Espaces de modules de revêtements en caractéristique positive : Modules des courbes de Potts

Matthieu ROMAGNY

17 mai 2001

Prépublication de l'Institut Fourier n° 535 (2001)
http ://www.fourier.ujf-grenoble.fr/prepublications.html

Moduli of Potts N-state curves

Abstract : In this note we study, with special attention to positive characteristic, the modular properties of a certain family of cyclic coverings of $\mathbf{P}^1$ with prescribed Hurwitz ramification data, previously studied by S-S. Roan [Ro] over the complex field. Namely we provide an example of an algebraic stack of wildly ramified covers whose moduli space has good reduction. In the first two sections we compute thoroughly the automorphism group of these curves, provided that the level N and the characteristic p are both prime to 2. On the way, we note an (expectable) important difference when dealing with the case $p|N$. Then in the third section we show, in the "tame" case (N prime to p), that there is a coarse moduli space, describe its cusps, and calculate the Picard group of the moduli problem. Finally, back to the case $p|N$ in the last section, we complete our work giving, in that situation also, the existence of a moduli space 1) over an algebraically closed field k of characteristic p, and 2) over a ring of Witt vectors of k. The latter has good reduction at the maximal ideal.

Dans ce travail on souhaite illustrer dans une situation concrète, assez simple pour pouvoir pousser l'investigation, les difficultés qui interviennent dans les problèmes modulaires des revêtements en caractéristique positive, ou en caractéristique mixte.

Les courbes auxquelles nous nous intéressons sont des courbes algébriques qui interviennent en Mécanique Statistique, où elles apparaissent comme surfaces de Riemann paramétrant un modèle dit *de Potts chiral à N états intégrable*. Dans [Ro], S-S. Roan présente le contexte physique duquel émergent ces courbes, et oriente son travail vers deux buts principaux : caractériser géométriquement les courbes de Potts parmi les courbes hyperelliptiques, et décrire la jacobienne d'une courbe de Potts à l'aide de ses symétries.

Nos motivations sont tout autres : ce sont les propriétés arithmétiques et modulaires qui font l'objet de notre discussion, notamment, l'étude des champs associés aux courbes de Potts, de leurs espaces modulaires et de leur réduction modulo p. En particulier, il est intéressant de disposer d'un exemple (ils sont encore peu nombreux) de champ algébrique de Hurwitz en caractéristique mixte : il s'agit du champ des courbes de Potts à $N = p$ états sur l'anneau des vecteurs de Witt d'un corps algébriquement clos de caractéristique $p > 0$ (section 4.2).

Il est à noter que des théorèmes généraux assurent l'existence d'un espace modulaire grossier (qui est en fait un espace algébrique) pour des champs algébriques séparés [KeMo]. Un tel espace exhibé en toute généralité est difficile à appréhender et à manipuler. Par contraste, nous proposons ici une construction « explicite » des espaces modulaires, qui présente l'avantage de répondre ensuite simplement au problème de la réduction. Schématiquement, deux situations se présentent : lorsque le niveau N est premier à la

Mots clés : revêtements de courbes algébriques, espace de modules de Hurwitz, champ algébrique, ramification sauvage, réduction mod p.
Classification AMS : 14D22, 14H10, 14L30.

caractéristique du corps de base k, on souhaite construire un espace sur $\mathbf{Z}[1/N]$ ou une de ses extensions ; lorsqu'au contraire $p|N$, on veut trouver un espace modulaire défini sur l'anneau des vecteurs de Witt de k, et étudier sa reduction modulo p.

Dans un premier temps, pour étudier les propriétés algébriques et arithmétiques de base des courbes de Potts, nous avons besoin d'une connaissance détaillée de certains sous-groupes finis du groupe projectif linéaire PGL_2 sur un corps (pour discuter leurs orbites pour l'action naturelle sur $\mathbf{P}^1$). La classification des sous-groupes finis de PGL_2 ne renseigne que sur la structure des sous-groupes en question, mais ne précise pas leur description ensembliste. Nous avons donc regroupé quelques résultats nécessaires dans la première section.

Dans le §2 nous introduisons les courbes de Potts, calculons leurs automorphismes et leurs corps de définition et de modules (deuxième section). Ces courbes se révèlent être hyperelliptiques ; c'est pourquoi, par commodité, sont écartés les cas d'un niveau N pair, ou de la caractéristique $p = 2$. Dans la troisième section, nous nous intéressons au comportement en familles dans le cas « modéré ». On montre alors, en reprenant le cas elliptique bien connu [MS], que la droite affine privée de l'origine est un espace modulaire grossier pour le problème $\mathcal{P}$ des courbes de Potts à N états. Des notions classiquement attachées à de tels problèmes peuvent alors être étudiées : le groupe de Picard du problème modulaire et la compactification par des courbes stables.

Enfin, dans la quatrième section, nous abordons le cas sauvage. Nous construisons l'espace modulaire des courbes de Potts à p états en caractéristique p, puis en caractéristique mixte (sur une extension d'un anneau de vecteurs de Witt $W(k)$, k de caractéristique p). On note l'apparition du schéma en groupes $\mathcal{G}^{(\lambda)}$ de [OSS]. En corollaire de la démonstration, on obtient la bonne réduction de l'espace modulaire.

Notations : dans tout le texte, nous notons (a, b) le pgcd de deux entiers a et b. Lorsque k est un corps de caractéristique $p > 0$ et n est un entier avec $n = p^v n_0$ et $(n_0, p) = 1$, nous notons $\mu_n^*(k) = \mu_{n_0}^*(k)$ l'ensemble des racines primitives n-èmes de l'unité. En particulier, on a $\mu_p^* = \{1\}$. Par ailleurs $|E|$ désigne le cardinal d'un ensemble E, par exemple, $|\mu_n^*(\bar{k})| = \varphi(n_0)$ où φ est l'indicateur d'Euler. Nous notons $\mathrm{expchar}(k) = \max\{1, \mathrm{char}(k)\}$ l'exposant caractéristique de k. Enfin, dans n'importe quelle $\mathbf{F}_p$-algèbre, on note $\wp$ l'application $\mathbf{F}_p$-linéaire $x \mapsto x^p - x$.

0 Présentation du problème modulaire et des résultats

Soit k un corps de caractéristique p différente de 2. Soit un entier impair $N \geq 3$, on suppose que k contient les racines N-ièmes de l'unité. Soit ζ_N une telle racine, fixée une fois pour toutes. Lorsque $(N, p) = 1$ les courbes de Potts sont issues d'un problème de Hurwitz sous sa forme la plus classique, comme revêtements de $\mathbf{P}^1$ possédant certaines données d'inertie :

Définition 0.1 *Une courbe de Potts à N états est un revêtement cyclique de degré N de $\mathbf{P}^1$, c'est-à-dire un couple (C, σ) défini sur k, où C est une courbe algébrique et σ un automorphisme d'ordre N de C, avec la donnée de Hurwitz suivante constituée de 4 classes de conjugaison dans $G = <\sigma> = \mathbf{Z}/N\mathbf{Z}$:*

$$H_1 = H_2 = G \text{ et } \quad \chi_1 = \chi_2 = \chi : \quad \sigma \mapsto \zeta_N \quad \text{(points } a, b \in \mathbf{P}^1\text{)}$$
$$H_3 = H_4 = G \text{ et } \quad \chi_3 = \chi_4 = \chi^{-1} : \quad \sigma \mapsto \zeta_N^{-1} \quad \text{(points } c, d \in \mathbf{P}^1\text{)}$$

Lorsque $p|N$ cette définition n'a plus de sens ; on peut cependant formuler une définition, équivalente à la précédente lorsque $(N, p) = 1$, et satisfaisante aussi dans cette situation (voir section 2, définition 0.1.ter) :

Définition 0.2 *Une courbe de Potts à N états est une courbe hyperelliptique de genre $N - 1$, qui est revêtement cyclique de degré N de $\mathbf{P}^1$.*

Il s'avère que seul le cas $N = p$ donne naissance à des courbes de Potts dans le cas de ramification non modérée (section 2.3). Cela étant, nous obtenons les résultats suivants :

Théorème [Groupe d'automorphismes] (théorème 2.1.5, proposition 2.3.3)
On a une description explicite du groupe d'automorphismes d'une courbe de Potts.

Théorème [Espace modulaire] (théorèmes 3.1.1, 4.1.3, 4.2.6)
Dans les trois situations de caractéristique première à N, égale à N, ou mixte, le champ des courbes de

Potts est un champ algébrique de Deligne Mumford — resp. sur $\mathbf{Z}[\frac{1}{2N}]$, $\mathbf{F}_p$, $W(k)[\zeta]$ — qui admet un espace modulaire grossier.

Théorème [Réduction] (théorèmes 3.2.1, 4.2.7)
Dans le cas de la caractéristique première à N, l'espace modulaire grossier des courbes de Potts a bonne réduction en tout premier q premier à $2n$. Dans le cas de la caractéristique mixte, il a bonne réduction en p.

1 Préliminaires : théorème de Dickson

Dans cette section, k est un corps algébriquement clos de caractéristique différente de 2. Les résultats que nous avons en vue n'ont pas d'autre objet dans la suite, que de permettre de démontrer 2.1.5 et 2.3.3 qui donnent les automorphismes des courbes de Potts. Pour arriver à nos fins nous précisons le théorème de Dickson, cité plus loin, à l'aide d'un résultat technique élémentaire :

Proposition 1.1 *Soit k un corps d'exposant caractéristique $p \neq 2$ algébriquement clos. Soit dans μ_n^* la relation d'équivalence définie par $\rho' \sim \rho$ ssi $\rho' = \rho$ ou $\rho' = 1/\rho$. Soit $A \in \mathrm{PGL}_2(k)$ un automorphisme d'ordre fini n ; alors,*

i) n est soit premier à p, soit égal à p.
ii) A vu comme automorphisme de $\mathbf{P}^1_k$ est conjugué à $x \mapsto \rho x$, pour un $\rho \in \mu_n^*$, lorsque $(n,p) = 1$, $x \mapsto x+1$, lorsque $n = p$.

L'ensemble $\mu_n^*/\sim$ classifie les classes de conjugaison des éléments d'ordre n, et plus précisément, $\mathrm{ord}(A) = n$ si et seulement si

$$\text{il existe } \rho \in \mu_n^*/\sim \text{ tel que } P_\rho(A) := (1+\rho)^2 \det A - \rho\,(\mathrm{tr}\,A)^2 = 0$$

(ceci a un sens car $P_\rho(A)$ est homogène en les coefficients de A).

Preuve : Les affirmations *i)* et *ii)* sont bien connues ; supposons $A \neq \mathrm{id}$.
i) si A n'a qu'*une* valeur propre $\lambda \in k$, alors elle est conjuguée à $\left[\begin{smallmatrix} \lambda & u \\ 0 & \lambda \end{smallmatrix}\right]$ avec $u\lambda \neq 0$, c'est-à-dire à $x \mapsto x+1$. On vérifie en faisant $\rho = 1$ que la dernière affirmation $P_1(A) = 0$ est vraie.
ii) dans le cas contraire, $(n,p) = 1$ et A a deux valeurs propres distinctes λ_+, λ_- ; elle est conjuguée à $\left[\begin{smallmatrix} \lambda_+ & 0 \\ 0 & \lambda_- \end{smallmatrix}\right]$ et on a $\lambda_+ = \rho\lambda_-$ pour un $\rho \in \mu_n^*$. D'autre part, à l'aide du polynôme caractéristique on peut calculer

$$\lambda_\pm = \frac{\mathrm{tr}\,A \pm \delta}{2}\,, \qquad \text{où } \delta^2 = \Delta = (\mathrm{tr}\,A)^2 - 4\det A.$$

Par suite, $\rho = \frac{\mathrm{tr}\,A + \delta}{\mathrm{tr}\,A - \delta}$
donc $(\mathrm{tr}\,A = 0, \rho = -1)$ ou $\delta = \frac{\rho-1}{\rho+1}\,\mathrm{tr}\,A$
donc $(\mathrm{tr}\,A = 0, \rho = -1)$ ou $(\mathrm{tr}\,A)^2 - 4\det A = (\frac{\rho-1}{\rho+1})^2 (\mathrm{tr}\,A)^2$
donc $(\mathrm{tr}\,A = 0, \rho = -1)$ ou $\det A = \frac{\rho}{(\rho+1)^2}(\mathrm{tr}\,A)^2$
donc $P_\rho(A) = 0$.
Réciproquement on peut remonter ces calculs ; l'élévation au carré oblige à changer, au besoin, ρ en $1/\rho$, mais P_ρ et $P_{1/\rho}$ sont proportionnels. ■

Exemples : $A \in \mathrm{PGL}_2$ est d'ordre 2 si et seulement si $\mathrm{tr}\,A = 0$; A est d'ordre 3 si et seulement si $\det A = (\mathrm{tr}\,A)^2$; A est d'ordre 4 si et seulement si $2\det A = (\mathrm{tr}\,A)^2$.

Corollaire 1.2 *Soit p un nombre premier et $q = p^n$. Alors, les éléments de $\mathrm{PGL}_2(\mathbf{F}_q)$ ont un ordre qui, s'il est distinct de p, divise $q-1$ ou $q+1$.*

Preuve : Soit A un élément d'ordre n premier à p. D'après la proposition 1.1, il existe $\rho \in \mu_n^*$ algébrique sur $\mathbf{F}_q$, de degré au plus 2, donc appartenant à $\mathbf{F}_{q^2}$. Dans le cas où $\rho \in \mathbf{F}_q$, on a $\rho^{q-1} = 1$. Sinon, le polynôme minimal de ρ sur $\mathbf{F}_q$ est

$$X^2 + (2 - \frac{(\mathrm{tr}\,A)^2}{\det A})X + 1\,.$$

Par ailleurs, le Frobenius $\mathrm{Fr}(x) = x^q$, générateur de $\mathrm{Gal}(\mathbf{F}_{q^2}/\mathbf{F}_q) = \mathbf{Z}/2\mathbf{Z}$, permet d'exprimer ce polynôme minimal par $X^2 - (\rho + \rho^q)X + \rho^{q+1}$, d'où $\rho^{q+1} = 1$ et la conclusion. ■

Corollaire 1.3 *Il y a q^2-1 éléments d'ordre p dans $\mathrm{PGL}_2(\mathbf{F}_q)$; tous appartiennent à $\mathrm{PSL}_2(\mathbf{F}_q)$. Par ailleurs l'ensemble des points fixes des éléments de $\mathrm{PGL}_2(\mathbf{F}_q)$ d'ordre p est $\mathbf{P}^1(\mathbf{F}_q)$.*

Preuve : Soit $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ d'ordre p, par la proposition c'est équivalent à dire que $4\det(A) = \mathrm{tr}(A)^2$, ou encore que $bc = -\left(\frac{a-d}{2}\right)^2 =: \delta$. Ceci mène à l'un des deux cas

$$\begin{cases} a = d \neq 0 & \text{et} \quad b \text{ ou (exclusif) } c \text{ nul} \\ a \neq \pm d & \text{et} \quad b \neq 0 \text{ quelconque, } c = \delta/b, \end{cases}$$

d'où (à homothétie près) les éléments

- $\left[\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right]$ avec $u \in \mathbf{F}_q^\times$, en nombre $q-1$, dont le point fixe est ∞ ;
- $\left[\begin{smallmatrix} 1 & 0 \\ u & 1 \end{smallmatrix}\right]$ avec $u \in \mathbf{F}_q^\times$, en nombre $q-1$, dont le point fixe est 0 ;
- $\left[\begin{smallmatrix} a & 1 \\ \delta & d \end{smallmatrix}\right]$ avec $a \neq \pm d$, en nombre $(q-1)^2$, et dont le point fixe est $\frac{2}{a-d}$.

Les images dans $\mathrm{PGL}_2(\mathbf{F}_q)$ de ces matrices sont en fait dans $\mathrm{PSL}_2(\mathbf{F}_q)$ puisque leur déterminant, qui vaut $\mathrm{tr}(A)^2/4$, est un carré dans $\mathbf{F}_q$. Pour conclure, il reste à voir que tout point de $\mathbf{P}^1(\mathbf{F}_q)$ est point fixe d'un de ces automorphismes ; ce n'est pas évident seulement pour $u \in \mathbf{F}_q^\times$, qui est point fixe d'une matrice du troisième type avec $d = 0$, $a = 2/u$. ■

En fait Dickson a donné la description de tous les sous-groupes finis de $\mathrm{SL}_2(k)$ (k algébriquement clos ; voir par exemple [Su, chap. 3, §6, th. 6.17]). Comme on désire simplement ceux de $\mathrm{PGL}_2(k) = \mathrm{PSL}_2(k)$, la forme du théorème 6.17 de [Su] se simplifie ainsi :

Théorème 1.4 (Dickson) *Soit k un corps algébriquement clos de caractéristique p distincte de 2, alors tout sous-groupe fini G de $\mathrm{PGL}_2(k)$ est isomorphe à l'un des groupes de la liste suivante :*
si $(p, |G|) = 1$,

1. *un groupe cyclique, un groupe diédral, $\mathfrak{S}_4$, $\mathfrak{A}_4$ ou $\mathfrak{A}_5$,*

et, si $p \mid |G|$,

2. *$G = Q \rtimes C$ produit semi-direct d'un p-Sylow distingué élémentaire abélien Q par un groupe cyclique d'ordre premier à p,*
3. *$\mathfrak{A}_5$ si $p = 3$,*
4. *$\mathrm{PSL}_2(\mathbf{F}_q)$, $q = p^s$,*
5. *$\mathrm{PGL}_2(\mathbf{F}_q)$ (lui-même sous-groupe de $\mathrm{PSL}_2(\mathbf{F}_{q^2})$).* ■

À l'aide du critère fourni par la proposition 1.1 nous pouvons expliciter certains sous-groupes finis de $\mathrm{PGL}_2(k)$: nous sommes intéressés par les groupes cycliques, diédraux, et par ceux isomorphes à $\mathfrak{S}_4$, $\mathrm{PSL}_2(\mathbf{F}_q)$ et $\mathrm{PGL}_2(\mathbf{F}_q)$. Nous noterons de manière concise $< \alpha(x) >$ le sous-groupe engendré par une homographie $\alpha \in \mathrm{PGL}_2(k)$.

