Corps Hilbertien

Jianfeng Yao et Junyi Xie

Sous la direction de Philippe Gille

École Normale Supérieure

Juin 2009

Table des matières

1 Introduction

Le but de cet exposé est d'étudier les corps hilbertiens et de comprendre le problème de Noether. D'abord en utilisant la théorie élémentaire de Galois, on donnera la définition et les propriétés d'un corps hilbertien. Ensuite on essaie de montrer le théorème d'irréductibilité de Hilbert avec quelques outils en analyse et un peu de calculs. La démonstration présentée ici est due à Dörge. Enfin on s'intéresse au problème de Noether. On montrera le théorème de Fischer et le lemme sans nom.

On se propose de considérer les corps hilbertiens et de décrire le problème de Noether pour étudier le problème d'inverse de Galois : la construction de l'extension galoisienne de $\mathbb{Q}$ avec un certain groupe de Galois donné. Le théorème d'irréductibilité de Hilbert montre qu'il suffit d'étudier les groupes de Galois sur $\mathbb{Q}(x)$. Cela nous permet d'utiliser les méthodes de la théorie des surfaces de Riemann et de la géométrie algébrique. Hilbert a appliqué sa méthode pour obtenir les réalisations galoisiennes des groupes symétriques et alternés.

2 Corps hilbertiens

2.1 Notations

Tous les corps mentionnés sont de caractéristique 0. Si k est un sous-corps de K, on dit que K est régulier sur k si k est algébriquement clos dans K.

2.2 Résultats préliminaires

Lemme 2.1. *Supposons que $x_1, x_2 \dots x_m$ sont algébriquement indépendants sur k. Posons $x = (x_1, x_2 \dots x_m)$ et $\overline{k}$ la clôture algébrique de k.*

1. *Si $k^{'}/k$ est une extention galoisienne finie, alors $k^{'}(x)/k(x)$ l'est aussi. De plus, la restriction $Gal(k^{'}(x)/k(x)) \to Gal(k^{'}/k)$ est un isomorphisme. En particulier, tous les corps entre $k(x)$ et $k^{'}(x)$ sont de la forme $k^{''}(x)$ avec $k \subseteq k^{''} \subseteq k^{'}$ et $[k^{''}(x) : k(x)] = [k^{''} : k]$.*
2. *Soit $f(x, y) \in k(x)[y]$ irréductible sur $k(x)$. Posons $K = k(x)[y]/(f)$, alors K est régulier sur k si et seulement si f est irréductible sur $\overline{k}(x)$. Dans ce cas f est irréductible sur $k_1(x)$ pour toute extension k_1 de k telle que $x_1, x_2 \dots x_m$ et y sont algébriquement indépendants sur k_1.*

Démonstration. 1) $x_1, x_2 \dots x_m$ étant fixés, le groupe $G = Gal(k^{'}/k)$ agit naturellement sur $k^{'}(x)$ avec le corps invariant $k(x)$. D'après le théorème d'Artin (qui dit que si G est un groupe fini d'automorphismes d'un corps K, alors K est galoisienne sur le corps invariant F de G et $\mathrm{Gal}(K/F) = G$), $k^{'}(x)/k(x)$ est galoisienne avec le groupe de Galois G. La dernière partie de 1 est vérifiée d'après le théorème de Galois.

2) On suppose que f est irréductible sur $\overline{k}(x)$. Notons $\widehat{k}$ la clôture algébrique de k dans K et α l'image de y dans K. $k \subseteq \widehat{k} \subseteq K = k(x)(\alpha)$, alors $k(x) \subseteq \widehat{k}(x) \subseteq K$. Comme f est irréductible sur $\overline{k}(x)$, f est irréductible sur $\widehat{k}(x)$. On en déduit que $[K : \widehat{k}(x)] = degf = [K : k(x)]$. Donc $\widehat{k}(x) = k(x)$. D'où $\widehat{k} = k$ par 1.

Inversement on suppose que K est régulier sur k (i.e. $\widehat{k} = k$). Soit $k^{'}$ une extension galoisienne finie sur k. $k(x) \subseteq k^{'}(x) \cap K \subseteq k^{'}(x)$. Par 1 il exsite un corps $k^{''}$ tel que $k \subseteq k^{''} \subseteq k^{'}$ et $k^{'}(x) \cap K = k^{''}(x)$. Le fait que $k^{''}(x) \subseteq K$ implique $k^{''} \subseteq K$. Il s'ensuit que $k \subseteq k^{''} \subseteq \widehat{k} = k \subseteq K$. Donc $k = k^{''}$ et $K \cap k^{'}(x) = k(x)$. D'après 1 l'extension $k^{'}(x)/k(x)$ est galoisienne finie. On a alors $[k^{'}(x)(\alpha) : k^{'}(x)] = [K : k(x)]$. Donc f est irréductible sur $k^{'}(x)$. f est bien irréductible sur $\overline{k}(x)$.

Pour la derinière affirmation, on montre par l'absurde. On suppose que $f = gh$ où g et $h \in k_1(\mathrm{x})[\mathrm{y}]$ de degré au moins 1 en y. Sans perte de généralité, g est unitaire en y. On note k_1 le corps qui est engendré par les coefficients de g (où g est considérée comme une fraction rationnelle en $x_1, x_2 \dots x_m, y$) et t l'un des coefficients tel que t est transcendant sur k. Alors il existe $k_2 = k(t_1, t_2 \dots t_s)$ où $t_1 = t$ et $t_1, t_2 \dots t_s$ sont algébriquement indépendants sur k tel que k_1/k_2 soit fini. Soit $\alpha_c \in Gal(k_2/k)$ tel que $\alpha_c(t) = t + c$ avec c $\in k$ et fixe $t_2 \dots t_s$. Tous les α_c peuvent être prolongés dans $Gal(\overline{k}_2/k)$. Comme $f = gh$ on a alors $\alpha_c(f) = \alpha_c(g)\alpha_c(h)$. Donc $f = \alpha_c(g)\alpha_c(h)$ et $\alpha_c(g) | f$ car α_c agit sur $\overline{k}_2(x)[y]$ en fixant $x_1, x_2 \dots, y$. On sait que $\alpha_c(g)$ est unitaire en y, donc f a une infinité de diviseurs unitaires distincts $\alpha_c(g)$ avec c $\in k$. On obtient une contradiction.

□

Lemme 2.2. *On se donne α un entier algébrique sur le corps L. Soit $f(y) = \sum_{i=0}^{n} a_i y^i$ un polynôme sur L de degré $n > 0$ avec $f(\alpha) = 0$. Alors*

$$g(Y) = Y^n + \sum_{i=0}^{n-1} a_i a_n^{n-i-1} Y^i$$

est un polynôme unitaire de degré n avec $g(a_n\alpha) = 0$ et $L(\alpha) = L(a_n\alpha)$.

Démonstration. C'est clair. □

Lemme 2.3. *Soit $f(x_1, x_2 \dots x_s)$ un polynôme en $s \geq 2$ variables de degré au moins 1 en x_s . Alors f est irréductible comme un polynôme en s variables si et seulement si f est irréductible et primitif comme un polynôme en x_s sur l'anneau $D = k[x_1, x_2 \dots x_{s-1}]$. Notons que f est irréductible sur D si et seulement si f est irréductible sur $k(x_1, x_2 \dots x_{s-1})$*

Démonstration. On suppose que f est irréductible et primitif comme un polynôme en x_s sur D. Si $f = gh$ avec g et h 2 polynômes en s variables. Alors l'un des deux polynôme , disons g est en x_1,...,x_{s-1}. Comme f est primitif, il suit que g est inversible sur D, donc $g \in k$. Cela montre que f est irréductible en s variables. La réciproque est claire. Pour la deuxième partie, c'est juste le lemme de Gauss.

□

2.3 Définition d'un corps hilbertien

Dans ce paragraphe, on va donner plusieurs définitions équivalentes d'un corps hilbertien. On utilise les lemmes suivants.

