Théorème d'irréductibilité de Hilbert

Colas Bardavid

20 janvier 2005 : la galette de Binet

Préliminaires : irréductibilité

Définition 1 *Soit k un corps et soit $P \in k[X_1, \ldots, X_n]$ un polynôme à n indéterminées à coefficients dans k ; on peut écrire $P = \sum_{\alpha \in \mathbf{N}^n} a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, où la somme est à support fini. On appelle degré total de P et on note* $\deg P$ *l'entier* $\max_{a_\alpha \neq 0}(\alpha_1 + \cdots + \alpha_n)$.

Définition 2 *Soit $P \in k[X_1, \ldots, X_n]$ non constant. On dit que P est irréductible si lorsqu'on décompose $P = QR$ dans $k[X_1, \ldots, X_n]$, on a forcément* $\deg P = 0$ *ou* $\deg Q = 0$.

1 Introduction

Soit un k un corps.

Soit $P(t, X)$ un polynôme à deux variables ; on verra t comme un paramètre et X comme l'indéterminée. On a $P(t, X) \in k[t, X]$ et en particulier $P \in k(t)[X]$, ce qui nous permettra de voir P comme un élément d'une algèbre de polynômes $L[X]$ au-dessus d'un corps.

1.1 Spécialisations et spécialisations acceptables

Soit $t_0 \in k$. Notons $\chi_{t_0} : \begin{array}{c} k[t] \to k \\ Q(t) \mapsto Q(t_0) \end{array}$ le morphisme d'évaluation. χ_{t_0} induit un morphisme $\widetilde{\chi_{t_0}} : \begin{array}{c} k[t, X] \to k[X] \\ P(t, X) \mapsto P(t_0, X) \end{array}$.

Est-ce que $\widetilde{\chi_{t_0}}$ conserve bien les propriétés d'irréductibilité ? Par exemple, est-ce que $\widetilde{\chi_{t_0}}$ envoie les irréductibles sur les irréductibles, pour un t_0 bien choisi ou pour tous ? (non) De façon inverse, si on se donne un polynôme P irréductible, est-ce qu'il existe un t_0 tel que $\widetilde{\chi_{t_0}}(P)$ est encore irréductible ? Dans ce cas, on dira que t_0 est une spécialisation (P-)acceptable. Que peut-on dire sur l'ensemble des spécialisations acceptables ?

Dans toute la suite, P est supposé irréductible et on note

$$P = \sum_{k=0}^{N} a_k(t) X^k,$$

où les $a_k(t)$ sont dans $k[t]$ et où $a_N \neq 0$. On supposera pour éviter les trivialités que $N \geq 2$.

1.2 Motivations (historiques)

Hilbert a étudié ce problème dans le but de construire des groupes de Galois.

1.3 Corps hilbertiens

Si k est un corps tel que la spécialisation $\widetilde{\chi_{t_0}}$ conserve bien les propriétés d'irréductibilité, on dit que k est un corps hilbertien. Plus précisément :

Définition 3 *Soit k un corps. On dit que k est hilbertien si $\forall r, s, n \in \mathbf{N}^*, \forall g \in k[t_1, \ldots, t_r] \setminus \{0\}, \forall f_1, \ldots, f_n \in k[t_1, \ldots, t_r, X_1, \ldots, X_s] \setminus k[t_1, \ldots, t_r]$ irréductibles, $\exists (t_1^\star, \ldots, t_r^\star) \in k^r$ tel que $g(t_1^\star, \ldots, t_r^\star) \neq 0$ et $\forall 0 \leq i \leq n, f_i(t_1^\star, \ldots, t_r^\star, X_1, \ldots, X_s) \in k[X_1, \ldots, X_s]$ est irréductible.*

Remarque : Il est équivalent de demander l'existence d'un r-uplet $(t_1^\star, \ldots, t_r^\star)$ ou d'une infinité.
Exemples : $\mathbf{R}$, $\mathbf{Q}_p$, $\mathbf{C}$, $\mathbf{F}_{p^n}$, tous les corps algébriquement clos ne sont pas des corps hilbertiens.

$\mathbf{Q}$, tous les corps de nombres, $k(X)$ pour tout corps k, tous les corps infinis finiment engendrés sont des corps hilbertiens.

1.4 Étude du cas général

Soit $\overline{L} = \overline{k(t)}$ une clôture algébrique de L.

