Courbes hyperelliptiques à multiplications réelles et une construction de Shih

Henri DARMON et Jean-François MESTRE

H.D.: Département de Mathématiques,
Université McGill, 805 Rue Sherbrooke Ouest, Montréal H3A-2K6, Canada;
E-mail: darmon@math.mcgill.ca

J-F.M.: Département de Mathématiques
Université de Paris VII (Denis Diderot), 75221 Paris, France.
E-mail: mestre@math.jussieu.fr

Résumé.- Soient r et p deux nombres premiers distincts, soit $K = \mathbb{Q}(\cos\frac{2\pi}{r})$, et soit $\mathbb{F}$ le corps résiduel de K en une place au-dessus de p. Lorsque l'image de $(2-2\cos\frac{2\pi}{r})$ dans $\mathbb{F}$ n'est pas un carré, nous donnons une construction géométrique d'une extension réguliere de $K(t)$ de groupe de Galois $\mathbf{PSL}_2(\mathbb{F})$. Cette extension correspond à un revêtement de $\mathbb{P}^1_{/K}$ de "signature (r,p,p)" au sens de [3], sec. 6.3, et son existence est prédite par le critère de rigidité de Belyi, Fried, Thompson et Matzat. Sa construction s'obtient en tordant la representation galoisienne associée aux points d'ordre p d'une famille de variétés abéliennes à multiplications réelles par K découverte par Tautz, Top et Verberkmoes [6]. Ces variétés abéliennes sont définies sur un corps quadratique, et sont isogènes à leur conjugué galoisien. Notre construction généralise une méthode de Shih [4,5], que l'on retrouve quand $r = 2$ et $r = 3$.

Hyperelliptic curves with real multiplications and a construction of Shih.

Abstract.- *Let r and p be distinct prime numbers, let $K = \mathbb{Q}(\cos\frac{2\pi}{r})$, and let $\mathbb{F}$ be the residue field of K at a place above p. When the image of $(2-2\cos\frac{2\pi}{r})$ in $\mathbb{F}$ is not a square, we describe a geometric construction of a regular extension of $K(t)$ with Galois group $\mathbf{PSL}_2(\mathbb{F})$. This extension corresponds to a covering of $\mathbb{P}^1_{/K}$ of "signature (r,p,p)" in the sense of [3], sec. 6.3, and its existence is predicted by the rigidity criterion of Belyi, Fried, Thompson and Matzat. Its construction is obtained by twisting the mod p galois representation attached to a family of abelian varieties with real multiplications by K discovered by Tautz, Top and Verberkmoes [6]. These abelian varieties are defined in general over a quadratic field, and are isogenous to their galois conjugate. Our construction generalises a method of Shih*

[4,5], which one recovers when $r = 2$ and $r = 3$.

1 Rigidité dans $\mathbf{PSL}_2(\mathbb{F})$

Soit r un nombre premier, et soit $\mathcal{C}$ un corps algébriquement clos de caractéristique zéro. On choisit une racine primitive r-ème (resp. 4-ème) de l'unité ζ dans $\mathcal{C}$ si r est impair (resp. $r = 2$), et on pose $\omega = \zeta + \zeta^{-1}$. Soit $K = \mathbb{Q}(\omega)$ le sous-corps réel du corps cyclotomique $\mathbb{Q}(\zeta)$, soit d son degré sur $\mathbb{Q}$, et soit $\mathcal{O}$ son anneau des entiers.

On se donne un corps $\mathbb{F}$ de caractéristique $p \neq r$ muni d'un homomorphisme surjectif $\varphi : \mathcal{O} \longrightarrow \mathbb{F}$. Le corps $\mathbb{F}$ est donc une extension finie de $\mathbb{F}_p$ de cardinalité p^f, où f est l'ordre de p dans $(\mathbb{Z}/r\mathbb{Z})^\times/\langle\pm 1\rangle$. Posons $G = \mathbf{PSL}_2(\mathbb{F})$. C'est un groupe fini simple lorsque $p^f > 3$, ce que l'on supposera désormais.

