SÉMINAIRE N. BOURBAKI

SERGE LANG

Le théorème d'irréductibilité de Hilbert

Séminaire N. Bourbaki, 1960, exp. n° 201, p. 451-463

<http://www.numdam.org/item?id=SB_1958-1960__5__451_0>

Séminaire BOURBAKI
12e année, 1959/60, n° 201

Mai 1960

LE THÉORÈME D'IRRÉDUCTIBILITÉ DE HILBERT

par Serge LANG

Le cas essentiel du théorème de Hilbert est le suivant. Soient k un corps, A un sous-ensemble infini de k (dans la pratique, un anneau d'entiers par exemple), et $f(t , X)$ un polynôme à deux variables qu'on suppose irréductible quand on le considère comme polynôme en X à coefficients dans $k(t)$. On demande une infinité de valeurs t_o de t dans A telles que le polynôme $f(t_o , X)$ soit irréductible dans $k[X]$, et éventuellement une borne inférieure au nombre de tels t_o , ou une densité. La morale de l'histoire est que, s'il n'est pas évident a priori qu'on ne peut pas trouver une infinité de tels t_o , alors on peut démontrer qu'il en existe toujours bien assez pour tout ce qu'on veut en faire.

Le cas général du théorème de Hilbert, où l'on prend plusieurs paramètres $t_1 , \dots , t_r$ et plusieurs variables $X_1 , \dots , X_s$ se ramène au cas précédent formellement (ce que nous montrerons plus bas). Nous allons donc commencer par le cas essentiel .

Remarquons qu'on peut prendre $f(t , X)$ avec coefficients dans $k(t)$. En multipliant alors f par un polynôme en t , soit $\varphi(t)$, on ne change rien à la propriété d'irréductibilité. En outre, en divisant alors $f(t , X)$ par le plus grand commun diviseur (p. g. c. d.) de ses coefficients dans $k[t]$, on peut supposer que ceux-ci sont premiers entre eux, et donc que $f(t , X)$ est irréductible comme polynôme à deux variables sur k . (Remarque analogue pour plusieurs t et plusieurs X). La réciproque est vraie d'après le lemme de Gauss. Si les coefficients de f sont dans $k(t)$, on exclura toujours le nombre fini de t_o pour lesquels ces coefficients n'ont pas de sens. De même pour plusieurs variables.

1. Enoncé des théorèmes principaux.

Soit k un corps, et $f(t_1 , \dots , t_r , X_1 , \dots , X_s)$ un élément de $k(t)[X]$ (notation vectorielle pour t et X) qu'on suppose irréductible sur $k(t)$. Soit $U_{f,k}$ (qu'on écrit aussi U_f si aucune confusion n'est à craindre) le sous-ensemble de l'espace affine S_k^r formé des $(t'_1 , \dots , t'_r)$ avec $t'_1 \in k$ pour lesquels les coefficients de f sont définis, et tels que $f(t' , X)$ soit

irréductible sur k .

Les ouverts de Zariski et les U_f engendrent ce qu'on appelle la topologie de Hilbert sur S_k^r . On note que si $r = 1$, alors $S_k^1 = k$, et les ouverts de Zariski (distincts de $\emptyset$) sont les complémentaires des sous-ensembles finis de k .

Un corps sera dit hilbertien si l'intersection d'un nombre fini d'ouverts non vides de Zariski et d'ouverts du type U_f est infinie. Une telle intersection sera appelée un ouvert fondamental de S_k^r . Un sous-ensemble A de k sera dit hilbertien dans k si l'intersection d'un ouvert fondamental de k avec A est infinie. Un anneau (toujours supposé intègre dans ce qui suit) sera dit hilbertien s'il est hilbertien dans son corps de fractions.

Nous démontrerons les résultats suivants. D'abord pour le cas d'un t et d'un X :

L'anneau $\underset{\sim}{Z}$ des entiers est hilbertien. Si U est ouvert, non-vide dans $\underset{\sim}{Q}$, il existe un nombre réel $\alpha < 1$ tel que le nombre $N(B)$ des éléments de $U \cap \underset{\sim}{Z}$ qui sont $\leqslant B$ satisfait à l'inégalité

$$N(B) \geqslant B - B^{\alpha}$$

pour tout B suffisamment grand.

