[Y]$.

Soit E l'ensemble union de E' avec l'ensemble des coefficients des polynômes f_i , g , p_i , q_j , v_i , v_i' , ℓ_j , ℓ_j' , m_j , z_j , z_j' . Soit σ une L-spécialisation de $K|k$ qui préserve E , donc aussi E' . Alors g^σ a une racine $\gamma \in \overline{L}$. De $v_i^\sigma = g^\sigma . v_i'^\sigma$, $\ell_j^\sigma = g^\sigma . \ell_j'^\sigma$ et $z_j^\ell = g^\sigma . z_j'^\sigma$, il résulte que γ est une racine de v_i^σ , c'est-à-dire $f_i^\sigma(p_i^\sigma(\gamma)) = v_i^\sigma(\gamma) = 0$, donc $b_i = p_i^\sigma(\gamma) \in \overline{L}$ est une racine de

f_i^σ . On a $\ell_j^\sigma(\gamma) = 0$, donc $b_{j+1} - b_j = p_{j+1}^\sigma(\gamma) - p_j^\sigma(\gamma) = (q_j^\sigma(\gamma))^2 \geqslant 0$, et puisque $z_j^\sigma(\gamma) = 0$, alors $m_j^\sigma(\gamma).q_j^\sigma(\gamma) = 1$, donc $q_j^\sigma(\gamma) \neq 0$ et $b_j < b_{j+1}$.

Soit $L|k$ une extension ordonnée. On dit que l'extension ordonnée $K|k$ est L-artinienne lorsque la propriété suivante est satisfaite : Si E est un sous-ensemble fini de K , il existe une L-spécialisation de $K|k$ qui préserve E .

Le résultat suivant est fondamental.

(D). - Soit $L|k$ une extension ordonnée telle que L soit dense (au sens de la topologie définie par les intervalles) dans sa clôture réelle $\overline{L}$. Si $K|k$ est une extension ordonnée L-artinienne et Y une indéterminée, alors $K(Y)|k$ est une extension L-artinienne (pour tout ordre de $K(Y)$ prologeant l'ordre de K).

Démonstration. - Soit E un sous-ensemble fini de $K(Y)$; il s'agit de montrer qu'il existe une L-spécialisation de $K(Y)|k$ qui préserve E . Il est facile de voir qu'on peut se réduire au cas où les éléments de E sont des polynômes unitaires irréductibles de $K[Y]$, ou bien des éléments de K .

Soit $\overline{K(Y)}$ une clôture réelle de $K(Y)$ (munie d'un ordre prolongeant celui de K) ; alors la clôture algébrique $\overline{K}$ de K dans $\overline{K(Y)}$ est une clôture réelle de K .

Soient $r_1 < r_2 < \ldots < r_t$ toutes les racines dans $\overline{K}$ des polynômes appartenant à E . Ces polynômes sont indexés de sorte que r_i est une racine de $f_i \in E$; il n'est pas exclu que $f_i = f_j$ pour $i \neq j$. Soit $g \in K[Y]$ le produit des polynômes non constants distincts appartenant à E . Les facteurs de g sont unitaires irréductibles, distincts, donc toutes les racines de g sont simples, et les racines de g dans $\overline{K}$ sont exactement r_1 , r_2 , ... , r_t .

Soit E' un sous-ensemble fini de K tel que :

1° E' contient les coefficients de g , les éléments de $E \cap K$ et les coefficients des polynômes appartenant à E ;

2° E' contient le discriminant $d \in K$ de g (on note que $d \neq 0$, car les racines de g sont simples) ;

3° E' est choisi (d'après (B) et (C)) de façon que, si σ est une L-spécialisation de $K|k$ qui préserve E' , alors g^σ a précisément t racines distinctes dans $\overline{L}$ (lesquelles sont simples, car le discriminant de g^σ est $d^\sigma \neq 0$), et il existe des éléments b_1 , ... , $b_t \in \overline{L}$ tels que $b_1 < b_2 < \ldots < b_t$, et b_i est une racine de f_i^σ .

D'après l'hypothèse, il existe une L-spécialisation σ de $K|k$ qui préserve

E' , donc la condition 3^c est satisfaite par σ . Il en résulte que $b_1 , \dots , b_t$ sont toutes les racines de g^σ dans $\overline{L}$.

On écrit $f_i = (Y - r_{i_1}) \dots (Y - r_{i_{t(i)}}).q_i$ avec $i_1 , \dots , i_{t(i)} \in \{1,,\dots , t\}$, $q_i \in \overline{K}[Y]$ n'ayant aucune racine dans $\overline{K}$. Or q_i est unitaire, donc un produit de polynômes quadratiques irréductibles de $\overline{K}[Y]$; alors q_i est une somme de carrés dans $\overline{K}[Y]$ et, par conséquent, q_i est positif dans $\overline{K(Y)}$.

$b_{i_1} , \dots , b_{i_{t(i)}}$ sont toutes les racines (dans $\overline{L}$) de f_i^σ (autrement g^σ aurait plus de t racines dans $\overline{L}$).

Alors $f_i^\sigma = (Y - b_{i_1}) \dots (Y - b_{i_{t(i)}}).p_i$, où $p_i \in \overline{L}[Y]$, p_i est unitaire sans racine dans $\overline{L}$. Alors p_i est un produit de polynômes quadratiques irréductibles dans $\overline{L}[Y]$, donc p_i est une somme de carrés dans $\overline{L}[Y]$. Alors, pour tout $Z \in \overline{L}$, $p_i(Z)$ est une somme de carrés dans $\overline{L}$, donc un élément positif de $\overline{L}$. Dans le corps ordonné $K(Y)$, il existe précisément un indice j tel que $r_{j-1} < Y < r_j$ (par convention $r_0 = - \infty$, $r_{t+1} = \infty$), car Y est transcendant sur K , tandis que chaque r_j est algébrique.

Par hypothèse, L est dense dans $\overline{L}$, donc il existe $Z \in L$ tel que $b_{j-1} < Z < b_j$.

Etant donné que q_i est positif dans $\overline{K(Y)}$, et $p_i(Z)$ est positif dans $\overline{L}$, il résulte que les signes de f_i et $f_i^\sigma(Z)$ sont le même, car le nombre de racines de f_i plus grandes que Y est le même que le nombre de racines de f_i^σ plus grandes que Z .

Soit $A \subseteq K[Y]$ l'anneau des polynômes à coefficients dans le domaine de σ . Alors $E \subseteq A$. Soit $\tau : A \longrightarrow L$ l'application, définie par $\tau(h) = h^\sigma(Z)$. Alors τ est une L-spécialisation de $K(Y)|k$ qui préserve E , en vertu des considérations précédentes. Ceci montre que $K(Y)|k$ est L-artinienne.

Comme corollaire, on a le résultat suivant.

(D'). - Soit $L|k$ une extension ordonnée telle que L soit dense dans $\overline{L}$. Si $n \geqslant 0$, alors, pour tout ordre de $k(X_1 , \dots , X_n)$ prolongeant celui de k , $k(X_1 , \dots , X_n)|k$ est L-artinienne.

Soit k un corps ; $f \in k(X_1 , \dots , X_n)$, $(x_1 , \dots , x_n) = x \in k^n$. On rappelle que f est définie en x lorsque $f = f_1/f_2$, avec $f_1 , f_2 \in k[X_1 , \dots , X_n]$ et $f_2(x_1 , \dots , x_n) \neq 0$. Alors on peut considérer la valeur de f en x , à savoir

$$f(x_1 , \dots , x_n) = \frac{f_1(x_1 , \dots , x_n)}{f_2(x_1 , \dots , x_n} \in k .$$

Soit $K|k$ une extension ordonnée, et soient L un sous-corps de K et

$$f \in k(X_1 , \dots , X_n) \subseteq K(X_1 , \dots , X_n) .$$

On dit que f est positive définie (sur L) lorsque $f(x) \geqslant 0$, si $x \in L^n$ et f est définie en x.

Comme corollaire de (D'), on déduit le résultat suivant.

(E). - Soient k un corps ordonné, $\bar{k}$ une clôture réelle de k,

$$f \in k(X_1 , \dots , X_n) \subseteq \bar{k}(X_1 , \dots , X_n) ,$$

positive définie (sur $\bar{k}$). Alors il existe des éléments

$$0 < p_i \in k , \quad g_i \in k(X_1 , \dots , X_n)$$

tels que $f = \sum p_i g_i^2$.

Démonstration. - Si f n'est pas de la forme indiquée, il résulte de (A) qu'il existe un ordre total sur $k(X_1 , \dots , X_n)$, prolongeant celui de k et tel que $f = f_1/f_2 < 0$. D'après (D), il existe une $\bar{k}$-spécialisation σ de $k(X_1, \dots, X_n)|k$ qui préserve $E = \{X_1 , \dots , X_n , f_2 , f\}$. Si $x_i = \sigma(X_i) \in \bar{k}$, alors

$$f_2(x_1 , \dots , x_n) = f_2(\sigma(X_1) , \dots , \sigma(X_n)) = \sigma(f_2) \neq 0 ,$$

donc f est définie en $(x_1 , \dots , x_n) \in \bar{k}^n$ et $f(x_1 , \dots , x_n) = \sigma(f) < 0$, contrairement à l'hypothèse.

En particulier, si $k = \bar{k}$, tout élément positif de $\bar{k}$ étant un carré, on peut écrire $f = \sum g_i^2$, $g_i \in k(X_1 , \dots , X_n)$, lorsque f est positive définie.

De façon analogue, (D) entraîne (E').

(E'). - Soit k un corps ordonné, qui est dense dans sa clôture réelle $\bar{k}$, et soit $f \in k(X_1 , \dots , X_n)$ positive définie (sur k) [Cette hypothèse est plus faible que celle de (E)]. Alors il existe des éléments

$$0 < p_i \in k , \quad g_i \in k(X_1 , \dots , X_n) ,$$

tels que $f = \sum p_i g_i^2$.

Démonstration. - Si f n'est pas de la forme indiquée, il résulte de (A) qu'il existe un ordre total sur $k(X_1 , \dots , X_n)$ prolongeant celui de k, et tel que $f = f_1/f_2 < 0$. D'après (D'), il existe une k-spécialisation σ de $k(X_1, \dots , X_n)|k$ qui préserve $E = \{X_1 , \dots , X_n , f , f_2\}$ (car k est dense dans $\bar{k}$). Si $x_i = \sigma(X_i) \in k$, alors $f_2(x_1 , \dots , x_n) = f_2(\sigma(X_1) , \dots , \sigma(X_n)) = \sigma(f_2) \neq 0$, donc f est définie en $(x_1 , \dots , x_n) \in k^n$ et $f(x_1 , \dots , x_n) = \sigma(f) < 0$, contrairement à l'hypothèse.

En prenant $k = \underline{Q}$, on déduit la réponse affirmative au 17e problème de Hilbert qui est due à ARTIN.

Dans cet exposé, on fera usage du résultat suivant.

(F). - Soient k un corps ordonné, $K = k(X_1 , \dots , X_n)$ muni d'un ordre prolongeant celui de k , $\overline{K}$ une clôture réelle de K . Soient $u_1 , \dots , u_m$ des éléments nuls de $k[X_1 , \dots , X_n]$, et f un polynôme à coefficients dans $k[X_1 , \dots , X_n]$ ayant une racine dans $\overline{K}$. Alors il existe un k-homomorphisme $\sigma : k[X_1 , \dots , X_n]$ tendant vers $\overline{k}$ (clôture réelle de k) tel que

1° $\sigma(u_i) \neq 0$ (pour tout $i = 1 , \dots , m$) ;

2° f^σ a une racine dans $\overline{k}$.

