# Autour du Problème de Galois Inverse

Hao Fu, Andrea Negro et Yiru Zheng

Prof. Jean-François Dat

Département de mathématiques et applications
École normale supérieure

June 2018

June 2018

# *Résumé*

Ce rapport concerne le problème inverse de Galois. À un polynôme irréductible $P \in \mathbb{Q}[X]$ est attaché son groupe de Galois, le groupe des automorphismes du corps engendré par les racines de $P$. Réciproquement, étant donné un groupe fini $G$, y a-t-il un polynôme dont le groupe de Galois est $G$ ? Cette question n'est pas encore résolue [4]. Par le théorème d'irréductibilité de Hilbert, on peut la réduire au même problème sur $\mathbb{Q}(T)$. Par des méthodes de géométrie, on peut résoudre le problème sur $\mathbb{C}(T)$. Et par la méthode de rigidité, on peut parfois descendre certaines extensions de $\mathbb{C}(T)$ à $\mathbb{Q}(T)$.

# Table des matières

# Chapitre 1

# Introduction à la théorie de Galois

## 1.1 Introduction

L'objectif de cette section est de fournir une introduction au problème de Galois inverse. Pour cela, nous allons d'abord commencer par une introduction à la théorie de Galois.

### 1.1.1 Extensions de décomposition

Soit un corps $K$ et un polynôme $P \in K[X]$. Une extension de corps $K \subset E$ est dite extension de décomposition de $P$ si $P$ est scindé dans $E$, et $E$ est engendré par ses racines. On a la propriété suivante, importante, sur les extensions de décomposition :

**Proposition 1.1.1.** *Soit un corps $K$ et $P \in K[X]$ non constant. Alors il existe une extension de décomposition de $P$, unique à isomorphisme près.*

Cette propriété se démontre par récurrence sur le degré de $P$.

Posons maintenant un corps $K$, un polynôme $P \in K[X]$ et une extension de décomposition $K \subset E$. Etudions les automorphismes de cette extension, c'est-à-dire les morphismes de corps de $E$ dans $E$ qui sont aussi des morphismes de $K$-algèbres. Puisque $E$ est engendré par les racines de $P$, l'image de celles-ci détermine entièrement un automorphisme. D'autre part, puisqu'un tel automorphisme est un morphisme de corps et d'algèbres, il commute avec les polynômes, et donc pour tout tel automorphisme $f$, $\forall x \in E, P(x) = 0 \Rightarrow P(f(x)) = 0$.

Par conséquent, si on a une extension de décomposition $K \subset E$ de $P$, et si on note $\mathcal{R}$ l'ensemble des racines de $P$ dans $E$, l'action de $Aut(E/K)$ permute les racines. En fait,

l'action de $Aut(E/K)$ sur $\mathcal{R}$ est fidèle, par conséquent $Aut(E/K)$ est isomorphe à un sous-groupe de $\mathfrak{S}(\mathcal{R})$.

### 1.1.2 Exemples

Etudions quelques exemples élémentaires d'extensions de décomposition, en se plaçant sur $\mathbb{Q}$.

- Le polynôme $P = X^2 - 2$ possède pour corps de décomposition $\mathbb{Q}(\sqrt{2})$, dont le groupe d'automorphismes est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
- Le polynôme $P = X^3 - 2$ possède pour corps de décomposition $\mathbb{Q}(\sqrt[3]{2}, j)$. Calculons son groupe d'automorphismes. Ce groupe contient :
  - Un élément d'ordre 2, le morphisme envoyant $j$ sur $j^2$ et $\sqrt[3]{2}$ sur $\sqrt[3]{2}$, qui est en fait la restriction de la conjugaison complexe au corps étudié.
  - Un élément d'ordre 3; le morphisme envoyant $\sqrt[3]{2}$ sur $\sqrt[3]{2}j$ et $j$ sur $j$. En fait soit un élément de $\mathbb{Q}(\sqrt[3]{2}, j)$. On peut en fait l'écrire sous la forme $\alpha + \beta\sqrt[3]{2} + \gamma\sqrt[3]{4}$ où $(\alpha, \beta, \gamma) \in \mathbb{Q}(j)^3$. On peut voir que le morphisme $\alpha + \beta\sqrt[3]{2} + \gamma\sqrt[3]{4} \to \alpha + \beta j\sqrt[3]{2} + \gamma j^2\sqrt[3]{4}$ est bien défini, et correspond bien à ce que l'on cherche.

  Puisque le groupe contient un élément d'ordre 2 et un élément d'ordre 3, et de plus est un sous-groupe de $\mathfrak{S}_3$, il s'agit donc de $\mathfrak{S}_3$.
- L'extension de décomposition du polynôme $P = X^3 + X^2 - 2X - 1$ possède pour groupe d'automorphismes $\mathbb{Z}/3\mathbb{Z}$.
- Le polynôme $P = X^n - 1$ possède pour corps de décomposition $K = \mathbb{Q}(\zeta_n)$ où $\zeta_n$ est une racine $n$-ième primitive de l'unité. Un automorphisme de $\mathbb{Q}(\zeta_n)$ vérifie $f(\zeta_n)^n = 1$ mais $f(\zeta_n)^d \neq 1$ pour $1 \leq d \leq n-1$. Par conséquent, il vérifie $f(\zeta_n) = \zeta_n^l$ où $1 \leq l \leq n-1$ et $l \wedge n = 1$. On a alors une action fidèle par automorphismes de groupes de $Gal(K/\mathbb{Q})$ sur le groupe $\mu_n$ des racines de l'unité, et on en déduit que $Gal(K/\mathbb{Q}) < (\mathbb{Z}/n\mathbb{Z})^*$. Montrons qu'en fait ces deux groupes sont isomorphes. On peut montrer par récurrence forte que les polynômes $\Phi_n = \Pi_{1\leq k\leq n-1, k\wedge n=1}(X - \zeta_n^k) \in \mathbb{Q}(\zeta_n)[X]$ sont en fait à coefficients entiers. Montrons de plus qu'ils sont irréductibles dans $\mathbb{Q}[X]$ : fixons pour cela $n \in \mathbb{N}$. Supposons $\Phi_n$ non irréductible, il existerait alors $f$ et $g$ tels que $\Phi_n = fg$ avec $f$ et $g$ premiers entre eux. Posons un nombre premier $p$ premier avec $n$. En passant dans $\mathbb{Z}/p\mathbb{Z}$, on obtiendrait alors $\bar{\Phi_n} = \bar{f}\bar{g}$ et il existe $(\bar{u}, \bar{v}) \in (\mathbb{Z}/p\mathbb{Z})^2$ tels que $\bar{u}\bar{f} + \bar{v}\bar{g}(X^p) = 1$, car $\bar{g}(X^p) = \bar{g}^p$. On peut relever ceci sur $\mathbb{Z}$, et on a l'existence de $u$, $v$ et $w$ polynômes sur $\mathbb{Z}$ tels que $uf(X) + vg(X^p) = 1 + pw$. S'il existe une racine de $f$ $\zeta$, elle vérifie alors $g(\zeta^p) \neq 0$ car $w(\zeta)$ est un entier algébrique. Donc $\zeta^p$ est racine de $f$. Faisant varier $p$, on voit que l'ensemble des racines de $f$ est stable par

élévation à la puissance $l$ pour tout $l$ premier à $p$ et donc $g$ est constant. Donc $\Phi_n$ est irréductible, et par construction il possède également $\mathbb{Q}(\zeta_n)$ comme corps de décomposition. On a alors que le degré de l'extension est en fait le degré de $\Phi_n$, c'est-à-dire ici $\phi(n)$. Donc $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

### 1.1.3 Extensions galoisiennes

Pour une extension de corps quelconque $K \subset L$, on définit son degré comme la dimension de $L$ en tant que $K$-algèbre, que l'on note $[K : L]$.

**Définition 1.1.2.** *Une extension $K \subset L$ est dite galoisienne si $|Aut(L/K)| = [K : L]$. Dans ce cas, le groupe d'automorphismes est appelé groupe de Galois de cette extension, et est noté $Gal(L/K)$.*

Une propriété connue des extensions galoisiennes est la propriété suivante :

**Proposition 1.1.3.** *Soit une extension de corps $K \subset L$. Elle est galoisienne si et seulement si il existe un polynôme $P \in K[X]$, scindé à racines simples sur $L$ dont elle est une extension de décomposition.*

Les exemples donnés précédemment sont donc des extensions galoisiennes, dont on a déjà déterminé le groupe de Galois.

Un théorème fondamental en théorie de Galois est la correspondance de Galois.

**Théorème 1.1.4.** *Soit une extension galoisienne $K \subset L$ de groupe de Galois $G$. Soit $H < G$. Alors $L^H \subset L$ est galoisienne de groupe $H$. De plus si $H \lhd G$, alors $K \subset L^H$ est galoisienne de groupe $G/H$.*

Ce théorème établit en fait une correspondance entre les sous-extensions d'extensions galoisiennes et les sous-groupes de leur groupe de Galois.

### 1.1.4 Introduction au problème de Galois inverse

Le problème de Galois inverse est le problème suivant : Sur un corps $K$ donné, connaissant un groupe $G$, peut-on trouver un polynôme $P \in K[X]$, dont les extensions de décomposition ont pour groupe de Galois $G$.

Une remarque intéressante est que pour tout groupe fini $G$, on peut trouver un corps $K$ et une extension $K \subset L$ de groupe de Galois $G$. Ceci provient en fait de la remarque suivante : si on a un corps $k$, alors pour tout entier $n$ on dispose du corps $k(X_1, \cdots, X_n)$ des fractions rationnelles en les $X_i$. Alors on peut poser l'extension de corps $k(S_1, \cdots, S_n) \subset k(X_1, \cdots, X_n)$, où les $S_1, \cdots, S_n$ sont les polynômes symétriques

élémentaires en $X_1, \cdots, X_n$. Cette extension est galoisienne, de groupe de Galois $\mathfrak{S}_n$. Puisque tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique, on peut conclure avec la correspondance de Galois.

Néanmoins, ceci ne résout pas le problème de Galois inverse, car le corps sur lequel on cherche l'extension est fixé.

En ce qui concerne la résolution du problème de Galois inverse sur $\mathbb{Q}$, on montrera plus loin qu'il est possible de le réduire au problème sur $\mathbb{Q}(T)$. En effet on montrera que pour tout $P \in \mathbb{Q}(T)[X]$ irréductible, il existe $t \in \mathbb{Q}$ tel que les extensions de décomposition de $P(t)$ sur $\mathbb{Q}$ et de $P$ sur $\mathbb{Q}(T)$ soient de groupes de Galois isomorphes. Ceci est en fait un cas particulier d'un théorème plus général, appelé théorème d'irréducibilité de Hilbert, qui sera aussi étudié plus loin.

La correspondance de Galois permet de résoudre sur $\mathbb{Q}$ le cas où $G$ est abélien fini.

**Proposition 1.1.5.** *Pour tout groupe $G$ abélien fini, il existe une extension de $\mathbb{Q}$ de groupe de Galois $G$.*

La démonstration repose sur le théorème suivant :

**Théorème 1.1.6.** *Soit $n$ un entier $\geq 2$. Il existe une infinité de nombres premiers congrus à 1 modulo $n$.*

Il s'agit d'un cas particulier du théorème de la progression arithmétique de Dirichlet, que l'on admettra ici.