Tout ouvert non-vide est dense pour la topologie induite sur $\underset{\sim}{Q}$ par celle des réels (i. e. la topologie ordinaire) et pour toute topologie p-adique.

Soit k un corps quelconque, et soit w transcendant sur k . Alors l'anneau $k[w]$ est hilbertien. (Ce résultat sera d'ailleurs beaucoup précisé plus bas).

Soit k un corps, et soit E une extension finie séparable de k . Si k est hilbertien, E l'est aussi. Tout ouvert $U_{f,E}$ contient un ouvert $U_{g,k}$ avec g convenable (dépendant de f).

On notera que tous les résultats qui sont exposés ici sont dans la littérature (qui va du papier de Hilbert jusqu'à environ 1930) depuis 30 ans. Les références précises seront faites au fur et à mesure de l'exposé.

2. Réduction du problème à l'existence de points entiers sur des courbes.

Sauf mention expresse du contraire, nous considérons le cas d'un t et d'un X. Ecrivons :

$$f(t , X) = a_n(t)\, X^n + \ldots + a_o(t) \quad .$$

On peut supposer que les $a_i(t)$ sont des polynômes en t, et nous excluons le nombre fini de valeurs de t dans k qui annulent $a_n(t)$. On suppose f irréductible en X sur $k(t)$. Si f se factorise en $f(X) = a_n(t) \prod (X - \alpha_i)$ dans la clôture algébrique de $k(t)$, toute valeur t_o de t dans k détermine homomorphisme $k[t] \to k[t_o] = k$ qui se prolonge à l'anneau engendré par les racines $\alpha_1 , \ldots , \alpha_n$. L'image de ces racines est bien déterminée à une permutation près. Soient α_i' $(i = 1 , \ldots , n)$ ces images. Si l'on a une factorisation

$$f(t_o , X) = g_o(X)\, h_o(X)$$

dans $k[X]$, les coefficients de g_o et h_o sont des fonctions polynômes en les α_i'. Soient g, h les polynômes correspondant à ces fonctions qui donnent une factorisation

$$f(t , X) = g(X)\, h(X)$$

dans la clôture algébrique de $k(t)$. Comme f est supposé irréductible, l'un au moins des coefficients de g ou h n'est pas dans $k(t)$. Soit y ce coefficient. Alors l'anneau $k[t , y]$ est l'anneau affine d'une courbe C (qui peut être réductible) sur k. On voit que la factorisation $f(t_o , X) = g_o\, h_o$ donne lieu à un point rationnel (t_o , y_o) sur la courbe C qui se projette en t_o.

Si l'on écrit $f(t , X) = g(X)\, h(X)$ de toutes les manières possibles dans la clôture algébrique de $k(t)$, avec g et h de degrés $\geqslant 1$, il y aura chaque fois un coefficient qui n'est pas dans $k(t)$, d'où un nombre fini de courbes $C_1 , \ldots , C_s$. Toute valeur t_o dans k qui ne peut se remonter à un point rationnel d'aucune de ces courbes sera telle que $f(t_o , X)$ est irréductible dans $k[X]$.

Supposons que k soit corps de fractions d'un anneau A. Quitte à remplacer y par $\varphi(t)\, y$ avec un polynôme $\varphi(t)$ dans $A[t]$, on peut supposer y entier sur $A[t]$. En excluant le nombre fini des t_o tels que $\varphi(t_o)$ est nul, on voit que y_o et $\varphi(t_o)\, y_o$ sont rationnels ou irrationnels par rapport à k simultanément, mais s'ils sont dans k, alors $\varphi(t_o)\, y_o$ sera entier sur A, et donc

dans A si A est intégralement clos, ce qui est le cas dans la pratique.

Remarquons pour finir ce numéro, qu'on peut définir la topologie de Hilbert comme suit. Soit T la droite affine, et $f : C \to T$ un morphisme d'une courbe affine C, définie sur k. (On ne suppose pas forcément C irréductible). Soit $U_f = U_{f,k}$ l'ensemble des $t_o \in k$ tels qu'il existe un point $y_o \in C_k$ de C rationnel sur k tel que $f(y_o) = t_o$. Alors les U_f et les ouverts de Zariski définissent la topologie de Hilbert sur k. Remarque analogue pour plusieurs variables, où l'on considère des "revêtements" de l'espace affine S_k^r.

