Andrej Schinzel

Le nombre de zéros des polynômes dans les anneaux de valuation des corps complets valués discrètement

Groupe de travail d'analyse ultramétrique, tome 9, n° 1 (1981-1982), exp. n° 6, p. 1-12

<http://www.numdam.org/item?id=GAU_1981-1982__9_1_A4_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
9e année, 1981/82, n° 6, 12 p.

23 novembre 1981

LE NOMBRE DE ZÉROS DES POLYNÔMES DANS LES ANNEAUX DE VALUATION DES CORPS COMPLETS VALUÉS DISCRÈTEMENT

par Andrej SCHINZEL (*)
[Varsovie]

Soit $\underset{\sim}{K}$ un corps complet par rapport à une valuation discrète v, et soit $\underset{\sim}{I}$ l'anneau de valuation, $\underset{\sim}{P}$ l'idéal de valuation, $\underset{\sim}{R}$ le corps résiduel $\underset{\sim}{I}/\underset{\sim}{P}$, p un élément de $\underset{\sim}{P}$ avec $v(p) = 1$.

Par une généralisation facile d'un résultat de NAGELL ([2], p. 349 ; voir aussi [3], th. 53), on démontre que le nombre de zéros dans $\underset{\sim}{I}$ d'un polynôme $f \in \underset{\sim}{I}[x]$, de discriminant, $\operatorname{disc} f \neq 0$ est égal au nombre de solution de la congruence

$$f(x) \equiv 0 \pmod{\underset{\sim}{P}^{2\delta+1}}, \text{ où } \delta = v(\operatorname{disc} f) .$$

Cependant, pour les équations binômes, il y a une formule plus simple : Si $f(x) = x^n - a$, et si on pose $\alpha = v(a)$, alors

$$\operatorname{card}\{\xi \in \underset{\sim}{I} ; \ f(\xi) = 0\} = \begin{cases} 0 & \text{si } \alpha \not\equiv 0 \mod n , \\ \operatorname{card}\{\eta \in \underset{\sim}{R} ; \ \eta^n = \overline{ap^{-\alpha}}\} & \text{si } \alpha \equiv 0 \mod n , \end{cases}$$

où la barre désigne le résidu $\mod \underset{\sim}{P}$.

Or, dans le cas général, il y a un résultat analogue pourvu que $\operatorname{car} \underset{\sim}{R} > \deg f$ ou que $\operatorname{car} \underset{\sim}{R} = 0$. Pour le formuler, on pose, pour tout polynôme $A \in \underset{\sim}{K}[y_1, \ldots, y_\ell]$,

$$A = \sum_{\mu=1}^{m} a_\mu \prod_{\lambda=1}^{\ell} y_\lambda^{\alpha_{\mu\lambda}}$$

(où les vecteurs $[\alpha_{\mu 1}, \ldots, \alpha_{\mu\ell}]$ sont distincts) :

$$v(A) = \min_{\mu \leq m} v(a_\mu) ,$$

$$\varkappa A = \begin{cases} p^{-v(A)} A & \text{si } A \neq 0 , \\ 0 & \text{si } A = 0 , \end{cases}$$

(*) Texte reçu le 21 juin 1982.

Andrej SCHINZEL, 12 m 24 ul. Brzozowa, PL-00286 WARSZAWA (Pologne).

et, si $A \in \underset{\sim}{I}[y_1 , \dots , y_\ell]$,

$$\mathfrak{L} A = \sum_{\mu=1}^{m} \bar{a}_\mu \prod_{\lambda=1}^{\ell} y_\lambda^{\alpha_{\mu\lambda}} .$$

En outre, on pose

$$\underset{\sim}{N}_+ := \underset{\sim}{N} \cup \{0 , \infty\} = \underset{\sim}{N}_0 \cup \{\infty\} = \{0 , 1 , \dots , \infty\} .$$

Maintenant on peut énoncer le théorème suivant.

THÉORÈME 1. - Pour tout $m \in \underset{\sim}{N}$, il existe un système de formes $R_i(a)$ $(i \leqslant i^*)$ et de polynômes $S_{jk\ell}(a , y_1 , \dots , y_\ell)$ $(j \leqslant j^* , \ k \leqslant k_j , \ \ell \leqslant \ell_{jk})$ à coefficients entiers, une décomposition

$$\underset{\sim}{N}_+^{i^*} = \bigcup_{j=1}^{j^*} \underset{\sim}{X}_j$$

et des fonctions $\sigma_{jk\ell}(v) : \underset{\sim}{X}_j \longrightarrow \underset{\sim}{N}_0$ qui ont les propriétés suivantes. Si car $\underset{\sim}{R} = 0$ ou si car $\underset{\sim}{R} > m$, si

$$f(x) = \sum_{\mu=0}^{m} a_\mu x^{m-\mu} \in \underset{\sim}{K}[x] , \quad f \neq 0 , \quad \underset{\sim}{a} = [a_0 , \dots , a_m] ,$$

$$\underset{\sim}{v} = [v(R_1(\underset{\sim}{a})) , \dots , v(R_{i^*}(\underset{\sim}{a}))] \in \underset{\sim}{X}_j$$

et

$$\tilde{S}_{jk\ell}(y_1 , \dots , y_\ell) = \mathfrak{L} \kappa S_{jk\ell}(\underset{\sim}{a} , p^{\sigma_{jk1}(v)} y_1 , \dots , p^{\sigma_{jk\ell}(v)} y_\ell) ,$$

alors

$$\begin{aligned} &\operatorname{card}\{\xi \in \underset{\sim}{I} ; \quad f(\xi) = 0\} \\ &\qquad = \sum_{k=1}^{k_j} \operatorname{card}\{[\eta_1 , \eta_2 , \dots] \in \underset{\sim}{R}^{\ell_{jk}} ; \quad \Lambda_{\ell=1}^{\ell_{jk}} \tilde{S}_{jk\ell}(\eta_1 , \dots , \eta_\ell) = 0\} . \end{aligned}$$

Les polynômes R_i , $S_{jk\ell}$, les ensembles $\underset{\sim}{X}_j$, et les fonctions $\sigma_{jk\ell}$ ne dépendent pas du corps $\underset{\sim}{K}$, de la valuation v , ni de l'élément p .