Proposition 1.5 *Les sous-groupes cycliques d'ordre n de $\mathrm{PGL}_2(k)$ sont les conjugués de*

$$\begin{array}{ll} \mathbb{C}_n = < \rho\, x > & (\rho \in \mu_n^*) \text{ pour } (n,p) = 1, \\ \mathbb{C}_p = < x+1 > & \text{pour } n = p. \end{array}$$

Les sous-groupes diédraux sont les conjugués de

$$\begin{array}{ll} \mathbb{D}_n = < \rho\, x, \frac{1}{x} > & (\rho \in \mu_n^*) \text{ pour } (n,p) = 1, \\ \mathbb{D}_p = < x+1, -x > & \text{pour } n = p. \end{array}$$

Preuve : C'est à peu près immédiat. ■

Proposition 1.6 *Les sous-groupes isomorphes à $\mathfrak{S}_4$ ($p \neq 2, 3$) sont les conjugués de*

$$\mathbb{S}_4 = < ix, \frac{x+1}{x-1} > \simeq < (1234), (12) > \ .$$

Preuve : Soit $\nu : \mathfrak{S}_4 \xrightarrow{\sim} G$ un isomorphisme à valeurs dans un sous-groupe de $\mathrm{PGL}_2(k)$; $a = \nu(1234)$ et $b = \nu(12)$ engendrent G. À conjugaison près, $a(x) = ix$; l'involution b s'écrit a priori sous la forme $b(x) = \frac{rx+s}{tx-r}$, et écrire que $ab = \nu(134)$ est d'ordre 3 fournit $r^2 = st$. La conjugaison par l'homothétie

de rapport $\lambda = r/t$ laisse a inchangé, et envoie b sur l'élément indiqué $x \mapsto \frac{x+1}{x-1}$. Il faut réciproquement vérifier que ces deux éléments engendrent un sous-groupe isomorphe à $\mathfrak{S}_4$, ce qui est laissé au lecteur. ■

Proposition 1.7 *Les sous-groupes isomorphes à* $\mathrm{PGL}_2(\mathbf{F}_q)$ *sont les conjugués de* $\mathrm{PGL}_2(\mathbf{F}_q)$ *« standard » correspondant à l'inclusion de corps* $\mathbf{F}_q \hookrightarrow k$ *; le même résultat vaut pour* $\mathrm{PSL}_2(\mathbf{F}_q)$.

Preuve : Comme ci-dessus, pour obtenir le résultat désiré nous allons utiliser les relations dans $\mathrm{PGL}_2(\mathbf{F}_q)$, engendré par trois éléments r, s, t

$$r(x) = x + 1, \quad s(x) = ux, \quad t(x) = 1/x$$

où u est un générateur du groupe multiplicatif $\mathbf{F}_q^*$. Si l'on pose $m = \frac{q-1}{p-1}$, alors $v = u^m$ est un générateur de $\mathbf{F}_p^*$; c'est en particulier un entier modulo p. Il est facile de voir que $r^v s^m = s^m r$: c'est l'homographie $x \mapsto vx + v$. Finalement notons que $n = \mathrm{ord}(rt)$ est premier à p. Par conséquent n divise $q-1$ ou $q+1$. Dans tous les cas, pour toute racine primitive n-ème de l'unité $\lambda \in \mathbf{F}_{q^2}^*$, on a $\lambda^{q\pm 1} = 1$ donc $\lambda^q = \lambda^{\mp 1}$, donc $\lambda + \lambda^{-1} \in \mathbf{F}_q$.

Soit maintenant G un sous-groupe de $\mathrm{PGL}_2(\mathbf{F}_q)$, et $\nu : \mathrm{PGL}_2(\mathbf{F}_q) \to G$ un isomorphisme. Notons $e = \nu(r)$, $f = \nu(s)$, $g = \nu(t)$, donc $G =< e, f, g >$. Avant tout, nous observons que $< f, g > \simeq < s, t > = \mathbf{D}_{q-1}$, donc par le résultat ci-dessus (proposition 1.5), à l'aide d'une première conjugaison et quitte à changer le générateur u, on peut supposer que $f = s$ et $g = t$. Les relations que nous allons exploiter sont :

$$e^p = 1 \tag{1}$$
$$e^v f^m = f^m e \tag{2}$$
$$(eg)^n = 1 \tag{3}$$

Écrivons $e(x) = \frac{ax+b}{cx+d}$, alors (1) s'écrit $bc = -\frac{1}{4}(a-d)^2$, et une récurrence utilisant cela donne

$$e^k(x) = \frac{\left(\frac{k+1}{2}a - \frac{k-1}{2}d\right)x + kb}{kcx - \frac{k-1}{2}a + \frac{k+1}{2}d}$$

On écrit alors (2) explicitement et on tire $a = d$, puis $c = 0$. À ce stade, $e(x) = x + b/a$. Or par (3) il existe $\lambda \in \mu_n^* \subset \mathbf{F}_{q^2}^*$ tel que $(1+\lambda)^2 a^2 = -\lambda b^2$, donc $\beta := \left(\frac{b}{a}\right)^2 = -(\lambda + \lambda^{-1} + 2) \in \mathbf{F}_q$. La conjugaison par $x \mapsto \frac{b}{a}x$ envoie $G =< x + b/a, ux, 1/x >$ sur $< x+1, ux, \frac{1}{\beta x} > \subset \mathrm{PGL}_2(\mathbf{F}_q)$, ce qui conclut. Pour $\mathrm{PSL}_2(\mathbf{F}_q)$, la démonstration est identique ; nous ne la reproduisons pas. ■

2 Courbes de Potts et leurs automorphismes

Soit k un corps de caractéristique p différente de 2. On fixe pour la suite un entier $N \geq 3$, et on suppose que k contient les racines N-ièmes de l'unité. Soit ζ_N une telle racine, fixée une fois pour toutes.

Par *courbe algébrique*, on entend ici schéma de type fini sur un corps, géométriquement intègre, projectif, lisse, et de dimension 1. On pourra se reporter à [Be] pour des détails sur la donnée de ramification de Hurwitz.

Nous rappelons que, lorsque $(N, 2, p) = 1$ *comme c'est le cas dans toute cette section jusqu'à 2.2 y compris*, une courbe de Potts est une courbe satisfaisant la définition 0.1 ; complétons cette définition en ajoutant qu'un isomorphisme entre courbes de Potts $\varphi : (C, \sigma) \to (C', \sigma')$ est un isomorphisme de courbes algébriques $\varphi : C \to C'$ qui commute à σ et σ' : $\varphi\sigma = \sigma'\varphi$.

Notons que, dans la définition, la racine ζ est fixée, ce qui revient à marquer le choix du générateur σ de G (voir aussi 2.3.2). Venons-en à quelques conséquences immédiates de la définition. Par la formule de Riemann-Hurwitz, on obtient le genre $g(C) = N - 1$. Notons qu'une équation birationnelle simple se déduit de la définition : l'extension $k(C)/k(x)$ du corps des fonctions de $\mathbf{P}^1$ est cyclique de degré N ; du fait que $p \nmid N$, on peut en choisir un générateur $t \in k(C)$ tel que $t^N \in k(x)$, donc

$$t^N = \frac{P(x)}{Q(x)} \tag{4}$$

et P, Q sont des polynômes de degré 2 d'après la ramification. En multipliant par Q^N et en faisant $t \to tQ$ on se ramène à

$$t^N = P(x)\,Q(x)^{N-1} = (x-a)(x-b)(x-c)^{N-1}(x-d)^{N-1}\ ; \tag{5}$$

σ agit par multiplication par ζ_N sur t.

Les courbes de Potts, définies à l'aide de leur ramification ξ comme revêtements de $\mathbf{P}^1$ (de genre $g' = 0$), avec $r = 4$ points de ramification, sont paramétrées par un schéma de Hurwitz $\mathcal{H}_{g,G}(\xi) = \mathcal{H}_{N-1,\mathbf{Z}/N\mathbf{Z}}(\xi)$, dont il est connu que, sur un corps algébriquement clos de caractéristique première à N, il est équidimensionnel de dimension $3g' - 3 + r = 0 - 3 + 4 = 1$ [Be, prop. 4.3].

Soulignons aussi le comportement fonctoriel des courbes de Potts par quotient du groupe G : soit M un entier diviseur de N, $H = <\sigma^M> = \mathbf{Z}/(N/M)\mathbf{Z}$ et σ/H un générateur de $G/H \simeq \mathbf{Z}/M\mathbf{Z}$, alors $(C/H, \sigma/H)$ est une courbe de Potts à M états, et on a un diagramme commutatif

$$\begin{array}{ccc} (C,\sigma) & \xrightarrow{N/M} & (C/H, \sigma/H) \\ & {\scriptstyle N}\searrow \quad \swarrow{\scriptstyle M} & \\ & \mathbf{P}^1 & \end{array}$$

2.1 Hyperellipticité des courbes de Potts ; automorphismes

Au vu de l'équation (5) nous observons que dans $\mathrm{Aut}(\mathbf{P}^1)$ il y a un unique sous-groupe isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ d'involutions qui permutent les 4 points a, b, c, d, soient

$$\tau_0 : \begin{cases} a \leftrightarrow b \\ c \leftrightarrow d \end{cases} \qquad \mu_0 : \begin{cases} a \leftrightarrow c \\ b \leftrightarrow d \end{cases} \qquad \tau_0\mu_0 = \mu_0\tau_0 : \begin{cases} a \leftrightarrow d \\ b \leftrightarrow c \end{cases}$$

Ces groupes d'involutions et leur action sur des « (2-2)-partitions » du type de celles de S-S. Roan, comme $(\{a,b\},\{c,d\})$, font l'objet d'une étude détaillée dans la première partie de [Ro] ; voir, notamment, [Ro, 1, Lemma 2].

Description 2.1.1 Une technique générale permet de décrire un revêtement cyclique modéré de courbes (ou même, de familles) en termes de faisceaux inversibles de la base. Nous renvoyons à diverses références : par exemple [Ha, IV,2,Ex 2.7.] ou [Mu3].

Soit $X \to S$ une S-courbe, et $G = <\sigma>$ cyclique d'ordre N ; on suppose N inversible dans les anneaux locaux. Alors le morphisme $f : X \to Y = X/G$ est fini donc affine, et l'on sait qu'alors $X \simeq \mathbf{Spec}\,\mathscr{A}$ où $\mathscr{A}$ est le faisceau d'algèbres quasi-cohérentes $f_*\mathcal{O}_X$. En fait, ici on a une description simple de $\mathscr{A}$ puisque, par l'hypothèse d'inversibilité de N, on a une décomposition $f_*\mathcal{O}_X = \oplus_{j=0}^{N-1}\mathscr{L}_j$ où $\mathscr{L}_j$ correspond au « sous-espace propre » associé à la valeur propre ζ^j. L'étude locale sur les fibres permet de voir que $\mathscr{L}_j$ est un faisceau inversible. Enfin, comme $(\sigma^\sharp)^N = \mathrm{id}$, on a $\mathscr{L}_1^N \simeq \mathcal{O}_Y(-D)$ où D est le diviseur de Cartier effectif de branchement de f, diviseur de zéros d'une section globale s.

Réciproquement, à l'aide de $\mathscr{L} = \mathscr{L}_1$ et de s on munit $f_*\mathcal{O}_X$ d'un produit naturel, qui envoie $(l, l') \in \mathscr{L}_j \times \mathscr{L}_{N-j}$ sur $sll' \in \mathcal{O}_Y$, et on récupère $X = \mathbf{Spec}(\oplus_{j=0}^{N-1}\mathscr{L}_j)$.

En conclusion, on peut considérer la donnée d'un revêtement cyclique N-uple $X \to Y = X/G$ comme étant équivalente, à isomorphisme près, à celle d'un triplet $(Y, \mathscr{L}, s)$ où $\mathscr{L} \in \mathrm{Pic}(Y)$ et s est une section globale de $\mathscr{L}^{-N}$. Pour la suite on notera $X = X(\mathscr{L}, s)$, la base Y étant sous-entendue. ■

Dans notre situation, le revêtement $C \xrightarrow{\pi} C/<\sigma> \simeq \mathbf{P}^1$ est décrit par $\mathscr{L} = \mathcal{O}(-2)$ et $s = (X-a)(X-b)(X-c)^{N-1}(X-d)^{N-1}$. Comme on a $\tau_0^*\mathscr{L} = \mathscr{L}$ et $\tau_0^* s = s$, alors τ_0 se relève :

$$\begin{array}{ccc} (C,\sigma) = C(\tau_0^*\mathscr{L}, \tau_0^* s) & \overset{\exists\tau}{\dashrightarrow} & C(\mathscr{L}, s) = (C,\sigma) \\ \downarrow & & \downarrow{\scriptstyle \pi} \\ \mathbf{P^1} & \xrightarrow{\tau_0} & \mathbf{P}^1 \end{array}$$

Il est important de noter que la construction 2.1.1 tient compte du fait que dans le revêtement $C \to C/G$, un générateur de G est marqué par le choix de ζ_N. En effet le faisceau inversible $\mathscr{L}$ est relatif au choix d'une racine primitive de l'unité, de sorte qu'un isomorphisme $X \to X'$ de revêtements de Y échange σ et σ' (et non simplement $<\sigma>$ et $<\sigma'>$).

Ainsi, τ vérifie $\tau\sigma\tau^{-1} = \sigma$. Par ailleurs, on a $\tau^2 = \sigma^j$ pour un j, car il induit l'identité sur $\mathbf{P}^1$. Comme $2 \in (\mathbf{Z}/N\mathbf{Z})^\times$ on peut supposer $j = 2k$ pair. Alors, $(\tau\sigma^{-k})^2 = 1$ et $\tau\sigma^{-k}$ induit le même automorphisme de $\mathbf{P}^1$ que τ. Donc on peut supposer que $\tau^2 = 1$.

Pour μ_0, on a $\mu_0^*\mathscr{L} = \mathscr{L}$ et $\mu_0^* s = (X-a)^{N-1}(X-b)^{N-1}(X-c)(X-d)$, donc μ_0 se relève en un isomorphisme

$$\begin{array}{ccc} (C,\sigma^{-1}) = C(\mu_0^*\mathscr{L}, \mu_0^* s) & \overset{\exists \mu}{\dashrightarrow} & (C,\sigma) \\ \downarrow & & \downarrow \\ \mathbf{P^1} & \xrightarrow{\mu_0} & \mathbf{P}^1 \end{array}$$

i.e. $\mu^{-1}\sigma\mu = \sigma^{-1}$. Comme ci-dessus on suppose $\mu^2 = 1$; en particulier, $<\mu, \sigma> \simeq \mathbf{D}_N$.

Proposition 2.1.2 *C est hyperelliptique, τ est l'involution hyperelliptique.*

Preuve : Un point fixe x de τ ne peut être point fixe de σ^j, car sinon, πx est un point fixe de τ_0, mais étant fixe pour σ^j, son image dans $\mathbf{P}^1$ est a, b, c ou d : c'est impossible.

Soit α l'un des deux points fixes de τ_0 et $\beta \in \pi^{-1}(\alpha)$. On sait que $\pi\tau\beta = \tau_0\pi\beta = \pi\beta$ donc $\exists j$, $\tau\beta = \sigma^j\beta$. Donc ($\tau^2 = 1$) il vient $\beta = \tau\sigma^j\beta = \sigma^j\tau\beta = \sigma^{2j}\beta$; si $2j \not\equiv 0\ (N)$, $\pi\beta = \alpha$ est point de branchement et point fixe de τ_0, impossible. Comme enfin $2 \in (\mathbf{Z}/N)^\times$, $j \equiv 0\ (N)$ i.e. $\tau\beta = \beta$. On obtient $2N$ points fixes pour τ : $\mathrm{Fix}\,\tau = \pi^{-1}(\mathrm{Fix}\,\tau_0)$, qui sont deux orbites de G. Considérons le quotient $C \to C/<\tau>$ de degré 2. Par la formule de Riemann-Hurwitz,

$$2(N-1) - 2 = 2\,(2g_{C/\tau} - 2) + 2N \quad \Longrightarrow \quad g_{C/\tau} = 0$$

c'est-à-dire $C/\tau \simeq \mathbf{P}^1$, ce que l'on voulait. ■

Remarque 2.1.3 Puisqu'une courbe de Potts est nécessairement hyperelliptique, on ne change pas le problème modulaire en ajoutant le caractère hyperelliptique dans la définition 0.1. Ceci revient à regarder des *triplets* (C, σ, τ). On y sera contraint lorsque $p|N$, pour pouvoir écrire une définition cohérente. Dans [Ro], la définition (équivalente) adoptée pour les courbes de Potts est d'ailleurs :

Définition 0.1.bis Une N-courbe de Potts est une courbe hyperelliptique de genre $N-1$, avec un automorphisme d'ordre N ayant exactement 4 points fixes.

Cependant, on sait que, lorsque $N = p$, la ramification de l'automorphisme d'ordre N dégénère. Par conséquent cette définition est certainement inopérante si $p > 0$ et $p|N$. En revanche, une dernière forme équivalente de la définition prend sens sans distinction sur N :

Définition 0.1.ter Une N-courbe de Potts est une courbe hyperelliptique de genre $N-1$, avec un automorphisme σ d'ordre N, telle que C/σ soit une courbe rationnelle. ■

En utilisant le quotient par τ on peut donner une nouvelle description affine de C. En effet σ induit sur $C/\tau \simeq \mathbf{P}^1$ un automorphisme d'ordre N (conjugué à) : $x \mapsto \zeta_N x$. Les points de Weierstraß $\mathrm{Fix}\,\tau$ donnent deux orbites de σ, à savoir $\{\zeta_N^j a\}_{0\le j\le N-1}$ et $\{\zeta_N^j b\}_{0\le j\le N-1}$ ($a^N \neq b^N \neq 0$). L'équation affine correspondante est

$$y^2 = (x^N - a^N)(x^N - b^N) = x^{2N} + Ax^N + B \tag{6}$$

à partir de laquelle on retrouve (4) en prenant un paramètre rationnel sur la conique $y^2 = u^2 + Au + B$, i.e. en posant $z = \frac{y+\sqrt{B}}{x^N}$, $t = \frac{x}{(2\sqrt{B})^{1/N}}$ (et $\lambda = \frac{-A}{2\sqrt{B}}$) :

$$t^N = \frac{z-\lambda}{z^2-1} \tag{7}$$

Les automorphismes σ, τ, μ s'obtiennent aisément,

sur le modèle (7) : $\sigma(z,t) = (z, \zeta_N t)$; $\tau(z,t) = (\frac{\lambda z - 1}{z - \lambda}, t)$; $\mu(z,t) = (\frac{z+1-2\lambda}{z-1}, \frac{1}{4^{1/N} t})$
sur le modèle (6) : $\sigma(x,y) = (\zeta_N x, y)$; $\tau(x,y) = (x, -y)$; $\mu(x,y) = (\frac{B^{1/N}}{x}, \frac{\sqrt{B} y}{x^N})$.