*Démonstration.* On sait, d'après le théorème de classification des groupes abéliens finis, que $G \cong \Pi_{i=1}^{r}(\mathbb{Z}/n_i\mathbb{Z})$, où $n_1, \cdots, n_r$ sont des entiers tels que $n_1 | \cdots | n_r$. En posant, $p_1, \cdots, p_r$ des nombres premiers distincts tels que pour $1 \leq i \leq r$, $p_i \equiv 1 \mod n_i$. Ils existent grâce au théorème admis ci-dessus. Puisque pour tout $1 \leq i \leq r$, $p_i | n_i - 1$, on peut écrire $G = \Pi_{i=1}^{r}((\mathbb{Z}/p_i\mathbb{Z})^*/(\mathbb{Z}/\alpha_i\mathbb{Z}))$, où $n_i\alpha_i + 1 = p_i$. Donc en fait $G$ est un quotient de $(\mathbb{Z}/n\mathbb{Z})^*$, où $n$ est le produit des $p_i$. Or on a montré, à l'aide des polynômes cyclotomiques, qu'il existe une extension de $\mathbb{Q}$ ayant pour groupe de Galois $(\mathbb{Z}/n\mathbb{Z})^*$. Par correspondance de Galois, on en déduit l'existence d'une sous-extension d'une extension cyclotomique ayant pour groupe de Galois $G$ sur $\mathbb{Q}$. □

## 1.2 Point de vue géométrique

Pour trouver des extensions de $\mathbb{Q}$, on peut chercher sur $\mathbb{Q}(T)$ et utiliser de la géométrie.

Par exemple, Considérons le groupe $\mathbb{Z}/2\mathbb{Z}$. Pour trouver toutes les extensions galoisiennes de groupe de Galois $\mathbb{Z}/2\mathbb{Z}$, on considère l'application $\mathbb{P}^1 \to \mathbb{P}^1$ donnée par $x \mapsto x^2$.

Ceci induit une application entre les corps de fonctions, $\mathbb{Q}(X) \to \mathbb{Q}(T)$ donnée par $X \mapsto T^2$. C'est une extension de corps donnée par un polynôme de degré 2, $T^2 - X$. Il s'agit d'une extension galoisienne du corps de fonctions $\mathbb{Q}(T)$ de groupe de Galois $\mathbb{Z}/2\mathbb{Z}$. Et en regardant les points de $\mathbb{P}^1$, l'image réciproque de l'idéal $(X - a)$ est $(T^2 - a)$. Le corps résiduel de l'idéal maximal $(T^2 - a)$ de $\mathbb{Q}[T]$ est $\mathbb{Q}[T]/(T^2 - a)$. Ces extensions de corps donnent toutes les extensions de $\mathbb{Q}$ de groupe de Galois $\mathbb{Z}/2\mathbb{Z}$.

Par le théorème d'irréductibilité de Hilbert qui va être démontré dans le chapitre 2, si on trouve une extension finie de $\mathbb{Q}(T)$ de groupe de Galois $G$, alors il existe une extension de $\mathbb{Q}$ de groupe de Galois $G$.

Pour trouver ces extensions de $\mathbb{Q}(T)$, considérons les extensions de $\mathbb{C}(T)$ de groupe de Galois $G$. Par la correspondance entre variétés analytiques et variétés algébriques complexes, une extension finie de $\mathbb{C}(T)$ correspond à un revêtement ramifié de $\mathbb{P}_1(\mathbb{C})$, donc à un quotient fini du groupe fondamental

$$\langle \gamma_1, \gamma_2, \cdots, \gamma_n | \gamma_1 \cdot \gamma_2 \cdot \cdots \cdot \gamma_n = 1 \rangle^\wedge$$

de $\mathbb{P}_1(\mathbb{C}) \backslash \{n \text{ points distincts}\}$. De plus, une telle extension induit aussi une extension de $\bar{\mathbb{Q}}(T)$ de même degré. Alors un système de générateur de $n$ éléments de $G$ induit un épimorphisme de $\langle \gamma_1, \gamma_2, \cdots, \gamma_n | \gamma_1 \cdot \gamma_2 \cdot \cdots \cdot \gamma_n = 1 \rangle^\wedge$ à $G$ ainsi qu'une action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur $G$ (bien définie à conjugaison près). La méthode de rigidité montre que si l'ensemble des classes de conjugaison des $\sigma_i$ est stable par $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ et si la conjugaison par $G$ est transitive sur la réunion de ces classes, alors $G$ est groupe de Galois d'une extension de $\mathbb{Q}(T)$.

Ceci donne une approche au problème inverse de Galois. Premièrement, trouvez une extension galoisienne de $\mathbb{Q}(T)$ de groupe de Galois $G$. Deuxièmement, en utilisant le théorème d'irréductibilité de Hilbert, spécialisez-la en un point $P$ à une extension de $\mathbb{Q}$.

Ce rapport sera divisé en deux parties. Au chapitre 2, la preuve du théorème d'irréductibilité de Hilbert sera donnée, ainsi que des applications et exemples. Au chapitre 3, certaines extensions de $\mathbb{Q}(T)$ seront trouvées.

# Chapitre 2

# Théorème d'irréductibilité de Hilbert

## 2.1 Démonstration du théorème d'irréductibilité de Hilbert

Soit $P$ un polynôme à coefficients dans le corps $\mathbb{Q}(T)$ des fractions rationnelles. Supposons $P$ irréductible en tant que polynôme de $\mathbb{Q}(T)[X]$. Nous allons montrer que pour beaucoup de valeurs $t \in \mathbb{Z}$, le polynôme $P(t, X)$ est irréductible. De plus, on rappelle que le groupe de Galois sur $\mathbb{Q}$ du polynôme $P(t, X)$ est un sous-groupe du groupe de Galois sur $\mathbb{Q}(T)$ du polynôme $P(T, X)$. Le théorème suivant affirme que pour beaucoup d'entiers $t$, ces groupes sont égaux.

**Théorème 2.1.1.** *(Théorème d'irréductibilité de Hilbert) Soit $P \in \mathbb{Q}(T)[X]$ un polynôme unitaire à coefficients dans $\mathbb{Q}(T)$, irréductible. Soit $N(B)$ le cardinal de l'ensemble des $t \in [0, B] \cap \mathbb{Z}$ tels que $t$ soit un pôle d'un coefficient de $P$, ou bien tels que $P(t, X)$ soit réductible dans $\mathbb{Q}[X]$. Alors, il existe $\alpha < 1$ tel que $N(B) = O(B^\alpha)$[2]*

Pour la démonstration on utilise les lemmes et les théorèmes suivants.

**Théorème 2.1.2.** *(Puiseux)[1] Soit $H(r)$ l'ensemble des fonctions continues sur le disque fermé $\overline{D}(0, r) \subset \mathbb{C}$ dont la restriction au disque ouvert $D(0, r)$ est holomorphe. $H(r)$ est un anneau et est intègre par le théorème des zéros isolés. Soit $P$ un polynôme unitaire de degré $n$ à coefficients dans $H(r)$. Alors il existe un entier $e \geq 1$, un nombre réel $\rho \in ]0, r^{1/e}[$, et des séries $x_1, \cdots, x_n \in H(\rho)$ telles que*

$$P(z^e, X) = \prod_{i=1}^{n} (X - x_i(z)) \tag{2.1}$$

**Proposition 2.1.3.** *Soit $e$ un entier $\geq 1$, et soit $\phi = \sum_{n \geq -n_0} a_n u^{-n/e}$ une série de Laurent en $u^{-1/e}$ qui n'est pas un polynôme en $u$. (En d'autres termes, cette série a un*

*coefficient $a_n \neq 0$ avec $n > 0$ ou e $\not| \ n$.) Supposons que $\phi(u)$ converge pour $|u| \geq B_0$. Soient l'ensemble $S = \{u \in \mathbb{Z} \mid u \in [B_0, B],\ \phi(u) \in \mathbb{Z}\}$ et $N(B) = |S|$. Alors il existe $\alpha < 1$ telle que $N(B)/B^\alpha$ reste bornée quand $B \to \infty$.*

*Démonstration.* Notons que $\phi$ définit une fonction $C^\infty$ sur l'intervalle $]B_0, +\infty]$, on peut donc calculer la dérivée terme à terme. Pour $m > n_0/e$ fixé, $\phi^{(m)}(u) \to 0$ quand $u \to \infty$, mais n'est pas identiquement nulle car $\phi$ n'est pas un polynôme. $\phi^{(m)}(u)$ est dominée par le coefficient dominant de la forme $cu^{-\mu}$ avec $c \neq 0$ et $\mu > 0$, donc pour $u$ assez grand, disons $u \geq B_1$, on a également $c_1 u^{-\mu} \leq |\phi^{(m)}(u)| \leq c_2 u^{-\mu}$.

On considère maintenant $m+1$ éléments de $S$, $u_0 < \cdots < u_m$ with $u_0 > B_1$, et le déterminant associé

$$D = \begin{vmatrix} 1 & \cdots & 1 \\ u_0 & \cdots & u_n \\ \vdots & \vdots & \vdots \\ u_0^{n-1} & \cdots & u_n^{n-1} \\ \phi(u_0) & \cdots & \phi(u_n) \end{vmatrix} \tag{2.2}$$

$D$ est un entier car tous les coefficients du déterminant le sont. On peut estimer la distance entre deux éléments de $S$ à l'aide du lemme suivant :

**Lemme 2.1.4.** *Soit $I$ un intervalle de $\mathbb{R}$, $f : I \to \mathbb{R}$ une fonction de classe $C^n$ et $x_0, \cdots, x_n$ des éléments de $I$. Alors il existe $\xi \in I$ tel que*

$$D(x_0) = \begin{vmatrix} 1 & \cdots & 1 \\ x_0 & \cdots & x_n \\ \vdots & \vdots & \vdots \\ x_0^{n-1} & \cdots & x_n^{n-1} \\ f(x_0) & \cdots & f(x_n) \end{vmatrix} = \frac{f^{(n)}(\xi)}{n!} \prod_{i>j} (x_i - x_j) \tag{2.3}$$

*[2]*

*Démonstration.* Sans perte de généralité nous pouvons supposer que les $x_i$ sont distincts. Définissons la fonction $F_A(x) = D(x) - A\prod_{i=1}^n (x - x_i)$ pour $A \in \mathbb{R}$, ce qui s'annule en $x_1, \cdots, x_n$; Choisissons $A$ pour qu'elle s'annule aussi en $x_0$.