Le théorème 1 entraîne facilement le théorème suivant.

THEOREME 2. - Pour tout $m \in \underset{\sim}{N}$, il existe $c_1(m) \in \underset{\sim}{N}$ et $c_2(m) \in \underset{\sim}{N}$ tels que, si $F \in \underset{\sim}{Z}[x , t]$ est de degré n par rapport à x et si on note $\ell(F)$ la somme des valeurs absolues de ses coefficients, alors, pour tous les nombres premiers p plus grands que $c_1(m) \ \ell(F)^{c_2(m)}$, on a

$$\operatorname{card}\{\xi \in \underset{\sim}{Z}_p \; ; \; F(\xi , p) = 0\} = \operatorname{card}\{\xi \in \underset{\sim}{F}_p[[t]] \; ; \; F(\xi , t) = 0\} ,$$

où $\underset{\sim}{Z}_p$ est l'anneau des entiers p-adiques, et $\underset{\sim}{F}_p$ le corps fini à p éléments.

Pour comprendre les deux théorèmes, il faut remarquer que les valeurs d'un polynôme, à coefficients entiers pour des arguments dans un corps de caractéristique positive, sont dans ce corps, un entier positif n étant interprété comme $1+1+\dots+1$ (n fois).

L'égalité affirmée dans le théorème 2, restreinte aux nombres premiers p plus grands qu'une fonction primitivement récursive convenable des coefficients de F, résulte d'un théorème de P. COHEN [1]. Son résultat (théorème 5.1) montre aussi que dans la situation plus générale du théorème 1 la résolubiblité de l'équation $f(x) = 0$ dans $\underset{\sim}{I}$ est décidable en termes de $\underset{\sim}{R}$ pourvu que car $\underset{\sim}{R}$ soit ou zéro, ou plus grande qu'une borne dépendant de f.

La démonstration du théorème 1 est compliquée, et nous ne donnons que les définitions et les lemmes principaux avec un schéma des implications. Même eux exigent beaucoup de notations.

Pour un polynôme $f = \sum_{\mu=0}^{m} a_\mu x^{m-\mu}$, $\underset{\sim}{f}$ est le vecteur $[a_0 , \dots , a_m]$. Donc $\underset{\sim}{f}$ est déterminé par f à une suite de zéros précédant le plus haut coefficient près. La longueur de cette suite est claire dans chaque contexte.

Les caractères majuscules ordinaires, sauf Σ , Π , E , désignent des polynômes à plusieurs variables, les caractères minuscules gras désignent des vecteurs, les caractères majuscules gras des ensembles, les caractères majuscules de ronde des opérations.

Enfin on pose

$$\deg 0 = -\infty , \quad \underset{\sim}{N}_- = \underset{\sim}{N}_0 \cup \{-\infty\} .$$

Définition 1. - $\underset{\sim}{C}_\ell(m_1 , m_2 , \dots , m_k)$ est la classe de tous les polynômes $A \in \underset{\sim}{Z}[\underset{\sim}{x}_1 , \underset{\sim}{x}_2 , \dots , \underset{\sim}{x}_k , y_1 , \dots , y_\ell]$ qui sont homogènes par rapport à chacune des variables $\underset{\sim}{x}_i = [x_{i0} , \dots , x_{im_i}]$ séparément, et isobariques par rapport à l'ensemble des variables, le poids de x_{ij} étant j et le poids de y_i étant 1. Le degré de A par rapport à $\underset{\sim}{x}_i$ est noté $\deg^i A$ et le poids commun de tous les termes de A est noté $w(A)$.

LEMME 1. - Si $A \in \underset{\sim}{C}_\ell(m_1 , m_2 , \dots , m_k)$, $B_i \in \underset{\sim}{C}_1(n_1 , \dots , n_r)$ $(1 \leq i \leq k)$, les B_i dépendant formellement des mêmes variables $\underset{\sim}{x}_1 , \dots , \underset{\sim}{x}_r$ et de $y_1 = y$, et si, pour tout i , on a $\deg_y B_i \leq m_i$, alors, pour tout vecteur $[p_1,\dots,p_k] \in \underset{\sim}{N}_0^k$ on a

$$B := A(B_1^{(p_1)} , \dots , B_k^{(p_k)} , y_1 , \dots , y_\ell) \in \underset{\sim}{C}_\ell(n_1 , \dots , n_r) ,$$

où B_i est dérivé par rapport à y, et $B_i^{(p_i)}$ traité comme un polynôme en y. En outre,

$$\deg^q B = \sum_{i=1}^{k} \deg^i A \deg^q B_i \quad (1 \leqslant q \leqslant r) ,$$

$$w(B) = w(A) + \sum_{i=1}^{k} \deg^i A(w(B_i) - m_i - p_i) .$$

Définition 2. - Pour un corps $\underset{\sim}{L}$ et $\alpha \in \underset{\sim}{L} \cup \{\infty\}$, on pose

$$sg_{\underset{\sim}{L}}\, \alpha = \begin{cases} 1 & \text{si } \alpha \neq 0 , \\ 0 & \text{si } \alpha = 0 . \end{cases}$$

