

FRANÇOIS BERRONDO

**Critère d'irréductibilité d'un polynôme sur un anneau  
de valuation hensélien**

*Publications des séminaires de mathématiques et informatique de Rennes*, 1973, fascicule 4

« Séminaire d'algèbre et de logique », , exp. n° 7, p. 1-12

[http://www.numdam.org/item?id=PSMIR\\_1973\\_\\_4\\_A7\\_0](http://www.numdam.org/item?id=PSMIR_1973__4_A7_0)

© Département de mathématiques et informatique, université de Rennes, 1973, tous droits réservés.

L'accès aux archives de la série « Publications mathématiques et informatiques de Rennes » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

CRITERE D'IRREDUCTIBILITE D'UN POLYNOME

SUR UN ANNEAU DE VALUATION HENSELIEN

par

François BERRONDO

Notations

Soient  $K$  un corps,  $v$  une valuation hensélienne de  $K$ ,  $A$  l'anneau de  $v$  et  $G$  son groupe de valeurs. Soit  $\hat{K}$  le complété de  $K$  pour  $v$ .

Pour tout  $h$  de  $G$ , soit  $I_h$  l'idéal de  $A$  défini par

$$I_h = \{x \in A : v(x) \geq h\}.$$

Pour tout polynôme  $f$  de  $A[X]$  on note  $f^{(h)}$  la classe de  $f$  dans  $\frac{A}{I_h}[X]$ .

On veut ramener la recherche de l'irréductibilité d'un polynôme  $f$  unitaire de  $A[X]$  à celle de l'irréductibilité de  $f^{(h)}$  pour un  $h$  convenable. Ceci est possible pour tout polynôme si  $K$  est de caractéristique 0 ou si  $A$  est un anneau de valuation discrète complet (théorème 3). Ceci est possible également lorsque  $f$  est séparable (théorème 2).

Théorème 2

Soit  $f$  un polynôme de  $A[X]$ , unitaire, irréductible et séparable, de degré  $n$ , et soit  $\Delta$  son discriminant. Pour tout  $h$  appartenant à  $G$  tel que  $2h > n v(\Delta)$   $f^{(h)}$  n'est pas produit de deux polynômes unitaires de degré non nul.

Démonstration

Soient  $z_1, \dots, z_n$  les racines de  $f$  dans une extension de  $K$ . On a  $\Delta = \prod_{i < j} (z_i - z_j)^2$  donc  $v(\Delta) \geq 2 \sup_{i \neq j} v(z_i - z_j)$  car les  $z_i$  sont entiers sur  $A$ .

Soit  $g$  unitaire de degré  $n$  tel que  $f - g \in I_h A[X]$ , et soient  $y_1, \dots, y_n$  ses racines.

$$g(z) = \prod_{i=1}^n (z - y_i) \text{ et } v \circ g(z) = v \circ (f - g)(z) \geq h.$$

Par suite, il existe  $y_\ell$  tel que  $n v(z - y_\ell) \geq h$ .

Si  $2h > n v(\Delta)$ , on a  $2 v(z - y_\ell) > v(\Delta)$  donc

$$v(z - y_\ell) > \sup_{i \neq j} v(z_i - z_j).$$

On conclut par (2, § 8, ex. 12,b) que  $K[z_k] = K[y_k] \cdot y_k$  est donc de degré  $n$  sur  $K$  et  $g$  est irréductible.

S'il existait deux polynômes unitaires de degré non nul,  $\varphi_1, \varphi_2$  tels que  $f^{(h)} = \varphi_1 \cdot \varphi_2$ . Soient  $g_1$  et  $g_2$  des polynômes unitaires de  $A[X]$  tels que  $g_1^{(h)} = \varphi_1, g_2^{(h)} = \varphi_2$  et posons  $g = g_1 \cdot g_2$ . On a  $f^{(h)} = g^{(h)}$  donc  $f = g$  dans  $A[X]$  et  $g$  est réductible, d'où la contradiction.

Lorsque la valuation  $v$  est discrète, nous donnerons une meilleure détermination de l'élément  $h$  qui est alors un nombre entier.