D'après le lemme de Rolle, il existe au moins un réel $\xi \in I$ tel que $F_A^{(n)}(\xi) = 0$. De plus,

$$F_A^{(n)}(\xi) = (-1)^n f^{(n)}(\xi) \begin{vmatrix} 1 & \cdots & 1 \\ x_0 & \cdots & x_n \\ \vdots & \vdots & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \\ f(x_0) & \cdots & f(x_n) \end{vmatrix} - An! \tag{2.4}$$

donc

$$D(x_0) = A\prod_{i=1}^{n}(x_0 - x_i) = \frac{f^{(n)}(\xi)}{n!}\prod_{i>j}(x_i - x_j) \tag{2.5}$$

□

Revenons à la preuve de la proposition 2.1.3. Par le lemme 2.1.4 il existe un réel $\xi \in ]u_0, u_m[$ tel que

$$D = \frac{1}{m!}\phi^{(m)}(\xi)\prod_{i>j}(u_i - u_j) \tag{2.6}$$

On a alors l'estimation, en utilisant $|D| \geq 1$

$$\prod_{i<j}(u_i - u_j) \geq \frac{m!}{|\phi^{(m)}(\xi)|} \geq \frac{m!}{c_2}\xi^{\mu} \tag{2.7}$$

et en remarquant que $u_i - u_j < u_m - u_0$ pour $i < j$ on a

$$(u_m - u_0)^{m(m+1)/2} \geq \frac{m!}{c_2}u_0^{\mu} \tag{2.8}$$

donc on conclut qu'il existe $b > 0$ et $\beta > 0$ tels que pour tous $B_1 < u_0 < \cdots < u_m$ avec $u_i \in S$ on a

$$u_m - u_0 \geq bu_0^{\beta} \tag{2.9}$$

Soit $\alpha = 1/(1+\beta) < 1$, on a

$$N(B^{\alpha}) \leq B^{\alpha}, \tag{2.10}$$

Pour $B$ suffisamment grand, par exemple $B^{\alpha} \geq B_1$, eq.2.8 implique que pour $m+1$ éléments ordonnés $u_0 < \cdots < u_m$ de $S \cap [B^{\alpha}, B]$ on a $u_m - u_0 \geq bB_1^{\alpha\beta}$, donc

$$N(B) - N(B^{\alpha}) \leq \frac{m}{b}B^{1-\alpha\beta} = \frac{m}{b}B^{\alpha} \tag{2.11}$$

Le résultat $N(B) \leq (1 + m/b)B^{\alpha}$ s'ensuit. □

**Théorème 2.1.5.** *Soit $P$ un polynôme unitaire de $\mathbb{Q}(T)[X]$. Soit $N(B)$ le cardinal de l'ensemble $\{t \in [0, B] \cap \mathbb{Z} \mid P(t, X)$ a une racine dans $\mathbb{Q}\}$. Si $P$ n'a pas de racine dans $\mathbb{Q}(T)$, alors il existe $\alpha < 1$ tel que quand $B \to \infty$, $N(B) = O(B^{\alpha})$.*

*Démonstration.* Nous pouvons supposer que $P \in \mathbb{Z}[T, X]$; Pour voir cela, en général soit $D \in \mathbb{Z}[T]$ un dénominateur commun des coefficients de $P$, de sorte que $P(T, X)D(T)^n = H(T, D(T)X)$, où $H(T, X)$ est un polynôme dans $\mathbb{Z}[T, X]$ n'ayant pas de racine dans $\mathbb{Q}(T)$ (autrement une telle racine $R(T)$ donne une racine $R(T)/D(T)$ de $P$ dans $\mathbb{Q}(T)$). Sauf un nombre fini de racine de $D(T)$, le polynôme spécialization $P(t, X)$ a une racine dans $\mathbb{Q}$ si et seulement si le polynôme $Q(t, X)$ a une racine dans $\mathbb{Q}$. Le supposition suit.

Alors pour tout $t \in \mathbb{Z}$ le pôlynome $P(t, X)$ est unitaire à coefficients entiers, donc ses racines dans $\mathbb{Q}$ ne peuvent être que des entiers d'après le fait que la clôture intégrale de

$\mathbb{Z}$ dans $\mathbb{Q}$ est $\mathbb{Z}$ lui-même. Pour se donner l'estimation que nous souhaitons en utilisant la proposition 2.1.3, il s'agit de introduire le lemme suivant

**Lemme 2.1.6.** *Soit $n$ le degré de $P$ en $X$. il existe un entier $e \geq 1$ et $n$ séries de Laurent $x_1, \cdots, x_n$ à coefficients complexes, de rayon de convergence non nul, tels que pour tout nombre complexe $t$ de module assez grand, les $n$ racines complexes de $P(t^e, X)$ soient les $x_j(1/t)$, pour $1 \leq j \leq n$.*

*Démonstration.* Tout d'abord nous effectuons le changement de variable $T = 1/U$. Nous avons que $L(T, X) = P(1/U, X)$ est un polynôme dans $\mathbb{Q}(U)[X]$, et nous pouvons supposer qu'il est aussi unitaire. Soit $R(U)$ un dénominateur commun des coefficients des $L(T, X)$ dans $\mathbb{Q}(U)$. Alors nous avons l'égalité $R(U)^n P(1/U, X) = H(U, R(U)X)$ avec $H(U, X) \in \mathbb{Q}[U, X]$. D'après le théorème 2.1.2, il existe un entier $e \geq 1$ et des séries entières $y_1, \cdots, y_n$ de rayon de convergence non nul telles que, pour $|u|$ assez petit, les racines du polynôme $H(u^e, Y)$ soient les $y_j(u)$, pour $1 \leq j \leq n$. Alors l'équation devient

$$P(1/u^e, R^{-1}(u^e)y_j(u))R^n(u^e) = 0 \tag{2.12}$$

En développant $R^{-1}(u^e)$ en série de Laurent qui converge pour $|u|$ petit mais non nul, nous avons trouvé $x_j(t) = R^{-1}(1/t^e)y_j(1/t)$ comme voulu. □

Pour terminer la démonstration du théorème 2.1.5, soient $x_1, \cdots, x_n$ les séries fournies par le lemme 2.1.6 telles que $X = x_j(1/t^{1/e})$ soit une solution de l'équation $P(t, X) = 0$ quand $|t|$ est assez grand. Puisque $P$ n'a aucune de racine dans $\mathbb{Q}(T)$, aucune de ces séries un polynôme. Il suffit d'appliquer à chacune d'entre elles la proposition 2.1.3 d'obtenir l'estimation souhaitée. □

**Théorème 2.1.7.** *Soit $P \in \mathbb{Q}(T)[X]$ un polynôme unitaire à coefficients dans $\mathbb{Q}(T)$, irréductible. Soit $N(B)$ le cardinal de l'ensemble des $t \in [0, B] \cap \mathbb{Z}$ tels que $t$ soit un pôle d'un coefficient de $P$, ou bien tels que $P(t, X)$ soit réductible dans $\mathbb{Q}[X]$. Alors, il existe $\alpha < 1$ tel que $N(B) = O(B^\alpha)$*

*Démonstration.* On peut supposer que $P \in \mathbb{Z}[T, X]$, puisque en général on a $D^n(X)P(T, X) = H(X, D(X)X)$ pour le dénominateur. Par le lemme 2.1.6, quand $t$ est assez grand, on peut factoriser $P$ sous la forme

$$P(t, X) = \prod_i (X - x_i(t^{-1/e})) \tag{2.13}$$

Il suffit donc de montrer que pour tout facteur $Q(t, X)$ de $P(t, X)$ sous la forme de produit de facteurs $X - x_i(t^{-1/e})$, l'ensemble des $t \in [0, B] \cap \mathbb{Z}$ tel que $Q(t, X) \in \mathbb{Z}[X]$ est de cardinal $O(B^\alpha)$. Puisque $P(T, X)$ est irréductible dans $\mathbb{Q}(T)[X]$ et $x_i(z)$ est holomorphe en $z$ quand $|z|$ est assez grand, donc en voyant $P_I(T, X)$ comme un polynôme dans $Q(T^{-1/e})[X]$, il existe au moins un coefficient $a_I(T)$ de ce polynôme qui n'est un

polynôme dans $\mathbb{Q}[T]$. Le théorème 2.1.3 nous donne que pour tout tel $a_I(T)$ l'ensemble des $t \in [0, B] \cap \mathbb{Z}$ tels que $a_I(t) \in \mathbb{Z}$ est de cardinal $O(B^\alpha)$ pour un certain $\alpha < 1$. □

**Théorème 2.1.8.** *Soit $P \in \mathbb{Q}(T)[X]$ un polynôme unitaire à coefficients dans $\mathbb{Q}(T)$. Soit $G$ son groupe de Galois sur $\mathbb{Q}(T)$. Soit $N(B)$ le cardinal de l'ensemble des $t \in [0, B] \cap \mathbb{Z}$, alors soit $t$ est un pôle de $P(t, X)$ sur $\mathbb{Q}$, soit le groupe de Galois du polynôme $P(t, X)$ sur $\mathbb{Q}$ est un sous-groupe propre de $G$. Alors il existe $\alpha < 1$ tel que $N(B) = O(B^\alpha)$.*

*Démonstration.* On peut supposer $P \in \mathbb{Z}[T, X]$ puisque l'action de $G$ sur $\mathbb{Q}(T)$ est l'identité. Soit $n = \deg P$ et $K$ le corps de décomposition de $P$ ce qui est galoisien. Soit $\kappa \in K$ un élément primitif de $K$ tel que $K = \mathbb{Q}(T)(\kappa)$ dont le polynôme minimal est $Q(T, X) \in \mathbb{Q}(T)[X]$, de degré $N$. Puisque $K$ est galoisien, on a $N = |G| = [K : \mathbb{Q}(T)]$. Soit $D \in \mathbb{Q}[T]$ un dénominateur commun des coefficients de $Q$, le polynôme minimal de $D\kappa$ est $D(T)^N Q(T, D^{-1}(T)X)$, qui nous permet de supposer que $Q \in \mathbb{Q}[T, X]$.
Notons que le corps de décomposition de $Q$ sur $\mathbb{Q}(T)$ est aussi $K$ d'après le fait que $K$ est normale donc tous l'injecton de $K$ dans la clôture algébrique $\overline{\mathbb{Q}(T)}$, et $K \cong \mathbb{Q}(T)[X]/Q$ permet une telle injection. Ensuite $P$ et $Q$ ont le même groupe de Galois sur $\mathbb{Q}(T)$
D'après le lemme suivant, sauf pour une partie finie $S \subset \mathbb{Q}$ les polynômes $Q(t, X)$ et $P(t, X)$ sont séparables et ont un corps de décomposition $K_t$. D'après le lemme 2.1.10, le groupe de Galois $Gal(K_t/\mathbb{Q})$ peut être considéré comme un sous-groupe de $Gal(K/\mathbb{Q}(T))$, donc $[K_t : \mathbb{Q}] \leq N$. D'après le théorème 2.1.7 appliqué au polynôme $Q$, il existe $\alpha < 1$ tel que le nombre de $t \in [0, B] \cap \mathbb{Z}$ tels que $Q(t, X)$ soit réductible est $O(B^\alpha)$. Cependant pour $t$ tel que $Q(t, X)$ soit irréductible, l'injection des corps $\mathbb{Q}[X]/Q(t, X) \to K_t$ implique $[K_t : \mathbb{Q}] \geq N$, donc on a $[K_t : \mathbb{Q}] = N$ et $Gal(K_t/\mathbb{Q}) \cong Gal(K/\mathbb{Q}(T))$ dans ce cas. Le théorème suit. □

*Remark* 2.1.1. Le théorème 2.1 nous dit qu'il y a beaucoup de $t$ pour lequel le polynôme reste irréductible et a le même groupe de Galois après spécialisation.