Définition 3. - Pour un sous-ensemble $\underset{\sim}{M}$ de $\underset{\sim}{N}_{-}^{k}$, $\Omega(\underset{\sim}{M})$ est la classe de toutes les opérations $\mathfrak{a}$ sur des polynômes à coefficients dans un corps telles que, pour tout vecteur $[m_1 , \ldots , m_k] \in \underset{\sim}{N}_0^k$, il existe des polynômes A_i, $B_i \in \underset{\sim}{C}_0(m_1,\ldots,m_k)$, $C_j \in \underset{\sim}{C}_1(m_1 , \ldots , m_k)$ $(i \leqslant i_0 , \quad j \leqslant j_0)$ et une décomposition

$$\{0 , 1\}^{i_0} = \bigcup_{j=1}^{j_0} \underset{\sim}{S}_j ,$$

qui ont la propriété suivante. Si $\underset{\sim}{L}$ est un corps,

$$f_i \in \underset{\sim}{L}[x] , \quad \deg f_i \leqslant m_i \quad (1 \leqslant i \leqslant k) ,$$

$$[\deg f_1 , \ldots , \deg f_k] \in \underset{\sim}{M} ,$$

$$[sg_{\underset{\sim}{L}}\, A_1(\underset{\sim}{f}_1 , \ldots , \underset{\sim}{f}_k) , \ldots , sg_{\underset{\sim}{L}}\, A_{i_0}(\underset{\sim}{f}_1 , \ldots , \underset{\sim}{f}_k)] \in \underset{\sim}{S}_j ,$$

alors $B_j(\underset{\sim}{f}_1 , \ldots , \underset{\sim}{f}_k) \neq 0$, et

$$\mathfrak{a}(f_1 , \ldots , f_k) = \frac{C_j(\underset{\sim}{f}_1 , \ldots , \underset{\sim}{f}_k , x)}{B_j(\underset{\sim}{f}_1 , \ldots , \underset{\sim}{f}_k)} .$$

Si, pour certains entiers $d_0 , \ldots , d_k$ et pour tous $[m_1 , \ldots , m_k] \in \underset{\sim}{N}_0^k$, $j \leqslant j_0$, on a ou $\underset{\sim}{C}_j = 0$, ou

$$\deg^{\varkappa} C_j - \deg^{\varkappa} B_j = d_{\varkappa} \quad (1 \leqslant \varkappa \leqslant k)$$

et

$$w(C_j) - w(B_j) = d_0 + \sum_{\varkappa=1}^{k} d_{\varkappa}\, m_{\varkappa} ,$$

alors on écrit

$$\alpha \in \Omega(\mathbf{M} \,;\ d_0 , \dots , d_k) .$$

LEMME 2. - *Soit* $\mathbf{M} \subset \mathbf{N}_-^k$, $\mathbf{M}_0 \subset \mathbf{N}_-^\ell$, $\alpha_\lambda \in \Omega(\mathbf{M})$ $(1 \leq \lambda \leq \ell)$, $\alpha_0 \in \Omega(\mathbf{M}_0)$, *et supposons que, pour tout corps* $\mathbf{L}$, *la condition*

$$f_i \in \mathbf{L}[x] , \ [\deg f_1 , \dots , \deg f_k] \in \mathbf{M}$$

entraîne

$$[\deg \alpha_1(\mathbf{f}_1 , \dots , \mathbf{f}_k) , \dots , \deg \alpha_\ell(\mathbf{f}_1 , \dots , \mathbf{f}_k)] \in \mathbf{M}_0 .$$

Alors

$$\alpha_0(\alpha_1 , \dots , \alpha_\ell) \in \Omega(\mathbf{M}) .$$

En outre, si $\alpha_\lambda \in \Omega(\mathbf{M} \,;\ d_{\lambda 0} , \dots , d_{\lambda k})$ $(1 \leq \lambda \leq \ell)$, $\alpha_0 \in \Omega(\mathbf{M}_0 \,;\ d_{00} , \dots , d_{0\ell})$ *alors*

$$\alpha_0(\alpha_1 , \dots , \alpha_\ell) \in \Omega(\mathbf{M} \,;\ d_{00} = \textstyle\sum_{\lambda=1}^{\ell} d_{0\lambda}\, d_{\lambda 0} , \sum_{\lambda=1}^{\ell} d_{0\lambda}\, d_{\lambda 1} , \dots , \sum_{\lambda=1}^{\ell} d_{0\lambda}\, d_{\lambda k}) .$$

LEMME 5. - *Les opérations "quotient incomplet"* $\mathcal{Q}(f , g)$ *et "reste"* $\mathcal{R}(f , g)$ *de la division de* f *par* g *appartiennent respectivement à* $\Omega(\mathbf{N}_- \times \mathbf{N}_0 \,;\ 0 , 1 , -1)$ *et à* $\Omega(\mathbf{N}_- \times \mathbf{N}_0 \,;\ 0 , 1 , 0)$.