On scinde dans $\overline{L}$ le polynôme P :

$$P = a_N(t) \prod_{i=1}^{N} (X - \alpha_i) \text{ où } \forall i, \alpha_i \in \overline{k(t)}.$$

Soit t_0 tel que que $a_N(t_0) \neq 0$, comme on le supposera souvent. On peut alors étendre χ_{t_0} à $k[t, a_N(t)^{-1}]$. Or les α_i sont entiers au-dessus de $k[t, a_N(t)^{-1}]$. Comme Serge Lang l'explique page 347 dans [Lang], on peut alors prolonger (algébriquement) χ_{t_0} en :

$$\widehat{\chi_{t_0}} : k[t]\left[\frac{1}{a_N(t)}\right][\alpha_i]_{1 \leq i \leq n} \to \overline{k}.$$

On notera (attention, ce n'est qu'une notation !) : $\widehat{\chi_{t_0}}(\alpha) = \alpha(t_0)$.

En particulier, on a :

$$\widetilde{\chi_{t_0}}(P(t, X)) = P(t_0, X) = \widehat{\chi_{t_0}}\left(a_N(t) \prod_{i=1}^{N} (X - \alpha_i)\right) = a_N(t_0)(X - \alpha_i(t_0)).$$

Ainsi, si $P(t_0, X) \in k[X]$ est réductible, il existe $\varnothing \subsetneq S \subsetneq \{1, \ldots, n\}$ tel que $\prod_{i \in S}(X - \alpha_i(t_0))$ soit dans $k[X]$ sans que cependant $\prod_{i \in S}(X - \alpha_i)$ ne puisse être dans $k(t)[X]$ puisqu'on a supposé P irréductible. C'est donc qu'il existe $y_S \in k[\alpha_i]_{1 \leq i \leq n}$ tel que d'une part $y_S \notin k(t)$ mais $y_S(t_0) \in k$.

En contraposant, on obtient que $(\forall \varnothing \subsetneq S \subsetneq \{1, \ldots, n\}, y_S(t_0) \notin k) \Rightarrow P(t_0, X)$ irréductible.

Une piste possible pour l'étude de la hilbertiannité d'un corps k est donc d'étudier le corps $\overline{k(t)}$.

1.5 Théorèmes de Puiseux (pour la culture)

On dispose en particulier des théorèmes suivants.

Si k est un corps, on note $k((X))$ le corps des fractions de $k[[X]]$, les séries formelles à coefficients dans k. Tout élément de $k((X))$ s'écrit $\sum_{k \geq n_0} a_k X^k$ où $n_0 \in \mathbf{Z}$ et $a_k \in k$.

Théorème 4 (Théorème de Puiseux formel) *Soit k un corps algébriquement clos de caractéristique nulle. Alors, $\bigcup_{n \geq 1} k((X^{1/n}))$ est une clôture algébrique de $k((X))$.*

Définition 5 *On note $\mathbf{C}\{X\}$ et on appelle algèbre des séries formelles convergentes la $\mathbf{C}$-algèbre des séries formelles dans $\mathbf{C}[[X]]$ qui ont un rayon de convergence non nul. On note $\mathbf{C}\langle X \rangle \subset \mathbf{C}((X))$ son corps des fractions.*

Théorème 6 (Théorème de Puiseux analytique 1) *$\bigcup_{n\geq 1} \mathbf{C}\langle X^{1/n}\rangle$ est une clôture algébrique de $\mathbf{C}\langle X\rangle$.*

Définition 7 *Soit $r > 0$. On note $\mathcal{A}(r)$ l'anneau des fonctions définies et continues sur $\{z \in \mathbf{C}/|z| \leq r\}$ et holomorphes à l'intérieur de ce domaine.*

Théorème 8 (Théorème de Puiseux analytique 2) *Soit $r > 0$. Soit $P \in \mathcal{A}(r)[X]$ unitaire de degré n. Alors, il existe $\rho > 0$, un entier e et n éléments $x_1, \ldots, x_n$ dans $\mathcal{A}(\rho)$ tels que :*

$$P(z^e, X) = \prod_{i=1}^{n} (X - x_i(z))$$

1.6 Le théorème d'irréductibilité de Hilbert (1892)

Le but de cet exposé est de démontrer que $\mathbf{Q}$ est hilbertien. Plus précisément :

