Des obstructions globales à la descente des revêtements

J.-M. Couveignes et Nicolas Ros*

3 mars 2004

Résumé

Nous donnons une mesure de l'obstruction pour que le corps des modules de certains revêtements, obtenus par changement de base, soit un corps de définition. Nous montrons que le principe local-global ou principe de Hasse ne gouverne pas cette obstruction. Plus précisément, nous construisons des revêtements ayant des modèles sur tous les complétés de $\mathbb{Q}$ mais pas de modèle sur $\mathbb{Q}$.

Classification de l'AMS : 12Y05, 12F10, 11R37.

1 Introduction

Dans cet article, si K est un corps, une K-variété est par défaut supposée quasi-projective, régulière et géométriquement connexe.

Si $\mathcal{B}$ est une K-variété et L une extension de K, un L-revêtement de $\mathcal{B}$ est par défaut un L-morphisme fini, étale $\phi : \mathcal{C} \to \mathcal{B} \otimes_K L$ où $\mathcal{C}$ est une L-variété.

Si $\psi : \mathcal{D} \to \mathcal{B} \otimes_K L$ est un autre L-revêtement, un L-morphisme de revêtements est un L-morphisme de variétés $\kappa : \mathcal{C} \to \mathcal{D}$ tel que $\phi = \psi \circ \kappa$.

On appelle $*$-L-morphisme de L-revêtements de $\mathcal{B}$ un couple (κ, β) de L-morphismes $\kappa : \mathcal{C} \to \mathcal{D}$ et $\beta : \mathcal{B} \otimes_K L \to \mathcal{B} \otimes_K L$ tels que β soit un L-isomorphisme et $\psi \circ \kappa = \beta \circ \phi$.

Fixons $\bar{K}$ une clôture algébrique de K. On définit la catégorie $\mathbf{REV}(\mathcal{B})$ des $\bar{K}$-revêtements de $\mathcal{B}$ avec leurs $\bar{K}$-morphismes.

On définit aussi la catégorie $\mathbf{REV}^*(\mathcal{B})$ qui a les mêmes objets que $\mathbf{REV}(\mathcal{B})$ mais qui admet comme morphismes les $*$-$\bar{K}$-morphismes de revêtements.

Soient $\mathbb{K}$ un corps de nombres, $\bar{\mathbb{K}}$ une clôture algébrique et $\mathcal{B}$ une $\mathbb{K}$-variété.

Le groupe de Galois absolu de $\mathbb{K}$ noté $\Gamma_{\mathbb{K}}$ agit fonctoriellement sur les catégories $\mathbf{REV}(\mathcal{B})$ et $\mathbf{REV}^*(\mathcal{B})$.

Si $\mathcal{O} \to \mathrm{Spec}(\bar{\mathbb{K}})$ est un objet et $\sigma \in \Gamma_{\mathbb{K}}$, l'objet ${}^{\sigma}\mathcal{O} \to \mathrm{Spec}(\bar{\mathbb{K}})$ est défini comme le tiré en arrière de $\mathcal{O} \to \mathrm{Spec}(\bar{\mathbb{K}})$ le long de $\mathrm{Spec}(\sigma) : \mathrm{Spec}(\bar{\mathbb{K}}) \to \mathrm{Spec}(\bar{\mathbb{K}})$; qui est isomorphe à la composition $\mathcal{O} \to \mathrm{Spec}(\bar{\mathbb{K}}) \overset{\mathrm{Spec}(\sigma^{-1})}{\to} \mathrm{Spec}(\bar{\mathbb{K}})$. Le stabilisateur dans $\Gamma_{\mathbb{K}}$ de la classe de $\bar{\mathbb{K}}$-isomorphisme d'un objet est un sous-groupe d'indice fini. Le sous-corps de $\bar{\mathbb{K}}$ fixé par ce sous-groupe est appelé *corps*

*Groupe de Recherche en Informatique et Mathématiques du Mirail, Université de Toulouse II, Le Mirail, 5 allées Antonio Machado, 31058 Toulouse cedex 9, France, couveig@univ-tlse2.fr, ros@univ-tlse2.fr

des modules de l'objet. Si $\mathbb{L}$ est un corps $\mathbb{K} \subset \mathbb{L} \subset \bar{\mathbb{K}}$, on dit que $\mathcal{O}$ est défini sur $\mathbb{L}$ s'il est isomorphe, comme $\bar{\mathbb{K}}$-objet, au tiré en arrière d'un $\mathbb{L}$-objet $\mathcal{O}' \to \mathrm{Spec}(\mathbb{L})$ par $\mathrm{Spec}(\bar{\mathbb{K}}) \to \mathrm{Spec}(\mathbb{L})$. On dit aussi que $\mathbb{L}$ est *un corps de définition* de $\mathcal{O}$. Le corps des modules est contenu dans tous les corps de définition. Donc si le corps des modules est aussi corps de définition, il est le plus petit.

Notons que Serre récapitule dans [14, V.20] diverses manières de définir l'action de $\Gamma_{\mathbb{K}}$ sur les $\bar{\mathbb{K}}$-variétés abstraites, selon qu'on adopte le point de vue des Foundations de Weil ou celui des schémas de Chevalley. On trouve dans [1, Chapter 6] une étude de cette question dans le langage des schémas de Grothendieck. Notons aussi que dans sa thèse [13], Bounab Sadi traite les questions de descente pour les revêtements dans le cadre souvent suffisant des extensions de corps de fonctions.

Le corps des modules d'un revêtement contient (parfois strictement) le corps des modules du $*$-revêtement associé. On en trouve des exemples dans [12].

On demande si le corps des modules d'un revêtement est un corps de définition. Les exemples construits dans [3, 5, 4] montrent que ce n'est pas toujours le cas. Il est donc naturel de se demander si le principe local-global s'applique dans ce contexte. Plus précisément, supposons qu'un revêtement a des modèles sur tous les complétés de $\mathbb{Q}$. Il a donc $\mathbb{Q}$ pour corps des modules. On demande s'il a un modèle sur $\mathbb{Q}$. On pose la même question pour les $*$-revêtements. Notons que dans le cas des G-revêtements (revêtements Galoisiens avec leur action de groupe) des exemples de Coombes et Harbater [2] montrent que le corps des modules n'est pas toujours corps de définition. En revanche, Dèbes et Douai ont montré dans [7, théorème 3.8] qu'un G-revêtement est défini sur $\mathbb{Q}$ si et seulement s'il est défini sur tous les complétés de $\mathbb{Q}$. Plus généralement, il en va de même si on remplace $\mathbb{Q}$ par un corps de nombres, hormis les *cas spéciaux* du théorème de Grunwald-Wang.

Le cas des revêtements demeure assez obscur. Dèbes et Douai parviennent dans [8] à distinguer certains cas de revêtements pour lesquels le principe local-global est vérifié. Il s'agit de cas particuliers pour lesquels l'obstruction cohomologique est levée. Voir [8, théorème 5.1], [6, théorème 8.1]. Geoffroy Derome nous signale qu'il a montré dans [9] que le principe local-global s'applique aux revêtements cycliques d'ordre non-divisible par 8. Toutefois, la validité du principe local-global n'est ni établie ni infirmée par ces travaux.

Dans cet article, nous construisons des revêtements et des $*$-revêtements de corps des modules $\mathbb{Q}$, définis sur $\mathbb{Q}_v$ pour toute place v de $\mathbb{Q}$ et qui ne sont pas définis sur $\mathbb{Q}$, ce qui constituera autant de contre-exemples au principe local-global dans ce contexte.

Dans la section 2 nous introduisons deux foncteurs de changement de base pour les revêtements et nous cherchons dans quelle mesure ils préservent le corps des modules et les corps de définition. Nous montrons que pour une vaste classe de revêtements, l'existence d'un modèle sur le corps des modules est conditionnée à la possibilité de relever un certain 1-cocycle. Dans la section 3 nous construisons des modules galoisiens similaires à ceux étudiés par Tate [16, III 4.7] et nous étudions leurs premiers et seconds groupes de cohomologie galoisienne pour y déceler des éléments non nuls mais nuls partout localement. Il ne nous reste plus alors qu'à réaliser les cocycles pathologiques de la section 3 dans le contexte géométrique de la section 2 pour obtenir les exemples annoncés. C'est ce qu'on fait dans la section 5 grâce à des techniques constructives de la théorie inverse de Galois présentées dans la section 4. La section 6 présente une variante de cette construction qui illustre mieux la situation plus simple des $*$-revêtements.

Notation : si k est un corps et $N > 1$ un entier, on notera parfois k^*/Nk^* le groupe $k^*/(k^*)^N$. On notera parfois fg la composée $f \circ g$ de deux applications f et g.

Remerciements : Nous remercions Geoffroy Derome, Philippe Satgé et le rapporteur pour leurs commentaires sur ce travail.

2 Changement de base et rationalité

Soient $\mathbb{K}$ un corps de nombres, $\mathcal{B}$ une $\mathbb{K}$-variété et $\mathcal{B}'$ une tordue de $\mathcal{B}$, c'est-à-dire une $\mathbb{K}$-variété telle que $\mathcal{B}' \otimes_{\mathbb{K}} \bar{\mathbb{K}}$ soit $\bar{\mathbb{K}}$-isomorphe à $\mathcal{B} \otimes_{\mathbb{K}} \bar{\mathbb{K}}$. Choisissons $I : \mathcal{B} \otimes_{\mathbb{K}} \bar{\mathbb{K}} \to \mathcal{B}' \otimes_{\mathbb{K}} \bar{\mathbb{K}}$ un isomorphisme. Il existe un foncteur de changement de base $\mathbb{T}_{\mathcal{B},\mathcal{B}',I}$ de $\mathbf{REV}(\mathcal{B})$ dans $\mathbf{REV}(\mathcal{B}')$ qui à tout revêtement $\phi : \mathcal{C} \to \mathcal{B} \otimes_{\mathbb{K}} \bar{\mathbb{K}}$ associe le tiré en arrière de ϕ le long de I^{-1} ; qui est isomorphe à $I \circ \phi : \mathcal{C} \to \mathcal{B}' \otimes_{\mathbb{K}} \bar{\mathbb{K}}$. Ce foncteur ne conserve pas les corps des modules en général. On construit de même un foncteur $\mathbb{T}^*_{\mathcal{B},\mathcal{B}',I}$ de $\mathbf{REV}^*(\mathcal{B})$ dans $\mathbf{REV}^*(\mathcal{B}')$. Celui-ci conserve les corps des modules et ne dépend que de $\mathcal{B}$ et $\mathcal{B}'$ à isomorphisme de foncteurs près, ce qui nous autorise à le noter $\mathbb{T}^*_{\mathcal{B},\mathcal{B}'}$.