Définition 4. - Pour deux polynômes f , g , on pose

$$\mathcal{E}_0(f , g) = f , \quad \mathcal{E}_1(f , g) = g$$

$$\mathcal{E}_{k+1}(f , g) = \begin{cases} \mathcal{E}_{k-1}(f , g) & \text{si } \mathcal{E}_k(f , g) = 0 . \\ \mathcal{R}(\mathcal{E}_{k-1}(f , g) , \mathcal{E}_k(f , g)) & \text{si } \mathcal{E}_k(f , g) \neq 0 . \end{cases}$$

LEMME 6. - $\mathcal{E}_k \in \Omega(\mathbf{N}_-^2 \,;\ 0 , 1 , 0)$ *si* k *est pair, et* $\mathcal{E}_k \in \Omega(\mathbf{N}_-^2 \,;\ 0 , 0 , 1)$ *si* k *est impair*.

LEMME 7. - *Pour tout* $k \geq 1$, *l'opération sur les polynômes*

$$\mathcal{D}_k : [f_1 , \dots , f_k] \longrightarrow \begin{cases} 0 & \text{si } f_1 = f_2 = \dots = f_k = 0 , \\ (f_1 , \dots , f_k) & \textit{autrement} , \end{cases}$$

appartient à $\Omega(\underset{\sim}{N}_{-}^{1})$. Dans le cas $k = 1$, $f_1 \neq 0$, (f_1) désigne le polynôme f_1, divisé par son plus haut coefficient.

LEMME 8. - Pour tout $n \geq 1$, l'opération sur les polynômes

$$\Theta_n f = \begin{cases} \dfrac{(f, \ldots, n f^{(n-1)})(f, \ldots, f^{(n+1)})}{(f, \ldots, f^{(n)})^2} & \text{si } f \neq 0 \\ 0 & \text{si } f = 0 \end{cases}$$

appartient à $\Omega(\underset{\sim}{N}_{-})$.

LEMME 9. - Pour tout corps $\underset{\sim}{L}$ et tout polynôme $f \in \underset{\sim}{L}[x]$ satisfaisant aux conditions $f \neq 0$ et $\operatorname{car} \underset{\sim}{L} = 0$ ou $\deg f < \operatorname{car} \underset{\sim}{L}$, on a

$$\Theta_n f = \prod_{(x-\xi)^n \| f(x), \xi \in \hat{\underset{\sim}{L}}} (x - \xi),$$

où $\hat{\underset{\sim}{L}}$ est la clôture algébrique de $\underset{\sim}{L}$.

Définition 5. - Pour un sous-ensemble $\underset{\sim}{M}$ de $\underset{\sim}{N}_{-}^{k}$, $\Omega^{*}(\underset{\sim}{M})$ est la classe de toutes les opérations $\mathfrak{B}$ sur les polynômes à coefficients dans un anneau de valuation telles que, pour tout vecteur $[m_1, \ldots, m_k] \in \underset{\sim}{N}_0^k$, il existe des polynômes F_i, $G_j \in \underset{\sim}{C}_0(m_1, \ldots, m_k)$ et $H_j \in \underset{\sim}{C}_1(m_1, \ldots, m_k)$ $(i \leq i_0, \ j \leq j_0)$ et une décomposition

$$\underset{\sim}{N}_{+}^{i_0} = \bigcup_{j=1}^{j_0} \underset{\sim}{T}_j$$

avec la propriété suivante :

Si $\underset{\sim}{\tilde{K}}$ est un corps muni d'une valuation discrète $\tilde{v}$, si $\underset{\sim}{\tilde{I}}$ est son anneau de valuation, $\underset{\sim}{\tilde{P}}$ son idéal de valuation et $\tilde{\mathfrak{L}}$ la réduction mod $\underset{\sim}{\tilde{P}}$ des polynômes à coefficients dans $\underset{\sim}{\tilde{I}}$, $f_\varkappa \in \underset{\sim}{\tilde{I}}[x]$, $\deg f_\varkappa \leq m_k$ $(1 \leq \varkappa \leq k)$,

$$[\deg f_1, \ldots, \deg f_k] \in \underset{\sim}{M},$$

$$[\tilde{v}(F_1(\underset{\sim}{f}_1, \ldots, \underset{\sim}{f}_k)), \ldots, \tilde{v}(F_{i_0}(\underset{\sim}{f}_1, \ldots, \underset{\sim}{f}_k))] \in \underset{\sim}{T}_j,$$

alors

$$G_j(\underset{\sim}{f}_1, \ldots, \underset{\sim}{f}_k) \neq 0, \quad \frac{H_j(\underset{\sim}{f}_1, \ldots, \underset{\sim}{f}_k, x)}{G_j(\underset{\sim}{f}_1, \ldots, \underset{\sim}{f}_k)} \in \underset{\sim}{I}[x]$$

et

$$\mathcal{B}(f_1 , \dots , f_k) = \tilde{\mathcal{E}} \frac{H_j(\underset{\sim}{f}_1 , \dots , \underset{\sim}{f}_k , x)}{G_j(\underset{\sim}{f}_1 , \dots , \underset{\sim}{f}_k)} .$$

LEMME 11. - <u>Si</u> $\mathcal{B}_\lambda \in \Omega^*(\underset{\sim}{M})$ $(1 \leq \lambda \leq \ell)$, $\alpha \in \Omega(\underset{\sim}{N}^{\ell})$, <u>alors</u> $\alpha(\mathcal{B}_1,\dots,\mathcal{B}_\ell) \in \Omega^*(\underset{\sim}{M})$.