Le groupe G possède d classes de conjugaison d'éléments d'ordre r. (En effet, une matrice d'ordre r dans $\mathbf{SL}_2(\mathbb{F})$ est déterminée à conjugaison près par sa trace, qui est égale à $\varphi(\omega^\sigma)$ pour un choix de $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.) Ces classes sont rationnelles sur le corps K au sens de [3], sec. 7.1., et sont permutées transitivement par $\mathrm{Gal}(K/\mathbb{Q})$. Empruntant les notations de l'atlas des groupes finis [1], appelons rA la classe de conjugaison d'éléments d'ordre r dans G représentés par une matrice de trace $\bar{\omega} := \varphi(\omega)$.

Si $p = 2$, le groupe G possède une seule classe de conjugaison d'éléments d'ordre p, contenant les matrices unipotentes. Si p est impair, alors G possède deux classes de conjugaisons d'éléments d'ordre p. La première, appelée pA, contient l'élément représenté par la matrice unipotente $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et la seconde, appelée pB, contient l'élément représenté par une matrice de la forme $\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}$ où γ appartient à $\mathbb{F}^\times - \mathbb{F}^{\times 2}$ (cf. [3], sec. 7.4.3). Lorsque f est pair, ces deux classes sont rationnelles sur $\mathbb{Q}$. Lorsque f est impair, elles sont rationnelles sur le corps $\mathbb{Q}(\sqrt{p^*})$ où $p^* := (-1)^{\frac{p-1}{2}}p$, et elles sont conjuguées l'une de l'autre sous l'action de $\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$.

Si $(\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3)$ est un triplet de classes de conjugaison dans G, on désigne par $\Sigma(\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3)$ l'ensemble des triplets $(x, y, z) \in \mathfrak{c}_1 \times \mathfrak{c}_2 \times \mathfrak{c}_3$ tels que x, y, z engendrent G et satisfont la relation $xyz = 1$. Le groupe G opère librement

sur $\Sigma(\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3)$ par conjugaison. On dit que le triplet $(\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3)$ est *rigide* si l'action de G sur $\Sigma(\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3)$ est transitive.

Proposition 1.1 *Si $p = 2$ ou si l'élément $2 - \bar{\omega}$ est un carré dans $\mathbb{F}$, alors $\Sigma(rA, pA, pB) = \emptyset$. Autrement, le triplet (rA, pA, pB) est rigide.*

Démonstration: On procède exactement comme dans [3], prop. 7.4.3 et 7.4.4 où sont traités les cas $r = 2$ et $r = 3$. Supposons désormais que r est impair. Alors les solutions de l'équation $xyz = 1$ avec $x \in rA$, $y \in pA$, et z d'ordre p sont conjugués à l'image dans $\mathbf{PSL}_2(\mathbb{F})$ d'un des deux triplets suivants:

$$\left(\begin{pmatrix} 1 & -1 \\ 2+\bar{\omega} & -1-\bar{\omega} \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -(2+\bar{\omega}) & 1 \end{pmatrix} \right), \tag{1}$$

$$\left(\begin{pmatrix} 1 & -1 \\ 2-\bar{\omega} & -1+\bar{\omega} \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -(2-\bar{\omega}) & 1 \end{pmatrix} \right). \tag{2}$$

Si $p = 2$, les éléments de chaque triplet engendrent un sous-groupe diédral d'ordre $2r$, et $\Sigma(rA, 2A, 2A) = \emptyset$. Si $p = 3$ et $r = 5$, les éléments du triplet (1) engendrent un sous-groupe exceptionnel de $\mathbf{PSL}_2(\mathbb{F}_9) \simeq A_6$ isomorphe à A_5, et $\Sigma(5A, 3A, 3A) = \emptyset$. Hormis ces exceptions, le sous-groupe de G engendré par les éléments de chaque triplet ne peut être contenu dans aucun des sous-groupes maximaux de G, dont on connaît la liste complète. Le triplet (1) appartient donc à $\Sigma(rA, pA, pA)$ puisque $2 + \omega$ est un carré dans $\mathcal{O}$. Quant au triplet (2), il appartient à $\Sigma(rA, pA, pB)$ si et seulement si $2 - \bar{\omega}$ n'est pas un carré dans $\mathbb{F}$.