Lemme 2.4. *Soit K/F une extension galoisienne finie avec le groupe de Galois G. Soit R un sous-anneau de F ayant F comme son corps de fractions. Soit α un générateur de K sur F et vérifie $f(\alpha) = 0$ où $f(y) \in R[y]$ est un polynôme unitaire de degré $n = [K : F]$. Notons A un sous-ensemble fini de K contenant α et invariant par G. Posons $S = R[A]$. Alors il existe $u \neq 0$ dans R tel que pour tout homomorphisme ω de R dans un corps F' vérifiant $\omega(u) \neq 0$, les propriétés suivantes sont vérifiées :*

1. *ω peut s'étendre en un homomorphisme $\widetilde{\omega} : S \to K'$, où K' est une extension finie de F'. On peut supposer que $K' = F'(\widetilde{\omega}(S))$.*
2. *Pour un tel $\widetilde{\omega}$, le corps K' est une extention galoisienne sur F' et est engendré par $\alpha' = \widetilde{\omega}(\alpha)$ sur F'. Alors on a $f'(\alpha') = 0$ où $f'(y) \in F'[y]$ est le polynôme obtenu en appliquant ω aux coefficients de f. De plus $[K' : F'] = [K : F]$ si et seulement si f' est irréductible. Dans ce cas, K' est isomorphe à $F'[y]/(f')$.*
3. *Dans le cas où f' est irréductible. Pour chaque $\widetilde{\omega}$ décrit comme dans 1, il y a un unique isomorphisme de G dans $G' = Gal(K'/F')$, $\sigma \to \sigma'$ tel que $\widetilde{\omega}(\sigma(s)) = \sigma'(\widetilde{\omega}(s))$ pour tout $\sigma \in G$ et $s \in S$.*

Démonstration. L'extension K/F étant galoisienne, le polynôme $f(y)$ est séparable. Alors son discriminant $D_f \neq 0$ dans R. De plus, on note $\omega(D_f)$ le discriminant de polynôme $f'(y)$ obtenu en appliquant ω aux coefficients de f. On peut seulement considérer les ω avec $\omega(D_f) \neq 0$. Alors $f'(y)$ est séparable.

L'idéal I de $R[y]$ enrendré par f est le noyau de l'application $R[y] \to R[\alpha]$, $h \to h(\alpha)$. Si $h \in R[y]$ avec $h(\alpha) = 0$, il existe $g \in F[y]$ tel que $h = gf$. Comme f est unitaire en y, $g \in R[y]$. Donc $h \in I$. On a alors un isomorphisme naturel

$$\phi : R[y]/I \to R[\alpha].$$

Etape 1 D'abord on peut envisager le cas particulier où $R[A] = R[\alpha]$. On veut montrer que $1), 2), 3)$ sont vrais pour chaque homomorphisme $\omega : R \to F'$ avec $\omega(D_f) \neq 0$. On prolonge ω en un homomorphisme $R[y] \to F'[y]$ (y étant fixé). On obtient un homomorphisme naturel

$$\psi : R[y]/I = R[y]/fR[y] \to F'[y]/f'F'[y] = F'[y]/(f').$$

Posons

$$\chi = \psi \circ \phi^{-1} : R[\alpha] \to F'[y]/(f').$$

(1) Notons $K' = F'[y]/(g')$ avec g' un facteur irréductible de f'. Alors K' est une extension finie de F'. En composant χ avec l'homomorphisme naturel $F'[y]/(f') \to F'[y]/(g') = K'$, on obtient un homomorphisme $\widetilde{\omega} : S = R[\alpha] \to K'$. L'assertion (1) est vérifiée.

(2) On a $K' = F'[\widetilde{\omega}(S)] = F'[\widetilde{\omega}(\alpha)] = F'[\alpha']$ car $S = R[\alpha]$. Les conjugués de α sur F, notés $\alpha_1, \alpha_2 \dots \alpha_n$, sont tous dans $A \subseteq S$. Posons $\alpha'_1, \alpha'_2 \dots \alpha'_n$ ces images par $\widetilde{\omega}$. Alors $f'(y) = \widetilde{\omega}(f(y)) = \widetilde{\omega}((y-\alpha_1)(y-\alpha_2)\dots(y-\alpha_n)) = (y-\alpha'_1)(y-\alpha'_2)\dots(y-\alpha'_n)$. Donc K' contient tous les conjugués de α' sur F' et de plus est normal sur F'. On sait que K'/F' est séparable car f' l'est. On en déduit que l'extension K'/F' est galoisienne. Le reste de 2 est clair.

(3) Supposons que f' soit irréductible. Alors $\alpha'_1, \alpha'_2 \dots \alpha'_n$ sont les conjugués deux à deux distincts sur F' car f' est séparable. Pour chaque $i \in 1, 2 \dots n$, il y a un unique $\sigma'_i \in G'$ tel que $\sigma'_i(\alpha) = \alpha'_i$. C'est-à-dire qu'il y a un unique $\sigma_i \in G$ tel que $\sigma_i(\alpha) = \alpha_i$. On définit $\theta : G \to G'$ par $\theta(\sigma_i) = \sigma'_i$ pour tout $i \in 1, 2 \dots n$. Alors θ est une bijection.

Pour chaque $s \in S = R[\alpha]$, il existe $h \in R[y]$ tel que $s = h(\alpha)$. Posons $h' = \widetilde{\omega}(h) \in F'[y]$ (y étant invariant par $\widetilde{\omega}$). Alors pour tout $s \in S$, $\sigma_i \in G$

$$\sigma'_i(\widetilde{\omega}(s)) = \sigma'_i(\widetilde{\omega}(h(\alpha))) = \sigma'_i(h'(\alpha')) = h'(\alpha'_i) = \widetilde{\omega}(h(\alpha_i)) = \widetilde{\omega}(\sigma_i(h(\alpha)) = \widetilde{\omega}(\sigma_i(s)).$$

En particulier

$$(\sigma\tau)'(\alpha') = (\sigma\tau)'(\widetilde{\omega}(\alpha)) = \widetilde{\omega}(\sigma\tau(\alpha)) = \sigma'(\widetilde{\omega}(\tau(\alpha))) = \sigma'\tau'(\widetilde{\omega}(\alpha)) = \sigma'\tau'(\alpha).$$

D'où $(\sigma\tau)' = \sigma'\tau'$. Donc θ est un homomorphisme. On en déduit qu'il est un isomorphisme.

Etape 2 Dans le cas général, chaque $a \in A$ est de la forme

$$a = \sum_{i=0}^{n-1} b_i \alpha^i$$

avec $b_i \in F$. En particulier, posons $a = \sum_{i=0}^{n-1} b_i^a \alpha^i$ avec $b_i^a \in F$ pour tout $a \in A$. Il est possible de choisir $v \neq 0$ dans R tel que $v b_i^a \in R$ pour tout $a \in A$ et $i \in 1, 2 \ldots n-1$ car F est le corps de fractions de R et A est fini. On note $u = vD_f$ et $\widetilde{R} = R[u^{-1}]$. Alors tous les $b_i^a \in \widetilde{R}$. Il s'ensuit que $A \subseteq \widetilde{R}[\alpha]$ et donc $\widetilde{R}[A] = \widetilde{R}[\alpha]$

Soit $\omega : R \to F^{'}$ est un homomorphisme avec $\omega(u) \neq 0$. Alors ω s'étend uniquement en un homomorphisme $\widetilde{R} \to F^{'}$. Donc il existe $K^{'}$ une extension finie de $F^{'}$ et $\widetilde{\omega} : \widetilde{R} \to K^{'}$ qui prolonge ω. Comme $K^{'} = F^{'}(\widetilde{\omega}(\widetilde{R}[\alpha]))$ et $\omega(1/u) = 1/\omega(u) \in F$,

$$K^{'} = F^{'}(\widetilde{\omega}(\widetilde{R}[A, 1/u])) = F^{'}(\widetilde{\omega}(R[A]), \widetilde{\omega}(1/u)) = F^{'}(\widetilde{\omega}(S)).$$

On applique l'étape 1 à $\widetilde{R}$. Cela achève la preuve.

