Travail de recherche encadré

Le problème de Noether

Pablo Chenal, sous la direction de David Harari

Laboratoire de mathématiques d'Orsay, 2023

Table des matières

1 Introduction

1.1 Le problème de Noether

Soit k un corps et $k(T_1, ..., T_n)$ le corps des fractions rationnelles à n variables sur k. Soit G un sous groupe du groupe symétrique S_n. On fait agir G sur $k(T_1, ..., T_n)$ par

$$\sigma.F = F(T_{\sigma(1)}, ..., T_{\sigma(n)})$$

pour tout $F \in k(T_1, ..., T_n) := K$ et $\sigma \in G$.

Le problème de Noether consiste alors à se demander quand est-ce-que $K^G = \{F \in K, \forall \sigma \in G, \sigma.F = F\}$ est une extension transcendante pure de k.

Pour cela, il faut définir ce qu'est une extension transcendante pure.

Définition : Soit K un corps. Si L/K est une extension de K, un élément de L annulé par un polynôme unitaire à coefficients dans K est dit algébrique. Si tout élément de L est algébrique, alors L/K est une extension algébrique de K.

Définition : Soit K un corps. Si L/K est une extension de K, L/K est dite transcendante si elle n'est pas algébrique.

Définition : Des éléments $(t_1, ..., t_n) \in L$ sont algébriquement indépendants si il n'existe pas de $P \in K[T_1, ..., T_n]$ non nul tel que $P(t_1, ..., t_n) = 0$. Si L/K est engendré par une famille d'éléments algébriquement indépendants, alors c'est une extension transcendante pure de K.

Nous verrons dans la partie 3 que lorsque $G = S_n$, le problème de Noether est vérifié puisqu'on dispose des polynômes symétriques et Fischer a montré en 1915 qu'avec un sous groupe commutatif et avec certaines hypothèses sur le corps, le problème de Noether reçoit également une réponse affirmative.

Dans la partie 5, nous verrons qu'avec $k = \mathbb{Q}$ et $G = \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Q}(T_1, ..., T_8)^{\mathbb{Z}/8\mathbb{Z}}/\mathbb{Q}$ n'est pas transcendante pure.

1.2 Le problème de Galois inverse

Problème : étant donnés un corps k et un groupe fini G, existe-t-il une extension K de k telle que Gal(K/k) soit isomorphe à G ?

Ce problème s'applique à différents corps comme $\mathbb{Q}$, $\mathbb{C}(T)$ ou encore $\mathbb{Q}_p(T)$ et obtient différentes réponses.

Le cas du corps $\mathbb{Q}$ est une des plus grandes conjectures autour de la théorie de Galois : tout groupe fini est le groupe de Galois d'une extension galoisienne de $\mathbb{Q}$. Comme pour le problème de Noether, de nombreux résultats on été montrés mais cette conjecture reste encore non résolue.

Au contraire, les cas des corps $\mathbb{C}(T)$ et $\mathbb{Q}_p(T)$ sont maintenant résolus et ces problèmes reçoivent une réponse positive. Le cas de $\mathbb{Q}_p(T)$ a été résolu par Harbater. Pour une démonstration du cas $\mathbb{C}(T)$, voir [AMS].

Définition : Un groupe fini G est dit réalisable si il existe une extension galoisienne de $\mathbb{Q}$ telle que le groupe de Galois de l'extension soit G.

Théorème (Selmer, 1956) : Soit $n > 1$ un entier. Le polynôme $T^n - T - 1$ dans $\mathbb{Z}[T]$ est irréductible sur $\mathbb{Q}$ et son groupe de Galois sur $\mathbb{Q}$ est S_n.

Pour une démonstration de ce résultat, voir [KRAUS] page 29.

Ainsi, tout groupe finie est groupe de Galois d'un corps de nombre car il est isomorphe à un sous groupe de S_n. Le théorème suivant est un résultat dont la preuve est longue et difficile :

Théorème (Šafarevič, 1954) : Tout groupe fini résoluble est réalisable.

Un résultat plus abordable est prouvé pour les groupes abéliens (qui sont résolubles car $D(G) = \{e\}$), mais nous aurons besoin d'une version simplifiée du théorème de la progression arithmétique de Dirichlet :

Théorème (Dirichlet, 1837) : Pour tout $n \in \mathbb{N}^*$, pour tout entier m premier avec n, il existe une infinité de nombres premier congrus

à m modulo n.

Définition : Soit n un entier non nul. On appelle n-ième polynôme cyclotomique que l'on note $\phi_n(T)$ le polynôme $\phi_n(T) = \prod(T - \mu)$ où le produit est pris sur les racines primitives n-ièmes de l'unité.

La version simplifiée du théorème que l'on va utiliser est la suivante : pour tout entier n non nul, il existe une infinité de nombres premiers congrus à 1 modulo n.

La démonstration est beaucoup plus simple que la version générale, on utilise le fait que si a est un entier et que p est un nombre premier tel que p divise $\phi_n(a)$ mais ne divise pas $\phi_d(a)$ pour d divisant n et différent de n, alors p est congru à 1 modulo n. Cela permet de trouver des nombres premiers arbitrairement grands vérifiant l'énoncé du théorème. Pour l'existence de tels p premiers, on fixe $k \in \mathbb{N}^*$ et on considère $a = 3k!$. Alors $\mid \phi_n(a) \mid \geq \prod(a-1) \geq 2$ et donc il existe un premier p qui divise $\phi_n(a)$ et ce premier est en fait plus grand que k et congru à 1 modulo n.

Théorème : Tout groupe abélien fini est réalisable.

démonstration :
Soit G un groupe abélien fini. Par le théorème de structure des groupes abéliens de type fini, il existe $(a_1, ..., a_n) \in \mathbb{N}^n$ tels que

$$G \simeq \prod_{k=1}^{n} \mathbb{Z}/a_k\mathbb{Z}$$

D'après la version faible du théorème de Dirichlet, $a_k \wedge 1 = 1 \ \forall$ $1 \leq k \leq n$ donc il existe $(p_1, ..., p_n) \in \mathbb{N}^n$ des nombres premiers 2 à 2 distincts tels que $a_k \mid p_k - 1 \ \forall \ 1 \leq k \leq n$. Comme $(\mathbb{Z}/p_k\mathbb{Z})^*$ est cyclique d'ordre $p_k - 1$, $\mathbb{Z}/a_k\mathbb{Z}$ en est un quotient et par théorème chinois,

$$(\mathbb{Z}/p_1...p_n\mathbb{Z})^* \simeq \prod_{k=1}^{n} (\mathbb{Z}/p_k\mathbb{Z})^*$$

Or par le théorème fondamental de la théorie de Galois, tout quotient d'un groupe réalisable est réalisable. Ainsi, G est un quotient d'un certain $(\mathbb{Z}/n\mathbb{Z})^*$ donc il reste à montrer que $(\mathbb{Z}/n\mathbb{Z})^*$ est réalisable.

Soit ζ une racine primitive n-ième de l'unité. Considérons l'extension cyclotomique $\mathbb{Q}(\zeta)/\mathbb{Q}$. Alors en utilisant le fait que ϕ_n

est irréductible sur $\mathbb{Q}$ et unitaire, on montre que ϕ_n est le polynôme minimal de ζ et comme ϕ_n est de degré $\varphi(n)$ tout comme le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$, $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ est de cardinal $\varphi(n)$.