On appelle G-revêtement de $\mathbb{P}_1$ (sur $\mathcal{C}$) un revêtement galoisien connexe $X \longrightarrow \mathbb{P}_1$ défini sur $\mathcal{C}$ et muni d'une identification de G avec $\mathrm{Gal}(X/\mathbb{P}_1)$. Un tel revêtement est dit de type (r, p, p) s'il est non-ramifié en dehors de 3 points P_1, P_2, P_3 et si les indices de ramification au-dessus de ces trois points sont égaux à r, p, et p respectivement. Etant donné un tel revêtement, appelons I_1, I_2, et I_3 le sous-groupe d'inertie en un point au-dessus de P_1, P_2, et P_3 respectivement. Le choix de ζ détermine un générateur σ_1 de I_1, et le choix d'une racine primitive p-ème de l'unité détermine des générateurs σ_2 et σ_3 de I_2 et I_3. L'élément $\sigma_i \in G$ dépend du choix d'un point de X au-dessus de P_i, mais il est bien défini à conjugaison près. On dit que le G-revêtement X est de type (rA, pA, pB) si σ_1, σ_2, et σ_3 appartiennent aux classes rA, pA, et pB respectivement. On peut alors s'arranger pour que le triplet $(\sigma_1, \sigma_2, \sigma_3)$

appartienne à $\Sigma(rA, pA, pB)$. (Cf. [3], th. 6.3.2.) La proposition 1.1 implique donc qu'un revêtement de type (rA, pA, pB) existe si et seulement si $p \neq 2$ et $2 - \bar{\omega}$ n'est pas un carré dans $\mathbb{F}$, et qu'il est alors unique, à un isomorphisme unique près, une fois P_1, P_2 et P_3 fixés.

On dit qu'un G-revêtement est défini sur un sous-corps de $\mathcal{C}$ si le revêtement $X \longrightarrow \mathbb{P}_1$ et les automorphismes dans $\mathrm{Gal}(X/\mathbb{P}_1)$ sont définis sur ce corps. Grâce au critère de rigidité de Matzat (cf. [3], sec. 8.1 et 8.2) on a la proposition suivante:

Proposition 1.2 *Si $p \neq 2$ et si $2 - \bar{\omega}$ n'est pas un carré dans $\mathbb{F}$, alors il existe un G-revêtement de $\mathbb{P}_1$ de type (rA, pA, pB) défini sur K. On peut s'arranger pour que ce revêtement soit ramifié en ∞ et ± 1 si f est pair, et en ∞ et $\pm\sqrt{p^*}$ si f est impair. Le G-revêtement ainsi obtenu est alors unique à un isomorphisme unique près.*

On se propose de donner une construction géométrique du G-revêtement dont l'existence est prédite par la proposition 1.2. Cette construction se fait en considérant l'action de Galois sur les points d'ordre p des Jacobiennes d'une famille de courbes hyperelliptiques de genre d à multiplications réelles par K. Lorsque f est impair, ces jacobiennes sont définies sur $\mathbb{Q}(\sqrt{p^*})$ et sont $(2-\omega)$-isogènes à leur conjugué galoisien, ce qui "explique" l'hypothèse qui apparaît dans les propositions 1.1 et 1.2. Notons que cette construction généralise un procédé de Shih, que l'on retrouve d'ailleurs quand $r = 2$ et $r = 3$. (Cf. [4], [5], ou [3], ch. 5.)

