

Déformations galoisiennes et groupe fondamental arithmétique : sur une conjecture de de Jong

Léo Gratien

Mathematical Institute, Oxford, encadré par James Newton

0.1 Prologue

Quelques mois avant de partir à Oxford, mon tuteur James Newton me conseille la lecture de *Modular Forms and Fermat's Last Theorem* [4]. Même le premier chapitre, introductif, m'est étranger et abscons.

0.2 Introduction

Le grand théorème de Fermat est démontré en 1994 par A. Wiles, et R. Taylor :

$$\text{FLT} : \quad a^n + b^n = c^n \quad \text{n'a pas de solution entière si } n > 2 \text{ et } abc \neq 0.$$

La démonstration de **FLT** repose sur la preuve d'un cas particulier de la conjecture dite de « modularité » (à savoir : toute courbe elliptique sur \mathbf{Q} est modulaire). Cette dernière est complètement résolue en 2001, mais les avancées conceptuelles majeures en ce sens ont lieu dans le travail de Wiles.

En particulier, l'étude des représentations des groupes de Galois ($\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, $\text{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$, etc.) s'avère cruciale (cf. remarque de 1.1). Soit k un corps, $n > 0$ et

$$\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \text{GL}_n(k)$$

une représentation continue. On a étudié principalement deux aspects de l'étude de ces morphismes :

1. Les déformations $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \text{GL}_n(A)$ de ρ ,
2. Une interprétation géométrique du groupe de Galois absolu : vu comme groupe fondamental.

On associe à ρ , sous quelques conditions, un anneau \mathcal{R}_ρ qui traite de l'ensemble de ces déformations (cf. section 1.3). La première partie du stage a consisté en l'étude d'un anneau de déformation particulier ([1], cf. sous-section 1.4). Le présent rapport traite surtout du second point.

Plus précisément, on étudie une conjecture formulée par A. de Jong en 2001 ([7], cf. section 2.3). Il est impossible de l'énoncer sans le détail de l'interprétation géométrique (cf. section 2), et nous renvoyons à la sous-section 2.3.1 pour un historique de celle-ci. La démonstration étudiée pendant le stage (de Khare et Böckle, [3] et [2]) utilise plusieurs outils tirés de la preuve de **FLT**. Il aurait été trop long de les introduire. On se contentera donc de présenter la preuve partielle de de Jong en sections 3 et 4.

Contents

0.1	Prologue	1
0.2	Introduction	1
1	Déformation de représentations galoisiennes	2
1.1	Groupe de Galois absolu	3
1.2	Déformations de représentation	3
1.3	Anneau de déformation universel	5
1.4	Utilité de l'anneau universel : le cas p -adique modulo p	6
2	Réinterprétation géométrique du groupe de Galois	7
2.1	Construction du groupe fondamental arithmétique	7
2.2	Le cas des courbes	9
2.3	Formulation de la conjecture de de Jong	10
3	Méthodes automorphes sur les corps de fonctions	13
3.1	Forme automorphe	13
3.2	Opérateurs de Hecke	14
3.3	Réciprocité de Drinfeld	15
4	Traduction et algébricité des valeurs propres : fin de la démonstration	15
4.1	Reformulation algébrique de la conjecture	15
4.2	Du côté automorphe	16
5	Épilogue	16
A	Schémas, courbes	17
B	Construction du groupe fondamental arithmétique	18
B.1	Morphismes étales	18
B.2	Le groupe fondamental — enfin !	18
B.3	Le groupe de Galois absolu de $\mathbb{C}(t)$	19
C	Cadre adélique	20

1 Déformation de représentations galoisiennes

L'intérêt des représentations de groupe de Galois est vaste. D'abord, la compréhension *en soi* du mystérieux groupe de Galois $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; ensuite, les théorèmes de relèvement de modularité aux applications que l'on sait en théorie des nombres (et sinon, cf. note de bas de page (4)).

1.1 Groupe de Galois absolu

Soit k un corps, supposé parfait. À toute extension galoisienne K/k est associée son groupe d'automorphismes $\text{Gal}(K/k)$ laissant k invariant. Si K est fini sur k , c'est un groupe d'ordre $[K : k]$. Si K est infini, $\text{Gal}(K/k)$ est un groupe profini¹, limite projective sur les extensions galoisiennes L/k finies incluses dans K . Il est compact pour la topologie associée.

Soit une extension intermédiaire $k \subset L \subset K$, alors K/L reste galoisienne et $\text{Gal}(K/L)$ est un sous-groupe de $\text{Gal}(K/k)$. Réciproquement, à $H \leq \text{Gal}(K/k)$ (fermé) est associée K^H le corps des éléments de K laissés invariants par H .

Rappelons la réciprocity sous-jacente, première pierre de la philosophie galoisienne:

Théorème 1.1. *La description du paragraphe précédent fournit un isomorphisme ordonné entre les extensions de corps intermédiaires et les sous-groupes fermés de $\text{Gal}(K/k)$. L'hypothèse de fermeture est superflue si k est fini. De plus, les sous-groupes normaux de $\text{Gal}(K/k)$ sont en bijection avec les extensions L/k galoisiennes.*

Définition 1.2. Le groupe de Galois absolu du corps k est le groupe de Galois associé à la clôture algébrique de k . Il est noté G_k dans toute la suite.

Remarque. Supposons k fini, disons $k = \mathbb{F}_{p^n}$. Alors $\bar{k} = \bigcup_d \mathbb{F}_{p^{dn}}$, et

$$G_k = \varprojlim_d \text{Gal}(\mathbb{F}_{p^{dn}}/\mathbb{F}_{p^n}) \cong \varprojlim_d \mathbb{Z}/d\mathbb{Z} = \hat{\mathbb{Z}}.$$

C'est bien un groupe profini, qui est généré topologiquement par 1. On appelle l'élément $x \mapsto x^p \in G_k$ correspondant le *frobenius arithmétique* du corps k .

Définition 1.3. Soit k un corps parfait, et A un anneau. Une A -représentation de G_k est un morphisme de groupe continu $G_k \rightarrow \text{GL}_n(A)$.

Remarque. ◦ L'anneau de base A est souvent choisi comme étant fini : \mathbb{F}_p , \mathbb{F}_l , ou comme l'anneau des entiers p -adiques ou leur corps de fractions \mathbb{Q}_l et \mathbb{Q}_p ².

- Les sources de représentations galoisiennes sont nombreuses. Soit V un A -module de rang n . Supposons que V est muni d'une action continue de G_k . C'est équivalent à la donnée d'une A -représentation de dimension n , tel que le stabilisateur de tout élément est ouvert. Alors le morphisme $G_k \rightarrow \text{GL}(V)$ donne une A -représentation de G_k .
- Une représentation est dite *modulaire* si elle « provient de la géométrie ». Exemple : soit E une courbe elliptique définie sur \mathbb{Q} (e.g. par $y^2 = x^3 + 1$), munie de sa loi de groupe commutatif, et p un nombre premier. On note $E[p^n]$ la p^n -torsion et $T_p(E) = (\varprojlim_n E[p^n]) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ le \mathbb{Q}_p -module de Tate de E . $G_{\mathbb{Q}}$ agit continûment sur chaque groupe de torsion, donc sur $T_p(E)$.

Par le point précédent, il en résulte une représentation galoisienne de dimension 2 :

$$\rho_{E,p} : G_{\mathbb{Q}} \rightarrow \text{GL}(T_p(E)) \cong \text{GL}_2(\mathbb{Q}_l).$$

1.2 Déformations de représentation

Soient Γ un groupe profini et k est un corps fini de caractéristique p , et $\bar{\rho} : \Gamma \rightarrow \text{GL}_n(k)$ une représentation de Γ , où. On définit, suivant [4], VIII, une classe d'anneaux de déformation, qui s'avère assez restrictive pour que les théorèmes de cette section soient vérifiés.

¹Un groupe est dit *profini* s'il est limite projective de groupe fini. C'est un pro- p -groupe s'il est limite projective de p -groupe.

²La précision des deux cas $l \neq p$ importe dans le cas où k est de caractéristique p . L'arithmétique change substantiellement d'un cas à l'autre, comme nous le verrons en sections 1.4, et 2.3.

Définition 1.4. Soit Λ un anneau à valuation discret complet de corps résiduel k . On définit $\mathcal{C}(\Lambda)$ la catégorie des Λ -algèbre locale noethérienne, artinienne, complète de corps résiduel k . Elle est munie de morphismes locaux, qui induisent l'identité sur k .

Remarque. Il suffit d'avoir en tête le cas $\Lambda = \mathbb{Z}_p$ ou $\mathcal{W}(k)$ l'anneau des vecteurs de Witt de k .

Définition 1.5. Soit $A \in \mathcal{C}(\Lambda)$. On dit qu'une déformation $\rho : \Gamma \rightarrow \mathrm{GL}_n(A)$ est un relèvement de $\bar{\rho}$ si la réduction modulo \mathfrak{m}_A donne $\bar{\rho}$:

$$\begin{array}{ccc} \Gamma & \xrightarrow{\bar{\rho}} & \mathrm{GL}_n(k) \\ & \searrow \rho & \uparrow (\text{mod } \mathfrak{m}_A) \\ & & \mathrm{GL}_n(A) \end{array}$$

Deux relèvements sont équivalents si et seulement si l'un est conjugué de l'autre par une matrice de $\ker(\mathrm{GL}_n(A) \rightarrow \mathrm{GL}_n(k))$. Une classe d'équivalence de relèvements est une déformation de $\bar{\rho}$.

On obtient deux foncteurs de déformation (le premier est dit *cadre*), selon la sensibilité au changement de base.

$$\begin{aligned} \mathcal{D}_{\bar{\rho}}^{\square} : \mathcal{C}_{\Lambda} &\longrightarrow \text{Ens} \\ A &\longmapsto \{\text{relèvements de } \bar{\rho} \text{ à coefficients dans } A\} \end{aligned}$$

et

$$\begin{aligned} \mathcal{D}_{\bar{\rho}} : \mathcal{C}_{\Lambda} &\longrightarrow \text{Ens} \\ A &\longmapsto \{\text{déformations de } \bar{\rho} \text{ à coefficients dans } A\} \end{aligned}$$

Exemple 1.6. ◦ Une déformation d'ordre 2 de $\bar{\rho}$ est la donnée de $\rho : \Gamma \rightarrow \mathrm{GL}_n(k[\varepsilon]/\varepsilon^2)$. On peut écrire toute matrice $\rho(\gamma) = \bar{\rho}(\gamma) + \varepsilon b(\gamma)$ avec $b(\gamma) \in M_n(k)$.