Démonstration. - On applique (B) avec $L = \overline{k}$. Il existe un ensemble fini $E \subset K$ tel que, si σ est une $\overline{k}$-spécialisation de $K|k$ qui préserve E , alors f^σ a une racine dans $\overline{k}$. En élargissant E si nécessaire, on peut supposer que

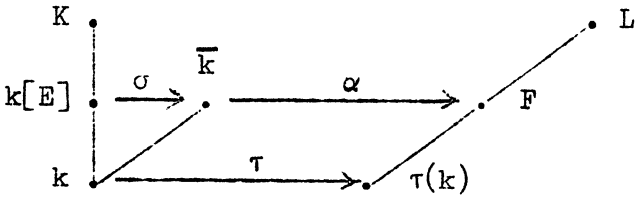
$$X_1 , \dots , X_n , u_1 , \dots , u_m \in E .$$

D'après (D), il existe une $\overline{k}$-spécialisation τ de $K|k$ qui préserve E . Soit σ la restriction de τ à $k[X_1 , \dots , X_n]$. Donc $\sigma(u_i) \neq 0$ (pour tout $i = 1 , \dots , r$) et f^σ a une racine dans $\overline{k}$.

(G) [LANG]. - Soit $\tau : k \to L$ une immersion ordonnée du corps ordonné k dans le corps ordonné maximal L . Soient $K|k$ une extension ordonnée, E un sous-ensemble fini de K . Alors il existe un homomorphisme $\psi : k[E] \to L$ qui prolonge τ .

Démonstration.

(α) Réduction au cas où $L = \overline{k}$ (clôture réelle de k) : On suppose le théorème vrai dans ce cas. Soit F la clôture algébrique de $\tau(k)$ dans L ; donc F est une clôture réelle de $\tau(k) \cong k$. D'après la théorie de ARTIN et SCHREIER, il existe un isomorphisme $\alpha : \overline{k} \to F$, qui prolonge τ . Par hypothèse, il existe un k-homomorphisme $\sigma : k[E] \to \overline{k}$. On prend $\psi = \alpha \circ \sigma$, donc ψ prolonge τ .



(β) Soit maintenant le cas où $L = \overline{k}$ et $\tau : k \to \overline{k}$ est l'inclusion. En remplaçant K par $k(E)$, on peut supposer que $K|k$ est une extension de type fini. Donc $K \cong k(X_1 , \dots , X_n)(u)$, où u est algébrique sur $k(X_1 , \dots , X_n)$. Sans

perte de généralité, on peut prendre u entier sur $k[X_1, \dots, X_n]$. Soient f le polynôme minimal de u sur $k[X_1, \dots, X_n]$, et s son degré ; donc f est unitaire, à coefficients dans $k[X_1, \dots, X_n]$. Si $t \in E$, on peut l'écrire sous la forme

$$t = (1/b^{(t)}) \sum_i a_i^{(t)} u^i , \quad 0 \leqslant i \leqslant s - 1$$

avec $a_i^{(t)}$, $b^{(t)} \in k[X_1, \dots, X_n]$.

L'ensemble $D = \{b^{(t)} \mid t \in E\}$ est fini. f a la racine u dans le corps ordonné K, donc f a une racine dans la clôture réelle $\overline{k(X_1, \dots, X_n)}$ de $k(X_1, \dots, X_n)$.

D'après (F), il existe un k-homomorphisme $\sigma : k[X_1, \dots, X_n] \to \overline{k}$ tel que

1° $\sigma(b^{(t)}) \neq 0$ (pour tout $t \in E$) ;

2° f^σ a une racine z dans $\overline{k}$.

Soit $\varphi : k[X_1, \dots, X_n][Y] \to \overline{k}$ l'homomorphisme défini par $\varphi(g) = g^\sigma(z)$. Si $g(u) = 0$, alors $g \in \mathrm{Ker}(\varphi)$. En effet, $g = fq$, avec $q \in k(X_1, \dots, X_n)[Y]$. Or f est unitaire, donc primitif ; d'après le lemme de Gauss, le contenu de g est égal au contenu de q ; les coefficients de g, étant dans $k[X_1, \dots, X_n]$, ceux de q sont aussi dans $k[X_1, \dots, X_n]$. On peut appliquer σ aux coefficients de g, f, q, en obtenant

$$g^\sigma(z) = f^\sigma(z).q^\sigma(z) = 0 ,$$

c'est-à-dire $\varphi(g) = 0$.

Ceci étant, φ induit un homomorphisme $\varphi' : k[X_1, \dots, X_n][u] \to \overline{k}$, à savoir $\varphi'(g(u)) = g^\sigma(z)$ pour tout $g \in k[X_1, \dots, X_n][Y]$. Il est clair que φ' prolonge σ.

Enfin, soit M la partie multiplicative de $k[X_1, \dots X_n]$ engendrée par l'ensemble D. Si $y \in M$, alors $\varphi'(y) = \sigma(y) \neq 0$. Donc φ' peut s'étendre à un k-homomorphisme $\psi : M^{-1}(k[X_1, \dots, X_n][u]) \to \overline{k}$.

Puisque $E \subseteq M^{-1}(k[X_1, \dots, X_n][u]$, on prend pour φ la restriction de φ' à $k[E]$.

Si k est un corps ordonné, et $a, b \in k$ sont des éléments positifs, on pose $a \sim b$ lorsqu'il existe des entiers $m, n > 0$ tels que $ma \geqslant b$ et $nb \geqslant a$.

La relation $\sim$ est une équivalence.

Si $0 < a, b$ sont des éléments de k, on écrit $a \ll b$ lorsque $na < b$ pour tout entier $n > 0$. On dit alors que a est <u>infiniment plus petit</u> que b, ou b est <u>infiniment plus grand</u> que a.

(H). - Quelques propriétés immédiates sont les suivantes :

1° Si $0 < a \leqslant b$, alors $b - a \sim b + a \sim b$;

2° Si $0 < a \leqslant b$, alors $0 < b^{-1} \leqslant a^{-1}$;

3° Si $0 < a, b$ et $a \sim b$, alors $a^{-1} \sim b^{-1}$;

4° Si $0 < a, b, a', b', a \sim a', b \sim b'$, alors $a + b \sim a' + b'$;

5° Si $0 < a, b, a', b', a \sim a', b \sim b'$, alors $ab \sim a'b'$;

6° Si $0 < a \leqslant b$, $0 < a' \leqslant b$, alors $a + a' \leqslant b$;

7° Si $0 < a \leqslant b$, $0 < a' \leqslant b'$, alors $0 < aa' \leqslant bb'$.

Démonstration.

1° $b - a \leqslant b$, car $0 < a$. De $2a \leqslant b$ vient $b \leqslant 2(b - a)$, ce qui montre $b - a \sim b$.

On a $b \leqslant b + a$. De $a \leqslant b$, on déduit $b + a \leqslant 2b$, donc $b + a \sim b$.

2° Soit $m > 0$, un entier tel que $mb^{-1} \geqslant a^{-1}$. Alors

$$ma = mb^{-1}(ab) \geqslant a^{-1}(ab) = b ,$$

contrairement à l'hypothèse.

3° Si $m, n > 0$ sont tels que $ma \geqslant b$ et $nb \geqslant a$, alors

$$mb^{-1} \geqslant a^{-1} \quad \text{et} \quad na^{-1} \geqslant b^{-1} , \text{ donc } a^{-1} \sim b^{-1} .$$

4° Soient $m, n > 0$ des entiers tels que $na \geqslant a'$, $mb \geqslant b'$. Si $mb \leqslant nb$, alors $n(a + b) \geqslant na + mb \geqslant a' + b'$. De même, il existe $n' > 0$ entier, tel que $n'(a' + b') \geqslant a + b$.

5° Soient $m, n > 0$ des entiers tels que $na \geqslant a'$, $mb \geqslant b'$. Donc

$$nm\, ab \geqslant a'b' \ (\text{car } a', b' > 0).$$

De même, un multiple entier de $a'b'$ est plus grand que ab, donc $ab \sim a'b'$.

6° S'il existe un entier $n > 0$ tel que $n(a + a') \geqslant b$, alors $na \geqslant b - na' > 0$. Donc $2na \geqslant 2(b - na') = 2b - 2na' \geqslant b$, car $a' \leqslant b$. Ceci est contraire à l'hypothèse que $a \leqslant b$.

7° S'il existe un entier $n > 0$ tel que $naa' \geqslant bb'$, alors de $0 < na < b$, il résulte $a' \geqslant b'$, ce qui est contraire à l'hypothèse.

Au cours de la démonstration du théorème principal, on fera usage du lemme suivant.

(i). - Soient K un corps ordonné, Y une indéterminée. Il existe un ordre sur $K(Y)$ qui prolonge l'ordre de K tel que :

1° $0 < Y$, et si $0 < a \in K$, alors $Y < a$;

2° Si $0 < h \in K[Y]$, $h(0) = a > 0$, alors $h \sim a$;

3° Si h_1 , $h_2 \in K[Y]$, $h_1(0) = h_2(0) = 1$, si $0 < a$, $b \in K$ et $r \geqslant 1$ est un entier, alors $b \ll a(h_1/h_2)(1/Y^r)$.

Démonstration. - Tout élément $h \in K(X)$ s'écrit de façon unique sous la forme canonique

$$h = \frac{h_1}{h_2} aY^r \quad \text{où } r \text{ est un entier, } a \in K ;$$

$$h_1 = 1 + a_1 Y + \ldots + a_m Y^m \in K[Y] ;$$

$$h_2 = 1 + b_1 Y + \ldots + b_n Y^n \in K[Y] .$$

Soit P l'ensemble des éléments $h \in K(Y)$ tels que $a \geqslant 0$ dans K .

On a $P + P \subseteq P$. En effet, si $h = (h_1/h_2)\, aY^r$, $h' = (h_1'/h_2')\, a'Y^{r'}$ sont sous forme canonique, et $a \geqslant 0$, $a' \geqslant 0$ si $r = r'$, alors

$$h + h' = \frac{(1/(a + a'))(h_1 h_2' a + h_2 h_1' a')}{h_2 h_2'} (a + a') Y^r \in P$$

(on note que $a + a' > 0$ à moins que $a = a' = 0$) ; par contre, si $r < r'$, alors

$$h + h' = \frac{(1/a)(h_1 h_2' a + h_2 h_1' a' Y^{r'-r})}{h_2 h_2'} aY^r \in P .$$

De même, $P.P \subseteq P$, $P \cap (-P) = \{0\}$, $P \cup (-P) = K(Y)$. Ceci montre que P est l'ensemble des éléments positifs pour un ordre total compatible sur $K(Y)$, prolongeant l'ordre de K (car $h = a \in K$ est dans P si, et seulement si, $a \geqslant 0$ dans K). Il reste à montrer les propriétés 1°, 2° et 3°.

1° C'est évident que $Y \in P$. Si $0 < a \in K$ de $1 - Y/a = ((1 - a^{-1} Y)/1).1.Y^0$, il résulte que $(1 - Y/a) \in P$, donc $Y < a$ dans $K(Y)$.

2° Pour tout entier $n \geqslant 1$ et pour tout élément $0 < b \in K$, on a $Y < (1/n)b$, donc $nY < b$, et alors $Y \ll b$. Il en résulte que si $h \in K[Y]$, $h(0) = a \neq 0$, alors la forme canonique de h est $h = (h_1/1)\, aY^0$ avec

$$h_1 = 1 + a_1 Y + \ldots + a_m Y^m ;$$

de (H), il résulte que $h_1 \sim 1$ (car $Y^i \ll 1$ pour $i = 1 , \ldots , m$) , et $h \sim a$.

3° D'après (H) et 2°, on a $0 < (a/b)(h_1/h_2) \sim a/b$; d'après 1°, on a $Y^r \ll a/b$, donc $b \ll a(h_1/h_2)(1/Y^r)$.

3. Sur les algèbres réelles.

Soit C un anneau (commutatif) totalement ordonné. Donc $0 < 1$, et C a la caractéristique 0. Soit $A|C$ une C-algèbre commutative.