Premier point : Soit $\phi : \mathcal{C} \to \mathcal{B}$ un $\mathbb{K}$-revêtement, galoisien sur $\bar{\mathbb{K}}$, et soit $\mathcal{B}'$ une tordue de $\mathcal{B}$. Le revêtement $\mathbb{T}^*_{\mathcal{B},\mathcal{B}'}(\mathcal{C}, \phi)$ a $\mathbb{K}$ pour corps des modules dans $\mathbf{REV}^*(\mathcal{B}')$. On demande s'il a $\mathbb{K}$ pour corps de définition.

Soit $\mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)$ le groupe des $\bar{\mathbb{K}}$-automorphismes de $\phi \otimes_{\mathbb{K}} \bar{\mathbb{K}}$. L'ordre de ce groupe est le degré de ϕ. Soit $\mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)$ le groupe des $*$-$\bar{\mathbb{K}}$-automorphismes de $\phi \otimes_{\mathbb{K}} \bar{\mathbb{K}}$. On vérifie que $\mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)$ est le normalisateur de $\mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)$ dans $\mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{C} \otimes_{\mathbb{K}} \bar{\mathbb{K}})$. On définit $\mathrm{Ex}_{\bar{\mathbb{K}}}(\phi)$ comme le quotient

$$\mathrm{Ex}_{\bar{\mathbb{K}}}(\phi) = \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi) / \mathrm{Aut}_{\bar{\mathbb{K}}}(\phi).$$

Ce quotient s'identifie à un sous-groupe de $\mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{B})$ et si on note $\underline{\phi}$ l'application quotient, on a la suite exacte de $\Gamma_{\mathbb{K}}$-groupes :

$$0 \to \mathrm{Aut}_{\bar{\mathbb{K}}}(\phi) \to \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi) \xrightarrow{\underline{\phi}} \mathrm{Ex}_{\bar{\mathbb{K}}}(\phi) \to 0 \tag{1}$$

d'où l'on dérive l'application :

$$\underline{\phi}^* : H^1(\mathbb{K}, \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)) \longrightarrow H^1(\mathbb{K}, \mathrm{Ex}_{\bar{\mathbb{K}}}(\phi)).$$

On note $\iota : H^1(\mathbb{K}, \mathrm{Ex}_{\bar{\mathbb{K}}}(\phi)) \to H^1(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{B}))$ l'application induite par l'inclusion de $\mathrm{Ex}_{\bar{\mathbb{K}}}(\phi)$ dans $\mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{B})$. Posons maintenant $a_\sigma = I^{-1}{}^\sigma I$ et soit $a = (a_\sigma)_\sigma$ dans $H^1(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{B}))$, le cocycle associé à $\mathcal{B}'$.

Théorème 1 *Il existe une tordue $\mathcal{C}'$ de $\mathcal{C}$, un revêtement $\psi : \mathcal{C}' \longrightarrow \mathcal{B}'$ définis sur $\mathbb{K}$ et un diagramme commutatif*

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{J} & \mathcal{C}' \\ \phi\downarrow & & \downarrow\psi \\ \mathcal{B} & \xrightarrow{I} & \mathcal{B}' \end{array}$$

où I et J sont des $\bar{\mathbb{K}}$-isomorphismes, si et seulement si le cocycle $a = (a_\sigma)_\sigma$ est dans l'image de l'application composée $H^1(\mathbb{K}, \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)) \overset{\phi^*}{\to} H^1(\mathbb{K}, \mathrm{Ex}_{\bar{\mathbb{K}}}(\phi)) \overset{\iota}{\to} H^1(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{B}))$. On dit alors qu'il existe une tordue de ϕ au dessus de $\mathcal{B}'$. Cela revient à dire que $\mathbb{T}^*_{\mathcal{B},\mathcal{B}'}(\mathcal{C}, \phi)$ a $\mathbb{K}$ pour corps de définition dans $\mathbf{REV}^*(\mathcal{B}')$.

Si un tel diagramme existe alors posons $b = (J^{-1\sigma}J)_\sigma \in H^1(\mathbb{K}, \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi))$ et $c = (I^{-1\sigma}I)_\sigma \in H^1(\mathbb{K}, \mathrm{Ex}_{\bar{\mathbb{K}}}(\phi))$. L'image de b par ϕ^* est c. L'image de c dans $H^1(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{B}))$ est a.

Réciproquement, soient $b = (b_\sigma)_\sigma$ dans $H^1(\mathbb{K}, \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi))$ et $c = \phi^*(b)$. Supposons que c s'envoie sur a dans $H^1(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{B}))$. Il existe $\mathcal{C}'/\mathbb{K}$ une tordue de $\mathcal{C}$ et $J : \mathcal{C} \to \mathcal{C}'$ un $\bar{\mathbb{K}}$-isomorphisme tels que $J^{-1\sigma}J = b_\sigma \in \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)$ pour tout $\sigma \in \Gamma_{\mathbb{K}}$ (une construction donnée par Weil dans [17]). L'image $J\,\mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)J^{-1}$ de $\mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)$ par J est un groupe de $\bar{\mathbb{K}}$-automorphismes de $\mathcal{C}'$ qui est globalement invariant par $\Gamma_{\mathbb{K}}$ car $J^{-1\sigma}J$ est dans le normalisateur de $\mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)$ pour tout σ. On peut donc définir $\mathcal{B}'' = \mathcal{C}'/(J\,\mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)J^{-1})$ et compléter le diagramme commutatif suivant

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{J} & \mathcal{C}' \\ \phi\downarrow & & \downarrow\psi \\ \mathcal{B} & \xrightarrow{I} & \mathcal{B}'' \end{array}.$$

On vérifie que $(I^{-1\sigma}I)_\sigma = \phi^*(b) = c$ et donc $\mathcal{B}''$ est $\mathbb{K}$-isomorphe à $\mathcal{B}'$. □

Si ι est bijective et si $\mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)$ est dans le centre de $\mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)$, l'obstruction est mesurée par un élément de $H^2(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\phi))$.

Le cas où ι n'est pas injective est particulièrement intéressant. Supposons que $\mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)$ et $\mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{B})$ sont abéliens. Soit

$$\delta_\phi : H^1(\mathbb{K}, \mathrm{Ex}_{\bar{\mathbb{K}}}(\phi)) \to H^2(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\phi))$$

le cobord dérivé de la suite exacte de l'équation 1. Supposons aussi que $(a_\sigma)_\sigma$ est à valeurs dans $\mathrm{Ex}_{\bar{\mathbb{K}}}(\phi)$. Notons $\mathcal{X}(\mathbb{K}, \phi)$ le quotient de $H^2(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\phi))$ par le cobord du noyau de ι soit

$$\mathcal{X}(\mathbb{K}, \phi) = H^2(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\phi))/\delta_\phi(\mathrm{Ker}(\iota)).$$

Soit $\mathfrak{d}_\phi$ l'application composée

$$\mathfrak{d}_\phi : H^1(\mathbb{K}, \mathrm{Ex}(\phi)) \overset{\delta_\phi}{\to} H^2(\mathbb{K}, \mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)) \to \mathcal{X}(\mathbb{K}, \phi).$$

Alors $\mathbb{T}^*_{\mathcal{B},\mathcal{B}'}(\mathcal{C}, \phi)$ a $\mathbb{K}$ pour corps de définition dans $\mathbf{REV}^*(\mathcal{B}')$ si et seulement si $\mathfrak{d}_\phi(a) = 0$. Un quotient tel que $\mathcal{X}(\mathbb{K}, \phi)$ viole volontiers le principe local-global. On donne dans la section 6 un exemple de cette dernière situation.

Second point : Soit encore $\phi : \mathcal{C} \to \mathcal{B}$ un revêtement galoisien sur $\bar{\mathbb{K}}$ et défini sur $\mathbb{K}$. Soient $\mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)$, $\mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)$ et $\mathrm{Ex}_{\bar{\mathbb{K}}}(\phi) = \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)/\mathrm{Aut}_{\bar{\mathbb{K}}}(\phi)$ comme précédemment et soit $\mathcal{B}'$ une tordue de $\mathcal{B}$ et $I : \mathcal{B} \to \mathcal{B}'$ un isomorphisme tel que $a_\sigma = I^{-1\sigma}I$ soit dans $\mathrm{Ex}_{\bar{\mathbb{K}}}(\phi)$. Le revêtement $\mathbb{T}_{\mathcal{B},\mathcal{B}',I}(\mathcal{C},\phi)$ a $\mathbb{K}$ pour corps des modules dans $\mathbf{REV}(\mathcal{B}')$ car ${}^\sigma(I \circ \phi) = II^{-1\sigma}I\phi = Ia_\sigma\phi = I\phi b_\sigma$ pour un $b_\sigma \in \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)$. On demande si $\mathbb{T}_{\mathcal{B},\mathcal{B}',I}(\mathcal{C},\phi)$ a $\mathbb{K}$ pour corps de définition. Le théorème suivant se prouve comme le théorème 1.

