Structures logarithmiques et modules galoisiens

Jean Gillibert

Arithmetic of Curves and Covers

22 novembre 2007

Structure galoisienne classique

K un corps de nombres

L/K une extension galoisienne finie de K, de groupe Γ

Théorème de la base normale : Il existe $\alpha \in L$ tel que l'ensemble $\{\sigma(\alpha)\}_{\sigma\in\Gamma}$ des conjugués de α soit une base de L en tant que K-espace vectoriel. C'est-à-dire que L est un $K[\Gamma]$-module libre de rang 1.

$\mathcal{O}_K$ et $\mathcal{O}_L$ les anneaux d'entiers de K et L.

Question (Hilbert) : Quelle est la structure de $\mathcal{O}_L$ en tant que $\mathcal{O}_K[\Gamma]$-module ?

Critère de Nœther : $\mathcal{O}_L$ est un $\mathcal{O}_K[\Gamma]$-module localement libre si et seulement si L/K est modérément ramifiée.

Le cas modéré

$\mathrm{Cl}(\mathbb{Z}[\Gamma]) := K_0(\mathbb{Z}[\Gamma])/\{\text{libres}\}$ le groupe des classes loc. libres
Si M est un $\mathbb{Z}[\Gamma]$-module loc. libre, soit (M) sa classe dans $\mathrm{Cl}(\mathbb{Z}[\Gamma])$

La conjecture de Fröhlich, prouvée par M. J. Taylor :

Théorème (M. J. Taylor, 1981) : Supposons L/K modérée, alors $2(\mathcal{O}_L) = 0$. En outre, si les constantes d'Artin des caractères irréductibles et symplectiques de Γ sont toutes égales à 1, alors $(\mathcal{O}_L) = 0$.

– Quelle est la structure galoisienne *relative* (structure de $\mathcal{O}_L$ en tant que $\mathcal{O}_K[\Gamma]$-module) ?

– Que se passe-t-il dans le cas des extensions *sauvagement* ramifiées ?

Approche schématique

$S := \mathrm{Spec}(\mathcal{O}_K)$ le spectre de l'anneau des entiers de K
G un S-schéma en groupes *commutatif*, fini et plat

Les G-torseurs (pour la topologie fppf sur S) sont des « extensions galoisiennes de groupe G ».

$H^1(S, G) := \{$classes d'isomorphie de G-torseurs sur $S\}$
c'est un groupe abélien.

Exemple : Si $G = \Gamma_S$ est un groupe constant, alors

$H^1(S, \Gamma_S) = \{\mathrm{Spec}(\mathcal{O}_L) \to S$ où L/K est une K-algèbre galoisienne de groupe Γ, partout non ramifiée$\}$

En général, les seuls premiers de $\mathcal{O}_K$ en lesquels un G-torseur est (éventuellement) ramifié sont ceux divisant l'ordre de G.

Structure galoisienne des torseurs

G^D le dual de Cartier de G

(W. Waterhouse, 1971). On dispose d'un homomorphisme

$$\pi : H^1(S,G) \xrightarrow{\sim} \mathrm{Ext}^1(G^D, \mathbf{G}_{\mathrm{m}}) \longrightarrow \mathrm{Pic}(G^D)$$

La première flèche est un isomorphisme déduit de la suite locale-globale pour les Ext^n
La deuxième flèche est l'application naturelle

On dit que π mesure la structure galoisienne des G-torseurs.

Dans le cas où $G = \Gamma_S$, le morphisme π est donné par

$$\begin{aligned} \pi : H^1(S, \Gamma_S) &\longrightarrow \mathrm{Pic}(\Gamma_S^D) \simeq \mathrm{Cl}(\mathcal{O}_K[\Gamma]) \\ (\mathrm{Spec}(\mathcal{O}_L) \to S) &\longmapsto (\mathcal{O}_L) \end{aligned}$$

(on retrouve le cas non ramifié de la théorie classique).

Isogénies et torseurs sur K

A_K une variété abélienne définie sur K
$G_K \subseteq A_K$ un sous-schéma en groupes fini de A_K

On a une suite exacte

$$0 \longrightarrow G_K \longrightarrow A_K \xrightarrow{\phi} B_K \longrightarrow 0$$

où B_K est une variété abélienne. La suite duale est

$$0 \longrightarrow G_K^D \longrightarrow B_K^t \xrightarrow{\phi^t} A_K^t \longrightarrow 0$$

Le cobord de la suite exacte ci-dessus est un morphisme

$$\delta_K : A_K^t(K) \longrightarrow H^1(\mathrm{Spec}(K), G_K^D)$$

Soit $P \in A_K^t(K)$ un point. Alors $\delta_K(P)$ est le spectre d'une K-algèbre, dont on aimerait déterminer la structure galoisienne de l'anneau d'entiers.