Si d est plus petit que n et est premier avec n, ζ^d est un conjugué de ζ donc il existe un unique $\mathbb{Q}$-automorphisme f_d qui envoie ζ sur ζ^d et l'isomorphisme de groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ sur $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ qui à d associe f_d montre que $(\mathbb{Z}/n\mathbb{Z})^*$ est le groupe de Galois d'une extension Galoisienne de $\mathbb{Q}$ ce qui achève la démonstration. □

Nous allons voir dans les prochains paragraphes que les problèmes de Noether et de Galois inverse sont liés puisqu'une réponse positive au problème de Noether implique une réponse positive au problème de Galois inverse, résultat que nous montrerons en utilisant le théorème d'irréductibilité de Hilbert. Néanmoins, il peut exister des groupes satisfaisant le problème de Galois inverse mais ne satisfaisant pas le problème de Noether.

1.3 Le lemme sans nom

Définition : Soit k un corps, et soient K et L deux extensions de k. On dit que K et L sont stablements équivalents si il existe des indéterminées $x_1, ..., x_r$ et $y_1, ..., y_s$ telles que $K(x_1, ..., x_r)$ soit isomorphe à $L(y_1, ..., y_s)$.

Soit V un k-espace vectoriel où k est de caractéristique nulle et algébriquement clos. Soit G un sous-groupe fini de $Gl(V)$. On suppose que G agit sur V avec la condition suivante : le stabilisateur de G en $v \in V$ est trivial pour tout $v \in V$. Soit $k(V)$ le corps des fractions de l'algèbre symétrique de V. On note $k(V)^G$ le sous corps de $k(V)$ des éléments invariants par G.

Théorème : Soit G un groupe fini. Soient V et W deux représentations fidèles linéaires de dimension finie de G sur k. Alors les corps $k(V)^G$ et $k(W)^G$ sont stablements équivalents.

Définition : Soit k un corps et K/k une extension finie. Soit $\alpha \in K$. On pose φ_α l'endomorphisme de K (qui est bien un k-espace vectoriel de dimension finie) qui à $x \in K$ associe αx. La trace de K sur k de α est la trace de l'endomorphisme φ_α, que l'on note $Tr_{K/k}(\alpha)$.

Définition : Soit G un groupe fini agissant sur E, un espace vectoriel sur un corps k, de dimension fnie. On dit que l'action est semi-linéaire si il existe un automorphisme σ de k tel que $\forall g \in G, \forall \lambda \in k, \forall v \in E, g.(\lambda v) = \sigma(\lambda) g.v$.

Lemme : Soit K/k une extension galoisienne finie de groupe de Galois G. Alors pour tout K-espace vectoriel E de dimension finie et pour toute action semi-linéaire de G sur E, on a $E = E^G \otimes_k K$. De plus, $K(E)^G/k = k(E)^G/k$ est pure.

démonstration :
Soit $\omega_1, ..., \omega_d$ une base linéaire de K/k et $G = \{\sigma_1, ...\sigma_d\}$. Soit $v \in E$. On considère pour $1 \leq i \leq n$

$$v_i = \sum_j \sigma_j(\omega_i v) \in E^G$$

Alors pour tout $1 \leq i \leq n$,

$$v_i = \sum_j \sigma_j(\omega_i)\sigma_j(v)$$

car l'action est semi-linéaire et la matrice $[\sigma_i(\omega_j)]$ étant inversible, on peut exprimer v comme combinaison linéaire des v_i à coefficients dans K, et donc $v \in E^G \otimes_k K$.

On a une application naturelle de $E^G \otimes_k K$ dans E, en montrant qu'elle est injective on aura bien $E = E^G \otimes_k K$. Si $\sum_i \lambda_i v_i = 0$, avec les λ_i non tous nuls, alors il existe un indice k et un élément $\alpha \in K$ tels que $Tr_{K/k}(\alpha\lambda_k) \neq 0$, ce qui donne que $\sum_i Tr_{K/k}(\alpha\lambda_i)v_i = 0$ est une relation linéaire sur k non triviale donc on a bien $E = E^G \otimes_k K$, la trace étant une forme non dégénérée et car $dim(E^G \otimes_k K) = dim(K)dim(E^G) = dim(E)$.

On montre maintenant le théorème. Par hypothèse, la représentation linéaire de G sur E est fidèle donc $k(V)/k(V)^G$ est galoisienne de groupe G. On applique le lemme à l'extension $k(V)/k(V)^G$. Ainsi, $k(V \oplus W)^G/k(V)^G = (k(V)(W))^G/k(V)^G$ est pure. De même, l'extension sur $k(W)^G$ est pure et $k(V \oplus W)^G$ est une extension pure commune à $k(V)^G$ et $k(W)^G$ donc ces corps sont stablements équivalents. $\square$

2 Liens entre ces deux problèmes

2.1 L'espace affine $\mathbb{A}_k^n$

Tous les anneaux considérés sont des anneaux commutatifs.
Définition : Soit A un anneau. On note Spec(A) l'ensemble des idéaux premiers de A.

Nous allons munir, pour tout anneau A, Spec(A) d'une topologie appelée topologie de Zariski. On fixe A un anneau pour la suite.

Définition : Pour tout I idéal de A, on note $V(I) = \{\mathfrak{p} \in$ Spec(A), $I \subset \mathfrak{p}\}$, et pour tout $f \in A$, $D(f) =$Spec(A)$\backslash V(fA)$ que l'on appelle ouverts principaux de Zariski.

Proposition : On munit Spec(A) d'une topologie en prenant pour fermés les ensembles $V(I)$ où I est un idéal de A. Les $D(f)$ forment une base de cette topologie.

Définition : Soit k un corps et $k[T_1, ..., T_n]$ son anneau de polynômes à n indéterminées. On note $\mathbb{A}_k^n =$Spec$(k[T_1, ..., T_n])$ l'espace affine sur k de dimension n.

2.2 Corps Hilbertiens

Soit k un corps. On considère la propriété d'irréductibilité suivante :

Soient $f_1(X_1, ...X_r, T_1, ..., T_s), ..., f_n(X_1, ...X_r, T_1, ..., T_s)$ des polynômes irréductibles dans l'anneau $k(X_1, ...X_r)[T_1, ..., T_s]$. Alors il existe un r-uplet dans k $(t_1, ..., t_r)$ tel que $f_1(t_1, ...t_r, T_1, ..., T_s), ..., f_n(t_1, ...t_r, T_1, ..., T_s)$ soient irréductibles dans l'anneau $k[T_1, ..., T_s]$.

Nous allons travailler à deux variables pour simplifier les notations. On considère $f(t, T) = f(t_1, ..., t_r, T_1, ..., T_s)$ appartenant à $k(t)[T] := k(t_1, ..., t_r)[T_1, ..., T_s]$.

Définition : On appelle ensemble hilbertien élémentaire et on note $U_{f,k}$ le sous ensemble de l'espace affine $\mathbb{A}_k^r$ constitué des points

$(a_1, ..., a_r) \in k^r$ tels que $f(a, T)$ soit irréductible dans $k[T]$.

Définition : On appelle partie hilbertienne de $\mathbb{A}_k^r$ tout intersection d'un nombre finie d'ensembles hilbertiens élémentaires avec un nombre finie d'ouverts non vide de $\mathbb{A}_k^r$ pour la topologie de Zariski.