On dit que $A|C$ est une algèbre réelle lorsque, si $a_i \in A$, $0 < p_i \in C$ et $\sum_i p_i a_i^2 = 0$, $1 \leqslant i \leqslant m$, alors $a_i = 0$ $(i = 1, \dots, m)$.

Il en résulte que l'homomorphisme canonique $C \to A$ est injectif.

Si $A|\underset{\sim}{Z}$ est une algèbre réelle, on dit simplement que A est un anneau réel. Ceci signifie que si $\sum_i a_i^2 = 0$, $1 \leqslant i \leqslant m$, $a_i \in A$, alors $a_i = 0$ $(i = 1, \dots, m)$.

Si $C = k$ est un corps ordonné, et $A = K$ est un corps, alors $K|k$ est une algèbre réelle si, et seulement si, $K|k$ est une extension ordonnable (§ 2, (A)).

Soient $A|C$ une algèbre, et I un idéal de la C-algèbre A. On dit que I est un idéal réel, lorsque A/I est une C-algèbre réelle. Ceci signifie que si

$$\sum_i p_i a_i^2 \in I, \quad 1 \leqslant i \leqslant m, \quad \text{avec} \quad a_i \in A, \quad 0 < p_i \in C,$$

alors $a_i \in I$ $(i = 1, \dots, m)$.

(A) On note les propriétés suivantes :

1° Si I est un idéal réel, alors $I = \sqrt{I}$;

2° Toute intersection d'idéaux réels de A est un idéal réel ;

3° L'union d'une chaîne croissante d'idéaux réels de A est un idéal réel ;

4° Tout idéal réel $I \neq A$ est contenu dans un idéal réel maximal (parmi les idéaux réels) ;

5° L'intersection d'une chaîne décroissante d'idéaux réels premiers est un idéal réel premier ;

6° Si P est un idéal réel premier contenant un idéal I, alors P contient un idéal réel premier P', contenant I et minimal avec cette propriété.

Démonstration.

1° Si $a \in \sqrt{I}$, il existe un entier $m \geqslant 1$, plus petit, tel que $a^m \in I$. Si m est pair, soit $m' = m$; si m est impair, soit $m' = m + 1$. Si $m' = 2\ell$, alors $(a^\ell)^2 \in I$, donc $a^\ell \in I$, car I est réel. D'après le choix minimal de m, on conclut que $m = 1$, donc $a \in I$.

2° et 3° sont évidents.

4° résulte du 3° et du lemme de Zorn.

5° est évident.

6° résulte du 5° et du lemme de Zorn appliqué à la famille des iédaux réels premiers contenant I et contenus dans P .

Soit $S(A|C) = \{1 + \sum_{i=1}^{m} p_i a_i^2 \mid 0 < p_i \in C , a_i \in A , m \geqslant 0\}$. $S(A|C)$ est une partie multiplicative de A .

Soit A^* l'anneau total de fractions de A ; donc $C \subseteq A^*$, et $A^*|C$ est une algèbre. Soit $S^*(A|C) = A \cap S(A^*|C)$, donc $S^*(A|C)$ est une partie multiplicative de A .

(B) Si $A|C$ est une algèbre réelle, alors :

1° $A^*|C$ est une algèbre réelle ;

2° $S(A|C)$, $S^*(A|C)$ n'ont pas de diviseurs de 0 .

Démonstration.

1° Soit $\sum_i p_i (a_i/b_i)^2 = 0$, avec a_i , $b_i \in A$, $1 \leqslant i \leqslant m$, b_i non diviseur de 0 , $0 < p_i \in C$. Soit $b = b_1 \dots b_m$, donc b n'est pas un diviseur de 0 , et on peut écrire (dans A^*) :

$$(1/b)^2 [\sum_i p_i a_i'^2] = 0 , \quad 1 \leqslant i \leqslant m , \text{ avec } a_i' = a_i(b/b_i) .$$

Alors $\sum_i p_i a_i'^2 = 0$, $1 \leqslant i \leqslant m$; ceci entraîne que $a_i' = 0$, donc $a_i = 0$;

2° Si $b(1 + \sum_i p_i a_i^2) = 0$, avec $a_i \in A$, $0 < p_i \in C$ et $1 + \sum_i p_i a_i^2 \neq 0$, $1 \leqslant i \leqslant m$, alors $b^2 + \sum_i p_i (ba_i)^2 = 0$, $1 \leqslant i \leqslant m$. Puisque $A|C$ est réelle, alors $b = 0$. D'après le 1°, $A^*|C$ est réelle, donc $S(A^*|C)$ n'a pas de diviseurd de 0 ; a fortiori, $S^*(A|C)$ n'a pas de diviseurs de 0 .

(C) Soit C un corps ordonné ou un anneau totalement ordonné archimédien. Soit $A|C$ une algèbre réelle, et soit P un idéal de A maximal parmi ceux qui sont disjoints de $S^*(A|C)$. Alors :

1° P est un idéal premier réel ;

2° Le corps des fractions F de A/P est une C-algèbre réelle.

Démonstration.

1° Soit $T = S^*(A|C)$; c'est une partie multiplicative de A . D'après le théorème bien connu de KRULL, P est un idéal premier.

Il reste à montrer que P est un idéal réel. Sinon, il existe un entier $m \geqslant 1$, des éléments $p_i \in C$, $0 < p_i$, et $a_i \in A$, $a_i \notin P$ $(i = 1 , \dots , m)$ tels que

$$a = \sum_{i=1}^{m} p_i a_i^2 \in P .$$

On a $p_1 a_1 \notin P$, autrement $p_1 \in P \cap C$. Si C est un corps, ceci est impossible, car $P \cap C = \{0\}$. Si C est archimédien et $n \geqslant 1$ est tel que $np_1 > 1$, alors $np_1 = 1 + (np_1 - 1).1^2 \in P \cap T$, ce qui est une contradiction.

Soit $J = P + Ap_1 a_1$, donc J contient strictement P et $J \cap T \neq 0$. Un élément de cet ensemble est de la forme $t = u + dp_1 a_1$, avec $t \in T$, $u \in P$, $d \in A$.

En prenant les carrés,

$$t^2 = u^2 + d^2 p_1^2 a_1^2 + 2udp_1 a_1$$
$$= u^2 + d^2 p_1(a - \textstyle\sum_{i=2}^{m} p_i a_i^2) + 2udp_1 a_1 .$$

D'après (B), T ne contient pas de diviseurs de 0 de A, donc

$$t^2[1 + \textstyle\sum p_1 p_i(da_i/t)^2] = u^2 + d^2 p_1 a + 2udp_1 a_1$$

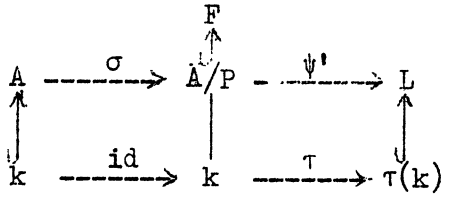
appartient à P et aussi à T. Ceci est une contradiction.

2° A/P est une C-algèbre réelle et intègre. Si F est son corps de fractions, il résulte de (B) que $F|C$ est une algèbre réelle.

Le résultat de LANG (§2, (G)) peut être généralisé, comme suit.

(D) Soit $\tau : k \to L$ une immersion ordonnée du corps ordonné k dans le corps ordonné maximal L. Soit $A|k$ une algèbre réelle de type fini. Alors il existe un homomorphisme $\psi : A \to L$ qui prolonge τ.

Démonstration.



$S^*(A|k)$ est une partie multiplicative de A. Donc il existe un idéal P, disjoint de $S^*(A|k)$, et maximal avec cette propriété. D'après (C), P est un idéal premier réel, donc A/P est une k-algèbre intègre et réelle. Soit F le corps de fractions de A/P ; il résulte de (C) que F est une k-algèbre réelle, c'est-à-dire $F|k$ est une extension ordonnable.

Par hypothèse, $A = k[x_1, \ldots x_n]$, donc $A/P = k[\overline{x}_1, \ldots, \overline{x}_n]$, où $\overline{x}_i$ est la classe de x_i modulo P. Soit $\sigma : A \to A/P$ l'homomorphisme canonique.

En vertu du résultat de LANG (§2, (G)), il existe un homomorphisme $\psi' : A/P \to L$ qui prolonge τ. En prenant $\psi = \psi' \circ \sigma$, on voit que $\psi \cdot A \to L$ est un homomorphisme qui prolonge τ.

Comme corollaire, on a le résultat suivant.

(E) Soient k un corps ordonné, $\overline{k}$ une clôture réelle de k, $A|k$ une algèbre réelle, et $u_1, \dots, u_n$ des éléments de A qui ne sont pas des diviseurs de 0. Alors il existe un k-homomorphisme $\psi : k[u_1, \dots, u_n] \longrightarrow \overline{k}$ tel que, pour $i = 1, \dots, n$, $\psi(u_i) \neq 0$.

Démonstration. - Soit A^* l'anneau total de fractions de A. D'après (A), $A^*|k$ est une algèbre réelle et chaque élément u_i est inversible dans A^*. Soit

$$B = k[u_1, \dots, u_n, u_1^{-1}, \dots, u_n^{-1}],$$

donc $B|k$ est une algèbre réelle de type fini. D'après (D), il existe un k-homomorphisme $\psi : B \longrightarrow \overline{k}$. De $u_i u_i^{-1} = 1$, il résulte que $\psi(u_i).\psi(u_i^{-1}) = 1$, donc $\psi(u_i) \neq 0$ pour $i = 1, \dots, n$.

4. Le théorème des zéros réels.

Soient k un corps ordonné, $\overline{k}$ une clôture réelle de k. On note

$$A = k[X] = k[X_1, \dots, X_n], \quad k(X) = k(X_1, \dots, X_n).$$

On déterminera les idéaux de $k[X]$ du type $I = \mathrm{Id}_k(S)$, où S est un k-ensemble algébrique de $\overline{k}^n$. Le théorème principal a été démontré par DUBOIS. Le cas particulier où $k = \underline{R}$, a été obtenu, sous une forme un peu différente et de façon indépendante (mais postérieure), par J.-J. RISLER [6].

Si I est un idéal de $k[X_1, \dots, X_n]$, le radical réel de I est l'ensemble $\sqrt[R]{I}$ des $f \in k[X_1, \dots, X_n]$ tels qu'il existe un entier $m \geqslant 1$ et des éléments $p_i \in k$, $0 < p_i$, $u_i \in k(X_1, \dots, X_n)$ avec $f^m(1 + \sum_i p_i u_i^2) \in I$, $1 \leqslant i \leqslant r$.

(A) Soient I, J des idéaux de $k[X_1, \dots, X_n]$. Alors

1° $I \subseteq \sqrt{I} \subseteq \sqrt[R]{I}$;

2° Si $I \subseteq J$, alors $\sqrt[R]{I} \subseteq \sqrt[R]{J}$;

3° $\sqrt[R]{\sqrt[R]{I}} = \sqrt[R]{I}$;

4° $\sqrt[R]{\sqrt{I}} = \sqrt{\sqrt[R]{I}} = \sqrt[R]{\sqrt{I}} = \sqrt[R]{I}$.

Démonstration.

1° et 2° sont triviaux.

3° Si $f \in \sqrt[R]{\sqrt[R]{I}}$, soit $m \geqslant 1$ entier, et $s \in S = S(k(X_1, \dots, X_n)|k)$ tels $f^m s \in \sqrt[R]{I}$. De même, soient $\ell \geqslant 1$ entier et $s' \in S$ tels que $(f^m s)^\ell s' \in I$. Alors $f^{m\ell}(s^\ell s') \in I$, avec $s^\ell s' \in S$, donc $f \in \sqrt[R]{I}$. L'autre inclusion est évidente.

4° $\sqrt[R]{I} \subseteq \sqrt[R]{\sqrt{I}} \subseteq \sqrt[R]{\sqrt[R]{I}} = \sqrt[R]{I}$ et aussi $\sqrt[R]{I} \subseteq \sqrt{\sqrt[R]{I}} \subseteq \sqrt[R]{\sqrt[R]{I}} = \sqrt[R]{I}$.