Cas de bonne réduction

$\mathcal{A}$, $\mathcal{A}^t$, $\mathcal{B}$ et $\mathcal{B}^t$ les modèles de Néron (sur S) de A_K, A_K^t, B_K, B_K^t
Supposons que A_K ait partout bonne réduction
Alors $\mathcal{A}$ est un S-schéma abélien et l'adhérence schématique de G_K dans $\mathcal{A}$ est un sous-groupe fini et plat $G \subseteq \mathcal{A}$.
De plus, le quotient $\mathcal{A}/G$ est isomorphe à $\mathcal{B}$, et nous avons des suites exactes

$$0 \longrightarrow G \longrightarrow \mathcal{A} \xrightarrow{\phi} \mathcal{B} \longrightarrow 0$$

$$0 \longrightarrow G^D \longrightarrow \mathcal{B}^t \xrightarrow{\phi^t} \mathcal{A}^t \longrightarrow 0$$

En composant le cobord de cette dernière avec π on obtient le class-invariant homomorphism (défini par M. J. Taylor en 1988)

$$\psi : A_K^t(K) = \mathcal{A}^t(S) \xrightarrow{\delta} H^1(S, G^D) \xrightarrow{\pi} \mathrm{Pic}(G)$$

Ainsi tout $P \in A_K^t(K)$ donne naissance à un G^D-torseur.

Conjecture de Taylor

Quels points donnent lieu à une structure galoisienne triviale ?

Conjecture : Si A_K est une courbe elliptique, les points de torsion appartiennent au noyau de ψ.

Cette conjecture est un théorème (Srivastav et Taylor, Agboola, Pappas) sous l'hypothèse que l'ordre de G est premier à 6.

Il y a des exemples pour lesquels ψ n'est pas nul sur les points de 2-torsion (Cassou-Noguès et Jehanne).

– Que peut-on dire dans le cas où $\mathcal{A}$ a mauvaise réduction ?

Cas de mauvaise réduction

L'adhérence schématique de G_K dans $\mathcal{A}$ est un sous-groupe quasi-fini et plat de $\mathcal{A}$, qui n'est pas fini en général.

Point de départ : un sous-groupe fini et plat $G \subseteq \mathcal{A}$

Nous avons une suite exacte de faisceaux fppf

$$0 \longrightarrow G \longrightarrow \mathcal{A} \longrightarrow B \longrightarrow 0$$

dans laquelle le faisceau quotient B est représentable par un S-schéma en groupes. Si $\mathcal{A}$ est semi-stable, B est un sous-groupe ouvert de $\mathcal{B}$.

Objectif : trouver une suite exacte « duale », permettant de construire des G^D-torseurs.

Construction de la suite exacte duale

On travaille avec le petit site fppf sur S, c'est-à-dire la catégorie des S-schémas plats munie de la topologie fppf.

On montre que $\underline{\mathrm{Hom}}_S(\mathcal{A}, \mathbf{G}_{\mathrm{m}}) = 0$ dans ce site.

On sait également (Grothendieck) que $\underline{\mathrm{Ext}}^1_S(G, \mathbf{G}_{\mathrm{m}}) = 0$ pour la topologie fppf.

En appliquant le foncteur $\underline{\mathrm{Hom}}_S(-, \mathbf{G}_{\mathrm{m}})$ à la suite exacte

$$0 \longrightarrow G \longrightarrow \mathcal{A} \longrightarrow B \longrightarrow 0$$

on obtient la suite exacte

$$0 \longrightarrow G^D \longrightarrow \underline{\mathrm{Ext}}^1_S(B, \mathbf{G}_{\mathrm{m}}) \longrightarrow \underline{\mathrm{Ext}}^1_S(\mathcal{A}, \mathbf{G}_{\mathrm{m}}) \longrightarrow 0$$

On en déduit un cobord

$$\delta : \mathrm{Ext}^1(\mathcal{A}, \mathbf{G}_{\mathrm{m}}) \longrightarrow H^1(S, G^D)$$

Soit $\mathcal{A}^{t,\circ}$ la composante neutre de $\mathcal{A}^t$.