◦ Une déformation $\rho_m : \Gamma \rightarrow \mathrm{GL}_n(k[\varepsilon]/\varepsilon^m)$ d'ordre m se réduit à une déformation d'ordre $m-1$ modulo ε^{m-1} . D'où un diagramme commutatif:

$$\begin{array}{ccccccc} & & & & \Gamma & & \\ & & & & \downarrow \bar{\rho} & & \\ & & \rho_m & & \swarrow \rho_2 & & \\ \mathrm{GL}_n(k[\varepsilon]/\varepsilon^m) & \longrightarrow & \dots & \xrightarrow{(\text{mod } \varepsilon^2)} & \mathrm{GL}_n(k[\varepsilon]/\varepsilon^2) & \xrightarrow{(\text{mod } \varepsilon)} & \mathrm{GL}_n(k) \end{array}$$

L'exemple précédent soulève deux questions. Quand est-ce qu'un tel relèvement existe ? A-t-on une factorisation de tout relèvement vers un « anneau universel » associé à $\bar{\rho}$? Dans le cas précédent, on s'attendrait à une représentation $\rho_{\infty} : \Gamma \rightarrow \mathrm{GL}_n(k[[\varepsilon]])$ où $k[[\varepsilon]] := \lim_m k[\varepsilon]/\varepsilon^m$.

Il convient d'ajouter des conditions \mathcal{P} aux déformations étudiés : il est parfois nécessaire de fixer le déterminant, ou la trace des déformations. On définit un foncteur $\mathcal{D}_{\bar{\rho}}^{\mathcal{P}}$ de manière analogue et les mêmes questions tiennent. Cela apparaît par exemple en section 2.3.

1.3 Anneau de déformation universel

La représentabilité du foncteur de déformation nécessite en général une hypothèse technique de finitude sur le groupe Γ . Elle est vérifiée dans toutes les applications de ce texte.

Définition 1.7 (Hypothèse Φ_ρ). Pour tout $\Gamma' \subset \Gamma$ sous groupe ouvert, $\text{Hom}(\Gamma', F_\rho)$ est fini.

Avec cette hypothèse, le foncteur de relèvement est toujours représentable. Ce n'est pas le cas du foncteur de déformation, qui nécessite une hypothèse supplémentaire.

Définition 1.8. La représentation $\bar{\rho}$ est *absolument irréductible* si

$$\bar{\rho} \otimes_k \bar{k} : \Gamma \longrightarrow \text{GL}_n(\bar{k})$$

est une représentation de groupe irréductible. De manière, équivalente, $\rho \otimes_k K$ est irréductible pour toute extension K finie de k .

Théorème 1.9. Soit $A \in \mathcal{C}(\Lambda)$. Supposons que Γ est un Φ_ρ -groupe.

- (i) Le foncteur $\mathcal{D}_{\bar{\rho}}^\square$ est représentable par un couple $(R_{\bar{\rho}}^\square, \rho^{\text{univ}})$ dans la catégorie $\mathcal{C}(\Lambda)$.
- (ii) On suppose $\bar{\rho}$ absolument irréductible, alors $\mathcal{D}_{\bar{\rho}}$ est représentable par un couple $(R_{\bar{\rho}}, \rho^{\text{univ}})$ dans la catégorie $\mathcal{C}(\Lambda)$.
Le couple $(R_{\bar{\rho}}, \rho^{\text{univ}})$ est alors unique à unique isomorphisme près.

Preuve. On construit l'anneau de relèvement explicitement. S'il on impose des conditions de déformations, d'autres méthodes existent ([4], VIII, Chapter 4). Γ étant profini, on distingue deux cas.

• *Cas 1* : Γ est un groupe fini. L'anneau universel $R_{\bar{\rho}}(\Gamma)$ doit 1. appartenir à $\mathcal{C}(\Lambda)$; 2. vérifier pour tout $A \in (\Lambda)$ la propriété universel

$$\text{Hom}_{\Lambda\text{-alg}}(R_{\bar{\rho}}(\Gamma), A) \cong \text{Hom}_{\text{gp}}(\Gamma, \text{GL}_n(A)). \quad (1.1)$$

Soit R_Γ la Λ -algèbre engendrée par $X_{i,j}^g$ ($1 \leq i, j \leq n$ et $g \in \Gamma$) et soumise aux relations :

- $X_{i,j}^e = \delta_{i,j}$,
- $X_{i,j}^{g^b} = \sum_{k=1}^n X_{i,k}^g X_{k,j}^b$.

Alors $f \mapsto (g \mapsto (f(X_{i,j}^g))_{i,j})$ réalise la bijection (1.1) pour toute Λ -algèbre A . Il reste à modifier R_Γ pour appartenir à $\mathcal{C}(\Lambda)$.

La bijection (1.1) donne un morphisme $R_\Gamma \mapsto k$. Son noyau est un idéal maximal $\mathfrak{m} \subset R_\Gamma$, et on peut compléter R_Γ pour la topologie \mathfrak{m} -adique :

$$R_{\bar{\rho}}(\Gamma) := \varprojlim_{l \rightarrow \infty} R_\Gamma / \mathfrak{m}^l.$$

C'est visiblement un objet de $\mathcal{C}(\Lambda)$. Soit $\rho : \Gamma \longrightarrow \text{GL}_n(A)$ une déformation de $\bar{\rho}$, A dans $\mathcal{C}(\Lambda)$. La bijection (1.1) donne $f : R_\Gamma \rightarrow A$ un morphisme de Λ -algèbre tel que $f(\cdot) \in \mathfrak{m}_A$. D'où, pour tout $l \geq 0$, un morphisme $R_{\bar{\rho}}(\Gamma) \twoheadrightarrow R_\Gamma / \mathfrak{m}^l \rightarrow A / \mathfrak{m}_A^l$. Il passe à la limite :

$$\tilde{f} : R_{\bar{\rho}}(\Gamma) \longrightarrow A = \varprojlim_l A / \mathfrak{m}_A^l \quad (A \in (\Lambda)),$$

et le diagramme suivant commute :

$$\begin{array}{ccc}
\Gamma & \xrightarrow{\rho} & \mathrm{GL}_n(A) \\
\mathrm{id} \uparrow & & \uparrow \tilde{f} \\
\Gamma & \xrightarrow{\rho^{\mathrm{univ}}} & \mathrm{GL}_n(R_{\bar{\rho}}(\Gamma))
\end{array}$$

Enfin \tilde{f} et $R_{\bar{\rho}}(\Gamma)$ sont uniquement déterminés par le diagramme ci-dessus.

• *Cas 2* : Γ est profini. Notons $\Gamma = \varprojlim G$ où G décrit les quotients finis de Γ tels que $\bar{\rho}$ se factorise³ par G .

Par le cas 1, on dispose de $(R_{\bar{\rho}}(G), \rho_G^{\mathrm{univ}})$ universel pour $\bar{\rho}|_G$. Grâce à la propriété de Φ_p -finitude, le système projectif $(R_{\bar{\rho}}(G))$ admet une limite $R_{\bar{\rho}}$ dans $\mathcal{C}(\Lambda)$.

Montrons que $R_{\bar{\rho}}$ est l'anneau de déformation universel associé à $\bar{\rho}$. Soit $A \in \mathcal{C}(\Lambda)$:

$$\begin{aligned}
\mathcal{D}_{\bar{\rho}}^{\square}(A) &= \varprojlim_G \mathcal{D}_{\bar{\rho}|_G}^{\square}(A) = \varprojlim_G \mathrm{Hom}_{\Lambda\text{-alg}}(R_{\bar{\rho}}(G), A) \\
&= \mathrm{Hom}_{\Lambda\text{-alg}}(\varprojlim_G R_{\bar{\rho}}(G), A) \\
&= \mathrm{Hom}_{\Lambda\text{-alg}}(R_{\bar{\rho}}, A). \quad \square
\end{aligned}$$

La compréhension des déformations de $\bar{\rho}$ revient à l'étude de ses anneaux de déformation universels donnés par le théorème 1.9. En effet, une déformation $\rho : \Gamma \rightarrow \mathrm{GL}_n(A)$ est équivalent à la donnée d'un morphisme d'anneaux $R_{\bar{\rho}} \rightarrow A$. Le premier résultat est le

Corollaire 1.10. *On dispose de $d \in \mathbb{N}$ et d'un morphisme surjectif*

$$\Lambda[[x_1, \dots, x_d]] \twoheadrightarrow R_{\bar{\rho}}.$$

En particulier $R_{\bar{\rho}}$ est quotient de l'anneau de série formelle $\Lambda[[x_1, \dots, x_r]]$ par un idéal I , appelé idéal des relations.

Remarque. L'entier d s'interprète comme la dimension du groupe $H^1(\Gamma, \mathrm{ad}(\rho))$. Le calcul de l'idéal des relations est difficile. Dans l'exemple présenté en section suivante, une description précise de I est donnée.

Exemple 1.11. Reprenons l'exemple 1.6, et supposons le foncteur de déformation représentable. On dispose alors d'une factorisation pour tout m :

$$\begin{array}{ccccc}
& & \rho^{\mathrm{univ}} & & \Gamma \\
& & \swarrow & \searrow & \downarrow \bar{\rho} \\
\mathrm{GL}_n(R_{\bar{\rho}}) & \dashrightarrow & \mathrm{GL}_n(k[[\varepsilon]]/\varepsilon^m) & \xrightarrow{(\mathrm{mod} \varepsilon)} & \mathrm{GL}_n(k)
\end{array}$$

donc d'un morphisme $R_{\bar{\rho}} \rightarrow k[[\varepsilon]]$, comme attendu.

1.4 Utilité de l'anneau universel : le cas p -adique modulo p

Nous présentons ici un autre résultat étudié au début du stage, à titre d'illustration. Cette section est indépendante du reste du texte.

