A COLLECTION OF PAPERS IN MATHEMATICS AND RELATED SCIENCES,
A FESTSCHRIFT IN HONOUR OF THE LATE GALAYE DIA
EDITORS : PROFS HAMET SEYDI, GANE SAMB LO, ABOUBAKARY DIAKHABY
SPAS-EDS (SAINT-LOUIS, CALGARY, 2018), WWW.STATPAS.ORG/SPASEDS/
IN EUCLID (WWW.PROJECTEUCLID.ORG)
DOI : 10.16929/SBS/2018.100

CHAPTER 3

Le théorème inverse de Galois, *by Hamet Seydi*

Hamet Seydi. Email : hseydi@gmail.com
Université Cheikh Anta Diop, Dakar

Abstract. The main aim of this article is to prove the following result.

THEOREM 3. *Let K be a hilbertian field and G a finite group. Then there exist a Galois extension L of K such that $Gal(L/K)$ is isomorphic to G.* $\Diamond$

Keywords. Galois Inverse Theorem. Galois representations .
AMS 2010 Mathematics Subject Classification. 11F80; 11R32.

Cite tha chapter as : :
Seydi H. (2018). Le théorème inverse de Galois.
In *A Collection of Papers in Mathematics and Related Sciences, a festschrift in honour of the late Galaye Dia* (Editors : Seydi H., Lo G.S. and Diakhaby A.). Spas Editions, Euclid Series Book, pp. 21 – 31
Doi : 10.16929/sbs/2018.100-01-03

Acknowledgment Ce travail est soutenu par le Centre d'Excellence en Mathématiques, Informatique et Nouvelles Technologie de l'Information et de la Communication (CE - MITIC) de l'Université Gaston Berger de Saint - Louis (SENEGAL).

1 - Enoncé du Théorème Inverse de Galois.

Le ésultat principal de cet article est le thórème suivant,

THEOREM 4. *Soient K un corps hilbertien et G un groupe fini. Alors il existe une extension galoisienne L de K telle que $Gal(L/K)$ soit isomorphe à G.*

qui est le théorème inverse de Galois.

2 - Démonstration.

La démonstration de ce résultat s'appuie sur le théorème suivant :

THEOREM 5. *Soient K un corps et G un groupe fini. Alors il existe une extension transcendante pure $L = K(y_1, \cdots, y_{n+1})$ de K de degré $n+1$ où n est l'ordre de G, telle que G soit isomorphe au groupe de Galois sur L d'une extension galoisienne finie F de L.*

Nous aurons besoin des lemmes suivants :

LEMMA 2. *Soient K un corps, F une extension galoisienne de K, $G = Gal(F/K)$, $f \in K[T]$ un polynôme non nul à coefficients dans K et Z l'ensemble des zéros de f dans K. On suppose que Z est non vide.*

Alors :

1) Les actions des éléments de G sur F permutent les éléments de Z.

2) Si les éléments de Z engendrent F sur K, alors G est isomorphe à un sous - groupe du groupe $\sum(Z)$ des permutations de Z.

3) Si f est un polynôme irréductible et si F est le corps de décomposiiton sur K d'un polynôme g à coefficients dans K, alors G opère transitivement sur Z.

Preuve du lemme 5: 1) Pour tout $\alpha \in F$ et tout $\sigma \in G$, on a $f(\sigma(\alpha)) = \sigma(f(\alpha))$ puisque σ laisse invariants les éléments de K. Par conséquent pour tout $\sigma \in Z$, on a

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0,$$

donc $\sigma(\alpha) \in Z$. Ce qui prouve que les actions des éléments de G sur F permutent les éléments de Z.

2) Supposons que F soit engendré sur K par les éléments de Z. Comme les actions des éléments de 'G permutent les éléments de Z d'après 1), on définit un homomorphisme naturel $\pi : G \longrightarrow \sum(Z)$. Pour démontrer 2) il faut montrer que $H = Ker(\pi) = \{e\}$. Il est clair que les éléments de H fixent tous éléments de Z et aussi ceux de K puisque $H \subseteq G = Gal(F/K)$. Par conséquent les éléments de H fixent tous les éléments de $F = K(Z)$. On en déduit donc que $H = \{e\}$, donc G est isomorphe à un sous - groupe de $\sum(Z)$.