3. Courbes réductibles.

Considérons la courbe C d'anneau affine $k[t, y]$ sur le corps k. Si y n'est pas séparable sur $k(t)$, une puissance y^{p^m} le sera pour m grand. Excluons le cas où y^{p^m} est dans $k(t)$. Nous sommes ramenés au cas où y est séparable sur $k(t)$, et donc la clôture algébrique k_1 de k dans $k(t, y)$ est séparable sur k.

Si $k_1 \neq k$, alors l'anneau $k_1[t, y]$ détermine une courbe C_1 ayant une conjuguée C_1^σ distincte de C_1, si σ est un isomorphisme de k_1 sur k distinct de l'identité. Tout point rationnel de C dans k donne lieu à un point rationnel de C_1 et de C_1^σ dans k. Mais dans le plan affine, l'intersection des deux courbes distinctes C_1 et C_1^σ n'a qu'un nombre fini de points. Donc, dans le cas où C est réductible, il n'y a qu'un nombre fini de points rationnels (sous l'hypothèse de séparabilité de y).

4. Corps des nombres rationnels.

Nous considérons le cas où la courbe C est supposée irréductible, et définie sur $\mathbb{Q}$. Soit (t, y) un point générique de C sur $\mathbb{Q}$, et supposons $y \notin \mathbb{Q}(t)$. Quitte à remplacer y par $f(t)\,y$ où $f(t)$ est un polynôme dans $\mathbb{Z}[t]$, on peut supposer y entier sur $\mathbb{Z}[t]$, de sorte que si $t_o \in \mathbb{Z}$ s'étend à un point rationnel (t_o, y_o) de C dans $\mathbb{Q}$, alors y_o est forcément dans $\mathbb{Z}$.

Nous allons donner l'exposé et la méthode de DÜRGE [1]. La fonction algébrique y peut se développer en une série de puissances fractionnaires à l'infini

$$y = \varphi(t) = at^{n/e} + \ldots + b + c\,\frac{1}{t^{1/e}} + \ldots$$

avec $a, \ldots, b, \ldots, c, \ldots$ complexes. Le paramètre $t^{1/e}$ est choisi réel, quitte à multiplier les coefficients par une racine e-ième de l'unité. De toute

façon, s'il existe une fnfinité de valeurs de t tendant vers l'infini telles que $\varphi(t)$ soit réel, alors les coefficients de la série sont en fait réels. En effet, si l'un d'eux était complexe, prenons celui le plus à gauche, soit α. Pour t réel, tous les termes à gauche de α sont réels. L'angle du terme ayant α pour coefficient est $\neq 0$, π. Pour t tendant vers l'infini, le terme à coefficient α domine nettement la série à droite de ce terme. Donc il ne peut y avoir d'annulation, et pour $t \to \infty$ les valeurs de $\varphi(t)$ seraient complexes, contrairement à l'hypothèse.

Nous sommes donc ramenés au théorème suivant, qui n'a plus rien à voir avec l'algèbre :

THÉORÈME 1 (DÜRGE). - Soit $\varphi(t)$, une série de puissances à coefficients réels, méromorphe à l'infini en fonction du paramètre réel $1/t^{1/e}$. Supposons que $\varphi(t)$ ne soit pas dans $\underset{\sim}{R}[t]$, i. e. ne soit pas un polynôme en t. Supposons qu'il y ait une infinité d'entiers positifs

$$t_o < t_1 < t_2 < \dots$$

tels que $\varphi(t_i)$ soit entier (i. e. dans $\underset{\sim}{Z}$). Alors il existe un entier i_o, un entier $m > 0$, un nombre réel $\lambda > 0$ tels que pour tout $i > i_o$, on ait

$$t_{i+m} - t_i > t_i^{\lambda} \quad .$$

Autrement dit, les t_i sont très espacés. Du théorème 1, on tire facilement l'énoncé suivant, plus facile à manier.