Définition : Un corps k est dit hilbertien si les parties hilbertiennes de $\mathbb{A}_k^r$ sont non vides.

Exemple : Le polynôme $P(X, Y) = X^2 - Y^2 + X$ est irréductible sur $\mathbb{R}[X, Y]$ car on aurait à trouver une racine sur $\mathbb{R}[Y]$ de $Q(Y) = 1 + 4Y^2$ ce qui n'existe pas. Mais

$$\forall y \in \mathbb{R}, P(X, y) = X^2 + X - y^2$$

n'est pas irréductible sur $\mathbb{R}[X]$ car justement

$$\forall y \in \mathbb{R}, 1 + 4y^2 > 0$$

Ainsi, $\mathbb{R}$ n'est pas un corps hilbertien, et il en est de même pour $\mathbb{C}$.

Théorème d'irréductibilité de Hilbert : $\mathbb{Q}$ est un corps hilbertien.

Si $f(t, T)$ est irréductible sur $\mathbb{Q}(t)[T]$, alors il existe un énoncé du théorème de Hilbert où il existe une infinité de $(q_1, ..., q_r) \in \mathbb{Q}^r$ tels que $f(q, T)$ est irréductible sur $\mathbb{Q}[T]$. De plus, on peut choisir les $(q_1, ..., q_r) = q$ tels que $Gal(f(t, T)/\mathbb{Q}(t)) \cong Gal(f(q, T)/\mathbb{Q})$.

Une démonstration de ce résultat est donnée dans [HLBT], l'article reprend la preuve originelle trouvée par Hilbert.

Proposition : Une solution au problème de Noether pour un groupe $G \subset S_n$ implique une solution au problème de Galois inverse pour G et $k = \mathbb{Q}$.

Démonstration :
On suppose que le problème de Noether est vérifié pour $G \subset S_n$. Soit donc $(q_1, ..., q_r)$ algébriquement indépendants tels que avec $K^G := \mathbb{Q}(T_1, ..., T_n)^G$, $K^G = \mathbb{Q}(q_1, ..., q_r)$.

Par le théorème de l'élément primitif, il existe $\alpha \in K$ tel que $K^G(\alpha) = K$. Soit g le polynôme minimal de α sur K^G.

Ainsi, K est le corps de décomposition de g sur K^G. Pour $x \in \mathbb{Q}^n$, soit $g_x \in \mathbb{Q}[T]$ le polynôme construit en substituant par la i-ième

coordonnée de x q_i dans g.

Par le théorème de Hilbert, il existe une infinité de x tels que g_x est irréductible sur $\mathbb{Q}$ et que le corps de décomposition de g_x sur $\mathbb{Q}$ ait pour groupe de Galois G, ce qui achève la démonstration. □

3 Cas particulier du problème de Noether

3.1 Les polynômes symétriques

Le théorème suivant est vrai sur un anneau commutatif A quelconque, mais nous ne pouvons pas utiliser la notion de divisibilité si A n'est pas intègre, et nous montrons le théorème dans le cas d'un corps k. Nous allons aussi utiliser la notion de "division euclidienne" d'un polynôme de $k[T_1, ..., T_n]$ que l'on peut voir comme $k[T_1, ..., T_{n-1}][T_n]$ par T_n, dont le coefficient dominant est 1 qui est inversible dans $k[T_1, ..., T_{n-1}]$.

Soit k un corps.

Définition : On dit que $P \in k[T_1, ..., T_n]$ est un polynôme symétrique si $P \in k[T_1, ..., T_n]^{S_n}$.

Définition : Pour $1 \leq i \leq n$, le i-ième polynôme symétrique élémentaire est

$$\sigma_i(T_1, ..., T_n) = \sum_{1 \leq k_1 < k_2 < ... < k_i \leq n} T_{k_1} ... T_{k_i}$$

De plus, on note $\sigma_{i,0}$ le i-ième polynôme symétrique élémentaire dont on évalue T_n en 0.

Théorème : Soit $P \in k[T_1, ..., T_n]$ symétrique. Alors il existe un unique $Q \in k[T_1, ..., T_n]$ tel que $P = Q(\sigma_1, ..., \sigma_n)$.

Existence :

Soit $A_{n,p}$ l'hypothèse :"le théorème est vérifié pour tout polynôme de degré $p \in \mathbf{N}$ à $n \in \mathbf{N}^*$ indéterminées".
On effectue une récurrence sur $n \in \mathbf{N}^*$ puis sur $p \in \mathbf{N}$.

$A_{1,p}$ est vrai pour tout p car $\sigma_1(T_1) = T_1$. Supposons que $A_{n-1,p}$ est

vraie pour tout $p \in \mathbf{N}$. On travaille donc à n fixé sur $k[T_1, ..., T_n]$ par récurrence sur $deg(P) = p$.
Si p=0, P est constant et $Q = P$ convient. Supposons le résultat vrai pour tout polynôme de degré inférieur ou égal à p.

Soit P un polynôme symétrique de degré p+1. Alors
$P(T_1, ..., T_{n-1}, 0)$ est symétrique en $n-1$ variables donc il existe $Q_1 \in k[T_1, ..., T_{n-1}]$ tel que

$$P(T_1, ..., T_{n-1}, 0) = Q_1(\sigma_{1,0}, ..., \sigma_{n-1,0})$$

On pose alors

$$P_1(T_1, ..., T_n) = P(T_1, ..., T_n) - Q_1(\sigma_1, ..., \sigma_{n-1})$$

et on a donc

$$P_1(T_1, ..., T_{n-1}, 0) = 0$$

d'où $T_n \mid P_1$. Mais comme P_1 est symétrique, $\sigma_n = T_1...T_n \mid P_1$ et il existe $P_2 \in k[T_1, ..., T_n]$ tel que $P_1 = \sigma_n P_2$.

On va appliquer l'hypothèse de récurrence à P_2.
Posons $P_2 = \sum_{k \in \mathbf{N}^n} a_k T_k$. On voit alors que $n + deg(P_2) \leq p$ donc il existe $Q_2 \in k[T_1, ..., T_n]$ tel que $P_2(T_1, ..., T_n) = Q_2(\sigma_1, ..., \sigma_n)$.
Ainsi,

$$P_1(T_1, ..., T_n) = \sigma_n Q_2(\sigma_1, ..., \sigma_n) = Q_3(\sigma_1, ..., \sigma_n)$$

et on obtient donc

$$P(T_1, ..., T_n) = (Q_3 + Q_1)(\sigma_1, ..., \sigma_n)$$

où $deg(Q_3 + Q_1) \leq p$ ce qui conclut l'existence. □

Unicité :

Soit $P \in k[T_1, ..., T_n]$. Alors montrer que
$P(T_1, ..., T_n) = Q(\sigma_1, ..., \sigma_n) = R(\sigma_1, ..., \sigma_n)$ implique $R = Q$ revient à montrer que si $Q(\sigma_1, ..., \sigma_n) = 0$, alors $Q = 0$ (*), ce qui par ailleurs montre que la famille des polynômes symétriques élémentaire est une famille algébriquement indépendante.

On considère la propriété $B_{n,p}$: " (*) est vraie pour tout polynôme à n indéterminées de degré p".
$B_{1,p}$ est vraie pour tout p car $\sigma_1 = T_1$.

On suppose que $B_{n-1,p}$ est vraie pour tout $p \in \mathbf{N}$. On travaille à n fixé et on procède par récurrence sur le degré de Q.