3) Supposons maintenant que F soit le corps de décomposition d'un polynôme g appartenant à $K[T]$ et que f soit irréductible dans $K[T]$. Soient α_1 et α_2 des éléments de Z. Nous allons montrer qu'il existe $\theta \in G$ tel que $\theta(\alpha_1) = \alpha_2$ Comme f est irréductible dans $K[T]$ et que α_1 et α_2 sont des racines de f, il existe un K-isomorphisme de corps $\varphi : K_1 = K[\alpha_1] \longrightarrow K_2 = K[\alpha_2]$ tel que $\varphi(\alpha_1) = \alpha_2$. Il est clair que F est le corps de décomposition de g sur K_1 et K_2. Pour tout polynÃťme h appartenant à $K_1[T]$, notons $\hat{\varphi}(h)$ le polynôme appartenant à $K_2[T]$ obtenu en appliquant φ aux coefficients de h. Comme g est un polynôme à coefficients dans K et que φ est un K-isomorphisme de K_1 dans K_2, on a $\hat{\varphi}(g) = g$.

fSupposons que φ se prolonge en un isomorphisme θ de F sur F, on en déduit que $\theta \in G$ et $\theta(\alpha_1) = \alpha_2$.
Le lemme suivant permettra donc de conclure.

LEMMA 3. *Soient $\varphi : K_1 \longrightarrow K_2$ un isomorphisme de corps, $f_1 \in K_1[T]$ un polynôme à coefficients dans K_1 et $f_2 = \hat{\varphi}(f_1) \in K_2[T]$ le polynôme à coefficients dans K_2 obtenue en faisant opérer φ sur les coefficients de f_1. Supposons que F_1 soit un corps de décomposition de f_1 sur K_1 et F_2 un corps de décomposition de f_2 sur K_2. Alors φ se prolonge en un isomorphisme de corps $\theta : F_1 \longrightarrow F_2$.*

Preuve du lemme 6: Nous raisonnerons par récurrence sur $n = [F_1 : K_1]$.

1) Si $n = 1$, alors f_1 se décompose sur K_1, donc $f_2 = \hat{\varphi}(f_1)$ se décompose aussi sur K_2. Ce qui implique donc que

$[F_2 : K_2] = 1$. Par conséquent on a : $F_1 = K_1,\ F_2 = K_2$ et $\theta = \varphi$.

2) Supposons maintenant que $n \geq 2$. Soit g_1 un facteur irréductible de f_1 dans $K_1[T]$, alors $g_2 = \hat{\varphi}(g_1)$ est un facteur irréductible de f_2 dans $K_2[T]$. Comme f_1 se décompose dans $F_1[T]$, alors g_1 possède une racine α_1 dans F_1 et g_2 possède une racine α_2 dans F_2. On sait que dans ce cas il existe un isomorphisme de corps

$$\theta_1 : L_1 = K_1[\alpha_1] \longrightarrow L_2 = K_2[\alpha_2]$$

tel que $\theta_1(\alpha_1) = \alpha_2$ prolonge φ. Comme $[L_1 : K_1] = deg(g) > 1$, on en conclut que $[F_1 : L_1] < [F_1 : K_1] = n$. Donc d'aprÃÍs l'hypothèse de récurrence $\theta_1 : L_1 \longrightarrow L_2$ se prolonge en un isomorphisme de corps $\theta : F_1 \longrightarrow F_2$ puisque F_1 est le corps de décomposition de f_1 sur L_1 et F_2 est le corps de décomposition de F_2 sur L_2.
Il est clair que θ prolonge φ, d'où la conclusion.

Lemma 4. *Soient K un corps et G un groupe fini d'ordre n. Alors il existe une extension de type fini L de K contenue dans l'extension transcendante pure $F = K(x_1, \cdots, x_n)$ de degré n de K telle que F soit une extension galoisienne de L et $Gal(F/L) \simeq G$.*

Preuve du lemme 7 : D'après le théorème de Cayley, G est un isomorphe à un sous - groupe du groupe $\sum(G)$ des permutations de l'ensemble sous - jacent à G. Or $\sum(G)$ est isomorphe au groupe $\sum_n$. des permutations de $P_n = \{1, \cdots, n\}$. Par conséquent G est isomorphe à un sous - groupe de $\sum_n$.. Or $\sum_n$. opère sur l'anneau des polynômes $A = K[x_1, \cdots, x_n]$ comme suit : $\sigma(a) = a$ quel que soit $a \in K$ et $\sigma(x_i) = x_{\sigma(i)}$ quel que soit l'entier i,
$1 \leq i \leq n$. Il est clair que σ se prolonge en un isomorphisme de corps $\varphi_\sigma : F \longrightarrow F$ pour tout $\sigma \in \sum_n$. On en déduit donc que G aussi opère sur F en tant que sous - groupe de $\sum_n$.