Les opérateurs de Hecke, étudiés en section 3.2, permettent de définir l'analogue \mathbf{T} de l'anneau universel « côté automorphe ». Il s'avère qu'un isomorphisme existe parfois entre l'algèbre de Hecke \mathbf{T} et certains

³Il existe une infinité de tels G . En effet Γ est compact et $\mathrm{GL}_n(k)$ est un groupe fini. Le morphisme continu $\bar{\rho}$ est donc induit par $G_0 \rightarrow \mathrm{GL}_n(k)$ où G_0 est fini. Tout quotient fini contenant G_0 convient.

anneaux de déformations. Ces algèbres sont donc les *points de jonctions* du pont conjectural entre théorie des nombres, et formes automorphes⁴. C'est le départ du programme de Langlands.

Soit F une extension finie de \mathbf{Q}_p , et une représentation continue $\bar{\rho} : G_F \longrightarrow \mathrm{GL}_n(\mathbf{F}_p)$. On pose dans cette section $\Lambda = \mathbf{Z}_p$.

Théorème 1.12. *L'anneau de déformation $R_{\bar{\rho}}^{\square}$ vérifie les propriétés suivantes :*

- (i) *il est local, plat, d'intersection complète (cf. le corollaire suivant),*
- (ii) *sa dimension en tant que \mathbf{Z}_p -module vaut $n^2 + n^2[F : \mathbf{Q}_p]$.*

Corollaire 1.13. *En particulier on a la présentation suivante :*

$$R_{\bar{\rho}}^{\square} \cong \frac{\mathbf{Z}_p[[x_1, \dots, x_r]]}{(f_1, \dots, f_s)},$$

où (f_1, \dots, f_s) est une suite régulière de $\mathbf{Z}_p[[x_1, \dots, x_r]]$.

La preuve de ce résultat récent [1] répond à une conjecture de Mazur ([9], section 10). Elle repose sur l'étude des dimensions des composantes d'une décomposition de $\mathrm{Spec}(R_{\bar{\rho}}^{\square})$, et est inaccessible sans introduire le langage des schémas.

Corollaire 1.14. *Soit $\bar{\rho} : G_F \longrightarrow \mathrm{GL}_n(\mathbf{F}_p)$ une représentation continue. Alors $\bar{\rho}$ admet un relèvement en caractéristique zéro $\rho : G_F \longrightarrow \mathrm{GL}_n(\mathbf{Z}_p)$.*

Preuve. Par le théorème 1.12, $R_{\bar{\rho}}^{\square}$ est plat donc $R_{\bar{\rho}}^{\square}[\frac{1}{p}]$ est non nul. Soit x un point fermé de $\mathrm{Spec}(R_{\bar{\rho}}^{\square}[\frac{1}{p}])$, il donne un morphisme $R_{\bar{\rho}}^{\square} \rightarrow \overline{\mathbf{Q}_p}$. Par composition, on dispose donc de $\rho_0 :$

$$\begin{array}{ccc} G_F & \xrightarrow{f_0} & \mathrm{GL}_n(\overline{\mathbf{Q}_p}) \\ & \searrow \rho^{\mathrm{univ}} & \nearrow x^* \\ & \mathrm{GL}_n(R_{\bar{\rho}}^{\square}) & \end{array}$$

et on conclut en prenant $\rho = \rho_0 \otimes \mathbf{Z}_p$. □

2 Réinterprétation géométrique du groupe de Galois

Avant de formuler le problème posé par de Jong, voyons comment il est possible de construire un groupe d'homotopie associé à une variété algébrique. La section suivante présente l'analogie au cas topologique de la construction complète donnée en annexe B.

2.1 Construction du groupe fondamental arithmétique

2.1.1 Détour par la construction topologique

On se donne un espace topologique X . La définition du groupe fondamental topologique $\pi_1^{\mathrm{top}}(X, a)$ est possible si l'on suppose par exemple X connexe par arcs : c'est le groupe des classes d'homotopies des lacets

⁴On a par exemple vu comment les représentations pouvaient provenir de courbes elliptiques. Je n'ai malheureusement pas la place de détailler la preuve du dernier théorème de Fermat par A. Wiles (présentée en [12]) dans cette note.

Elle exploita une correspondance représentations—formes modulaires et initia la théorie des déformations. Il s'avère que l'existence d'une solution non-triviale $a^n + b^n = c^n$ permet de construire une représentation, donc une forme modulaire à propriétés spécifiques (une *newform* de poids 2) dont on sait par ailleurs l'inexistence.

de point de base $a \in X$ fixé. Or une variété générique n'aura pas une telle propriété topologique. On procède donc autrement :

Soit $p : Y \rightarrow X$ un revêtement topologique, non ramifié (i.e. en tout point x de X , on dispose d'un voisinage U tel que chaque composante connexe de $p^{-1}(U)$ soit homéomorphe U par p). Il est dit *fini* si le nombre de composantes connexes de $p^{-1}(U)$ est fini. Soit $\mathbf{Rev}(X, x)$ la catégorie des revêtements non-ramifiés connexes de X pointés en x . Rappelons que sous des hypothèses plus restreintes, on a la

Proposition 2.1. *Soit X connexe, localement connexe par arcs et localement simplement connexe, la catégorie ordonnée $\mathbf{Rev}(X, a)$ est équivalente à l'ensemble ordonné des sous-groupes de $\pi_1^{\text{top}}(X, a)$.*

Preuve. Soit $(Y, b) \in \mathbf{Rev}(X, a)$. L'image de l'application injective $\pi_1^{\text{top}}(Y, b) \rightarrow \pi_1^{\text{top}}(X, a)$ fournit le sous-groupe.

Réciproquement, à N un sous-groupe de $\pi_1^{\text{top}}(X, a)$ on associe l'espace (Y_N, a_N) donné par :

$$Y_N = \{\gamma \text{ un chemin de source } a \text{ dans } X\} / \sim_N,$$

où deux chemins sont équivalents dans Y_N si et seulement si leur but est identique et le lacet obtenu par composition est dans N . \square

Si de plus le sous-groupe $N \subset \pi_1^{\text{top}}(X, a)$ est distingué, le revêtement correspondant est dit *galoisien*.

En particulier, N trivial correspond au revêtement universel \widehat{X} de X , et $\text{Aut}(\widehat{X}/X)^{\text{op}}$ donne une interprétation du groupe fondamental n'utilisant pas les lacets. Si nous savons construire un tel espace au dessus de X , nous sommes en mesure de définir le groupe fondamental sans considération intrinsèquement topologique. Seulement, plusieurs aspects algébriques seraient alors occultés, comme la functorialité, et la dépendance en a . On notera dans la suite $\widehat{p} : \widehat{X} \rightarrow X$ le revêtement universel au dessus de a .

2.1.2 Formulation catégorique

Les hypothèses de la proposition 2.1 sont en vigueur. Notons $\mathbf{Rev}^*(X)$ la catégorie des revêtements non-ramifiés *plus nécessairement connexes* sans mention d'un point de base.

Soit $(Y, p) \in \mathbf{Rev}^*(X)$. Un chemin continu de a à b dans X donne lieu, par propriété de relèvement universel, à l'action du groupe fondamental sur les fibres du revêtement:

$$\begin{aligned} \pi_1^{\text{top}}(X; a, b) \times p^{-1}(a) &\longrightarrow p^{-1}(b) \\ (\gamma, a') &\longmapsto \widehat{\gamma}(a'). \end{aligned} \tag{2.1}$$

Remarque. Avec ce point de vue,

- un N sous-groupe est galoisien si l'action du groupe fondamental sur $Y_N \rightarrow X$ est fidèle et transitive.
- L'action de $\pi_1^{\text{top}}(X, a)$ sur le groupe des automorphismes de Y_N au dessus de X est bien définie, et de plus $\pi_1(X, a)/N \cong \text{Aut}(Y_N/X)^{\text{op}}$.

Définition 2.2. Soit F_a le foncteur covariant « fibre en a » $\mathbf{Rev}^*(X) \rightarrow \mathbf{Ens}$ qui à un revêtement (Y, p) associe $p^{-1}(a)$.

Soit γ un élément de $\pi_1^{\text{top}}(X; a, b)$. Par (2.1), γ définit le morphisme $\alpha(Y) : F_a(Y) \rightarrow F_b(Y)$ et donc une transformation naturelle de F_a vers F_b . Réciproquement,

Proposition 2.3. *Sous les mêmes hypothèses sur X , le groupe fondamental topologique correspond aux transformations des foncteurs fibres :*

$$\text{Hom}(F_a, F_b) \cong \pi_1^{\text{top}}(X; a, b).$$

Preuve. Un sens a été vu. Reste à obtenir un chemin de a à b sachant une transformation naturelle $\alpha : F_a \mapsto F_b$.

Notons qu'un revêtement universel \widehat{X} au dessus de a représente canoniquement le foncteur $F_a : F_a(Y) \cong \text{Hom}_{\mathbf{Rev}^*(X)}(\widehat{X}, Y)$.

L'élément $\alpha(\widehat{X}) : F_a(\widehat{X}) \longrightarrow F_b(\widehat{X})$ s'écrit donc $\alpha(\widehat{X})^{\text{op}} : \pi_1^{\text{top}}(X; b) \longrightarrow \pi_1^{\text{top}}(X; a)$ sachant l'isomorphisme $F_a(\widehat{X}) \cong \text{Aut}(\widehat{X}/X) \cong \pi_1^{\text{top}}(X; a)^{\text{op}}$. Le chemin de a à b en découle. \square

Pour résumer, nous avons obtenu les isomorphismes suivants (à l'ordre de l'opération près), nous permettant enfin une définition (qui a perdu en clarté, certes) du groupe fondamental d'un espace « général » :

$$\pi_1^{\text{top}}(X; a) \cong \text{Aut}(\text{Hom}_{\mathbf{Rev}^*(X)}(\widehat{X}, -)) \cong \text{Aut}(F_a).$$

En particulier, l'équivalence entre $\mathbf{Rev}^*(X)$ des revêtements non ramifiés de X et les $\pi_1(X, a)$ -ensembles, donnée par la fibre en a .

2.1.3 Groupe fondamental arithmétique

En appendice est construit le groupe fondamental arithmétique d'un schéma connexe grâce à l'aperçu catégorique précédent. Seul le cas des courbes et des points ($\text{Spec } k$ avec k un corps) seront utilisés, mais les théorèmes 2.7 et 2.8 en justifient le cadre général.