Si Q est constant ou nul, (*) est vérifiée. Supposons Q de degré p. On effectue la division euclidienne de Q par T_n et il existe S et R tels que

$$Q(T_1, ..., T_n) = T_n S(T_1, ..., T_n) + R(T_1, ..., T_{n-1})$$

et donc

$$Q(\sigma_1, ..., \sigma_n) = \sigma_n S(\sigma_1, ..., \sigma_n) + R(\sigma_1, ..., \sigma_{n-1}) = 0$$

et en évaluant T_n en 0 il vient

$$Q(\sigma_{1,0}, ..., \sigma_{n-1,0}, 0) = R(\sigma_{1,0}, ..., \sigma_{n-1,0}) = 0$$

et donc $R = 0$ par $B_{n-1,p}$ et alors

$$Q(T_1, ..., T_n) = T_n S(T_1, ..., T_n)$$

et donc par $B_{n,p-1}, S = Q = 0$ ce qui achève la démonstration. □

3.2 Le théorème de Fisher

Théorème (Fisher, 1915) : Soit k un corps. Soit G un sous-groupe abélien fini de $GL_n(k)$ d'exposant e. On suppose que car(k) ne divise pas e et que k contient les racines e-ièmes de l'unité. Alors $k(T_1, ..., T_n)^G$ est isomorphe à $k(T_1, ..., T_n)$, ie (G, k) vérifie le problème de Noether.

démonstration :
Soit $g \in G$. Alors $P(T) = T^e - 1$ annule g et est scindé à racines simples sur k puisque k contient les racines e-ième de l'unité et car(k) ne divise pas e donc g est diagonalisable. Les éléments de G commutant dans leur ensemble, il existe une base de k^n telle que toute $g \in G$ soit diagonale dans cette base.

Supposons que φ soit un isomorphisme de $k(T_1, ..., T_n)^{pGp^{-1}}$ sur $k(T_1, ..., T_n)$. Alors ψ définie de $k(T_1, ..., T_n)^G$ sur $k(T_1, ..., T_n)$ par $\psi(P) = p.\varphi(p^{-1}.P)$ est un isomorphisme donc on peut considérer que les éléments de G sont diagonaux, à diagonale à valeurs dans les racines e-ièmes de l'unité de k.

Ainsi, l'action de $g \in G$ sur T_i^m prend la forme $\lambda_i^m T_i^m$ où λ_i est une racine e-ième de l'unité. Un polynôme est donc dans $k(T_1, ..., T_n)^G$ ssi il est somme de monômes de $K^G := k(T_1, ..., T_n)^G$.

Soit $P = \frac{Q}{R} \in K^G$. Alors on peut écrire $P = \frac{1}{|G|} \sum_{g \in G} \frac{g.Q}{g.R}$ car P est invariant sous l'action de G et en réduisant au même dénominateur, on peut écrire $P = \frac{Q_1}{R_1}$ où Q_1 et R_1 sont des polynômes invariants donc sommes de monômes de K^G. Ainsi, l'ensemble des $T_1^{k_1}...T_n^{k_n}$ qui sont dans K^G où $(k_1, ..., k_n) \in \mathbb{Z}^n$ engendre K^G.

Posons $G' = \{(k_1, ..., k_n) \in \mathbb{Z}^n, T_1^{k_1}...T_n^{k_n} \in K^G\}$ qui est un sous-groupe de $\mathbb{Z}^n$ car $T_1^{k_1}...T_n^{k_n} \in K^G$ ssi $\lambda_1(g)...\lambda_n(g) = 1 \ \forall g \in G$. Or G' contient les $(e, 0, ..., 0), ..., (0, ..., 0, e, 0, ..., 0), ..., (0, ..., 0, e)$ qui sont indépendants sur $\mathbb{Z}$ donc il existe $(k_1, ..., k_n) \in \mathbb{Z}^n$ tels que $G' = k_1\mathbb{Z} \oplus ... \oplus k_n\mathbb{Z}$ car G' est un sous groupe de $\mathbb{Z}^n$ de rang n.

On considère alors le morphisme qui à T_i associe T_i^e qui est bien définie d'après la somme directe du dessus et qui est surjectif d'après ce qu'on a vu au début, c'est donc un isomorphisme de corps, ce qui achève la démonstration. □

4 Un peu de théorie des nombres

Pour montrer le contre exemple au problème de Noether, nous allons travailler avec $\mathbb{Q}_2$ et nous aurons besoin de plusieurs résultats sur les corps p-adiques. Nous allons suivre le livre Corps locaux de Serre [SERRE].

4.1 Construction topologique de $\mathbb{Q}_p$

Définition : Un anneau A est appelé anneau de valuation discrète si c'est un anneau principal et s'il possède un idéal premier $\mathfrak{m}(A)$ et un seul. En particulier, $\mathfrak{m}(A)$ est un idéal maximal.

Dans ce cas, le corps $A/\mathfrak{m}(A)$ est appelé corps résiduel de A, et les éléments de A qui ne sont pas dans $\mathfrak{m}(A)$ sont les inversibles de A.

Dans un anneau principal, les idéaux premiers non nuls sont de la forme πA où π est un élément irréductible, que l'on appelle uniformisante. Un anneau de valuation discrète a donc une unique uniformisante (à une unité près), et ses idéaux sont de la forme $\pi^n A$. Ainsi, si $x \in A$ est non nul, on peut l'écrire sous la forme $\pi^n u$ où u est une unité de A. L'entier n est appelé la valuation de x et noté $v(x)$ et ne dépend pas du choix de π (dans le sens où on

regarde la valuation à une unité près).

Soit K le corps des fractions de A. Si $x = a/b \in K^*$, alors $x = \pi^n u$ où cette fois $n \in \mathbb{Z}$ et on peut poser $v(a/b) = n$. Les propriétés suivantes sont alors vérifiées :

1. l'application $v : K^* \to \mathbb{Z}$ est surjective
2. $v(x+y) \geq \inf(v(x), v(y))$

La fonction v détermine l'anneau A, c'est l'ensemble des éléments de valuation positive, et $\mathfrak{m}(A)$ est l'ensemble des éléments de valuation strictement positive.

On fixe un corps k.

Définition : On appelle valeur absolue sur k une application N de k dans $\mathbb{R}^+$ telle que :

1. $\forall x \in k, N(x) = 0 \iff x = 0$;
2. $\forall (x,y) \in k^2, N(xy) = N(x)N(y)$;
3. $\forall (x,y) \in k^2, N(x+y) \leq N(x) + N(y)$.

Proposition : Soit p un nombre premier. L'application N_p définie par $N_p(a) = p^{-v_p(a)}$ pour $a \in \mathbb{Q}^*$ et $N_p(0) = 0$ où v_p est la valuation p-adique est une valeur absolue sur $\mathbb{Q}$.

Défnition : Une valeur absolue $|.|$ est ultra-métrique si $\forall (x,y) \in k^2, N(x+y) \leq \max(N(x), N(y))$.

Proposition : Une valeur absolue $|\ .\ |$ est ultra-métrique si et seulement si $\forall k \in \mathbb{Z}, |k| \leq 1$.

Proposition : Soit p un nombre premier. Alors N_p est ultra métrique.