(B) Soient $g = f^m s$, où $f \in k[X_1 , \dots , X_n]$, $m \geqslant 1$ un entier, et s appartenant à $S(k(X_1 , \dots , X_n)|k)$. Soit $K|k$ une extension ordonnée. Si g appartient à $k[X_1 , \dots , X_n]$, $x = (x_1 , \dots , x_n) \in K$, et $g(x) = 0$, alors $f(x) = 0$.

Démonstration. - Si $f(x) \neq 0$, alors $s = (f^m s)/f^m$ est définie en x , donc $g(x) = (f(x))^m . s(x)$.

Si $g(x) = 0$, alors $s(x) = 0$.

D'autre part, $s = 1 + \Sigma\, p_i\, u_i^2$ (avec $0 < p_i \in k$, $u_i \in k(X_1 , \dots , X_n)$) et K est un corps ordonné, alors $s(x) \geqslant 1$, donc $s(x) \neq 0$, c'est une contradiction.

THÉORÈME [DUBOIS]. - Si k est un corps ordonné et $\overline{k}$ une clôture réelle de k , alors

$$Id_k(V_{\overline{k}}(I)) = \sqrt[R]{I}$$

pour tout idéal I de $k[X]$.

Démonstration. - On montre d'abord que $\sqrt[R]{I} \subseteq Id_k(V_{\overline{k}}(I))$. Si $f \in \sqrt[R]{I}$, il existe un entier $m \geqslant 1$ et des éléments $0 < p_i \in k$, $u_i \in k(X_1 , \dots , X_n)$ tels que

$$f^m(1 + \Sigma_i\, p_i\, u_i^2) \in I , \quad 1 \leqslant i \leqslant \ell .$$

Si $x \in V_{\overline{k}}(I)$, alors

$$[f^m(1 + \Sigma_i\, p_i\, u_i^2)](x) = 0 , \quad 1 \leqslant i \leqslant \ell .$$

D'après (B), on a $f(x) = 0$, ce qui montre que $f \in Id_k(V_{\overline{k}}(I))$.

Pour montrer l'inclusion opposée, on établira d'abord quelques faits simples.

(α) $I \cap S^*(A|k) = \emptyset$ si, et seulement si, $1 \notin \sqrt[R]{I}$.

En effet, si $1 \in \sqrt[R]{I}$, il existe $s \in S(k(X_1 , \dots , X_n)|k)$ tel que $s = 1.s \in I$; donc $s \in S^*(A|k) \cap I$. D'autre part, si $s \in S^*(A|k) \cap I$, alors $1 \in \sqrt[R]{I}$, car $1.s = s \in I$.

(β) Si $1 \notin \sqrt[R]{I}$, alors $V_{\overline{k}}(I) = \emptyset$.

D'après (α) , $I \cap S^*(A|k) = \emptyset$. Soit J un idéal, disjoint de $S^*(A|k)$, contenant I et maximal avec ces propriétés. Alors $V_{\overline{k}}(J) \subseteq V_{\overline{k}}(I)$, et il suffit de montrer que $V_{\overline{k}}(J) \neq \emptyset$. D'après le § 3, (C), A/J est une k-algèbre réelle et de type fini. D'après le § 3, (D), il existe un k-homomorphisme $\psi : A/J \to \overline{k}$.

Soient $x_i = X_i + J$ (classe résidue de x_i modulo J), et

$$(\psi(x_1) , \dots , \psi(x_n)) \in \overline{k}^n .$$

Alors

$$f(\psi(x_1) , \dots , \psi(x_n)) = \psi(f(X_1 , \dots , X_n)) = 0$$

pour tout $f \in J$. Donc $V_{\overline{k}}(J) \neq \emptyset$.

Ceci étant, soient $f_1 , \ldots , f_t \in A$ des générateurs de l'idéal I , donc $I = \sum_i Af_i$, $1 \leqslant i \leqslant t$. Soit $f \in Id_k(V_{\overline{k}}(I))$; on peut supposer $f \neq 0$, donc f est inversible dans le corps $k(X_1 , \ldots , X_n)$. On considère sur $k(X_1 , \ldots , X_n)$ un ordre prolongeant celui de k et tel que f soit positif (quitte à considérer $-f$ à la place de f).

Soit T une nouvelle indéterminée, et soit $A' = k[X_1 , \ldots , X_n , T] = A[T]$. Soit $I' = \sum_i A' f_i + A'(1 - fT)$, $1 \leqslant i \leqslant t$. Alors $V_{\overline{k}}(I') = \emptyset$, car si

$$(x_1 , \ldots , x_n , y) \in \overline{k}^{n+1} \text{ appartient à } V_{\overline{k}}(I') ,$$

alors

$$f_i(x_1 , \ldots , x_n) = 0 \quad \text{pour} \quad i = 1 , \ldots , t ,$$

donc $f(x_1 , \ldots , x_n) = 0$, car $f \in Id_k(V_{\overline{k}}(I)$; il en résulte que

$$(1 - fT)(x_1 , \ldots , x_n , y) = 1 - f(x_1 , \ldots , x_n)y = 1 ,$$

qui est une contradiction.

D'après (β), $1 \in \sqrt[R]{I'}$, et ainsi il existe des éléments

$$0 < p_i \in k , \quad g_i \in k(X_1 , \ldots , X_n , T) , \quad u_j , u \in k[X_1 , \ldots , X_n , T]$$

tels que

$$(*) \qquad 1 + \sum_i p_i g_i^2 = \sum_j u_j f_j + u(1 - fT) , \quad 1 \leqslant i \leqslant \ell , \quad 1 \leqslant j \leqslant t .$$

On écrit $g_i = e_i/d_i$ avec $d_i , e_i \in k[X_1 , \ldots , X_n , T]$, et e_i , d_i premiers entre eux.

Il suffira de montrer le résultat ci-après.

(γ) $d_i(X_1 , \ldots , X_n , f^{-1}) \neq 0$ dans $k(X_1 , \ldots , X_n)$.

Si cela est vrai pour tout indice $i = 1 , \ldots , \ell$, on peut remplacer T par f^{-1} dans la relation (*), et on obtient

$$1 + \sum_i p_i[g_i(X_1 , \ldots , X_n , f^{-1})]^2 = \sum_j u_j(X_1 , \ldots , X_n , f^{-1}).f_j ,$$

avec $1 \leqslant i \leqslant \ell$, $1 \leqslant j \leqslant t$.

Puisque chaque u_j est un polynôme en T , il existe un entier $m \geqslant 0$ tel que

$$f^m.u_j(X_1 , \ldots , X_n , f^{-1}) \in k[X_1 , \ldots , X_n] \quad \text{pour} \quad j = 1 , \ldots , t .$$

Alors

$$f^m(1 + \sum_i p_i(g_i(X_1 , \ldots , X_n , f^{-1})^2) \in \sum_j Af_j = I , \quad 1 \leqslant i \leqslant \ell , \quad 1 \leqslant j \leqslant t .$$

Ceci montre que $f \in \sqrt[R]{I}$.

Tout se ramène à la démonstration de (γ) .

On suppose que $d_j(X_1 , \dots , X_n , f^{-1}) = 0$ (pour un indice j). Alors

$$d_j \in k(X_1 , \dots , X_n)[T]$$

est multiple de $T - f^{-1}$ dans $k(X_1 , \dots , X_n)[T]$:

$$d_j = (T - f^{-1}).q_j = (fT - 1).q'_j \quad \text{avec} \quad q'_j = \frac{1}{f}\, q_j \in k(X)[T] .$$

En prenant les contenus de ces polynômes en T (idéal engendré par les coefficients), d'après le lemme de Gauss :

$$\mathrm{cont}(d_j) = \mathrm{cont}(fT - 1).\mathrm{cont}(q'_j) .$$

Or $\mathrm{cont}(fT - 1)$ est l'idéal unitaire de $k[X_1 , \dots , X_n]$. Donc

$$\mathrm{cont}(q'_j) = \mathrm{cont}(d_j) \subseteq k[X_1 , \dots , X_n] ,$$

c'est-à-dire d_j est divisible par $Y = fT - 1$ dans l'anneau $A[T]$. Puisque e_j , d_j sont premiers entre eux, alors e_j n'est pas divisible par Y .

De $k(X_1 , \dots , X_n)[T] = k(X_1 , \dots , X_n)[Y]$, il résulte qu'on peut écrire

$$g_j = \frac{h_1}{h_2}\, \frac{1}{Y^r} \quad \text{avec} \quad r \geqslant 1 \quad \text{entier} ,$$

$$h_1 , h_2 \in k(X_1 , \dots , X_n)[Y] , \quad c \in k(X_1 , \dots , X_n) , \quad h_1(0) = h_2(0) = 1 .$$

D'après le § 2, (I), il existe un ordre sur $k(X_1 , \dots , X_n)(Y)$ prolongeant l'ordre de $k(X_1 , \dots , X_n)$, tel que $Y \ll 1$ et, si $h \in k(X_1 , \dots , X_n)$, $0 < h$, alors

$$h \ll p_j\, g_j^2 = p_j\, \frac{h_1^2}{h_2^2}\, c^2\, \frac{1}{Y^{2r}} .$$

Etant donné que $0 < p_j\, g_j^2$ pour tout indice $i = 1 , \dots , \ell$, on conclut que $1 + \sum_i p_i\, g_i^2$ est infiniment plus grand que tout élément de $k(X_1 , \dots X_n)$.

D'autre part, le 2e membre de la relation (*) est positif (dans $k(X_1,\dots,X_n,T)$) et de la forme $h_0 + h_1\, T + \dots + h_r\, T^r$ avec $h_i \in k(X_1 , \dots , X_n)$. Soient $h' = |h_0| + |h_1|.f^{-1} + \dots + |h_r|.f^{-r} \in k(X_1 , \dots , X_n)$. De $T = f^{-1}(1 + Y)$ et $0 < f$, $Y \ll 1$, il résulte que $0 < 1 + Y \sim 1$, donc $0 < T \sim f^{-1}$. Alors

$$h' \sim |h_0| + |h_1|.T + \dots + |h_r|.T^r \geqslant |h_0 + h_1\, T + \dots + h_r\, T^r|$$

$$= h_0 + h_1\, T + \dots + h_r\, T^r = 1 + \sum_i p_i\, g_i^2 , \quad 1 \leqslant i \leqslant \ell .$$

Ainsi il existe un entier $n' \geqslant 1$ tel que $n'\, h' \geqslant 1 + \sum_i p_i\, g_i^2$, $1 \leqslant i \leqslant \ell$, ce qui est un contradiction.

(C) Pour tout idéal I de $k[X_1, \dots, X_n]$, $\sqrt[R]{I}$ est un idéal réel.

Démonstration. - On a vu que $\sqrt[R]{I} = Id_k(V_{\overline{k}}(I))$, donc $\sqrt[R]{I}$ est un idéal.

Maintenant, soient des éléments $0 < p_i \in k$, $f_i \in k[X_1, \dots, X_n]$ tels que $\sum p_i f_i^2 \in \sqrt[R]{I}$.

D'après le théorème ci-dessus [DUBOIS], si $x \in V_{\overline{k}}(I)$, alors

$$(\sum p_i f_i^2)(x) = \sum p_i [f_i(x)]^2 = 0 .$$

Il en résulte que $f_i(x) \equiv 0$, pour tout i et tout $x \in V_{\overline{k}}(I)$. D'après le même théorème, $f_i \in \sqrt[R]{I}$ pour tout indice i, ce qui montre que l'idéal $\sqrt[R]{I}$ est réel.

Pour montrer (F), on établira d'abord le résultat qui suit.

(D) Soit C un anneau totalement ordonné. Soient $A|C$ une C-algèbre, I un idéal réel de A. Si $a \in A$, $a \notin I$, alors l'idéal $\sqrt{(I : Aa)}$ est réel.