Théorème 3

Soit  $A$  un anneau de valuation discrète hensélien et  $f$  un polynôme unitaire irréductible de  $A[X]$  tel que la clôture intégrale de  $\frac{A[X]}{(f)}$  soit un  $A$ -module de type fini. Il existe un entier  $h$  tel que les propriétés équivalentes

a) et b) soient vérifiées :

- a)  $f^{(h)}$  est irréductible.
- b)  $f^{(h)}$  n'est pas produit de polynômes unitaires de degré non nul.

Montrons que,  $\forall h$ , a) et b) sont équivalentes.

b) implique a) car un polynôme unitaire de degré non nul n'est pas inversible.

a) implique b) car,  $\frac{A}{\mu}$  étant local et complet, tout polynôme n'appartenant pas à  $\mu A[X]$  est associé à un polynôme unitaire (10, th. 3, 8).

$A$  étant hensélien,  $f^{(1)}$  est une puissance d'un polynôme irréductible ;

posons  $f^{(1)} = \bar{\varphi}^r$ , et soit  $\varphi \in A[X]$ , un polynôme tel que  $\varphi^{(1)} = \bar{\varphi}$ .

L'anneau  $C = \frac{A[X]}{(f)}$  est local d'idéal maximal.  $\mathfrak{m} = \omega C + \varphi(\alpha)C$ ,

$\omega$  désignant une uniformisante de  $A$  et  $\alpha$  la classe de  $X$  (théorème de Kummer [7] vol. 1, § 13). Soit  $w$  la fonction d'ordre  $\mathfrak{m}$ -adique de  $C$ .

Etablissons le

LEMME 1 :

Il existe un entier  $T$  tel que  $\forall z, z' \in C - \{0\}, w(z - z') - w(z) - w(z') \leq T$ .

Soit B la clôture intégrale de C. B est un A-module de type fini et donc un anneau de Dedekind. Comme A est hensélien, B est local ([3], ch. I, § 1, Prop. 5) c'est donc un anneau de valuation discrète. Soit v la valuation de B et P son idéal maximal. Remarquons que si C est intégralement clos, w se confond avec v et nous avons  $T = 0$ . Si non, comme B est un C-module de type fini, le théorème d'Artin-Rees établit l'existence d'un entier q tel que,  $\forall n, \mathfrak{m}^{q+n} B \cap C \subset \mathfrak{m}^{n+1}$ . Nous poserons  $\mathfrak{m} B = P^\ell$ . Considérons deux éléments z et z' de  $C - \{0\}$  et posons  $w(z) = a, w(z') = a'$ .  $z \notin \mathfrak{m}^{a+1}$  donc  $z \in \mathfrak{m}^{a+q} B = P^{\ell(a+q)}$ ;  $v(z) \leq \ell(a+q) - 1$  et de même  $v(z') \leq \ell(a'+q) - 1$ . Par suite  $v(z z') \leq \ell(a+a'+2q) - 2$ .  $z z' \notin P^{\ell(a+a'+2q)} = \mathfrak{m}^{a+a'+2q} B$ . Ce qui prouve que  $w(z z') \leq a + a' + 2q$  d'où le lemme en choisissant  $T = 2q - 1$ .

LEMME 2

Soient P et Q deux polynômes de  $A[X]$ , unitaires de degré non nul, tels que  $f^{(1)} = P^{(1)} Q^{(1)}$ . Alors  $w[P(\alpha)] + w[Q(\alpha)] \leq r$ .

Posons  $P^{(1)} = (\bar{\varphi})^{r_1}$  et  $Q^{(1)} = \bar{\varphi}^{r_2}$  avec  $r_1 + r_2 = r$ .

Si  $P(\alpha) \in \mathfrak{m}^t = (\omega, \varphi(\alpha))^t$ ,  $P \in (\omega, \varphi)^t + (f)$  et  $P^{(1)} \in (\bar{\varphi})^t + (f^{(1)})$ , soit  $\bar{\varphi}^{r_1} \in (\bar{\varphi})^t + (\bar{\varphi})^r$  d'où la relation  $r_1 \geq \inf(r, t)$ . Mais  $r_1 < r$ , donc  $r_1 \geq t$ , ce qui prouve que  $w[P(\alpha)] \leq r_1$ . De même  $w[Q(\alpha)] \leq r_2$ , donc  $w[P(\alpha)] + w[Q(\alpha)] \leq r$ .