Partons d'une variété algébrique, ou d'un schéma. Deux difficultés se posent :

1. La notion de *ramification* est plus subtile dans le cas algébrique.
2. L'existence d'un revêtement universel tombe en défaut.

En réponse aux deux difficultés soulevées : les morphismes entre schémas connexes analogues des revêtements non-ramifiés sont construits en appendice B. Ils sont dit *étales* ; le groupe fondamental est une limite de groupe fini : il est profini.

Définition 2.4. Soit X un schéma connexe. Le *groupe fondamental arithmétique* de X est la limite des groupes d'automorphismes $\text{Aut}(Y/X)$, où $Y \rightarrow X$ est un morphisme fini galoisien, et étale de schémas :

$$\pi_1^{\text{ét}}(X) = \varprojlim_{Y \rightarrow X} \text{Aut}(Y/X).$$

Si X est une courbe projective et lisse, on obtient l'expression simplifiée

$$\pi_1^{\text{ét}}(X) = \text{Gal}(\widehat{k(X)}/k(X)),$$

où $\widehat{k(X)}$ est la composée des corps $k(Y)$ où Y est un revêtement étale fini et galoisien de X .

Proposition 2.5. Soit $\phi : X \rightarrow Y$ un morphisme de schémas envoyant un point \bar{x} sur \bar{y} . Par construction, un morphisme continu de groupes profinis $\phi^* : \pi_1(X, \bar{x}) \longrightarrow \pi_1(Y, \bar{y})$.

2.2 Le cas des courbes

Bien que la conjecture de de Jong soit formulée en toute généralité en section 2.3, nous travaillerons dans le reste de notre travail avec X une courbe lisse et projective. En fait, le cas général s'en déduit ; cf. remarque 2.13.

Nous avons vu que le groupe fondamental arithmétique fournit une généralisation de la notion groupe d'automorphismes de revêtements d'espace topologique. Quand ce dernier est un point (muni, tout de même, de sa structure de schéma) $\text{Spec } k$, on retrouve le groupe de Galois absolu de k ; cf. exemple B.7.

2.2.1 Du corps à la courbe

Étant donné X sur k une courbe, on construit sa « réalisation géométrique »⁵ $\overline{X} = X_{\overline{k}}$. Si un polynôme $f \in k[x, y]$ définit X sur k , \overline{X} est la courbe sur \overline{k} défini par le même polynôme vu sur $\overline{k}[x, y]$. Les morphismes $\overline{X} \rightarrow X \rightarrow \text{Spec } k$ donnent par functorialité (prop. 2.5) une suite :

$$\pi_1(\overline{X}, \overline{x}) \longrightarrow \pi_1(X, \overline{x}) \longrightarrow \pi_1(\text{Spec } k, \overline{x}) \cong G_k.$$

Définition 2.6. On appelle $\pi_1(X, \overline{x})$ (resp. $\pi_1(\overline{X}, \overline{x})$) le groupe fondamentale arithmétique (resp. géométrique) de X .

Théorème 2.7 (Suite exacte homotopique). *Le complexe ainsi construit est une extension de groupe profinis :*

$$1 \longrightarrow \pi_1(\overline{X}, \overline{x}) \longrightarrow \pi_1(X, \overline{x}) \longrightarrow G_k \longrightarrow 1.$$

Ce théorème est fondamental. Comme notre notation le suggère, le groupe géométrique capture la géométrie de X , tandis qu'à l'opposé se trouve son contenu arithmétique. Le groupe $\pi_1(X, \overline{x})$ synthétise ces deux aspects, et reste dans la majorité des cas mystérieux. Nous renvoyons à la sous-section 2.2.2 suivante pour une quantification de ce phénomène.

La conjecture de de Jong (section 2.3) donne un autre aperçu de la différence de complexité des groupes fondamentaux arithmétique et géométrique.

2.2.2 De la topologie à l'algèbre

Si nous prenons $k = \mathbb{C}$, la courbe X peut être vue soit algébriquement, soit topologiquement. Les deux groupes fondamentaux correspondant sont en relation, la plus simple qui soit :

Théorème 2.8. *Soit X une courbe sur \mathbb{C} et $X(\mathbb{C})$ sa réalisation comme variété topologique de \mathbb{C} . Le groupe fondamental géométrique de X est la complétion profinie du π_1 topologique :*

$$\pi_1^{\text{ét}}(X, \overline{x}) \cong \widehat{\pi_1^{\text{top}}(X(\mathbb{C}), \overline{x})}.$$

Exemple 2.9. Soit $X = \mathbb{P}^1(\mathbb{C})$ le plan projectif. Ce n'est pas une courbe algébrique, n'étant pas affine. Mais X privé d'un point devient l'espace affine $\mathbb{A}^1(\mathbb{C}) = \text{Spec}(\mathbb{C}[t]) \cong \mathbb{C}$. En effet, \mathbb{C} est algébriquement clos et tout idéal premier de $\mathbb{C}[t]$ est de la forme $(x - \lambda)$ pour λ complexe. D'après le théorème précédent, $\pi_1^{\text{géo}}(X - \{x\}) = 1$.

Remarque. Ce dernier théorème permet en particulier de décrire explicitement le groupe $\mathbb{C}(t)$. C'est assez spectaculaire pour qu'on en donne le détail ; cf. appendice B.3.

2.3 Formulation de la conjecture de de Jong

On énonce la conjecture de de Jong avant d'en faire un bref historique, et d'en donner les limites.

Soit X une courbe lisse et projective sur un corps fini \mathbb{F}_q , et ρ une représentation continue

$$\pi_1(X) \longrightarrow \text{GL}_n(\mathbb{F}_l((t))),$$

avec l un nombre premier ne divisant pas q . Supposons que $\rho|_{\pi_1(\overline{X})}$ est absolument irréductible.

Conjecture 1 (de Jong). *Sous les hypothèses ci-dessous, le groupe $\rho(\pi_1(\overline{X}))$ est fini.*

Sauf mention du contraire, par « courbe » sera entendu « courbe lisse et projective sur \mathbb{F}_p » dans le reste de cette section.

⁵La terminologie vient du cas $k = \mathbb{Q}$ ou k un corps de nombres, auquel cas \overline{X} est une courbe sur \mathbb{C} .

2.3.1 Historique et intérêt

Dans *Conjecture de Weil : II* ([5], Conjecture (1.2.10)), Deligne formule une conjecture sur valeurs propres d'un opérateur sur les fibres d'un faisceau $\overline{\mathbf{Q}}_l$ -lisse sur une courbe X . Drinfeld et Deligne démontre le cas des faisceaux de rang 2 grâce aux travaux de ce dernier.

Remplaçant les corps de coefficients $\overline{\mathbf{Q}}_l$ par $\overline{\mathbf{F}_l((t))}$, on obtient la conjecture de de Jong, reformulée dans [7] en la conjecture 1 :

Conjecture 2. *Soit X une courbe définie sur un corps fini de caractéristique $p \neq \ell$. Le groupe de monodromie géométrique de tout $\overline{\mathbf{F}_l((t))}$ -faisceau lisse est fini.*

Il est naturel de se demander si remplacer $\mathbf{F}_l((t))$ par $\mathbf{F}_p((t))$, \mathbf{Q}_p ou \mathbf{Q}_l dans la conjecture 1 donne encore un énoncé plausible. Malheureusement, il n'en est rien. Détaillons le premier cas.

Proposition 2.10. *La conjecture 1 avec p au lieu de l est fausse.*

Preuve. Supposons $F = \mathbf{F}_p((t))$. On pose $X := \mathbf{A}_{\mathbf{F}_p}^1$. Soit $f(t) \in \mathbf{F}_p[t]$ irréductible et $Y \rightarrow X$ le morphisme (étale) correspondant à l'extension d'Artin-Schreier $\mathbf{F}_p[t, x]/(x^p - x - f(t))$ sur $\mathbf{F}_p[t]$. C'est une extension cyclique de degré p de $\mathbf{F}_p(t)$. Pour f premier à g , on obtient deux réalisations distinctes de \mathbf{F}_p dans $\pi_1(\overline{X})$. Soient $f_i(t)$, $i \geq 0$ des polynômes de $\mathbf{F}_p[t]$ deux à deux premiers entre eux. On construit à l'aide des extensions (restant galoisiennes)

$$\mathbf{F}_p[t, x_1, \dots, x_n]/(x_i^p - x_i - f_i(t))$$

des morphismes surjectifs et compatibles $\phi_n : \pi_1(\overline{X}) \twoheadrightarrow \mathbf{F}_p^n$. D'où une flèche *surjective*

$$\pi_1(\overline{X}) \longrightarrow \bigcup_n \mathbf{F}_p^n \cong \mathbf{F}_p((t)).$$

Composée à l'injection $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} : \mathbf{F}_p((t)) \longrightarrow \mathrm{SL}_2(\mathbf{F}_p((t)))$, la conjecture de de Jong tombe en défaut. \square

Dans le même papier [7], il est démontré que la conjecture 1 équivaut la finitude de l'anneau de déformation universel attaché à la représentation résiduelle $R_{X, \overline{\rho}}$ définie en section 1.3.

Théorème 2.11. *Avec les même hypothèses que dans la conjecture de de Jong, s'équivalent :*

- (i) *le groupe $\rho(\pi_1(\overline{X}))$ est fini,*
- (ii) *$R_{X, \overline{\rho}}$ est un \mathbf{Z}_l -module fini.*

L'auteur démontre en 2001 sa conjecture dans le cas $n = 2$ grâce à la réciprocity de Drinfeld par des méthodes automorphes que nous présentons en section 3.2. Dans [2], ultérieurement pendant le stage, Böckle et Khare démontre la conjecture 1 pour tout $n \geq 1$ avec de fortes hypothèses sur la représentation ρ . Leur démonstration est complètement différente car elle prouve la finitude de $R_{X, \overline{\rho}}$ et conclut par le théorème 2.11, par des méthodes dues à Wiles, Skinner et Taylor. Enfin, D. Gaitsgory en 2006 démontre la conjecture en toute généralité dans [6] en utilisant la réciprocity de Drinfeld pour tout n .

Ainsi, avec de Jong et Gaitsgory, on *déduit* la finitude de $R_{X, \overline{\rho}}$. Avec Böckle-Khare, on *utilise*.