LEMME 12. - <u>Dans la situation de la définition 5, soit</u> $\tilde{\mathcal{K}}$ <u>l'analogue de l'opération</u> $\mathcal{K}$ <u>défini à l'aide d'un élément</u> $\tilde{p}$ <u>de</u> $\underset{\sim}{\tilde{K}}$ <u>avec</u> $\tilde{v}(\tilde{p}) = 1$. <u>Alors l'opération</u> $\tilde{\mathcal{M}}$ <u>sur les polynômes</u> $f \in \underset{\sim}{K}[x]$, <u>définie par la formule</u>

$$\tilde{\mathcal{M}} f = \begin{cases} \mathcal{D}_1 \tilde{\mathcal{E}} \tilde{\mathcal{K}} f & \text{si } f \neq 0 , \\ 1 & \text{si } f = 0 . \end{cases}$$

<u>appartient à</u> $\Omega^*(\underset{\sim}{N})$ <u>et pour toute opération</u> $\alpha \in \Omega(\underset{\sim}{N}^2)$, <u>l'opération</u> $\tilde{\mathcal{M}}\alpha$ <u>appartient à</u> $\Omega^*(\underset{\sim}{N}^2)$.

LEMME 14. - <u>Soit</u> $f , g \in \underset{\sim}{I}[x]$, $\operatorname{car} \underset{\sim}{R} = 0$ <u>ou</u> $\operatorname{car} \underset{\sim}{R} > \max\{\deg f , \deg g\}$, $\xi \in \underset{\sim}{I}$, $E_\lambda = \tilde{\mathfrak{a}}_\lambda(f , g) \neq 0$ <u>pour</u> $\lambda \leq \ell$, $E_{\ell+1} = 0$,

$$(x - \bar{\xi})^{d_\lambda} \parallel \mathcal{E}\mathcal{K} E_\lambda , \quad d_0 = 1 .$$

<u>Alors si</u> $d_\ell > 0$, <u>on a</u> $g(\xi) = 0$; <u>si</u> $d_\ell = 0$, <u>on a</u> $g(\xi) \neq 0$,

$$g(\xi) \equiv \prod_{\lambda=1}^{\ell} (-1)^{d_{\lambda-1} d} \left(\frac{E_\lambda^{(d_\lambda)}(\xi)}{d_\lambda !}\right)^{d_{\lambda-1}} \left(\frac{E_{\lambda-1}^{(d_{\lambda-1})}(\xi)}{d_{\lambda-1} !}\right) \mod \underset{\sim}{P}^{v(g(\xi))+1}$$

<u>et</u>

$$v(E_\lambda^{(d_\lambda)}(\xi)) = v(E_\lambda) \quad (1 \leq \lambda \leq \ell)$$

<u>Définition</u> 6. - L'opération $\mathcal{M}$ sur les polynômes $f \in \underset{\sim}{K}[x]$ est définie par la formule

$$\mathcal{M} f = \begin{cases} \mathcal{D}_1 \mathcal{E} \mathcal{K} f & \text{si } f \neq 0 , \\ 1 & \text{si } f = 0 . \end{cases}$$

LEMME 15. - <u>Pour des entiers non négatifs quelconques</u> $m , \alpha , n_1 , \dots , n_k$ <u>plus petits que</u> $\operatorname{car} \underset{\sim}{R}$ <u>si</u> $\operatorname{car} \underset{\sim}{R} \neq 0$, <u>il existe des polynômes</u> $f_i , G_{j\upsilon} , H_{j\upsilon}$ $(i \leq i_0 , j \leq j_0 , \upsilon \leq \upsilon_0)$, $K_{j\upsilon\varkappa}$, $L_{j\upsilon\varkappa}$ $(\varkappa \leq k , j \leq j_0 , \upsilon \leq \upsilon_0)$ <u>et une décomposition</u>

$$\underset{\sim}{N}_+^{i_0} = \cup_{j=1}^{j_0} \underset{\sim}{T}_j$$

<u>indépendants de</u> $\underset{\sim}{K}$, v <u>et</u> p <u>qui ont les propriétés suivantes</u>.

$$F_i \, , \, G_{j\upsilon} \in \underset{\sim}{C}_0(m \, , \, m \, , \, n_1 \, , \, \cdots \, , \, n_k) \, , \quad H_{j\upsilon} \in \underset{\sim}{C}_1(m \, , \, m \, , \, n_1 \, , \, \cdots \, , \, n_k) \, ,$$

$$K_{j\upsilon\varkappa} \, , \, L_{j\upsilon\varkappa} \in \underset{\sim}{C}_1(m \, , \, n_k)$$

<u>et ou bien</u> $L_{j\upsilon\varkappa} = 0$, <u>ou bien</u>

$$\deg^1 L_{j\upsilon\varkappa} = \deg^1 K_{j\upsilon\varkappa} \, , \quad \deg^2 L_{j\upsilon\varkappa} = \deg^2 K_{j\upsilon\varkappa} + 1 \, ,$$

$$w(L_{j\upsilon\varkappa}) = w(K_{j\upsilon\varkappa}) + n_\varkappa \, .$$

<u>Si</u> $f_1 \, , \, f_2 \, , \, g_1 \, , \, \cdots \, , \, g_k \in \underset{\sim}{I}[x]$,

$$\deg f_\sigma \leq m \quad (\sigma = 1 \, , \, 2) \, , \quad \deg g_\varkappa \leq n_\varkappa \quad (\varkappa \leq k)$$

$$f_2 \neq 0 \, , \quad \Theta_\alpha \, \mathfrak{M} f_2 \mid \mathfrak{M} f_1 \, , \quad (\Theta_\alpha \mathfrak{M} f_2 \, , \, \frac{\mathfrak{M} f_1}{\Theta_\alpha \mathfrak{M} f_2}) = 1$$