□

Remarque 2.5. Ce lemme est encore vrai pour un corps de caractéristique quelconque.(voir Völklein [5])

Lemme 2.6. *Soient L un corps et $f(x,y) \in L[x,y]$ un polynôme séparable en y sur $L(x)$. Alors $f(b,y) \in L[y]$ est séparable pour presque tous les $b \in L$ (i.e. $f(b,y) \in L[y]$ est séparable sauf un nombre fini de $b \in L$).*

Démonstration. D'après le lemme 2.2, on peut supposer que f est unitaire en y. Son discriminant $D(x) \in L[x]$ est non nul car f est séparable en y. Pour chaque $b \in L$, le discriminant de $f(b,y) \in L[y]$ est $D(b)$. Donc $f(b,y)$ est séparable pour tout $b \in L$ qui n'est pas une racine de $D(x)$.

□

Proposition 2.7. *Soit K une extension galoisienne de $k(x)$ de degré $n > 1$. S'il existe un polynôme $f(x,y) \in k[x,y]$ unitaire de degré n en y et α un générateur de K sur $k(x)$ tel que $f(x,\alpha) = 0$, alors*

1. *Pour presque tout $b \in k$, si $f_b(y) := f(b,y)$ est irréductible dans $k[y]$, alors le corps $k[y]/(f_b)$ est galoisienne sur k dont le groupe de Galois est isomorphe à $G = G(K/k(x))$.*
2. *Soit l une extension finie de k contenue dans K. On suppose que $h(x,y) \in l(x,y)$ est irréductible comme un polynôme en y sur $l(x)$ et les racines de $h(x,y)$ sont dans K. Pour presque tout $b \in k$, si $f(b,y)$ est irréductible dans $k[y]$, alors $h(b,y)$ est irréductible dans $l[y]$.*
3. *Il existe un nombre fini de polynômes $P_I(x,y) \in k[x][y]$, irréductibles de degré > 1 en y tels que pour presque tout $b \in k$, si chaque $P_I(b,y)$ n'a pas de racine sur k, alors $f(b,y)$ est irréductible dans $k[y]$.*

Démonstration. Chaque générateur α de K sur $k(x)$ est une racine d'un polynôme $f(y)$ de degré n sur $k(x)$. En multipliant un certain élément de $k[x]$, on peut considérer $f = f(x,y)$ comme un polynôme en 2 variables. D'après le lemme 2.2 on peut supposer que

f est unitaire en y. Alors $f(x) = (y-\alpha_1)(y-\alpha_2)\dots(y-\alpha_n)$ où $\alpha_1, \alpha_2 \dots \alpha_n$ sont les conjugués de α sur $k(x)$.

(1) Pour $b \in k$, posons $\omega_b : k[x] \to k$ l'évaluation en b (i.e $h(x) \to h(b)$). On applique le lemme 2.4 avec $F = k(x)$, $K = K$, $R = k[x]$, $A = \{\alpha_1, \alpha_2 \dots \alpha_n\}$, $F^{'} = k$ et $\omega = \omega_b$, $S = R[A]$. Alors il existe u[x] tel que pour chaque b verifiant $u(b) \neq 0$ (i.e $\omega_b(u) \neq 0$), ω_b peut être prolongé en $\widetilde{\omega}_b : k[x][\alpha_1, \alpha_2 \dots \alpha_n] \to K^{'} = k(\widetilde{\omega}(S))$. Si $f_b = \omega_b(f)$ est irréductible, alors $K^{'} = k[y]/(f_b)$ et $Gal(K^{'}/k) = Gal(K/k(x))$. Comme pour presque tout $b \in k$, $u(b) \neq 0$, on obtient (1).

On suppose maintenant que $u(b) \neq 0$.

(3) Notons I un sous-ensemble propre non vide de $\{1, 2 \dots n\}$. Comme f est irréductible comme un polynôme en y sur $k(x)$, le produit $\prod_{i \in I}(y - \alpha_i)$ ne se situe pas dans $k(x)[y]$. Alors il a quelques coefficients $d_I \in k(x)$. On en déduit que $d_I \in S$ car $\alpha_i \in S$ pour $i = 1, 2 \dots n$. Et d_I verifie un polynôme irréductible P_I sur $k(x)$ de degré >1. On peut choisir P_I pour que les coefficients de P_I soient dans $k[x]$.

Si f_b n'est pas irréductible, il y a un certain I comme ci-dessus tel que $\prod_{i \in I}(y - \alpha_i^{'}) \in k[y]$. Posons $c = \widetilde{\omega}_b(d_I)$. Alors $c \in k$ et $P_I(b, c) = \widetilde{\omega}(P_I(d_I)) = 0$. Donc (3) est établi.

(2) Soit $h(x, y) = h_0(x) \prod_{i=1}^{t}(y - \beta_i)$ avec $h_0 \in l[x]$ et $\beta_i \in K$. Posons

$$A = \{\alpha_1, \alpha_2 \dots \alpha_n\} \cup \{\beta_1, \beta_2 \dots \beta_t\} \cup \{\text{tous les conjugués de } \gamma_1, \gamma_2 \dots \gamma_s\}$$

où $l = k(\gamma_1, \gamma_2 \dots \gamma_s)$. D'après le lemme 2.4 pour presque tout $b \in k$, ω_b peut être prolongé en $\widetilde{\omega}_b : S = k[x][A] \to K^{'}$.

On suppose que f_b est irréductible, alors $K^{'} = k[y]/(f_b)$. Comme $l \subseteq S$, $\widetilde{\omega}_b$ est isomorphe à un sous-corps de $K^{'}$ que l'on identifie avec l (via $\widetilde{\omega}_b$). Via cette identification on a :

$$h(b, y) = h_0(b) \prod_{i=1}^{t}(y - \beta_i^{'}).$$

Posons $H = G(K/l(x))$. Alors pour tout s $\in l$ et tout $\sigma \in H$, on a $\sigma^{'}(s) = \sigma^{'}(\widetilde{\omega}_b(s)) = \widetilde{\omega}_b(\sigma(s)) = \widetilde{\omega}_b(s) = s$. On en déduit que $\sigma^{'} \in G(K^{'}/l)$. h étant irréductible comme un polynôme en y sur $l(x)$, il est séparable et le groupe H permute ses racines β_i transitivement. Alors $H^{'} = \{\sigma^{'} | \sigma \in H\}$ permute $\beta_i^{'}$ transitivement. Pour presque tout $b \in k$, on a $h_0(b) \neq 0$ et $h(b, y)$ séparable. Alors le groupe $H^{'} \subseteq G(K^{'}/l)$ permute ses racines β_i transitivement. Donc $h(b, y)$ est irréductible sur l. □

Corollaire 2.8. *Les conditions suivantes sur k sont équivalentes :*

1. *Pour chaque polynôme $f(x, y)$ irréductible en 2 variables sur k de degré ≥ 1 en y, il y a une infinité de $b \in k$ tel que $f(b, y)$ est irréductible comme un polynôme en y.*
2. *Si l/k est une extension finie et $h_1(x, y), h_2(x, y) \dots h_m(x, y) \in l[x][y]$ sont irréductibles comme les polynômes en y sur $l(x)$, alors il y a une infinité de $b \in k$ tel que $h_1(b, y), h_2(b, y) \dots h_m(b, y)$ sont irreductibles dans $l[y]$.*
3. *Si $P_1(x, y), P_2(x, y) \dots P_r(x, y) \in k[x, y]$ sont irréductibles de degré>1 comme un polynôme en y sur $k(x)$, il y a une infinité de $b \in k$ tel que tout le $P_i(b, y)$ n'a pas de racine dans k.*

Démonstration. (2) $\Rightarrow$ (3) : Posons $l = k, h_1 = P_1, h_2 = P_2 \dots h_t = P_t$.

(1) $\Rightarrow$ (2) : Soit K une extention galoisienne finie de $k(x)$ telle que $h_1(x,y), h_2(x,y) \dots h_m(x,y)$ sont réductibles et $l(x) \subseteq K$. Alors il existe $\alpha \in K$ tel que $K = k(x)(\alpha)$ avec le polynôme minimal $f(x,y) \in k[x,y]$. D'après la proposition 2.7(2) et la condition (1), il y a une infinité de $b \in k$ tel que $h_1(b,y), h_2(b,y) \dots h_m(b,y)$ soient irréductibles dans $l[y]$.