Si N est une valeur absolue ultra métrique sur k, on définit

$$\mathcal{O} = \{x \in k, N(x) \leq 1\}, \mathfrak{p} = \{x \in k, N(x) < 1\}$$

Alors $\mathcal{O}$ est un sous anneau de k appelé anneau de valuation de k associé à N et $\mathfrak{p}$ est un idéal de $\mathcal{O}$.

Proposition :

1. L'idéal $\mathfrak{p}$ est maximal

2. L'idéal $\mathfrak{p}$ est l'unique idéal maximal de $\mathcal{O}$

Démonstration :
Un élément de $\mathcal{O}$ est inversible dans $\mathcal{O}$ ssi il est de valeur absolue 1 par multiplicativité de N. Ainsi, $\mathcal{O}^* = \mathcal{O} \setminus \mathfrak{p}$ et donc tout idéal non trivial de $\mathcal{O}$ est inclus dans $\mathfrak{p}$. $\mathfrak{p}$ est donc le plus grand idéal de l'ensemble des idéaux non triviaux de $\mathcal{O}$ ce qui montre le résultat. □

Le corps $\mathcal{O}/\mathfrak{p}$ est appelé corps résiduel de (k,N), et en particulier, $\mathcal{O}$ est un anneau local.

Construction de $\mathbb{Q}_p$:

Soit p un nombre premier. $\mathbb{Q}$ n'est pas complet pour la norme N_p et nous allons le compléter comme pour la construction de $\mathbb{R}$ avec la valeur absolue. Soit C_p l'ensemble des suites de Cauchy à valeurs dans $\mathbb{Q}$ pour la norme N_p . Alors C_p est un anneau. On pose

$$\forall (a,b) \in C_p, a \sim b \Longleftrightarrow \lim_{n\to\infty} N_p(a_n - b_n) = 0$$

Alors $\sim$ est une relation d'équivalence sur C_p et avec
$I = \{a \in C_p, \lim_{n\to\infty} N_p(a_n) = 0\}$, I est un idéal maximal de C_p et on pose

$$\mathbb{Q}_p = C_p/I = C_p/\sim$$

Définition : On appelle anneau de Dedekind un anneau intègre, noethérien, et tel que pour tout idéal premier non nul $\mathfrak{p}$ de A, $A_{\mathfrak{p}}$ est un anneau de valuation discrète.

La notation $A_{\mathfrak{p}}$ correspond à la localisation de A en la partie multiplicative $A - \mathfrak{p}$, que l'on appelle localisation de A en $\mathfrak{p}$.

Définition : Si K est le corps des fonctions de A, un idéal fractionnaire $\mathfrak{a}$ de A est un sous A-module de type fini sur K. Un idéal fractionnaire est inversible s'il existe $\mathfrak{a}' \subset K$ tel que $\mathfrak{a}\mathfrak{a}' = A$.

Proposition : Les idéaux fractionnaires d'un anneau de Dedekink forment un groupe multiplicatif.
La démonstration est dans [SERRE], chapitre 1, paragraphe 3, proposition 5.

Proposition : Si $x \in A$ non nul, alors il n'y a qu'un nombre fini

d'idéaux premiers contenant x.

démonstration : Les idéaux contenant x vérifient la condition de chaîne descendante : si $xA \subset \mathfrak{a} \subset \mathfrak{a}' \subset A$, alors on a $(xA)^{-1} \supset \mathfrak{a}'^{-1} \supset \mathfrak{a}^{-1} \supset A$ et A est noethérien. Ainsi, si $x \in \mathfrak{p}_1, ..., \mathfrak{p}_r, ...$, la suite

$$\mathfrak{p}_1 \supset \mathfrak{p}_1 \cap \mathfrak{p}_2, ..., \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_r, ...$$

est stationnaire donc à partir d'un certain rang, on a $\mathfrak{p}_i \subset \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_r \supset \mathfrak{p}_1 ... \mathfrak{p}_r$ ce qui donne que $\mathfrak{p}_i$ est l'un des $\mathfrak{p}_k$ car ils sont premiers. □

On peut donc énoncer la proposition qui va nous permettre de définir la ramification des idéaux :

Proposition : Soit A un anneau de Dedekind. Tout idéal fractionnaire $\mathfrak{a}$ de A s'écrit de manière unique sous la forme

$$\mathfrak{a} = \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$$

où les $v_\mathfrak{p}(\mathfrak{a})$ sont des entiers presque tous nuls, et où $v_\mathfrak{p}$ est la valuation associée à l'anneau de valuation discrète $A_\mathfrak{p}$.

4.2 Construction algébrique de $\mathbb{Q}_p$

Limite projective d'ensembles

Soient $(I, \leq)$ un ensemble ordonné, $(A_i)_{i \in I}$ une famille d'ensembles indexés par I et pour tout $i \leq j$, f_i^j une application de $A_j \to A_i$ vérifiant les propriétés suivantes :

1. $\forall i \in I, f_i^i = Id_{A_i}$
2. $\forall (i,j,k) \in I^3, i \leq j \leq k \Rightarrow f_i^k = f_i^j f_j^k$

Une telle structure est appelée système projectif d'ensembles. On appelle limite projective de cet ensemble et on le note

$$\varprojlim A_i = \{(a_i) \in \prod_{i \in I} A_i, \forall i \leq j, a_i = f_i^j(a_j)\}$$

Soit p un nombre premier. $\forall n \leq m$, les idéaux $p^m\mathbb{Z}$ et $p^n\mathbb{Z}$ vérifient $p^m\mathbb{Z} \subset p^n\mathbb{Z}$ donc il existe un morphisme d'anneau surjectif

$f_n^m : p^m\mathbb{Z} \to p^n\mathbb{Z}$ et le système $(\mathbb{Z}/p^n\mathbb{Z}, f_n^m)$ est un système projectif.

On note $\mathbb{Z}_p$ sa limite projective, que l'on appelle anneau des entiers p-adiques. Ainsi, un entier p-adique est une suite $(a_n)_{n\in\mathbb{N}}$ telle que $\forall n \in \mathbb{N}, a_n \in \mathbb{Z}/p^n\mathbb{Z}$ et si $n < m, a_n \equiv a_m[p^n]$. De plus, les règles opératoires coordonnées par coordonnées font de $\mathbb{Z}_p$ un anneau.

On obtient alors $\mathbb{Q}_p$ comme étant le corps des fractions de l'anneau intègre $\mathbb{Z}_p$.

4.3 Ramification des idéaux

Soit K un corps de nombre. Un élément x de K est un entier algébrique si il est racine d'un polynôme à coefficients dans $\mathbb{Z}$. On note $\mathcal{O}_K$ l'ensemble des entiers algébrique de K qui est un sous anneau de K.

Soit K un corps de nombre et L/K une extension de K. Si $x \in \mathcal{O}_K$, et que x est irréductible sur $\mathcal{O}_K$, on peut se demander s'il l'est également sur $\mathcal{O}_L$. Par exemple, 2 est irréductible sur $\mathbb{Z}$ mais ne l'est pas sur $\mathbb{Z}(i)$ car $2 = (1+i)(1-i)$ où $1+i$ et $1-i$ sont annulés par $T^2 - 2T - 2$ donc entiers et irréductibles. On peut donc aussi se demander plus généralement comment les idéaux de $\mathcal{O}_K$ se factorisent dans $\mathcal{O}_L$, ce qui motive les paragraphes suivants.