Théorème 9 *Soit $P(t, X) \in \mathbf{Q}[t, X]$ un polynôme irréductible. Alors :*

a) *il y a une infinité de spécialisations $t_0 \in \mathbf{Q}$ P-acceptables.*

b) *il y a une infinité de spécialisations $t_0 \in \mathbf{Z}$ P-acceptables et une infinité de spécialisations $t_0 \in \mathcal{P}$ P-acceptables.*

c) *l'ensemble $\{t_0 \in \mathbf{Q}/P(t_0, X)$ irréductible$\}$ des spécialisations acceptables est dense dans $\mathbf{Q}$ pour la topologie usuelle, pour toutes les topologies p-adiques et pour la topologie de Zariski.*

Remarque : Le premier point du b) entraîne le a) et le c), en faisant des changements de variables judicieux.

2 Démonstration du théorème d'irréductibilité de Hilbert

Rappelons qu'on a fixé $P \in k[t, X]$ irréductible, etc. Maintenant, on fixe $k = \mathbf{Q}$.

2.1 Étude de $\overline{\mathbf{Q}(t)}$

Commençons par une petite

Définition 10 *On dit $t_0 \in \mathbf{Q}$ est une valeur régulière si $a_N(t_0) \neq 0$ et si $P(t_0, X) \in \mathbf{Q}[X]$ est à racines simples dans $\mathbf{C}$.*

On montre en utilisant l'irréductibilité de P la

Proposition 11 *Toutes les spécialisations $t_0 \in \mathbf{Q}$ sauf un nombre fini d'entre elles sont régulières.*

Muni de ces armes, on peut énoncer le :

Théorème 12 (théorème des fonctions implicites analytique) *Soit $t_0 \in \mathbf{Q}$ un spécialisation régulière. Alors, il existe N fonctions $x_1(t), \ldots, x_N(t)$ définies autour de t_0, deux-à-deux distinctes en tout point et analytiques en t_0 telles que :*

$$x_i(t) = \sum_{k=0}^{\infty} A_k^{(i)} (t - t_0)^k \text{ avec } A_k^{(i)} \in \mathbf{Q}[x_i(t_0)]$$
$$\forall 1 \leq i \leq N, \forall\, |t - t_0| \text{ petit}, P(t, x_i(t)) = 0$$

Donnons une esquisse de preuve de ce théorème.

Démonstration : Par un changement de variable on se ramène au cas où $t_0 = 0$ et, quitte à soustraire à P une de ses racines, au cas où $P(t_0, 0) = 0$. Notre polynôme s'écrit alors $P(t, X) = a_{0,1}X + a_{1,0}t + \sum_{i+j\geq 2} a_{i,j}t^iX^j$. La régularité de t_0 nous dit que $a_{0,1} \neq 0$ et donc, quitte à diviser P par $-a_{0,1}$, on peut écrire $P(t, X) = -X + a_{1,0}t + \sum_{i+j\geq 2} a_{i,j}t^iX^j$. Supposons alors que la série formelle $x(t) = \sum_{k=1}^{\infty} B_kt^k$ vérifie $P(t, x(t)) = 0$. Cela s'écrit $x(t) = a_{1,0}t + \sum_{i+j\geq 2} a_{i,j}t^ix(t)^j$. Par récurrence, on en déduit que les B_k sont uniquement déterminés par les formules $B_k = p_k(a_{i,j})_{i,j\leq k}$ où p_k est un polynôme à plusieurs variables à coefficients entiers positifs.

Il faut alors montrer que cette série formelle a un rayon de convergence non nul. Soit A plus grand que tous les $|a_{i,j}|$. On considère alors le problème où on a remplacé tous les $a_{i,j}$ par A. On trouve des coefficients B'_k qui sont plus grands que $|B_k|$. Cependant, on sait résoudre explicitement aussi l'équation $x(t) = At + \sum_{i+j\geq 2} At^ix(t)^j$ et la solution est analytique en 0. ■

On connaît donc la forme locale des $\alpha \in \overline{\mathbf{Q}(t)}$.

2.2 Un changement de variable

Soit T_0 une valeur régulière.

On pose $Q(t, X) = P\left(T_0 + \frac{1}{t}, X\right) t^d$ où d est le plus grand des degrés des $a_k(t)$, grâce à quoi $Q(t, X) \in \mathbf{Q}[t, X]$. Ce changement de variable est pertinent dans la mesure où $Q(t, X)$ est encore irréductible et où si t_0 est une spécialisation Q-acceptable, alors $T_0 + \frac{1}{t_0}$ est une spécialisation P-acceptable.