(3) $\Rightarrow$ (1) : C'est une application de la propsition 2.7(3). Comme tous les $P_l(x,y) \in k[x,y]$ sont irréductibles, il y a un nombre infini de $b \in k$ tel que tout le $P_l(b,y)$ n'a pas de racine dans k. Alors il y a une infinité de $b \in k$ tel que $f(b,y)$ soit irréductible comme un polynôme en y. □

Définition 2.9. Un corps k est dit hilbertien s'il vérifie l'un des 3 conditions du corollaire 2.8.

2.4 Les propriétés d'un corps hilbertien

Lemme 2.10. *Si k est hilbertien et $f(x_1, x_2 \dots x_s)$ est un polynôme irréductible en $s \geq 2$ variables sur k de degré ≥ 1 en x_s. Alors :*

1. *Il y a une infinité de $b \in k$ tel que $f(b, x_2 \dots x_s)$ (en $s-1$ variables) est irréductible sur k.*
2. *Si $p \in k[x_1, x_2 \dots x_s]$ n'est pas nul, il existe $b_1, b_2 \dots b_{s-1}$ tels que $p(b_1, b_2 \dots b_{s-1}) \neq 0$ et $f(b_1, b_2 \dots b_{s-1}, x_s)$ est irréducible comme un polynôme en x_s.*

Démonstration. (1) On se donne d un entier plus grand que la plus grande puissance de toutes les variables présentes dans f. Notons $S_d f(x,y) = f(x, y, y^d \dots y^{(d^{s-2})})$. Il est de la forme

$$S_d f(x,y) = g(x) \prod_i g_i(x,y)$$

où $g_i(x,y)$ est irréductible de degré ≥ 1 en y et $g(x) \in k[x]$. Comme k est hilbertien, il y a une infinité de $b \in k$ tel que tous les $g_i(b,y)$ soient irréductibles. Prenons seulement tels b à partir de maintenant. Et on suppose de plus que $g(b) \neq 0$.

Si $f(b, x_2 \dots x_s) = h(b, x_2 \dots x_s) h'(b, x_2 \dots x_s)$ où h et h' ne sont pas constantes. $S_d h(y)$ et $S_d h'(y)$ sont définis de la même façon. On a $S_d f(b,y) = S_d h(y) S_d h'(y)$. Donc $S_d h(y)$ et $S_d h'(y)$ sont à la fois les produits de certains $g_i(b,y)$ (à un facteur près sur k). Notons $H(x,y)$ et $H'(x,y)$, les produits de $g_i(x,y)$ correspondants. Alors

$$S_d f(x,y) = g(x) H(x,y) H'(x,y).$$

En utilisant l'unicité de la décomposition d-adique, on a deux polynômes uniques $\widetilde{h}(x_1, x_2 \dots x_s)$ et $\widetilde{h'}(x_1, x_2 \dots x_s)$ tels que $S_d \widetilde{h} = gH$ et $S_d \widetilde{h'} = H'$ et la plus grande puissance de $x_2 \dots x_s$ présente dans $\widetilde{h}$, $\widetilde{h'}$ est plus petite que d. Si la plus grande puissance de $\widetilde{f} := \widetilde{h}\widetilde{h'}$ est aussi plus petit que d, on a $\widetilde{f} = f$ d'après l'unicité de la décomposition d-adique. Donc $\widetilde{f} = \widetilde{h}\widetilde{h'}$ avec $\widetilde{h}$ et $\widetilde{h'}$ ne sont pas constants. Cela contredit le fait que f est irréductible.

Donc $\widetilde{f}$ contient un monôme $\kappa(x_1)x_2^{i_2}\dots x_s^{i_s}$ avec un certain $i_\nu \geq d$ et $\kappa \neq 0$. Comme $\widetilde{h}(b, x_2 \dots x_s)$ (resp $\widetilde{h'}(b, x_2 \dots x_s)$) est un multiple de $h(x_2 \dots x_s)$ (resp h'), $\widetilde{f}(b, x_2 \dots x_s)$ est un multiple de $f(b, x_2 \dots x_s)$. Donc $\kappa(b) = 0$.

Il y a un nombre fini de possibilités pour κ (à un éléments de k près) correspondant à toutes les décompositions $S_d f = gHH'$. Si on choisit b distinct de ces racines dans κ, alors $f(b, x_2 \dots x_s)$ est irréductible.

(2) On montre par récurrence sur s. Le cas où $s = 2$ est juste (1). Supposons que c'est vrai jusquà $s-1$. Alors p est un polynôme en $x_2 \dots x_s$ à coefficients dans $k[x_1]$. Par (1) il existe $b_1 \in k$ tel que $f'(x_2 \dots x_s) := f(b_1, x_2 \dots x_s)$ est irréducible et pour certains coefficients $c_j(b_1) \neq 0$ de p. Donc $p'(x_2 \dots x_s) := p(b_2, x_2 \dots x_s)$ n'est pas nul. On applique maintenant l'hypothèse de récurrence, il existe $b_2 \dots b_{s-1} \in k$ tels que $p'(b_2, x_2 \dots x_s) \neq 0$ et $f'(x_2 \dots x_s)$ est irréductible. Ainsi $(b_1, b_2 \dots b_{s-1})$ convient. □

Corollaire 2.11. *Si k est hilbertien, alors chaque extension engendrée par un nombre fini d'éléments l'est aussi.*

Démonstration. 1) Dans le cas où F est une extension transcendante pure et engendrée par un nombre fini d'éléments, on suppose que $F = k(x_1, x_2 \dots x_m)$ avec $x_1, x_2 \dots x_m$ algébriquement indépendants sur k. Notons $D = k[x_1, x_2 \dots x_m]$. Soit $f(x, y) \in F[x, y]$ est irreductible de degré ≥ 1 en y. On peut supposer que $f \in D[x_1, x_2 \dots x_m, x, y]$ est irréductible d'après le lemme 2.3. Donc il y a une infinité de $b \in k$ tel que $f(x_1, x_2 \dots x_m, b, y)$ soient irréductibles par le lemme 2.10. Alors il est irréductible en y sur F. Finalement F est hilbertien.

2) Soit K/k une extension engendrée par un nombre fini d'éléments. Il existe F une extension décrite dans (1) telle que K/F soit fini. F est hilbertien par 1. D'après la définition 2.9 et corollaire 2.8(2), chaque extension finie sur un corps hilbertien est encore un corps hilbertien. Donc K est hilbertien.

□

Théorème 2.12. *Supposons k est hilbertien. Si G est un groupe de Galois fini d'une certaine extension sur $k(x_1, x_2 \dots x_m)$. Alors G est un groupe de Galois d'une certaine extension sur k.*

Démonstration. Le cas $m = 1$ est claire par la proposition 2.7(1).

Si $m > 1$, $k(x_1, x_2 \dots x_m) = k(x_1, x_2 \dots x_{m-1})(x_m)$. Comme $k(x_1, x_2 \dots x_{m-1})$ est hilbertien, on peut se ramener au cas $m = 1$. □

3 $\mathbb{Q}$ est hilbertien

Dans le deuxième chapitre, on a déjà vu la définition et les propriétés d'un corps hilbertien. Dans ce chapitre, on va démontrer que $\mathbb{Q}$ est un corps hilbertien en utilisant la caractérisation du corollaire 2.8(3). On s'intéresse aux racines des polynômes. On étudie plutôt les points où un certain méromorphe prend les valeurs entières.

3.1 Aspect analytique

Théorème 3.1 (Théorème des fonctions implicites). *Soit $f(x,y) \in \mathbb{C}[x,y]$ de degré $n \geq 1$ en y. Soit $c_0 \in \mathbb{C}$ tel que $\frac{\partial f}{\partial y}(c_0,b) \neq 0$ pour toutes les racines b de $f(c_0,y)$. Alors il existe un voisinage V de c_0 et des fonctions holomorphes ψ_1,...,ψ_n définies sur V telles que pour tout $c \in V$, $f(c,y)$ a n racines distinctes $\psi_1(c)$,...,$\psi_n(c)$.*

Remarque 3.2. La condition $\frac{\partial f}{\partial y}(c_0,b) \neq 0$ est équivalente à dire que f(c_0, y) $\in \mathbb{C}$[y] est un polyôme séparable.

