Le problème de Galois inverse sur $\mathbb{Q}_p(t)$

Salim Alloun, Alonso Beaumont Llona

30 Mars 2023

Abstract

Il s'agit de présenter le problème de Galois inverse sur un corps, et en particulier une construction analytique rigide qui résout le problème pour $\mathbb{Q}_p(t)$. Tout cela se base sur un article de Qing Liu [1].

1 Théorème d'irréductibilité de Hilbert, revêtements galoisiens

La théorie de l'ambiguité associe à chaque équation algébrique irréductible à une variable un groupe qui permute ses racines. Dans le langage moderne, chaque extension de corps $E|F$ finie galoisienne se voit associée un groupe fini noté $\mathrm{Gal}(E|F)$, et cette association est fonctorielle contravariante. Une grande question de la théorie des nombres est de savoir si le corps des rationnels en un sens est assez riche pour construire arithmétiquement tous les groupes finis. Autrement dit, il s'agit de résoudre le *problème de Galois inverse* sur le corps $\mathbb{Q}$ défini en général de la manière suivante :

Définition 1.1 Soit F un corps. Étant donné un groupe fini G, on dit qu'il est *réalisable* sur F s'il existe une extension galoisienne $E|F$ telle que $\mathrm{Gal}(E|F) \simeq G$.

On peut essayer de construire de telles extensions à la main, et par exemple cela fonctionne sur $\mathbb{Q}$ pour les groupes finis commutatifs en considérant une sous-extension convenable d'un corps cyclotomique assez grand.

On peut également reformuler le problème en utilisant une clôture séparable de F (si F est parfait alors $F^{\mathrm{sep}} = \overline{F}$) et la correspondance de Galois.

Proposition 1.1 *G est réalisable sur F si et seulement si c'est un quotient de $\mathrm{Gal}(F^{\mathrm{sep}}|F)$.*

On peut donc penser à un objet universel qui géométriquement ou topologiquement correspond à un revêtement universel.

Mais en général c'est assez difficile. Une idée originellement d'Emmy Noether est d'ajouter des transcendants à $\mathbb{Q}$ et la situation devient ainsi clairement géométrique. Par exemple le corps des fractions rationnelles $\mathbb{Q}(t)$ est le corps des fonctions régulières sur $\mathbb{P}^1_{\mathbb{Q}}$, et certaines de ses extensions finies correspondent à des revêtements de $\mathbb{P}^1_{\mathbb{Q}}$.

Pour $\mathbb{Q}$ l'intérêt de cette approche provient du théorème suivant :

Théorème 1.2 (Hilbert) Si un groupe est réalisable sur $\mathbb{Q}(t)$ alors il est réalisable sur $\mathbb{Q}$.

Plus précisément, si G provient d'un polynôme $P(Z,t)$ irréductible sur $\mathbb{Q}(t)[Z]$ alors il existe une infinité de rationnels r tels que $P(Z,r)$ soit irréductible sur $\mathbb{Q}[Z]$ et le corps associé soit galoisien de groupe de Galois G. Ce théorème se généralise en fait aux corps de fonctions de certaines courbes dont les extensions peuvent être spécialisées dans le complémentaire d'une partie mince des points de la courbe. Pour plus de détails, voir la partie 3 de [2].

Ainsi, pour un corps K il s'agit de considérer une extension galoisienne de corps $K(X)|K(t)$ provenant d'un revêtement $f : X \longrightarrow \mathbb{P}^1_K$, où X est une courbe lisse projective connexe. En fait, cela revient à se donner une extension galoisienne finie régulière de $K(t)$.

Définition 1.3 Soit K un corps. Une extension finie $L|K(t)$ est dite *régulière* si $\overline{K} \cap L = K$.

2 Revêtements cycliques et recollements

Définition 2.1 Soient X et Y deux courbes projectives, lisses et connexes, et $f : X \to Y$ un morphisme surjectif. On dit qu'un point $p \in X$ est *non ramifié* si le morphisme d'anneaux locaux $f^* : \mathcal{O}_{Y,f(p)} \to \mathcal{O}_{X,p}$ envoie des uniformisantes vers des uniformisantes. Autrement dit, f induit un isomorphisme entre les espaces tangents T_pX et $T_{f(p)}Y$.

Lemme 2.2 Soit K un corps de caractéristique nulle et $n \geq 1$. Il existe un revêtement galoisien $\pi : X \to \mathbb{P}^1_K$ de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$, avec un point K-rationnel non ramifié.