2 Courbes hyperelliptiques

On supposera désormais que r est impair et que $p \neq 2, r$. Soit $g(x)$ le polynôme caractéristique de $-\omega$, et soit $f(x)$ une primitive du polynôme $(-1)^d r g(x) g(-x)$. Par exemple, on choisira

$$f(x) = xg(x^2 - 2) = g(-x)^2(x - 2) + 2 = g(x)^2(x + 2) - 2.$$

Soient C_1 et C_2 les courbes hyperelliptiques de genre d sur $\mathbb{Q}(t)$ considérées dans [6], données par les équations

$$C_1(t) \quad : \quad y^2 = f(x) - 2t, \tag{3}$$
$$C_2(t) \quad : \quad y^2 = (x + 2)(f(x) - 2t), \tag{4}$$

et soient J_1 et J_2 (ou encore $J_1(t)$ et $J_2(t)$) leurs jacobiennes sur $\mathbb{Q}(t)$.

Proposition 2.1 *Les variétés abéliennes J_1 et J_2 admettent des multiplications réelles par K. Plus précisément, on a $\mathrm{End}_{\mathcal{C}(t)}(J_i) \simeq \mathcal{O}$. Les endomorphismes de J_i sont définis sur K, et l'action de $\mathrm{Gal}(K/\mathbb{Q})$ sur $\mathrm{End}(J_i)$ est compatible à son identification avec $\mathcal{O}$.*

Démonstration: Cette proposition est démontrée par Tautz, Top et Verberkmoes, cf. le théorème 1 et la remarque à la fin de la section 2 de [6]. On rappelle ici les grandes lignes de leur démonstration. On considère les courbes

$$D_1 : y^2 = x^r + 1/x^r - 2t, \qquad D_2 : y^2 = x^{2r} - 2tx^r + 1.$$

Ce sont des courbes munies d'un automorphisme $[\zeta]$ d'ordre r qui à x associe ζx, ainsi que d'une involution τ_i définie par

$$\tau_1(x, y) = (\frac{1}{x}, y), \qquad \tau_2(x, y) = (\frac{1}{x}, \frac{y}{x^r}).$$

Ces automorphismes satisfont la relation de commutation $\tau_i[\zeta] = [\zeta^{-1}]\tau_i$, et engendrent donc un groupe dihédral d'ordre $2r$. Les morphismes de degré deux

$$\pi_1(x, y) = (x + \frac{1}{x}, y), \qquad \pi_2(x, y) = (x + \frac{1}{x}, (y + \frac{y}{x^r})/g(x + \frac{1}{x}))$$

de $D_i(t)$ vers $C_i(t)$ satisfont $\pi_i\tau_i = \pi_i$, et identifient donc C_i à D_i/τ_i. L'application $D_i \longrightarrow C_i \times C_i$ donnée par

$$P \mapsto (\pi_i P, \pi_i[\zeta]P)$$

définit une correspondance η_ζ de C_i vers C_i décrite par la formule

$$\eta_\zeta(Q) = (\pi_i[\zeta]P) + (\pi_i[\zeta^{-1}]P), \tag{5}$$

où $P \in D_i$ est tel que $\pi_i(P) = Q$. On remarque que $\eta_\zeta^\sigma = \eta_{\zeta^\sigma}$ pour tout $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, et que $\eta_\zeta = \eta_{\zeta^{-1}}$. Par conséquent η_ζ est défini sur K. La formule (5) montre aussi que l'application de $\mathcal{O}$ vers $\mathrm{End}(J_i)$ qui à ω associe η_ζ établit une inclusion de $\mathcal{O}$ dans $\mathrm{End}(J_i)$.