**Lemme 2.1.9.** *Soit $P \in \mathbf{Q}(T)[X]$ un polynôme unitaire en $X$, et soit $\mathbf{Q}(T) \to K$ un corps de décomposition de $P$. Alors il existe un ensemble fini $\Sigma \subset \mathbb{Q}$ tel que pour tout $t \notin \Sigma$, les polynômes $Q(t, X)$ et $P(t, X)$ soient séparables en ayant le même corps de décomposition.*

*Démonstration.* Notons $x_1, \cdots, x_n$ les racines de $P$ dans $K$. Puisque $\mathbb{Q}(T)$ est de caractéristique nulle, il existe un élément primitif $y \in K$ de polynôme minimal $Q \in \mathbb{Q}(T)[X]$ tel que $K = \mathbb{Q}(T)(y)$. Donc il existe des polynômes $A_i \in \mathbb{Q}(T)[Y]$ tels que $x_i = A_i(y)$ et $P(T, X)$ est scindé avec

$$P(T, X) = \prod_{i=1}^{n} (X - A_i(T, y)) \tag{2.14}$$

Alors $Y = y$ est une racine du polynôme $G(T, X, Y) \in \mathbb{Q}(T)[X, Y]$ défini par

$$G(T, X, Y) = P(T, X) - \prod_{i=1}^{n}(X - A_i(T, Y)) \tag{2.15}$$

ensuite il existe un polynôme $R \in \mathbb{Q}(T)[X, Y]$ tel que

$$P(T, X) - \prod_{i=1}^{n}(X - A_i(T, Y)) + R(T, Y)Q(T, Y) \tag{2.16}$$

puisque $Q(T, Y)$ est le polynôme minimal de $y$. Puisque $K = \mathbb{Q}(T)(x_1, \cdots, x_n)$, on peut trouver un polynôme $B \in \mathbb{Q}(T)[X_1, \cdots, X_n]$ tel que $y = B(T, x_1, \cdots, x_n)$. Pour la même raison que précédemment il existe un polynôme $S \in \mathbb{Q}(T)[Y]$ tel que

$$Y - B(T, A_1(T, Y), \cdots, A_n(T, Y)) = S(T, Y)Q(T, Y) \tag{2.17}$$

Enfin, le polynôme $Q$ est scindé dans $K$, donc il existe des polynômes $C_i \in \mathbb{Q}(T)[Y]$ tels que l'on ait

$$Q(T, X) = \prod_{i=1}^{n}(X - C_i(T, y)) \tag{2.18}$$

Donc comme précédemment, il existe un polynôme $U \in \mathbb{Q}(T)[X, Y]$ tel que

$$U(T, X, Y)Q(T, Y) = Q(T, X) - \prod_{i=1}^{N}(X - C_i(T, Y)) \tag{2.19}$$

où $N = \deg Q$. On va trouver un ensemble en dehors duquel les polynômes $P(t, X)$ et $Q(t, X)$ sont séparables et les egalités restent vraies une fois évaluées en $T = t$. Les coefficients des polynômes $P, Q, A_1, \cdots, A_n, B, C_1, \cdots, C_N, R, S$ appartiennent à $\mathbb{Q}(T)$. Soit $\Sigma$ l'ensemble des $t \in \mathbb{Q}$ tels que ou bien $t$ est un pôle de l'un de ces coefficients, ou bien le discriminant de $P$ s'annule en $t$, ou bien celui de $Q$ s'annule en $t$. $\Sigma$ est l'ensemble tel que voulu.
Soit $t \in \mathbb{Q}\backslash\Sigma$. Il suffit de montrer que le polynôme $P(t, X)$ est scindé dans toute extension où $Q(t, X)$ l'est, et réciproquement.
Soit $L$ une extension de $\mathbb{Q}$ dans laquelle $Q(t, X)$ a une racine $\eta$. Par equation 2.14 on a

$$P(t, X) = \prod_{i=1}^{n}(X - A_i(t, \eta)) \tag{2.20}$$

donc ,en rappelant que $A_i \in \mathbb{Q}(T)[Y]$, donc $P$ est scindé dans $L$.
Réciproquement, soit $L$ une extension de $\mathbb{Q}$ dans laquelle $P(t, X)$ est scindé. Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ dans laquelle $Q(t, X)$ a une racine $\eta$. Par l'argument précédent, les $A_i(t, \eta) \in L$ sont les racines de $P(t, X)$ dans $\overline{\mathbb{Q}}$, donc par l'égalité 2.17 on a

$$\eta = B(t, A_1(t, \eta), \cdots, A_n(t, \eta)) \tag{2.21}$$

ce qui entraîne $\eta \in L$. Alors l'égalité 2.18 donne

$$Q(t, X) = \prod_{i=1}^{n} (X - C_i(t, \eta)) \tag{2.22}$$

ce qui nous dit $Q(t, X)$ est scindé dans $L$. □

**Lemme 2.1.10.** *Soit $P(T, X)$ un polynôme dans $\mathbb{Q}(T)[X]$ ayant pour corps de décomposition $K_P$ sur $\mathbb{Q}[T]$, de degré $n$. Notons son groupe de Galois $G_P = Gal(K_P/\mathbb{Q}(T))$. La spécialisation de $P(T, X)$ sur $T = t \in \mathbb{Q}$ est $P_t(X) := P(t, X)$, son corps de décomposition et groupe de Galois sur $Q$ sont notés $K_{P_t}$ et $G_{P_t}$ respectivement. Supposons que $P_t(X)$ soit séparable. Alors on a que $G_{P_t}$ est un sous-groupe de $G_P$, et donc $[K_{P_t} : \mathbb{Q}] \leq [K_P : \mathbb{Q}(T)]$*

*Démonstration.* Soient $A = \mathbb{Q}[T]$ et $A_P = A[\alpha_1, \cdots, \alpha_n]$ une $A-$algèbre engendrée par les $n$ racines distinctes $\{\alpha_1, \cdots, \alpha_n\}$ de $P$ dans $K_P$. Tout d'abord on a un isomorphisme $\mathbb{Q}[T]/[T - t] \cong \mathbb{Q}$. Soit $S$ l'ensemble des idéaux maximaux dans $A_P$ qui contiennent l'idéal $(T - t)A_p$. Choisissons un idéal maximal $\mathfrak{m} \in S$, on a montré que $A_P/\mathfrak{m} \cong K_{P_t}$. En effet, on a la décomposition $P_t(X) = \prod_{i=1}^{n}(X - \overline{\alpha_i})$ où $\overline{\alpha_i}$ est l'image de $\alpha_i$ dans $A_P/\mathfrak{m}$, et de plus $A_P/\mathfrak{m}$ est une $\mathbb{Q}-$algèbre engendrée par $\{\overline{\alpha_1}, \cdots, \overline{\alpha_n}\}$.
Notons $G_{P,\mathfrak{m}}$ le sous-groupe de $G_P$ qui stabilise $\mathfrak{m}$

$$G_{P,\mathfrak{m}} = \{\sigma \in G_P \,|\, \sigma(\mathfrak{m}) = \mathfrak{m}\} \tag{2.23}$$

Tout élément $\sigma \in G_{P,\mathfrak{m}} : K_P \to K_P$ induit un élément $\overline{\sigma} \in G_{P_t} : K_{P_t} \to K_{P_t}$ par $\overline{\sigma}(\overline{\alpha_i}) = \overline{\sigma(\alpha_i)}$. On va montrer que le morphisme $G_{P,\mathfrak{m}} \to G_{P_t}$ est un isomorphisme. En effet il est injectif d'après l'injection de $G_P$ et $G_{P_t}$ sur le groupe de permutation $S_n$, et la séparabilité de $G_{P_t}$, et donc on a $|G_{P,\mathfrak{m}}| \leq |G_{P_t}|$. De plus, soit $M$ l'orbite de l'idéal maximal sur $G_f$ representé par les idéaux maximaux qui contiennent $(T - t)A_P$, et notons $|M| < \infty$, le théorème des restes chinois nous donne un isomorphisme de $\mathbb{Q}-$algèbres.

$$A_P/\cap_{\mathfrak{n}\in M} \mathfrak{n} \cong \oplus_{\mathfrak{n}\in M} A_P/\mathfrak{n} \tag{2.24}$$

Puisque $(T - t)A_P \in \cap_{\mathfrak{n}\in M}\mathfrak{n}$, on a que le morphisme canonique $A_P/(T - t)A_P \to \oplus_{\mathfrak{n}\in M} A_P/\mathfrak{n}$ est surjectif, donc $\dim_k A_P/(T-t)A_P \geq \sum_{\mathfrak{n}\in M} \dim_k A_P/\mathfrak{n}$. Puisque $\dim_k A_P/(T-t)A_P = [K_{P_t} : \mathbb{Q}] = |G_{P_t}|$ et $\dim_k A_P/\mathfrak{n} = |G_{P_t}|$, on a $|G_f| \geq [G_P : G_{P,\mathfrak{m}}]|G_{P_t}|$, ce qui nous amène à $|G_{P,\mathfrak{m}}| \geq |G_{P_t}|$. La finitude de $|G_{P_t}|$ nous donne $|G_{P,\mathfrak{m}}| = |G_{P_t}|$, donc $G_{P,\mathfrak{m}} \cong G_{P_t}$. Cet isomorphisme nous permet de considérer $G_{P,\mathfrak{m}}$ comme un sous-groupe de $G_P$, donc on a $[K_{P_t} : \mathbb{Q}] = |G_{P,\mathfrak{m}}| \leq |G_P| = [K_P : \mathbb{Q}(T)]$. □

## 2.2 Exemple de $\mathfrak{S}_n$

Soit $Y_n$ la sous-variété de $\mathbb{P}_{n-1}$ défini par l'équation homogène

$$f_i := X_1^i + X_2^i + \cdots + X_n^i, \quad f_i = 0 \qquad \text{for } i = 1, 2, \cdots, n-2.$$

Pour montrer que $Y_n$ est une courbe lisse, il est suffisant de montrer que la matrice

$$(\frac{\partial f_i}{X_j})_{1\leq i\leq n-2, 1\leq j\leq n} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 2X_1 & 2X_2 & \cdots & 2X_n \\ 3X_1^2 & 3X_2^2 & \cdots & 3X_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ (n-2)X_1^{n-3} & (n-2)X_2^{n-3} & \cdots & (n-2)X_n^{n-3} \end{pmatrix}$$

est de rang $n-2$.

Supposons qu'il y ait $1 \leq i \neq j \leq n-2$, tel que $X_i = X_j$. Comme $X_i = X_j \neq 0$(sinon, $X_1 = X_2 = \cdots = X_n = 0$), par homogénéité, on peut supposer que $X_1 = X_2 = 1$. En calculant la somme symétrique de $X_3, \cdots, X_n$, $X_3, \cdots, X_n$ sont les solutions de l'équation:

$$X^{n-2} + 2X^{n-3} + 3X^{n-4} + \cdots + (n-2)X + n - 1 = 0.$$

Le côté gauche de l'équation est égal à

$$\frac{X^n - nX + n - 1}{(X-1)^2}.$$

Donc l'équation n'a pas de racines multiples et $X = 1$ n'est pas une racine de l'équation. Par déterminant de Vandermonde, le rang de la matrice $(\frac{\partial f_i}{\partial X_j})_{1\leq i\leq n-2, 1\leq j\leq n}$ est $n-2$.

Donc $Y_n$ est une courbe lisse irréductible.

Et on peut définir un morphisme:

$$\phi : Y_n \to \mathbb{P}_1$$

$$[X_1, X_2, \cdots, X_n] \mapsto [(X_1^{n-1} + X_2^{n-1} + \cdots + X_n^{n-1})^n, (X_1^n + X_2^n + \cdots + X_n^n)^{n-1}].$$

Le degré de $\phi$ est $n!$, c'est à dire que l'image réciproque d'un point général de $\mathbb{P}_1$ a $n!$ points. Les points ramifiés de $\phi$ sont $[X_1, X_1, X_3, \cdots, X_n]$, $[1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}]$, $[0, 1, \zeta_{n-1}, \zeta_{n-1}^2, \cdots, \zeta_{n-1}^{n-2}]$ (sous la permutation des coordonnées).