Démontrons maintenant le théorème 1 en montrant que l'on peut choisir  $h = r + T + 1$ .

Si  $f^{(r+T+1)}$  était réductible, nous aurions  $f^{(r+T+1)} = P^* Q^*$  où  $P^*$  et  $Q^*$  sont des polynômes unitaires de degré non nul. Désignons par P et Q des polynômes unitaires de  $A[X]$  tels que  $P^{(r+T+1)} = P^*$  et  $Q^{(r+T+1)} = Q^*$ .

La relation  $f^{(r+T+1)} = P^{(r+T+1)} Q^{(r+T+1)}$  entraîne que  $f^{(1)} = P^{(1)} Q^{(1)}$  et, par le lemme 2, nous aurions  $w[P(\alpha)] + w[Q(\alpha)] \leq r$ . Par le lemme 1,

$w[P(\alpha) \cdot Q(\alpha)] \leq w[P(\alpha)] + w[Q(\alpha)] + T \leq r + T$ . Mais  $f = P Q \in \omega^{r+T+1} A[X]$  donc  $P(\alpha) Q(\alpha) \in \omega^{r+T+1} C \subset \mathfrak{m}^{r+T+1}$ , d'où la contradiction.  $f^{(r+T+1)}$  est irréductible.

Donnons des conditions sur  $A$  et  $f$  qui entraînent que la clôture intégrale de  $\frac{A[X]}{(f)}$  soit un  $A$ -module de type fini. Cette hypothèse est réalisée,

1°) si  $f$  est séparable ([2], ch. V, § 1, n° 6 Cor. 2, prop. 18) donc en particulier si  $A$  est de caractéristique 0.

2°) Si  $A$  est complet, ou plus généralement, si l'extension  $\hat{K} : K$  est séparable,  $K$  désignant le corps des fractions de  $A$  et  $\hat{K}$  son complété.

3°) Si  $A$  est entier sur un anneau géométrique ayant même corps des fractions que  $A$ .

Démonstration lorsque  $\hat{K} : K$  est séparable :

Soit  $v'$  la valuation de  $B$ ,  $L$  son corps des fractions et  $\hat{L}$  le complété de  $L$ .

Comme  $\hat{K}$  est séparable sur  $K$ ,  $\hat{K} \otimes_K L = \hat{L}$  ([2], ch. VI, § 8, n° 2, Cor. 2).

Soit  $n$  le degré de  $f$  et  $\alpha$  la classe de  $X$  dans  $C$ .  $1, \dots, \alpha^{n-1}$  est une base de  $L$  sur  $K$  et donc aussi de  $\hat{K} \otimes_K L = \hat{L}$  sur  $\hat{K}$ .

Comme  $\hat{K}$  est complet, l'isomorphisme entre  $(\hat{K})^n$  et  $\hat{L}$  défini par  $(x_0, x_1, \dots, x_{n-1}) \xrightarrow{g} x_0 + \alpha x_1 + \dots + \alpha^{n-1} x_{n-1}$  est un homéomorphisme topologique (Bourbaki E.V.T. Ch. I, § 1, th. 2) et sa restriction à  $K^n$  établit un homéomorphisme entre  $K^n$  et  $L$  puisque  $K^n$  est sous-espace topologique de  $(\hat{K})^n$  et  $L$  de  $\hat{L}$ .

$A^n$  est voisinage de 0 dans  $K^n$  donc  $g(A^n) = C$  contient un voisinage de 0 dans  $L_v$ .  $\exists k : v'(z) \geq k \implies z \in C, B \subset \frac{1}{\omega} C$  qui est un  $A$ -module de type fini, donc  $B$  aussi.

Démonstration lorsque  $A$  est entier sur un anneau géométrique  $E$  ayant  $K$  pour corps des fractions.

Montrons que dans ce cas, B est encore un C-module de type fini. E est le localisé par un idéal premier d'une algèbre affine sur un corps k ([11], appendice 1, page 102).