Avant d'aller plus loin, il faut remarquer que l'existence des courbes de Potts, qui n'était jusqu'à présent pas établie, est maintenant acquise puisqu'on a une forme explicite, et que l'on peut vérifier qu'elle satisfait la définition 0.1.

On définit ensuite un invariant modulaire par

$$j = \frac{B}{A^2 - 4B} \neq 0$$

pour la forme (6) ; il s'écrit $j = \frac{1/4}{\lambda^2 - 1}$ pour la forme (7). Par ailleurs il a aussi une forme agréable pour l'équation générale (4)

$$t^N = \frac{P(x)}{Q(x)} = \frac{(x-a)(x-b)}{(x-c)(x-d)} ;$$

en effet on peut ramener cette dernière à une forme (7) en appliquant sur x une homographie qui envoie a sur ∞, c sur 1 et d sur -1. On calcule alors

$$\lambda = \frac{2(ab+cd) - (a+b)(c+d)}{(a-b)(c-d)} \quad \text{et} \quad \lambda^2 - 1 = 4\frac{(a-c)(a-d)(b-d)(b-c)}{(a-b)^2(c-d)^2}$$

donc

$$j = \frac{\operatorname{disc}(P)\operatorname{disc}(Q)}{16\ \text{rés}(P,Q)}$$

(disc est le discriminant, rés le résultant). Enfin, comme on attend d'un tel invariant,

Proposition 2.1.4 *Deux courbes de Potts (C,σ) et (C',σ') sont $\bar{k}$-isomorphes ssi $j = j'$.*

Preuve : Soit φ un isomorphisme : $\sigma'\varphi = \varphi\sigma$. Si C et C' sont toutes deux représentées par une équation (6), il est clair que φ passe au quotient en un morphisme $\bar{\varphi} : C/\tau \to C'/\tau'$ tel que $\zeta_N \bar{\varphi}(x) = \bar{\varphi}(\zeta_N x)$. Alors, nécessairement $\bar{\varphi}(x) = \lambda x$, d'où $A = \lambda^N A'$, $B = \lambda^{2N} B'$ et $j = j'$.

Réciproquement, si $j = j'$ avec C et C' représentées par une équation (6), on choisit un $\lambda \in k$ tel que $A = \lambda^N A'$, $B = \lambda^{2N} B'$. Alors $\varphi : (x,y) \mapsto (\lambda x, \lambda^N y)$ donne une application birationnelle entre C et C', et telle que $\sigma'\varphi = \varphi\sigma$. Comme C et C' sont lisses, φ est un isomorphisme. ■

Nous sommes maintenant en mesure, à l'aide des résultats de la première partie, d'expliciter le groupe des automorphismes d'une courbe de Potts. Nous corrigeons ce faisant une erreur dans la section 2, proposition 5 de [Ro], où le cas de $j = -1/4$ est oublié.

On note par $O_\Gamma(x)$ l'orbite d'un point x sous l'action d'un groupe Γ, et Γ_x son stabilisateur.

Théorème 2.1.5 *Soit k un corps d'exposant caractéristique $p \neq 2$, et $N \geq 3$ un entier, avec $(N,2,p) = 1$. Soit (C,σ) une courbe de Potts à N états.*
1) Le groupe $\operatorname{Aut}_{\bar{k}}(C)$ des automorphismes de C est le suivant.
Si $N = 3$ et $p \neq 5$,

$$\begin{aligned} j \neq -1/4, -1/54 : &\quad (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{D}_N \\ j = -1/4 : &\quad (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{D}_{2N} \\ j = -1/54 : &\quad (\mathbf{Z}/2\mathbf{Z}) \times \mathfrak{S}_4 . \end{aligned}$$

Si $p > 0$ et si $2N - 1 = q$ est une puissance de p (dont le cas $N = 3$, $p = 5$),

$$\begin{aligned} j \neq -1/4 : &\quad (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{D}_N \\ j = -1/4 : &\quad (\mathbf{Z}/2\mathbf{Z}) \times \mathrm{PGL}_2(\mathbf{F}_q). \end{aligned}$$

Dans tous les autres cas,

$$\begin{aligned} j \neq -1/4 : &\quad (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{D}_N \\ j = -1/4 : &\quad (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{D}_{2N}. \end{aligned}$$

2) Le groupe $\mathrm{Aut}_{\bar{k}}(C,\sigma)$ *des automorphismes « modulaires » (c'est-à-dire ceux qui commutent à* σ*) est, pour tous* N, p *:*

$$j \neq -1/4 : \quad (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/N\mathbf{Z})$$
$$j = -1/4 : \quad (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2N\mathbf{Z}).$$

Preuve : On sait que $<\tau>$ est d'ordre 2 et distingué (unicité de l'involution hyperelliptique), donc central. Soit

- $\Sigma = O_\sigma(a) \sqcup O_\sigma(b)$ l'ensemble des $2N$ points de branchement,
- $G = \mathrm{Aut}_{\bar{k}}(C)/ <\tau>$

Par 2.1.1, G s'identifie au sous-groupe de $\mathrm{Aut}(\mathbf{P}^1)$ des homographies qui stabilisent Σ. Observons que $<\tau,\sigma,\mu> \simeq (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{D}_N \subset \mathrm{Aut}_{\bar{k}}(C)$ de sorte que $\mathbf{D}_N \subset G$. L'action de G sur Σ est transitive (car $\mathbf{D}_N$ agit déjà transitivement), par conséquent

$$\forall s \in \Sigma, \quad 2N = |O_G(s)| = |G| \,/\, |G_s| \ .$$

Comme G est un sous-groupe fini de $\mathrm{PGL}_2(\bar{k})$, on passe en revue les différentes possibilités du théorème de Dickson. Nous remarquons auparavant que, compte tenu des résultats de la partie précédente, on connaît des représentants simples des classes de conjugaison de sous-groupes finis de $\mathrm{PGL}_2(\bar{k})$ isomorphes à un sous-groupe donné parmi

$$\mathbf{D}_n \ , \mathfrak{S}_4, \ \mathrm{PSL}_2(\mathbf{F}_q), \ \mathrm{PGL}_2(\mathbf{F}_q)$$

(exception faite de $\mathbf{D}_n$, il n'y a d'ailleurs qu'une classe à chaque fois). Or, une telle conjugaison sur G n'affecte pas la classe d'isomorphisme de C : elle correspond à un changement de variable sur X dans une équation (6). Ceci explique qu'à partir de 1), nous identifierons G avec l'un des représentants donnés dans les propositions 1.5, 1.6, 1.7.

1) Les groupes qui ne peuvent jamais apparaître.

Tout d'abord, ni les groupes cycliques ni $\mathfrak{A}_4$ ne contiennent de sous-groupe diédral $\mathbf{D}_N$ (car $N \geq 3$), ce qui les exclut.

Ensuite, l'éventualité de $G \simeq \mathfrak{A}_5$ est impossible ; en effet, celui-ci n'a pour sous-groupes diédraux que $\mathbf{D}_3$ et $\mathbf{D}_5$, ce qui impose $N = 3$ ou 5. Supposons que $N = 3$; alors on doit avoir, pour un $s \in \Sigma$, $G_s \simeq \mathbf{D}_5$ (seule possibilité parmi les sous-groupes de cardinal 10 de $\mathfrak{A}_5$) et $H := <\sigma,\mu> \simeq \mathbf{D}_3$. Mais alors, on a $G_s \cap H \simeq \mathbf{Z}/2\mathbf{Z}$ (voir annexe), donc il existe dans H un automorphisme non trivial, avec un point fixe dans Σ, ce qui est impossible. Lorsque $N = 5$, les rôles de G_s et H sont inversés (le premier est $\mathbf{D}_3$, le second $\mathbf{D}_5$), et le raisonnement est le même. Notons que ceci vaut quelque soit p (cas 1 et 3 du théorème de Dickson 1.4).

Enfin, un groupe de la forme $Q \rtimes C$ (cas 2) ne peut pas contenir $\mathbf{D}_N$ avec $(N,p) = 1$.

2) Le cas de $G = \mathrm{PSL}_2(\mathbf{F}_q)$ ou $\mathrm{PGL}_2(\mathbf{F}_q)$, $q = p^n$.

Nous procédons par étapes. Soit Q un p-Sylow du stabilisateur G_a (et donc, de G).

a) on montre que Σ est constitué des points fixes des éléments de G d'ordre p. En effet, si g est d'ordre p, il appartient à un p-Sylow Q' qui est conjugué à Q (dans G), ainsi $t^{-1}gt \in G_a$ donc g fixe ta. Réciproquement, si $s \in \Sigma$, alors G_s contient un p-Sylow de G, donc un élément d'ordre p.

b) par le corollaire 1.3, $\Sigma = \mathbf{P}^1(\mathbf{F}_q)$; en particulier, $2N = |\Sigma| = q+1$. On a ainsi la description d'une courbe hyperelliptique dont une équation affine birationnelle est

$$y^2 = x^q - x \ ; \tag{8}$$

le genre est bien $\frac{q-1}{2} = N-1$, et un élément $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ de G agit par

$$(x,y) \mapsto \left(\frac{ax+b}{cx+d} \ , \ \frac{\sqrt{ad-bc}\, y}{(cx+d)^{\frac{q+1}{2}}} \right) \quad .$$

c) pour exhiber l'automorphisme σ d'ordre $N = \frac{q+1}{2}$ et calculer l'invariant, on choisit un générateur ξ de $\mathbf{F}_{q^2}^\times$ tel que $\zeta = \zeta_N = \xi^{2(q-1)} \in \mathbf{F}_{q^2} - \mathbf{F}_q$. Le polynôme minimal de ζ est $X^2 - \psi X + 1$ où

$\psi = \zeta + \zeta^{-1} \in \mathbf{F}_q$. Par ailleurs $\phi = \xi^{q-1}$ est une racine carrée de ζ (d'ordre $q+1$), et $\theta = \phi + \phi^{-1} \in \mathbf{F}_q$, d'où l'on remarque que $\psi+2 = \theta^2$ est un carré dans $\mathbf{F}_q$, alors que ce n'est pas le cas de $\psi^2-4 = (\zeta-\zeta^{-1})^2$.

Un automorphisme $g \in G$ est conjugué à $x \mapsto \zeta x$ si, et seulement si $(1+\zeta)^2 \det g = \zeta\,(\mathrm{tr}\, g)^2$ c'est-à-dire $\theta^2 \det g = (\mathrm{tr}\, g)^2$. Ainsi $\sigma = \left[\begin{array}{cc} \theta^2 & -\theta^2 \\ 1 & 0 \end{array}\right]$ (à conjugaison près) donc, remonté à C, de la forme

$$(x,y) \mapsto \left(\theta^2 \frac{x-1}{x}\ ,\ \frac{y\, x^{\frac{q+1}{2}}}{\theta}\right)\ .$$

Les points fixes sont donnés par l'équation $X^2 - \theta^2 X + \theta^2 = 0$ de discriminant $\Delta = \psi^2 - 4$. Comme celui-ci n'est pas un carré dans $\mathbf{F}_q$, on obtient deux solutions hors de $\mathbf{F}_q$ qui chacune donne lieu à deux points (x,y). D'où les quatre points de ramification de la définition 0.1 : on vérifie que la courbe est bien de Potts.

d) enfin on diagonalise σ pour calculer l'invariant. Les valeurs propres sont données par la même équation que celle des points fixes ; ce sont $1+\zeta^{\pm 1}$. La matrice de conjugaison est

$$P = \left[\begin{array}{cc} 1+\zeta & 1+\zeta^{-1} \\ 1 & 1 \end{array}\right] \quad \text{et} \quad P^{-1}\sigma P = \left[\begin{array}{cc} \zeta & 0 \\ 0 & 1 \end{array}\right]\ .$$

Gardant en tête que $\zeta^q = \zeta^{-1}$ et $\phi^q = \phi^{-1}$, on calcule

$$P(\phi^j)^q \ = \ \left[\tfrac{(1+\zeta)\phi^j+1+\zeta^{-1}}{\phi^j+1}\right]^q \ = \ \tfrac{(1+\zeta^{-1})\phi^{-j}+1+\zeta}{\phi^{-j}+1} \ = \ \tfrac{(1+\zeta)\phi^j+1+\zeta^{-1}}{\phi^j+1} \ = \ P(\phi^j)$$

et ceci même si $j = \frac{q+1}{2}$ pour lequel $P(\phi^j) = \infty$. En conclusion, $P(\phi^j) \in \mathbf{P}^1(\mathbf{F}_q)$ donc les deux orbites de σ qui partitionnent $\mathbf{P}^1(\mathbf{F}_q)$ sont envoyées par P^{-1} dans $\{\phi^{2j}\}_{0\le j\le \frac{q+1}{2}} \sqcup \{\phi^{2j+1}\}_{0\le j\le \frac{q+1}{2}}$. L'équation « de Potts » après conjugaison par P est

$$Y^2 = (X^{\frac{q+1}{2}} - 1)(X^{\frac{q+1}{2}} + 1)$$

et l'invariant de la courbe est $j = -1/4$.

e) le groupe d'automorphismes de cette courbe contient $(\mathbf{Z}/2\mathbf{Z}) \times \mathrm{PGL}_2(\mathbf{F}_q)$ (voir équation (8)) ; il y a en fait égalité car les sous-groupes finis de $\mathrm{PGL}_2(\bar{k})$ contenant $\mathrm{PGL}_2(\mathbf{F}_q)$ sont de la forme $\mathrm{PSL}_2(\mathbf{F}_{q'})$ ou $\mathrm{PGL}_2(\mathbf{F}_{q'})$ pour $q' > q$, or ceux-ci sont exclus par $2N-1 = q$. On déduit également que $G = \mathrm{PSL}_2(\mathbf{F}_q)$ n'est pas admissible, puisque sa possibilité supposée amène nécessairement à la courbe précédente (8).

3) Le cas de $G = \mathbb{S}_4 = < ix, \frac{x+1}{x-1} >$ (pour $N = 3$).

Dans les notations de la proposition 1.6, $x \mapsto ix$ est $(1234)^\nu$ et $x \mapsto \frac{x+1}{x-1}$ est $(12)^\nu$. À permutation près sur les symboles 1,2,3,4, on identifie σ et μ à $(123)^\nu$ et $(12)^\nu$, respectivement. Soit $s \in \Sigma$, son stabilisateur G_s doit être de cardinal 4, donc il est cyclique ou isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Le second cas est en fait impossible, car deux involutions qui commutent n'ont jamais de point fixe commun. Donc, $G_s \simeq \mathbf{Z}/4\mathbf{Z}$, et, quitte à changer s, on suppose que le générateur de G_s est $a(x) = ix$.

D'autre part, a ne peut avoir un seul point fixe dans Σ, car si tel était le cas, il agirait librement sur $\Sigma - \{s\}$, et son ordre diviserait $2N-1 = 5$. Donc, $\mathrm{Fix}(a) = \{0,\infty\} \subset \Sigma$. L'orbite de $\{0,\infty\}$ sous G est $\{0,\infty,\pm 1,\pm i\} = \Sigma$. Pour mettre C sous la forme (6) on diagonalise $\sigma : x \mapsto -i\frac{x-1}{x+1}$: la matrice de passage est

$$P = \left[\begin{array}{cc} 1-\sqrt{3} & 1+\sqrt{3} \\ i-1 & i-1 \end{array}\right]$$

et la conjugaison envoie
σ sur $x \mapsto jx$ où $j = \frac{-1+i\sqrt{3}}{2}$
μ sur $x \mapsto \frac{-j^2(2+\sqrt{3})}{x}$
a sur $x \mapsto \frac{-2j^2x+1+\sqrt{3}}{(-1+\sqrt{3})x+2j}$.

On a $P^{-1}(0) = 2+\sqrt{3}$, $P^{-1}(\infty) = -1$, et l'équation est $y^2 = (x^3 - (2+\sqrt{3})^3)\,(x^3+1)$ d'invariant $j = -1/54$. Le groupe $\mathbf{Z}/2\mathbf{Z} \times \mathbb{S}_4$ agit bien sur cette courbe, mais il se pourrait que $\mathrm{Aut}_{\bar{k}}(C)$ soit plus gros. En effet les groupes $\mathrm{PSL}_2(\mathbf{F}_q)$ et $\mathrm{PGL}_2(\mathbf{F}_q)$ contiennent des copies de $\mathfrak{S}_4$. Si tel est le cas, alors on sait qu'on doit avoir $q = 2N-1 = 5$; or, lorsque $p = q = 5$, on a $-1/54 = -1/4$ et, d'après l'analyse

précédente, la courbe a pour groupe d'automorphismes $\mathrm{PGL}_2(\mathbf{F}_5) \simeq \mathfrak{S}_5$.

4) Le cas diédral $G = \mathbb{D} = < \varepsilon\, x,\, \frac{1}{x} >$, $\varepsilon \in \mu_M^*$, pour M un multiple de N.

C'est l'unique possibilité restante. Les orbites sont de la forme

$$\{x, \varepsilon x, \ldots, \varepsilon^{M-1} x,\, \frac{1}{x}, \ldots, \frac{\varepsilon^{M-1}}{x}\}\ ;$$

leur cardinal est 2 si $x = 0$ ou ∞, $2M$ si x est en position générale, et M si x égale l'un des $\pm\sqrt{\varepsilon^j}$. On conclut que $M = N$ dans le cas général ; $M = 2N$ se produit lorsque les points de l'orbite sont sommets d'un polygone régulier, auquel cas l'équation est $y^2 = x^{2N} - 1$, avec $j = -1/4$, et σ a une « racine » $\sqrt{\sigma} : x \mapsto \zeta_{2N} x$.

5) Calcul du commutant de σ.