Théorème 2 *Il existe une tordue $\mathcal{C}'$ de $\mathcal{C}$, un morphisme $\psi : \mathcal{C}' \longrightarrow \mathcal{B}'$ définis sur $\mathbb{K}$ et un $\bar{\mathbb{K}}$-morphisme $J : \mathcal{C} \to \mathcal{C}'$ qui rende le diagramme suivant commutatif*

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{J} & \mathcal{C}' \\ \phi\downarrow & & \downarrow\psi \\ \mathcal{B} & \xrightarrow{I} & \mathcal{B}' \end{array}$$

si et seulement si $(a_\sigma)_\sigma$ est dans l'image de l'application

$$\phi^* : H^1(\mathbb{K}, \mathrm{Aut}^*_{\bar{\mathbb{K}}}(\phi)) \to H^1(\mathbb{K}, \mathrm{Ex}_{\bar{\mathbb{K}}}(\phi)).$$

On dit alors qu'il existe une tordue de ϕ au dessus de I. Cela revient à dire que $\mathbb{T}_{\mathcal{B},\mathcal{B}',I}(\mathcal{C},\phi)$ a $\mathbb{K}$ pour corps de définition dans $\mathbf{REV}(\mathcal{B})$.

On construit dans la section 5 des obstructions globales de cette sorte.

3 Une famille de modules galoisiens

Dans cette section on construit un cocycle qui se relève partout localement mais pas globalement.

Soient A et B deux rationnels non nuls tels que -1, 2, A et B soient linéairement indépendants dans $\mathbb{Q}^*/2\mathbb{Q}^*$. Soit $\sqrt[8]{A}$ la racine huitième de A (la réelle positive si A est positif et celle d'argument $\pi/8$ si A est négatif). Soit de même $\sqrt[8]{B}$ la racine huitième de B. Soit ζ_8 la racine huitième de 1 d'argument $\pi/4$.

Soit $\mathbb{D} = \mathbb{Q}(\zeta_8, \sqrt[8]{A}, \sqrt[8]{B})$. L'extension $\mathbb{D}/\mathbb{Q}$ est galoisienne de groupe $\Gamma = (\mathbb{Z}/8\mathbb{Z})^* \ltimes (\mathbb{Z}/8\mathbb{Z})^2$. Pour c dans $(\mathbb{Z}/8\mathbb{Z})^*$ et (a,b) dans $(\mathbb{Z}/8\mathbb{Z})^2$ on note $[c,a,b]$ l'élément de ce groupe de Galois qui envoie ζ_8 sur ζ_8^c, $\sqrt[8]{A}$ sur $\sqrt[8]{A}\,\zeta_8^a$ et $\sqrt[8]{B}$ sur $\sqrt[8]{B}\,\zeta_8^b$.

On considère le module galoisien $G_{A,B}$ défini comme le quotient

$$< \zeta_8, \sqrt[8]{A}, \sqrt[8]{B} > / < A, B > \quad \subset \quad \bar{\mathbb{Q}}^* / < A, B > .$$

Comme groupe commutatif, il est isomorphe à $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Comme module galoisien, il est une extension

$$1 \to \mu_8 \to G_{A,B} \to C_8 \times C_8 \to 0$$

où C_8 est le groupe cyclique d'ordre 8 avec action triviale de $\Gamma_{\mathbb{Q}}$ et μ_8 le module galoisien des racines huitièmes de l'unité.

On note G_A le sous-module $< \zeta_8, \sqrt[8]{A} > / < A >$ de $G_{A,B}$. La suite exacte

$$1 \to G_A \to G_{A,B} \to C_8 \to 0 \tag{2}$$

induit un morphisme cobord $\delta_{A,B} : H^1(\mathbb{Q}, C_8) \to H^2(\mathbb{Q}, G_A)$.

On cherche un cocycle non nul b dans $H^2(\mathbb{Q}, G_A)$ qui soit nul partout localement. Un tel cocycle est construit par Tate et donné par Serre dans [16, III.4.7]. On prend $A = 14$. On rappelle que $H^2(\mathbb{Q}, \mu_8)$ n'est autre que la 8-torsion $\mathrm{Br}_8(\mathbb{Q})$ du groupe de Brauer de $\mathbb{Q}$. Le groupe de Brauer de $\mathbb{Q}$ s'injecte dans le produit des groupes de Brauer $\mathrm{Br}(\mathbb{Q}_v)$ où v parcourt l'ensemble des places de $\mathbb{Q}$. Le groupe $\mathrm{Br}(\mathbb{R})$ est $\{0, \frac{1}{2}\} \subset \mathbb{Q}/\mathbb{Z}$ et pour v une place p finie, le groupe $\mathrm{Br}(\mathbb{Q}_p)$ est égal à $\mathbb{Q}/\mathbb{Z}$. On a une suite exacte [15, X.7]

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \oplus \mathrm{Br}(\mathbb{Q}_v) \stackrel{\Sigma}{\to} \mathbb{Q}/\mathbb{Z} \to 0$$

où Σ est l'application somme des composantes locales. Pour spécifier un élément b de $\mathrm{Br}(\mathbb{Q})$ il suffit donc de donner ses composantes locales b_v, pourvu que leur somme soit nulle.

On choisit donc pour $b \in H^2(\mathbb{Q}, \mu_8)$ l'élément de composantes locales nulles en dehors de 2 et 17 et $b_2 = -b_{17} = \frac{1}{8}$. On appelle encore b les images de b dans $H^2(\mathbb{Q}, G_A)$, $H^2(\mathbb{Q}, G_B)$, et $H^2(\mathbb{Q}, G_{A,B})$. Tate montre que le cocycle $b \in H^2(\mathbb{Q}, G_A)$ est non nul mais nul partout localement. On cherche un a dans $H^1(\mathbb{Q}, C_8)$ tel que $b = \delta_{A,B}(a) \in H^2(\mathbb{Q}, G_A)$. Un tel a existe pourvu que b s'annule dans $H^2(\mathbb{Q}, G_{A,B})$. Cette dernière condition est satisfaite si b s'annule déjà dans $H^2(\mathbb{Q}, G_B)$ ce qui revient à dire que b est de la forme $\delta_B(\chi)$ où

$$\delta_B : H^1(\mathbb{Q}, C_8) \to H^2(\mathbb{Q}, \mu_8)$$

est déduite de la suite exacte

$$0 \to \mu_8 \to G_B \to C_8 \to 0$$

et $\chi \in H^1(\mathbb{Q}, C_8) = H^1(\mathbb{Q}, \frac{1}{8}\mathbb{Z}/\mathbb{Z})$. Il y a un accouplement naturel entre $\frac{1}{8}\mathbb{Z}/\mathbb{Z}$ et μ_8 qui associe ζ_8 au couple $(\frac{1}{8}, \zeta_8)$ et $\delta_B(\chi)$ n'est autre que le cup-produit $\chi.\delta_K B$ de χ et de $\delta_K B \in H^1(\mathbb{Q}, \mu_8)$ pour cet accouplement. Ici

$$\delta_K : \mathbb{Q}^*/8\mathbb{Q}^* \to H^1(\mathbb{Q}, \mu_8)$$

est le cobord déduit de la suite exacte de Kummer. Si

$$d : H^1(\mathbb{Q}, \frac{1}{8}\mathbb{Z}/\mathbb{Z}) \to H^2(\mathbb{Q}, \mathbb{Z})$$

est le cobord déduit de la suite exacte

$$0 \to \mathbb{Z} \to \frac{1}{8}\mathbb{Z} \to \frac{1}{8}\mathbb{Z}/\mathbb{Z} \to 0$$

alors $\chi.\delta_K B = B^{-1}.d\chi$ est le cocycle central dans la définition cohomologique de l'application d'Artin et il a pour composantes locales les $-\chi_v(B)$. Pour que b prenne la forme $B^{-1}.d\chi$ il faut et il suffit qu'il se décompose sur l'extension cyclique de degré 8 définie par χ (voir [15, XIV, Corollaire 2]). On choisit donc pour χ le caractère associé à une extension octique cyclique de $\mathbb{Q}$ qui a une seule place au dessus de 2 et 17. Qu'une telle extension existe, cela est assuré par le théorème de Grunwald-Wang [10, 4.16.4]. Qu'elle décompose b, cela résulte de [15, XIII, Proposition 7].

Donnons un exemple concret de cette situation. Une agréable extension cyclique de degré 8, gentiment suggérée par Christian Maire, est obtenue comme sous-corps $\mathbb{L}$ de $\mathbb{K} = \mathbb{Q}(x, y)$ avec $x = \zeta_{32} + \zeta_{32}^{-1}$ et $y = \zeta_{17} + \zeta_{17}^{-1}$. Ici $\zeta_{32} = \exp(2i\pi/32)$ et $\zeta_{17} = \exp(2i\pi/17)$. Le groupe de Galois G de $\mathbb{K}$ sur $\mathbb{Q}$ est isomorphe à $(\mathbb{Z}/8\mathbb{Z})^2$ et on note $[a, b]$ l'automorphisme de $\mathbb{K}$ qui envoie x sur $\zeta_{32}^a + \zeta_{32}^{-a}$ et y sur $\zeta_{17}^b + \zeta_{17}^{-b}$ où $a \in \{3, 9, 27, 17, 19, 25, 11, 1\}$ et $b \in \{14, 9, 7, 13, 12, 15, 6, 16\}$. Le corps $\mathbb{L}$ est défini comme sous-corps de $\mathbb{K}$ fixé par $[3, 14]$. Les symboles locaux pour une extension cyclotomique sont aisés à calculer.

On choisit un nombre premier p congru à 3 modulo 32 et à 14 modulo 17. Par exemple, on peut prendre $p = 643$. On calcule les symboles locaux :

En 2 on a

$$(p, \mathbb{K}_2/\mathbb{Q}_2)\zeta_{32} = \zeta_{32}^{11} \text{ et } (p, \mathbb{K}_2/\mathbb{Q}_2)\zeta_{17} = \zeta_{17}$$

donc $(p, \mathbb{K}_2/\mathbb{Q}_2) = [11, 1] = [3^{-1}, 1]$.

En 17 on a

$$(p, \mathbb{K}_{17}/\mathbb{Q}_{17})\zeta_{32} = \zeta_{32} \text{ et } (p, \mathbb{K}_{17}/\mathbb{Q}_{17})\zeta_{17} = \zeta_{17}^{11}$$

donc $(p, \mathbb{K}_{17}/\mathbb{Q}_{17}) = [1, 11] = [1, 14^{-1}]$.