Soit alors L le sous - corps des invariants de F sous l'action des éléments de G. Il est clair que F est une extension galoisienne de L et $Gal(F/L) \simeq G$. En outre comme L est un sous - corps de F contenant K, L est une extension de type fini de K d'après (Issacs (1993) 24.9).

Démonstration du Théorème 12

D'après le lemme 7, si n désigne l'ordre de G, il existe une extension de type fini $\overline{L}$ de K contenue dans l'extension transcendante pure $\overline{F} = K(x_1, \cdots, x_n)$ de K telle que $\overline{F}$ soit une extension galoisienne de $\overline{L}$ et $Gal(F/I) \simeq G$. Il est clair que $\bar{L}$ est une extension séparable de K, donc il existe $y_1, \cdots, y_n$ des éléments algébriquement indépendants sur K telle que $\overline{L}$ soit une extension finie séparable de $K(y_1, \cdots, y_n)$. Il existe donc $\alpha \in \overline{L}$ et $\bar{\alpha}_1 \in \overline{F}$ tels que $\overline{L} = K(y_1, \cdots, y_n)[\alpha]$ et $\overline{F} = \overline{L}[\bar{\alpha}_1]$. Soient $\bar{f}(y)$ le polynôme unitaire minimal de α sur $\overline{F}$ et $\bar{f}_1(T_1)$ le polynôme unitaire minimal de $\bar{\alpha}_1$ sur $\overline{L}$ et $\bar{\alpha}_1, \cdots, \bar{\alpha}_n$ les racines de $\bar{f}$. Alors $\bar{f}_1 = \sum_{0 \leq 1 \leq n} a_i(\alpha) T_1^i$, où $a_i(y)$ est un polynôme en y à coefficients dans $K(y_1, \cdots, y_n)$.

En posant $f_1 = \sum_{0 \leq 1 \leq n} a_i(y) T_1^i$, alors f est un polynôme irréductible à coefficients dans $K(y_1, \cdots, y_n, y)$ puisque $\bar{f}_1$ est un polynôme irréductible à coefficients dans $\overline{L}$. En outre si $\Delta(f_1)$ est le discriminant de f_1 sur $K(y_1, \cdots, y_n, y)$, son image dans $\overline{L}$ est le discriminant $\Delta(\bar{f}_1)$ de $\bar{f}_1$. Comme on a $\Delta(\bar{f}) \neq 0$, on en conclut que $\Delta(f_1) \neq 0$. Ce qui signifie que f_1 est un polynôme séparable à coefficients dans $K(y_1, \cdots, y_n, y)$.

On a un homomorphisme d'anneaux

$$\pi : B = K(y_1, \cdots, y_n)[y][T_1]/(f_1(T_1)) \longrightarrow \bar{F}$$

défini par $\pi(y) = \alpha$ et $\pi(\alpha_1) = \bar{\alpha}_1$ où α_1 est l'image de T_1 dans B et $\mathcal{M} = Ker(\pi)$ est l'idéal de B engendré par $\bar{f}(y)$. Comme $f_1(T_1)$ est un polynôme irréductible de $K(y_1, \cdots, y_n)[y][T_1]$, B est un anneau intègre. Si B_1 est la clôture intégrable de B, comme $V = B_{\mathcal{M}}$ est un anneau de valuation discrète, $\mathcal{M}_1 = \mathcal{M}V \cap B_1$ est le seul idéal premier de B_1 contenant $\bar{f}(y)$ et $\mathcal{M}_1(B_1)_{\mathcal{M}_1} = \bar{f}(y)(B_1)_{\mathcal{M}_1}$. Comme B_1 est un anneau de Dedekind, on en déduit que $\mathcal{M}_1 = \bar{f}(y)B_1$ d'après (Issacs (1993) 29.3). Posons $R = (B_1)_{\mathcal{M}_1}$, soient R^* le henselisé de R et $\alpha_1, \cdots, \alpha_n$ les racines de $f_1(T_1)$.