COROLLAIRE. - Il existe un nombre réel $\alpha < 1$ tel que le nombre $N(B)$ des $t_i \leqslant B$ pour lesquels $\varphi(t_i)$ soit entier satisfait pour B suffisamment grand à l'inégalité

$$N(B) \leqslant B^{\alpha} \quad .$$

DÉMONSTRATION. - Choisissons $0 < \beta < 1$. Soit N_1 le nombre des entiers t_i tels que $t_i \leqslant B^{\beta} + 1$, et N_2 le nombre des t_i tels que $B^{\beta} < t_i \leqslant B$. Ecrivons $N_2 = sm + m_o$ avec $s \geqslant 0$ et $0 \leqslant m_o < m$. D'après la condition du théorème, on vérifie immédiatement par une estimation grossière que

$$B^{\beta} + sB^{\beta\lambda} \leqslant B \quad ,$$

d'où $s \leqslant B^{1-\beta\lambda}$ et donc $N(B) \leqslant N_1 + N_2 \leqslant B^{\beta} + 1 + m_o + mB^{1-\beta\lambda}$. Le nombre α du corollaire se voit maintenant immédiatement.

Pour démontrer le théorème 1, nous aurons besoin d'un lemme de la moyenne

dû à H. A. SCHWARZ.

LEMME. - Soit $\varphi(t)$ une fonction m fois continûment dérivable dans l'intervalle $t_i \leqslant t \leqslant t_{i+m}$. On suppose que $t_i < t_{i+1} < \ldots < t_{i+m}$ sont des nombres réels (pas forcément entiers). Alors il existe un nombre τ avec $t_i < \tau < t_{i+m}$ tel que

$$\frac{\varphi^{(m)}(\tau)}{m!} = \frac{\begin{vmatrix} 1 & t_i & t_i^2 & \ldots & t_i^{m-1} & \varphi(t_i) \\ & & \ldots & & & \\ 1 & t_{i+m} & t_{i+m}^2 & \ldots & t_{i+m}^{m-1} & \varphi(t_{i+m}) \end{vmatrix}}{V_m}$$

où V_m est le déterminant de Vandermonde.

(On voit donc que le numérateur diffère du dénominateur seulement par la dernière colonne).

DÉMONSTRATION. - Je dois la démonstration à Walter STRODT. Soit $F(t)$ la fonction

$$F(t) = \begin{vmatrix} 1 & t_i & t_i^2 & \ldots & t_i^{m-1} & \varphi(t_i) \\ & & \ldots & & & \\ 1 & t_{i+m-1} & t_{i+m-1}^2 & \ldots & & \varphi(t_{i+m-1}) \\ 1 & t & t^2 & \ldots & t^{m-1} & \varphi(t) \end{vmatrix}$$

Alors $F(t)$ s'annule en les m points $t_i, \ldots, t_{i+m-1}$. Avec une constante convenable C, la fonction

$$G(t) = F(t) - C(t - t_i)(t - t_{i+1}) \ldots (t - t_{i+m-1})$$

s'annule aussi en t_{i+m}, c'est-à-dire s'annule en $m + 1$ points. Donc $G^{(m)}(t)$ s'annule au moins en un point τ entre t_i et t_{i+m}. Mais $G^{(m)}(t) = F^{(m)}(t) - m!\,C$ (tous les autres termes s'annuleront). On déduit que

$$F^{(m)}(\tau) = m!\,C \quad .$$

Comme on le voit de suite, $F^{(m)}(\tau)$ aura un 0 dans tous les termes de la ligne du bas, sauf le dernier, qui sera $\varphi^{(m)}(\tau)$. Donc $F^{(m)}(\tau) = \varphi^{(m)}(\tau)\, V_{m-1}$ où V_{m-1} est le petit Vandermonde. Comme

$$C = \frac{F(t_{i+m})}{(t_{i+m} - t_i) \ldots (t_{i+m} - t_{i+m-1})}$$

et que $F(t_{i+m})$ n'est autre que le numérateur de l'expression dans l'énoncé du lemme, on voit que le lemme est démontré (compte-tenu du fait que V_{m-1} multiplié

par les produits ci-dessus est égal à V_m).