Proposition 2.2 *1. Les courbes C_1 et C_2 ont bonne réduction en dehors de $t = \infty$ et $t = \pm 1$.*

2. *Ce sont des* courbes de Mumford *en $t = \pm 1$, c'est-à-dire que leurs fibres spéciales sur $K[[t-1]]$ et $K[[t+1]]$ sont des unions de droites projectives qui se coupent transversalement en des points doubles ordinaires.*

3. *Elles ont potentiellement bonne réduction en $t = \infty$. Plus précisément,*

   - *la courbe C_1 possède une tordue par l'involution hyperelliptique qui acquiert bonne réduction sur $\mathcal{C}((1/t^{\frac{1}{r}}))$;*
   - *la courbe C_2 acquiert bonne réduction sur $\mathcal{C}((1/t^{\frac{1}{r}}))$.*

Cela se vérifie par un calcul direct.

On remarque que la fonction $(x, y) \mapsto (-x, y)$ est un isomorphisme entre $C_1(t)$ et $C_1(-t)$. Par contre $C_2(t)$ n'est pas isomorphe à $C_2(-t)$. (Cela peut se voir lorsque $r = 5$ en calculant les invariants d'Igusa associés aux courbes $C_2(t)$ et $C_2(-t)$ qui sont de genre 2. Plus généralement, on observe que les fibres spéciales d'un modèle minimal de $C_2(t)$ en $t = 1$ et $t = -1$ ne sont pas isomorphes.) Par contre, on a:

Proposition 2.3 *Il existe une isogénie $\eta : J_2(t) \longrightarrow J_2(-t)$ qui satisfait*

$$\eta(-t)\eta(t) = \omega - 2.$$

En particulier, η est de degré r: son noyau est un sous-groupe cyclique des points de $(2 - \omega)$-torsion de J_2.

Démonstration: La fonction $\alpha : D_2 \longrightarrow C_2(-t)$ définie par

$$\alpha(x, y) = (-x - \frac{1}{x}, (y - \frac{y}{x^r})/g(-x - \frac{1}{x}))$$

identifie $C_2(-t)$ au quotient $D_2(t)/w\tau_2$, où w est l'involution hyperelliptique de D_2 (qui commute avec τ_2). Soit s un entier qui satisfait $2s \equiv 1 \pmod{r}$. La correspondance $D_2(t) \longrightarrow C_2(t) \times C_2(-t)$ de $C_2(t)$ vers $C_2(-t)$ définie par

$$P \mapsto (\pi_2 P, \alpha[\zeta^s]P)$$

induit un morphisme η de $J_2(t)$ vers $J_2(-t)$, et on vérifie que

$$\eta(-t)\eta(t) = \omega - 2.$$

3 Représentations galoisiennes et revêtements

Après le choix d'une identification de $\mathcal{O}$ avec $\mathrm{End}(J_i)$, le module $H := H_1(J_i, \mathbb{Q})$ devient un K-espace vectoriel de dimension deux. Par la proposition 2.2, la monodromie en $t = \infty$ correspondant à $-\zeta$ détermine une transformation d'ordre $2r$ (resp. r) de $\mathrm{Aut}_K(H)$ quand $i = 1$ (resp. $i = 2$). On fixe l'identification de $\mathcal{O}$ avec $\mathrm{End}(J_i)$ de sorte à ce que cette transformation soit de trace $-\omega$ (resp. ω).

Soit V_i $(i = 1, 2)$ le module $(J_i)_p \otimes_\varphi \mathbb{F}$. C'est un $\mathbb{F}$-espace vectoriel de dimension 2, et l'action de $\mathrm{Gal}(\overline{\mathcal{C}(t)}/\mathcal{C}(t))$ sur V_i détermine une représentation galoisienne

$$\rho_i : \mathrm{Gal}(\overline{\mathcal{C}(t)}/\mathcal{C}(t)) \longrightarrow \mathbf{SL}_2(\mathbb{F}). \tag{6}$$

Soit $\bar{\rho}_i$ la représentation projective déduite de ρ_i, et soit X_i le revêtement qui lui est associé.