Démonstration. Il suffit de montrer le résultat pour une racine. Soit b une racine de $f(c_0,y)$. Posons $f(x_1+iy_1, x_2+iy_2) = f_1(x_1,y_1,x_2,y_2) + if_2(x_1,y_1,x_2,y_2)$. f étant holomorphe par rapport à chaque variable, la relation de Cauchy-Riemann s'écrit $\frac{\partial f_1}{\partial x_2} = \frac{\partial f_2}{\partial y_2}$, $\frac{\partial f_1}{\partial y_2} = -\frac{\partial f_2}{\partial x_2}$. La matrice jacobienne est

$$\begin{vmatrix} \frac{\partial f_1}{\partial x_2} & \frac{\partial f_2}{\partial x_2} \\ \frac{\partial f_1}{\partial y_2} & \frac{\partial f_2}{\partial y_2} \end{vmatrix} = (\frac{\partial f_1}{\partial x_2})^2 + (\frac{\partial f_1}{\partial y_2})^2 = |\frac{\partial f}{\partial y}|^2.$$

Par hypothèse, $\frac{\partial f}{\partial y}|_{(c_0,b)} \neq 0$. Donc d'après le théorème des fonctions implicites, il existe ψ_1, ψ_2 de classe C^1 telles que dans un voisinage V de (c_0,b)

$$f_1(x_1,y_1,\psi_1(x_1,y_1),\psi_2(x_2,y_2)) = 0.$$

$$f_2(x_1,y_1,\psi_1(x_1,y_1),\psi_2(x_2,y_2)) = 0.$$

De plus, $\frac{\partial f}{\partial y} \neq 0$ dans V. On dérive par rapport à x_1 (resp y_1) dans la première équation (resp la deuxième). On obtient :

$$1)\quad \frac{\partial f_1}{\partial x_1} + \frac{\partial f_1}{\partial x_2}\frac{\partial \psi_1}{\partial x_1} + \frac{\partial f_1}{\partial y_2}\frac{\partial \psi_2}{\partial x_1} = 0$$

$$2)\quad \frac{\partial f_2}{\partial y_1} + \frac{\partial f_2}{\partial x_2}\frac{\partial \psi_1}{\partial y_1} + \frac{\partial f_2}{\partial y_2}\frac{\partial \psi_2}{\partial y_1} = 0$$

En utilisant la formule de Cauchy-Riemann, on fait (1)−(2) et on a :

$$\frac{\partial f_1}{\partial x_2}(\frac{\partial \psi_1}{\partial x_1} - \frac{\partial \psi_2}{\partial y_1}) + \frac{\partial f_1}{\partial y_2}(\frac{\partial \psi_2}{\partial x_1} + \frac{\partial \psi_1}{\partial y_1}) = 0 \text{ (a)}$$

.

De même, on obtient :

$$\frac{\partial f_1}{\partial y_1}+\frac{\partial f_1}{\partial x_2}\frac{\partial \psi_1}{\partial y_1}+\frac{\partial f_1}{\partial y_2}\frac{\partial \psi_2}{\partial y_1}=0$$

$$\frac{\partial f_2}{\partial x_1}+\frac{\partial f_2}{\partial x_2}\frac{\partial \psi_1}{\partial x_1}+\frac{\partial f_2}{\partial y_2}\frac{\partial \psi_2}{\partial x_1}=0.$$

En sommant les deux équations, on a :

$$-\frac{\partial f_1}{\partial y_2}(\frac{\partial \psi_1}{\partial x_1}-\frac{\partial \psi_2}{\partial y_1})+\frac{\partial f_1}{\partial x_2}(\frac{\partial \psi_2}{\partial x_1}+\frac{\partial \psi_1}{\partial y_1})=0 \text{ (b)}.$$

En combinant (a) et (b), on a un système de Cramer et le déterminant non nul. Alors $\frac{\partial \psi_1}{\partial x_1}=\frac{\partial \psi_2}{\partial y_1}$ et $\frac{\partial \psi_2}{\partial x_1}=-\frac{\partial \psi_1}{\partial y_1}$. Donc $\psi=\psi_1+i\psi_2$ convient.

□

3.2 Valeurs entières des fonctions méromorphes

Définition 3.3. Soit M $\subset \mathbb{N}$ On dit que M est *mince* s'il existe k $\in]0,1[$ tel que

$$Card(M\cap\{1,2...N\})\leq N^k$$

pour presque tout N.

Remarque 3.4. Il est clair qu'un ensemble fini est mince. Plus généralement, une réunion finie d'ensembles minces est mince.

On a besoin d'une généralisation à m points du théroème des valeurs intermédiaires. Il est dû à H.A. Schwarz.

Lemme 3.5. *Soient $s_0<s_1<...<s_m$ avec $m\geq 1$. On se donne $\chi(s)$, une fonction réelle définie sur $[s_0,s_m]$ de classe C^m. Notons V_m le déterminant de Vandermonde :*

$$V_m=\begin{vmatrix}1 & s_0 & s_0^2 & \cdots & s_0^m\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & s_m & s_m^2 & \cdots & s_m^m\end{vmatrix}=\prod_{0\leq j<i\leq m}(s_i-s_j)$$

Alors il existe $\sigma\in]s_0,s_m[$ tel que

$$\frac{\chi^{(m)}(\sigma)}{m!}=\frac{1}{V_m}\begin{vmatrix}1 & s_0 & \cdots & s_0^{m-1} & \chi(s_0)\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & s_m & \cdots & s_m^{m-1} & \chi(s_m)\end{vmatrix}.$$

Démonstration. Soit F(s) la fonction définie par

$$F(s) = \begin{vmatrix} 1 & s_0 & \cdots & s_0^{m-1} & \chi(s_0) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & s_{m-1} & \cdots & s_{m-1}^{m-1} & \chi(s_{m-1}) \\ 1 & s & \cdots & s^{m-1} & \chi(s) \end{vmatrix}$$

Notons

$$c = \frac{F(s_m)}{(s_m - s_0)...(s_m - s_{m-1})}$$

et

$$G(s) = F(s) - c(s - s_0)...(s - s_{m-1}).$$

La fonction G(s) s'annule en $s = s_0, ..., s_m$. Donc par le théorème de Rolle, $G^{(m)}$(s) s'annule au moins une fois dans $]s_0, s_m[$. Comme $G^{(m)}(s) = F^{(m)}(s) - m!c$, il existe $\sigma \in]s_0, s_m[$ tel que

$$F^{(m)}(\sigma) = m!c$$

D'autre part, en développant le déterminant F(s) par rapport à la dernière ligne, on a

$$F(s) = \sum_{i=0}^{m-1} c_i s^i + V_{m-1}\chi(s)$$

où les c_i sont constantes (qui ne dependent que de $s_0, ..., s_{m-1}$) et V_{m-1} est le déterminant de Vandermonde de $s_0, ..., s_{m-1}$. D'où

$$F^{(m)}(\sigma) = V_{m-1}\chi^{(m)}(\sigma).$$

En comparant les deux expressions on obtient

$$\frac{\chi^{(m)}(\sigma)}{m!} = \frac{c}{V_{m-1}} = \frac{F(s_m)}{(s_m - s_0)...(s_m - s_{m-1})V_{m-1}} = \frac{F(s_m)}{V_m}.$$

Par la définition de F(s_m),le résultat en découle. □

Théorème 3.6. *Soient $i_0 \in \mathbb{Z}$ et*

$$\phi(t) = \sum_{k=i_0}^{\infty} a_i t^i$$

une série de Laurent à coefficients complexes et convergente dans un voisinage de 0. Notons B, l'ensemble des $b \in \mathbb{N}$ tel que $\phi(1/b)$ soit un entier. Alors $B(\phi)$ est mince sauf si presque tous les a_i sont nuls (i.e. les a_i sont nuls à partir d'un certain rang).

Démonstration. : La démonstration se fait en plusieurs étapes. Soit $\phi(t)$ une fonction comme dans le théorème 3.6 et on suppose que les a_i ne sont pas presque tous nuls et montre par l'absurde. Supposons que B(ϕ) soit infini car si c'est fini, la remarque 3.4 conclut. Alors on a :

Etape 1 Les coefficients a_i sont réels.