On désigne par la lettre Z un commutant. Seul le cas de $G = \mathrm{PGL}_2(\mathbf{F}_q)$ n'est pas évident ; on a alors

$$\mathrm{Aut}_{\bar{k}}(C, \sigma) \,/\, < \tau >= \mathrm{Z}_{\mathrm{PGL}_2(\mathbf{F}_q)}(\sigma) = P.\,\mathrm{Z}_{\mathrm{PGL}_2(\bar{k})}\left(\left[\begin{array}{cc} \zeta & 0 \\ 0 & 1 \end{array}\right]\right).P^{-1} \cap \mathrm{PGL}_2(\mathbf{F}_q)\ .$$

Or les homographies commutant à $x \mapsto \zeta x$ sont celles de la forme $x \mapsto ux$. En exprimant l'appartenance de $P \left[\begin{smallmatrix} u & 0 \\ 0 & 1 \end{smallmatrix}\right] P^{-1}$ à $\mathrm{PGL}_2(\mathbf{F}_q)$, il vient $u^{q+1} = u^{2N} = 1$. Le commutant quotient ci-dessus est donc de cardinal inférieur à $2N$. Pour conclure, il ne reste qu'à remarquer que

$$\sqrt{\sigma} = \left[\begin{array}{cc} \theta(\theta+1) & -\theta^2 \\ 1 & \theta \end{array}\right]$$

dont le carré est σ, est d'ordre $2N$. ■

Le dessin suivant illustre le cas $j = -1/4$ où l'orbite de b vient s'intercaler entre les points de l'orbite de a, sur les sommets d'un polygone régulier.

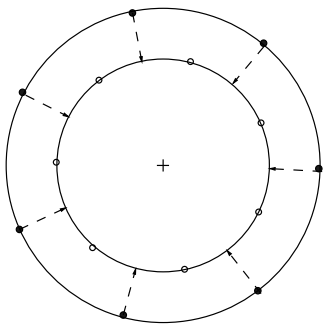


FIG. 1 – Configuration exceptionnelle des points fixes de τ

2.2 Corps de définition, corps des modules

Nous notons maintenant $\bar{k}$ et k_s des clôtures algébrique et séparable de k, respectivement ; $\mathbf{F}_p$ désigne le corps premier de k, en particulier $\mathbf{F}_0 = \mathbf{Q}$. Une courbe de Potts (C, σ) est définie sur k si, et seulement si, C et σ sont définies sur k. On peut s'interroger sur l'existence de N-courbes de Potts définies sur le corps premier $\mathbf{F}_p$ ou sur son extension cyclotomique $\mathbf{F}_p(\zeta_N)$. En fait, il n'est raisonnable de rechercher le corps de définition d'une courbe de Potts à N états que parmi les extensions de $\mathbf{F}_p(\zeta_N)$: en effet si (C, σ) est définie sur k, alors σ est défini sur k et, notant A une matrice à coefficients dans k lui correspondant, il existe $\zeta \in \mu_n^*$ tel que $(1+\zeta)^2 \det A - \zeta\,(\mathrm{tr}\, A)^2 = 0$ (proposition 1.1). Si on est en caractéristique 0 et $N \geq 5$, ceci impose que $\zeta_N \in k$. Nous supposons donc délibérément que les corps envisagés contiennent tous ζ_N. Rappelons les notions élémentaires :

– corps de définition : κ est un tel corps si il existe $(C_0,\sigma_0) \overset{\bar{k}}{\simeq} (C,\sigma)$ définie sur κ.
– corps des modules : c'est le corps des invariants κ de k_s sous

$$G = \{\, \rho \in \mathrm{Aut}(k_s/\mathbf{F}_p) \,|\, (C,\sigma)^\rho \overset{\bar{k}}{\simeq} (C,\sigma) \,\}\,,$$

en d'autres termes, pour $\rho \in \mathrm{Aut}(k_s/\mathbf{F}_p)$, $(C,\sigma)^\rho \simeq (C,\sigma) \iff \rho$ fixe κ.

Proposition 2.2.1 *Soit N avec $(N,2,p)=1$. Soit (C,σ) une courbe de Potts à N états, définie (a priori) sur k_s. Son corps de définition minimal est égal à son corps des modules, et c'est $\mathbf{F}_p(\zeta_N,j)$.*

Preuve : Soit (C,σ) d'invariant modulaire j. La courbe C_j de modèle affine

$$\begin{aligned} y^2 = x^{2N} + (1+4j)x^N + j(1+4j) \qquad & \text{si } j \neq -1/4 \\ y^2 = x^{2N} - 1 \qquad & \text{si } j = -1/4 \end{aligned}$$

est d'invariant modulaire égal à j, et définie sur $\mathbf{F}_p(j)$. Son automorphisme σ est défini sur $\mathbf{F}_p(\zeta_N)$.

Pour le corps des modules, soit (C,σ) d'invariant $j \in k_s$, montrons que $\mathbf{F}_p(\zeta_N,j) = k_s^G$. On montre d'abord l'inclusion directe. Si $C^\rho \simeq C$, alors $j(C)^\rho = j(C^\rho) = j(C)$; d'autre part, . Pour voir l'inclusion $\supset$, donnons-nous $j_1 \in k_s^G$; alors

$$\begin{array}{ll} & C^\rho \simeq C \Rightarrow \rho(j_1) = j_1 \\ \text{i.e.} & \rho(j(C)) = j(C) \Rightarrow \rho(j_1) = j_1 \\ \text{i.e.} & \mathrm{Gal}(k_s/\mathbf{F}_p(j)) \subset \mathrm{Gal}(k_s/\mathbf{F}_p(j_1)) \\ \text{donc} & \mathbf{F}_p(j_1) \subset \mathbf{F}_p(j) \text{ par théorie de Galois.} \end{array}$$

■

Remarque 2.2.2 On a montré au passage (courbes C_j) qu'on avait bien une bijection

$$\{\,\text{Courbes de Potts}\,\} \Big/ \text{isomorphismes} \quad \overset{1-1}{\longrightarrow} \quad \mathbf{A}^1_*(k) \quad .$$

2.3 Courbes de Potts à N états, $p\,|N$

On suppose ici que $p \neq 2$; k est un corps de caractéristique p. Dans ce paragraphe, nous voulons étudier les courbes de Potts dans le cas où le nombre d'états N est divisible par p. Alors, la donnée de ramification qui constitue la définition 0.1 n'a plus de sens, mais on a vu qu'une définition équivalente 0.1.ter pouvait être obtenue, et celle-ci semble satisfaisante lorsque $p|N$. On conviendra donc que :

Définition 2.3.1 *Lorsque $p|N$, une courbe de Potts à N états est une courbe hyperelliptique de genre $g(C) = N-1$, avec un automorphisme σ d'ordre N, telle que $g(C/\sigma) = 0$. Cette donnée est notée (C,τ,σ).*

Il n'est pas encore clair que de telles courbes existent. Ceci étant, on observe que l'automorphisme de Potts induit, sur le quotient $C/\tau \simeq \mathbf{P}^1$, un automorphisme d'ordre N. Par la proposition 1.1, le seul cas possible est

$$N = p\,,$$

et l'automorphisme $\bar{\sigma}$ induit est $x \mapsto x+1$ à conjugaison près. D'une autre manière, notons que la formule de Riemann-Hurwitz, telle qu'on la trouve dans [Se], interdit a priori une valuation $v_p(N)$ supérieure ou égale à 2. Désormais C est une courbe de Potts à p états. Comme dans la proposition 2.1.2, il est facile de compter $2p$ points fixes pour l'involution hyperelliptique τ, qui constituent deux orbites de σ (on remonte les 2 points fixes de l'involution induite sur C/σ). Le modèle affine ainsi décrit est l'équation

$$y^2 = (x^p - x)^2 + A(x^p - x) + B \qquad (A,B \in \bar{k}). \tag{9}$$

On veut maintenant définir un invariant modulaire pour les courbes de Potts. Il est clair ici que le problème modulaire est différent selon que l'on cherche à classifier les objets (C,G) ou (C,σ) (voir remarque initiale suivant 0.1). Dans le premier cas, un isomorphisme $\varphi : (C,G) \to (C',G')$ est un isomorphisme $\varphi : C \to C'$ qui envoie σ sur un générateur $(\sigma')^i$ de G' : $\varphi\sigma\varphi^{-1} = \sigma'^i$. Définissons des invariant modulaires distincts, dans $\mathbf{A}^1_*(k)$, par

$$\mathrm{j}(C,G) = \frac{1}{(A^2-4B)^{\frac{p-1}{2}}} \qquad \text{et} \qquad j(C,\sigma) = \frac{1}{A^2-4B}\,.$$

Proposition 2.3.2

1. *deux « couples » de Potts (C,G) et (C',G') sont $\bar{k}$-isomorphes ssi* $\mathrm{j} = \mathrm{j}'$.
2. *deux courbes de Potts (C,σ) et (C',σ') sont $\bar{k}$-isomorphes ssi $j = j'$.*

Preuve : 1. Soit C et C' données par une équation (7). Si on a un isomorphisme $\varphi : C \to C'$ avec $\sigma'\varphi = \varphi\sigma^i$ ($i \in \mathbf{F}_p^\times$), alors il passe au quotient sur $\mathbf{P}^1$ en un automorphisme tel que $\tilde{\varphi}(x+iu) = \tilde{\varphi}(x)+u'$, donc $\tilde{\varphi}(x) = rx+t$, $r = u'/iu \in \mathbf{F}_p^\times$, $t \in \bar{k}$. À un point (x,y), φ associe $(rx+t, \pm ry)$, et en reportant dans l'équation de C',

$$\begin{aligned} r^2y^2 &= \big((rx+t)^p - (rx+t)\big)^2 + A'\big((rx+t)^p - (rx+t)\big) + B' \\ r^2y^2 &= r^2\left(x^p - x + t^p - t\right)^2 + A'r\left(x^p - x + t^p - t\right) + B' \\ y^2 &= (x^p-x)^2 + \underbrace{\frac{A' + 2r(t^p-t)}{r}}_{A}(x^p-x) + \underbrace{\frac{r^2(t^p-t)^2 + A'r(t^p-t) + B'}{r^2}}_{B} \end{aligned}$$

d'où $A^2 - 4B = \frac{A'^2 - 4B'}{r^2}$ et donc $\mathrm{j} = \mathrm{j}'$.

Réciproquement, supposons $\mathrm{j} = \mathrm{j}'$; on sait que w carré dans $\mathbf{F}_p^\times \Leftrightarrow w^{\frac{p-1}{2}} = 1$ donc il existe $r \in \mathbf{F}_p^\times$ tel que $A'^2 - 4B' = r^2(A^2-4B)$. Alors on choisit un $t \in \bar{k}$ racine de $t^p - t = \frac{1}{2r}(rA - A')$, d'où

$$A = \frac{A' + 2r(t^p-t)}{r} \quad \text{et} \quad B = \frac{1}{4}\left[A^2 - \frac{A'^2 - 4B'}{r^2}\right] = \frac{r^2(t^p-t)^2 + A'r(t^p-t) + B'}{r^2}$$

donc, en remontant les calculs ci-dessus, on voit que $\varphi : (x,y) \mapsto (rx+t, ry)$ donne une application birationnelle entre C et C' qui envoie $\sigma : x \mapsto x+1$ sur $\sigma' : x \mapsto x+r$.

2. Dans ce qui précède il suffit de faire $u = u' = 1$, ainsi que $i = 1$. On voit qu'alors $r = 1$, d'où le résultat. ■

Soit (C,σ) une courbe de Potts donnée par l'équation (9). Soit r, s les racines du trinôme $T^2 + AT + B$, et α (resp. β) une racine de $T^p - T - r$ (resp. $T^p - T - s$), de sorte que (9) s'écrit

$$y^2 = (x^p - x - r)(x^p - x - s) = \prod_{i=0}^{p-1}(x - \alpha + i)\prod_{i=0}^{p-1}(x - \beta + i)\ .$$

On connaît les automorphismes suivants :

$$\sigma(x,y) = (x+1, y) \quad ; \quad \tau(x,y) = (x,-y) \quad ; \quad \mu(x,y) = (\alpha + \beta - x, y)\ .$$

Proposition 2.3.3 *Soit (C,σ) une courbe de Potts à p états, alors le groupe des automorphismes de C est* $\mathrm{Aut}_{\bar{k}}(C) \simeq (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{D}_p$ *, de sorte que* $\mathrm{Aut}_{\bar{k}}(C,\sigma) \simeq (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z})$.

Preuve : Il est toujours vrai (*cf* proposition 2.1.5) que

- $<\tau>$ est d'ordre 2, distingué et central,
- $G = \mathrm{Aut}_{\bar{k}}(C)/ <\tau>$ s'identifie au sous-groupe de $\mathrm{Aut}(\mathbf{P}^1)$ des homographies qui préservent $\Sigma = O_\sigma(\alpha) \sqcup O_\sigma(\beta)$,
- $\mathbf{D}_p \subset G$ et $2p = [G : G_x]$, $\quad \forall x \in \Sigma$.

Soit Q un p-Sylow de G contenant σ ; par le théorème de Dickson il est élémentaire abélien. Supposons que $|Q| > p$, alors il existe $\theta \in Q$ commutant à σ (d'où $\theta(x) = x+u$), et n'appartenant pas à $<\sigma>$ (d'où $u \notin \mathbf{F}_p$). De plus θ stabilise Σ ; comme $u \notin \mathbf{F}_p$, θ permute les σ-orbites $O_\sigma(\alpha)$ et $O_\sigma(\beta)$. Ainsi

$$(\exists i, j \in \mathbf{F}_p) \qquad \begin{cases} \alpha + u = \beta + i \\ \beta + u = \alpha + j \end{cases}$$

donc $u = \frac{i+j}{2} \in \mathbf{F}_p$, ce qui est contradictoire. Par conséquent, $Q = <\sigma>$; on peut passer en revue les différentes possibilités du théorème de Dickson.

Si $G = \mathrm{PSL}_2(\mathbf{F}_p)$ ou $\mathrm{PGL}_2(\mathbf{F}_p)$, alors $|G_\alpha| = (p^2-1)/d$ avec $d = 1$ ou 2. Cet ordre est premier à p, donc G_α est cyclique, ceci contredit le corollaire 1.2.

Il ne reste que la possibilité de $G = Q \rtimes C = <\sigma> \rtimes <\varphi>$, car $\mathfrak{A}_5$ est écarté par les mêmes arguments que dans le cas $(N,p) = 1$. L'ordre de φ est $2m$ premier à p ; quitte à changer le point α dans l'orbite, on peut supposer que l'isotropie de α est $G_\alpha = <\varphi^2>$. Comme Q est distingué, $\varphi^{-1}\sigma\varphi = \sigma^k$, $k \in \mathbf{F}_p^*$,

dont on déduit que $\varphi(x) = \frac{1}{k}x + b$, pour un $b \in \bar{k}$. Comme φ^2 fixe α, on tire $(k^2-1)\alpha = k(k+1)b$. Si $k+1 \neq 0$ ceci entraîne $\varphi(\alpha) = \frac{\alpha}{k} + b = \alpha$; donc on a en fait $k = -1$, $\varphi^2 = 1$ et $m = 1$. ■

L'analogue de la situation de la figure 1 est représenté ci-dessous. On voit que la symétrie remarquable obtenue auparavant pour $j = -1/4$ ne peut se produire pour une courbe à p états, car, pour s'intercaler entre les points de l'orbite de α, les points de l'orbite de β doivent prendre les valeurs « demi-entières » $\alpha + i/2$ qui ne sont autres que les valeurs entières $\alpha + i$, d'où $j = 0$: la courbe doit dégénérer.

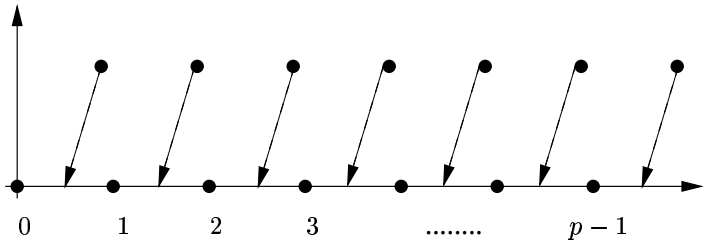


FIG. 2 – Collision des orbites dans le cas exceptionnel en caractéristique p

3 L'espace modulaire des courbes de Potts

Soit toujours N un entier impair. Nous avons établi, dans la section précedente, que lorsque k est un corps algébriquement clos de caractéristique différente de 2 et première à N, on avait une bijection entre la droite affine épointée $\mathbf{A}^1_* := \mathbf{A}^1 - \{0\}$ sur k et les classes d'isomorphisme de k-courbes de Potts à N états. Nous allons montrer maintenant que la droite affine épointée sur $\mathbf{Z}[\frac{1}{2N}]$ est l'espace modulaire (grossier) du champ des courbes de Potts.