Dans ce paragraphe, on considère un corps K et une extension L de degré fini n. On se donne également un anneau A noethérien et intégralement clos, de corps de fraction K. On note B la fermeture intégrale de A dans L et on peut alors montrer que le corps des fractions de B est L.

Nous ferons dans ce qui suit l'hypothèse suivante : (F) l'anneau B est un A-module de type fini.

Proposition : L'hypothèse (F) est vérifiée lorsque L/K est séparable.

La proposition suivante permet de considérer les idéaux fractionnaires de B car :

Proposition : Si A est de Dedekind, alors B est aussi de

Dedekind.

Si $\mathfrak{b}$ est un idéal premier non nul de B, et que $\mathfrak{p} = \mathfrak{b} \cap A$, on dit que $\mathfrak{b}$ divise $\mathfrak{p}$ ou que $\mathfrak{b}$ est au dessus de $\mathfrak{p}$. On notera $e_{\mathfrak{b}}$ l'exposant de $\mathfrak{b}$ dans la décomposition de $\mathfrak{p}B$ en idéaux premiers. Cet entier est appelé indice de ramification de $\mathfrak{b}$ dans l'extension L/K.

D'autre part, si $\mathfrak{b}$ divise $\mathfrak{p}$, le corps $B/\mathfrak{b}$ est une extension du corps $A/\mathfrak{p}$. Comme B est de type fini sur A, $B/\mathfrak{b}$ est un extension de degré fini sur $A/\mathfrak{p}$. Le degré de cette extension est le degré résiduel de $\mathfrak{b}$ dans l'extension L/K et noté $f_{\mathfrak{b}}$. On a donc $f_{\mathfrak{b}} = [B/\mathfrak{b}, A/\mathfrak{p}]$.

Lorsqu'il y a un seul idéal premier $\mathfrak{b}$ qui divise $\mathfrak{p}$, et que $f_{\mathfrak{b}} = 1$, on dit que L/K est totalement ramifiée en $\mathfrak{p}$. Lorsque $e_{\mathfrak{b}} = 1$ et que $B/\mathfrak{b}$ est séparable sur $A/\mathfrak{p}$, on dit que L/K est non ramifiée en $\mathfrak{b}$. Si L/K est non ramifiée en tous les idéaux premiers au dessus de $\mathfrak{p}$, on dit que L/K est non ramifiée au dessus de $\mathfrak{p}$.

Définition : Soit L/K une extension de corps de nombre. Soit S une partie finie d'idéaux premiers de $\mathcal{O}_K$. On dit que l'extension est non ramifié en dehors de S si elle est non ramifiée partout sauf éventuellement en ces idéaux.

4.4 Lemme de Krasner et corollaires

Soit $(K, |.|)$ un corps valué complet non archimédien, $\overline{K}$ une cloture algébrique de K et $|.|$ l'unique extension de la valeur absolue à $\overline{K}$. Pour $\alpha \in \overline{K}$ posons $d_\alpha = \min\{|\alpha - \alpha'|, \alpha' \neq \alpha \text{ conjugué de } \alpha\}$.

Lemme de Krasner : Si $\beta \in \overline{K}$ est tel que $|\alpha - \beta| < d_\alpha$ alors on a $K[\alpha] \subset K[\beta]$.

démonstration :
Nous allons montrer que pour tout $\sigma \in \mathrm{Gal}(\overline{K}/K[\beta])$, on a $\sigma(\alpha) = \alpha$ ce qui montrera que si $x \in K[\alpha]$, alors pour tout $\sigma \in \mathrm{Gal}(\overline{K}/K[\beta])$, $\sigma(x) = x$ ie $x \in K[\beta]$.
Soit donc $\sigma \in \mathrm{Gal}(\overline{K}/K[\beta])$. Alors $|\sigma(\alpha) - \alpha| \leq \max(|\alpha - \beta|, |\sigma(\alpha) - \beta|) \leq |\alpha - \beta|$ donc par hypothèse $\sigma(\alpha) = \alpha$. $\square$

Pour $f, g \in K[T]$, notons $\|f - g\| = \max|a_k - b_k|$ où $f = \sum a_k T^k$ et

$g = \sum b_k T^k$.

Corollaire : Soit $f \in K[T]$ un polynôme unitaire irréductible séparable. Il existe un $\delta_f > 0$ tel que pour tout $g \in K[T]$ unitaire, si $\|f - g\| < \delta_f$, alors :

1. g est irréductible
2. pour toute racine β de g, il existe une racine α de f telle que $K[\alpha] = K[\beta]$.

démonstration :
Un δ_f convenable sera plus petit que 1 et dans ce cas, si g est tel que $\|f - g\| < \delta_f$, g sera de même degré que f.
Soit d_f =min$\{|\alpha - \alpha'|, \alpha, \alpha' \in \overline{K}, f(\alpha) = f(\alpha') = 0, \alpha \neq \alpha'\}$. Pour une racine β de g, on aura

$$\prod_{\alpha \in \overline{K}, f(\alpha)=0} |\beta - \alpha| = |f(\beta)| = |(f-g)(\beta)| \leq \|f - g\| max(1, \beta^n)$$

Or $\beta \leq$max$(|b_i^{1/i}|) \leq$max$(1, \|g\|)$ =max$(1, \|f\|)$ si $\|f - g\| < \|f\|$ donc si $\|f - g\| <$min$(\|f\|, \frac{(d_f)^n}{max(1, \|f\|^n)})$, alors il existe une racine β de g telle que $|\alpha - \beta| < d_f$.
D'après le lemme de Krasner, on a $K[\alpha] \subset K[\beta]$ mais $K[\alpha]$ est de degré n et $K[\beta]$ est de degré au plus n par la première remarque de la démonstration donc finalement, $K[\alpha] = K[\beta]$ et g est irréductible, ce qui conclut la preuve. □

Corollaire : Soit F une extension finie de $\mathbb{Q}_p$, équipée de la valeur absolue $|.|_p$. Il existe un sous-corps K de F tel que $[K; \mathbb{Q}] = [F; \mathbb{Q}_p]$ et $F = K\mathbb{Q}_p$. De plus, F est le complété de K pour la norme induite par $|.|_p$.

démonstration : On écrit $F = \mathbb{Q}_p[\alpha]$ et $f_\alpha \in \mathbb{Q}_p[T]$ le polynôme minimal de α. Alors par densité de $\mathbb{Q}$ dans $\mathbb{Q}_p$, il existe $f \in \mathbb{Q}[T]$ tel que $\|f - f_\alpha\| < d_\alpha$. Par le corollaire précédent, f est irréductible sur $\mathbb{Q}_p[T]$ et admet une racine β dans F telle que $F = \mathbb{Q}_p[\beta]$. Alors f est irréductible dans $\mathbb{Q}[T]$ et le corps $K = \mathbb{Q}[\beta]$ convient. □

5 Un contre-exemple

5.1 Le théorème de Grunwald-Wang

Dans la démonstration du contre-exemple au problème de Noether, nous allons utiliser le contre-exemple de Wang au problème de Grunwald-Wang : il n'existe pas d'extension $k/\mathbb{Q}$ cyclique de degré 8 (donc de groupe $\mathbb{Z}/8\mathbb{Z}$) telle que $k_2/\mathbb{Q}_2$ soit non ramifiée de degré 8. Nous allons donc énoncer le théorème de Grunwald-Wang puis montrer ce résultat.