Démonstration. La série

$$\bar{\phi}(t) = \sum_{i=i_0}^{\infty} \bar{a}_i t^i$$

a le même rayon de convergence que ϕ. On a $\bar{\phi}$ (1/b) = ϕ(1/b) pour tout b ∈ B(ϕ). Comme B(ϕ) est infini, par le principe des zéros isolés on en déduit que $\bar{\phi} = \phi$. Cela montre le lemme. □

Ensuite on considère la fonction réelle χ(s) : = $\phi(s^{-1})$ definie sur $\mathbb{C}^*$. On a

$$\chi(s) = \sum_{i=i_0}^{\infty} a_i s^{-i}$$

Etape 2 Montrer qu'il existe $\lambda > 0$ et m , S ∈ $\mathbb{N}$ satisfaisant la propriété suivante : Si $s_0, ..., s_m \in \mathbb{Z}$ avec $\chi(s_0)$,..., $\chi(s_m) \in \mathbb{Z}$ et $S < s_0 < ... < s_m$ alors

$$s_m - s_0 \geq s_0^{\lambda}.$$

Démonstration. Pour m assez grand la série

$$\chi^{(m)}(s) = \sum_{i=\mu}^{\infty} d_i s^{-i}$$

n'a que des termes de puissance négative. i.e. $\mu > 0$. Les d_i sont réels et on peut supposer que $d_\mu \neq 0$ car ϕ n'est pas un polynôme. Alors $s^\mu \chi^{(m)}$(s) tend vers d_μ quand s tend vers plus l'infini. Donc il existe $S_1 > 0$ tel que $0 < |s^\mu \chi^{(m)}(s)| < |2d_\mu|$ pour s ≥ S_1.

On suppose maintenant que $S_1 < s_0 < ... < s_m$ et on prend σ comme dans le lemme 3.5. Alors $\frac{V_m \chi^{(m)}(\sigma)}{m!}$ = F(s_m) est un entier non nul, donc sa valeur absolue est non nulle. On en déduit l'inégalité

$$V_m \geq \frac{m!}{|\chi^{(m)}(\sigma)|} \geq \frac{1}{|\chi^{(m)}(\sigma)|}$$

et

$$(s_m - s_0)^{m(m+1)/2} \geq V_m \geq \frac{1}{|\chi^{(m)}(\sigma)|} \geq \frac{1}{|2d_\mu|}\sigma^\mu \geq \frac{1}{|2d_\mu|}s_0^\mu.$$

D'où

$$s_m - s_0 \geq (\frac{1}{|2d_\mu|})^{2/m(m+1)} s_0^{2\mu/m(m+1)}.$$

De plus, il existe S_2 tel que $(\frac{1}{|2d_\mu|})^{2/m(m+1)} S_2^{\mu/m(m+1)} \geq 1$. Donc si l'on prend S = max(S_1, S_2), $\lambda = \mu/m(m+1)$, on a :

$$(\frac{1}{|2d_\mu|})^{2/m(m+1)} s_0^{\mu/m(m+1)} \geq 1$$

et

$$s_m - s_0 \geq s_0^{\mu/m(m+1)} = s_0^{\lambda}$$

D'où le résultat. □

Etape 3 Soient $b_1 < b_2 < ...$ une suite des entiers positifs avec $b_{i+1} - b_i \geq b_i^\lambda$ pour $\lambda > 0$. Alors l'ensemble $B = \{b_1, b_2, ...\}$ est mince.

Démonstration. On se donne un entier positif N. Soit m le nombre de $b_i \in B$ avec $\sqrt{N} < b_i \leq$ N. Alors en notant p= inf$\{i, b_i \in [|\sqrt{N}, N|]\}$, on a :

$$(m-1)\sqrt{N}^\lambda \leq b_{m+p-1} - b_p \leq N.$$

Il suit que $(m-1)\sqrt{N}^\lambda \leq$ N, d'où

$$m - 1 \leq N^{1-\lambda/2}.$$

Donc

$$|B \cap \{1, 2...N\}| \leq \sqrt{N} + m \leq \sqrt{N} + N^{1-\lambda/2} + 1.$$

Cela implique que B est mince. □

Finalement on a :

Etape 4 $B(\phi)$ est mince.

Démonstration. On rappelle que $B(\phi)$ contient les entiers b tels que χ(b) (= $\phi(1/b)$) est un entier. On supprime les entiers plus petits que S dans B où S est défini dans l'étape 2. Par l'étape 2, le reste de l'ensemble peut s'écrire comme une union de m sous-ensembles $B_1, ..., B_m$ qui satisfont la condition de l'étape 3. Ces ensembles sont minces par l'étape 3. Donc B(ϕ) est mince par la remarque 1.4. □

Cela termine la preuve. □

3.3 Théorème d'irréductibilité de Hilbert

Maintenant on va montrer le résultat central.

Lemme 3.7. *Soit $p(x, y) \in \mathbb{Q}[x][y]$ irréductible sur $\mathbb{Q}(x)$ et de degré $r > 1$ en y. Alors pour presque tout $x_0 \in \mathbb{Z}$ on a :*

(a) Il existe $\varepsilon > 0$ et des fonctions holomorphes $\psi_1(t), ..., \psi_r(t)$ définies pour les complexes t avec $|t| < \varepsilon$ telles que $\psi_1(t), ..., \psi_r(t)$ sont les racines du polynôme $p(x_0 + t, y) \in \mathbb{Q}[y]$.

(b) Si un certain $\psi_i(t)$ est une fraction rationnelle à coefficients complexes, alors il y a un nombre fini de $q \in \mathbb{Q}$ tel que $\psi_i(q) \in \mathbb{Q}$.

(c) Soit $B(p, x_0)$ l'ensemble des $b \in \mathbb{N}$ tel que $p(x_0 + \frac{1}{b}, c)$=0 pour certain $c \in \mathbb{Q}$. Alors $B(p, x_0)$ est mince.

Démonstration. Le polynôme p est irréductible, donc séparable sur $\mathbb{Q}$(x). Donc p(x_0,y) est séparable pour presque tout $x_0 \in \mathbb{Z}$ (lemme 2.6). On considère un tel x_0 dans la suite.

(a) C'est le théorème 3.1.

(b) Soit $\psi := \psi_i$ une fraction rationnelle en t. Alors p(x_0 + t, ψ(t)) est identiquement nul. Donc p(x_0+ x, ψ(x)) = 0 sur $\mathbb{Q}$(x) pour x un nombre transcendant sur $\mathbb{C}$. Puisque ψ(x) $\in \mathbb{C}$(x) est algébrique sur $\mathbb{C}$(x), donc sur $\bar{\mathbb{Q}}$(x). Mais $\bar{\mathbb{Q}}$(x) est algébriquement clos dans $\mathbb{C}$(x) par le lemme 2.1. On en déduit que ψ(x) $\in \bar{\mathbb{Q}}$(x).

Soit $\beta \in$ Gal($\bar{\mathbb{Q}}/\mathbb{Q}$). On considère la fraction rationnelle ψ^β obtenue en appliquant β aux coefficients de ψ. Alors ψ^β(q) = ψ(q) pour tous q $\in \mathbb{Q}$ avec ψ(q) $\in \mathbb{Q}$. S'il y a une infinité de q, on en déduit que $\psi^\beta = \psi$ pour tout β. Donc les coefficients de ψ sont dans $\mathbb{Q}$. Ainsi ψ(x − x_0) $\in \mathbb{Q}$(x) est un zéro de p(x, y) sur $\mathbb{Q}$(x). Cela contredit le fait que p est irréductible sur $\mathbb{Q}$(x). D'où le résultat.