Pour alléger nous notons $\mathbf{Z}_{2N} := \mathbf{Z}[\frac{1}{2N}]$. Nous identifierons un schéma T avec la catégorie (T) des schémas au-dessus de T, c'est-à-dire, avec son foncteur de points. Nous nous plaçons toujours dans le cadre de la définition 0.1 pour poser :

Définition 3.1 *Une famille de courbes de Potts à N états (N impair) est un morphisme de $\mathbf{Z}_{2N}$-schémas $p : C \to S$ projectif, lisse, associé à un S-automorphisme $\sigma : C \to C$ d'ordre N, tels que les fibres géométriques (C_s, σ_s) sont des courbes de Potts.*

Il est manifeste que la catégorie $\mathcal{P}$ fibrée sur $(\mathbf{Z}_{2N})$ (munie de la topologie étale), dont les objets sont les familles de courbes de Potts à N états, est un champ dit *de Potts*; par des arguments de [DM] repris dans [We], ce champ est algébrique. Il est connu [We] que ce champ admet un espace de modules grossier, ce dont nous rappelons la définition :

Définition 3.2 *Un espace modulaire grossier pour le champ $\mathcal{P}$ est un schéma $\mathbf{P} \in (\mathbf{Z}_{2N})$ avec un morphisme $\mathcal{P} \to (\mathbf{P})$, tels que*

- *pour tout point géométrique* $\mathrm{Spec}(k)$ *de* $\mathrm{Spec}\,\mathbf{Z}_{2N}$, *le morphisme $\mathcal{P} \to (\mathbf{P})$ induit une bijection $\mathcal{P}(\mathrm{Spec}\,k)/\simeq \longrightarrow \mathbf{P}(k)$ entre les classes d'isomorphisme de familles de $\mathcal{P}$ au-dessus de k, et les points k-rationnels de $\mathbf{P}$,*
- *tout morphisme $\mathcal{P} \to (P)$ à valeurs dans un schéma $P \in (\mathbf{Z}_{2N})$ factorise par $\mathcal{P} \to (\mathbf{P})$.*

3.1 Démonstration du résultat

Nous allons montrer le résultat suivant :

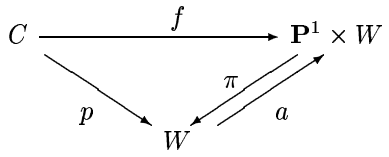
Théorème 3.1.1 *Il existe un morphisme de foncteurs $\Phi : \mathcal{P} \to (\mathbf{A}^1_*)$ qui fait de $\mathbf{A}^1_* = \mathrm{Spec}\left(\mathbf{Z}_{2N}[j, \frac{1}{j}]\right)$ un espace modulaire grossier pour les courbes de Potts à N états.*

Soit une famille de courbes de Potts $p : C \to S$. Nous allons construire de manière canonique un morphisme classifiant $j : S \to \mathbf{A}^1_*$, ce qu'il suffit de faire localement (pour la topologie fppf ou la topologie étale) sur la base S, pourvu que la construction soit canonique. D'abord, il est nécessaire de voir $p : C \to S$ comme une courbe hyperelliptique :

Proposition 3.1.2 *Il existe, après un changement de base étale fini surjectif $W \to S$, une involution $\tau : C_W \to C_W$ qui fait de $p : C_W \to W$ une famille de courbes hyperelliptiques (au sens de* [KL]*).*

Preuve : Soit $G =< \sigma >$. Comme C est projectif sur S, le quotient $D = C/G$ existe et la projection naturelle $f : C \to D$ est finie de degré N et étale (car G agit fidèlement). On peut ajouter que sa formation commute au changement de base (donc aux fibres géométriques), comme précisé par [KL, th. 4.12]. Ainsi pour $s : \operatorname{Spec}\Omega \to S$ un point géométrique, $D_s \simeq C_s/G \simeq \mathbf{P}^1$, c'est-à-dire que D est un fibré en droites sur S. Par un changement de base étale surjectif (que nous n'écrivons pas) on peut le « détordre » de sorte que $D \simeq \mathbf{P}^1 \times S$.

Pour construire τ on doit manipuler la ramification de f. Soit $W = C^G$ le sous-schéma de Weierstraß des points fixes de G : il est étale et fini de degré 4 sur S, et associé à un diviseur de Cartier effectif relatif sur S. L'immersion fermée $i : W \hookrightarrow C$ induit après le changement de base par W, une section a de $\pi : \mathbf{P}^1 \times W \to W$.



Quitte à réitérer avec $W - A$ où A est l'image de a, on suppose qu'on dispose de quatre sections a, b, c, d *disjointes* (à cause de la description de la ramification sur une fibre). Leurs images sont des sous-schémas fermés A, B, C, D qui sont supports de diviseurs de Cartier effectifs encore notés A, B, C, D — ce que l'on peut noter en termes de faisceaux d'idéaux : $\mathscr{I}_A \simeq \mathcal{O}_{\mathbf{P}^1_W}(-A)$, etc. Quitte à localiser, nous supposons maintenant $W = \operatorname{Spec} R$ affine. Comme A, B, C, D sont images de sections de π les faisceaux inversibles $\mathscr{I}_A, \ldots, \mathscr{I}_D$ sont de degré 1, c'est-à-dire qu'il existe un recouvrement ouvert $\{U_i = \operatorname{Spec} R_i\}_{i \in I}$ — que l'on suppose commun aux quatre faisceaux, en le raffinant si besoin est — avec des polynômes homogènes de degré 1 dans $R_i[X, Y]$, tels que

$$\left\{ \begin{array}{ll} \mathscr{I}_{A|U_i} & = (a_2^{(i)} X - a_1^{(i)} Y)\, \mathcal{O}_{U_i} \\ \mathscr{I}_{B|U_i} & = (b_2^{(i)} X - b_1^{(i)} Y)\, \mathcal{O}_{U_i} \\ \quad \vdots & \end{array} \right.$$

Soit alors la transformation $\tau^{(i)} \in \operatorname{End}(R_i^2)$ donnée par

$$\tau^{(i)} = \left[\begin{array}{cc} a_1 b_1 c_2 d_2 - c_1 d_1 a_2 b_2 & a_1 c_1 d_1 b_2 + b_1 c_1 d_1 a_2 - a_1 b_1 c_1 d_2 - a_1 b_1 d_1 c_2 \\ (a_1 b_2 + a_2 b_1) c_2 d_2 - (c_1 d_2 + c_2 d_1) a_2 b_2 & -(a_1 b_1 c_2 d_2 - c_1 d_1 a_2 b_2) \end{array} \right]$$

(les indices i sont omis). Son déterminant

$$\delta = -(a_1 c_2 - a_2 c_1)(a_1 d_2 - a_2 d_1)(b_1 c_2 - b_2 c_1)(b_1 d_2 - b_2 d_1)$$

est inversible dans R_i. En effet soit $\mathfrak{m}$ un idéal maximal de R_i, et Ω une extension algébriquement close de $R_i/\mathfrak{m}$. Cela définit un Ω-point w de W ; la fibre correspondante est une courbe de Potts C_w dont les points de branchement dans $\mathbf{P}^1_\Omega$ sont $a_w := [a_{1,w} : a_{2,w}], \ldots, d_w := [d_{1,w} : d_{2,w}]$, d'où

$$\delta \bmod \mathfrak{m} = \delta_w = -(a_w - c_w)(a_w - d_w)(b_w - c_w)(b_w - d_w) \neq 0$$

(en coordonnées non homogènes). Les $\tau^{(i)}$ se recollent en une involution de $\mathbf{P}^1_W$ — le fait que τ soit involutif provient de la nullité de la trace, cf proposition 1.1 — , qui vérifie clairement

$$\tau^* \mathscr{I}_A = \mathscr{I}_B \ , \quad \tau^* \mathscr{I}_C = \mathscr{I}_D$$

(l'expression locale de τ étant calquée sur l'expression dans le cas de la droite projective sur un corps).

La description 2.1.1 du revêtement cyclique $C \to C/G \simeq \mathbf{P}^1 \times W$ en termes de faisceaux inversibles est

$$\left\{ \begin{array}{l} \mathscr{L} = \mathcal{O}_{\mathbf{P}^1}(-2) \otimes \mathcal{O}_W \\ \mathscr{L}^N \simeq \mathcal{O}_{\mathbf{P}^1_W}(-\mathcal{D}) \quad \text{où} \quad \mathcal{D} = A + B + (N-1)C + (N-1)D. \end{array} \right.$$

Il est clair que τ respecte la donnée $(\mathscr{L}, \mathcal{D})$, donc il se relève en un automorphisme τ de C avec : $\tau\sigma = \sigma\tau$. Comme dans le cas d'une unique courbe de Potts, on peut se ramener à $\tau^2 = \mathrm{id}$. ■

Preuve du théorème 3.1.1 : Nous la séparons en deux étapes.

1ère étape : construction de j et de Φ.

Pour les résultats essentiels relatifs aux fibrés projectifs, nous renvoyons à [Ha]. Soit $p : C \to S$ une courbe de Potts sur S. Après un éventuel changement de base étale, on sait par la proposition 3.1.2 qu'il existe une involution globale $\tau \in \mathrm{Aut}_S(C)$. Soit $E = C/ <\tau>$ qui est un fibré en droites projectives sur S, $\pi : C \to E$ la projection naturelle et $q : E \to S$ le morphisme de structure. Comme σ commute à τ il induit un S-automorphisme d'ordre N sur E. Le diviseur $W \subset C$ des points fixes de G, de degré 4 sur S, a une image dans E qui est une 2-section étale de E/S. Quitte à faire une extension étale de la base, on se ramène au cas où cette section est somme de deux sections disjointes : $\Delta = \Delta_0 \sqcup \Delta_\infty$. Si on pose $\mathcal{O}(1) = \mathcal{O}(\Delta_0)$ (de degré 1 sur les fibres), alors E est l'espace fibré projectif $\mathbf{P}(\mathscr{V})$ associé à $\mathscr{V} = q_*(\mathcal{O}(1))$. Par ce choix, on a $\mathcal{O}(1)_{|\Delta_0} \simeq \mathcal{O}_{\Delta_0} \simeq \mathcal{O}_S$. La donnée de la section Δ_0 équivaut à celle d'un morphisme surjectif dont nous notons $\mathscr{M}$ le noyau :

$$0 \to \mathscr{M} \to \mathscr{V} \to \mathscr{L} = \mathcal{O}(1)_{|\Delta_0} \simeq \mathcal{O}_S \to 0$$

Par ailleurs la section Δ_∞ fournit une suite similaire

$$0 \to \mathscr{M}_\infty \to \mathscr{V} \to \mathscr{L}_\infty \to 0$$

et on a $\mathcal{O}(\Delta_\infty) = \pi^*(\mathscr{M}_\infty^{-1}) \otimes \mathcal{O}(1)$, ou encore $\pi^*(\mathscr{M}_\infty) = \mathcal{O}(-\Delta_\infty) \otimes \mathcal{O}(1)$. Le fait que les deux sections soient disjointes se traduit par : $\mathcal{O}(-\Delta_\infty)_{|\Delta_0} \simeq \mathcal{O}_{\Delta_0}$. Ainsi, par restriction à Δ_0,

$$\pi^*(\mathscr{M}_\infty)_{|\Delta_0} \simeq \mathcal{O}(1)_{|\Delta_0}$$

c'est-à-dire $\mathscr{M}_\infty \simeq \mathscr{L}$. L'isomorphisme inverse donne une flèche $\mathscr{L} \to \mathscr{M}_\infty \to \mathscr{V}$ qui scinde la suite exacte ci-dessus. Par suite, $E \simeq \mathbf{P}(\mathscr{M} \oplus \mathcal{O}_S)$; σ agit par multiplication par ζ_N^{-1} sur $\mathscr{M}$, et trivialement sur $\mathcal{O}_S$.

Considérons maintenant le revêtement double $h : C \to E$: il est décrit par la décomposition $h_*\mathcal{O}_C = \mathcal{O}_E \oplus \mathscr{L}$ et par une section $\theta \in \Gamma(E, \mathscr{L}^{-2})$, image de la section de Weierstraß. Comme $\mathscr{L}^{-1}$ est de degré N sur les fibres, on a $\mathscr{L}^{-1} \simeq \mathcal{O}(N) \otimes \pi^*\mathscr{K}$ (pour un $\mathscr{K} \in \mathrm{Pic}(S)$). Par restriction à Δ_0, comme $\theta_{|\Delta_0}$ est partout non nulle (les lieux fixes pour les actions respectives de G et de τ sont disjoints dans le cas ponctuel), on obtient $\mathscr{K}^2 \simeq \mathcal{O}_S$, donc $\mathscr{L}^{-2} \simeq \mathcal{O}_E(2N)$. Par conséquent on peut identifier θ à une section σ-invariante de

$$\Gamma(E, \mathcal{O}_E(2N)) = \Gamma(S, \pi_*\mathcal{O}_E(2N)) = \Gamma(S, \mathrm{Sym}^{2N}(\mathscr{V})) = \bigoplus_{j=0}^{2N} \Gamma(S, \mathscr{M}^j) \ .$$

L'invariance se traduit par $\theta \in \Gamma(S, \mathcal{O}_S \oplus \mathscr{M}^N \oplus \mathscr{M}^{2N})$. Il est facile de voir (en regardant sur les fibres) que la composante de θ sur $\mathcal{O}_S$ est inversible. On la suppose égale à 1, et on note $A \in \Gamma(S, \mathscr{M}^N)$, $B \in \Gamma(S, \mathscr{M}^{2N})$ les autres composantes (en utilisant des coordonnées globales X, Z sur $\mathbf{P}(\mathscr{V})$, on écrit : $\theta = X^{2N} + AX^NZ^N + BZ^{2N}$). Enfin B ne s'annule nulle part, donc $\mathscr{M}^{2N} \simeq \mathcal{O}_S$, de même que $A^2 - 4B$, donc

$$j = \frac{B}{A^2 - 4B} \quad \in \Gamma(S, \mathcal{O}_S)^\times$$

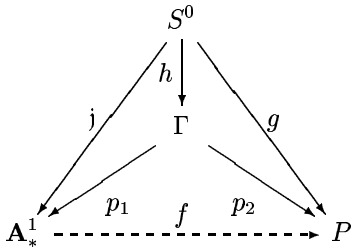
définit bien un morphisme $S \to \mathbf{A}^1_*$. Enfin il est clair que cette construction est fonctorielle, d'où le morphisme $\Phi : \mathcal{P} \to (\mathbf{A}^1_*)$.

2ème étape : vérification des propriétés d'universalité.

Le fait que $\Phi(\mathrm{Spec}\, k) : \mathcal{P}(\mathrm{Spec}\, k)/\simeq \to \mathbf{A}^1_*(k)$ soit bijectif, pour tout point géométrique de $\mathrm{Spec}\, \mathbf{Z}_{2N}$, est conséquence de la première section. Pour vérifier la seconde propriété, soit $\Psi : \mathcal{P} \to (P)$ un morphisme de champs. On utilise la forme (7) à un paramètre pour donner une famille tautologique, c'est-à-dire une famille dont le morphisme classifiant $S \to \mathbf{A}^1_*$ est fini surjectif. Considérons donc $S^0 = \mathrm{Spec}\left(\mathbf{Z}_{2N}\left[\lambda, \frac{1}{\lambda^2-1}\right]\right)$ et $p^0 : C^0 \to S^0$ la courbe décrite, comme revêtement de $\mathbf{P}^1_{S^0}$, par

$$\mathscr{L} = \mathcal{O}(-2) \otimes \mathcal{O}_{S^0} \quad \text{et} \quad s = Y(Z - \lambda Y)(Z^2 - Y^2)^{N-1} \ \in \Gamma(\mathbf{P}^1_{S^0}, \mathscr{L}^{-N}) \tag{10}$$

Son invariant $\mathrm{j} = \frac{1/4}{\lambda^2-1}$ détermine le morphisme classifiant $\mathrm{j} = \Phi(p^0) : S^0 \to \mathbf{A}^1_*$. Soit $g : S^0 \to P$ le morphisme $\Psi(p^0)$; soit $\Gamma \subset \mathbf{A}^1_* \times P$ l'image schématique de $h = (\mathrm{j}, g)$:



On remarque d'abord que, comme j est fini, et p_1 est séparé (car affine), alors h est fini. En particulier, h est fermé, donc ensemblistement $\Gamma = h(S^0)$. D'autre part Γ est intègre : il est irréductible car c'est l'image de S^0 irréductible, et réduit car muni de la structure réduite induite de sous-schéma fermé. On note ensuite que p_1 est fermé et bijectif. Il est surjectif et fermé, car j l'est, et injectif, car pour $\mu, \mu' \in S^0$,

$$\mathrm{j}(\mu) = \mathrm{j}(\mu') \Rightarrow C^0_\mu \simeq C^0_{\mu'} \Rightarrow g(\mu) = g(\mu')$$

où la dernière implication provient du diagramme de naturalité de Ψ pour le morphisme $\mathrm{Spec}\, k(\mu) \to S^0$, $k(\mu)$ désignant le corps résiduel du point μ :

$$\begin{array}{ccccc} C^0 \in & \mathcal{P}(S^0) & \longrightarrow & \mathcal{P}(\mathrm{Spec}\, k(\mu)) & \ni C^0_\mu \\ & \Big\downarrow \Psi & & \Big\downarrow \Psi & \\ g = \Psi(p^0) \in & h_P(S^0) & \longrightarrow & h_P(\mathrm{Spec}\, k(\mu)) & \ni g(\mu) = \Psi(p^0_\mu) \end{array}$$

Ainsi, p_1 est dominant, bijectif et séparable (car j l'est), donc c'est une application birationnelle. D'autre part il est quasi-fini, et $\mathbf{A}^1_*$ est normal, donc par le Théorème Principal de Zariski, p_1 est un isomorphisme. Soit alors f le composé $p_2 \circ p_1^{-1} : \mathbf{A}^1_* \to P$; il vérifie $g = f \circ \mathrm{j}$, donc donne lieu à une factorisation de Ψ

$$\mathcal{P}(\mathbf{Z}_{2N}) \to \mathbf{A}^1_*(\mathbf{Z}_{2N}) \xrightarrow{f} P(\mathbf{Z}_{2N})$$

Il alors formel de vérifier que le diagramme commute pour tout $\mathbf{Z}_{2N}$-schéma S remplaçant $\mathrm{Spec}(\mathbf{Z}_{2N})$. ■

On observe aussitôt que $\mathbf{A}^1_*$ n'est pas un espace modulaire fin : en général l'application $\Phi(S) : \mathcal{P}(S) \to \mathbf{A}^1_*(S)$ n'est pas bijective. En effet, il est clair par la proposition 2.1.4 qu'il suffit de choisir un corps k ne contenant pas les racines N-ièmes pour construire deux courbes de Potts à N états non isomorphes sur k, mais de même j-invariant. Par exemple, pour $a, b \in k$ et $\lambda \notin k^N$,

$$\begin{array}{ll} C_1 : & Y^2 = X^{2N} + aX^N + b \\ C_2 : & Y^2 = X^{2N} + \lambda a X^N + \lambda^2 b. \end{array}$$

montrent que $\Phi(\mathrm{Spec}(k))$ n'est pas injective. Par ailleurs, l'excès d'automorphismes lorsque $j = -1/4$ (voir proposition 2.1.5), qui se traduit par la ramification de j au-dessus de -1/4 :

$$j + \frac{1}{4} = \frac{A^2}{4(A^2 - 4B)}$$

empêche en général l'application $\Phi(S)$ d'être surjective.