Faisons agir $\mathfrak{S}_n$ sur $Y_n$ par permutation de coordonnées. Puisque $\phi$ est invariant sous $\mathfrak{S}_n$, ceci induit un morphisme $\phi' : Y_n/\mathfrak{S}_n :\to \mathbb{P}_1$. Puisque toute fonction régulière sur

un ouvert de $Y_n/\mathfrak{S}_n$ est induite par le quotient de polynômes symétriques homogènes, on peut donc l'écrire comme une fonction rationnelle de

$$T = \frac{(X_1^n + X_2^n + \cdots + X_n^n)^{n-1}}{(X_1^{n-1} + X_2^{n-1} + \cdots + X_n^{n-1})^n}.$$

Donc $\phi'$ est un isomorphisme.

Rappelons que $X_1, X_2, \cdots, X_n$ vérifient que

$$k\Sigma_{i_1<i_2<\cdots<i_k} X_{i_1}X_{i_2}\cdots X_{i_k} = (\Sigma_{i_1<i_2<\cdots<i_{k-1}} X_{i_1}\cdots X_{i_2}X_{i_{k-1}})\cdot(\Sigma_{i=1}^n X_i) -$$

$$(\Sigma_{i_1<i_2<\cdots<i_{k-2}} X_{i_1}X_{i_2}\cdots X_{i_{k-2}})\cdot(\Sigma_{i=1}^n X_i^2) + \cdots + (-1)^{k-1}(\Sigma_{i=1}^n X_i^k).$$

Donc $X_i, i = 1, \cdots, n$ sont les solutions de l'équation

$$X^n - (\Sigma_{i=1}^n X_i^{n-1})X - \Sigma_{i=1}^n X_i^n = 0.$$

Donc $\frac{\Sigma_{i=1}^n X_i^n}{X_i \Sigma_{i=1}^n X_i^{n-1}}, i = 1, \cdots, n$ sont les solutions de l'équation

$$Z^n + Z^{n-1} + T = 0.$$

Et le revêtement galoisien $\phi : Y_n \to \mathbb{P}_1$ correspond à l'extension de décomposition donnée par le polynôme $f(Z) = Z^n + Z^{n-1}$.

On obtient donc une extension galoisienne de $\mathbb{Q}(T)$ dont le groupe de Galois est $\mathfrak{S}_n$.

## 2.3 Version géométrique du théorème d'irréductibilité de Hilbert

### 2.3.1 Ensemble mince et ensemble Hilbert

**Définition 2.3.1.** *Soit $k$ un corps de caractéristique nulle. Soit $I$ un idéal engendré par des polynomes $f_1, f_2, \cdots, f_s$ de $k[T_1, T_2, \cdots, T_n]$. On dit que $V$ est une variété algébrique affine si elle est l'ensemble des solutions communes des $f_1, f_2, \cdots, f_s$. On dit que $V$ est intègre, si $I$ est premier dans $k[T_1, T_2, \cdots, T_n]$. On note $R = k[T_1, T_2, \cdots, T_n]/I$,*

Un sous-ensemble fermé de $V$ est un ensemble des solutions de quelques polynômes. On peut vérifier que c'est une topologie définie sur $V$.

**Définition 2.3.2.** *On dit que l'idéal maximal $P$ est $K$-rationnel, si $R/P \cong K$. Si $K = k$, la condition devient $P = (T_1 - t_1, T_2 - t_2, \cdots, T_n) + I$, où $(t_1, t_2, \cdots, t_n) \in k^n$. On note $V(k)$ l'ensemble des points $k$-rationnels.*

On note dim $V$ le degré de transcendance de $R$.

Le corps des fonctions $k(V)$ de $V$ est le corps des fractions de $R$.

**Définition 2.3.3.** *On dit qu'un sous-ensemble $A$ de $V(k)$ est de type ($C_1$) s'il existe un sous-ensemble fermé $W \subset V$, $W \neq V$, et $A \subset W(k)$, i.e., $A$ n'est pas dense dans $V(k)$. On dit qu'un sous-ensemble $A$ of $V(k)$ est de type ($C_2$), s'il existe une variété irréductible $V'$, et dim $V$=dim$V'$, et il existe un morphisme avec image dense $\pi : V' \to V$, dont le degré de l'extension de corps de fonctions $[k(V') : k(V)] \leq 2$, et $A \subset \pi(V'(k))$*

**Définition 2.3.4.** *On dit qu'un sous-ensemble $A$ de $V(k)$ est mince s'il est contenu dans une union finie d'ensembles de type ($C_1$) ou de type ($C_2$). [4]*

**Définition 2.3.5.** *On dit que une variété $V$ sur $k$ est Hilbertienne si $V(k)$ n'est pas mince.[4]*

**Définition 2.3.6.** *Soit $V$ une variété sur $k$, et $K/k(V)$ une extension de décomposition du polynôme irréductible $f(X) \in k(V)[X]$. Pour tout sous-ensemble ouvert affine $U$ de $V$ où $f$ est défini, on dit qu'un point $k$-rationnel $P$ vérifie la propriété d'irréductibilité relative à $f$, si après spécialisation à $P$, $f(X)$ est encore irréductible. On le note par Irr(P).*

On peut aussi voir ceci d'un point de vue géométrique. Puisque le degré de transcendance de $K$ sur $k$ est le même que celui de $k(V)$ et est donc fini, $K$ peut être réalisé comme le corps des fonctions d'une variété, noté $W$. L'extension $K/k(V)$ induit un morphisme rationnel $\pi : W \to V$, à image dense. Et pour un point fermé $P$, satisfaire Irr($P$) est équivalent à ce que $\pi^{-1}(P)$ ait un unique point $Q$ non ramifié.[4]

**Proposition 2.3.7.** *Les points fermés $P$ de $V(k)$ ne satisfaisant pas Irr(P) forment un sous-ensemble mince de $V$.*

*Démonstration.* Considérons un point fermé de $V(k)$, $P$ ne satisfaisant pas Irr(P). Comme construit plus haut, $P$ est soit contenu dans une sous-variété fermée de $V$ où $f$ n'est pas définie, ou $f(X)$ spécialisée en $P$ est réductible. Considérons un sous-ensemble ouvert affine quelconque $U$ de $V$ contenant $P$ dans lequel $f$ est définie. Notons $R$ l'anneau des coordonnées de $U$ sur $k$. Alors, $f(X)$ est un polynôme unitaire à coefficients dans $R$. Décomposons

$$\bar{f}(X) = \bar{g}(X)\bar{h}(X)$$

in $k[X]$ et dans la clôture algébrique de $k(V)[X]$, écrivons $f(X) = g(X)h(X)$. Puisque les coefficients de $g$ et $h$ sont dans l'algèbre générée par les racines de $f(X)$, donc ils sont intégrals sur $R$. Soit

$\Omega = \{y \in k(V) \backslash R[x] \quad : y$ est un coefficient de $g(X), g(X)$ est un polynôme unitaire divisant $f(X)\}$.

$\Omega$ est un ensemble fini dont les éléments sont intégrals sur $R$. Ecrivons l'anneau $R$ sous la forme $k[T_1, T_2, \cdots, T_n]/I$, où I est un idéal de $k[T_1, T_2, \cdots, T_n]/I$. Soit $F_y(T_1, T_2, \cdots, T_n, X)$ le polynôme minimal de $y \in \Omega$. Posons $P = (t_1, t_2, \cdots, t_n) \in k^n$. Puisque $f(X) = g(X)h(X)$ , il existe $y \in \Omega$ tel que $F_y(T_1, T_2, \cdots, T_n, X)$ a une solution dans $k^n \times k$. Géométriquement, comme $F_y$ n'est pas contenue dans $R[x]/I$, $F_y(T_1, T_2, \cdots, T_n, X)$ définit un morphisme de variétés de degré $\geq 2$ à $V$. Et $P$ est contenue dans l'image du morphisme. Dans l'ensemble, les points fermés qui ne vérifient pas Irr, sont soit contenus dans un sous-ensemble fermé (C1) ou contenus dans une union finie d'ensembles minces (C2), et donc forment un ensemble mince. □

Maintenant si on suppose que $V$ est Hilbertienne, alors il existe un point fermé $P$ ayant pour corps résiduel $k$, tel que $P$ satisfasse Irr$(P)$. Et la préimage de $P$ contient un et un seul point, que l'on notera $Q$. Le groupe de décomposition de $Q$ est just Gal$(K/k(V))$. On trouve donc une extension de $k$, de groupe de Galois Gal$(K/k(V))$.

### 2.3.2 $\mathbb{A}^n(K)$ est hilbertien

**Démontrons que $\mathbb{A}^n(\mathbb{Q})$ est hilbertien.** Soit V l'espace projectif $\mathbb{P}^n$ de dimension n, et soit $A \in V(K)$ un ensemble mince. On note $Grass_n^d$ la variété grassmannienne des sous-espaces d-linéaires de $\mathbb{P}^n$, où $1 \leq d \leq n$

**Proposition 2.3.8.** *Il existe un sous-ensemble non vide ouvert pour la topologie de Zariski $U \subset Grass_n^d$ tel que si $W$ appartient à $U(K)$, alors $A \cap W$ est mince dans $W$.[4]*

**Proposition 2.3.9.** *Si $\mathbb{P}^n$ est hilbertien sur $K$ pour un certain $n \geq 1$, alors tous les espaces projectifs $\mathbb{P}^n$ sur $K$ vérifient la propriété de Hilbert.[4]*

**Démontrons que $\mathbb{A}^n(\mathbb{K})$ est hilbertien.**

**Définition 2.3.10.** *On dit qu'une variété algébrique intègre irréductible $V$ sur un corps $k$ est absolument irréductible si elle satisfait les conditions équivalentes suivantes:*

- *L'intersection de son corps de fonctions $k(V)$ et de la clôture algébrique $k^c$ de $k$ est $k$;*
- *La variété $V$ sous toute extension de scalaires reste irréductible.*

Soit $L/K$ une extension finie, $V$ une variété absolument irréductible sur $K$. L'extension des scalaires à $L$ fournit une variété sur $L$, notée $V_{/L}$.

**Proposition 2.3.11.** *Si $A \subset V(L)$ est mince relativement à $L$, alors $A \cap V(K)$ est mince relativement à $K$. [4]*

Cette démonstration utilise la restriction du foncteur des scalaires $R_{L/K} : Var_L \to Var_K$ des L-varieties aux $K$-varieties.

It is the right adjoint to the extension of scalars $R_{L/K} : Var_L \to Var_K$. i.e., for every K-variety T and L-variety W, one has:

$$\text{Mor }_K(T, R_{L/K}W) = \text{Mor }_L(T_{/L}, W); \tag{2.25}$$

In particular, taking T to be a point which is rational over K, the above formula yields

$$(R_{L/K}W)(K) = W(L) \tag{2.26}$$

Soit $\Sigma_L$ l'ensemble des plongements de L dans une clôture algébrique fixée $K^c$; pour tout $\sigma \in \Sigma_L$, soit $W^\sigma$ la variété déduite de la L-variété donnée W par extension des scalaires via $\sigma$. Le produit $X = \prod_\sigma W^\sigma$ est une $K^c$-variété. De plus, on a des isomorphismes naturels entre $X$ et $X^s$ pour tout $s \in G_K$. Par la théorie des descentes de Weil, ces isomorphismes donnent lieu à une $K$-variété.

Si $A$ est de type $(C_1)$, alors $A \cap V(K)$ est de type $(C_1)$.