2.3.2 Quelques réductions

On formule une réduction de la représentation $\pi_1(X) \rightarrow \mathrm{GL}_n(\mathbf{F}_l((t)))$ qui sera nécessaire à l'attribution d'une forme automorphe propre à ρ , cf. section 3.3.

Définition 2.12. Soit Γ un groupe profini et V un k -espace vectoriel. Soit ρ une représentation continue $\Gamma \rightarrow \mathrm{GL}(V)$.

- (i) On dit que ρ est *irréductible* si l'action de Γ sur V n'a pas d'espace propre non nul stable par Γ .
- (ii) On dit que ρ est *absolument irréductible* si $\rho \otimes_k \bar{k}$ est irréductible. Il est équivalent de demander à ce que $V \otimes_k K$ soit irréductible pour toute extension K/k finie.

Proposition 2.13. *Il suffit de démontrer la conjecture 1 pour tout couple (X, V, ρ) avec X une courbe lisse et projective, $\dim V \leq n$ et de plus :*

- (i) $\det(\rho)$ est trivial,
- (ii) $\rho|_{\pi_1(\bar{X})}$ est absolument irréductible.

2.3.3 Démonstration en dimension $n = 1$

Notons $F = \mathbf{F}_l((t))$. Soit $\rho : \pi_1(X) \rightarrow F^*$ une représentation continue. On tire parti du fait qui n'est vrai que si $n = 1$: $\mathrm{GL}_1(F) = F^*$ est abélien. D'où la factorisation⁶ $\rho : \pi_1(X)^{\mathrm{ab}} \rightarrow F^*$. Or nous avons le

Théorème 2.14. *Avec les notations ci-dessus, on a les décompositions suivantes*

$$F^* = (\text{pro-}l\text{-groupe}) \times \mathbf{F}_l^* \times \mathbf{Z} \quad \text{et} \quad \pi_1(X)^{\mathrm{ab}} = (\text{pro-}p\text{-groupe}) \times (\text{groupe fini}) \times \hat{\mathbf{Z}}.$$

De plus, le groupe fondamental géométrique $\pi_1(\bar{X})$ s'envoie par la flèche $\pi_1(\bar{X}) \rightarrow \pi_1(X) \rightarrow \pi_1(X)^{\mathrm{ab}}$ dans les deux premiers facteurs de $\pi_1(X)^{\mathrm{ab}}$.

Définition 2.15. Soit $\mathcal{W}(X, \bar{x}) \subset \pi_1(X, \bar{x})$ l'image inverse du sous-groupe $\langle \mathrm{Fr}_p \rangle \subset \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$, c'est à dire l'image de \mathbf{Z} dans $\hat{\mathbf{Z}}$, par 2.7. C'est le groupe de Weil de X . Par exactitude de la suite d'homotopie 2.7, on voit $\pi_1(\bar{X}, \bar{x})$ comme un sous-groupe de $\mathcal{W}(X, \bar{x})$.

Soit \tilde{X} la courbe complétée projective lisse de X et S l'ensemble (fini) des places (finies) $\tilde{X} - X$. Le lemme suivant est un corollaire de la théorie du corps de classe, dont on rappelle seulement le cadre en appendice C (pour la preuve, cf. [11], IV, Théorème 7).

Lemme 2.16. *Soit $K = k(X)$ le corps de fonction de X et $K^{\mathcal{S}, \mathrm{ab}}$ l'extension de K abélienne non-ramifiée maximale hors de S . Alors*

$$\mathcal{W}(X, \bar{x})^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathcal{S}, \mathrm{ab}}/K) = \left(\prod_{v \notin S} \mathcal{O}_v^* \right) \backslash \mathbf{A}_K^*/K^*,$$

et l'image du groupe géométrique dans le groupe de Weil s'obtient en prenant les éléments $\mathbf{A}_K^1 \subset \mathbf{A}_K^*$ de norme 1 :

$$\pi_1(\bar{X}, \bar{x})^{\mathrm{ab}} = \left(\prod_{v \notin S} \mathcal{O}_v^* \right) \backslash \mathbf{A}_K^1/K^*.$$

Preuve (du théorème 2.14).

• Soit $f(t) \in F^*$. On peut écrire $f(t) = at^m(1 + tg(t))$ avec m entier relatif et $g(t) \in \mathbf{F}_l[[t]]$, ce qui donne la décomposition

$$\mathbf{F}_l((t))^* \cong \mathbf{F}_l^* \times \mathbf{Z} \times (1 + t\mathbf{F}_l[[t]]).$$

Or le groupe $1 + t\mathbf{F}_l[[t]]$ quotienté par $1 + t^k\mathbf{F}_l[[t]]$ ($k \geq 1$) est isomorphe à l'ensemble des polynômes à coefficients dans \mathbf{F}_l de degré inférieur ou égal à $k - 1$. C'est un espace vectoriel de dimension finie sur \mathbf{F}_l , en particulier c'est un l -groupe.

⁶L'abélianisé G^{ab} d'un groupe topologique G vérifie la propriété universel : pour tout $G \rightarrow H$ morphisme de groupes continu, et H abélien, on a la factorisation continue $G^{\mathrm{ab}} \rightarrow H$. Explicitement, $G^{\mathrm{ab}} = G/[\overline{G}, G]$.

• C'est plus délicat. On prend l'abélianisé de la suite d'homotopie (théorème 2.7), donnant la suite exacte

:

$$\pi_1(\overline{X}, \overline{x})^{\text{ab}} \longrightarrow \pi_1(X, \overline{x})^{\text{ab}} \longrightarrow \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \longrightarrow 1.$$

Il reste à montrer que $\pi_1(\overline{X}, \overline{x})^{\text{ab}}$ a pour image le produit d'un groupe fini et d'un pro- p -groupe, ce que le lemme 2.16 implique (ce n'est pas immédiat). \square

Preuve de la conjecture 1 pour $n = 1$. Par le lemme, la pro- p partie de $\pi_1(X)^{\text{ab}}$ est tuée donc l'image géométrique est finie. \square

3 Méthodes automorphes sur les corps de fonctions

Cette section consiste en une large généralisation de la théorie du corps de classe. En effet, cette dernière donne une correspondance entre l'ensemble des caractères d'ordre fini associés au groupe de Galois G_K et le groupe des idéles \mathbf{A}_K^*/K^* (pour les groupes fondamentaux c'est un plus compliqué, comme nous l'avons vu en 2.3.3 dans le cas $n = 1$).

Dans le cas deux dimensionnel, la correspondance de Drinfeld énonce qu'à certaines représentations galoisiennes correspond une forme automorphe (cf. théorème 3.6). Le reste du travail peut donc s'effectuer « du côté automorphe ». Dans cette section, on rappelle que :

- k est un corps de caractéristique p ,
- X une courbe lisse, géométriquement connexe sur k ,
- K le corps de fonctions de X ,
- \mathbf{A}_k son anneau adélique, et
- \mathcal{O}_v est un anneau local, d'idéal maximal \mathfrak{m}_v . On note π_v une uniformisante,
- Λ un anneau noetherien dans lequel p admet un inverse. (e.g. \mathbf{Q}_l , ou $\mathbb{F}_l((t))$.)

3.1 Forme automorphe

On définit dans cette section les formes automorphes de degré 2. Puis des endomorphismes particulier sur l'espace de ces formes : les opérateurs de Hecke. Les formes automorphes d'intérêt seront les formes propres associées à ces opérateurs.

Définition 3.1. Une *forme automorphe*⁷ à coefficients dans Λ est une fonction

$$f : \text{GL}_2(\mathcal{O}) \backslash \text{GL}_2(\mathbf{A}_K) / \text{GL}_2(K) \longrightarrow \Lambda$$

vérifiant pour tout $x \in \text{GL}_2(\mathbf{A}_K)$:

$$\int_{z \in \mathbf{A}_K/K} f(xb(z)) dz = 0, \quad \text{où } b(z) = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}. \quad (3.1)$$

Explicitons cette définition. Le double quotient dénote les deux invariances sur $x \in \text{GL}_2(\mathbf{A}_K)$: $f(x\gamma) = f(x)$ pour $\gamma \in \text{GL}_2(K)$ et $f(ux) = f(x)$ pour $u \in \text{GL}_2(\mathcal{O})$.

⁷C'est plus justement une forme automorphe non-ramifiée parabolique. Le texte ne traitant que de celle-ci, on omet cette précision.

L'ensemble $\mathrm{GL}_2(\mathcal{O})x$ est un ouvert de $\mathrm{GL}_2(\mathbf{A}_K)$ pour $x \in \mathrm{GL}_2(\mathbf{A}_K)$. Une forme automorphe est donc localement constante et continue, de même que l'intégrande de (3.1). Or par invariance par translation de $K : f(xb(z)) = f(xb(z+k))$ de sorte qu'intégrer sur le groupe topologique compact \mathbf{A}_K/K est licite (implicitement est utilisée l'existence de la mesure de Haar normalisée dz sur \mathbf{A}_K/K).

Enfin, $\int_U dz \in p^Z$ si U est ouvert. Or Λ est une $\mathbb{Z}\left[\frac{1}{p}\right]$ -algèbre et l'intégration de $f(xb(\cdot))$ est bien définie.

3.2 Opérateurs de Hecke

Définition 3.2. Soit v une place de X et f une forme automorphe, on appelle l'opérateur de Hecke associé à la place v l'endomorphisme

$$(T_v f)(x) := \int_{g \in M_v} f(g^{-1}x) dg,$$

et l'homothétie

$$(U_v f)(x) := f\left(\begin{pmatrix} \pi_v^{-1} & 0 \\ 0 & \pi_v^{-1} \end{pmatrix} x\right),$$

où $M_v \subset M_2(\mathcal{O}_v)$ est l'ensemble des matrices g à déterminant dans $\pi_v \mathcal{O}_v^*$, et dg l'intégrale de Haar sur $\mathrm{GL}_2(K_v)$ normalisé sur le sous-groupe compact $\mathrm{GL}_2(\mathcal{O}_v)$.