Démonstration. - Si $\sum_i p_i u_i^2 \in \sqrt{(I : Aa)}$, $1 \leqslant i \leqslant \ell$ (avec $0 < p_i \in C$, et $u_i \in A$), il existe un entier $m \geqslant 1$ tel que $(\sum_i p_i u_i^2)^m a \in I$, donc aussi $(\sum_i p_i u_i^2)^m a^2 \in I$, $1 \leqslant i \leqslant \ell$. Alors on obtient

$$\sum_i p_i^m (u_i^m a)^2 + \sum q_j v_j^2 \in I , \quad 1 \leqslant i \leqslant \ell ,$$

avec $0 < q_j \in C$, $v_j \in A$. Puisque I est réel, alors $u_i^m a \in I$, donc

$$u_i \in \sqrt{(I : Aa)} \quad \text{pour tout indice } i = 1, \dots, \ell .$$

Ceci montre que $\sqrt{(I : Aa)}$ est réel.

On rappelle que si A est un anneau, et I un idéal de A, un idéal premier P de A est associé à I lorsqu'il existe $a \in A$, $a \notin I$, tel que $P = (I : Aa)$, donc $P = \sqrt{(I : Aa)}$.

Tout idéal premier P de A contenant I contient un idéal premier P', contenant I et minimal avec cette propriété ; en plus, si A est noethérien, P' est un idéal associé à I.

Ainsi, si I est un idéal réel de $A|C$, alors tout idéal premier associé à I est réel. En plus, si A est noethérien, tout idéal premier minimal contenant I est réel.

(E) Soient k un corps ordonné et P un idéal réel premier de $k[X_1, \dots X_n]$. Alors $\sqrt[R]{P} = P$.

Démonstration. - Soit $f \in \sqrt[R]{P}$, donc il existe un entier $m \geqslant 1$ et des éléments $0 < p_i \in k$, $u_i \in k(X_1, \dots, X_n)$ tels que $g = f^m(1 + \sum p_i u_i^2) \in P$.

$k[X_1 , \dots , X_n]/P$ est une k-algèbre intègre et réelle ; soit K son corps de fractions, donc $K|k$ est une algèbre réelle, c'est-à-dire une extension ordonnable. Si x_i est l'image de X_i dans $k[X_1 , \dots , X_n]/P$ par l'homomorphisme canonique ψ , et $x = (x_1 , \dots , x_n) \in K^n$, alors $g(x_1 , \dots , x_n) = \psi(g) = 0$, puisque $g \in P$. Il résulte de (B) que $\psi(f) = f(x_1 , \dots , x_n) = 0$, donc $f \in P$. L'autre inclusion est évidente.

(F) Soit k un corps ordonné maximal. Tout idéal réel maximal (parmi les idéaux réels) de $k[X_1 , \dots , X_n]$ est un idéal maximal.

Démonstration. - Soit I un idéal réel, maximal parmi les idéaux réels de $A = k[X_1 , \dots , X_n]$. Si P est un idéal premier minimal contenant I , alors $P \neq A$ est un idéal réel, $P \supseteq I$. D'après l'hypothèse, $P = I$, et d'après (E), $P = {}^R\sqrt{P}$, c'est-à-dire $I = {}^R\sqrt{I}$. Donc $V_{\overline{k}}(I) \neq 0$ (sinon ${}^R\sqrt{I} = Id_k(V_{\overline{k}}(I)) = A$). Soient

$$x = x_1 , \dots , x_n) \quad \text{et} \quad M = \sum_i A(X_i - x_i) , \quad 1 \leqslant i \leqslant n .$$

Alors M est un idéal maximal de A , car $\overline{k} = k$,

$$M = Id_k(\{x\}) \supseteq Id_k(V_{\overline{k}}(I)) \supseteq I .$$

Mais $\{x\} = V_{\overline{k}}(M)$, donc ${}^R\sqrt{M} = M$ est un idéal réel (d'après (C)). Ainsi $I = M$ est un idéal maximal de A .

(G) I est un idéal réel de $k[X_1 , \dots , X_n]$ si, et seulement si, $I = {}^R\sqrt{I}$.

Démonstration. - On a vu au § 3, (A), que $I = \sqrt{I}$. Il suffit de montrer que $\sqrt{I} = {}^R\sqrt{I}$.

Si P est un idéal premier minimal contenant I , alors P est un idéal réel, donc $P = {}^R\sqrt{P} \supseteq {}^R\sqrt{I}$ (d'après (E)). Ainsi $\sqrt{I} \supseteq {}^R\sqrt{I}$. D'autre part, $\sqrt{I} \subseteq {}^R\sqrt{I}$ (d'après (A)), donc $\sqrt{I} = {}^R\sqrt{I}$.

Comme corollaire, on a le résultat suivant.

(H) I est un idéal d'un k-ensemble algébrique de $\overline{k}^n$, si, et seulement si, I est un idéal réel.

Démonstration. - L'affirmation résulte aussitôt du théorème de Dubois et de (G).

(I) Pour tout idéal I de $k[X_1 , \dots , X_n]$, on a ${}^R\sqrt{I} = \cap \{P \mid P \text{ idéal réel premier contenant } I\} = P_1 \cap \dots \cap P_s$ (intersection des idéaux premiers minimaux contenant ${}^R\sqrt{I}$).

Démonstration. - Puisque ${}^R\sqrt{I}$ est réel, alors chaque idéal P_i est réel. Il résulte de (A) que

$\sqrt[R]{I} = \sqrt{\sqrt[R]{I}} = P_1 \cap \dots \cap P_s \supseteq \cap \{P \mid P \text{ idéal réel premier contenant } I\} \supseteq \sqrt[R]{I}$, car $P = \sqrt[R]{P} \supseteq \sqrt[R]{I}$ lorsque P est un idéal réel premier contenant I .

5. Algèbre commutative réelle.

Soient C un anneau totalement ordonné, et $A|C$ une C-algèbre. Le radical réel de l'idéal I de A est, par définition, l'intersection des idéaux réels premiers de A qui contiennent I . On le note $\sqrt[R]{I}$.

D'après le § 4, (I), si $A = k[X_1, \dots, X_n]$, cette notion de radical réel coïncide avec celle introduite auparavant.

(A) Soient $A|C$ une C-algèbre, I et J des idéaux de A .

1° $I \subseteq \sqrt{I} \subseteq \sqrt[R]{I}$;

2° Si $I \subseteq J$, alors $\sqrt[R]{I} \subseteq \sqrt[R]{J}$;

3° $\sqrt[R]{\sqrt[R]{I}} = \sqrt{\sqrt[R]{I}} = \sqrt[R]{\sqrt{I}} = \sqrt[R]{I}$;

4° $\sqrt[R]{I}$ est un idéal réel.

Démonstration.

1° et 2° sont évidents.

3° D'abord on a $\sqrt[R]{\sqrt[R]{I}} = \sqrt[R]{I}$. En effet, si P est un idéal réel premier contenant I , alors il contient $\sqrt[R]{I}$. Donc

$$\sqrt[R]{\sqrt[R]{I}} = \cap \{P \mid P \text{ idéal réel premier contenant } \sqrt[R]{I}\}$$

$$\subseteq \cap \{P \mid P \text{ idéal réel premier contenant } I\} = \sqrt[R]{I} ,$$

et ainsi $\sqrt[R]{I} = \sqrt[R]{\sqrt[R]{I}}$. De ceci et du 1°, il résulte (comme dans le § 4, (A) 4°) que $\sqrt[R]{\sqrt[R]{I}} = \sqrt{\sqrt[R]{I}} = \sqrt[R]{\sqrt{I}} = \sqrt[R]{I}$.

4° $\sqrt[R]{I}$ est une intersection d'idéaux réels, donc c'est un idéal réel (§ 3 , (A)).

(B) Si $A|C$ est une C-algèbre noethérienne et I un idéal de A tel que $\sqrt[R]{I} \neq A$, alors :

1° Il existe un nombre fini d'idéaux réels premiers minimaux contenant I , à savoir P_1 , ... , P_s (avec $s > 0$) ;

2° $\sqrt[R]{I} = P_1 \cap \dots \cap P_s$, cette intersection est irréductible, et P_1 , ... , P_s sont les idéaux premiers minimaux contenant $\sqrt[R]{I}$;

3° $\sqrt{I} = \sqrt[R]{I}$ si, et seulement si, tout idéal premier minimal contenant I est réel ;

4° I est un idéal réel si, et seulement si, $I = \sqrt[R]{I}$.

Démonstration.

1° et 2°. Soient $P_1, \dots, P_s$ $(s > 0)$ les idéaux premiers minimaux contenant ${}^R\sqrt{I} \neq A$. Puisque A est noethérien, ces idéaux sont associés à ${}^R\sqrt{I}$; celui-ci étant un idéal réel (d'après (A)), il résulte du § 4, (D) que chaque P_i est réel.

Si P est un idéal réel premier et $P_i \supseteq P \supseteq I$, alors $P \supseteq {}^R\sqrt{I}$; d'après la minimalité, on a $P_i = P$. Ceci montre que $\{P_1, \dots, P_s\}$ est contenu dans l'ensemble des idéaux réels premiers minimaux P' contenant I. Mais $P' \supseteq {}^R\sqrt{I}$, donc P' contient un des idéaux P_i, c'est-à-dire $P' = P_i$. Ceci montre les affirmations 1° et 2°, en tenant compte que ${}^R\sqrt{I} = \sqrt{{}^R\sqrt{I}} = P_1 \cap \dots \cap P_s$ et qu'une telle intersection est nécessairement irréductible.

3° Si $\sqrt{I} = {}^R\sqrt{I}$, alors $\sqrt{I}$ est un idéal réel. Si P est un idéal premier minimal contenant I, alors $P \supseteq \sqrt{I}$, et P est minimal contenant $\sqrt{I}$. Donc P est associé à $\sqrt{I}$, et d'après le § 4, (D), P est réel.

Réciproquement, si tout idéal premier minimal P contenant I est réel, alors $\sqrt{I} \supseteq {}^R\sqrt{I}$, d'où l'égalité.

4° Si $I = {}^R\sqrt{I}$, alors I est un idéal réel. Réciproquement, si I est un idéal réel, d'après le § 3, (A), on a $I = \sqrt{I}$. Or tout idéal premier minimal contenant I est réel ; d'après le 3°, on a $\sqrt{I} = {}^R\sqrt{I}$, donc $I = {}^R\sqrt{I}$.

(C) *Soient $A|C$ une C-algèbre noethérienne, I un idéal de A, et I' l'ensemble des éléments $x \in A$ tels qu'il existe des éléments $a_i \in A$ satisfaisant $x^2 + \sum a_i^2 \in I$. Alors I' est un idéal de A, et $\sqrt{I'} = {}^R\sqrt{I}$.*

Démonstration. - Soient $x, y \in I'$ et $a_i, b_j \in A$ tels que $x^2 + \sum a_i^2 \in I$, $y^2 + \sum b_j^2 \in I$. Si $z \in A$, alors $(zx)^2 + \sum (za_i)^2 \in z^2 I \subseteq I$, donc $zx \in I'$. De même,

$$(x + y)^2 + (x - y)^2 + 2 \sum a_i^2 + 2 \sum b_j^2 \in I ,$$

donc $x - y \in I'$. Ceci montre que I' est un idéal de A ; en outre, $I \subseteq I'$.

Si $x \in \sqrt{I'}$, alors il existe un entier $m \geqslant 1$ tel que $x^m \in I'$; donc il existe des éléments $a_i \in A$, tels que $x^{2m} + \sum a_i^2 \in I$. Si P est un idéal réel premier contenant I, alors $x^m \in P$, donc $x \in P$; ceci implique que $x \in {}^R\sqrt{I}$, et montre l'inclusion $\sqrt{I'} \subseteq {}^R\sqrt{I}$.