<u>et</u>

$$[v(F_1(\underset{\sim}{f}_1 \, , \, \underset{\sim}{f}_2 \, , \, \underset{\sim}{g}_1 \, , \, \cdots \, , \, \underset{\sim}{g}_k)) \, , \, \cdots \, , \, v(F_{i_0}(\underset{\sim}{f}_1 \, , \, \underset{\sim}{f}_2 \, , \, \underset{\sim}{g}_1 \, , \, \cdots \, , \, \underset{\sim}{g}_k))] \in \underset{\sim}{T}_j \, ,$$

<u>alors</u>

$$G_{j\upsilon}(\underset{\sim}{f}_1 \, , \, \underset{\sim}{f}_2 \, , \, \underset{\sim}{g}_1 \, , \, \cdots \, , \, \underset{\sim}{g}_k) \neq 0 \, , \quad \frac{H_{j\upsilon}(\underset{\sim}{f}_1 \, , \, \underset{\sim}{f}_2 \, , \, \underset{\sim}{g}_1 \, , \, \cdots \, , \, \underset{\sim}{g}_k \, , \, x)}{G_{j\upsilon}(\underset{\sim}{f}_1 \, , \, \underset{\sim}{f}_2 \, , \, \underset{\sim}{g}_1 \, , \, \cdots \, , \, \underset{\sim}{g}_k)} \in \underset{\sim}{I}[x] \, ,$$

$$\Theta_\alpha \, \mathfrak{M} f_2 = \prod_{\upsilon=1}^{\upsilon_0} \mathfrak{L} \, \frac{H_{j\upsilon}(\underset{\sim}{f}_1 \, , \, \underset{\sim}{f}_2 \, , \, \underset{\sim}{g}_1 \, , \, \cdots \, , \, \underset{\sim}{g}_k \, , \, x)}{G_{j\upsilon}(\underset{\sim}{f}_1 \, , \, \underset{\sim}{f}_2 \, , \, \underset{\sim}{g}_1 \, , \, \cdots \, , \, \underset{\sim}{g}_k)} \, ,$$

<u>et si</u> $\xi \in \underset{\sim}{I}$,

$$f_1(\xi) = 0 \, , \quad \varkappa \overline{H_{j\upsilon}(\underset{\sim}{f}_1 \, , \, \underset{\sim}{f}_2 \, , \, \underset{\sim}{g}_1 \, , \, \cdots \, , \, \underset{\sim}{g}_k \, , \, x) \Big|_{x=\xi}} = 0$$

<u>alors, pour tout</u> $\varkappa \leq k$,

$$K_{j\upsilon\varkappa}(f_1 \, , \, g_\varkappa \, , \, \xi) \neq 0 \, , \quad \frac{L_{j\upsilon\varkappa}(\underset{\sim}{f}_1 \, , \, \underset{\sim}{g}_\varkappa \, , \, \xi)}{K_{j\upsilon\varkappa}(\underset{\sim}{f}_1 \, , \, \underset{\sim}{g}_\varkappa \, , \, \xi)} \in \underset{\sim}{I}$$

<u>et</u>

$$g_{\varkappa}(\xi) \equiv \frac{L_{j\cup\varkappa}(\underset{\sim}{f}_1 , \underset{\sim}{g}_{\varkappa} , \xi)}{K_{j\cup\varkappa}(\underset{\sim}{f}_1 , \underset{\sim}{g}_{\varkappa} , \xi)} \mod \underset{\sim}{P}^{v(g_{\varkappa}(\xi))+1}$$

$$(L_{j\cup\varkappa}(\underset{\sim}{f}_1 , \underset{\sim}{g}_{\varkappa} , \xi) = 0 \ \underline{\text{entraîne}} \ g_{\varkappa}(\xi) = 0) .$$

<u>En outre,</u>

$$v(K_{j\cup\varkappa}(\underset{\sim}{f}_1 , \underset{\sim}{g}_{\varkappa} , \xi)) = v(K_{j\cup\varkappa}(\underset{\sim}{f}_1 , \underset{\sim}{g}_{\varkappa} , x)) ,$$

$$v(L_{j\cup\varkappa}(\underset{\sim}{f}_1 , \underset{\sim}{g}_{\varkappa} , \xi)) = v(L_{j\cup\varkappa}(\underset{\sim}{f}_1 , \underset{\sim}{g}_{\varkappa} , x)) .$$

LEMME 17. - <u>Pour tout</u> $m \in \underset{\sim}{N}$, <u>il existe une décomposition</u>

$$\underset{\sim}{N}_+^{m+1} = \bigcup_{r=1}^{r_m} \underset{\sim}{U}_r ,$$

<u>et, pour tout</u> $r \leqslant r_m$, <u>il y a un ensemble fini (éventuellement vide) de fonctions</u> $\pi \langle r , s\rangle : \underset{\sim}{U}_r \longrightarrow \underset{\sim}{N}$ $(1 \leqslant s \leqslant s_r)$ <u>qui ont la propriété suivante</u> : <u>Si</u>

$$f(x) = \sum_{\mu=0}^{m} a_{\mu} x^{m-\mu} \in \underset{\sim}{I}[x] , \quad f \neq 0$$

$$\underset{\sim}{u} = [v(a_0) , \dots , v(a_m)] \in \underset{\sim}{U}_r ,$$

$$h_{rs}(y) = f(p^{\pi\langle r,s\rangle(\underset{\sim}{u})} y) ,$$

<u>alors</u>

$$\operatorname{card}\{\xi \in \underset{\sim}{P} \setminus \{0\} ; \quad f(\xi) = 0\} = \sum_{s=1}^{s_r} \operatorname{card}\{\eta \in \underset{\sim}{I} \setminus \underset{\sim}{P} ; \quad h_{rs}(\eta) = 0\} .$$

<u>Les ensembles</u> $\underset{\sim}{U}_r$ <u>et les fonctions</u> $\pi \langle r , s\rangle$ <u>ne dépendent pas de</u> K , v <u>et</u> p .