Proposition 3.3. Les opérateurs de Hecke sont bien définis : $T_v f$ est une forme automorphe. On le voit avec l'expression :

$$(T_v f)(x) = f\left(\begin{pmatrix} \pi_v^{-1} & 0 \\ 0 & 1 \end{pmatrix} x\right) + \sum_{0 \leq i \leq q_v} f\left(\begin{pmatrix} 1 & 0 \\ -\lambda_i \pi_v^{-1} & \pi_v^{-1} \end{pmatrix} x\right)$$

où q_v est le cardinal du corps résiduel $\kappa_v := \mathcal{O}_v/(\pi_v)$, et λ_i des représentants de κ_v dans \mathcal{O}_v .

Preuve. On écrit toute matrice $g \in M_v$ comme un produit $g_1 d g_2$ avec g_1, g_2 triangulaires inférieure et supérieure et d diagonale (décomposition de Bruhat). Les propriétés d'invariance de f permettent d'obtenir la formule ci-dessus. \square

Définition 3.4. Une forme automorphe f sera dite *propre* si f prend une valeur inversible dans Λ et si on dispose de $(t_v), (u_v)$ dans Λ tels que

$$T_v f = t_v f \quad \text{et} \quad U_v f = u_v f \quad \text{pour tous } v.$$

Remarque. Dans une démarche qui n'est pas celle de ce texte (cf. section 2.3.1), on peut former une algèbre de Hecke engendré par des opérateurs de Hecke et homothéties en des places choisies.

Soit enfin le Λ -module des formes propres à valeurs propres prescrites :

$$\mathcal{C}(\Lambda) = \{f \text{ forme automorphe telle que } U_v f = q_v^{-1} f \text{ pour tous } v.\}$$

Les opérateurs de Hecke se transportent en endomorphismes Λ -linéaires de $\mathcal{C}(\Lambda)$.

Définition 3.5. Soit $f \in \mathcal{C}(\Lambda)$. Les valeurs propres des homothéties U_v sont des unités de Λ . Le caractère central associé à f est le morphisme

$$\begin{aligned} \chi_f : \quad \mathcal{O}^* \backslash \mathbf{A}_K^* / K^* &\longrightarrow \Lambda^* \\ (1, \dots, 1, \pi_v, 1, \dots) &\longmapsto u_v^{-1}, \end{aligned}$$

bien défini par invariance de f .

3.3 Réciprocité de Drinfeld

Nous sommes en mesure d'énoncer, sans démonstration, le théorème de Drinfeld ([7], Theorem 4.9) pour les corps de fonctions.

Théorème 3.6 (Réciprocité de Drinfeld). *Soit $l \neq p$ et une représentation continue $\pi_1(X) \longrightarrow \mathrm{GL}_2(\mathbf{F}_l((t)))$ telle que*

1. $\det(\rho)$ est trivial,
2. $\rho|_{\pi_1(\overline{X})}$ est absolument irréductible.

Alors il existe une forme propre $f \in \mathcal{C}(\Lambda)$ telle que $t_v = \mathrm{Tr} \rho(\mathrm{Fr}_v)$.

On termine par le théorème de Lafforgue, utilisé à la fois dans la construction de l'isomorphisme entre l'algèbre de Hecke et l'anneau de déformation universel par Böckle et Khare [2] et dans la preuve générale de Gaitsgory [6]. Il a en outre permis de démontrer la conjecture de Deligne complète mentionnée en historique 2.3.1 :

Théorème 3.7 (Lafforgue, [8]). *Soit K le corps de fonction de X de caractéristique $p > 0$. On a une bijection σ entre*

1. les classes d'équivalences de représentations « paraboliques » π de $\mathrm{GL}_n(K)$, et
2. les classes d'équivalences de représentations irréductibles $\sigma(\pi) : G_K \longrightarrow \mathrm{GL}_n(\overline{\mathbf{Q}}_l)$.

Cette bijection respecte les constructions des fonctions $L : L_v(\pi, s) = L_v(\sigma(\pi), s)$ pour toute place finie $v \in X$ et s complexe.

4 Traduction et algébricité des valeurs propres : fin de la démonstration

En section 2.3, on a traduit la conjecture de de Jong par la finitude de $R_{X,\overline{\rho}}$ en tant que \mathbf{Z} -module. On donne plus bas une autre interprétation de la conjecture.

Plus précisément, c'est le caractère algébrique des éléments $\mathrm{Tr}(\rho(\mathrm{Fr}_v))$ qui est impliqué. Ce dernier point peut à présent être établi du côté automorphe, et la réciprocité de Drinfeld (théorème 3.6) nous permettra de conclure.

4.1 Reformulation algébrique de la conjecture

Rappelons que X est une courbe lisse et projective sur \mathbf{F}_p et $\rho : \pi_1(X) \longrightarrow \mathrm{GL}_n(F) = \mathrm{GL}(V)$.

Proposition 4.1. *Soient X et ρ comme dans la conjecture de de Jong 1. On a l'équivalence :*

- (i) $\rho(\pi_1(\overline{X}))$ est fini,
- (ii) Pour toute place finie v de X , le polynôme caractéristique de $\rho(\mathrm{Fr}_v)$ est à coefficients dans \mathbf{F}_l .

Preuve. Supposons (i), alors $\rho(\mathrm{Fr}_v)$ est d'ordre fini dans $\mathrm{GL}(V)$. Donc ses valeurs propres sont algébriques sur \mathbf{F}_l . Or tout élément non-constant de F est transcendant, donc les valeurs propres sont dans \mathbf{F}_l . Par somme et produit, les coefficients du polynôme caractéristique de $\rho(\mathrm{Fr}_v)$ sont dans \mathbf{F}_l aussi.

Réciproquement, supposons (ii). On considère pour $i \leq \dim V$ les fonctions continues

$$f_i : \pi_1(X) \longrightarrow \Lambda^*$$

$$\gamma \longmapsto \mathrm{Tr} \left(\rho(\gamma), \bigwedge^i V \right).$$

où l'élément $\text{Tr}(\cdot, \wedge^i V)$ est la trace de ρ transportée en la représentation $\rho_i : \pi_1(X) \longrightarrow \text{GL}(\wedge^i V)$ ⁸. Par hypothèse, les f_i appliquée en tout frobenius Fr_v sont à valeurs dans F_l . Or par le théorème de Cebotarev, les Fr_v sont denses dans $\pi_1(X)$. Par conséquent, toutes les f_i sont à valeurs dans F_l , donc localement constantes.

On dispose donc d'un sous groupe ouvert $H \leq \pi_1(X)$ tel que les f_i soient constantes sur H , de valeurs $\text{Tr}(\mathbf{1}_V, \wedge^i V)$. Pour $b \in H$, $\rho(b)$ à donc même polynôme caractéristique que l'identité de $V : (X - 1)^{\dim V}$. On en déduit que $\rho(b)$ est unipotente.

Il suffit de montrer que $\rho(H)$ est fini. En effet, $\pi_1(X)$ est compact de sorte qu'un nombre fini d'ouverts γH suffisent à recouvrir $\pi_1(X)$. On mentionne seulement comment conclure : un argument cohomologique montre que le pro- l -quotient maximal H^l à un nombre de générateurs (topologiques) fini, son image par ρ est alors un pro- l -groupe nilpotent, finiment engendré. Elle est finie et $\rho(H) = \rho(H^l)$ aussi. \square

4.2 Du côté automorphe

Terminons cette section par deux lemmes fondamentaux du côté automorphe : l'un sur la finitude de $\mathcal{C}(\Lambda)$, l'autre sur l'algébricité des valeurs propres des opérateurs de Hecke.

Lemme 4.2. *Le Λ -module $\mathcal{C}(\Lambda)$ est finiment engendré. Si de plus Λ est un corps, et $F \subset \Lambda$ désigne son corps premier, alors*

$$\mathcal{C}(F) \otimes_F \Lambda \cong \mathcal{C}(\Lambda),$$

et cet isomorphisme commute aux opérateurs de Hecke.

Remarque. On est forcé d'admettre le lemme 4.2 sans (de nouveau...) introduire un dictionnaire entre $\text{GL}_2(\mathcal{O}) \backslash \text{GL}_2(\mathbf{A}_K) / \text{GL}_2(K)$ et des classes d'isomorphismes de faisceaux localement libres de rang 2 sur X .

Théorème 4.3. *Soit $f \in \mathcal{C}(\Lambda)$ de caractère central $q^{\deg(-)}$. Alors les valeurs propres t_v sont algébriques de degré uniformément borné : il existe une extension finie E de F tel que $t_v \in E$ pour toute v .*

Avant de démontrer l'énoncé 4.3, concluons la démonstration de la conjecture de de Jong. On pose $\Lambda = F = F_l((t))$, et pour appliquer la correspondance de Drinfeld, $n = 2$.

Preuve de la conjecture 1 pour $n = 2$. Soit $f \in \mathcal{C}(\Lambda)$ la forme propre associée à la représentation $\rho : \pi_1(X) \longrightarrow \text{GL}_2(F_l((t)))$ d'un couple (X, ρ) comme en proposition 2.13.

Il suffit d'après la proposition 4.1 d'obtenir l'algébricité des valeurs propres $t_v = \text{Tr} \rho(\text{Fr}_v)$. Mais le caractère central est par la condition $u_v = q_v^{-1}$ tel que le théorème 4.3 s'applique. Par conséquent, $\rho(\pi_1(\bar{X}))$ est fini. \square

Preuve du théorème 4.3. Supposons le lemme précédent démontré : l'application $\mathcal{C}(F_l) \longrightarrow \mathcal{C}(F)$ induit un isomorphisme par extension des scalaires. Par compatibilité, un opérateur de Hecke T_v sur provient d'un opérateur $\mathcal{C}(F_l) \rightarrow \mathcal{C}(F_l)$. Or $\mathcal{C}(F)$ est un F -espace vectoriel de dimension finie, donc $\mathcal{C}(F_l)$ est un F_l -espace vectoriel de dimension finie. Ainsi les valeurs propres des T_v sont algébriques de degré au plus $[\mathcal{C}(F_l) : F_l]$. \square

5 Épilogue

Après avoir terminé ce rapport début juillet, je m'essaye de nouveau à une lecture de *Modular Forms and Fermat's Last Theorem* [4]. Si de nombreux éléments techniques me manquent encore, au moins le brouillard de ma première lecture s'est complètement dissipé.

⁸Les images d'un élément γ en les f_i sont au signe près les coefficients du polynôme caractéristique de $\rho(\gamma)$.