Théorème (Grothendieck) : Il existe une unique biextension W de $(\mathcal{A}, \mathcal{A}^{t,\circ})$ par $\mathbf{G}_{\mathrm{m}}$ prolongeant la biextension de Weil.

Cette biextension W permet de définir un isomorphisme

$$\gamma : \mathcal{A}^{t,\circ}(S) \xrightarrow{\ \sim\ } \mathrm{Ext}^1(\mathcal{A}, \mathbf{G}_{\mathrm{m}})$$

En composant γ, δ et π on obtient un morphisme

$$\psi : \mathcal{A}^{t,\circ}(S) \simeq \mathrm{Ext}^1(\mathcal{A}, \mathbf{G}_{\mathrm{m}}) \xrightarrow{\ \delta\ } H^1(S, G^D) \xrightarrow{\ \pi\ } \mathrm{Pic}(G)$$

ce qui généralise la construction de Taylor.

Bilan provisoire

$\mathcal{A}^{t,\circ}(S)$ est le sous-groupe de $A^t_K(K)$ constitué des « points de bonne réduction ».

Si P est un tel point, on vient de montrer que $\delta_K(P)$ se prolonge en un G^D-torseur, bien que $\mathcal{A}$ ait mauvaise réduction.

La conjecture de Taylor est encore vraie dans ce cadre, sous l'hypothèse de semi-stabilité de $\mathcal{A}$.

Théorème (J. G., 2004) : Si A_K est une courbe elliptique à réduction semi-stable, et si l'ordre de G est premier à 6, alors les points de torsion de $\mathcal{A}^{t,\circ}(S)$ appartiennent au noyau de ψ.

– Que se passe-t-il pour un point $P \notin \mathcal{A}^{t,\circ}(S)$?

Une question existentielle

$U \subseteq S$ l'ouvert de bonne réduction de $\mathcal{A}$

$\mathcal{A}_U$ est un U-schéma abélien, donc tout point $P \in A^t_K(K)$ donne lieu à un torseur $\delta_U(P) \in H^1(U, G^D_U)$. On aimerait le prolonger en un G^D-torseur sur S.

En général c'est impossible, pour des questions de ramification.

Mais on peut éventuellement considérer des G^D-torseurs dans une autre catégorie, contenant la catégorie des schémas.

Log schémas

Une pré-log structure sur un schéma X est un couple (α, M_X) où M_X est un faisceau de monoïdes (commutatifs !) sur le site étale de X et $\alpha : M_X \to \mathcal{O}_X$ est un morphisme de faisceaux de monoïdes, $\mathcal{O}_X$ étant muni de sa loi de multiplication.

Une log structure est une pré-log structure (α, M_X) telle que α induise un isomorphisme $\alpha^{-1}(\mathcal{O}_X^*) \to \mathcal{O}_X^*$.

La log structure triviale sur X est donnée par $(i, \mathcal{O}_X^*)$ où $i : \mathcal{O}_X^* \hookrightarrow \mathcal{O}_X$ est l'inclusion canonique.

On dispose d'un foncteur pleinement fidèle de la catégorie des schémas dans la catégorie des log schémas, qui envoie un schéma sur lui même muni de sa log structure triviale.

Cartes

Le morphisme (injectif) de monoïdes multiplicatifs

$$\mathbb{N} \longrightarrow \mathbb{Z}[X]$$

qui envoie 1 sur X, définit une log structure sur $\mathbb{A}^1 = \mathrm{Spec}(\mathbb{Z}[X])$. Plus généralement, si P est un monoïde, alors l'inclusion naturelle

$$P \longrightarrow \mathbb{Z}[P]$$

définit une log structure (qualifiée de canonique) sur $\mathrm{Spec}(\mathbb{Z}[P])$.

Une carte d'un log schéma X est la donnée d'un monoïde P et d'un morphisme $P \to M_X$ qui induit un isomorphisme sur la log structure associée. De façon équivalente, une carte de X est la donnée d'un morphisme de log schémas $X \to \mathrm{Spec}(\mathbb{Z}[P])$ induisant un isomorphisme sur les log structures.

Travailler avec les cartes

Localement pour la topologie étale, tout log schéma (resp. tout morphisme de log schémas) admet une carte.

Soit P un monoïde, et soit P^{gp} son groupe de fractions totales.
On dit que P est intègre si $P \to P^{\mathrm{gp}}$ est injectif.
On dit que P est saturé s'il est intègre et satisfait la condition suivante : pour tout $a \in P^{\mathrm{gp}}$ et pour tout entier $n \geq 1$, la relation $a^n \in P$ implique que $a \in P$.