Alors d'après (Nagata (1962) 43.9), il existe un élément a de $\mathcal{M}_1\ R^*$ entier sur R tel que $N_o = \mathcal{M}_1\ B_1[a] + aB_1[a]$ engendre un idéal maximal N de $C = R[a]$ et que $\alpha_1, \cdots, \alpha_n$ soient des éléments de $C_N = R[a]_N$. D'après (Nagata (1962) loc. cit), on peut choisir a tel que R^* soit le henselisé de C_N. Par conséquent C_N est un anneau de valuation discrète puisque R est un anneau de valuation discrète. On a $a = a'\bar{f}(y)$ avec $a' \in R^*$ puisque $a \in \mathcal{M}_1 R^* = \bar{f}(y)R^*$. Posons $C' = R[a']$ et $N' = \mathcal{M}_1 R^* \cap C'$. Alors comme $C'_{N'}$ domine $C_{N'}$ et que C'_N et C_N ont le même corps des fractions on a $C_{N'} = C'_{N'}$. Donc si D est la clôture intégrale de C', alors $M = NC_N \cap D = N'C'_{N'} \cap D$ est le seul idéal maximal de D qui contient N_o, donc M est le seul idéal premier de D qui contient $\bar{f}(y)$, puisque si P est un idéal premier de D contenant $\bar{f}(y)$, P contient $a = a'\bar{f}(y)$ et $\mathcal{M}_1$. Donc P contient N_o, ce qui implique que $P = M$. Comme $\bar{f}(y)D_M = N_o D_M = MD_M$, on en déduit que $M = \bar{f}(y)D$ d'après (Issacs (1993) 29/3) puisque D est un anneau de Dedekind.

En posant $S = C[\alpha_1, \cdots, \alpha_n]$, on voit que $P = NC_N \cap S$ est le seul idéal premier de S au dessus de N et NS est P-primaire. Comme $PS_P = NC_N = NS_P$, on en déduit donc que $P = NS$.

Soient E une extension galoisienne de $K(y_1, \cdots, y_n, y)$ qui contient D, $\bar{D}$ la fermeture intégrale de D dans E, $\bar{C}$ la fermeture intégrale de C dans E, $I'' = \bar{f}(y)\ D''$ où $D'' = \bigcap_{g' \in G'} g'(\bar{D})$ et G' est le groupe de Galois de E sur $K(y_1, \cdots, y_n, y)$. Donc $I'' \neq D''$ puisque $\bar{f}(y)\bar{D} \neq \bar{D}$ d'après le premier théorème de Cohen-Seidenberg, étant donné que $\bar{D}$ est entier sur D et $\bar{f}(y)D$ est un idéal premier de D. Comme $\bar{C}$ est la fermeture intégrale de R dans E, alors $\bar{C}$ est invariant par G', donc D'' contient $\bar{C}$ puisque $\bar{D}$ contient $\bar{C}$. Par conséquent E est le corps des fractions de D''. Posons $D_o = D \cap D''$. Comme D'' est un anneau de Dedekind d'après le théorème de Krull-Akisuki (Nagata (1962) 33.2) puisqu'il contient $\bar{C}$ qui est un anneau de Dedekind, D'' est l'intersection des anneaux de valuation discrète définis par ses idéaux maximaux. Donc D_o est l'intersection de ces derniers anneaux valuation discrète avec $K(y_1, \cdots, y_n, y)$ et qui sont aussi des anneaux valuation discrète. Mais tout idéal maximal de D_o définit un de ces derniers anneaux de valuation discrète, d'après (Nagata (1962) 33.6), ce qui prouve que tout idéal maximal de D_o est l'intersection d'un idéal maximal de D'' avec D_o. En outre $M_o = M \cap D_o$ est le seul idéal premier de D_o contenant $\bar{f}(y)$ puisque $(D_o)_{M_o} = D_M = S_P = C_N$. En effet si Q_o est un idéal premier de D_o contenant $\bar{f}(y)$, $Q_o = D \cap Q''$ oÃź Q'' est un idéal maximal de D'' et $Q'' = \bar{Q} \cap D''$ oÃź $\bar{Q}$ est un idéal maximal de $\bar{D}$ puisque $\bar{D}$ est entier sur D''. Or $\bar{Q} \cap D = M$, donc $Q = M \cap D_o = M_o$. Comme D'' contient S puisque $\bar{C}$ contient S, alors