Si $A$ est de type $(C_1)$, alors on suppose qu'il existe une variété absolument irréductible $W$, avec dim $W$=dim $V$, et un morphisme $\pi : W \to V$ avec deg$\pi > 1$, tels que $A \subset \pi(W(L))$. En restreignant convenablement V, on peut supposer que $\pi$ est étale finie. Le foncteur $R_{L/K}W$ donne alors un revêtement étale $R_{L/K}W \to R_{L/K}V_{/L}$. En utilisant le plongement diagonal $\Delta : V \to R_{L/K}V_{/L}$, on obtient un revêtement étale $\pi' : V' \to V$, et un diagramme cartésien :

$$\begin{array}{ccc} V' & \longrightarrow & R_{L/K}W \\ {\scriptstyle \pi'}\downarrow & & \downarrow \\ V & \longrightarrow & R_{L/K}V_{/L} \end{array}$$

L'ensemble $A \cap V(K)$ est contenu dans $\pi'(V'(K))$, et il est facile de vérifier que toutes les composantes de V' sont de degré sur $V$ au moins égal à deg$\pi$. Ainsi $\pi'(V'(K))$ est mince, et c'est aussi vrai pour $A \cap V(K)$.

Par exemple, une localisation du diagramme suivant donne une version affine du diagramme si-dessus.

$$\begin{array}{ccc} \mathbb{R}[x,y,e,f]/(x^2+y^2-1, e^2-f^2-y, ef) & \longleftarrow & \mathbb{R}[a,b,c,d,e,f]/(a^2-b^2+c^2-d^2-1, ab+cd, e^2-f^2-c, 2ef-d) \\ {\scriptstyle \pi'}\uparrow & & \uparrow \\ \mathbb{R}[x,y]/(x^2+y^2-1) & \longleftarrow & \mathbb{R}[a,b,c,d]/(a^2-b^2+c^2-d^2-1, ab+cd) \end{array}$$

Spec$(\mathbb{R}[x,y,e]/(x^2+y^2, e^2-f^2-y, ef))$ a deux composantes irréductible, chacune de degré 2 sur Spec$(\mathbb{R}[x,y]/(x^2+y^2-1))$

## 2.4 Exemple

Maintenant on regarde sur le groupe $G := \mathbb{Z}/3\mathbb{Z}$.

Considerons l'équation : $X^3 - TX^2 + (T-3)X + 1 = 0$.

Le groupe $G$ agit sur $\mathbb{P}_1$ par $\sigma X = \frac{1}{1-X}$, où $\sigma$ est un générateur de $G$.

La fonction

$$T = X + \sigma X + \sigma^2 X = \frac{X^3 - 3X + 1}{X^2 - X}$$

est $G$-invariante et donne une application $\mathbb{P}_1 \to \mathbb{P}_1/G$.

On va montrer que toute extension de corps du groupe de Galois $G$ est induite par l'équation spécialisée sur un certain $T_0 \in \mathbb{Q}$.

Soit $K$ un tel extension galoisienne de $\mathbb{Q}$ du groupe de Galois $G$.

$$\begin{array}{ccc} \mathbb{Q}(T) & \longrightarrow & K(T) \\ \downarrow & & \downarrow \\ \mathbb{Q}(X) & \longrightarrow & K(X) \end{array} \qquad \begin{array}{ccc} \mathbb{P}^1_{\mathbb{Q}}/G(\mathbb{Q}), P & \longrightarrow & \mathbb{P}^1_K/G(K), P' \\ {\scriptstyle\pi}\uparrow & & {\scriptstyle\pi'}\uparrow \\ \mathbb{P}^1_{\mathbb{Q}}(\mathbb{Q}),\, \nexists Q? & \longrightarrow & \mathbb{P}^1_K(K), \exists Q'? \end{array}$$

Soit $\delta$ un générateur de $\mathrm{Gal}(K/\mathbb{Q})$. Puisque $K(T)/\mathbb{Q}(T)$, $\mathbb{Q}(X)/\mathbb{Q}(T)$ sont les extensions galoisiennes, $K(X)$ est galoisien sur $\mathbb{Q}(T)$. Et et le groupe de Galois $\mathrm{Gal}(K(X)/\mathbb{Q}(T)) = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \langle\delta\rangle \times \langle\sigma\rangle$. Considérons le sous-groupe $G'$ de $\mathrm{Gal}(K(X)/\mathbb{Q}(T))$ généré par l'élément $(\delta, \sigma^{-1})$. On peut identifier $\mathbb{P}^1_{\mathbb{Q}}(\mathbb{Q})/G$ à un sous-ensemble de $\mathbb{P}^1_K(K)/G$.

Le corps $K$ est généré en résolvant l'équation spécialisée à certains $a \in \mathbb{Q}$, si et seulement si il existe un point $P$ de $(\mathbb{P}^1_{\mathbb{Q}}/G)(\mathbb{Q})$, qui

(i) est dans l'image de $\pi'$ de $\mathbb{P}^1_K(K)$, i.e., les solutions de l'equation spécialisée à $a$ sont dans $K$.

(ii) n'est pas dans l'image de $\pi$ $\mathbb{P}^1_{\mathbb{Q}}(\mathbb{Q})$, i.e., aucune solution de l'équation spécialisée à $a$ n'est pas dans $\mathbb{Q}$.

Supposons que $P$ est un point dans $(\mathbb{P}^1_{\mathbb{Q}}/G)(\mathbb{Q})$. Puisque $\delta$ et $\sigma$ fixent $P$, $\delta$ et $\sigma$ agissent sur $\pi^{-1}(P)$.

Il existe un point $P$ dans $(\mathbb{P}^1_{\mathbb{Q}}/G)(\mathbb{Q})$ satisfiant les condition (i) et (ii)
$\iff$ il existe un point $Q'$ dans $\pi^{-1}((\mathbb{P}^1_{\mathbb{Q}}/G)(\mathbb{Q}))$ qui est fixé par $\sigma^{-1}\cdot\delta$ ou $\sigma\cdot\delta$ mais pas fixé par $\delta$.
$\iff$ il existe un point $\mathbb{Q}$-rationnel $Q'$ non invariant par $\sigma$, dans un $\mathbb{P}^1$ tordue $V$ par $\mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{Z}/3\mathbb{Z} \to \langle\sigma\rangle$

$\sigma$ est donne par la matrice $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ qui est d'ordre 3. Et par Hilbert 90, $H^1(\mathrm{Gal}(K/\mathbb{Q}), GL_2(K)) = 0$. $\mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{Z}/3\mathbb{Z} \to GL_2(K)$ est un cocycle et donc un cobord. Donc il y a une matrice $M$ dans $GL_2(K)$, tel que $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = M\delta \cdot M^{-1}$. $M$ induit un isomorphism entre $V$ et $\mathbb{P}^1_{\mathbb{Q}}$.

Comme le point de $V$ fixé par $\sigma$ est fixé par $\delta$, donc est dans $\mathbb{P}^1_{\mathbb{Q}}/G(\mathbb{Q})$. Mais $V(K) = \mathbb{P}^1_K \neq \mathbb{P}^1_K/G$. , donc il y a un point $\mathbb{Q}$ de $V$, pas invariant par $\sigma$. Donc $K$ est induit par l'equation specialisée à quelque $a \in \mathbb{Q}$.

# Chapitre 3

# Recherche d'extensions de $\mathbb{Q}(T)$

Dans ce chapitre, on montre que tout groupe fini est groupe de Galois d'une extension finie de $\mathbb{C}(T)$ en utilisant la géométrie de Riemann. Puis on montre que la même propriété est vraie sur $\overline{\mathbb{Q}}(T)$. Enfin, on explique une méthode pour descendre cette propriété à $\mathbb{Q}(T)$.

## 3.1 Extension maximale de $\mathbb{C}(T)$ non ramifiée en dehors d'un ensemble fini de points

Le corps $\mathbb{C}(T)$ est le corps des fonctions méromorphes (en fait, rationnelles) de $\mathbb{P}_1(\mathbb{C})$. Pour trouver les extensions de $\mathbb{C}(T)$, on utilise les revêtements galoisiens (ramifiés) de $\mathbb{P}_1(\mathbb{C})$.

Pour tout ensemble fini de points $\mathcal{S} = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_s\}$ de $\mathbb{P}_1(\mathbb{C})$, soit $\mathbb{S} = \{\mathfrak{P}_1, \mathfrak{P}_2, ..., \mathfrak{P}_s\}$ l'ensemble correspondant de places de $\mathbb{C}(T)$. Considérons l'extension maximale $\mathbf{M}_{\mathbb{S}}$ de $\mathbb{C}(T)$ non ramifiée en dehors de $\mathbb{S}$. Notons son groupe de Galois $\mathrm{Gal}(\mathbf{M}_{\mathbb{S}}/\mathbb{C}(T))$ comme $\pi_1^{alg}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S})$. Soit $K_{\mathcal{S}}$ l'ensemble des extensions finies de $\mathbb{C}(T)$ non ramifiées en dehors de $\mathcal{S}$. L'union de toutes ces extensions est $\mathbf{M}_{\mathbb{S}}$. Donc

$$\pi_1^{alg}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}) = \varprojlim(\mathrm{Gal}(K/\mathbb{C}(T))_{K\in K_{\mathcal{S}}}.$$

Notons aussi que $\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}$ est homotope à un bouquet de $s-1$ cercles $\bigvee_{s-1} S^1$. Son groupe fondamental est donc $\pi_1^{top}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}; \mathcal{P}_0) = \langle\gamma_1, ..., \gamma_s | \gamma_1 \cdot ... \cdot \gamma_s = 1\rangle$.

**Théorème 3.1.1.** *(Théorème d'existence profinie de Riemann) Le groupe fondamental algébrique $\pi_1^{alg}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S})$ est isomorphe à la complétion profinie du groupe topologique $\pi_1^{top}(\mathbb{P}_1(\mathbb{C}); \mathcal{P}_0)$:*

$$\pi_1^{alg}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}) = \hat{\pi}_1^{top}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}; \mathcal{P}_0).$$

*où $\mathcal{P}_0$ et $\pi_1^{top}(\mathbb{P}_1(\mathbb{C});\mathcal{P}_0)$ sont tels que décrits ci-dessus.[3]*

*Démonstration.* Puisque $\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}$ est connexe par arcs, localement connexe par arcs et semi-localement simplement connexe, il existe un revêtement universel $Y$ de $\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}$. Et son groupe d'automorphismes est isomorphe au groupe fondamental $\pi_1^{top}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S})$.

À tout sous-groupe normal $G$ de $\pi_1^{top}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S})$ d'indice fini, il correspond un revêtement galoisien fini $\widetilde{Y} = Y/G$ de $\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}$, dont le groupe fondamental est $G$. Alors, $\widetilde{Y}$ est naturellement une variété analytique complexe de dimension 1 (une surface de Riemann) et par le théorème d'extension de Riemann, on peut étendre le revêtement (non ramifié) $\widetilde{Y} \to \mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}$ à un revêtement ramifié entre surfaces de Riemann compactes, et donc entre courbes algébriques $\phi : \bar{Y} \to \mathbb{P}_1(\mathbb{C})$. Par tiré en arrière, $\phi$ induit alors un plongement entre corps de fonctions (méromorphes ou rationnelles) : $\phi' : \mathbb{C}(T) \to \mathbb{C}(\bar{Y})$. L'extension $\mathbb{C}(\bar{Y})$ est non ramifiée en dehors de $\mathbb{S}$ et

$$\mathrm{Gal}(\mathbb{C}(\widetilde{Y})/\mathbb{C}(T)) = \pi_1^{top}(\mathbb{P}_1(\mathbb{C}) \setminus \mathcal{S};\mathcal{P}_0)/G.$$

Inversement, pour toute extension galoisienne finie $K$ de $\mathbb{C}(T)$ non ramifiée en dehors de $\mathbb{S}$, $K$ correspond à une surface de Riemann compacte $\bar{Y}$. Le revêtement ramifié de $\bar{Y}$ sur $\mathbb{P}_1(\mathbb{C})$ est de degré fini et est non ramifié en dehors de $\mathcal{S}$. Et

$$\mathrm{Gal}(K/\mathbb{C}(T)) = \{\text{automorphismes de } \bar{Y}\} = \pi_1^{top}(\mathbb{P}_1(\mathbb{C}) \setminus \mathcal{S};\mathcal{P}_0)/\pi_1(\bar{Y} \setminus \pi^{-1}(\mathcal{S}), \widetilde{\mathcal{P}_0}),$$

où $\widetilde{\mathcal{P}_0}$ est une image réciproque de $\mathcal{P}_0$.