3.2 Réduction modulo un entier premier ne divisant pas $2N$

D'après l'étude de 2.3, l'espace modulaire $\mathbf{P}_{\mathbf{Z}_{2N}}$ des courbes de Potts à N états ne se réduit pas modulo un entier p diviseur de N, si $N \neq p$. Par ailleurs, le cas de $N = p$ sera traité plus tard. Enfin, le paragraphe précédent (construction explicite du morphisme classifiant d'une famille $p : C \to S$), montre que l'on peut réduire l'invariant en p lorsque $(p, 2N) = 1$. Nous obtenons donc (comparer avec le cas elliptique [KaMa]) :

Théorème 3.2.1 *Soit $p \geq 3$ un entier premier, avec $(p, 2N) = 1$. Alors, l'espace modulaire $\mathbf{P}_{\mathbf{Z}_{2N}}$ se réduit en p sur $\mathbf{P}_{\mathbf{F}_p}$, c'est-à-dire que le morphisme de réduction $\mathcal{P}_{\mathbf{Z}_{2N}} \to \mathcal{P}_{\mathbf{F}_p}$ (changement de base par $\operatorname{Spec} \mathbf{F}_p \to \operatorname{Spec} \mathbf{Z}_{2N}$), entre champs de courbes de Potts à N états, rend le carré suivant commutatif :*

$$\begin{array}{ccc} \mathcal{P}_{\mathbf{Z}_{2N}} & \xrightarrow{red} & \mathcal{P}_{\mathbf{F}_p} \\ \downarrow & & \downarrow \\ \mathbf{P}_{\mathbf{Z}_{2N}} & \longrightarrow & \mathbf{P}_{\mathbf{F}_p} \end{array}$$

■

3.3 Calcul du groupe de Picard du problème modulaire

De ce qui précède il ressort que, pour tout entier $N \geq 3$ premier à $2p$, le schéma modulaire de Potts $\mathbf{P}_{\mathbf{Z}_{2N}}$ relatif au niveau N, est le même. Cependant nous allons voir que les groupes de Picard associés à la topologie modulaire (dont les ouverts sont les familles de courbes de Potts) sont distincts.

Renvoyons à la discussion de [Mu1], qui introduit le concept de groupe de Picard modulaire, et reprenons simplement la définition :

Définition 3.3.1 *Un faisceau inversible $\mathscr{L}$ sur le champ $\mathcal{P}$ est la donnée*

- *d'un faisceau inversible $\mathscr{L}(p)$ sur S, pour toute famille $p : C \to S$,*
- *d'un isomorphisme $\mathscr{L}(F) : \mathscr{L}(p') \xrightarrow{\sim} g^*\mathscr{L}(p)$ pour tout morphisme $F : p' \to p$; ces isomorphismes doivent être compatibles à la composition en un sens évident.*

Le groupe de Picard $\operatorname{Pic}(\mathcal{P})$ est l'ensemble des classes d'isomorphisme de faisceaux inversibles, muni du produit tensoriel évident.

En regardant l'action des automorphismes d'une courbe de Potts on va définir un morphisme

$$\beta : \operatorname{Pic}(\mathcal{P}) \to (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2N\mathbf{Z}).$$

Dans toute la suite on note, lorsque $j = -1/4$, $\sqrt{\sigma}$ l'automorphisme exceptionnel, de sorte que $G = \operatorname{Aut}(C, \sigma)$ est engendré par τ, et σ ou $\sqrt{\sigma}$.

Construction du morphisme β :

Soit $\mathscr{L}$ un faisceau inversible sur une famille $p : C \to S$, par la définition 3.3.1 ci-dessus pour le morphisme F constitué par le S-morphisme $\tau : C \to C$, il existe un (auto-)morphisme $\mathscr{L}(\tau) : \mathscr{L}(p) \to \mathscr{L}(p)$; un tel objet est la multiplication par une section globale β_1 de $\mathcal{O}_S^\times$. Par ailleurs comme τ est involutif, $(\beta_1)^2 = 1$.

Par ailleurs, comme τ induit l'involution hyperelliptique sur les fibres, il est clair que $\beta_1(\mathscr{L}_s)$ est une fonction continue de s. Considérant une famille à base connexe qui contient dans ses fibres toutes les classes de courbes de Potts (on en a déjà rencontré une), on voit que $\beta_1(\mathscr{L})$ est bien défini comme étant $\beta_1(\mathscr{L}_s)$ sur une fibre quelconque d'une famille quelconque de courbes de Potts.

De manière évidente, si $\mathscr{L}$ et $\mathscr{M}$ sont deux faisceaux inversibles sur $\mathcal{P}$, alors $(\mathscr{L} \otimes \mathscr{M})(\tau) = \mathscr{L}(\tau) \otimes \mathscr{M}(\tau)$, et c'est donc la multiplication par $\beta_1(\mathscr{L})\,\beta_1(\mathscr{M})$. On a donc obtenu un morphisme ; par ailleurs en menant la même construction avec σ ou $\sqrt{\sigma}$ au lieu de τ, on construit finalement $\beta = (\beta_1, \beta_2) : \operatorname{Pic}(\mathcal{P}) \to (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2N\mathbf{Z})$.

Le résultat suivant est assez intuitif :

Lemme 3.3.2 *β est surjectif.*

Preuve : Pour montrer la surjection on est tenté, comme dans [Mu1], d'évaluer β sur le faisceau déterminant $\omega_C = \bigwedge^{N-1} \Omega_C$, avec Ω_C le faisceau des 1-formes différentielles. Sur la courbe hyperelliptique $C : y^2 = x^{2N} + Ax^N + B$, il est classique de calculer une base de $\Gamma(C, \Omega_C)$, qui de plus a la vertu de diagonaliser l'action de G :

$$\begin{array}{ll} \varphi_i = x^{i-1}\frac{dx}{y} & (1 \leq i \leq N-1) \\ \sigma^*\varphi_i = \zeta_N^i \varphi_i & \text{ou } \sqrt{\sigma}^*\varphi_i = \zeta_{2N}^i \varphi_i \\ \tau^*\varphi_i = -\varphi_i\,. & \end{array}$$

Malheureusement l'action induite sur ω_C est triviale. À la place on remarque qu'on peut tirer profit du fait que l'action n'est pas triviale sur Ω_C et ses sous-faisceaux propres. En effet, on a un scindage

$$\Omega_C = \oplus_{i=1}^{N-1} \mathscr{F}_i$$

où $\mathscr{F}_i = \ker(\sigma^* - \zeta^i \,\mathrm{id})$ est un faisceau inversible. L'action de σ sur $\mathscr{F}_1$ est (tautologiquement) la multiplication par ζ_N, et l'action de $\sqrt{\sigma}$ est la multiplication par ζ_{2N}. On obtient $\beta(\mathscr{F}_1) = (-1, \zeta_{2N})$.

On doit exhiber un autre élément pour engendrer $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2N\mathbf{Z})$. On sait que la donnée d'une courbe $C \to S$ et de son involution τ détermine canoniquement un faisceau inversible $\mathscr{L}$ de degré $-N$ sur $C/ < \tau >$:

$$\begin{array}{ccc} C & \xrightarrow{\quad\pi\quad} & C/\tau \leftarrow \text{faisceau } \mathscr{L} \\ & {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle q} & \\ & S & \end{array}$$

On peut définir un faisceau $q_*(\mathscr{L}^{-1})$ sur S, ce faisceau est localement libre de rang $N+1$. Si $S = \mathrm{Spec}(k)$, le quotient π est donné sur l'équation habituelle (6) par $(x, y) \mapsto x$; le faisceau $q_*(\mathscr{L}^{-1})$ est $\Gamma(\mathbf{P}^1_k, \mathcal{O}(N))$, il s'agit des polynômes homogènes en (x, x') de degré N ; σ agit par multiplication par ζ_N sur x, et trivialement sur x'. De la même façon qu'au-dessus on remarque que l'action diagonale de σ permet de scinder le faisceau en sous-faisceaux localement libres

$$q_*(\mathscr{L}^{-1}) = \oplus_{i=0}^{N} \mathscr{G}_i$$

où $\mathscr{G}_i = \ker(\sigma^* - \zeta^i \,\mathrm{id})$. Si $i \geq 1$, $\mathscr{G}_i$ est un faisceau inversible, et $\mathscr{G}_0$ est localement libre de rang 2. On a illico $\beta(\mathscr{G}_1) = (1, \zeta_{2N})$; il est clair que $\beta(\mathscr{F}_1)$ et $\beta(\mathscr{G}_1)$ engendrent $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2N\mathbf{Z})$. ■

De manière analogue au cas elliptique, on a :

Proposition 3.3.3 *Lorsque $(N, p, 2) = 1$, le groupe de Picard de $\mathcal{P}$ est canoniquement isomorphe à $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2N\mathbf{Z})$.*

Preuve : Suivons Mumford [Mu1, §6, p. 74, Main Theorem]. Pour obtenir l'injectivité de β, soit $\mathscr{L} \in \mathrm{Pic}(\mathcal{P})$ tel que $\beta(\mathscr{L}) = 0$; il suffit de montrer que $\mathscr{L}(p) \simeq \mathcal{O}_S$ pour une famille $p : C \to S$ contenant toutes les courbes de Potts dans ses fibres. On en a déjà donné une, à savoir la famille (10) notée p désormais.

L'ouvert (dans la topologie modulaire) correspondant à p est la donnée de $j : S \to \mathbf{A}^1_*$ (qui est plat et surjectif) et du revêtement $I \to S$, de groupe $\mathbf{Z}/2N\mathbf{Z}$, où $I := \mathrm{Isom}(p, p)$. On considère les compositions $q_i = p_i \circ g \circ f, \quad i = 1, 2$:

$$I \xrightarrow{\ f\ } \widetilde{S \times_{\mathbf{A}^1_*} S} \xrightarrow{\ g\ } S \times_{\mathbf{A}^1_*} S \underset{p_1}{\overset{p_2}{\rightrightarrows}} S$$

(le tilde $\tilde{}$ désigne la normalisation). Le morphisme f est un revêtement étale cyclique $2N$-uple. Par définition d'un faisceau inversible, on a un isomorphisme ψ

$$q_1^* \mathscr{L} \xrightarrow{\sim} \mathscr{L}(\pi_I) \xrightarrow{\sim} q_2^* \mathscr{L} \quad .$$

A ce stade, on utilise $\beta(\mathscr{L}) = 0$ pour montrer que ψ provient en fait d'un isomorphisme $\psi_0 : p_1^* \mathscr{L} \xrightarrow{\sim} p_2^* \mathscr{L}$: ici tout se passe tel que dans [Mu1]. On observe ensuite que ψ_0 est une donnée de descente relativement au morphisme plat $j : S \to \mathbf{A}^1_*$, pour le faisceau inversible $\mathscr{L} = \mathscr{L}(p)$ sur S. Par un théorème de descente de Grothendieck, on obtient l'existence d'un faisceau inversible $\mathscr{L}_0$ sur $\mathbf{A}^1_*$, et d'un isomorphisme $\phi : \mathscr{L}(p) \xrightarrow{\sim} j^* \mathscr{L}_0$. Comme $\mathrm{Pic}(\mathbf{A}^1_*) = 0$, on a en fait $\mathscr{L}_0 \simeq \mathcal{O}_{\mathbf{A}^1_*}$, puis $\mathscr{L} \simeq \mathcal{O}_S$, ce que l'on voulait. ■

3.4 Compactification

Soient les données de Potts $G = \mathbf{Z}/N\mathbf{Z}$, $g = N - 1$ et ξ la ramification précisée dans la définition 0.1. Pour déterminer les points du bord on utilise 1) le morphisme discriminant $\overline{H}_{g,G}(\xi) \to \overline{M}_{0,(2,2)}$, qui à une classe de courbe $[C]$ associe $[C/G]$ marquée par les points de branchement, et 2) la description combinatoire des courbes stables à l'aide de leur graphe dual Γ (voir [DM], [Be]). Dans ces graphes, par une demi-arête ondulée, on indiquera des points marqués. Soit donc (C, G) une courbe de Potts (stable)

du bord. On a $\Gamma_\Sigma = \Gamma_C/G$, où $\Sigma = C/G$ est de genre nul. Rappelons que $g' = \sum_i g_{\Sigma_i} + h^1(\Gamma_\Sigma)$, et que par conséquent les composantes irréductibles Σ_i de Σ sont toutes rationnelles, et que Γ_Σ est un arbre (connexe). En tenant compte des quatre points marqués (ce sont les points de la donnée de ramification, réguliers sur C) et des conditions de stabilité, Γ_Σ est donc l'un des deux graphes

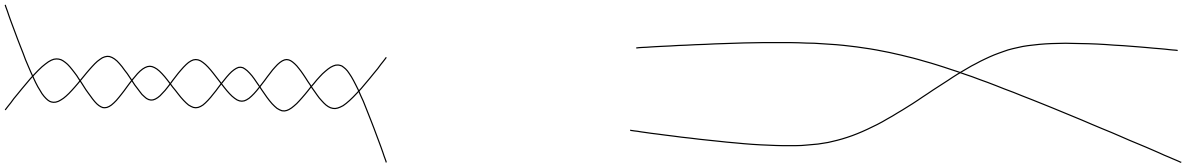
Mais comme G est cyclique, il n'y a pas d'isotropies diédrales possibles, ainsi un point double de C a pour image un point double dans Σ [Be, lemme 5.1]. Le premier graphe est donc écarté.

Soit C_i, $i = 1, 2$, des composantes irréductibles de C au-dessus de Σ_i, choisies avec un point d'intersection p (double). Soit $H = G_p$ l'isotropie de ce point double, et h l'indice de H dans G. Soit $a \in C_1$ un point de ramification ; son stabilisateur est par hypothèse $G_a = G$. Or, comme a appartient à la seule composante C_1, on voit que G_a est inclus dans le stabilisateur G_1 de C_1. En conséquence, $G_1 = G$ et de même $G_2 = G$; donc $C = G.C_1 \cup G.C_2 = C_1 \cup C_2$ n'a que deux composantes irréductibles.

Ecrivons maintenant la formule de Riemann-Hurwitz pour les restrictions $\pi_{|C_i}$, de C_i à valeurs dans $C_i/G_i \simeq \Sigma_i \simeq \mathbf{P}^1$. Comme il n'y a qu'une orbite de points doubles, on sait que le nombre de ces points est $|G.p| = |G/G_p| = h$. La formule fournit :

$$2g_i - 2 = N(-2) + \underbrace{2(N-1)}_{(r)} + \underbrace{h(N-h)}_{(d)} = h(N-h) - 2, \quad \forall i = 1, 2.$$

où (r) est la contribution des points (marqués) de ramification, et (d) la contribution des points doubles. En particulier $g_1 = g_2$, or on sait que $g(C) = N - 1 = g_1 + g_2 + h^1(\Gamma_C) = g_1 + g_2 + h - 1$. Ainsi, $h(N-h) = 2g_1 = N - h$, donc $h = N$ ou 1. Les deux courbes correspondantes sont



2 branches $\simeq \mathbf{P}^1$ avec N intersections

2 branches de genre $\frac{N-1}{2}$

Il n'est pas difficile d'identifier la première comme étant la courbe de Potts stable d'invariant $j = \infty$ et la seconde, celle d'invariant $j = 0$, dans le compactifié $\overline{\mathbf{P}} = \mathbf{P}^1$.

4 Le niveau $N = p$

4.1 Espace modulaire pour les courbes à p états en caractéristique p

Dans ce cas nous formulons :

Définition 4.1.1 *Une famille de courbes de Potts à p états en caractéristique p est un triplet (C, σ, τ) de S-objets, $S \in (\mathbf{F}_p)$, avec $C \to S$ projectif lisse, $\sigma : C \to C$ d'ordre p, $\tau : C \to C$ involutif, tel que les fibres géométriques (C_s, σ_s, τ_s) sont des courbes de Potts au sens de la définition 0.1.ter. Le champ des courbes de Potts à p états en caractéristique p est encore noté $\mathcal{P}$.*

Donnons tout d'abord le lemme immédiat :

Lemme 4.1.2 *Soit A une $\mathbf{F}_p$-algèbre et $\psi \in A$ inversible. Soit σ l'automorphisme de $A[X]$ agissant par $X \mapsto X + \psi$. Alors l'algèbre des invariants $A[X]^\sigma$ est $A[X^p - \psi^{p-1}X]$.* ■

Alors l'existence d'un espace modulaire grossier subsiste :

Théorème 4.1.3 *Il existe un morphisme $\Phi : \mathcal{P} \to (\mathbf{A}^1_{*,\mathbf{F}_p})$ qui fait de $\mathbf{A}^1_{*,\mathbf{F}_p}$ un espace modulaire grossier pour les courbes de Potts à p états en caractéristique p.*

Avant de donner la preuve, faisons la remarque suivante. Nous rappelons (calculs de 2.3.2) qu'un changement de variables préservant la forme de l'équation $y^2 = (x^p - x)^2 + A(x^p - x) + B$ est de la forme $(x, y) \mapsto (x + t, y)$. Par une telle transformation, on a $A' = A + 2\wp(t)$ et $B' = B + A\wp(t) + \wp(t)^2$. Ainsi pour k une extension de $\mathbf{F}_p$, on a une action du groupe additif $\mathbf{G}_a(k)$ sur $k[A, B]$:

$$t \in k \text{ agit par } (A, B) \mapsto (A + 2\wp(t), B + A\wp(t) + \wp(t)^2)$$

(il est facile de voir que c'est bien une action). La classification des courbes de Potts via celle des couples (A, B) peut s'exprimer en disant que l'espace modulaire du problème de Potts à p états en caractéristique p est le quotient

$$\mathbf{A}^2_{A,B} - \{A^2 - 4B = 0\} \Big/ \mathbf{G}_a$$

Dans $k[A, B]$ on note $j = \frac{1}{A^2 - 4B}$; montrons qu'en effet

$$\frac{\operatorname{Spec} k[A, B, j]}{\mathbf{G}_a(k)} \;=\; \operatorname{Spec}\left(k[A, B, j]^{\mathbf{G}_a(k)}\right) = \mathbf{A}^1_{*,k} \; .$$

Pour expliciter l'algèbre $k[A, B, j]^{\mathbf{G}_a(k)}$, soit $t \in k$ et P un polynôme t-invariant ; comme $B = (A^2 - 1/j)/4$, c'est un polynôme en A, j et $1/j$. Ecrire qu'il est t-invariant, c'est écrire que, comme polynôme dans $k[j, 1/j][A]$, il est invariant par $A \mapsto A + \wp(2t)$. Par 4.1.2, c'est un polynôme en $A^p - \wp(2t)^{p-1}A$, ainsi

$$k[A, B, j]^t = k[j, 1/j, A^p - \wp(2t)^{p-1}A] \qquad \text{donc} \qquad k[A, B, j]^{\mathbf{G}_a(k)} = k[j, 1/j] \; .$$

Ainsi l'espace modulaire $\mathbf{A}^1_*$ est bien le quotient attendu ; à la différence du cas $p \not| N$, $\mathbf{G}_a$ tient le rôle de $\mathbf{G}_m$, et n'est plus réductif. La démonstration qui suit consiste essentiellement à effectuer ce quotient « en familles ».