(c) On peut supposer que p(x, y) $\in \mathbb{Z}$[x, y]. Notons

$$p(x,y) = \sum_{k=0}^{r} p_i(x) y^i$$

avec p_i(x) $\in \mathbb{Z}$[x]. Pour R suffisamment grand ,

$$x^R p(x_0 + \frac{1}{x}, y) = \sum_{k=0}^{r} x^R p_i(x_0 + \frac{1}{x}) y^i$$

est un élément de $\mathbb{Z}$[x, y]. Notons ces coefficients par $\hat{p_i}$(x). Alors h(x) : = $\hat{p_r}$(x) est un élément non nul de $\mathbb{Z}$[x]. On définit aussi

$$\hat{p}(x,Z) = Z^r + \sum_{i=0}^{r-1} \hat{p_i}(x) h(x)^{r-i-1} Z^i$$

un élément de $\mathbb{Z}$[x, Z], unitaire en Z.

Supposons que $p(x_0 + \frac{1}{b}$, c) = 0 pour $c \in \mathbb{Q}$, $b \in \mathbb{Z}$. Alors $\hat{p}(b, h(b)c) = 0$. Comme $\hat{p}$(b, Z) $\in \mathbb{Z}$[Z] est unitaire, $h(b)c$ est un entier sur $\mathbb{Z}$. Donc $h(b)c \in \mathbb{Z}$.

De plus, si $|1/b| < \epsilon$, alors c = ψ_i(1/b) pour un certain i = 1,..,r. Donc $h(b)\psi_i$(1/b) $= h(b)c \in \mathbb{Z}$.

Soit ϕ_i(t) = h(t^{-1})ψ_i(t) pour $0 < |t| < \epsilon$ et i = 1,..,r. L'argument précédent montre que si b $\in$ B(p, x_0) et 1/b $< \epsilon$, alors ϕ_i(1/b) = h(b)ψ_i(1/b) $\in \mathbb{Z}$ pour certains i = 1,..,r. B(p, x_0) est contenu dans l'union de B(ϕ_i). Par le théorème 3.6, l'ensemble B(ϕ_i) est mince si ϕ_i n'est pas une fraction rationnelle. Or si ϕ_i est une fraction rationnnelle, alors B(ϕ_i) est fini par (b). Par la remarque 3.2, B(p, x_0) est mince. Donc (c) en découle.

□

Théorème 3.8 (Théorème d'irréductibilité de Hilbert)**.** *Q est hilbertien.*

Démonstration. On se donne p_j(x, y) $\in \mathbb{Q}$[x][y] comme la condition (3) dans la définition. On peut choisir $x_0 \in \mathbb{Z}$ comme dans le lemme 3.7. Soit C l'ensemble des $b \in \mathbb{N}$ tel que les polynômes $p_j(x_0 + \frac{1}{b}$, y) n'ont pas de racines dans $\mathbb{Q}$. Notons l'ensemble B le complémentaire de C dans $\mathbb{N}$. Alors B est l'union de B(p_j, x_0). B(p_j, x_0) est mince par Lemme 3.7(c). Donc B est mince. Donc son complémentaire C est infini. Cela achève la démonstration. □

Exemple 3.9. On considère le polynôme avec les coefficients $1, x_1, .., x_n$

$$f(y) = y^n + x_1 y^{n-1} + ... + x_n = \prod_{i=1}^{n} (y - t_i).$$

comme un polynôme en y sur $k(x_1, ..., x_n)$. Alors les racines sont aussi algébriquement indépendantes sur k. Donc l'action naturelle du groupe symétrique S_n on $t_1, ...t_n$ peut être prolongé en une action de S_n sur $k(t_1, ..., t_n)$. Le corps invariant F par S_n contient $x_1, ..., x_n$ et $[k(t_1, ..., t_n) : F]$=$|S_n|$=n !. D'autre part, comme $t_1, ..., t_n$ sont les racines d'un polynôme de degré n sur $k(x_1, ..., x_n)$, on a $[k(t_1, ...t_n) : k(x_1, ..., x_n)] \leq$ n !. Il suit que $F = k(x_1, ..., x_n)$. D'où par le théorème d'Artin,

$$Gal(k(t_1, ..., t_n)/k(x_1, ..., x_n)) = S_n.$$

Donc si k est un corps hilbertien, S_n est un groupe de Galois d'une cartaine extension sur k par le théorème 2.12. En particulier, on obtient la réalisation galoisienne de S_n sur $\mathbb{Q}$.

4 Le problème de Noether

On s'intéresse maintenant au problème suivant :

Problème de Noether : Soit V un $\mathbb{Q}$-espace vectoriel de dimension finie. On suppose qu'un groupe fini G agit $\mathbb{Q}$-linéairement et fidèlement sur V. Est-il vrai que le corps invariant $\mathbb{Q}(V)^G$ est une extension transcendante pure de $\mathbb{Q}$?

Théorème 4.1 (Fischer 1905). *Soit k un corps algébriquement clos de caractéristique 0. On suppose qu'un groupe abélien fini A agit k-linéairement et fidèlement sur un k-espace vectoriel V de dimension finie. Alors le corps $k(V)^A$ est une extension transcendante pure de k.*

Démonstration. Comme k est algébriquement clos et de caractéristique 0, la représentation sur V est semi-simple et le k[A]-module V se décompose en somme directe des sous-k[A]-module V_i de dimension 1 tels que sur V_i l'action est donnée par σ(v)= $\chi_i(\sigma)$v pour un certain caractère χ_i : A $\rightarrow$ k*. Soit v_i un vecteur non nul de V_i et soit X le sous groupe de k(V)* engendré par les v_i. Comme les v_i sont linéairement indépendants, X est un groupe abélien libre.

Soit $\hat{A}$= Hom(A, k*) le groupe de caractères et on considère l'homomorphisme ϕ : X $\rightarrow \hat{A}$ défini par $v_i \rightarrow x_i$. Par construction, on a σ(x)=(ϕ(x)(σ))x pour x $\in$ X et $\sigma \in$ A. En particulier, en notant Y := ker(ϕ) on obtient que Y $\subset k(V)^A$. D'autre part, le degré de Y dans X est plus petit que $|\hat{A}|$=|A|, donc [k(V) : k(Y)] $\leq$ |A|. Or [k(V) : $k(V)^A$]=|A| car c'est une extension galoisienne de groupe de Galois A. On en déduit que k(Y)= $k(V)^A$. Comme Y est un groupe abélien libre car X l'est, on a k(Y) = k($y_1, .., y_m$) pour une base $y_1, .., y_m$ de Y. Cela montre le résultat.

□

Remarque 4.2. Il suffit de supposer seulement que k contient toutes les $|A|$-ièmes racines de l'unité.

Lemme 4.3 (Speiser)**.** *Soit K/k est une extension galoisienne finie avec le groupe de Galois G. Soit V un $K-$espace vectoriel sur lequel G agit (i.e. $\sigma(\lambda v)=\sigma(\lambda)\sigma(v)$ pour tout $\sigma\in G$, $\lambda\in K$, $v\in V$). Soit $\phi : V\otimes_k K\to V$ définie par $\phi(v\otimes_k\lambda)=\lambda v$. Alors $\phi|_{V^G\otimes_k K}$ est un isomorphisme.*

Démonstration. On note $\widetilde{K}=K$, un corps sur lequel G agit trivialement. Alors G agit sur $K\otimes_k\widetilde{K}$ avec l'action $\sigma(\lambda\otimes_k\mu)=\sigma(\lambda)\otimes_k\mu$. On prend $\alpha\in K$ un générateur de K avec le polynôme minimal f. Donc $K=k[x]/(f)$. On a alors $K\otimes_k\widetilde{K}=k[x]/(f)\otimes_k\widetilde{K}=\widetilde{K}[x]/(f)=\widetilde{K}[x]/\prod_{\sigma\in G}(x-\sigma(\alpha))=\oplus_{\sigma\in G}Ke_\sigma$. Ici on identifie $f(\alpha)\otimes_k\lambda=\sum_{\sigma\in G}\lambda f(\sigma(\alpha))e_\sigma$. Posons $\pi : K\otimes_k\widetilde{K}\to K$ définie par $\pi(\lambda\otimes_k\mu)=\lambda\mu$. Alors pour tout $\omega\in K\otimes_k\widetilde{K}$,