Si $\sum a_i^2 \in \sqrt{I'}$ (avec $a_i \in A$), alors il existe un entier $m \geqslant 1$ et des éléments $b_j \in A$ tels que

$$(\sum a_i^2)^{2m} + \sum b_j^2 \in I ;$$

ceci s'écrit sous la forme

$$(a_i^{2m})^2 + \sum c_k^2 \in I \quad (\text{avec } c_k \in A) ,$$

donc $a_i \in \sqrt{I'}$. On en déduit que $\sqrt{I'}$ est un idéal réel.

D'après (B), on déduit que $\sqrt{I'} = {}^R\sqrt{\sqrt{I'}} \supseteq {}^R\sqrt{I}$, car $I' \supseteq I$. Ceci montre que $\sqrt{I'} = {}^R\sqrt{I}$.

Le comportement des idéaux réels par homomorphisme et localisation est facile à décrire.

(D) Soient $A|C$ une C-algèbre, I un idéal de A , $\varphi : A \to A/I$ l'homomorphisme canonique (donc A/I est encore une C-algèbre). Soit J un idéal de A contenant I . Alors J est un idéal réel si, et seulement si, $\varphi(J) = J/I$ est un idéal réel.

Démonstration. - Soit J un idéal réel de A , et soient $0 < p_i \in C$, $a_i \in A$ des éléments tels que $\sum p_i[\varphi(a_i)]^2 = \varphi(b)$ avec $b \in J$. Donc $\varphi(\sum p_i a_i^2 - b) = 0$ et ainsi $\sum p_i a_i^2 - b = c \in I$. Alors $\sum p_i a_i^2 = b + c \in J$. Puisque J est un idéal réel, alors $a_i \in J$ et $\varphi(a_i) \in J/I$, prouvant que $\varphi(J)$ est un idéal réel.

Réciproquement, si $0 < p_i \in C$, $a_i \in A$ sont des éléments tels que

$$\sum p_i a_i^2 = b \in J ,$$

alors

$$\sum p_i[\varphi(a_i)]^2 = \varphi(b) \in J/I .$$

Par hypothèse, $\varphi(a_i) \in J/I$, donc $a_i \in J + I = J$. Ceci montre que J est un idéal réel.

(E) Soient $A|C$ une C-algèbre, S une partie multiplicative de A , et soit $\varphi : A \to S^{-1}A$ l'homomorphisme canonique.

1° Si I est un idéal réel de A , alors $\varphi(I) = S^{-1}I$ est un idéal réel de $S^{-1}A$;

2° Si J' est un idéal réel de $S^{-1}A$, alors $\varphi^{-1}(J')$ est un idéal réel de A ;

3° Q est un idéal réel premier de A , disjoint de S si, et seulement si, $S^{-1}Q$ est un idéal réel premier de $S^{-1}A$.

Démonstration.

1° On suppose que $\sum_i p_i(a_i/s_i)^2 = b/t$, $1 \leqslant i \leqslant \lambda$, avec

$$0 < p_i \in C , \quad s_i , t \in S , \quad a_i \in A , \quad b \in I .$$

Si $s = \prod_i s_i = s_i s_i'$, $1 \leqslant i \leqslant \lambda$, il existe $u \in S$ tel que

$$u^2 t^2(\textstyle\sum_i p_i s_i'^2 a_i^2) = u^2 t s^2 b \in I , \quad 1 \leqslant i \leqslant \lambda .$$

D'après l'hypothèse, uts$_i$! $a_i \in I$, donc $a_i \in S^{-1} I$ pour tout indice i. Ainsi, $S^{-1} I$ est un idéal réel.

2° Soit $\varphi(\sum_i p_i a_i^2) = b \in J'$ $(1 \leqslant i \leqslant s)$ avec $0 < p_i \in C$, $a_i \in A$. Alors $\varphi(a_i) \in J'$ pour tout indice i, car J' est un idéal réel. Ceci montre que $\varphi^{-1}(J')$ est un idéal réel.

3° Ceci résulte des propriétés 1°, 2° et des faits bien connus sur la localisation des idéaux premiers.

6. Quelques compléments.

On indiquera des résultats de nature variée pour le cas où $A = k[X] = k[X_1, \ldots, X_n]$, k étant un corps ordonné.

(A) Sur le radical réel - Soit $\overline{k}$ une clôture réelle de k. Sur

$$k[X] = k[X_1 , \ldots , X_n] ,$$

on définit la relation suivante :

$f \lesssim g$ signifie que, si $x = (x_1 , \ldots , x_n) \in \overline{k}^n$, alors $f(x) \leqslant g(x)$.

On vérifie sans difficulté que $\lesssim$ est un ordre sur $k[X]$ qui prolonge l'ordre donné sur k. Il est compatible avec les opérations. Si $n > 0$, cet ordre n'est pas total (par exemple, il est faux que $X_1 \gtrsim 0$ ou $-X_1 \gtrsim 0$).

On rappelle que si E est un ensemble ordonné, un sous-ensemble C de E est convexe lorsque la propriété suivante est satisfaite : Si $c_1 , c_2 \in C$, si $c \in E$ et $c_1 \leqslant c \leqslant c_2$, alors $c \in C$.

Toute intersection d'ensembles convexes de E est encore un ensemble convexe. Donc, si S est un sous-ensemble de E, il existe le plus petit sous-ensemble convexe contenant S ; il est noté $\langle S \rangle$, et consiste en des éléments $c \in E$ tels qu'il existe $c_1 , c_2 \in S$ satisfaisant $c_1 \leqslant c \leqslant c_2$.

(a) Soient $k[X]$ muni de l'ordre considéré ci-dessus, et I un idéal de $k[X]$. Soit $I' = \{f \in k[X] \mid$ il existe $q \in I$ tel que si $x \in \overline{k}^n$, alors $|f(x)| \leqslant q(x)\}$. Alors I' est un idéal et $\langle I \rangle = I + I'$, donc $\langle I \rangle$ est un idéal.

Démonstration. - Si $f , f' \in I'$, soient $q , q' \in I$ tels que, si $x \in \overline{k}^n$, alors $|f(x)| \leqslant q(x)$, $|f'(x)| \leqslant q'(x)$. Alors

$$|(f + f')(x)| \leqslant |f(x)| + |f'(x)| \leqslant q(x) + q'(x) \quad \text{avec} \quad q + q' \in I .$$

Donc $f + f' \in I'$.

De même, si $f \in I'$, alors $-f \in I'$.

Si $g \in k[X]$ et $f \in I'$, alors

$$|g(x).f(x)| \leqslant |g(x)|.q(x) \leqslant [1 + g(x) + (g(x))^2].q(x) = q(x) + g(x).q(x) + g^2(x).q(x).$$

Or, $q + gq + g^2 q \in I$, donc $gf \in I'$.

Ceci montre que I' est un idéal.

On montrera maintenant que $\langle I \rangle = I + I'$. Si $f \in \langle I \rangle$, il existe des éléments q_1, $q_2 \in I$ telq que $q_1(x) \leqslant f(x) \leqslant q_2(x)$ pour tout $x \in \overline{k}^n$. Donc

$$0 \leqslant (f - q_1)(x) \leqslant (q_2 - q_1)(x) \quad \text{et} \quad |(f - q_1)(x)| \leqslant (q_2 - q_1)(x)$$

pour tout $x \in \overline{k}^n$. Alors $f - q_1 \in I'$, donc $f \in I + I'$.

D'autre part, si $f = q + q'$ avec $q \in I$ et $q' \in I'$, il existe $g \in I$ tel que $|q'(x)| \leqslant g(x)$ pour tout $x \in \overline{k}^n$. Alors

$$-g(x) \leqslant q'(x) \leqslant g(x) \quad \text{et} \quad (q - g)(x) \leqslant (q + g')(x) \leqslant (q + g)(x)$$

pour tout $x \in \overline{k}^n$. Or, $q - g$, $q + g \in I$, donc $f = q + q' \in \langle I \rangle$. Ceci termine la démonstration.

Il est bon de noter que I n'est pas nécessairement contenu dans I' ; toutefois le carré de tout élément de I est dans I'.

(b) <u>Si</u> I <u>est un idéal de</u> $k[X]$, <u>alors</u> $\sqrt[R]{I} = \sqrt{I'} = \sqrt{\langle I \rangle}$.

<u>Démonstration</u>. - Soit $f \in \sqrt[R]{I}$; il existe un entier $m \geqslant 1$ et

$$s = 1 + \sum_i p_i (a_i/b_i)^2 , \quad 1 \leqslant i \leqslant \ell$$

(avec $0 < p_i \in k$, a_i, $b_i \in k[X]$ tels que $f^m s = q \in I$. En prenant le carré, et en notant que s^2 est du même type que s, on peut supposer m pair et $q(x) \geqslant 0$ pour tout $x \in \overline{k}^n$. Donc $|f^m(x)| \leqslant q(x)$ pour tout $x \in \overline{k}^n$. C'est évident lorsque $f(x) = 0$. Si $f(x) \neq 0$, alors $s = (f^m s)/f^m$ est définie en x et $|f^m(x)| = f^m(x) \leqslant f^m(x)[1 + \sum(a_i(x)/b_i(x))^2] = q(x)$ (voir la démonstration du § 4, (B)). Donc $f^m \in I'$ et $f \in \sqrt{I'}$.

D'après (a), on a $\sqrt{I'} \subseteq \sqrt{\langle I \rangle}$. Soit $f \in \sqrt{\langle I \rangle}$, donc il existe un entier $m \geqslant 1$ tel que $f^m = q + q'$ avec $q \in I$, $q' \in I'$. Alors $f^{2m} = q^2 + 2qq' + q'^2 \in I'$ (car le carré d'un élément de I est dans I'). Ainsi il existe un entier pair ℓ et $g \in I$ tels que $0 < f^\ell(x) = |f^\ell(x)| \leqslant g(x)$ pour tout $x \in \overline{k}^n$.

Soit $s = g/f^\ell$, donc $s - 1 = (g - f^\ell)/f^\ell$ et si $f(x) \neq 0$, alors

$$(s - 1)(x) = \frac{g(x) - f^\ell(x)}{f^\ell(x)} \geqslant 0 .$$

D'après le § 2, (E), on a $s - 1 = \sum p_i (a_i/b_i)^2$ avec $0 < p_i \in k$ et a_i, $b_i \in k[X]$. Ceci montre que $f \in \sqrt[R]{I}$.

Les idéaux premiers réels admettent la caractérisation suivante :

(c) Soit P un idéal premier de $k[X]$, soit x_i l'image canonique de X_i $(i = 1, \dots, n)$ par l'homomorphisme $\varphi : k[X] \to k[X]/P = k[X]$. Alors les conditions suivantes sont équivalentes :

1° P est un idéal réel ;

2° Il existe des ordres totaux compatibles sur $k[X]$ et $k[x]$, prolongeant l'ordre de k, tels que φ préserve l'ordre ;

3° Il existe un ordre total compatible sur $k[X]$, prolongeant l'ordre de k et tel que P soit convexe.

Démonstration.

1° $\to$ 2° : Soient $x = (x_1, \dots, x_n)$ et $k[x] = k[x_1, \dots, x_n]$. $k[x]$ est est une k-algèbre réelle intègre, car P est un idéal réel premier. Il existe donc un ordre sur F prolongeant celui de k (§ 2, (A)). On considère, sur le corps $F(X) = F(X_1, \dots, X_n) = F(X_1 - x_1, \dots, X_n - x_n)$, un ordre total compatible, prolongeant l'ordre de F, tel que $0 < X_i - x_i$ et que $X_i - x_i$ soit infiniment plus petit que tout élément de F (§ 2, (i)). Sur l'anneau $k[X]$, on considère l'ordre induit par celui de $F(X)$.

Si $f \in k[X] \subseteq F[X]$, on peut écrire son développement de Taylor, par rapport à $X_1 - x_1, \dots, X_n - x_n$,

$$f = a + \Sigma_i f_i(X_i - x_i), \quad 1 \leqslant i \leqslant n,$$

avec $a \in F$, $f_i \in F[X_1 - x_1, \dots, X_n - x_n]$.