En p on a

$$(p, \mathbb{K}_p/\mathbb{Q}_p)\zeta_{32} = \zeta_{32}^{p} \text{ et } (p, \mathbb{K}_p/\mathbb{Q}_p)\zeta_{17} = \zeta_{17}^{p}$$

donc $(p, \mathbb{K}_p/\mathbb{Q}_p) = [p, p] = [3, 14]$.

Partout ailleurs le symbole est nul.

Le groupe de Galois de $\mathbb{L}/\mathbb{Q}$ est le quotient de G par le sous-groupe engendré par $[3, 14]$. Donc posant $B = p$ et χ le caractère de ce quotient tel que $\chi([3, 1]) = \frac{1}{8} = -\chi([1, 14])$ on a $\delta_B(\chi) = B^{-1}.d\chi = b$.

Ceci montre qu'il existe un cocycle $a = \chi \in H^1(\mathbb{Q}, C_8)$ qui se relève partout localement dans $H^1(\mathbb{Q}, G_{A,B})$ selon la suite exacte 2 mais qui ne se relève pas globalement.

4 Une méthode constructive

Soit $\mathbb{K}$ un corps de nombres. Dans cette section, on cherche à réaliser certains $\Gamma_{\mathbb{K}}$-modules finis (groupes abéliens finis munis d'une action de $\Gamma_{\mathbb{K}}$) comme groupes de $\bar{\mathbb{K}}$-automorphismes d'une $\mathbb{K}$-variété. Dans la section 5, nous appliquerons cette méthode au module galoisien construit à la section 3

Soit donc $\mathcal{A}$ une $\mathbb{K}$-variété quasi-affine munie d'un point $\mathbb{K}$-rationnel o. On note $\mathcal{U}$ l'ensemble des unités de $\bar{\mathbb{K}}[\mathcal{A}]$ qui prennent la valeur 1 en o. Soit $N = p^k$ une puissance d'un nombre premier. On se donne $\mathbb{U}$ un sous $(\mathbb{Z}/N\mathbb{Z})$-module libre et fini de $\mathcal{U}/N\mathcal{U}$, globalement invariant par l'action de $\Gamma_{\mathbb{K}}$. Il existe un entier r et

r unités f_i pour $1 \leq i \leq r$ telles que les f_i soient linéairement indépendantes dans $\mathcal{U}/N\mathcal{U}$ et qu'elles engendrent $\mathbb{U}$. Pour tout $\sigma \in \Gamma_{\mathbb{K}}$, il existe des entiers $e(i,j,\sigma)$ et des unités $A_{i,\sigma} \in \mathcal{U}$ tels que

$$^{\sigma}f_i = \Pi_{j=1}^{r} f_j^{e(i,j,\sigma)} A_{i,\sigma}^N.$$

On définit alors une extension abélienne $\mathcal{F} = \bar{\mathbb{K}}(\mathcal{A}, y_1, ..., y_r)$ de $\bar{\mathbb{K}}(\mathcal{A})$ en posant $y_i^N = f_i$. On note Π le groupe de Galois de cette extension. C'est un $(\mathbb{Z}/N\mathbb{Z})$-module libre de rang r.

L'extension $\mathcal{F}/\mathbb{K}(\mathcal{A})$ est galoisienne de groupe de Galois $\Gamma_{\mathbb{K}} \ltimes \Pi$. En effet, l'action de $\Gamma_{\mathbb{K}}$ s'étend à $\mathcal{F}$ en posant

$$^{\sigma}y_i = \Pi_{j=1}^{r} y_j^{e(i,j,\sigma)} A_{i,\sigma}.$$

On note $\mathcal{F}_0$ le sous-corps de $\mathcal{F}$ fixé par $\Gamma_{\mathbb{K}}$. C'est une extension régulière de $\mathbb{K}(\mathcal{A})$. On appelle $\mathcal{C}$ la normalisée de $\mathcal{A}$ dans $\mathcal{F}_0$. C'est une $\mathbb{K}$-variété quasi-affine, géométriquement irréductible. Le morphisme $\phi : \mathcal{C} \to \mathcal{A}$ est fini étale, donc la régularité de $\mathcal{A}$ entraine celle de $\mathcal{C}$.

Le groupe $\mathrm{Aut}_{\bar{\mathbb{K}}}(\mathcal{C})$ contient Π et Π agit sans point fixe car ϕ est étale. Il reste à déterminer l'action de $\Gamma_{\mathbb{K}}$ sur Π. Notons $\kappa : \mathbb{U} \times \Pi \to \mu_N$ l'accouplement de Kummer défini par $(f, \theta) \mapsto \frac{\theta(\sqrt[N]{f})}{\sqrt[N]{f}}$. Cet accouplement est $\Gamma_{\mathbb{K}}$-équivariant en ce sens que pour tout $\sigma \in \Gamma_{\mathbb{K}}$ on a $\kappa(f, {}^{\sigma}\theta) = {}^{\sigma}\kappa(\sigma^{-1}(f), \theta)$. L'application dérivée à gauche $\kappa_g : \mathbb{U} \to \hat{\Pi}$, qui à f associe le caractère $* \mapsto \kappa(f, *)$ est donc un isomorphisme de $\Gamma_{\mathbb{K}}$-modules. Donc Π est le dual de $\mathbb{U}$.

Prenons $\mathbb{K} = \mathbb{Q}$ et supposons par exemple que l'on veuille réaliser $\Pi = C_N$ le groupe cyclique à N éléments avec action triviale de $\Gamma_{\mathbb{Q}}$. On doit contruire un $\mathbb{U}$ isomorphe à μ_N. On prend pour $\mathcal{A}$ la droite affine $\mathbb{A}^1$ privée des racines primitives N-ièmes de l'unité

$$\mathcal{A} = \mathrm{Spec}\, \mathbb{Q}[X, \frac{1}{\Phi_N(X)}]$$

et pour o le point de coordonnée $X = 0$. Ici $\Phi_N(X)$ est le N-ième polynôme cyclotomique.

Posons

$$f(X) = \prod_{i \in (\mathbb{Z}/N\mathbb{Z})^*} (1 - \zeta_N^i X)^{i^{-1}}$$

qui est bien défini dans $\mathcal{U}/N\mathcal{U}$. Notons que les exposants sont des classes modulo N.

Pour $\sigma \in \Gamma_{\mathbb{Q}}$ on note $\chi(\sigma) \in \hat{\mathbb{Z}}$ le caractère cyclotomique et on vérifie que

$$^{\sigma}f = \prod_{i \in (\mathbb{Z}/N\mathbb{Z})^*} (1 - \zeta_N^{i\chi(\sigma)} X)^{i^{-1}} = \prod_{i \in (\mathbb{Z}/N\mathbb{Z})^*} (1 - \zeta_N^i X)^{i^{-1}\chi(\sigma)} = f^{\chi(\sigma)}$$

dans $\mathcal{U}/N\mathcal{U}$.

On a donc réalisé C_N comme groupe d'automorphismes d'une variété. Tous les groupes abéliens avec action triviale s'obtiennent de même.

Plus généralement, soit $\mathbb{K}/\mathbb{Q}$ une extension galoisienne de groupe de Galois G. On en déduit un morphisme surjectif $\Gamma_{\mathbb{Q}} \to G$. On définit un $\Gamma_{\mathbb{Q}}$-module $\mathcal{M}$ comme le groupe commutatif $(\mathbb{Z}/N\mathbb{Z})[G]$ muni de la loi d'addition sur lequel agit $\Gamma_{\mathbb{Q}}$ de la façon suivante : si $\gamma \in \Gamma_{\mathbb{Q}}$ s'envoie sur $g \in G$, alors γ agit sur $\sum_{h\in G} a_h h \in \mathcal{M}$ par $\gamma(\sum_{h\in G} a_h h) = \sum_{h\in G} a_{g^{-1}h} h$. On peut réaliser le dual de $\mathcal{M}$ comme groupe d'automorphismes d'une $\mathbb{Q}$-variété. On prend un élément primitif α dans $\mathbb{K}$ et pour tout $g \in G$ on pose $f_g(X) = 1 + g(\alpha)X$. On pose $\mathcal{A} = \operatorname{Spec} \mathbb{Q}[X, \frac{1}{\prod_g f_g}] \subset \mathbb{A}^1_{\mathbb{Q}}$ et on prend pour o le point de coordonnée $X = 0$. Posant $\mathbb{U} =< (f_g)_{g\in G} >$ on a ainsi plongé le $\Gamma_{\mathbb{Q}}$-module $\mathcal{M}$ dans $\mathcal{U}/N\mathcal{U}$.

Dans la section 5 on voit comment réaliser les modules galoisiens extensions de $(C_N)^k$ par μ_N.

5 Une famille de revêtements

Dans cette section on applique les méthodes de la section 4 pour réaliser le module galoisien $G_{A,B}$ comme groupe d'automorphismes d'une courbe. On reprend les notations de la section 3.

On se donne deux familles de polynômes dans $\mathbb{D}(X)$, sur lesquelles Γ agit transitivement, par

$$Q_{c,a}(X) = 1 + (\zeta_8^c + \sqrt[8]{A}\zeta_8^a)X \text{ et } R_{c,b}(X) = 1 + (\zeta_8^c + \sqrt[8]{B}\zeta_8^b)X$$

pour $c \in (\mathbb{Z}/8\mathbb{Z})^*$, $a, b \in \mathbb{Z}/8\mathbb{Z}$ et on pose

$$S = \prod_{c,a} Q_{c,a}^{ca} \ , \ T = \prod_{c,b} R_{c,b}^{cb} \ , \ U = \prod_{c,a} Q_{c,a}^{c} \ , \text{ et } V = \prod_{c,b} R_{c,b}^{c}$$

où les indices a et b parcourent $\mathbb{Z}/8\mathbb{Z}$ et l'indice c parcourt $(\mathbb{Z}/8\mathbb{Z})^*$. Ces derniers polynômes sont bien définis modulo les puissances huitièmes.