Par ailleurs, on a

$$\forall i \leq N, \forall |t| \text{ suffisamment grand, } Q(t, \alpha_i(t)) = 0 \text{ avec}$$
$$\forall i, \alpha_i(t) = \sum_{k=0}^{\infty} A_k^{(i)} \left(\frac{1}{t}\right)^k \in \mathbf{C}$$

En particulier, miracle de l'algèbre polynômiale, si t_0 est suffisamment grand, on a la factorisation :

$$Q(t_0, X) = \underbrace{t_0^d a_N \left(T_0 + \frac{1}{t_0}\right)}_{=\lambda(t_0)\in\mathbf{Q}} \prod_{i=1}^{N} \left(X - \underbrace{\alpha_i(t_0)}_{\in\mathbf{C}}\right)$$

Si on trouve des spécialisations Q-acceptables arbitrairement grandes, alors on saura que t_0 est un point adhérent à l'ensemble des spécialisations P-acceptables. En particulier, on en déduira que l'ensemble des spécialisations P-acceptables est dense dans $\mathbf{Q}$ pour la topologie usuelle.

2.3 Le moteur de la preuve

Supposons que $t_0 \in \mathbf{Q}$ est une spéciliasation inacceptable, c'est-à-dire que $Q(t_0, X) \in \mathbf{Q}[X]$ est réductible. Comme $Q(t_0, X)$ se scinde dans $\mathbf{C}$ en $\lambda(t_0) \prod_{i=1}^{N} (X - \alpha_i(t_0))$, c'est donc forcément qu'il existe deux paquets de racines $\varnothing \subsetneq S \subsetneq \{1, \dots, n\}$ et $\{1, \dots, n\} \setminus S$ tels que

$$Q(t_0, X) = \lambda(t_0) \prod_{i\in S}(X - \alpha_i(t_0)) \prod_{i\notin S}(X - \alpha_i(t_0))$$

est une factorisation dans $\mathbf{Q}[X]$ de $Q(t_0, X)$.

Cependant, n'oublions pas que $Q(t, X) \in \mathbf{Q}[t, X]$ est irréductible. En particulier, si on relève la décomposition de $Q(t_0, X)$ en une décomposition

$$Q(t, X) = t^d a_N \left(T_0 + \frac{1}{t}\right) \prod_{i\in S}(X - \alpha_i(t)) \prod_{i\notin S}(X - \alpha_i(t)),$$

on voit qu'un au moins des coefficients de $\prod_{i\in S}(X-\alpha_i(t))$ ou de $\prod_{i\notin S}(X-\alpha_i(t))$, qu'on notera y_S, n'est pas dans $\mathbf{Q}(t)$. Cependant, $y_S(t_0)\in\mathbf{Q}$ puisque la factorisation considérée provient d'une factorisation dans $\mathbf{Q}[X]$.

En contraposant, on obtient que $(\forall\varnothing\subsetneq S\subsetneq\{1,\dots,n\}, y_S(t_0)\notin\mathbf{Q})\Rightarrow Q(t_0,X)$ irréductible.

Dès lors, notre nouveau but est de montrer que si y est l'une des fonctions y_S, alors, $\{t_0\in\mathbf{Z}/y(t_0)\in\mathbf{Q}\}$ est petit.

2.4 Entièreté

Notons y une des fonctions y_S. Comme y est une somme de produits de α_i, y est algébrique au-dessus de $\mathbf{Q}(t)$. Ainsi, quitte à multiplier y par $R\in\mathbf{Z}[t]$, Ry est entier au-dessus de $\mathbf{Z}[t]$. Si $t_0\in\mathbf{Z}$ et $y(t_0)\in\mathbf{Q}$ alors, $Ry(t_0)\in\mathbf{Q}$ en même temps que $Ry(t_0)$ est entier au-dessus de $\mathbf{Z}$. Ainsi, $Ry(t_0)\in\mathbf{Z}$. On note maintenant $z=Ry$ et on cherche à montrer que $\{t_0\in\mathbf{Z}/z(t_0)\in\mathbf{Q}\}=\{t_0\in\mathbf{Z}/z(t_0)\in\mathbf{Z}\}$ est petit.

Comme tous les α_i s'expriment comme série entière au voisinage de l'infini, il en est de même de tous les y_S, de y et de z : on peut écrire $z(t)=\sum_{k=0}^{\infty}B_k\left(\frac{1}{t}\right)^k$ pour $|t|$ suffisamment grand, avec les $B_k\in\mathbf{C}$. Par ailleurs, comme les y_S ne sont pas des fractions rationnelles, z n'est pas un polynôme.