D'' est un anneau de Dedekind d'après le théorème de KRULL - AKIZUKI (Nagata (1962) loc. cit), donc, $M_o = \bar{f}(y)D_o$ d'après (Issacs (1993) 29.3). Soit $B' = K(y_1, \cdots, y_n)[y][\alpha_1, \cdots, \alpha_n] \subseteq S$.

Alors $\mathcal{M}' = B' \cap I'' = B' \cap M_o = B' \cap P$ est un idéal maximal de B'. Comme B' et $I'' = \bar{f}(y)D''$ sont invariants par G', alors $\mathcal{M}'$ est invariant par G'. On en déduit donc que si u et v sont des éléments de B' tels que $u \equiv v \ mod\ \mathcal{M}'$, on a $g'(u) \equiv g'(v) \ mod\ \mathcal{M}'$ quel que soit l'élément g' de G'. En outre on a un homomorphisme d'anneaux $\varphi : B' \longrightarrow \bar{F}$ qui prolonge l'homomorphisme d'anneaux $\pi : B \longrightarrow \bar{F}$ et $\mathcal{M}' = Ker(\varphi)$. Donc si u et v sont deux éléments de B' tels que $\varphi(u) = \varphi(v)$, alors $\varphi(g'(u)) = \varphi(g'(v))$ quel que soit l'élément g' de G'.

On peut donc définir une application $\theta : G' \longrightarrow G$ par $\theta(g')(\varphi(u)) = \varphi(g'(u))$. En effet $\theta(g')$ est un homomorphisme de $\bar{F}$ dans $\bar{F}$ puisque g' est un homomorphisme de B' dans B' et $\theta(g')$ laisse invariants les éléments de $\overline{L}$ puisque G' laisse invariants les éléments de $K(y_1, \cdots, y_n, y)$, donc $\theta(g') \in G$ quel que soit $g' \in G'$.
D'autre part comme G opère transitivement sur $\{\bar{\alpha}_1, \cdots, \bar{\alpha}_n\}$ d'après le lemme 5 , l'application $h : G \longrightarrow \{\bar{\alpha}_1, \cdots, \bar{\alpha}_n\}$ définie par $h(g) = g(\alpha_1)$ est surjective donc bijective puisque l'ordre de G est égal Ãă n. Soient $g \in G$ et $\bar{\alpha}_k = g(\bar{\alpha}_1)$. Comme G' opère transitivement sur $\{\alpha_1, \cdots, \alpha_n\}$, en admettant que $\varphi(\alpha_1) = \bar{\alpha}_1$ puisque φ établit une bijection entre $\{\alpha_1, \cdots, \alpha_n\}$ et $\{\bar{\alpha}_1, \cdots, \bar{\alpha}_n\}$, il existe donc $g' \in G'$ tel que $\varphi(g'(\alpha_1)) = \theta(g')(\bar{\alpha}_1)$ qui est un élément de $\{\bar{\alpha}_1, \cdots, \bar{\alpha}_n\}$ soit égal Ãă $g(\bar{\alpha}_1 = \bar{\alpha}_k$. On en conclut donc que l'on a $g = \theta(g')$, puisque $h(g) = h(\theta(g'))$ et h est bijective, ce qui prouve que θ est surjective.

On a aussi $\theta(g'_1 g'_2)(\varphi(u)) = \varphi(g'_1 g_2(u)) = \theta(g'_1)(\varphi(g'_2(u))) = \theta(g'_1)\theta(g'_2)(\varphi(u))$. En remplaçant u par α_1 dans cette relation, on obtient $h(\theta(g'_1, g'_2)) = h(\theta(g'_1) \circ \theta(g'_2)$, donc $\theta(g'_1, g'_2) = \theta(g'_1) \circ \theta(g'_2)$ puis que h est bijective. On en conclut donc θ est un homomorphisme de groupes. Par conséquent si F est le sous - corps des invariants de $H = Ker(\theta)$, F est une extension galoisienne de $K(y_1, \cdots, y_n, y_{n+1})$ où $y_{n+1} = y$, d'après le Théorème Fondamental de la Théorie de Galois puisque H est un sous - groupe normal de G' et $G \simeq G'/H \simeq Gal(F/K(y_1, \cdots, y_n, y_{n+1})$, d'où la conclusion.