On vérifie que les égalités suivantes

$$(3) \qquad {}^{[w,u,v]}Q_{c,a} = Q_{wc,wa+u} \ , \ {}^{[w,u,v]}R_{c,b} = R_{wc,wb+v} \ , \ {}^{[w,u,v]}S = SU^{-u}$$

et

$$(4) \qquad {}^{[w,u,v]}T = TV^{-v} \ , \ {}^{[w,u,v]}U = U^{w} \ , \ {}^{[w,u,v]}V = V^{w}$$

sont vraies dans le groupe $\mathbb{D}(X)^*/8\mathbb{D}(X)^*$.

On voit sans peine que le produit $\Delta = \prod_{c,a} Q_{c,a} \prod_{c,b} R_{c,b}$ est séparable. On pose $W = ST$. Gardant les notations de la section 4 on prend $\mathcal{A} = \operatorname{Spec} \mathbb{Q}[X, \frac{1}{\Delta}] \subset \mathbb{A}^1_{\mathbb{Q}}$ et o le point de coordonnée $X = 0$. On prend $p = 2$, $N = 8$ et $\mathbb{U}$ le sous-groupe de $\mathcal{U}/8\mathcal{U}$ engendré par $W = ST$, U et V. Il est clair que U et V sont linéairement indépendants (n'ayant aucune racine commune). On déduit facilement des équations 4 que W n'est pas dans le sous-espace engendré par U et V. On note Π le groupe de Galois de l'extension $\mathcal{F}/\bar{\mathbb{Q}}(X)$. On a vu que Π et $\mathbb{U}$ sont duaux. Plus précisément, on note (Ξ, Φ, Ψ) la base de Π duale de (W, U, V)

pour l'accouplement de Kummer, c'est-à-dire $\kappa(W,\Xi)=\kappa(U,\Phi)=\kappa(V,\Psi)=\zeta_8$ et tous les autres accouplements valent 1. Une telle base duale existe car l'accouplement de Kummer est non dégénéré.

On déduit alors de l'équation 3

$$^{[w,u,v]}\Xi=\Xi^w\ ,\ ^{[w,u,v]}\Phi=\Phi\Xi^u,\text{ et }^{[w,u,v]}\Psi=\Psi\Xi^v$$

de sorte que le module galoisien Π est isomorphe à $G_{A,B}$. On prend l'isomorphisme qui envoie Ξ sur ζ_8, Φ sur $\sqrt[8]{A}$ et Ψ sur $\sqrt[8]{B}$. Appliquant la méthode de la section 4 on obtient une variété $\mathcal{C}$ qui est une courbe affine sur laquelle agit $G_{A,B}$ sans point fixe puisque le revêtement construit est non ramifié. On appelle $\mathcal{B}$ le quotient de $\mathcal{C}$ par $G_A\subset G_{A,B}$ et on note $\phi:\mathcal{C}\to\mathcal{B}$ le revêtement galoisien associé. On a $\mathrm{Aut}_{\bar{\mathbb{Q}}}(\phi)=G_A$, $\mathrm{Aut}^*_{\bar{\mathbb{Q}}}(\phi)\supset G_{A,B}$ et $\mathrm{Ex}_{\bar{\mathbb{Q}}}(\phi)\supset C_8$. On ne se soucie pas de connaître $\mathrm{Aut}^*_{\bar{\mathbb{Q}}}(\phi)$ exactement car un cocycle de $H^1(\mathbb{Q},C_8)$ se relève dans $H^1(\mathbb{Q},G_{A,B})$ si et seulement si son image dans $H^1(\mathbb{Q},\mathrm{Ex}_{\bar{\mathbb{Q}}}(\phi))$ se relève dans $H^1(\mathbb{Q},\mathrm{Aut}^*_{\bar{\mathbb{Q}}}(\phi))$. Soit alors $I:\mathcal{B}\to\mathcal{B}'$ une tordue de $\mathcal{B}$ telle que les $I^{-1\sigma}I=a_\sigma\in C_8\subset\mathrm{Ex}_{\bar{\mathbb{Q}}}(\phi)$ forment le cocycle $a=(a_\sigma)_\sigma=H^1(\mathbb{Q},C_8)$ construit à la section 3. Le revêtement $\mathbb{T}_{\mathcal{B},\mathcal{B}',I}(\phi)$ est $\psi=I\circ\phi:\mathcal{C}\to\mathcal{B}'$. Les propriétés de relèvement du cocycle a établies à la section 3 prouvent le

Théorème 3 *Il existe une courbe affine lisse, définie sur $\mathbb{Q}$ et géométriquement irréductible, et un $\bar{\mathbb{Q}}$-revêtement de cette courbe, dont le corps des modules est $\mathbb{Q}$, qui admet des modèles sur tous les complétés de $\mathbb{Q}$ mais pas de modèle sur $\mathbb{Q}$.*

On peut bien sûr considérer la complétée projective lisse $\bar{\mathcal{B}}'$ de $\mathcal{B}'$ et étendre le revêtement ψ en un revêtement ramifié de courbes projectives lisses $\bar{\psi}:\bar{\mathcal{C}}\to\bar{\mathcal{B}}'$. Voir [11, I.2]. Cette opération préserve évidemment le corps des modules et les corps de définition (notions qui s'étendent à la catégorie des revêtements ramifiés de $\bar{\mathcal{B}}'$). On en déduit le

Corollaire 1 *Il existe une courbe projective lisse, définie sur $\mathbb{Q}$ et géométriquement irréductible, et un $\bar{\mathbb{Q}}$-revêtement ramifié de cette courbe dont le corps des modules est $\mathbb{Q}$, qui admet des modèles sur tous les complétés de $\mathbb{Q}$ mais pas de modèle sur $\mathbb{Q}$.*

Notons que le genre de $\bar{\mathcal{B}}'$, calculé avec la formule de Hurwitz, vaut 105. Son groupe d'automorphismes est donc fini. Le lemme 2 ci-dessous montre alors qu'il existe une $\mathbb{Q}$-fonction $\nu\in\mathbb{Q}(\bar{\mathcal{B}}')$ sans automorphismes telle que $\lambda=\nu\circ\bar{\psi}:\bar{\mathcal{C}}\to\mathbb{P}^1$ vérifie $\mathrm{Aut}_{\bar{\mathbb{Q}}}(\lambda)=\mathrm{Aut}_{\bar{\mathbb{Q}}}(\bar{\psi})$.

Lemme 1 *Le revêtement λ a les mêmes corps de définition et le même corps des modules que $\bar{\psi}$.*

En effet, de tout $\mathbb{K}$-modèle $\lambda':\mathcal{C}'\to\mathbb{P}^1$ de λ, on déduit un $\mathbb{K}$-modèle

$$\mathcal{C}'/\mathrm{Aut}_{\bar{\mathbb{Q}}}(\lambda')\to\mathbb{P}^1$$

de ν. Il existe donc un $\bar{\mathbb{Q}}$-isomorphisme de revêtements $\omega:\mathcal{C}'/\mathrm{Aut}_{\bar{\mathbb{Q}}}(\lambda')\to\bar{\mathcal{B}}'$ entre $\mathcal{C}'/\mathrm{Aut}_{\bar{\mathbb{Q}}}(\lambda')\to\mathbb{P}^1$ et ν. En fait ω est unique car ν n'a pas d'automorphismes. Donc ω est défini sur $\mathbb{K}$ et $\bar{\mathcal{B}}'$ est $\mathbb{K}$-isomorphe à $\mathcal{C}'/\mathrm{Aut}_{\bar{\mathbb{Q}}}(\lambda')$. On a donc un $\mathbb{K}$-modèle $\mathcal{C}' \to \mathcal{C}'/\operatorname{Aut}_{\bar{\mathbb{Q}}}(\lambda') \xrightarrow{\omega} \bar{\mathcal{B}}'$ de $\bar{\psi}$. Ainsi, de tout $\mathbb{K}$-modèle de λ on déduit un $\mathbb{K}$-modèle de $\bar{\psi}$. La réciproque est évidente. On montre que λ et $\bar{\psi}$ ont même corps des modules par un semblable raisonnement, ou bien, plus simplement encore, en rappelant que le corps des modules est l'intersection des corps de définitions [2]. Cette construction est utilisée dans [3] et [4]. $\square$

On en déduit le

Corollaire 2 *Il existe un $\bar{\mathbb{Q}}$-revêtement ramifié de $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ dont le corps des modules est $\mathbb{Q}$, qui admet des modèles sur tous les complétés de $\mathbb{Q}$ mais pas de modèle sur $\mathbb{Q}$.*

Il nous reste à montrer le

Lemme 2 *Soient $\mathbb{K}$ un corps de nombres, $\mathcal{B}$ et $\mathcal{C}$ deux $\mathbb{K}$-courbes projectives lisses et géométriquement irréductibles et $\psi : \mathcal{C} \to \mathcal{B}$ un $\mathbb{K}$-morphisme non-constant c'est-à-dire un $\mathbb{K}$-revêtement ramifié. On note $\operatorname{Aut}_{\bar{\mathbb{K}}}(\psi)$ le groupe des automorphismes de $\psi \otimes_{\mathbb{K}} \bar{\mathbb{K}}$. On suppose que le genre de $\mathcal{B}$ est au moins 2. Il existe une fonction non constante et sans automorphismes $\nu \in \mathbb{K}(\mathcal{B})$ telle que $\operatorname{Aut}_{\bar{\mathbb{K}}}(\nu \circ \psi) = \operatorname{Aut}_{\bar{\mathbb{K}}}(\psi)$.*

Pour tout automorphisme non trivial $\mathfrak{a} \in \operatorname{Aut}_{\bar{\mathbb{K}}}(\mathcal{B})$ notons $U_{\mathfrak{a}}$ le sous-$\bar{\mathbb{K}}$-espace vectoriel strict de $\bar{\mathbb{K}}(\mathcal{B})$ invariant par $\mathfrak{a}$. On note $U^0_{\mathfrak{a}}$ l'intersection de $U_{\mathfrak{a}}$ et de $\mathbb{K}(\mathcal{B})$. C'est un sous-$\mathbb{K}$-espace vectoriel strict de $\mathbb{K}(\mathcal{B})$.