2.5 L'essence (arithmétique) qui fait tourner le moteur

Lemme 13 *Soient $t_0<t_2<\cdots<t_m\in\mathbf{R}$ et $f\in\mathcal{C}^m([t_0,t_m],\mathbf{R})$. Alors, il existe $t_0<t^\star<t_m$ tel que*

$$\frac{f^{(m)}(t^\star)}{m!}=\begin{vmatrix}1 & t_0 & t_0^2 & \cdots & t_0^{m-1} & f(t_0)\\ 1 & t_1 & t_1^2 & \cdots & t_1^{m-1} & f(t_1)\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ 1 & t_m & t_m^2 & \cdots & t_m^{m-1} & f(t_m)\end{vmatrix}\cdot\underbrace{\begin{vmatrix}1 & t_0 & t_0^2 & \cdots & t_0^{m-1} & t_0^m\\ 1 & t_1 & t_1^2 & \cdots & t_1^{m-1} & t_1^m\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ 1 & t_m & t_m^2 & \cdots & t_m^{m-1} & t_m^m)\end{vmatrix}^{-1}}_{V_m}$$

Démonstration : C'est plus ou moins le théorème de Rolle.■

On distingue alors deux cas : si $\{t_0\in\mathbf{Z}/z(t_0)\in\mathbf{Z}\}$ est un ensemble fini, en particulier, $\psi(N)=\#\{t_0\in\mathbf{Z},|t_0|\leq N/z(t_0)\in\mathbf{Z}\}\in\mathcal{O}(N^{1-\varepsilon})$ pour un certain $\varepsilon>0$.

D'autre part, si $\{t_0\in\mathbf{Z}/z(t_0)\in\mathbf{Z}\}$ est un ensemble infini, alors les B_k de l'écriture $z(t)=\sum_{k=0}^{\infty}B_k\left(\frac{1}{t}\right)^k$ sont forcément tous réels (sinon, la partie imaginaire de $z(t)$ est équivalente à c/t^{k_0} pour un certain k_0 au voisinage de l'infini et est donc non nulle à partir d'un certain rang, ce qui empêche z d'avoir une infinité de valeurs réelles en des points entiers).

Par ailleurs, comme z n'est pas un polynôme, en la dérivant un nombre suffisant (disons m) de fois, on tue tous les monômes t^k où $k\geq 0$. Alors, $z^{(m)}(t)\sim_{t\to\infty}\frac{p}{t^q}$ et donc, pour $t\geq A$, $0<|z^m(t)|<\frac{2|p|}{t^q}$. On peut alors appliquer le lemme à la fonction z et aux entiers $t_0<t_1<\cdots<t_m$ tous plus grands que A et tels que $z(t_i)\in\mathbf{Z}$.

La non nullité de $z^{(m)}(t^\star)$ entraîne que les matrices qui interviennent dans le lemme, qui sont à coefficients entiers, sont de module plus grand que 1. On a

$$\frac{1}{V_m}\leq\left|\frac{z^{(m)}(t^\star)}{m!}\right|<\frac{2\,|p|}{t_0^q}.$$

Or, $V_m=\prod_{0\leq i<j\leq m}(t_j-t_i)<(t_m-t_0)^{\frac{m(m+1)}{2}}$. Donc : $(t_m-t_0)^{-\frac{m(m+1)}{2}}<\frac{1}{V_m}\leq\left|\frac{z^{(m)}(t^\star)}{m!}\right|<\frac{2|p|}{t_0^q}$. Donc, $\exists\lambda>0/t_m-t_0>t_0^\lambda$, ce qui signifie que les t_i sont de plus en plus écartés. On va en déduire que $\psi(N)$ est un $\mathcal{O}(N^{1-\varepsilon})$.