Un log schéma fin et saturé (ou log schéma fs) est un log schéma admettant (localement pour la topo étale) une carte modelée sur un monoïde fin (i.e. de type fini) et saturé.

Topologies logarithmiques ?

Pour avoir des torseurs, il faut définir une topologie de Grothendieck dans la catégorie des log schémas.

l'idée est de partir d'une topologie classique (fppf, étale, etc.) et de rajouter des revêtements supplémentaires, rendus possibles grâce aux log structures.

Revêtements kummériens standards

Soit $u : P \to Q$ un morphisme de monoïdes fins et saturés. On dit que u est kummérien (ou de Kummer) s'il est injectif, et si pour tout $a \in Q$, il existe un entier $n \geq 1$ tel que $a^n \in u(P)$.

Soient X un log schéma fs muni d'une carte $P \to M_X$ et $u : P \to Q$ un morphisme kummérien de monoides fins et saturés. Soit

$$Y := X \times_{\mathrm{Spec}(\mathbb{Z}[P])} \mathrm{Spec}(\mathbb{Z}[Q]),$$

le produit étant calculé dans la catégorie des log schémas fs. Alors la projection naturelle $Y \to X$ est un *espace formellement principal homogène* pour le groupe $(Q^{\mathrm{gp}}/u(P^{\mathrm{gp}}))^D$.

Explication technique

Soit $u : P \to Q$ un morphisme kummérien de monoïdes fins et saturés. Alors le morphisme naturel

$$\begin{aligned} (Q \oplus_P Q)^{\mathrm{fs}} &\longrightarrow (Q^{\mathrm{gp}}/u(P^{\mathrm{gp}})) \oplus Q \\ (a, b) &\longmapsto (\bar{b}, a + b) \end{aligned}$$

est un isomorphisme, où le membre de gauche est la somme amalgamée dans la catégorie des monoïdes fins saturés.

Ce résultat est faux si l'on se place dans la catégorie des monoïdes fins. L'hypothèse de saturation est essentielle ici.

Si M est un monoïde fs, nous notons $D(M)$ le schéma $\mathrm{Spec}(\mathbb{Z}[M])$ muni de sa structure canonique de log schéma fs.

En appliquant D à l'isomorphisme de la page précédente, on obtient un isomorphisme

$$\begin{aligned} D(Q^{\mathrm{gp}}/u(P^{\mathrm{gp}})) \times D(Q) &\longrightarrow D(Q) \times_{D(P)} D(Q) \\ (g, x) &\longmapsto (x, g.x) \end{aligned}$$

dans la catégorie des log schémas fs.

Le morphisme $D(Q) \to D(P)$ est formellement principal homogène pour le groupe $D(Q^{\mathrm{gp}}/u(P^{\mathrm{gp}}))$.

Par changement de base $X \to D(P)$, le morphisme $Y \to X$ est formellement principal homogène de groupe $D(Q^{\mathrm{gp}}/u(P^{\mathrm{gp}}))$.

On dit que $Y \to X$ ci-dessus est un revêtement kummérien plat standard.

La topologie Kummer plate est la topologie engendrée par les ouverts fppf classiques et par les revêtements kummériens plats standards, qui deviennent des torseurs pour cette topologie.

Si l'ordre de $Q^{\mathrm{gp}}/u(P^{\mathrm{gp}})$ est inversible sur X, alors on dit que $Y \to X$ est un revêtement kummérien étale standard. On définit ainsi la topologie Kummer étale.

Si X est un log schéma fs et si U est l'ouvert de trivialité de la log structure de X, alors le foncteur

$$j : (Sch/U) \to (fsLogSch/X)$$

est un morphisme de localisation, et la topo induite par la topo Kummer plate sur X est la topo fppf sur U.

Torseurs sur un trait

R un anneau de valuation discrète, π une uniformisante de R. On définit une log structure sur $T := \mathrm{Spec}(R)$ donnée par la carte

$$\mathbb{N} \longrightarrow R, \quad 1 \longmapsto \pi$$

on note $T^{\log}$ le log schéma ainsi obtenu. L'ouvert de trivialité de $T^{\log}$ est le point générique η.

Soit $n > 0$ un entier naturel, alors $n : \mathbb{N} \to \mathbb{N}$ est un morphisme kummérien de monoïdes fs.