Preuve. Soit $\xi \in \overline{K}$ une racine primitive $n-$ième de l'unité. Si $\xi \in K$, alors on peut définir l'extension de Kummer $K(y)/K(t)$, où $y^n = t$. Le polynôme

$$P(Y) = Y^n - t = Y^n - y^n = \prod_{k=0}^{n-1}(Y - \xi^k y)$$

est irréductible dans $K(t)[Y]$ par le critère d'Eisenstein et donc l'extension est de degré n, de groupe de Galois $\langle \sigma : y \mapsto \xi y \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Le point $p := (t = 1, y = 1)$, par exemple, est non ramifié : $t - 1$ engendre $\mathfrak{m}_{\pi(p)}$ et son image dans $\mathcal{O}_{X,p}$ engendre $\mathfrak{m}_p$, car $y - 1 = (y^{n-1} + \cdots + 1)^{-1}(t - 1)$.

Dans le cas général, on doit considérer l'extension cyclotomique $K(\xi,t)|K(t)$. Son groupe de Galois est un sous-groupe de $\mathrm{Gal}(\mathbb{Q}(\xi)|\mathbb{Q})$ et donc il est cyclique, engendré par un élément τ. Comme auparavant, on peut définir une extension de Kummer $K(\xi,y)|K(\xi,t)$ d'ordre n et de groupe de Galois engendré par σ. Cette fois-ci, on veut la définir de telle sorte que τ se prolonge en un $K(t)$-automorphisme de $K(\xi,y)$, qui commute avec σ. Ainsi, $K(\xi,y)|K(t)$ sera galoisienne de groupe de Galois $\langle \sigma, \tau \rangle$. Donc tous les sous-groupes sont distingués et en particulier $\mathrm{Gal}(K(\xi,y)^{\langle \tau \rangle}|K(t)) = \langle \sigma \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. □

On suppose dans la suite que K est non archimédien complet, et on munit $\mathbb{P}^1_K$ de sa structure analytique rigide.

Lemme 2.3 Soit $\pi : X \to \mathbb{P}^1_K$ un revêtement galoisien de degré n et $p \in X$ un point non ramifié pour π. Alors, il existe un disque fermé (rigide) $\overline{D}$ de centre $\pi(p)$ tel que $\pi^{-1}(\overline{D})$ soit isomorphe à n copies disjointes de $\overline{D}$, et $\pi^{-1}(\mathbb{P}^1_K \backslash D)$ soit connexe.

Preuve. Comme p est non ramifié, la fibre de $f(p)$ est consitué de n points, et π induit des isomorphismes sur les espaces tangents en ces points. Par la version analytique rigide du théorème des fonctions implicites, π induit localement des isomorphismes sur chaque point de la fibre. Maintenant, soit ϕ une fonction régulière sur $\pi^{-1}(\mathbb{P}^1_K \backslash D)$ telle que $\phi^2 = \phi$. Alors elle est constante sur les composantes connexes de $\pi^{-1}(\overline{D} \backslash D)$ (n couronnes disjointes), et donc elle se prolonge sur chaque compostante connexe de $\pi^{-1}(\overline{D})$. Comme X est connexe, ϕ est constante. □

Lemme 2.4 Soit G un groupe fini, H_1, H_2 de sous-groupes qui engendrent G, et π_1, π_2 des revêtements galoisiens de groupes de Galois H_1 et H_2, respectivement, avec des points rationnels non ramifiés. Alors il existe un revêtement galoisien de groupe de Galois G avec un point rationnel non ramifié.

Preuve. Soit $i \in \{1, 2\}$. On fixe un disque fermé $\overline{D}'_i$ associé à π_i comme dans le lemme précédent, et on pose $\overline{D}_i = \mathbb{P}^1_K \backslash D'_i$. Ce disque contient toute la ramification de π_i, et son image réciproque est connexe. Quitte à translater dans $\mathbb{P}^1_K$, on peut supposer que $\overline{D}_1$ et $\overline{D}_2$ sont disjoints. On pose

$$U_0 = \bigsqcup_{g \in G} U_0^{(g)}$$

où chaque $U_0^{(g)}$ est isomorphe à $\mathbb{P}^1_K \backslash \{D_1 \cup D_2\}$, et donc contient une couronne $C_i^{(g)} \cong \overline{D}_i \backslash D_i$. On fixe un système de représentants S_i de G/H_i qui contient l'élément neutre e, et on pose

$$U_i = \bigsqcup_{s \in S_i} U_i^{(s)}$$

où chaque $U_i^{(s)}$ est isomorphe à $\pi_i^{-1}(\overline{D}_i)$, et donc contient $|H_i|$ couronnes $\cong C_i$. On fixe une de ces couronnes et on la note $C_i^{(s,e)}$: commes les couronnes sont permutés par l'action de H_i sur l'espace de départ, on obtient une notation $C_i^{(s,h)}$, où $h \in H_i$, pour chacune. On recolle alors U_0, U_1, et U_2 en identifiant $C_i^{(s,h)}$ à $C_i^{(sh)}$ à travers π_i.