A Schémas, courbes

Dans cet appendice, tous les anneaux seront supposés commutatifs et intègres. k est un corps parfait, de caractéristique p et \bar{k} dénote une clôture algébrique de k .

La notion de schéma généralise la notion de variété algébrique aussi bien que celle d'espace topologique. De même qu'une variété différentielle est localement modélée sur l'espace \mathbf{R}^n ou \mathbf{C}^n , un schéma est localement modélée sur un ensemble beaucoup plus vaste d'espaces.

Définition A.1. Soit A un anneau, le spectre de A est l'espace topologique $\text{Spec } A$ dont les points sont les idéaux premiers de A . Une base d'ouverts est donnée par $D(f) = \{\mathfrak{p} \in \text{Spec } A, f \notin \mathfrak{p}\}$. En particulier c'est un point si A est un corps.

La « structure différentielle » du schéma nécessite plus que l'espace topologique de base :

Définition A.2. Le couple (X, \mathcal{O}_X) est un *espace localement annelé* si X est un espace topologique et \mathcal{O}_X un faisceau d'anneaux commutatifs, i.e. :

- (i) \mathcal{O}_X est un foncteur contravariant de $\text{Ouv}(X)$ dans \mathbf{Ann} : pour tout $U \in \text{Ouv}(X)$ ouvert de X , $\mathcal{O}_X(U)$ est un anneau, tel que ce foncteur soit compatible à l'inclusion.
- (ii) De plus, les sections locales se recollent uniquement. Plus précisément, pour $U = \bigcup U_i$ un recouvrement par des ouverts, la suite est exacte :

$$\begin{array}{ccc} \mathcal{O}_X(U) & \longrightarrow & \bigcup_i \mathcal{O}_X(U_i) & \longrightarrow & \bigcup_{i,j} \mathcal{O}_X(U_i \cap U_j) & \longrightarrow & 0 \\ s & \longmapsto & (s|_{U_i})_i & ; & (s_i) & \longmapsto & (s_i|_{U_i \cap U_j} - s_j|_{U_i \cap U_j}). \end{array}$$

- (iii) Le germe $\mathcal{O}_{X,x} = \lim_{x \in U \in \text{Ouv}(X)} \mathcal{O}_X(U)$ est un anneau local.

Définition A.3. Un schéma (X, \mathcal{O}_X) est un espace localement annelé, tel que tout point $x \in X$ admet un voisinage ouvert affine, i.e. de la forme $\text{Spec } A$.

Un schéma est de *type fini* sur k si en tout point, un voisinage affine $\text{Spec } R$ existe avec A de type fini sur k : on dispose de $n > 0$ et I un idéal de $k[X_1, \dots, X_n]$ tels que $A \cong k[X_1, \dots, X_n]/I$.

On définit le cadre algébrique des courbes, que l'on supposera irréductible et projective.

Définition A.4. Une courbe algébrique X est un type particulier de schéma :

1. X est de type fini sur k ,
2. X est de dimension 1, c'est à dire que la dimension de Krull des anneaux de type fini A sont ≤ 1 .

Si de plus X est supposé irréductible, on obtient les composantes de bases d'une courbe algébrique :

Proposition A.5. Une courbe irréductible plane X sur k est la donnée d'un polynôme irréductible $P \in k[X, Y]$ tel que $\mathcal{C} = \text{Spec}(k[X, Y]/P(X, Y))$.

Le texte ne parle que de courbe projective : on peut toujours s'y ramener par normalisation. Les composantes irréductible sont alors la donnée d'un polynôme irréductible homogène $P \in k[X, Y, Z]$ tel que $\mathcal{C} = \text{Spec}(k[X, Y, Z]/P(X, Y, Z))$.

Soit X une courbe irréductible projective. Son corps de fonction $k(X, Y, Z)/P$ est une extension de type fini de k , de degré de transcendance 1. Réciproquement, une telle extension donne lieu à une courbe projective irréductible :

Théorème A.6. Pour toute extension K de k de type fini et de degré de transcendance 1, on lui associe la courbe projective irréductible $\mathcal{X}_K = \{\text{valuations } v : K \rightarrow \mathbf{Z} \cup \infty\}$, munie de la topologie cofinie.

B Construction du groupe fondamental arithmétique

Rappelons que tout schéma est recouvert par une collection de schémas affines. Pour la lisibilité, les définitions qui suivent se place dans le cas affine.

B.1 Morphismes étales

Définition B.1. Un morphisme d'anneaux $f : A \rightarrow B$ est dit *fini étale* si

- (i) B est un A -module plat et finiment engendré,
- (ii) Pour tout $\mathfrak{p} \in \text{Spec } A$, on a un isomorphisme de $\kappa(\mathfrak{p})$ -algèbre :

$$B \otimes \kappa(\mathfrak{p}) \cong K_1 \times \dots \times K_r,$$

où les K_i sont des extensions séparable finie de $\kappa(\mathfrak{p})$.

Soit A un anneau intégralement clos et F sont corps de fraction.

Définition B.2. Une A -algèbre B est dite *fini étale* et *connexe* s'il existe une extension finie séparable de F telle que

- (i) B est la clôture intégrale de A dans K ,
- (ii) L'inclusion $A \hookrightarrow B$ est fini étale.

Une A -algèbre *fini étale* est isomorphe à un produit finie de A -algèbres finies étales connexes.

Elle est de plus dite de *Galois* si K/F est une extension galoisienne de corps. On note $\text{Aut}(B/A)$ le groupe des automorphismes de A -algèbre de B . Si B est de Galois, alors $\text{Aut}(B/A) = \text{Gal}(K/F)$.

Exemple B.3. Notons $\text{Fét}(A)$ (resp. $\text{Fét}_c(A)$) la catégorie des A -algèbres finies étales (resp. connexes). On décrit cette catégorie (à isomorphisme près) dans les cas suivants :

1. A est un corps k . On obtient les extensions finies séparables de k .
2. A est un anneau de valuation discrète complet ; κ_A son corps résiduel κ . Alors $B \in \text{Fét}(A)$ est aussi de valuation discrète complet, et κ_B/κ_A est une extension séparable finie. Pour $A = \mathbb{Z}_p$, on en déduit $\text{Fét}_c(\mathbb{Z}_p) = \{\mathbb{W}(\mathbb{F}_{p^n}), n \geq 1\}$.
3. A est un anneau de Dedekind. Si F désigne son corps de fractions, et K le corps de fraction d'une A -algèbre B ,

B est fini étale connexe si et seulement si K est une extension non ramifiée de F .

Définition B.4. Soit $X = \text{Spec } A$ un schéma affine. Un morphisme de schémas $\phi : Y \rightarrow X$ est *fini étale* s'il existe $B \in \text{Fét}(A)$ tel que $Y = \text{Spec } B = \bigsqcup_i \text{Spec } B_i$ et $A \hookrightarrow B$ induit ϕ . On pose auquel cas $\text{Aut}(Y/X) = \text{Aut}(B/A)$.

B.2 Le groupe fondamental — enfin !

Soit $x \in X$ correspondant à un idéal premier \mathfrak{p} . Son germe est un anneau local et donne lieu à un morphisme $x : \text{Spec } \kappa(\mathfrak{p}) \rightarrow X$. Le *point géométrique* associé à x est un morphisme $\bar{x} : \text{Spec } \kappa(\Omega) \rightarrow X$, où Ω est une clôture algébrique de $\kappa(\mathfrak{p})$.

On peut définir le foncteur fibre en un point géométrique \bar{x} . Soit $\phi : Y \rightarrow X$ un morphisme fini étale,

$$\begin{aligned} F_{\bar{x}}(Y) &:= \{\bar{y} : \text{Spec } \Omega \rightarrow Y, \phi \circ \bar{y} = \bar{x}\} \\ &= \text{Hom}_{A\text{-alg}}(B, \Omega). \end{aligned}$$

Soit $\psi : Y \rightarrow Y'$ un morphisme dans $\text{Fét}(X)$ (on impose donc $\psi \circ (Y \rightarrow X) = (Y' \rightarrow X)$).⁹ Alors

$$\begin{aligned} F_{\bar{x}}(\psi) : F_{\bar{x}}(Y) &\longrightarrow F_{\bar{x}}(Y') \\ \bar{y} &\longmapsto \psi \circ \bar{y} \end{aligned}$$

Remarque. Comme dans le cadre topologique, $Y \rightarrow X$ dans $\text{Fét}(X)$ sera dit galoisien si l'action de $\text{Aut}(Y/X)$ sur $F_{\bar{x}}(Y)$ est transitive et fidèle.

Théorème B.5. On dispose d'un système projectif $((Y_i \rightarrow X, \bar{y}_i), \phi_{ij})$ de revêtements finis étales galoisiens pointés tel que pour tout $Y \in \text{Fét}(X)$, on ait

$$\varprojlim_i \mathcal{C}_X(Y_i, Y) \cong F_{\bar{x}}(Y),$$

le foncteur fibre en \bar{x} est pro-représentable.

Définition B.6. Soit X un schéma, on définit son groupe fondamental arithmétique, ou étale, comme $\text{Aut}(F_{\bar{x}})$. Grâce au théorème précédent, on a explicitement :

$$\pi_1(X, \bar{x}) = \varprojlim_i \text{Gal}(Y_i/X),$$

où la limite projective est prise respectivement à

$$\text{Gal}(Y_j/X) \cong F_{\bar{x}}(Y_j) \xrightarrow{F_{\bar{x}}(\phi_{ij})} F_{\bar{x}}(Y_i) \cong \text{Gal}(Y_i/X).$$

Remarque. La structure de groupe $\pi_1(X, \bar{x})$ ne dépend pas du point de base \bar{x} , à isomorphisme (non-canonique) près ; on s'autorise à l'omettre.