Ce théorème consiste à se demander quand est-ce-qu'une racine n-ième d'un coprs de nombre k est une racine n-ième dans les complétés k_p de k et réciproquement. C'est un principe local-global qui permet de ramener sous certaines hypothèses la recherche de racines n-ièmes de k sur ses complétés, c'est le même principe que la réduction des équations sur $\mathbb{Z}$ modulo un nombre premier.

Définition : Soit k un corps de nombre. On dit que k est s-spécial si k contient η_s mais ne contient ni η_{s+1} ni $i\eta_{s+1}$ où on définit η_s par $\eta_s = 2\cos(\frac{2\pi}{2^s})$.

Notations :
Pour k un corps de nombre et n un entier, on note $\mu_n(k)$ l'ensemble des racines $n-$ièmes de k, et pour S un ensemble fini d'éléments premiers de k, on note $k(n,S) = \{x \in k, \forall p \notin S, x \in \mu_n(k_p)\}$.

Théorème :
On a avec les notations précédentes, $k(n,S) = \mu_n(k)$ sauf dans le cas *spécial*, cas où les deux conditions suivantes sont satisfaites :

1. k est s-spécial pour un s tel que 2^{s+1} divise n
2. S contient l'ensemble S_0 des premiers p tels que k_p est s-spécial

Proposition : Soit $L/\mathbb{Q}$ une extension galoisienne de groupe $\mathbb{Z}/8\mathbb{Z}$. Si l'extension $L_2/\mathbb{Q}_2$ est non ramifiée, alors $Gal(L_2/\mathbb{Q}_2)$ n'est pas $\mathbb{Z}/8\mathbb{Z}$.

démonstration :

On suppose par l'absurde que $L_2/\mathbb{Q}_2$ est non ramifiée et que

$Gal(L_2/\mathbb{Q}_2) = \mathbb{Z}/8\mathbb{Z}$. Soit $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ une extension quadratique contenue dans $L/\mathbb{Q}$ où D est sans facteurs carrés. Comme L_2 est non ramifiée, l'idéal premier $2\mathcal{O}_{L_2}$ est non ramifié donc il en est de même pour $2\mathcal{O}_L$. Ainsi, $2\mathcal{O}_L = P_1...P_n$ pour $n \leq 8$. Nous allons montrer que $2\mathcal{O}_L$ est inerte.

On sait d'après la partie 4 que $[L_{P_i} : \mathbb{Q}_2] = e_{P_i} f_{P_i}$ où L_{P_i} est la complétion de L avec la norme $|.|_{P_i}$ et comme $L = \mathbb{Q}(\alpha)$ où $\alpha \in L$, on a $L_{P_i} = (\mathbb{Q}(\alpha))_2$ qui est aussi $\mathbb{Q}_2(\alpha)$. Nous avons donc $L_{P_i} = \mathbb{Q}(\alpha))_2 = L_2$ et donc $f_{P_i} = [L_2 : \mathbb{Q}_2] = 8$ donc comme $\sum_1^n e_{P_i} f_{P_i} = 8$, on en déduit que $n = 1$ et donc $2\mathcal{O}_L$ est inerte. Nous allons maintenant montrer que cela implique que D n'est pas congru à 1 modulo 8.

L'anneau des entiers de $\mathbb{Q}(\sqrt{D})$ est $\mathbb{Z}[\frac{d+\sqrt{d}}{2}]$ où d est le discriminant de $\mathbb{Q}(\sqrt{D})$. Le polynôme minimal de $\frac{d+\sqrt{d}}{2}$ est

$$(T - \frac{d+\sqrt{d}}{2})(T - \frac{d-\sqrt{d}}{2}) = T^2 - dT + \frac{d^2-d}{4}$$

On sait que $d = D$ si $D \equiv 1[4]$ et $d = 4D$ sinon. En supposant que $D \equiv 1[8]$, alors $d = D \equiv 1[8]$ et $d^2 - d \equiv 1 - 1 \equiv 0[8]$ donc $\frac{d+\sqrt{d}}{2} \equiv 0[2]$. Ainsi,

$$T^2 - dT + \frac{d^2-d}{4} \equiv T^2 + T[2] = T(T+1)[2],$$

donc $2\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = (2, \frac{d+\sqrt{d}}{2})(2, \frac{d+\sqrt{d}}{2} + 1)$ qui est totalement décomposé, ce qui contredit le fait que $2\mathcal{O}_L$ est inerte. Ainsi, D n'est pas congru à 1 modulo 8.

Si la décomposition de D en facteurs premiers ne contenait que des premiers congrus à 1 modulo 8, alors D serait congru à 1 modulo 8 donc il existe un premier p tel que ce ne soit pas le cas. Nous allons montrer que p est aussi congru à 1 modulo 8, ce qui sera contradictoire et conclura la preuve. Nous allons montrer que p est totalement ramifié dans L.

Soit τ un idéal premier au dessus de p et $I(\tau/p)$ son groupe d'inertie, ie $I(\tau/p) = \{\sigma \in Gal(L/\mathbb{Q}), \forall x \in \mathcal{O}_L, \sigma(x) = x \ mod \ \tau\}$. On a $e_{L/\mathbb{Q}}(p) = |I(\tau/p)|$. Soit q l'idéal premier $\tau \cap \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ dans $\mathbb{Q}(\sqrt{D})$. D'après la définition, $I(\tau/q) = H \cap I(\tau/p)$ où $H = Gal(L/\mathbb{Q}(\sqrt{D})) = \mathbb{Z}/4\mathbb{Z}$.

Si $I(\tau/p)$ était contenu dans H, alors $|I(\tau/p)| = |I(\tau/q)|$ et alors

$e_{L/\mathbb{Q}} = e_{L/\mathbb{Q}(\sqrt{D})}$ et p ne serait pas ramifié dans $\mathbb{Q}(\sqrt{D})$ ce qui n'est pas vrai car p divise D. $I(\tau/p)$ n'est pas contenu dans H et comme $Gal(L/\mathbb{Q}) = \mathbb{Z}/8\mathbb{Z}$, le seul sous-groupe non contenu dans H de $\mathbb{Z}/8\mathbb{Z}$ est $\mathbb{Z}/8\mathbb{Z}$ lui-même et donc $e_{L/\mathbb{Q}}(p) = 8 = |I(\tau/p)|$ et donc p est totalement ramifié dans L.

D'après un résultat de théorie algébrique des nombres, le groupe d'inertie de τ est un sous groupe de $\mathbb{F}_p^*$ mais c'est également $\mathbb{Z}/8\mathbb{Z}$ donc $8 \mid p-1$ et donc $p \equiv 1[8]$, ce qui est une contradiction. Ainsi, $Gal(L_2/\mathbb{Q}_2)$ n'est pas $\mathbb{Z}/8\mathbb{Z}$. □

5.2 Birationalité des variétés algébriques

Soit k un corps. Soit X une variété algébrique intègre sur k. On note $k(X)$ le corps des fonctions de la variété X sur k. On note également $\mathbb{A}_n$ l'espace affine de dimension n sur k et $\mathbb{P}_n$ l'espace projectif. L'ensemble des points rationnels sur k de X est noté $X(k)$.

Définition : Soit X et Y deux variétés intègres sur k. On dit que X et Y sont birationnellements équivalentes si les deux conditions suivantes sont respectées :

1. les corps de fonctions $k(X)$ et $k(Y)$ sont isomorphes sur k
2. il existe des ouverts de Zariski non vides $U \subset X$ et $V \subset Y$ qui sont isomorphes sur k.