Definition 1. *On dira qu'un corps K est un corps quasi - hilbertien si tout groupe fini G est isomorphe au groupe de Galois d'une extension galoisienne de K.*

Theorem 6. *Soient K un corps et L une extension transcendante pure de K de degré de transcendance sur K infini. Alors L est un corps quasi - hilbertien.*

Preuve du théorème 6. Soit $(x_i)_{i\in I}$ une famille d'éléments de L algébriquement indépendants sur K qui engendrent L sur K. Soient G un groupe fini d'ordre n, I_1 une partie Ãă $n+1$ éléments de I et I_2 sont complémentaire dans I. D'après le théorème 12, il existe une extension galoisienne F' de $L' = K(x_i)_{i\in I_1}$ telle que $Gal(F'/L') \simeq G$. On a $L'[x_i]_{i\in I_2} \otimes_{L'} F' \simeq F'[x_i]_{i\in I_2}$, donc si S est l'ensemble des éléments non nuls de $L'[x_i]_{i\in I_2}$.

$$F = L \otimes_{L'} F' = S^{-1}(L'[x_i]_{i\in I_2}) \otimes_{L'} F'$$

est un anneau intègre qui est entier sur le corps L. Par conséquent F est un corps et $[F : L] = [F' : L'] = n$.

D'autre part si $g \in G,$ on a une application bilinéaire
$\theta_g : L \times F' \longrightarrow F = L \otimes_{L'} F'$ définie par $\theta_g(u, v) = u \otimes g(v),$ qui induit un homomorphisme $F = L\otimes_{L'} F' \longrightarrow F = L\otimes_{L'} F'$ défini par $\theta_g(u\otimes v) = u\otimes g(v)$. Cet homomorphisme est un automorphisme de F qui laisse invariant L. En définissant $g(u \otimes v) = \theta_f(u \otimes v)$,

$$g\left(\sum_{1\leq i\leq n} u_i \otimes v_i\right) = \theta_g\left(\sum_{1\leq i\leq n} u_i \otimes v_i\right) = \sum_{1\leq i\leq n} u_i \otimes g(v_i),$$

G est un groupe d'automorphisme de F qui laisse L invariant et comme $n = [F : L]$ et n est l'ordre de G, on en déduit que $G = Gal(F/L),$ d'où la conclusion.

Theorem 7. *Soient K un corps, n un entier positif et L une extension transcendante pure de K de degré de transcendance égal Ãă $n + 1$. Alors tout groupe G d'ordre $m \leq n$ est isomorphe au groupe de Galois sur L d'une extension galoisienne F de L.*

Preuve du théorème 7: Soit $L_o = K(x_1, \cdots, x_{m+1})$ une sous - extension de $L = K(x_1, \cdots, x_{m+1}, \cdots, x_{n+1}$ sur K transcendante et de degré de transcendance égal à $m+1$ sur K. D'après le théorème 12, il existe une extension galoisienne F_o de L_o de degré fini telle que $Gal(F_o/L_o) \simeq G$. On prouve comme dans la dÃľmonstration précédente que $F = L \otimes_{L_o} F_o$ est un corps et une extension galoisienne de L et que $Gal(F/L)$ est isomorphe à G.

THEOREM 8 (Théorème inverse de Galois généralisé). *Soient K un corps hilbertien et G un groupe fini. Alors il existe une extension galoisienne finie L de K telle que $Gal(L/K)$ soit isomorphe à G. Autrement dit K est un corps quasi - hilbertien.*

Preuve du théorème 8 : L'assertion découle du théorème 12 et de (Yao and Xie (2009) Th. 2.12).

COROLLARY 3. *Soient K un corps hilbertien, Ω sa clôture algébrique séparble et G un groupe fini. Alors G est isomorphe à un groupe quotient de $Gal(\Omega/K)$.*

Proof of Corollary 3 : D'après le théorème précédent, il existe une extension galoisienne L de K contenue dans Ω telle que $Gal(L/K)$ soit isomorphe à G.