Proposition 3.1 *Les courbes X_1 et X_2 sont des revêtements de type (r, p, p) en $(P_1, P_2, P_3) = (\infty, 1, -1)$. Plus précisément, après un choix convenable de racine p-ème de l'unité, on a:*

1. *La courbe X_1 est un G-revêtement de type (rA, pA, pA) si $(p, r) \neq (3, 5)$. (Son groupe de Galois est isomorphe à $A_5 \subset \mathbf{PSL}_2(\mathbb{F}_9)$ si $(p, r) = (3, 5)$.)*

2. *La courbe X_2 est un G-revêtement de type (rA, pA, pA) si $2 - \bar{\omega}$ est un carré dans $\mathbb{F}$, et de type (rA, pA, pB) autrement.*

Démonstration: Comme la courbe C_i a bonne réduction en dehors de $t = \infty$ et ± 1, le revêtement X_i est non-ramifié en dehors de ces trois points. La proposition 2.2, 3, implique que $\bar{\rho}_i$ envoie le groupe d'inertie en $t = \infty$ sur un sous-groupe de G d'ordre r, et le revêtement X_i est donc ramifié d'ordre r au-dessus de $t = \infty$. La proposition 2.2, 2, implique par la théorie de Mumford que la Jacobienne J_i a réduction purement multiplicative en $t = \pm 1$. La monodromie de X_i autour de ces points est donc unipotente, ou triviale. Elle ne peut être triviale en $t = 1$ ou $t = -1$, car l'hypothèse $p \neq r$ forcerait X_i a être ramifié nulle part, alors qu'on sait qu'il est ramifié en $t = \infty$. Par conséquent, X_i est de type (r, p, p) en $(\infty, 1, -1)$. La démonstration de la proposition 1.1 implique alors que l'homomorphisme $\bar{\rho}_i$ est surjectif,

du moins lorsque $(p,r) \neq (3,5)$. Il munit donc X_i d'une structure de G-revêtement. Soit $\sigma_\infty \in \mathbf{SL}_2(\mathbb{F})$ l'image par ρ_i du générateur de l'inertie en $t=\infty$ correspondant à l'élément $-\zeta$. Le choix de l'identification de $\mathcal{O}$ avec $\mathrm{End}(J_i)$ fixé plus haut implique que σ_∞ a pour trace $-\bar{\omega}$ (resp. $\bar{\omega}$) quand $i=1$ (resp. $i=2$). Soit ζ_p une racine p-ème de l'unité, et soit $\sigma_1 \in \mathbf{SL}_2(\mathbb{F})$ l'image par ρ_i du générateur de l'inertie en $t=1$ correspondant à ζ_p. On choisit ζ_p de sorte à ce que σ_1 appartienne à la classe de conjugaison pA. Finalement soit σ_{-1} l'image du générateur de l'inertie en $t=-1$ (correspondant à ζ_p). Les éléments σ_∞, σ_1 et σ_{-1} ne sont définis qu'à conjugaison près; on s'arrange pour qu'ils satisfassent la relation $\sigma_\infty\sigma_1\sigma_{-1}=1$. Par le même raisonnement que dans la démonstration de la proposition 1.1, on voit que le triplet $(\sigma_\infty,\sigma_1,\sigma_{-1})$ est conjugué au triplet (1) (resp. (2)) quand $i=1$ (resp. $i=2$), ce qui achève la démonstration de la proposition 3.1.

Remarques:
1. La démonstration de la proposition 3.1 montre que les revêtements X_1 et X_2 fournissent une *liste complète* des G-revêtements de type (r,p,p).
2. En particulier, pour $i=1,2$ les représentation galoisiennes $\rho_i(t)$ et $\rho_i(-t)$ sont isomorphes. Il s'ensuit par la conjecture d'isogénie sur le corps de fonctions $\mathcal{C}(t)$ que $J_i(t)$ est isogène à $J_i(-t)$ sur $\mathcal{C}(t)$. Comme le revêtement $\bar{\rho}_2(t)$ est de type (rA,pA,pB) pour une infinité de p, on sait que $J_2(t)$ n'est pas isomorphe à $J_2(-t)$ sur $\mathcal{C}(t)$. De plus, la restriction de $\rho_2(t)$ à $\mathrm{Gal}(\overline{\mathcal{C}(t)}/\mathcal{C}(t))$ est irréductible pour tout $p \neq r$. Par conséquent $J_2(t)$ est lié à $J_2(-t)$ par une isogénie de degré une puissance de r. Ces considérations auraient permis d'anticiper ce qui est démontré dans la prop. 2.3 par un calcul direct.