Appliquons notre lemme, en prenant pour m un entier tel que $\varphi^{(m)}(t)$ n'ait pas de termes négatifs en $1/t$, donc que son développement soit de la forme

$$\varphi^{(m)}(t) = \xi \frac{1}{t^{\lambda}} + \ldots$$

avec ξ réel. Comme φ n'est pas un polynôme en t , ou bien la série est infinie, et sa dérivée ne sera pas nulle, ou bien il y entre effectivement une puissance fractionnaire de t , et $\varphi^{(m)}$ ne sera de nouveau pas nulle. On pourra donc supposer $\xi \neq 0$ et $\lambda > 0$. Ce terme domine la série pour t grand. Donc pour i suffisamment grand, $\varphi^{(m)}(\tau) \neq 0$. Or le déterminant du numérateur dans le lemme est entier. On vient de voir que $\varphi^{(m)}(\tau)$ (et a fortiori $\varphi^{(m)}(\tau)/m!$) est petit, d'ordre de grandeur $t^{-\lambda}$). Ceci implique que V_m est grand. Mais V_m est un produit de différences des t_j , et on ne fait que l'agrandir en prenant

$$t_{i+m} - t_i$$

élevé à la puissance égale au nombre de termes dans ce produit, soit $\frac{m(m+1)}{2}$. On trouve donc

$$t_{i+m} - t_i > t_i^{\lambda'}$$

avec un λ' convenable, en prenant une racine $\frac{m(m+1)}{2}$ -ième.

Comme le remarque DÖRGE, l'énoncé vaut aussi pour une suite décroissante d'entiers négatifs. D'autre part, soit a un nombre rationnel. Considérons le polynôme $f(t , X)$ supposé irréductible. Alors

$$f(a + \frac{1}{t} , X)$$

est aussi irréductible. Des valeurs entières de t tendant vers l'infini qui rendent le polynôme spécialisé irréductible seront telles que $a + \frac{1}{t}$ est proche de a pour la topologie ordinaire, ce qui montre qu'un ouvert de Hilbert est dense. Astuce semblable pour la topologie p-adique, en prenant $f(a + tp^N , X)$ avec N grand. On étend immédiatement ceci à un corps de nombres.

5. Réductions au cas essentiel.

Nous montrons dans ce numéro comment on ramène le cas général (plusieurs t , plusieurs X) au cas essentiel. Ces réductions sont faites dans HILBERT ([3]) que nous copions. Nous supposons k hilbertien.

a. Un t , plusieurs X . Soit K un corps, $f(X_1 , \dots , X_n)$ un polynôme à coefficients dans K de degré $<d$ en chaque X_i . L'ensemble de ces polynômes est noté $P(n , d , K)$. La spécialisation de Kronecker S_d transforme f en un polynôme d'une variable, à savoir

$$S_d f(Y) = f(Y , Y^d , \dots , Y^{d^{n-1}}) \quad .$$

Si on a un monôme $X_1^{i_1} , \dots , X_n^{i_n}$, alors S_d appliqué à ce monôme donne

$$Y^{i_1+i_2 d+\dots+i_{n-1} d^{n-1}} \quad .$$

Compte tenu de l'expansion d-adique d'un entier $\geqslant 0$, on voit que S_d applique bijectivement $P(n , d , K)$ sur les polynômes dans $k[Y]$ de degré $\leqslant d^n - 1$. En outre, si f , g , et fg sont dans $P(n , d , K)$ alors

$$S_d(fg) = S_d(f) \, S_d(g) \quad .$$

Soit $f \in P(n , d , K)$ et supposons que $S_d f$ soit réductible,

$$S_d f(Y) = G(Y) \, H(Y) \quad .$$

On voit que le degré de G et H est $\leqslant d^n - 1$, et donc $G = S_d g$ et $H = S_d h$, avec g , h uniquement déterminés par G , H . On en déduit le critère de Kronecker :

f est irréductible dans K si et seulement si pour toute factorisation $S_d f = GH$ avec $G = S_d g$ et $H = S_d h$, le polynôme gh contient un terme monômial

$$\varphi X_1^{i_1} , \dots , X_n^{i_n}$$

avec $\varphi \in K$, $\varphi \neq 0$, de degré $\geqslant d$ pour l'un des X_i .