$$e_{id}\omega=\pi(\omega)e_{id}.$$

En particulier $e_{id}=e_{id}e_{id}=\pi(e_{id})e_{id}$. Donc $\pi(e_{id})=1$. Pour tout $a\otimes_k b\in K\otimes_k\widetilde{K}$ et $v\otimes_k\lambda\in V\otimes_k\widetilde{K}$, on a $\phi(a\otimes_k b\cdot v\otimes_k\lambda)=\phi(av\otimes_k b\lambda)=ab\lambda v=\pi(a\otimes_k b)\phi(v\otimes_k\lambda)$ On en déduit que $\phi(\omega y)=\pi(\omega)\phi(y)$. Soit G agissant sur $V\otimes_k K$ avec l'action $\sigma(v\otimes_k\lambda)=\sigma(v)\otimes_k\lambda$. Alors $(V\otimes_k\widetilde{K})^G=V^G\otimes_k\widetilde{K}$. Donc $V\otimes_k\widetilde{K}$ est un $K\otimes_k\widetilde{K}$-module et $e_\sigma e_\tau=\delta_{\sigma,\tau}e_\sigma$. Il s'ensuit que $V\otimes_k\widetilde{K}=\oplus_{\sigma\in G}e_\sigma(V\otimes_k\widetilde{K})$. Donc tous les éléments de $\omega\in V\otimes_k K$ sont de la forme $\sum_{\sigma\in G}e_\sigma y_\sigma$ avec $y_\sigma\in V\otimes_k K$. Pour tout $\sigma,\tau\in G$ $\omega\in(V\otimes_k\widetilde{K})^G\iff\tau(\omega)=\omega\iff\sum_{\sigma\in G}e_\sigma\tau(y_\sigma)=\sum_{\sigma\in G}e_\sigma y_\sigma\iff e_\sigma y_\sigma=\tau(e_{\tau^{-1}\sigma}y_{\tau^{-1}\sigma})\iff e_\sigma y_\sigma=\sigma(e_{id}y_{id})\iff\omega=\sum_{\sigma\in G}\sigma(e_{id}y_{id})$. ω est bien de la forme $\sum_{\sigma\in G}\sigma(e_{id}y)$.

Notons $W=e_{id}V\otimes_k\widetilde{K}$ et on définit $P:(V\otimes_k\widetilde{K})^G\to W$ par $P(\omega)=e_{id}y=e_{id}\sum_{\sigma\in G}\sigma(e_{id})y=e_{id}\omega$ et $Q:W\to(V\otimes_k\widetilde{K})^G$ par $Q(e_{id}y)=\sum_{\sigma\in G}\sigma(e_{id}y))$. On trouve facilement que $Q\circ P=id_{(V\otimes_k\widetilde{K})^G}$ et $P\circ Q=id_W$. Alors P est un isomorphisme et vérifie $\phi|_{(V\otimes_k\widetilde{K})^G}=\phi\circ P$ car $\phi\circ P(\omega)=\phi(e_{id}\omega)=\pi(e_{id})\phi(\omega)=\phi(\omega)$.

Ensuite on définit $\psi:V\to W$ par $\psi(v)=e_{id}(v\otimes_k 1)$. Alors $\phi\circ\psi(v)=\phi(e_{id}(v\otimes_k 1))=\pi(e_{id})\phi(v\otimes_k 1)=v\ \forall v\in V$. D'où $\phi\circ\psi=id_V$. Or pour tout $v\otimes\lambda\neq 0$ dans $V\otimes_k\widetilde{K}$, $\psi\circ\phi|_W(e_{id}(v\otimes\lambda))=\psi(\lambda v)=e_{id}(\lambda v\otimes_k 1)=e_{id}(\lambda\otimes_k\lambda^{-1})(v\otimes_k\lambda)=\pi(\lambda\otimes_k\lambda^{-1})e_{id}(v\otimes_k\lambda)=e_{id}(v\otimes_k\lambda)$. D'où $\psi\circ\phi|_W=id_W$. Finalement $\phi|_W$ est un isomorphisme et $\phi|_{V^G\otimes_k\widetilde{K}}$ est un isomorphisme.

□

Lemme 4.4. *Soit K/k est un extension galoisienne finie avec le groupe de Galois G. Soit V un $K-$espace vectoriel de dimension m sur lequel G agit fidèlement et satisfaisant pour tout $\lambda\in K$, $v\in V$, $\sigma\in G$, $\sigma(\lambda v)=\sigma(\lambda)\sigma(v)$. Alors il existe $t_1,t_2\dots t_m$ algébriquement indépendants tels que $(K(V))^G\cong k(t_1,t_2\dots t_m)$.*

Démonstration. D'après le lemme précédent $(K(V))^G\cong(K(K\otimes_k V^G))^G$. On en déduit que $dim_k V^G=dim_K K\otimes_k V^G=dim_K V=m$. Donc on prend $(v_1,v_2\dots v_m)$ une $k-base$ de V^G. Alors $(1\otimes_k v_1,1\otimes_k v_2\dots 1\otimes_k v_m)$ est une $K-base$ de $V=K\otimes_k V^G$.

Posons $t_i=1\otimes_k v_i$ pour $i=1,2\dots m$. Alors $K(K\otimes_k V^G)=K(t_1,t_2\dots t_m)$. Comme G fixe $t_1,t_2\dots t_m$, $(K(V))^G\cong K^G(t_1,t_2\dots t_m)=k(t_1,t_2\dots t_m)$. On conclut que $(K(V))^G\cong k(t_1,t_2\dots t_m)$.

□

Lemme 4.5 (Lemme sans Nom)**.** *Soient G un groupe fini. V (resp. W) un k-espace vectoriel de dimension n(resp. m). De plus on suppose que G agit fidèlement sur V et W. Alors* $k(V \oplus W)^G \backsimeq k(V)^G(t_1, t_2 \dots t_m)$ *où* $t_1, t_2 \dots t_m$ *sont algébriquement indépendants.*

Démonstration. On applique le lemme 4.4 en posant $K^{'}/k' = k(V)/k(V)^G$, $V^{'} = k(V) \otimes_k W$. Alors $dim_{K^{'}}V^{'} = dim_{k(V)}k(V) \otimes_k W = dim_k W = m$. Donc il existe $t_1, t_2 \dots t_m$ algébriquement indépendants tels que $k(V \oplus W)^G = (k(V)(k(V) \otimes_k W))^G \backsimeq k(V)^G(t_1, t_2 \dots t_m)$. □

La réponse au problème de Noether ne dépend donc essentiellement pas de la représentation fidèle choisie de G.

5 Conclusion

Emmy Noether était intéressé par ce problème qui est lié au théorème d'inverse de Galois. C'est une conséquence du théorème d'irréductibilité de Hilbert. Si c'était vrai, cela entraînerait qu'il y aurait une infinité de familles de l'extension galoisienne sur $\mathbb{Q}$ avec le groupe de Galois G obtenu par la spécialisation $t_i \to a_i$(cf. le théorème 2.12). Cependant, la réponse peut être négative même pour un groupe cyclique G. Swan et Voskresensky ont trouvé le contre-exemple avec $G = \mathbb{Z}/47\mathbb{Z}$. C'est le plus petit groupe de cardinal premier. Ensuite, Lenstra a trouvé un contre-exemple avec $G = \mathbb{Z}/8\mathbb{Z}$ et donné une condition nécessaire et suffisante pour que la réponse soit positive pour un groupe commutatif.

Références

[1] J.-L. Colliot-Thélène, *The Rationality Problem for Fields of Invariants*

[2] Philippe Gille et Tamás Szamuely, *Central Simple Algebras and Galois Cohomology*

[3] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Braunschweig, Allemagne, Vieveg, 1997

[4] Swan, Richard G., *Invariant rational functions and a problem of Steenrod*, Invent. Math. 7 (1969), 148–58.

[5] Helmut Völklein, *Groups as Galois Groups*, Cambridge, 1996

[6] Voskresensky, Valentin E. *On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field Q(x1,..., xn) (Russe)*, Izv. Akad. Nauk SSSR Ser. Mat. 34 (1970), 366–75 ; English translation in Math. USSR Izv. 4 (1971), 371–80.

[7] Lenstra, Hendrik W. *Rational functions invariant under a finite abelian group*, Invent. Math. 25 (1974), 299–325.