Soit $\tilde{\varphi} = F[X] \to F[x]$ l'extension naturelle de φ à $F[X]$; alors

$$\varphi(f) = \tilde{\varphi}(f) = a .$$

Si f est positif selon l'ordre de $k[X]$, il est positif selon l'ordre de $F(X)$. Or $X_i - x_i$ est infiniment plus petit que tout élément positif de F. Donc

$$\Sigma_i f_i(X_i - x_i), \quad 1 \leqslant i \leqslant n$$

est infiniment plus petit que $a \in F$, et alors $a = \varphi(f) > 0$. Ceci montre que φ préserve l'ordre.

2° $\to$ 3° : Puisque φ est un homomorphisme de $k[X]$ sur $k[x]$, préservant l'ordre, alors son noyau P est un idéal convexe de $k[X]$.

3° $\to$ 1° : L'anneau $k[x] \cong k[X]/P$ peut être ordonné, en posant $\varphi(f) \geqslant 0$ si, et seulement si, $f \geqslant 0$ dans $k[X]$.

Il est immédiat que cette relation est bien définie ; il s'agit d'un ordre total

compatible sur $k[x]$ prolongeant l'ordre sur k . Ainsi, $k[x]|k$ est une algèbre réelle, donc P est un idéal réel.

(B) Rapports entre les ensembles algébriques de k^n et de $\tilde{k}^n$. - Soient k un corps ordonné maximal, et $\tilde{k}$ sa clôture algébrique, donc $\tilde{k} = k(i)$, où $i^2 = -1$.

Si $x = a + ib \in \tilde{k}$ (avec a , $b \in k$), on note $\overline{x} = a - ib$ le conjugué de x . Si $x = (x_1 , \dots , x_n) \in \tilde{k}^n$, on note $\overline{x} = (\overline{x}_1 , \dots , \overline{x}_n) \in \tilde{k}^n$ le conjugué de x. On a $x \in k^n$ si, et seulement si, $\overline{x} = x$.

Si $f \in \tilde{k}[X_1 , \dots , X_n]$, on note $\overline{f}$ le polynôme dont les coefficients sont les conjugués de ceux de f . On a $f = \overline{f}$ si, et seulement si, f a ses coefficients dans k . Alors $\overline{f}(x) = f(\overline{x})$ pour tout $x \in \tilde{k}^n$.

Soit $f^* = \frac{1}{2}(f + \overline{f})$; alors $f^* \in k[X_1 , \dots , X_n]$ et $f = f^* - i(if)^*$.

On indiquera des relations entre les ensembles algébriques de k^n et de $\tilde{k}^n$. Le premier résultat est dû à WHITNEY [7].

(d) Soit I un idéal de $k[X]$. Alors

$$\mathrm{Id}_{\tilde{k}}(V_k(I)) = \mathrm{Id}_{\tilde{k}}\, V_{\tilde{k}}(\mathrm{Id}_k\, V_k(I)) = \mathrm{Id}_{\tilde{k}}\, V_{\tilde{k}}(\sqrt[R]{I}) \quad \text{et} \quad V_{\tilde{k}}(\mathrm{Id}_k\, V_k(I))$$

est le plus petit $\tilde{k}$-ensemble algébrique de $\tilde{k}^n$ contenant $V_k(I)$.

Démonstration. - De $V_k(I) \subseteq V_{\tilde{k}}(\mathrm{Id}_k\, V_k(I))$ vient

$$\mathrm{Id}_{\tilde{k}}(V_k(I)) \supseteq \mathrm{Id}_{\tilde{k}}\, V_{\tilde{k}}(\mathrm{Id}_k\, V_k(I)) .$$

D'autre part, soient $f \in \mathrm{Id}_{\tilde{k}}(V_k(I))$ et $x \in V_{\tilde{k}}(\mathrm{Id}_k\, V_k(I))$, il s'agit de montrer que $f(x) = 0$.

Si $y \in V_k(I)$, on a $f(y) = 0$, donc $\overline{f}(y) = \overline{f(\overline{y})} = \overline{f(y)} = 0$. Il en résulte que $f^*(y) = 0$, donc $f^* \in \mathrm{Id}_k\, V_k(I)$, et alors $f^*(x) = 0$.

De même, on a $if \in \mathrm{Id}_{\tilde{k}}(V_k(I))$, donc $(if)^*(x) = 0$. Alors

$$f(x) = f^*(x) - i(if)^*(x) = 0 .$$

Ceci montre que $\mathrm{Id}_{\tilde{k}}(V_k(I)) = \mathrm{Id}_{\tilde{k}}\, V_{\tilde{k}}(\mathrm{Id}_k\, V_k(I)) = \mathrm{Id}_{\tilde{k}}\, V_{\tilde{k}}(\sqrt[R]{I})$, la dernière égalité résultant du théorème de Dubois, car k est égal à sa clôture réelle.

On a $V_{\tilde{k}}(\mathrm{Id}_k\, V_k(I)) \supseteq V_k(I)$. Si $V_{\tilde{k}}(I') \supseteq V_k(I)$ (où I' est l'idéal de $\tilde{k}[X]$, alors

$$\mathrm{Id}_{\tilde{k}}(V_{\tilde{k}}(I')) \subseteq \mathrm{Id}_{\tilde{k}}(V_k(I)) = \mathrm{Id}_{\tilde{k}}\, V_{\tilde{k}}(\mathrm{Id}_k\, V_k(I)) ,$$

donc $V_{\tilde{k}}(I') \supseteq V_{\tilde{k}}(\mathrm{Id}_k\, V_k(I))$.

Comme corollaire, on a le résultat suivant.

(e) Soit I un idéal de $k[X]$. Les affirmations suivantes sont équivalentes :

1° $V_k(I)$ est dense dans $V_{\tilde{k}}(I)$, selon la topologie de Zariski de $\tilde{k}^n$;

2° $Id_{\tilde{k}}(V_k(I)) = Id_{\tilde{k}}(V_{\tilde{k}}(I))$;

3° ${}^R\sqrt{I} = \sqrt{I}$;

4° Tout idéal premier minimal contenant I est réel.

Démonstration.

1° $\rightarrow$ 2° : Si $V_k(I)$ est dense dans $V_{\tilde{k}}(I)$ selon la topologie de Zariski de $\tilde{k}^n$, alors $V_{\tilde{k}}(I)$ est le plus petit $\tilde{k}$-ensemble algébrique de $\tilde{k}^n$ contenant $V_k(I)$. D'après (d), on a

$$V_{\tilde{k}}(I) = V_{\tilde{k}}(Id_k\, V_k(I)) ;$$

donc

$$Id_{\tilde{k}}(V_{\tilde{k}}(I)) = Id_{\tilde{k}}\, V_{\tilde{k}}(Id_k\, V_k(I)) = Id_{\tilde{k}}(V_k(I)) .$$

2° $\rightarrow$ 3° : D'après (d) et l'hypothèse

$$Id_{\tilde{k}}\, V_{\tilde{k}}({}^R\sqrt{I}) = Id_{\tilde{k}}\, V_{\tilde{k}}(Id_k\, V_k(I)) = Id_{\tilde{k}}(V_k(I)) = Id_{\tilde{k}}(V_{\tilde{k}}(I)) .$$

Il en résulte que $Id_{\tilde{k}}\, V_{\tilde{k}}({}^R\sqrt{I}.\tilde{k}[X]) = Id_{\tilde{k}}\, V_{\tilde{k}}(I.\tilde{k}[X])$, et, d'après le théorème des zéros de Hilbert (car $\tilde{k}$ est algébriquement clos),

$${}^R\sqrt{I} = \sqrt{{}^R\sqrt{I}} \subseteq \sqrt{\tilde{k}[X].{}^R\sqrt{I} \cap k[X]} = \sqrt{\tilde{k}[X].I \cap k[X]} \subseteq \sqrt{\tilde{k}[X].I \cap k[X]} .$$

Il résultera de (f) ci-dessous que $\tilde{k}[X].I \in k[X] = I$. Donc ${}^R\sqrt{I} \subseteq \sqrt{I}$, d'où l'égalité.

3° $\rightarrow$ 4° : Ceci a été démontré au § 5, (P).

3° $\rightarrow$ 1° : D'après (d), $V_k(I)$ est dense dans $V_{\tilde{k}}({}^R\sqrt{I}) = V_{\tilde{k}}(\sqrt{I}) = V_{\tilde{k}}(I)$ selon la topologie de Zariski de $\tilde{k}^n$.

(f) Soient $K|F$ une extension algébrique, et I un idéal de $F[X] = F[X_1,\ldots,X_n]$. Alors $K[X].I \cap F[X] = I$.

Démonstration. - Il suffit de montrer une inclusion, l'autre étant évidente. Soit $\{q_1 , \ldots , q_n\}$ un ensemble de générateurs de l'idéal I.

Si $f \in K[X].I \cap F[X]$, on peut écrire

$$f = \sum_i u_i\, q_i , \quad 1 \leq i \leq r , \text{ avec } u_i \in K[X] , \quad q_i \in I .$$

Soit F' le sous-corps de K engendré par les coefficients des polynômes u_i $(i = 1 , \ldots , r)$. Donc $F'|F$ est une extension de degré fini ; soit $\{w_1,\ldots,w_s\}$ une base de $F'|F$, avec $w_1 = 1$. Alors on peut écrire

$$u_i = \sum_j f_{ji}\, w_j \qquad (i = 1 , \dots , r , \quad j = 1 , \dots , s)$$

avec $f_{ji} \in F[X]$, donc

$$f = \sum_i (\sum_j f_{ji}\, w_j)\, q_i = \sum_i f_{1i}\, q_i + (\sum_i f_{2i}\, q_i)\, w_2 + \dots + (\sum_i f_{si}\, q_i)\, w_s$$

avec $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$.

Si $Y = X_1 \dots X_n$ est un monôme quelconque, si c est son coefficient dans f , et si a_j est son coefficient dans $\sum_i f_{ji}\, q_i$, $1 \leqslant i \leqslant r$, alors

$$c = a_1 + a_2\, w_2 + \dots + a_s\, w_s .$$

Puisque $c \in F$, et $\{w_1 , w_2 , \dots , w_s\}$ est une base, alors $c = a_1$, $a_2 = \dots = a_s = 0$. Puisque Y était arbitraire, ceci montre que

$$f = \sum_i f_{1i}\, q_i \in I , \quad 1 \leqslant i \leqslant r .$$

Un autre résultat intéressant est le suivant.

(g) <u>Si</u> P <u>est un idéal premier réel de</u> $k[X]$, <u>alors</u> $\tilde{k}[X].P$ <u>est un idéal premier.</u>

<u>Démonstration.</u> - On peut choisir un système de générateurs $\{f_1 , \dots , f_r\}$ pour l'idéal P , tel que chaque f_i est irréductibe (car P est un idéal premier). En effet, on considère un système de générateurs $\{g_1 , \dots , g_r\}$ de P ; cet idéal étant premier, chaque g_j a un facteur irréductible f_j appartenant à P ; alors $\{f_1 , \dots , f_r\}$ engendre P .

Soient $f , g \in \tilde{k}[X]$ tels que $fg \in \tilde{k}[X].P$ et $f \notin \tilde{k}[X].P$. Puisque $\tilde{k} = k[i]$, on peut écrire $f = a + ib$, $g = c + id$ avec $a , b , c , d \in k[X]$. De même, on peut écrire $fg = \sum_i (u_j + iv_j).f_j = \sum_j u_j f_j + i(\sum v_j f_j)$ avec $u_j , v_j \in k[X]$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant \ell$. Alors

$$\left.\begin{aligned} ac - bd &= \sum_j u_j f_j \in P \\ ad + bc &= \sum_j v_j f_j \in P \end{aligned}\right\} (i \leqslant j \leqslant \ell)$$

Donc

$$ac^2 - bcd \in P \quad \text{et} \quad ad^2 + bcd \in P ,$$

d'où il résulte que $a(c^2 + d^2) \in P$. De même, $b(c^2 + d^2) \in P$.