<u>Définition</u> 7. - Pour un polynôme $f(x) \neq 0$,

$$\mathfrak{J}f = x^{-\operatorname{ord}_x f} f .$$

LEMME 18. - <u>Soit, pour un</u> $f \in \underset{\sim}{I}[x]$ <u>et un</u> $\rho \in \underset{\sim}{R}$, $0 \leqslant \deg f \leqslant m$,

$$\alpha := \operatorname{ord}_{x-\rho} \mathfrak{M}f \geqslant 1 , \qquad (f , \prod_{i=1}^{\deg f-1} f^{(i)}) = 1 ,$$

<u>soit</u> ξ_{ρ} <u>l'unique élément de</u> $\underset{\sim}{I}$ <u>tel que</u>

$$f^{(\alpha-1)}(\xi_{\rho}) = 0 , \quad \overline{\xi_{\rho}} = \rho$$

<u>et soit</u>, <u>avec la notation du lemme 17</u>,

$$\underset{\sim}{u}_\rho := [v(\frac{f^{(m)}(\xi_\rho)}{m!}) , \dots , v(f(\xi_\rho))] \in \underset{\sim}{U}_r$$

$$h_{\rho rs} := f(\xi_\rho + p^{\pi\langle r,s\rangle(\underset{\sim}{u}_\rho)} x) \quad (1 \leq s \leq s_r) .$$

<u>Alors</u>

$\operatorname{card}\{\xi \in \underset{\sim}{I} \setminus \underset{\sim}{P} ; \quad f(\xi) = 0\}$

$$= \operatorname{card}\{\rho \in \underset{\sim}{R} ; \mathcal{J}\mathcal{O}_1 \mathfrak{M} f(x) \mid_{x=\rho} = 0\} + \sum_{\substack{\rho \in \underset{\sim}{R}\setminus\{0\} \\ \operatorname{ord}_{x-\rho} \mathfrak{M} f \geq 2}} \sum_{s=1}^{s_r} \operatorname{card}\{\xi \in \underset{\sim}{I} \setminus P ; \; h_{\rho rs}(\xi) = 0\}.$$

LEMME 20. - <u>Si</u> $A \in \underset{\sim}{C}_\ell(m)$, $h(x) = g(cx)$, $g \in \underset{\sim}{K}[x]$, $\deg g \leq m$, $c \in \underset{\sim}{K}$, <u>alors</u>

$$A(h , y_1 , \dots , y_\ell) = c^{m \deg^1 A - w(A)} A(g , cy_1 , \dots , cy_\ell) .$$

LEMME 22. - <u>Pour toute paire d'entiers non négatifs</u> m <u>et</u> $n \leq m$, <u>il existe un système fini de formes</u> $M_i(\underset{\sim}{a})$ $(i \leq i_{mn})$ <u>et de polynômes</u> $N_{jk\ell}(\underset{\sim}{a} , y_1 , \dots , y_\ell)$ $(j \leq j_{mn} , \; k \leq k_j , \; \ell \leq \ell_{jk})$ <u>à coefficients entiers, une décomposition</u>

$$\underset{\sim}{N}_+^{i_{mn}} = \bigcup_{j=1}^{j_{mn}} \underset{\sim}{V}_j ,$$

<u>et des fonctions</u> $\upsilon \langle j , k , \ell\rangle : \underset{\sim}{V}_j \longrightarrow \underset{\sim}{N}_0$ <u>qui ont les propriétés suivantes</u>

$$M_i \in \underset{\sim}{C}_0(m) , \quad N_{jk\ell} \in \underset{\sim}{C}_\ell(m) ,$$

<u>si</u> $\operatorname{car} \underset{\sim}{R} = 0$ <u>ou si</u> $\operatorname{car} \underset{\sim}{R} > m$, $f(x) \in \underset{\sim}{I}[x]$, $0 \leq \deg f \leq m$, <u>tous les zéros de</u> $\mathfrak{M} f$, <u>sauf</u> 0 , <u>ont une multiplicité</u> $\leq n$,

$$(f(x) , \; \prod_{i=1}^{\deg f-1} f^{(i)}(x)) = 1 ,$$

$$\underset{\sim}{v} = [v(M_1(\underset{\sim}{f})) , \dots , v(M_{i_{mn}}(\underset{\sim}{f}))] \in \underset{\sim}{V}_j$$

<u>et</u>

$$\tilde{N}_{jk\ell}(y_1 , \dots , y_\ell) = \mathfrak{L}\mathfrak{K} N_{jk\ell}(f , p^{\upsilon\langle j,k,1\rangle(\underset{\sim}{v})} y_1 , \dots , p^{\upsilon\langle j,k,\ell\rangle(\underset{\sim}{v})} y_\ell) ,$$