PROPOSITION 1. - Soit k un corps, $f(t , X_1 , \dots , X_n)$ un polynôme à coefficients dans k , de degré $<d$ en chaque X_i , et S_d la substitution de Kronecker. Soit

$$S_d f = \prod g_j(t , Y)$$

la factorisation de $S_d f$ dans $k(t)[X]$ en facteurs irréductibles en X . Alors, à l'exception d'un nombre fini de valeurs de t_o dans k , toute valeur t_o qui soit telle que chaque $g_j(t_o , Y)$ est irréductible dans k , est aussi telle que $f(t_o , X_1 , \dots , X_n) = f_o$ est irréductible dans k .

DÉMONSTRATION. - Sauf pour un nombre fini de t_o , on a

$$S_d f_o = \prod g_j(t_o , Y)$$

une factorisation de $S_d f_o$ en facteurs irréductibles dans k . Si l'on exclut encore un nombre fini de t_o (ceux qui annuleront le coefficient $\varphi(t)$ d'un monôme dans le critère de Kronecker), il est clair que f_o sera irréductible dans k .

b. Plusieurs t , plusieurs X . On considère le polynôme $f(t_1 , \ldots , t_r , X_1 , \ldots , X_s)$ comme un polynôme en t_1 et $r + s - 1$ variables $t_2 , \ldots , t_r , X_1 , \ldots , X_s)$. On spécialise alors t_1 et on continue inductivement.

c. Extension finie séparable.

PROPOSITION 2. - Soit E une extension finie séparable d'un corps k . Soit $f(t , X) \in E(t)[X]$ irréductible sur $E(t)$. On suppose que le coefficient du plus haut terme en X soit égal à 1 , et que si σ parcourt les monomorphismes de E sur k , les conjugués f^σ de f sont distincts. Posons :

$$F(t , X) = \prod_\sigma f^\sigma(t , X) \quad .$$

Alors $F(t , X)$ est dans $k(t)[X]$. A l'exclusion d'un nombre fini de $t_o \in k$ près, $F(t_o , X)$ est irréductible sur k si et seulement si $f(t_o , X)$ est irréductible sur E .

DÉMONSTRATION. - Par la théorie de Galois, $F(t , X)$ est dans $k(t)[X]$. Si on avait $F(t , X) = G(X) H(X)$, une factorisation sur $k(t)$, on peut supposer G et H ayant le plus haut coefficient égal à 1 . On conclut que $f(t , X)$ divise l'un des G ou H sur $E(t)[X]$, soit G . Mais alors f^σ divise G pour tout σ . Comme les f^σ sont supposés distincts, leur produit divise G , une contradiction. Si, maintenant, on choisit t_o dans k tel que $F(t_o , X)$ soit irréductible sur k , on conclut immédiatement que $f(t_o , X)$ le sera sur E , compte tenu de l'unique factorisation dans $E[X]$.

Pour appliquer la proposition 2, même au cas où les conjugués f^σ ne seraient pas distincts, il faut changer f légèrement. En effet, il existe un élément $\varphi = \varphi(t) \in E(t)$

$$g(t , X) = f(t , X + \varphi)$$

tel que tous les g^σ soient distincts. (Par exemple, le terme constant de g en X est $f(t , \varphi)$ et l'existence d'un φ tel que les $f(t , \varphi)^\sigma$ soient distincts est évidente : astuce de FRANZ). On peut alors appliquer la proposition 2 à $g(t , X)$, dont l'irréductibilité sur $E(t)$ est équivalente à celle de $f(t , X)$.

6. Extension transcendante pure.

Ce paragraphe est dû à FRANZ ([2]).