De même, soit $\mathfrak{b} \in \operatorname{Aut}_{\bar{\mathbb{K}}}(\mathcal{C})$ un automorphisme tel que $\mathfrak{b} \notin \operatorname{Aut}_{\bar{\mathbb{K}}}(\psi)$. On note $V_{\mathfrak{b}} \subset \bar{\mathbb{K}}(\mathcal{B})$ le sous-$\bar{\mathbb{K}}$-espace vectoriel de $\bar{\mathbb{K}}(\mathcal{B})$ des fonctions f telles que $f \circ \psi = f \circ \psi \circ \mathfrak{b}$. C'est un sous-espace vectoriel strict car $\mathfrak{b} \notin \operatorname{Aut}_{\bar{\mathbb{K}}}(\psi)$. On note $V^0_{\mathfrak{b}}$ l'intersection de $V_{\mathfrak{b}}$ et de $\mathbb{K}(\mathcal{B})$. C'est un sous-$\mathbb{K}$-espace vectoriel strict de $\mathbb{K}(\mathcal{B})$.

La réunion $\mathbb{K} \cup_{\mathfrak{a}} U^0_{\mathfrak{a}} \cup \cup_{\mathfrak{b}} V^0_{\mathfrak{b}}$ est une union finie de sous-espaces vectoriels stricts de $\mathbb{K}(\mathcal{B})$. Elle a donc un complémentaire non vide (et même infini). On choisit ν dans ce complémentaire. $\square$

6 Une autre famille de revêtements

Dans cette section, on construit des obstructions globales à la descente pour les $*$-revêtements selon le premier point de la section 2. Observons qu'une telle obstruction peut être obtenue à partir des exemples construits à la section précédente. Il suffit de restreindre les revêtements obtenus à des ouverts non vides sans automorphismes. Plus généralement, un changement de base bien choisi suffit à tuer le groupe d'automorphismes.

On veut construire ici des exemples d'obstructions provenant de la non injectivité de l'application ι du théorème 1, comme nous l'avons expliqué à la fin du premier point de la section 2. Il nous suffit de considérer un quotient de $\mathrm{Br}_2(\mathbb{Q})$ qui viole le principe de Hasse. On va voir que de tels quotients sont légion.

6.1 Principe

Soient A, B et C trois rationnels non nuls tels que -1, A et B soient linéairement indépendants dans $\mathbb{Q}^*/2\mathbb{Q}^*$.

Soit $\sqrt{A}$ la racine carrée de A (la positive si $A > 0$ et celle de partie imaginaire positive sinon). Soit de même $\sqrt{B}$ et $\sqrt{-1}$ et appelons $\mathbb{K}$ le corps octique $\mathbb{Q}(\sqrt{A}, \sqrt{B}, \sqrt{-1})$ engendré par ces trois racines carrées. Soient σ et τ les automorphismes non triviaux de $\mathbb{K}/\mathbb{Q}(\sqrt{-1})$ fixant $\sqrt{B}$ et $\sqrt{A}$ respectivement. Soit μ l'automorphisme non trivial de $\mathbb{K}/\mathbb{Q}(\sqrt{A}, \sqrt{B})$. On note désormais Γ le groupe engendré par σ, μ et τ.

On note E_A le $\Gamma_{\mathbb{Q}}$-groupe cyclique d'ordre 4, décomposé sur $\mathbb{Q}(\sqrt{-A})$ et dont un générateur ϵ_A vérifie ${}^{\sigma}\epsilon_A = \epsilon_A^{-1} = {}^{\mu}\epsilon_A$ et ${}^{\tau}\epsilon_A = \epsilon_A$. On note F_B le $\Gamma_{\mathbb{Q}}$-groupe $< -1, \sqrt{B} > / < B > \subset \bar{\mathbb{Q}}^* / < B >$.

Dans le prochain paragraphe, nous allons construire une $\mathbb{Q}$-courbe $\mathcal{C}$, quasi-projective, lisse et géométriquement irréductible satisfaisant un certain nombre d'exigences que nous énumérons maintenant. Tout d'abord, $\mathcal{C}$ admet deux $\bar{\mathbb{Q}}$-automorphismes notés $\Omega_{\mathcal{C}}$ et $\Theta_{\mathcal{C}}$ tels qu'il existe un isomorphisme de $\Gamma_{\mathbb{Q}}$-groupes $< \Omega_{\mathcal{C}}, \Theta_{\mathcal{C}} > \rightarrow F_B$ qui envoie $\Omega_{\mathcal{C}}$ sur -1 et $\Theta_{\mathcal{C}}$ sur $\sqrt{B}$. Le groupe F_B agit donc sur $\mathcal{C}$ et on demande qu'il agisse sans point fixe. La $\mathbb{Q}$-courbe quotient $\mathcal{C}/ < \Omega_{\mathcal{C}} >$ est appelée $\mathcal{B}$ et on note $\phi : \mathcal{C} \rightarrow \mathcal{B}$ le morphisme quotient. Donc $\mathrm{Aut}_{\bar{\mathbb{Q}}}(\phi) =< \Omega_{\mathcal{C}} >$. De plus $\mathrm{Aut}^*_{\bar{\mathbb{Q}}}(\phi)$ contient $< \Omega_{\mathcal{C}}, \Theta_{\mathcal{C}} >$. L'automorphisme $\Theta_{\mathcal{C}}$ induit un automorphisme de $\mathcal{B}$ noté $\Theta_{\mathcal{B}}$ et $\mathrm{Ex}_{\bar{\mathbb{Q}}}(\phi)$ contient donc $< \Theta_{\mathcal{B}} >$. On demande qu'il existe un $\bar{\mathbb{Q}}$-automorphisme $\Upsilon_{\mathcal{B}}$ de $\mathcal{B}$, sans point fixe et tel que $\Upsilon_{\mathcal{B}}^2 = \Theta_{\mathcal{B}}$. On demande aussi que les $\Gamma_{\mathbb{Q}}$-modules $< \Upsilon_{\mathcal{B}} >$ et E_A soient isomorphes en envoyant $\Upsilon_{\mathcal{B}}$ sur ϵ_A. On demande enfin que le groupe $\mathrm{Aut}_{\bar{\mathbb{Q}}}(\mathcal{B})$ soit exactement égal à $< \Upsilon_{\mathcal{B}} >$, que le groupe $\mathrm{Aut}^*_{\bar{\mathbb{Q}}}(\phi)$ soit exactement égal à $< \Omega_{\mathcal{C}}, \Theta_{\mathcal{C}} >$ et donc que le groupe $\mathrm{Ex}_{\bar{\mathbb{Q}}}(\phi)$ soit exactement $< \Theta_{\mathcal{B}} >$.

La suite exacte

$$1 \rightarrow \mathrm{Ex}_{\bar{\mathbb{Q}}}(\phi) \rightarrow \mathrm{Aut}_{\bar{\mathbb{Q}}}(\mathcal{B}) \rightarrow \mathrm{Aut}_{\bar{\mathbb{Q}}}(\mathcal{B}) / \mathrm{Ex}_{\bar{\mathbb{Q}}}(\phi) \rightarrow 1$$

n'est autre que

$$1 \rightarrow < \Theta_{\mathcal{B}} > \rightarrow < \Upsilon_{\mathcal{B}} > \rightarrow < \Upsilon_{\mathcal{D}} > \rightarrow 1$$

où $\mathcal{D} = \mathcal{B}/\Theta_{\mathcal{B}}$ et $\Upsilon_{\mathcal{D}}$ est l'automorphisme induit par $\Upsilon_{\mathcal{B}}$ sur $\mathcal{D}$.

Cette dernière suite n'est autre que

$$0 \rightarrow C_2 \rightarrow E_A \rightarrow C_2 \rightarrow 0$$

d'où l'on dérive la suite exacte de cohomologie galoisienne

$$\rightarrow H^0(\mathbb{Q}, < \Upsilon_{\mathcal{D}} >) =< \Upsilon_{\mathcal{D}} > \rightarrow H^1(\mathbb{Q}, < \Theta_{\mathcal{B}} >) = \mathbb{Q}^*/2\mathbb{Q}^* \rightarrow H^1(\mathbb{Q}, < \Upsilon_{\mathcal{B}} >) \rightarrow$$

L'image de $\Upsilon_{\mathcal{D}}$ dans $H^1(\mathbb{Q}, < \Theta_{\mathcal{B}} >) = \mathbb{Q}^*/2\mathbb{Q}^*$ est $-A$. Donc le noyau de $\iota : H^1(\mathbb{Q}, < \Theta_{\mathcal{B}} >) \rightarrow H^1(\mathbb{Q}, \mathrm{Aut}_{\mathbb{K}}(\mathcal{B}))$ est $< -A >$.