En prenant la limite projective,

$$\begin{aligned}
\pi_1^{alg}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S}) &= \varprojlim_{K\in K_{\mathcal{S}}} \mathrm{Gal}(K/\mathbb{C}(T)) \\
&= \varprojlim_{\substack{\widetilde{Y} \text{ finite Galois} \\ \text{covering of } \mathbb{P}_1(\mathbb{C})}} (\pi_1^{top}(\mathbb{P}_1(\mathbb{C});\mathcal{P}_0)/\pi_1(\widetilde{Y}, \widetilde{\mathcal{P}_0})) \\
&= \varprojlim_{\substack{G\lhd\pi_1^{top}(\mathbb{P}_1(\mathbb{C});\mathcal{P}_0) \\ \text{with finite index}}} (\pi_1^{top}(\mathbb{P}_1(\mathbb{C});\mathcal{P}_0)/G) \\
&= \hat{\pi}_1^{top}(\mathbb{P}_1(\mathbb{C})\backslash\mathcal{S};\mathcal{P}_0),
\end{aligned}$$

et on obtient le résultat. □

**Corollary 3.1.2.** *Soit $G$ un groupe fini. Alors il existe toujours une extension galoisienne de $\mathbb{C}(T)$ de groupe de Galois $G$.*

*Démonstration.* Soit le groupe fini $G$ généré par $s-1$ éléments $\sigma_1, ..., \sigma_{s-1}$, $s \geq 2$. Alors il existe un épimorphisme

$$\phi : \langle \gamma_1, ..., \gamma_s | \gamma_1 \cdot ... \cdot \gamma_s = 1 \rangle \to G, \text{ avec } \phi(\gamma_i) = \sigma_i, \text{ pour } i = 1, 2, ..., s-1.$$

En combinant $\langle \gamma_1, ..., \gamma_s | \gamma_1 \cdot ... \cdot \gamma_s = 1 \rangle\hat{} \to \langle \gamma_1, ..., \gamma_s | \gamma_1 \cdot ... \cdot \gamma_s = 1 \rangle / \ker(\phi)$,

on obtient un épimorphisme continu $\phi' : \langle \gamma_1, ..., \gamma_s | \gamma_1 \cdot ... \cdot \gamma_s = 1 \rangle\hat{} \to G$. Alors $\mathbf{M}_{\mathbb{S}}^{\ker\phi'}$ est une extension galoisienne de $\mathbb{C}(T)$ de groupe de Galois $G$. □

## 3.2 De $\mathbb{C}(T)$ à $\bar{\mathbb{Q}}(T)$

**Théorème 3.2.1.** *Soient $\bar{k}$ un sous-corps algébriquement clos de $\mathbb{C}$, $\mathcal{S} = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_s\}$ un sous-ensemble fini de $\mathbb{P}_1(\bar{k})$, et $\mathbb{S} = \{\mathfrak{P}_1, ..., \mathfrak{P}_s\}$ l'ensemble des idéaux de valuation de $\bar{k}(\mathbb{P}_1(k)) \cong \bar{k}(T)$ correspondant à $\mathcal{S}$. Alors pour toute extension finie $\mathbf{N}/\mathbb{C}(T)$ non ramifiée en dehors de $\mathbb{S}$ il existe précisément une extension $\bar{\mathbf{N}}/\bar{k}(T)$ qui est géométrique sur $\bar{k}$ et avec $\bar{\mathbf{N}}\mathbb{C} := \mathbf{N} \otimes_{\bar{k}} \mathbb{C} = \mathbf{N}$.[3]*

*Démonstration.* Soit $\mathbf{N}/\mathbb{C}(T)$ une extension Galoisienne finie de $\mathbb{C}(T)$ non ramifiée en dehors de $\mathbb{S}$. Soit $\mathbf{M}_{\mathbb{S}}$ l'extension maximale de $\mathbb{C}(T)$ non ramifiée en dehors de $\mathbb{S}$.

Identifions $\mathrm{Aut}(\mathbb{C}/\bar{k})$ à $\Delta :=\mathrm{Aut}(\mathbb{C}(T)/\bar{k}(T))$ qui est un quotient de $\widetilde{\Delta} :=\mathrm{Aut}(\mathbf{M}_{\mathbb{S}}/\bar{k}(T))$. Alors $\mathbf{M}_{\mathbb{S}}^{\widetilde{\Delta}} = \bar{k}(T)$, $\mathbb{C}^{\Delta|_{\mathbb{C}}} = \bar{k}$.

Pour tout $\widetilde{\delta} \in \widetilde{\Delta}$, l'image $\widetilde{\delta}(\mathbf{N})$ de $\mathbf{N}$ par l'action de $\widetilde{\delta}$ est une extension finie de $\mathbb{C}(T)$ de degré $[\widetilde{\delta}(\mathbf{N}) : \mathbb{C}(T)] = [\mathbf{N} : \mathbb{C}(T)]$.

Puisque $\mathrm{Gal}(\mathbf{M}_{\mathbb{S}}/\mathbb{C}(T))$ est la complétion profinie d'un groupe de type fini, il n'y a qu'un nombre fini de sous-groupe d'indice égal à $[\mathbf{N} : \mathbb{C}(T)]$ et donc un nombre fini d'extensions de $\mathbb{C}(T)$ de degré $[\mathbf{N} : \mathbb{C}(T)]$. Soit

$$\Delta' := \{\delta' \in \widetilde{\Delta} : \delta'(\mathbf{N}) = \mathbf{N}\}.$$

Alors $\Delta'$ est un sous-groupe normal d'indice fini dans $\widetilde{\Delta}$ et, en particulier, $\mathbb{C}(T)^{\Delta'}$ est une extension scalaire et finie de $\bar{k}(T)$. Puisque $\bar{k}$ est algébriquement clos, $\mathbb{C}(T)^{\Delta'} = \bar{k}(T)$.

Choisissons $a \in \mathbb{P}_1(\bar{k}) \backslash \mathcal{S}$, soient $\mathfrak{P}_a$ l'idéal de valuation dans $\mathbb{C}(T)$ correspondant à $a$, $\widetilde{\mathfrak{P}_a}$ un des idéaux de valuation dans $\mathbf{N}$ au-dessus de $\mathfrak{P}_a$. En d'autres termes, on choisit un point $\tilde{a}$ de la surface de Riemann $Y(\mathbf{N})$ au-dessus de $a$. Puisqu'il n'y a qu'un nombre fini d'idéaux de valuation reposant sur $\mathfrak{P}_a$, le groupe

$$\Delta'' := \{\delta'' \in \Delta' : \delta''(\widetilde{\mathfrak{P}_a}) = \widetilde{\mathfrak{P}_a}\}.$$

est d'indice fini dans $\Delta'$. Comme ci-dessus, $\mathbb{C}(T)^{\Delta''} = \bar{k}(T)$, et donc $\mathbf{N}^{\Delta''}$ est une extension finie régulière de $\bar{k}(T)$.

Par le théorème de Riemann-Roch, il existe sur $Y(\mathbf{N})$ des fonctions méromorphes non constantes dont le seul pôle est en $\tilde{a}$. Soit $m$ le plus petit ordre d'un tel pôle. Alors l'espace vectoriel des fonctions méromorphes dont le seul pôle est en $\tilde{a}$ et d'ordre $\leq m$ est de dimension 2, engendré par 1 et une certaine fonction $z \in \mathbf{N}$. Puisque $a \in S$, la fibre de $a$ dans $Y(\mathbf{N})$ est de cardinal $[\mathbf{N} : \mathbb{C}(T)]$, et les conjugués de $z$ sous $\mathrm{Gal}(\mathbf{N}/\mathbb{C}(T))$ sont donc tous distincts, de sorte que l'on a $\mathbf{N} = \mathbb{C}(T, z)$.

Localement on peut écrire,

$$z = \frac{a_{-m}}{(T-a)^m} + \frac{a_{-m+1}}{(T-a)^{m-1}} + ... + \frac{a_{-1}}{(T-a)} + a_0 + ...$$

en divisant par une constante et soustrayant une constante, on peut supposer $a_{-m} = 1$ et $a_0 = 0$. Pour $\delta'' \in \Delta''$, la fonction $\delta''(z)$ est de la forme $\delta''(z) = az + b$, avec $a, b \in \mathbb{C}$, donc $\delta''(a_{-i}) = a_{-i}$ pour $i = 1, 2, ..., m-1$. Donc $z$ est invariant sous l'action de $\Delta''$. Donc $\bar{k}(T, z) \subset \mathbf{N}^{\Delta''}$ est une extension finie de $\bar{k}(T)$. C'est l'extension $\bar{\mathbf{N}}$ cherchée.

Pour l'unicité, s'il existe $\bar{\mathbf{N}}_1 \neq \bar{\mathbf{N}}_2$ Galoisiennes finies de $\bar{k}(T)$ telles que $\mathbf{N_i}.\mathbb{C} = \bar{\mathbf{N}}$, pour $i = 1, 2$, alors

$$[\bar{\mathbf{N}}_1\bar{\mathbf{N}}_2 : \bar{k}(T)] > [\bar{\mathbf{N}}_1 : \bar{k}(T)] = [\bar{\mathbf{N}} : \mathbb{C}(T)] = [\mathbb{C}\bar{\mathbf{N}}_1\bar{\mathbf{N}}_2 : \mathbb{C}(T)]$$

contredisant le fait que $\bar{\mathbf{N}}_1\bar{\mathbf{N}}_2$ est linéairement disjoint de $\mathbb{C}(T)$. D'où l'unicité de $\bar{\mathbf{N}}$. □

**Corollary 3.2.2.** *Il existe une extension de corps maximale $\bar{\mathbf{M}}_{\mathbb{S}}/\bar{k}(T)$ non ramifiée en dehors de $\mathbb{S}$, de groupe de Galois $\langle \gamma_1, ..., \gamma_s | \gamma_1 \cdot ... \cdot \gamma_s = 1 \rangle\hat{}$, où $\langle \gamma_i \rangle\hat{}$ s'identifie au groupe d'inertie $I(\widetilde{\mathfrak{P}}_i|\mathfrak{P}_i)$ en une place $\widetilde{\mathfrak{P}}_i$ de $\bar{\mathbf{M}}_{\mathbb{S}}$ au-dessus de $\mathfrak{P}_i$, $i = 1, 2, ..., s$.*

## 3.3 De $\bar{\mathbb{Q}}(T)$ à $\mathbb{Q}(T)$

Dans cette section, on considèrera l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur $\mathrm{Gal}(\bar{\mathbf{N}}/\bar{\mathbb{Q}})$, où $\bar{\mathbf{N}}$ est une extension finie de $\bar{\mathbb{Q}}$. Notons

$$\Gamma_s = \mathrm{Gal}(\bar{\mathbf{M}}_{\mathbb{S}}/\mathbb{Q}(T)) = \langle \gamma_1, ..., \gamma_s | \gamma_1 \cdot ... \cdot \gamma_s = 1 \rangle\hat{}.$$

On introduit le caractère cyclotomique. Tout $\delta \in \Gamma_{\mathbb{Q}}$ envoie une racine primitive $n$-ème de l'unite $\zeta_n$, sur une autre telle racine, donc sur une puissance de $\zeta_n$. On obtient ainsi un morphisme de groupes $\Gamma_{\mathbb{Q}} \to (\mathbb{Z}/n\mathbb{Z})^*$. Faisant varier $n$, on obtient le caractère cyclotomique $c : \Gamma_{\mathbb{Q}} \to \hat{\mathbb{Z}}^*$. On a donc $\delta(\zeta) = \zeta^{c(\delta)}$ pour toute racine de l'unité.