THÉORÈME 2. - Soit k un corps infini, et w transcendant sur k . Alors $k[w]$ est hilbertien. Soient t transcendant sur $k(w)$, et y séparable sur $k(w , t)$, mais pas dans $k(w , t)$. Soit U l'ouvert de Hilbert non-vide de $k(w)$ correspondant à (t , y) . Soit m entier $\geqslant 1$. Dans le plan (w , t) , il existe un ouvert de Zariski non-vide V , tel que pour tout $\lambda_o \in k$ (sauf un nombre fini dépendant de U , m , V) toutes les valeurs de t de la forme

$$t_o + \lambda_o (w - w_o)^m$$

avec $t_o , w_o \in k$ et $(t_o , w_o) \in V$ soient dans U .

DÉMONSTRATION. - Commençons par traiter le cas séparable. Quitte à multiplier y par un polynôme en w et t , on peut supposer que y est entier sur $k[w , t]$ (et même sur $A[w , t]$ si A est un sous-anneau de k dont k soit le corps de fractions). On considère donc la surface de point générique (w , t , y) définie sur k , qui est un revêtement du plan (w , t) .

Comme on a supposé y séparable sur $k(w , t)$, il existe une relation

$$\varphi(w , t) = P(w , t , Y) f(w , t , Y) + Q(w , t , Y) f'(w , t , Y)$$

si l'on désigne par $f(w , t , Y)$ le polynôme irréductible de y par rapport à $k[w , t]$ et par f' sa dérivée par rapport à Y , et par P , Q des polynômes dans $k[w , t , Y]$, $\varphi \in k[w , t]$. Par conséquent, si (w_o , t_o , y_o) est un point de la surface tel que $\varphi(w_o , t_o) \neq 0$, alors la surface est non-ramifiée au-dessus du point (w_o , t_o) dans le plan, et y admet une expression en série formelle :

$$y = \Sigma\, c_{ij} (t - t_o)^i (w - w_o)^j \quad ,$$

à coefficients dans $k(w_o , t_o , y_o)$.

Les zéros de $\varphi(w , t)$ déterminent un fermé de Zariski dont le complémentaire

est notre ouvert V . Dorénavant, on supposera toujours que (w_o , t_o) est dans V , et $w_o , t_o \in k$.

S'il n'existe aucun point (w_o , t_o , y_o) de la surface dans k au-dessus de (w_o , t_o) , alors, pour tout $\lambda_o \in k$, il n'y a pas de point de la courbe (t , y) dans $k(w)$ au-dessus de

$$t_o + \lambda_o(w - w_o)^m \quad .$$

En effet, un tel point aurait pour coordonnées des polynômes de $k[w]$, et l'homomorphisme appliquant $w \to w_o$ donnerait alors un point de la surface dans k au-dessus de (w_o , t_o) .

Supposons d'autre part, que (w_o , t_o , y_o) soit un point de la surface dans k . Si on substitue

$$\lambda(w - w_o)^m$$

pour $(t - t_o)$ dans la série, on obtient un homomorphisme de $k[w , t , y]$ dans $k[[w - w_o]]$. Il faut s'arranger pour que l'image de y ne soit pas dans $k[w - w_o] = k[w]$ (on sait que cette image sera entière sur $k[w]$), c'est-à-dire ne soit pas uh polynôme. Mis encore d'une autre façon, il faut que la série ne s'arrête pas.

Or y n'est pas un polynôme en w , t par hypothèse. Donc une infinité des c_{ij} ne sont pas nuls. On peut écrire

$$y_{\lambda,m} = \sum_{i,j} c_{ij} \lambda^i (w - w_o)^{mi+j}$$

$$= \sum_{\nu} c_\nu(\lambda)(w - w_o)^\nu \quad .$$

Chaque $c_\nu(\lambda)$ est un polynôme en λ , (considérant λ comme variable).