Exemple B.7. Reprenons les exemples donnés en B.3 :

1. A est un corps k . On a donné dans le texte le groupe fondamental du corps fini F_q . Plus généralement,

$$\pi_1(\text{Spec } k, \text{Spec } \bar{k}) = \varprojlim_{K/k \text{ finie galoisienne}} \text{Gal}(K/k) = G_k.$$

2. A est un anneau de valuation discrète complet. La donnée de $B \in \text{Fét}(A)$ est la donnée de son corps de fraction. Ces derniers forment un système projectif I pour la composition de corps. On définit $\tilde{F} = \varprojlim_{i \in I} K_i$ la composée de tous ces corps ; l'extension maximale non ramifiée de F . Alors

$$\pi_1(\text{Spec } A, \bar{x}) = \varprojlim_i \text{Gal}(K_i/F) = \text{Gal}(\tilde{F}/F).$$

3. Toute extension algébrique K/\mathbb{Q} stricte se ramifie en un premier divisant le discriminant Δ_K (qui n'est pas trivial par le théorème de Minkowski.) Par conséquent, $\pi_1(\text{Spec } \mathbb{Z}) = \{1\}$.
4. Soit E une courbe elliptique définie sur \mathbb{Q} , alors $E \xrightarrow{xn} E$, pour $n \geq 1$ forme un système projectif et

$$\pi_1(E) \cong \varprojlim_n E[n] =: T(E).$$

B.3 Le groupe de Galois absolu de $\mathbb{C}(t)$

Ce dernier énoncé nous renseigne sur $\text{Gal}(\overline{\mathbb{C}(t)}/\mathbb{C}(t))$:

Définition B.8. Soit X une surface de Riemann compacte connexe et $X' = X - S$ où S est un ensemble fini. On note \mathcal{C}_X l'ensemble des surfaces de Riemann compactes connexes Y munie d'un morphisme $Y \xrightarrow{\phi} X$, qui est un revêtement topologique une fois restreint à

$$Y - \phi(S) \longrightarrow X'.$$

⁹On note $\mathcal{C}_{\bar{x}}(Y, Y')$ l'ensemble de tels morphismes.

Lemme B.9. Soit X une surface de Riemann compacte connexe et $X' = X - S$ où S est un ensemble fini. Soit $K_{X'}$ le corps composé des corps de fonctions $\mathcal{M}(Y)$ pour Y dans \mathcal{C}_X . Alors par le théorème 2.8,

$$\text{Gal}(K_{X'}/\mathcal{M}(X)) = \widehat{\pi_1^{\text{top}}}(X', x).$$

Lemme B.10. On a une équivalence de catégories entre :

- les extensions finies $\mathcal{M}(X) \subset K \subset \overline{\mathcal{M}(X)}$,
- les surfaces de Riemann compactes connexes Y munies d'un morphisme $Y \rightarrow X$ fini galoisien et de corps de fonction $\mathcal{M}(Y) = K$.

Le lemme B.9 amène :

$$\text{Gal}(\overline{\mathcal{M}(X)}/\mathcal{M}(X)) = \lim_{X' \subset X} \widehat{\pi_1^{\text{top}}}(X', x).$$

Corollaire B.11. En particulier, $\mathbf{C}(t)$ est le corps de fonction de $\mathbf{P}^1(\mathbf{C})$. Si $S \in \mathbf{P}^1(\mathbf{C})$ est fini de cardinal $n + 1$, le groupe fondamental de $X - S$ est le groupe libre à n générateur F_n . Ainsi le lemme B.10 implique la description

$$\text{Gal}(\overline{\mathbf{C}(t)}/\mathbf{C}(t)) = \lim_n \widehat{F}_n \cong \widehat{F(\mathbf{C})}$$

où le dernier isomorphisme est donné par un théorème de A. Douady.

Remarque. La description du groupe de Galois absolue est complète. Nous voyons en particulier que tout sous-groupe fini est un quotient de $G_{\mathbf{C}(t)}$, ce qui est loin d'être connu pour $G_{\mathbf{Q}}$.

Donnons un dernier aperçu de la profondeur des théorèmes principaux 2.7 et 2.8. D'une part le groupe $G_{\mathbf{Q}}$ et d'autre part $G_{\mathbf{C}(t)}$: qu'en est-il de $G_{\mathbf{Q}(t)}$? La suite homotopique donne une réponse partielle :

Proposition B.12. La suite exacte de 2.7 appliquée à $X = \mathbf{P}^1(\mathbf{Q})$ s'écrit

$$1 \longrightarrow \widehat{F(\mathbf{C})} \longrightarrow G_{\mathbf{Q}(t)} \longrightarrow G_{\mathbf{Q}} \longrightarrow 1.$$

La compréhension du groupe de Galois absolu de $\mathbf{Q}(t)$ revient à la description de cette suite exacte, ce qui est l'objet de la conjecture des sections de Grothendieck.

C Cadre adélique

Soit K un corps global, c'est-à-dire une extension finie de \mathbf{Q} ou de $\mathbf{F}_q(t)$ où \mathbf{F}_q est un corps fini. Les nombres premiers sur \mathbf{Q} ont pour analogues les places de K : une classe d'équivalence de valuations sur le corps K . Chaque place permet de compléter K en un corps noté K_v .

Exemple C.1. Si $K = \mathbf{Q}$, le théorème d'Ostrowski décrit l'ensemble des valuations de \mathbf{Q} : elles sont, à équivalence près, soit ultramétriques $x \mapsto |x|_p = p^{-v_p(x)}$, soit archimédienne $x \mapsto |x|$ la valeur absolue usuelle. Les corps obtenus après complétion sont respectivement les nombres p -adiques \mathbf{Q}_p et \mathbf{R} .

Soit v une place non-archimédienne de K , on note \mathcal{O}_v l'ensemble des éléments de K tel que $v(x) \leq 1$. C'est aussi l'anneau des entiers¹⁰ de K_v . Une adèle, c'est une collection (x_v) d'éléments de $\prod_v K_v$ tels que tous sauf un nombre fini sont entiers, c'est à dire dans $\mathcal{O}_v \subset K_v$. Plus formellement :

Définition C.2. L'anneau des adèles sur K est le produit restreint respectivement à $\{\mathcal{O}_v\}$ des K_v . On le note $\mathbf{A}_K = \prod'_v K_v$.

Son anneau des entiers est défini par $\mathcal{O} = \prod_v \mathcal{O}_v$.

¹⁰Si v est archimédienne, on pose $\mathcal{O}_v = K_v$.

Exemple C.3. Pour $K = \mathbf{Q}$,

$$\mathbf{A} = \mathbf{R} \cdot \prod_p \mathbf{Q}_p.$$

L'anneau des entiers de \mathbf{Q} en p est \mathbf{Z}_p , et \mathbf{R} sinon.

Remarque. ◦ On muni \mathbf{A}_K d'une topologie donnée par la base d'ouvert $\prod_{v \in \mathcal{S}} U_v \cdot \prod_{v \notin \mathcal{S}} \mathcal{O}_v$ où $U_v \subset K_v$ est un ouvert et \mathcal{S} fini.

- Munies de cette topologie, les adèles forment un groupe topologique localement compact (pour ces constructions et plus, cf. la thèse de Tate (1950), chap. 3 [10], et l'ouvrage de Weil [11]). Notons que la topologie produit restreinte à \mathbf{A}_K ne coïncide pas à celle construite au point précédent.
- K se plonge dans \mathbf{A}_K par $x \mapsto (x, x, \dots)$ ($K \subset \mathcal{O}_v$ pour toute place v), et \mathbf{A}_K/K est alors un groupe compact.

Soit v non-archimédienne. L'anneau des entiers $\mathcal{O}_v = \{x \in K, v(x) \leq 1\}$ est local, d'idéal maximal $\mathfrak{m}_v = \{x \in K, v(x) < 1\}$. Notons $\kappa(v) = \mathcal{O}_v/\mathfrak{m}_v$ son corps résiduel.

Définition C.4 (Frobénius sur X). La place $v \in X$ donne lieu à un morphisme $\text{Spec } \kappa(v) \longrightarrow X$ (d'image v dans X). On en déduit une flèche

$$\pi_1(\text{Spec } \kappa(v)) \longrightarrow \pi_1(X). \tag{C.1}$$

D'après la remarque 1.1, on a un élément distingué générant topologiquement $\pi_1(\text{Spec } \kappa(v)) = \text{Gal}(\overline{\kappa(v)}/\kappa(v)) \cong \hat{\mathbf{Z}}$. Soit $\text{Fr}_v \in \pi_1(X)$ son image via (C.1), le *frobénius* associée à la place finie v .

References

- [1] Gebhard Böckle, Ashwin Iyengar, and Vytautas Paškūnas. *On local Galois deformation rings*. 2021. arXiv: [2110.01638](https://arxiv.org/abs/2110.01638).
- [2] Gebhard Boeckle and Chandrashekhara Khare. *Mod ℓ representations of arithmetic fundamental groups II (A conjecture of A.J. de Jong)*. 2004. eprint: [math/0312490](https://arxiv.org/abs/math/0312490).
- [3] Gebhard Boeckle and Chandrashekhara Khare. *Mod ℓ representations of arithmetic fundamental groups: Part I (An analog of Serre's conjecture for function fields)*. 2004. arXiv: [math/0312489](https://arxiv.org/abs/math/0312489).
- [4] Gary Cornell, Joseph H. Silverman, and Glenn Stevens, eds. *Modular Forms and Fermat's Last Theorem*. Springer, New York, 1997.
- [5] Pierre Deligne. “La conjecture de Weil : II”. fr. In: *Publications Mathématiques de l'IHÉS* 52 (1980), pp. 137–252.
- [6] Dennis Gaitsgory. *On de Jong's conjecture*. 2006. arXiv: [math/0402184](https://arxiv.org/abs/math/0402184).
- [7] A. J. de Jong. *A conjecture on arithmetic fundamental groups*. 2001. DOI: <https://doi.org/10.1007/BF02802496>.
- [8] Laurent Lafforgue. *Chtoucas de Drinfeld et conjecture de Ramanujan-Petersson*. Astérisque 243. Société mathématique de France, 1997.
- [9] Barry Mazur. “Deforming Galois Representations”. In: *Galois Groups over \mathbf{Q}* . Springer, New York, 1989, pp. 385–437.
- [10] John Tate. “Fourier analysis in number fields, and Hecke's zeta-functions”. In: *Algebraic Number Theory*. Ed. by A. Fröhlich and John W. S. Cassels. Academic Press, 1967, pp. 305–348.
- [11] André Weil. *Basic Number Theory*. Classics in Mathematics. Springer Berlin Heidelberg, 1974. ISBN: 9783540586555.
- [12] Andrew Wiles. “Modular elliptic curves and Fermat's Last Theorem”. In: *Annals of Mathematics* 141 (1995), pp. 443–551.