Posons  $E = S^{-1} k[x_1, \dots, x_s]$ , S étant le complémentaire de cet idéal premier dans  $k[x_1, \dots, x_s]$ .

$$C = \frac{A[X]}{(f)} = A[\alpha] \quad \text{est entier sur } S^{-1} k[x_1, \dots, x_s, \alpha] = E[\alpha]$$

Le corps des fractions de E est K donc celui de  $E[\alpha]$  est L, corps des fractions de C. B est donc la clôture intégrale de  $E[\alpha]$ .

La clôture intégrale  $\overline{k[x_1, \dots, x_s, \alpha]}$  de  $k[x_1, \dots, x_s, \alpha]$  est un  $k[x_1, \dots, x_s, \alpha]$ -module de type fini ([11], appendice 1, page 102, lemme 1).

Or,  $B = S^{-1} \overline{k[x_1, \dots, x_s, \alpha]}$  est un  $E[\alpha]$ -module de type fini, et à fortiori, un C-module de type fini.

Montrons sur un contre-exemple qu'il existe un anneau de valuation discrète hensélien A et un polynôme unitaire irréductible  $f \in A[X]$  tel que  $\forall h, f^{(h)}$  soit réductible.

D'après ([2], ch. V, § 1, Ex. 20), posons  $K = F_p(X_0, \dots, X_n, \dots)$  (p nombre premier) et  $L = K((Z))$ ,  $B = K[[Z]]$  est un anneau de valuation discrète complet.

Soit E le sous-corps de L engendré par  $L^p$ ,  $(X_n)_{n \in \mathbb{N}}$  et Z. E est différent de L, en effet dans les éléments de E, presque tous les  $X_n$  ne figurent que par leur puissance p-ième et par suite la série  $c = \sum X_n Z^n$ , par exemple, n'appartient pas à E.

Posons  $A = B \cap E$ , c'est un anneau de valuation discrète, montrons qu'il est hensélien.

Il suffit pour cela que tout polynôme de  $A[X]$   $f = X^s + a_1 X^{s-1} + \dots + a_{s-1} X + a_s$  où  $v(a_s) > 0$  et  $v(a_{s-1}) = 0$  ait une racine  $\alpha$  dans  $A$  telle que  $v(\alpha) > 0$  ([11], Lemme, page 94).

Or  $B$  étant complet,  $f$  a une racine  $\alpha$  dans  $B$  telle que  $v(\alpha) > 0$ . Montrons que  $\alpha \in A$ . Comme  $L^P \subset E$ , le polynôme minimal de  $\alpha$  sur  $E$  est  $X^P - \alpha^P$  si  $\alpha \notin E$  ([4], ch. II, § 5, th. 7)  $X^P - \alpha^P$  diviserait  $f$  ;  $(X^P - \alpha^P)(X^t + \dots + b_{t-1} X + b_t) = f$  et  $a_{s-1} = -\alpha^P b_{t-1}$ . Mais  $A$  est intégralement clos, donc les  $b_i$  appartiennent à  $A$ .  $v(b_{t-1}) \geq 0$  et  $v(\alpha) > 0$  donc  $v(\alpha^P b_{t-1}) \geq 0$  ce qui contredit l'hypothèse  $v(a_{s-1}) = 0$ .  $\alpha$  appartient donc à  $E$  et à  $E \cap B = A$ .  $A$  est hensélien.

Comme  $E$  contient  $K(Z)$ ,  $E$  est partout dense dans  $L$  et  $A$  est partout dense dans  $B$  qui est donc le complété de  $A$ .

$Z$  est une uniformisante et  $\forall h \frac{A}{Z^h_A} = \frac{B}{Z^h_B}$ . Considérons le polynôme  $f = X^P - c^P \in A[X]$ .  $f$  est irréductible puisque  $c \notin A$  mais  $f = (X - c)^P$  dans  $B[X]$  donc  $\forall h, f^{(h)} = (X - \bar{c})^P$  dans  $\frac{B}{Z^h_B} = \frac{A}{Z^h_A}$ . D'où le contre-exemple.

Calcul de l'entier  $h$  du théorème 3 dans le cas où  $f$  est séparable.

Avec les notations du théorème 1, supposons de plus que  $f$  est séparable et soit  $\Delta$  son discriminant qui est donc non nul.