Soit H le sous - groupe de $M = Gal(\Omega/K)$ constitué des éléments de M qui laissent invariants les éléments de L. Alors d'après le Théorème Fondamental de Galois, G est isomorphe au groupe quotient M/H, d'où la conclusion.

THEOREM 9 (Théorème Inverse de Galois). *Soit G un groupe fini. Alors il existe une extension galoisienne finie L de $\mathbb{Q}$ telle que $Gal(L/\mathbb{Q})$ soit isomorphe à G, autrement dit $\mathbb{Q}$ est un corps quasi - hilbertien.*

Preuve du théorème 9 : L'assertion découle du théorème d'irréductibilité de HILBERT qui dit que $\mathbb{Q}$ est un corps hilbertien et du théorème précédent.

COROLLARY 4. *Soient $\bar{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ et G un groupe fini. Alors G est isomorphe à un groupe quotient de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.*

Preuve du corrolaire 4: L'assertion découle du corollaire précédent.

THEOREM 10. *Soient K un corps quasi - hilbertien et $L = K(x_1, \cdots, x_n)$ une extension transcendante pure de degré fini de K. Alors L est un corps quasi - hilbertien.*

Preuve du théorème 10 : Soient G un groupe fini et F une extension galoisienne finie de K dont le groupe de Galois sur K est isomorphe à G. Il est facile de voir que $E = F(x_1, \cdots, x_n)$ est une extension galoisienne finie de $L = K(x_1, \cdots, x_n)$ dont le groupe de Galois sur $L = K(x_1, \cdots, x_n)$ est isomorphe à G, d'où la conclusion.

3 - Quelques remarks and further results.

Nous avons les résultats suivants :

1) Si K est un corps hilbertien, alors toute extensin de type fini L de K est un corps hilbertien (cf. Yao and Xie (2009) Cor. 2.11).

2) Si K est un corps hilbertien, alors toute extension transcendante pure de degré infini L de K est un corps hilbertien (cf Lang (1959-1960)).

3) Si K est un corps hilbertien, alors l'extension abélienne maximale séparable L de K est un corps hilbertien (cf Kuyk (1970) Cor. 1).

4) Si K est un corps hilbertien, alors l'extension nilpotente maximale séparable L de K est un corps hilbertien (cf. Kuyk (1970) Cor. 2).

5) Si K est un corps infini, alors toute extension de type fini L de K de degré de transcendance supérieur ou égal à 1 est un corps hilbertien (cf. Lang (1959-1960) Théorème 6). Ce qui implique donc que le corps L du théorème 6 est un corps hilbertien, et le corps L du théorème 8 est un corps hilbertien si $n \geq 2$, même si K n'est pas un corps quasi-hilbertien.

6) On peut même se demander si un corps quasi-hilbertien n'est pas un corps hilbertien.

Bibliography

Douady, A. (1964). Détermination d'un groupe de GALOIS. *C.R. Acad. Sci.* Paris, 258, 5305 - 5308.

Franz, W. (1931). Untersuchungen zum Hilbertichen Irreduzibilitätssatz, Math. 33 , 275 - 293.

Hilbert, D. (1892). Uber die Irreduzilität ganzer Funktionen mit ganzahligne Koeffizienten. *I.f.d. reine u. a. Math, Bel* 110.

Inaba, E. (1944). Uber die Hilbertschen Irreduzibilitätssatz, *Jap. J. Math.* 19 , 1 - 25.

Kuyk, W. (1970). Extensions de corps hilbertiens. *Journal of Algebra* 14, 112 - 124.

Lang, S. (1959-1960). Le théorème d'irréductibilité de HILBERT, *Séminaire BOURBAKI*, nÂř 201.

Issacs, I.M. (1993). Algebra, Brooks . Cole Publishing Company.

Nagata, M. (1962). Local Rings. *Interscience Publishers*, New - York - London - Sydney.

Noether, E. (1926). Gleichungen mit vorges chriebener Gruppe, *Math. Ann.* 78, 221 - 225.

Völklein, H. (1996). Groups as Galois Groups, Cambridge.

Yao,J and XieE, . (2009). Corps Hilbertien, Ecole Normale Supérieure.