2.6 Fin de la démonstration

On pose $\alpha=\frac{1}{1+\lambda}$. Comptons les t_i entiers compris entre 0 et N tels que $z(t_i)\in\mathbf{Z}$. D'abord, dans $[0,N^\alpha[$, il y en a au plus N^α. Ensuite, dans $[N^\alpha,N]$, si $N^\alpha>A$ et si on classe les $\{t_i\}_{0\leq i\leq M}$ par ordre croissant, on a $t_{i+m} - t_i > t_i^\lambda > N^{\alpha\lambda}$. On fait la division euclidienne $M = km + r$ de M et on écrit :

$$\begin{aligned} N > N - N^\alpha &\geq t_M - t_0 \\ &= t_{km+r} - t_{km} + (t_{km} - t_{(k-1)m}) + (t_{(k-1)m} - t_{(k-2)m}) + \cdots + (t_m - t_0) \\ &\geq kN^{\alpha\lambda} + t_{km+r} - t_{km} \geq (k+1)N^{\alpha\lambda}. \end{aligned}$$

Le nombre de t_i dans l'intervalle, $km + r + 1$, peut donc être majoré par $(k+1)m \leq mN^{1-\alpha\lambda} = mN^\alpha$.

Finalement, en mettant bout à bout les majorations et en faisant le même travail pour les t_i négatifs, on obtient que $\psi(N)$ est un $\mathcal{O}(N^{1-\varepsilon})$.

De même, $\#\{t_0 \in \mathbf{Z}, |t_0| \leq N/\exists S, y_S(t_0) \in \mathbf{Q}\} = \#\bigcup_S\{t_0 \in \mathbf{Z}, |t_0| \leq N/y_S(t_0) \in \mathbf{Q}\}$ est un $\mathcal{O}(N^{1-\varepsilon'})$. Donc le complémentaire de cet ensemble dans $\mathbf{Z} \cap [-N, N]$ a un cardinal plus grand que $N - N^{1-\epsilon''}$ au voisinage de $+\infty$. On en conclut qu'il y a une infinité de spécialisations t_0 Q-acceptables, ce qui achève la preuve du fait que les spécialisations acceptables sont denses pour la norme usuelle.

Remarque : En fait, la même démonstration prouve que pour une famille finie de polynômes $P_i \in \mathbf{Q}[t, X]$ irréductibles, il y a une infinité dense de spécialisations acceptables pour tous les P_i en même temps. Il suffit, au lieu d'étudier les fonctions y_S d'un polynôme, d'étudier en même temps toutes les fonctions y_S de tous les P_i.

2.7 Généralisation dans $\mathbf{Q}[t_1, \ldots, t_r, X_1, \ldots, X_s]$

Nous nous contenterons de présenter la transformation de Kronecker qui permet (voir [Hadlock]) de faire cette généralisation.

Soit k un corps ; on note $\mathcal{P}(k, n, d)$ l'ensemble $\{f \in k[X_1, \ldots, X_n]/\forall i, \deg_{X_i} f < d\}$ et $\mathcal{Q}(k, n, d)$ l'ensemble $\{f \in k[Y]/\deg f \leq d^n - 1\}$. Alors,

$$\begin{aligned} \mathcal{P}(k, n, d) &\to \mathcal{Q}(k, n, d) \\ f(X_1, \ldots, X_n) &\mapsto \widehat{f} = f\left(Y, Y^d, Y^{d^2}, \ldots, Y^{d^{n-1}}\right) \end{aligned},$$

appelée transformation de Kronecker, est une bijection qui vérifie $\forall f, g \in \mathcal{P}(k, n, d), \widehat{fg} = \widehat{f}\widehat{g}$.

Grâce à cette transformation, on peut transposer un problème de réductibilité dans $k[X_1, \ldots, X_n]$ en un problème dans $k[Y]$.

Proposition 14 (Critère de Kronecker) *Soit $f \in \mathcal{P}(k, n, d)$. Alors, f est irréductible si et seulement si, pour toute factorisation $\widehat{f} = GH$ avec $\widehat{g} = G$ et $\widehat{h} = H$, on a $gh \notin \mathcal{P}(k, n, d)$.*

Références

[Lang] Serge Lang, *Algebra*, troisième édition révisée, Springer.

Pour la preuve du théorème de Hilbert

[Hadlock] C. R. Hadlock, *Field Theory and its classical problems*, Carus Mathematical Monographs, Mathematical Association of America, 1978, chapitre 4.

Pour les résultats sur les corps hilbertiens

[1] Schinzel, *Polynomials with special regard to reductiblity.*

Pour les théorèmes de Puiseux

[2] Jean-Marie Arnaudiès, *Séries entières, séries de Puiseux, séries de Fourier et compléments sur les fonctions presque périodiques*, Ellipses, 1999.

[3] Antoine Chambert-Loir, *Algèbre corporelle*, disponible sur Internet.