Puisque $f = a + ib \notin \tilde{k}[X].P$, alors $a \notin P$ ou $b \notin P$. Donc $c^2 + d^2 \in P$.

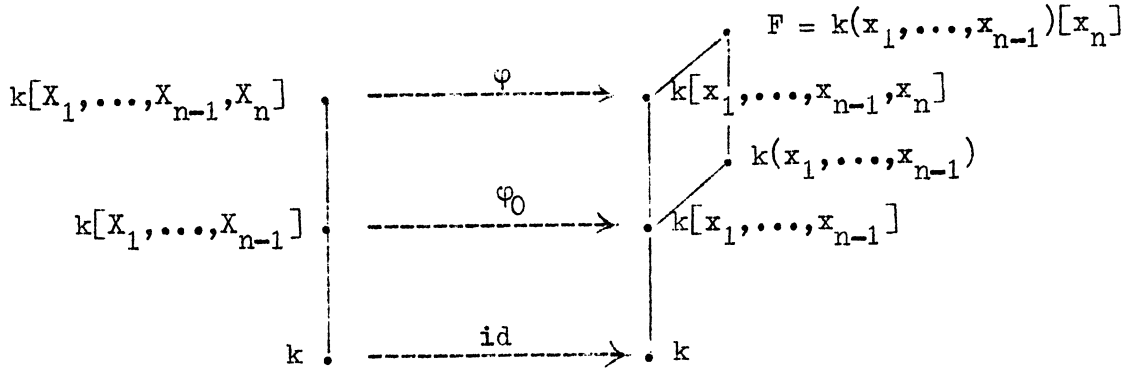
P étant un idéal réel, alors $c , d \in P$, donc $g = c + id \in \tilde{k}[X].P$. Ceci montre que $\tilde{k}[X].P$ est un idéal premier.

(C) Idéaux réels principaux.

Pour conclure, on caractérisera les idéaux réels principaux.

(h) Soient k un corps ordonné, et $g \in k[X_1, \dots, X_n] = k[X]$ un polynôme irréductible. L'idéal principal (g) est réel si, et seulement si, g change de signe en $\overline{k}^n$.

Démonstration. - Soit (g) un idéal réel, donc $k[X]/(g)$ est une k-algèbre intègre et réelle ; sur son de corps de fractions F, il existe un ordre tel que $F|k$ est une extension ordonnée. Etant donné que g est irréductible, on sait que $F|k$ a un degré de transcendance $n-1$. Soit x_i l'image de X_i par l'homomorphisme canonique $\varphi : k[X] \to k[X]/(g)$, donc $F = k(x_1, \dots, x_n)$. Alors, on peut numéroter les indéterminées de façon que $\{x_1, \dots, x_n\}$ soit une base de transcendance de $F|k$. La restriction φ_0 de φ à $k[X_1, \dots, X_n]$ est alors un isomorphisme.



φ_0 s'étend de façon naturelle à un isomorphisme.

$\tilde{\varphi}_0 : k[X_1, \dots, X_{n-1}, X_n] \to k[x_1, \dots, x_{n-1}, X_n]$.

Soit $h = \tilde{\varphi}_0(g) = g(x_1, \dots, x_{n-1}, X_n)$, donc h est encore un polynôme en X_n, irréductible sur $k[x_1, \dots, x_{n-1}]$, donc aussi sur $k(x_1, \dots, x_{n-1})$ (d'après le lemme de Gauss). Alors h n'a pas de racines multiples. Puisque $h(x_n) = \varphi(g) = 0$, alors h a une racine simple dans une clôture réelle $\overline{F}$ de F ; donc h change de signe en $\overline{F}$, c'est-à-dire qu'il existe des éléments $x_n', x_n'' \in \overline{F}$ tels que $h(x_n') < 0 < h(x_n'')$. Ceci signifie que

$$g(x_1, \dots, x_{n-1}, x_n') < 0 < g(x_1, \dots, x_{n-1}, x_n'') ,$$

donc g change de signe en $\overline{F}^n$.

Par conséquent, g et $-g$ ne sont pas des sommes de carrés d'éléments de $\overline{F}(X_1, \dots, X_n)$. Si $\overline{k}$ est une clôture réelle de k, contenue dans $\overline{F}$, alors g et $-g$ ne sont pas des sommes de carrés d'éléments de $\overline{k}(X_1, \dots, X_n)$. D'après le § 2, (E), g change de signe en $\overline{k}^n$. Sinon, g (ou $-g$) serait positive définie sur $\overline{k}^n$, donc $\pm g = \sum_i p_i u_i^2$, $1 \leqslant i \leqslant \ell$, avec $u_i \in \overline{k}(X_1, \dots, X_n)$,

$0 < p_i \in \overline{k}$; or $p_i = q_i^2$ avec $0 < q_i \in \overline{k}$, car tout élément positif de $\overline{k}$ est un carré, donc

$$\pm g = \Sigma_i (q_i\, u_i)^2 \ , \quad 1 \leqslant i \leqslant \ell \ ,$$

ce qui est une contradiction.

Réciproquement, soit g un polynôme irréductible qui change de signe en $\overline{k}^n$.

On suppose d'abord que $n = 1$. Alors g est le produit de facteurs linéaires ou quadratiques irréductibles à coefficients dans $\overline{k}$; les facteurs quadratiques ne changent pas de signe en $\overline{k}$. Donc g a un facteur linéaire en $\overline{k}[X]$, c'est-à-dire qu'il existe $x \in \overline{k}$ tel que $g(x) = 0$.

Le k-homomorphisme $\varphi : k[X] \to k[x]$ tel que $\varphi(X) = x$ a le noyau égal à (g) ; donc $k[X]/(g) \cong k[x] \subseteq \overline{k}$, et ceci montre que l'idéal (g) est réel.

Maintenant, soit $n > 1$; on procède par récurrence sur n . Par hypothèse, il existe des éléments x , $x' \in \overline{k}^n$ tels que $g(x') < 0 < g(x)$. Par un changement linéaire de coordonnées, on peut supposer que

$$x = (0 \ , \ x_2 \ , \ \dots \ , \ x_n) \ , \quad x' = (0 \ , \ x_2' \ , \ \dots \ , \ x_n') \ .$$

On peut considérer sur le corps $\overline{k}(X_1 \ , \ \dots \ , \ X_n)$ un ordre qui prolonge celui de $\overline{k}$ et tel que $0 < X_1 \leqslant a$ pour tout élément $a \in \overline{k}$, $0 < a$ (d'après § 2, (i)).

Soient $h = g(X_1 \ , \ x_2 \ , \ \dots \ x_n) \in \overline{k}[X_1]$ et $h' = g(X_1 \ , \ x_2' \ , \ \dots \ , \ x_n') \in \overline{k}[X_1]$. Si $h = a_m X_1^m + a_{m-1} X_1^{m-1} + \dots + a_0$ (avec $a_i \in \overline{k}$), alors

$$a_0 = h(0) = g(0 \ , \ x_2 \ , \ \dots \ , \ x_n) > 0 \ ;$$

en outre $a_i X_1^i \leqslant a_0$ (pour tout $i = 1 \ , \ \dots \ , \ m$) , donc $h > 0$ dans $\overline{k}(X_1)$. De même, $h' < 0$ dans $\overline{k}(X_1)$. Puisque $k[X_1 \ , \ \dots \ , \ X_n] \cong k[X_1][X_2 \ , \ \dots \ , \ X_n]$, on peut considérer le polynôme $f \in k[X_1][X_2 \ , \ \dots \ , \ X_n]$, qui correspond à g par cet isomorphisme canonique.

D'après le lemme de Gauss, f est irréductible sur le corps $k(X_1)$ (car g est irréductible en $k[X_1 \ , \ X_2 \ , \ \dots \ , \ X_n]$). En outre,

$$k[X_1 \ , \ \dots \ , \ X_n]/(g) \cong k[X_1][X_2 \ , \ \dots \ , \ X_n]/(f) \subseteq k(X_1)[X_2, \ \dots \ , \ X_n]/(f)$$

et

$$f(x_2 \ , \ \dots \ , \ x_n) = g(X_1 \ , \ x_2 \ , \ \dots \ , \ x_n) = h > 0 \quad \text{en} \quad \overline{k}(X_1) \ ,$$

tandis que $f(x_2' \ , \ \dots \ , \ x_n') = g(X_1 \ , \ x_2' \ , \ \dots \ , \ x_n') = h' < 0$ en $\overline{k}(X_1)$.

A un isomorphisme d'ordre près, une clôture réelle $\overline{k(X_1)}$ de $k(X_1)$ contient $\overline{k}$, donc $\overline{k}(X_1)$; alors f change de signe en $\overline{k(X_1)}$.

D'après l'hypothèse de récurrence, (f) est un idéal réel de $k(X_1)[X_2 \ , \ \dots \ , \ X_n]$ c'est-à-dire que $k(X_1)[X_2 \ , \ \dots \ , \ X_n]/(f)$ est une $k(X_1)$-algèbre réelle ; alors

$k(X_1)[X_2 , \ldots , X_n]/(f)$ est aussi une k-algèbre réelle, donc $k[X_1 , \ldots , X_n]/(g)$ est une k-algèbre réelle, ce qu'il fallait démontrer.

Pour des polynômes réductibles, on a le résultat suivant.

(i) Soit $f \in k[X_1 , \ldots , X_n]$ un polynôme unitaire. L'idéal principal (f) est réel si, et seulement si, $f = f_1 f_2 \ldots f_m$, où chaque f_i est unitaire irréductible, (f_i) est réel, et $f_i \neq f_j$ (pour $i \neq j$).

Démonstration. - Si (f) est réel, alors $(f) \subseteq \sqrt{(f)} \subseteq {}^R\sqrt{(f)} = (f)$. D'après le § 5, (B), tout idéal premier minimal contenant (f) est réel. Si $f_1 , \ldots , f_m$ sont les différents facteurs irréductibles unitaires de f, alors

$$(f) = \sqrt{(f)} = (f_1) \cap \ldots \cap (f_m) = (f_1 f_2 \ldots f_m) ,$$

donc $f = f_1 f_2 \ldots f_m$, et (f_i) est réel.

Réciproquement, $(f) = (f_1 f_2 \ldots f_m) = (f_1) \cap (f_2) \cap \ldots \cap (f_m) = \sqrt{(f)}$. Mais, d'après le § 5 (B), ${}^R\sqrt{(f)} = \sqrt{(f)}$, donc (f) est réel.

BIBLIOGRAPHIE

[1] DUBOIS (D. W.). - A Nullstellensatz for ordered fields, Arkiv för Mat., Stockholm, t. 8, 1969-1970, p. 111-114.

[2] DUBOIS (D. W.) and EFROYMSON (G.). - Algebraic theory of real varieties, I., Studies and essays presented to Yu Why Chen on his 60th birthday, p. 107-135. - Taipei, Academia Sinica, 1970.

[3] JACOBSON (Nathan). - Lectures in abstract algebra, Vol. 3. - Princeton, D. Van Nostrand Company, 1964 (University Series in higher Mathematics).

[4] LANG (Serge). - Algebra. - Reading, Addison-Wesley publishing Company, 1965 (Addison-Wesley Series in Mathematics).

[5] RIBENBOIM (Paulo). - L'arithmétique des corps. - Paris, Hermann, 1972.

[6] RISLER (J.-J.). - Une caractérisation des idéaux des variétés algébriques réelles, C. R. Acad. Sc. Paris, t. 271, 1970, Série A, p. 1171-1173.

[7] WHITNEY (H.). - Elementary structure of real algebraic varieties, Annals of Math., Series 2, t. 66, 1957, p. 545-556.

(Texte reçu le 9 septembre 1971)

Paulo RIBENBOIM
Queen's University
Department of Mathematics
KINGSTON, Ont. (Canada)