4 La construction de Shih

Puisque J_i est défini sur $\mathbb{Q}$ et que l'action de $\mathcal{O}$ sur J_i est définie sur K, la représentation ρ_i de l'équation (6) se prolonge en une représentation galoisienne (que l'on dénotera par le même symbole, par abus de notation)

$$\rho_i : \mathrm{Gal}(\overline{K(t)}/K(t)) \longrightarrow \mathbf{GL}_2(\mathbb{F}).$$

Comme ρ_i provient des points de p-division d'une variété abélienne, on a de plus

$$\det(\rho_i) = \chi_p,$$

où $\chi_p : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathbb{F}_p^\times$ est le caractère cyclotomique donnant l'action de Galois sur les racines p-èmes de l'unité.

Soit

$$\bar{\rho}_i : \mathrm{Gal}(\overline{K(t)}/K(t)) \longrightarrow \mathbf{PGL}_2(\mathbb{F})$$

la représentation projective déduite de ρ_i, et soit L_i l'extension de $K(t)$ fixée par le noyau de $\bar{\rho}_i$.

Si f est pair, alors $\mathbb{F}_p^\times \subset (\mathbb{F}^\times)^2$, et l'image de $\bar{\rho}_i$ est donc contenue dans $\mathbf{PSL}_2(\mathbb{F})$; les extensions L_1 et L_2 sont alors des extensions régulières de $K(t)$ de groupe de Galois G. Les revêtements X_1 et X_2 correspondant à ces extensions sont les deux G-revêtements distincts de type (r, p, p) définis sur K et ramifiés en ∞ et ± 1. En particulier, lorsque $2 - \bar{\omega}$ n'est pas un carré, le revêtement X_2 est celui dont l'existence est prédite par la proposition 1.2.

Lorsque f est impair, l'image de $\bar{\rho}_i$ n'est plus contenue dans $\mathbf{PSL}_2(\mathbb{F})$. On a alors $L_i \cap \bar{K} = K(\sqrt{p^*})$, et l'extension L_i n'est pas régulière sur $K(t)$.

Pour traiter ce cas, on considère la variété abélienne $J := J_2(t/\sqrt{p^*})$. C'est une variété définie sur $K(t, \sqrt{p^*})$ qui est isogène à son conjugué galoisien $J' := J(-t/\sqrt{p^*})$ sur $K(t)$. En effet, par la proposition 2.3, $\eta := \eta(t/\sqrt{p^*})$ est une isogénie de degré r entre J et J'. On pose $\eta' = \eta(-t/\sqrt{p^*})$. L'action de $\mathrm{Gal}(K(t, \sqrt{p^*})/K(t))$ interchange J et J', ainsi que η et η'.

On pose comme avant $V := J_p \otimes_\varphi \mathbb{F}$, et $V' := J'_p \otimes_\varphi \mathbb{F}$. Parce que p est différent de r, l'isogénie η' induit un isomorphisme

$$\alpha : V' \longrightarrow V$$

de $\mathbb{F}$-espaces vectoriels.