La suite exacte de l'équation 1 est ici

$$1 \rightarrow < \Omega_{\mathcal{C}} > \rightarrow < \Omega_{\mathcal{C}}, \Theta_{\mathcal{C}} > \rightarrow < \Theta_{\mathcal{B}} > \rightarrow 1$$

qui donne la suite exacte de cohomologie galoisienne

$$\cdots \to H^1(\mathbb{Q}, <\Omega_{\mathcal{C}}, \Theta_{\mathcal{C}}>) \to H^1(\mathbb{Q}, <\Theta_{\mathcal{B}}>) = \mathbb{Q}^*/2\mathbb{Q}^* \to H^2(\mathbb{Q}, <\Omega_{\mathcal{C}}>) \to \dots$$

L'image de $-A \in H^1(\mathbb{Q}, <\Theta_{\mathcal{B}}>) = \mathbb{Q}^*/2\mathbb{Q}^*$ dans $H^2(\mathbb{Q}, <\Omega_{\mathcal{C}}>)$ est le symbole de Hilbert $(-A, B)$. Donc avec les notations de la section 2 on a

$$\mathcal{X}(\mathbb{Q}, \phi) = H^2(\mathbb{Q}, \mathrm{Aut}_{\bar{\mathbb{Q}}}(\phi))/\delta_\phi(\mathrm{Ker}(\iota)) = \mathrm{Br}_2(\mathbb{Q})/(-A, B).$$

On appelle $\mathcal{B}'$ la tordue de $\mathcal{B}$ associée au cocycle

$$C \in \mathbb{Q}^*/2\mathbb{Q}^* = H^1(\mathbb{Q}, <\Theta_{\mathcal{B}}>) \xrightarrow{\iota} H^1(\mathbb{Q}, \mathrm{Aut}_{\bar{\mathbb{Q}}}(\mathcal{B})).$$

Le revêtement $\mathbb{T}^*_{\mathcal{B},\mathcal{B}'}(\mathcal{C} \to \mathcal{B})$ a pour corps des modules $\mathbb{Q}$. L'existence d'un $\mathbb{Q}$-modèle pour ce revêtement dépend de la nullité dans $\mathcal{X}(\mathbb{Q}, \phi)$ de $\mathfrak{d}_\phi(C)$ qui est la classe union des deux symboles de Hilbert (C, B) et $(-AC, B) = (-A, B) + (C, B)$. Cette classe est nulle si et seulement si la variété union disjointe des deux coniques d'équations $X^2 - CY^2 - BZ^2 = 0$ et $X^2 + ACY^2 - BZ^2 = 0$ admet un point rationnel. Une telle union peut violer le principe de Hasse. C'est le cas si (C, B) ni $(-AC, B)$ ne sont nuls et si leurs supports sont disjoints, ce qui revient à dire que le support de (C, B) est contenu dans celui de $(-A, B)$. Alors le revêtement $\mathbb{T}^*_{\mathcal{B},\mathcal{B}'}(\mathcal{C} \to \mathcal{B})$ a un modèle sur tous les complétés de $\mathbb{Q}$ mais pas sur $\mathbb{Q}$.

Exemple numérique : on choisit $A = 1547 = 7 \times 13 \times 17$ et $B = 5$. On vérifie que $(-A, B) = [5, 7, 13, 17]$. Ici un élément d'ordre deux du groupe de Brauer est ici décrit par son support.

On prend $C = -7$ et on vérifie que $(C, B) = (-7, 5) = [7, 5]$ a son support strictement contenu dans celui de $(-A, B) = [5, 7, 13, 17]$ ce qui termine la construction de l'exemple.

6.2 Construction

Nous construisons dans ce paragraphe une courbe satisfaisant les propriétés requises dans le paragraphe précédent.

Soit $\mathcal{Q}$ la quadrique de $\mathbb{A}^4$ d'équation

$$a^2 - Ab^2 + Bc^2 - ABd^2 = \frac{1}{2}. \tag{5}$$

Posons

$$u = a + b\sqrt{A} + \sqrt{B}(c + d\sqrt{A}) = a + c\sqrt{B} + \sqrt{A}(b + d\sqrt{B}).$$

On rappelle que Γ est ici le groupe des automorphismes de $\mathbb{K}/\mathbb{Q}$, engendré par σ, μ et τ.

Ces automorphismes s'étendent à $\mathbb{K}(\mathcal{Q})$ en posant pour tout $\theta \in \Gamma$, $\theta(a) = a$, $\theta(b) = b$, $\theta(c) = c$, $\theta(d) = d$.

Les fonctions a, b, c, d sont des coordonnées de l'espace affine de dimension 4. Il en va de même des fonctions u, ${}^{\sigma}u$, ${}^{\tau}u$, et ${}^{\sigma\tau}u$. Dans ce dernier système de coordonnées l'équation de la quadrique $\mathcal{Q}$ est

$$u^{\sigma}u + {}^{\tau}u^{\sigma\tau}u = 1.$$

On définit des diviseurs D_1, D_σ, D_τ et $D_{\sigma\tau}$ sur $\mathcal{Q}$ en disant que pour tout $\theta \in \Gamma$ le diviseur D_θ a pour équation ${}^{\theta}u = 0$.

Posons $v = \sqrt{A}u^{\tau}u$ et $w = \frac{{}^{\sigma}u}{u}$ et

$$f = -w^{\tau}w = \frac{{}^{\sigma}v}{v} = -\frac{{}^{\sigma}u^{\sigma\tau}u}{u^{\tau}u}. \tag{6}$$

Le diviseur $(f) = D_\sigma + D_{\sigma\tau} - D_1 - D_\tau$ n'étant pas nul dans $\mathrm{Div}(\mathcal{Q})/2\mathrm{Div}(\mathcal{Q})$, on définit une extension quadratique géométrique de $\mathbb{K}(\mathcal{Q})$ en posant

$$Y^2 = f = -w^{\tau}w = \frac{{}^{\sigma}v}{v}$$

et on étend σ, μ et τ en posant $\sigma(Y) = Y^{-1}$ et $\tau(Y) = \mu(Y) = Y$.

Soit alors $\Phi = {}^{\sigma}u + {}^{\tau}uY$. On vérifie que

$${}^{\tau}\Phi\Phi = ({}^{\sigma}u + {}^{\tau}uY)({}^{\sigma\tau}u + uY) = {}^{\sigma}u^{\sigma\tau}u + u^{\tau}uf + Y(u^{\sigma}u + {}^{\tau}u^{\sigma\tau}u) = Y$$

par les équations 5 et 6.

De même

$${}^{\sigma}\Phi\Phi = ({}^{\sigma}u + {}^{\tau}uY)(u + {}^{\sigma\tau}uY^{-1}) = u^{\sigma}u + {}^{\tau}u^{\tau\sigma}u + u^{\tau}uY + {}^{\sigma}u^{\sigma\tau}uY^{-1} = 1.$$

Le diviseur de Φ est

$$\frac{1}{2}(D_\sigma - D_1).$$

Le diviseur de Y est quant à lui

$$\frac{1}{2}(D_\sigma + D_{\sigma\tau} - D_\tau - D_1).$$

Des considérations simples de ramification géométrique, montrent alors que l'on définit une extension biquadratique géométrique de $\mathbb{K}(\mathcal{Q}, Y)$ en posant $y^2 = Y$ et $\xi^2 = \Phi$. On étend σ, τ et μ à $\mathbb{K}(\mathcal{Q}, y, \xi)$ en posant $\sigma(y) = y^{-1}$, $\tau(y) = \mu(y) = y$, $\sigma(\xi) = \xi^{-1}$, $\tau(\xi) = y\xi^{-1}$ et $\mu(\xi) = \xi$.

On note Υ l'automorphisme de $\mathbb{K}(\mathcal{Q}, y)$ qui fixe $\mathbb{K}(\mathcal{Q})$ et envoie y sur $\sqrt{-1}y$. On pose $\Theta = \Upsilon^2$ et Θ s'étend à $\mathbb{K}(\mathcal{Q}, y, \xi)$ en posant $\Theta(\xi) = \xi$. On note Ω l'automorphisme de $\mathbb{K}(\mathcal{Q}, y, \xi)$ qui fixe $\mathbb{K}(\mathcal{Q}, y)$ et envoie ξ sur $-\xi$.

Les propriétés de l'accouplement de Kummer rappelées à la section 4 montrent que le groupe $< \Omega, \Theta >$ est un Γ-module dual de celui engendré par Y et Φ dans $\mathbb{K}(\mathcal{Q}, Y)^*$ modulo les carrés. Plus précisément, l'action de $\sigma, \mu, \tau \in \Gamma$ est donnée par

$$(7) \qquad {}^{\tau}\Theta = \tau\Theta\tau^{-1} = \Theta\Omega \text{ et } {}^{\sigma}\Theta = {}^{\mu}\Theta = \Theta \text{ et } {}^{\sigma}\Omega = {}^{\mu}\Omega = {}^{\tau}\Omega = \Omega.$$

De même

$$(8) \qquad {}^{\sigma}\Upsilon = {}^{\mu}\Upsilon = \Upsilon^{-1} = \Upsilon\Theta \text{ et } {}^{\tau}\Upsilon = \Upsilon.$$

On a le diagramme d'extensions de corps :

$$\begin{tikzcd}
\mathbb{K}(\mathcal{Q}, y, \xi) \arrow[d, dash, "\Theta"] \arrow[dr, dash, "\Omega"] & \\
\mathbb{K}(\mathcal{Q}, Y, \xi) \arrow[dr, dash] & \mathbb{K}(\mathcal{Q}, y) \arrow[d, dash, "\Theta"] \\
& \mathbb{K}(\mathcal{Q}, Y) \arrow[d, dash, "\Upsilon"] \\
& \mathbb{K}(\mathcal{Q})
\end{tikzcd}$$

On note $\mathcal{A}^0$ l'ouvert de $\mathcal{Q}$ complémentaire de $D = D_1 \cup D_\sigma \cup D_\tau \cup D_{\sigma\tau}$.

Le sous-corps de $\mathcal{L} = \mathbb{K}(\mathcal{Q}, y, \xi)$ fixé par $\Gamma = < \sigma, \tau, \mu >$ est noté $\mathcal{L}^0$. On note $\mathcal{C}^0$ la normalisée de $\mathcal{A}^0$ dans $\mathcal{L}^0$. C'est une $\mathbb{Q}$-variété lisse sur laquelle $< \Omega, \Theta >$ agit sans point fixe. On note $\mathcal{B}^0$ le quotient de $\mathcal{C}^0$ par Ω et $\mathcal{D}^0$ le quotient de $\mathcal{C}^0$ par $< \Omega, \Theta >$.

Afin de mieux contrôler les groupes d'automorphismes impliqués, on choisit maintenant un $\mathbb{Q}$-morphisme $\rho : \mathcal{A} \to \mathcal{A}^0$ de variétés.

On reprend les valeurs numériques du précédent paragraphe soit $A = 1547 = 7 \times 13 \times 17$ et $B = 5$. La quadrique $\mathcal{Q}$ a un point rationnel de coordonnées $a = 37/2$, $b = 1/2$, $c = 3$, $d = 0$. Elle est donc rationnelle.