Preuve de 4.1.3 : Reprenons la démonstration et les notations de 3.1.1. Soit (C, σ, τ) une courbe de Potts à p états, en caractéristique p, sur S. Soit $\pi : C \to C/ <\tau>$. Alors σ induit un automorphisme d'ordre p sur $E = C/ <\tau>$, encore noté σ. Soit $G =< \sigma >$, le diviseur des points fixes $W = C^G$, de degré 4 sur S, n'est plus étale. Néanmoins son image dans E : $\Delta = E^G$ est un diviseur de Cartier effectif relatif sur S, de degré 2 ; en perticulier il est fppf sur S. En effectuant le changement de base $\Delta \to S$, l'inclusion $\Delta \hookrightarrow E$ donne une section i de π. Par ce changement de base, le pullback de $\Delta \subset E$ vaut $2i(\Delta)$. Quitte donc à changer S en Δ et Δ en $i(\Delta)$, nous conservons nos notations et supposons que Δ est un diviseur de Cartier effectif sur E, de degré 1.

En posant $\mathcal{O}(1) = \mathcal{O}(\Delta)$ et $\mathscr{V} = q_*\mathcal{O}(1)$, on a $E = \mathbf{P}(\mathscr{V})$ et une suite exacte

$$0 \to \mathscr{M} \to \mathscr{V} \to \mathcal{O}_S \to 0 \tag{11}$$

qui, ici, n'est pas scindée globalement. Nous pouvons, comme mentionné dans la section 3.1, nous restreindre à un ouvert affine de la base S sur lequel les faisceaux sont libres : $\mathscr{M} \simeq \mathcal{O}_S$, etc. Comme on est alors sur un schéma affine, la suite (11) est scindée : $\mathscr{V} = \mathscr{M} \oplus \mathcal{O}_S$.

Décrivons l'action de σ sur $\mathscr{V}$. Comme σ est un automorphisme (de E), on a $\sigma^*\mathcal{O}(1) \simeq \pi^*\mathscr{K} \otimes \mathcal{O}(1)$. De plus σ est l'identité sur Δ, donc en restreignant à Δ il vient $\mathcal{O}_S \simeq \mathscr{K} \otimes \mathcal{O}_S$ donc $\mathscr{K}$ est trivial. En conséquence on a un isomorphisme $u_\sigma : \sigma^*\mathcal{O}(1) \to \mathcal{O}(1)$. On obtient un autre tel isomorphisme en multipliant par une section globale de $\mathcal{O}_S$ jamais nulle ; ainsi on peut rendre u_σ canonique en exigeant de plus $u_{\sigma\,|\Delta} = \mathrm{id}$. D'autre part, le morphisme σ est décrit par un morphisme surjectif de faisceaux

$$q^*\mathscr{V} \;\to\; \sigma^*\mathcal{O}(1) \overset{u_\sigma}{\simeq} \mathcal{O}(1) \; .$$

En prenant les images directes par q_*, on obtient un automorphisme $\varphi_\sigma : \mathscr{V} \to \mathscr{V}$ qui décrit l'action de σ sur $\mathscr{V}$. Comme $\sigma = \mathrm{id}$ sur Δ, cet automorphisme doit stabiliser le noyau $\mathscr{M}$ de (11) ; par suite il passe aussi au quotient en un morphisme $\mathscr{V}/\mathscr{M} \to \mathscr{V}/\mathscr{M}$. On obtient deux automorphismes

$$\varphi_{\sigma\,|\mathscr{M}} : \mathscr{M} \to \mathscr{M} \quad \text{et} \quad \bar{\varphi}_\sigma : \mathcal{O}_S \to \mathcal{O}_S$$

auxquels correspondent deux sections globales ζ et η de ${\mathcal{O}_S}^*$. Précisément, $\varphi_{\sigma\,|\mathscr{M}}$ est la multiplication par ζ, mais $(\varphi_\sigma)^p = \mathrm{id}$, donc $\zeta^p = 1$, puis $\zeta = 1$. De même, $\eta = 1$. En conséquence, $\varphi_\sigma - \mathrm{id}$ induit un

morphisme de $\mathcal{O}_S$ à valeurs dans $\mathscr{M}$, c'est-à-dire la multiplication par une section $\psi \in \Gamma(S, \mathcal{O}_S^*)$. Ainsi, φ_σ est de la forme $\left[\begin{smallmatrix} 1 & \psi \\ 0 & 1 \end{smallmatrix}\right]$ et ψ est partout non nulle. En fait, on voit que les ψ ainsi définies localement se recollent, ce qui montre que $\mathscr{M} \simeq \mathcal{O}_S$ (globalement), et de plus, en conjuguant par $\left[\begin{smallmatrix} \psi & 0 \\ 0 & 1 \end{smallmatrix}\right]$ on se ramène à $\psi = 1$.

Le revêtement double $h : C \to E$ est décrit par la décomposition $h_*\mathcal{O}_C = \mathcal{O}_E \oplus \mathscr{L}$ et par une section $\theta \in \Gamma(E, \mathscr{L}^{-2})$. Comme précédemment, $\mathscr{L}^{-2} \simeq \mathcal{O}_E(2p)$. Par conséquent on peut identifier θ à une section σ-invariante de

$$\Gamma(E, \mathcal{O}_E(2N)) = \Gamma(S, \mathrm{Sym}^{2N}(\mathscr{V})) = \bigoplus_{j=0}^{2N} \Gamma(S, \mathscr{M}^j) \ .$$

On obtient, en coordonnées globales X, T,

$$\theta = U(X^p - T^{p-1}X)^2 + A(X^p - T^{p-1}X)T^p + BT^{2p}$$

pour des sections U, A, B appartenant à $\Gamma(S, \mathcal{O}_S)$. En regardant sur les fibres on voit que U est partout non nulle : on la normalise par $U = 1$. De même, $A^2 - 4B$ ne s'annule nulle part, donc $j = \frac{1}{(A^2-4B)} \in \Gamma(S, \mathcal{O}_S)^\times$ définit un morphisme $S \to \mathbf{A}^1_*$.

Pour vérifier la propriété d'universalité, les arguments de la démonstration du théorème 3.1.1 se reconduisent tels quels ; le seul point est d'exhiber une famille tautologique. Ceci peut ici être fait en recollant au-dessus de $\mathbf{A}^1_*$ les deux schémas affines

$$\begin{cases} X_0 \subset \mathbf{A}^2 \times \mathbf{A}^1_* & \text{défini par} \quad y^2 = (x^p - x)^2 - \frac{1}{4j} = f(x) \\ X_1 \subset \mathbf{A}^2 \times \mathbf{A}^1_* & \text{défini par} \quad w^2 = f^*(v) = v^{2p} f(1/v) \end{cases}$$

La fibre au-dessus de j est une courbe de Potts d'invariant j. ■

Au vu du comportement des automorphismes (section 2.3), on peut se demander si l'espace modulaire est fin. Le schéma en automorphismes $\mathbf{Aut}_{(C,\sigma)/S}$, qui est dans tous les cas non ramifié (voir [DM]), est ici le schéma en groupes constant $S \times G$, où $G = (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z})$ (si on se restreint aux schémas de base $S/\mathbf{F}_p$ connexes).

Cependant, comme lorsque $(N, p) = 1$, il existe des couples de courbes (i.e. de familles triviales) sur un corps k, isomorphes sur $\bar{k}$ mais pas sur k. Précisément, choisissons un corps k tel que $\wp : x \mapsto x^p - x$ n'est pas surjectif, et prenons $\lambda \notin \wp(k)$. Par exemple, $k = \mathbf{F}_p$ et $\lambda = 1$ conviennent. Alors, on voit que

$$\begin{aligned} C_1 : &\quad y^2 = (x^p - x)^2 + A(x^p - x) + B \\ C_2 : &\quad y^2 = (x^p - x)^2 + (A + 2\lambda)(x^p - x) + B + \lambda A + \lambda^2 \end{aligned}$$

où $A, B \in k$, sont isomorphes sur $\bar{k}$ mais pas sur k. Par conséquent, l'espace modulaire n'est pas fin. On a donc l'exemple d'un problème modulaire dans lequel les automorphismes ne sont pas à l'origine de l'obstruction à la représentabilité du foncteur modulaire.

4.2 Espace modulaire en caractéristique mixte

Nous constatons que les courbes de Potts à p états ($p \geq 3$ un entier premier) peuvent être définies par 0.1.ter indépendamment de la caractéristique. Il est naturel de vouloir réunir les deux approches (caractéristique p et caractéristique 0), rejoignant ainsi les délicates questions de relèvement d'un revêtement de courbes (sauvagement) ramifié (de caractéristique p en caractéristique 0), ou de réduction d'un espace modulaire modulo p. Voir travaux [OSS], [BM], et récents travaux de Bouw-Wewers [BW] basés sur [Ra].

Classiquement nous travaillerons avec un corps k fixé, de caractéristique p et algébriquement clos ; $R = W(k)[\zeta]$ désignera l'extension de l'anneau des vecteurs de Witt de k par une racine primitive p-ème de l'unité. Nous notons $\lambda = \zeta - 1$ comme dans [OSS] ; c'est une uniformisante de R, et

$$p = v\lambda^{p-1}$$

où v est l'unité $(1+\zeta)(1+\zeta+\zeta^2)\dots(1+\dots+\zeta^{p-2})$. Introduisons enfin le polynôme de [OSS] :

$$\Theta(X) = (X+\lambda^{-1})^p - \lambda^{-p} = \sum_{i=1}^{p} \binom{p}{i} (\lambda^{-1})^{p-i} X^i \ ,$$

et son homogénéisé $\Theta(X,T) = T^p\Theta(X/T)$. Nous adoptons la définition

Définition 4.2.1 *Une famille de courbes de Potts à p états sur R est un triplet (C,σ,τ) de S-objets, $S \in (R)$, avec $C \to S$ projectif, lisse, $\sigma : C \to C$ d'ordre p, $\tau : C \to C$ involutif, tel que les fibres géométriques sont des courbes de Potts (C_s,σ_s,τ_s) au sens de la définition 0.1.ter.*

Nous ferons l'hypothèse supplémentaire que la catégorie des schémas de base est constituée des schémas localement de type fini, pour pouvoir appliquer des arguments de théorie des déformations. Ici le champ de Potts $\mathcal{P}$ est la catégorie dont les objets sont les familles de R-courbes de Potts sur S. Pour obtenir l'espace modulaire par la même construction que précédemment, le calcul d'invariants 4.1.2 qui est utilisé dans la démonstration de 4.1.3, n'est plus possible en caractéristique mixte, même (Zariski) localement sur la base. C'est l'étude de la déformation universelle d'une courbe de Potts sur k qui va nous permettre de conclure.

Proposition 4.2.2 *Toute courbe de Potts C sur k a une déformation infinitésimale universelle $\mathfrak{p} : \mathfrak{C} \to \mathfrak{s}$ sur l'anneau de séries formelles en une variable $\mathfrak{s} = \operatorname{Spec} R[[W]]$. En effectuant un extension quadratique R' de la base $R[[W]]$, $\mathfrak{p}$ est donnée par une équation $y^2 = \Theta(x)^2 + A\Theta(x) + B$, et en posant $j^* = \frac{B^*}{A^2-4B}$ (où $B^* = 1 - \lambda A + \lambda^2 B$), on peut en donner une forme isomorphe*

$$y^2 = \Theta(x)^2 - \frac{1}{\lambda^2 + 4j^*} \quad ;$$

l'invariant j^* se réduit sur l'invariant j de C.

Preuve : elle se fait en deux étapes.

1) L'existence de la déformation universelle est conséquence des critères de Schlessinger [BM, th. 2.1], et le calcul de l'anneau de déformation universel $R[[W]]$ est effectué dans [BM] dans un cas presque identique. Reprenons-le ici. Nous déformons un couple formé d'une courbe C/k et du groupe $G =< \sigma,\tau >$ d'ordre $2p$. Soit $\pi : C \to \Sigma = C/G$ le quotient. Ce sont les points de branchement (dans $\Sigma \simeq \mathbf{P}^1$) qui contribuent à la déformation, à savoir,

- le point image des 2 points fixes de σ, unique point de branchement sauvage, de stabilisateur $\mathbf{Z}/p\mathbf{Z}$,
- les 2 points images des σ-orbites de points fixes de τ ; les stabilisateurs sont cycliques de degré 2.

Par [BM, cor. 3.3.5], l'anneau de déformation est $R_1[[U_1,\dots,U_N]]$; l'anneau local de déformation au point de branchement sauvage, calculé dans [BM, th. 4.2.8], est $r = W(k)[[X]]/(\psi(X))$ où ψ est un certain polynôme donné dans le texte. Comme nous travaillons sur une base contenant une racine primitive p-ème de l'unité ζ et que $r = W(k)[\zeta+\zeta^{-1}-2] \subset W(k)[\zeta] = R$, on a $R_1 = r \otimes R = R$. D'autre part on peut reprendre le calcul de $N = \dim_k H^1(\Sigma, \pi_*^G(\mathcal{T}_C))$ en suivant la lecture de [BM, prop. 5.3.2] qui traite le cas $G \simeq \mathbf{Z}/p\mathbf{Z}$. Il faut noter que, dans l'énoncé et la démonstration de cette proposition, sont interverties systématiquement parties entières supérieures $\lceil\ \rceil$ et parties entières inférieures $\lfloor\ \rfloor$, comme nous l'ont mentionné les auteurs. En conservant leurs notations, on a

$$\pi_*^G(\mathcal{T}_C) \simeq \mathcal{T}_\Sigma \otimes (\mathcal{O}_\Sigma \cap \pi_*(\mathcal{O}_C(-\mathfrak{r})))$$

où $\mathfrak{r}$ est le diviseur de ramification sur C. En un point de branchement x_i, l'idéal de définition de $\mathfrak{r}$ a pour valuation l'exposant de la différente β_i :

- $\beta_i = 2(p-1)$ au point de branchement sauvage, car en ce point le conducteur est $m_i = 1$,
- $\beta_i = e_i - 1 = 1$ aux autres points de branchement, d'indice de ramification 2.

Il s'ensuit que $N = 3g_\Sigma - 3 + \sum_{i=1}^{r} \left\lceil \frac{\beta_i}{p} \right\rceil = 0 - 3 + 2 + 1 + 1 = 1$, comme annoncé.

2) Dans un deuxième temps, on forme le quotient $\mathfrak{E} = \mathfrak{C}/\tau$. Comme $R[[W]]$ est complet et local, on a l'injection des groupes de Brauer $\operatorname{Br}(R[[W]]) \hookrightarrow \operatorname{Br}(k)$ (cf [AG, cor. 6.2]) ; le second est nul car le corps résiduel k est algébriquement clos, et par suite, $\operatorname{Br}(R[[W]]) = 0$. Le groupe de Brauer classifie les classes d'isomorphisme de fibrés « de Severi-Brauer » [Gr] (ce sont les fibrés projectifs localement triviaux pour la topologie étale), aussi le fibré en droites projectives $\mathfrak{E} \to \mathfrak{s}$, est-il un fibré projectif $\mathbf{P}(\mathscr{Y})$ associé à un

faisceau localement libre de rang 2 sur $\mathfrak{s}$. En particulier $\mathscr{V}$ doit être libre sur un ouvert contenant le point fermé de $\mathfrak{s}$; le seul tel ouvert est $\mathfrak{s}$, donc on a $\mathfrak{E} \simeq \mathbf{P}^1 \times \mathfrak{s}$. L'automorphisme σ, agissant sur $\mathfrak{E}$, est une matrice de $\mathrm{PGL}_2(R[[W]])$, que nous allons réduire en mimant ce qui est fait dans la proposition 1.1 sur un corps.

Lemme 4.2.3 *Sur une extension quadratique $R' \supset R[[W]]$, $\sigma = \left[\begin{smallmatrix} \zeta & -1 \\ 0 & 1 \end{smallmatrix}\right]$ à conjugaison près.*

Preuve : Dans la fibre au-dessus du point fermé x de $\mathfrak{s}$, σ_x est conjugué à $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ par un élément $\gamma_x \in \mathrm{PGL}_2(k)$. N'importe quel γ relevant γ_x à $R[[W]]$ est inversible, et en faisant $\sigma \leftarrow \gamma^{-1}\sigma\gamma$ on se ramène à une situation où $\sigma_x = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, en particulier, a, b, d sont inversibles. Pour trouver un vecteur propre de σ on considère, comme dans 1.1, l'extension quadratique $R' = R[[W]][\delta]$ par une racine carrée δ de $\mathrm{tr}(\sigma)^2 - 4\det(\sigma) \in m_{R[[W]]}$. Soit $\mu = \frac{\mathrm{tr}(\sigma)+\delta}{2}$ l'une des valeurs propres, alors en conjuguant par $g = \left[\begin{smallmatrix} b & 0 \\ \mu - a & 1 \end{smallmatrix}\right]$ on se ramène à $\sigma = \left[\begin{smallmatrix} \mu & 1 \\ 0 & a+d-\mu \end{smallmatrix}\right] = \left[\begin{smallmatrix} \zeta & -\psi \\ 0 & 1 \end{smallmatrix}\right]$ où $\zeta = \mu/(a+d-\mu)$ et $-\psi = 1/(a+d-\mu)$. On observe que $\zeta^p = 1 \Rightarrow \zeta \in R$, aussi quitte à changer le choix de l'uniformisante de R, on suppose que ζ correspond bien à $\zeta = \lambda + 1 \in R$ fixé au départ. Enfin la condition exprimant que σ est d'ordre p : $(\zeta - 1, \psi) = R'$ montre que ψ est inversible, donc on peut conjuguer par $\left[\begin{smallmatrix} \psi & 0 \\ 0 & 1 \end{smallmatrix}\right]$ et obtenir finalement $\sigma = \left[\begin{smallmatrix} \zeta & -1 \\ 0 & 1 \end{smallmatrix}\right]$. ∎

Alors on a le résultat suivant (lemme 4.2.4). Soit $\mathcal{R}$ une R-algèbre intègre de caractéristique 0, et $\sigma \in \mathrm{Aut}_{\mathcal{R}}\mathcal{R}[X,T]$ l'automorphisme défini par $\sigma(T) = \zeta T$ et $\sigma(X) = X - T$ (extension à l'algèbre symétrique de l'endomorphisme linéaire ci-dessus).