L'action de $\mathrm{Gal}(\overline{K(t)}/K(t, \sqrt{p^*}))$ sur V donne lieu à une représentation galoisienne

$$\rho : \mathrm{Gal}(\overline{K(t)}/K(t, \sqrt{p^*})) \longrightarrow \mathrm{Aut}_{\mathbb{F}}(V).$$

On étend ρ à une fonction sur $\mathrm{Gal}(\overline{K(t)}/K(t))$ en posant

$$\tilde{\rho}(\sigma) = \alpha\sigma, \quad \text{quand } \sigma(\sqrt{p^*}) = -\sqrt{p^*}.$$

En se servant de la proposition 2.3, on vérifie alors que

$$\begin{aligned} \tilde{\rho}(\sigma_1)\tilde{\rho}(\sigma_2) &= (\bar{\omega} - 2)\tilde{\rho}(\sigma_1\sigma_2), \quad \text{si } \sigma_1(\sqrt{p^*}) = \sigma_2(\sqrt{p^*}) = -\sqrt{p^*}; \\ \tilde{\rho}(\sigma_1)\tilde{\rho}(\sigma_2) &= \tilde{\rho}(\sigma_1\sigma_2), \quad \text{autrement.} \end{aligned}$$

Ainsi, la fonction $\tilde{\rho}$ n'est pas un homomorphisme, mais sa projectivisée $\bar{\rho}$ l'est. Après le choix d'une base de V sur $\mathbb{F}$, on obtient ainsi un homomorphisme

$$\bar{\rho} : \mathrm{Gal}(\overline{K(t)}/K(t)) \longrightarrow \mathbf{PGL}_2(\mathbb{F}).$$

Soit

$$\det(\bar{\rho}) : \mathrm{Gal}(\overline{K(t)}/K(t)) \longrightarrow \mathbb{F}^\times/(\mathbb{F}^\times)^2 = \pm 1$$

le caractère d'ordre 2 obtenu à partir du déterminant de $\bar{\rho}$. La proposition suivante se démontre comme la proposition 5.2.1 de [3], sec. 5.2.

Proposition 4.1 *Soit $\epsilon_p : \mathrm{Gal}(\overline{K(t)}/K(t)) \longrightarrow \pm 1$ le caractère quadratique associé à l'extension $K(t, \sqrt{p^*})$. Alors on a*

$$\begin{aligned} \det(\bar{\rho}) &= \epsilon_p, \ \textit{si } 2 - \bar{\omega} \textit{ est un carré dans } \mathbb{F}. \\ &= 1, \ \textit{si } 2 - \bar{\omega} \textit{ n'est pas un carré dans } \mathbb{F}. \end{aligned}$$

Soit L l'extension de $K(t)$ fixée par le noyau de $\bar{\rho}$. La proposition 4.1 montre que L est une G-extension régulière de $K(t)$ lorsque $2 - \bar{\omega}$ n'est pas un carré. Cette extension est ramifiée en ∞ et $\pm\sqrt{p^*}$; c'est donc le corps de fonctions du revêtement rigide de type (rA, pA, pB) de la proposition 1.2.

Remerciements: Le premier auteur remercie l'Université Paris VI et l'Institut Henri Poincaré pour leur hospitalité pendant l'élaboration de cet article, ainsi que le CRSNG, le FCAR et la fondation Sloan pour leur soutien financier.

Références bibliographiques

[1] Conway J.H., Curtis R.T., Norton S.P., Parker R.A., et Wilson R.A., *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups.* Clarendon Press, New York. 1985.

[2] Mestre, J.F., Familles de courbes hyperelliptiques à multiplications réelles, *Arithmetic algebraic geometry* (Texel, 1989), 193–208, Progr. Math., **89**, Birkhäuser Boston, Boston, MA 1991.

[3] Serre, J.-P., *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992.

[4] Shih, K-y., On the construction of Galois extensions of function fields and number fields, *Math. Ann.* **207**, 1974, 99–120.

[5] Shih, K-y., p-division points on certain elliptic curves, *Comp. Math.* **36**, 1978, 113–129.

[6] Tautz, W., Top, J., Verberkmoes, A., Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.* **43**, no. 5, 1991, 1055–1064.