<u>alors</u>

$$\text{card}\{\xi \in \underset{\sim}{I} \setminus \underset{\sim}{P} \; ; \quad f(\xi) = 0\}$$

$$= \sum_{k=1}^{k_j} \text{card}\{[\eta_1 , \eta_2 , \ldots] \in \underset{\sim}{R}^{\ell_{jk}} \; ; \quad \Lambda_{\ell=1}^{\ell_{jk}} \underset{\sim}{N}_{jk\ell}(\eta_1 , \ldots , \eta_\ell) = 0 \; .$$

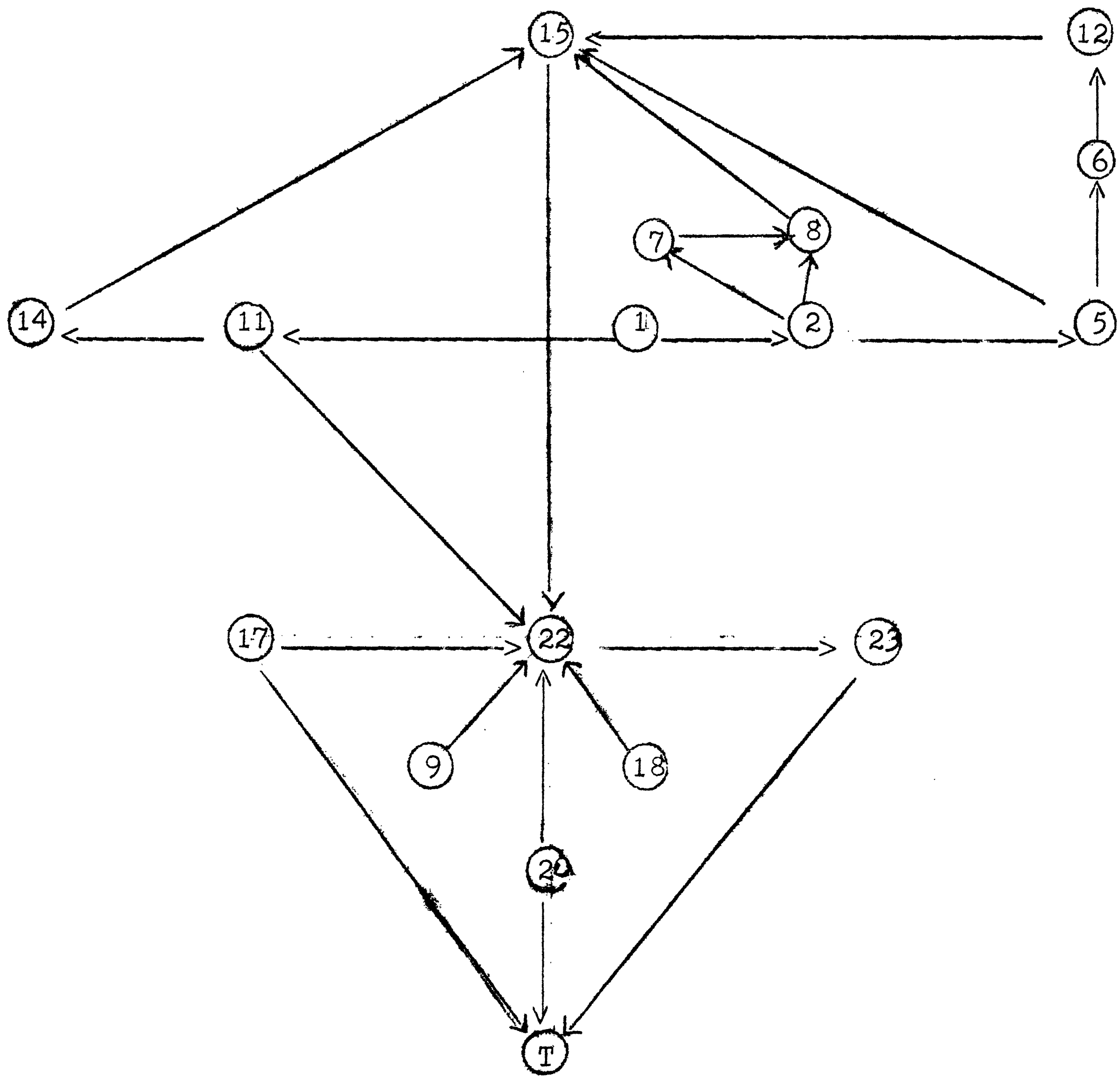
Les polynômes M_i , $N_{jk\ell}$, les ensembles $\underset{\sim}{V}_j$ et les fonctions $\upsilon \langle j , k , \ell \rangle$ ne dépendent pas de $\underset{\sim}{K}$, v et p .

Preuve par recurrence par rapport à n .

LEMME 23. - Le lemme 22 reste vrai avec $n = m$ et avec $0 \leqslant \deg f \leqslant m$ comme seule restriction sur le polynôme $f \in \underset{\sim}{I}[x]$.

Preuve par récurrence par rapport à m .

Voici un schéma des implications conduisant au théorème 1



T désigne le théorème 1, les flèches des implications, les nombres les lemmes. Les lemmes 3, 4, 10, 13, 16, 19 et 21, comme moins importants, sont omis. La démonstration complète paraîtra dans un article proposé aux Fundamenta Mathematicae.

RÉFÉRENCES

[1] COHEN (P.). - Decision procedures for real and p-adic fields, Comm. pure and appl. Math., t. 22, 1969, p. 131-151.

[2] NAGELL (T.). - Généralisation d'un théorème de Tchebycheff, J. Math. pur. et appl., Série 8, t. 4, 1921, p. 343-356.

[3] NAGELL (T.). - Introduction to number theory, 2nd edition. - New York, Chelsea Publishers, 1964.