On obtient ainsi un espace analytique X propre et lisse, ainsi qu'un morphisme fini $\pi : X \to \mathbb{P}^1_K$ qui envoie U_0 vers $\mathbb{P}^1_K \backslash \{D_1 \cup D_2\}$ et U_i vers $\pi_i^{-1}(\overline{D}_i)$. Par le principe GAGA rigide, X et une courbe algébrique. Elle est connexe car H_1 et H_2 engendrent G: en effet, si $g \in G$ et $h \in H_i$, alors $U_0^{(g)}$ et $U_0^{(gh)}$ sont dans la même composante connexe que $U_i^{(s)}$ où $g \in sH_i$. Finalement, l'action de G sur X est donné par $g \cdot U_0^{g'} = U_0^{gg'}$ et $g \cdot U_i^{(s')} = h \cdot U_i^{(s)}$ où $gs' = sh$.

3 Et si on enlève des points ?

Cette preuve marche de façon identique pour résoudre le problème de Galois inverse sur $\mathbb{C}(t)$. Une autre preuve emploie des outils topologiques : on fixe $z_1, \cdots, z_n \in \mathbb{P}^1(\mathbb{C})$ et on considère le revêtement universel $\tilde{\pi} : \tilde{X} \to \mathbb{P}^1(\mathbb{C})\backslash\{z_1, \cdots, z_n\}$. Son groupe d'automorphismes est le groupe libre à $n-1$ générateurs, et donc pour tout groupe fini G d'ordre n, on peut factoriser $\tilde{\pi}$ par un revêtement de la forme $\pi : X \to \mathbb{P}^1(\mathbb{C})\backslash\{z_1, \cdots, z_n\}$ de groupe d'automoprhismes égal à G. Il s'agit bien en fait d'un revêtement analytique (et donc correspondant à une extension finie de $\mathbb{C}(t)$) car grâce à l'isomorphie locale on peut remonter la structure analytique de $\mathbb{P}^1(\mathbb{C})$ sur X.

En complétant π, on obtient le revêtement galoisien souhaité. Cette méthode ne marche pas dans le cas non archimédien, car $\mathbb{P}^{1,an}_K$ privé d'un nombre fini de points est encore simplement connexe.

Soit K un corps algébriquement clos, et D un ensemble fini de points rationnels dans $\mathbb{P}^1_K$. On définit le *groupe fondamental étale* de $\mathbb{P}^1_K\backslash D$, noté $\pi_1(\mathbb{P}^1_K\backslash D)$, comme la limite projective des groupes d'automorphismes des revêtements galoisiens $X \to \mathbb{P}^1_K$ non ramifiés en dehors de D. Par exemple, si $|D| = n$ et $K = \mathbb{C}$, $\pi_1(\mathbb{P}^1_K\backslash D)$ est la complétion profinie du groupe libre à $n-1$ générateurs. Ce résultat reste vrai pour tout corps algébriquement clos de caractéristique nulle.

En particulier, on peut considérer le lien entre le groupe fondamental associé à un corps K non archimédien de caractéristique nulle et celui associé à son corps résiduel $\widetilde{K}$, qu'on suppose aussi algébriquement clos, de caractéristique $p > 0$. Dans ce cadre, la flèche de spécialisation entre en jeu. On note $\pi_1^t(\mathbb{P}^1_K\backslash D)$ le groupe fondamental étale modérément ramifié (des revêtements localement cycliques d'ordre premier à p au-dessus des points de ramifications), et $\pi_1(\mathbb{P}^1_K\backslash D)_{p'}$ le quotient premier à p maximal de $\pi_1(\mathbb{P}^1_K\backslash D)$.

Proposition 3.1 On a un morphisme surjectif $\pi_1^t(\mathbb{P}^1_K\backslash D) \longrightarrow \pi_1^t(\mathbb{P}^1_{\widetilde{K}}\backslash \widetilde{D})$ qui induit un isomorphisme $\pi_1(\mathbb{P}^1_K\backslash D)_{p'} \longrightarrow \pi_1(\mathbb{P}^1_{\widetilde{K}}\backslash \widetilde{D})_{p'}$.

Pour avoir plus de détails sur ces constructions, voir l'article *Fundamental Group* de Ariane Mézard dans [3].

Références.

[1] : Qing Liu. Tout groupe fini est un groupe de Galois sur $\mathbb{Q}_p(T)$, d'après Harbater. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 261–265. Amer. Math. Soc., Providence, RI, 1995.

[2] : Serre, Darmon, & Darmon Henri ... (2008). Topics in Galois theory (2nd ed., Research notes in mathematics v. 1).

[3] : Bost, Loeser, Raynaud, Bost Jean-Benoît ..., Loeser François ..., Raynaud Michel, & Centre international de rencontres mathématiques. (2000). Courbes semi-stables et groupe fondamental en géométrie algébrique Luminy, décembre 1998 (Progress in mathematics 187). Basel Boston Berlin: Birkhäuser.