Désignons par  $M$  la matrice de passage d'une base du  $A$ -module  $B$  à une base du  $A$ -module  $C$ . Nous avons  $\Delta = \text{Discr}(C) = [\text{Det}(M)]^2$ .  $\text{Discr}(B)$  ([7], ch. 2 § 7, prop. 1). D'où  $v[\text{Det}(M)] \leq \frac{1}{2} v(\Delta)$ . L'inclusion  $B \subset \frac{1}{\text{Det}(M)} C$  montre que  $\omega^E B \subset C$ , où  $E$  désigne la partie entière de  $\frac{1}{2} v(\Delta)$ . Si  $v(\Delta) = 0$  ou 1,  $B = C$  donc  $T = 0$  et on peut choisir  $h = r + 1$ . Si  $v(\Delta) \geq 2$ ,  $\omega^E B$  est un idéal propre donc  $\omega^E B \subset \mathfrak{m}$ . Remarquons que  $\mathfrak{m}^r \subset \omega C$  car  $\mathfrak{m} = (\omega, \varphi(\alpha))$  et, puisque  $f - \varphi^r \in \omega A[X]$ ,  $\varphi^r(\alpha) \in \omega C$ . Nous avons donc  $\mathfrak{m}^{Er} B \subset \omega^E B \subset \mathfrak{m}$  ce qui montre que le nombre  $q$  du théorème 1 peut être pris égal à  $E r$ , d'où  $T = 2 E r - 1$  et  $h = (2 E + 1)r$ . Comme  $2 E \leq v(\Delta)$ ,

nous avons démontré le :

Théorème 4

Soient A un anneau de valuation discrète hensélien et v sa valuation.  
Soit f un polynôme de  $A[X]$ , unitaire et séparable de discriminant  $\Delta$  et  
tel que  $f^{(1)}$  soit la puissance r-ième d'un polynôme irréductible.

$$\text{Posons } h = \begin{cases} r+1 & \text{si } v(\Delta) = 0 \text{ ou } 1 \\ [v(\Delta)+1]r & \text{si } v(\Delta) \geq 2 \end{cases}$$

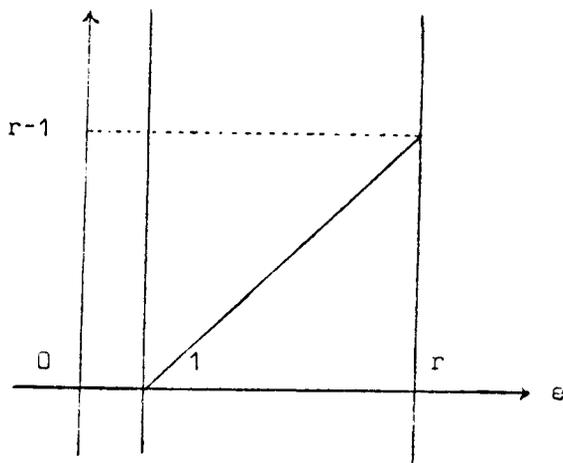
Alors f est irréductible si et seulement si  $f^{(h)}$  l'est.

En faisant intervenir la différentielle, on obtient une meilleure majoration pour h.

Soit e l'indice de ramification de la valuation de B par rapport à celle de A. On a  $\omega_B = p^e$ . Soit F son degré résiduel. Posons  $d = v[\text{Det}(M)]$ . Si  $d = 0$ ,  $B = C$ . Si  $d > 0$ ,  $\omega^d B \subset C$ , et comme  $\omega^d B$  est un idéal propre,  $\omega^d B \subset \mathfrak{m}$ . Ce qui montre que le nombre q du lemme 1 peut être pris égal à d.e et donc  $h = 2q + r$ , égal à  $2d.e + r$ .

Soit  $\delta$  la différentielle, et m l'exposant différentiel. On a  $\delta = P^m$ . La norme de  $\delta$  est  $\omega^{mF} A$ . C'est aussi l'idéal engendré par le discriminant de B, donc  $v(\Delta) - 2d = mF = m \frac{n}{e}$ ;  $2de = e v(\Delta) - mn$ . Majorons la quantité  $e v(\Delta) - mn$  considérée comme fonction de e et m.