Si, pour une valeur λ_o de λ dans k , tous les $c_\nu(\lambda_o)$ sont nuls sauf un nombre fini, il s'ensuit que $y_{\lambda_o,m}$ (notation évidente) considéré comme fonction rationnelle de w a un pôle à l'infini $(w = \infty)$ d'ordre égal au plus grand ν tel que $c_\nu(\lambda_o)$ ne soit pas nul. Mais on a

$$f(w , t_o + \lambda_o(w - w_o)^m , y_{\lambda_o,m}) = 0 \quad .$$

Comme m est fixe, si l'on exclut encore un nombre fini de λ_o , on voit que l'ordre d'un pôle de $y_{\lambda_o,m}$ à l'infini est borné (en fonction des coefficients de f). Si l'on choisit un ν_1 plus grand que cette valeur critique, et tel que

$c_{\nu_1}(\lambda_o)$ ne soit pas identiquement nul (ce qui est possible puisqu'il y a une infinité de c_{ij} non nuls), toute valeur λ_o telle que $c_{\nu_1}(\lambda_o) \neq 0$ donne lieu à un $y_{\lambda_o,m}$ dont la série ne peut s'arrêter, car si elle s'arrêtait, on aurait un mauvais pôle. Cela termine notre démonstration dans le cas où y est séparable sur $k(w, t)$.

Pour le cas où y ne l'est pas, on considère une puissance y^{p^i} avec i grand. Ou bien cette puissance est encore irrationnelle sur $k(w, t)$, auquel cas on peut appliquer ce qu'on vient de faire, ou bien y est radiciel sur $k(w, t)$, et on a

$$y^{p^i} = \varphi(t, w)$$

avec $\varphi(t, w) \in k[w, t]$, $\varphi(t, w)$ n'étant pas une puissance p-ième dans $k[w, t]$. On distingue alors deux cas : celui où il apparaît une puissance de t ou w dans φ qui ne soit pas divisible par la caractéristique p, et celui où p divise l'exposant de t et w dans chaque terme de φ. Dans le deuxième cas, cela implique que l'un des coefficients de φ n'est pas une puissance p-ième.

Dans le premier cas, on trouve des m arbitrairement grands tels que, pour une substitution

$$t = t_o + \lambda_o(w - w_o)^m \quad ,$$

le polynôme en w contienne une puissance de w non divisible par p. (Après une translation, c'est essentiellement la substitution de Kronecker, $t = w^m$). Dans le second cas, le même genre de substitution pour m grand, i. e. $t = w^m$, préserve les coefficients dans k. Donc, si l'un d'eux n'est pas une puissance p-ième dans k, le polynôme en w qu'on obtient ne sera pas une puissance p-ième dans $k[w]$.

On remarquera qu'on a eu besoin de k infini pour faire marcher l'argument. Le théorème d'irréductibilité est encore valable pour k fini (pour le corps $k(w)$), mais il faut employer d'autres méthodes. Comme pour les rationnels, on peut alors compter le nombre de points dans un ouvert, mais cela conduit à de l'arithmétique plus profonde qui n'a pas sa place ici. Par exemple, des arguments à la SIEGEL ([5], notamment page 45) (qui s'était déjà rendu compte de l'effet de son théorème sur celui de Hilbert) ou des arguments à la NÉRON [4].

7. Application à la théorie de Galois.

Comme HILBERT ([3]), terminons cet exposé avec la remarque suivante : si k est un corps hilbertien, alors, chaque fois que $k(t_1 , \dots , t_r)$ est une extension transcendante pure, et K une extension galoisienne de groupe G sur $k(t_1 , \dots , t_r)$, on peut spécialiser les t en t' dans k de sorte que le groupe de décomposition reste du même ordre que celui de G , et on obtient donc une extension galoisienne de groupe G de k . (On prendra par exemple, un générateur y de K sur $k(t)$ qui soit entier sur $k[t]$, et t' tel que notre revêtement (t , y) de (t) soit non-ramifié au-dessus de t' , et du même degré).

BIBLIOGRAPHIE

[1] DÖRGE (Karl). - Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes, Math. Annalen, t. 96, 1927, p. 176-182.

[2] FRANZ (Wolfgang). - Untersuchungen zum Hilbertschen Irreduzibilitätssatz, Math. Z., t. 33, 1931, p. 275-293.

[3] HILBERT (David). - Über die Irreduzibilität ganzen rationaler Funktionen mit ganzzahligen Koeffizienten, J. reine und angew. Math., t. 110, 1892, p. 104-129.

[4] NÉRON (André). - Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique d'un corps, Bull. Soc. math. France, t. 80, 1952, p. 101-166.

[5] SIEGEL (Carl Ludwig). - Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss., 1929, p. 1-70.