Le torseur kummérien standard, de groupe μ_n, qui en découle a pour morphisme de schémas sous-jacent

$$\mathrm{Spec}(R[X]/(X^n - \pi)) \longrightarrow T$$

Corollaire

Le morphisme de restriction

$$j^* : H^1_{\mathrm{kpl}}(T^{\log}, \mu_n) \longrightarrow H^1_{\mathrm{fppf}}(\eta, \mu_n)$$

est un isomorphisme.

Si n est inversible sur T alors on peut remplacer la topologie Kummer plate par la topologie Kummer étale dans le calcul du membre de gauche.

Cas global

Retour à notre S spectre d'anneau d'entiers

$U \subseteq S$ un ouvert de S

L'immersion canonique $j : U \to S$ définit une log structure sur S, donnée par

$$M_S = \mathcal{O}_S \cap j_* \mathcal{O}_U^* \longrightarrow \mathcal{O}_S$$

On note $S^{\log}$ le log schéma ainsi obtenu.

U est l'ouvert de trivialité de $S^{\log}$.

Si $T \subseteq S$ est un trait dont le point fermé appartient à U (resp. à $S - U$), alors la log structure induite sur T par celle de $S^{\log}$ est la log structure triviale (resp. canonique) de T.

Torseurs sous un groupe fini

G un S-schéma en groupes fini et plat

Le morphisme de restriction

$$j^* : H^1_{\mathrm{kpl}}(S^{\log}, G) \longrightarrow H^1_{\mathrm{fppf}}(U, G_U)$$

est injectif.

Exemple : Si $G = \Gamma_S$ est un groupe constant, alors

$H^1_{\mathrm{kpl}}(S^{\log}, \Gamma_S) = \{\mathrm{Spec}(\mathcal{O}_L) \to S$ où L/K est une K-algèbre galoisienne de groupe Γ, non ramifiée en les points de U et modérément ramifiée en les points de $S - U$ $\}$

Structure galoisienne des torseurs Kummer plats

Soit $X \to S^{\log}$ un G-torseur pour la topologie Kummer plate. Alors le morphisme de schémas $\overset{\circ}{X} \to S$ sous-jacent est fini surjectif (donc plat, S étant régulier de dimension 1).

De plus, l'action de G sur $\overset{\circ}{X}$ est *modérée*, au sens de Chinburg-Erez-Pappas-Taylor et de Childs-Hurley.

L'algèbre de $\overset{\circ}{X}$ est donc un G^D-module localement libre.

L'application

$$cl : H^1_{\mathrm{kpl}}(S^{\log}, G) \longrightarrow \mathrm{Pic}(G^D)$$

qui mesure cette structure n'est pas un morphisme de groupes en général, même si G est un groupe constant.

Retour à la construction précédente

On peut refaire (moyennant quelques log retouches) toute la construction de ψ en topologie Kummer plate : on a un cobord

$$\delta^{\log} : \mathrm{Ext}^1_{\mathrm{kpl}}(\mathcal{A}, \mathbf{G}_{\mathrm{m}}) \longrightarrow H^1_{\mathrm{kpl}}(S^{\log}, G^D)$$

et il ne reste plus qu'à construire une biextension $(\mathcal{A}, \mathcal{A}^t)$ par $\mathbf{G}_{\mathrm{m}}$ dans le topos Kummer plat.

On dispose déjà d'une biextension de $(\mathcal{A}, \mathcal{A}^{t,\circ})$ par $\mathbf{G}_{\mathrm{m}}$. Sous l'hypothèse que $\mathcal{A}$ est semi-stable, on réussit à la prolonger, d'où un isomorphisme

$$\gamma^{\log} : \mathcal{A}^t(S) \xrightarrow{\ \sim\ } \mathrm{Ext}^1_{\mathrm{kpl}}(\mathcal{A}, \mathbf{G}_{\mathrm{m}})$$

Ceci répond à la question posée : pour tout $P \in A^t_K(K)$, le torseur $\delta_U(P)$ se prolonge en un torseur dans $H^1_{\mathrm{kpl}}(S^{\log}, G^D)$.

Conclusion

Si $\mathcal{A}$ est semi-stable, on vient de construire une application ensembliste

$$\psi^{\log} : \mathcal{A}^t(S) \longrightarrow H^1_{\mathrm{kpl}}(S^{\log}, G^D) \xrightarrow{cl} \mathrm{Pic}(G)$$

qui généralise le ψ de départ.

Remarque : On ne peut pas raisonnablement espérer que la conjecture de Taylor soit encore satisfaite dans ce cadre.