Les inclusions de corps  $\frac{A}{\omega A} \subset \frac{C}{\mathfrak{m}} \subset \frac{B}{P}$  montrent que  $[\frac{C}{\mathfrak{m}} : \frac{A}{\omega A}] = \text{degré de } \varphi$  divise  $[\frac{B}{P} : \frac{A}{\omega A}] = F$ , comme le degré  $\varphi$  est  $\frac{n}{r}$  et comme  $F = \frac{n}{e}$  on déduit que e divise r. D'autre part e et m sont liés par l'inégalité  $m \geq e-1$  ([4], ch. V, § 11, th. 28). Le domaine de variation de e et m est le suivant.



Les courbes  $e v(\Delta) - mn = \text{Constante}$  sont des droites de pente  $\frac{v(\Delta)}{n}$ .

Si cette pente est inférieure à 1, le maximum est atteint au point (1, 0) et vaut  $v(\Delta)$ . Si cette pente est supérieure à 1, le maximum est atteint au point (r, r-1) et vaut  $r v(\Delta) - (r-1)n$ . On a démontré le

Théorème 5

Soient A un anneau de valuation discrète hensélien et v sa valuation.

Soit f un polynôme de  $A[X]$ , unitaire et séparable de degré n, de discriminant  $\Delta$  et tel que  $f^{(1)}$  soit la puissance r-ième d'un polynôme irréductible.

Posons h =

$$\begin{cases} r+1 & \text{si } v(\Delta) = 0 \text{ ou } 1 \\ r+v(\Delta) & \text{si } 1 \leq v(\Delta) \leq n \\ n+r[v(\Delta)+1-n] & \text{si } v(\Delta) \geq n \end{cases}$$

Alors f est irréductible si et seulement si  $f^{(h)}$  l'est.

Remarque

Lorsque A est à corps résiduel fini, on peut programmer sur machine un test d'irréductibilité des  $f^{(k)}$  successifs. Une réponse affirmative pour un  $k \leq h$  signifie que f est irréductible. Des réponses négatives pour  $k = 1, 2, \dots, h$  signifient que f ne l'est pas.

Exemples

- 1)  $f = X^4 - 3X^2 + 4$  est irréductible sur  $\mathbb{Q}$ , l'est-il sur  $\mathbb{Q}_7$  corps des nombres 7-adiques ?

$$f^{(1)} = X^4 + 4X^2 + 4 = (X^2 + 2)^2 \quad r = 2$$

Le discriminant de  $f$  est  $\Delta = 2^6 \times 7^2$  ;  $v(\Delta) = 2$  ;  $v(\Delta) \leq n - 4$   
donc  $h = 4$ .

Nous sommes ramenés à chercher si  $X^4 - 3X^2 + 4$  est produit de polynômes unitaires dans  $\frac{\mathbb{Z}}{(7^4)} = \frac{\mathbb{Z}}{(2401)}$ . Un calcul montre qu'il n'en est rien donc  $f$  est irréductible sur  $\mathbb{Q}_7$ . En fait  $f$  n'a pas de diviseurs unitaires dans  $\frac{\mathbb{Z}}{(7^2)} = \frac{\mathbb{Z}}{(49)}$ .

- 2)  $f = X^4 + 2X + 4$  est irréductible sur  $\mathbb{Q}$ , l'est-il sur  $\mathbb{Q}_2$  ?

$$f^{(1)} = X^4 \quad r = 4$$

$$\Delta = 4^7 - 3^3 \times 2^4 \quad v(\Delta) = 4 \quad h = 8$$

On trouve que dans  $\frac{\mathbb{Z}}{(2^8)}$ ,  $f$  a la racine  $-10$  car  $(-10)^4 - 20 + 4 = +9984 = 2^8 \times 3 \times 13$ .

$f$  est donc réductible dans  $\mathbb{Q}_2$ .

Un calcul montre que  $X^4 + 2X + 4$  n'a pas de diviseur unitaire de degré 2 dans  $\frac{\mathbb{Z}}{(4)}$ , il en est donc de même dans  $\mathbb{Q}_2$  et par suite  $f$  admet une racine et une seule dans  $\mathbb{Q}_2$ .