Soit T une coordonnée sur la droite projective c'est-à-dire une fonction telle que $\mathbb{Q}(\mathbb{P}^1) = \mathbb{Q}(T)$. Posons $t = T^3 + T + 716297$ et posons

$$\begin{aligned}
P(T) = Q(t) = (1+5t^2)^{-4}(&246419 - 5279160t + 13489200t^2 + 184770600t^3 \\
&-48645350t^4 - 923853000t^5 + 337230000t^6 + 659895000t^7 + 154011875t^8).
\end{aligned}$$

Soit $\mathcal{A}$ l'ouvert de $\mathbb{P}^1$ défini par l'inéquation

$$P(T) \notin \{0, \infty\}.$$

On prend pour $\rho : \mathcal{A} \to \mathcal{A}^0$ le morphisme non constant et de degré trois sur son image défini par $b(T) = \frac{1}{2}$, $d(T) = 0$,

$$a(T) = \frac{185t^2 - 60t - 37}{2(1+5t^2)} \text{ et } c(T) = \frac{3 - 37t - 15t^2}{1+5t^2}$$

On vérifie que $P(T) = -4u(T)^{\sigma}u(T)^{\tau}u(T)^{\sigma\tau}u(T)$. Donc l'image de ρ est une courbe affine rationnelle contenue dans $\mathcal{A}^0$.

On note $\mathcal{C} \to \mathcal{A}$ le tiré en arrière de $\mathcal{C}^0 \to \mathcal{A}^0$ par $\rho : \mathcal{A} \to \mathcal{A}^0$.

Le revêtement $\mathcal{C} \to \mathcal{A}$ est géométriquement connexe car sa fibre générique a des places géométriques totalement ramifiées. En effet, le numérateur de $P(T)$, qui exprime les données de ramification, est un polynôme *séparable* de degré 24. On note $\Theta_{\mathcal{C}}$ l'automorphisme de $\mathcal{C}$ induit par Θ. On procède ainsi pour tous les automorphismes afin d'éviter les confusions. On note $\mathcal{B}$ le quotient de $\mathcal{C}$ par $\Omega_{\mathcal{C}}$ et $\mathcal{D}$ le quotient de $\mathcal{B}$ par $\Theta_{\mathcal{B}}$. On note $\phi : \mathcal{C} \to \mathcal{B}$ l'application quotient.

Le sous-groupe $< \Upsilon_{\mathcal{B}} >$ de $\mathrm{Aut}_{\bar{\mathbb{Q}}}(\mathcal{B})$ est cyclique d'ordre 4.

Lemme 3 *Le groupe* $\mathrm{Aut}_{\bar{\mathbb{Q}}}(\mathcal{B})$ *des automorphismes de* $\mathcal{B}$ *est exactement égal à* $< \Upsilon_{\mathcal{B}} >$.

En effet $\mathcal{B}$ est revêtement cyclique ramifié de $\mathbb{P}^1$ de degré 4 donné par l'équation $y^4 = \frac{{}^{\sigma}v(T)}{v(T)}$ où $v(T) = \sqrt{A}u(T)^{\tau}u(T)$.

Soit $\mathfrak{a}$ un automorphisme de $\mathcal{B}$. Nous montrons d'abord que $\mathfrak{a}$ normalise $< \Upsilon_{\mathcal{B}} >$ c'est-à-dire que $\bar{\mathbb{Q}}(T) = \bar{\mathbb{Q}}(\mathfrak{a}(T))$.

Comme $\bar{\mathbb{Q}}(T)$ est un sous-corps d'indice 4 de $\bar{\mathbb{Q}}(\mathcal{B}) = \bar{\mathbb{Q}}(y, T)$, si $\bar{\mathbb{Q}}(T) \neq \bar{\mathbb{Q}}(\mathfrak{a}(T))$ alors $\bar{\mathbb{Q}}(T, \mathfrak{a}(T))$ est $\bar{\mathbb{Q}}(T, y^2)$ ou $\bar{\mathbb{Q}}(T, y)$.

Dans le premier cas cela prouve que la courbe $\mathcal{D}$ admet un modèle dans $\mathbb{P}^1 \times \mathbb{P}^1$ de degré 2 en T et en $T' = \mathfrak{a}(T)$. Une telle courbe est de genre arithmétique 1. Mais le genre géométrique de $\mathcal{D}$ est 11, contradiction.

Dans le deuxième cas la courbe $\mathcal{B}$ admet un modèle dans $\mathbb{P}^1 \times \mathbb{P}^1$ de degré 4 en T et en $T' = \mathfrak{a}(T)$. Une telle courbe est de genre arithmétique 9. Mais le genre géométrique de $\mathcal{B}$ est 33, contradiction.

Donc $\bar{\mathbb{Q}}(T) = \bar{\mathbb{Q}}(\mathfrak{a}(T))$. Il existe donc une homographie H qui envoie T sur T'. Cette homographie H stabilise l'ensemble des racines et des pôles de $v^{-1}(T)^{\sigma}v(T)$ qui sont aussi les racines de $P(T)$. Le nombre 10000121 est premier. Le numérateur de $P(T)$ est totalement décomposé modulo 10000121, de racines

$$\{59435, 90886, 233753, 1332408, 1894271, 2674630, 2992629, 3045168, 3309236, 3349763, 3605190, 4902092,$$
$$5038594, 5270020, 6662370, 7983563, 8014964, 8067852, 8086586, 8134787, 8433960, 8604420, 9024050, 9190825\}$$

et on vérifie par un calcul exhaustif mais exact qu'aucune permutation de ces résidus modulo 10000121 n'est induite par une homographie hormis l'identité. Cela finit le calcul du groupe $\mathrm{Aut}_{\bar{\mathbb{Q}}}(\mathcal{B})$. □

Remarque 1 *Les valeurs* 10000121 *et* 716297 *ont été choisies pour que* $P(T)$ *soit totalement décomposable modulo* 10000121*, ce qui simplifie ce calcul. Le changement de variables* $t = T^3 + T + 716297$ *sert uniquement à augmenter le genre de* $\mathcal{B}$ *pour simplifier le calcul de son groupe d'automorphismes. Les valeurs de* A*,* B *et* C *on été choisies pour que* (C, B) *soit non nul et que le support de* $(-A, B)$ *contienne strictement celui de* (C, B)*, ce qui requiert que le support de* $(-A, B)$ *contienne au moins quatre places.*

Il reste à prouver que $\mathrm{Ex}_{\bar{\mathbb{Q}}}(\phi) =< \Theta_{\mathcal{B}} >$ c'est-à-dire $\Upsilon_{\mathcal{B}} \notin \mathrm{Ex}_{\bar{\mathbb{Q}}}(\phi)$. Cela revient à vérifier que $\Phi = {}^{\sigma}u + {}^{\tau}uY$ et $\Upsilon(\Phi) = {}^{\sigma}u - {}^{\tau}uY$ ne sont pas égaux à un carré près dans $\bar{\mathbb{Q}}(T, y)^*$. Or le quotient $\Upsilon(\Phi)/\Phi$ vaut ${}^{\sigma}uu$ à un carré près. Et dans

$\mathrm{Div}(\bar{\mathbb{Q}}(T))/2\mathrm{Div}(\bar{\mathbb{Q}}(T))$, le diviseur de ${}^{\sigma}uu(T)$ est non nul et différent de celui de f.

Enfin, les formules 7 montrent qu'il existe un isomorphisme de $\Gamma_{\mathbb{Q}}$-groupes de $< \Omega_{\mathcal{C}}, \Theta_{\mathcal{C}} >$ dans F_B qui envoie $\Omega_{\mathcal{C}}$ sur -1 et $\Theta_{\mathcal{C}}$ sur $\sqrt{B}$. De même, les formules 8 montrent qu'il existe un isomorphisme de $\Gamma_{\mathbb{Q}}$-groupes de $< \Upsilon_{\mathcal{C}} >$ dans E_A qui envoie $\Upsilon_{\mathcal{C}}$ sur ϵ_A.

Références

[1] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models.* Springer, 1990.

[2] K. Coombes and D. Harbater. Hurwitz families and arithmetic Galois groups. *Duke Math. J.*, 52 :821–839, 1985.

[3] J.-M. Couveignes. Calcul et rationalité de fonctions de Belyi en genre 0. *Ann. Inst. Fourier*, 44 :1–38, 1994.

[4] J.-M. Couveignes. Quelques revêtements définis sur $\mathbb{Q}$. *Manuscripta math.*, 92 :409–445, 1997.

[5] J.-M. Couveignes and L. Granboulan. Dessins from a geometric point of view. In L. Schneps, editor, *The Grothendieck theory of dessins d'enfants.* Cambridge University Press, 1994.

[6] P. Dèbes. Covers of $\mathbb{P}^1$ over the p-adics. *AMS. Contemporary Math.*, 186 :217–328, 1995.

[7] P. Dèbes and J.-C. Douai. Algebraic covers : field of moduli versus field of definition. *Annales scient. ENS*, 4ème série, tome 30 :303–338, 1997.

[8] P. Dèbes and J.-C. Douai. Local-global principle for algebraic covers. *Israel Journal of Math.*, 103 :237–257, 1998.

[9] Geoffroy Derome. Sur le principe local-global des revêtements. *communivation personnelle*, 2003.

[10] G. Gras. *Class field theory.* Springer Verlag, 2003.

[11] G. Malle and B.H. Matzat. *Inverse Galois Theory.* Springer-Verlag, 1999.

[12] Layla Pharamond. Comparaison de deux notions de rationalité d'un dessin d'enfant. *Journal de théorie des nombres de Bordeaux*, 13(2) :529–538, 2001.

[13] Bounab Sadi. *Descente effective du corps de définition des revêtements.* Thèse de doctorat, sous la direction de Pierre Dèbes. Université des Sciences et Technologies de Lille, 1999.

[14] J.-P. Serre. *Groupes algébriques et corps de classes.* Hermann, 1959.

[15] J.-P. Serre. *Corps locaux.* Hermann, 1962.

[16] J.-P. Serre. *Cohomologie galoisienne.* Springer, 1991.

[17] André Weil. The field of definition of a variety. *Amer. J. Math.*, 78 :509–524, 1956.