**Théorème 3.3.1.** *Si le corps $\bar{k}$ dans le théorème 3.2.1 est choisi comme étant le corps $\bar{\mathbb{Q}}$ des nombres algébriques, et si l'ensemble $\mathcal{S} \subset \mathbb{P}^1(\bar{\mathbb{Q}})$ est stable sous $\Gamma_{\mathbb{Q}}$, alors $\bar{\mathbf{M}}_{\mathbb{S}}$ est galoisienne (infinie) sur $\mathbb{Q}(T)$ et on a une suite exacte $\Gamma_s \hookrightarrow Gal(\bar{\mathbf{M}}_{\mathbb{S}}/\mathbb{Q}(T) \twoheadrightarrow \Gamma_{\mathbb{Q}}$. De plus, pour tout point $a \in \mathbb{P}^1(\mathbb{Q})$ et toute place $\widetilde{\mathcal{P}}$ de $\bar{\mathbf{M}}_{\mathbb{S}}$ au-dessus de $a$, le groupe de décomposition $\widetilde{\Delta}$ en $\widetilde{\mathcal{P}}$ s'identifie à $\Gamma_{\mathbb{Q}}$, d'où un isomorphisme*

$$Gal(\bar{\mathbf{M}}_{\mathbb{S}}/\mathbb{Q}(T)) \cong \Gamma_s \rtimes \Gamma_{\mathbb{Q}}.[3]$$

**Théorème 3.3.2.** *Soit $\bar{\Delta} \cong \Gamma_{\mathbb{Q}}$ un complémentaire fermé de*

$$\Gamma_s = \langle \gamma_1, ..., \gamma_s | \gamma_1 \cdot ... \cdot \gamma_s = 1 \rangle^{\wedge}$$

*dans $Gal(\bar{\mathbf{M}}_{\mathbb{S}}/\mathbb{Q}(T)$ comme dans le théorème 3.3.1, et $\bar{\delta} \in \bar{\Delta}$ un relèvement d'un élément $\delta \in Gal(\bar{\mathbb{Q}}(T))/\mathbb{Q}(T)) = \Gamma_{\mathbb{Q}}$ à $\bar{\mathbf{M}}_{\mathbb{S}}$. Alors $\bar{\delta}(\gamma_i)$ est conjugué dans $\Gamma_s$ à $\gamma_{\delta(i)}^{c(\bar{\delta})}$, où $\delta(i)$ est l'indice tel que $\delta(P_i) = P_{\delta(i)}$.[3]*

Nous allons maintenant expliquer l'idée des classes rigides rationnelles.

Soit $\Sigma$ l'ensemble des systèmes $s$-générateurs $\sigma = (\sigma_1, \sigma_2, ..., \sigma_s)$ dans $G$, c'est-à-dire, $\sigma_1 \cdot \sigma_2 \cdot ... \cdot \sigma_s = 1$ et $G$ est engendré par $\sigma_1, \sigma_2, ..., \sigma_s$. Par la proposition 4.2.2, il existe un épimorphisme continu $\phi : \Gamma_s \to G$. Alors $\bar{\mathbf{M}}_{\mathbb{S}}^{\ker\ \phi}$ est une extension galoisienne de $\bar{\mathbb{Q}}(T)$. Notons que $\Gamma_{\mathbb{Q}} = \bar{\Delta}$ agit sur $\Sigma$ par $\delta(\sigma_1, \cdots, \sigma_s) = (\sigma_{\delta(1)}^{c(\delta)}, \cdots, \sigma_{\delta(s)}^{c(\delta)})$.

Soit maintenant $\mathbf{C} \in Cl(G)^s$ un $s$-uplet de classes de conjugaison de $G$. On dit qu'il est rationnel s'il est invariant sous l'action de $\bar{\Delta}$. Par ailleurs, soit

$$\Sigma_{\mathbf{C}} = \{(\sigma_1, \sigma_2, ..., \sigma_s) \in \Sigma : \sigma_i \in \mathbf{C}_i \text{ pour } i = 1, 2, ..., s\}.$$

Le $s$-uplet est dit rigide si $\#|\Sigma_{\mathbf{C}}/Inn(G)|$ vaut un, c'est-à-dire s'il y a une seule classe de conjugaison de s-systèmes $[\sigma]$ de $G$ de composantes $\sigma_i \in C_i$.

Ainsi, si $\mathbf{C}$ est rationnel et rigide, pour tout $\delta \in \Gamma_{\mathbb{Q}}$ il existe $g_\delta \in G$ tel que $\delta(\sigma_1, \cdots, \sigma_s) = {}^{g_\delta}(\sigma_1, \cdots, \sigma_s)$. Si de plus le centre de $G$ est trivial, alors $g_\delta$ est unique et on a $g_{\delta\delta'} = g_\delta g_{\delta'}$. Alors le morphisme $\phi : \Gamma_s \longrightarrow G$ se prolonge à $\Gamma_s \rtimes \Gamma_{\mathbb{Q}}$ en posant $\tilde{\phi}(\gamma, \delta) = \phi(\gamma) g_\delta$.

**Théorème 3.3.3.** *Soit $G$ un groupe fini dont le centre admet un supplémentaire, et $\mathbf{C} \in Cl(G)^s$ un $s$-uplet de classes rigide rationnel de $G$. Alors il existe un épimorphisme $\Gamma_s \rtimes \Gamma_{\mathbb{Q}} \twoheadrightarrow G$ et donc il existe une extension galoisienne $\mathbf{N}/\mathbb{Q}(T)$ non ramifiée en dehors de $\mathbb{S}$ avec*

$$Gal(\mathbf{N}/\mathbb{Q}(T)) \cong G$$

*telle que les groupes d'inertie sur $\mathfrak{P}_i$ sont générés par des éléments $\sigma_i \in \mathbf{C}_i$.*

## 3.4 Exemples de rigidité

$S_n$ Le groupe symétrique dispose de classes de conjugaison $nA$, $2A$, and $(n-1)A$ correspondant aux cycles d'ordre $n$, 2 et $n-1$ respectivement. Le 3-uplet de classes $(nA, 2A, (n-1)A)$ est rigide. En fait, considérons n'importe quel triplet $(\sigma, \delta, \delta^{-1}\sigma^{-1})$ avec $\sigma$ un 2-cycle, $\delta$ un $n$-cycle, $\delta^{-1}\sigma^{-1}$ un $(n-1)$-cycle. Par conjugaison, on peut supposer $\delta = (12\cdots n)$ et $\sigma = (1k)$ pour un certain $k \in \{1, 2, \cdots, n\}$. Puisque $\sigma\delta = (12\cdots k-1)(k\cdots n)$, $k$ doit être 2. Donc il y a exactement $n!$ tels triplets. Le 3-uplet de classes $(2A, nA, (n-1)A)$ est donc rigide. Et $(2A, nA, (n-1)A)$ est rationnel, i.e., $(2A, nA, (n-1)A)^{\delta} = (2A, nA, (n-1)A)$, car $c(\delta)$ restreint à $G$ est pris comme élément de $(\mathbb{Z}/|G|\mathbb{Z})^*$. Par théorème basique de rigidité, il existe un revêtement galoisien de $\mathbb{P}^1(\mathbb{Q})$ de groupe de Galois $S_n$.

Rappelons l'exemple du chapitre 2, le revêtement $\mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ donné par $X \mapsto X^n + X^{(n-1)}$ a 3 points ramifiés d'ordre $2, n-1, n$ respectivement en $0$, $\frac{(-n+1)^{n-1}}{n^n}$, $\infty$, et le revêtement galoisien obtenu par ce polynôme est simplement $S_n$.

**$\mathbf{PSL}_2(\mathbb{F}_p)$** $\mathrm{PSL}_2(\mathbb{F}_p)$, où $p > 2$ contient des classes de conjugaison uniques d'éléments d'ordre 2 et 3, notées par $2A$ et $3A$ respectivement. Il existe deux classes $pA$ et $pB$ d'éléments d'ordre $p$, qui sont représentés par des matrices unipotentes $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, où $(\frac{\alpha}{p}) = 1$. et le triplet $(2A, 3A, pA)$ est rigide mais non rationnel.[4]

**Groupes abéliens finis** Pour arriver au résultat sur les groupes abéliens, on a besoin d'une modification de la condition sur les points ramifiés. En fait, on peut ajuster la condition que $\mathfrak{P}_i$ soient dans $\mathbb{P}(\mathbb{Q}(t))$ à la condition qu'ils soient dans $\mathbb{P}(\bar{\mathbb{Q}}(t))$ et donc les points de ramifications $\{\mathfrak{P}_i,\ i = 1, 2, \cdots, s\}$ sont sujets à l'action du groupe $\Gamma_{\mathbb{Q}}$.

Pour un groupe abélien fini $G$, on peut écrire $G$ comme $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \mathbb{Z}/n_m\mathbb{Z}$, avec $n_1 | n_2, \cdots, n_{m-1} | n_m$.

Soit $s_t$ le nombre de $i$ tels que $n_i = t$. Si $n_i = 2$, prenons $\mathfrak{P}_{2i+1} = (X - a_i), \mathfrak{P}_{2i+2} = (X - a_i)$, où $a_i \in \mathbb{Q}$.

Si $n_i = t \neq 2$, prenons $\mathfrak{P}_{2s_2+3s_3+\cdots+(t-1)s_{t-1}+j} = (X - a_i \cdot \zeta_{n_i}^{j^{-1}})$, pour $j \in (\mathbb{Z}/n_i\mathbb{Z})^*$, où $a_i \in \mathbb{Q}$ et $a_i$ sont deux à deux distincts.

Alors un épimorphisme $\Gamma_s \rtimes \Gamma_{\mathbb{Q}} \to G$ peut être défini par $(\gamma_{2s_2+3s_3+\cdots+(t-1)s_{t-1}+j}, \delta) \mapsto j \cdot \bar{1}_{n_t}$, en remarquant que la classe $[\gamma_{2s_2+3s_3+\cdots+(t-1)s_{t-1}+j}]$ sous l'action de $\delta$ est $[\gamma^{c(\delta)}_{2s_2+3s_3+\cdots+(t-1)s_{t-1}+j\cdot c(\delta)^{-1}}]$. On a donc une extension galoisienne de $\mathbb{Q}(T)$ de groupe de Galois $G$.

# Bibliography

[1] Antoine Chambert-Loir. *A field guide to algebra*. Springer Science & Business Media, 2004.

[2] Serge Lang. *Fundamentals of Diophantine geometry*. Springer Science & Business Media, 2013.

[3] Gunter Malle and Bernd Heinrich Matzat. *Inverse Galois Theory*. Springer Science & Business Media, 2013.

[4] Jean-Pierre Serre. *Topics in Galois theory*. CRC Press, 2016.