APPLICATION I

CRITERE D'UNICITE DU PROLONGEMENT  
D'UNE VALUATION DISCRETE

Comme application du théorème 3 nous obtenons le :

Théorème 0

Soient K un corps muni d'une valuation discrète v et A l'anneau de v.  
Soit L = K[α] une extension finie de K où α est racine d'un polynôme f  
à coefficients dans A, unitaire, irréductible et séparable, de degré n  
et discriminant Δ, tel que f<sup>(1)</sup> soit la puissance r-ième d'un polynôme  
irréductible.

$$\text{Posons } h = \begin{cases} r[(\Delta)+1-n] + n & \text{si } v(\Delta) \geq n \\ v(\Delta)+r & \text{si } 2 < v(\Delta) \leq n \\ r+1 & \text{si } v(\Delta) = 0 \text{ ou } 1 \end{cases}$$

Alors le prolongement de v à L est unique si et seulement si f<sup>(h)</sup>  
est irréductible.

Nous savons par ([2], ch. 6, § 8, n° 2, corollaire 2) que le nombre de prolongements de v à L est égal au nombre de facteurs irréductibles figurant dans la décomposition de f dans  $\hat{K}[X]$  ( $\hat{K}$  désignant le complété de K pour la métrique de v).

Par suite le prolongement de v est unique si et seulement si f est irréductible dans  $\hat{K}[X]$  ou dans  $\hat{A}[X]$ .

Or  $\hat{A}$  étant hensélien, on peut appliquer le théorème 3 à  $\hat{A}$  et à f.

Comme  $\forall k, \frac{\hat{A}}{\omega_{k\hat{A}}} = \frac{A}{\omega_{kA}}$ , l'irréductibilité de  $f$  dans  $\hat{A}[X]$  équivaut à celle de  $f^{(h)}$ .

### Exemples

1°) Soit  $L = \mathbb{Q}[\alpha]$  où  $\alpha$  est racine de  $X^4 - 3X^2 + 4$  (en fait  $L = \mathbb{Q}[i, \sqrt{7}]$ )

La valuation 7-adique a un prolongement unique à  $L$  puisque  $X^4 - 3X^2 + 4$  est irréductible dans  $\mathbb{Q}_7$ .

2°) Soit  $L = \mathbb{Q}[\alpha]$  où  $\alpha$  est racine de  $X^4 + 2X + 4$ .

La valuation 2-adique admet deux prolongements à  $L$  puisque  $X^4 + 2X + 4$  est produit dans  $\mathbb{Q}_2[X]$  d'un polynôme du premier degré et d'un polynôme du troisième degré irréductible.

B I B L I O G R A P H I E

-----

- [1] SAMUEL Théorie algébrique des nombres.  
(Hermann 1967).
- [2] BOURBAKI Algèbre commutative, ch. V et ch. VI.  
(Hermann 1964).
- [3] RAYNAUD Anneaux henséliens.  
(Springer-Verlag (169) 1970).
- [4] ZARISKI-SAMUEL Commutative algebra vol. 1  
(Van Nostrand 1958).
- [5] LANG Algebra.  
(Addison-Wesley 1965).
- [6] KNUTH The art of Computer Programming, vol. 2,  
semi numerical Algorithms Reading Mass.  
(Addison Wesley 1969).
- [7] GROTHENDIECK Eléments de Géométrie Algébrique. (ch. IV, part. 1)  
(Publ. Math. n° 20, Inst. Hautes Etudes Sci. 1960).
- [8] BERLEKAMP On the factorization of polynomials over finite field  
(Bell Teleph. Lab. Inc. Murray Hill N.J. 1967).
- [9] GRECO Henselization of a ring with respect to an ideal.  
(Trans. A.M.S. 144, 1969).
- [10] GRECO-SALMON Topics in  $\mathcal{M}_0$ -adic topologies.  
(Springer Verlag 1971).
- [11] LAFON Anneaux henséliens.  
(Bul. Soc. Math. 91 1963).
- [12] MATSUMARA Commutative Algebra  
(Benjamin, New-York, 1970).
- [13] ENDLER Valuation Theory  
(Springer Verlag)