Définition : Une variété X sur k est dite k-rationnelle si elle est intègre et k-birationnelle à un espace affine (on a donc $k(X)$ isomorphe à $k(T_1, ..., T_n)$ pour un certain entier n, on dit que $k(X)$ est pure sur k). Une variété X sur k est stablement k-rationnelle si il existe un entier n tel que $X \times_k \mathbb{A}_n$ soit k-rationnelle.

Avec cette définition , on voit que l'espace affine $\mathbb{A}_n$ est k-rationnel. On voit aussi que si X est k-rationnelle, alors elle est aussi stablement k-rationnelle.

Exemple : On considère la variété C définie par l'équation $x^2 + y^2 - 1 = 0$ qui correspond au cercle dans le plan affine. Elle est k-rationnelle car on peut paramétrer le cercle par $t \mapsto (\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2})$ qui est une application rationnelle de $\mathbb{A}_1$ dans C dont la réciproque est donnée par la projection stéréographique du

cercle privé d'un point sur la droite.

5.3 $\mathbb{Q}(T_1, ..., T_8)^{\mathbb{Z}/8}/\mathbb{Q}$ n'est pas rationnelle

L'idée de la preuve est la suivante : d'après le théorème de Lüroth, tout sous corps de $\mathbb{Q}(T)$ différent de $\mathbb{Q}$ est isomorphe à $\mathbb{Q}(T)$, et donc l'extension est rationnelle. C'est pour cette raison que l'on se demande si $\mathbb{Q}(T_1, ..., T_8)^{\mathbb{Z}/8}/\mathbb{Q}$ est rationnelle. Si c'est le cas, cette extension serait isomorphe à $\mathbb{Q}(T_1, ..., T_8)$.

Or $\mathbb{Q}(T_1, ..., T_8)$ est le corps de fonctions de l'espace affine $\mathbb{A}^8_{\mathbb{Q}}$, et si l'on note $V = \mathbb{A}^n_{\mathbb{Q}}/G$ une variété algébrique dont $\mathbb{Q}(T_1, ..., T_8)^{\mathbb{Z}/8}$ est le corps de fonctions, alors V est birationnelle à l'espace affine $\mathbb{A}^8_{\mathbb{Q}}$.

Il existe donc $U \subset V$ et $U' \subset \mathbb{A}^8_{\mathbb{Q}}$ des ouverts pour la topologie de Zariski isomorphes, et de même il existe $U_2 \subset V_2$ et $U'_2 \subset \mathbb{A}^8_{\mathbb{Q}_2}$ correspondant aux points 2-adiques où $V_2 = \mathbb{A}^n_{\mathbb{Q}_2}/G$ est la variété dont le corps de fonctions est $\mathbb{Q}_2(T_1, ..., T_8)^{\mathbb{Z}/8\mathbb{Z}}$.

Mais les points rationnels de U' sont denses dans ceux de U'_2 et donc les points de U devraient être denses dans les points rationnels 2-adiques de U_2. Mais en utilisant le lemme de Krasner, on aurait une extension $L/\mathbb{Q}$ de groupe de Galois $\mathbb{Z}/8\mathbb{Z}$ telle que si L_2 est l'unique extension non ramifiée de $\mathbb{Q}_2$ de groupe de Galois $\mathbb{Z}/8\mathbb{Z}$ (cette assertion est démontrée dans [STEV]), alors $L_2 \simeq L \otimes_{\mathbb{Q}} \mathbb{Q}_2$ ce qui contredit le contre exemple de Wang au problème de Grunwald-Wang démontré à la partie 5.

Ainsi, les points rationnels de U ne sont pas denses dans ceux de U_2 et alors V n'est pas birationnelle à l'espace affine $\mathbb{A}^8_{\mathbb{Q}}$, ce qui veut encore dire que l'extension $\mathbb{Q}(T_1, ..., T_8)^{\mathbb{Z}/8}/\mathbb{Q}$ n'est pas rationnelle.

6 Conclusion

Le premier contre exemple au problème de Noether a été trouvé par Swan (démonstration dans [CONJ]) avec $k = \mathbb{Q}$ et $G = \mathbb{Z}/47\mathbb{Z}$ dans les années 60. Plus tard, Saltman publie dans [SALT] une démonstration pour $k = \mathbb{Q}$ et $G = \mathbb{Z}/8\mathbb{Z}$. Il utilise les extensions galoisiennes génériques et la notion de polynôme générique associé

à une extension galoisienne.

Les différents liens qui apparaissent sont qu'une réponse affirmative au problème de Noether implique une réponse affirmative à l'existence de polynômes génériques qui implique une réponse affirmative au problème de Galois inverse, mais les réciproques sont fausses. Saltman fait également un lien avec le problème de Grunwald en montrant qu'une réponse affirmative au problème de Noether implique une réponse affirmative au problème de Grunwald.
Une importante contribution de Saltman a aussi été de trouver le premier contre exemple pour $\mathbb{C}$ (dans [SALT1], page 71) : il a montré que pour tout nombre premier p, il existe un groupe d'ordre p^9 tel que l'extension ne soit pas rationnelle.

Le problème pour $G = A_n$ et $k = \mathbb{Q}$ reste encore une question ouverte.

Pour conclure, on peut énoncer un théorème de Lenstra (voir l'article [LNSTR])qui donne une caractérisation de la rationnalité pour $k = \mathbb{Q}$ et $G = \mathbb{Z}/n\mathbb{Z}$:

Théorème : Soit $n \geq 1$ un entier. Soit $G = \mathbb{Z}/n\mathbb{Z}$ agissant fidèlement sur $\mathbb{A}^n_{\mathbb{Q}}$ par permutation des coordonnées. Les conditions suivantes sont équivalentes :

1. La variété $\mathbb{A}^n_{\mathbb{Q}}/G$ est $\mathbb{Q}$-rationnelle
2. La variété $\mathbb{A}^n_{\mathbb{Q}}/G$ est stablement $\mathbb{Q}$-rationnelle
3. L'entier n n'est pas divisible par 8 et pour tout p premier dans la décomposition en facteurs premiers de n, si s est la valuation p-adique de n, l'anneau $\mathbb{Z}[\xi_{(p-1)p^{s-1}}]$ contient un élément dont la norme vaut p ou $-p$.

Références

[HLBT] Villarino, Gasarch and Regan, Hilbert's Proof of His Irreducibility Theorem, 2018

[AMS] Fehm, Haran and Paran, The inverse Galois problem over $\mathbb{C}(z)$, Abelian Varieties and Number Theory, 2021

[KRAUS] Kraus, Théorie de Galois, Cours accéléré de DEA, 1998

[SERRE] Serre, Corps locaux, 1962

[STEV] Stevenhagen, Number Rings, 2017

[CONJ] Martinet, Un contre-exemple à une conjecture d'E.Noether, Séminaire Bourbaki, 1969

[LNSTR] Lenstra, Rational functions invariant under a cyclic group, Proc. Queen's Number Theory Conf. 1979, Queen's Pap. Pure Appl. Math. 54, 91-99 (1980)., 1980.

[SALT] Saltman, Generic Galois extensions and problems in field theory, Adv. Math. 43 (1982), 250–283

[SALT1] Saltman, Noether's problem over an algebraically closed field, Invent.math, 77 (1984)