Lemme 4.2.4 *La composante homogène de degré $2p$ de $(\mathcal{R}[X,T])^\sigma$ est le $\mathcal{R}$-module libre engendré par T^{2p}, $T^p\Theta(X,T)$ et $\Theta(X,T)^2$.*

Preuve : On remarque que σ se diagonalise dans $\mathrm{Frac}(\mathcal{R})$ avec le vecteur propre $Z = \lambda X + T$ relatif à la valeur propre 1. Ainsi, si $\mathcal{R}_{(\lambda)}$ désigne le localisé de $\mathcal{R}$ en λ,

$$(\mathcal{R}[X,T])^\sigma = \mathcal{R}[X,T] \cap \left(\mathcal{R}_{(\lambda)}[X,T]\right)^\sigma = \mathcal{R}[X,T] \cap \left(\mathcal{R}_{(\lambda)}[Z,T]\right)^\sigma = \mathcal{R}[X,T] \cap \mathcal{R}_{(\lambda)}[Z][T^p]\,,$$

où la dernière égalité est un simple argument de théorie de Galois dans le corps des fractions de $\mathcal{R}_{(\lambda)}[Z]$. Soit donc $P \in \mathcal{R}[X,T]$ homogène de degré $2p$ et σ-invariant ; a priori on a

$$P(X,T) = a\,T^{2p} + b\,T^p(\lambda X + T)^p + c\,(\lambda X + T)^{2p}$$

avec $a, b, c \in \mathcal{R}_{(\lambda)}$. En particulier les coefficients de T^{2p}, T^pX^p et X^{2p} sont dans $\mathcal{R}$, à savoir, respectivement,

$$\mathbf{a} = a + b + c\,, \quad \mathbf{b} = (b + c\binom{2p}{p})\lambda^p \quad \text{et} \quad \mathbf{c} = c\,\lambda^{2p}\,.$$

Par suite,

$$c = \frac{\mathbf{c}}{\lambda^{2p}}\,, \quad b = \frac{\mathbf{b}}{\lambda^p} - \frac{\mathbf{c}}{\lambda^{2p}}\binom{2p}{p} \quad \text{et} \quad a = \mathbf{a} - \frac{\mathbf{b}}{\lambda^p} + \frac{\mathbf{c}}{\lambda^{2p}}\left(\binom{2p}{p} - 1\right).$$

Avant de poursuivre, observons qu'il existe $n \in \mathbf{Z}_{\geq 0}$ tel que $\binom{2p}{p} = 2 + p^2 n$. En effet, on a

$$\binom{2p}{p} - 2 = \frac{2}{(p-1)!}\Big((2p-1)\ldots(p+1) - (p-1)!\Big) = \frac{2}{(p-1)!}\left(\prod_{j=1}^{p-1}(p+j) - \prod_{j=1}^{p-1} j\right),$$

or, dans la parenthèse, vue comme polynôme en p, le coefficient constant est nul, et le coefficient de p : $\sum_{j=1}^{p-1}\frac{(p-1)!}{j}$, est lui-même multiple de p, car son image modulo p est $\sum_{x\in\mathbf{F}_p^*} x = 0$.

En écrivant $p = v\lambda^{p-1}$ et $\binom{2p}{p} = 2 + p^2 n = 2 + v^2\lambda^{2p-2}n$, on reporte les expressions de a, b, c et on obtient

$$P(X,T) = \mathbf{a}\,T^{2p} + \mathbf{b}\,T^p\,\Theta(X,T) + \mathbf{c}\,\Theta(X,T)\Big[\Theta(X,T) - nv^2\lambda^{p-2}\,T^p\Big]\,;$$

les coefficients sont alors dans $\mathcal{R}$, d'où le résultat. ∎

Rappelons que la donnée du quotient $\mathfrak{C} \to \mathfrak{E}$ est équivalente à celle d'un triplet $(\mathfrak{E}, \mathscr{L}, \theta)$ où $\mathscr{L} \simeq \mathcal{O}_{\mathbf{P}^1 \times \mathfrak{s}}(-2)$ et $\theta \in \Gamma(\mathfrak{E}, \mathcal{O}_{\mathfrak{E}}(2p))^{\sigma}$. Compte tenu du calcul précédent pour $\mathcal{R} = R'$, on a

$$\theta = U\Theta(X,T)^2 + AT^p\Theta(X,T) + BT^{2p}$$

pour des sections $U, A, B \in R'$. Comme précédemment (4.1.3) on normalise U à 1. On peut encore rigidifier la donnée $(\mathfrak{E}, \mathscr{L}, \theta)$ en examinant les automorphismes de $\mathbf{P}^1_{\mathfrak{s}}$ qui agissent trivialement dessus, c'est-à-dire, ceux qui préservent θ. Déshomogénéisons en faisant $T = 1$; les automorphismes en question sont les changements de variable sur X qui commutent à σ, et il est facile de voir qu'il s'agit des changements de la forme $X \mapsto \alpha.X = (1+\lambda\alpha)X + \alpha$, $\alpha \in R'$. En d'autres termes le groupe $\mathrm{Aut}(\mathfrak{E}, \mathscr{L}, \theta)$ cherché est le schéma en groupes affine

$$\mathcal{G}^{(\lambda)} = \mathrm{Spec}(R[x, 1/(\lambda x + 1)]) \,,$$

dont la multiplication est donnée, sur les points à valeurs dans une R-algèbre S :

$$\mathcal{G}^{(\lambda)}(S) = \{\, s \in S \,|\, \lambda s + 1 \in S^{\times} \,\} \,,$$

par $s.t = \lambda st + s + t$. L'action de $\mathcal{G}^{(\lambda)}$ sur les polynômes (i.e. les fonctions de $\mathbf{P}^1$) provient de

$$\begin{array}{ccc} \mathcal{G}^{(\lambda)}(S) \times \mathbf{P}^1(S) & \to & \mathbf{P}^1(S) \\ (s, x) & \mapsto & s.x = \lambda sx + s + x \end{array}$$

L'action correspondante (notée :) sur A et B est

$$\alpha : (A,B) \;=\; \left(\frac{A + 2\alpha}{u}, \frac{B + \alpha A + \alpha^2}{u^2} \right)$$

où $u = (1 + \lambda\alpha)$. Elle est diagonale sur les variables

$$\left\{ \begin{array}{l} A^* = \lambda A - 2 \\ B^* = 1 - \lambda A + \lambda^2 B \end{array} \right.$$

et précisément $\alpha : (A^*, B^*) = (A^*/u, B^*/u^2)$; par ailleurs $\lambda^{-2}(A^{*\,2} - 4B^*) = A^2 - 4B =: \Delta$.

Compte tenu du fait que $\mathfrak{C} \otimes k = C$, Δ est inversible car il se réduit sur le discriminant de C, qui est non nul. Donc les « paramètres » de θ vivent dans $\mathfrak{R} = R\left[A, B, \frac{1}{\Delta}, \frac{1}{B^*}\right]$. Le choix d'un nouvel invariant découle du calcul de l'algèbre des invariants :

Lemme 4.2.5 *On a* $\mathfrak{R}^{\mathcal{G}^{(\lambda)}(R)} = R\big[j^*, 1/j^*\big]$ *, où* $j^* = \frac{B^*}{A^2 - 4B} \in \mathfrak{R}^{\times}$.

Preuve : Il est clair que $\mathfrak{R} = R\big[A, \Delta, \frac{1}{\Delta}, j^*, \frac{1}{j^*}\big]$; par ailleurs $R\big[j^*, \frac{1}{j^*}\big]$ est clairement invariant. Soit donc $P = P(A, \Delta)$ un polynôme à coefficients dans $R\big[j^*, \frac{1}{j^*}\big]$ en A, Δ et $1/\Delta$. Ecrivons-le comme somme de ses composantes homogènes en degrés pondérés (1,2) pour A, Δ :

$$P = P_m + P_{m+1} + \ldots + P_n \,, \quad n \geq m \;\text{ entiers relatifs.}$$

Alors, $\alpha.P = P$ si et seulement si

$$P_m + \ldots + P_n = P_m\big(\frac{A + 2\alpha}{u}, \frac{\Delta}{u^2}\big) + \ldots + P_n\big(\frac{A + 2\alpha}{u}, \frac{\Delta}{u^2}\big)$$

en regardant P_n on voit qu'alors nécessairement $u^n = (1+\lambda\alpha)^n = 1$; ceci ne peut être vrai pour tout α que si $n = 0$ (R est intègre). Ensuite, en considérant le degré minimal, on voit que P_m doit être indépendant de A, puis que $u^m = 1$ là encore ; donc $m = 0$ et P est constant. ∎

En effectuant le changement de variables sur X donné par $\alpha = -A/2$, on obtient la nouvelle description

$$y^2 = \Theta(x)^2 - \frac{1}{\lambda^2 + 4j^*}$$

pour $\mathfrak{p}$, ce qui clôt la démonstration de 4.2.2. ∎

En corollaire de cette étude on a le résultat :

Théorème 4.2.6 *Le champ $\mathcal{P}$ est un champ algébrique de Deligne-Mumford, et il existe un morphisme $\Phi : \mathcal{P} \to (\mathbf{A}^1_*)$ qui fait de $\mathbf{A}^1_{*,R}$ un espace modulaire grossier pour les courbes de Potts à p états sur R.*

Preuve : Soit une R-courbe de Potts à p états $p : C \to S$. On souhaite d'abord définir un morphisme $j : S \to \mathbf{A}^1_*$, c'est-à-dire une section globale inversible de $\mathcal{O}_S$; on définit ce morphisme étale localement sur S. Appliquons les théorèmes d'algébrisation d'Artin [Ar1] pour le foncteur $F : (R\text{−Alg}) \to (\text{Ens})$ des R-courbes de Potts (de base le spectre d'une algèbre donnée). Par le théorème d'algébrisation [Ar1, 1.6], la déformation formelle universelle et effective $\mathfrak{p}$ de $C_s \otimes k$ est algébrisable, c'est-à-dire, est la complétée formelle d'une courbe $\mathscr{C}$ sur une R-algèbre de type fini $\mathscr{R}$.

Revenons à notre famille de départ $p : C \to S$, ou plutôt à p_s qui s'en déduit par le changement de base $\operatorname{Spec} \mathcal{O}_{S,s} \to S$. Par hypothèse ($\mathcal{O}_{S,s}$ de type fini sur R), p_s est une déformation algébrique de $C_s \otimes k$; par versalité, elle provient localement de $\mathscr{C}$ par un morphisme local pour la topologie étale. Cela veut dire qu'on a un morphisme $\mathscr{R} \to \tilde{R}$ à valeurs dans une $\mathcal{O}_{S,s}$-algèbre étale $\tilde{R}$. Enfin par théorie de la descente, les morphismes définis sur les ouverts étales $\operatorname{Spec} \tilde{R}$ de S :

$$\operatorname{Spec} \tilde{R} \to \operatorname{Spec} \mathscr{R} \to \mathbf{A}^1_*$$

se recollent en $S \to \mathbf{A}^1_*$: le morphisme classifiant est construit. Il reste à montrer la propriété universelle de l'espace modulaire ; ici un argument direct nous permettra de le déduire de l'algébricité du champ.

Pour montrer que $\mathcal{P}$ est algébrique on observe d'abord que le morphisme diagonal $\Delta : \mathcal{P} \to \mathcal{P} \times_R \mathcal{P}$ est représentable et non ramifié (donc, quasi-compact et séparé). Cela découle directement du fait que le schéma $\mathbf{Isom}_X$, qui représente le pullback par Δ d'un point schématique $X \to \mathcal{P} \times_R \mathcal{P}$, est fini et non ramifié sur X [DM].

Ensuite on doit construire un atlas étale surjectif $U \to \mathcal{P}$, où U est un schéma sur R. Faisons-le localement. Soit

$$x : \operatorname{Spec} k \to \mathcal{P}$$

un point géométrique de $\mathcal{P}$; c'est une courbe de Potts C_k sur k. Comme on vient de le voir (remplacer $\mathcal{O}_{S,s}$ par k), les théorèmes d'Artin fournissent une courbe de Potts $\tilde{C}$ sur une k-algèbre étale $\tilde{R}$, et telle que $\tilde{C}$ est verselle en x. Par ailleurs, la propriété de versalité étant ouverte [Ar2, 4.4], on peut supposer que $\tilde{C}$ est verselle en tout point de $\operatorname{Spec} \tilde{R}$. Ainsi on obtient un recouvrement étale local $\operatorname{Spec} \tilde{R} \to \mathcal{P}$ en x, et donc, par recollement (propriétés de champ), un atlas $U \to \mathcal{P}$.

Revenons à la propriété universelle laissée de côté ci-dessus. Par [KeMo, cor 1.3] $\mathcal{P}$ a un espace modulaire grossier M, et il est facile de voir que c'est un schéma. Par définition le morphisme $\Phi : \mathcal{P} \to (\mathbf{A}^1_*)$ factorise donc par $\mathcal{P} \to (M)$; par 3.1.1 et 4.1.3 le morphisme en question $f : M \to \mathbf{A}^1_*$ est un isomorphisme à la fois au-dessus de la fibre générique de R, et au-dessus de sa fibre spéciale. En particulier f est bijectif. Une composante irréductible de M est envoyée dans une composante irréductible de $\mathbf{A}^1_*$; par bijectivité et comme $\mathbf{A}^1_*$ est irréductible, M l'est aussi. En conclusion f est bijectif, birationnel, quasi-fini, et $\mathbf{A}^1_*$ est normal donc le Théorème Principal de Zariski s'applique et f est un isomorphisme. ■

On peut maintenant établir le résultat de réduction de l'espace modulaire des courbes de Potts à p états sur R :

Théorème 4.2.7 *La fibre spéciale de l'espace modulaire $\mathbf{P}_R$ est isomorphe à $\mathbf{P}_k$, c'est-à-dire que le morphisme de réduction $\mathcal{P}_R \to \mathcal{P}_k$ (changement de base par $\operatorname{Spec} k \to \operatorname{Spec} R$), entre champs de courbes de Potts à p états, rend le carré suivant commutatif :*

$$\begin{array}{ccc} \mathcal{P}_R & \xrightarrow{red} & \mathcal{P}_k \\ \downarrow & & \downarrow \\ \mathbf{P}_R & \longrightarrow & \mathbf{P}_k \end{array}$$

Preuve : Soit $p : C \to S$ une R-courbe de Potts à p états. Par définition, la famille fibre $p_k : C \otimes k \to S \otimes k$ au-dessus du point fermé de $\operatorname{Spec}(R)$ est une famille de courbes de Potts à p états sur k. On a défini les invariants $j_R = j(p)$ et $j_k = j(p_k)$, et l'énoncé du théorème siginifie que $j_k = j_R \otimes k$, c'est-à-dire que le diagramme suivant (pullback par $\operatorname{Spec}(k) \to \operatorname{Spec}(R)$) est cartésien :

$$\begin{array}{ccc} S \otimes k & \xrightarrow{j_k} & \mathbf{A}^1_*(k) \\ \downarrow & & \downarrow \\ S & \xrightarrow{j_R} & \mathbf{A}^1_*(R) \end{array}$$

Or, il suffit de le vérifier localement pour la topologie étale sur S : c'est donc résultat de l'algébrisation de la déformation universelle (démonstration de 4.2.6) et de la proposition 4.2.2. ■

Références

[AG] M. Auslander, O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97**, 367-409, 1960.

[Ar1] M. Artin, *Algebrization of formal moduli I*, Global Analysis, papers in honor of K. Kodaira, Spencer and Iyanaga Eds, Univ. of Tokyo Press, 21-71, 1969.

[Ar2] M. Artin, *Versal deformations and algebraic stacks*, Invent. Math. **27**, 165-189, 1974.

[Be] J. Bertin, *Compactification des schémas de Hurwitz*, C. R. Acad. Sci. Paris **322**, Série I, 1996 (+ preprint, même titre, 1996).

[BM] J. Bertin, A. Mézard, *Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques*, Invent. Math. **141**, 195-238, 2000.

[BW] I. Bouw, S. Wewers, *Reduction of covers and Hurwitz spaces*, prépublication électronique AG/0005120, 2000.

[DM] P. Deligne, D. Mumford, *The irreducibility of the space of curves of given genus*, Publ. Math. de l'IHES **36**, 75-109, 1969.

[Gr] A. Grothendieck, *Le groupe de Brauer I, II*, Séminaire Bourbaki n°290 et n°297, 1964/65/66.

[Ha] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.

[KL] S.L. Kleiman, K. Lønsted, *Basics on families of hyperelliptic curves*, Københavns Univ. Mat. Inst. Preprint Ser. 1977 no. 7, March 1977.

[KaMa] N. Katz, B. Mazur, *Arithmetic moduli of elliptic curves*, Ann. of Math. Stud. **108**, Princeton University Press, 1985.

[KeMo] S. Keel, S. Mori, *Quotients by groupoids*, Ann. Math., II. Ser. 145, No.1, 193-213, 1997.

[MS] D. Mumford, K. Suominen, *Introduction to the theory of moduli*, Algebraic Geometry, Oslo 1970, F. Oort, ed., Woltes-Noordhoff, Groningen, 1972.

[Mu1] D. Mumford, *Picard Groups of Moduli Problems*, Proc. Conf. on Arith. Alg. Geom. at Purdue, 1963.

[Mu3] D. Mumford, *Prym varieties I*, in Contributions to Analysis, Ahlfors, Kra, Maskit, Nirenberg Eds, Academic Press, 1974.

[OSS] T. Sekiguchi, F. Oort, N. Suwa, *On the deformation of Artin-Schreier to Kummer*, Ann. Scient. Ec. Norm. Sup. **22** 4ème série, 345-375, 1989.

[Ra] M. Raynaud, *Spécialisation des revêtements en caractéristique $p > 0$*, Ann. Scient. Ec. Norm. Sup. **32** 4ème série, 87-126, 1999.

[Ro] S-S. Roan, *A characterization of "rapidity" curve in the Chiral Potts Model*, Comm. Math. Phys. **145**, 605-634, 1992.

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

[SGA1] A. Grothendieck, *Revêtements étales et groupe fondamental*, LNM 224, Springer-Verlag, 1971.

[Su] M. Suzuki, *Group Theory I*, Springer-Verlag, 1980.

[We] S. Wewers, *Construction of Hurwitz spaces*, Thèse, prépublication n°21 de l'IEM, Essen, 1998.

courriel : matthieu.romagny@ujf-grenoble.fr

Université de Grenoble I
Institut Fourier
UMR 5582 CNRS-UJF
UFR de Mathématiques
B.P. 74
38402 Saint Martin d'Hères Cedex (France)